

# Configurazione dell'autenticazione esterna FMC e FTD con ISE come server RADIUS

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Autenticazione esterna per FMC](#)

[Autenticazione esterna per FTD](#)

[Topologia della rete](#)

[Configurazione](#)

[Configurazione di ISE](#)

[Configurazione FMC](#)

[Configurazione FTD](#)

[Verifica](#)

---

## Introduzione

Questo documento descrive un esempio di configurazione dell'autenticazione esterna per Secure Firewall Management Center e Firewall Threat Defense.

## Prerequisiti

### Requisiti

È consigliabile conoscere i seguenti argomenti:

- Configurazione iniziale di Cisco Secure Firewall Management Center tramite GUI e/o shell.
- Configurazione dei criteri di autenticazione e autorizzazione su ISE.
- Conoscenze base di RADIUS.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- vFMC 7.2.5
- FTD 7.2.5
- ISE 3.2.2

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.

## Premesse

Quando si abilita l'autenticazione esterna per gli utenti amministrativi e di gestione del sistema Secure Firewall, il dispositivo verifica le credenziali dell'utente con un server LDAP (Lightweight Directory Access Protocol) o RADIUS come specificato in un oggetto di autenticazione esterno.

Gli oggetti di autenticazione esterna possono essere utilizzati dai dispositivi FMC e FTD. È possibile condividere lo stesso oggetto tra diversi tipi di accessorio/dispositivo oppure creare oggetti distinti.

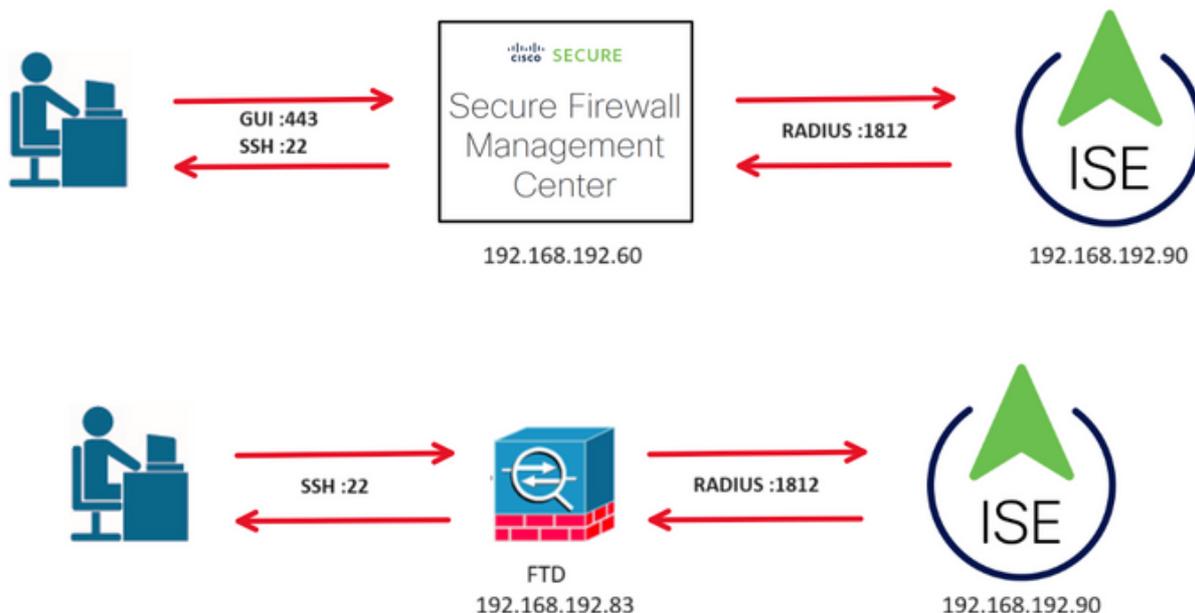
### Autenticazione esterna per FMC

È possibile configurare più oggetti di autenticazione esterna per l'accesso all'interfaccia Web. È possibile utilizzare un solo oggetto di autenticazione esterno per l'accesso alla CLI o alla shell.

### Autenticazione esterna per FTD

Per l'FTD, è possibile attivare un solo oggetto di autenticazione esterna.

### Topologia della rete



## Configurazione

### Configurazione di ISE



Nota: esistono diversi modi per configurare l'autenticazione ISE e i criteri di autorizzazione per i dispositivi di accesso alla rete (NAD), ad esempio FMC. L'esempio descritto in questo documento è un punto di riferimento in cui vengono creati due profili (uno con diritti di amministratore e l'altro di sola lettura) che possono essere adattati in modo da soddisfare le linee di base per l'accesso alla rete. In ISE è possibile definire uno o più criteri di autorizzazione che restituiscono al CCP i valori degli attributi RADIUS che vengono quindi mappati a un gruppo di utenti locale definito nella configurazione dei criteri di sistema del CCP.

---

Passaggio 1. Aggiungere un nuovo dispositivo di rete. Passare all'icona del hamburger situata nell'angolo superiore sinistro > Amministrazione > Risorse di rete > Dispositivi di rete > +Aggiungi.



The screenshot shows the Cisco ISE Administration console. At the top, there is a navigation bar with the Cisco ISE logo and the title 'Administration - Network Resources'. Below this is a sub-navigation bar with tabs for 'Network Devices', 'Network Device Groups', 'Network Device Profiles', 'External RADIUS Servers', 'RADIUS Server Sequences', and 'More'. The 'Network Devices' tab is selected. On the left, there is a sidebar with 'Network Devices', 'Default Device', and 'Device Security Settings'. The main content area is titled 'Network Devices' and shows a table with columns for Name, IP/Mask, Profile Name, Location, Type, and Description. Above the table, there is a toolbar with buttons for Edit, Add (highlighted with a red box), Duplicate, Import, Export, Generate PAC, and Delete. The status bar indicates 'Selected 0 Total 2'.

