

在FMC上配置RAVPN证书身份验证和ISE授权

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[第1步：安装受信任CA证书](#)

[第2步：配置ISE/Radius服务器组和连接配置文件](#)

[第3步：配置ISE](#)

[第3.1步：创建用户、组和证书身份验证配置文件](#)

[第3.2步：配置身份验证策略](#)

[第3.3步：配置授权策略](#)

[验证](#)

[故障排除](#)

简介

本文档介绍如何为FMC上的CSF管理的RAVPN连接中的证书身份验证配置ISE服务器授权策略。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全防火墙(CSF)
- 思科安全防火墙管理中心(FMC)
- 思科身份服务引擎(ISE)
- 证书注册和SSL基础知识。
- 证书颁发机构 (CA)

使用的组件

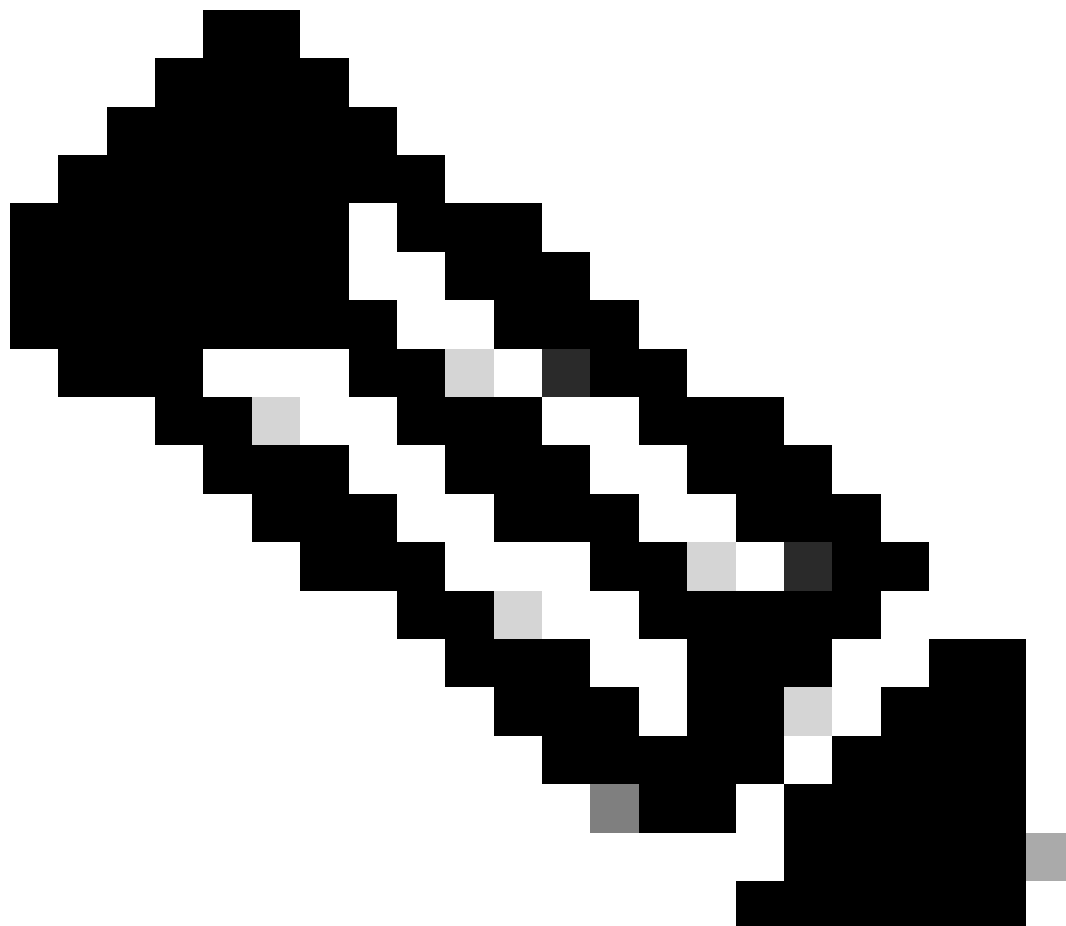
本文档的内容基于这些软件和硬件版本。

- 思科安全客户端5.1.6版
- 思科安全防火墙版本7.2.8
- 思科安全防火墙管理中心版本7.2.8

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。

配置

第1步：安装受信任CA证书



注意：如果CA证书与用于服务器身份验证的证书不同，则需要执行此步骤。如果同一CA服务器颁发用户证书，则无需再次导入同一CA证书。

Firewall Management Center
Devices / Certificates

Overview Analysis Policies **Devices** Objects Integration

Name	Domain	Enrollment Type	Status
FTD1			
cisco.com	Global	PKCS12 file	Server Certificate
InternalCA Server	Global	Manual (CA Only)	Internal CA certificate

- a. 导航至 `Devices > Certificates` 并单击 `Add`。
- b. 输入 `trustpoint name` 并在 CA 信息下选择 `Manual` 作为登记类型。
- c. 检查 `CA Only` 并粘贴以 `pem` 格式表示的受信任/内部 CA 证书。
- d. 选中 `Skip Check for CA flag in basic constraints of the CA Certificate` 并单击 `Save`。

Add Cert Enrollment ?

Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

CA Only
Check this option if you do not require an identity certificate to be created from this CA

CA Certificate:

```
-----BEGIN CERTIFICATE-----  
MIIB/  
zCCA WigAwIBAgIBATANBgkqhki  
G9w0BAQsFADATMREwDwYDV  
QQDEwhDQVNI  
cnZlclAeFw0yNDEwMTcxMDU5  
MDBaFw0yNTEwMjAxMDU5MDB  
aMBMxETAPBgNVBAMT  
CENBU2VydMvyMIGfMA0GCSq  
GS1b3DQEBAQUAA4GNADCBiQ  
KPaOC+IDQA2/wcPQW
```

Validation Usage: IPsec Client SSL Client SSL Server

Skip Check for CA flag in basic constraints of the CA Certificate

- e. 在 `Cert Enrollment` 下，从刚创建的下拉菜单中选择 `trustpoint`，然后单击 `Add`。

Add New Certificate



Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

Cert Enrollment*:

 +

Cert Enrollment Details:

Name:	InternalCAServer
Enrollment Type:	Manual (CA Only)
Enrollment URL:	N/A

Cancel

Add

第2步：配置ISE/Radius服务器组和连接配置文件

- 导航到Objects > AAA Server > RADIUS Server Group并单击Add RADIUS Server Group。选中Enable authorize only选项。



警告：如果未选中“仅启用授权”选项，则防火墙会发送身份验证请求。但是，ISE会随该请求接收用户名和密码，并且证书中未使用密码。因此，ISE将请求标记为身份验证失败。

Edit RADIUS Server Group



Name:*

ISE_Authorization

Description:

Group Accounting Mode:

Single

Retry Interval:* (1-10) Seconds

10

Realms:

Enable authorize only

Enable interim account update

Interval:* (1-120) hours

24

Enable dynamic authorization

Port:* (1024-65535)

b. 点击Add (+)图标，然后使用IP地址或主机名添加Radius server/ISE server。

Edit RADIUS Server



IP Address/Hostname:*

ISELocal

Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:* (1-65535)

1812

Key:*

•••••

Confirm Key:*

•••••

Accounting Port: (1-65535)

1813

Timeout: (1-300) Seconds

10

Connect using:

Routing Specific Interface

Default: Management/Diagnostic ▾ +

Redirect ACL:

▾ +

Cancel

Save

C. 导航至 **Devices > Remote Access configuration**。创建 new connection profile，并将身份验证方法设置为 Client Certificate Only。对于授权服务器，选择之前步骤中创建的授权服务器。

确保您选中 **Allow connection only if user exists in authorization database** 选项。此设置可确保只有在授权允许的情

况下才能完成与RAVPN的连接。

Edit Connection Profile ?

