

# Configurazione dell'autenticazione esterna SWA con ISE come server RADIUS

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Topologia della rete](#)

[Configurazione](#)

[Configurazione di ISE](#)

[Configurazione SWA](#)

[Verifica](#)

[Informazioni correlate](#)

---

## 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

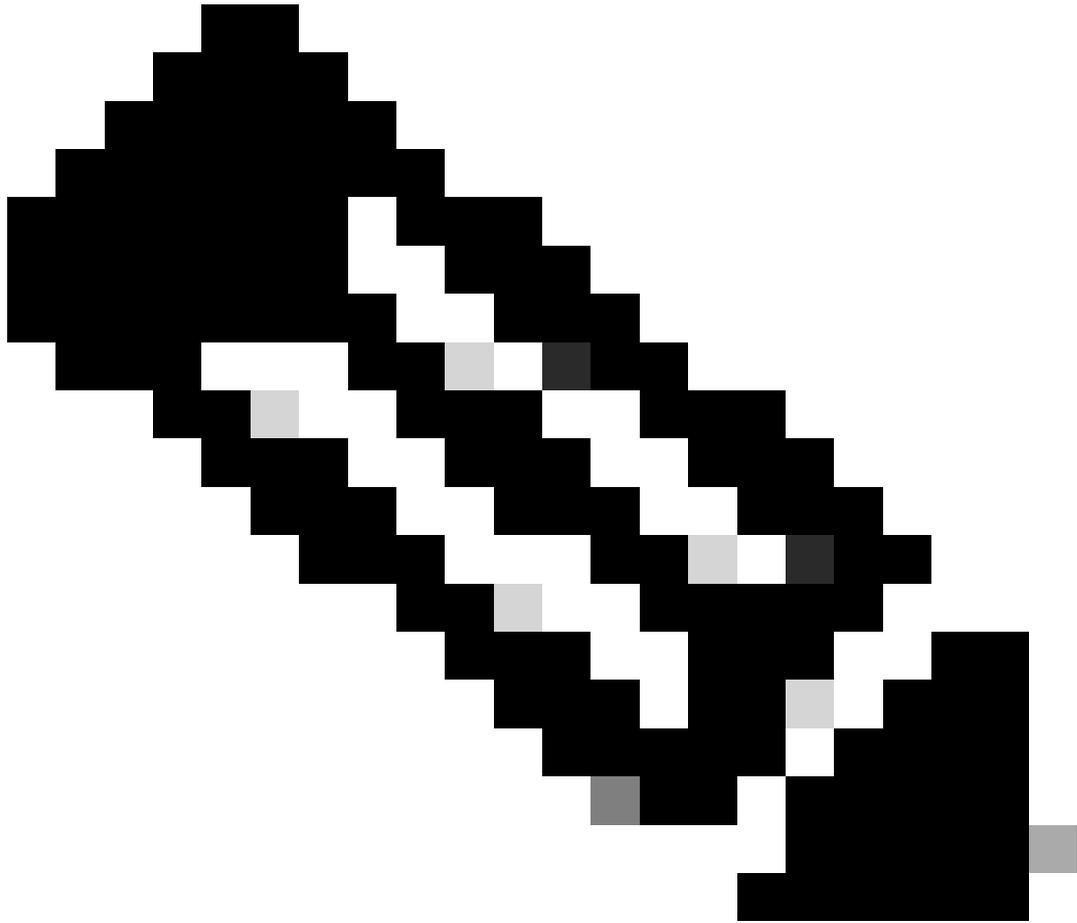
Passaggio 1. Aggiungere un nuovo dispositivo di rete. Selezionare Amministrazione > Risorse di rete > Dispositivi di rete > +Aggiungi.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Under Administration, the 'Network Resources' section is expanded, showing 'Network Devices', 'Network Device Groups', 'Network Device Profiles', 'External RADIUS Servers', 'RADIUS Server Sequences', 'NAC Managers', and 'External MDM'. The 'Network Devices' page is active, displaying a table with columns for Name, IP/Mask, Profile Name, Location, and Type. The table is currently empty, with the text 'No data available' at the bottom right. Action buttons for Edit, Add, Duplicate, Import, Export, Generate PAC, and Delete are visible above the table.

