Intersight仮想アプライアンスでのLDAPの設定

内容

はじめに

このドキュメントでは、Intersightプライベート仮想アプライアンス(PVA)でLDAP認証を設定するプロセスについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Lightweight Directory Access Protocol(LDAP)プロトコル。
- Intersightプライベート仮想アプライアンス。
- ドメインネームサーバ(DNS)サーバ。

使用するコンポーネント

- Intersightプライベート仮想アプライアンス。
- Microsoft Active Directory.
- DNS サーバ.

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

LDAPは、ネットワークを介してディレクトリからリソースにアクセスするために使用されるプロトコルです。これらのディレクトリには、ユーザ、組織、およびリソースに関する情報が格納されます。LDAPは、認証および認可プロセスに使用できる情報にアクセスして管理するための標準的な方法を提供します。

このドキュメントでは、LDAPを使用したリモート認証をIntersight PVAに追加するための設定プロセスについて説明します。

設定

LDAPの基本設定

1. System > Settings > AUTHENTICATION > LDAP/ADの順に移動します。
2. Configure LDAPをクリックします。
3. 必要な情報を入力します。次の推奨事項を検討します。
    1. Nameは任意に設定され、設定には影響しません。
    2. BaseDN(AD)とBindDNの場合は、Active Directory(AD)設定から対応する値をコピーアンドペーストします。
    3. Group Attributeのデフォルト値はmemberです。

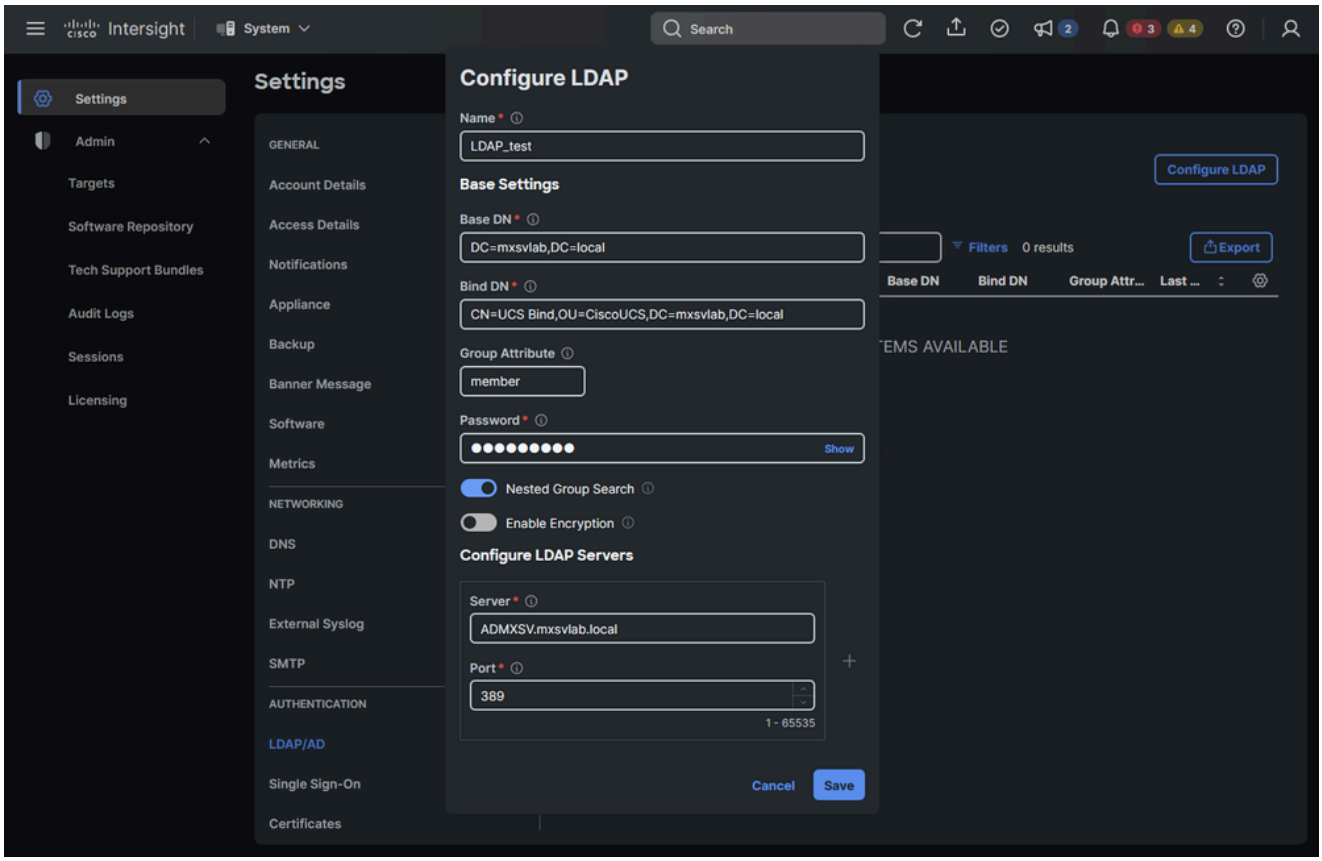
    > 注：UCSMやCIMCなどの他のUCS管理ツールでは、Group属性がmemberOfに設定されます。Intersightでは、メンバーとして残しておくことをお勧めします。

