

Configurar a integração do console do dispositivo do modo gerenciado de interceptação (IMM - Intersight Managed Mode) com autenticação multifator LDAP e Duo

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Configurar](#)

[Diagrama de Rede](#)

[Etapa 1.](#)

[Etapa 2.](#)

[Etapa 3.](#)

[Etapa 4.](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar a autenticação multifator no console do dispositivo IMM usando LDAP e o proxy de autenticação Duo.

Pré-requisitos

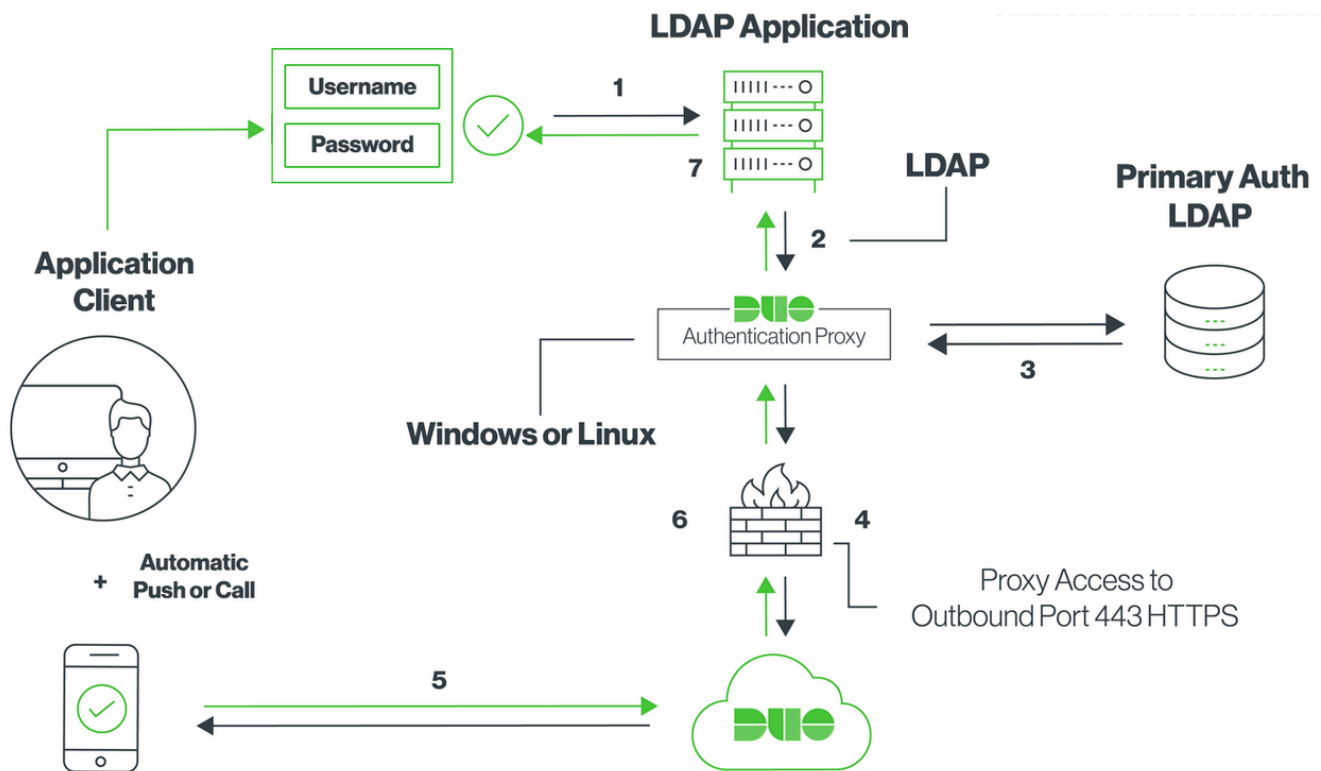
Requisitos

Interconexões em malha UCS no IMM (Intersight Managed Mode).

Duo com um usuário inscrito.

