

Configure Duo Integration with Active Directory and ISE for Two-Factor Authentication on Anyconnect/Remote Access VPN Clients

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Network Diagram and scenario](#)

[Communication process](#)

[Active Directory Configurations](#)

[Duo configurations](#)

[Duo Auth Proxy Configuration](#)

[Cisco ISE configurations](#)

[Cisco ASA RADIUS/ISE configuration](#)

[Cisco ASA Remote Access VPN configuration](#)

[Test](#)

[Troubleshoot](#)

[Work Debugs](#)

Introduction

This document describes Duo push integration with AD and ISE as Two-Factor Authentication for AnyConnect clients connected to ASA.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- RA VPN configuration on ASA
- RADIUS configuration on ASA
- ISE
- Active Directory
- Duo applications

Components Used

The information in this document is based on these software and hardware versions:

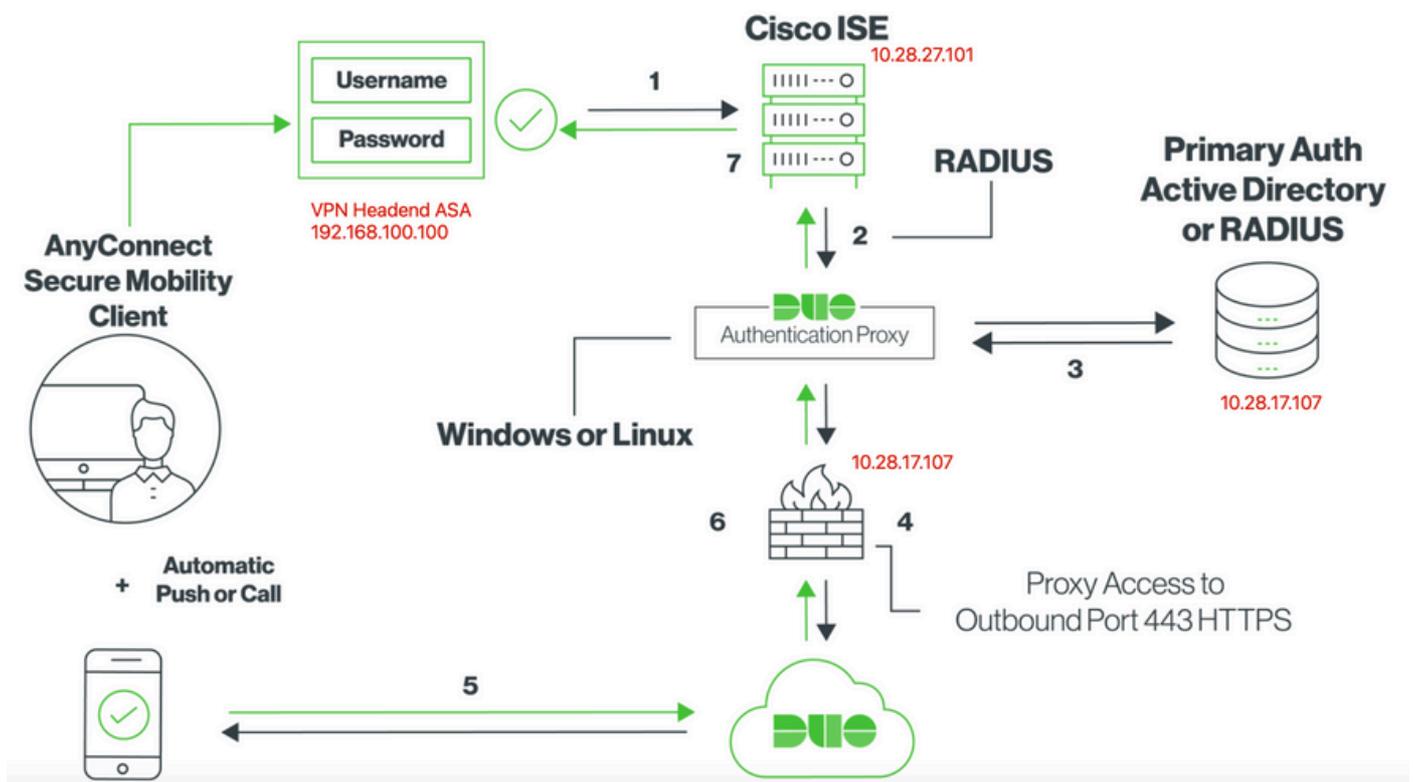
- Microsoft 2016 Server
- ASA 9.14(3)18
- ISE Server 3.0
- Duo Server
- Duo Authentication Proxy Manager

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document describes how to configure Duo push integration with Active Directory (AD) and Cisco Identity Service Engine (ISE) as Two-Factor Authentication for AnyConnect clients that connect to Cisco Adaptive Security Appliance (ASA).

Network Diagram and scenario



Communication process

<https://duo.com/docs/ciscoise-radius>

1. Primary authentication initiated to Cisco ISE
2. Cisco ASA sends authentication request to the Duo Authentication Proxy
3. Primary authentication uses Active Directory or RADIUS
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 access granted

User Accounts:

- Active Directory Admin: This is used as the directory account to allow the Duo Auth Proxy to bind to the Active Directory server for primary authentication.
- Active Directory test user
- Duo test user for secondary authentication

Active Directory Configurations

Windows server is pre-configured with Active Directory Domain services.

 **Note:** If RADIUS Duo Auth Proxy Manager runs on the same Active Directory host machine, Network Policy Server (NPS) Roles must be uninstalled/deleted, if both RADIUS services run, they can conflict and impact performance.

In order to achieve AD configuration for authentication and user identity on Remote Access VPN users, a few values are required.

All these details must be created or collected on the Microsoft Server before configuration can be done on the ASA and Duo Auth proxy server.

The main values are:

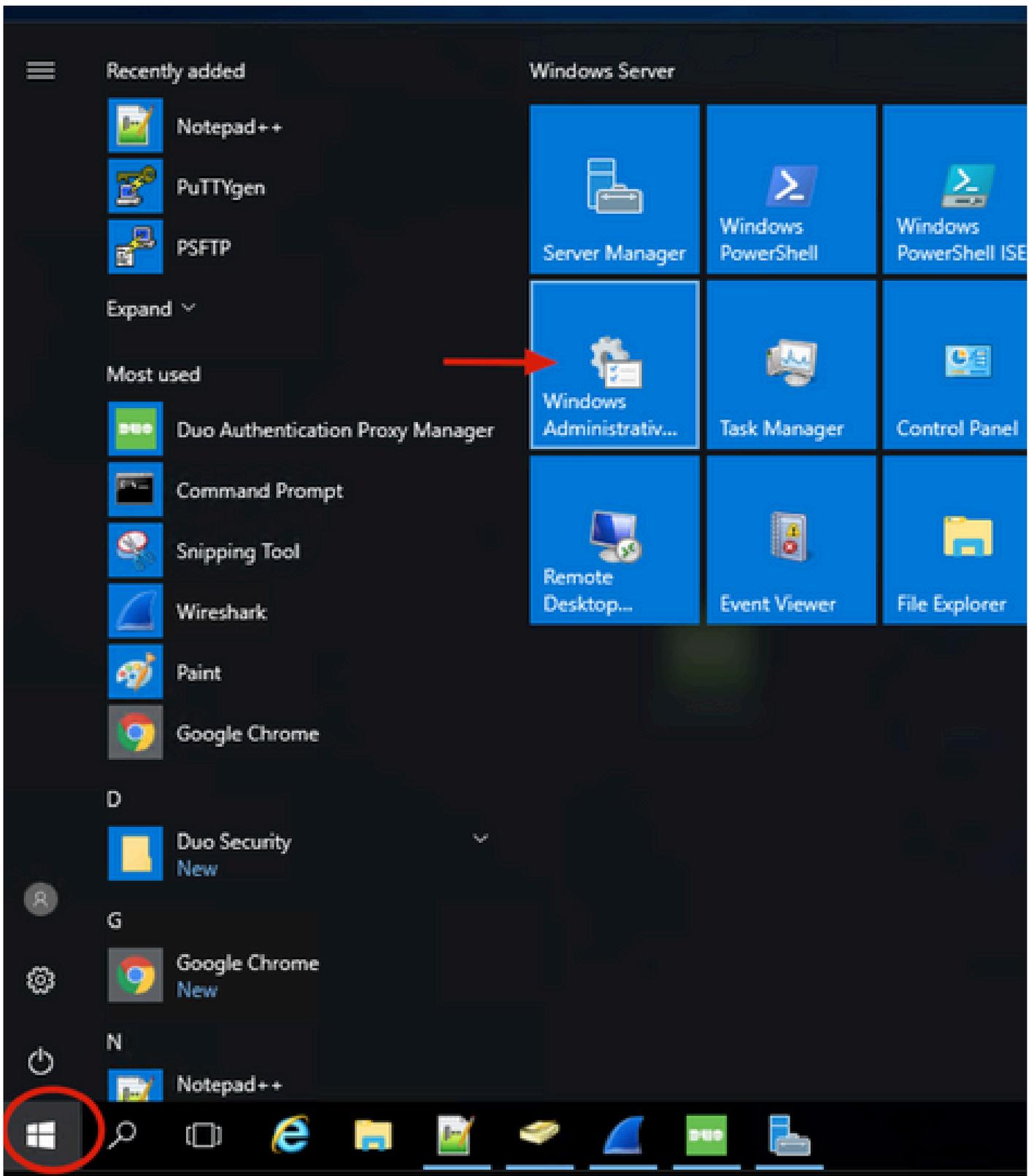
- Domain Name. This is the domain name of the server. In this configuration guide, agarciam.cisco is the domain name.
- Server IP/FQDN Address. The IP address or FQDN used to reach the Microsoft server. If an FQDN is used, a DNS server must be configured within ASA and Duo Auth proxy to resolve the FQDN.

In this configuration guide, this value is agarciam.cisco (which resolves to 10.28.17.107).

- Server port. The port used by the LDAP service. By default, LDAP and STARTTLS uses TCP port 389 for LDAP, and LDAP over SSL (LDAPS) uses TCP port 636.
- Root CA. If LDAPS or STARTTLS is used, the root CA used to sign the SSL certificate used by LDAPS is required.
- Directory Username and Password. This is the account used by Duo Auth proxy server to bind to the LDAP server and authenticate users and search for users and groups.
- Base and Group Distinguished Name (DN). The Base DN is the point of departure for Duo Auth proxy and it tells the Active directory to begin the search for and authenticate users.

