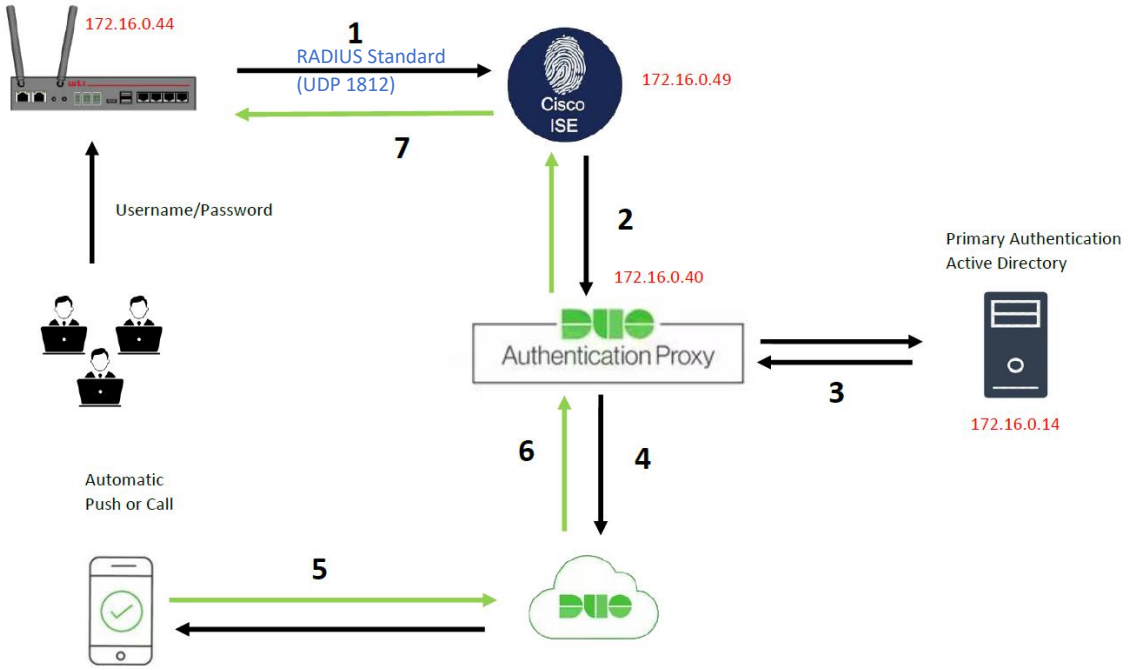
# Cisco ISE + Duo MFA + Windows AD Integration for WTI (Standard RADIUS)




## 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

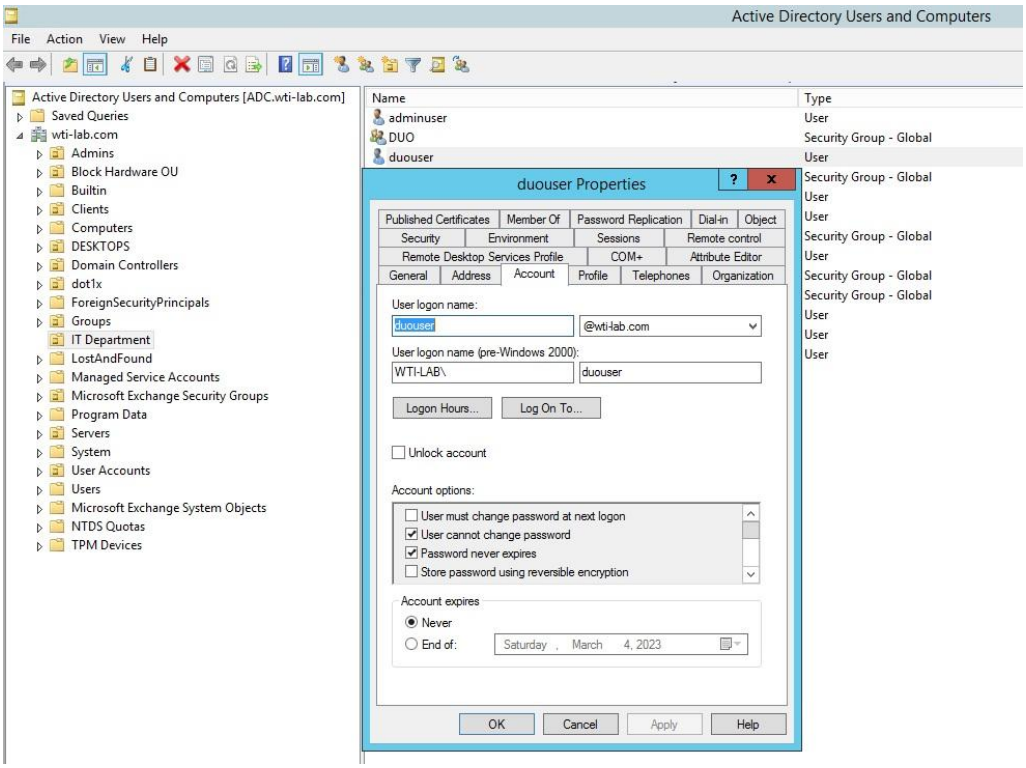
- Windows Active Directory
- Duo
- Duo Authentication Proxy Manager
- Cisco ISE
- WTI Radius client

## 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

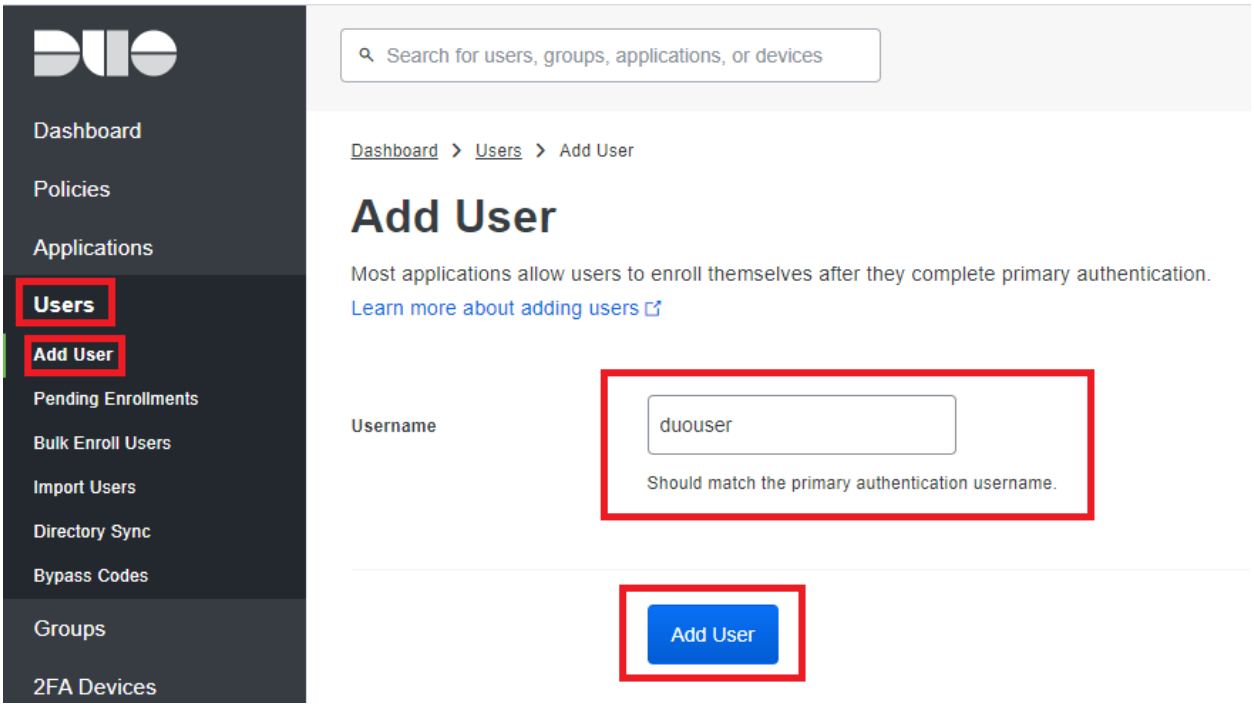
1. Navigate to Active Directory Users and Computers > Add new User and Password. In this example we created **duouser** account in active directory users and computers.




## Duo configuration

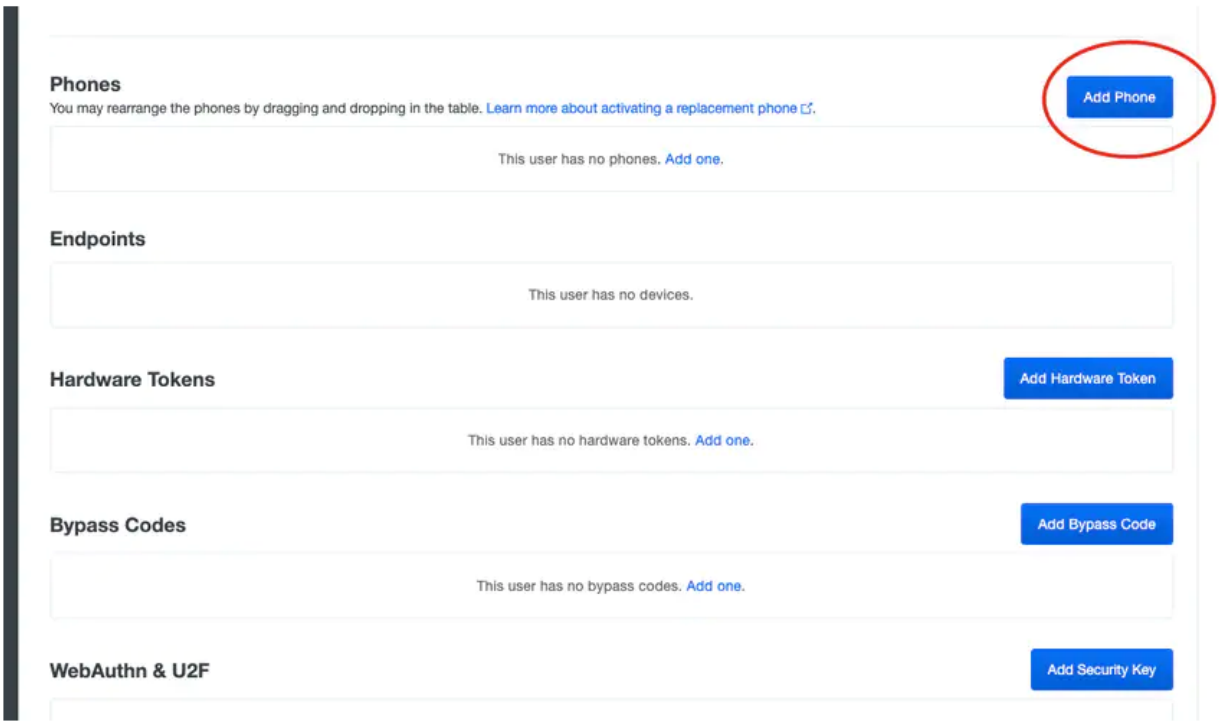
1. Log in into your Duo Admin portal

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.

