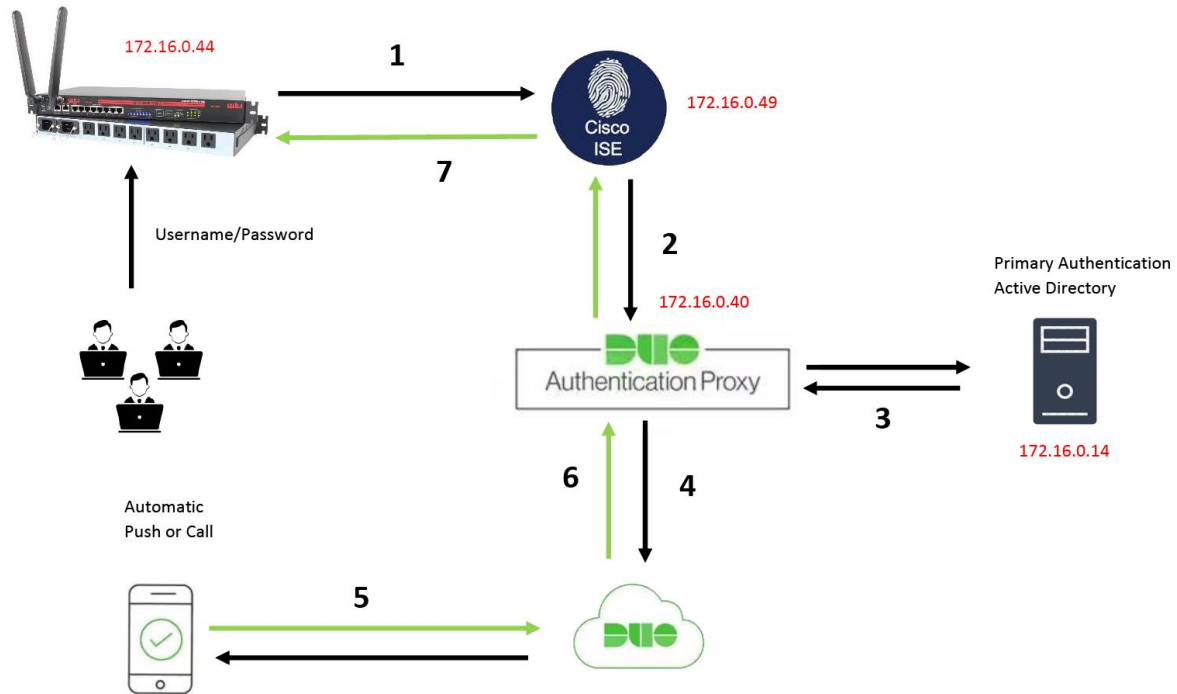


Duo Integration with Active Directory and Cisco ISE for Two-Factor Authentication on WTI Radius client



