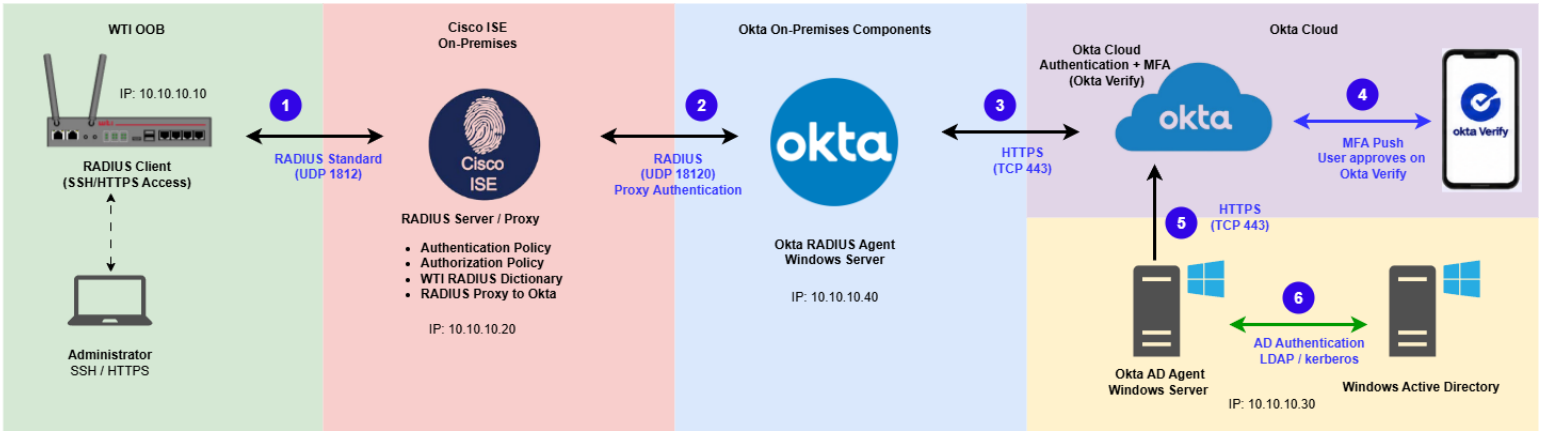
Cisco ISE + OKTA MFA + Windows AD Integration for WTI (Standard RADIUS)



How it works:

1. WTI → Cisco ISE

- RADIUS authentication from WTI OOB device to Cisco ISE
- Standard RADIUS (UDP 1812)
- WTI is the RADIUS client

2. Cisco ISE → Okta RADIUS Agent

- Cisco ISE proxies the RADIUS request to Okta RADIUS Agent. RADIUS (UDP 18120)
- ISE handles Access-Challenge and Access-Accept/Reject
- WTI vendor-specific authorization attributes must be passed to WTI (verify in ISE configuration)

3. Okta RADIUS Agent → Okta Cloud

- Okta RADIUS Agent communicates with Okta cloud service over HTTPS (TCP 443)
- Forwards authentication request and handles MFA challenge/response

4. Okta Cloud → Okta Verify

- Okta send MFA push notification to the user's Okta Verify App
- User approves the push

5. Okta Cloud → Okta AD Agent

- Okta cloud connects to on-premises Okta AD Agent for primary authentication
- HTTPS (TCP 443)

6. Okta AD Agent → Active Directory

- Okta AD Agent validates the user credentials with Windows Active Directory
- LDAP / Kerberos

1. Prerequisites and Requirement

1.1 In this Demo:

- WTI with Radius Client (device ip: 10.10.10.10)
- Cisco ISE (server ip: 10.10.10.20)
- Okta RADIUS Agent/Windows Server (server ip: 10.10.10.40)
- Okta AD Agent and Active Directory synchronized (server ip: 10.10.10.30)
- Okta Verify on mobile App install and enrolled.

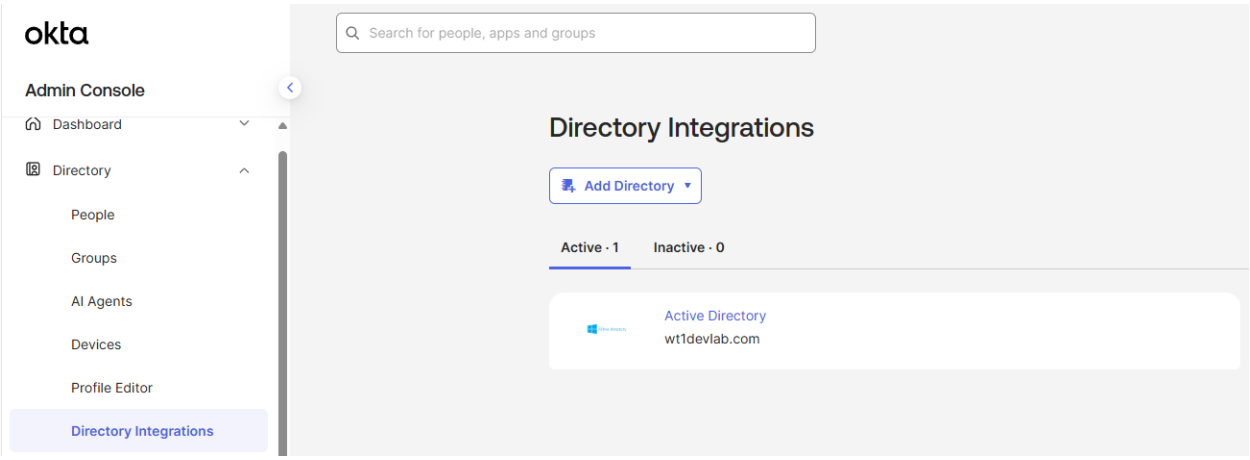
1.2 Network and firewall requirement

Source	Destination	Protocol / Port	Purpose
WTI device	Cisco ISE	UDP 1812	RADIUS authentication request
WTI device	Cisco ISE	UDP 1813	RADIUS accounting, if used
Cisco ISE	Okta RADIUS Agent	UDP 18120	Proxied RADIUS authentication (custom port)
Okta RADIUS Agent	Okta cloud	HTTPS 443	Okta authentication, policy, and MFA communication

2. Okta Configuration

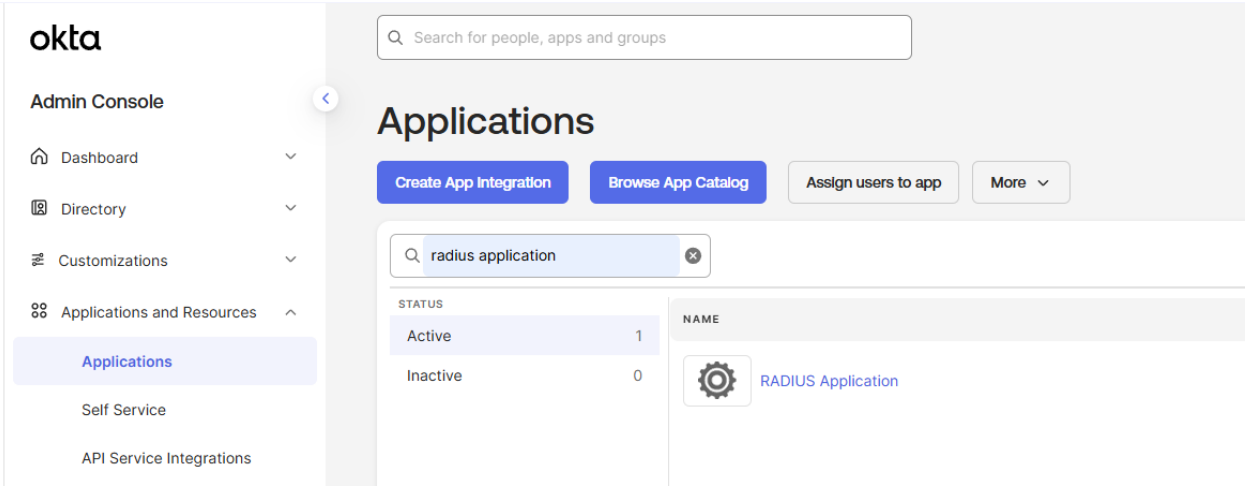
2.1 Directory Integrations

1. Add Active Directory and install Okta AD Agent in your active directory Windows server and follow the setup from the screen until complete.

