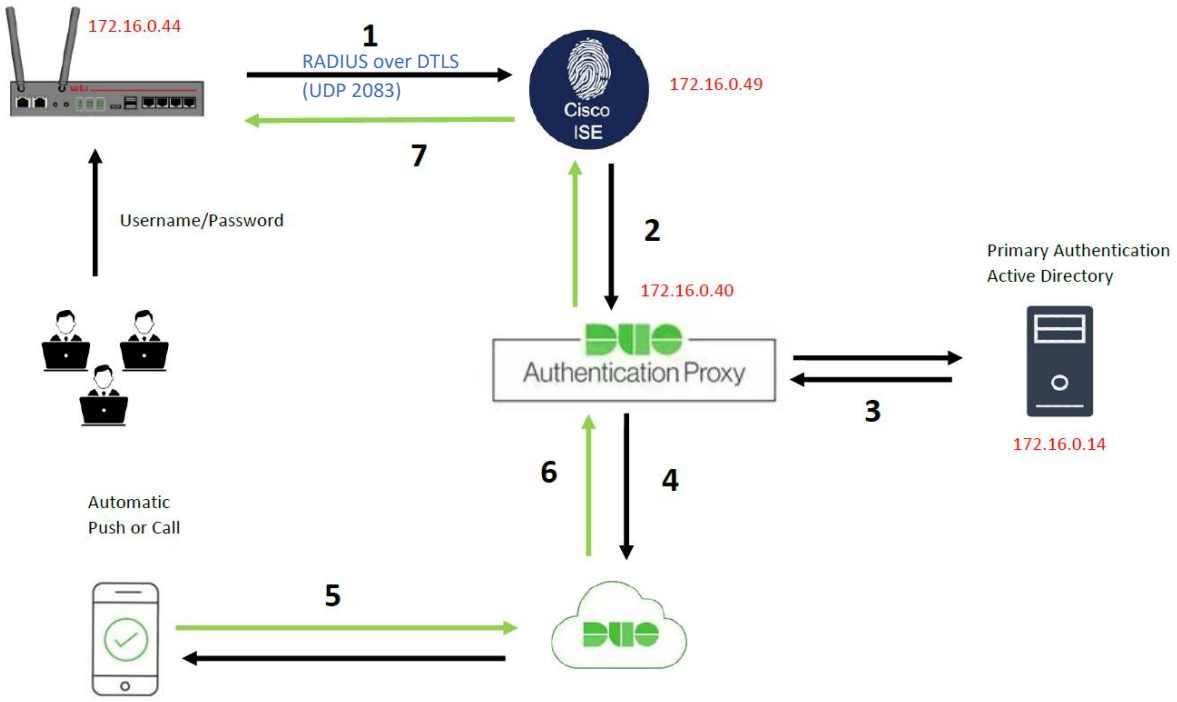
Cisco ISE + Duo MFA + Windows AD Integration for WTI (RADIUS over DTLS)



Introduction

This document describes how to configure Duo push integration with Active Directory (AD) and Cisco Identity Service (ISE) as Two-Factor Authentication that connect to WTI Radius client.

Components used

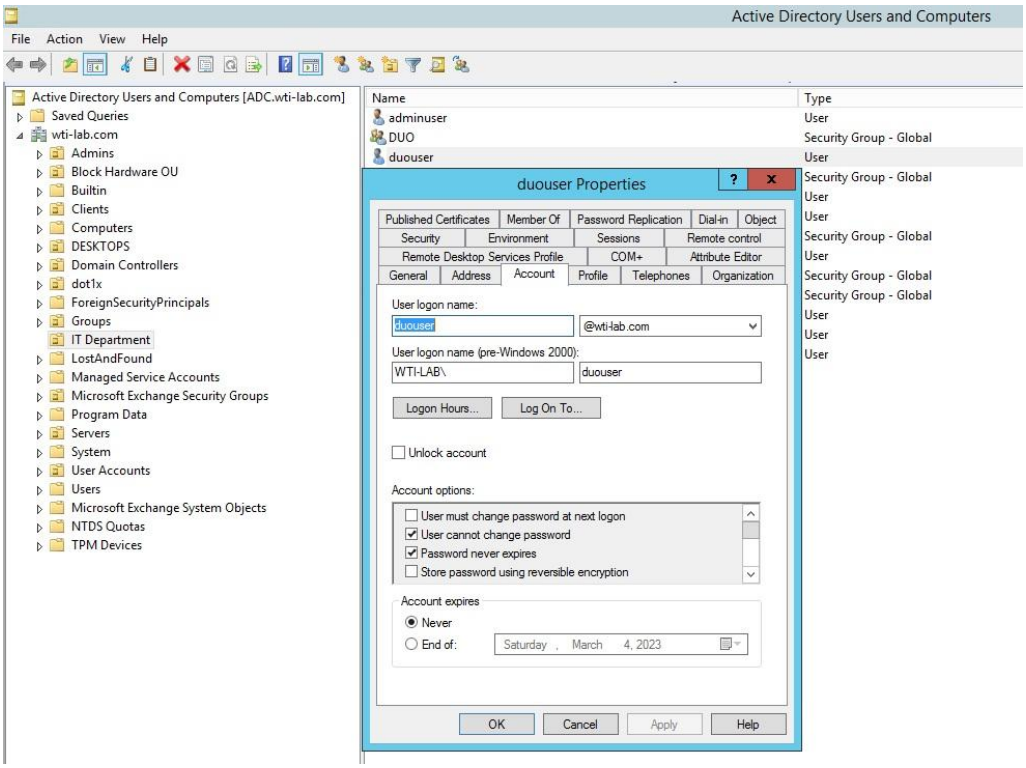
- Windows Active Directory
- Duo
- Duo Authentication Proxy Manager
- Cisco ISE
- WTI Radius client

Communication process

1. WTI makes an authentication request to Cisco ISE
2. Cisco ISE sends authentication request to the Duo Authentication Proxy
3. Duo Proxy sends a request to Active Directory
4. Duo Authentication Proxy connection established to Duo security over TCP port 443
5. Secondary authentication via Duo Security's service
6. Duo authentication proxy receives authentication response
7. Cisco ISE return to WTI with Access Accept + Radius attribute 41 and WTI permits the user access.

Active Directory Configurations

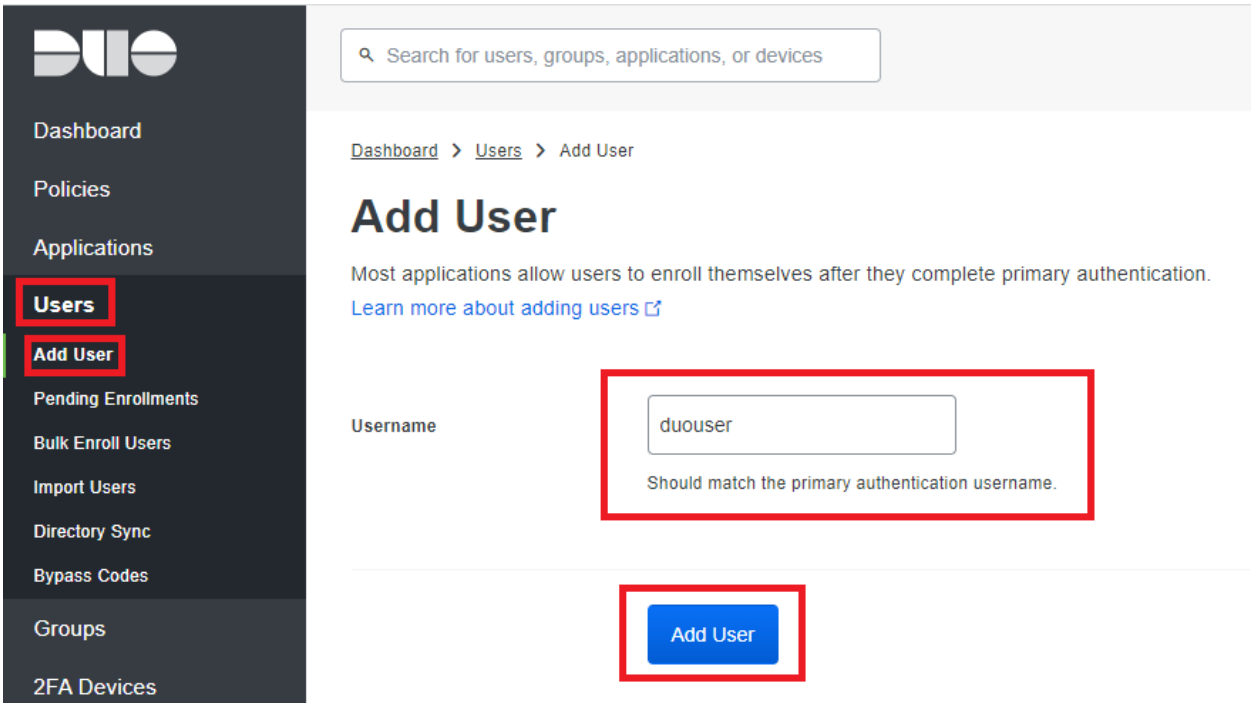
1. Navigate to Active Directory Users and Computers > Add new User and Password. In this example we created **duouser** account in active directory users and computers.



Duo configuration

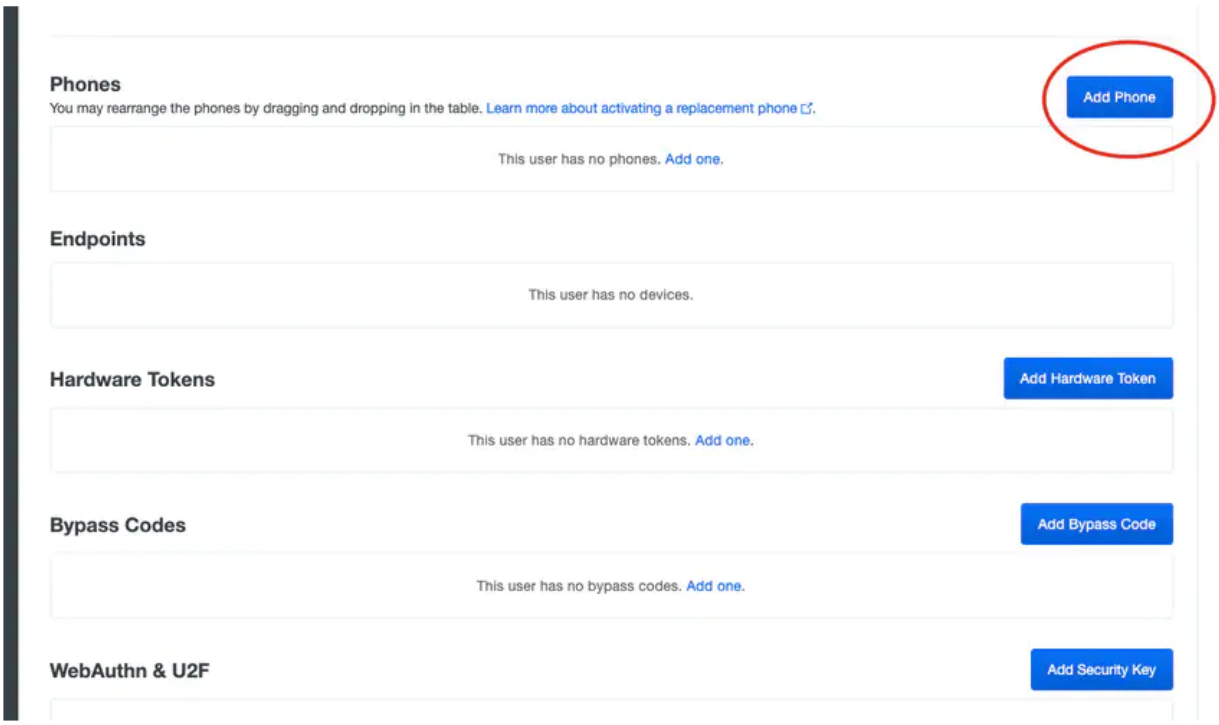
1. Log in into your Duo Admin portal

2. On the left side panel, navigate to **Users**, click **Add User** and type the name of the user that matches your Active Domain username, then click Add User.

