

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

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Diagrama de la red](#)

[Configuración](#)

[Configuración Duo](#)

[Configuración de ISE](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

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

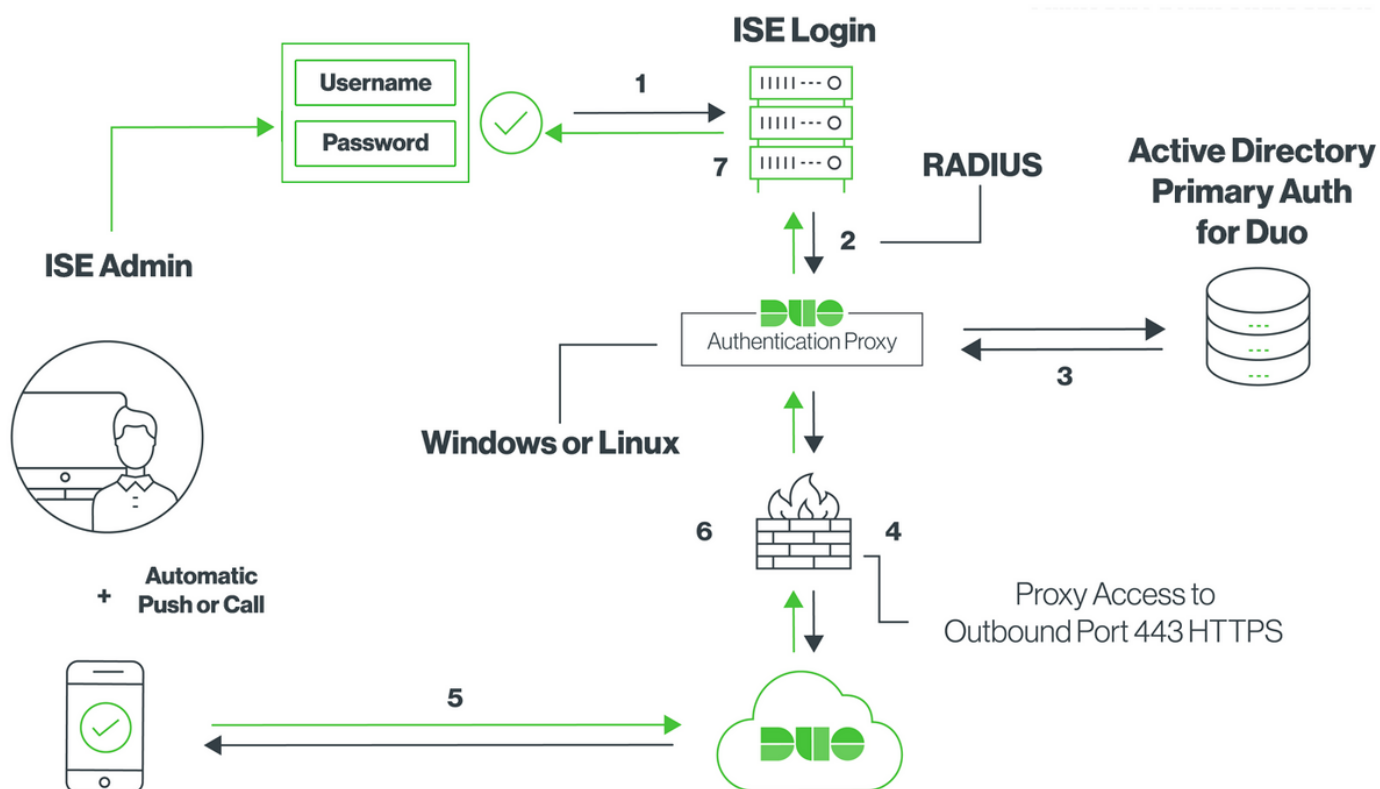
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- 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= xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
skey= xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=api-xxxxxxx.duosecurity.com
radius_ip_1=10.127.196.189
radius_secret_1=*****
failmode=secure
client=ad_client
port=1812

```

Sample IP address of the ISE server

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.

