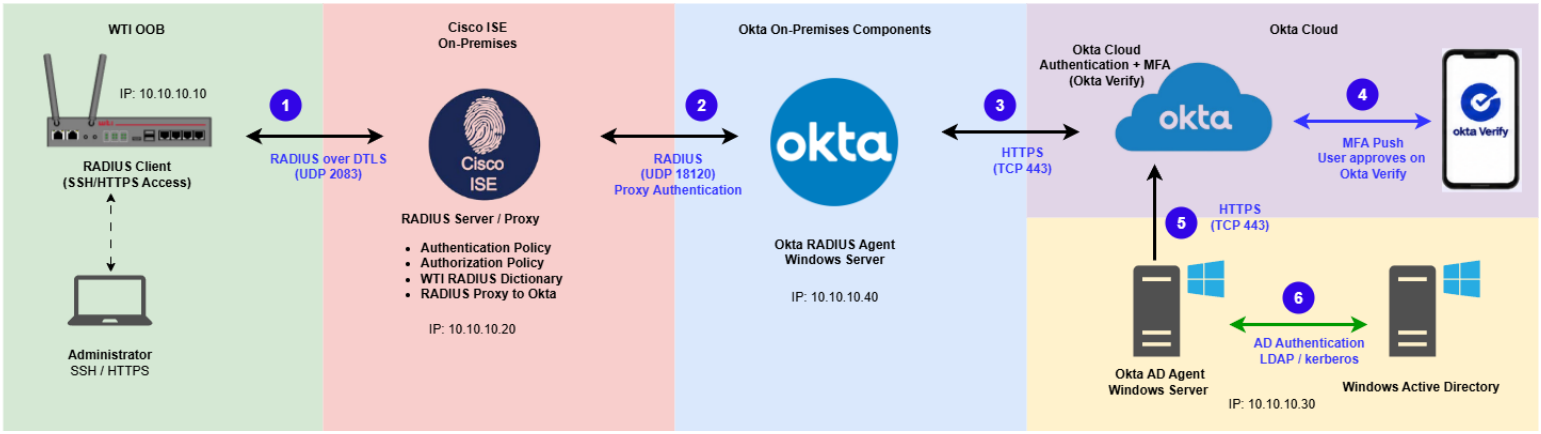
Cisco ISE + OKTA MFA + Windows AD Integration for WTI (RADIUS over DTLS)



How it works:

1. WTI → Cisco ISE

- RADIUS authentication from WTI OOB device to Cisco ISE
- RADIUS over DTLS (UDP 2083)
- 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.

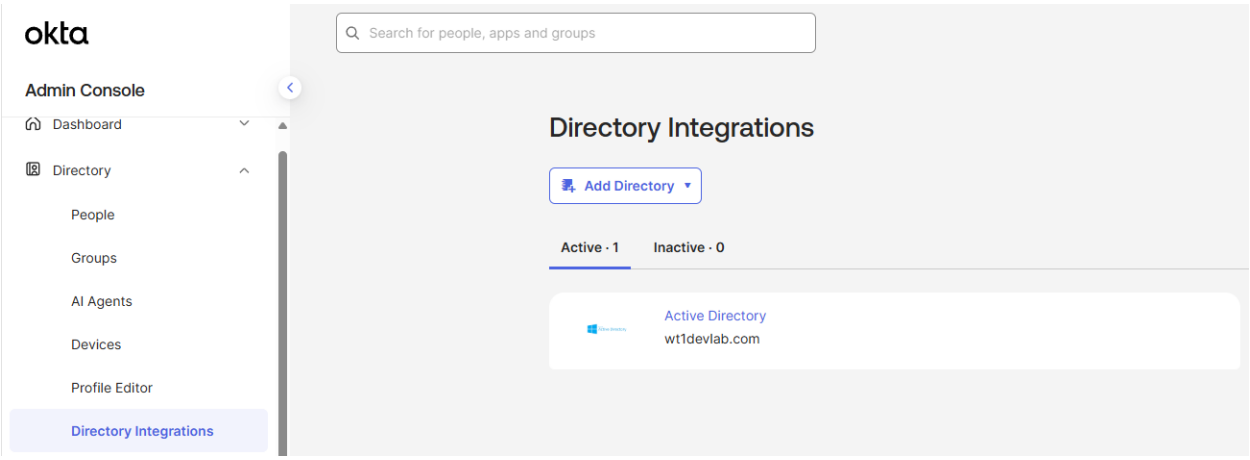
1.2 Network and firewall requirement

Source	Destination	Protocol / Port	Purpose
WTI device	Cisco ISE	UDP 2083	RADIUS DTLS authentication
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

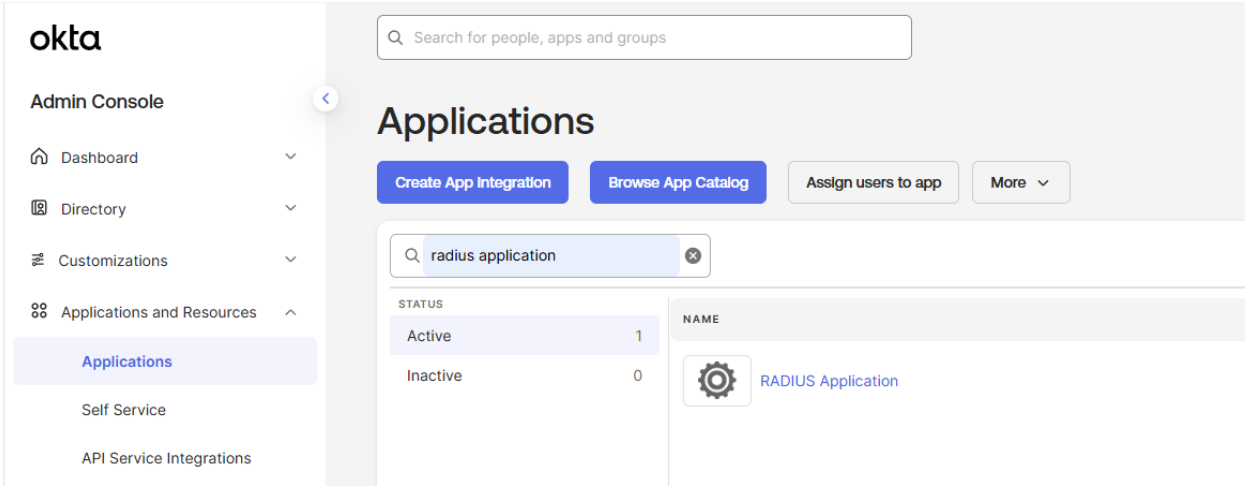
2.1 Directory Integrations

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

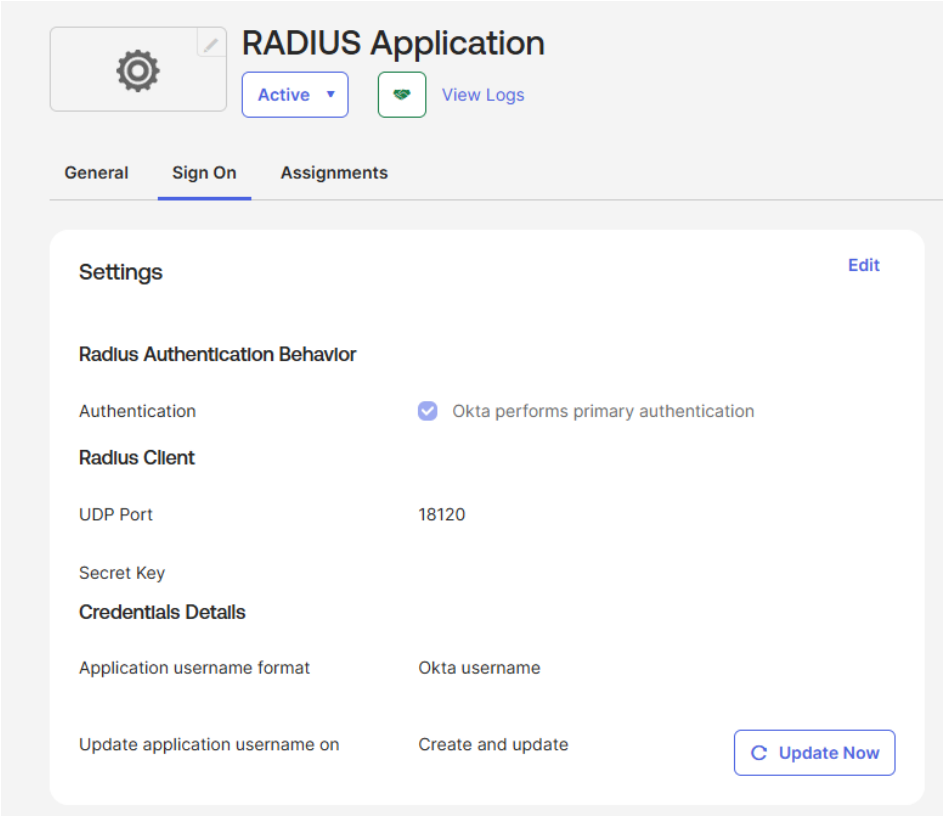


2.2 Configure the RADIUS application

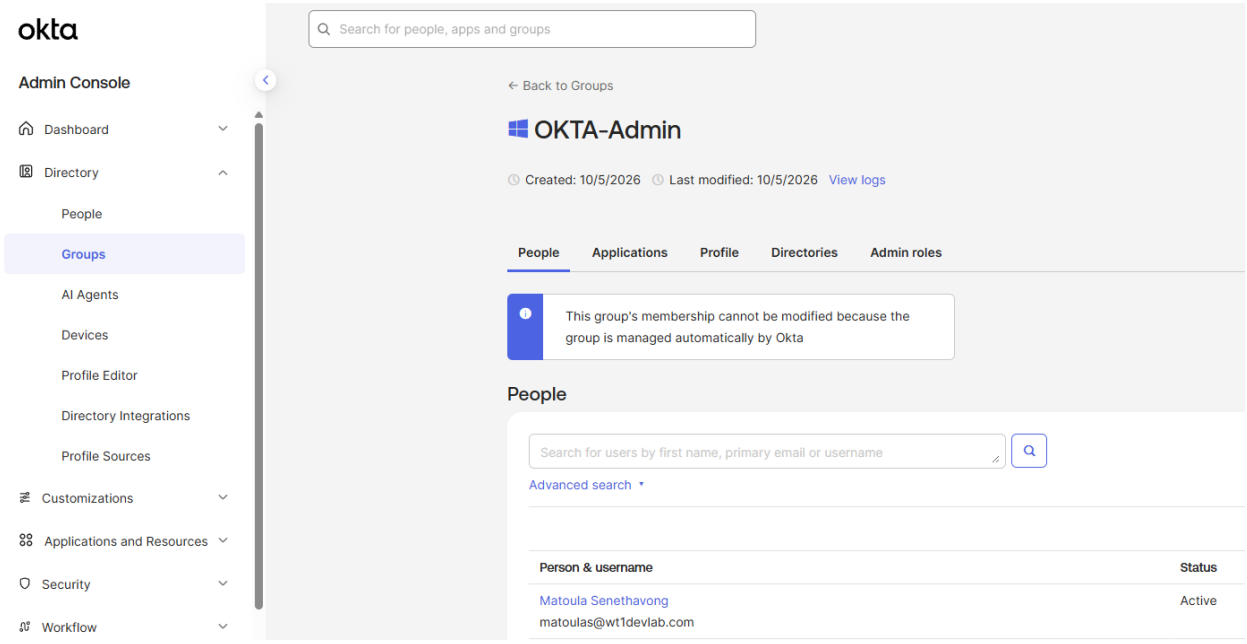
Go to **Applications and Resources** > **Application** > in the search box type **radius application**



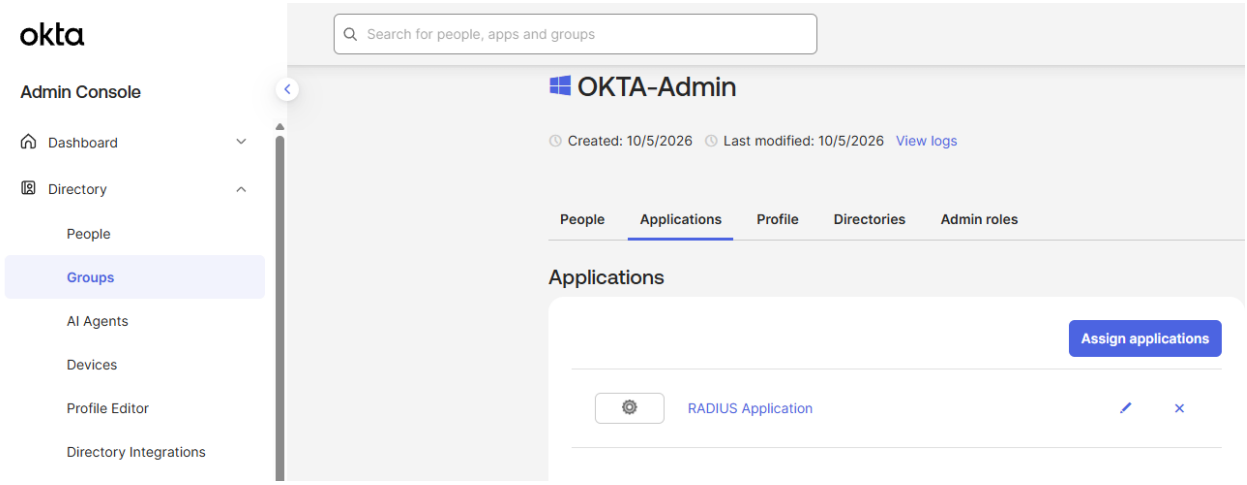
2. Configure the Okta RADIUS application to use the Okta RADIUS Agent.
3. Use the RADIUS authentication port configured on the agent. UDP Port: 18120.
4. Configure the RADIUS client/shared secret so Cisco ISE is accepted as the client when ISE proxies' requests to Okta.
5. Enable the desired MFA behavior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



