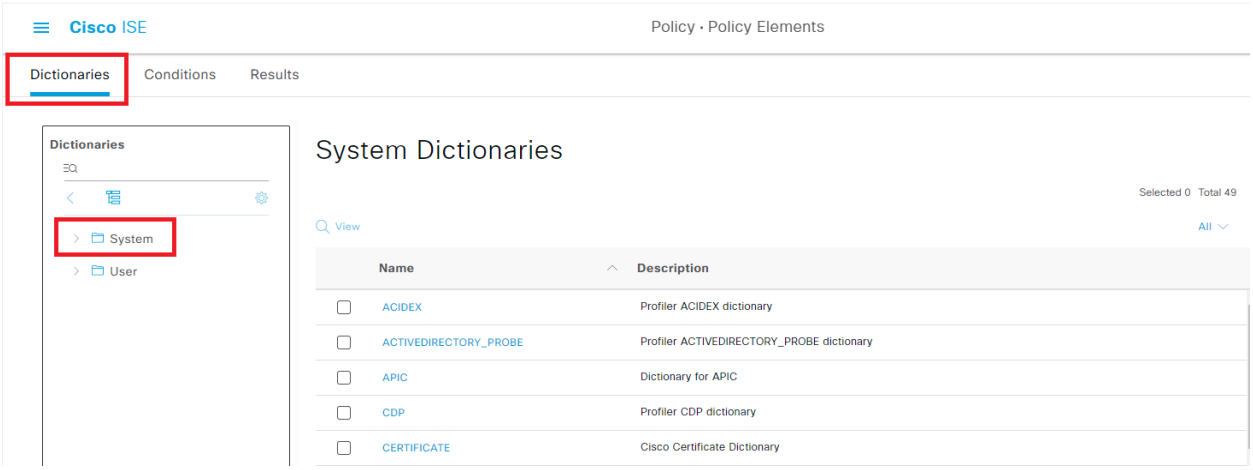
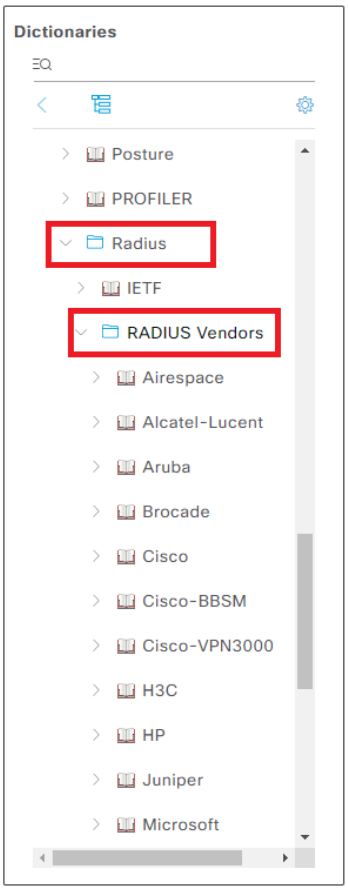
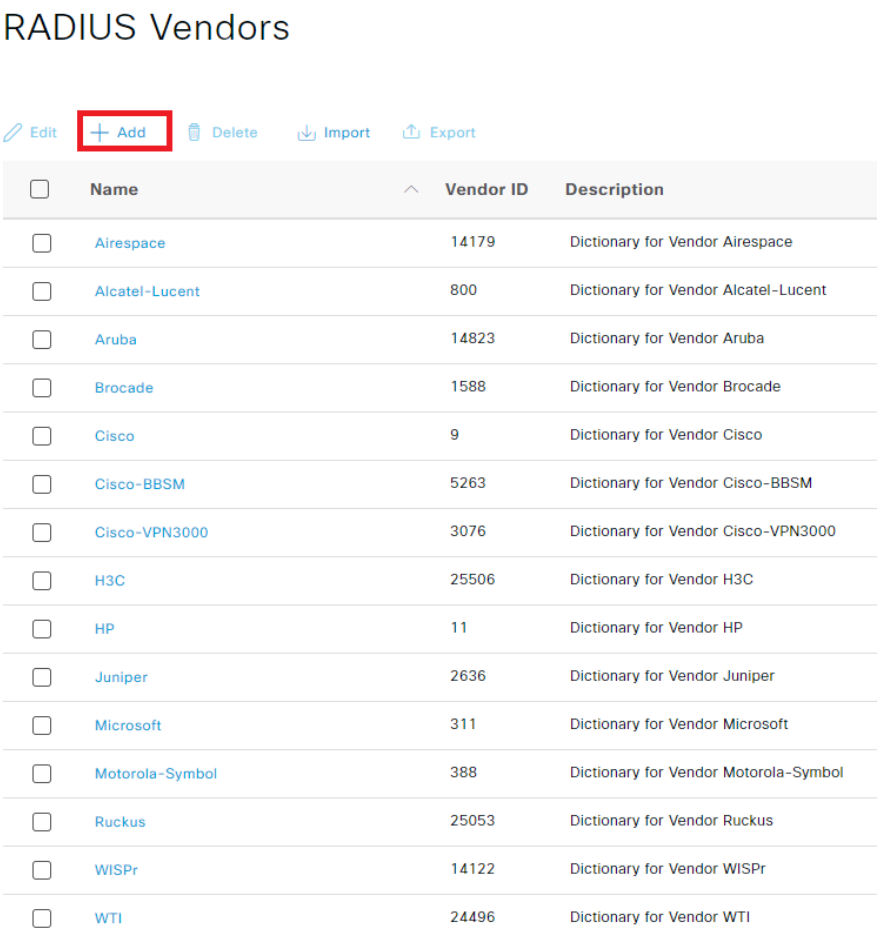
RADIUS with Cisco ISE

