Configurazione dell'autenticazione esterna SWA con ISE come server RADIUS

Sommario

Introduzione

In questo documento viene descritto come configurare l'autenticazione esterna su Secure Web Access (SWA) con Cisco ISE come server RADIUS.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di Cisco Secure Web Appliance.
- Conoscenza della configurazione dei criteri di autenticazione e autorizzazione su ISE.
- Conoscenze base di RADIUS.

Cisco consiglia inoltre di:

- Accesso amministrativo a SWA e ISE.
- Versioni compatibili WSA e ISE.

Componenti usati

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

- SWA 14.0.2-012
- ISE 3.0.0

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

Quando si abilita l'autenticazione esterna per gli utenti amministrativi del file SWA, il dispositivo verifica le credenziali dell'utente con un server LDAP (Lightweight Directory Access Protocol) o RADIUS come specificato nella configurazione dell'autenticazione esterna.

Topologia della rete

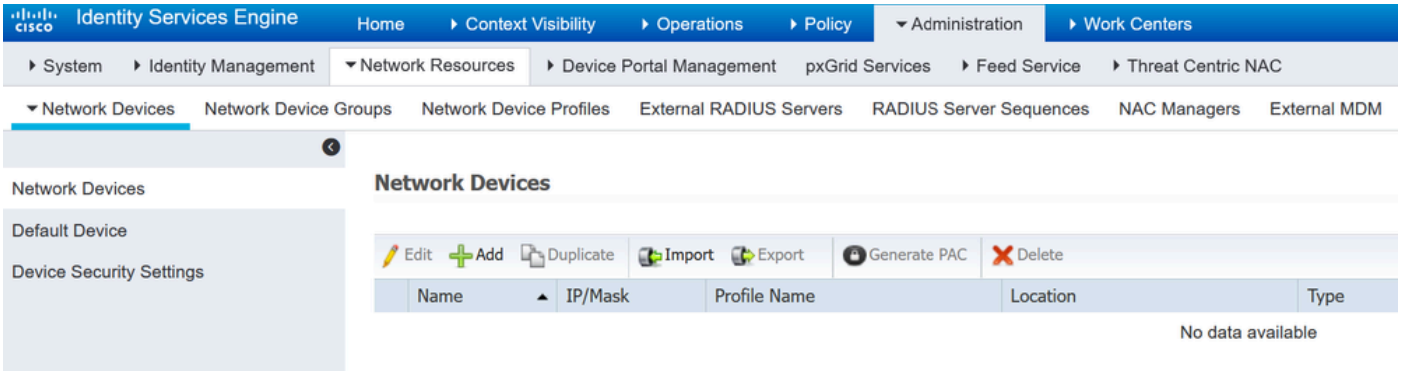
Esempio di topologia di rete

Gli utenti con privilegi amministrativi accedono all'interfaccia SWA sulla porta 443 con le proprie credenziali. SWA verifica le credenziali con il server RADIUS.

Configurazione

Configurazione di ISE

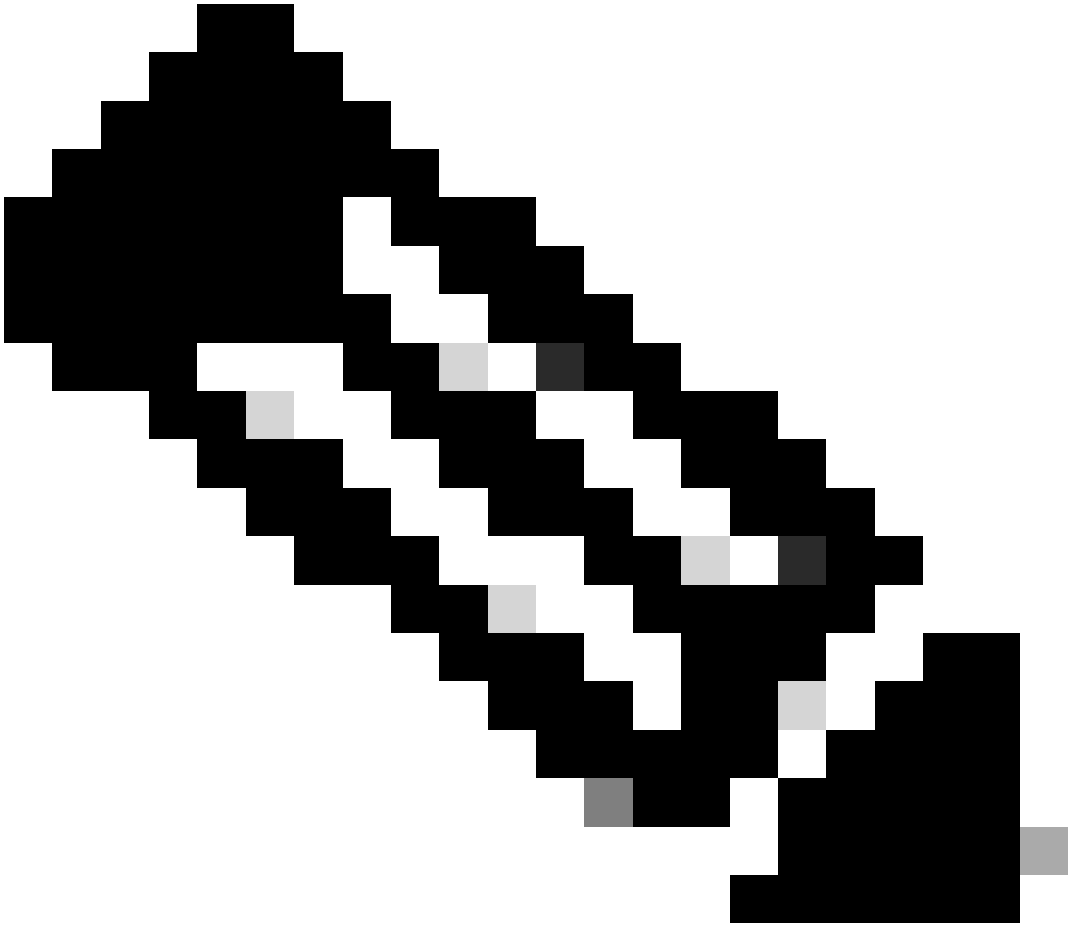
Passaggio 1. Aggiungere un nuovo dispositivo di rete. Selezionare Amministrazione > Risorse di rete > Dispositivi di rete > +Aggiungi.



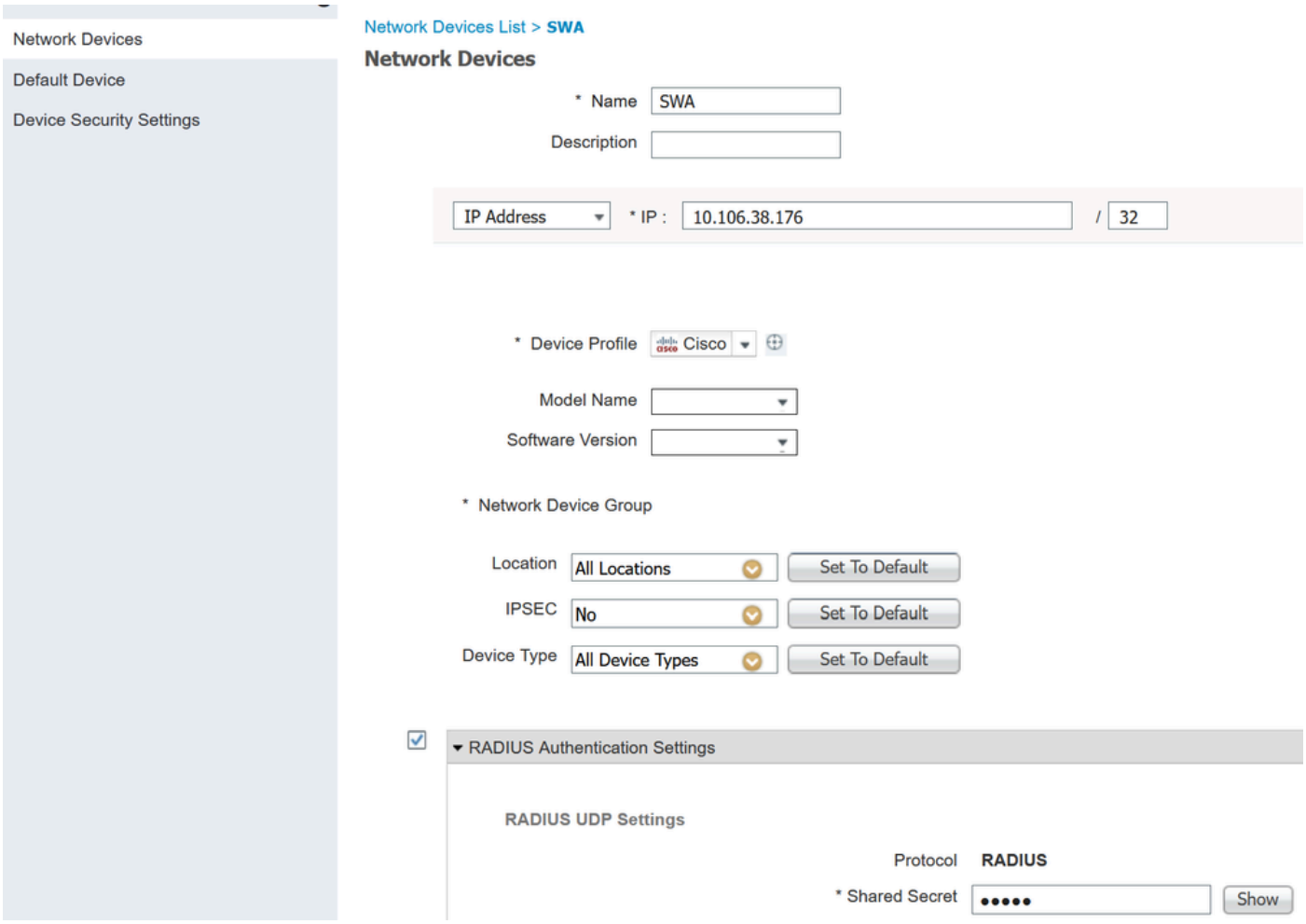
Aggiungi SWA come dispositivo di rete in ISE

Passaggio 2. Assegnate un nome all'oggetto dispositivo di rete e inserite l'indirizzo IP SWA.

