

Configuration de l'intégration Duo avec Active Directory et ISE pour l'authentification à deux facteurs sur les clients VPN Anyconnect/Remote Access

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Schéma de réseau et scénario](#)

[Processus de communication](#)

[Configurations Active Directory](#)

[Configurations Duo](#)

[Configuration du proxy Duo Auth](#)

[Configurations Cisco ISE](#)

[Configuration de Cisco ASA RADIUS/ISE](#)

[Configuration VPN d'accès à distance Cisco ASA](#)

[Essai](#)

[Dépannage](#)

[Débogages de travail](#)

Introduction

Ce document décrit l'intégration de la transmission Duo avec AD et ISE en tant qu'authentification à deux facteurs pour les clients AnyConnect connectés à ASA.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration VPN RA sur ASA
- Configuration RADIUS sur ASA
- ISE
- Active Directory
- Applications duo

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

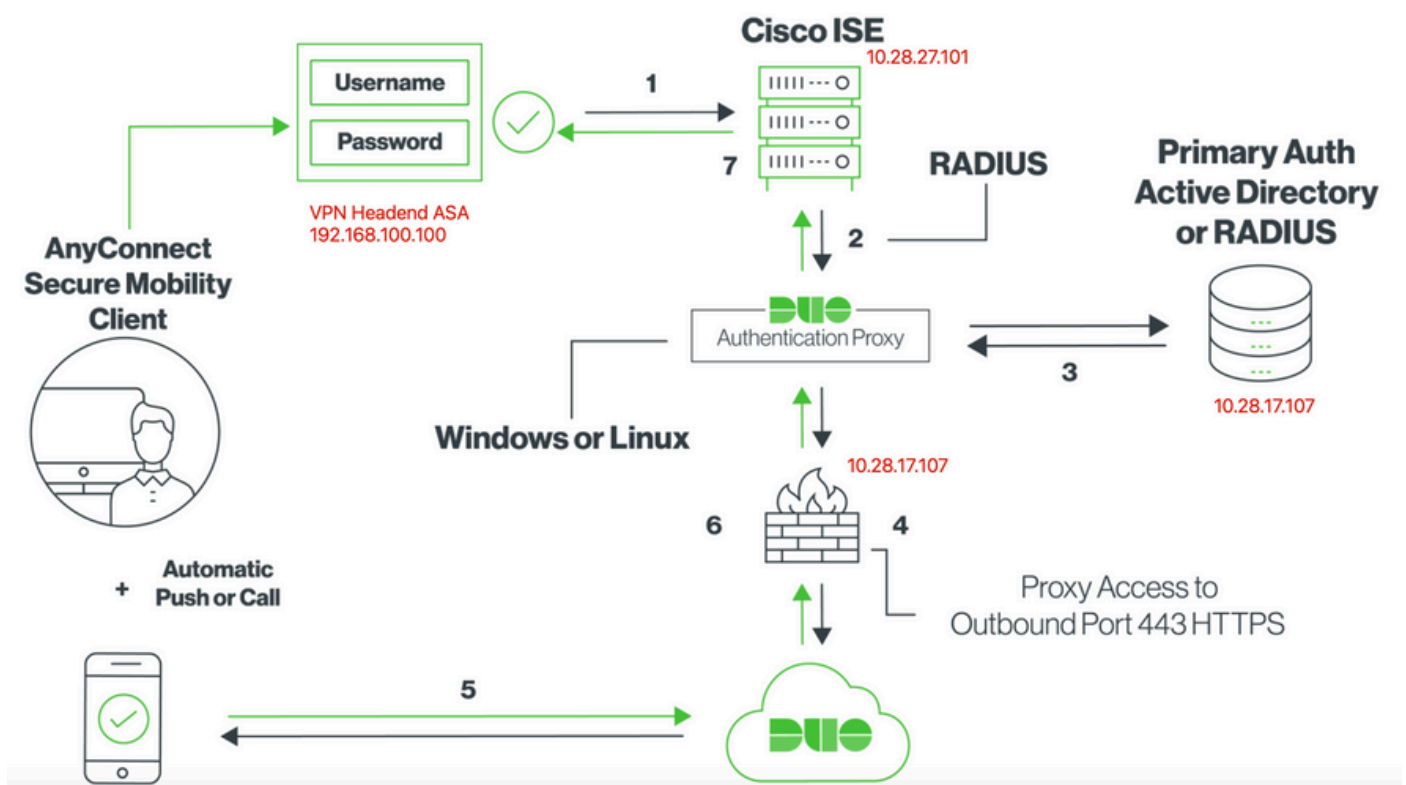
- Microsoft 2016 Server
- ASA 9.14(3)18
- Serveur ISE 3.0
- Serveur Duo
- Duo Authentication Proxy Manager

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Ce document décrit comment configurer l'intégration Duo Push avec Active Directory (AD) et Cisco Identity Service Engine (ISE) en tant qu'authentification à deux facteurs pour les clients AnyConnect qui se connectent à Cisco Adaptive Security Appliance (ASA).

Schéma de réseau et scénario



Processus de communication

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


1. Authentification principale initiée vers Cisco ISE
2. Cisco ISE envoie une demande d'authentification au proxy d'authentification duo
3. L'authentification principale utilise Active Directory ou RADIUS
4. Connexion proxy d'authentification duo établie avec Duo Security sur le port TCP 443
5. Authentification secondaire via le service de Duo Security
6. Le proxy d'authentification duo reçoit une réponse d'authentification
7. Accès Cisco ISE accordé

Comptes utilisateurs:

- Active Directory Admin : compte d'annuaire permettant au proxy d'authentification Duo de se lier au serveur Active Directory pour l'authentification principale.
- Utilisateur de test Active Directory
- Utilisateur de test duo pour authentification secondaire

Configurations Active Directory

Le serveur Windows est préconfiguré avec les services de domaine Active Directory.

 Remarque : si le Gestionnaire proxy d'authentification RADIUS Duo s'exécute sur le même ordinateur hôte Active Directory, les rôles NPS (Network Policy Server) doivent être désinstallés/supprimés. Si les deux services RADIUS s'exécutent, ils peuvent créer des conflits et affecter les performances.

Afin d'obtenir la configuration AD pour l'authentification et l'identité d'utilisateur sur les utilisateurs VPN d'accès à distance, quelques valeurs sont requises.

Tous ces détails doivent être créés ou collectés sur le serveur Microsoft avant que la configuration puisse être effectuée sur le serveur proxy ASA et Duo Auth.

Les principales valeurs sont les suivantes :

- le nom de domaine. Il s'agit du nom de domaine du serveur. Dans ce guide de configuration, agarciam.cisco est le nom de domaine.
- Adresse IP/FQDN du serveur. Adresse IP ou nom de domaine complet (FQDN) utilisé pour atteindre le serveur Microsoft. Si un nom de domaine complet est utilisé, un serveur DNS doit être configuré au sein du proxy ASA et Duo Auth pour résoudre le nom de domaine complet.

