

# Configurer l'authentification VPN SSL via FTD, ISE, DUO et Active Directory

## Table des matières

---

[Introduction](#)

[Exigences](#)

[Composants utilisés](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configurations FTD.](#)

[Intégrer un serveur RADIUS dans Firepower Management Center \(FMC\)](#)

[Configurez le VPN distant.](#)

[Configurations ISE.](#)

[Intégrer DUO en tant que serveur Radius externe.](#)

[Intégrez le FTD en tant que périphérique d'accès réseau.](#)

[Configurations DUO.](#)

[Installation du proxy DUO.](#)

[Intégrer le proxy DUO avec ISE et le cloud DUO.](#)

[Intégrer DUO à Active Directory.](#)

[Exporter des comptes d'utilisateurs depuis Active Directory \(AD\) via le cloud DUO.](#)

[Inscrivez les utilisateurs dans le cloud Cisco DUO.](#)

[Procédure de validation de configuration.](#)

[Problèmes courants.](#)

[Scénario de travail.](#)

[Erreur11353 Plus de serveurs RADIUS externes ; impossible d'effectuer le basculement](#)

[Les sessions RADIUS n'apparaissent pas dans les journaux en direct ISE.](#)

[Dépannage supplémentaire.](#)

---

## Introduction

Ce document décrit l'intégration de SSLVPN dans Firepower Threat Defense en utilisant Cisco ISE et DUO Security pour AAA.

## Exigences

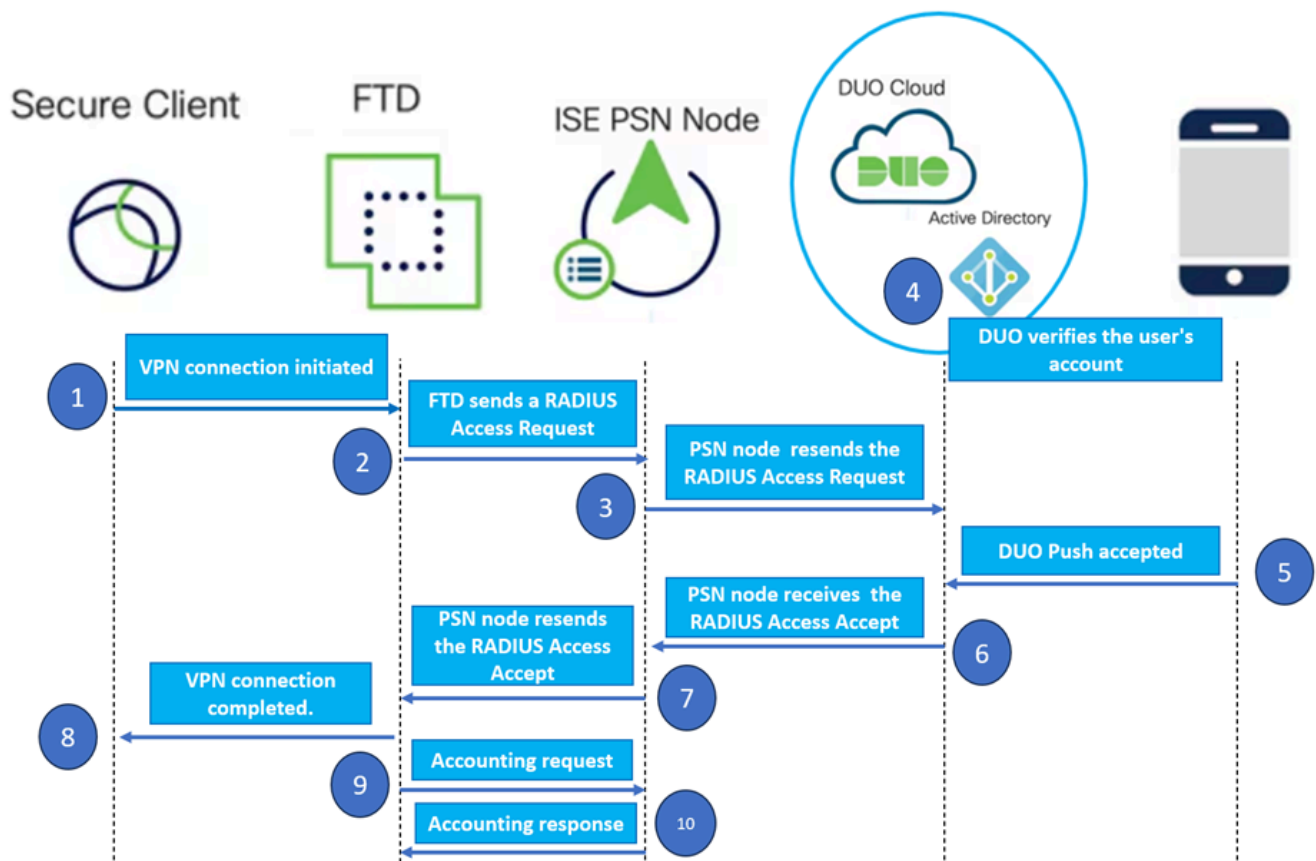
- ISE 3.0 ou supérieur.
- FMC 7.0 ou version ultérieure.
- FTD 7.0 ou supérieur.
- Proxy d'authentification DUO.
- Licences ISE Essentials
- Licence DUO Essentials.

# Composants utilisés

- ISE 3.2 Patch 3
- FMC 7.2.5
- DFT 7.2.5
- Proxy DUO 6.3.0
- Any Connect 4.10.08029

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 du réseau

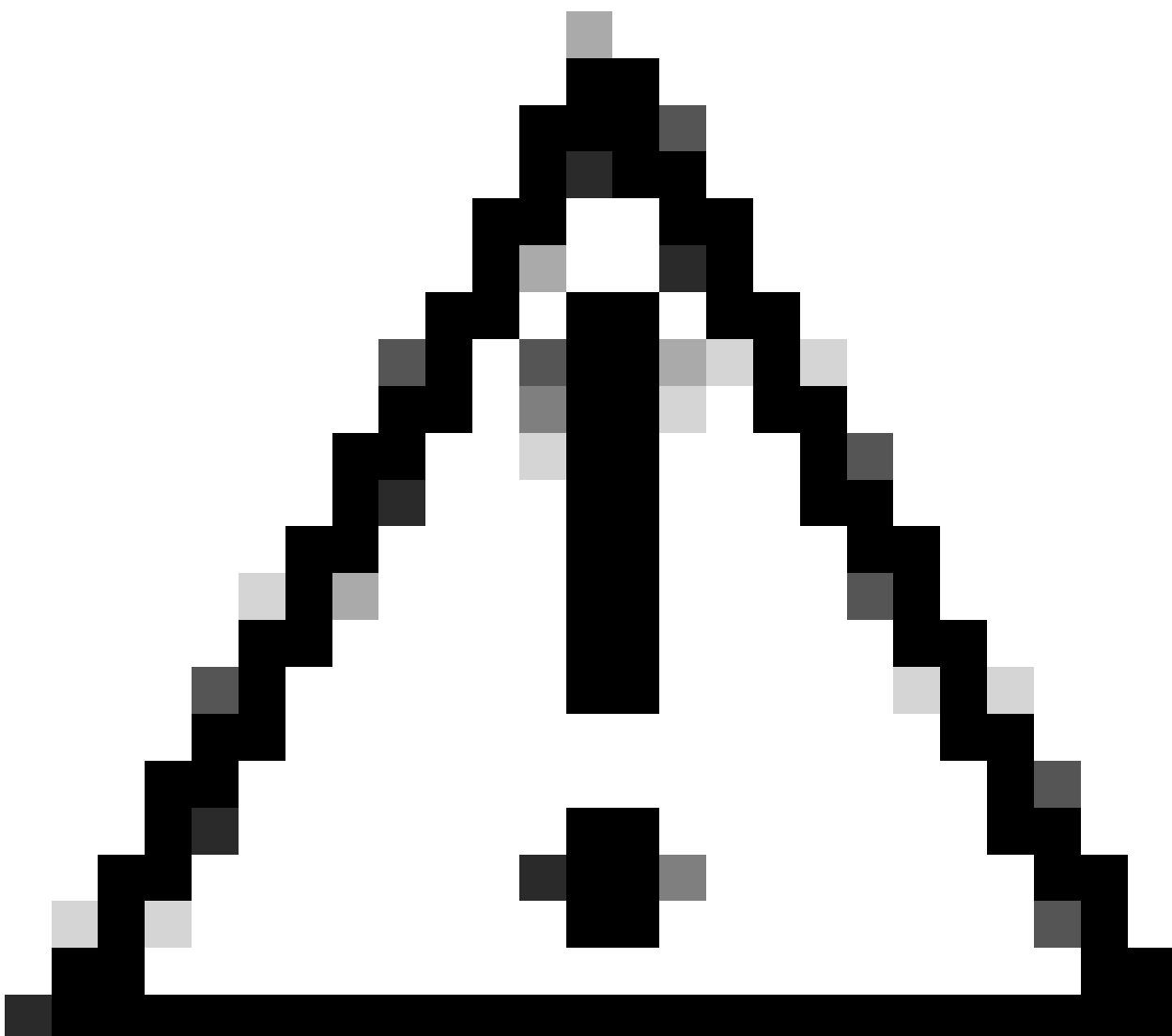


Topologie.

Dans notre solution proposée, Cisco ISE est un proxy de serveur RADIUS essentiel. Plutôt que d'évaluer directement les stratégies d'authentification ou d'autorisation, ISE est configuré pour transférer les paquets RADIUS du FTD au proxy d'authentification DUO.

Le proxy d'authentification DUO fonctionne comme un intermédiaire dédié dans ce flux d'authentification. Installé sur un serveur Windows, il comble le fossé entre Cisco ISE et le cloud DUO. La fonction principale du proxy est de transmettre les demandes d'authentification - encapsulées dans des paquets RADIUS - au cloud DUO. Le cloud DUO autorise ou refuse l'accès au réseau en fonction des configurations d'authentification à deux facteurs.

1. L'utilisateur lance le processus d'authentification VPN en saisissant son nom d'utilisateur et son mot de passe uniques.
2. Firewall Threat Defense (FTD) envoie la demande d'authentification à Cisco Identity Services Engine (ISE).
3. Le noeud de services de stratégie (PSN) transfère la demande d'authentification au serveur proxy d'authentification DUO. Par la suite, le serveur d'authentification DUO valide les informations d'identification via le service cloud DUO.
4. Le cloud DUO valide le nom d'utilisateur et le mot de passe par rapport à sa base de données synchronisée.



Attention : la synchronisation entre le cloud DUO et les organisations Active Directory doit être active pour maintenir une base de données utilisateur à jour dans le cloud DUO.

5. Une fois l'authentification réussie, le cloud DUO initie une transmission DUO Push vers l'appareil mobile enregistré des utilisateurs via une notification de transmission sécurisée et

chiffrée. L'utilisateur doit ensuite approuver la transmission DUO pour confirmer son identité et continuer.

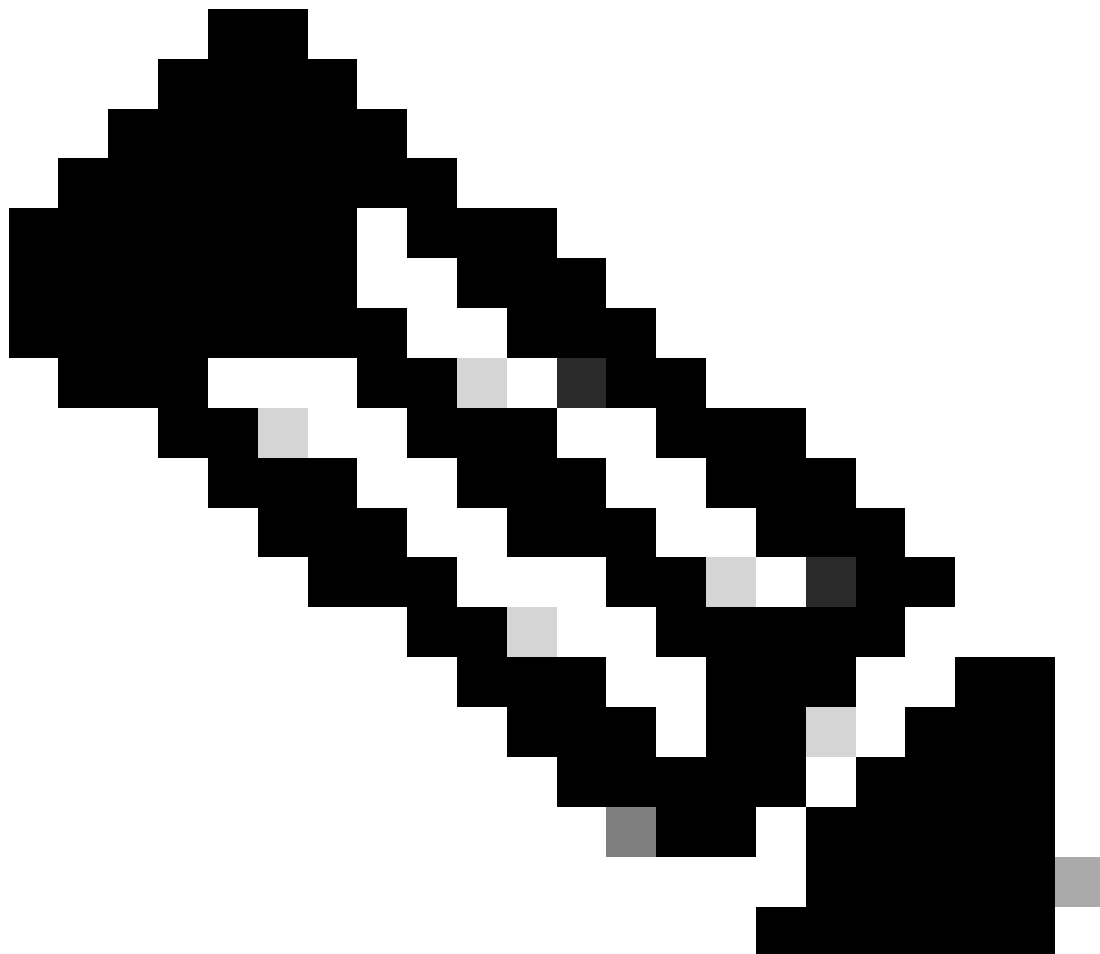
6. Une fois que l'utilisateur a approuvé la transmission DUO, le serveur proxy d'authentification DUO renvoie une confirmation au PSN pour indiquer que la demande d'authentification a été acceptée par l'utilisateur.

