Configure LDAP in Intersight Virtual Appliance

Contents

Introduction

This document describes the process to configure LDAP authentication in an Intersight Private Virtual Appliance (PVA).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Lightweight Directory Access Protocol (LDAP) protocol.
- Intersight Private Virtual Appliance.
- Domain Name Server (DNS) Server.

Components Used

- Intersight Private Virtual Appliance.
- Microsoft Active Directory.

- DNS Server.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

LDAP is a protocol used to access resources from a directory over the network. These directories store information about users, organizations, and resources. LDAP provides a standard way to access and manage that information that can be used for authentication and authorization processes.

This document shows the configuration process to add remote authentication through LDAP to an Intersight PVA.

Configure

Configuration of LDAP Basic Settings

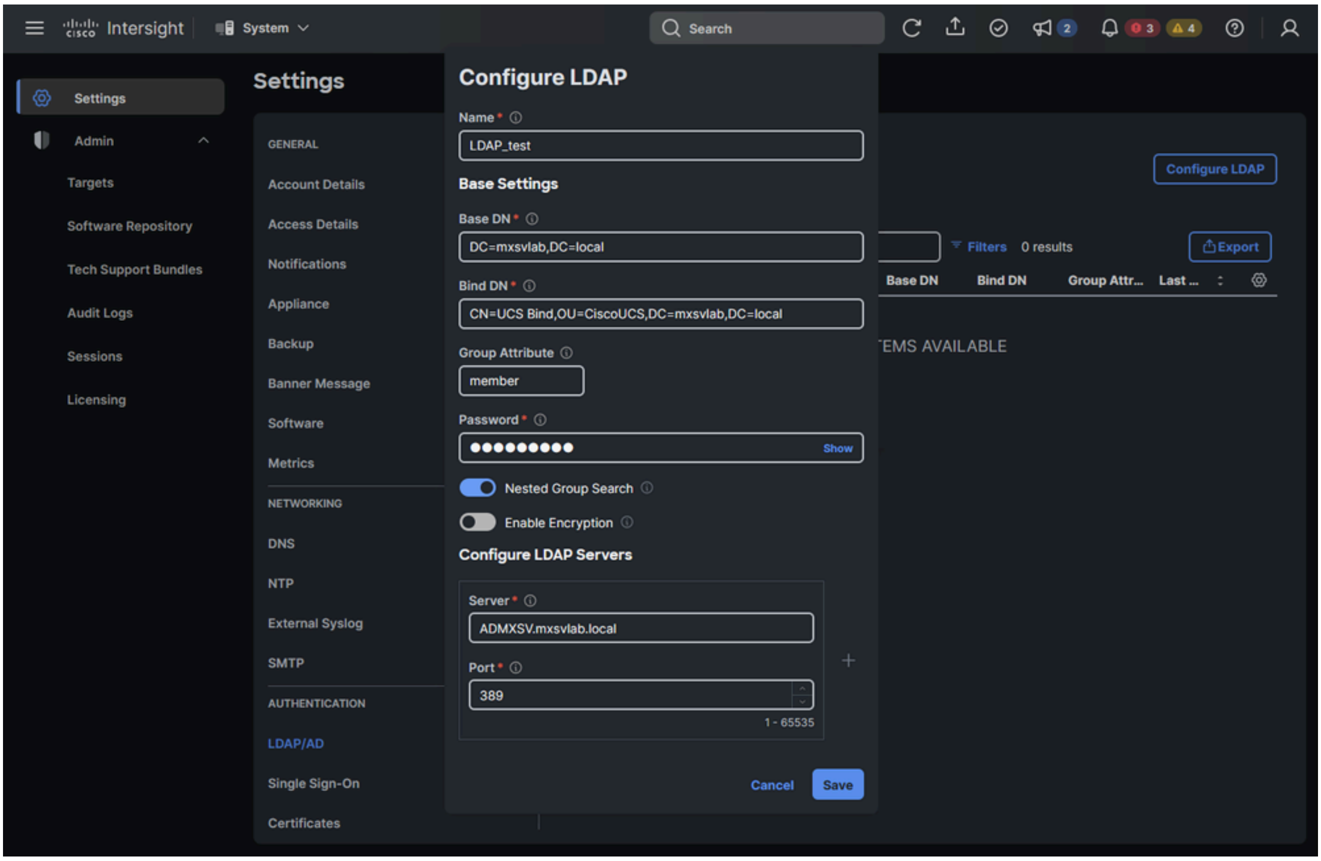
1. Navigate to **System > Settings > AUTHENTICATION > LDAP/AD**.
2. Click **Configure LDAP**.
3. Enter the required information. Consider the next recommendations:
    1. The **Name** is set arbitrarily and does not affect the configuration.
    2. For the **BaseDN** and **BindDN**, copy and paste the corresponding values from your Active Directory (AD) configuration.
    3. The default value for **Group Attribute** is **member**.

        Note: In other UCS management tools like UCSM or CIMC, Group attribute is set to memberOf. In Intersight it is recommended to leave it as member.

    4. Enter the password for this LDAP provider.
    5. Enable **Nested Group Search** toggle if you want to allow a recursive search in your AD for all the groups from root and their contained groups.
    6. Leave **Enable Encryption** disabled for a regular LDAP configuration. If secure LDAP is needed, enable it and ensure to review the section Configuration of LDAPS (Secure LDAP) for the complementary steps you need to configure.
4. Add the configuration for one LDAP server:
    1. In **Server** introduce the IP or hostname of the LDAP server.

        ⚠ **Caution**: If hostname is used, ensure the DNS is able to map that hostname correctly.

