

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](#)

[トラブルシューティング](#)

[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

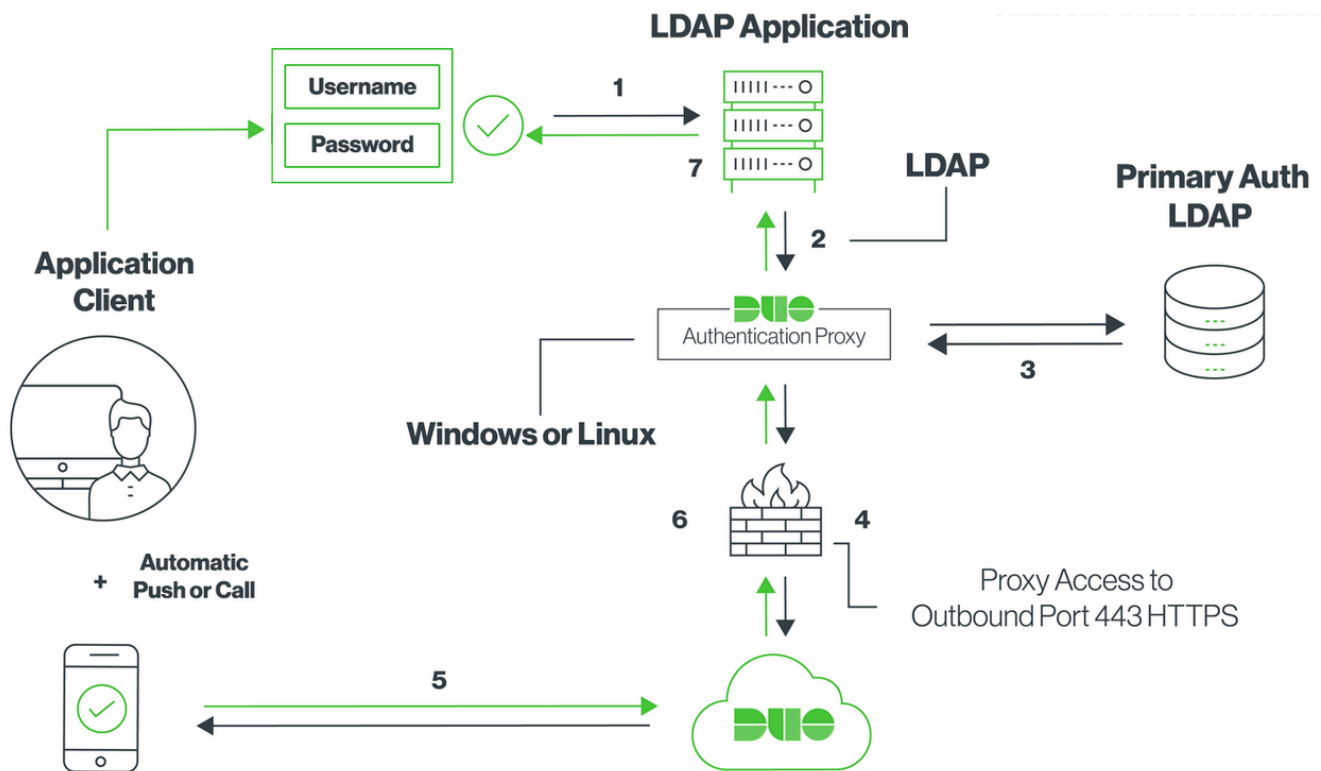