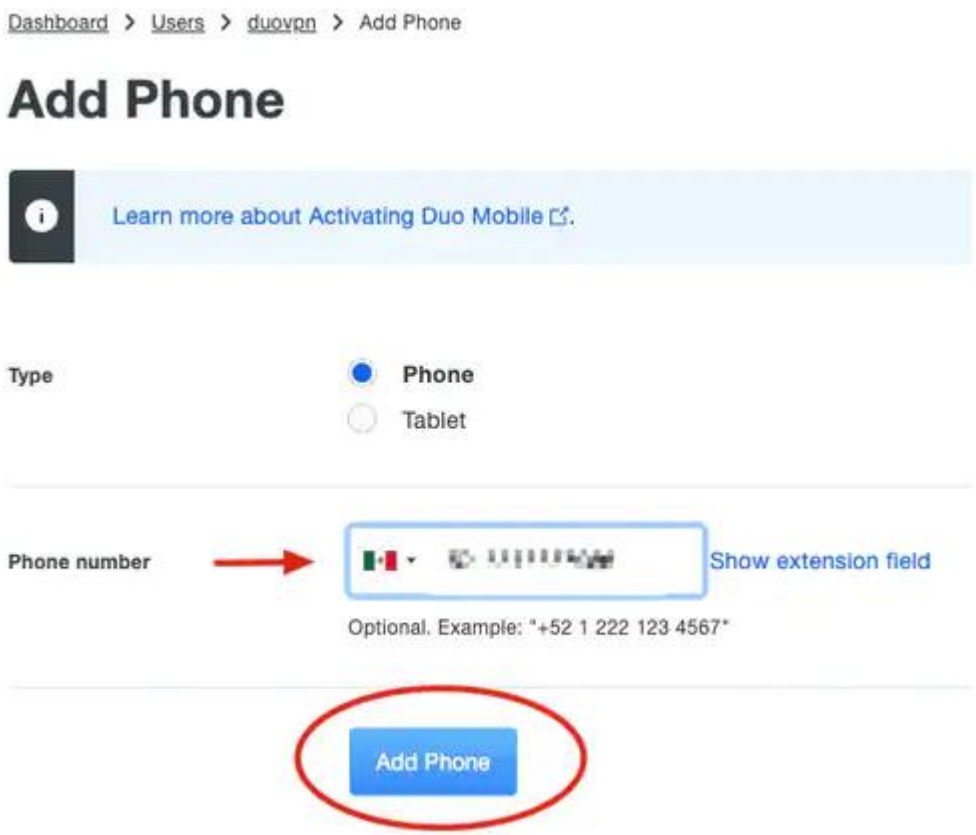


3. On the new user's panel, fill in the blank all the necessary information.

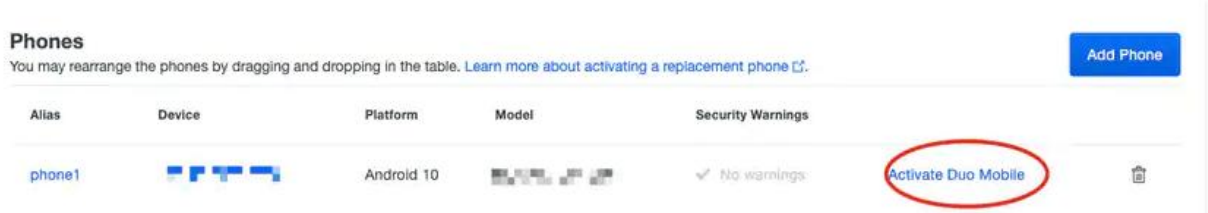
4. Under user devices specify the secondary authentication method. Click **Add Phone**



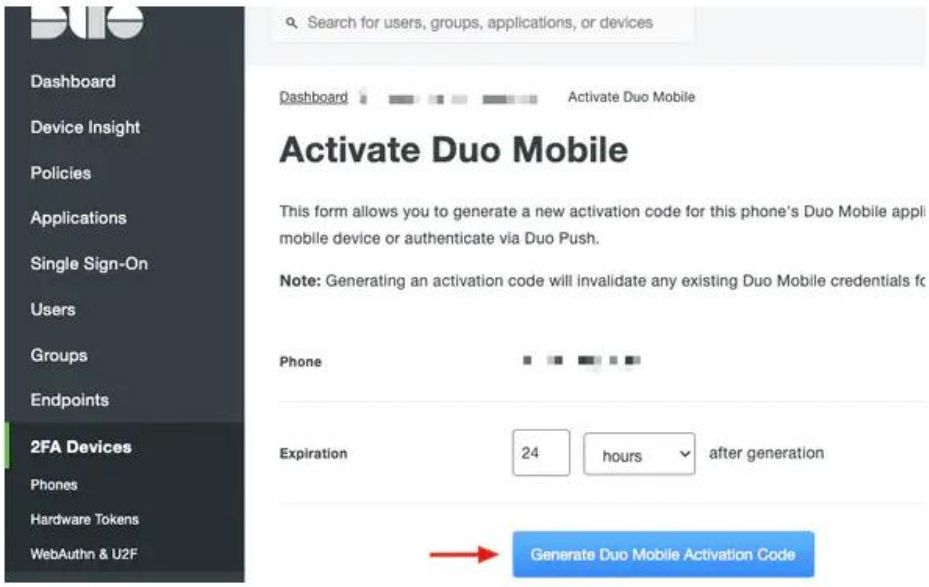
5. Type in the user's phone number and click **Add Phone**



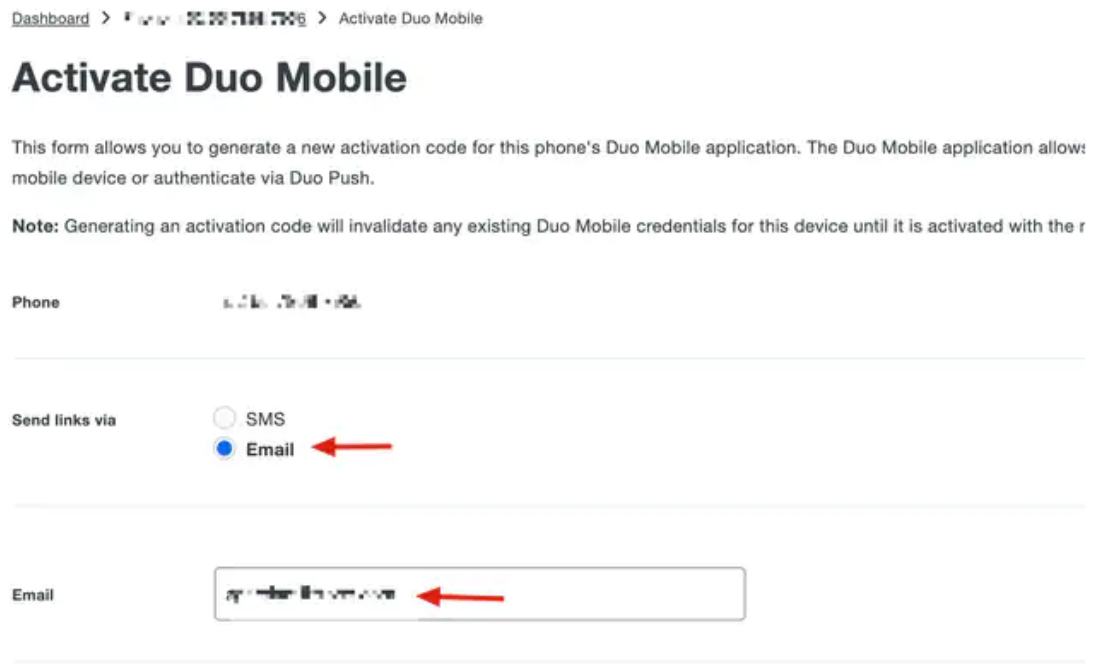
6. Navigate to **Phones** section and click **Activate Due Mobile**.



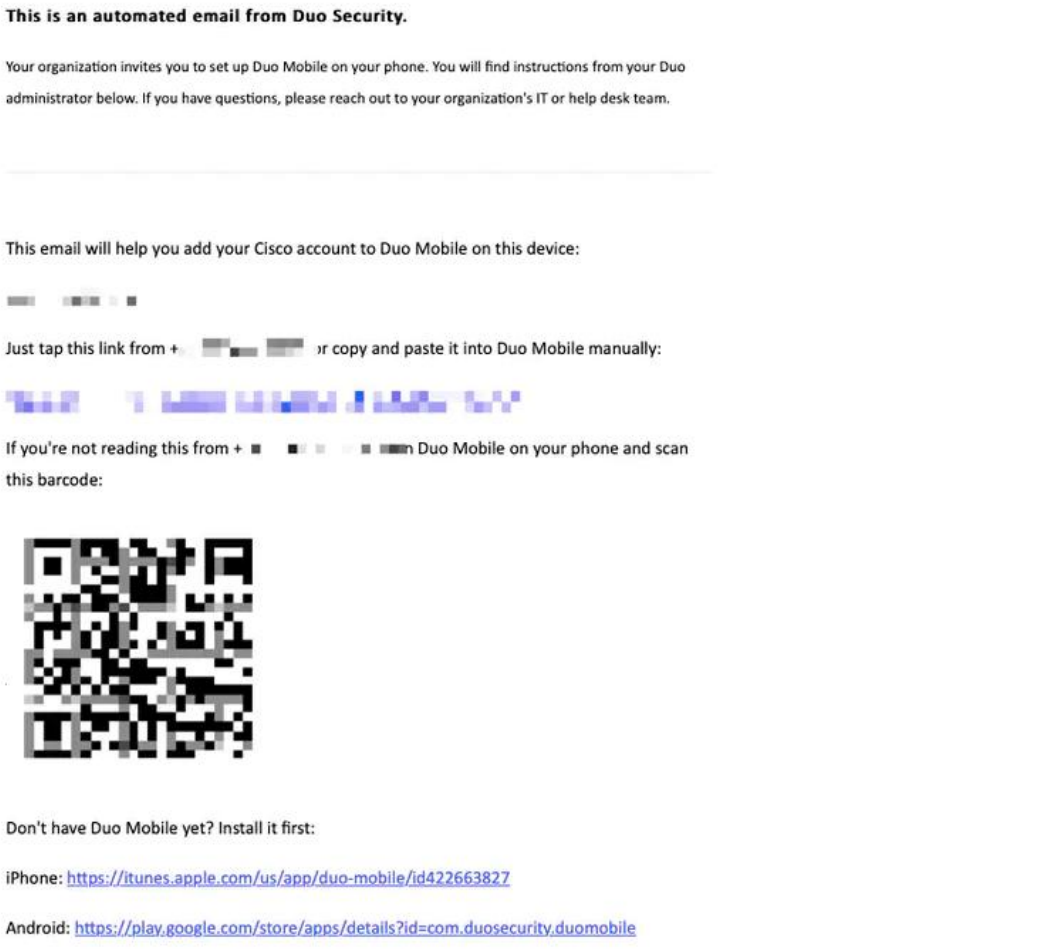
7. Click **Generate Duo Mobile Activation Code.**



8. Select **Email** in order to receive the instruction via email, type your email address and click **Send Instructions by email**.



9. You receive an email with the instructions, as show in the image



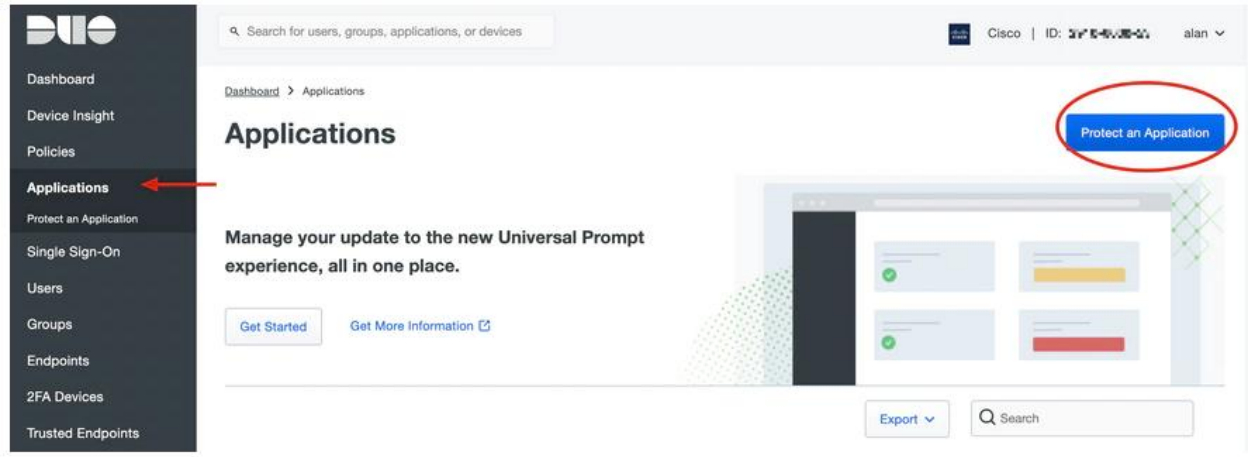
10. Open the Duo Mobile App from your mobile device and click **Add** then select **Use QR code** and scan the code from the instructions email.