Passaggio 2. Assegnare un nome all'oggetto dispositivo di rete e inserire l'indirizzo IP del CCP.

Selezionare la casella di controllo RADIUS e definire un segreto condiviso.

La stessa chiave deve essere utilizzata successivamente per configurare il CCP.

Al termine, fare clic su Salva.

The screenshot shows the configuration page for a Network Device in Cisco ISE. The page title is 'Network Devices List > FMC'. The main content area is titled 'Network Devices' and contains a form for configuring a device. The 'Name' field is filled with 'FMC'. The 'Description' field is empty. The 'IP Address' field is filled with '192.168.192.60 / 32'. The 'Device Profile' is set to 'Cisco'. The 'Model Name' is 'vFMC'. The 'Software Version' is '7.2.5'. The 'Network Device Group' is empty. The 'Location' is 'All Locations'. The 'IPSEC' is 'No'. The 'Device Type' is 'All Device Types'. The 'RADIUS Authentication Settings' section is expanded, and the 'RADIUS' protocol is selected. The 'Shared Secret' field is filled with a redacted value and is highlighted with a red box. The 'Use Second Shared Secret' checkbox is unchecked.

Passaggio 2.1. Ripetete la stessa procedura per aggiungere l'FTD.

Assegnare un Nome all'oggetto dispositivo di rete e inserire l'indirizzo IP FTD.

Selezionare la casella di controllo RADIUS e definire un segreto condiviso.

Al termine, fare clic su Salva.

The screenshot shows the Cisco ISE Administration interface for configuring a Network Device. The device name is 'FTD'. The IP Address is '192.168.192.83 / 32'. The Device Profile is 'Cisco', Model Name is 'vFTD', and Software Version is '7.2.5'. The Network Device Group is 'All Locations'. The Location is 'All Locations', IPSEC is 'No', and Device Type is 'All Device Types'. The RADIUS Authentication Settings section is expanded, showing the RADIUS UDP Settings with the Protocol set to 'RADIUS' and a Shared Secret field. The 'Use Second Shared Secret' checkbox is unchecked.

Passaggio 2.3. Verificare che entrambe le periferiche siano visualizzate in Periferiche di rete.

The screenshot shows the Cisco ISE Administration interface displaying a list of Network Devices. The list includes two devices: FMC and FTD. Both devices have the Profile Name 'Cisco', Location 'All Locations', and Type 'All Device Types'. The FMC device has an IP/Mask of 192.168.192.60/32, and the FTD device has an IP/Mask of 192.168.192.83/32. The interface also shows a table with columns for Name, IP/Mask, Profile Name, Location, Type, and Description.

Name	IP/Mask	Profile Name	Location	Type	Description
FMC	192.168.192.60/32	Cisco	All Locations	All Device Types	
FTD	192.168.192.83/32	Cisco	All Locations	All Device Types	

Passaggio 3. Creare i gruppi di identità utente richiesti. Passare all'icona del hamburger situata nell'angolo superiore sinistro > Amministrazione > Gestione delle identità > Gruppi > Gruppi identità utente > + Aggiungi

The screenshot shows the Cisco ISE Administration interface for Identity Management. The breadcrumb trail is Administration > Identity Management > Groups > User Identity Groups. On the left, there is a sidebar for 'Identity Groups' with a search bar and a tree view showing 'Endpoint Identity Groups' and 'User Identity Groups'. The main area is titled 'User Identity Groups' and shows a table with columns 'Name' and 'Description'. Above the table, there are action buttons: 'Edit', '+ Add' (highlighted with a red box), 'Delete', 'Import', and 'Export'. The table is currently empty, with 'Selected 0' and 'Total 11' items.

Passaggio 4. Assegnare un nome a ogni gruppo e scegliere Salva singolarmente. In questo esempio viene creato un gruppo per gli utenti con privilegi di amministratore e un altro per gli utenti di sola lettura. Creare innanzitutto il gruppo per l'utente con diritti di amministratore.

The screenshot shows the configuration page for an 'Identity Group' named 'FMC and FTD admins'. The breadcrumb trail is Administration > Identity Management > Groups > User Identity Groups > FMC and FTD admins. The 'Identity Group' section has a '\* Name' field containing 'FMC and FTD admins' and a 'Description' field containing 'FMC and FTD admins ISE local.'. At the bottom, there are 'Save' and 'Reset' buttons, with the 'Save' button highlighted by a red box.

Passaggio 4.1. Creare il secondo gruppo per l'utente ReadOnly.

The screenshot shows the configuration page for an 'Identity Group' named 'FMC and FTD ReadOnly'. The breadcrumb trail is Administration > Identity Management > Groups > User Identity Groups > FMC and FTD ReadOnly. The 'Identity Group' section has a '\* Name' field containing 'FMC and FTD ReadOnly' and a 'Description' field containing 'FMC and FTD ReadOnly.'. At the bottom, there are 'Save' and 'Reset' buttons, with the 'Save' button highlighted by a red box.

Passaggio 4.2. Verificare che entrambi i gruppi siano visualizzati nell'elenco Gruppi identità utente. Utilizzare il filtro per trovarli facilmente.

The screenshot shows the Cisco ISE Administration interface for Identity Management. The main heading is 'User Identity Groups'. On the left, there is a sidebar for 'Identity Groups' with a search bar and a tree view showing 'Endpoint Identity Groups' and 'User Identity Groups'. The main content area has a toolbar with 'Edit', '+ Add', 'Delete', 'Import', and 'Export' buttons. Below the toolbar is a table with columns 'Name' and 'Description'. The table contains one entry: 'fmc'. Below the table, there are two rows of user groups: 'FMC and FTD ReadOnly' and 'FMC and FTD admins ISE local'. A 'Quick Filter' dropdown is visible on the right, and a red box highlights the 'Add' button in the toolbar.

