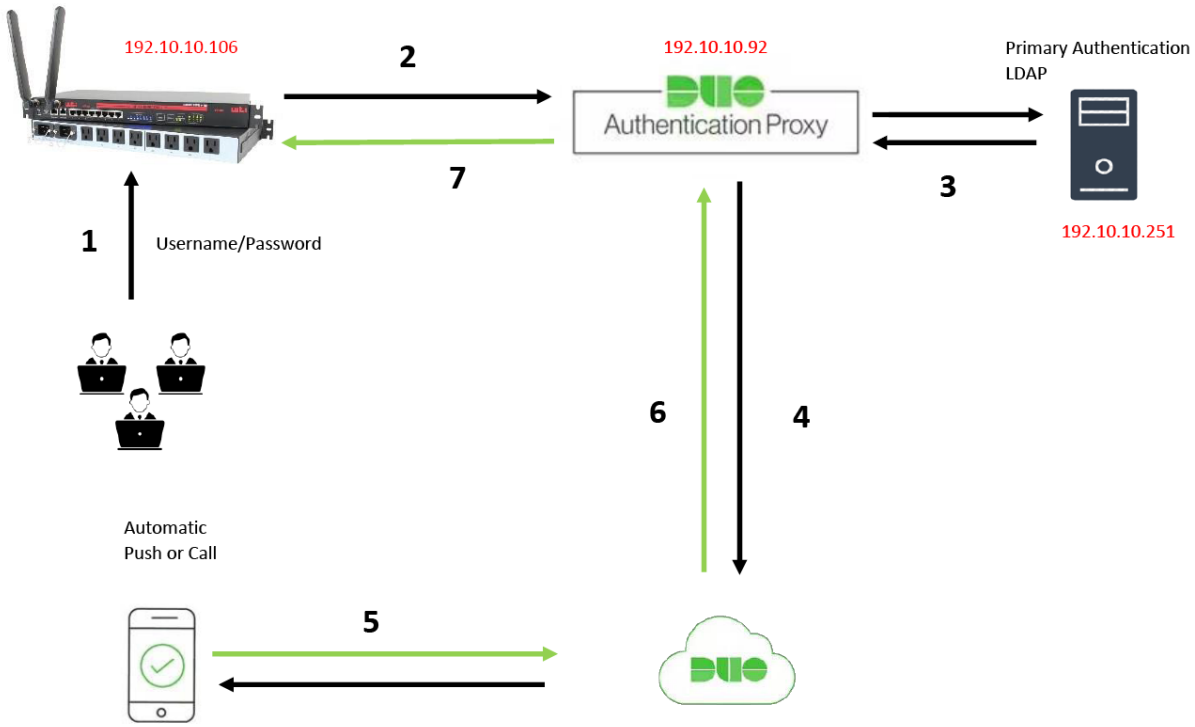
DUO Two Factor Authentication via LDAP WTI



