

Firepower eXtensible Operating System (FXOS)

2.2: Autenticazione/autorizzazione dello chassis per la gestione remota con ISE tramite TACACS+

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurazione dello chassis FXOS](#)

[Configurazione del server ISE](#)

[Verifica](#)

[Verifica chassis FXOS](#)

[Verifica ISE 2.0](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come configurare l'autenticazione e l'autorizzazione TACACS+ per lo chassis Firepower eXtensible Operating System (FXOS) tramite Identity Services Engine (ISE).

Lo chassis FXOS include i seguenti ruoli utente:

- Amministratore: accesso completo in lettura e scrittura all'intero sistema. All'account amministratore predefinito viene assegnato questo ruolo per impostazione predefinita e non può essere modificato.
- Sola lettura - Accesso in sola lettura alla configurazione del sistema senza privilegi per la modifica dello stato del sistema.
- Operazioni: accesso in lettura e scrittura alla configurazione NTP, alla configurazione di Smart Call Home per Smart Licensing e ai registri di sistema, inclusi i server syslog e i relativi errori. Accesso in lettura al resto del sistema.
- AAA: accesso in lettura e scrittura a utenti, ruoli e configurazione AAA. Accesso in lettura al resto del sistema.

Dalla CLI, questa condizione può essere vista come segue:

```
fpr4120-TAC-A /security* # show role
```

Ruolo:

Priv nome ruolo

—

aaa aaa

admin admin

operazioni

sola lettura

Contributo di Tony Ramirez, Jose Soto, Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza di Firepower eXtensible Operating System (FXOS)
- Conoscenza della configurazione ISE
- Per ISE, è richiesta la licenza TACACS+ Device Administration

Componenti usati

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

- Cisco Firepower 4120 Security Appliance versione 2.2
- Virtual Cisco Identity Services Engine 2.2.0.470

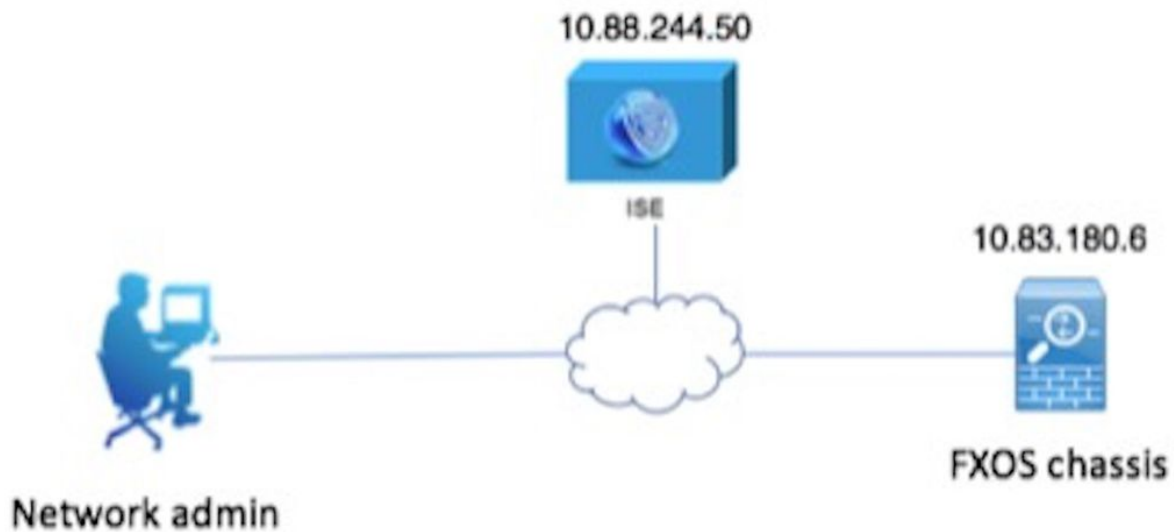
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Configurazione

L'obiettivo della configurazione è:

- Autenticazione degli utenti che accedono alla GUI e SSH basata sul Web di FXOS tramite ISE
- Permette agli utenti di accedere alla GUI basata sul Web di FXOS e al protocollo SSH in base al loro ruolo con ISE.
- Verificare il corretto funzionamento dell'autenticazione e dell'autorizzazione su FXOS tramite ISE

Esempio di rete



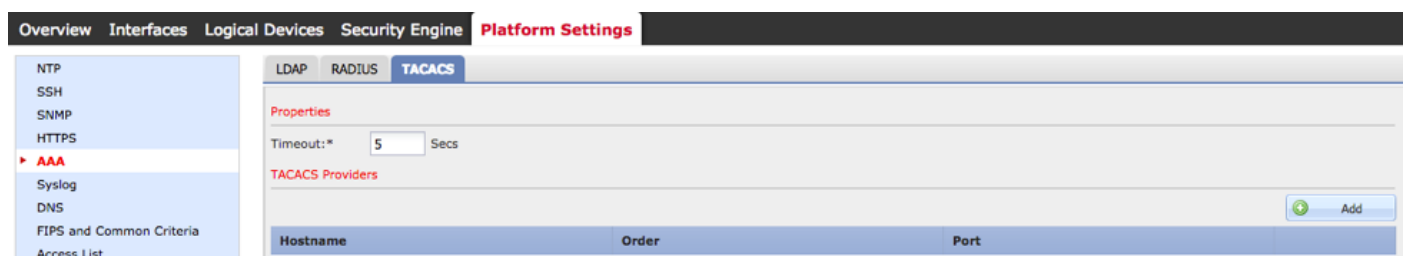
Configurazioni

Configurazione dello chassis FXOS

Creazione di un provider TACACS+

Passaggio 1. Passare a **Impostazioni piattaforma > AAA**.

Passaggio 2. Fare clic sulla scheda **TACACS**.

