Configuración de Duo Two Factor Authentication para el Acceso a la Administración de ISE

Contenido

Introducción

Este documento describe los pasos necesarios para configurar la autenticación externa de dos factores para el acceso de administración de Identity Services Engine (ISE). En este ejemplo, el administrador de ISE se autentica con el servidor de token RADIUS y el servidor de proxy de autenticación Duo envía una autenticación adicional en forma de notificación de inserción al dispositivo móvil del administrador.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Protocolo RADIUS
- Configuración de ISE RADIUS Token Server e Identities

Componentes Utilizados

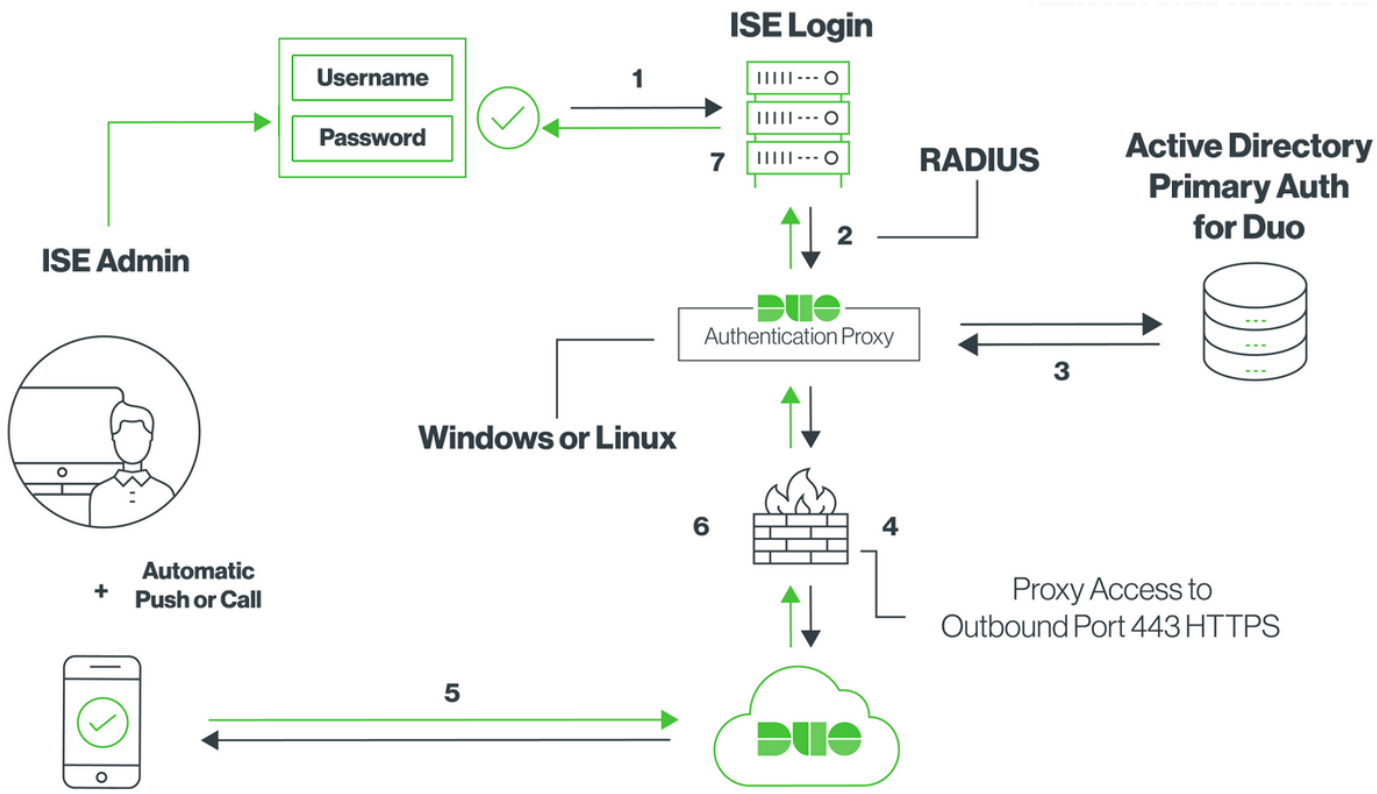
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Identity Services Engine (ISE)
- Active Directory (AD)
- Servidor Proxy de Autenticación Duo
- Duo Cloud Service

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.

Diagrama de la red



Configuración

Configuración Duo

Paso 1. Descargue e instale Duo Authentication Proxy Server en una máquina con Windows o Linux: https://duo.com/docs/ciscoise-radius#install-the-duo-authentication-proxy

> Nota: Esta máquina debe tener acceso a ISE y a la nube Duo (Internet)

Paso 2. Configure el archivo **authproxy.cfg**.

Abra este archivo en un editor de texto como Notepad++ o WordPad.

> Nota: La ubicación predeterminada se encuentra en **C:\Program Files (x86)\Duo Security Authentication Proxy\conf\authproxy.cfg**

Paso 3. Cree una aplicación "Cisco ISE RADIUS" en el Duo Admin Panel: https://duo.com/docs/ciscoise-radius#first-steps

Paso 4. Edite el archivo **authproxy.cfg** y agregue esta configuración.

