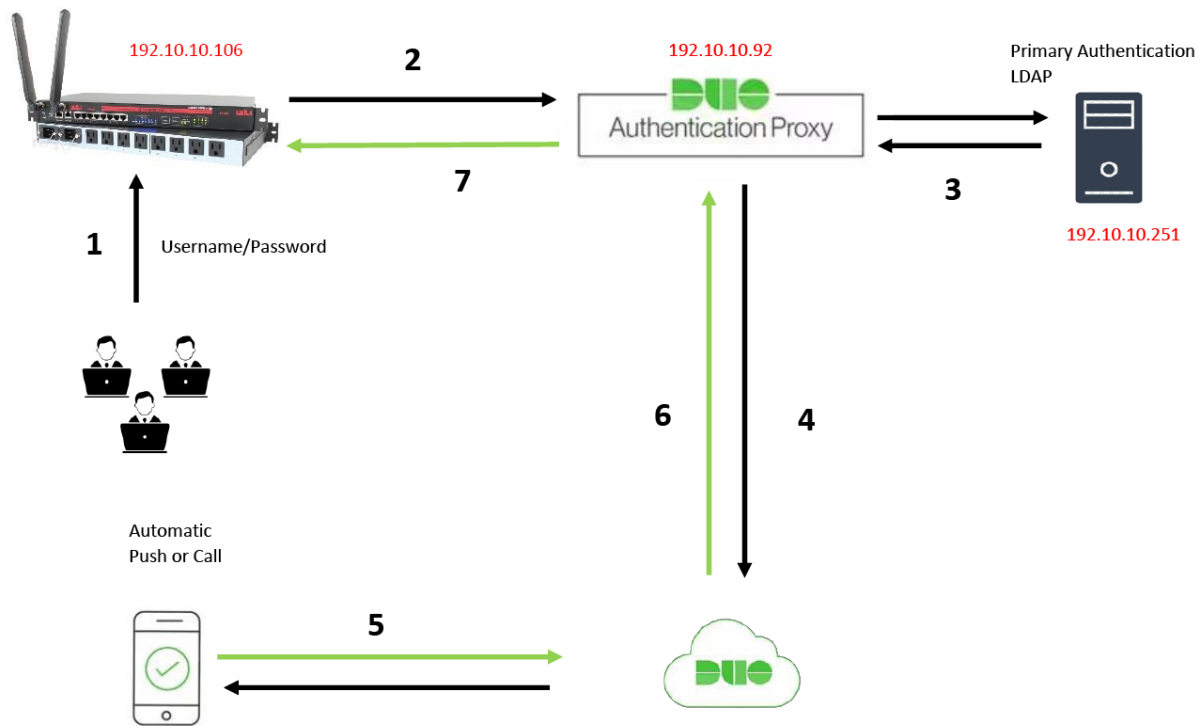


## DUO Two Factor Authentication via LDAP WTI



### Introduction

This document describes how to configure Duo push integration with Active Directory (AD) as Two-Factor Authentication via LDAP WTI.