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 Radius client

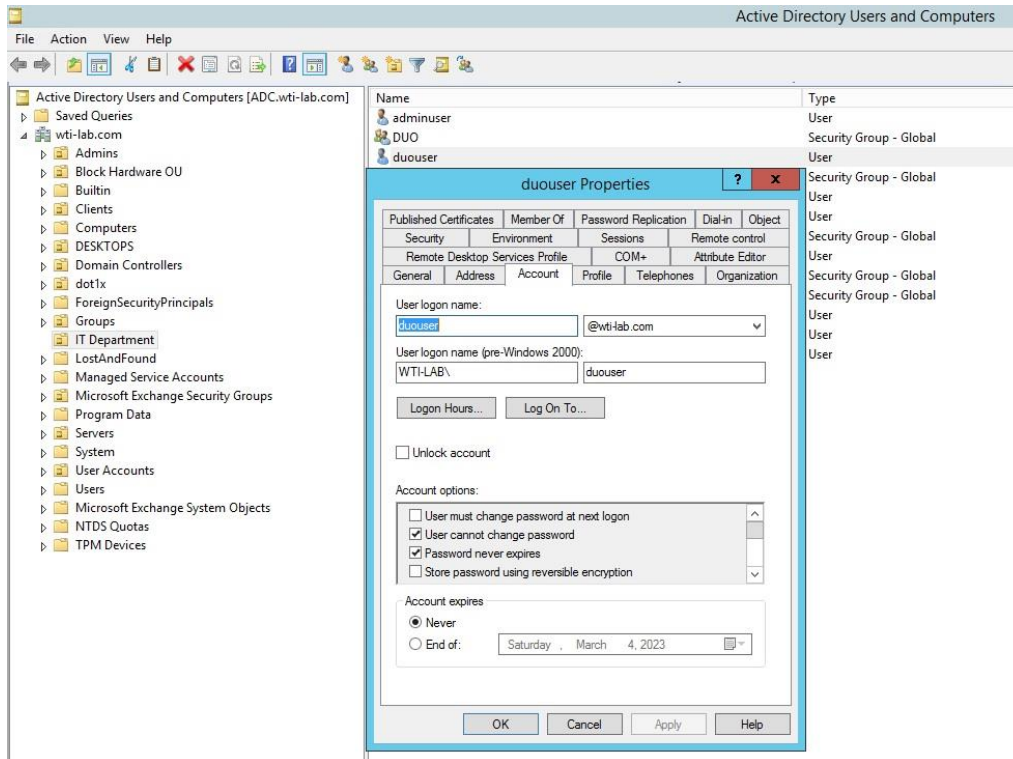
Communication process

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.

Dashboard

Policies

Applications

Users

Add User

Pending Enrollments

Bulk Enroll Users

Import Users

Directory Sync

Bypass Codes

Groups

2FA Devices

Search for users, groups, applications, or devices

Dashboard > Users > Add User

Add User

Most applications allow users to enroll themselves after they complete primary authentication. [Learn more about adding users >](#)

Username

Should match the primary authentication username.

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**

Phones

You may rearrange the phones by dragging and dropping in the table. [Learn more about activating a replacement phone >](#)

This user has no phones. [Add one.](#)

Endpoints

This user has no devices.

Hardware Tokens **Add Hardware Token**

This user has no hardware tokens. [Add one.](#)


Bypass Codes **Add Bypass Code**

This user has no bypass codes. [Add one.](#)


WebAuthn & U2F **Add Security Key**

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




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

Phones

You may rearrange the phones by dragging and dropping in the table. [Learn more about activating a replacement phone](#)

Alias	Device	Platform	Model	Security Warnings	
phone1		Android 10		✓ No warnings	 <input type="button" value="Activate Duo Mobile"/> 

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

 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 appli mobile device or authenticate via Duo Push.

Note: Generating an activation code will invalidate any existing Duo Mobile credentials fc

Phone

Expiration after generation



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

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 r

Phone

XXXXXXXXXX

Send links via

SMS

Email



Email

XXXXXXXXXX



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 + [blurred] or copy and paste it into Duo Mobile manually:



If you're not reading this from + [blurred] 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>

