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

Sommario

Introduzione

In questo documento viene descritto come configurare l'autenticazione e l'autorizzazione RADIUS 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

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

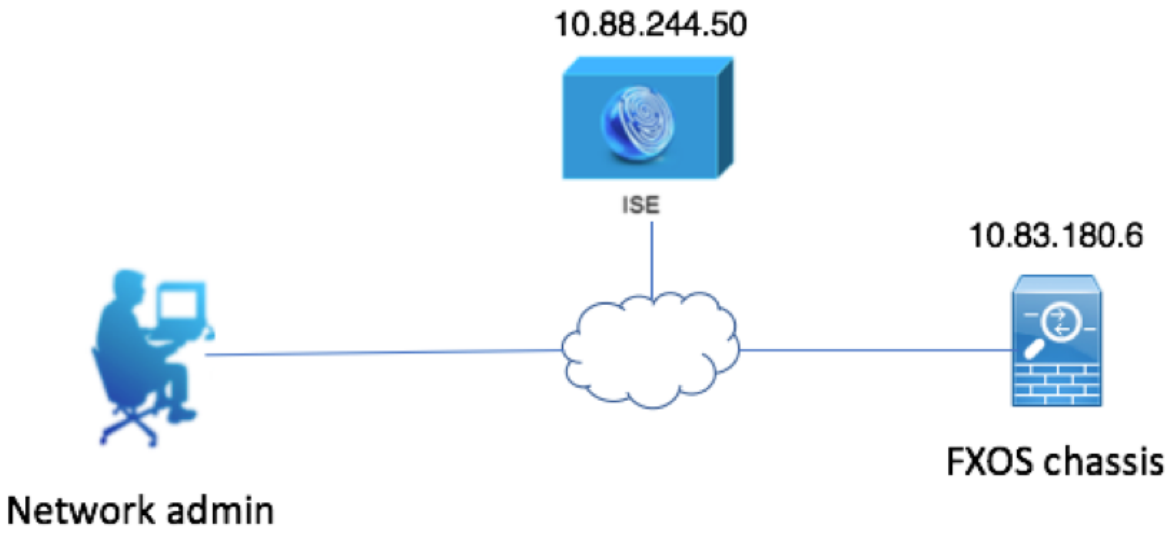
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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



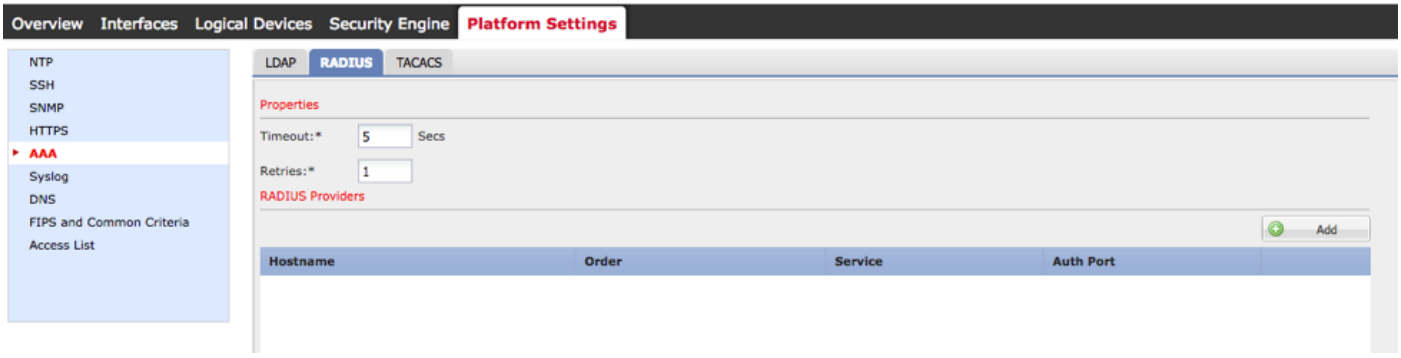
Configurazioni

Configurazione dello chassis FXOS

Creazione di un provider RADIUS mediante Chassis Manager

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

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

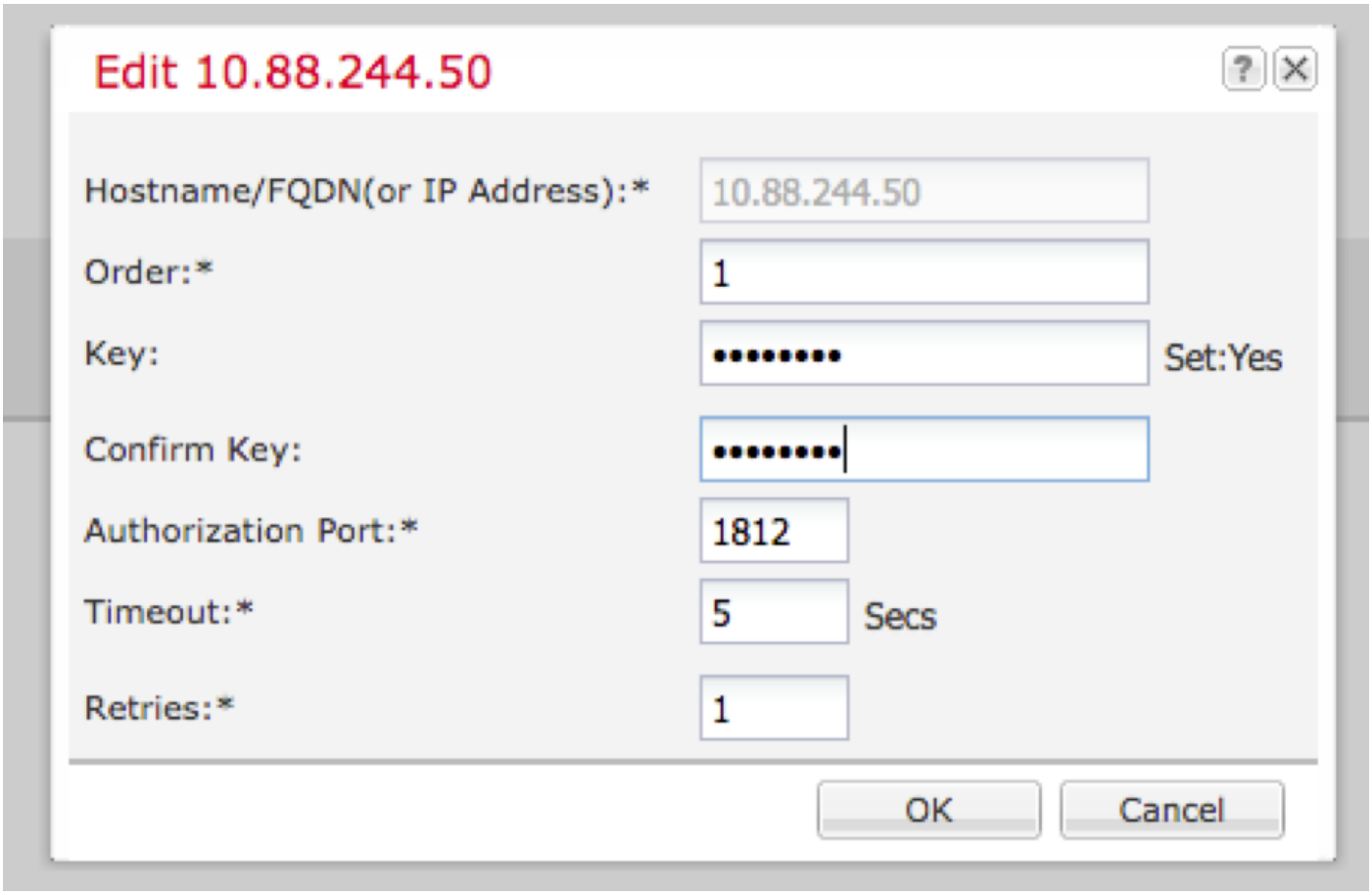


Passaggio 3. Per ogni provider RADIUS che si desidera aggiungere (fino a 16 provider).

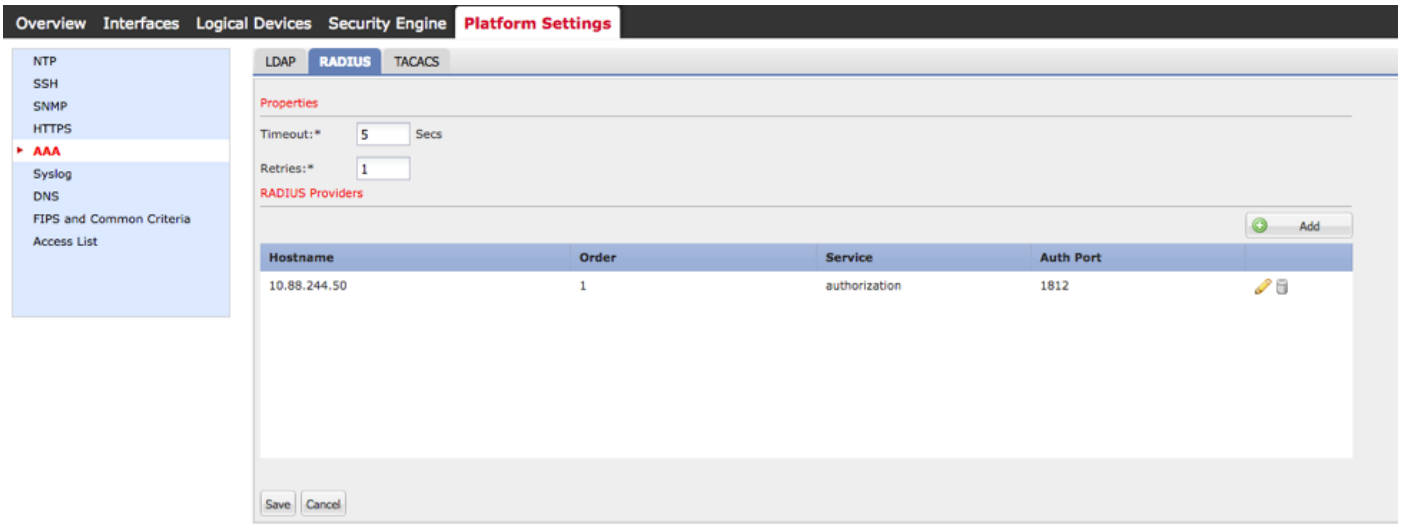
3.1. Nell'area Provider RADIUS, fare clic su **Aggiungi.**