Passaggio 5. Creare gli utenti locali e aggiungerli al gruppo corrispondente. Passare a > Amministrazione > Gestione delle identità > Identità > + Aggiungi.

The screenshot shows the Cisco ISE Administration interface for Identity Management. The main heading is 'Network Access Users'. On the left, there is a sidebar for 'Users' with a search bar and a tree view showing 'Latest Manual Network Scan Res...'. The main content area has a toolbar with 'Edit', '+ Add', 'Change Status', 'Import', 'Export', and 'Delete' buttons. Below the toolbar is a table with columns: 'Status', 'Username', 'Description', 'First Name', 'Last Name', 'Email Address', 'User Identity Groups', and 'Adn'. The table is currently empty, with the text 'No data available' displayed below it. A red box highlights the '+ Add' button in the toolbar.

Passaggio 5.1. Creare innanzitutto l'utente con diritti di amministratore. Assegnare un nome, una password e il gruppo FMC e FTD admins.

## Users

Latest Manual Network Scan Res...

Network Access Users List &gt; New Network Access User

## Network Access User

\* Username firewall\_admin

Status  Enabled ▾

Account Name Alias  ⓘ

Email

## Passwords

Password Type: Internal Users ▾

Password Lifetime:

- With Expiration ⓘ
- Never Expires ⓘ

	Password	Re-Enter Password	
* Login Password	<input type="password"/>	<input type="password"/>	<input type="button" value="Generate Password"/> ⓘ
Enable Password	<input type="password"/>	<input type="password"/>	<input type="button" value="Generate Password"/> ⓘ

## Users

Latest Manual Network Scan Res...

## User Groups

 ⓘ +FMC and FTD admins ▾

Passaggio 5.2. Aggiungere l'utente con diritti di sola lettura. Assegnare un nome, una password e il gruppo FMC e FTD ReadOnly.

Users  
Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

\* Username firewall\_readuser

Status  Enabled ▾

Account Name Alias  ⓘ

Email

Passwords

Password Type: Internal Users ▾

Password Lifetime:

With Expiration ⓘ

Never Expires ⓘ

Password Re-Enter Password

\* Login Password    ⓘ

Enable Password    ⓘ

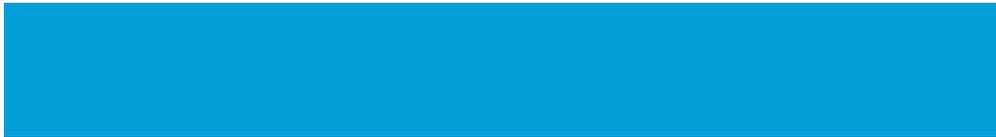
Users  
Latest Manual Network Scan Res...

User Groups

⋮ FMC and FTD ReadOnly ▾ ⓘ +

Passaggio 6. Creare il profilo di autorizzazione per l'utente Admin.

Passare a



> Criterio > Elementi criteri > Risultati > Autorizzazione > Profili di autorizzazione > +Aggiungi.

Definire un nome per il profilo di autorizzazione, lasciare il tipo di accesso impostato su ACCESS\_ACCEPT e in Impostazioni avanzate attributi aggiungere un raggio > Classe—[25] con il valore Administrator e fare clic su Submit (Invia).

The screenshot shows the Cisco ISE web interface for configuring a Policy Element. The breadcrumb trail is: Policy > Policy Elements > Authorization Profiles > FMC and FTD Admins. The main heading is "Authorization Profile". The configuration fields are as follows:

- Name:** FMC and FTD Admins
- Description:** (Empty text area)
- Access Type:** ACCESS\_ACCEPT (selected from a dropdown menu)
- Network Device Profile:** Cisco (selected from a dropdown menu)
- Service Template:** (Empty selection box)

The left sidebar shows a navigation menu with categories: Authentication (Allowed Protocols), Authorization (Authorization Profiles, Downloadable ACLs), Profiling, Posture, and Client Provisioning. The "Results" tab is currently active.

Dictionarys Conditions **Results**

Authentication >

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Advanced Attributes Settings

⋮ Radius:Class = Administrator - +

Attributes Details

Access Type = ACCESS\_ACCEPT  
Class = Administrator

**Submit** Cancel

Passaggio 7. Ripetere il passaggio precedente per creare il profilo di autorizzazione per l'utente di sola lettura. Creare la classe Radius con il valore ReadUser invece di Administrator.

Dictionarys Conditions **Results**

Authentication >

Allowed Protocols

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Authorization Profiles > New Authorization Profile

Authorization Profile

\* Name FMC and FTD ReadUser

Description

\* Access Type ACCESS\_ACCEPT

Network Device Profile Cisco

Service Template

Navigation: Dictionaries | Conditions | **Results**

Left sidebar menu:

- Authentication >
- Authorization ▾
  - Authorization Profiles
  - Downloadable ACLs
- Profiling >
- Posture >
- Client Provisioning >

Main content area:

Advanced Attributes Settings

⋮ Radius:Class ▾ = ReadUser ▾ - +

Attributes Details

Access Type = ACCESS\_ACCEPT  
Class = ReadUser

Buttons: **Submit** (highlighted with a red box) | Cancel

Passaggio 8. Creare un set di criteri corrispondente all'indirizzo IP del CCP. In questo modo si impedisce ad altre periferiche di concedere l'accesso agli utenti.



Selezionare

> Criterio > Set di criteri > icona



posizionata nell'angolo superiore sinistro.