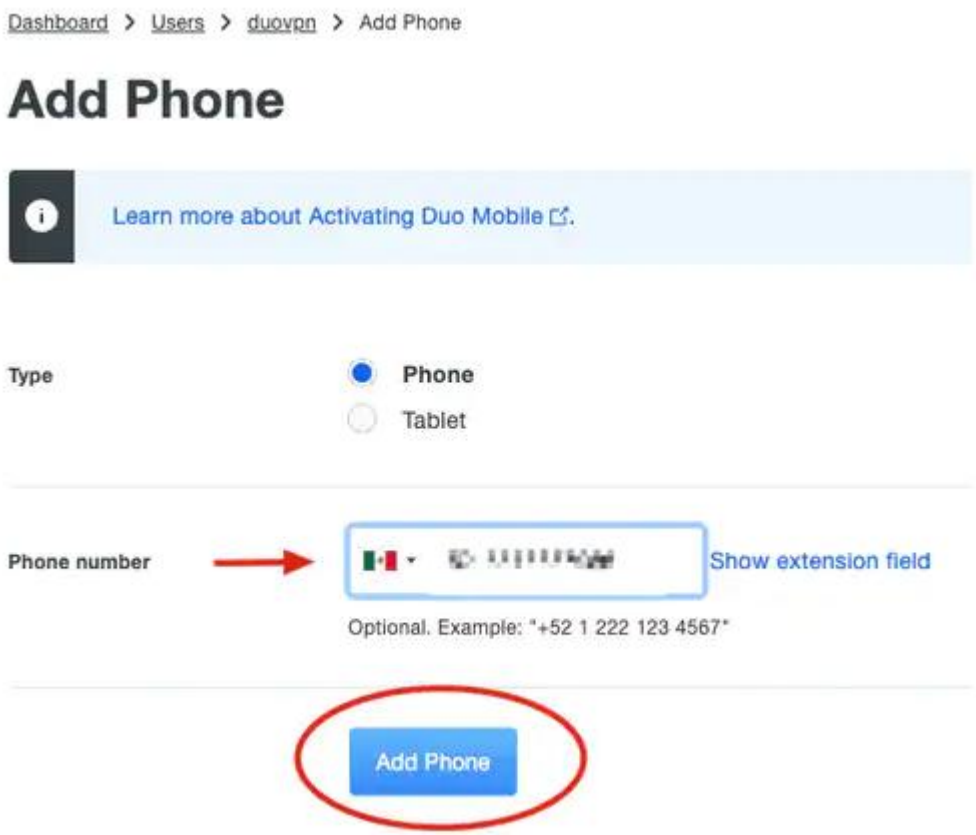



3. On the new user's panel, fill in the blank all the necessary information.

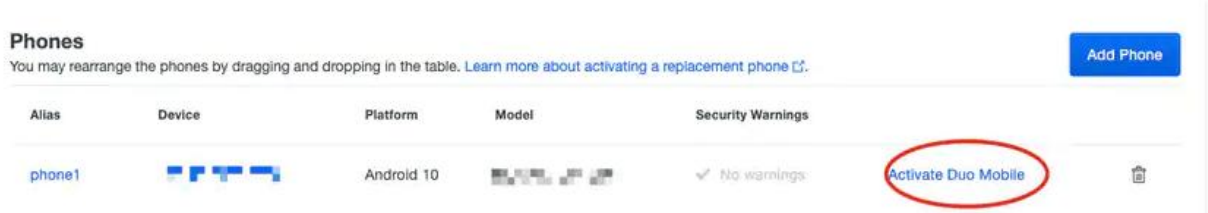
4. Under user devices specify the secondary authentication method. Click **Add Phone**



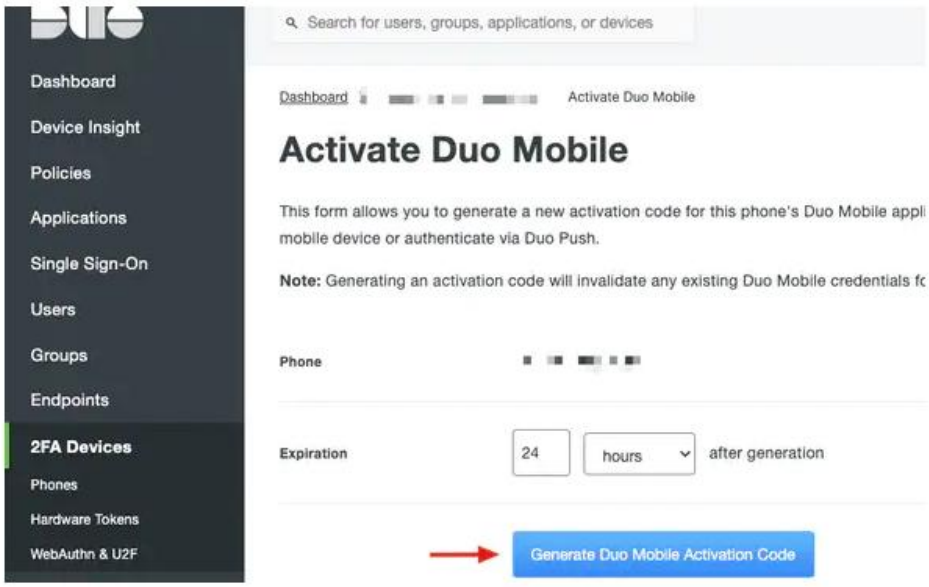
5. Type in the user's phone number and click **Add Phone**



