Configurar a autenticação de dois fatores para o acesso de gerenciamento do ISE

Contents

Introduction

Este documento descreve as etapas necessárias para configurar a autenticação externa de dois fatores para o acesso de gerenciamento do Identity Services Engine (ISE). Neste exemplo, o administrador do ISE autentica no servidor de token RADIUS e uma autenticação adicional na forma de notificação push é enviada pelo servidor Proxy de Autenticação Duo para o dispositivo móvel do administrador.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Protocolo RADIUS
- Configurando o servidor de token RADIUS ISE e identidades

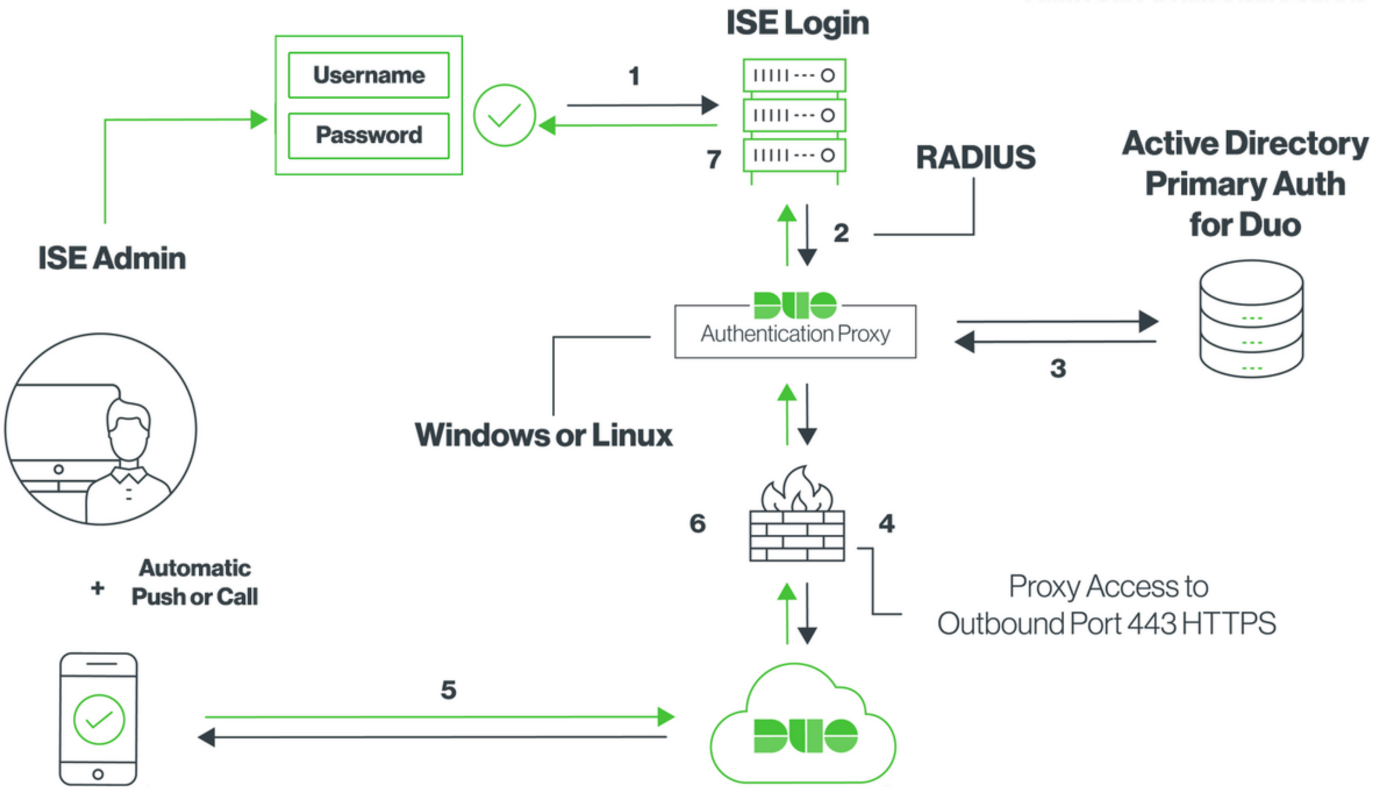
Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Identity services engine (ISE)
- Active Directory (AD)
- Servidor Proxy de Autenticação Duo
- Serviço 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.

Diagrama de Rede



Configuração

Configuração Duo

Etapa 1. Baixe e instale o Duo Authentication Proxy Server em uma máquina Windows ou linux: https://duo.com/docs/ciscoise-radius#install-the-duo-authentication-proxy

Note: Esta máquina deve ter acesso ao ISE e à Duo Cloud (Internet)

Etapa 2. Configure o arquivo **authproxy.cfg**.

Abra este arquivo em um editor de texto, como o Notepad++ ou WordPad.

Observação: o local padrão é **C:\Program Files (x86)\Duo Security Authentication Proxy\conf\authproxy.cfg**

Etapa 3. Crie um aplicativo "Cisco ISE RADIUS" no Painel de administração do Duo: **https://duo.com/docs/ciscoise-radius#first-steps**

