

Configuración de la integración de la consola de dispositivos del modo gestionado de información (IMM) con autenticación multifactor LDAP y Duo

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Configurar](#)

[Diagrama de la red](#)

[Paso 1.](#)

[Paso 2.](#)

[Paso 3.](#)

[Paso 4.](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar la autenticación multifactor en la consola del dispositivo IMM usando LDAP y el proxy de autenticación Duo.

Prerequisites

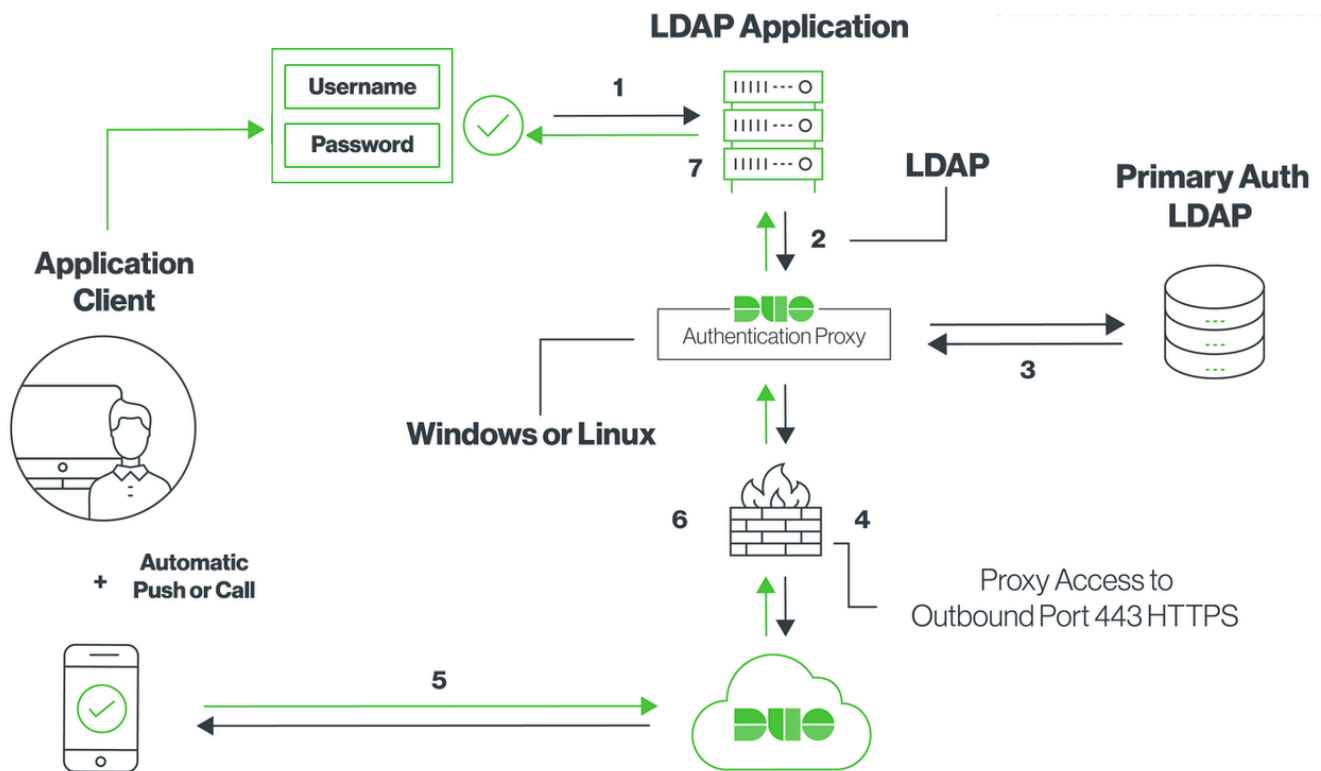
Requirements

Fabric Interconnects UCS en modo gestionado por intercambio (IMM).

Suscripción Duo con un usuario inscrito.

