在Intersight虛擬裝置中配置LDAP

目錄

簡介

本文檔介紹在Intersight專用虛擬裝置(PVA)中配置LDAP身份驗證的過程。

必要條件

需求

思科建議您瞭解以下主題：

- 輕型目錄訪問協定(LDAP)協定。
- Intersight專用虛擬裝置。
- 網域名稱伺服器(DNS)伺服器。

採用元件

- Intersight專用虛擬裝置。

- Microsoft Active Directory。
- DNS伺服器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

LDAP是一種協定，用於通過網路從目錄訪問資源。這些目錄儲存有關使用者、組織和資源的資訊。LDAP提供了一種訪問和管理可用於身份驗證和授權過程資訊的標準方法。

本文檔介紹通過LDAP向Intersight PVA新增遠端身份驗證的配置過程。

設定

LDAP基本設定的配置

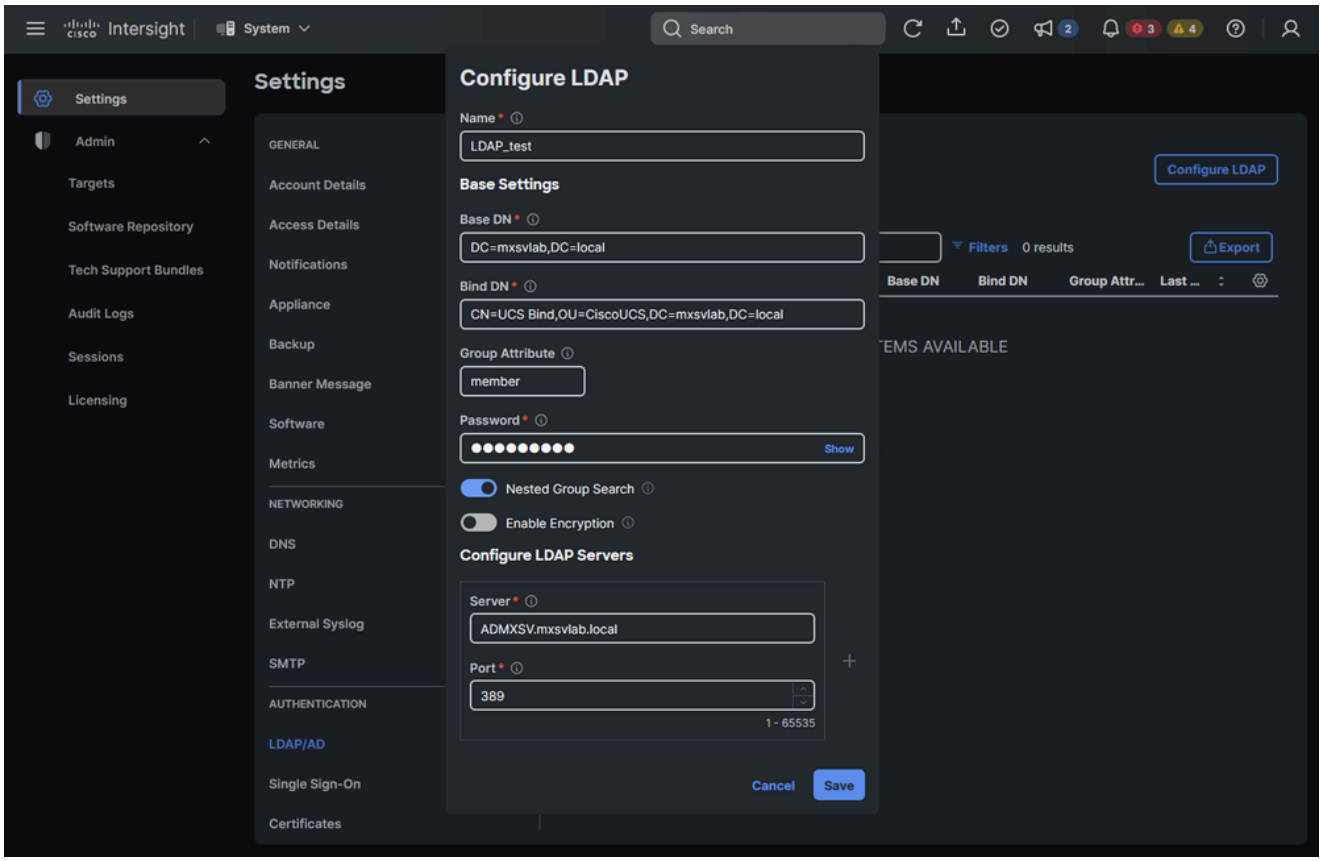
1. 導航到System > Settings > AUTHENTICATION > LDAP/AD。
2. 按一下Configure LDAP。
3. 輸入所需資訊。考慮以下建議：
    1. Name是任意設定的，不會影響配置。
    2. 對於BaseDN和BindDN，請從Active Directory(AD)配置複製並貼上相應的值。
    3. Group Attribute的預設值為member。

    > 附註：在其他UCS管理工具（如UCSM或CIMC）中，組屬性設定為memberOf。在Intersight中，建議將其保留為成員。

    4. 輸入此LDAP提供程式的密碼。
    5. 如果您希望在AD中允許對來自根的所有組及其包含的組進行遞迴搜尋，請啟用巢狀組搜尋。
    6. 對常規LDAP配置禁用啟用加密。如果需要安全LDAP，請啟用它，並確保檢視LDAPS（安全LDAP）的配置部分，瞭解需要配置的補充步驟。
4. 新增一個LDAP伺服器的配置：
    1. 在Server中，介紹LDAP伺服器的IP或主機名。

