Configuration de l'authentification à deux facteurs Duo pour l'accès à la gestion FMC

Table des matières

Introduction

Ce document décrit les étapes requises pour configurer l'authentification à deux facteurs externe pour l'accès à la gestion sur Firepower Management Center (FMC).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration d'objets Firepower Management Center (FMC)
- Administration ISE (Identity Services Engine)

Composants utilisés

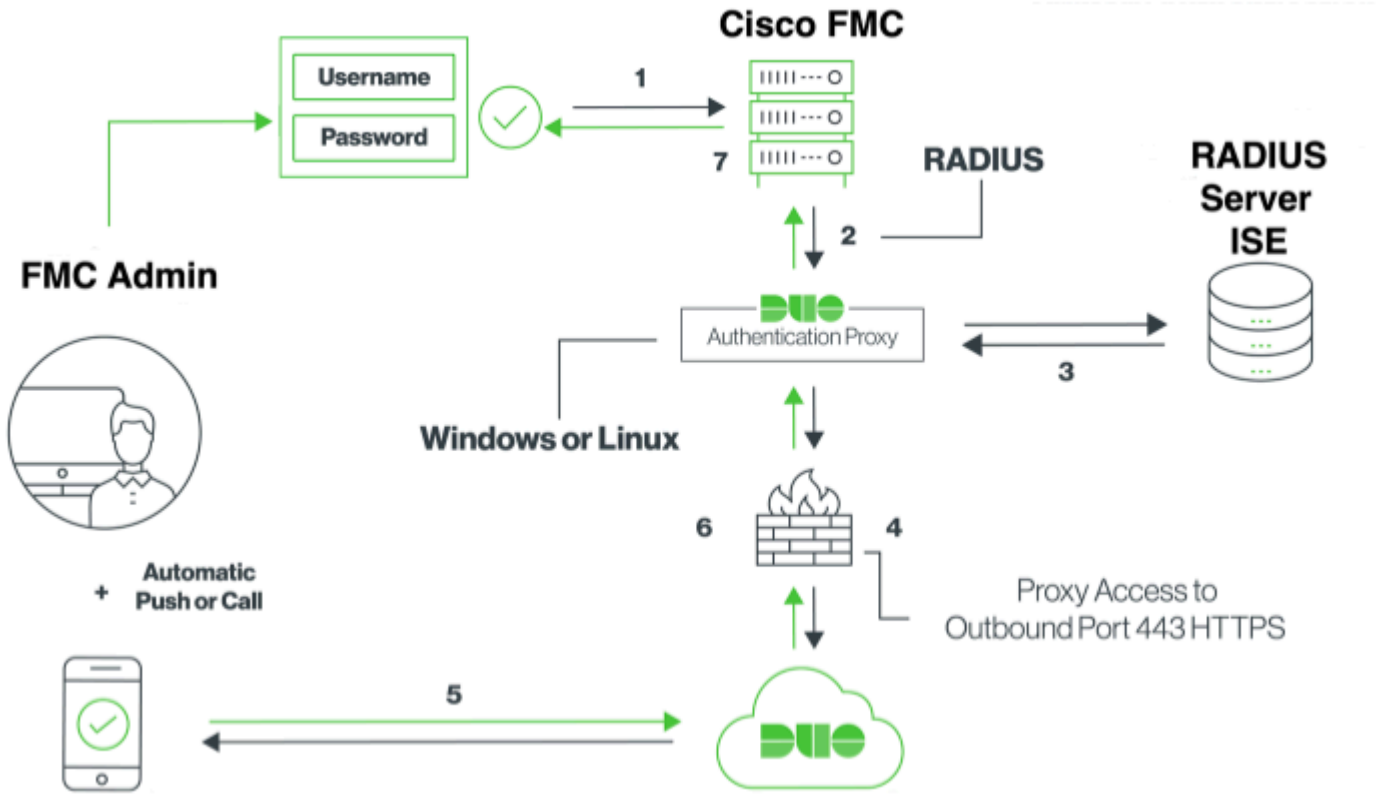
- Cisco Firepower Management Center (FMC) version 6.3.0
- Cisco Identity Services Engine (ISE) exécutant la version 2.6.0.156
- Version prise en charge de Windows (https://duo.com/docs/authproxy-reference#new-proxy-install) avec connectivité à FMC, ISE et Internet pour servir de serveur proxy d'authentification Duo
- Machine Windows afin d'accéder à FMC, ISE et Duo Administration Portal
- Compte Web 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 lâ€™incidence possible des commandes.

Informations générales

L'administrateur FMC s'authentifie auprès du serveur ISE et une authentification supplémentaire sous la forme d'une notification de transmission est envoyée par le serveur proxy d'authentification duo au périphérique mobile de l'administrateur.

Flux d'authentification



Flux d'authentification expliqué

1. Authentification principale initiée vers Cisco FMC.
2. Cisco FMC envoie une demande dâ€™authentification au proxy dâ€™authentification duo.
3. L'authentification principale doit utiliser 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 la réponse d'authentification.
7. L'accès à l'interface utilisateur graphique Cisco FMC est autorisé.