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

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

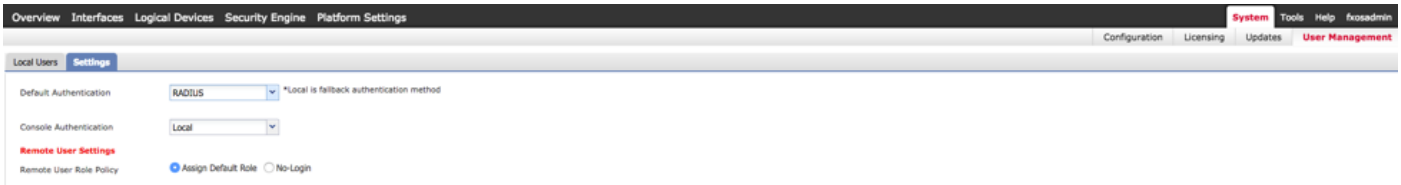


Passaggio 4. Fare clic su **Salva**.



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

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



Creazione di un provider RADIUS tramite CLI

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

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

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

fpr4120-TAC-A /security/default-auth # **set realm radius**

Passaggio 2. Utilizzare il comando **show detail** per visualizzare i risultati.

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

Autenticazione predefinita:

Area di autenticazione amministrativa: **Raggio**

Area operativa: **Raggio**

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 RADIUS, eseguire i comandi seguenti.

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

fpr4120-TAC-A /security # **raggio ambito**

fpr4120-TAC-A /security/radius # **invio al server 10.88.244.50**

fpr4120-TAC-A /security/radius/server # **set descr "ISE Server"**

fpr4120-TAC-A /security/radius/server* # **set key**

Immettere la chiave: *****

Confermare la chiave: *****

Passaggio 4. Per visualizzare i risultati, utilizzare il comando **show detail**.

fpr4120-TAC-A /security/radius/server* # **show detail**

Server RADIUS:

Nome host, FQDN o indirizzo IP: 10.88.244.50

Descr.:

Ordine: 1

Auth Port (Porta autenticazione): 1812

Chiave: ****

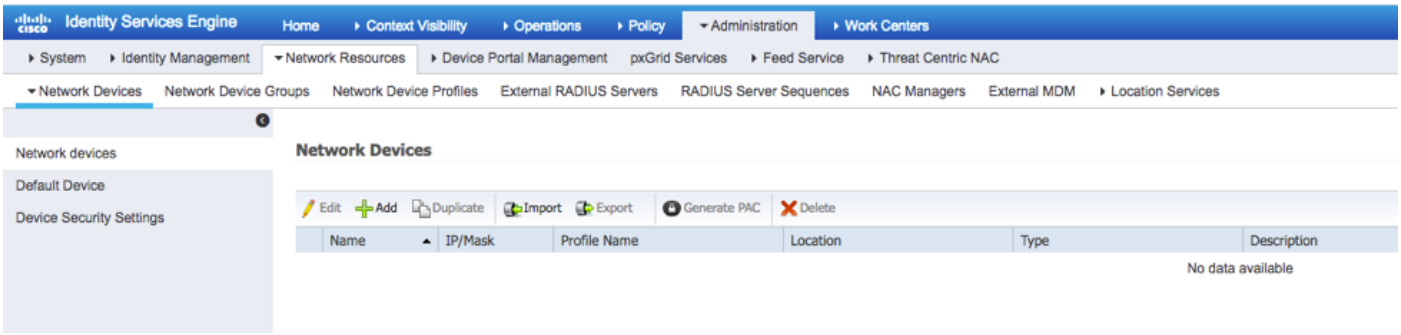
Timeout: 5

Configurazione del server ISE

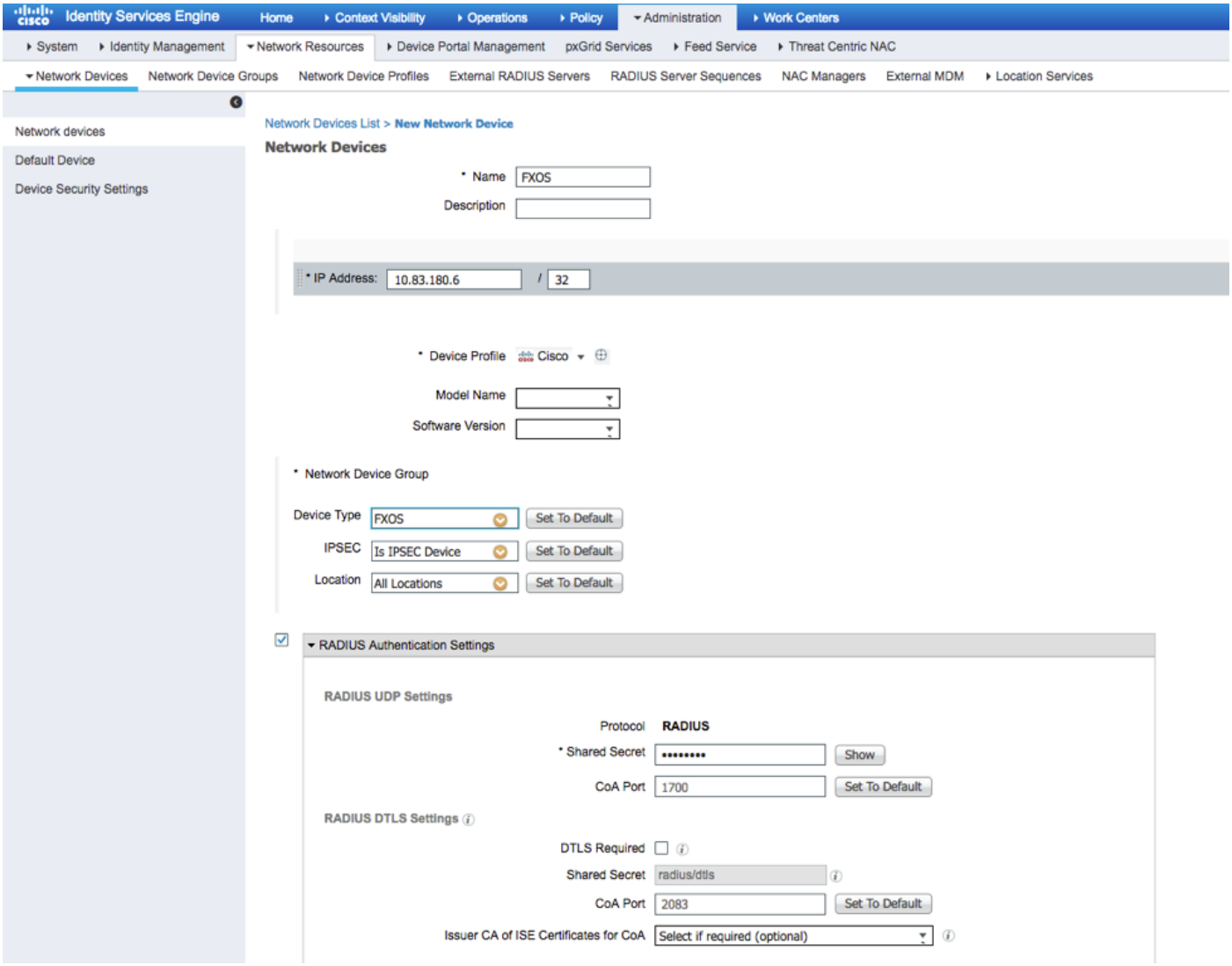
Aggiunta di FXOS come risorsa di rete

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

Passaggio 2. Fare clic su **ADD**



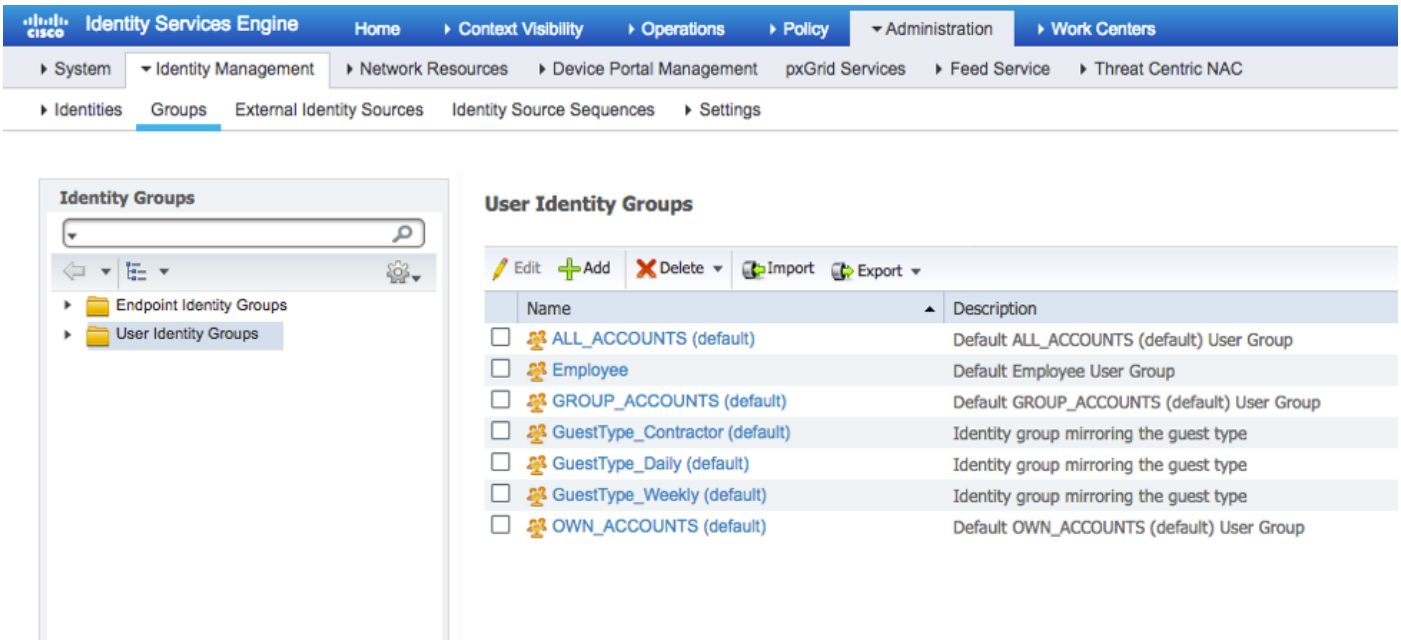
Passaggio 3. Inserire i valori richiesti (Nome, Indirizzo IP, Tipo di dispositivo, Attiva RADIUS e aggiungere la CHIAVE), quindi fare clic su **Submit (Invia).**



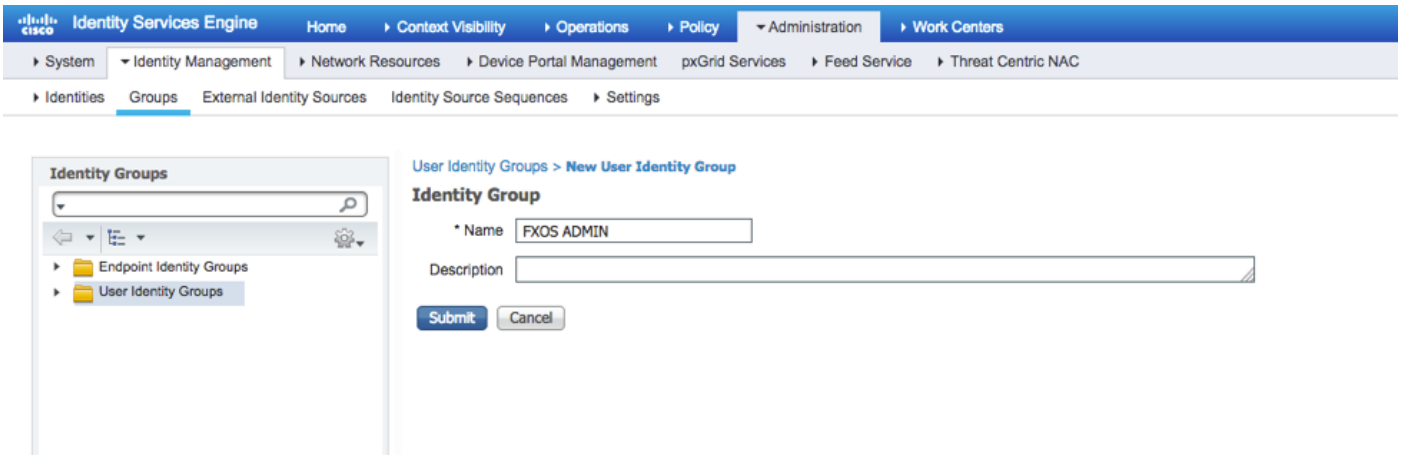
Creazione di gruppi di identità e utenti

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

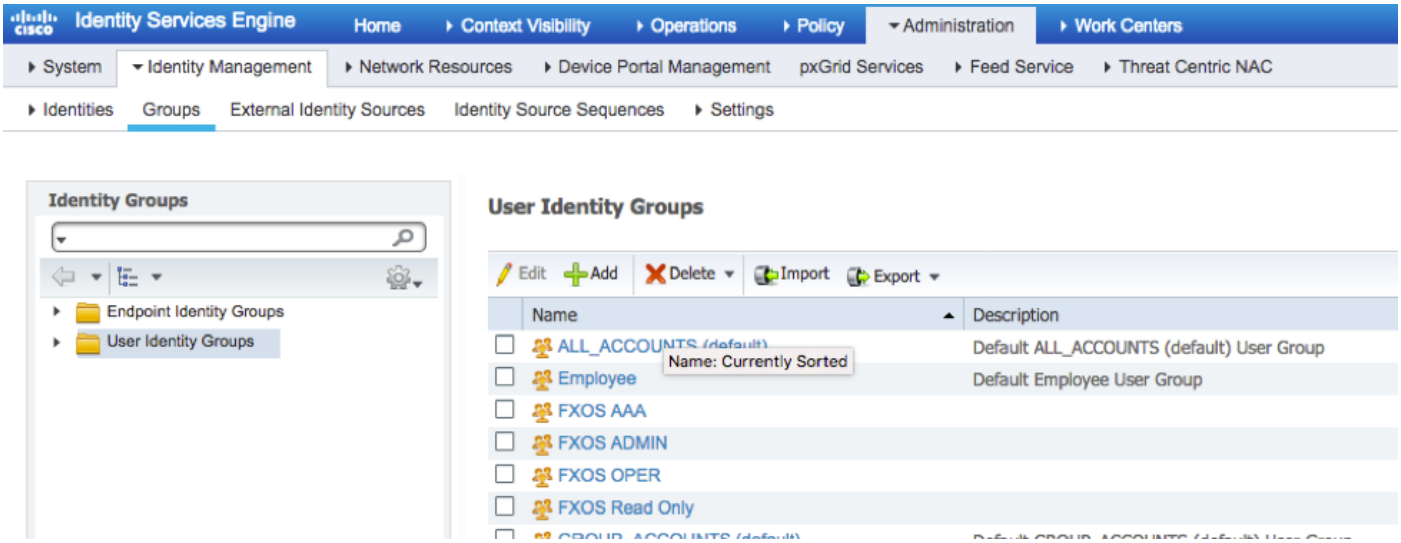
Passaggio 2. Fare clic su **ADD.**



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

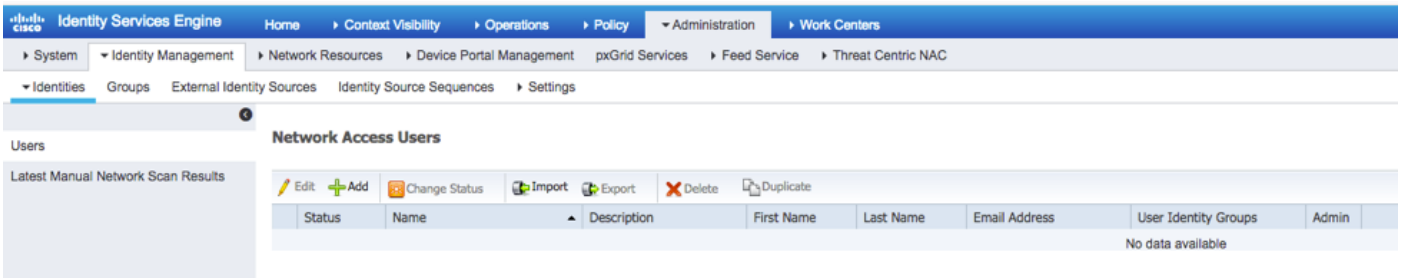


Passaggio 4. Ripetere il passaggio 3 per tutti i ruoli utente richiesti.