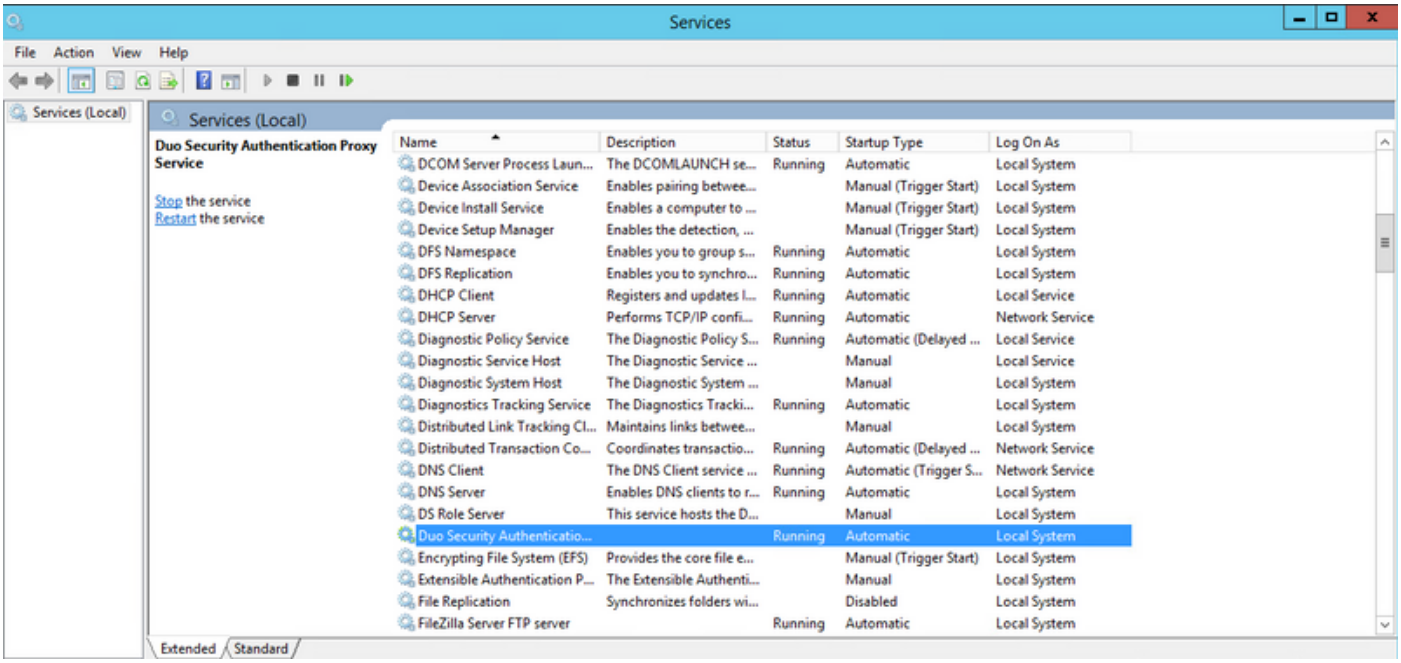
```
ikey= xxxxxxxxxxxxxxxxxxxxxxxx
skey= xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=api-xxxxxxxx.duosecurity.com
radius_ip_1=10.127.196.189                    Sample IP address of the ISE server
radius_secret_1=******
failmode=secure
client=ad_client
port=1812
```

Paso 5. Configure ad_client con los detalles de Active Directory. Duo Auth Proxy utiliza la siguiente información para autenticarse contra AD para la autenticación primaria.

```
[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
```

