Configurer l'authentification à deux facteurs pour l'accès à la gestion ISE

Contenu

Introduction

Ce document décrit les étapes requises pour configurer l'authentification externe à deux facteurs pour l'accès à la gestion ISE (Identity Services Engine). Dans cet exemple, l'administrateur ISE s'authentifie auprès du serveur de jetons RADIUS et une authentification supplémentaire sous forme de notification push est envoyée par le serveur proxy d'authentification Duo à l'appareil mobile de l'administrateur.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Components Used

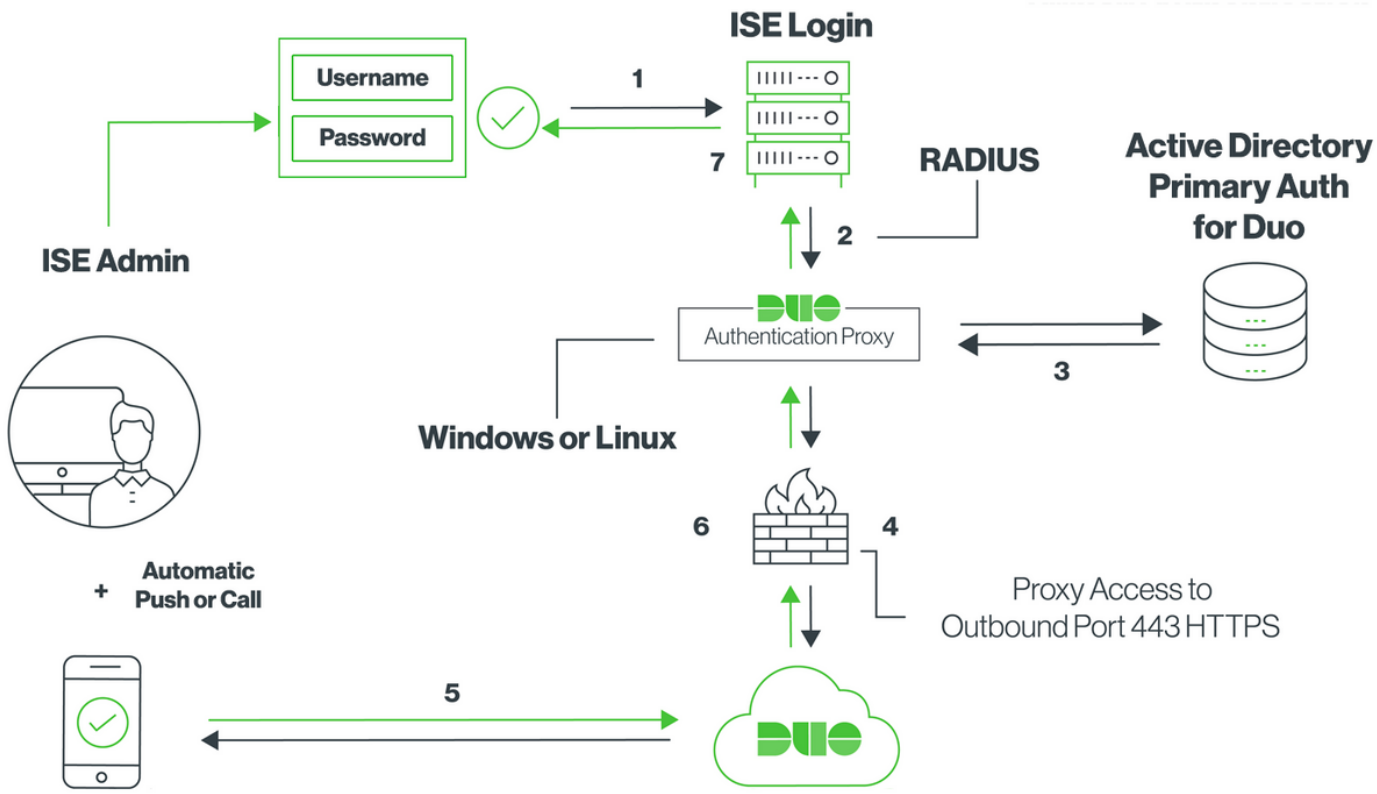
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Identity Services Engine (ISE)
- Active Directory (AD)
- Serveur proxy d'authentification Duo
- Service Cloud 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. If your network is

live, make sure that you understand the potential impact of any command.

Diagramme du réseau



Configuration

Configuration duo

Étape 1. Télécharger et installer Duo Authentication Proxy Server sur un ordinateur Windows ou Linux : https://duo.com/docs/ciscoise-radius#install-the-duo-authentication-proxy

> Note: Cette machine doit avoir accès au cloud ISE et duo (Internet)

Étape 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**

Étape 3. Créez une application Cisco ISE RADIUS dans le panneau d'administration de Duo : https://duo.com/docs/ciscoise-radius#first-steps

Étape 4. Modifiez le fichier **authproxy.cfg** et ajoutez cette configuration.

