Integrazione CSM TACACS con ISE

Sommario

Introduzione

Questo documento descrive la procedura per integrare Cisco Security Manager (CSM) con Identity Services Engine (ISE) per autenticare gli utenti amministratori con il protocollo TACACS+.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Security Manager (CSM).
- Identity Services Engine (ISE).
- Protocollo TACACS.

Componenti usati

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

- CSM Server versione 4.2
- ISE versione 3.0

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

Per impostazione predefinita, Cisco Security Manager (CSM) utilizza una modalità di autenticazione chiamata Ciscoworks per autenticare e autorizzare gli utenti a livello locale, in modo da avere un metodo di autenticazione centralizzato che è possibile utilizzare Cisco Identity Service Engine tramite il protocollo TACACS.

Configurazione

Esempio di rete

Procedura di autenticazione

Passaggio 1. Accedere all'applicazione CSM con le credenziali dell'utente amministratore.

Passaggio 2. Il processo di autenticazione attiva e ISE convalida le credenziali localmente o tramite Active Directory.

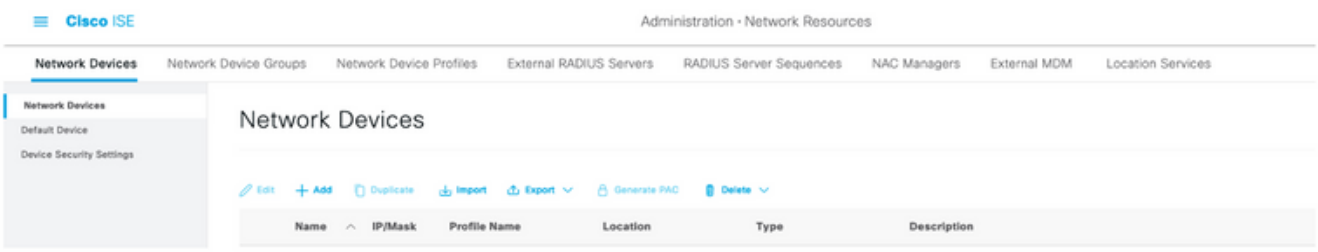
Passaggio 3. Una volta completata l'autenticazione, ISE invia un pacchetto di autorizzazione per autorizzare l'accesso al CSM.

Passaggio 4. CSM esegue il mapping del nome utente con l'assegnazione del ruolo utente locale.

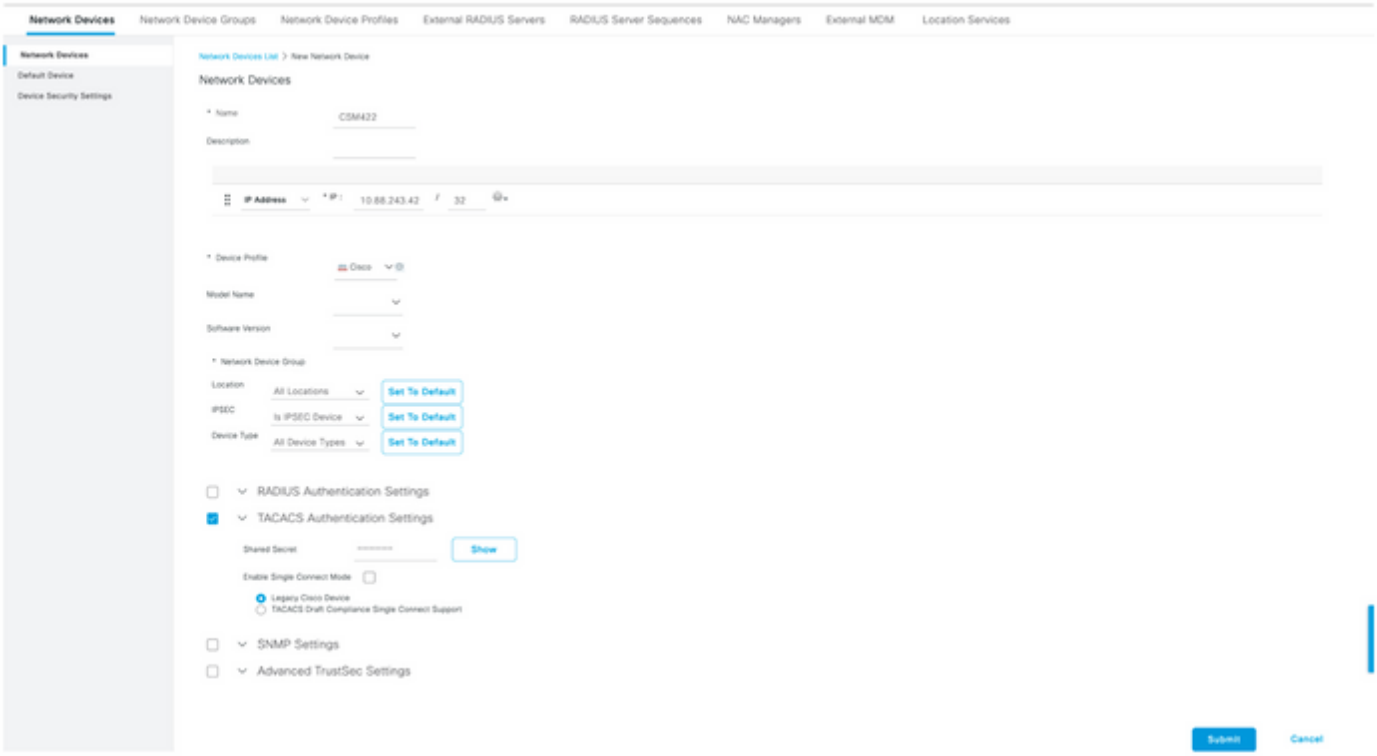
Passaggio 5. ISE mostra un log live di autenticazione completato.

Configurazione di ISE

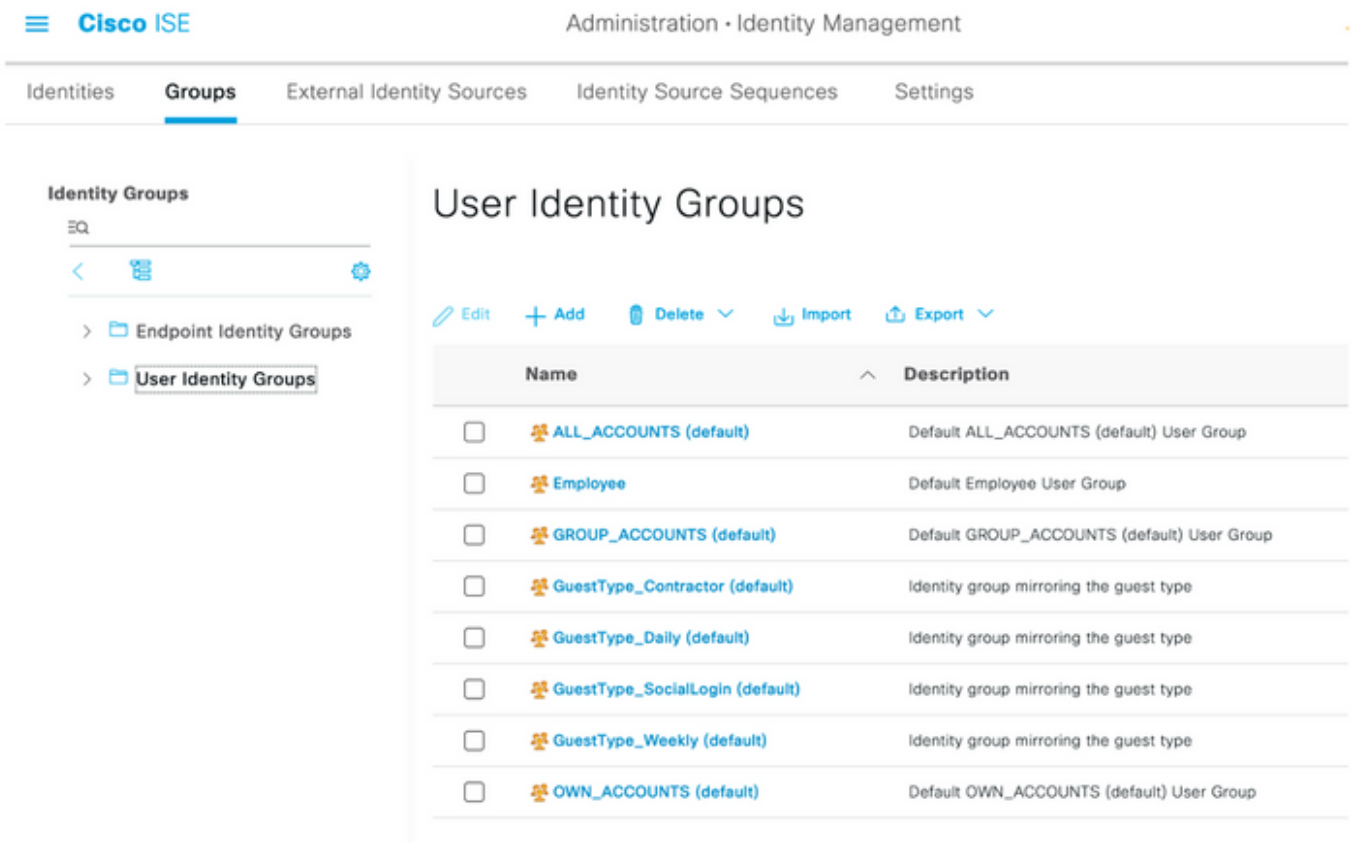
Passaggio 1. Selezionare l'icona a tre righe nell'angolo superiore sinistro e selezionare **Amministrazione > Risorse di rete > Dispositivi di rete.**



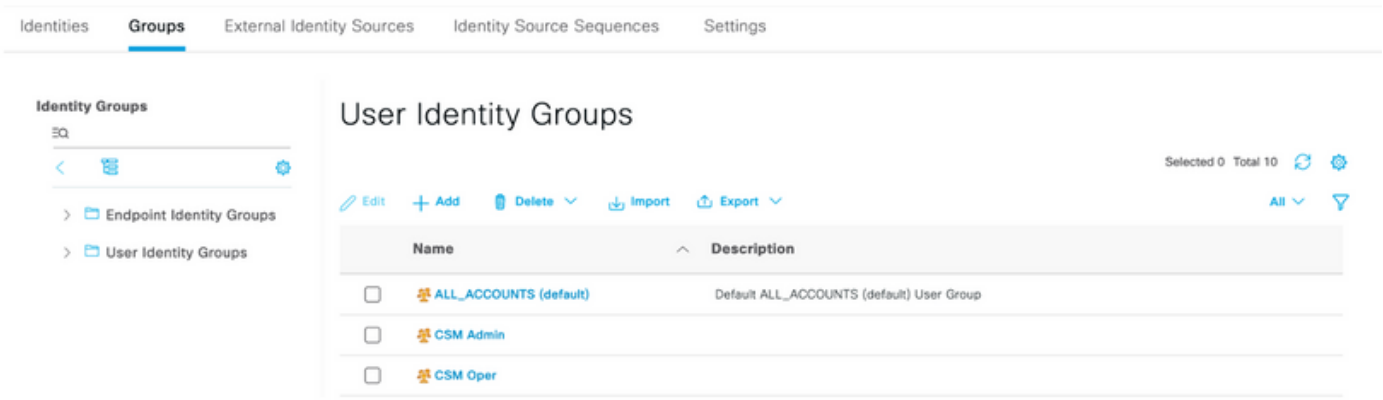
Passaggio 2. Selezionare il pulsante **+Add** e immettere i valori corretti per Network Access Device Name e IP Address, quindi verificare la casella di controllo **TACACS Authentication Settings** e definire un segreto condiviso. Selezionare il pulsante **Invia**.