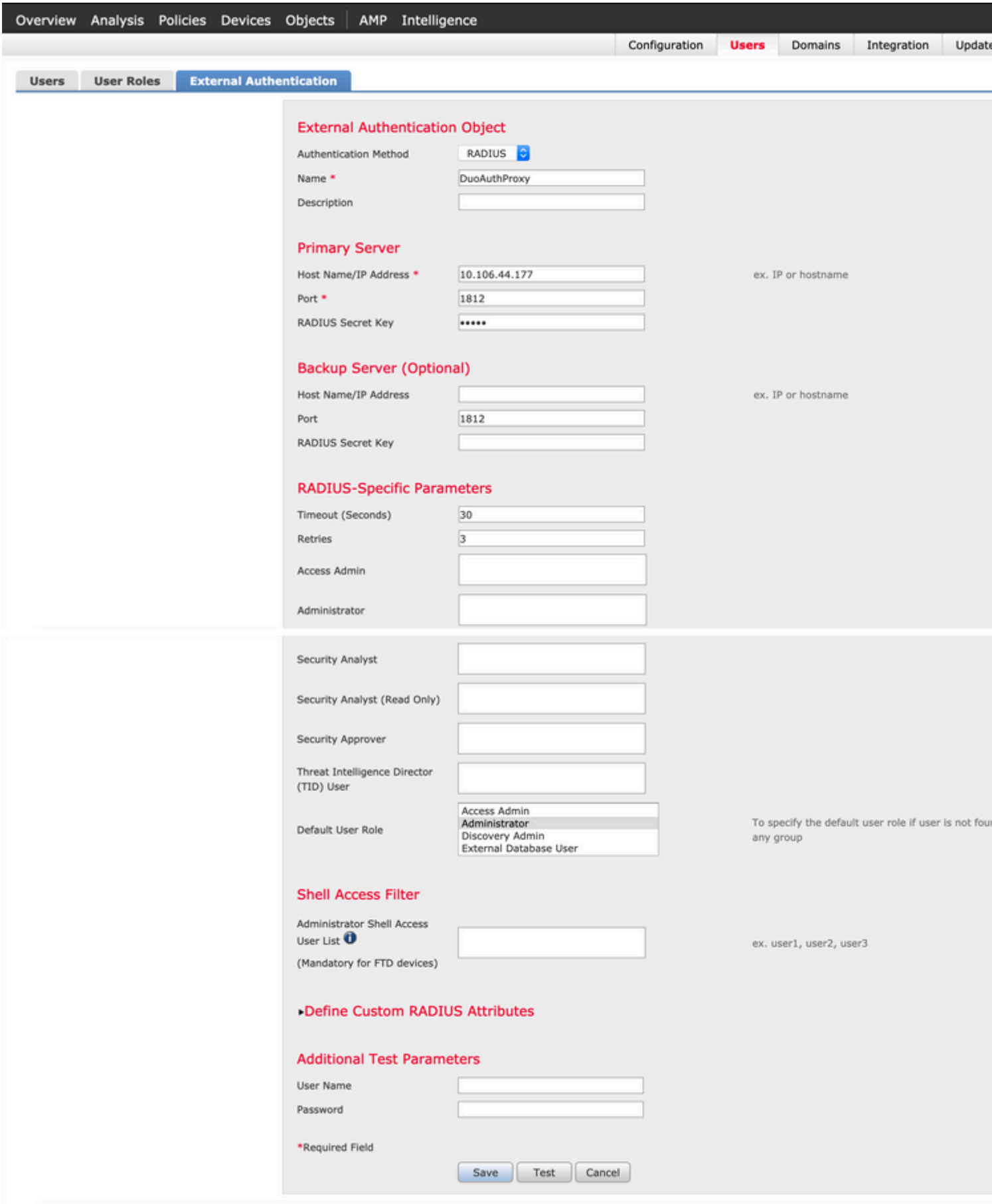
Configurer

Pour terminer la configuration, tenez compte des sections suivantes :

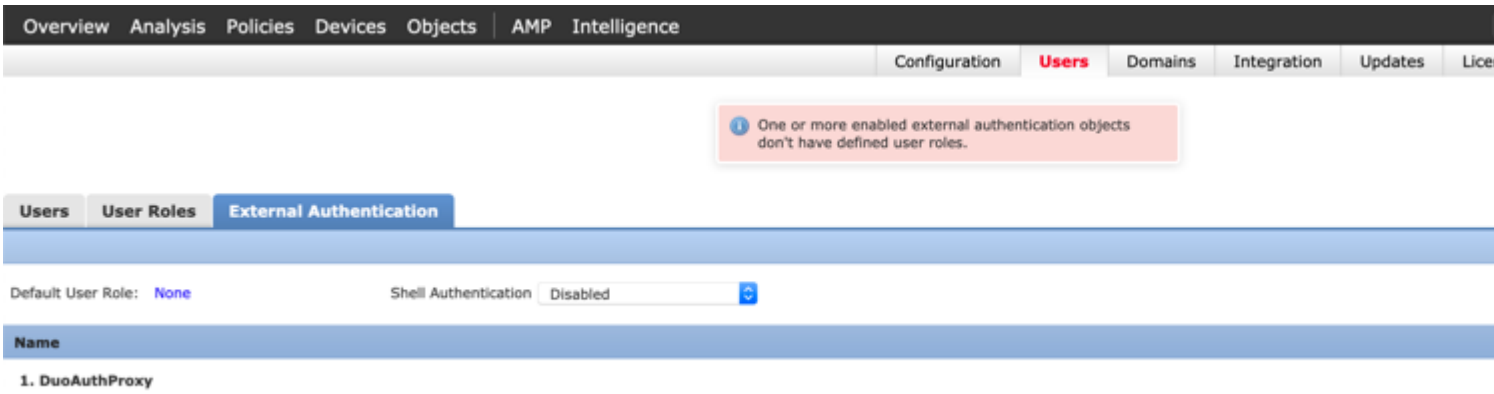
Étapes de configuration sur FMC

Étape 1. Accédez à System > Users > External Authentication. Créez un objet d'authentification externe et définissez la méthode d'authentification sur RADIUS. Assurez-vous que l'administrateur est sélectionné sous Rôle d'utilisateur par défaut, comme indiqué dans l'image :

