Configure TACACS+ Authentication on Arista Switch with ISE

Contents

Introduction

Prerequisites

Components Used

Network Diagram

Configurations

- TACACS+ Configuration onISE
- Configure Arista Switch
  - Step 1. Enable TACACS+ Authentication
  - Step 2. Save the Configuration

Verify

- ISE Review

Troubleshooting

- Problem 1
  - Possible Causes
- Problem 2
  - Possible Causes
  - Solution

Introduction

This document describes how to integrate Cisco ISE TACACS+ with an Arista switch for centralized AAA of administrator access.

Prerequisites

Cisco recommends that you have knowledge of these topics:

- Cisco ISE and TACACS+ protocol.
- Arista switches

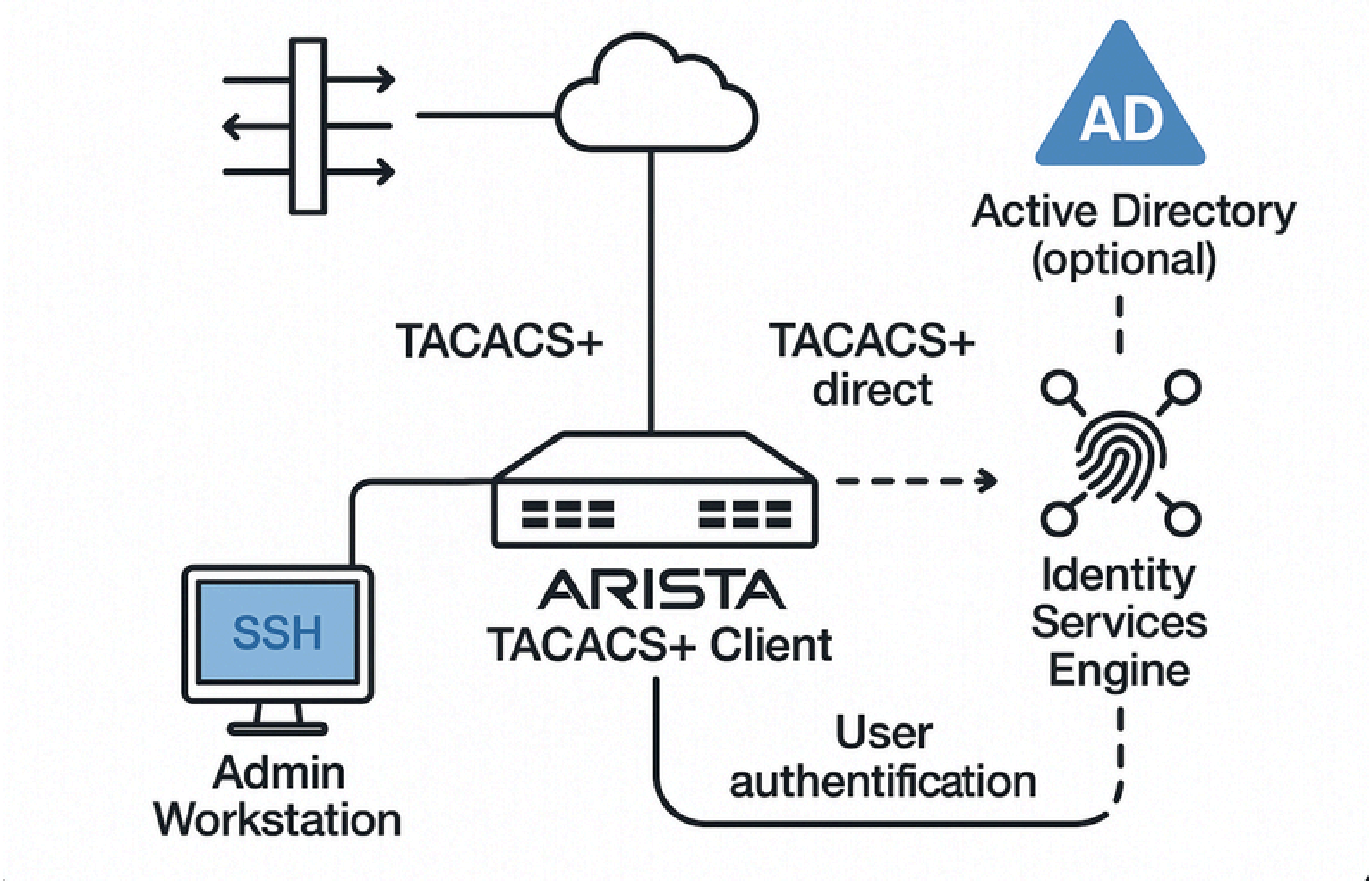
Components Used

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

- Arista switch Software image version: 4.33.2F
- Cisco Identity Services Engine (ISE) version 3.3 Patch 4

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

Network Diagram

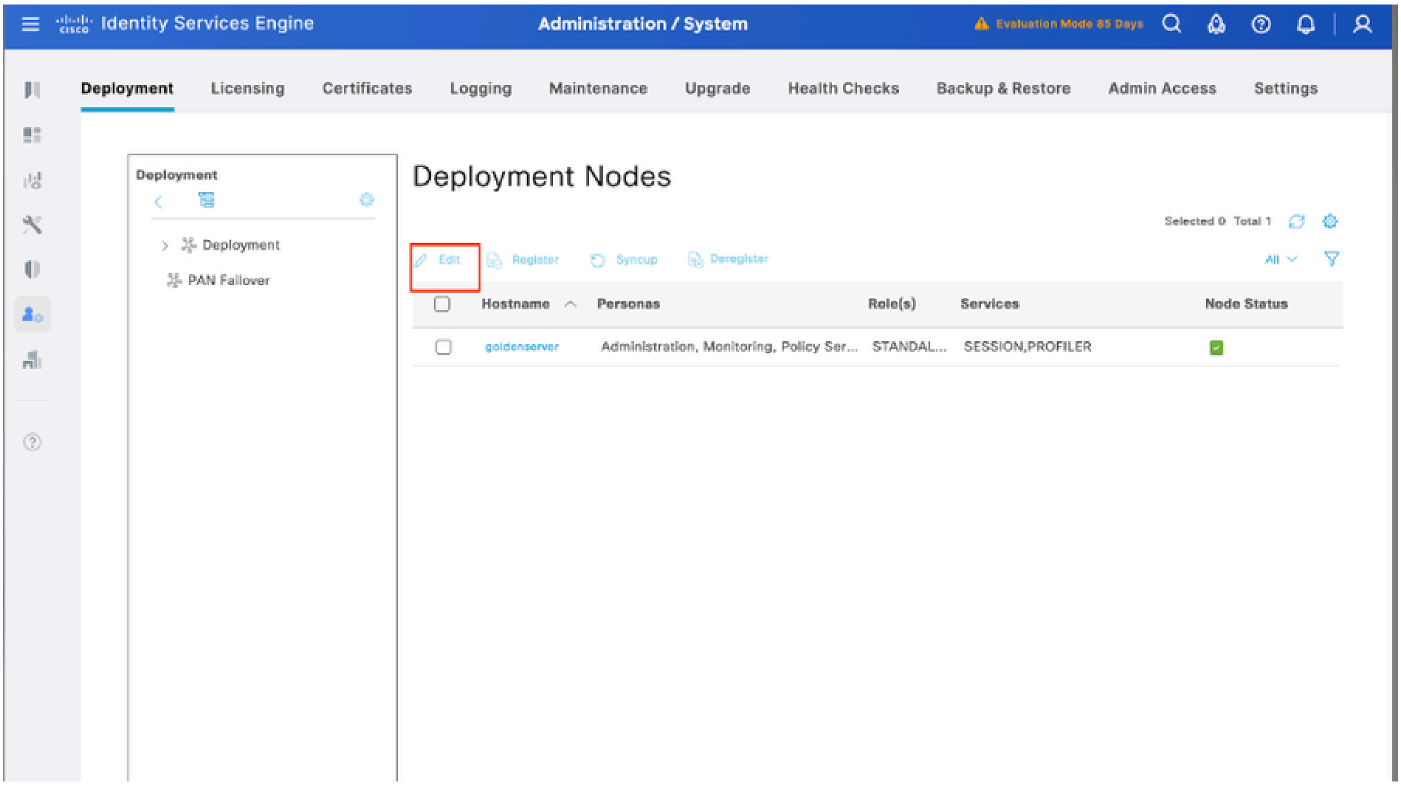


Configurations

TACACS+ Configuration on ISE

Step 1. The initial step is to verify whether Cisco ISE has the necessary capabilities to handle TACACS+ authentication. To do this, confirm that the desired Policy Service Node (PSN) has the Device Admin Service feature enabled.