Connection Profile:*

Group Policy:* +
[Edit Group Policy](#)

Client Address Assignment **AAA** Aliases

Authentication

Authentication Method: Enable multiple certificate authentication

▼ Map username from client certificate

Map specific field

Primary Field: Secondary Field:

Use entire DN (Distinguished Name) as username

Authorization

Authorization Server: Allow connection only if user exists in authorization database

Accounting

来自客户端证书的Map Username是指从证书获取的信息以识别用户。在本例中，您将保留默认配置，但可根据用于识别用户的信息进行更改。

单击。Save

d. 导航至Advanced > Group Policies。单击右侧的Add (+)图标。

Firewall Management Center
Devices / VPN / Edit Advanced

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin | **SECURE**

FTD_PolicyVPN Save Cancel

Enter Description Policy Assignments (1)

Local Realm: None Dynamic Access Policy: None

Connection Profile Access Interfaces **Advanced**

AnyConnect Client Images
Address Assignment Policy
Certificate Maps
Group Policies
LDAP Attribute Mapping
Load Balancing
IPsec
Crypto Maps
IKE Policy
IPsec/IKEv2 Parameters

Group Policies
Group policy can be assigned to VPN user through connection profile or by RADIUS server during authentication.
Following are the group policies that are associated with this Remote Access VPN configuration. Add a group policy if it is required to be assigned by RADIUS server during authentication.

Name	Protocol	DNS Servers	VPN Filter
DfltGrpPolicy	SSL_IKEV2		
Marketing_Group	SSL_IKEV2		
IT_Group	SSL_IKEV2		

e. 创建group policies。根据组织组和每个组可以访问的网络，配置每个组策略。

Group Policy ?

Available Group Policy ↻ +

Search

DfltGrpPolicy

FTD1_GPCertAuth

FTD1_GPISE

FTD1_GPLocalFull

Add

Selected Group Policy

DfltGrpPolicy

Cancel OK

f. 在组策略上，执行特定于每个组的配置。可以添加标语消息以在连接成功后显示。

Add Group Policy



Name:*

IT_Group

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

Banner:

Maximum total size: 3999, Maximum characters in a line : 497.

In case of a line spanning more than 497 characters, split the line into multiple lines.

** Only plain text is supported (symbols '<' and '>' are not allowed)

IT Group

1

Cancel

Save

g. 选择左侧的group policies命令，然后单击Add将其移到右侧。此关键字指定配置中使用的组策略。

Group Policy



Available Group Policy  

Q Search

FTD1_GPCertAuth

FTD1_GPISE

FTD1_GPLocalFull


IT_Group

Marketing_Group

Add

Selected Group Policy

DfltGrpPolicy 

Marketing_Group 

IT_Group 

Cancel

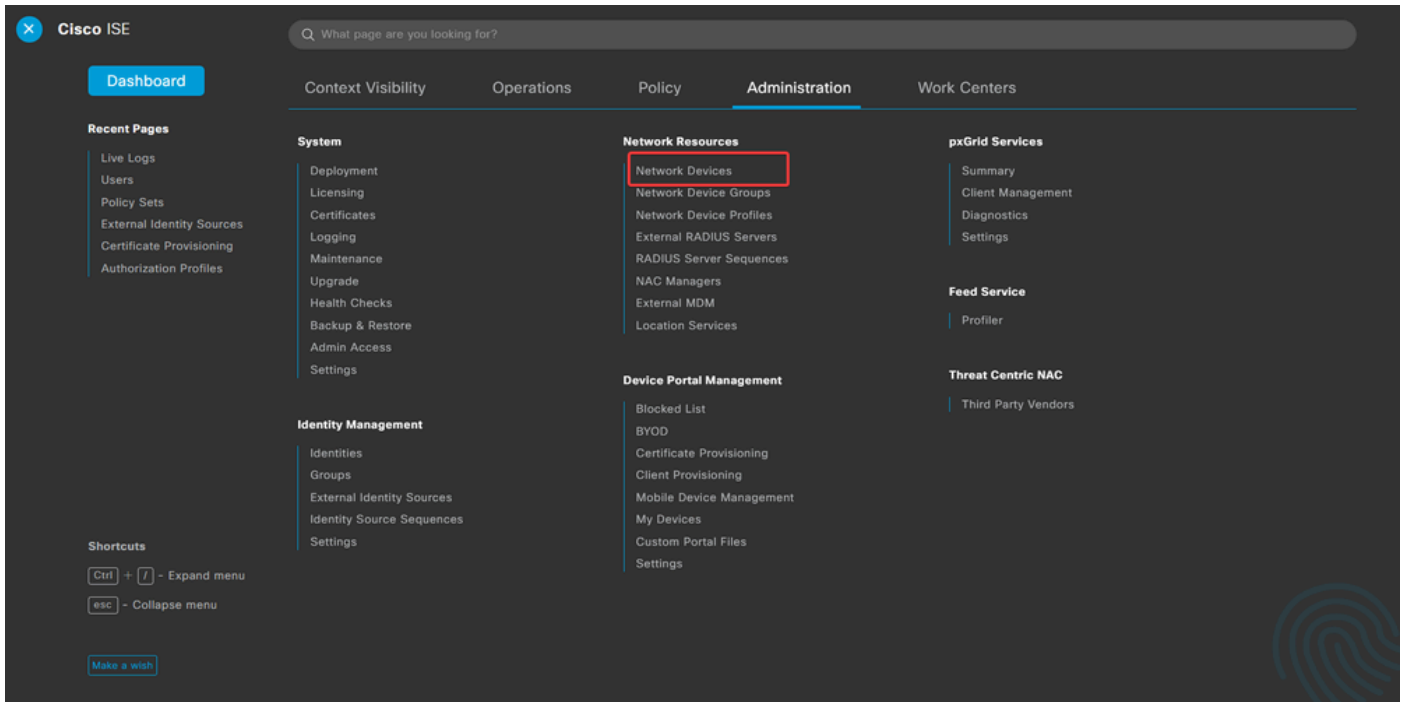
OK

e. 部署更改。

第3步：配置ISE

第3.1步：创建用户、组和证书身份验证配置文件

a. 登录到ISE服务器并导航至 **Administration > Network Resources > Network Devices**。



b. 单击Add将防火墙配置为AAA客户端。

Network Devices

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

c. 输入网络设备名称和IP地址字段，然后选中RADIUS Authentication Settings框并添加Shared Secret. 此值必须与在FMC上创建RADIUS服务器对象时使用的值相同。单击。 Save

