Configure Catalyst Center External Authentication TACACS with ISE

Contents

Introduction

This document describes the steps required to integrate Cisco Identity Services Engine with Catalyst Center to enable TACACS+ authentication.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Administrator access to both Cisco ISE and Cisco Catalyst Center.
- Basic understanding of AAA (Authentication, Authorization, and Accounting) concepts.
- Working knowledge of TACACS+ protocol.
- Network connectivity between Catalyst Center and the ISE server.

Components Used

The information in this document is based on these hardware and software version:

- Cisco Catalyst Center version *2.3.7.x*
- Cisco Identity Services Engine (ISE) version *3.x* (or later)
- TACACS+ protocol for external user authentication

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This integration allows external users to log in to Catalyst Center for administrative access and management.

Configure

Cisco Identity Services Engine (ISE)

License and Enable the TACACS+ Services

Before you start with the TACACS+ configuration in ISE, you must confirm that the correct license is installed and the feature is enabled.

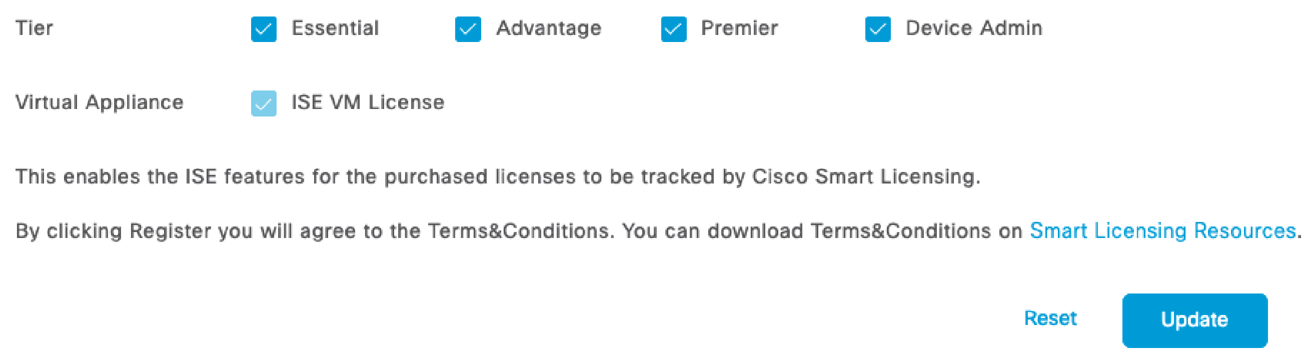
1. Verify that you have the PID license L-ISE-TACACS-ND= in the Cisco Smart Software Manage or Cisco License Central portal.

Enable Device Administration in the ISE Licensing portal.

- The Device Admin license (PID: L-ISE-TACACS-ND=) enables TACACS+ services on a Policy Service Node (PSN).
- Navigate to:

Administration > **System** > **Licensing**

- Check the box for **Device Admin** under the Tier options.



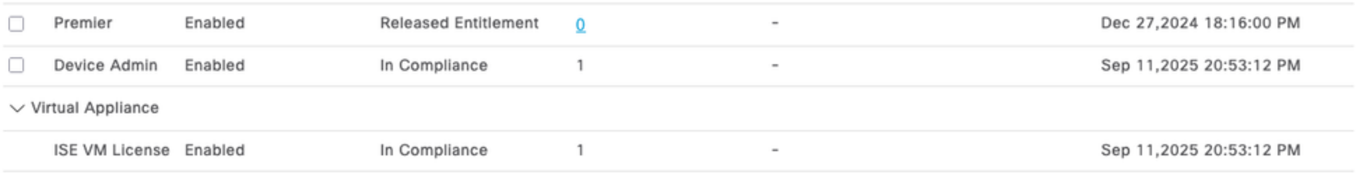
Tier ☑ Essential ☑ Advantage ☑ Premier ☑ Device Admin

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.

Device Admin



□	Premier	Enabled	Released Entitlement	0	-	Dec 27,2024 18:16:00 PM
□	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

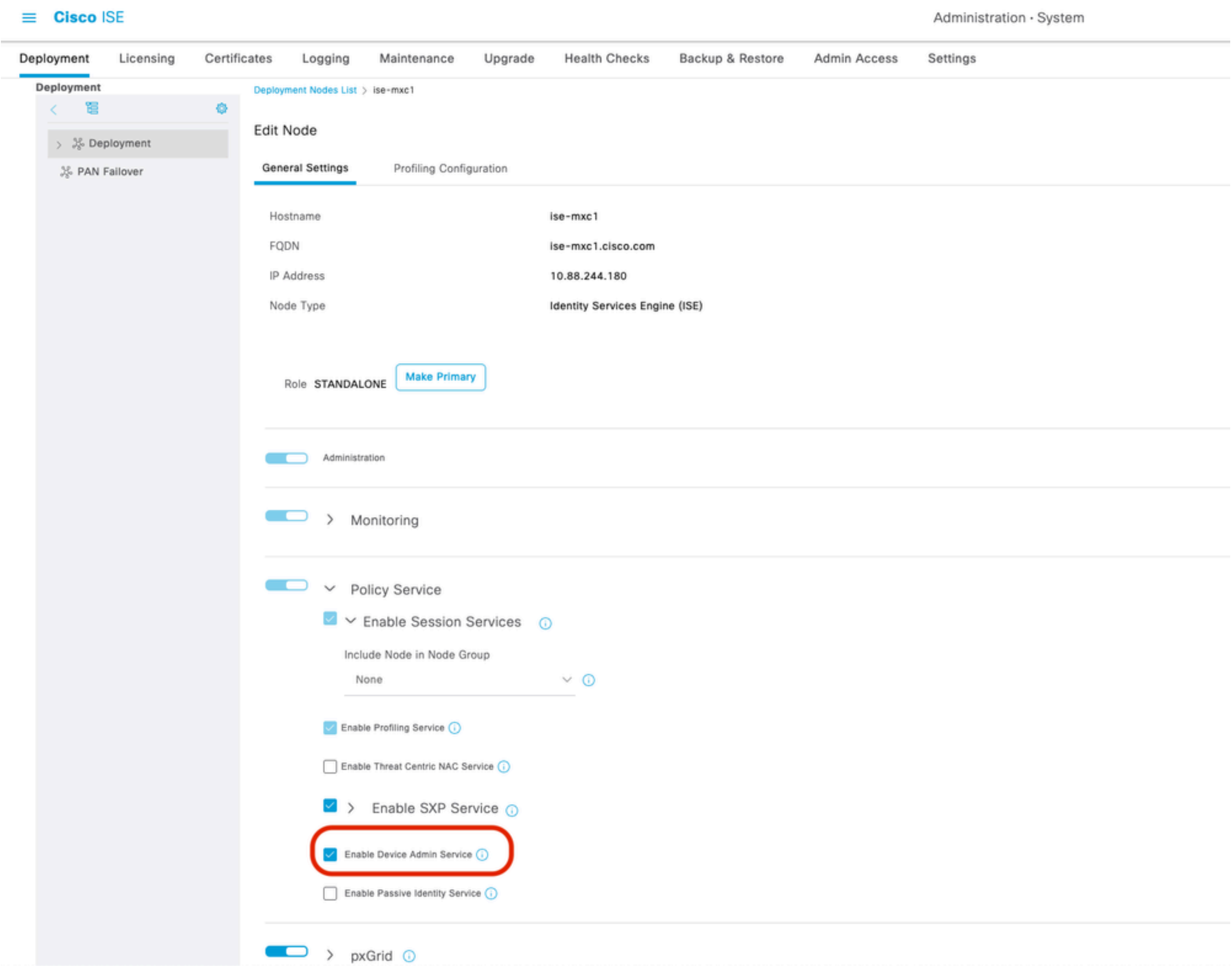
License Device Admin

3. Enable the **Device Admin Service** on the ISE node that runs the TACACS+ service.

- Navigate to:

  Administration > System > Deployment > Select the node

- Check the option **Enable Device Admin Service**.



≡ Cisco ISE — Administration · System

Deployment | Licensing | Certificates | Logging | Maintenance | Upgrade | Health Checks | Backup & Restore | Admin Access | Settings

Deployment

Deployment

PAN Failover

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

Enable Device Admin Service

Create Admin User and Add Network Device

1. Create the **Admin User**.

- This user account is used to log in to the **Catalyst Center UI** through ISE authentication.