Passaggio 3. Selezionare l'icona delle tre linee nell'angolo superiore sinistro e selezionare **Amministrazione > Gestione delle identità > Gruppi.**

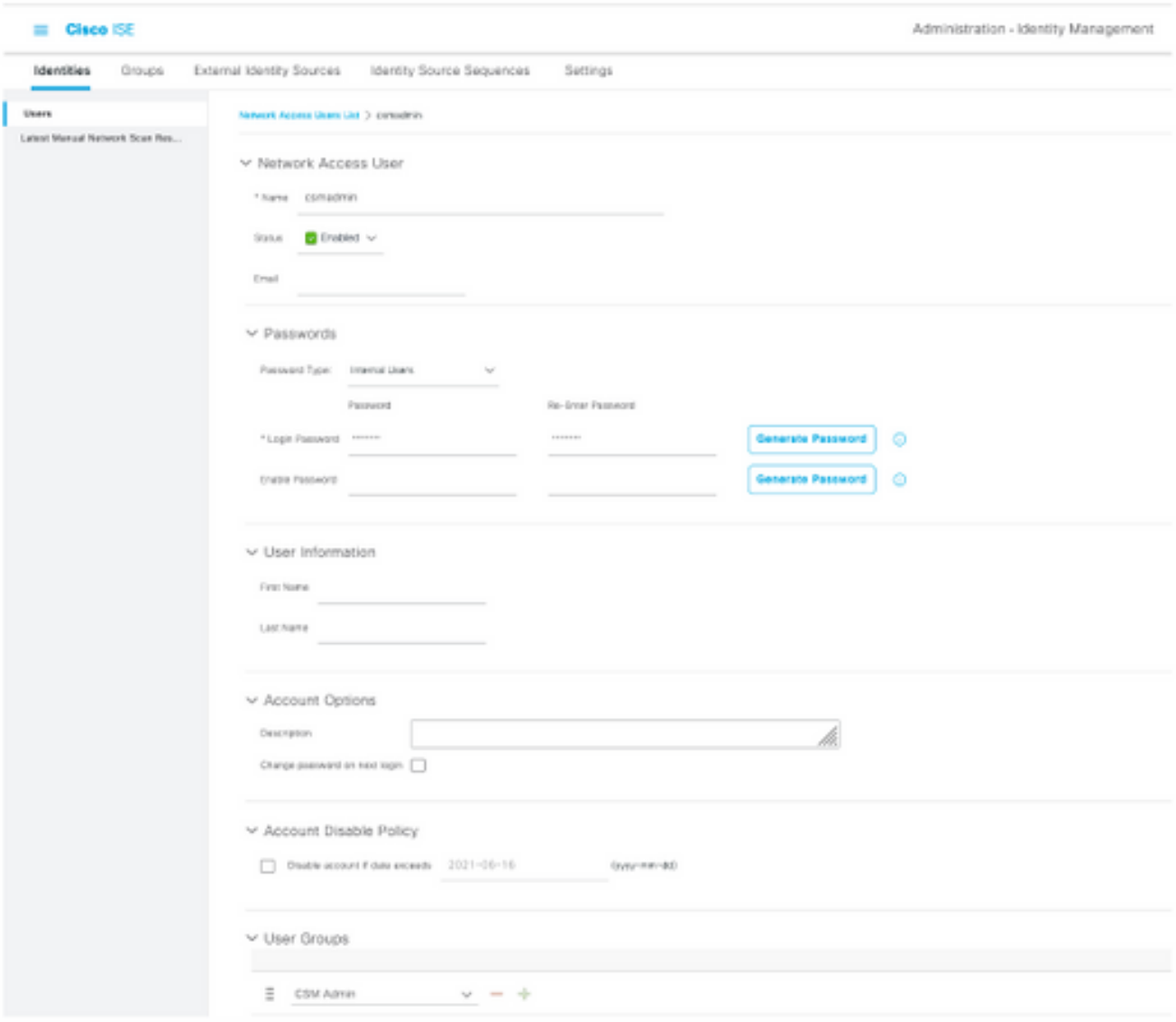


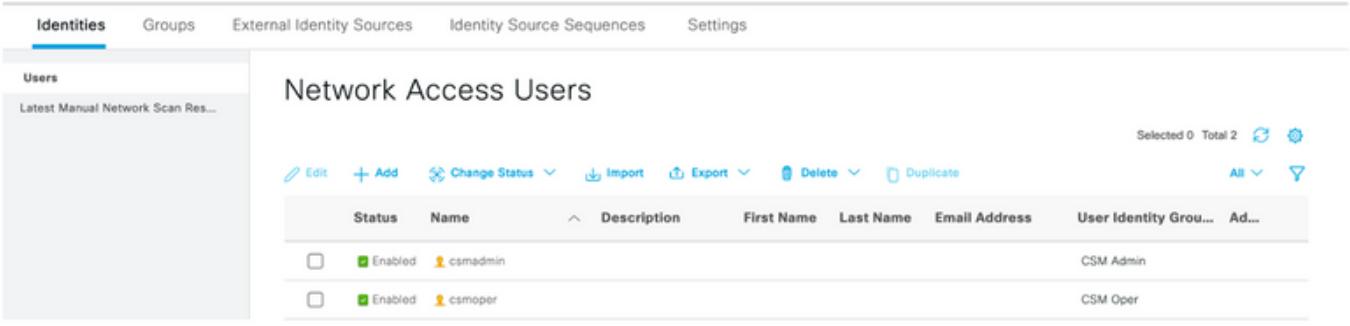
Passaggio 4. Passare alla cartella **Gruppi di identità utente** e selezionare il pulsante **+Aggiungi**. Definire un nome e selezionare il pulsante **Invia**.



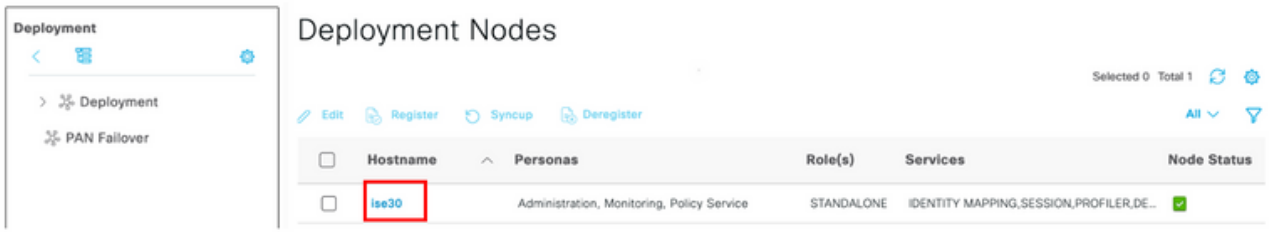
Nota: In questo esempio vengono creati i gruppi CSM Admin e CSM Oper Identity. È possibile ripetere il passaggio 4 per ogni tipo di utente Admin su CSM

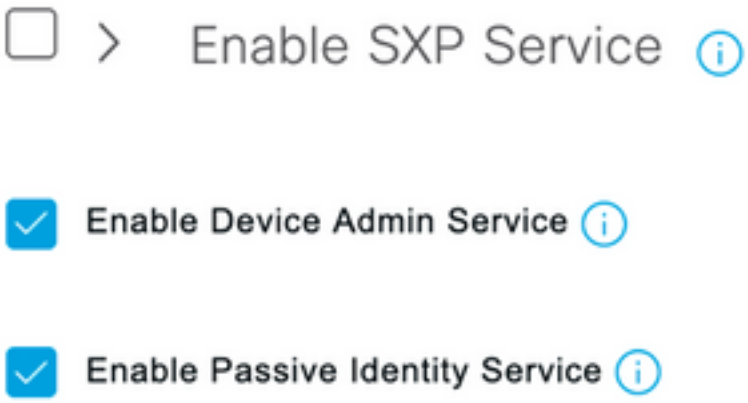
Passaggio 5. Selezionare l'icona a tre righe e selezionare **Amministrazione > Gestione delle identità > Identità.** Selezionare il pulsante **+Aggiungi** e definire il nome utente e la password, quindi selezionare il gruppo a cui appartiene l'utente. In questo esempio vengono creati gli utenti **csmadmin** e **csmoper**, assegnati rispettivamente ai gruppi CSM Admin e CSM Oper.





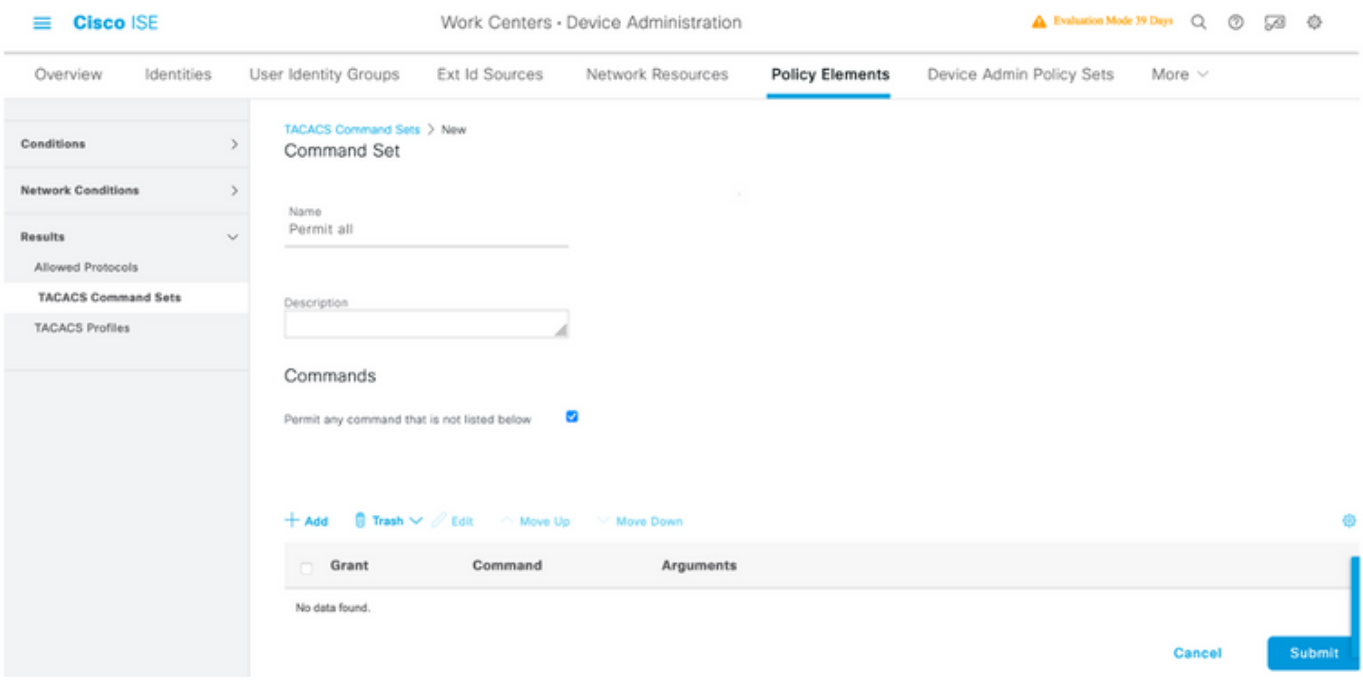
Passaggio 6. Selezionare e selezionare **Amministrazione > Sistema > Distribuzione.** Selezionare il nodo hostname e abilitare il **servizio Device Admin**