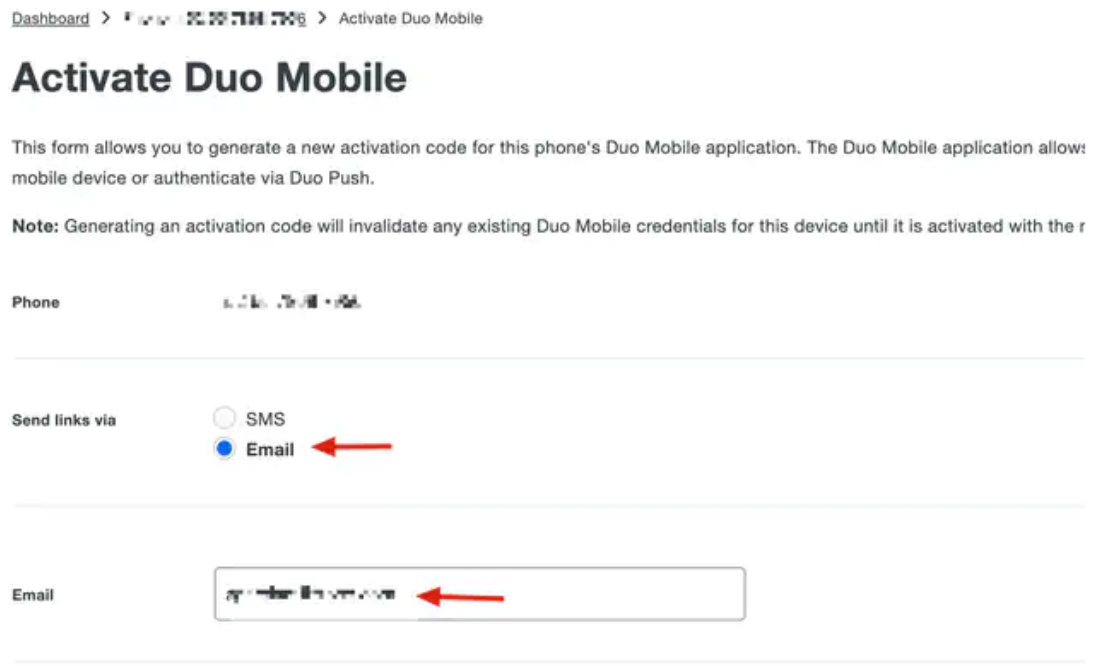

6. Navigate to **Phones** section and click **Activate Due Mobile**.



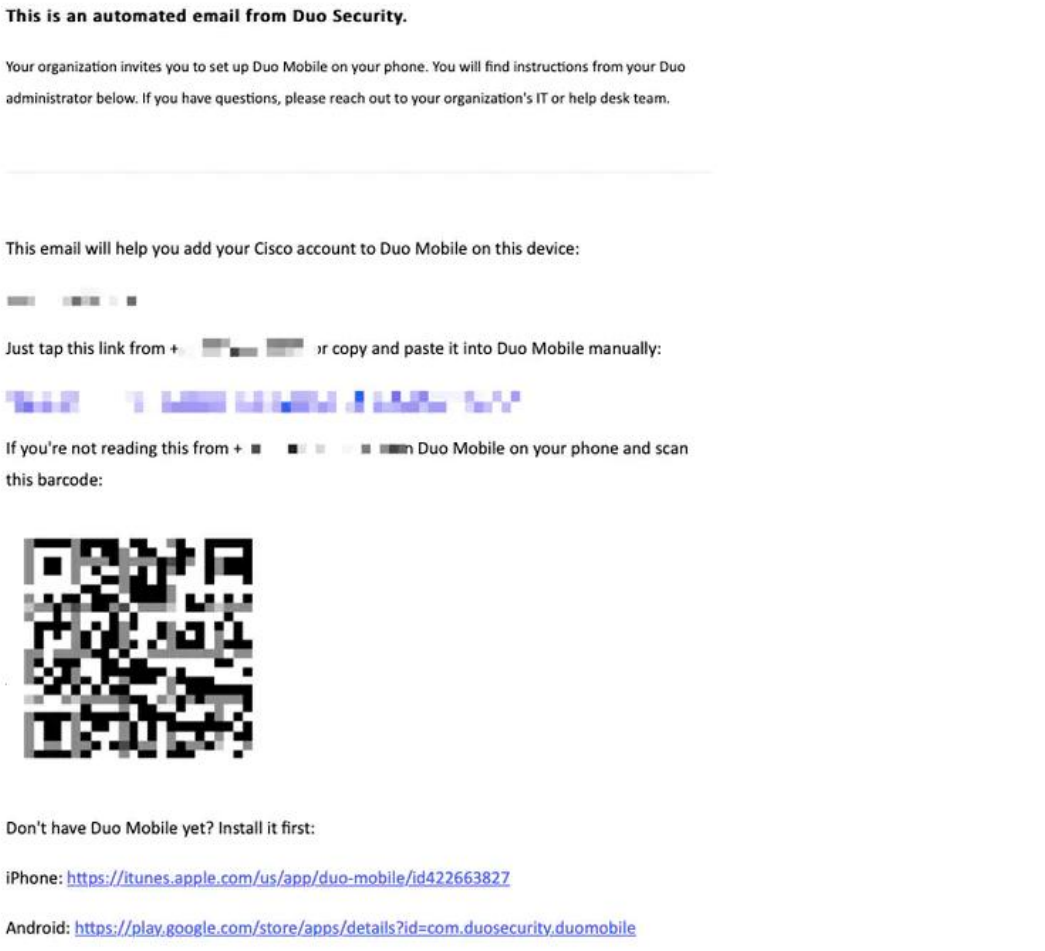

7. Click **Generate Duo Mobile Activation Code.**



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



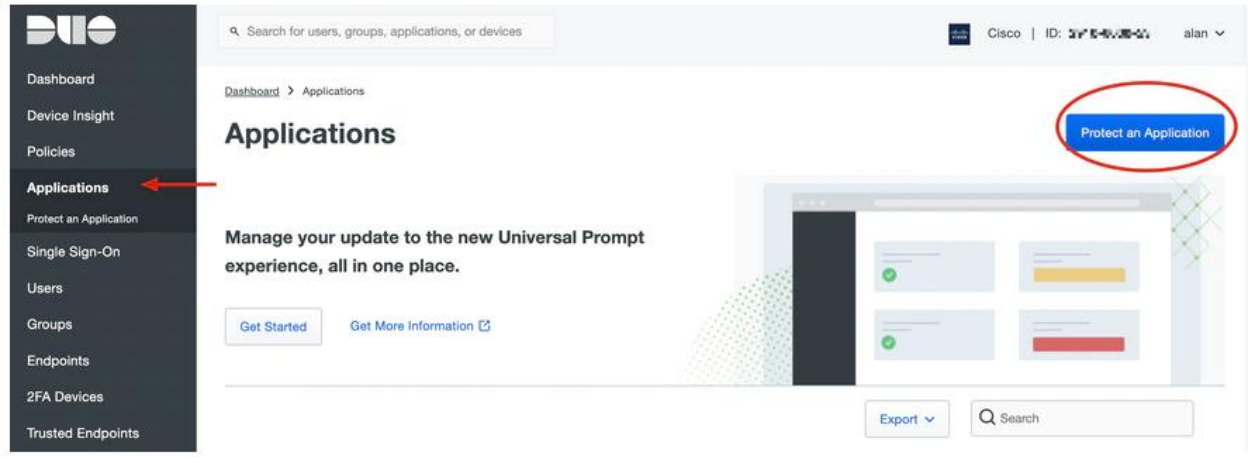
10. Open the Duo Mobile App from your mobile device and click **Add** then select **Use QR code** and scan the code from the instructions email.

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

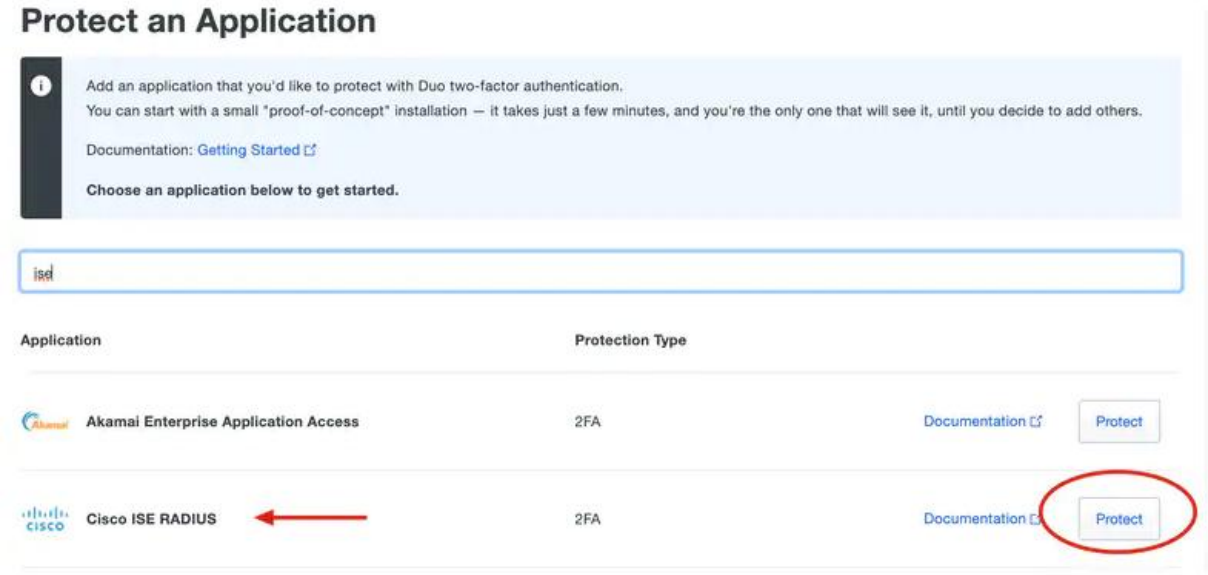
## Duo Authentication Proxy Configuration

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.

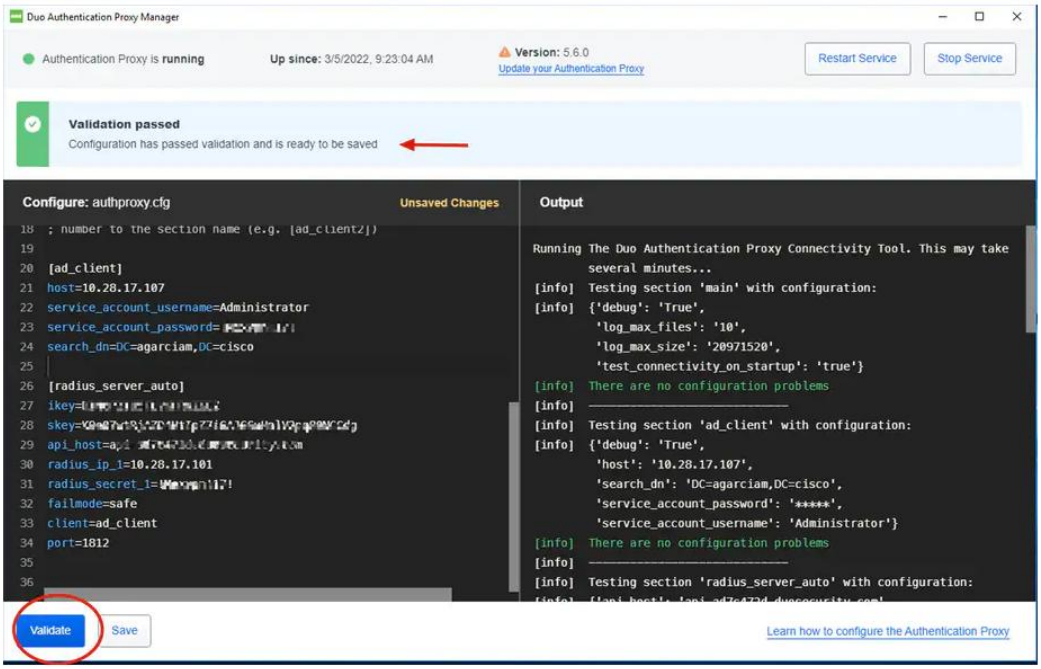



5. Run the Duo Authentication Proxy manager application and complete the configuration for both Active Directory client ISE Radius server and click Validate.