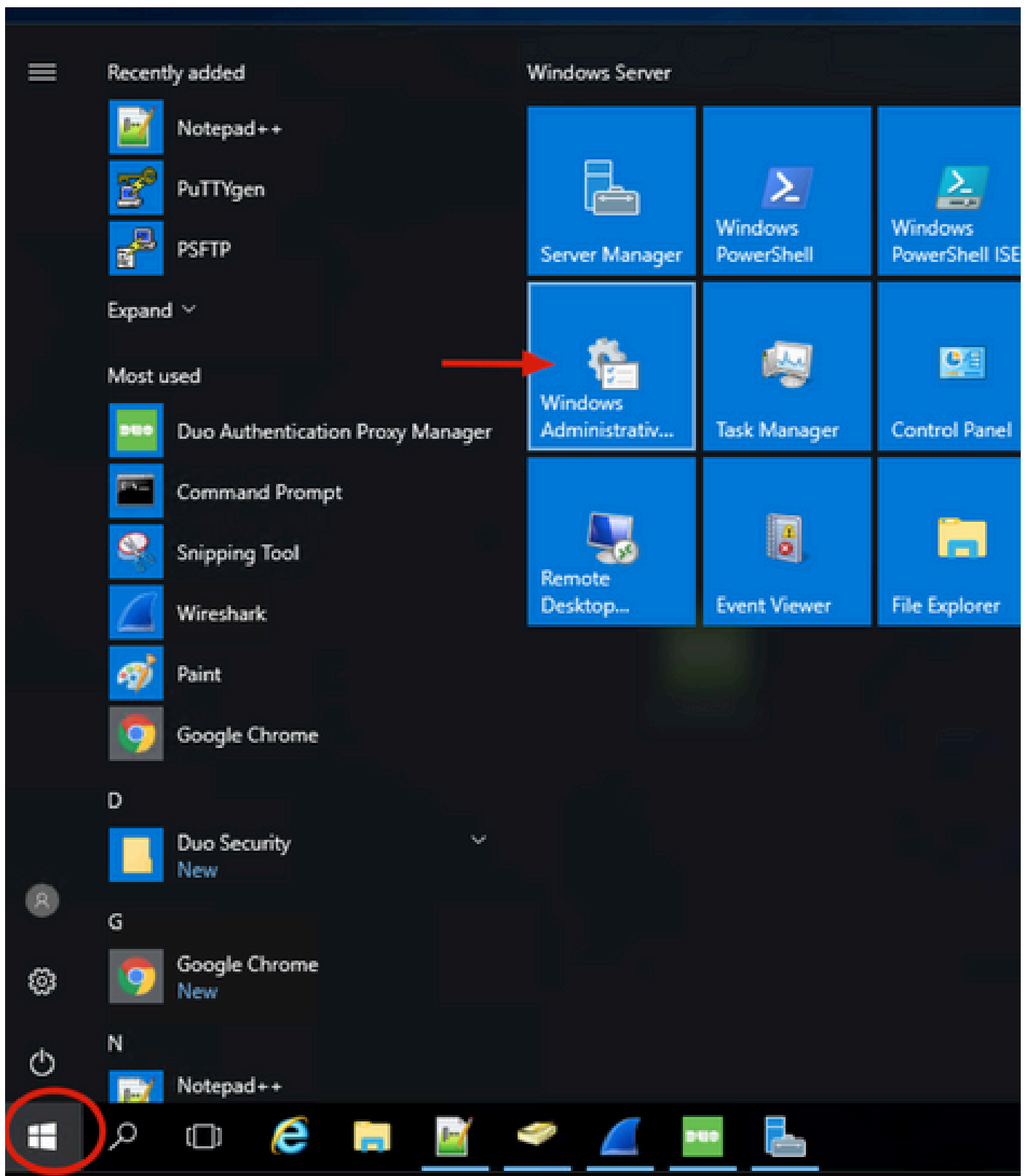
Dans ce guide de configuration, cette valeur est agarciam.cisco (qui correspond à 10.28.17.107).

- Port du serveur. Port utilisé par le service LDAP. Par défaut, LDAP et STARTTLS utilisent le port TCP 389 pour LDAP, et LDAP sur SSL (LDAPS) utilise le port TCP 636.
- CA racine. Si LDAPS ou STARTTLS est utilisé, l'autorité de certification racine utilisée pour signer le certificat SSL utilisé par LDAPS est requise.

- Nom d'utilisateur et mot de passe du répertoire Il s'agit du compte utilisé par le serveur proxy Duo Auth pour se lier au serveur LDAP et authentifier les utilisateurs et rechercher des utilisateurs et des groupes.
- Nom distinctif (DN) de base et de groupe. Le DN de base est le point de départ du proxy Duo Auth et il indique à Active Directory de commencer la recherche et l'authentification des utilisateurs.

Dans ce guide de configuration, le domaine racine agarciam.cisco est utilisé comme DN de base et le DN de groupe est Duo-USERS.

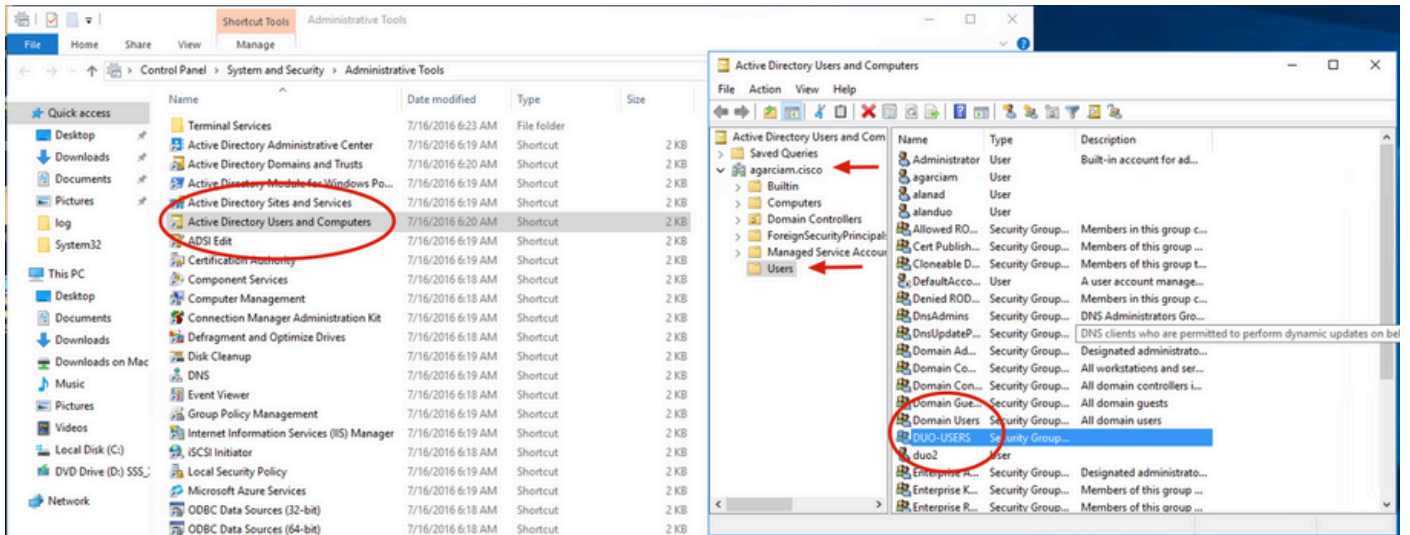
1. Afin d'ajouter un nouvel utilisateur Duo, sur Windows Server, naviguez vers l'icône Windows en bas à gauche et cliquez sur Outils d'administration Windows, comme illustré dans l'image.



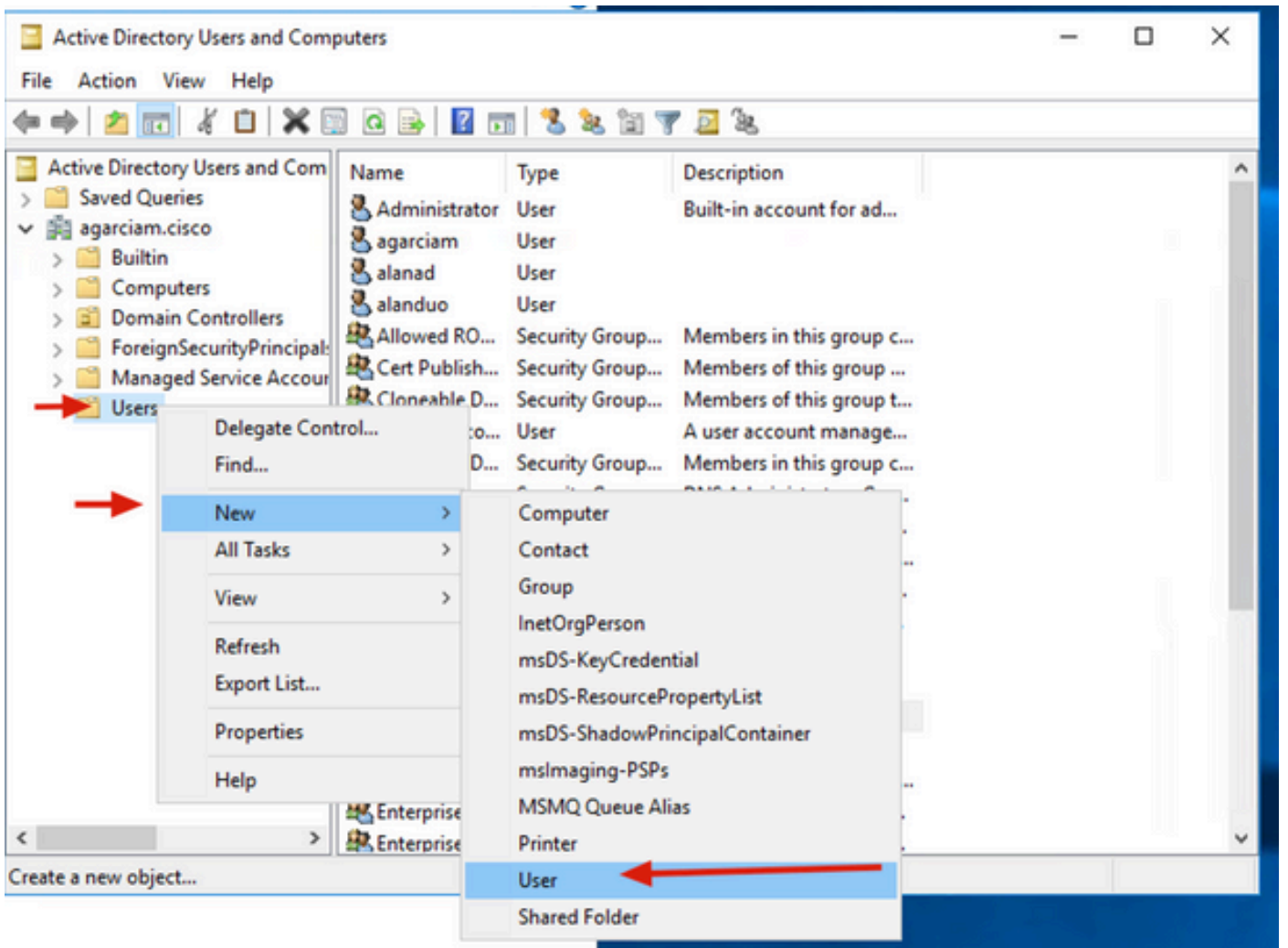
2. Dans la fenêtre Outils d'administration de Windows, accédez à Utilisateurs et ordinateurs Active Directory.

