

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

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Diagramme du réseau](#)

[Configuration](#)

[Configuration duo](#)

[Configuration ISE](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

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

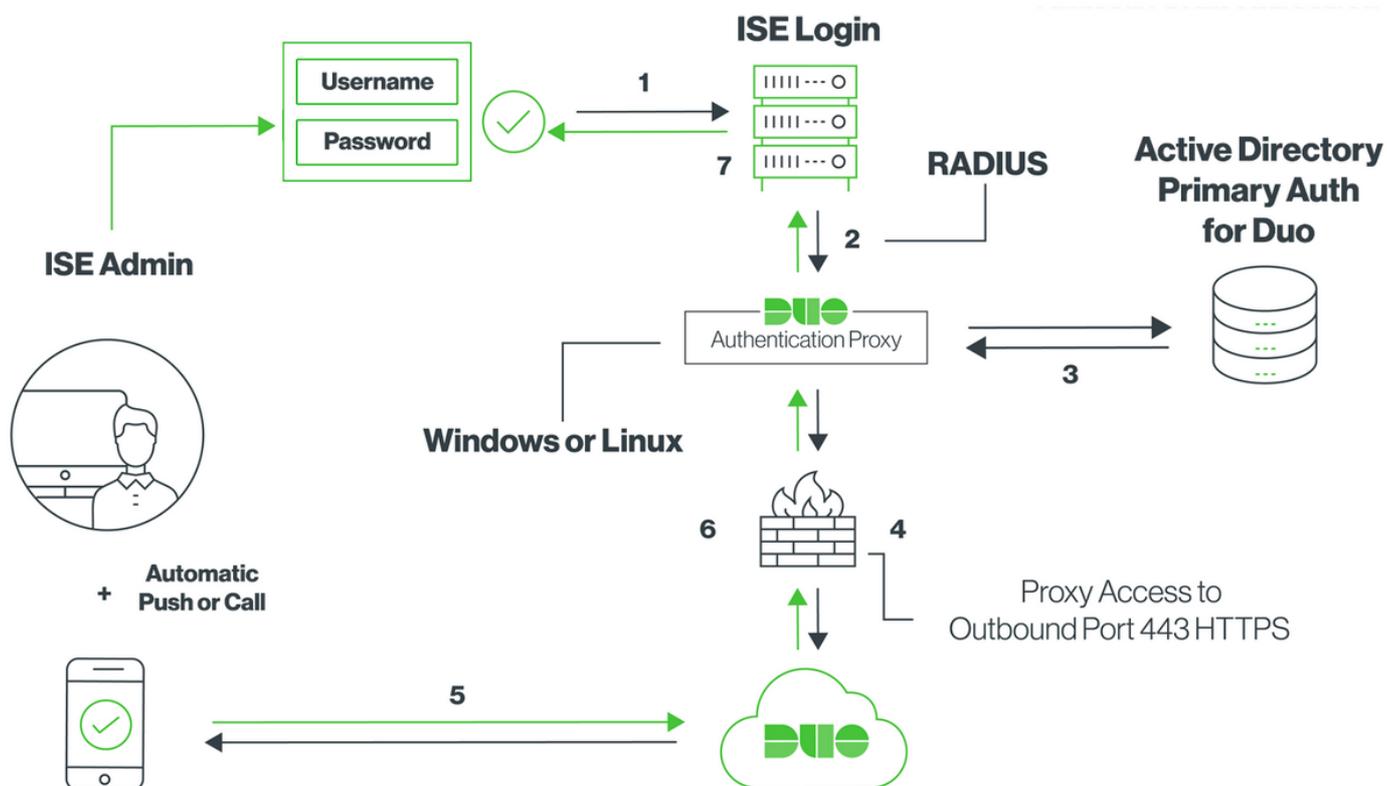
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- 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.

The screenshot shows the Duo Admin console interface. On the left is a dark sidebar with navigation options: Dashboard, Policies, Applications, Users (highlighted), Add User (highlighted), Pending Enrollments, Bulk Enroll Users, Import Users, Directory Sync, Bypass Codes, 2FA Devices, Groups, Administrators, and Reports. The main content area has a search bar at the top with the text "Search for users, groups, applications, or devices". Below it is a breadcrumb trail: Dashboard > Users > Add User. The main heading is "Add User". A section titled "Adding Users" contains the text "Most applications allow users to enroll themselves after they complete primary authentication." and a link "Learn more about adding users". Below this is a form field for "Username" containing the text "duoadmin", with a note below it: "Should match the primary authentication username." At the bottom of the form is a blue button labeled "Add User".

