配置與LDAP和Duo Multifactor Authentication整合的Intersight管理模式(IMM)裝置控制檯

目錄

簡介

本文檔介紹如何使用LDAP和Duo身份驗證代理在IMM裝置控制檯上配置多重身份驗證。

必要條件

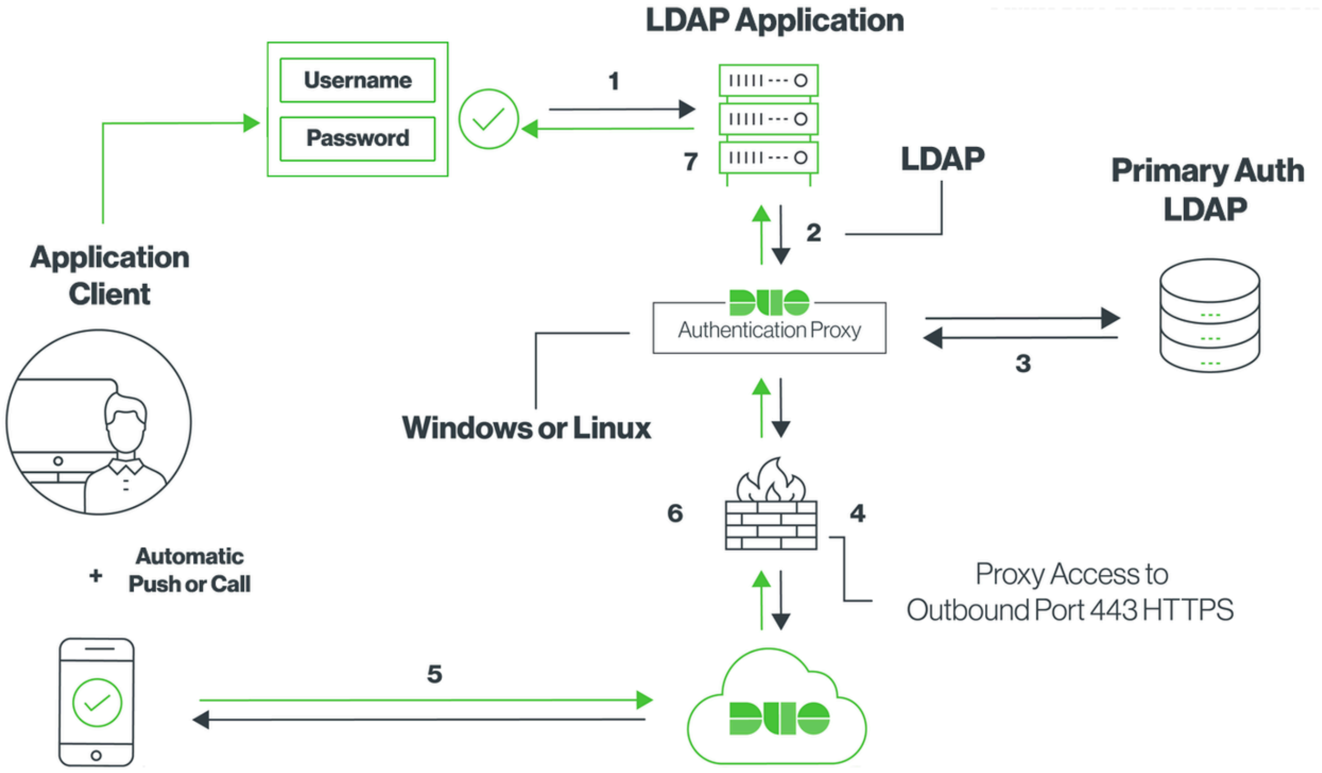
需求

Intersight託管模式(IMM)下的UCS交換矩陣互聯。

註冊使用者的Duo訂閱。

設定

網路圖表



