

Configurazione di TACACS di autenticazione esterna Catalyst Center con ISE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Cisco Identity Services Engine \(ISE\)](#)

[Licenza e abilitazione dei servizi TACACS+](#)

[Crea utente amministratore e aggiungi dispositivo di rete](#)

[Configura profilo TACACS+](#)

[Configurare le policy TACACS+](#)

[Cisco Catalyst Center](#)

[Configurazione del server ISE/AAA](#)

[Attivare e configurare l'autenticazione esterna.](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[1. Configurazione errata degli attributi](#)

[2. Mancata corrispondenza del segreto condiviso](#)

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).

Tier Essential Advantage Premier Device Admin

Virtual Appliance ISE VM License

This enables the ISE features for the purchased licenses to be tracked by Cisco Smart Licensing.

By clicking Register you will agree to the Terms&Conditions. You can download Terms&Conditions on [Smart Licensing Resources](#).

[Reset](#)

[Update](#)

Amministratore del dispositivo

<input type="checkbox"/>	Premier	Enabled	Released Entitlement	0	-	Dec 27,2024 18:16:00 PM
<input type="checkbox"/>	Device Admin	Enabled	In Compliance	1	-	Sep 11,2025 20:53:12 PM
∨ Virtual Appliance						
	ISE VM License	Enabled	In Compliance	1	-	Sep 11,2025 20:53:12 PM

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.

Deployment Nodes List > ise-mxc1

Edit Node

General Settings Profiling Configuration

Hostname: ise-mxc1
FQDN: ise-mxc1.cisco.com
IP Address: 10.88.244.180
Node Type: Identity Services Engine (ISE)

Role: STANDALONE [Make Primary](#)

Administration

> Monitoring

Policy Service

- Enable Session Services ⓘ
Include Node in Node Group: None ⓘ
- Enable Profiling Service ⓘ
- Enable Threat Centric NAC Service ⓘ
- > Enable SXP Service ⓘ
- Enable Device Admin Service ⓘ**
- Enable Passive Identity Service ⓘ

> pxGrid ⓘ

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).

The screenshot shows the Cisco ISE interface for configuring a Network Device. The device name is 'Catalyst-Center_6'. The IP address is set to 10.88.244.160 / 32. The device profile is 'Cisco'. The 'TACACS Authentication Settings' section is highlighted with a red box and contains the following configuration:

- TACACS Authentication Settings
 - Shared Secret: Show Retire
 - Enable Single Connect Mode
 - Legacy Cisco Device
 - TACACS Draft Compliance Single Connect Support

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.

Cisco ISE Work Centers - Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources **Policy Elements** Device Admin Policy Sets Reports Settings

TACACS Profiles > CatC_TACACS_Profile
TACACS Profile

Name
 CatC_TACACS_Profile

Description
 Catalyst Center External Authentication

Task Attribute View **Raw View**

Common Tasks

Common Task Type **Shell**

Default Privilege _____ (Select 0 to 15)

Maximum Privilege _____ (Select 0 to 15)

Access Control List _____

Auto Command _____

No Escape _____ (Select true or false)

Timeout _____ Minutes (0-9999)

Idle Time _____ Minutes (0-9999)

Custom Attributes

Add Trash Edit

Type	Name	Value
<input type="checkbox"/> MANDATORY	cisco-av-pair	Role=SUPER-ADMIN-ROLE

Cancel Save

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.

The screenshot shows the Cisco ISE interface for configuring a TACACS Command Set. The breadcrumb trail is: TACACS Command Sets > PermitAllCommands. The page title is "Command Set". The "Name" field is filled with "PermitAllCommands". The "Description" field is empty. Under the "Commands" section, the checkbox "Permit any command that is not listed below" is checked. Below this, there are buttons for "Add", "Trash", "Edit", "Move Up", and "Move Down". A table with columns "Grant", "Command", and "Arguments" is shown, but it is empty with the text "No data found." at the bottom. At the bottom right, there are "Cancel" and "Save" buttons.