- Navigate to:

  Work Centers > Network Access > Identities > Network Access User

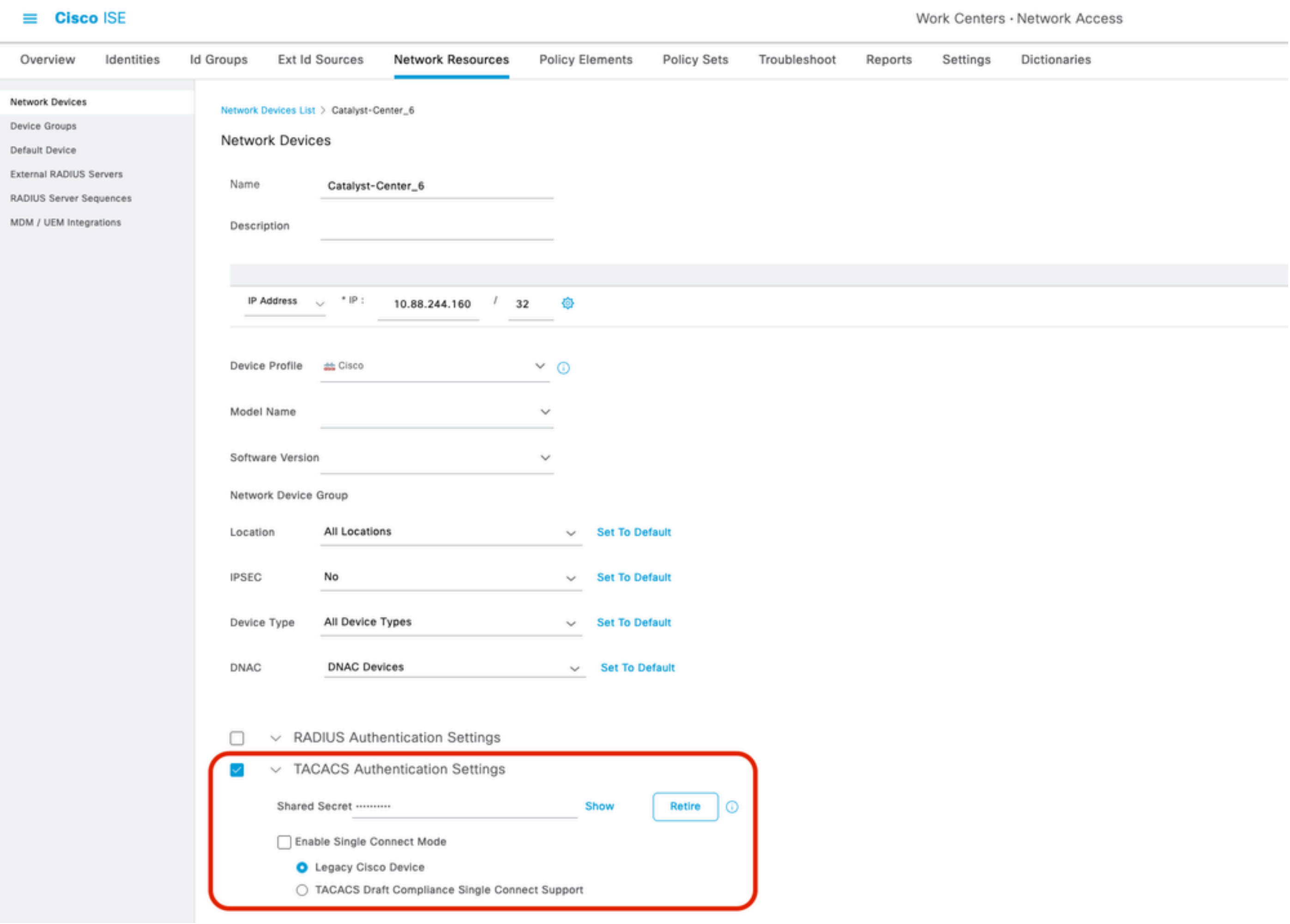
- Add a **new user** (for example, catc-user).
- If the user already exists, proceed to the next step.

2. Create the **Network Device**.

- Navigate to:

  Work Centers > Network Access > Identities > Network Resource

- Add the **IP address** of Catalyst Center, or define the **subnet** where the Catalyst Center IP is located.
- If the device already exists, verify that it contains the parameters:
  - TACACS Authentication Settings are enabled.
  - The **Shared Secret** is configured and known (save this value, as it is required later in Catalyst Center).



Network Devices

Name: Catalyst-Center_6

Description:

IP Address * IP : 10.88.244.160 / 32

Device Profile: Cisco

Model Name:

Software Version:

Network Device Group

Location: All Locations

IPSEC: No

Device Type: All Device Types

DNAC: DNAC Devices

□ RADIUS Authentication Settings

☑ TACACS Authentication Settings

Shared Secret ··········

□ Enable Single Connect Mode

● Legacy Cisco Device

○ TACACS Draft Compliance Single Connect Support

TACACS Authentication Settings

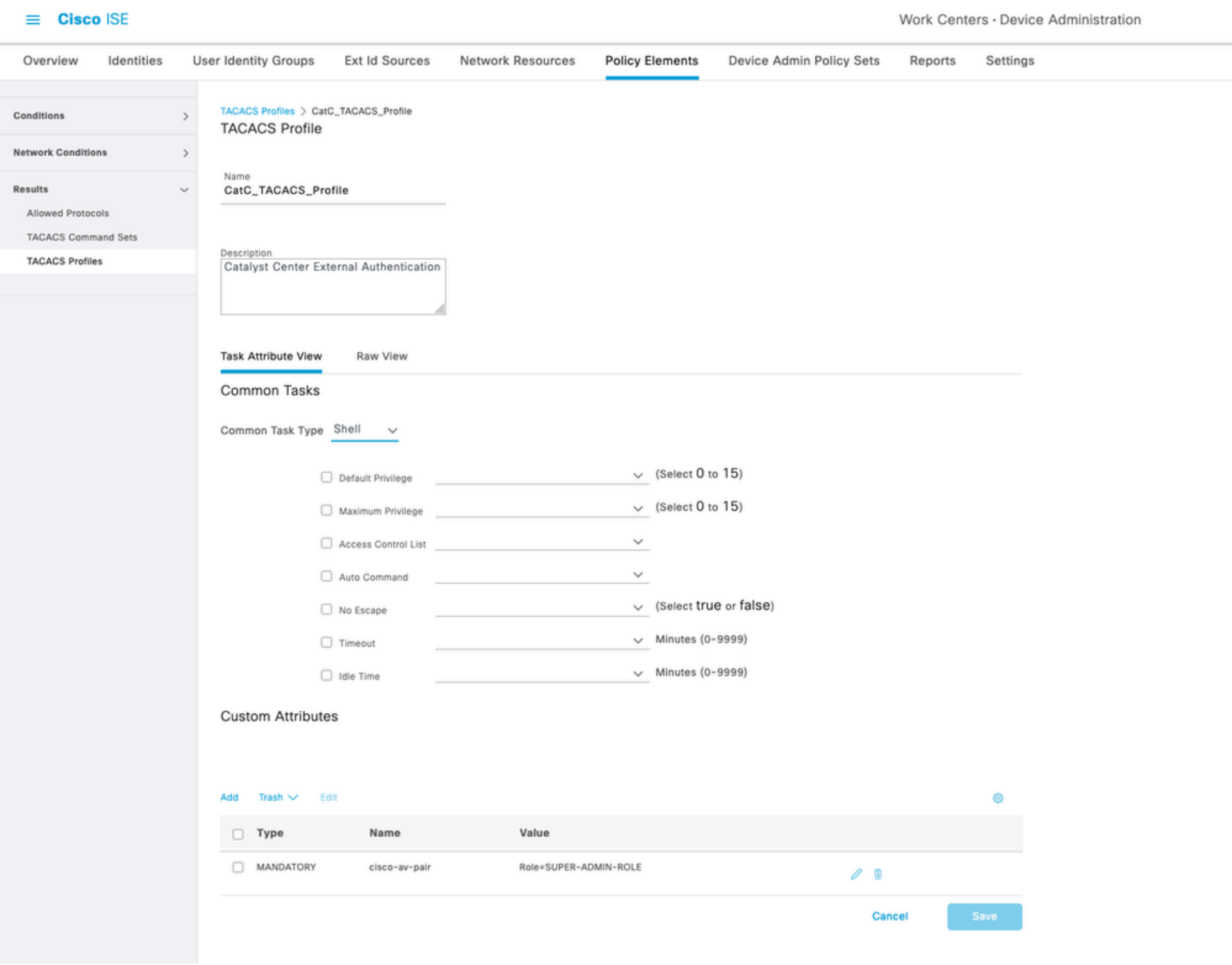
Configure TACACS+ Profile

1. Create a New **TACACS+ Profile**.

- Navigate to:

  Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles

- Add a **profile name**.
- Add a **Custom Attribute** as follows:
  - **Type:** Mandatory
  - **Name:** cisco-av-pair
  - **Value:** Role=SUPER-ADMIN-ROLE
- Save the **profile**.



