

Configurazione dell'autorizzazione ISE e dell'autenticazione del certificato RAVPN in FMC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Passaggio 1: Installare un certificato CA attendibile](#)

[Fase 2. Configurazione del gruppo di server ISE/Radius e del profilo di connessione](#)

[Fase 3: configurare ISE](#)

[Passaggio 3.1: Creazione di utenti, gruppi e profili di autenticazione certificato](#)

[Passaggio 3.2: Configurazione dei criteri di autenticazione](#)

[Passaggio 3.3: Configurazione dei criteri di autorizzazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare i criteri di autorizzazione dei server ISE per l'autenticazione dei certificati nelle connessioni RAVPN gestite da CSF su FMC.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Firewall (CSF)
- Cisco Secure Firewall Management Center (FMC)
- Cisco Identity Services Engine (ISE)
- Nozioni fondamentali su Registrazione certificato e SSL.
- CA (Certificate Authority)

Componenti usati

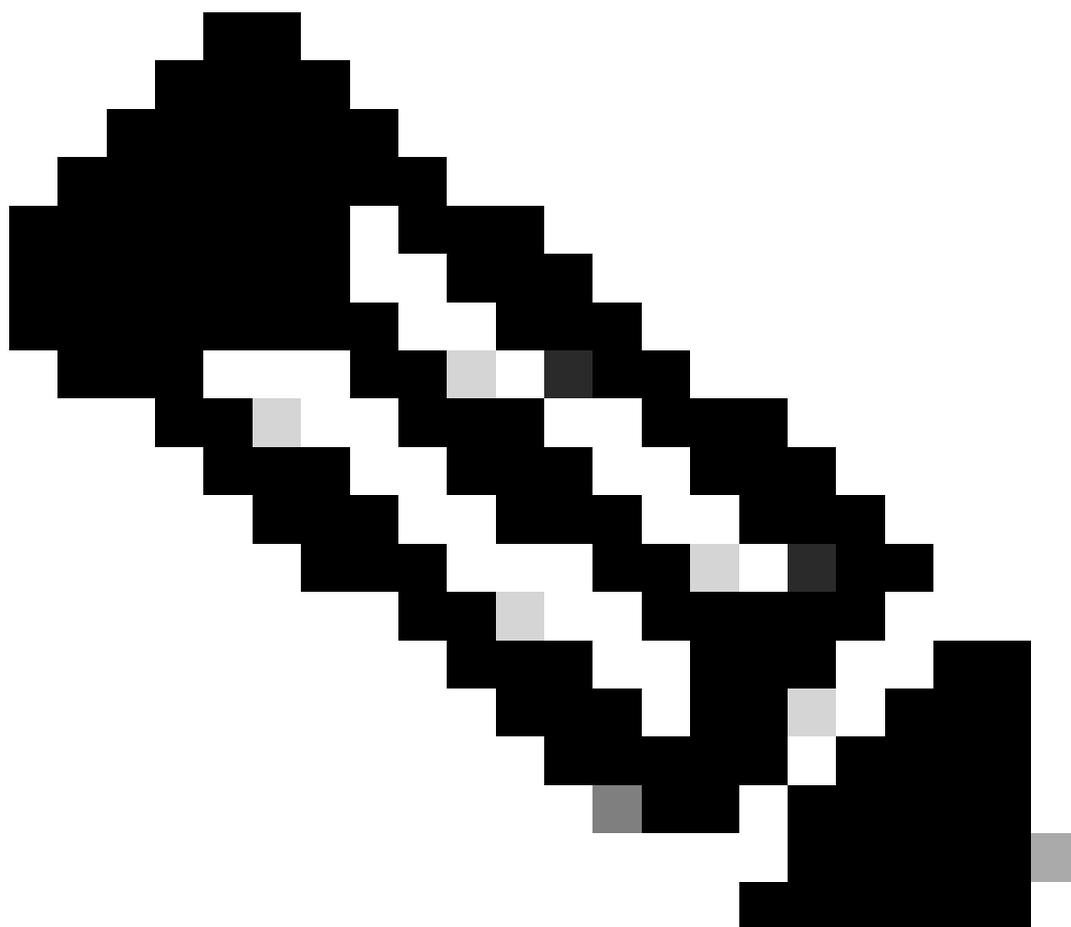
Il contenuto di questo documento si basa su queste versioni software e hardware.

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Passaggio 1: Installare un certificato CA attendibile



Nota: questo passaggio deve essere eseguito se il certificato CA è diverso da quello utilizzato per l'autenticazione del server. Se lo stesso server CA rilascia i certificati degli utenti, non è necessario importare di nuovo lo stesso certificato CA.



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

- Individuare **Devices > Certificates** e fare clic su **Add**.
- Inserire un **trustpoint name** e selezionare **Manuale** come tipo di iscrizione in **Informazioni CA**.
- Controllare **CA Only** e incollare il certificato **CA attendibile/interna** in formato pem.
- Selezionare **Skip Check for CA flag in basic constraints of the CA Certificate** e fare clic su **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. In Cert Enrollment, selezionare il trustpoint nome dall'elenco a discesa appena creato e fare clic su 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

Fase 2. Configurazione del gruppo di server ISE/Radius e del profilo di connessione

a. Individuare **Objects > AAA Server > RADIUS Server Group** e fare clic su **Add RADIUS Server Group**.
Selezionare **Enable authorize only** l'opzione.



Avviso: se l'opzione Abilita solo autorizzazione non è selezionata, il firewall invia una richiesta di autenticazione. Tuttavia, ISE si aspetta di ricevere un nome utente e una password con tale richiesta e non viene utilizzata una password nei certificati. Di conseguenza, ISE contrassegna la richiesta come autenticazione non riuscita.

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. Fare clic **Add (+)** sull'icona, quindi aggiungere l'indirizzo IP o il nome host desiderato 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. Passare a **Devices > Remote Access configuration** . Creare un **new connection profile** e impostare il metodo di autenticazione su **Client Certificate Only**. Per il server di autorizzazione, scegliere quello creato nei passaggi precedenti.

Accertarsi di selezionare l'Allow connection only if user exists in authorization database opzione. Questa impostazione garantisce che la connessione a RAVPN venga completata solo se l'autorizzazione è consentita.

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

Mappare il nome utente dal certificato client fa riferimento alle informazioni ottenute dal certificato per identificare l'utente. In questo esempio viene mantenuta la configurazione predefinita, ma è possibile modificarla a seconda delle informazioni utilizzate per identificare gli utenti.