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

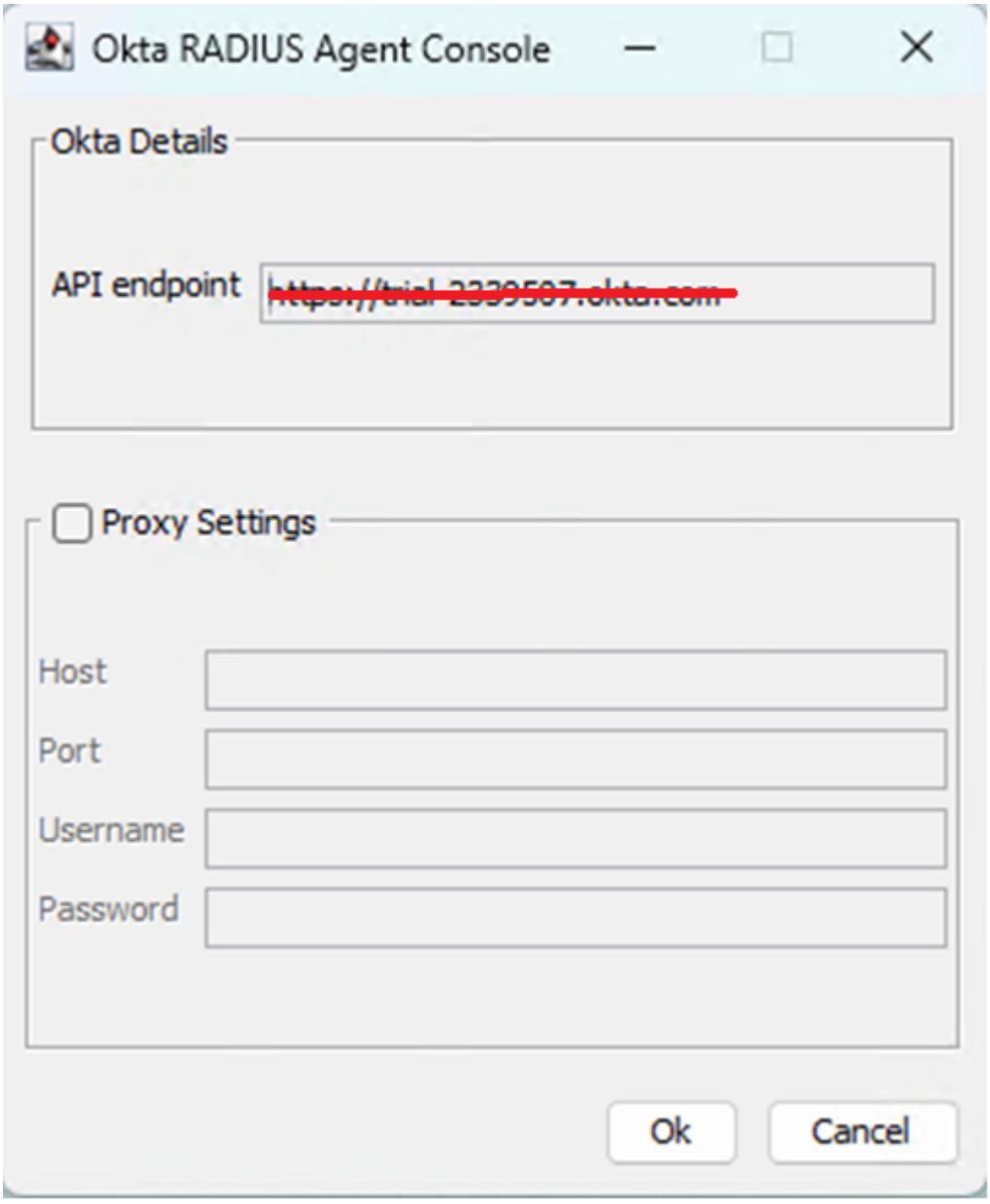


7. Assign the user to the Okta RADIUS application.



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:

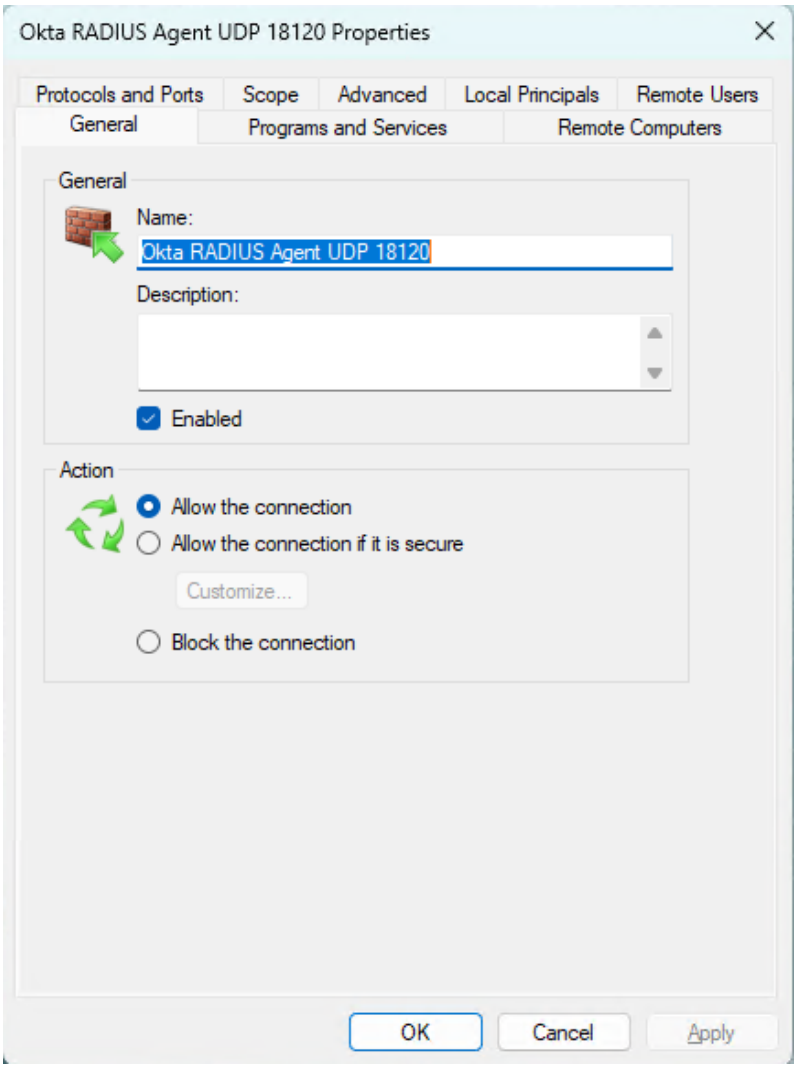
ragent.client_ip_allow_list.18120=10.10.10.20,10.10.10.30

(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

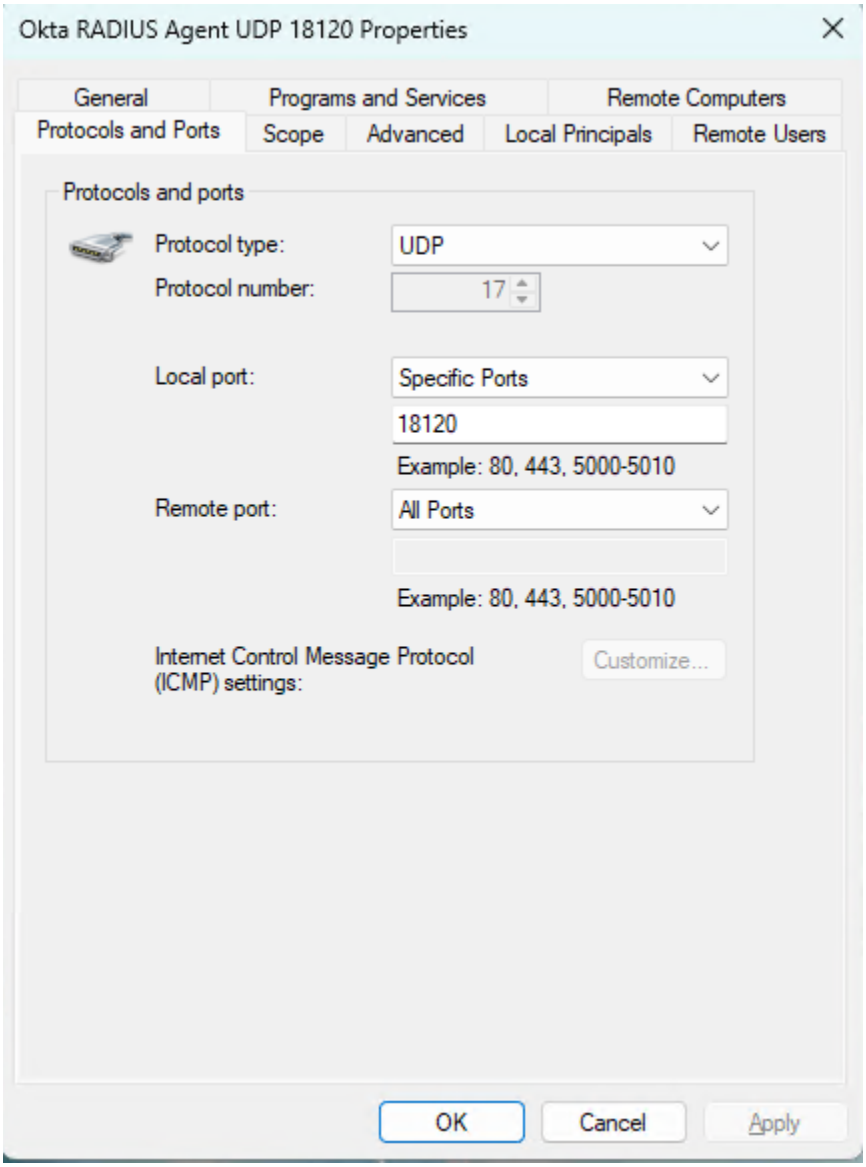
Allow Okta Radius Agent UDP 18120 for remote IP Address 10.10.10.20 and 10.10.10.30