要件

Intersight Managed Mode(IMM)のUCSファブリックインターコネクト

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



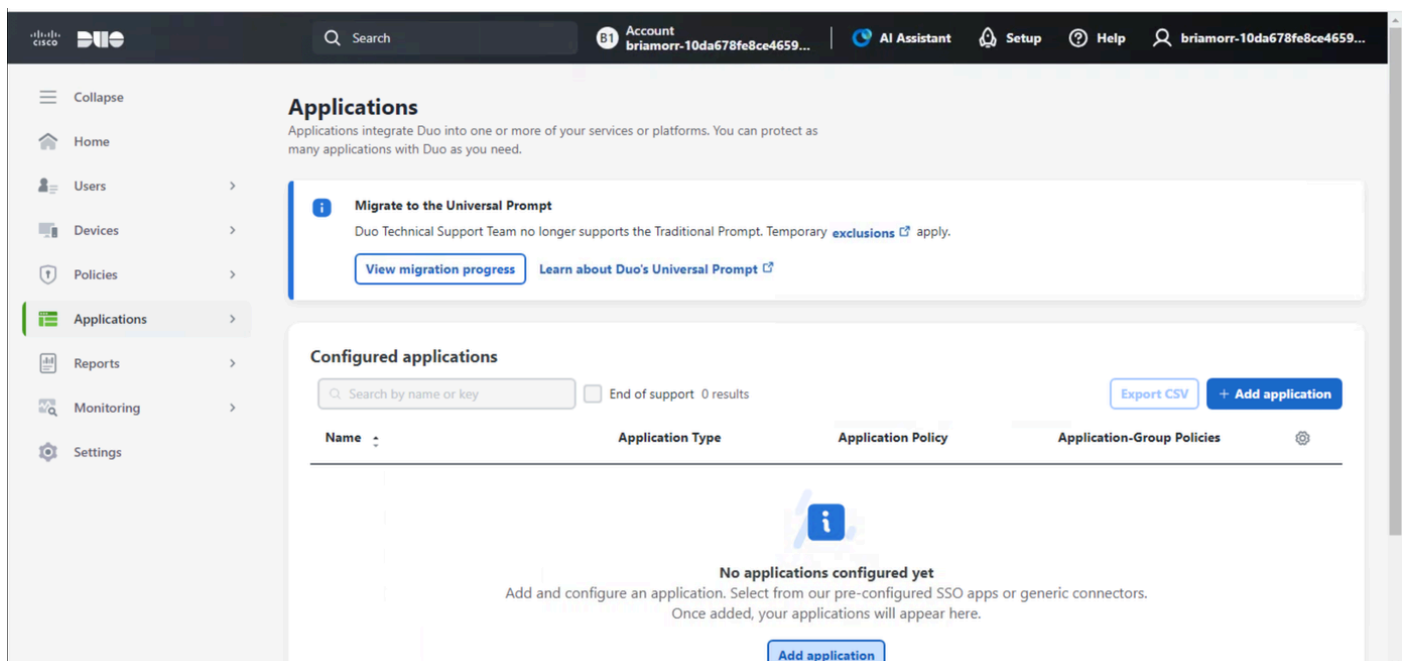
ステップ 1 :