7. Le noeud PSN envoie la confirmation au FTD pour informer que l'utilisateur a été authentifié.

8. Le FTD reçoit la confirmation d'authentification et établit la connexion VPN au terminal avec les mesures de sécurité appropriées en place.

9. Le FTD consigne les détails de la connexion VPN réussie et transmet en toute sécurité les données de comptabilité au noeud ISE à des fins d'enregistrement et d'audit.

10. Le noeud ISE consigne les informations de comptabilité dans ses journaux de lancement, en s'assurant que tous les enregistrements sont stockés en toute sécurité et sont accessibles pour des audits ou des contrôles de conformité futurs.



Remarque :

La configuration de ce guide utilise les paramètres réseau suivants :

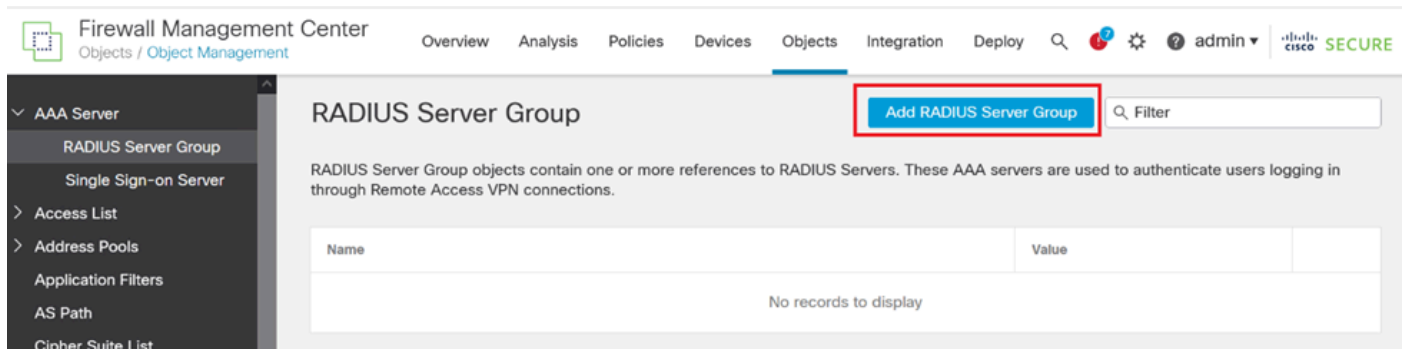
- Adresse IP du noeud PNS (Primary Network Server) : 10.4.23.21
- IP Firepower Threat Defense (FTD) pour Peer VPN : 10.4.23.53
- IP du proxy d'authentification DUO : 10.31.126.207
- Nom de domaine : testlab.local

## Configurations

### Configurations FTD.

Intégrer un serveur RADIUS dans Firepower Management Center (FMC)

1. Accédez au FMC en lançant votre navigateur Web et en saisissant l'adresse IP du FMC pour ouvrir l'interface utilisateur graphique (GUI).
2. Accédez au menu Objects, sélectionnez AAA Server, puis passez à l'option RADIUS Server Group.
3. Cliquez sur le bouton Add RADIUS Server Group pour créer un nouveau groupe pour les serveurs RADIUS.



Groupe de serveurs RADIUS.

4. Entrez un nom descriptif pour le nouveau groupe de serveurs RADIUS AAA afin de garantir une identification claire au sein de votre infrastructure réseau.
5. Ajoutez un nouveau serveur RADIUS en sélectionnant l'option appropriée dans la configuration du groupe.

*Serveur*

## RADIUS Servers (Maximum 16 servers)

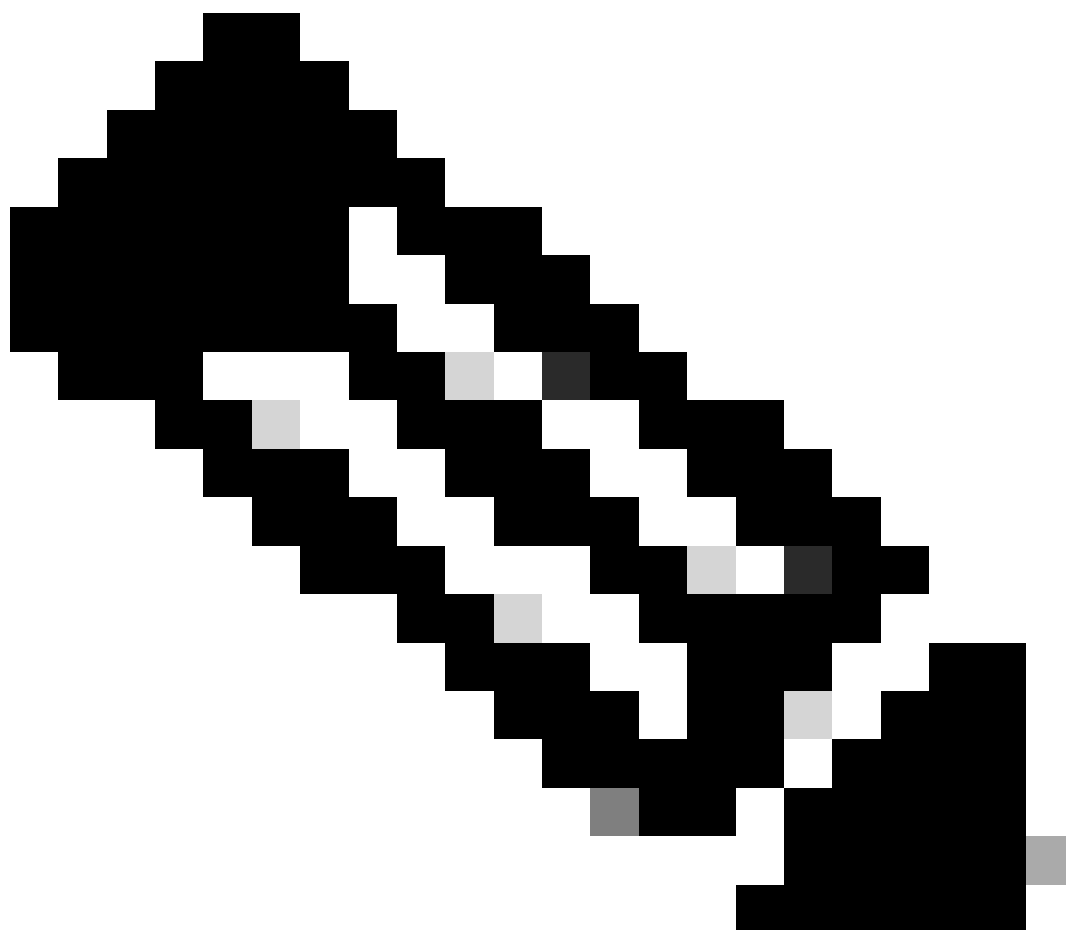


IP Address/Hostname	
No records to display	

RADIUS.

6. Spécifiez l'adresse IP des serveurs RADIUS et entrez la clé secrète partagée.

---



Remarque : il est essentiel de s'assurer que cette clé secrète est partagée en toute sécurité avec le serveur ISE pour établir une connexion RADIUS réussie.

---

## New RADIUS Server



IP Address/Hostname:\*

10.4.23.21

*Configure DNS at Threat Defense Platform Settings to resolve hostname*

Authentication Port:\* (1-65535)

1812

Key:\*

●●●●●●●●

Confirm Key:\*

●●●●●●●●

Accounting Port: (1-65535)

1813

Timeout: (1-300) Seconds

10

Connect using:

Routing  Specific Interface 

Cancel

Save

*Nouveau serveur RADIUS.*

7. Après avoir configuré les détails du serveur RADIUS, cliquez sur Save pour conserver les paramètres du groupe de serveurs RADIUS.

## Add RADIUS Server Group



Enable authorize only

Enable interim account update

Interval:\* (1-120) hours

24

Enable dynamic authorization

Port:\* (1024-65535)

1700

RADIUS Servers (Maximum 16 servers)



IP Address/Hostname

10.4.23.21



Cancel

Save

Détails du groupe de serveurs.

8. Pour finaliser et implémenter la configuration du serveur AAA sur votre réseau, accédez au menu Déployer, puis sélectionnez Tout déployer pour appliquer les paramètres.

The screenshot shows the Firewall Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'Integration', and 'Deploy'. The 'Deploy' menu is highlighted with a red box. Below the navigation bar, the left sidebar shows a tree view with 'AAA Server' expanded, and 'RADIUS Server Group' selected. The main content area displays the configuration for the 'RADIUS Server Group' object, including a table with one entry: 'FTD\_01' with a status of 'Ready for Deployment'. The 'Deploy All' button is highlighted with a red box.

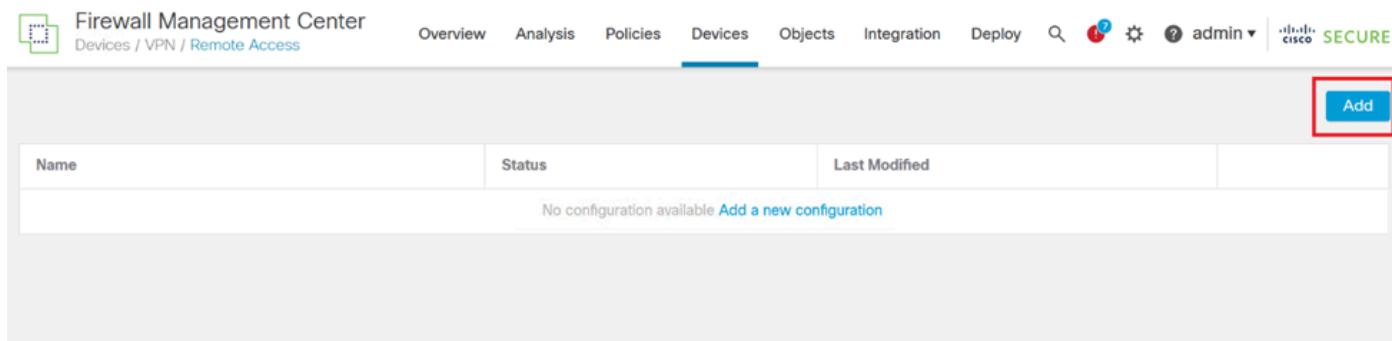
Déploiement du serveur AAA.

Configurez le VPN distant.



1. Accédez à Devices > VPN > Remote Access dans l'interface graphique FMC pour commencer le processus de configuration VPN.

2. Cliquez sur le bouton Add pour créer un nouveau profil de connexion VPN.

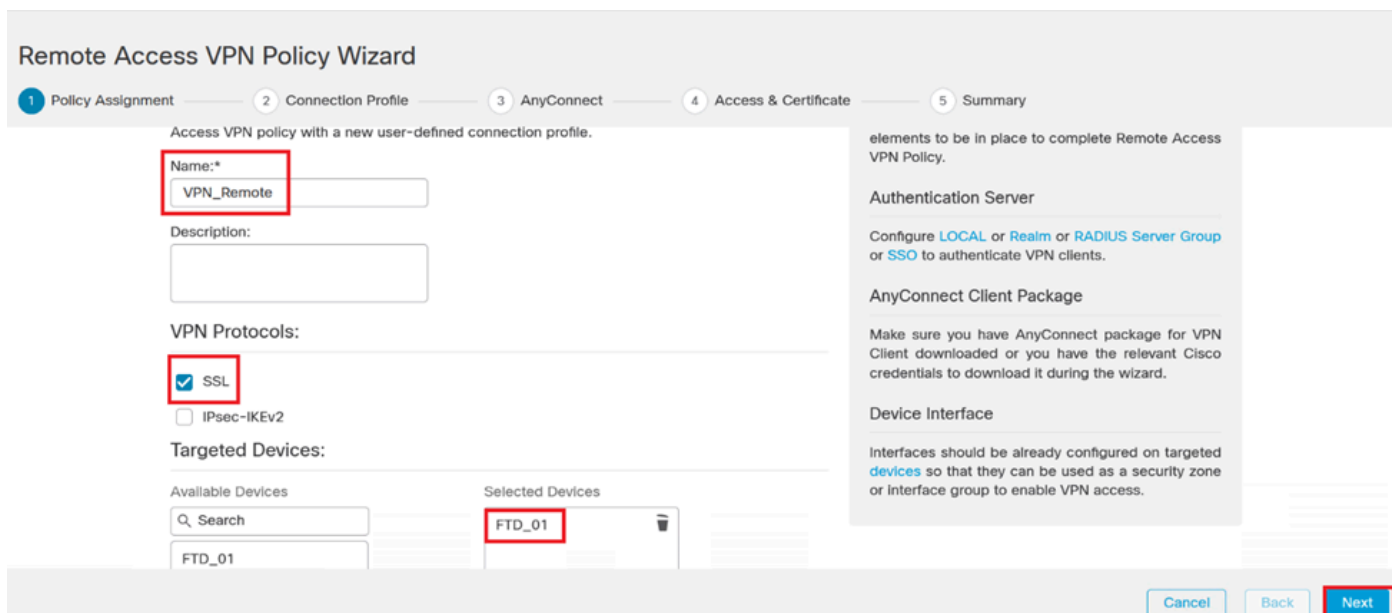


Profil de connexion VPN.