Etapa 4. Edite o arquivo **authproxy.cfg** e adicione esta configuração.

```
ikey= xxxxxxxxxxxxxxxxxxxxxxxxxx
skey= xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

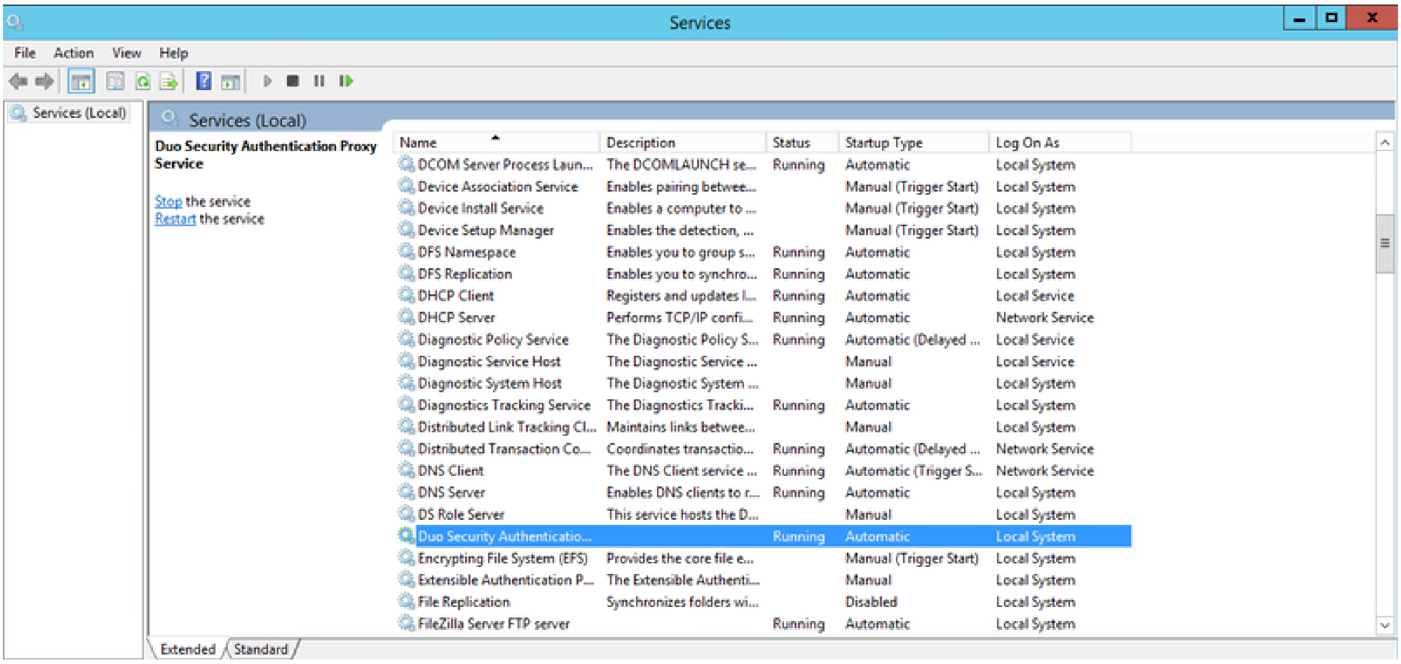
```
api_host=api-xxxxxxxx.duosecurity.com
radius_ip_1=10.127.196.189                   Sample IP address of the ISE server
radius_secret_1=******
failmode=secure
client=ad_client
port=1812
```

Etapa 5. Configure o ad_client com seus detalhes do Ative Diretory. O Proxy de Autenticação Duo usa as informações abaixo para autenticar no AD para a autenticação primária.

```
[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: Se a sua rede exigir uma conexão de proxy HTTP para acesso à Internet, adicione detalhes http_proxy em authproxy.cfg.

Etapa 6. Reinicie o Serviço Proxy de Autenticação de Segurança Duo. Salve o arquivo e **reinicie** o **serviço Duo** na máquina Windows.Abra o console do Windows Services (services.msc), localize o **Serviço Proxy de Autenticação de Segurança Duo** na lista de serviços e clique em **Reiniciar** como mostrado na imagem:



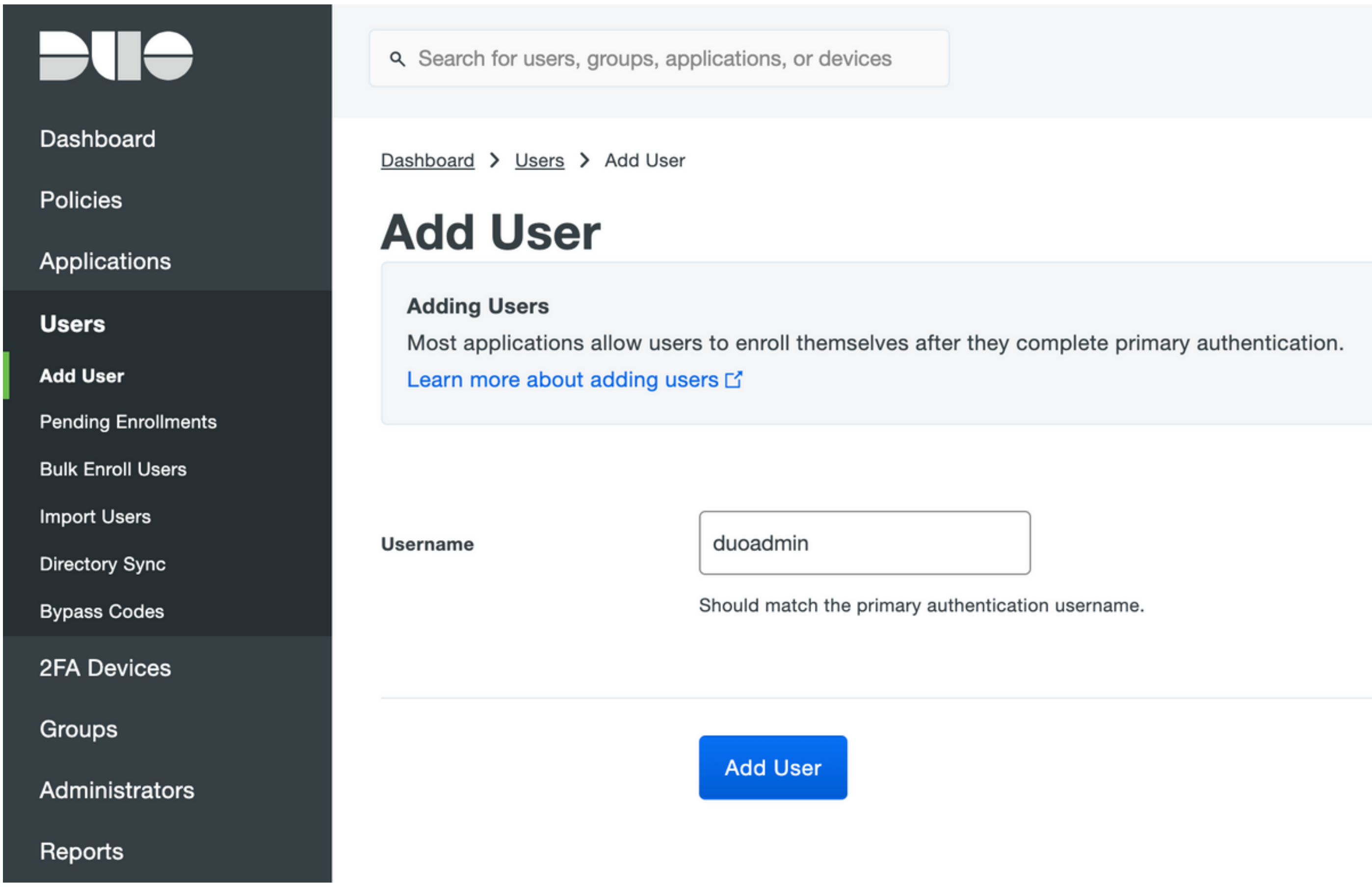
Duo Security Authentication Proxy Service

