Konfigurieren von LDAP in der virtuellen Intersight-Appliance

Inhalt

Einleitung

In diesem Dokument wird der Prozess zur Konfiguration der LDAP-Authentifizierung in einer Intersight Private Virtual Appliance (PVA) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

Verwendete Komponenten

- Intersight Private Virtual Appliance
- Microsoft Active Directory
- DNS-Server

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

LDAP ist ein Protokoll, das verwendet wird, um über das Netzwerk von einem Verzeichnis auf Ressourcen zuzugreifen. Diese Verzeichnisse speichern Informationen über Benutzer, Organisationen und Ressourcen. LDAP bietet eine Standardmethode für den Zugriff auf und die Verwaltung dieser Informationen, die für Authentifizierungs- und Autorisierungsprozesse verwendet werden können.

Dieses Dokument zeigt den Konfigurationsprozess zum Hinzufügen einer Remote-Authentifizierung über LDAP zu einem Intersight PVA.

Konfigurieren

Konfiguration der LDAP-Grundeinstellungen

1. Navigieren Sie zu System > Settings > AUTHENTICATION > LDAP/AD.
2. Klicken Sie auf LDAP konfigurieren.
3. Geben Sie die erforderlichen Informationen ein. Empfehlungen:
    1. Der Name ist willkürlich festgelegt und hat keine Auswirkungen auf die Konfiguration.
    2. Kopieren Sie für BaseDN und BindDN die entsprechenden Werte aus der Active Directory (AD)-Konfiguration, und fügen Sie sie ein.
    3. Der Standardwert für Gruppenattribut ist member.

    > Anmerkung: In anderen UCS-Managementtools wie UCSM oder CIMC ist das Gruppenattribut auf memberOf festgelegt. In Intersight wird empfohlen, es als Mitglied zu belassen.

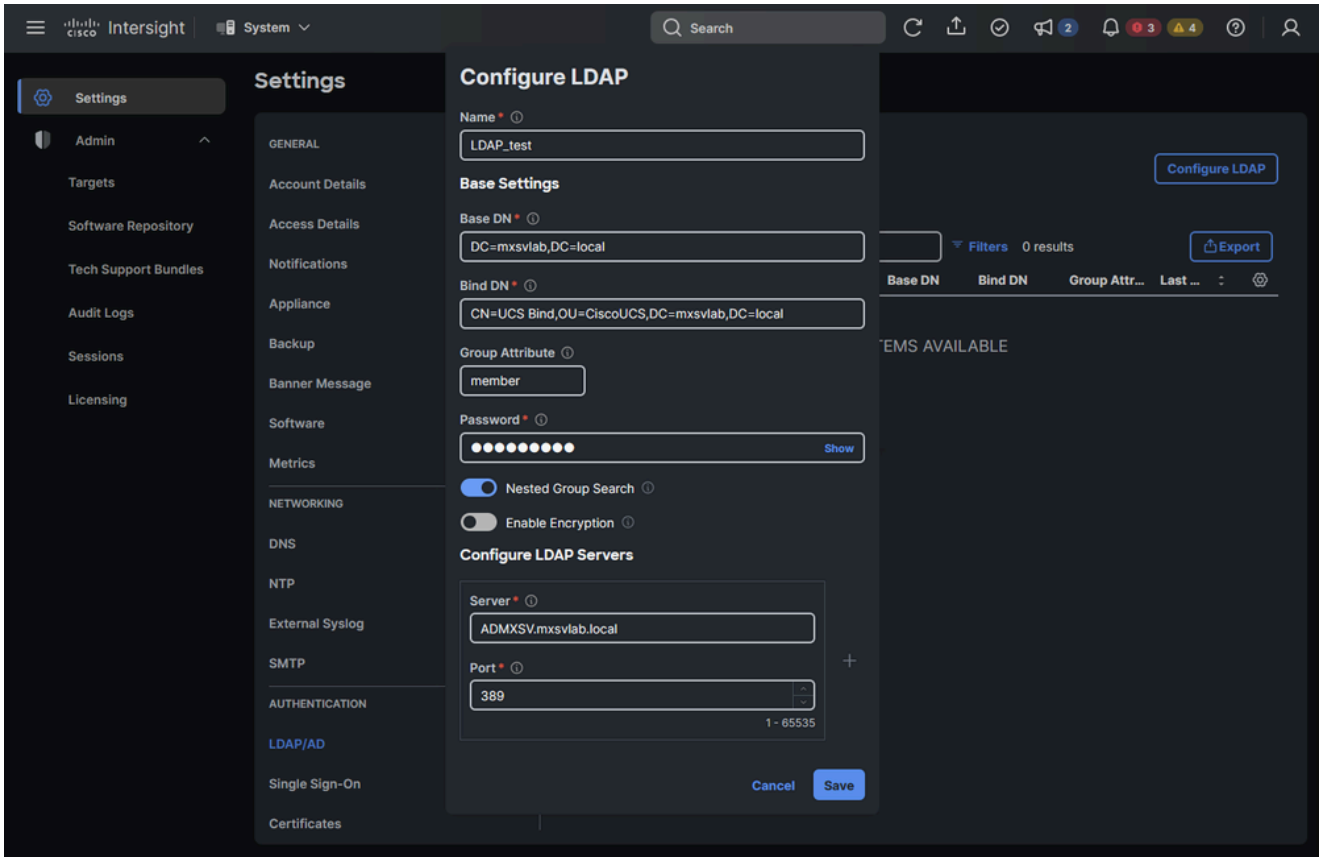
    4. Geben Sie das Kennwort für diesen LDAP-Anbieter ein.
    5. Aktivieren Sie die Option Geschachtelte Gruppensuche, wenn Sie eine rekursive Suche in Ihrem AD für alle Gruppen aus dem Stammverzeichnis und den enthaltenen Gruppen zulassen möchten.
    6. Lassen Sie Encryption für eine reguläre LDAP-Konfiguration deaktiviert. Wenn

sicheres LDAP benötigt wird, aktivieren Sie es, und überprüfen Sie den Abschnitt Konfiguration von LDAPS (sicheres LDAP) für die zusätzlichen Schritte, die Sie konfigurieren müssen.

4. Fügen Sie die Konfiguration für einen LDAP-Server hinzu:
    1. Geben Sie in Server die IP-Adresse oder den Hostnamen des LDAP-Servers ein.