[Network Devices List](#) > FTD

Network Devices

Name

Description

IP Address / 32

RADIUS Authentication Settings

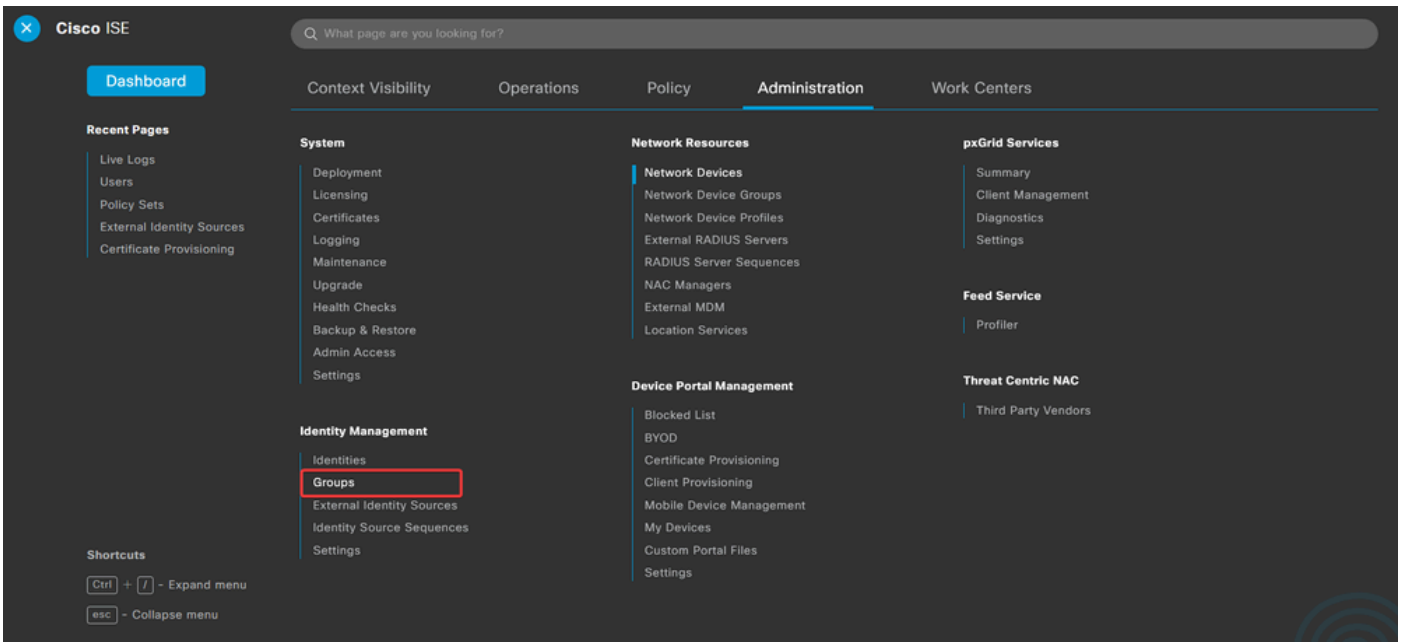
RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret Show

