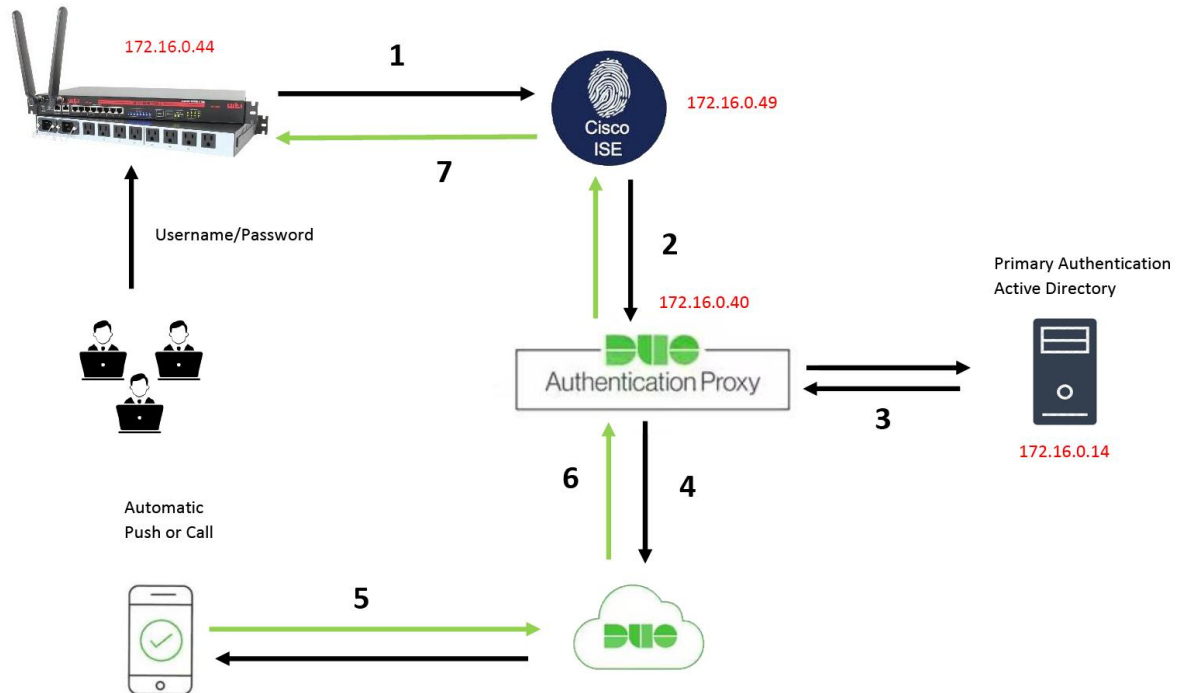


## DUO with Active Directory and Cisco ISE with WTI TACACS Client



### 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

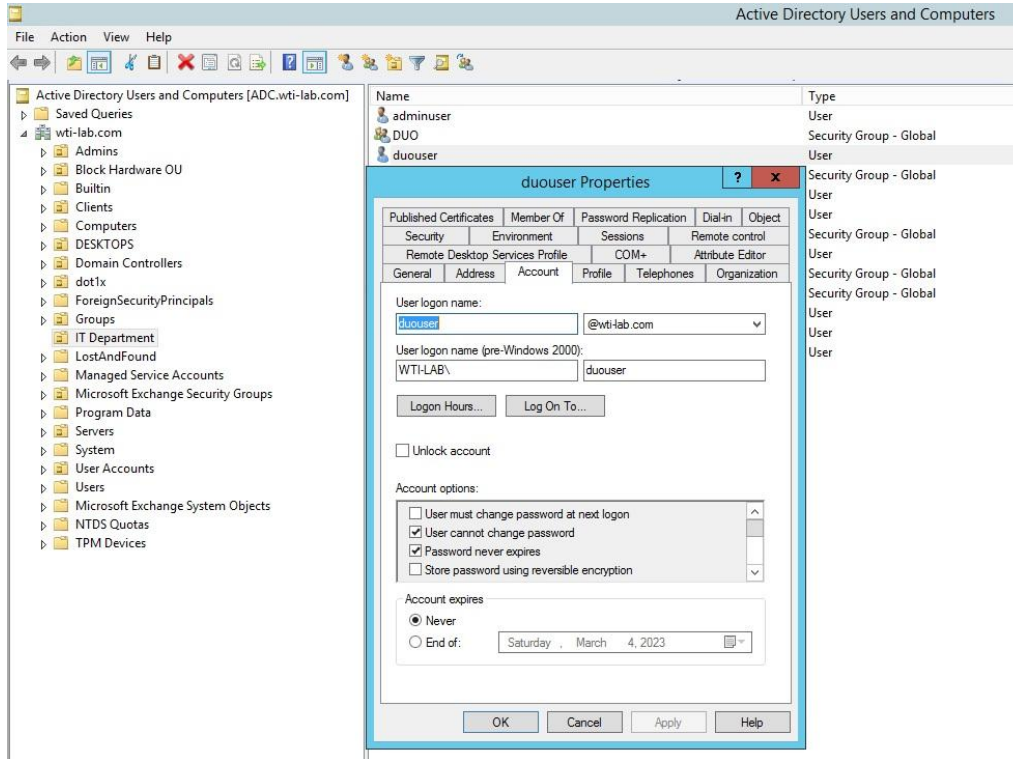
- Windows Active Directory
- Duo
- Duo Authentication Proxy Manager
- Cisco ISE
- WTI TACACS client

