

Configuración de la autorización de ISE y la autenticación de certificados RAVPN en FMC

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Paso 1: Instalación de un certificado de CA de confianza](#)

[Paso 2: Configuración del grupo de servidores ISE/Radius y el perfil de conexión](#)

[Paso 3: Configuración de ISE](#)

[Paso 3.1: Crear usuarios, grupos y perfiles de autenticación de certificados](#)

[Paso 3.2: Configurar la política de autenticación](#)

[Paso 3.3: Configuración de la política de autorización](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe la configuración de las políticas de autorización del servidor ISE para la autenticación de certificados en conexiones RAVPN administradas por CSF en FMC.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Firewall seguro de Cisco (CSF)
- Cisco Secure Firewall Management Center (FMC)
- Cisco Identity Services Engine (ISE)
- Conceptos básicos de Inscripción de certificados y SSL.
- Autoridad de certificación (CA)

Componentes Utilizados

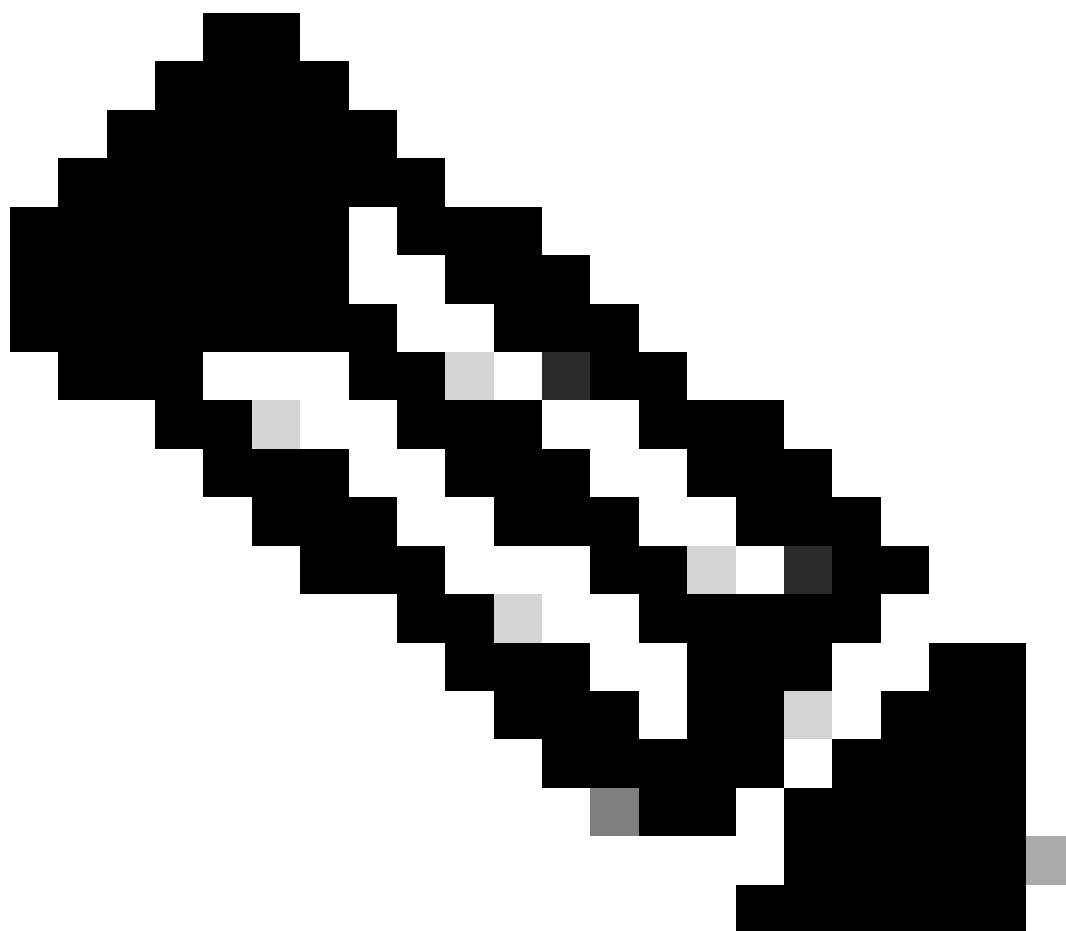
El contenido de este documento se basa en estas versiones de software y hardware.

- Cisco Secure Client versión 5.1.6
- Cisco Secure Firewall versión 7.2.8
- Cisco Secure Firewall Management Center versión 7.2.8

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Paso 1: Instalación de un certificado de CA de confianza



Nota: Este paso debe seguirse si el certificado de la CA es diferente del que se utiliza para la autenticación del servidor. Si el mismo servidor de la CA emite los certificados de los usuarios, no es necesario volver a importar el mismo certificado de la CA.



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

- Desplácese hasta **Devices > Certificates** y haga clic en **Add**.
- Ingrese un **trustpoint name** y seleccione **Manual** como el tipo de inscripción en **Información de CA**.
- Compruebe **CA Only** y pegue el certificado de CA interna/de confianza en formato pem.
- Marque **Skip Check for CA flag in basic constraints of the CA Certificate** y haga clic en **Save**.

Add Cert Enrollment



Name*

InternalCA Server

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

Manual

CA Only

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

CA Certificate:

```
-----BEGIN CERTIFICATE-----  
MIIB/  
zCCAWigAwIBAgIBATANBgkqhki  
G9w0BAQsFADATMREwDwYDVo  
QQDEwhDQVNI  
cnZlclAeFw0yNDEwMTcxMDU5  
MDBaFw0yNTEwMjAxMDU5MDBB  
aMBMxETAPBgNVBAMT  
CENBU2VydMvyMIGfMA0GCSq  
GS1b3DQEBAQUAA4GNADCBiQ  
KBgQC+IDQA2/wcPQWl
```

Validation Usage:

IPsec Client SSL Client SSL Server

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

Cancel

Save

e. En Cert Enrollment, seleccione el trustpoint de la lista desplegable que se acaba de crear y haga clic en 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

Paso 2: Configuración del grupo de servidores ISE/Radius y el perfil de conexión

a. Desplácese hasta **Objects > AAA Server > RADIUS Server Group** y haga clic en **Add RADIUS Server Group**. Marque la **Enable authorize only** opción.



Advertencia: si la opción Enable authorized only (Activar sólo autorización) no está activada, el firewall envía una solicitud de autenticación. Sin embargo, ISE espera recibir un nombre de usuario y una contraseña con esa solicitud, y no se utiliza una contraseña en los certificados. Como resultado, ISE marca la solicitud como error de autenticación.