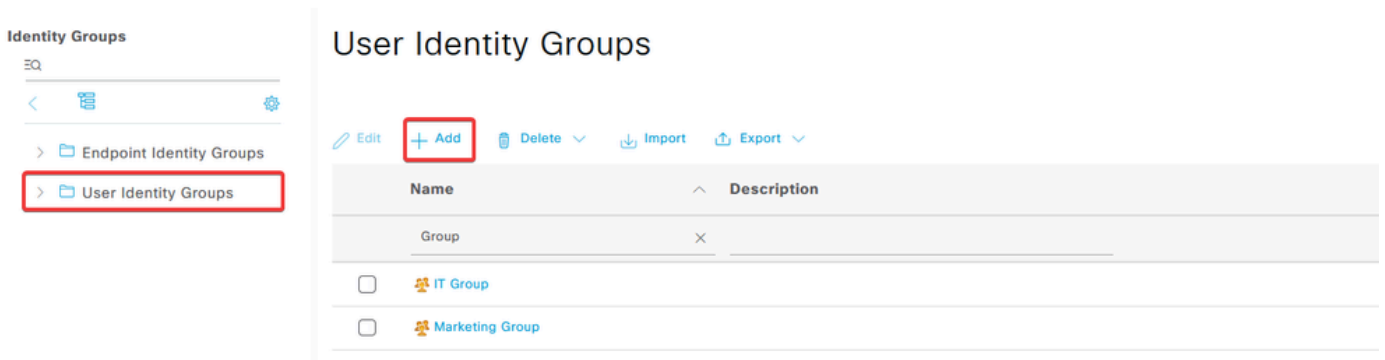
Use Second Shared Secret ⓘ

d. 导航至 Administration > Identity Management > Groups。



e. 单击 User Identity Groups，然后单击 Add。

输入 group Name，然后单击 Submit。



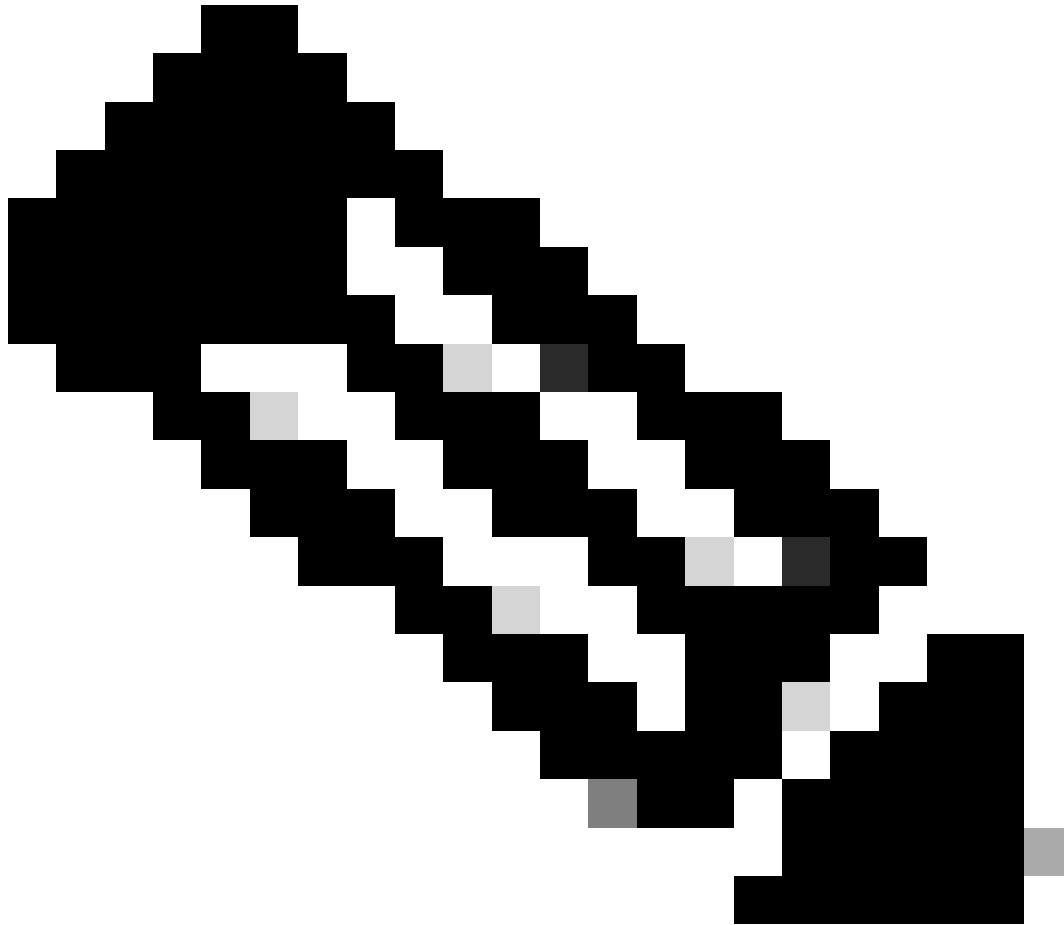
Identity Group

* Name

Description

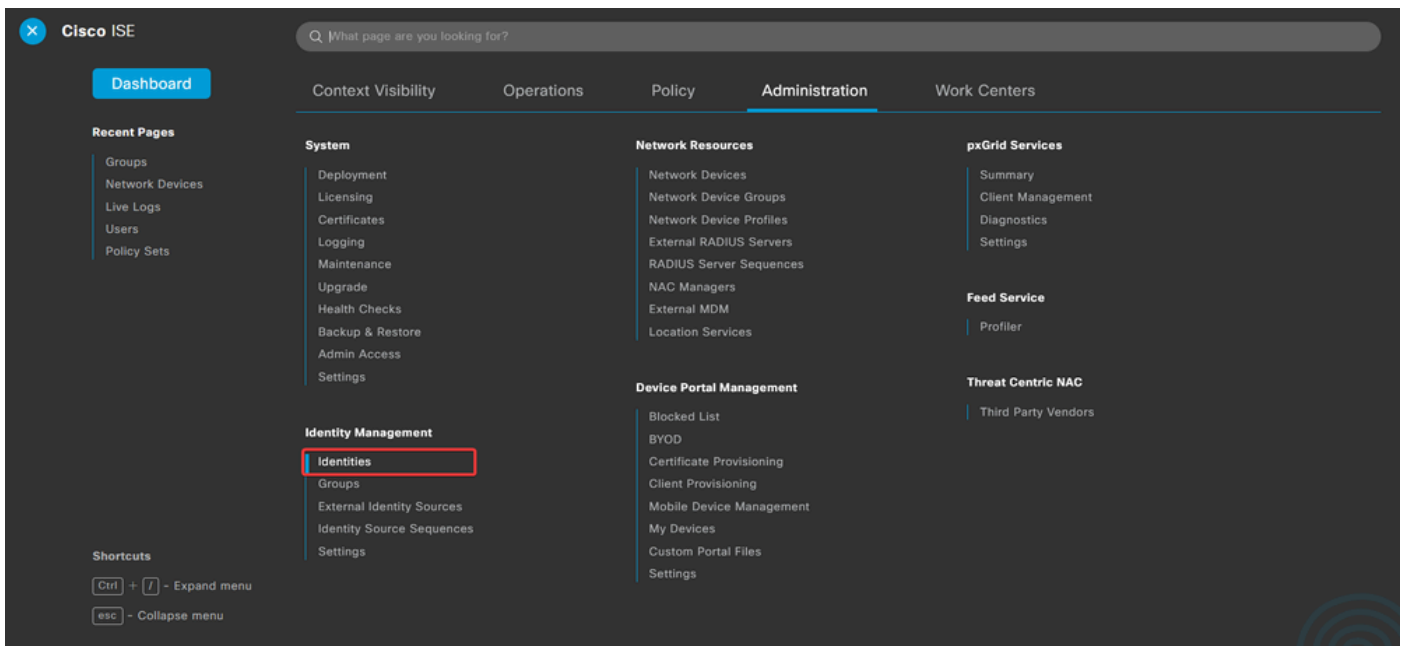
Submit

Cancel



注意：重复上述步骤可根据需要创建多个组。

d. 导航至 [Administration > Identity Management > Identities](#)。



e. 单击Add以便在服务器本地数据库中创建新用户。

输入Username和Login Password。然后，导航到此页末尾，选择User Group。

单击。Save

Network Access Users

Status	Username	Description	First Name	Last Name	Email Address	User Identity Grou...	Admin
<input type="checkbox"/>	Enabled	user1				IT Group	
<input type="checkbox"/>	Enabled	user2				Marketing Group	