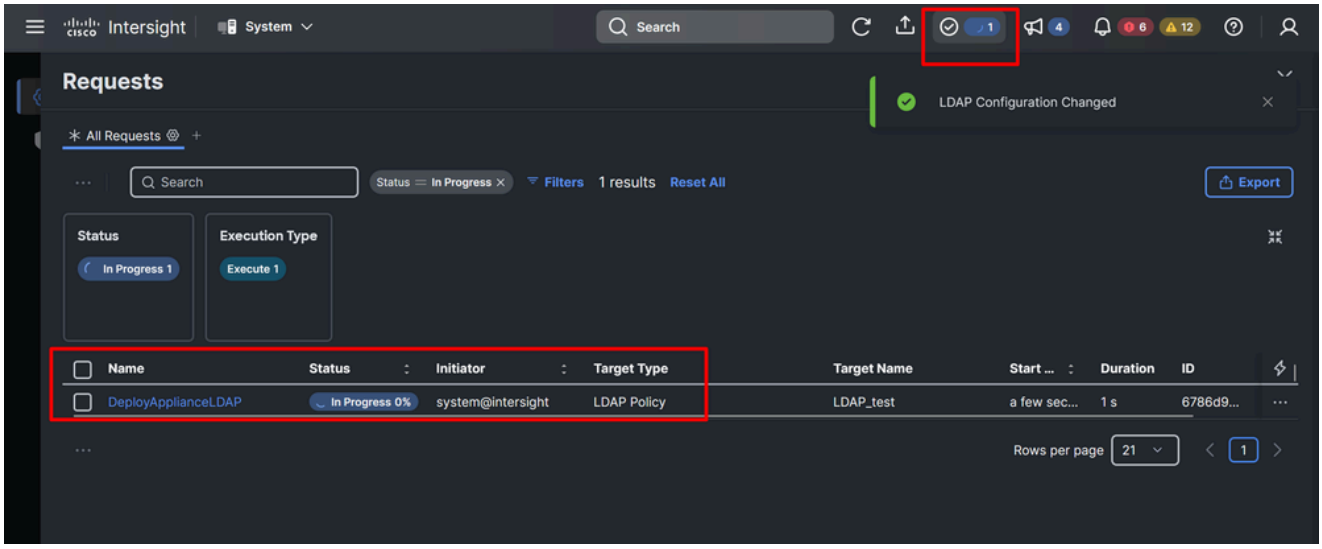
    > 注意：如果使用主機名，請確保DNS能夠正確對映該主機名。

    2. LDAP的預設埠和推薦埠為389。
5. 按一下「Save」。



基本LDAP設定的配置示例

6. 從頂欄中的Requests監控工作流DeployApplianceLDAP。



部署請求

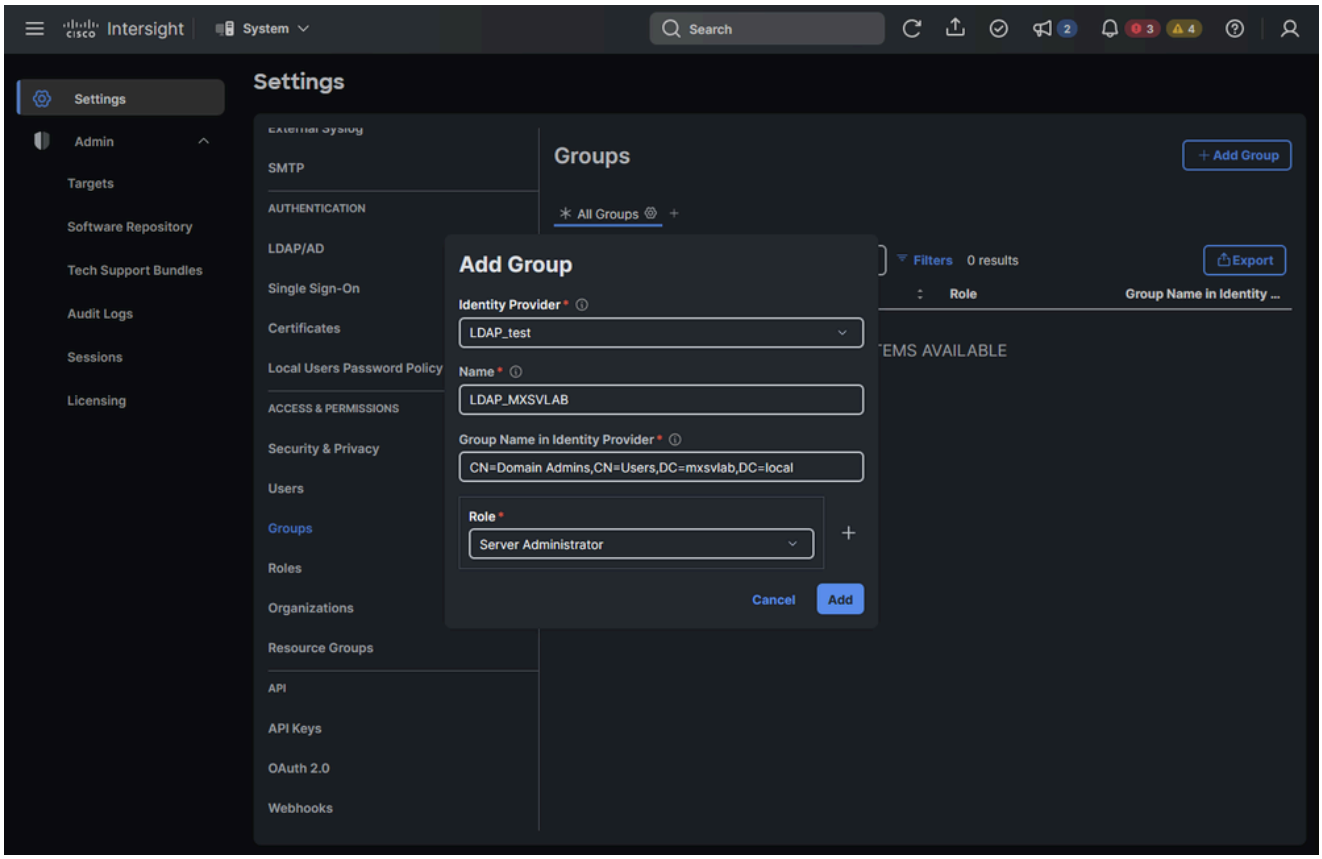
配置使用者和組

工作流程DeployApplianceLDAP完成後，您可以配置Groups或單個Users。

如果您決定使用組，授權將提供給屬於該組的所有使用者。如果您使用單個使用者，則需要新增每個具有其自己的授權角色的使用者。

配置組

1. 導航到System > Settings > ACCESS & PERMISSION > Groups.
2. 按一下Add Group。
3. 選擇身份提供程式。它是您在配置LDAP基本設定一節中設定的名稱。
4. 設定組的名稱。
5. 在身份提供程序中輸入組名稱的值。它需要與LDAP伺服器中組的配置相匹配。
6. 根據要向此組中的使用者提供訪問許可權的級別選擇角色。請參閱Intersight中的角色和許可權。



