Configurazione di TACACS di autenticazione esterna Catalyst Center con ISE

Sommario

Introduzione

In questo documento viene descritto come integrare Cisco Identity Services Engine con Catalyst Center per abilitare l'autenticazione TACACS+.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso come amministratore a Cisco ISE e Cisco Catalyst Center.
- Conoscenza di base dei concetti di AAA (autenticazione, autorizzazione e accounting).
- Conoscenza operativa del protocollo TACACS+.
- Connettività di rete tra Catalyst Center e il server ISE.

Componenti usati

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

- Cisco Catalyst Center versione 2.3.7.x
- Cisco Identity Services Engine (ISE) versione 3.x (o successiva)
- Protocollo TACACS+ per autenticazione utente esterno

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

Questa integrazione consente agli utenti esterni di accedere al Catalyst Center per l'accesso amministrativo e la gestione.

Configurazione

Cisco Identity Services Engine (ISE)

Licenza e abilitazione dei servizi TACACS+

Prima di iniziare con la configurazione di TACACS+ in ISE, è necessario verificare che sia installata la licenza corretta e che la funzionalità sia abilitata.

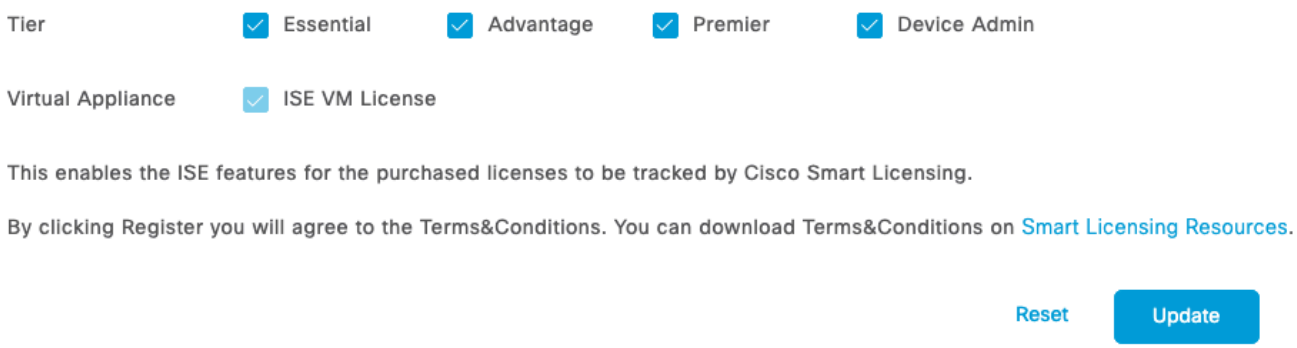
1. Verificare di disporre della licenza PID L-ISE-TACACS-ND= nel portale Cisco Smart Software Manager o Cisco License Central.

Abilitare Device Administration nel portale delle licenze ISE.

- La licenza di amministrazione del dispositivo (PID: L-ISE-TACACS-ND=) abilita i servizi TACACS+ su un Policy Service Node (PSN).
- Accedere a:

  Amministrazione > Sistema > Licenze

- Selezionare la casella Device Admin in Tier options (Opzioni livello).



Amministratore del dispositivo

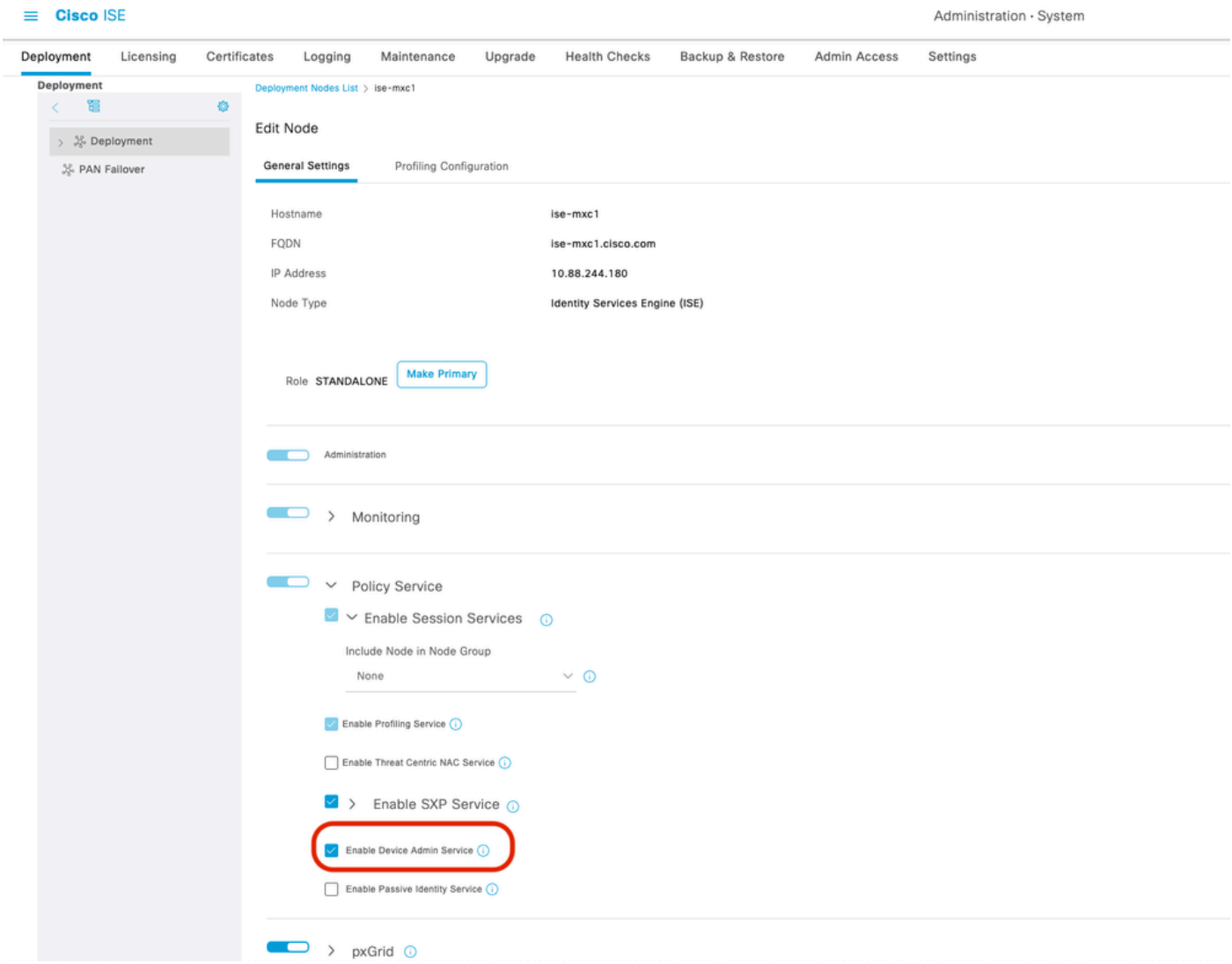
Amministratore del dispositivo di licenza

3. Abilitare il servizio Device Admin sul nodo ISE in cui è in esecuzione il servizio TACACS+.

- Accedere a:

  Amministrazione > Sistema > Distribuzione > Selezionare il nodo

- Selezionare l'opzione Enable Device Admin Service.



