Configure Intersight Managed Mode (IMM) Device Console Integration with LDAP and Duo Multifactor Authentication

Contents

Introduction

This document describes how to configure multifactor authentication on the IMM Device Console using LDAP and The Duo authentication proxy.

Prerequisites

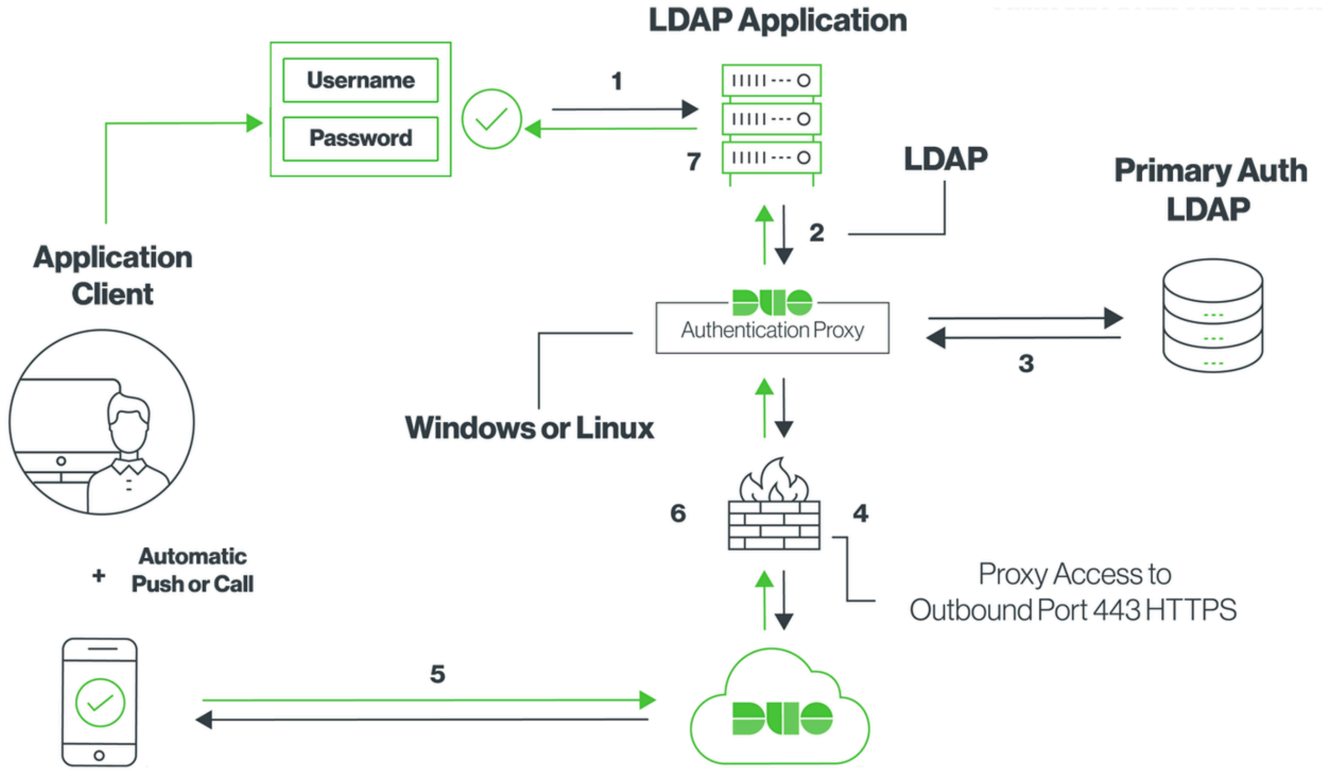
Requirements

UCS Fabric Interconnects in Intersight Managed Mode (IMM).

Duo subscription with an enrolled user.