Configurar

Diagrama de Rede



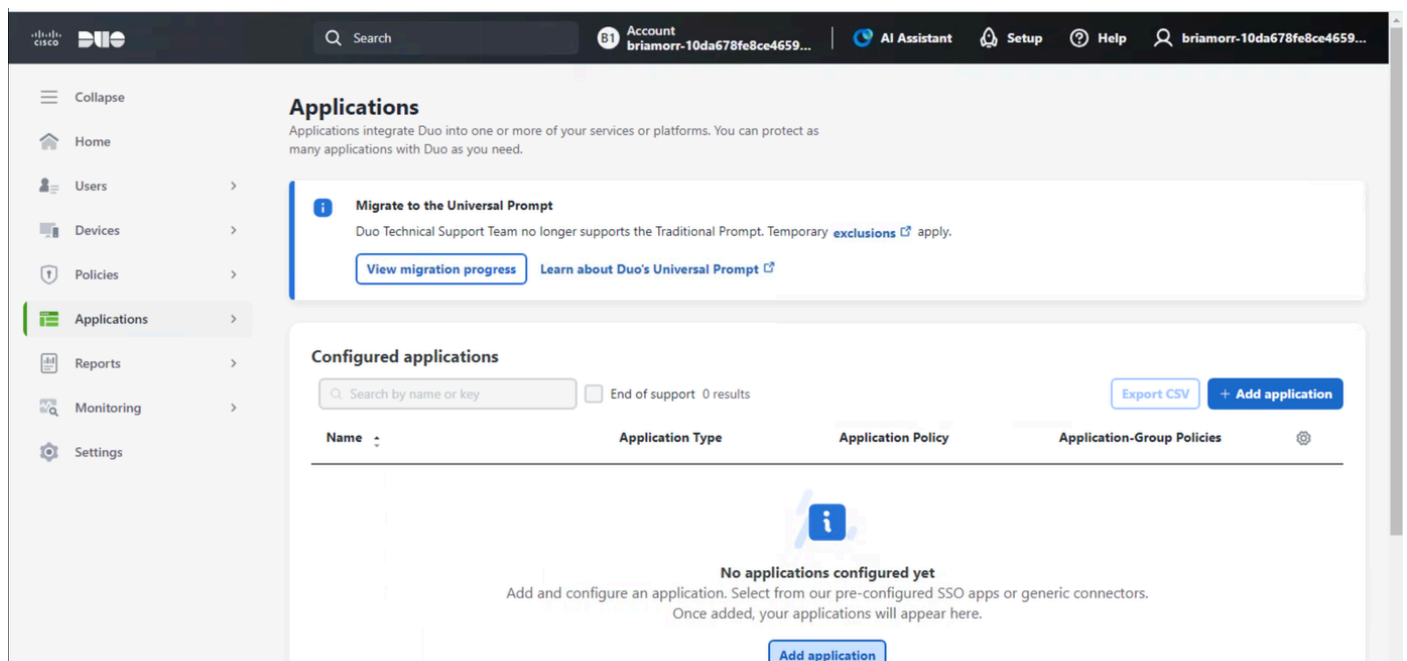
Etapa 1.

Instale o Proxy de Autenticação Duo em um servidor Windows que seja acessível ao Active Directory e ao Console do Dispositivo IMM.

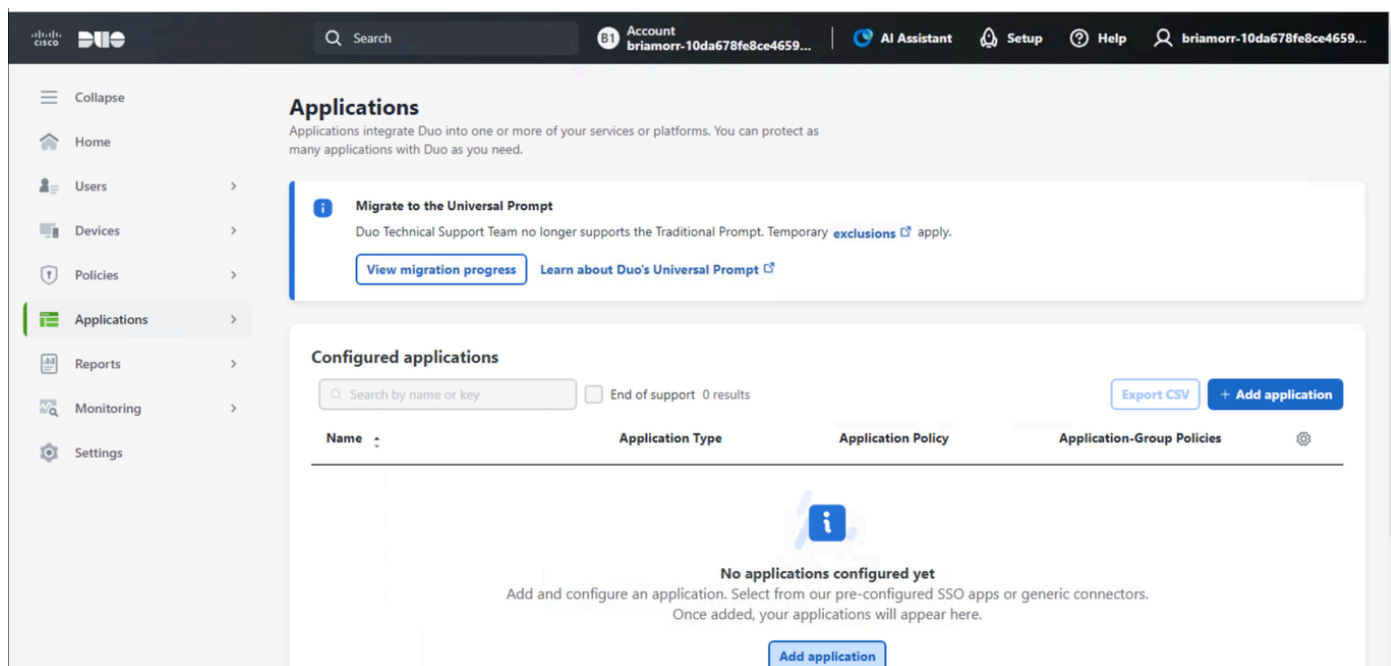
O proxy de autenticação Duo pode ser encontrado [aqui](#).