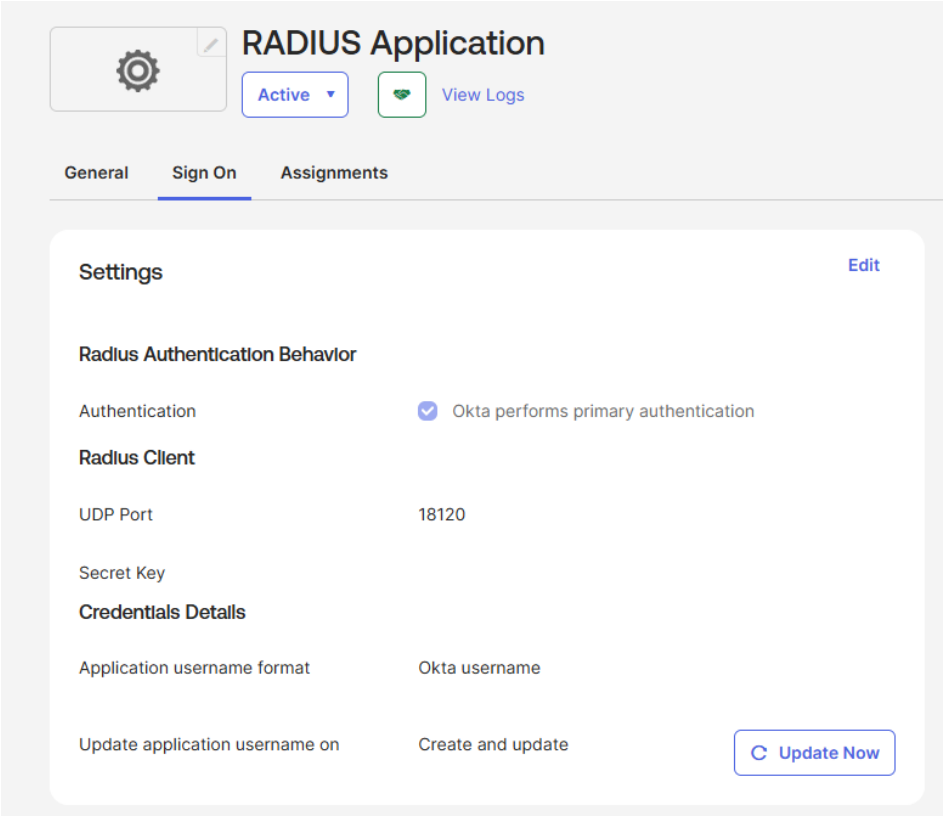


2.2 Configure the RADIUS application

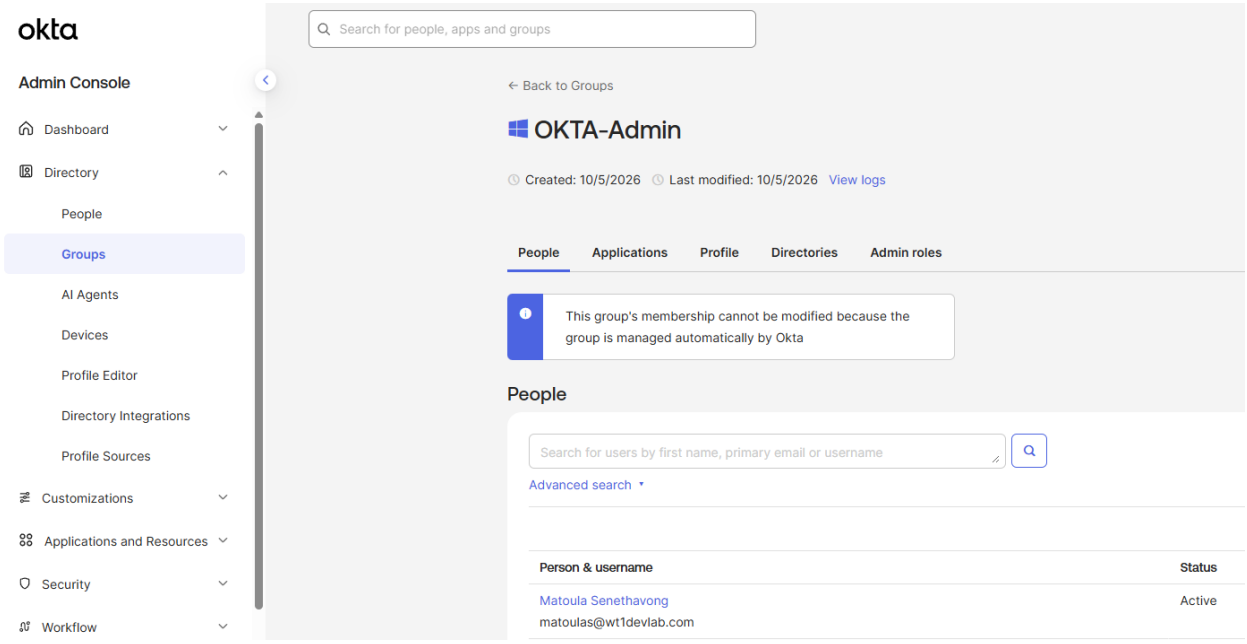
1. Go to **Applications and Resources** > **Application** > in the search box type **radius application**



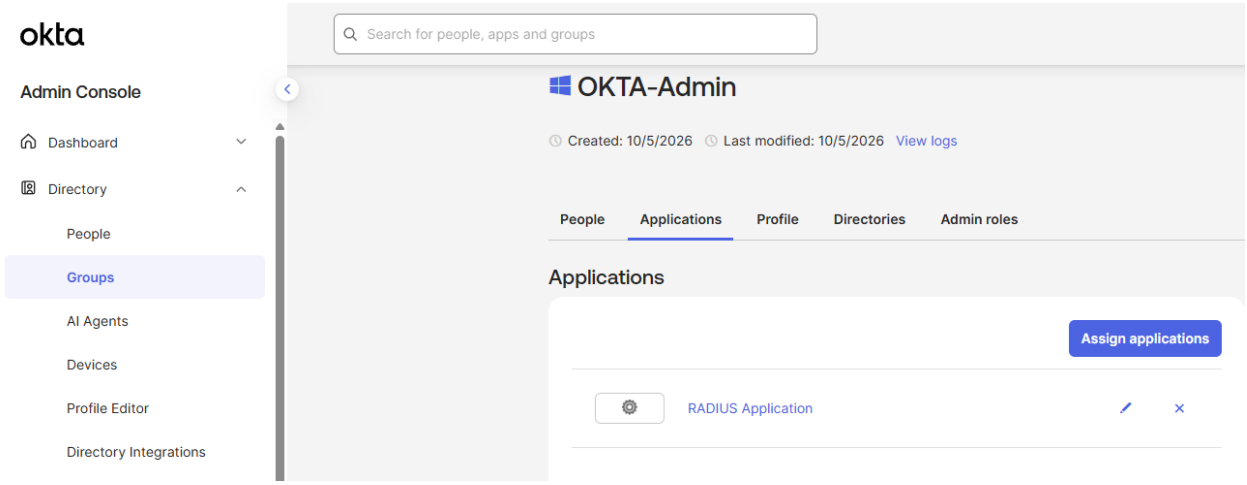
2. Configure the Okta RADIUS application to use the Okta RADIUS Agent.
3. Use the RADIUS authentication port configured on the agent. UDP Port: 18120.
4. Configure the RADIUS client/shared secret so Cisco ISE is accepted as the client when ISE proxies' requests to Okta.
5. Enable the desired MFA behavior (for example, Okta Verify Push).



6. Create or use role group such as OKTA-Admin and OKTA-User from Active Directory security group.

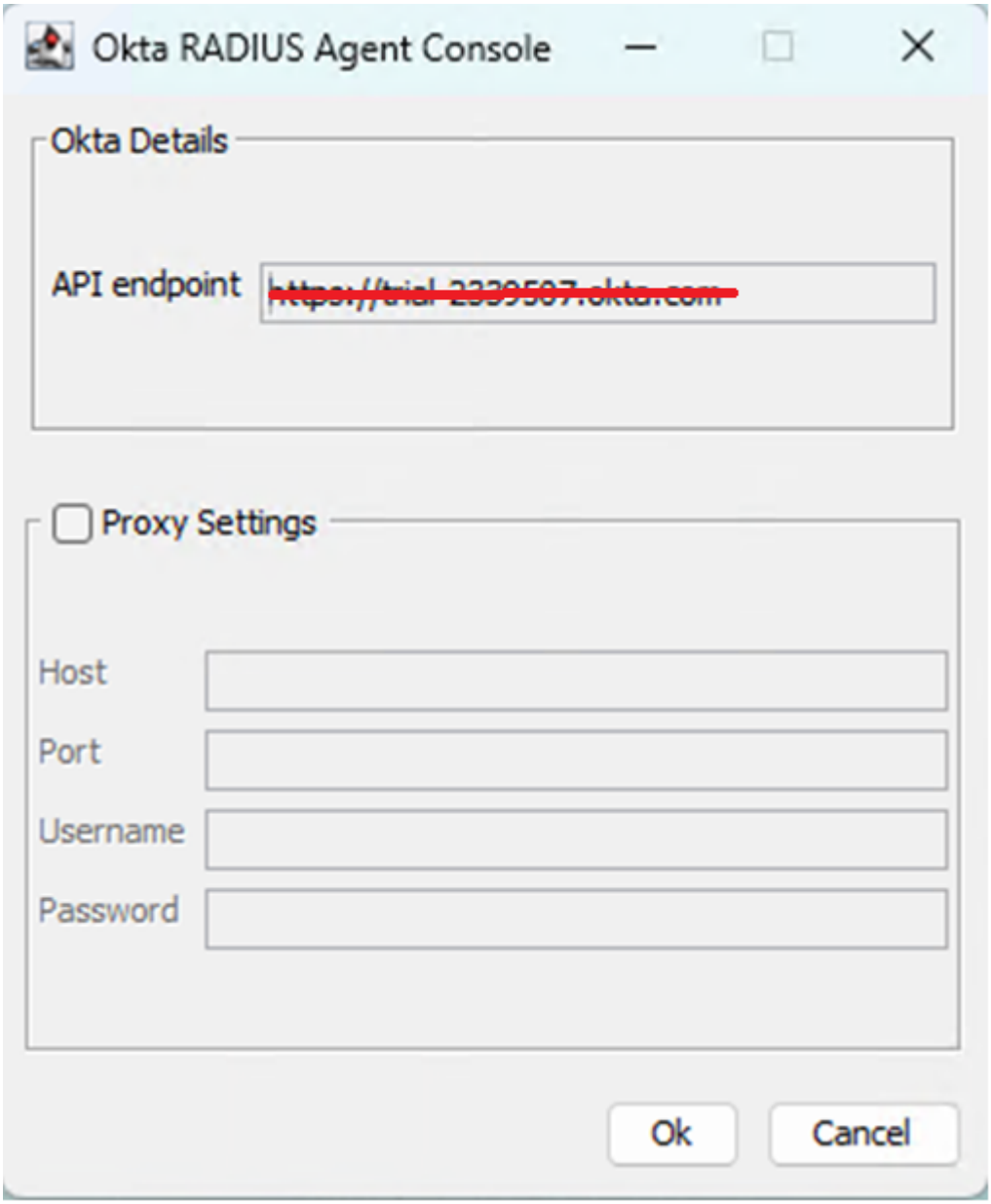


7. Assign the user to the Okta RADIUS application.



3. Okta RADIUS Agent Windows Server Configuration

3.1. Install Okta Radius Agent in windows server and complete the setup from the screen until complete.



3.2 Okta RADIUS Agent – Authorized RADIUS Client IP Addresses

Purpose: Restrict RADIUS authentication requests to approved RADIUS clients for security.

The Okta RADIUS Agent uses an IP allow list to control which RADIUS servers or network devices are permitted to send authentication requests to the agent.