Fare clic su **.Save**

d. Passare a **Advanced > Group Policies**. Fare clic **Add (+)** sull'icona a destra.

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. Creare il **group policies**file. Ogni criterio di gruppo è configurato in base ai gruppi dell'organizzazione e alle reti a cui ogni gruppo può accedere.

Group Policy ?

Available Group Policy ↻ +

Search

DfltGrpPolicy

FTD1_GPCertAuth

FTD1_GPISE

FTD1_GPLocalFull

Add

Selected Group Policy

DfltGrpPolicy

Cancel OK

f. In Criteri di gruppo, eseguire le configurazioni specifiche per ogni gruppo. Dopo la connessione, è possibile aggiungere un banner messaggio da visualizzare.

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. Selezionare il **group policies** lato sinistro e fare clic su **Add** per spostarlo sul lato destro. Specifica i criteri di gruppo utilizzati nella configurazione.

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

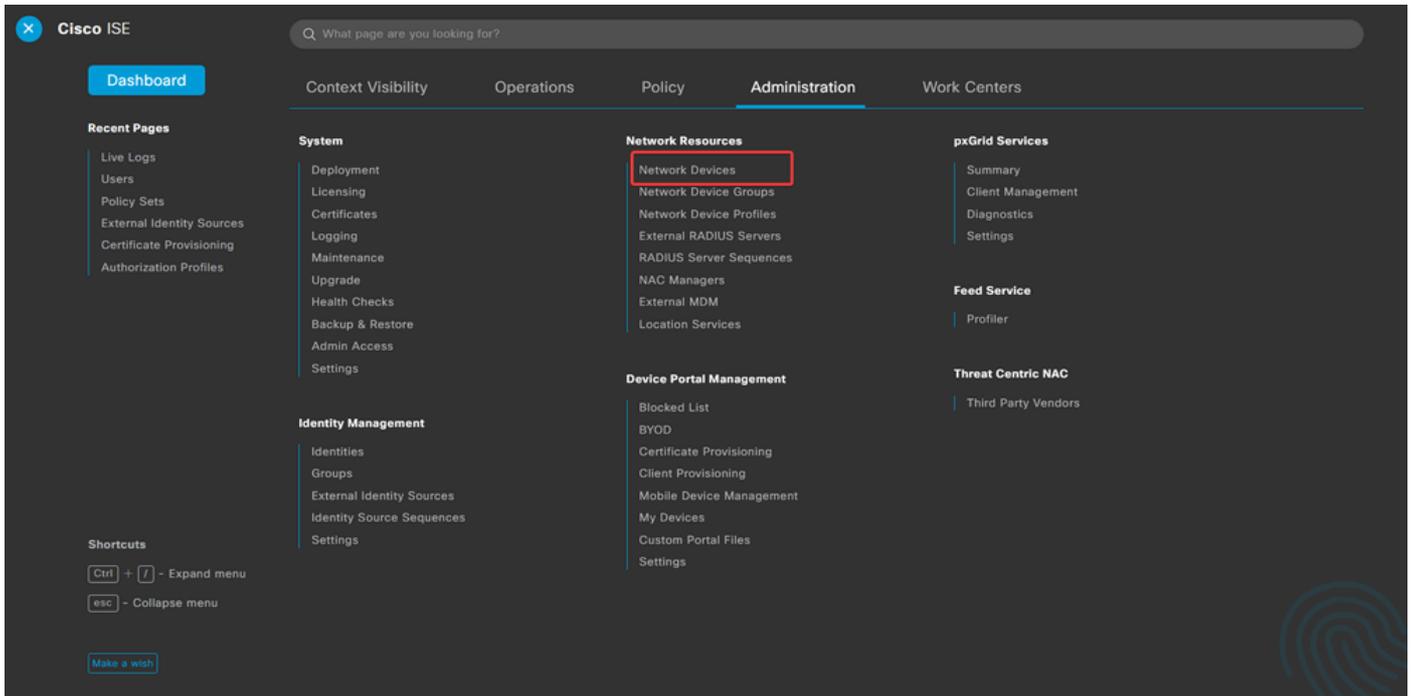
OK

e. Distribuire le modifiche.

Fase 3: configurare ISE

Passaggio 3.1: Creazione di utenti, gruppi e profili di autenticazione certificato

a. Accedere al server ISE e selezionare **Administration > Network Resources > Network Devices**.



b. Fare clic **Add** per configurare il firewall come client AAA.

Network Devices

Edit + Add Duplicate Import Export Generate PAC Delete						
<input type="checkbox"/>	Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/>	FTD		Cisco	All Locations	All Device Types	

c. Immettere i campi Nome dispositivo di rete e Indirizzo IP, quindi selezionare la casella di controllo **RADIUS Authentication Settings** e aggiungere il valore **Shared Secret**. This must be the same that was used when the RADIUS Server object on FMC was creation (Questo valore deve essere lo stesso utilizzato quando è stato creato l'oggetto server RADIUS in FMC). Fare clic su **.Save**