Introduction

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

Components used

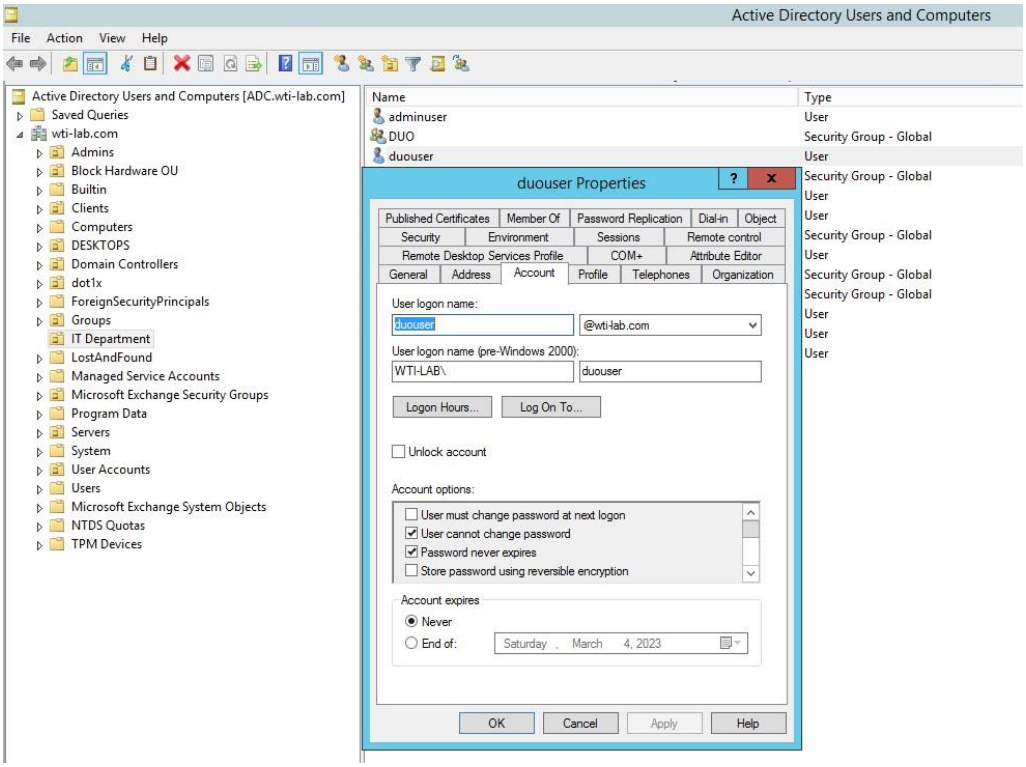
- Windows Active Directory
- Duo
- Duo Authentication Proxy Manager
- WTI LDAP client

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

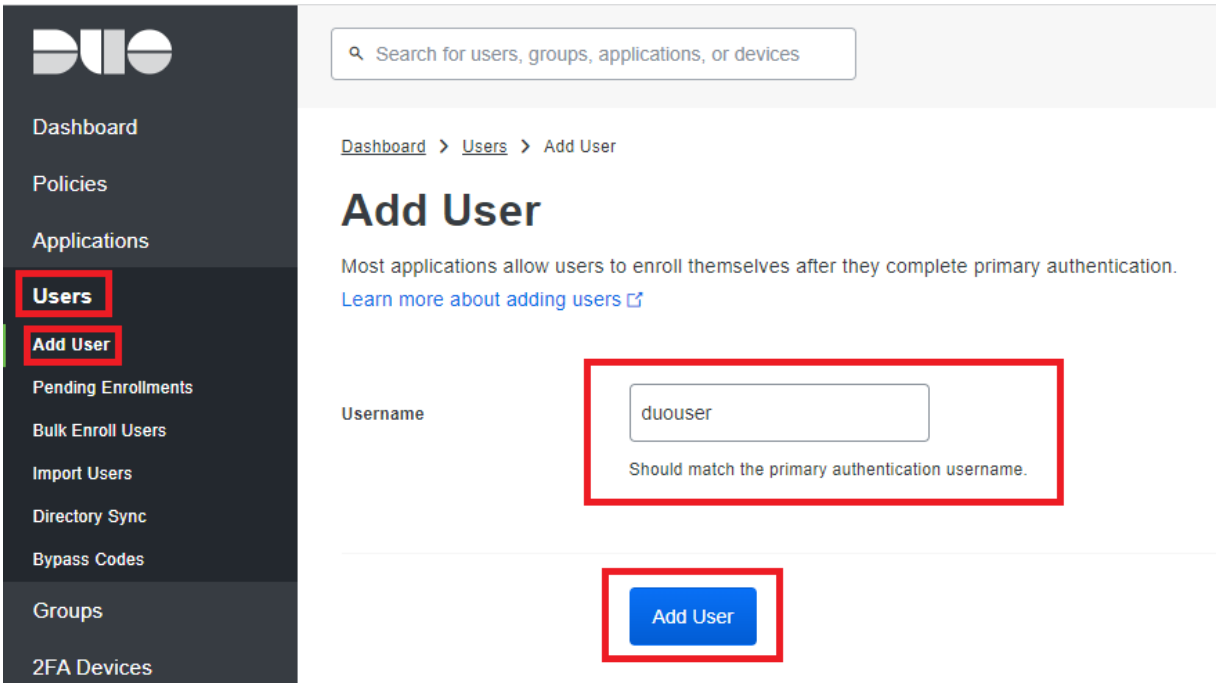
1. Navigate to Active Directory Users and Computers > Add new User and Password. In this example we created **duouser** account in active directory users and computers.



