

LDAPおよびDuo Multifactor Authenticationを使用したIntersight Managed Mode(IMM)デバイスコンソール統合の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[設定](#)

[ネットワーク図](#)

[ステップ 1:](#)

[ステップ 2](#)

[ステップ 3](#)

[ステップ 4](#)

[確認](#)

[トラブルシュート](#)

[関連情報](#)

はじめに

このドキュメントでは、 LDAPおよびDuo認証プロキシを使用してIMMデバイスコンソールで多要素認証を設定する方法について説明します。

前提条件

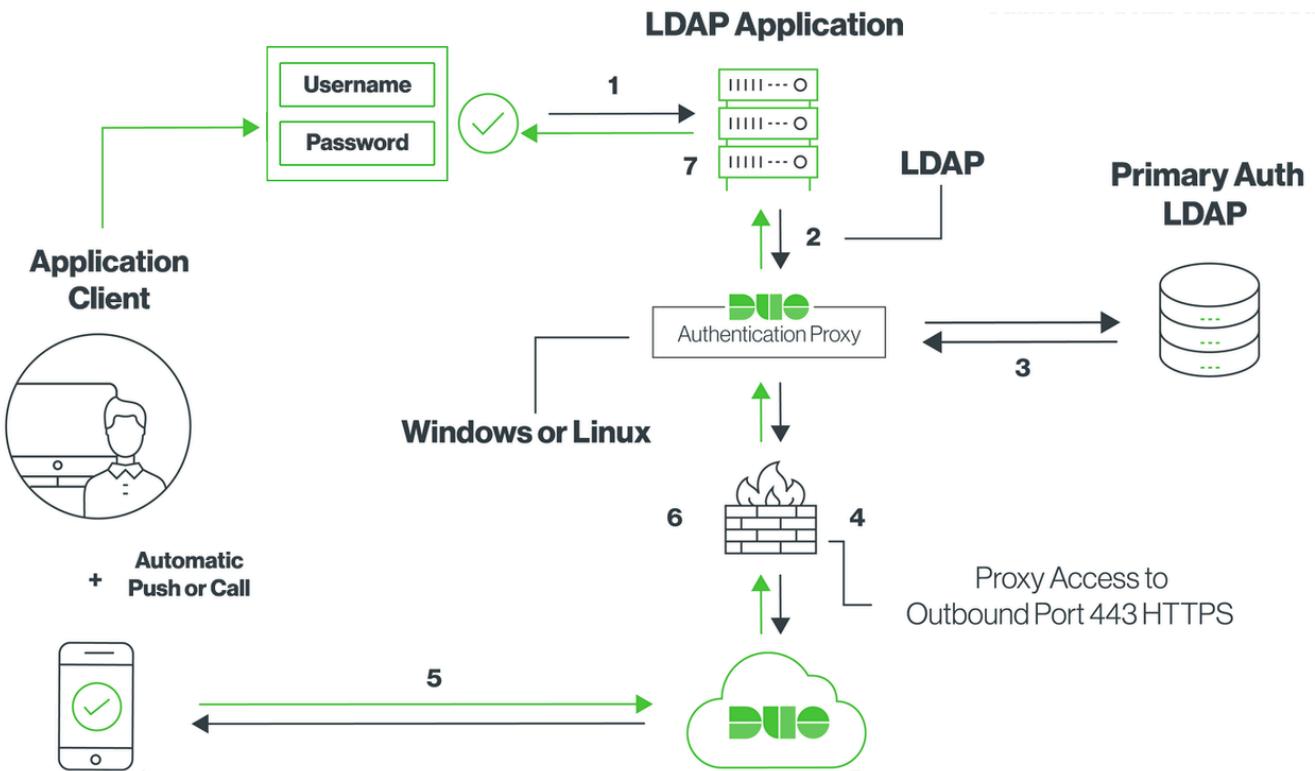
要件

Intersight Managed Mode(IMM)のUCSファブリックインターフェクト

登録済みユーザのDuoサブスクリプション

設定

ネットワーク図



ステップ 1 :

Active DirectoryとIMMデバイスコンソールの両方からアクセス可能なWindowsサーバにDuo Authentication Proxyをインストールします。

Duo認証プロキシは、[ここ](#)から入手できます。

ステップ 2

私たちのDuoインスタンスでは、新しいアプリケーションを追加することができます。

The screenshot shows the Duo Applications configuration interface:

- Left Sidebar:** Includes links for Home, Users, Devices, Policies, Applications (selected), Reports, Monitoring, and Settings.
- Header:** Shows the account name "briamorr-10da678fe8ce4659..." and various navigation icons.
- Applications Section:**
 - A message about migrating to the Universal Prompt.
 - A "Configured applications" table with columns: Name, Application Type, Application Policy, and Application-Group Policies.
 - A note stating "No applications configured yet" with instructions to add applications.
 - A "Add application" button.

ldapを検索し、LDAPプロキシを追加して続行します。

The screenshot shows the 'Applications' section of the Duo Management Console. On the left, there's a sidebar with links like Home, Users, Devices, Policies, Applications (which is selected), Reports, Monitoring, and Settings. The main area is titled 'Configured applications' and shows a table with no data. There's a search bar at the top of the table, and a message below it says 'No applications configured yet' with a note to add and configure an application. At the bottom right of the table area is a blue 'Add application' button.