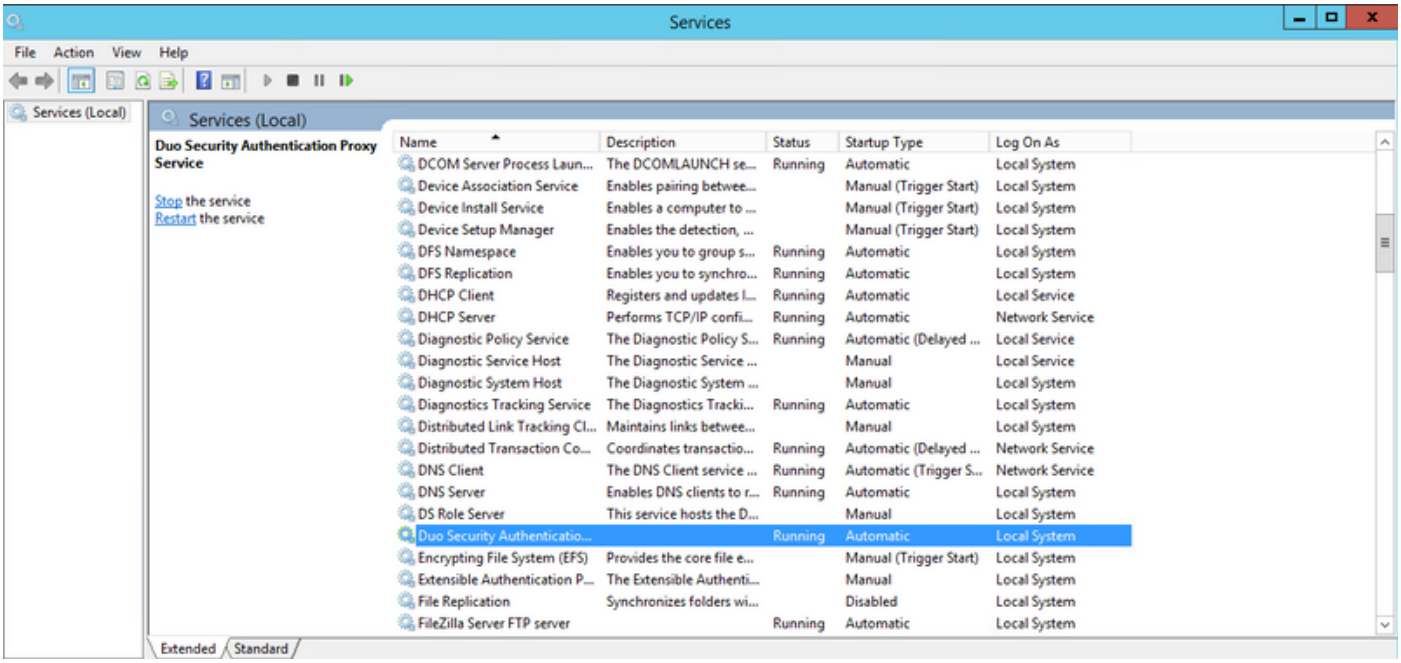
```
ikey= xxxxxxxxxxxxxxxxxxxxxxxx
skey= xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=api-xxxxxxxx.duosecurity.com
radius_ip_1=10.127.196.189                    Sample IP address of the ISE server
radius_secret_1=******
failmode=secure
client=ad_client
port=1812
```

Étape 5. Configurez ad_client avec vos détails Active Directory. Duo Auth Proxy utilise les informations ci-dessous pour s'authentifier contre AD pour l'authentification principale.

```
[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
```