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.

---

Network Devices

Default Device

Device Security Settings

[Network Devices List > SWA](#)

### Network Devices

\* Name

Description

IP Address  /

\* Device Profile

Model Name

Software Version

\* Network Device Group

Location

IPSEC

Device Type

**RADIUS Authentication Settings**

RADIUS UDP Settings

Protocol **RADIUS**

\* Shared Secret

Configurazione della chiave condivisa del dispositivo di rete SWA

Passaggio 2.1. Fare clic su Invia.

**RADIUS Authentication Settings**

**RADIUS UDP Settings**

Protocol **RADIUS**

\* Shared Secret

Use Second Shared Secret  ⓘ

CoA Port

**RADIUS DTLS Settings ⓘ**

DTLS Required  ⓘ

Shared Secret  ⓘ

CoA Port

Issuer CA of ISE Certificates for CoA  ⓘ

DNS Name

**General Settings**

Enable KeyWrap  ⓘ

\* Key Encryption Key

\* Message Authenticator Code Key

Key Input Format  ASCII  HEXADECIMAL

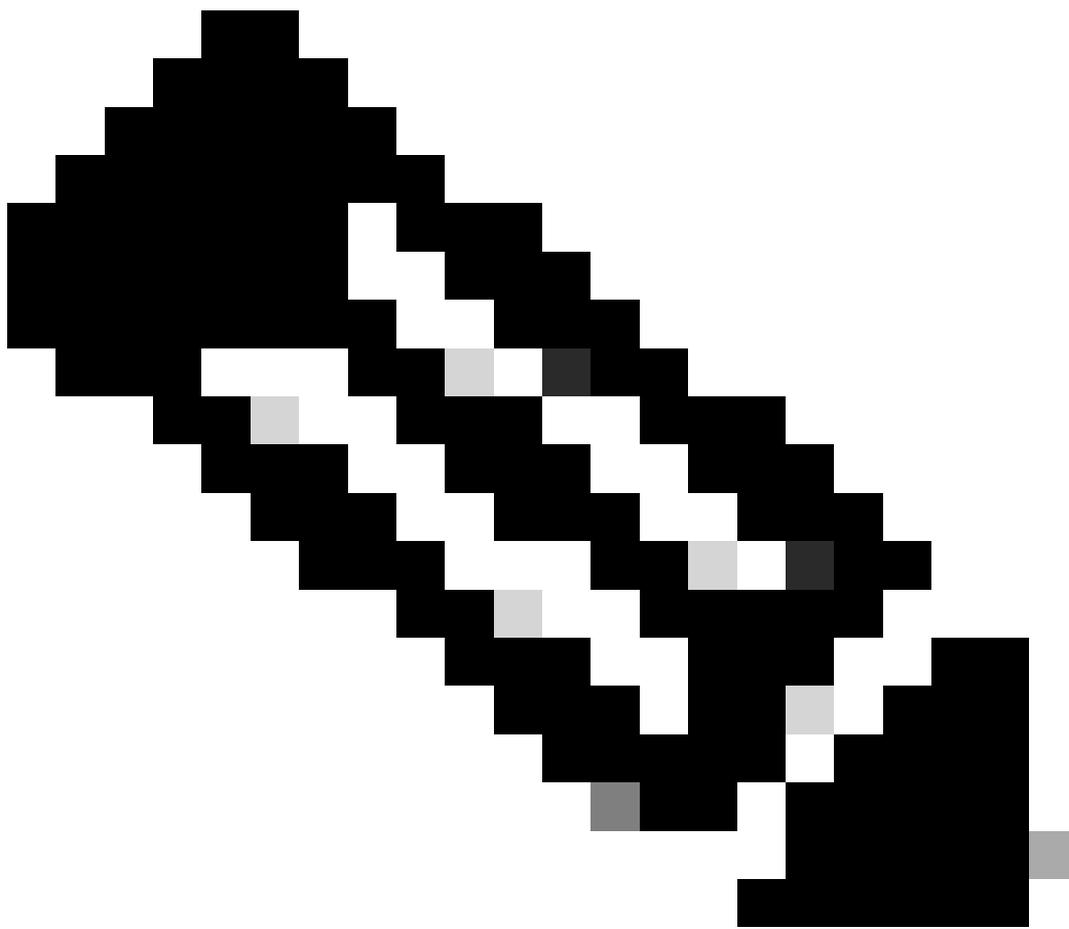
▶ TACACS Authentication Settings

▶ SNMP Settings

▶ Advanced TrustSec Settings

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.