In this configuration guide, the root domain agarciam.cisco is used as the Base DN and Group DN is Duo-USERS.

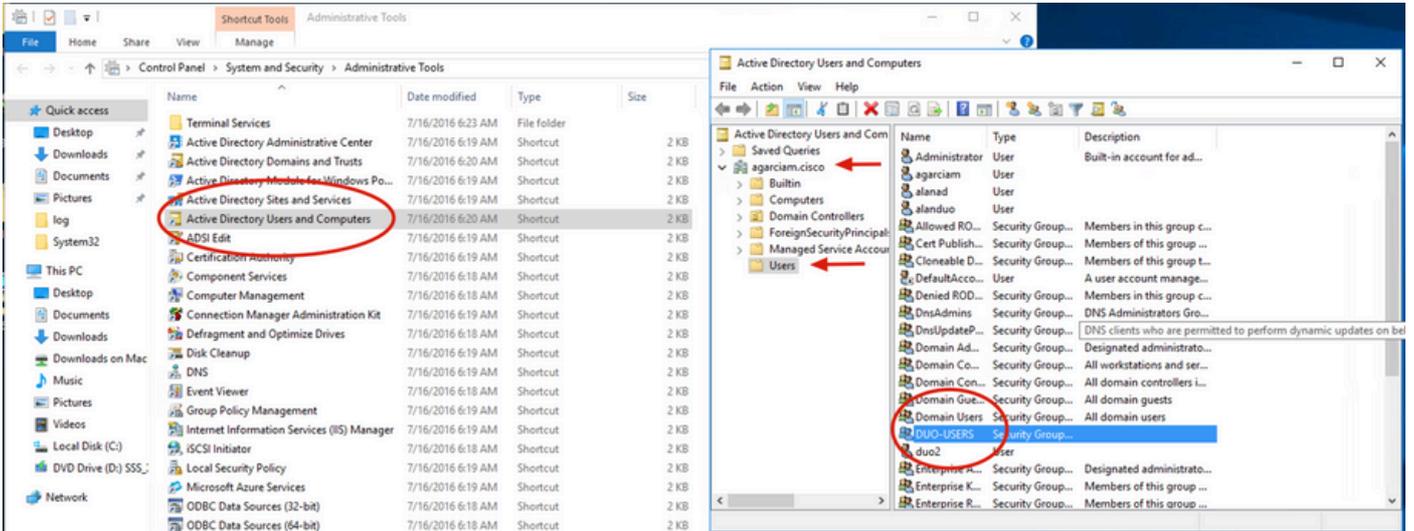
1. In order to add a new Duo user, on Windows Server, navigate to **Windows** icon at the bottom left and click **Windows Administrative tools**, as shown in the image.



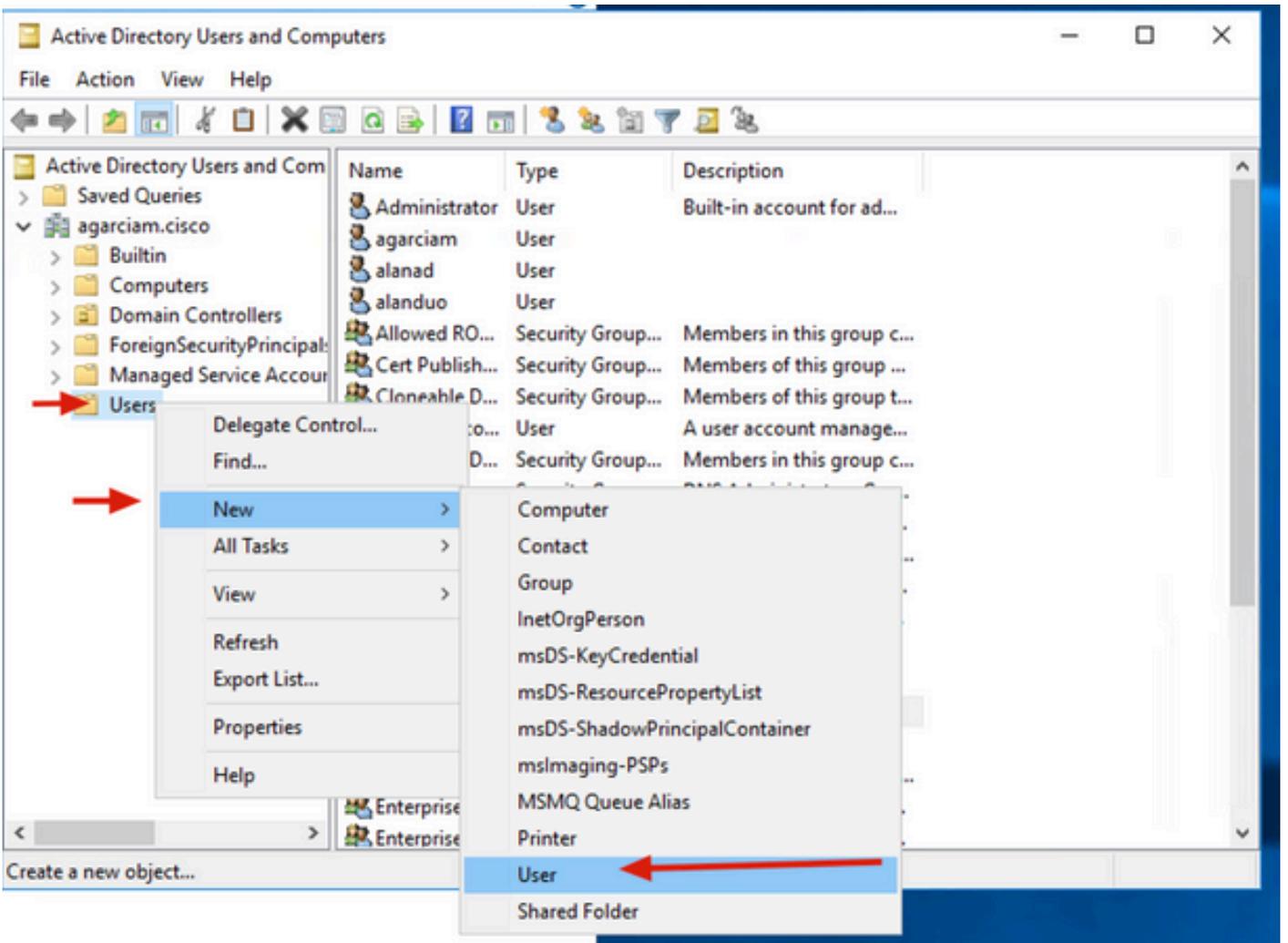
2. On Windows Administrative tools window navigate to **Active Directory Users and Computers**.

On the Active Directory Users and Computers panel, expand the domain option and navigate to **Users** folder.

In this configuration example Duo-USERS is used as the target group for secondary authentication.



3. Right click on the **Users** folder and select **New > User**, as shown in the image.



4. On the New Object-User window, specify the identity attributes for this new user and click **Next**, as shown in the image.

New Object - User ✕

 Create in: `agarciam.cisco/Users`

First name:  Initials:

Last name:

Full name:

User logon name:
  ▼

User logon name (pre-Windows 2000):