組的配置示例

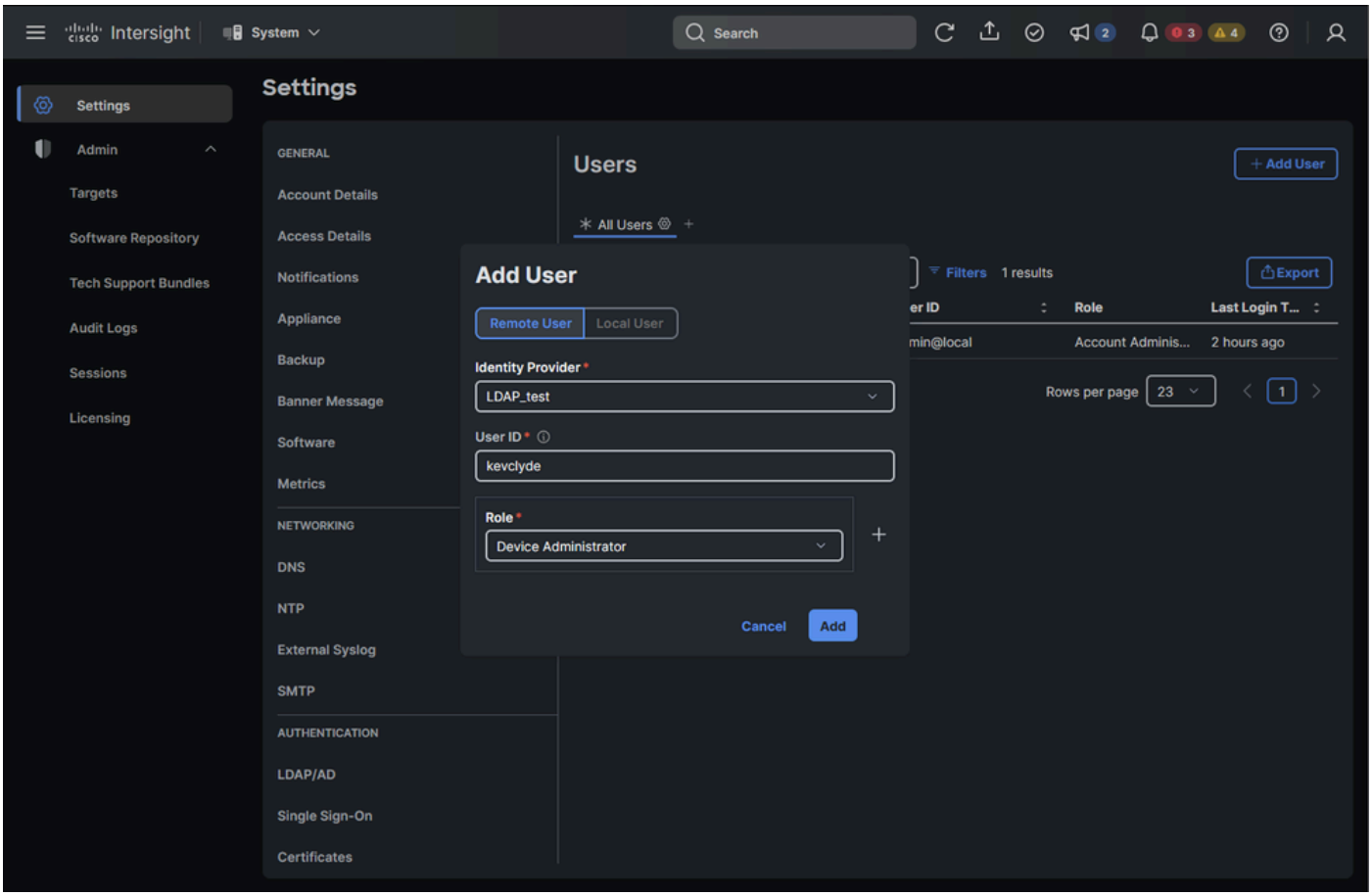
配置使用者

如果您希望配置單個使用者而不是組，請遵循以下說明：

1. 導航至System > Settings > ACCESS & PERMISSION > Users。
2. 按一下「Add User」。
3. 選擇Remote User。
4. 選擇身份提供程式。它是您在配置LDAP基本設定一節中設定的名稱。
5. 設定用戶ID。

提示：要將使用者名稱用作登入方法，請在使用者ID欄位中複製在LDAP伺服器中配置為sAMAccountName的值。
如果要使用電子郵件，請確保在LDAP伺服器的mail屬性中設定使用者的電子郵件。