Configurar

Diagrama de la red



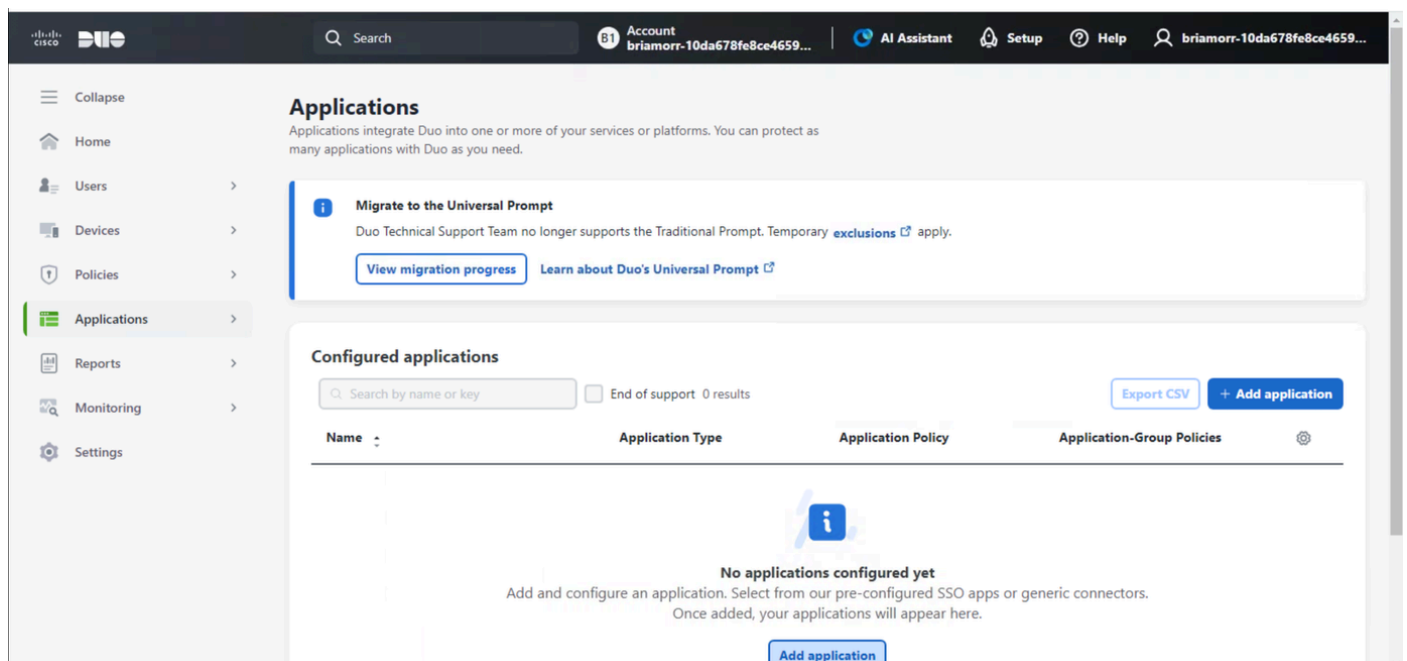
Paso 1.

Instale el proxy de autenticación doble en un servidor Windows al que puedan acceder tanto Active Directory como la consola del dispositivo IMM.