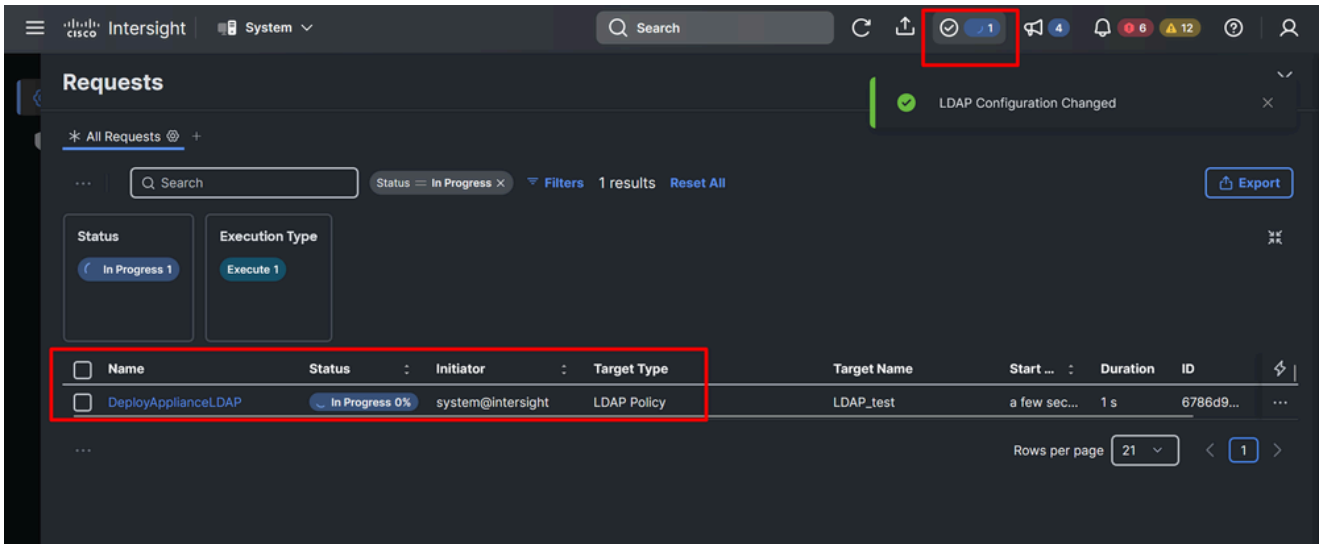
    ⚠ Vorsicht: Wenn ein Hostname verwendet wird, stellen Sie sicher, dass der DNS diesen Hostnamen korrekt zuordnen kann.

    2. Der empfohlene Standardport für LDAP ist 389 .
5. Klicken Sie auf Speichern.



Konfigurationsbeispiel für grundlegende LDAP-Einstellungen

6. Überwachen Sie den Workflow DeployApplianceLDAP über die Anforderungen in der oberen Leiste.



Bereitstellungsanforderung

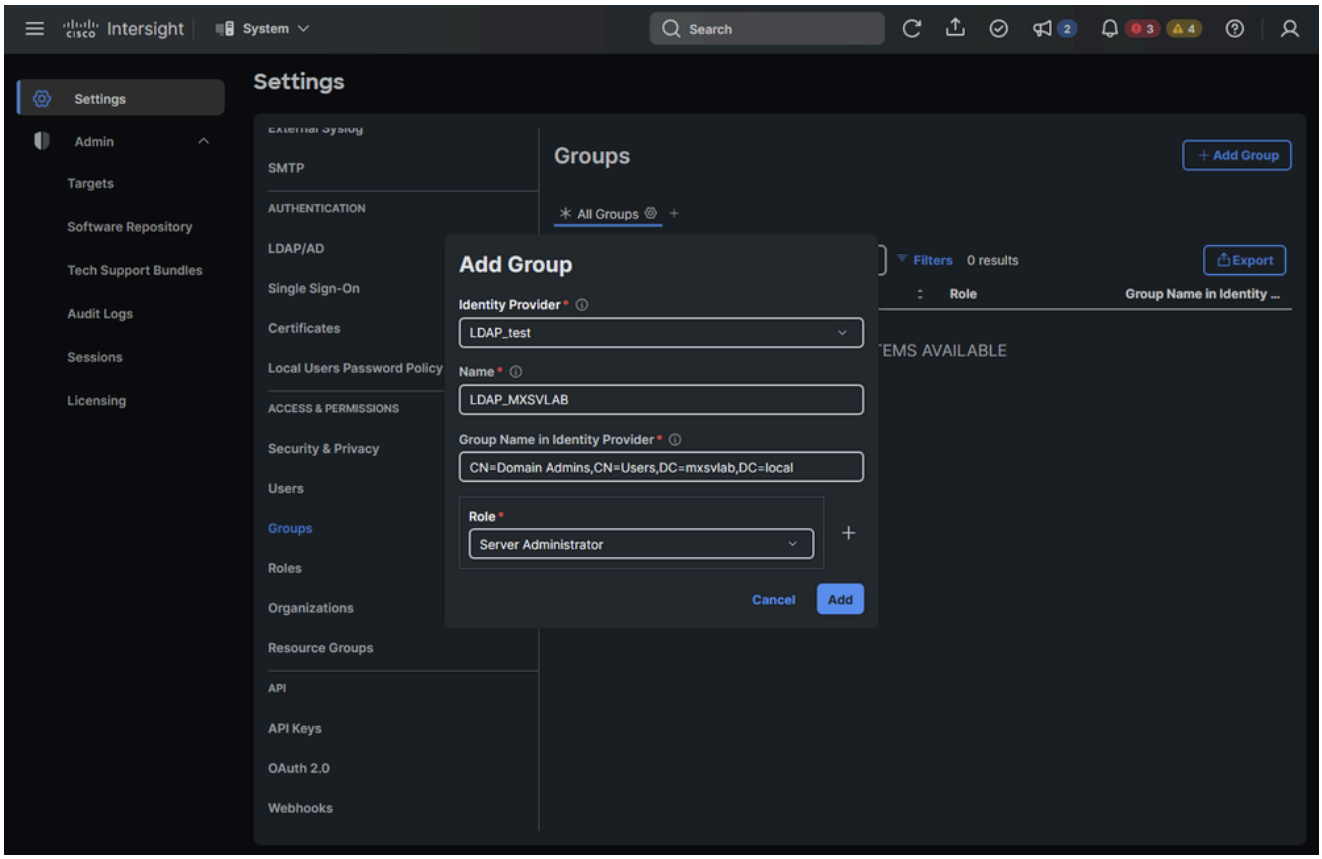
Konfigurieren von Benutzern und Gruppen

Nach Abschluss des Workflows DeployApplianceLDAP können Sie entweder Gruppen oder einzelne Benutzer konfigurieren.

Wenn Sie sich für die Verwendung von Gruppen entscheiden, wird die Autorisierung allen Benutzern bereitgestellt, die dieser Gruppe angehören. Wenn Sie einzelne Benutzer verwenden, müssen Sie jedem Benutzer eine eigene Autorisierungsrolle hinzufügen.

Gruppen konfigurieren

1. Navigieren Sie zu System > Settings > ACCESS & PERMISSION > Groups (System > Einstellungen > ZUGRIFF & BERECHTIGUNG > Gruppen)..
2. Klicken Sie auf Gruppe hinzufügen.
3. Wählen Sie den Identitätsanbieter aus. Dies ist der Name, den Sie im Abschnitt Grundeinstellungen für LDAP konfigurieren festgelegt haben.
4. Legen Sie einen Namen für die Gruppe fest.
5. Geben Sie den Wert für Gruppenname im Identitätsanbieter ein. Sie muss mit den Konfigurationen der Gruppe in Ihrem LDAP-Server übereinstimmen.
6. Wählen Sie die Rolle abhängig von der Zugriffsebene aus, die Sie den Benutzern in dieser Gruppe bereitstellen möchten. Siehe Rollen und Berechtigungen in Intersight.



