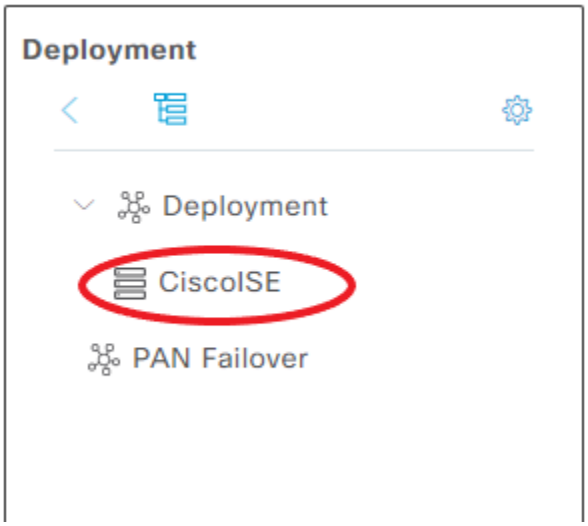
TACACS with Cisco ISE

Overview:

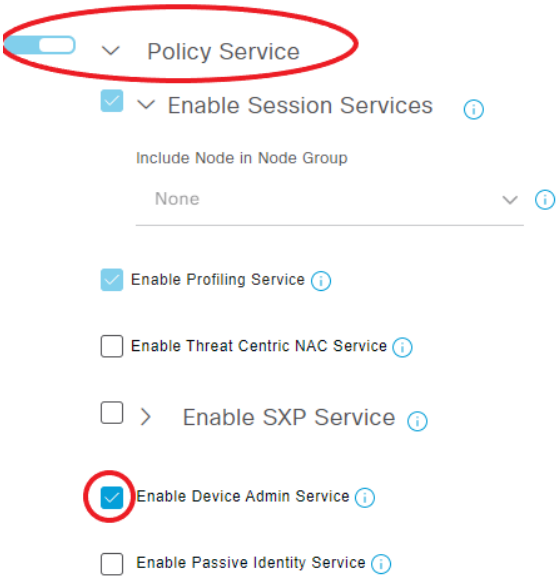
This document describes the steps on how to add WTI unit to Cisco ISE 3.1 for TACACS administration and provide privilege levels from the server.

Step 1: Enable Device Admin Services:

- Go to **Administration > Deployment**. From there select the node you want to enable the service of in the left-hand menu.

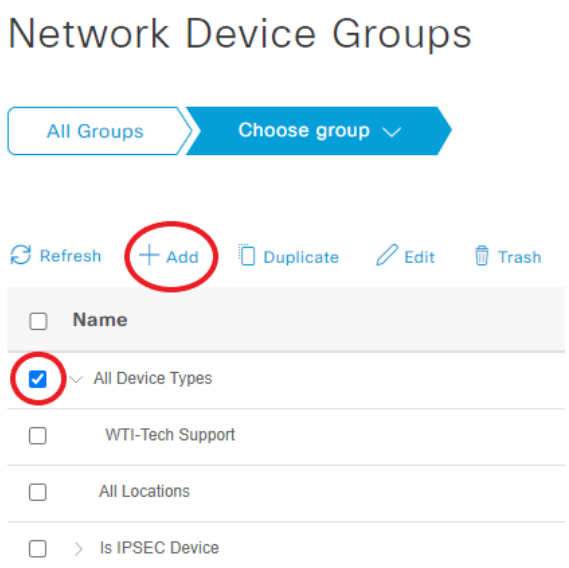


- This should load the **General Settings** tab on the right-hand side. Scroll down to **Policy Service** and enable it. Check the box next to **Device Admin Services**.