Network Access User

* Username user1

Status Enabled

Email

Passwords

Password Type: Internal Users

Password Re-Enter Password
* Login Password

Generate Password ⓘ

Enable Password

Generate Password ⓘ

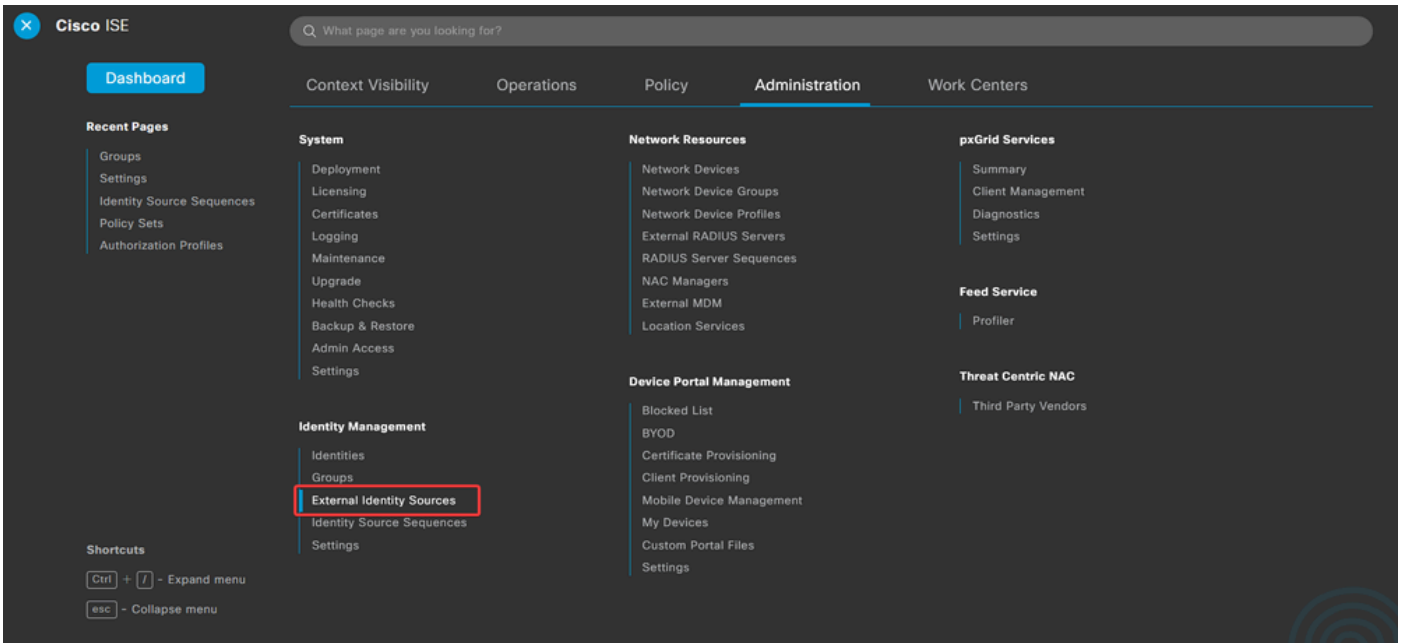
User Groups

IT Group



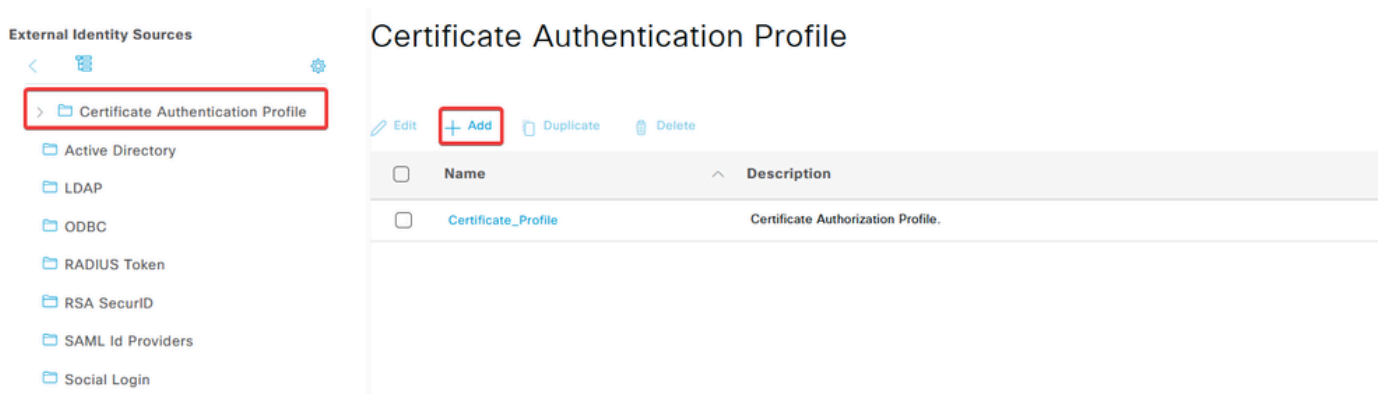
注意：必须配置用户名和密码才能创建内部用户。即使在使用证书执行的RAVPN身份验证中不需要此功能，这些用户也可以用于不需要密码的其他内部服务。因此，请确保使用强密码。

f. 导航至 **Administration > Identity Management > External Identify Sources**。



g. 单击Add创建Certificate Authentication Profile。

Certificate Authentication Profile指定如何验证客户端证书，包括可以检查证书中的哪些字段（Subject Alternative Name、Common Name等）。



Certificate Authentication Profile

* Name

Description

Identity Store

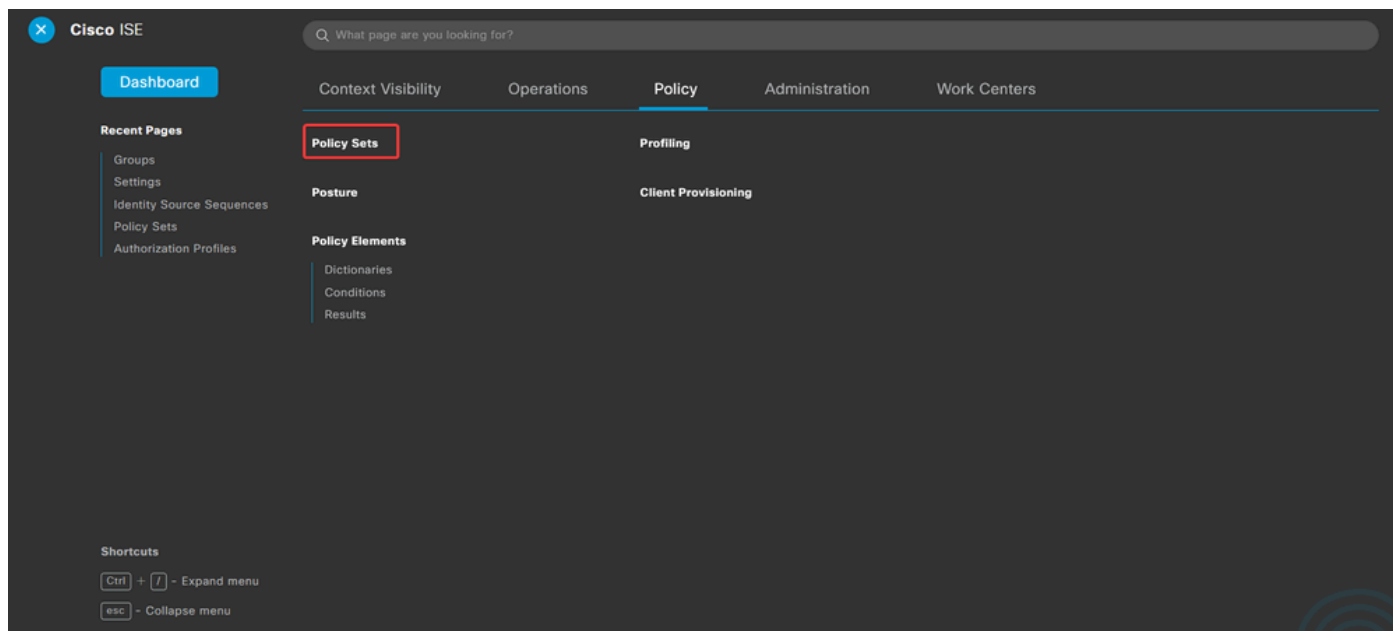
Use Identity From Certificate Attribute Subject - Common Name Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

Match Client Certificate Against Certificate In Identity Store Never Only to resolve identity ambiguity Always perform binary comparison

