Configuration de l'authentification à deux facteurs duo pour l'accès à la gestion ISE

Table des matières

[Introduction](#)

[Conditions préalables](#)

- [Exigences](#)
- [Composants utilisés](#)

[Diagramme du réseau](#)

[Configuration](#)

- [Configuration Duo](#)
- [Configuration ISE](#)
- [Intégrer ISE au proxy d'authentification Duo](#)

[Vérifier](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit les étapes requises pour configurer l'authentification à deux facteurs externe pour l'accès à la gestion Identity Services Engine (ISE).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Protocole RADIUS
- Configuration du serveur et des identités de jeton RADIUS ISE

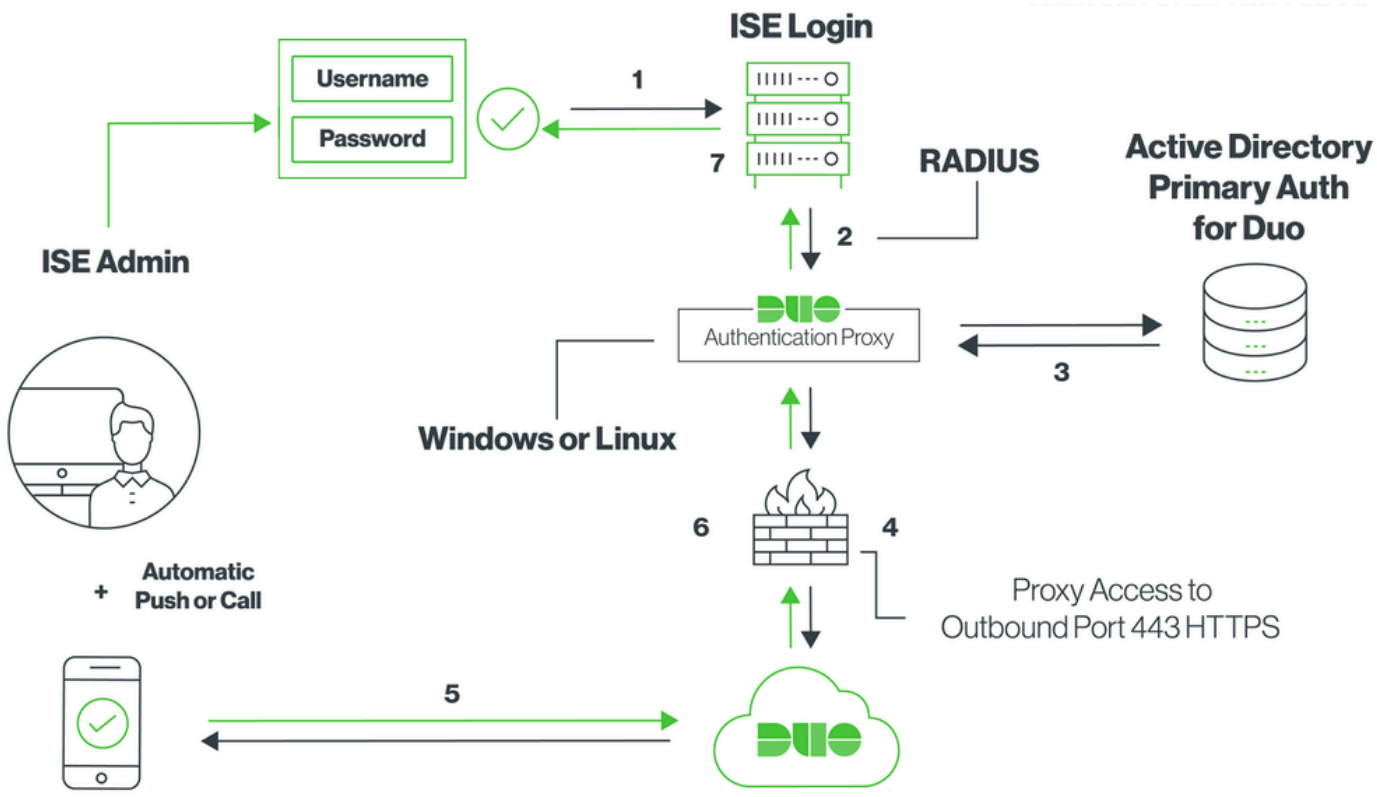
Composants utilisés

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

- Service cloud Duo
- Active Directory (AD)
- Moteur du service de vérification des identités (ISE)
- Serveur proxy d'authentification duo

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



Configuration

Configuration Duo

1. Téléchargez et installez le serveur proxy d'authentification Duo sur une machine Windows ou Linux - Proxy d'authentification Duo

---

Remarque : Cette machine doit avoir accès au cloud ISE et Duo (Internet)

---

2. Configurez le fichier authproxy.cfg. Ouvrez ce fichier dans un éditeur de texte tel que Notepad++ ou WordPad.

Remarque : l'emplacement par défaut se trouve à l'adresse C:\Program Files (x86)\Duo Security Authentication Proxy\conf\authproxy.cfg.