Configure

Network Diagram



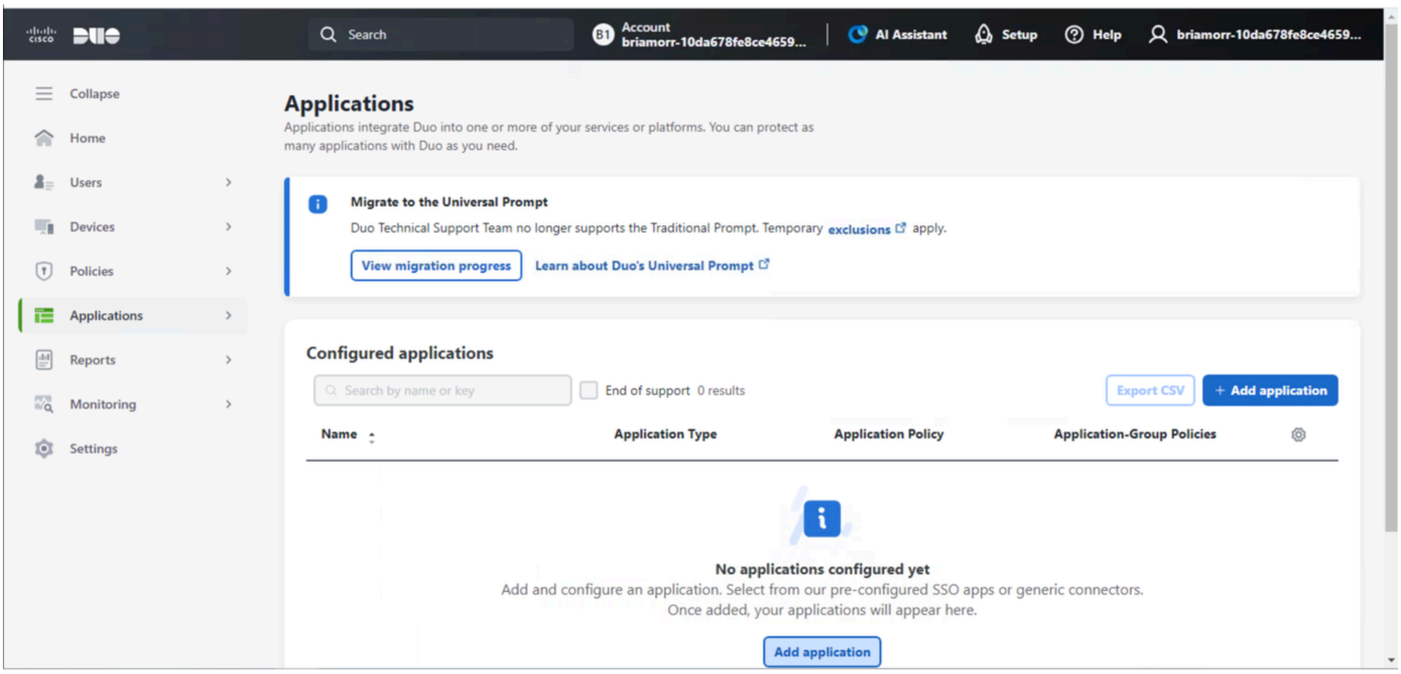
Step 1.

Install the Duo Authentication Proxy on a Windows server that is accessible to both the Active Directory and the IMM Device Console.

The Duo authentication proxy can be found [here.](#)

Step 2.

In our Duo instance , you can add a new application.



Applications

Applications integrate Duo into one or more of your services or platforms. You can protect as many applications with Duo as you need.

Migrate to the Universal Prompt

Duo Technical Support Team no longer supports the Traditional Prompt. Temporary exclusions apply.