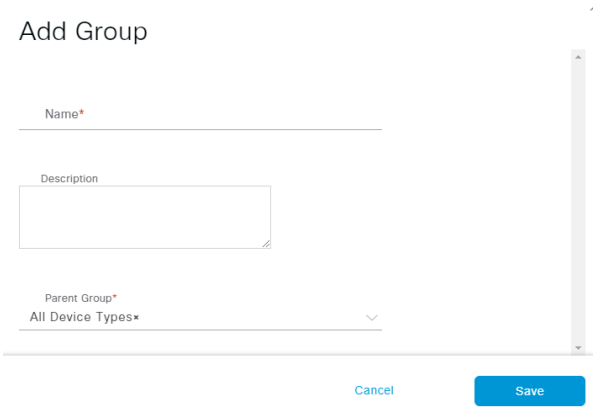


Step 2: Create Network Device Group

- Navigate to **Administration > Network Device Groups**. Check box next to the **All Device Types** and click on **+Add**.

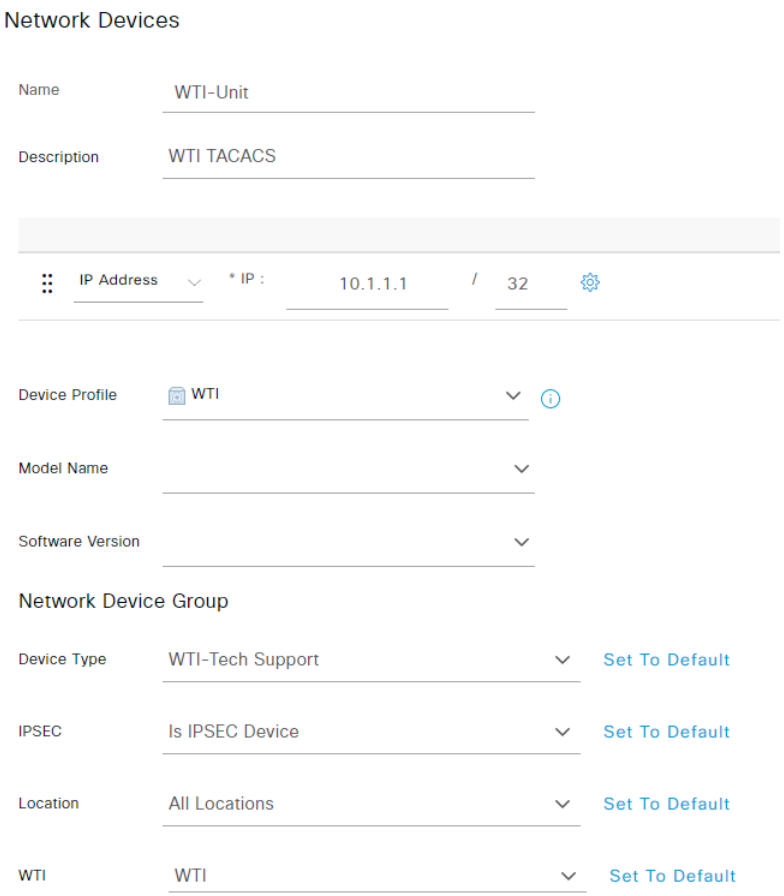


- This should pop a window asking to **Add Group.** Fill one out for each Device Type that you would like to add.

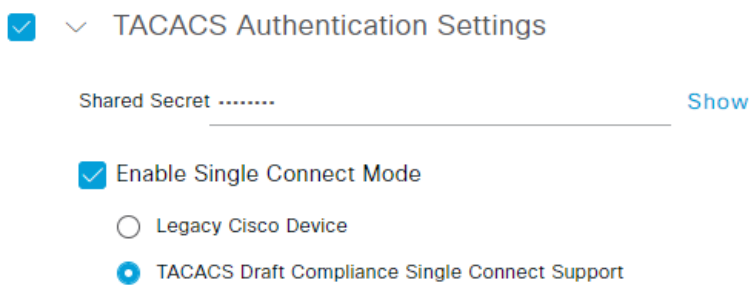


Step 3: Add Network Device

- Navigate to **Administration > Network Devices**. Click add and fill out all the fields with an asterisk next to them. Select the Network device group we created as Device type.