---

3. Créez une application « Cisco ISE RADIUS » dans le panneau d'administration Duo.

---

4. Modifiez le fichier authproxy.cfg et ajoutez la configuration suivante :

<#root>

```
        ikey= xxxxxxxxxxxxxxxxxxxxxxxx
        skey= xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
        api_host=api-xxxxxxxx.duosecurity.com
        radius_ip_1=10.127.196.189
```

Sample IP address of the ISE server

```
        radius_secret_1=******
        failmode=secure
        client=ad_client
        port=1812
```

---

5. Configurez ad_client avec vos détails Active Directory. Le proxy d'authentification duo utilise les informations de l'exemple suivant pour s'authentifier auprès d'Active Directory pour l'authentification principale :

<#root>

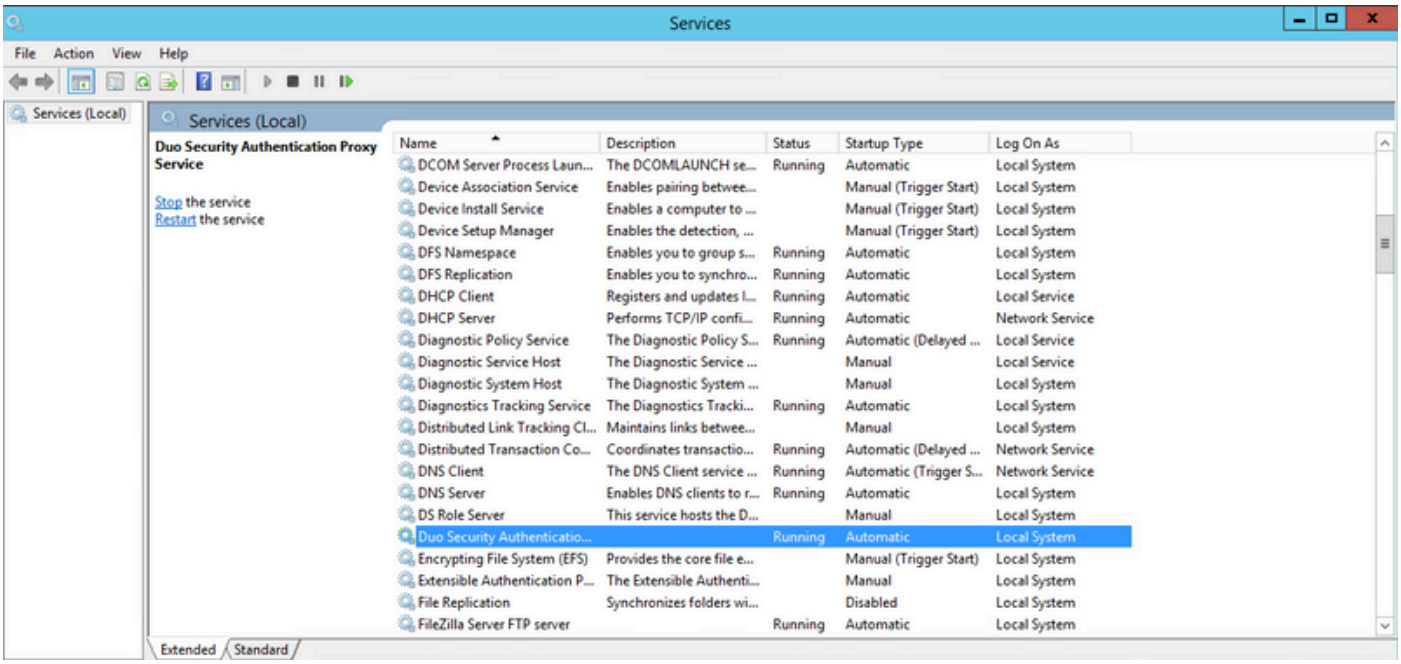
```
        [ad_client]
        host=10.127.196.230
```

Sample IP address of the Active Directory

```
service_account_username=< AD-username >
service_account_password=< AD-password >
search_dn=CN=Users,DC=gce,DC=iselab,DC=local
```

