

配置Intersight管理模式(IMM)设备控制台与LDAP和多因素身份验证的集成

目录

[简介](#)

[先决条件](#)

[要求](#)

[配置](#)

[网络图](#)

[步骤1:](#)

[Step 2:](#)

[第3步:](#)

[第4步:](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍如何使用LDAP和Duo身份验证代理在IMM设备控制台上配置多重身份验证。

先决条件

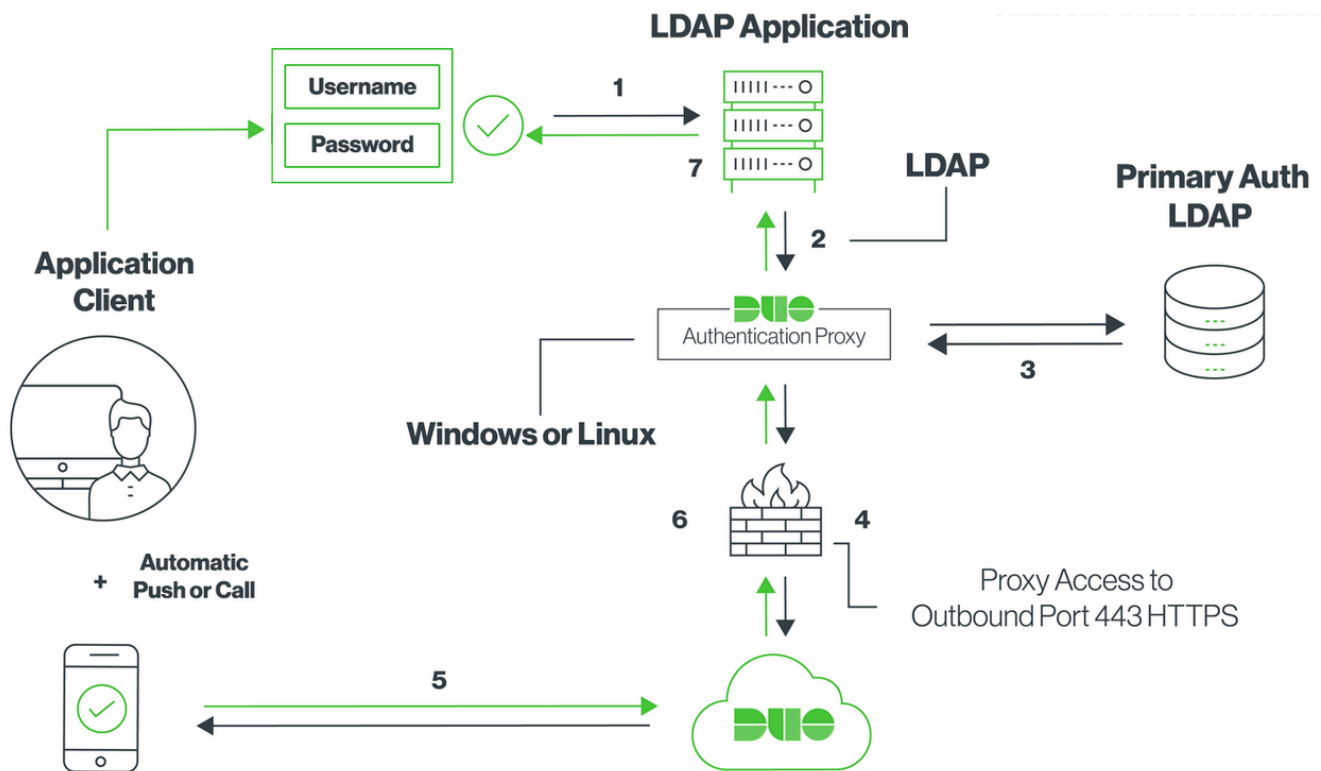
要求

Intersight管理模式(IMM)下的UCS交换矩阵互联。

注册用户的双用户订阅。

配置

网络图



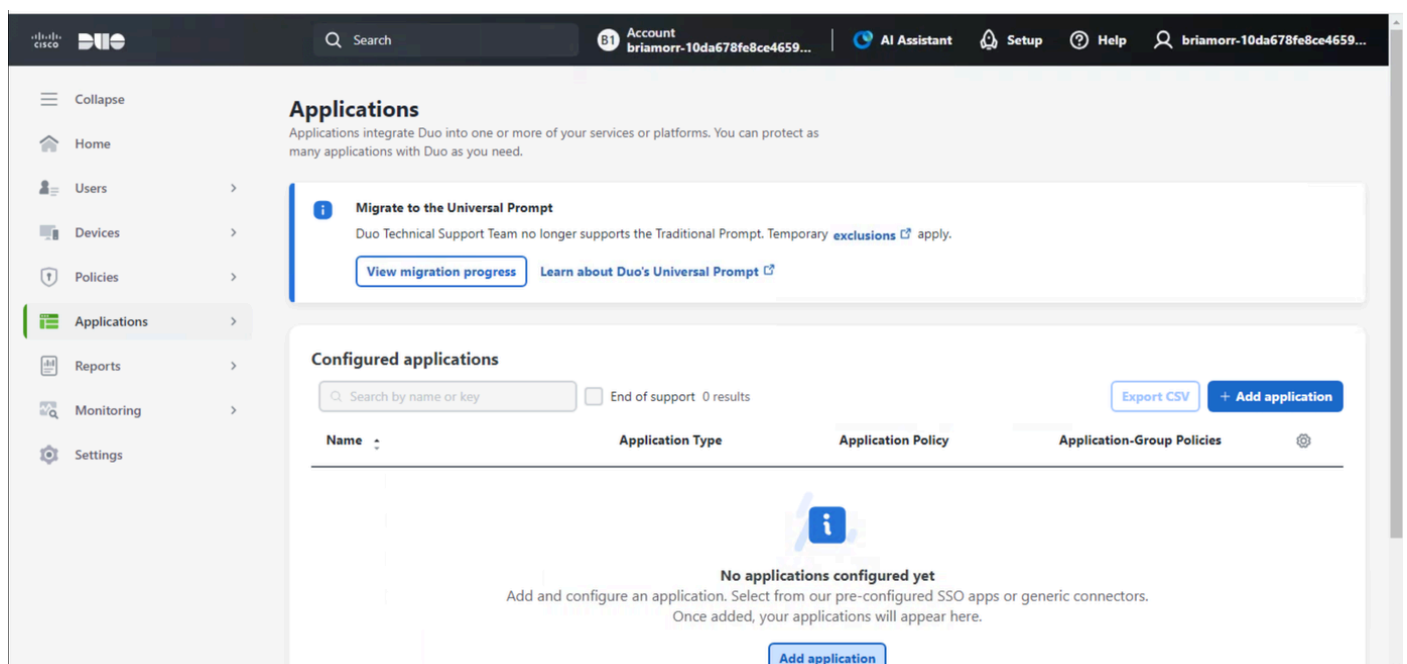
步骤1:

在Active Directory和IMM设备控制台均可访问的Windows服务器上安装双身份验证代理。

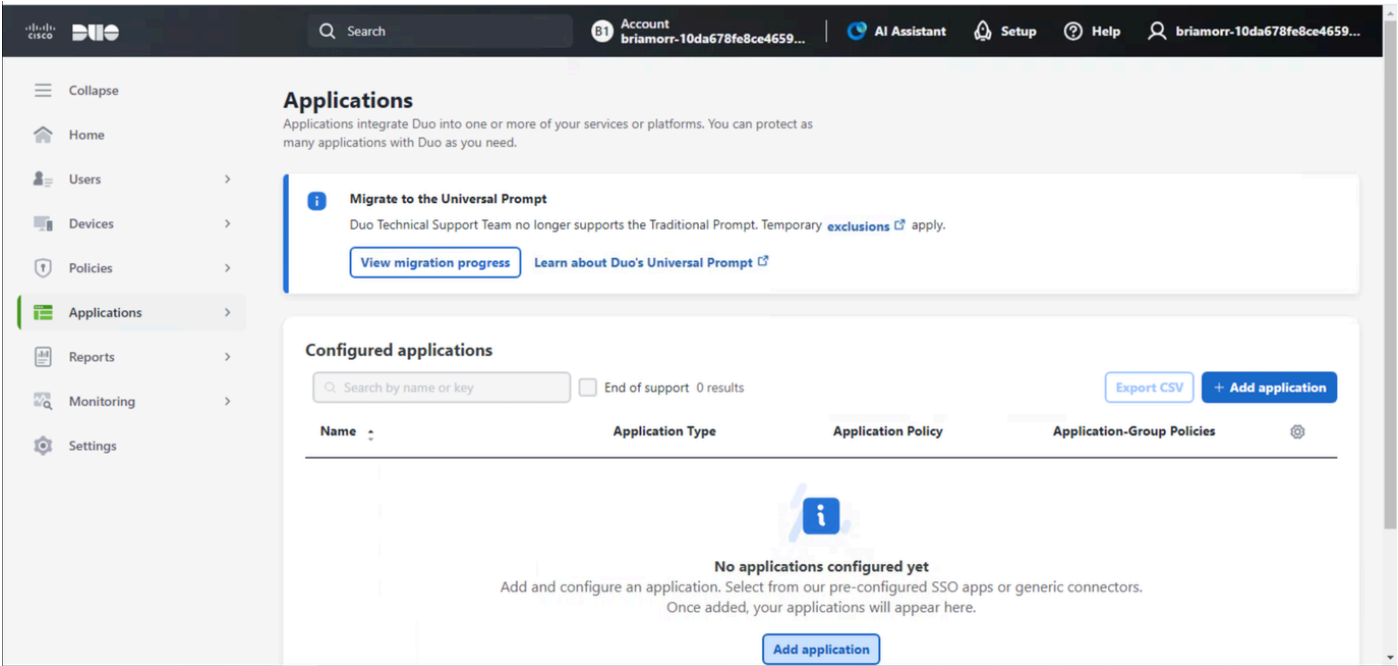
此处可以找到Duo身份验证[代理](#)。

Step 2.