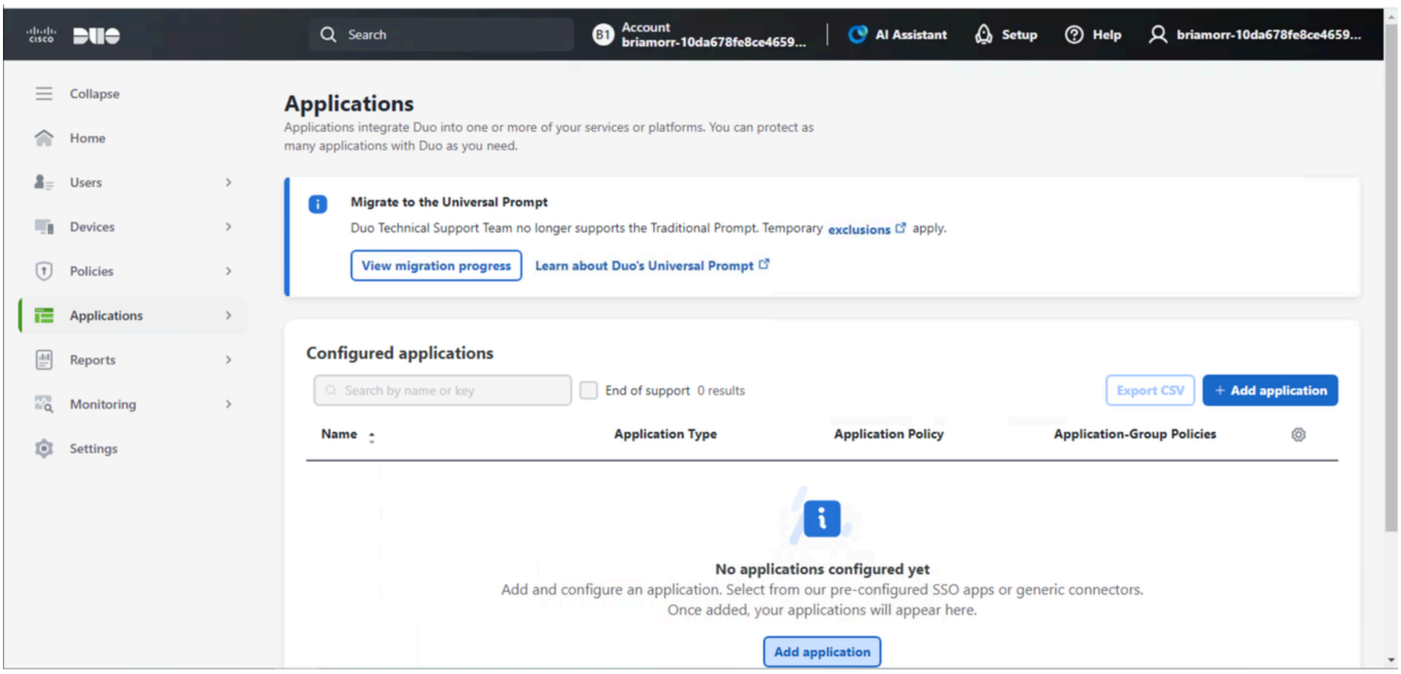
Configured applications

Name	Application Type	Application Policy	Application-Group Policies

No applications configured yet

Add and configure an application. Select from our pre-configured SSO apps or generic connectors. Once added, your applications will appear here.

Search for ldap and add the **LDAP Proxy** to continue.



Applications

Applications integrate Duo into one or more of your services or platforms. You can protect as many applications with Duo as you need.

Migrate to the Universal Prompt

Duo Technical Support Team no longer supports the Traditional Prompt. Temporary exclusions apply.