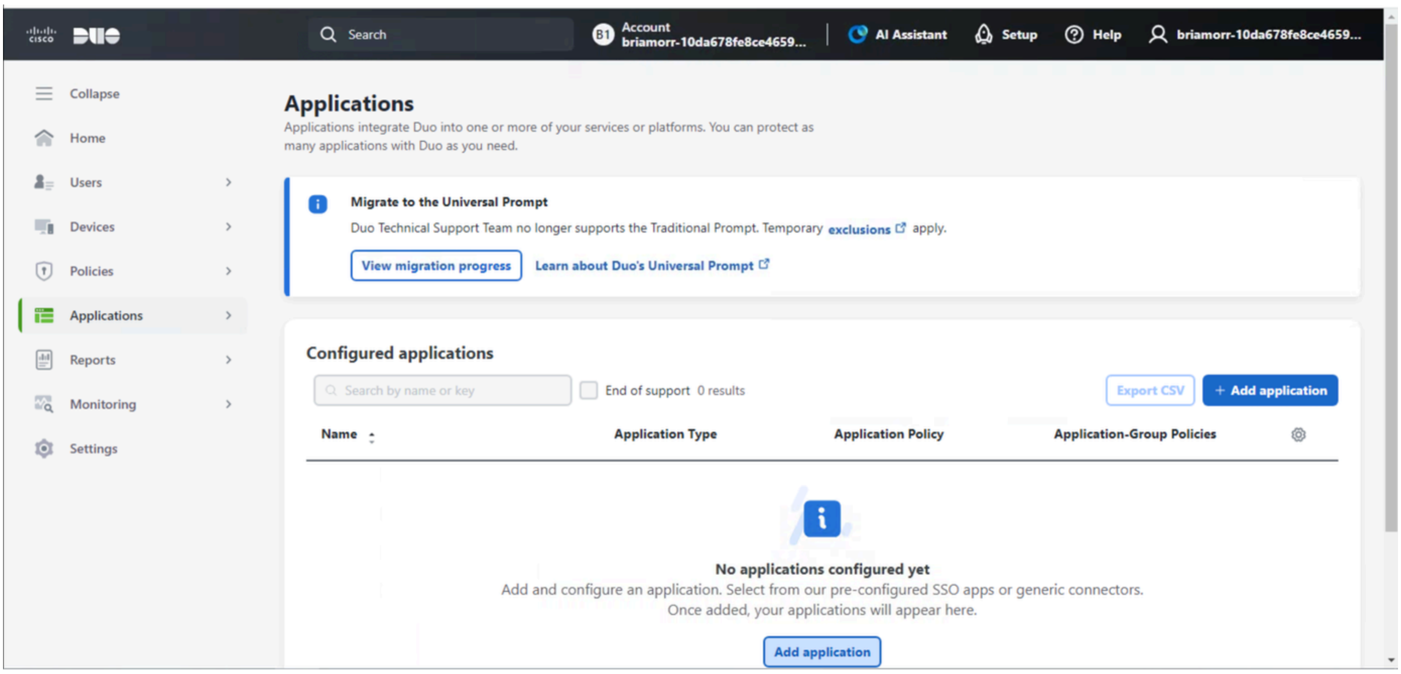
步驟 1.

在Active Directory和IMM裝置控制檯都可以訪問的Windows伺服器上安裝Duo Authentication Proxy。

此處可以找到Duo身份驗證代理。

步驟 2.

在我們的Duo例項中，可以新增新的應用程式。



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.