6. 根據要提供給使用者的訪問級別選擇角色。請參閱Intersight中的角色和許可權。

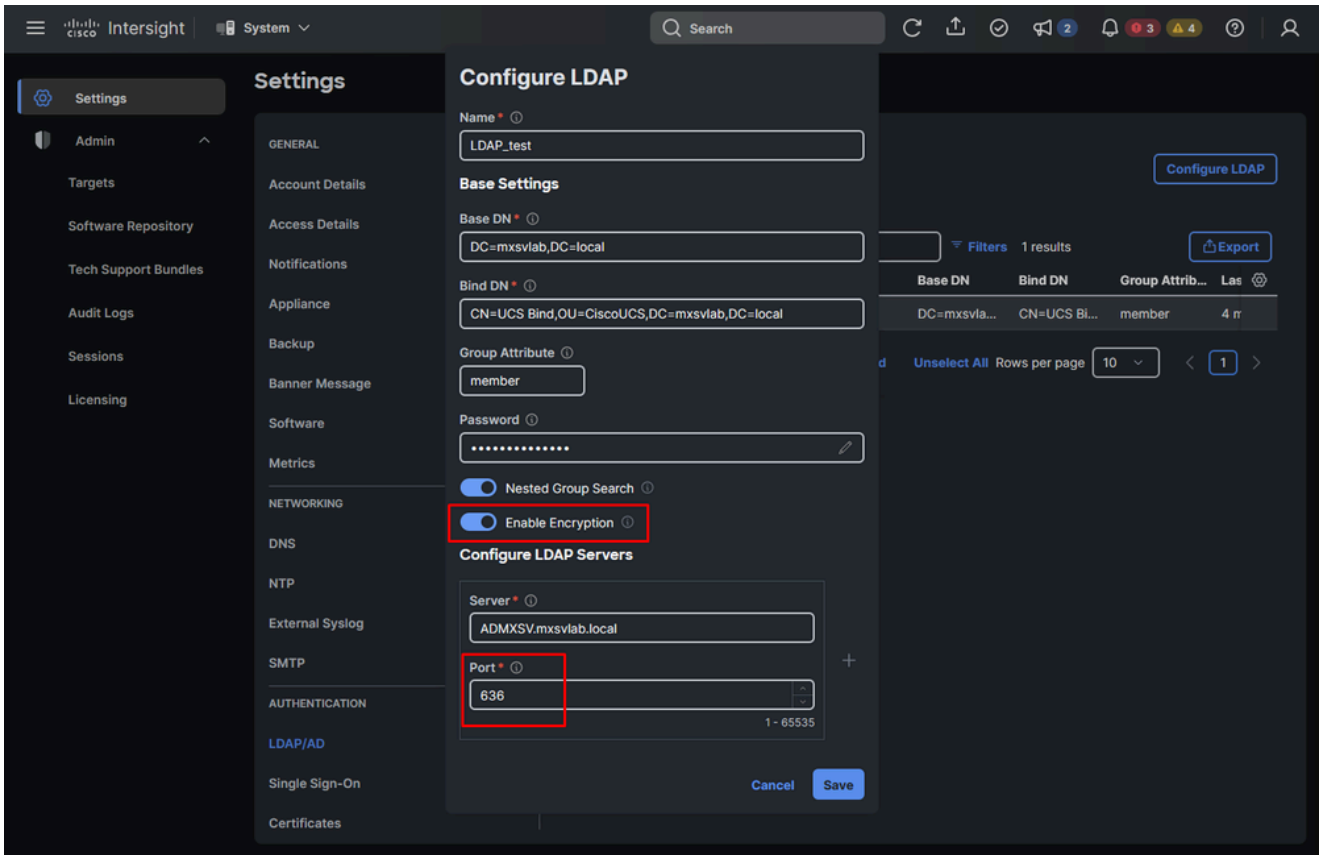


使用者的配置示例

LDAPS（安全LDAP）的配置

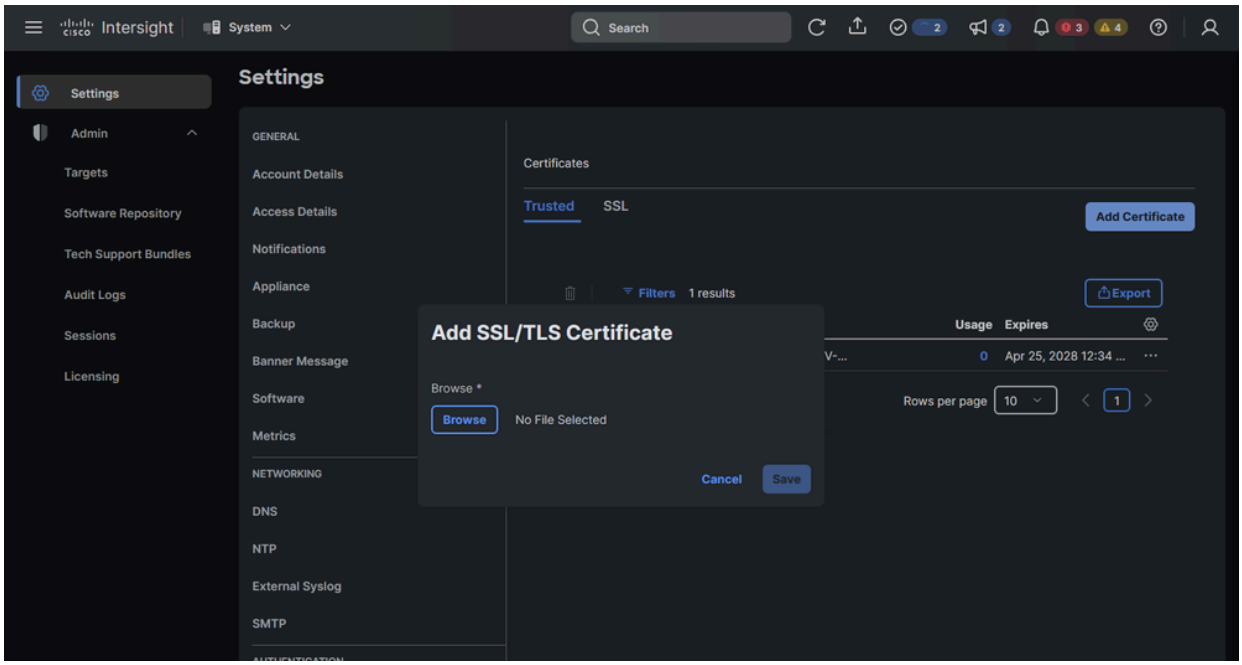
如果您希望通過加密保護您的LDAP通訊，則需要您的CA簽署一個證書。確保將這些更改應用到配置：

1. 完成LDAP基本設定配置中的步驟，但確保將滑塊Enable Encryption移動到右側（步驟3.g）。
2. 確保使用的埠是636或3269，它們是支援LDAPS的埠（安全）。 所有其他埠都支援使用TLS的LDAP。