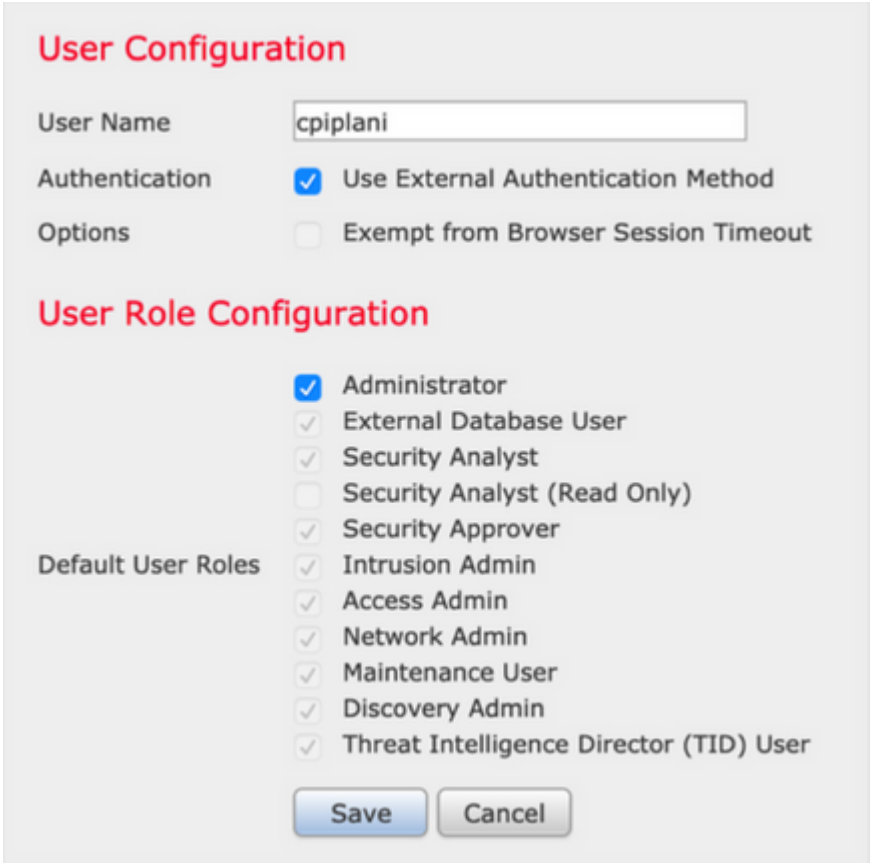
Remarque : 10.106.44.177 est l'exemple d'adresse IP du serveur proxy d'authentification duo.



Cliquez sur **Enregistrer** et **appliquer**. Ignorez l'avertissement comme indiqué dans l'image :



Étape 2. Accédez à **Système > Utilisateurs > Utilisateurs**. Créez un utilisateur et cochez la case Authentication Method as External (Méthode d'authentification externe), comme indiqué dans l'image :



Étape 1. Téléchargez et installez Duo Authentication Proxy Server.

Connectez-vous à l'ordinateur Windows et installez le serveur proxy d'authentification Duo

Il est recommandé d'utiliser un système avec au moins 1 processeur, 200 Mo d'espace disque et 4 Go de RAM

> Remarque : cette machine doit avoir accès à FMC, au serveur RADIUS (ISE dans notre cas) et au cloud Duo (Internet)

Étape 2. Configurez le fichier **authproxy.cfg**.

Ouvrez ce fichier dans un éditeur de texte tel que Bloc-notes++ ou WordPad.

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

---

Modifiez le fichier **authproxy.cfg** et ajoutez cette configuration :

<#root>

```
[radius_client]
```

host=10.197.223.23 Sample IP Address of the ISE server

secret=cisco

Password configured on the ISE server in order to register the network device

Lâ€™adresse IP du FMC doit être configurée avec la clé secrète RADIUS.

<#root>

```
[radius_server_auto]
ikey=xxxxxxxxxxxxxx
skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=api-xxxxxxxx.duosecurity.com
```