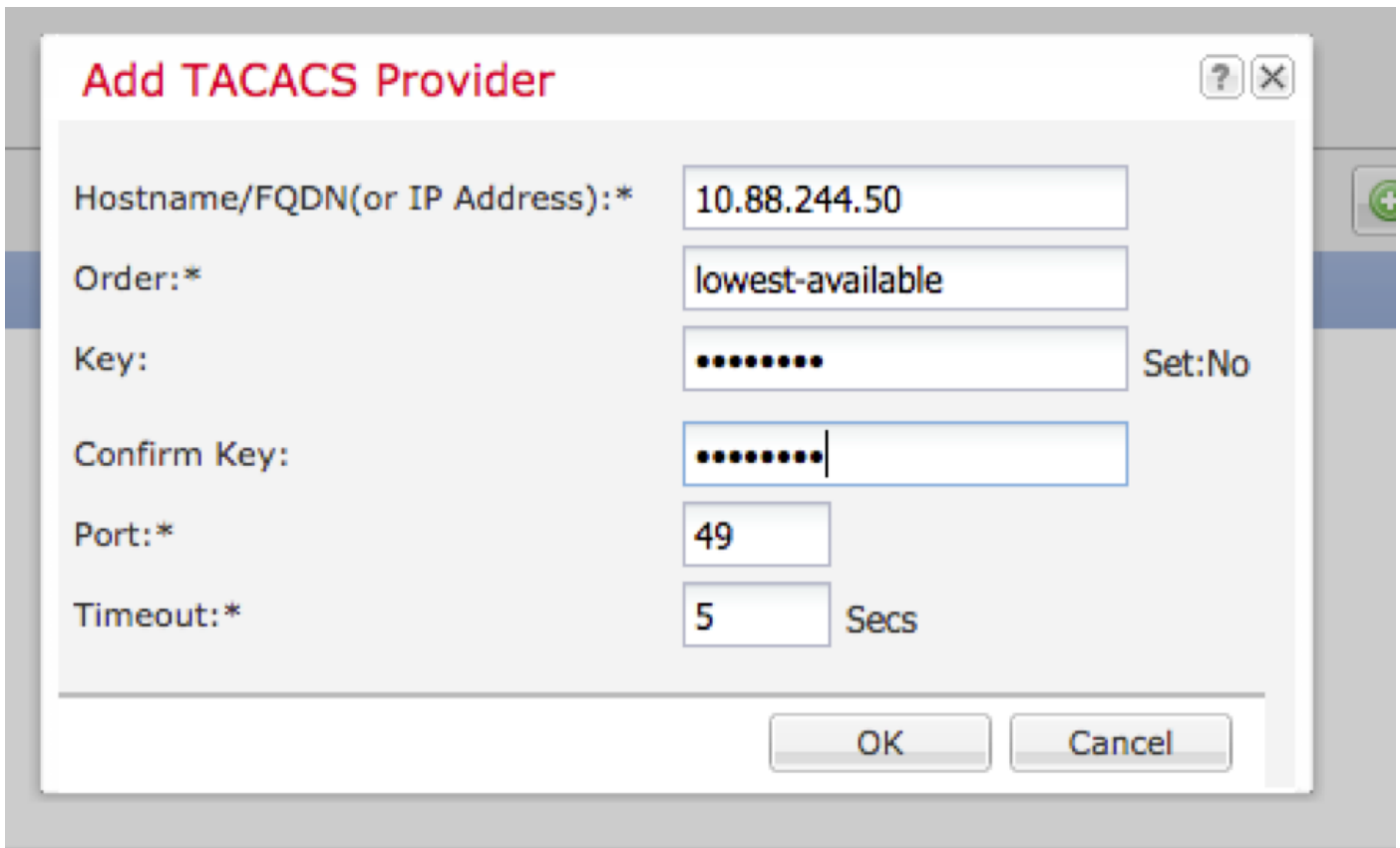


Passaggio 3. Per ogni provider TACACS+ che si desidera aggiungere (fino a 16 provider).

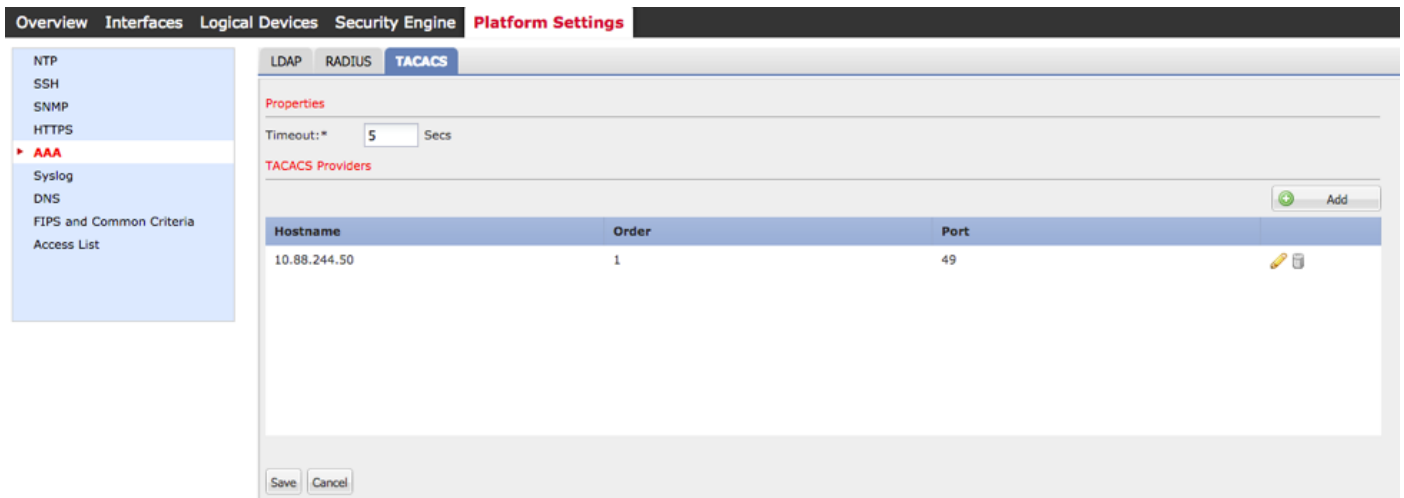
3.1. Nell'area dei provider TACACS, fare clic su **Add**.

3.2. Una volta aperta la finestra di dialogo **Aggiungi provider TACACS**, immettere i valori richiesti.

3.3. Fare clic su **OK** per chiudere la finestra di dialogo **Aggiungi provider TACACS**.

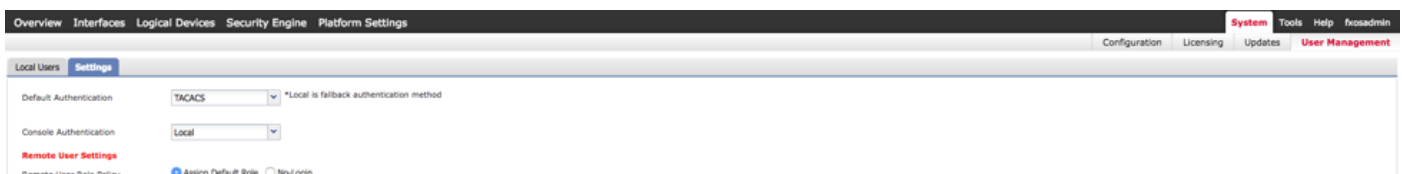


Passaggio 4. Fare clic su **Salva**.



Passaggio 5. Passare a **Sistema > Gestione utente > Impostazioni**.

Passaggio 6. In Autenticazione predefinita scegliere **TACACS**.



Creazione di un provider TACACS+ tramite CLI

Passaggio 1. Per abilitare l'autenticazione TACACS, eseguire i seguenti comandi.

fpr4120-TAC-A# **ambito sicurezza**

```
fpr4120-TAC-A /security # ambito default-auth
```

```
fpr4120-TAC-A /security/default-auth # set realm tacacs
```

Passaggio 2. Per verificare la configurazione, utilizzare il comando **show detail**.

```
fpr4120-TAC-A /security/default-auth # show detail
```

Autenticazione predefinita:

Area di autenticazione amministrativa: **Tacacacs**

Area operativa: **Tacacacs**

Periodo di aggiornamento sessione Web (sec): 600

Timeout sessione (in sec) per sessioni Web, ssh e telnet: 600

Timeout sessione assoluta (in secondi) per sessioni Web, ssh e telnet: 3600

Timeout sessione console seriale (sec): 600

Timeout sessione assoluta console seriale (sec): 3600

Gruppo server Autenticazione amministratore:

Gruppo server di autenticazione operativo:

Utilizzo del secondo fattore: No

Passaggio 3. Per configurare i parametri del server TACACS, eseguire i seguenti comandi.

```
fpr4120-TAC-A# ambito sicurezza
```

```
fpr4120-TAC-A /security # ambito tacacs
```

```
fpr4120-TAC-A /security/tacacs # invio al server 10.88.244.50
```

```
fpr4120-TAC-A /security/tacacs/server # set descr "server ACS"
```

```
fpr4120-TAC-A /security/tacacs/server* # set key
```