Step 1. Create the Vendor-Specific Attribute

1. Navigate to **Policy > Policy Element > Dictionaries > System > Radius > Radius Vendors > Add**

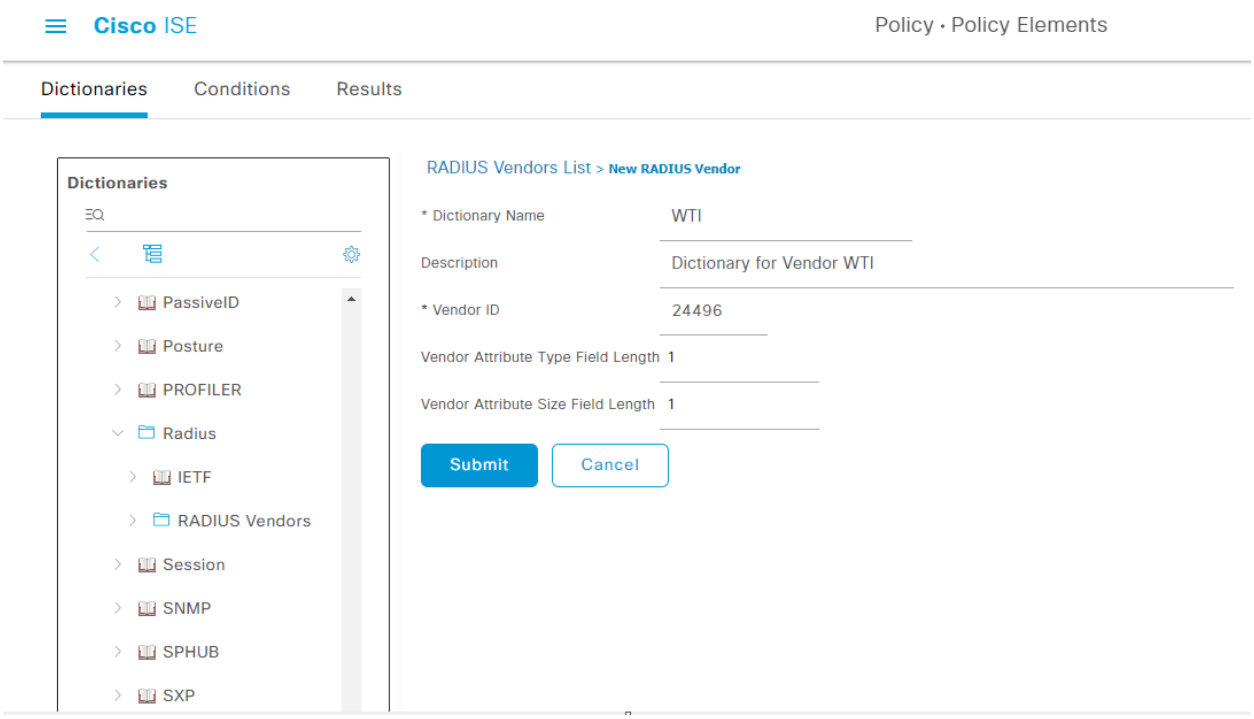




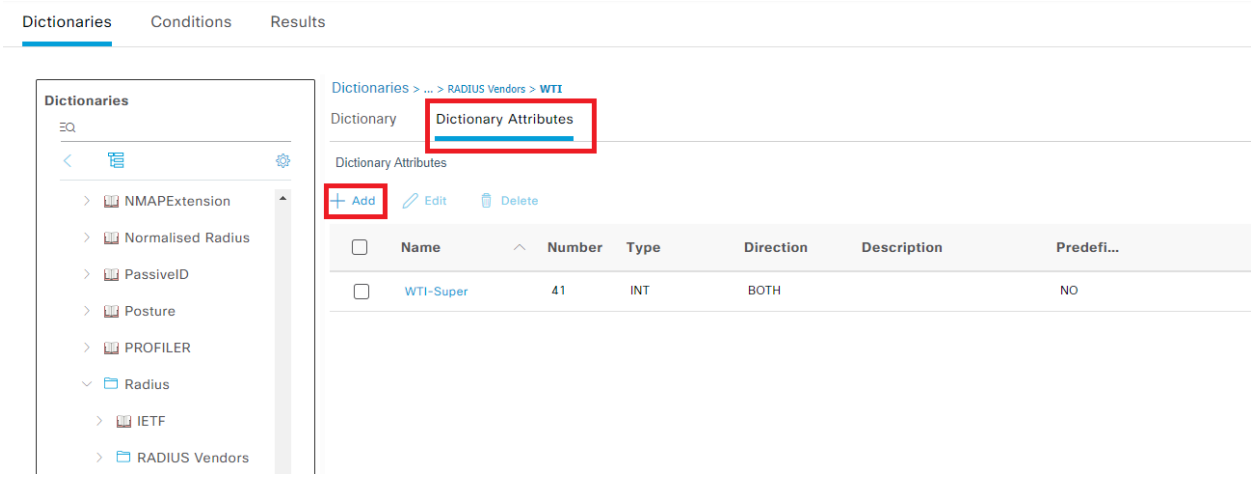


2. The name and the Vendor IDs are to be entered and saved.

Dictionary Name: **WTI**
Vendor ID: **24496**



3. Click the saved Radius Vendor and navigate to Dictionary Attributes.



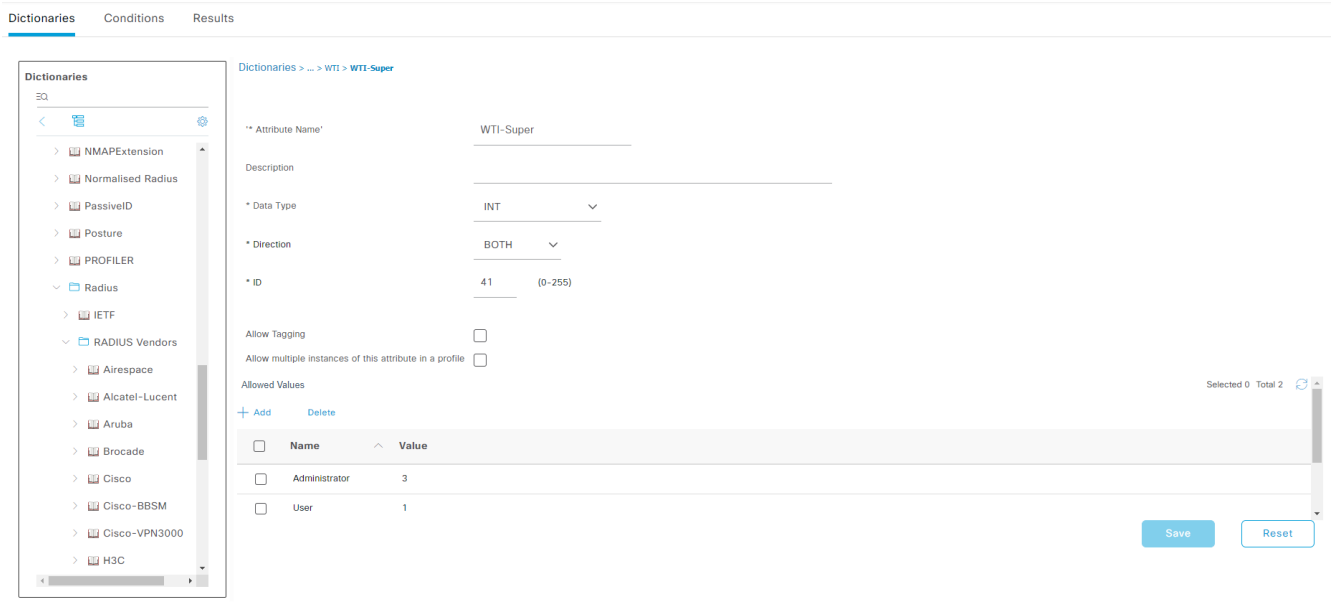
4. Click Add and fill out the Attribute Name, Data Type, Direction and ID and Add allow values for access level.