Duo configuration

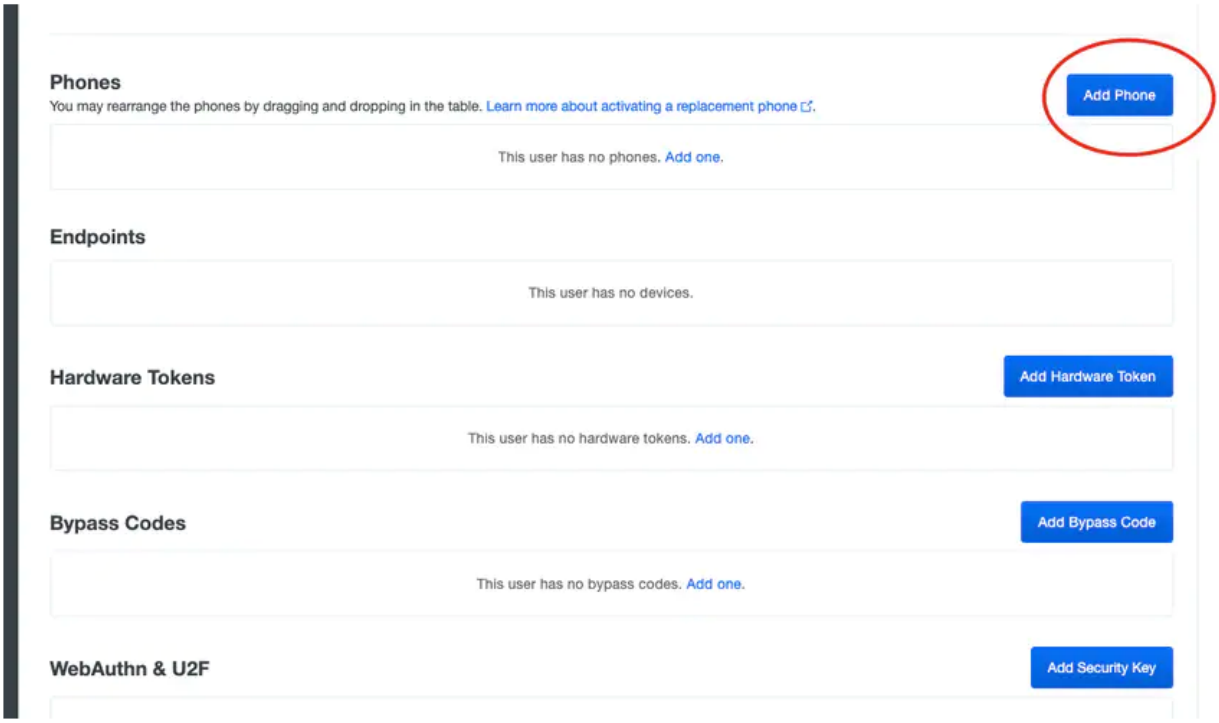
1. Log in into your Duo Admin portal

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.