Configuration file:

C:\Program Files\Okta\Okta RADIUS Agent\current\user\config\radius\config.properties

Configuration setting:

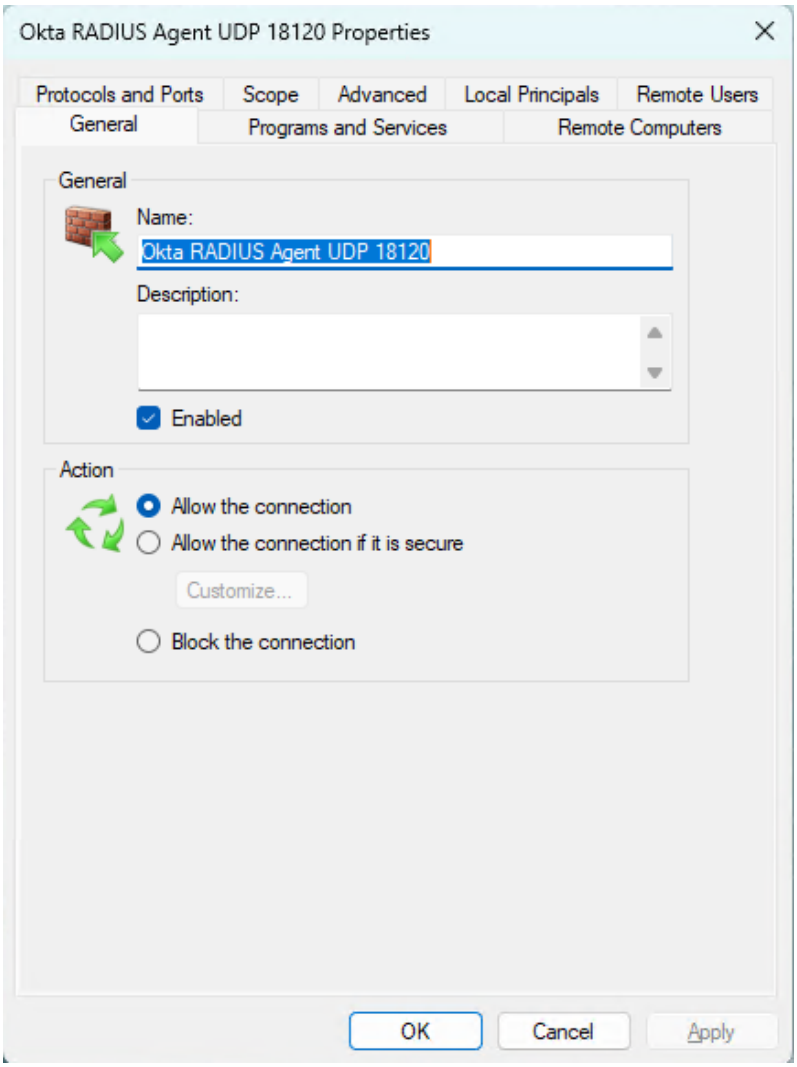
ragent.client_ip_allow_list.18120=10.10.10.20,10.10.10.30

(this will be your Cisco ISE server and your Windows AD server IP Address)

3.3 Allow Inbound rule go to Windows Firewall GUI >> Inbound rule

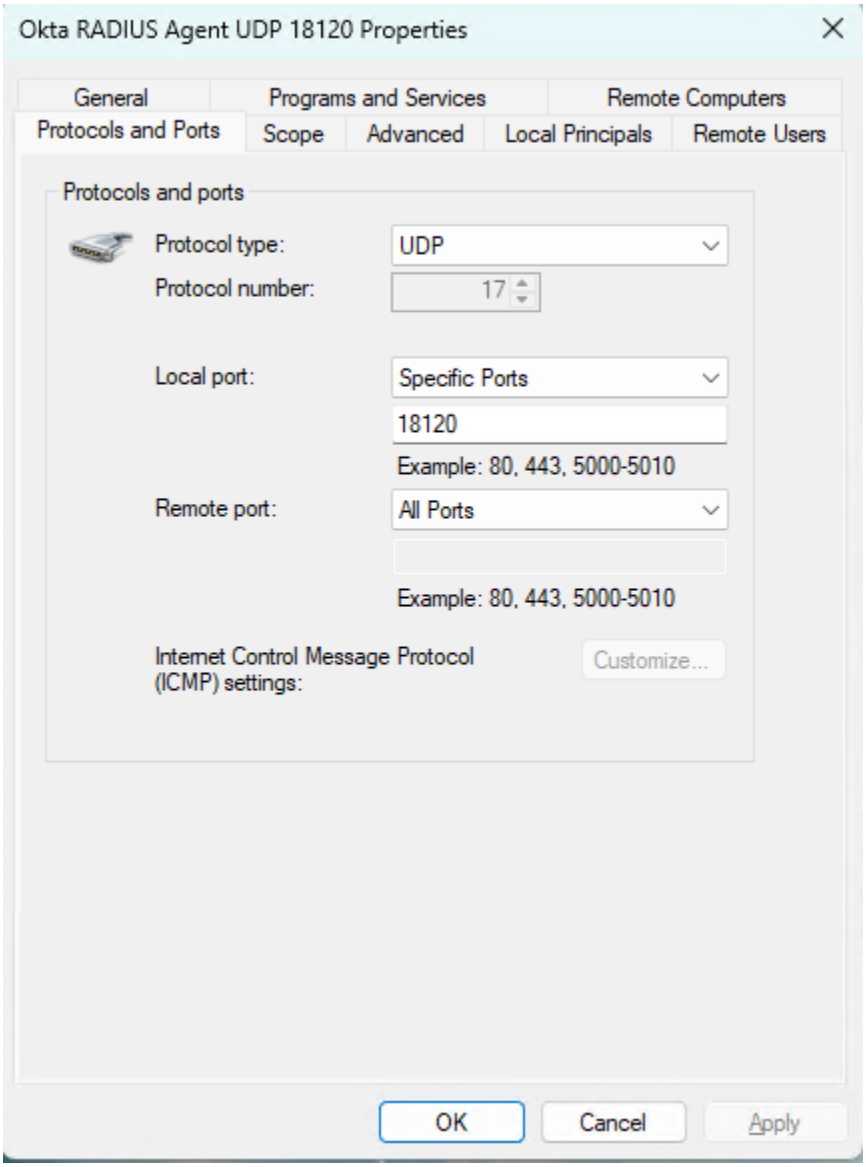
Allow Okta Radius Agent UDP 18120 for remote IP Address 10.10.10.20 and 10.10.10.30

- On the Okta RADIUS Agent server (ip address 10.10.10.40), press **Win + R**.
- Type ***wf.msc*** and press Enter.
- Select Inbound Rules
- New Rule >> Port >> Next >> UDP >> Specific local ports: 18120
- Name: Okta RADIUS Agent UDP 18120



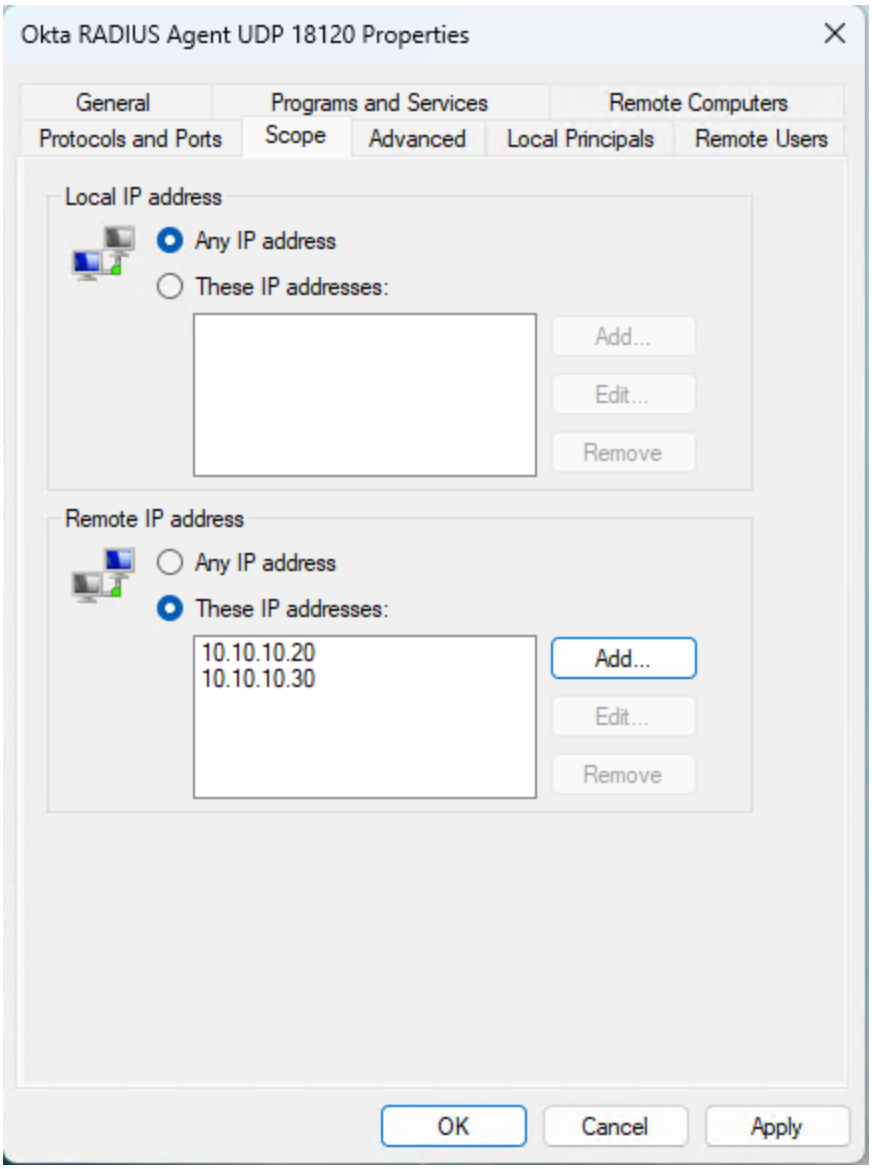
In **Protocols and Ports** section

- Protocol type: UDP
- Local port: Specific ports 18120



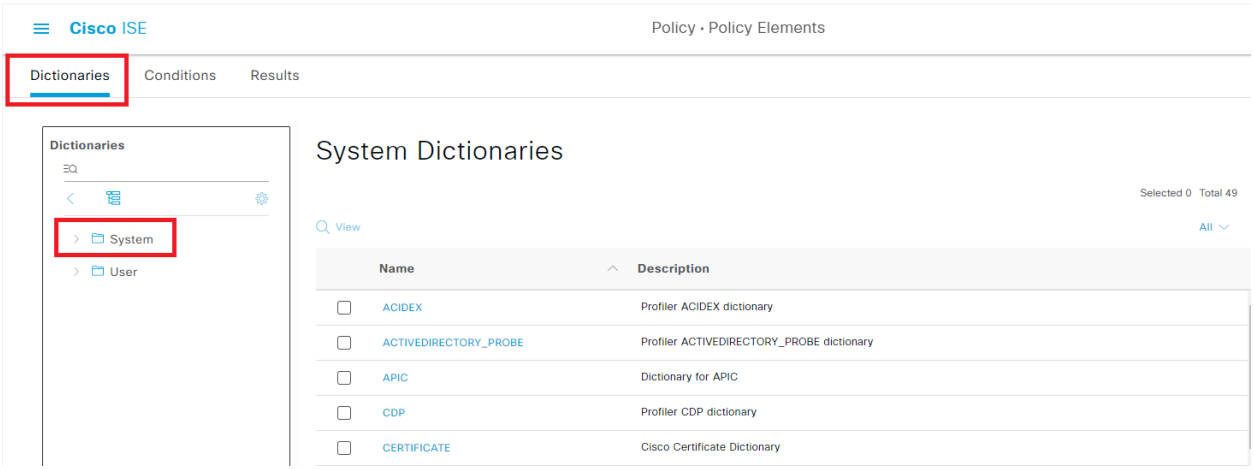
In **Scope** section

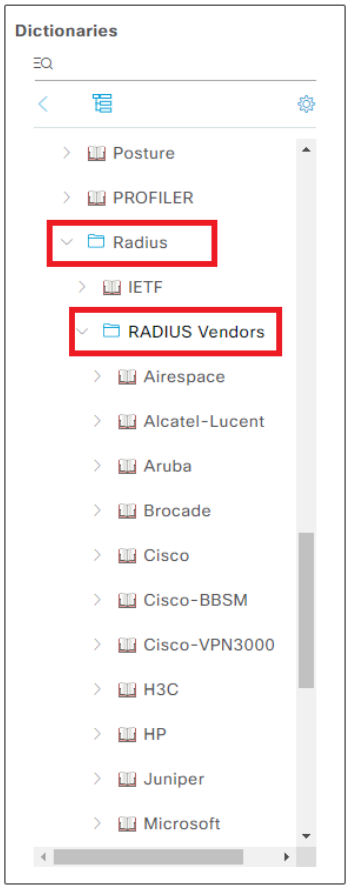
Remote IP Address: 10.10.10.20 and 10.10.10.30 (this is your Cisco ISE Sever & Windows Server AD IP Address)

