Configuration de l'intégration duo avec AD et ISE pour RAVPN 2FA

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Diagramme et scénario du réseau
  - Processus de communication
- Configurations Active Directory
- Configurations Duo
- Configuration du proxy Duo Auth
- Configurations Cisco ISE
- Configuration de Cisco ASA RADIUS/ISE
  - Configuration CLI
- Configuration VPN d'accès à distance Cisco ASA
- Essai
- Dépannage
  - Débogages de travail
- Problèmes courants
    - 1. Problèmes de connectivité, adresse IP incorrecte, nom de domaine complet/nom d'hôte non résolu dans la configuration Active Directory
    - 2. Mot de passe incorrect pour l'utilisateur administrateur sur Active Directory
    - 3. Domaine de base incorrect
    - 4. Valeur iKey RADIUS incorrecte
    - 5. Vérifier que le serveur ISE envoie des paquets de demande d'accès
    - 6. Utilisez l'utilitaire NTRadPing pour vérifier que le proxy d'authentification duo fonctionne

Introduction

Ce document décrit l'intégration Duo Push avec AD et Cisco ISE en tant que 2FA pour les clients sécurisés Cisco connectés à ASA.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Applications duo
- Active Directory (AD)
- Moteur du service de vérification des identités (ISE)
- Configuration RADIUS sur ASA
- Configuration du VPN d'accès à distance (RAVPN) sur un dispositif de sécurité adaptatif (ASA)

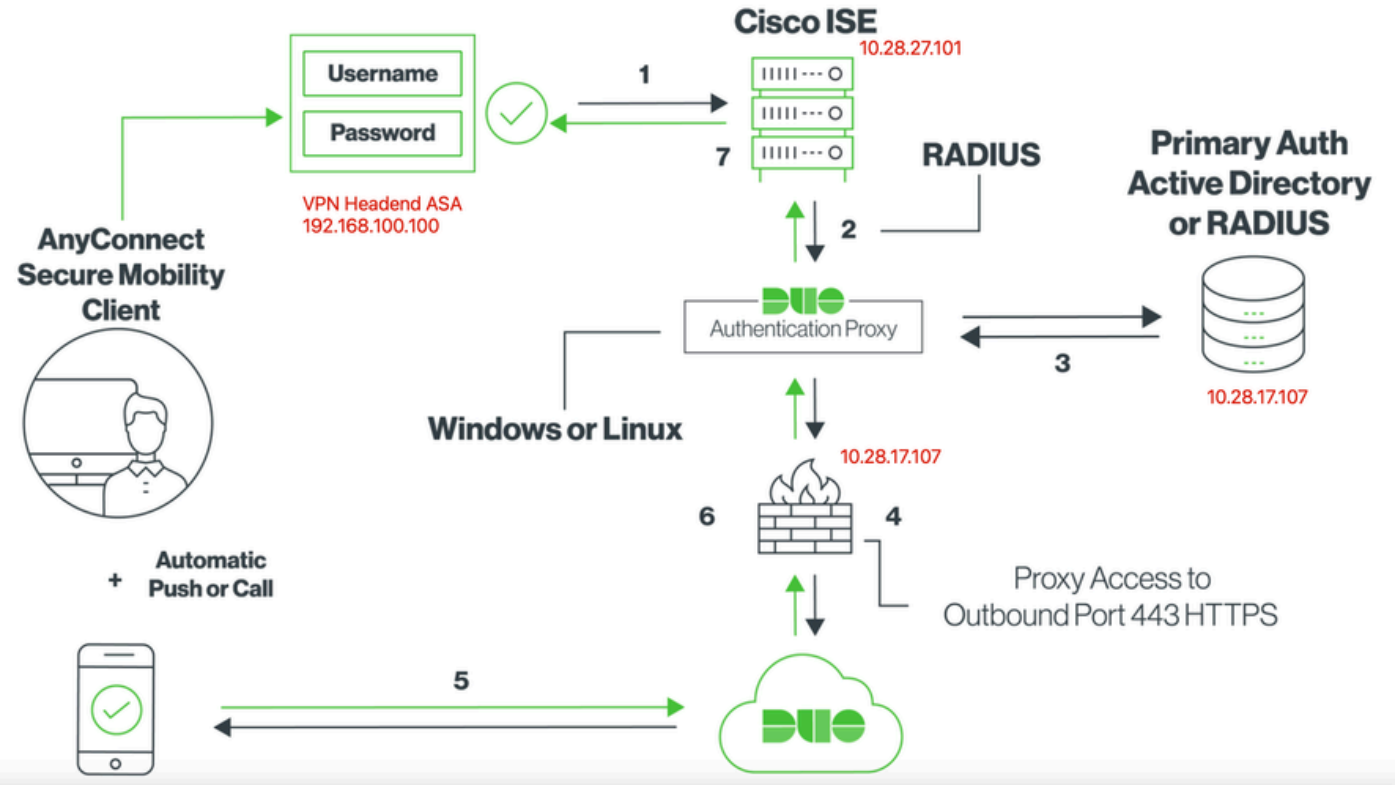
Composants utilisés

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

- Serveur Duo
- Serveur ISE 3.0
- ASA 9.14(3)18
- Microsoft 2016 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Diagramme et scénario du réseau



Processus de communication

[Authentification double RADIUS à deux facteurs pour Cisco ISE]

1. Authentification principale initiée vers Cisco ISE.
2. Cisco ASA 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:

- Administrateur Active Directory : Il est utilisé comme compte d'annuaire pour permettre 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 2FA secondaire.

Configurations Active Directory

Windows Server est préconfiguré avec les services de domaine Active Directory.

Remarque : Si RADIUS Duo Auth Proxy Manager s'exécute sur le même ordinateur hôte Active Directory, les rôles NPS (Network Policy Server) doivent être désinstallés/supprimés. Si les deux services RADIUS fonctionnent, ils peuvent entrer en conflit et affecter les performances.

Pour obtenir la configuration AD pour l'authentification et l'identité 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 terminée sur le serveur proxy ASA et Duo Auth.

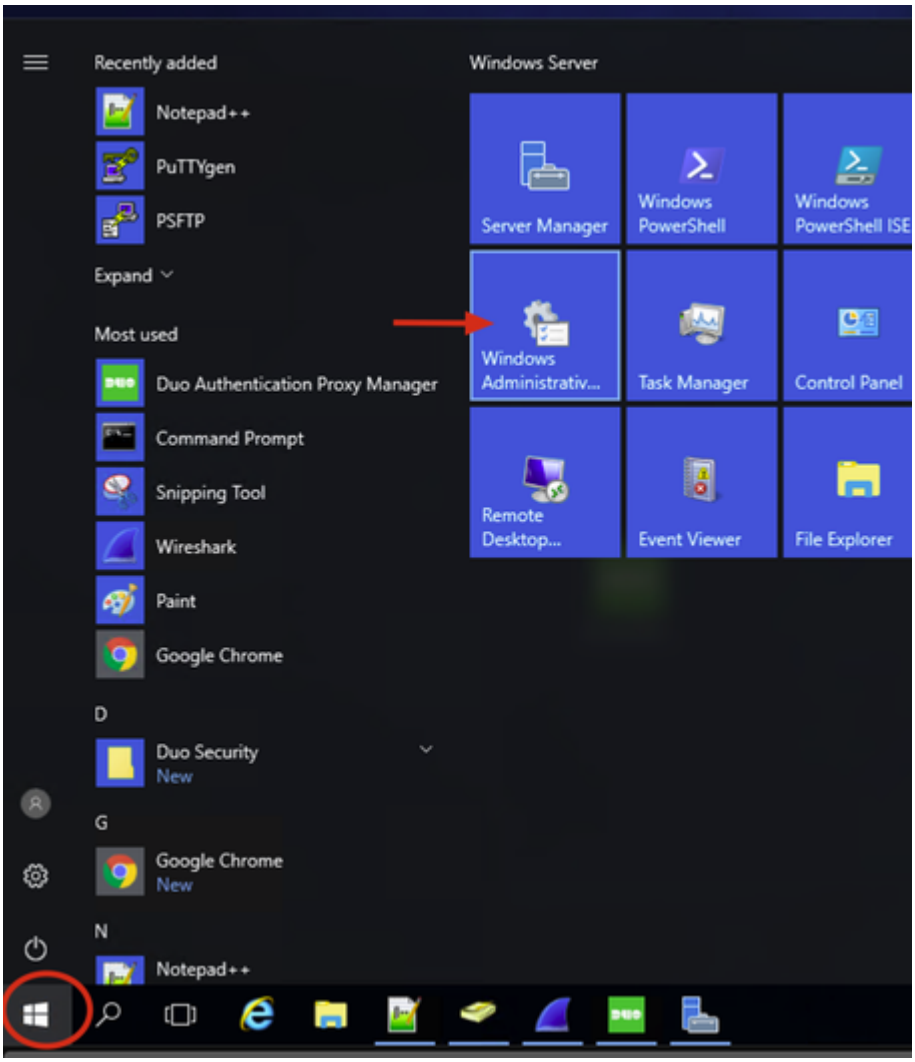
Les principales valeurs sont les suivantes :

- Nom de domaine : Il s'agit du nom de domaine du serveur. Dans ce guide de configuration, agarciam.cisco est le nom de domaine.
- Server IP/Fully Qualified Domain Name (FQDN) Address : adresse IP ou FQDN utilisée pour atteindre le serveur Microsoft. Si un nom de domaine complet est utilisé, un serveur DNS doit être configuré dans ASA et le proxy 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.
- Autorité de certification 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 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 alerte Active Directory pour commencer à rechercher et à authentifier 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. Pour ajouter un nouvel utilisateur Duo sur Windows Server, accédez à l'icône Windows en bas à gauche, puis cliquez sur Outils d'administration Windows :



---

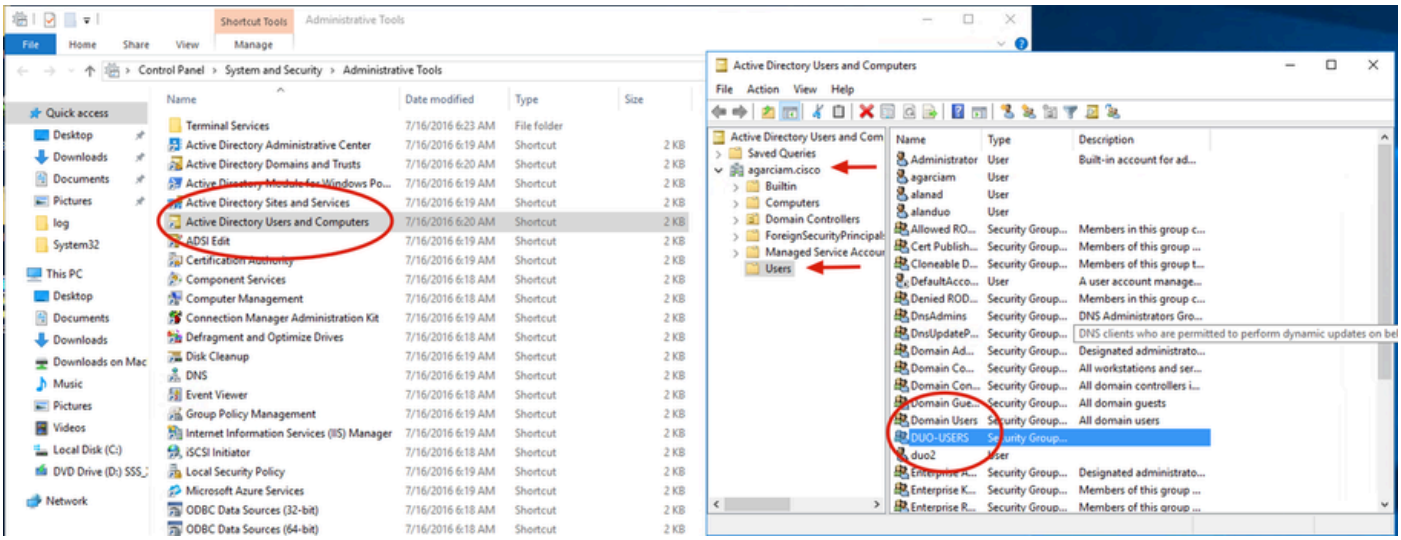
2. Dans la fenêtre Outils d'administration Windows, accédez à Utilisateurs et ordinateurs Active Directory.

---

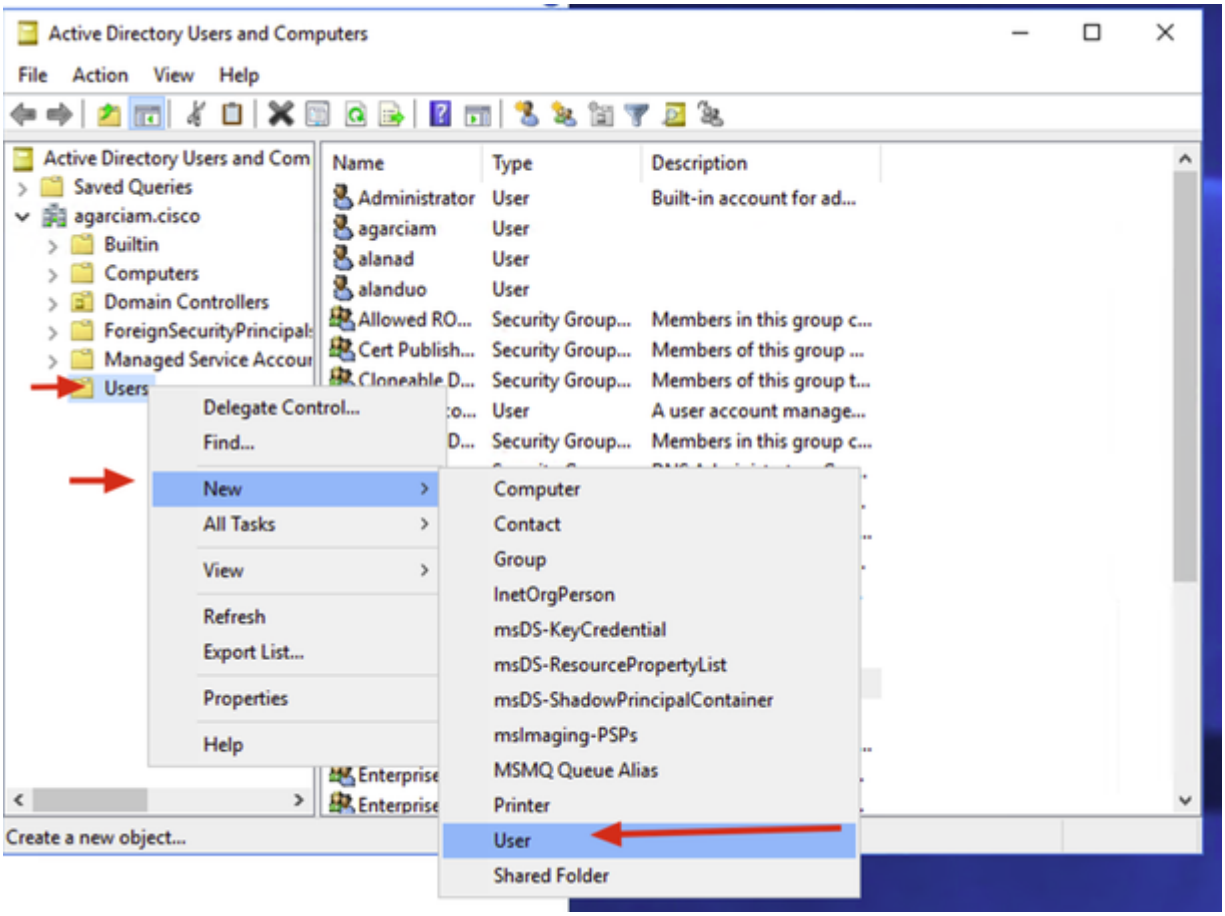
3. Dans le panneau Utilisateurs et ordinateurs Active Directory, développez l'option de domaine et accédez au dossier Utilisateurs.