### 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.

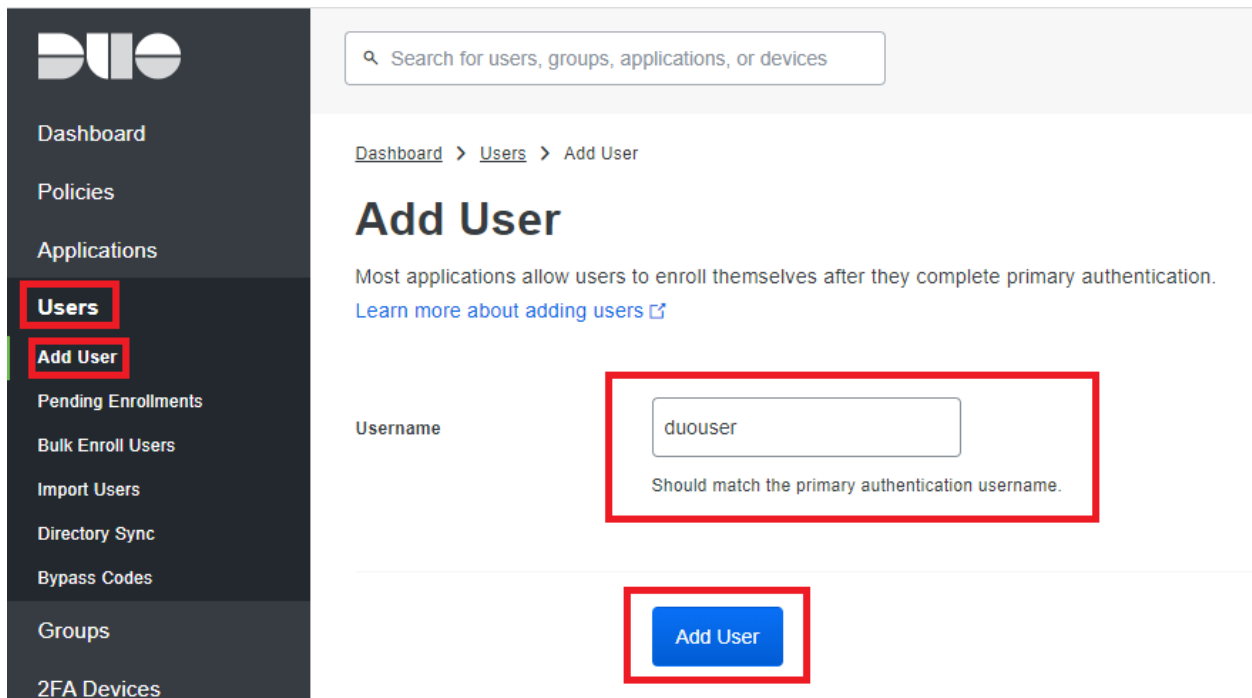
## Active Directory Configurations

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.