Attribute Name: **WTI-Super**
Data Type: **INT**
Direction: **BOTH**
ID: **41**

Add allow Values for access level

Name: **Administrator**
Value: **3**

Name: **User**
Value: **1**



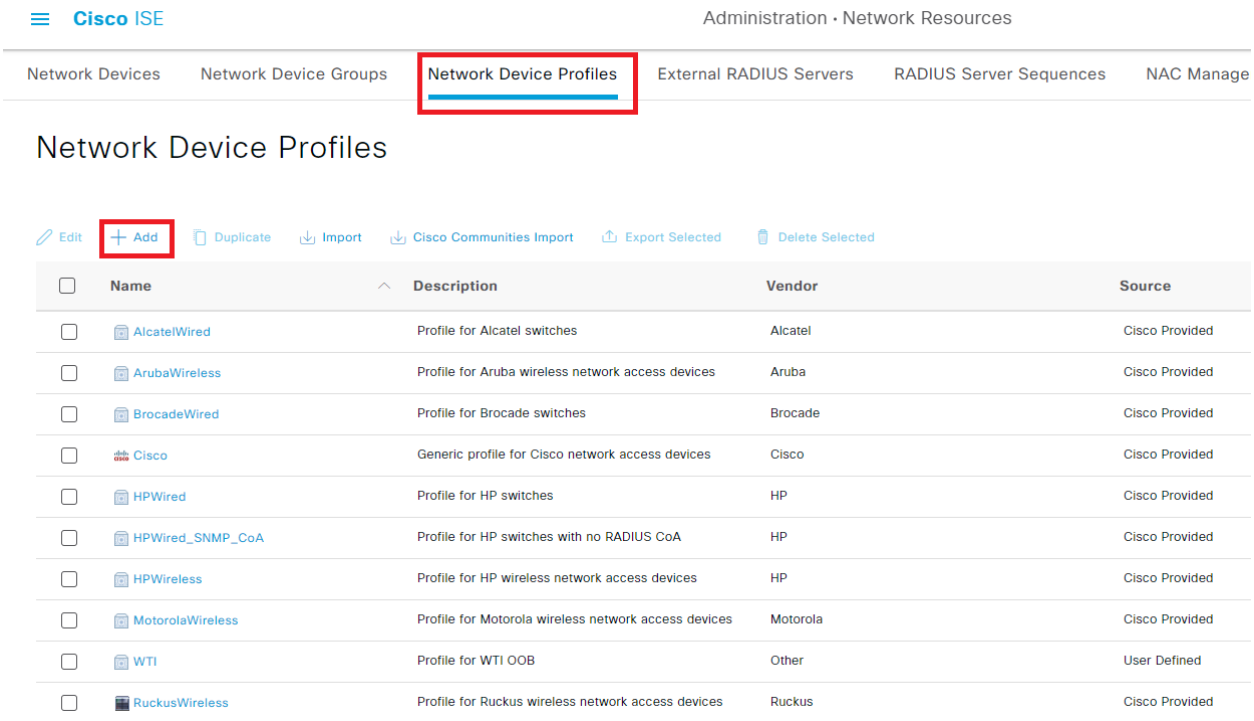
5. Save the attribute.

6. Add other Attributes on the same page if there are multiple Attributes to be added to the same Dictionary.

WTI RADIUS Dictionary https://ftp.wti.com/InfoCenter/rsa/dictionary/dictionary.wti

Step 2. Create a Network Device Profile

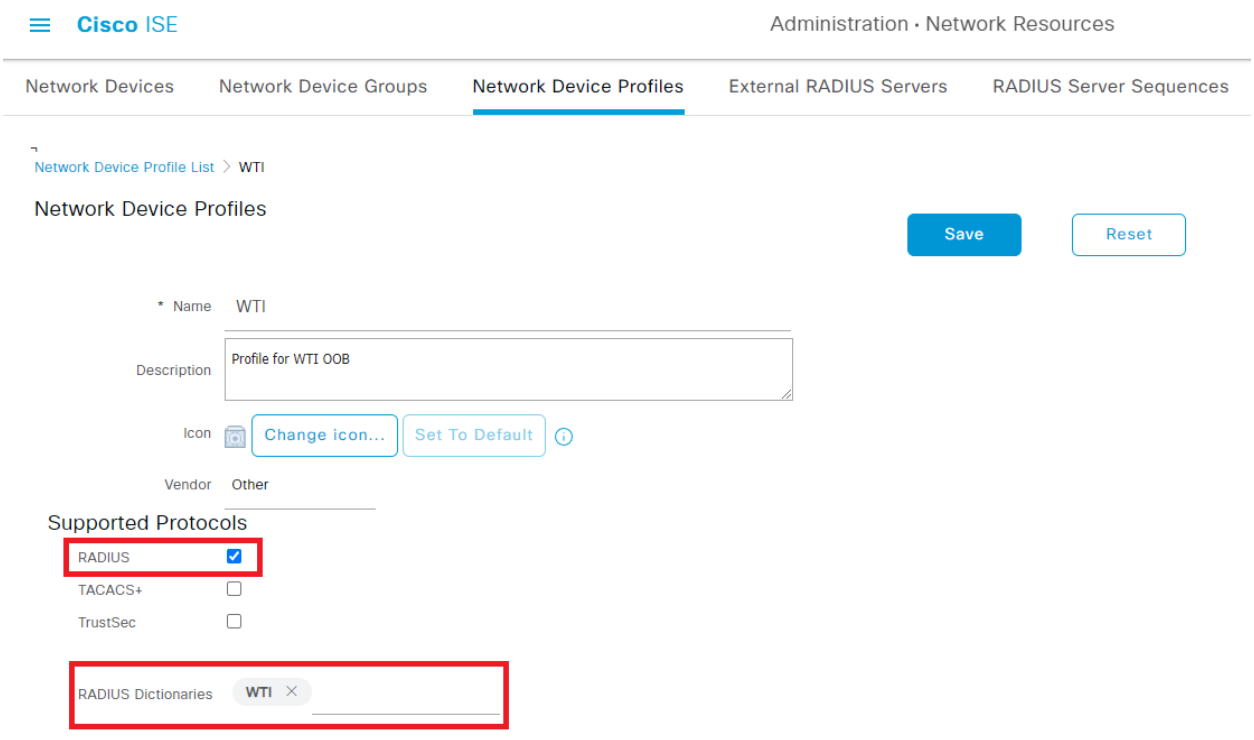
1. Navigate to **Administration > Network Resources > Network Device Profile > Add**