Konfigurationsbeispiel für eine Gruppe

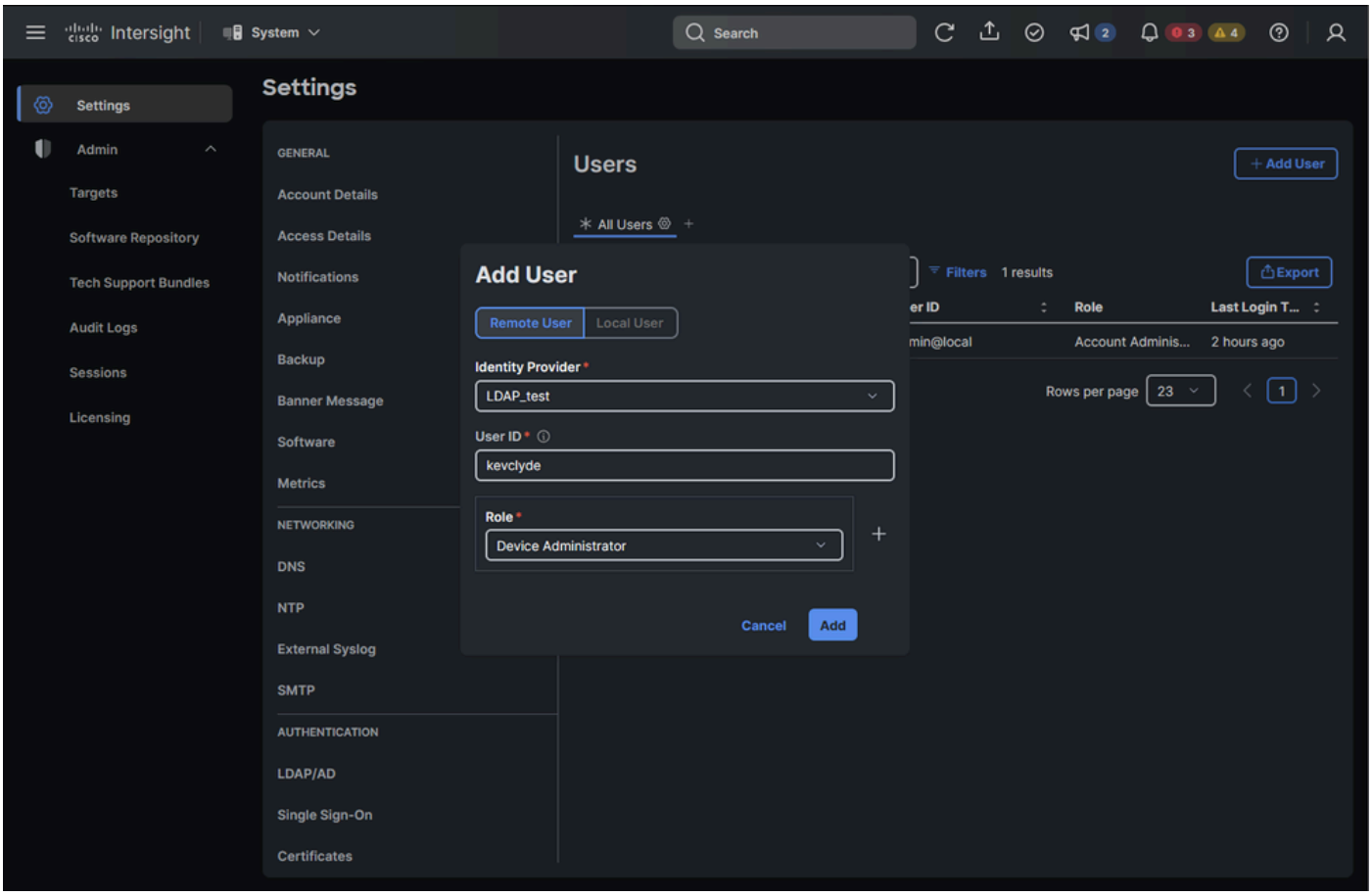
Benutzer konfigurieren

Wenn Sie einzelne Benutzer anstelle von Gruppen konfigurieren möchten, befolgen Sie die folgenden Anweisungen:

1. Navigieren Sie zu System > Settings > ACCESS & PERMISSION > Users.
2. Klicken Sie auf Benutzer hinzufügen.
3. Wählen Sie Remote User aus.
4. Wählen Sie den Identitätsanbieter aus. Dies ist der Name, den Sie im Abschnitt Grundeinstellungen für LDAP konfigurieren festgelegt haben.
5. Richten Sie eine Benutzer-ID ein.

> Tipp: Um den Benutzernamen als Anmeldemethode zu verwenden, kopieren Sie im Feld Benutzer-ID den Wert, der im LDAP-Server als sAMAccountName konfiguriert wurde.
> Wenn Sie die E-Mail verwenden möchten, stellen Sie sicher, dass Sie die E-Mail des Benutzers im Mail-Attribut im LDAP-Server festlegen.

6. Wählen Sie die Rolle je nach der Zugriffsebene aus, die Sie dem Benutzer bereitstellen möchten. Siehe Rollen und Berechtigungen in Intersight.