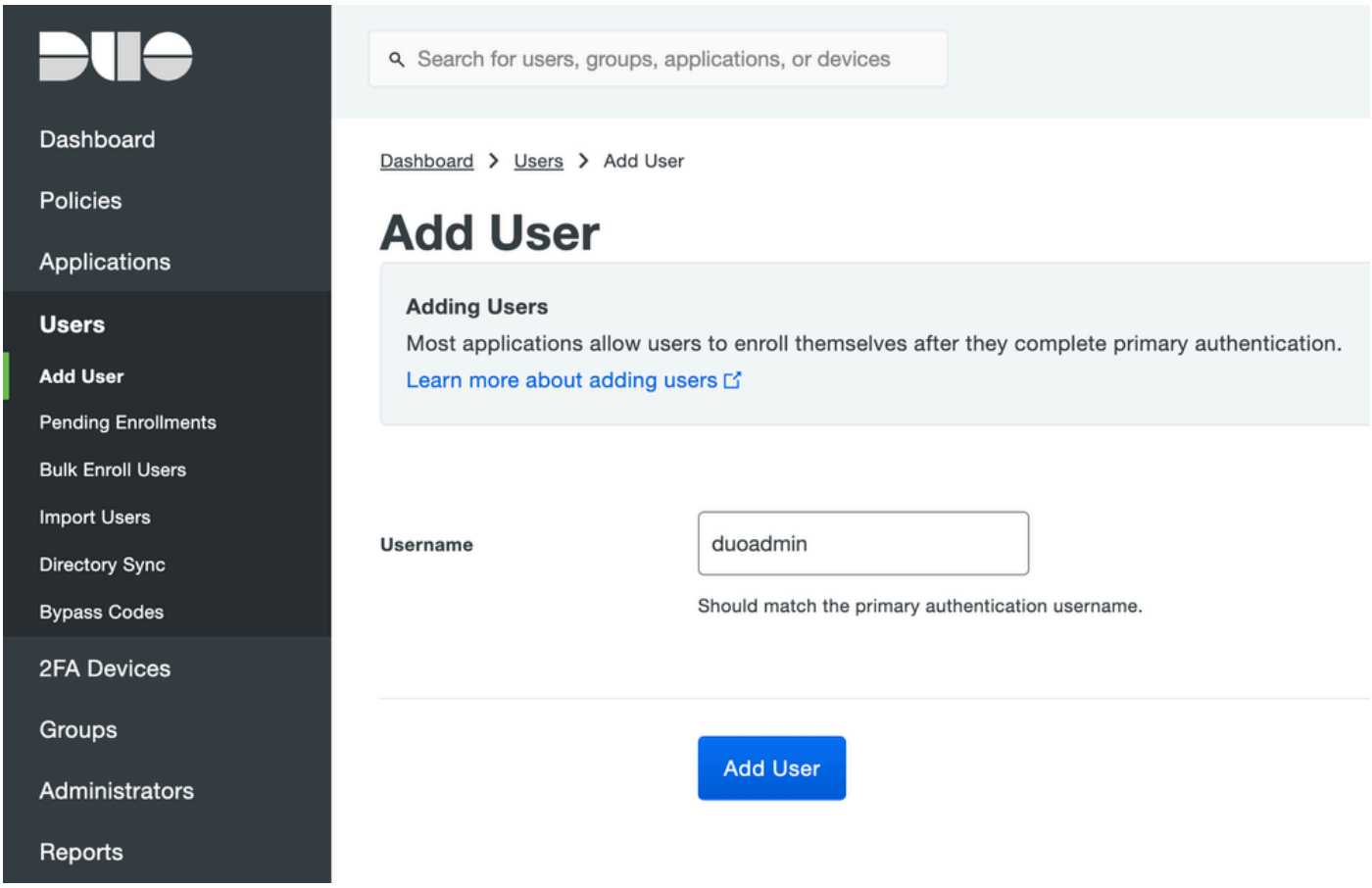
Remarque : Si votre réseau nécessite une connexion proxy HTTP pour l'accès à Internet, ajoutez les détails http_proxy dans authproxy.cfg.

6. Redémarrez le service proxy d'authentification de sécurité Duo. Enregistrez le fichier et redémarrez le service Duo sur l'ordinateur Windows. Ouvrez la console des services Windows (services.msc), localisez le service proxy d'authentification de sécurité Duo dans la liste des services, puis cliquez sur Redémarrer comme indiqué dans l'image :