**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**

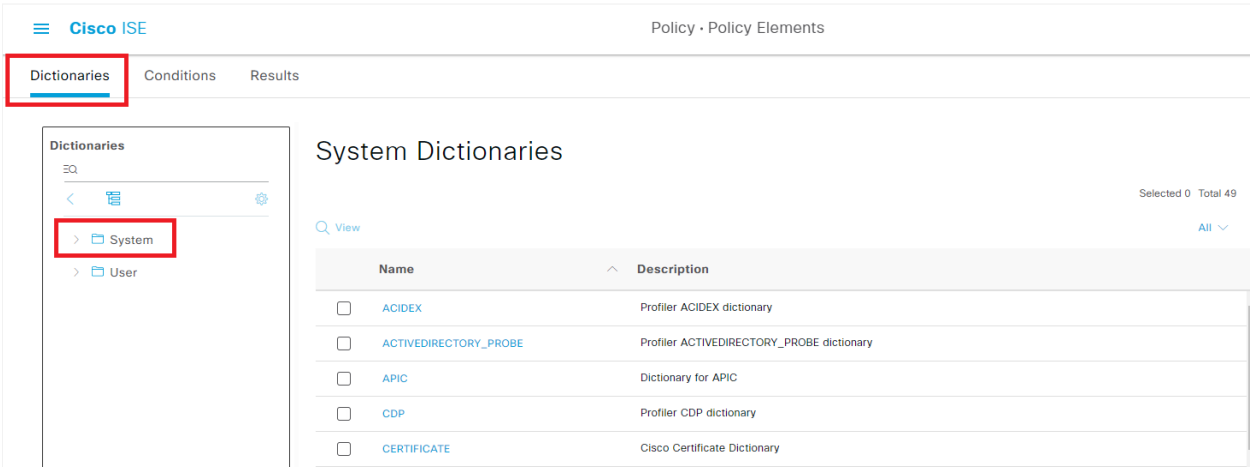
```
[ad_client]
host=172.16.0.14
service_account_username=duouser
service_account_password=duosecret
search_dn=DC=wti-lab,DC=com
security_group_dn=CN=DUO,OU=IT Department,DC=wti-lab,DC=com

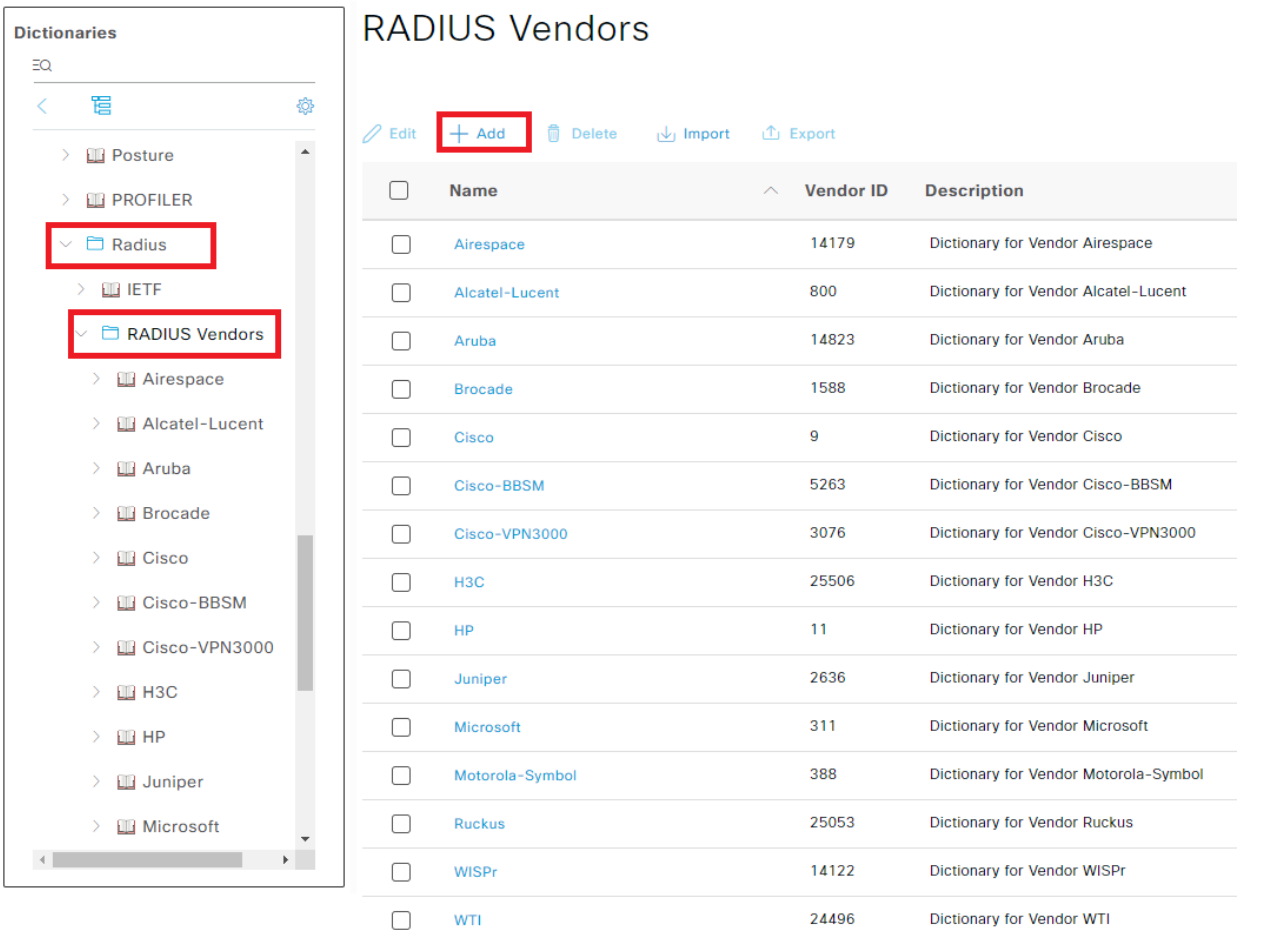
[radius_server_auto]
ikey=XXXXXXXXXXXXXXXXX
skey=YYYYYYYYYYYYYYYYY
api_host=api-123456789.duosecurity.com
radius_ip_1=172.16.0.49
radius_secret_1=test123
client=ad_client
port=1812
```

## Cisco ISE Configurations

### Step 1: Create vendor-specific attribute

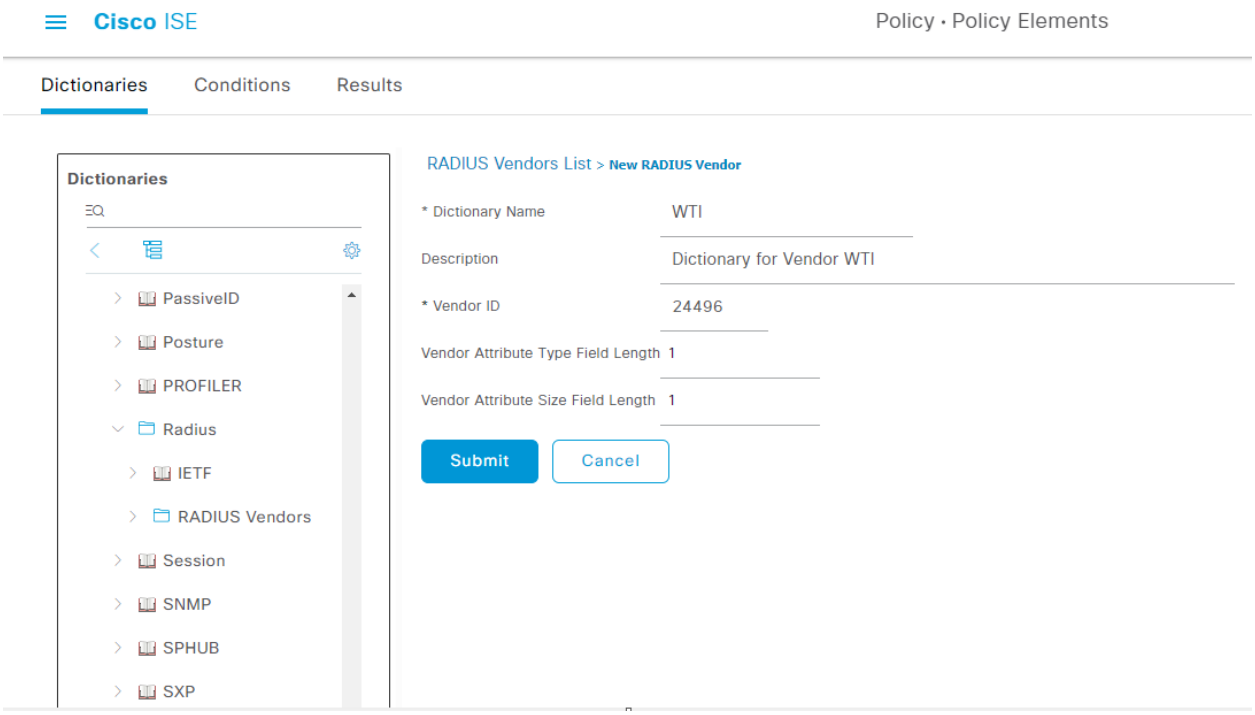
1. Navigate to **Policy > Policy Element > Dictionaries > System > Radius > Radius Vendors > Add**