    2. The default and recommended port for LDAP is 389 .
5. Click **Save**.



Configure LDAP

Name * LDAP_test

Base Settings

Base DN * DC=mxsvlab,DC=local

Bind DN * CN=UCS Bind,OU=CiscoUCS,DC=mxsvlab,DC=local

Group Attribute member

Password * ●●●●●●●●● Show

Nested Group Search: on

Enable Encryption: off

Configure LDAP Servers

Server * ADMXSV.mxsvlab.local

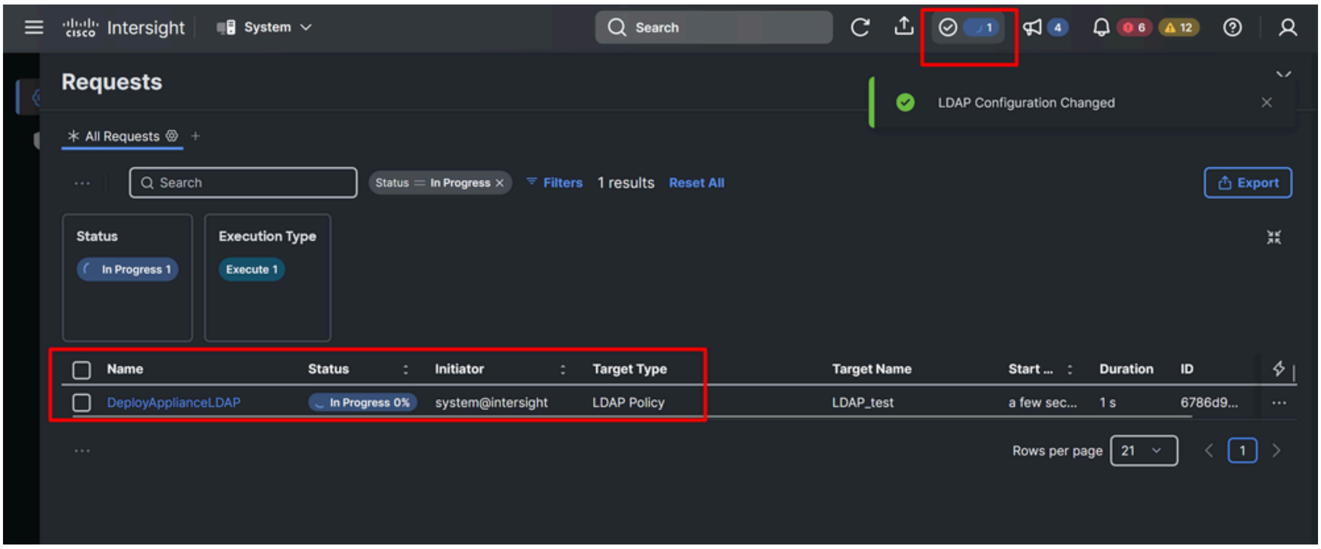
Port * 389 (1 - 65535)

Cancel Save

0 results

Configuration Example for Basic LDAP Settings

6. Monitor the workflow **DeployApplianceLDAP** from the **Requests** in the top bar.



LDAP Configuration Changed

Status = In Progress — 1 results

Status: In Progress 1 — Execution Type: Execute 1

Name	Status	Initiator	Target Type	Target Name	Start ...	Duration	ID
DeployApplianceLDAP	In Progress 0%	system@intersight	LDAP Policy	LDAP_test	a few sec...	1 s	6786d9...

Deployment Request

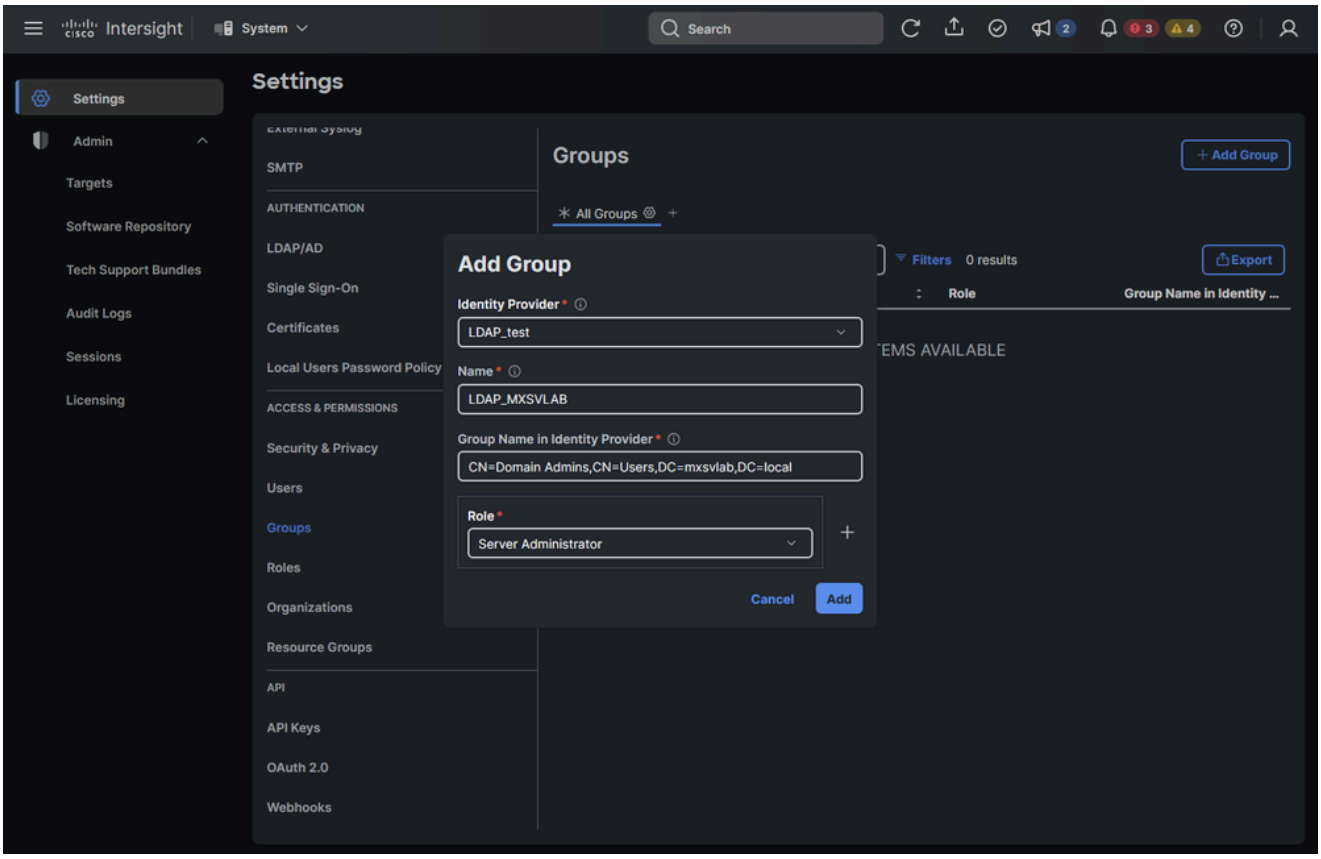
Configure Users and Groups

Once the workflow **DeployApplianceLDAP** is completed, you can configure either **Groups** or individual **Users**.

If you decide to use Groups, the authorization is provided to all the users that belong to that Group. If you use individual Users, then you need to add each user with its own authorization role.

Configure Groups

1. Navigate to **System** > **Settings** > **ACCESS & PERMISSION** > **Groups**.
2. Click **Add Group**.
3. Select the **Identity Provider**. It is the name you set on the section **Configure LDAP Basic Settings**.
4. Set a name for the group.
5. Enter the value for **Group Name in Identity Provider.** It needs to match the configurations of the Group in your LDAP server.
6. Select the **Role** depending on the level of access that you want to provide to the users in this group. See Roles and Privileges in Intersight.