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

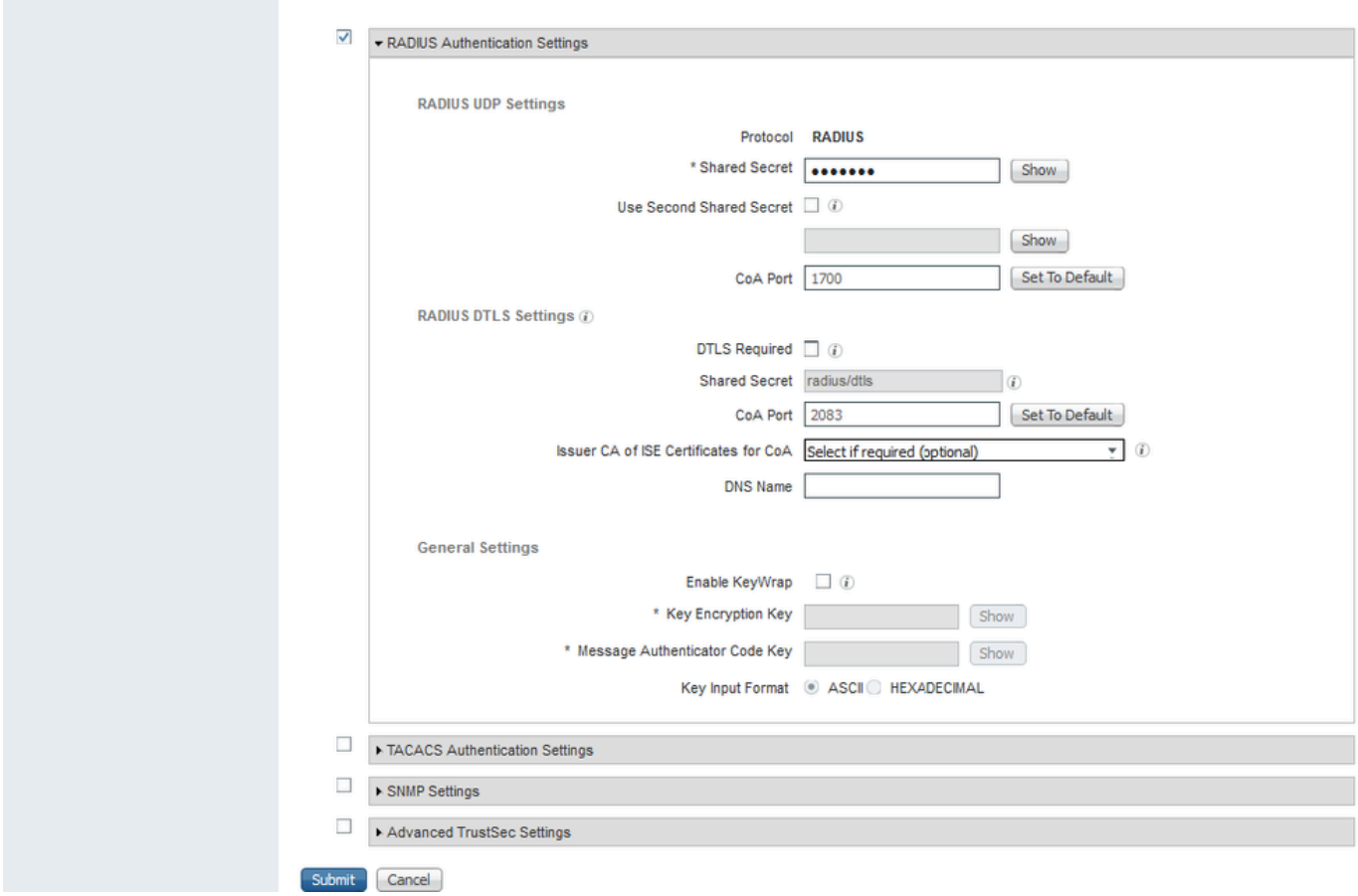


Nota: la stessa chiave deve essere utilizzata successivamente per configurare il server RADIUS in SWA.



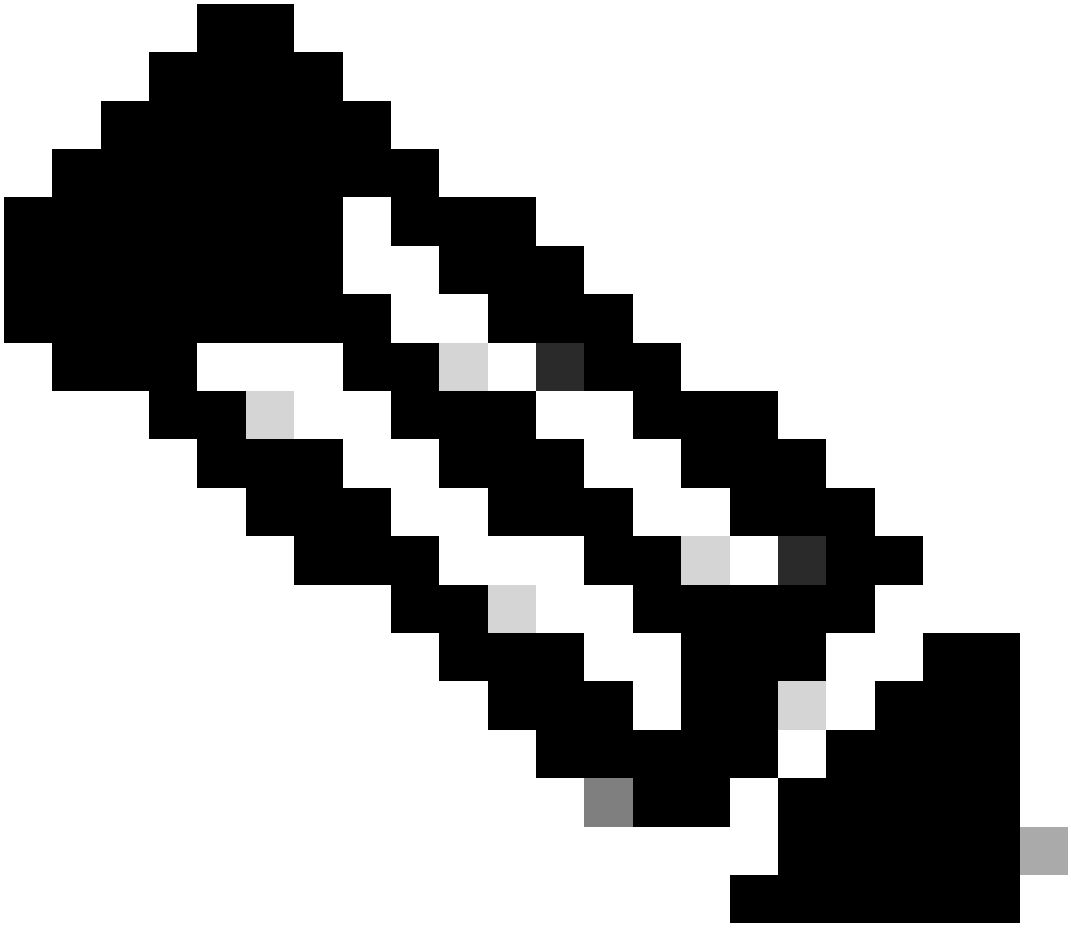
Configurazione della chiave condivisa del dispositivo di rete SWA

Passaggio 2.1. Fare clic su Invia.

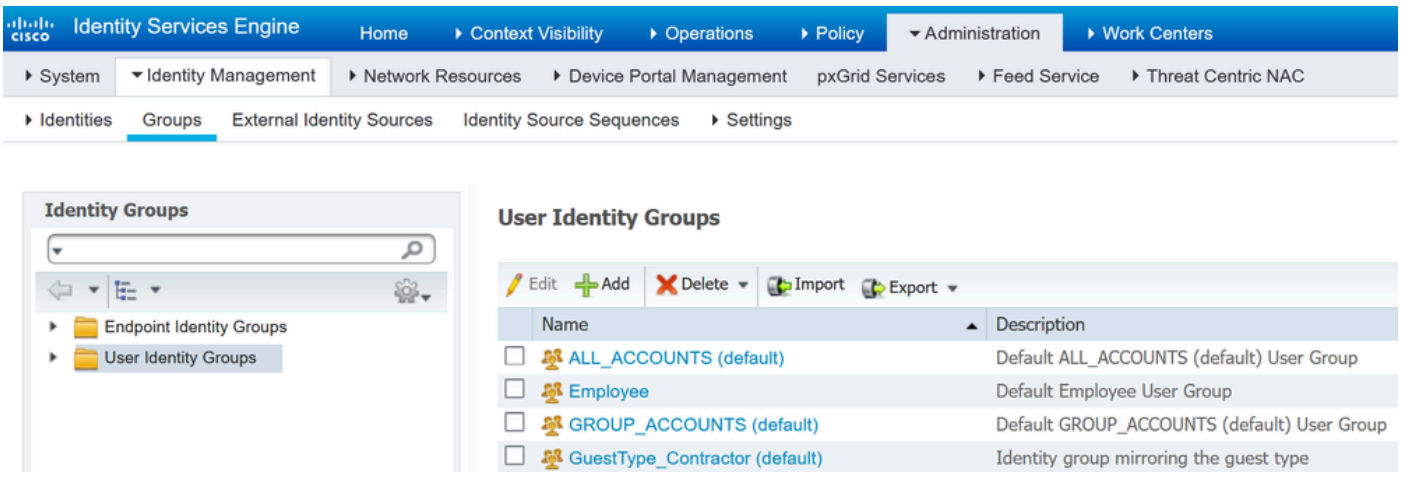


Invia configurazione dispositivo di rete

Passaggio 3. Creare i gruppi di identità utente richiesti. Passare a Amministrazione > Gestione delle identità > Gruppi > Gruppi identità utente > + Aggiungi.



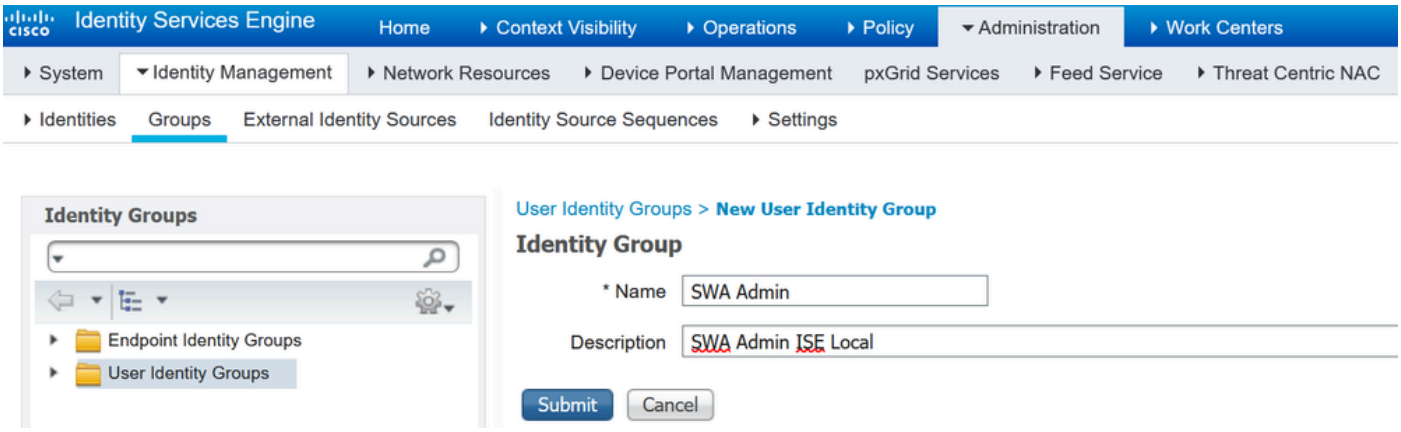
Nota: è necessario configurare gruppi di utenti diversi in modo che corrispondano a tipi di utenti diversi.



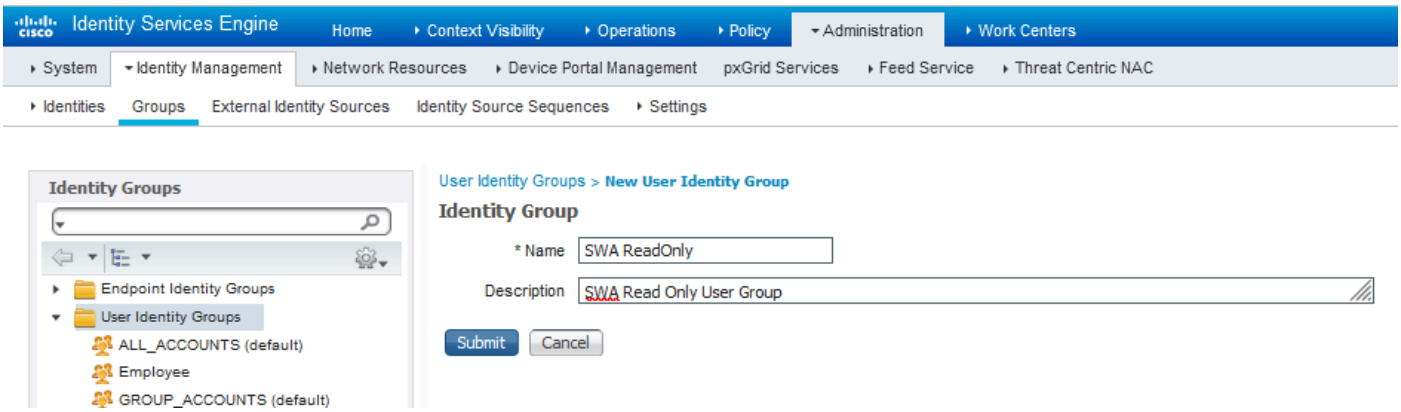
Aggiungi gruppo di identità utente

Passaggio 4. Immettere il nome del gruppo, la descrizione (facoltativa) e Invia. Ripetere questi

passaggi per ogni gruppo. In questo esempio vengono creati un gruppo per gli utenti con privilegi di amministratore e un altro gruppo per gli utenti con privilegi di sola lettura.