The screenshot displays the Cisco ISE Administration interface. The top navigation bar includes 'Identity Services Engine', 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Administration' menu is expanded to show 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', 'Feed Service', and 'Threat Centric NAC'. The 'Identity Management' menu is further expanded to show 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'Groups' menu item is selected.

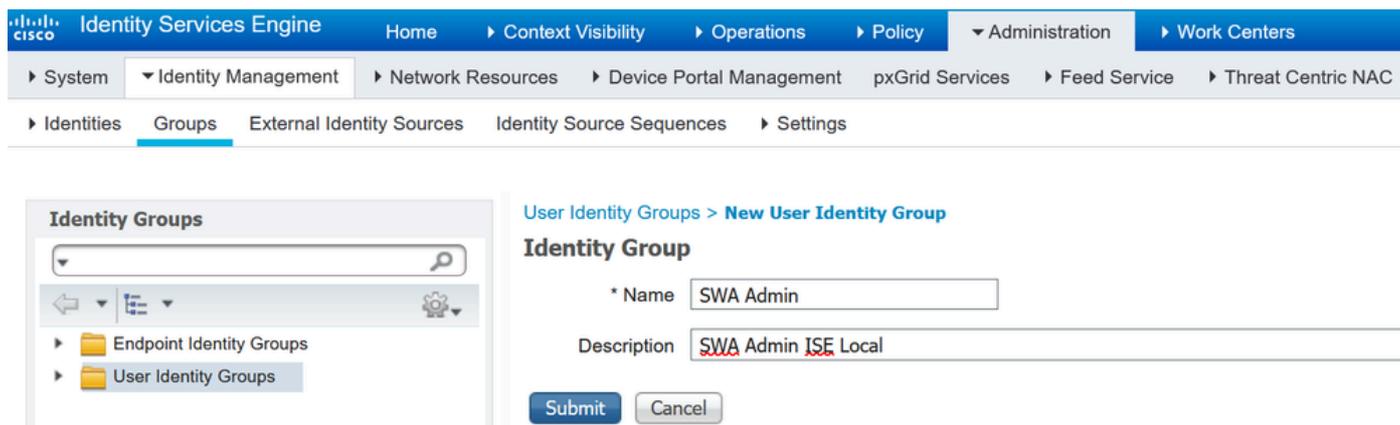
The main content area is titled 'User Identity Groups'. It features a search bar and a list of existing groups. The list has columns for 'Name' and 'Description'. The groups listed are:

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

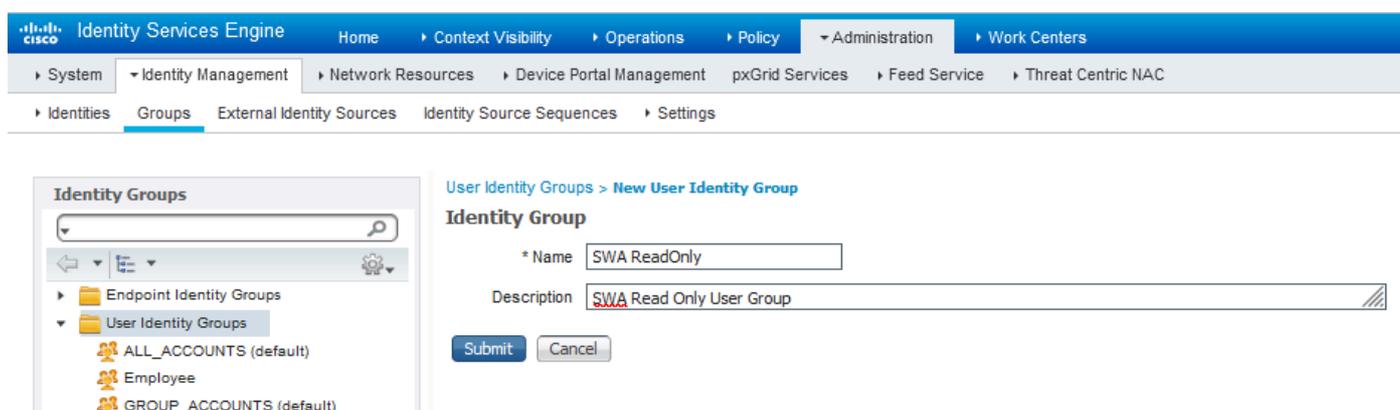
Aggiungi gruppo di identità utente

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.



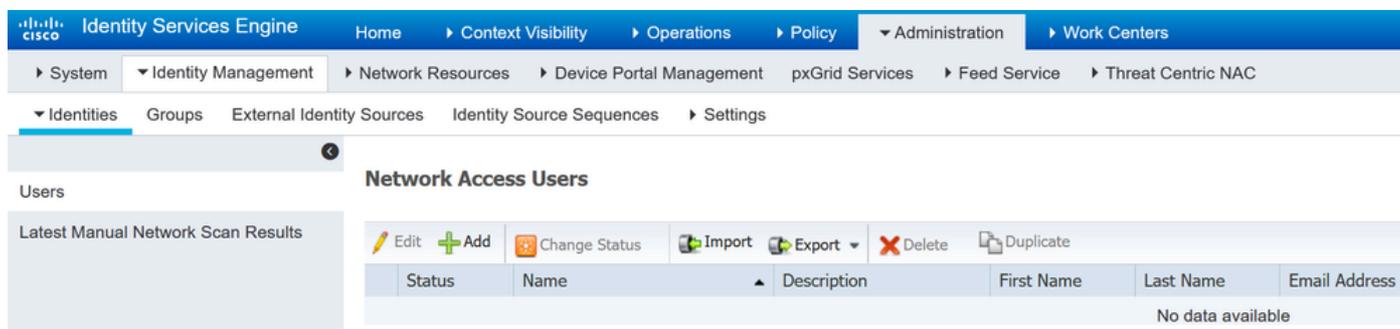
Aggiungi



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.

**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:

Password  Re-Enter Password

Aggiungi utente amministratore

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

**Account Disable Policy**

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

**User Groups**

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.

**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:

	Password	Re-Enter Password	
* Login Password	<input type="password" value="••••••"/>	<input type="password" value="••••••"/>	<input type="button" value="Generate Password"/> ⓘ
Enable Password	<input type="password"/>	<input type="password"/>	<input type="button" value="Generate Password"/> ⓘ

Aggiungi utente di sola lettura

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

**Account Disable Policy**

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

**User Groups**

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.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionaryes Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > New Authorization Profile

**Authorization Profile**

\* Name SWA Admin

Description

\* Access Type ACCESS\_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Passive Identity Tracking

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.

Advanced Attributes Settings

Radius:Class = Administrator

Attributes Details

Access Type = ACCESS\_ACCEPT  
Class = Administrator

Submit Cancel

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.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > New Authorization Profile

### Authorization Profile

\* Name: SWA ReadOnly

Description:

\* Access Type: ACCESS\_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:

Passive Identity Tracking:

Aggiungi profilo di autorizzazione per utenti di sola lettura

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

Advanced Attributes Settings

Radius:Class = ReadUser

Attributes Details

Access Type = ACCESS\_ACCEPT  
Class = ReadUser

Submit Cancel

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.