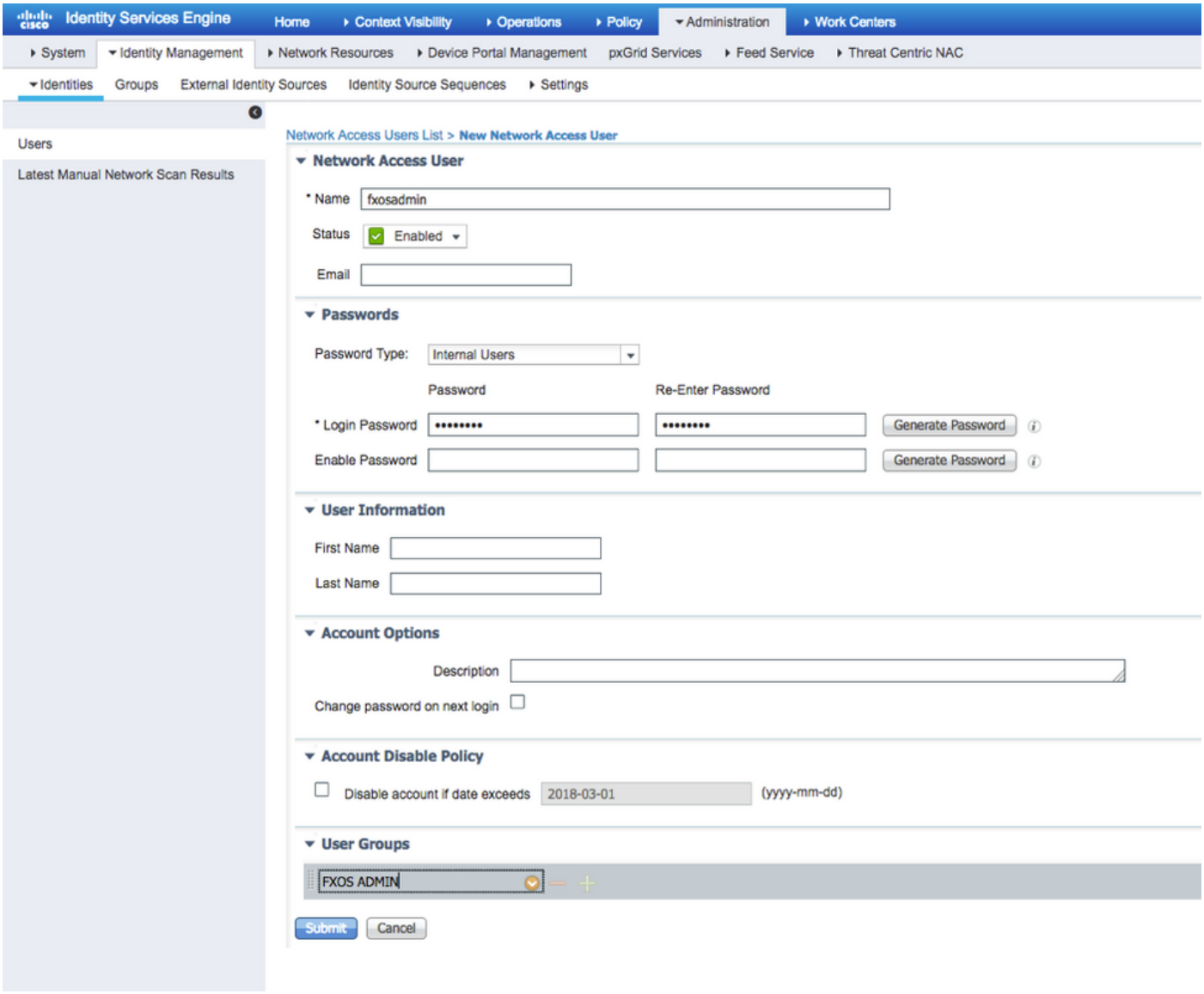


Passaggio 5. Passare a **Amministrazione > Gestione delle identità > Identità > Utenti.**

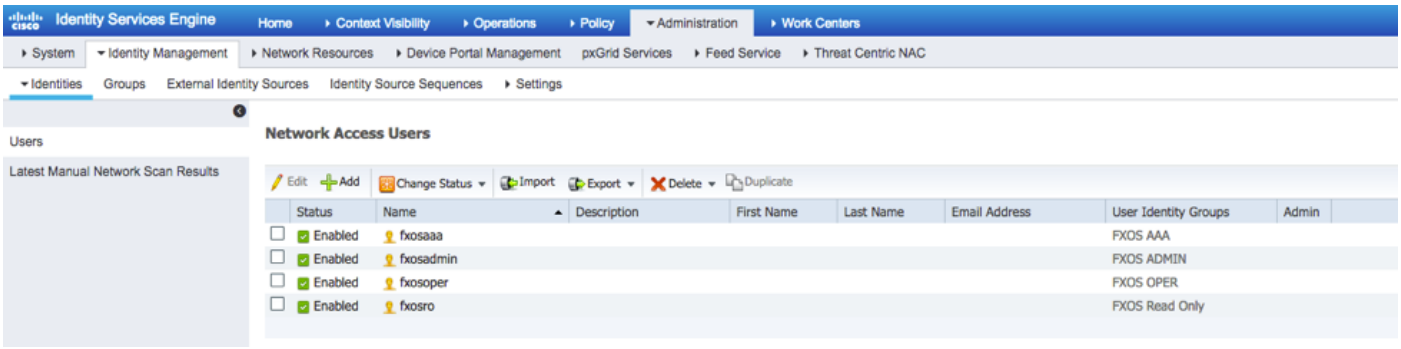
Passaggio 6. Fare clic su **ADD.**



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

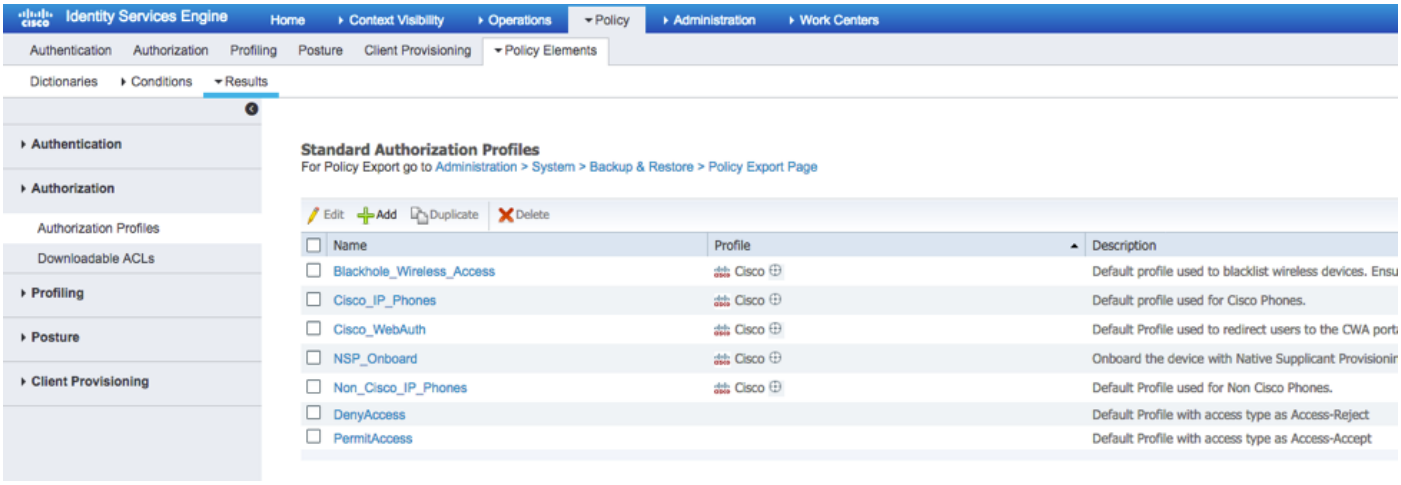


Passaggio 8. Ripetere il passaggio 6 per tutti gli utenti richiesti.



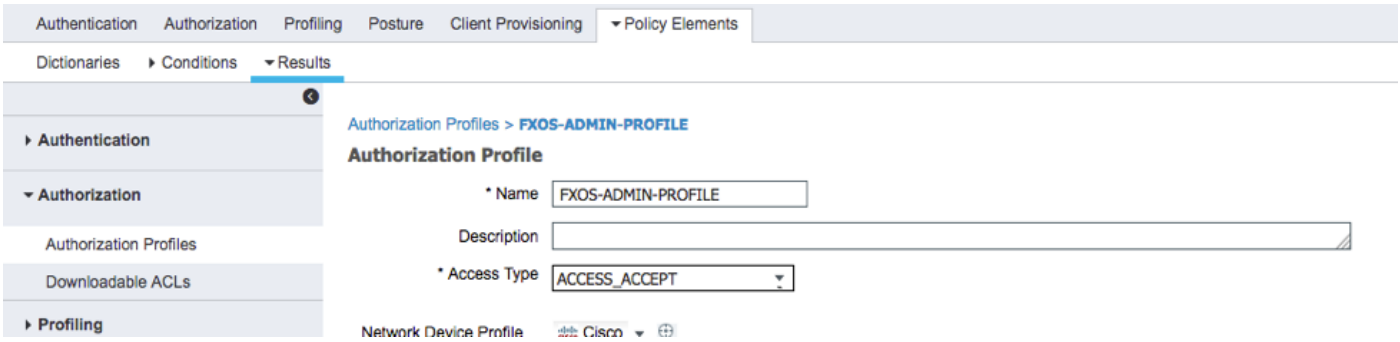
Creazione del profilo di autorizzazione per ogni ruolo utente

Passaggio 1. Andare a Policy > Policy Elements > Results > Authorization > Authorization Profiles (Policy > Elementi della policy > Risultati > Autorizzazione > Profili di autorizzazione).



Passaggio 2. Inserire tutti gli attributi per il profilo di autorizzazione.

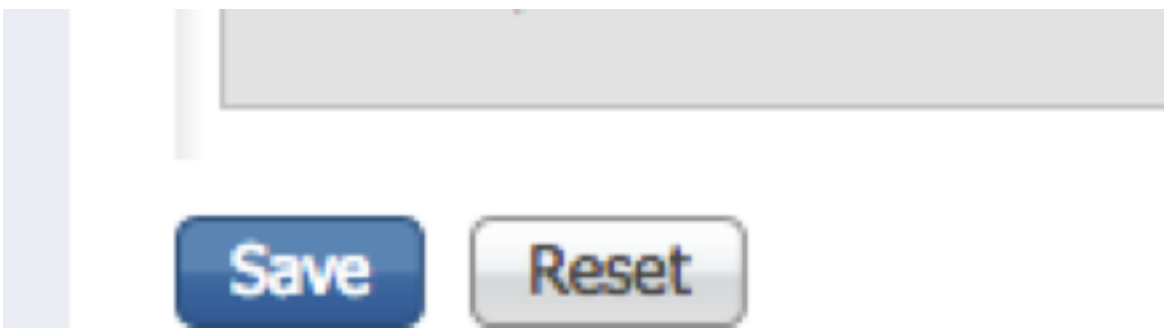
2.1. Configurare il nome del profilo.