Add Group

Identity Provider * LDAP_test

Name * LDAP_MXSVLAB

Group Name in Identity Provider * CN=Domain Admins,CN=Users,DC=mxsvlab,DC=local

Role * Server Administrator

Cancel Add

Configuration Example for a Group

Configure Users

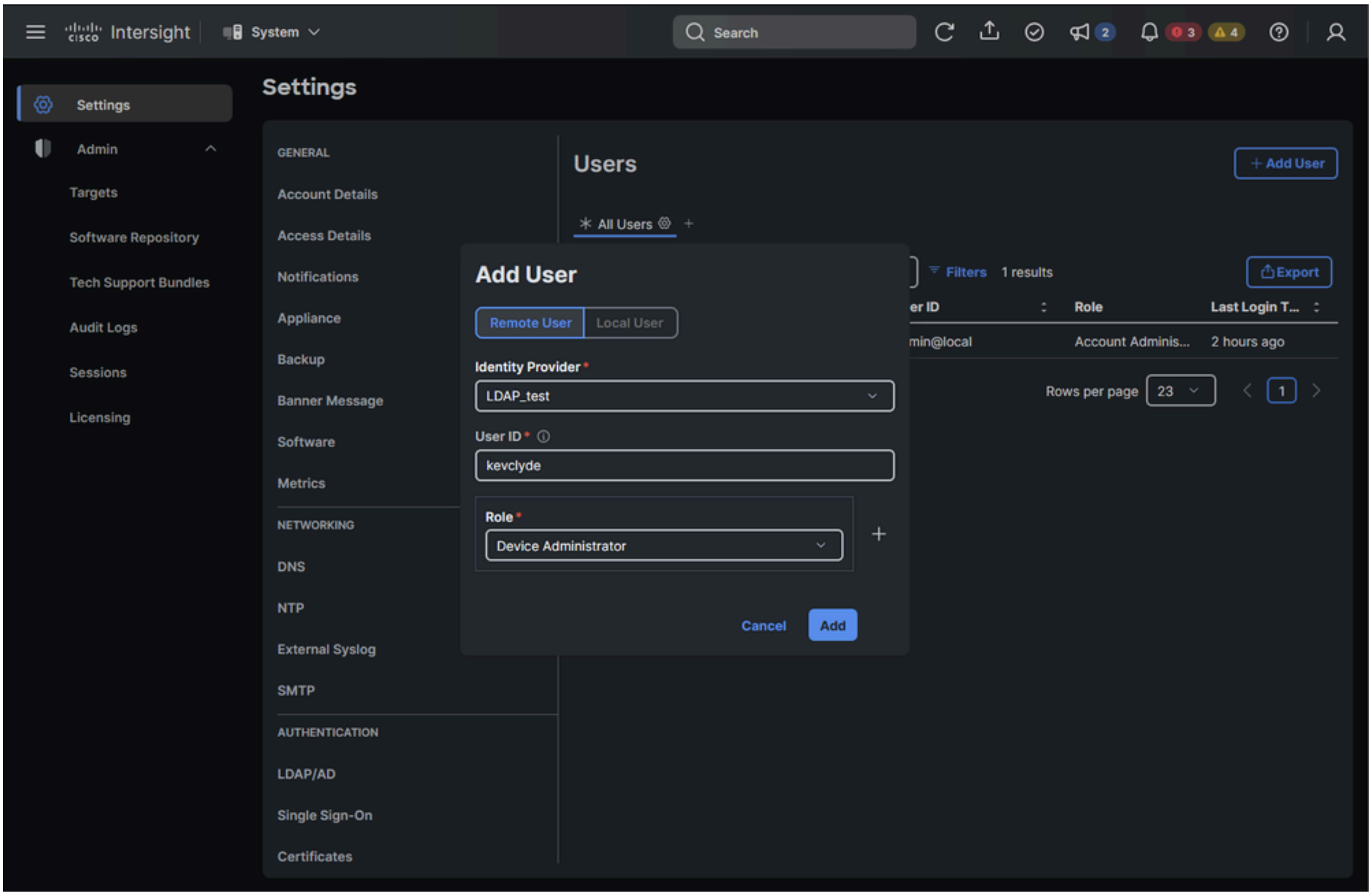
If you prefer to configure individual users instead of Groups, please adhere to these instructions:

1. Navigate to **System** > **Settings** > **ACCESS & PERMISSION** > **Users.**
2. Click **Add User**.
3. Select **Remote User**.
4. Select the **Identity Provider**. It is the name you set on the section **Configure LDAP Basic Settings**.
5. Set a **User ID**.

> **Tip:** To use the username as login method, copy in the **User ID** field, the value configured as **sAMAccountName** in your LDAP server.
> If you want to use the email, ensure that you set the email of the user in the **mail** attribute in the LDAP server.

6. Select the Role depending on the level of access that you want to provide to the user. See Roles and

[Privileges in Intersight](#).