View migration progress   Learn about Duo's Universal Prompt

Configured applications

Search by name or key   □ End of support 0 results   Export CSV   + Add application

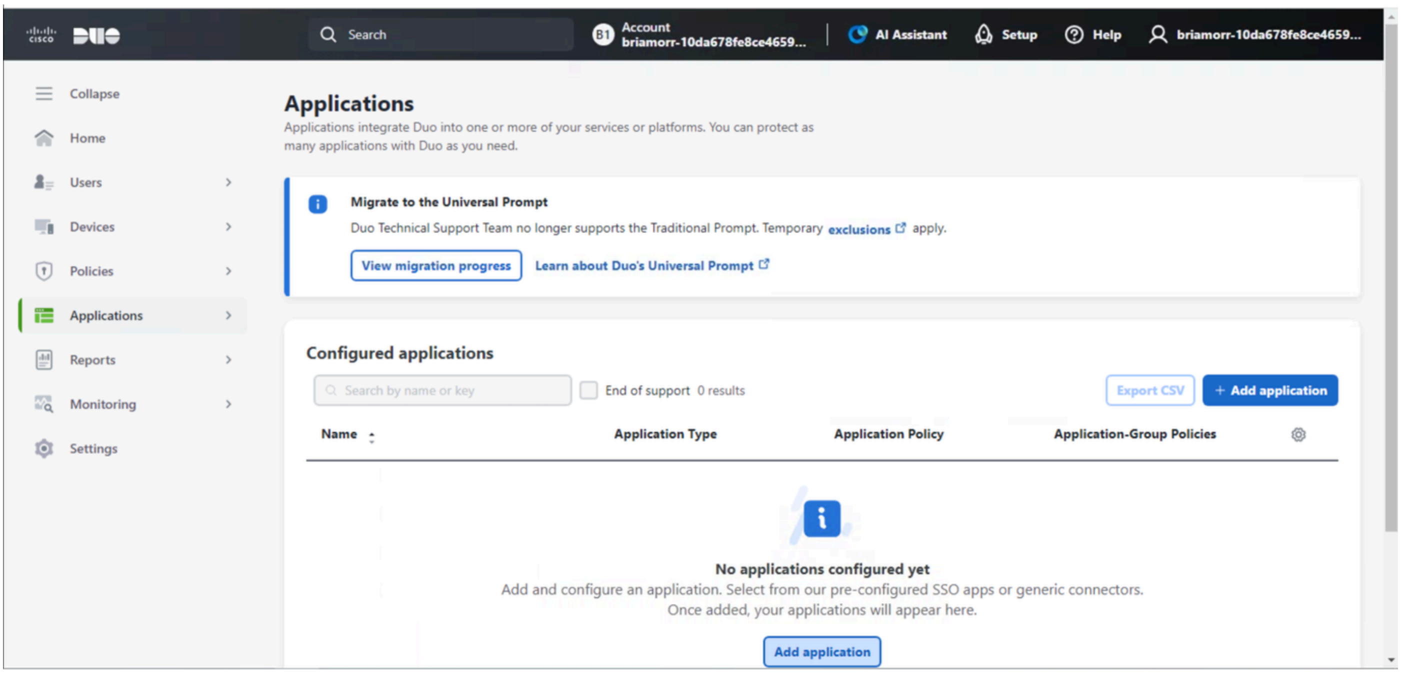
Name	Application Type	Application Policy	Application-Group Policies

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.

Add application

搜尋ldap並新增LDAP代理以繼續。



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.