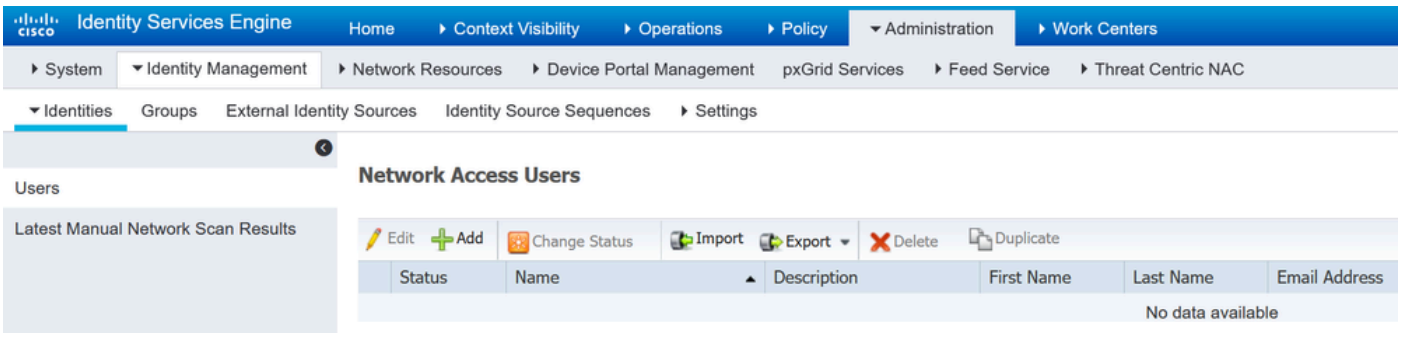
Aggiungi



gruppo di identità utenteAggiungi gruppo di identità utente per utenti SWA sola lettura

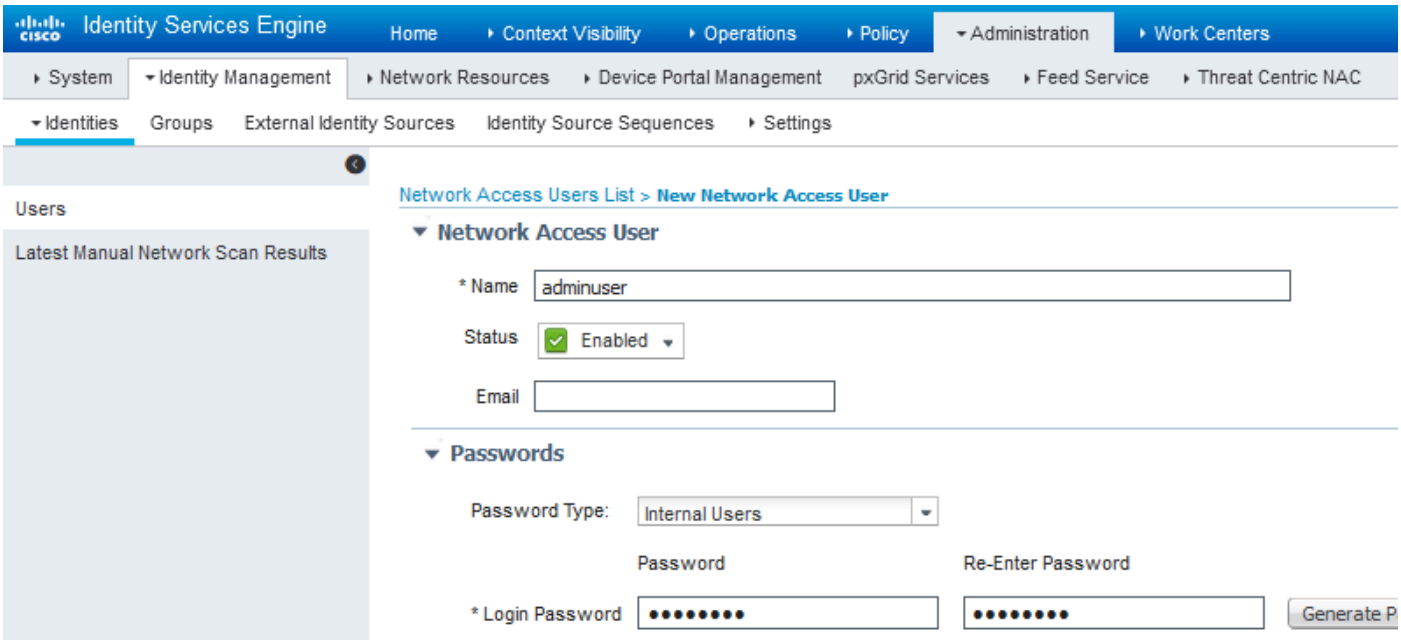
Passaggio 5. È necessario creare utenti di accesso alla rete corrispondenti al nome utente configurato in SWA.

Creare gli utenti di Accesso alla rete e aggiungerli al gruppo corrispondente. Passare a Amministrazione > Gestione delle identità > Identità > + Aggiungi.



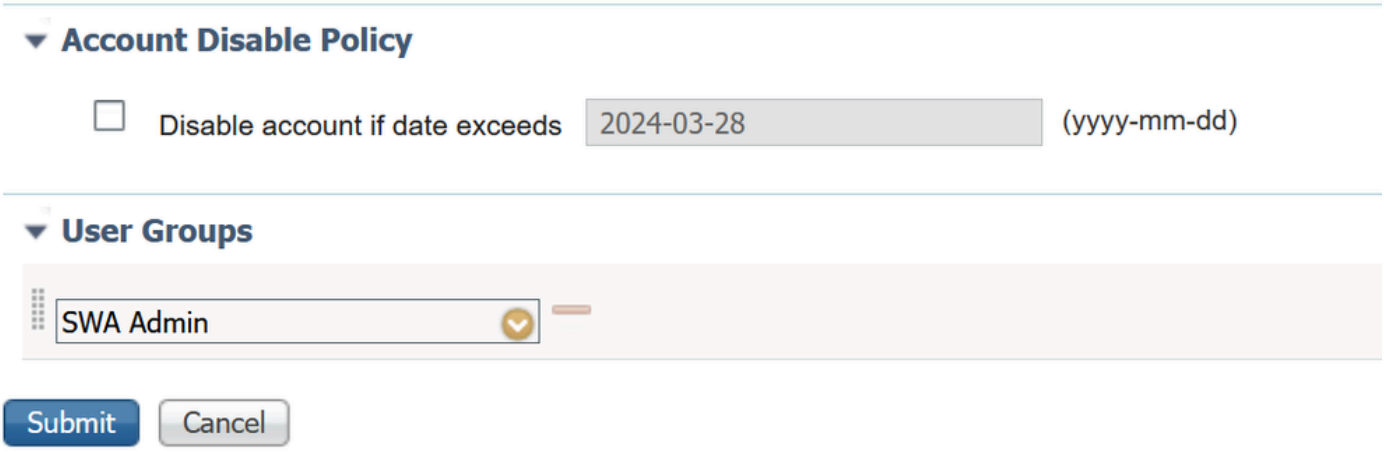
Aggiungi utenti locali in ISE

Passaggio 5.1. È necessario creare un account Utenti accesso alla rete con diritti di amministratore. Assegnare nome e password.



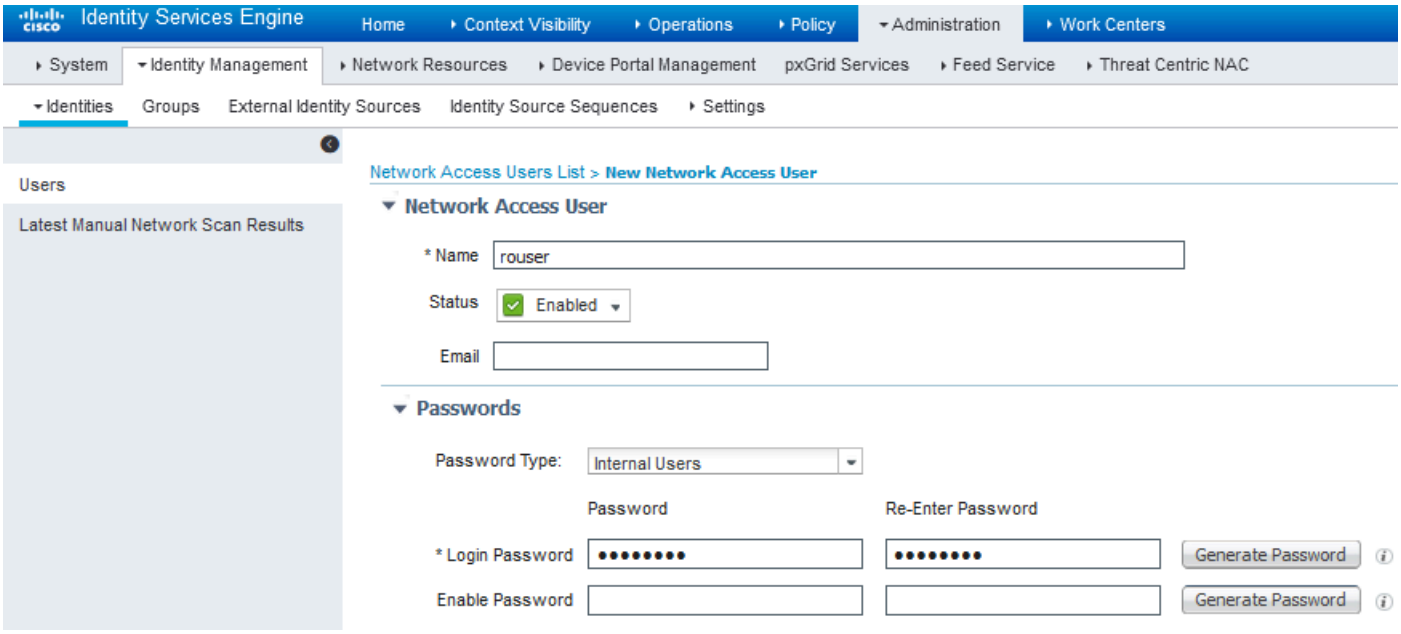
Aggiungi utente amministratore

Passaggio 5.2. Scegliere Amministratore SWA nella sezione Gruppi di utenti.



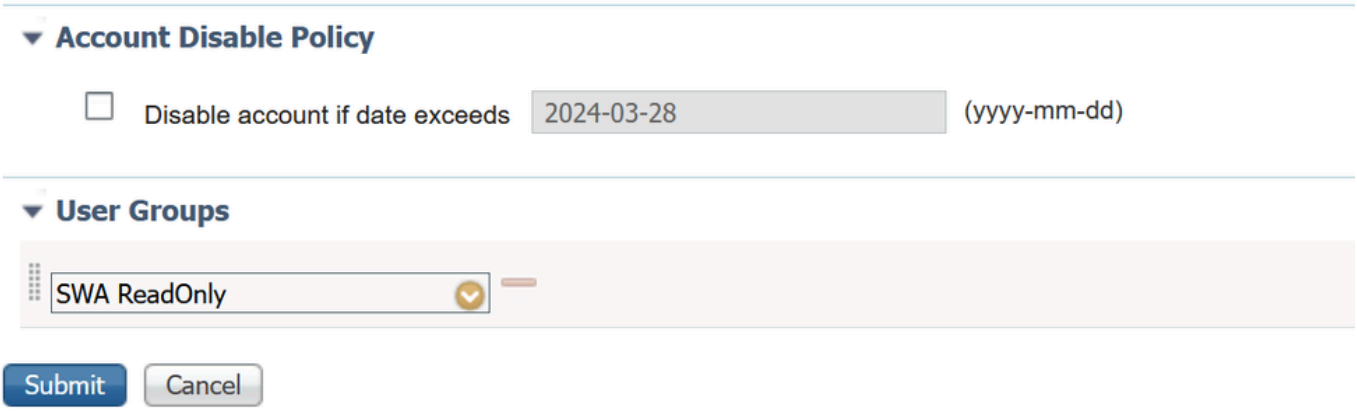
Assegna il gruppo di amministratori all'utente amministratore

Passaggio 5.3. È necessario creare un utente con diritti di sola lettura. Assegnare nome e password.