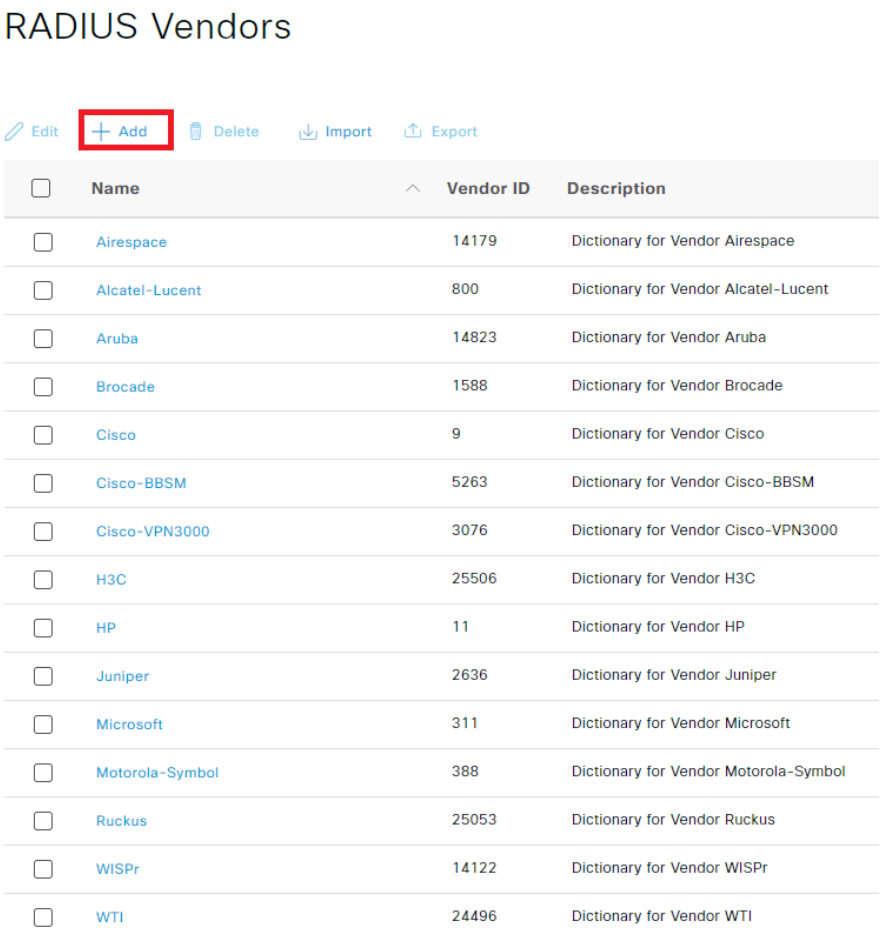

Okta RADIUS Agent UDP 18120 Properties
General
Programs and Services
Remote Computers
Protocols and Ports
Scope
Advanced
Local Principals
Remote Users
Local IP address
Any IP address
These IP addresses:
Add...
Edit...
Remove
Remote IP address
Any IP address
These IP addresses:
10.10.10.20
10.10.10.30
Add...
Edit...
Remove
OK
Cancel
Apply

4. [Cisco ISE Configuration]

4.1 Create vendor-specific attribute - Navigate to **Policy > Policy Element > Dictionaries > System > Radius > Radius Vendors > Add**

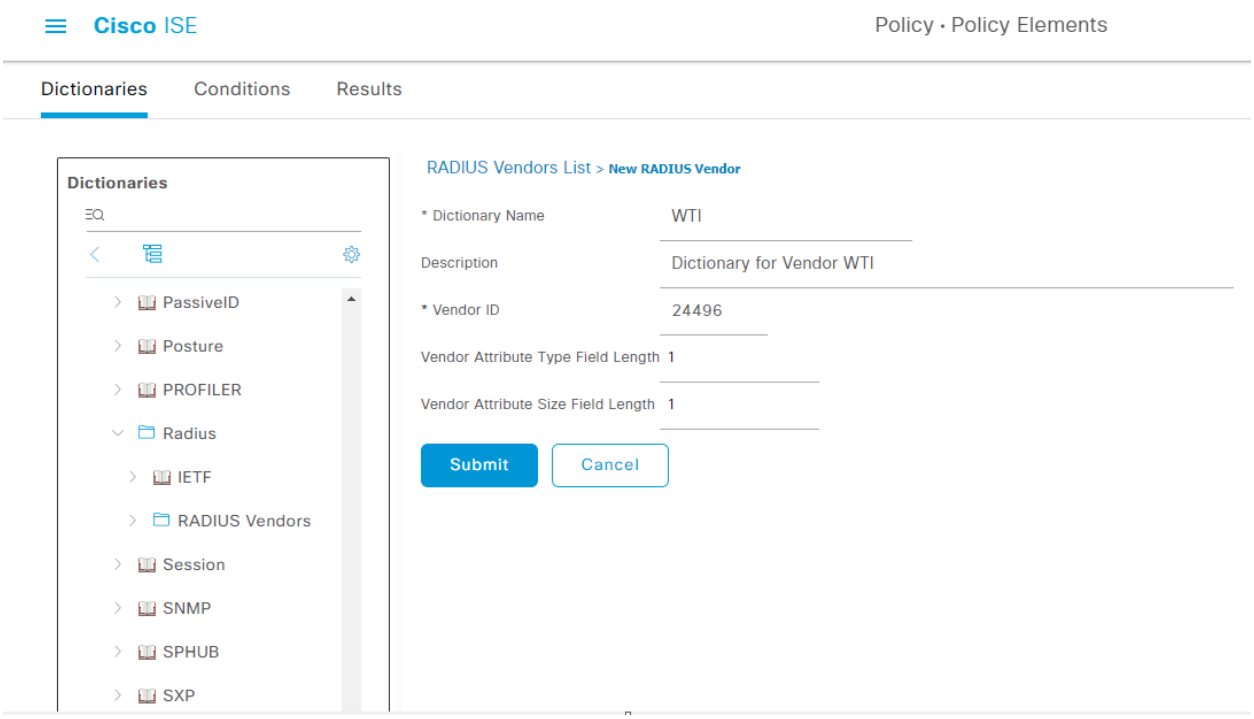


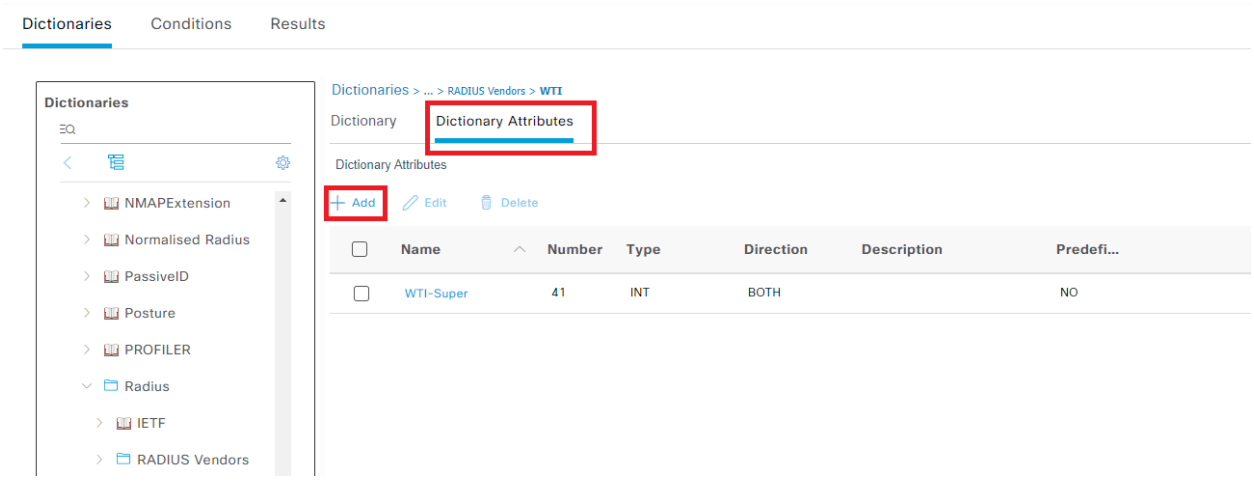




4.2 The name and the Vendor IDs are to be entered and saved

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





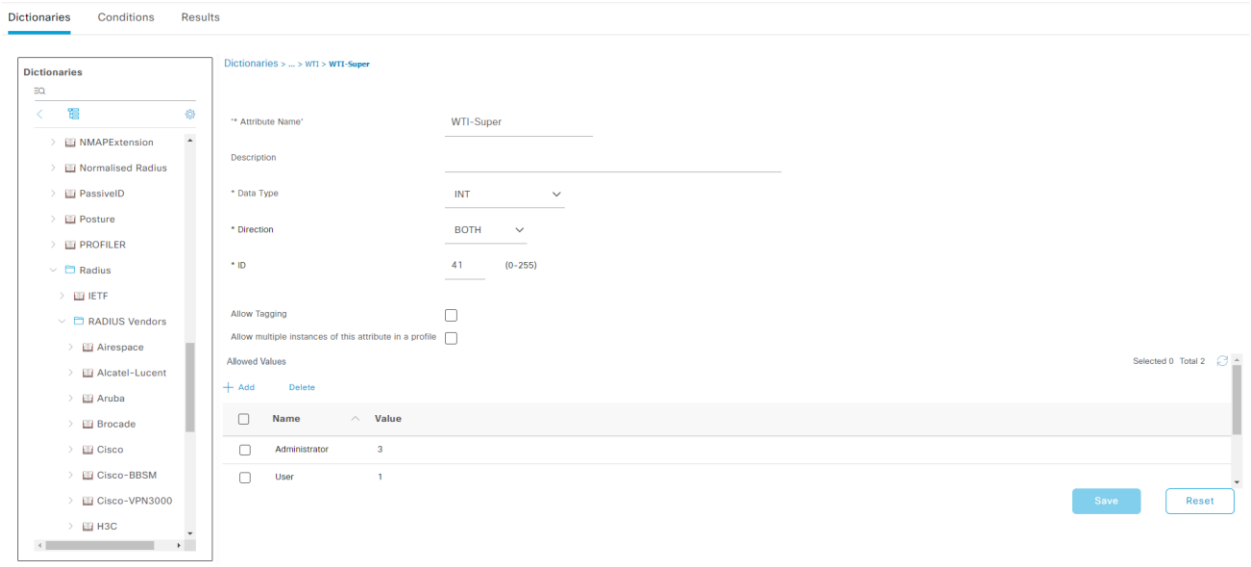
4.3 Click Add and fill out the Attribute Name, Data Type, Direction and ID and Add allow values for access level.