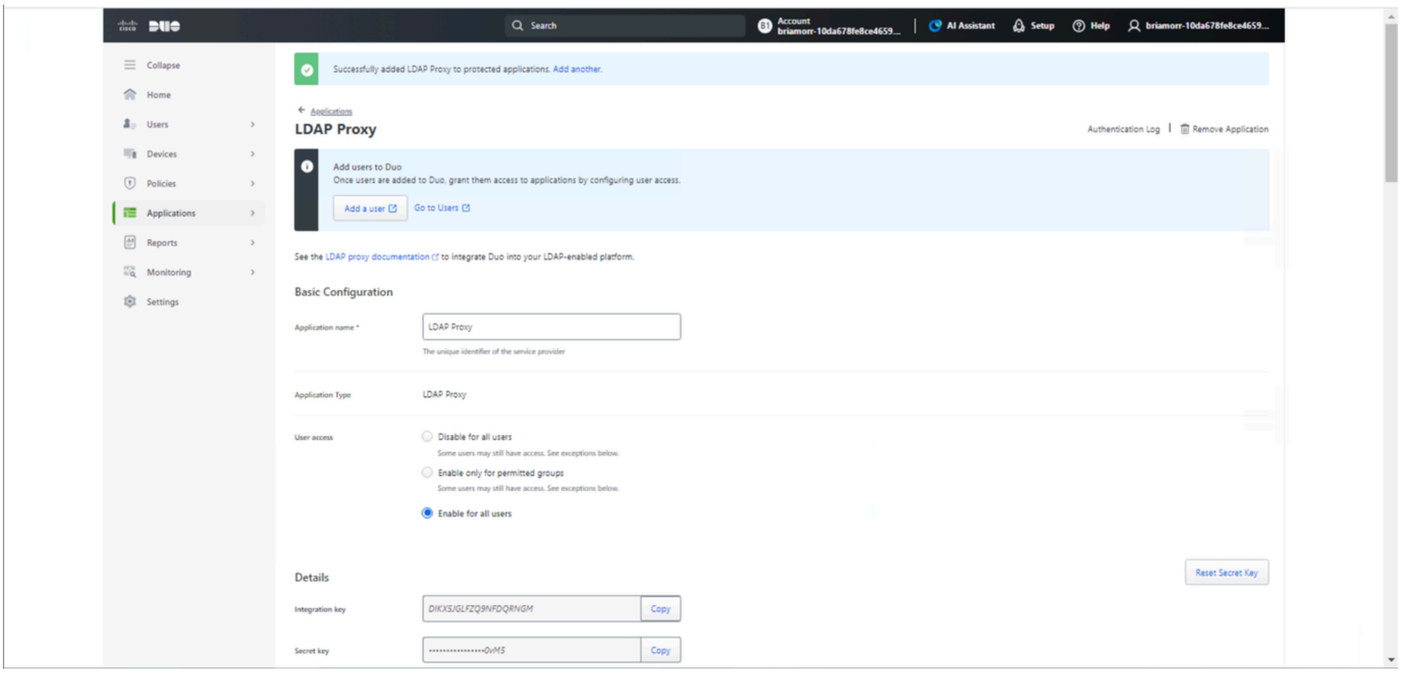
Configured applications

□ End of support 0 results

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.