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. Haga clic en el **Add (+)** icono y, a continuación, agregue el RADIUS server/ISE server mediante la dirección IP o un nombre de host.

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. Desplácese hasta **Devices > Remote Access configuration** . Cree un **new connection profile** y establezca el método de autenticación en **Client Certificate Only**. Para el servidor de autorización, elija el que se creó en los pasos anteriores.

Asegúrese de marcar la **Allow connection only if user exists in authorization database** opción. Esta configuración garantiza que la conexión a RAVPN se complete solo si se permite la autorización.

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

Map Username del certificado del cliente hace referencia a la información obtenida del certificado para identificar al usuario. En este ejemplo, se mantiene la configuración predeterminada, pero se puede cambiar en función de la información que se utilice para identificar a los usuarios.

Haga clic en **Save**.

d. Acceda a **Advanced > Group Policies**. Haga clic en el **Add (+)** icono de la derecha.

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. Cree el **group policies**. Cada política de grupo se configura en función de los grupos de organización y las redes a las que cada grupo puede acceder.

Group Policy ?

Available Group Policy ↻ +

🔍 Search

DfltGrpPolicy

FTD1_GPCertAuth

FTD1_GPISE

FTD1_GPLocalFull

Add

Selected Group Policy

DfltGrpPolicy 🗑️

Cancel OK

f. En la directiva de grupo, realice las configuraciones específicas de cada grupo. Se puede agregar un mensaje de banner para mostrarlo después de una conexión correcta.

Add Group Policy



Name:*

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. Seleccione el **group policies** en el lado izquierdo y haga clic **Add** para moverlo al lado derecho. Esto especifica qué políticas de grupo se están utilizando en la configuración.

Group Policy



Available Group Policy  

 Search

FTD1_GPCertAuth

FTD1_GPISE

FTD1_GPLocalFull


IT_Group

Marketing_Group

Add

Selected Group Policy

DfltGrpPolicy 

Marketing_Group 

IT_Group 

Cancel

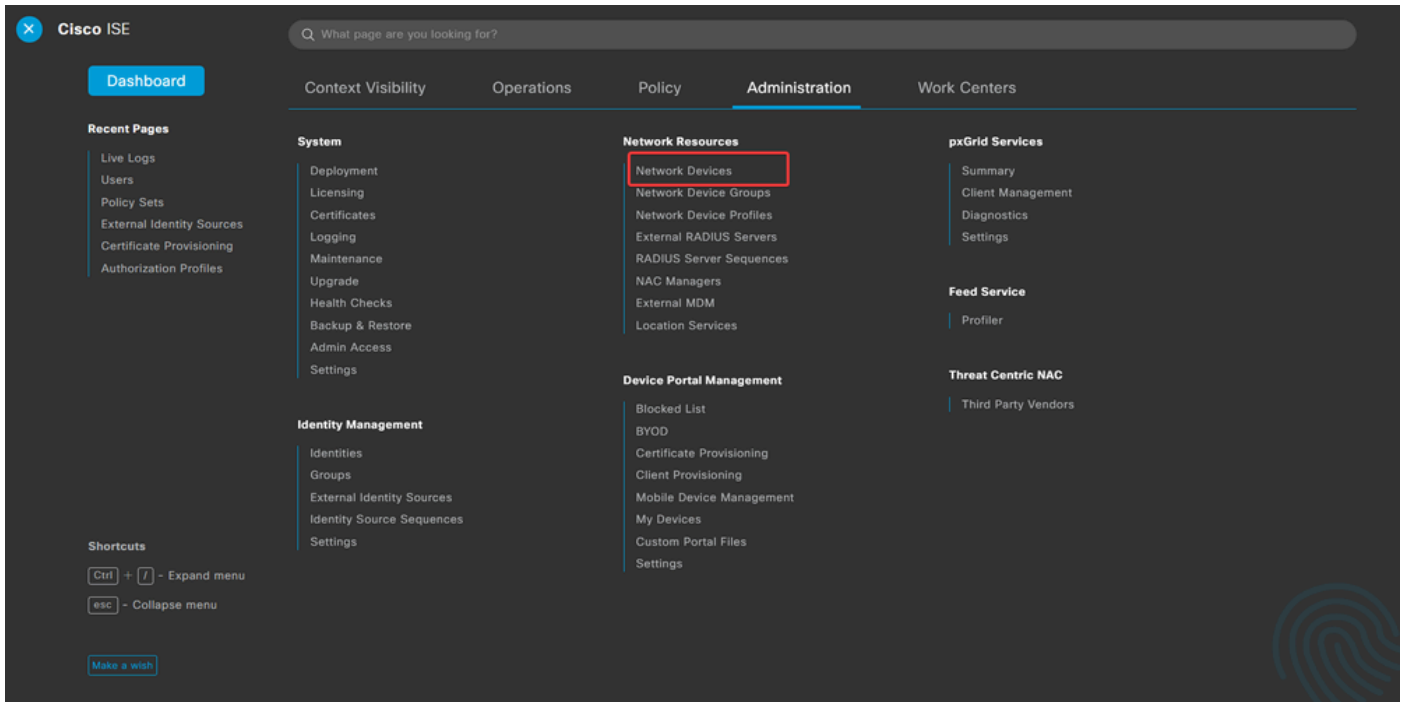
OK

e. Implementar los cambios.

Paso 3: Configuración de ISE

Paso 3.1: Crear usuarios, grupos y perfiles de autenticación de certificados

a. Inicie sesión en el servidor ISE y navegue hasta **Administration > Network Resources > Network Devices**.



b. Haga clic **Add** para configurar el firewall como cliente AAA.

Network Devices

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

c. Ingrese los campos Network Device Name y IP Address y luego marque la **RADIUS Authentication Settings** casilla y agregue el valor **shared Secret**. This debe ser el mismo que se utilizó cuando se creó el objeto RADIUS Server en FMC. Haga clic en **Save**.