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**

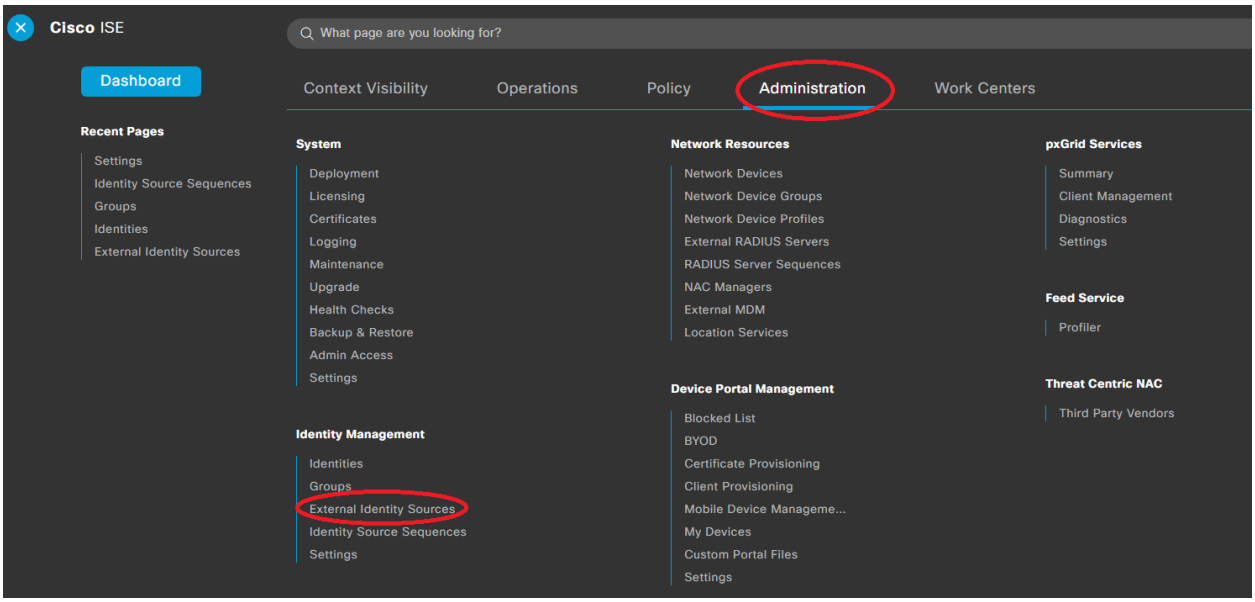


4.4 Add other Attributes on the same page if there are multiple Attributes to be added to the same Dictionary.

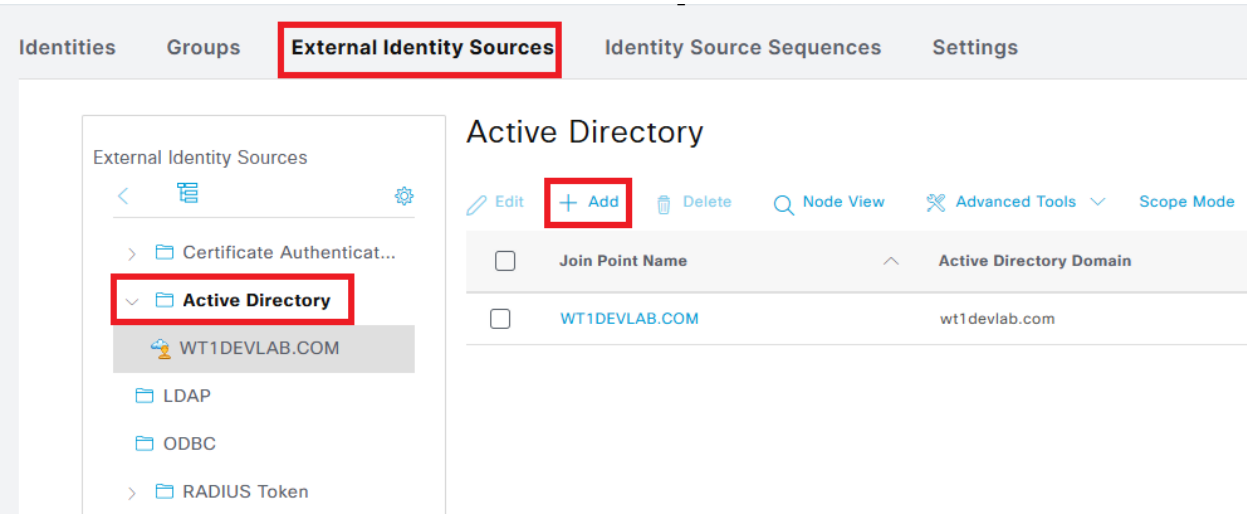
WTI RADIUS Dictionary https://ftp.wti.com/InfoCenter/rsa/dictionary/dictionary.wti

5. **Connect Active Directory joint point in ISE**

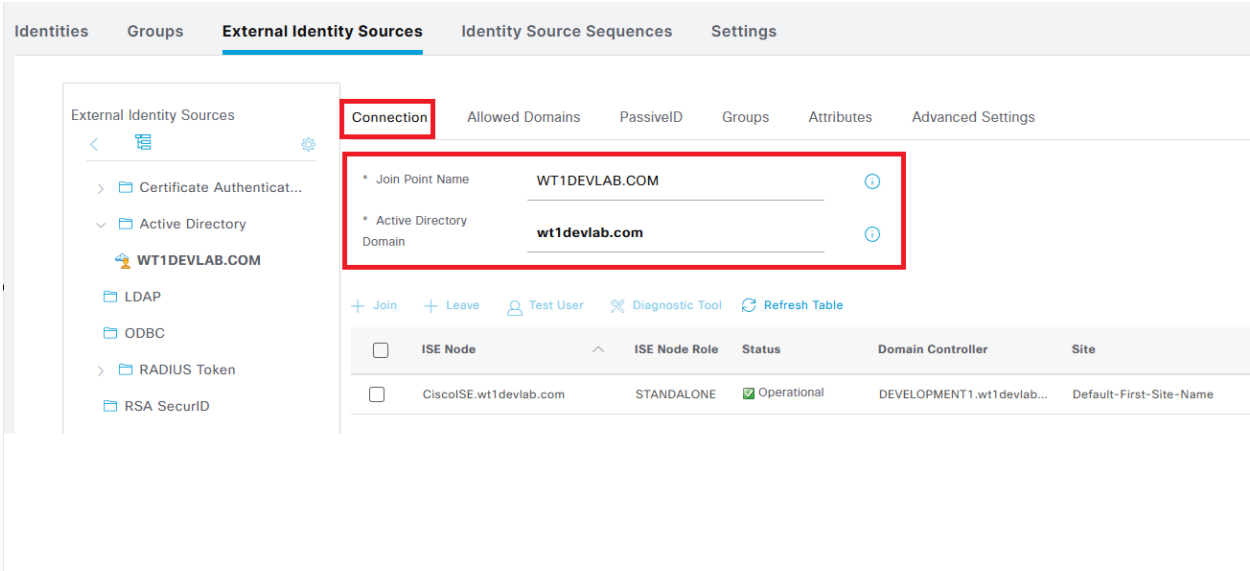
5.1 Navigate to **Administration** then click **Identity Management** and click **External Identity Sources**.



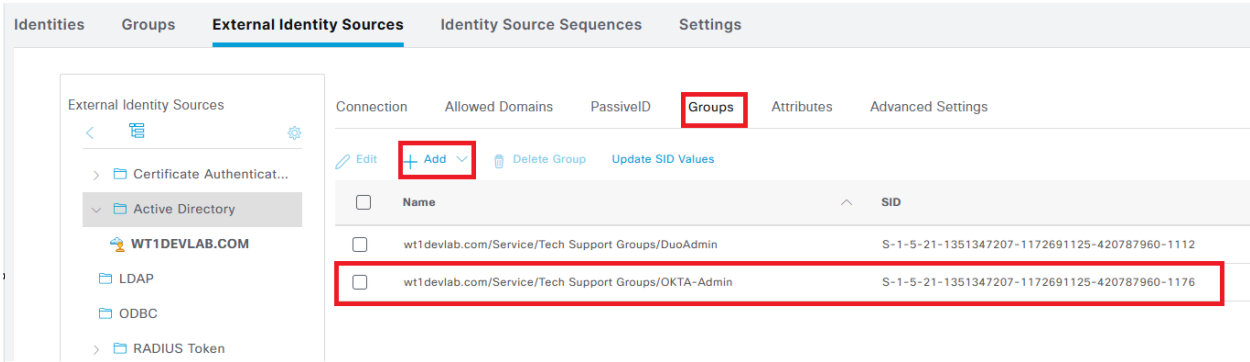
5.2 On **External Identity** Sources tab, Navigate to Active Directory and click **Add**



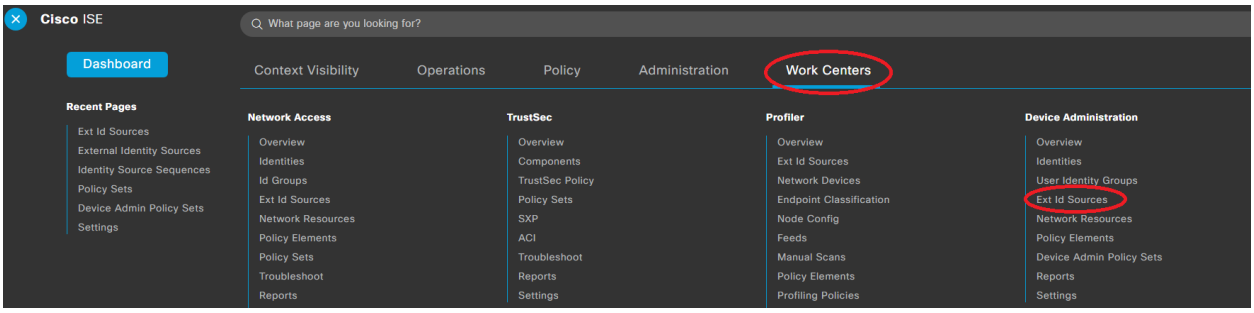
5.3 Under Connection section. Fill in the all requirement and click submit.



