

Konfigurieren der Integration der IMM-Gerätekonzole (Intersight Managed Mode) mit LDAP und Duo Multifactor Authentication

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Schritt 1:](#)

[Schritt 2:](#)

[Schritt 3:](#)

[Schritt 4:](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie die mehrstufige Authentifizierung auf der IMM-Gerätekonzole mithilfe von LDAP und dem Duo-Authentifizierungsproxy konfigurieren.

Voraussetzungen

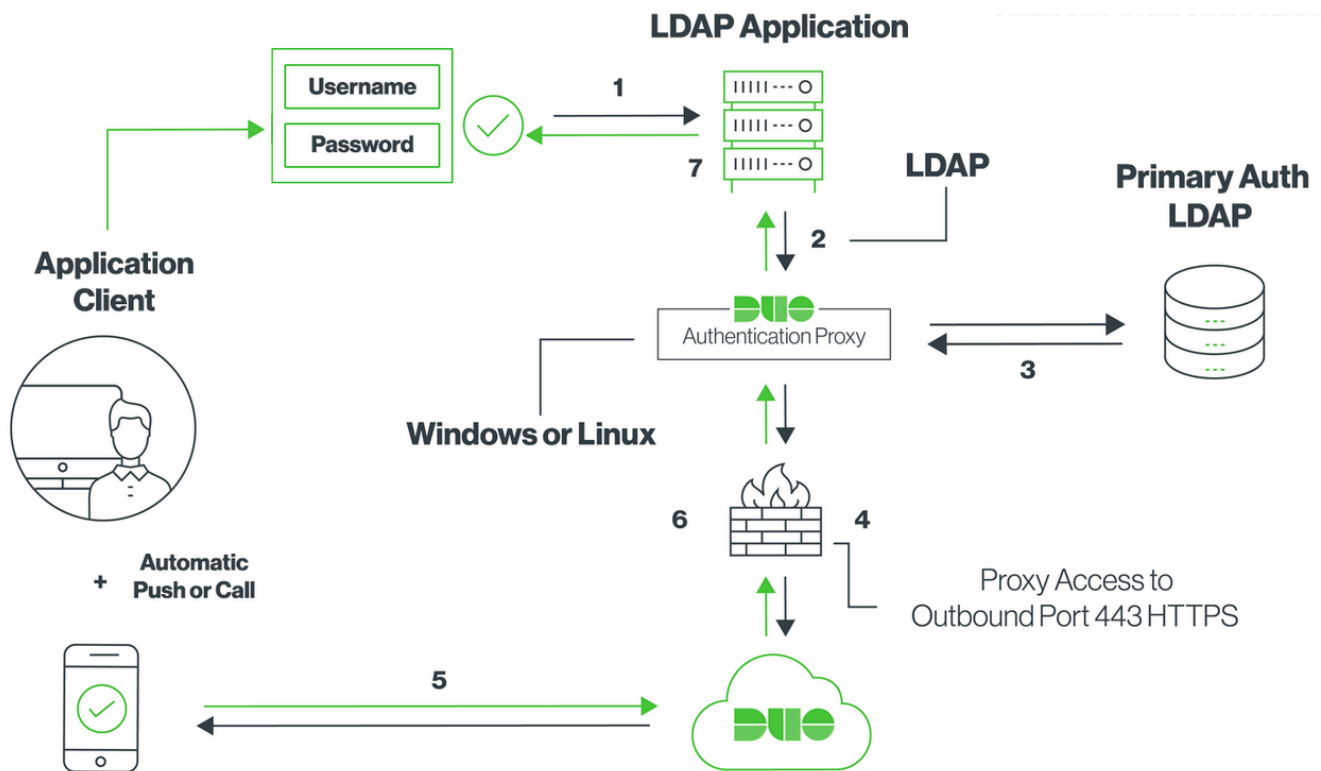
Anforderungen

UCS Fabric Interconnects im Intersight Managed Mode (IMM).

Duo Abonnement mit einem angemeldeten Benutzer.