5. Confirm password and click **Next**, then **Finish** once user information is verified.

New Object - User X

 Create in: agarciam.cisco/Users

Password: ←

Confirm password: ←

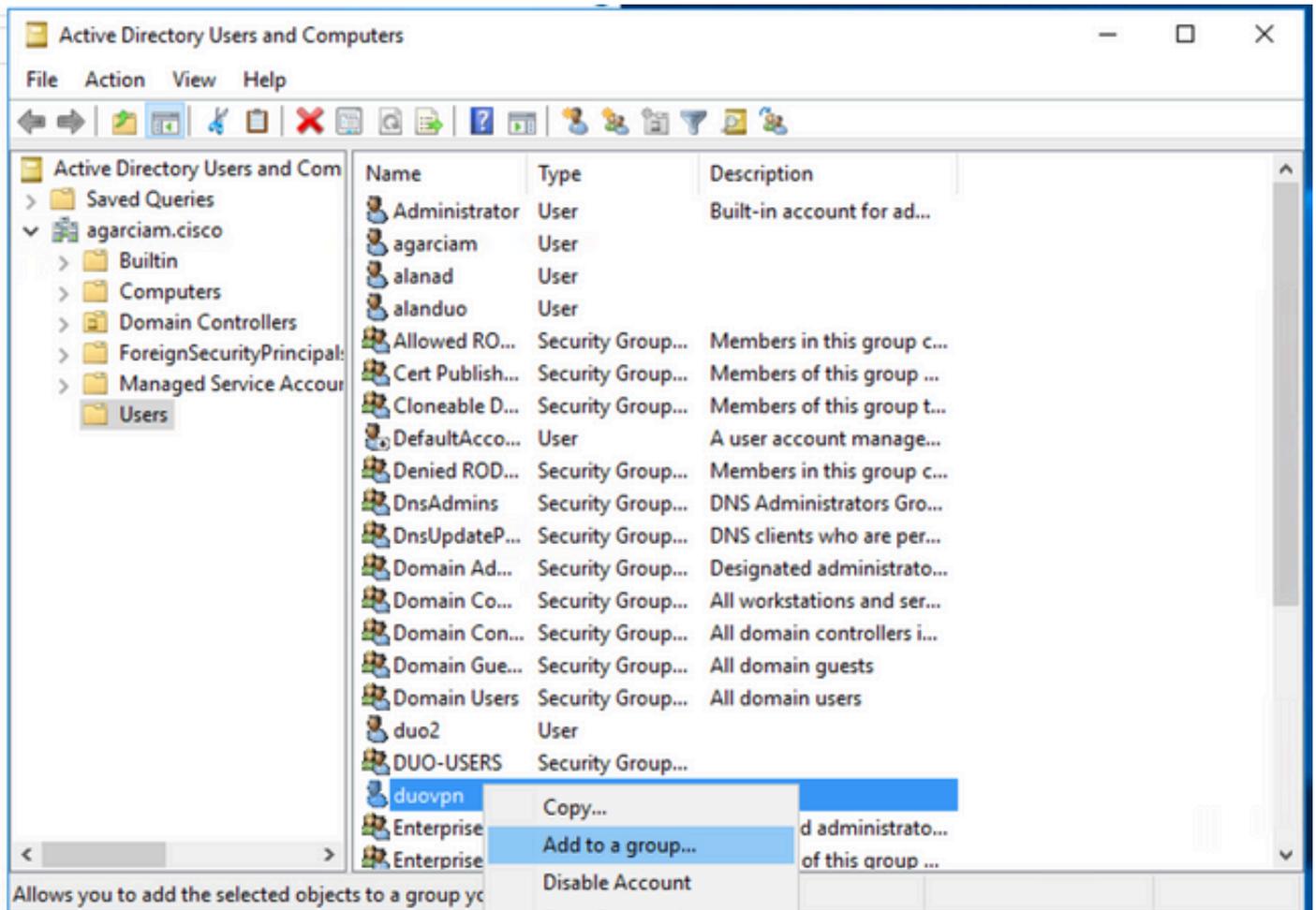
User must change password at next logon

User cannot change password

Password never expires

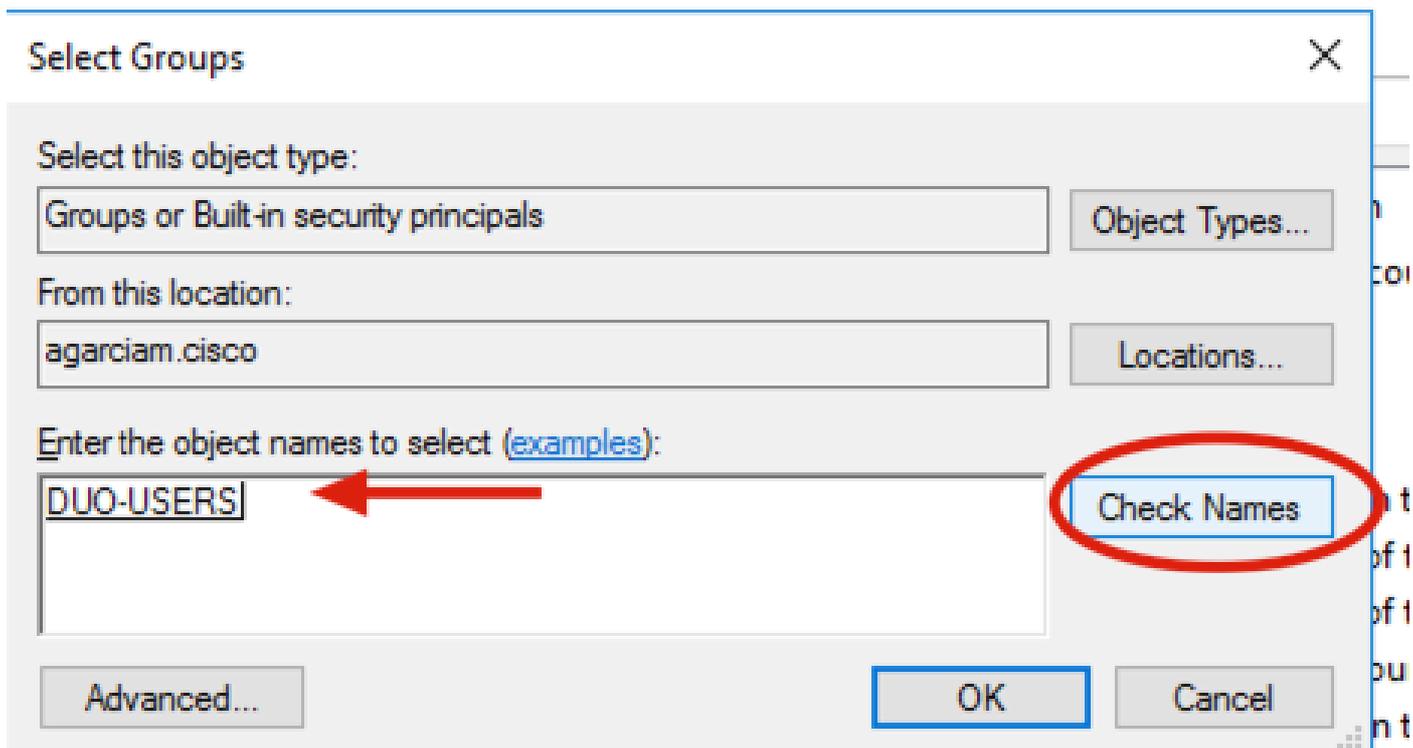
Account is disabled

6. Assign the new user to an specific group, right click it and select **Add to a group**, as shown in the image.



7. On the Select groups panel, type the name of the desired group and click **Check names**.

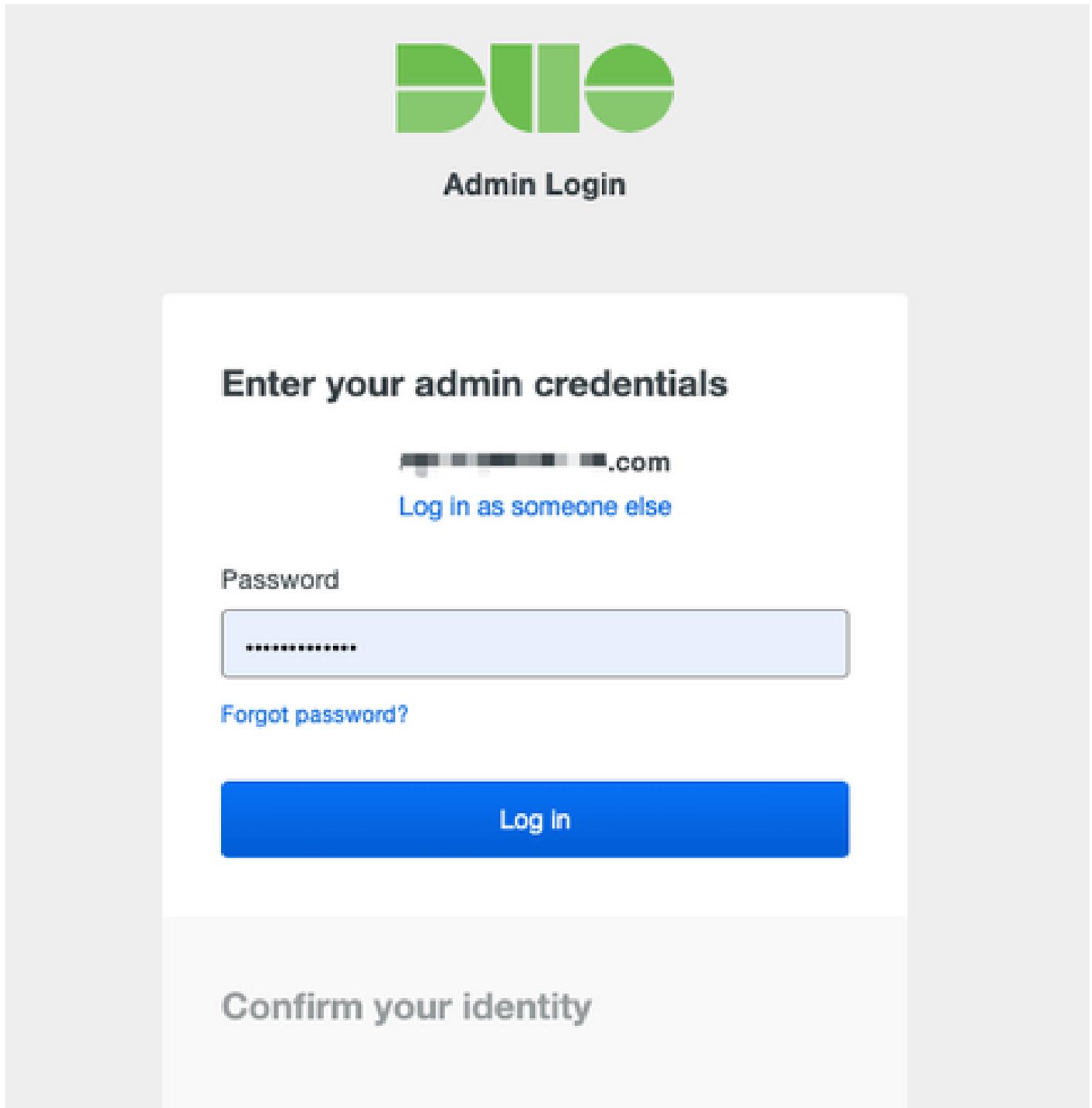
Then select the name that matches your criteria and click **Ok**.



8. This is the user that is used on this document as an example.

Duo configurations

1. Log in into your Dudo Admin portal.



DUDO

Admin Login

Enter your admin credentials

██████████.com

[Log In as someone else](#)

Password

[Forgot password?](#)

Log In

Confirm your identity

2. On the left side panel, navigate to **Users**, click **Add User** and type the name of the user that matches our Active Domain username, then click **Add User**.

DUO

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 panel, fill in the blank all the necessary information.

- Policies
- Applications
- Single Sign-On
- Users**
 - Add User
 - Pending Enrollments
 - Bulk Enroll Users
 - Import Users
 - Directory Sync
 - Bypass Codes
- Groups
- Endpoints
- 2FA Devices
- Trusted Endpoints
- Trust Monitor
- Reports
- Settings
- Need Help?**
 - [Chat with Tech Support](#)
 - [Email Support](#)
 - Call us at 1-855-386-2884
- Versioning**
 - Core Authentication Service:
 - D235.6
 - Admin Panel:
 - D235.6
 - [Read Release Notes](#)
- Account ID**
 - 2910-6030-53
- Deployment ID**
 - DUO63
- Helpful Links**
 - [Documentation](#)
 - [User Guide](#)
 - [Knowledge Base](#)

duovpn

i This user has not enrolled yet. See our [enrollment documentation](#) to learn more about enrolling users.

Username ←

Username aliases [+ Add a username alias](#)
 Users can have up to 8 aliases. Optionally, you may choose to reserve using an alias number for a specific alias (e.g., Username alias 1 should only be used for Employee ID).