[Network Devices List](#) > FTD

Network Devices

Name

Description

IP Address / 32

RADIUS Authentication Settings

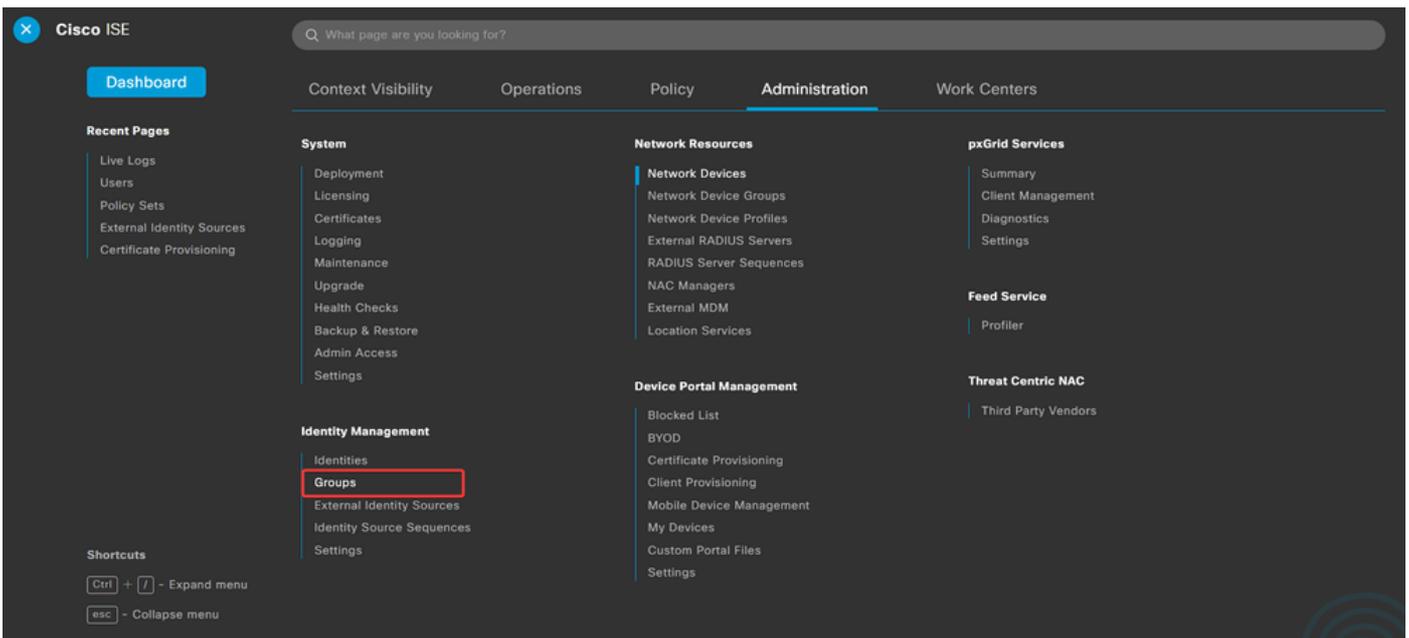
RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret Show

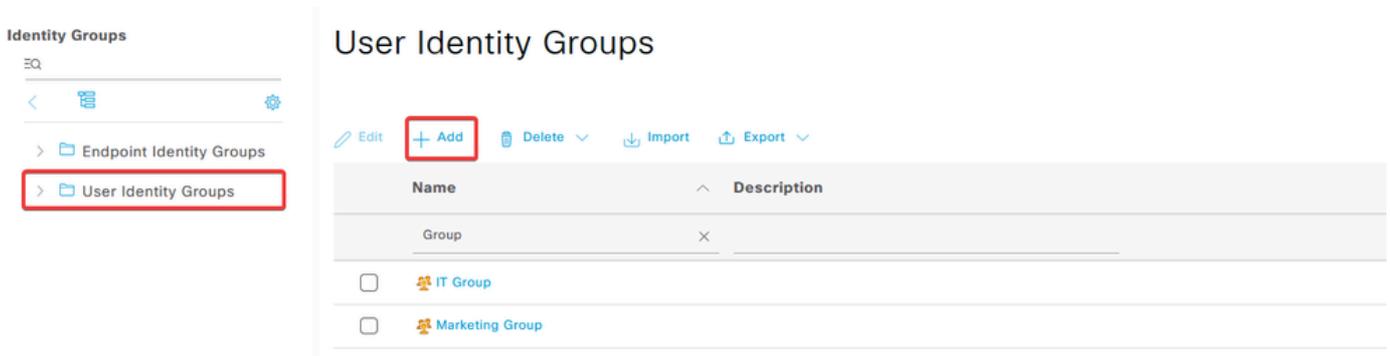
Use Second Shared Secret ⓘ

d. Passare a Administration > Identity Management > Groups.



e. Fare clic su User Identity Groups, quindi su Add.

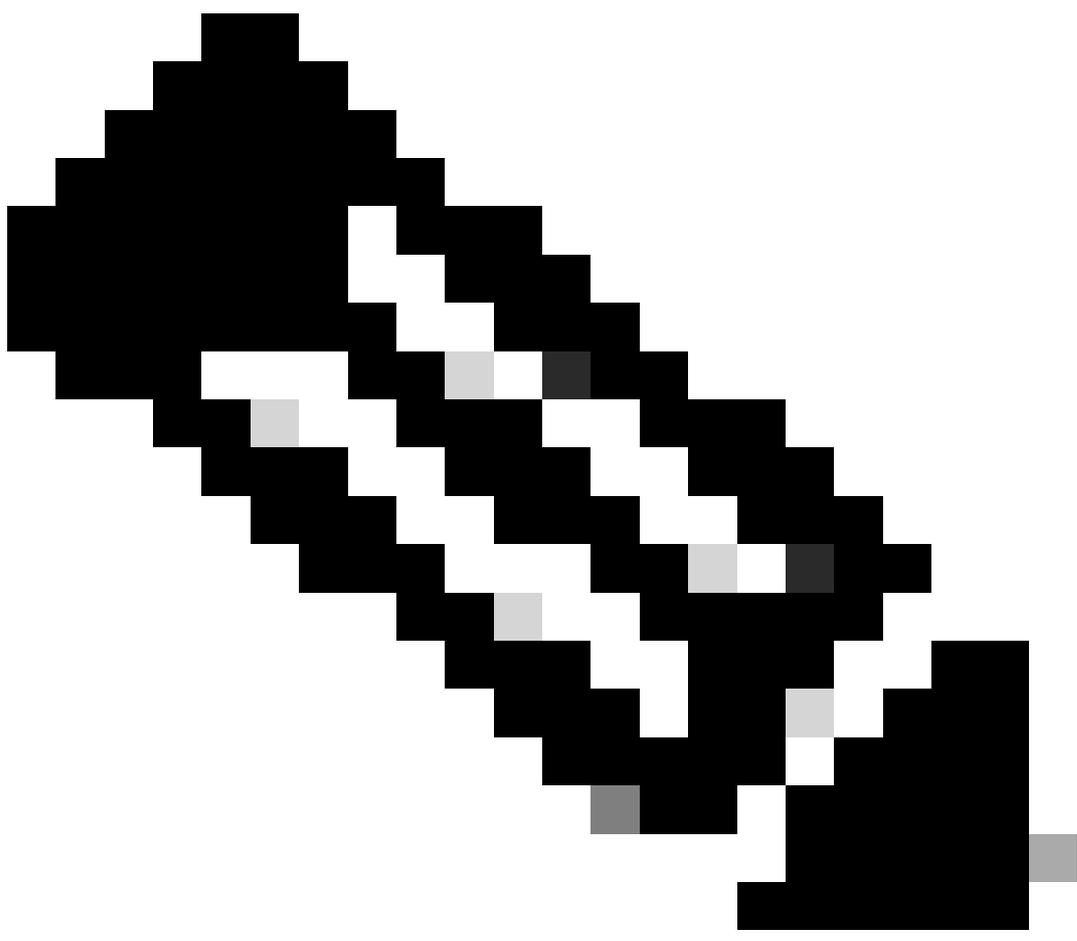
Immettere il nome del gruppo e fare clic su Submit.