Etapa 2.

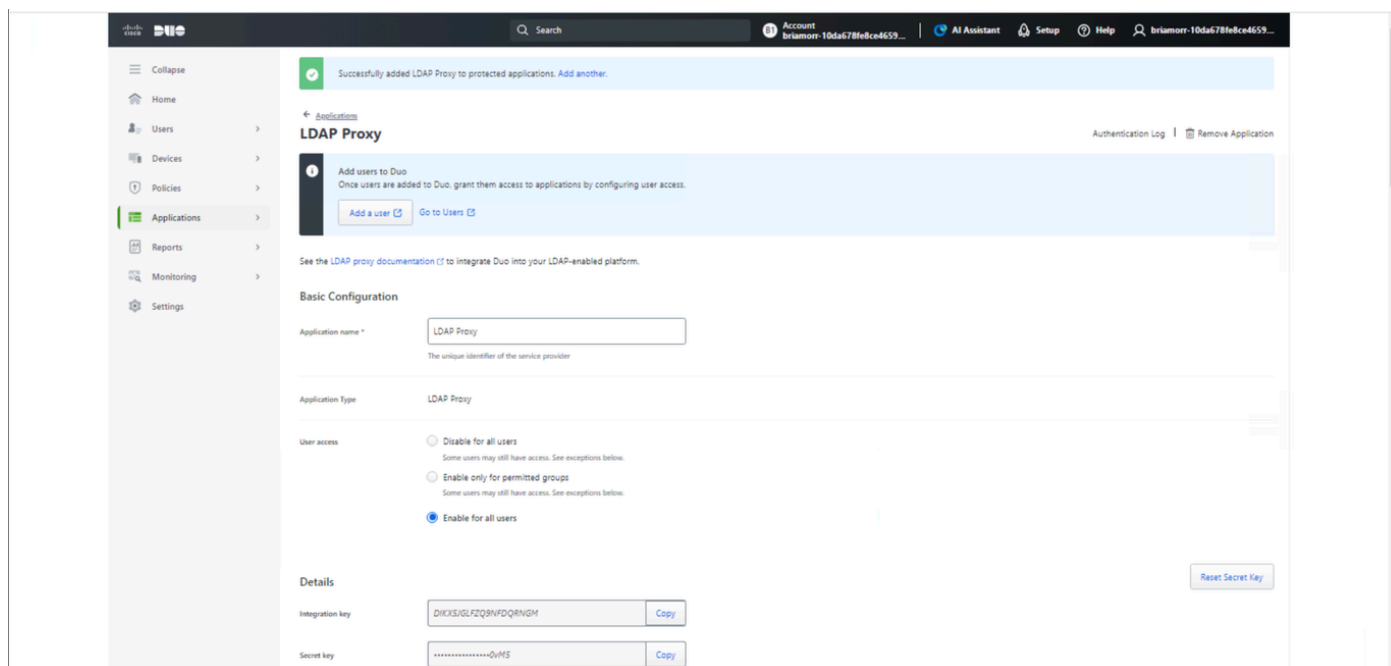
Em nossa instância Duo , você pode adicionar um novo aplicativo.