Identity Provider * LDAP_test

User ID * kevclyde

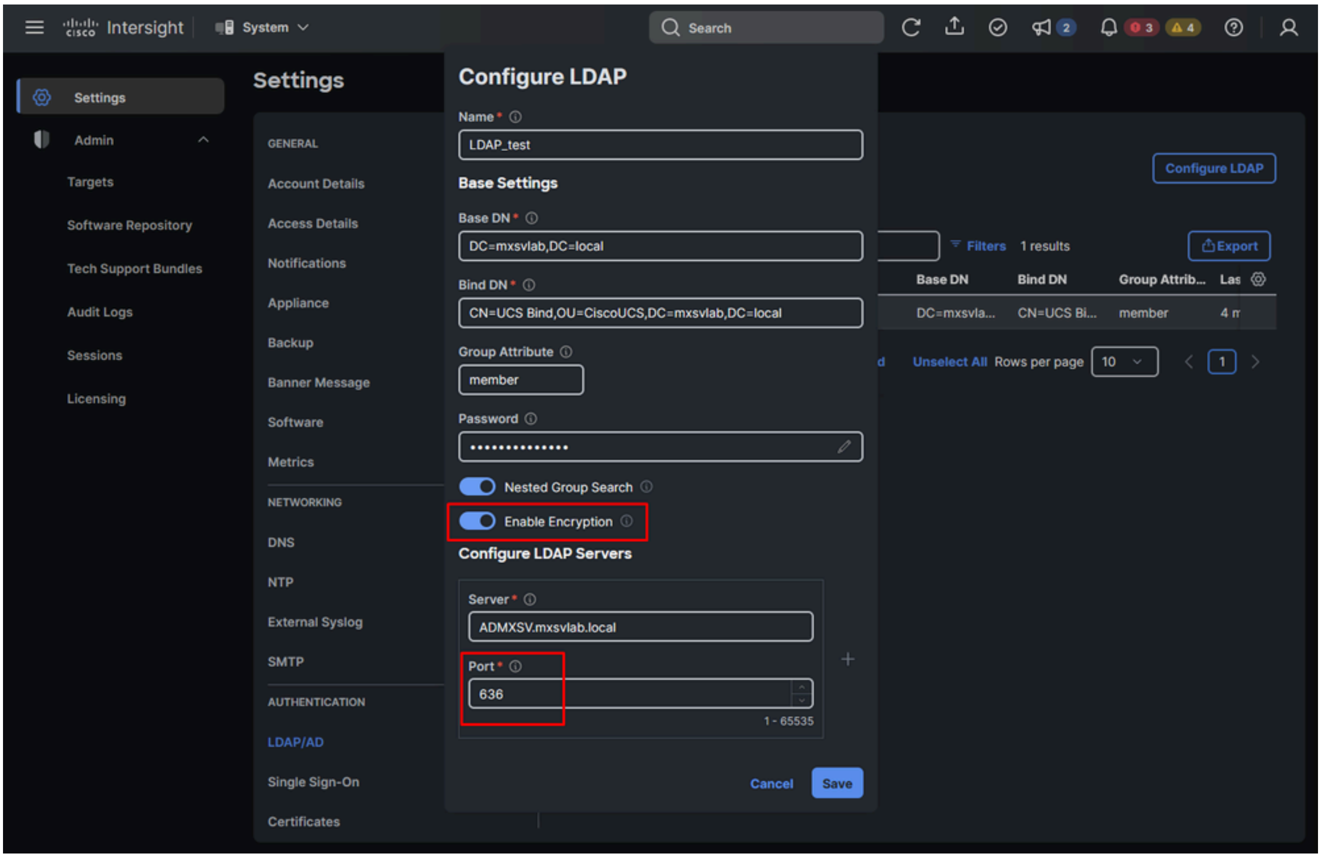
Role * Device Administrator

Configuration Example for a User

Configuration of LDAPS (Secure LDAP)

If you want your LDAP communication to be secured with encryption, you need to have a certificate signed by your CA. Ensure to apply these changes to the configuration:

1. Complete the steps from **Configuration of LDAP Basic Settings** but ensure to move the slider **Enable Encryption** to the right (Step 3.g).
2. Ensure that the port used is either **636** or **3269** which are the ports that support LDAPS (secure). All other ports support LDAP over TLS.



Configure LDAP

Name * LDAP_test

Base Settings

Base DN * DC=mxsvlab,DC=local

Bind DN * CN=UCS Bind,OU=CiscoUCS,DC=mxsvlab,DC=local

Group Attribute member

Password ••••••••••••••

Nested Group Search

Enable Encryption

Configure LDAP Servers

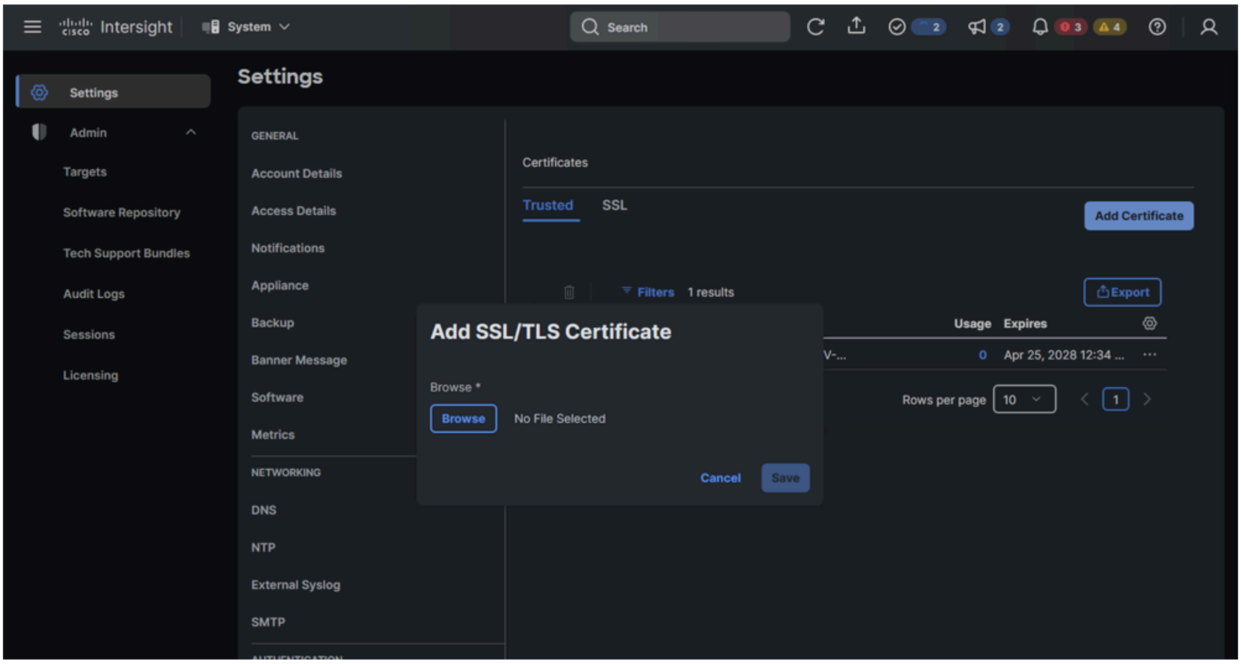
Server * ADMXSV.mxsvlab.local

Port * 636

1 - 65535

Configuration Changes for Secure LDAP

3. Save the configuration and wait for the workflow **DeployApplianceLDAP** to finish.
4. Add a certificate with the next steps:
   1. Navigate to **System** > **Settings** > **AUTHENTICATION** > **Certificates** > **Trusted.**
   2. Click **Add Certificate**.
   3. Click **Browse** and select a **.pem** file that contains the certificate issued by your CA.