radius_ip_1=10.197.223.76

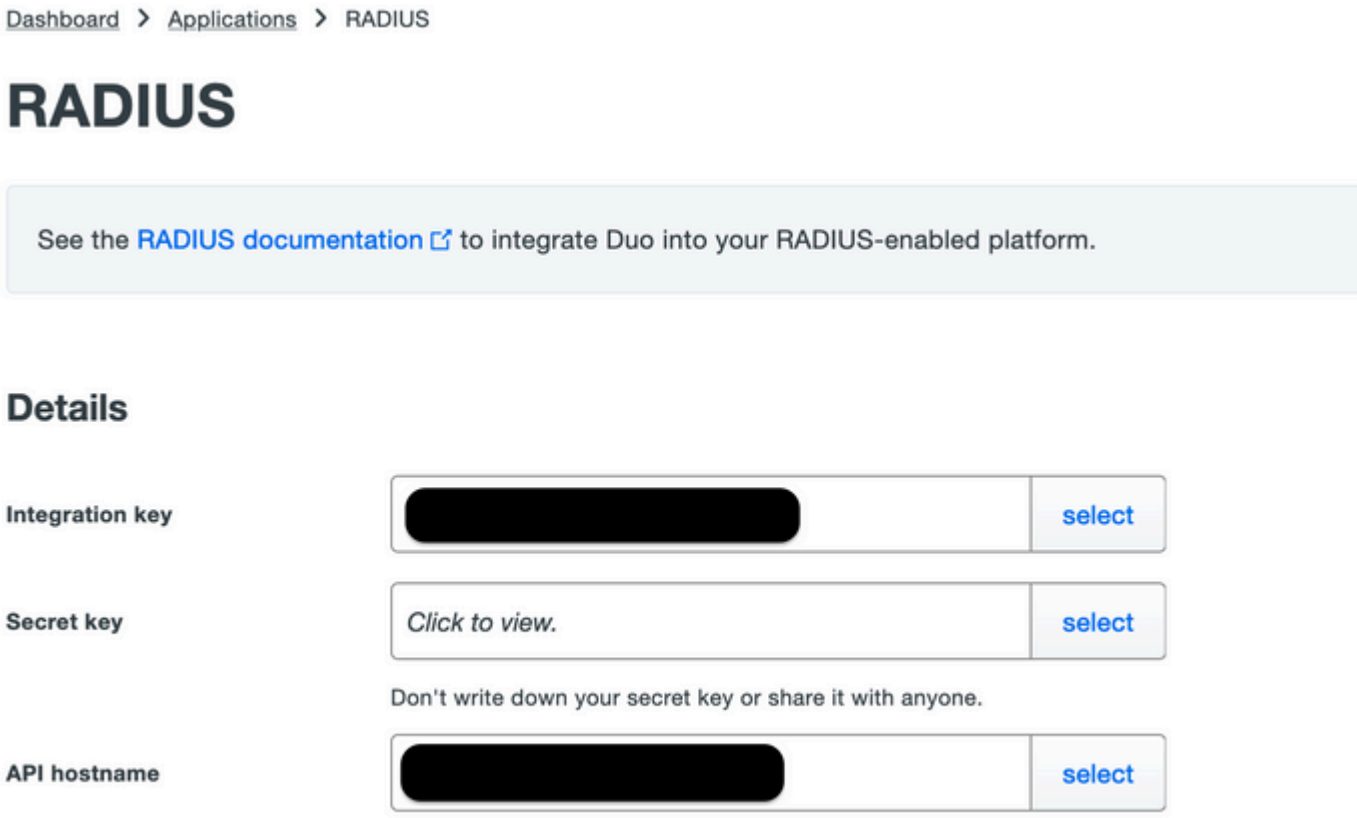
IP of FMC

radius_secret_1=cisco

Radius secret key used on the FMC

```
failmode=safe
client=radius_client
port=1812
api_timeout=
```

Assurez-vous de configurer les paramètres ikey, skey et api_host. Afin d'obtenir ces valeurs, connectez-vous à votre compte Duo (Connexion Admin Duo) et naviguez vers **Applications > Protect an Application**. Sélectionnez ensuite l'application d'authentification RADIUS comme indiqué dans l'image :



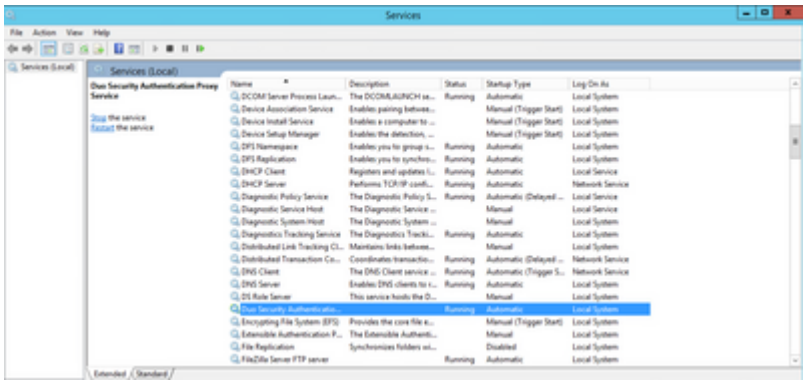
Clé d'intégration = ikey

clé secrète = skey

Nom d'hôte API = api_host

Étape 3. Redémarrez le service proxy d'authentification de sécurité duo. **Enregistrez** le fichier et **redémarrez** le service Duo sur l'ordinateur Windows.

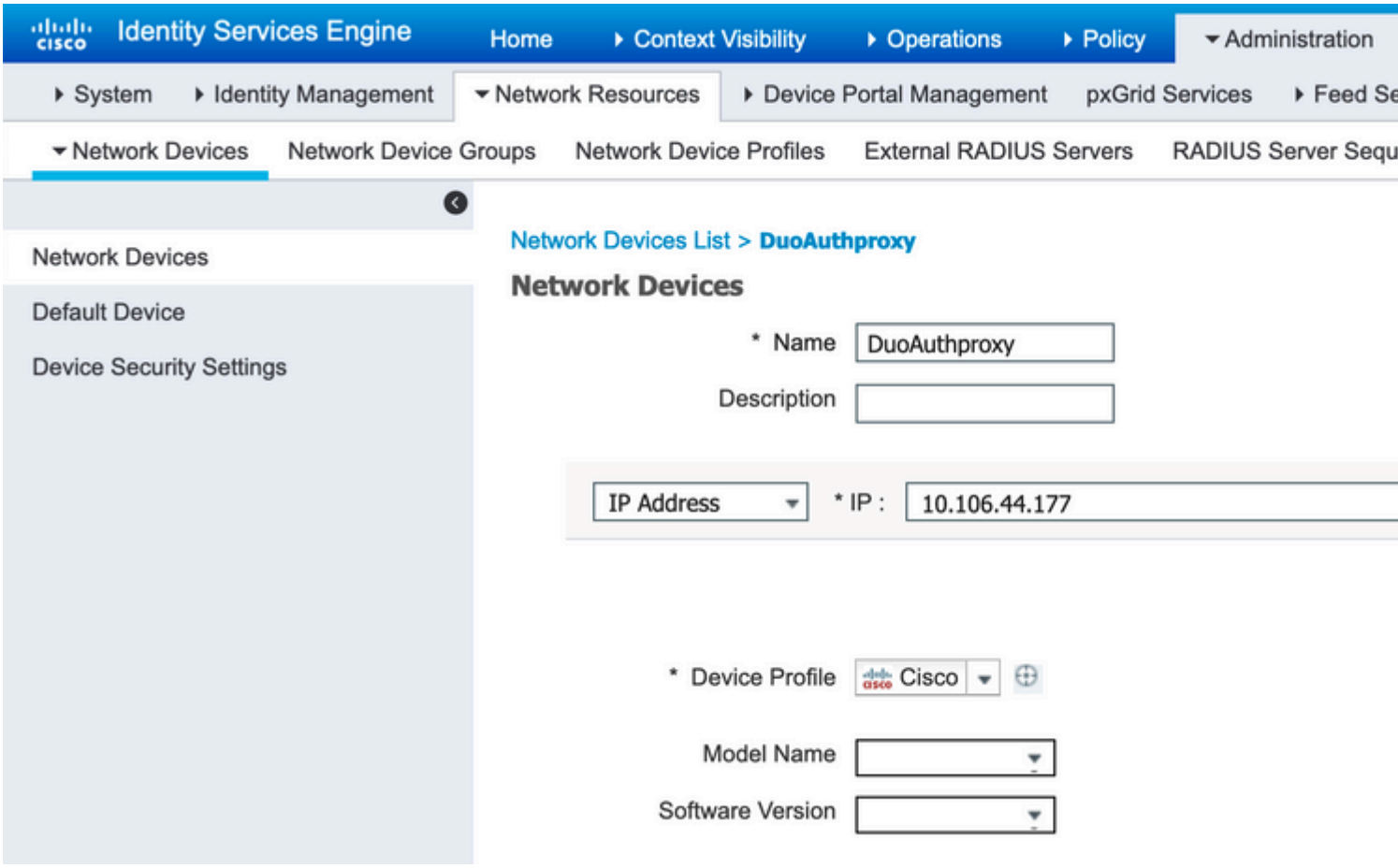
Ouvrez la console des services Windows (services.msc). Recherchez **Duo Security Authentication Proxy Service** dans la liste des services, puis cliquez sur **Restart** comme indiqué dans l'image :