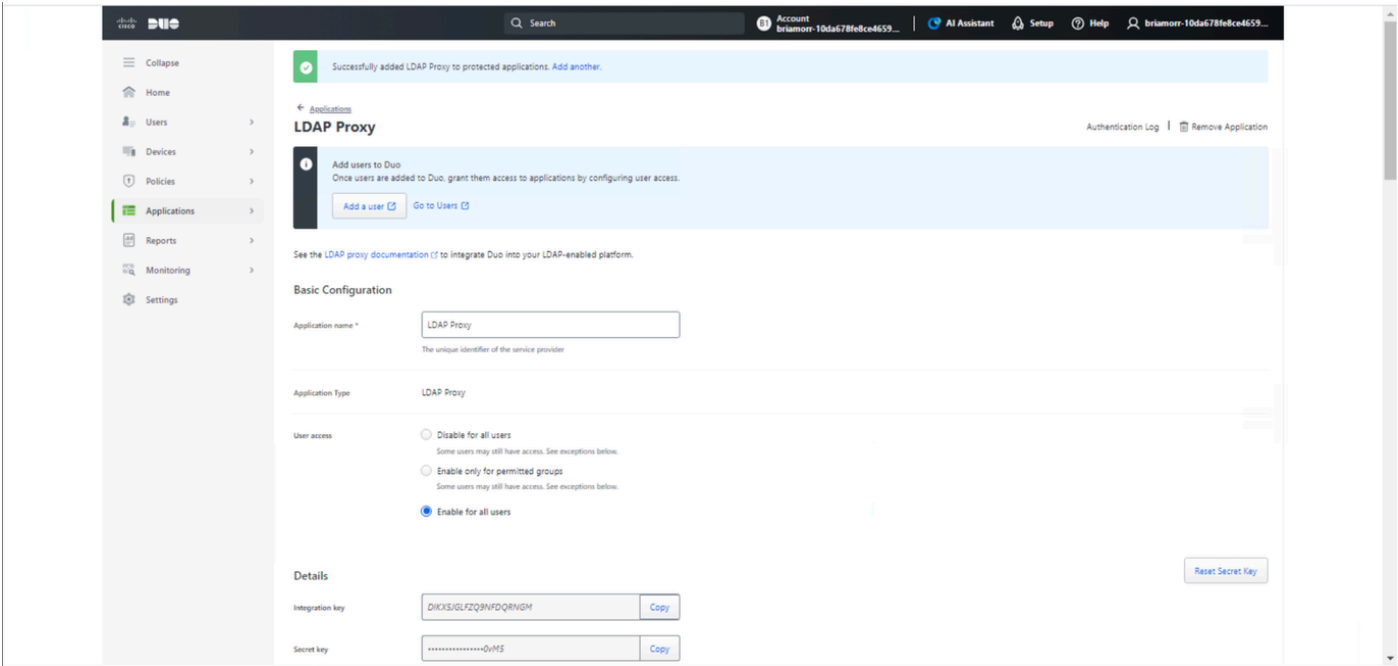
在我们的Duo实例中，您可以添加新应用程序。



搜索ldap并添加LDAP代理以继续。



在LDAP代理应用下，您可以配置应用名称，为所有用户启用，并复制集成密钥、密钥和API主机名供以后使用。



第 3 步：

在安装了Duo Authentication Proxy的服务器上，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

```

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

```

Output

Validate the configuration to view output

Validate

Save

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

Duo身份验证代理示例配置：



注意：添加了#条注释以供阅读。

```

[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

```

第 4 步：

在Intersight中，您可以创建指向具有必要Active Directory设置（如基本dn、绑定dn、LDAP服务器ip、密码等）的Duo LDAP代理的LDAP策略。建议首先直接指向Active Directory并确保在将LDAP服务器更改为Duo LDAP代理之前正常工作，以便简化故障排除。