安全LDAP的配置更改

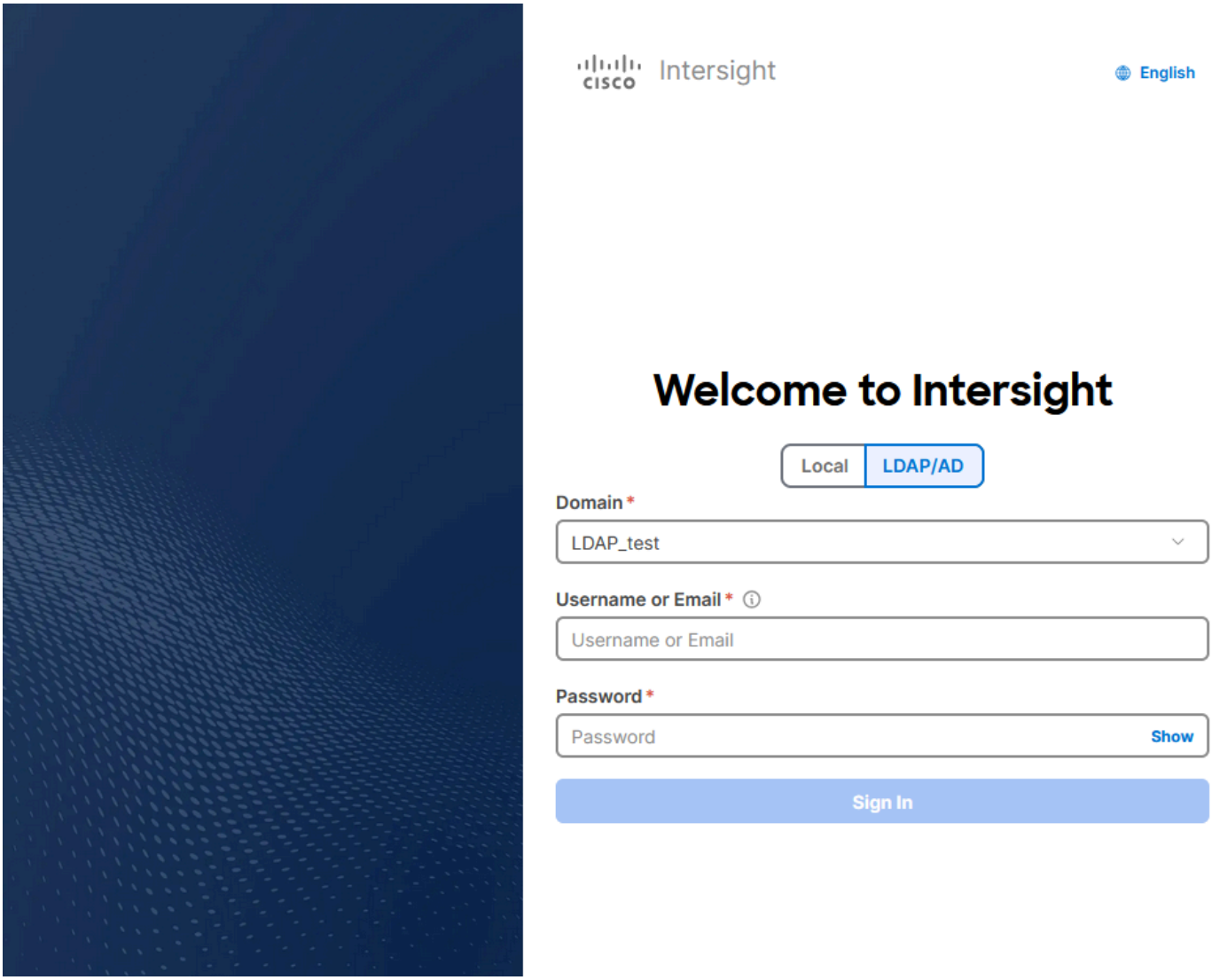
3. 儲存配置並等待工作流DeployApplianceLDAP完成。
4. 使用以下步驟新增證書：
    1. 導覽至System > Settings > AUTHENTICATION > Certificates > Trusted。
    2. 按一下「新增憑證」。
    3. 按一下Browse，然後選擇.pem檔案，其中包含由CA頒發的憑證。