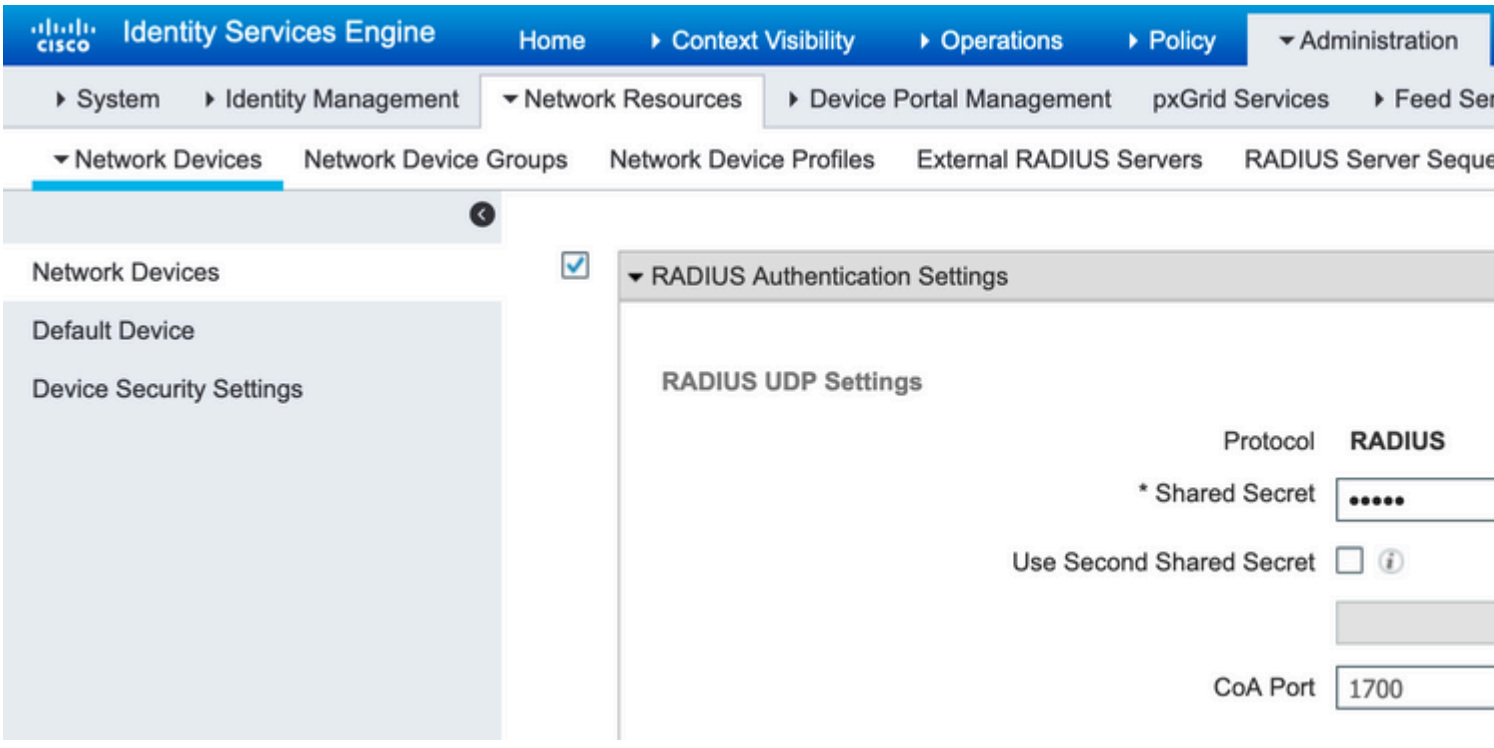
Étapes de configuration sur ISE

Étape 1. Accédez à **Administration > Network Devices,** cliquez sur **Add** afin de configurer le périphérique réseau comme indiqué dans l'image :

Remarque : 10.106.44.177 est l'exemple d'adresse IP du serveur proxy d'authentification duo.