Immettere la chiave: *****

Confermare la chiave: *****

Passaggio 4. Per verificare la configurazione, usare il comando **show detail**.

```
fpr4120-TAC-A /security/tacacs/server* # show detail
```

Server TACACS+:

Nome host, FQDN o indirizzo IP: 10.88.244.50

Descr.:

Ordine: 1

Port: 49

Chiave: ****

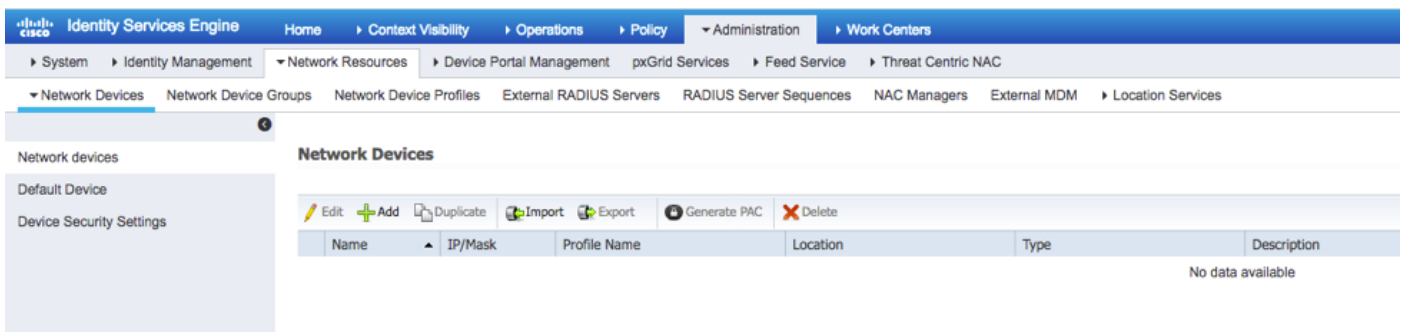
Timeout: 5

Configurazione del server ISE

Aggiunta di FXOS come risorsa di rete

Passaggio 1. Passare a **Amministrazione > Risorse di rete > Dispositivi di rete.**

Passaggio 2. Fare clic su **ADD.**



Passaggio 3. Immettere i valori richiesti (Nome, Indirizzo IP, Tipo di dispositivo, Abilita TACACS+ e aggiungere la CHIAVE), quindi fare clic su **Submit (Invia).**

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network devices

Default Device

Device Security Settings

Network Devices List > FXOS

Network Devices

* Name

Description

* IP Address: /

* Device Profile

Model Name

Software Version

* Network Device Group

Device Type

IPSEC

Location

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

SNMP Settings

Advanced TrustSec Settings

Creazione di gruppi di identità e utenti

Passo 1: passare a Amministrazione > Gestione delle identità > Gruppi > Gruppi identità utente.

Passaggio 2. Fare clic su ADD.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Identity Groups

Endpoint Identity Groups

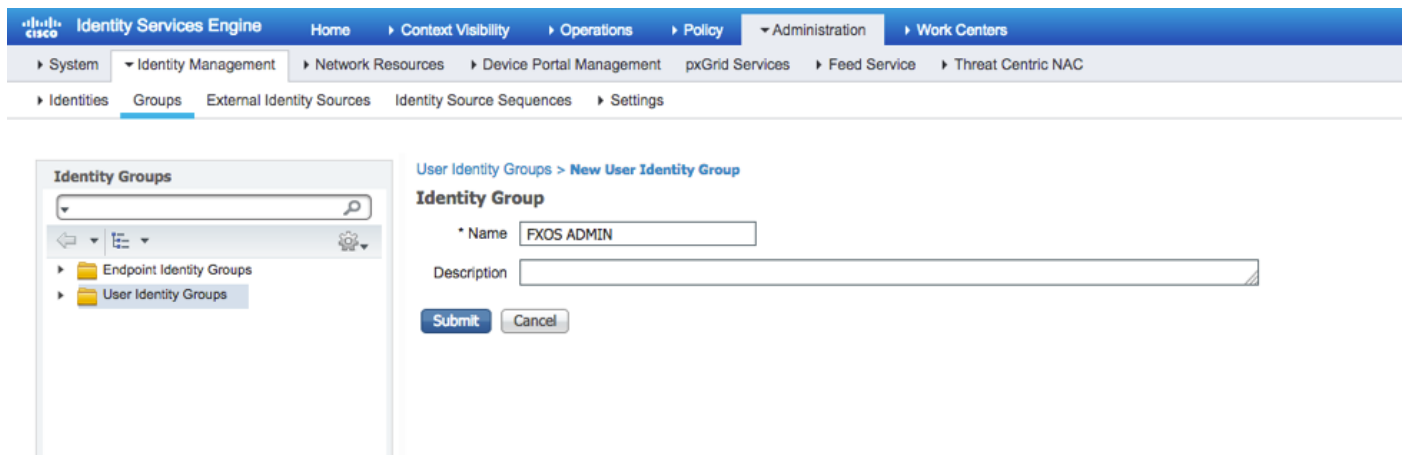
User Identity Groups

User Identity Groups

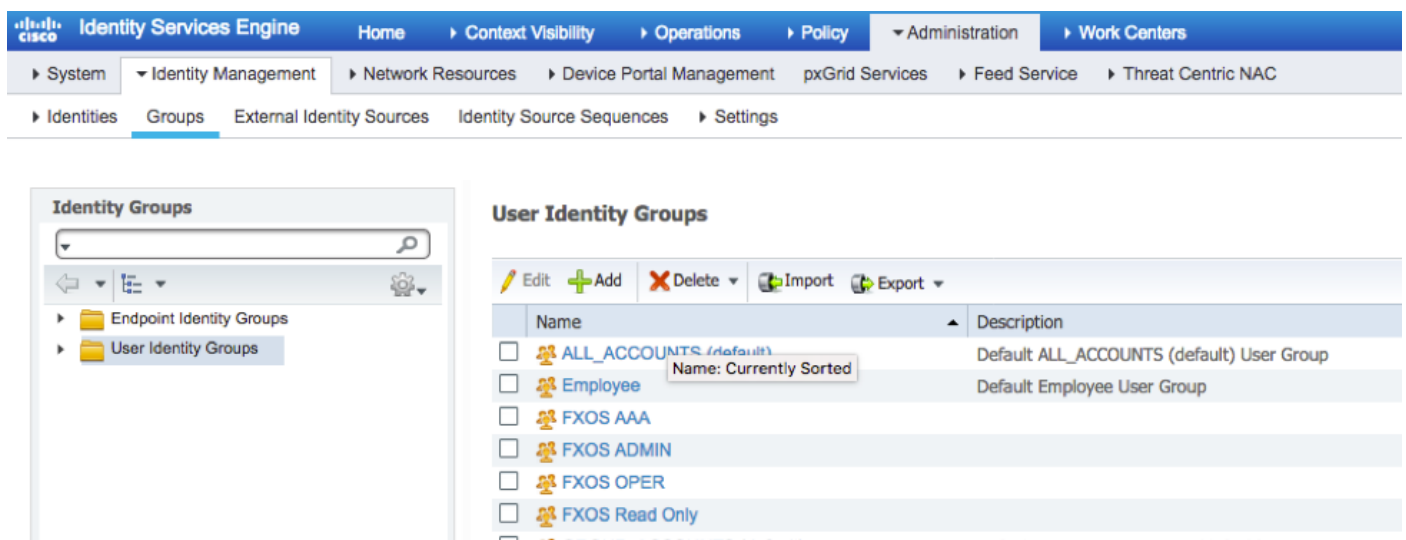
Edit Add Delete Import Export

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/> GuestType_Contractor (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Daily (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Weekly (default)	Identity group mirroring the guest type
<input type="checkbox"/> OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

Passaggio 3. Immettere il valore per Nome e fare clic su **Sottometti**.