新增證書的配置

驗證

在瀏覽器中，導航到Intersight虛擬裝置URL。螢幕現在顯示一個使用LDAP憑據登入的選項：

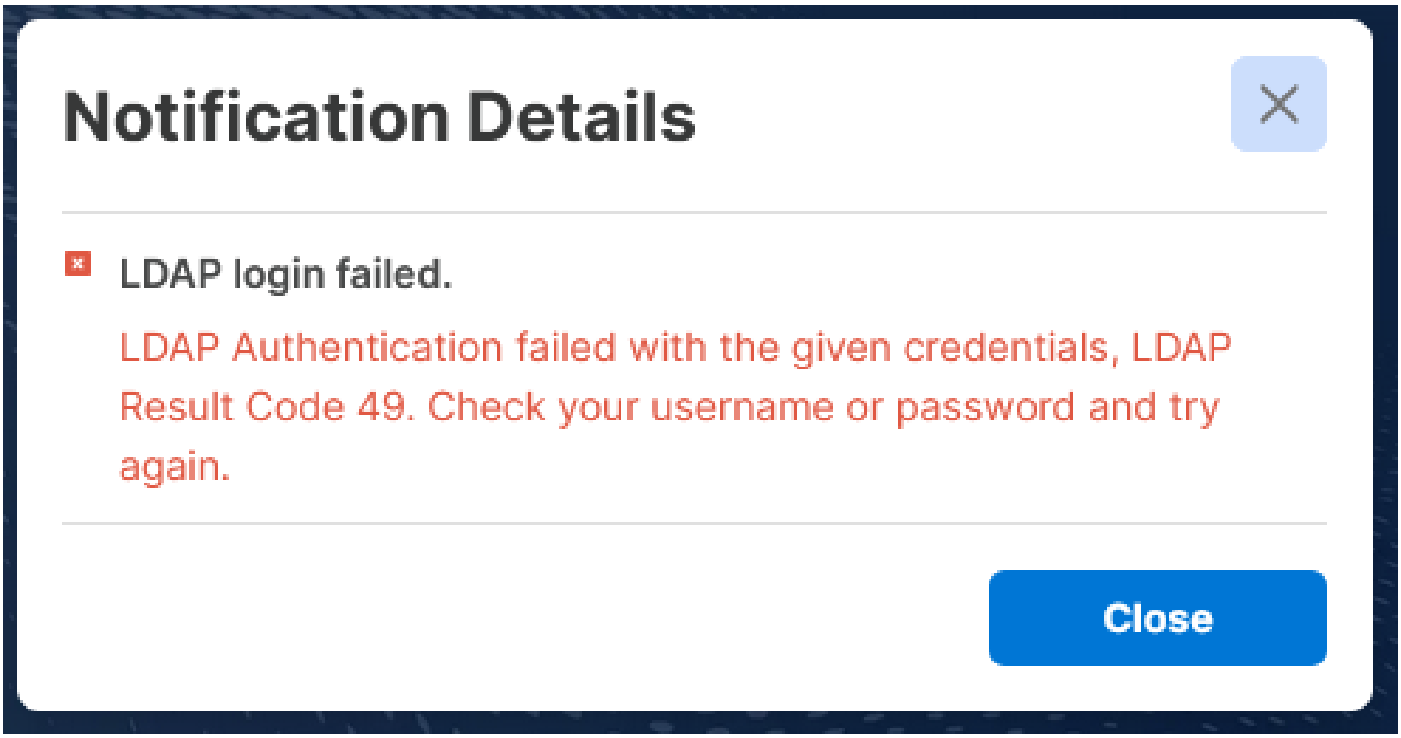


從登入螢幕啟用LDAP配置

疑難排解

如果登入失敗，則錯誤消息會提供有關可能錯誤的提示。

錯誤1.訪問詳細資訊錯誤

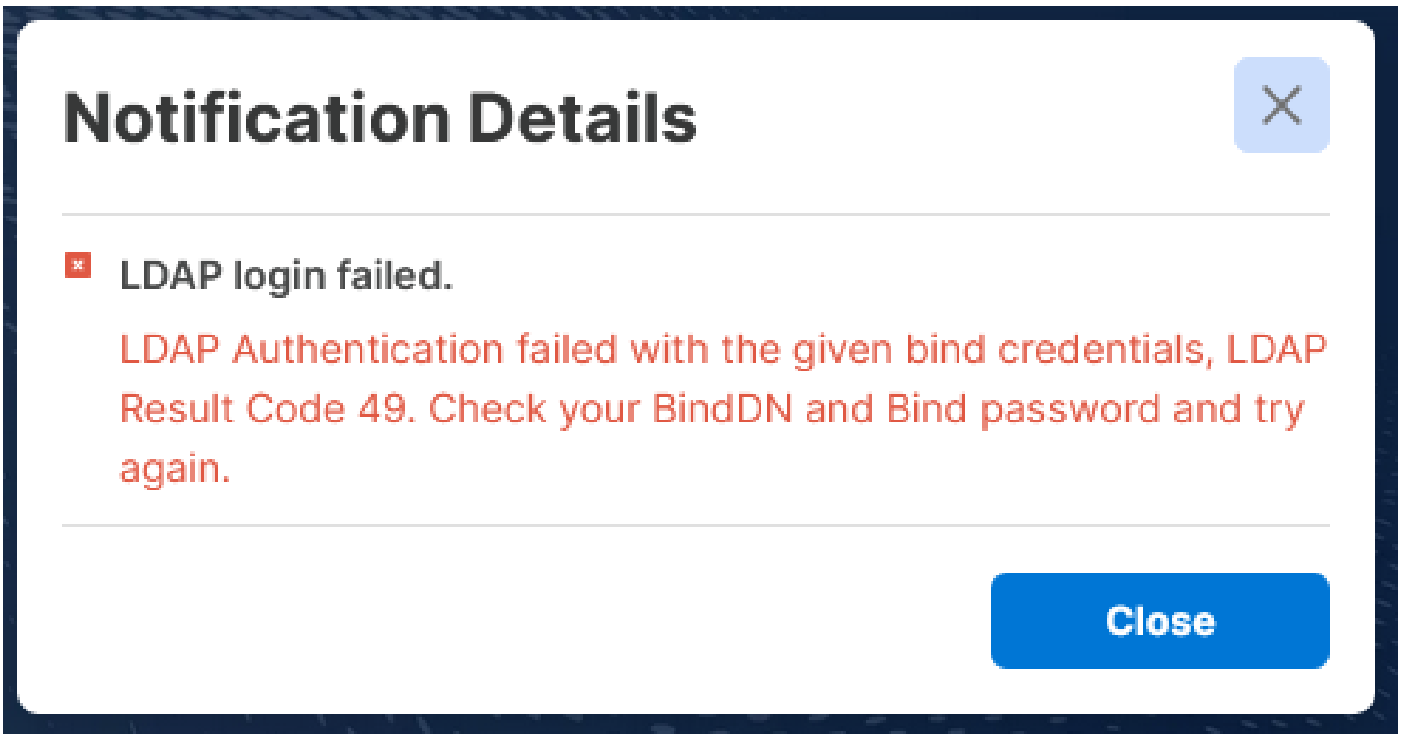


錯誤密碼錯誤錯誤消息

此錯誤表示存取資料不正確。

1. 驗證使用者名稱和密碼是否正確。

錯誤2.錯誤的繫結資料

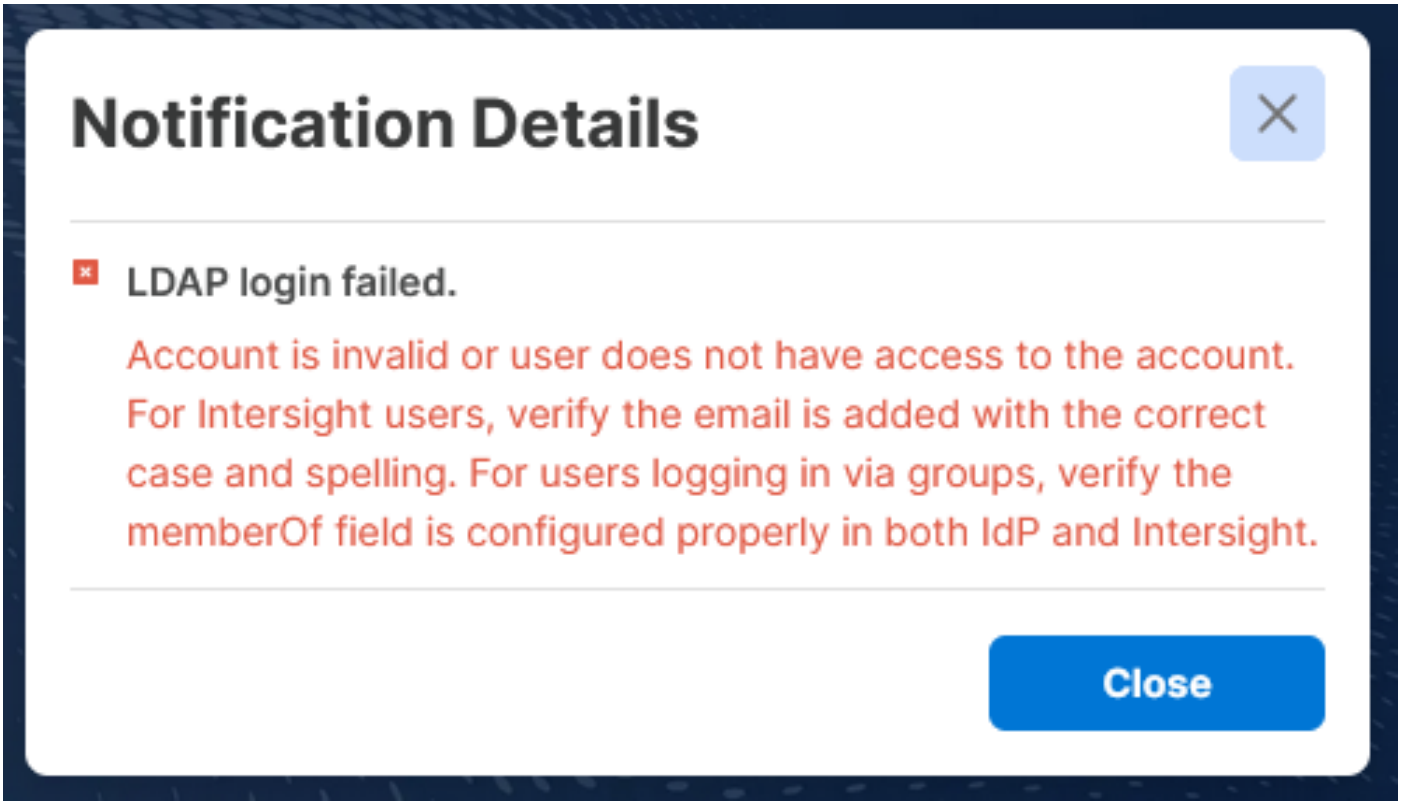


錯誤繫結資料的錯誤消息

此錯誤表示繫結資料不正確。