Add SSL/TLS Certificate

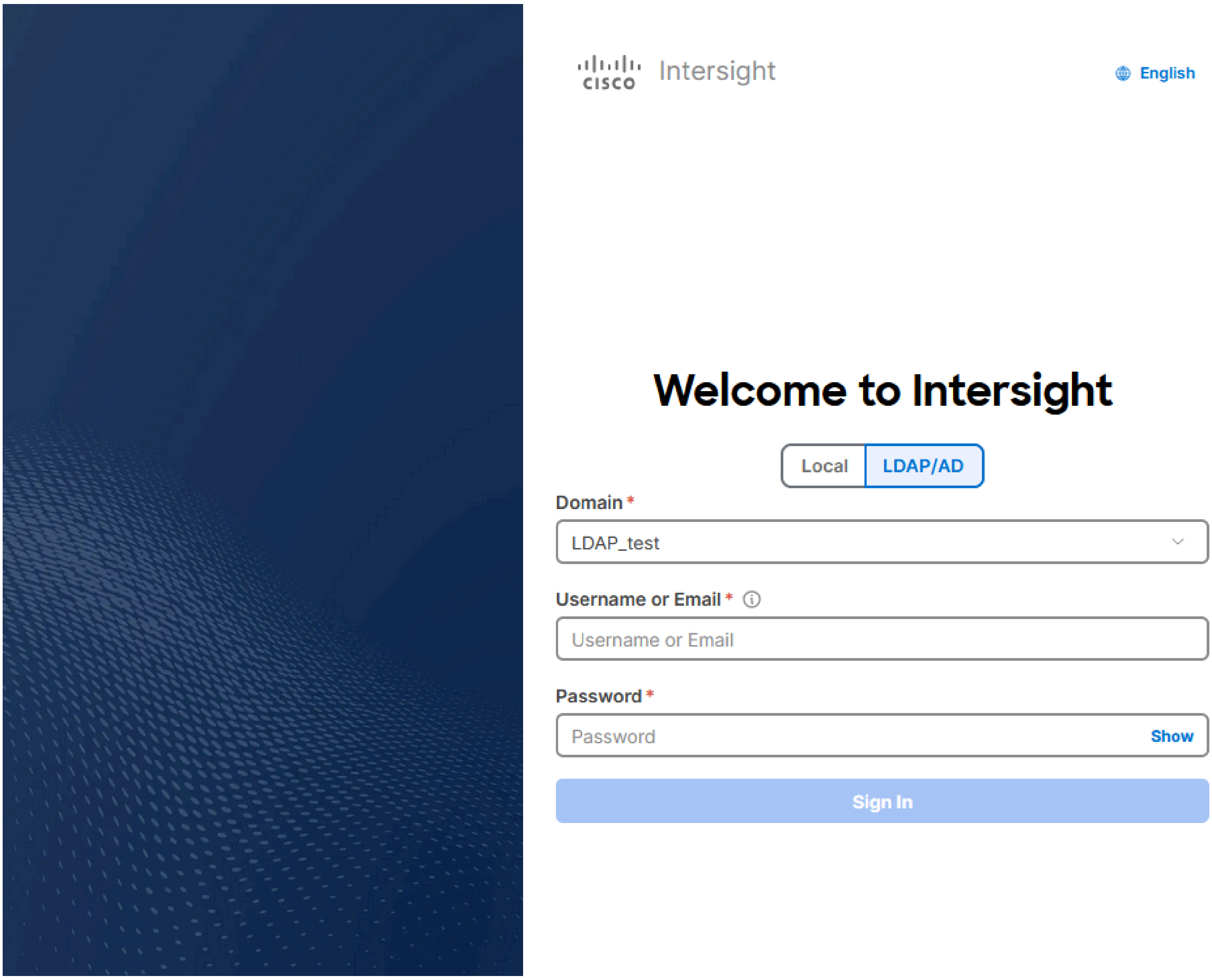
Browse *

Browse No File Selected

Configuration to Add a Certificate

Verify

In your browser, navigate to your Intersight Virtual Appliance URL. The screen now displays an option to login with LDAP credentials:



Welcome to Intersight

Domain * LDAP_test

Username or Email * Username or Email

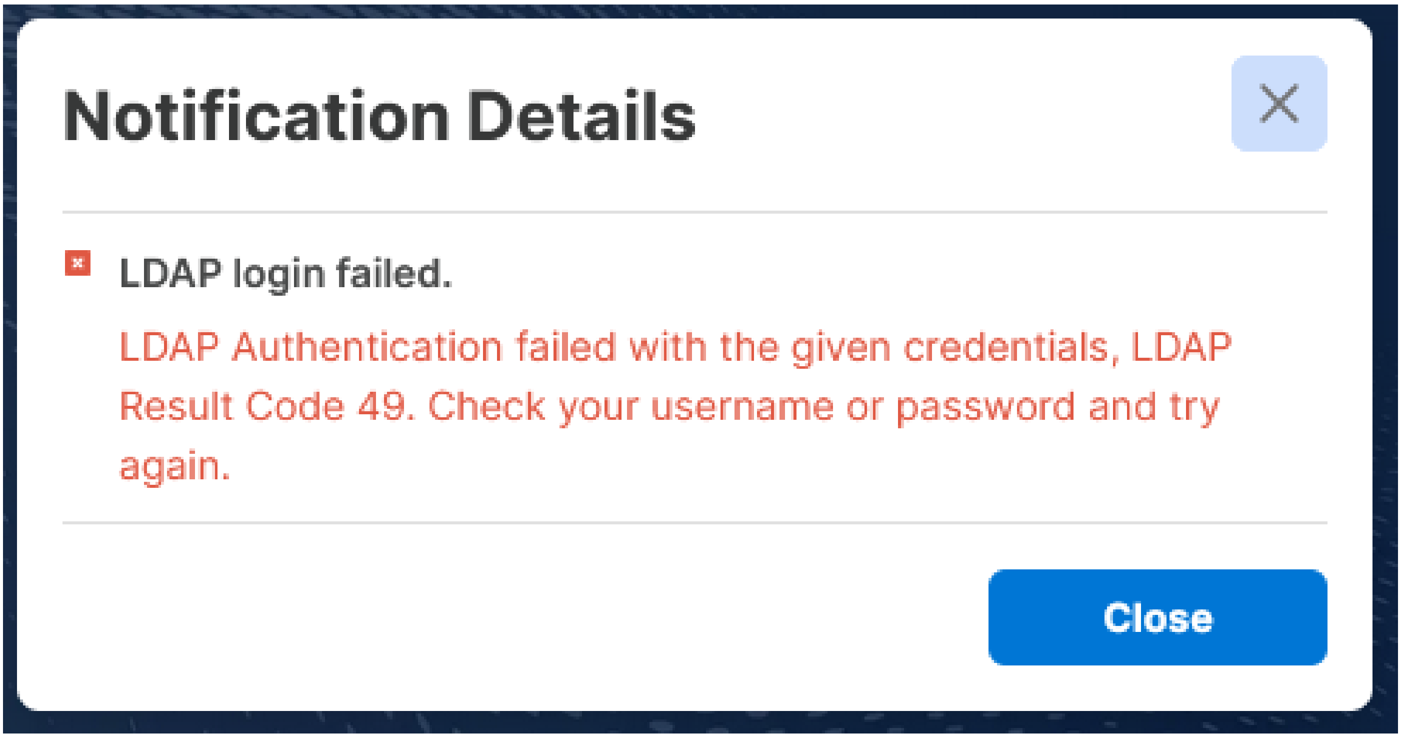
Password * Password

LDAP Configuraton Enabled from Login Screen

Troubleshoot

If the login fails, the error messages provide hints on what could be wrong.

Error 1. Wrong Access Details



LDAP login failed.