Abilita servizio di amministrazione dispositivi

Crea utente amministratore e aggiungi dispositivo di rete

1. Creare l'utente Admin.

- Questo account utente viene utilizzato per accedere all'interfaccia utente di Catalyst Center tramite l'autenticazione ISE.
- Accedere a:

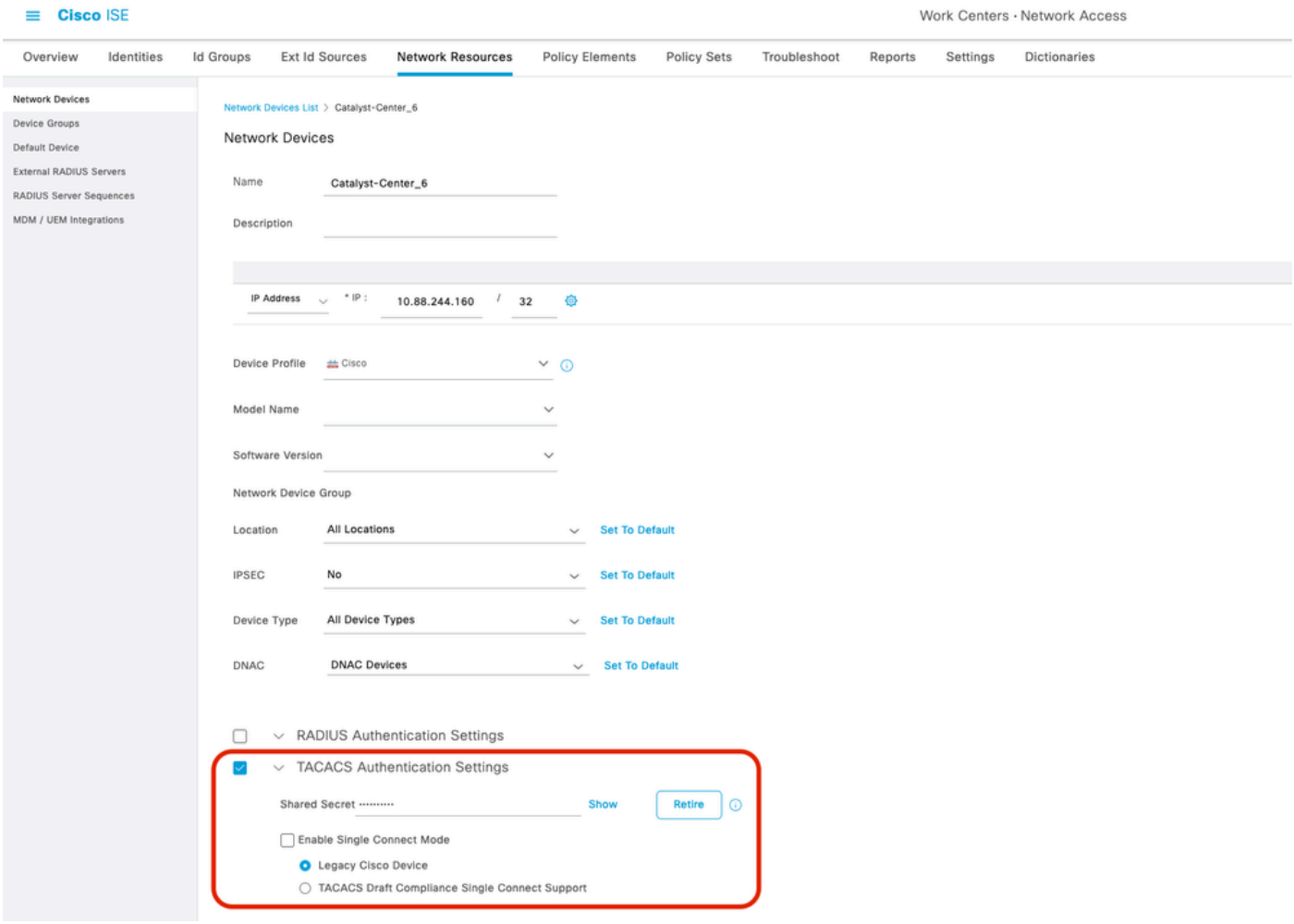
  Centri di lavoro > Accesso alla rete > Identità > Utente di accesso alla rete
- Aggiungere un nuovo utente, ad esempio catc-user.
- Se l'utente esiste già, procedere al passaggio successivo.

2. Creare la periferica di rete.

- Accedere a:

  Centri di lavoro > Accesso alla rete > Identità > Risorsa di rete

- Aggiungere l'indirizzo IP del Catalyst Center o definire la subnet in cui si trova l'indirizzo IP del Catalyst Center.
- Se il dispositivo esiste già, verificare che contenga i parametri seguenti:
    - Le impostazioni di autenticazione TACACS sono abilitate.
    - Il segreto condiviso è configurato e conosciuto (salvare questo valore, come richiesto in seguito in Catalyst Center).



Impostazioni autenticazione TACACS

Configura profilo TACACS+

1. Creare un nuovo profilo TACACS+.

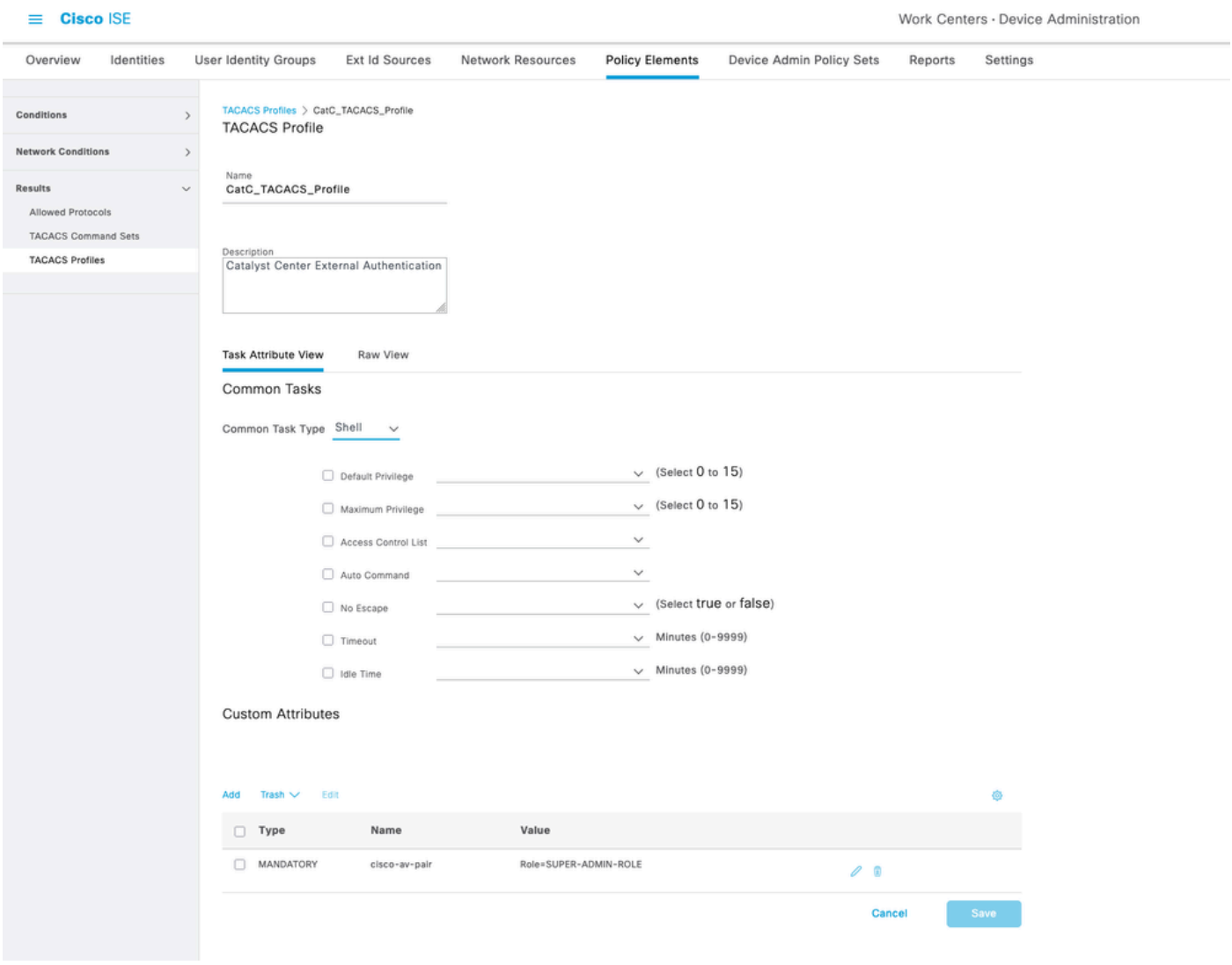
- Accedere a:

Centri di lavoro > Amministrazione dispositivi > Elementi della policy > Risultati > Profili TACACS

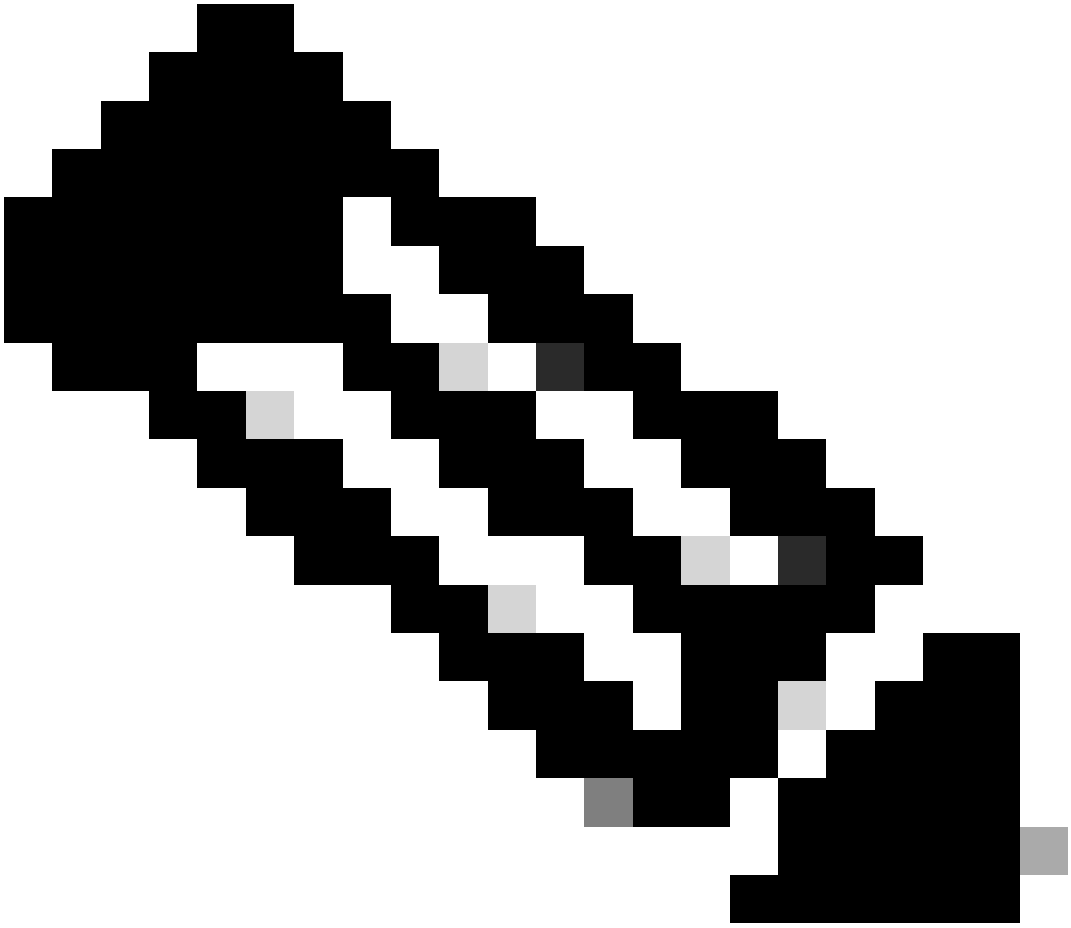
- Aggiungere un nome di profilo.
- Aggiungere un attributo personalizzato nel modo seguente:

- Tipo: Obbligatorio
- Nome: cisco-av-pair
- Valore: Role=SUPER-ADMIN-ROLE

- Salvare il profilo.



Profilo TACACS+



Nota: Cisco Catalyst Center supporta server esterni di autenticazione, autorizzazione e accounting (AAA) per il controllo degli accessi. Se si utilizza un server esterno per l'autenticazione e l'autorizzazione degli utenti esterni, è possibile abilitare l'autenticazione esterna in Cisco Catalyst Center. L'impostazione predefinita dell'attributo AAA corrisponde all'attributo predefinito del profilo utente.

Il valore predefinito dell'attributo AAA del protocollo TACACS è cisco-av-pair.

Il valore predefinito dell'attributo AAA del protocollo RADIUS è Cisco-AVPair.

La modifica è necessaria solo se il server AAA dispone di un attributo personalizzato nel profilo utente. Sul server AAA, il formato del valore dell'attributo AAA è Role=role1. Sul server Cisco Identity Services Engine (Cisco ISE), durante la configurazione del profilo RADIUS o TACACS, l'utente può selezionare o immettere cisco av-pair come attributo AAA.