[Network Devices List](#) > FTD

Network Devices

Name

Description

IP Address

RADIUS Authentication Settings

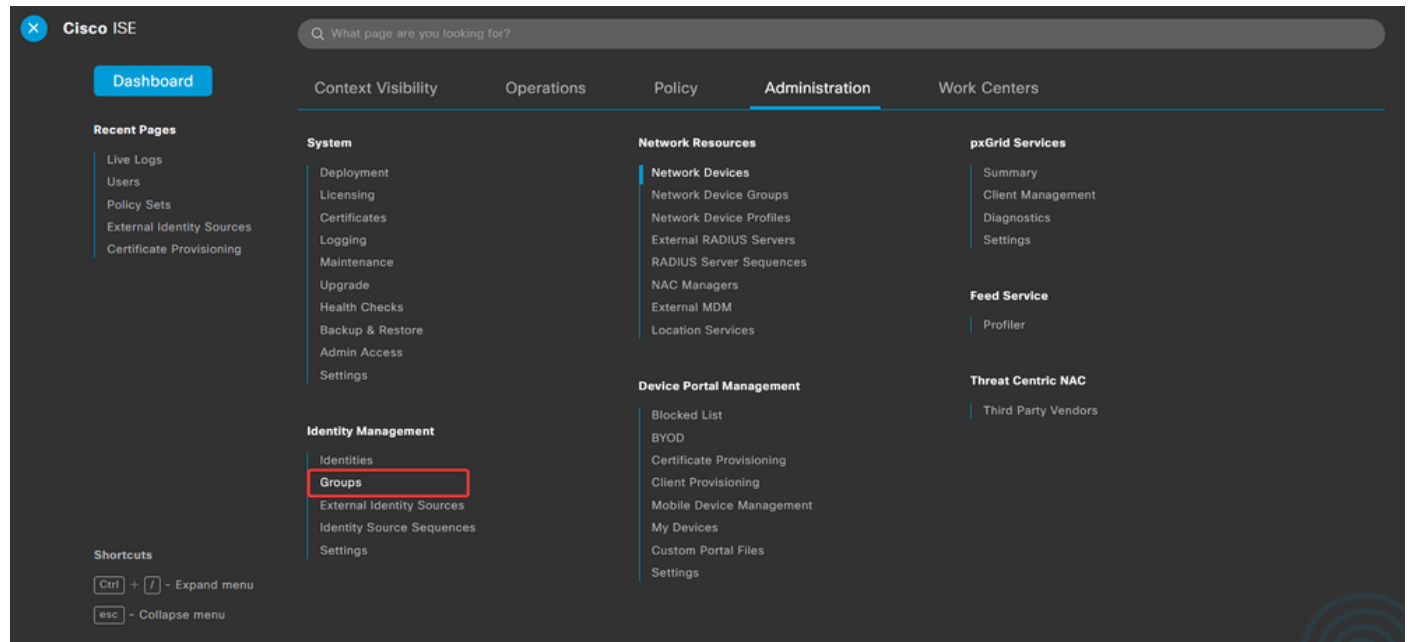
RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret [Show](#)

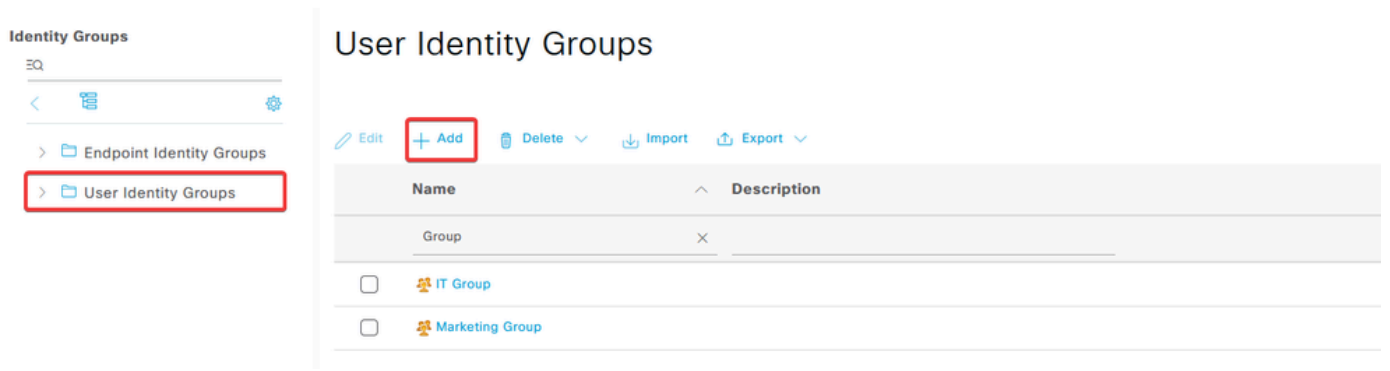
Use Second Shared Secret ⓘ

d. Acceda a Administration > Identity Management > Groups.



e. Haga clic en User Identity Groups, a continuación, haga clic en Add.

Introduzca el nombre del grupo y haga clic en Submit.