---

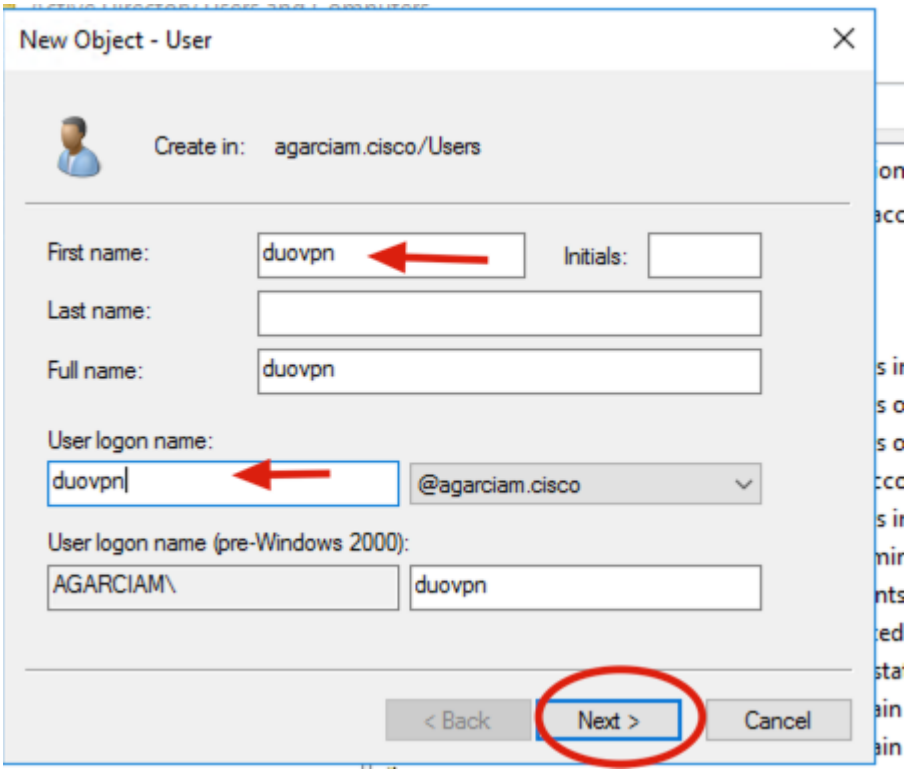
4. Dans cet exemple de configuration, Duo-USERS est utilisé comme groupe cible pour l'authentification secondaire.



5. Cliquez avec le bouton droit sur le dossier Users et sélectionnez New > User :

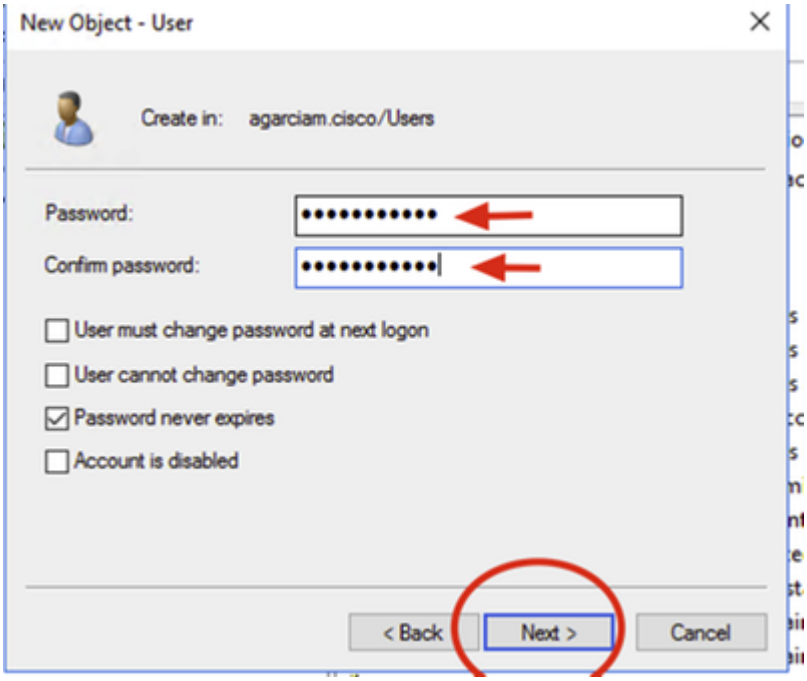


6. Dans la fenêtre Nouvel objet-utilisateur, spécifiez les attributs d'identité du nouvel utilisateur et cliquez sur Suivant :



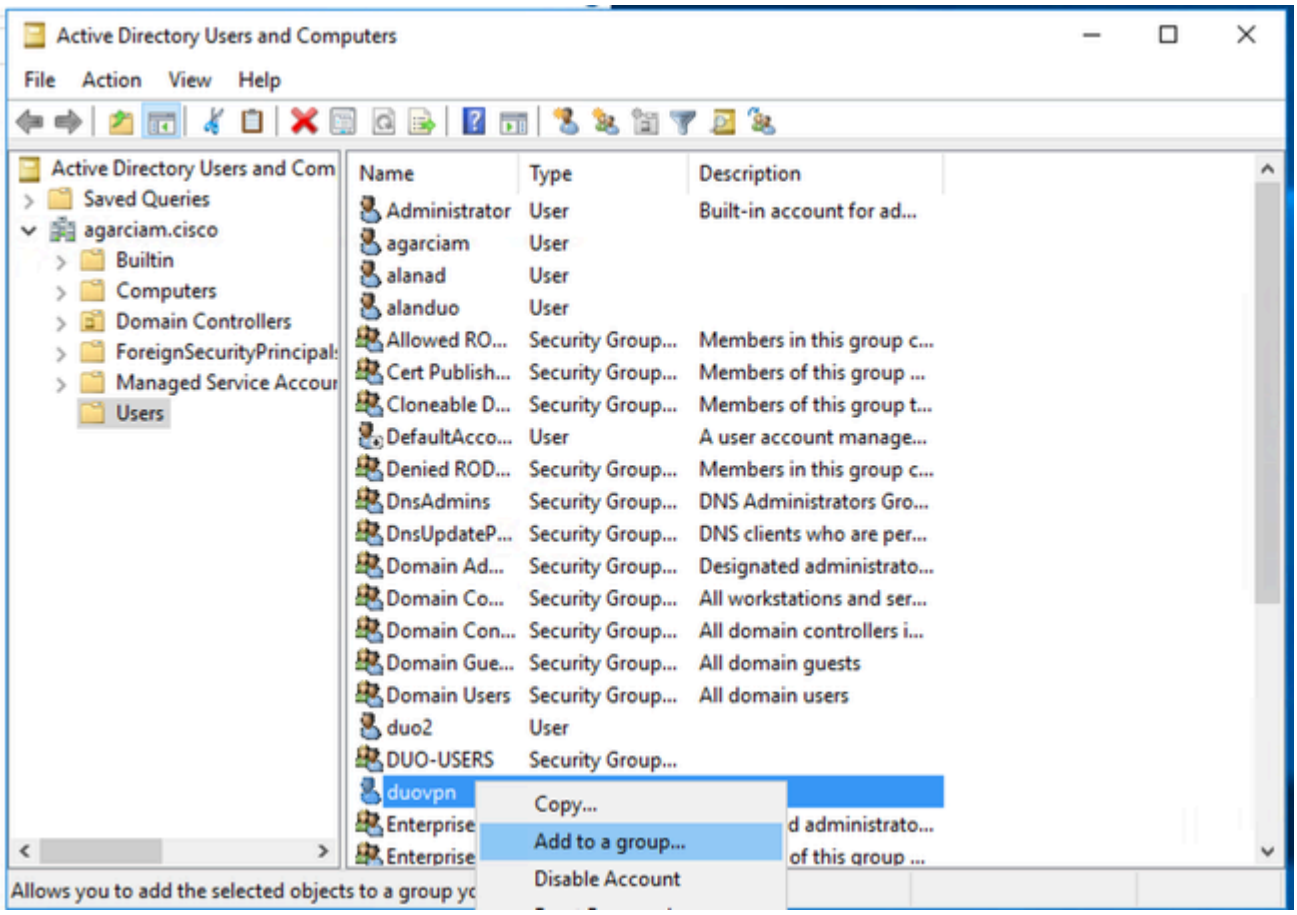
---

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



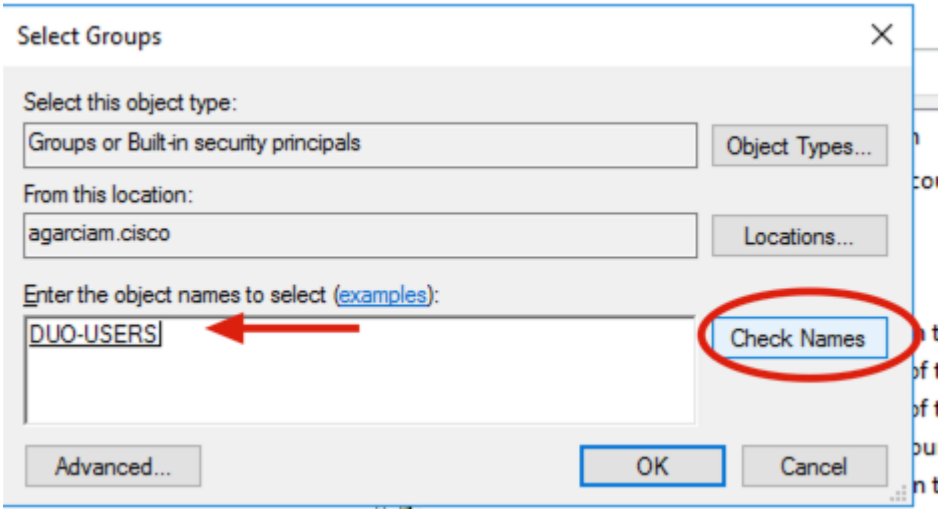
---

8. Affectez le nouvel utilisateur à un groupe spécifique, cliquez avec le bouton droit de la souris et sélectionnez Ajouter à un groupe :



---

9. 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.

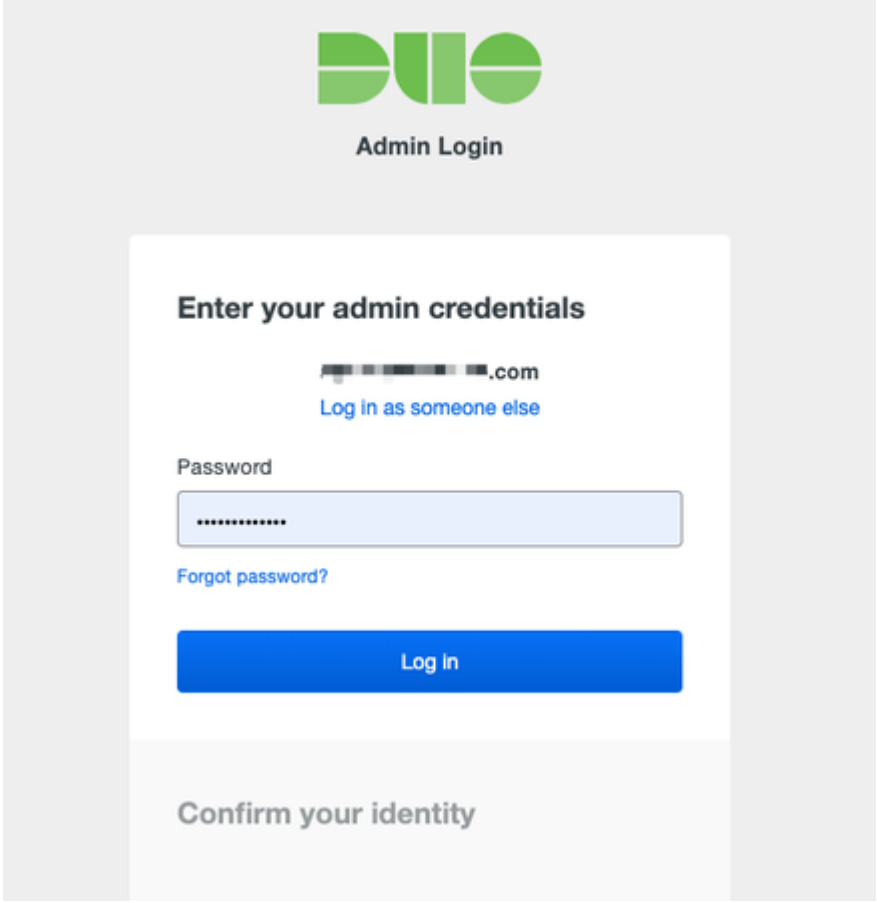


---

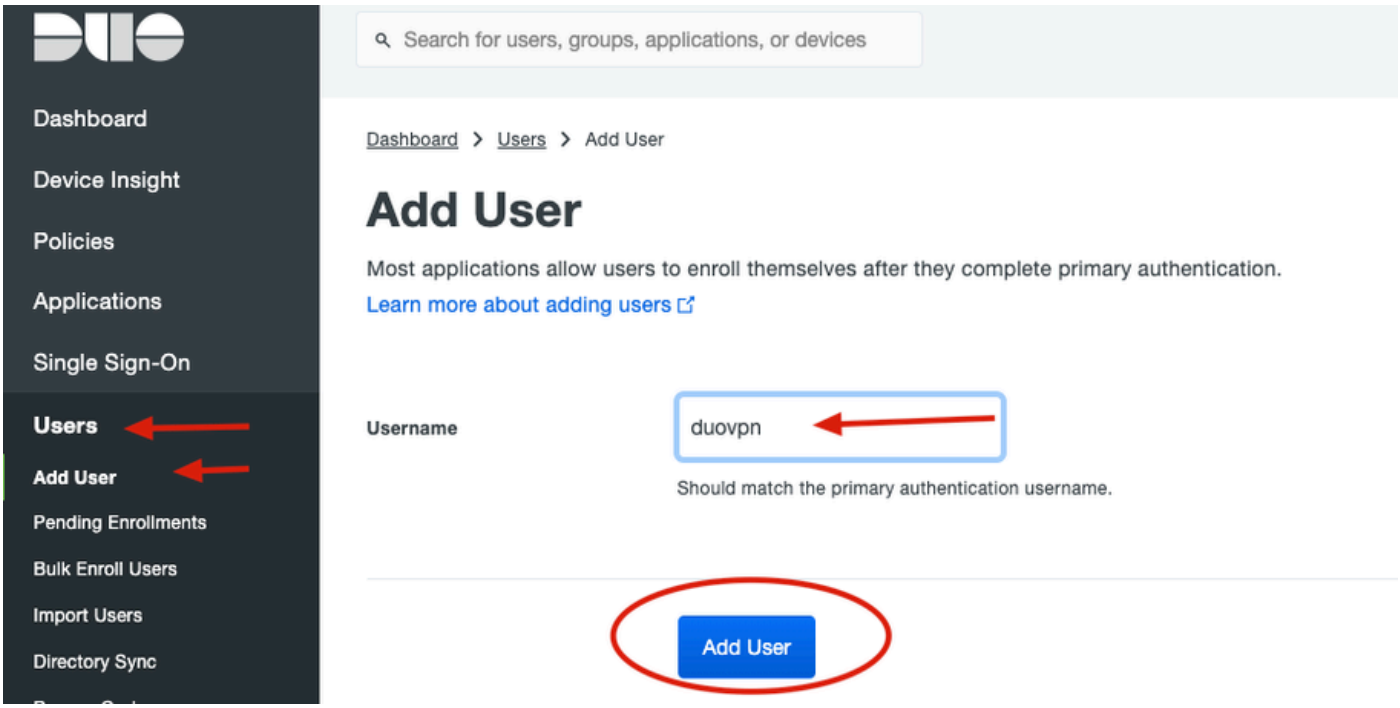
10. Il s'agit de l'utilisateur utilisé dans ce document à titre d'exemple.