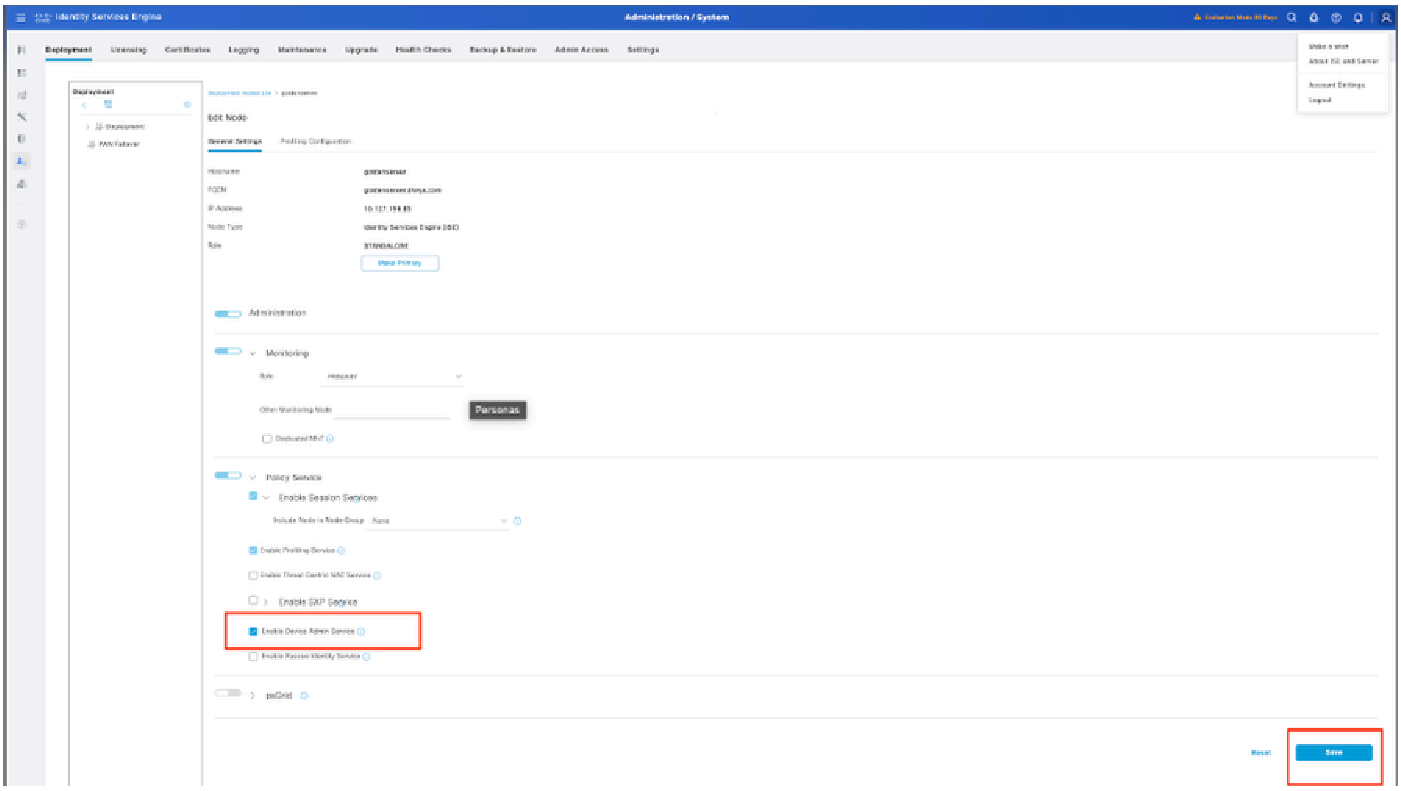
Navigate to **Administration** > **System** > **Deployment**, select the appropriate node where ISE processes TACACS+ authentication, and click **Edit** to review its configuration.



□	Hostname	Personas	Role(s)	Services	Node Status
□	goldenserver	Administration, Monitoring, Policy Ser...	STANDAL...	SESSION,PROFILER	✓

Step 2. Scroll down to locate the Device Administration Service feature. Note that enabling this feature requires the Policy Service persona to be active on the node, along with available TACACS+ licenses in the deployment.

Select the checkbox to enable the feature, then save the configuration.



Hostname goldenserver
FQDN goldenserver.durya.com
IP Address 10.127.198.85
Node Type Identity Services Engine (ISE)
Role STANDALONE

Administration

Monitoring
Role PRIMARY
Other Monitoring Node
□ Dedicated MnT

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

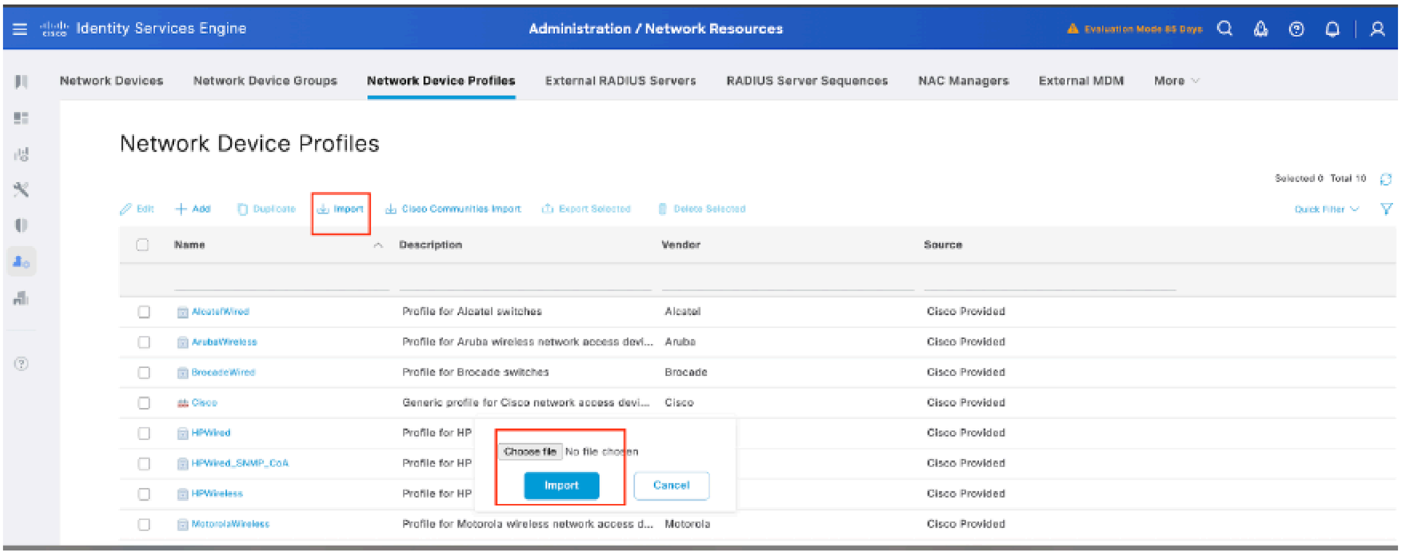
pxGrid

Step 3. Obtaining the Arista Network Device Profile for Cisco ISE.

The Cisco Community has shared a dedicated NAD profile for Arista devices. This profile, along with the necessary dictionary files, can be found in the article Arista CloudVision WiFi Dictionary and NAD Profile for ISE Integration. Downloading and importing this profile into your ISE setup facilitates smoother integration.

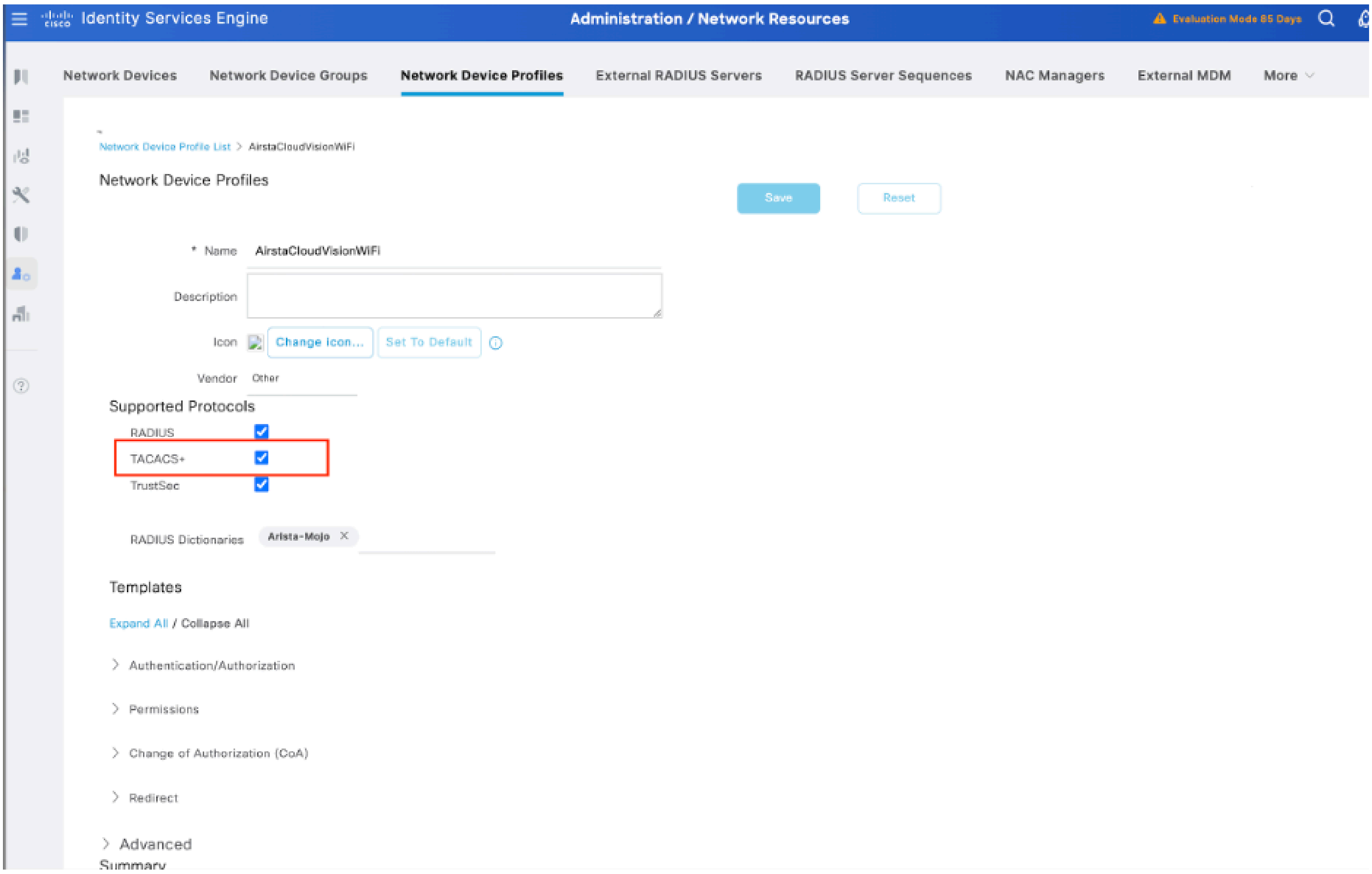
Steps to Import the Arista NAD Profile into Cisco ISE:

1. Download the Profile:
    - Obtain the Arista NAD profile from the Cisco Community link provided above.Cisco Community
2. Access Cisco ISE:
    - Log in to your Cisco ISE administrative console.
3. Import the NAD Profile:
    - Navigate to **Administration** > **Network Resources** > **Network Device Profiles**.
    - Click on the Import button.
    - Upload the downloaded Arista NAD profile file.



