Firepower eXtensible Operating System (FXOS) 2.2: Autenticazione/autorizzazione dello chassis per la gestione remota con ISE tramite TACACS+

Sommario

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 Remirez, 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

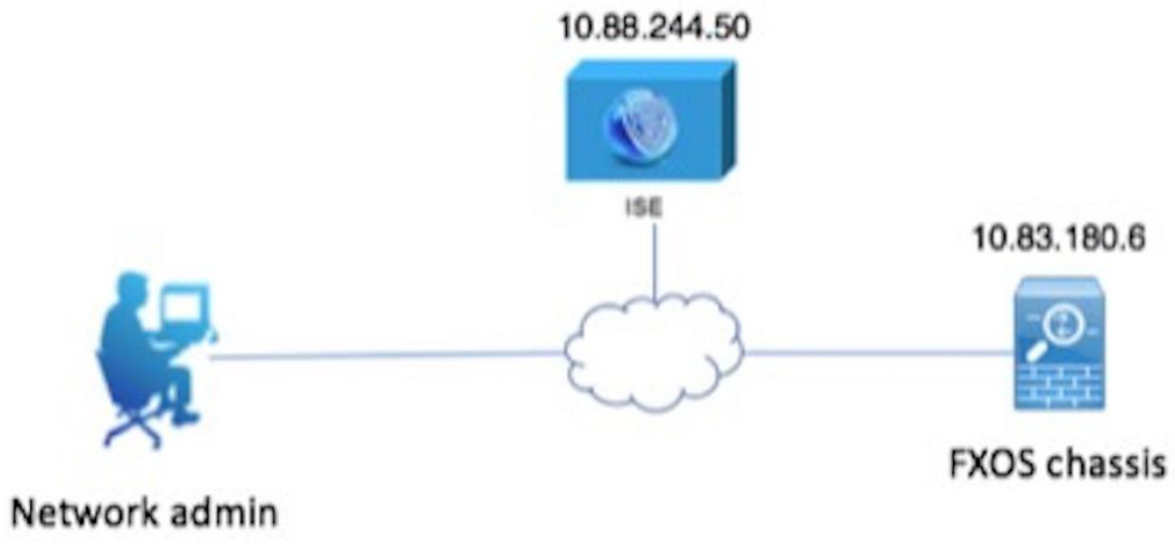
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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



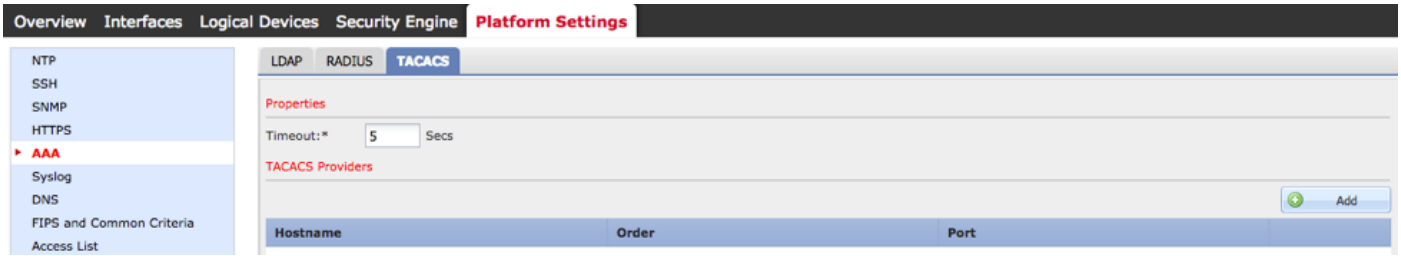
Configurazioni

Configurazione dello chassis FXOS

Creazione di un provider TACACS+

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

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

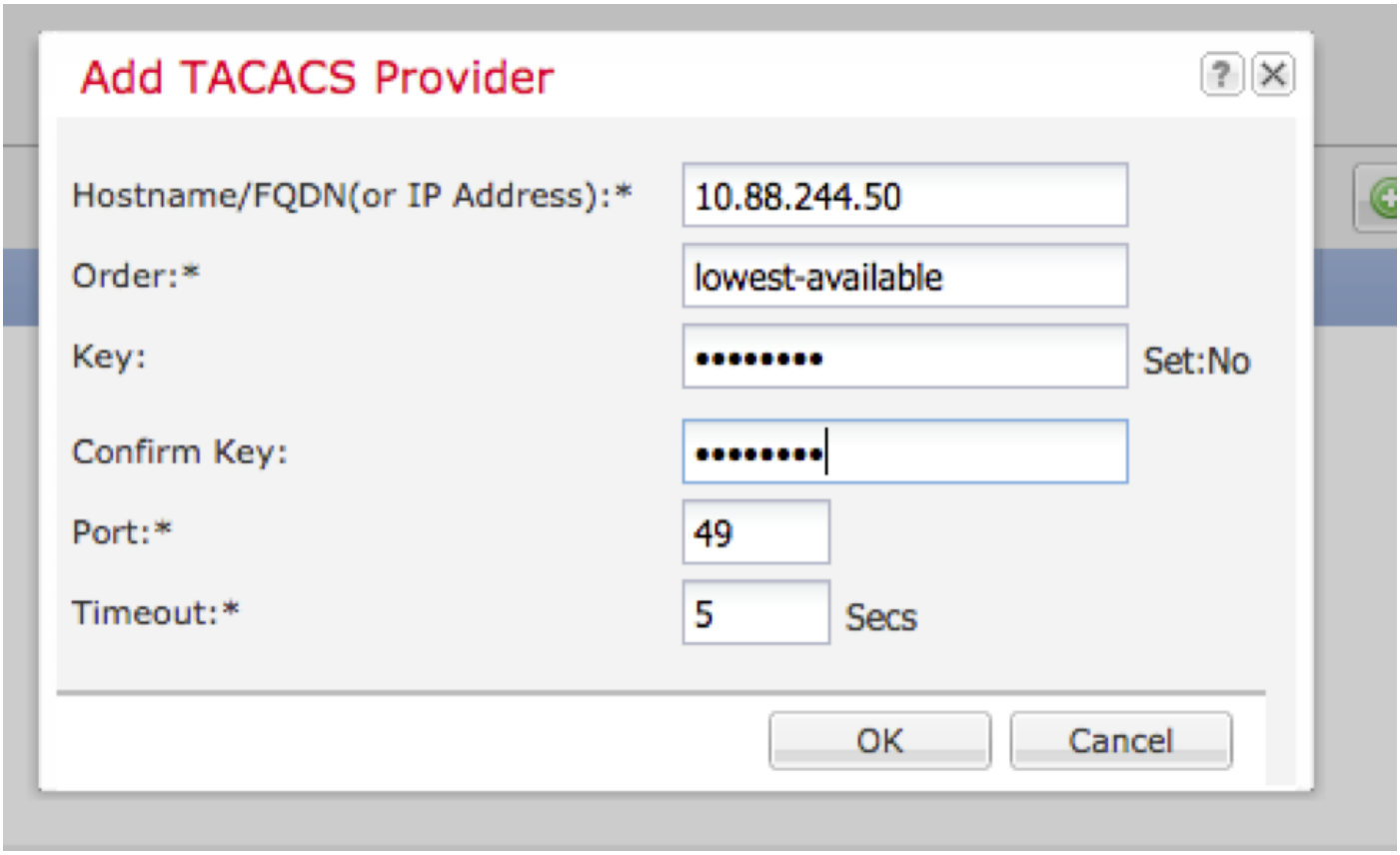


Passaggio 3. Per ogni provider TACACS+ che si desidera aggiungere (fino a 16 provider).