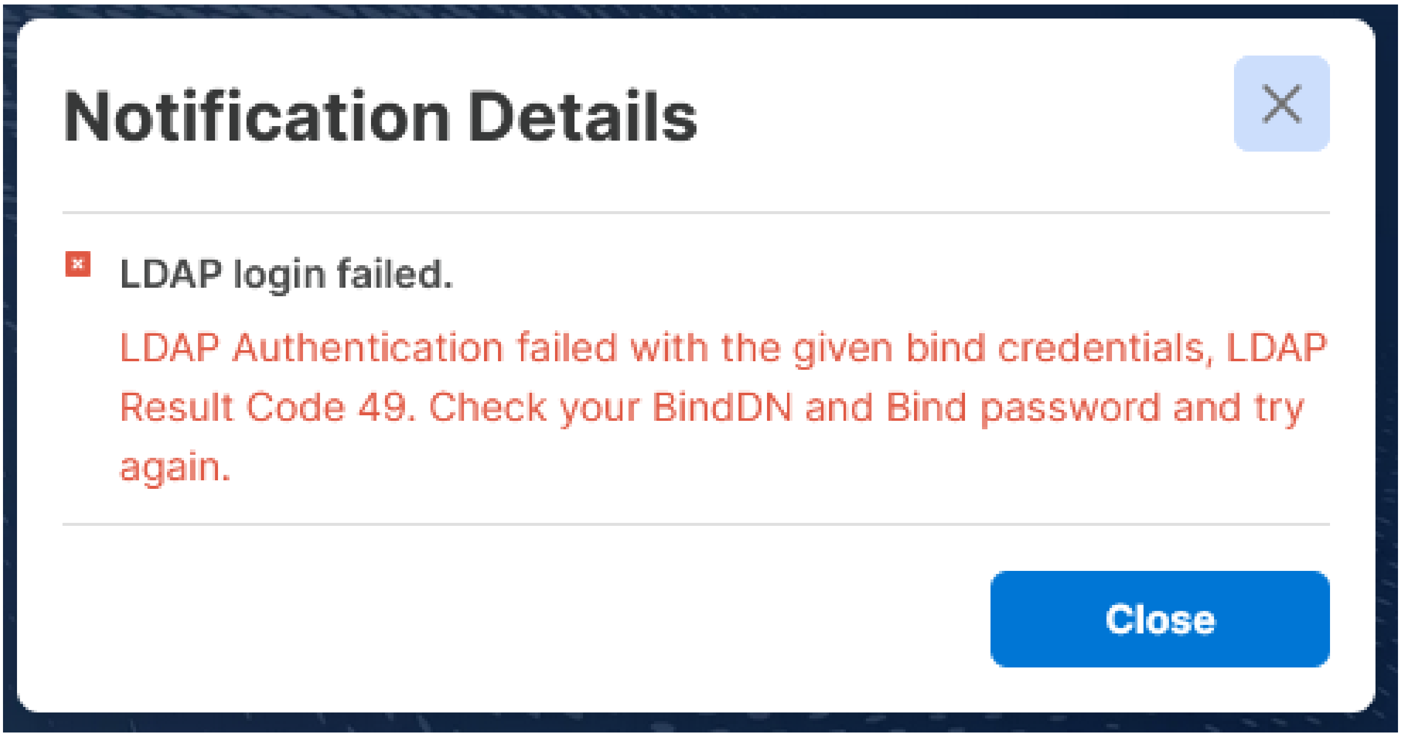
LDAP Authentication failed with the given credentials, LDAP Result Code 49. Check your username or password and try again.

Error Message for Wrong Password Error

This error means the access data is incorrect.

1. Verify the username and password are correct.

Error 2. Wrong Bind Data



LDAP login failed.

LDAP Authentication failed with the given bind credentials, LDAP Result Code 49. Check your BindDN and Bind password and try again.

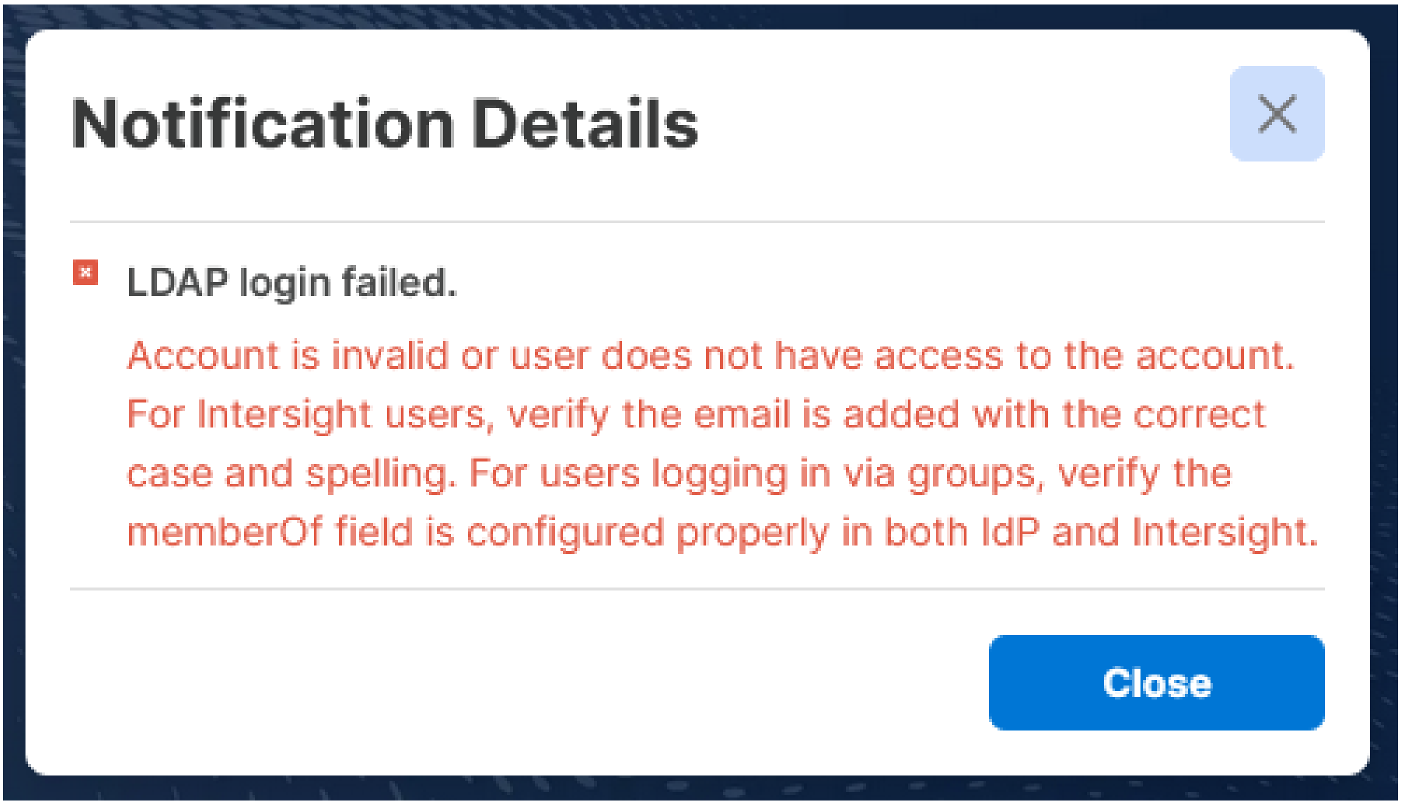
Error Message for Wrong Bind Data

This error means the bind data is incorrect.