```

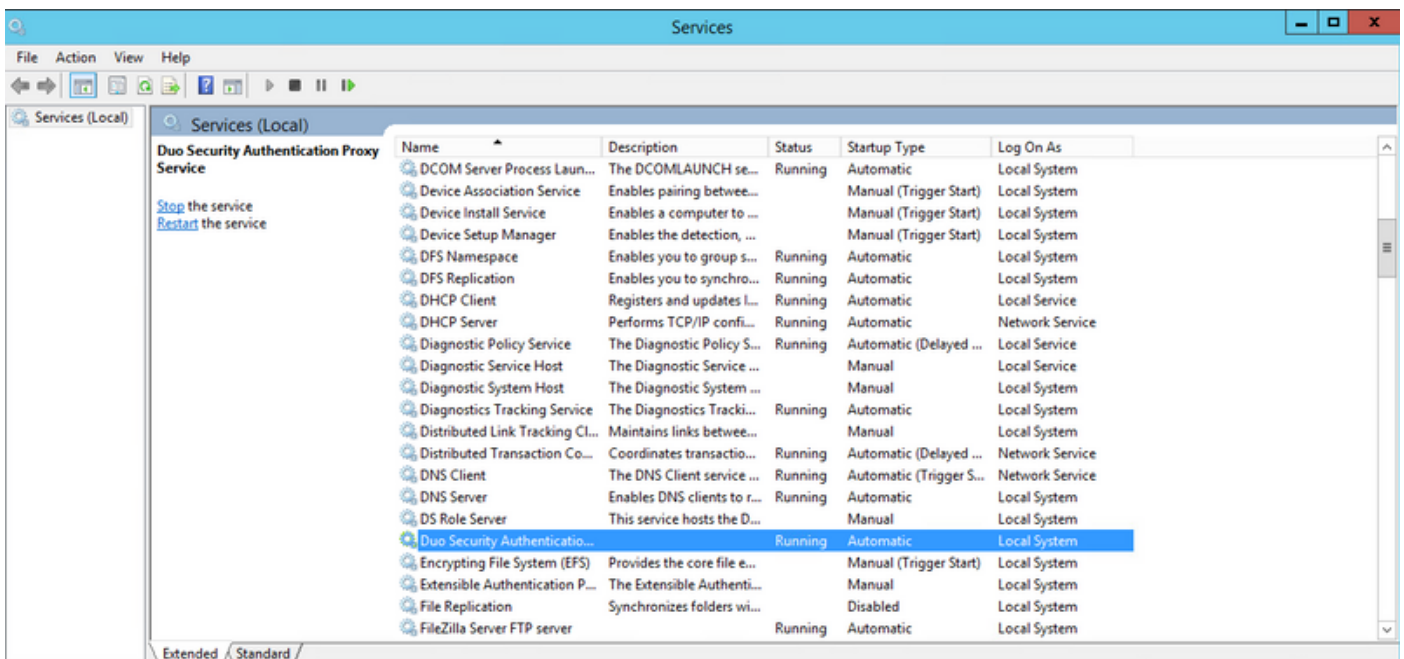
[ad_client]
host=10.127.196.230
service_account_username=< AD-username >
service_account_password=< AD-password >
search_dn=CN=Users,DC=gce,DC=iselab,DC=local

```

Sample IP address of the Active Directory

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:

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 the search bar 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". A note below the field states "Should match the primary authentication username." At the bottom of the form is a blue "Add User" button.

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

The screenshot shows the "Phones" section of the Duo Admin console. The heading is "Phones" and there is a blue "Add Phone" button in the top right corner. Below the heading is the text "You may rearrange the phones by dragging and dropping in the table." A large empty box contains the text "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 screenshot, 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 the search bar is a breadcrumb trail: "Dashboard > Users > duoadmin > Add Phone". The main heading is "Add Phone". Under the heading is a "Type" section with 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". To the right of the field is a link "Show extension field". At the bottom of the form is a blue "Add Phone" button.