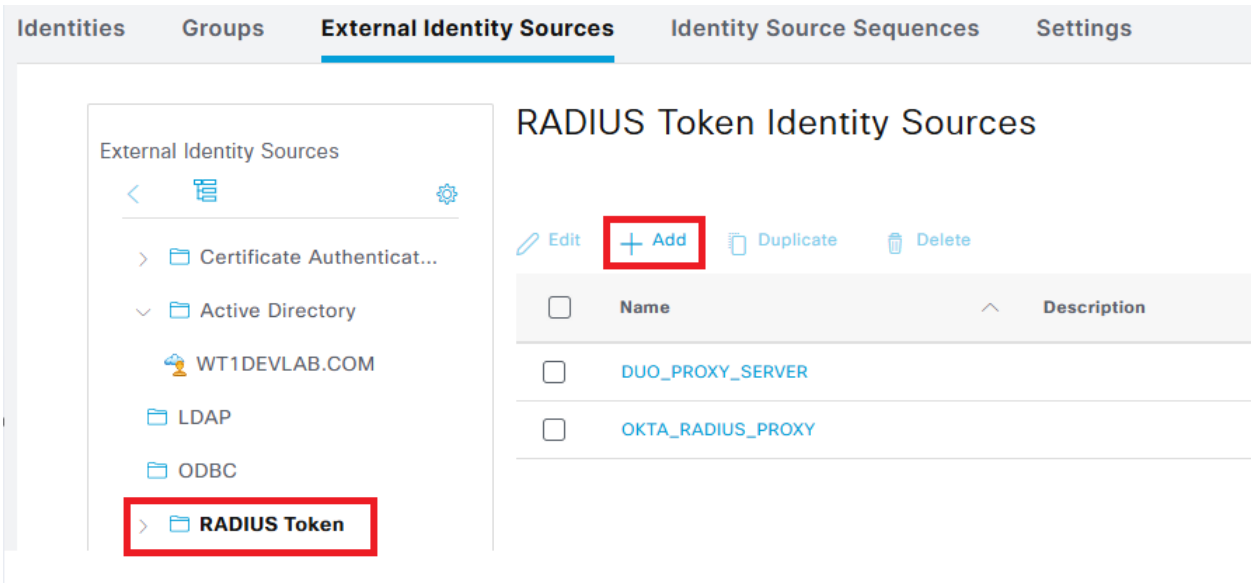
5.4 Navigate to **Groups** tab and click **Add** > **Select Group from Directory**.



5.5 Configuration for RADIUS communication between ISE and DUO - Navigate to **Work Center > Device Administration > Ext Id Sources**



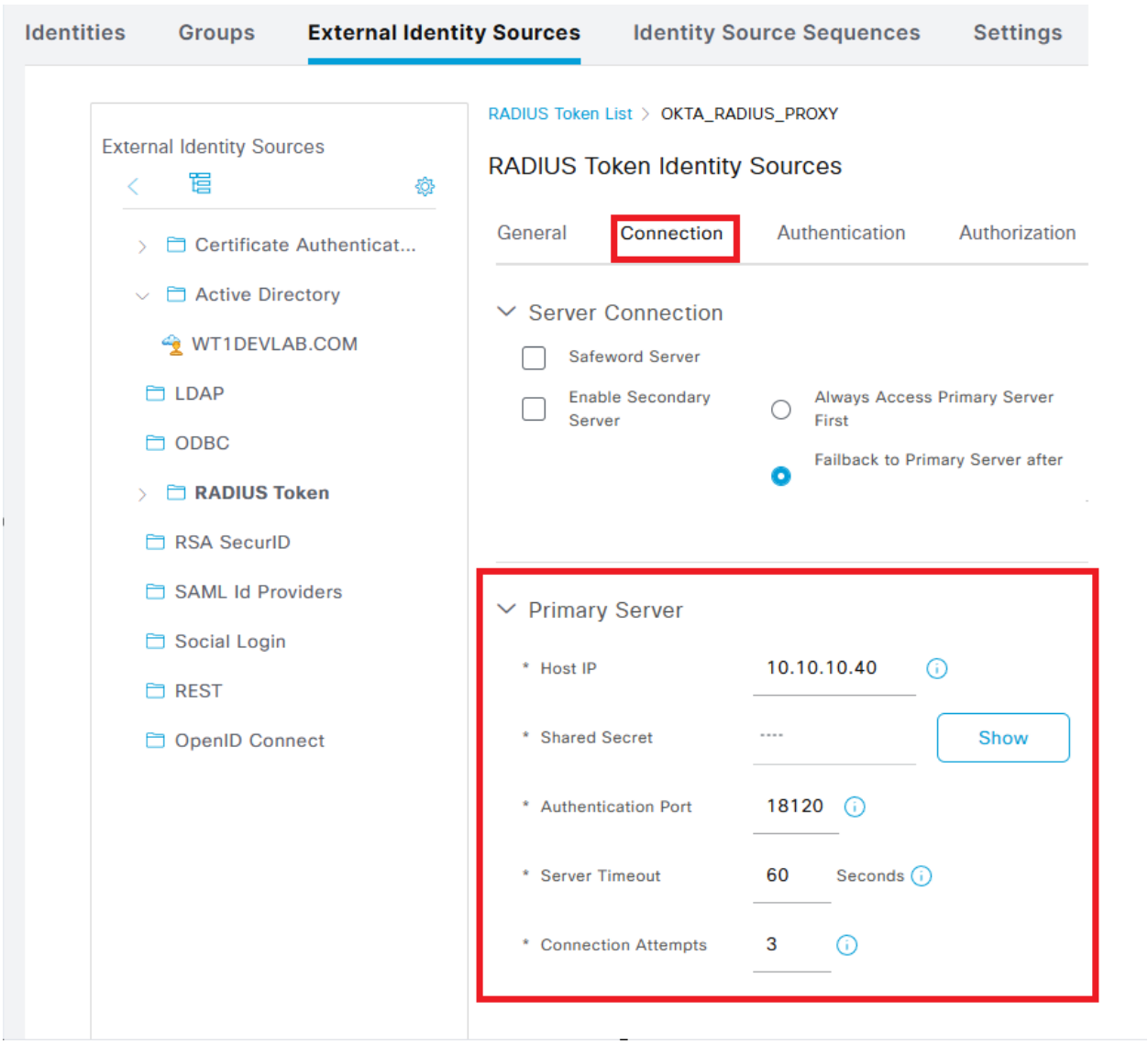
5.6 On RADIUS Token click **Add.**



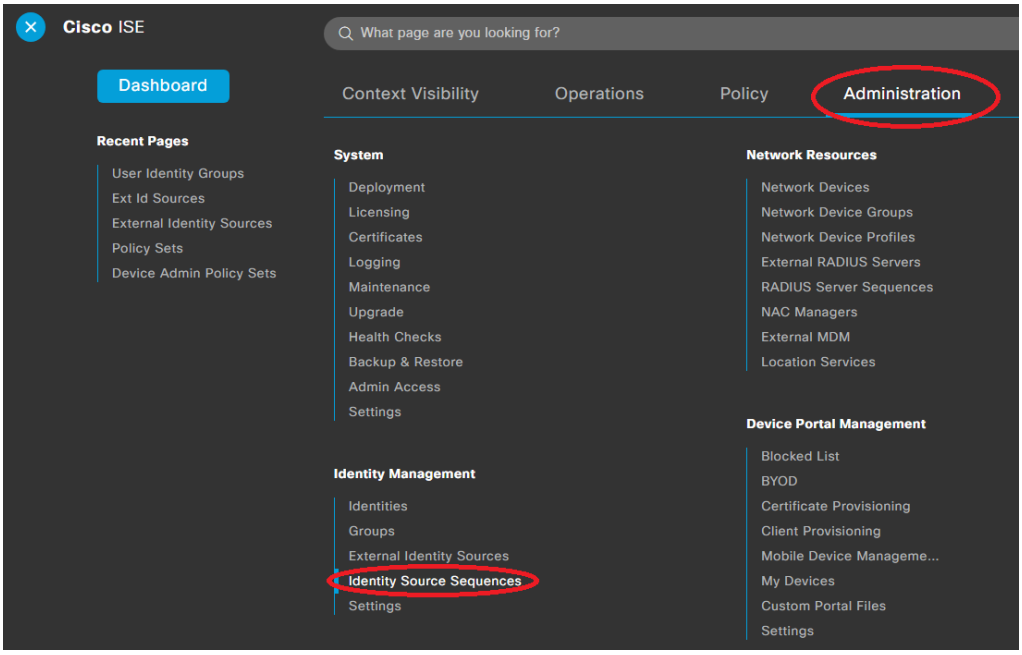
5.7 Starting from the left to right, configure the settings within each tab menu item as follow.

a. In General tab, configure the name for the configuration.