**Cisco ISE** Policy · Policy Sets Q ? 🗨 ⚙

Policy Sets Reset Reset Policyset Hitcounts Save

<span>+</span>	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	🟢	Default	Default policy set		Default Network Access <span>📧</span> <span>⌵</span> <span>+</span>	45	⚙	➔

Reset Save

Passaggio 8.1. Una nuova riga viene posizionata all'inizio dei set di criteri.

Assegnare un nome al nuovo criterio e aggiungere una condizione superiore per l'attributo RADIUS NAS-IP-Address corrispondente all'indirizzo IP della console centrale di gestione.

Aggiungere una seconda condizione con la congiunzione OR per includere l'indirizzo IP dell'FTD.

Fate clic su Usa (Use) per mantenere le modifiche e uscire dall'editor.

Conditions Studio

Library

Search by Name

5G

Catalyst\_Switch\_Local\_Web\_Authentication

Source FMC

Switch\_Local\_Web\_Authentication

Switch\_Web\_Authentication

Wired\_802.1X

Wired\_MAB

Wireless\_802.1X

Wireless\_Access

Editor

Radius-NAS-IP-Address

Equals 192.168.192.60

OR

Radius-NAS-IP-Address

Equals 192.168.192.83

NEW AND OR

Set to 'is not'

Duplicate Save

Close Use

Passaggio 8.2. Al termine, fare clic su Salva.

Cisco ISE

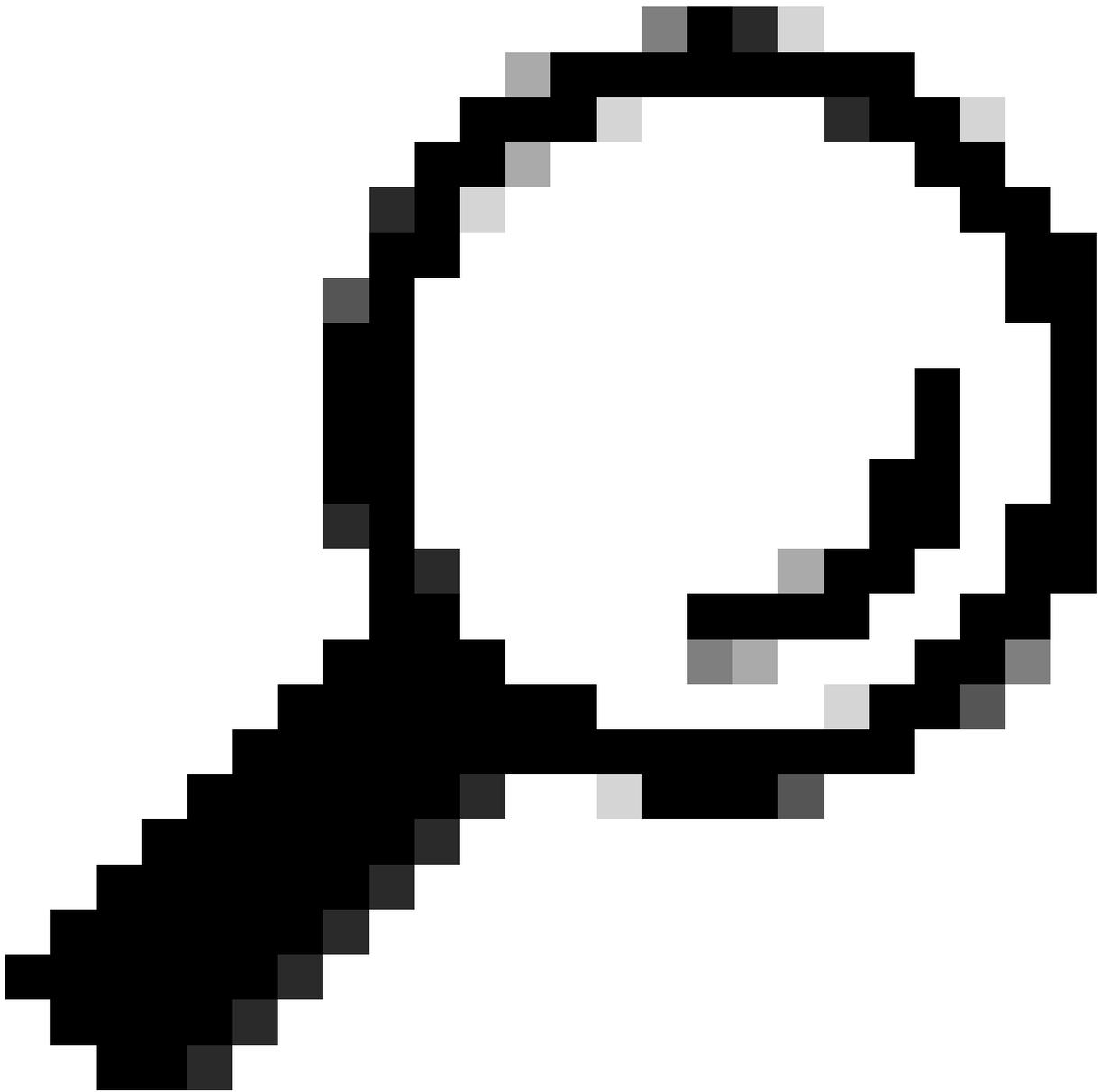
Policy · Policy Sets

Policy Sets

Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	FMC and FTD Access	Management Access	OR Radius-NAS-IP-Address EQUALS 192.168.192.60 Radius-NAS-IP-Address EQUALS 192.168.192.83	Default Network Access	0	⚙️	➔
✓	Default	Default policy set		Default Network Access	0	⚙️	➔