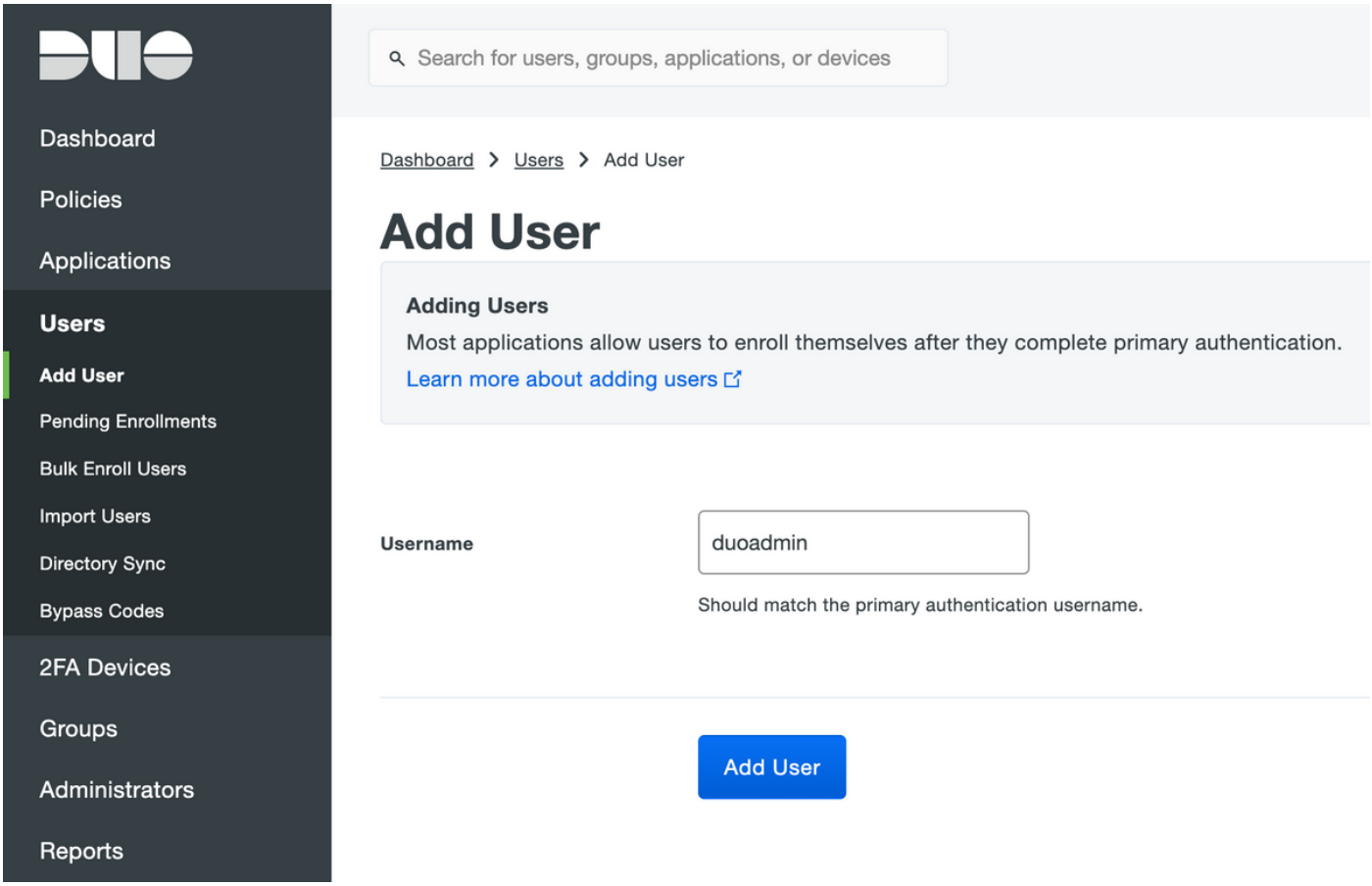
Nota: Si la red requiere una conexión proxy HTTP para el acceso a Internet, agregue los detalles http_proxy en authproxy.cfg.

Paso 6. Reinicie el servicio Duo Security Authentication Proxy. Guarde el archivo y **Reinicie** el **servicio Duo** en el equipo de Windows.Abra la consola de servicios de Windows (services.msc), ubique **Duo Security Authentication Proxy Service** en la lista de servicios y haga clic en **Reiniciar** como se muestra en la imagen:

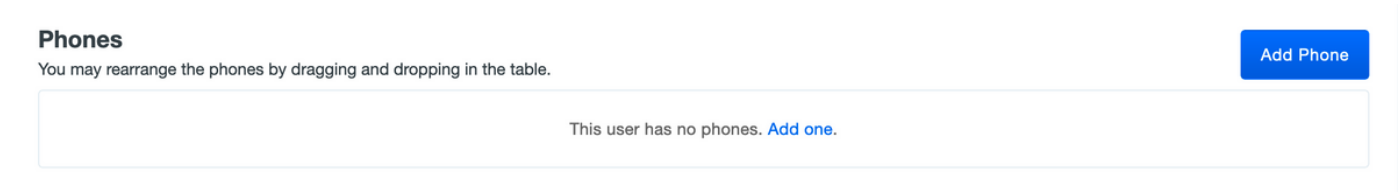


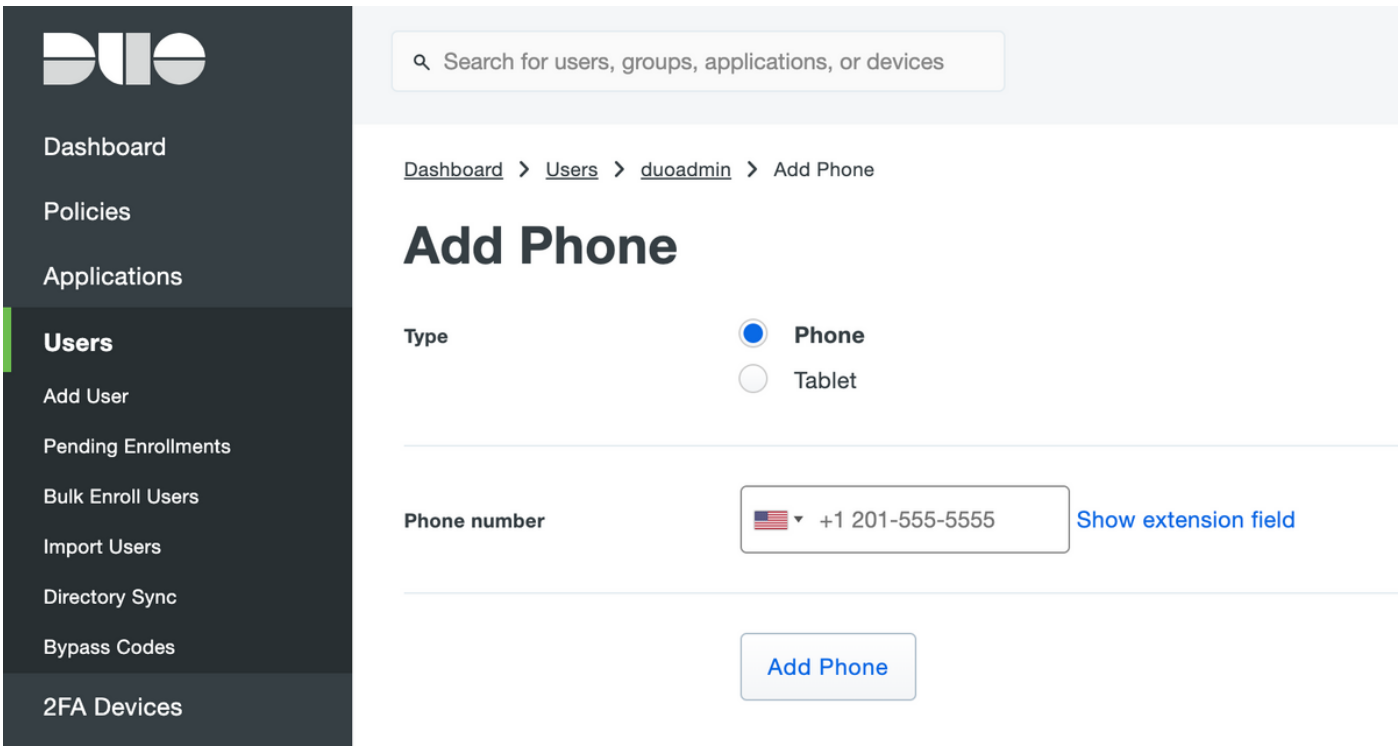
Paso 7. Cree un nombre de usuario y active Duo Mobile en el dispositivo final: https://duo.com/docs/administration-users#creating-users-manually