Configurations Duo

1. Connectez-vous au portail Duo Admin.

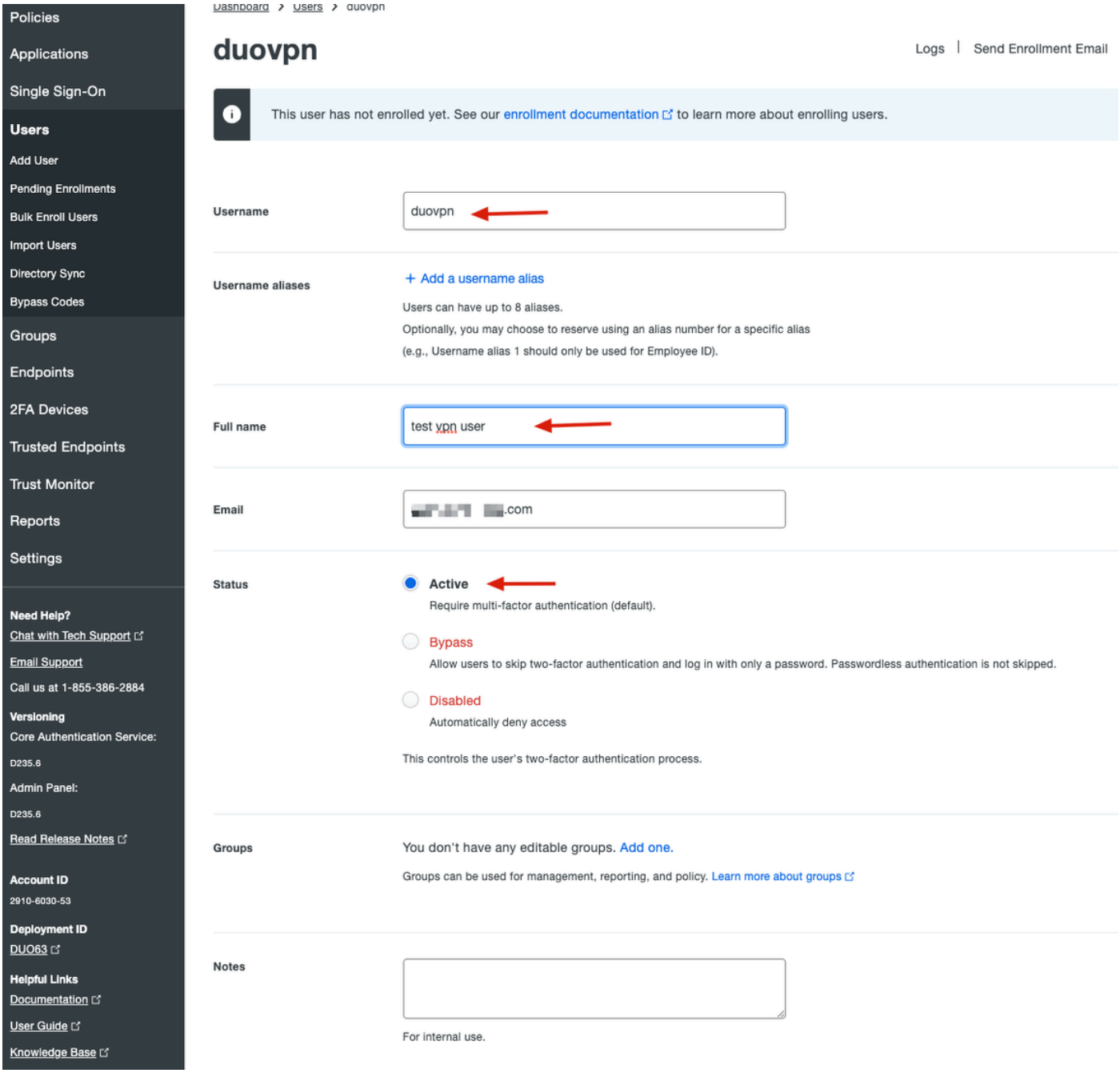


2.Dans le panneau de gauche, accédez à Users, cliquez sur Add User et tapez le nom de l'utilisateur qui correspond au nom d'utilisateur du domaine actif, puis cliquez sur Add User.



---

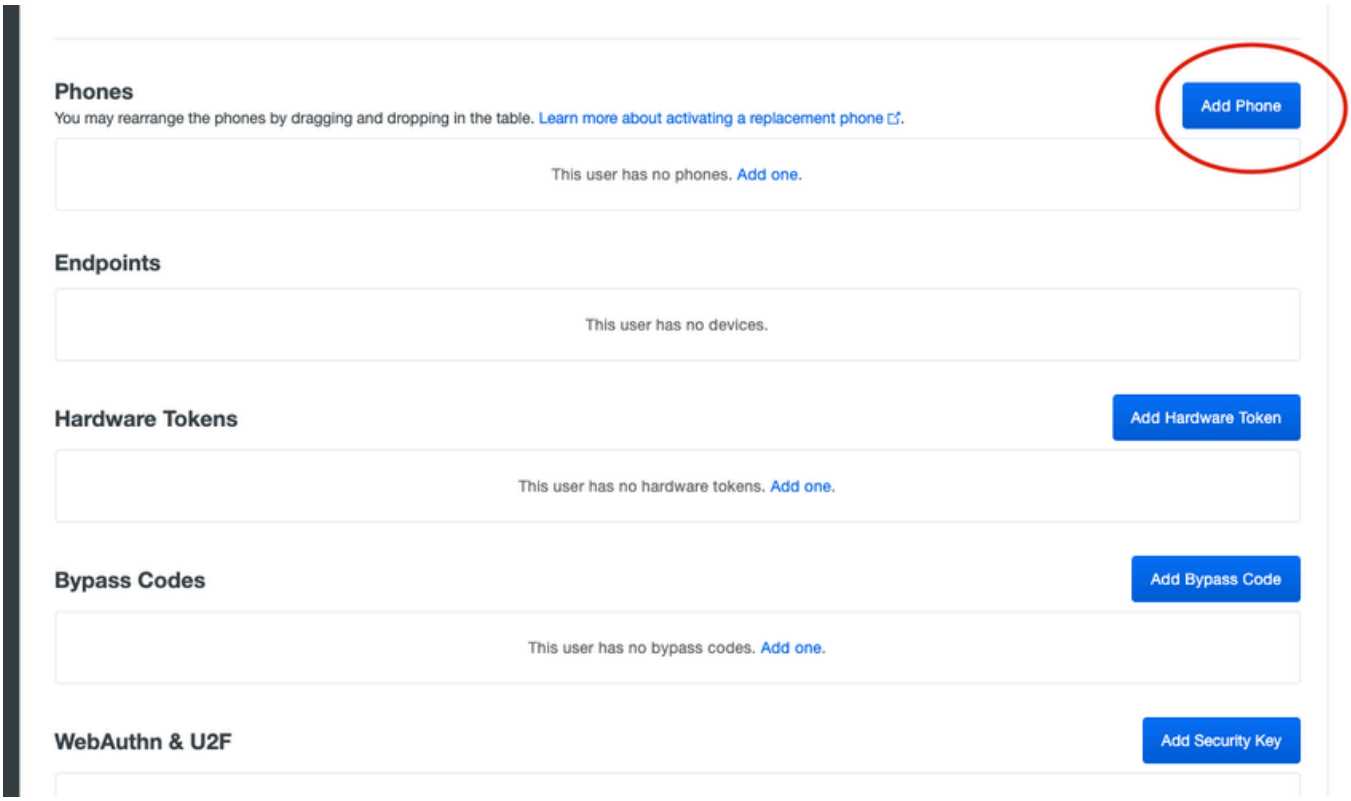
3. Dans le nouveau panneau utilisateur, renseignez toutes les informations nécessaires.



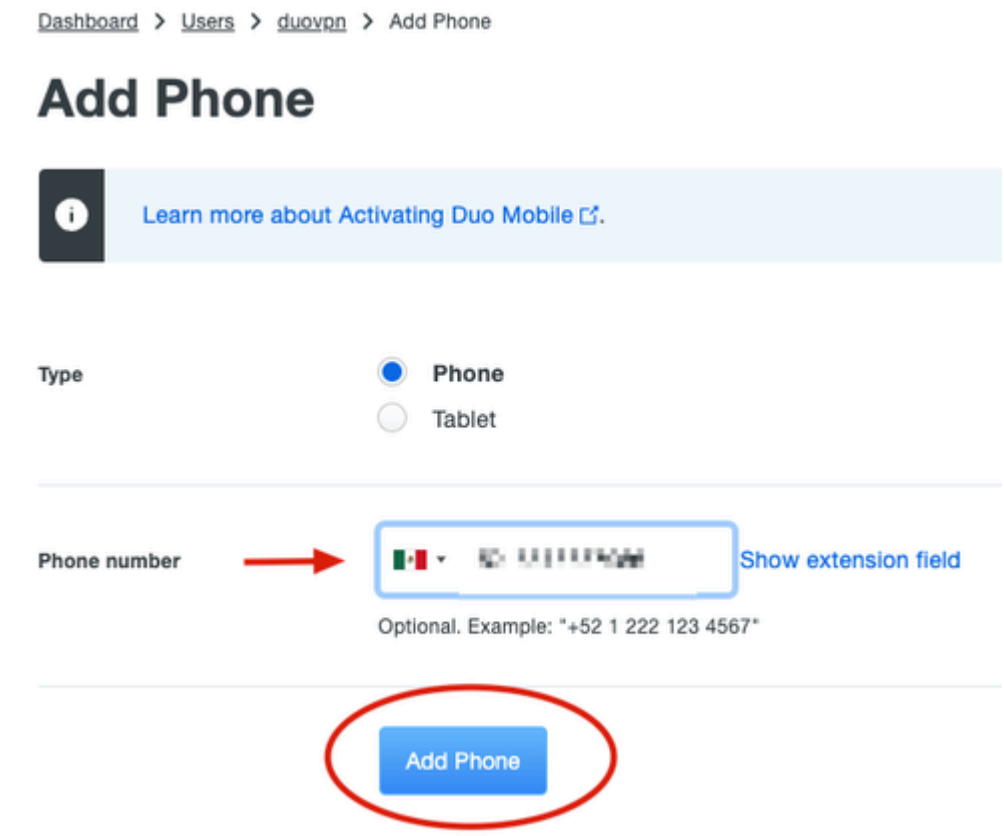
4. Sous user devices, spécifiez la méthode d'authentification secondaire.

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

5. Cliquez sur Ajouter un téléphone.

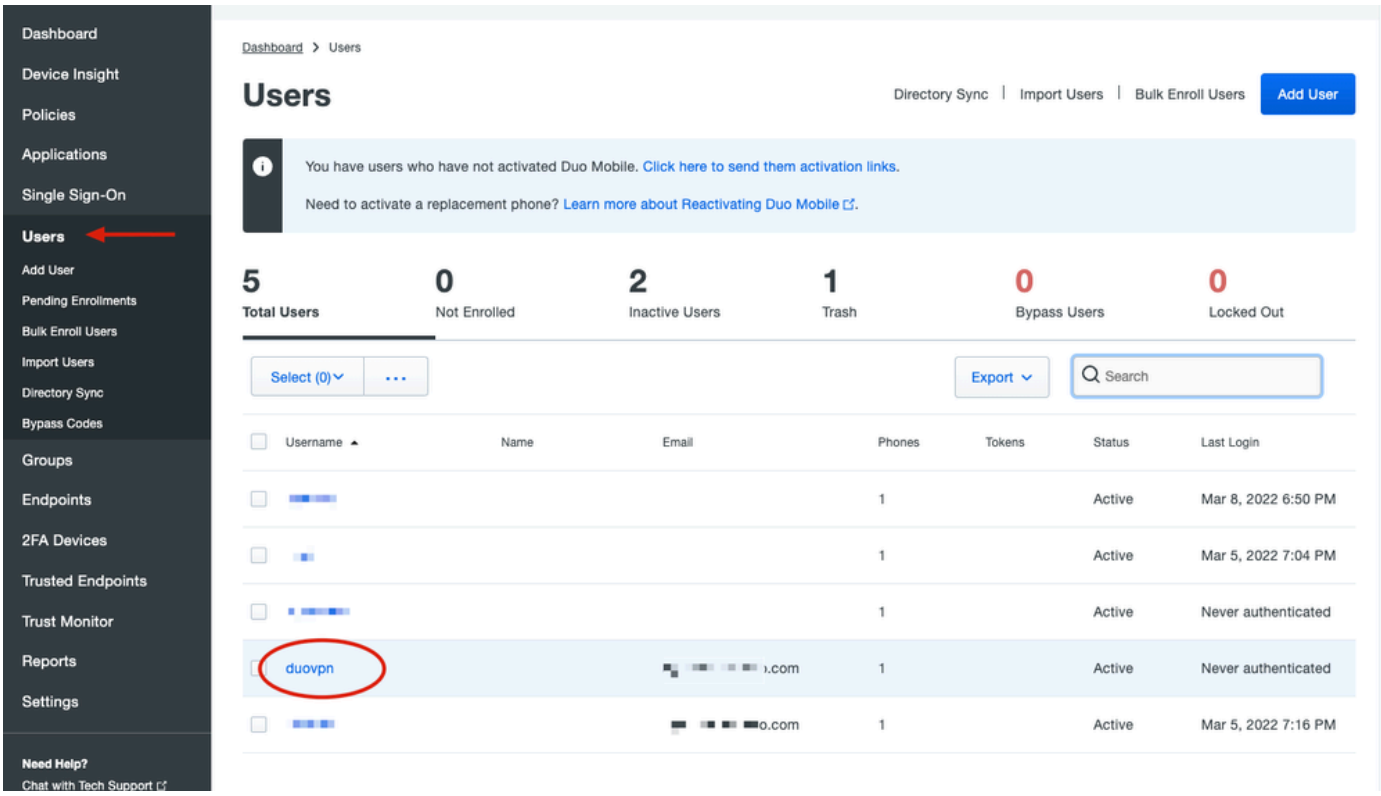


6. Tapez le numéro de téléphone de l'utilisateur et cliquez sur Ajouter un téléphone.



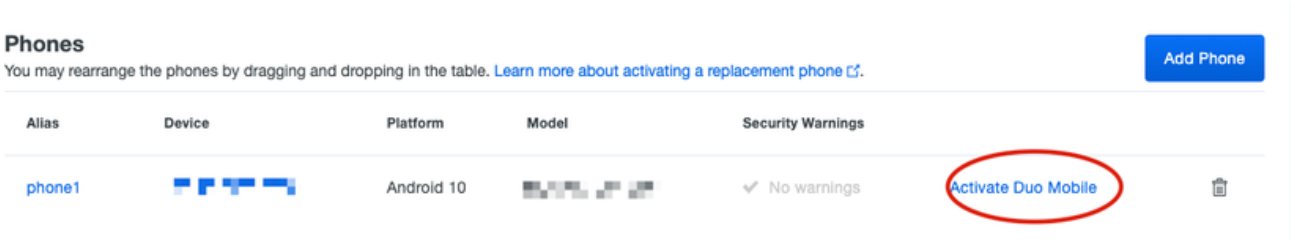
7. Dans le panneau d'administration Duo de gauche, accédez à Utilisateurs et cliquez sur le

nouvel utilisateur.

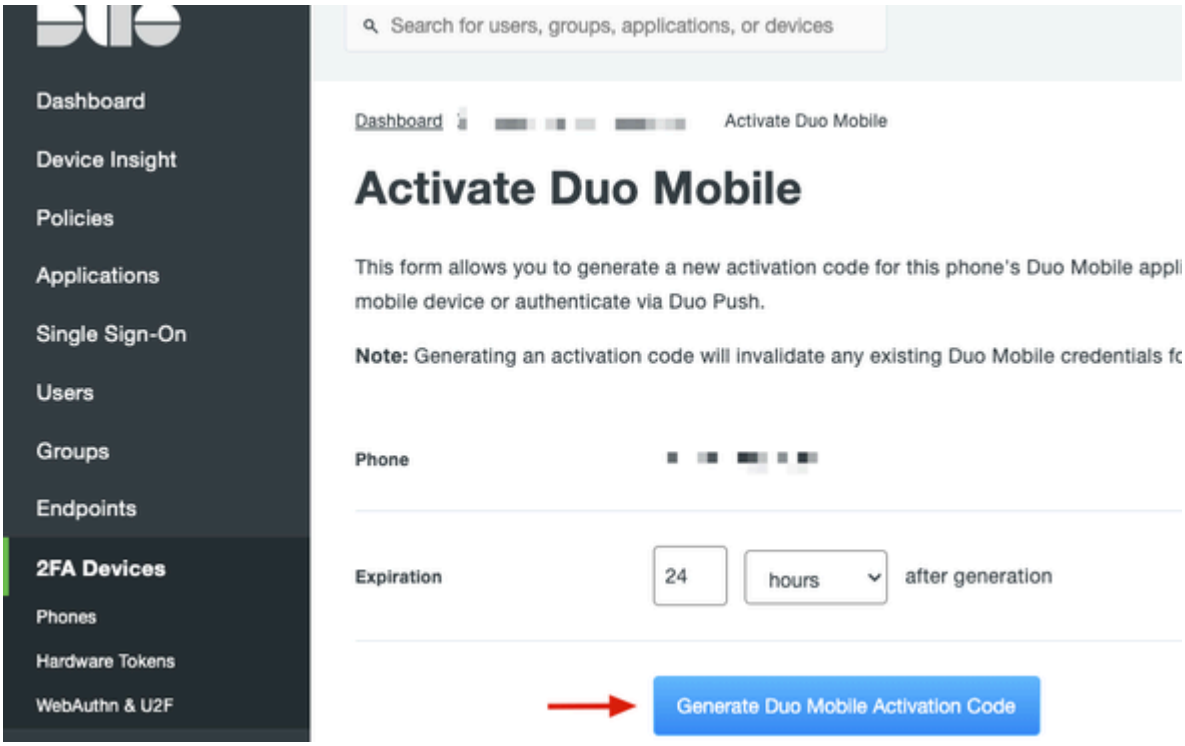


Remarque : Si vous n'avez pas accès à votre téléphone au moment de la configuration, vous pouvez sélectionner l'option de messagerie.