Nota: In caso di distribuzione distribuita, selezionare il nodo PSN che gestisce le richieste TACACS

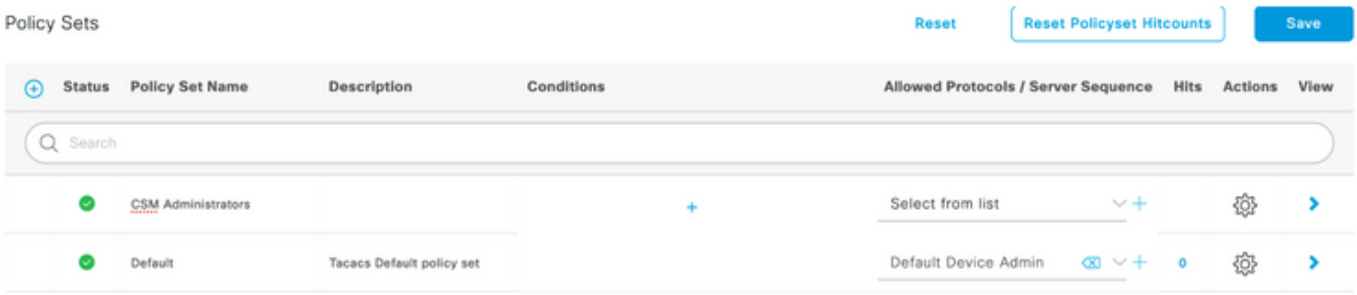
Passaggio 7. Selezionare l'icona a tre righe e passare ad **Amministrazione > Amministrazione dispositivi > Elementi della policy.** Passare a **Risultati > Set di comandi TACACS.** Selezionare **+**Pulsante **Aggiungi,** definire un nome per il set di comandi e attivare la **casella di controllo Consenti qualsiasi comando non elencato sotto** la casella di controllo. Selezionare **Sottometti.**



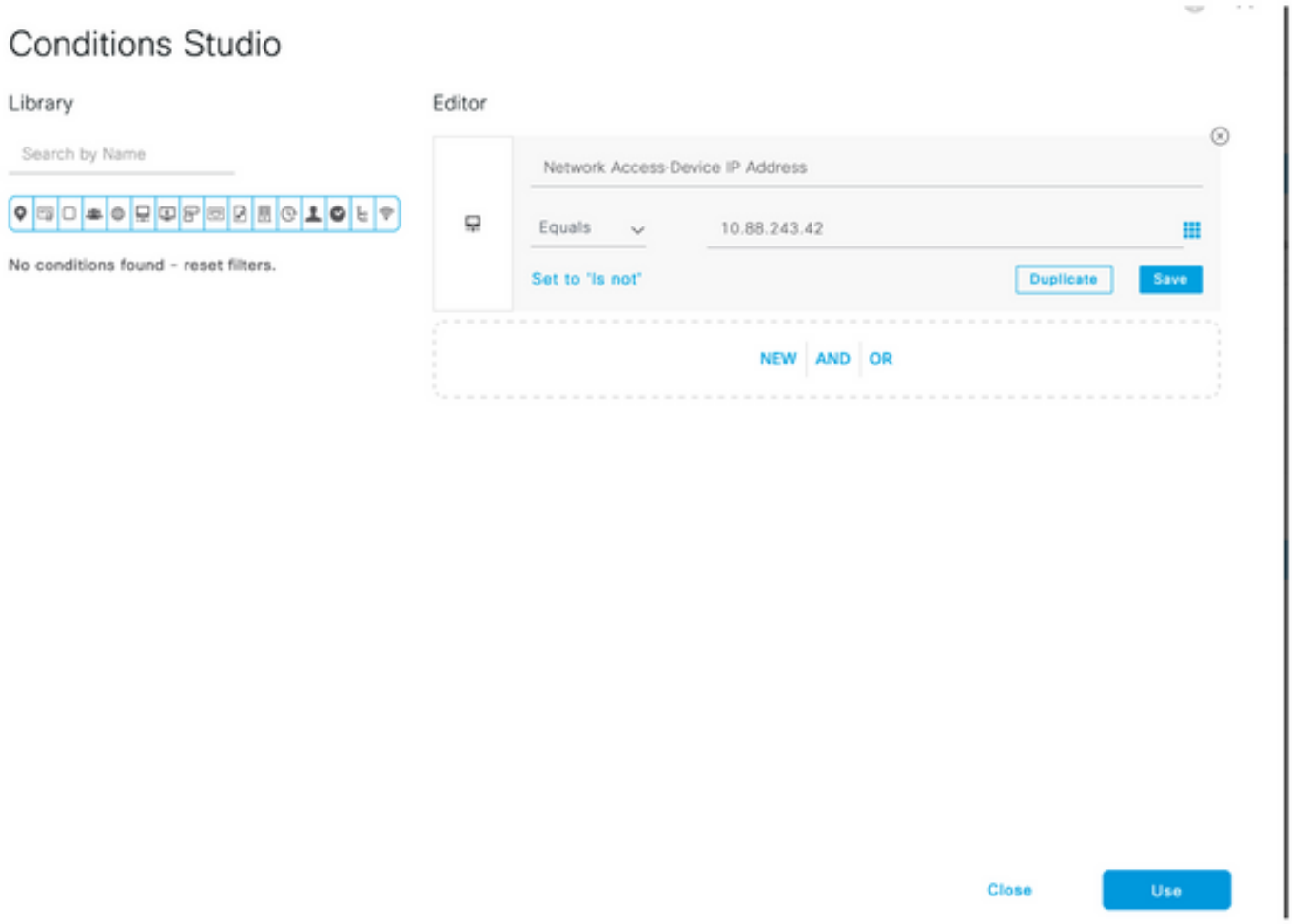
Passaggio 8. Selezionare l'icona a tre righe nell'angolo superiore sinistro e selezionare

Amministrazione->Amministrazione dispositivi->Set di criteri di amministrazione dispositivi.

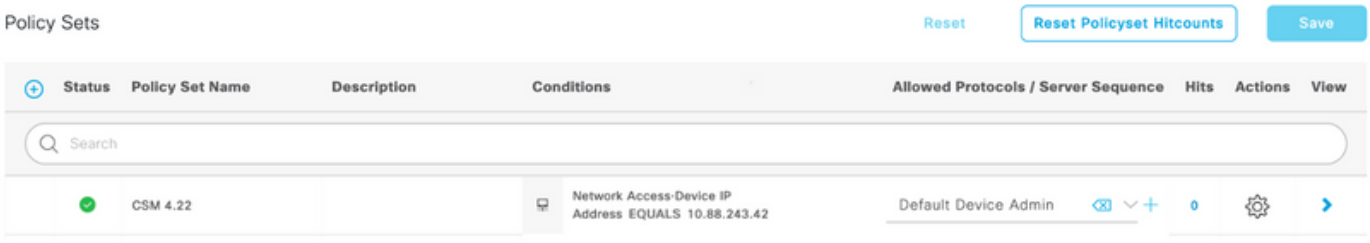
Seleziona  situato sotto il titolo Set di criteri, definire un nome e selezionare il pulsante **+** al centro per aggiungere una nuova condizione.



Passaggio 9. Nella finestra Condizione, selezionare Aggiungi attributo, quindi selezionare Icona **periferica di rete** seguito da Indirizzo IP periferica di accesso alla rete. Selezionare **Attribute Value** (Valore attributo) e aggiungere l'indirizzo IP del CSM. Selezionare **Use** once done (Usa al termine).



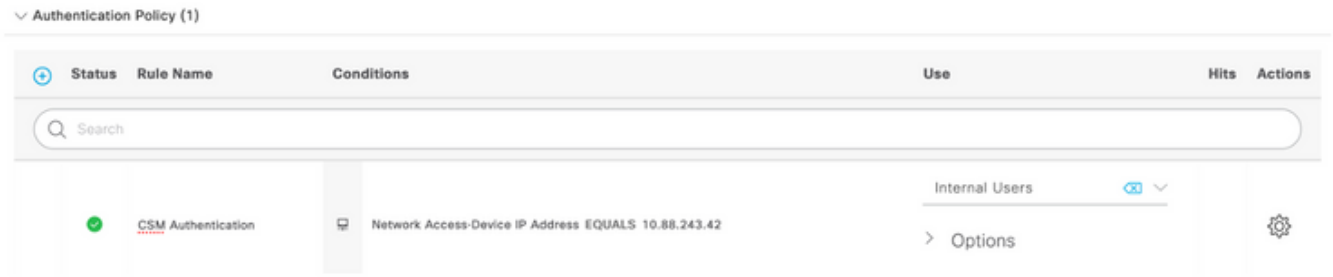
Passaggio 10. In Consenti protocolli, sezione, selezionare **Device Default Admin**. Selezionare **Salva**



Passaggio 11. Selezionare la freccia destra icona del set di criteri per la definizione dei criteri di autenticazione e autorizzazione