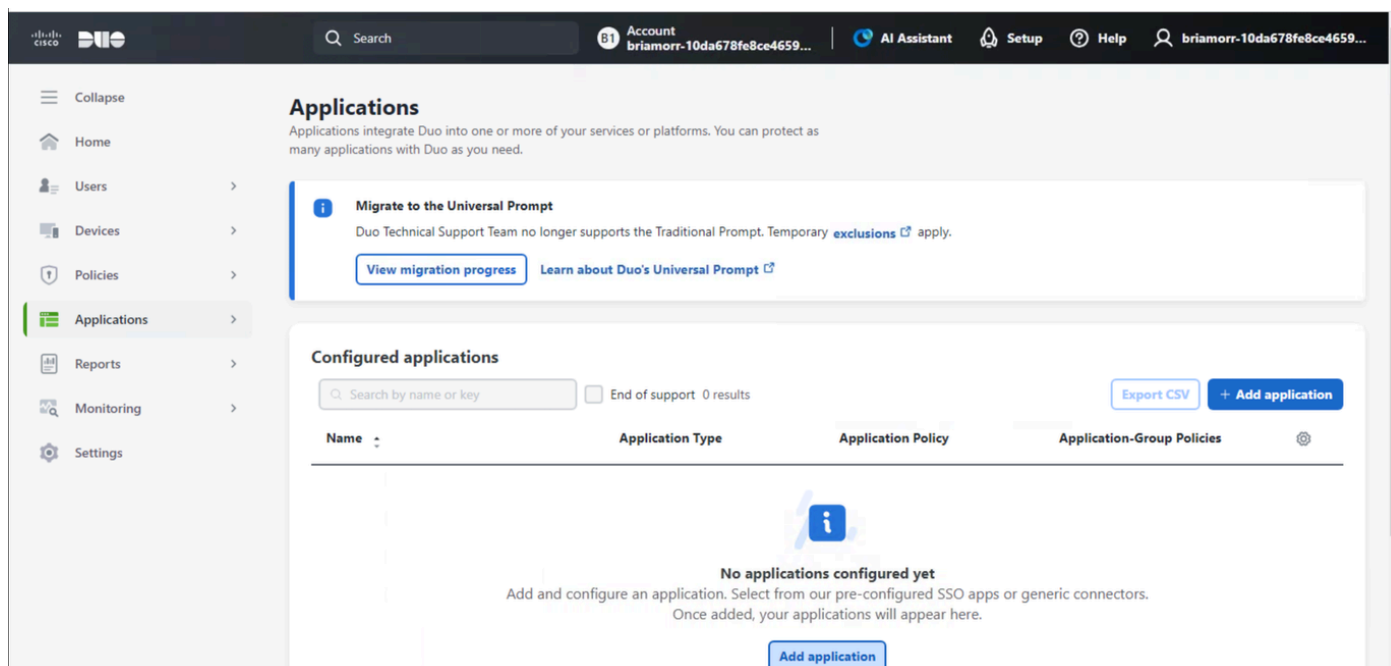
El proxy de autenticación Duo se puede encontrar [aquí](#).

Paso 2.

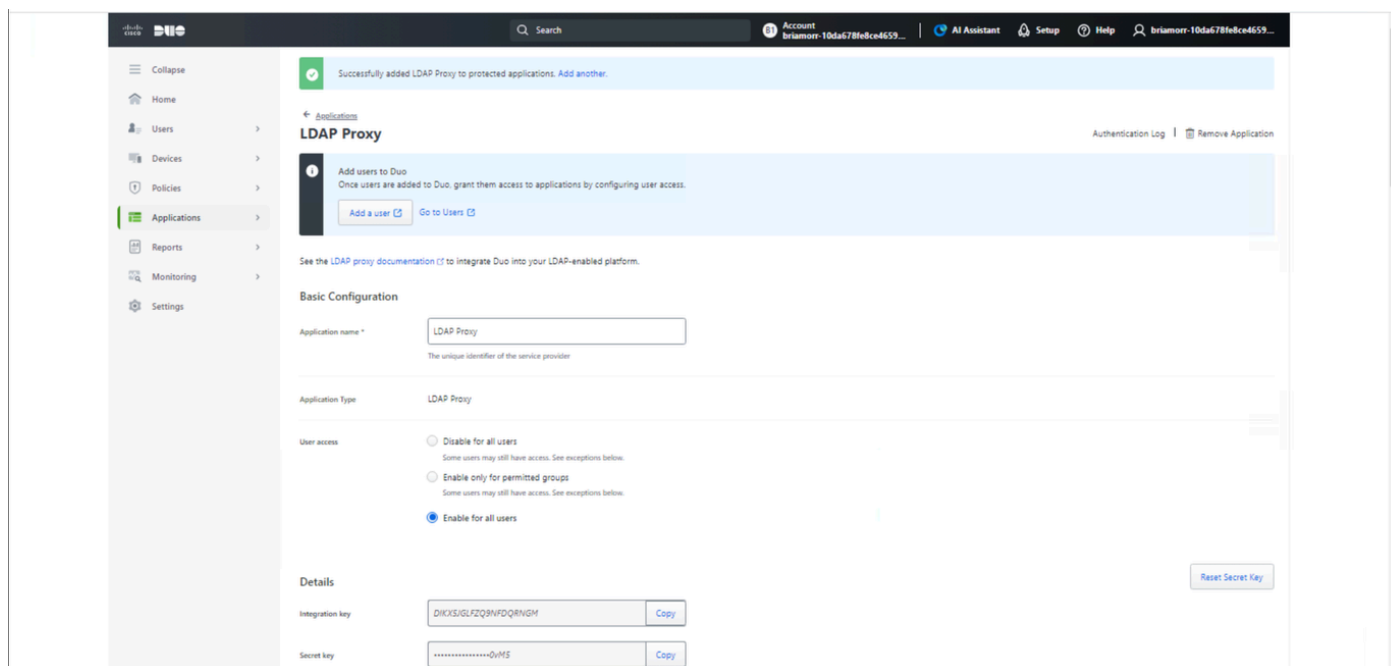
En nuestra instancia Duo , puede agregar una nueva aplicación.