### Components used

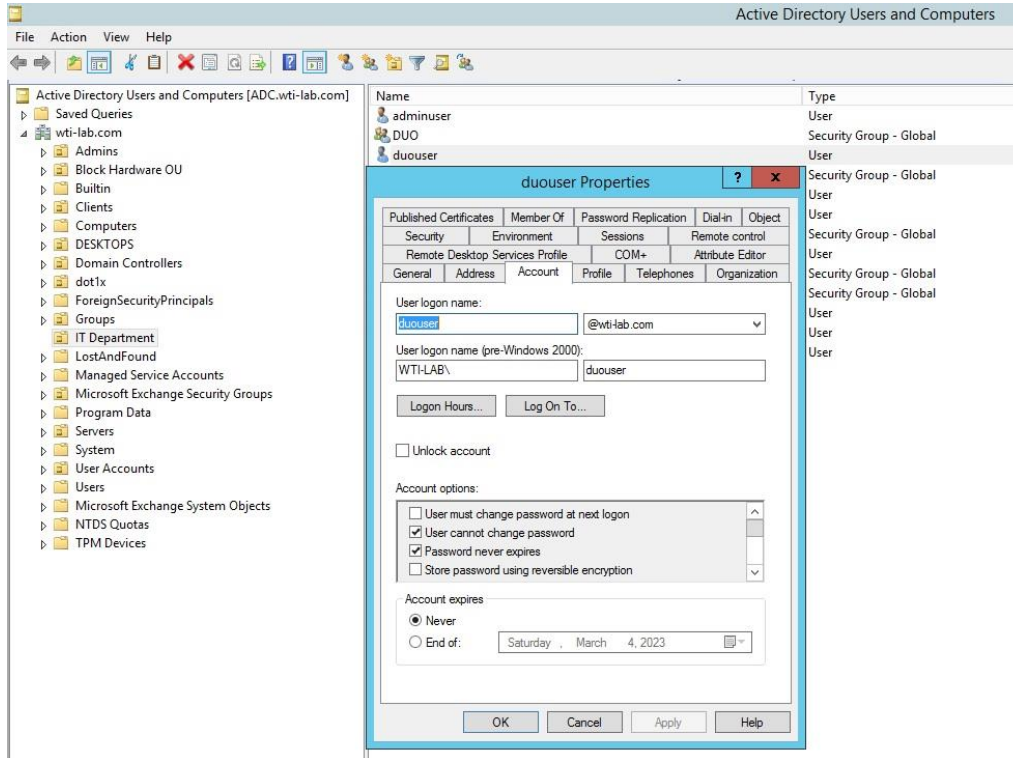
- Windows Active Directory
- Duo
- Duo Authentication Proxy Manager
- WTI LDAP client

### Communication process

1. Primary authentication initiated to WTI.
2. WTI send authentication request to the Duo Security Authentication Proxy.
3. Primary authentication using 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. WTI access grated.

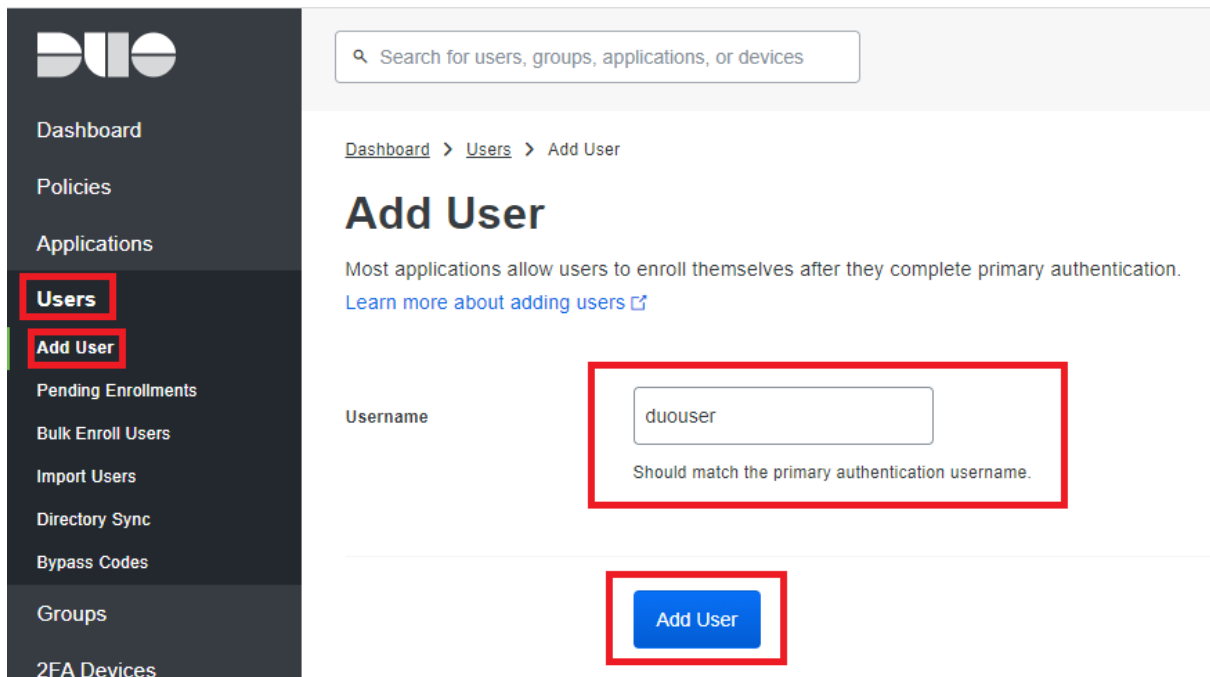
## Active Directory Configurations

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.