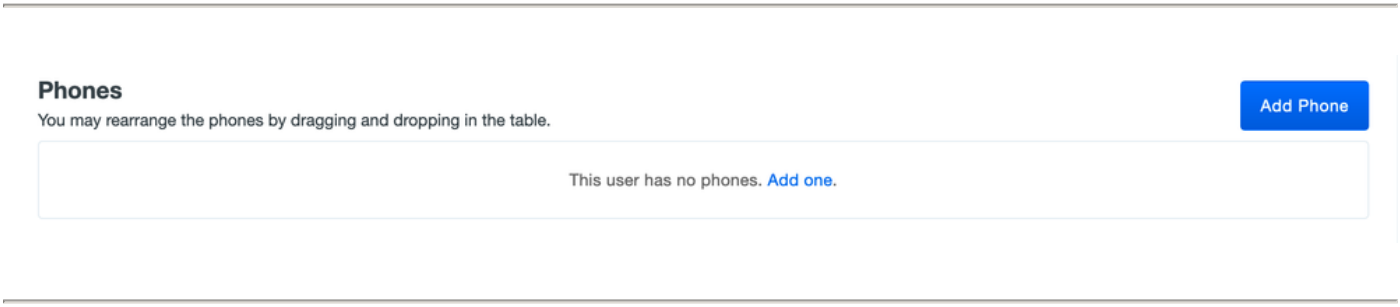


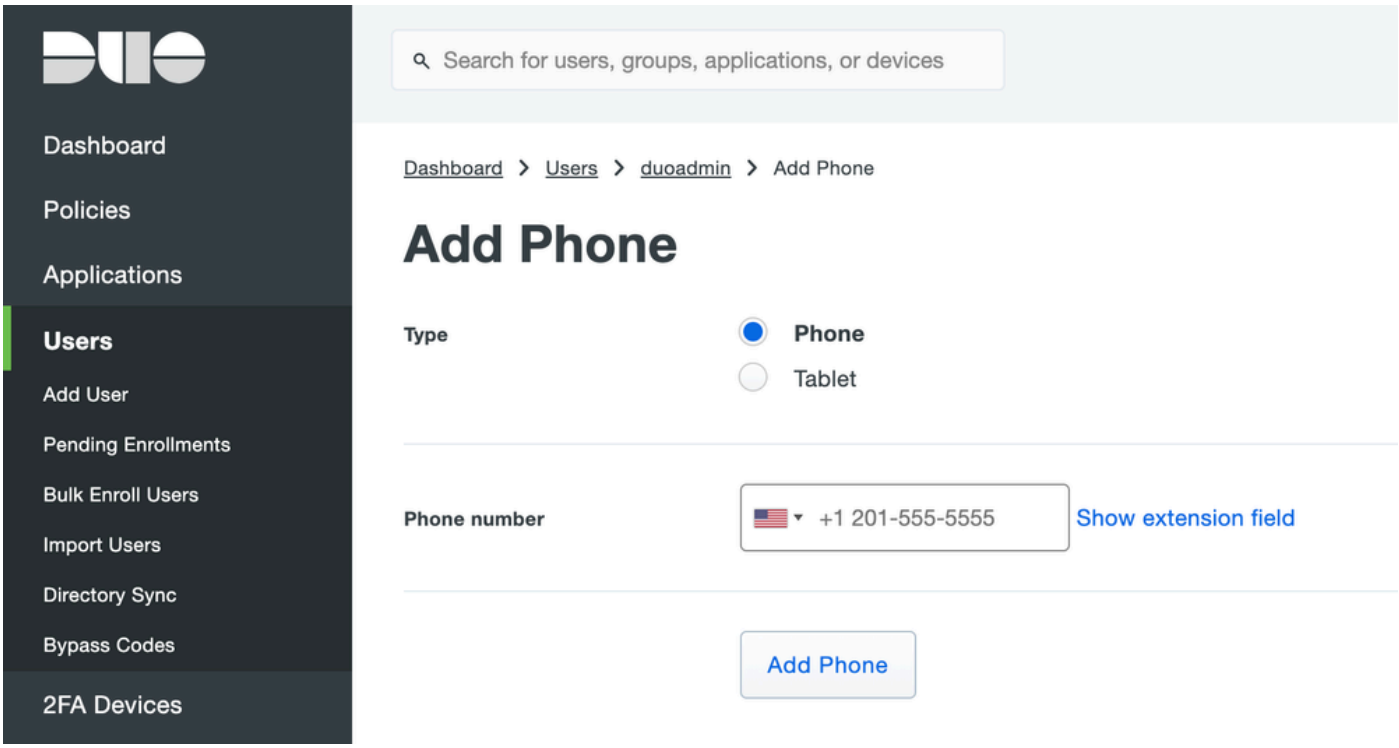
7. Créez un nom d'utilisateur et activez Duo Mobile sur le périphérique final.

8. Ajoutez un utilisateur dans le panneau d'administration Duo. Naviguez jusqu'à Users > Add Users, comme indiqué dans l'image :