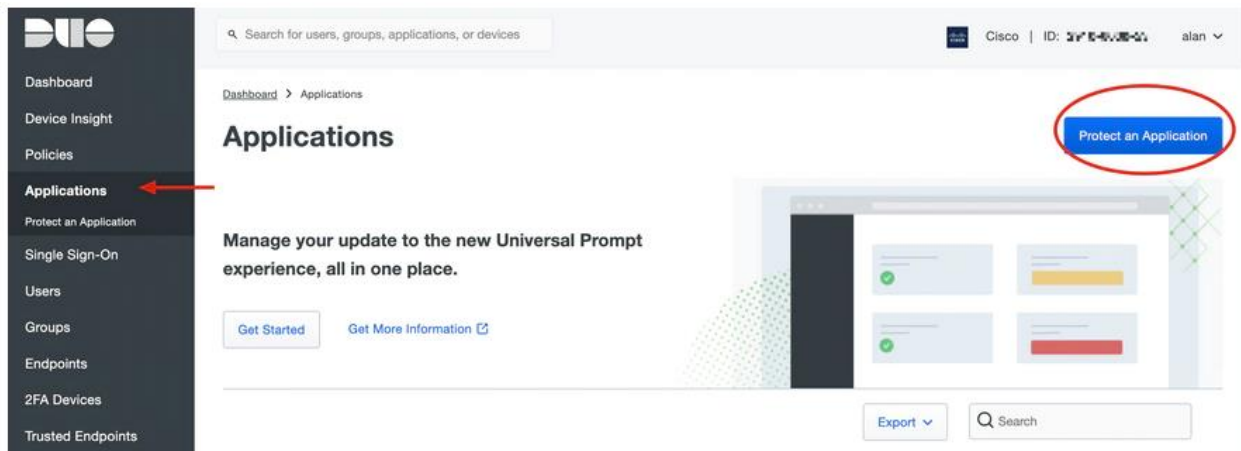
10. Open the Duo Mobile App from your mobile device and click **Add** then select **Use QR code** and scan the code from the instructions email.

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

Duo Authentication Proxy Configuration

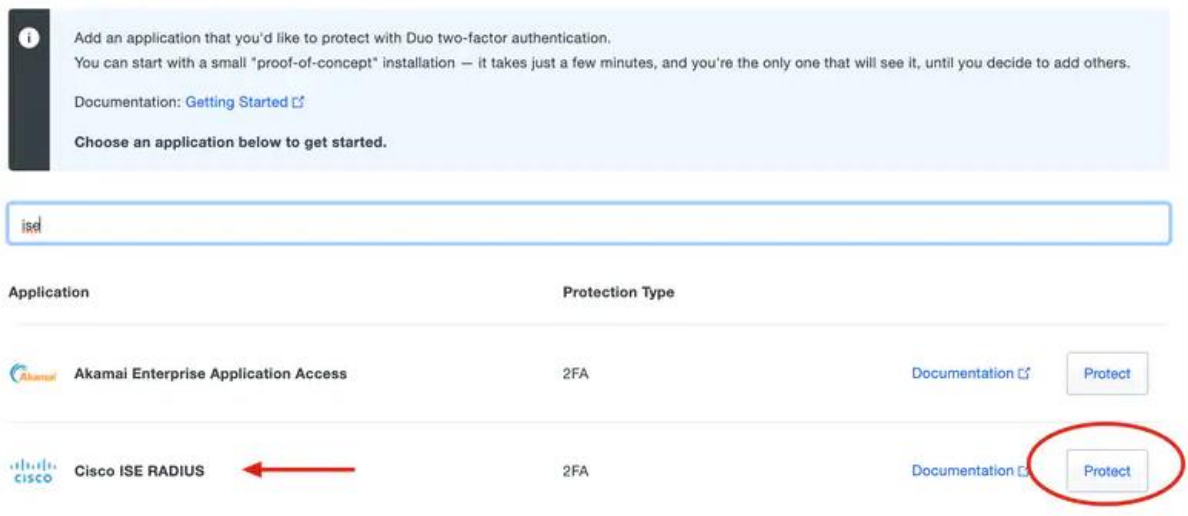
1. Download and Install Duo Auth Proxy manager from <https://duo.com/docs/authproxy-reference>.