在LDAP代理應用程式下，您可以配置應用程式名稱，為所有使用者啟用，並複製整合金鑰、金鑰和API主機名供以後使用。



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

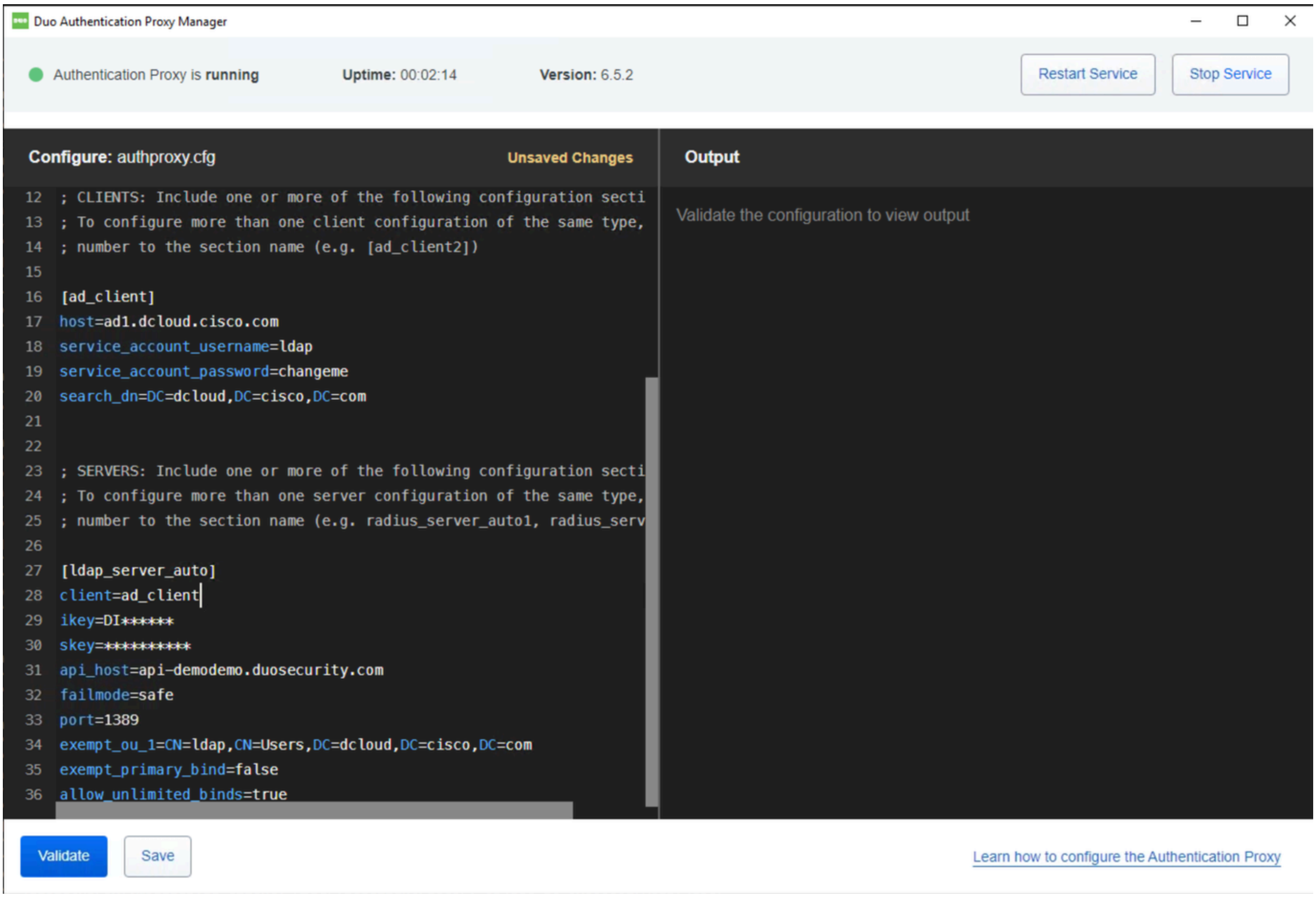
Details

Integration key: DIKX5JGLFZQ9NFDQRNGM

Secret key: ••••••••••••••••0vM5

步驟 3.

在安裝了Duo Authentication Proxy的伺服器上，您可以配置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示例配置：

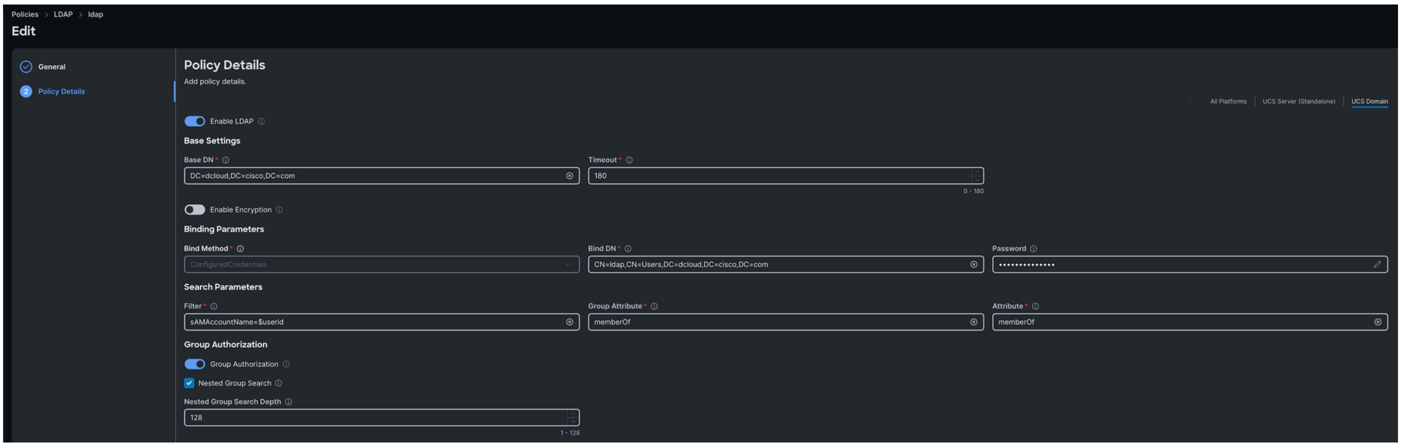
附註：#為便於閱讀而新增的註釋。

```
[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
```