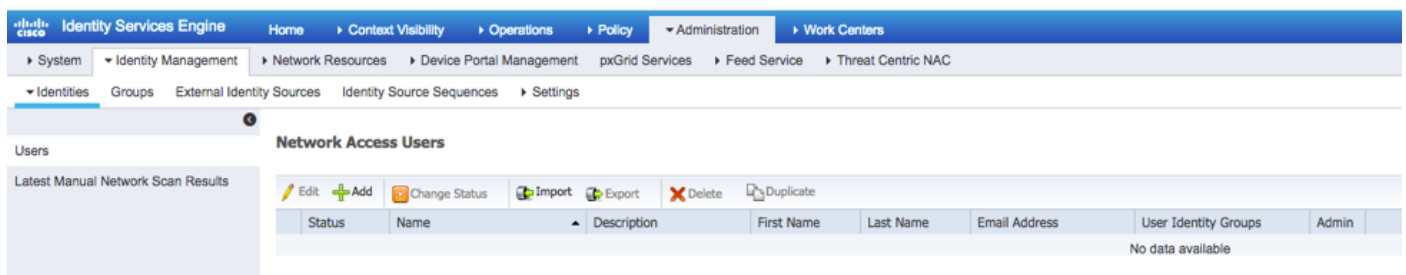


Passaggio 4. Ripetere il passaggio 3 per tutti i ruoli utente richiesti.



Passaggio 5. Passare a **Amministrazione > Gestione delle identità > Identità > Utenti**.

Passaggio 6. Fare clic su **ADD**.



Passaggio 7. Inserire i valori richiesti (Nome, Gruppo di utenti, Password).

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users List > New Network Access User

Network Access User

Name:

Status: Enabled

Email:

Passwords

Password Type: Internal Users

Password: Re-Enter Password: *i*

Enable Password: *i*

User Information

First Name:

Last Name:

Account Options

Description:

Change password on next login:

Account Disable Policy

Disable account if date exceeds: (yyyy-mm-dd)

User Groups

Passaggio 8. Ripetere il passaggio 6 per tutti gli utenti richiesti.

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users

Edit Add Change Status Import Export Delete Duplicate

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/> Enabled	fxosaaa					FXOS AAA	
<input type="checkbox"/> Enabled	fxosadmin					FXOS ADMIN	
<input type="checkbox"/> Enabled	fxosoper					FXOS OPER	
<input type="checkbox"/> Enabled	fxosro					FXOS Read Only	

Creazione del profilo di shell per ogni ruolo utente

Passaggio 1. Passare a Work Center > Device Administration > Policy Elements > Results > TACACS Profiles e fare clic su +ADD.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

TACACS Profiles

0 Selected Rows/Page 4 / 1 / 1 Go 4 Total Rows

Refresh Add Duplicate Trash Edit Filter

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile

Passaggio 2. Inserire i valori richiesti per il profilo TACACS

2.1. Inserire il nome.

TACACS Profiles > New

TACACS Profile

Name

Description

Task Attribute View Raw View

2.2. Nella SCHEDA Visualizzazione RAW configurare la seguente coppia CISCO-AV.

cisco-av-pair=shell:roles="admin"

TACACS Profile

Name

Description

Task Attribute View

Raw View

Profile Attributes

```
cisco-av-pair=shell:roles="admin"
```

Cancel

Submit

2.3. Fare clic su **Invia**.

TACACS Profile

Name

Description

Task Attribute View Raw View

Common Tasks

Common Task Type

<input type="checkbox"/> Default Privilege	<input type="text"/>	(Select 0 to 15)
<input type="checkbox"/> Maximum Privilege	<input type="text"/>	(Select 0 to 15)
<input type="checkbox"/> Access Control List	<input type="text"/>	
<input type="checkbox"/> Auto Command	<input type="text"/>	
<input type="checkbox"/> No Escape	<input type="text"/>	(Select true or false)
<input type="checkbox"/> Timeout	<input type="text"/>	Minutes (0-9999)
<input type="checkbox"/> Idle Time	<input type="text"/>	Minutes (0-9999)

Custom Attributes

+ Add Trash Edit

Type	Name	Value	
<input type="checkbox"/> MANDATORY	cisco-av-pair	shell:roles="admin"	

Cancel Save

Passaggio 3. Ripetere il passaggio 2 per gli altri ruoli utente utilizzando le seguenti coppie Cisco-AV.

cisco-av-pair=shell:roles="aaa"

cisco-av-pair=shell:roles="operazioni"

cisco-av-pair=shell:roles="sola lettura"

Custom Attributes

+ Add Trash Edit

Type	Name	Value	
<input type="checkbox"/> MANDATORY	cisco-av-pair	shell:roles="aaa"	

Cancel Save

Custom Attributes

+ Add Trash Edit ⚙️

<input type="checkbox"/>	Type	Name	Value	
<input type="checkbox"/>	MANDATORY	cisco-av-pair	shell:roles="operations"	<input type="checkbox"/> <input type="checkbox"/>

Custom Attributes

+ Add Trash Edit ⚙️

<input type="checkbox"/>	Type	Name	Value	
<input type="checkbox"/>	MANDATORY	cisco-av-pair	shell:roles="read-only"	<input type="checkbox"/> <input type="checkbox"/>

TACACS Profiles

0 Selected

Rows/Page 1 / 1 8 Total Rows

+ Add Duplicate Trash Edit Filter ⚙️

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile
<input type="checkbox"/>	FXOS_Admin_Profile	Shell	
<input type="checkbox"/>	FXOS_AAA_Shell	Shell	
<input type="checkbox"/>	FXOS_Operations_Shell	Shell	
<input type="checkbox"/>	FXOS_ReadOnly_Shell	Shell	

Creazione del criterio di autorizzazione TACACS

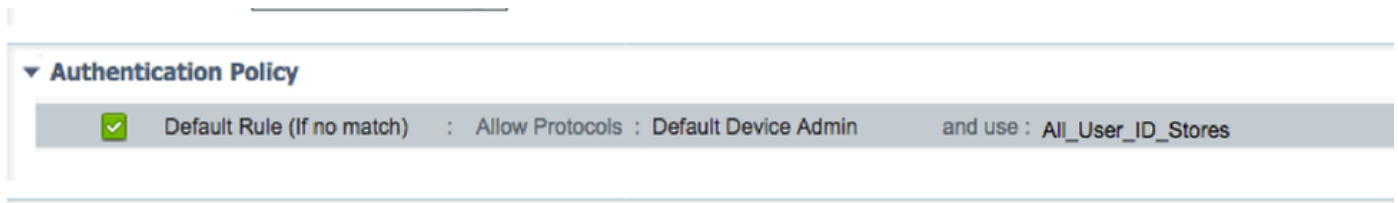
Passaggio 1. Passare a **Centri di lavoro > Amministrazione dispositivi > Set di criteri di amministrazione dispositivi**.