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



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

Protect an Application



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

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
```

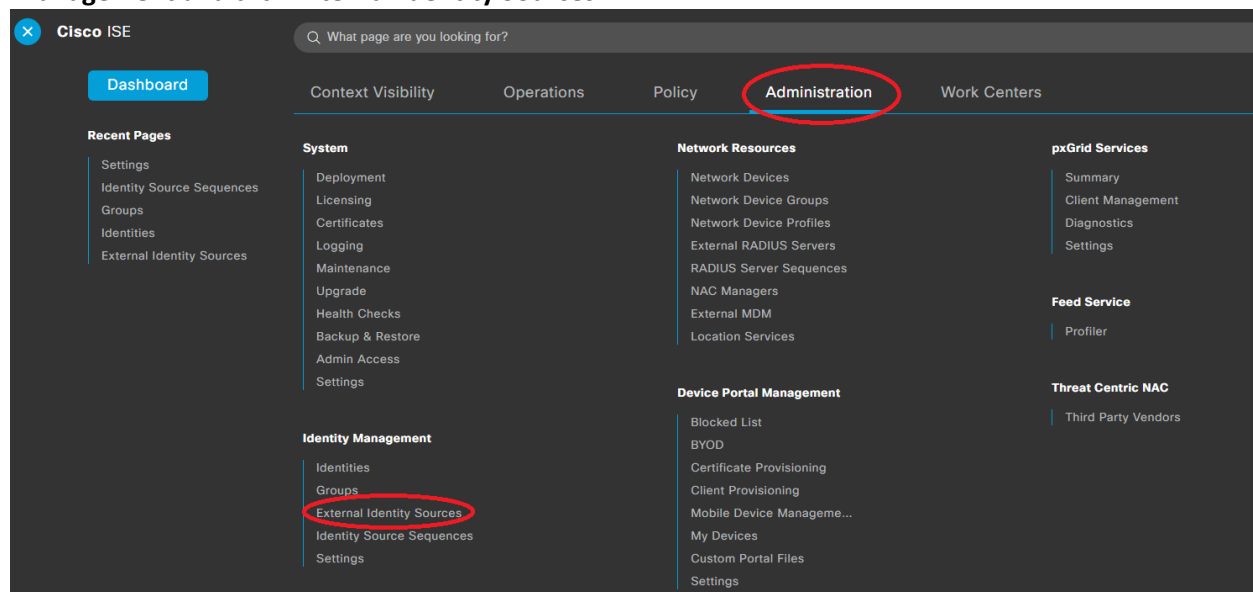
```
[radius_server_auto]
ikey=XXXXXXXXXXXXXXXXXXXX
skey=YYYYYYYYYYYYYYYYYYYY
api_host=api-123456789.duosecurity.com
radius_ip_1=172.16.0.49
radius_secret_1=test123
client=ad_client
port=1812
```

Cisco ISE Configurations

1. Log in into the Cisco ISE Admin portal
2. Create the vendor-specific attribute, WTI Dictionary Attributes and user access level. Please follow the step 1 – 5 from this article below

<https://wtiftip.wti.com/pub/TechSupport/Articles/RADIUS%20with%20Cisco%20ISE.pdf>

3. Create an Active Directory joint point in ISE. Navigate to **Administration** then click **Identity Management** and click **External Identity Sources**.



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

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes "Identities", "Groups", "External Identity Sources" (highlighted with a red box), "Identity Source Sequences", and "Settings". The main content area is titled "Active Directory". On the left, a sidebar shows a tree view of "External Identity Sources" with "Active Directory" selected and highlighted by a red box. In the main area, there are buttons for "Edit", "+ Add" (highlighted with a red box), "Delete", "Node View", "Advanced Tools", and "Scope Mode". Below these buttons, there is a table with two rows:

Join Point Name	Active Directory Domain
<input type="checkbox"/>	WTI-LAB-AD-User
<input type="checkbox"/>	wti-lab.com

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

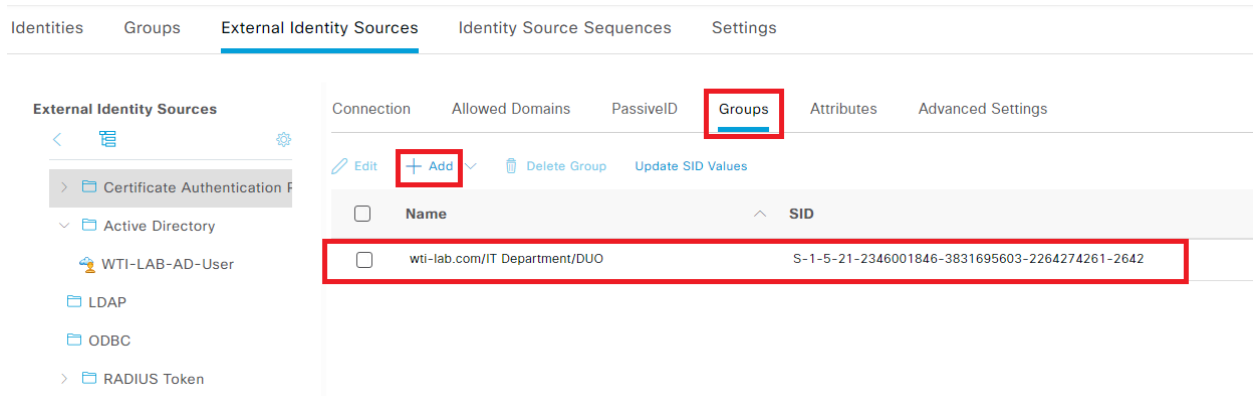
The screenshot shows the "Connection" section for an Active Directory source. The top navigation bar includes "Identities", "Groups", "External Identity Sources" (highlighted with a red box), "Identity Source Sequences", and "Settings". The main content area is titled "Connection". On the left, a sidebar shows a tree view of "External Identity Sources" with "Active Directory" selected and highlighted by a red box. In the main area, there are tabs for "Connection" (highlighted with a red box), "Allowed Domains", "PassiveID", "Groups", "Attributes", and "Advanced Settings". Below these tabs, there is a form with two fields:

* Join Point Name	WTI-LAB-AD-User	<input type="text"/>
* Active Directory Domain	wti-lab.com	<input type="text"/>

Below the form, there are buttons for "+ Join", "+ Leave", "Test User", "Diagnostic Tool", and "Refresh Table". At the bottom, there is a table with the following data:

ISE Node	ISE Node R...	Status	Domain Controller	Site	
<input type="checkbox"/>	ise.wti-lab.com	STANDALONE	Operational	ADC.wti-lab.com	Default-First-Site-Name

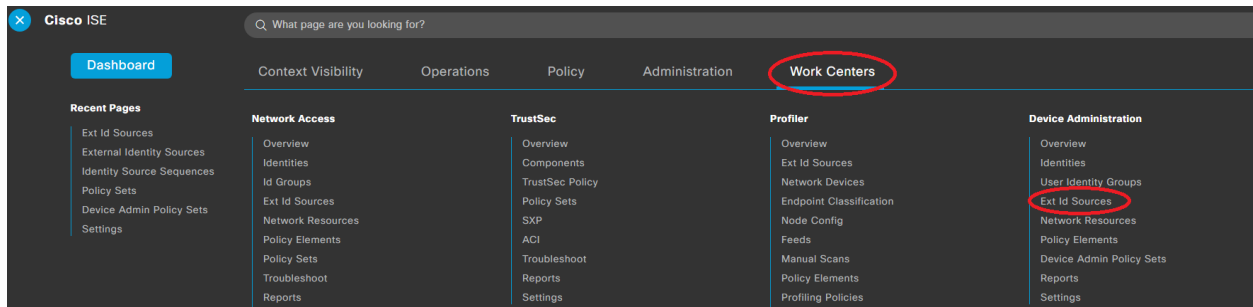
6. Navigate to **Groups** tab and click **Add > Select Group from Directory**.