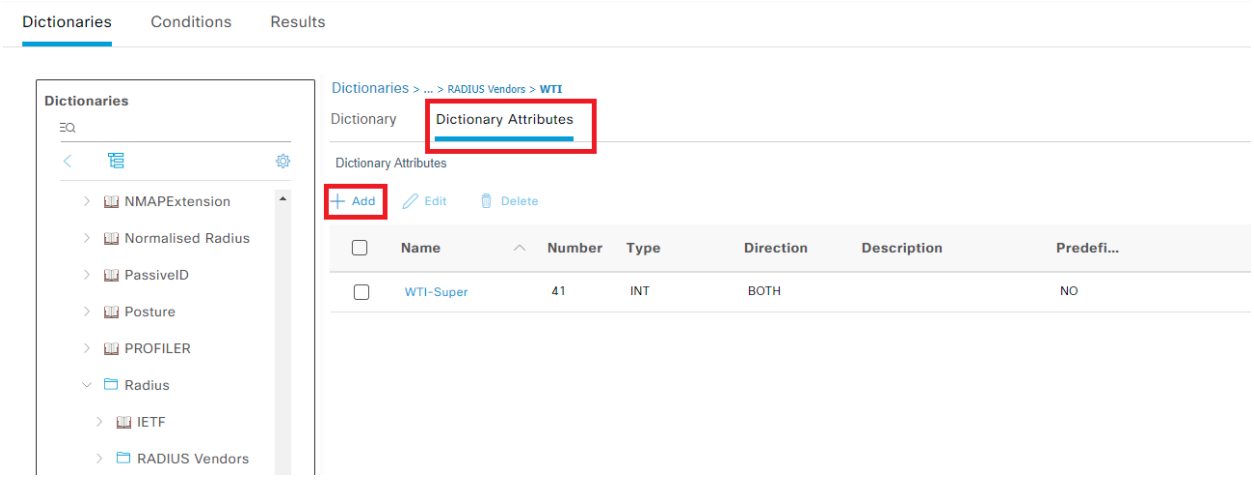





2. The name and the Vendor IDs are to be entered and saved.

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





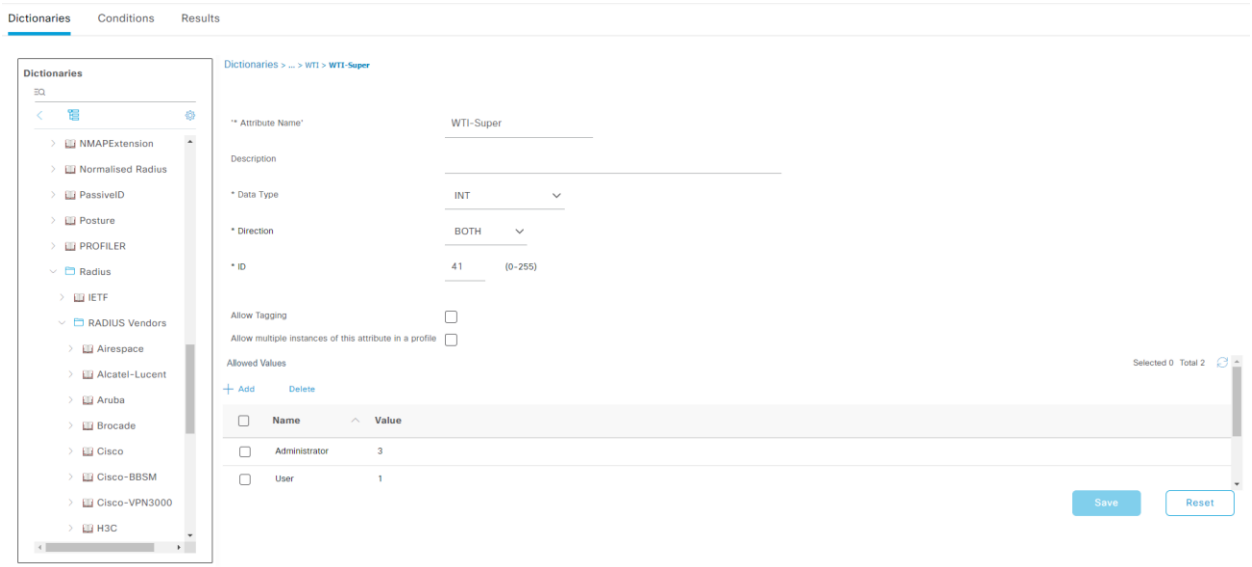

4. Click Add and fill out the Attribute Name, Data Type, Direction and ID and Add allow values for access level.

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**



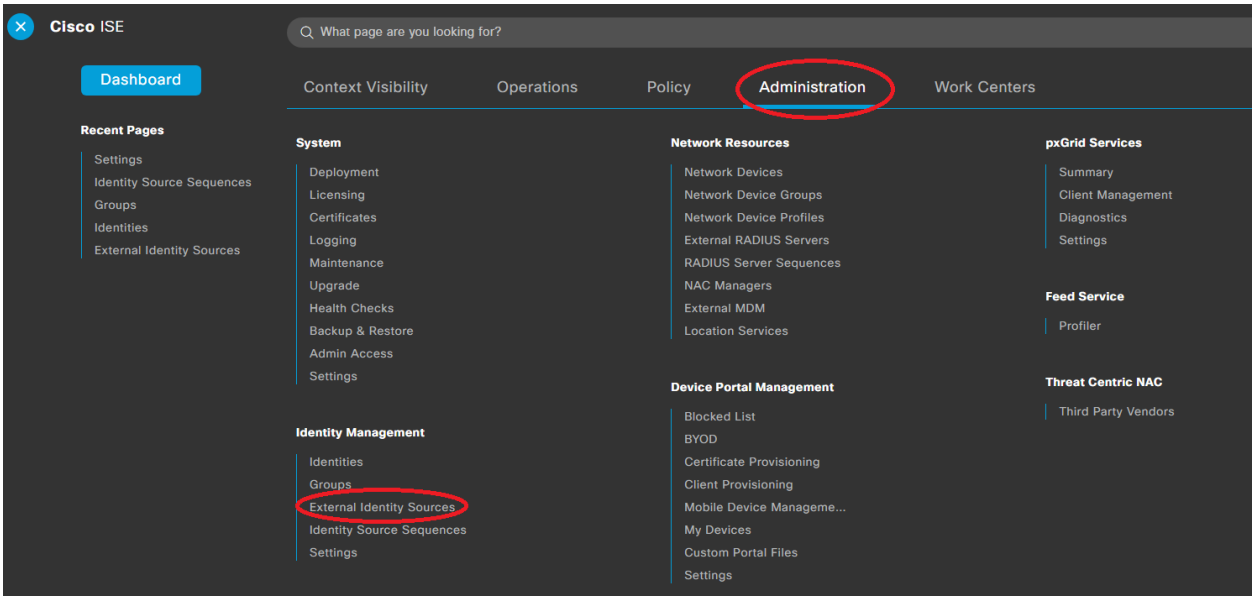
5. Save the attribute.

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

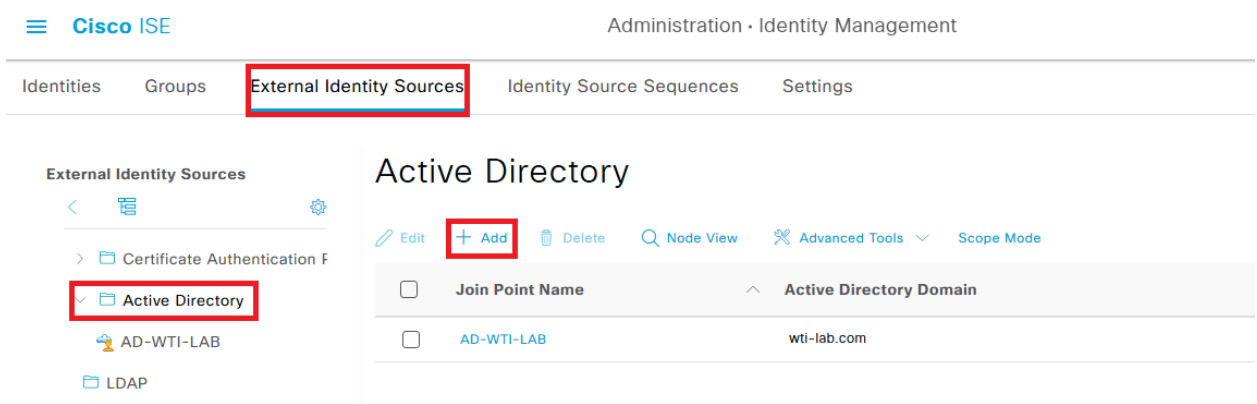
WTI RADIUS Dictionary https://ftp.wti.com/InfoCenter/rsa/dictionary/dictionary.wti

**Step 2: Connect Active Directory joint point in ISE**

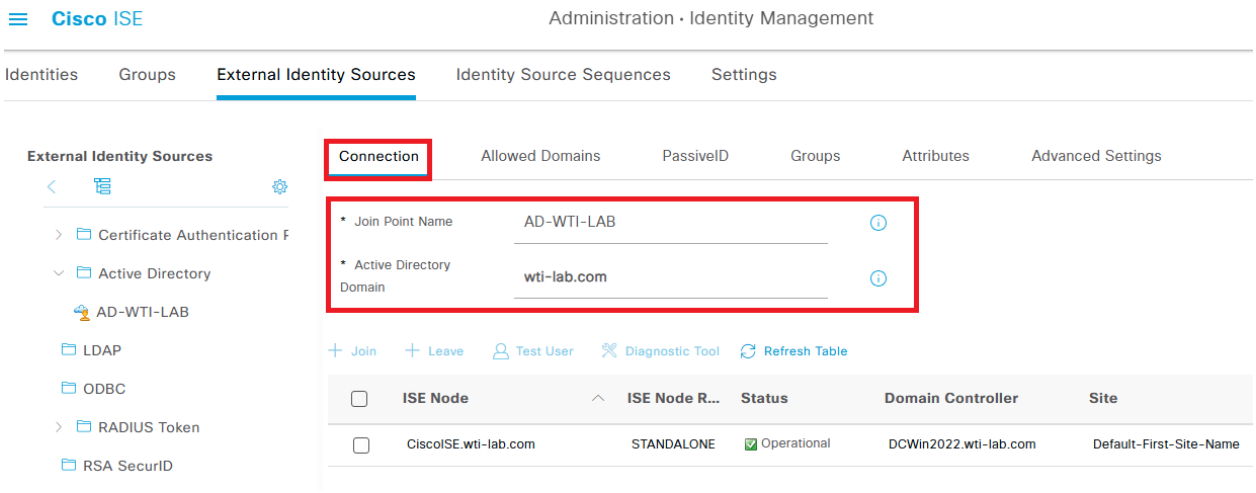
1. Navigate to **Administration** then click **Identity Management** and click **External Identity Sources**.