- 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



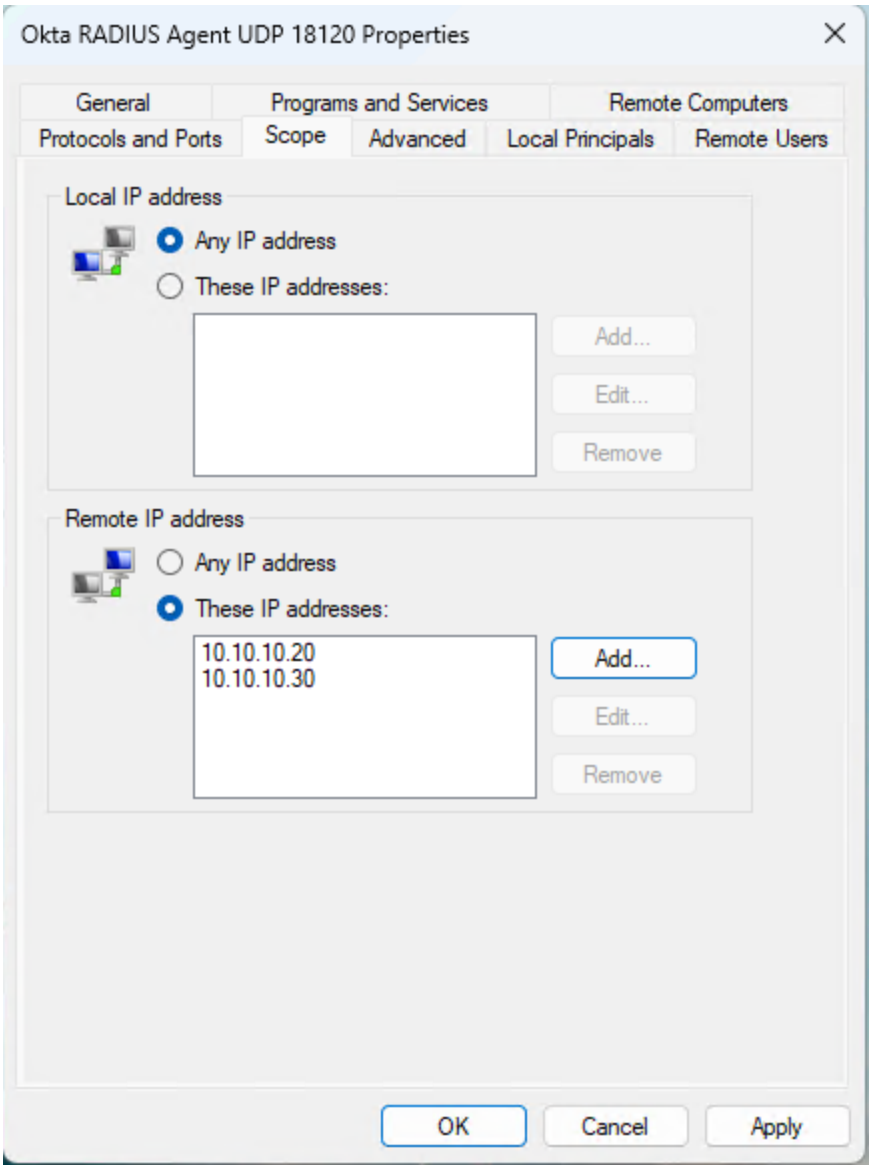
In **Protocols and Ports** section

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



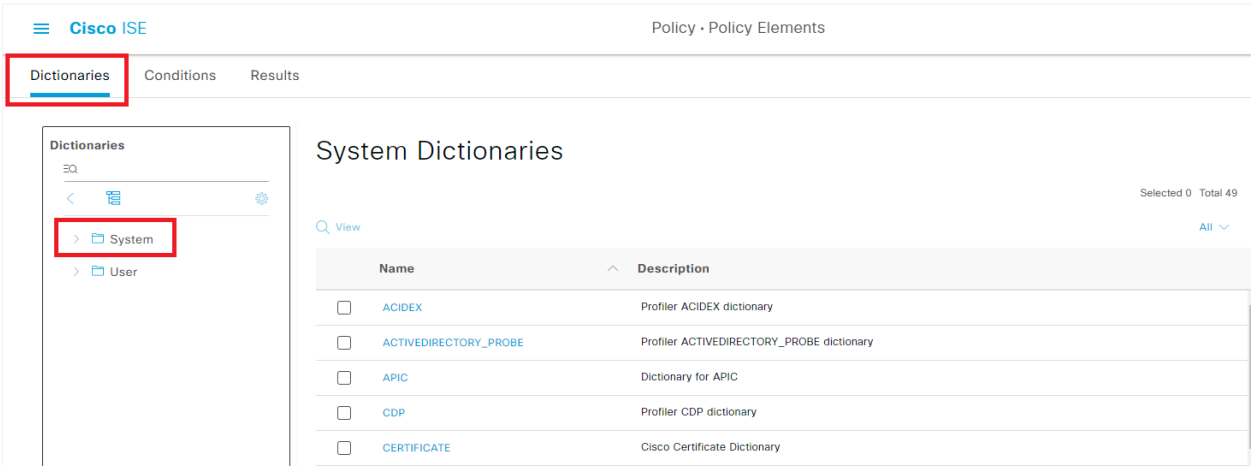
In **Scope** section

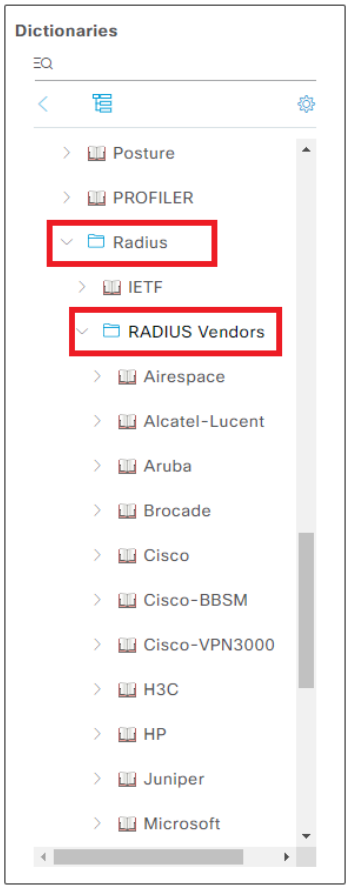
Remote IP Address: 10.10.10.20 and 10.10.10.30 (this is your Cisco ISE Sever & Windows Server AD IP Address)

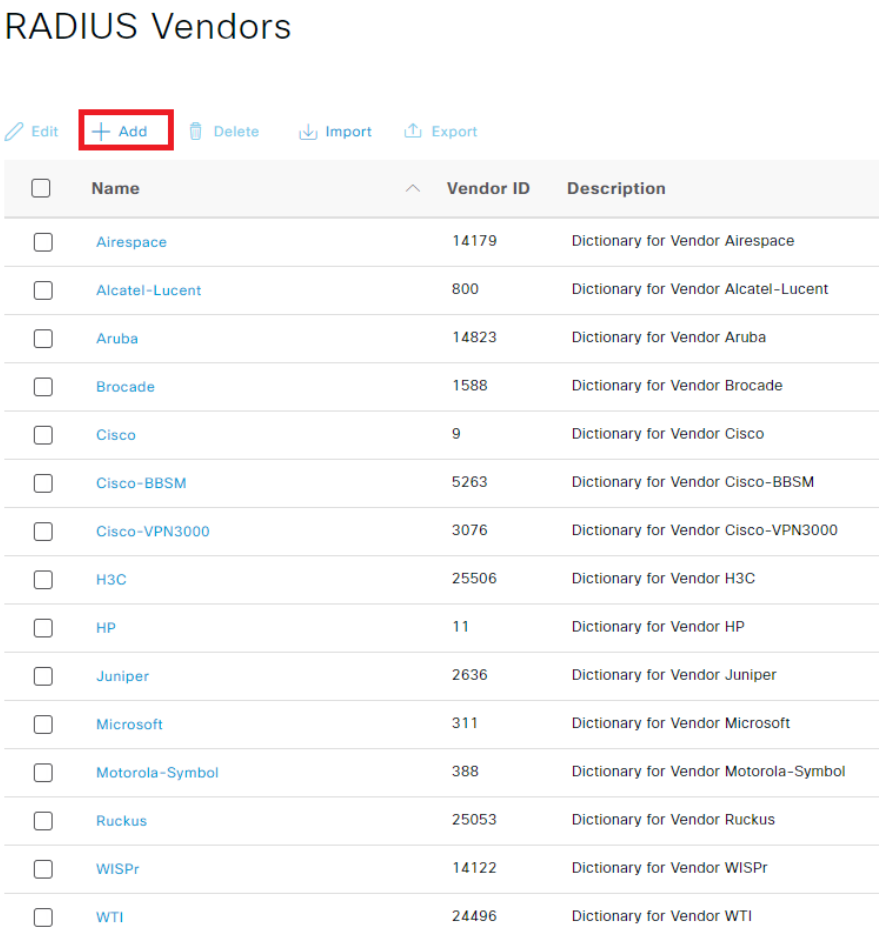

Okta RADIUS Agent UDP 18120 Properties
General
Programs and Services
Remote Computers
Protocols and Ports
Scope
Advanced
Local Principals
Remote Users
Local IP address
Any IP address
These IP addresses:
Add...
Edit...
Remove
Remote IP address
Any IP address
These IP addresses:
10.10.10.20
10.10.10.30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

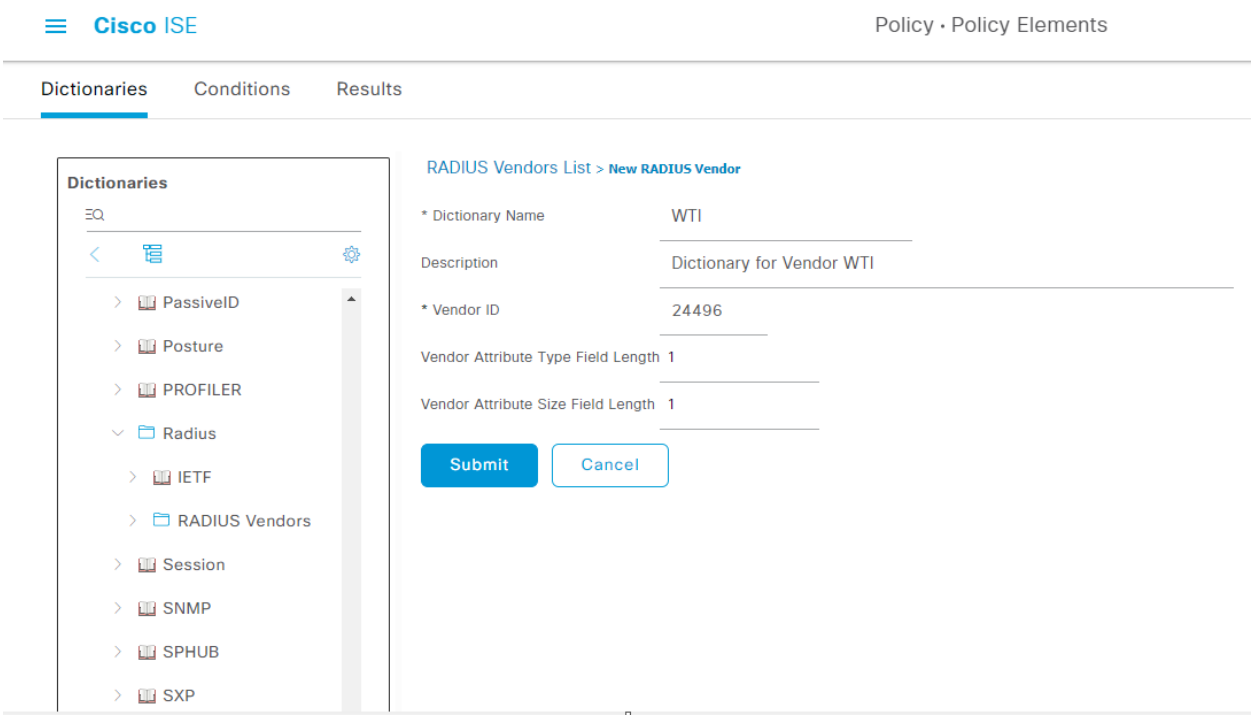


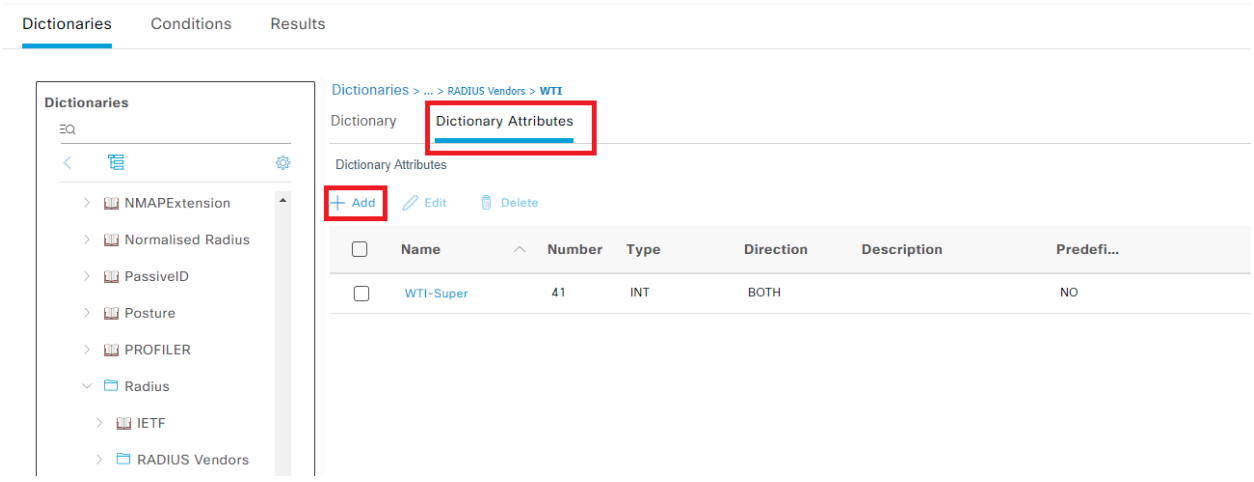




4.2 The name and the Vendor IDs are to be entered and saved

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





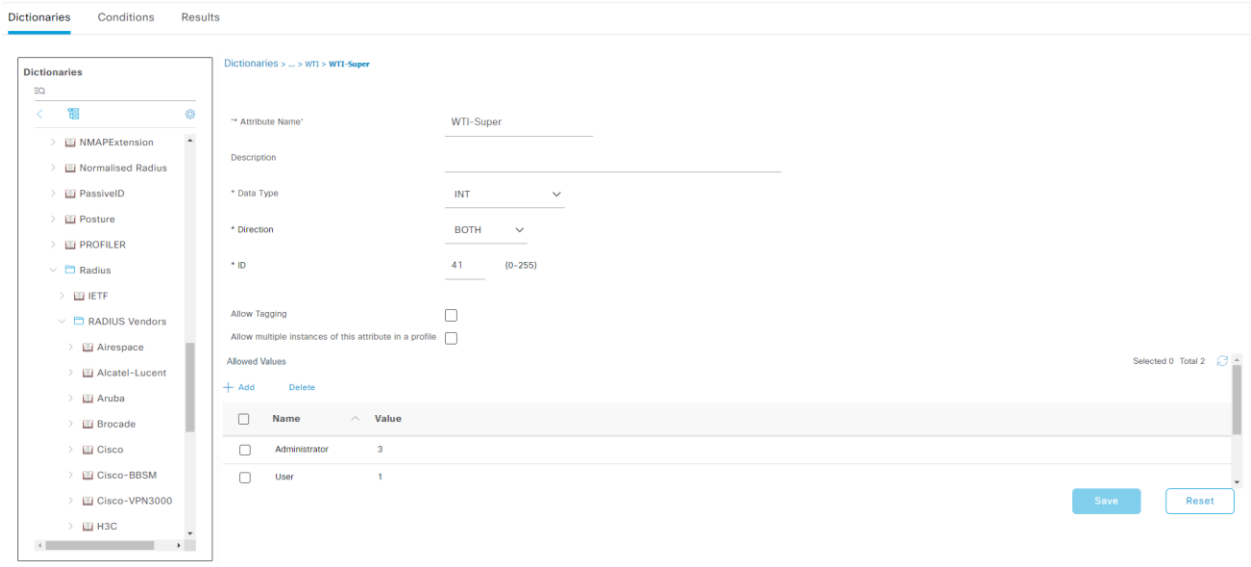
4.3 Click Add and fill out the Attribute Name, Data Type, Direction and ID and Add allow values for access level.