1. 驗證BindDN。
2. 驗證在LDAP設定中配置的繫結密碼。

錯誤3.無法找到使用者

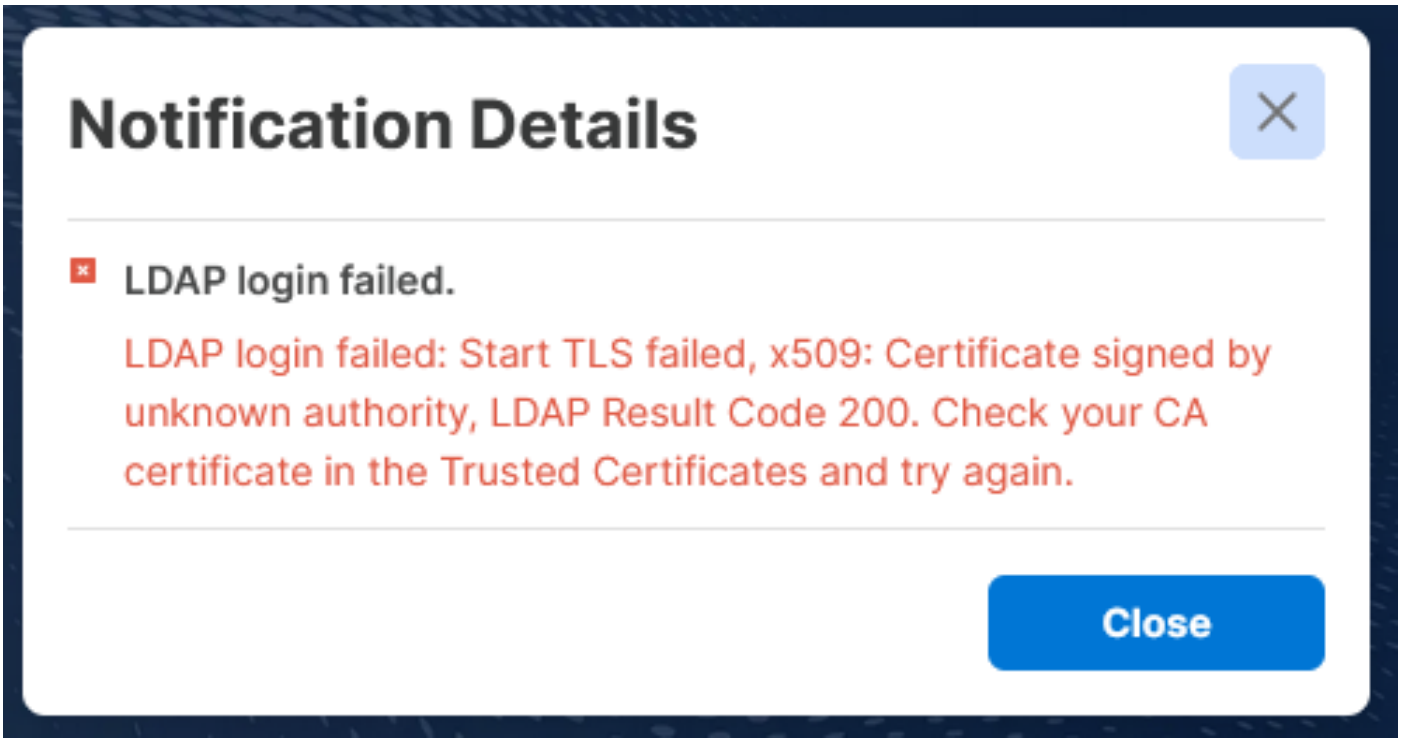


找不到使用者的錯誤消息

當LDAP伺服器中的搜尋未返回任何授權使用者時，會觸發此功能。驗證下一個設定是否正確：

1. 檢查BaseDN。用於查詢使用者的引數錯誤。
2. 確保將Group Attribute設定為member而不是memberOf。
3. 驗證Groups配置中Identity Provider中的Group Name是否正確。僅當通過組提供授權時才適用。
4. 驗證使用者的AD配置中的mail欄位是否正確設定了使用者的電子郵件。這僅適用於向單個使用者提供授權的情況。

