

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](#)

[必要條件](#)

[需求](#)

[設定](#)

[網路圖表](#)

[步驟 1.](#)

[步驟 2.](#)

[步驟 3.](#)

[步驟 4.](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

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

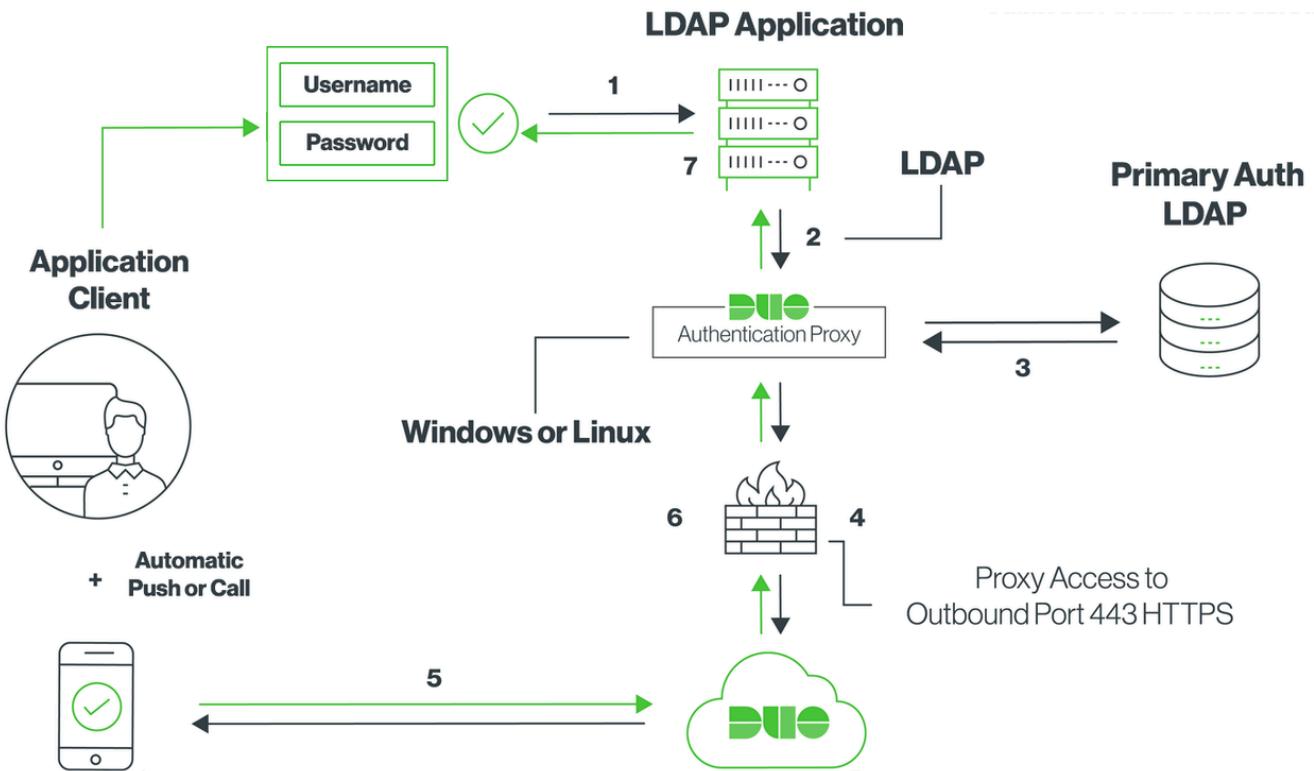
需求

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項目中，可以新增新的應用程式。

The screenshot shows the Duo Admin Panel interface with the following details:

- Left Sidebar:** Shows navigation links for Home, Users, Devices, Policies, Applications (selected), Reports, Monitoring, and Settings.
- Header:** Displays the account name "briamorr-10da678fe8ce4659...", AI Assistant, Setup, Help, and search bar.
- Middle Section - Applications:**
 - A message box: "Migrate to the Universal Prompt" (Info icon) - Duo Technical Support Team no longer supports the Traditional Prompt. Temporary [exclusions](#) apply. Buttons: "View migration progress" and "Learn about Duo's Universal Prompt".
 - A "Configured applications" table header with columns: Name, Application Type, Application Policy, Application-Group Policies, and a gear icon.
 - A message at the bottom: "No applications configured yet" with instructions: "Add and configure an application. Select from our pre-configured SSO apps or generic connectors. Once added, your applications will appear here." A "Add application" button is located below this message.

搜尋ldap並新增LDAP代理以繼續。

The screenshot shows the Duo Authentication Manager's Applications page. The sidebar on the left includes options like Home, Users, Devices, Policies, Applications (which is selected), Reports, Monitoring, and Settings. The main content area has a heading 'Applications' with a sub-section 'Migrate to the Universal Prompt'. It mentions that Duo Technical Support no longer supports the Traditional Prompt, and temporary exclusions apply. Below this are two buttons: 'View migration progress' and 'Learn about Duo's Universal Prompt'. The 'Configured applications' section contains a search bar, a note about the end of support (0 results), and three columns: Name, Application Type, Application Policy, and Application-Group Policies. At the bottom, there is an 'Add application' button and a large informational icon with the text 'No applications configured yet'.