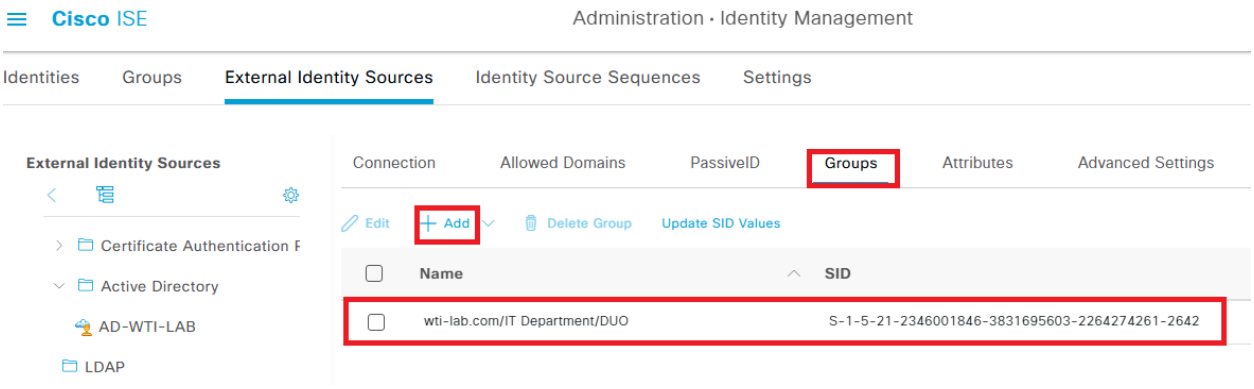

2. On **External Identity** Sources tab, Navigate to Active Directory and click **Add**



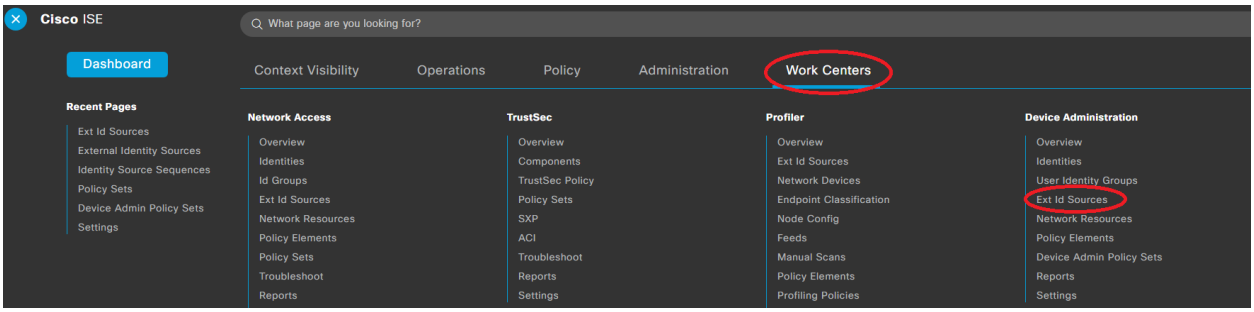
3. Under Connection section. Fill in the all requirement and click submit.