Name: CatC_TACACS_Profile

Description: Catalyst Center External Authentication

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)

□	Type	Name	Value
□	MANDATORY	cisco-av-pair	Role=SUPER-ADMIN-ROLE

TACACS+ Profile

Note: Cisco Catalyst Center supports external Authentication, Authorization and Accounting (AAA) servers for access control. If you are using an external server for authentication and authorization of external users, you can enable external authentication in Cisco Catalyst Center. The default AAA attribute setting matches the default user profile attribute.

TACACS protocol default AAA attribute value is cisco-av-pair.

RADIUS protocol default AAA attribute value is Cisco-AVPair.

Change is only required if your AAA server has a custom attrribute in the user profile. On the AAA server, the format of the AAA attribute value is Role=role1. On the Cisco Identity Services Engine (Cisco ISE) server, while configuring RADIUS or TACACS profile, the user can select or input cisco av-pair as AAA attribute.

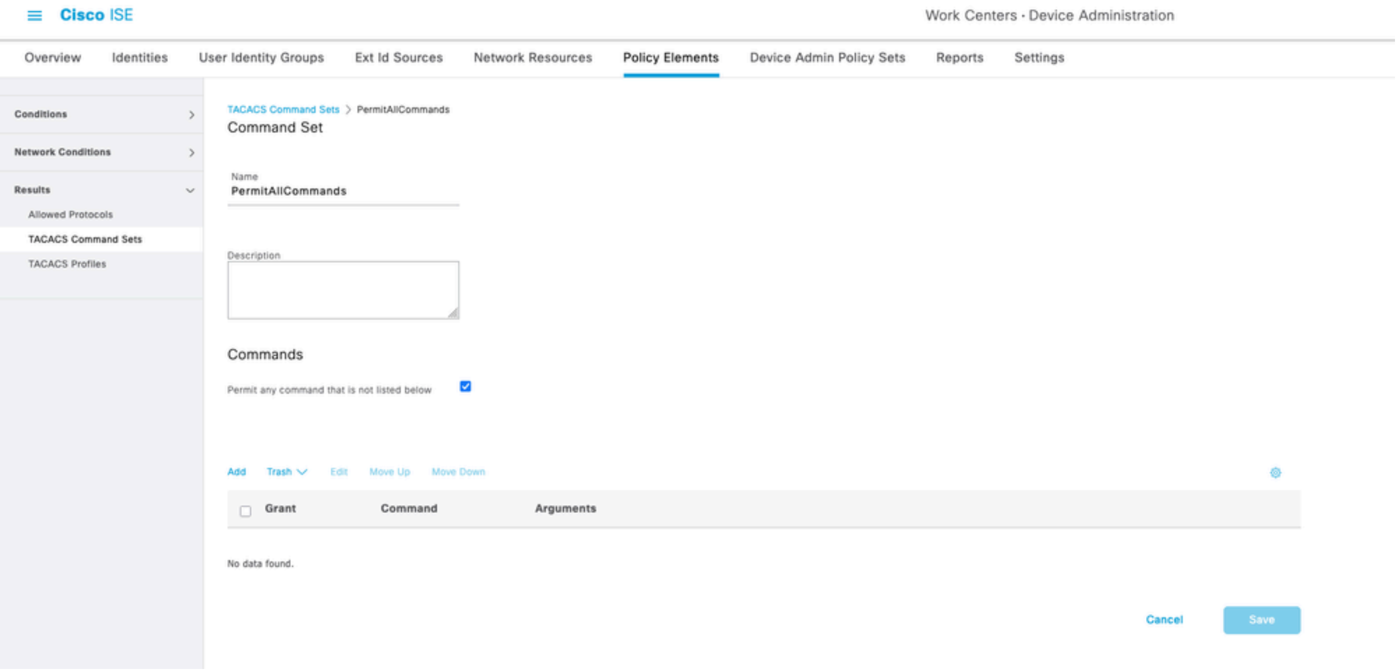
For example, you can manually select & configure the AAA attribute as cisco-av-pair=Role=SUPER-ADMIN-ROLE or Cisco-AVPair=Role=SUPER-ADMIN-ROLE.

2. Create a **TACACS+ Command Set**.

- Navigate to:

Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets

- Add a **name**.
- Check the option **Permit any command that is not listed below**.
- Save the **Command Set**.



Command Set

Name: PermitAllCommands

Description:

Commands

Permit any command that is not listed below ☑

□ Grant	Command	Arguments

No data found.

TACACS Command Sets

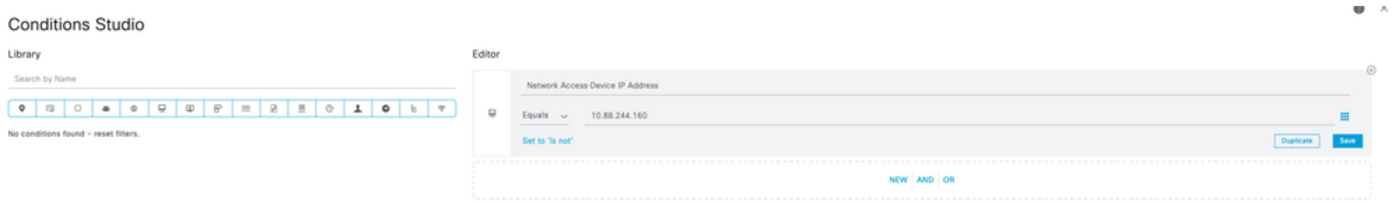
Configure TACACS+ Policies

1. Create a New **TACACS+ Policy Set**.

- Navigate to:

Work Centers > Device Administration > Device Admin Policy Set

- Add a **name** for the Policy Set.
- Configure the **Condition**.
  - In this example, the condition matches the **Catalyst Center IP address**.

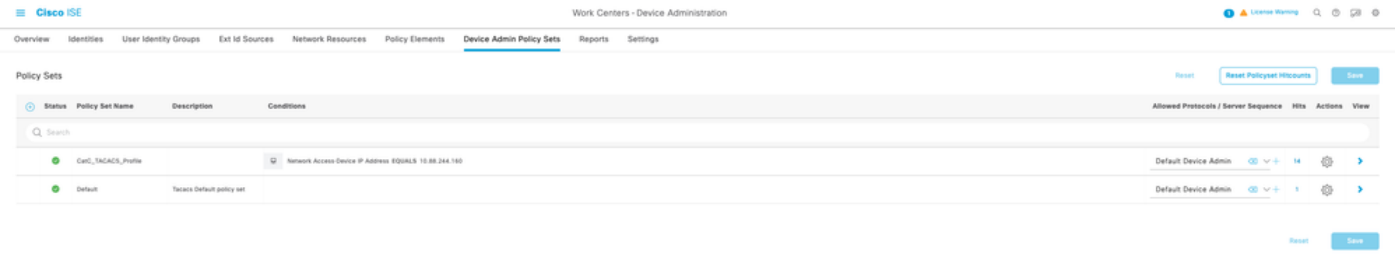


Network Access·Device IP Address

Equals 10.88.244.160

Catalyst Center IP address

1.3 On the Allowed Protocols / Server Sequence Select Default Device Admin.



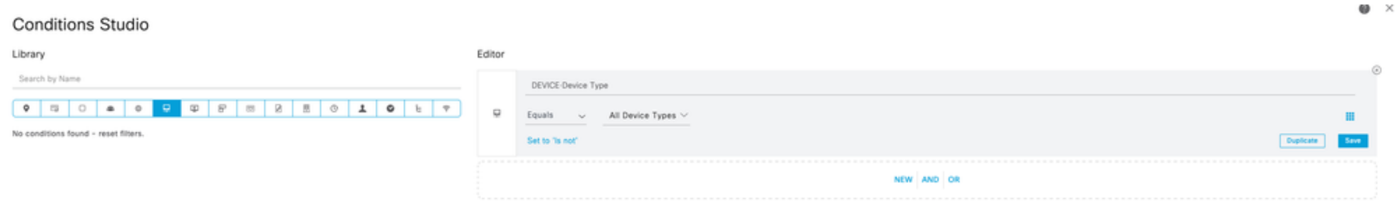
Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	CatC_TACACS_Profile		Network Access Device IP Address EQUALS 10.88.244.160	Default Device Admin	14	⚙	>
●	Default	Tacacs Default policy set		Default Device Admin	1	⚙	>