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**

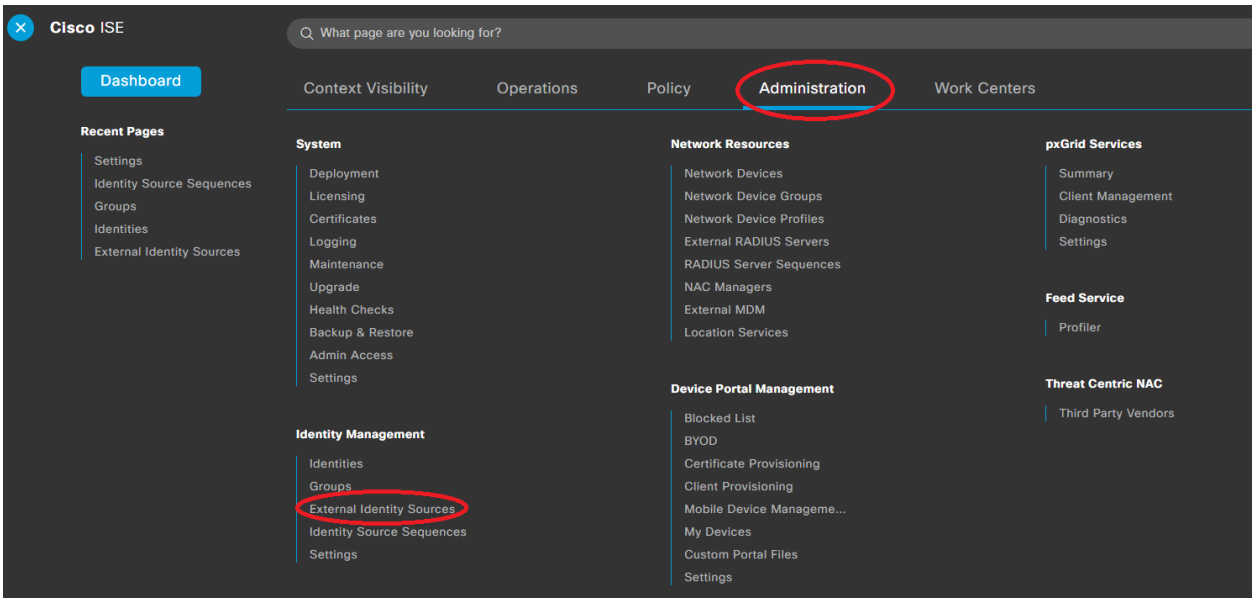


4.4 Add other Attributes on the same page if there are multiple Attributes to be added to the same Dictionary.

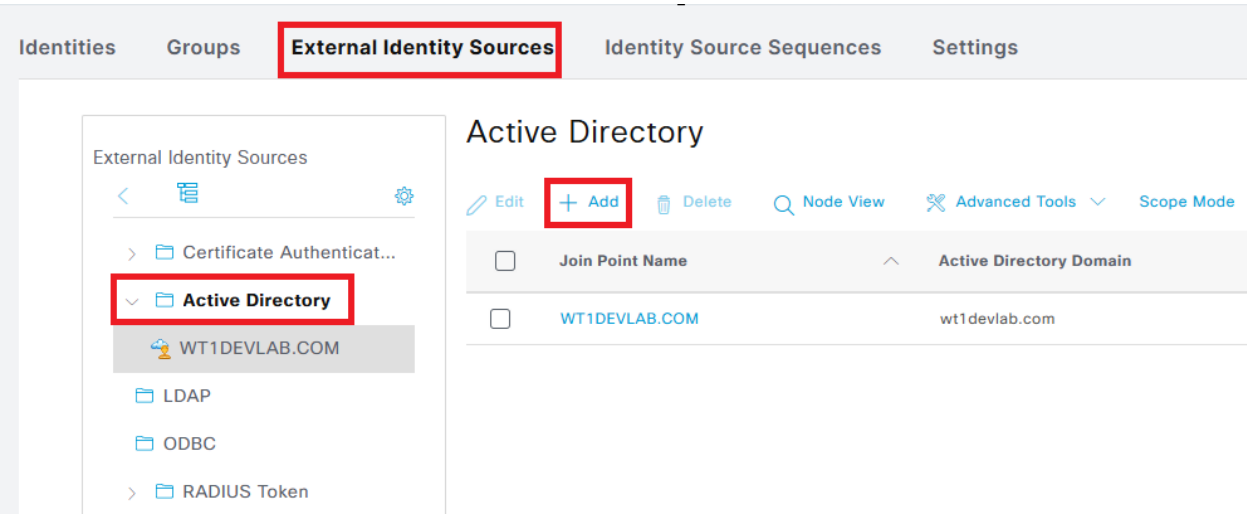
WTI RADIUS Dictionary https://ftp.wti.com/InfoCenter/rsa/dictionary/dictionary.wti

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

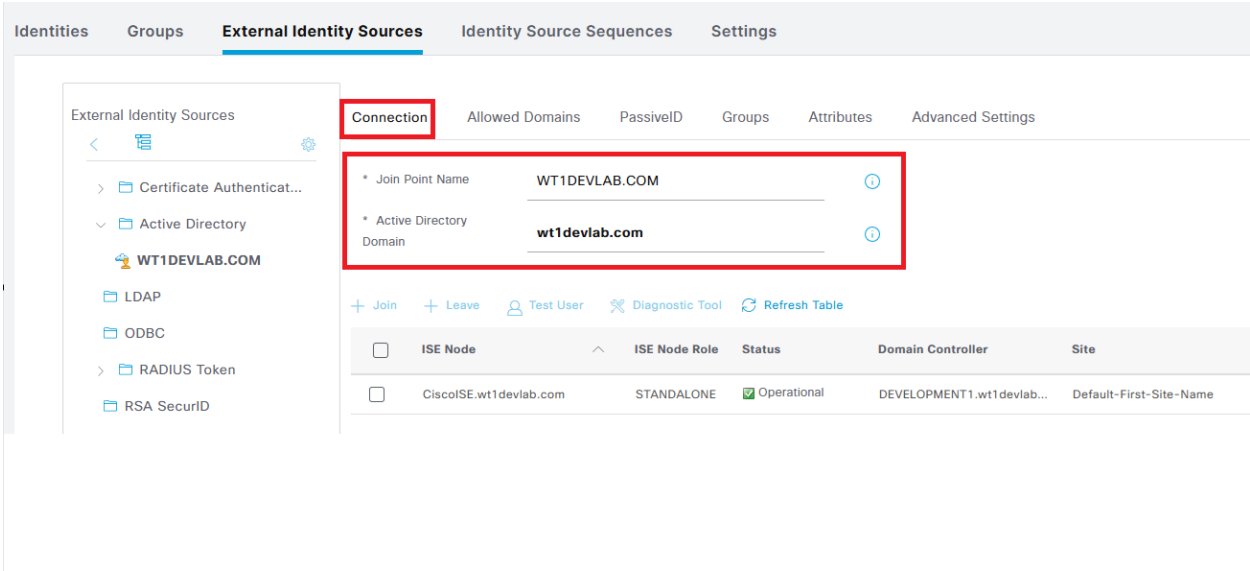
5.1 Navigate to **Administration** then click **Identity Management** and click **External Identity Sources**.



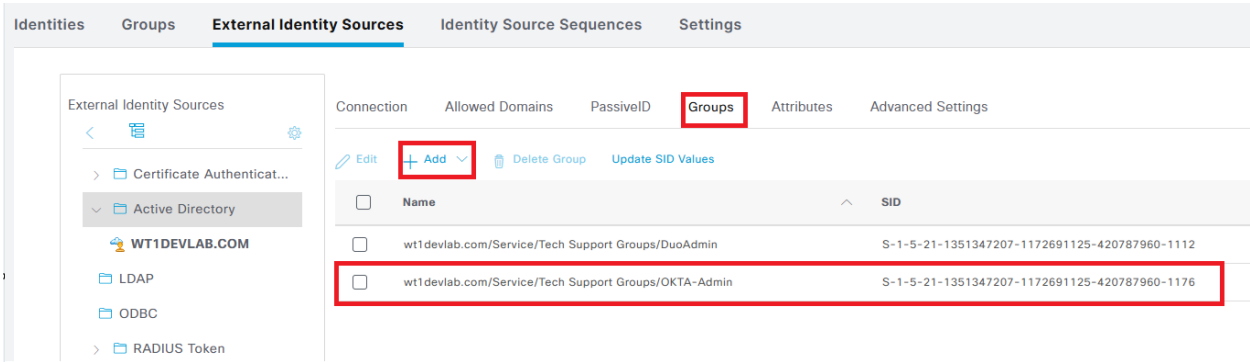
5.2 On **External Identity** Sources tab, Navigate to Active Directory and click **Add**



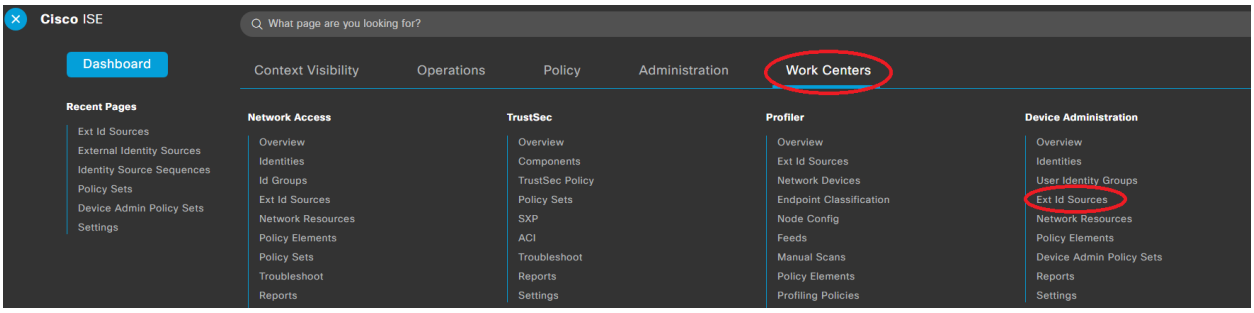
5.3 Under Connection section. Fill in the all requirement and click submit.



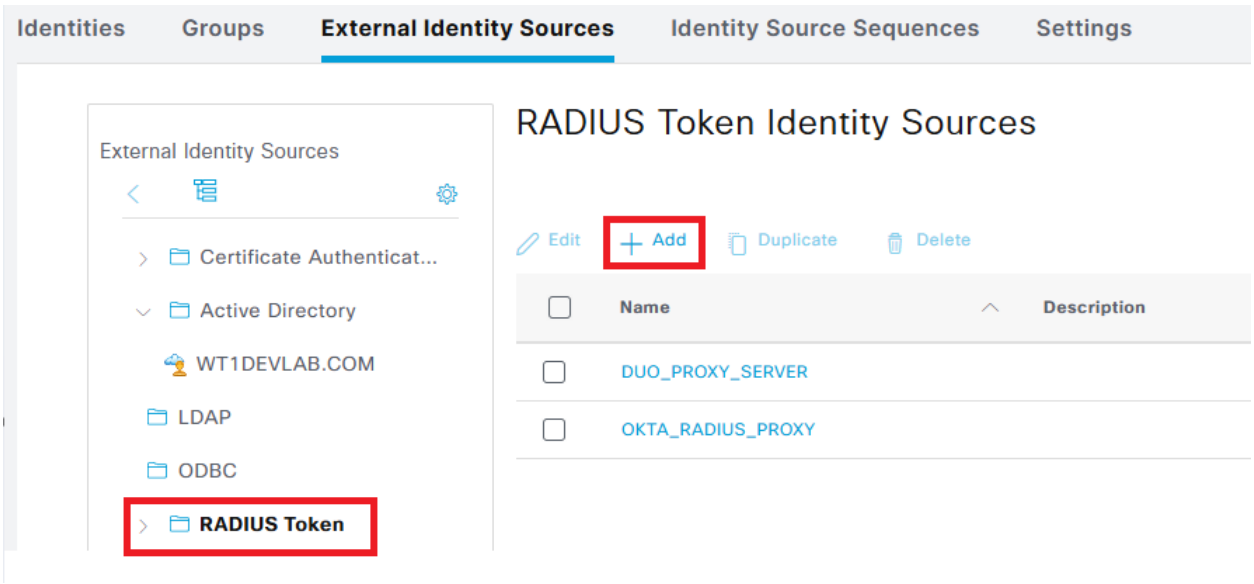
5.4 Navigate to **Groups** tab and click **Add** > **Select Group from Directory**.