Konfigurieren

Netzwerkdiagramm



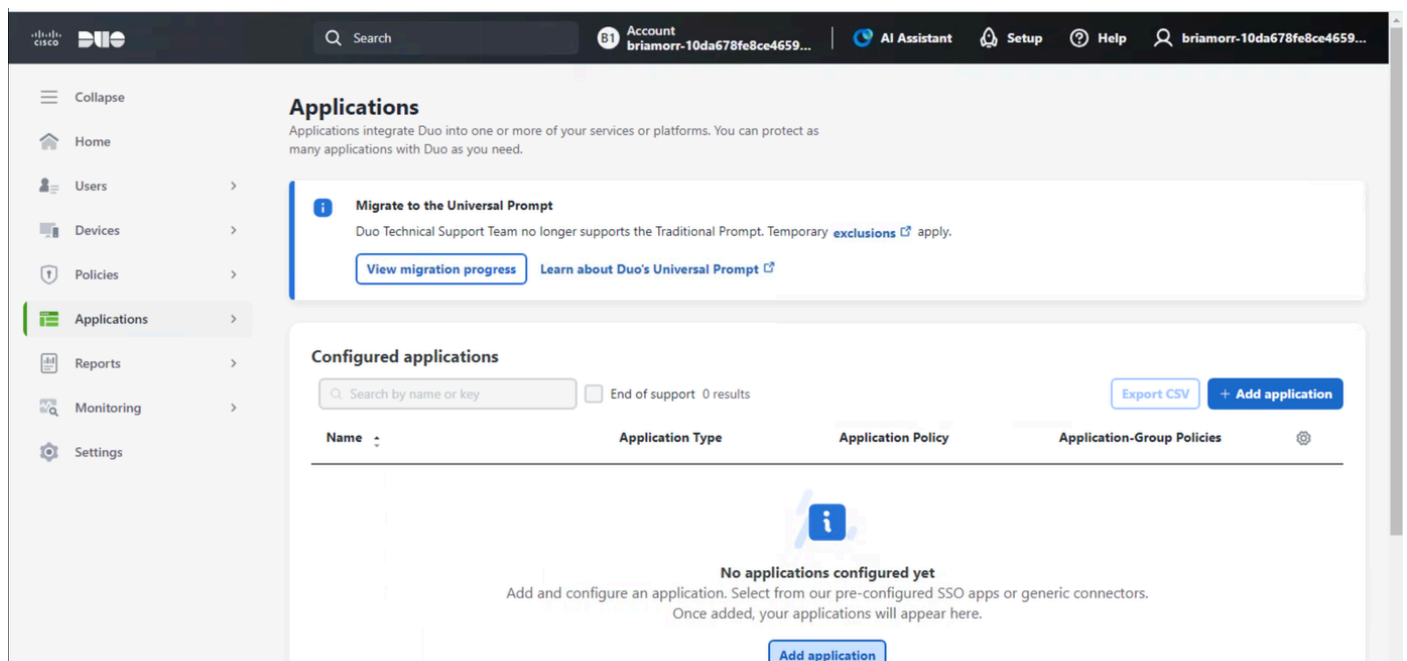
Schritt 1:

Installieren Sie den Duo Authentifizierungsproxy auf einem Windows-Server, auf den sowohl Active Directory als auch die IMM-Gerätekonsole zugreifen können.

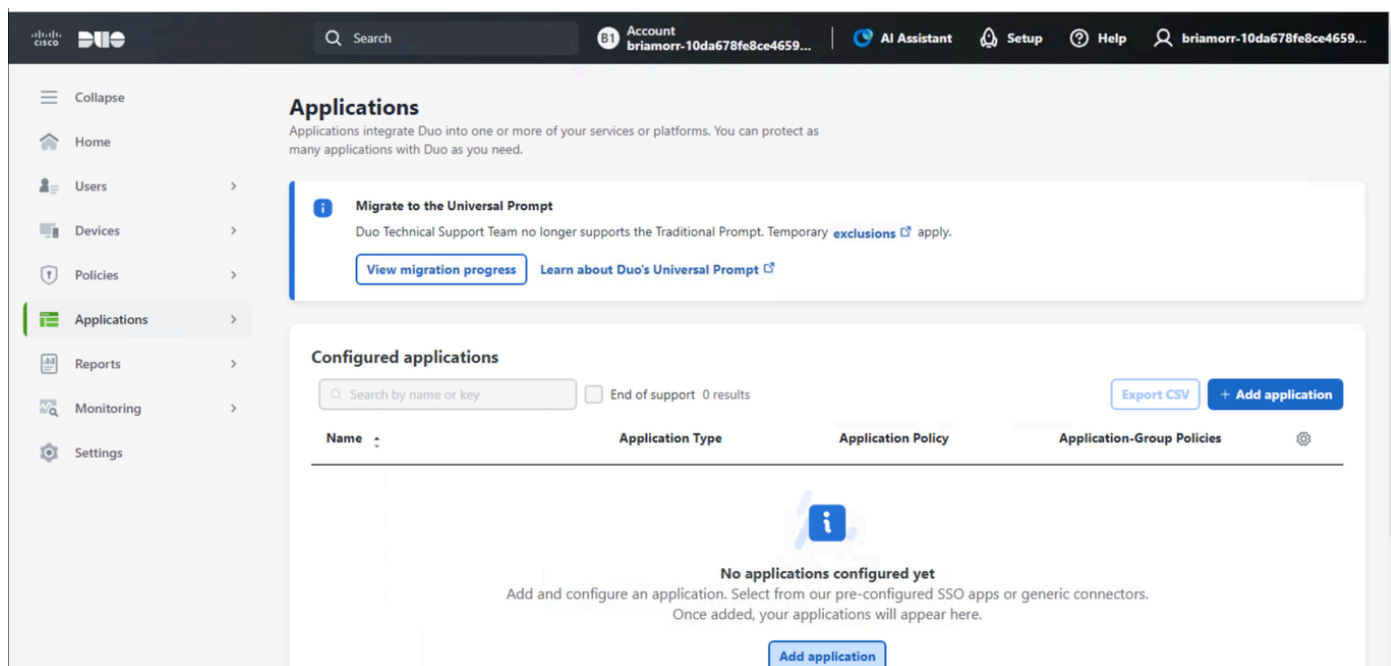
Den Duo Authentifizierungsproxy finden Sie [hier](#).