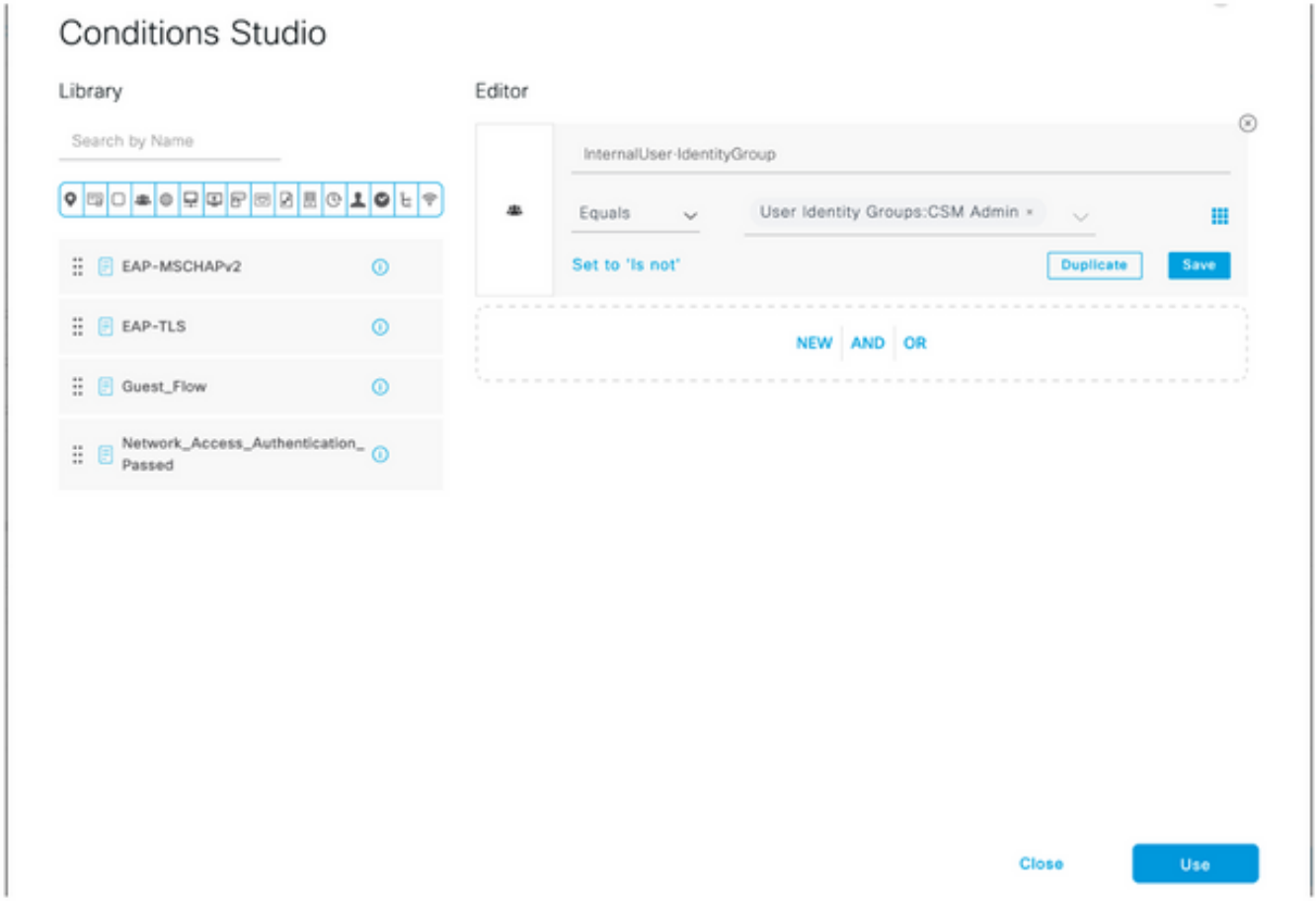
Passaggio 12. Selezionare situato sotto il titolo del criterio di autenticazione, definire un nome e selezionare il segno + al centro per aggiungere una nuova condizione. Nella finestra Condizione selezionare Aggiungi attributo, quindi **Icona periferica di rete** seguito da Indirizzo IP periferica di accesso alla rete. Selezionare **Attribute Value** (Valore attributo) e aggiungere l'indirizzo IP del CSM. Selezionare **Use** once done (Usa al termine)

Passaggio 13. Selezionare gli utenti **interni** nell'archivio identità e selezionare **Salva**



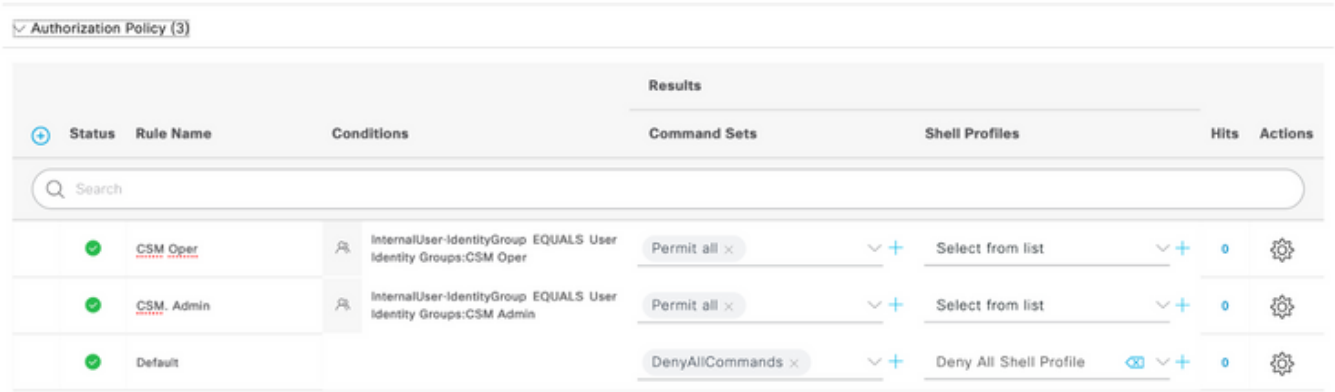
Nota: È possibile modificare l'archivio identità in archivio AD se ISE è aggiunto a un Active Directory.

Passaggio 14. Selezionare sotto il titolo del criterio di autorizzazione, definire un nome e selezionare il pulsante **+** al centro per aggiungere una nuova condizione. Nella finestra Condizione selezionare Aggiungi attributo, quindi selezionare **l'**icona **Gruppo di identità** seguita da **Utente interno: Gruppo di identità.** Selezionare il gruppo CSM Admin e **Usa**.



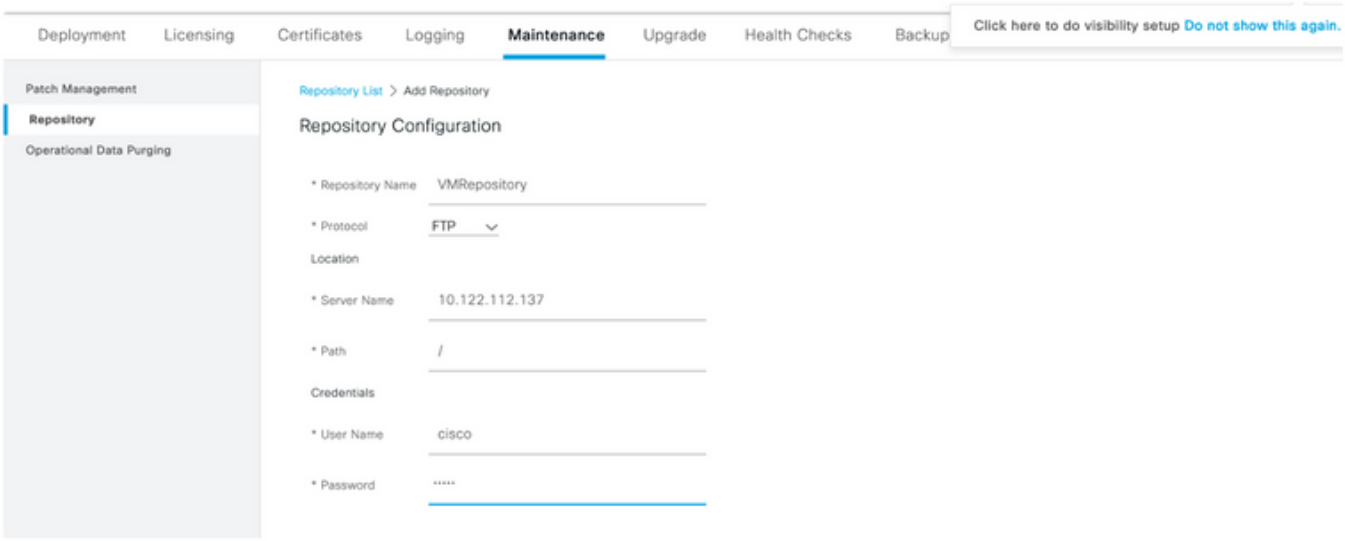
Passaggio 15. In Set di comandi selezionare Consenti tutti i set di comandi creati nel passaggio 7, quindi selezionare **Salva**

Ripetere i passaggi 14 e 15 per il gruppo Oper CSM



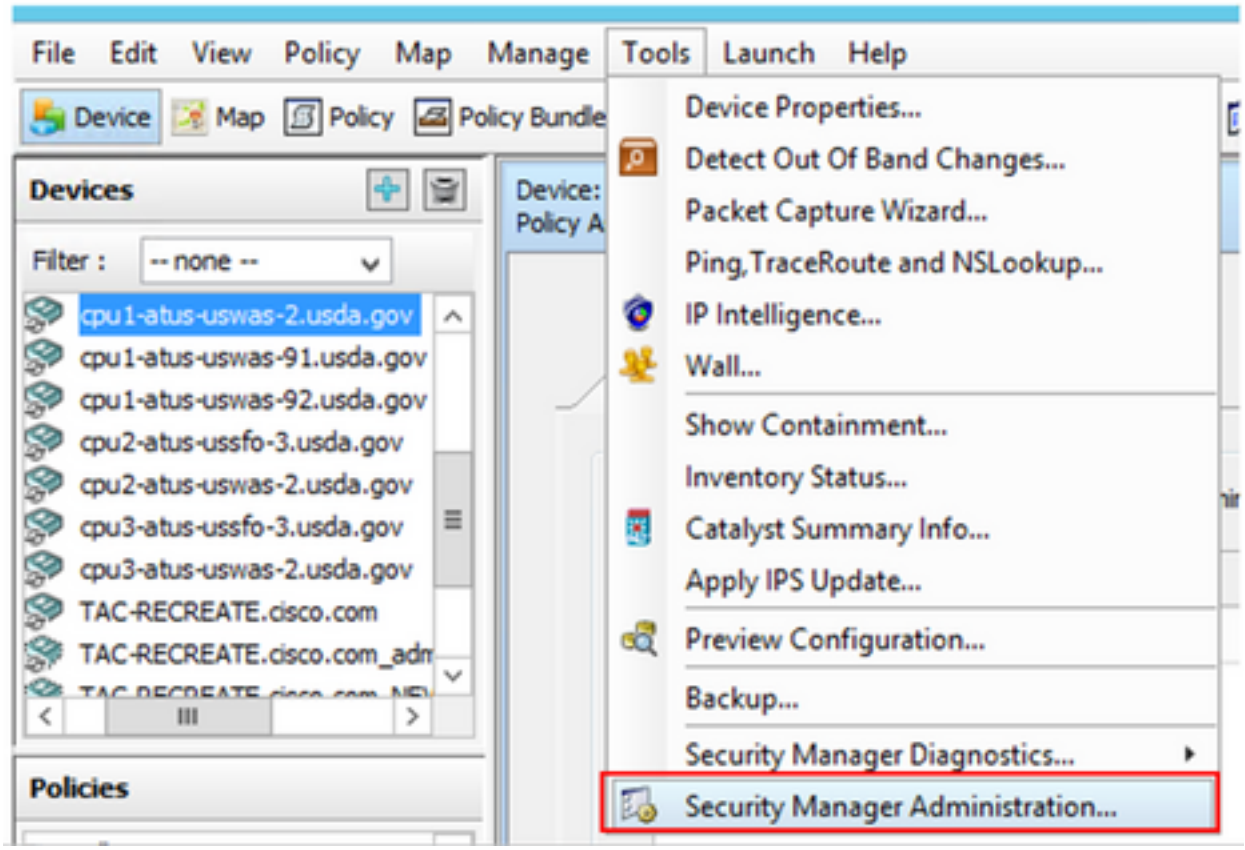
Passaggio 16 (facoltativo). Selezionare l'icona a tre righe nell'angolo superiore sinistro e Selezionare **Amministrazione>Sistema>Manutenzione>Repository**, selezionare **+Aggiungi** per aggiungere un repository utilizzato per memorizzare il file di dump TCP per la risoluzione dei problemi.

Passaggio 17 (facoltativo). Definire un nome repository, un protocollo, un nome server, un percorso e le credenziali. Al termine, selezionare **Invia**.