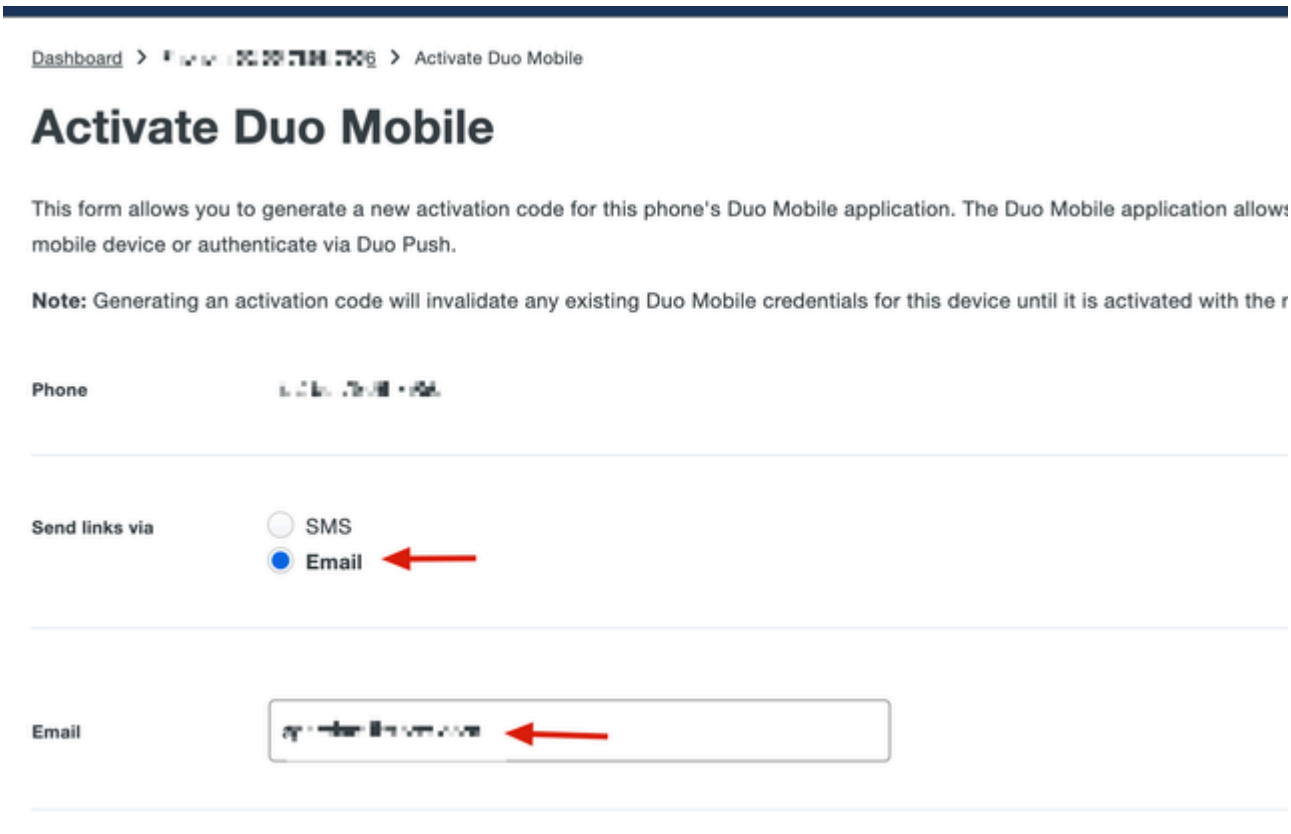
8. Accédez à la section Téléphones et cliquez sur Activer Duo Mobile.



9. Cliquez sur Générer le code d'activation Duo Mobile.



10. Sélectionnez E-mail pour recevoir les instructions par e-mail, tapez votre adresse e-mail et cliquez sur Envoyer les instructions par e-mail.



11. Vous recevez un e-mail contenant les instructions.

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] 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

---

12. 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.

---

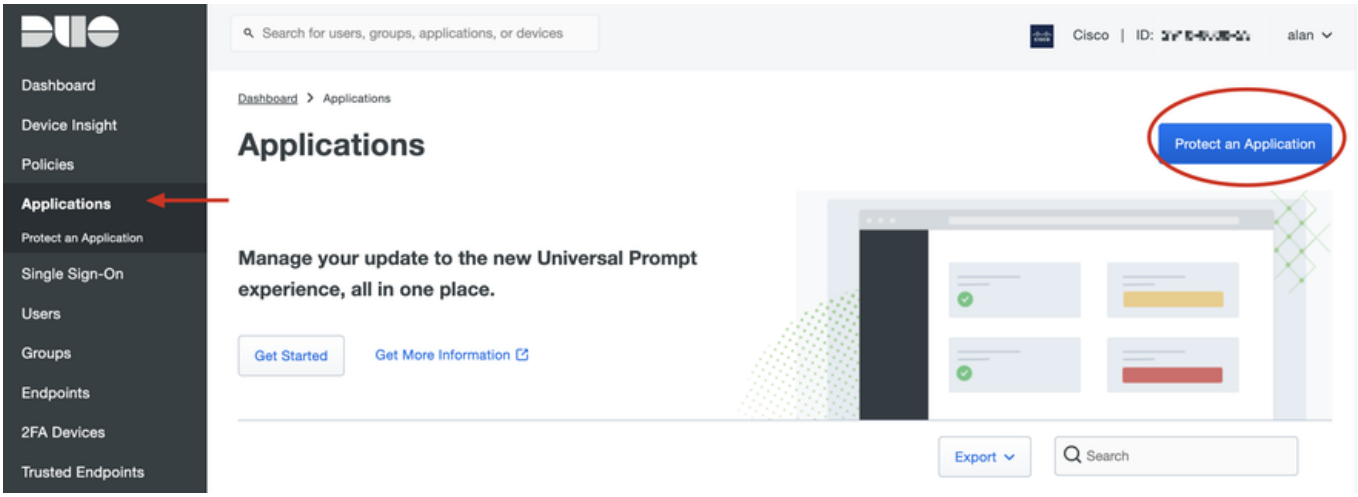
13. Le nouvel utilisateur est ajouté à votre application mobile Duo.

Configuration du proxy Duo Auth

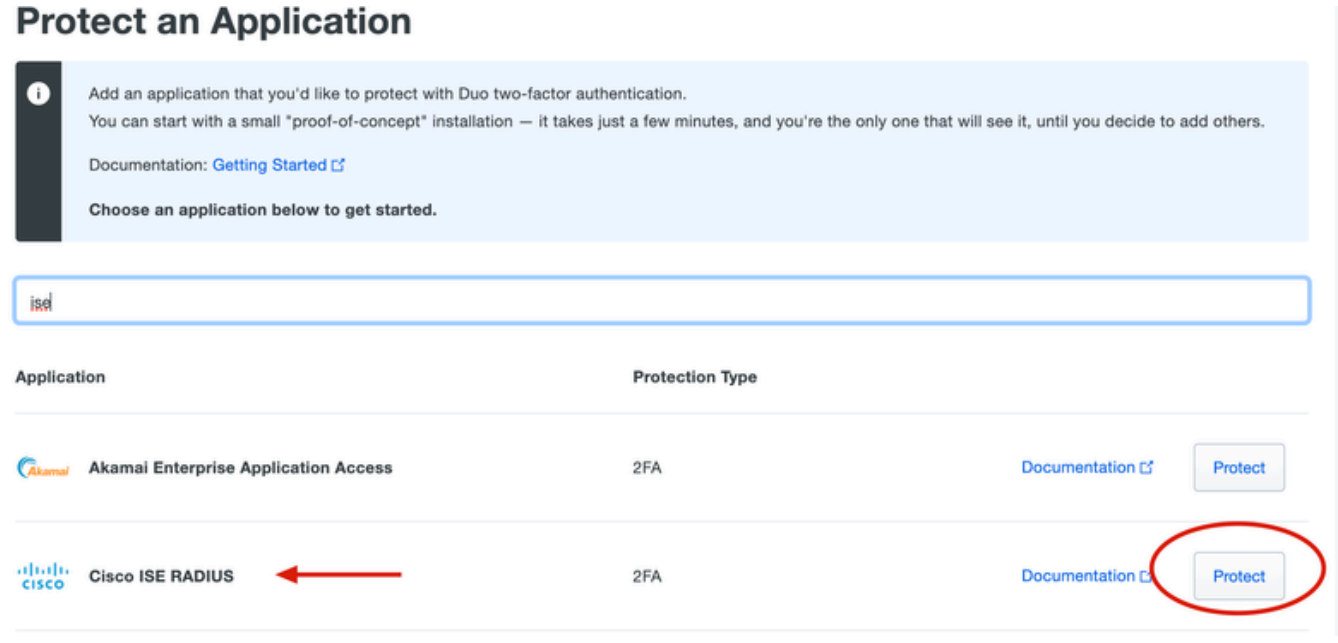
1. Téléchargez et installez Duo Auth Proxy Manager à partir de Cisco Duo Authentication.

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

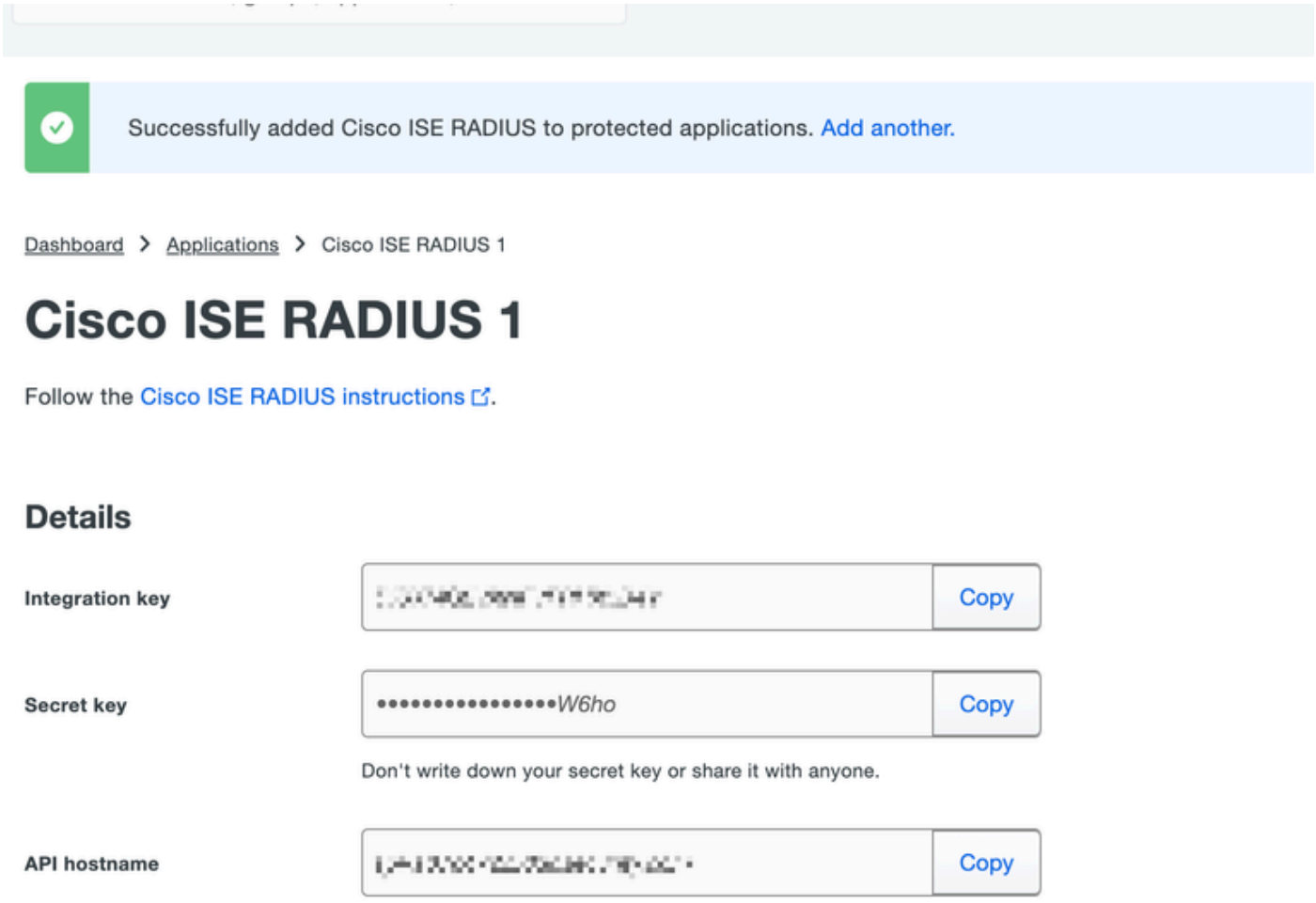
2. Dans le panneau d'administration Duo, accédez à Applications et cliquez sur Protéger une application.



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

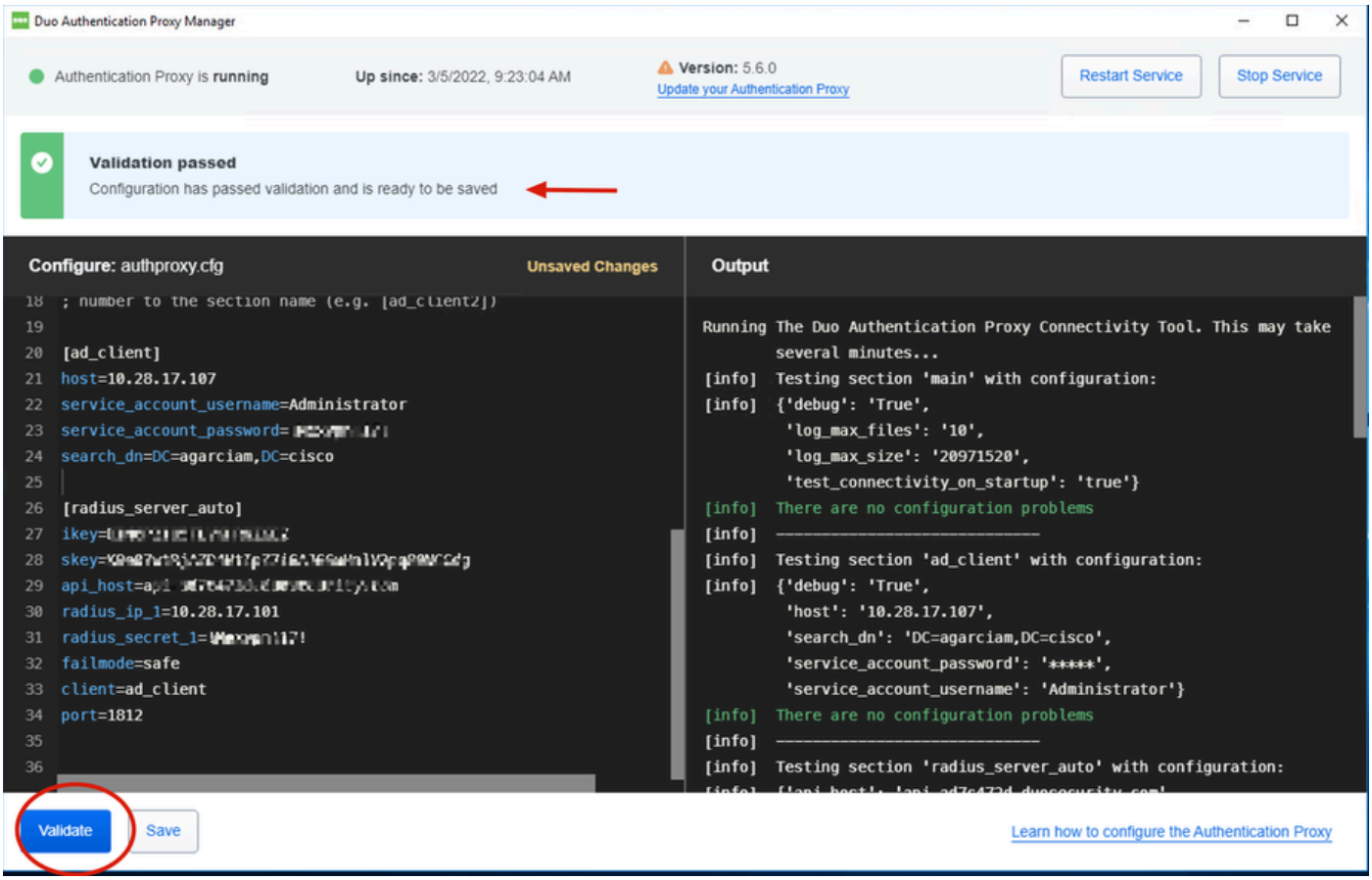


4. Copiez la clé d'intégration, la clé secrète et le nom d'hôte de l'API. Vous avez besoin de ces informations pour la configuration du proxy d'authentification duo.