Schritt 2:

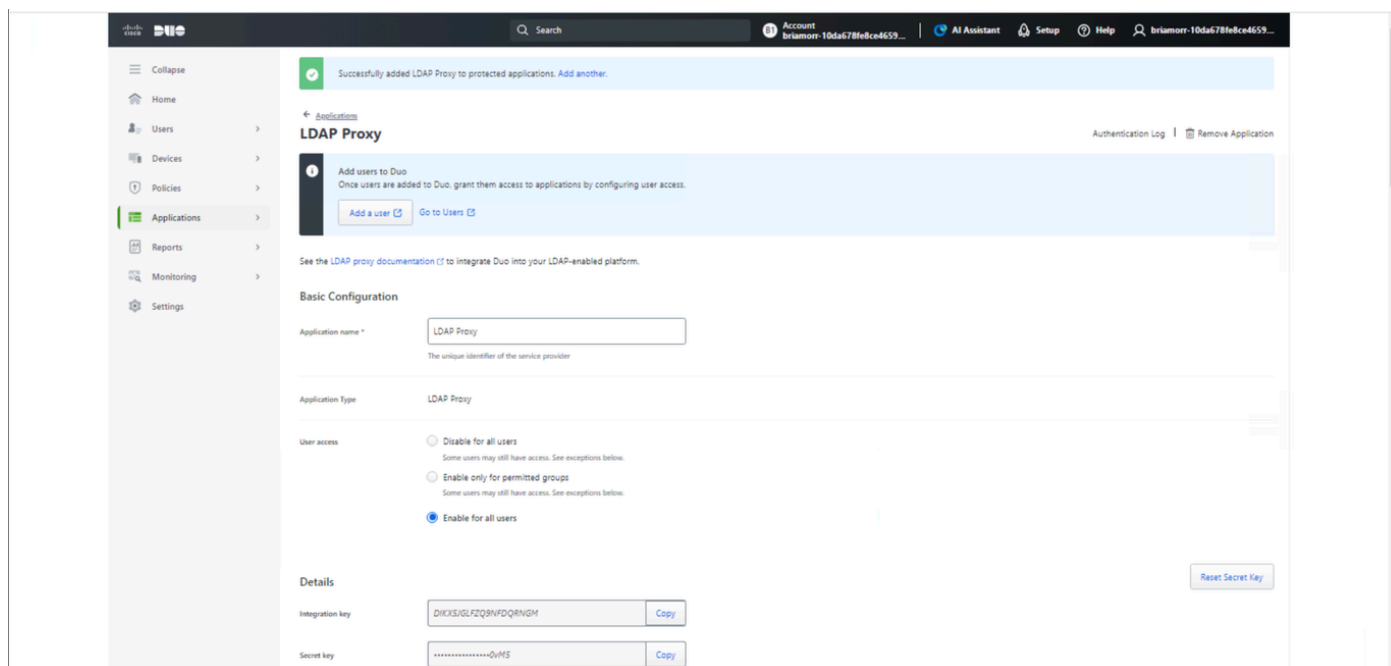
In unserer Duo-Instanz können Sie eine neue Anwendung hinzufügen.



Suchen Sie nach LDAP, und fügen Sie den LDAP-Proxy hinzu, um fortzufahren.



Unter der LDAP-Proxy-Anwendung können Sie einen Anwendungsnamen konfigurieren, für alle Benutzer aktivieren und den Integrationsschlüssel, den geheimen Schlüssel und den API-Hostnamen zur späteren Verwendung kopieren.



Schritt 3:

Zurück auf dem Server, auf dem wir den Duo-Authentifizierungsproxy installiert haben, können Sie den Duo-Authentifizierungsproxy-Manager konfigurieren.