2.2. In **Advanced Attributes Settings** configurare la seguente coppia CISCO-AV

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

2.3. Fare clic su **Salva.**



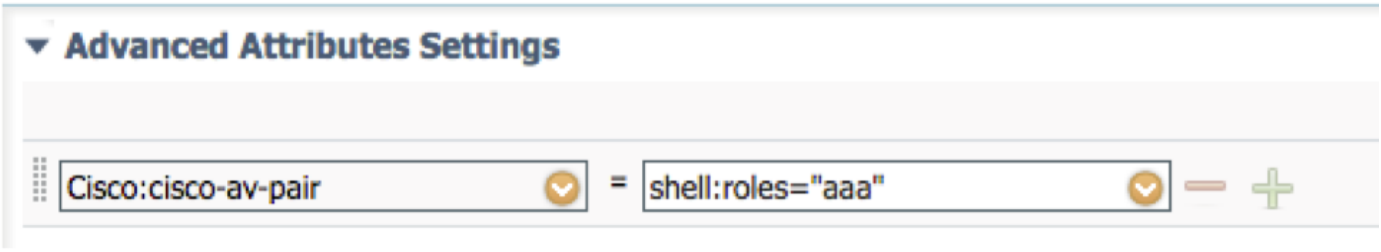
Passaggio 3. Ripetere il passaggio 2 per i ruoli utente rimanenti utilizzando le seguenti coppie

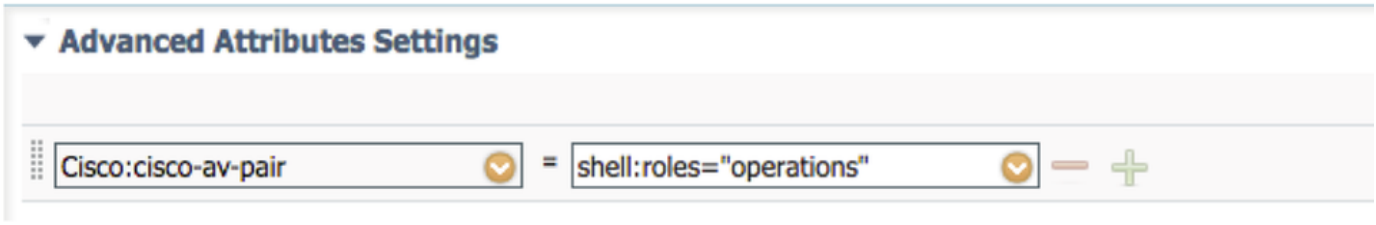
Cisco-AV

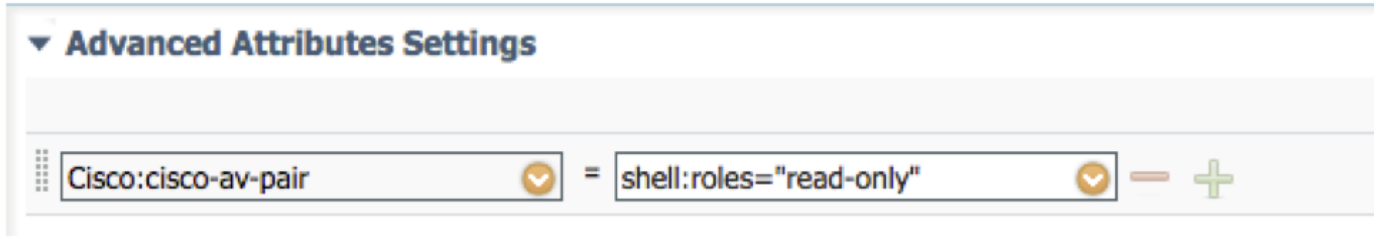
cisco-av-pair=shell:roles="aaa"

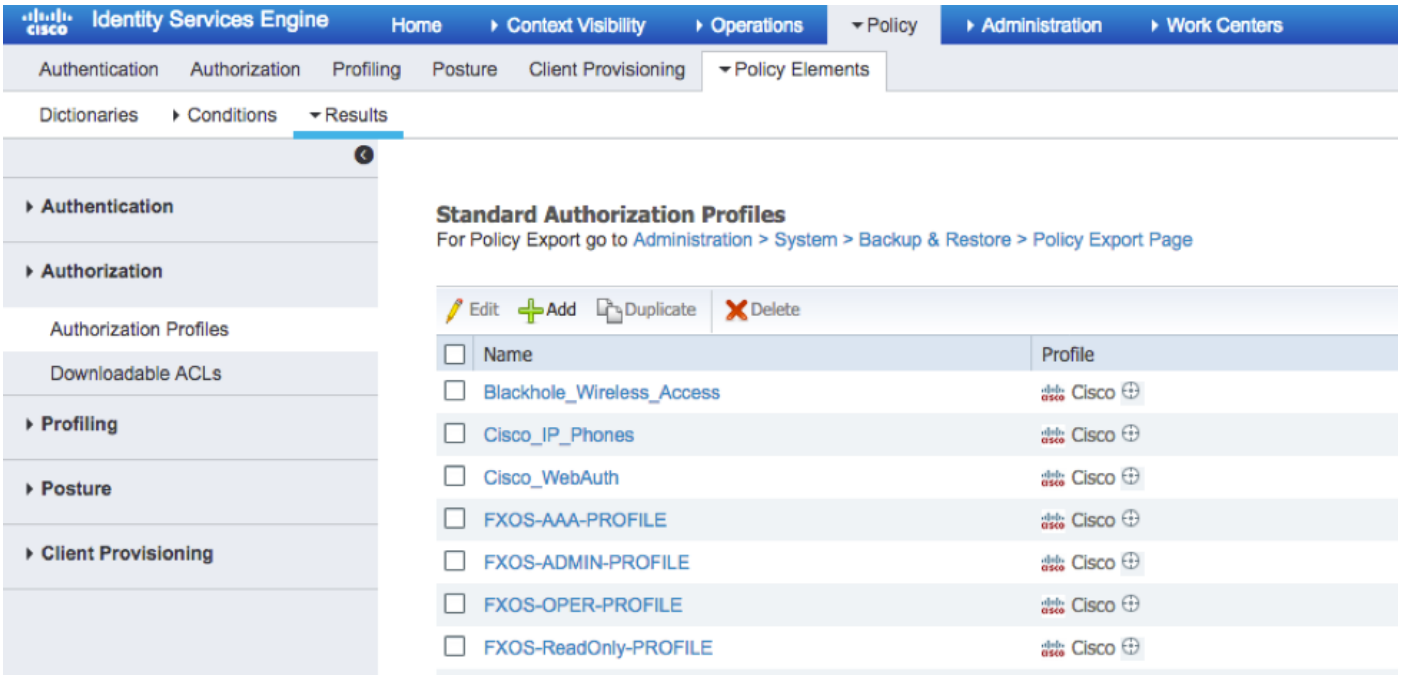
cisco-av-pair=shell:roles="operazioni"

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



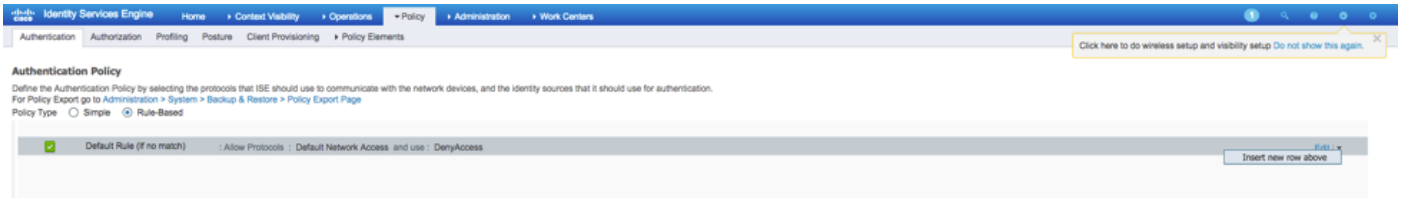






Creazione del criterio di autenticazione

Passaggio 1. Passare a **Criterio > Autenticazione >** E fare clic sulla freccia accanto a Modifica nel punto in cui si desidera creare la regola.