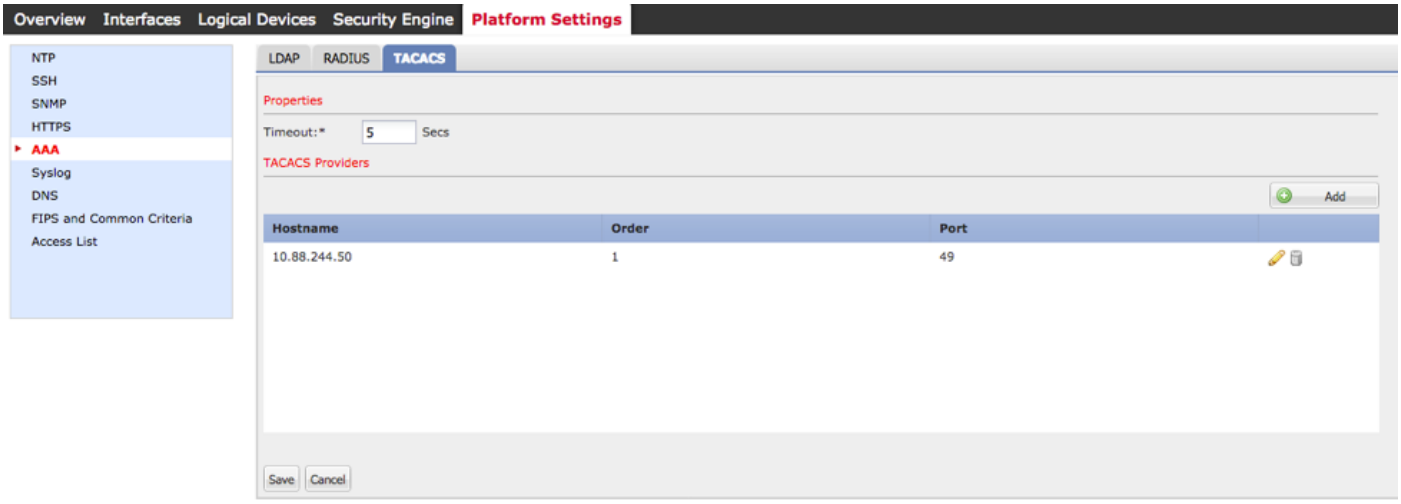
3.1. Nell'area dei provider TACACS, fare clic su **Add.**

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.

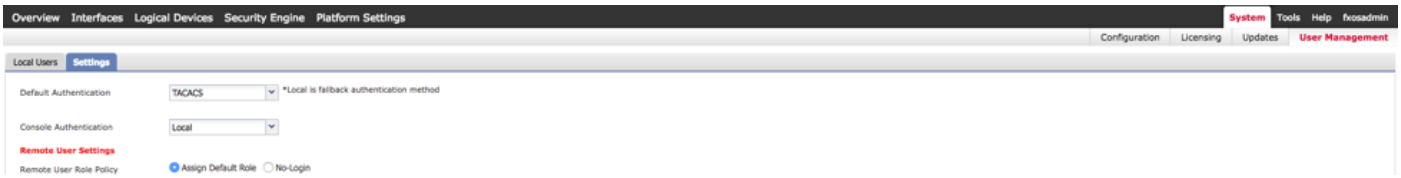


Passaggio 4. Fare clic su **Salva**.



