

# 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

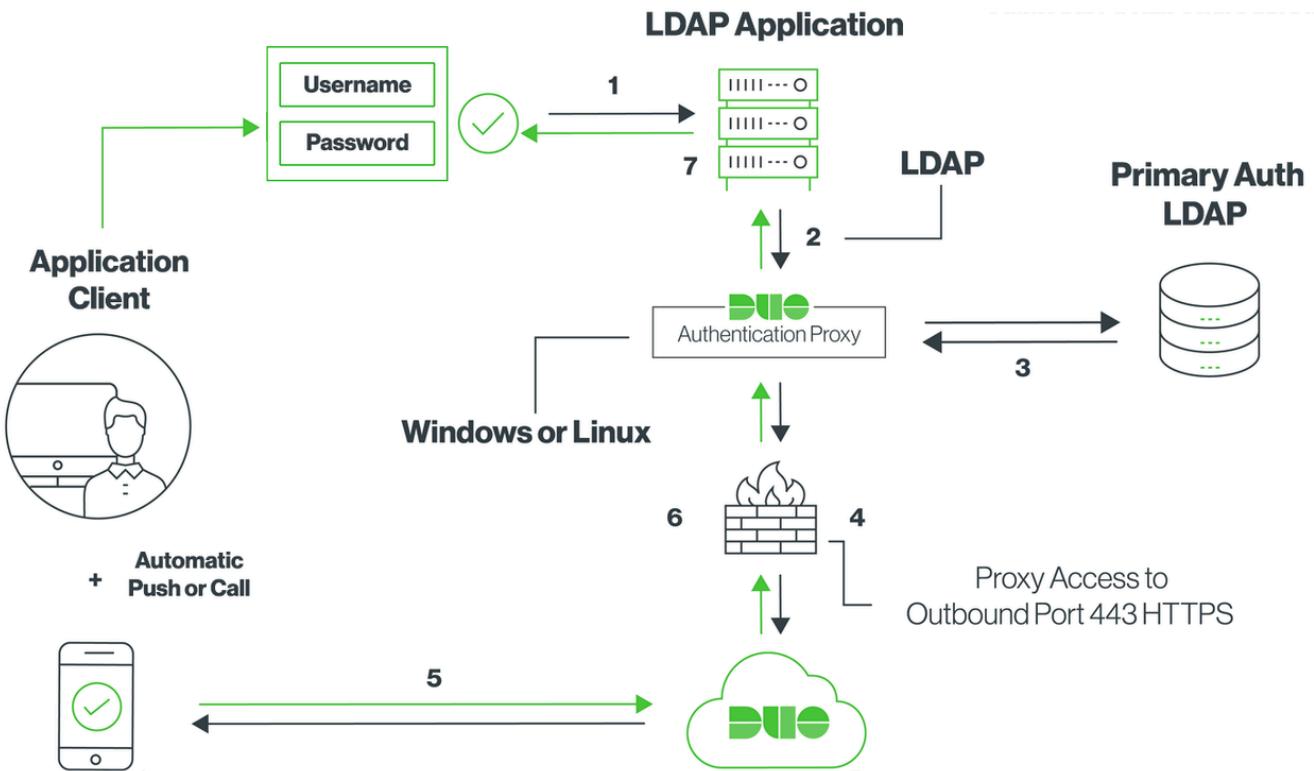
### 要求

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。

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 account information (briamorr-10da678fe8ce4659...) and navigation links for AI Assistant, Setup, Help, and search.
- Applications Section:**
  - Applications:** Subtitle explaining applications integrate Duo into services.
  - Migrate to the Universal Prompt:** Information about the migration to the Universal Prompt.
  - Configured applications:** A table with columns: Name, Application Type, Application Policy, Application-Group Policies, and a search bar.
  - No applications configured yet:** A message encouraging users to add applications.
  - Add application:** A blue button to start adding a new application.