3. Entrez un nom unique et descriptif pour le VPN afin de l'identifier dans vos paramètres réseau.

4. Choisissez l'option SSL pour garantir une connexion sécurisée à l'aide du protocole VPN SSL.

5. Dans la liste des périphériques, sélectionnez le périphérique FTD spécifique.



Paramètres VPN.

6. Configurez la méthode AAA pour utiliser le noeud PSN dans les paramètres d'authentification.

## Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

### Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: **AAA Only** ▼

Authentication Server:\* **ISE** ▼ +

(LOCAL or Realm or RADIUS)

Fallback to LOCAL Authentication

Authorization Server: **Use same authentication server** ▼ +

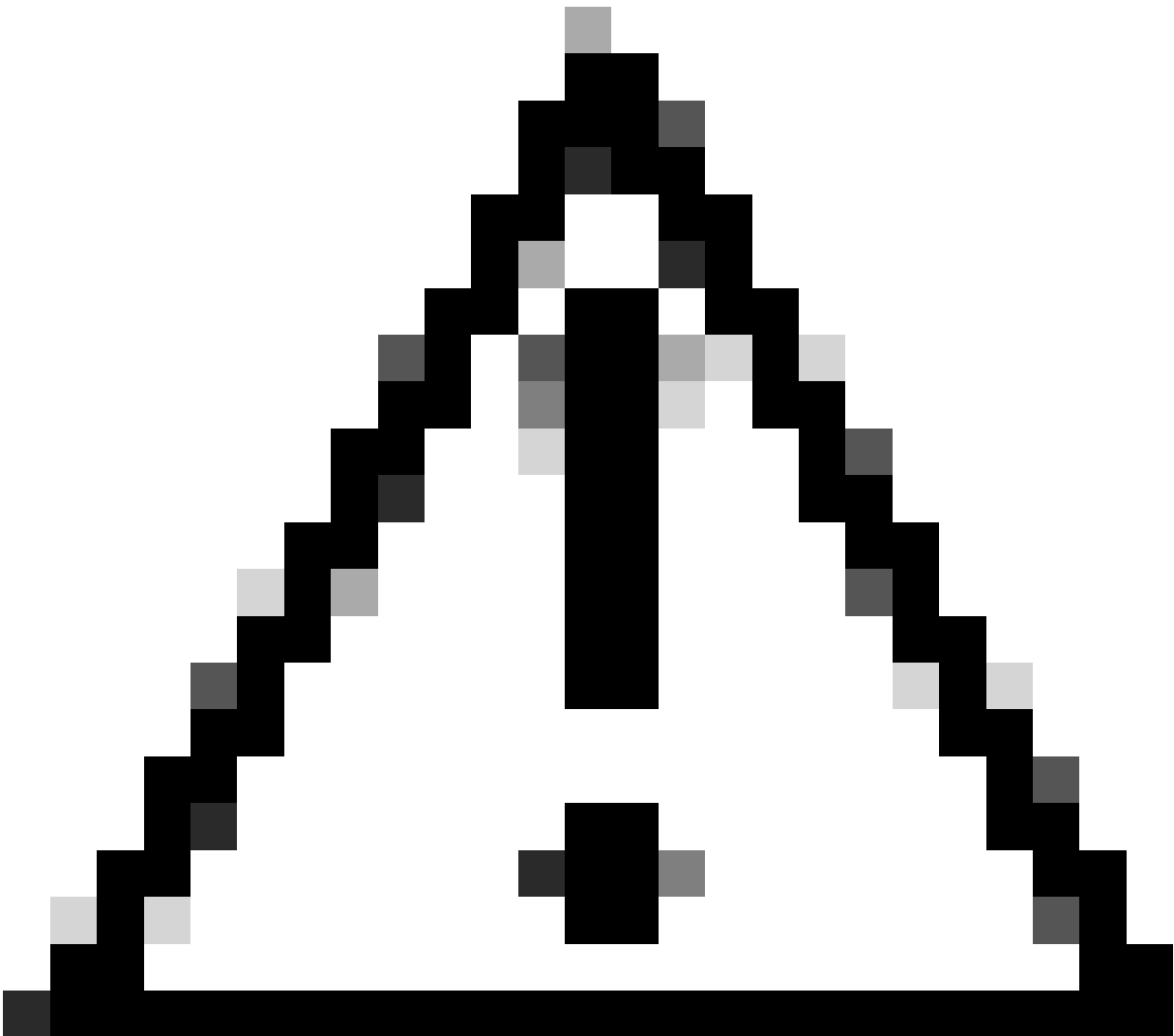
(realm or RADIUS)

Accounting Server: **ISE** ▼ +

(RADIUS)

*Profil de connexion.*

7. Configurez l'attribution dynamique d'adresses IP pour le VPN.



---

Attention : par exemple, le pool VPN DHCP a été sélectionné.

---

#### Client Address Assignment:

---

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only) ⓘ

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools:  

IPv6 Address Pools:  

*Pool d'adresses IP.*

#### 8. Créez une nouvelle stratégie de groupe.

#### Group Policy:

---

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:\*  

[Edit Group Policy](#)

*Stratégie de groupe.*

#### 9. Dans les paramètres Stratégie de groupe, vérifiez que le protocole SSL est sélectionné.

## Add Group Policy



Name:\*

VPN\_Remote\_Policy

Description:

General

AnyConnect

Advanced

### VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

VPN Tunnel Protocol:

Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

SSL

IPsec-IKEv2

Cancel

Save

Protocoles VPN.

10. Créez un nouveau pool VPN ou sélectionnez-en un existant pour définir la plage d'adresses IP disponibles pour les clients VPN.

## Add Group Policy



Name:\*

VPN\_Remote\_Policy

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

IP Address Pools:



Name

IP Address Range

Cancel

Save

*VPN de pool.*

11. Spécifiez les détails du serveur DNS pour la connexion VPN.

## Add Group Policy



Name:\*

VPN\_Remote\_Policy

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

Primary DNS Server:

+

Secondary DNS Server:

+

Primary WINS Server:

+

Secondary WINS Server:

+

DHCP Network Scope:

+

Only network object with ipv4 address is allowed (Ex: 10.72.3.5)

Default Domain:

Cancel

Save

Paramètres DNS.



Avertissement : notez que des fonctionnalités supplémentaires telles que les options Bannière, Fractionnement de tunnel, AnyConnect et Avancé sont considérées comme facultatives pour cette configuration.

---

12. Après avoir configuré les détails nécessaires, cliquez sur Next pour passer à la phase suivante de la configuration.

## Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Use AAA Server (Realm or RADIUS only) ●

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools:

IPv6 Address Pools:

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:\*

[Edit Group Policy](#)

Cancel

Back

Next

Stratégie de groupe.

13. Sélectionnez le package AnyConnect approprié pour les utilisateurs VPN. Si le package requis n'est pas répertorié, vous avez la possibilité d'ajouter le package nécessaire à ce stade.

## Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from [Cisco Software Download Center](#).

Select at least one AnyConnect Client image

[Show Re-order buttons](#)

<input type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input type="checkbox"/>	anyconnect-win-4.10.08029-we...	anyconnect-win-4.10.08029-webdeploy-k9...	Windows

Cancel

Back

Next

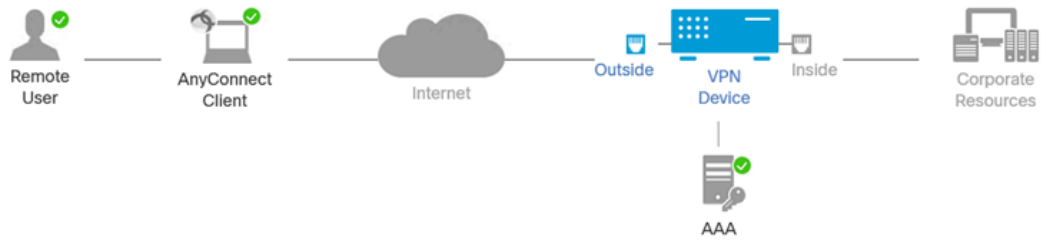
Installation du package.

14. Choisissez l'interface réseau sur le périphérique FTD dans lequel vous souhaitez activer la fonctionnalité VPN à distance.



## Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary



### Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

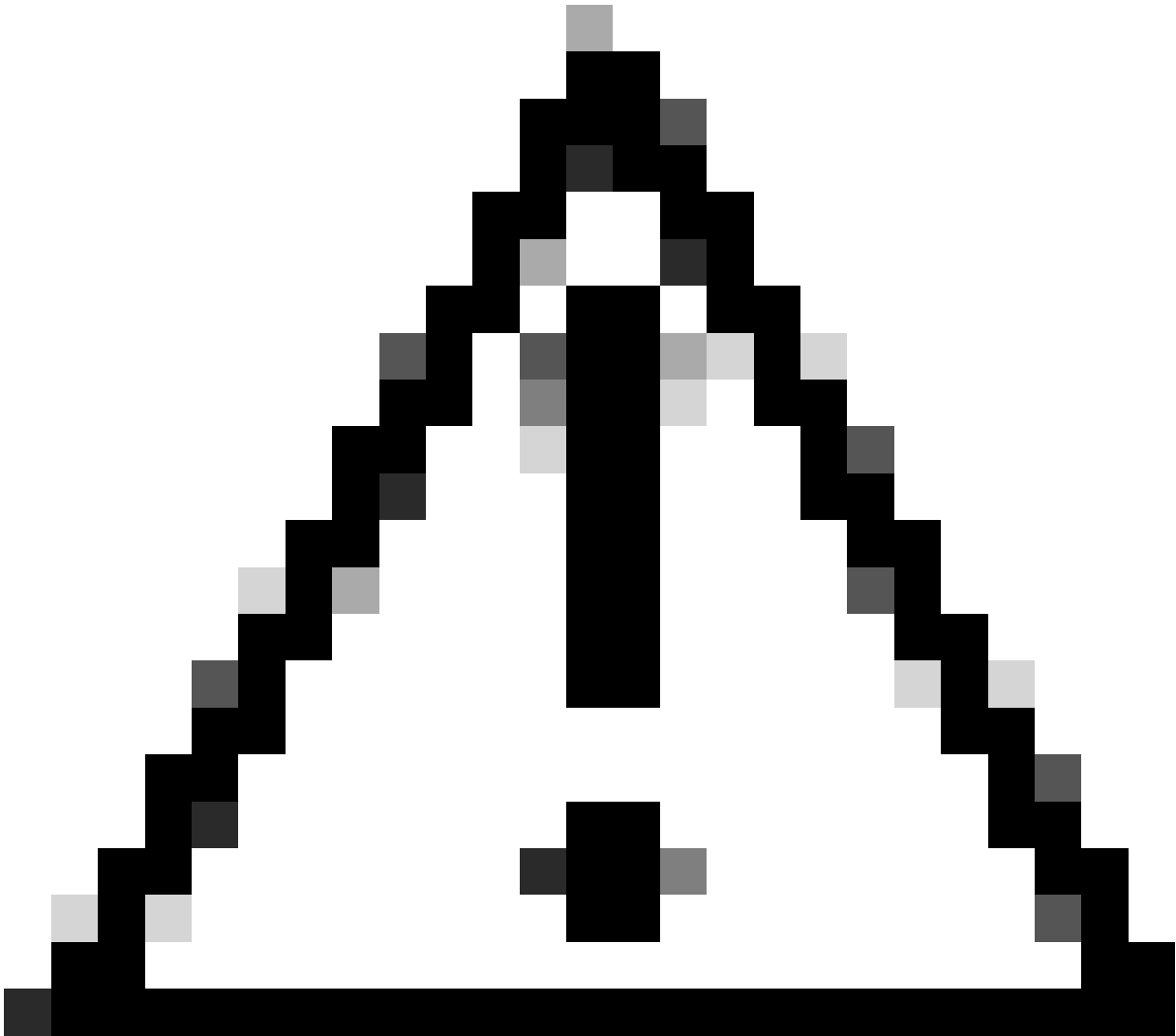
Interface group/Security Zone:\*  +

Enable DTLS on member interfaces

**▲ All the devices must have interfaces as part of the Interface Group/Security Zone selected.**

*Interface VPN*

15. Établissez un processus d'inscription de certificat en sélectionnant l'une des méthodes disponibles pour créer et installer le certificat sur le pare-feu, ce qui est crucial pour les connexions VPN sécurisées.



Attention : par exemple, un certificat auto-signé a été sélectionné dans ce guide.