11. New user is added to your Duo Mobile App.

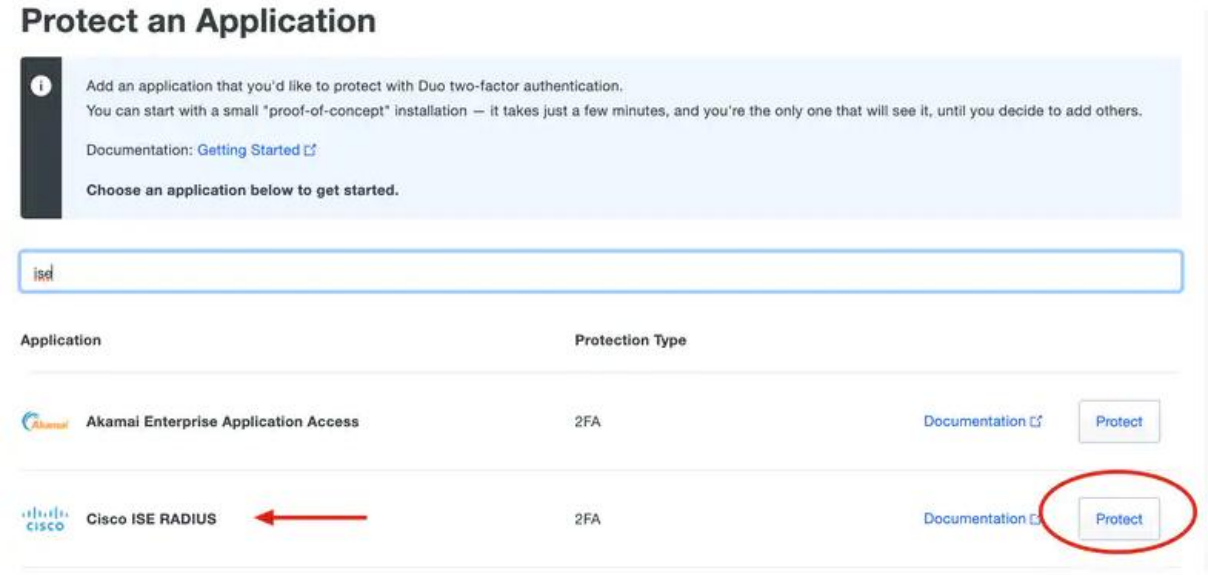
Duo Authentication Proxy Configuration

1. Download and Install Duo Auth Proxy manager from https://duo.com/docs/authproxy-reference.

2. On the Duo Admin Panel navigate to **Applications** and click **Protect an Application**.



3. On the search bar, look for Cisco ISE Radius.



4. Copy the Integration key, Secret key and the API Hostname. You need this information for the Duo Authentication Proxy configuration.

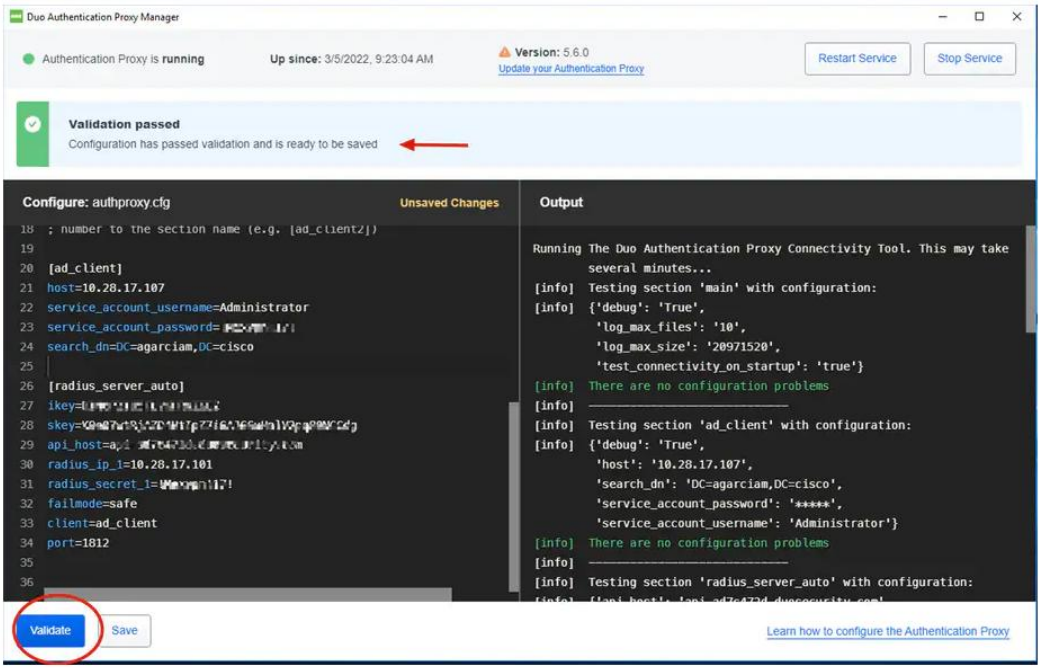


5. Run the Duo Authentication Proxy manager application and complete the configuration for both Active Directory client ISE Radius server and click Validate.

Duo proxy config: authproxy.cfg
The Duo proxy config file should be on the machine you installed the Duo proxy program, at this file location:

Windows
C:\Program files\Duo Security Authentication Proxy\conf\authproxy.cfg

Linux
/opt/duoauthproxy/conf/authproxy.cfg



Below is sample configuration of authproxy.cfg

- Primary authenticator, Windows Active Directory Server is on **172.16.0.14**
- Duo Authentication Proxy manager is on Windows Server **172.16.0.40**
- WTI Device is on **172.16.0.44**
- Cisco ISE is on **172.16.0.49**

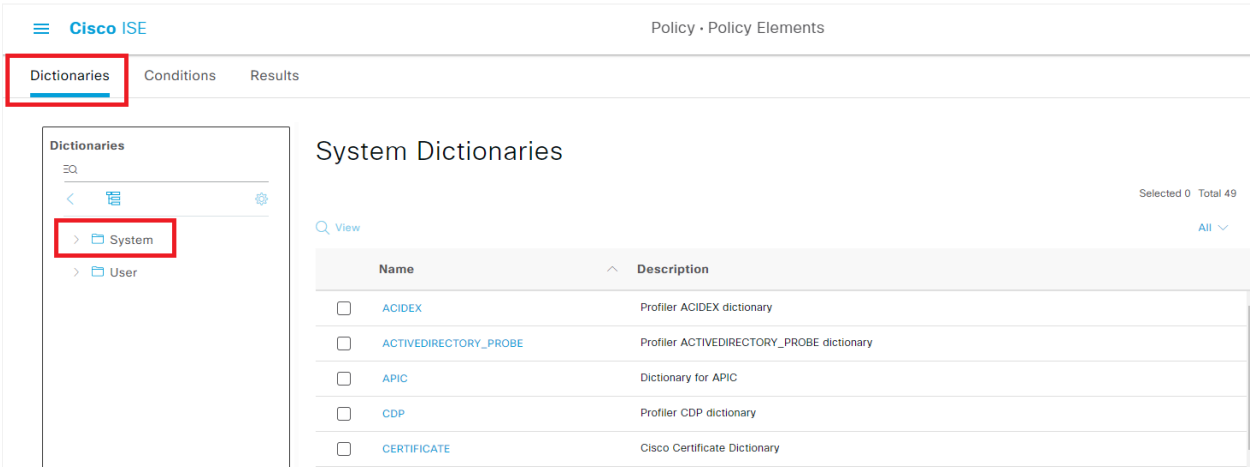
```
[ad_client]
host=172.16.0.14
service_account_username=duouser
service_account_password=duosecret
search_dn=DC=wti-lab,DC=com
security_group_dn=CN=DUO,OU=IT Department,DC=wti-lab,DC=com

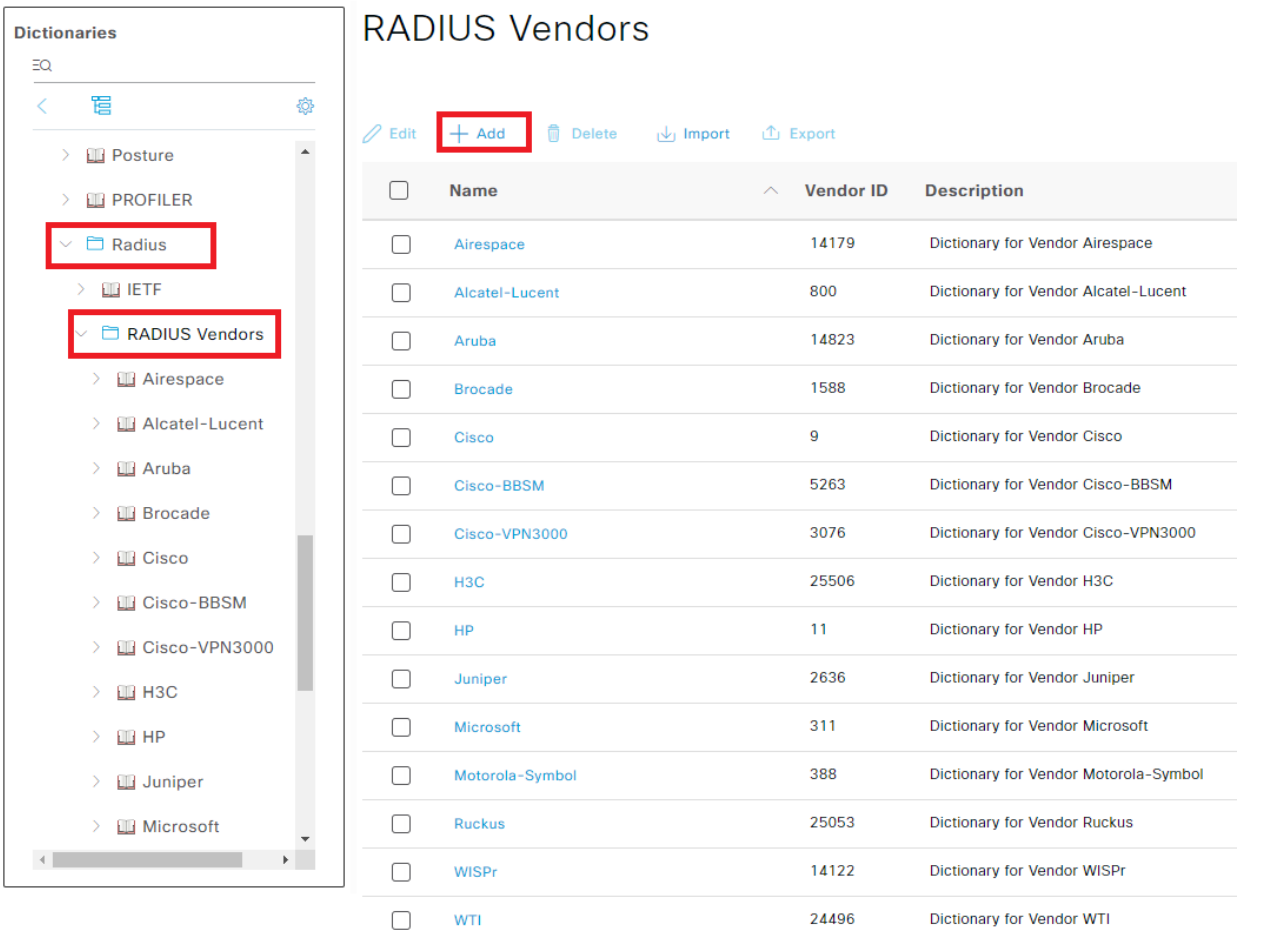
[radius_server_auto]
ikey=XXXXXXXXXXXXXXXXX
skey=YYYYYYYYYYYYYYYYY
api_host=api-123456789.duosecurity.com
radius_ip_1=172.16.0.49
radius_secret_1=test123
client=ad_client
port=1812
```