9. Vérifiez que l'application Duo est installée sur le téléphone de l'utilisateur final.

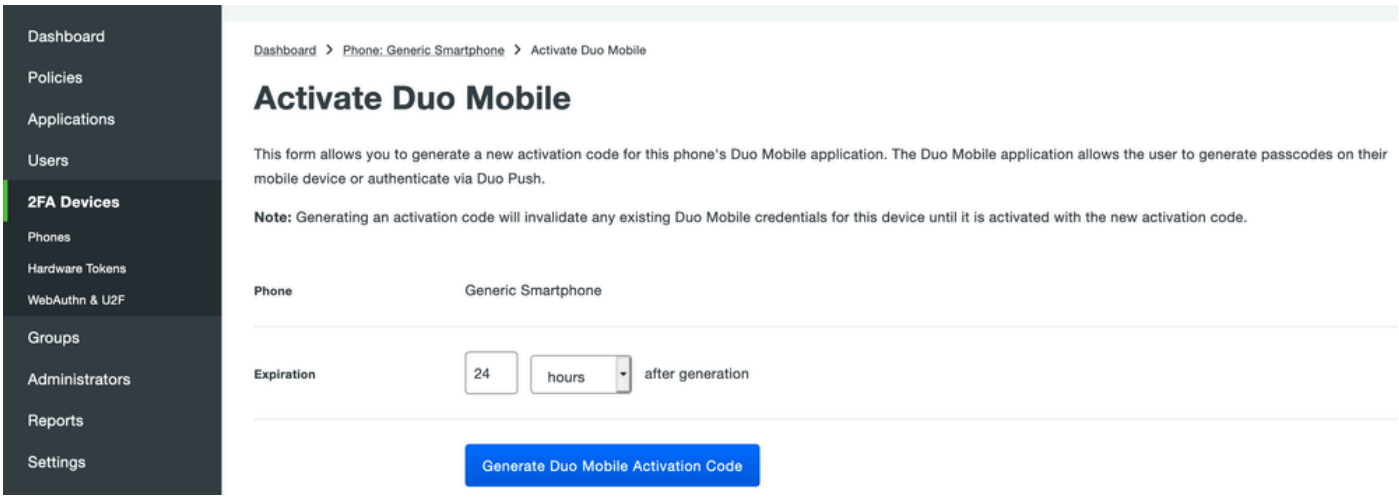




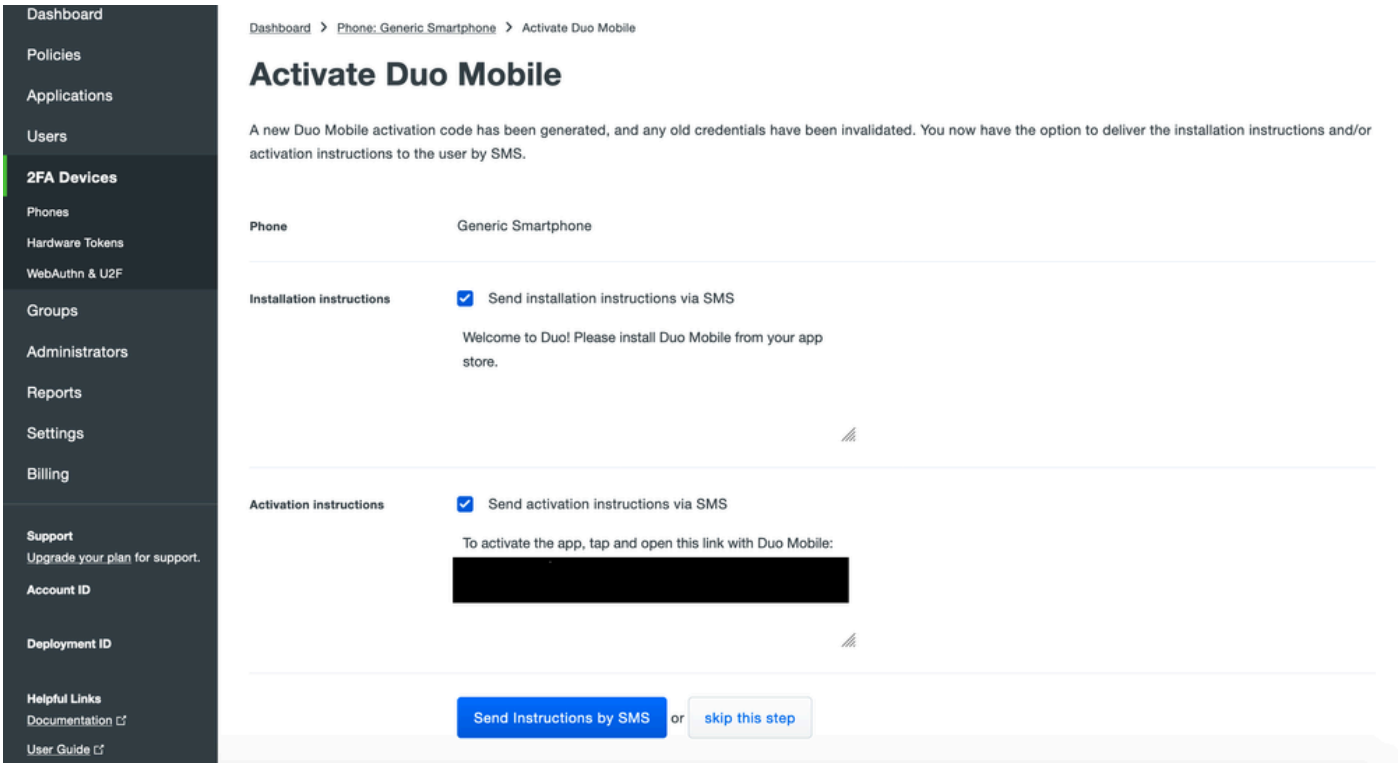
10. Sélectionnez Activate Duo Mobile, comme indiqué dans l'image :



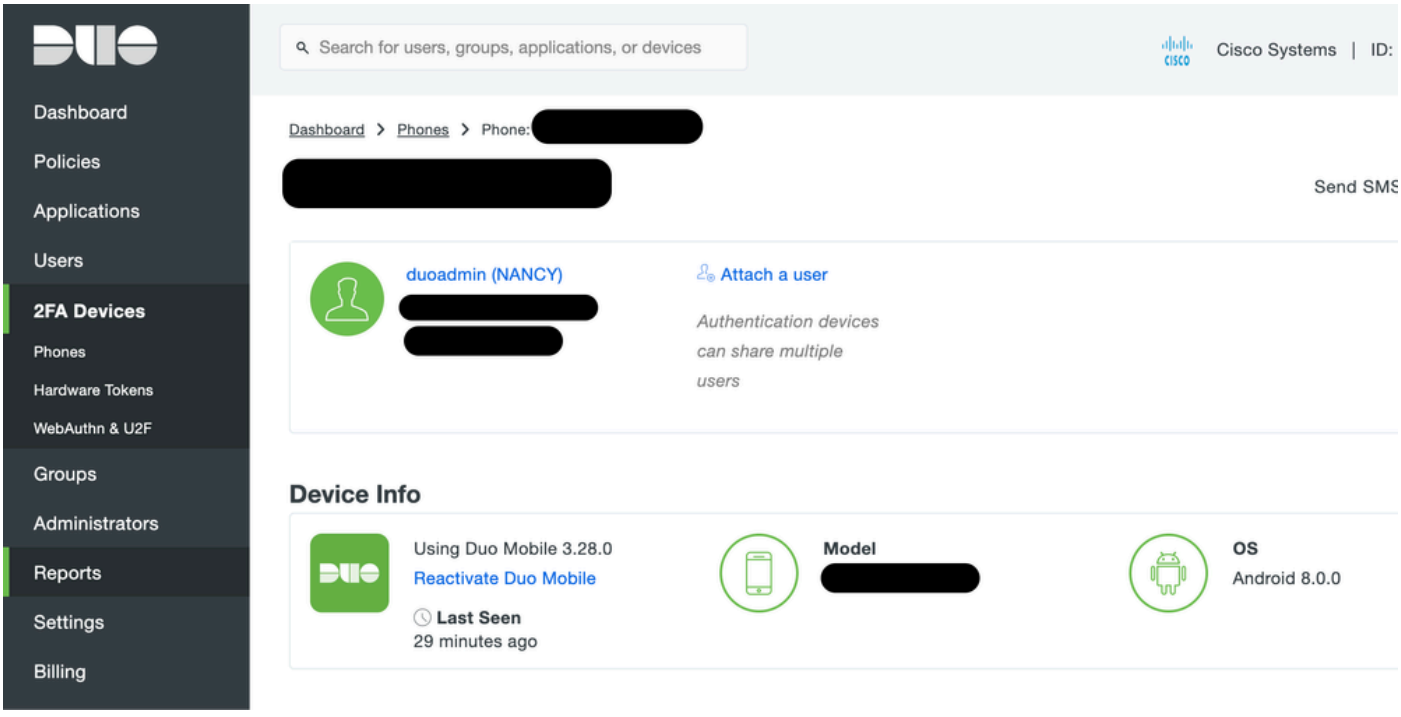
11. Sélectionnez Generate Duo Mobile Activation Code, comme indiqué dans l'image :



