

在Intersight虚拟设备中配置LDAP

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[LDAP基本设置的配置](#)

[配置用户和组](#)

[配置组](#)

[配置用户](#)

[配置LDAPS \(安全LDAP\)](#)

[验证](#)

[故障排除](#)

[错误1.访问详细信息错误](#)

[错误2.错误的绑定数据](#)

[错误3.找不到用户](#)

[错误4.错误的证书](#)

[错误5.启用加密用于安全端口](#)

[错误6.连接参数错误](#)

[相关信息](#)

简介

本文档介绍在Intersight专用虚拟设备(PVA)中配置LDAP身份验证的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- 轻型目录访问协议(LDAP)协议。
- Intersight专用虚拟设备。
- 域名服务器(DNS)服务器。

使用的组件

- Intersight专用虚拟设备。

- Microsoft Active Directory.
- DNS 服务器.

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

LDAP是一种用于通过网络从目录访问资源的协议。这些目录存储有关用户、组织和资源的信息。LDAP提供了访问和管理可用于身份验证和授权过程信息的标准方法。

本文档显示通过LDAP向Intersight PVA添加远程身份验证的配置流程。

配置

LDAP基本设置的配置

1. 导航到System > Settings > AUTHENTICATION > LDAP/AD。
2. 单击Configure LDAP。
3. 输入所需信息。考虑以下建议：
 1. Name是任意设置的，不会影响配置。
 2. 对于BaseDN和BindDN，请从Active Directory(AD)配置复制并粘贴相应的值。
 3. Group Attribute的默认值为member。



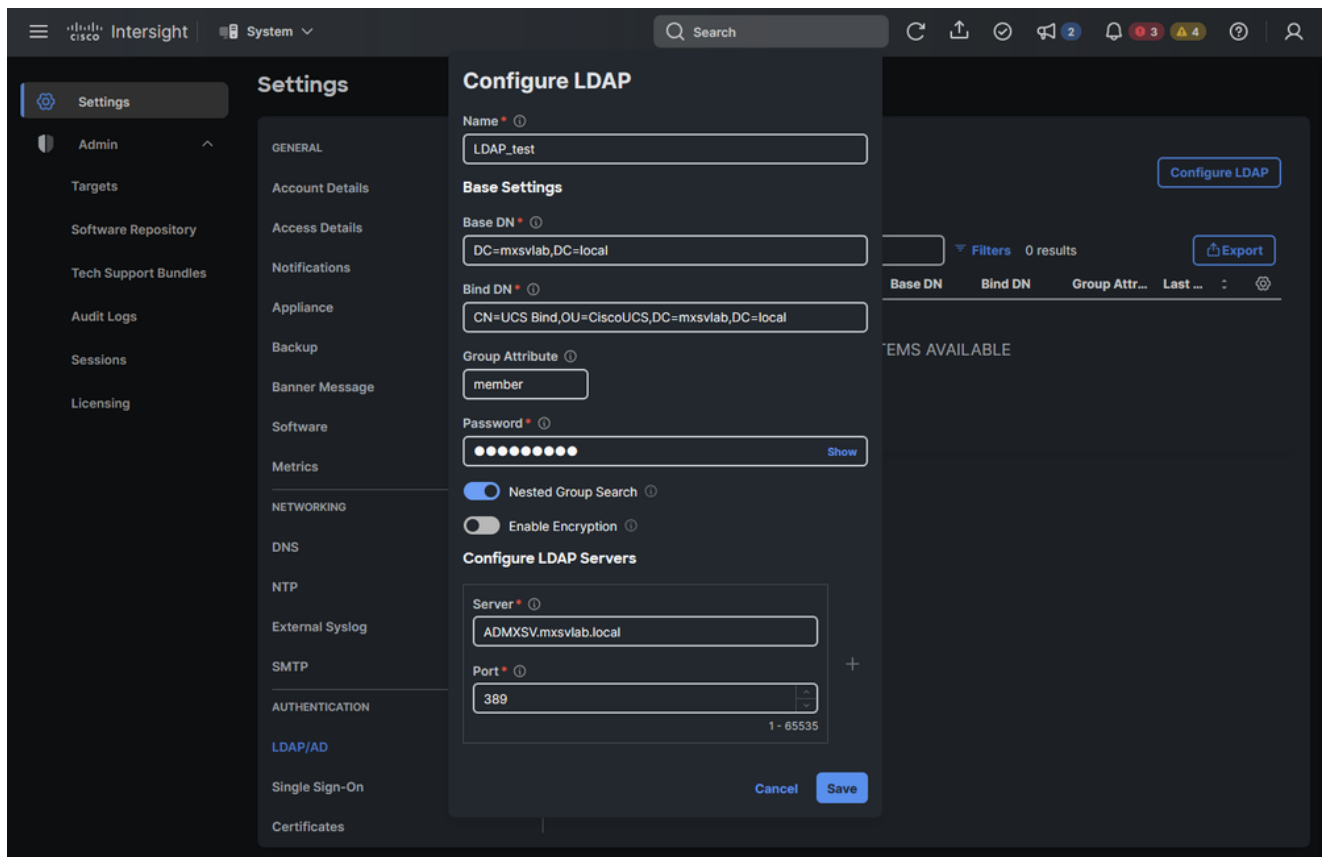
注意：在其他UCS管理工具（如UCSM或CIMC）中，组属性设置为memberOf。在Intersight中，建议将其保留为成员。

4. 输入此LDAP提供程序的密码。
5. 如果要在AD中允许对来自根的所有组及其包含的组进行递归搜索，请启用嵌套组搜索切换。
6. 对于常规LDAP配置，请将Enable Encryption保留为禁用。如果需要安全LDAP，请启用它，并确保查看LDAPS（安全LDAP）的配置部分，了解需要配置的补充步骤。
4. 添加一个LDAP服务器的配置：
 1. 在Server中，介绍LDAP服务器的IP或主机名。