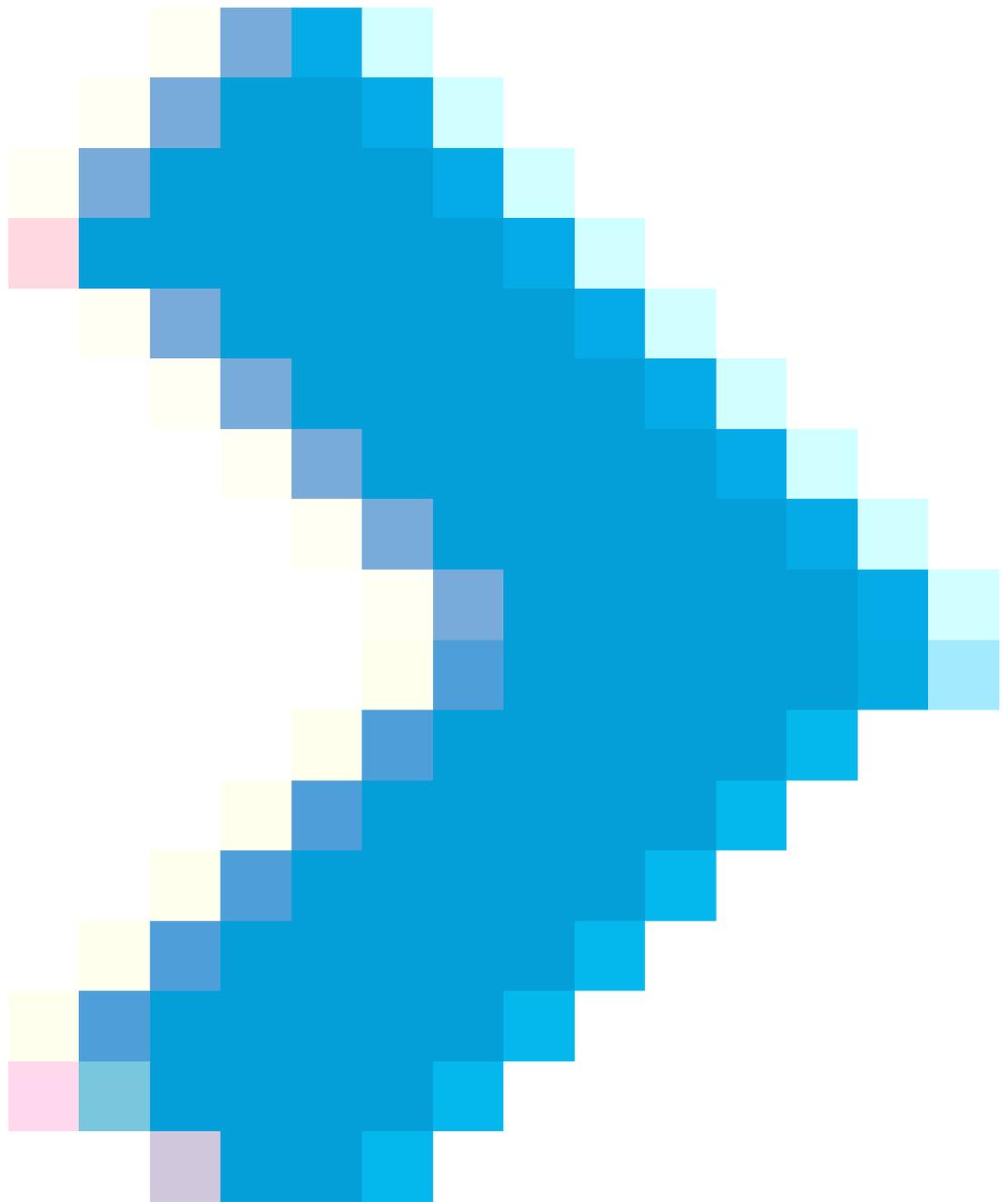
Reset Save



Suggerimento: per questo esercizio è stato consentito l'utilizzo dell'elenco Protocolli di accesso alla rete predefiniti. È possibile creare un nuovo elenco e restringerlo in base alle esigenze.