Full name ←

Email

Status

- Active** ←
Require multi-factor authentication (default).
- Bypass**
Allow users to skip two-factor authentication and log in with only a password. Passwordless authentication is not skipped.
- Disabled**
Automatically deny access

This controls the user's two-factor authentication process.

Groups You don't have any editable groups. [Add one.](#)
 Groups can be used for management, reporting, and policy. [Learn more about groups](#)

Notes

For internal use.

4. Under user devices specify the secondary authentication method.

 **Note:** In this document Duo push for mobile devices method is used, so a phone device needs to be added.

Click **Add Phone**.

Phones

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

Add 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 phone number and click **Add Phone**.

Add Phone



[Learn more about Activating Duo Mobile](#)

Type

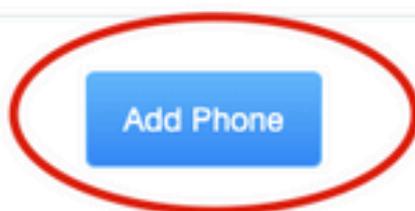
- Phone
- Tablet

Phone number



[Show extension field](#)

Optional. Example: "+52 1 222 123 4567"



6. On the left Duo Admin panel, navigate to **Users** and click the new user.

Dashboard > Users

Users

Directory Sync | Import Users | Bulk Enroll Users [Add User](#)

i You have users who have not activated Duo Mobile. [Click here to send them activation links.](#)
Need to activate a replacement phone? [Learn more about Reactivating Duo Mobile](#).

5 Total Users **0** Not Enrolled **2** Inactive Users **1** Trash **0** Bypass Users **0** Locked Out

Select (0) ... [Export](#) Search

<input type="checkbox"/>	Username	Name	Email	Phones	Tokens	Status	Last Login
<input type="checkbox"/>	duovpn		...@...i.com	1		Active	Mar 8, 2022 6:50 PM
<input type="checkbox"/>				1		Active	Mar 5, 2022 7:04 PM
<input type="checkbox"/>				1		Active	Never authenticated
<input type="checkbox"/>	duovpn		...@...o.com	1		Active	Mar 5, 2022 7:16 PM

 **Note:** In case you don't have access to your phone at the moment, you can select the email option.

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

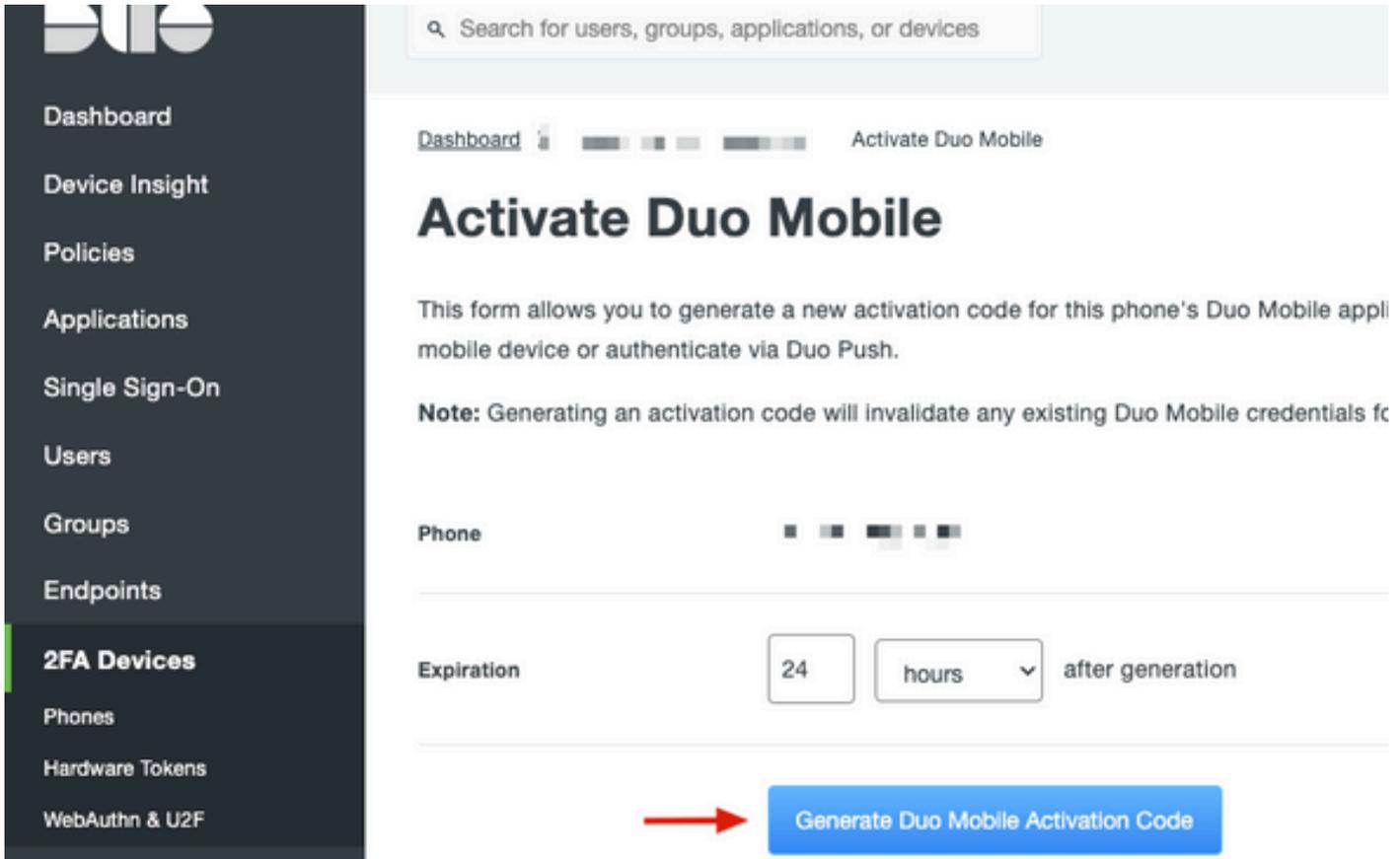
Phones

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

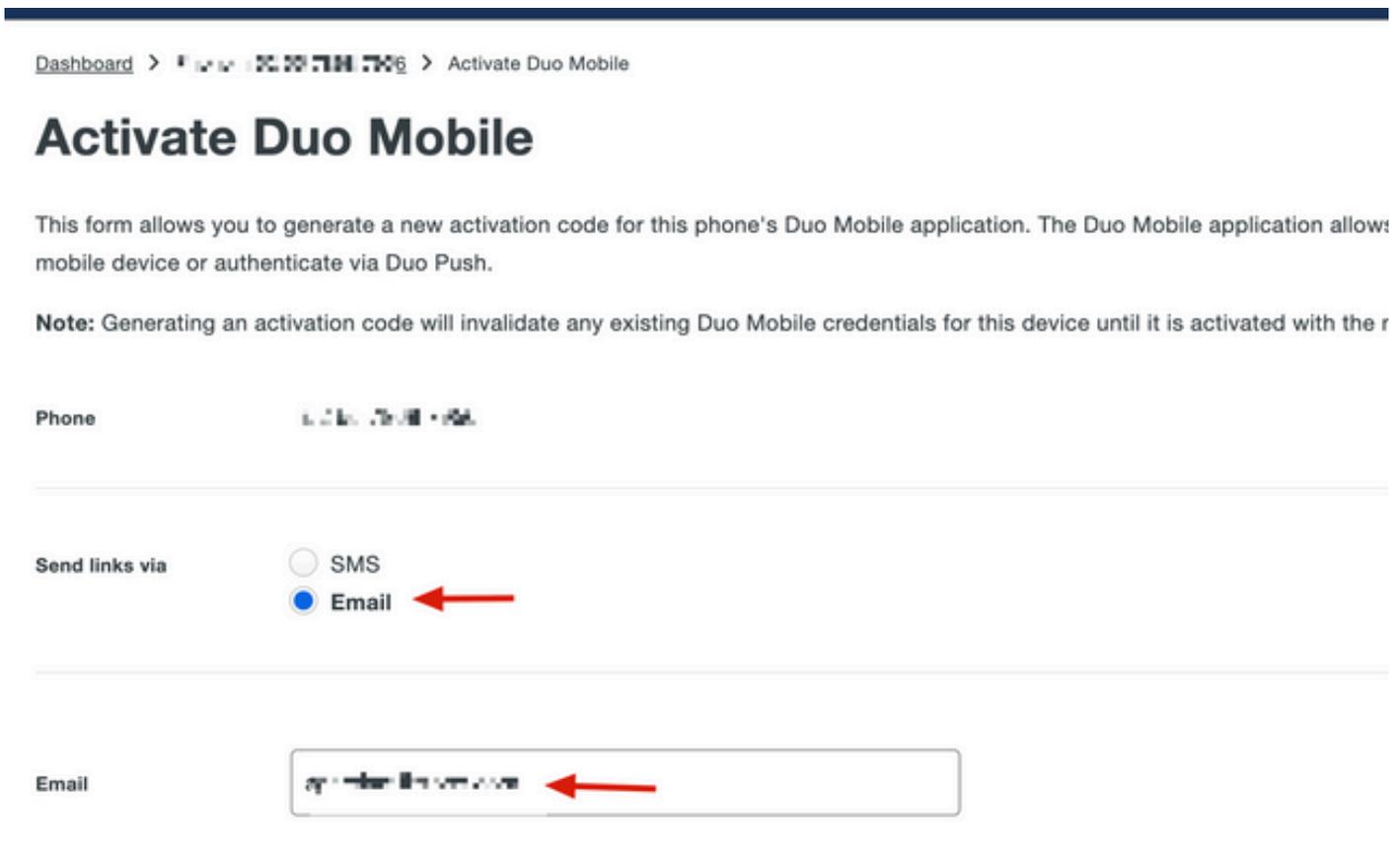
[Add Phone](#)

Alias	Device	Platform	Model	Security Warnings	
phone1		Android 10		✓ No warnings	Activate Duo Mobile 

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



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



10. You receive an email with the instructions, as shown 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>

11. 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.