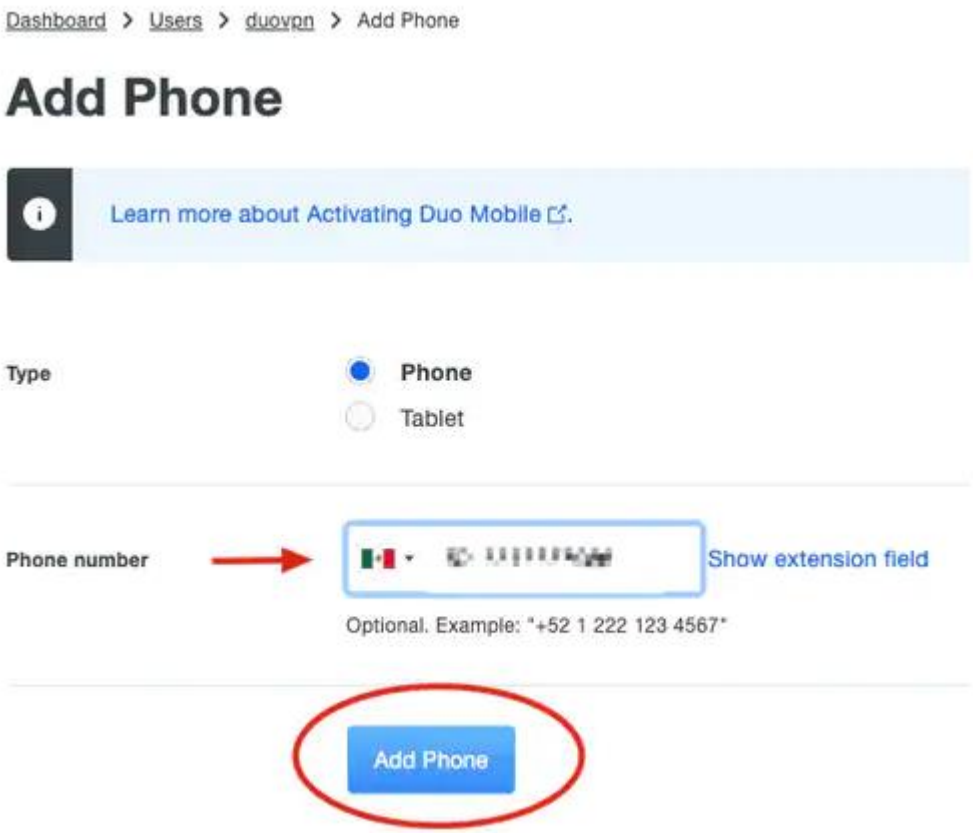


3. On the new user's panel, fill in the blank all the necessary information.

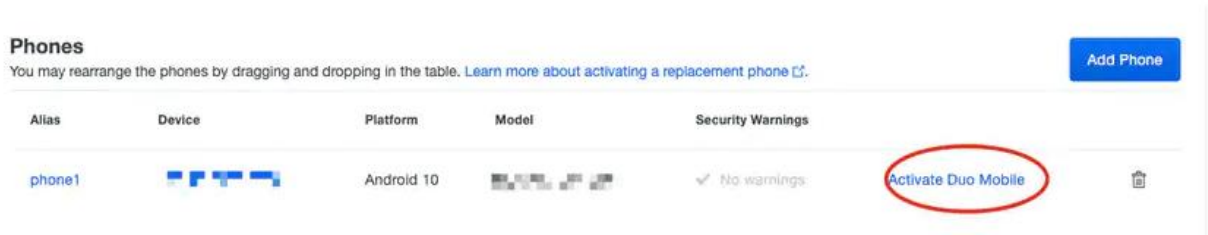
4. Under user devices specify the secondary authentication method. Click **Add Phone**



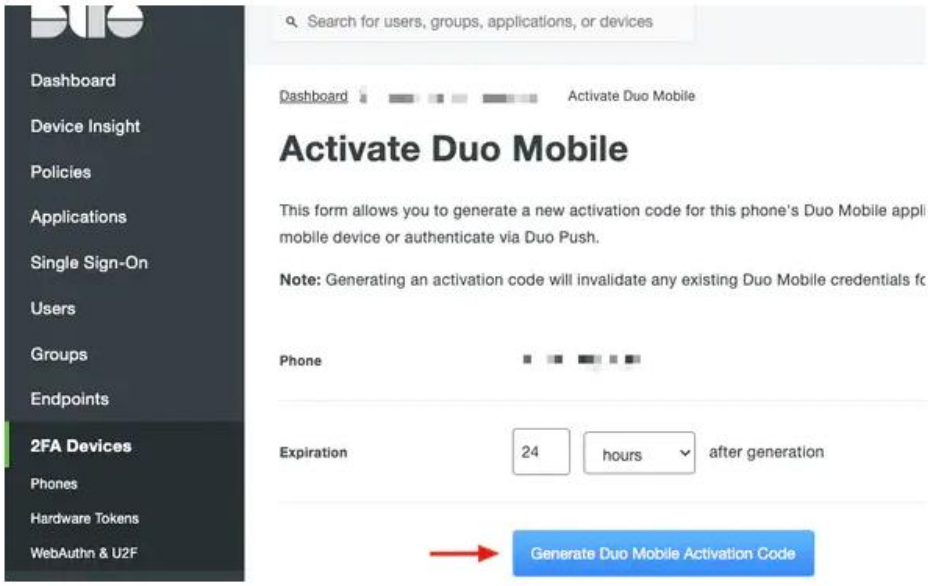
5. Type in the user's phone number and click **Add Phone**