Dans le panneau Utilisateurs et ordinateurs Active Directory, développez l'option de domaine et accédez au dossier Utilisateurs.

Dans cet exemple de configuration, Duo-USERS est utilisé comme groupe cible pour l'authentification secondaire.





3. Cliquez avec le bouton droit sur le dossier Users et sélectionnez New > User, comme illustré dans l'image.



4. Dans la fenêtre Nouvel objet-utilisateur, spécifiez les attributs d'identité pour ce nouvel utilisateur et cliquez sur Suivant, comme indiqué dans l'image.


New Object - User X

 Create in: `agarciam.cisco/Users`

First name:  Initials:

Last name:


Full name:

User logon name:
 

User logon name (pre-Windows 2000):

5. Confirmez le mot de passe et cliquez sur Next, puis sur Finish une fois que les informations utilisateur sont vérifiées.

New Object - User X

 Create in: `agarciam.cisco/Users`

Password: ←

Confirm password: ←

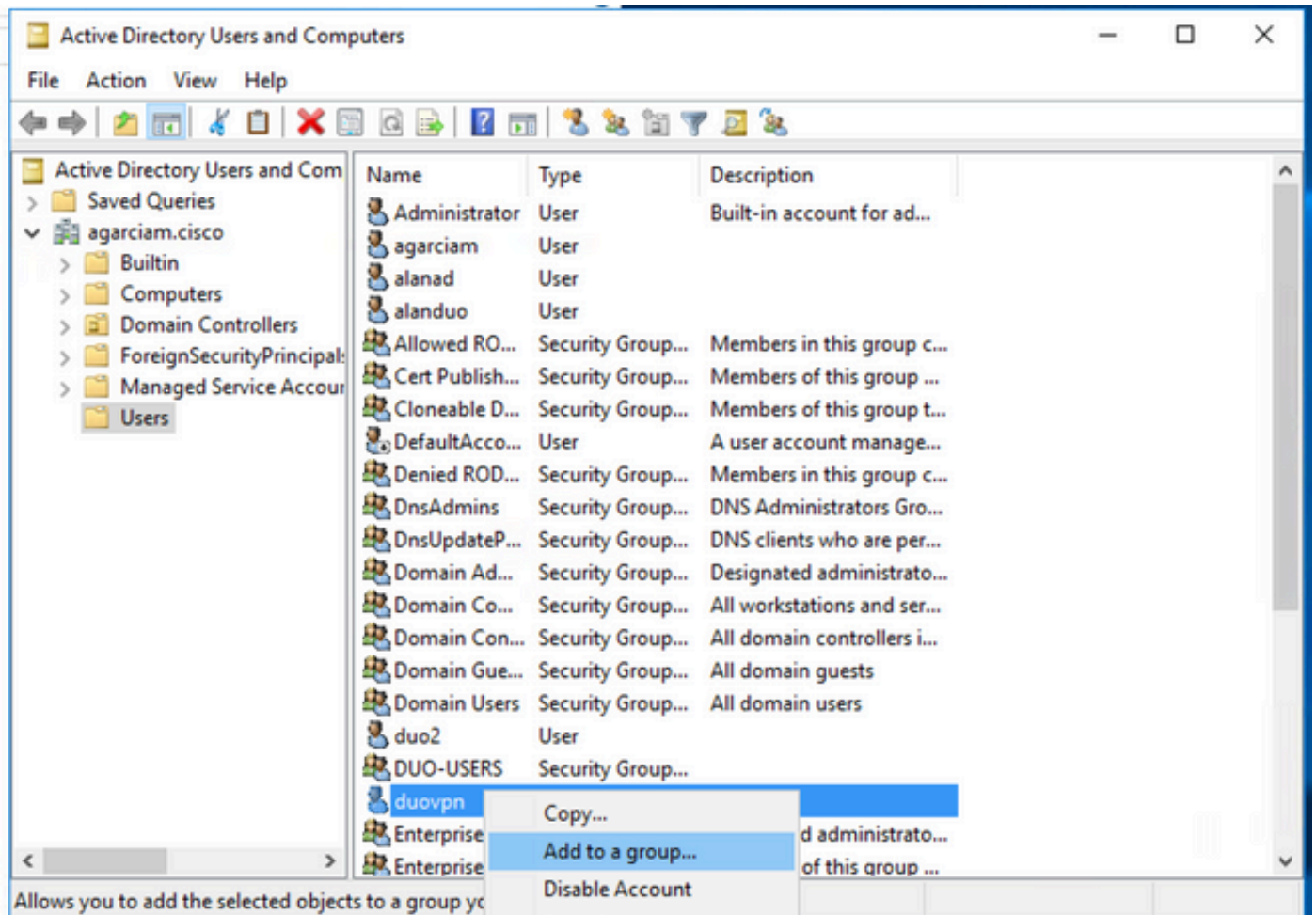
User must change password at next logon

User cannot change password

Password never expires

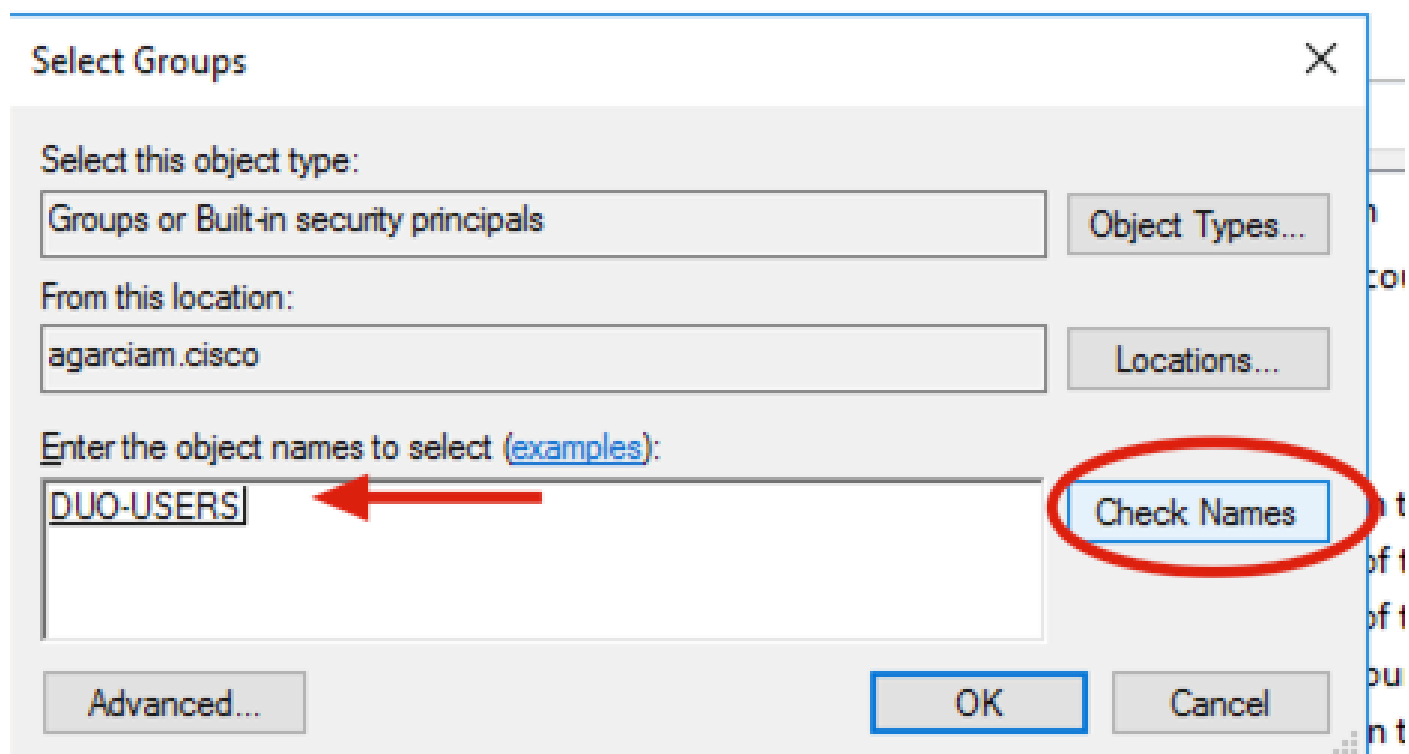
Account is disabled

6. Affectez le nouvel utilisateur à un groupe spécifique, cliquez dessus avec le bouton droit et sélectionnez Ajouter à un groupe, comme illustré dans l'image.