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: ****

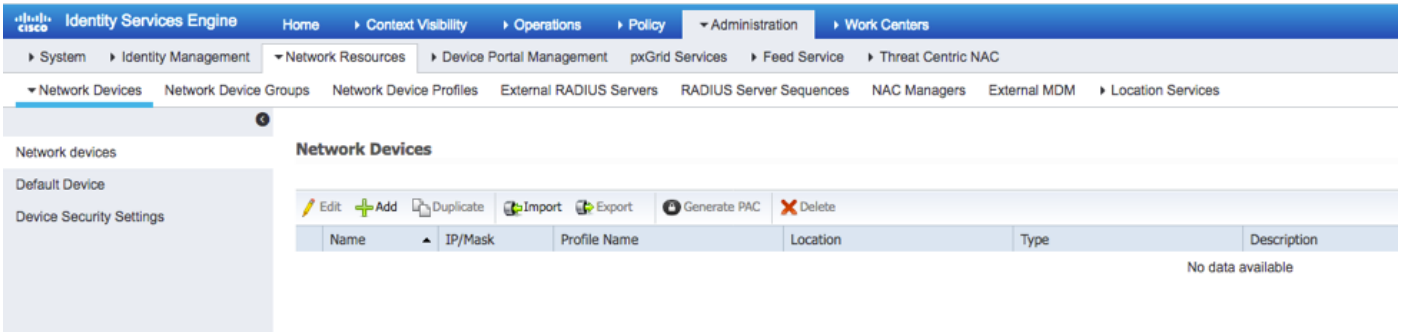
Timeout: 5

Configurazione del server ISE

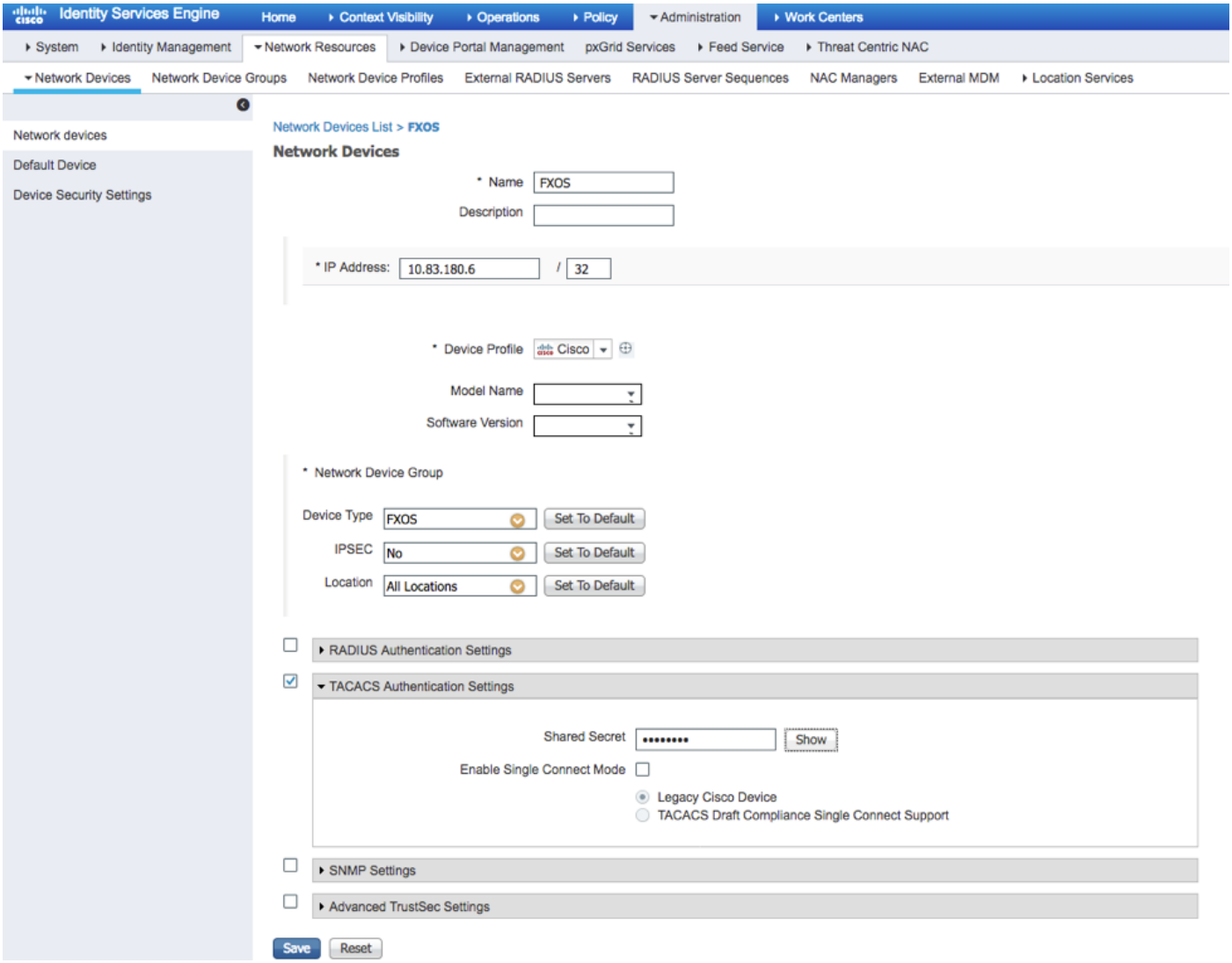
Aggiunta di FXOS come risorsa di rete

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

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



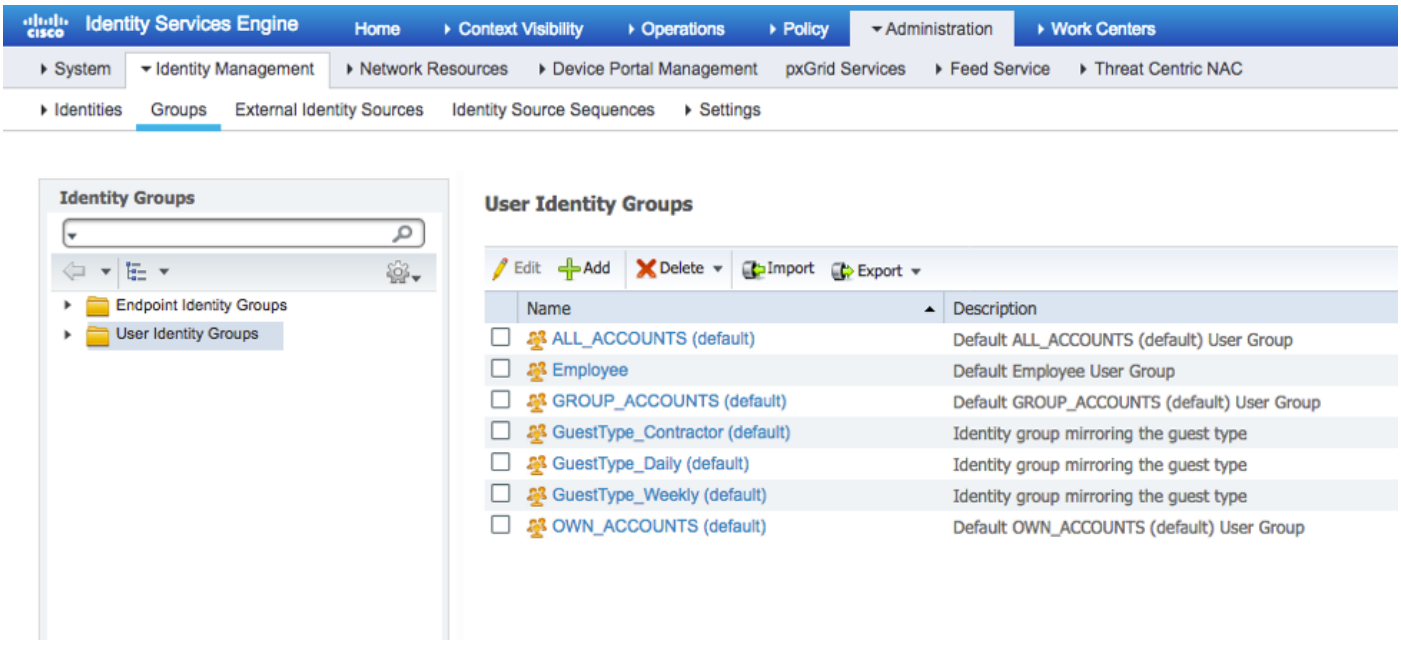
Passaggio 3. Immettere i valori richiesti (Nome, Indirizzo IP, Tipo di dispositivo, Abilita TACACS+ e aggiungere la CHIAVE), quindi fare clic su **Submit (Invia).**



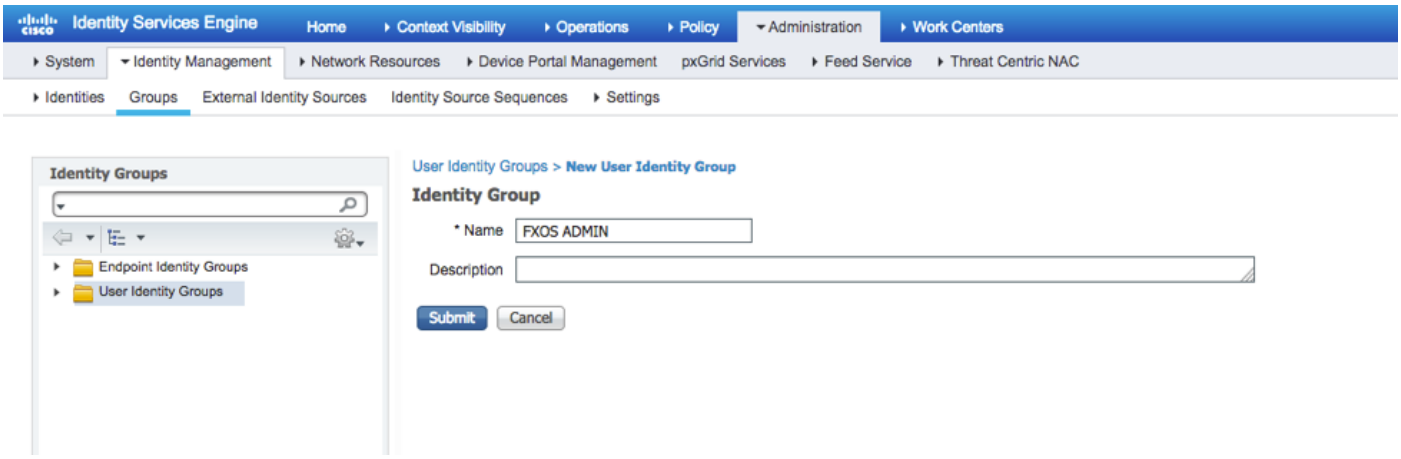
Creazione di gruppi di identità e utenti

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

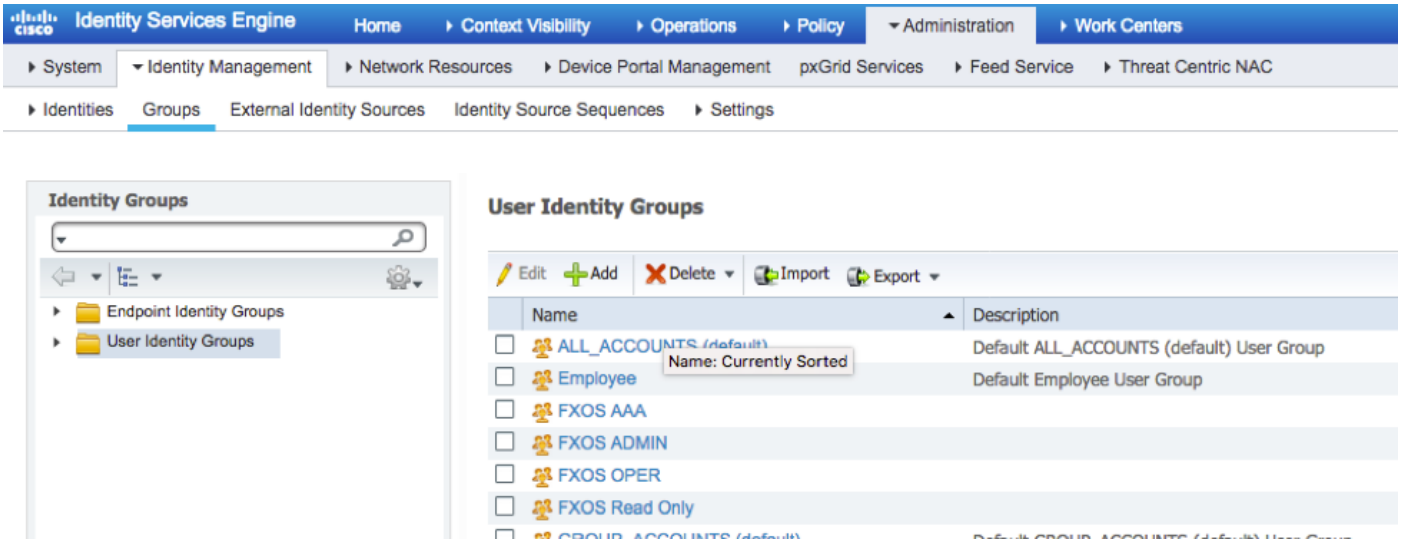
Passaggio 2. Fare clic su **ADD.**



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

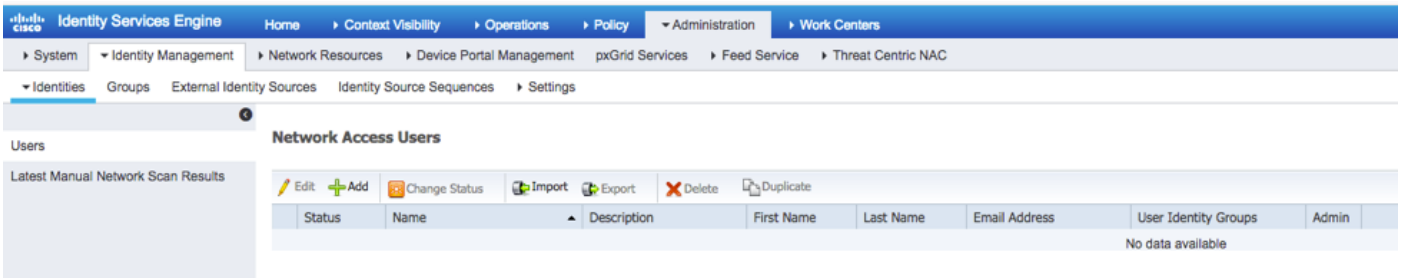


Passaggio 4. Ripetere il passaggio 3 per tutti i ruoli utente richiesti.