Agregue el usuario en Duo Admin Panel. Navegue hasta **Usuarios > agregar usuarios,** como se muestra en la imagen:

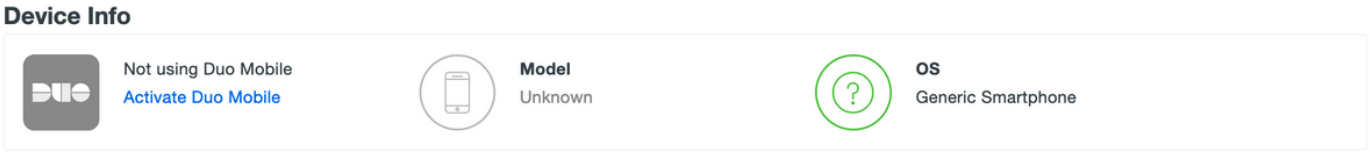


Asegúrese de que el usuario final tiene instalada la aplicación Duo en el teléfono.

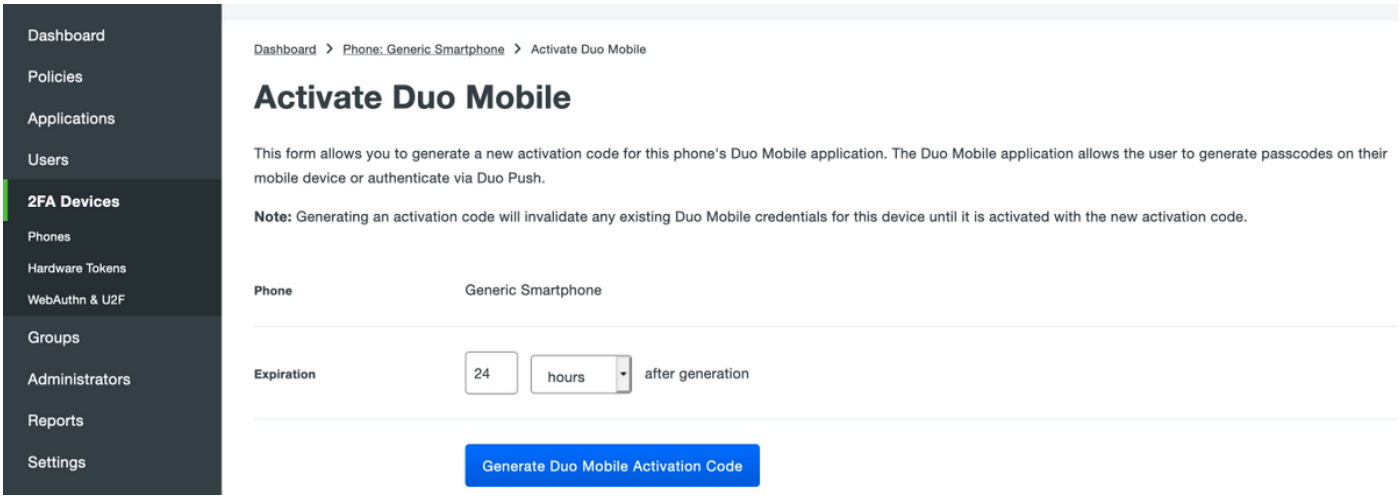




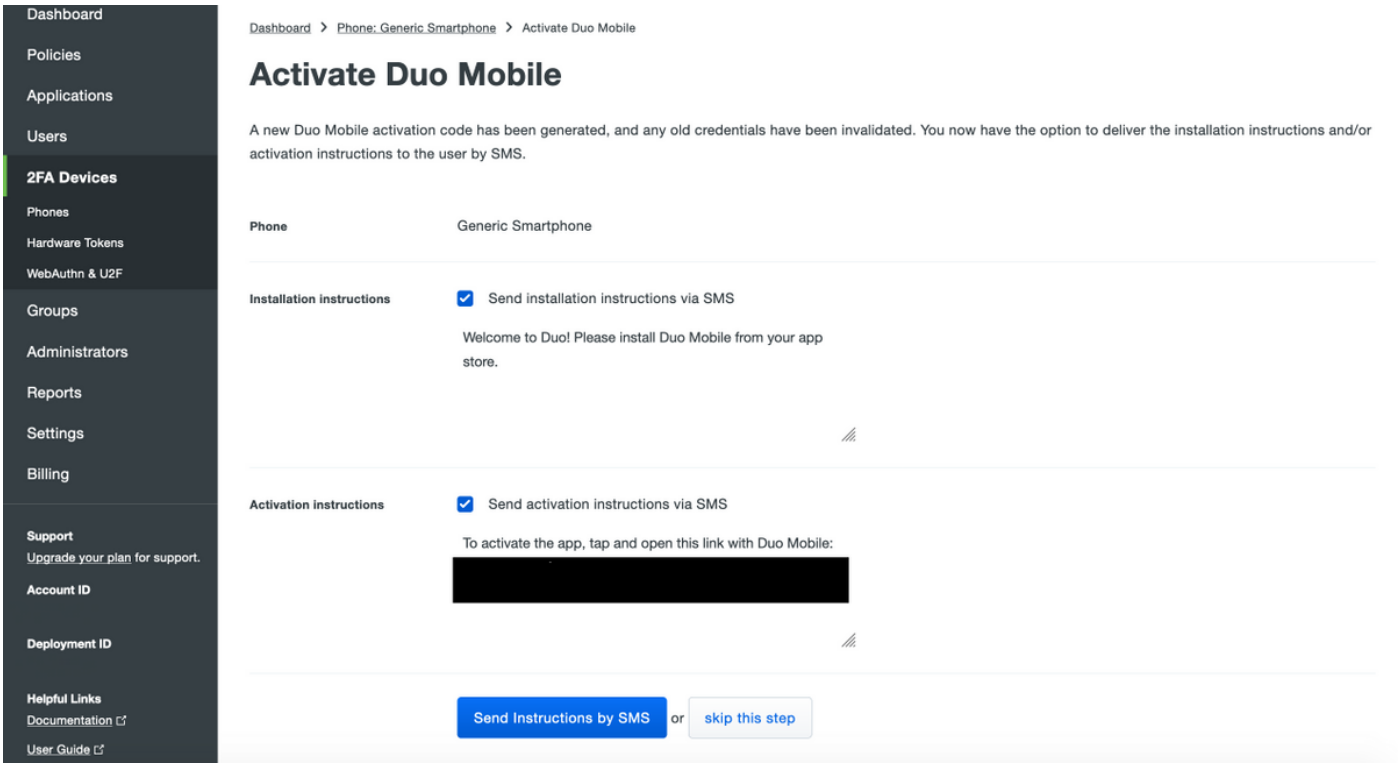
Seleccione **Activate Duo Mobile,** como se muestra en la imagen:



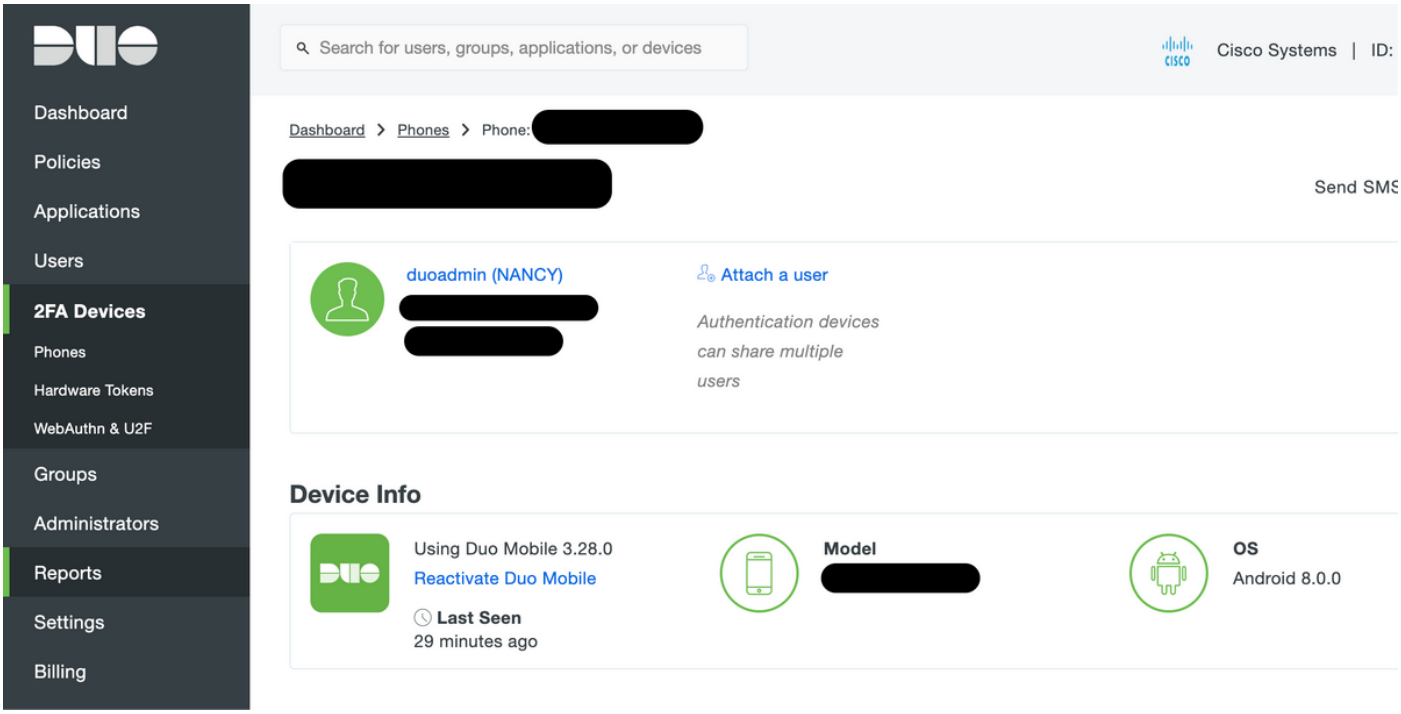
Seleccione **Generate Duo Mobile Activation Code,** como se muestra en la imagen:



Seleccione **Enviar instrucciones por SMS,** como se muestra en la imagen:



Haga clic en el enlace del SMS y la aplicación Duo se vinculará a la cuenta de usuario en la sección **Información del dispositivo**, como se muestra en la imagen:

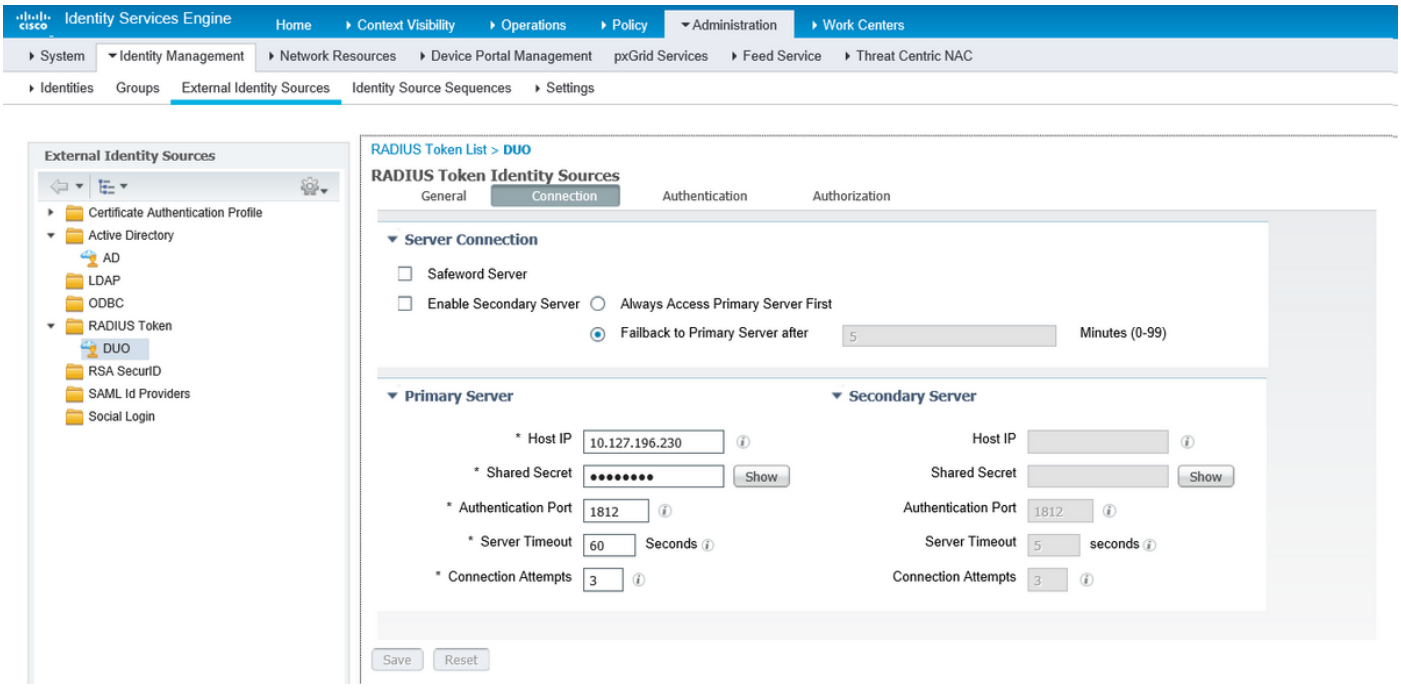


Configuración de ISE

Paso 1. Integre ISE con Duo Auth Proxy.