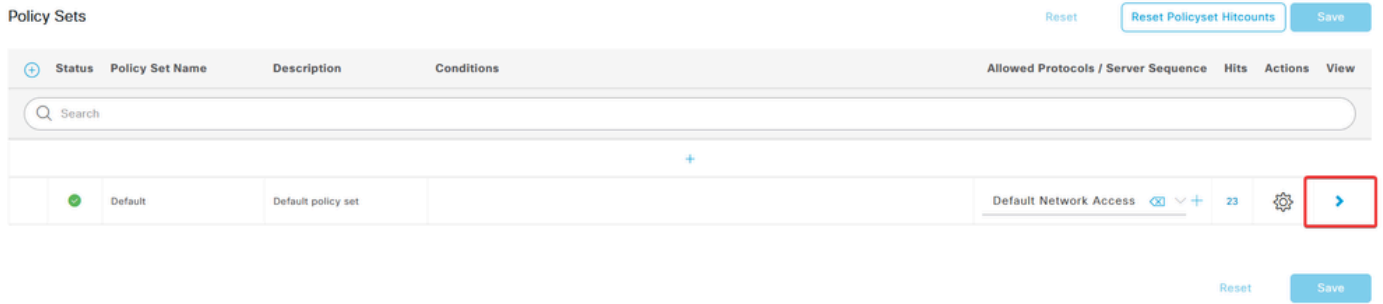
第3.2步：配置身份验证策略

身份验证策略用于验证请求是否来自防火墙和特定连接配置文件。

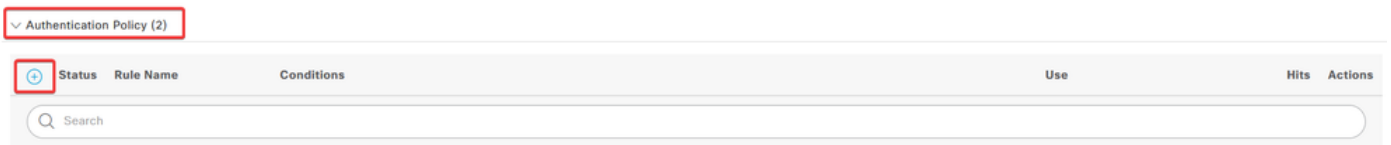
a. 导航至Policy > Policy Sets。



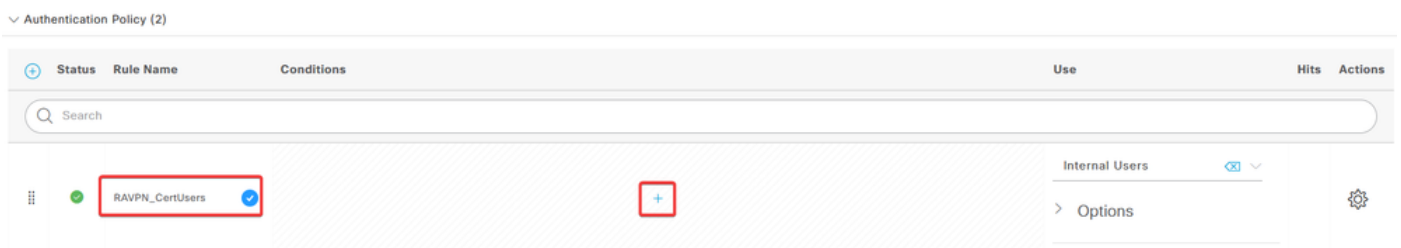
通过点击屏幕右侧的箭头选择默认授权策略：



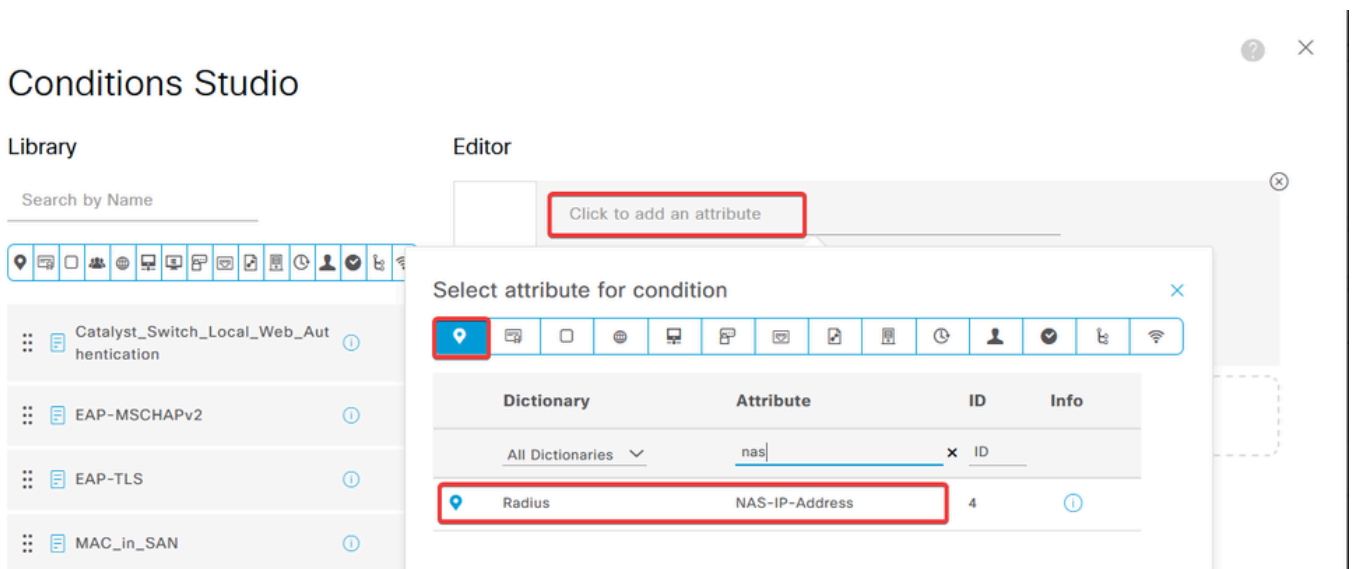
b. 点击Authentication Policy旁边的下拉菜单箭头将其展开。然后，点击add (+)图标添加新规则。



输入规则的名称，然后选择条件列下的add (+)图标。



c. 单击属性编辑器文本框并单击NAS-IP-Address图标。输入防火墙的IP地址。



d. 单击New然后添加另一个属性Tunnel-Group-name。输入在FMC上配置的名称Connection Profile。

Conditions Studio

Library

Search by Name



- Catalyst_Switch_Local_Web_Authentication
- EAP-MSCHAPv2
- EAP-TLS
- MAC_in_SAN
- Switch_Local_Web_Authentication
- Switch_Web_Authentication

Editor

Dictionary	Attribute	ID	Info
All Dictionaries	tunnel-group-name	x	
Cisco-VPN3000	CVPN3000/ASA/PIX7x-Tunnel-Group-Name	146	

Conditions Studio

Library

Search by Name



- Catalyst_Switch_Local_Web_Authentication
- EAP-MSCHAPv2
- EAP-TLS
- MAC_in_SAN
- Switch_Local_Web_Authentication

Editor

e.在“使用”列下，选择创建的Certificate Authentication Profile。通过执行此操作，可以指定配置文件中定义用于识别用户的信息。

Status	Rule Name	Conditions	Use	Hits	Actions
●	RAVPN_CertUsers	VerifyCertAuth	Certificate_Profile	7	Options