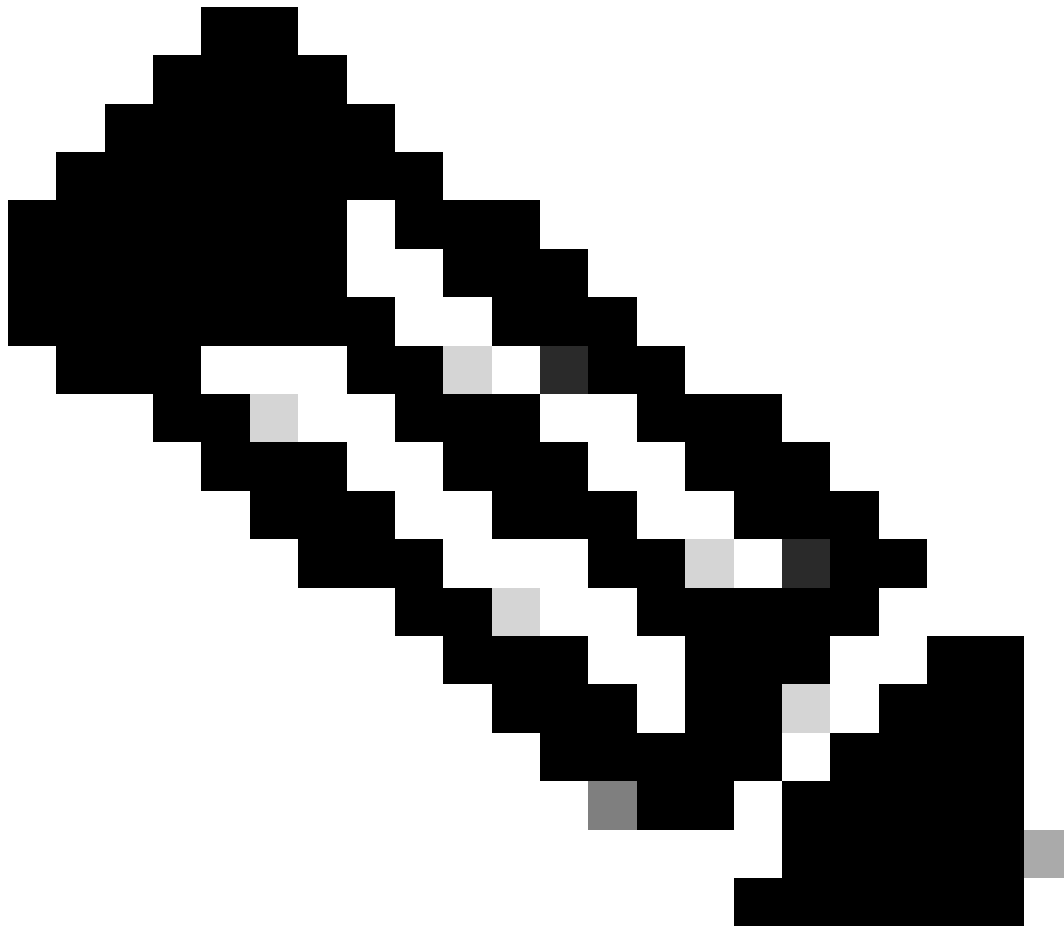
Identity Group

* Name

Description

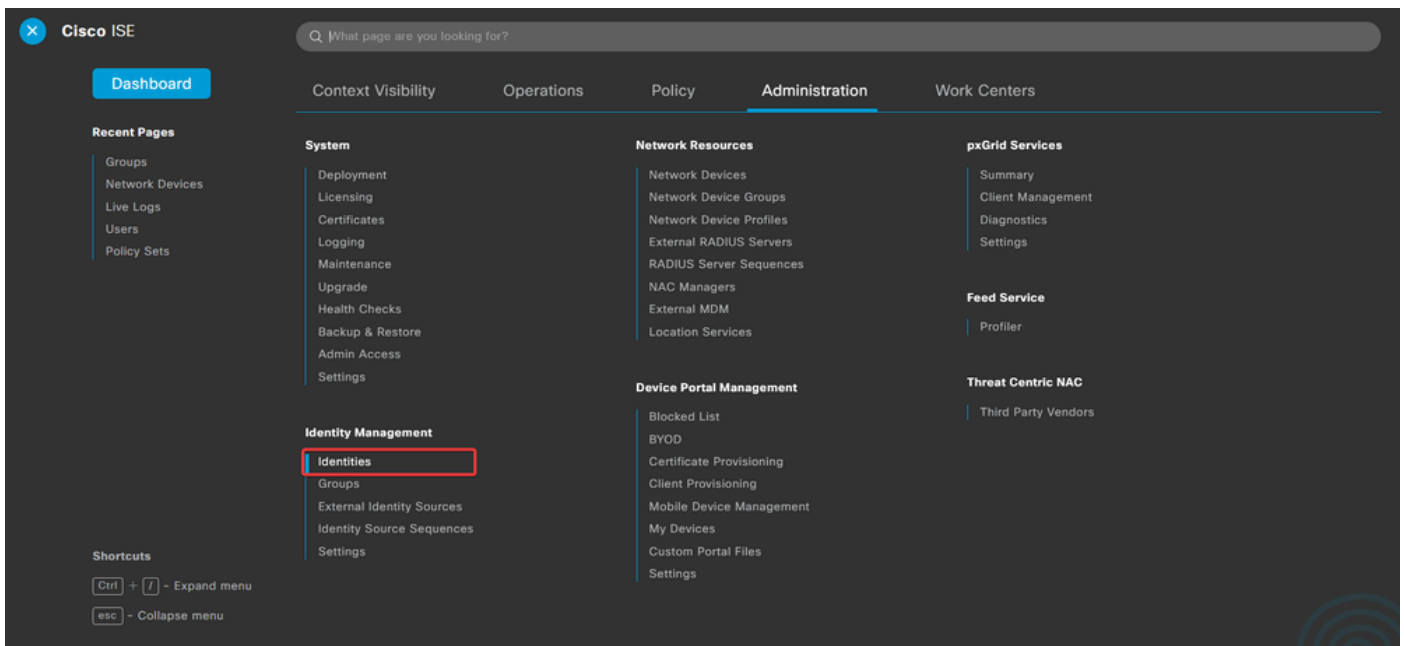
Submit

Cancel



Nota: Repita este procedimiento para crear tantos grupos como sea necesario.

d. Acceda a **Administration > Identity Management > Identities**.



e. Haga clic **Add** para crear un nuevo usuario en la base de datos local del servidor.

Introduzca el **Username** y **Login Password**. A continuación, desplácese hasta el final de esta página y seleccione la opción **User Group**.

Haga clic en **Save**.

Network Access Users

[Edit](#) [+ Add](#) [Change Status](#) [Import](#) [Export](#) [Delete](#) [Duplicate](#)