---

## Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:\*

*Certificat de périphérique.*

## Add Cert Enrollment



Name\*

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

SCEP

Enrollment URL:\*

Self Signed Certificate

Challenge Password:

EST

Confirm Password:

SCEP

Manual

Retry Period:

PKCS12 File

Retry Count:

10

(Range 0-100)

Fingerprint:

Cancel

Save

*Inscription au certificat.*

16. Cliquez sur Next une fois que l'inscription de certificat est configurée.

## Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

will access for VPN connections.

Interface group/Security Zone:\*  +

Enable DTLS on member interfaces

▲ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

### Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:\*  +

### Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

Récapitulatif des accès et des services

17. Vérifiez le résumé de toutes vos configurations pour vous assurer qu'elles sont correctes et reflètent la configuration prévue.

## Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Firepower Management Center will configure an RA VPN Policy with the following settings

Name:	VPN_Remote
Device Targets:	FTD_01
Connection Profile:	VPN_Remote
Connection Alias:	VPN_Remote
AAA:	
Authentication Method:	AAA Only
Authentication Server:	ISE (RADIUS)
Authorization Server:	ISE (RADIUS)
Accounting Server:	ISE
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	Pool_VPN
Address Pools (IPv6):	-
Group Policy:	VPN_Remote_Policy
AnyConnect Images:	anyconnect-win-4.10.08029-webdeploy-k9.pkg
Interface Objects:	Outside
Device Certificates:	Cert_Enrollment

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- Access Control Policy Update
 

An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption
 

If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.
- DNS Configuration
 

To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.
- Port Configuration
 

SSL will be enabled on port 443. Please ensure that these ports are not used in [NAT Policy](#) or other services before deploying the configuration.
- ▲ Network Interface Configuration
 

Make sure to add interface from targeted

Résumé des paramètres VPN.

18. Pour appliquer et activer la configuration d'accès à distance VPN, accédez à Déployer > Tout déployer et exécutez le déploiement sur le périphérique FTD sélectionné.

Firewall Management Center  
Devices / VPN / Edit Connection Profile

Overview Analysis Policies Devices Objects Integration **Deploy** admin

VPN\_Remote  
Enter Description

Connection Profile Access Interfaces Advanced

Name	AAA
DefaultWEBVPGGroup	Authentication: No Authorization: No Accounting: No
VPN_Remote	Authentication: ISE Authorization: ISE Accounting: ISE

Advanced Deploy **Deploy All**

FTD\_01 Ready for Deployment (1)

1 device is available for deployment

Déploiement des paramètres VPN.

## Configurations ISE.

Intégrer DUO en tant que serveur Radius externe.

1. Accédez à Administration > Network Resources > External RADIUS Servers dans l'interface d'administration de Cisco ISE.
2. Cliquez sur le bouton Add pour configurer un nouveau serveur RADIUS externe.

Cisco ISE Administration · Network Resources

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

External RADIUS Servers

Selected 0 Total 0

Edit **Add** Duplicate Delete

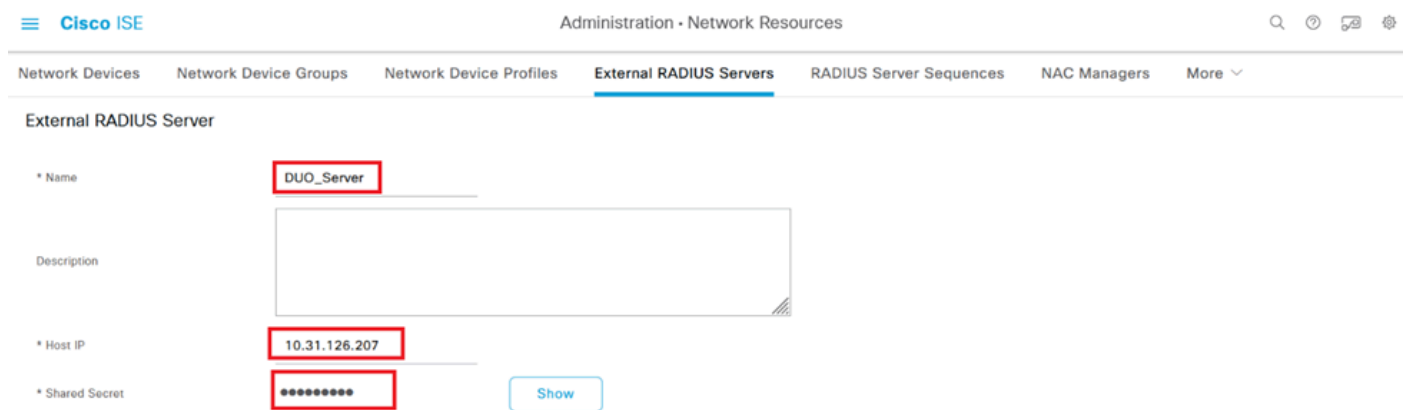
Name	Description
No data available	

Serveurs Radius externes

3. Entrez un nom pour le serveur proxy DUO.
4. Entrez l'adresse IP correcte pour le serveur DUO proxy afin d'assurer une communication correcte entre l'ISE et le serveur DUO.
5. Définissez la clé secrète partagée.

**Remarque** : cette clé secrète partagée doit être configurée dans le serveur proxy DUO pour établir une connexion RADIUS.

6. Une fois que tous les détails sont correctement entrés, cliquez sur **Submit** pour enregistrer la nouvelle configuration du serveur proxy DUO.



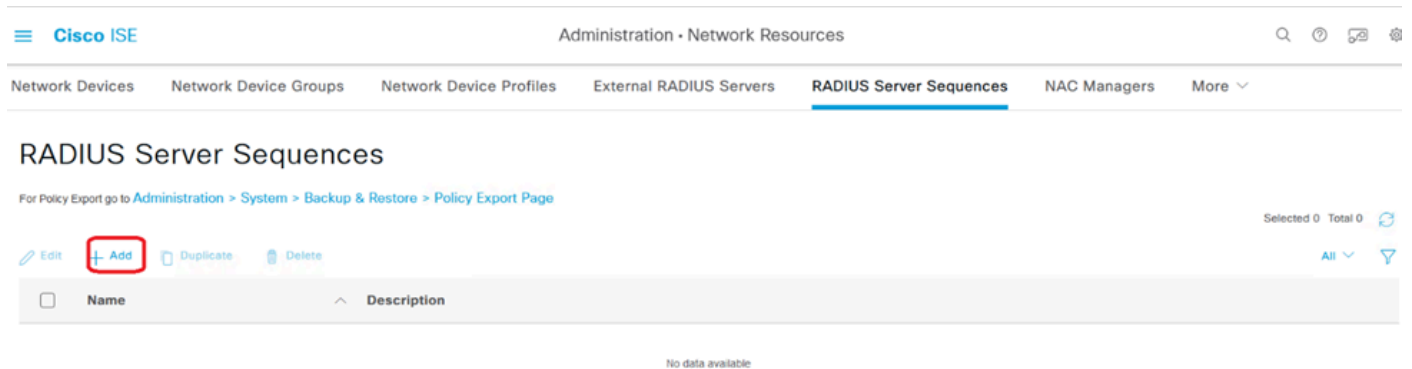
The screenshot shows the Cisco ISE Administration interface for configuring an External RADIUS Server. The breadcrumb trail is "Administration > Network Resources > External RADIUS Servers". The "External RADIUS Server" configuration form has the following fields:

- \* Name:
- Description:
- \* Host IP:
- \* Shared Secret:

Serveurs RADIUS externes

7. Passez à Administration > Séquences du serveur RADIUS.

8. Cliquez sur Add pour créer une nouvelle séquence de serveur RADIUS.

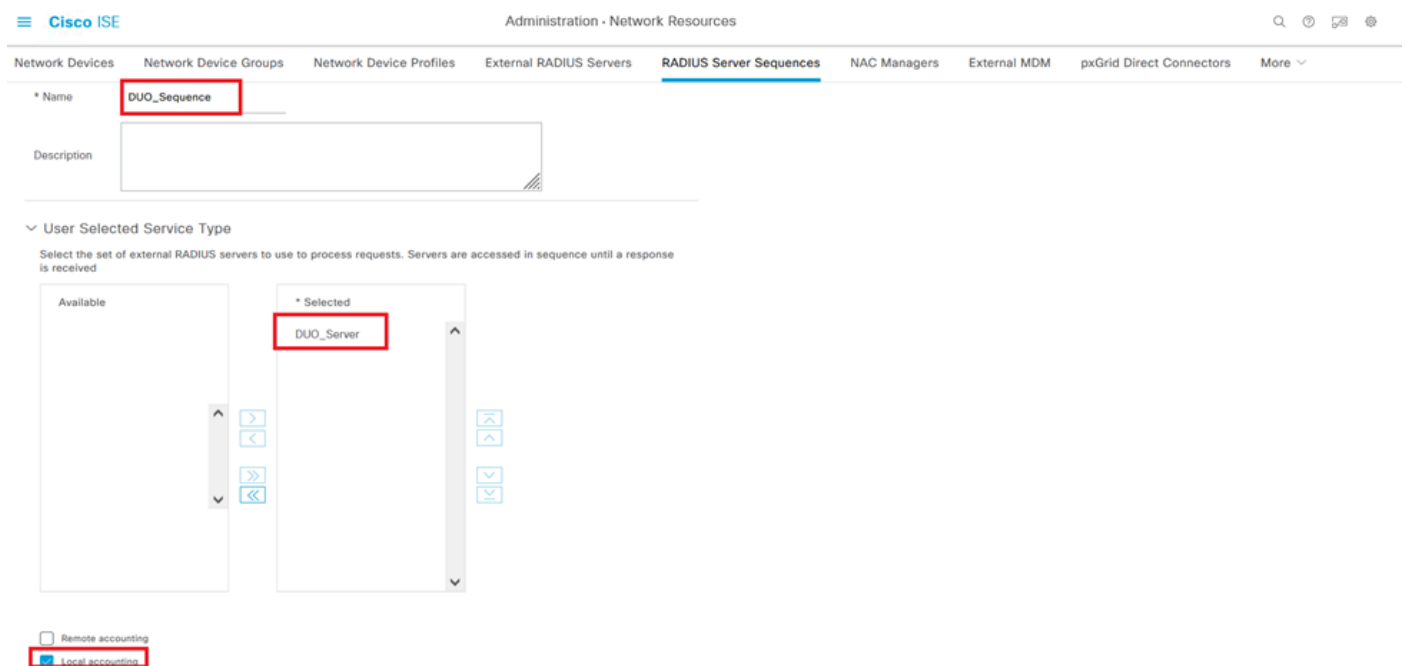


Séquences de serveur RADIUS

9. Attribuez un nom distinct à la séquence de serveurs RADIUS pour faciliter son identification.

10. Localisez le serveur DUO RADIUS précédemment configuré, appelé DUO\_Server dans ce guide, et déplacez-le vers la liste sélectionnée à droite pour l'inclure dans la séquence.

11. Cliquez sur Submit pour finaliser et enregistrer la configuration de la séquence de serveurs RADIUS.



Configuration des séquences du serveur Radius.

Intégrez le FTD en tant que périphérique d'accès réseau.

1. Accédez à la section Administration de votre interface système et, à partir de là, sélectionnez Network Resources pour accéder à la zone de configuration des périphériques réseau.

2. Une fois dans la section Ressources réseau, localisez et cliquez sur le bouton Ajouter pour lancer le processus d'ajout d'un nouveau périphérique d'accès réseau.

Network Devices

Network Device Groups   Network Device Profiles   External RADIUS Servers   RADIUS Server Sequences   NAC Managers   More ▾

Network Devices

Default Device

Device Security Settings

Selected 0 Total 0

✎ Edit **+ Add** 📄 Duplicate 📄 Import 📄 Export ▾ 📄 Generate PAC 🗑 Delete ▾ All ▾ 🔍

<input type="checkbox"/>	Name	IP/Mask	Profile Name	Location	Type	Description
No data available						

Périphériques d'accès réseau.

3. Dans les champs fournis, saisissez le nom du périphérique d'accès réseau pour identifier le périphérique sur votre réseau.
4. Spécifiez l'adresse IP du périphérique FTD (Firepower Threat Defense).
5. Saisissez la clé précédemment définie lors de la configuration de FMC (Firepower Management Center). Cette clé est essentielle pour sécuriser la communication entre les périphériques.
6. Terminez le traitement en cliquant sur le bouton Lancer.

[Network Devices List](#) > **FTD**

## Network Devices

Name

FTD

Description

IP Address ▾

\* IP :

10.4.23.53

/

32



Ajout de FTD comme NAD.