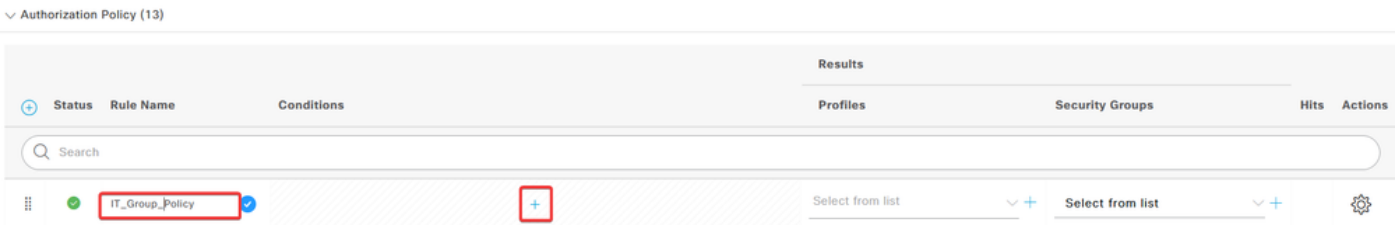
单击。Save

第3.3步：配置授权策略

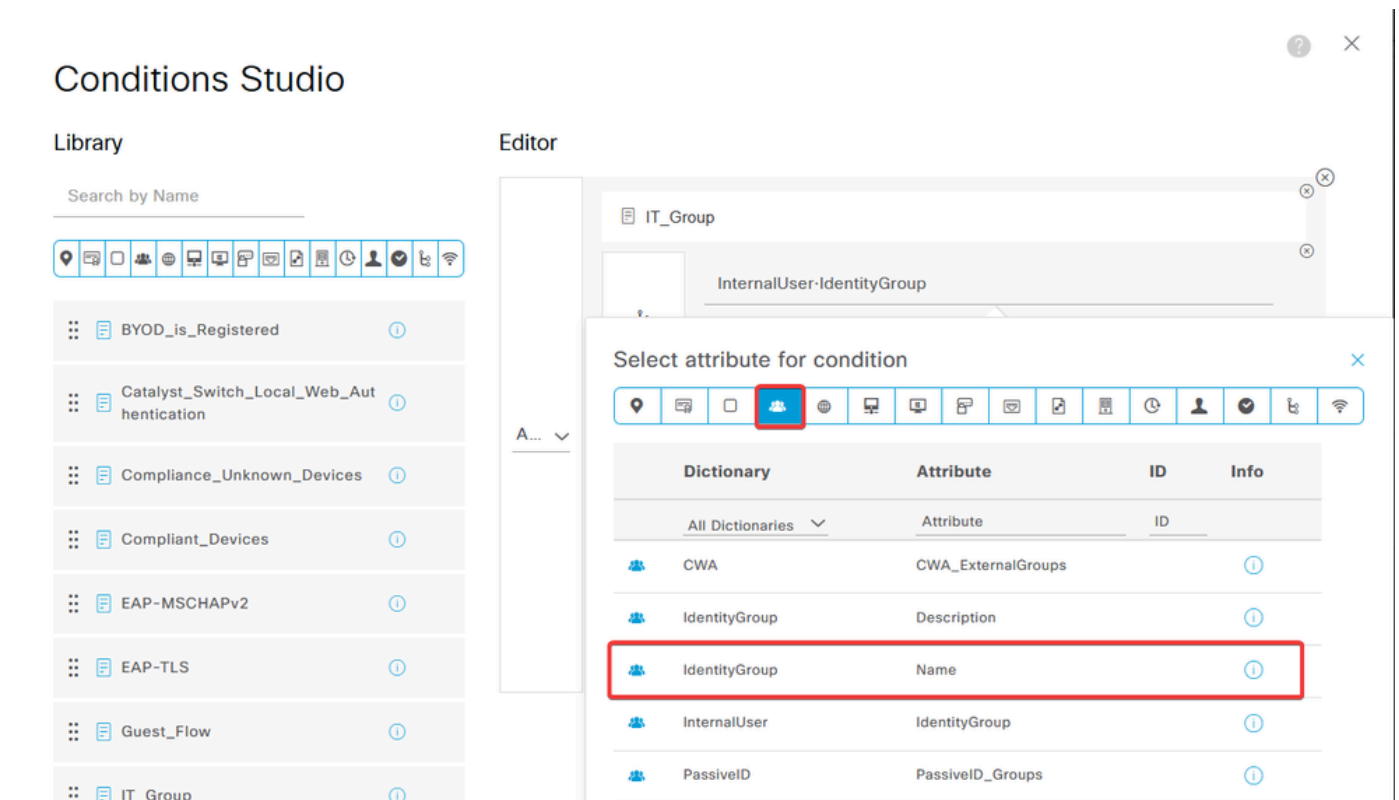
a. 点击Authorization Policy旁边的下拉菜单箭头将其展开。然后，点击add (+)图标添加新规则。



输入规则的名称，然后选择条件列下的add (+)图标。



b. 单击属性编辑器文本框并单击Identity group图标。选择Identity group - Name属性。



选择Equals作为运算符，然后单击下拉菜单箭头以显示可用选项并选择User Identity Groups:

o

Conditions Studio

Library

Search by Name

BYOD_is_Registered

Catalyst_Switch_Local_Web_Authentication

Compliance_Unknown_Devices

Compliant_Devices

EAP-MSCHAPv2

Editor

IT_Group

InternalUser-IdentityGroup

Equals

Choose from list or type

- User Identity Groups:GuestType_SocialLogin (default)
- User Identity Groups:GuestType_Weekly (default)
- User Identity Groups:IT Group
- User Identity Groups:Marketing Group
- User Identity Groups:OWN_ACCOUNTS (default)

Set to 'Is not'

c. 在配置文件列中，点击add (+)图标并选择Create a New Authorization Profile。

Authorization Policy (13)

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
●	IT_Group_Policy	AND IT_Group InternalUser-IdentityGroup EQUALS User Identity Groups:IT Group	Select from list	Select from list		⚙️
●	Wireless Black List Default	AND Wireless_Access IdentityGroup-Name EQUALS Endpoint Identity Groups:Blacklist	Create a New Authorization Profile	Select from list	0	⚙️

输入profile Name。

Authorization Profile

* Name: IT_Group_Profile

Description: [Empty text area]

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement: ⓘ

Agentless Posture: ⓘ

Passive Identity Tracking: ⓘ

导航到Common Tasks并选中ASA VPN。然后，键入group policy name，它需要与FMC上创建的相同。

∨ Common Tasks

ASA VPN

IT_Group



AVC Profile Name

UDN Lookup

下一个属性已分配给每个组：

∨ Attributes Details

Access Type = ACCESS_ACCEPT

Class = IT_Group

Click Save.

注意：重复第3.3步：为创建的每个组配置授权策略。

验证

1. 运行命令 `show vpn-sessiondb anyconnect` 并验证用户是否使用正确的组策略。

```
<#root>
```

```
firepower#
```

```
show vpn-sessiondb anyconnect
```

```
Session Type : AnyConnect
```

```
Username      : user1
```

```
Index         : 64
```

```
Assigned IP   : 192.168.55.2      Public IP     :
```

Protocol : AnyConnect-Parent
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none
Hashing : AnyConnect-Parent: (1)none
Bytes Tx : 15084 Bytes Rx : 99611
Group Policy : IT_Group Tunnel Group : FTD_CertAuth

Login Time : 22:21:43 UTC Tue Oct 22 2024
Duration : 3h:03m:50s
Inactivity : 0h:41m:44s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 96130a0f0004000067182577
Security Grp : none Tunnel Zone : 0