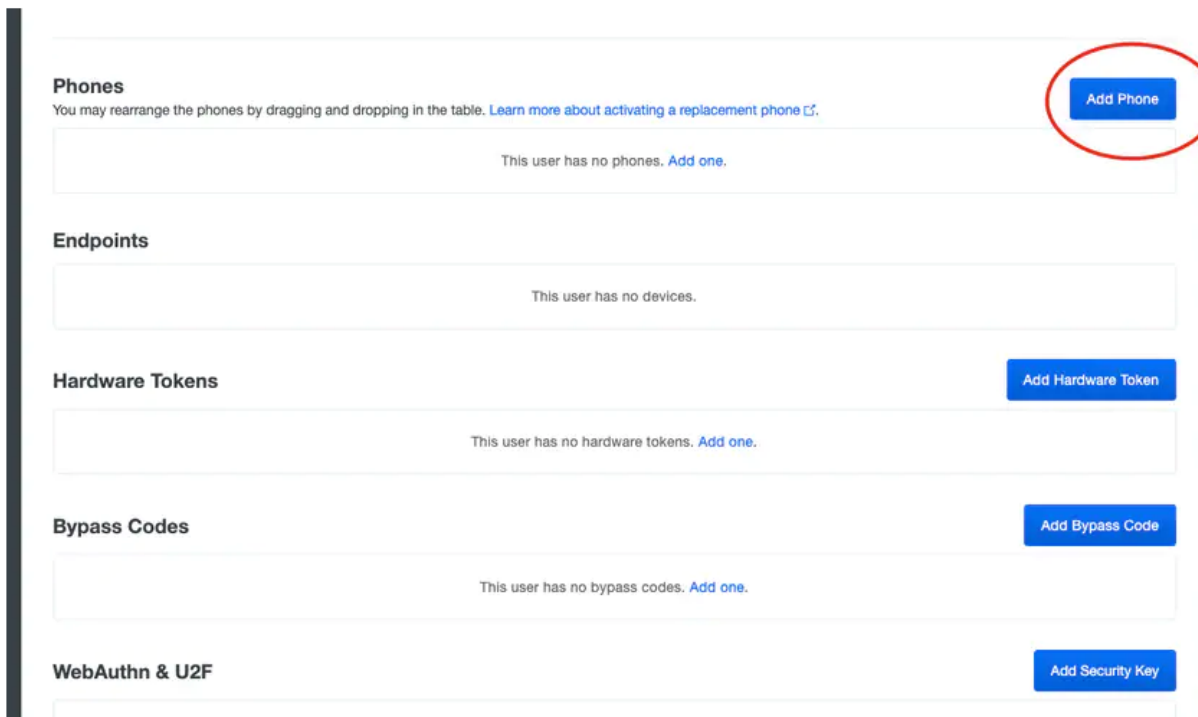


## Duo configuration

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**



The screenshot shows a user management interface with several sections for configuring authentication methods. Each section has a corresponding 'Add' button:

- Phones**: Includes a sub-header, a note about rearranging phones, and an **Add Phone** button (circled in red).
- Endpoints**: Includes a note that the user has no devices.
- Hardware Tokens**: Includes a note that the user has no hardware tokens and an **Add Hardware Token** button.
- Bypass Codes**: Includes a note that the user has no bypass codes and an **Add Bypass Code** button.
- WebAuthn & U2F**: Includes an **Add Security Key** button.


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

[Dashboard](#) > [Users](#) > [duovpn](#) > Add Phone

## Add Phone

 [Learn more about Activating Duo Mobile](#)

Type  Phone  Tablet

Phone number   [Show extension field](#)  
Optional. Example: "+52 1 222 123 4567"

**Add Phone**

# Activate Duo Mobile

This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows a mobile device to authenticate via Duo Push.

**Note:** Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new code.

Phone

---

Send links via  SMS  Email

---

Email

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

Search for users, groups, applications, or devices

Dashboard > Activate Duo Mobile

## Activate Duo Mobile

This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows a mobile device to authenticate via Duo Push.

**Note:** Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new code.

Phone

Expiration   after generation

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

**This is an automated email from Duo Security.**

Your organization invites you to set up Duo Mobile on your phone. You will find instructions from your Duo administrator below. If you have questions, please reach out to your organization's IT or help desk team.

This email will help you add your Cisco account to Duo Mobile on this device:



Just tap this link from + [redacted] or copy and paste it into Duo Mobile manually:



If you're not reading this from + [redacted] Duo Mobile on your phone and scan this barcode:



Don't have Duo Mobile yet? Install it first:

iPhone: <https://itunes.apple.com/us/app/duo-mobile/id422663827>

Android: <https://play.google.com/store/apps/details?id=com.duosecurity.duomobile>