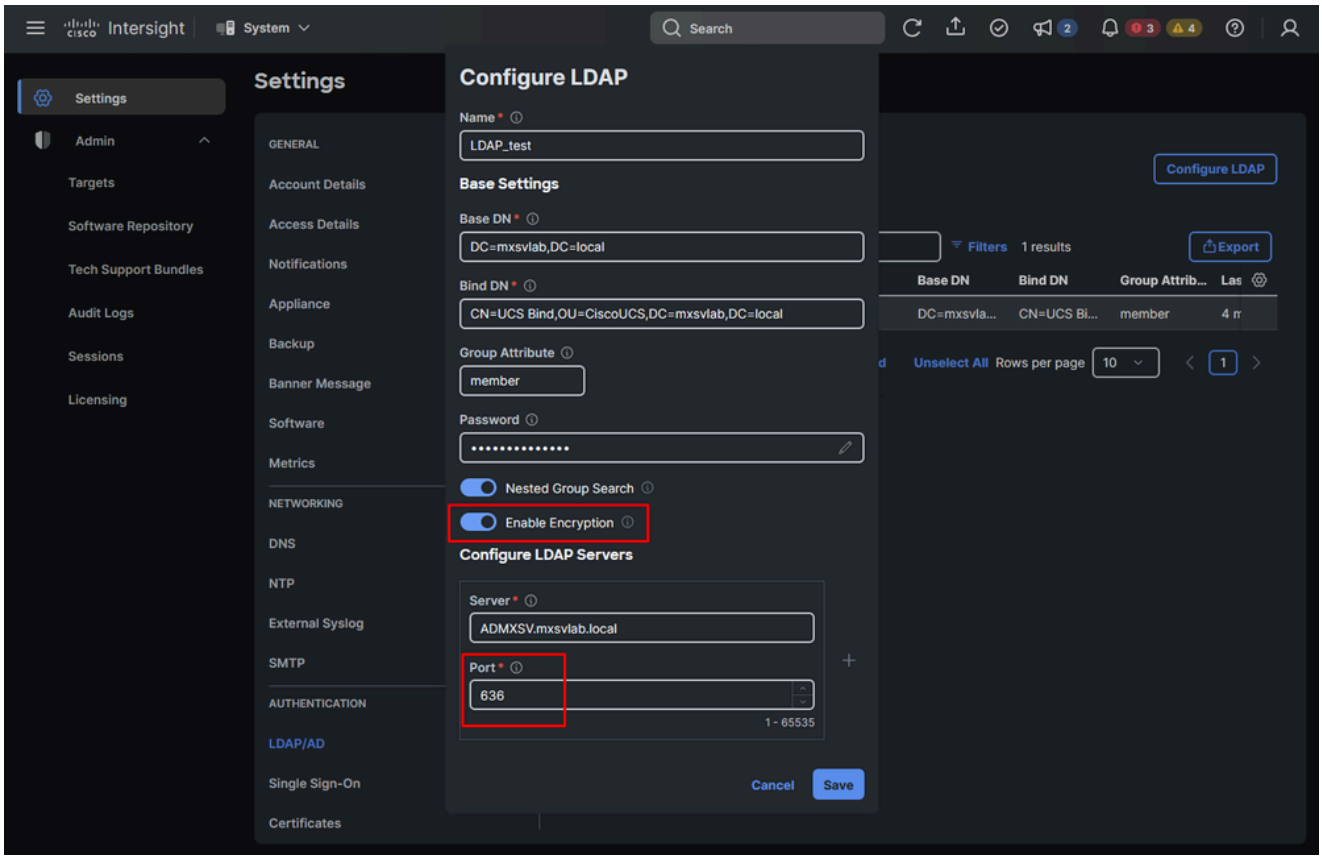


Konfigurationsbeispiel für einen Benutzer

Konfiguration von LDAPS (Secure LDAP)

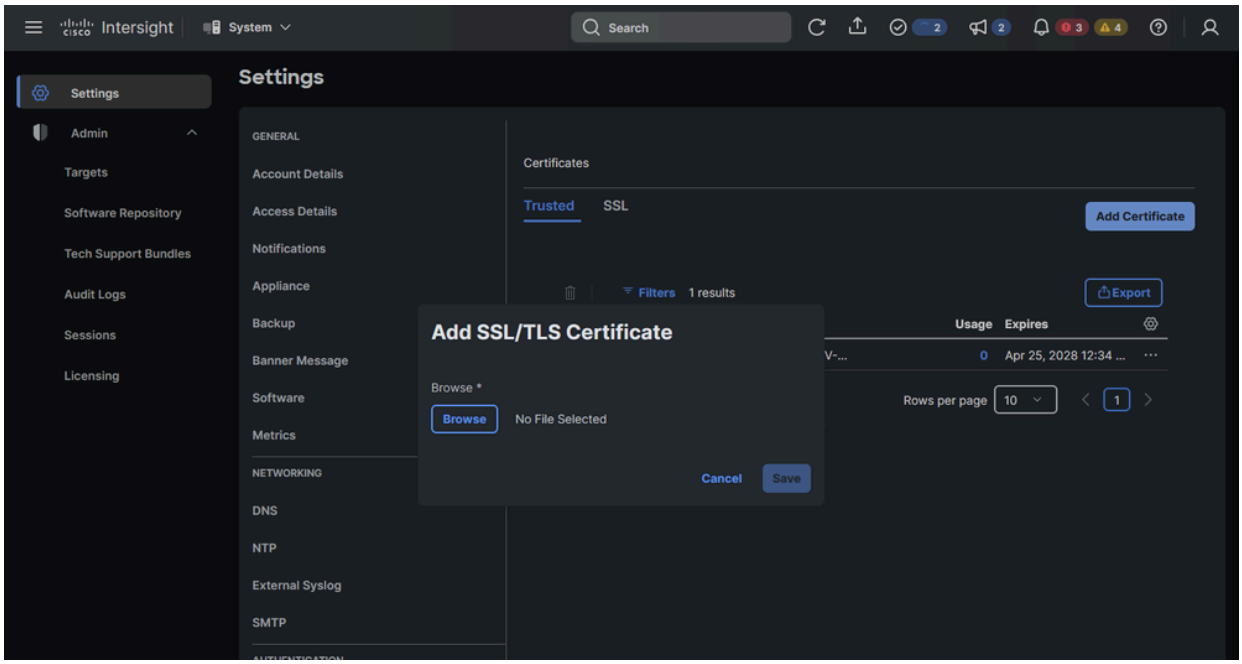
Wenn Sie Ihre LDAP-Kommunikation verschlüsselt sichern möchten, benötigen Sie ein von Ihrer Zertifizierungsstelle signiertes Zertifikat. Stellen Sie sicher, dass Sie die folgenden Änderungen auf die Konfiguration anwenden:

1. Führen Sie die Schritte aus Konfiguration der LDAP-Grundeinstellungen aus, aber stellen Sie sicher, dass Sie den Schieberegler Verschlüsselung aktivieren nach rechts verschieben (Schritt 3.g).
2. Stellen Sie sicher, dass Sie den Port 636 oder 3269 verwenden, d. h. die Ports, die LDAPS unterstützen (sicher). Alle anderen Ports unterstützen LDAP über TLS.