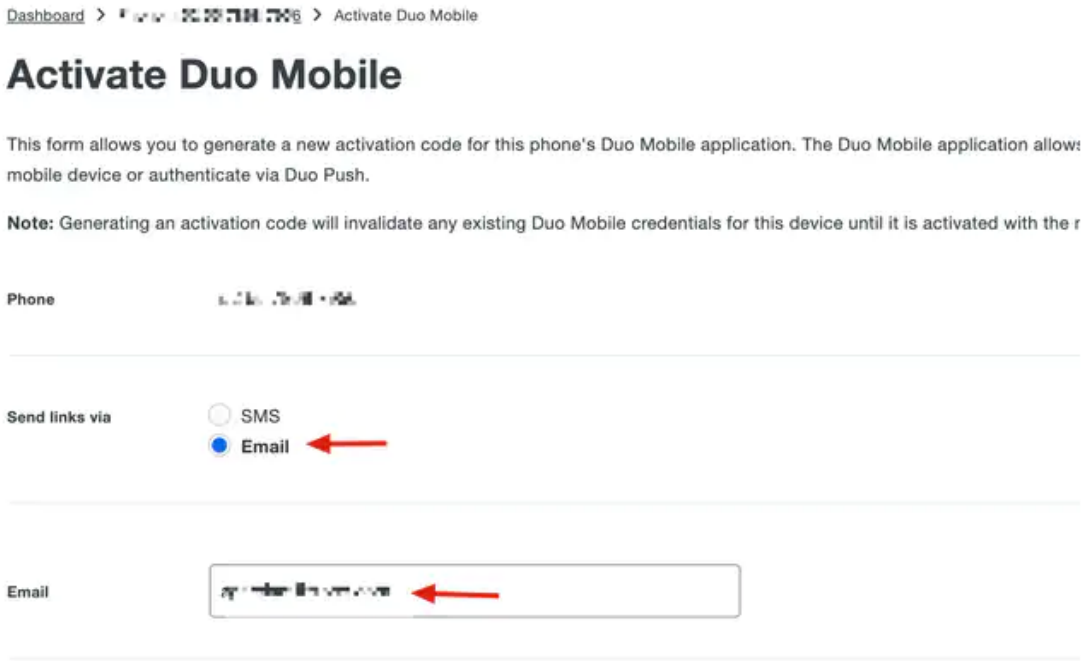
6. Navigate to **Phones** section and click **Activate Due Mobile**.



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

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] n 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

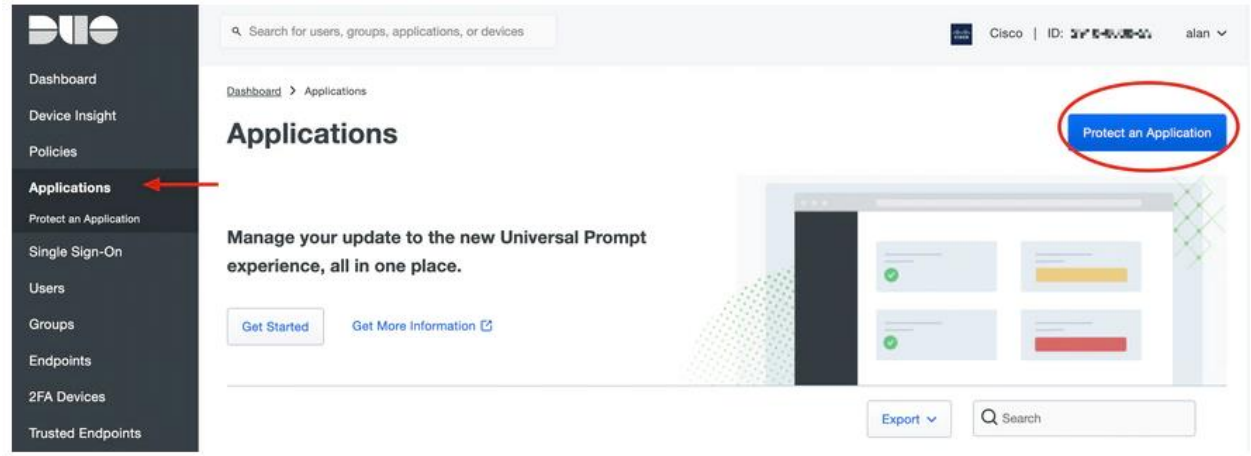
10. Open the Duo Mobile App from your mobile device and click **Add** then select **Use QR code** and scan the code from the instructions email.