Select Default Device Admin

2. Configure the **Policy Set**.

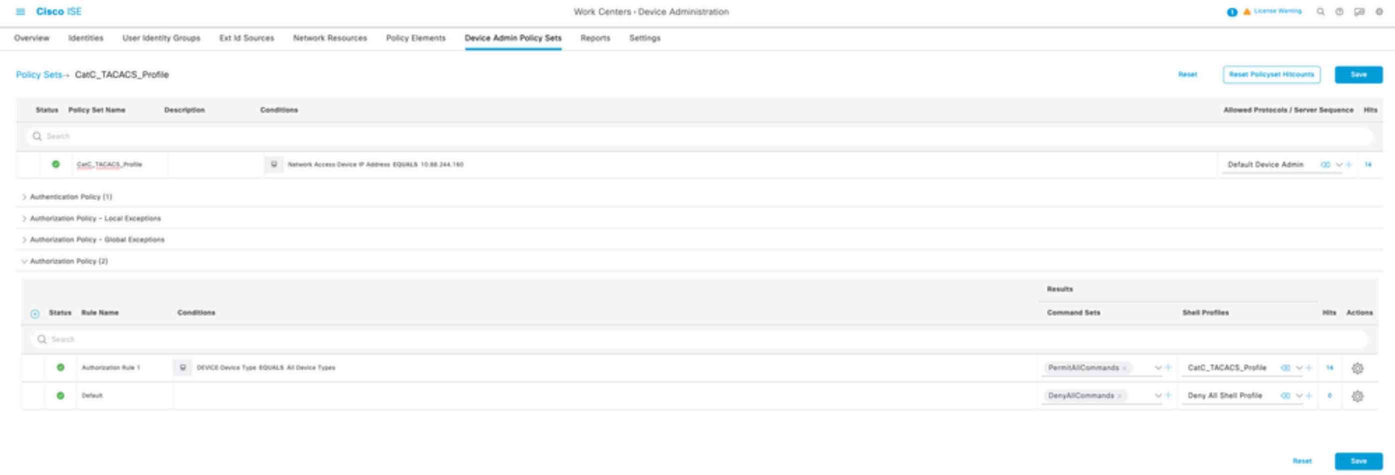
- Click the **arrow (>)** on the right to expand and configure the Policy Set.
- Add a new **Rule** under **Authorization Policy**.
- Configure the new rule as follows:
    - **Name:** Enter a descriptive rule name.
    - **Condition:** For this example, the condition matched All Device Types.



DEVICE·Device Type
Equals All Device Types
Set to 'Is not'

All Device Types

- **Command Set:** Select the **TACACS+ Command Set** created earlier.
- **Shell Profile:** Select the **TACACS+ Profile** created earlier.



Policy Sets→ CatC_TACACS_Profile

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	CatC_TACACS_Profile		Network Access Device IP Address EQUALS 10.88.244.160	Default Device Admin	14

> Authentication Policy (1)
> Authorization Policy - Local Exceptions
> Authorization Policy - Global Exceptions
∨ Authorization Policy (2)

			Results			
Status	Rule Name	Conditions	Command Sets	Shell Profiles	Hits	Actions
●	Authorization Rule 1	DEVICE·Device Type EQUALS All Device Types	PermitAllCommands	CatC_TACACS_Profile	14	⚙
●	Default		DenyAllCommands	Deny All Shell Profile	0	⚙

TACACS+ Command Set

Cisco Catalyst Center

Configure the ISE / AAA Server

1. Log in to the **Catalyst Center** web interface.

- Navigate to:

Main menu > System > Settings > External Services > Authentication and Policy Servers

2. Add a **new server**. You can select either **ISE** or **AAA**.

- For this demo, the **AAA server** option is used.

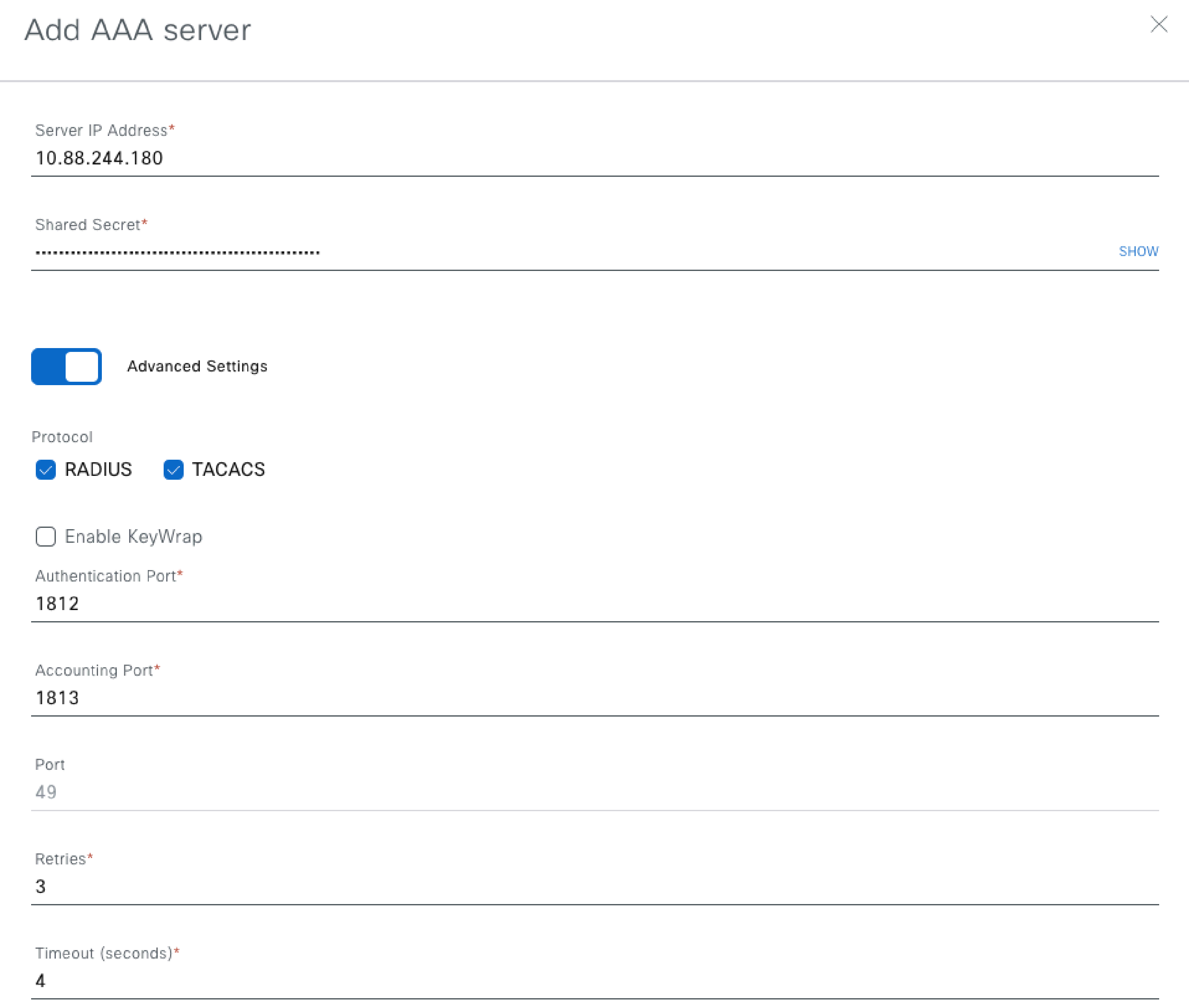
Note: A Catalyst Center cluster can have only one ISE cluster configured.

---

3. Configure these options and then save:

- Enter the **IP address** of the AAA server.
- Add the **Shared Secret** (the same secret configured in the Cisco ISE Network Resource).
- Toggle **Advanced Settings** to **On**.