Busque ldap y agregue el proxy LDAP para continuar.



En la aplicación LDAP Proxy, puede configurar un nombre de aplicación, habilitar para todos los usuarios y copiar la clave de integración, la clave secreta y el nombre de host de la API para su uso posterior.



Paso 3.

En el servidor donde instalamos el proxy de autenticación doble, puede configurar el administrador de proxy de autenticación doble.

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](#)

Configuración de Ejemplo de Proxy de Autenticación Duo:



Nota: # comentarios añadidos para facilitar la lectura.

```

[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

```

Paso 4.

En Intersight, puede crear una política LDAP que apunte a nuestro proxy LDAP Duo con la configuración necesaria de Active Directory como base dn, bind dn, IP del servidor LDAP, contraseña, etc. La recomendación es apuntar primero directamente a Active Directory y asegurarse de que funcione correctamente antes de cambiar el servidor LDAP a Duo LDAP proxy para facilitar la resolución de problemas.

The screenshot shows the 'Edit' page for a policy in Intersight, specifically the 'Policy Details' tab. The 'General' tab is selected. The 'Policy Details' section includes the following fields:

- Enable LDAP:** A toggle switch that is currently turned on.
- Base Settings:**
 - Base DN:** A text field containing 'DC=dccloud,DC=csico,DC=com'.
 - Timeout:** A text field containing '180'.
- Enable Encryption:** A toggle switch that is currently turned off.
- Binding Parameters:**
 - Bind Method:** A dropdown menu showing 'Configure Credentials'.
 - Bind DN:** A text field containing 'CN=idap,CN=Users,DC=dccloud,DC=csico,DC=com'.
 - Password:** A text field containing '*****'.
- Search Parameters:**
 - Filter:** A text field containing 'sAMAccountName=\$userid'.
 - Group Attribute:** A text field containing 'memberOf'.
 - Attribute:** A text field containing 'memberOf'.
- Group Authorization:**
 - Group Authorization:** A toggle switch that is currently turned on.
 - Nested Group Search:** A checkbox that is currently checked.
 - Nested Group Search Depth:** A text field containing '128'.

The screenshot shows the 'Edit' page for a policy in Intersight, specifically the 'Policy Details' tab. The 'General' tab is selected. The 'Policy Details' section includes the following fields:

- Search Parameters:**
 - Filter:** A text field containing 'sAMAccountName=\$userid'.
 - Group Attribute:** A text field containing 'memberOf'.
 - Attribute:** A text field containing 'memberOf'.
- Group Authorization:**
 - Group Authorization:** A toggle switch that is currently turned on.
 - Nested Group Search:** A checkbox that is currently checked.
 - Nested Group Search Depth:** A text field containing '128'.
- Configure LDAP Servers:**
 - Server:** A text field containing '3.135.250.11'.
 - Port:** A text field containing '12956'.
 - Vendor:** A dropdown menu showing 'MSAD'.
- Add New LDAP Group:** A button.
- LDAP Groups Table:**

Name	Group DN	End Point Role
Domain Users	CN=Domain Users,CN=Users,DC=dccloud,DC=csico	admin
- Export:** A button.

Verificación

En la consola del dispositivo, inicie sesión como el usuario LDAP que estaba previamente inscrito en Duo.