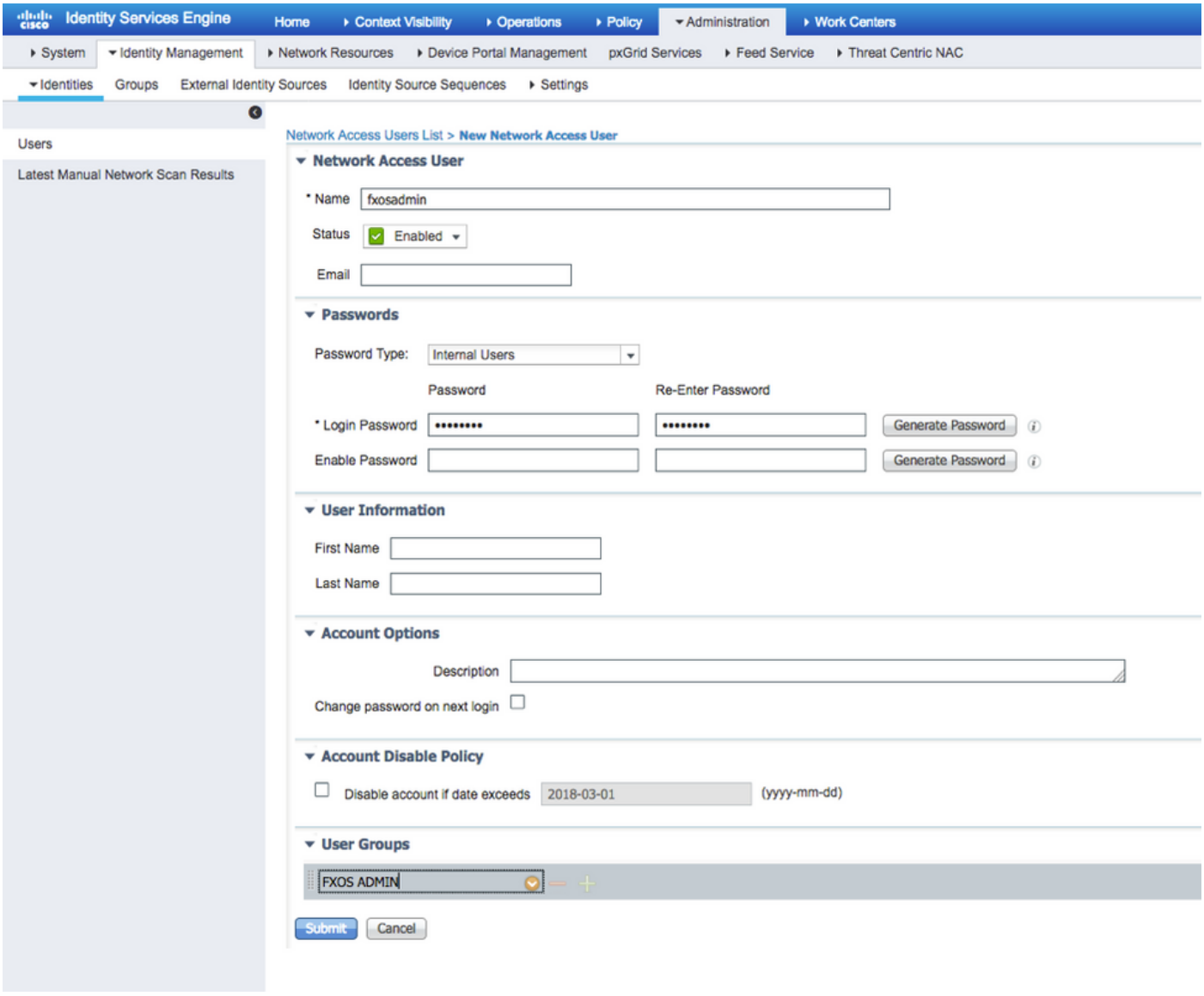


Passaggio 5. Passare a **Amministrazione > Gestione delle identità > Identità > Utenti.**

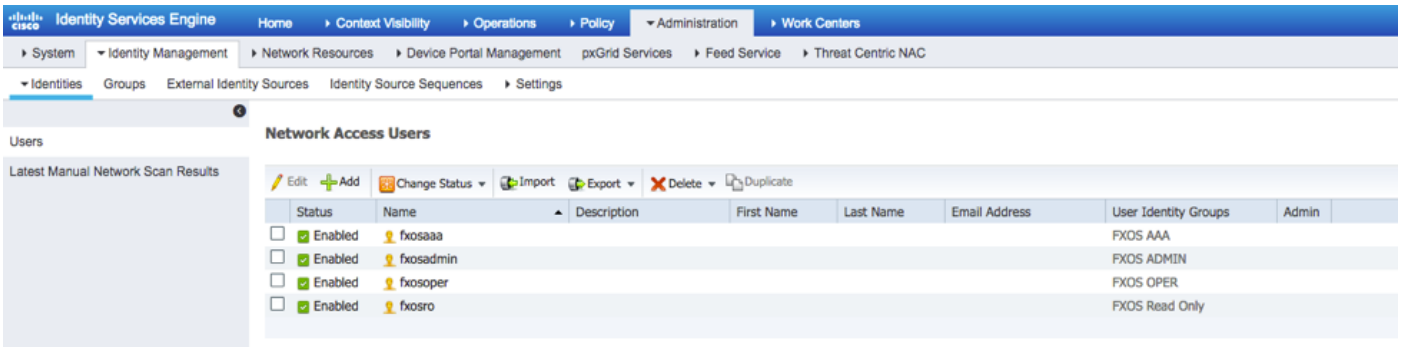
Passaggio 6. Fare clic su **ADD.**



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

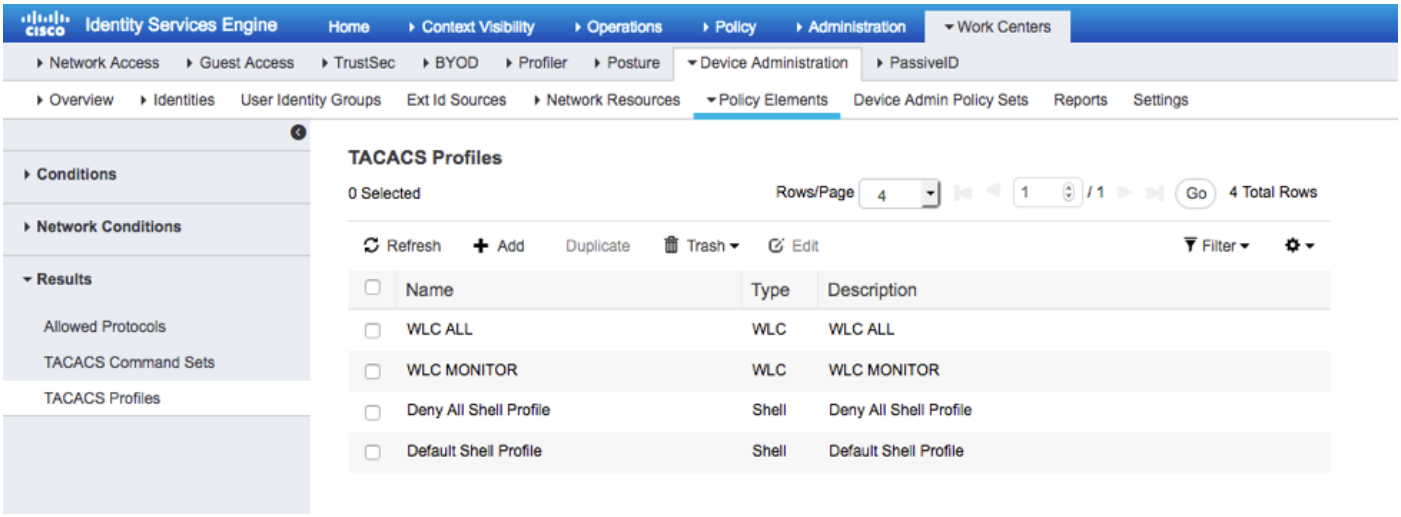


Passaggio 8. Ripetere il passaggio 6 per tutti gli utenti richiesti.