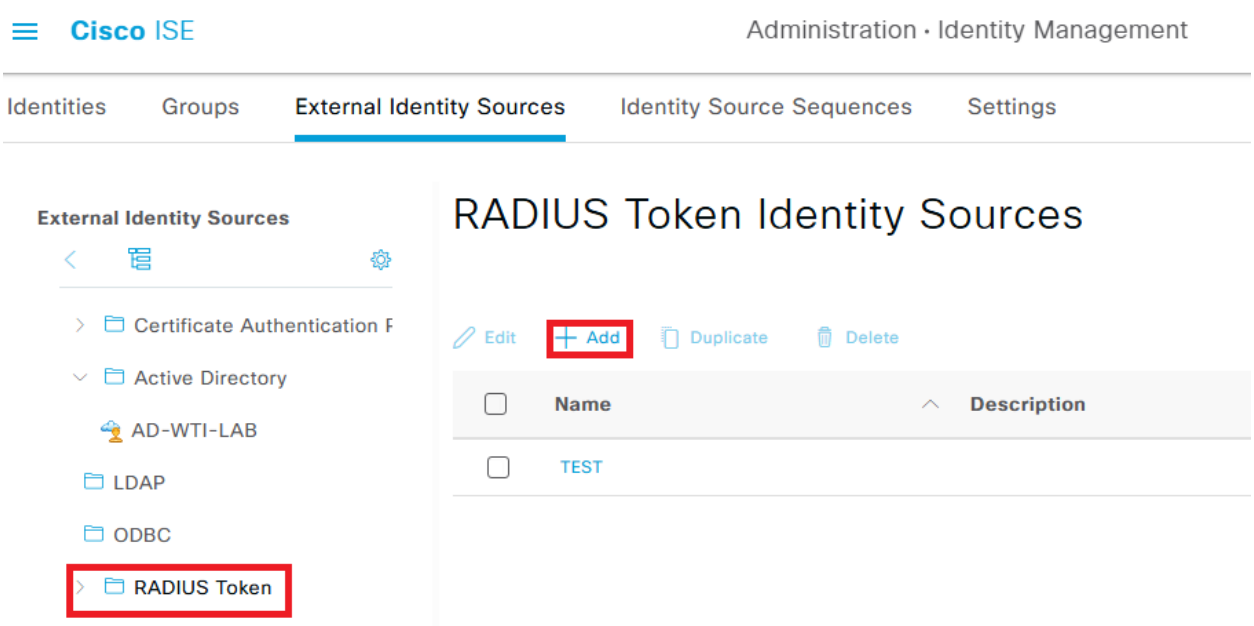

4. Navigate to **Groups** tab and click **Add** > **Select Group from Directory**.




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



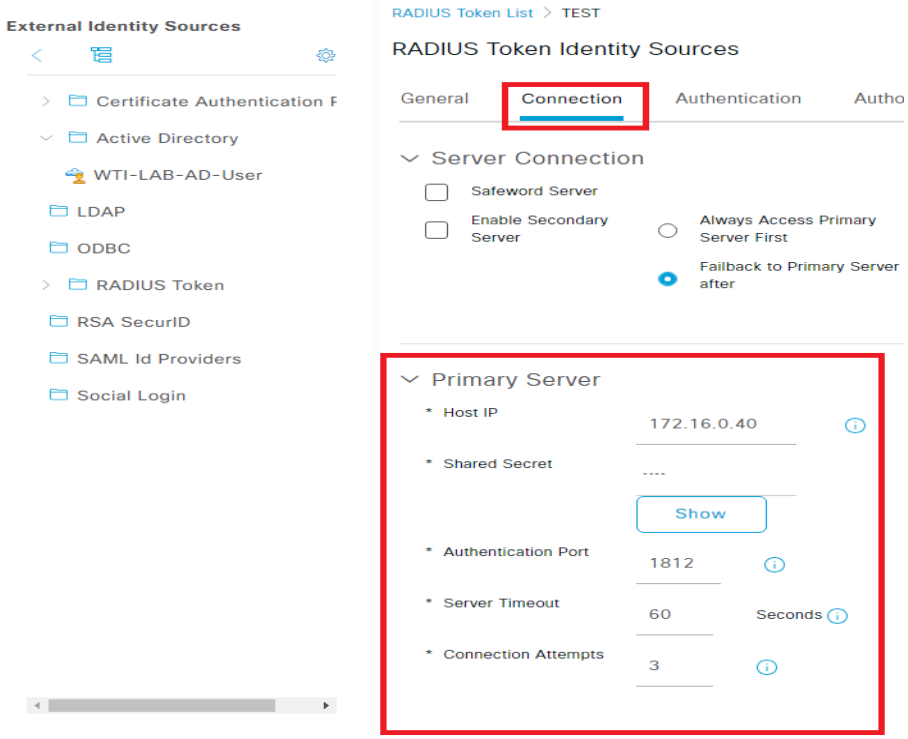
6. On RADIUS Token click **Add.**



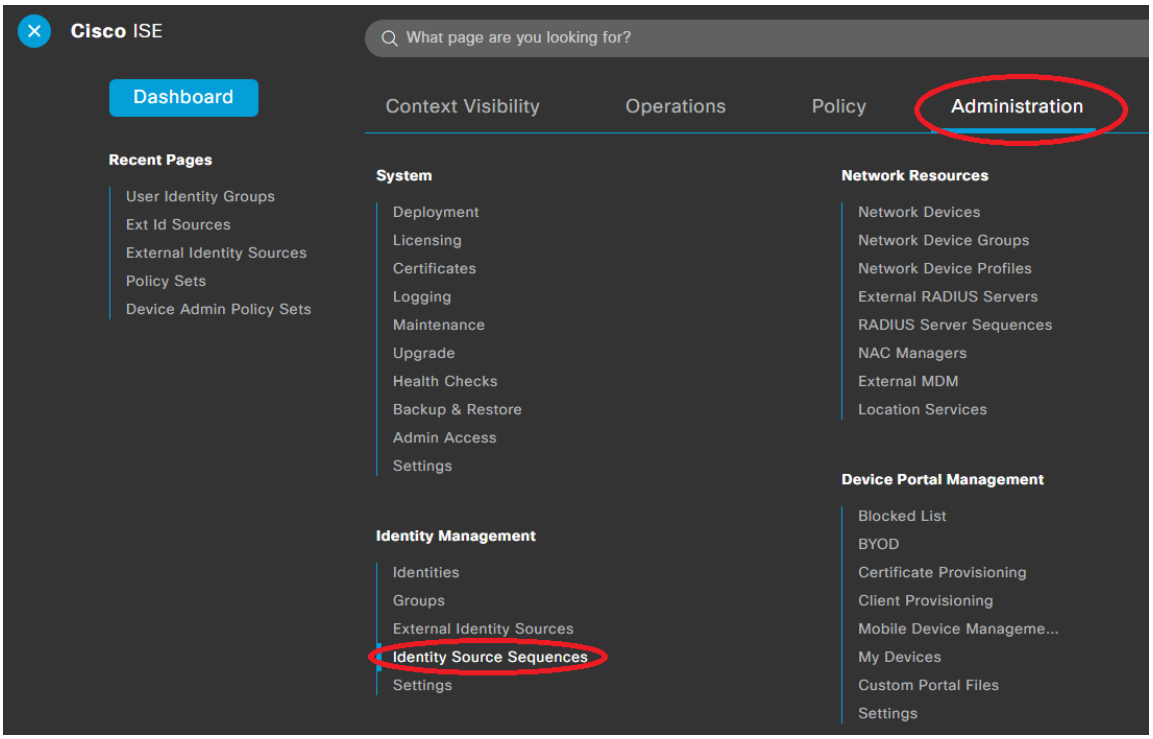

7. Starting from the left to right, configure the settings within each tab menu item as follow.

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

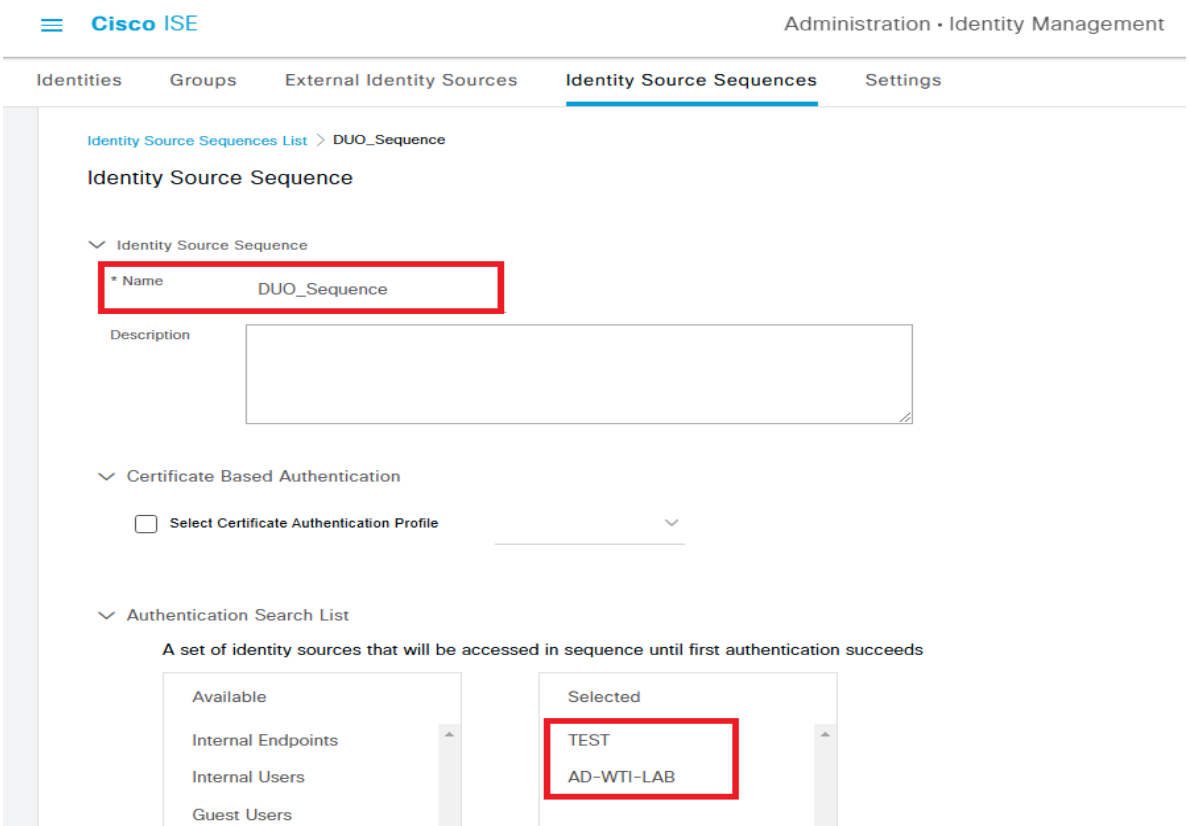
b. In Connection tab, configure the primary server details. (Primary Server is DUO Proxy Authentication Server)



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

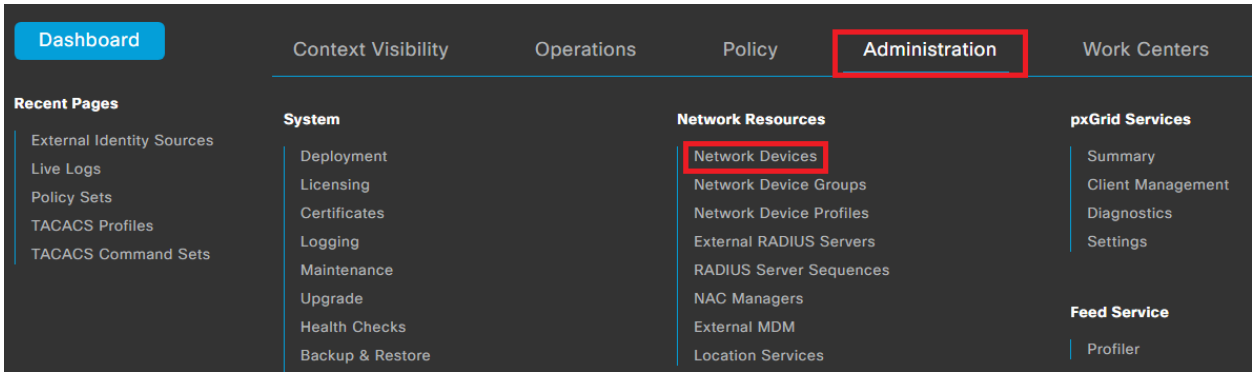



9. In Identity Sources Sequence click **Add** name identity source sequence and select authentication available search list and click Save.