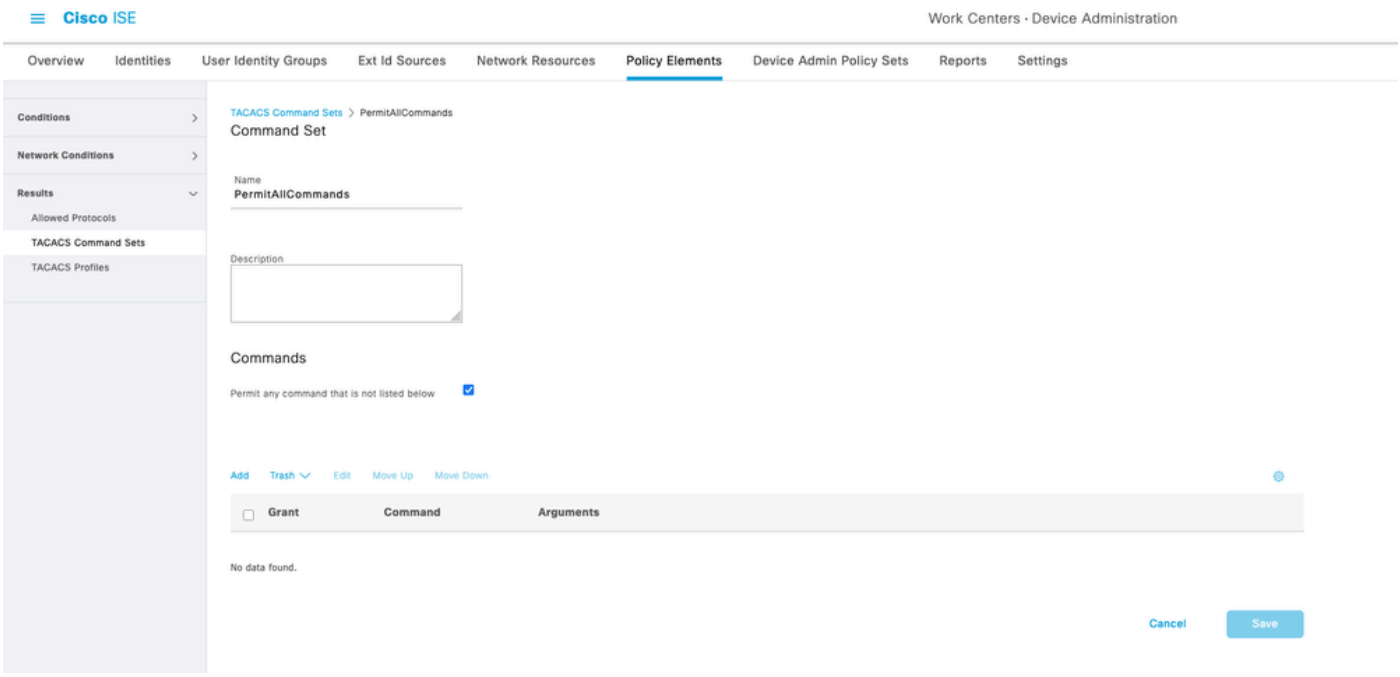
Ad esempio, è possibile selezionare e configurare manualmente l'attributo AAA come cisco-av-pair=Role=SUPER-ADMIN-ROLE o Cisco-AVPair=Role=SUPER-ADMIN-ROLE.

2. Creare un set di comandi TACACS+.

- Accedere a:

Centri di lavoro > Amministrazione dispositivi > Elementi della policy > Risultati > Set di comandi TACACS

- Aggiungere un nome.
- Selezionare l'opzione Permit (Consenti) per i comandi non elencati di seguito.
- Salvare il set di comandi.



Set di comandi TACACS

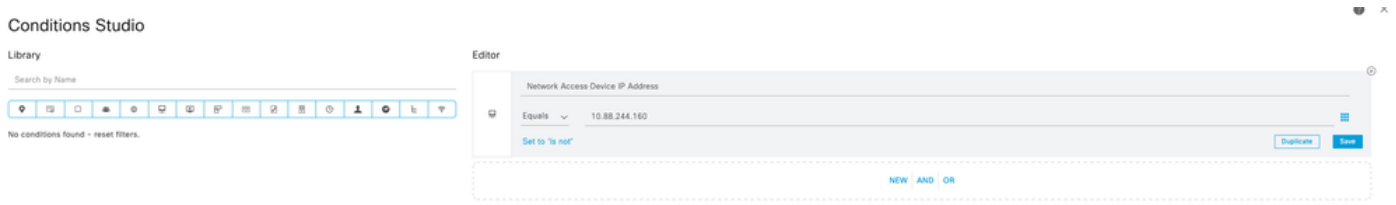
Configurare le policy TACACS+

1. Creare un nuovo set di criteri TACACS+.

- Accedere a:

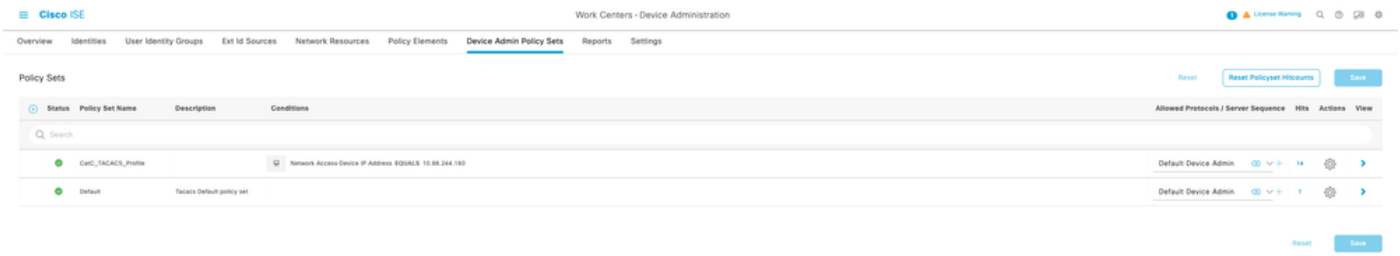
Area di lavoro > Amministrazione dispositivi > Set di criteri di amministrazione dispositivi

- Aggiungere un nome per il set di criteri.
- Configurare la condizione.
  - Nell'esempio, la condizione corrisponde all'indirizzo IP del Catalyst Center.



Indirizzo IP Catalyst Center

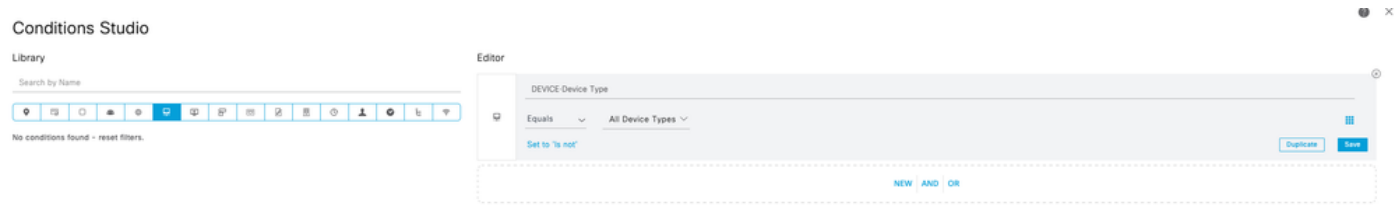
1.3 In Protocolli consentiti/Sequenza server selezionare Amministratore predefinito dispositivo.