The screenshot shows the Cisco ISE configuration interface for the 'Tactics_Default' policy set. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows 'Policy Sets' with 'Tactics_Default' selected. The main content area is titled 'Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.' It includes sections for 'Proxy Server Sequence', 'Authentication Policy' (with a default rule for 'Allow Protocols'), and 'Authorization Policy' (with an 'Exceptions (0)' section). A table at the bottom lists the policy rules:

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
<input checked="" type="checkbox"/>	Tactics_Default	If no matches, then (Select Profiles)	Deny All Shell Profile	

Passaggio 2. Verificare che il criterio di autenticazione punti al database Internal Users o

all'archivio identità richiesto.



Passaggio 3. Fare clic sulla freccia alla fine del criterio di autorizzazione predefinito e fare clic su Inserisci regola.

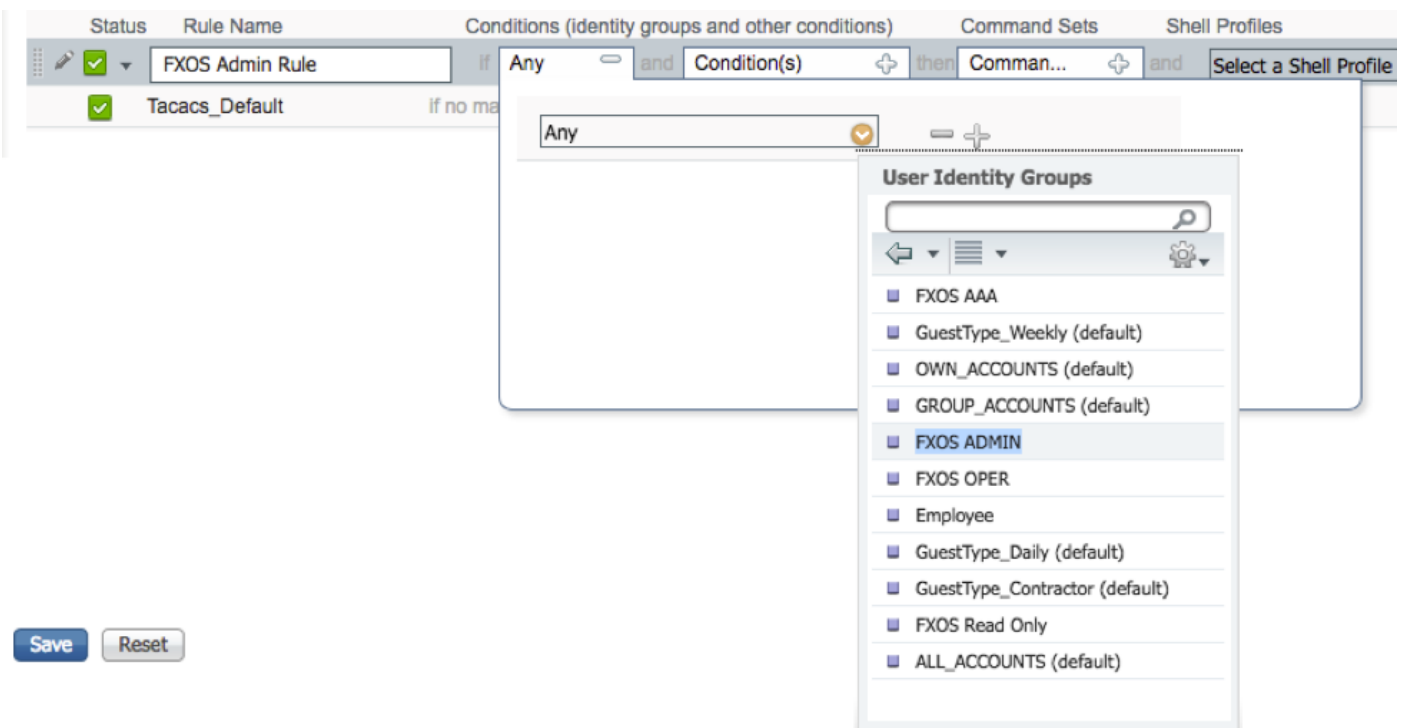


Passaggio 4. Inserire i valori per la regola con i parametri obbligatori:

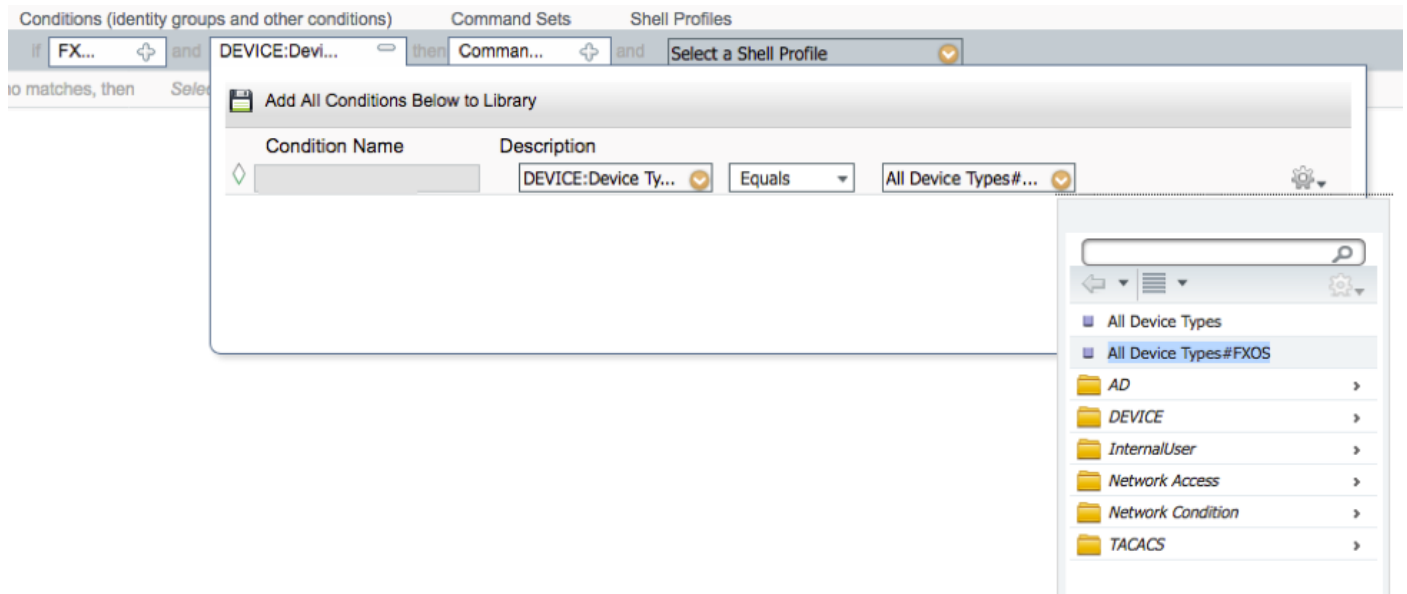
4.1. Nome della regola: Regola di amministrazione FXOS.