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

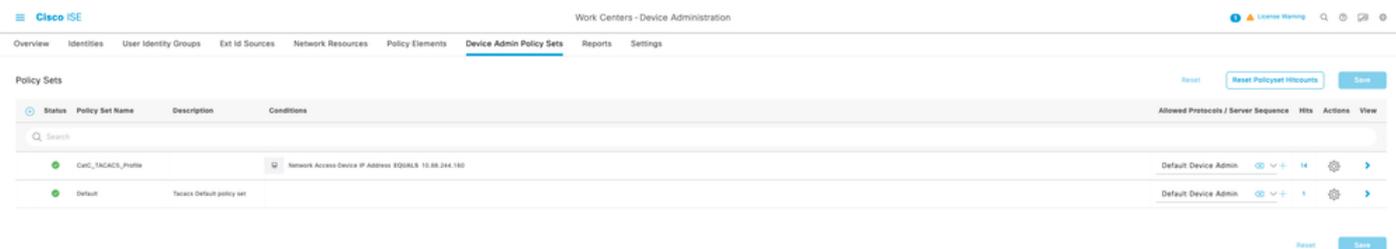
- Aggiungere un nome per il set di criteri.
- Configurare la condizione.
 - Nell'esempio, la condizione corrisponde all'indirizzo IP del Catalyst Center.

Conditions Studio



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.

Conditions Studio



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.

The screenshot displays the Cisco ISE Device Administration interface. The top navigation bar includes 'Overview', 'Identities', 'User Identity Groups', 'Ext ID Sources', 'Network Resources', 'Policy Elements', 'Device Admin Policy Sets', 'Reports', and 'Settings'. The main content area is titled 'Policy Sets - CatC_TACACS_Profile'. It features a search bar and a table with columns for 'Status', 'Policy Set Name', 'Description', and 'Conditions'. Below this, there are sections for 'Authentication Policy (1)', 'Authorization Policy - Local Exceptions', 'Authorization Policy - Global Exceptions', and 'Authorization Policy (2)'. The 'Authorization Policy (2)' section contains a table with columns for 'Status', 'Rule Name', 'Conditions', 'Results', 'Command Sets', 'Shell Profiles', 'Hits', and 'Actions'. The table lists two rules: 'Authorization Rule 1' and 'Default'.

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.

Add AAA server



Server IP Address*

10.88.244.180

Shared Secret*

.....

[SHOW](#)



Advanced Settings

Protocol

RADIUS TACACS

Enable KeyWrap

Authentication Port*

1812

Accounting Port*

1813

Port

49

Retries*

3

Timeout (seconds)*

4

Server di autenticazione e policy

The screenshot shows the 'Authentication and Policy Servers' configuration page in Catalyst Center. It includes a table with the following data:

IP Address	Protocol	Type	Status	Actions
192.168.31.228	RADIUS	ISE	INACTIVE	--
10.88.244.180	RADIUS_TACACS	AAA	ACTIVE	--

Impostazioni avanzate

Attivare e configurare l'autenticazione esterna.