Aggiungi utente di sola lettura

Passaggio 5.4. Scegliere SWA ReadOnly nella sezione User Groups (Gruppi di utenti).

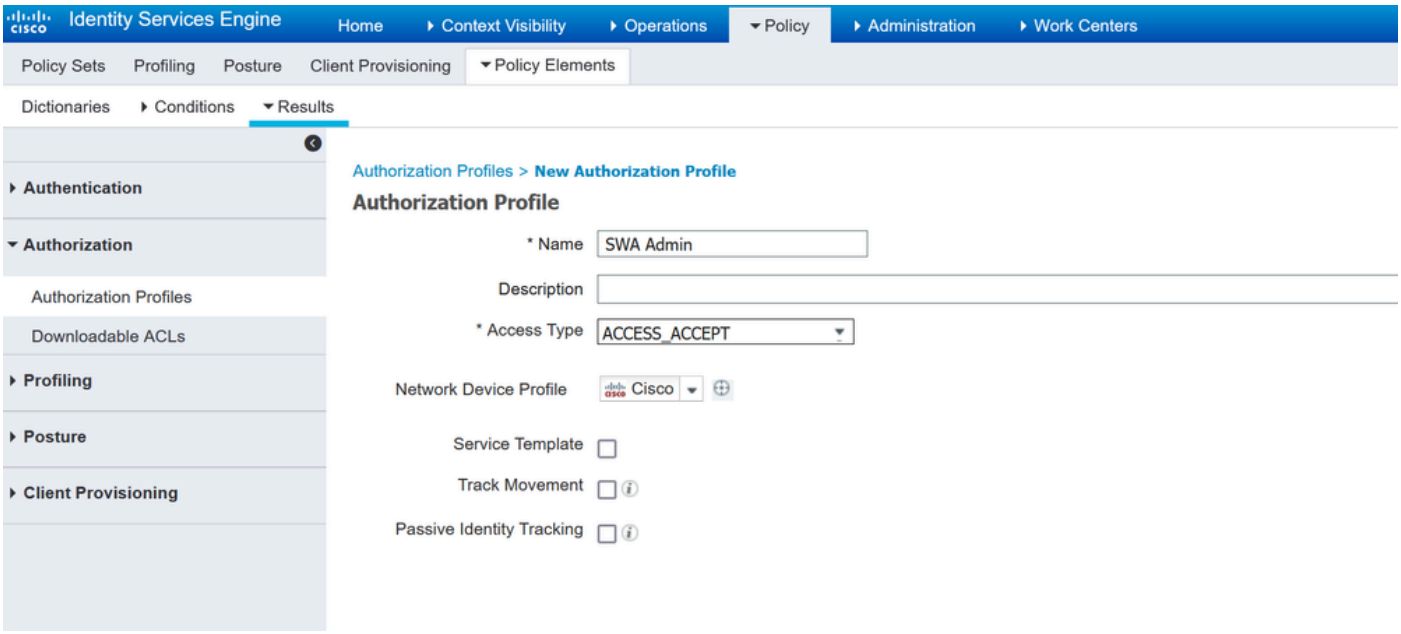


Assegna il gruppo di utenti di sola lettura all'utente di sola lettura

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

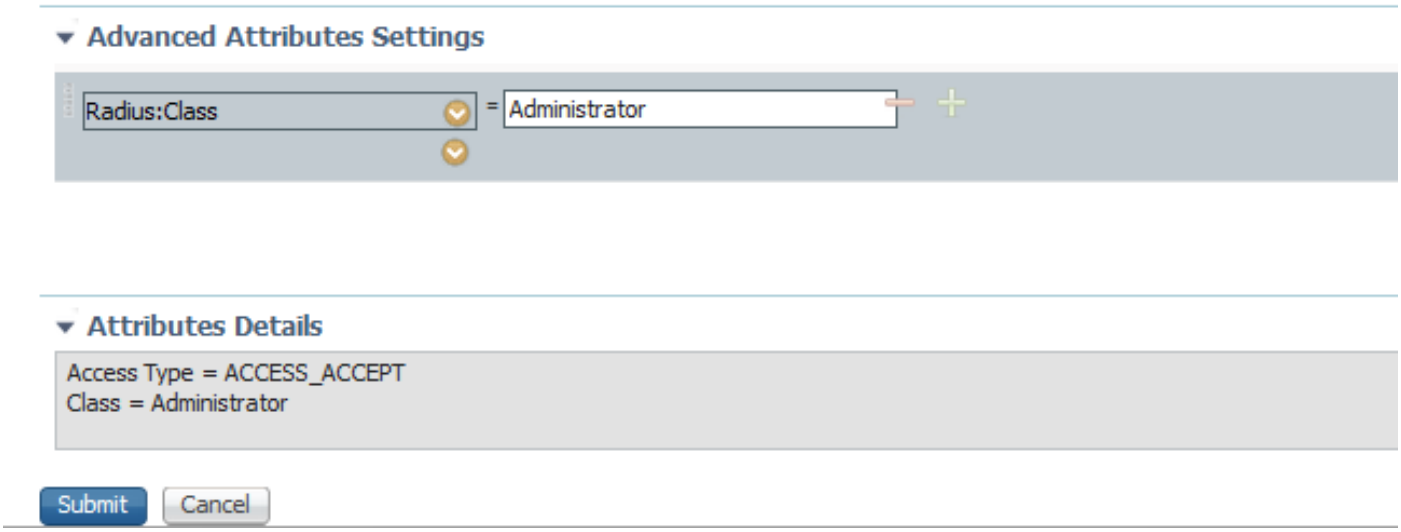
Passare a Criterio > Elementi criteri > Risultati > Autorizzazione > Profili di autorizzazione > +Aggiungi.

Assegnare un nome al profilo di autorizzazione e accertarsi che il tipo di accesso sia impostato su ACCESS_ACCEPT.



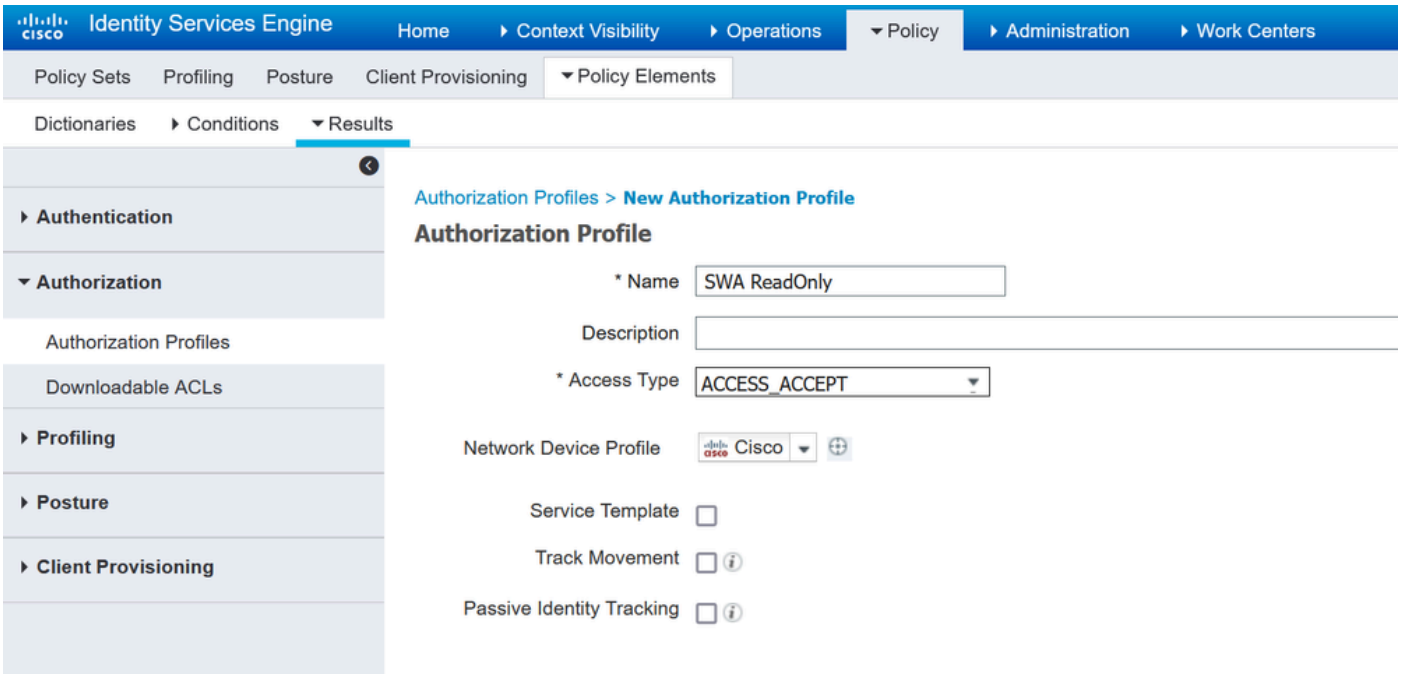
Aggiungi profilo di autorizzazione per utenti amministratori

Passaggio 6.1. In Impostazioni avanzate attributi, passare a Raggio > Classe—[25] e immettere il valore Amministratore e fare clic su Invia.



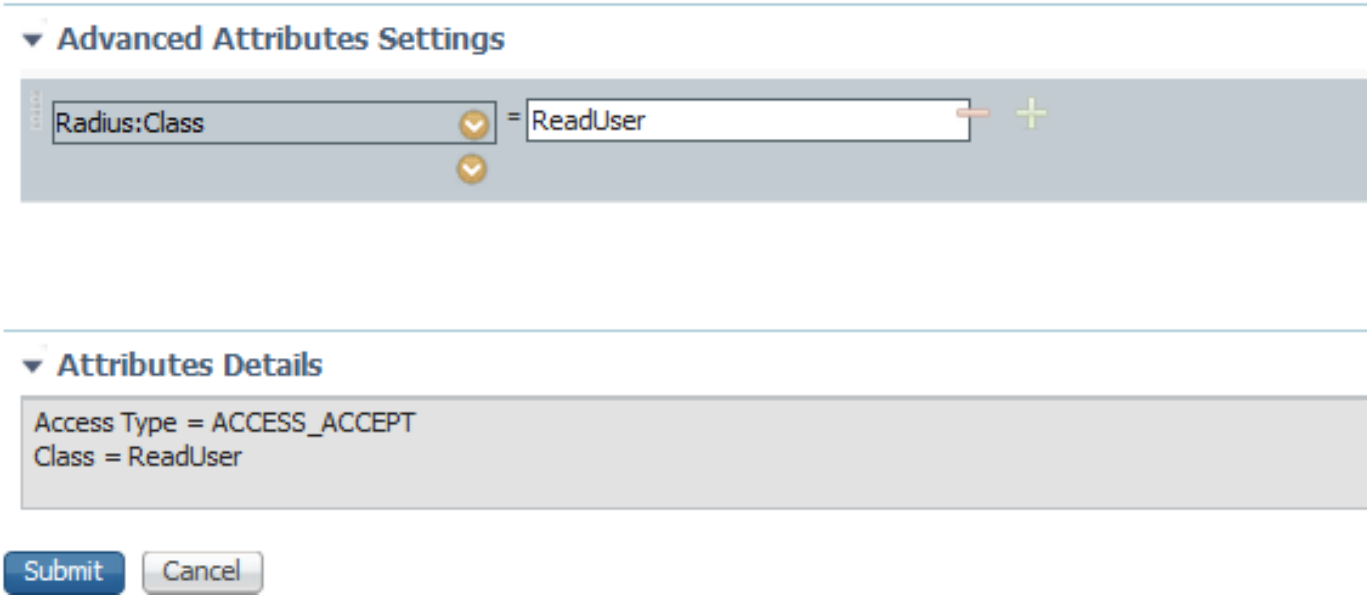
Aggiungi profilo di autorizzazione per utenti amministratori

Passaggio 7. Ripetere il passaggio 6 per creare il profilo di autorizzazione per l'utente di sola lettura.