General

Policy Details

Policy Details

Enable LDAP

Base Settings

Base DN

DC=dccloud,DC=cisco,DC=com

Timeout

180

0 - 180

Enable Encryption

Binding Parameters

Bind Method

Configure Credentials

Bind DN

CN=idap,CN=Users,DC=dccloud,DC=cisco,DC=com

Password

Search Parameters

Filter

sAMAccountName=\$userid

Group Attribute

memberOf

Attribute

memberOf

Group Authorization

Group Authorization

Nested Group Search

Nested Group Search Depth

128

1 - 128

General

Policy Details

Search Parameters

Filter

sAMAccountName=\$userid

Group Attribute

memberOf

Attribute

memberOf

Group Authorization

Group Authorization

Nested Group Search

Nested Group Search Depth

128

1 - 128

Configure LDAP Servers

Server

3.135.250.11

Port

12356

1 - 65535

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

验证

在设备控制台上，以之前在Duo中注册的LDAP用户身份登录。

Device Console

Username * ⓘ

mfauser

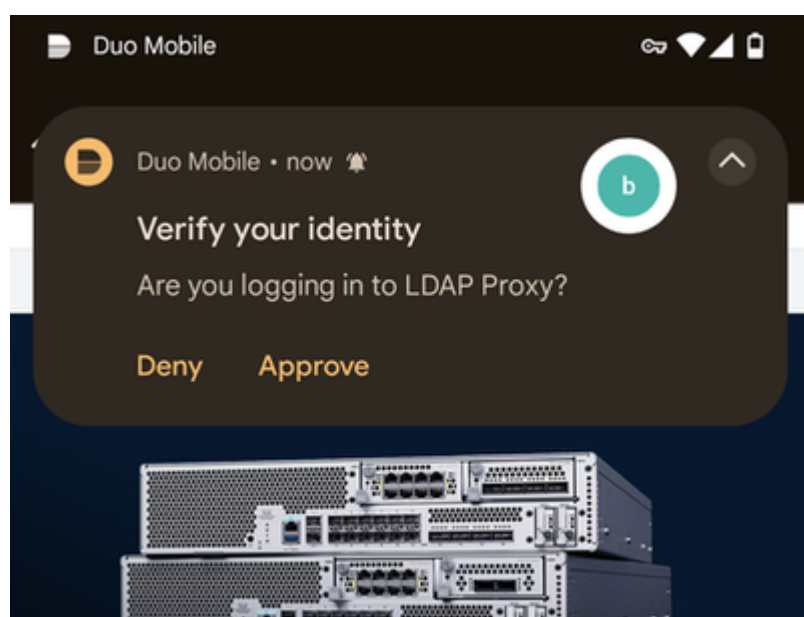
Password *

.....

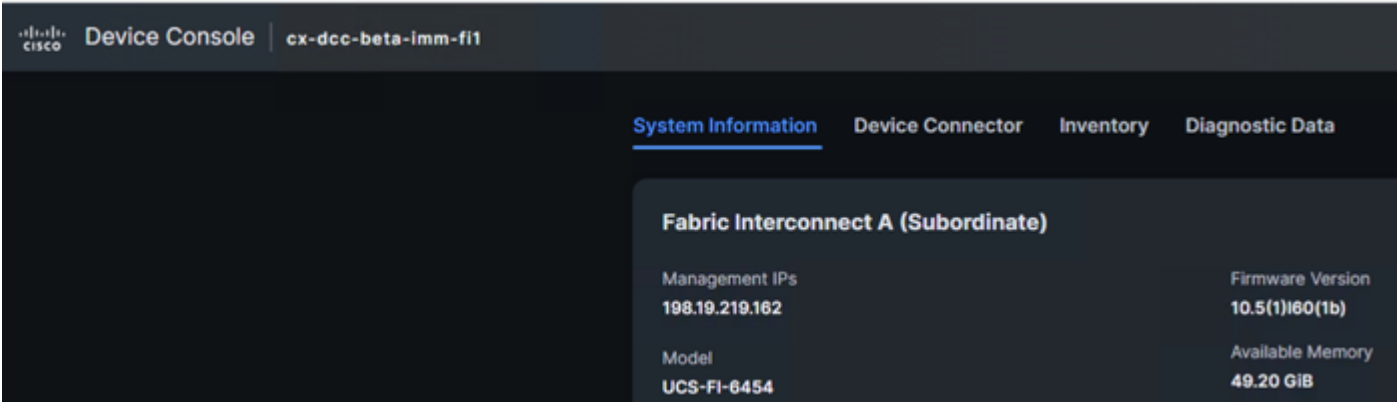
Show

Sign In

注册用户随后可以在其设备上获得登录提示：



验证请求后，您可以使用双因素身份验证和LDAP成功登录设备控制台。



故障排除

Duo LDAP代理日志位于：

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

在Intersight管理模式交换矩阵互联上：

connect nxos

debug ldap

相关信息

- [设备控制台指南](#)
- [什么是Duo?](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。