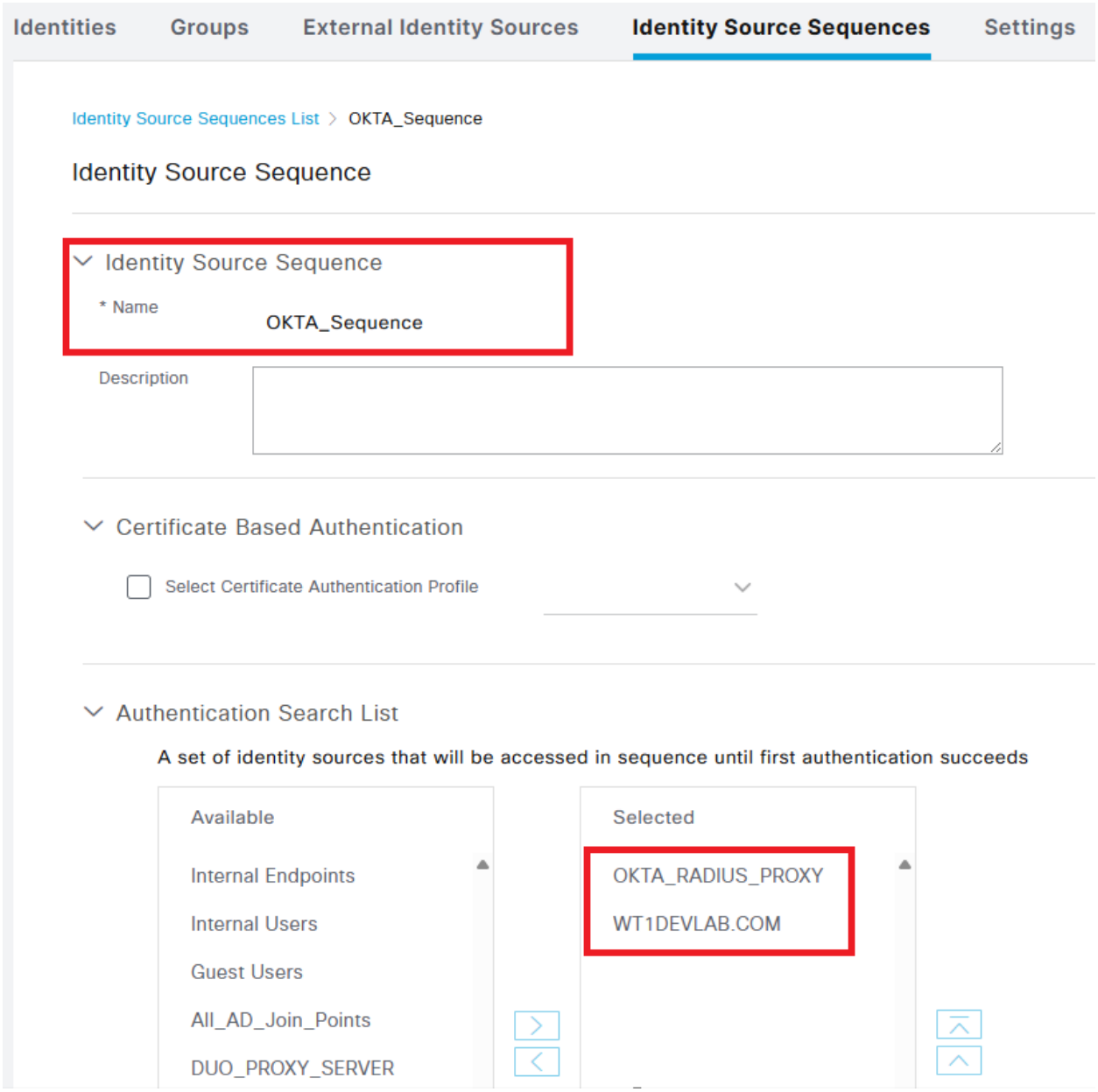
b. In Connection tab, configure the primary server details. (Primary Server is OKTA RADIUS Agent Authentication Server, UDP port and share secret password)



6. Create Identity Source sequences. Navigate to **Administration > Identity management > Identity Sources Sequence**

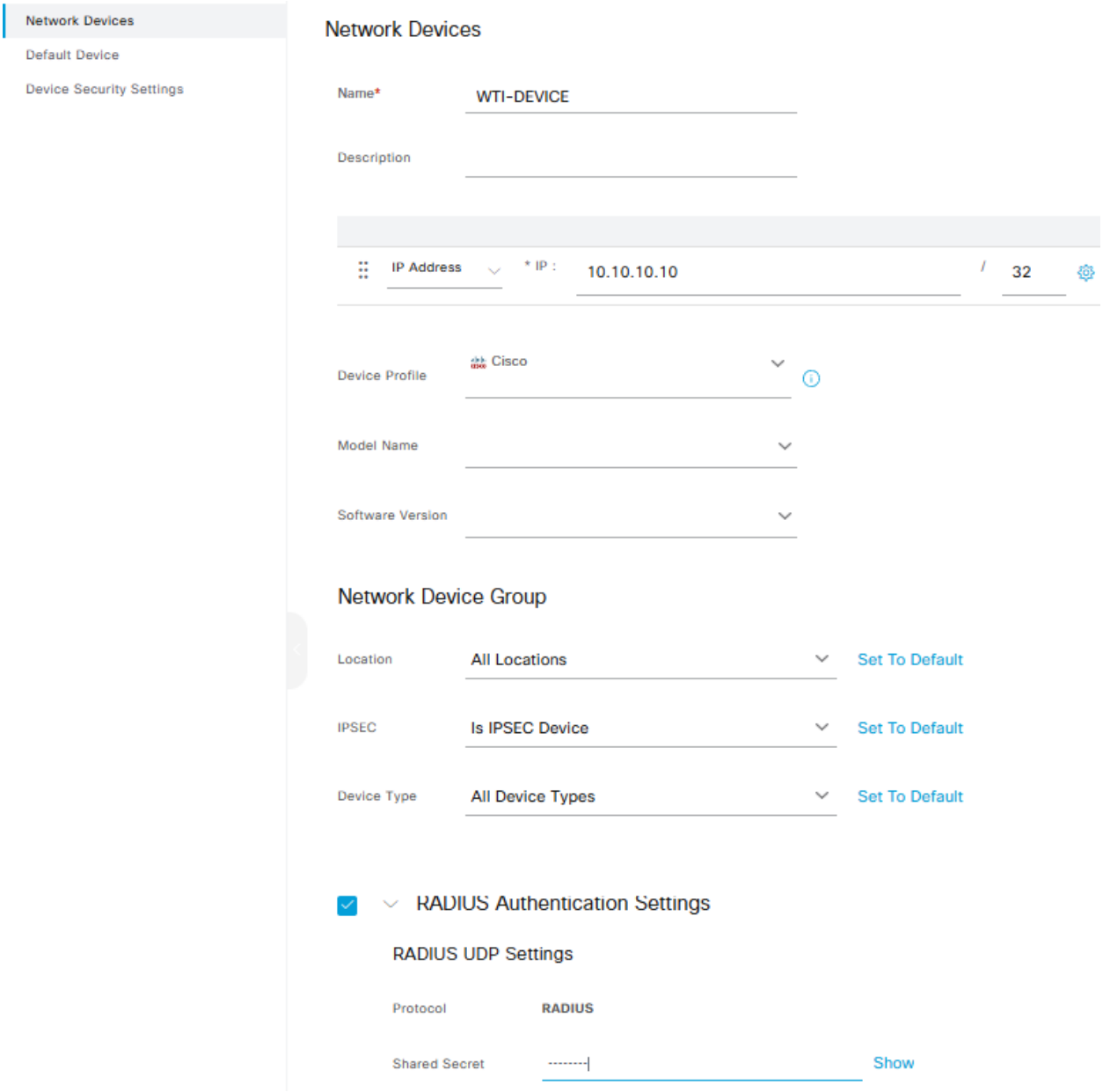


6.1 In Identity Sources Sequence - click **Add** name identity source sequence and select authentication available search list and click Save.



7. Add Network Device - Navigate to **Administration** > **Network Resources** > **Network Devices** and create an entry for each WTI device (or an appropriate IP range).

Setting	Lab example
Name	WTI-DEVICE
IP Address	10.10.10.10 /32
RADIUS Authentication Settings	Enabled
Shared Secret	Must exactly match the WTI Primary Secret Word