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。

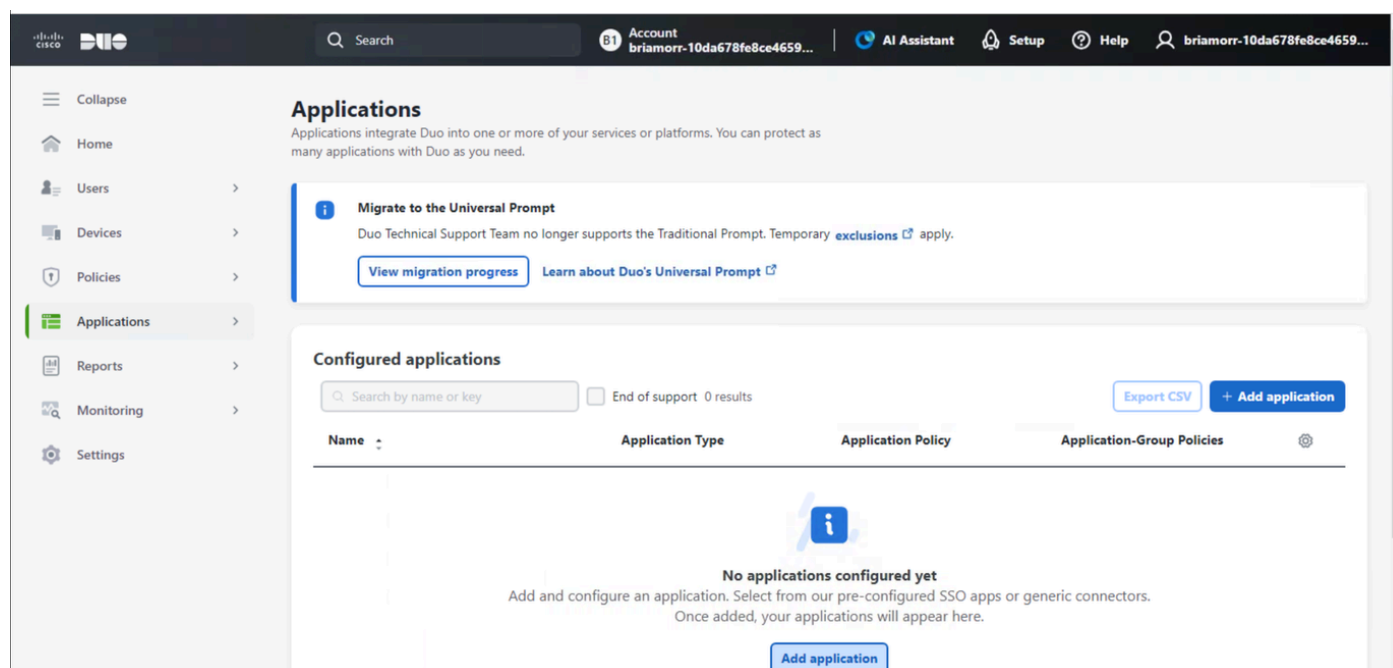
Duo認証プロキシは、[ここ](#)から入手でき[ます](#)。

ステップ 2

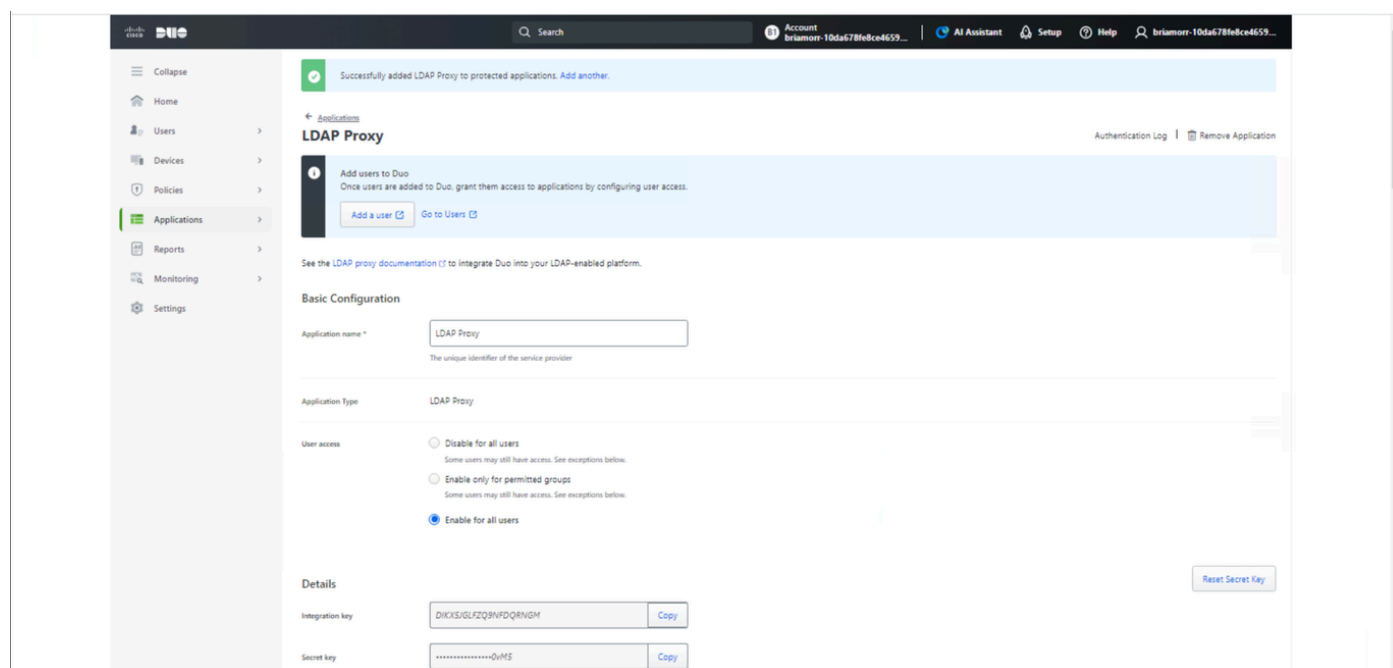
私たちのDuoインスタンスでは、新しいアプリケーションを追加することができます。