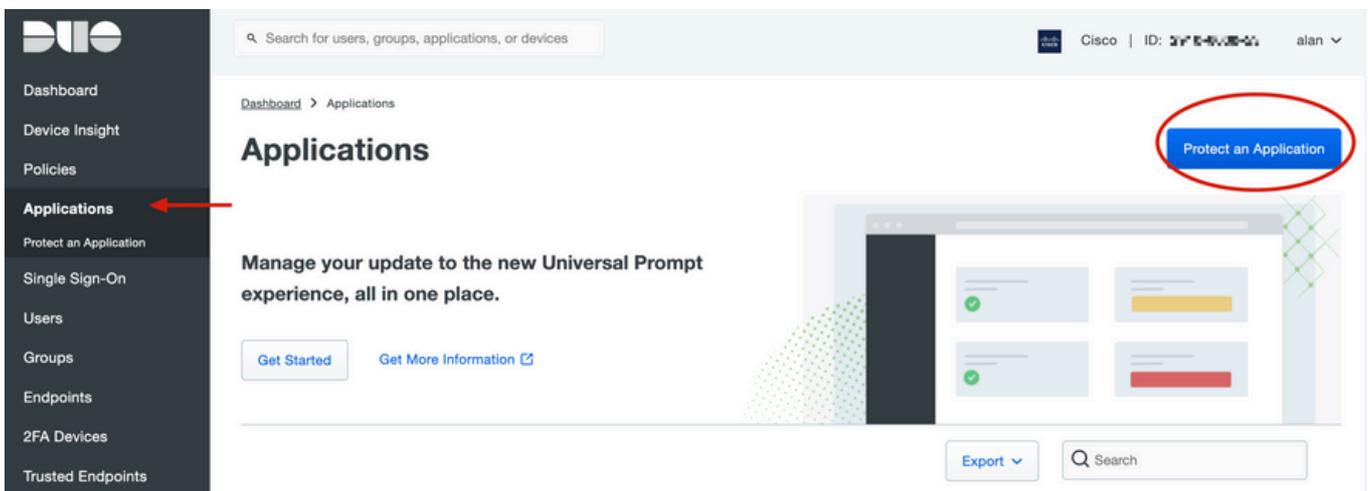
12. New user is added to your Duo Mobile App.

Duo Auth Proxy Configuration

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

 **Note:** On this document the Duo Auth Proxy Manager is installed on the same Windows Server that hosts Active Directory services.

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

i Add an application that you'd like to protect with Duo two-factor authentication. You can start with a small "proof-of-concept" installation — it takes just a few minutes, and you're the only one that will see it, until you decide to add others.

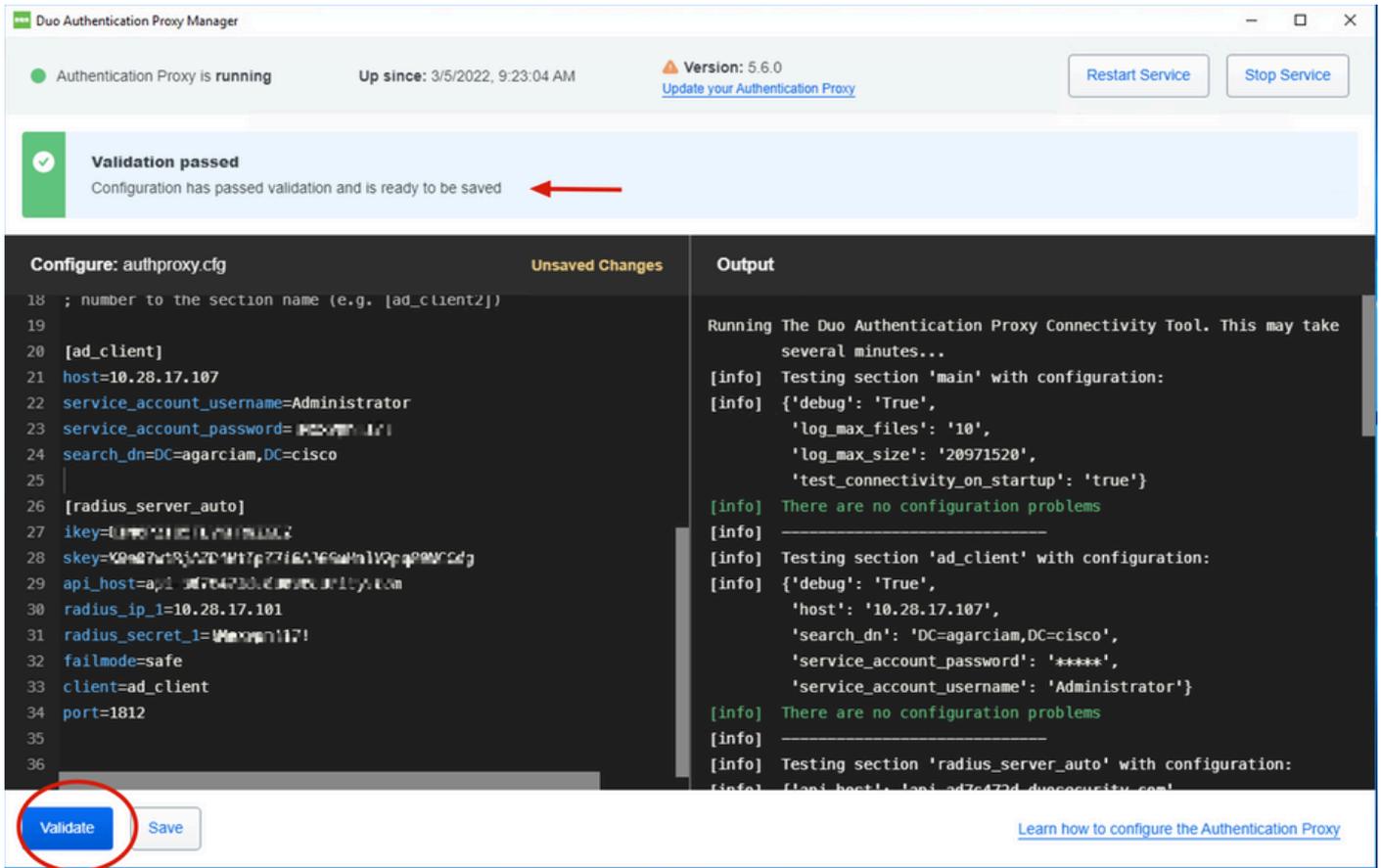
Documentation: [Getting Started](#)

Choose an application below to get started.

ise

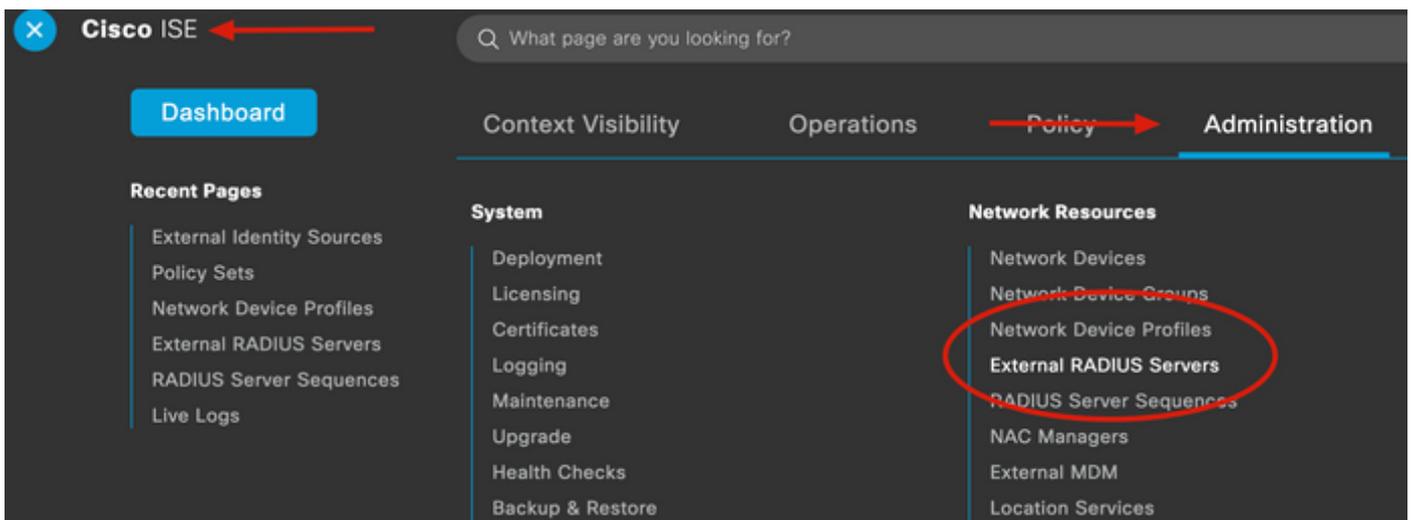
Application	Protection Type	
 Akamai Enterprise Application Access	2FA	Documentation Protect
 Cisco ISE RADIUS 	2FA	Documentation Protect