5. Exécutez l'application Duo Authentication Proxy Manager et terminez la configuration du client Active Directory et du serveur RADIUS ISE, puis cliquez sur Valider.

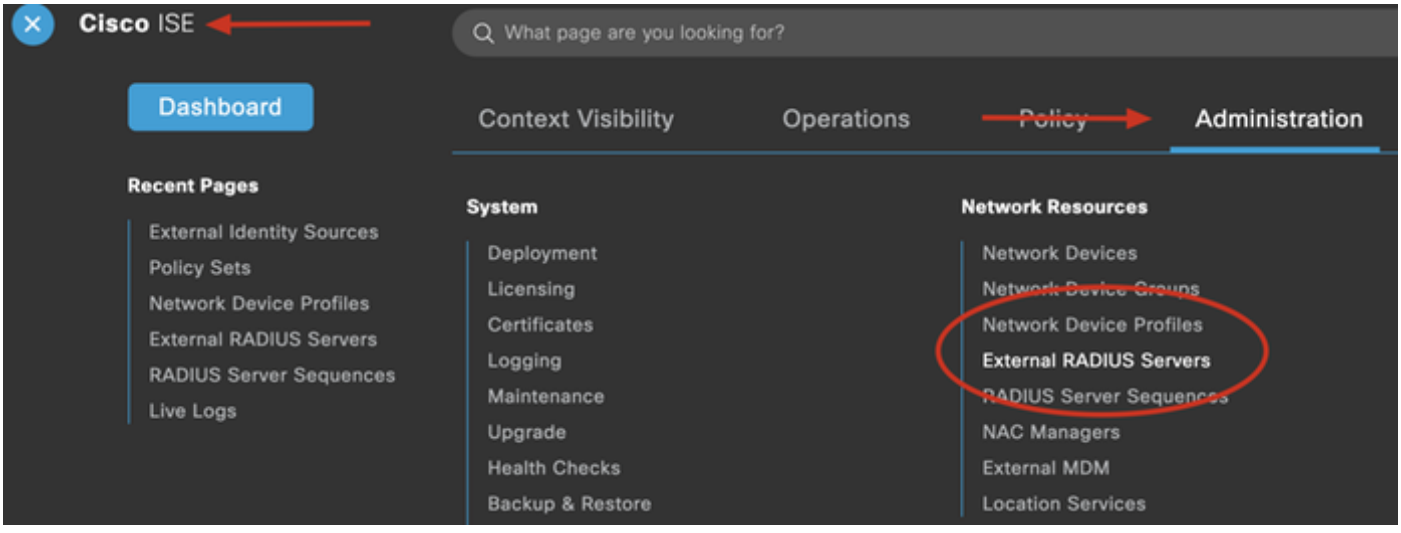
Remarque : si la validation échoue, reportez-vous à l'onglet debug pour plus de détails et corrigez-les en conséquence.



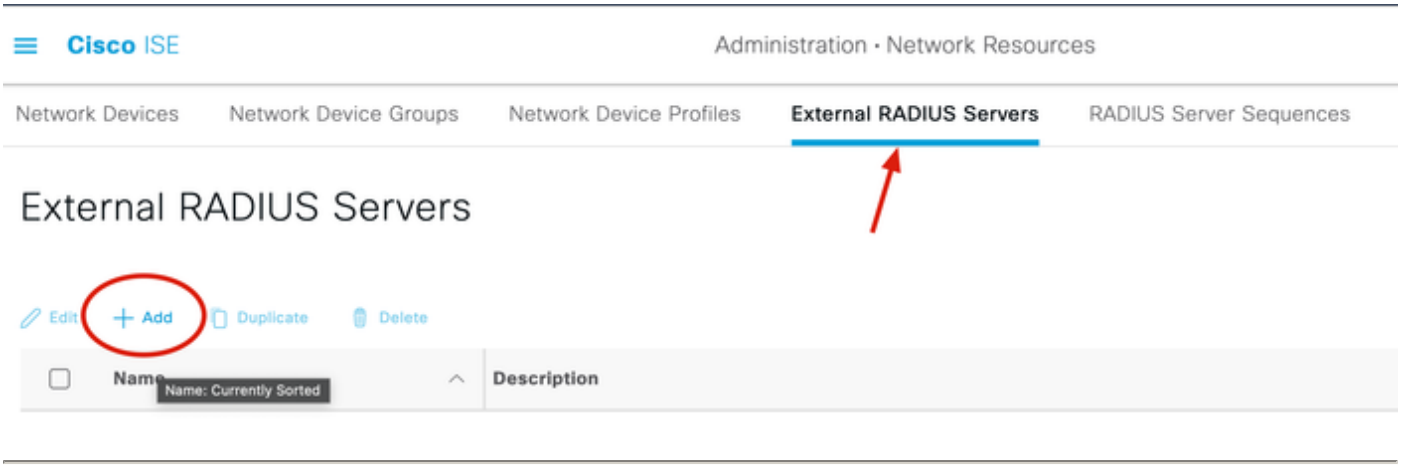
Configurations Cisco ISE

1. Connectez-vous au portail d'administration ISE.

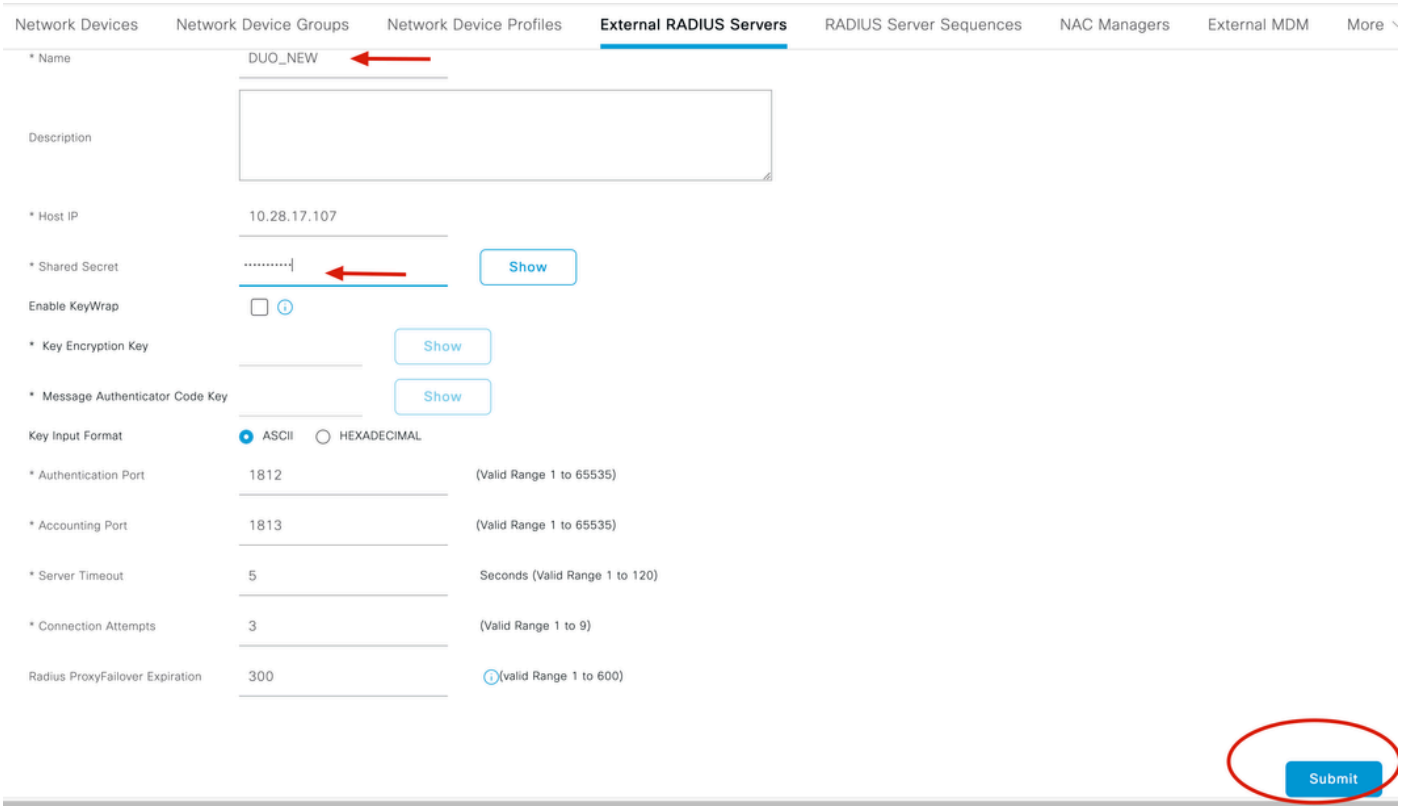
2. Développez l'onglet Cisco ISE et accédez à Administration, puis cliquez sur Network Resources, et cliquez sur External RADIUS Servers.



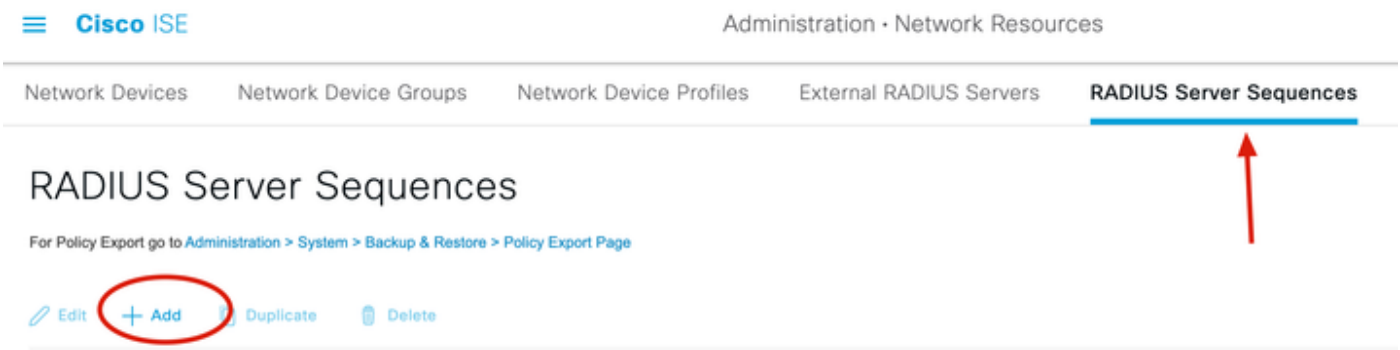
3. Dans l'onglet Serveurs Radius externes, cliquez sur Ajouter.



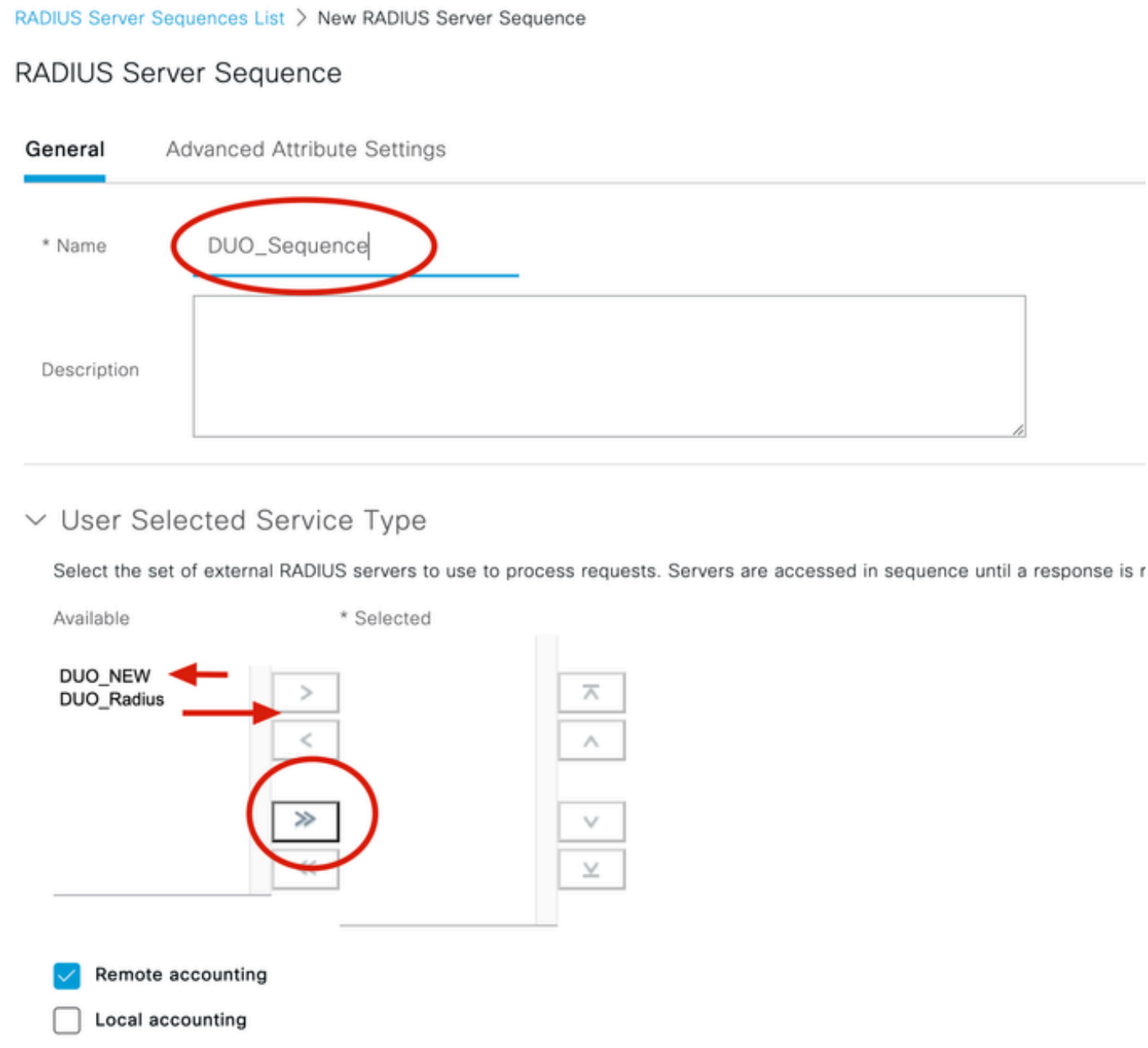
4. Complétez la zone vide avec la configuration RADIUS utilisée dans le Duo Authentication Proxy Manager et cliquez sur Submit.



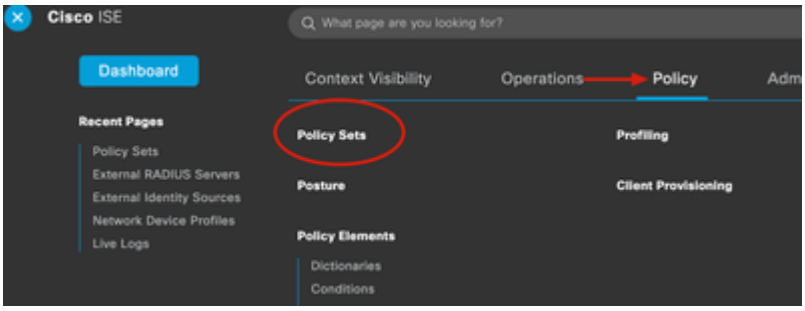
5. Accédez à l'onglet Séquences de serveur RADIUS et cliquez sur Ajouter.