Cisco ISE Configurations

Step 1: Create vendor-specific attribute

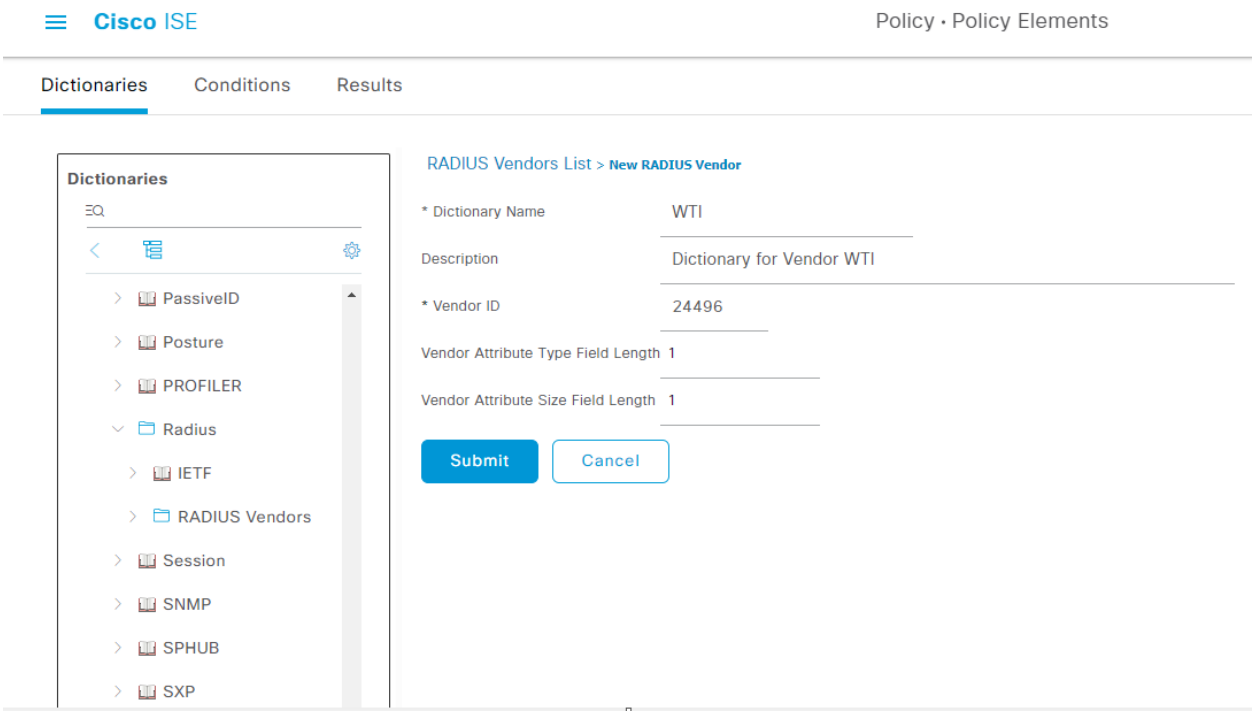
1. Navigate to **Policy > Policy Element > Dictionaries > System > Radius > Radius Vendors > Add**

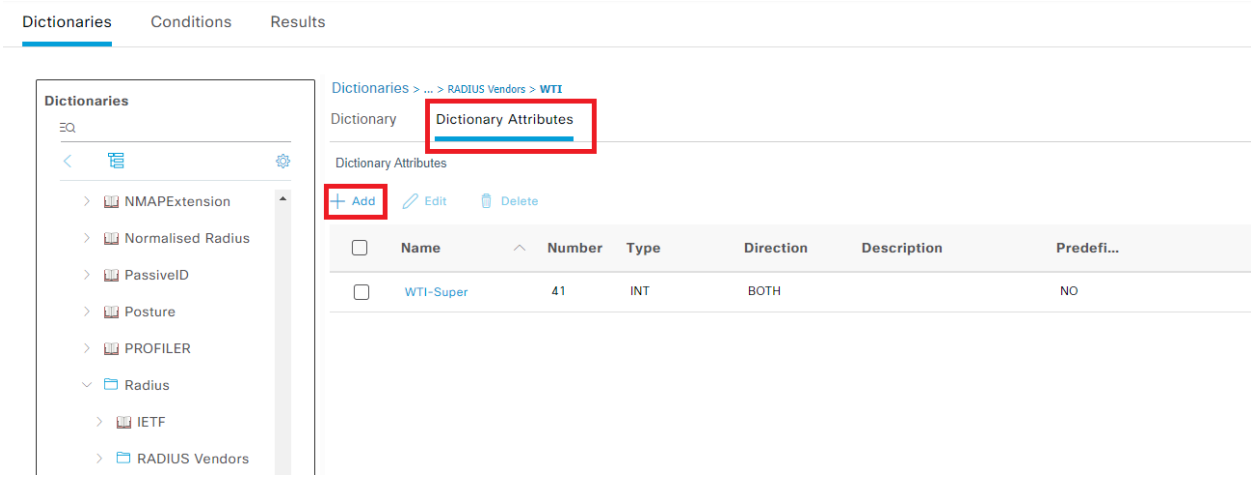




2. The name and the Vendor IDs are to be entered and saved.

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





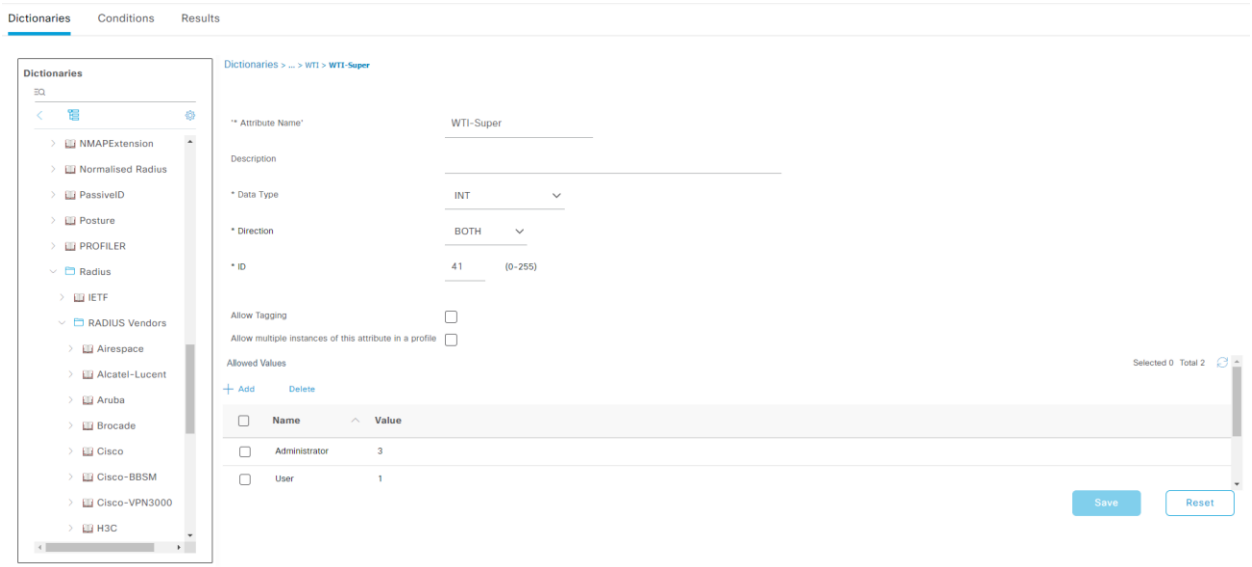
4. Click Add and fill out the Attribute Name, Data Type, Direction and ID and Add allow values for access level.

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**



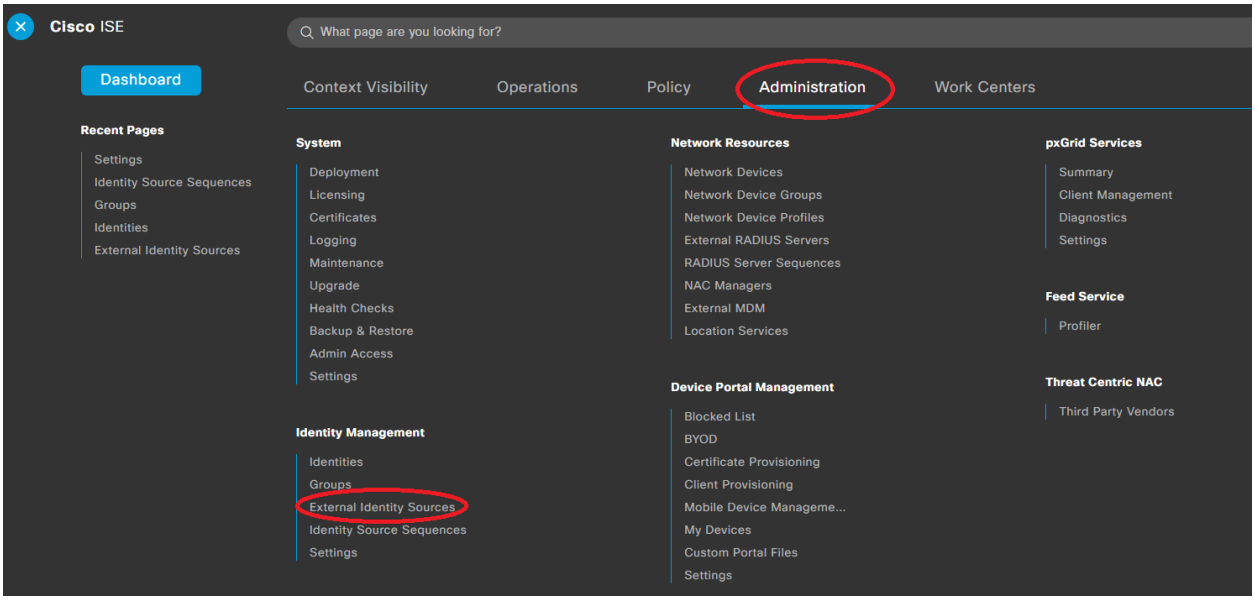
5. Save the attribute.