步驟 4.

在Intersight中，然後可以建立一個LDAP策略，該策略使用必要的Active Directory設定（如基本dn、繫結dn、LDAP伺服器ip、密碼等）指向我們的Duo LDAP代理。　建議先直接指向Active Directory並確保其正常工作，然後再將LDAP伺服器更改為Duo LDAP代理，以簡化故障排除。



Policy Details
Add policy details.

Enable LDAP: on

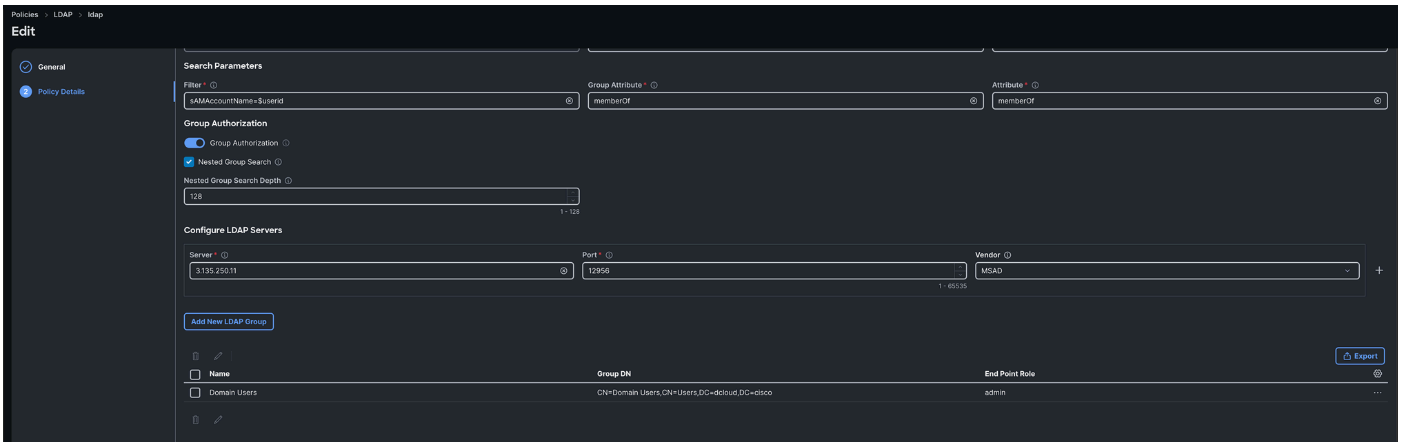
Base Settings
Base DN *: DC=dcloud,DC=cisco,DC=com
Timeout *: 180 (0 - 180)