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。

The screenshot shows the configuration of the 'LDAP Proxy' application. The sidebar on the left is identical to the previous screenshot. The main content area shows a success message: 'Successfully added LDAP Proxy to protected applications. Add another.' Below this is the 'LDAP Proxy' configuration page. It has a 'Basic Configuration' section where 'Application name' is set to 'LDAP Proxy' and 'Application Type' is 'LDAP Proxy'. Under 'User access', the radio button 'Enable for all users' is selected. In the 'Details' section, there are fields for 'Integration key' (containing 'DICKSUGLZQ9NFDQRNGH') and 'Secret key' (containing '.....QvMS'), each with a 'Copy' button. There is also a 'Reset Secret Key' button.

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 |
|--|-----------------|---|
| <pre> 12 ; CLIENTS: Include one or more of the following configuration sections 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 sections 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 </pre> | Unsaved Changes | Validate the configuration to view output |

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

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 can't 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。

The screenshot shows the 'Edit' screen for a policy named 'ldap'. The 'Policy Details' tab is selected. Under 'General', 'Enable LDAP' is checked. In 'Base Settings', 'Base DN' is set to 'DC=dccloud,DC=cisco,DC=com' and 'Timeout' is set to '180'. Under 'Binding Parameters', 'Bind Method' is set to 'Configured Credentials'. 'Search Parameters' include 'Filter' (sAMAccountName=\$userid), 'Group Attribute' (memberOf), and 'Attribute' (memberOf). Under 'Group Authorization', 'Nested Group Search' is checked. 'Nested Group Search Depth' is set to '128'. The top right corner shows 'All Platforms', 'UCS Server (Standalone)', and 'UCS Domain'.

The screenshot shows the 'Edit' screen for an LDAP policy. The 'Configure LDAP Servers' section is visible. It includes fields for 'Server' (3.135.250.11), 'Port' (12956), and 'Vendor' (MSAD). Below this, there's a table for 'Add New LDAP Group' with columns for 'Name' (Domain Users), 'Group DN' (CN=Domain Users,CN=Users,DC=dccloud,DC=cisco), and 'End Point Role' (admin). An 'Export' button is also present.

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 * ⓘ

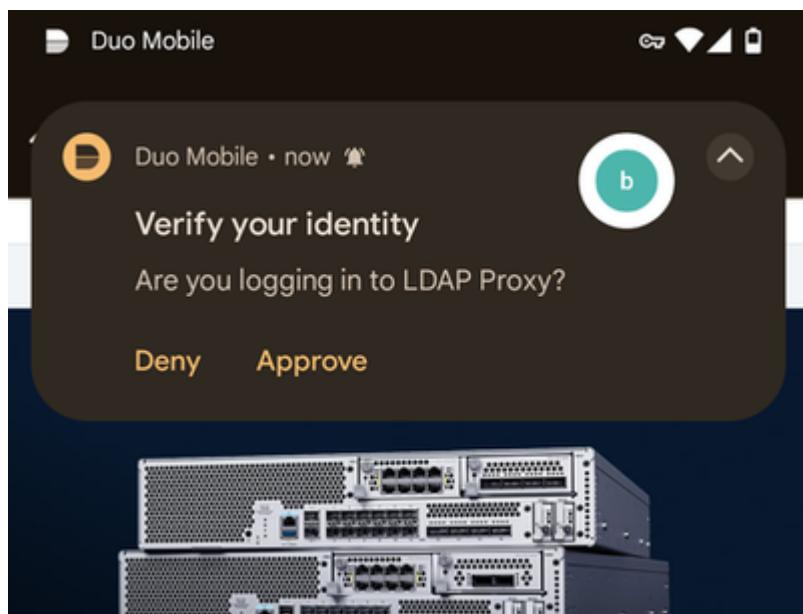


Password *

Show

Sign In

註冊使用者隨後可以在其裝置上獲得登入提示：



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。

The screenshot shows the Cisco Device Console interface. At the top, it displays "Device Console | cx-dcc-beta-imm-fi1". Below the header, there are tabs: "System Information" (which is underlined, indicating it's the active tab), "Device Connector", "Inventory", and "Diagnostic Data". Under the "System Information" tab, there is a section titled "Fabric Interconnect A (Subordinate)". This section contains two rows of information:

| Management IPs | Firmware Version |
|----------------|------------------|
| 198.19.219.162 | 10.5(1)I60(1b) |

Below this, another row of information is shown:

| Model | Available Memory |
|-------------|------------------|
| UCS-FI-6454 | 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）。