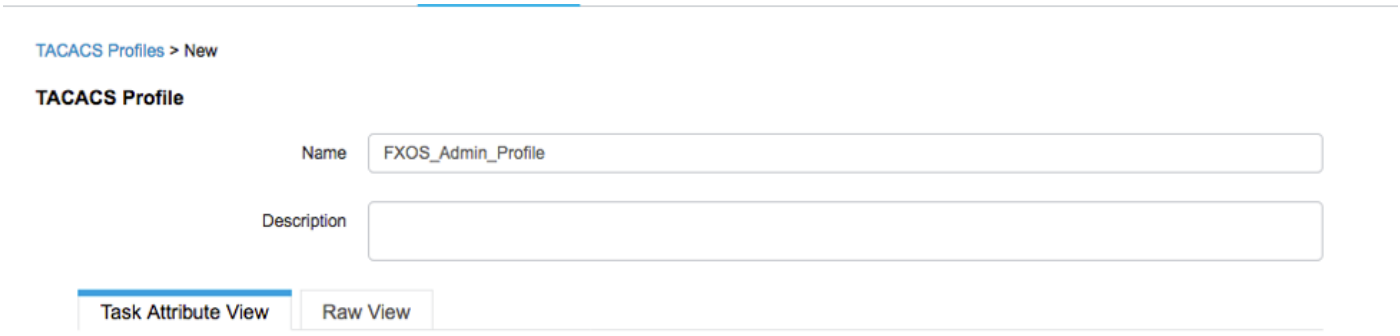
Creazione del profilo di shell per ogni ruolo utente

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



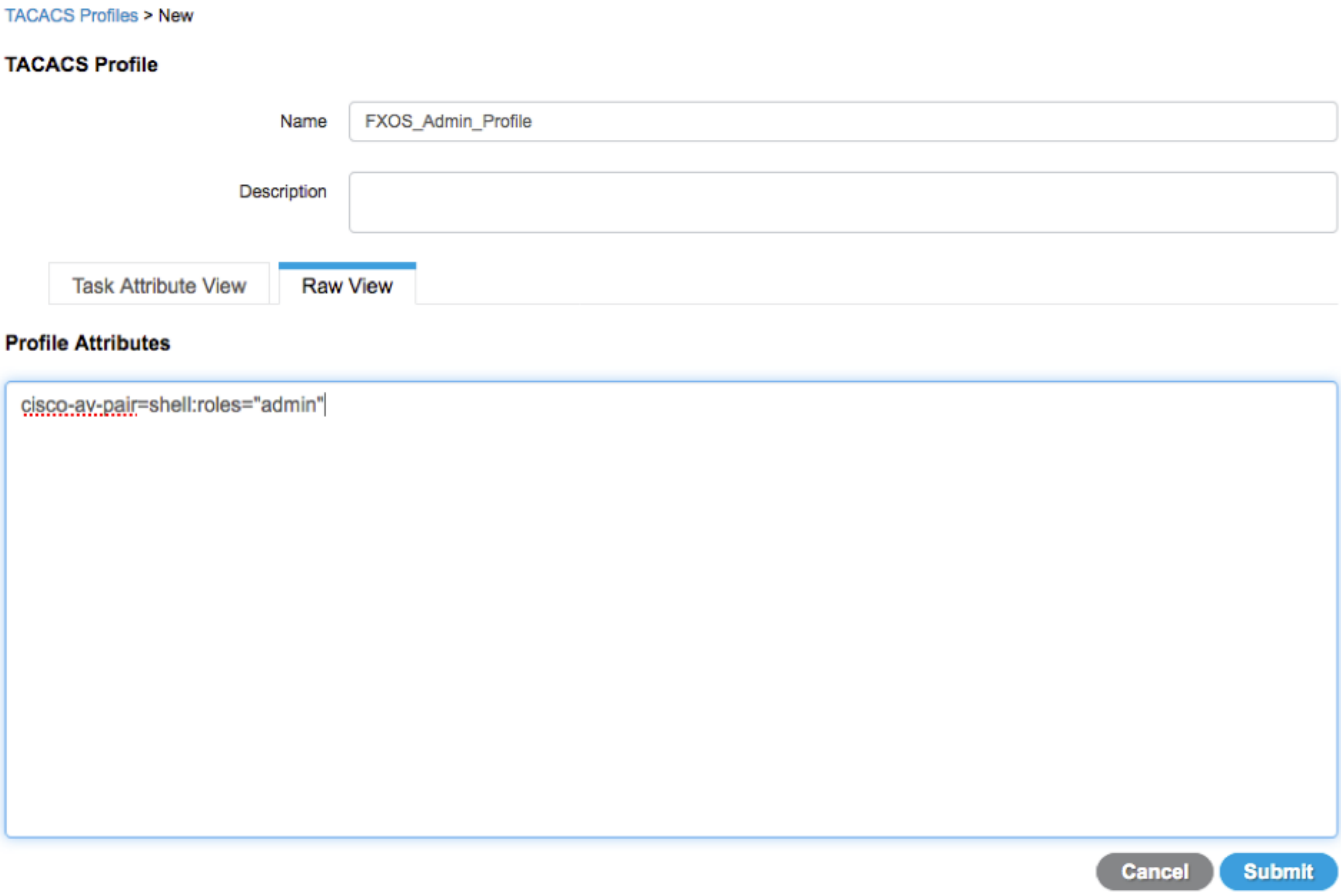
Passaggio 2. Inserire i valori richiesti per il profilo TACACS