Procure ldap e adicione o proxy LDAP para continuar.



No aplicativo Proxy LDAP, você pode configurar um nome de aplicativo, habilitar para todos os usuários e copiar a chave de integração, a chave secreta e o nome de host da API para uso posterior.



Etapa 3.

De volta ao servidor onde instalamos o Duo Authentication Proxy, você pode configurar o Duo Authentication Proxy Manager.

Duo Authentication Proxy Manager
Authentication Proxy is running
Uptime: 00:02:14
Version: 6.5.2
Restart Service
Stop Service

Configure: authproxy.cfg
Unsaved Changes

```

12 ; CLIENTS: Include one or more of the following configuration secti
13 ; To configure more than one client configuration of the same type,
14 ; number to the section name (e.g. [ad_client2])
15
16 [ad_client]
17 host=ad1.dcloud.cisco.com
18 service_account_username=ldap
19 service_account_password=changeme
20 search_dn=DC=dcloud,DC=cisco,DC=com
21
22
23 ; SERVERS: Include one or more of the following configuration secti
24 ; To configure more than one server configuration of the same type,
25 ; number to the section name (e.g. radius_server_auto1, radius_serv
26
27 [ldap_server_auto]
28 client=ad_client
29 ikey=DI*****
30 skey=*****
31 api_host=api-demodemo.duosecurity.com
32 failmode=safe
33 port=1389
34 exempt_ou_1=CN=ldap,CN=Users,DC=dcloud,DC=cisco,DC=com
35 exempt_primary_bind=false
36 allow_unlimited_binds=true

```

Output

Validate the configuration to view output

Validate
Save

[Learn how to configure the Authentication Proxy](#)

Exemplo de configuração do proxy de autenticação Duo:



Note: # comentários adicionados para legibilidade.

```

[ad_client]
host=ad1.dcloud.cisco.com    # Our Domain Controller
service_account_username=ldap # Our BIND Service Account in AD
service_account_password=changeme # Service Accounts BIND password
search_dn=DC=dcloud,DC=cisco,DC=com # LDAP Search DN

[ldap_server_auto]
client=ad_client
ikey=DI*****      # Copy from Duo LDAP Proxy App Page
skey=*****        # Copy from Duo LDAP Proxy App Page
api_host=api-demodemo.duosecurity.com # Copy from Duo LDAP Proxy App Page
failmode=safe      # If proxy cant communicate with Duo cloud, allow auth with credentials only
port=1389          # Port the LDAP Proxy listen on
exempt_ou_1=CN=ldap,CN=Users,DC=dcloud,DC=cisco,DC=com # Exempt the Service Account from MFA
exempt_primary_bind=false # Exempt the Service Account from MFA on initial bind
allow_unlimited_binds=true # Allow multiple binds, needed to prevent "Attempt to bindRequest multiple

```

Etapa 4.

Em Intersight, você pode criar uma política LDAP que aponte para nosso proxy LDAP Duo com as configurações necessárias do Active Directory, como dn base, dn de ligação, ip do servidor LDAP, senha e assim por diante. A recomendação é primeiro apontar diretamente para o Active Directory e garantir que o funcione corretamente antes de alterar o servidor LDAP para o proxy LDAP Duo para facilitar a solução de problemas.

Políticas > LDAP > Map

Edit

General

Policy Details

Policy Details

Add policy details.

Enable LDAP

Base Settings

Base DN

DC=dccloud,DC=csico,DC=com

Timeout

180

Enable Encryption

Binding Parameters

Bind Method

Configure Credentials

Bind DN

CN=ldap,CN=Users,DC=dccloud,DC=csico,DC=com

Password

Search Parameters

Filter

sAMAccountName=\$userid

Group Attribute

memberOf

Attribute

memberOf

Group Authorization

Group Authorization

Nested Group Search

Nested Group Search Depth

128

All Platforms

UCS Server (Standard)

UCS Domain

Políticas > LDAP > Map

Edit

General

Policy Details

Policy Details

Search Parameters

Filter

sAMAccountName=\$userid

Group Attribute

memberOf

Attribute

memberOf

Group Authorization

Group Authorization

Nested Group Search

Nested Group Search Depth

128

Configure LDAP Servers

Server

3.135.250.11

Port

12956

Vendor

MSAD

Add New LDAP Group

Export

Name	Group DN	End Point Role
Domain Users	CN=Domain Users,CN=Users,DC=dccloud,DC=csico	admin

All Platforms

UCS Server (Standard)

UCS Domain

Verificar

No console do dispositivo, efetue login como o usuário LDAP que estava previamente inscrito no Duo.