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

Device Info



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

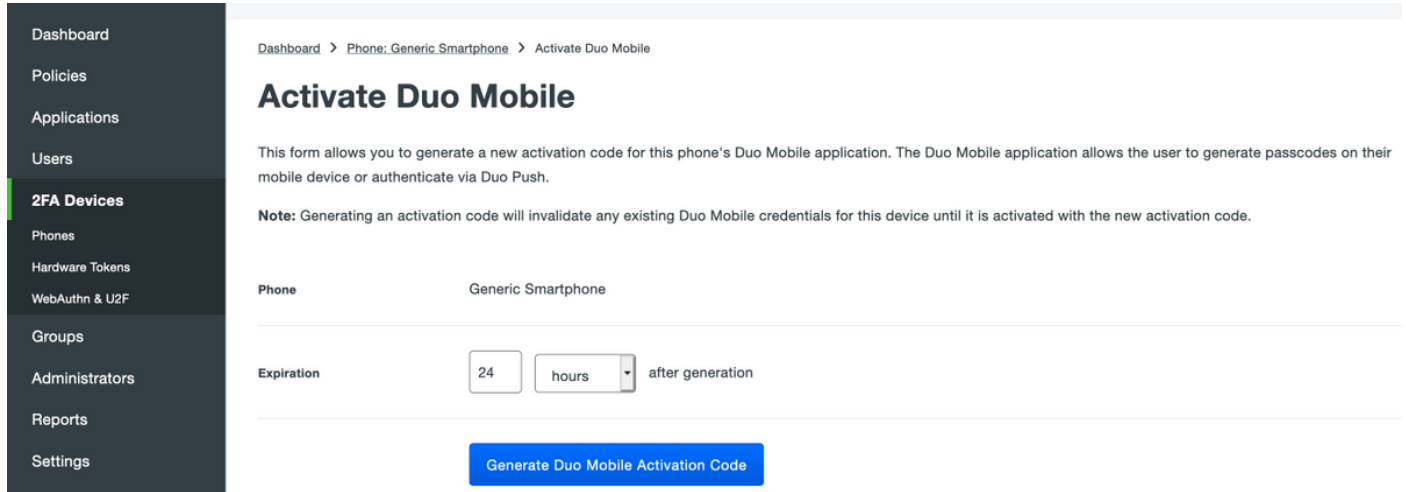


Model
Unknown



OS
Generic Smartphone

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



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.

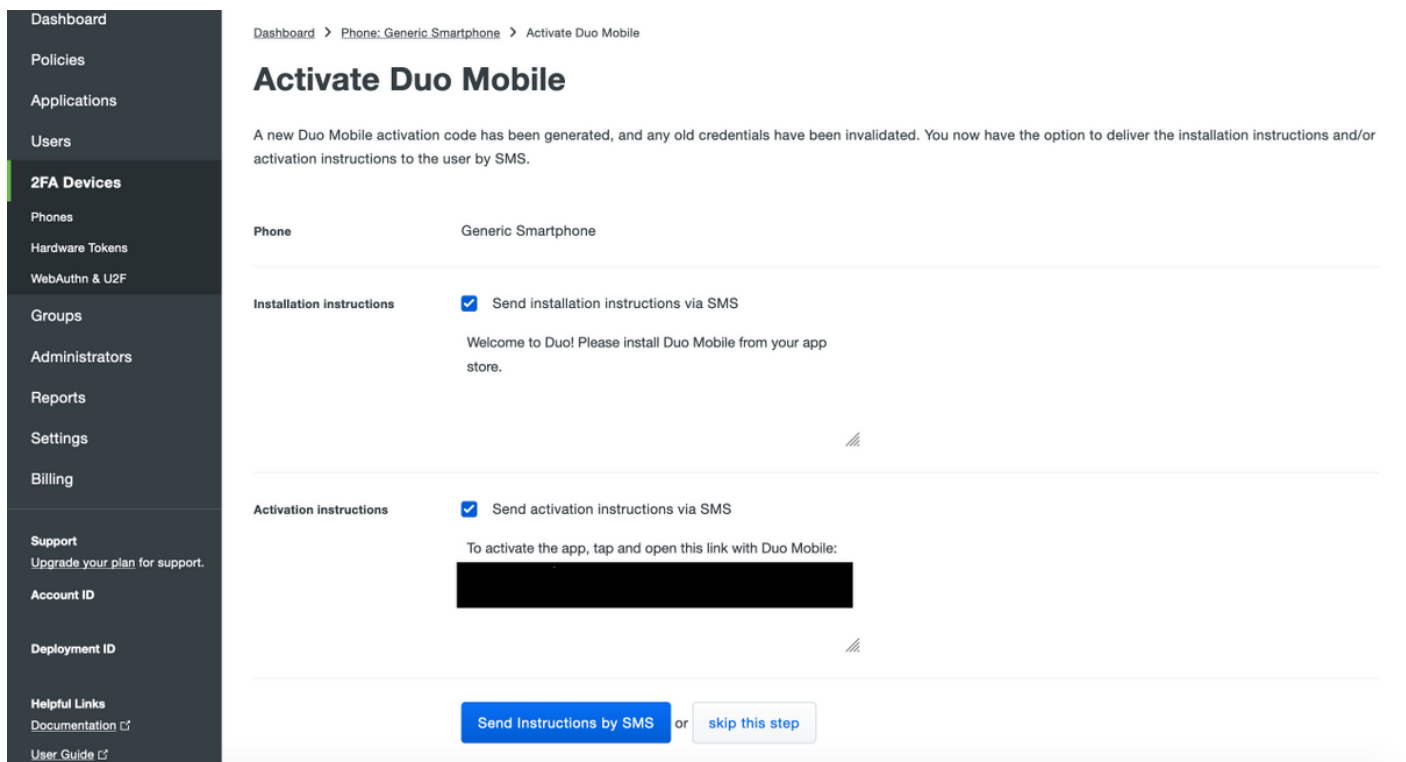
Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.

Phone: Generic Smartphone

Expiration: 24 hours after generation

[Generate Duo Mobile Activation Code](#)

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



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](#)

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:

The screenshot shows the Cisco Duo Admin interface. On the left is a navigation menu with options like Dashboard, Policies, Applications, Users, 2FA Devices (highlighted), Phones, Hardware Tokens, WebAuthn & U2F, Groups, Administrators, Reports, Settings, and Billing. The main content area shows a search bar at the top right with the text 'Cisco Systems | ID:'. Below the search