- Check the **TACACS** option.



Add AAA server

Server IP Address*
10.88.244.180

Shared Secret*
••• SHOW

Advanced Settings

Protocol
☑ RADIUS ☑ TACACS

□ Enable KeyWrap

Authentication Port*
1812

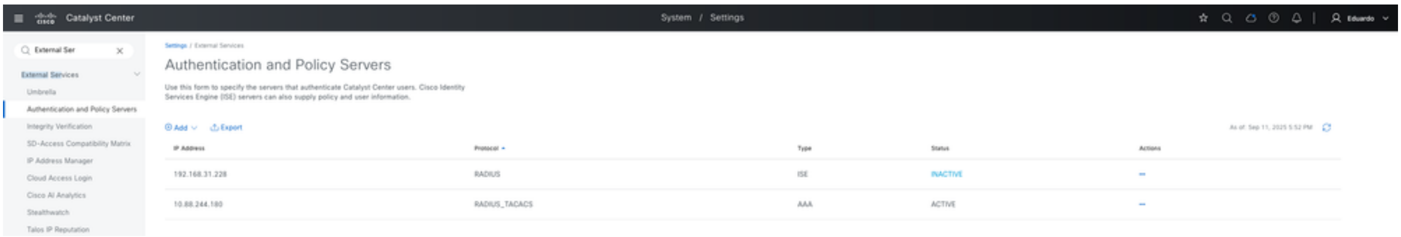
Accounting Port*
1813

Port
49

Retries*
3

Timeout (seconds)*
4

Authentication and Policy Servers



Authentication and Policy Servers

Use this form to specify the servers that authenticate Catalyst Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

As of: Sep 11, 2025 5:52 PM

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

Advanced Settings

Enable and Configure the External Authentication.

1. Navigate to the **External Authentication** page:

Main menu > System > User & Role > External Authentication

2. Add the AAA attribute **cisco-av-pair** and click **Update** to save the changes.

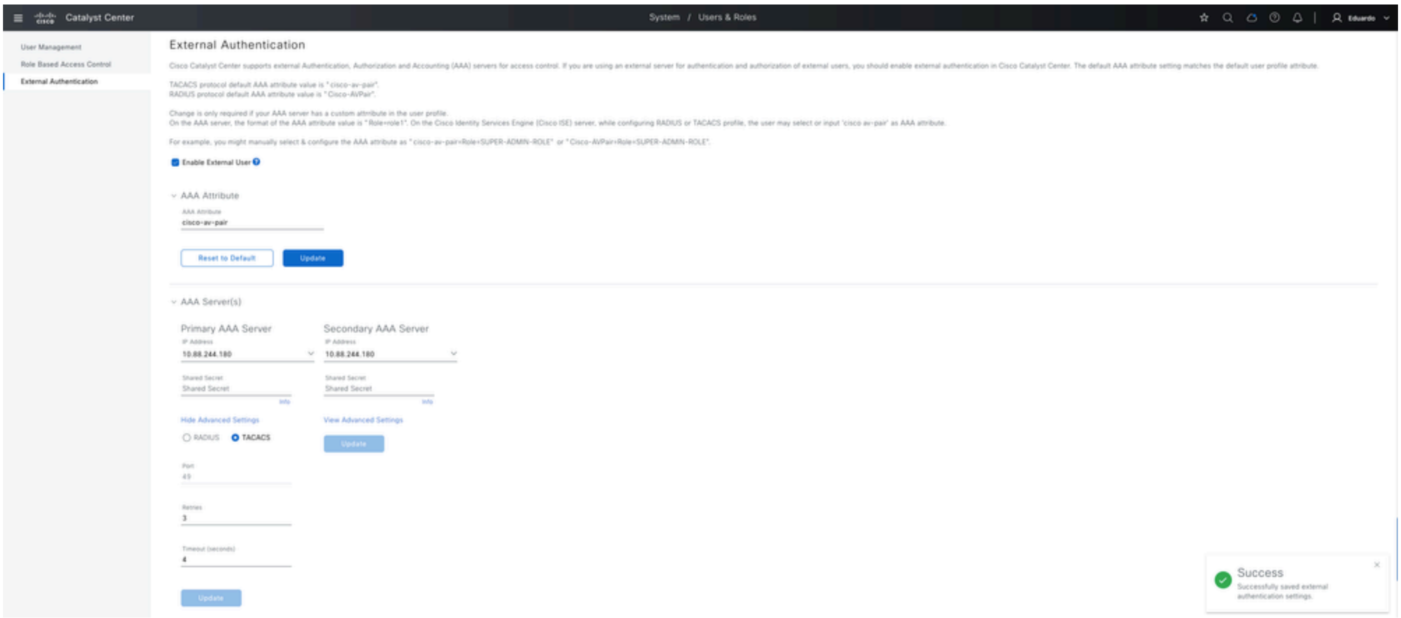
Note: This step is not mandatory since the default attribute for TACACS+ is already cisco-av-pair, but it is considered a best practice to configure it explicitly.

3. Under **Primary AAA Server**, select the **AAA server** configured earlier.

- Click **View Advanced Settings** to display additional options.
- Select the **TACACS+** option.
- Enter the **Shared Secret** configured in Cisco ISE’s Network Resource.
- Click **Update** to save the changes.

4. Enable the **External User** checkbox.

- This action automatically saves the configuration.



External Authentication

Cisco Catalyst Center supports external Authentication, Authorization and Accounting (AAA) servers for access control. If you are using an external server for authentication and authorization of external users, you should enable external authentication in Cisco Catalyst Center. The default AAA attribute setting matches the default user profile attribute.

TACACS protocol default AAA attribute value is "cisco-av-pair".
RADIUS protocol default AAA attribute value is "Cisco-AVPair".

Change is only required if your AAA server has a custom attribute in the user profile.
On the AAA server, the format of the AAA attribute value is "Role=role1". On the Cisco Identity Services Engine (Cisco ISE) server, while configuring RADIUS or TACACS profile, the user may select or input 'cisco av-pair' as AAA attribute.

For example, you might manually select & configure the AAA attribute as "cisco-av-pair=Role=SUPER-ADMIN-ROLE" or "Cisco-AVPair=Role=SUPER-ADMIN-ROLE".

☑ Enable External User

AAA Attribute

AAA Attribute: cisco-av-pair

AAA Server(s)