7. Dans le panneau Sélectionner des groupes, tapez le nom du groupe souhaité et cliquez sur Vérifier les noms.

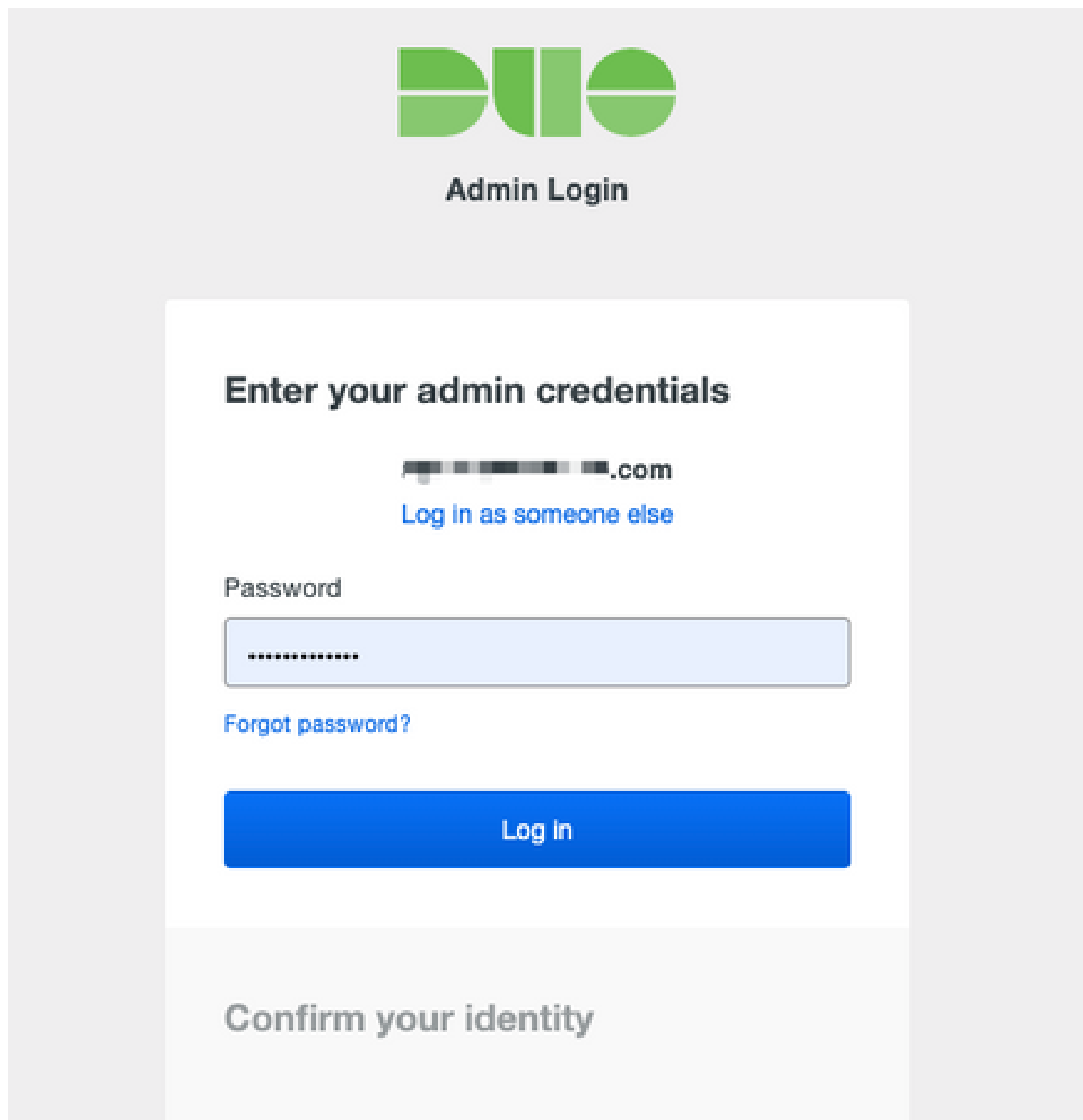
Sélectionnez ensuite le nom qui correspond à vos critères et cliquez sur Ok.



8. Il s'agit de l'utilisateur utilisé dans ce document à titre d'exemple.

Configurations Duo

1. Connectez-vous à votre portail d'administration Dudo.



Admin Login

Enter your admin credentials

██████████@██████████.com
[Log in as someone else](#)

Password

.....

[Forgot password?](#)

Log In

Confirm your identity

2. Sur le panneau latéral gauche, naviguez vers Users, cliquez sur Add User et tapez le nom de l'utilisateur qui correspond à votre nom d'utilisateur Active Domain, puis cliquez sur 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. Sur le nouveau panneau de l'utilisateur, remplissez le vide toutes les informations nécessaires.

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. Sous user devices, spécifiez la méthode d'authentification secondaire.

 Remarque : dans ce document, la méthode « Duo push for mobile devices » est utilisée. Un appareil téléphonique doit donc être ajouté.

Cliquez sur Ajouter un téléphone.

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. Tapez le numéro de téléphone de l'utilisateur et cliquez sur Ajouter un téléphone.

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

6. Dans le panneau d'administration Duo de gauche, accédez à Utilisateurs et cliquez sur le nouvel utilisateur.

Dashboard > Users


Users

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

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

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




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

 Remarque : si vous n'avez pas accès à votre téléphone pour le moment, vous pouvez sélectionner l'option e-mail.

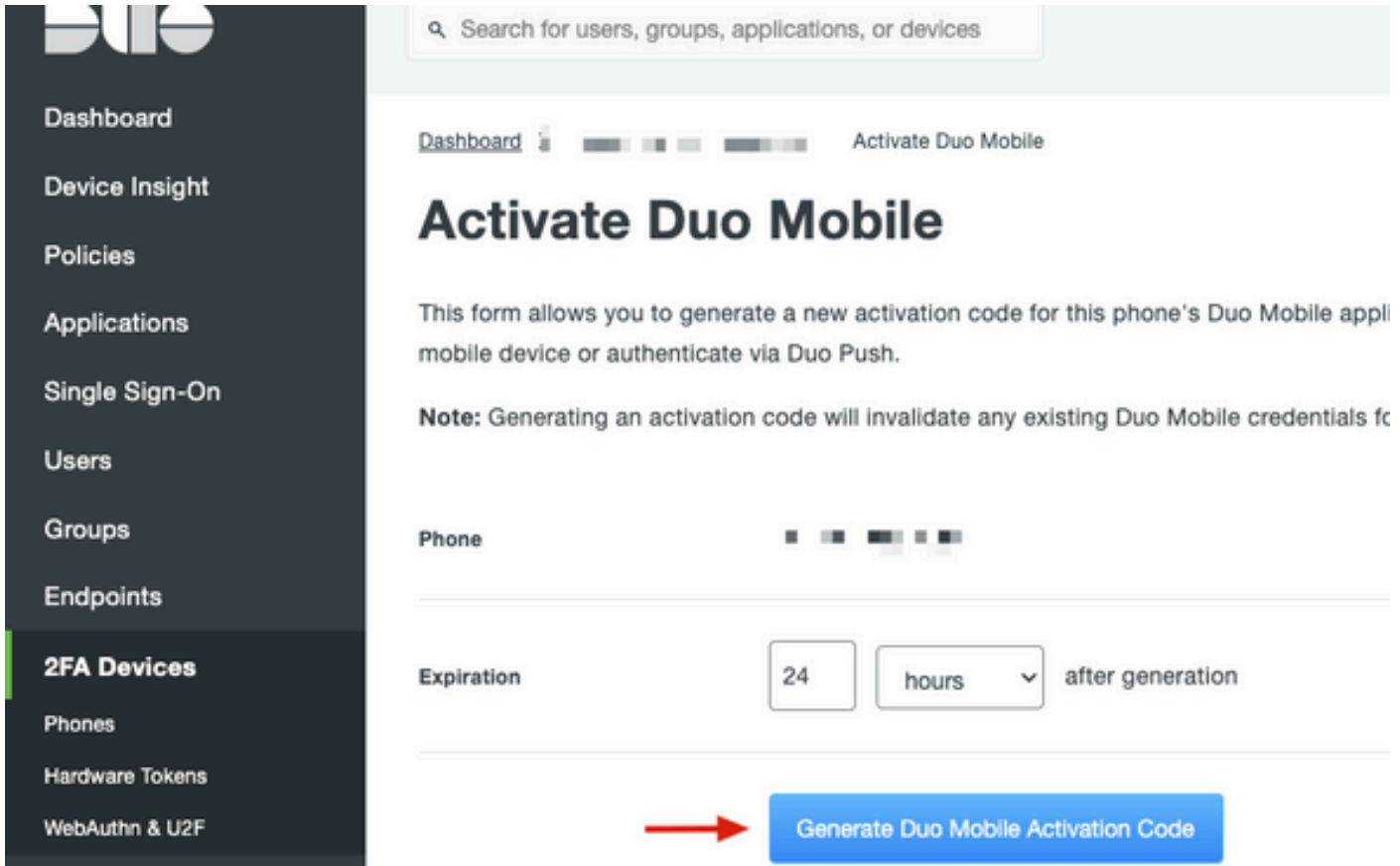
7. Accédez à la section Téléphones et cliquez sur Activer Duo Mobile.