Identity Group

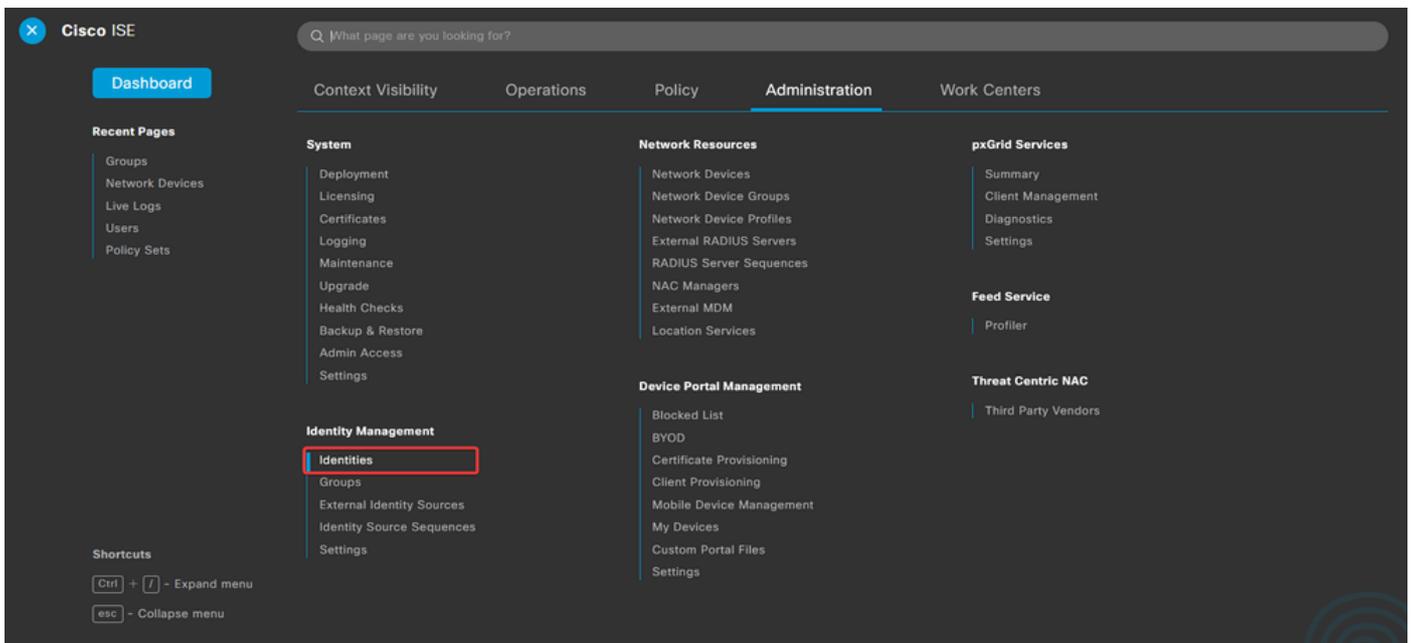
* Name

Description



Nota: ripetere l'operazione per creare il numero di gruppi desiderato.

d. Passare a Administration > Identity Management > Identities.



e. Fare clic **Add** per creare un nuovo utente nel database locale del server.

Immettere il valore **Username** e **Login Password**. Quindi, spostarsi alla fine di questa pagina e selezionare il **User Group**.

Fare clic su **.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"/>	<input checked="" type="checkbox"/> Enabled	user1				IT Group	
<input type="checkbox"/>	<input checked="" 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