□	Name	Description	Vendor	Source
□	AlcatelWired	Profile for Alcatel switches	Alcatel	Cisco Provided
□	ArubaWireless	Profile for Aruba wireless network access devi...	Aruba	Cisco Provided
□	BrocadeWired	Profile for Brocade switches	Brocade	Cisco Provided
□	Cisco	Generic profile for Cisco network access devi...	Cisco	Cisco Provided
□	HPWired	Profile for HP		Cisco Provided
□	HPWired_SNMP_CoA	Profile for HP		Cisco Provided
□	HPWireless	Profile for HP		Cisco Provided
□	MotorolaWireless	Profile for Motorola wireless network access d...	Motorola	Cisco Provided

After the upload is complete, navigate to the **Edit** option and enable TACACS+ as a supported protocol.



Network Device Profiles

* Name AirstaCloudVisionWiFi

Description

Icon

Vendor Other

Supported Protocols

RADIUS ☑

TACACS+ ☑

TrustSec ☑

RADIUS Dictionaries Arista-Mojo

Templates

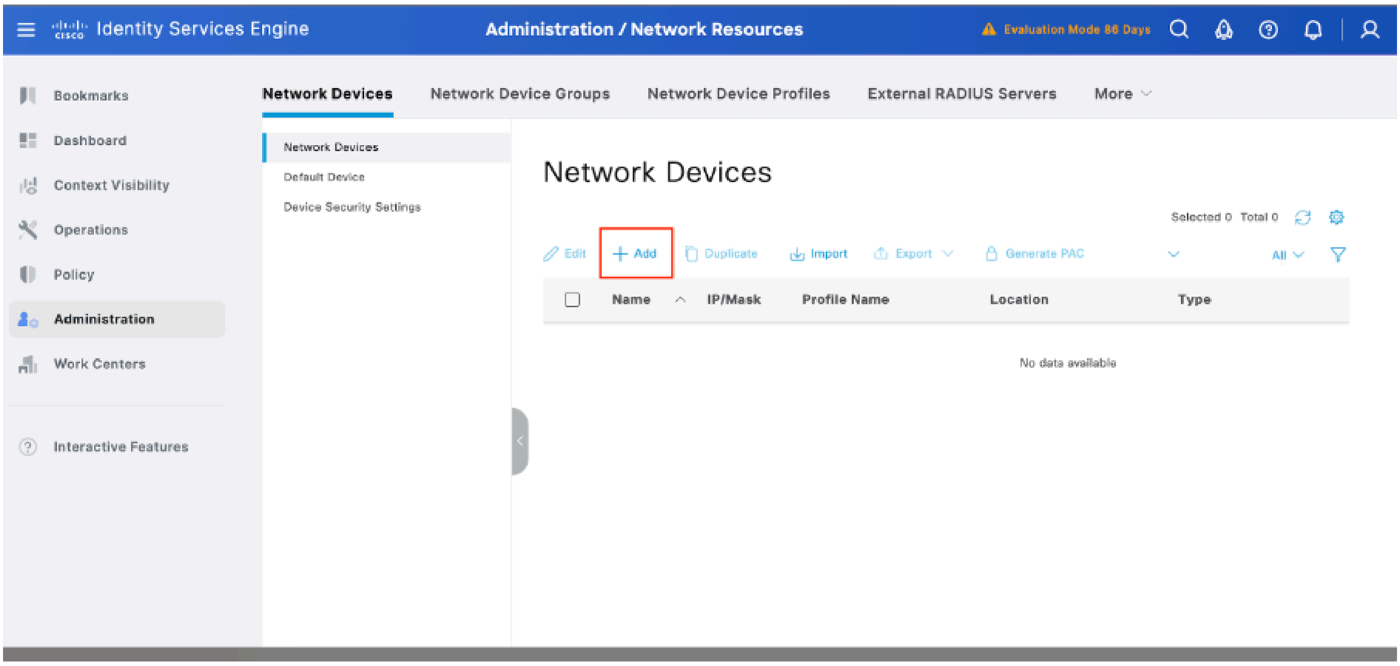
- Authentication/Authorization
- Permissions
- Change of Authorization (CoA)
- Redirect

Advanced

Summary

Step 2: Add Arista Switch as a Network Device.

1. Navigate to **Administration > Network Resources > Network Devices> +Add**:



Network Devices

□	Name	IP/Mask	Profile Name	Location	Type

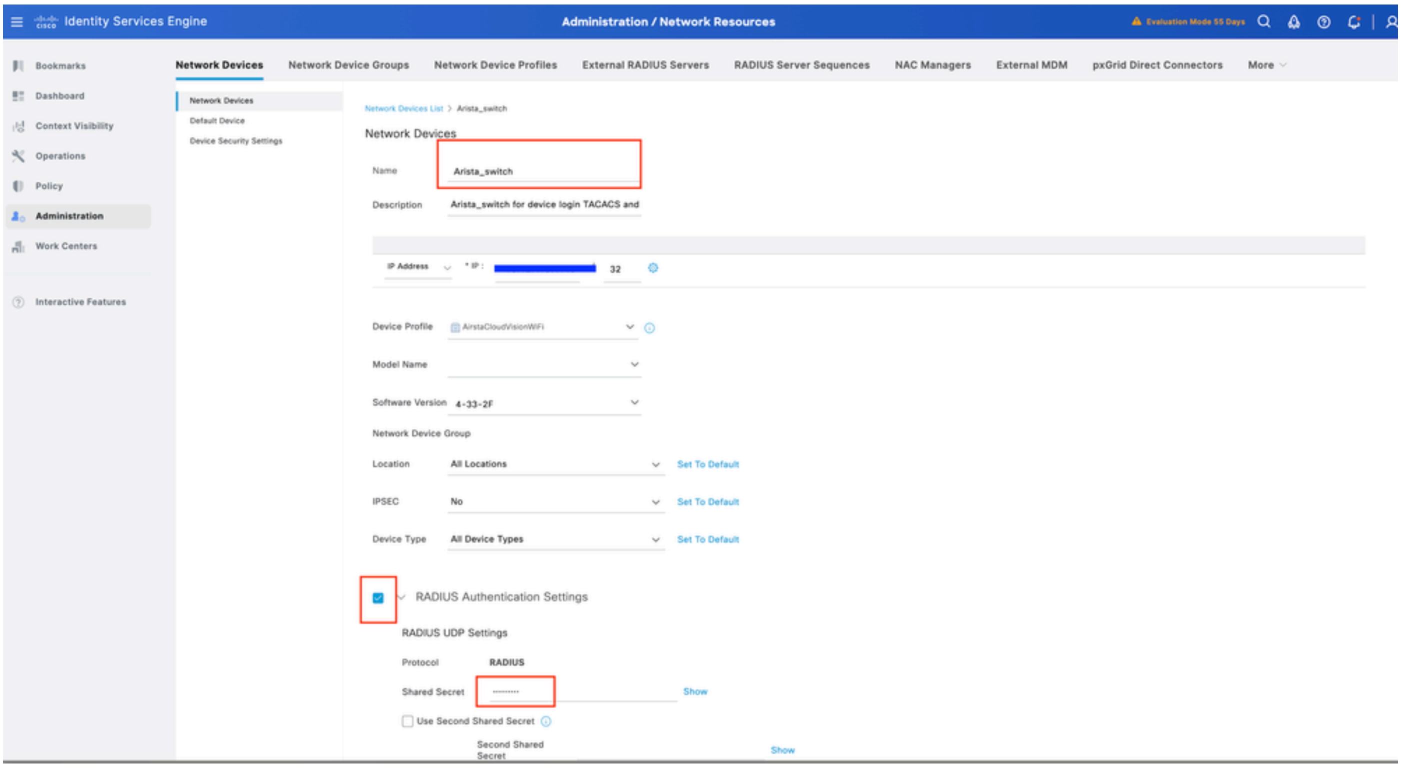
No data available

2.Click **Add** and enter these details:

- **IP Address**: <Switch-IP>
- **Device Type**: Choose Other Wired
- **Network Device Profile**: select **AirstaCloudVisionWiFi.**
- **RADIUS Authentication Settings**:

- ◦ Enable **RADIUS Authentication.**
- ◦ Enter the **Shared Secret** (must match switch configuration).