Phones

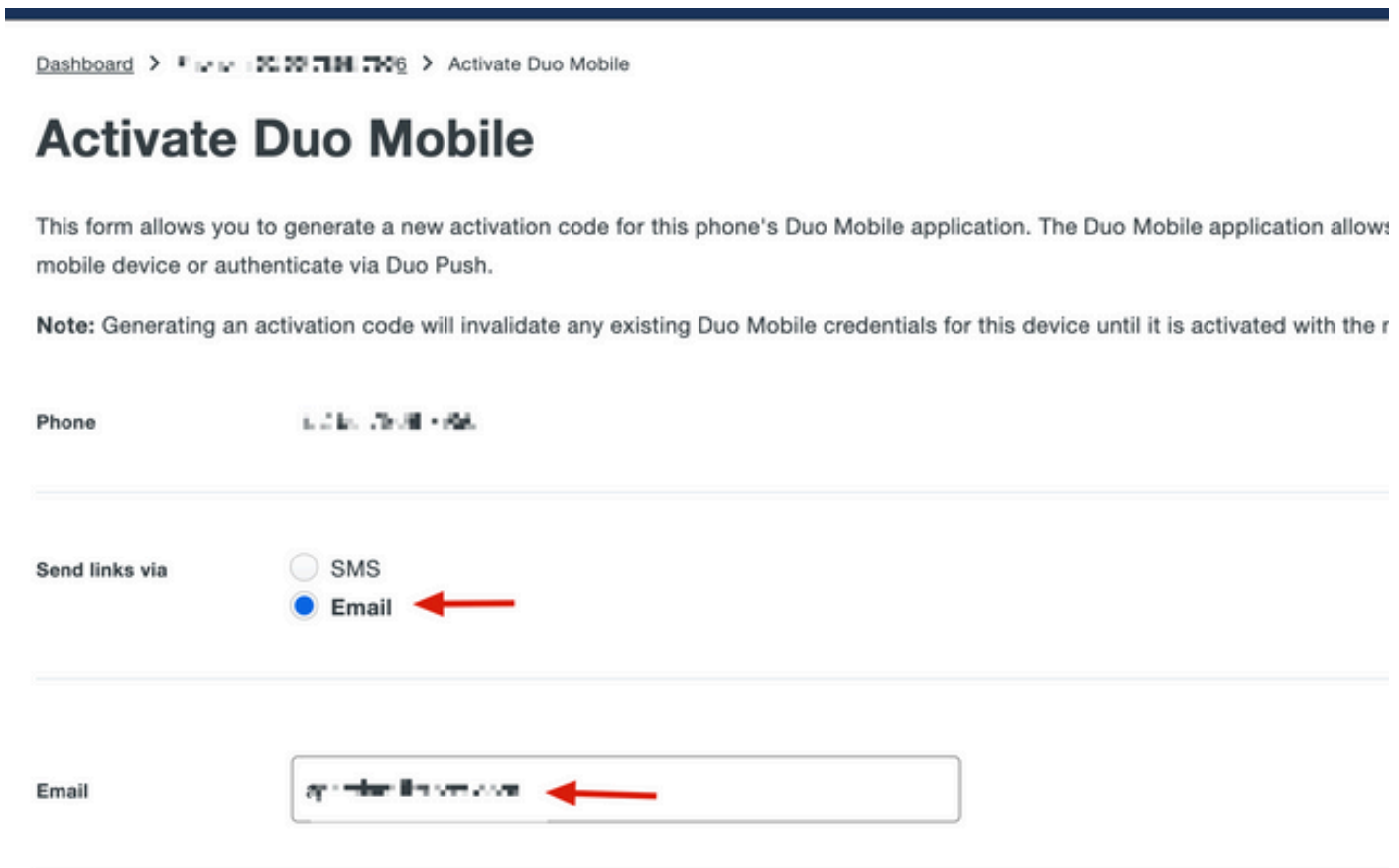
You may rearrange the phones by dragging and dropping in the table. [Learn more about activating a replacement phone](#) [Add Phone](#)

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

8. Cliquez sur Generate Duo Mobile Activation Code.



9. Sélectionnez Email afin de recevoir les instructions par e-mail, tapez votre adresse e-mail et cliquez sur Send Instructions by email.



10. Vous recevez un e-mail contenant les instructions, comme illustré dans l'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. Ouvrez l'application mobile Duo à partir de votre appareil mobile et cliquez sur Ajouter, puis sélectionnez Utiliser le code QR et numérisez le code à partir de l'e-mail des instructions.

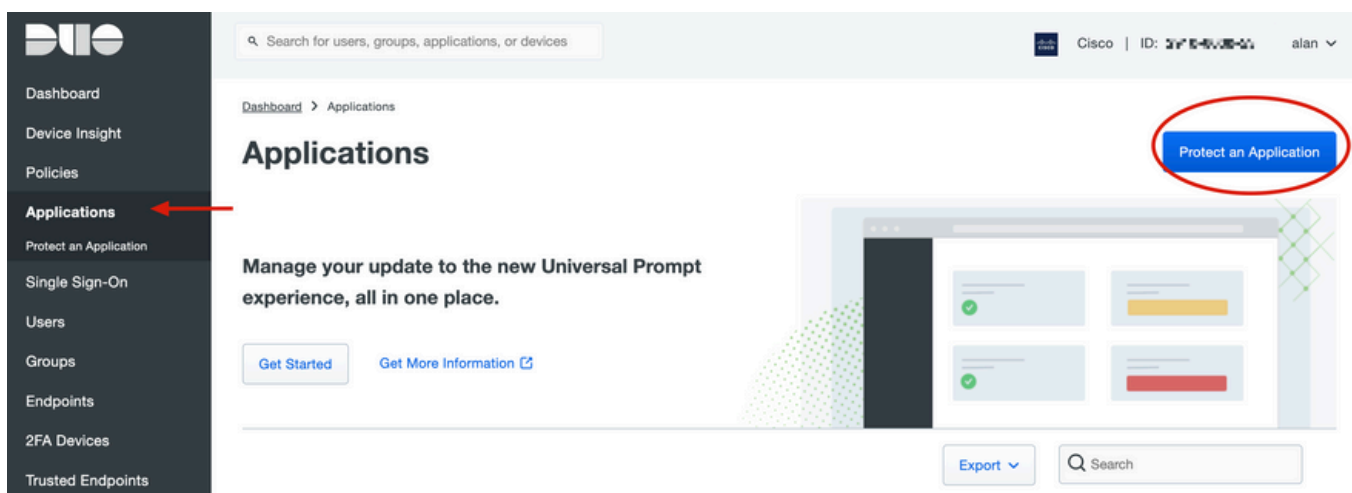
12. Un nouvel utilisateur est ajouté à votre application mobile Duo.

Configuration du proxy Duo Auth

1. Téléchargez et installez Duo Auth Proxy Manager à partir de <https://duo.com/docs/authproxy-reference>.


 Remarque : dans ce document, le Duo Auth Proxy Manager est installé sur le même serveur Windows que celui qui héberge les services Active Directory.