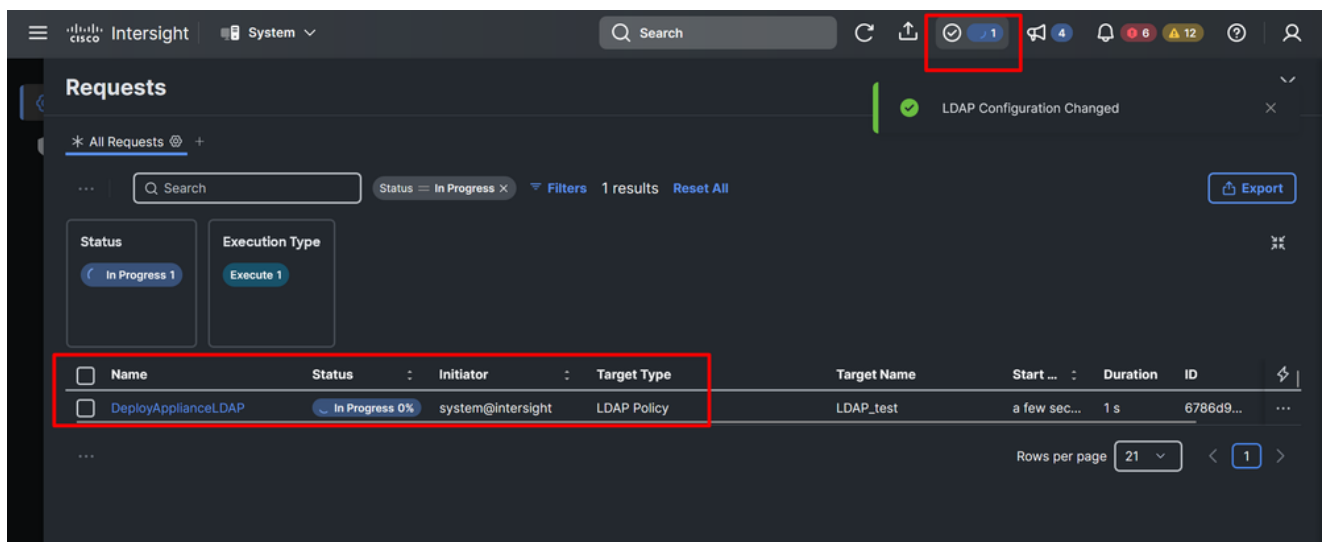
警告：如果使用主机名，请确保DNS能够正确映射该主机名。

2. LDAP的默认端口和推荐端口为389（1000到1000）。
5. Click Save.



基本LDAP设置的配置示例

6. 从顶部栏中的请求监控 workflows DeployApplianceLDAP。



部署请求

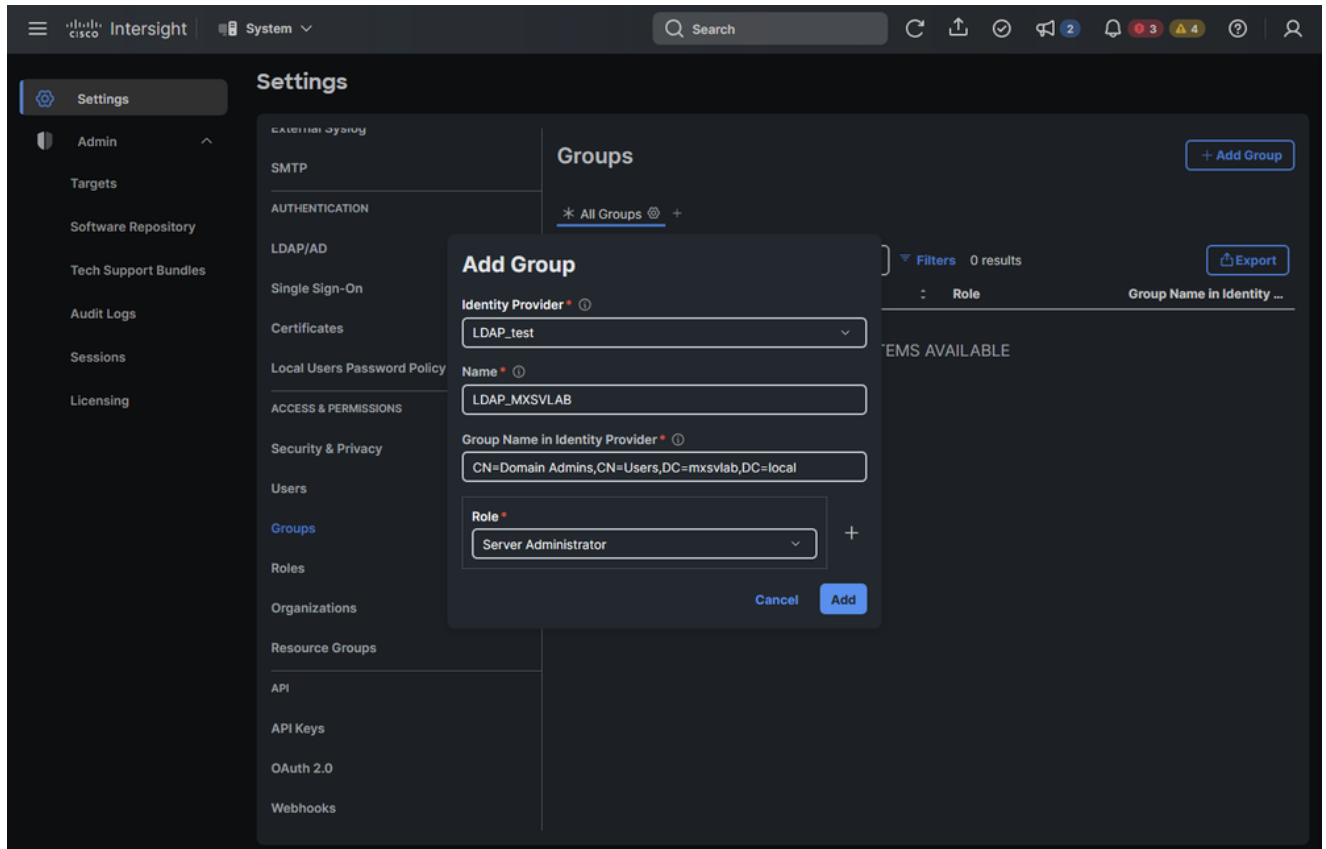
配置用户和组

工作流程DeployApplianceLDAP完成后，您可以配置Groups或单个Users。

如果您决定使用组，授权将提供给属于该组的所有用户。如果您使用单个用户，则需要添加每个具有其自己的授权角色的用户。

配置组

1. 导航到系统>设置>访问和权限>组。
2. 单击Add Group。