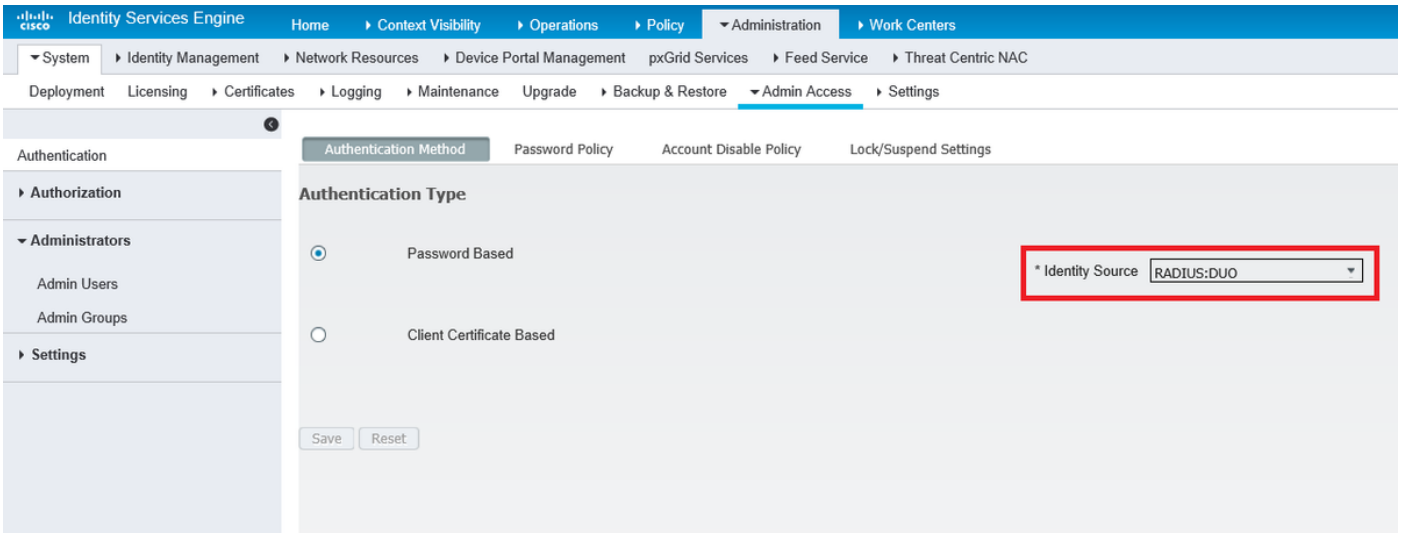
Vaya a **Administration > Identity Management > External Identity Sources > RADIUS Token**, haga clic en **Add** para agregar un nuevo servidor RADIUS Token. Defina el nombre del servidor en la ficha general, la dirección IP y la clave compartida en la ficha de conexión, como se muestra en la imagen:

> **Nota:** Establecer el tiempo de espera del servidor en 60 segundos para que los usuarios tengan tiempo suficiente para actuar en la inserción