Primary AAA Server
IP Address: 10.88.244.180
Shared Secret: Shared Secret

○ RADIUS ● TACACS

Port: 49
Retries: 3
Timeout (seconds): 4

Secondary AAA Server
IP Address: 10.88.244.180
Shared Secret: Shared Secret

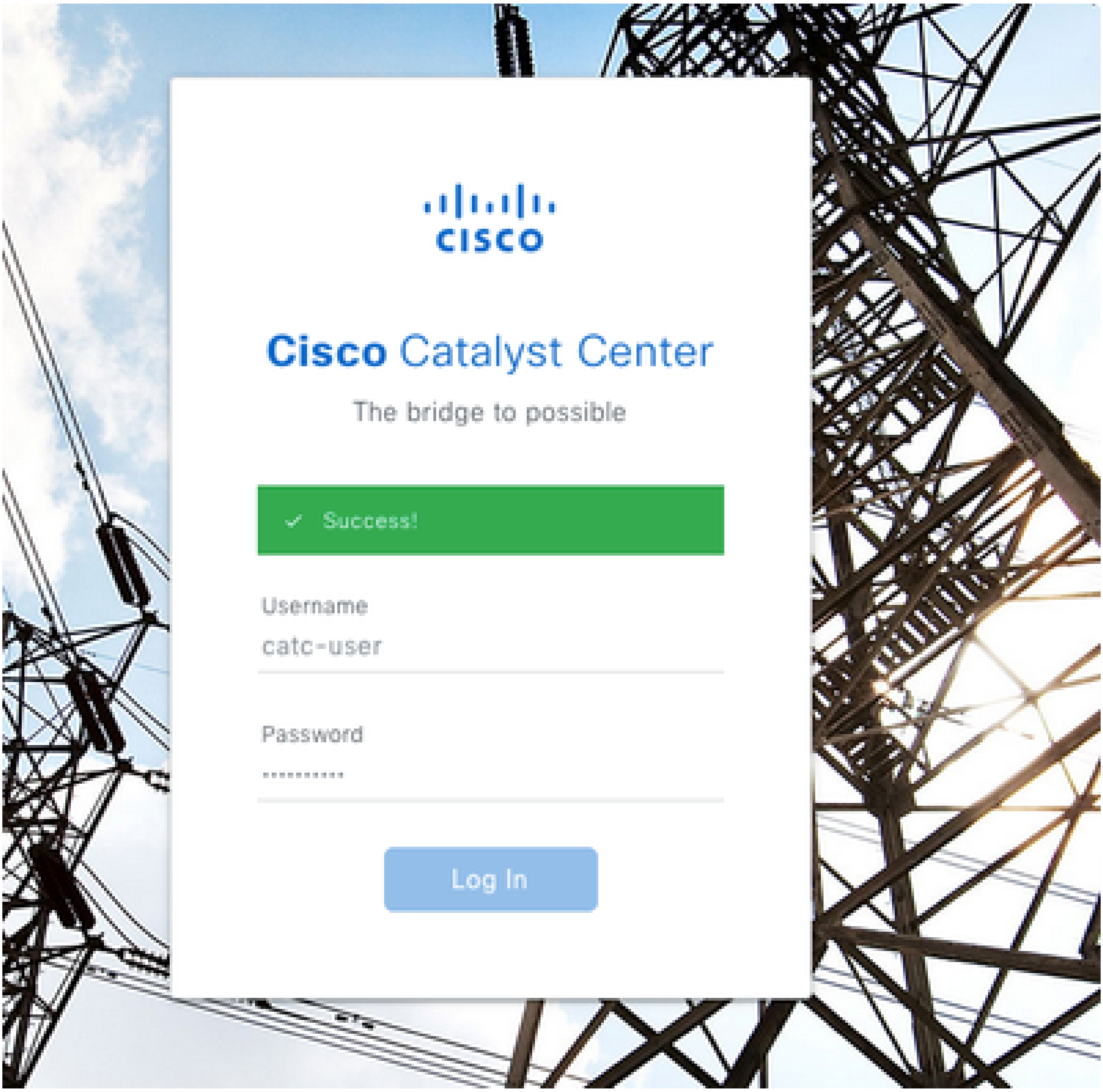
Success
Successfully saved external authentication settings.

External Authentication

Verify

1. Open a **new browser** session or use **Incognito Mode** and log in to the **Catalyst Center web page** with the user account configured in Cisco ISE.

2. From **Catalyst Center**, confirm that the login is successful.



Cisco Catalyst Center

The bridge to possible

✓ Success!

Username: catc-user

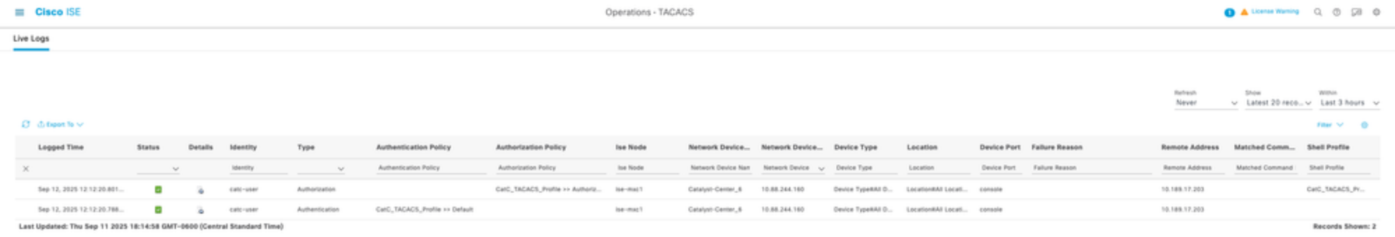
Password: ••••••••••

Log In Configure Catalyst Center External Authentication TACACS with ISE

3. From **Cisco ISE**, validate the logs:

Operations > TACACS > Live Logs

- **Authentication** status: Pass
- **Authorization** status: Pass



Refresh: Never | Show: Latest 20 reco... | Within: Last 3 hours

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		

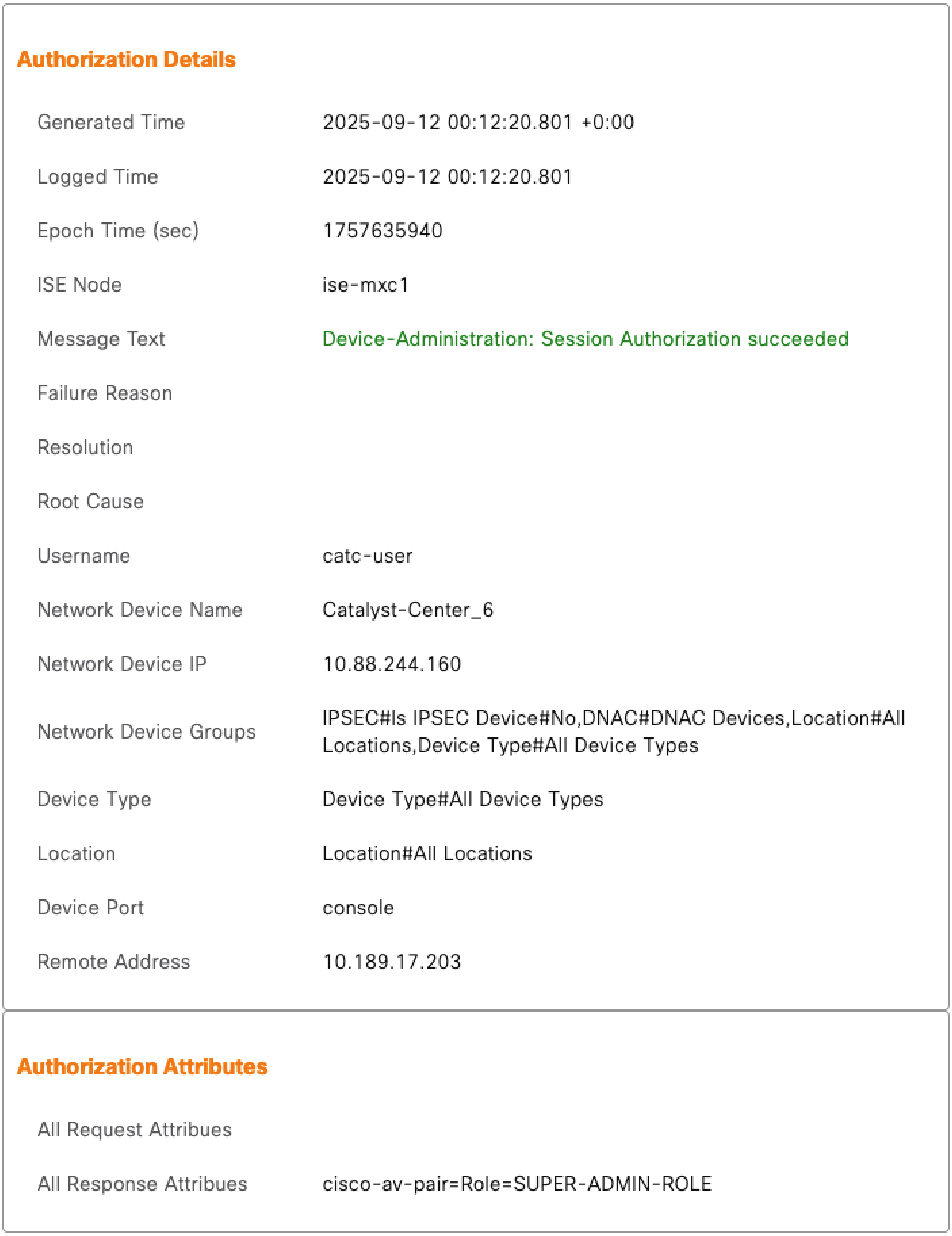
Last Updated: Thu Sep 11 2025 18:14:58 GMT-0600 (Central Standard Time)

Records Shown: 2

Live Logs

4. In the **Authorization Details**, compare with the next output :

    - Message Text: Device-Administration: Session Authorization succeeded
    - All Response Attribues: 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