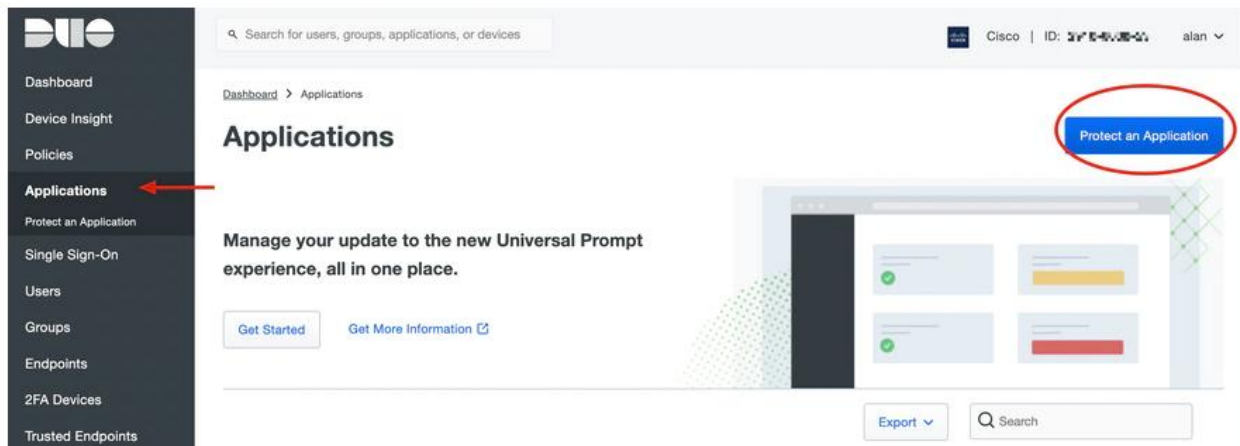
10. Open the Duo Mobile App from your mobile device and click **Add** then select **Use QR code** and scan the code from the instructions email.

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**.





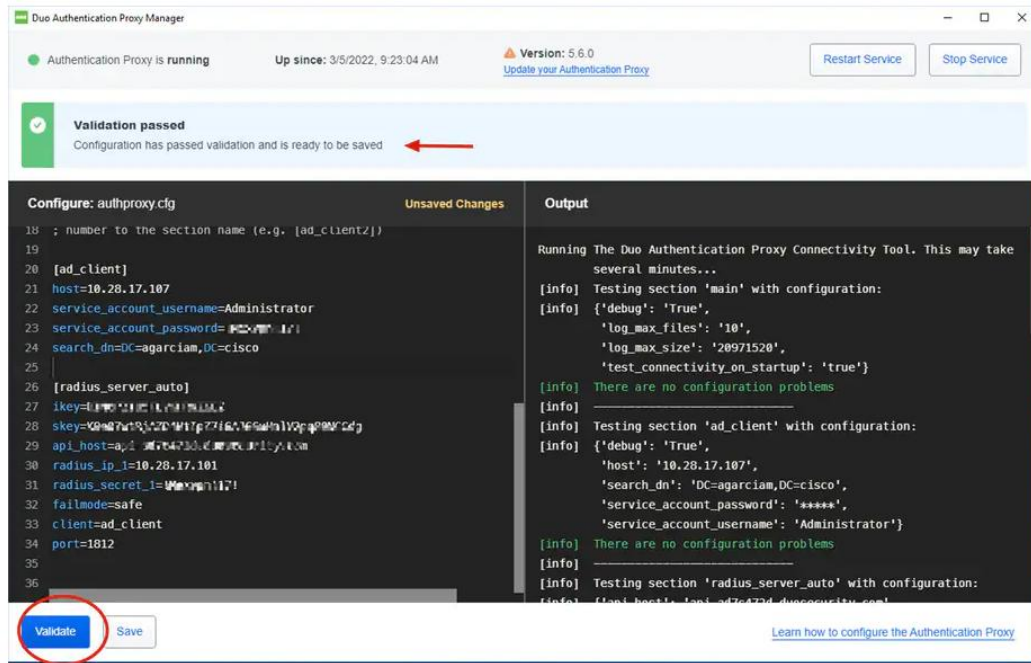
The Duo proxy config file should be on the machine you installed the Duo proxy program, at this file location:

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=XXXXXXXXXXXXXXXXXXXX
skey=YYYYYYYYYYYYYYYYYYY
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 TACCAS profile and TACACS command set

To configure the profile, navigate to **Work Centers > Policy Elements**. On the left-hand side select Results and click the dropdown arrow.

The screenshot shows the Cisco ISE Policy Elements configuration page. The navigation bar at the top includes Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, and Policy Elements (highlighted with a red box). The left sidebar shows a tree view with Conditions, Network Conditions, Results (highlighted with a red box), Allowed Protocols, TACACS Command Sets, and TACACS Profiles (highlighted with a red box). The main content area is titled "TACACS Profiles" and contains a table of profiles. The table has columns for Name, Type, and Description. The profiles listed are Default Shell Profile, Deny All Shell Profile, WLC ALL, WLC MONITOR, WTI Admin, and WTI User. The WTI Admin and WTI User rows are highlighted with a red box. Above the table are buttons for Refresh, Add (highlighted with a red box), Duplicate, Trash, and Edit.

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR
<input type="checkbox"/>	WTI Admin	Shell	
<input type="checkbox"/>	WTI User	Shell	



## For WTI Admin access level with privilege level 15.

The screenshot shows the configuration page for a TACACS Profile named 'WTI Admin'. The breadcrumb path is 'TACACS Profiles > WTI Admin'. The profile name is 'WTI Admin'. The description field is empty. Under 'Common Tasks', the 'Common Task Type' is set to 'Shell'. Two checkboxes are checked: 'Default Privilege' and 'Maximum Privilege', both set to a value of 15. The range '(Select 0 to 15)' is shown for both.