錯誤4.證書錯誤

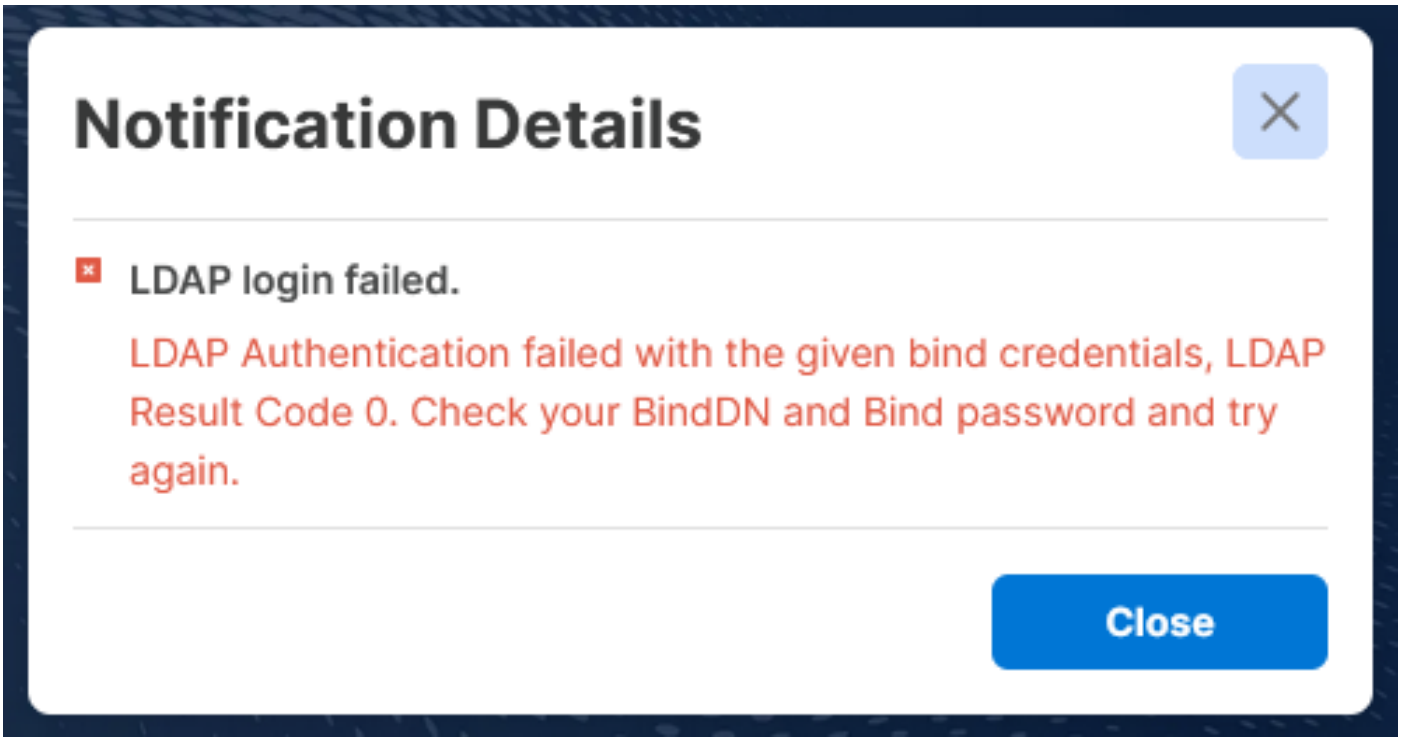


錯誤證書的錯誤消息

如果啟用加密的LDAP:

1. 驗證是否已配置證書並且其中包含正確的完整證書。

錯誤5.將啟用加密與安全埠一起使用

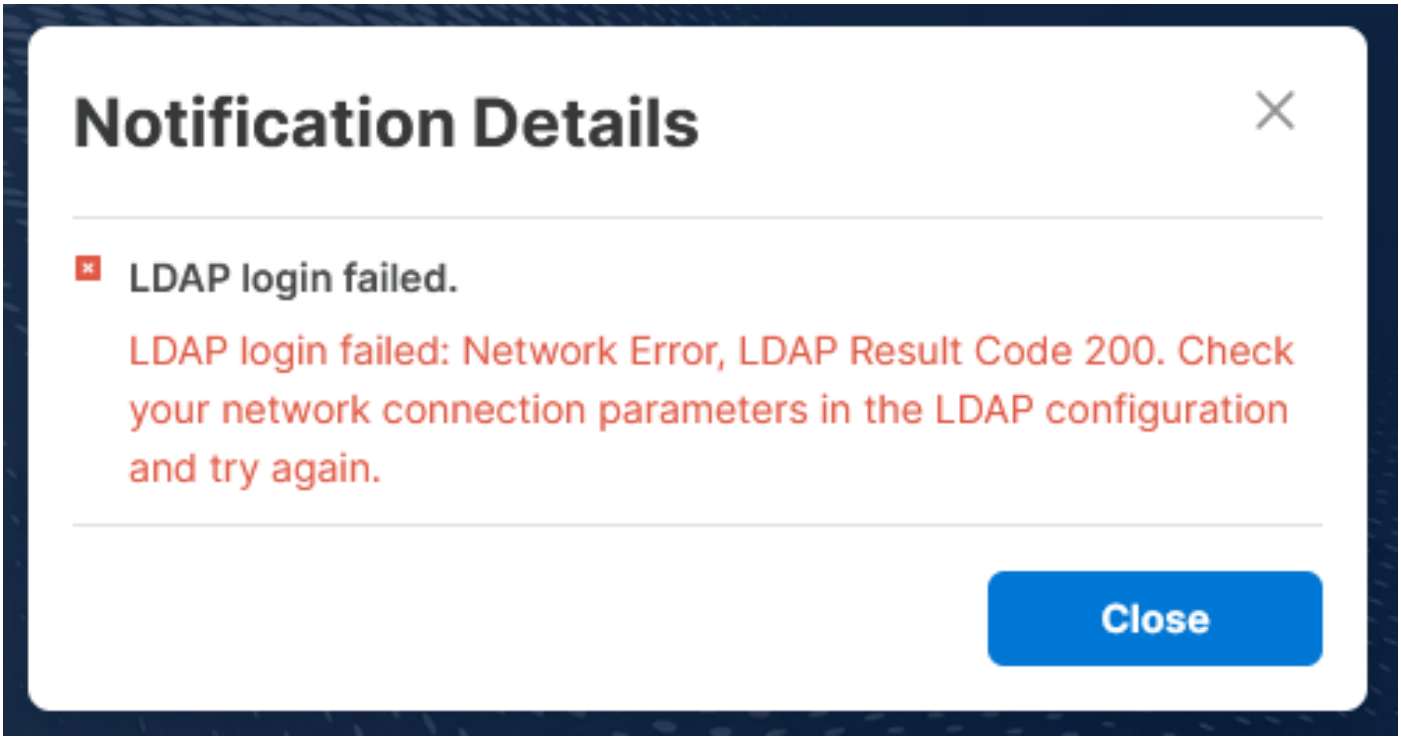


禁用啟用加密的錯誤消息

如果未啟用啟用加密，但配置了安全LDAP的埠，則會出現此錯誤。

1. 如果沒有啟用加密，請確保使用埠389。

錯誤6.連線引數錯誤



錯誤埠錯誤消息

此錯誤表示無法成功建立與LDAP伺服器的連線。請驗證：

1. DNS伺服器必須將LDAP伺服器的主機名解析為正確的IP。
2. Intersight裝置能夠訪問LDAP伺服器。
3. 確保埠389用於未加密的LDAP，636或3269用於安全LDAP(LDAPS)，任何其他埠用於TLS（啟用加密並設定證書）。

相關資訊

- 將Cisco Intersight虛擬裝置與LDAP整合（影片）
- 在Intersight裝置中配置LDAP設定
- Intersight中的角色和許可權
- UCSM中的LDAP配置示例

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。