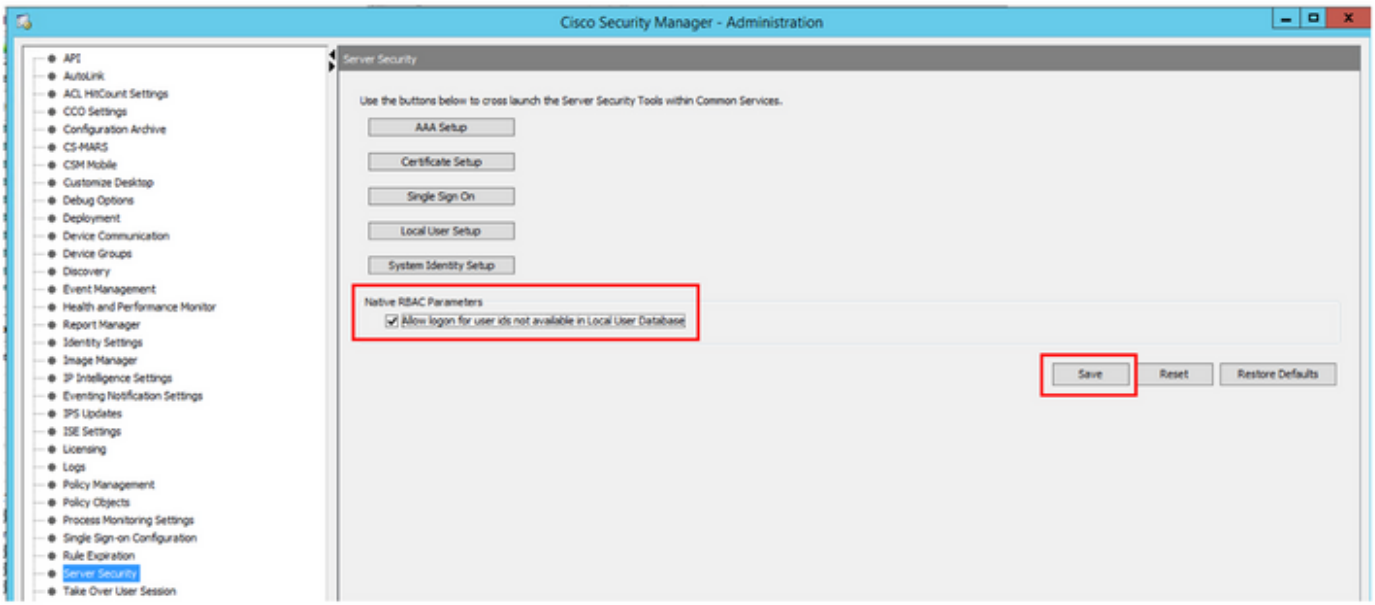


Configurazione CSM

Passaggio 1. Accedere all'applicazione client Cisco Security Manager con l'account admin locale. Dal menu passare a **Strumenti > Amministrazione di Security Manager**



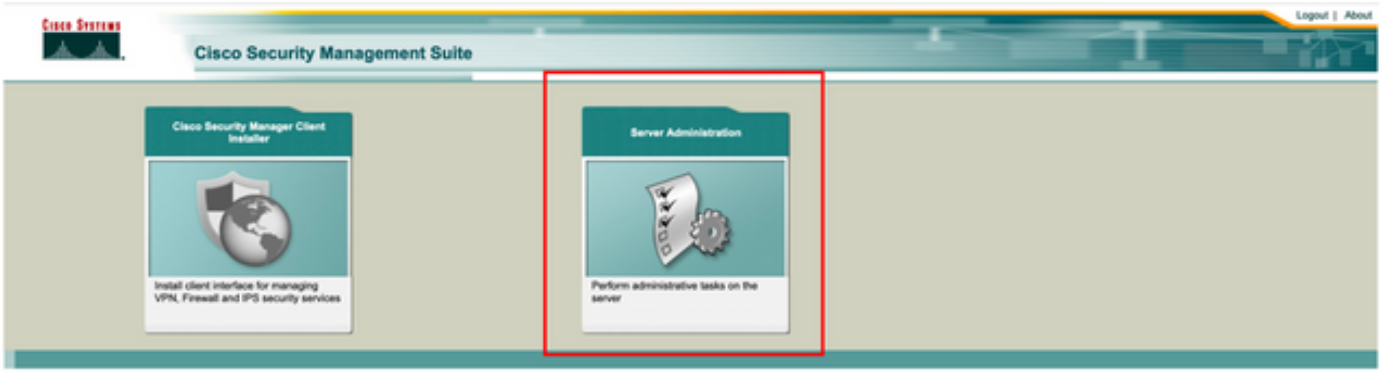
Passaggio 2. Selezionare la casella in **Parametri RBAC nativo.** Selezionare **Salva** e **chiudi**



Passaggio 3. Dal menu selezionare **File > Sottometti. File > Invia (Submit).**

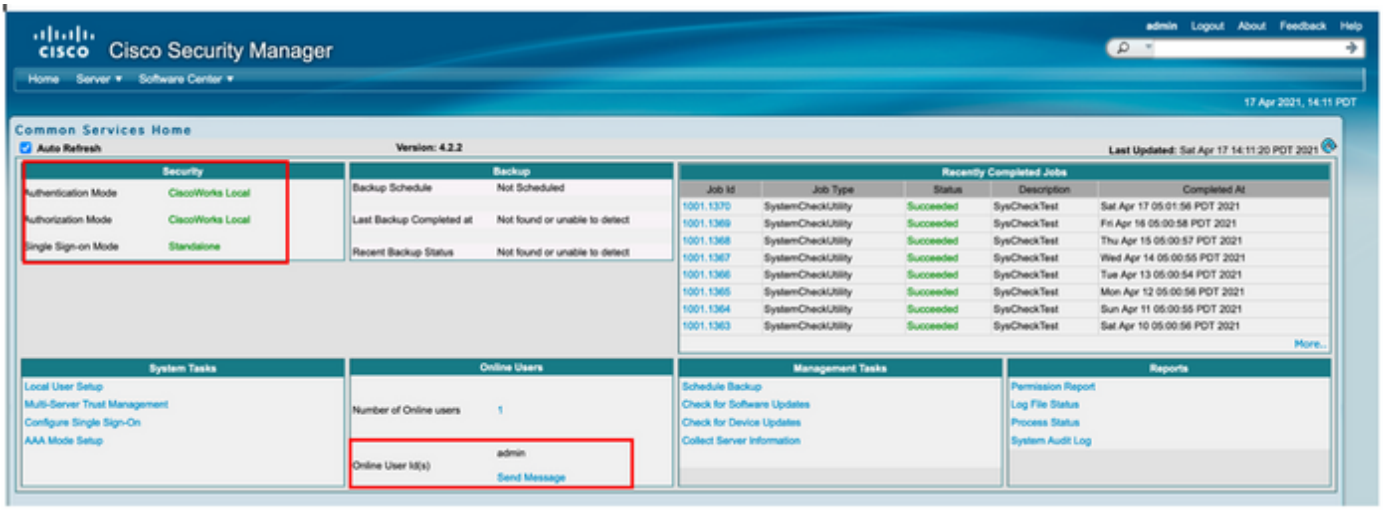
> **Nota:** Tutte le modifiche devono essere salvate e, in caso di modifiche alla configurazione, devono essere inviate e distribuite.

Passaggio 4. Passare all'interfaccia utente di gestione CSM, digitare https://<enter_CSM_IP_Address e selezionare **Amministrazione server.**



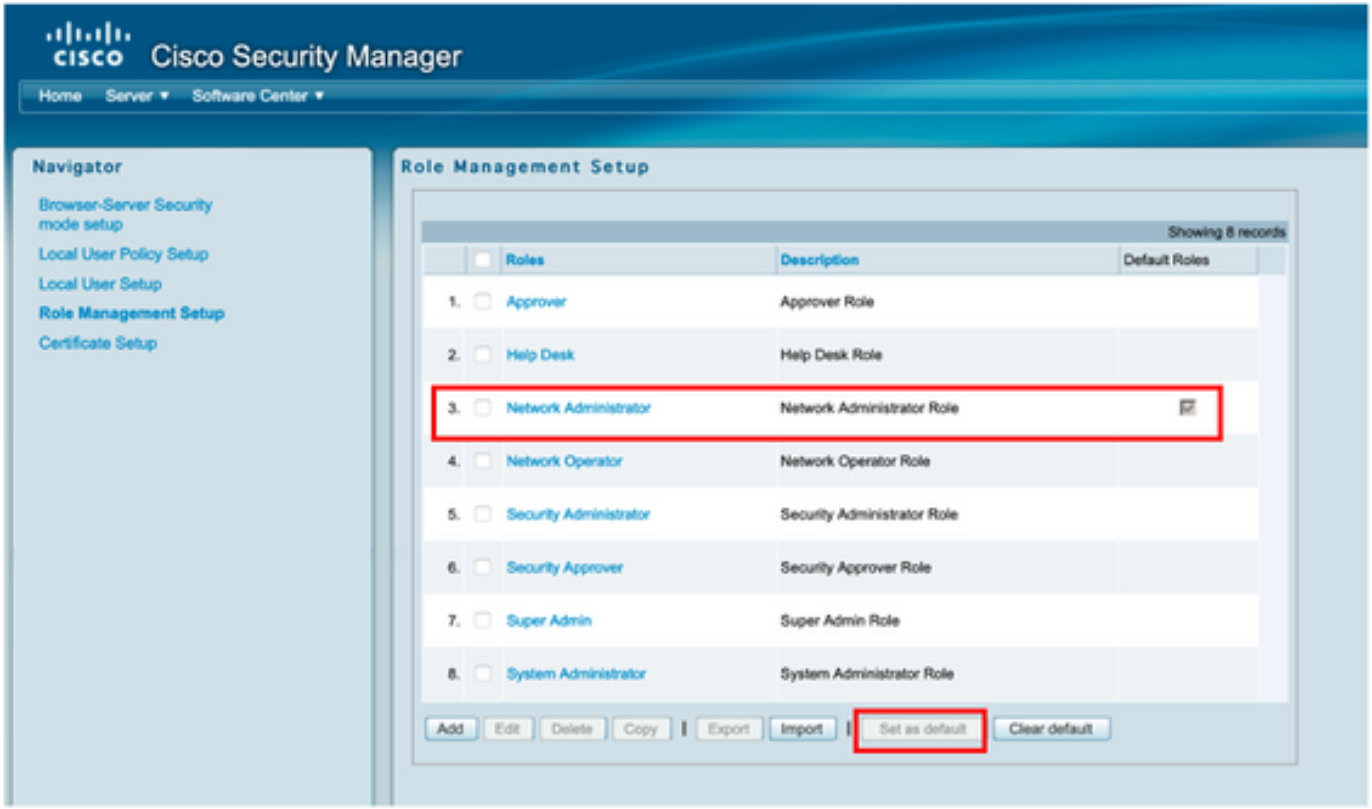
Nota: I passaggi da 4 a 7 mostrano la procedura per definire il ruolo predefinito per tutti gli amministratori che non sono definiti su ISE. Questi passaggi sono facoltativi.

Passaggio 5. Verificare che la modalità di autenticazione sia impostata su **CiscoWorks Local** e **Online** userID è l'account amministratore locale creato su CSM.