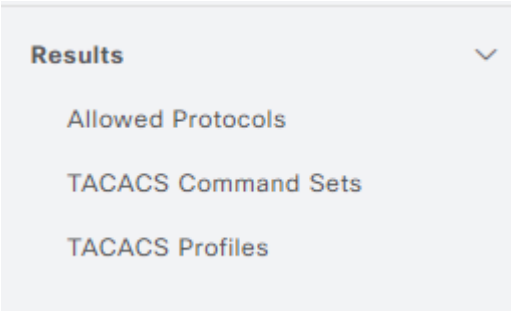


- Go to **TACACS Authentication Settings** and type the **Shared Secret**. Select **Enable Single Connect Mode** and the **TACACS Draft Compliance Single Connect Support**.

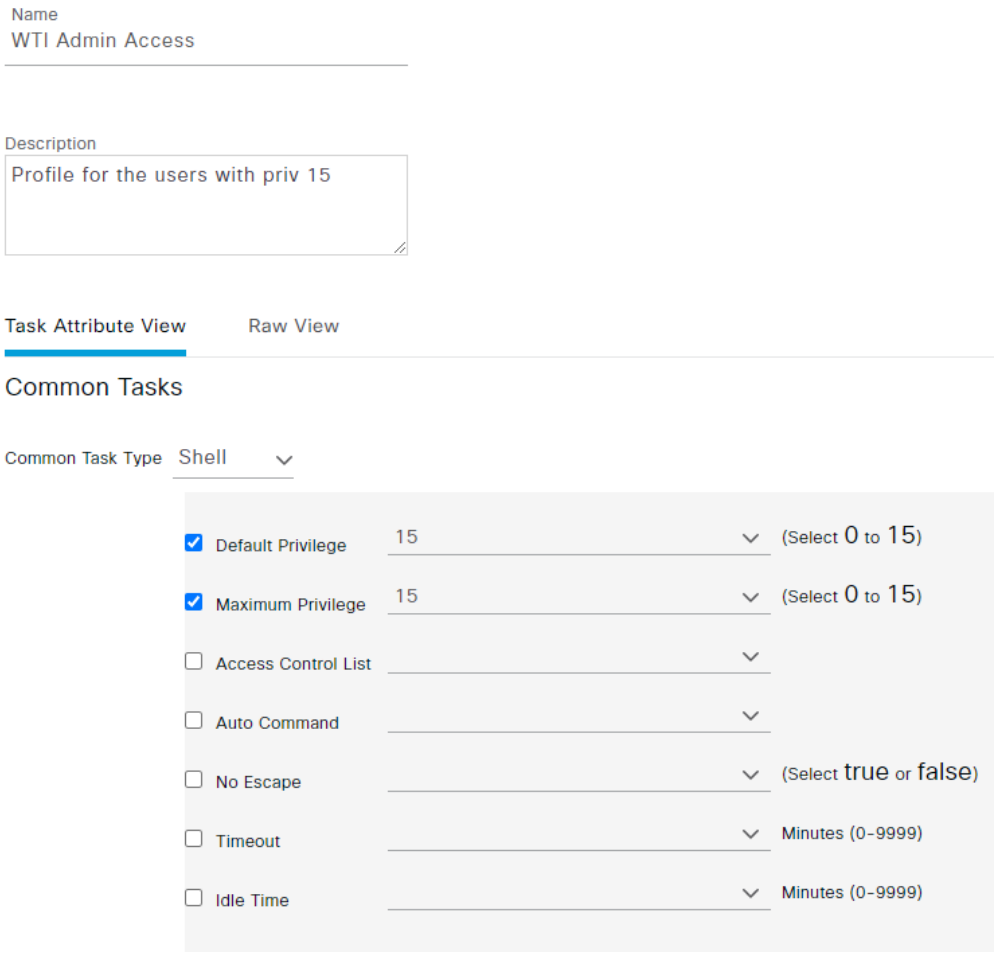


Step 4: TACACS Profiles and TACACS Command Sets

- To configure the profile, navigate to **Work Centers > Policy Elements**. On the left-hand side select **Results** and click the dropdown arrow.