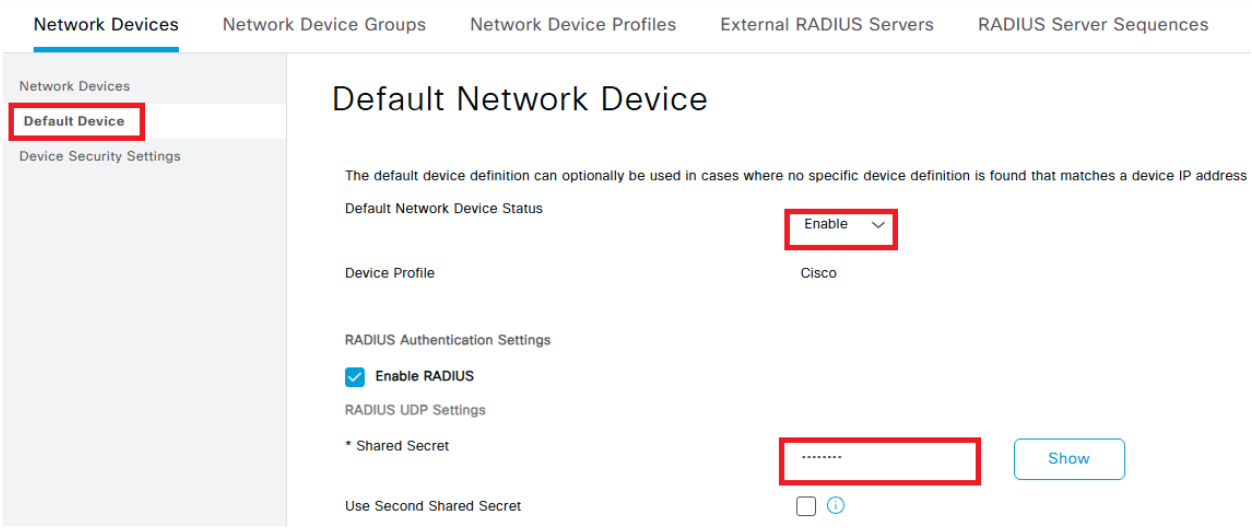


## Step 3: Create Network Device

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

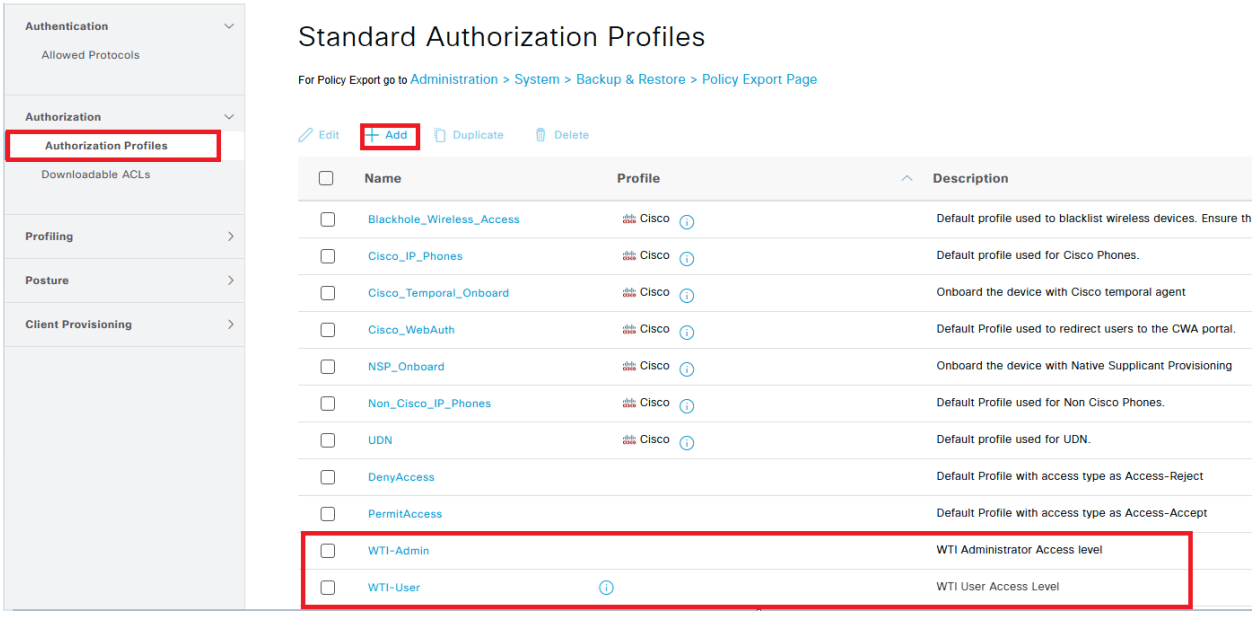



2. Enable Radius and define shared secret in Device Default

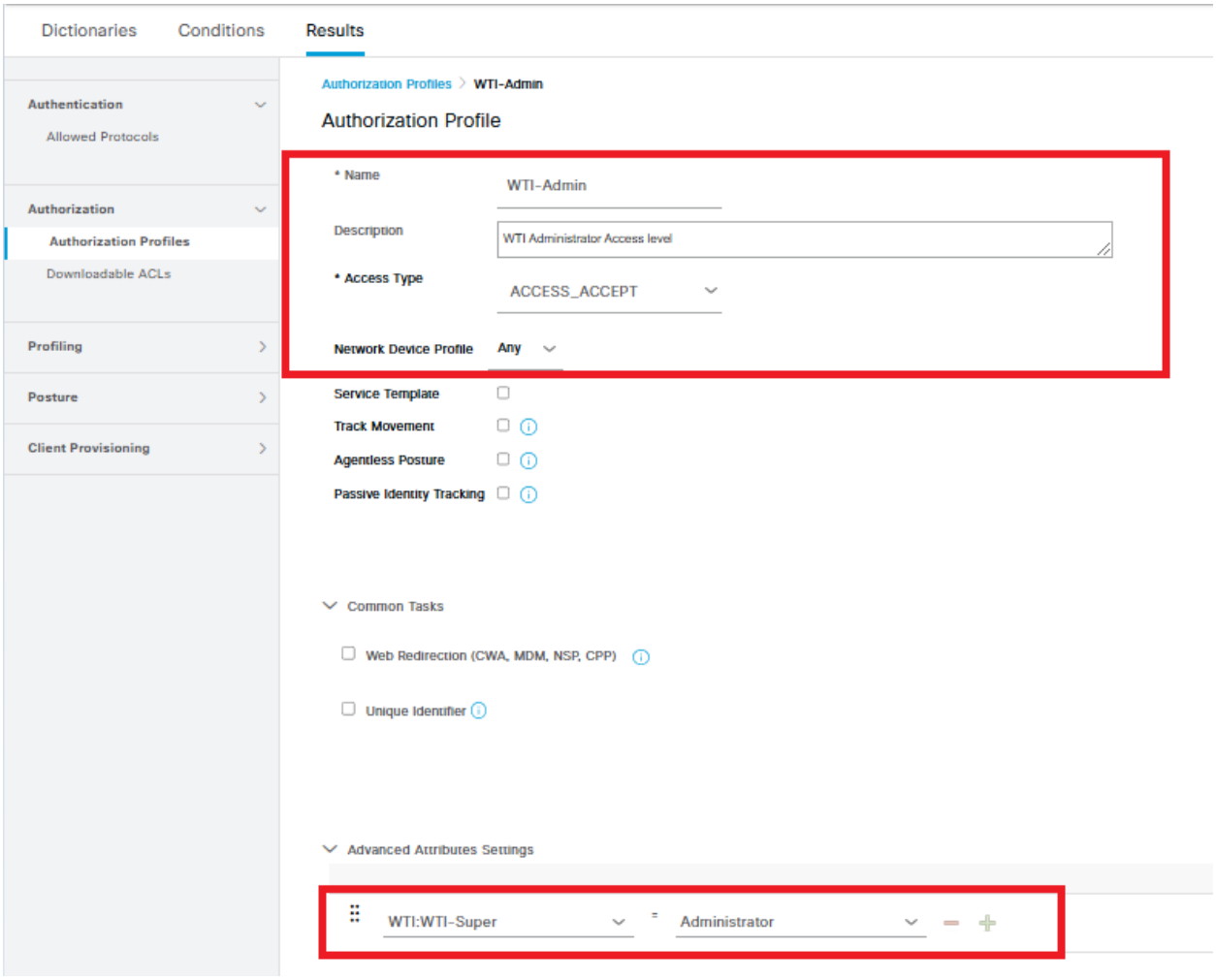



## Step 4: Create Radius Authorization Profile

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

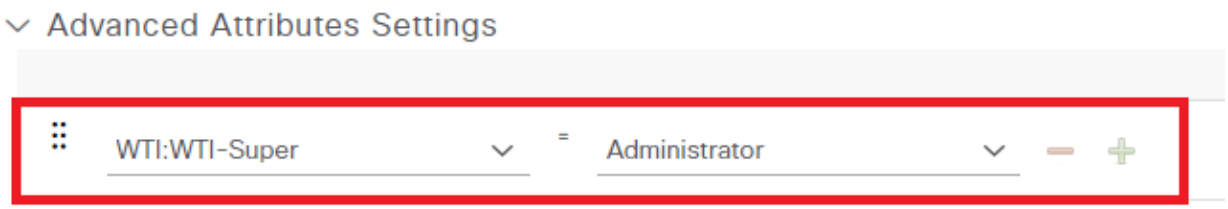


2. Create two Authorization Profile. One for WTI_Admin (Administrator access level) and another for WTI_User (User access level).




**For WTI_Admin**

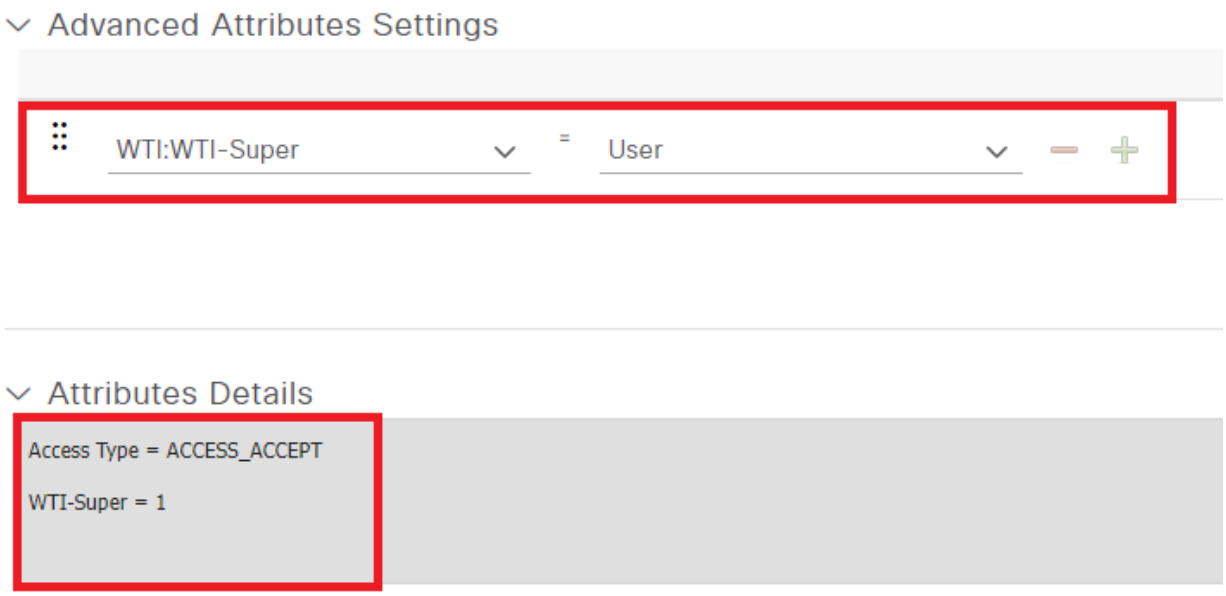
In advanced Attribute Settings





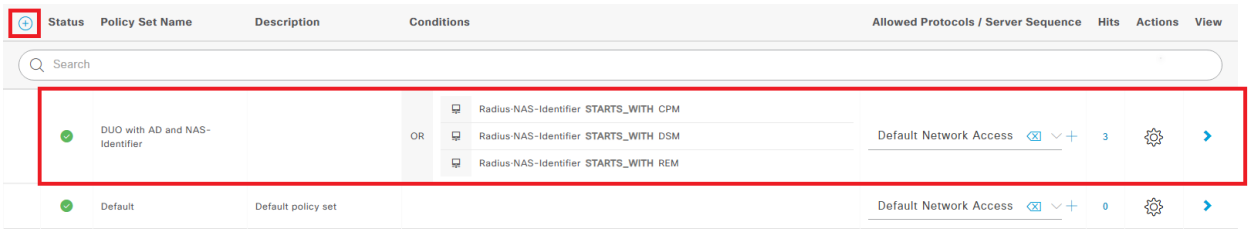

**For WTI_User**

In Advance Attribute Settings




## Step 5: Create Policy with NAS-Identifier

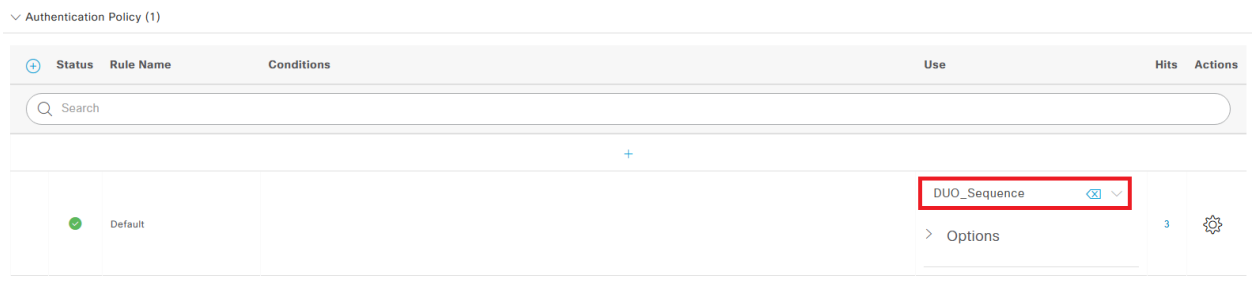
1. Navigate to **Policy > Policy Sets > click (+) to add new policy set**.



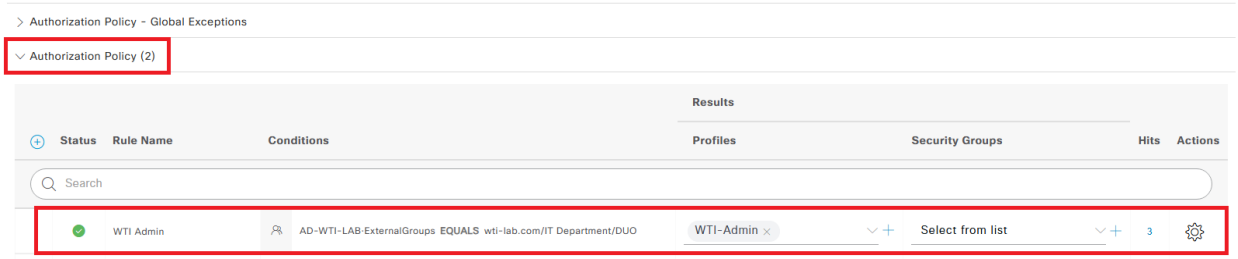

Policy Set Name: **DUO with AD and NAS-Identifier**
Condition: **Radius-NAS-Identifier START_WITH CPM** (DSM or REM)
Allowed Protocols: **Default Network Access**

2. Authentication Policy

   Rule Name: Default
   Use: **DUO_Sequence**



. 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**




## WTI Radius Setting

1. Go to /N option 29 for Radius

2. RADIUS Setting