2. Give a name and check the box for **RADIUS**.

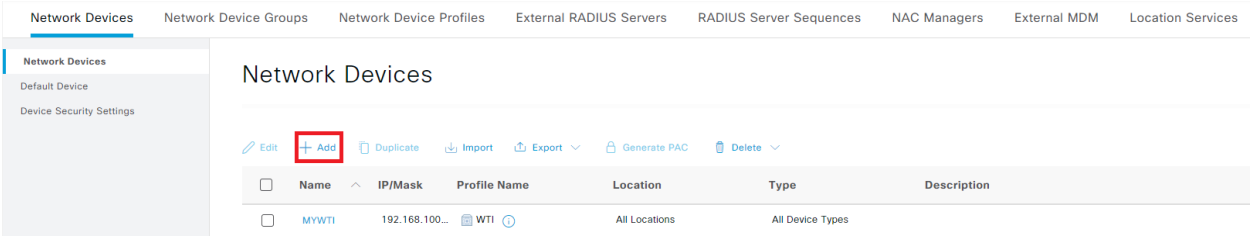
3. Under the **RADIUS Dictionaries**, select the dictionary created in the previous section.

4. If multiple dictionaries were created for the same type of device, all of them can be selected under **RADIUS Dictionaries**.



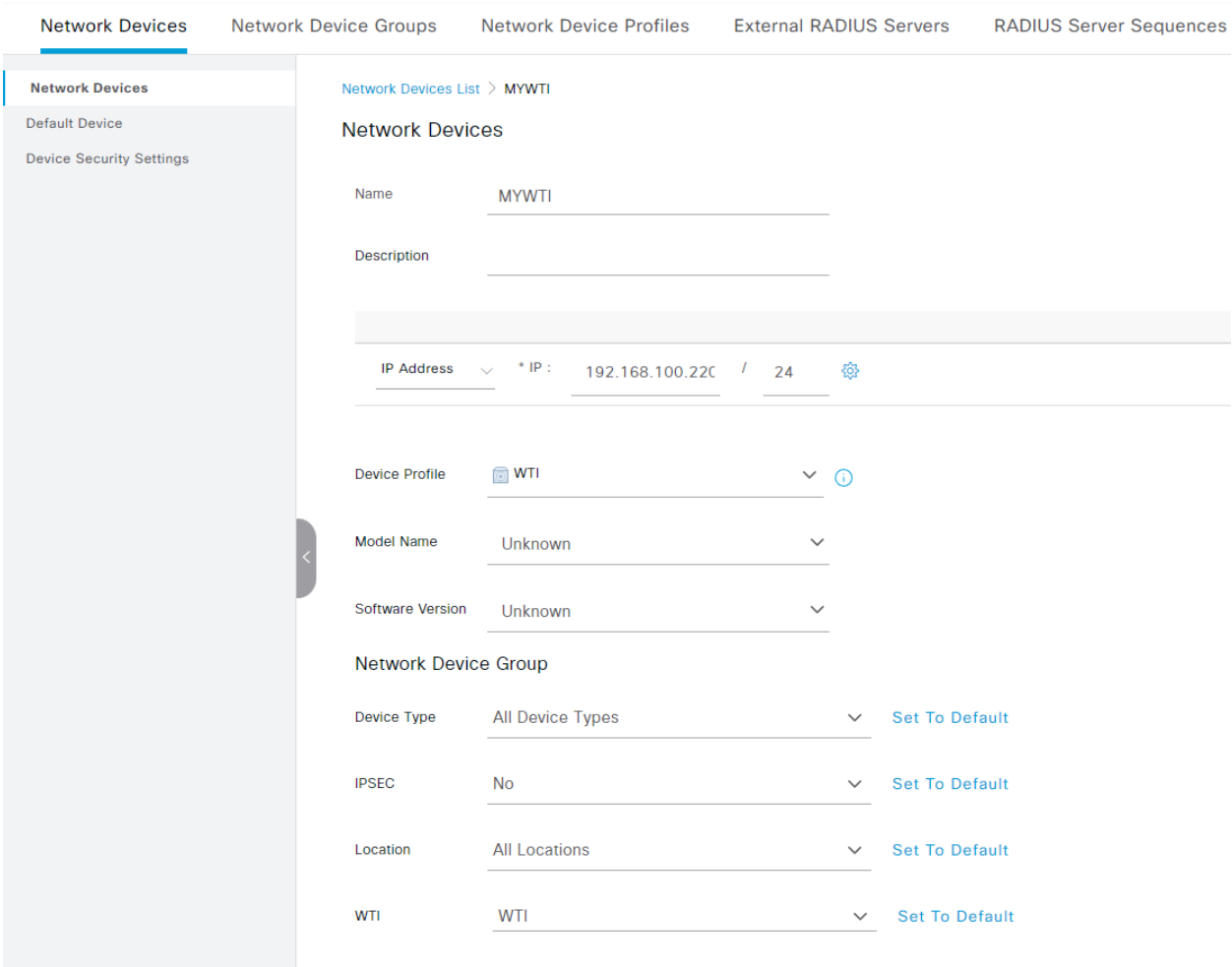
Step 3. Add Network Device on ISE

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



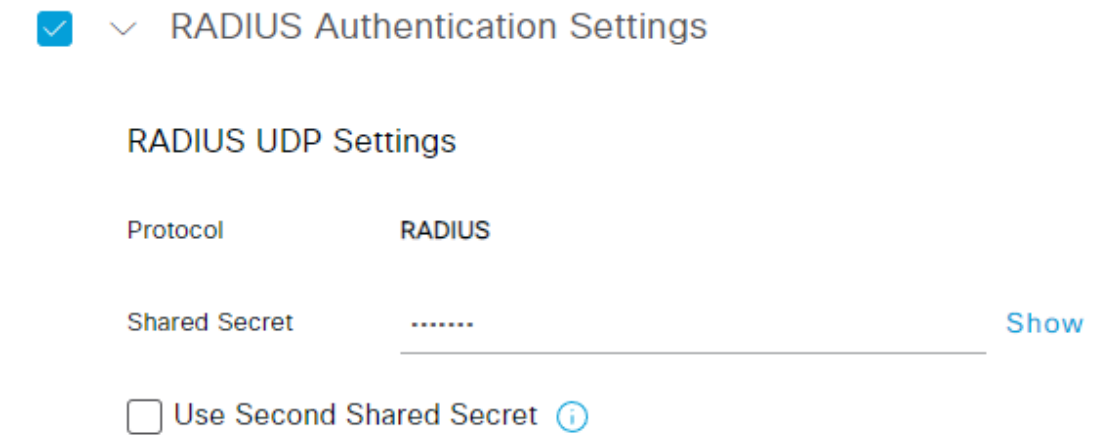
2. Give a name and the IP Address

3. The Device Profile can be chosen from the dropdown list to be the one defined. If a profile was not created, the default Cisco can be used as it is.