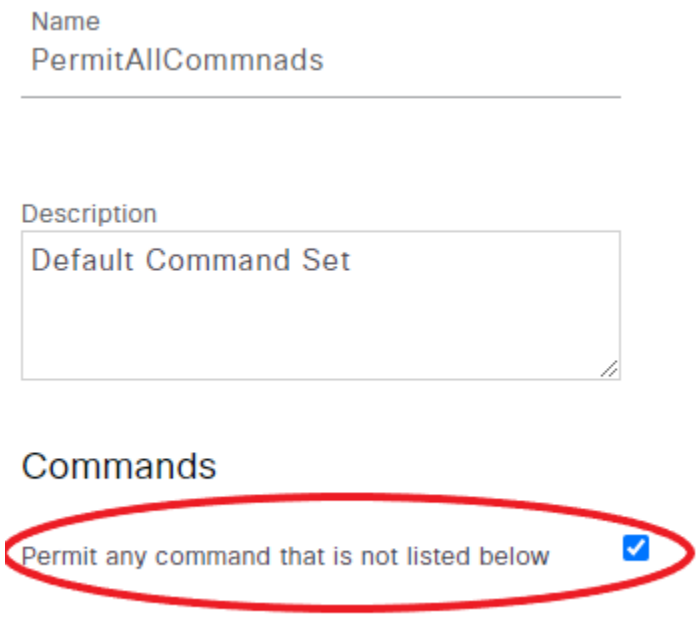
- Select TACACS Profiles and click Add. Below is the profile for Admin level access witht the privilege level 15.



- **Privilege levels for the different access levels:**

  View Only – 0-4
  User – 5-9
  Superuser – 10-14
  Admin – 15

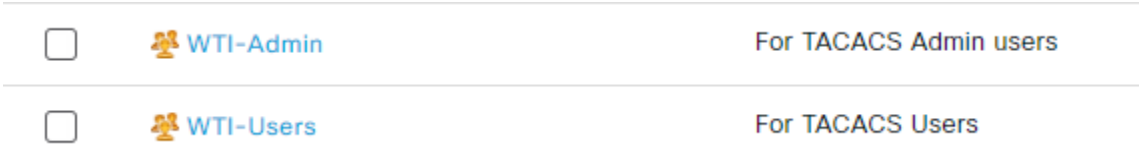
- Add a command set in **TACACS Command Sets** to permit all. Click Add from the top menu and fill out as below:



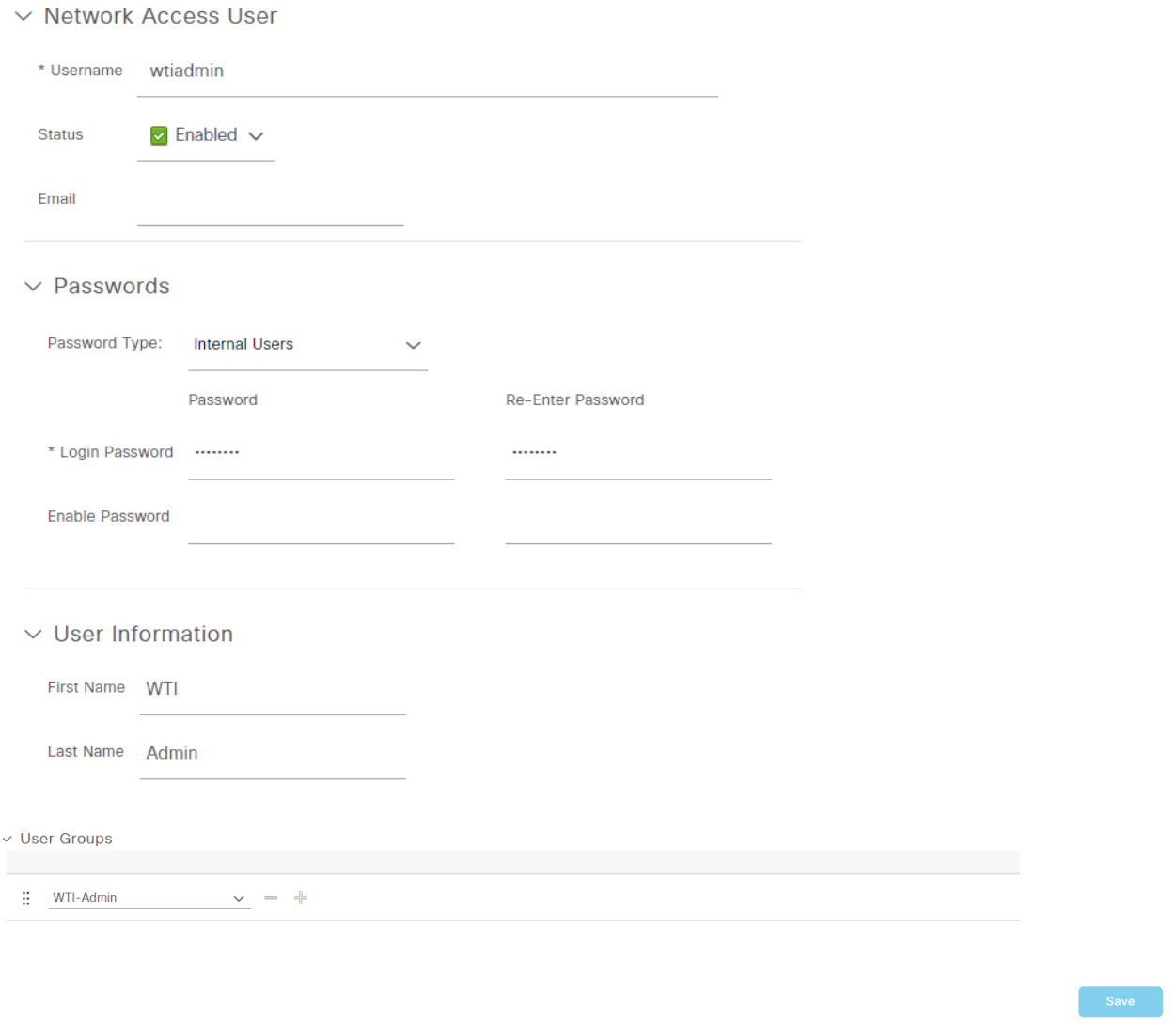
Step 5: Create Users and User Groups

- Navigate to **Work Centers > Device Administration > User Identity Groups** to create User Groups.
- Below is the example for the Admin level group:

- Create one group for Admin level access and one group for User level access.