Seleziona amministratore di dispositivo predefinito

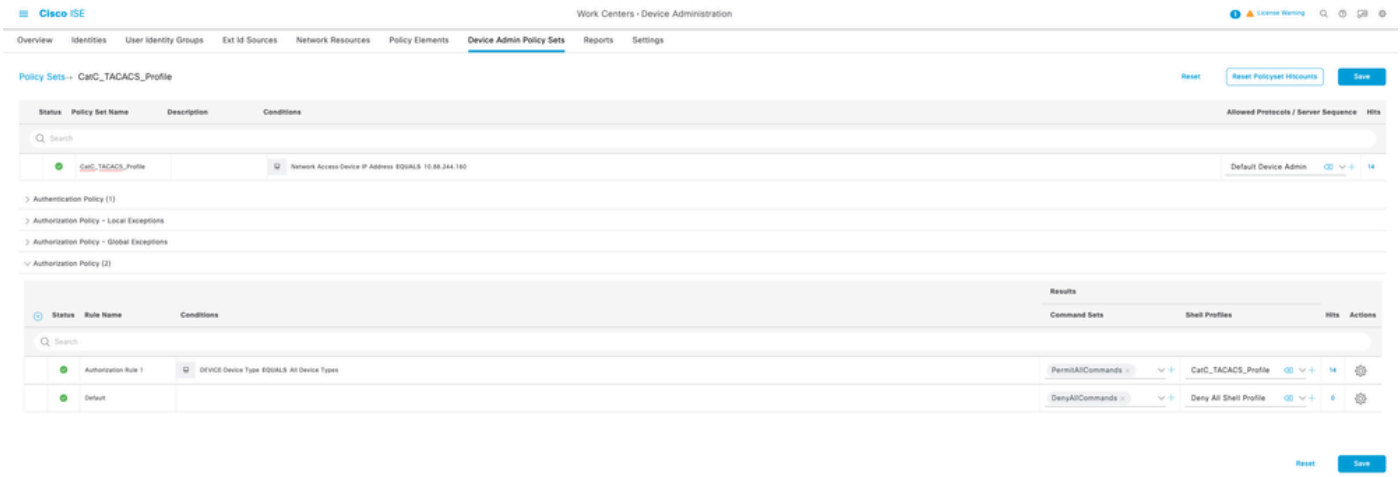
2. Configurare il set di criteri.

- Fare clic sulla freccia (>) a destra per espandere e configurare il set di criteri.
- Aggiungere una nuova regola in Criteri di autorizzazione.
- Configurare la nuova regola nel modo seguente:
  - Nome: Inserire un nome descrittivo per la regola.
  - Condizione: Per questo esempio, la condizione corrisponde a All Device Types.



Tutti i tipi di dispositivo

- Set di comandi: Selezionare il set di comandi TACACS+ creato in precedenza.
- Profilo shell: Selezionare il profilo TACACS+ creato in precedenza.



Set di comandi TACACS+

Cisco Catalyst Center

Configurazione del server ISE/AAA

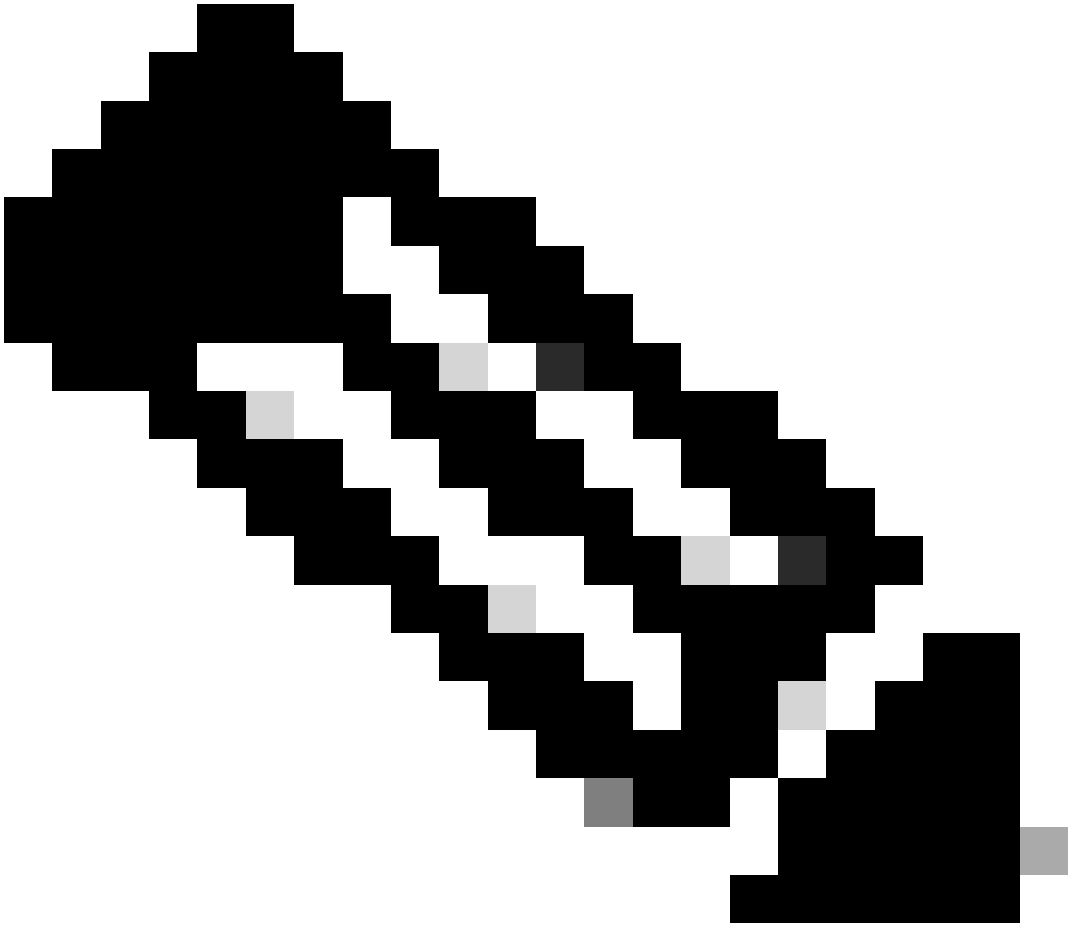
1. Accedere all'interfaccia Web del Catalyst Center.

- Accedere a:

Menu principale > Sistema > Impostazioni > Servizi esterni > Server di autenticazione e criteri