3. 选择Identity Provider。它是在配置LDAP基本设置部分中设置的名称。
4. 设置组的名称。
5. 在身份提供程序中输入组名称的值。它需要与LDAP服务器中的组配置匹配。
6. 选择Role，具体取决于要为此组中的用户提供访问的级别。请参阅[Intersight中的角色和权限](#)。



组的配置示例

配置用户

如果您更喜欢配置单个用户而不是组，请遵循以下说明：

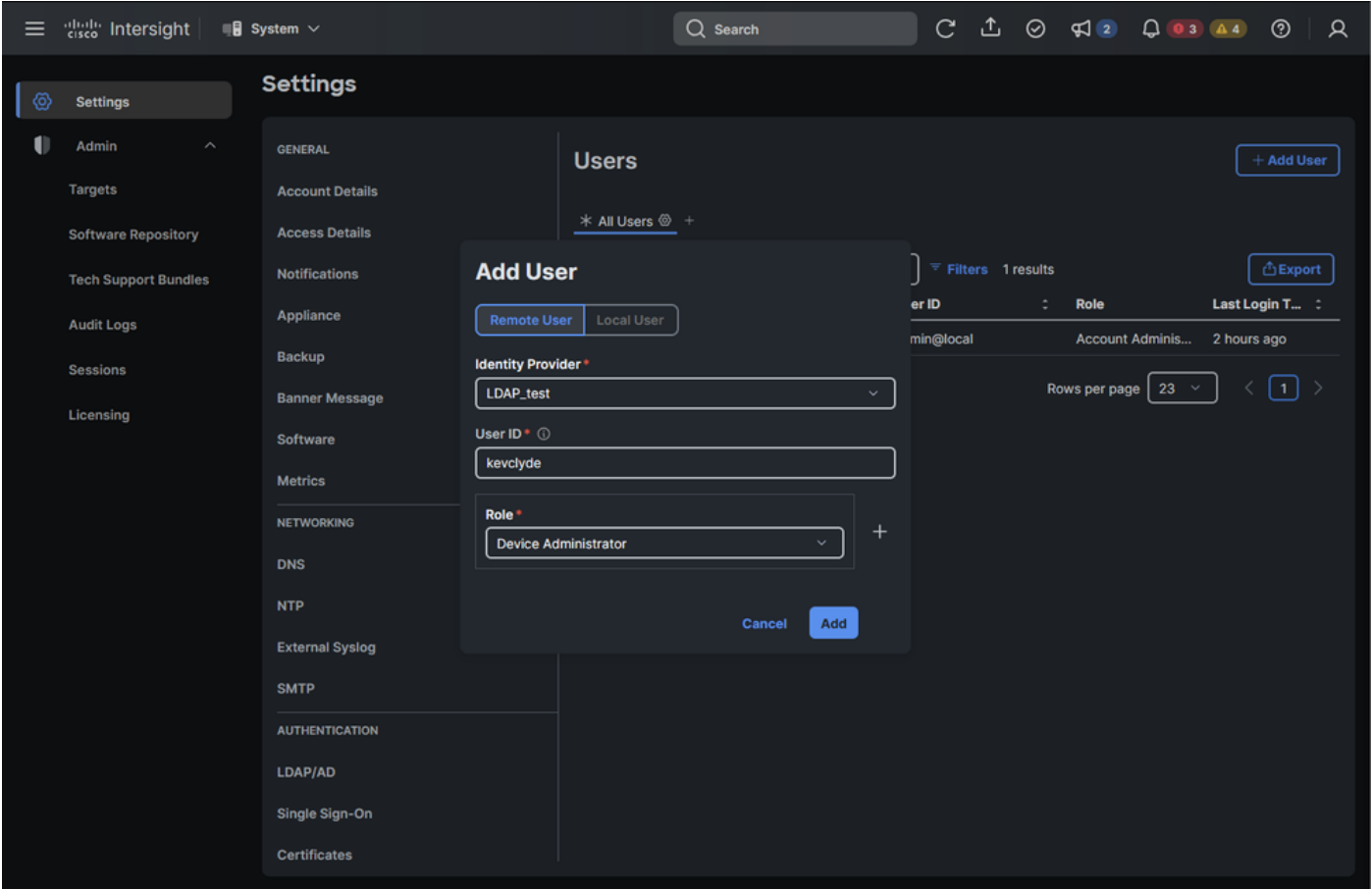
1. 导航到System > Settings > ACCESS & PERMISSION > Users。
2. 单击Add User。
3. 选择Remote User。
4. 选择Identity Provider。它是在配置LDAP基本设置部分中设置的名称。
5. 设置用户ID。