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

The screenshot shows the "Phones" section of the Duo Admin console. The heading is "Phones" and the text below it says "You may rearrange the phones by dragging and dropping in the table." In the top right corner is a blue button labeled "Add Phone". The main content area contains a message: "This user has no phones. [Add one.](#)"

The screenshot shows the Duo Admin console interface for adding a phone. The sidebar is the same as in the previous image, but "Users" is highlighted and "Add User" is selected. The main content area has a search bar at the top with the text "Search for users, groups, applications, or devices". Below it is a breadcrumb trail: Dashboard > Users > duoadmin > Add Phone. The main heading is "Add Phone". The "Type" section has two radio buttons: "Phone" (selected) and "Tablet". Below this is a form field for "Phone number" containing a dropdown menu with the US flag and the text "+1 201-555-5555", followed by a link "Show extension field". At the bottom of the form is a blue button labeled "Add Phone".

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

Device Info



Not using Duo Mobile
[Activate Duo Mobile](#)



Model
Unknown



OS
Generic Smartphone

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

Dashboard > Phone: Generic Smartphone > Activate Duo Mobile

Activate Duo Mobile

This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to generate passcodes on their mobile device or authenticate via Duo Push.

Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.

Phone: Generic Smartphone

Expiration: 24 hours after generation

[Generate Duo Mobile Activation Code](#)

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

Dashboard > Phone: Generic Smartphone > Activate Duo Mobile

Activate Duo Mobile

A new Duo Mobile activation code has been generated, and any old credentials have been invalidated. You now have the option to deliver the installation instructions and/or activation instructions to the user by SMS.

Phone: Generic Smartphone

Installation instructions: Send installation instructions via SMS

Welcome to Duo! Please install Duo Mobile from your app store.

Activation instructions: Send activation instructions via SMS

To activate the app, tap and open this link with Duo Mobile:

[Send Instructions by SMS](#) or [skip this step](#)

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

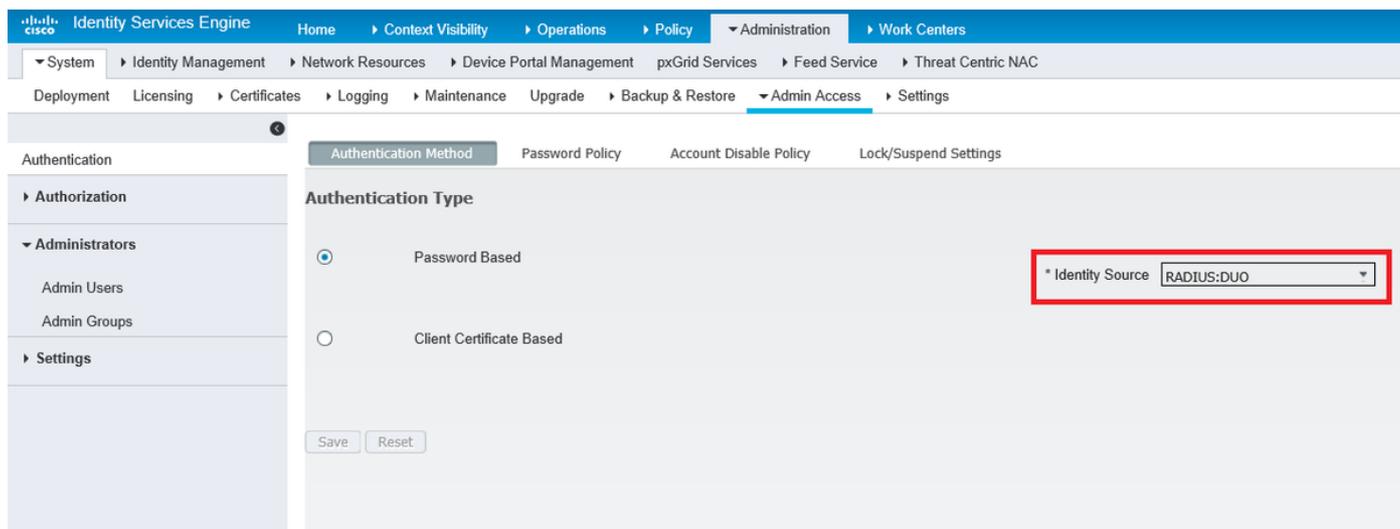
Étape 1. Intégrez ISE au proxy Auth Duo.