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

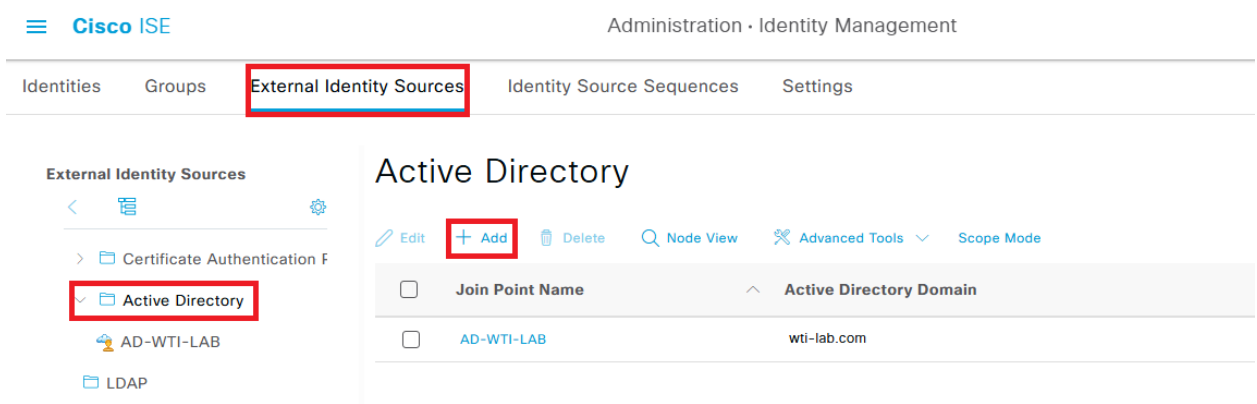
WTI RADIUS Dictionary https://ftp.wti.com/InfoCenter/rsa/dictionary/dictionary.wti

Step 2: Connect Active Directory joint point in ISE

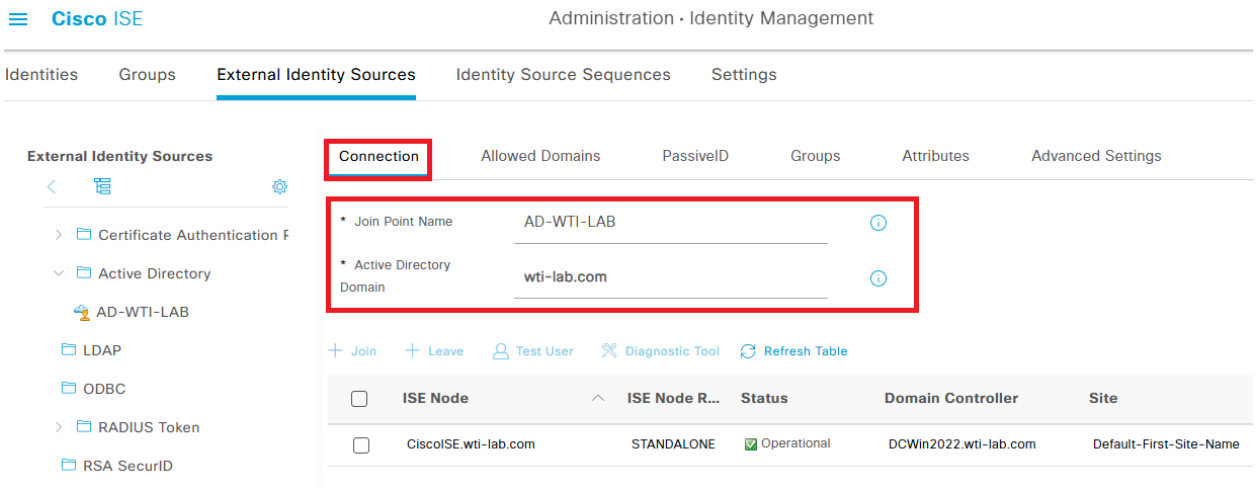
1. Navigate to **Administration** then click **Identity Management** and click **External Identity Sources**.



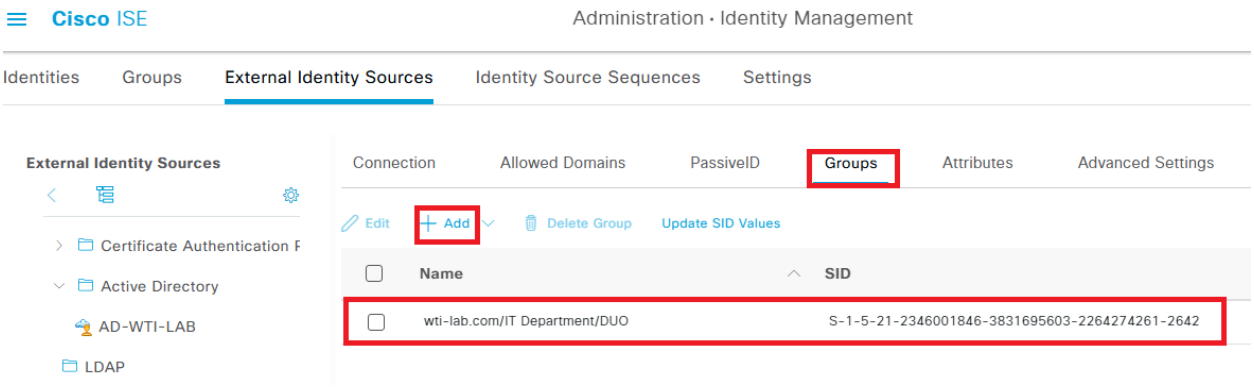
2. On **External Identity** Sources tab, Navigate to Active Directory and click **Add**



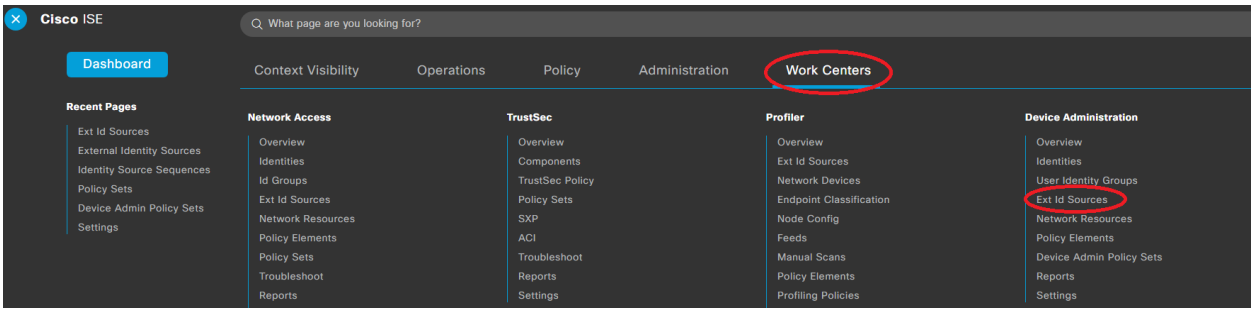
3. Under Connection section. Fill in the all requirement and click submit.



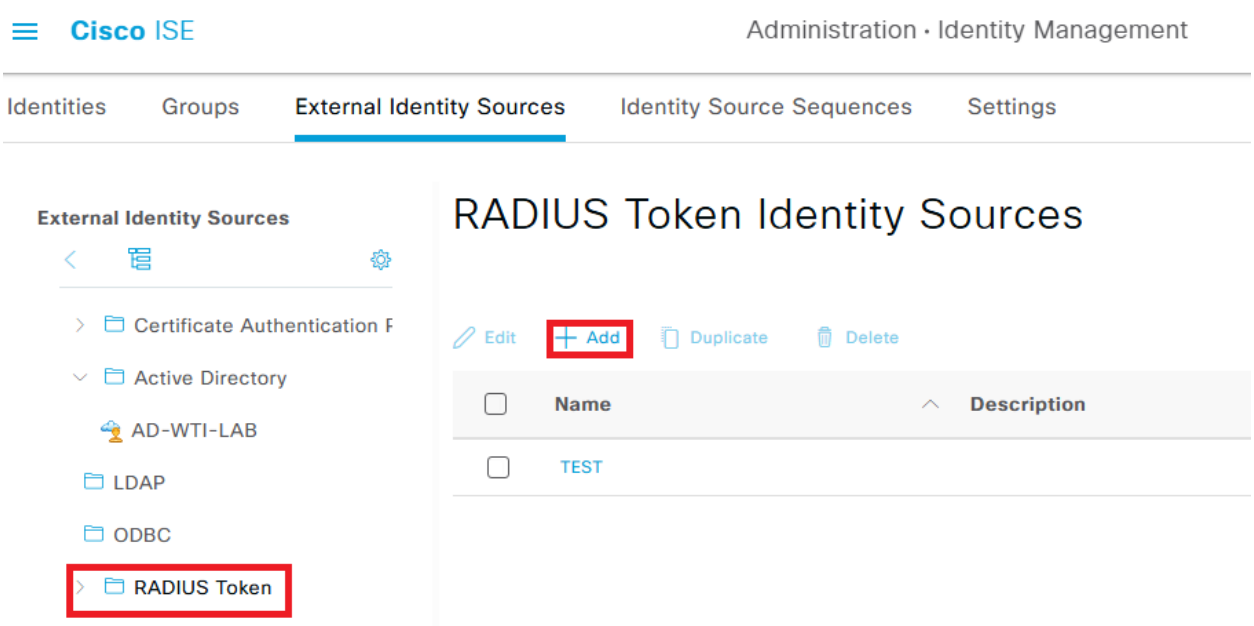
4. Navigate to **Groups** tab and click **Add** > **Select Group from Directory**.



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



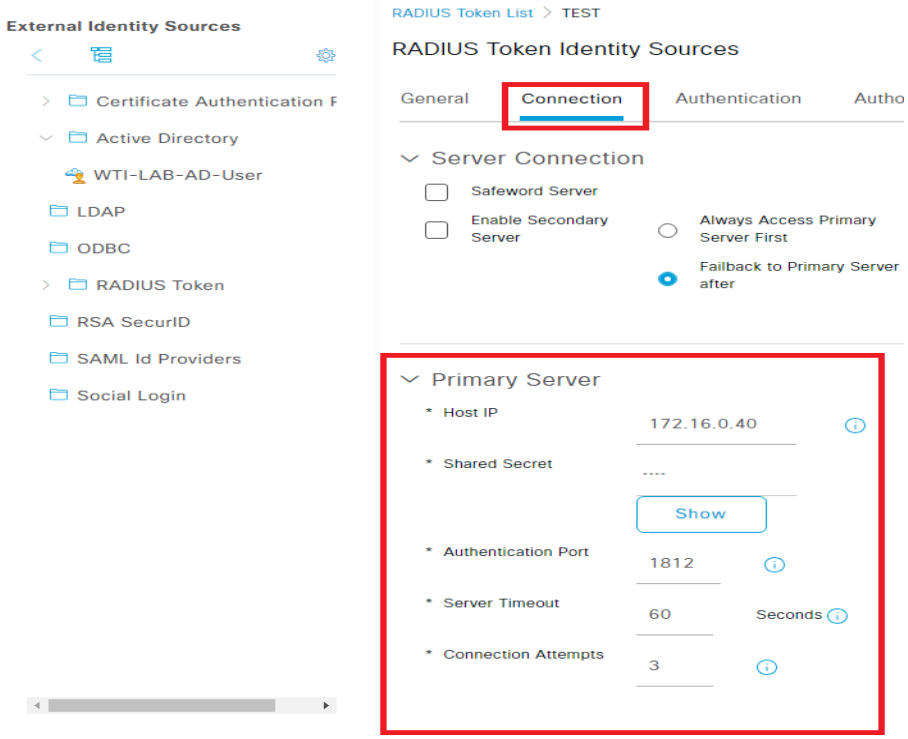
6. On RADIUS Token click **Add.**



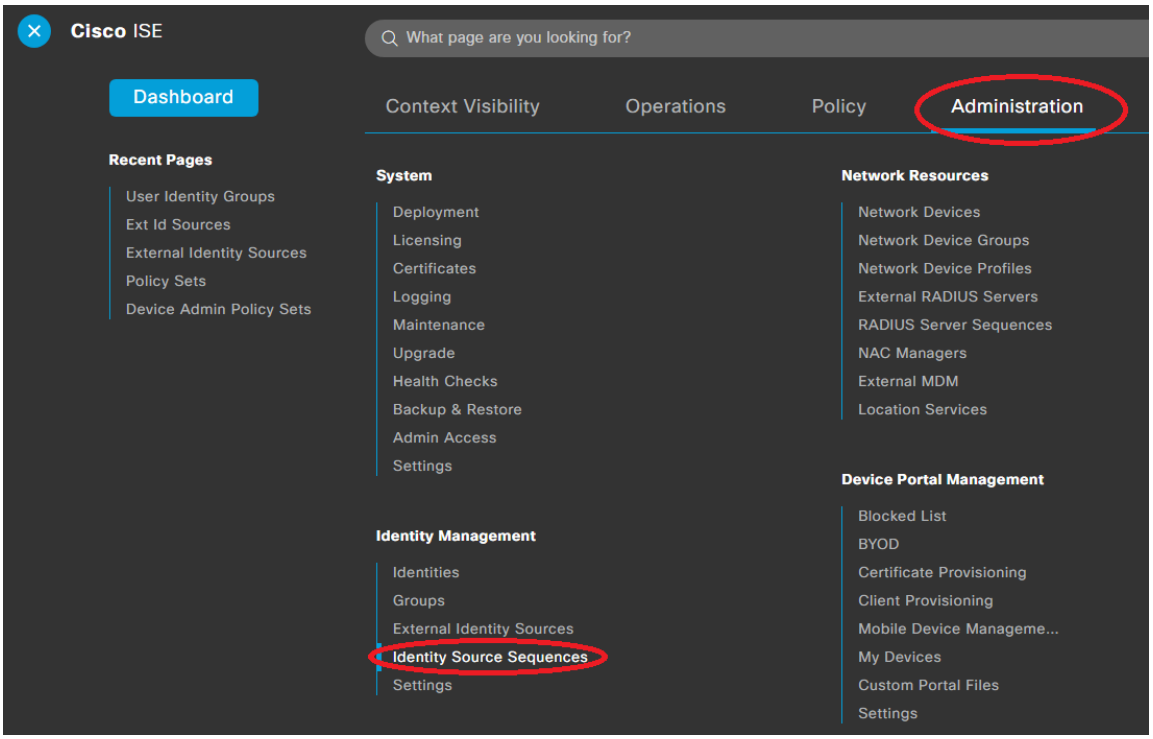
7. Starting from the left to right, configure the settings within each tab menu item as follow.