1. Passare alla pagina Autenticazione esterna:

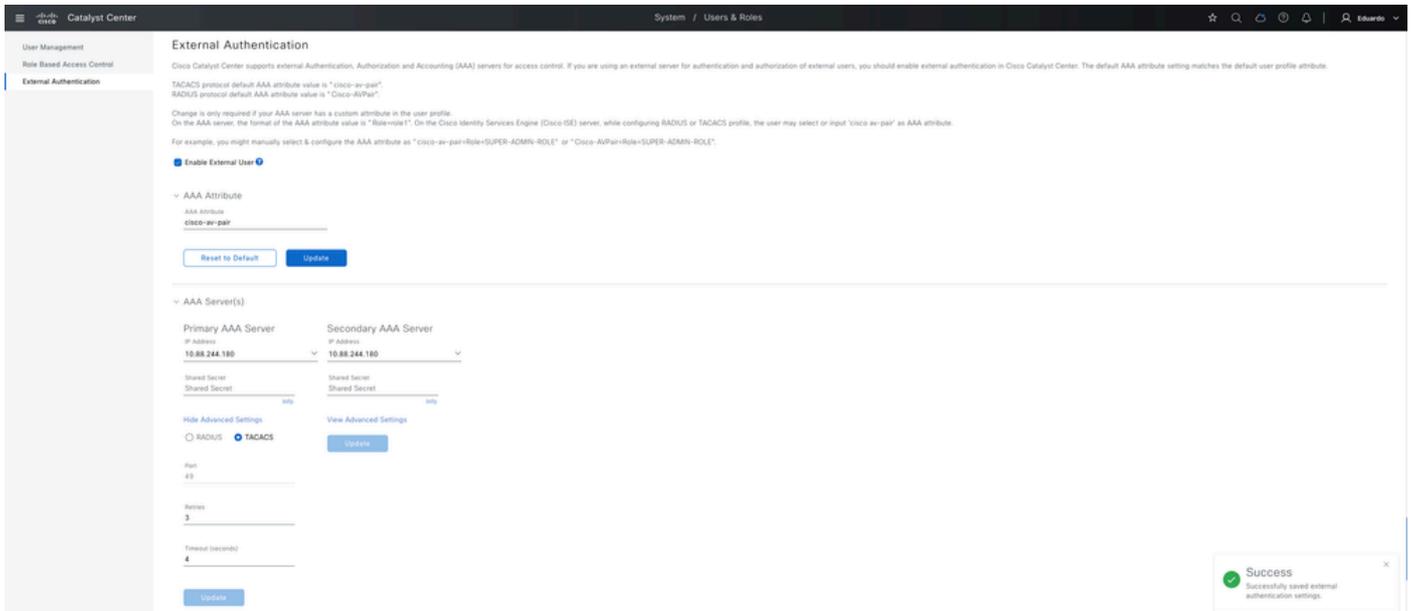
Menu principale > Sistema > Utente e ruolo > Autenticazione esterna

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.

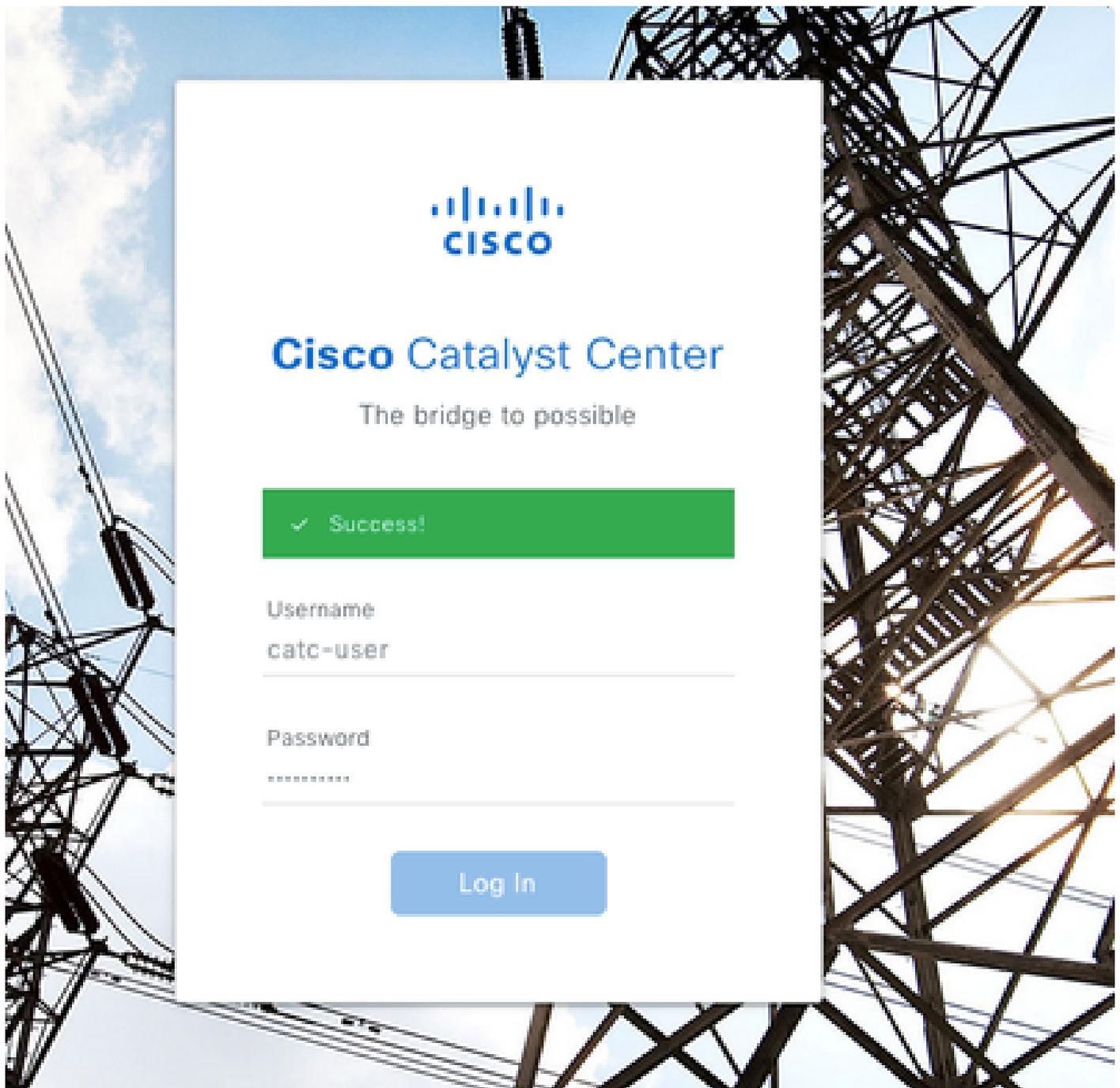
-
3. In Server AAA primario, selezionare il server AAA configurato precedentemente.
 - Fare clic su Visualizza impostazioni avanzate per visualizzare opzioni aggiuntive.
 - Selezionare l'opzione TACACS+.
 - Immettere il segreto condiviso configurato nella risorsa di rete di Cisco ISE.
 - Fare clic su 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