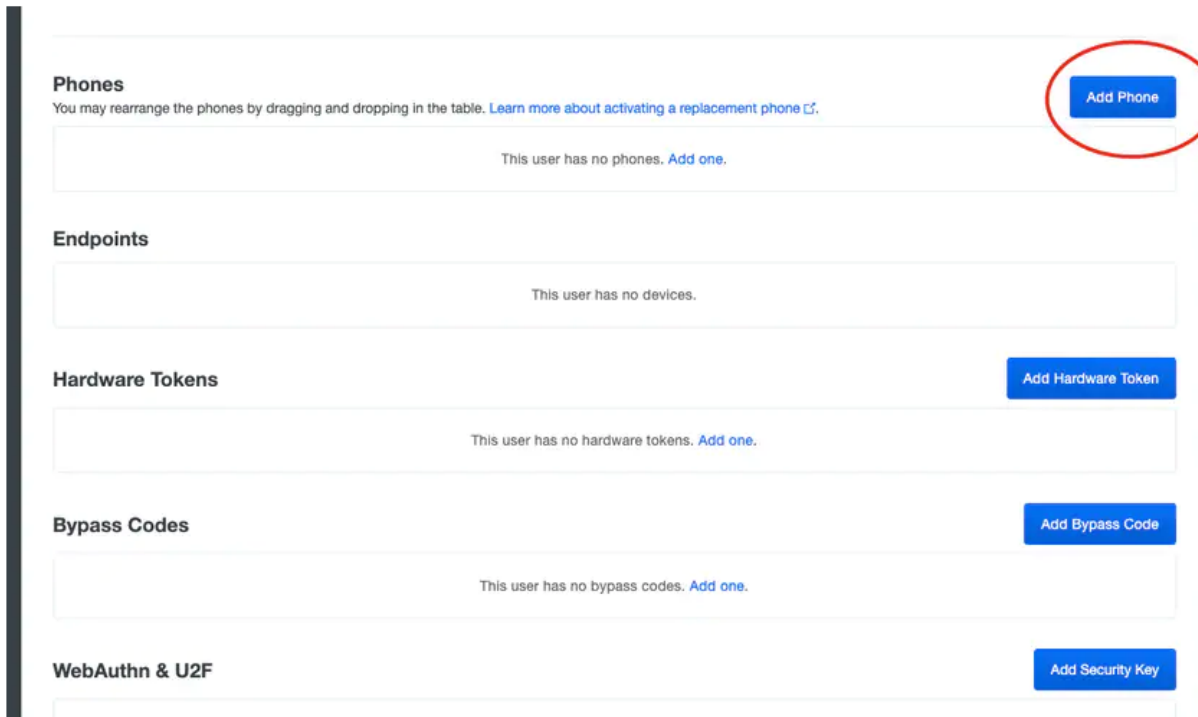
## Duo configuration

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**



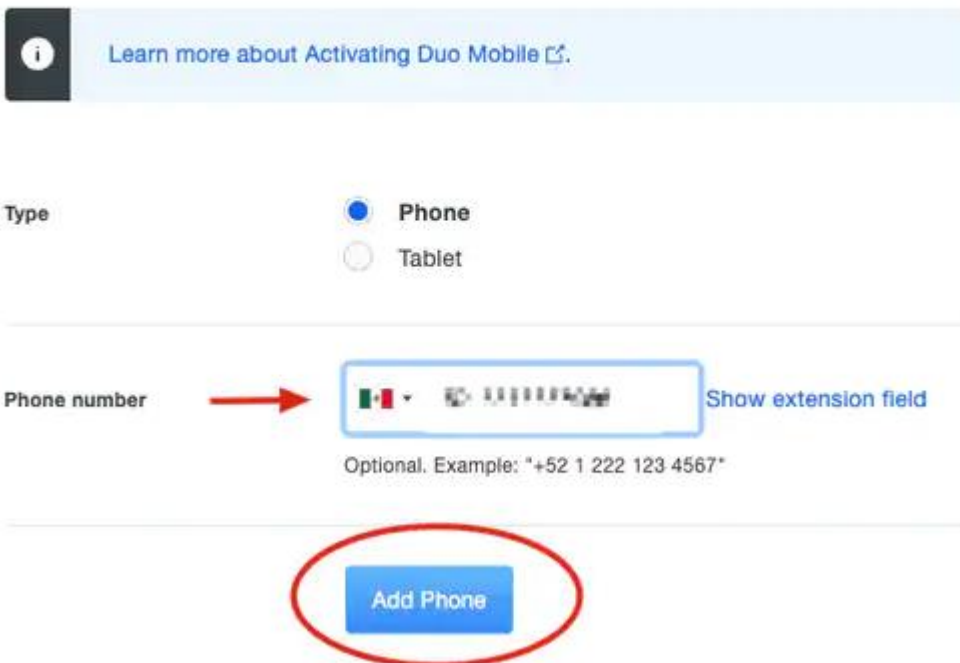
The screenshot shows a user management interface with several sections for adding authentication methods:

- Phones**: A section with a blue "Add Phone" button circled in red. Below it, a message states "This user has no phones. [Add one.](#)"
- Endpoints**: A section with a message stating "This user has no devices."
- Hardware Tokens**: A section with a blue "Add Hardware Token" button. Below it, a message states "This user has no hardware tokens. [Add one.](#)"
- Bypass Codes**: A section with a blue "Add Bypass Code" button. Below it, a message states "This user has no bypass codes. [Add one.](#)"
- WebAuthn & U2F**: A section with a blue "Add Security Key" button.

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

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

## Add Phone



The screenshot shows the "Add Phone" form with the following elements:

- An information icon and a link: "Learn more about Activating Duo Mobile [↗](#)."
- Type**: Radio buttons for "Phone" (selected) and "Tablet".