3. Click **Save**:



Network Devices

Name: Arista_switch

Description: Arista_switch for device login TACACS and

IP Address * IP : [redacted] / 32

Device Profile: AirstaCloudVisionWiFi

Model Name:

Software Version: 4-33-2F

Network Device Group

Location: All Locations — Set To Default

IPSEC: No — Set To Default

Device Type: All Device Types — Set To Default

☑ RADIUS Authentication Settings

RADIUS UDP Settings

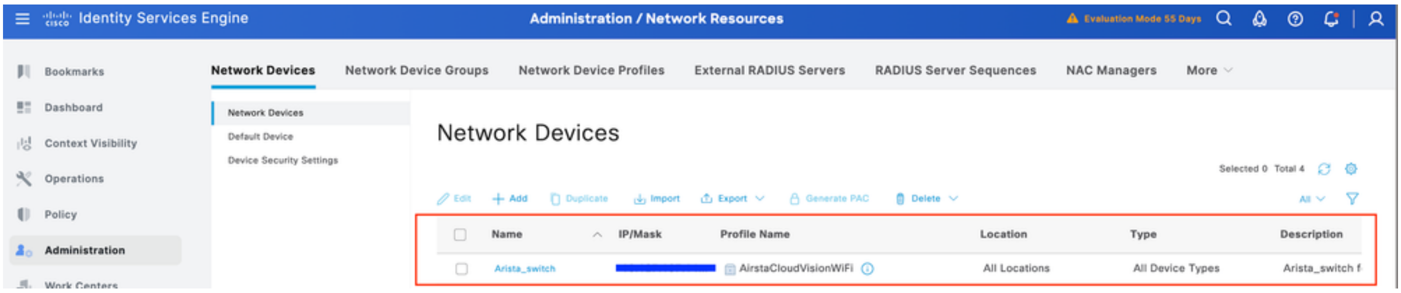
Protocol: RADIUS

Shared Secret: ·········· Show

□ Use Second Shared Secret

Second Shared Secret — Show

Step 3. Validate the new device is shown under **Network Devices**:



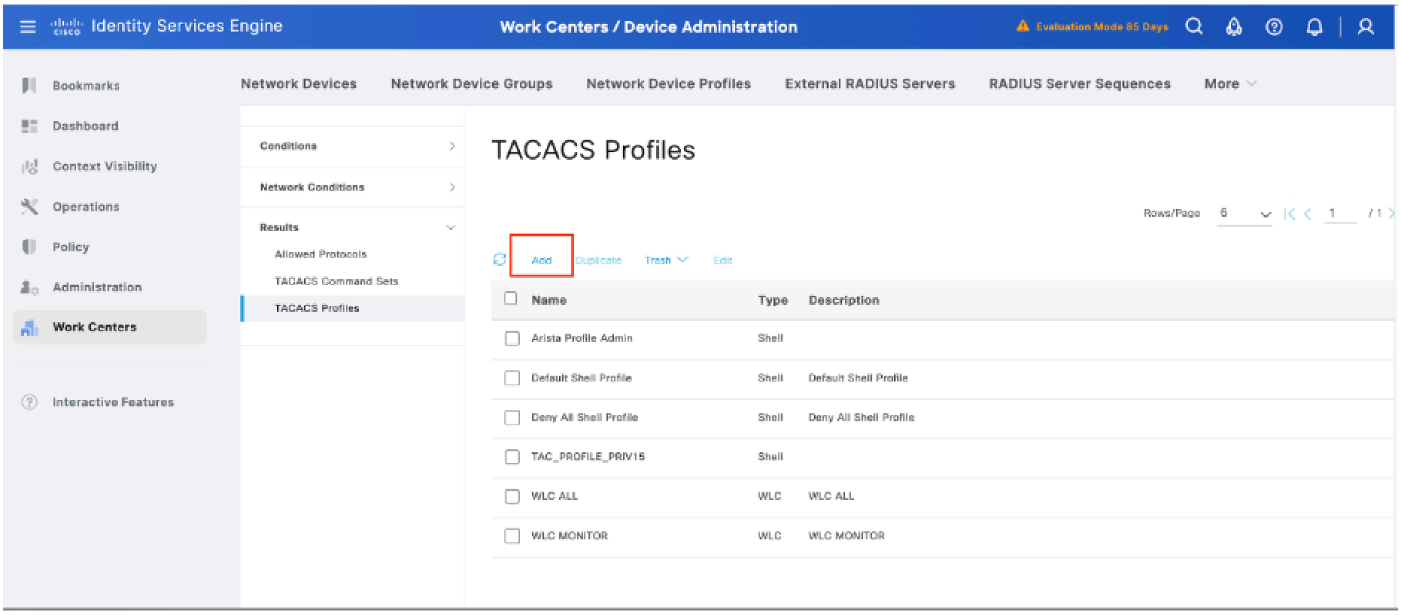
Network Devices

Selected 0 Total 4

□	Name	IP/Mask	Profile Name	Location	Type	Description
□	Arista_switch	[redacted]	AirstaCloudVisionWiFi	All Locations	All Device Types	Arista_switch f

Step 4. Configure the TACACS profile.

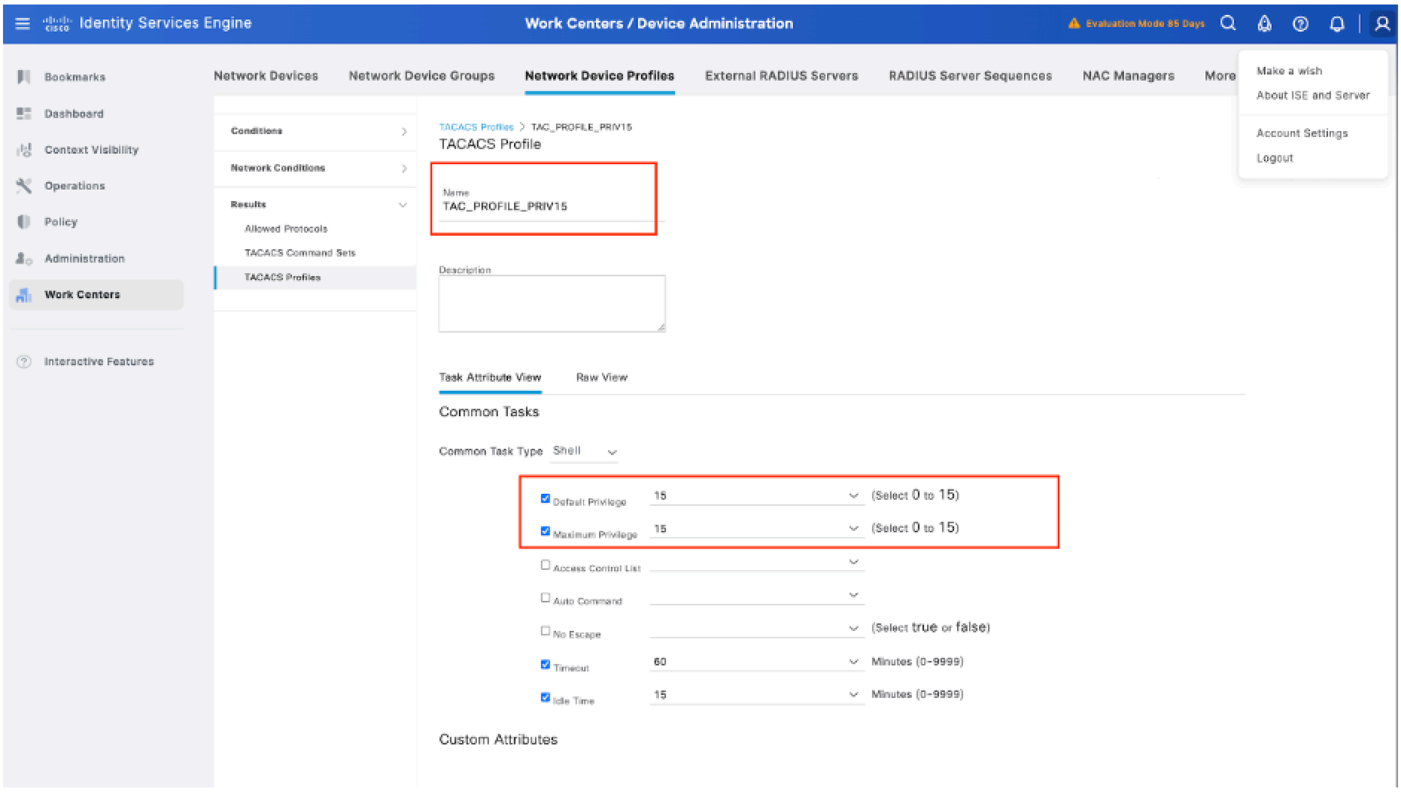
Create a TACACS profile, navigate to the menu **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles**, then select **Add**:



TACACS Profiles

Name	Type	Description
Arista Profile Admin	Shell	
Default Shell Profile	Shell	Default Shell Profile
Deny All Shell Profile	Shell	Deny All Shell Profile
TAC_PROFILE_PRIV15	Shell	
WLC ALL	WLC	WLC ALL
WLC MONITOR	WLC	WLC MONITOR

Enter a Name, select the **Default Privilege** checkbox, and set the value to 15. Additionally, select Maximum Privilege, set its value to 15, and click **Submit**:



TACACS Profile

Name: TAC_PROFILE_PRIV15

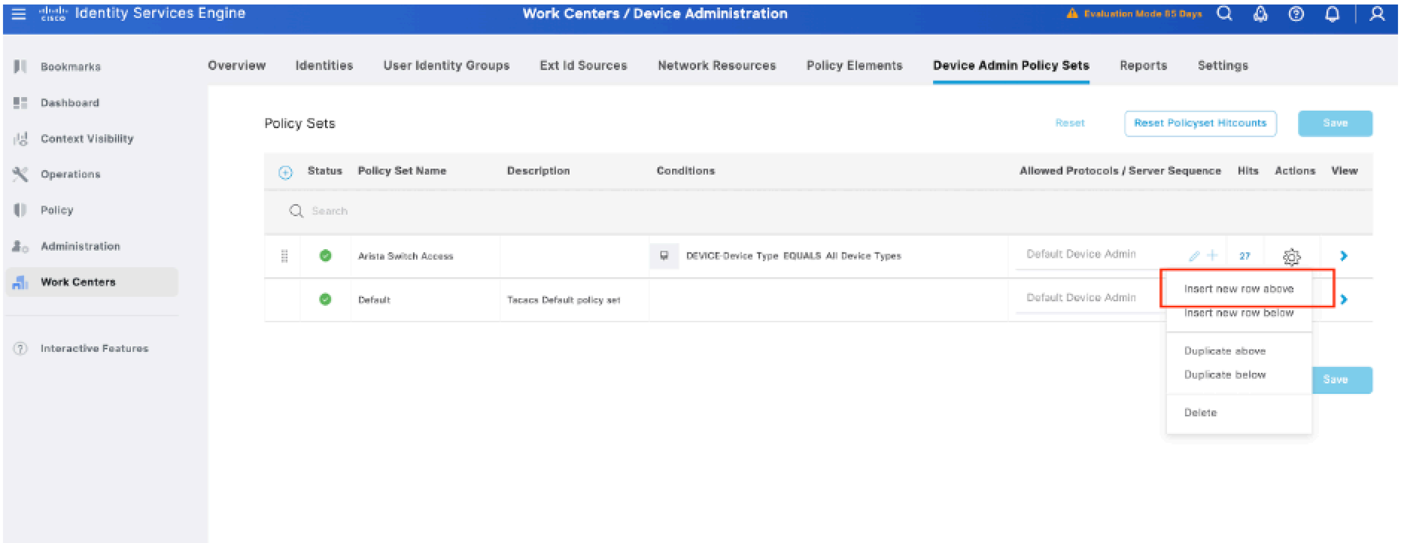
Description:

Common Tasks

Common Task Type: Shell

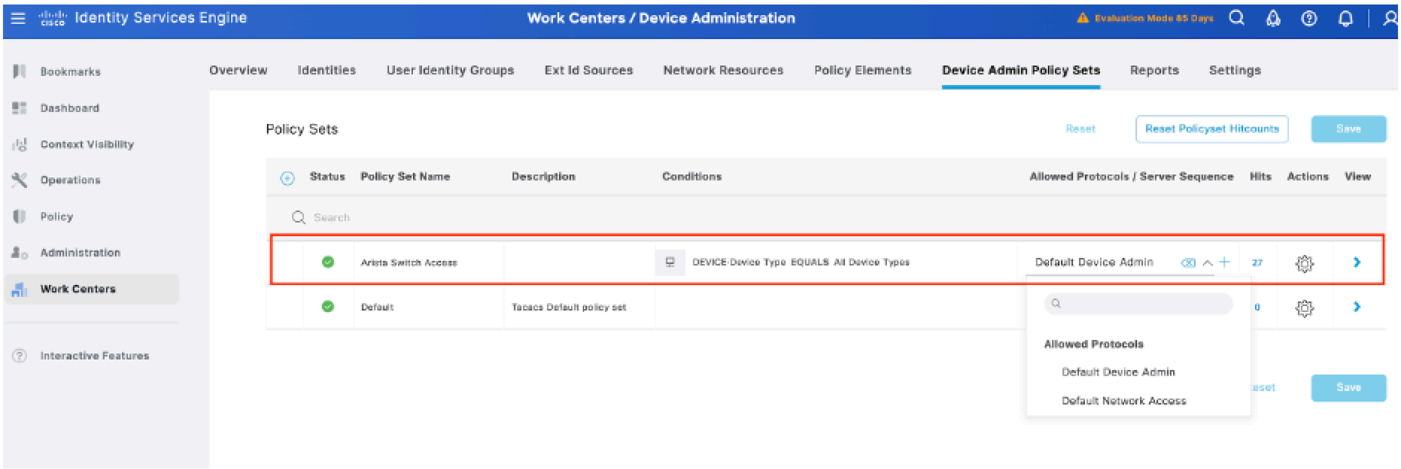
☑ Default Privilege	15	(Select 0 to 15)
☑ Maximum Privilege	15	(Select 0 to 15)
□ Access Control List		
□ Auto Command		
□ No Escape		(Select true or false)
☑ Timeout	60	Minutes (0-9999)
☑ Idle Time	15	Minutes (0-9999)

Step 5. Create a Device Admin Policy Set to be used for your Arista Switch, navigate to the menu **Work Centers > Device Administration > Device Admin Policy Sets**, then from an existent policy set select the gear icon to then select Insert new row above.



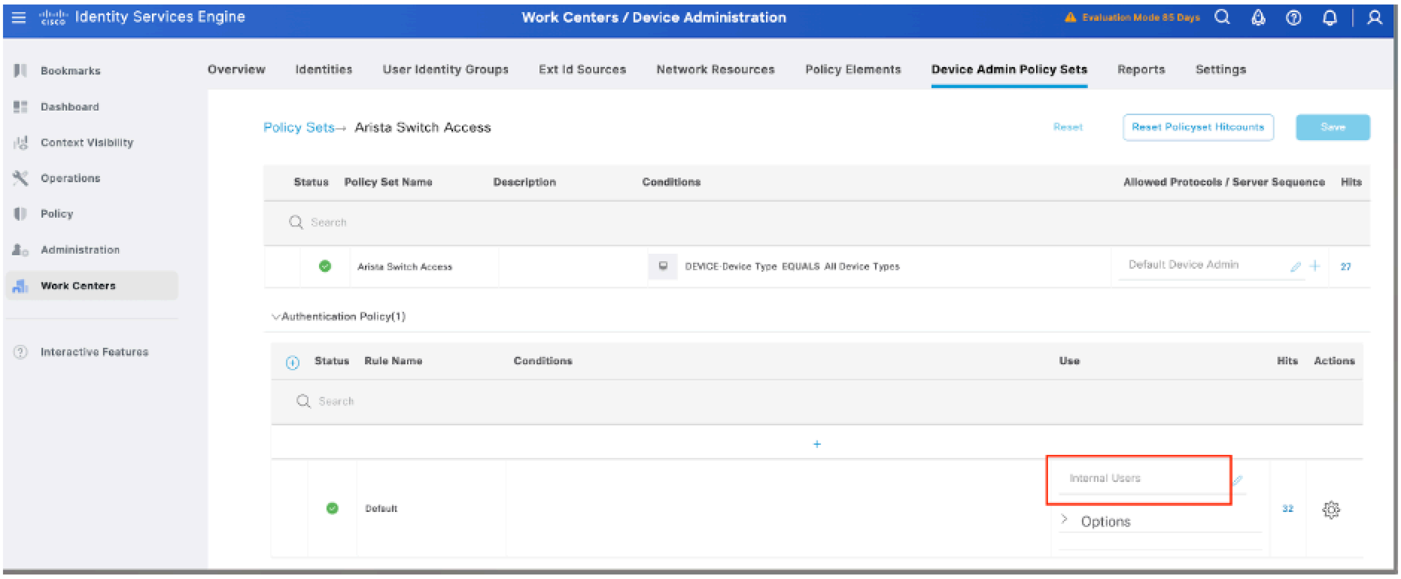
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Arista Switch Access		DEVICE·Device Type EQUALS All Device Types	Default Device Admin	27	⚙	>
✓	Default	Tacacs Default policy set		Default Device Admin			>

Step 6. Name this new Policy Set, add conditions depending upon the characteristics of the TACACS+ authentications that is ongoing from the Arista switch, and select as **Allowed Protocols > Default Device Admin**, save your configuration.



Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Arista Switch Access		DEVICE·Device Type EQUALS All Device Types	Default Device Admin	27	⚙	>
✓	Default	Tacacs Default policy set			0	⚙	>

Step 7. Select in the > **view** option, then in the **Authentication Policy** section, select the external identity source that Cisco ISE uses to query the username and credentials for authentication on the Arista switch. In this example, the credentials correspond to Internal Users stored within ISE.



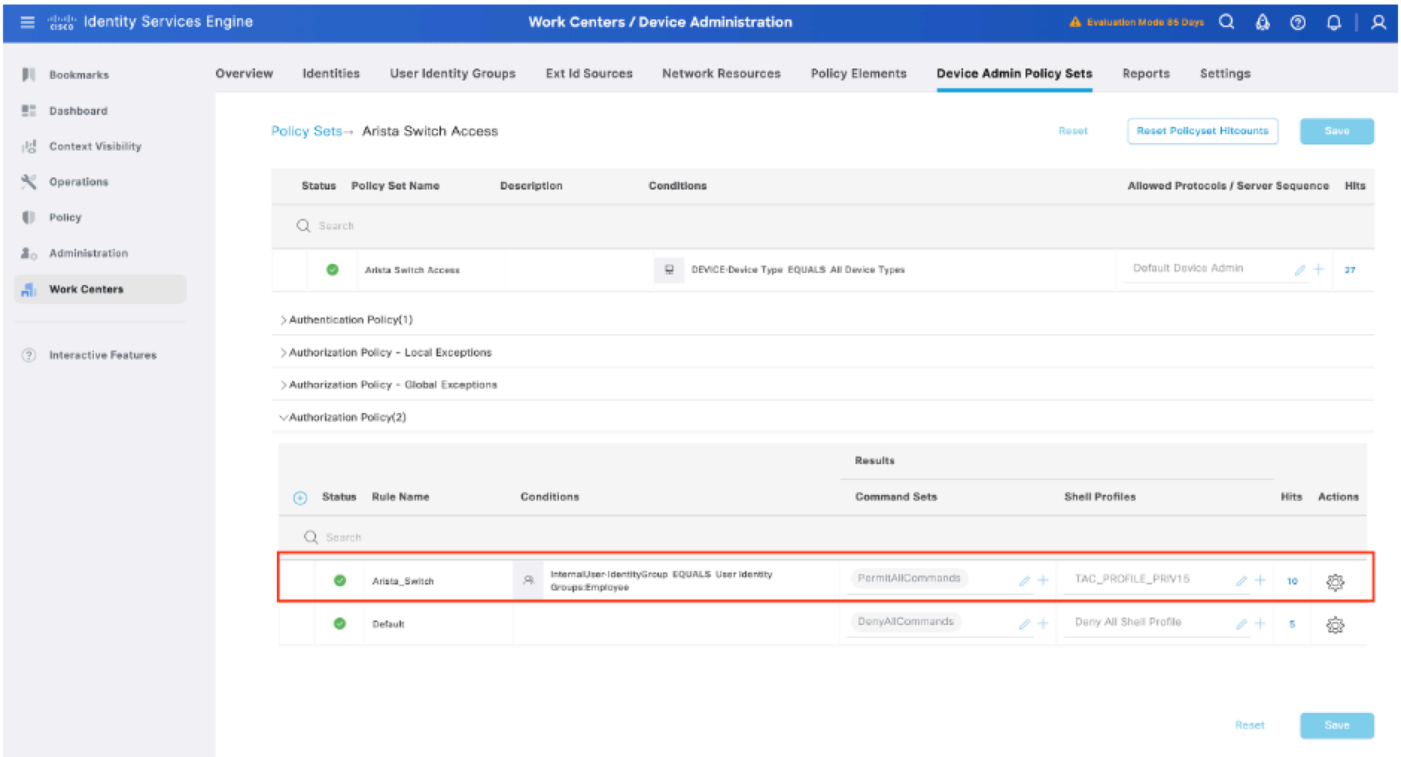
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Arista Switch Access		DEVICE·Device Type EQUALS All Device Types	Default Device Admin	27

Authentication Policy(1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		Internal Users	32	⚙

Step 8. Scroll down until the section named **Authorization Policy** to **Default policy**, select the gear icon, and then insert one rule above.