    4. このLDAPプロバイダーのパスワードを入力します。
    5. ルートからのすべてのグループとそれらに含まれるグループをADで再帰検索できるようにする場合は、ネストグループ検索切り替えを有効にします。
    6. 通常のLDAP設定では、Enable Encryptionをディセーブルのままにします。セキュアLDAPが必要な場合は、これを有効にし、「LDAPSの設定（セキュアLDAP）」の項で、設定する必要のある補足手順を確認してください。
4. 1つのLDAPサーバの設定を追加します。
    1. 「サーバ」で、LDAPサーバのIPまたはホスト名を紹介します。

> ⚠ 注意:hostnameを使用する場合、DNSがそのホスト名を正しくマッピングできることを確認してください。

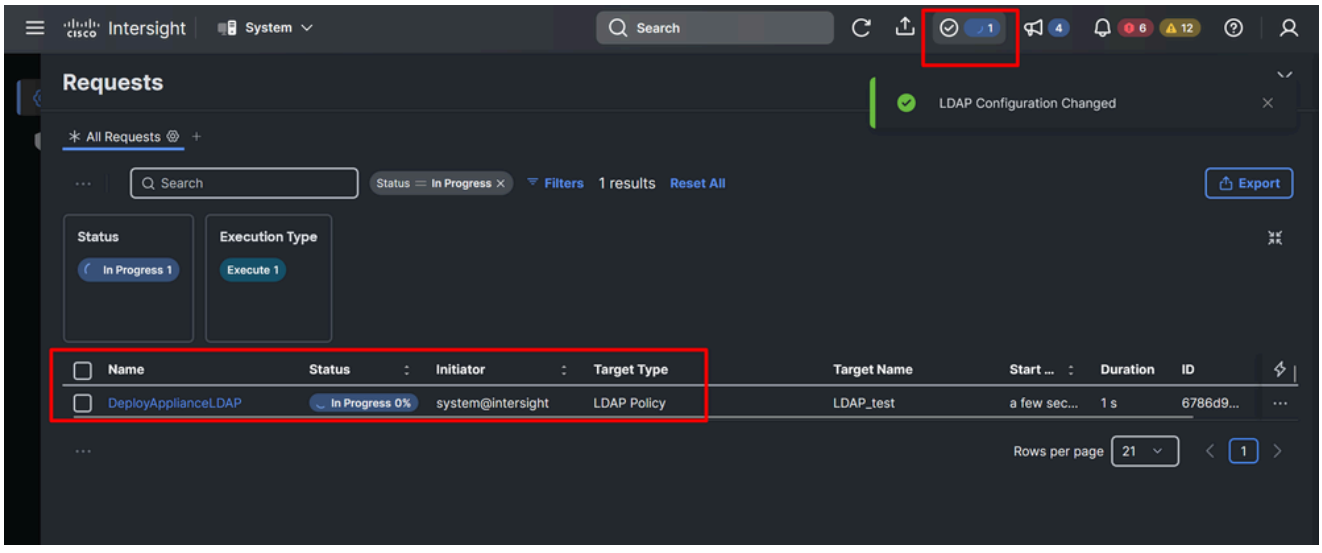
2. LDAPのデフォルトおよび推奨ポートは389です。

5. [Save] をクリックします。



基本的なLDAP設定の設定例

6. トップバーのRequestsからワークフローDeployApplianceLDAPをモニタします。