Overview Identities User Identity Groups Ext Id Sources Network Resources **Policy Elements** Device Admin Policy Sets

TACACS Profiles > WTI Admin  
TACACS Profile

Name  
WTI Admin

Description

Task Attribute View Raw View

Common Tasks

Common Task Type Shell

Default Privilege 15 (Select 0 to 15)  
 Maximum Privilege 15 (Select 0 to 15)

### Privilege levels for the different access levels:

View Only – 0-4

User – 5-9

Superuser – 10-14

Admin – 15

Add a command set in TACACS Command Sets to permit all. Click Add from the top menu and fill out as below:

The screenshot shows the configuration page for a TACACS Command Set named 'PermitAllCommands'. The breadcrumb path is 'TACACS Command Sets > PermitAllCommands'. The command set name is 'PermitAllCommands'. The description field is empty. Under 'Commands', the checkbox 'Permit any command that is not listed below' is checked.

Overview Identities User Identity Groups Ext Id Sources Network Resources **Policy Elements**

TACACS Command Sets > PermitAllCommands  
Command Set

Name  
PermitAllCommands

Description

Commands

Permit any command that is not listed below

## Step 2: Create network Device

1. Navigate to **Administrator > Network Resource > Network Device > Default Device**  
Enable TACACS and define shared secret.

The screenshot shows the Cisco ISE configuration interface for a 'Default Device'. The left sidebar has 'Default Device' highlighted. The main content area shows various settings for RADIUS and TACACS. The 'TACACS Authentication Settings' section is highlighted with a red box, showing the following configuration:

- Enable TACACS
- Shared Secret: [Redacted] [Show] [Retire]
- Enable Single Connect Mode:
- Options:  Legacy Cisco Device,  TACACS Draft Compliance Single Connect Support

## Step 3: Connect or join Active Directory user with Cisco ISE

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

The screenshot shows the Cisco ISE Administration menu. The 'Administration' tab is circled in red. The 'Identity Management' section is expanded, and 'External Identity Sources' is circled in red.

- Administration
- Identity Management
  - External Identity Sources

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

Cisco ISE Administration - Identity Management

Identities Groups **External Identity Sources** Identity Source Sequences Settings

External Identity Sources

- Certificate Authentication F
- Active Directory**
- AD-WTI-LAB
- LDAP

Active Directory

Edit **+ Add** Delete Node View Advanced Tools Scope Mode

Join Point Name	Active Directory Domain
AD-WTI-LAB	wti-lab.com

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

Cisco ISE Administration - Identity Management

Identities Groups **External Identity Sources** Identity Source Sequences Settings

External Identity Sources

- Certificate Authentication F
- Active Directory
- AD-WTI-LAB
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID

**Connection** Allowed Domains PassivID Groups Attributes Advanced Settings

Join Point Name AD-WTI-LAB

Active Directory Domain wti-lab.com

+ Join + Leave Test User Diagnostic Tool Refresh Table

ISE Node	ISE Node R...	Status	Domain Controller	Site
CiscoISE.wti-lab.com	STANDALONE	Operational	DCWin2022.wti-lab.com	Default-First-Site-Name

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

Cisco ISE Administration - Identity Management

Identities Groups **External Identity Sources** Identity Source Sequences Settings

External Identity Sources

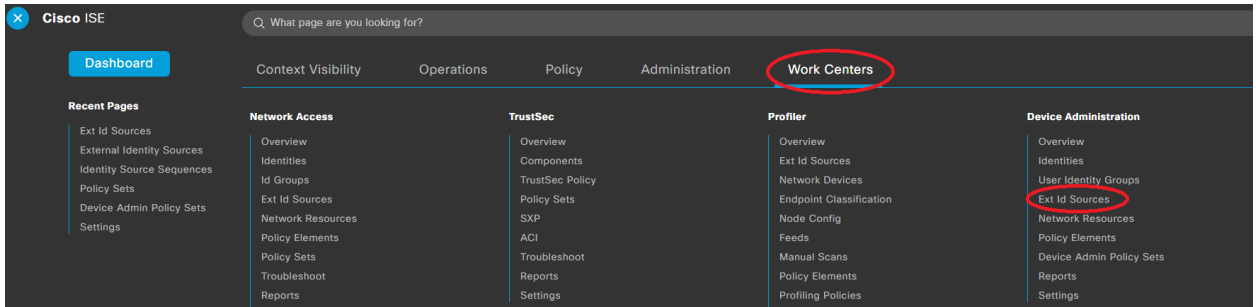
- Certificate Authentication F
- Active Directory
- AD-WTI-LAB
- LDAP