Step 9. Name the new Authorization Rule, add conditions concerning the user that is authenticated already as group membership, and in the **Shell Profiles** section add the TACACS profile that you configured previously, save the configuration.



Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	Arista Switch Access		DEVICE-Device Type EQUALS All Device Types	Default Device Admin	27

			Results			
Status	Rule Name	Conditions	Command Sets	Shell Profiles	Hits	Actions
●	Arista_Switch	InternalUser-IdentityGroup EQUALS User Identity Groups:Employee	PermitAllCommands	TAC_PROFILE_PRIV15	10	⚙
●	Default		DenyAllCommands	Deny All Shell Profile	5	⚙

Configure Arista Switch

Step 1. Enable TACACS+ Authentication

Log into the Arista switch and enter configuration mode:

```
configure

!

tacacs-server host <ISE-IP> key <TACACS-SECRET>

!

aaa group server tacacs+ ISE_TACACS

  server <ISE-IP>

!

aaa authentication login default group ISE_TACACS local

aaa authorization exec default group ISE_TACACS local

aaa accounting commands 15 default start-stop group ISE_TACACS
```

!

End

Step 2. Save the Configuration

To persist the configuration across reboots:

# write memory

OR

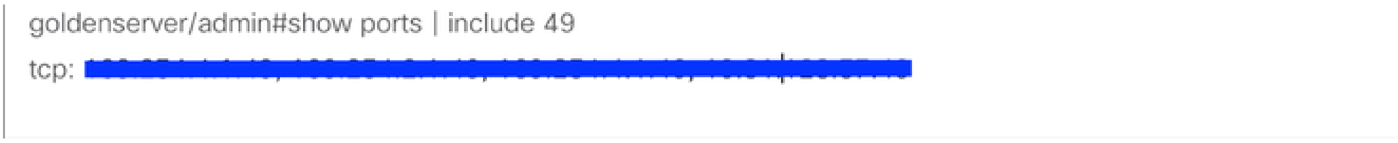
# copy running-config startup-config

Verify

ISE Review

Step 1. Review if the TACACS+ serviceability is running, this can be checked in:

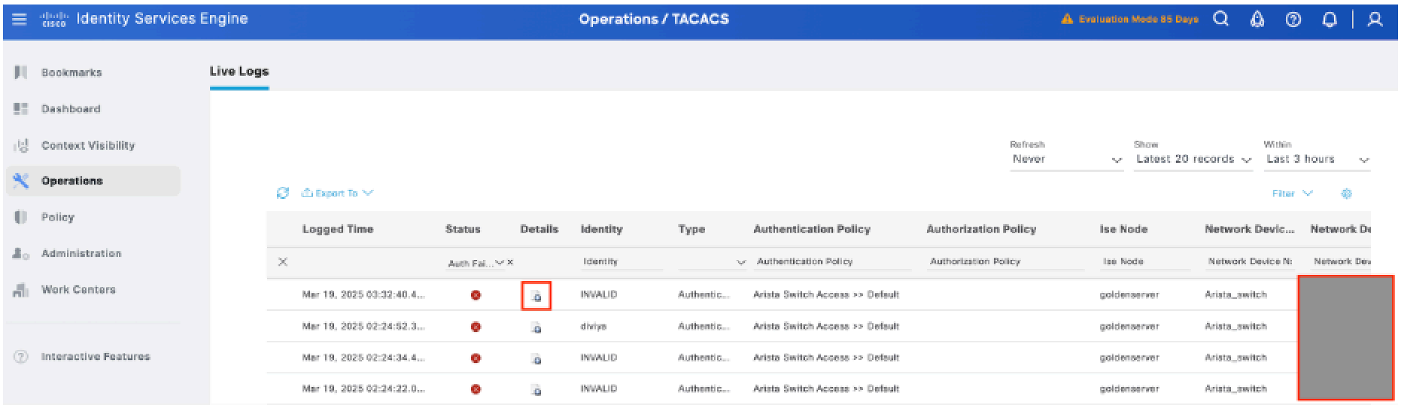
- GUI: Review if you have the node listed with the service DEVICE ADMIN in **> System > Deployment.**
- CLI: Run the command **show ports | include 49** to confirm that there are connections in the TCP port that belong to TACACS+



```
goldenserver/admin#show ports | include 49
tcp: [redacted]
```

Step 2. Confirm if there are livelogs concerning TACACS+ authentications attemps : this can be checked in the menu **Operations > TACACS > Live logs**,

Depending upon the failure reason you can adjust your configuration or address the cause of failure.



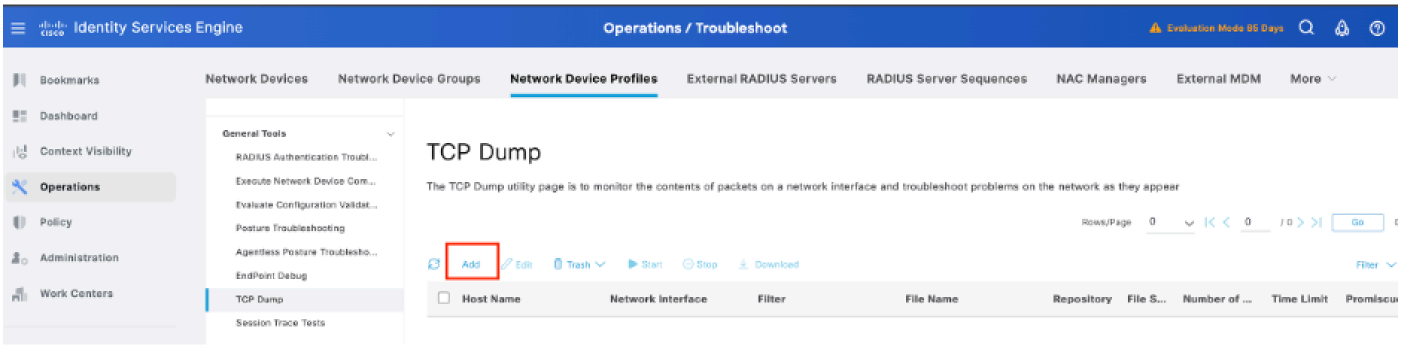
Refresh: Never

Show: Latest 20 records

Within: Last 3 hours

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devic...	Network De
	Auth Fai...		Identity		Authentication Policy	Authorization Policy	Ise Node	Network Device N:	Network Dev
Mar 19, 2025 03:32:40.4...	●	🔍	INVALID	Authentic...	Arista Switch Access >> Default		goldenserver	Arista_switch	[redacted]
Mar 19, 2025 02:24:52.3...	●	🔍	diviya	Authentic...	Arista Switch Access >> Default		goldenserver	Arista_switch	[redacted]
Mar 19, 2025 02:24:34.4...	●	🔍	INVALID	Authentic...	Arista Switch Access >> Default		goldenserver	Arista_switch	[redacted]
Mar 19, 2025 02:24:22.0...	●	🔍	INVALID	Authentic...	Arista Switch Access >> Default		goldenserver	Arista_switch	[redacted]

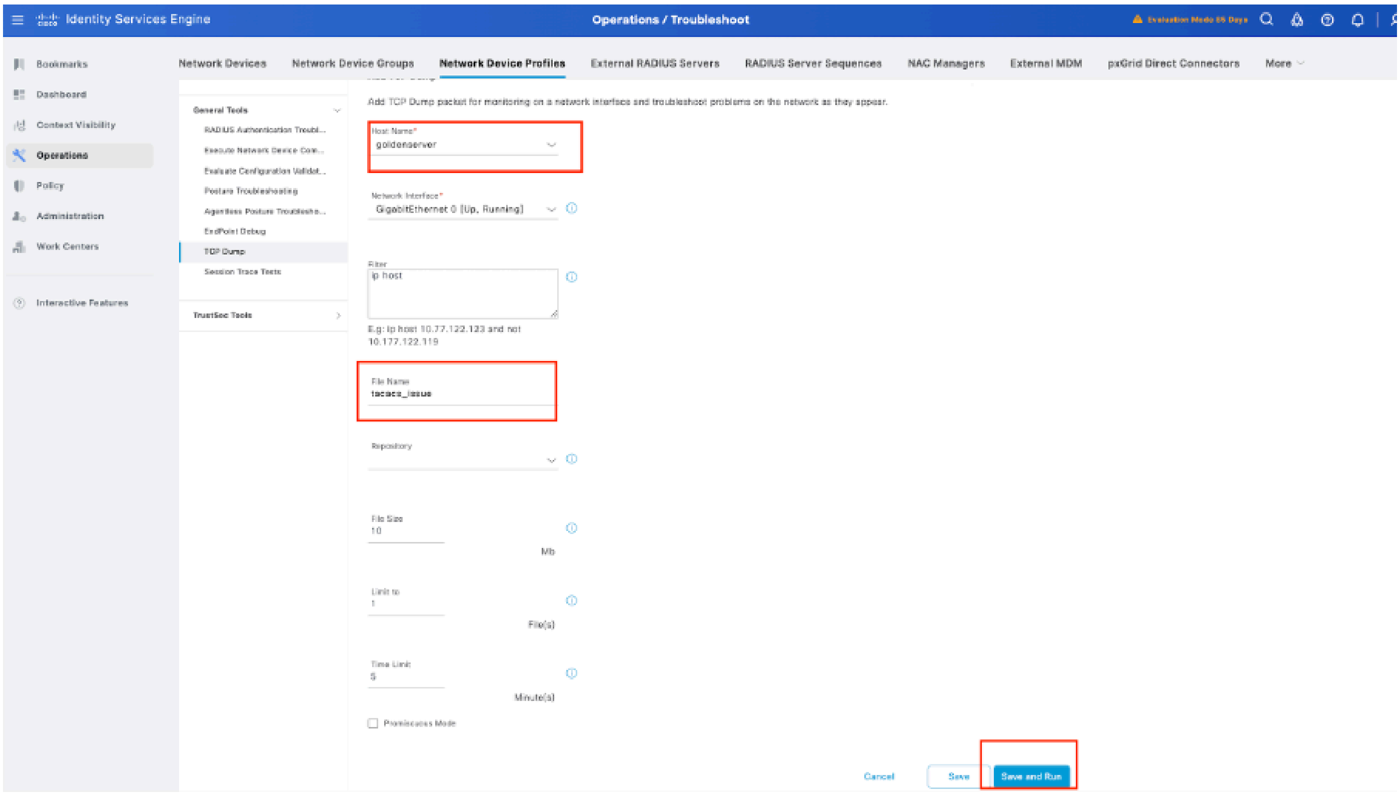
Step 3. In case you don’t see any livelog, proceed to take a packet capture. Navigate to the menu **Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump** , select **Add**:



TCP Dump

The TCP Dump utility page is to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear

☐	Host Name	Network Interface	Filter	File Name	Repository	File S...	Number of ...	Time Limit	Promiscu



Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.

Host Name*: goldenserver

Network Interface*: GigabitEthernet 0 [Up, Running]

Filter: ip host

E.g: ip host 10.77.122.123 and not 10.177.122.119

File Name: tacacs_issue

Repository:

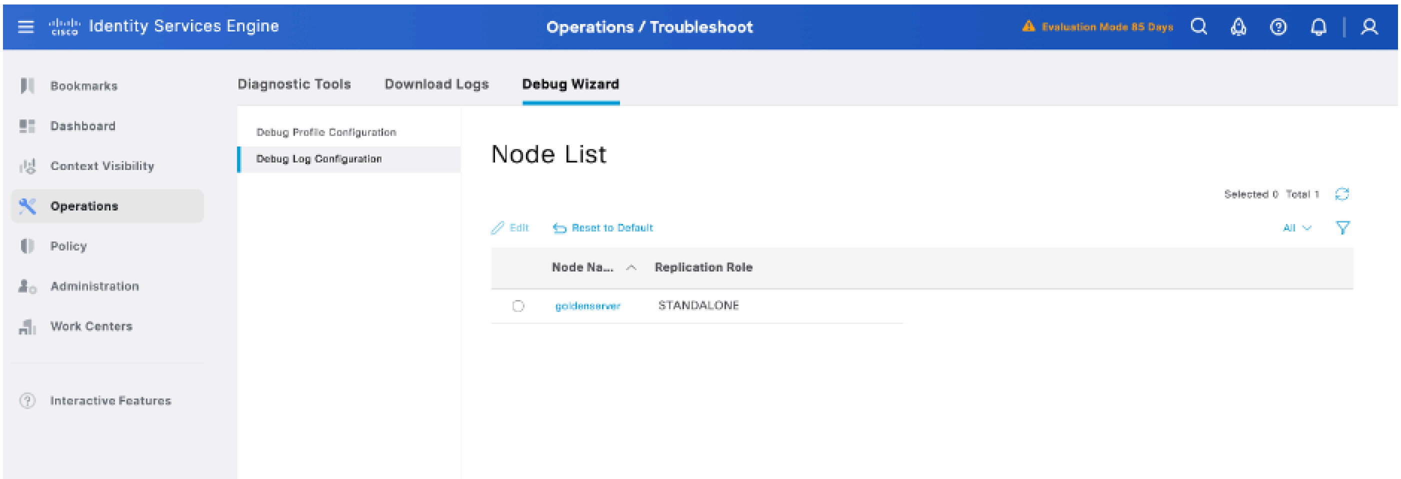
File Size: 10 Mb

Limit to: 1 File(s)

Time Limit: 5 Minute(s)

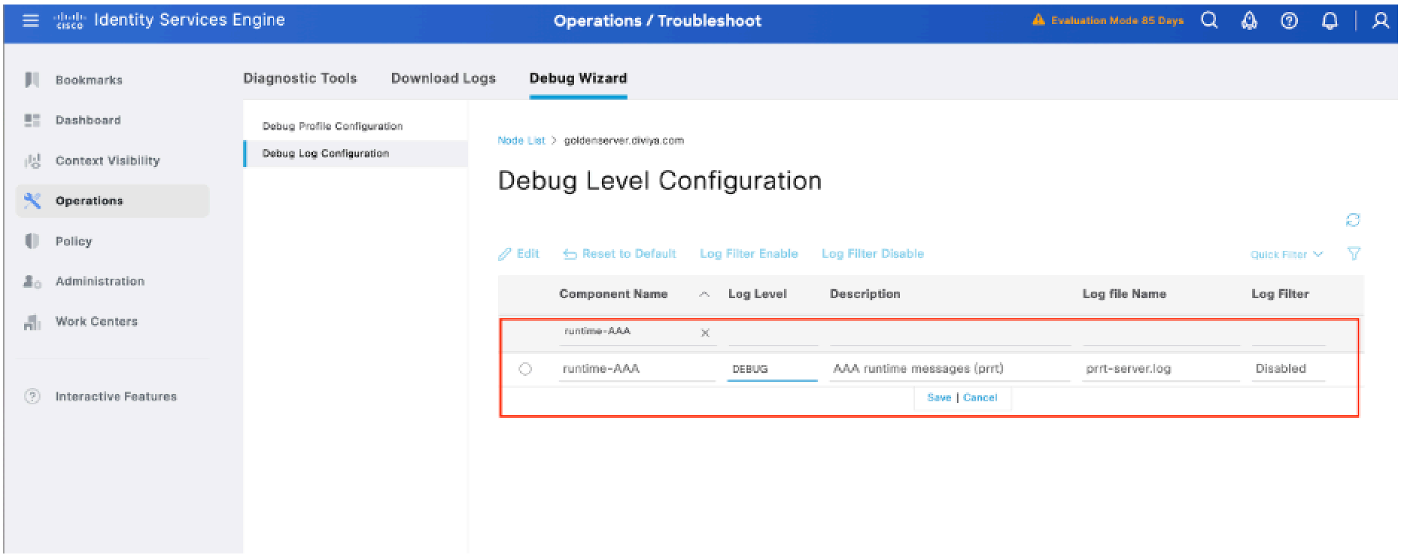
☐ Promiscuous Mode

Step 4. Enable the component runtime-AAA in debug within the PSN from where the authentication is being performed in **Operations > Troubleshoot > Debug Wizard > Debug log configuration**, select **PSN node**, then select the **Edit** button:



Node List

	Node Na...	Replication Role
○	goldenserver	STANDALONE



Node List > goldenserver.diviya.com

Debug Level Configuration

	Component Name	Log Level	Description	Log file Name	Log Filter
	runtime-AAA				
○	runtime-AAA	DEBUG	AAA runtime messages (prrt)	prrt-server.log	Disabled

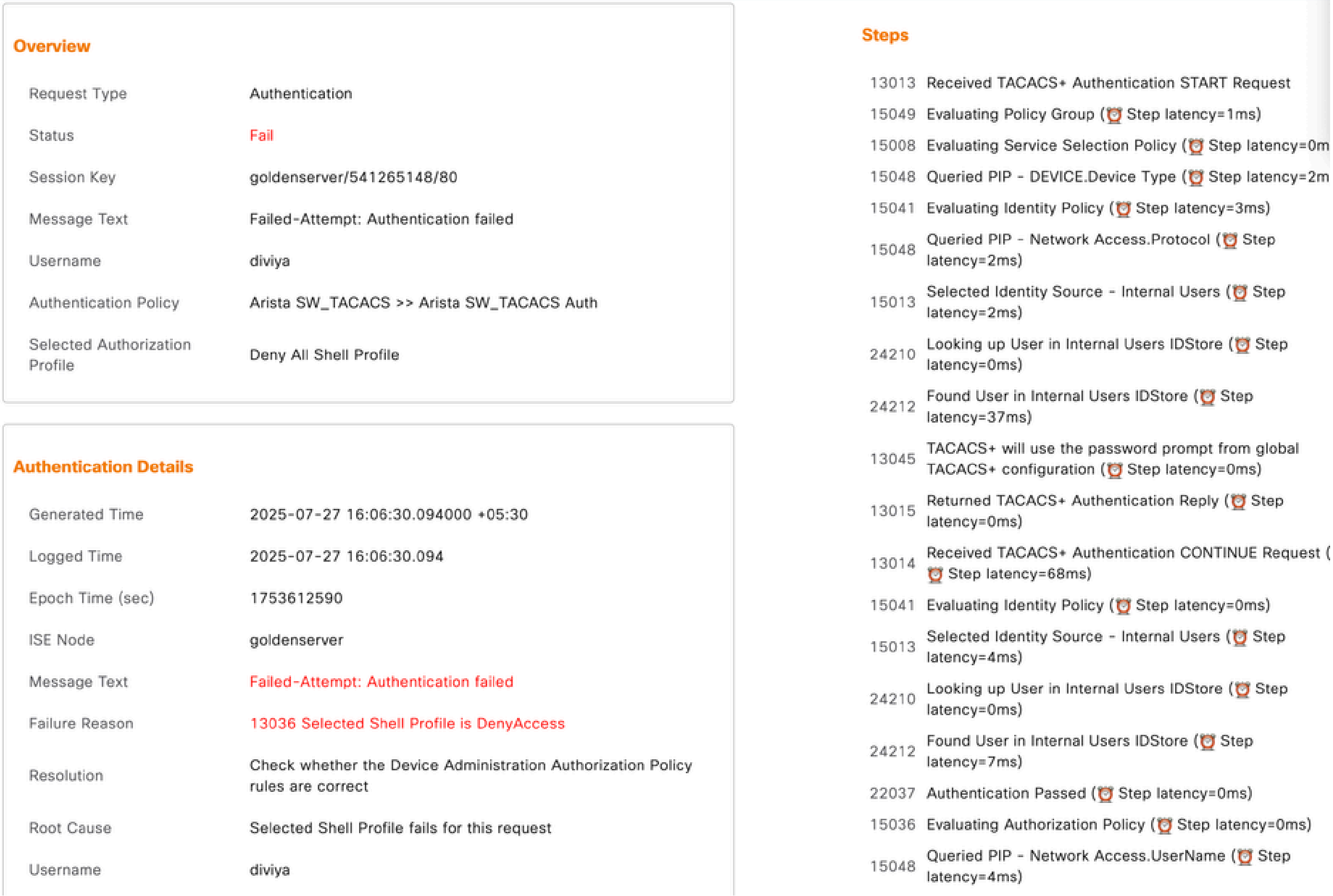
Identify the **runtime-AAA** component, set its logging level to **debug**, reproduce the issue, and analyse the logs for further investigation.