提示：要将用户名用作登录方法，请在User ID字段中复制在LDAP服务器中配置为sAMAccountName的值。

如果要使用电子邮件，请确保在LDAP服务器的mail属性中设置用户的电子邮件。

6. 根据要提供给用户的访问级别选择角色。请参阅[Intersight中的角色和权限](#)。

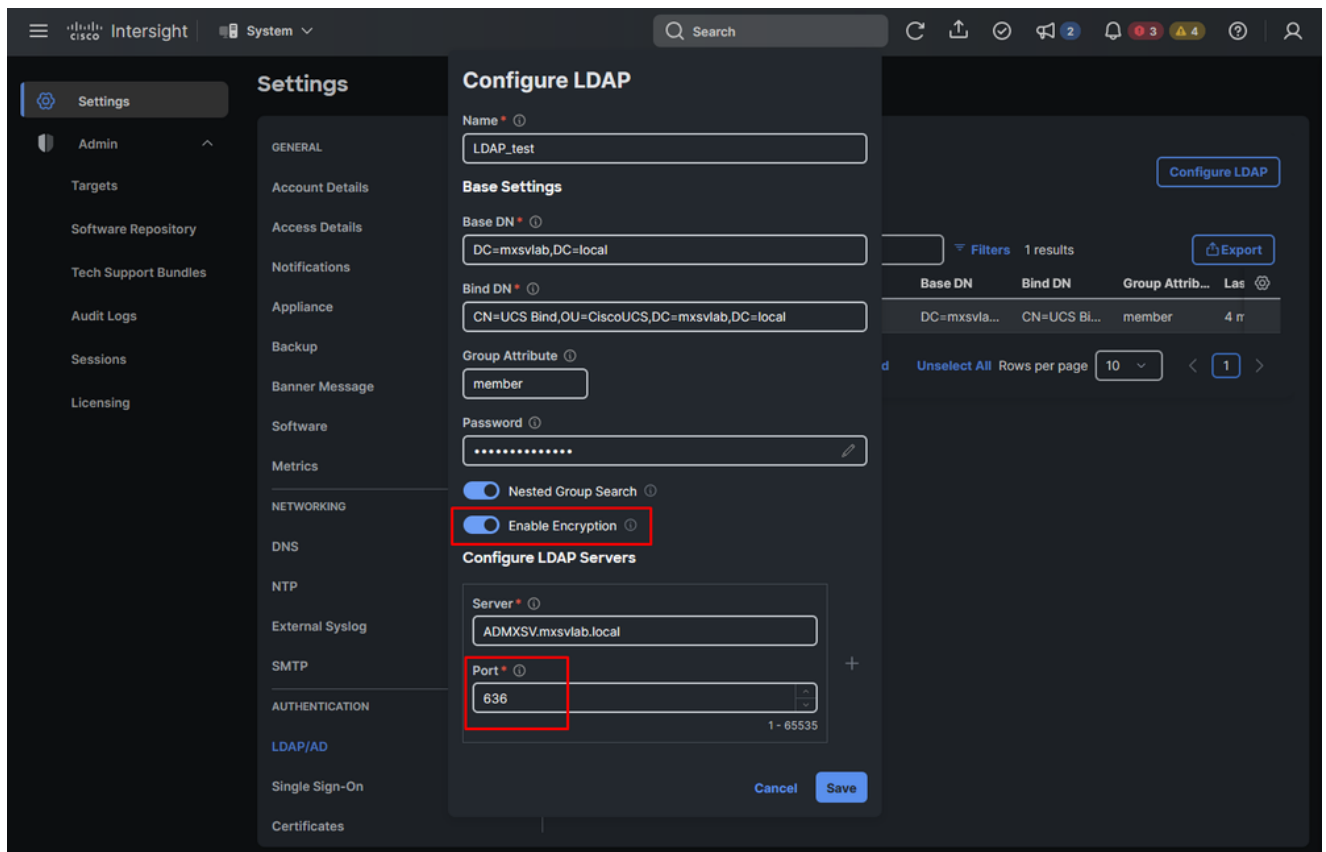


用户的配置示例

配置LDAPS (安全LDAP)