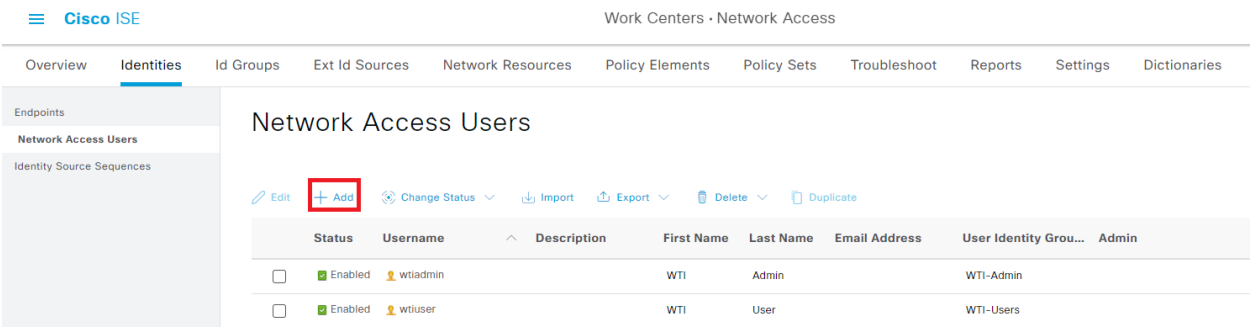
4. Check Radius Authentication Settings.