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 ⓘ

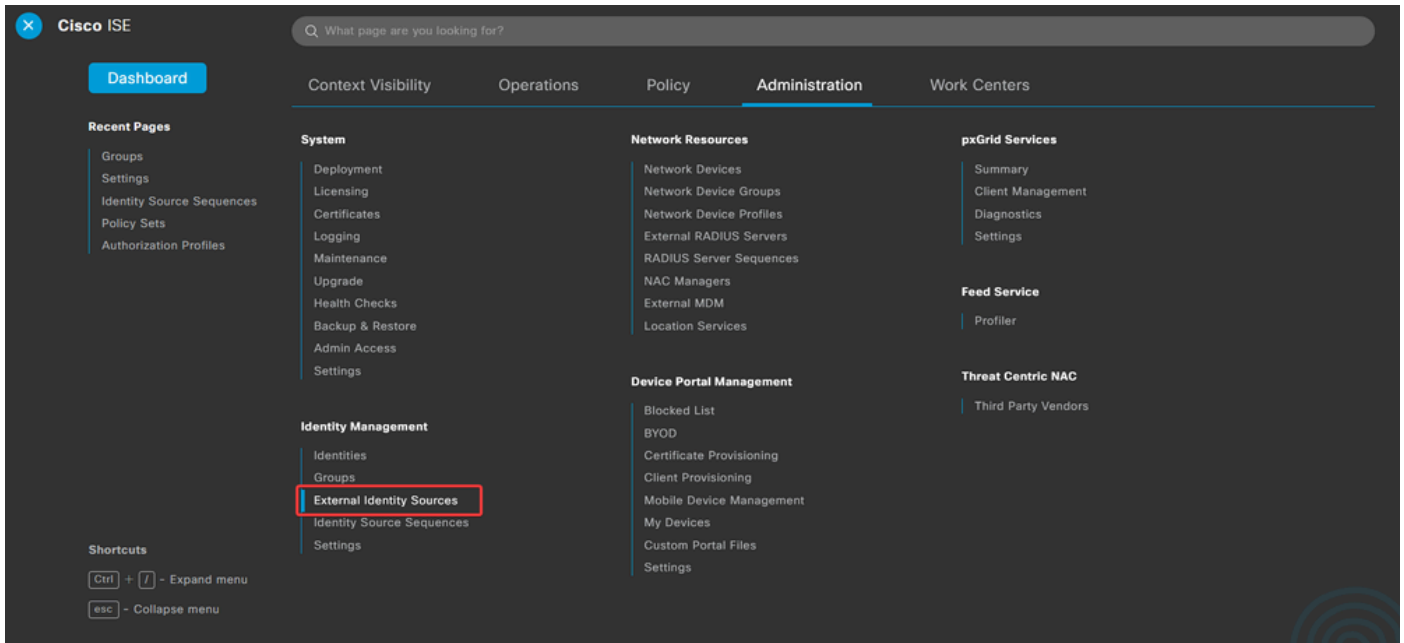
User Groups

IT Group



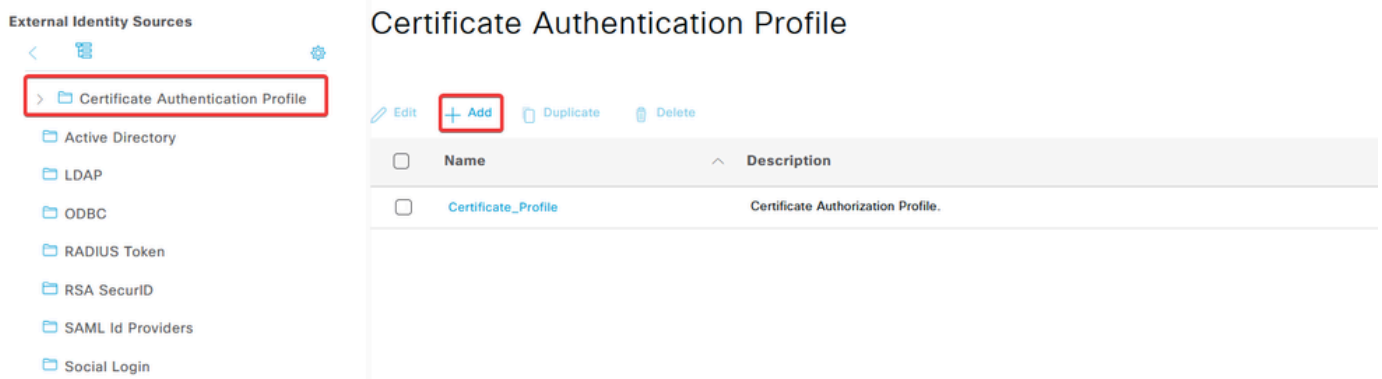
Nota: Es necesario configurar un nombre de usuario y una contraseña para crear usuarios internos. Aunque no es necesario para la autenticación RAVPN, que se realiza mediante certificados, estos usuarios se pueden utilizar para otros servicios internos que requieren una contraseña. Por lo tanto, asegúrese de utilizar una contraseña segura.

f. Desplácese hasta **Administration > Identity Management > External Identify Sources**.



g. Haga clic **Add** para crear una **Certificate Authentication Profile**.

El perfil de autenticación de certificados especifica cómo se validan los certificados de cliente, incluidos los campos del certificado que se pueden comprobar (nombre alternativo del sujeto, nombre común, etc.).



Certificate Authentication Profile

* Name

Description

Identity Store

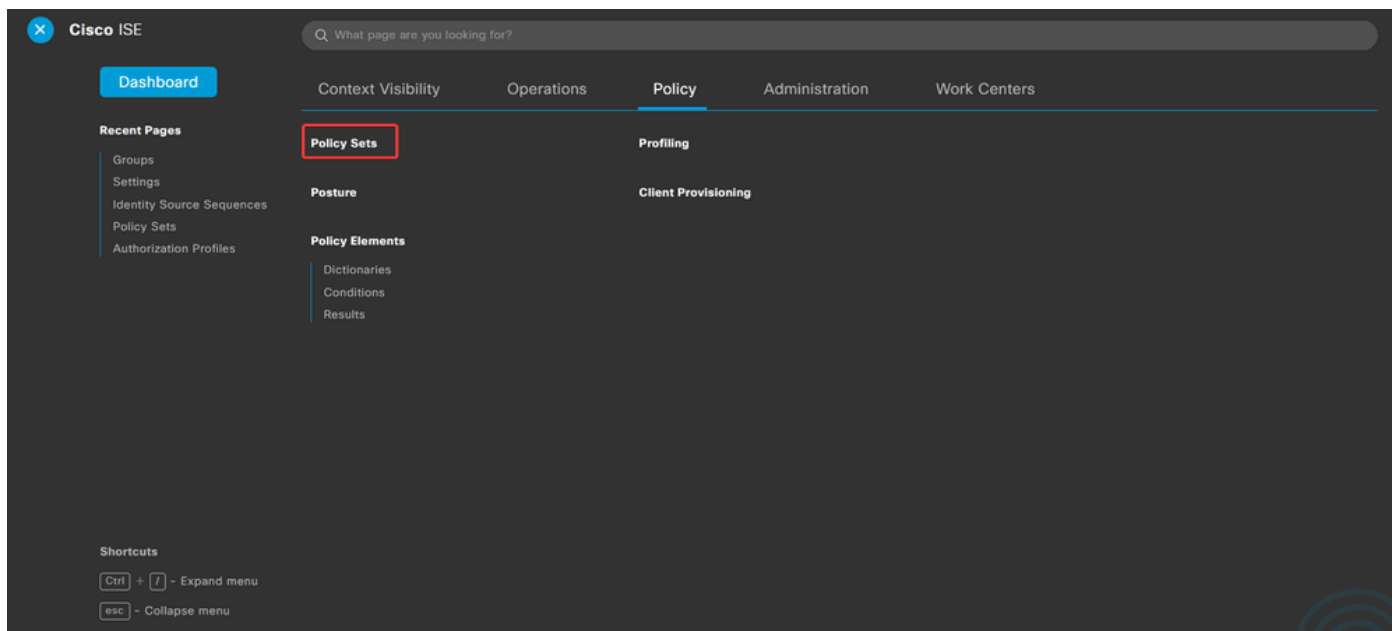
Use Identity From Certificate Attribute Subject - Common Name Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