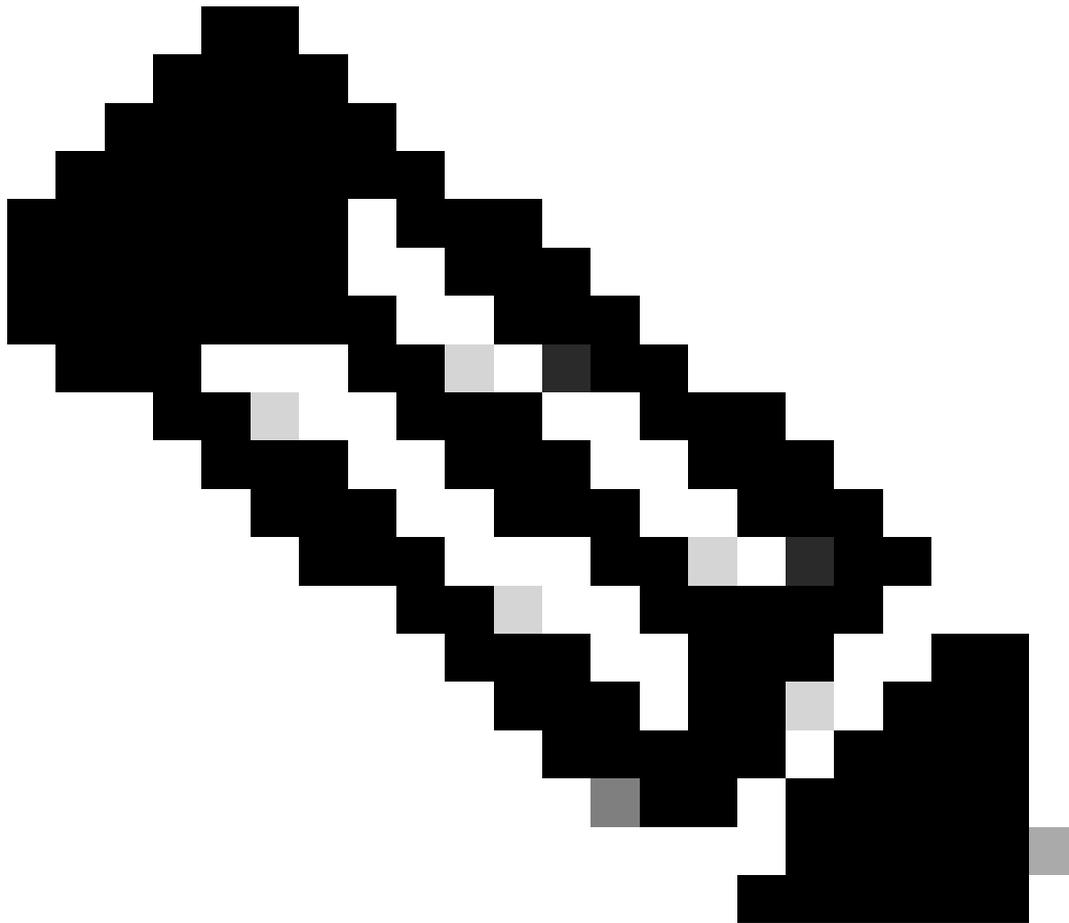
Generate Password ⓘ

Enable Password

Generate Password ⓘ

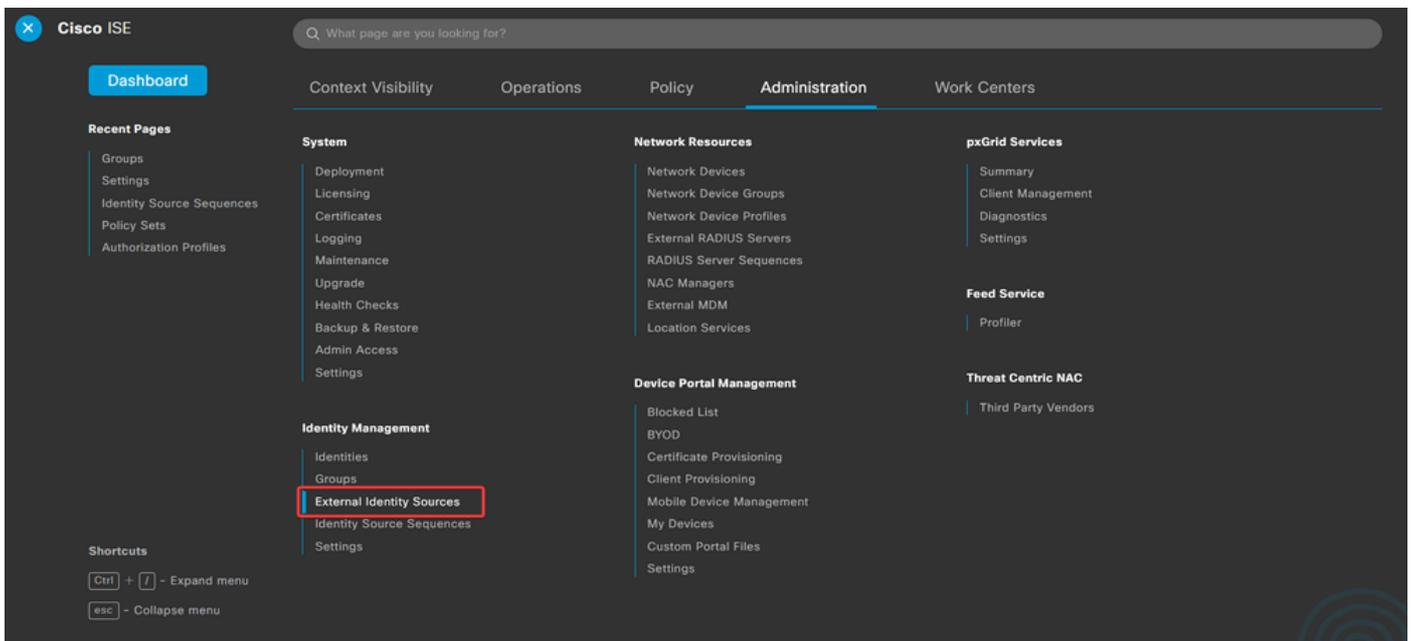
User Groups

IT Group



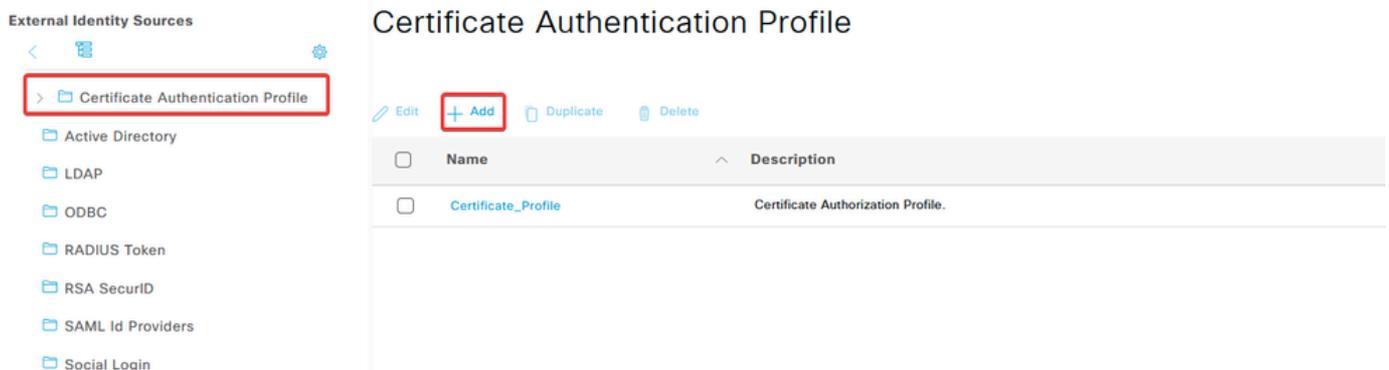
Nota: è necessario configurare un nome utente e una password per creare utenti interni. Anche se non è necessaria per l'autenticazione RAVPN, che viene eseguita utilizzando i certificati, questi utenti possono essere utilizzati per altri servizi interni che richiedono una password. Pertanto, assicurarsi di utilizzare una password complessa.

f. Passare a **Administration > Identity Management > External Identify Sources**.



g. Fare clic su **Add** per creare una **Certificate Authentication Profile** maschera.

Profilo di autenticazione certificato specifica la modalità di convalida dei certificati client, inclusi i campi del certificato che è possibile controllare (Nome alternativo soggetto, Nome comune e così via).