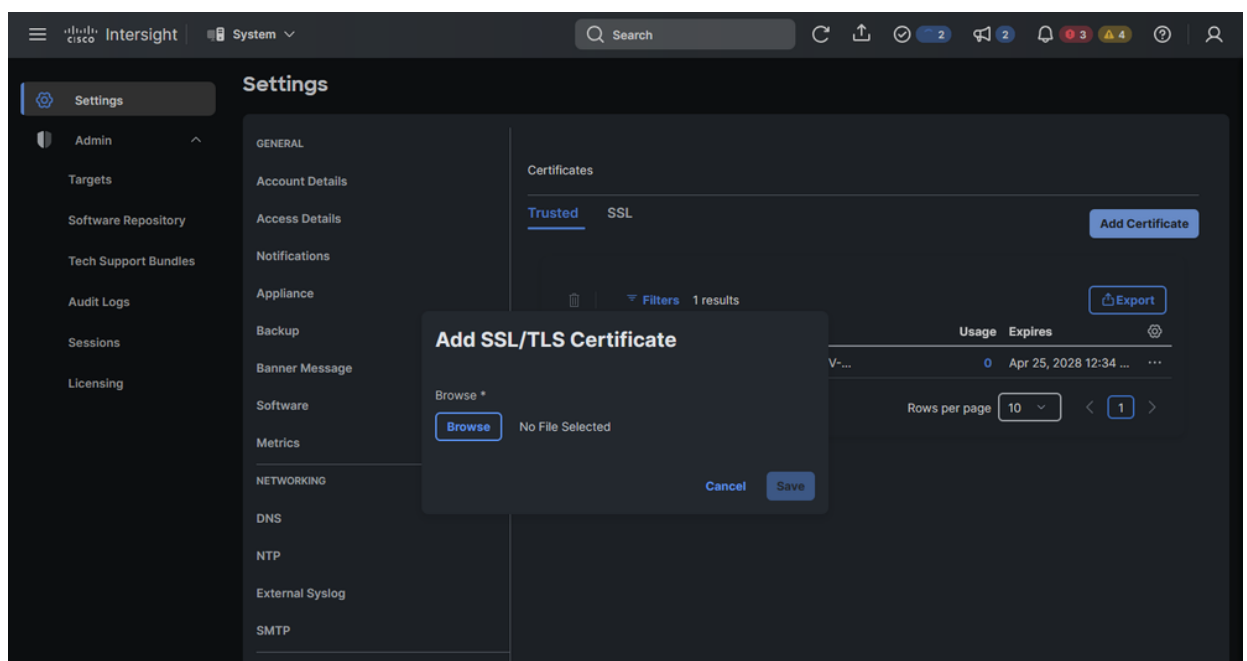
如果您希望通过加密保护您的LDAP通信，则需要由CA签名的证书。确保将这些更改应用到配置：

1. 完成LDAP基本设置配置中的步骤，但确保将启用加密滑块移至右侧（第3.g步）。
2. 确保使用的端口是636或3269，它们是支持LDAPS（安全）的端口。所有其他端口都支持通过TLS的LDAP。



安全LDAP的配置更改

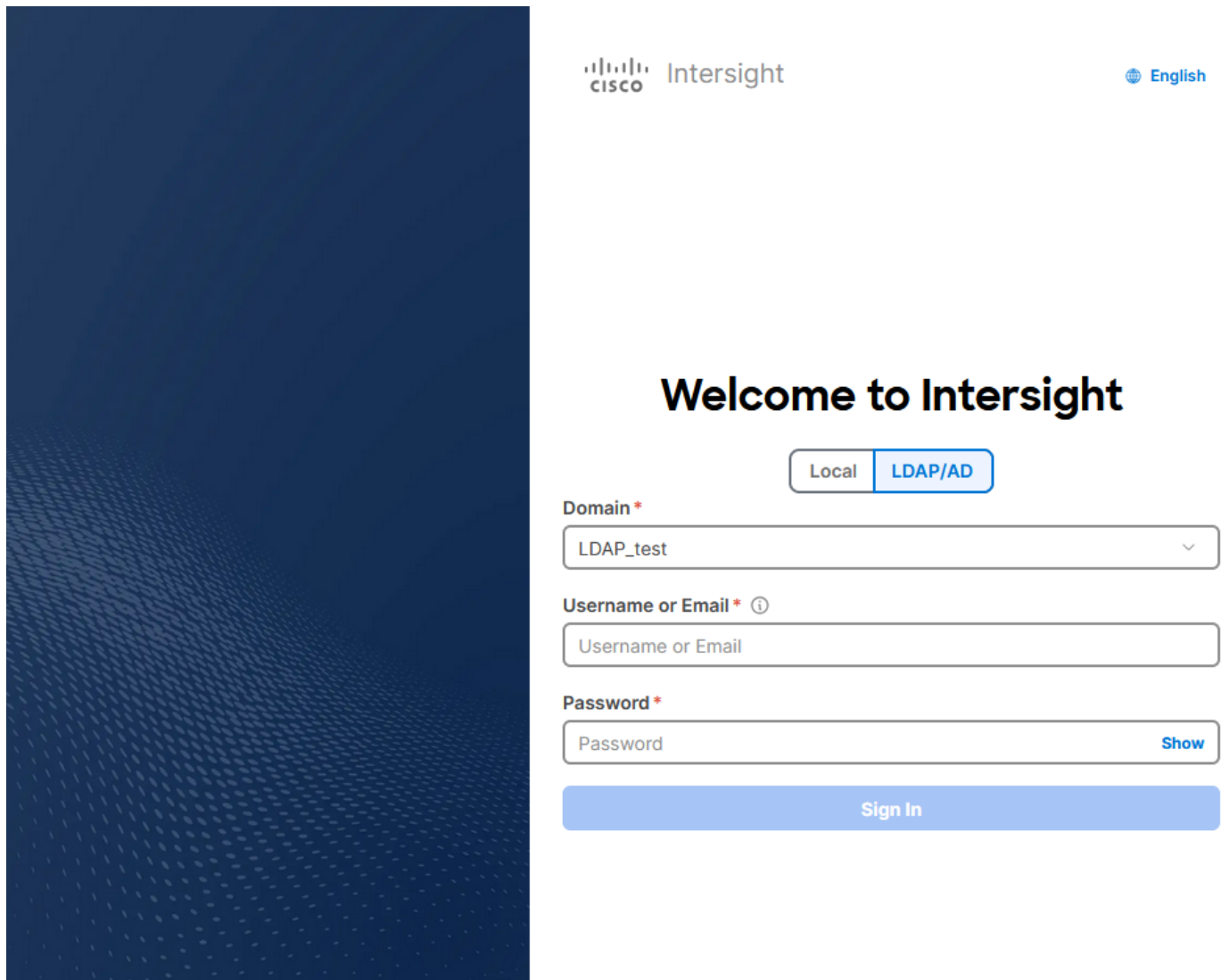
3. 保存配置并等待工作流DeployApplianceLDAP完成。
4. 使用后续步骤添加证书：
 1. 导航到System > Settings > AUTHENTICATION > Certificates > Trusted。
 2. 点击添加证书。
 3. 单击Browse并选择包含CA颁发的证书的 .pem 文件。