4.2. Condizioni.

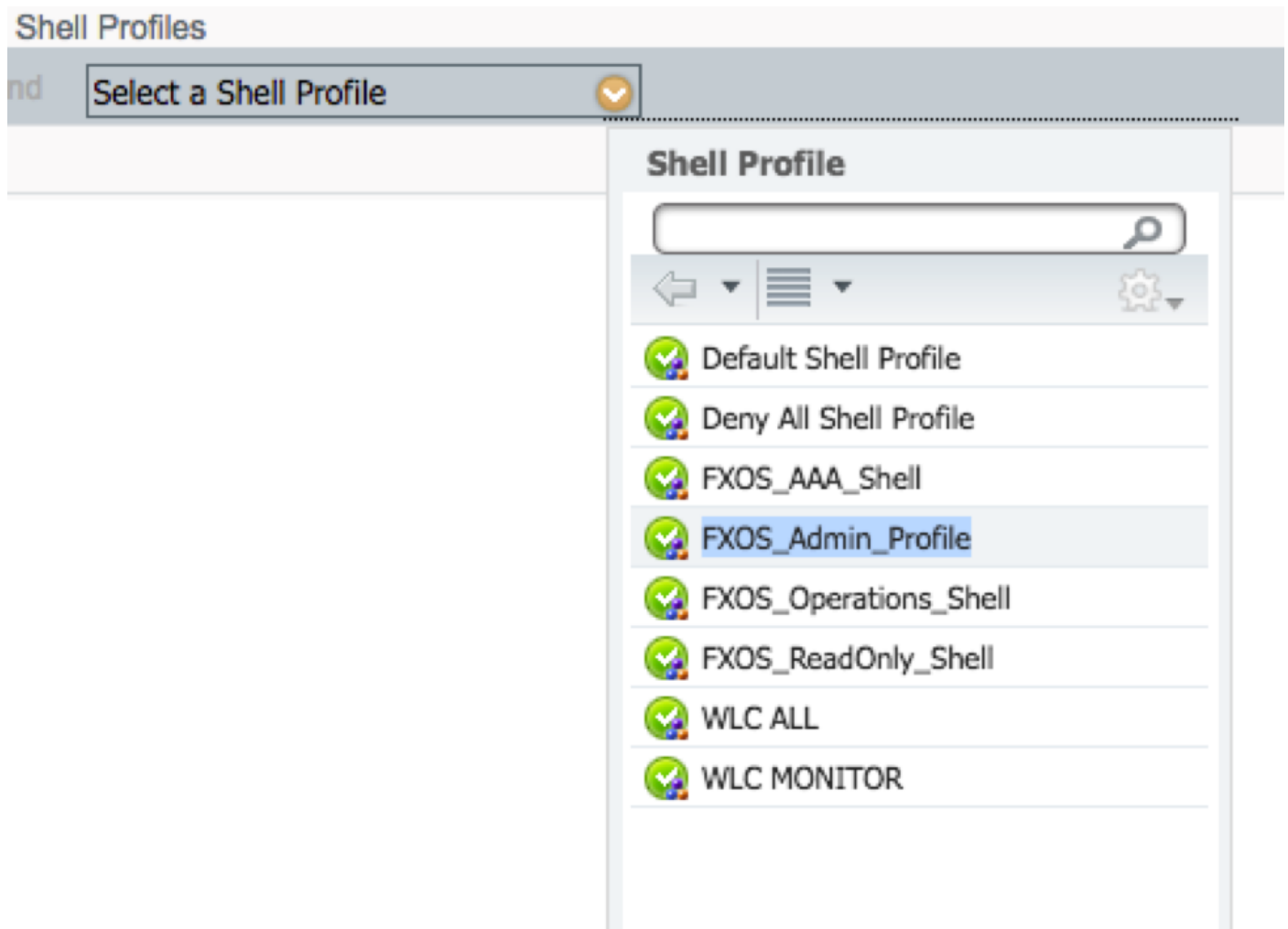
Se: Il gruppo di identità utente è FXOS ADMIN



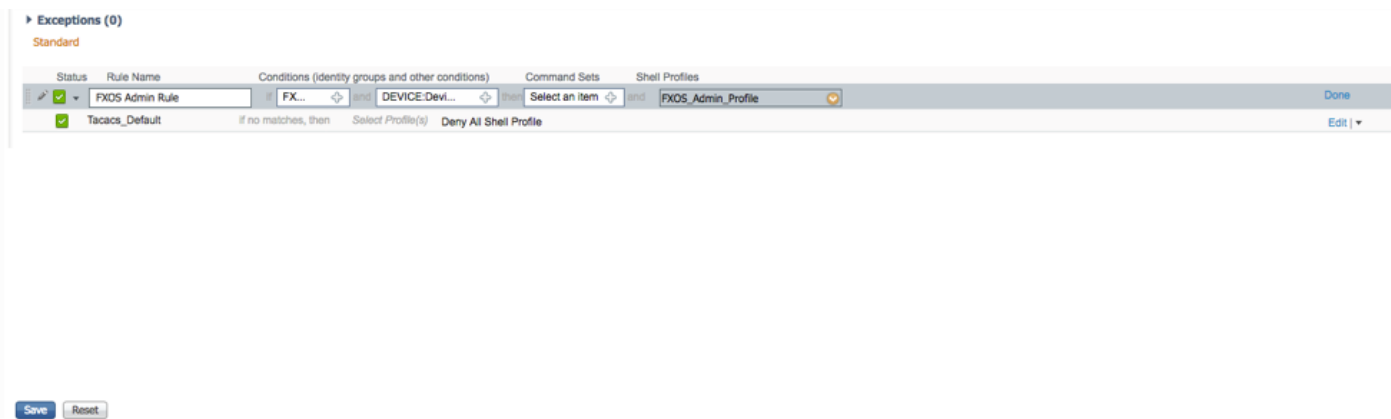
E Dispositivo: Tipo di dispositivo è uguale a Tutti i tipi di dispositivo #FXOS



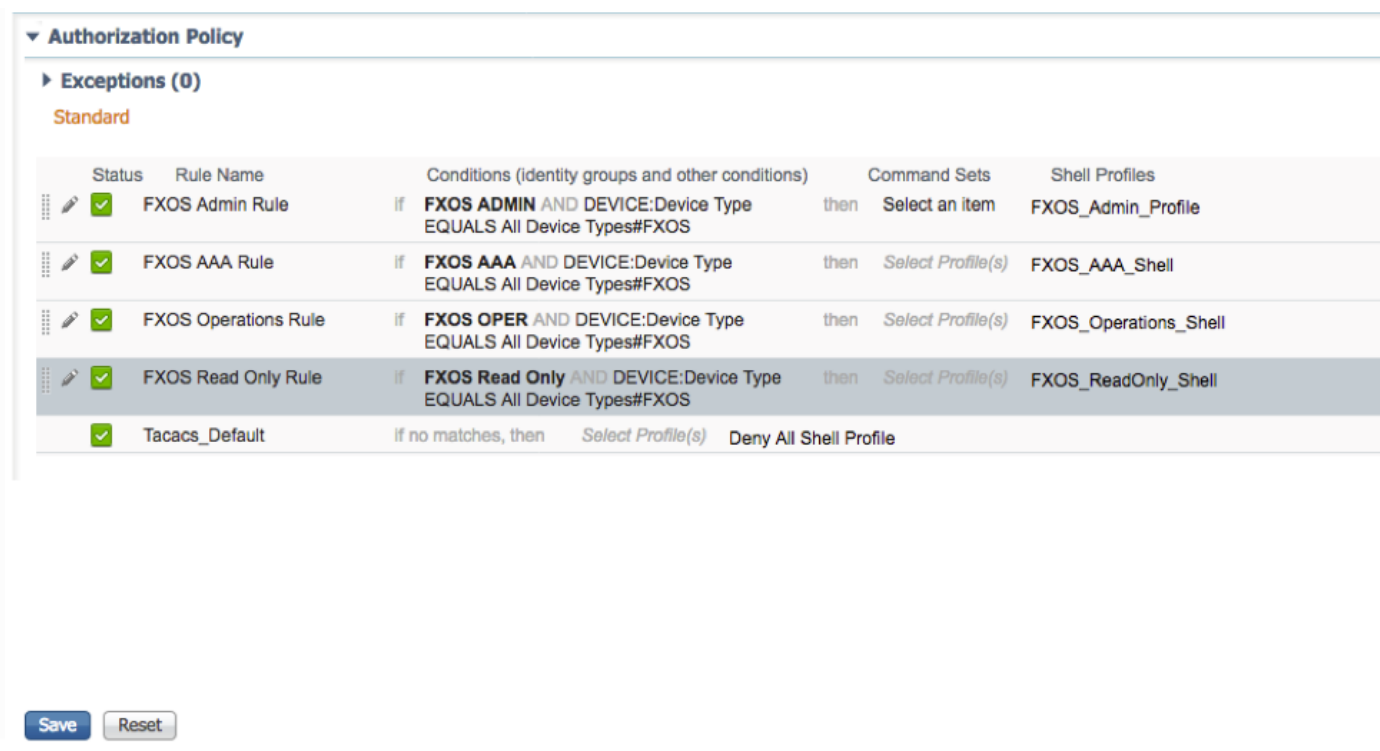
Profilo shell: Profilo_amministrazione_FXOS