Troubleshooting

Problem 1

TACACS+ authentication between the Cisco ISE and the Arista switch (or any network device) fails with the error message:

"13036 Selected Shell Profile is DenyAccess"



Overview

Request Type	Authentication
Status	Fail
Session Key	goldenserver/541265148/80
Message Text	Failed-Attempt: Authentication failed
Username	diviya
Authentication Policy	Arista SW_TACACS >> Arista SW_TACACS Auth
Selected Authorization Profile	Deny All Shell Profile

Authentication Details

Generated Time	2025-07-27 16:06:30.094000 +05:30
Logged Time	2025-07-27 16:06:30.094
Epoch Time (sec)	1753612590
ISE Node	goldenserver
Message Text	Failed-Attempt: Authentication failed
Failure Reason	13036 Selected Shell Profile is DenyAccess
Resolution	Check whether the Device Administration Authorization Policy rules are correct
Root Cause	Selected Shell Profile fails for this request
Username	diviya

Steps

```
13013  Received TACACS+ Authentication START Request
15049  Evaluating Policy Group (⏰ Step latency=1ms)
15008  Evaluating Service Selection Policy (⏰ Step latency=0m
15048  Queried PIP - DEVICE.Device Type (⏰ Step latency=2m
15041  Evaluating Identity Policy (⏰ Step latency=3ms)
15048  Queried PIP - Network Access.Protocol (⏰ Step
       latency=2ms)
15013  Selected Identity Source - Internal Users (⏰ Step
       latency=2ms)
24210  Looking up User in Internal Users IDStore (⏰ Step
       latency=0ms)
24212  Found User in Internal Users IDStore (⏰ Step
       latency=37ms)
13045  TACACS+ will use the password prompt from global
       TACACS+ configuration (⏰ Step latency=0ms)
13015  Returned TACACS+ Authentication Reply (⏰ Step
       latency=0ms)
13014  Received TACACS+ Authentication CONTINUE Request (
       ⏰ Step latency=68ms)
15041  Evaluating Identity Policy (⏰ Step latency=0ms)
15013  Selected Identity Source - Internal Users (⏰ Step
       latency=4ms)
24210  Looking up User in Internal Users IDStore (⏰ Step
       latency=0ms)
24212  Found User in Internal Users IDStore (⏰ Step
       latency=7ms)
22037  Authentication Passed (⏰ Step latency=0ms)
15036  Evaluating Authorization Policy (⏰ Step latency=0ms)
15048  Queried PIP - Network Access.UserName (⏰ Step
       latency=4ms)
```

The error "13036 Selected Shell Profile is DenyAccess" in Cisco ISE typically means that during a TACACS+ device administration attempt, the authorization policy matched a shell profile set to **DenyAccess**.This is not usually a result of a misconfigured shell profile itself, but rather indicates that none of the configured authorization rules matched the incoming user attributes (such as group membership, device type, or location). As a result, ISE falls back to a default rule or an explicit deny rule, resulting in the access being denied.

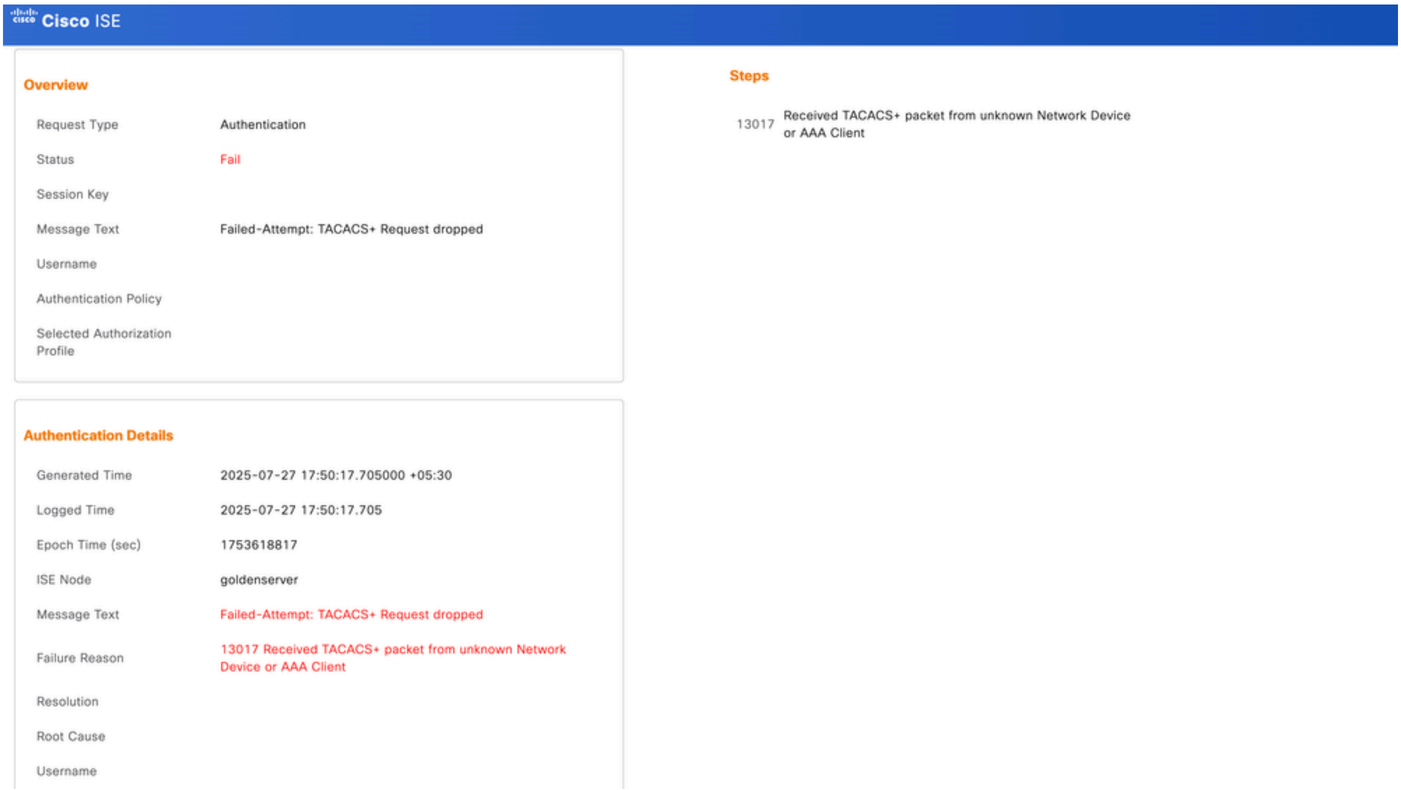
Possible Causes

- Review the authorization policy rules in ISE. Confirm that the user or device is matching the correct rule that assigns the intended shell profile, such as one that permits appropriate access.
- Ensure that the AD or internal user group mapping is correct and that the policy conditions, such as user group membership, device type, and protocol, are accurately specified.
- Use ISE live logs and details of the failed attempt to see exactly which rule is matched and why.

Problem 2

TACACS+ authentication between the Cisco ISE and the Arista Switch (or any network device) fails with the error message:

"13017 Received TACACS+ packet from unknown Network Device or AAA Client"



Overview

Request Type	Authentication
Status	Fail
Session Key	
Message Text	Failed-Attempt: TACACS+ Request dropped
Username	
Authentication Policy	
Selected Authorization Profile	

Authentication Details

Generated Time	2025-07-27 17:50:17.705000 +05:30
Logged Time	2025-07-27 17:50:17.705
Epoch Time (sec)	1753618817
ISE Node	goldenserver
Message Text	Failed-Attempt: TACACS+ Request dropped
Failure Reason	13017 Received TACACS+ packet from unknown Network Device or AAA Client
Resolution	
Root Cause	
Username	

Steps

13017 Received TACACS+ packet from unknown Network Device or AAA Client

Possible Causes

- The most common reason is that the IP address of the switch is not added as a Network Device in ISE (under Administration > Network Resources > Network Devices).
- Ensure the IP address or range matches exactly the source IP being used by the Arista switch to send TACACS+ packets.
- If your switch uses a management interface, verify that its exact IP (not just a subnet/range) is added in ISE.

Solution

- Go to **Administration > Network Resources > Network Devices** in the ISE GUI.
- Verify if the exact source IP address on the Arista switch is using for TACACS+ communication (most often the management interface IP).
- Specify the shared secret (it must match what is set on the Arista switch).