Connection Allowed Domains PassivID **Groups** Attributes Advanced Settings

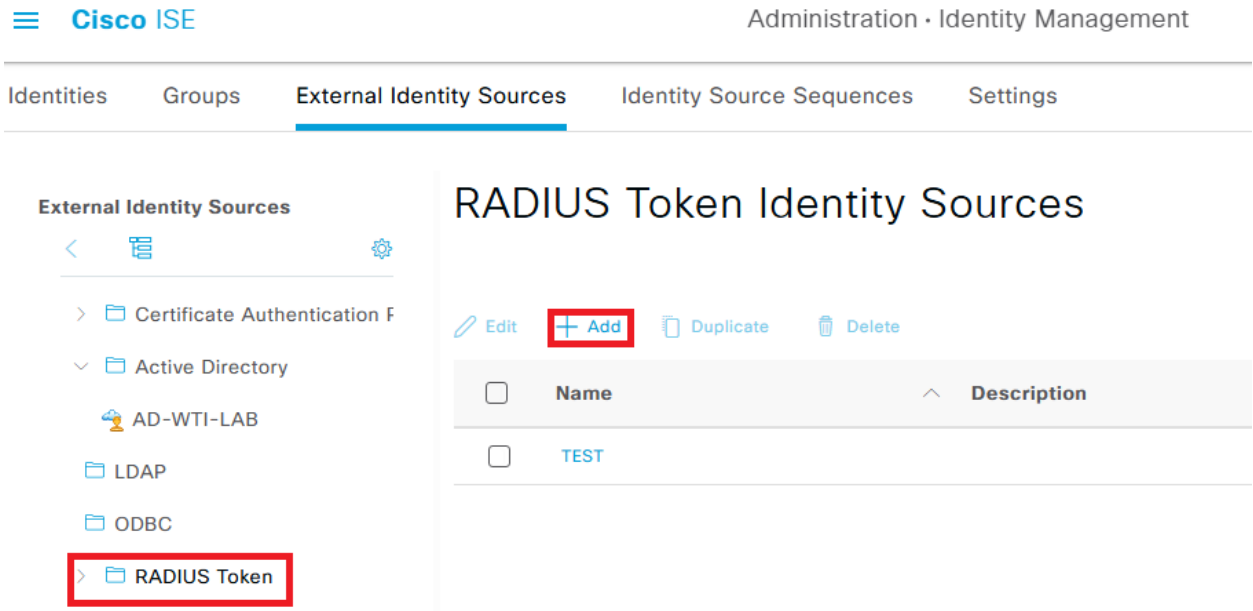
Edit **+ Add** Delete Group Update SID Values

Name	SID
wti-lab.com/IT Department/DUO	S-1-5-21-2346001846-3831695603-2264274261-2642

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



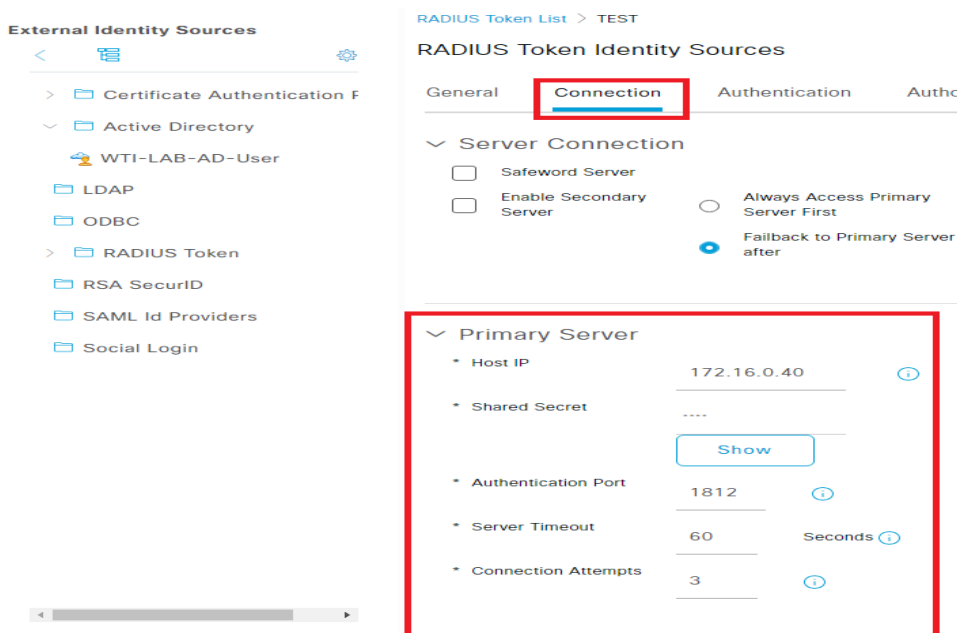
6. On RADIUS Token click **Add**.