12. Sélectionnez Send Instructions by SMS, comme indiqué dans l'image :



13. Cliquez sur le lien dans SMS, et l'application Duo est liée au compte d'utilisateur dans la section Device Info :

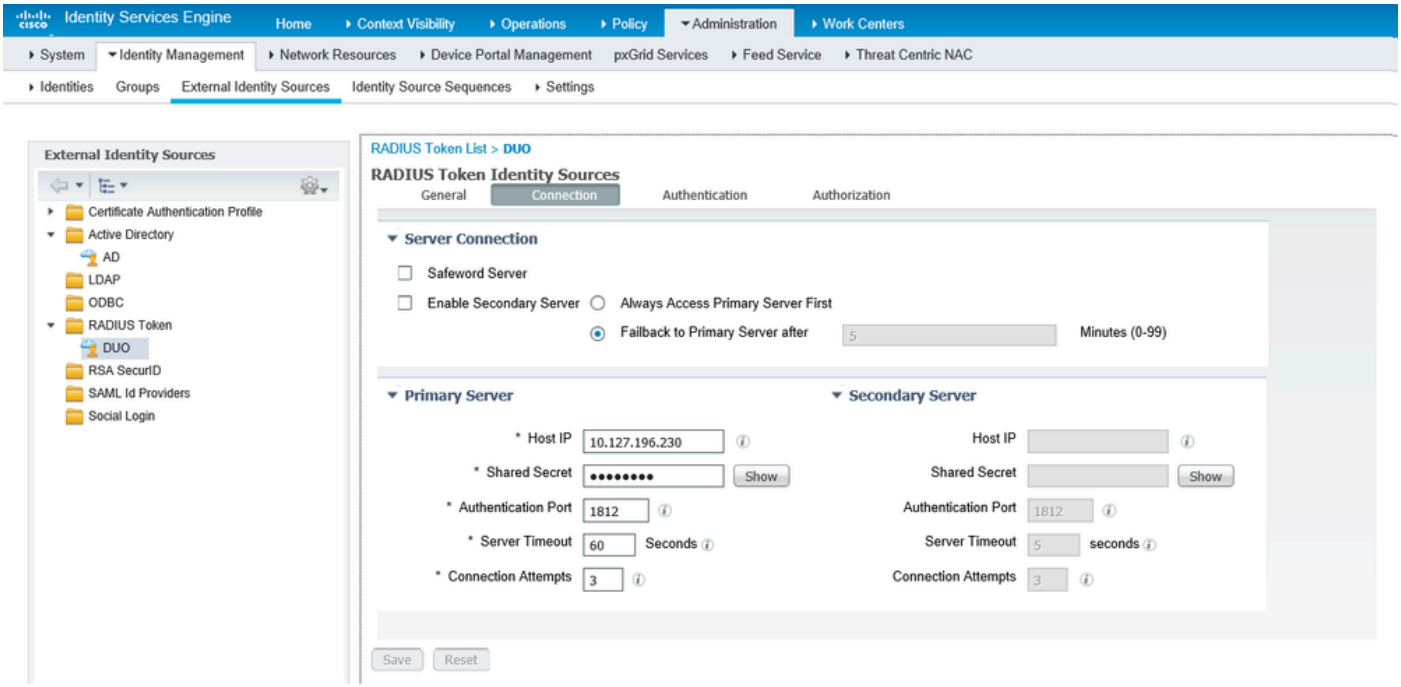


Configuration ISE

Intégrer ISE au proxy d'authentification Duo

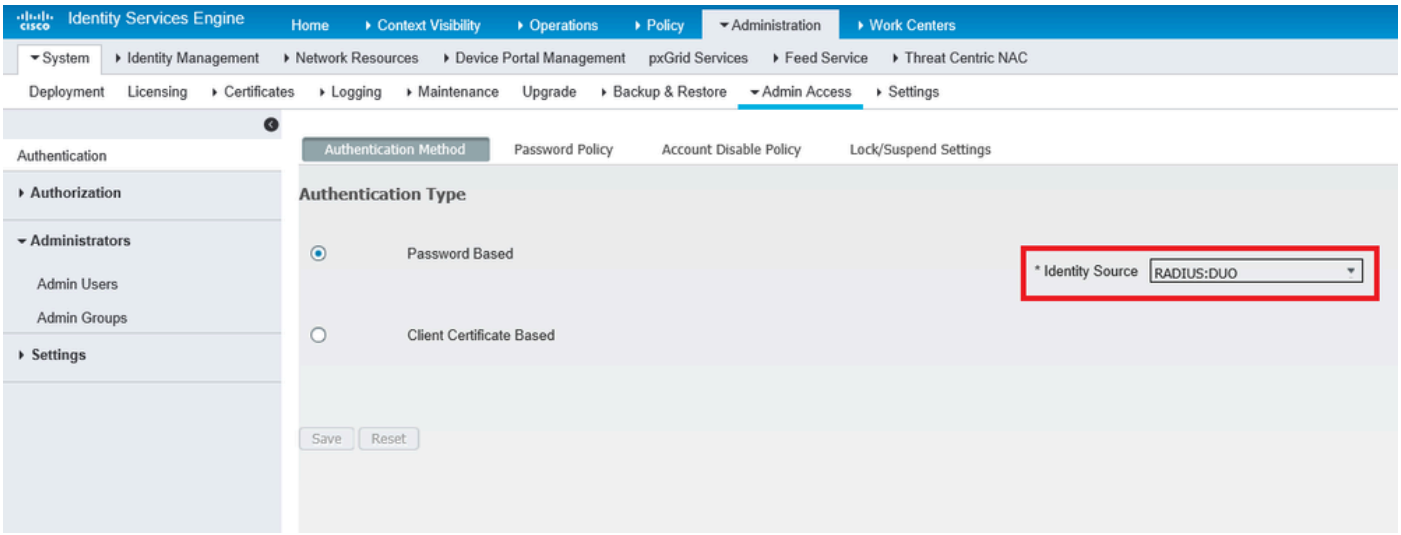
1. Accédez à Administration > Identity Management > External Identity Sources > RADIUS Token. Cliquez sur Add pour ajouter un nouveau serveur de jetons RADIUS. Définissez le nom du serveur dans l'onglet Général, l'adresse IP et la clé partagée dans l'onglet Connexion, comme indiqué dans l'image :