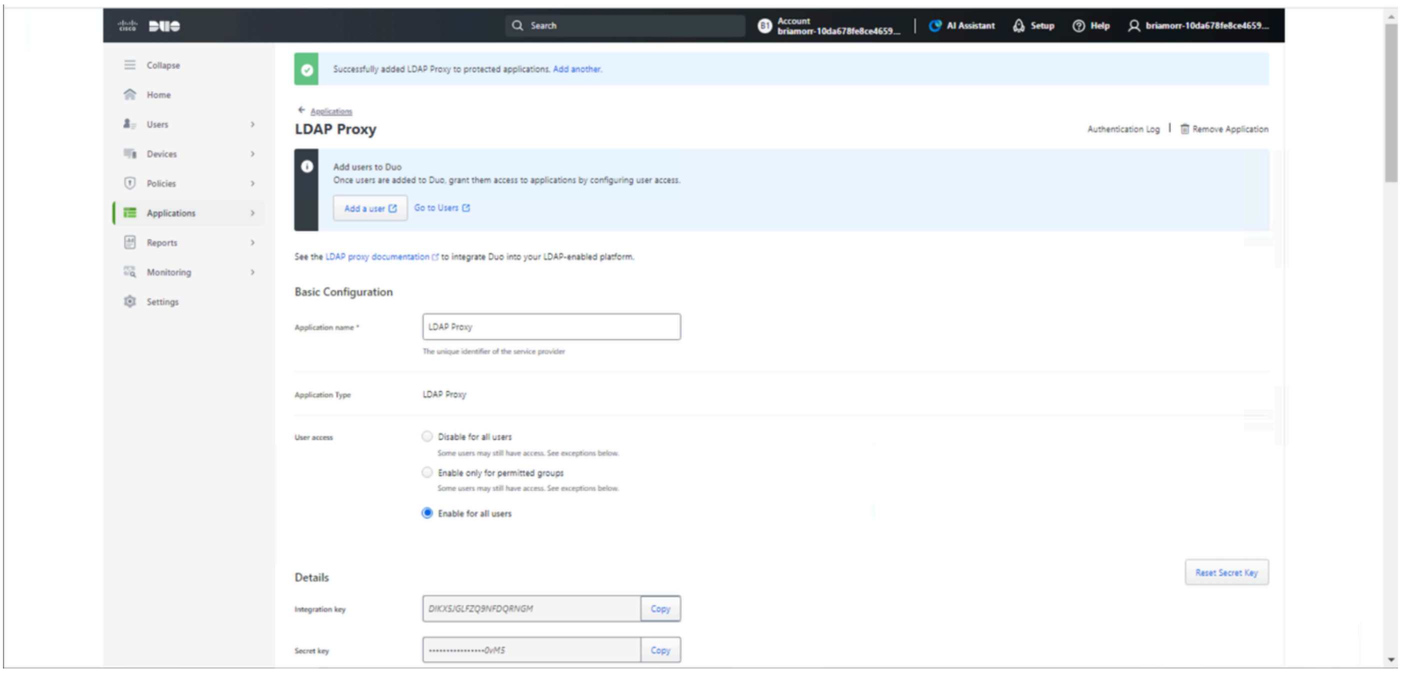
Configured applications

Name	Application Type	Application Policy	Application-Group Policies

No applications configured yet

Add and configure an application. Select from our pre-configured SSO apps or generic connectors. Once added, your applications will appear here.

Under the LDAP Proxy application, you can configure an application name, enable for all users, and copy down the integration key, secret key, and API hostname for use later on.



Successfully added LDAP Proxy to protected applications. Add another.

LDAP Proxy

Add users to Duo

Once users are added to Duo, grant them access to applications by configuring user access.

See the LDAP proxy documentation to integrate Duo into your LDAP-enabled platform.

Basic Configuration

Application name *: LDAP Proxy

The unique identifier of the service provider

Application Type: LDAP Proxy

User access:

○ Disable for all users

Some users may still have access. See exceptions below.

○ Enable only for permitted groups

Some users may still have access. See exceptions below.