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

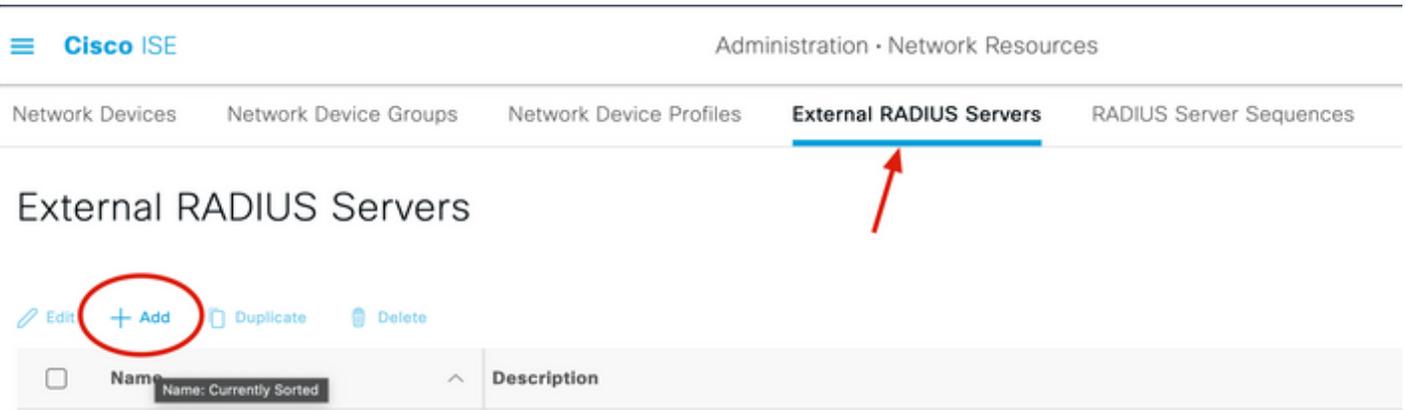


Cisco ISE configurations

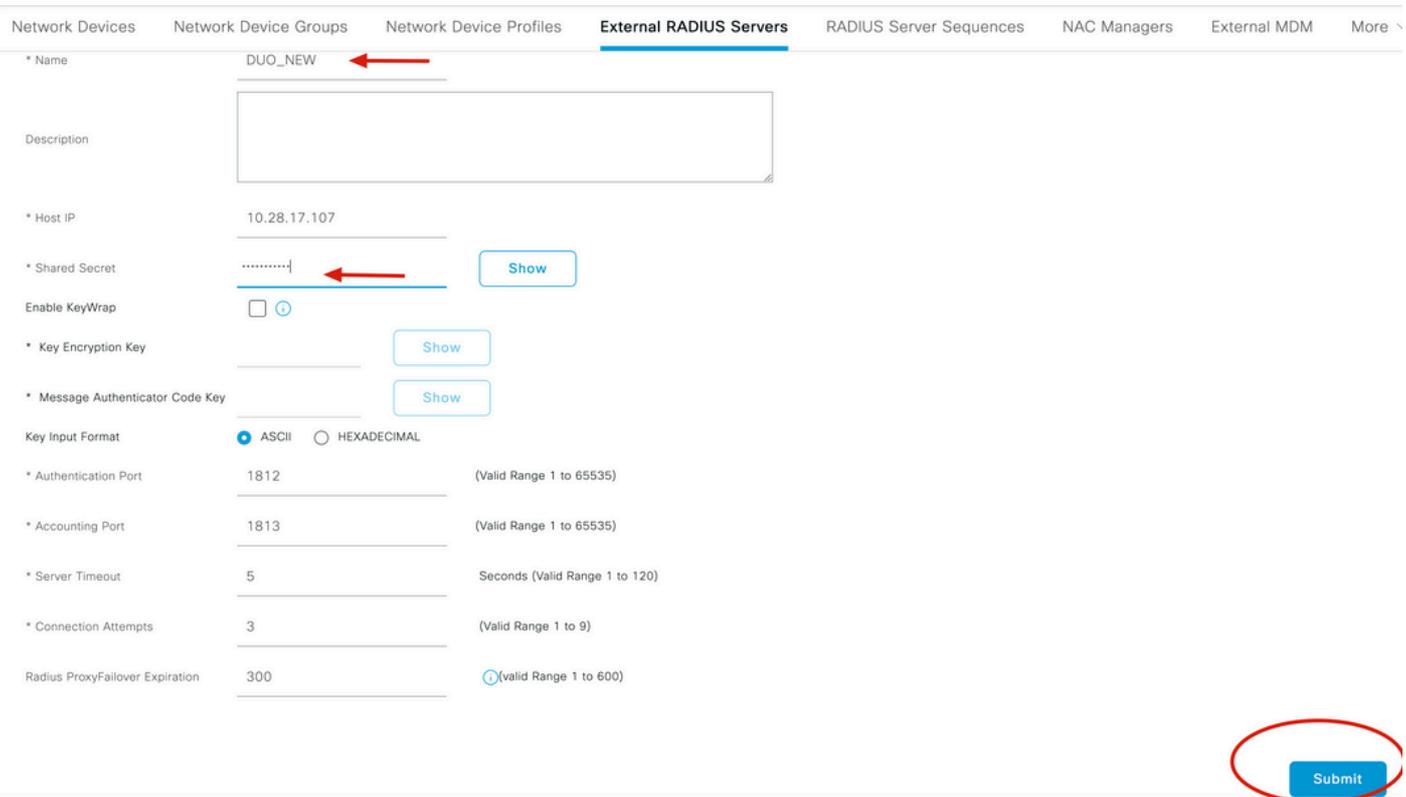
1. Log in into the ISE Admin portal.
2. Expand Cisco ISE tab and Navigate to **Administration** then click **Network Resources** and click **External RADIUS Servers**.



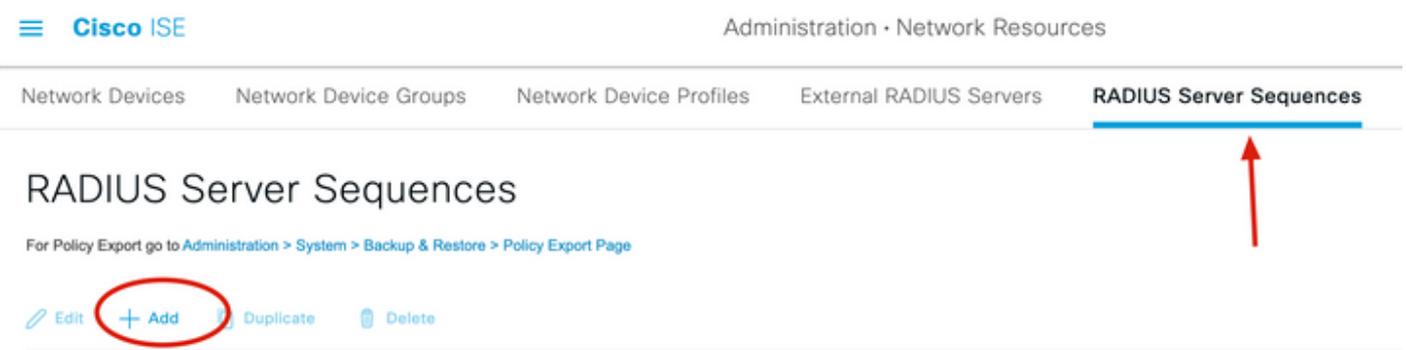
3. On **External Radius Servers** tab, click **Add**.



4. Fill in the blank with the RADIUS configuration used in the Duo Authentication Proxy Manager and click **Submit**.



5. Navigate to **RADIUS Server Sequences** tab and click **Add**.



6. Specify the name of the sequence and assign the new RADIUS External server, click **Submit**.

RADIUS Server Sequence

General

Advanced Attribute Settings

* Name

DUO_Sequence

Description

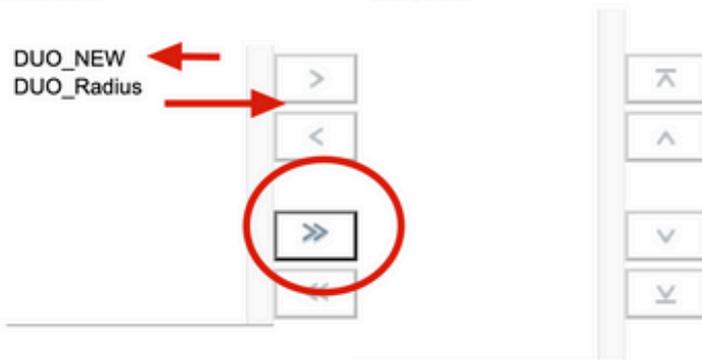
User Selected Service Type

Select the set of external RADIUS servers to use to process requests. Servers are accessed in sequence until a response is received.

Available

* Selected

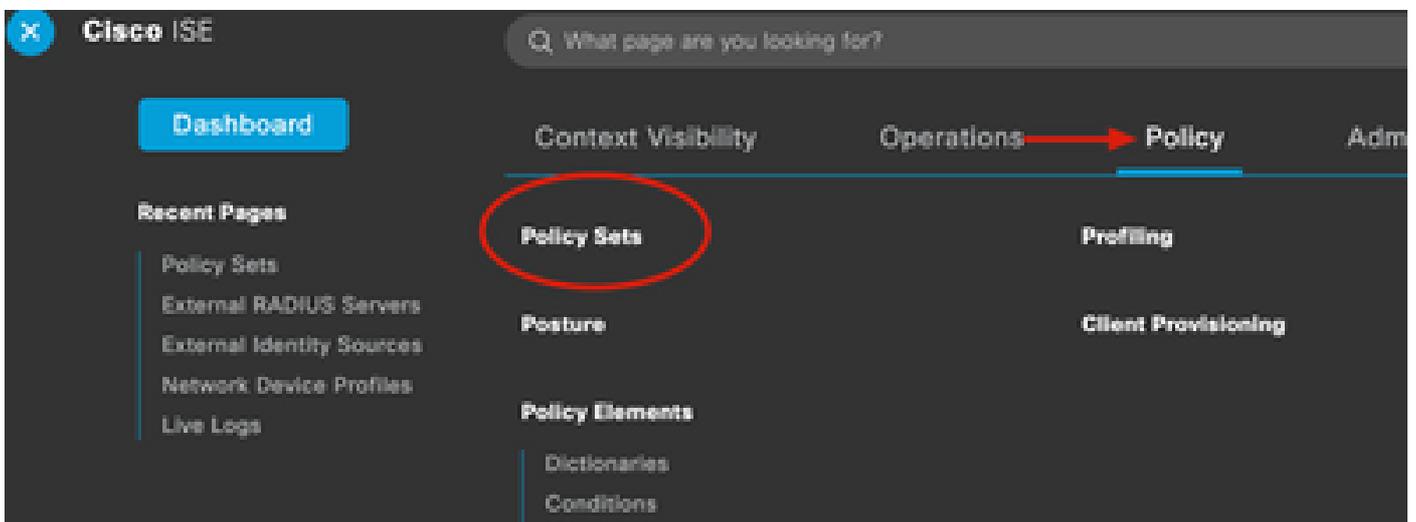
DUO_NEW
DUO_Radius



Remote accounting

Local accounting

7. Navigate from the Dashboard menu to **Policy** and click **Policy Sets**.



8. Assign the RADIUS Sequence to the default policy.

 **Note:** In this document, the Duo sequence to all of the connections is applied, so Default policy is used. Policy assignment can vary as per requirements.