Aggiungi profilo di autorizzazione per utenti di sola lettura

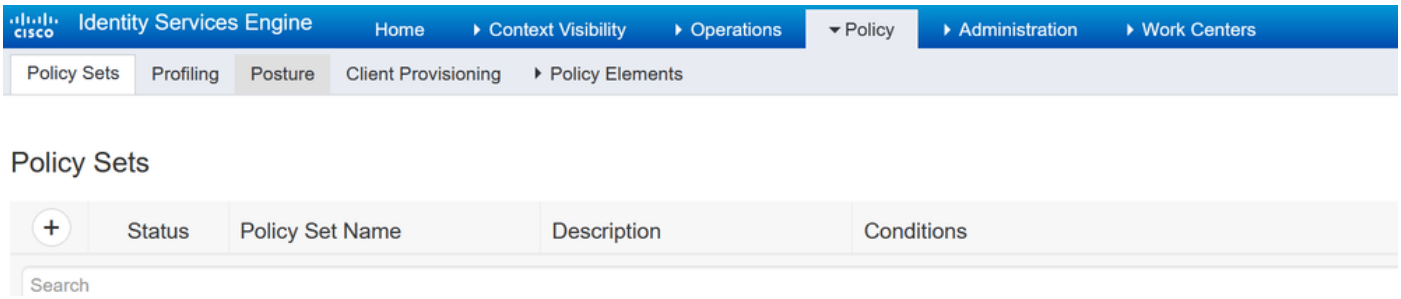
PASSAGGIO 7.1. Creare Radius:Class con il valore ReadUser invece di Administrator.



Aggiungi profilo di autorizzazione per utenti di sola lettura

Passaggio 8. Creare set di criteri corrispondenti all'indirizzo IP SWA. In questo modo è possibile impedire l'accesso ad altre periferiche con queste credenziali utente.

Passare a Policy > PolicySets e fare clic sull'icona + posizionata nell'angolo superiore sinistro.

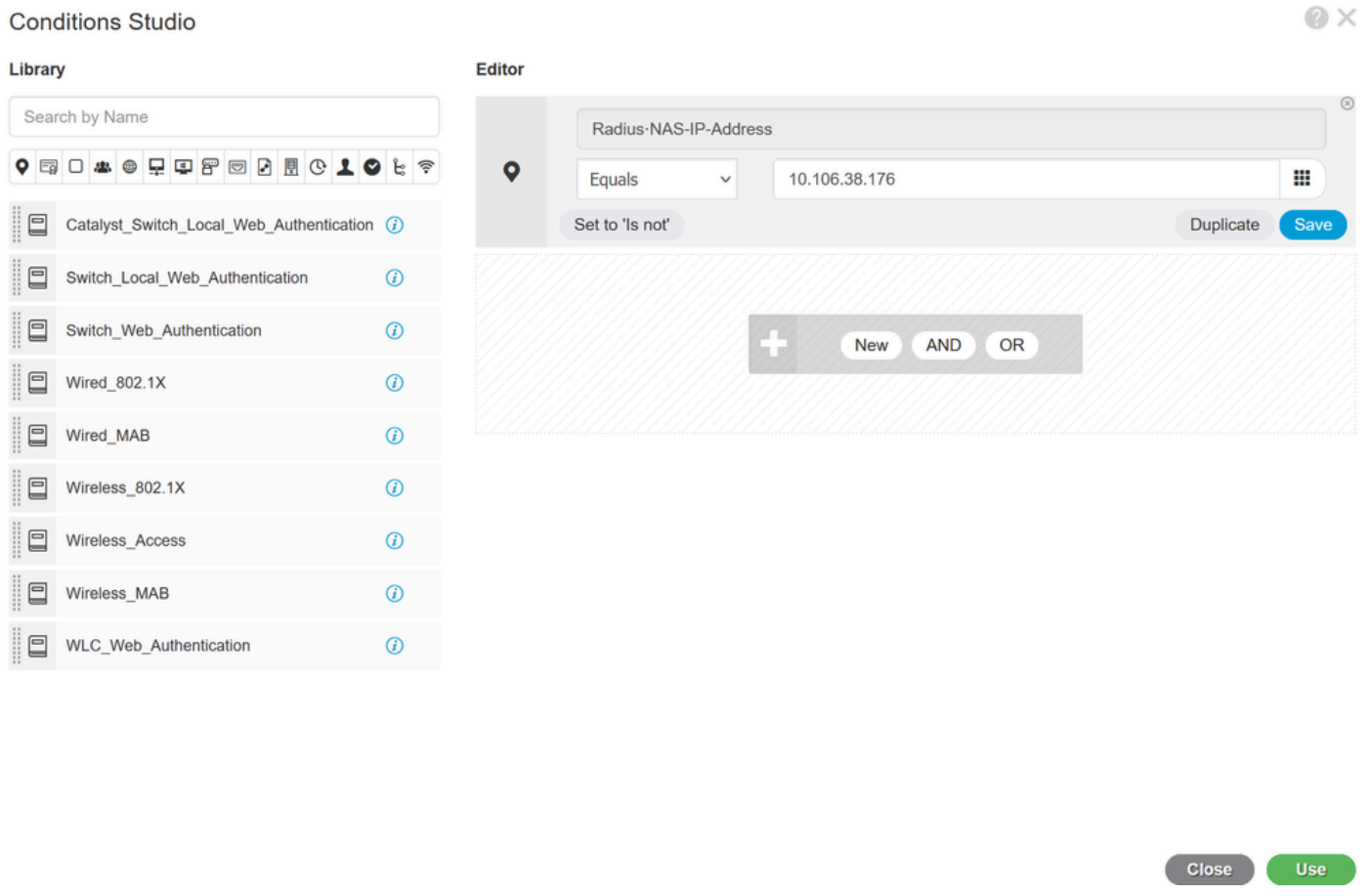


Aggiungi set di criteri in ISE

Passaggio 8.1. Nella parte superiore dei set di criteri viene inserita una nuova riga.

Assegnare un nome al nuovo criterio e aggiungere una condizione affinché l'attributo RADIUS NAS-IP-Address corrisponda all'indirizzo IP SWA.

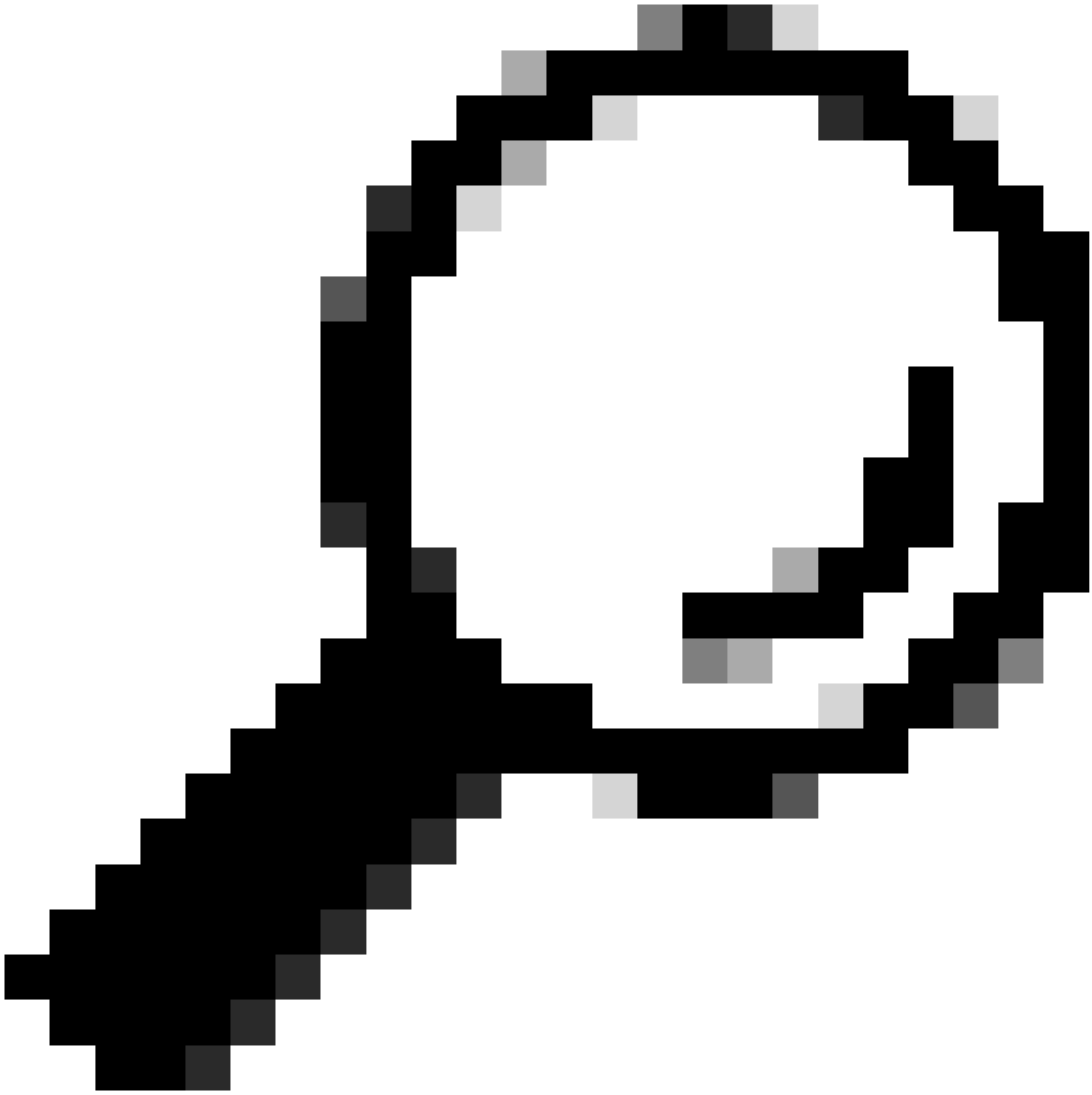
Fate clic su Usa (Use) per mantenere le modifiche e uscire dall'editor.



Aggiungi criterio per mappare il dispositivo di rete SWA

Passaggio 8.2. Fare clic su Save (Salva).

Salvataggio criteri



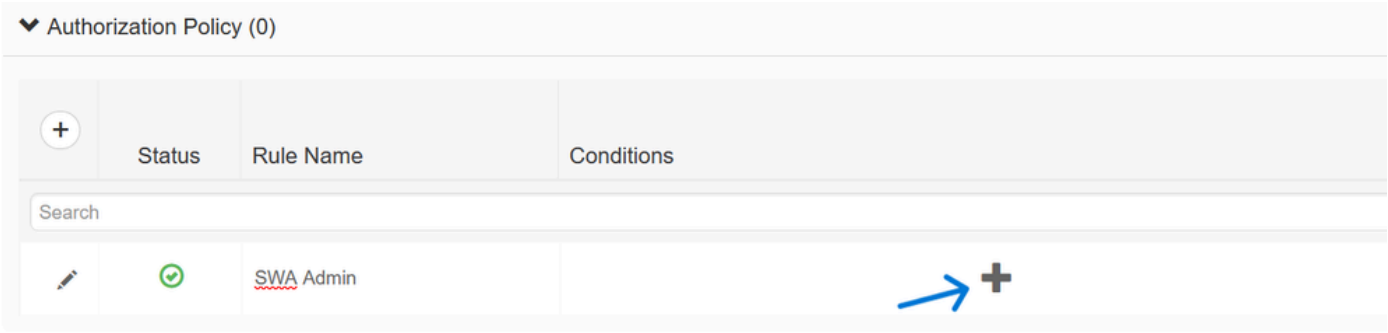
Suggerimento: in questo articolo è consentito utilizzare l'elenco Protocolli di accesso alla rete predefiniti. È possibile creare un nuovo elenco e restringerlo in base alle esigenze.