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](#)

Beispielkonfiguration für den Duo-Authentifizierungsproxy:



Anmerkung: # Kommentare zur Lesbarkeit hinzugefügt.

```

[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

```

Schritt 4:

In Intersight können Sie dann eine LDAP-Richtlinie erstellen, die auf unseren Duo LDAP-Proxy mit den erforderlichen Active Directory-Einstellungen wie base dn, bind dn, LDAP-Server-IP, Kennwort usw. verweist. Es wird empfohlen, zunächst direkt auf Active Directory zu verweisen und sicherzustellen, dass die Konfiguration ordnungsgemäß funktioniert, bevor Sie den LDAP-Server in den Duo LDAP-Proxy ändern, um die Fehlerbehebung zu vereinfachen.

The screenshot shows the 'Edit' page for a policy in the Duo console. The left sidebar has 'General' and 'Policy Details' tabs, with 'Policy Details' selected. The main content area is titled 'Policy Details' and includes a toggle for 'Enable LDAP' which is turned on. Below this are 'Base Settings' with fields for 'Base DN' (DC=dccloud,DC=csico,DC=com) and 'Timeout' (180). There is also a toggle for 'Enable Encryption'. The 'Binding Parameters' section includes 'Bind Method' (Configured Credentials), 'Bind DN' (CN=idap,CN=Users,DC=dccloud,DC=csico,DC=com), and 'Password'. The 'Search Parameters' section includes 'Filter' (sAMAccountName=\$userid), 'Group Attribute' (memberOf), and 'Attribute' (memberOf). The 'Group Authorization' section has a toggle for 'Group Authorization' which is on, a checkbox for 'Nested Group Search' which is checked, and a 'Nested Group Search Depth' field set to 128.

This screenshot shows the lower portion of the 'Policy Details' page. The 'Search Parameters' and 'Group Authorization' sections are visible. Below them is the 'Configure LDAP Servers' section, which includes fields for 'Server' (3.135.250.11), 'Port' (12956), and 'Vendor' (MSAD). At the bottom, there is a table of LDAP groups. The table has columns for 'Name', 'Group DN', and 'End Point Role'. One group is listed: 'Domain Users' with Group DN 'CN=Domain Users,CN=Users,DC=dccloud,DC=csico' and End Point Role 'admin'. There is an 'Add New LDAP Group' button and an 'Export' button.

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

Überprüfung

Melden Sie sich auf der Gerätekonsole als LDAP-Benutzer an, der zuvor bei Duo registriert war.

Device Console

Username * ⓘ

mfauser

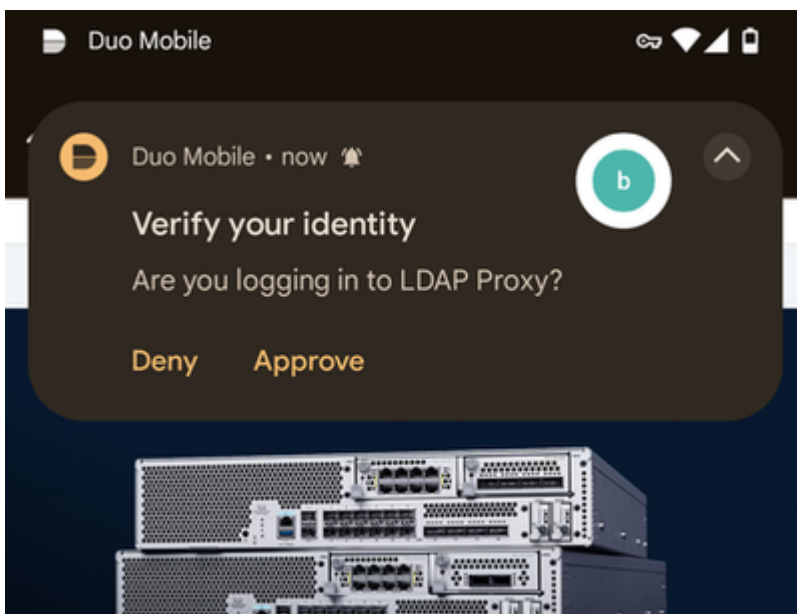
Password *

.....

Show

Sign In

Die angemeldeten Benutzer erhalten dann eine Aufforderung zur Anmeldung auf ihrem Gerät:



Nach der Überprüfung der Anforderung können Sie sich mithilfe von 2-Faktor-Authentifizierung und LDAP erfolgreich bei der Gerätekonsole anmelden.



Fehlerbehebung

Duo LDAP-Proxyprotokolle finden Sie unter:

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

Bei Intersight Managed Mode Fabric Interconnect:

```
connect nxos
```

```
debug ldap
```

Zugehörige Informationen

- [Gerätekonsolenleitfaden](#)
- [Was ist Duo?](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.