Policy Sets Reset [Reset Policyset Hitcount](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓			Radius-User-Name EQUALS isevpn	Default Network Access  	3
✓			Radius-NAS-Port-Type EQUALS Virtual	DUO_Sequence  	22
✓	Default	Default policy set		Default Network Access  	0

Allowed Protocols

- Default Network Access
- Proxy Sequence
- DUO_NEW
- DUO_Sequence**

Cisco ASA RADIUS/ISE configuration

1. Configure ISE RADIUS Server under AAA Server groups, navigate to **Configuration** then click **Device Management** and expand the **Users/AAA** section, select **AAA Server Groups**.

Bookmarks

To bookmark a page, right-click on a node in the navigation tree and select "Add to bookmarks".

Go Delete

Configuration

AAA Server Groups

Server Group	Pro
ISE	RA
LOCAL	LO
ad-agarciam	LD

Device Management

- > Management Access
- > Licensing
- > System Image/Configuration
- > High Availability and Scalability
- > Logging
- Smart Call-Home
- Cloud Web Security
- Service Module Settings
- Users/AAA
 - AAA Server Groups
 - LDAP Attribute Map
 - AAA Kerberos
 - Authentication Prompt
 - AAA Access
 - Dynamic Access Policies
 - User Accounts
 - Password Policy
 - Change My Password
 - Login History
- > Certificate Management
- > DHCP
- > DNS
- REST API Agent

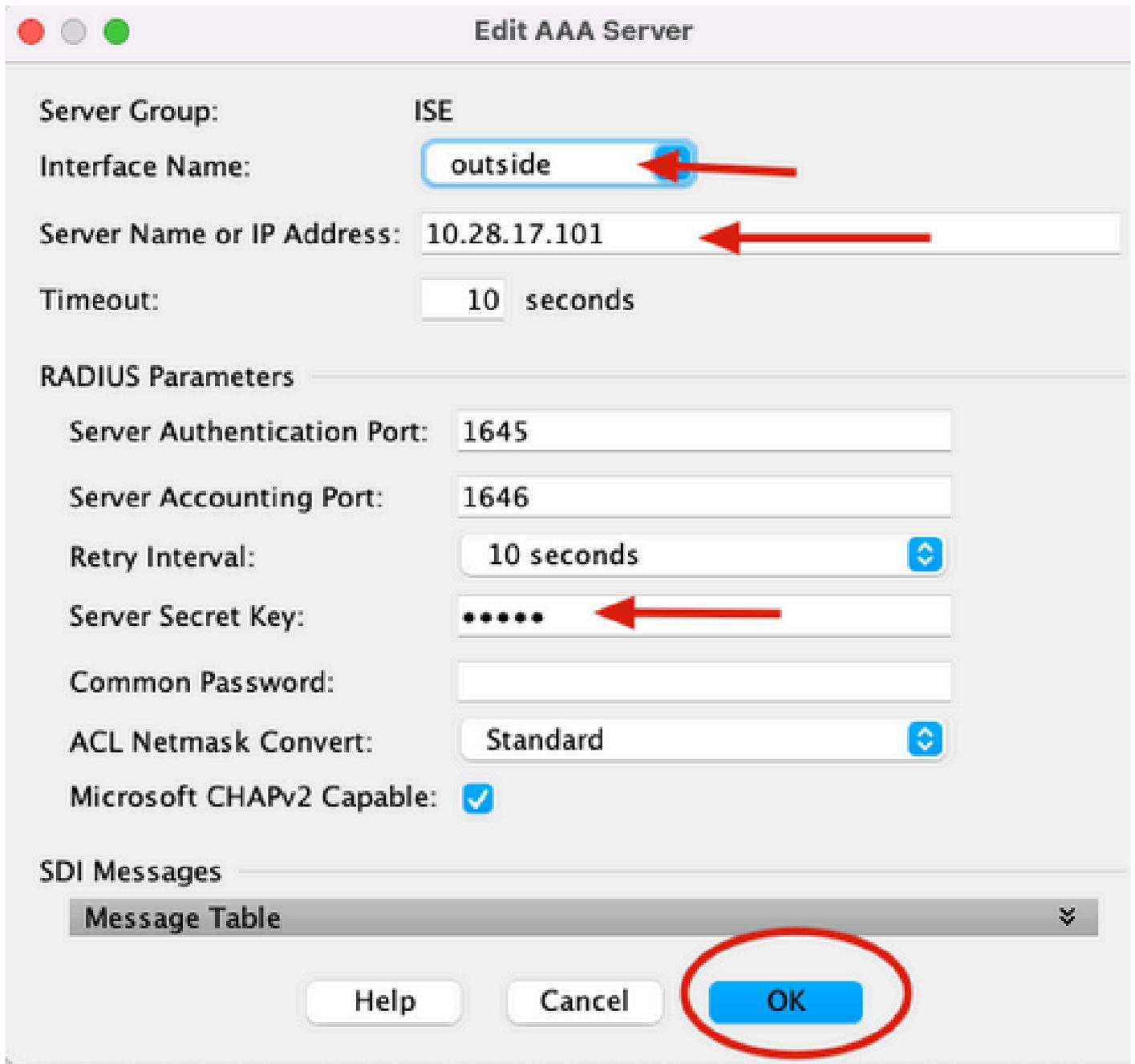
Find:

Servers in the Selected

Server Name or IP Address
10.28.17.101

window, select the interface name, specify the IP address of the ISE Server and type the RADIUS secret key and click **Ok**.

 **Note:** All this information must match the one specified on the Duo Authentication Proxy Manager.



Edit AAA Server

Server Group: ISE

Interface Name: outside

Server Name or IP Address: 10.28.17.101

Timeout: 10 seconds

RADIUS Parameters

Server Authentication Port: 1645

Server Accounting Port: 1646

Retry Interval: 10 seconds

Server Secret Key: *****

Common Password:

ACL Netmask Convert: Standard

Microsoft CHAPv2 Capable:

SDI Messages

Message Table

Help Cancel **OK**

CLI Configuration.

```
aaa-server ISE protocol radius
dynamic-authorization
aaa-server ISE (outside) host 10.28.17.101
key *****
```

Cisco ASA Remote Access VPN configuration

```
ip local pool agarciam-pool 192.168.17.1-192.168.17.100 mask 255.255.255.0
```

```
group-policy DUO internal
group-policy DUO attributes
  banner value This connection is for DUO authorized users only!
  vpn-tunnel-protocol ikev2 ssl-client
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value split-agarciam
  address-pools value agarciam-pool
```

```
tunnel-group ISE-users type remote-access
tunnel-group ISE-users general-attributes
  address-pool agarciam-pool
  authentication-server-group ISE
  default-group-policy DUO
tunnel-group ISE-users webvpn-attributes
  group-alias ISE enable
  dns-group DNS-CISCO
```

Test

1. Open **Anyconnect** app on your PC device. Specify the hostname of the VPN ASA Headend and log in with the user created for Duo secondary authentication and click **OK**.



2. You received a Duo push notification on the specified user Duo Mobile device.
3. Open the Duo Mobile App notification and click **Approve**.

14:41

Lunes, 14 de marzo

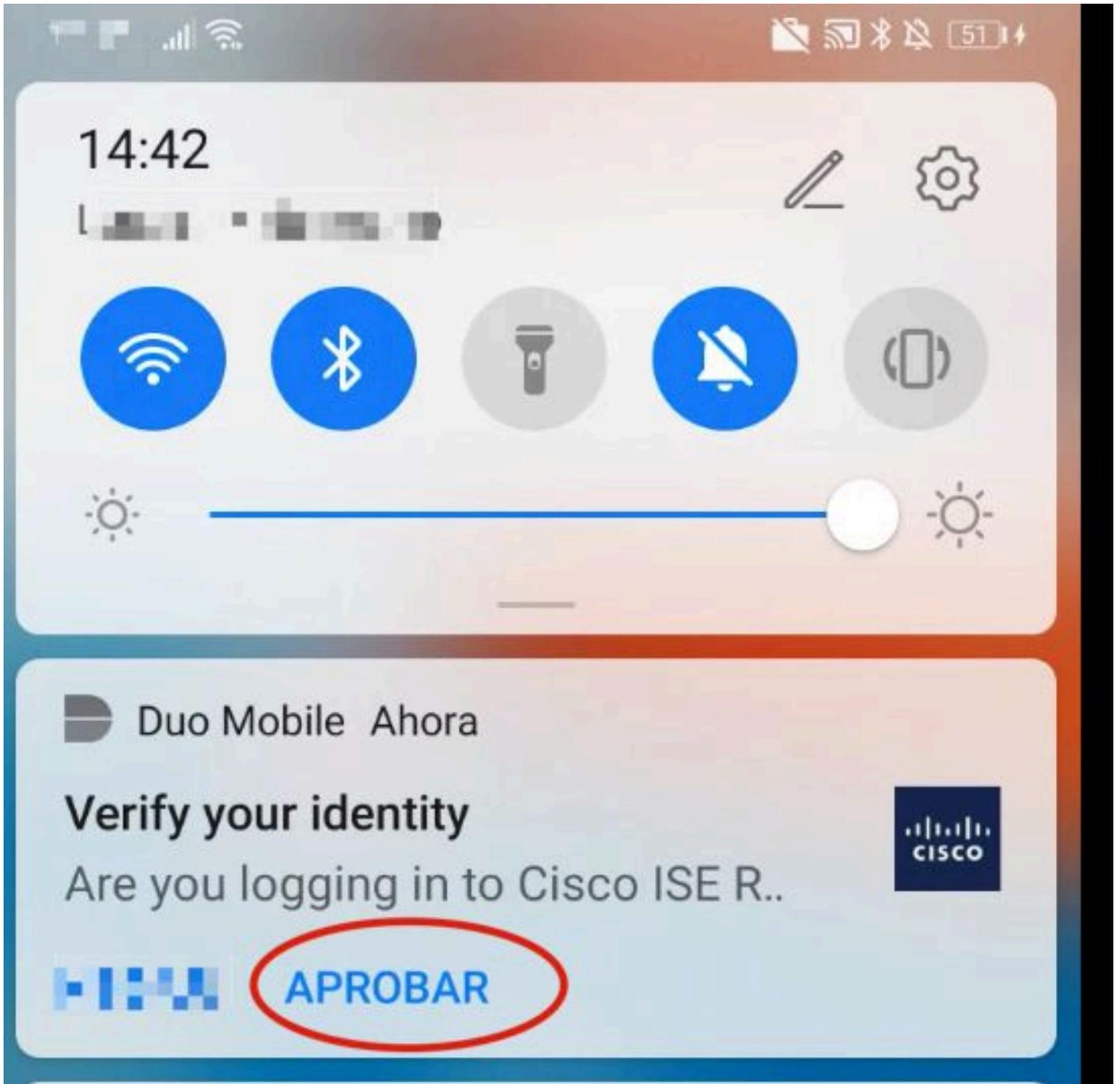


Duo Mobile Ahora

Verify your identity

Are you logging in to Cisco ISE R..