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

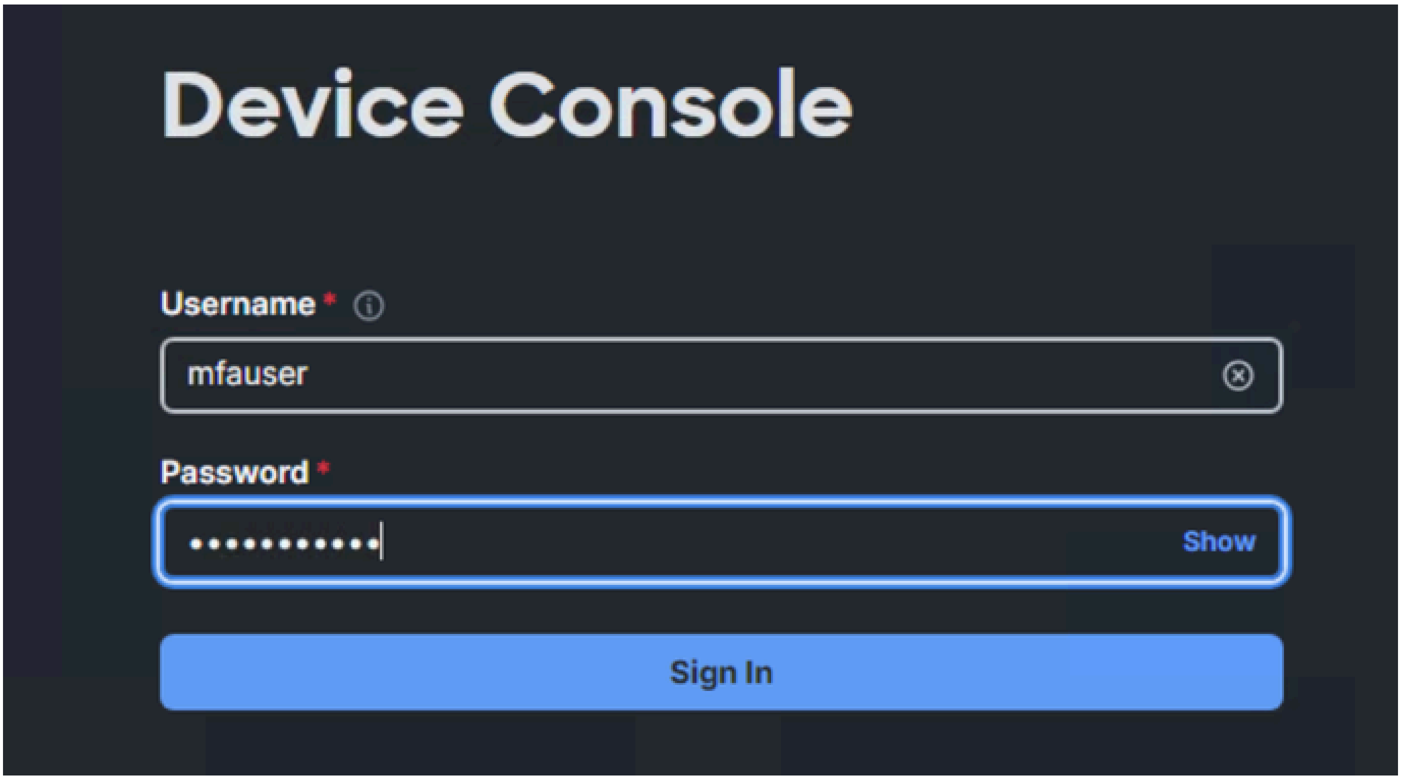
Group Authorization
Group Authorization: on
☑ Nested Group Search
Nested Group Search Depth: 128 (1 - 128)