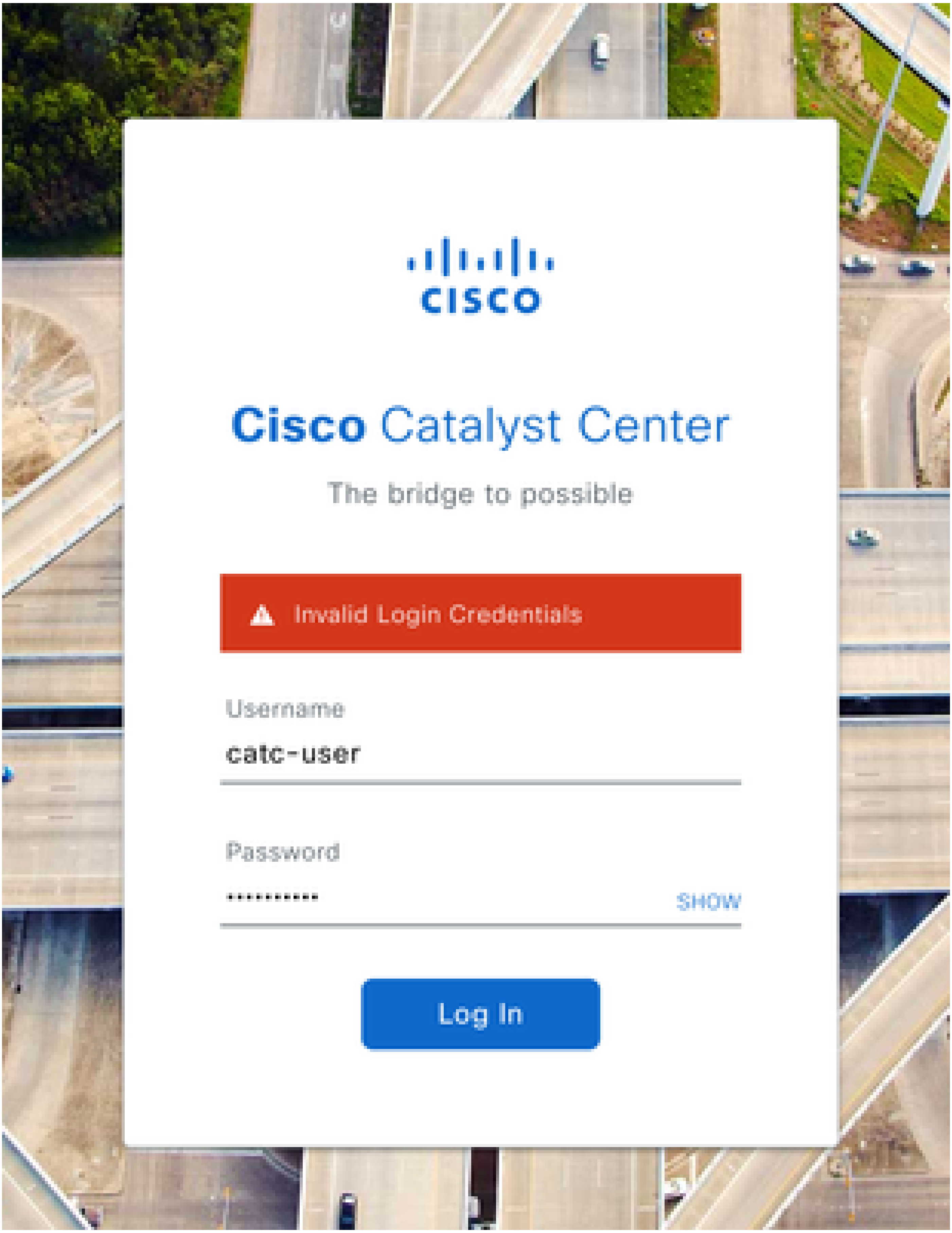
cisco-av-pair=Role=SUPER-ADMIN-ROLE

Troubleshoot

Here are some common issues you can encounter during the integration and how to identify them:

1. Attribute Misconfiguration

Symptom in Catalyst Center: Invalid login credentials



Cisco Catalyst Center

The bridge to possible

⚠ Invalid Login Credentials

Username

catc-user

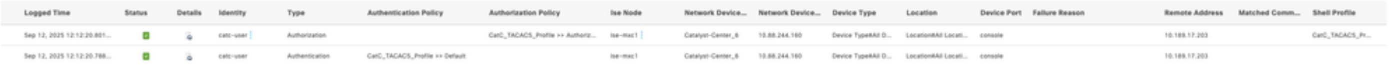
Password

•••••••••••

Attribute Misconfiguration

- Symptom in Cisco ISE (TACACS Logs):

    - Authentication: Pass
    - Authorization: Pass

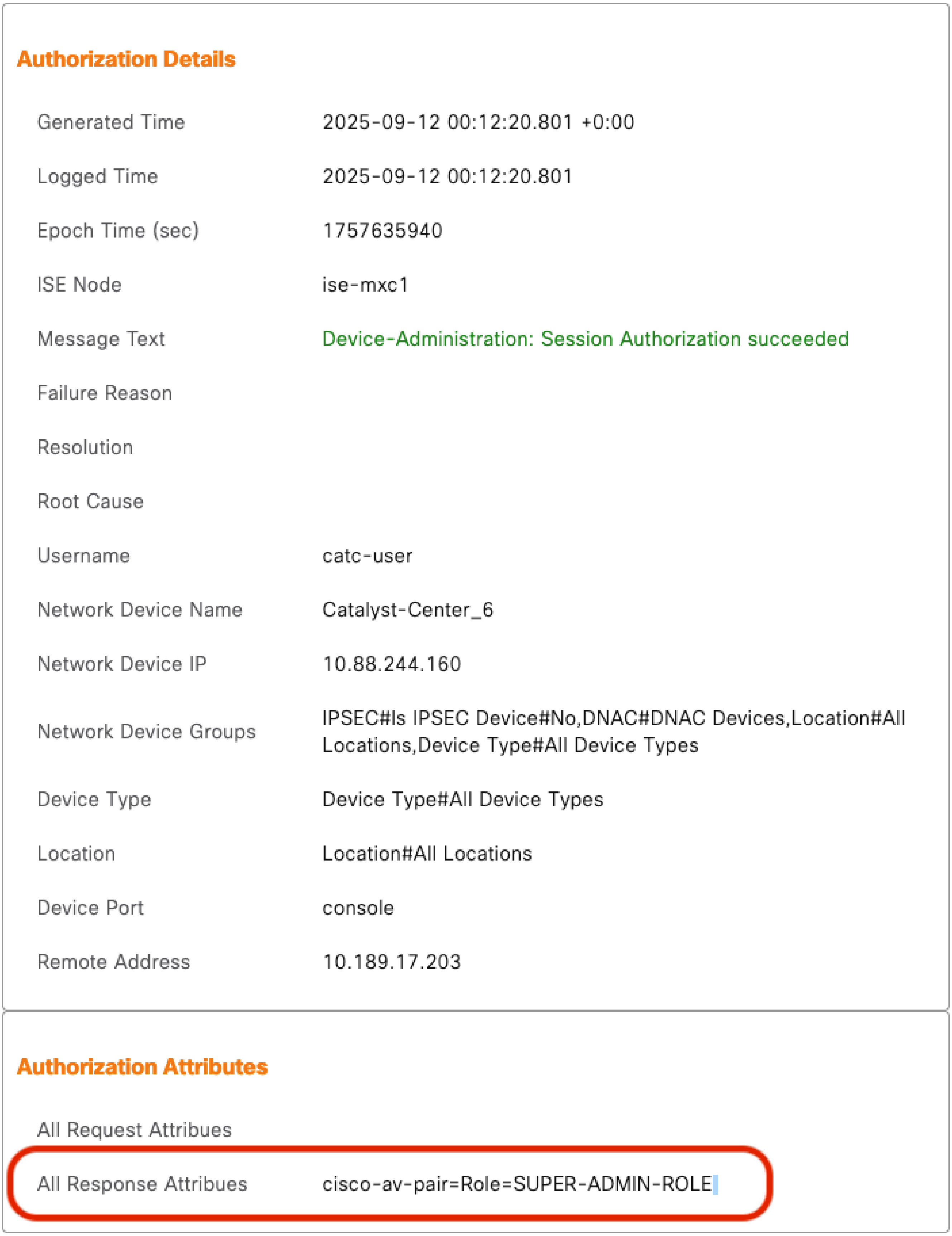


Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device...	Network Device...	Device Type	Location	Device Port	Failure Reason	Remote Address	Matched Comm...	Shell Profile
Sep 12, 2025 12:12:20.801...	✓	🔍	catc-user	Authorization		CatC_TACACS_Profile >> 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		

Attribute Misconfiguration

- Possible Causes:
    - A space exists in the attribute value.