## RADIUS Authentication Settings

### RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret

••••••••

Show

Use Second Shared Secret ⓘ

Second Shared Secret

Show

CoA Port **1700**

Set To Default

Paramètres RADIUS

## Configurations DUO.

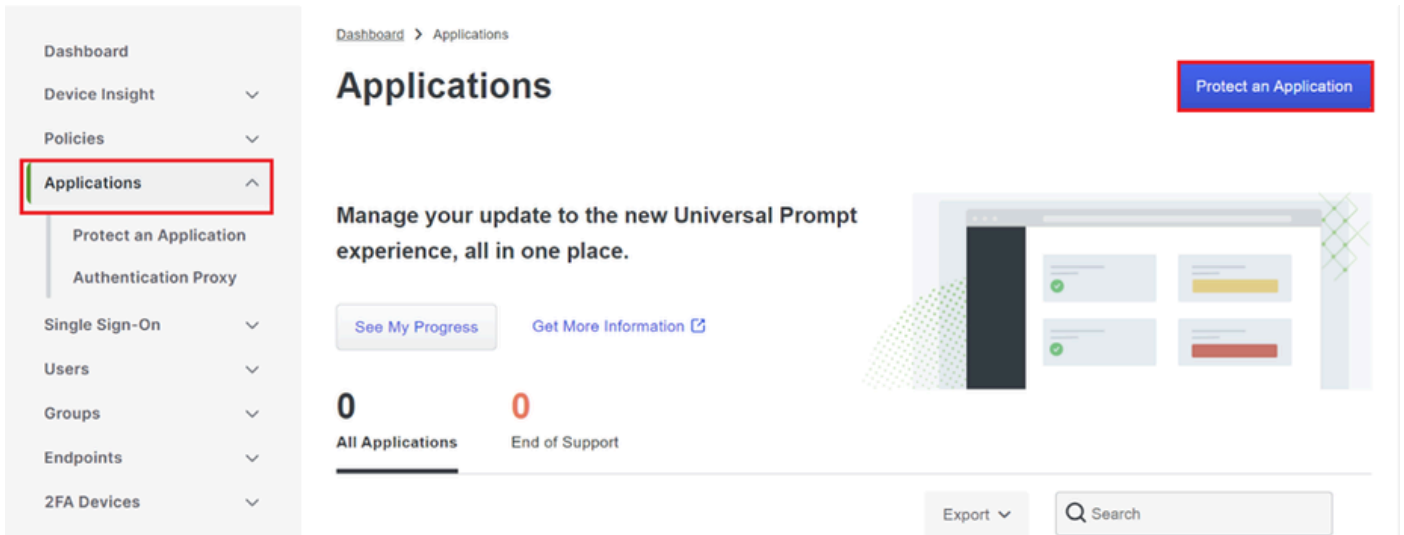
Installation du proxy DUO.

Accédez au Guide d'installation et de téléchargement du proxy DUO en cliquant sur le lien suivant :

<https://duo.com/docs/authproxy-reference>

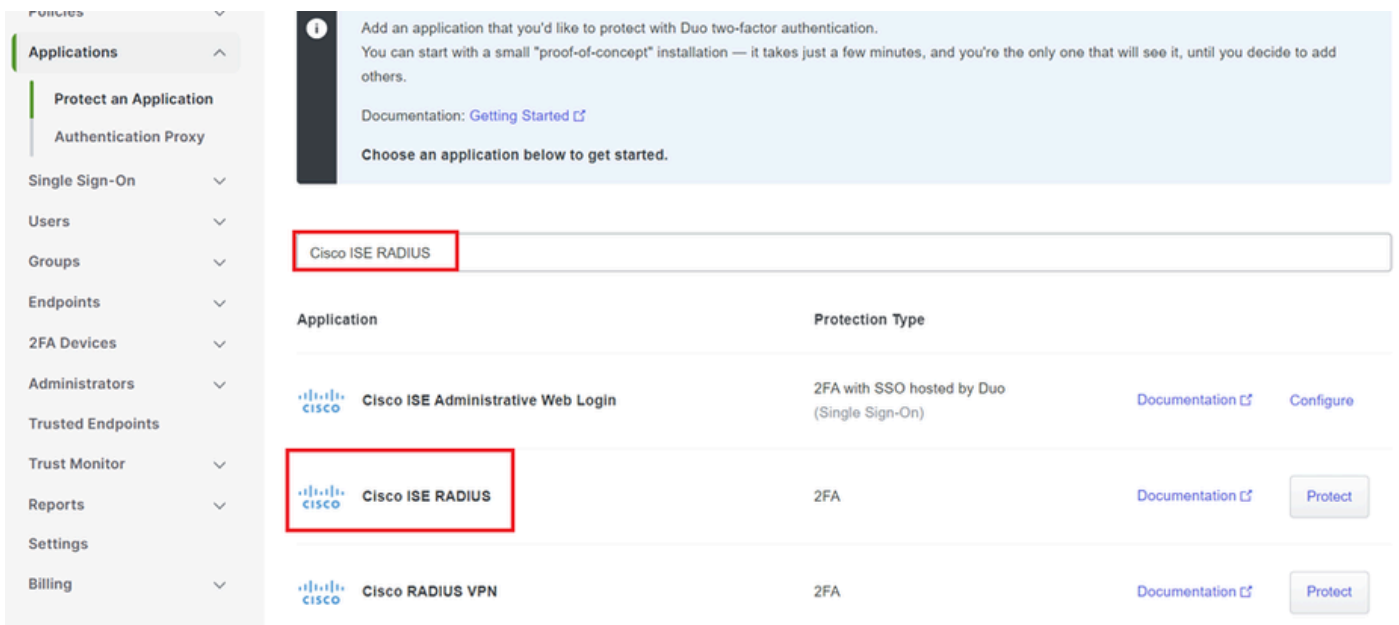
Intégrer le proxy DUO avec ISE et le cloud DUO.

1. Connectez-vous au site Web de DUO Security à l'adresse <https://duo.com/> à l'aide de vos informations d'identification.
2. Accédez à la section Applications et sélectionnez Protéger une application pour continuer.



Applications DUO

3. Recherchez l'option "Cisco ISE RADIUS" dans la liste et cliquez sur Protect pour l'ajouter à vos applications.



Option RADIUS ISE

4. Une fois l'ajout réussi, vous allez voir les détails de l'application DUO. Faites défiler vers le bas et cliquez sur Save.

5. Copiez la clé d'intégration, la clé secrète et le nom d'hôte de l'API fournis ; ces éléments sont essentiels pour les étapes à venir.

✓ Application modified successfully.

Dashboard > Applications > Cisco ISE RADIUS

# Cisco ISE RADIUS

Authentication Log | Remove Application

Follow the [Cisco ISE RADIUS instructions](#).

## Details

Reset Secret Key

Integration key  Copy

Secret key  Copy

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

API hostname  Copy

Détails du serveur ISE

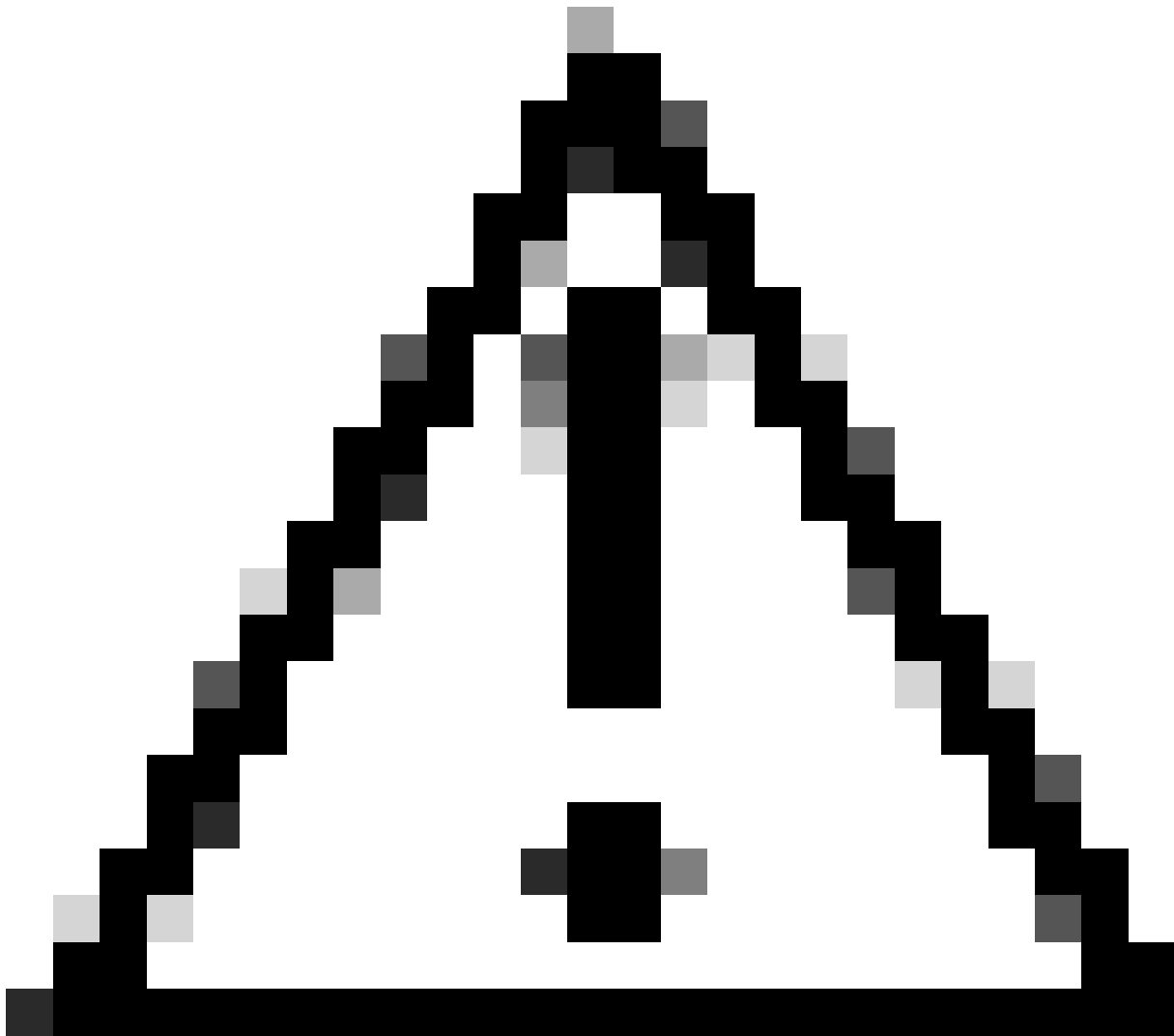
6. Lancez le DUO Proxy Manager sur votre système pour poursuivre la configuration.



DUO Proxy Manager

7. (Facultatif) Si votre serveur proxy DUO nécessite une configuration de proxy pour se connecter au cloud DUO, saisissez les paramètres suivants :

```
[main]
http_proxy_host=<Proxy IP Address or FQDN >
http_proxy_port=<port>
```

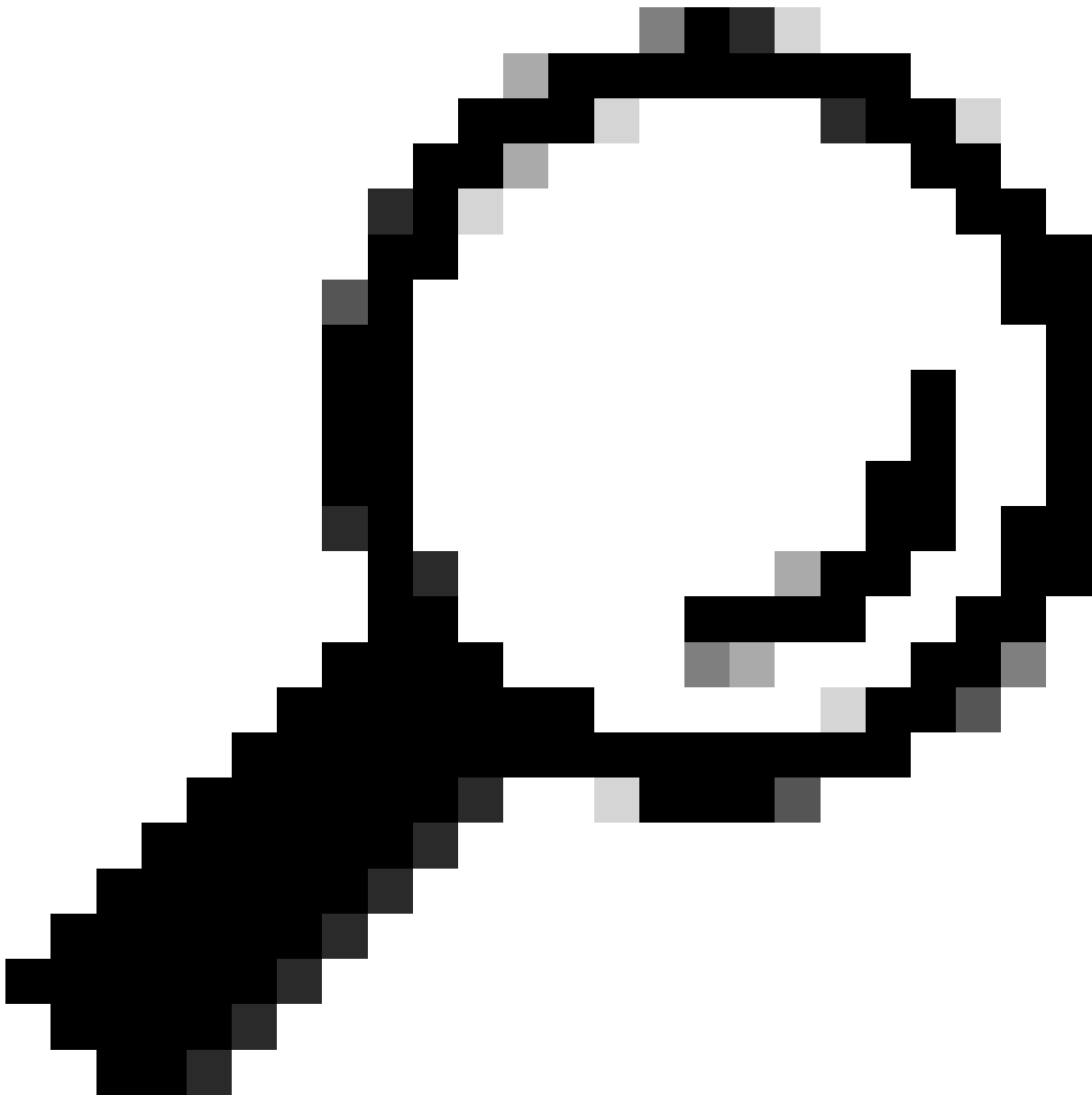


**Attention :** assurez-vous de remplacer et par vos informations de proxy réelles.

---

8. À présent, utilisez les informations que vous avez copiées précédemment pour terminer la configuration de l'intégration.

```
[radius_server_auto]
ikey=<integration key>
skey=<secret key>
api_host=<API hostname>
radius_ip_1=<ISE IP address>
radius_secret_1=<secret key configured in the external RADIUS server section>
failmode=safe
port=1812
client=ad_client
```



**Conseil :** la ligne `client=ad_client` indique que le proxy DUO s'authentifie à l'aide d'un compte Active Directory. Vérifiez que ces informations sont correctes pour terminer la synchronisation avec Active Directory.