1. Verify the **BindDN.**

2. Verify the bind password configured in the LDAP settings.

Error 3. Unable to Find User



Notification Details

LDAP login failed.

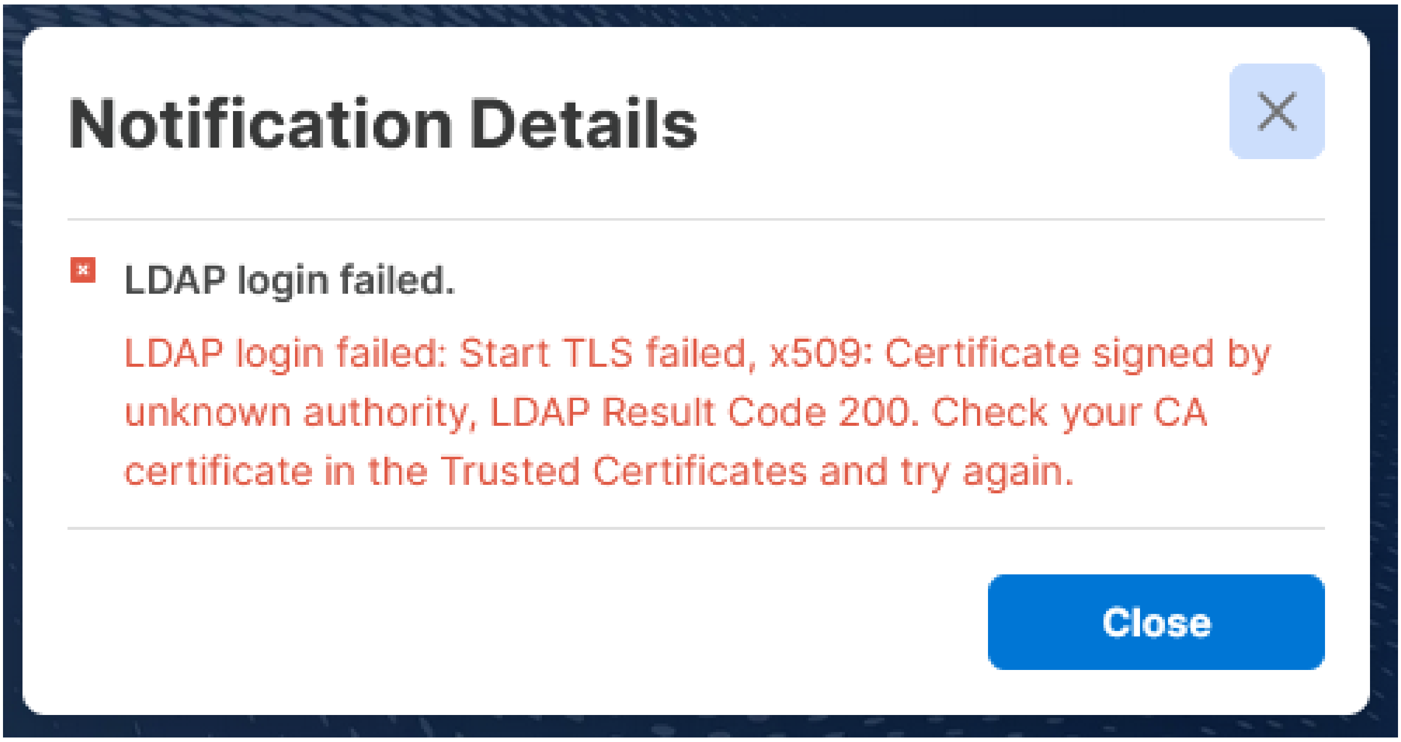
Account is invalid or user does not have access to the account. For Intersight users, verify the email is added with the correct case and spelling. For users logging in via groups, verify the memberOf field is configured properly in both IdP and Intersight.

Error Message for User not Found

This is triggered when the search in the LDAP server does not return any authorized users. Verify the next settings are correct:

1. Check **BaseDN**. The parameters used to look for the user are wrong.
2. Ensure the **Group Attribute** is set to member instead of memberOf.
3. Verify the **Group Name in Identity Provider** in the **Groups** configuration is correct. This applies only when authorization is provided via Groups.
4. Verify the email of the user is set properly in the **mail** field in the AD configuration for the user. This applies only when authorization is provided to individual Users.

Error 4. Wrong Certificate



LDAP login failed.