Example:



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

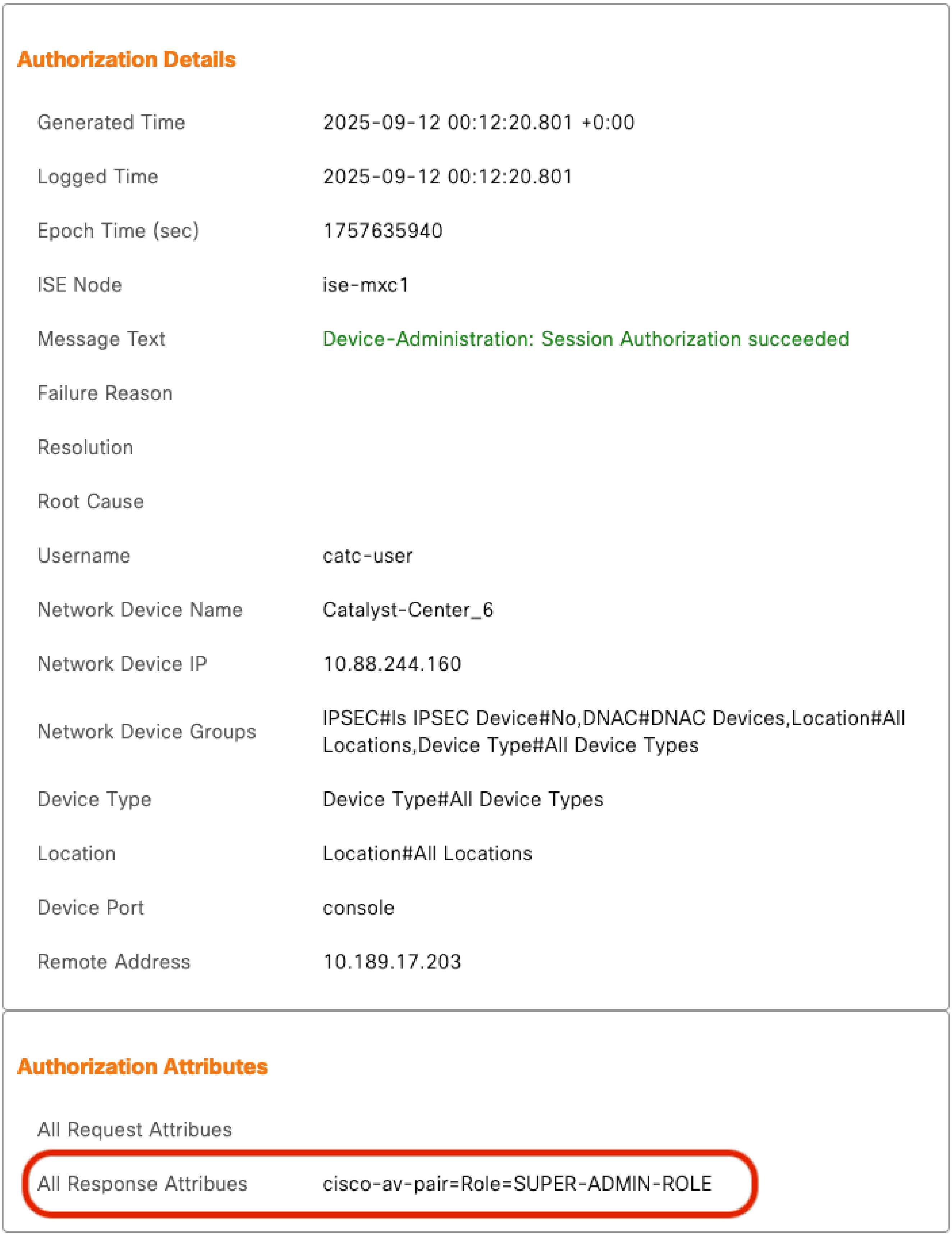
Authorization Attributes

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

Attribute Misconfiguration

- The attribute is incorrectly configured, the Role= keyword is missed.

  Example:



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

Attribute Misconfiguration

2. Shared Secret Mismatch

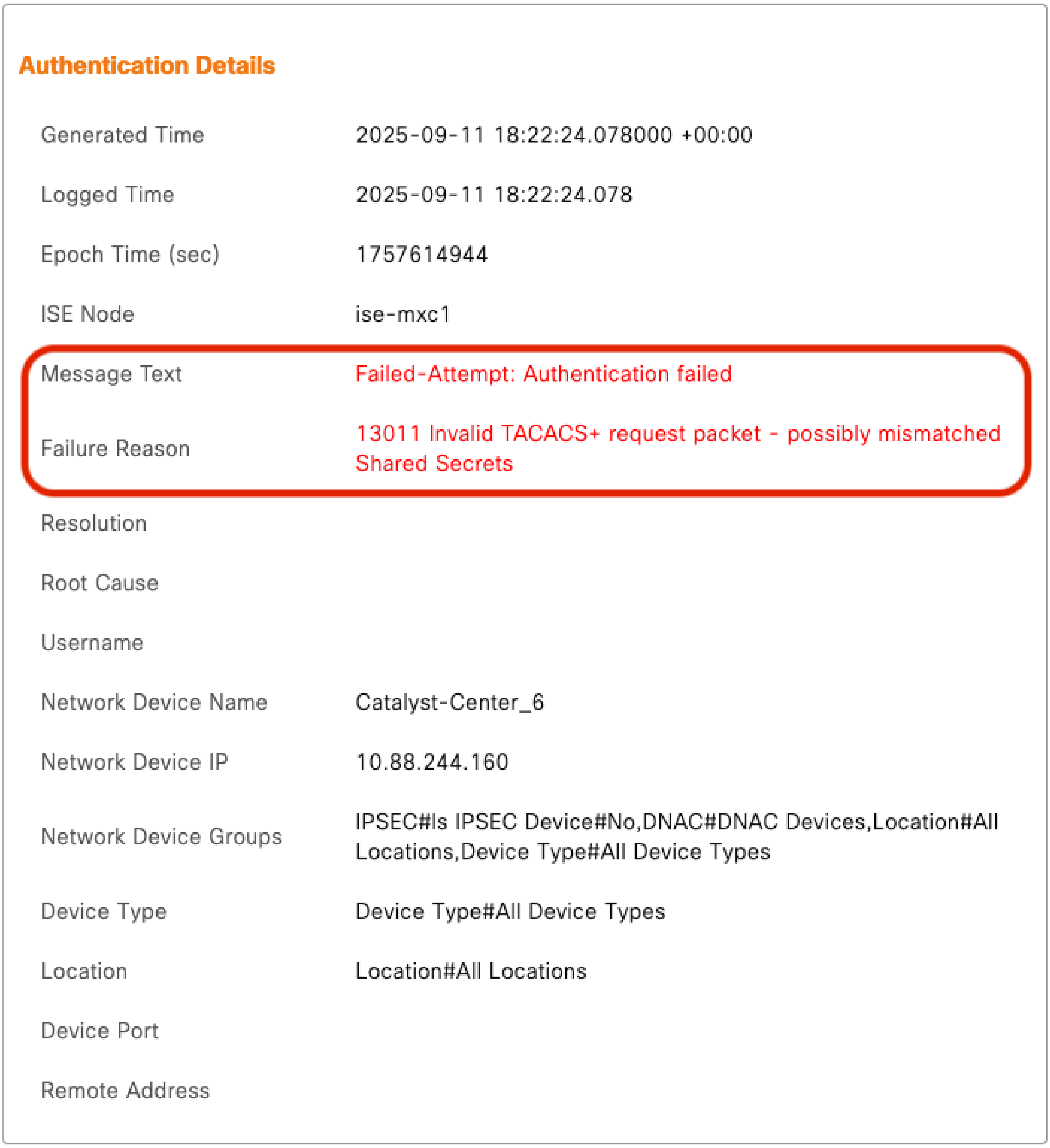
- Symptom**:** Authentication packets fail between Catalyst Center and Cisco ISE.

- Possible Cause: The **Shared Secret** configured in ISE's Network Resourcedoes not match the one configured in **Catalyst Center > External Authentication page**.

How to Verify:

- Check the **Network Resource configuration** in ISE.
- Compare the Shared Secret with the configuration under **Catalyst Center > External Authentication**.

Example:



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	

Shared Secret Mismatch