Passaggio 5. Fare clic su **Fine**.



Passaggio 6. Ripetere i passaggi 3 e 4 per i ruoli utente rimanenti e al termine fare clic su **SAVE**.



Verifica

È ora possibile eseguire il test di ogni utente e verificare il ruolo utente assegnato.

Verifica chassis FXOS

1. Telnet o SSH sullo chassis FXOS ed effettuare il login utilizzando uno degli utenti creati sull'ISE.

Username: ffoxadmin

Password:

fpr4120-TAC-A# scope security

fpr4120-TAC-A /security # show remote-user detail

Utente remoto **fxosaaa**:

Descrizione:

Ruoli utente:

Nome: **aaa**

Nome: **read-only**

Utente remoto **fxosadmin**:

Descrizione:

Ruoli utente:

Nome: **admin**

Nome: **read-only**

Fxosoper utente remoto:

Descrizione:

Ruoli utente:

Nome: **operazioni**

Nome: **read-only**

Fxosro utente remoto:

Descrizione:

Ruoli utente:

Nome: **read-only**

A seconda del nome utente immesso, nella cli dello chassis FXOS verranno visualizzati solo i comandi autorizzati per il ruolo utente assegnato.

Ruolo utente amministratore.

fpr4120-TAC-A /security # ?

conferma conferma conferma

clear-user-session Cancella sessioni utente

creazione Creazione di oggetti gestiti

delete Elimina oggetti gestiti

disabilita Disabilita i servizi

abilita Abilita i servizi

enter Immette un oggetto gestito

scope Modifica la modalità corrente

impostare i valori delle proprietà

show Mostra informazioni di sistema

termina sessioni Active Cisco

fpr4120-TAC-A#connect fxos

fpr4120-TAC-A (fxos)# debug aaa-request

fpr4120-TAC-A (fxos)#

Ruolo Utente Di Sola Lettura.

fpr4120-TAC-A /security # ?

scope Modifica la modalità corrente

impostare i valori delle proprietà

show Mostra informazioni di sistema

fpr4120-TAC-A#connect fxos

fpr4120-TAC-A (fxos)# debug aaa-request

% Autorizzazione negata per il ruolo

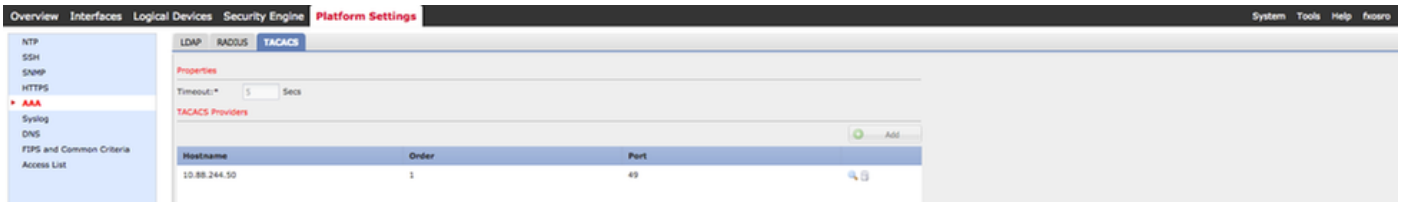
2. Individuare l'indirizzo IP dello chassis FXOS e accedere usando uno degli utenti creati sull'ISE.

Ruolo utente amministratore.

The screenshot displays the Cisco ISE Platform Settings interface. The main window shows the 'TACACS' configuration page under 'Platform Settings'. The 'Properties' section shows a 'Timeout' of 5 seconds. Below, the 'TACACS Providers' table lists one provider with Hostname '10.88.244.50' and Order '1'. An 'Add TACACS Provider' dialog box is open, showing fields for Hostname/FQDN, Order (set to 'lowest-available'), Key, Confirm Key, Port (set to '49'), and Timeout (set to '5' seconds). The dialog has 'OK' and 'Cancel' buttons.

Hostname	Order
10.88.244.50	1

Ruolo utente di sola lettura.



Nota: Il pulsante **ADD** è disattivato.

Verifica ISE 2.0

1. Passare a **Operazioni > TACACS LiveLog**. Dovrebbe essere possibile visualizzare i tentativi riusciti e quelli non riusciti.

Logged Time	Status	Details	Username	Type	Authentication Policy	Authorization Policy	Failure Reason	Matched Command	Shell Profile
Jan 17, 2018 08:57:23.272 PM	✓		frosadmin	Authorization	Tacacs_Default >> Default >> Default	Tacacs_Default >> FXOS Admin Rule			FXOS_Admin_Profile
Jan 17, 2018 08:57:22.852 PM	✓		frosadmin	Authentication	Tacacs_Default >> Default >> Default				
Jan 17, 2018 08:57:10.829 PM	✗		frosadmin	Authentication	Tacacs_Default >> Default >> Default		22040 Wrong password or invalid shared...		
Jan 17, 2018 08:57:01.069 PM	✓		frosro	Authorization	Tacacs_Default >> Default >> Default	Tacacs_Default >> FXOS Read Only ...			FXOS_ReadOnly_S...
Jan 17, 2018 08:57:00.825 PM	✓		frosro	Authentication	Tacacs_Default >> Default >> Default				
Jan 17, 2018 08:56:50.888 PM	✗		frosro	Authentication	Tacacs_Default >> Default >> Default		22040 Wrong password or invalid shared...		