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

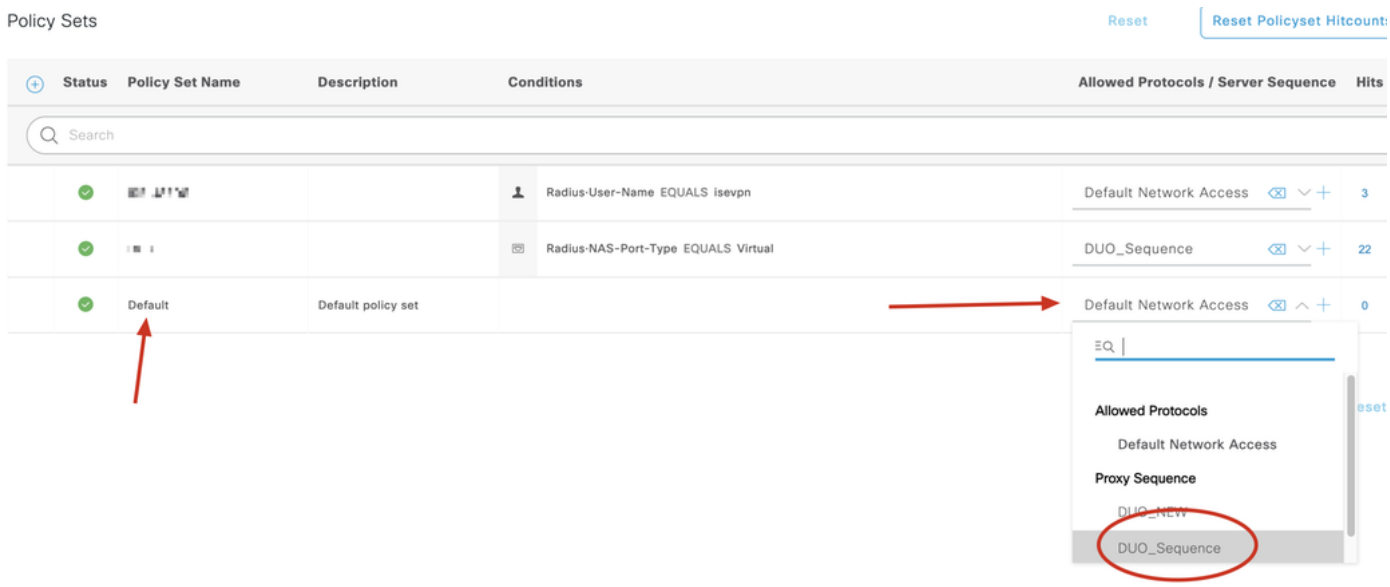


7. Accédez à Stratégie à partir du menu Tableau de bord, puis cliquez sur Jeux de stratégies.



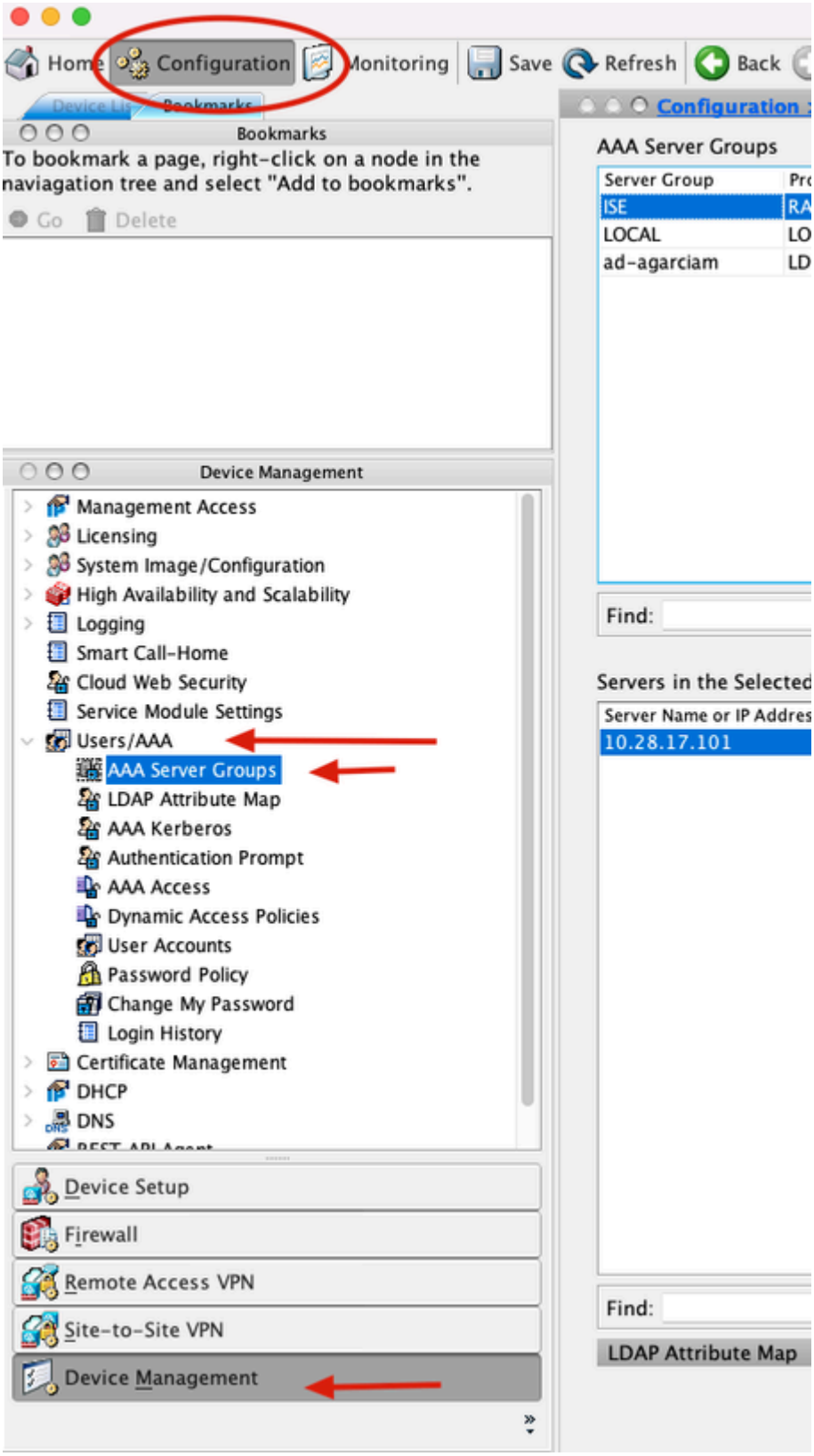
8. Affectez la séquence RADIUS à la stratégie par défaut.

Remarque : La séquence duo de toutes les connexions est appliquée avec la stratégie par défaut utilisée ; l'affectation des stratégies peut varier.