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

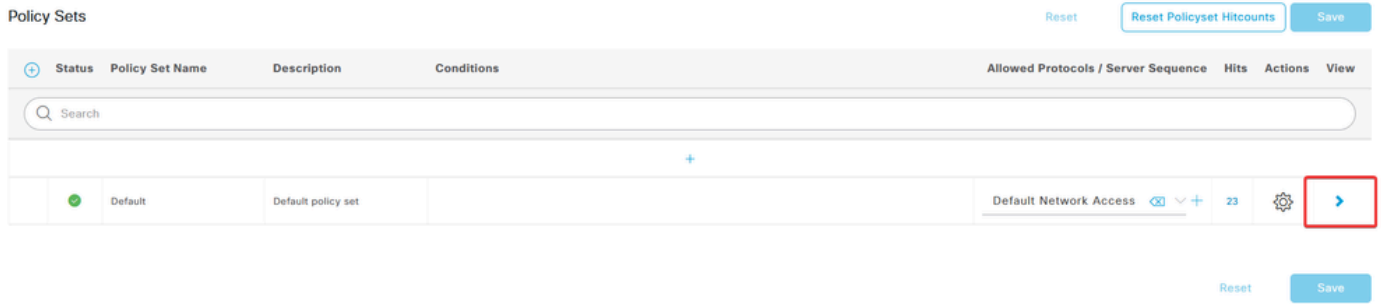
Paso 3.2: Configurar la política de autenticación

La directiva de autenticación se utiliza para autenticar que la solicitud se origina en el firewall y en el perfil de conexión específico.

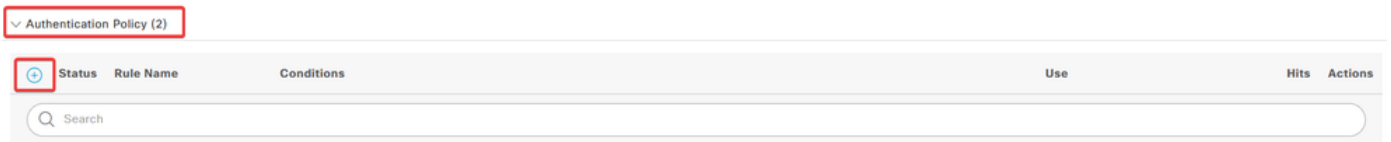
a. Desplácese hasta **Policy > Policy Sets**.



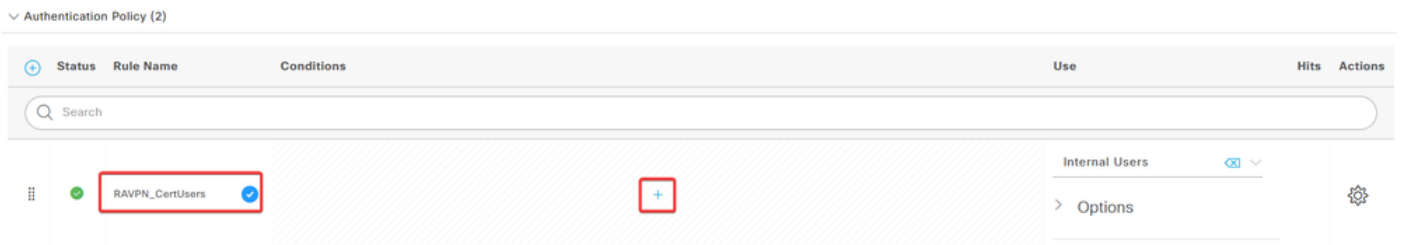
Seleccione la política de autorización predeterminada haciendo clic en la flecha en el lado derecho de la pantalla:



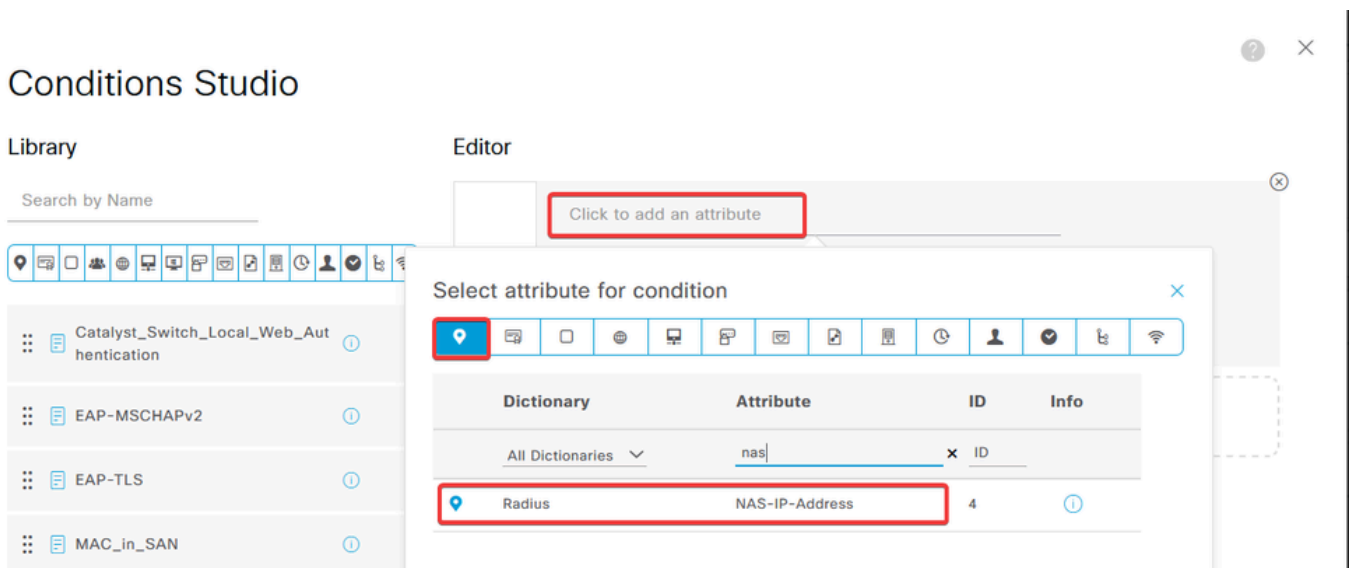
b. Haga clic en la flecha del menú desplegable junto Authentication Policy a para expandirlo. Luego, haga clic en el add (+) icono para agregar una nueva regla.