5. Enter the **Shared Secret Key** and **save** the device.

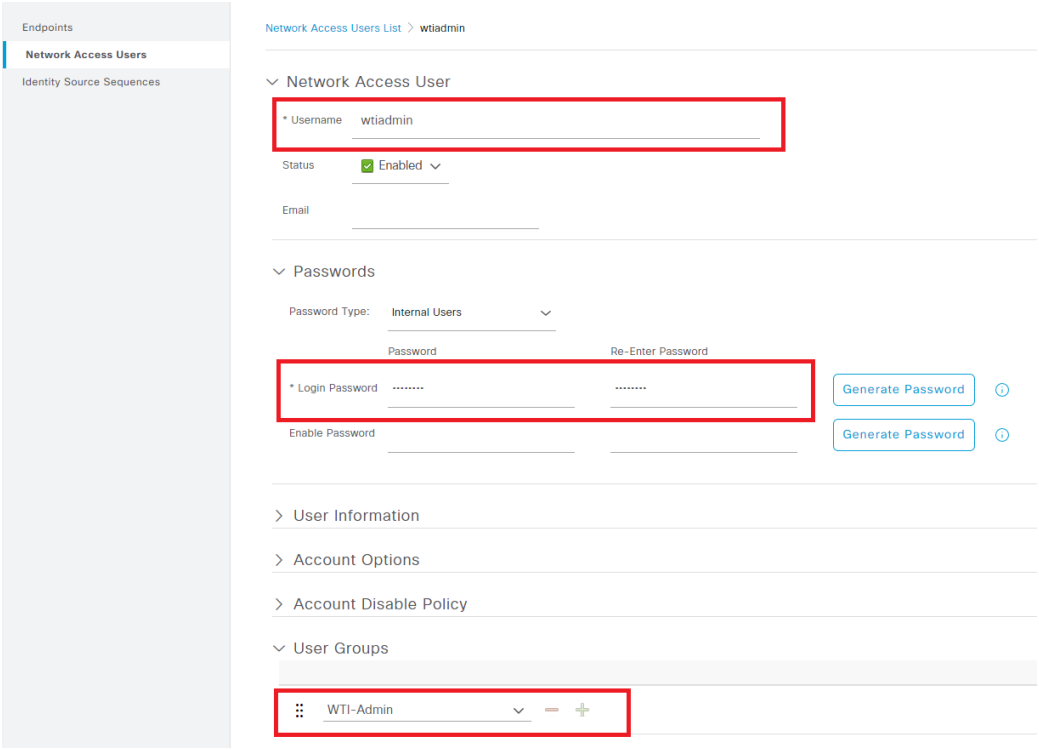


Step 4. Create Network Access Users

1. Navigate to **Work Centers > Network Access > Identities > Network Access Users > Add**

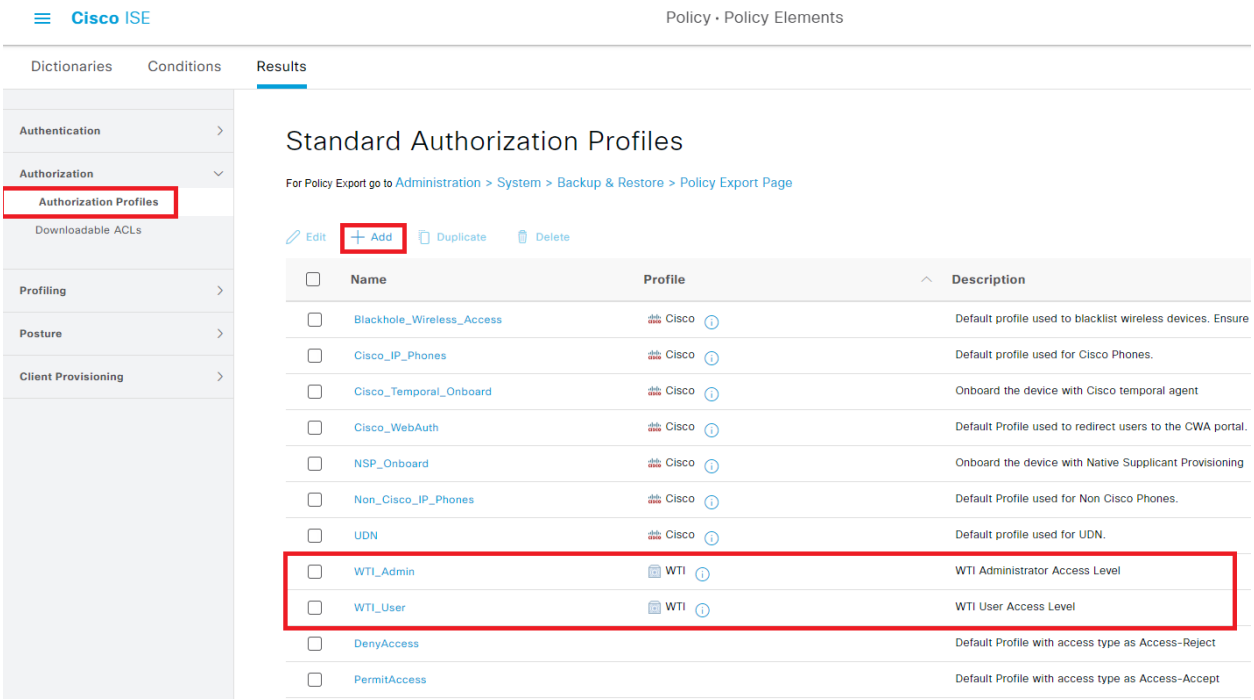


2. Fill out network access, password section and assign User Groups

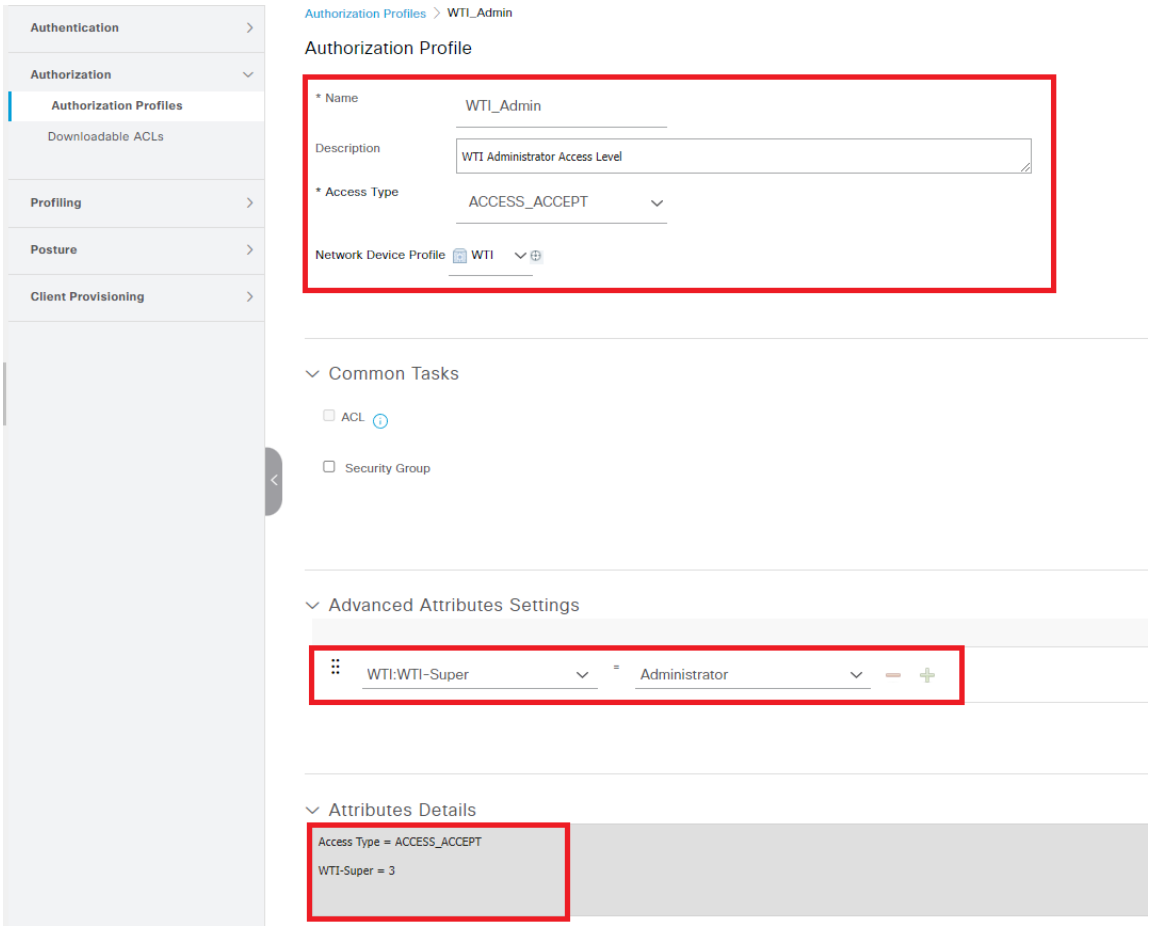


Step 5. Create Authorization Profiles

1. Navigate to **Policy > Policy Elements > Results > Authorization Profiles > Add**

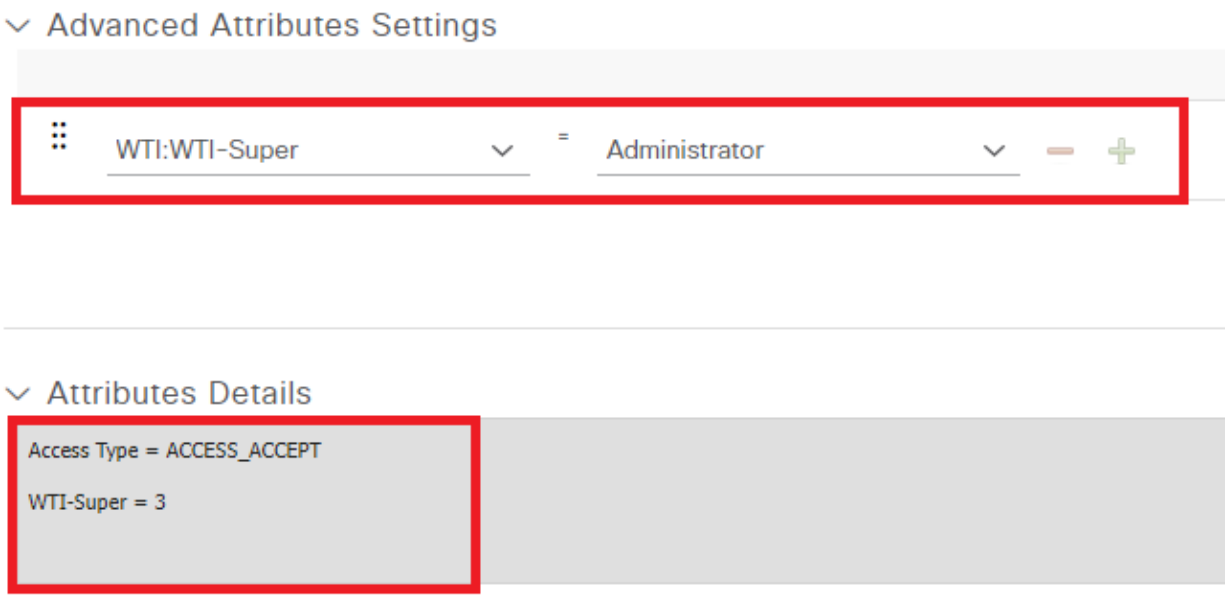


2. Create two Authorization Profile. One for WTI_Admin (Administrator access level) and another for WTI_User (User access level).