Stop the service
Restart the service

Name	Description	Status	Startup Type	Log On As
DCOM Server Process Laun...	The DCOMLAUNCH se...	Running	Automatic	Local System
Device Association Service	Enables pairing betwee...		Manual (Trigger Start)	Local System
Device Install Service	Enables a computer to ...		Manual (Trigger Start)	Local System
Device Setup Manager	Enables the detection, ...		Manual (Trigger Start)	Local System
DFS Namespace	Enables you to group s...	Running	Automatic	Local System
DFS Replication	Enables you to synchro...	Running	Automatic	Local System
DHCP Client	Registers and updates I...	Running	Automatic	Local Service
DHCP Server	Performs TCP/IP confi...	Running	Automatic	Network Service
Diagnostic Policy Service	The Diagnostic Policy S...	Running	Automatic (Delayed ...	Local Service
Diagnostic Service Host	The Diagnostic Service ...		Manual	Local Service
Diagnostic System Host	The Diagnostic System ...		Manual	Local System
Diagnostics Tracking Service	The Diagnostics Tracki...	Running	Automatic	Local System
Distributed Link Tracking Cl...	Maintains links betwee...		Manual	Local System
Distributed Transaction Co...	Coordinates transactio...	Running	Automatic (Delayed ...	Network Service
DNS Client	The DNS Client service ...	Running	Automatic (Trigger S...	Network Service
DNS Server	Enables DNS clients to r...	Running	Automatic	Local System
DS Role Server	This service hosts the D...		Manual	Local System
Duo Security Authenticatio...		Running	Automatic	Local System
Encrypting File System (EFS)	Provides the core file e...		Manual (Trigger Start)	Local System
Extensible Authentication P...	The Extensible Authenti...		Manual	Local System
File Replication	Synchronizes folders wi...		Disabled	Local System
FileZilla Server FTP server		Running	Automatic	Local System

Etapa 7. Crie um nome de usuário e ative o Duo Mobile no dispositivo final: https://duo.com/docs/administration-users#creating-users-manually

Adicione o usuário ao Painel de administração do Duo. Navegue até **Usuários > adicionar usuários,** conforme mostrado na imagem:



Adding Users

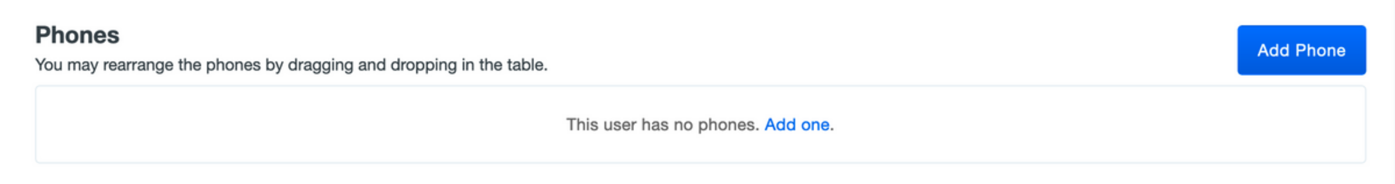
Most applications allow users to enroll themselves after they complete primary authentication.