添加证书的配置

验证

在浏览器中，导航至Intersight虚拟设备URL。屏幕现在显示使用LDAP凭证登录的选项：



The screenshot shows the Cisco Intersight login interface. On the left is a dark blue background with a subtle pattern of small white dots. On the right, the Cisco Intersight logo is at the top, with a language selector set to 'English'. Below the logo, the text 'Welcome to Intersight' is displayed. There are two tabs for authentication: 'Local' and 'LDAP/AD', with 'LDAP/AD' being the active tab. Below the tabs, there are three input fields: 'Domain' with a dropdown menu showing 'LDAP_test', 'Username or Email' with a placeholder 'Username or Email', and 'Password' with a placeholder 'Password' and a 'Show' link. At the bottom is a large blue 'Sign In' button.

从登录屏幕启用LDAP配置

故障排除

如果登录失败，则错误消息会提供关于可能出错内容的提示。

错误1.访问详细信息错误

Notification Details



✖ LDAP login failed.

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

Close

错误密码错误错误消息

此错误表示访问数据不正确。

1. 验证用户名和密码是否正确。

错误2.错误的绑定数据

Notification Details



✖ LDAP login failed.

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

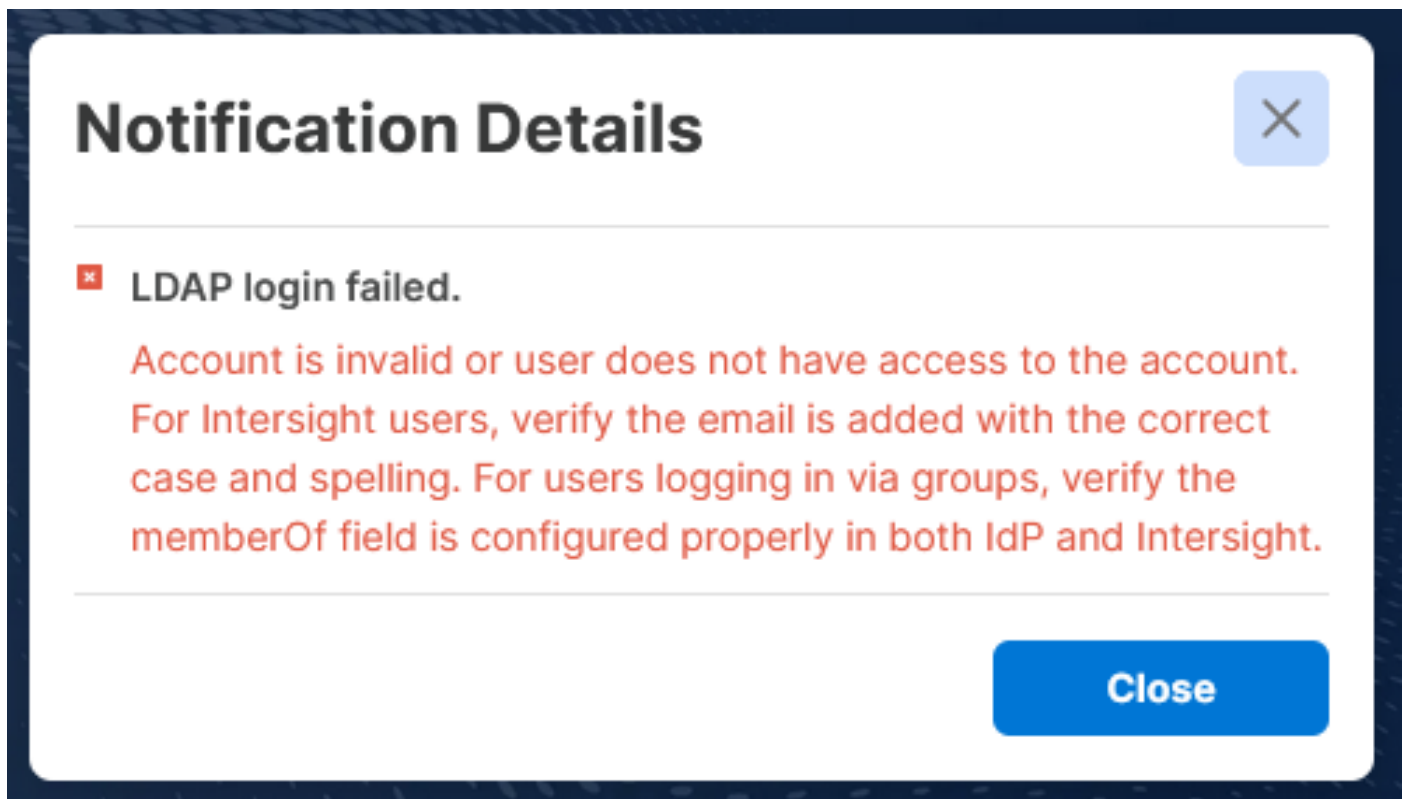
Close

错误绑定数据的错误消息

此错误表示绑定数据不正确。

1. 检验BindDN。
2. 验证在LDAP设置中配置的绑定密码。

错误3.找不到用户

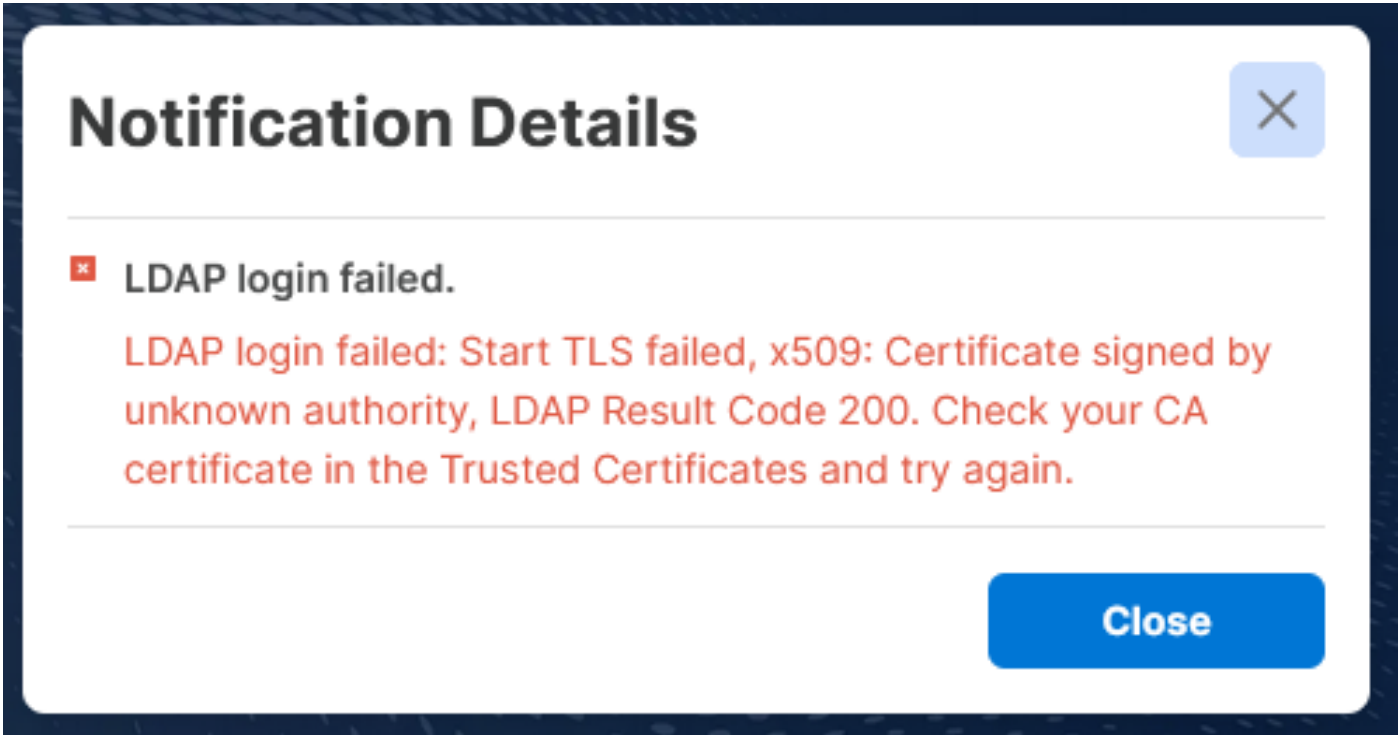


未找到用户的错误消息

当LDAP服务器中的搜索未返回任何授权用户时，会触发此功能。验证下一个设置是否正确：

1. 选中BaseDN。用于查找用户的参数错误。
2. 确保Group Attribute设置为member而不是memberOf。
3. 验证Groups配置中身份提供程序中的组名是否正确。这仅适用于通过组提供授权的情况。
4. 验证用户的AD配置中的mail字段是否正确设置了用户的邮件。这仅适用于向单个用户提供授权的情况。