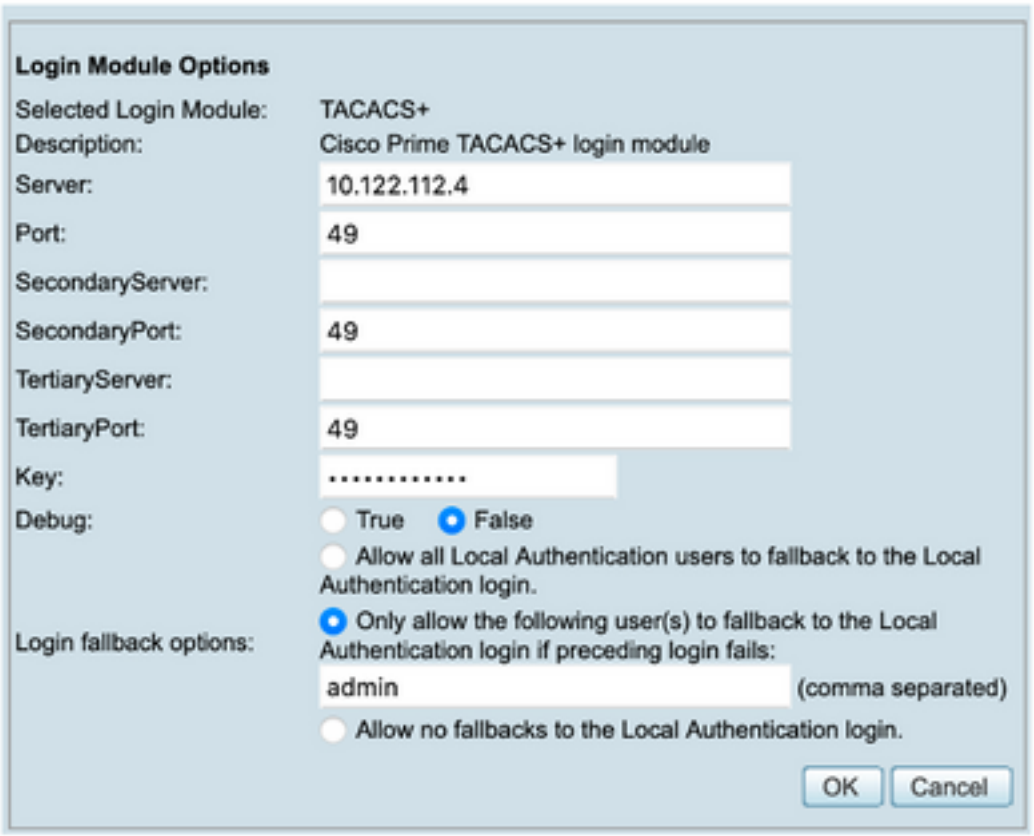
Passaggio 6. Passare a **Server** e selezionare **Gestione server singolo**

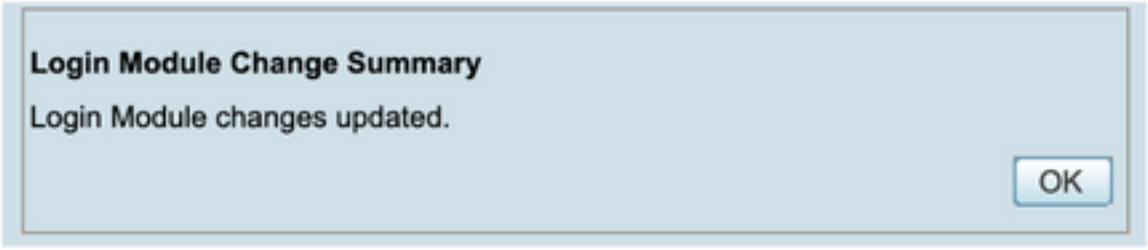
Passaggio 7. Selezionare Impostazione gestione ruoli e selezionare il privilegio predefinito che tutti gli utenti amministratori ricevono al momento dell'autenticazione. Nell'esempio viene utilizzato Amministratore di rete. Una volta selezionato, selezionare **Imposta come predefinito.**



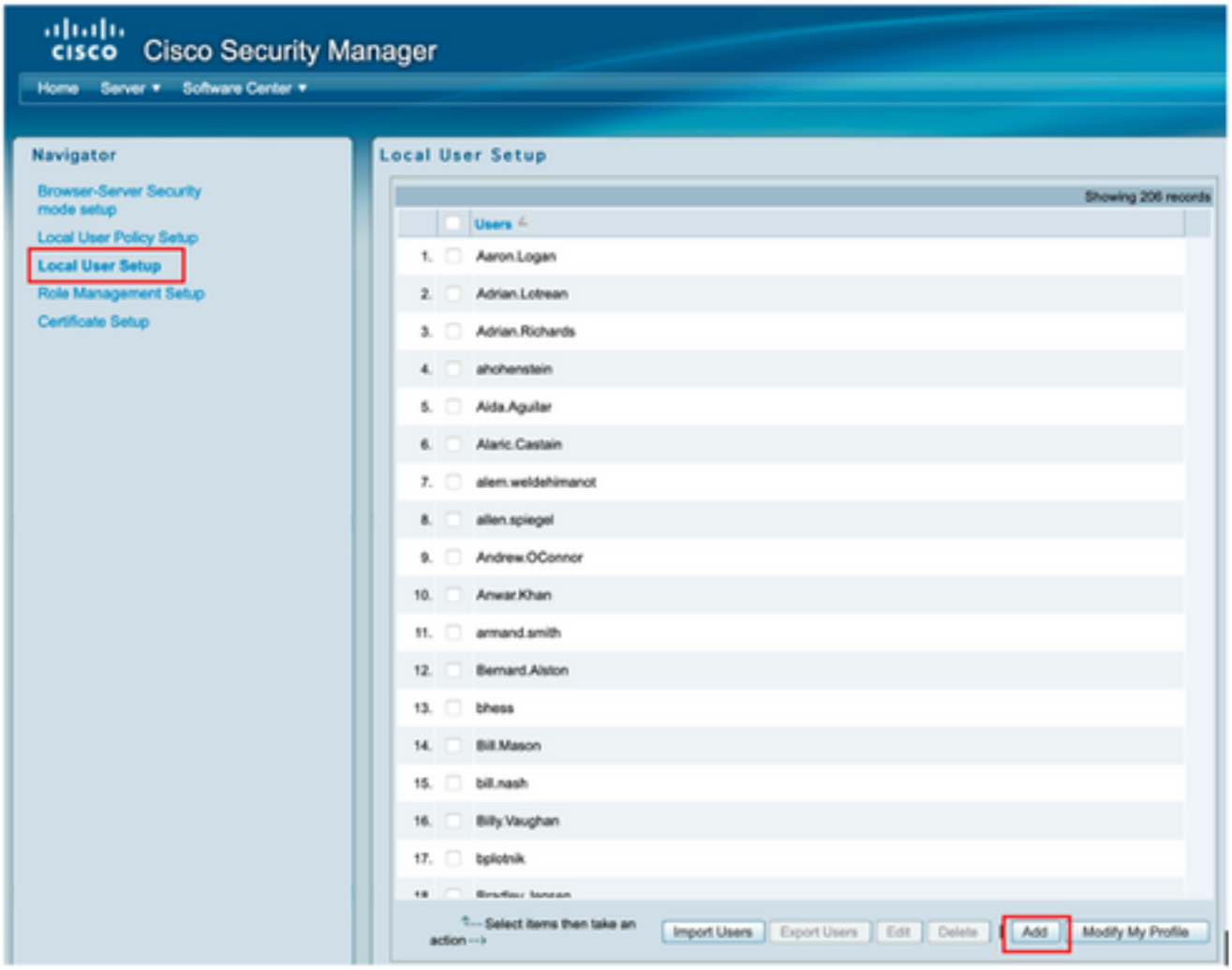
Passaggio 8. Selezionare **Server>Ruolo di installazione della modalità AAA**, quindi selezionare l'opzione **TACACS+** e infine selezionare **change** per aggiungere informazioni ISE.

Passaggio 9. Definire l'indirizzo IP e la chiave ISE. Facoltativamente, è possibile selezionare l'opzione che consente a tutti gli utenti con autenticazione locale o a un solo utente se l'accesso non riesce**.** Per questo esempio, come metodo di fallback è consentito l'utilizzo dell'opzione Solo utente amministratore. Selezionare **OK** per salvare le modifiche.

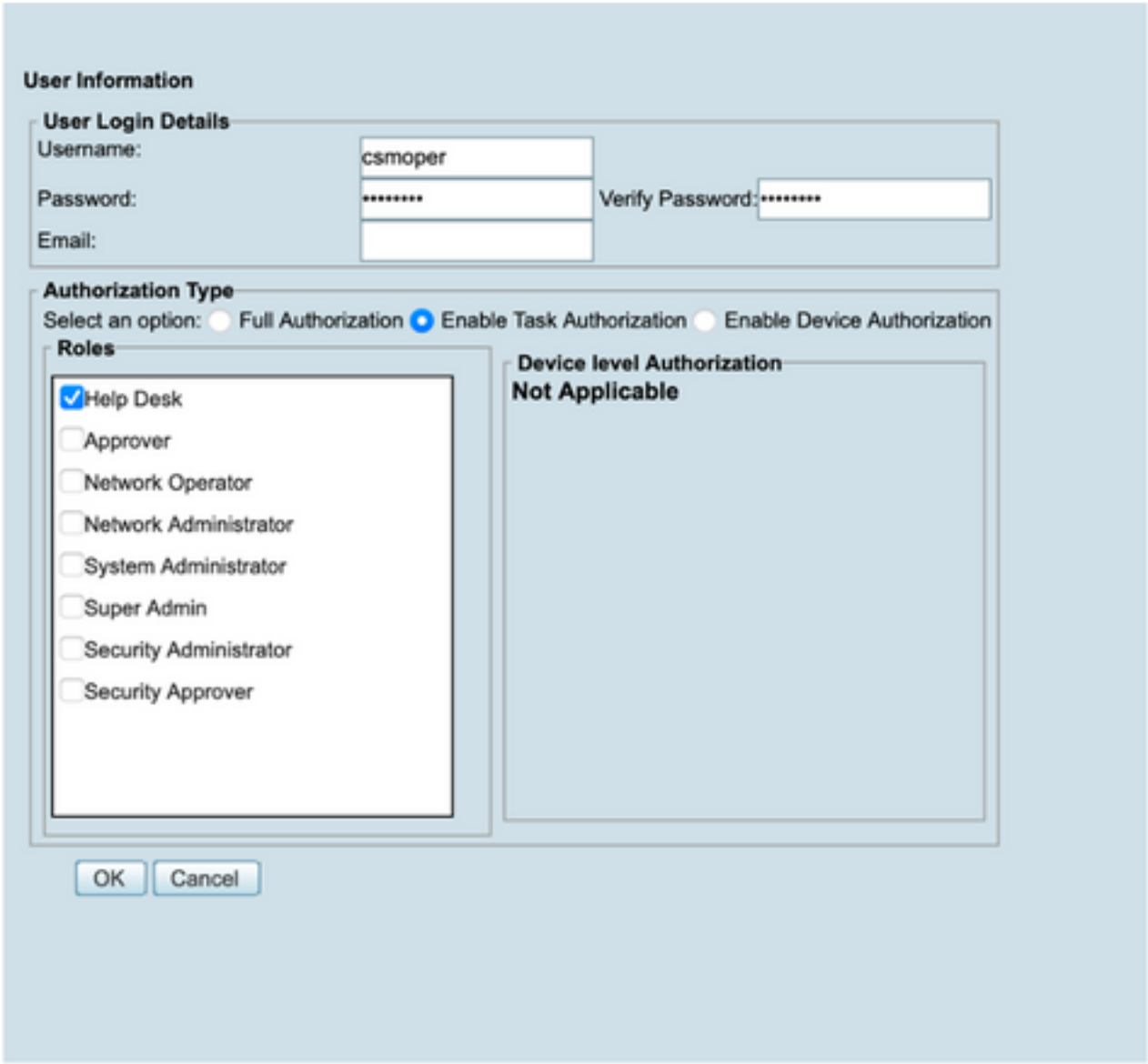




Passaggio 10. Selezionare **Server> Gestione server singolo**, quindi selezionare **Configurazione utente locale** e selezionare **Aggiungi.**