---

Intégrer DUO à Active Directory.

1. Intégrez le proxy d'authentification DUO à votre Active Directory.

```
[ad_client]
host=<AD IP Address>
service_account_username=<service_account_username>
service_account_password=<service_account_password>
search_dn=DC=<domain>,DC=<TLD>
```

2. Rejoignez votre Active Directory avec les services cloud DUO. Connectez-vous à <https://duo.com/>.

3. Accédez à "Users" et sélectionnez "Directory Sync" pour gérer les paramètres de synchronisation.

Dashboard > Users

## Users

Directory Sync | Import Users | Bulk Enroll Users | Add User

Need to activate a replacement phone? [Learn more about Reactivating Duo Mobile](#).

0 Total Users | 0 Not Enrolled | 0 Inactive Users | 0 Trash | 0 Bypass Users | 0 Locked Out

Select (0) | ... | Export | Search

No users shown based on your search.

*Synchronisation du répertoire*

4. Cliquez sur "Ajouter une nouvelle synchronisation" et choisissez "Active Directory" dans les options fournies.

Dashboard > Users > Directory Sync

## Directory Sync

Add New Sync

Directory Syncs | Connections

You don't have any directories yet.

*Ajouter une nouvelle synchronisation*

5. Sélectionnez Ajouter une nouvelle connexion et cliquez sur Continuer.

Dashboard > Users > Directory\_Sync > New Active Directory Sync

## New Active Directory Sync

**Connection**  
Set up a new connection using a new Authentication Proxy.

Reuse existing connection  
 **Add new connection**  
 You will be redirected to a new page

[Continue](#)

---

**Directory Sync Setup**

Waiting for connection to directory

Sync setup is disabled until a connection to the directory has been established.

**Directory Sync Setup**

- Connect to AD
- Add groups
- Review synced attributes

[Complete Setup](#)

Ajout d'Active Directory

6. Copiez la clé d'intégration, la clé secrète et le nom d'hôte de l'API générés.

### Authentication Proxy

[Delete Connection](#) [No Changes](#)

**Configuration metadata**

- To set up this directory, you need to install the Duo Authentication Proxy software on a machine that Duo can connect to and that can connect to your LDAP server. [View instructions](#)
- Configure your Authentication Proxy. Update the `ikey`, `skey`, and `api_host` entries in the `[cloud]` section of your configuration, or [download a pre-configured file](#).

**Integration key**  [Copy](#)

**Secret key**  [Copy](#)

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

[Reset Secret Key](#)

**API hostname**  [Copy](#)

- If you are using NTLM or plain authentication, update the `[cloud]` section of your configuration with the username and password for the LDAP account that has read access for your LDAP directory.

**Status**

Not connected

- Add Authentication Proxy
- Configure Directory

**Connected Directory Syncs**

**User Syncs**  
[AD Sync](#)

Détails du proxy d'authentification

7. Revenez à la configuration du proxy d'authentification DUO et configurez la section `[cloud]` avec les nouveaux paramètres que vous avez obtenus, ainsi que les informations d'identification du compte de service pour un administrateur Active Directory :

```
[cloud]
ikey=<integration key>
skey=<secret key>
api_host=<API hostname>
service_account_username=<your domain>\<service_account_username>
service_account_password=<service_account_password>
```

8. Validez votre configuration en sélectionnant l'option "valider" pour vous assurer que tous les paramètres sont corrects.

```
1 [main]
2 http_proxy_host=cx[redacted]
3 http_proxy_port=3128
4
5 [radius_server_auto]
6 ikey=DIX[redacted]
7 skey=[redacted]uXWYwLM
8 api_host=a[redacted].duosecurity.com
9 radius_ip_1=10.4.23.21
10 radius_secret_1=po[redacted]
11 failmode=safe
12 port=1812
13 client=ad_client
14
15 [ad_client]
16 host=10.4.23.42
17 service_account_username=administrator
18 service_account_password=[redacted]
```

Configuration du proxy DUO.

9. Après la validation, enregistrez votre configuration et redémarrez le service proxy d'authentification DUO pour appliquer les modifications.

```
Running The Duo Authentication Proxy Connectivity Tool. This may take
several minutes...
[info] Testing section 'main' with configuration:
[info] {'http_proxy_host': 'cx[redacted]',
'http_proxy_port': '3128'}
[info] There are no configuration problems
[info]
[info] Testing section 'radius_server_auto' with configuration:
[info] {'api_host': '[redacted].duosecurity.com',
'client': 'ad_client',
'failmode': 'safe',
'http_proxy_host': '[redacted]',
'http_proxy_port': '3128',
'key': 'DIX[redacted]'}
```

Redémarrez l'option Service.

10. Dans le tableau de bord d'administration DUO, entrez l'adresse IP de votre serveur Active Directory avec le DN de base pour la synchronisation des utilisateurs.



---

## Directory Configuration

### Domain controller(s)

Hostname or IP address (1) \*

Port (1) \*

[+ Add Domain controller](#)

The port is typically 389 for cleartext LDAP or STARTTLS, and 636 for LDAPS.

---

### Base DN \*

Enter the full distinguished name (DN) of the directory location to search for users and groups. We recommend setting this to the directory root (example: DC=domain,DC=local). If specifying the DN of an OU or container, ensure it is **above both the users and groups to sync**.

---

*Paramètres du répertoire.*

11. Sélectionnez l'option Plain pour configurer le système pour l'authentification non-NTLMv2.

---

## Authentication type



**Integrated**

Performs Windows authentication from a domain-joined system.



**NTLMv2**

Performs Windows NTLMv2 authentication.



**Plain**

Performs username-password authentication.

*Type d'authentification.*

12. Enregistrez vos nouveaux paramètres pour vous assurer que la configuration est mise à jour.

 Delete Connection

Save

## Status

Not connected

Add Authentication Proxy



Configure Directory

---

## Connected Directory Syncs

### User Syncs

[AD Sync](#)

*Enregistrer, option*

13. Utilisez la fonction « test de connexion » pour vérifier que le service cloud DUO peut

communiquer avec votre Active Directory.

## Authentication Proxy

1. To set up this directory, you need to install the Duo Authentication Proxy software on a machine that Duo can connect to and that can connect to your LDAP server. [View instructions](#)
2. Configure your Authentication Proxy. Update the `ik`, `skey`, and `api_host` entries in the `[cloud]` section of your configuration, or [download a pre-configured file](#).

**Integration key**  [Copy](#)

**Secret key**  [Copy](#)

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

[Reset Secret Key](#)

**API hostname**  [Copy](#)

3. If you are using NTLM or plain authentication, update the `[cloud]` section of your configuration with the username and password for the LDAP account that has read access for your LDAP directory.

```
service_account_username=myusername  
service_account_password=mypassword
```

4. Restart your Authentication Proxy.

5. [Test Connection](#).

*Tester l'option de connexion*

14. Vérifiez que l'état d'Active Directory s'affiche sous la forme "Connecté", ce qui indique une intégration réussie.

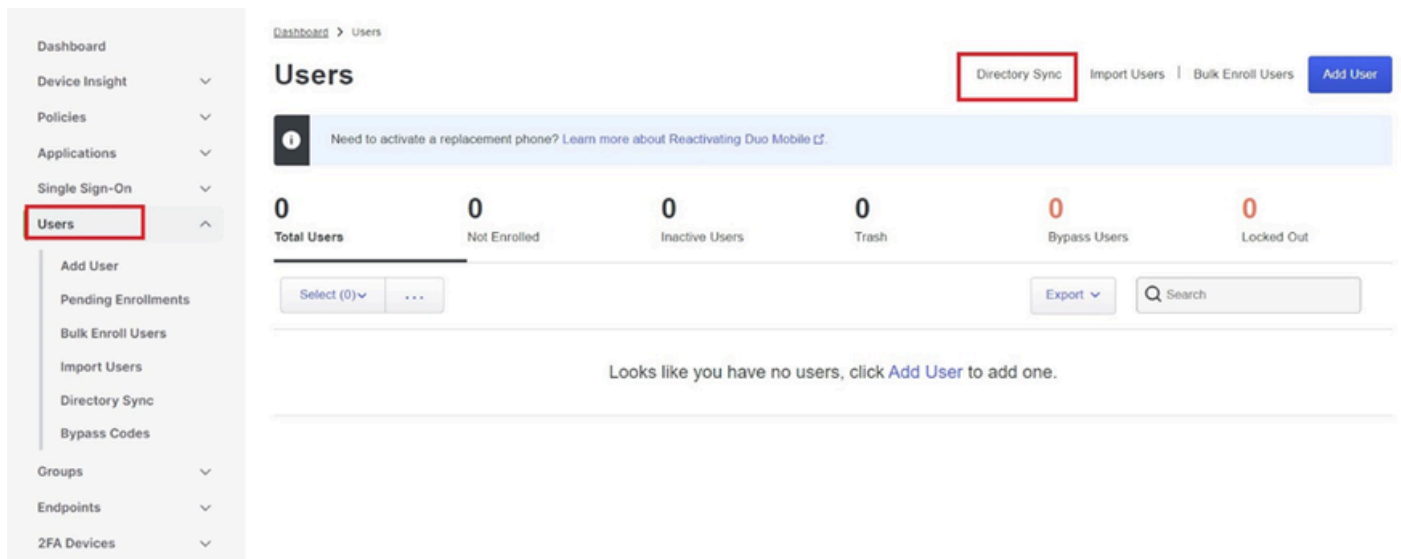
## Status

Connected

*État réussi.*

Exporter des comptes d'utilisateurs depuis Active Directory (AD) via le cloud DUO.

1. Accédez à Users > Directory Sync dans le panneau d'administration Duo pour localiser les paramètres liés à la synchronisation d'annuaire avec Active Directory.

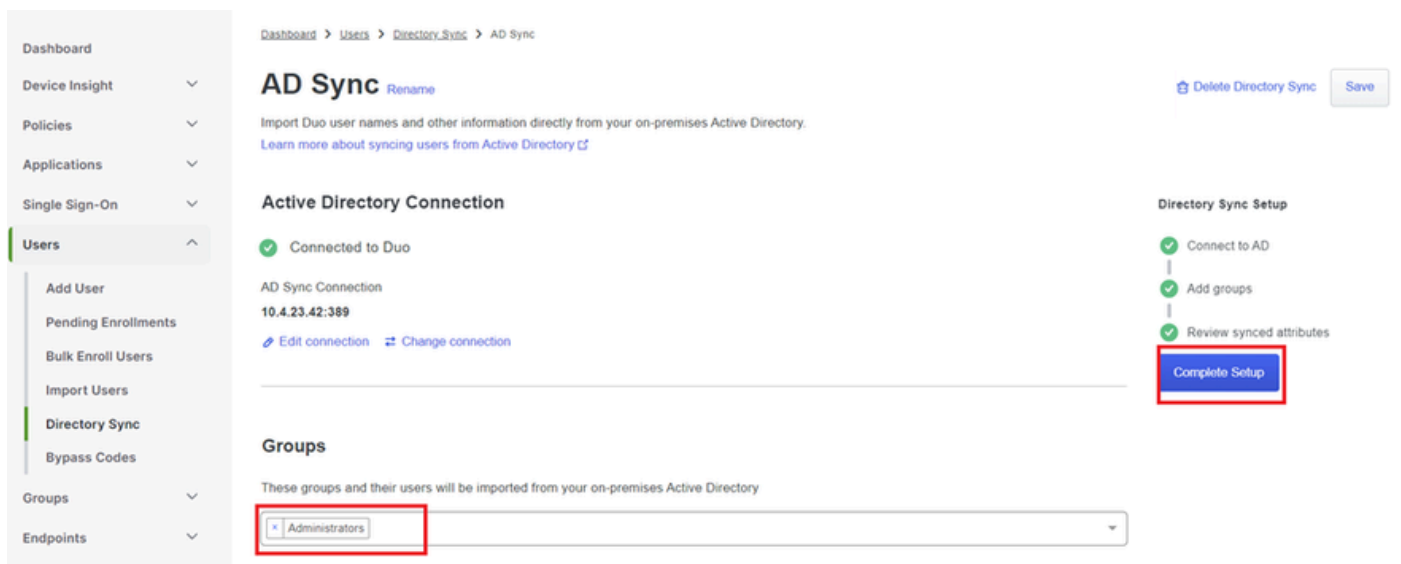


Liste des utilisateurs.