The screenshot shows the Cisco ISE interface for External Identity Sources. The 'Groups' tab is selected and highlighted with a red box. Below the tab, there are buttons for 'Edit', '+ Add', 'Delete Group', and 'Update SID Values'. The '+ Add' button is also highlighted with a red box. A table below shows a list of groups with columns for 'Name' and 'SID'. One group is listed: 'wti-lab.com/IT Department/DUO' with SID 'S-1-5-21-2346001846-3831695603-2264274261-2642'. This row is highlighted with a red box.

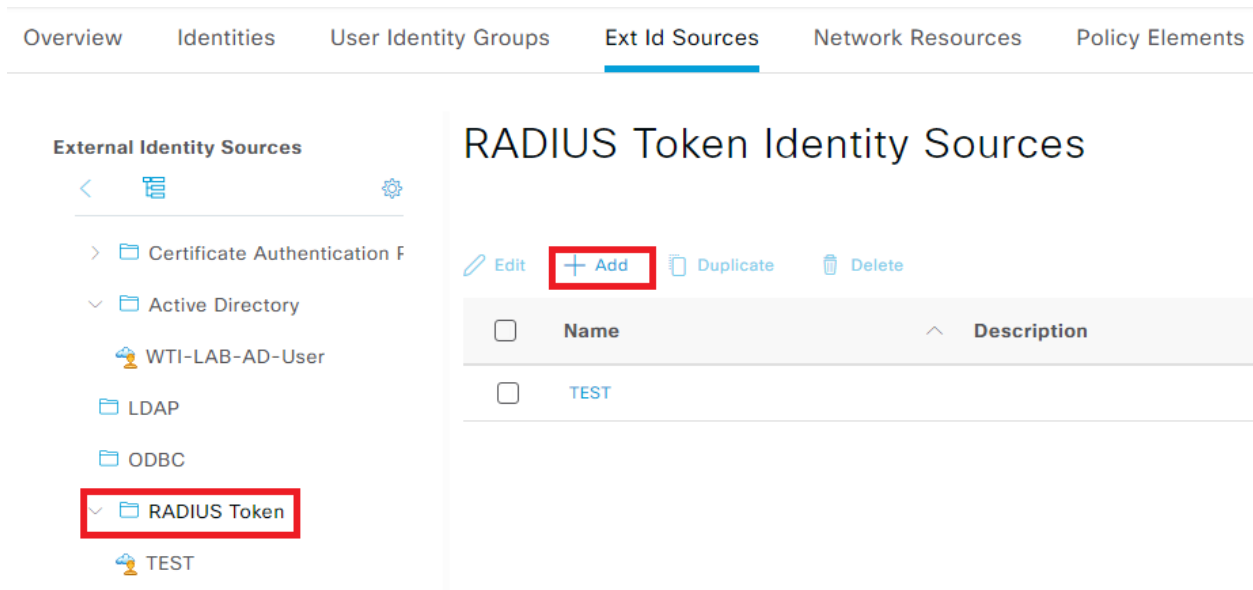
Name	SID
wti-lab.com/IT Department/DUO	S-1-5-21-2346001846-3831695603-2264274261-2642

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



The screenshot shows the Cisco ISE dashboard with the 'Work Centers' tab selected and circled in red. The 'Device Administration' section is visible, and 'Ext Id Sources' is circled in red within the 'Device Administration' menu.

8. On RADIUS Token click **Add**.



The screenshot shows the Cisco ISE interface for External Identity Sources. The 'Ext Id Sources' tab is selected. The 'RADIUS Token' category is selected in the left sidebar and highlighted with a red box. The '+ Add' button is highlighted with a red box. Below the '+ Add' button, there is a table with columns for 'Name' and 'Description'. One entry is listed: 'TEST'.

Name	Description
TEST	

9. 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)

External Identity Sources



> Certificate Authentication F

Active Directory

WTI-LAB-AD-User

LDAP

ODBC

> RADIUS Token

RSA SecurID

SAML Id Providers