Konfigurationsänderungen für sicheres LDAP

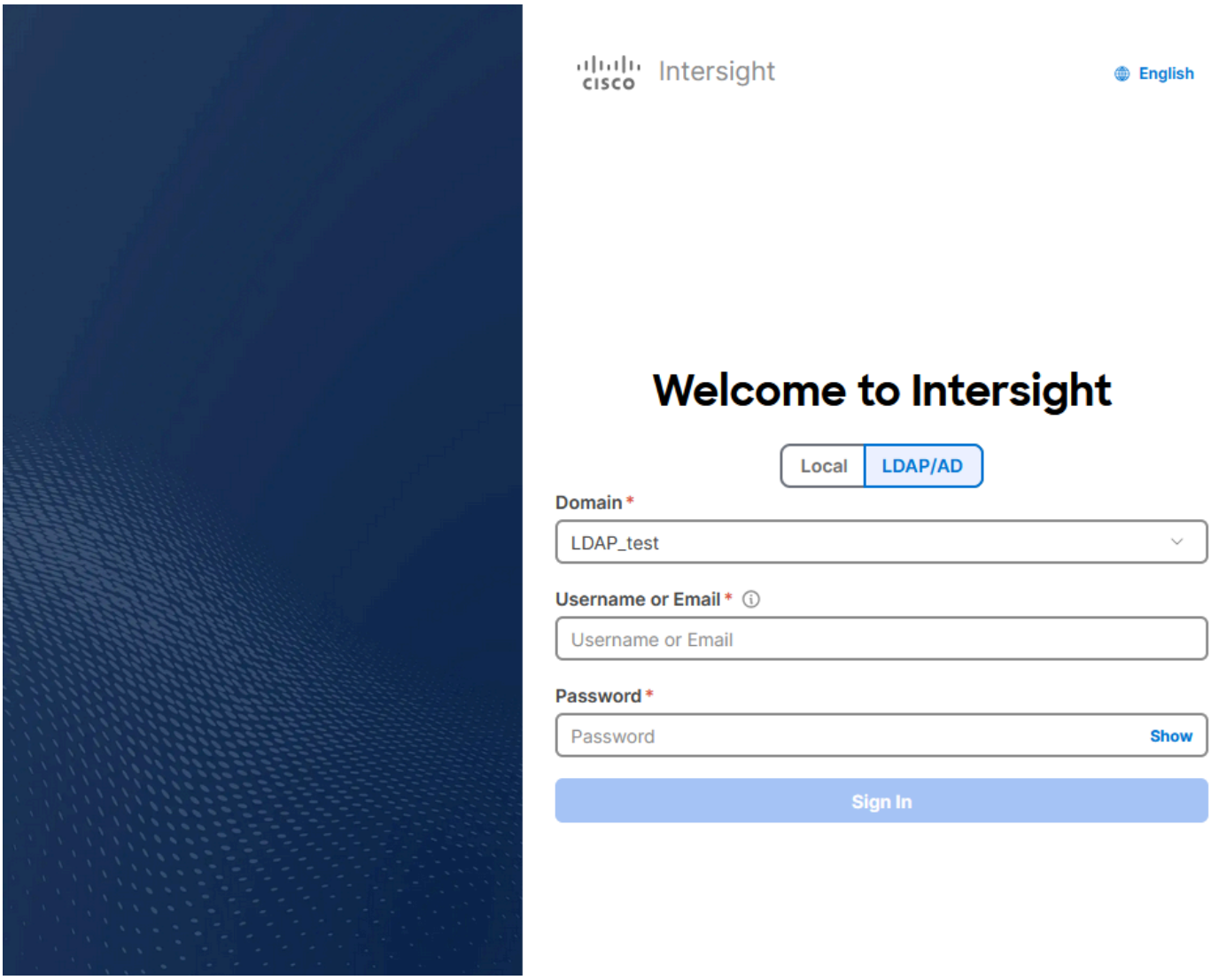
3. Speichern Sie die Konfiguration, und warten Sie, bis der Workflow DeployApplianceLDAP abgeschlossen ist.
4. Fügen Sie ein Zertifikat mit den folgenden Schritten hinzu:
    1. Navigieren Sie zu System > Settings > AUTHENTICATION > Zertifikate > Vertrauenswürdig.
    2. Klicken Sie auf Zertifikat hinzufügen.
    3. Klicken Sie auf Durchsuchen, und wählen Sie eine .pem-Datei aus, die das von Ihrer Zertifizierungsstelle ausgestellte Zertifikat enthält.



Konfiguration zum Hinzufügen eines Zertifikats

Überprüfung

Navigieren Sie in Ihrem Browser zu Ihrer URL für die Intersight Virtual Appliance. Der Bildschirm zeigt nun eine Option zur Anmeldung mit LDAP-Anmeldeinformationen an:

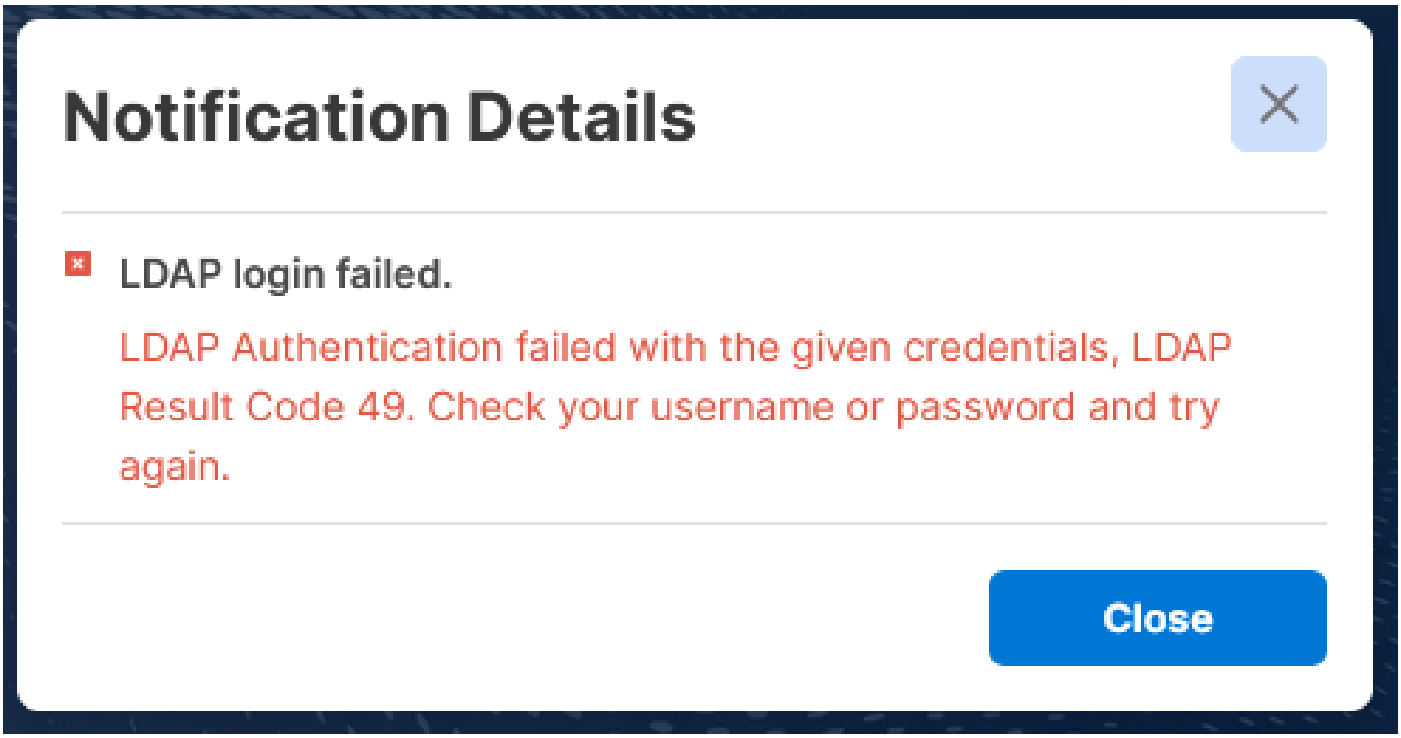


LDAP-Konfiguration im Anmeldebildschirm aktiviert

Fehlerbehebung

Wenn die Anmeldung fehlschlägt, enthalten die Fehlermeldungen Hinweise darauf, was falsch sein könnte.