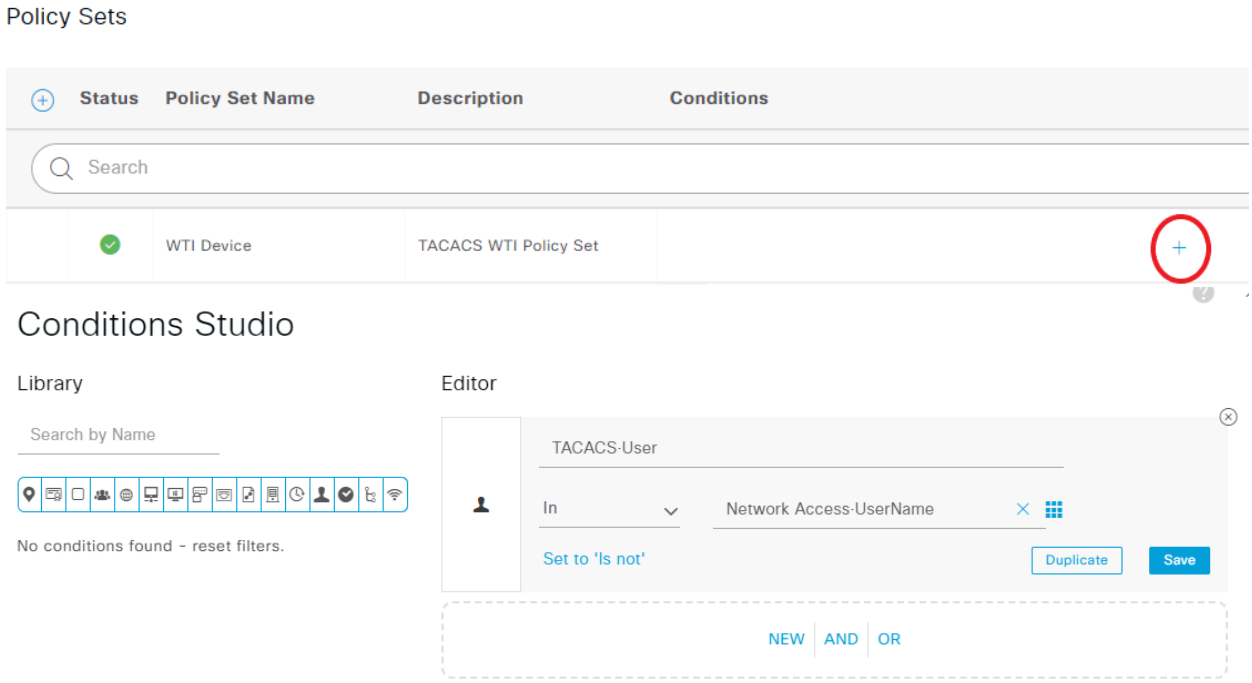
- Navigate to **Work Centers > Device Administration > Identities** to create Users.
- Below is the example for User with the Admin level and added to the User Group:



- Create one User with Admin level access and one User with User level access.

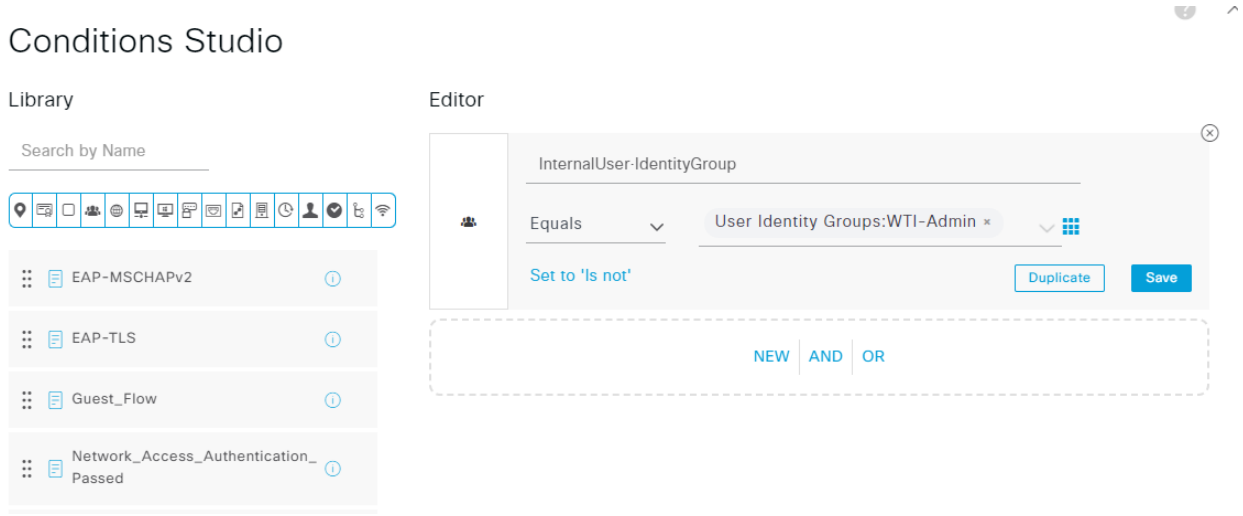
Step 6: Create Policy Sets for device administration

- Go to **Work Centers > Device Administration > Device Admin Policy Sets** and click ADD**.** Then, select the + icon and it will open a new window for **Conditions Studio**.