導入要求

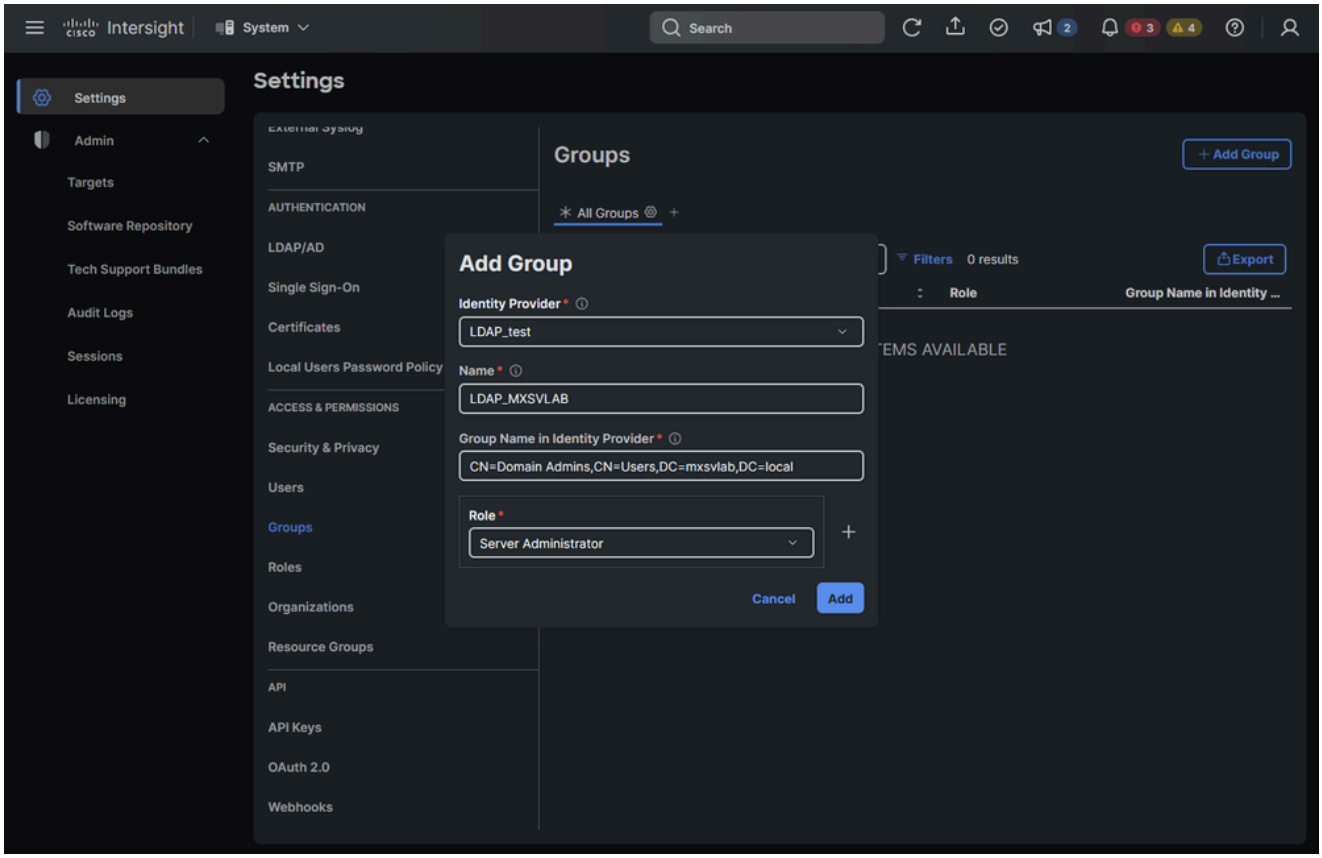
ユーザとグループの設定

ワークフローDeployApplianceLDAPが完了したら、グループまたは個々のユーザを設定できます。

グループを使用すると、そのグループに属するすべてのユーザに認可が提供されます。個々のユーザを使用する場合は、各ユーザを独自の許可ロールで追加する必要があります。

グループの設定

1. System > Settings > ACCESS & PERMISSION > Groupsの順に移動します。.
2. Add Groupをクリックします。
3. Identity Providerを選択します。これは、「LDAPの基本設定の設定」セクションで設定した名前です。
4. グループの名前を設定します。
5. IDプロバイダーのグループ名の値を入力します。LDAPサーバのグループの設定と一致している必要があります。
6. このグループのユーザに提供するアクセスレベルに応じて、ロールを選択します。「Intersightでのロールと権限」を参照してください。