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



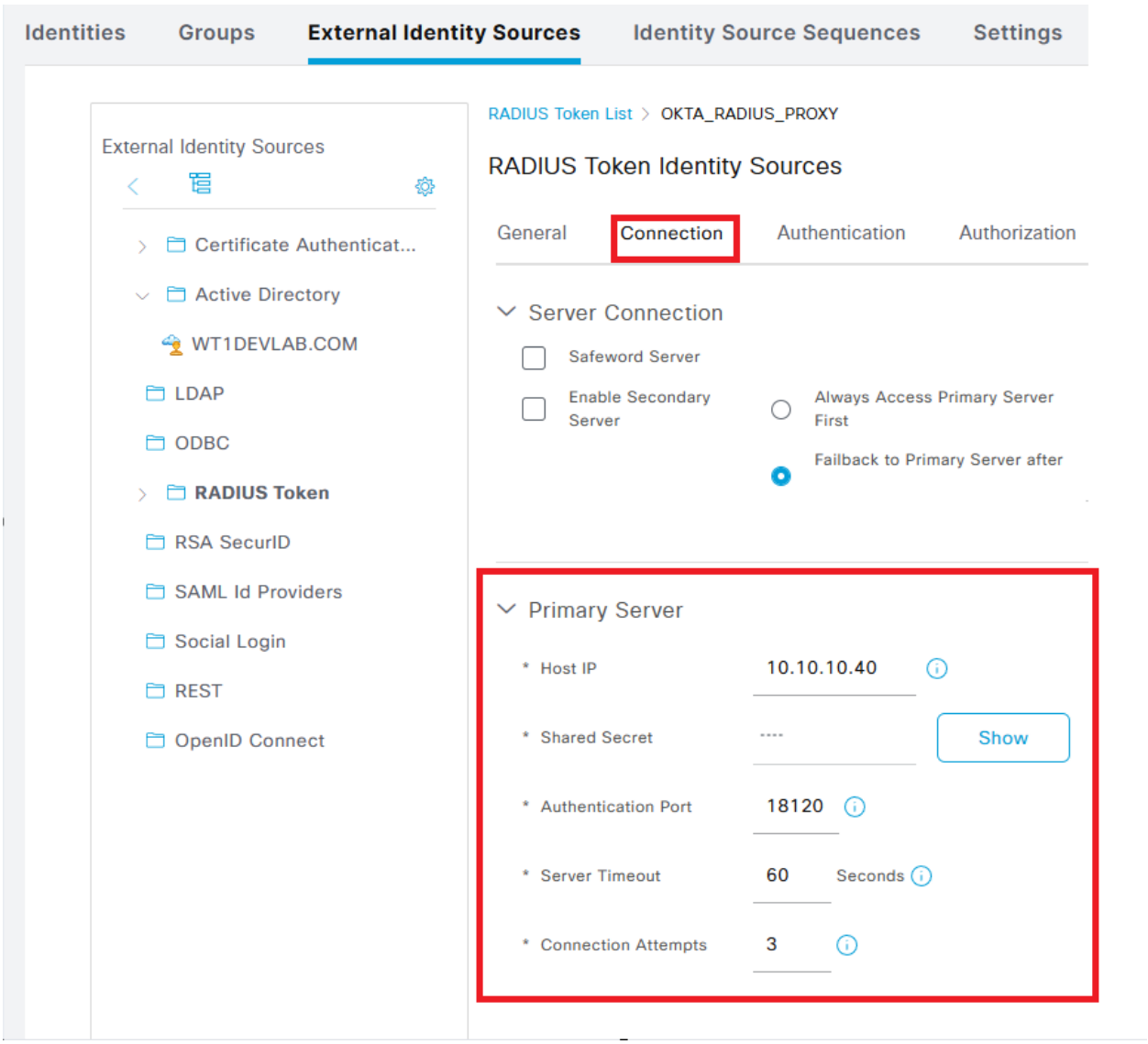
5.6 On RADIUS Token click **Add.**



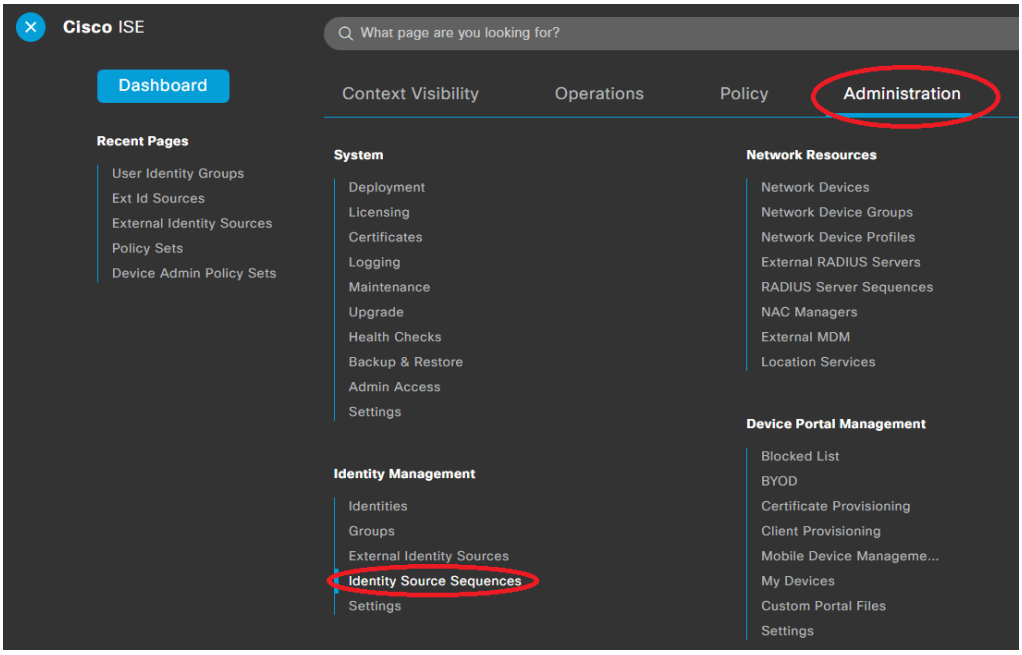
5.7 Starting from the left to right, configure the settings within each tab menu item as follow.

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

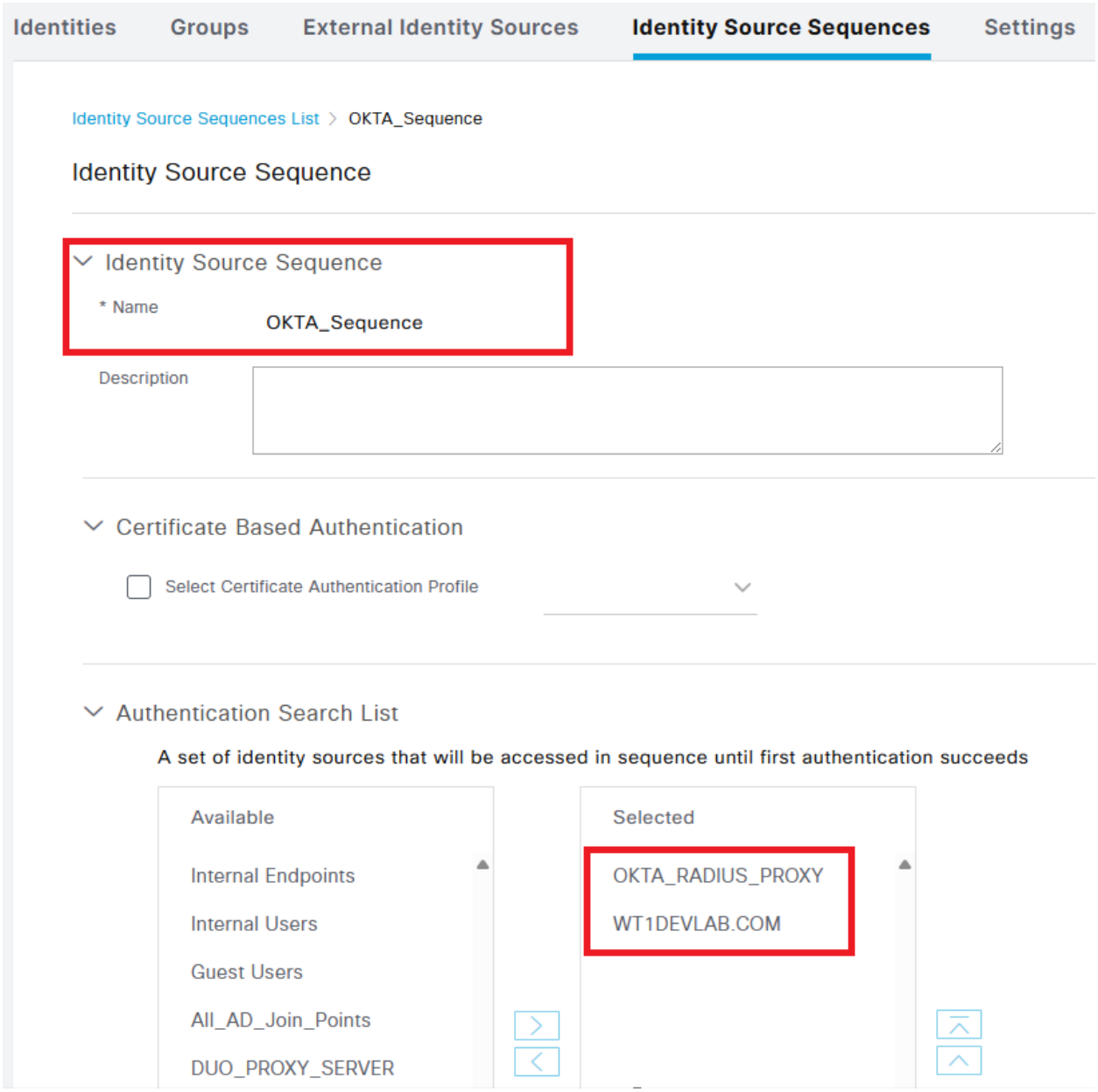
b. In Connection tab, configure the primary server details. (Primary Server is OKTA RADIUS Agent Authentication Server, UDP port and share secret password)



6. [Create Identity Source sequences](). Navigate to **Administration > Identity management > Identity Sources Sequence**