Learn more about adding users

Username: duoadmin

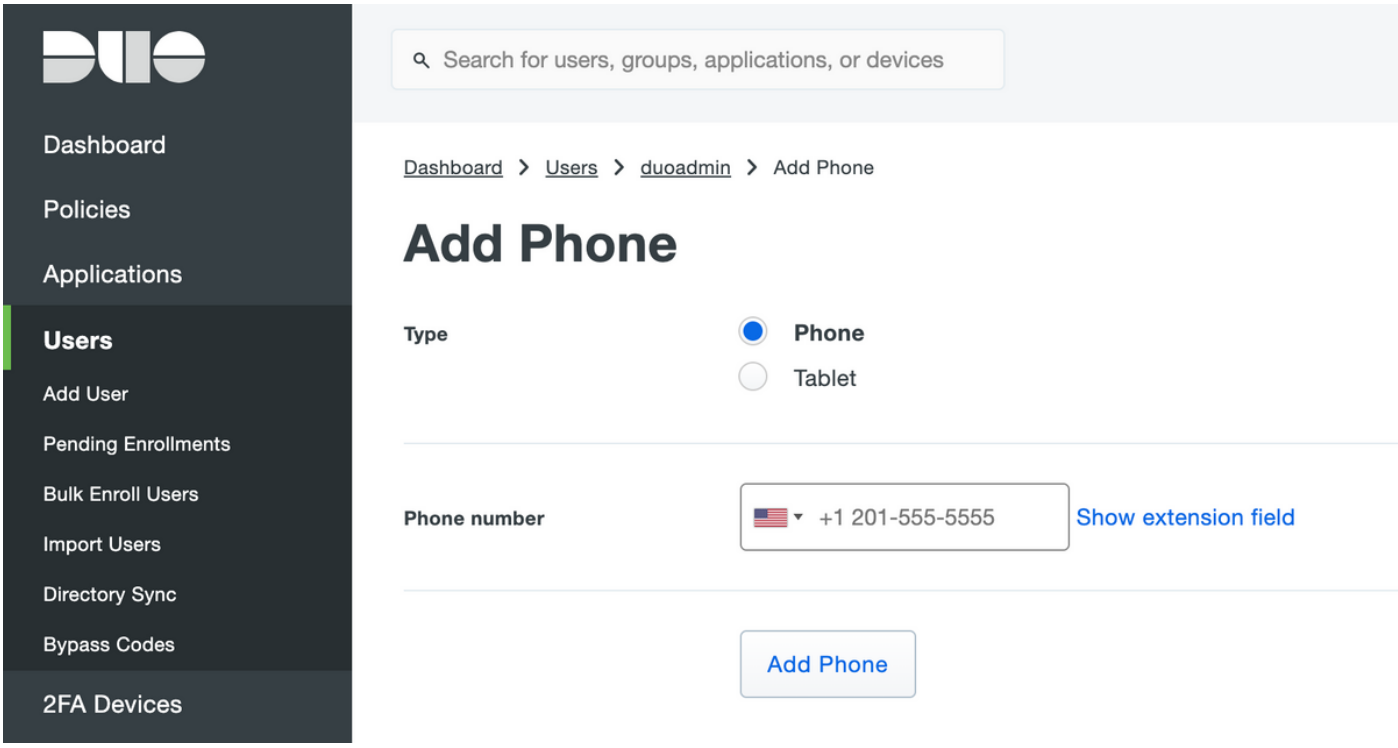
Should match the primary authentication username.

Verifique se o usuário final tem o aplicativo Duo instalado no telefone.


Phones

You may rearrange the phones by dragging and dropping in the table.

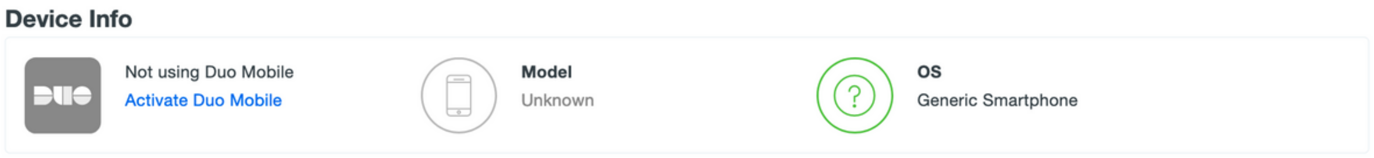
This user has no phones. Add one.



Type: ● Phone ○ Tablet

Phone number: +1 201-555-5555

Selecione **Ativate Duo Mobile,** conforme mostrado na imagem:



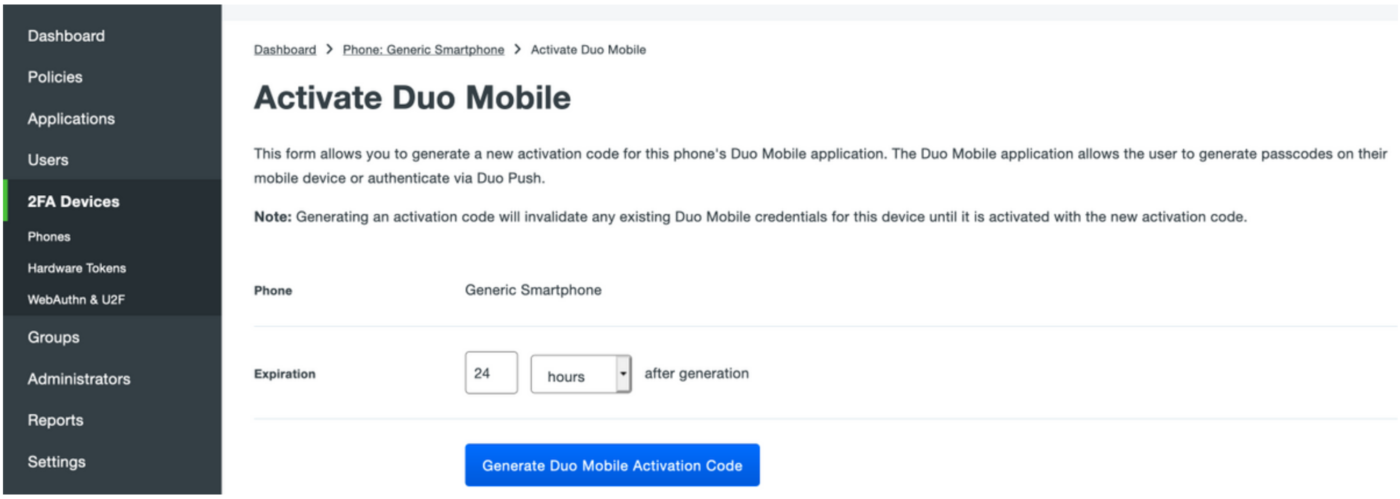
Device Info

Not using Duo Mobile
Activate Duo Mobile

Model
Unknown

OS
Generic Smartphone

Selecione **Gerar Código de Ativação Móvel Duo,** conforme mostrado na imagem:



Dashboard > Phone: Generic Smartphone > Activate Duo Mobile

Activate Duo Mobile

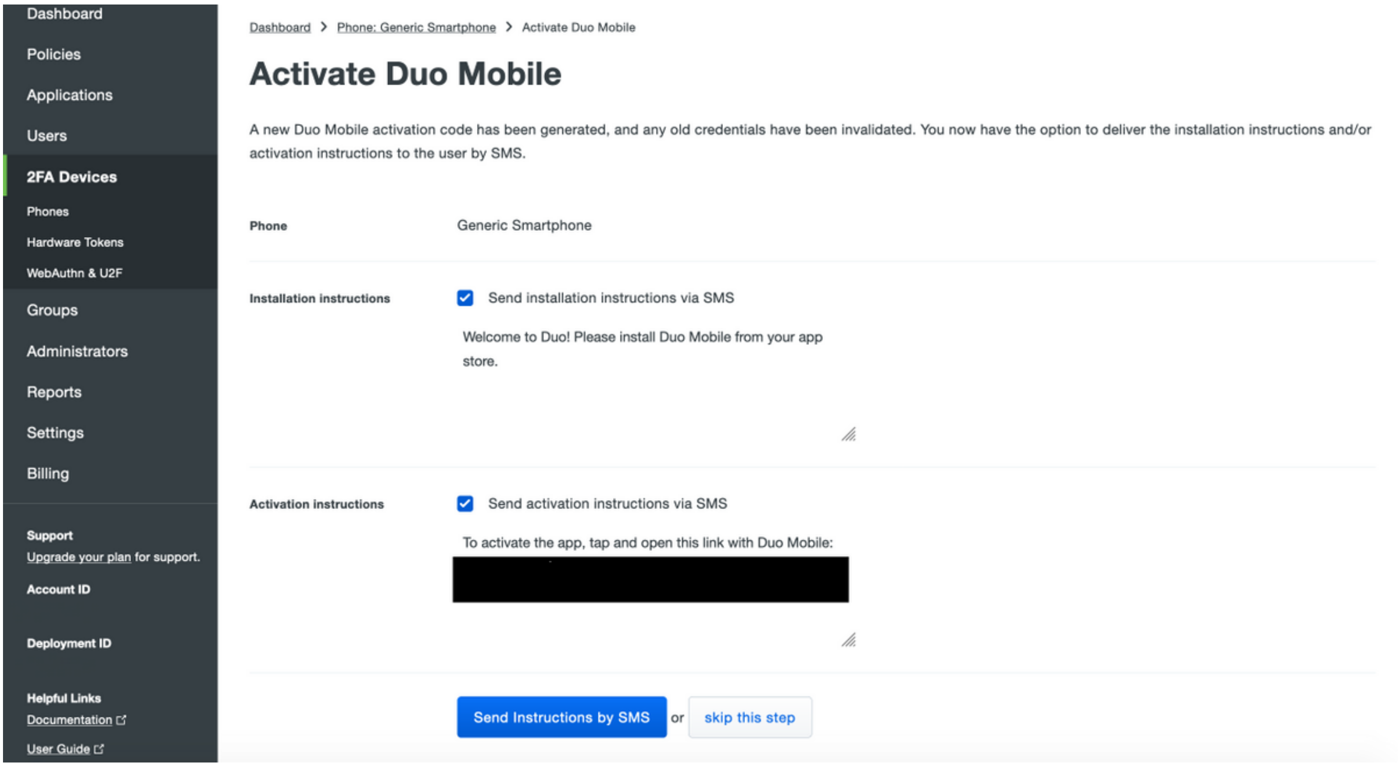
This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to generate passcodes on their mobile device or authenticate via Duo Push.

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

Selecione **Enviar instruções por SMS,** conforme mostrado na imagem:



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

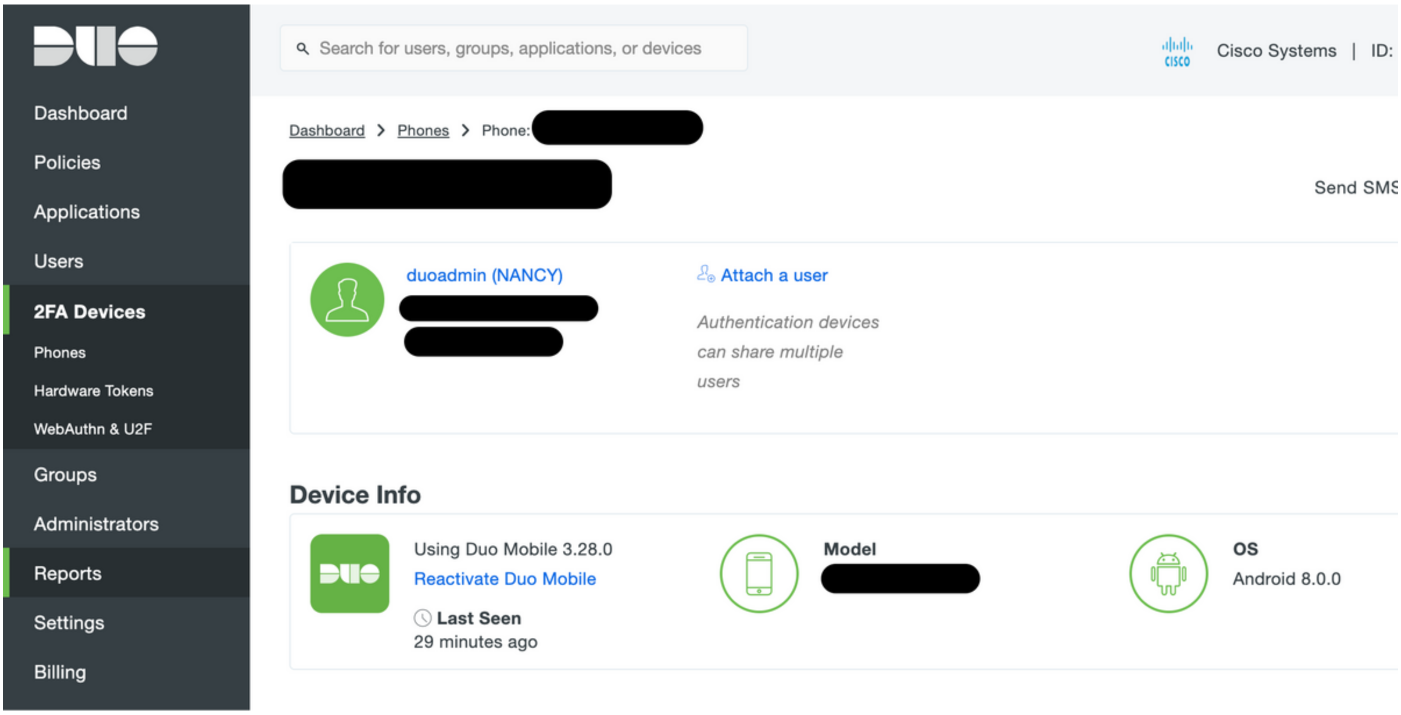
Installation instructions: ☑ Send installation instructions via SMS