2.1. Inserire il nome.

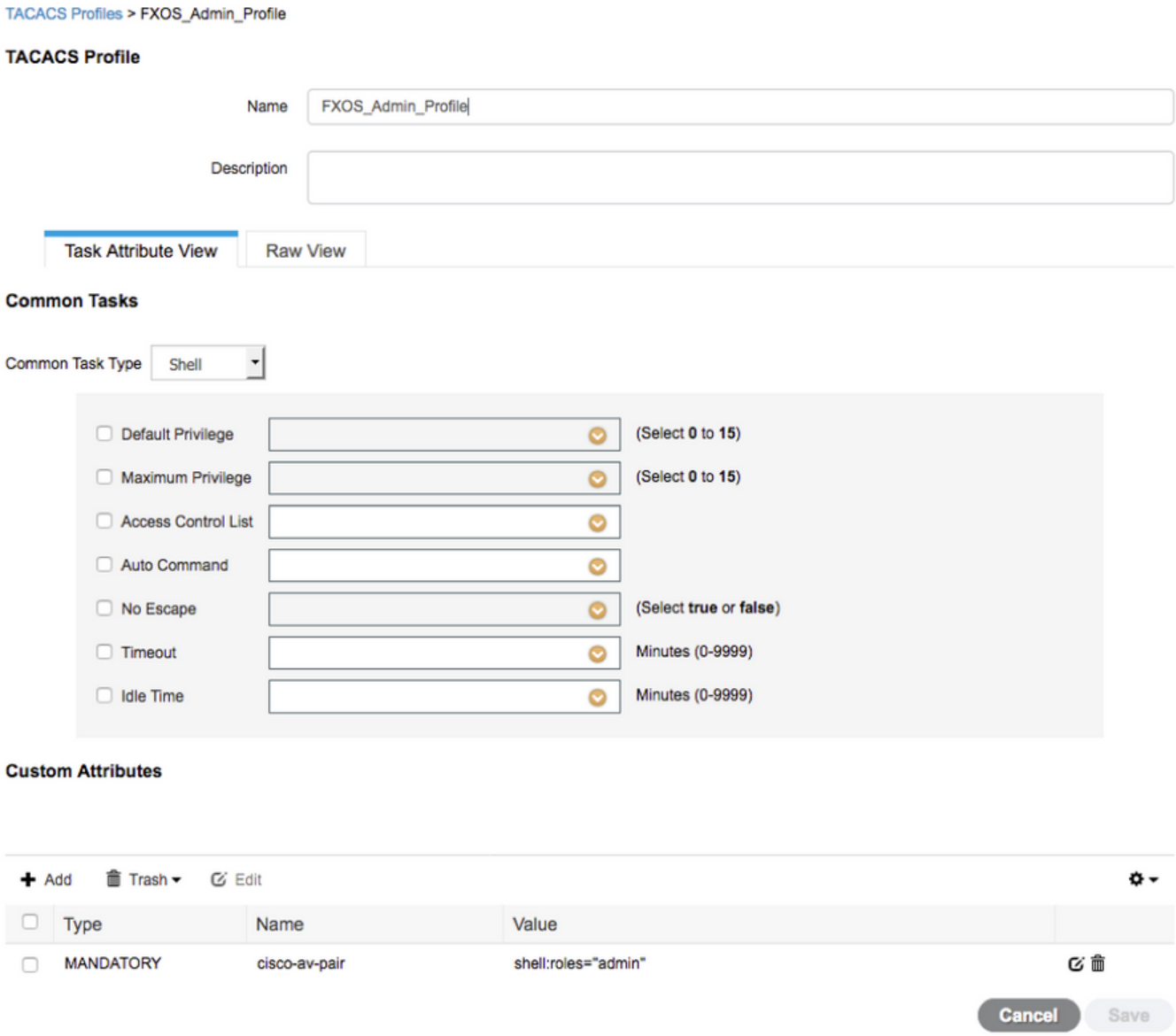


2.2. Nella SCHEDA **Visualizzazione RAW** configurare la seguente coppia CISCO-AV.

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



2.3. Fare clic su **Invia**.

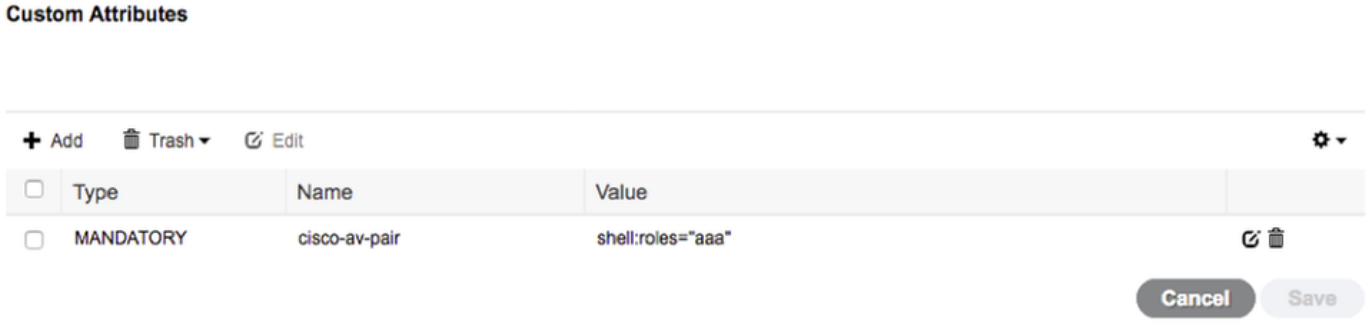


Passaggio 3. Ripetere il passaggio 2 per gli altri ruoli utente utilizzando le seguenti coppie Cisco-AV.

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
MANDATORY	cisco-av-pair	shell:roles="operations"

Custom Attributes

+ Add | Trash | Edit

Type	Name	Value
MANDATORY	cisco-av-pair	shell:roles="read-only"

TACACS Profiles

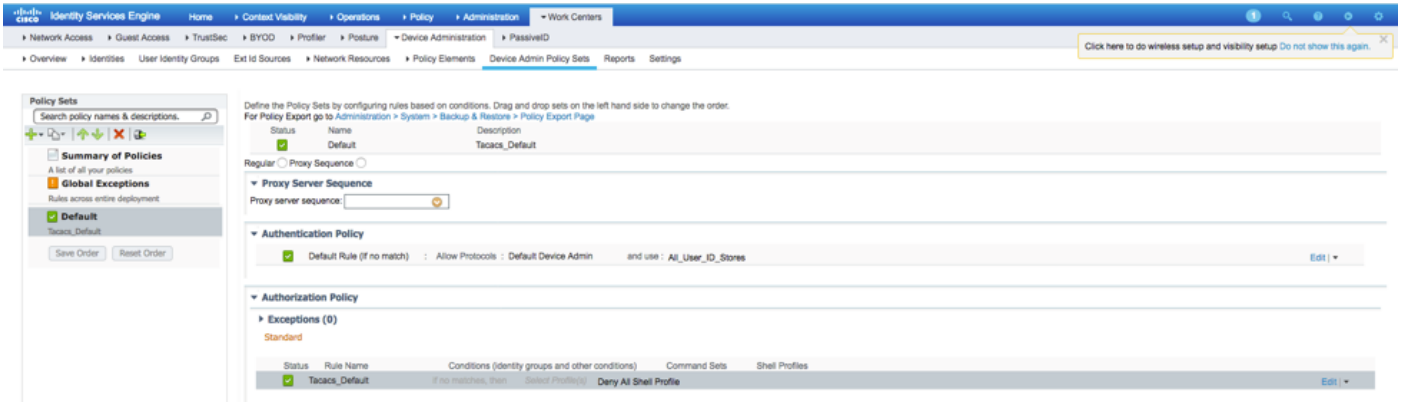
0 Selected | Rows/Page 8 | 1 / 1 | Go | 8 Total Rows

Refresh | + Add | Duplicate | Trash | Edit | Filter

Name	Type	Description
WLC ALL	WLC	WLC ALL
WLC MONITOR	WLC	WLC MONITOR
Deny All Shell Profile	Shell	Deny All Shell Profile
Default Shell Profile	Shell	Default Shell Profile
FXOS_Admin_Profile	Shell	
FXOS_AAA_Shell	Shell	
FXOS_Operations_Shell	Shell	
FXOS_ReadOnly_Shell	Shell	

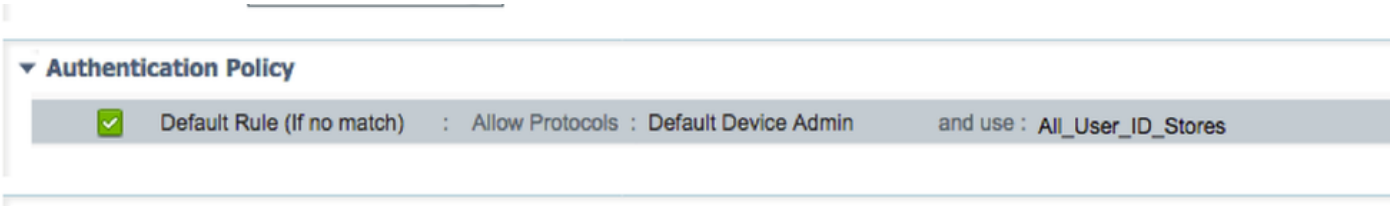
Creazione del criterio di autorizzazione TACACS

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



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

all'archivio identità richiesto.



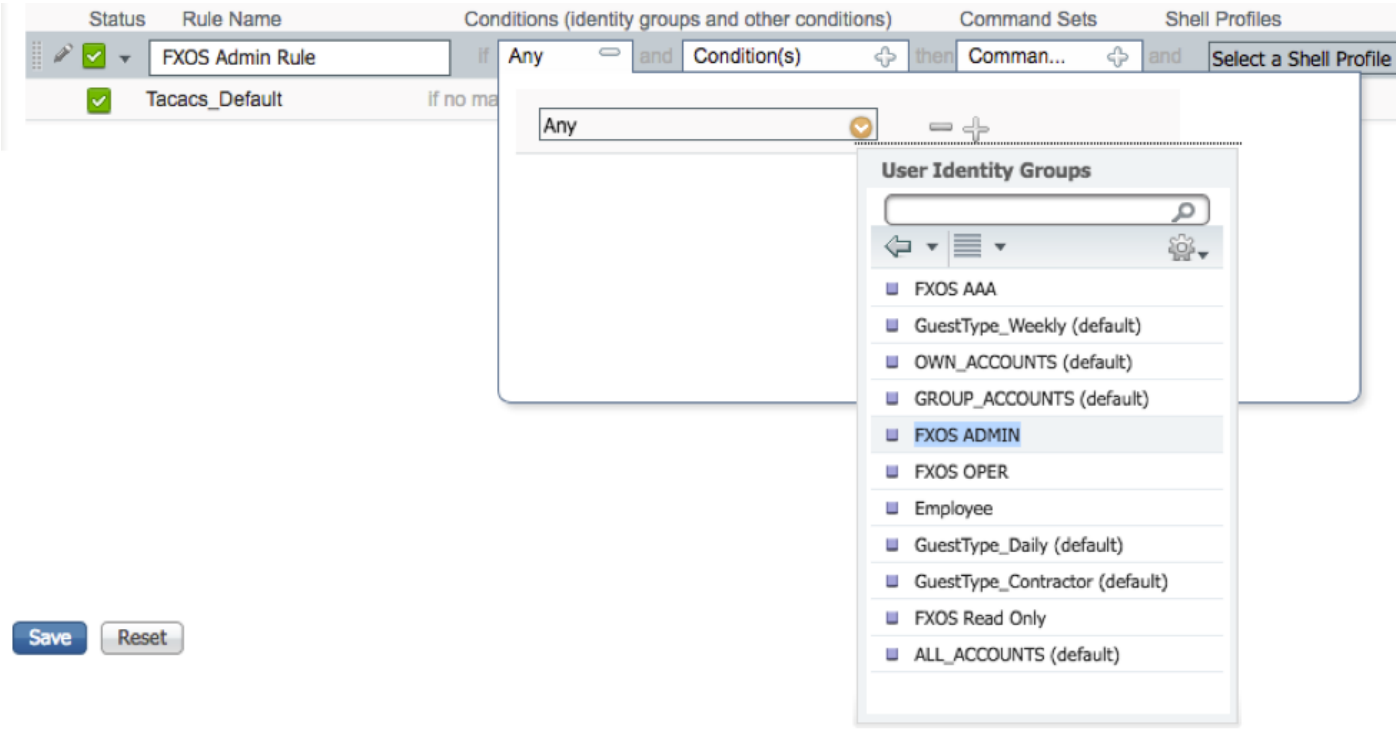
Passaggio 3. Fare clic sulla freccia alla fine del criterio di autorizzazione predefinito e fare clic su Inserisci regola.