4. Accept the banner and connection is be established.



VPN:

Please respond to banner.

192.168.100.100



Connect

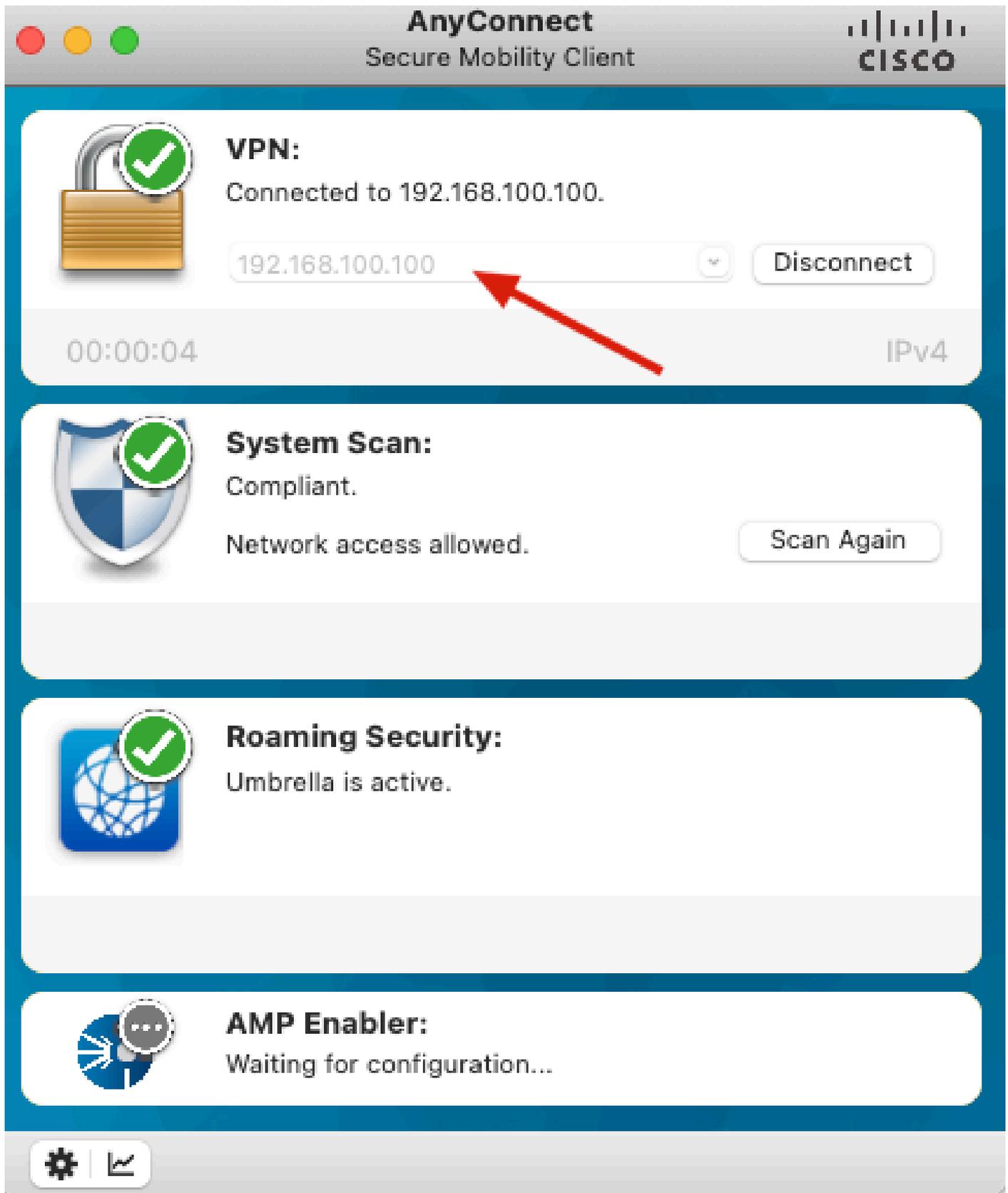
Cisco AnyConnect - Banner

This connection is for DUO authorized users only!

Disconnect

Accept





Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Duo Authentication Proxy comes with a debug tool that displays error and failure reasons.

Work Debugs

 **Note:** The next information is stored in C:\Program Files\Duo Security Authentication Proxy\log\connectivity_tool.log.

Output

```
Running The Duo Authentication Proxy Connectivity Tool. This may take
several minutes...
[info] Testing section 'main' with configuration:
[info] {'debug': 'True',
        'log_max_files': '10',
        'log_max_size': '20971520',
        'test_connectivity_on_startup': 'true'}
[info] There are no configuration problems
[info] -----
[info] Testing section 'ad_client' with configuration:
[info] {'debug': 'True',
        'host': '10.28.17.107',
        'search_dn': 'DC=agarciam,DC=cisco',
        'service_account_password': '*****',
        'service_account_username': 'Administrator'}
[info] There are no configuration problems
```

```
[info] -----  
[info] Testing section 'radius_server_auto' with configuration:  
[info] {'api_host': 'api_host',  
      'client': 'ad_client',  
      'debug': 'True',  
      'failmode': 'safe',  
      'ikey': 'XXXXXXXXXXXXXXXXXXXX',  
      'port': '1812',  
      'radius_ip_1': '10.28.17.101',  
      'radius_secret_1': '****',  
      'skey': '****[40]'}  
[info] There are no configuration problems
```

```
[info] Testing section 'main' with configuration:  
[info] {'debug': 'True',  
      'log_max_files': '10',  
      'log_max_size': '20971520',  
      'test_connectivity_on_startup': 'true'}  
[info] There are no connectivity problems with the section.
```



```
[ad_client]
```

```
host=10.28.17.106
```



```
service_account_username=Administrator
```

```
service_account_password=!@#%&*~!@#%&*~!@#%&*~!@#%&*~!
```

```
search_dn=DC=agarciam,DC=cisco
```

Output

```
'host': '10.28.17.106',
```

```
'search_dn': 'DC=agarciam,DC=cisco',
```

```
'service_account_password': '*****',
```

```
'service_account_username': 'Administrator']
```

```
[warn] The LDAP Client section has connectivity problems.
```

```
[warn] The LDAP host clear connection to 10.28.17.106:389 has connectivity problems.
```

```
[error] The Auth Proxy was not able to establish a connection to 10.28.17.106:389.
```



2. Wrong password for Administrator user on Active Directory.

```
[ad_client]
```

```
host=10.28.17.107
```

```
service_account_username=Administrator
```

```
service_account_password=!@#%&*~!@#%&*~!@#%&*~!@#%&*~!
```

```
search_dn=DC=agarciam,DC=cisco
```



Debugs.

```
[info] The Auth Proxy was able to establish a connection to 10.28.17.107:389.
[info] The Auth Proxy was able to establish an LDAP connection to 10.28.17.107:389.
[error] The Auth Proxy was unable to bind as Administrator.
[error] Please ensure that the provided service account credentials are correct.
[debug] Exception: invalidCredentials: 8009030C: LdapErr: DSID-0C090516, comment: AcceptSecurityContext error, data 52e, v3839.
[warn] The Auth Proxy did not run the search check because of the problem(s) with the bind check. Resolve that issue and rerun the tester.
```

3. Wrong Base Domain.

```
[ad_client]
host=10.28.17.107
service_account_username=Administrator
service_account_password=!R009030C
search_dn=DC=agarciam,DC=ciscoo ←
```

Debugs.

```
[info] The Auth Proxy was able to bind as Administrator.
[error] The Auth Proxy got an error searching the LDAP DN DC=agarciam,DC=ciscoo.
[debug] Exception: referral: 0000202B: RefErr: DSID-031007F9, data 0, 1 access points
        ref 1: 'agarciam.ciscoo'
```

4. Wrong ikey RADIUS value.

NTRadPing Test Utility

RADIUS Server/port: 10.28.17.107 1812

Reply timeout (sec.): 3 Retries: 6

RADIUS Secret key: !Mexvpr!17!

User-Name: duovpn ←

Password: ██████████ CHAP

Request type: Authentication Request 0

Additional RADIUS Attributes:

NTRadPing 1.5 - RADIUS Server Testing Tool
 © 1999-2003 Master Soft SpA - Italy - All rights reserved
<http://www.dialways.com/>




RADIUS Server reply:

```

Sending authentication request to server 10.28.17.107:1812
Transmitting packet, code=1 id=12 length=46
no response from server (timed out), new attempt (#1)
received response from the server in 4000 milliseconds
reply packet code=2 id=12 length=49
response: Access-Accept ←
..... attribute dump .....
Reply-Message=Success. Logging you in... ←
    
```

700	20.866684	10.28.17.3	10.28.17.107	RADIUS	88 Access-Request id=13, Duplicate Request
737	22.184895	10.28.17.107	10.28.17.3	RADIUS	90 Access-Accept id=13 ←

```

> Frame 700: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface \Device\NPF_{CA092CEE-552B-4E0A-9310-2D5231600D60}, id 0
> Ethernet II, Src: VMware_b3:f2:72 (00:50:56:b3:f2:72), Dst: VMware_b3:b4:3e (00:50:56:b3:b4:3e)
> Internet Protocol Version 4, Src: 10.28.17.3, Dst: 10.28.17.107
> User Datagram Protocol, Src Port: 51188, Dst Port: 1812
v RADIUS Protocol
  Code: Access-Request (1)
  Packet identifier: 0xd (13)
  Length: 46
  Authenticator: 20202020202031363436393335333230
  [Duplicate Request Frame Number: 532]
  [The response to this request is in frame 737]
v Attribute Value Pairs
  > AVP: t=User-Name(1) l=8 val=duovpn ←
  > AVP: t=User-Password(2) l=18 val=Encrypted
    
```