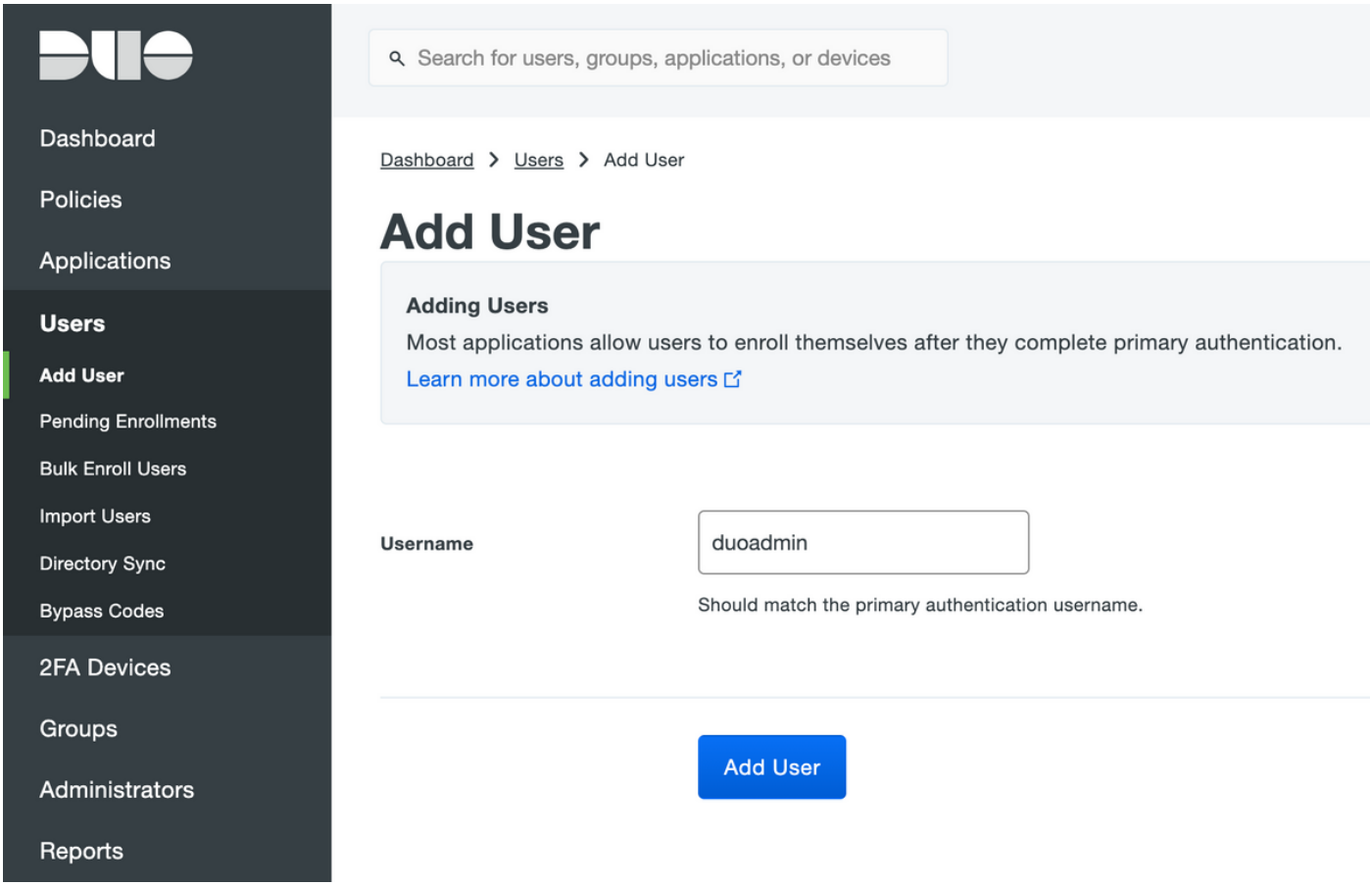
Note: Si votre réseau nécessite une connexion proxy HTTP pour l'accès à Internet, ajoutez les détails http_proxy dans authproxy.cfg.

Étape 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), recherchez **Duo Security Authentication Proxy Service** dans la liste des services, puis cliquez sur **Restart** comme indiqué dans l'image :

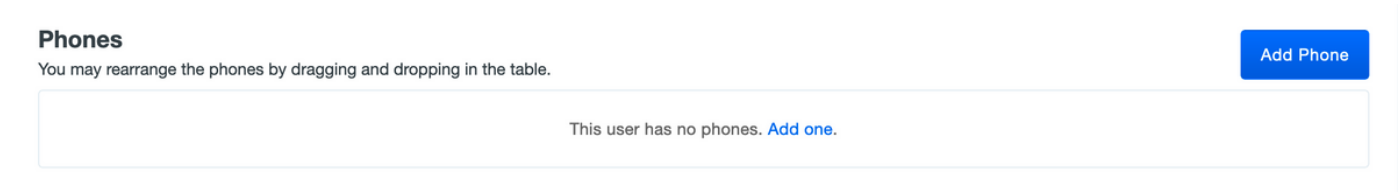


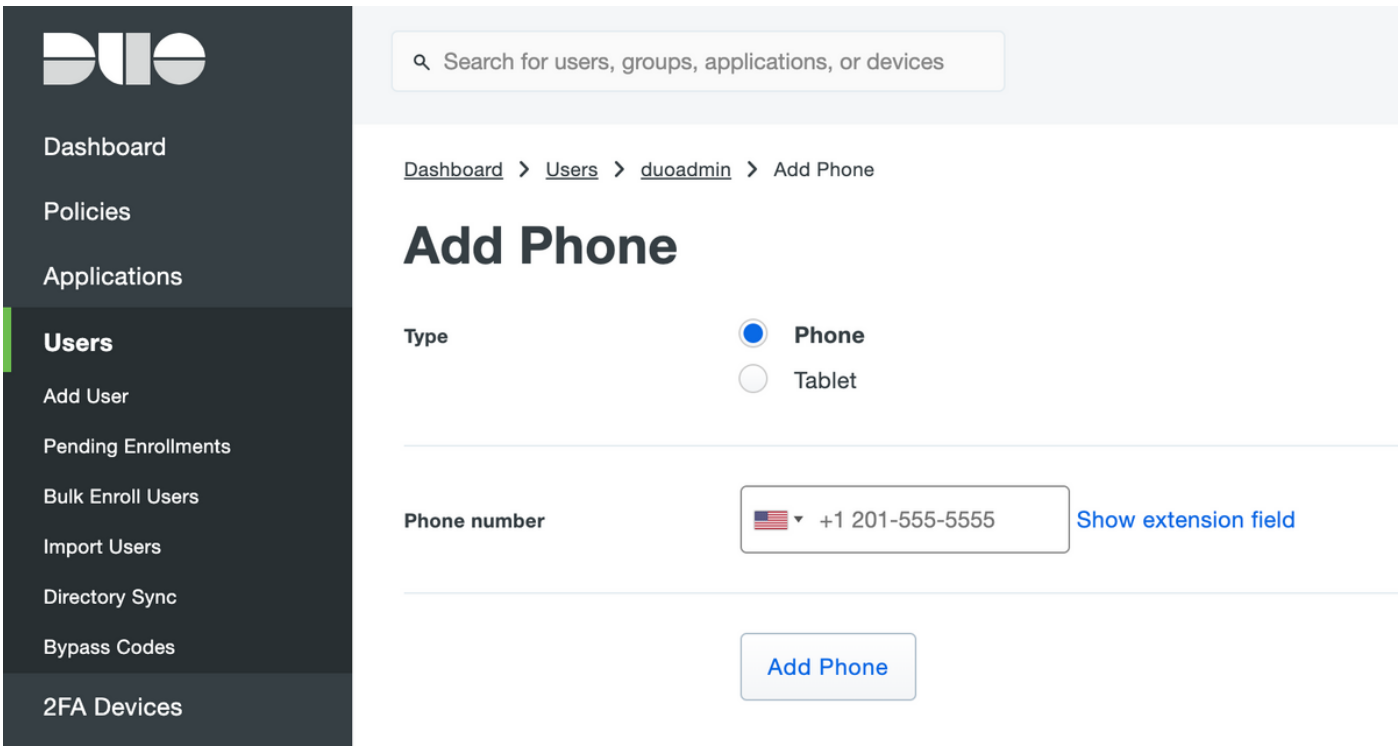
Étape 7. Créez un nom d'utilisateur et activez Duo Mobile sur le périphérique final : https://duo.com/docs/administration-users#creating-users-manually