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:
[redacted]

Clique no link no SMS e o aplicativo Duo será vinculado à conta de usuário na seção **Informações do dispositivo**, como mostrado na imagem:



duoadmin (NANCY)
[redacted]
[redacted]

Attach a user

Authentication devices can share multiple users

Device Info

Using Duo Mobile 3.28.0
Reactivate Duo Mobile
Last Seen
29 minutes ago

Model
[redacted]

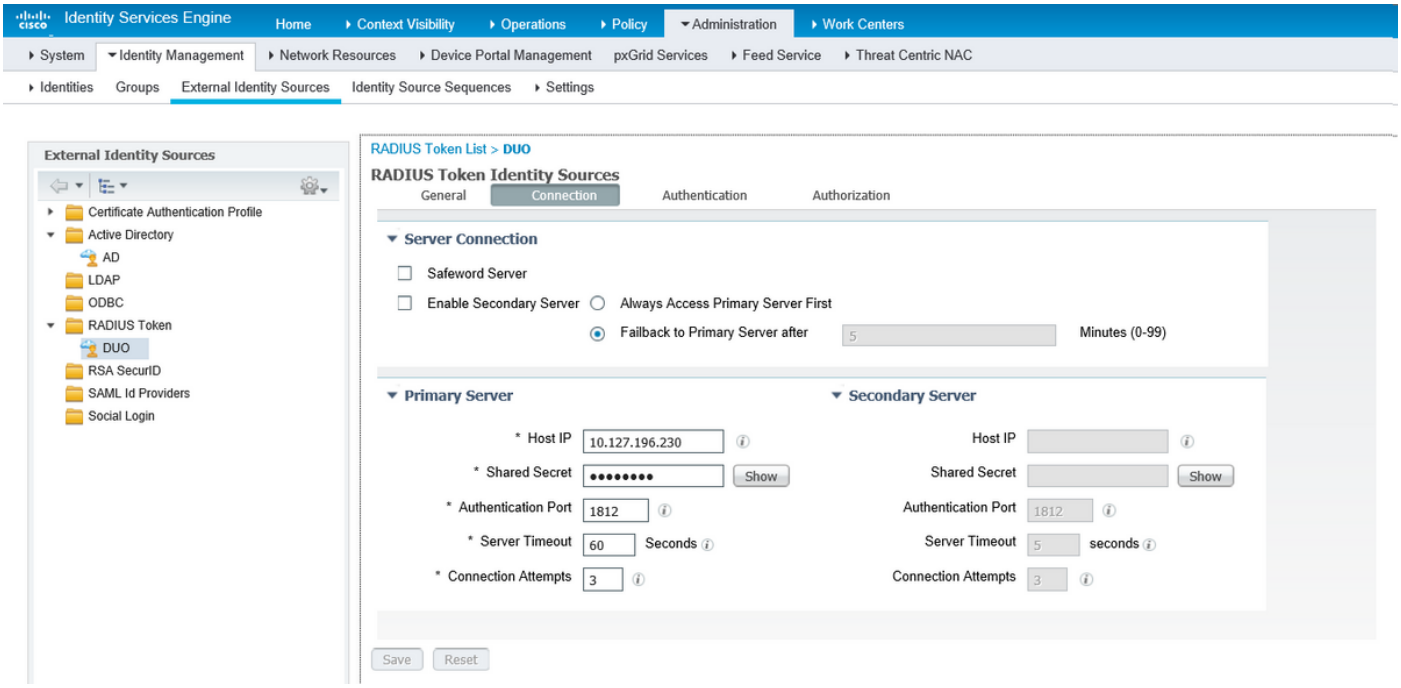
OS
Android 8.0.0

Configuração do ISE

Etapa1. Integre o ISE ao proxy de autenticação Duo.