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

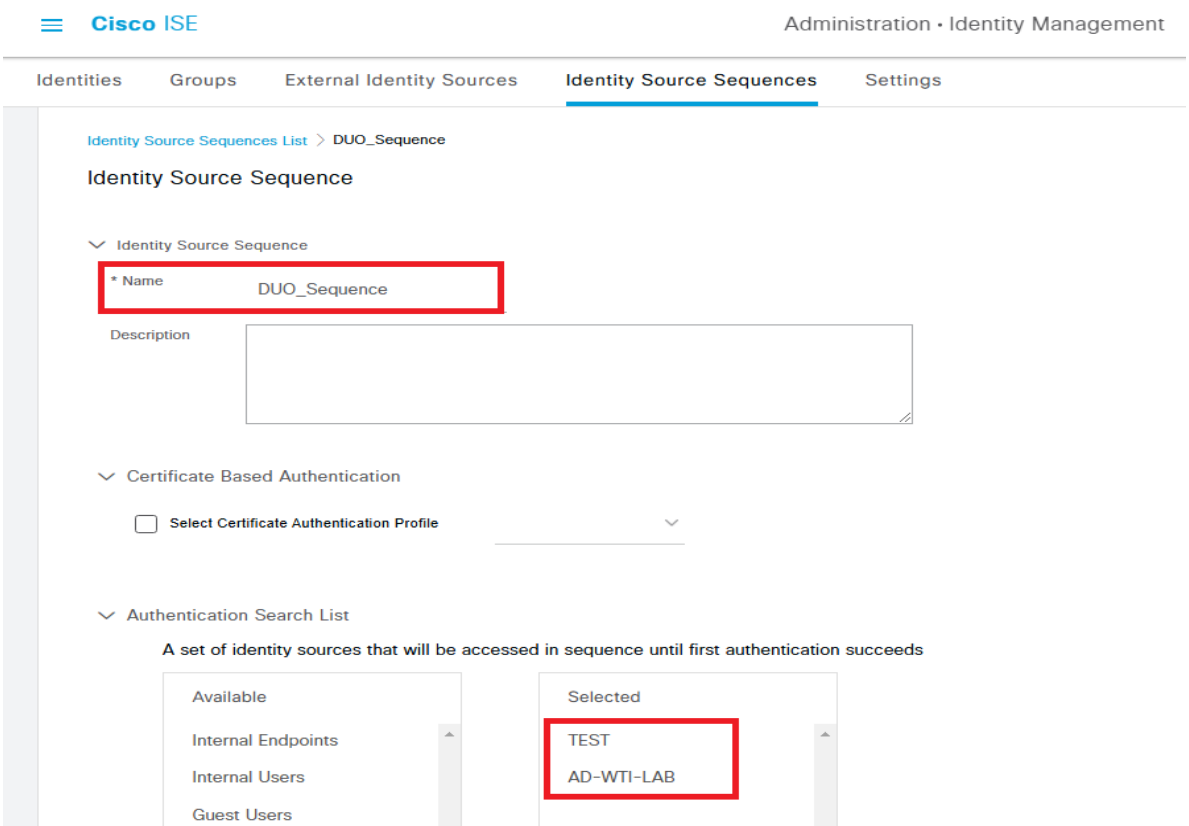
b. In Connection tab, configure the primary server details. (Primary Server is DUO Proxy Authentication Server)



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

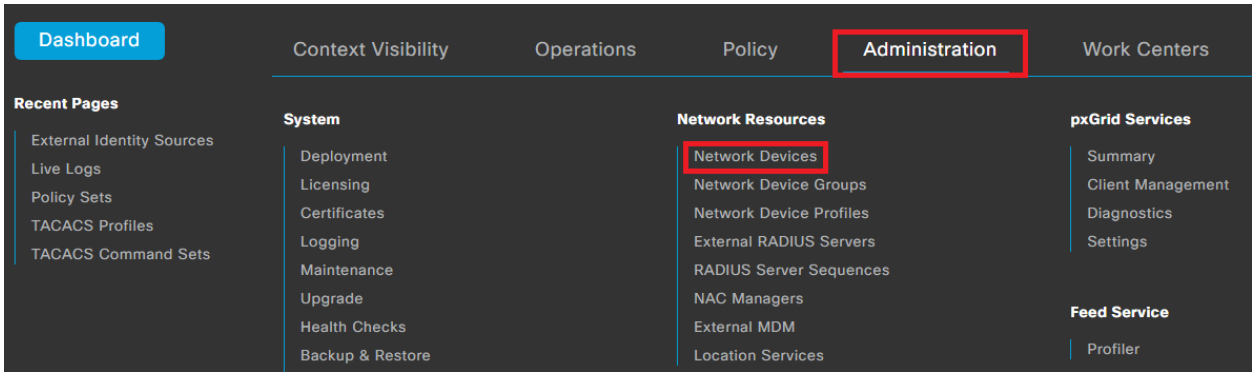


9. In Identity Sources Sequence click **Add** name identity source sequence and select authentication available search list and click Save.