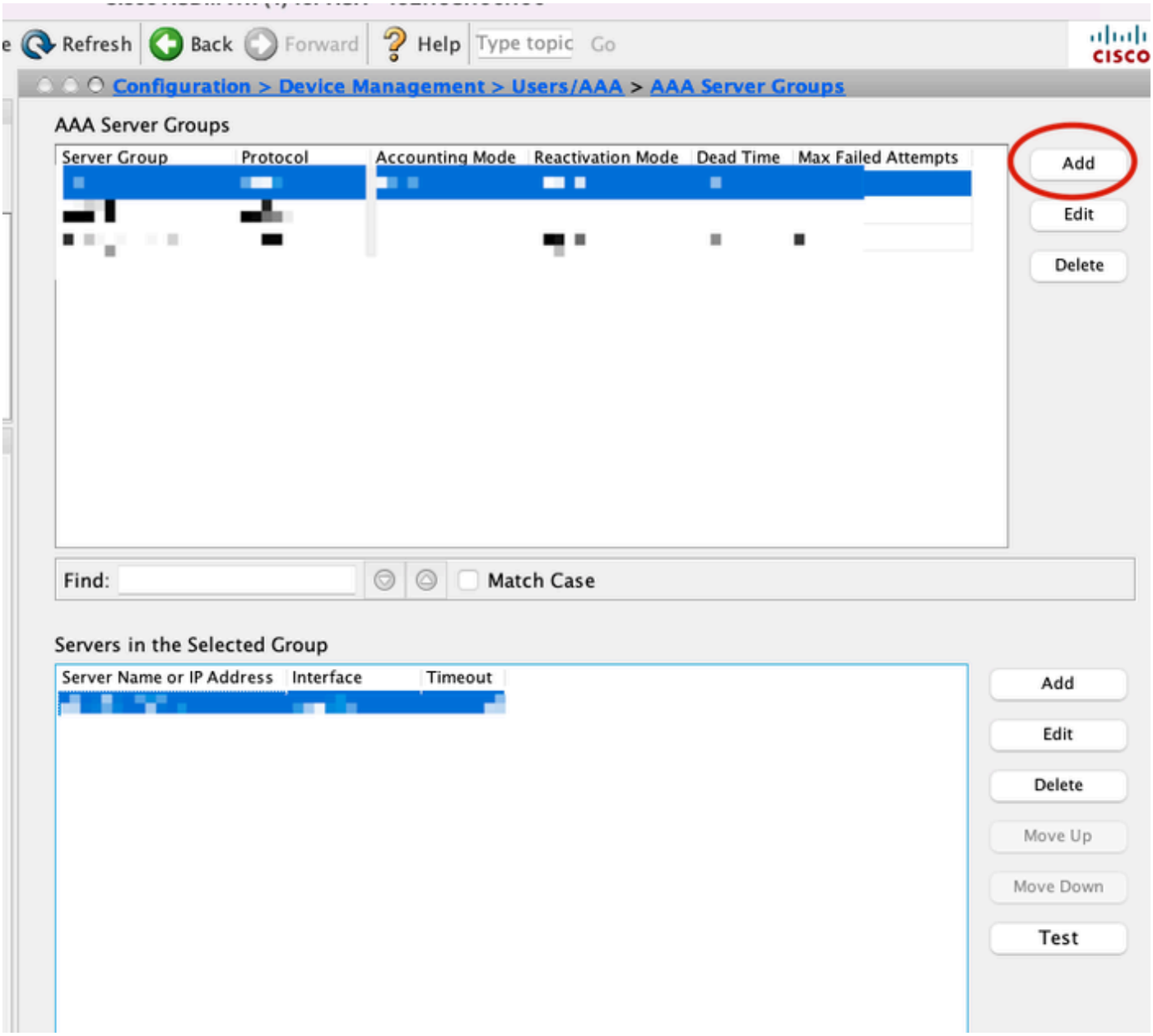
Configuration de Cisco ASA RADIUS/ISE

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



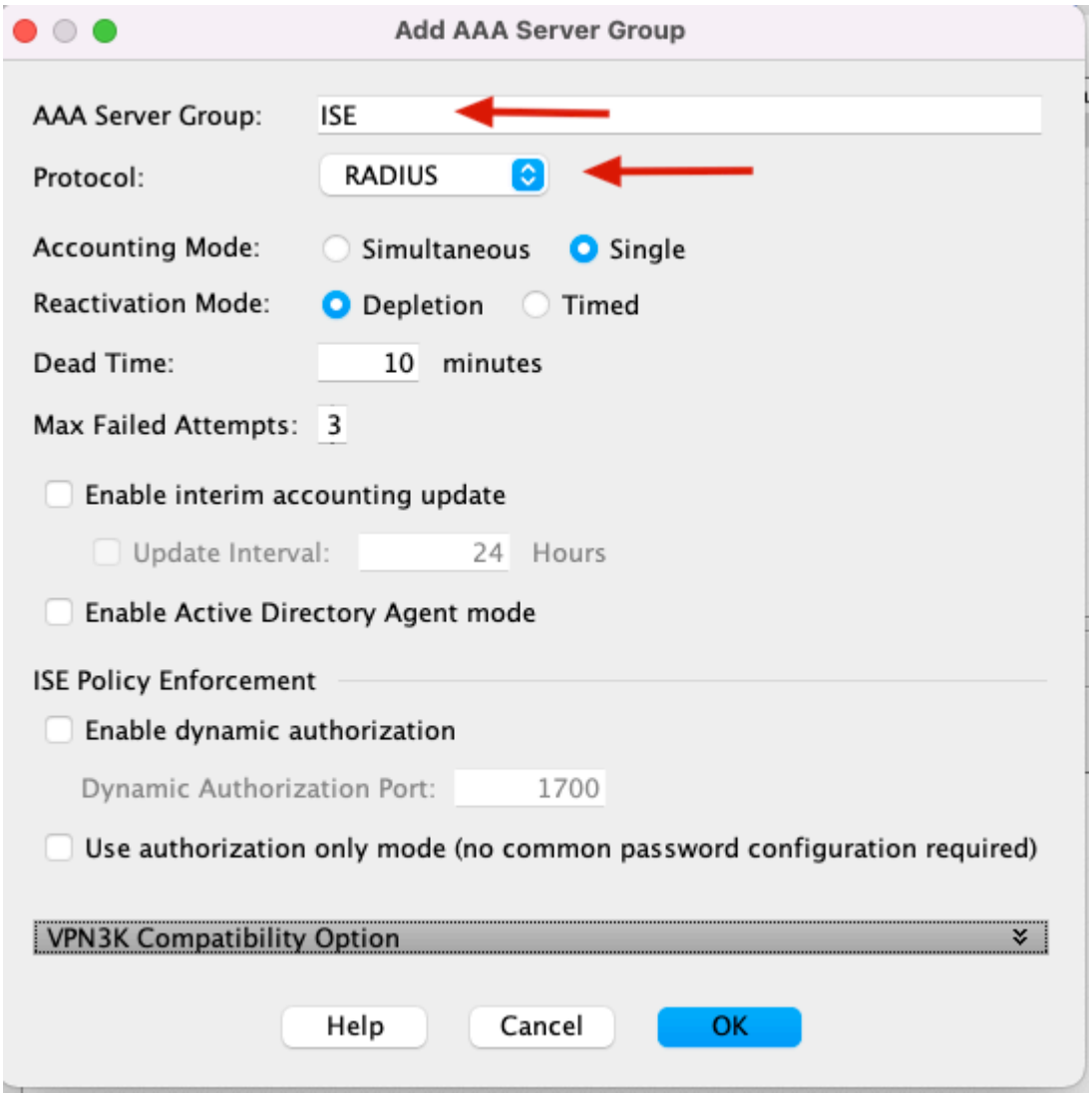
---

2. Dans le panneau AAA Server Groups, cliquez sur Add.



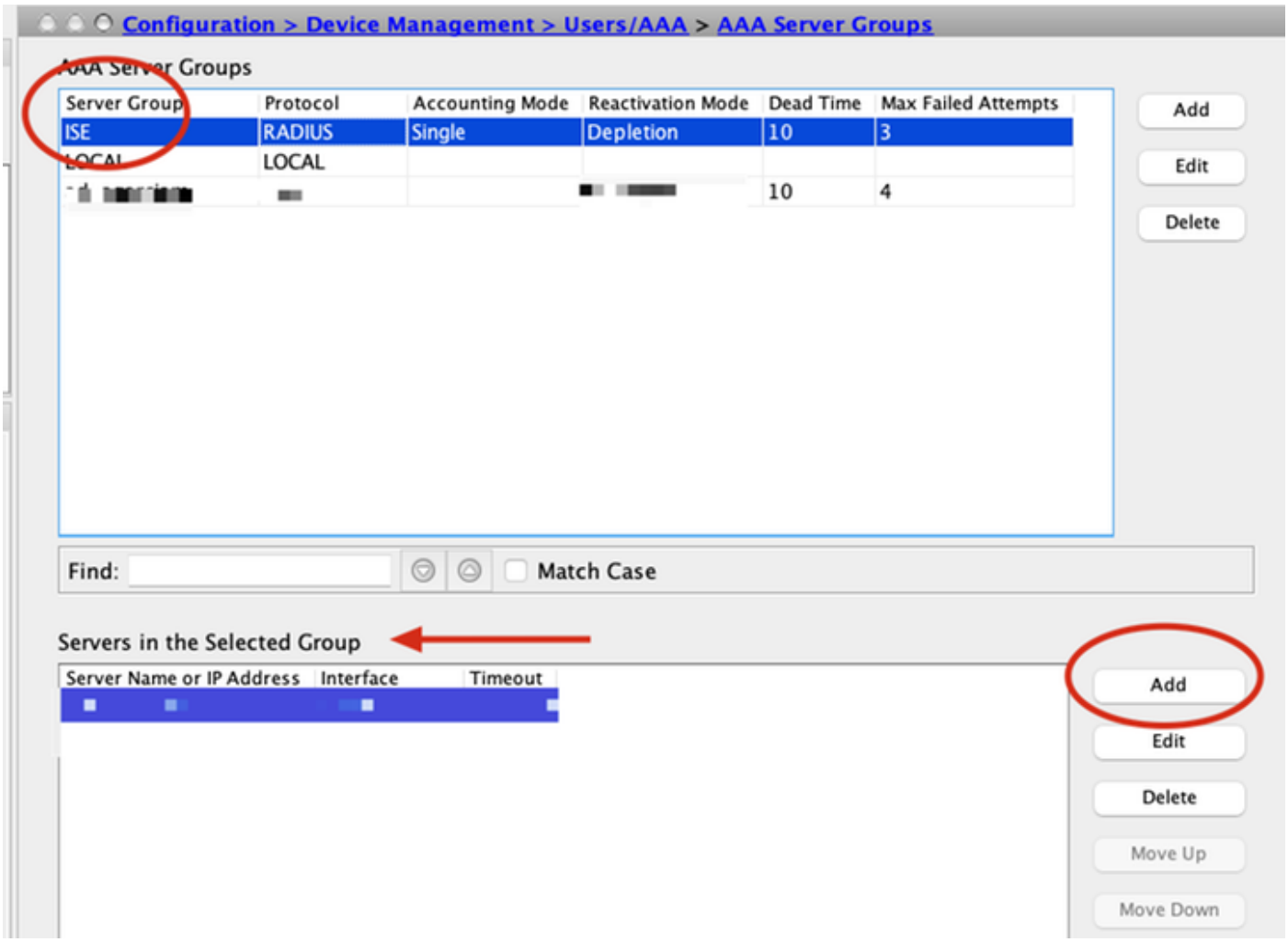
---

3. Sélectionnez le nom du groupe de serveurs et spécifiez RADIUS comme protocole à utiliser, puis cliquez sur OK.



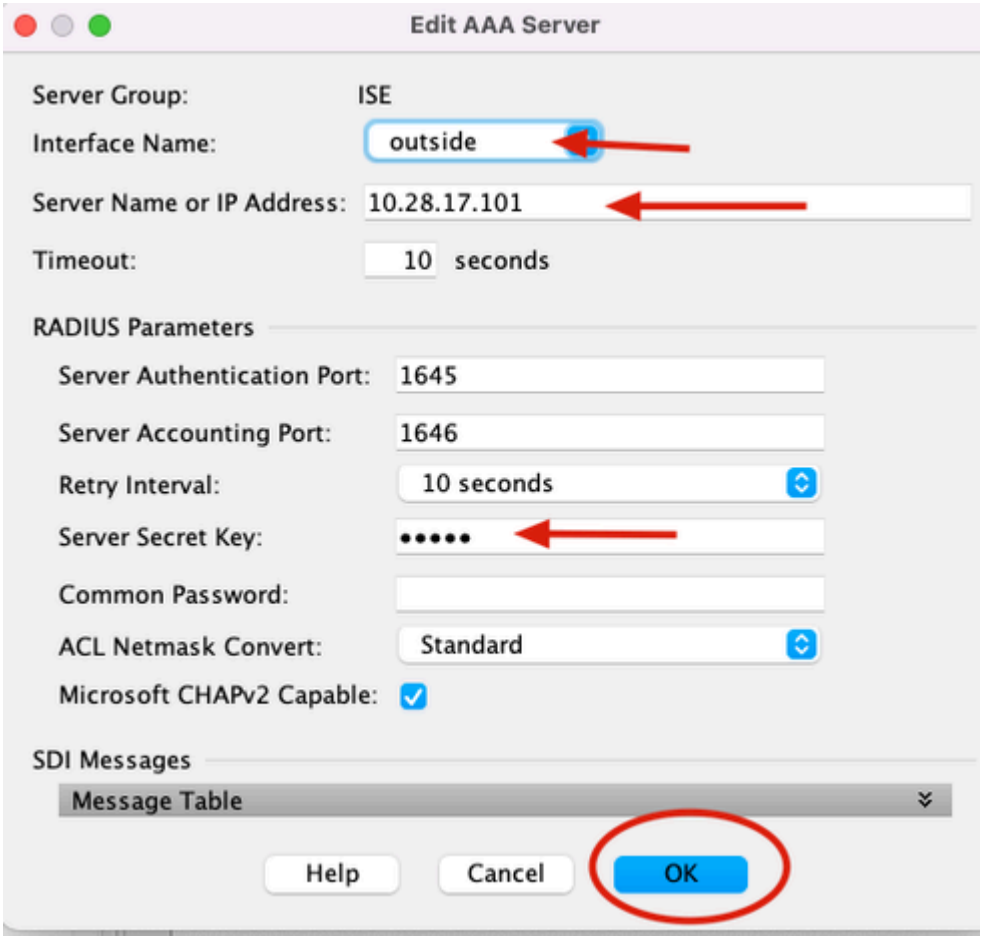
---

5. Sélectionnez votre nouveau groupe de serveurs et cliquez sur Ajouter sous Serveurs dans le panneau Groupe sélectionné :



6. Dans la fenêtre Edit AAA Server, sélectionnez le nom de l'interface, spécifiez l'adresse IP du serveur ISE et tapez la clé secrète RADIUS, puis cliquez sur OK.

Remarque : Toutes les informations doivent correspondre à celles spécifiées dans le Duo Authentication Proxy Manager.



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 Cisco Secure Client/AnyConnect sur votre PC. Spécifiez le nom d'hôte de la tête de réseau VPN ASA et connectez-vous avec l'utilisateur créé pour l'authentification Duo secondaire, puis cliquez sur OK.

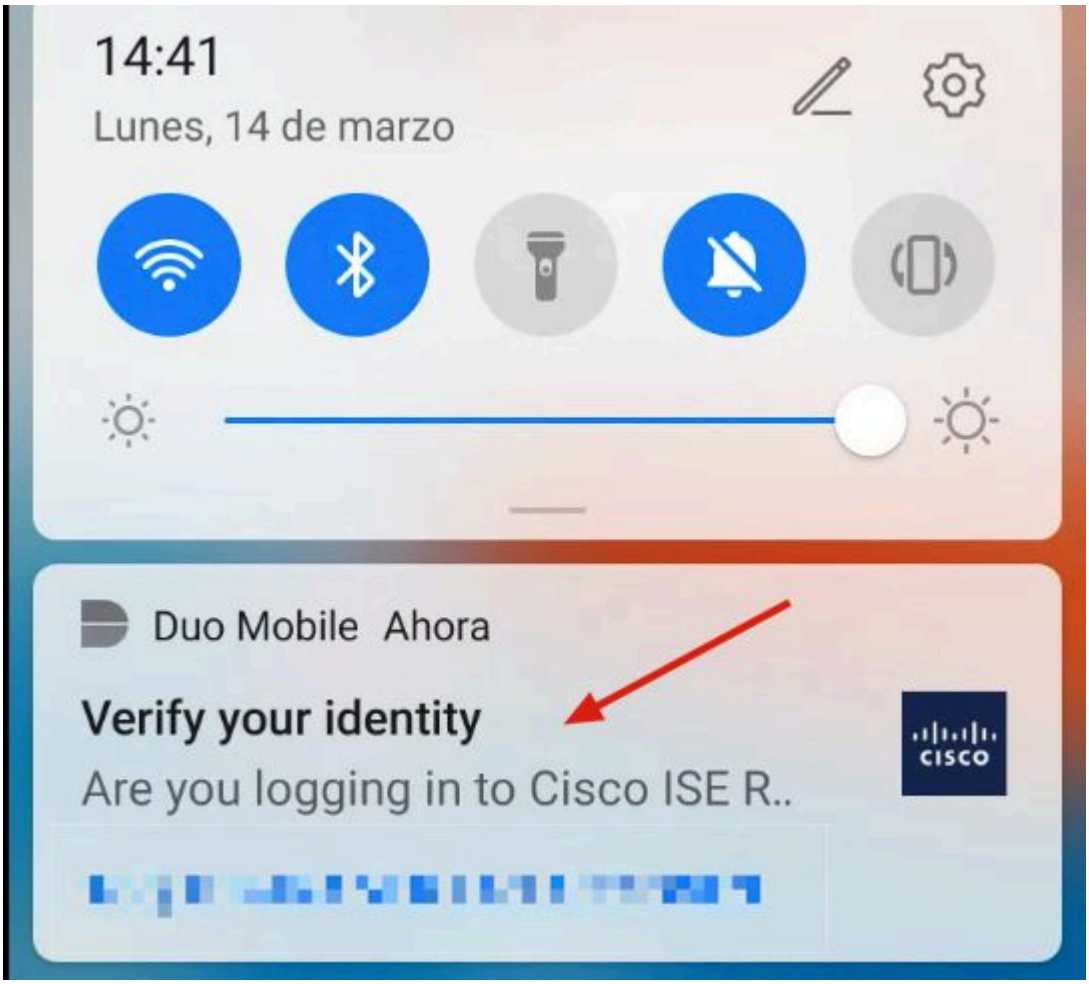


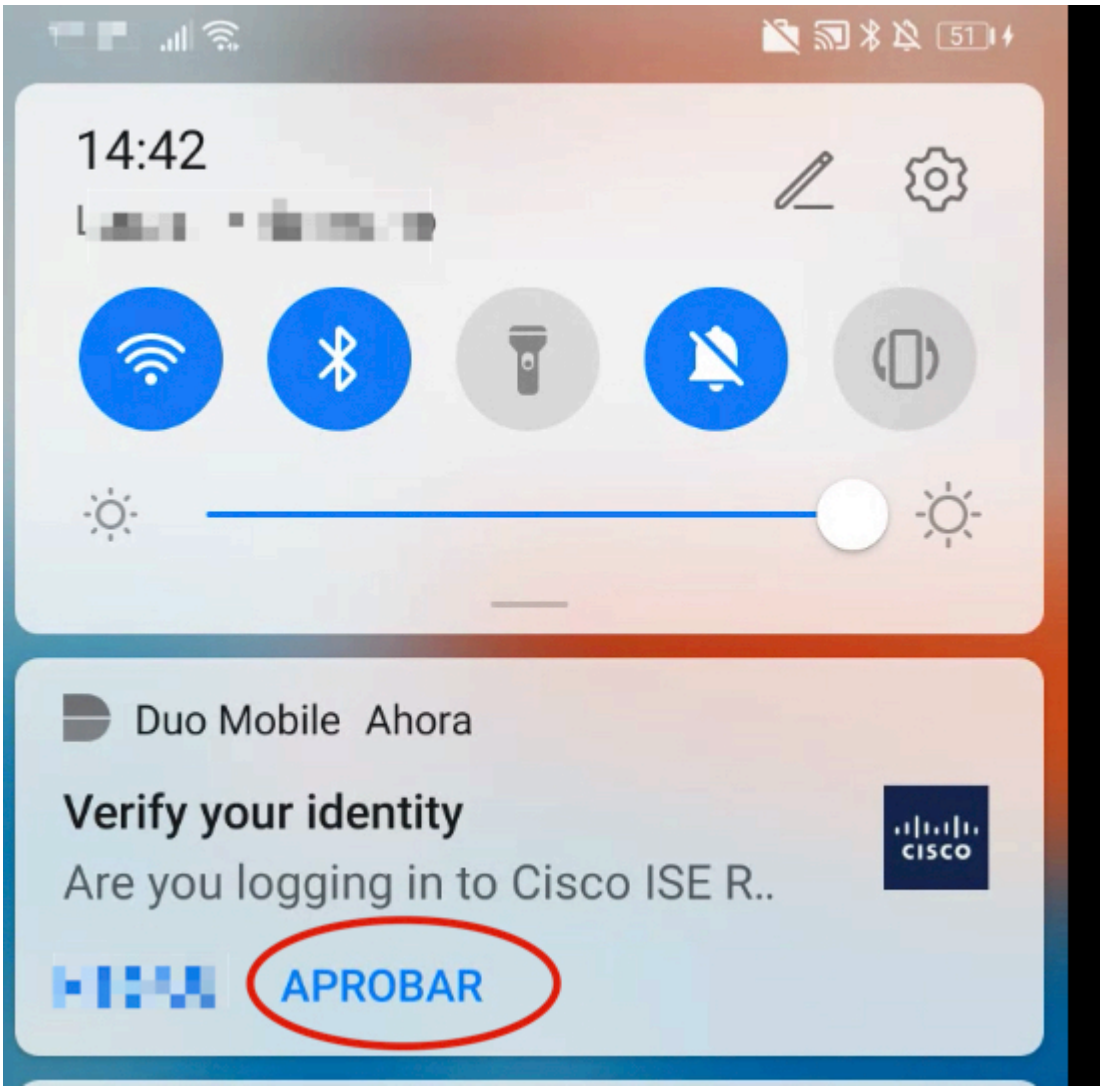
---

2. Vous recevez une notification de transmission Duo sur l'appareil Duo Mobile de l'utilisateur spécifié.

---

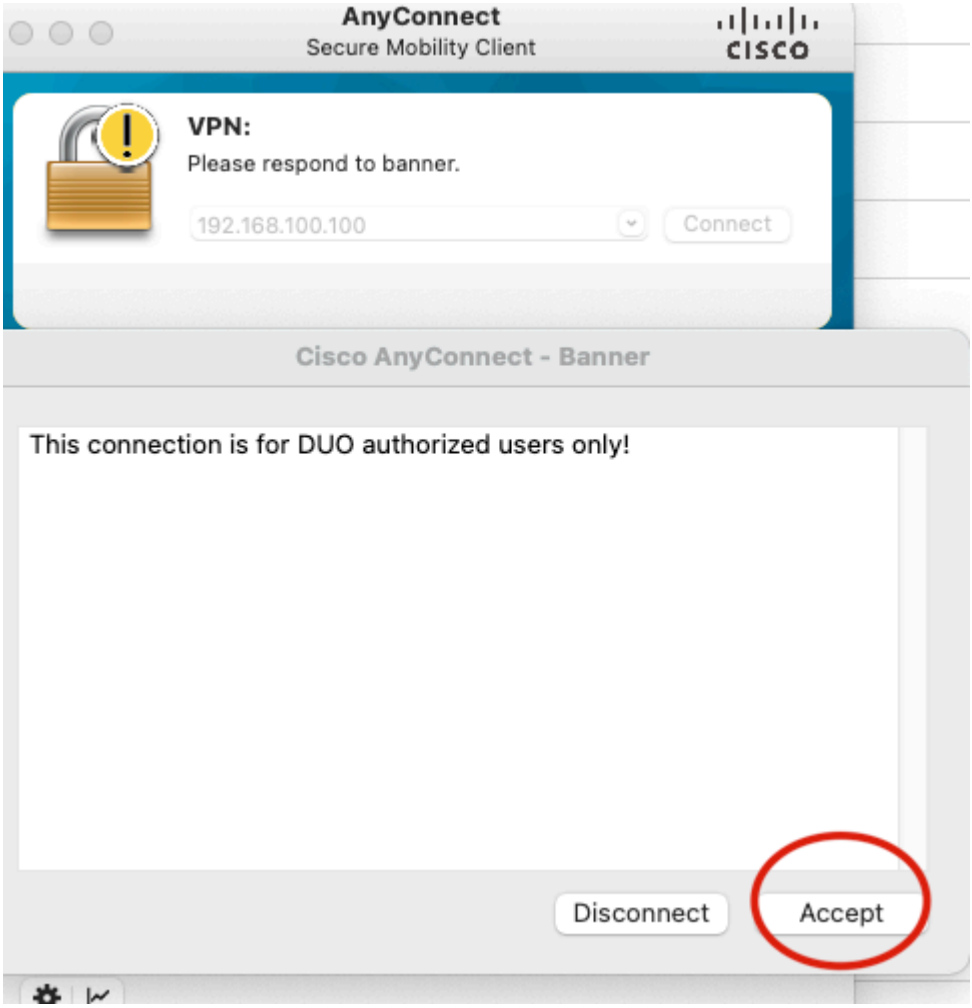
3. Ouvrez la notification de l'application mobile Duo et cliquez sur Approuver.