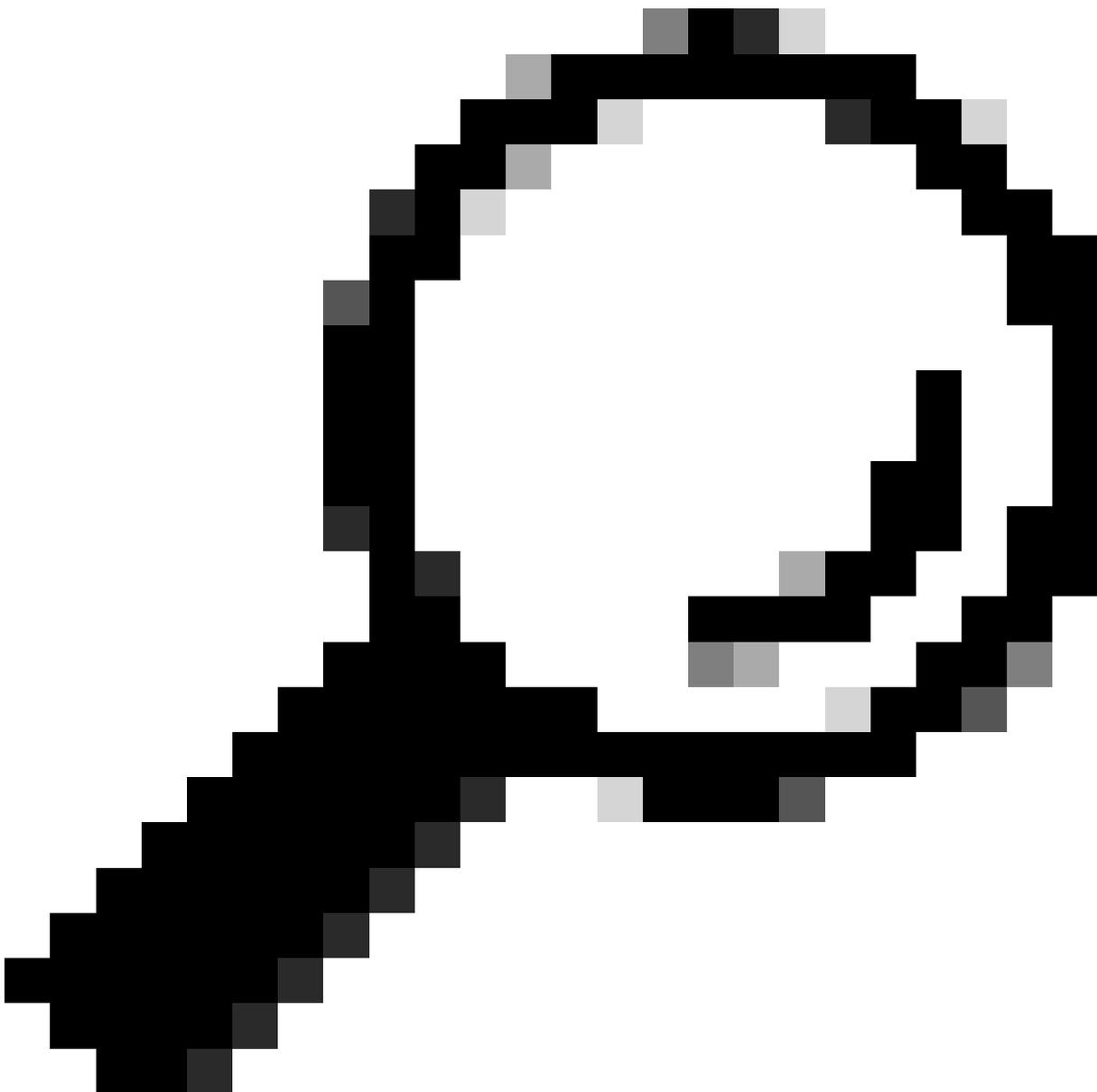
## Policy Sets

[Reset Policyset Hitcounts](#)[Reset](#)[Save](#)

	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
		SWA Access		Radius-NAS-IP-Address EQUALS 10.106.38.176	Default Network Access x v +			
		Default	Default policy set		Default Network Access x v +	0		

[Reset](#)[Save](#)