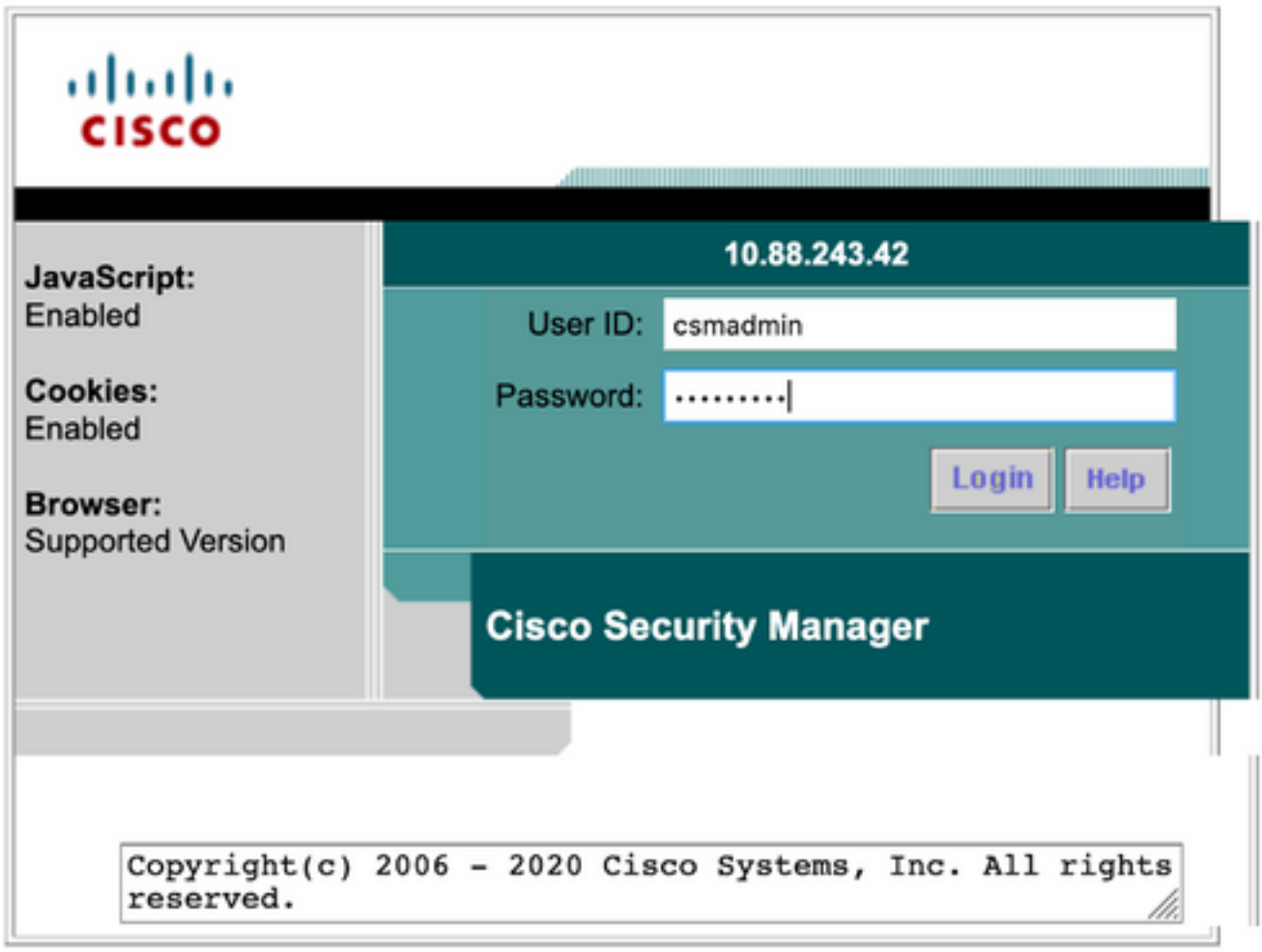
Passaggio 11. Definire lo stesso nome utente e la stessa password creati per ISE nel passaggio 5 nella sezione Configurazione ISE. In questo esempio vengono utilizzati i **ruoli di autorizzazione delle attività csmoper** e **Help Desk**. Per salvare l'utente amministratore, selezionare **OK**.



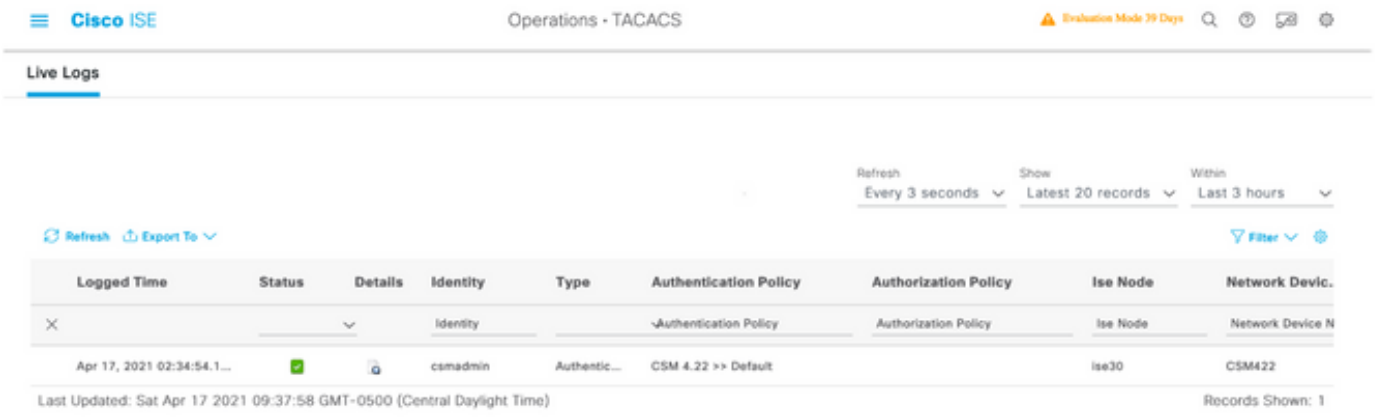
Verifica

Interfaccia utente client di Cisco Security Manager

Passaggio 1. Aprire una nuova finestra del browser e digitare https://<enter_CSM_IP_Address, utilizzare il nome utente e la password **csmadmin** creati nel passaggio 5 della sezione di configurazione ISE.



Sui log live ISE TACACS è possibile verificare l'esito del log nel tentativo

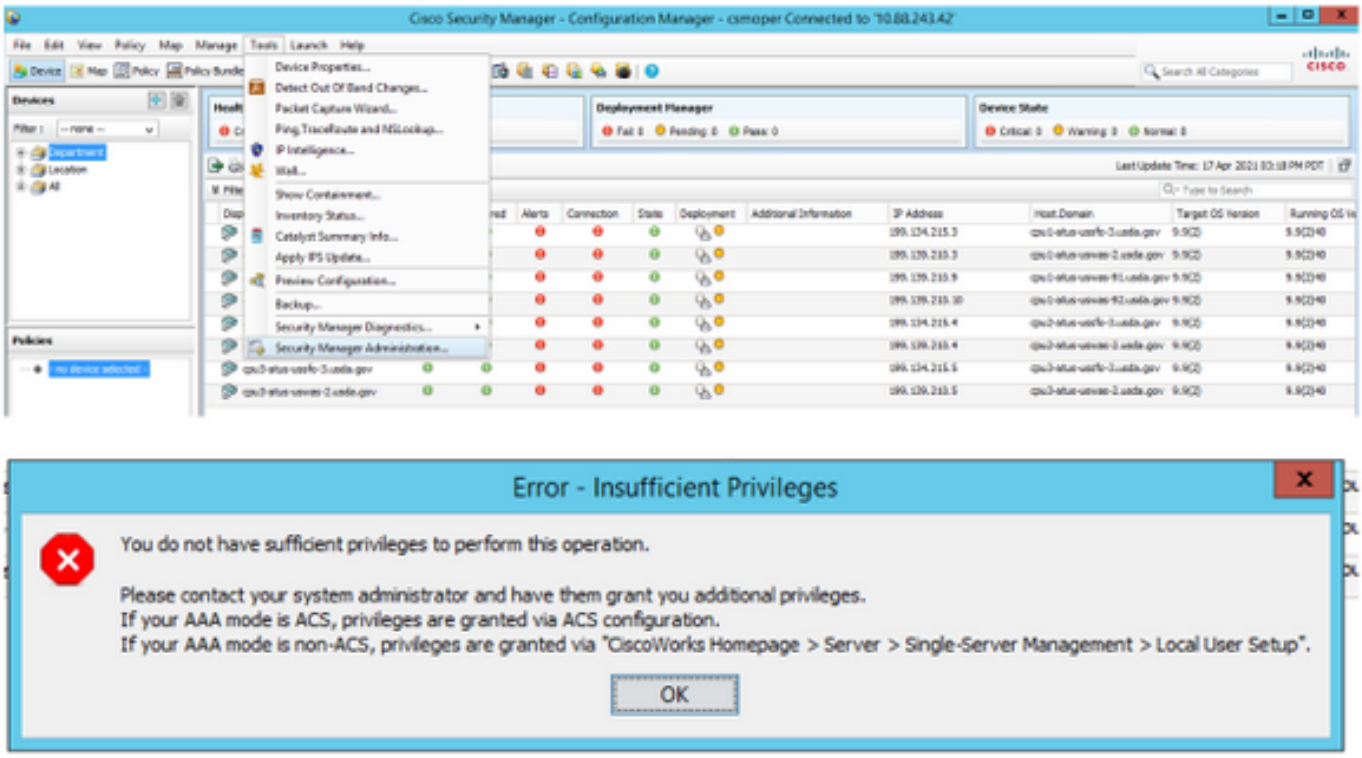


Applicazione client Cisco Security Manager

Passaggio 1. Accedere all'applicazione client Cisco Security Manager con l'account di amministratore dell'helpdesk.

Sui log live ISE TACACS è possibile verificare l'esito del log nel tentativo

Passaggio 2. Dal menu dell'applicazione client CSM selezionare **Strumenti > Amministrazione Security Manager**, deve essere visualizzato un messaggio di errore che indica la mancanza di privilegi.



Passaggio 3. Ripetere i passaggi da 1 a 3 con l'account **csmadmin** per verificare che all'utente siano state fornite le autorizzazioni appropriate.