ldapを検索し、LDAPプロキシを追加して続行します。



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。



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

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

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 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
```

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。

Policy Details

Enable LDAP

Base Settings

Base DN: DC=dccloud,DC=ntelco,DC=com

Timeout: 180

Enable Encryption

Binding Parameters

Bind Method: Configured Credentials

Bind DN: CN=ldap,CN=Users,DC=dccloud,DC=cisco,DC=com

Password: [masked]

Search Parameters

Filter: SAMAccountName=\$userid

Group Attribute: memberOf

Attribute: memberOf

Group Authorization

Group Authorization: [checked]

Nested Group Search: [checked]

Nested Group Search Depth: 128

Search Parameters

Filter: SAMAccountName=\$userid

Group Attribute: memberOf

Attribute: memberOf

Group Authorization

Group Authorization: [checked]

Nested Group Search: [checked]

Nested Group Search Depth: 128

Configure LDAP Servers

Server: 3.135.250.11

Port: 12956

Vendor: MSAD

Add New LDAP Group

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

Export

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 * ⓘ

mfauser

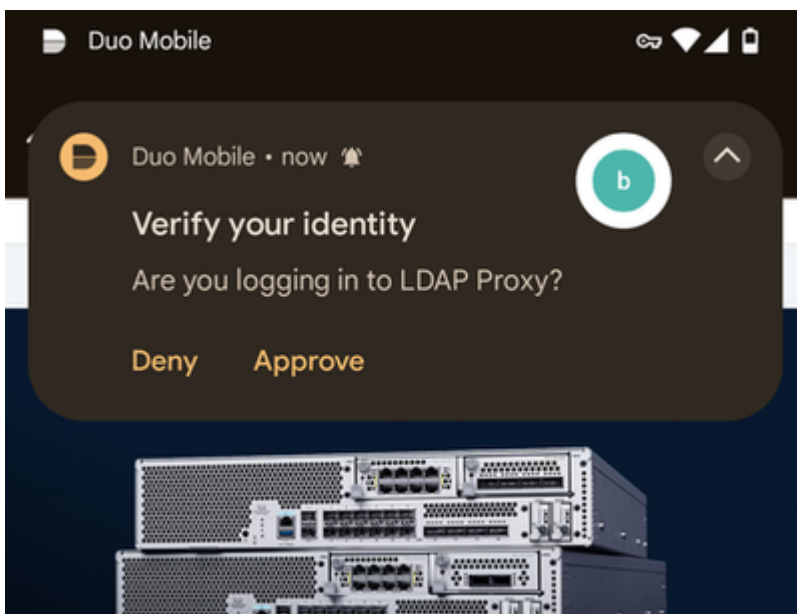
Password *

.....

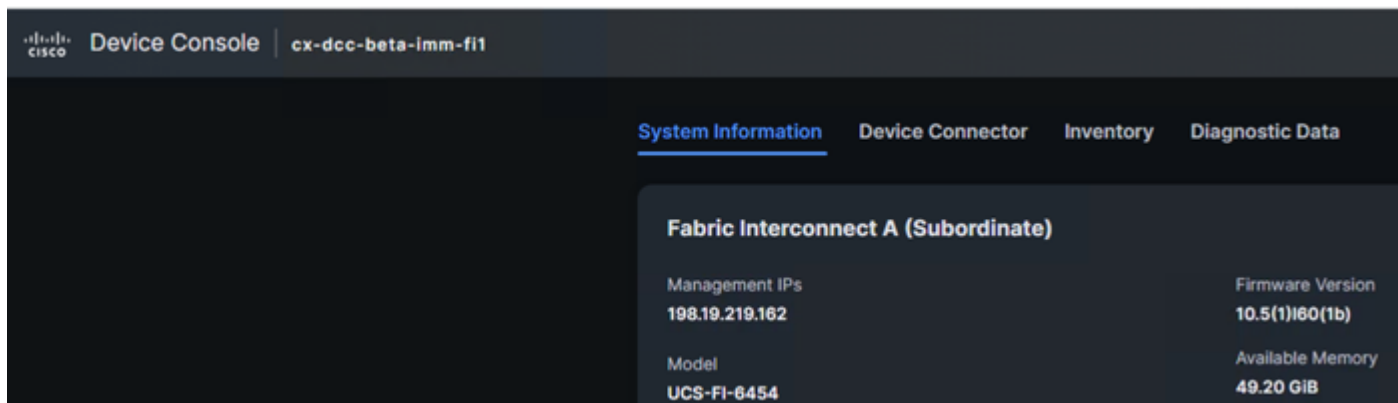
Show

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。



トラブルシューティング

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コネクト上：

```
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。