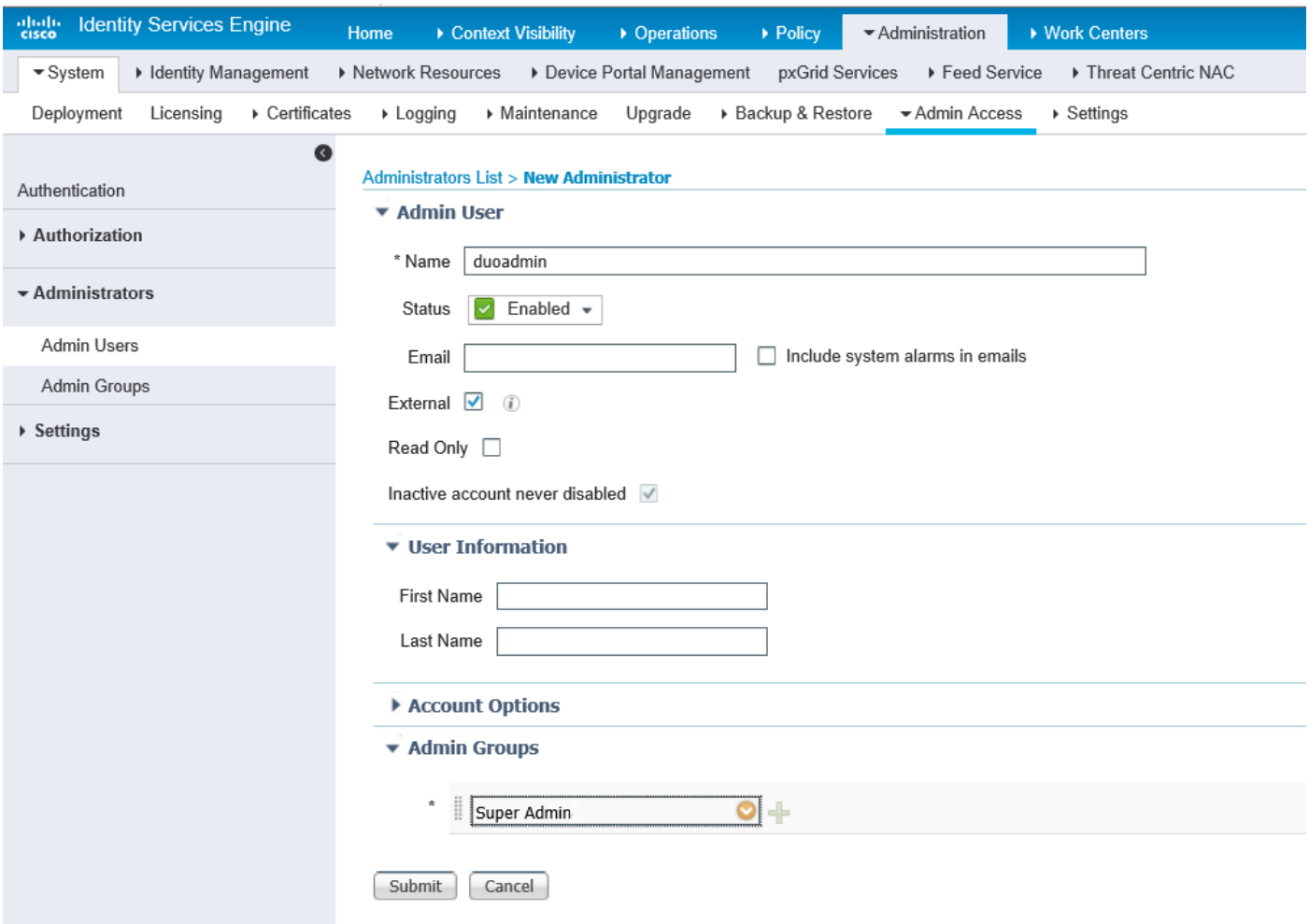


Paso 2. Navegue hasta **Administration > System > Admin Access > Authentication > Authentication Method** y **Select** previamente configurado como servidor de token RADIUS como

origen de identidad, como se muestra en la imagen:



Paso 3. Navegue hasta **Administración > Sistema > Acceso de administrador > Administradores > Usuarios de administrador** y Crear un usuario de administrador como Externo y proporcione privilegio de superadministrador, como se muestra en la imagen:

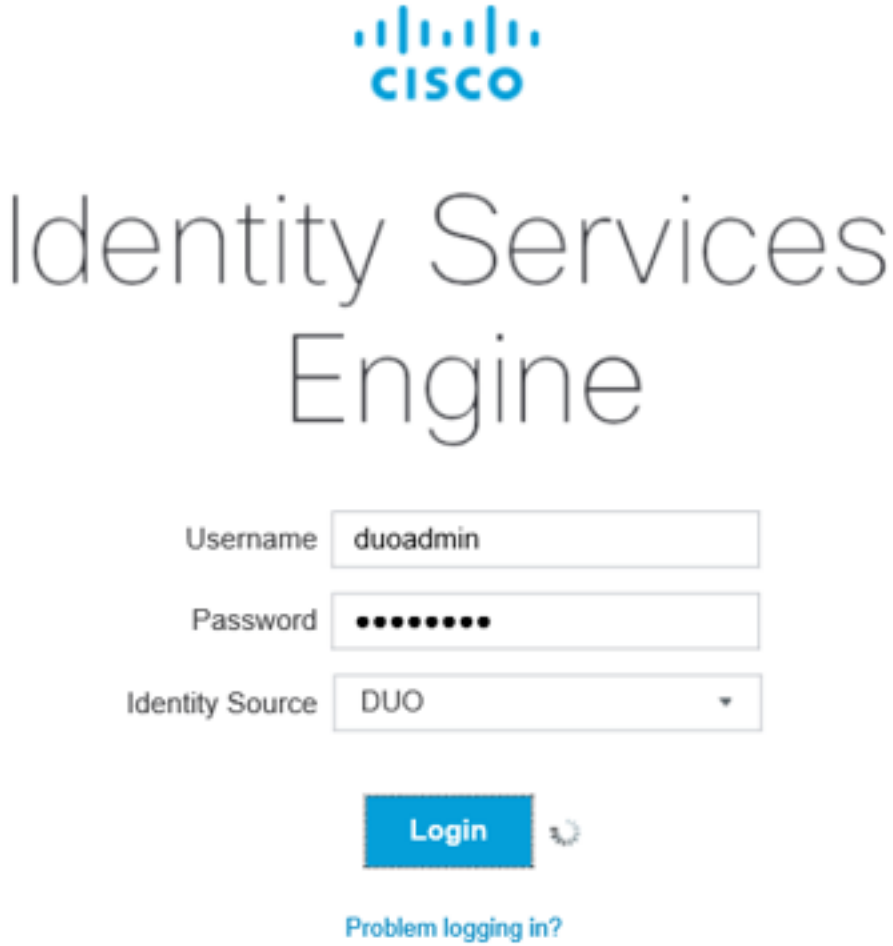


Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Abra la GUI de ISE, seleccione Servidor Token RADIUS como Origen de identidad e inicie sesión

con el usuario administrador.



Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Para resolver problemas relacionados con la conectividad de proxy Duo con la nube o Active Directory, habilite debug en el proxy de autenticación Duo agregando "debug=true" en la sección principal de authproxy.cfg.

Los registros se encuentran en la siguiente ubicación:

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

Abra el archivo **authproxy.log** en un editor de texto como Notepad++ o WordPad.

Registre fragmentos de Duo Auth Proxy que reciben la solicitud de ISE y la envía a 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
```

Los fragmentos de registro del proxy Duo Auth no pueden alcanzar la nube Duo.

```
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
```

Información Relacionada

- Autenticación de VPN de RA con DUO
- Soporte Técnico y Documentación - Cisco Systems