Ajouter un utilisateur sur le panneau d'administration Duo. Accédez à **Utilisateurs > ajouter des utilisateurs,** comme indiqué dans l'image :

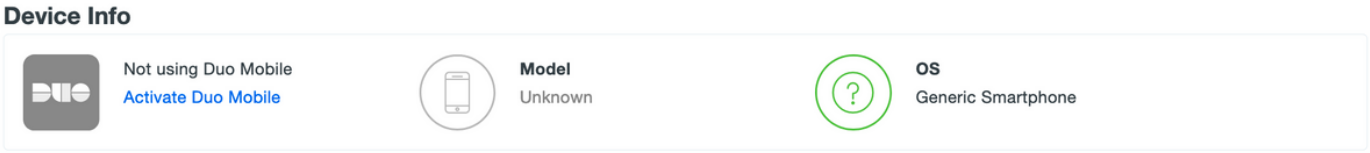


Vérifiez que l'application Duo est installée sur le téléphone de l'utilisateur final.

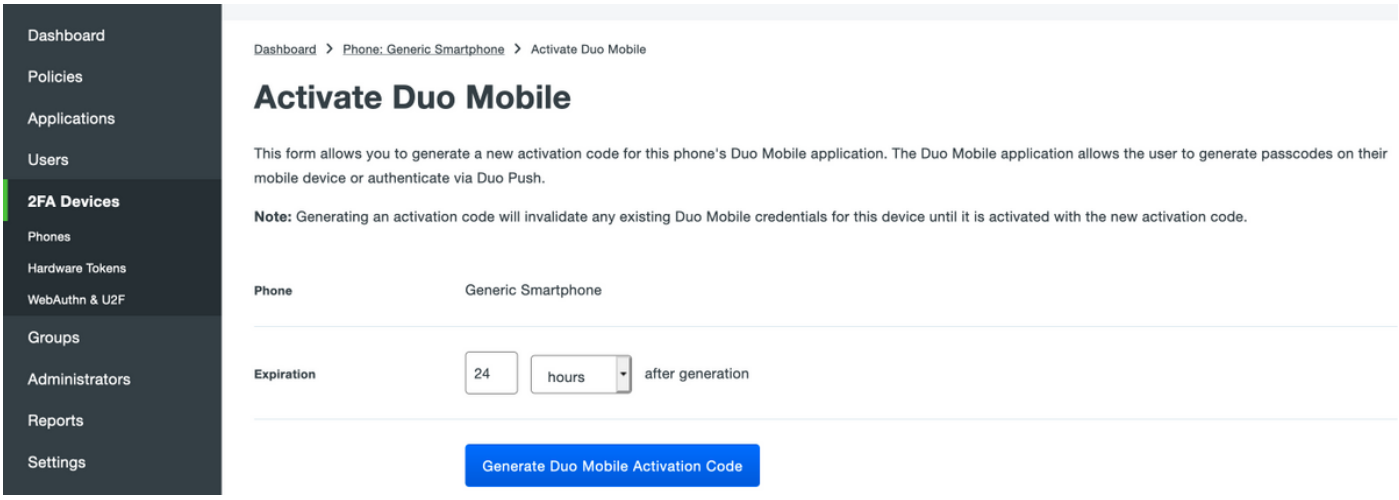




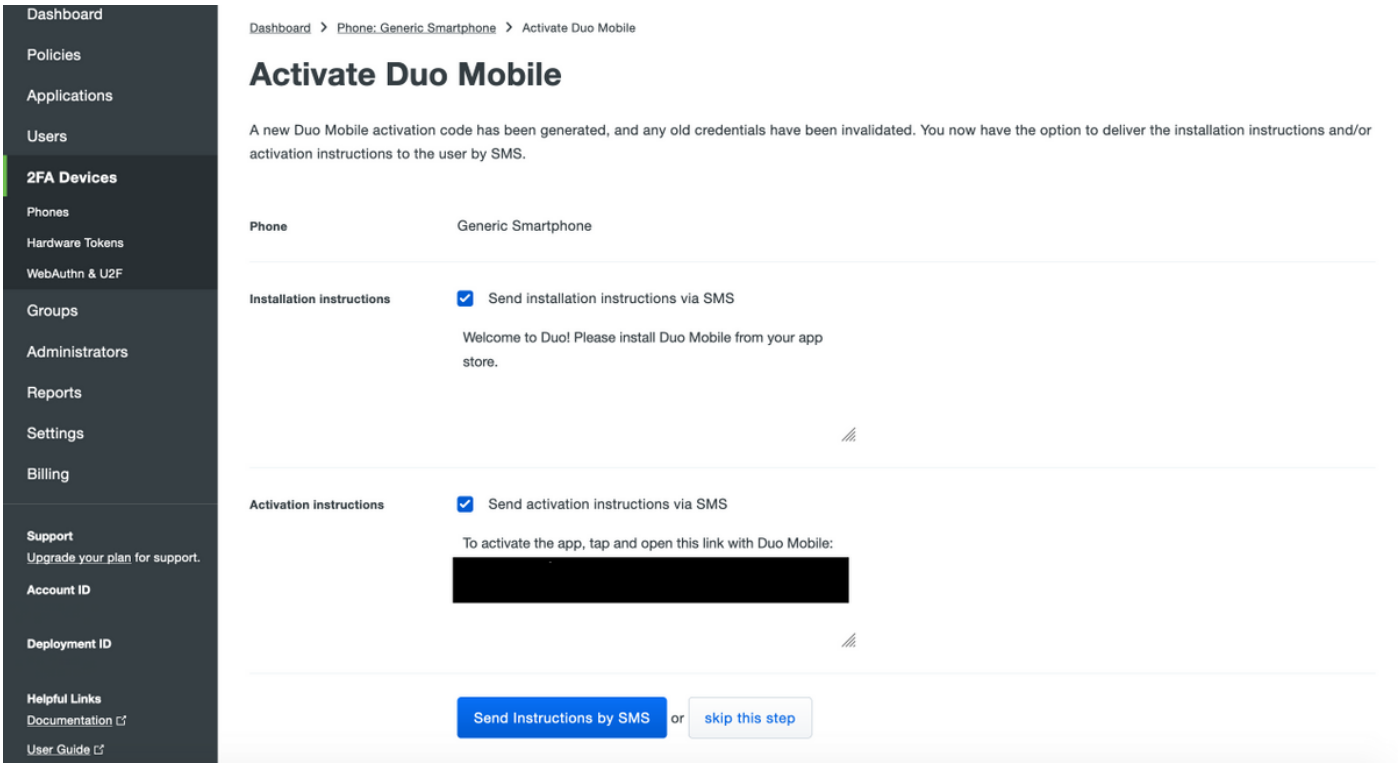
Sélectionnez **Activate Duo Mobile,** comme indiqué dans l'image :



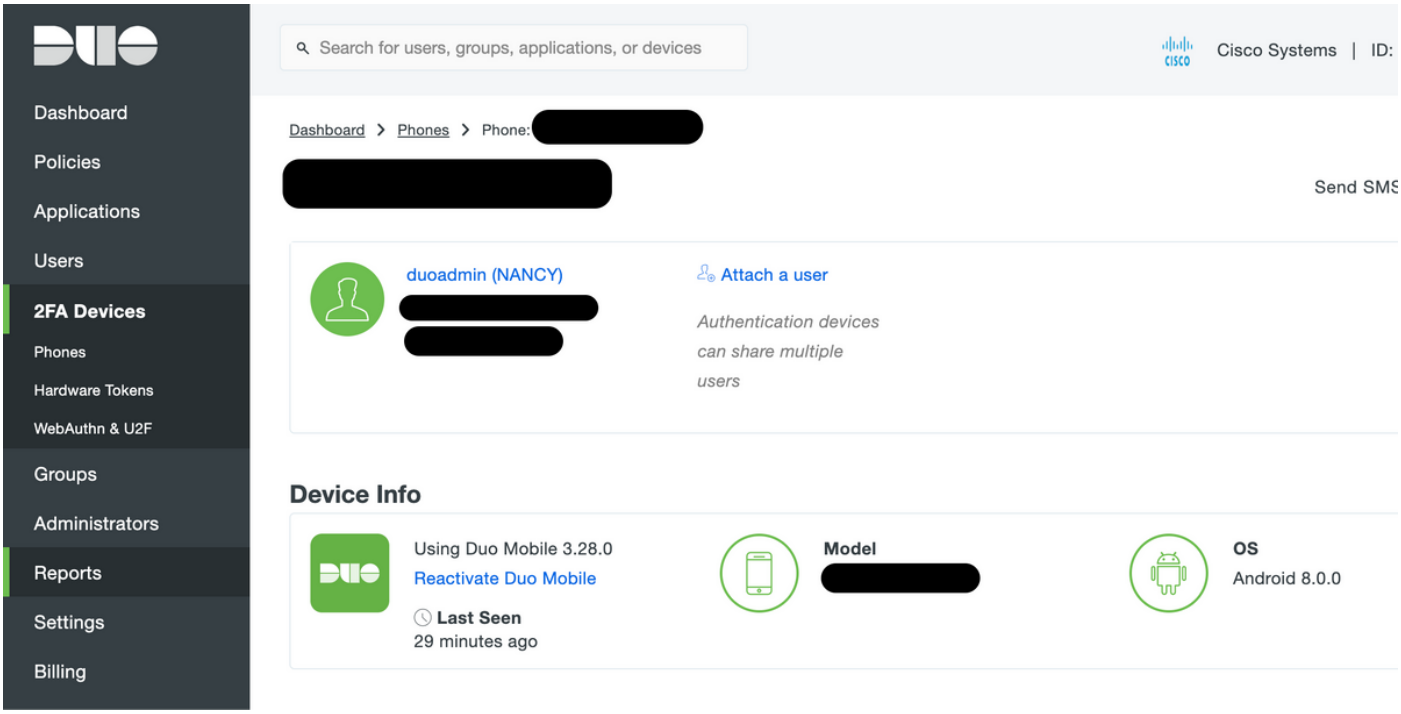
Sélectionnez **Generate Duo Mobile Activation Code,** comme indiqué dans l'image :