错误4.错误的证书

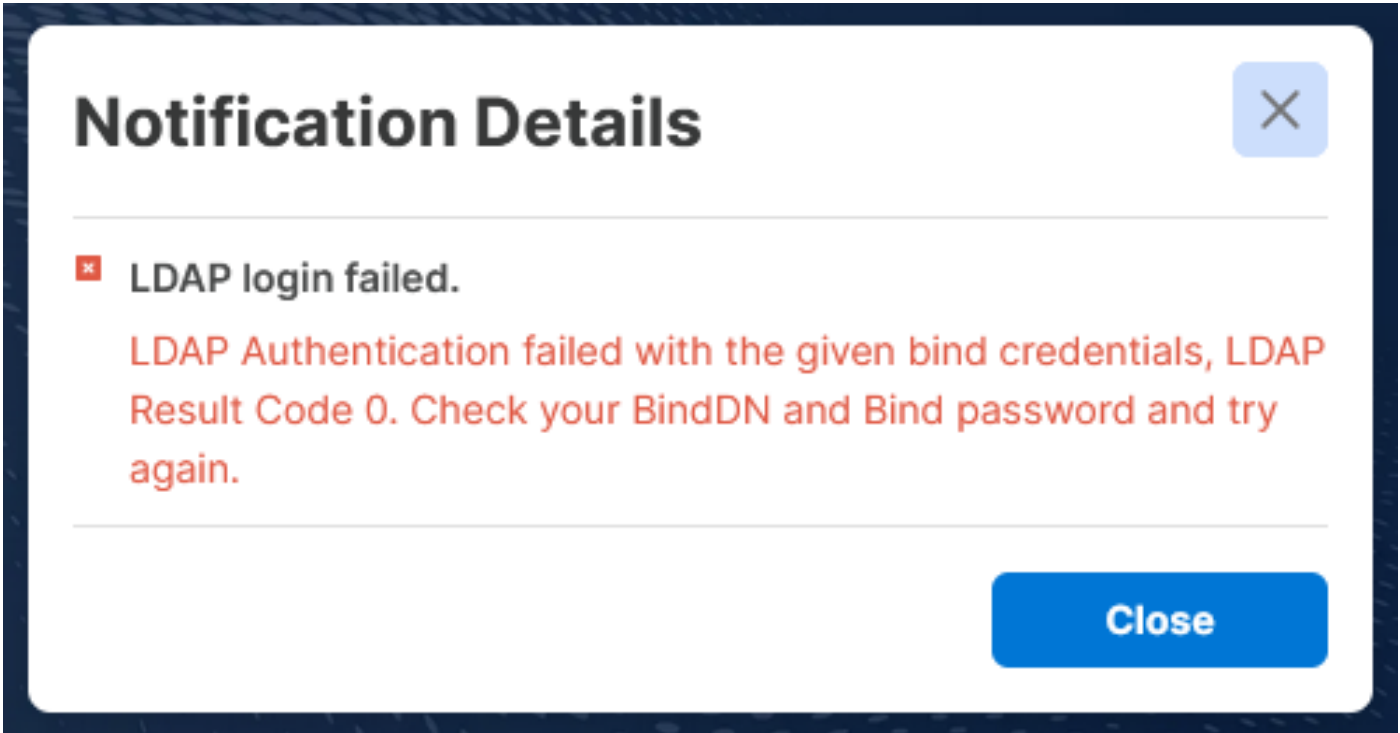


错误证书的错误消息

如果启用加密LDAP:

1. 验证证书是否已配置且包含正确的完整证书。

错误5.启用加密用于安全端口

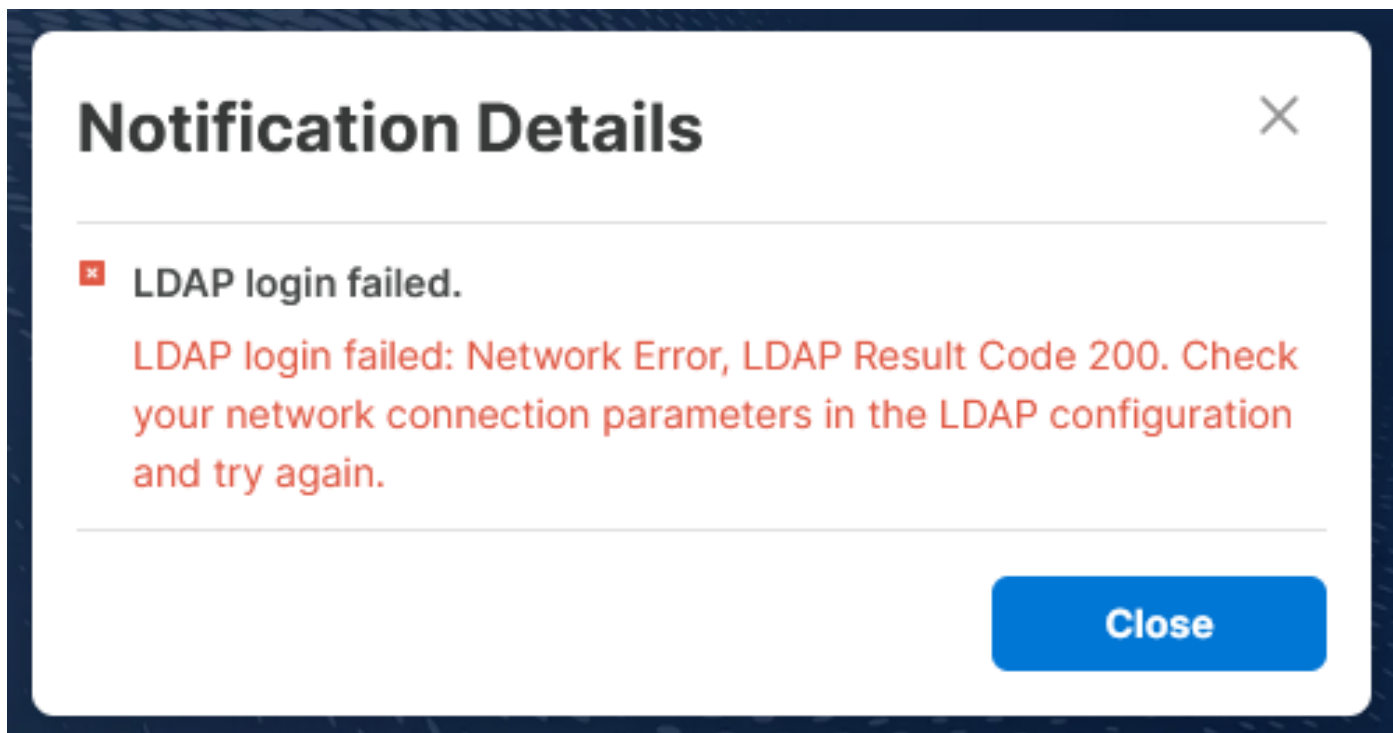


禁用启用加密的错误消息

如果未启用启用加密，但配置了安全LDAP的端口，则会出现此错误。

1. 如果未启用加密，请确保使用端口389。

错误6.连接参数错误



错误端口错误消息

此错误表示无法成功建立到LDAP服务器的连接。请验证：

1. DNS服务器必须将LDAP服务器的主机名解析为正确的IP。
2. Intersight设备能够访问LDAP服务器。
3. 确保端口389用于未加密的LDAP，636或3269用于安全LDAP(LDAPS)，而任何其他端口用于TLS（启用加密并设置证书）。

相关信息

- [将Cisco Intersight虚拟设备与LDAP集成（视频）](#)
- [在Intersight设备中配置LDAP设置](#)
- [Intersight中的角色和权限](#)
- [UCSM中LDAP的示例配置](#)

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）。