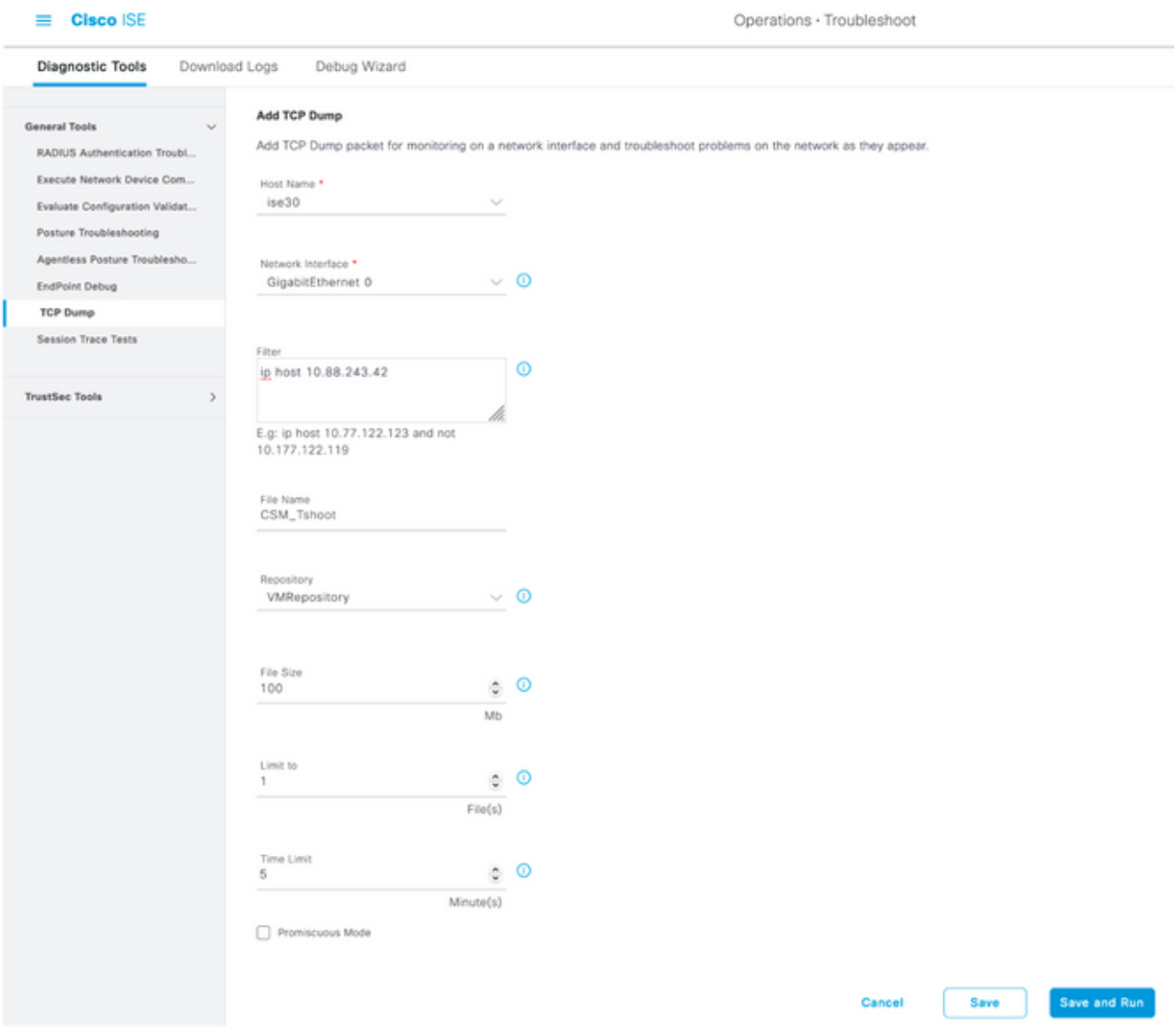
Risoluzione dei problemi

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

Convalida della comunicazione con lo strumento TCP Dump su ISE

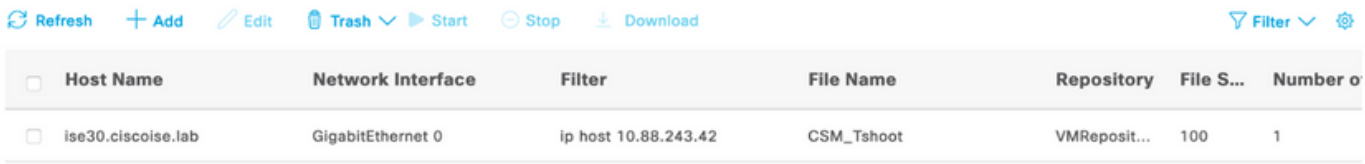
Passaggio 1. Accedere ad ISE e selezionare l'icona con le tre righe nell'angolo superiore sinistro, quindi selezionare **Operations>Troubleshoot>Diagnostic Tools.**

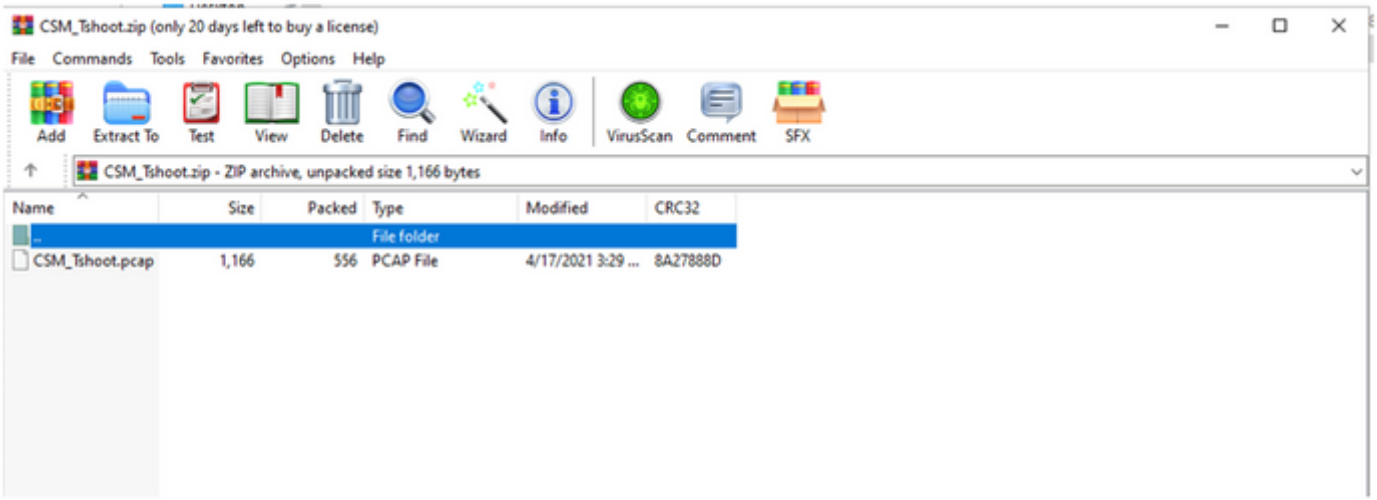
Passaggio 2. In **Strumenti generali** selezionare **TCP Dump,** quindi selezionare **Add+.** Selezionare Nome host, Nome file interfaccia di rete, Repository e, facoltativamente, un filtro per raccogliere solo il flusso di comunicazione dell'indirizzo IP del CSM. Selezionare **Salva ed esegui**



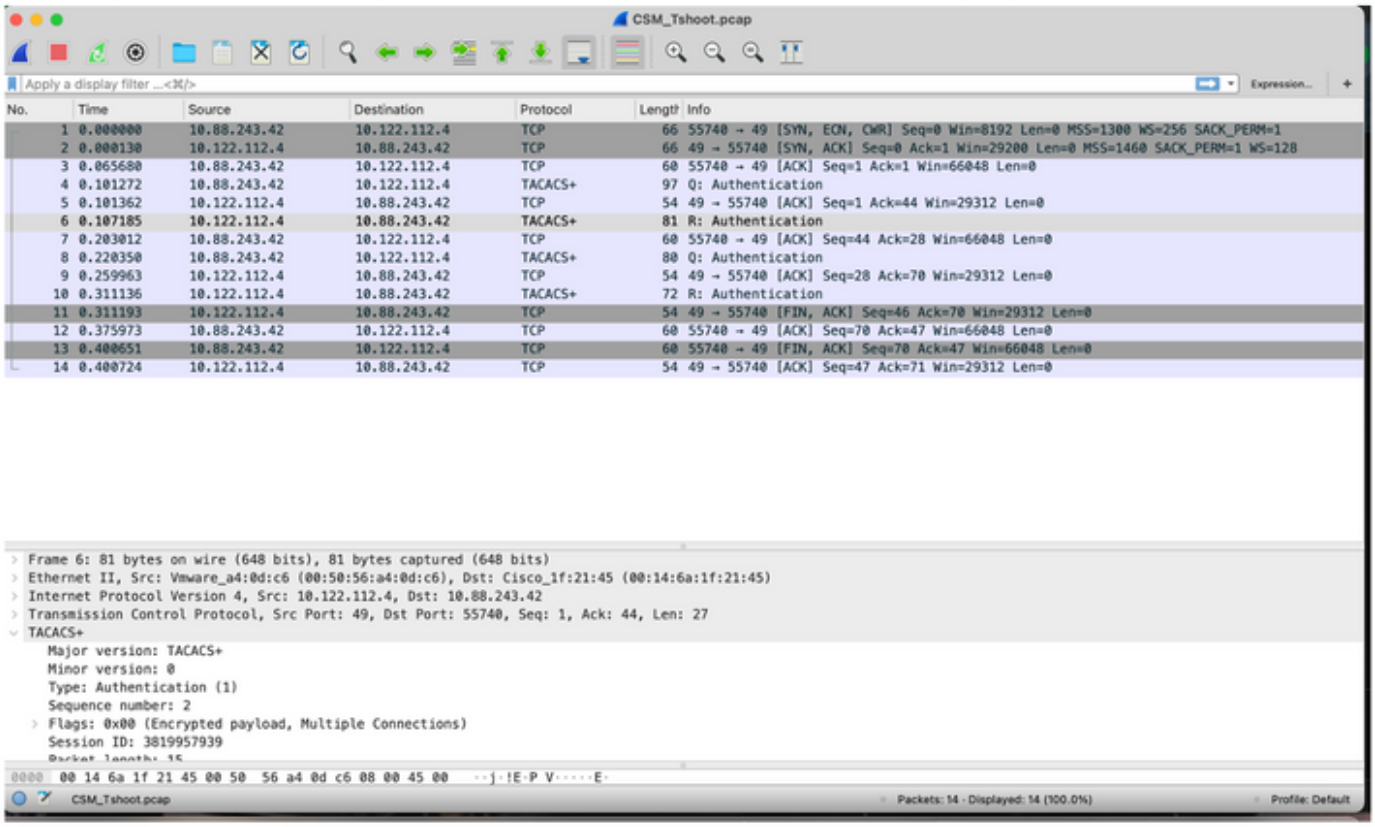
Passaggio 3. Accedere all'applicazione client CSM o all'interfaccia utente client e digitare le credenziali dell'amministratore.

Passaggio 4. Su ISE, selezionare **il** pulsante **Stop** e verificare che il file pcap sia stato inviato al repository definito.





Passaggio 5. Aprire il file pcap per verificare la corretta comunicazione tra CSM e ISE.



Se nel file pcap non sono visualizzate voci, verificare quanto segue:

1. Il servizio Amministrazione dispositivi è abilitato sul nodo ISE
2. L'indirizzo IP ISE destro è stato aggiunto alla configurazione CSM
3. Se il firewall si trova nella parte centrale, verificare che la porta 49 (TACACS) sia autorizzata.