Salvataggio criteri



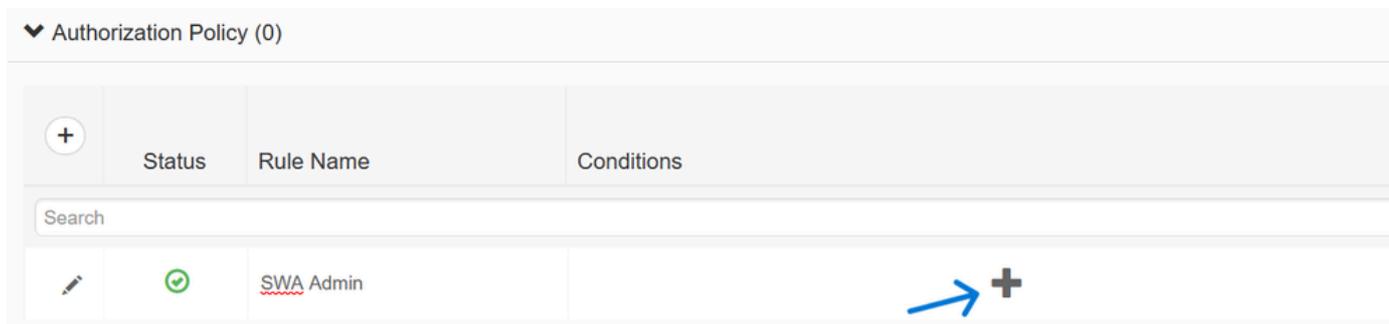
Suggerimento: in questo articolo è consentito utilizzare l'elenco Protocolli di accesso alla rete predefiniti. È possibile creare un nuovo elenco e restringerlo in base alle esigenze.

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.

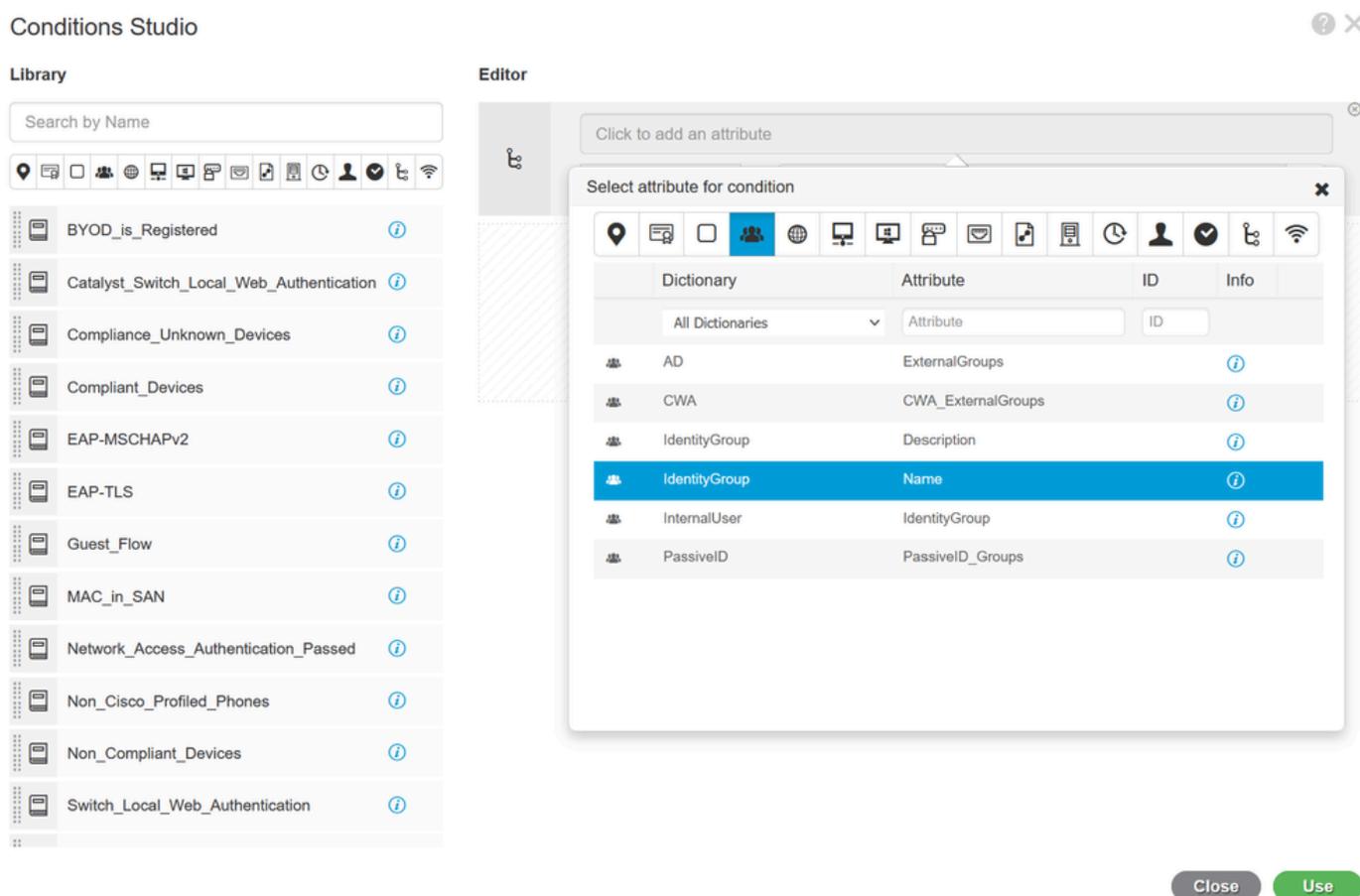
Impostare un nome.