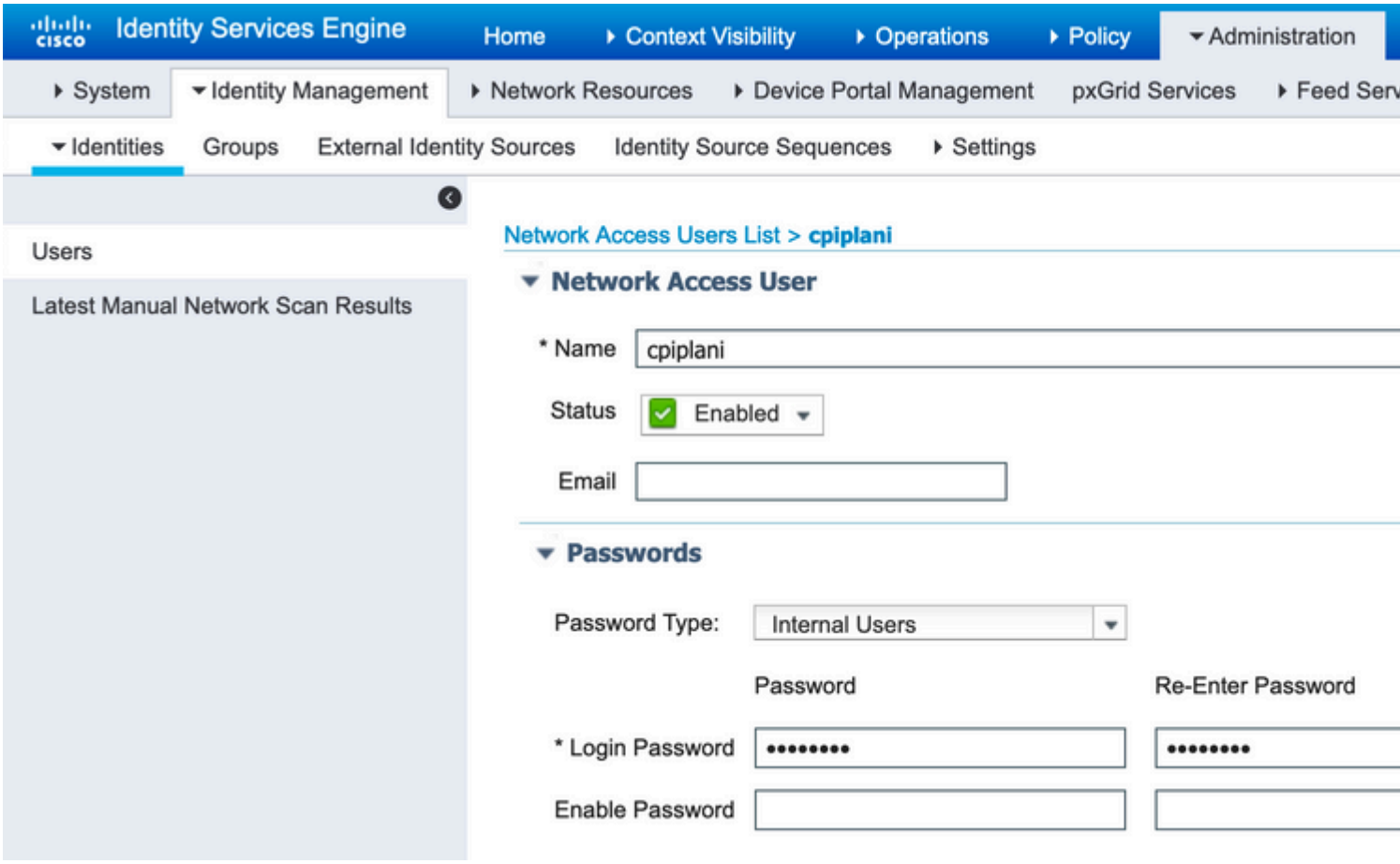


Configurez le **secret partagé** comme indiqué dans le fichier **authproxy.cfg** dans le fichier **secret** comme indiqué dans l'image :



Étape 2. Accédez à Administration > Identities. Cliquez sur **Add** afin de configurer l'utilisateur Identity

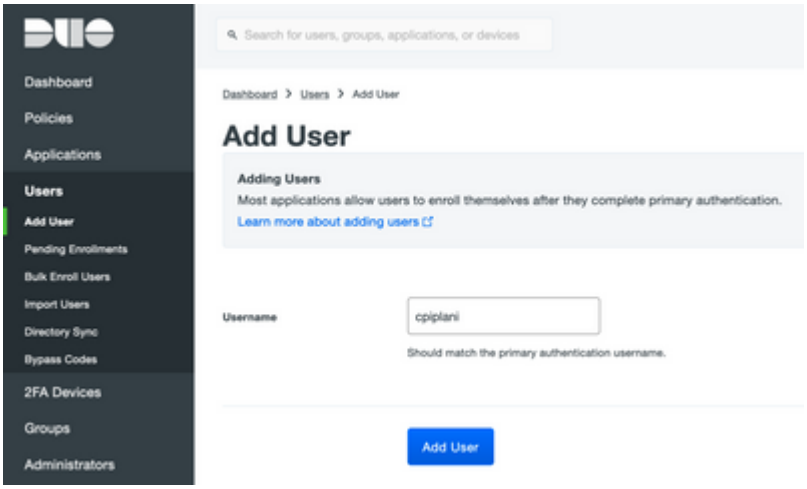
comme indiqué dans l'image :



Étapes de configuration sur le portail Duo Administration

Étape 1. Créez un nom d'utilisateur et activez Duo Mobile sur le périphérique final.

Ajoutez l'utilisateur sur la page Web d'administration du cloud Duo. Accédez à **Users** > **Add users** comme indiqué dans l'image :



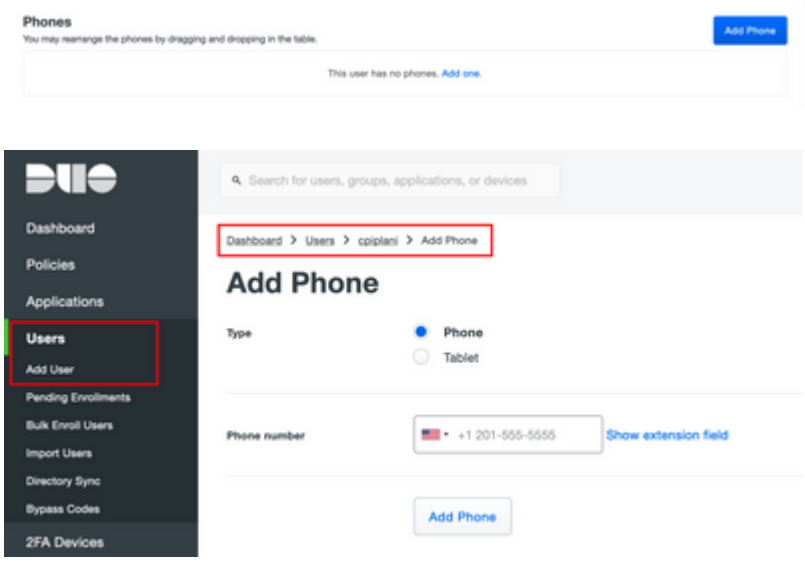
Remarque : vérifiez que l'application Duo est installée sur l'utilisateur final.