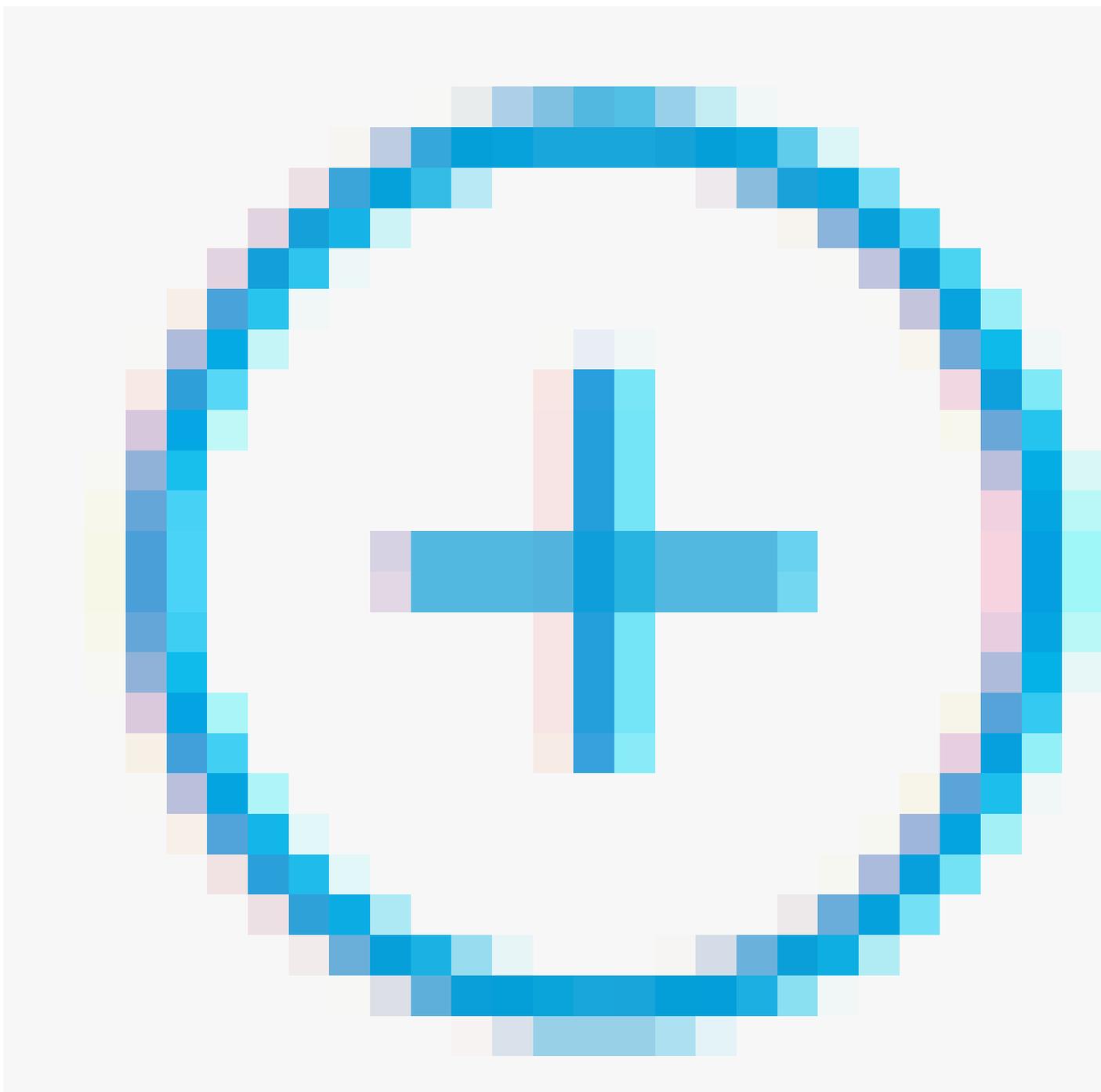
---

Passaggio 9. Visualizzare il nuovo set di criteri facendo clic sull



'icona posizionata alla fine della riga.

Espandere il menu Criteri di autorizzazione e fare clic sull



Icona per aggiungere una nuova regola per consentire l'accesso all'utente con diritti di amministratore.

Dagli un nome.

Impostare le condizioni in modo che corrispondano al gruppo di identità del dizionario con Nome attributo Uguale a Gruppi di identità utente: Amministratori FMC e FTD (il nome del gruppo creato nel passaggio 4) e fare clic su Usa.



attributo Uguale a Gruppi di identità utente: FMC e FTD Sola lettura (il nome del gruppo creato al passaggio 4) e fare clic su Usa.

## Conditions Studio

Passaggio 11. Impostare i profili di autorizzazione per ogni regola e fare clic su Salva.

## Configurazione FMC

Passaggio 1. Creare l'oggetto di autenticazione esterna in Sistema > Utenti > Autenticazione esterna > + Aggiungi oggetto di autenticazione esterna.

Firewall Management Center  
System / Users / External Authentication

Overview Analysis Policies Devices Objects Integration Deploy 🔍 🟢 ⚙️ 👤 admin 🔒 cisco SECURE

Users User Roles External Authentication Single Sign-On (SSO)

Default User Role: None Shell Authentication Disabled

Save Cancel Save and Apply

+ Add External Authentication Object

Name	Method	Enabled
No data to Represent		

Passaggio 2. Selezionare RADIUS come metodo di autenticazione.

In Oggetto autenticazione esterna assegnare un nome al nuovo oggetto.

Quindi, nell'impostazione Server primario, inserire l'indirizzo IP ISE e la stessa chiave privata RADIUS usata nel passo 2 della configurazione ISE.

Firewall Management Center  
System / Users / Create External Authentication Object

Overview Analysis Policies Devices Objects Integration Deploy 🔍 🟢 ⚙️ 👤 admin 🔒 cisco SECURE

Users User Roles External Authentication Single Sign-On (SSO)

### External Authentication Object

Authentication Method: RADIUS

Name: ISE\_Radius

Description:

### Primary Server

Host Name/IP Address: 192.168.192.90 (ex. IP or hostname)

Port: 1812

RADIUS Secret Key: ●●●●●●●●

### Backup Server (Optional)

Host Name/IP Address: (ex. IP or hostname)

Port: 1812

RADIUS Secret Key:

### RADIUS-Specific Parameters

Timeout (Seconds): 30

Passaggio 3. Inserire i valori degli attributi della classe RADIUS configurati nei passaggi 6 e 7 della configurazione ISE: Administrator e ReadUser rispettivamente per firewall\_admin e firewall\_readuser.