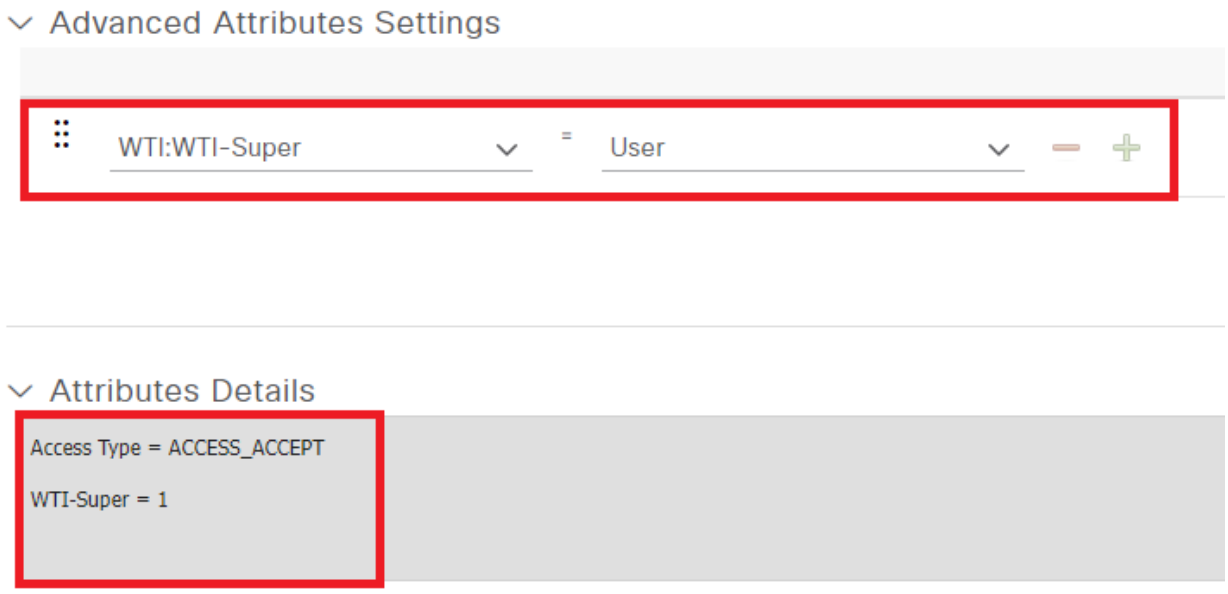
For WTI_Admin

In advanced Attribute Settings



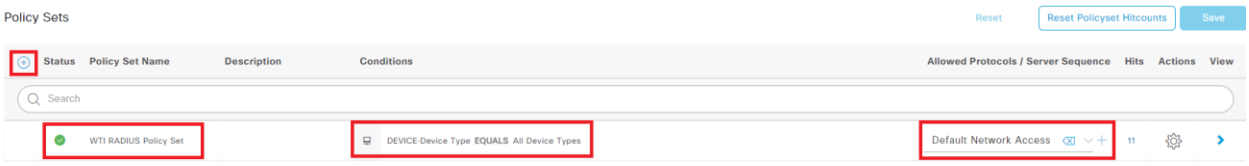
For WTI_User

In Advance Attribute Settings



Step 6. Create Policy

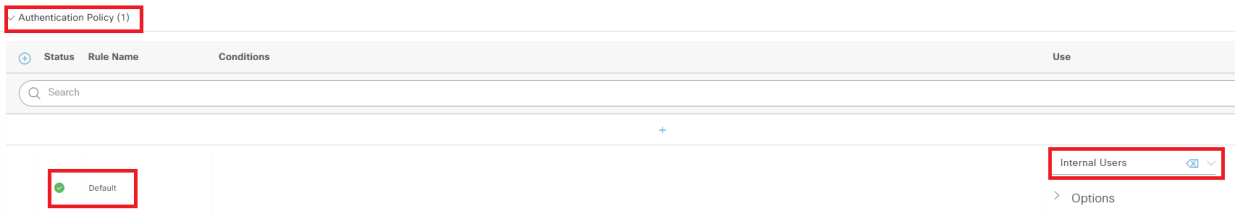
1. Navigate to **Policy > Policy Sets > click (+) to add new policy set**.



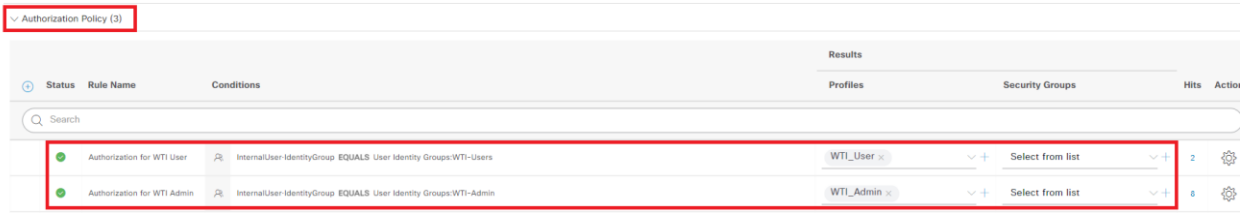
Policy Set Name: **WTI RADIUS Policy Set**
Condition: DEVICE: Device Type **EQUALS** All Device Types
Allowed Protocols: **Default Network Access**

2. Authentication Policy

Rule Name: Default
Use: **Internal User**

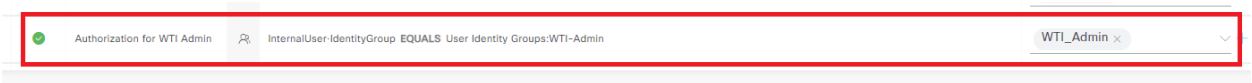


3. Authorization Policy – create two authorization policy, one for WTI_Admin and another for WTI_User.



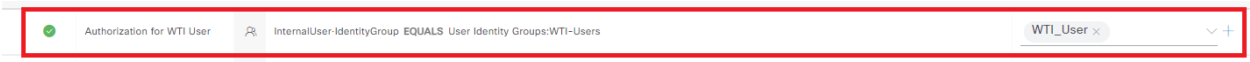
For WTI_Admin

Rule Name: **Authorization for WTI-Admin**
Condition: Internal User-IdentityGroup **EQUALS** User Identity Groups:WTI-Admin
Profile: **WTI_Admin**