グループの設定例

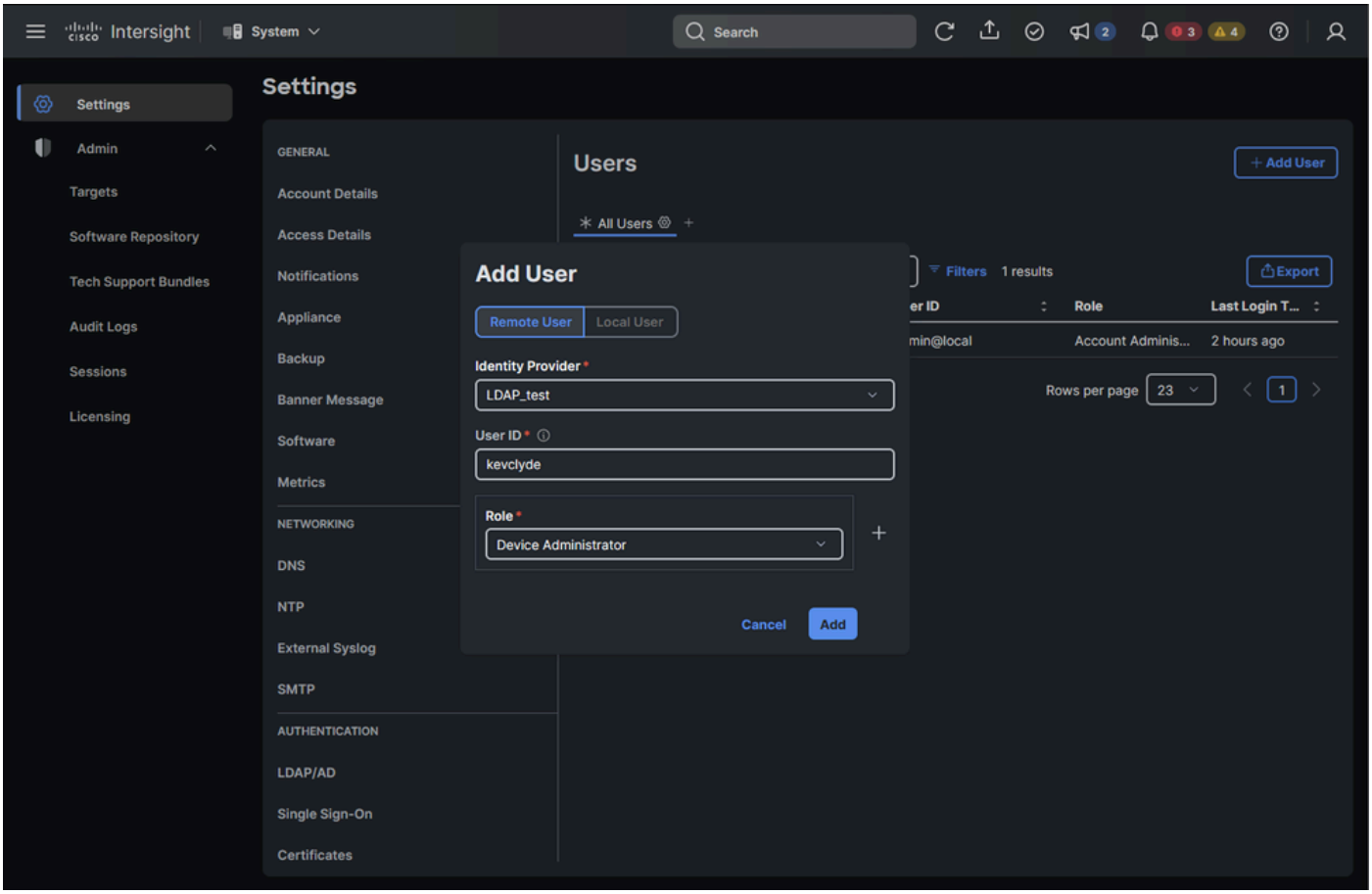
ユーザの設定

グループの代わりに個々のユーザを設定する場合は、次の手順に従ってください。

1. System > Settings > ACCESS & PERMISSION > Usersの順に移動します。
2. Add Userをクリックします。
3. Remote Userを選択します。
4. Identity Providerを選択します。これは、「LDAPの基本設定の設定」セクションで設定した名前です。
5. ユーザIDを設定します。

> ヒント：ユーザ名をログイン方式として使用するには、LDAPサーバのUser IDフィールドに、sAMAccountNameとして設定した値をコピーします。
> 電子メールを使用する場合は、LDAPサーバのmail属性にユーザの電子メールが設定されていることを確認してください。