Remarque : Définissez le délai d'attente du serveur sur 60 secondes, afin que les utilisateurs disposent de suffisamment de temps pour agir sur la transmission.

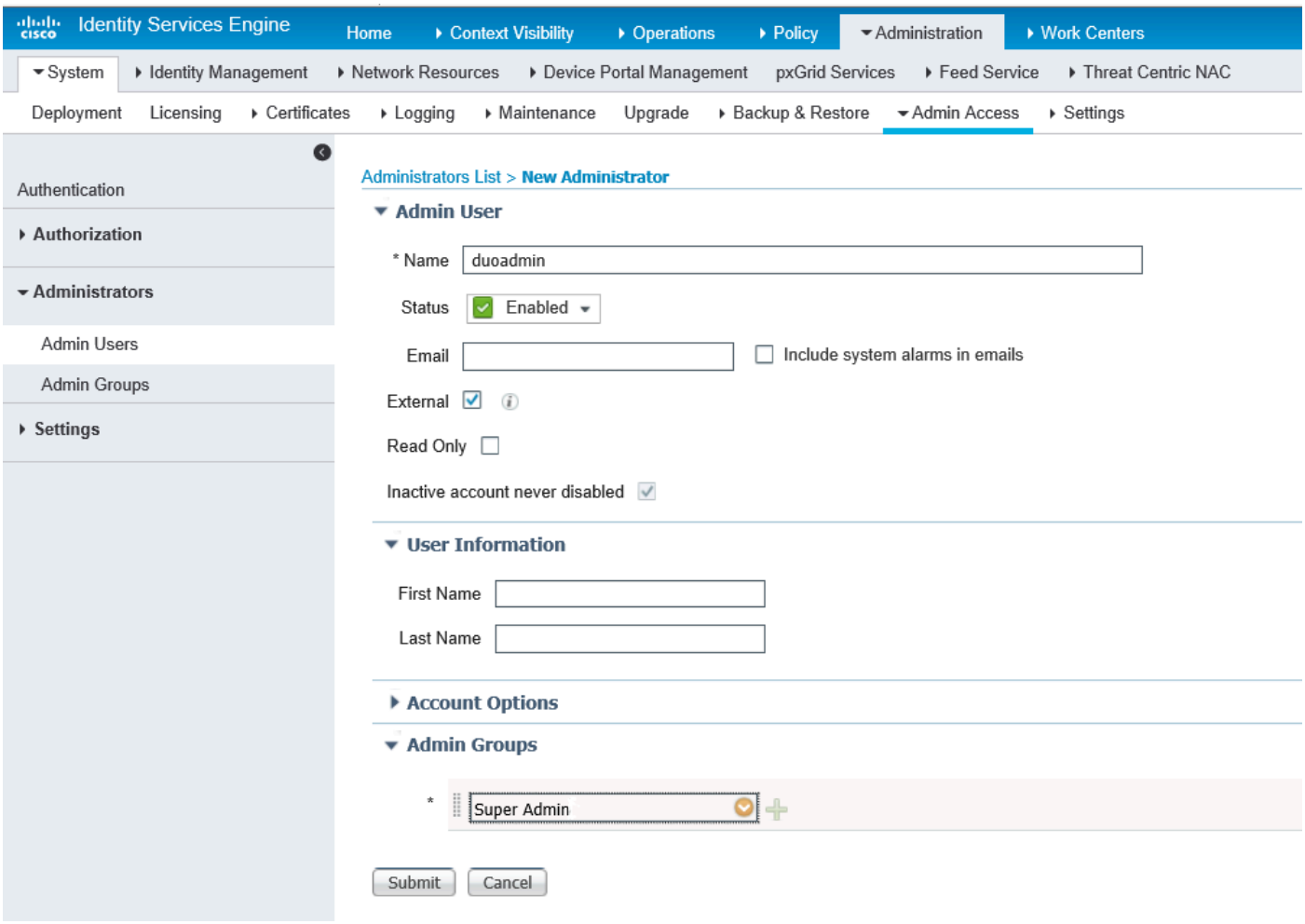


---

2. Accédez à Administration > System > Admin Access > Authentication > Authentication Method et sélectionnez le serveur de jeton RADIUS précédemment configuré comme source d'identité :