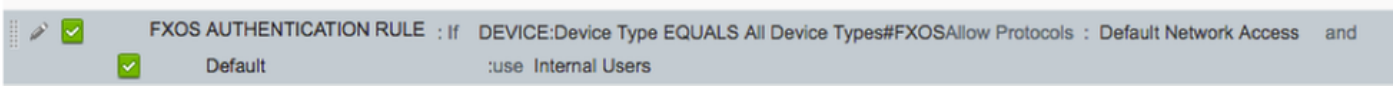
Passaggio 2. L'impostazione è semplice; è possibile eseguire un'operazione più granulare, ma per questo esempio verrà utilizzato il tipo di dispositivo:

Nome: **REGOLA DI AUTENTICAZIONE FXOS**

IF Seleziona nuovo attributo/valore: **Dispositivo:Tipo di dispositivo uguale a Tutti i tipi di dispositivo #FXOS**

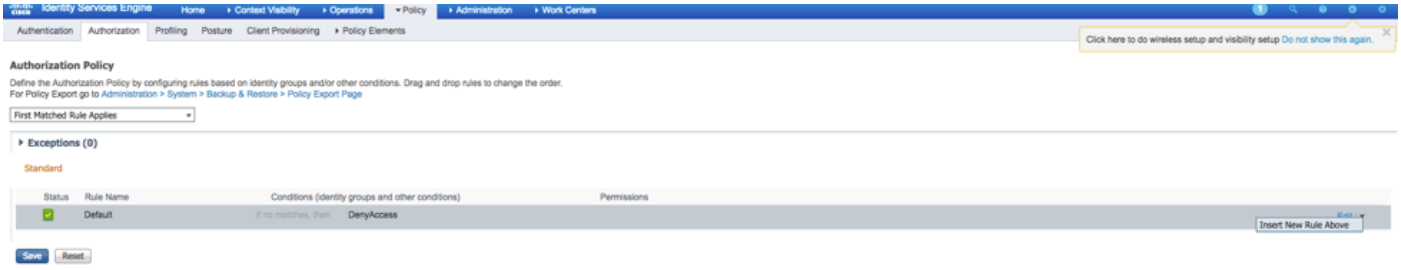
Consenti protocolli: Accesso alla rete predefinito

Utilizzo: Utenti interni



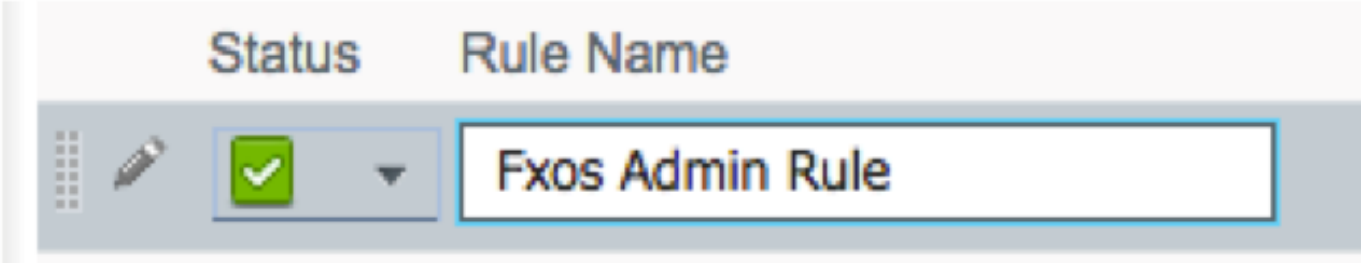
Creazione del criterio di autorizzazione

Passaggio 1. Passare a **Criterio > Autorizzazione >** E fare clic sulla freccia accanto a Modifica nel punto in cui si desidera creare la regola.

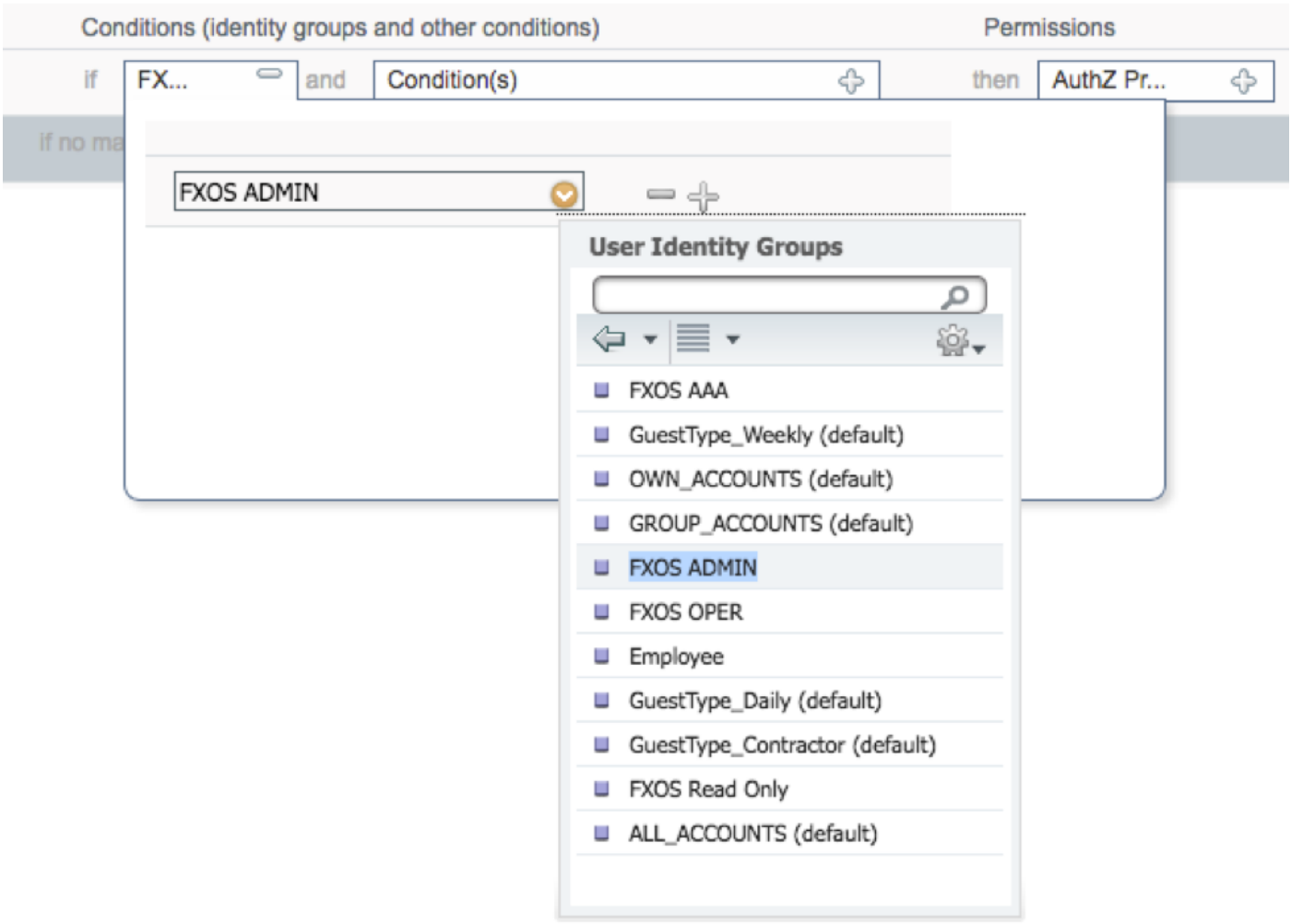


Passaggio 2. Inserire i valori per la regola di autorizzazione con i parametri obbligatori.

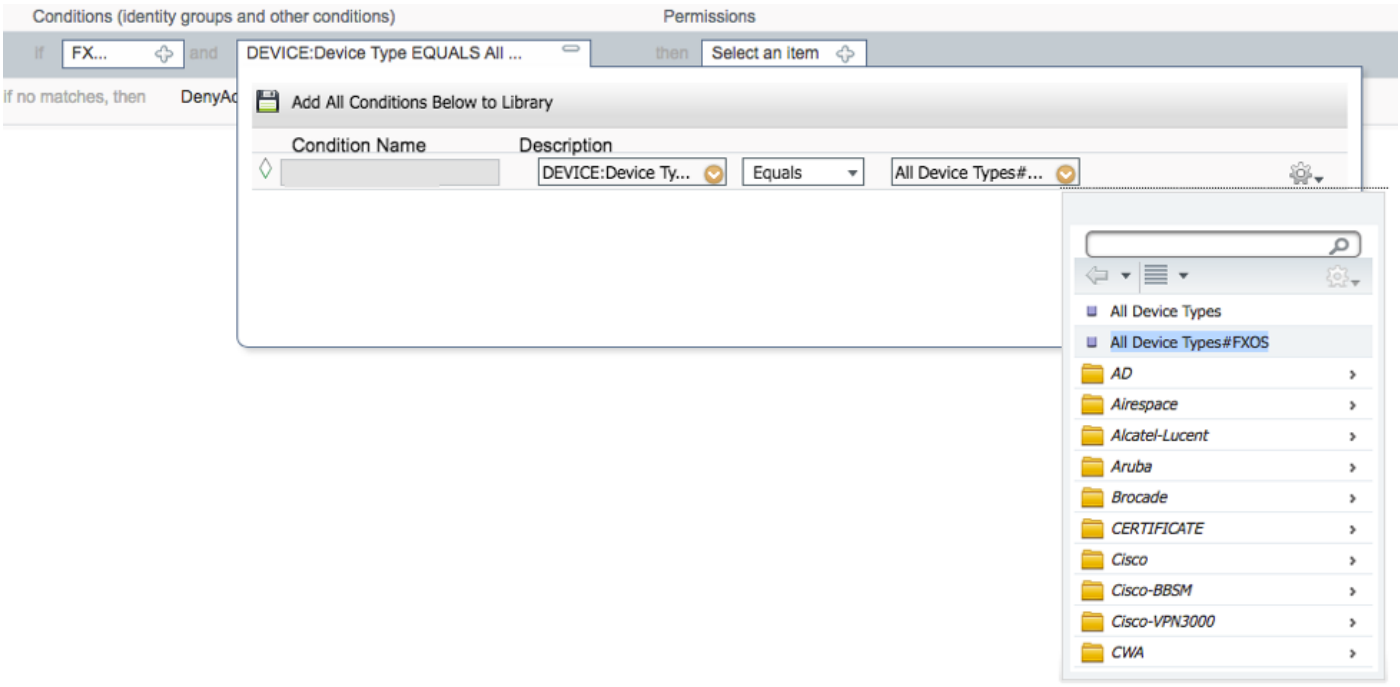
2.1. Nome della regola: **Regola Fxos <RUOLO UTENTE>.**