LDAPプロキシアプリケーションでは、アプリケーション名を設定し、すべてのユーザに対してイネーブルにし、後で使用できるように統合キー、秘密キー、およびAPIホスト名をコピーできます。

The screenshot shows the 'LDAP Proxy' configuration page. The sidebar on the left is identical to the previous one. The main page has a success message 'Successfully added LDAP Proxy to protected applications. Add another.' Below it, there's a section for 'Add users to Duo' with 'Add user' and 'Go to Users' buttons. A note says 'See the LDAP proxy documentation' to integrate Duo into your LDAP-enabled platform. The 'Basic Configuration' section includes fields for 'Application name' (set to 'LDAP Proxy'), 'Application type' (set to 'LDAP Proxy'), and 'User access' (radio button selected for 'Enable for all users'). The 'Details' section contains 'Integration key' (value: 'DICKSUGLZQ9NFDQRNGM') and 'Secret key' (value: '*****QyH5').

ステップ 3

Duo Authentication Proxyをインストールしたサーバに戻ると、Duo Authentication Proxy Managerを設定できます。

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認証プロキシ設定例：



注：読みやすいように#個のコメントが追加されています。

```

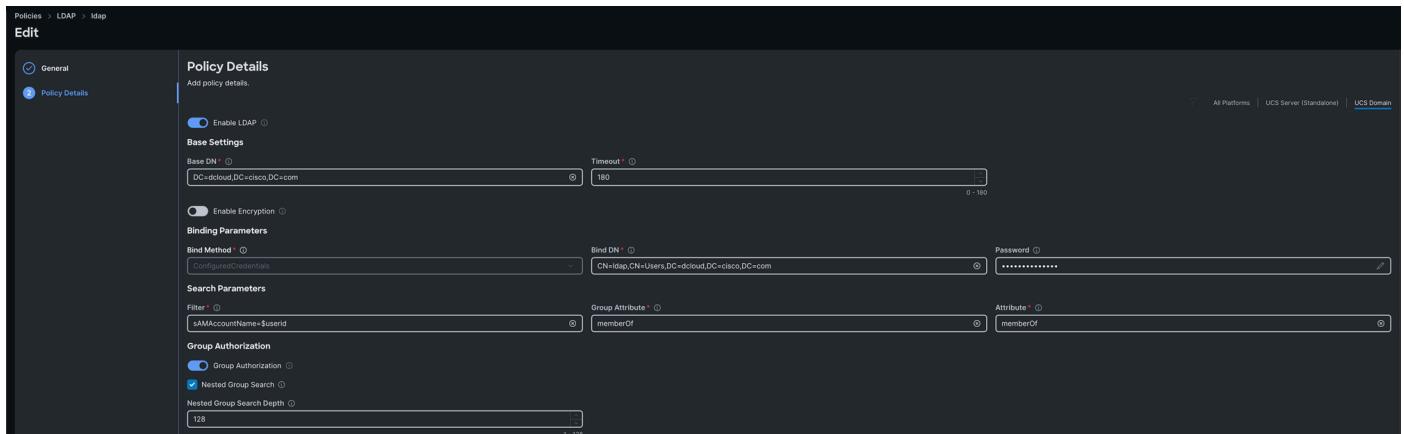
[ad_client]
host=ad1.dcloud.cisco.com # Our Domain Controller
service_account_username=ldap # Our BIND Service Account in AD
service_account_password=changeme # Service Accounts BIND password
search_dn=DC=dcloud,DC=cisco,DC=com # LDAP Search DN

[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

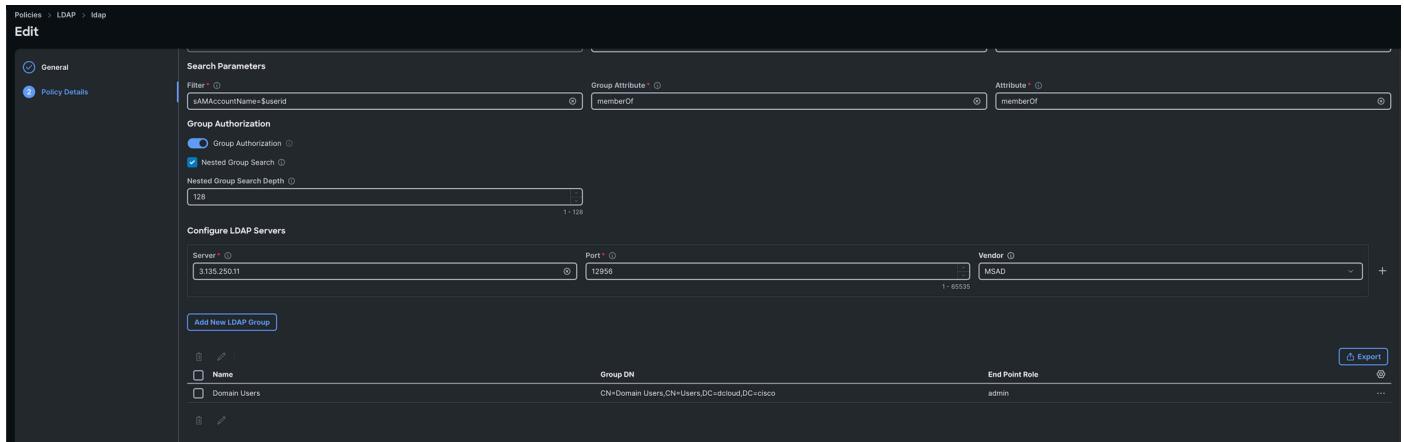
```