3. Accédez à Administration > System > Admin Access > Administrators > Admin Users et Create an admin user as external et fournissez le privilège super admin :

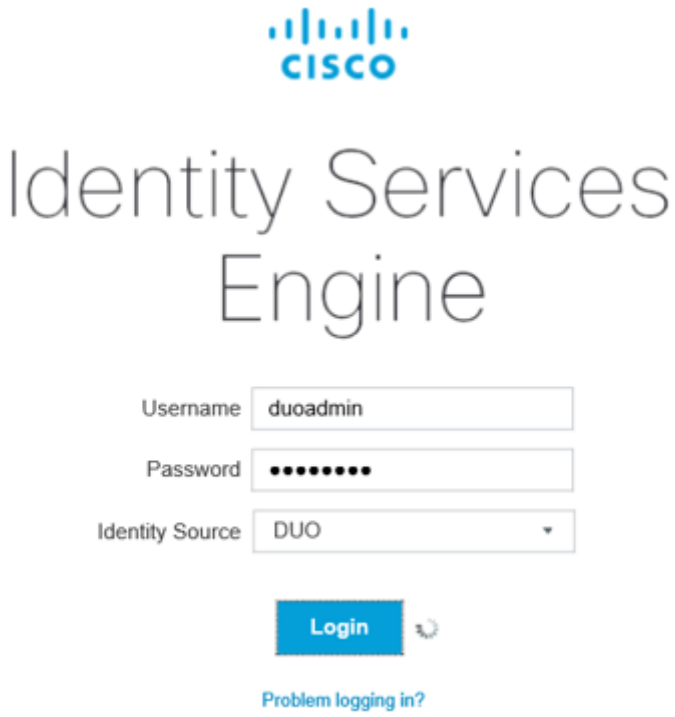


Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

---

1. Ouvrez l'interface utilisateur graphique ISE, sélectionnez le serveur de jetons RADIUS comme source d'identité et connectez-vous avec l'utilisateur admin.



Dépannage

Cette section fournit des informations pour dépanner votre configuration.

Pour résoudre les problèmes liés à la connectivité Duo Proxy avec le cloud ou Active Directory, activez le débogage sur le proxy Duo Auth en ajoutant « debug=true » sous la section principale de authproxy.cfg.

- Les journaux sont situés à l'adresse suivante : C:\Program Files (x86)\Duo Security Authentication Proxy\log

- Ouvrez le fichier authproxy.log dans un éditeur de texte tel que Notepad++ ou WordPad.

Consignez les extraits de la requête de proxy d'authentification Duo reçue d'ISE et envoyée à Duo Cloud :

<#root>

```
2019-08-19T04:59:27-0700 [DuoForwardServer (UDP)] Sending request from 10.127.196.189 to radius_server_
2019-08-19T04:59:27-0700 [DuoForwardServer (UDP)] Received new request id 2 from ('10.127.196.189', 620
2019-08-19T04:59:27-0700 [DuoForwardServer (UDP)] (('10.127.196.189', 62001), duoadmin, 2):

login attempt for username u'duoadmin'

2019-08-19T04:59:27-0700 [DuoForwardServer (UDP)]

Sending AD authentication request for 'duoadmin' to '10.127.196.230'

2019-08-19T04:59:27-0700 [duoauthproxy.modules.ad_client._ADAuthClientFactory#info] Starting factory
```

Extraits de journal du proxy d'authentification Duo ne pouvant pas atteindre le cloud Duo :

<#root>

```
2019-08-19T04:59:27-0700 [duoauthproxy.modules.ad_client._ADAuthClientFactory#info] Stopping factory
2019-08-19T04:59:37-0700 [-] Duo preauth call failed
Traceback (most recent call last):
File "twisted\internet\defer.pyc", line 654, in _runCallbacks
File "twisted\internet\defer.pyc", line 1475, in gotResult
File "twisted\internet\defer.pyc", line 1416, in _inlineCallbacks
File "twisted\python\failure.pyc", line 512, in throwExceptionIntoGenerator

File "duoauthproxy\lib\radius\duo_server.pyc", line 111, in preauth
File "twisted\internet\defer.pyc", line 1416, in _inlineCallbacks
File "twisted\python\failure.pyc", line 512, in throwExceptionIntoGenerator
File "duoauthproxy\lib\duo_async.pyc", line 246, in preauth
File "twisted\internet\defer.pyc", line 1416, in _inlineCallbacks
File "twisted\python\failure.pyc", line 512, in throwExceptionIntoGenerator
File "duoauthproxy\lib\duo_async.pyc", line 202, in call
File "twisted\internet\defer.pyc", line 654, in _runCallbacks
File "duoauthproxy\lib\duo_async.pyc", line 186, in err_func

duoauthproxy.lib.duo_async.DuoAPIFailOpenError: API Request Failed: DNSLookupError('api-xxxxxxxx.duosecu



2019-08-19T04:59:37-0700 [-] (('10.127.196.189', 62001), duoadmin, 3): Failmode Secure - Denied Duo log
2019-08-19T04:59:37-0700 [-] (('10.127.196.189', 62001), duoadmin, 3):

Returning response code 3: AccessReject
```

```
2019-08-19T04:59:37-0700 [-] (('10.127.196.189', 62001), duoadmin, 3): Sending response
```

Informations connexes

- Authentification VPN RA avec DUO
- Assistance et documentation techniques - Cisco Systems

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.