6. ユーザに提供するアクセスレベルに応じて、ロールを選択します。「Intersightでのロールと権限」を参照してください。



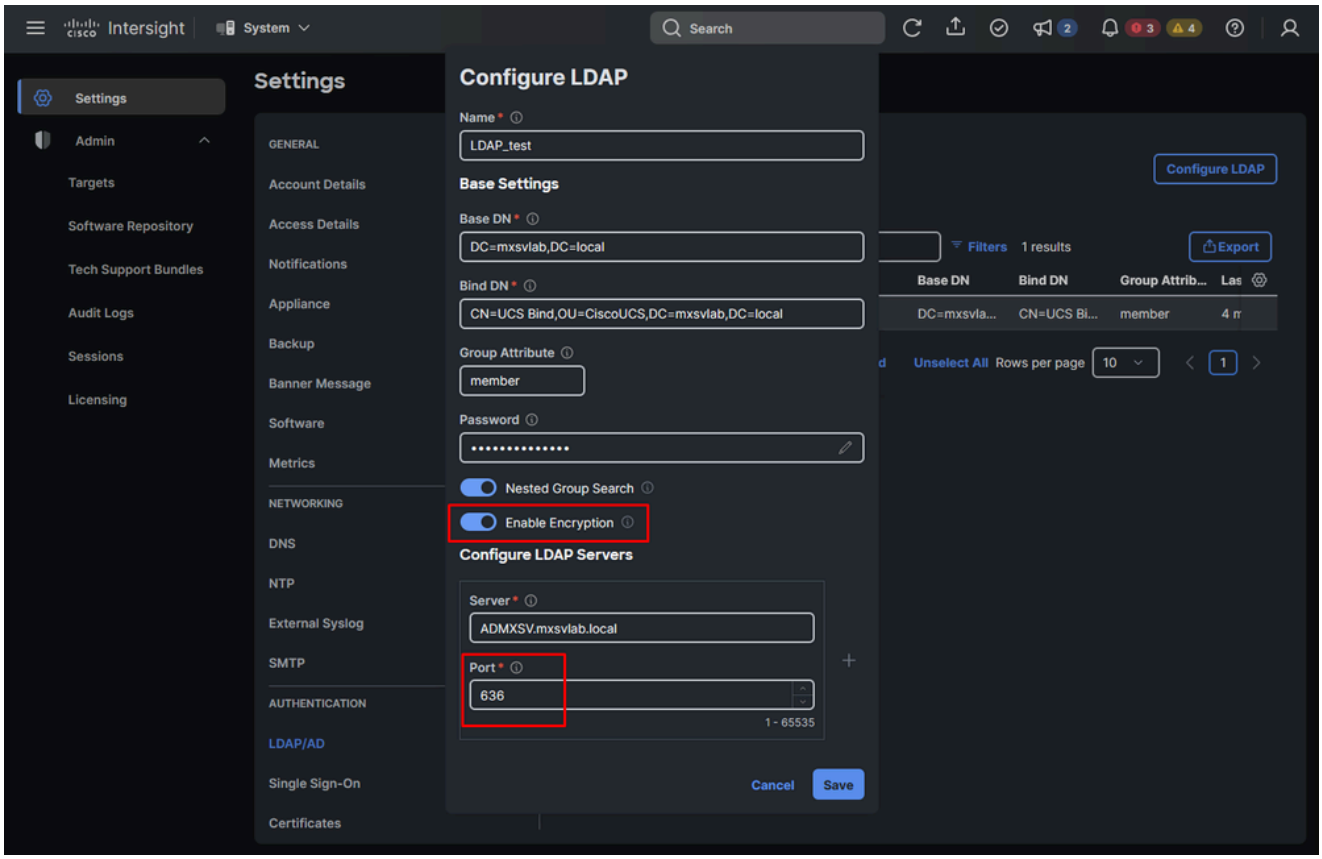
ユーザの設定例

LDAPS（セキュアLDAP）の設定

LDAP通信を暗号化で保護する場合は、CAによって署名された証明書が必要です。これらの変更を設定に適用します。

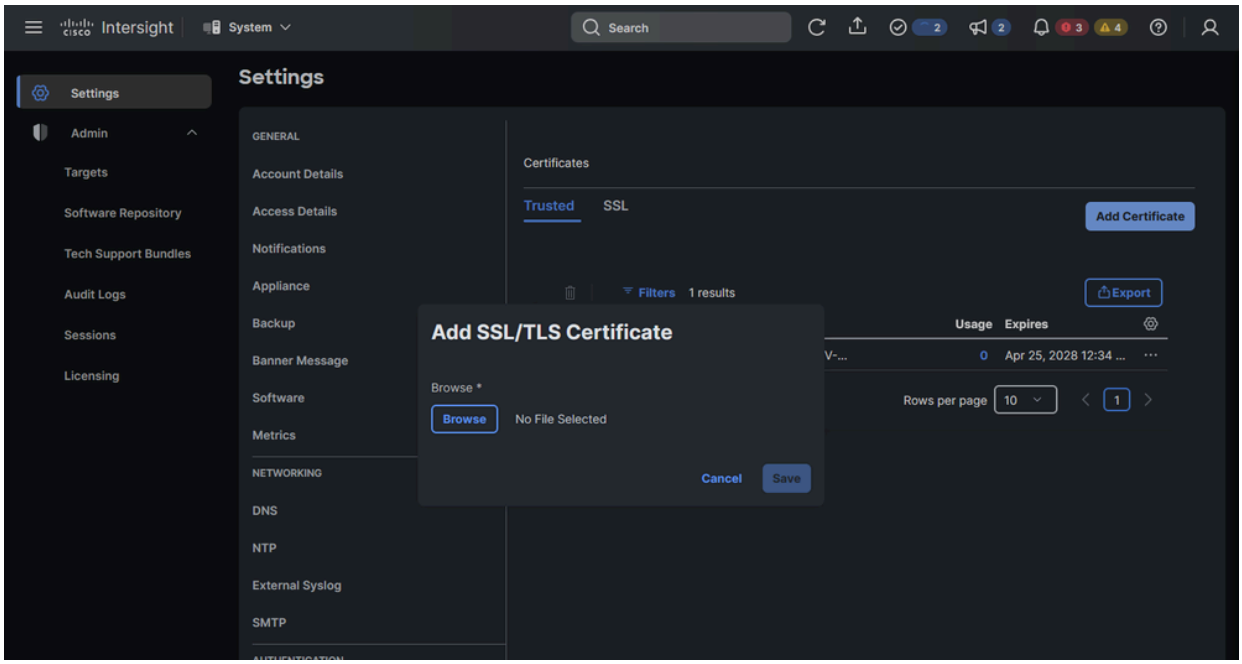
1. 「LDAP基本設定の設定」の手順を実行しますが、スライダEnable Encryption（ステップ3.g）が右に移動していることを確認します。
2. 使用されているポート（ポート番号）が、LDAPS（セキュア）をサポートしているポート