Passaggio 9. Per visualizzare i nuovi set di criteri, fare clic sull'icona > nella colonna Visualizza. Espandere il menu Criteri di autorizzazione e fare clic sull'icona + per aggiungere una nuova

regola per consentire l'accesso all'utente con diritti di amministratore.

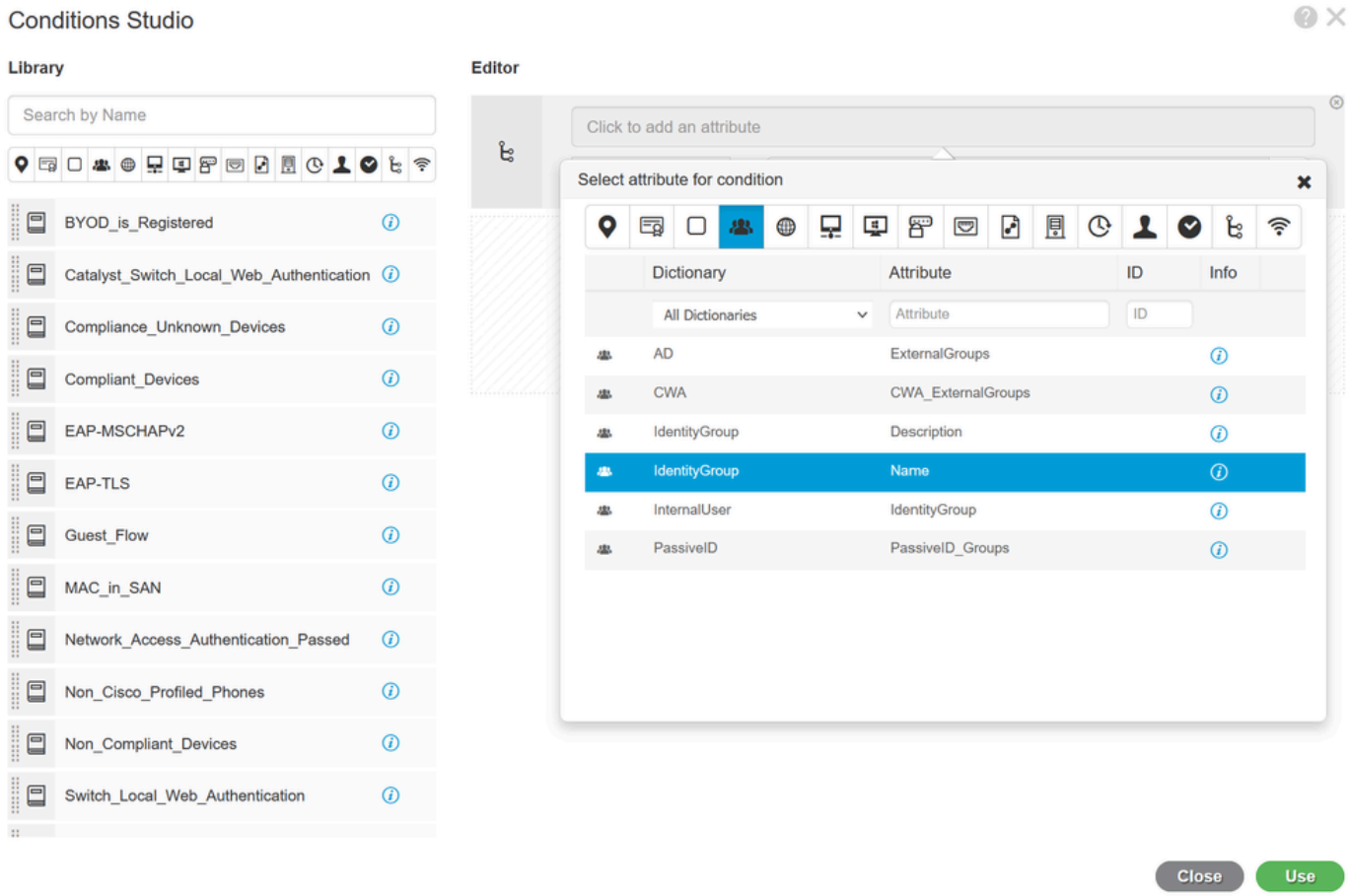
Impostare un nome.

Passaggio 9.1. Per creare una condizione corrispondente al gruppo di utenti Amministratore, fare clic sull'icona +.



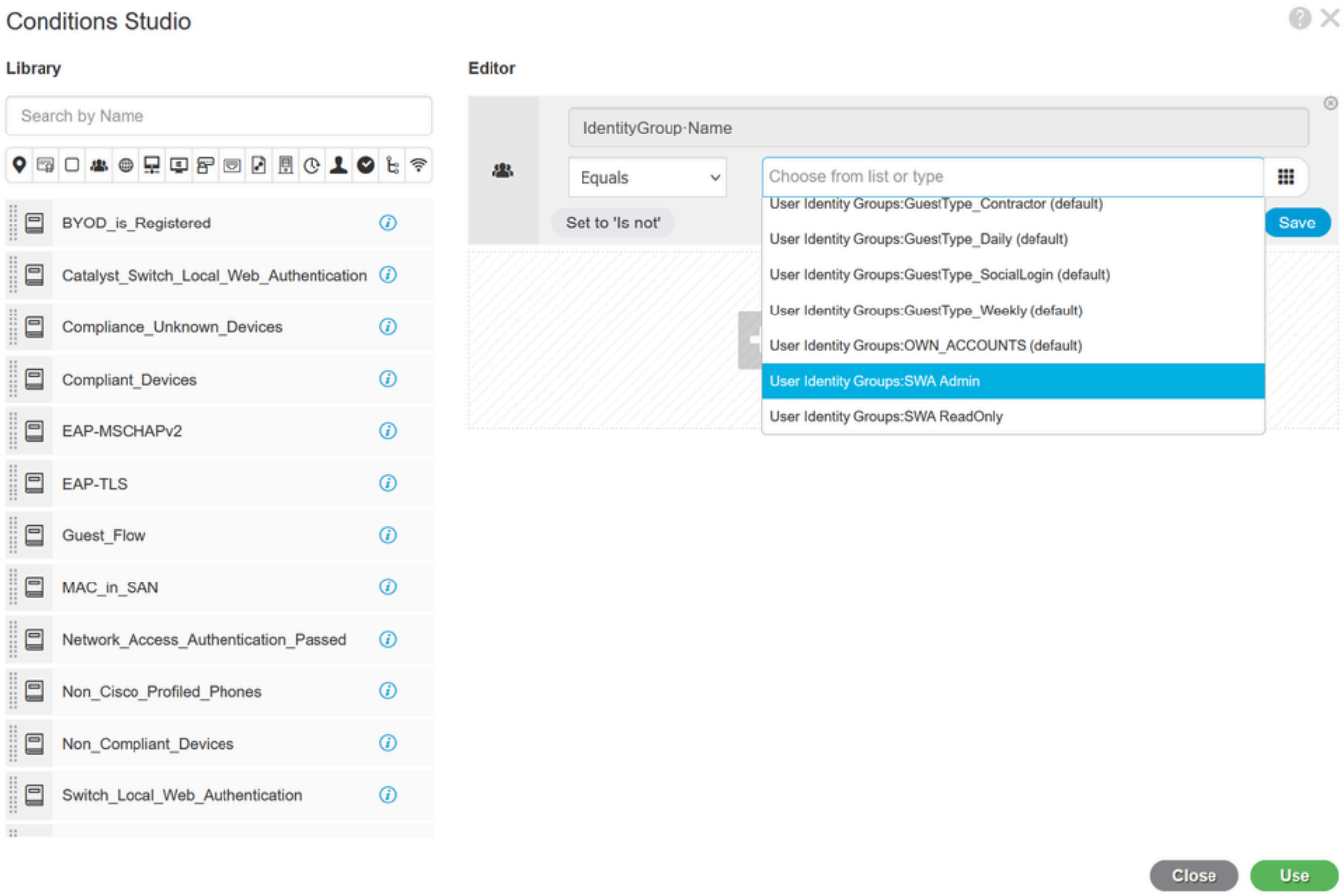
Aggiungi condizione del criterio di autorizzazione

Passaggio 9.2. Impostare le condizioni in modo che corrispondano al gruppo di identità del dizionario con attributo Nome uguale a gruppi di identità utente: SWA admin.



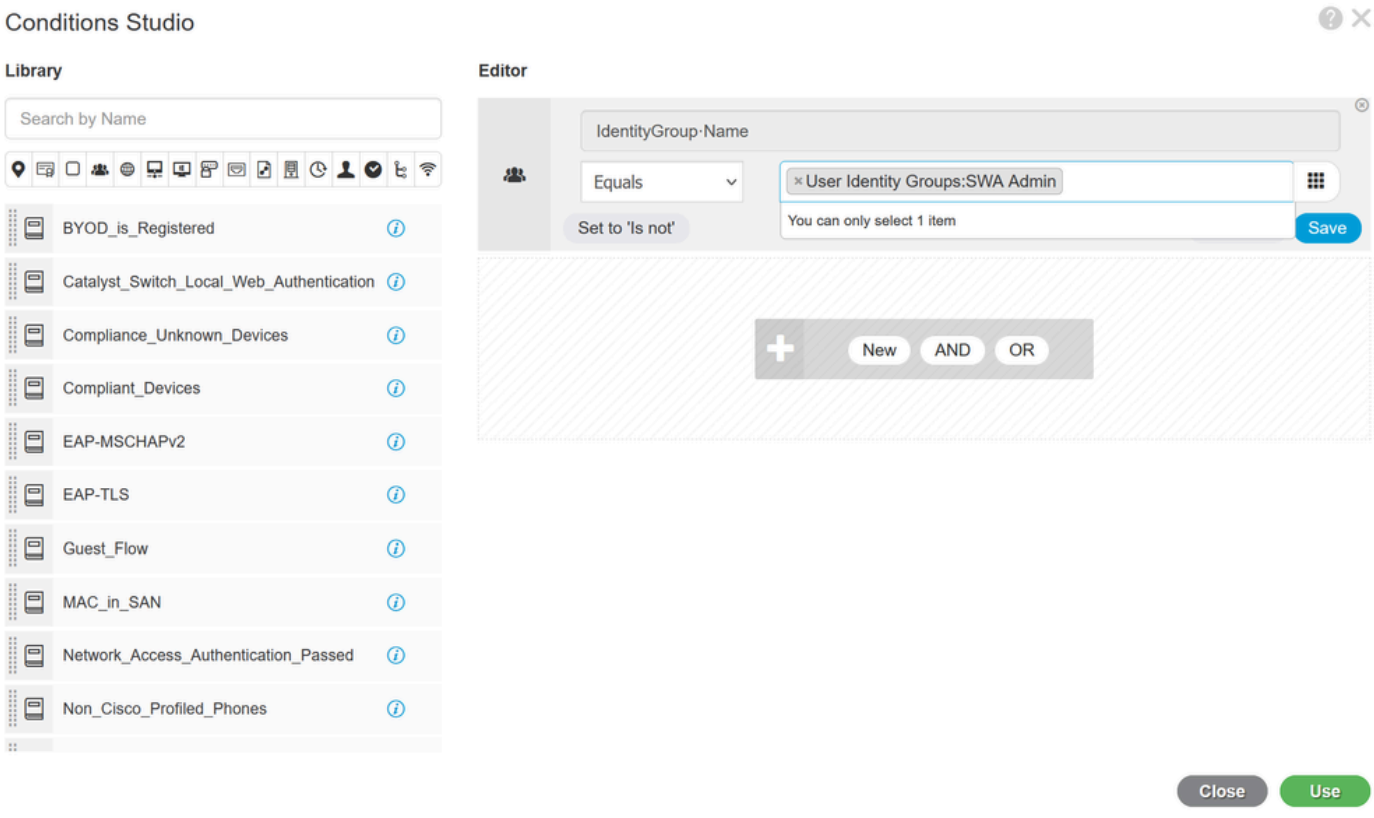
Select Identity Group as Condition

Passaggio 9.3. Scorrere verso il basso e selezionare User Identity Groups: SWA admin.