2. Dans le panneau d'administration Duo, accédez à Applications et cliquez sur Protect an Application.






3. Dans la barre de recherche, recherchez Cisco ISE Radius.

Protect an Application

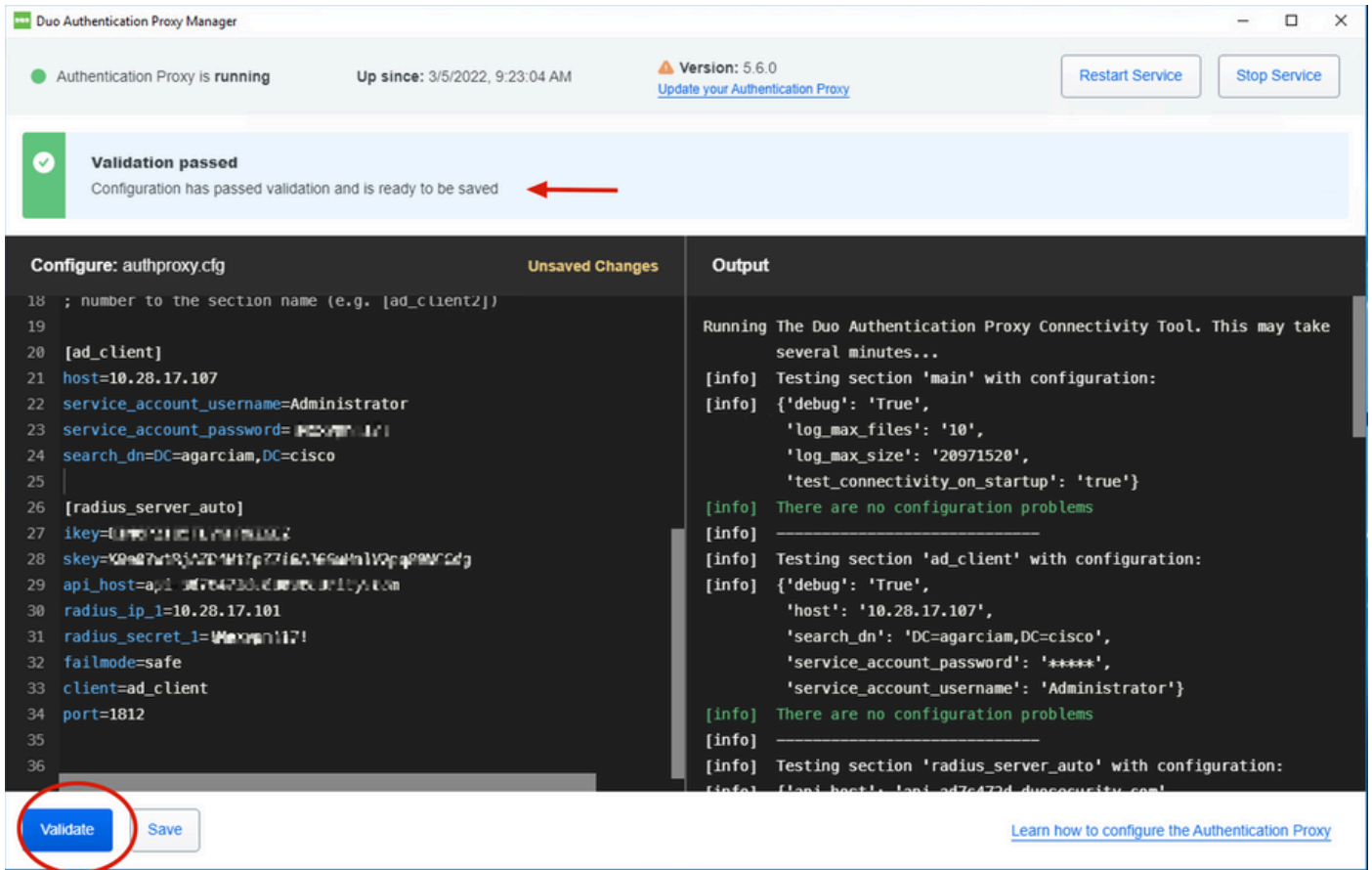
 Add an application that you'd like to protect with Duo two-factor authentication. You can start with a small "proof-of-concept" installation — it takes just a few minutes, and you're the only one that will see it, until you decide to add others.

Documentation: [Getting Started](#)

Choose an application below to get started.

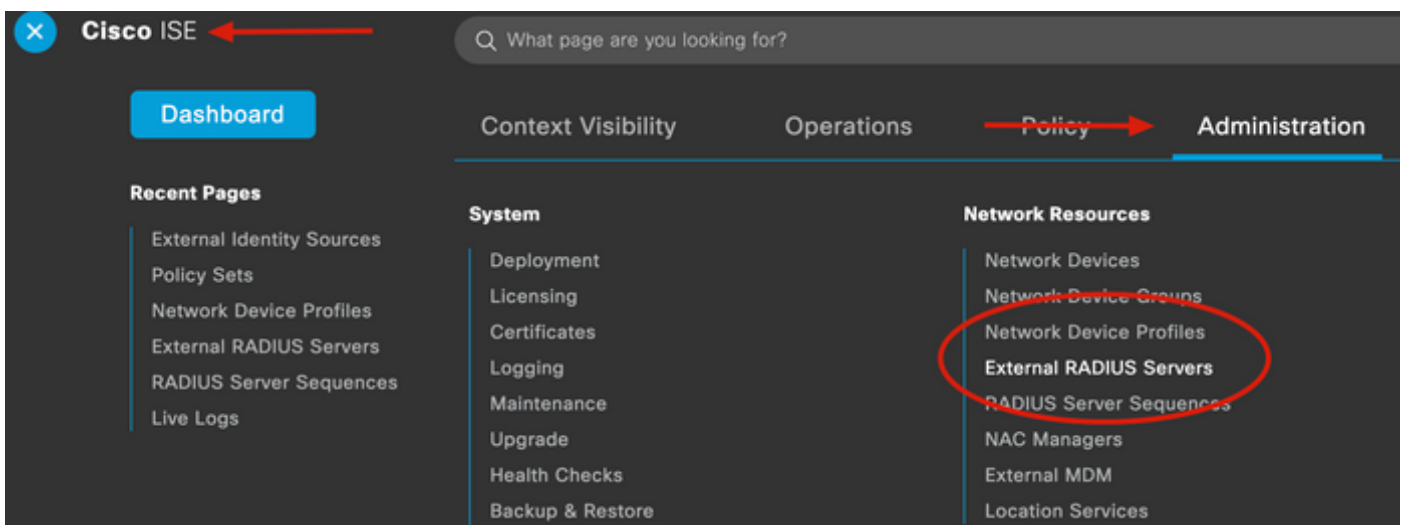
Application	Protection Type	
 Akamai Enterprise Application Access	2FA	Documentation Protect
 Cisco ISE RADIUS 	2FA	Documentation Protect

4. Copiez la clé d'intégration, la clé de sécurité et le nom d'hôte de l'API. Vous avez besoin de ces informations pour la configuration Duo Authentication Proxy.



Configurations Cisco ISE

1. Connectez-vous au portail d'administration ISE.
2. Développez l'onglet Cisco ISE et accédez à Administration, puis cliquez sur Network Resources et cliquez sur External RADIUS Servers.



3. Dans l'onglet Serveurs Radius externes, cliquez sur Ajouter.

External RADIUS Servers

Edit **+ Add** Duplicate Delete

Name: Currently Sorted Description

4. Complétez la zone vide avec la configuration RADIUS utilisée dans le Duo Authentication Proxy Manager et cliquez sur Submit.