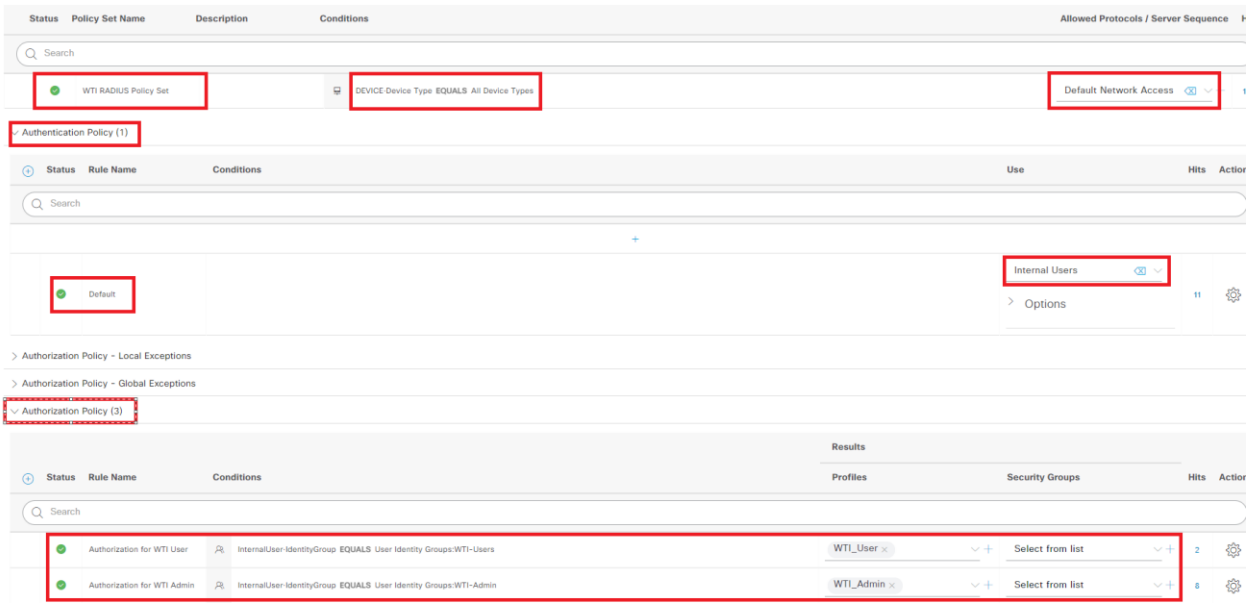


For WTI_User

Rule Name: **Authorization for WTI-User**
Condition: Internal User-IdentityGroup **EQUALS** User Identity Groups:WTI-User
Profile: **WTI_User**



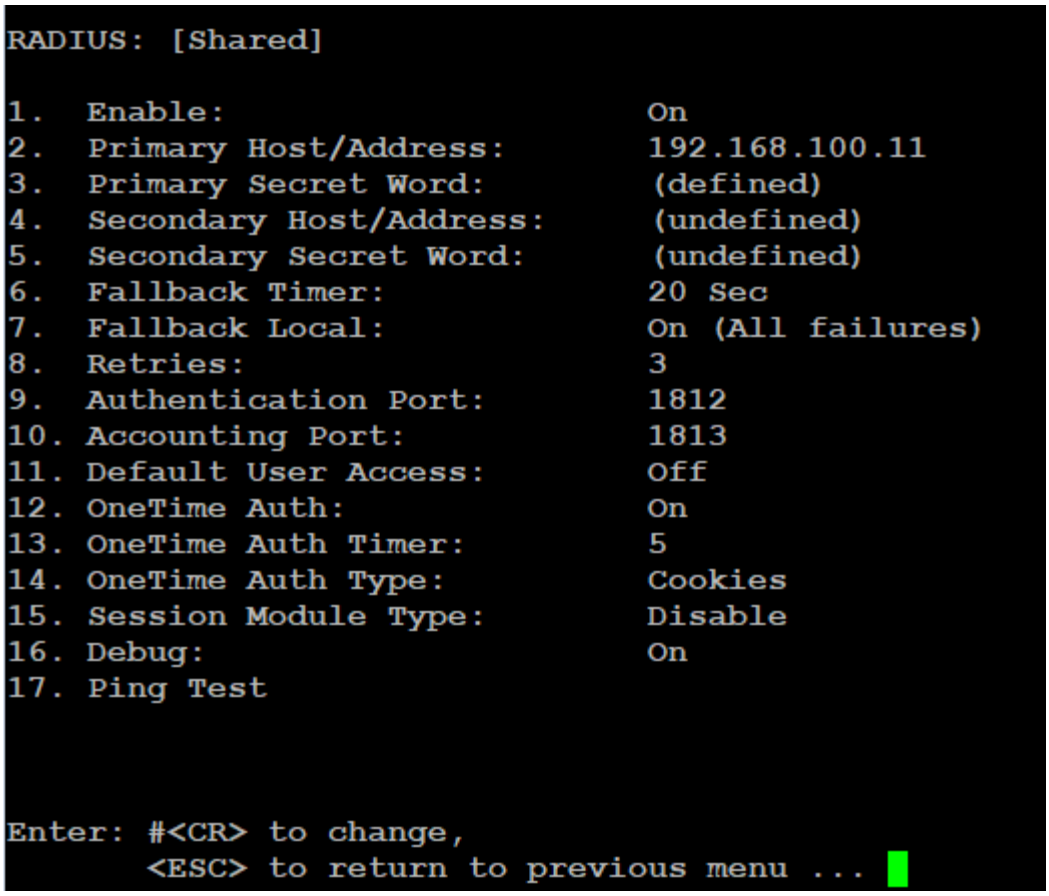
Overview of Policy



WTI RADIUS Setting

1. Go to /N option 29 for Radius
2. RADIUS Setting

Enable: **ON**
Primary Host/Address IPv4: **XXX.XXX.XXX.XXX** (Cisco ISE IP Address)
Primary Secret word: **xxx** (Radius secret from Cisco ISE)
Fallback Timer: **20**
Fallback Local: **On (All failure)**
Retries: **3**
Authentication Port: **1812**
Accounting Port: 1813
Default User Access: **OFF**
OneTime Auth: **On**
OneTime Auth Timer: **5**
OneTime Auth Type: **Cookies**
Session Module Type: **Disable**
Debug: **On**


RADIUS: [Shared]
1. Enable: On
2. Primary Host/Address: 192.168.100.11
3. Primary Secret Word: (defined)
4. Secondary Host/Address: (undefined)
5. Secondary Secret Word: (undefined)
6. Fallback Timer: 20 Sec
7. Fallback Local: On (All failures)
8. Retries: 3
9. Authentication Port: 1812
10. Accounting Port: 1813
11. Default User Access: Off
12. OneTime Auth: On
13. OneTime Auth Timer: 5
14. OneTime Auth Type: Cookies
15. Session Module Type: Disable
16. Debug: On
17. Ping Test
Enter: #<CR> to change,
<ESC> to return to previous menu ...