Certificate Authentication Profile

* Name

Description

Identity Store

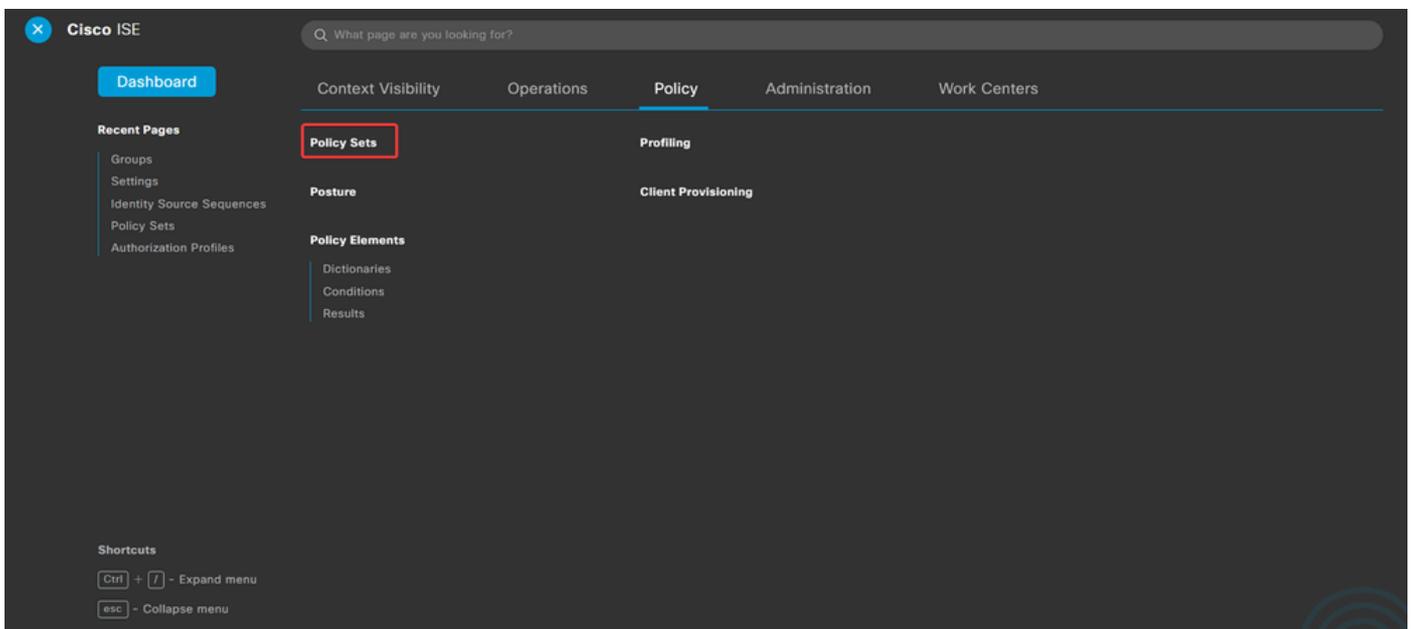
Use Identity From Certificate Attribute Subject - Common Name Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

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

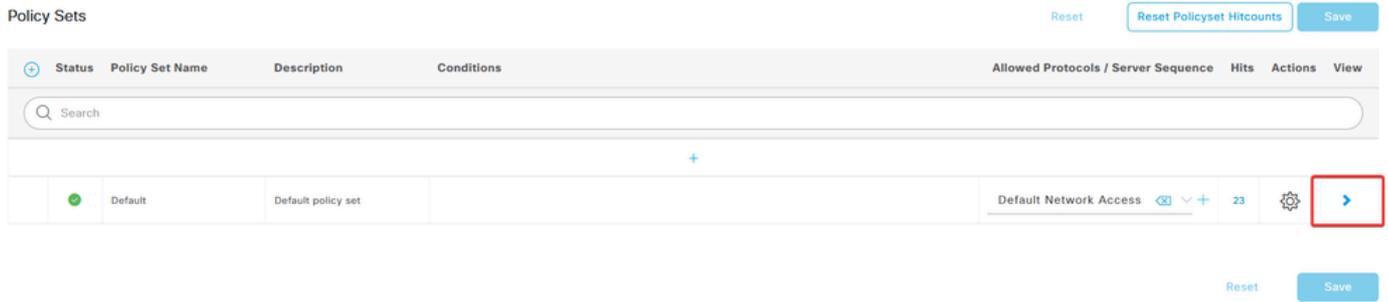
Passaggio 3.2: Configurazione dei criteri di autenticazione

Il criterio di autenticazione viene utilizzato per autenticare che la richiesta proviene dal firewall e dal profilo di connessione specifico.

a. Passare a Policy > Policy Sets.



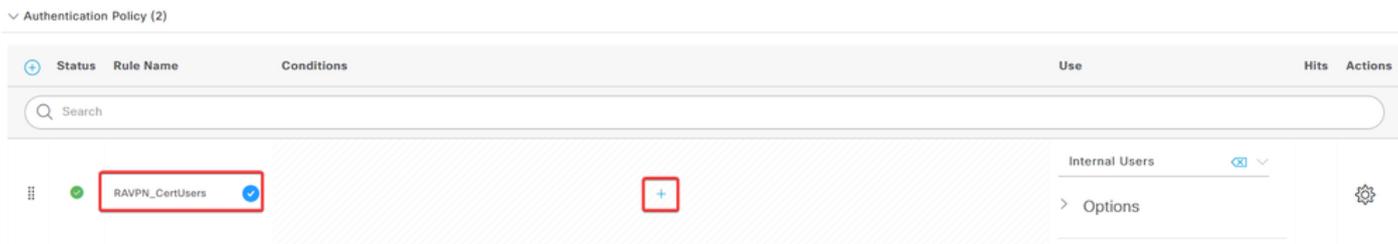
Selezionare il criterio di autorizzazione predefinito facendo clic sulla freccia sul lato destro della schermata:



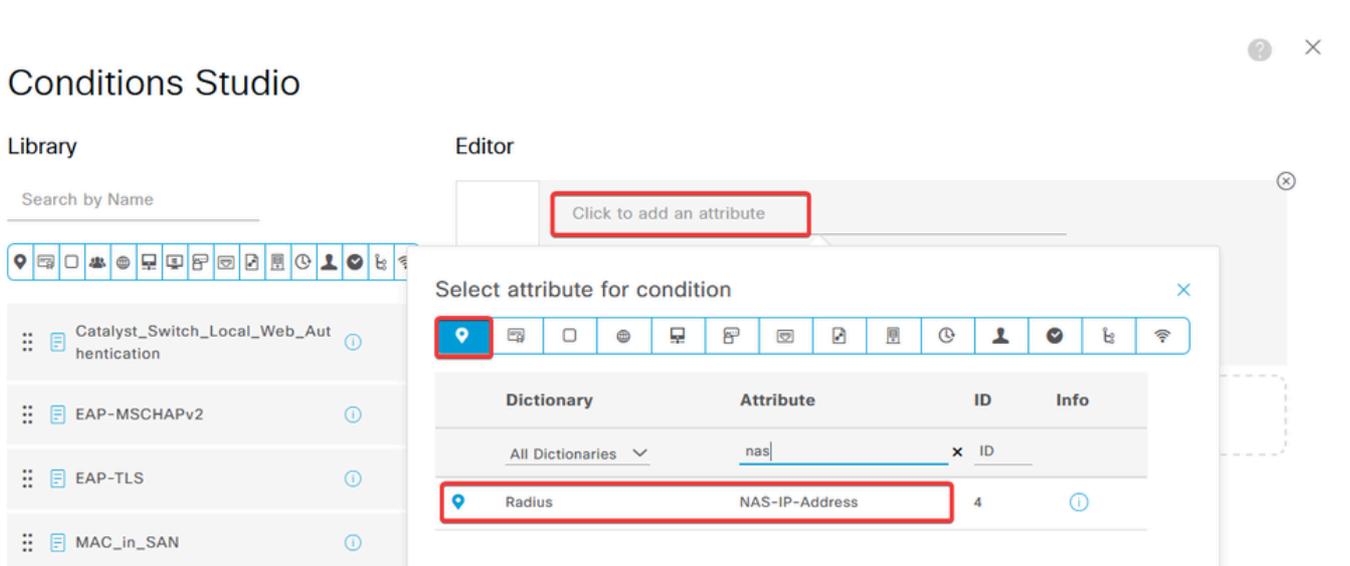
b. Fare clic sulla freccia del menu a discesa accanto Authentication Policy a per espanderlo. Quindi, fare clic sull'add (+) icona per aggiungere una nuova regola.