Network Devices Network Device Groups Network Device Profiles **External RADIUS Servers** RADIUS Server Sequences NAC Managers External MDM More

* Name DUO_NEW

Description

* Host IP 10.28.17.107

* Shared Secret Show

Enable KeyWrap

* Key Encryption Key Show

* Message Authenticator Code Key Show

Key Input Format ASCII HEXADECIMAL

* Authentication Port 1812 (Valid Range 1 to 65535)

* Accounting Port 1813 (Valid Range 1 to 65535)

* Server Timeout 5 Seconds (Valid Range 1 to 120)

* Connection Attempts 3 (Valid Range 1 to 9)

Radius ProxyFailover Expiration 300 (Valid Range 1 to 600)

Submit

5. Accédez à l'onglet Séquences de serveur RADIUS et cliquez sur Ajouter.

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers **RADIUS Server Sequences**

RADIUS Server Sequences

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Edit **+ Add** Duplicate Delete

6. Spécifiez le nom de la séquence et affectez le nouveau serveur externe RADIUS, cliquez sur Submit.

RADIUS Server Sequence

General

Advanced Attribute Settings

* Name

DUO_Sequence

Description

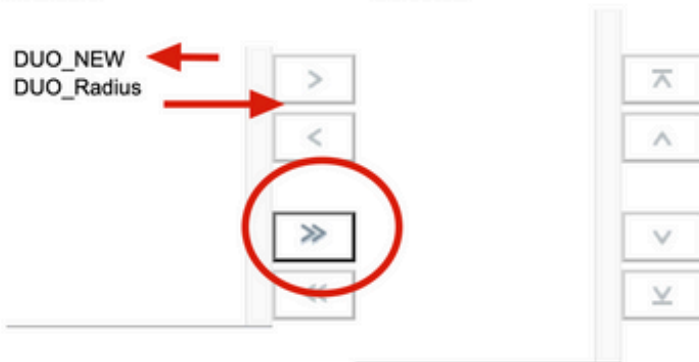
User Selected Service Type

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

Available

* Selected

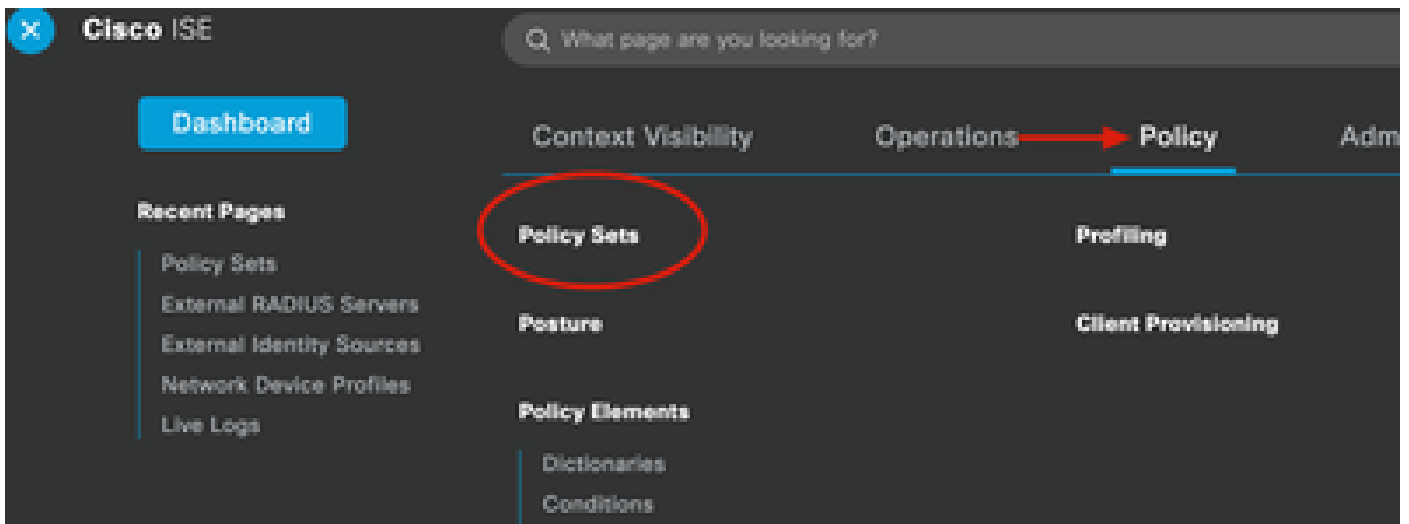
DUO_NEW
DUO_Radius




Remote accounting

Local accounting

7. Accédez à Policy à partir du menu Tableau de bord et cliquez sur Policy Sets.





8. Affectez la séquence RADIUS à la stratégie par défaut.

 Remarque : dans ce document, la séquence Duo est appliquée à toutes les connexions. La stratégie par défaut est donc utilisée. L'affectation des stratégies peut varier selon les besoins.

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

EQ |

Allowed Protocols

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

Configuration de Cisco ASA RADIUS/ISE

1. Configurez le serveur RADIUS ISE sous les groupes de serveurs AAA, accédez à Configuration, cliquez sur Device Management et développez la section Users/AAA, sélectionnez 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

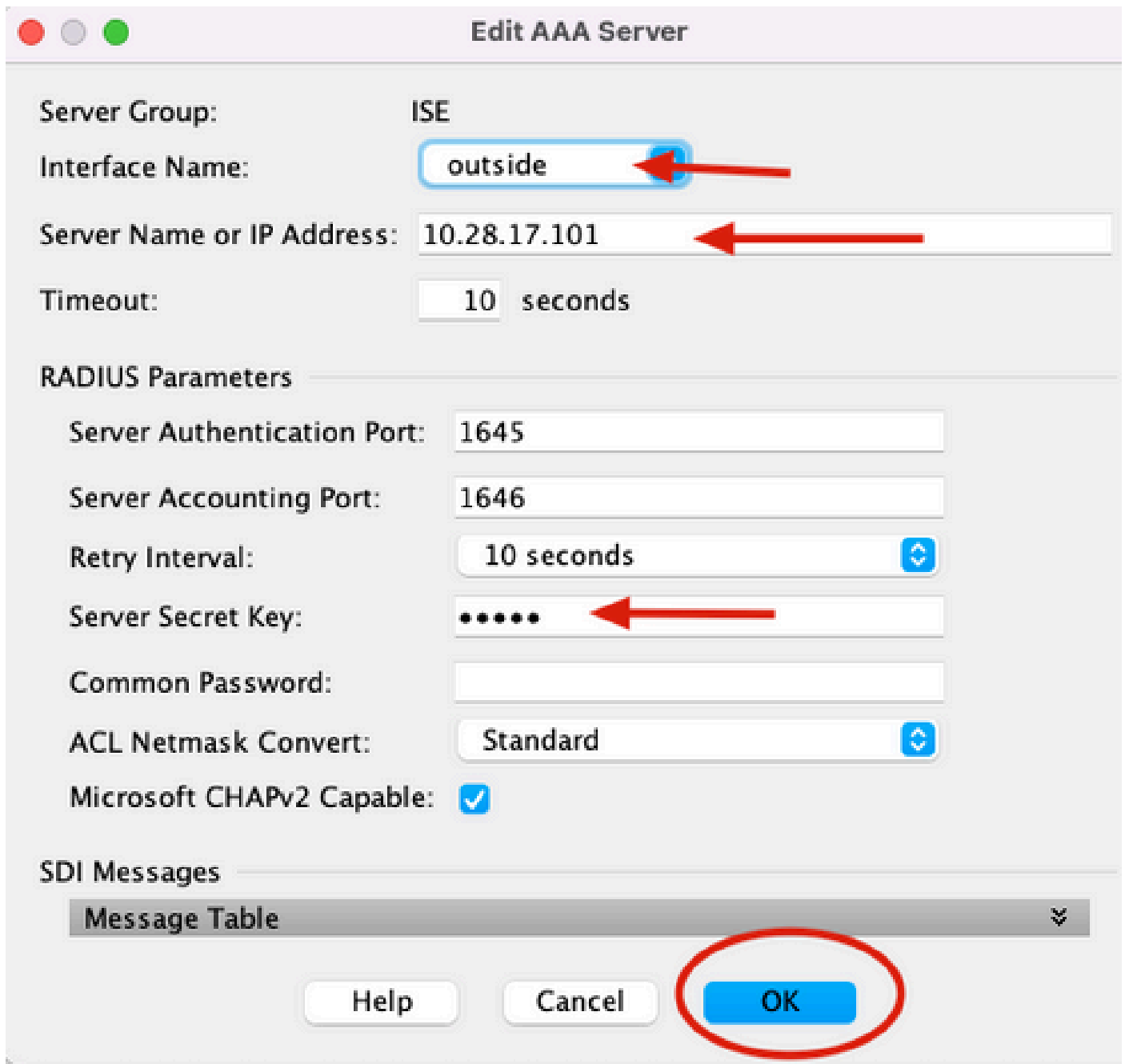
Find:

Servers in the Selected

Server Name or IP Address
10.28.17.101

, sélectionnez le nom de l'interface, spécifiez l'adresse IP du serveur ISE et tapez la clé secrète RADIUS et cliquez sur Ok.

 Remarque : toutes ces informations doivent correspondre à celles spécifiées dans le 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**

Configuration CLI.

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

Configuration VPN d'accès à distance Cisco ASA

```
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
```

Essai

1. Ouvrez l'application Anyconnect sur votre appareil PC. Spécifiez le nom d'hôte de la tête de réseau VPN ASA et connectez-vous avec l'utilisateur créé pour l'authentification secondaire Duo et cliquez sur OK.