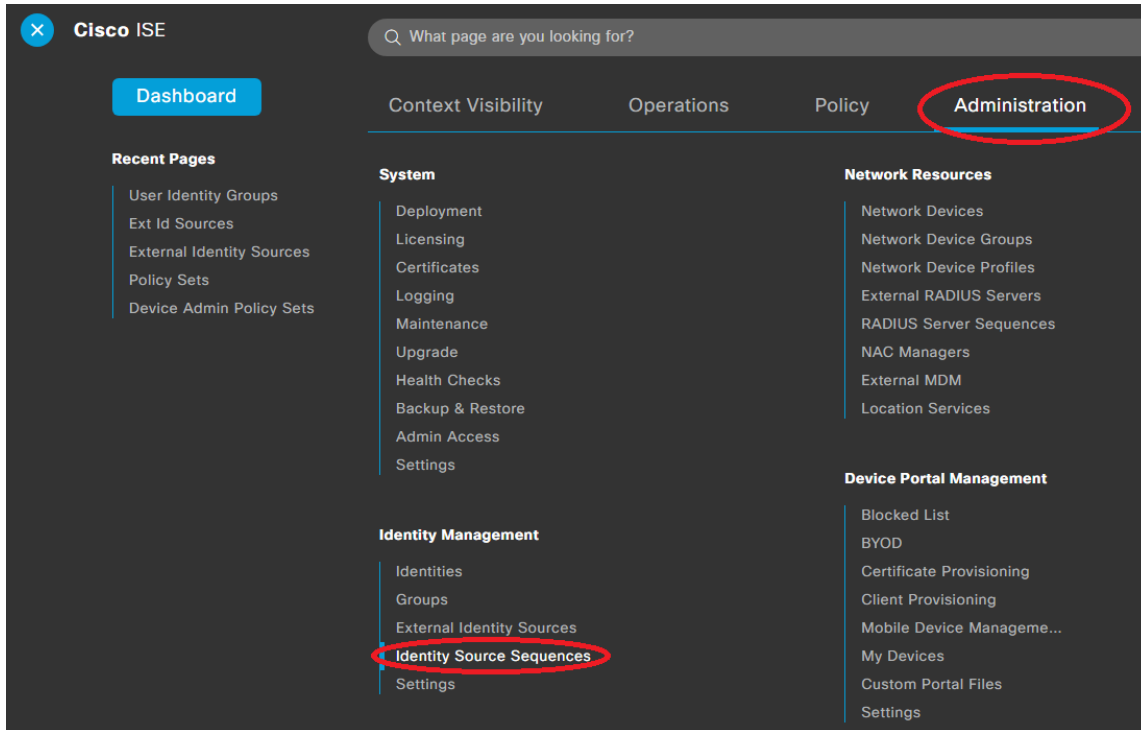
7. Starting from the left to right, configure the settings within each tab menu item as follow.