Device Console

Username * ⓘ

mfauser

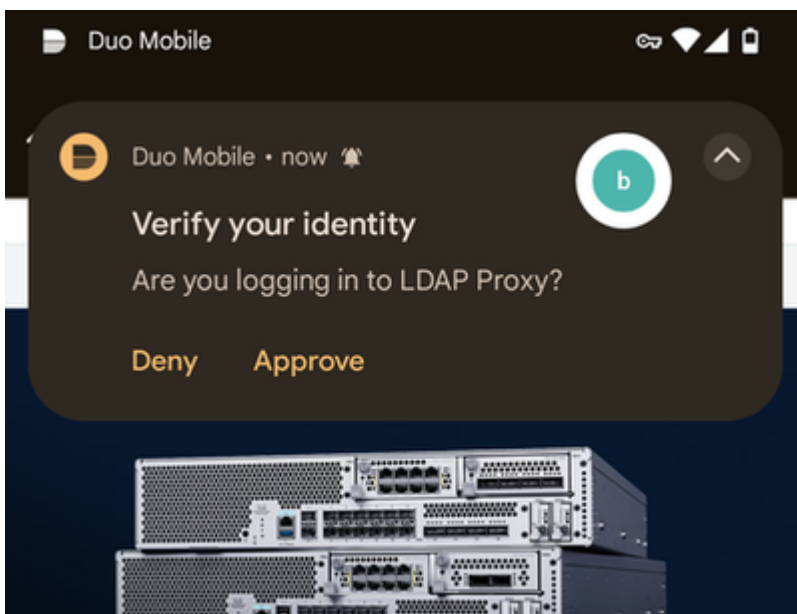
Password *

.....

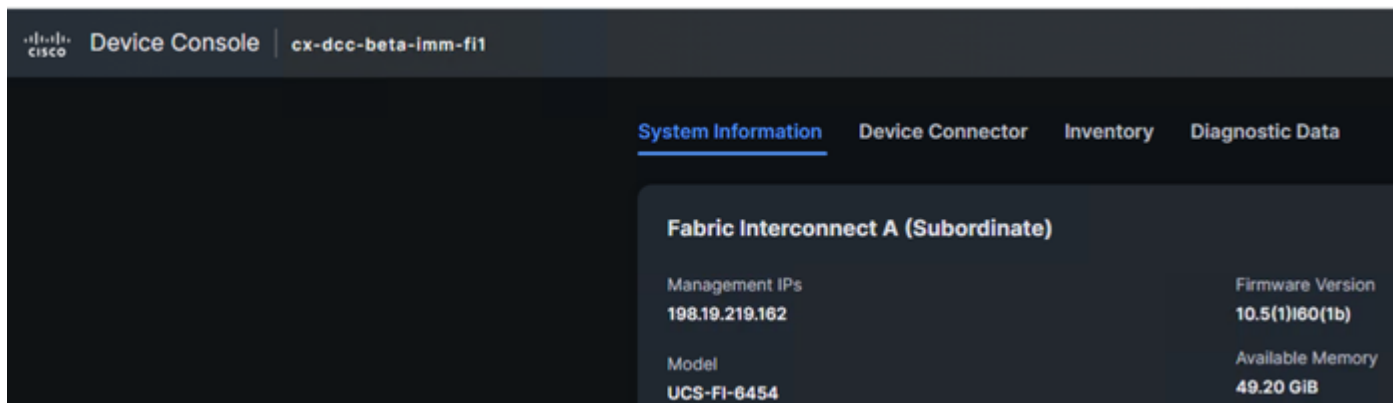
Show

Sign In

El usuario inscrito puede obtener una indicación en su dispositivo para iniciar sesión:



Una vez verificada la solicitud, puede iniciar sesión correctamente en la consola del dispositivo mediante la autenticación de factor 2 y LDAP.



Troubleshoot

Los registros de proxy LDAP dobles se encuentran en:

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

En Intersight Managed Mode Fabric Interconnect:

connect nxos

debug ldap

Información Relacionada

- [Guía de consola del dispositivo](#)
- [¿Qué es Duo?](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).