Immettere il nome della regola e selezionare l'icona add (+) nella colonna Condizioni.



c. Fare clic sulla casella di testo Editor attributi e fare clic sull'NAS-IP-Address' icona. Immettere l'indirizzo IP del firewall.



d. Fare clic su New, quindi aggiungere l'altro attributo Tunnel-Group-name. Immettere il nome configurato nel Connection Profile CCP.

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. Nella colonna Utilizza, selezionare la colonna **Certificate Authentication Profile** creata. In questo modo vengono specificate le informazioni definite nel profilo utilizzato per identificare gli utenti.

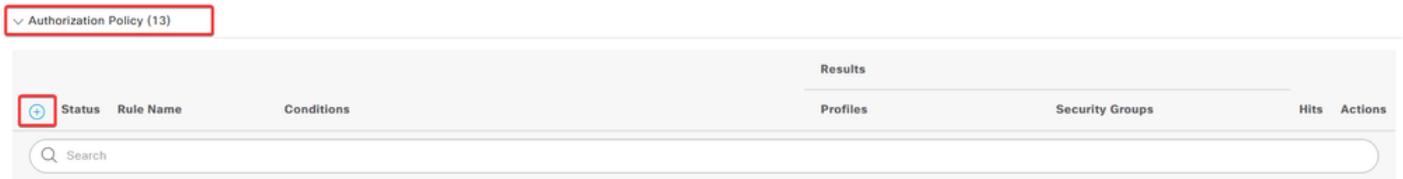
Authentication Policy (2)

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

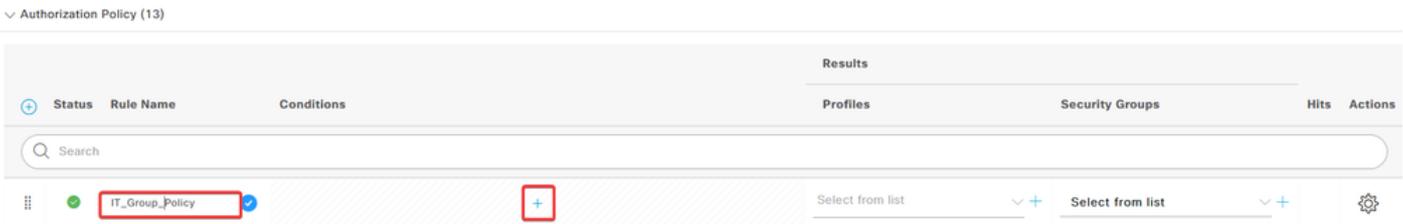
Fare clic su .Save

Passaggio 3.3: Configurazione dei criteri di autorizzazione

a. Fare clic sulla freccia del menu a discesa accanto **Authorization Policy** a per espanderlo. Quindi, fare clic sull'**add (+)** icona per aggiungere una nuova regola.



Immettere il nome della regola e selezionare l'**add (+)** icona nella colonna Condizioni.



b. Fare clic sulla casella di testo Editor attributi e fare clic sull'**Identity group** icona. Selezionare l'**Identity group - Name** attributo.

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

IT_Group

InternalUser-IdentityGroup

Select attribute for condition

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

Selezionare **Equals** come operatore, quindi fare clic sulla freccia del menu a discesa per visualizzare le opzioni disponibili e selezionare **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. Nella colonna Profili, fare clic sull'add (+) icona e scegliere **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	

Immettere il profilo **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: ⓘ

Passare alla sezione **Common Tasks** e selezionare **ASA VPN**. Digitare quindi **group policy name**, che deve corrispondere a quello creato nel CCP.

∨ Common Tasks

ASA VPN

IT_Group



AVC Profile Name

UDN Lookup

Gli attributi successivi sono stati assegnati a ciascun gruppo:

∨ Attributes Details

Access Type = ACCESS_ACCEPT

Class = IT_Group

Fare clic su **Save (Salva)**.

Nota: ripetere il passo 3.3: configurare i criteri di autorizzazione per ogni gruppo creato.