Scorrere verso il basso e selezionare Identity Group Name

Passaggio 9.4. Fare clic su Usa.

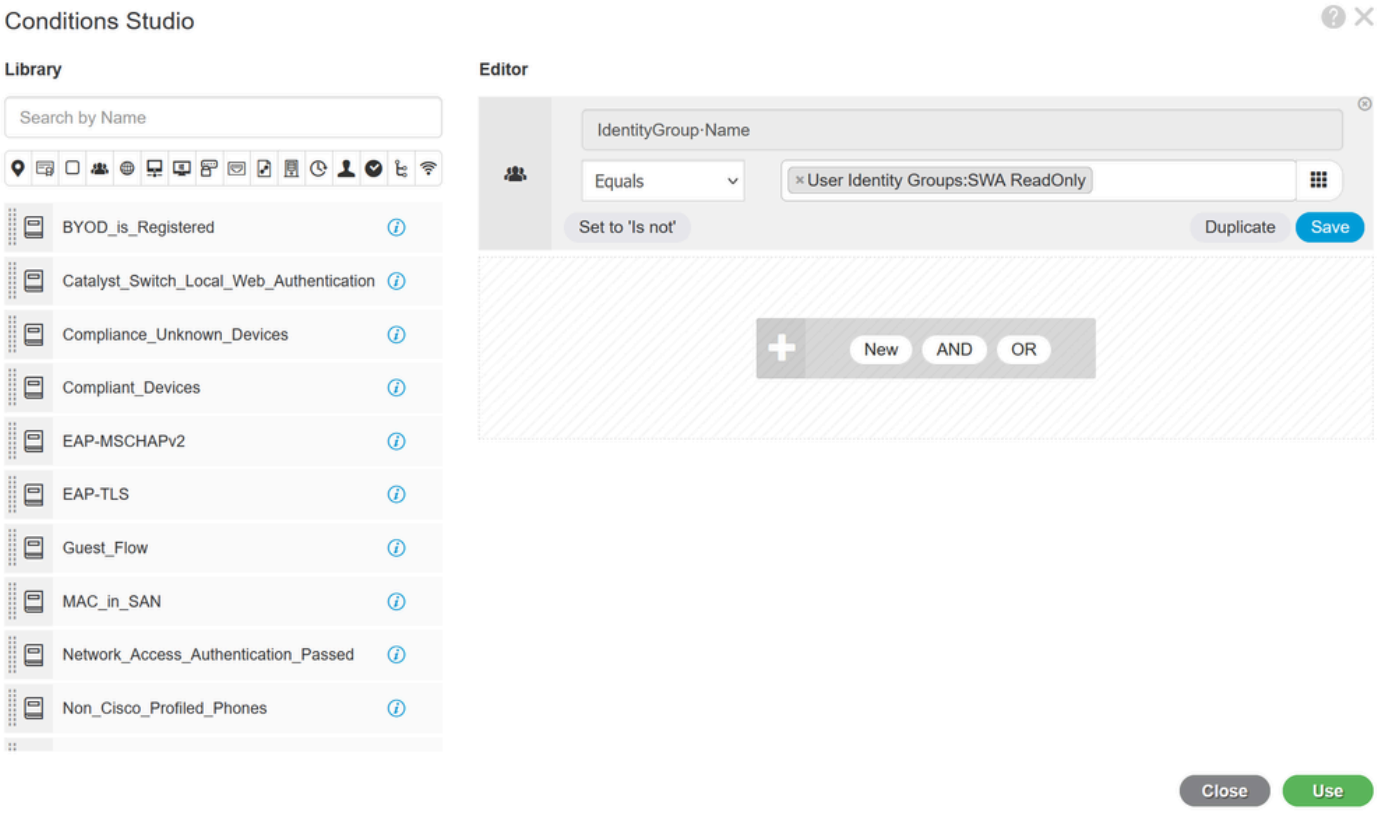


Selezionare i criteri di autorizzazione per il gruppo di utenti Amministratore SWA

Passaggio 10. Fare clic sull'icona + per aggiungere una seconda regola per consentire l'accesso all'utente con diritti di sola lettura.

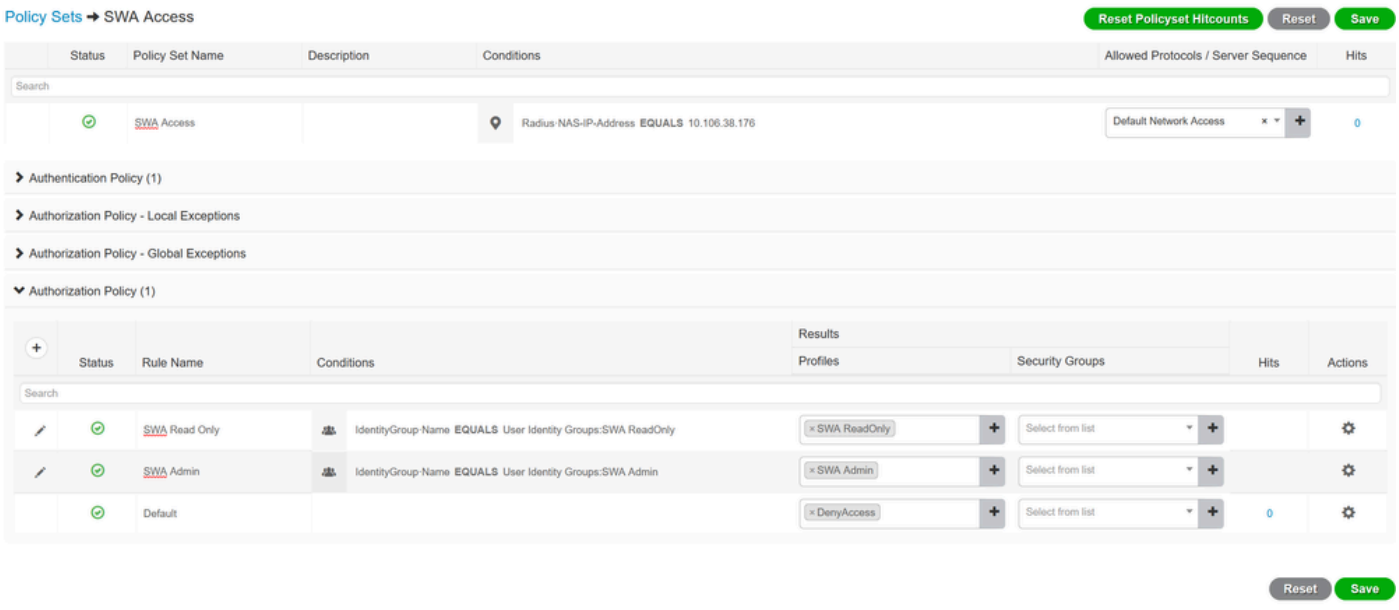
Impostare un nome.

Impostate le condizioni in modo che corrispondano al gruppo di identità del dizionario con il nome dell'attributo Uguale ai gruppi di identità dell'utente: SWA ReadOnly e fate clic su Usa.



Selezionare i criteri di autorizzazione per il gruppo di utenti di sola lettura

Passaggio 11. Impostare il profilo di autorizzazione per ogni regola e fare clic su Salva.

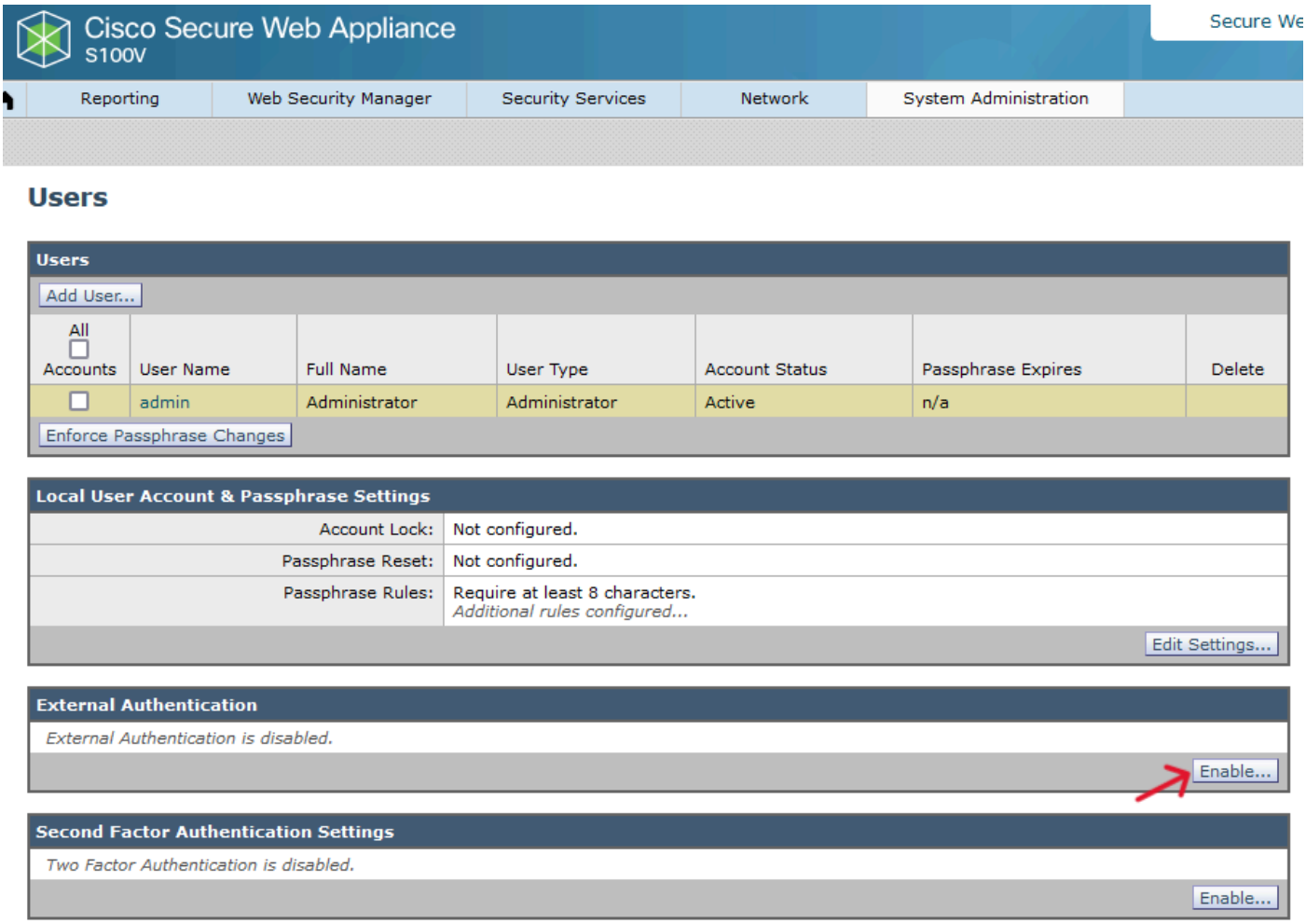


Seleziona profilo di autorizzazione

Configurazione SWA

Passaggio 1. Dalla GUI SWA, passare a System Administration (Amministrazione sistema) e fare clic su Users (Utenti).

Passaggio 2. Fare clic su Enable (Abilita) in External Authentication (Autenticazione esterna).