**RADIUS-Specific Parameters**

Timeout (Seconds)

Retries

Access Admin

Administrator

Discovery Admin

External Database User

Intrusion Admin

Maintenance User

Network Admin

Security Analyst

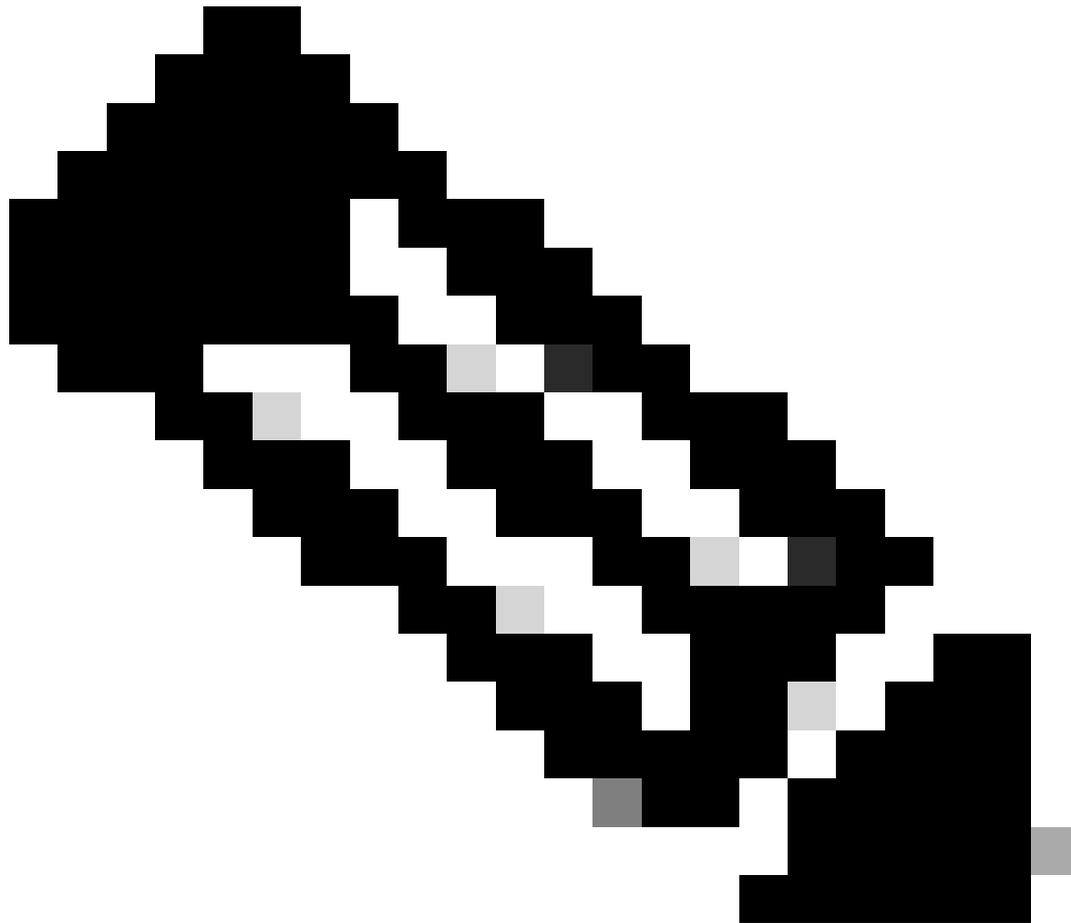
Security Analyst (Read Only)

Security Approver

Threat Intelligence Director (TID) User

Default User Role

To specify the default user role if user is not found in any group



Nota: l'intervallo di timeout è diverso per l'FTD e il FMC, quindi se si condivide un oggetto e si modifica il valore predefinito di 30 secondi, assicurarsi di non superare l'intervallo di timeout più piccolo (1-300 secondi) per i dispositivi FTD. Se si imposta il timeout su un valore superiore, la configurazione RADIUS di difesa dalle minacce non funziona.

---

Passaggio 4. Compilare l'elenco degli utenti di accesso alla CLI dell'amministratore in CLI Access Filter con i nomi utente autorizzati ad accedere alla CLI.

Fare clic su Save (Salva) una volta terminato.

### CLI Access Filter

(For Firewall Management Center (all versions) and Firewall Threat Defense (6.2.3 and 6.3), define users for CLI access. For Firewall Threat Defense 6.4 and later, we recommend defining users on the RADIUS server. Click [here](#) for more information)

Administrator CLI Access User List  ex. user1, user2, user3 (lowercase letters only).

▸ Define Custom RADIUS Attributes

Additional Test Parameters

User Name

Password

\*Required Field

Passaggio 5. Attivare il nuovo oggetto. Impostarlo come metodo di autenticazione della shell per FMC e fare clic su Salva e applica.

Firewall Management Center  
System / Users / External Authentication

Overview Analysis Policies Devices Objects Integration Deploy

Users User Roles External Authentication Single Sign-On (SSO)

Default User Role: None Shell Authentication Enabled (ISE\_Radius) + Add External Authentication Object

Name	Method	Enabled	
1. ISE_Radius	RADIUS	<input checked="" type="checkbox"/>	

## Configurazione FTD

Passaggio 1. Nell'interfaccia utente di FMC, selezionare Devices > Platform Settings (Dispositivi > Impostazioni piattaforma). Modificare il criterio corrente o crearne uno nuovo se non si dispone di alcuna assegnazione all'FTD a cui è necessario accedere. Abilitare il server RADIUS in Autenticazione esterna e fare clic su Salva.