搜索ldap并添加LDAP代理以继续。

The screenshot shows the Duo Applications interface. On the left, there's a sidebar with links for Home, Users, Devices, Policies, Applications (which is selected), Reports, Monitoring, and Settings. The main area is titled 'Applications' and contains a message about migrating to the Universal Prompt. Below this is a section titled 'Configured applications' with a search bar and a table header. The table has columns for 'Name', 'Application Type', 'Application Policy', and 'Application-Group Policies'. A large message in the center says 'No applications configured yet' with a 'Add application' button.

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。

The screenshot shows the 'LDAP Proxy' configuration page. The sidebar on the left is identical to the previous one. The main area has a success message 'Successfully added LDAP Proxy to protected applications. Add another.' Below this is a section for 'Basic Configuration' with fields for 'Application name' (set to 'LDAP Proxy') and 'Application Type' (set to 'LDAP Proxy'). Under 'User access', there are three radio button options: 'Disable for all users', 'Enable only for permitted groups', and 'Enable for all users' (which is selected). In the 'Details' section, there are fields for 'Integration key' (containing 'DICKSUGLZQ9NFDQRNGM') and 'Secret key' (containing '.....QyMS'), each with a 'Copy' button. There's also a 'Reset Secret Key' button.

第3步：

在安装了Duo Authentication Proxy的服务器上，您可以配置Duo Authentication Proxy Manager。

The screenshot shows the Duo Authentication Proxy Manager configuration interface. The main area displays the configuration file content:

```

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

```

Below the configuration text are two buttons: "Validate" and "Save". To the right, there is a link: "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 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"

```

## 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。

The screenshot shows the 'Policy Details' section of the Intersight interface. It includes fields for 'Base DN' (DC=dcloud,DC=cisco,DC=com), 'Bind DN' (CN=idap,CN=Users,DC=dcloud,DC=cisco,DC=com), 'Password' (redacted), 'Filter' (sAMAccountName=\$userid), 'Group Attribute' (memberOf), and 'Attribute' (memberOf). Other settings like 'Group Authorization' and 'Nested Group Search Depth' (128) are also visible.

The screenshot shows the 'Configure LDAP Servers' section. It lists a single server entry: 'Server' (3.135.250.11), 'Port' (12956), and 'Vendor' (MSAD). There is also a table for 'Add New LDAP Group' with columns for 'Name', 'Group DN' (CN=Domain Users,CN=Users,DC=dcloud,DC=cisco), and 'End Point Role' (admin).

## 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 \* ⓘ

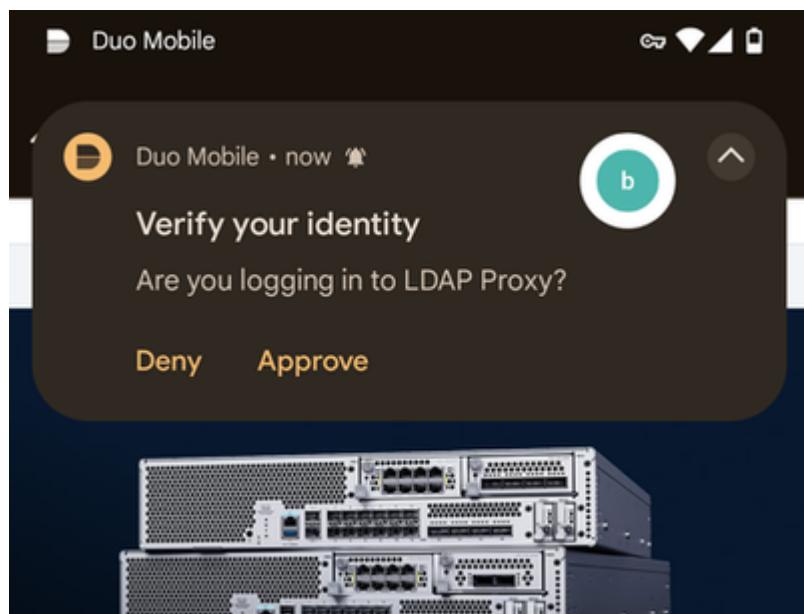


Password \*

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。

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" (198.19.219.162) and "Firmware Version" (10.5(1)I60(1b)), and "Model" (UCS-FI-6454) and "Available Memory" (49.20 GiB).

## 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）。