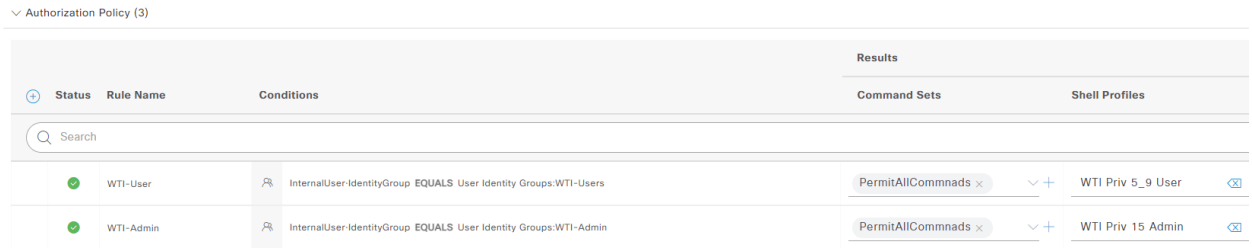


- Next verify that **Default Device Admin** is selected in Allowed Protocols/Server Sequence. Then select left-hand arrow under View to open the Authentication & Authorization Policy section.

- Select **Internal Users** under the **Authentication Policy** option.
- In **Authorization Policy**, click on the + icon to add rule. Assign Rule Name, Command sets to PermitAllCommands and Shell Profiles. To add conditions, click on the + icon and provide information as below in the Conditions Studio.



- Create rules for both Admin and User level Users.



Step 7: Configure the TACACS parameters on WTI

- Issue /n command and select option 28 for TACACS Parameters.

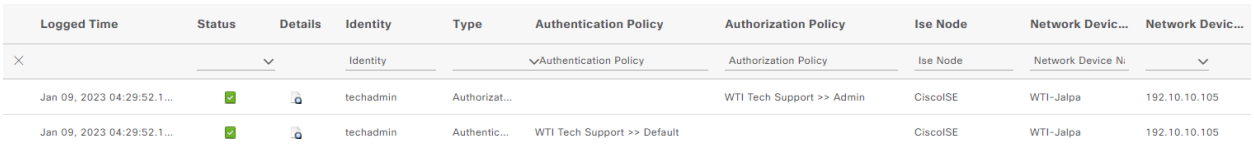
- TACACS Parameters:

  1. Enable: On
  2. Primary host/address: **XXX.XXX.XXX.XXX** (Cisco ISE IP Address)
  3. Secondary host/address: (undefined)
  4. Secret Word: xxxx (TACACS Secret work from CISCO ISE)
  5. Fallback Timer: 15 Sec
  6. Fallback Local: On (All failures)
  7. Authentication Port: 49
  8. Default User Access: Off
  9. Account Management Module: Enabled
  10. Session Management Module: Enabled
  11. Service Name: wti
  12. Debug: Off
  13. Ping Test

- Note: Account Management Module and Session Management Module should be Enabled.

Step 8: Verification

- Navigate to **Operations > TACACS > Live Logs** to view. A successful Authentication should look like the following:



Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devic...	Network Devic...
			Identity		Authentication Policy	Authorization Policy	Ise Node	Network Device Na	
Jan 09, 2023 04:29:52.1...	✓		techadmin	Authorizat...		WTI Tech Support >> Admin	CiscoISE	WTI-Jalpa	192.10.10.105
Jan 09, 2023 04:29:52.1...	✓		techadmin	Authentic...	WTI Tech Support >> Default		CiscoISE	WTI-Jalpa	192.10.10.105

- If you see failures in the Live Logs for different Authorization requests, this could be the result of users trying to issue unauthorized commands.