Firewall Management Center  
Devices / Platform Settings Editor

Overview Analysis Policies Devices Objects Integration

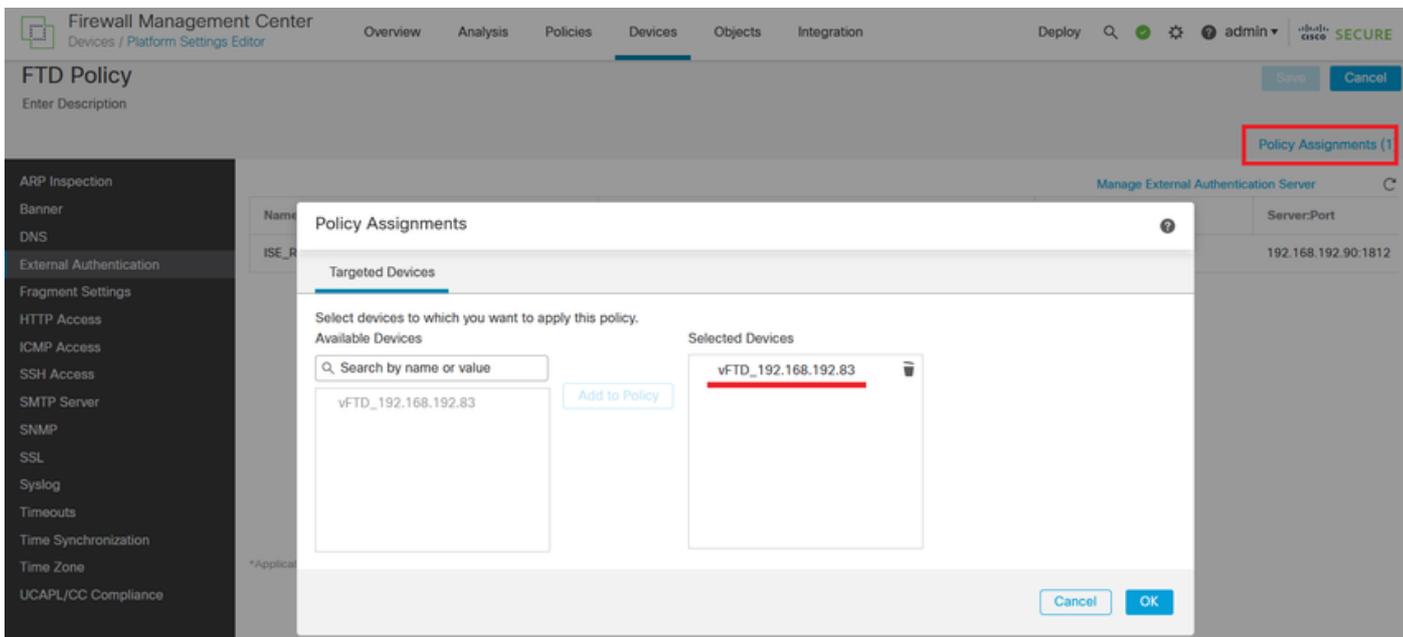
FTD Policy You have unsaved changes

Enter Description

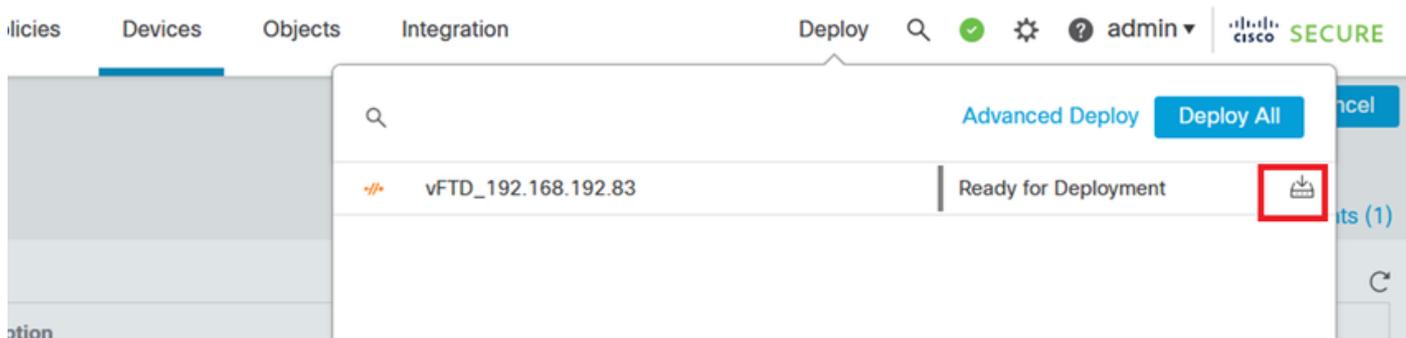
Manage External Authentication Server

Name	Description	Method	Server/Port	Encryption	Enabled
ISE_Radius		RADIUS	192.168.192.90:1812	no	<input checked="" type="checkbox"/>

Passaggio 2. Accertarsi che l'FTD a cui è necessario accedere sia elencato in Assegnazioni criteri come dispositivo selezionato.



Passaggio 3. Distribuire le modifiche.



## Verifica

- Verificare che la nuova distribuzione funzioni correttamente.
- Nell'interfaccia utente di FMC passare alle impostazioni del server RADIUS e scorrere verso il basso fino alla sezione Parametri di test aggiuntivi.
- Immettere un nome utente e una password per l'utente ISE e fare clic su Test.



- Se il test ha esito positivo, nella parte superiore della finestra del browser viene visualizzato il messaggio verde Test completato.



Success  
Test Complete.

### External Authentication Object

Authentication Method

Name \*

- Per ulteriori informazioni, espandere Dettagli in Output test.

▸ Define Custom RADIUS Attributes

### Additional Test Parameters

User Name

Password

### Test Output

Show Details

```
check_auth_radius: szUser: firewall_admin
RADIUS config file: /var/tmp/4VQqxhXof/radiusclient_0.conf
radiusauth - response: [User-Name=firewall_admin]
radiusauth - response: [Class=Administrator]
radiusauth - response: [Class=CACS:c0a8c05a_cNaQKf8ZB2sOTPFOSbmj8V6n727Es2627TeUjzXUdA:ISE-LVILLAFR/479011358/67]
"firewall_admin" RADIUS Authentication OK
check_is_radius_member attrib match found: [Class=Administrator] - [Class=Administrator] *****
role_bee2eb18-e129-11df-a04a-42c66f0a3b36:
```

\*Required Field

## 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).