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

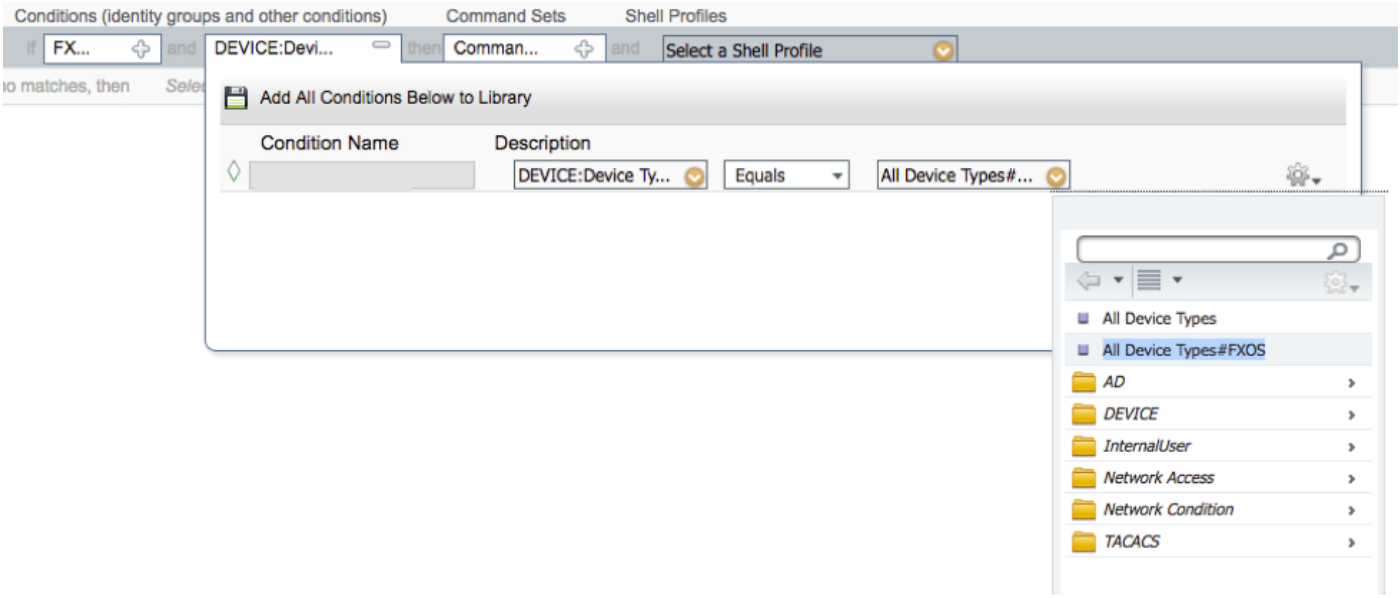
4.1. Nome della regola: Regola di amministrazione FXOS.

4.2. Condizioni.

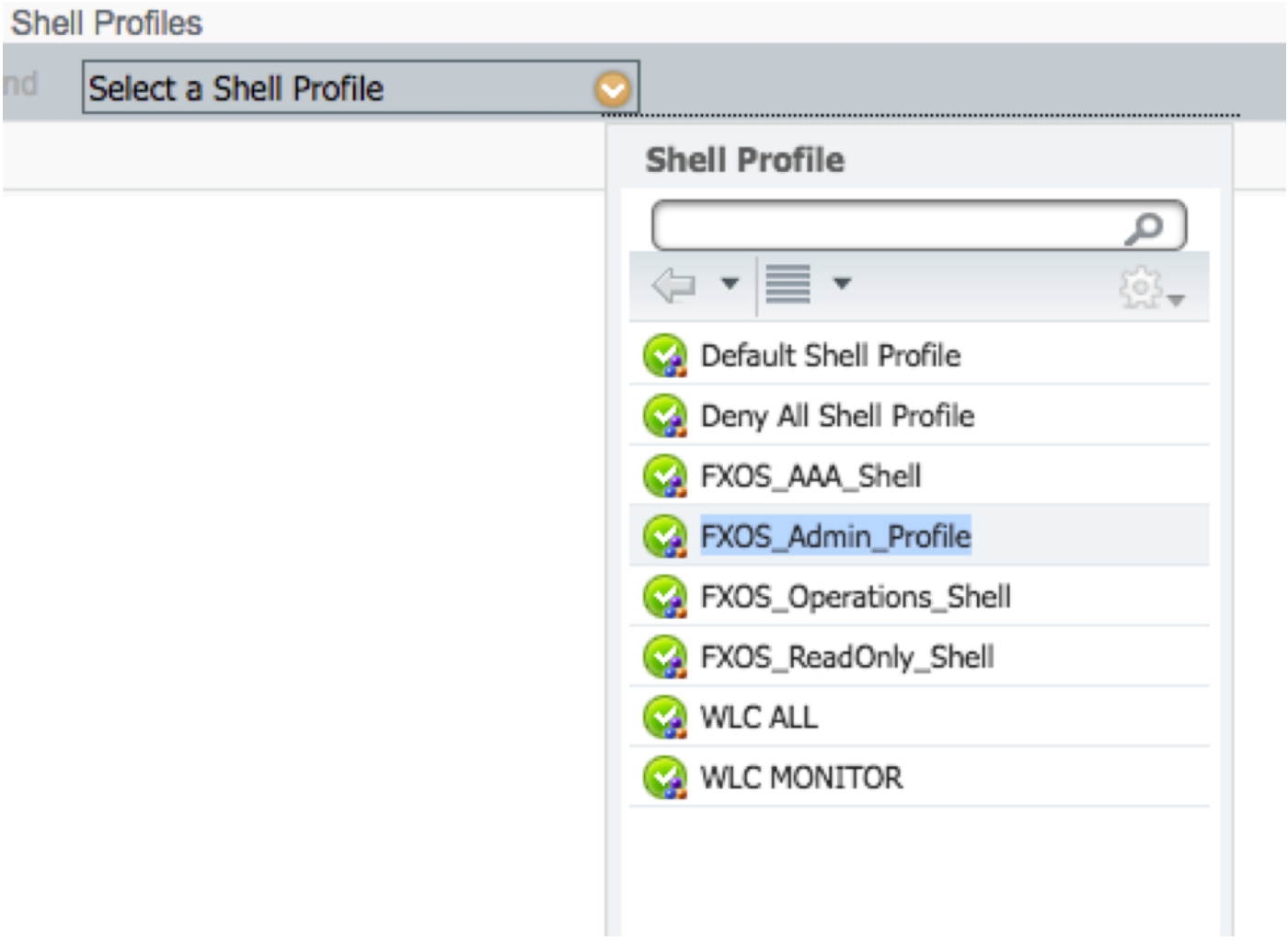
Se: Il gruppo di identità utente è FXOS ADMIN



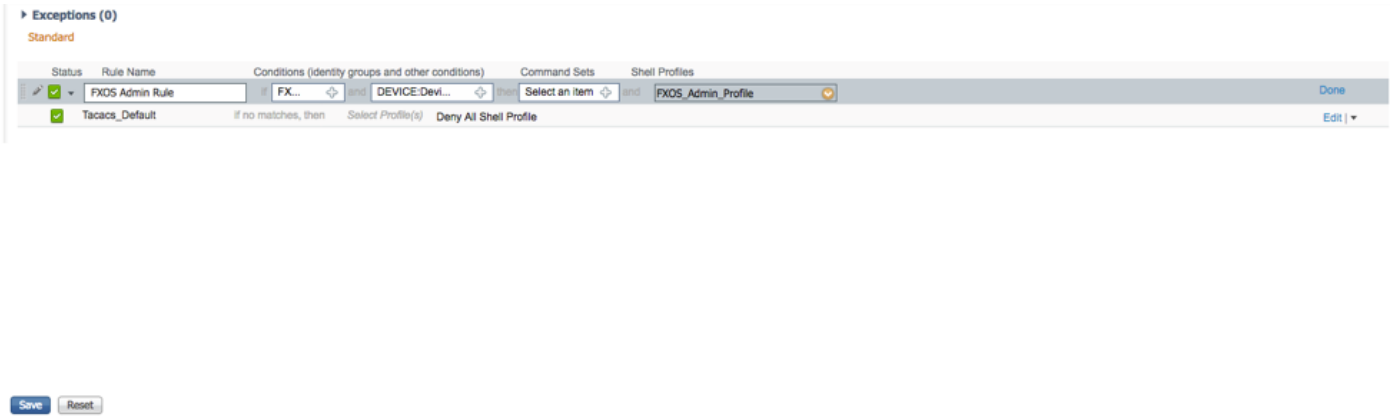
E Dispositivo: Tipo di dispositivo è uguale a Tutti i tipi di dispositivo #FXOS