Fehler 1. Falsche Zugriffsdetails

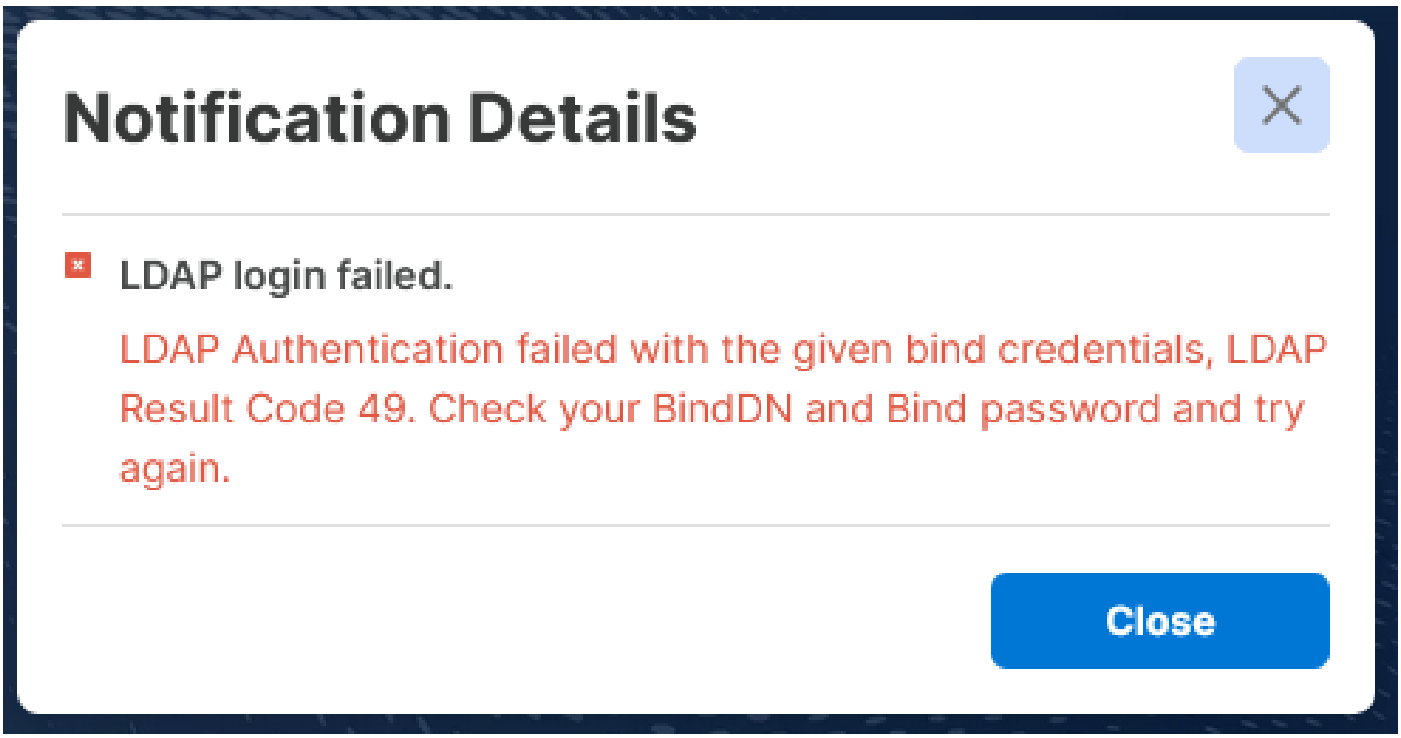


Fehlermeldung für Fehler bei falschem Kennwort

Dieser Fehler bedeutet, dass die Zugriffsdaten falsch sind.

1. Vergewissern Sie sich, dass Benutzername und Kennwort korrekt sind.

Fehler 2. Falsche Bindungsdaten

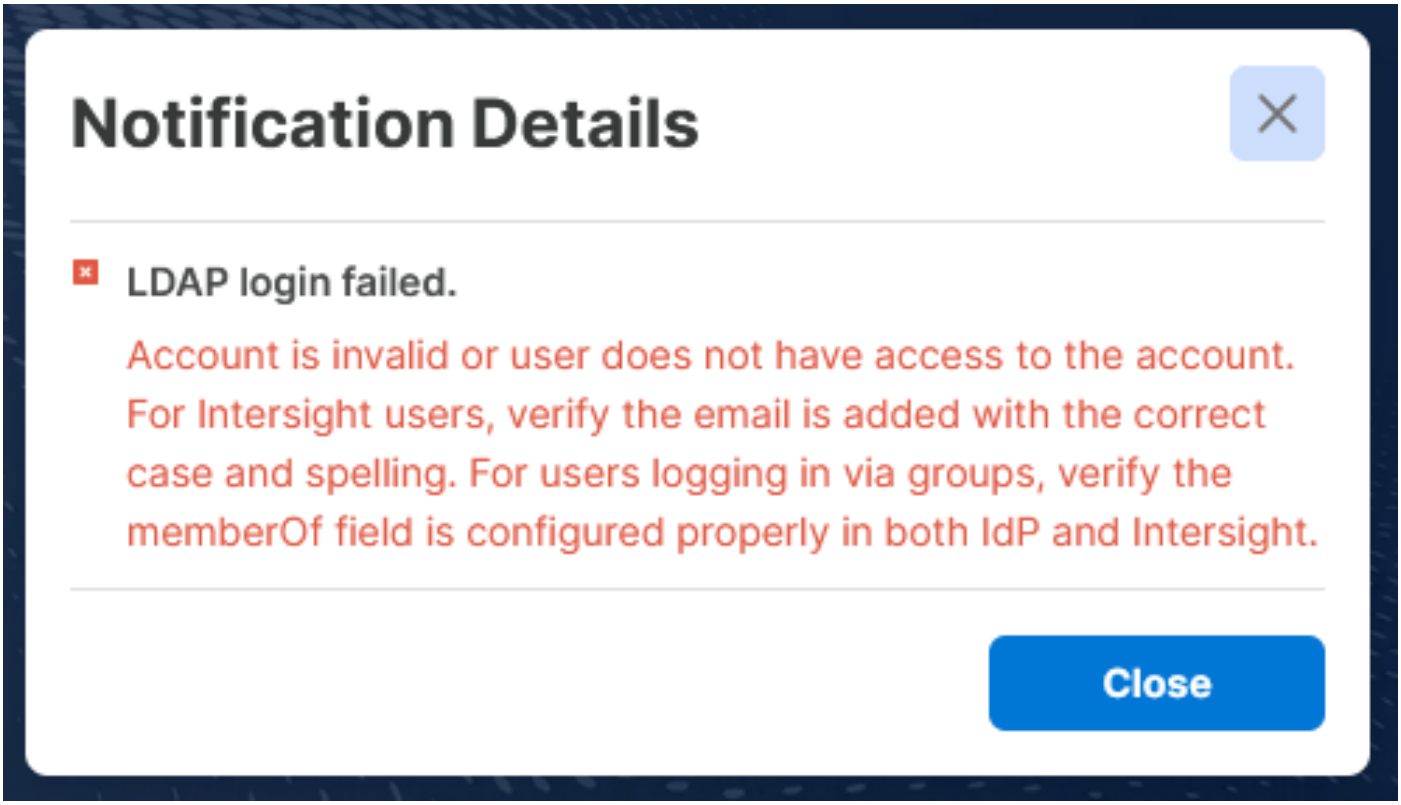


Fehlermeldung für falsche Bindungsdaten

Dieser Fehler bedeutet, dass die Bindungsdaten falsch sind.