● Enable for all users

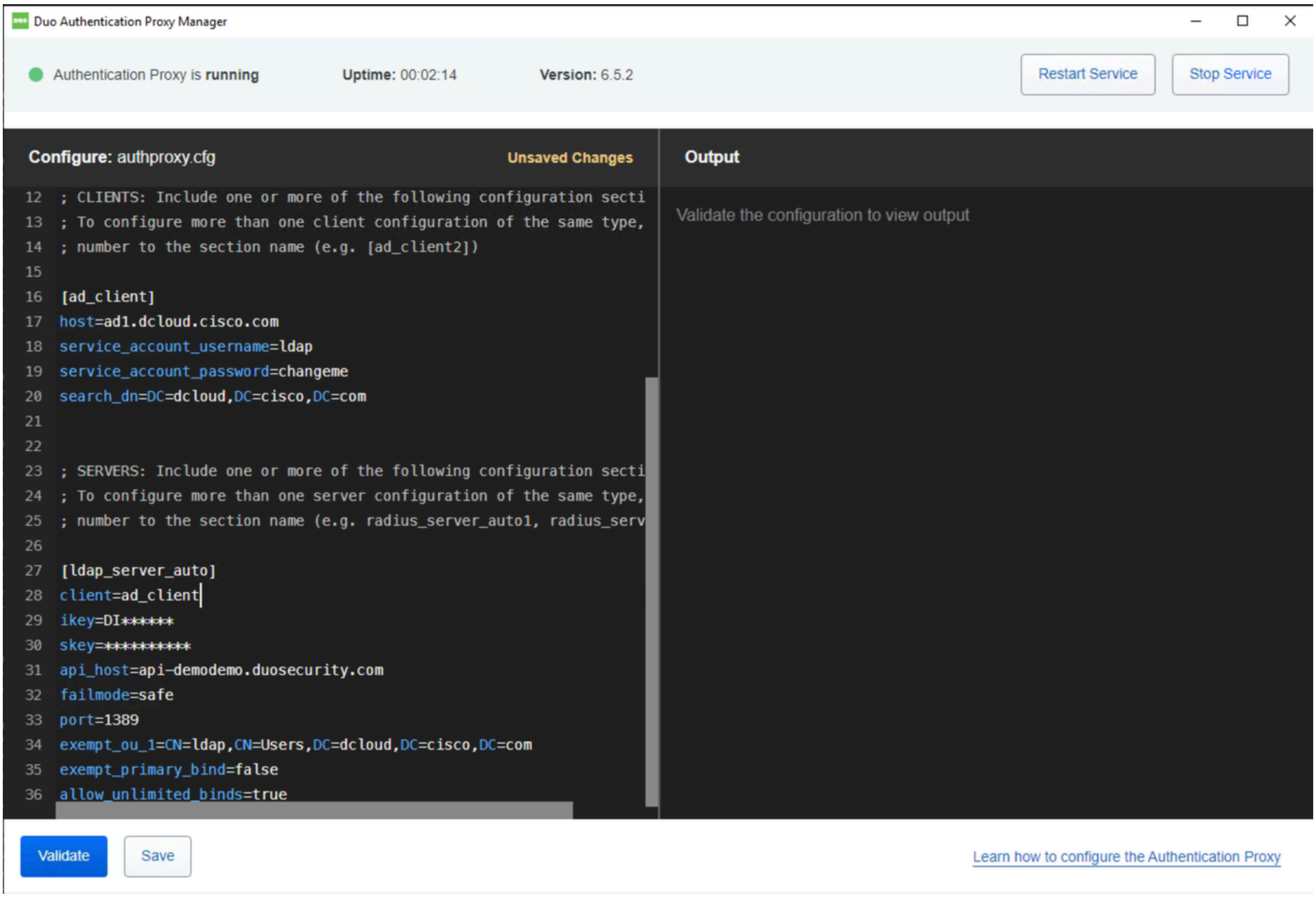
Details

Integration key: DIKXSJGLFZQ9NFDQRNGM

Secret key: ••••••••••••••••0vM5

Step 3.

Back on the server where we installed the Duo Authentication Proxy, you can configure the 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
Output
Validate the configuration to view output
Validate
Save
Learn how to configure the Authentication Proxy

```
; CLIENTS: Include one or more of the following configuration secti
; To configure more than one client configuration of the same type,
; number to the section name (e.g. [ad_client2])

[ad_client]
host=ad1.dcloud.cisco.com
service_account_username=ldap
service_account_password=changeme
search_dn=DC=dcloud,DC=cisco,DC=com


; SERVERS: Include one or more of the following configuration secti
; To configure more than one server configuration of the same type,
; number to the section name (e.g. radius_server_auto1, radius_serv

[ldap_server_auto]
client=ad_client
ikey=DI******
skey=**********
api_host=api-demodemo.duosecurity.com
failmode=safe
port=1389
exempt_ou_1=CN=ldap,CN=Users,DC=dcloud,DC=cisco,DC=com
exempt_primary_bind=false
allow_unlimited_binds=true
```

Duo Authentication Proxy Sample Configuration:

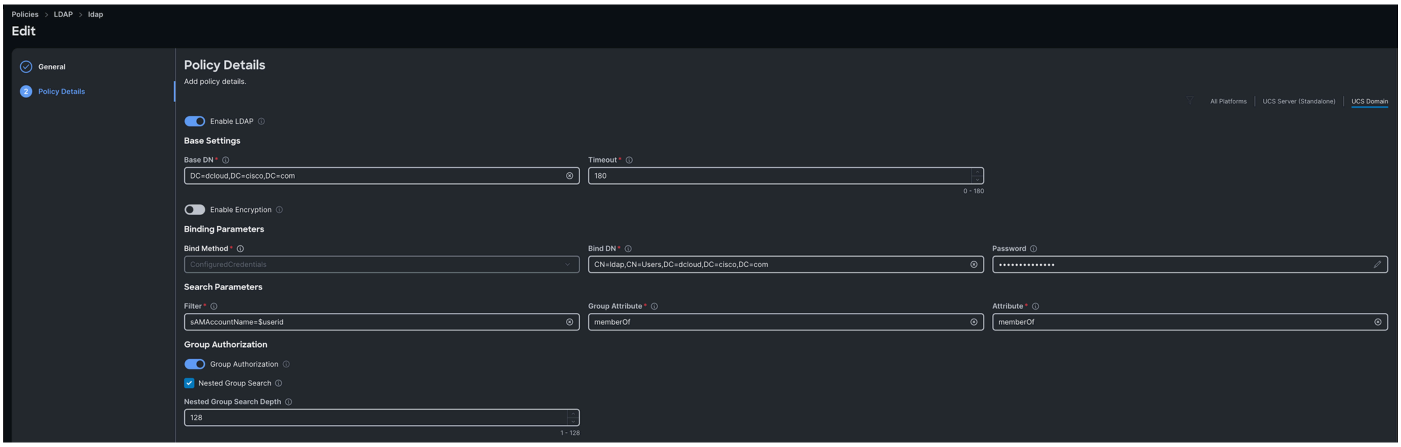
Note: # comments added for readability.

```
[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
```

Step 4.

In Intersight, you can then create a LDAP policy that points to our Duo LDAP proxy with the necessary Active Directory settings like base dn, bind dn, LDAP server ip, password and so on. The recommendation is to first point directly to Active Directory and ensure that works correctly before changing the LDAP server to the Duo LDAP proxy to make troubleshooting easier.



Policy Details
Add policy details.

Enable LDAP: on

Base Settings

Base DN *: DC=dcloud,DC=cisco,DC=com
Timeout *: 180 (0 - 180)

Enable Encryption: off

Binding Parameters

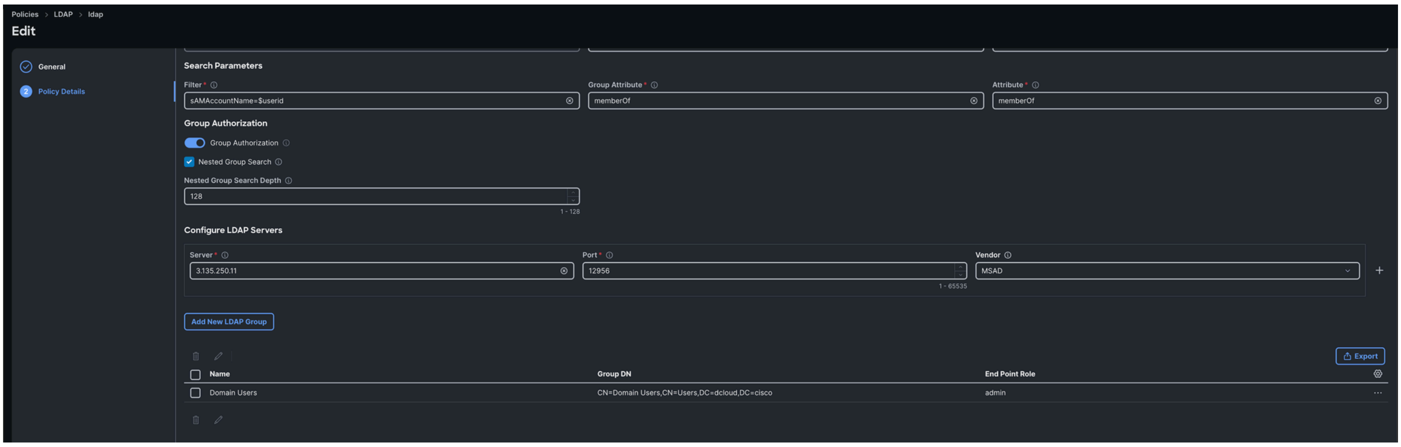
Bind Method *: ConfiguredCredentials
Bind DN *: CN=ldap,CN=Users,DC=dcloud,DC=cisco,DC=com
Password: ••••••••••••••

Search Parameters

Filter *: sAMAccountName=$userid
Group Attribute *: memberOf
Attribute *: memberOf

Group Authorization

Group Authorization: on
☑ Nested Group Search
Nested Group Search Depth: 128 (1 - 128)