Device Console

Username * ⓘ

mfauser

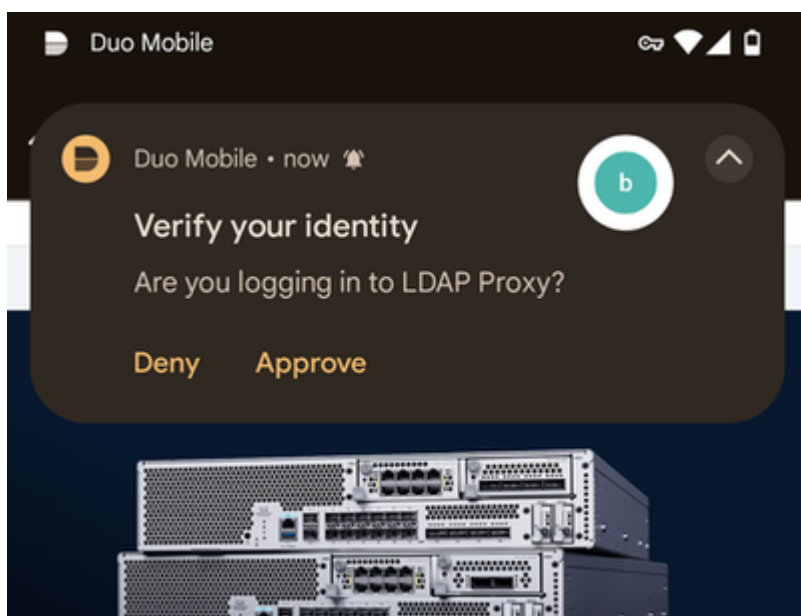
Password *

.....

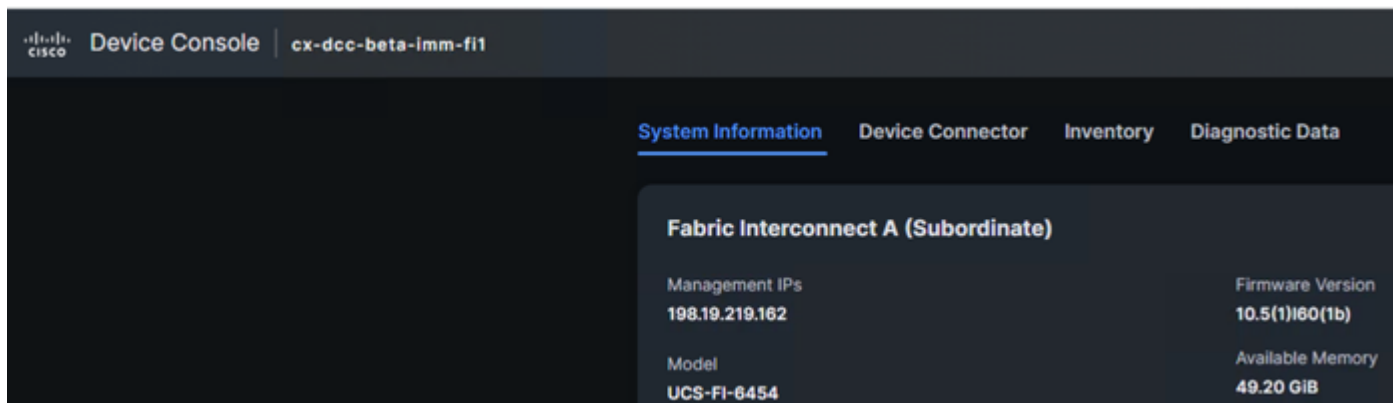
Show

Sign In

O usuário registrado pode receber um prompt em seu dispositivo para fazer login:



Depois que a solicitação for verificada, você poderá fazer login com êxito no console do dispositivo usando a autenticação de 2 fatores e o LDAP.



Troubleshooting

Os logs de proxy LDAP do Duo estão localizados em:

```
C:\Program Files\Duo Security Authentication Proxy\log\authproxy.log
```

Em Interconexão de malha no modo gerenciado de intervisão:

```
connect nxos
```

```
debug ldap
```

Informações Relacionadas

- [Guia do console do dispositivo](#)
- [O que é o Duo?](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.