Social Login



RADIUS Token List > TEST

RADIUS Token Identity Sources

General

Connection

Authentication

Autho

Server Connection

Safeword Server

Enable Secondary Server

Always Access Primary Server First

Failback to Primary Server after

Primary Server

* Host IP 172.16.0.40 ⓘ

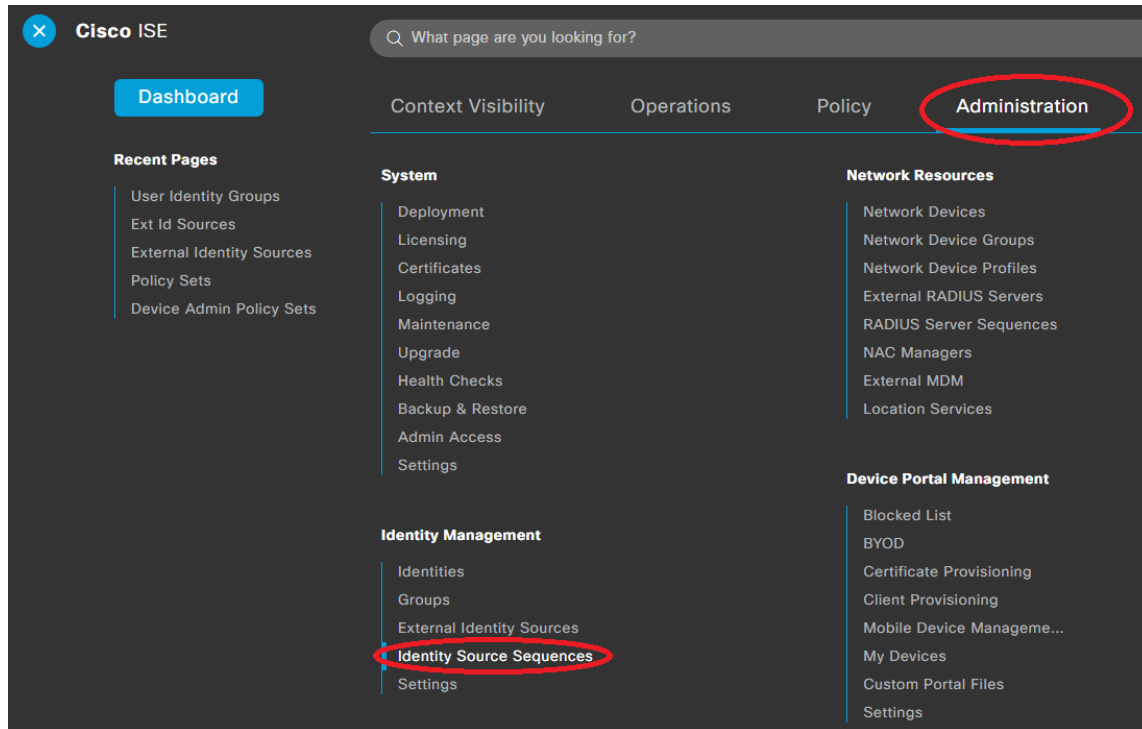
* Shared Secret
....
[Show](#)

* Authentication Port 1812 ⓘ

* Server Timeout 60 Seconds ⓘ

* Connection Attempts 3 ⓘ

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



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

[Identity Source Sequences List](#) > TEST_DUO_AD_Sequence

Identity Source Sequence

Identity Source Sequence

* Name TEST_DUO_AD_Sequence

Description

Certificate Based Authentication

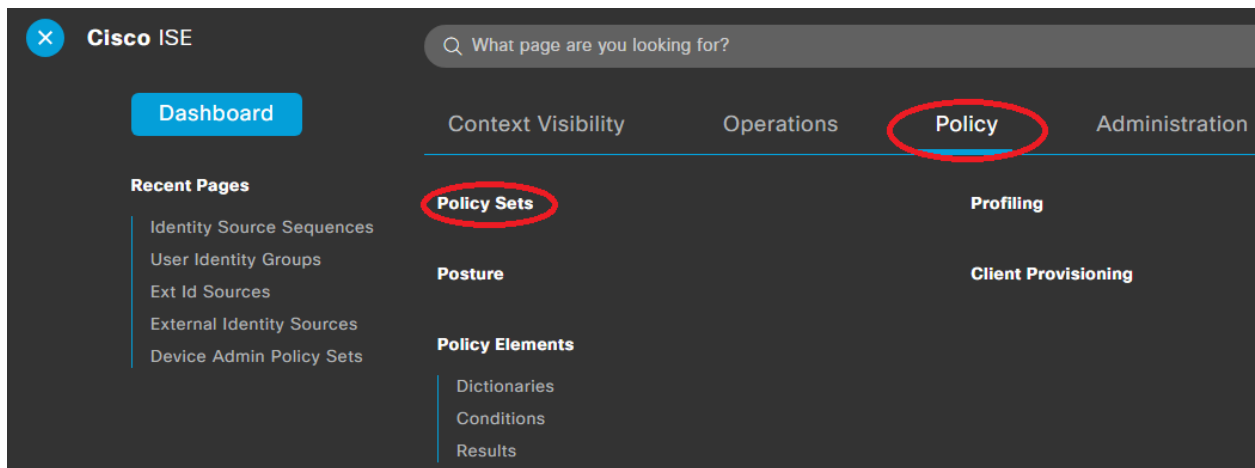
Select Certificate Authentication Profile

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints	TEST
Internal Users	WTI-LAB-AD-User
Guest Users	

12. Create Device Admin Policies. Navigate to **Policy > Policy Set**



13. Create a new policy set name, condition and allowed protocol/server sequence

Policy Sets Reset [Reset Policies](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
●	WTI External RADIUS with DUO		DEVICE Device Type EQUALS All Device Types	Default Network Access ⌵ +

Policy Set Name: WTI External RADIUS with Duo

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

Allowed Protocols: Default Network Access

14. In Authentication Policy. Select TEST_DUO_AD_Sequence in dropdown.

Authentication Policy (1)