Verifica

1. Eseguire il comando `show vpn-sessiondb anyconnect` e verificare se l'utente utilizza i criteri di gruppo corretti.

```
<#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

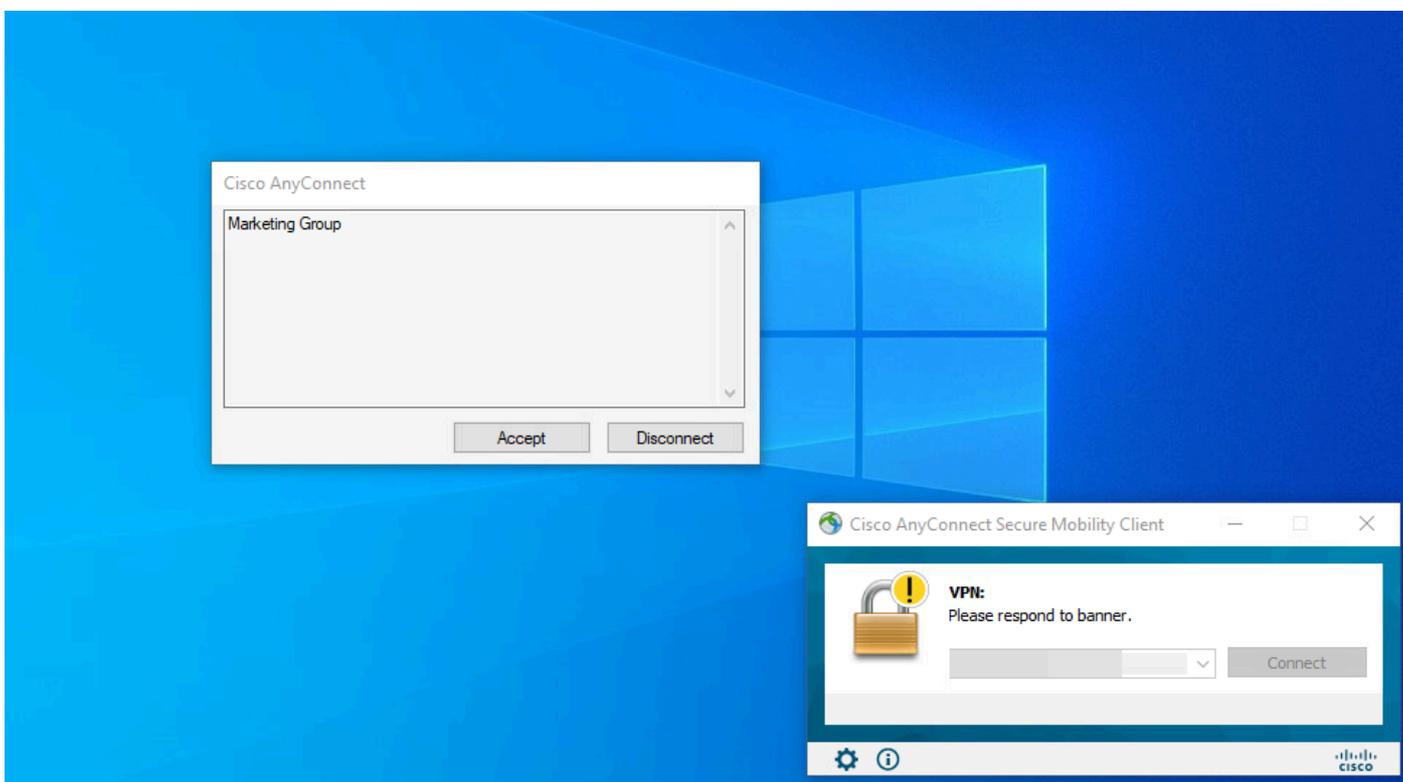
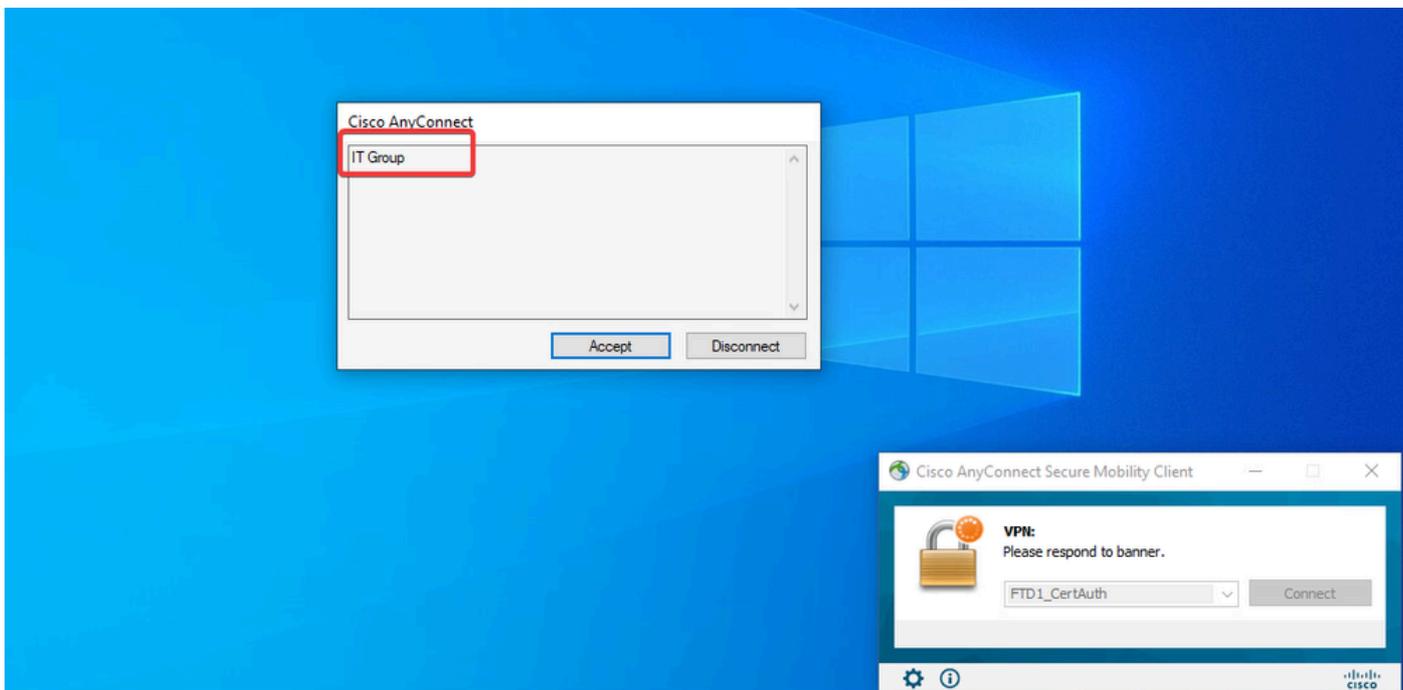
Assigned IP : 192.168.55.3 Public IP :
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes 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. Nei Criteri di gruppo è possibile configurare un messaggio di intestazione che verrà visualizzato quando l'utente si connette correttamente. Ogni banner può essere utilizzato per identificare il gruppo che ha l'autorizzazione.



3. Nei registri attivi verificare se la connessione utilizza i criteri di autorizzazione appropriati.
Fare clic su **Details** e visualizzare il report di autenticazione.

Live Logs Live Sessions

Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 0

Client Stopped Responding 0

Repeat Counter 0

Refresh
NeverShow
Latest 100 rec...Within
Last 30 minu...

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 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

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

1. I debug possono essere eseguiti dalla CLI diagnostica di CSF per l'autenticazione del certificato.

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

2. Utilizzare i debug AAA per verificare l'assegnazione degli attributi locali e/o remoti.

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

ISE:

1. Passare 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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).