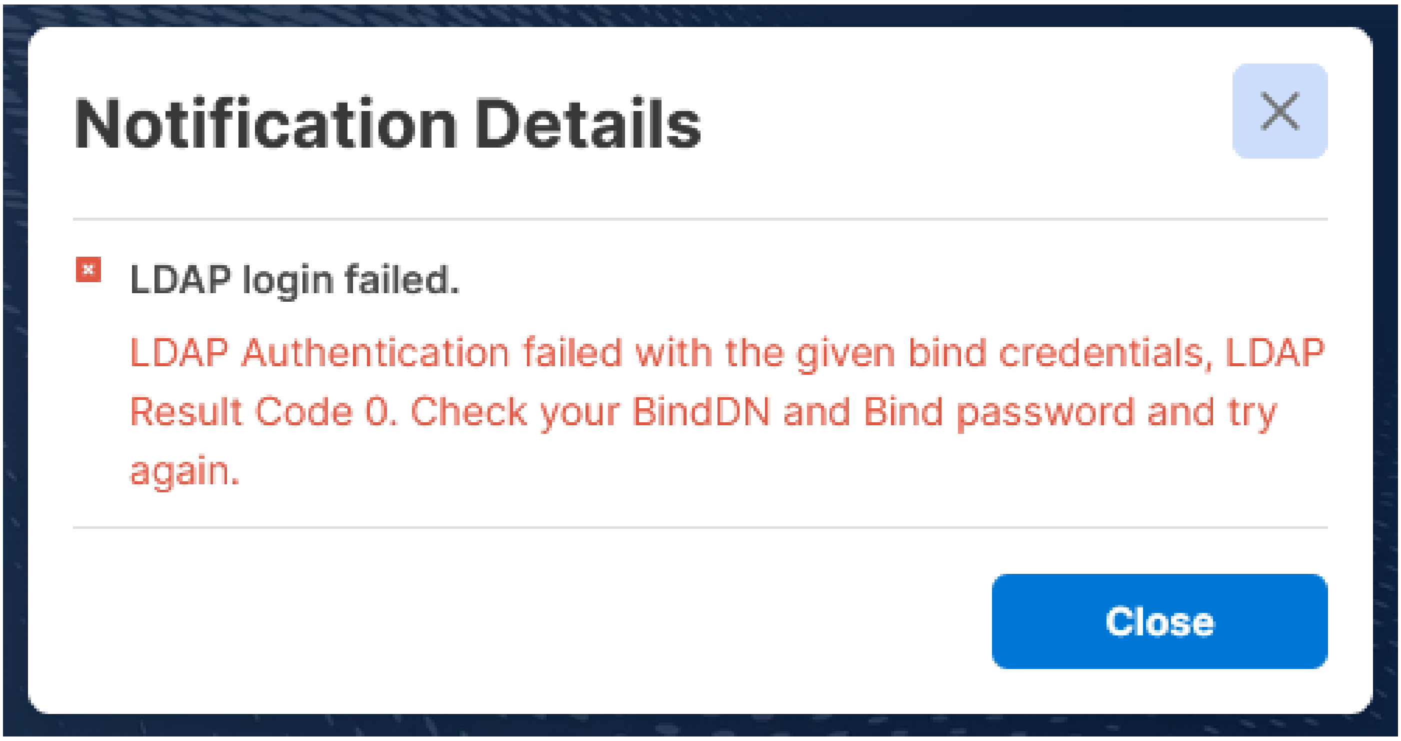
LDAP login failed: Start TLS failed, x509: Certificate signed by unknown authority, LDAP Result Code 200. Check your CA certificate in the Trusted Certificates and try again.

Error Message for Wrong Certificate

If encrypted LDAP is enabled:

1. Verify the certificate is configured and it includes the correct complete certificate.

Error 5. Enable Encryption is Used with a Secure Port



LDAP login failed.

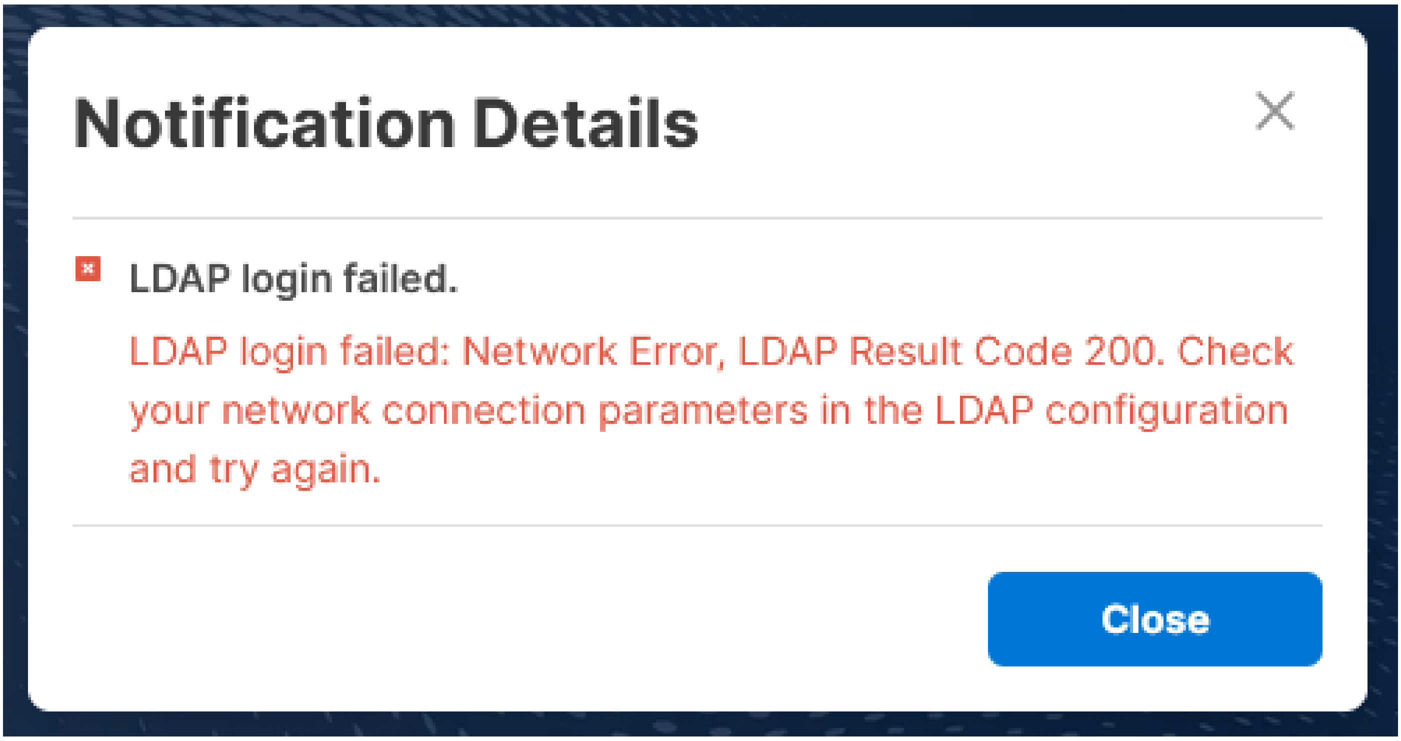
LDAP Authentication failed with the given bind credentials, LDAP Result Code 0. Check your BindDN and Bind password and try again.

Error Message for Enable Encryption is Disabled

This error appears when **Enable Encryption** is not enabled but a port for secure LDAP is configured.

1. Ensure that you use port 389 if encryption is not enabled.

Error 6. Connection Parameters Wrong



Notification Details

☒ LDAP login failed.

LDAP login failed: Network Error, LDAP Result Code 200. Check your network connection parameters in the LDAP configuration and try again.

Error Message for Wrong Port

This error means that it was not possible to establish a successful connection to the LDAP server. Please verify:

1. The DNS server rmust resolve the hostname of the LDAP server to the correct IP.
2. Intersight appliance is able to reach the LDAP server.
3. Ensure port 389 is used for unencrypted LDAP, 636 or 3269 for secure LDAP (LDAPS) and any other for TLS (enable encryption and set up a certificate).

Related Information

- Integrating the Cisco Intersight Virtual Appliance with LDAP (video)
- Configure LDAP settings in Intersight Appliance
- Roles and Privileges in Intersight
- Sample Configuration for LDAP in UCSM