[Installation manuelle de l'application Duo pour les périphériques IOS]

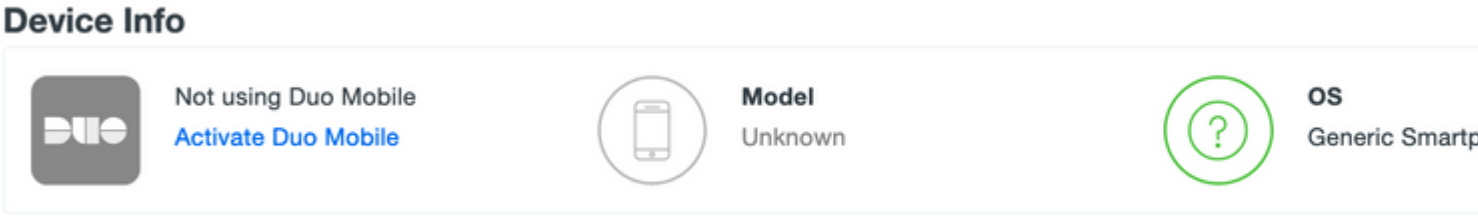
[Installation manuelle de l'application Duo pour les appareils Android]

Étape 2. Génération automatique de code.

Ajoutez le numéro de téléphone de l'utilisateur comme illustré dans l'image :



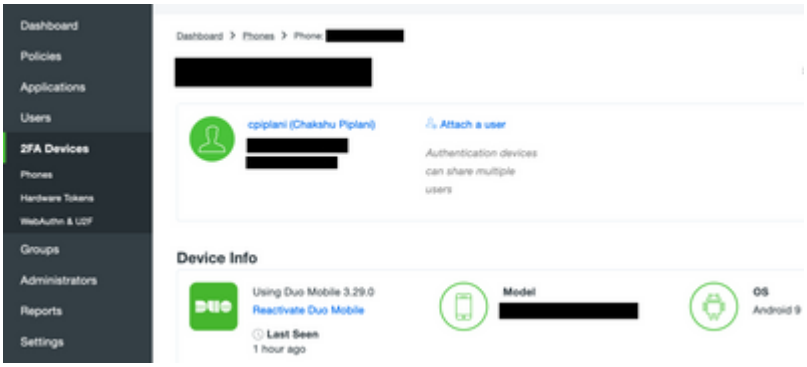
Choisissez **Activate Duo Mobile** comme indiqué dans l'image :



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

Choisissez **Send Instructions by SMS** comme indiqué dans l'image :

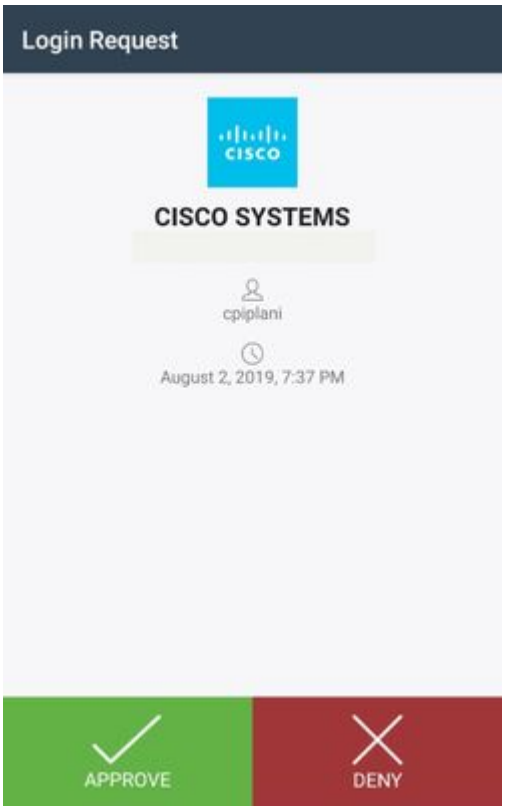
Cliquez sur le lien dans le SMS, et l'application Duo est liée au compte d'utilisateur dans la section Device Info, comme le montre l'image :