である636（非セキュア）または3269であることを確認します。 他のすべてのポートはTLS経由のLDAPをサポートします。



セキュアLDAPの設定の変更

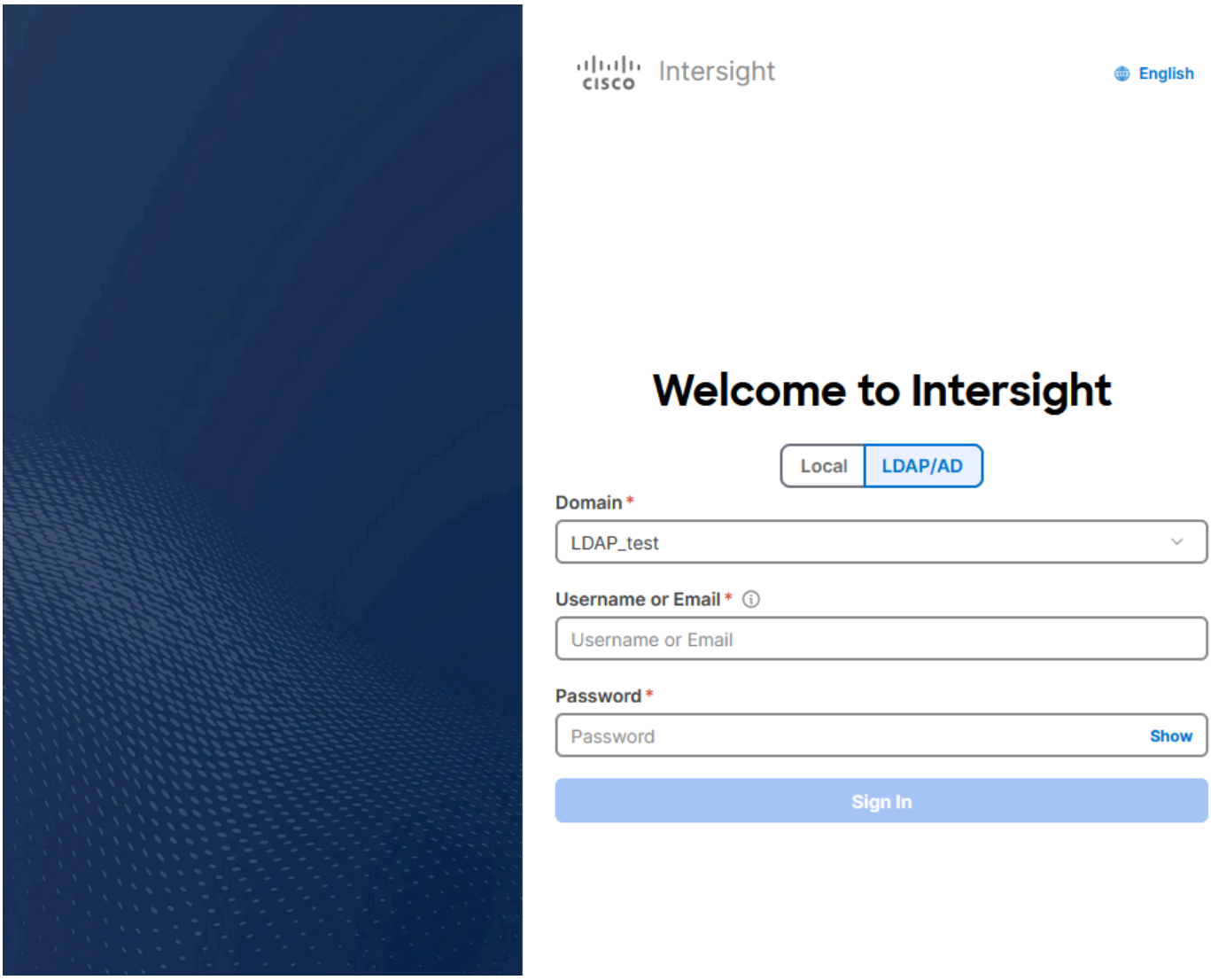
3. 設定を保存し、ワークフローDeployApplianceLDAPが完了するのを待ちます。
4. 次の手順で証明書を追加します。
    1. System > Settings > AUTHENTICATION >の順に移動します。 Certificates > Trustedの順に選択します。
    2. [証明書の追加（Add Certificate）] をクリックします。
    3. Browseをクリックし、CAによって発行された証明書を含む.pemファイルを選択します。