- Phone number**: A text input field with a red arrow pointing to it. The field contains a dropdown menu with the Italian flag, a phone icon, and the number "02 123456789". To the right of the field is a link "Show extension field". Below the field, it says "Optional. Example: '+52 1 222 123 4567'".
- A blue "Add Phone" button circled in red at the bottom.

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

Alias	Device	Platform	Model	Security Warnings	
phone1		Android 10		✓ No warnings	<b>Activate Duo Mobile</b>

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 application mobile device or authenticate via Duo Push.

**Note:** Generating an activation code will invalidate any existing Duo Mobile credentials for this device.

Phone:

Expiration: 24 hours after generation

**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**.

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 mobile device or 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:

Send links via

SMS

**Email**

Email:

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:

[Redacted]

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

[Redacted]

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

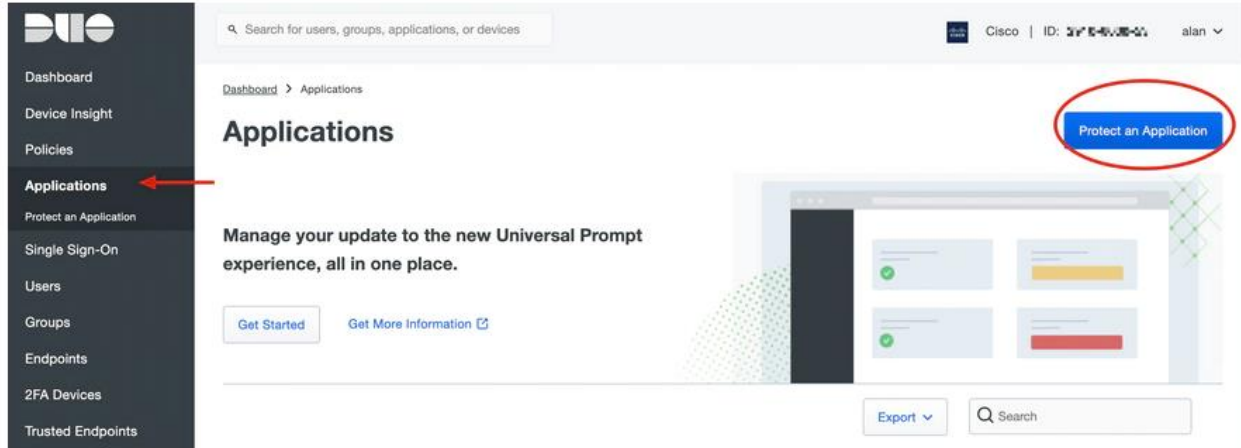
10. Open the Duo Mobile App from your mobile device and click **Add** then select **Use QR code** and scan the code from the instructions email.