Username : User2

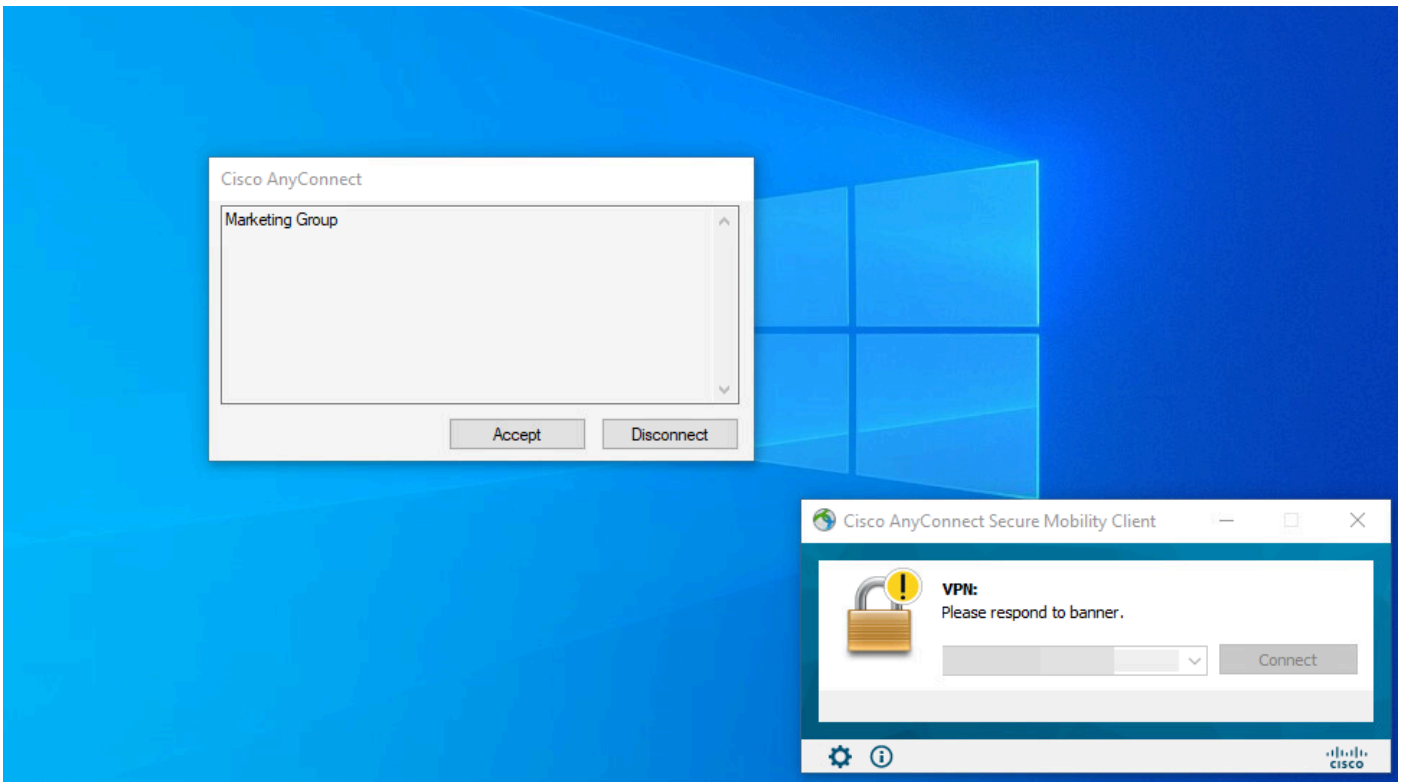
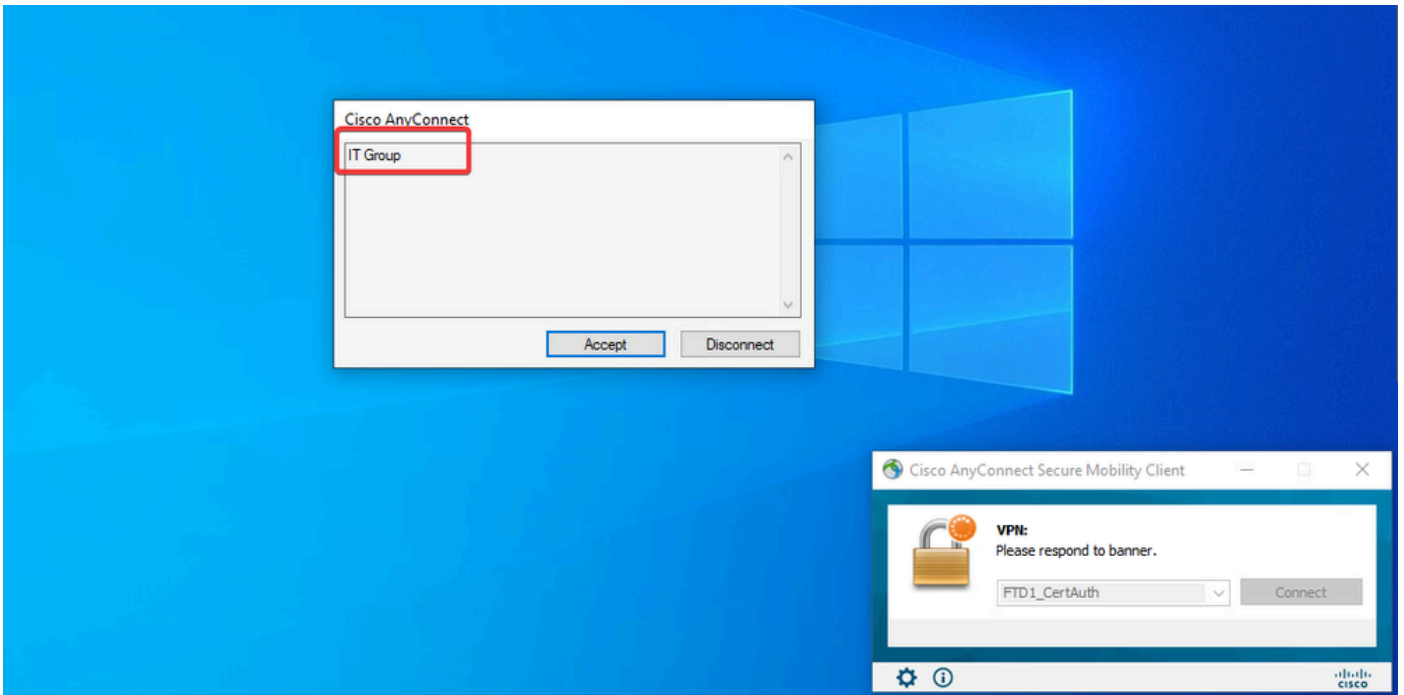
Index : 70

Assigned IP : 192.168.55.3 Public IP :
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx : 15112 Bytes Rx : 19738
Group Policy : Marketing_Group Tunnel Group : FTD_CertAuth

Login Time : 01:23:08 UTC Wed Oct 23 2024
Duration : 0h:02m:25s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 96130a0f0004600067184ffc
Security Grp : none Tunnel Zone : 0

firepower#

2. 在组策略中，可以配置在用户成功连接时显示的标语消息。每个标语都可用于标识拥有授权的组。



3. 在实时日志中，验证连接是否使用适当的授权策略。单击Details并显示身份验证报告。

Live Logs Live Sessions

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

Refresh: Never | Show: Latest 100 rec... | Within: Last 30 minu... | Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity G
Oct 25, 2024 08:38:03.6...	●	🔒	0	user1		Windows1...	Default	Default >>...	IT_Group_...				
Oct 25, 2024 08:38:03.6...	■	🔒		user1		Windows1...	Default	Default >>...	IT_Group_...		FTD		User Identit

Last Updated: Fri Oct 25 2024 14:42:41 GMT-0600 (GMT-06:00) Records Shown: 2

故障排除

本部分提供了可用于对配置进行故障排除的信息。

1. 可以从CSF的诊断CLI运行调试以进行证书身份验证。

```
debug crypto ca 14
debug webvpn anyconnect 255
debug crypto ike-common 255
```

2. 使用AAA调试验证本地和/或远程属性的分配。

```
debug aaa common 255
debug aaa shim 255
debug aaa authentication
debug aaa authorization
debug radius all
```

在ISE上：

1. 定位至Operations > RADIUS > Live Logs。

Cisco ISE Q What page are you looking for?

Dashboard | Context Visibility | **Operations** | Policy | Administration | Work Centers

Recent Pages

- Policy Sets
- Authorization Profiles
- Results
- External Identity Sources
- Groups

RADIUS

- Live Logs**
- Live Sessions

TACACS

- Live Logs

Adaptive Network Control

- Policy List
- Endpoint Assignment

Threat-Centric NAC Live Logs

Troubleshoot

- Diagnostic Tools
- Download Logs
- Debug Wizard

Reports

Shortcuts

- Ctrl + F** - Expand menu
- esc** - Collapse menu

Live Logs | Live Sessions

Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 0

Client Stopped Responding 3

Repeat Counter 0

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

Refresh | Reset Repeat Counts | Export To | Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity G
Oct 23, 2024 01:26:29.3...	✓	🔒		User2		Windows1...	Default	Default >>...	Marketing...		FTD		User Identit
Oct 23, 2024 01:22:29.3...	✗	🔒		User2					DenyAccess		FTD		User Identit
Oct 23, 2024 01:21:46.9...	✗	🔒		User2					DenyAccess		FTD		User Identit
Oct 23, 2024 01:16:33.4...	✗	🔒		User2					DenyAccess		FTD		User Identit
Oct 22, 2024 10:25:14.1...	✓	🔒		user1		Windows1...	Default	Default >>...	IT_Group_...		FTD		User Identit
Oct 22, 2024 10:24:18.9...	✓	🔒		user1		Windows1...	Default	Default >>...	IT_Group_...		FTD		User Identit

Last Updated: Wed Oct 23 2024 12:33:54 GMT-0600 (GMT-06:00) Records Shown: 6

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）。