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

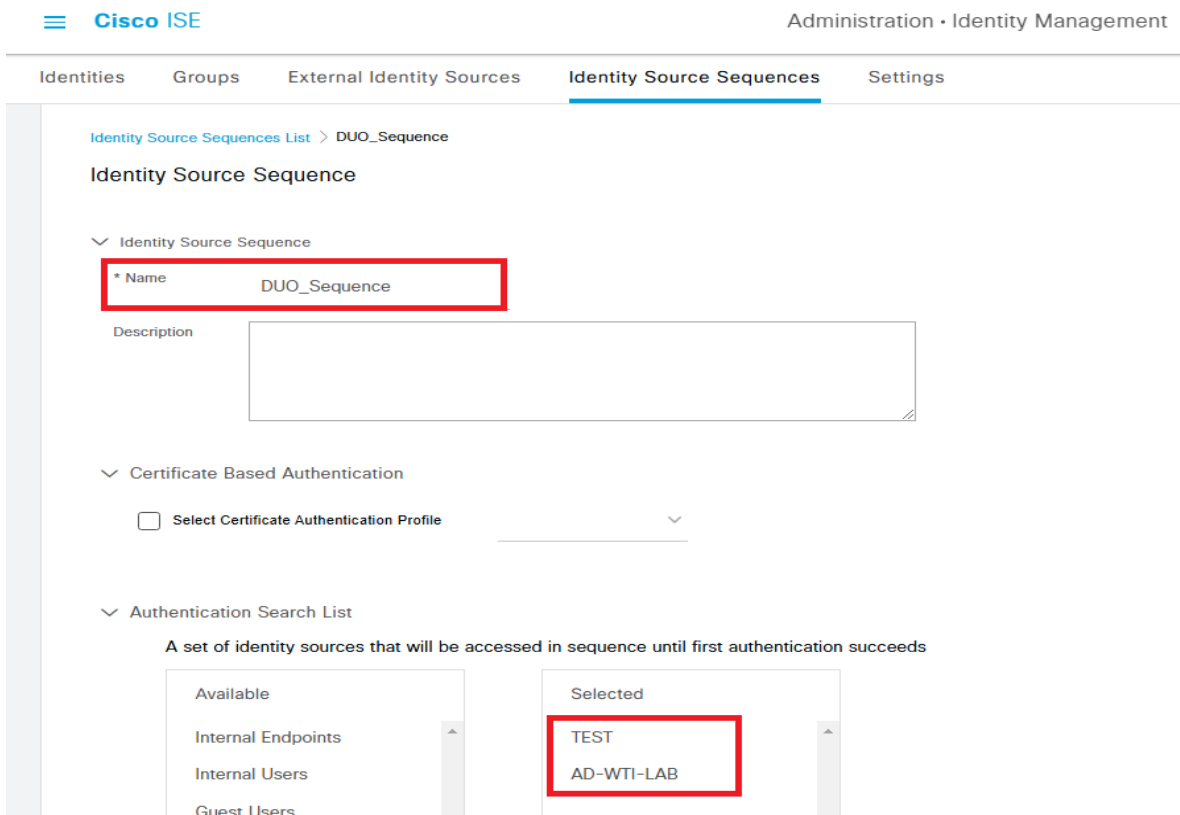
b. In Connection tab, configure the primary server details. (Primary Server is DUO Proxy Authentication Server)



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 4: Create TACACS Policy Set

1. Navigate to **Work Centers > Device Administration > Device Admin Policy Set**
2. Under Policy set click **(+)** to add new policy set.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✔	DUO TACACS with AD		DEVICE-Device Type EQUALS All Device Types	Default Device Admin	24	⚙️	➔
✔	Default	Tacacs Default policy set		Default Device Admin	0	⚙️	➔

Policy Set Name: **DUO TACACS with AD**

Condition: **DEVICE-Device Type EQUALS All Device Type**

Allowed Protocols: **Default Device Admin**

3. Authentication Policy

Rule Name: **Default**

Use: **DUO\_Sequence**

Status	Rule Name	Conditions	Use	Hits	Actions
✔	Default		DUO_Sequence	3	⚙️

3. Authorization Policy – create two authorization policy, one for WTI\_Admin and another for WTI\_User.

Status	Rule Name	Conditions	Results		Hits	Actions
			Command Sets	Shell Profiles		
✔	WTI Admin	AD-WTI-LAB-ExternalGroups EQUALS wti-lab.com/IT Department/DUO	PermitAllCommands	WTI Admin	16	⚙️

### For WTI Admin

Rule Name: **WTI Admin**

Condition: **AD-WTI-LAB-ExternalGroup EQUALS wti-lab.com/IT Department/DUO**

Profile: **WTI Admin**

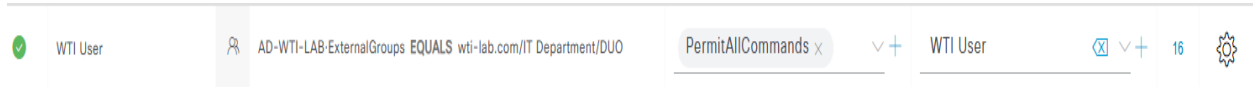
Status	Rule Name	Conditions	Results		Hits	Actions
			Command Sets	Shell Profiles		
✔	WTI Admin	AD-WTI-LAB-ExternalGroups EQUALS wti-lab.com/IT Department/DUO	PermitAllCommands	WTI Admin	16	⚙️

## For WTI User

Rule Name: **WTI user**

Condition: **AD-WTI-LAB-ExternalGroup EQUALS wti-lab.com/IT Department/DUO**

Profile: **WTI user**



### WTI TACACS Setting

1. Go to /N option 28 for TACACS
2. TACACS Setting

```
TACACS: [Shared]
1. Enable: On
2. Primary host/address: 172.16.0.49
3. Secondary host/address:
4. Secret Word: <defined>
5. Fallback Timer: 15 Sec
6. Fallback Local: On <All failures>
7. Authentication Port: 49
8. Default User Access: Off
9. Account Management Module: Enabled
10. Session Management Module: Enabled
11. Service Name: wti
12. Debug: Off
13. Ping Test
```