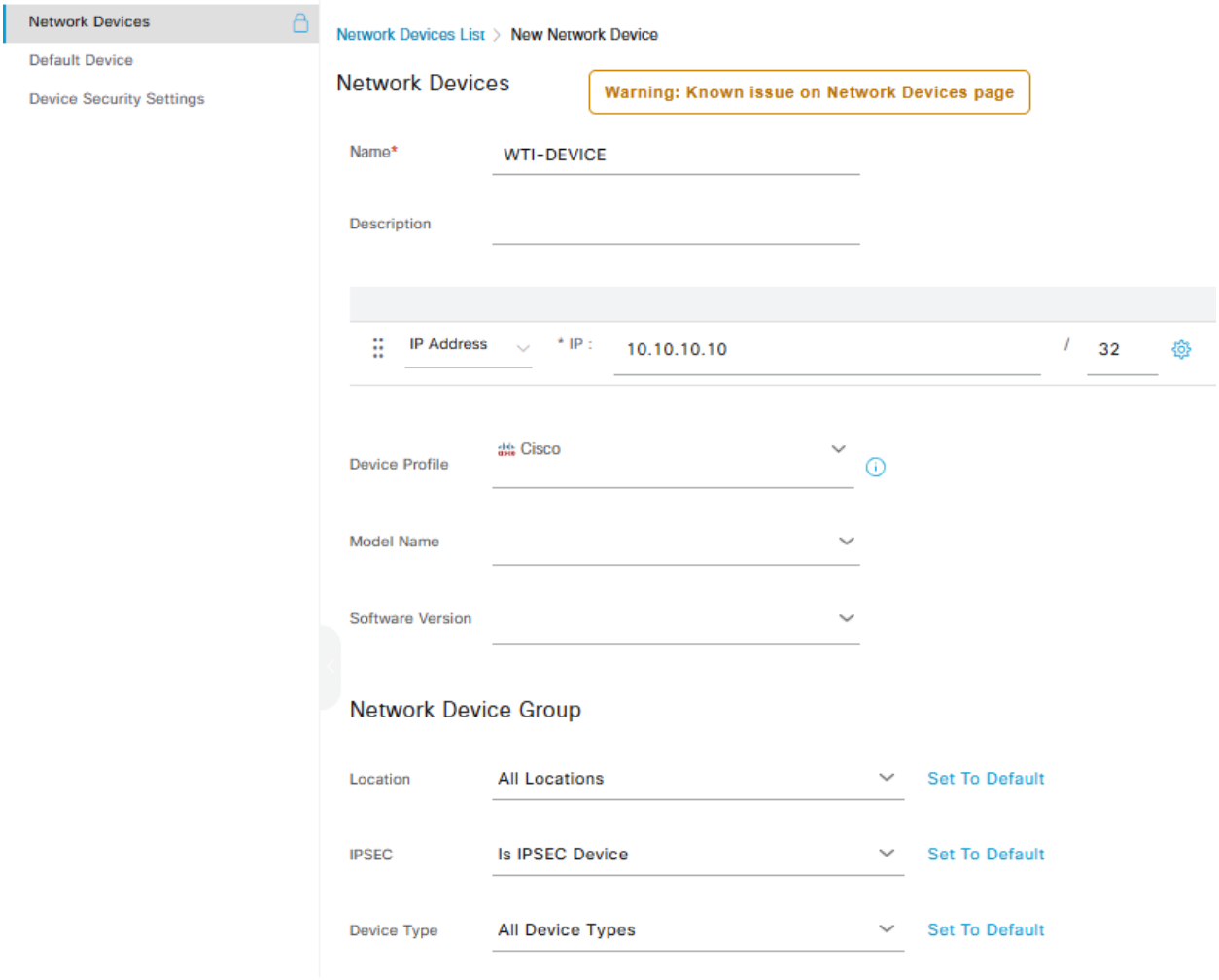


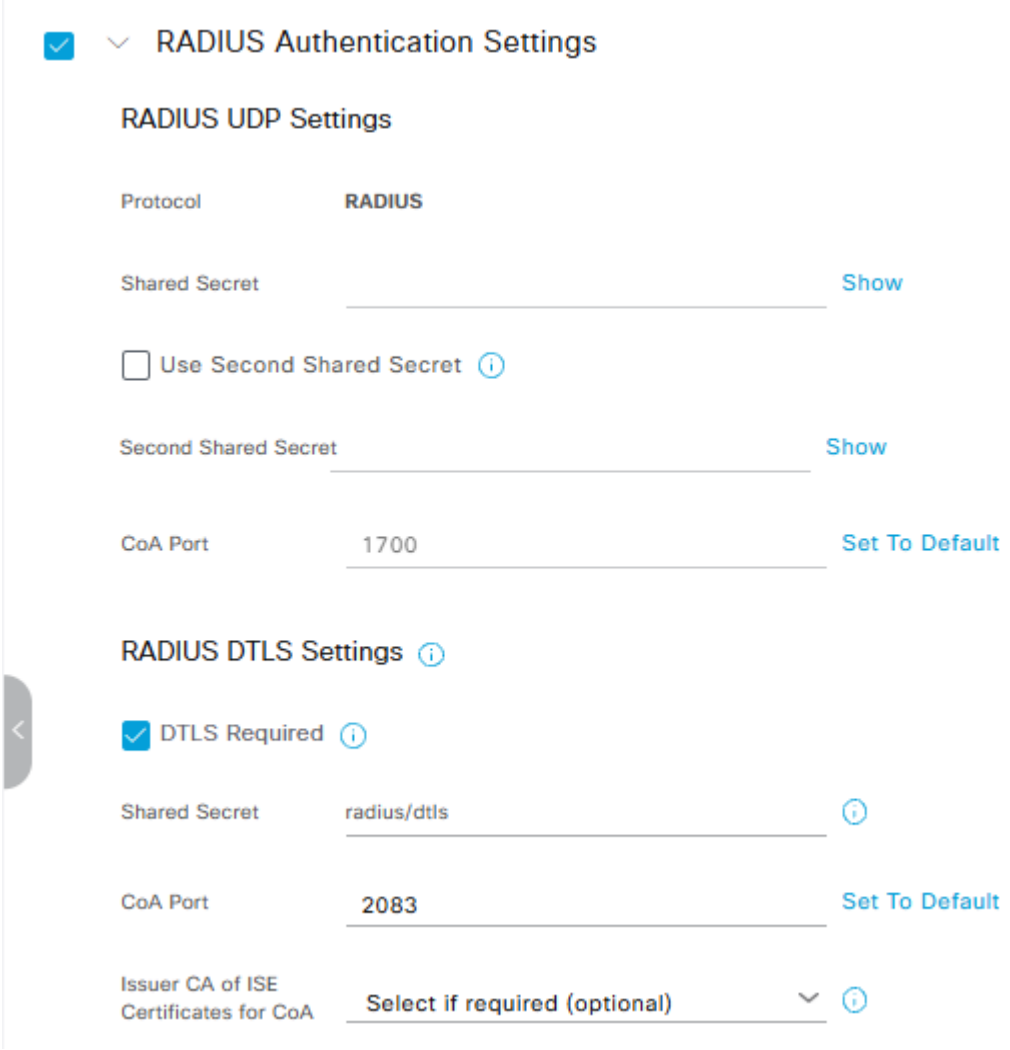
6.1 In Identity Sources Sequence - click **Add** name identity source sequence and select authentication available search list and click Save.



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 DTLS Authentication Settings	Enabled
Shared Secret	Leave is blank (not required)



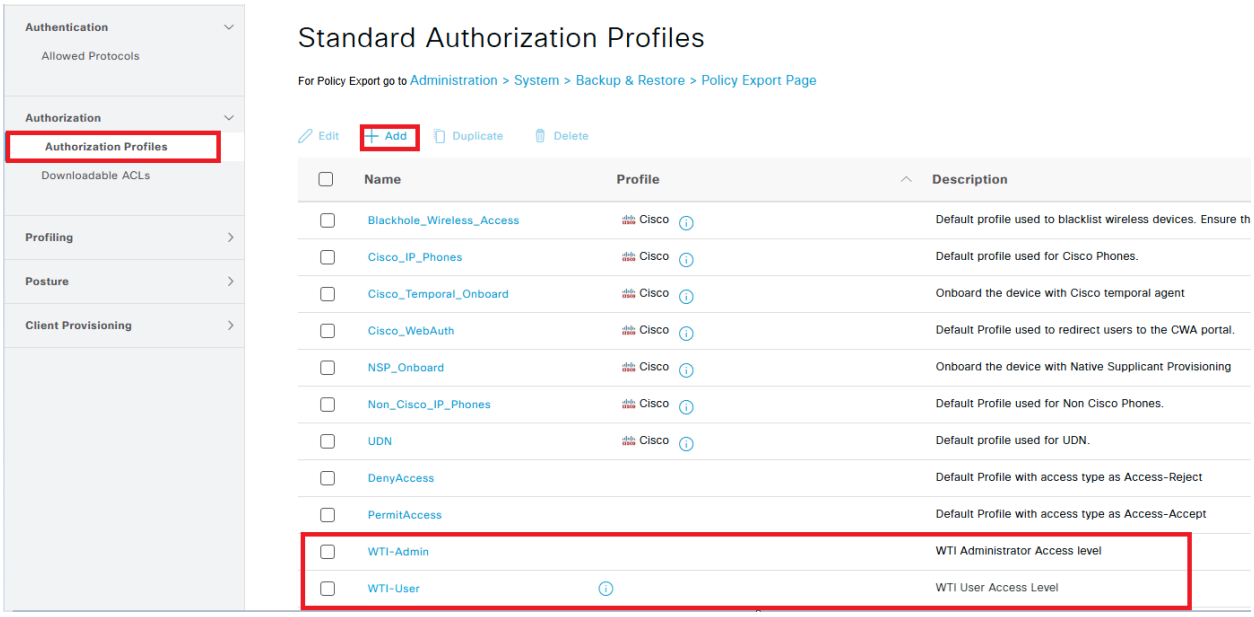


8. Create WTI Radius Authorization Profile in Cisco ISE

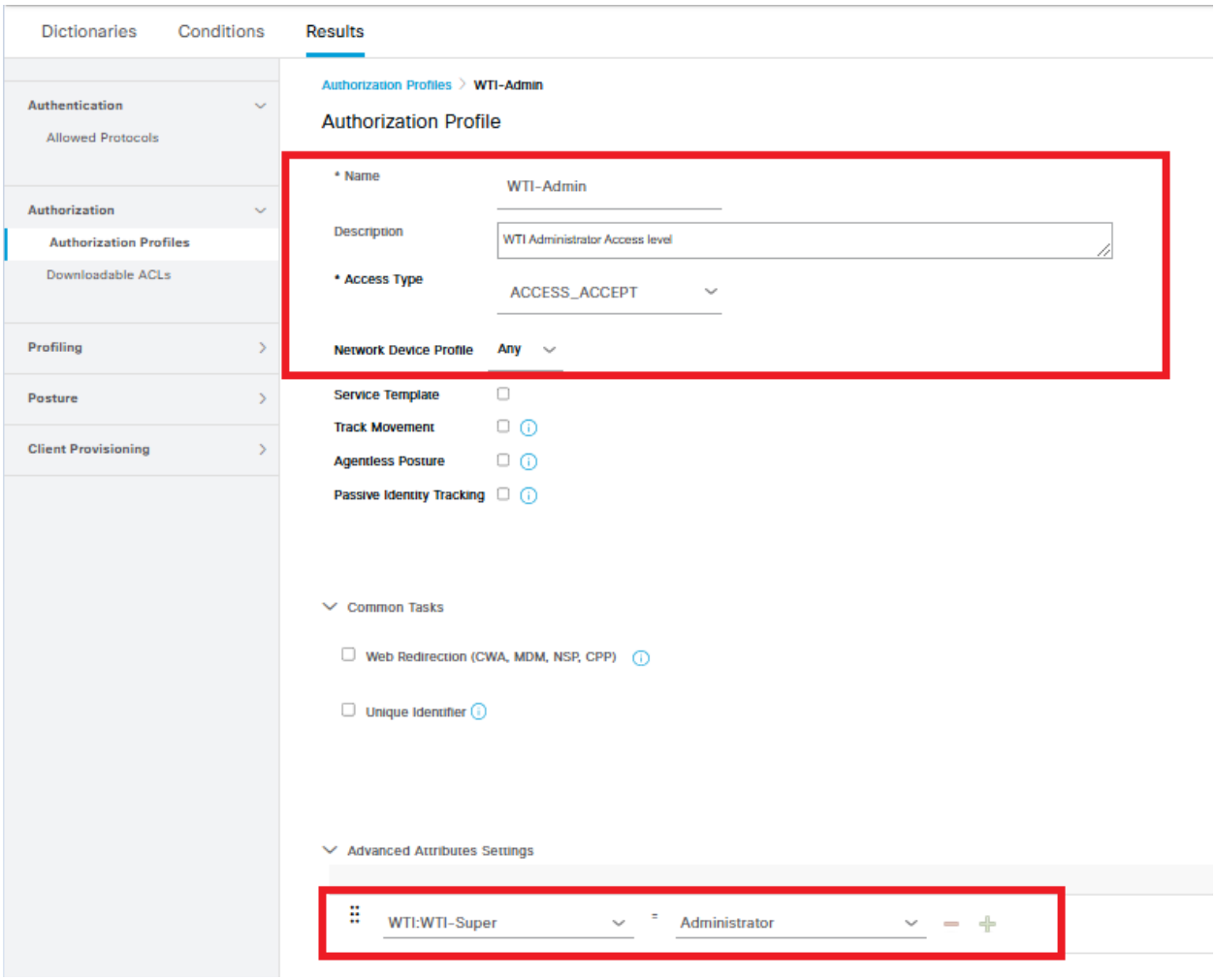
Create separate Cisco ISE Authorization Profiles for each WTI privilege level required by the customer. Cisco ISE must return the WTI vendor-specific attribute with the correct data type.

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**

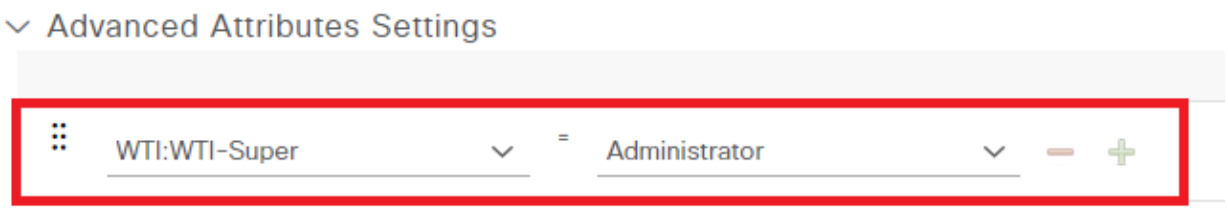


8.2 Create two Authorization Profile. One for WTI_Admin (Administrator access level) and another for WTI_User (User access level).