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.

## Conditions Studio



### Library

Search by Name

BYOD\_is\_Registered ⓘ

Catalyst\_Switch\_Local\_Web\_Authentication ⓘ

Compliance\_Unknown\_Devices ⓘ

Compliant\_Devices ⓘ

EAP-MSCHAPv2 ⓘ

EAP-TLS ⓘ

Guest\_Flow ⓘ

MAC\_in\_SAN ⓘ

Network\_Access\_Authentication\_Passed ⓘ

Non\_Cisco\_Profiled\_Phones ⓘ

Non\_Compliant\_Devices ⓘ

Switch\_Local\_Web\_Authentication ⓘ

### Editor

IdentityGroup-Name

Equals

Set to 'Is not'

Choose from list or type

- User Identity Groups:GuestType\_Contractor (default)
- User Identity Groups:GuestType\_Daily (default)
- User Identity Groups:GuestType\_SocialLogin (default)
- User Identity Groups:GuestType\_Weekly (default)
- User Identity Groups:OWN\_ACCOUNTS (default)
- User Identity Groups:SWA Admin**
- User Identity Groups:SWA ReadOnly

Save

Close Use

Scorrere verso il basso e selezionare Identity Group Name

## Passaggio 9.4. Fare clic su Usa.

## Conditions Studio



### Library

Search by Name

BYOD\_is\_Registered ⓘ

Catalyst\_Switch\_Local\_Web\_Authentication ⓘ

Compliance\_Unknown\_Devices ⓘ

Compliant\_Devices ⓘ

EAP-MSCHAPv2 ⓘ

EAP-TLS ⓘ

Guest\_Flow ⓘ

MAC\_in\_SAN ⓘ

Network\_Access\_Authentication\_Passed ⓘ

Non\_Cisco\_Profiled\_Phones ⓘ

### Editor

IdentityGroup-Name

Equals

Set to 'Is not'

\* User Identity Groups:SWA Admin

You can only select 1 item

Save

+ New AND OR

Close Use

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.

Conditions Studio

Library

Search by Name

BYOD\_is\_Registered

Catalyst\_Switch\_Local\_Web\_Authentication

Compliance\_Unknown\_Devices

Compliant\_Devices

EAP-MSCHAPv2

EAP-TLS

Guest\_Flow

MAC\_in\_SAN

Network\_Access\_Authentication\_Passed

Non\_Cisco\_Profiled\_Phones

Editor

IdentityGroup-Name

Equals

× User Identity Groups:SWA ReadOnly

Set to 'Is not'

Duplicate

Save

+ New AND OR

Close Use

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.