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

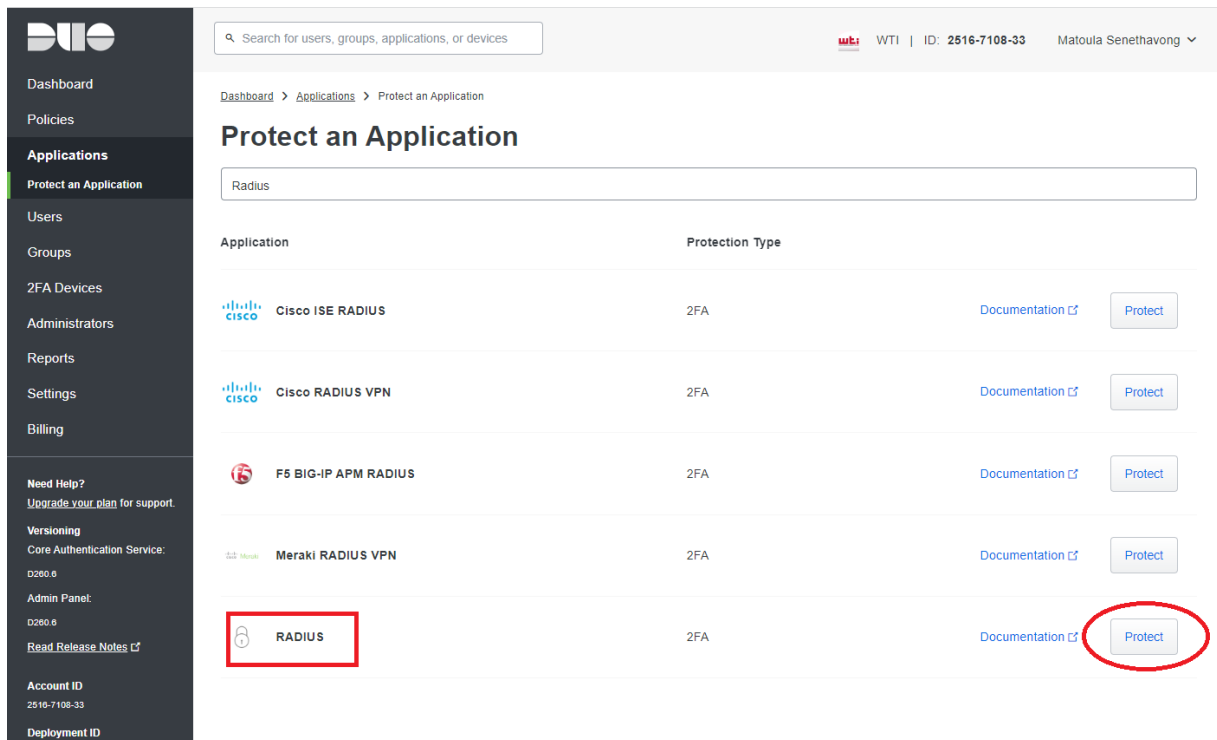
### **Duo Authentication Proxy Configuration**

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 Radius.



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

# RADIUS

See the [RADIUS documentation](#) to integrate Duo into your RADIUS-enabled platform.

## Details

Integration key

 Copy

Secret key

 Copy

Don't write down your secret key or share it with anyone.