Status	Rule Name	Conditions	Use
●	Default		TEST_DUO_AD_Seque... ⌵ > Options

15. In Authorization Policy.

Authorization Policy (2)

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
●	Authorization for WTI Admin	WTI-LAB-AD-User-ExternalGroups EQUALS wti-lab.com/IT Department/DUO	WTI_Admin x	Select from list	32	⌵ + ⚙

Rule Name: Authorization for WTI Admin

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

Profiles: WTI_Admin

Editor

WTI-LAB-AD-User-ExternalGroups

Equals ⌵ wti-lab.com/IT Department/DUO x ⌵

[Set to 'Is not'](#) [Duplicate](#) [Save](#)

WTI Radius client configuration

Log in into WTI device CLI, type /n and select 29 for RADIUS

Radius Setting:

1. Enable: **On**
2. Primary Host/Address: **172.16.0.49** (Your Cisco ISE)
3. Primary Secret Word: **test123** (Your secret defines in Proxy Authentication Manager under [radius_server_auto])
4. Secondary Host/Address:
5. Secondary Secret Word:
6. Fallback Timer: **30 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: **15**
14. OneTime Auth Type: **Cookies**
15. Session Module Type: **Disable**
16. Debug: **On**

```
RADIUS: [Shared]
1. Enable: On
2. Primary Host/Address: 172.16.0.49
3. Primary Secret Word: (defined)
4. Secondary Host/Address: (undefined)
5. Secondary Secret Word: (undefined)
6. Fallback Timer: 30 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: 15
14. OneTime Auth Type: Cookies
15. Session Module Type: Disable
16. Debug: On
17. Ping Test

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