For WTI_Admin

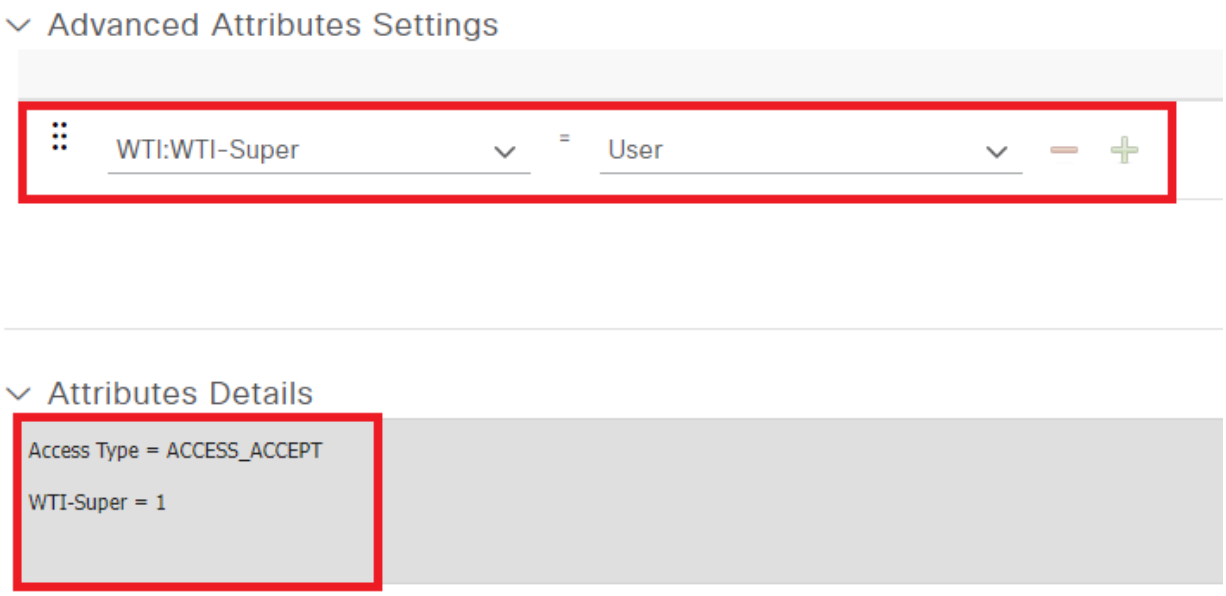
In advanced Attribute Settings





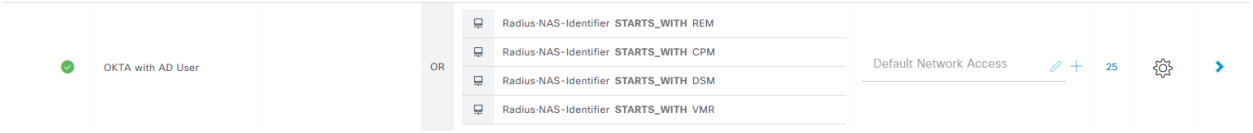
For WTI_User

In Advance Attribute Settings



9. Create Policy with NAS-Identifier

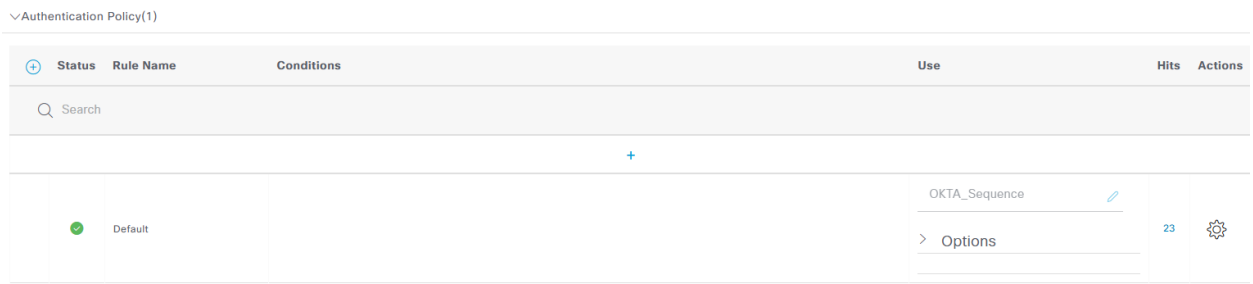
9.1 Navigate to **Policy > Policy Sets > click (+) to add new policy set**.



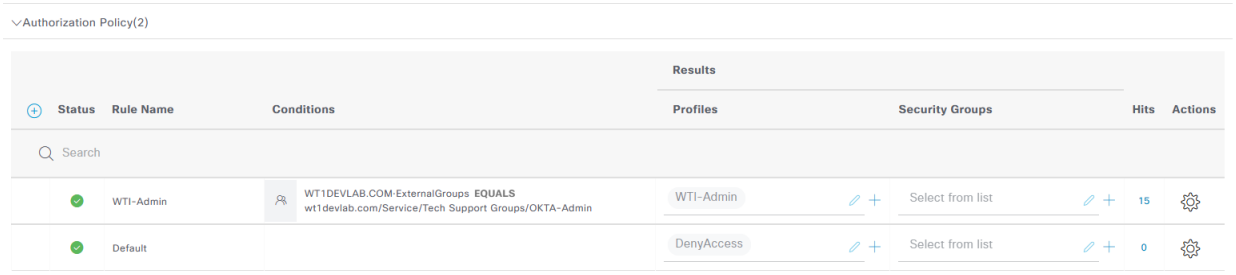
Policy Set Name: **OKTA with AD User**
Condition: **Radius-NAS-Identifier START_WITH REM** (CPM or DSM)
Allowed Protocols: **Default Network Access**

9.2 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

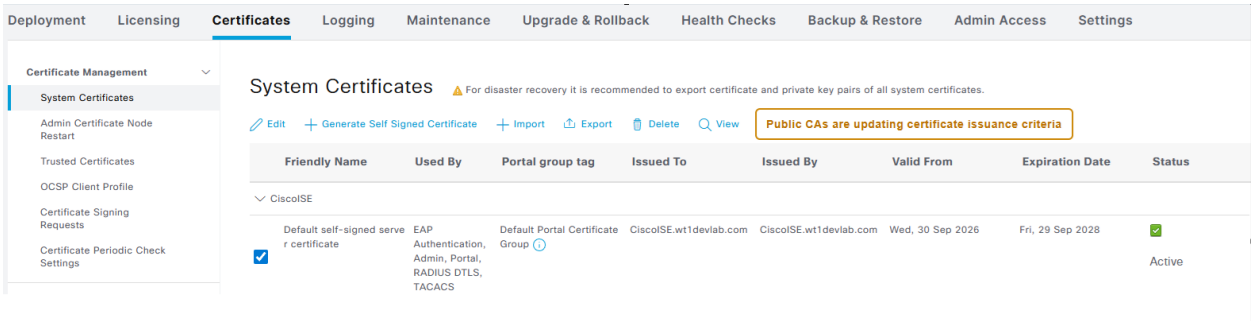
Rule Name: **WTI-Admin**
Condition: **WT1DEVLAB.COM-ExternalGroup EQUALS wt1devlab.com/Service/Tech Support Groups/OKTA-Admin**
Profile: **WTI_Admin**

10. **Export System Certificate**

10.1 Export System Certificates for RADIUS DTLS. In the example we used Self-sign certificate.

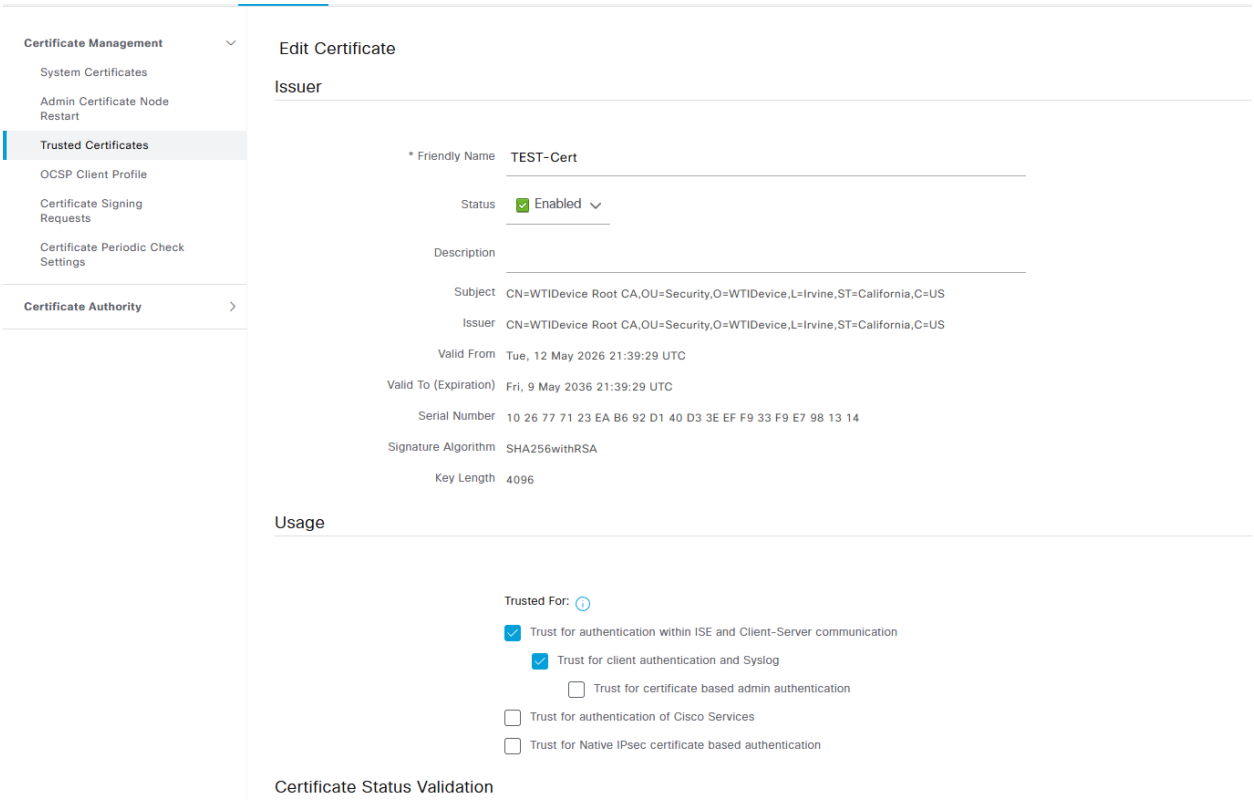
10.2. Go to **Administration** >> **System** >> **Certificate** >> **System Certificate**

10.3. Export Default self-signed server certificate that has RADIUS DTLS under used by column. This certificate will be use to import into **WTI Primary Radius/DTLS Server Certificate**.



10.4 Import WTI **Local RADIUS DTLS CA Public Certificate** into Cisco ISE Trusted Certificate and make sure these two are checked.

- **Trust for authentication within ISE and Client-Server communication.**
- **Trust for client authentication and Syslog.**