Sélectionnez **Envoyer des instructions par SMS,** comme indiqué dans l'image :



Cliquez sur le lien dans le SMS, et l'application Duo est associée au compte d'utilisateur dans la section **Informations sur le périphérique**, comme illustré dans l'image :

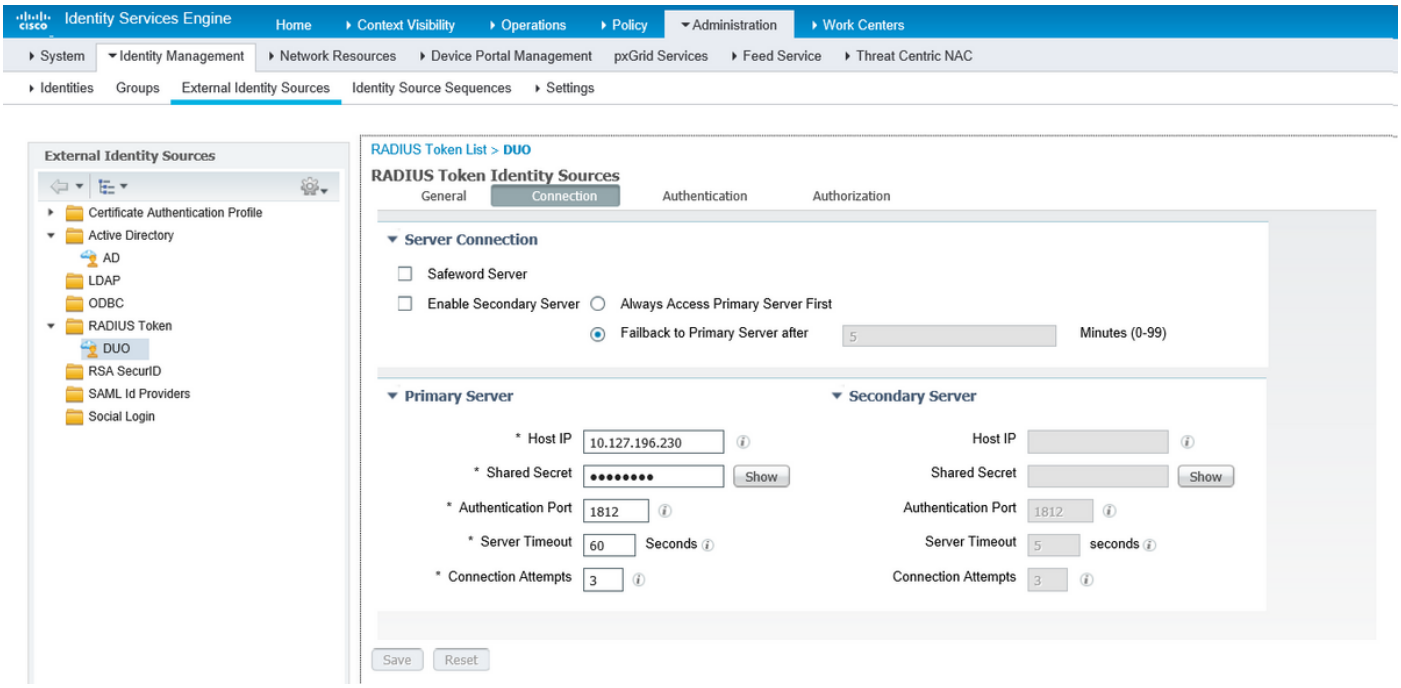


Configuration ISE

Étape 1. Intégrez ISE au proxy Auth Duo.