証明書を追加するための設定

確認

ブラウザで、Intersight仮想アプライアンスURLに移動します。画面に、LDAPクレデンシャルでログインするオプションが表示されます。

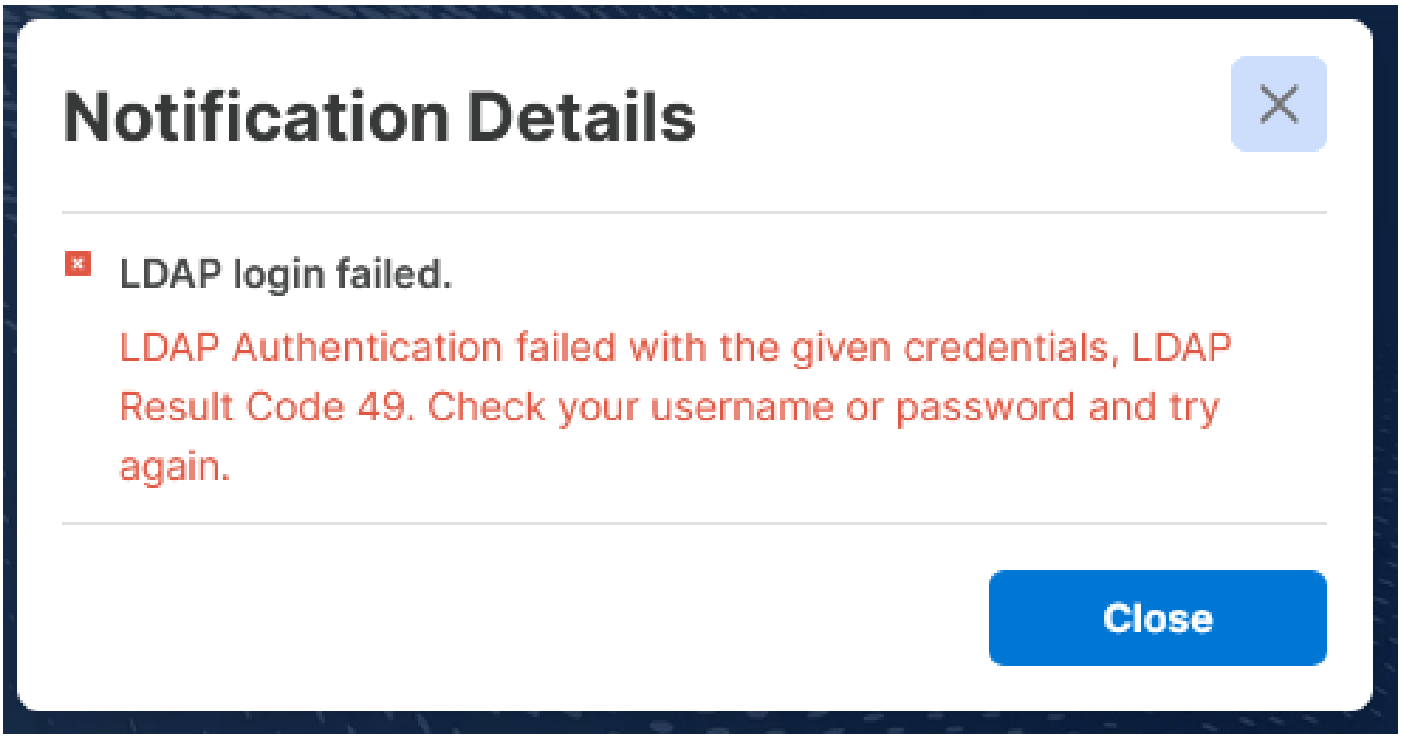


ログイン画面からLDAP設定を有効化

トラブルシュート

ログインが失敗すると、エラーメッセージに問題のヒントが表示されます。