2. Sélectionnez la configuration Active Directory que vous souhaitez gérer.

3. Dans les paramètres de configuration, identifiez et choisissez les groupes spécifiques dans Active Directory que vous souhaitez synchroniser avec le cloud Duo. Envisagez d'utiliser les options de filtrage pour votre sélection.

4. Cliquez sur Terminer la configuration.



Synchronisation AD.

5. Pour lancer immédiatement la synchronisation, cliquez sur Synchroniser maintenant. Les comptes d'utilisateurs sont ainsi exportés des groupes spécifiés dans Active Directory vers le cloud Duo, ce qui leur permet d'être gérés dans l'environnement de sécurité Duo.

# AD Sync Rename

Delete Directory Sync No Changes

Import Duo user names and other information directly from your on-premises Active Directory.  
[Learn more about syncing users from Active Directory](#)

## Sync Controls

### Sync status

Scheduled to automatically synchronize every 12 hours, next around 2:00 AM UTC [Pause automatic syncs](#)

**Sync Now**

Troubleshooting

### Active Directory Connection

Connected to Duo

AD Sync Connection

10.4.23.42:389

[Edit connection](#)

[Change connection](#)

Démarrage de la synchronisation

Inscrivez les utilisateurs dans le cloud Cisco DUO.

L'inscription de l'utilisateur permet la vérification de l'identité par diverses méthodes, telles que l'accès au code, la diffusion DUO, les codes SMS et les jetons.

1. Accédez à la section Users du tableau de bord Cisco Cloud.
2. Recherchez et sélectionnez le compte de l'utilisateur que vous souhaitez inscrire.

Dashboard > Users

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

Need to activate a replacement phone? [Learn more about Reactivating Duo Mobile](#)

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

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

<input type="checkbox"/>	Username	Name	Email	Phones	Tokens	Status	Last Login
<input checked="" type="checkbox"/>	administrator		oteg			Active	Never authenticated

1 total

Liste des comptes utilisateur.

3. Cliquez sur le bouton Envoyer un e-mail d'inscription pour lancer le processus d'inscription.

# administrator

Logs

Send Enrollment Email

Sync This User



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



This user was synced from the directory **AD Sync**. Some fields are read-only.

Username

administrator

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).

Inscription par e-mail.

4. Consultez la boîte de réception de l'e-mail et ouvrez l'invitation d'inscription pour terminer le processus d'authentification.

Pour plus d'informations sur le processus d'inscription, veuillez consulter les ressources suivantes :

- Guide d'inscription universel : <https://guide.duo.com/universal-enrollment>
- Guide d'inscription traditionnel : <https://guide.duo.com/traditional-enrollment>

Procédure de validation de configuration.

Pour vous assurer que vos configurations sont correctes et opérationnelles, validez les étapes suivantes :

1. Lancez un navigateur Web et saisissez l'adresse IP du périphérique Firepower Threat Defense (FTD) pour accéder à l'interface VPN.

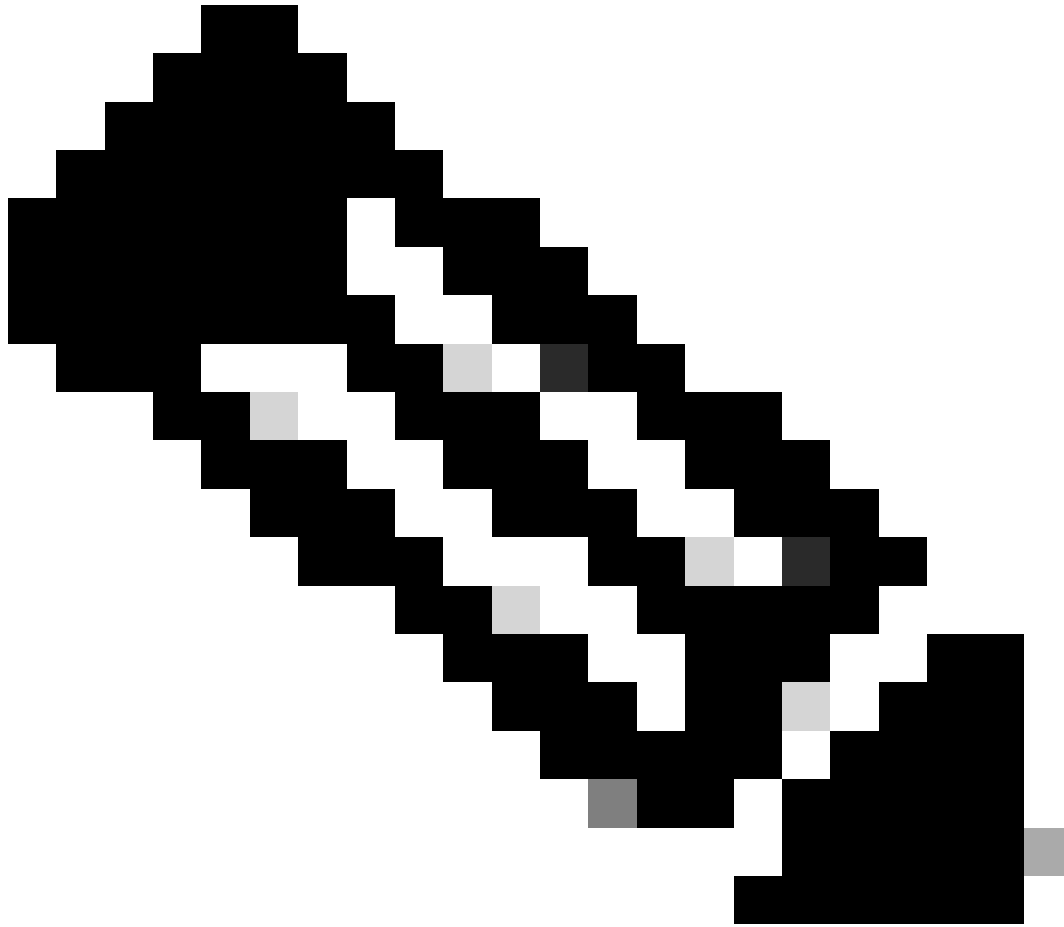


The screenshot shows a web browser window with a title bar that says "Logon". Inside the window, there is a form with the following elements:

- A "Group" label followed by a dropdown menu showing "VPN\_Remote".
- A "Username" label followed by a text input field.
- A "Password" label followed by a text input field.
- A "Logon" button centered below the input fields.

Connexion VPN.

2. Entrez votre nom d'utilisateur et votre mot de passe lorsque vous y êtes invité.



Remarque : les informations d'identification font partie des comptes Active Directory.

---

3. Lorsque vous recevez une notification DUO Push, approuvez-la en utilisant le logiciel DUO Mobile pour poursuivre le processus de validation.



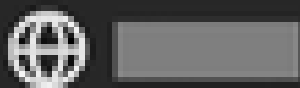


(1) Login request waiting.

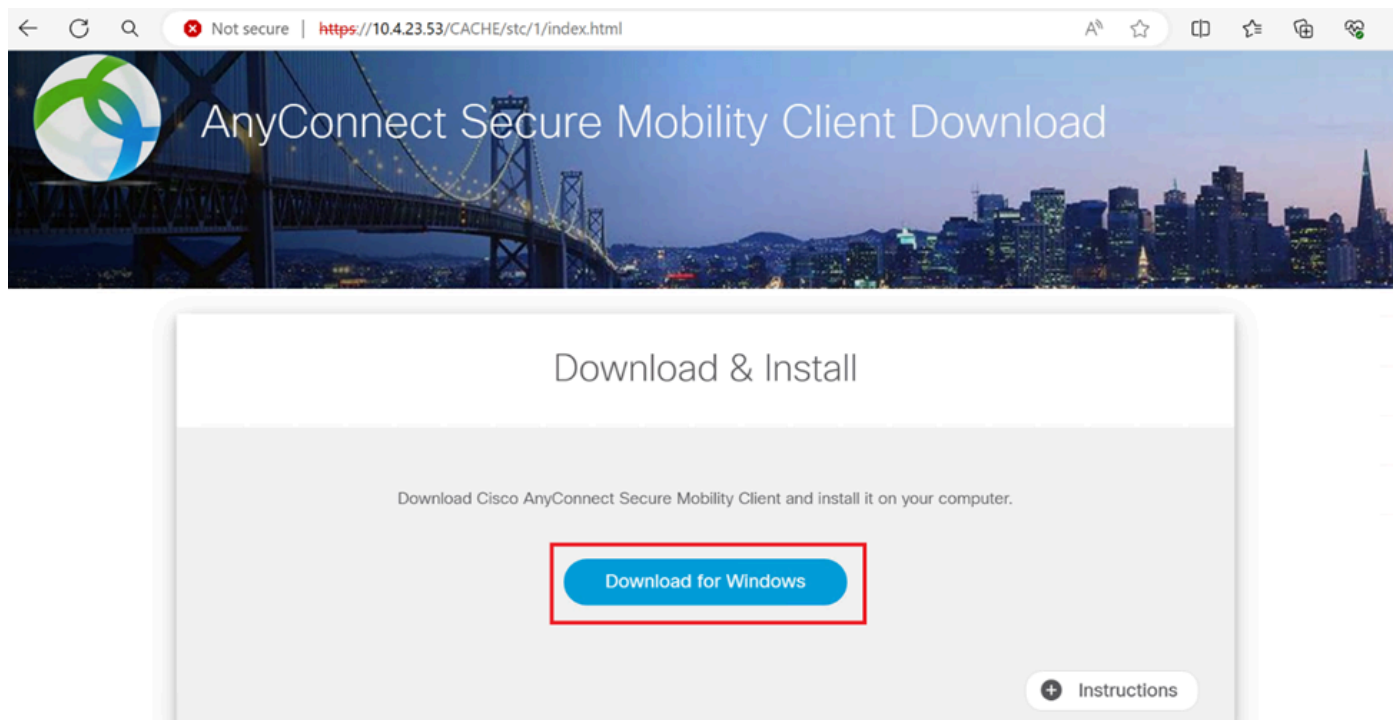
[Respond](#)



Are you logging in to Cisco ISE  
**RADIUS?**

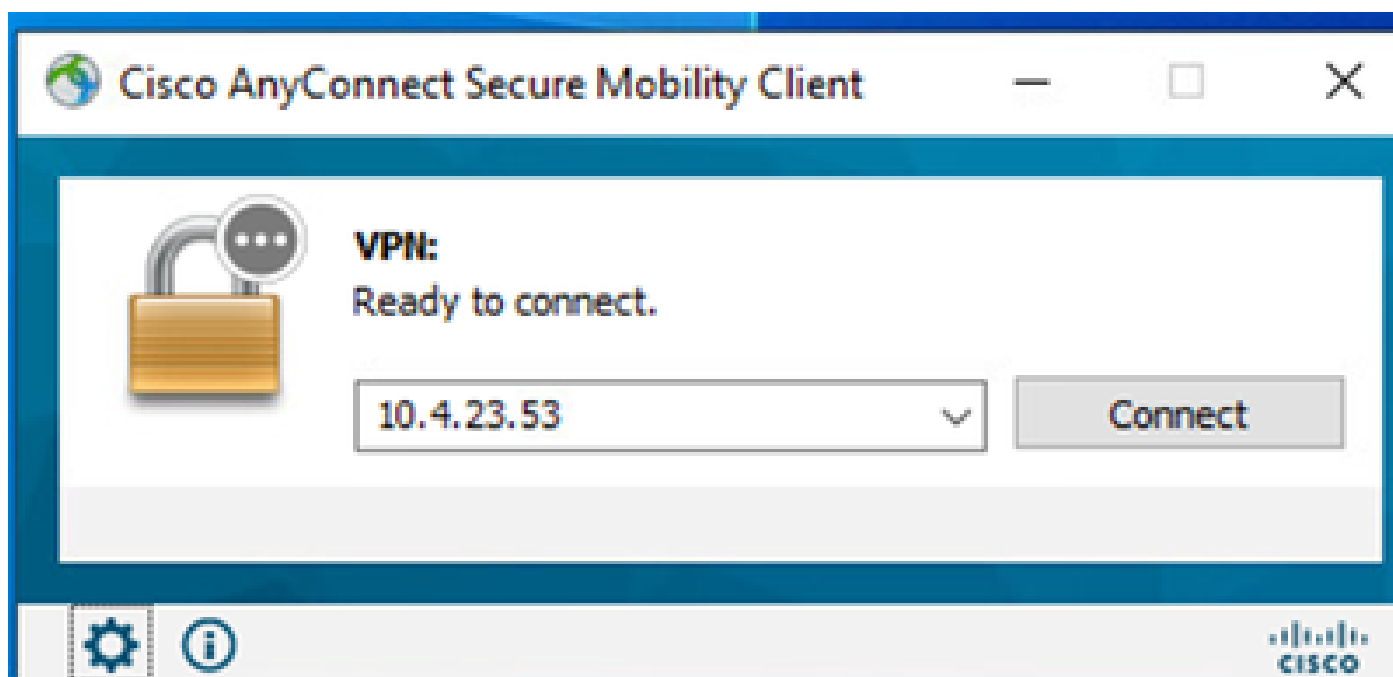


Localisez et téléchargez le package client VPN Cisco AnyConnect approprié pour les systèmes Windows.



Télécharger et installer.

5. Exécutez le fichier d'installation AnyConnect téléchargé et suivez les instructions fournies par le programme d'installation sur votre périphérique Windows.
6. Ouvrez le logiciel Cisco AnyConnect Secure Mobility Client. Connectez-vous au VPN en entrant l'adresse IP du périphérique FTD.