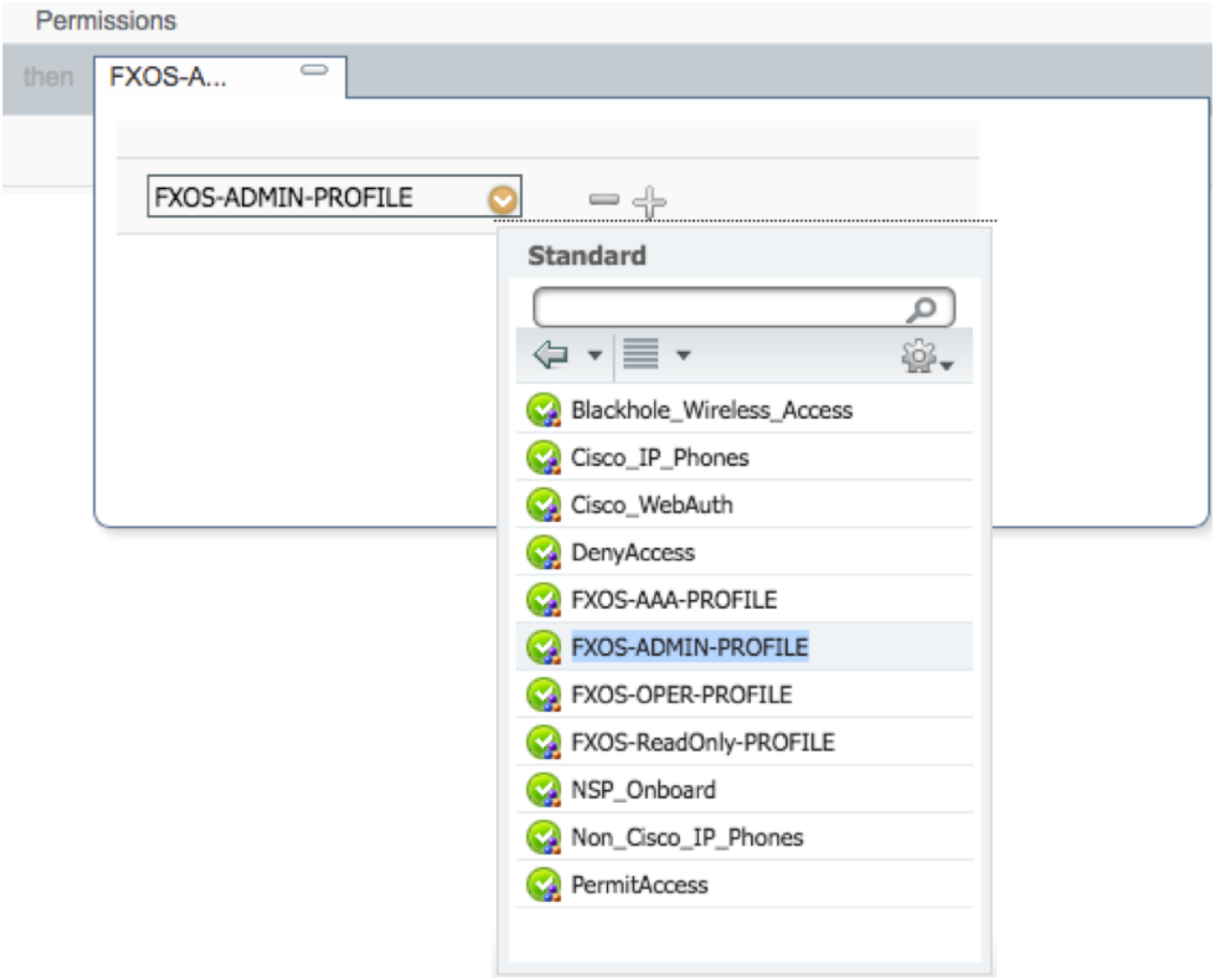
2.2. Se: Gruppi di identità utente > Seleziona **<RUOLO UTENTE>**.



2.3. E: Crea nuova condizione > Periferica:Tipo di periferica uguale a **Tutti i tipi di periferica #FXOS**.



2.4. Autorizzazioni: Standard > Scegli **profilo ruolo utente**

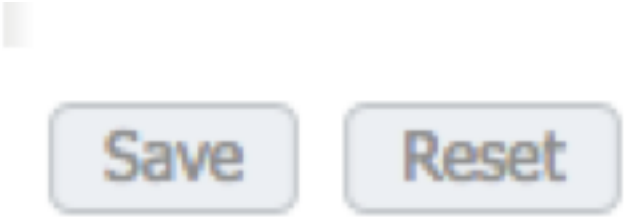


Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Fxos Admin Rule	if **FXOS ADMIN** AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-ADMIN-PROFILE

Passaggio 3. Ripetere il passaggio 2 per tutti i ruoli utente.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Fxos Admin Rule	if **FXOS ADMIN** AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-ADMIN-PROFILE
✓	Fxos AAA Rule	if **FXOS AAA** AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-AAA-PROFILE
✓	Fxos Oper Rule	if **FXOS OPER** AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-OPER-PROFILE
✓	Fxos Read only Rule	if **FXOS Read Only** AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-ReadOnly-PROFILE
✓	Default	if no matches, then	DenyAccess

Passaggio 4. Fare clic su **Save** in fondo alla pagina.



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 e accedere con 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

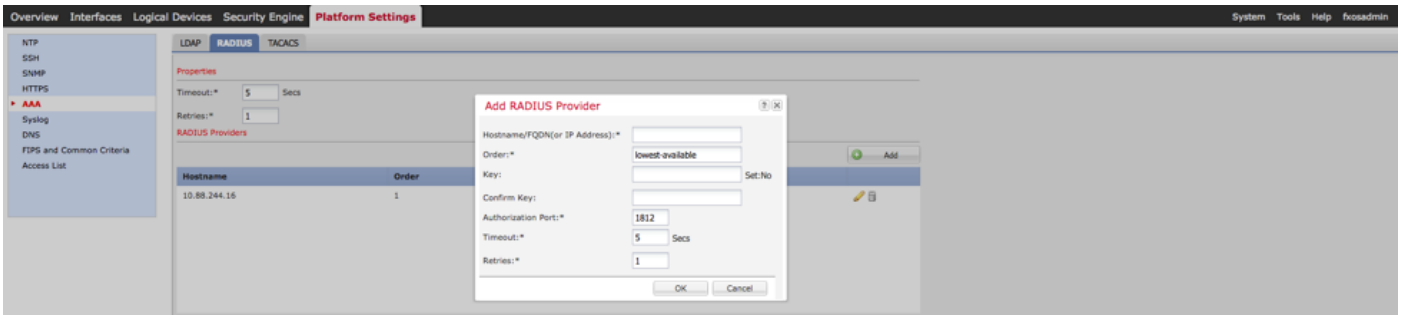
fpr4120-TAC-A#**connect fxos**

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

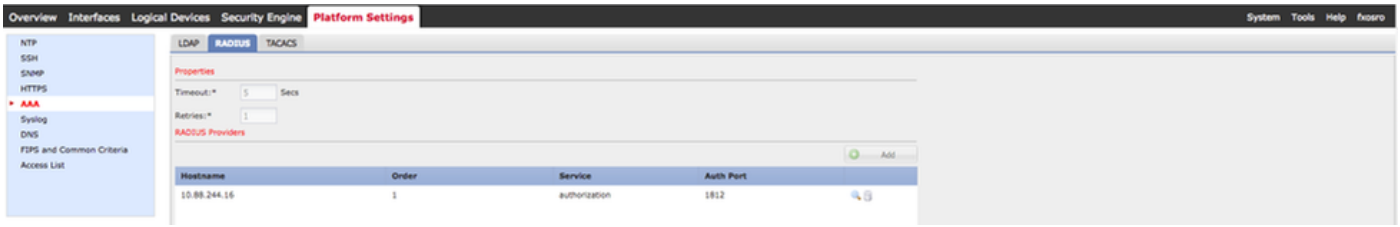
% Autorizzazione negata per il ruolo

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

Ruolo utente amministratore.



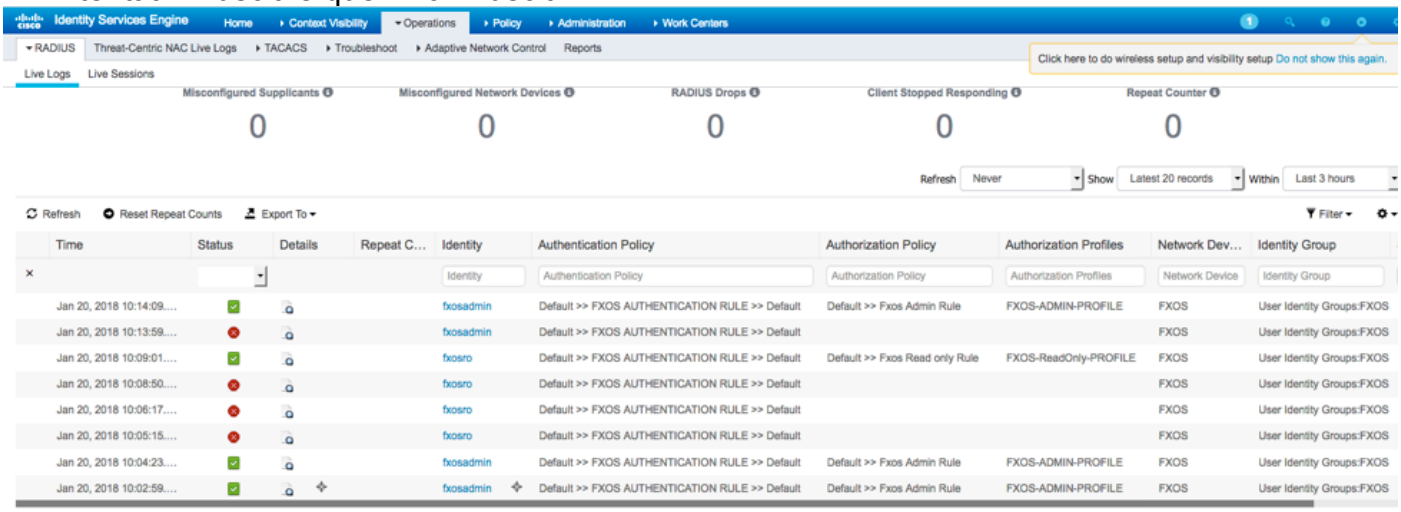
Ruolo utente di sola lettura.