1. Überprüfen Sie die BindDN.
2. Überprüfen Sie das in den LDAP-Einstellungen konfigurierte Bindungskennwort.

Fehler 3. Benutzer konnte nicht gefunden werden

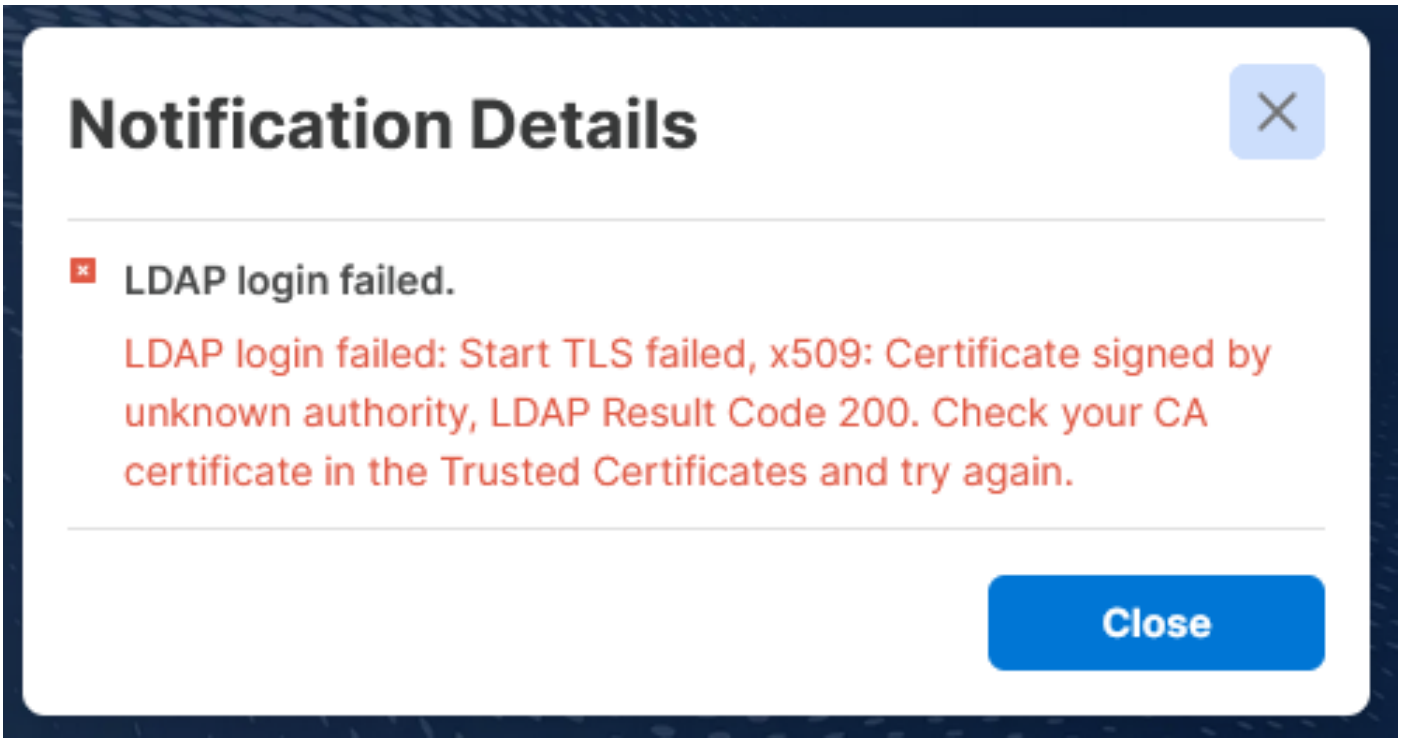


Fehlermeldung für Benutzer nicht gefunden

Dies wird ausgelöst, wenn bei der Suche im LDAP-Server keine autorisierten Benutzer zurückgegeben werden. Überprüfen Sie, ob die nächsten Einstellungen richtig sind:

1. Aktivieren Sie BaseDN. Die Parameter, die zum Suchen des Benutzers verwendet werden, sind falsch.
2. Stellen Sie sicher, dass das Gruppenattribut auf member anstelle von memberOf festgelegt ist.
3. Überprüfen Sie, ob der Gruppenname im Identitätsanbieter in der Gruppen-Konfiguration richtig ist. Dies gilt nur, wenn die Autorisierung über Gruppen erfolgt.
4. Vergewissern Sie sich, dass die E-Mail-Adresse des Benutzers in der AD-Konfiguration für den Benutzer im E-Mail-Feld richtig festgelegt ist. Dies gilt nur, wenn die Autorisierung einzelnen Nutzern erteilt wird.