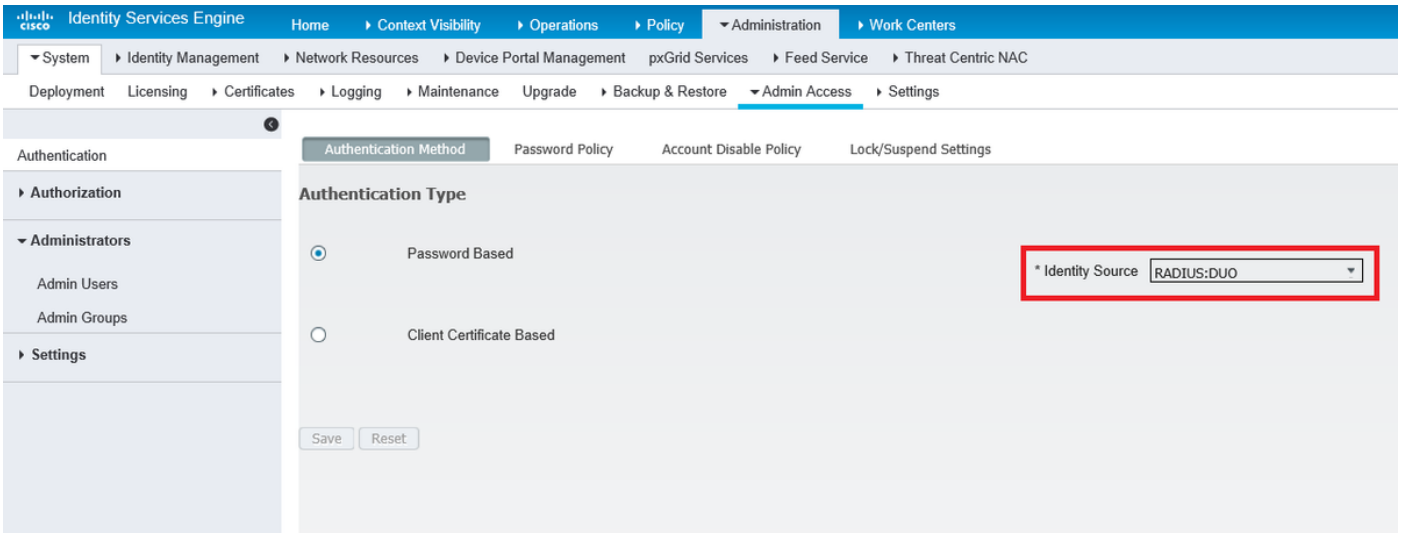
Accédez à **Administration > Identity Management > External Identity Sources > RADIUS Token**, cliquez sur **Add** pour ajouter un nouveau serveur RADIUS Token. Définissez le nom du serveur dans l'onglet Général, l'adresse IP et la clé partagée dans l'onglet Connexion, comme illustré dans l'image :