Live Logs

Refresh Never Show Latest 20 records Within Last 3 hours Filter

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Isa Node	Network Device...	Network Device...	Device Type	Location	Device Port	Failure Reason	Remote Address	Matched Comm...	Shell Profile
Sep 12, 2025 12:12:20.851...			isa01-user	Authentication	CatC_TACACS_Profile >> Authn...	CatC_TACACS_Profile >> Authori...	isa-mac1	Catalyst-Centr_8	10.88.244.160	Device Type680 D...	Location&M Locat...	console		10.189.17.203	Matched Command	CatC_TACACS_P...
Sep 12, 2025 12:12:20.798...			isa01-user	Authentication	CatC_TACACS_Profile >> Default		isa-mac1	Catalyst-Centr_8	10.88.244.160	Device Type680 D...	Location&M Locat...	console		10.189.17.203		

Last Updated: Thu Sep 11 2025 18:14:58 GMT-0600 (Central Standard Time) Records Shown: 2

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 Attributes	
All Response Attributes	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



Cisco Catalyst Center

The bridge to possible

 Invalid Login Credentials

Username

catc-user

Password

.....

[SHOW](#)

Log In

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 12:12:25.861...	■		catc-user	Authorization	CatC_TACACS_Profile >> Authoriz...	CatC_TACACS_Profile >> Authoriz...	ise-mst1	Catalyst-Center_8	10.88.244.180	Device Type:AAA D...	Location:AAA Local...	console		10.188.17.203		CatC_TACACS_Pt...
Sep 12, 2025 12:12:26.788...	■		catc-user	Authentication	CatC_TACACS_Profile >> Default		ise-mst1	Catalyst-Center_8	10.88.244.180	Device Type:AAA D...	Location:AAA Local...	console		10.188.17.203		

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 Attributes

All Response Attributes 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 Attributes

All Response Attributes 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

Mancata Corrispondenza Del Segreto Condiviso

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).