API hostname

 Copy

5. Run the Duo Authentication Proxy manager application and complete the configuration for both Active Directory client 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

The screenshot shows the Duo Authentication Proxy Manager interface. At the top, it displays 'Authentication Proxy is running', 'Uptime: 02:28:58', and 'Version: 5.8.0'. A 'Restart Service' button is visible. Below this, a green checkmark indicates 'Validation passed' with the message 'Configuration has passed validation and is ready to be saved'. The main area is split into two panes: 'Configure: authproxy.cfg' and 'Output'. The configuration pane shows the following content:

```
16 [ad_client]
17 host=192.10.10.251
18 service_account_username=duouser
19 service_account_password=secret123
20 search_dn=DC=wt1devlab,DC=com
21 security_group_dn=CN=DuoAdmin,OU=Tech Support Groups,OU=Service,DC=wt1devlab,DC=com
22
23
24 [ldap_server_auto]
25 client=ad_client
26 ikey=
27 skey=
28 api_host=
29 failmode=safe
30
31
32
33
```

The output pane shows the following log messages:

```
Running The Duo Authentication Proxy Connectivity Tool. This may take several minutes...
[info] Testing section 'ad_client' with configuration:
[info] {'host': '192.10.10.251',
'search_dn': 'DC=wt1devlab,DC=com',
'security_group_dn': 'CN=DuoAdmin,OU=Tech Support
Groups,OU=Service,DC=wt1devlab,DC=com',
'service_account_password': 'secret123',
'service_account_username': 'duouser'}
[info] There are no configuration problems
[info]
[info] Testing section 'ldap_server_auto' with configuration:
[info] {'api_host': 'api-9601f5b1.duosecurity.com',
'client': 'ad_client',
'failmode': 'safe',
'ikey': 'D15J0Z2S1L4PDCG510I',
'skey': '*****[40]'}
[info] There are no configuration problems
```

Below is sample configuration of authproxy.cfg

- Primary authenticator, Windows Active Directory Server is on **192.10.10.251**
- Duo Authentication Proxy manager is on Windows Server **192.10.10.92**
- WTI Device is on **192.10.10.106**

```
[ad_client]
host=192.10.10.251
service_account_username=duouser
service_account_password=secret123
search_dn=DC=wt1devlab,DC=com
security_group_dn=CN=DUOAdmin,OU=Tech Support Groups,OU=Service,DC=wt1devlab,DC=com
```

```
[ldap_server_auto]
client=ad_client
ikey=XXXXXXXXXXXXXXXXXXXX
skey=YYYYYYYYYYYYYYYYYYYY
api_host=api-123456789.duosecurity.com
failmode=safe
```

### WTI LDAP client configuration

Log in into WTI device CLI, type /n and select 27 for LDAP

LDAP Setting:

1. Enable: **On**
2. Primary Host/Address: **192.10.10.92 (Your Duo Proxy Authentication IP Address)**
3. Secondary Host/Address: **(undefined)**
4. LDAP Port: **389**
5. TLS/SSL: **Off**
6. Bind Type: **Simple**
7. Search Bind DN: **CN=duouser,OU=testing,OU=Service,DC=wt1devlab,DC=com**
8. Search Bind Password: **(defined) (Bind DN user password)**
9. User Search Base DN: **DC=wt1devlab,DC=com**
10. User Search Filter: **sAMAccountName=%s**
11. Group Membership Attribute: **memberOf**
12. Group Membership Value Type: **DN**
13. Fallback: **On**
14. LDAP Group Setup **(you can add LDAP Group if any)**



15. LDAP Kerberos Setup
16. Debug: **Off**
17. Ping Test

```
LDAP: [Shared]
1.  Enable:                               On
2.  Primary Host/Address:                 192.10.10.92
3.  Secondary Host/Address:              (undefined)
4.  LDAP Port:                           389
5.  TLS/SSL:                              Off
6.  Bind Type:                            Simple
7.  Search Bind DN:                      CN=duouser,OU=testing,OU=Service,DC=wtid
                                          evlab,DC=com
8.  Search Bind Password:                 (defined)
9.  User Search Base DN:                  DC=wtidevlab,DC=com
10. User Search Filter:                   sAMAccountName=%s
11. Group Membership Attribute:           memberOf
12. Group Membership Value Type:          DN
13. Fallback:                             On
14. LDAP Group Setup
15. LDAP Kerberos Setup
16. Debug:                                Off
17. Ping Test

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