bar is a breadcrumb trail: 'Dashboard > Phones > Phone: [redacted]'. A 'Send SMS' button is visible. The user profile for 'duoadmin (NANCY)' is shown with a green profile icon and a blue 'Attach a user' link. Below the profile, it says 'Authentication devices can share multiple users'. The 'Device Info' section shows a Duo Mobile device (3.28.0) with a 'Reactivate Duo Mobile' link and a 'Last Seen' timestamp of '29 minutes ago'. It also displays the device model as '[redacted]' and the OS as 'Android 8.0.0'.

Configuración de ISE

Paso 1. Integre ISE con Duo Auth Proxy.

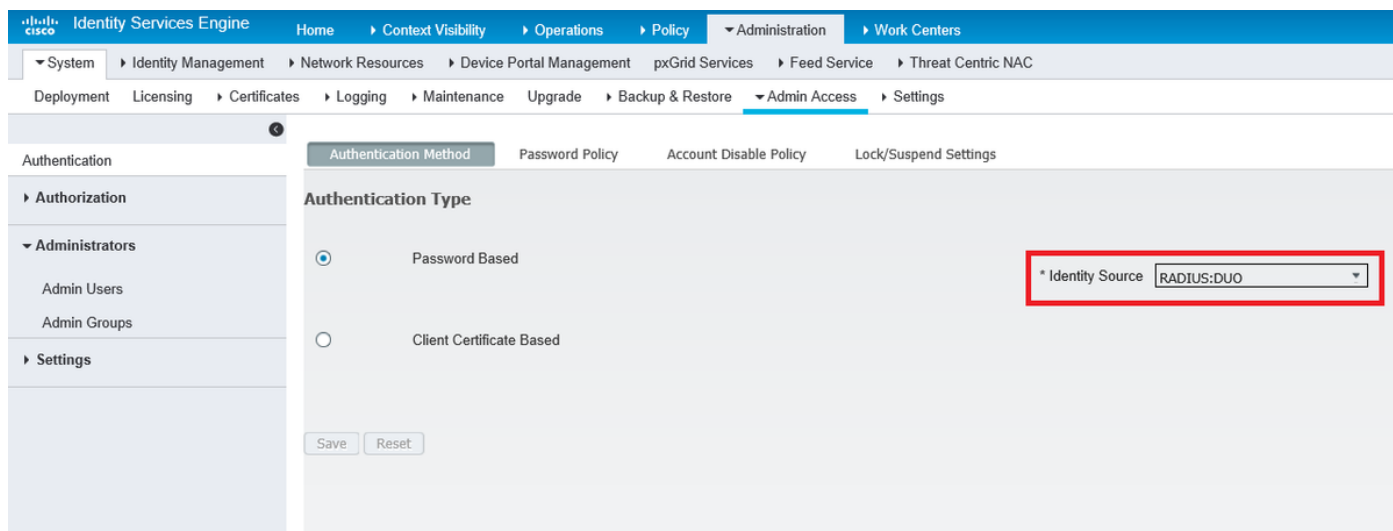
Vaya a **Administration > Identity Management > External Identity Sources > RADIUS Token**, haga clic en **Add** para agregar un nuevo servidor RADIUS Token. Defina el nombre del servidor en la ficha general, la dirección IP y la clave compartida en la ficha de conexión, como se muestra en la imagen:

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

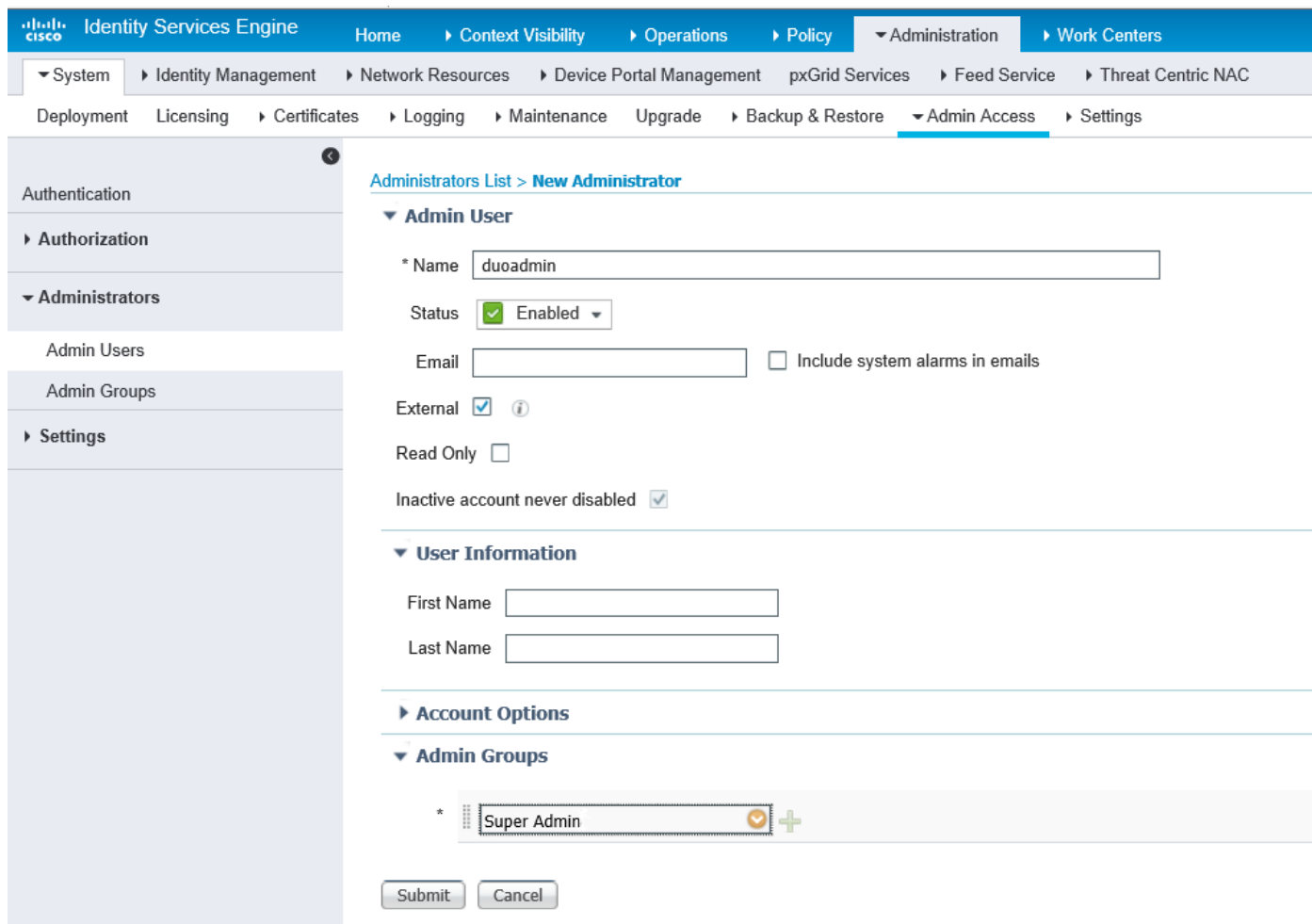
The screenshot shows the Cisco ISE Administration console. The breadcrumb trail is 'Administration > Work Centers > External Identity Sources > Identity Source Sequences > Settings'. The 'External Identity Sources' sidebar is visible on the left. The main content area shows the 'RADIUS Token List > DUO' configuration page. The 'RADIUS Token Identity Sources' section is active, with tabs for 'General', 'Connection', 'Authentication', and 'Authorization'. The 'Connection' tab is selected. Under 'Server Connection', there are checkboxes for 'Safeword Server' and 'Enable Secondary Server'. The 'Fallback to Primary Server after' is set to 5 minutes. The 'Primary Server' configuration includes: Host IP (10.127.196.230), Shared Secret (masked), Authentication Port (1812), Server Timeout (60 seconds), and Connection Attempts (3). The 'Secondary Server' configuration includes: Host IP (empty), Shared Secret (masked), Authentication Port (1812), Server Timeout (5 seconds), and Connection Attempts (3). 'Save' and 'Reset' buttons are at the bottom.

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

Utilice 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.



Identity Services Engine

Username

Password

Identity Source

[Problem logging in?](#)

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 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-xxxxxxx.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](#)