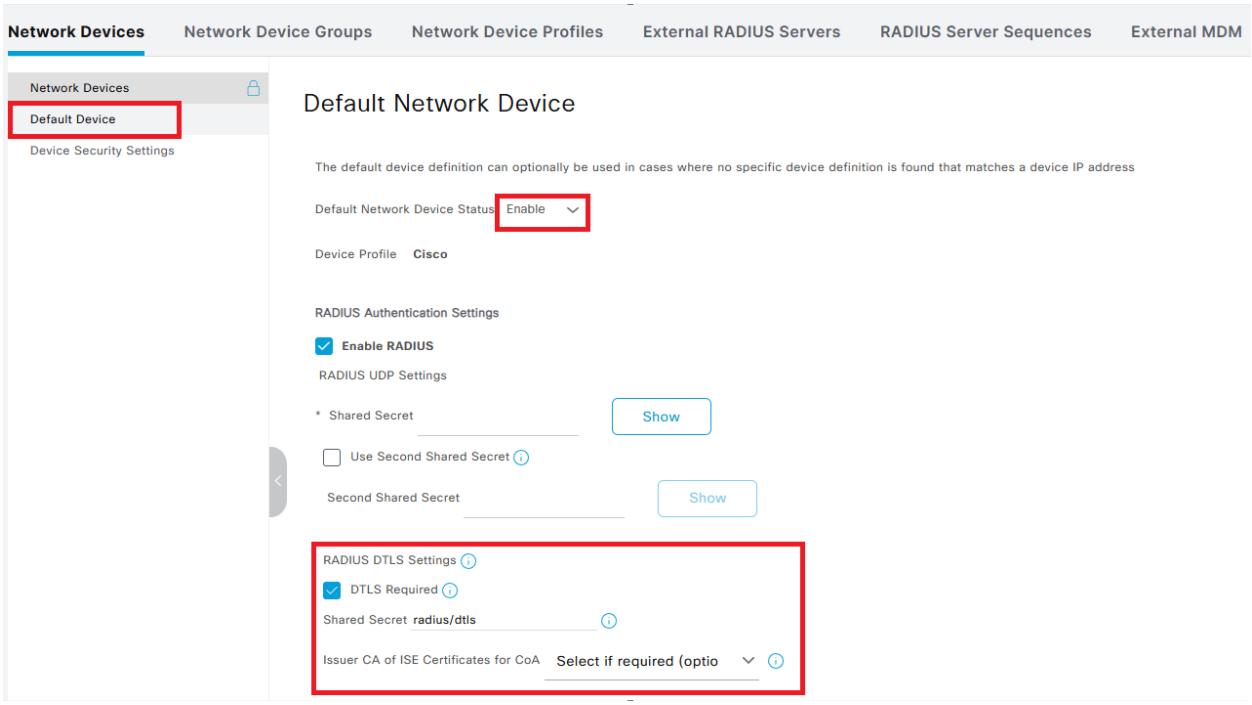


Step 3: Create Network Device

1. Navigate to **Administrator** > **Network Resource** > **Network Device**

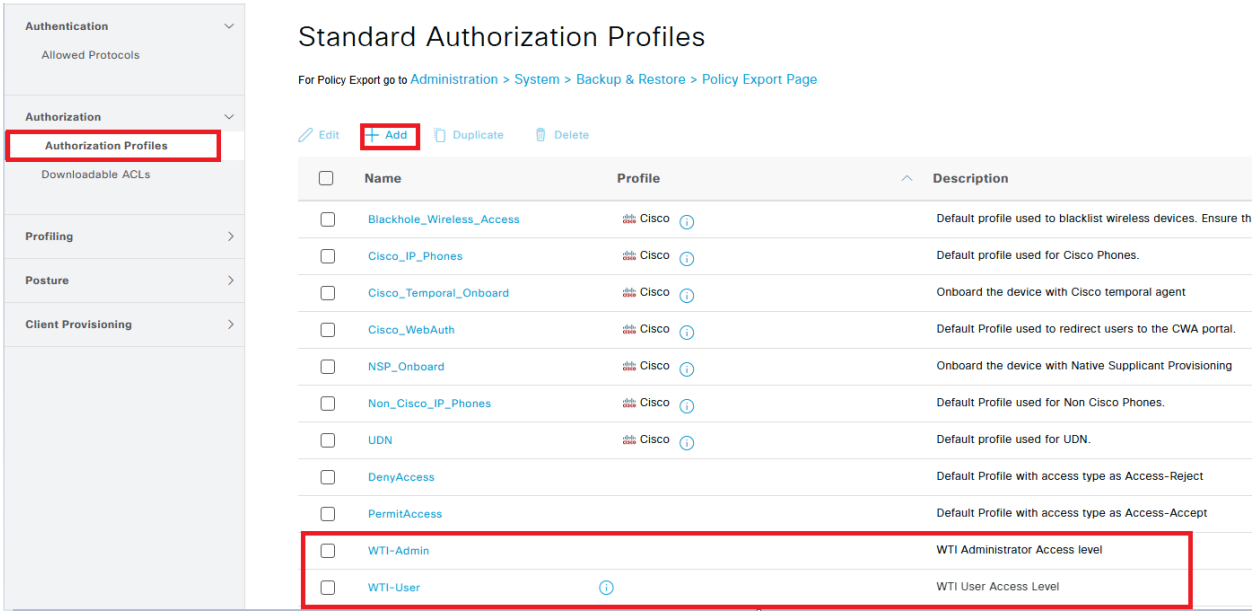


2. Enable Radius DTLS in Device Default

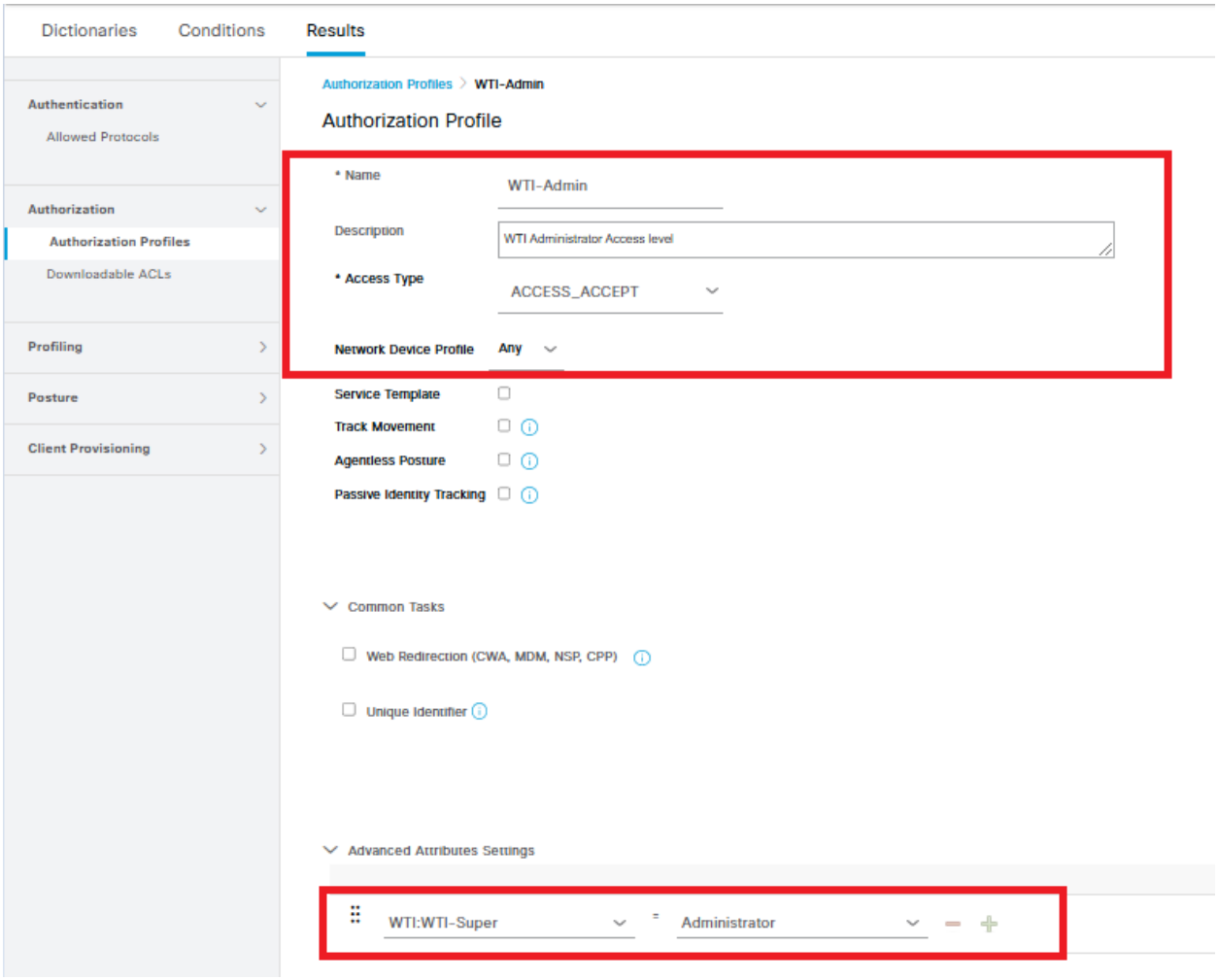


Step 4: Create Radius Authorization Profile

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

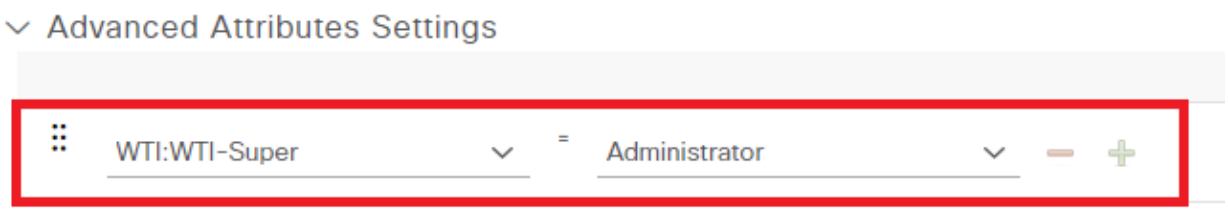


2. Create two Authorization Profile. One for WTI_Admin (Administrator access level) and another for WTI_User (User access level).

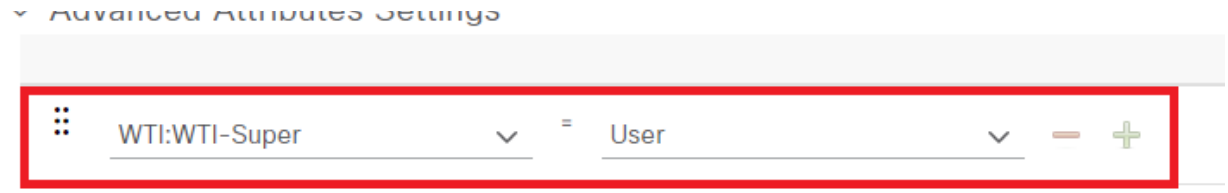


For WTI_Admin

In advanced Attribute Settings



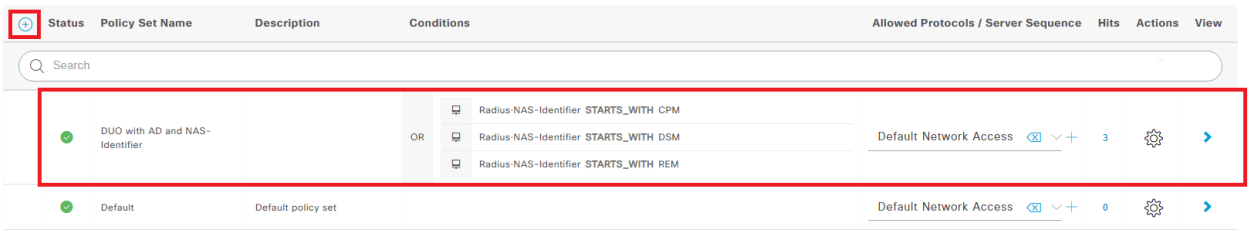






Step 5: Create Policy with NAS-Identifier

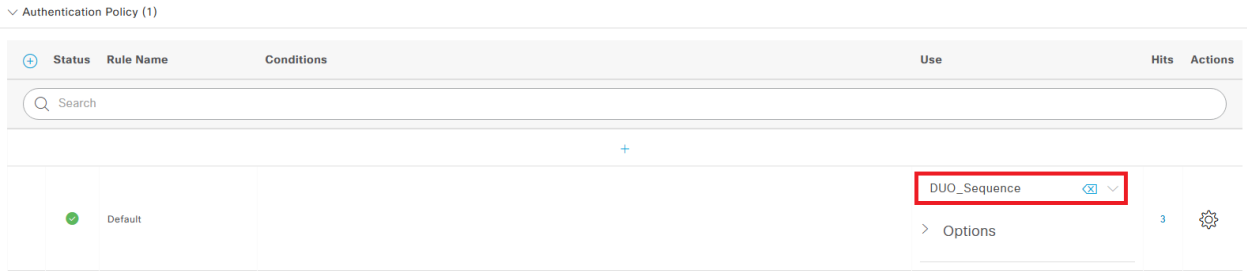
1. Navigate to **Policy > Policy Sets > click (+) to add new policy set**.



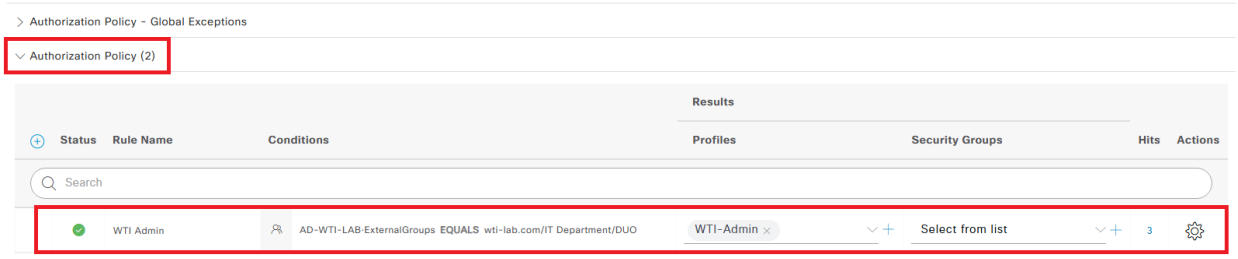
Policy Set Name: **DUO with AD and NAS-Identifier**
Condition: **Radius-NAS-Identifier START_WITH CPM** (DSM or REM)
Allowed Protocols: **Default Network Access**

2. Authentication Policy

Rule Name: Default
Use: **DUO_Sequence**



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



For WTI_Admin

Rule Name: **WTI-Admin**
Condition: **AD-WTI-LAB-ExternalGroup EQUALS wti-lab.com/IT Department/DUO**
Profile: **WTI_Admin**



For WTI_User

Rule Name: **WTI-User**
Condition: **AD-WTI-LAB-ExternalGroup EQUALS wti-lab.com/IT Department/DUO**
Profile: **WTI_User**

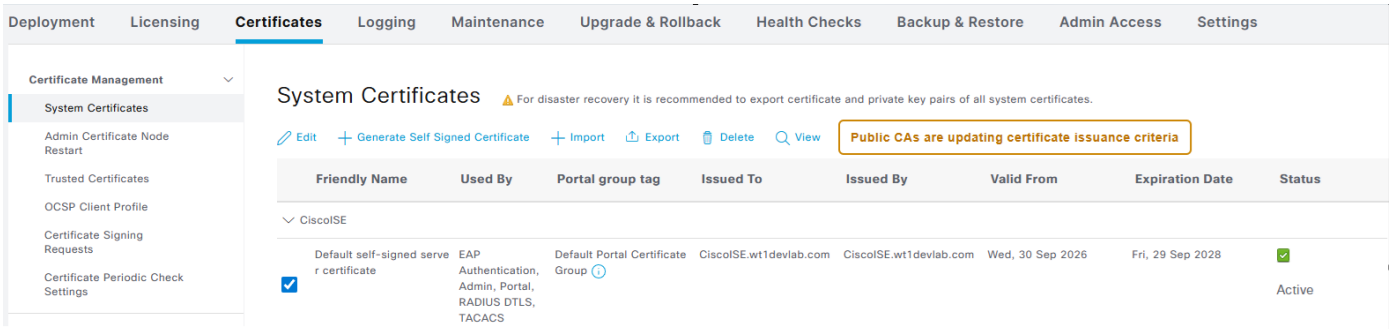


Step 6: Export System Certificate

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

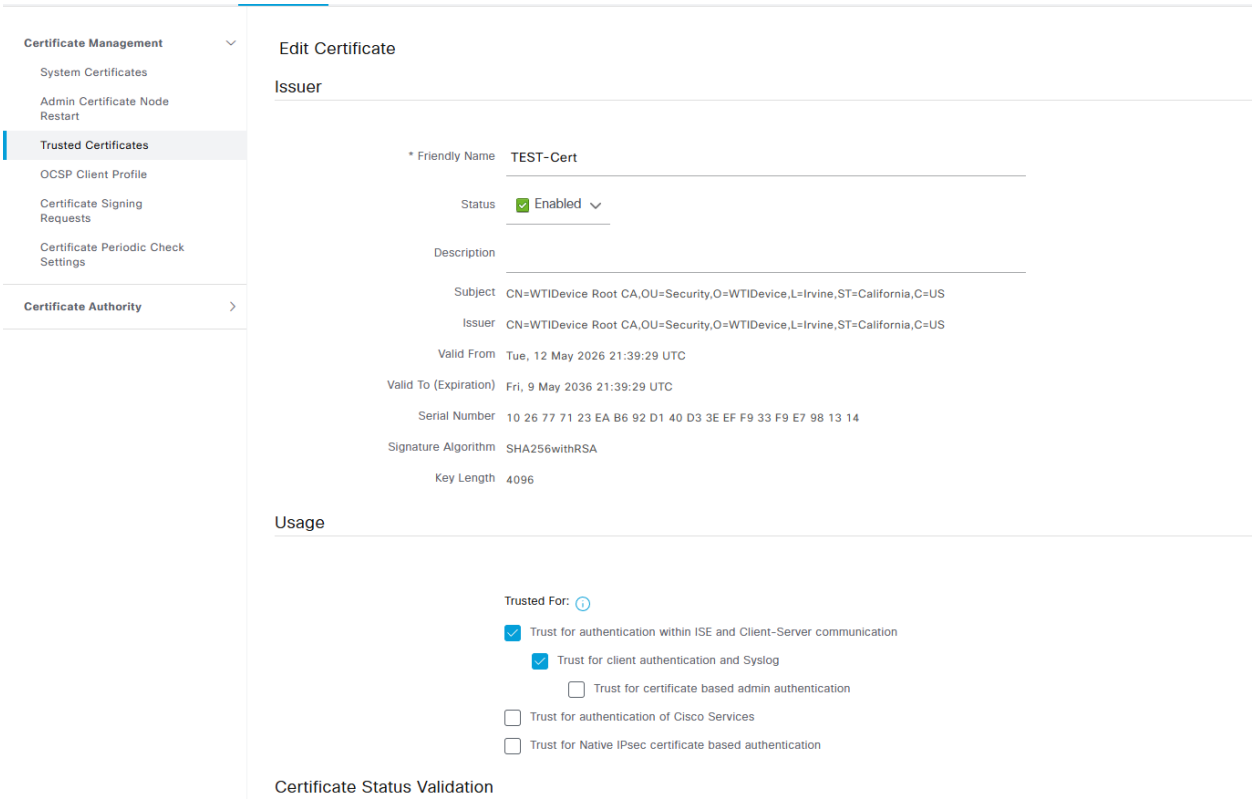
2. Go to **Administration** >> **System** >> **Certificate** >> **System Certificate**

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**.