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

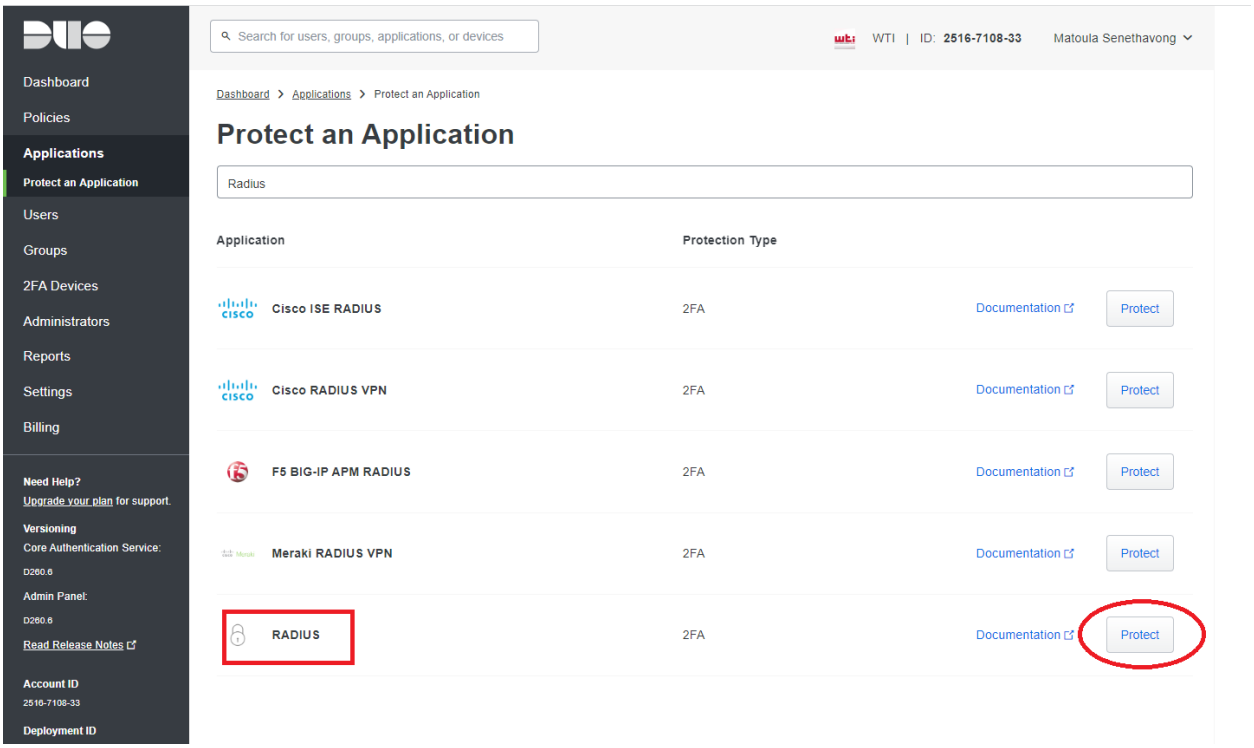
Duo Authentication Proxy Configuration

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

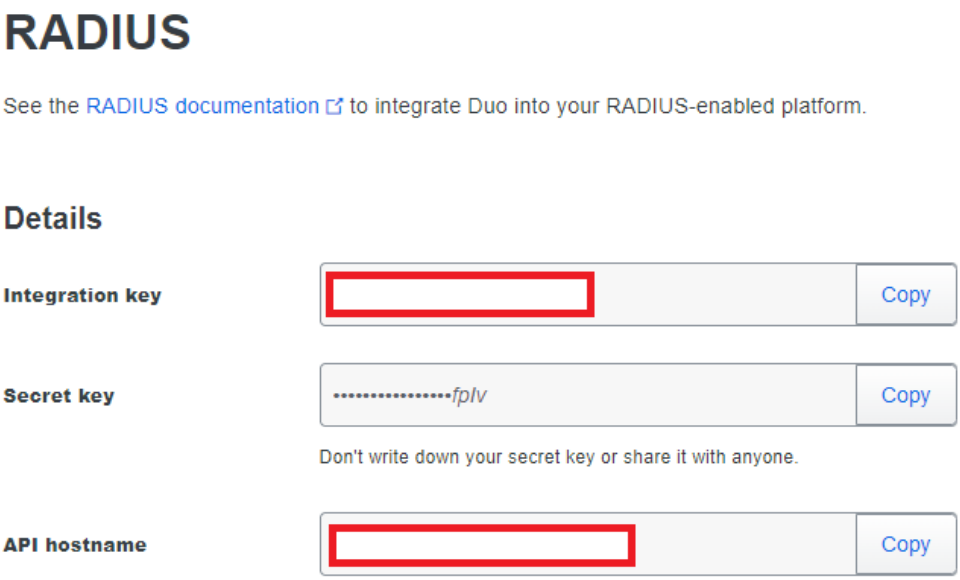
2. On the Duo Admin Panel navigate to **Applications** and click **Protect an Application**.



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.