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 :

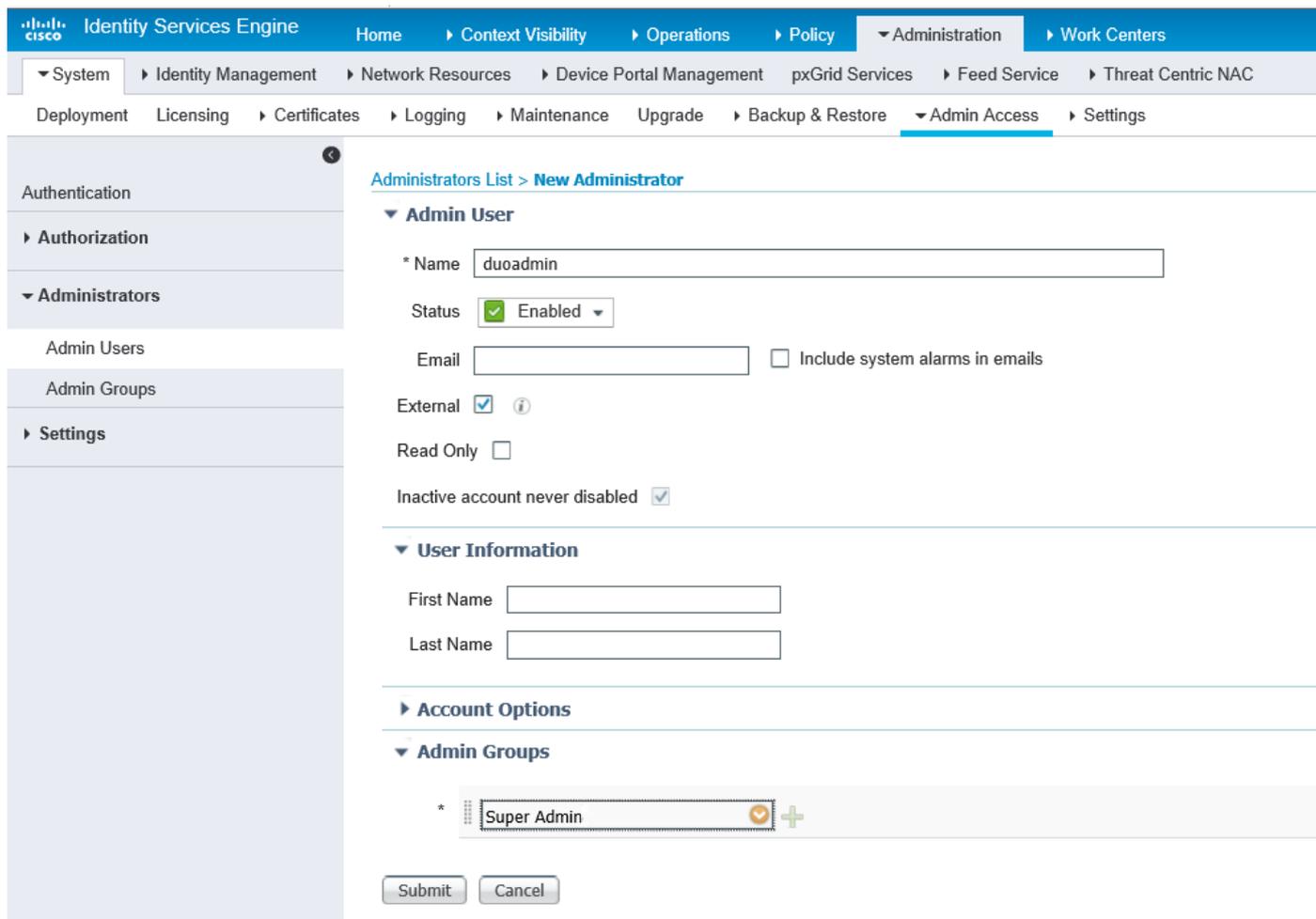
Note: Définissez le délai d'attente du serveur sur 60 secondes afin que les utilisateurs disposent de suffisamment de temps pour agir sur la transmission

Étape 2. 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.



Identity Services Engine

Username

Password

Identity Source



[Problem logging in?](#)

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 getResult

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-xxxxxxxxx.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](#)