2. Aggiungere un nuovo server. È possibile selezionare ISE o AAA.

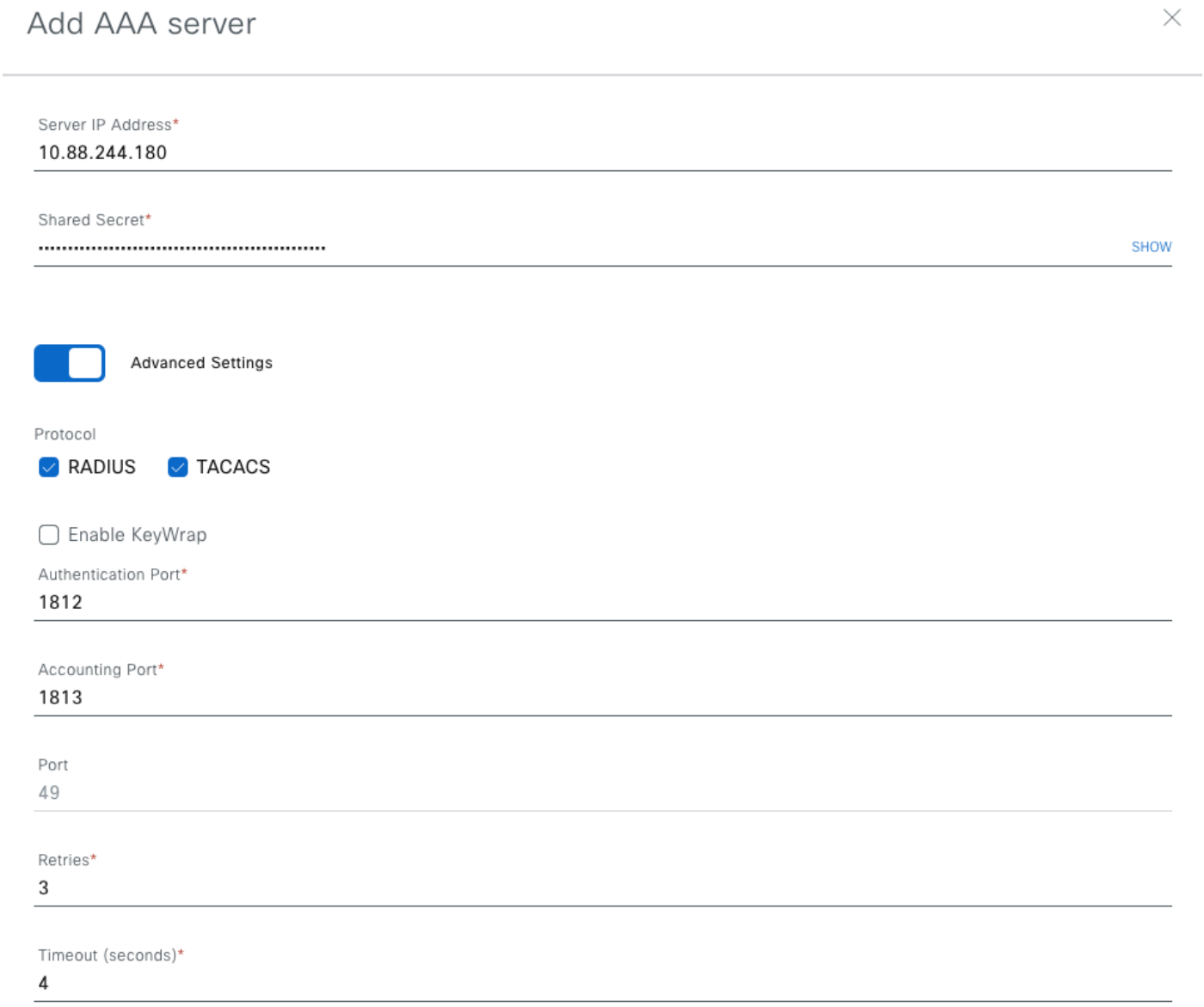
- Per questa demo, viene utilizzata l'opzione server AAA.



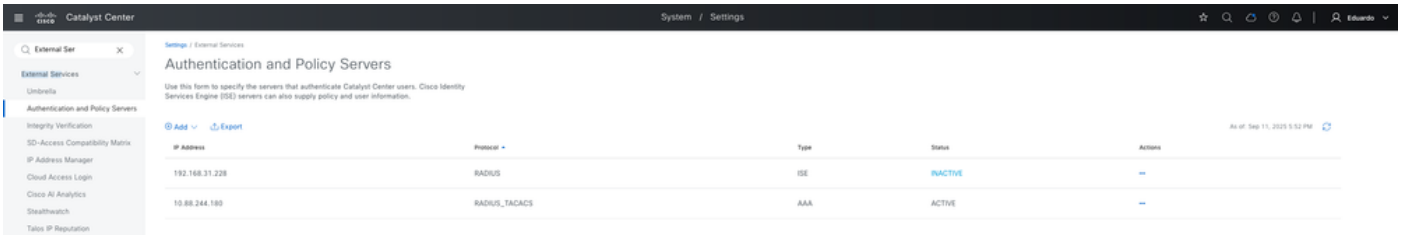
Nota: Per un cluster Catalyst Center può essere configurato un solo cluster ISE.

3. Configurare queste opzioni e quindi salvare:

- Immettere l'indirizzo IP del server AAA.
- Aggiungere il segreto condiviso (lo stesso segreto configurato nella risorsa di rete Cisco ISE).
- Attiva/disattiva Impostazioni avanzate su Attivato.
- Selezionare l'opzione TACACS.



Server di autenticazione e policy



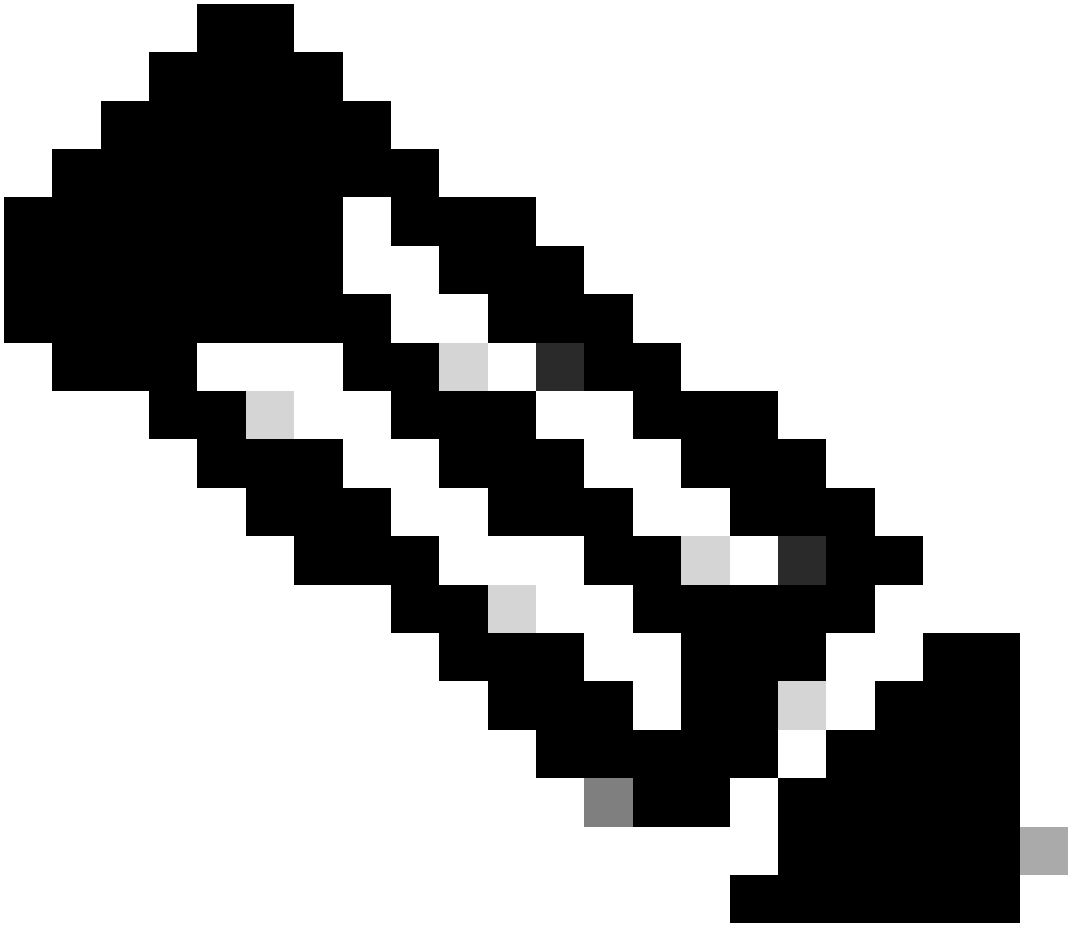
Impostazioni avanzate

Attivare e configurare l'autenticazione esterna.