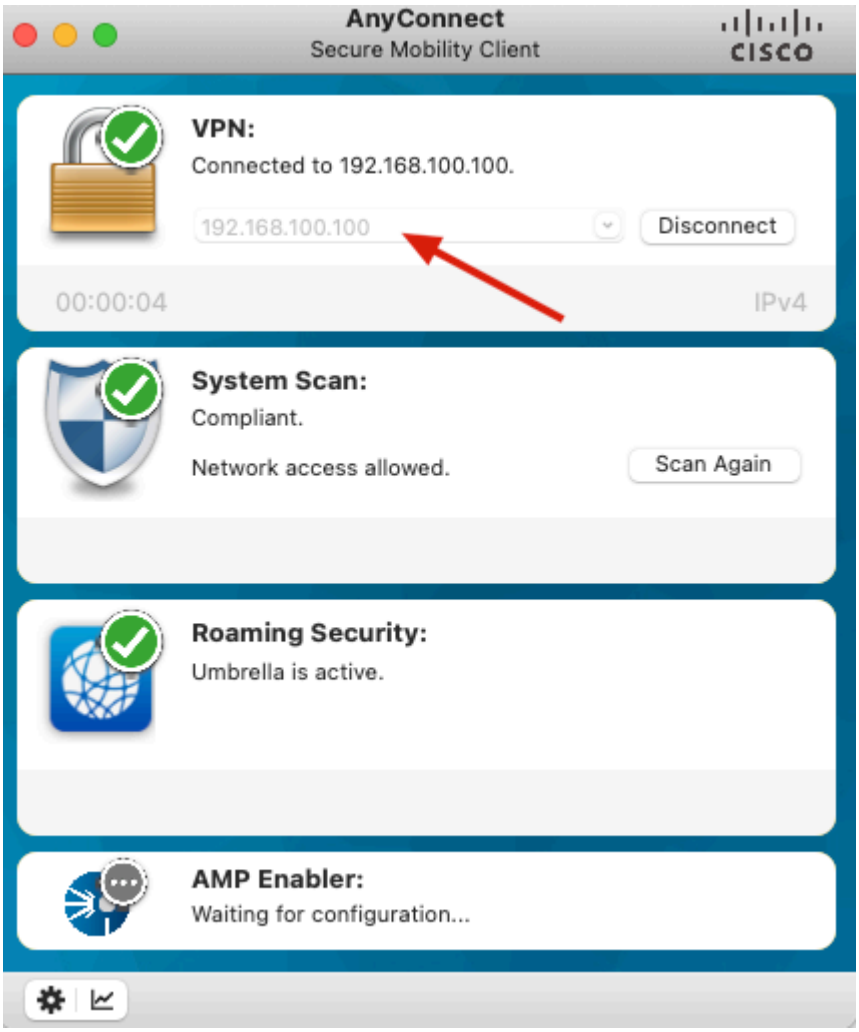

14:41
Lunes, 14 de marzo
Duo Mobile Ahora
Verify your identity
Are you logging in to Cisco ISE R..
cisco



---

4. Acceptez la bannière et la connexion est établie.


AnyConnect
Secure Mobility Client
CISCO
VPN:
Please respond to banner.
192.168.100.100
Connect
Cisco AnyConnect - Banner
This connection is for DUO authorized users only!
Disconnect
Accept



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': [redacted],
         'client': 'ad_client',
         'debug': 'True',
         'failmode': 'safe',
         'ikey': [redacted],
         '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.
```

```
[info]  There are no connectivity problems with the section.
[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]  The LDAP Client section has no connectivity issues.
[info]  ----------------------------
[info]  Testing section 'radius_server_auto' with configuration:
[info]  {'api_host': '[redacted]',
         'client': 'ad_client',
         'debug': 'True',
         'failmode': 'safe',
         'ikey': '[redacted]',
         'port': '1812',
         'radius_ip_1': '10.28.17.101',
         'radius_secret_1': '*****',
         'skey': '*****[40]'}
[info]  The RADIUS Server has no connectivity problems.
[info]  ----------------------------
[info]  SUMMARY
[info]  No issues detected
```

Problèmes courants

1. Problèmes de connectivité, adresse IP incorrecte, nom de domaine complet/nom d'hôte non résolu dans la configuration Active Directory

```
[ad_client]
host=10.28.17.106
service_account_username=Administrator
service_account_password=[redacted]
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=!
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=!
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 iKey RADIUS incorrecte

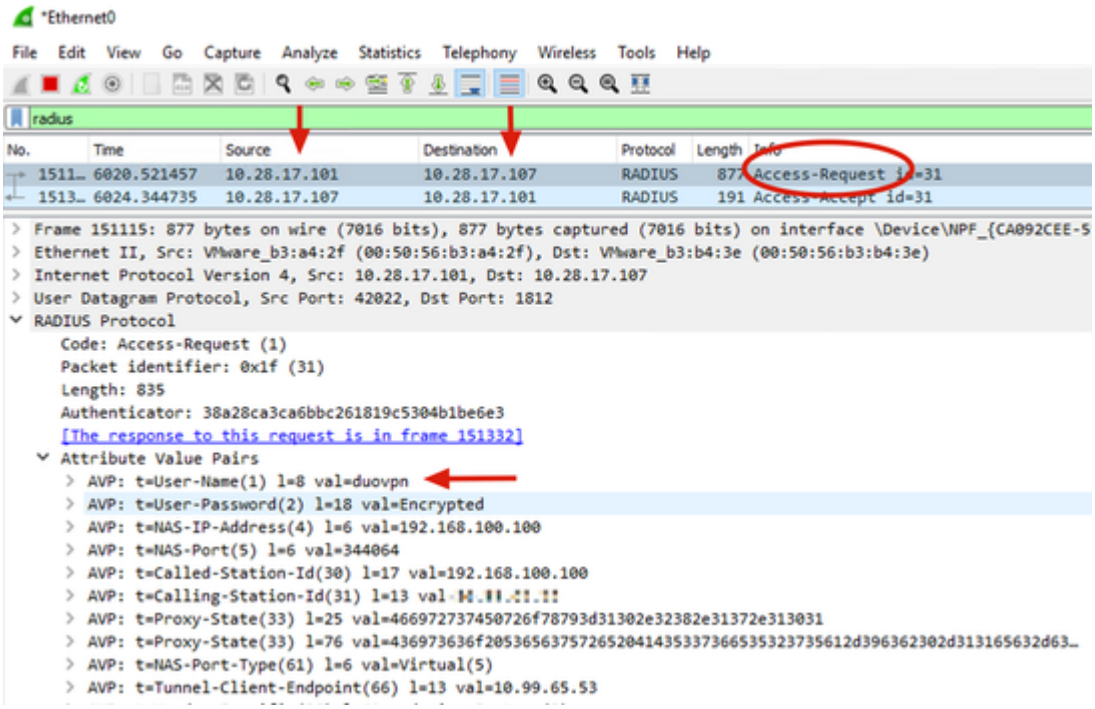
```
[radius_server_auto]
ikey=[redacted]XHRNZ6EZ1
skey=[redacted]
api_host=[redacted]ity.com
radius_ip_1=10.28.17.101
radius_secret_1=!Mexvpn!17!
failmode=safe
client=ad_client
port=1812
```

Débogages:

```
[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. Vérifier que le serveur ISE envoie des paquets de demande d'accès



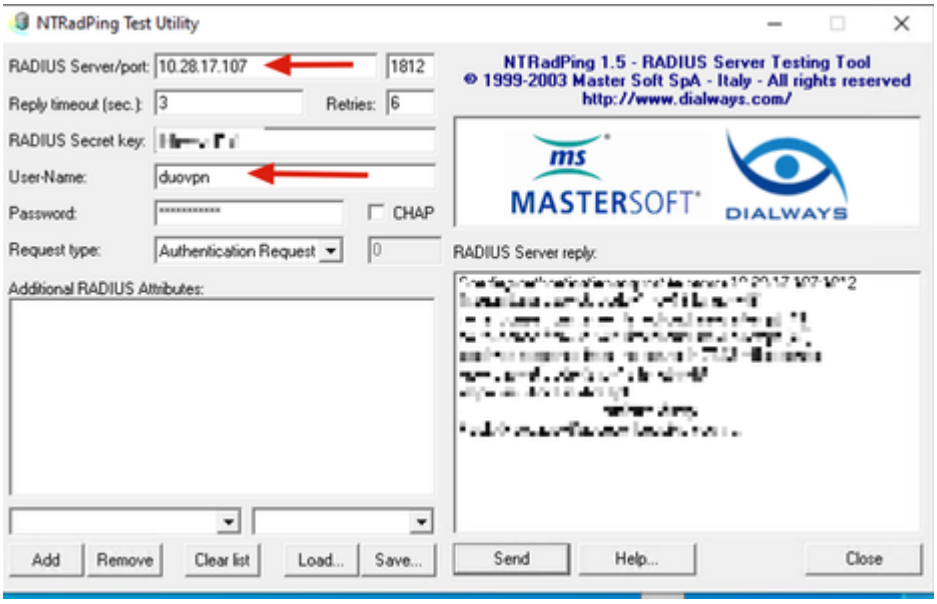
6. Utilisez l'utilitaire NTRadPing pour vérifier que le proxy d'authentification duo fonctionne

Pour confirmer que le serveur proxy d'authentification Duo fonctionne, Duo fournit l'outil NTRadPing pour simuler des paquets et des réponses de demande d'accès avec Duo.

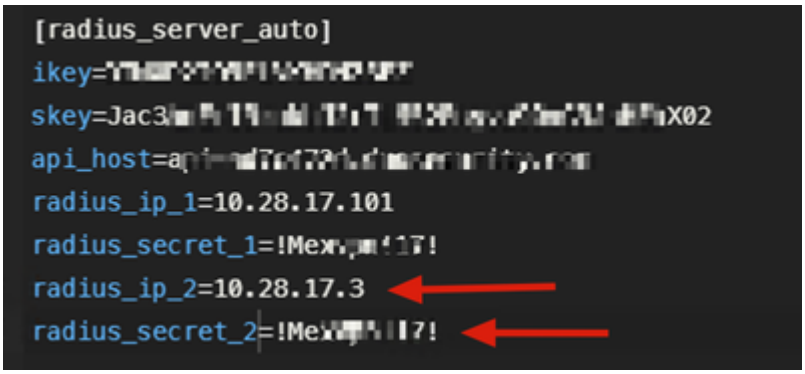
6.1 Installation de NTRadPing sur un autre PC et génération de trafic

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

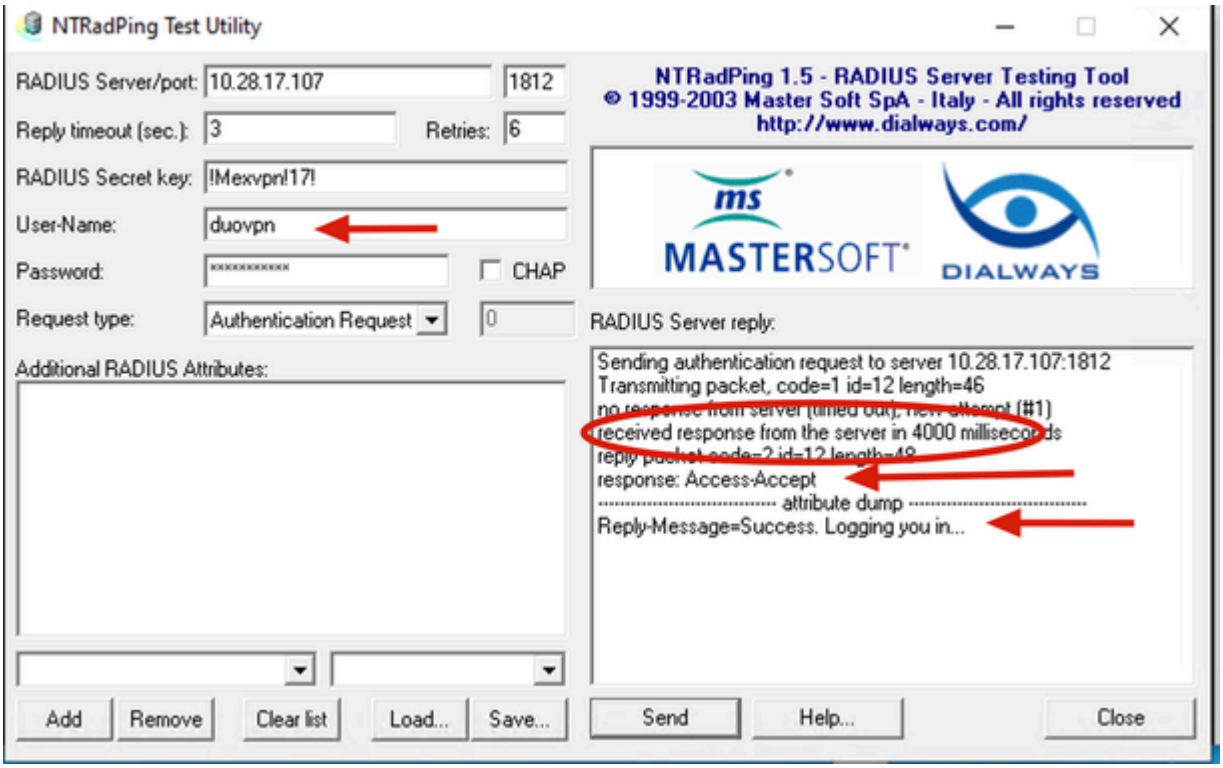
6.2 Configuration à l'aide des attributs utilisés dans la configuration ISE Radius

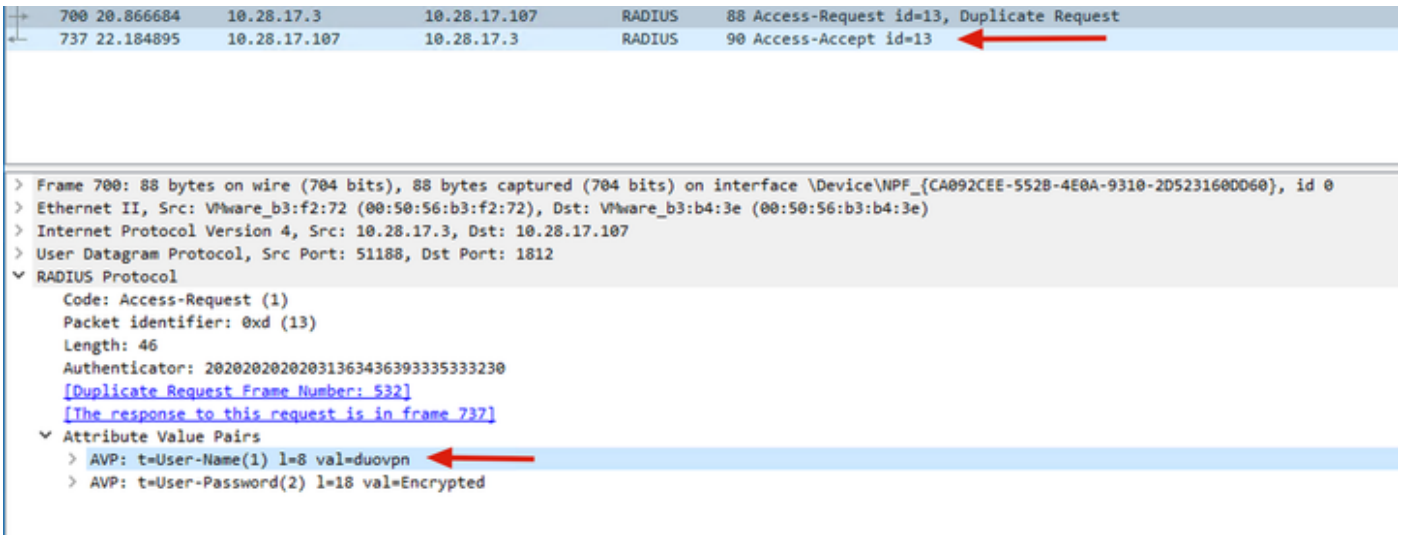


6.3 Configuration du Duo Authentication Proxy Manager comme dans l'exemple suivant :



6.4. Accédez à votre outil NTRadPing et cliquez sur Send (Envoyer). Vous recevez une notification de transmission Duo sur l'appareil mobile attribué.





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.