Fehler 4. Falsches Zertifikat

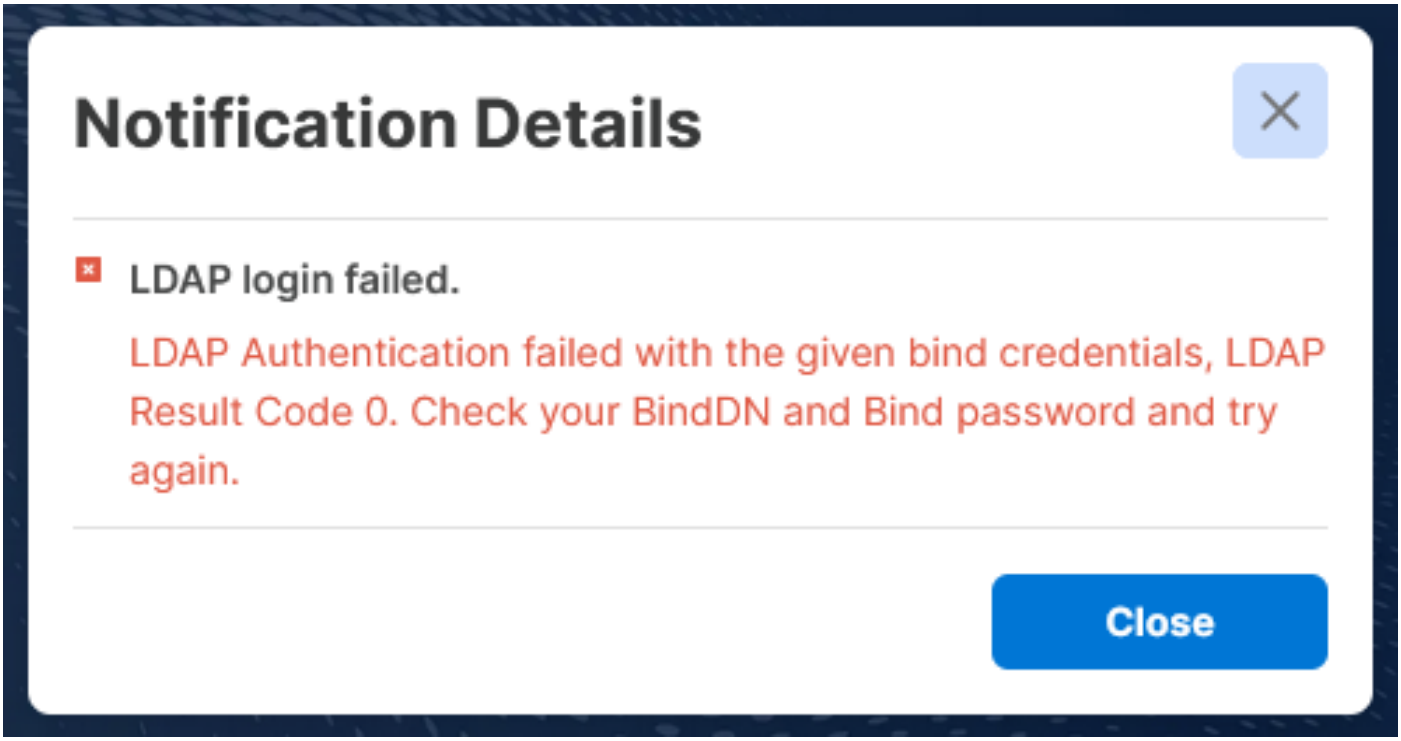


Fehlermeldung für falsches Zertifikat

Wenn verschlüsseltes LDAP aktiviert ist:

1. Überprüfen Sie, ob das Zertifikat konfiguriert ist und das richtige vollständige Zertifikat enthält.

Fehler 5. Die Verschlüsselung aktivieren wird mit einem sicheren Port verwendet.

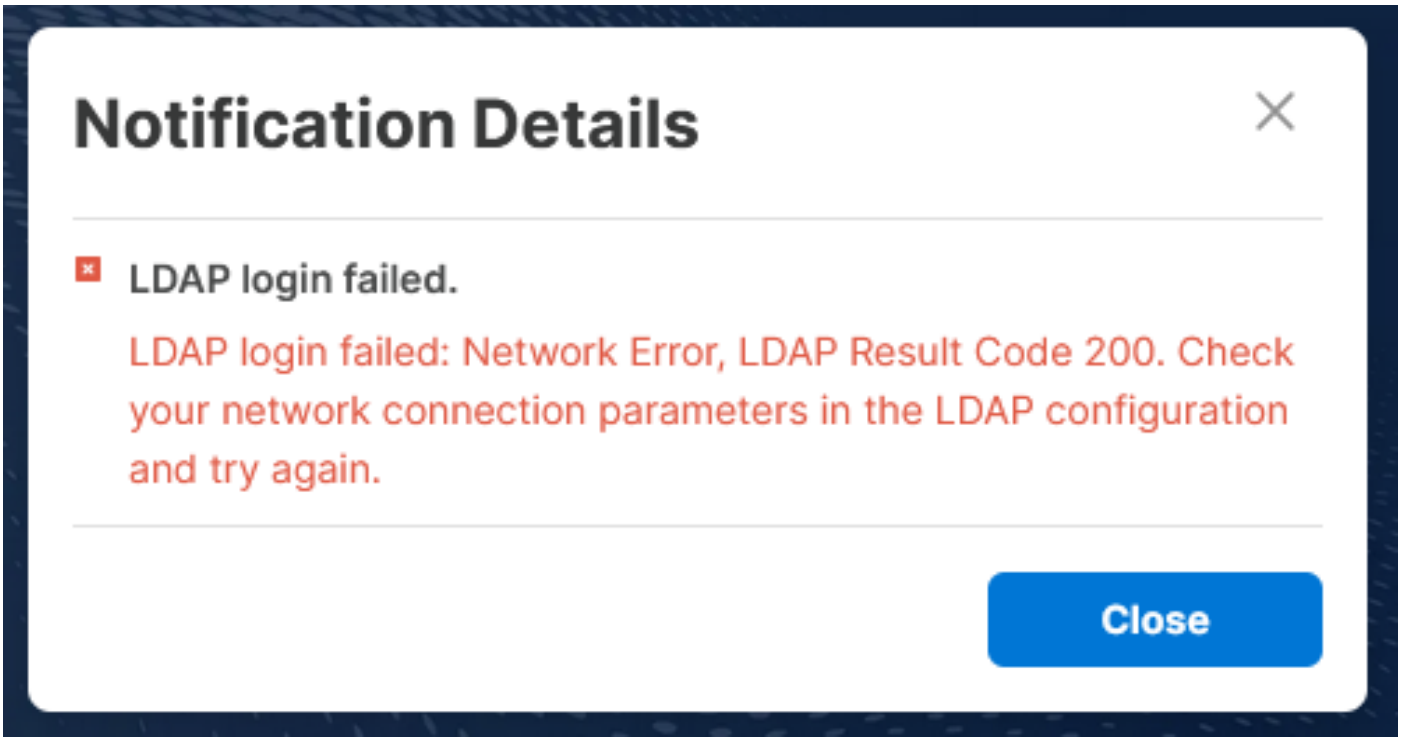


Fehlermeldung zum Aktivieren der Verschlüsselung ist deaktiviert

Dieser Fehler wird angezeigt, wenn Encryption aktivieren nicht aktiviert ist, aber ein Port für sicheres LDAP konfiguriert ist.

1. Stellen Sie sicher, dass Sie Port 389 verwenden, wenn die Verschlüsselung nicht aktiviert ist.

Fehler 6. Falsche Verbindungsparameter



Fehlermeldung für falschen Port

Dieser Fehler bedeutet, dass keine erfolgreiche Verbindung zum LDAP-Server hergestellt werden konnte. Bitte überprüfen Sie:

1. Der DNS-Server muss den Hostnamen des LDAP-Servers in die richtige IP auflösen.
2. Die Intersight-Appliance kann den LDAP-Server erreichen.
3. Stellen Sie sicher, dass Port 389 für unverschlüsseltes LDAP, 636 oder 3269 für sicheres LDAP (LDAPS) und jeder andere für TLS verwendet wird (aktivieren Sie die Verschlüsselung, und richten Sie ein Zertifikat ein).

Zugehörige Informationen

- Integration der Cisco Intersight Virtual Appliance in LDAP (Video)
- LDAP-Einstellungen in Intersight-Appliance konfigurieren
- Rollen und Berechtigungen in Interviews
- Beispielkonfiguration für LDAP in UCSM

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.