Introduzca el nombre de la regla y seleccione el add (+) icono en la columna Condiciones.



c. Haga clic en el cuadro de texto Attribute Editor y haga clic en el NAS-IP-Address icono. Introduzca la dirección IP del firewall.



d. Haga clic New y, a continuación, agregue el otro atributo Tunnel-Group-name. Introduzca el Connection Profile nombre configurado en el FMC.

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. En la columna Usar, seleccione el **Certificate Authentication Profile** que se ha creado. Al hacerlo, especifica la información definida en el perfil que se utiliza para identificar a los usuarios.

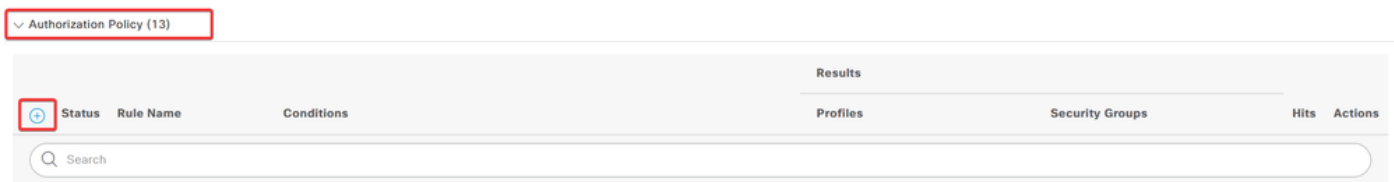
Authentication Policy (2)

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

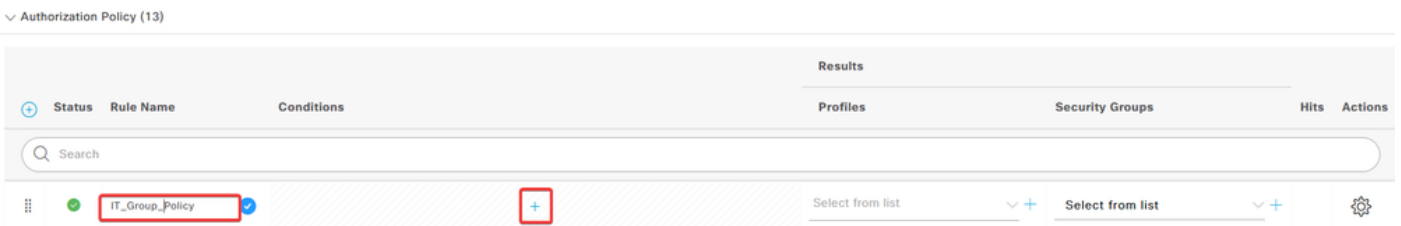
Haga clic en Save.

Paso 3.3: Configuración de la política de autorización

a. Haga clic en la flecha del menú desplegable junto a **Authorization Policy** para expandirlo. Luego, haga clic en el **add (+)** icono para agregar una nueva regla.



Introduzca el nombre de la regla y seleccione el **add (+)** icono en la columna Condiciones.

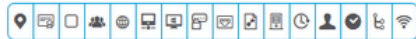


b. Haga clic en el cuadro de texto **Attribute Editor** y haga clic en el **Identity group** icono. Seleccione el **Identity group - Name** atributo.

Conditions Studio

Library

Search by Name



BYOD_is_Registered	ⓘ
Catalyst_Switch_Local_Web_Authentication	ⓘ
Compliance_Unknown_Devices	ⓘ
Compliant_Devices	ⓘ
EAP-MSCHAPv2	ⓘ
EAP-TLS	ⓘ
Guest_Flow	ⓘ
IT_Group	ⓘ

Editor

The screenshot shows the 'Attribute Editor' dialog box. The 'Select attribute for condition' title is at the top. Below it is a toolbar with icons. A table lists available attributes:

Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
CWA	CWA_ExternalGroups		ⓘ
IdentityGroup	Description		ⓘ
IdentityGroup	Name		ⓘ
InternalUser	IdentityGroup		ⓘ
PassiveID	PassiveID_Groups		ⓘ

The 'IdentityGroup - Name' row is highlighted with a red box. The 'Identity group' icon in the toolbar is also highlighted with a red box.

Seleccione **Equals** como operador y, a continuación, haga clic en la flecha del menú desplegable para mostrar las opciones disponibles y seleccione **User Identity Groups**:

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. En la columna Profiles, haga clic en el add (+) icono y seleccione **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	⚙️

Ingrese el perfilName.

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: ⓘ

Desplácese hasta **Common Tasks** y active **ASA VPN**. A continuación, escriba el **group policy name**, que debe ser el mismo que el creado en el FMC.

∨ Common Tasks

ASA VPN

IT_Group



AVC Profile Name

UDN Lookup

Los atributos que vienen a continuación se asignaron a cada grupo:

∨ Attributes Details

Access Type = ACCESS_ACCEPT

Class = IT_Group

Click Save.

Nota: Repita el paso 3.3: Configure la política de autorización para cada grupo que se creó.