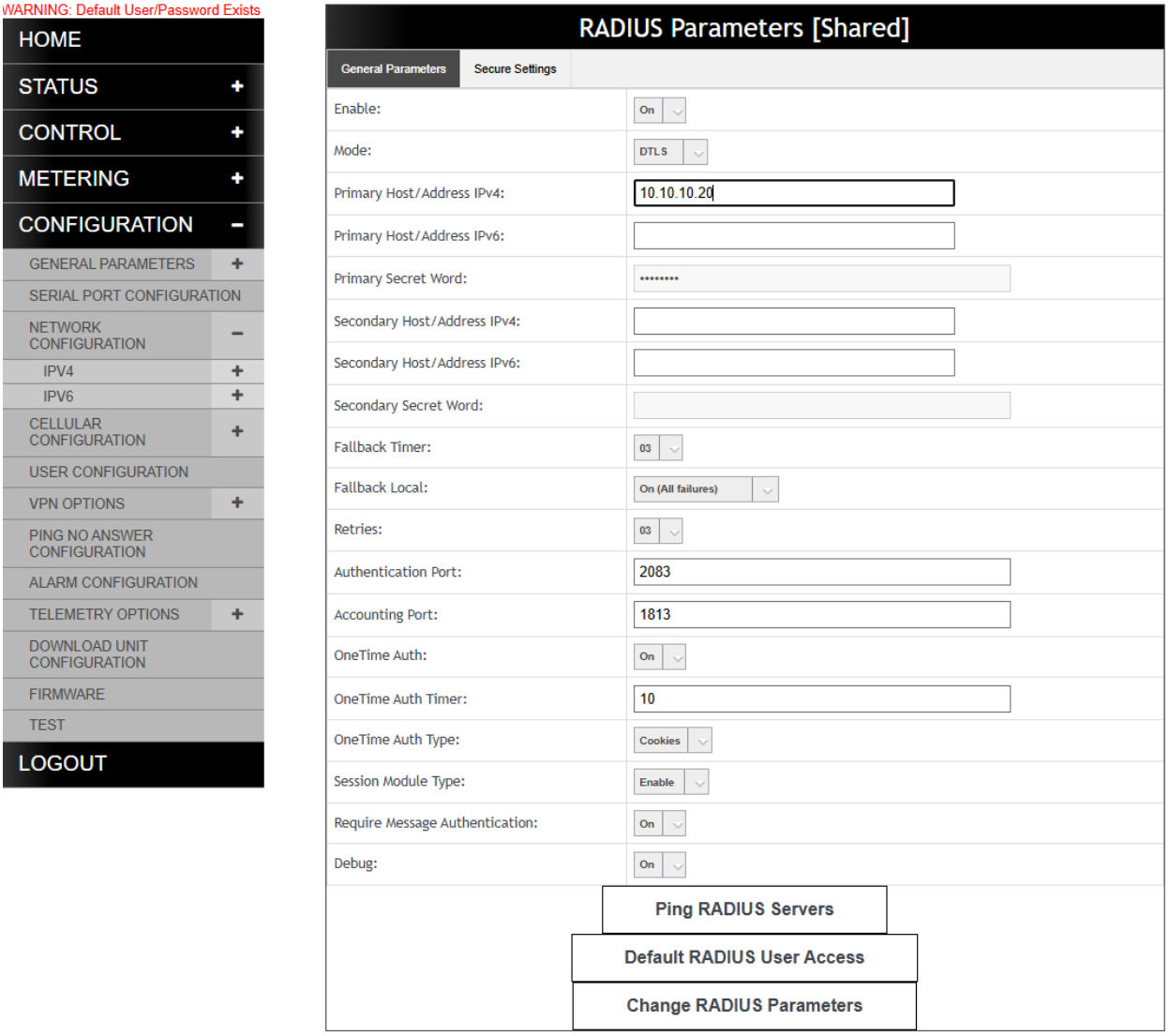


11 WTI Radius Configuration

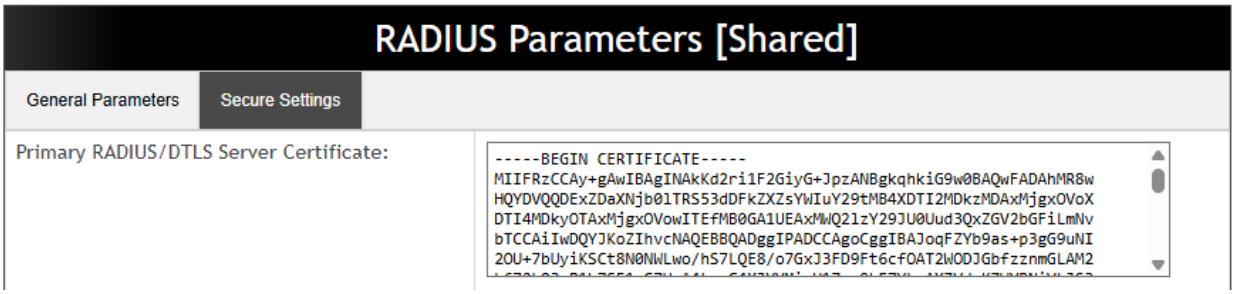
11.1 Import System Certificate from Cisco ISE into WTI primary RADIUS/DTLS Server Certificate.

11.2 Login into Web GUI >> **Configuration** >> **Network Configuration** >> **IPV4** >> **eth0** >> **RADIUS**

13.3 In **General Parameter** tap. Fill out the requirement:



11.4. In **Secure Settings tab**, paste Cisco ISE system certificate that we export from step 10.3 into **Primary RADIUS/DTLS Server Certificate**



11.5 Fill out the requirement associate to your network environment.

Common Name:	10.10.10.10
State or Province:	California
Locality:	Irvine
Country Code:	US
Organization (O):	Organization Name
Organizational Unit (OU):	Organization Unit Nam

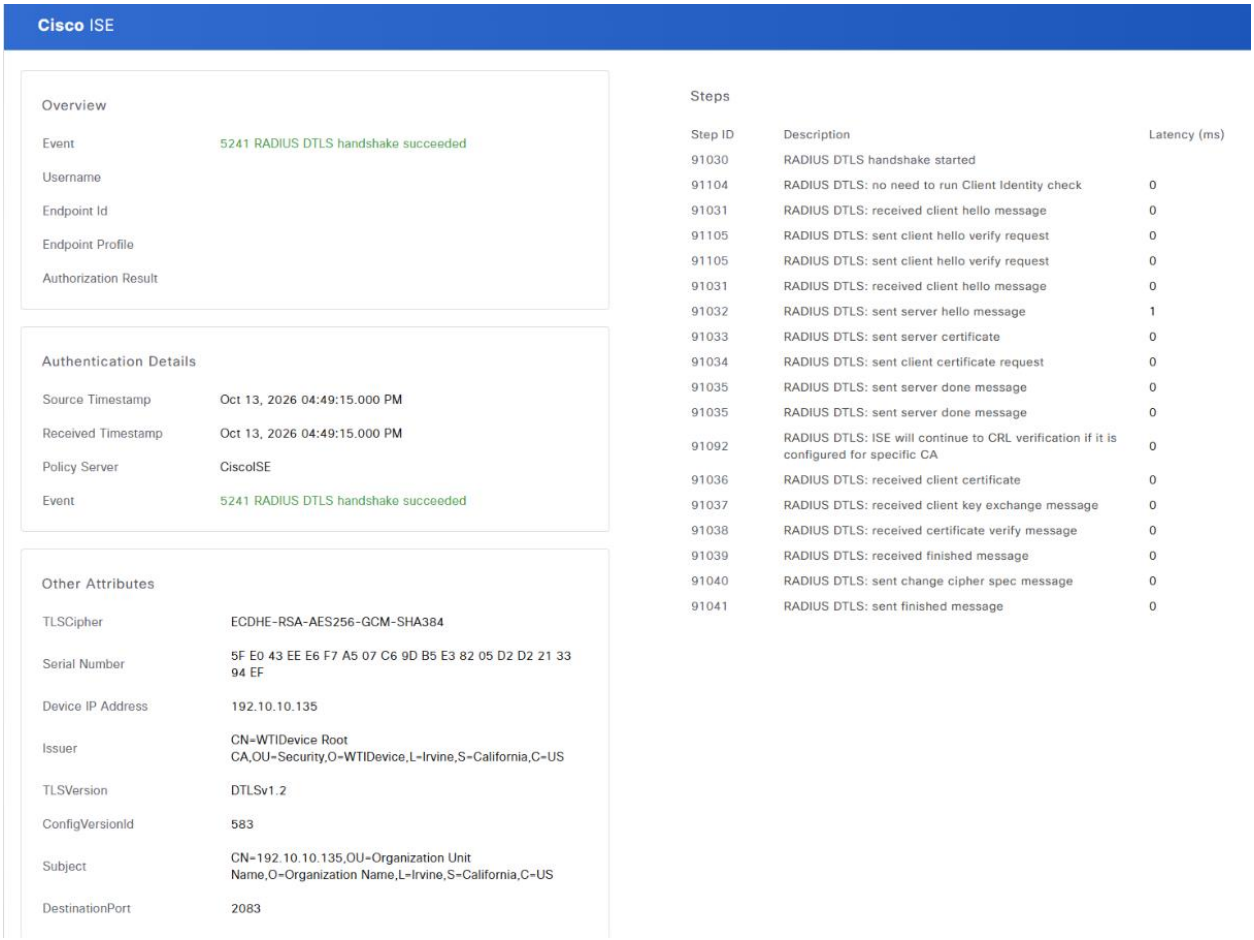
11.6 click on Re-Create Client Certificate and click Change RADIUS Parameters.

Re-Create Client Certificates	Re-Create Client Certificates

11.7 Copy and paste **Local RADIUS DTLS CA Public Certificate** into notepad and import it into Cisco ISE trusted certificate as mentioned in Step 10.4. Done

Local RADIUS DTLS CA Public Certificate: Read Only View Certificate Details	-----BEGIN CERTIFICATE----- MIIGdDCCBFygAwIBAgIUECZ3cSPqtpLRQNM+7/kz+eeYExQwDQYJKoZIhvcNAQEL BQAwdjELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWExDzANBgNVBAcM BklydmluZTESMBAGA1UECgwJV1RJRGV2aWNlMREwDwYDVQQLDAhTZWN1cml0eTEa MBgGA1UEAwwRV1RJRGV2aWNlIFJvb3QgQ0EwHhcNMjYwNTEyMjEzOTI5WhcNMzYw NTA5MjEzOTI5WjB2MQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEP MA0GA1UEBwwGSXJ2aW5lMRIwEAYDVQQKDAlXVElEZXZpY2UxETAPBgNVBAsMCFNl

Cisco ISE Radius Live Log



Cisco ISE

Overview

Event	5241 RADIUS DTLS handshake succeeded
Username	
Endpoint Id	
Endpoint Profile	
Authorization Result	

Authentication Details

Source Timestamp	Oct 13, 2026 04:49:15.000 PM
Received Timestamp	Oct 13, 2026 04:49:15.000 PM
Policy Server	CiscoISE
Event	5241 RADIUS DTLS handshake succeeded

Other Attributes

TLSCipher	ECDHE-RSA-AES256-GCM-SHA384
Serial Number	5F E0 43 EE E6 F7 A5 07 C6 9D B5 E3 82 05 D2 D2 21 33 94 EF
Device IP Address	192.10.10.135
Issuer	CN=WTIDevice Root CA,OU=Security,O=WTIDevice,L=Irvine,S=California,C=US
TLSVersion	DTLSv1.2
ConfigVersionId	583
Subject	CN=192.10.10.135,OU=Organization Unit Name,O=Organization Name,L=Irvine,S=California,C=US
DestinationPort	2083

Steps

Step ID	Description	Latency (ms)
91030	RADIUS DTLS handshake started	
91104	RADIUS DTLS: no need to run Client Identity check	0
91031	RADIUS DTLS: received client hello message	0
91105	RADIUS DTLS: sent client hello verify request	0
91105	RADIUS DTLS: sent client hello verify request	0
91031	RADIUS DTLS: received client hello message	0
91032	RADIUS DTLS: sent server hello message	1
91033	RADIUS DTLS: sent server certificate	0
91034	RADIUS DTLS: sent client certificate request	0
91035	RADIUS DTLS: sent server done message	0
91035	RADIUS DTLS: sent server done message	0
91092	RADIUS DTLS: ISE will continue to CRL verification if it is configured for specific CA	0
91036	RADIUS DTLS: received client certificate	0
91037	RADIUS DTLS: received client key exchange message	0
91038	RADIUS DTLS: received certificate verify message	0
91039	RADIUS DTLS: received finished message	0
91040	RADIUS DTLS: sent change cipher spec message	0
91041	RADIUS DTLS: sent finished message	0

WTI Log

Issue this command **/bash cat /var/log/radsec.log**

```
REM> /bash cat /var/log/radsec.log
Tue Oct 13 09:46:59 2026: radsecproxy 1.12.0-dev starting
Tue Oct 13 09:46:59 2026: resolvehostport: (src info not available) -> 0.0.0.0, ::
Tue Oct 13 09:46:59 2026: addserver: starting new client writer for ise1
Tue Oct 13 09:46:59 2026: resolvehostport: 127.0.0.1 -> 127.0.0.1
Tue Oct 13 09:46:59 2026: disable_DF_bit: disabling DF bit (Linux variant)
Tue Oct 13 09:46:59 2026: createlistener: listening for udp on 127.0.0.1:1812
Tue Oct 13 09:46:59 2026: resolvehostport: 127.0.0.1 -> 127.0.0.1
Tue Oct 13 09:46:59 2026: disable_DF_bit: disabling DF bit (Linux variant)
Tue Oct 13 09:46:59 2026: createlistener: listening for udp on 127.0.0.1:1813
Tue Oct 13 09:46:59 2026: radsecproxy startup complete
Tue Oct 13 09:46:59 2026: dtlsconnect: initial connection to ise1
Tue Oct 13 09:46:59 2026: dtlsconnect: trying to open DTLS connection to server ise1 (192.10.10.250 port 2083)
Tue Oct 13 09:46:59 2026: disable_DF_bit: disabling DF bit (Linux variant)
Tue Oct 13 09:46:59 2026: udp server writer, waiting for signal
Tue Oct 13 09:46:59 2026: verifyconfcert: verify certificate for host ise1, subject CN=CiscoISE.wt1devlab.com
Tue Oct 13 09:46:59 2026: dtlsconnect: DTLS connection to ise1 (192.10.10.250 port 2083), subject CN=CiscoISE.wt1devlab.com up
Tue Oct 13 09:47:13 2026: radudpget: got 90 bytes from 127.0.0.1
Tue Oct 13 09:47:13 2026: radsrv: code 4, id 177
Tue Oct 13 09:47:13 2026: radsrv: got Accounting-Request (id 177) with username: super1 from client localhost (127.0.0.1)
Tue Oct 13 09:47:13 2026: found matching realm: *
Tue Oct 13 09:47:13 2026: found matching conf: ise1
Tue Oct 13 09:47:13 2026: sendrq: inserting packet with id 0 in queue for ise1
Tue Oct 13 09:47:13 2026: sendrq: signalling client writer
Tue Oct 13 09:47:13 2026: freerealm: called with refcount 4
Tue Oct 13 09:47:13 2026: clientwr: got new request
Tue Oct 13 09:47:13 2026: clientradputdtls: Sent 90 bytes, Radius packet of length 90 to DTLS peer ise1
Tue Oct 13 09:47:13 2026: radtlsget: got 20 bytes, ignoring 0 bytes of padding
Tue Oct 13 09:47:13 2026: got Accounting-Response message with id 0
Tue Oct 13 09:47:13 2026: Accounting-Response for user super1 from ise1 to localhost (127.0.0.1)
Tue Oct 13 09:47:13 2026: replyh: passing Accounting-Response (id 177) to client localhost (127.0.0.1)
Tue Oct 13 09:47:13 2026: signalling server writer
Tue Oct 13 09:47:13 2026: freerq: called with refcount 3
Tue Oct 13 09:47:13 2026: udp server writer, got signal
Tue Oct 13 09:47:13 2026: udpserverwr: refcount 2
Tue Oct 13 09:47:13 2026: freerq: called with refcount 2
```