ステップ 4

Intersightでは、ベースdn、バインドdn、LDAPサーバIP、パスワードなどの必要なActive Directory設定でDuo LDAPプロキシをポイントするLDAPポリシーを作成できます。 最初に Active Directoryを直接指し示し、が正しく動作することを確認してから、LDAPサーバをDuo LDAPプロキシに変更してトラブルシューティングを容易にすることを推奨します。



The screenshot shows the 'Policy Details' section of an LDAP policy. It includes fields for 'Base DN' (DC=dcloud,DC=cisco,DC=com), 'Bind DN' (CN=ldap,CN=Users,DC=dcloud,DC=cisco,DC=com), 'Password' (redacted), 'Bind Method' (Configure Credentials), 'Search Parameters' (Filter: sAMAccountName=\$userid, Group Attribute: memberOf, Attribute: memberOf), 'Group Authorization' (Group Authorization checked, Nested Group Search checked, Nested Group Search Depth: 128), and 'Configure LDAP Servers' (Server: 3.135.250.11, Port: 12956, Vendor: MSAD).



The screenshot shows the 'Search Parameters' section of the LDAP policy. It includes fields for 'Filter' (sAMAccountName=\$userid), 'Group Attribute' (memberOf), 'Attribute' (memberOf), 'Group Authorization' (Group Authorization checked, Nested Group Search checked, Nested Group Search Depth: 128), and 'Configure LDAP Servers' (Server: 3.135.250.11, Port: 12956, Vendor: MSAD).

確認

デバイスコンソールで、以前Duoに登録したLDAPユーザとしてログインします。

Device Console

Username * ⓘ

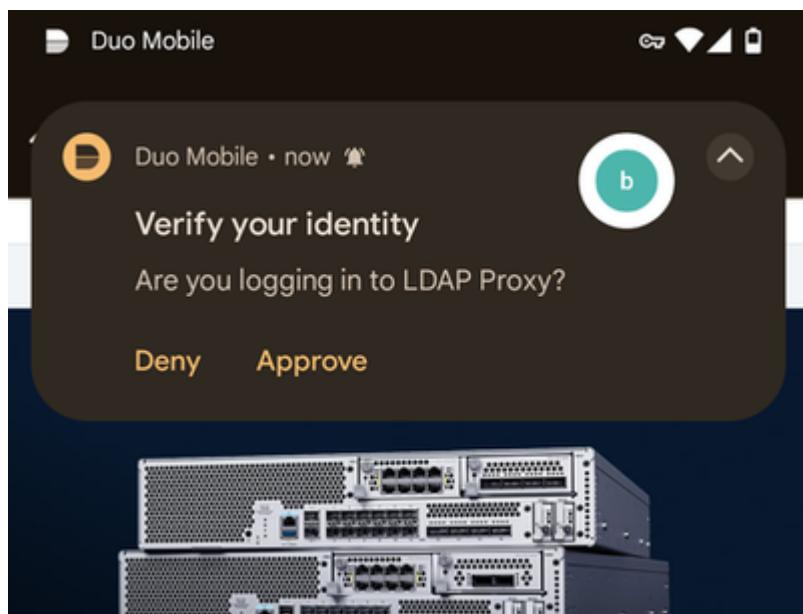


Password *

Show

Sign In

登録済みユーザは、デバイスでログインを求めるプロンプトを受け取ることができます。



要求を確認したら、2要素認証とLDAPを使用してデバイスコンソールにログインします。

The screenshot shows the Cisco Device Console interface. The top bar displays "Device Console | cx-dcc-beta-imm-fi1". Below it is a navigation bar with tabs: "System Information" (which is underlined), "Device Connector", "Inventory", and "Diagnostic Data". The main content area is titled "Fabric Interconnect A (Subordinate)". It contains two rows of information: "Management IPs" (198.19.219.162) and "Firmware Version" (10.5(1)I60(1b)), and "Model" (UCS-FI-6454) and "Available Memory" (49.20 GiB).

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

Model	Available Memory
UCS-FI-6454	49.20 GiB

トラブルシュート

Duo LDAPプロキシログは次の場所にあります。

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

Intersightマネージドモードファブリックインターネット上：

```
connect nxos  
debug ldap
```

関連情報

- [デバイスコンソールガイド](#)
- [デュオって何？](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。