2. Vous avez reçu une notification de transmission Duo sur l'appareil Duo Mobile de l'utilisateur spécifié.
3. Ouvrez la notification de l'application mobile Duo et cliquez sur Approuver.

14:41

Lunes, 14 de marzo

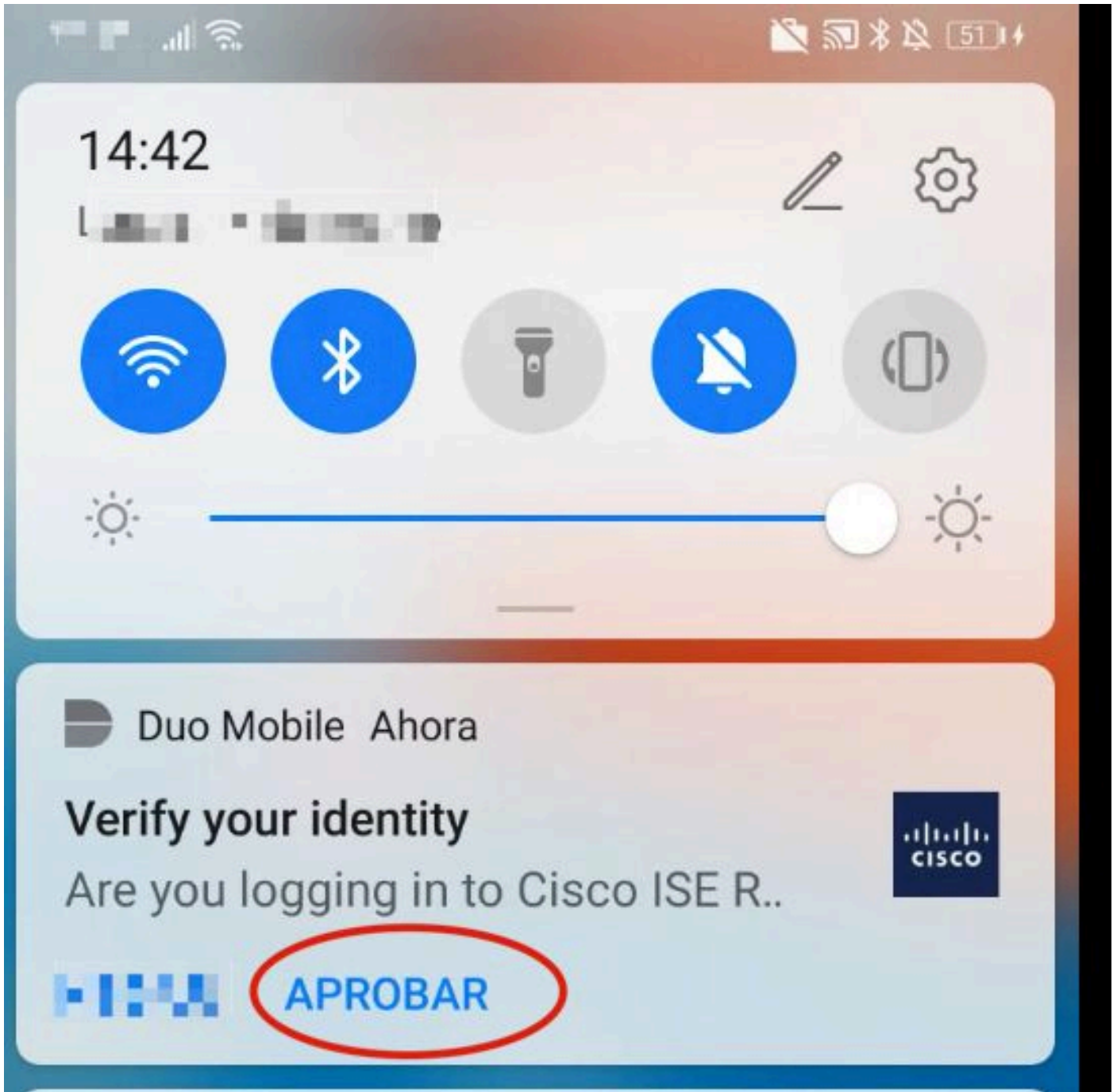


Duo Mobile Ahora

Verify your identity

Are you logging in to Cisco ISE R..





4. Acceptez la bannière et la connexion est établie.



VPN:

Please respond to banner.

192.168.100.100



Connect

Cisco AnyConnect - Banner


This connection is for DUO authorized users only!


Disconnect



Accept





AnyConnect
Secure Mobility Client





 **VPN:**
Connected to 192.168.100.100.



192.168.100.100  

00:00:04 IPv4

 **System Scan:**
Compliant.
Network access allowed. 

 **Roaming Security:**
Umbrella is active.

 **AMP Enabler:**
Waiting for configuration...


 

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Duo Authentication Proxy est fourni avec un outil de débogage qui affiche les raisons de l'erreur et de l'échec.

Débogages de travail

 Remarque : les informations suivantes sont stockées dans le fichier 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.10.28.17.101',  
      '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=!H...@17!!
```

```
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. Mot de passe incorrect pour l'utilisateur Administrateur sur Active Directory.

```
[ad_client]
```

```
host=10.28.17.107
```

```
service_account_username=Administrator
```

```
service_account_password=!H...@17!!
```



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

Débogages.

```
[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. Domaine de base incorrect.

```
[ad_client]
host=10.28.17.107
service_account_username=Administrator
service_account_password=!P@ssw0rd!
search_dn=DC=agarciam,DC=ciscoo ←
```

Débogages.

```
[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. Valeur RADIUS ikey incorrecte.

```
[radius_server_auto]
ikey=UJN5P21059LVXHRNZ6EZ1
skey=Ja2XmFh14h1LLP10P0Thp0d49eUd00A00c
api_host=api.ise.pan.com
radius_ip_1=10.28.17.101
radius_secret_1=!Mexvpn!17!
failmode=safe
client=ad_client
port=1812
```

Déboguages

```
[error] The ikey value provided is invalid.
[info] -----
[info] SUMMARY
[warn] Checks for external connectivity were not run. Please fix the
configuration and try again.
```

5. Vérifiez que le serveur ISE envoie des paquets de demande d'accès.

*Ethernet0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

radius

No.	Time	Source	Destination	Protocol	Length	Info
1511	6020.521457	10.28.17.101	10.28.17.107	RADIUS	877	Access-Request id=31
1513	6024.344735	10.28.17.107	10.28.17.101	RADIUS	191	Access-Accept id=31

> Frame 151115: 877 bytes on wire (7016 bits), 877 bytes captured (7016 bits) on interface \Device\NPF_{CA092CEE-5}

> Ethernet II, Src: VMware_b3:a4:2f (00:50:56:b3:a4:2f), Dst: VMware_b3:b4:3e (00:50:56:b3:b4:3e)

> Internet Protocol Version 4, Src: 10.28.17.101, Dst: 10.28.17.107

> User Datagram Protocol, Src Port: 42022, Dst Port: 1812

▼ RADIUS Protocol

Code: Access-Request (1)

Packet identifier: 0x1f (31)

Length: 835

Authenticator: 38a28ca3ca6bbc261819c5304b1be6e3

[The response to this request is in frame 151332]

▼ Attribute Value Pairs

- > AVP: t=User-Name(1) l=8 val=duovpn
- > AVP: t=User-Password(2) l=18 val=Encrypted
- > AVP: t=NAS-IP-Address(4) l=6 val=192.168.100.100
- > AVP: t=NAS-Port(5) l=6 val=344064
- > AVP: t=Called-Station-Id(30) l=17 val=192.168.100.100
- > AVP: t=Calling-Station-Id(31) l=13 val=M.##.!!.!!
- > AVP: t=Proxy-State(33) l=25 val=466972737450726f78793d31302e32382e31372e313031
- > AVP: t=Proxy-State(33) l=76 val=436973636f205365637572652041435337366535323735612d396362302d313165632d63...
- > AVP: t=NAS-Port-Type(61) l=6 val=Virtual(5)
- > AVP: t=Tunnel-Client-Endpoint(66) l=13 val=10.99.65.53

6. Afin de confirmer que le serveur proxy d'authentification Duo fonctionne, Duo fournit l'outil [NTRadPing](#) pour simuler les paquets de demande d'accès et la réponse avec Duo.

6.1 Installation de NTRadPing sur un autre PC et génération de trafic



Remarque : dans cet exemple, la machine Windows 10.28.17.3 est utilisée.

6.2 Configuration à l'aide des attributs utilisés dans la configuration ISE Radius

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:

Buttons: Add Remove Clear list Load... Save... Send Help... Close

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: 202020202031363436393335333230
  [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
    
```


À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.