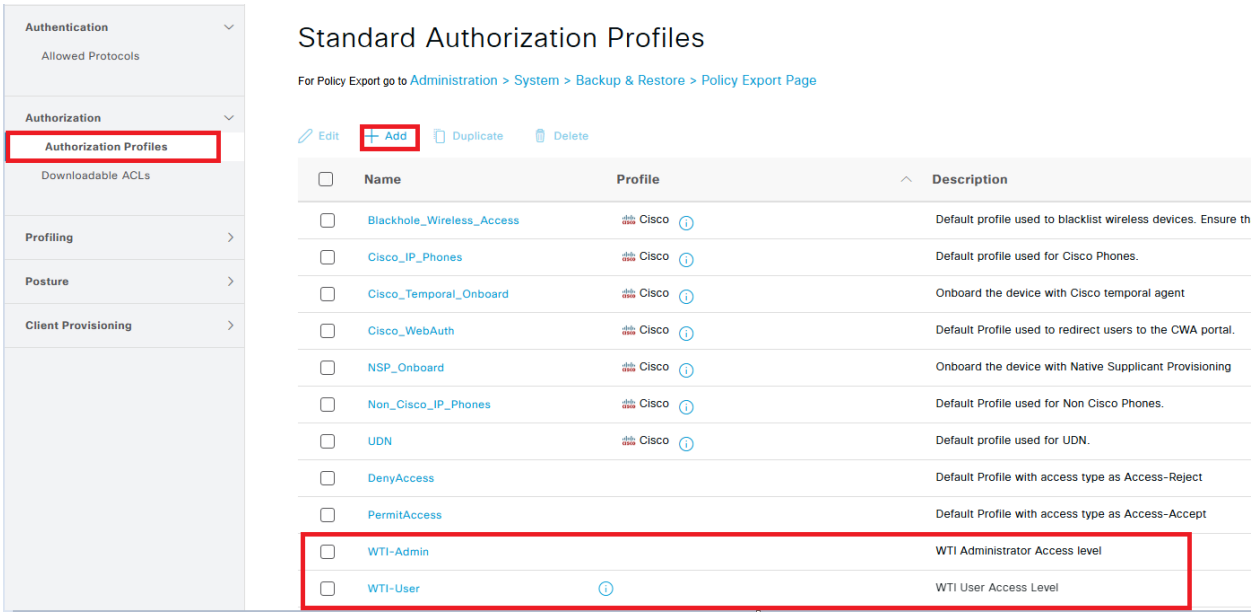


8. Create WTI Radius Authorization Profile in Cisco ISE

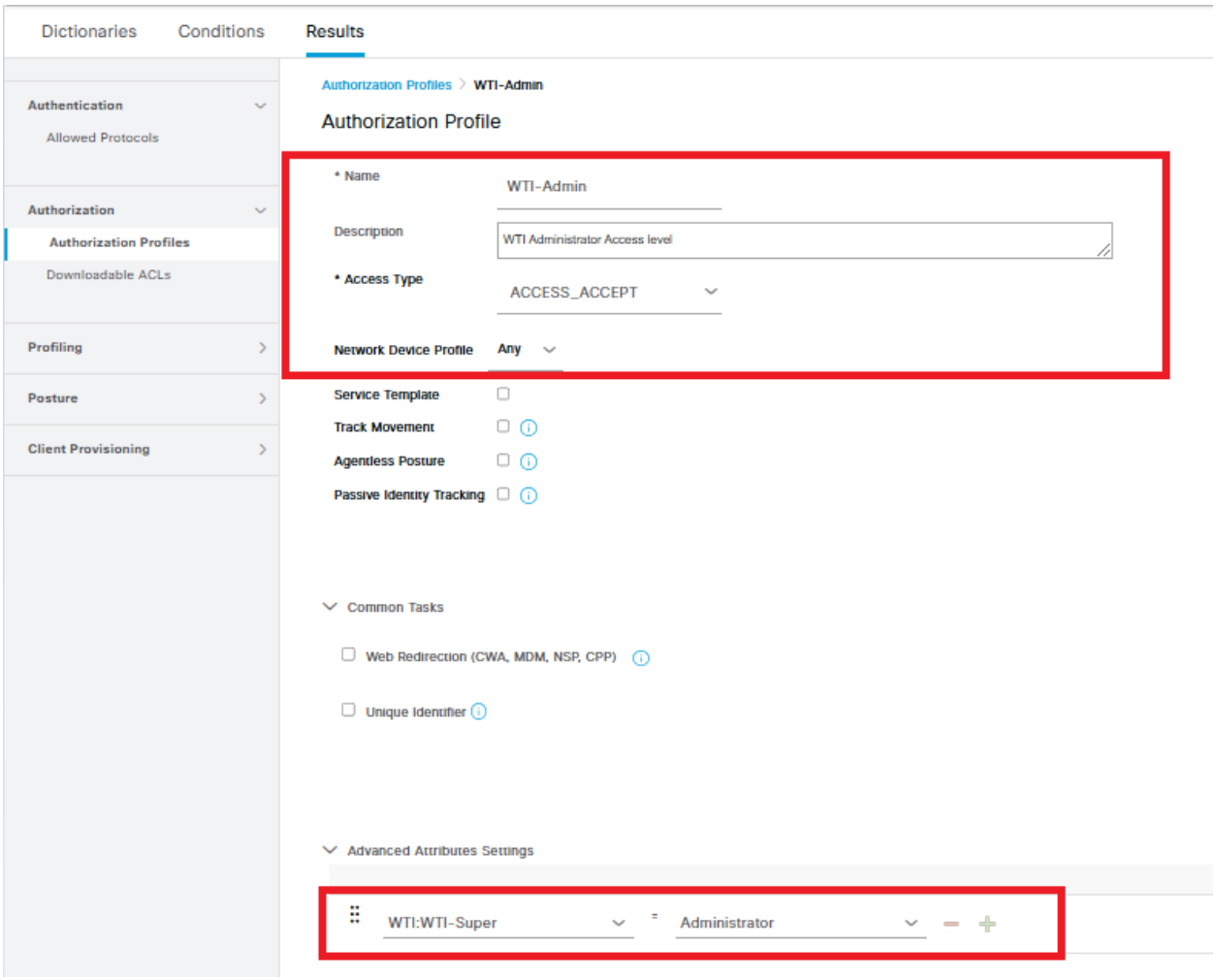
Create separate Cisco ISE Authorization Profiles for each WTI privilege level required by the customer. Cisco ISE must return the WTI vendor-specific attribute with the correct data type.

Profile	WTI attribute	Validated use
WTI-Admin	WTI:WTI-Super = Administrator (3)	Administrator access
WTI-User	WTI:WTI-Super = User (1)	Normal/restricted user access

8.1 Navigate to **Policy > Policy Elements > Results > Authorization Profiles > Add**

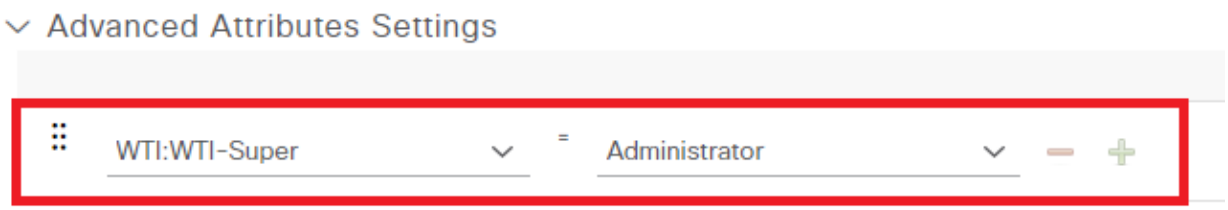


8.2 Create two Authorization Profile. One for WTI_Admin (Administrator access level) and another for WTI_User (User access level).



For WTI_Admin

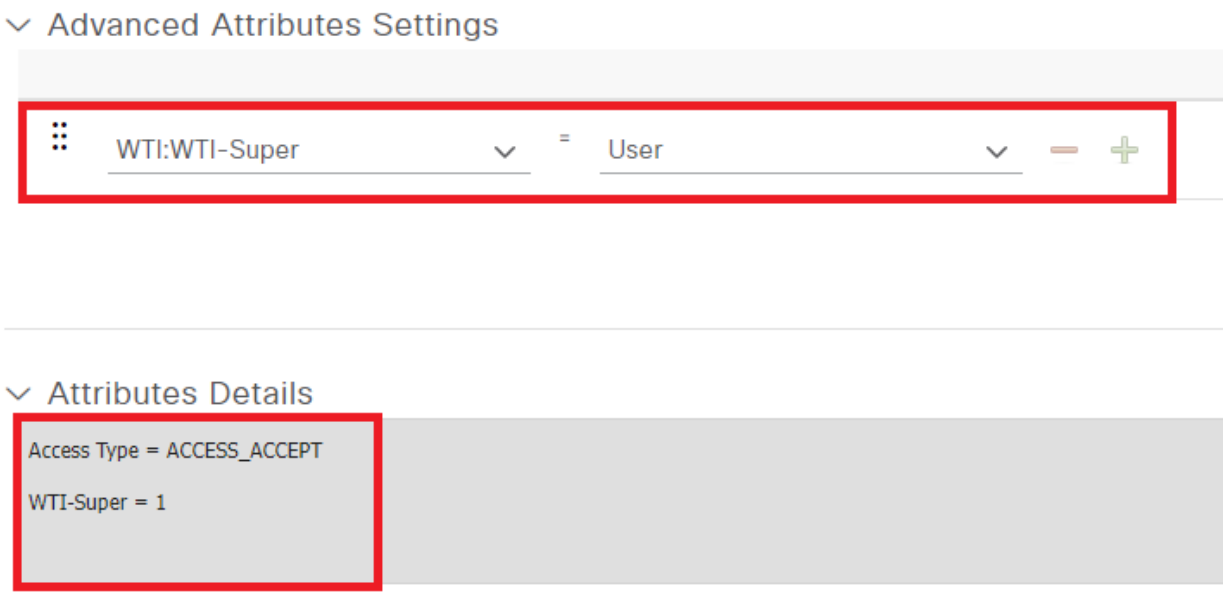
In advanced Attribute Settings





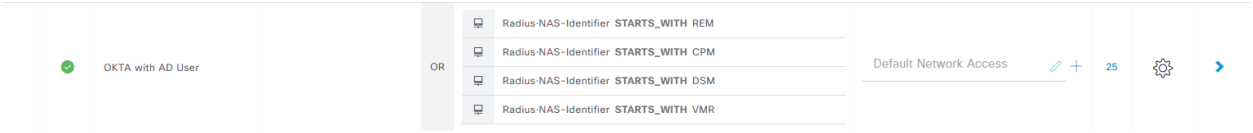
For WTI_User

In Advance Attribute Settings



9. Create Policy with NAS-Identifier

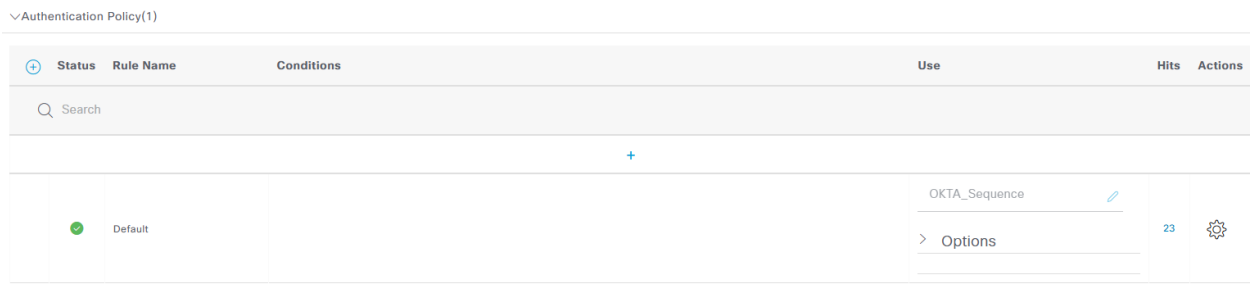
9.1 Navigate to **Policy > Policy Sets > click (+) to add new policy set**.



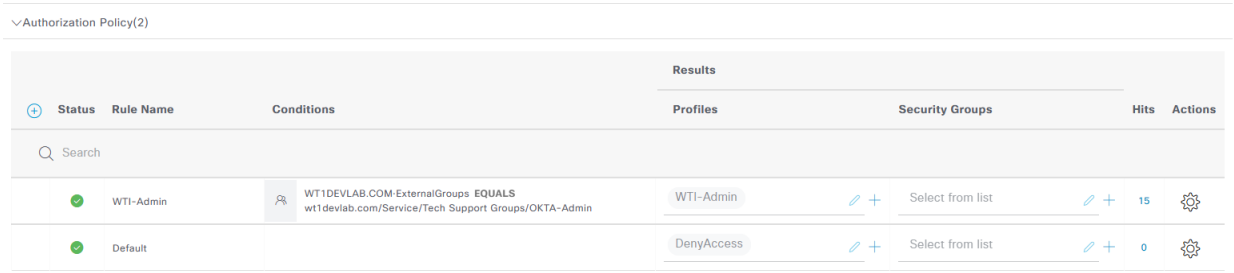
Policy Set Name: **OKTA with AD User**
Condition: **Radius-NAS-Identifier START_WITH REM** (CPM or DSM)
Allowed Protocols: **Default Network Access**

8.2 Authentication Policy

Rule Name: Default
Use: **OKTA_Sequence**



9. 3 Authorization Policy – create two authorization policy, one for WTI_Admin and another for WTI_User.



For WTI_Admin

Rule Name: **WTI-Admin**
Condition: **WT1DEVLAB.COM-ExternalGroup EQUALS wt1devlab.com/Service/Tech Support Groups/OKTA-Admin**
Profile: **WTI_Admin**

10 **WTI Radius Configuration**

10.1 Go to /N option 29 for Radius > RADIUS Settings

```
RADIUS: [Shared]

1.  Enable:                    On
2.  Primary Host/Address:      10.10.10.20
3.  Primary Secret Word:       (defined)
4.  Secondary Host/Address:    (undefined)
5.  Secondary Secret Word:     (undefined)
6.  Fallback Timer:            3 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:       Enable
16. Require Message Authentic: On
17. Debug:                     Off
18. Ping Test


Enter: #<CR> to change,
       <ESC> to return to previous menu ...
```