Search Parameters

Filter *: sAMAccountName=$userid
Group Attribute *: memberOf
Attribute *: memberOf

Group Authorization

Group Authorization: on
☑ Nested Group Search
Nested Group Search Depth: 128 (1 - 128)

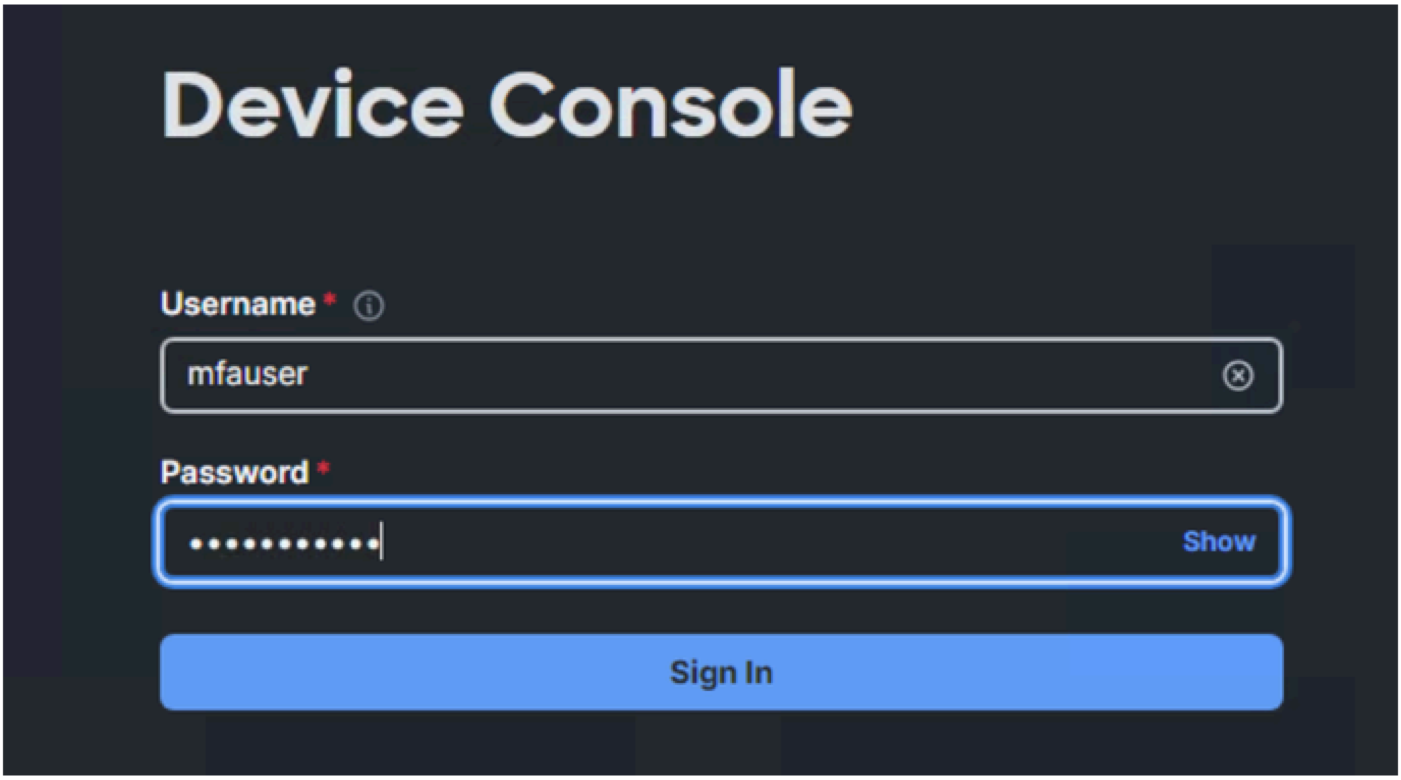
Configure LDAP Servers

Server *: 3.135.250.11
Port *: 12956 (1 - 65535)
Vendor: MSAD

□	Name	Group DN	End Point Role
□	Domain Users	CN=Domain Users,CN=Users,DC=dcloud,DC=cisco	admin

Verify

On device console, logon as the LDAP user that was previously enrolled in Duo.