Policy Sets → SWA Access

Reset Pollicyset Hitcounts

Reset

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	SWA Access		Radius-NAS-IP-Address EQUALS 10.106.38.176	Default Network Access × +	0

Authentication Policy (1)

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (1)

+ Status	Rule Name	Conditions	Results Profiles	Security Groups	Hits	Actions
✓	SWA Read Only	IdentityGroup-Name EQUALS User Identity Groups:SWA ReadOnly	× SWA ReadOnly +	Select from list +		⚙
✓	SWA Admin	IdentityGroup-Name EQUALS User Identity Groups:SWA Admin	× SWA Admin +	Select from list +		⚙
✓	Default		× DenyAccess +	Select from list +	0	⚙

Reset

Save

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).

The screenshot shows the Cisco Secure Web Appliance (SWA) GUI. The top navigation bar includes 'Reporting', 'Web Security Manager', 'Security Services', 'Network', and 'System Administration'. The main content area is titled 'Users' and contains the following sections:

- Users:** A table with columns: Accounts, User Name, Full Name, User Type, Account Status, Passphrase Expires, and Delete. The 'admin' user is listed with the role 'Administrator' and 'Active' status. There is an 'Add User...' button and an 'Enforce Passphrase Changes' button.
- Local User Account & Passphrase Settings:** A table with settings for Account Lock, Passphrase Reset, and Passphrase Rules. The 'Passphrase Rules' section indicates 'Require at least 8 characters. Additional rules configured...'. There is an 'Edit Settings...' button.
- External Authentication:** A section with the text 'External Authentication is disabled.' and an 'Enable...' button, which is highlighted with a red arrow.
- Second Factor Authentication Settings:** A section with the text 'Two Factor Authentication is disabled.' and an 'Enable...' button.

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.

### Edit External Authentication

**External Authentication Settings**

**Enable External Authentication**

Authentication Mode: Password based Authentication

Authentication Type: RADIUS

Protocol: UDP

RADIUS Server Information:							Add Row
RADIUS Server Hostname	Port	Shared Secret	Timeout Value (in seconds)	Authentication protocol	Certificate		
10.106.38.150	1812	*****	5	PAP	Select any		

External Authentication Cache Timeout: 0 seconds

Group Mapping:

Map externally authenticated users to multiple local roles. (recommended)

RADIUS CLASS Attribute	Role	Add Row
administrator	Administrator	
ReadUser	Read-Only Operator	

*RADIUS CLASS attributes are case-sensitive.*

Map all externally authenticated users to the Administrator role.

Cancel Submit

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						
<input type="button" value="Add User..."/>						
<small>* 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.</small>						
<input type="checkbox"/> Accounts	User Name	Full Name	User Type*	Account Status	Passphrase Expires	Delete
<input type="checkbox"/>	adminuser	Admin User	Administrator	Active	n/a	
<input type="checkbox"/>	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:

The screenshot displays the Cisco Identity Services Engine (ISE) Live Log interface. At the top, the Cisco logo and 'Identity Services Engine' are visible. The main content is divided into two primary sections: 'Overview' and 'Authentication Details', with a 'Steps' list on the right.

**Overview**

Event	5200 Authentication succeeded
Username	adminuser
Endpoint Id	
Endpoint Profile	
Authentication Policy	SWA Access >> Default
Authorization Policy	SWA Access >> SWA Admin
Authorization Result	SWA Admin

**Authentication Details**

Source Timestamp	2024-01-28 17:28:31.573
Received Timestamp	2024-01-28 17:28:31.573

**Steps**

- 11001 Received RADIUS Access-Request
- 11017 RADIUS created a new session
- 11117 Generated a new session ID
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15048 Queried PIP - Radius.NAS-IP-Address
- 15041 Evaluating Identity Policy
- 22072 Selected identity source sequence - All\_User\_ID\_Stores
- 15013 Selected Identity Source - Internal Users
- 24210 Looking up User in Internal Users IDStore - adminuser
- 24212 Found User in Internal Users IDStore
- 22037 Authentication Passed
- 15036 Evaluating Authorization Policy
- 15016 Selected Authorization Profile - SWA Admin
- 22081 Max sessions policy passed
- 22080 New accounting session created in Session cache
- 11002 Returned RADIUS Access-Accept

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).