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

驗證

在裝置控制檯上，以以前在Duo中註冊的LDAP使用者身份登入。



Device Console

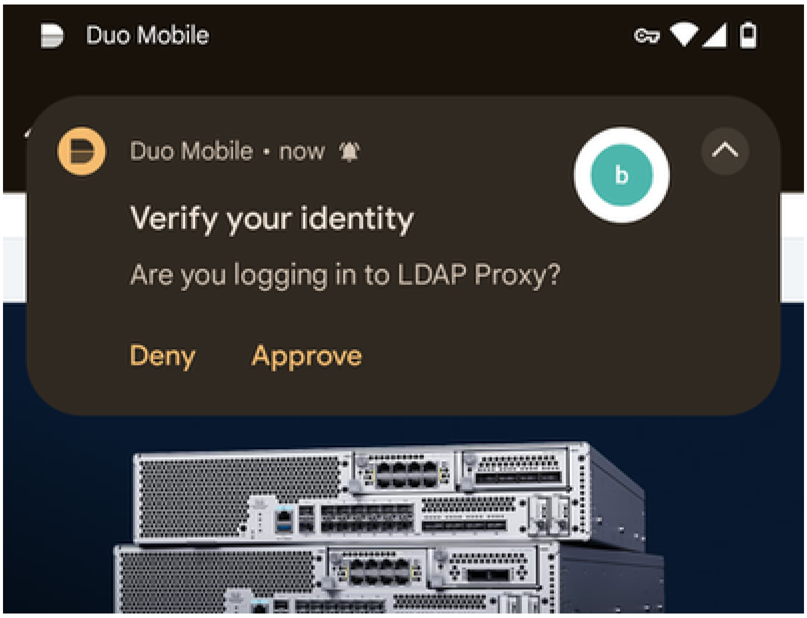
Username *

mfauser

Password *

••••••••••••

註冊使用者隨後可以在其裝置上獲得登入提示：

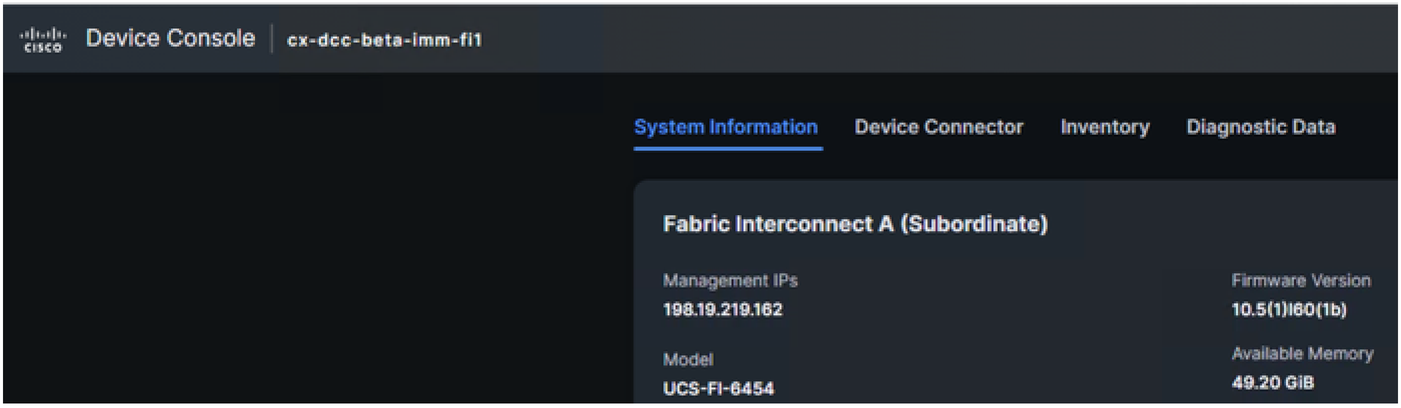


Duo Mobile • now

Verify your identity

Are you logging in to LDAP Proxy?

驗證請求後，即可使用2因素身份驗證和LDAP成功登入到裝置控制檯。



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

疑難排解

Duo LDAP代理日誌位於：

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

在Intersight管理模式交換矩陣互聯上：

```
connect nxos

debug ldap
```

相關資訊

- [裝置控制檯指南]
- [什麼是Duo?]

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。