1. Passare alla pagina Autenticazione esterna:

   Menu principale > Sistema > Utente e ruolo > Autenticazione esterna

2. Aggiungere l'attributo AAA cisco-av-pair e fare clic su Update per salvare le modifiche.



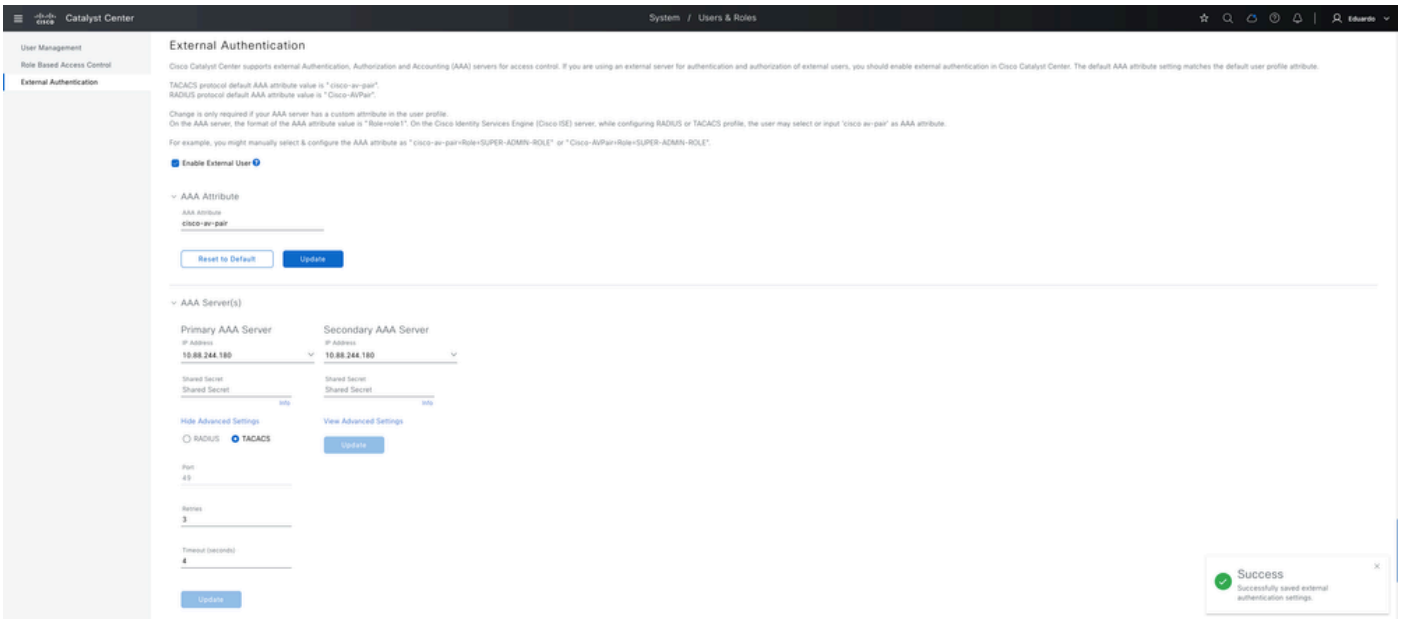
Nota: Questo passaggio non è obbligatorio in quanto l'attributo predefinito per TACACS+ è già cisco-av-pair, ma è considerata una best practice per configurarlo esplicitamente.

3. In Server AAA primario, selezionare il server AAA configurato precedentemente.

- Fare clic su Visualizza impostazioni avanzate per visualizzare opzioni aggiuntive.
- Selezionare l'opzione TACACS+.
- Immettere il segreto condiviso configurato nella risorsa di rete di Cisco ISE.
- Fare clic su Aggiorna per salvare le modifiche.

4. Selezionare la casella di controllo Utente esterno.

- Questa azione consente di salvare automaticamente la configurazione.



Autenticazione esterna

Verifica

1. Aprire una nuova sessione del browser o usare la modalità Incognito ed accedere alla pagina Web Catalyst Center con l'account utente configurato in Cisco ISE.
2. Da Catalyst Center, verificare che l'accesso sia riuscito.

Log In Configurare Catalyst Center External Authentication TACACS con ISE

3. Da Cisco ISE, convalidare i log:

   Operazioni > TACACS > Live Log

- Stato autenticazione: Superato
- Stato autorizzazione: Superato

Registri attivi

4. In Dettagli autorizzazione, confronta con l'output successivo:

    - Testo messaggio: Amministrazione periferica: Autorizzazione della sessione completata
    - Tutti gli attributi di risposta: cisco-av-pair=Role=SUPER-ADMIN-ROLE

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attribues	
All Response Attribues	cisco-av-pair=Role=SUPER-ADMIN-ROLE

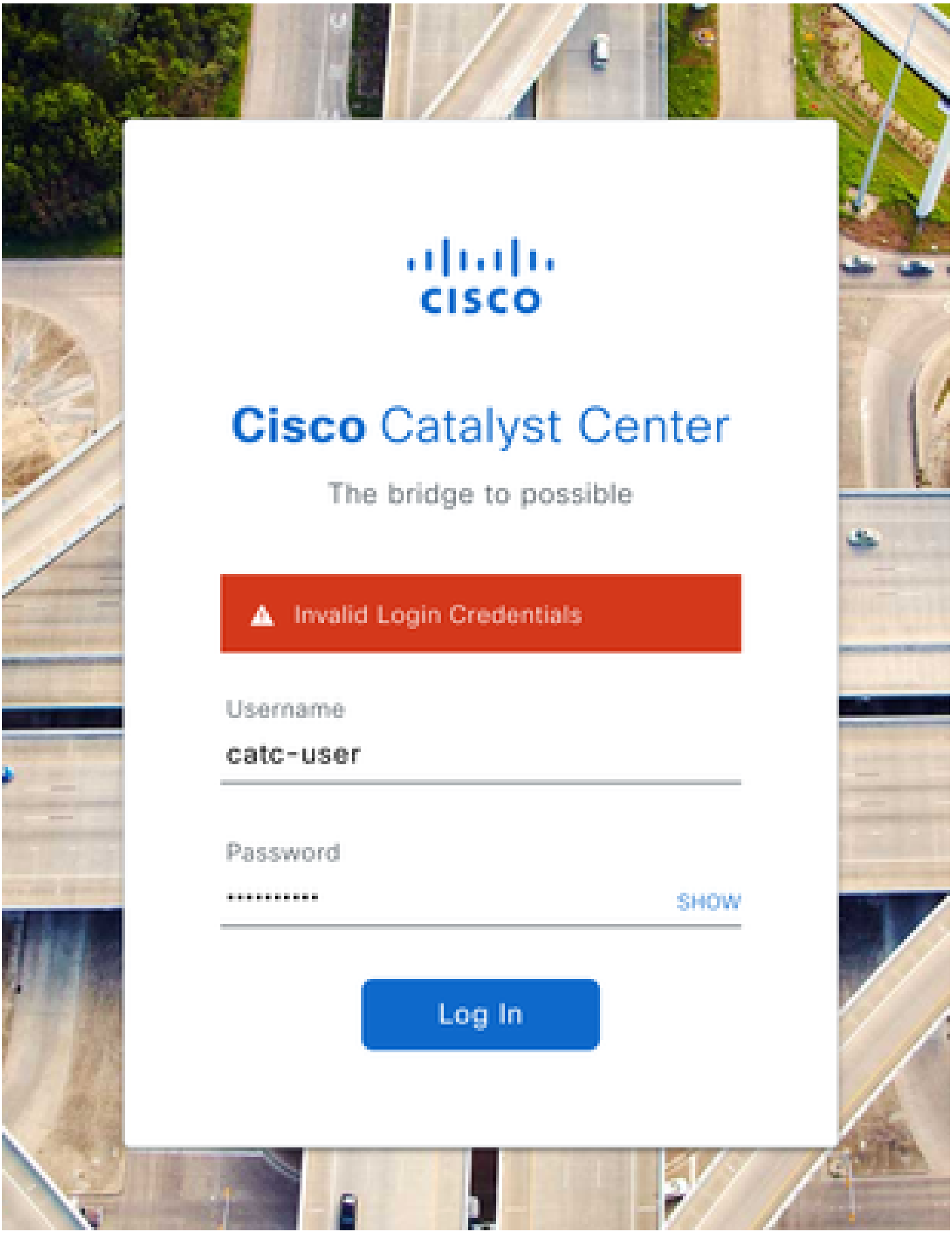
cisco-av-pair=Role=SUPER-ADMIN-ROLE

Risoluzione dei problemi

Di seguito sono riportati alcuni problemi comuni che è possibile incontrare durante l'integrazione e come identificarli:

1. Configurazione errata degli attributi

Sintomo in Catalyst Center: credenziali di accesso non valide



Configurazione errata degli attributi

- Sintomo in Cisco ISE (TACACS Logs):

- Autenticazione: Superato
- Authorization: Superato

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device...	Network Device...	Device Type	Location	Device Port	Failure Reason	Remote Address	Matched Comm...	Shell Profile
Sep 12, 2025 12:12:20.801...	✓		catc-user	Authorization		CatC_TACACS_Profile >> Authoriz...	ise-mac1	Catalyst-Center_6	10.88.244.160	Device Type#All D...	Location#All Locati...	console		10.189.17.203		CatC_TACACS_Pr...
Sep 12, 2025 12:12:20.788...	✓		catc-user	Authentication	CatC_TACACS_Profile >> Default		ise-mac1	Catalyst-Center_6	10.88.244.160	Device Type#All D...	Location#All Locati...	console		10.189.17.203		

Configurazione errata degli attributi

- Possibili cause:
  - Spazio nel valore dell'attributo.

Esempio:

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attribues	
All Response Attribues	cisco-av-pair=Role=SUPER-ADMIN-ROLE

Configurazione errata degli attributi

- L'attributo non è configurato correttamente, la parola chiave Role= è mancante.

  Esempio:

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attribues	
All Response Attribues	cisco-av-pair=Role=SUPER-ADMIN-ROLE

Configurazione errata degli attributi

2. Mancata corrispondenza del segreto condiviso

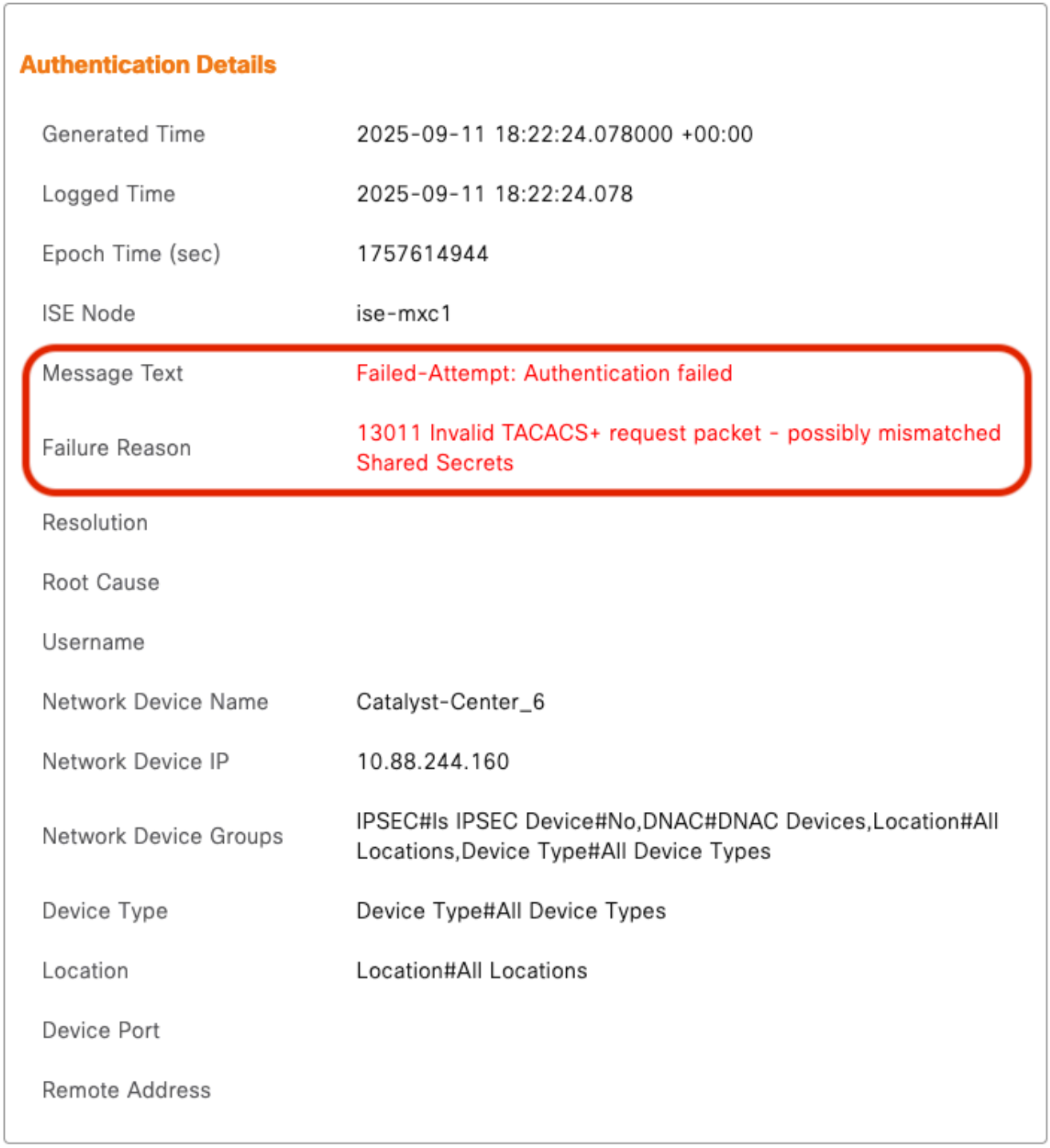
- Sintomo: I pacchetti di autenticazione hanno esito negativo tra Catalyst Center e Cisco ISE.

- Possibile causa: Il segreto condiviso configurato nella risorsa di rete di ISE non corrisponde a quello configurato nella pagina Catalyst Center > Autenticazione esterna.

Verifica:

- Controllare la configurazione delle risorse di rete in ISE.
- Confrontare il segreto condiviso con la configurazione in Catalyst Center > Autenticazione esterna.

Esempio:



Authentication Details

Generated Time	2025-09-11 18:22:24.078000 +00:00
Logged Time	2025-09-11 18:22:24.078
Epoch Time (sec)	1757614944
ISE Node	ise-mxc1
Message Text	Failed-Attempt: Authentication failed
Failure Reason	13011 Invalid TACACS+ request packet - possibly mismatched Shared Secrets
Resolution	
Root Cause	
Username	
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	
Remote Address	

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).