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.**

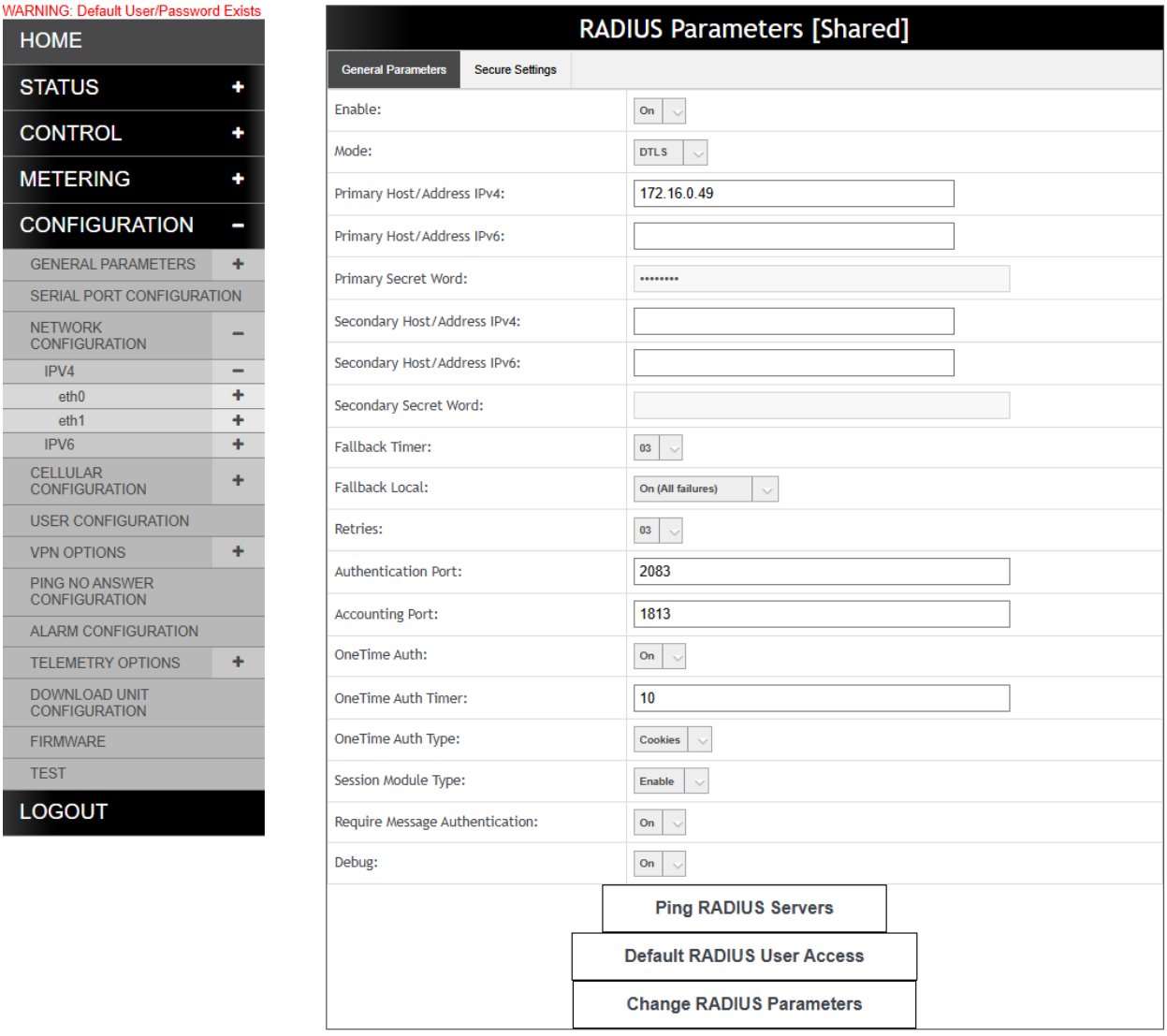


WTI Device setup and Configuration

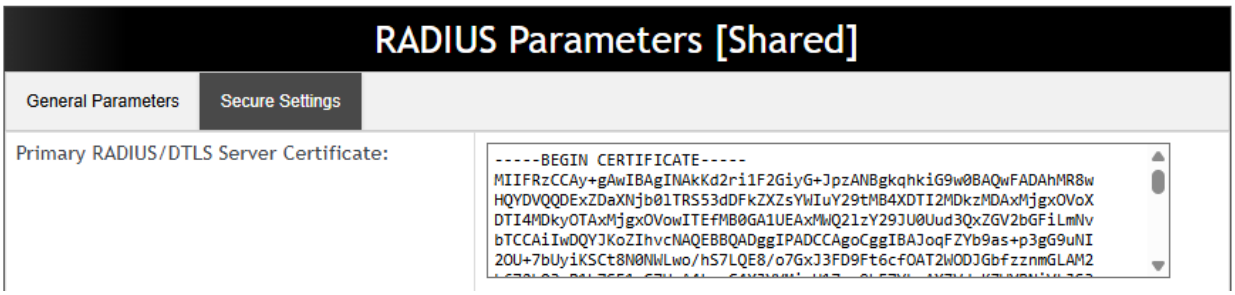
1. Import System Certificate from Cisco ISE into WTI primary RADIUS/DTLS Server Certificate.

2. Login into Web GUI >> **Configuration** >> **Network Configuration** >> **IPV4** >> **eth0** >> **RADIUS**

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



4. In **Secure Settings tab**, paste Cisco ISE system certificate that we export from step 6-3 into **Primary RADIUS/DTLS Server Certificate**



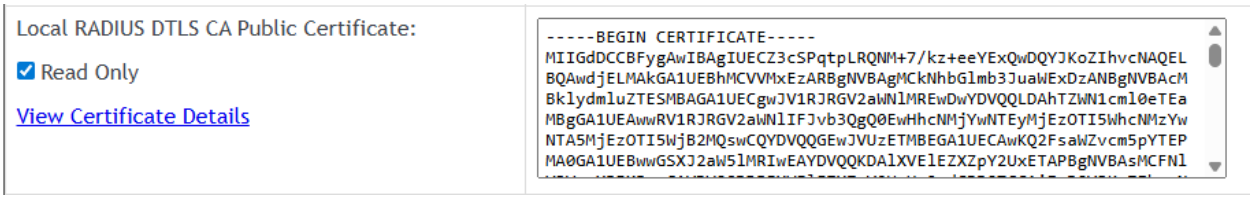
5. Fill out the requirement associate to your network environment.

Common Name:	172.16.0.44
State or Province:	California
Locality:	Irvine
Country Code:	US
Organization (O):	Organization Name
Organizational Unit (OU):	Organization Unit Nam

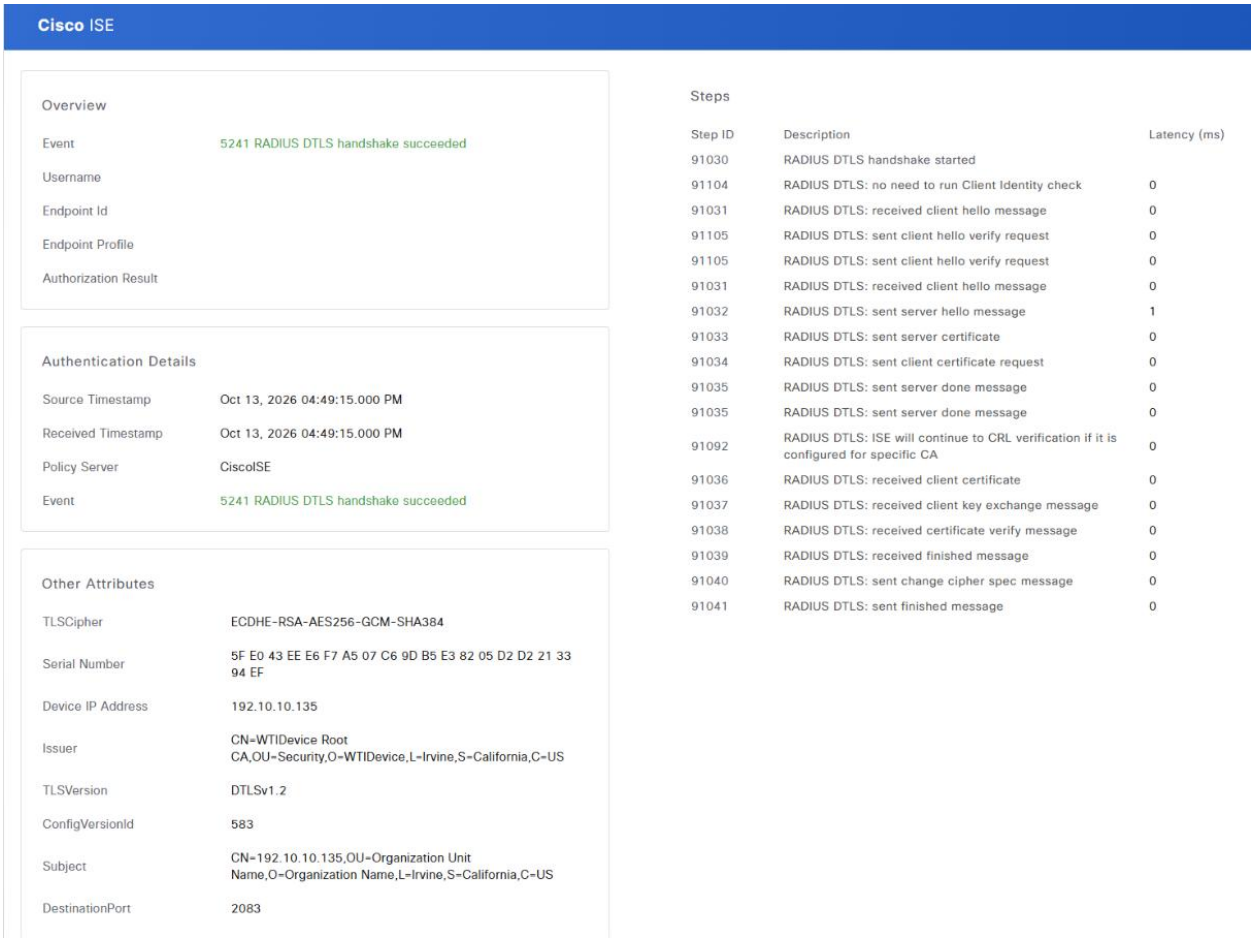
click on Re-Create Client Certificate and click Change RADIUS Parameters.

Re-Create Client Certificates	☑ Re-Create Client Certificates

6. Copy and paste **Local RADIUS DTLS CA Public Certificate** into notepad and import it into Cisco ISE trusted certificate as mentioned in Step 6-4. Done



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
```