Tout logiciel Connect.

7. Lorsque vous y êtes invité, saisissez vos informations d'identification d'accès VPN et autorisez

à nouveau la notification de transmission DUO pour authentifier votre connexion.



(1) Login request waiting.

[Respond](#)



Are you logging in to Cisco ISE  
RADIUS?

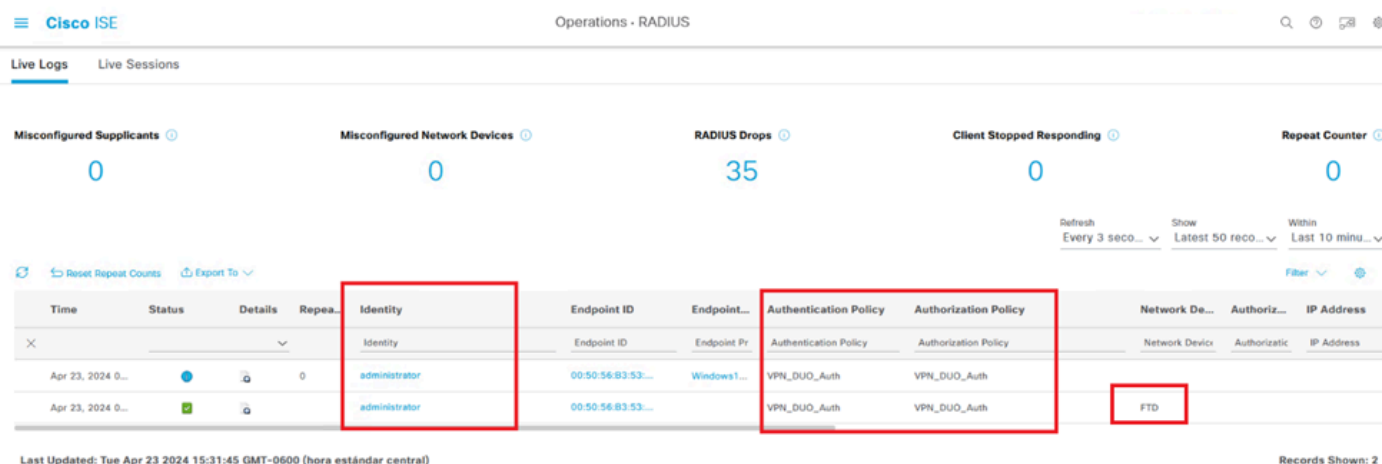


 Unknown

 3:22 PM CST

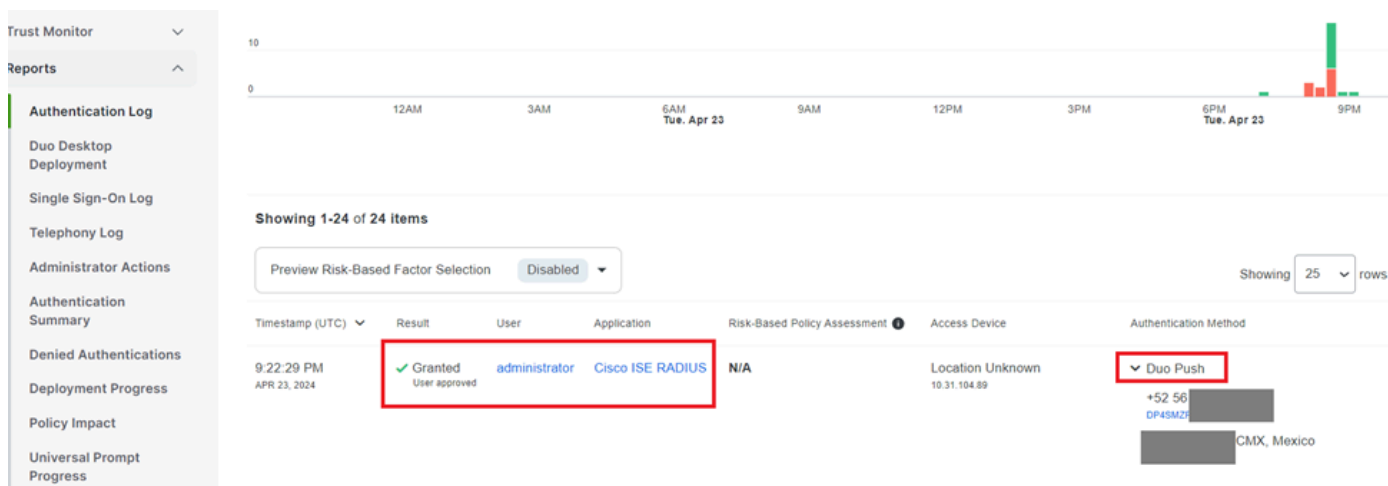
 administrator

pour surveiller l'activité en temps réel et vérifier la connectivité appropriée, accéder aux journaux en direct dans Cisco Identity Services Engine (ISE).



Logs ISE.

9. Accédez à Rapports > Journaux d'authentification pour consulter les journaux d'authentification dans le panneau d'administration DUO pour confirmer les vérifications réussies.



Journaux d'authentification.

## Problèmes courants.

### Scénario de travail.

Avant d'explorer les erreurs spécifiques liées à cette intégration, il est essentiel de comprendre le scénario de travail global.

Dans les journaux de connexion ISE, nous pouvons confirmer que ISE a transféré les paquets RADIUS au proxy DUO, et une fois que l'utilisateur a accepté la transmission DUO, l'acceptation d'accès RADIUS a été reçue du serveur proxy DUO.

Overview

Event	5200 Authentication succeeded
Username	administrator
Endpoint Id	00:50:56:B3:53:D6
Endpoint Profile	
Authentication Policy	VPN_DUO_Auth
Authorization Policy	VPN_DUO_Auth
Authorization Result	

Authentication Details

Source Timestamp	2024-04-24 20:03:33.142
Received Timestamp	2024-04-24 20:03:33.142
Policy Server	asc-ise32p3-1300
Event	5200 Authentication succeeded
Username	administrator
Endpoint Id	00:50:56:B3:53:D6
Calling Station Id	10.31.104.89
Audit Session Id	000000000002e000662965a9
Network Device	FTD

Steps

- 11001 Received RADIUS Access-Request
- 11017 RADIUS created a new session
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15048 Queried PIP - Network Access.NetworkDeviceName
- 11358 Received request for RADIUS server sequence.
- 11361 Valid incoming authentication request
- 11355 Start forwarding request to remote RADIUS server
- 11365 Modify attributes before sending request to external radius server
- 11100 RADIUS-Client about to send request - ( port = 1812 )
- 11101 RADIUS-Client received response ( Step latency=5299 ms)
- 11357 Successfully forwarded request to current remote RADIUS server
- 11002 Returned RADIUS Access-Accept

Authentication réussie.

CiscoAVPair

mdm-tlv=device-platform=win,  
mdm-tlv=device-mac=00-50-56-b3-53-d6,  
mdm-tlv=device-type=VMware, Inc. VMware7,1,  
mdm-tlv=device-platform-version=10.0.19045 ,  
mdm-tlv=device-public-mac=00-50-56-b3-53-d6,  
mdm-tlv=ac-user-agent=AnyConnect Windows 4.10.08029,  
mdm-tlv=device-uid-  
global=4CEBE2C21A8B81F490AC91086452CF3592593437,  
mdm-tlv=device-  
uid=3C5C68FF5FD3B6FA9D364DDB90E2B0BFA7E44B0EAAA  
CA383D5A8CE0964A799DD,  
audit-session-id=000000000002e000662965a9,  
ip:source-ip=10.31.104.89  
coa-push=true,  
proxy-flow=[10.4.23.53,10.4.23.21]

Result

Reply-Message Success. Logging you in...

Résultat réussi.

Une capture de paquets du côté ISE affiche les informations suivantes :

Source	Destination	Protocol	Length	Info	
10.4.23.53	10.4.23.21	RADIUS	741	Access-Request id=138	→ The FTD sends the RADIUS request to ISE
10.4.23.21	10.31.126.207	RADIUS	883	Access-Request id=41	→ ISE resends the same RADIUS requests to the DUO Proxy
10.31.126.207	10.4.23.21	RADIUS	190	Access-Accept id=41	→ DUO Proxy sends the RADIUS accept (DUO push approved)
10.4.23.21	10.4.23.53	RADIUS	90	Access-Accept id=138	→ ISE resend the RADIUS accept to the FTD
10.4.23.53	10.4.23.21	RADIUS	739	Accounting-Request id=139	→ FTD sends the accounting for the current VPN connection
10.4.23.21	10.4.23.53	RADIUS	62	Accounting-Response id=139	→ ISE registered the accounting on its dashboard

Capture de paquets ISE.

**Error11368** Veuillez consulter les journaux sur le serveur RADIUS externe pour déterminer la raison précise de l'échec.

Event	5400 Authentication failed
Failure Reason	11368 Please review logs on the External RADIUS Server to determine the precise failure reason.
Resolution	Please review logs on the External RADIUS Server to determine the precise failure reason.
Root cause	Please review logs on the External RADIUS Server to determine the precise failure reason.

Erreur 11368 .

Dépannage :

- Vérifiez que la clé secrète partagée RADIUS dans ISE est identique à la clé configurée dans le FMC.

1. Ouvrez l'interface utilisateur graphique ISE.
2. Administration > Ressources réseau > Périphériques réseau.
3. Sélectionnez le serveur proxy DUO.
4. À côté du secret partagé, cliquez sur "Afficher" pour afficher la clé au format texte brut.
5. Ouvrez l'interface graphique FMC.
6. Objets > Gestion des objets > Serveur AAA > Groupe de serveurs RADIUS.
7. Sélectionnez le serveur ISE.
8. Saisissez à nouveau la clé secrète.

- Vérifiez l'intégration Active Directory dans DUO.

1. Ouvrez le DUO Authentication Proxy Manager.

2. Confirmez l'utilisateur et le mot de passe dans la section [ad\_client].
3. Cliquez sur Valider pour confirmer que les informations d'identification actuelles sont correctes.

### Erreur 11353 : plus de serveurs RADIUS externes ; impossible d'effectuer le basculement

Event	5405 RADIUS Request dropped
Failure Reason	11353 No more external RADIUS servers; can't perform failover
Resolution	Verify the following: At least one of the remote RADIUS servers in the ISE proxy service is up and configured properly ; Shared secret specified in the ISE proxy service for every remote RADIUS server is same as the shared secret specified for the ISE server ; Port of every remote RADIUS server is properly specified in the ISE proxy service.
Root cause	Failover is not possible because no more external RADIUS servers are configured. Dropping the request.

Erreur 11353 .

#### Dépannage :

- Vérifiez que la clé secrète partagée RADIUS dans ISE est identique à la clé configurée dans le serveur proxy DUO.

1. Ouvrez l'interface utilisateur graphique ISE.
2. Administration > Ressources réseau > Périphériques réseau.
3. Sélectionnez le serveur proxy DUO.
4. À côté du secret partagé, cliquez sur "Afficher" pour afficher la clé au format texte brut.
5. Ouvrez le DUO Authentication Proxy Manager.
6. Vérifiez la section [radius\_server\_auto] et comparez la clé secrète partagée.

Les sessions RADIUS n'apparaissent pas dans les journaux en direct ISE.

#### Dépannage :

- Vérifiez la configuration DUO.

1. Ouvrez le DUO Authentication Proxy Manager.
2. Vérifiez l'adresse IP ISE dans la section [radius\_server\_auto]



- Vérifiez la configuration FMC.

1. Ouvrez l'interface graphique FMC.

2. Accédez à Objets > Gestion des objets > Serveur AAA > Groupe de serveurs RADIUS.

3. Sélectionnez le serveur ISE.

4. Vérifiez l'adresse IP ISE.

- Effectuez une capture de paquets dans ISE pour confirmer la réception des paquets RADIUS.

1. Accédez à Operations > Troubleshoot > Diagnostic Tools > TCP Dump

## Dépannage supplémentaire.

- Activez les composants suivants dans le PSN en tant que debug :

Moteur de politiques

Prt-JNI

runtime-AAA

Pour plus d'informations sur le dépannage dans DUO Authentication Proxy Manager, consultez le lien suivant :

[https://help.duo.com/s/article/1126?language=en\\_US](https://help.duo.com/s/article/1126?language=en_US)

## Modèle DUO.

Vous pouvez utiliser le modèle suivant pour terminer la configuration dans votre serveur proxy DUO.

```
[main] <--- OPTIONAL
http_proxy_host=<Proxy IP address or FQDN>
http_proxy_port=<Proxy port>
[radius_server_auto]
ikey=xxxxxxxxxxxxxxxx
skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=xxxxxxxxxxxxxxxxxxxxxx
radius_ip_1=<PSN IP Address>
radius_secret_1=xxxxxxxxxx
failmode=safe
port=1812
client=ad_client

[ad_client]
host=<AD IP Address>
service_account_username=xxxxxxxx
```

service\_account\_password=xxxxxxxxxx  
search\_dn=DC=xxxxxx,DC=xxxx

[cloud]

apikey=xxxxxxxxxxxxxxxxxxxxxx  
skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx  
api\_host=xxxxxxxxxxxxxxxxxxxxxx  
service\_account\_username=<your domain\username>  
service\_account\_password=xxxxxxxxxxxx

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.