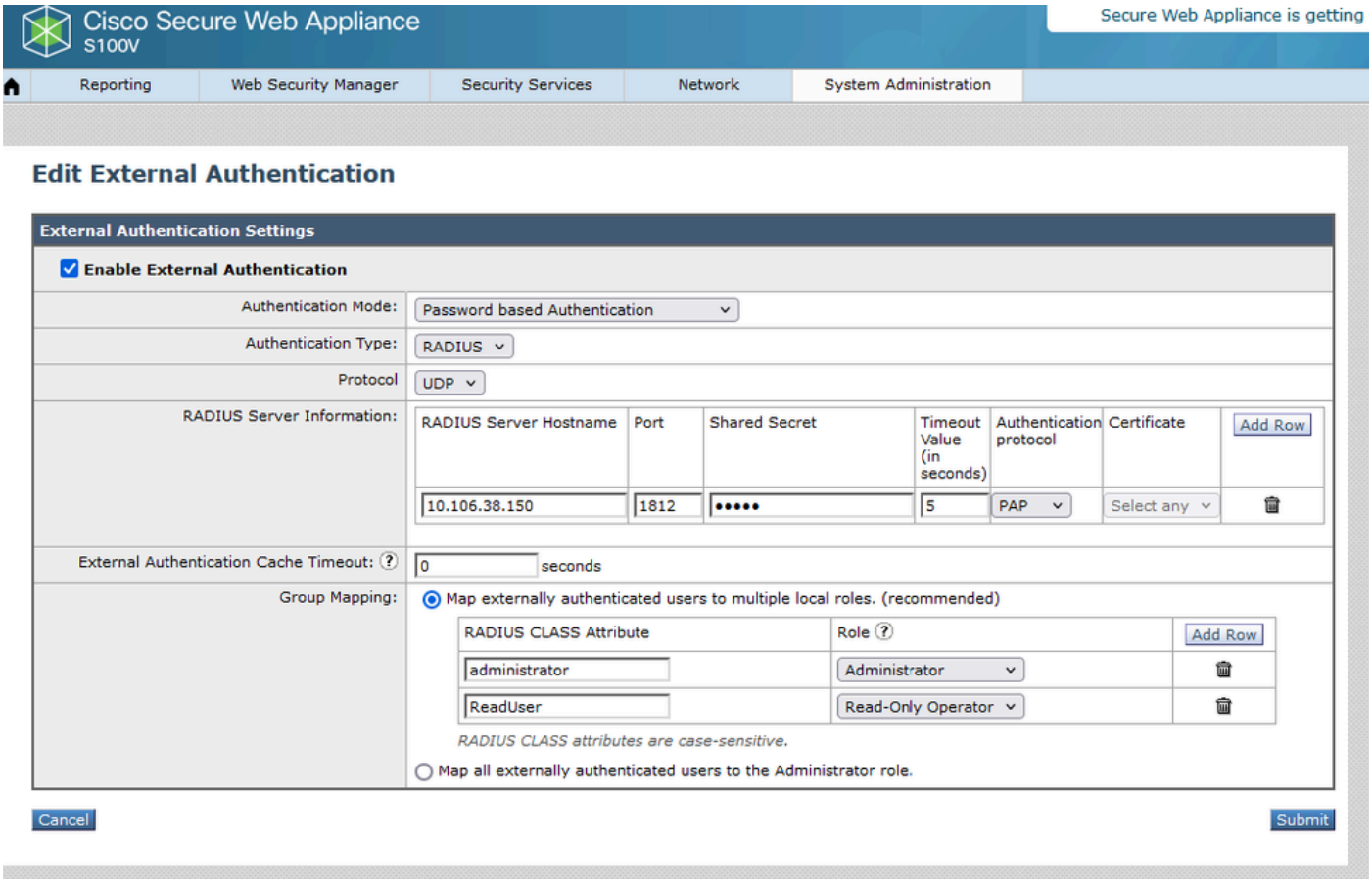
Abilita autenticazione esterna in SWA

Passaggio 3. Immettere l'indirizzo IP o il nome di dominio completo (FQDN) dell'ISE nel campo RADIUS Server Hostname e immettere lo stesso segreto condiviso configurato nel passaggio 2, ISE Configuration.

Passaggio 4. Selezionare Esegui mapping degli utenti autenticati esternamente a più ruoli locali in Mapping gruppi.

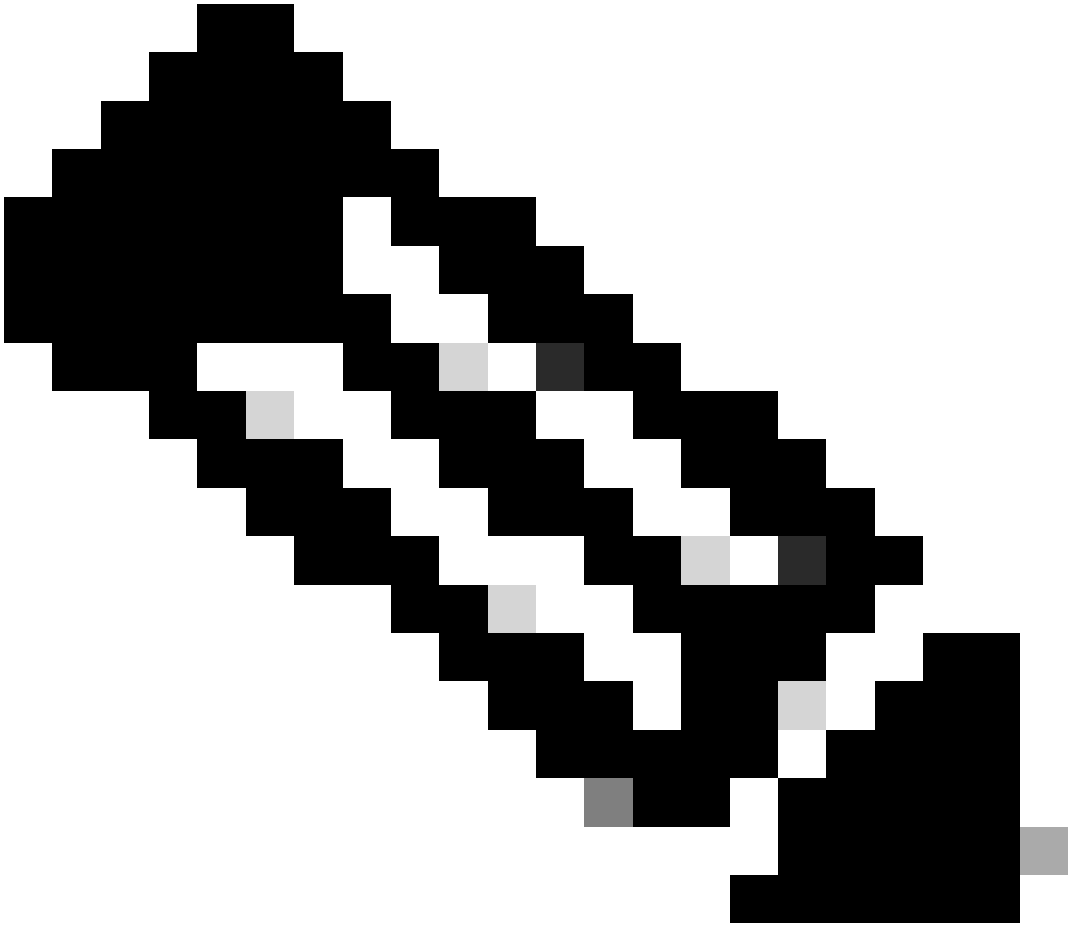
Passaggio 4.1. Immettere Amministratore nel campo Attributo CLASSE RADIUS e selezionare Amministratore ruolo.

Passaggio 4.2. Immettere ReadUser nel campo Attributo CLASSE RADIUS e selezionare l'operatore di sola lettura Role.



Configurazione dell'autenticazione esterna per il server RADIUS

Passaggio 5: per configurare gli utenti in SWA, fare clic su Aggiungi utente. Immettere Nome utente e selezionare Tipo utente richiesto per il ruolo desiderato. Immettere Passphrase e digitare nuovamente la passphrase necessaria per l'accesso tramite interfaccia grafica se l'accessorio non è in grado di connettersi a un server RADIUS esterno.



Nota: se l'accessorio non è in grado di connettersi ad alcun server esterno, tenta di autenticare l'utente come utente locale definito in Secure Web Appliance.

Users

Users

Add User...

** When RADIUS external authentication is enabled, all local user accounts except "admin" are disabled. If all RADIUS services fail, local user accounts will be used for authentication.*

All Accounts	User Name	Full Name	User Type*	Account Status	Passphrase Expires	Delete
☐	adminuser	Admin User	*Administrator*	Active	n/a	🗑
☐	rouser	RO User	*Read-Only Operator*	Active	n/a	🗑

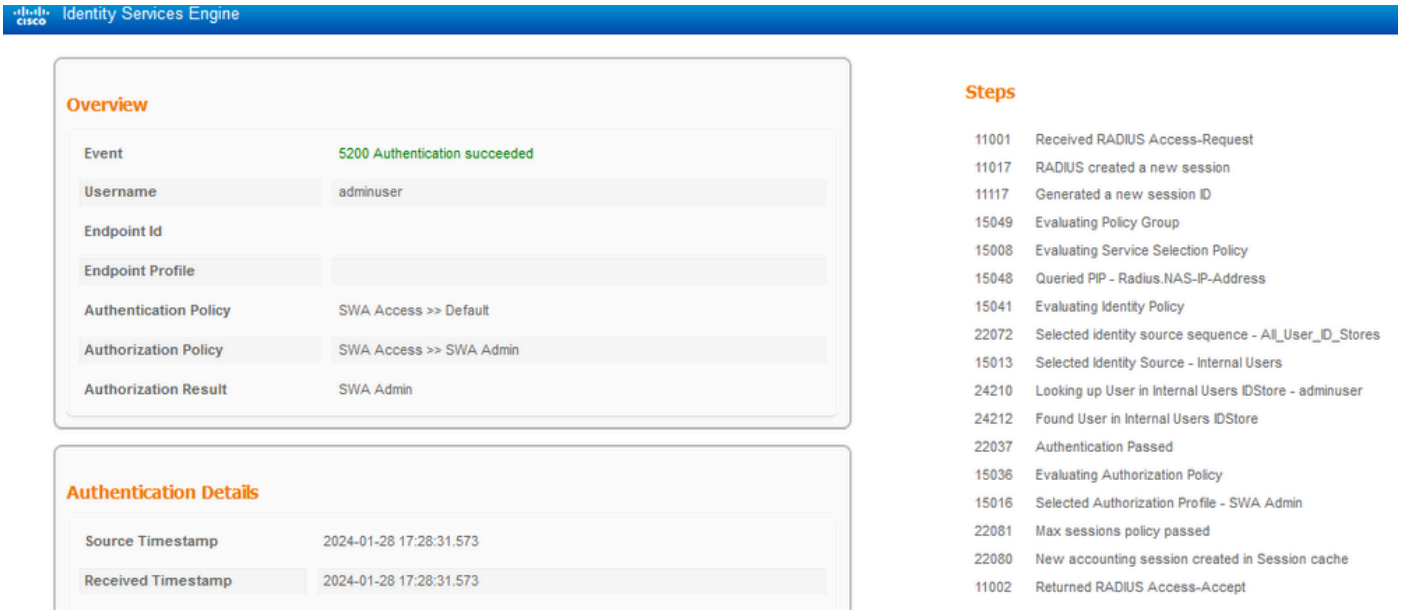
Configurazione utente in SWA

Passaggio 6: fare clic su Sottometti e conferma modifiche.

Verifica

Accedere alla GUI SWA con le credenziali utente configurate e controllare i log attivi in ISE. Per

controllare i log attivi in ISE, selezionare Operations > Live Log:



Verifica accesso utente ISE

Informazioni correlate

- Guida per l'utente di AsyncOS 14.0 per Cisco Secure Web Appliance
- Guida per l'amministratore di ISE 3.0
- ISE Compatibility Matrix per Secure Web Appliance
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).