Navegue até **Administration > Identity Management > External Identity Sources > RADIUS Token**, clique em **Add** para adicionar um novo servidor de Token RADIUS. Defina o nome do servidor na guia geral, o endereço IP e a chave compartilhada na guia de conexão, como mostrado na imagem:

> **Note**: Defina o tempo limite do servidor como 60 segundos para que os usuários tenham tempo suficiente para agir no envio



RADIUS Token Identity Sources

Server Connection

☐ Safeword Server
☐ Enable Secondary Server ○ Always Access Primary Server First
● Failback to Primary Server after 5 Minutes (0-99)

Primary Server

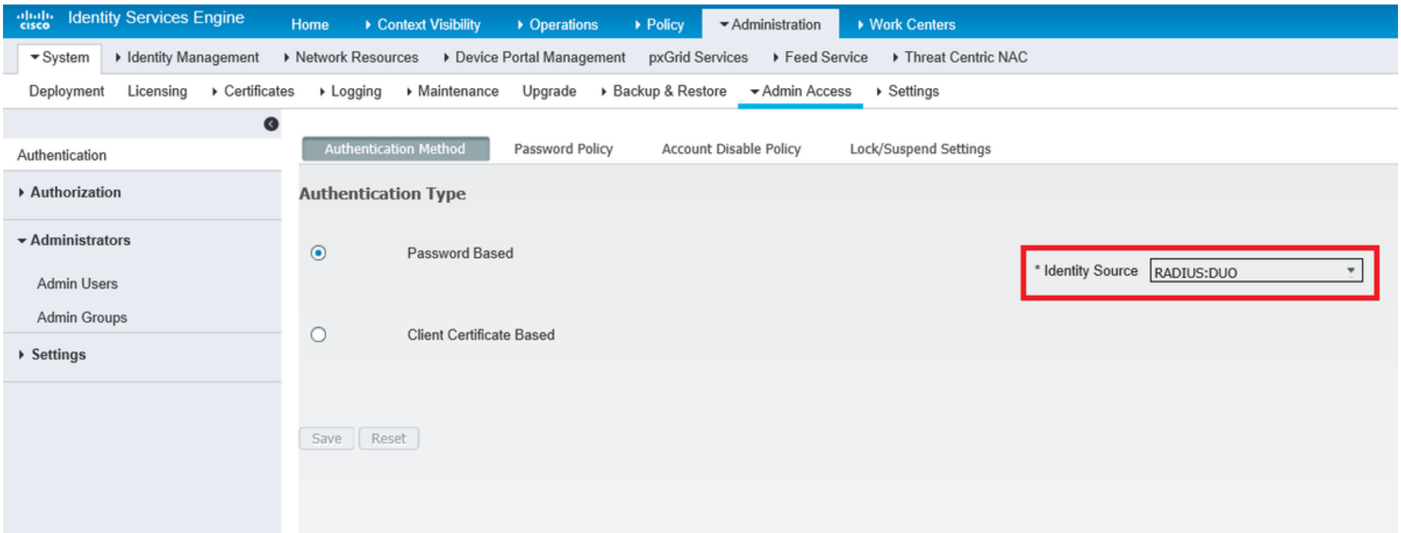
* Host IP: 10.127.196.230
* Shared Secret: •••••••• Show
* Authentication Port: 1812
* Server Timeout: 60 Seconds
* Connection Attempts: 3

Secondary Server

Host IP:
Shared Secret: Show
Authentication Port: 1812
Server Timeout: 5 seconds
Connection Attempts: 3

Etapa 2. Navegue até **Administration > System > Admin Access > Authentication > Authentication Method** e **Select** previamente configurado como o servidor de token RADIUS como a Identity

Source, como mostrado na imagem:



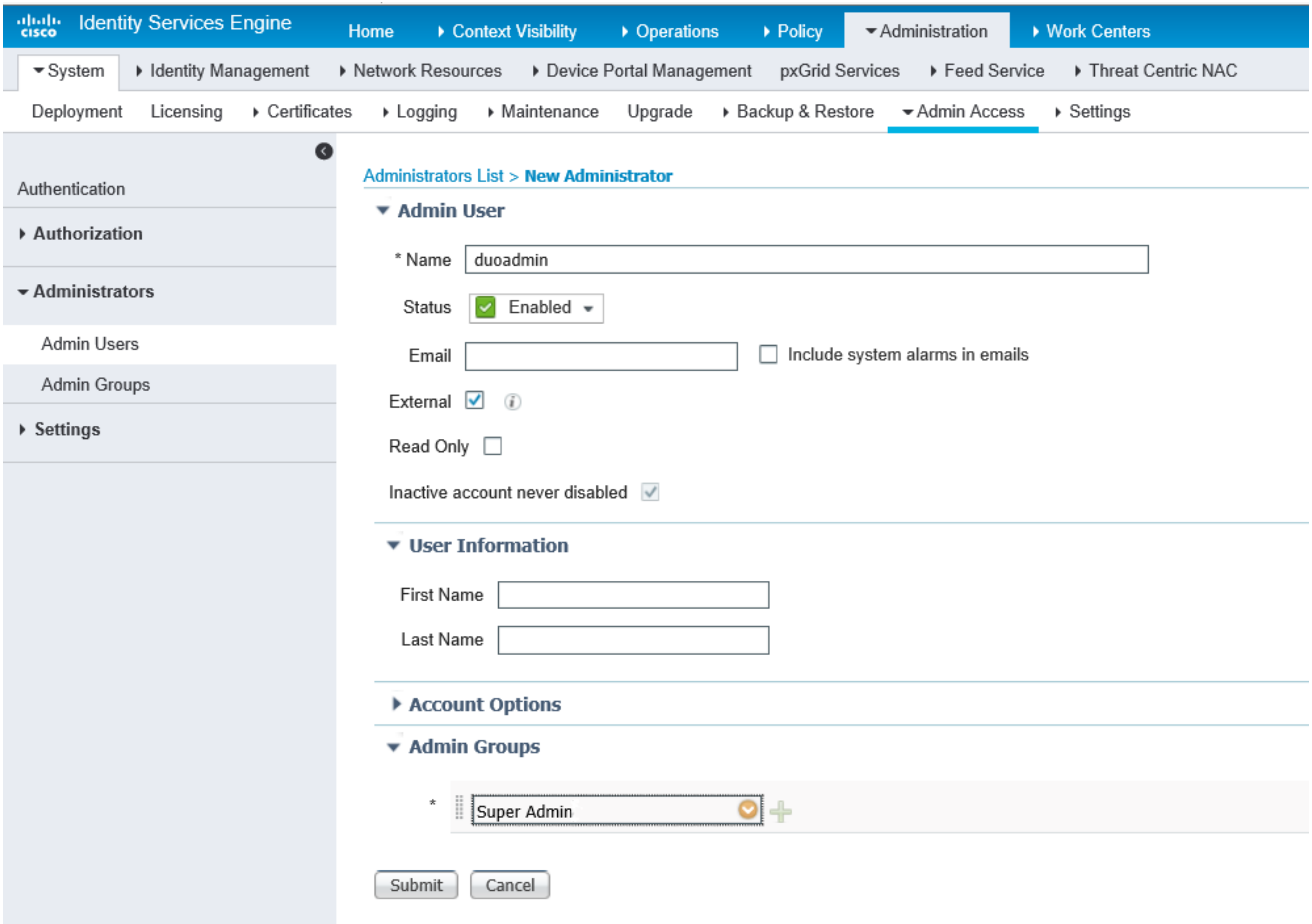
Authentication Type

● Password Based

○ Client Certificate Based

* Identity Source RADIUS:DUO

Etapa 3. Navegue até **Administration > System > Admin Access > Administrators > Admin Users** e Create an admin user as External e forneça o privilégio de superadministrador, como mostrado na imagem:



Administrators List > New Administrator

Admin User

* Name duoadmin

Status ☑ Enabled

Email

□ Include system alarms in emails

External ☑

Read Only □

Inactive account never disabled ☑

User Information

First Name

Last Name

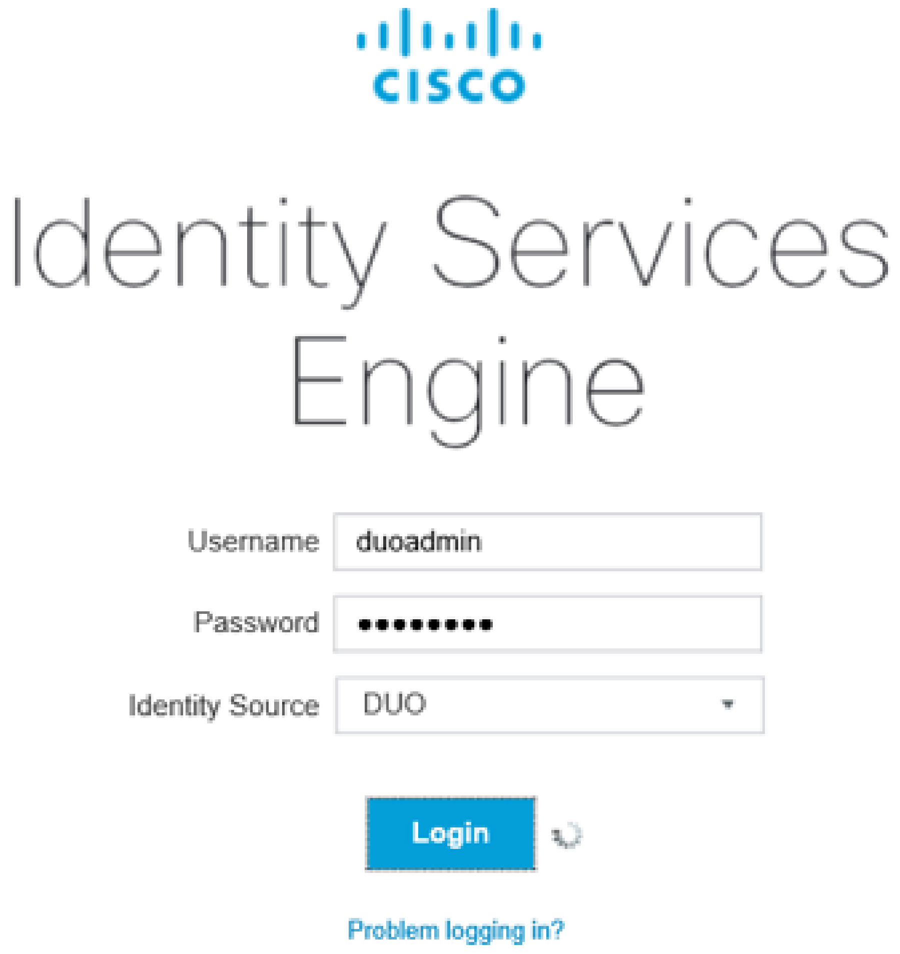
Admin Groups

* Super Admin

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Abra a GUI do ISE, selecione RADIUS Token Server como Identity Source e faça login com o usuário admin.



Username duoadmin

Password ●●●●●●●●●

Identity Source DUO

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Para solucionar problemas relacionados à conectividade de proxy Duo com a nuvem ou Ative Diretory, habilite a depuração no proxy de autenticação Duo adicionando "debug=true" na seção principal de authproxy.cfg.

Os registros estão localizados no seguinte local:

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

Abra o arquivo **authproxy.log** em um editor de texto, como o Bloco de Notas+ ou WordPad.

Registre os trechos do Proxy de Autenticação Duo recebendo solicitação do ISE e enviando-o para a Nuvem Duo.

```
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
```

Os trechos de log do Proxy de Autenticação Duo não conseguem acessar a Nuvem 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
```

Informações Relacionadas

- Autenticação de VPN RA usando DUO
- Suporte Técnico e Documentação - Cisco Systems