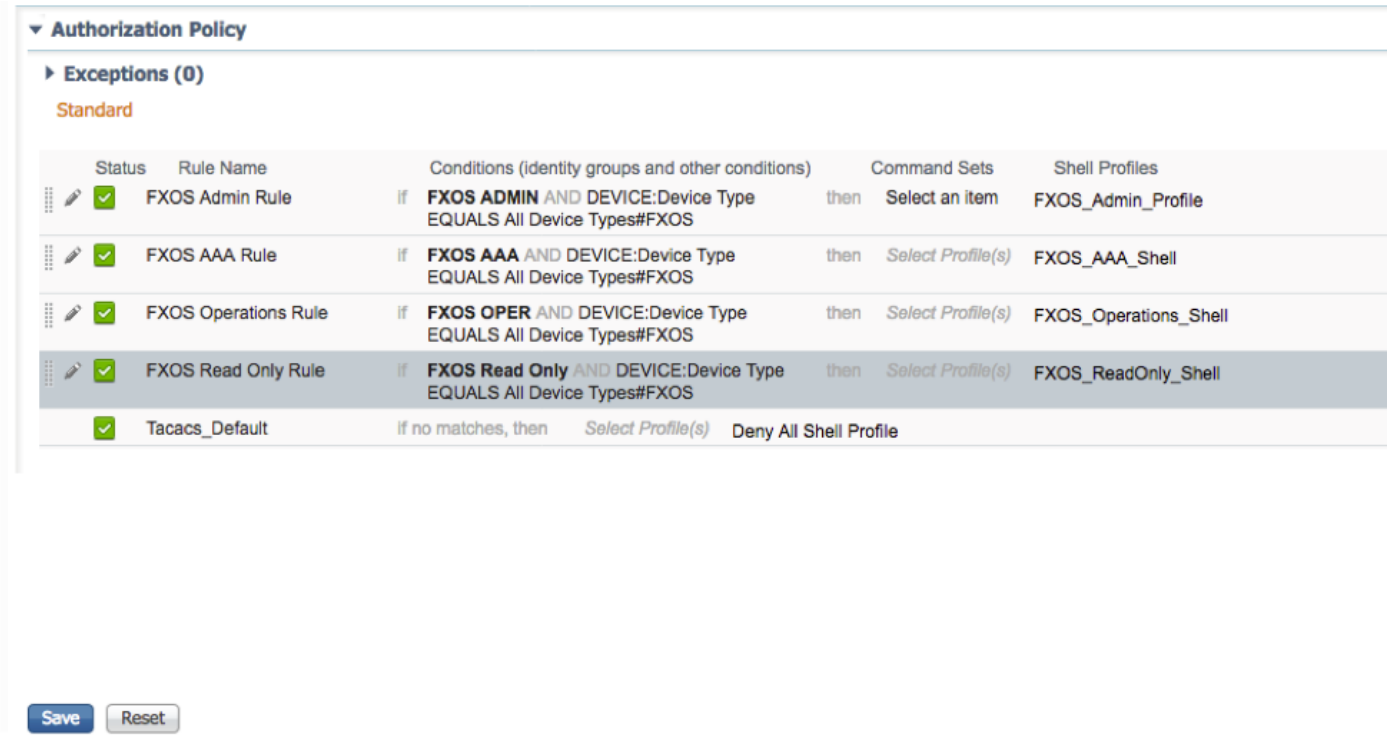
Profilo shell: Profilo_amministrazione_FXOS



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

Èora 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: fxosadmin

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

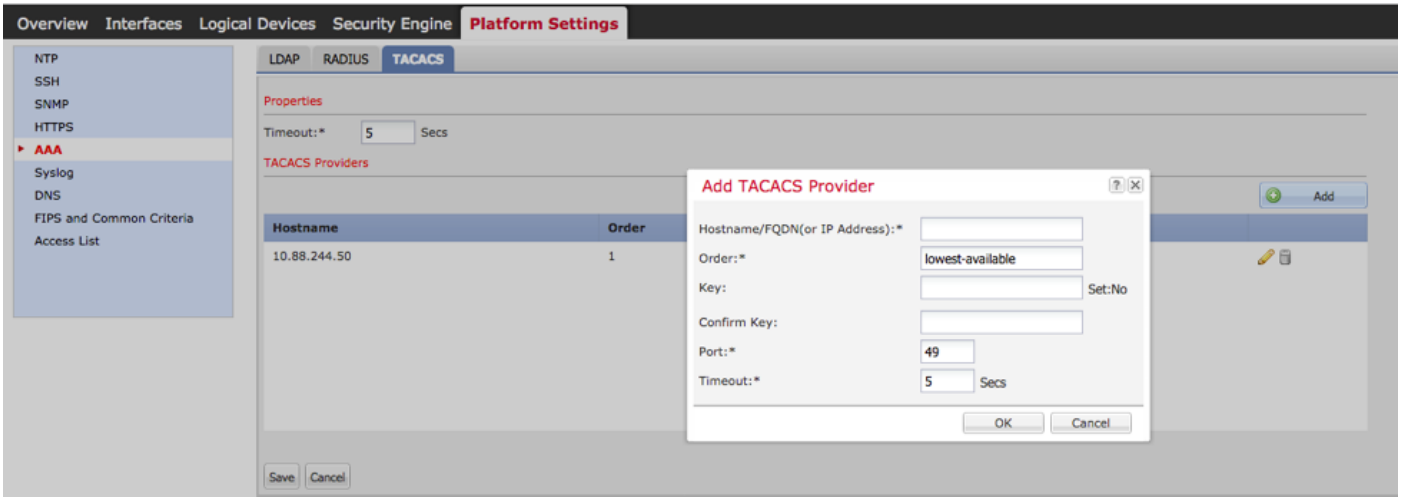
fpr4120-TAC-A#**connect fxos**

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

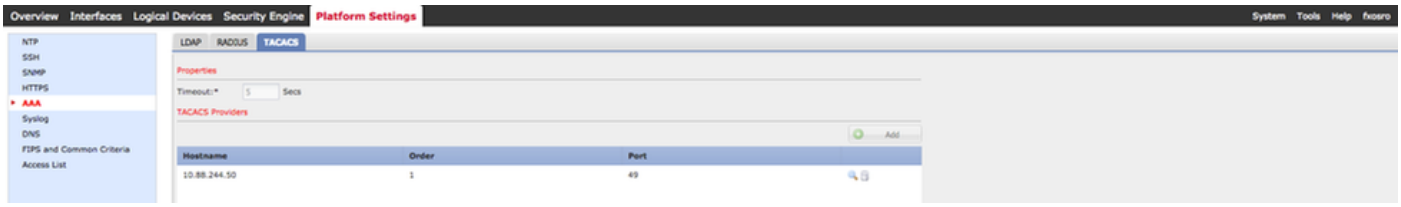
% Autorizzazione negata per il ruolo

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

Ruolo utente amministratore.



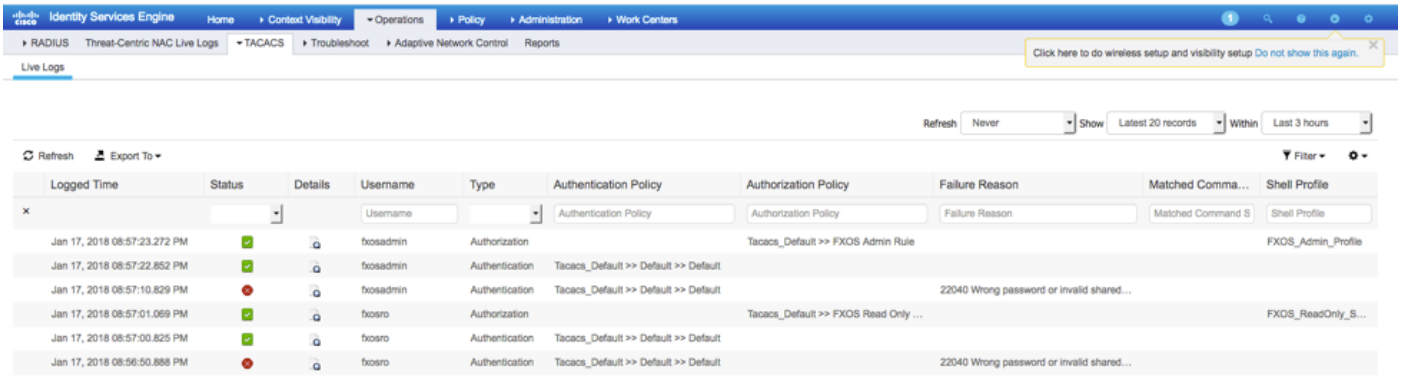
Ruolo utente di sola lettura.



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.



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 inoltro). 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 Ethanalyzer 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