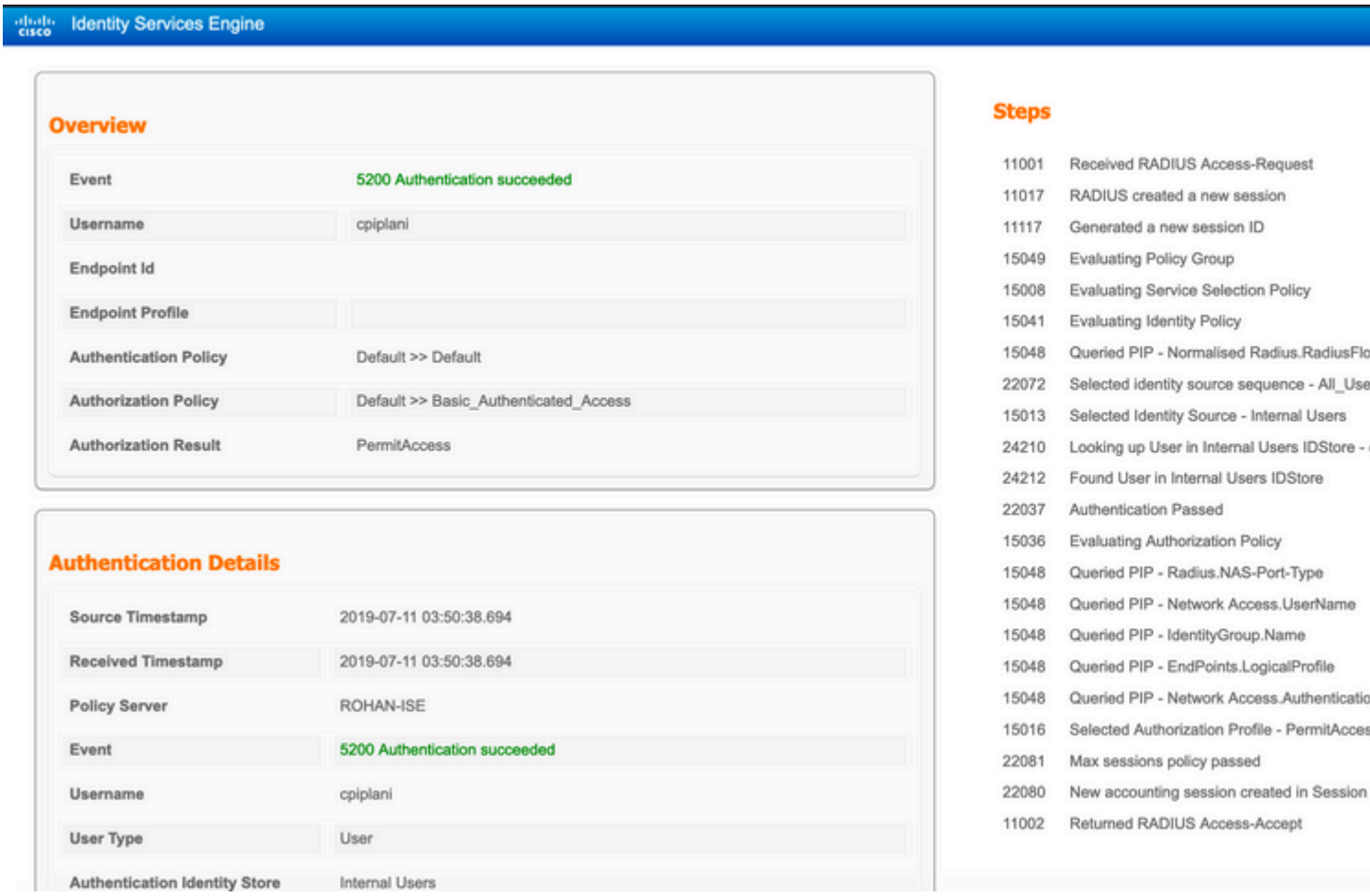
Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Connectez-vous au FMC à l'aide de vos identifiants d'utilisateur qui ont été ajoutés sur la page d'identité de l'utilisateur ISE. Vous devez obtenir une notification PUSH Duo sur votre terminal pour l'authentification à deux facteurs (2FA), l'approuver et FMC se connecterait comme indiqué dans l'image :



Sur le serveur ISE, accédez à **Operations > RADIUS > Live Logs**. Recherchez le nom d'utilisateur utilisé pour l'authentification sur FMC et sélectionnez le rapport d'authentification détaillé sous la colonne Détail. Dans cette section, vous devez vérifier si l'authentification a réussi, comme indiqué dans l'image :



Dépannage

Cette section fournit les informations que vous pouvez utiliser afin de dépanner votre configuration.

- Vérifiez les débogages sur Duo Authentication Proxy Server. Les journaux se trouvent à l'emplacement suivant :

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

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

Enregistre les extraits de journal lorsque des informations d'identification incorrectes sont saisies et que l'authentification est rejetée par le serveur ISE.

<#root>

2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] Sending request from

10.197.223.76

to radius_server_auto

10.197.223.76 is the IP of the FMC

2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] Received new request id 4 from ('10.197.223.76', 34524
2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] (('10.197.223.76', 34524), 4):

login attempt for username u'cpiplani'

2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] Sending request for user u'cpiplani' to ('10.197.223.2
2019-08-04T18:54:17+0530 [RadiusClient (UDP)]

Got response

for id 199 from ('

10.197.223.23

', 1812);

code 3 10.197.223.23 is the IP of the ISE Server.

2019-08-04T18:54:17+0530 [RadiusClient (UDP)] (('10.197.223.76', 34524), 4): Primary credentials rejecte
2019-08-04T18:54:17+0530 [RadiusClient (UDP)] (('10.197.223.76', 34524), 4):

Returning response code 3: AccessReject

2019-08-04T18:54:17+0530 [RadiusClient (UDP)] (('10.197.223.76', 34524), 4): Sending response

- Sur ISE, accédez à **Operations > RADIUS > Live Logs** pour vérifier les détails de l'authentification.

Consignez les extraits d'authentification réussie avec ISE et Duo :

<#root>

2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] Sending request from

10.197.223.76

```
 to radius_server_auto
2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] Received new request id 5 from ('10.197.223.76', 34095
2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] (('10.197.223.76', 34095), 5): login attempt for usern
2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] Sending request for user u'cpiplani' to ('10.197.223.2
2019-08-04T18:56:16+0530 [RadiusClient (UDP)] Got response for id 137 from ('
```

10.197.223.23

```
', 1812);
```

code 2 <<<< At this point we have got successful authentication from ISE Server.

```
2019-08-04T18:56:16+0530 [RadiusClient (UDP)] http POST to https://api-f754c261.duosecurity.com:443/rest
2019-08-04T18:56:16+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <_DuoHTTPCl
2019-08-04T18:56:17+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5): G
2019-08-04T18:56:17+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] Invalid ip. Ip was None
2019-08-04T18:56:17+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] http POST to https://api-f754c26
2019-08-04T18:56:17+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <_DuoHTTPCl
2019-08-04T18:56:17+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_DuoHTTPCl
2019-08-04T18:56:30+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5):
```

Duo authentication returned 'allow': 'Success. Logging you in...

```
'
2019-08-04T18:56:30+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5):
```

Returning response code 2: AccessAccept <<<< At this point, user has hit the approve button

```
2019-08-04T18:56:30+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5): S
2019-08-04T18:56:30+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_DuoHTTPCl
```

Informations connexes

- **Authentification VPN RA utilisant 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.