Risoluzione dei problemi

Per eseguire il debug dell'autenticazione e dell'autorizzazione AAA, eseguire i seguenti comandi nella cli di FXOS.

```
fpr4120-TAC-A#connect fxos
```

```
fpr4120-TAC-A (fxos)# debug aaa-request
```

```
fpr4120-TAC-A (fxos)# evento debug aaa
```

```
fpr4120-TAC-A (fxos)# errori debug aaa
```

```
fpr4120-TAC-A (fxos)# termine mon
```

Dopo un tentativo di autenticazione riuscito, verrà visualizzato l'output seguente.

```
2018 Gen 17 15:46:40,305247 aaa: aaa_req_process per l'autenticazione. sessione n. 0
```

```
2018 Gen 17 15:46:40,305262 aaa: aaa_req_process: Richiesta generale AAA da parte dell'appn:  
login sottotipo_applicazione: predefinito
```

```
2018 Gen 17 15:46:40,305271 aaa: try_next_aaa_method
```

```
2018 Gen 17 15:46:40,305285 aaa: il numero totale di metodi configurati è 1, l'indice corrente da  
provare è 0
```

2018 gen 17 15:46:40,305294 aaa: handle_req_using_method

2018 Gen 17 15:46:40,305301 aaa: AAA_METHOD_SERVER_GROUP

2018 Gen 17 15:46:40,305308 aaa: gruppo aaa_sg_method_handler = tacacs

2018 Gen 17 15:46:40,305315 aaa: Utilizzo di sg_protocol passato a questa funzione

2018 Gen 17 15:46:40,305324 aaa: Invio della richiesta al servizio TACACS

2018 Gen 17 15:46:40,305384 aaa: Gruppo di metodi configurato completato

2018 Gen 17 15:46:40,554631 aaa: aaa_process_fd_set

2018 Gen 17 15:46:40,555229 aaa: aaa_process_fd_set: mtscallback su aaa_q

2018 Gen 17 15:46:40,55817 aaa: mts_message_response_handler: risposta mts

2018 Gen 17 15:46:40,556387 aaa: gestore_risposta_daemon

2018 gen 17 15:46:40,557042 aaa: sessione: 0x8dfd68c rimosso dalla tabella delle sessioni 0

2018 Gen 17 15:46:40,557059 aaa: is_aaa_resp_status_success status = 1

2018 Gen 17 15:46:40,557066 aaa: is_aaa_resp_status_success è TRUE

2018 gen 17 15:46:40,557075 aaa: aaa_send_client_response per l'autenticazione. session->flags=21. aaa_resp->flags=0.

2018 gen 17 15:46:40,557083 aaa: AAA_REQ_FLAG_NORMAL

2018 Gen 17 15:46:40,557106 aaa: mts_send_response riuscito

2018 Gen 17 15:46:40,557364 aaa: aaa_req_process per l'autorizzazione. sessione n. 0

2018 Gen 17 15:46:40,557378 aaa: aaa_req_process richiamato con contesto da appln: login sottotipo_applicazione: auto_type:2, auto_method: 0

2018 Gen 17 15:46:40,557386 aaa: aaa_send_req_using_context

2018 gen 17 15:46:40,557394 aaa: gruppo aaa_sg_method_handler = (null)

2018 Gen 17 15:46:40,557401 aaa: Utilizzo di sg_protocol passato a questa funzione

2018 Gen 17 15:46:40,557408 aaa: richiesta AAA basata sul contesto o diretta(eccezione: non è una richiesta di inoltrò). Non riceve copia della richiesta aaa

2018 Gen 17 15:46:40,557415 aaa: Invio della richiesta al servizio TACACS

2018 gen 17 15:46:40,801732 aaa: aaa_send_client_response per l'autorizzazione. session->flags=9. aaa_resp->flags=0.

2018 Gen 17 15:46:40,801740 aaa: AAA_REQ_FLAG_NORMAL

2018 Gen 17 15:46:40,801761 aaa: mts_send_response riuscito

2018 gen 17 15:46:40,848932 aaa: CODICE OPERATIVO PRECEDENTE:
accounting_interim_update

2018 gen 17 15:46:40,848943 aaa: aaa_create_local_acct_req: user=, session_id=, log=aggiunto
user:fxosadmin al ruolo:admin

2018 gen 17 15:46:40,848963 aaa: aaa_req_process per l'accounting. sessione n. 0

2018 gen 17 15:46:40,848972 aaa: Il riferimento alla richiesta MTS è NULL. richiesta LOCALE

2018 gen 17 15:46:40,848982 aaa: Impostazione di AAA_REQ_RESPONSE_NOT_NEEDED

2018 gen 17 15:46:40,848992 aaa: aaa_req_process: Richiesta generale AAA da parte dell'appn:
default appln_subtype: predefinito

2018 gen 17 15:46:40,849002 aaa: try_next_aaa_method

2018 gen 17 15:46:40,849022 aaa: nessun metodo configurato per l'impostazione predefinita

2018 gen 17 15:46:40,849032 aaa: nessuna configurazione disponibile per questa richiesta

2018 gen 17 15:46:40,849043 aaa: try_fallback_method

2018 gen 17 15:46:40,849053 aaa: handle_req_using_method

2018 gen 17 15:46:40,849063 aaa: gestore_metodo_locale

2018 gen 17 15:46:40,849073 aaa: aaa_local_accounting_msg

2018 gen 17 15:46:40,849085 aaa: update::added user:fxosadmin to the role:admin

Dopo un tentativo di autenticazione non riuscito, verrà visualizzato l'output seguente.

2018 gen 17 15:46:17,836271 aaa: aaa_req_process per l'autenticazione. sessione n. 0

2018 gen 17 15:46:17,836616 aaa: aaa_req_process: Richiesta generale AAA da parte dell'appn:
login sottotipo_applicazione: predefinito

2018 gen 17 15:46:17,837063 aaa: try_next_aaa_method

2018 gen 17 15:46:17,837416 aaa: il numero totale di metodi configurati è 1, l'indice corrente da
provare è 0

2018 gen 17 15:46:17,837766 aaa: handle_req_using_method

2018 gen 17 15:46:17,838103 aaa: AAA_METHOD_SERVER_GROUP

2018 gen 17 15:46:17,838477 aaa: gruppo aaa_sg_method_handler = tacacs

2018 gen 17 15:46:17,838826 aaa: Utilizzo di sg_protocol passato a questa funzione

2018 gen 17 15:46:17,839167 aaa: Invio della richiesta al servizio TACACS

2018 gen 17 15:46:17,840225 aaa: Gruppo di metodi configurato completato

2018 Gen 17 15:46:18,043710 aaa: is_aaa_resp_status_success status = 2

2018 Gen 17 15:46:18,044048 aaa: is_aaa_resp_status_success è TRUE

2018 Gen 17 15:46:18,044395 aaa: aaa_send_client_response per l'autenticazione. session->flags=21. aaa_resp->flags=0.

2018 Gen 17 15:46:18,044733 aaa: AAA_REQ_FLAG_NORMAL

2018 Gen 17 15:46:18,045096 aaa: mts_send_response riuscito

2018 Gen 17 15:46:18,045677 aaa: sessione_pulizia_aaa

2018 Gen 17 15:46:18,045689 aaa: mts_drop del messaggio di richiesta

2018 Gen 17 15:46:18,045699 aaa: aaa_req deve essere liberato.

2018 Gen 17 15:46:18,045715 aaa: aaa_process_fd_set

2018 Gen 17 15:46:18,045722 aaa: aaa_process_fd_set: mtscallback su aaa_q

2018 Gen 17 15:46:18,045732 aaa: aaa_enable_info_config: GET_REQ per il messaggio di errore di accesso aaa

2018 Gen 17 15:46:18,045738 aaa: è stato restituito il valore restituito dell'operazione di configurazione:elemento di sicurezza sconosciuto

Informazioni correlate

Il comando Ethalyzer sulla cli di FX-OS richiederà una password quando l'autenticazione TACACS/RADIUS è abilitata. Questo comportamento è causato da un bug.

ID bug: [CSCvg87518](#)