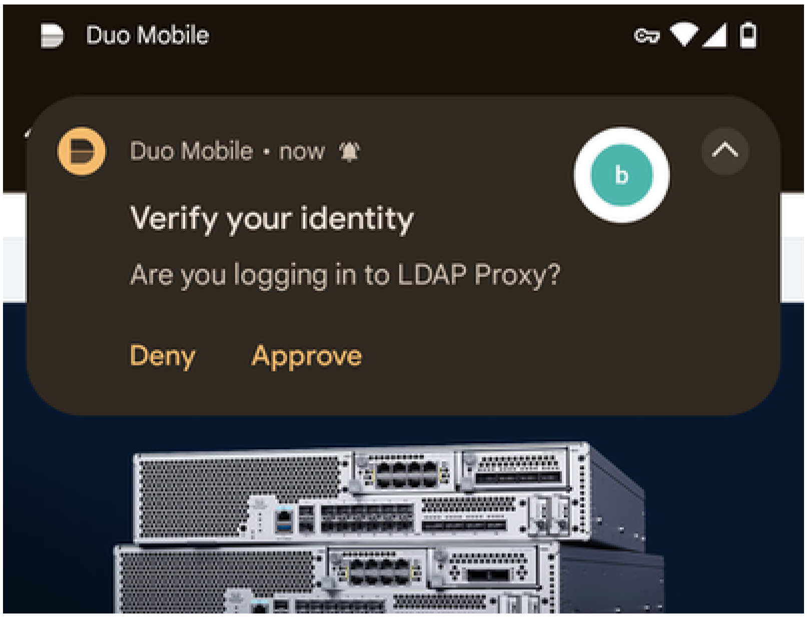


Device Console

Username * mfauser

Password * •••••••••••

The enrolled user can then get a prompt on their device to login:

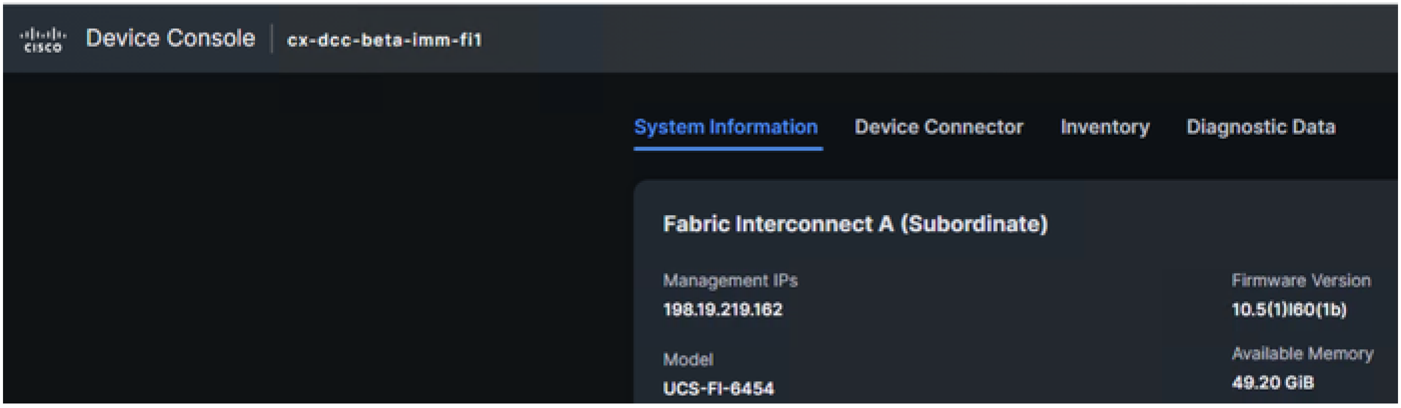


Duo Mobile • now

Verify your identity

Are you logging in to LDAP Proxy?

Once the request is verified, you can sucesfully log into the device console using 2-factor authentication and LDAP.



Fabric Interconnect A (Subordinate)

Management IPs
198.19.219.162

Firmware Version
10.5(1)I60(1b)

Model
UCS-FI-6454

Available Memory
49.20 GiB

Troubleshoot

Duo LDAP proxy logs are located at:

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

On Intersight Managed Mode Fabric Interconnect:

```
connect nxos

debug ldap
```

Related Information

- [Device Console Guide]()
- [What is Duo?]()