Verificación

1. Ejecute el comando `show vpn-sessiondb anyconnect` y verifique si el usuario está utilizando la política de grupo correcta.

```
<#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

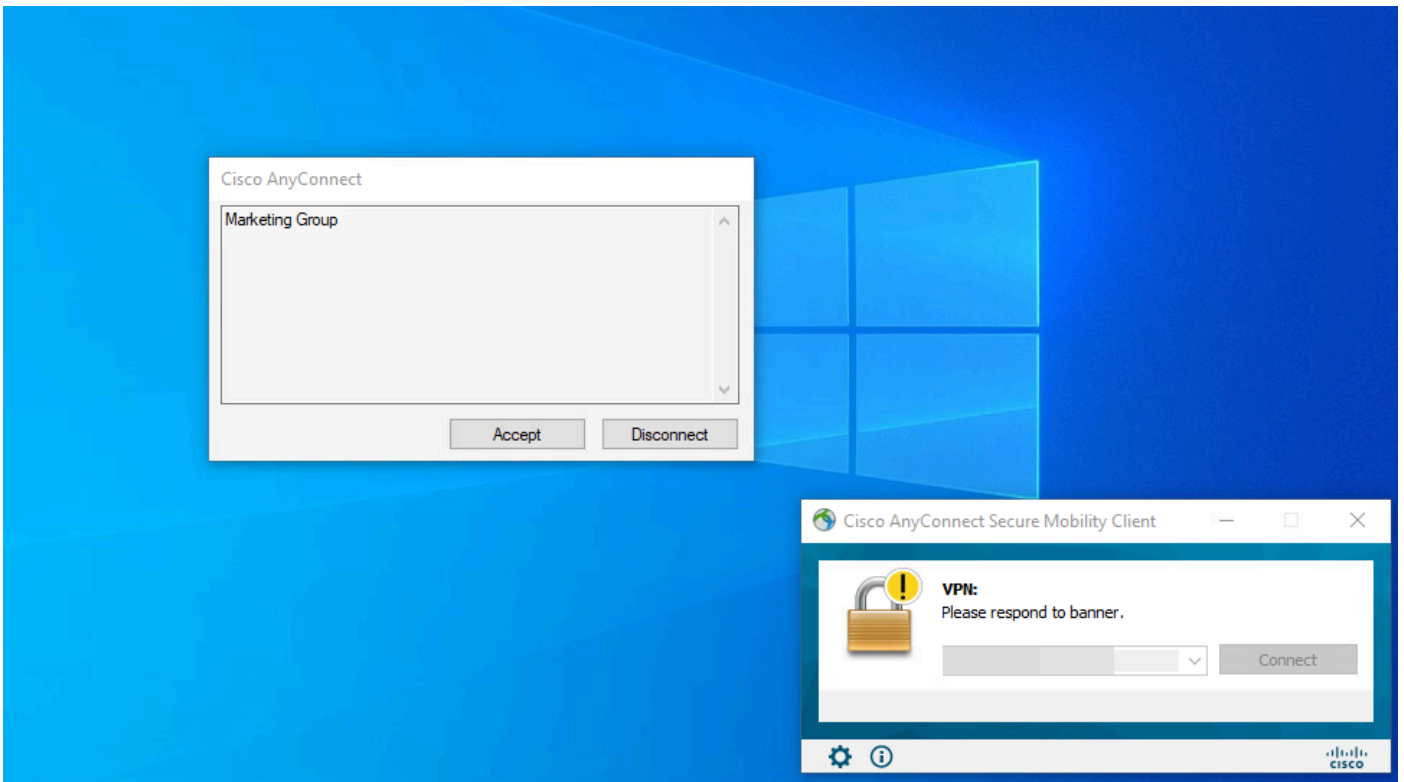
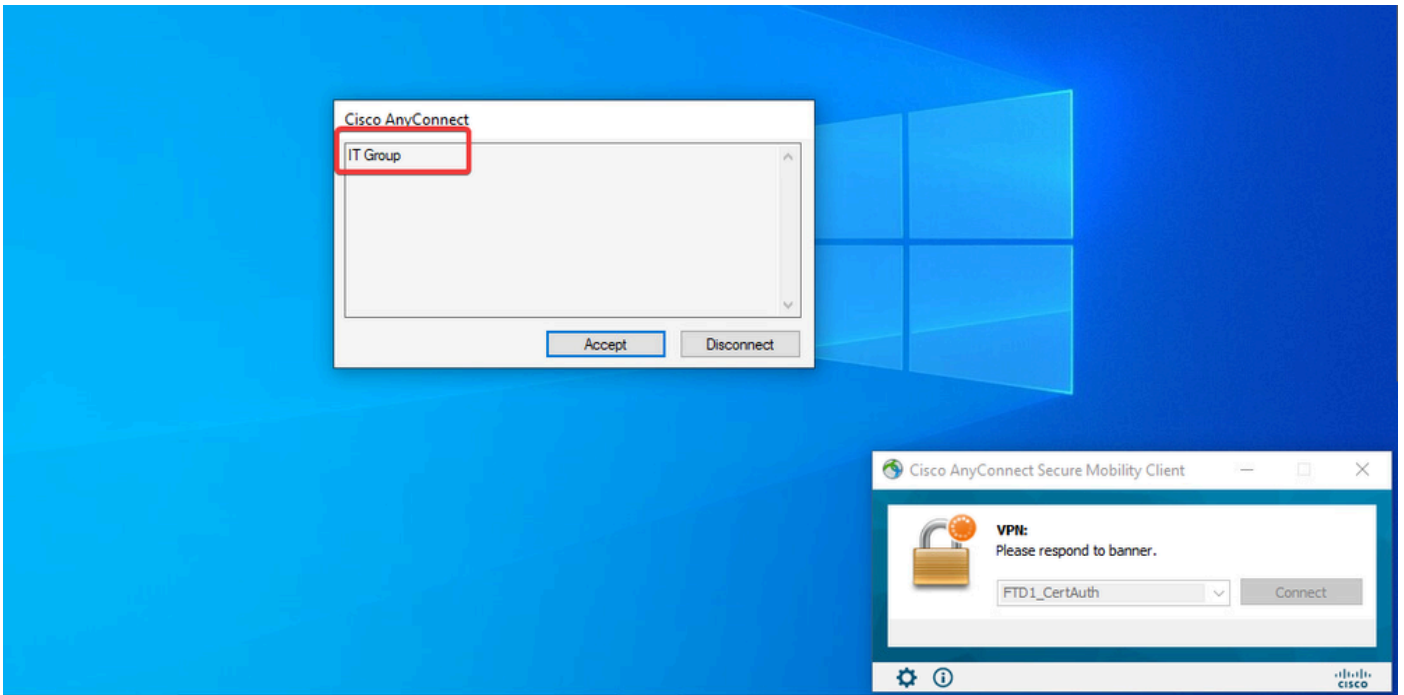
Username : User2

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. En la directiva de grupo, puede configurar un mensaje de titular que se muestre cuando el usuario se conecte correctamente. Cada banner se puede utilizar para identificar el grupo que tiene autorización.



3. En los registros activos, compruebe si la conexión está utilizando la directiva de autorización adecuada. Haga clic en **Details** y muestre el informe de autenticación.

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

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

1. Las depuraciones se pueden ejecutar desde la CLI de diagnóstico del CSF para la autenticación de certificados.

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

2. Utilice los debugs AAA para verificar la asignación de atributos locales y/o remotos.

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

En ISE:

1. Acceda a **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

Shortcuts

Ctrl + F - Expand menu

esc - Collapse menu

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

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

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).