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

Verifica ISE 2.0

1. Passare a **Operazioni > RADIUS > Live Log.** 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 20 17:18:02,410275 aaa: aaa_req_process per l'autenticazione. sessione n. 0

2018 gen 20 17:18:02,410297 aaa: aaa_req_process: Richiesta generale AAA da parte dell'appn: login sottotipo_applicazione: predefinito

2018 gen 20 17:18:02,410310 aaa: try_next_aaa_method

2018 gen 20 17:18:02,410330 aaa: il numero totale di metodi configurati è 1, l'indice corrente da provare è 0

2018 gen 20 17:18:02,410344 aaa: handle_req_using_method

2018 gen 20 17:18:02,410356 aaa: AAA_METHOD_SERVER_GROUP

2018 gen 20 17:18:02,410367 aaa: gruppo aaa_sg_method_handler = raggio

2018 gen 20 17:18:02,410379 aaa: Utilizzo di sg_protocol passato a questa funzione

2018 gen 20 17:18:02,410393 aaa: Invio della richiesta al servizio RADIUS

2018 gen 20 17:18:02,412944 aaa: mts_send_msg_to_port_daemon: Lunghezza payload = 374

2018 gen 20 17:18:02,412973 aaa: sessione: 0x8dfd68c aggiunto alla tabella delle sessioni 1

2018 gen 20 17:18:02,412987 aaa: Gruppo di metodi configurato completato

2018 gen 20 17:18:02,656425 aaa: aaa_process_fd_set

2018 gen 20 17:18:02,656447 aaa: aaa_process_fd_set: mtscallback su aaa_q

2018 gen 20 17:18:02,656470 aaa: mts_message_response_handler: risposta mts

2018 gen 20 17:18:02,656483 aaa: gestore_risposta_daemon

2018 gen 20 17:18:02,656497 aaa: sessione: 0x8dfd68c rimosso dalla tabella delle sessioni 0

2018 gen 20 17:18:02,656512 aaa: is_aaa_resp_status_success status = 1

2018 gen 20 17:18:02,656525 aaa: is_aaa_resp_status_success è TRUE

2018 gen 20 17:18:02,656538 aaa: aaa_send_client_response per l'autenticazione. session->flags=21. aaa_resp->flags=0.

2018 gen 20 17:18:02,656550 aaa: AAA_REQ_FLAG_NORMAL

2018 gen 20 17:18:02,656577 aaa: mts_send_response riuscito

2018 gen 20 17:18:02,700520 aaa: aaa_process_fd_set: mtscallback su aaa_accounting_q

2018 gen 20 17:18:02,700688 aaa: CODICE OPERATIVO PRECEDENTE: accounting_interim_update

2018 gen 20 17:18:02,700702 aaa: aaa_create_local_acct_req: user=, session_id=, log=added user fxosro

2018 gen 20 17:18:02,700725 aaa: aaa_req_process per l'accounting. sessione n. 0

2018 gen 20 17:18:02,700738 aaa: Il riferimento alla richiesta MTS è NULL. richiesta LOCALE

2018 gen 20 17:18:02,700749 aaa: Impostazione di AAA_REQ_RESPONSE_NOT_NEEDED

2018 gen 20 17:18:02,700762 aaa: aaa_req_process: Richiesta generale AAA da parte dell'appn: default appln_subtype: predefinito

2018 gen 20 17:18:02,700774 aaa: try_next_aaa_method

2018 gen 20 17:18:02,700798 aaa: nessun metodo configurato per l'impostazione predefinita

2018 gen 20 17:18:02,700810 aaa: nessuna configurazione disponibile per questa richiesta

2018 gen 20 17:18:02,700997 aaa: aaa_send_client_response per accounting. session->flags=254. aaa_resp->flags=0.

2018 gen 20 17:18:02,701010 aaa: la risposta per la richiesta di accounting della libreria precedente verrà inviata come SUCCESS

2018 gen 20 17:18:02,701021 aaa: risposta non necessaria per la richiesta

2018 gen 20 17:18:02,701033 aaa: AAA_REQ_FLAG_LOCAL_RESP

2018 gen 20 17:18:02,701044 aaa: sessione_pulizia_aaa

2018 gen 20 17:18:02,701055 aaa: aaa_req deve essere liberato.

2018 gen 20 17:18:02,701067 aaa: Metodo di fallback locale riuscito

2018 gen 20 17:18:02,706922 aaa: aaa_process_fd_set

2018 gen 20 17:18:02,706937 aaa: aaa_process_fd_set: mtscallback su aaa_accounting_q

2018 gen 20 17:18:02,706959 aaa: CODICE OPERATIVO PRECEDENTE: accounting_interim_update

2018 gen 20 17:18:02,706972 aaa: aaa_create_local_acct_req: user=, session_id=, log=added user:fxosro to the role:read-only

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

2018 gen 20 17:15:18,102130 aaa: aaa_process_fd_set

2018 gen 20 17:15:18,102149 aaa: aaa_process_fd_set: mtscallback su aaa_q

2018 gen 20 17:15:18,102267 aaa: aaa_process_fd_set

2018 gen 20 17:15:18,102281 aaa: aaa_process_fd_set: mtscallback su aaa_q

2018 gen 20 17:15:18,102363 aaa: aaa_process_fd_set

2018 gen 20 17:15:18,102377 aaa: aaa_process_fd_set: mtscallback su aaa_q

2018 gen 20 17:15:18,102456 aaa: aaa_process_fd_set

2018 gen 20 17:15:18,102468 aaa: aaa_process_fd_set: mtscallback su aaa_q

2018 gen 20 17:15:18,102489 aaa: mts_aaa_req_process

2018 gen 20 17:15:18,102503 aaa: aaa_req_process per l'autenticazione. sessione n. 0

2018 gen 20 17:15:18,102526 aaa: aaa_req_process: Richiesta generale AAA da parte dell'appn: login sottotipo_applicazione: predefinito

2018 gen 20 17:15:18,102540 aaa: try_next_aaa_method

2018 gen 20 17:15:18,102562 aaa: il numero totale di metodi configurati è 1, l'indice corrente da provare è 0

2018 gen 20 17:15:18,102575 aaa: handle_req_using_method

2018 gen 20 17:15:18,102586 aaa: AAA_METHOD_SERVER_GROUP

2018 gen 20 17:15:18,102598 aaa: gruppo aaa_sg_method_handler = raggio

2018 gen 20 17:15:18,102610 aaa: Utilizzo di sg_protocol passato a questa funzione

2018 gen 20 17:15:18,102625 aaa: Invio della richiesta al servizio RADIUS

2018 gen 20 17:15:18,102658 aaa: mts_send_msg_to_port_daemon: Lunghezza payload = 371

2018 gen 20 17:15:18,102684 aaa: sessione: 0x8dfd68c aggiunto alla tabella delle sessioni 1

2018 gen 20 17:15:18,102698 aaa: Gruppo di metodi configurato completato

2018 gen 20 17:15:18,273682 aaa: aaa_process_fd_set

2018 gen 20 17:15:18,273724 aaa: aaa_process_fd_set: mtscallback su aaa_q

2018 gen 20 17:15:18,273753 aaa: mts_message_response_handler: risposta mts

2018 gen 20 17:15:18,273768 aaa: gestore_risposta_daemon

2018 gen 20 17:15:18,273783 aaa: sessione: 0x8dfd68c rimosso dalla tabella delle sessioni 0

2018 gen 20 17:15:18,273801 aaa: is_aaa_resp_status_success status = 2

2018 gen 20 17:15:18,273815 aaa: is_aaa_resp_status_success è TRUE

2018 gen 20 17:15:18,273829 aaa: aaa_send_client_response per l'autenticazione. session->flags=21. aaa_resp->flags=0.

2018 gen 20 17:15:18,273843 aaa: AAA_REQ_FLAG_NORMAL

2018 gen 20 17:15:18,273877 aaa: mts_send_response riuscito

2018 gen 20 17:15:18,273902 aaa: sessione_pulizia_aaa

2018 gen 20 17:15:18,273916 aaa: mts_drop del messaggio di richiesta

2018 gen 20 17:15:18,273935 aaa: aaa_req deve essere liberato.

2018 gen 20 17:15:18,280416 aaa: aaa_process_fd_set

2018 gen 20 17:15:18,280443 aaa: aaa_process_fd_set: mtscallback su aaa_q

2018 gen 20 17:15:18,280454 aaa: aaa_enable_info_config: GET_REQ per il messaggio di errore di accesso aaa

2018 gen 20 17:15:18,280460 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