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

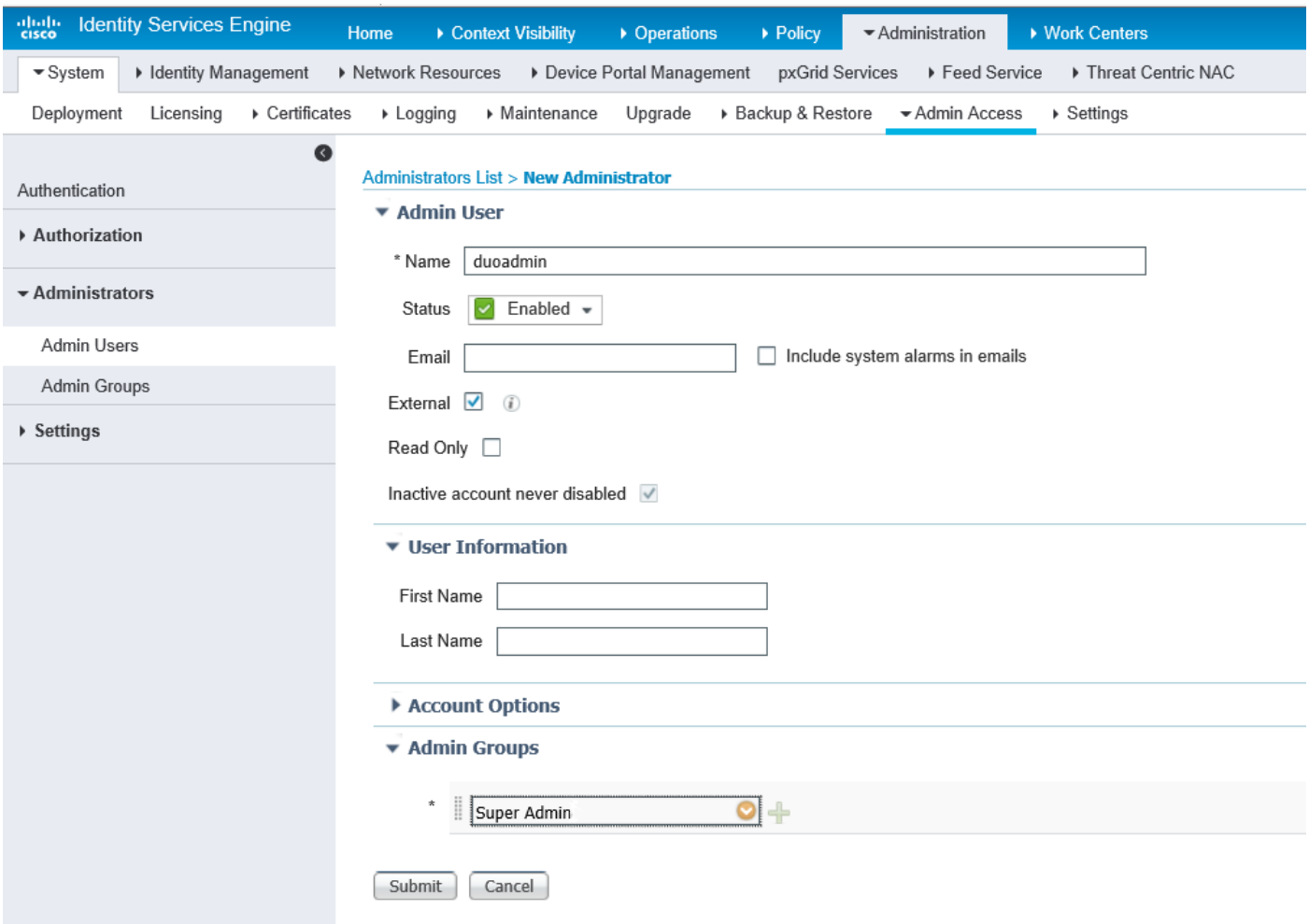


Étape2. Naviguez jusqu'à **Administration > System > Admin Access > Authentication > Authentication Method** et **sélectionnez** le serveur de jetons RADIUS précédemment configuré

comme source d'identité, comme illustré dans l'image :



Étape 3. Accédez à **Administration > System > Admin Access > Administrators > Admin Users** and Create an admin user as External et fournissez le privilège super admin, comme illustré dans l'image :

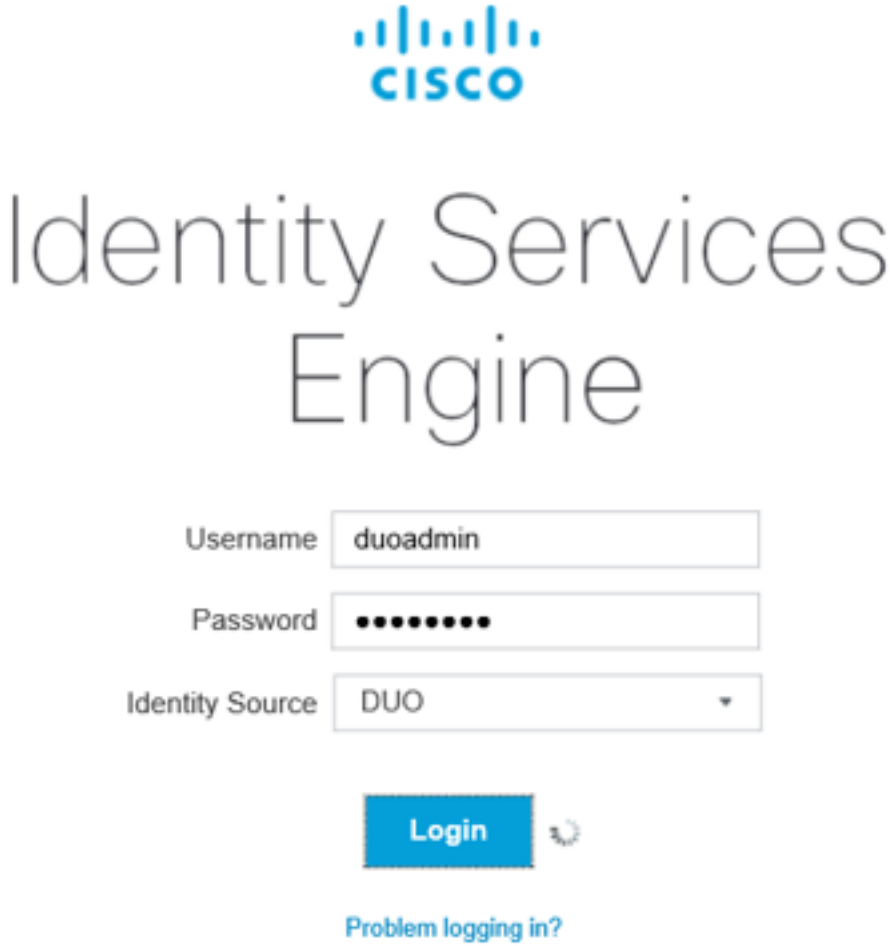


Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Ouvrez l'interface utilisateur de l'ISE, sélectionnez RADIUS Token Server en tant que source

d'identité et connectez-vous avec l'utilisateur admin.



Dépannage

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

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

Les journaux se trouvent à l'emplacement suivant :

C:\Program Files (x86)\Duo Security Authentication Proxy\log

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

Des extraits de journaux du proxy Auth Duo reçoivent une demande d'ISE et l'envoient à Duo Cloud.

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

Les extraits de journaux du proxy Auth Duo ne peuvent pas atteindre Duo Cloud.

```
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.duosecurity.com',)

2019-08-19T04:59:37-0700 [-] (('10.127.196.189', 62001), duoadmin, 3): Failmode Secure - Denied
Duo login on preauth failure
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 via DUO
- Support et documentation techniques - Cisco Systems