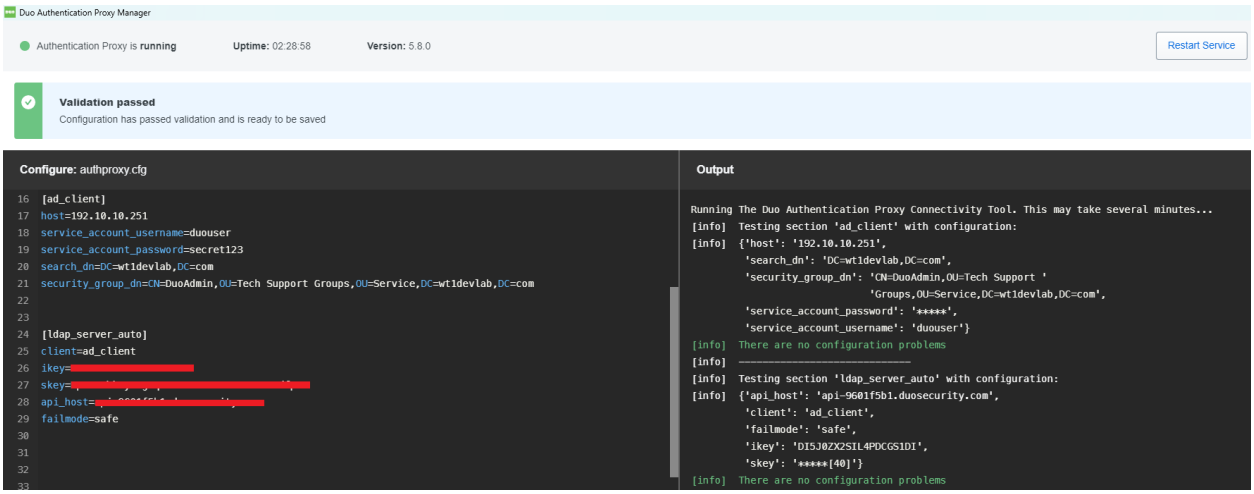
5. Run the Duo Authentication Proxy manager application and complete the configuration for both Active Directory client Radius server and click Validate.

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



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=XXXXXXXXXXXXXXXXX
skey=YYYYYYYYYYYYYYYYYY
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