Error 1.不正なアクセスの詳細

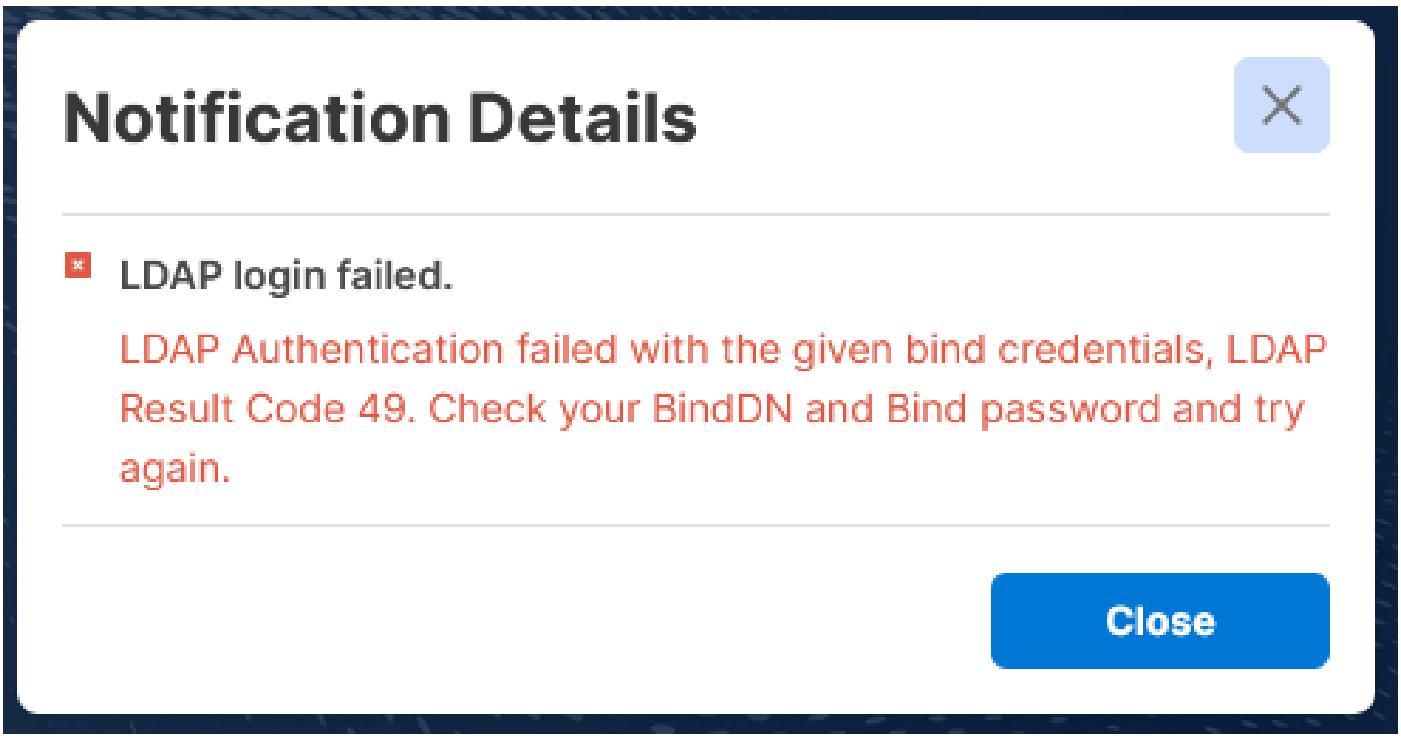


誤ったパスワードエラーのエラーメッセージ

このエラーは、アクセスデータが正しくないことを意味します。

1. ユーザ名とパスワードが正しいことを確認します。

Error 2.バインドデータが正しくありません

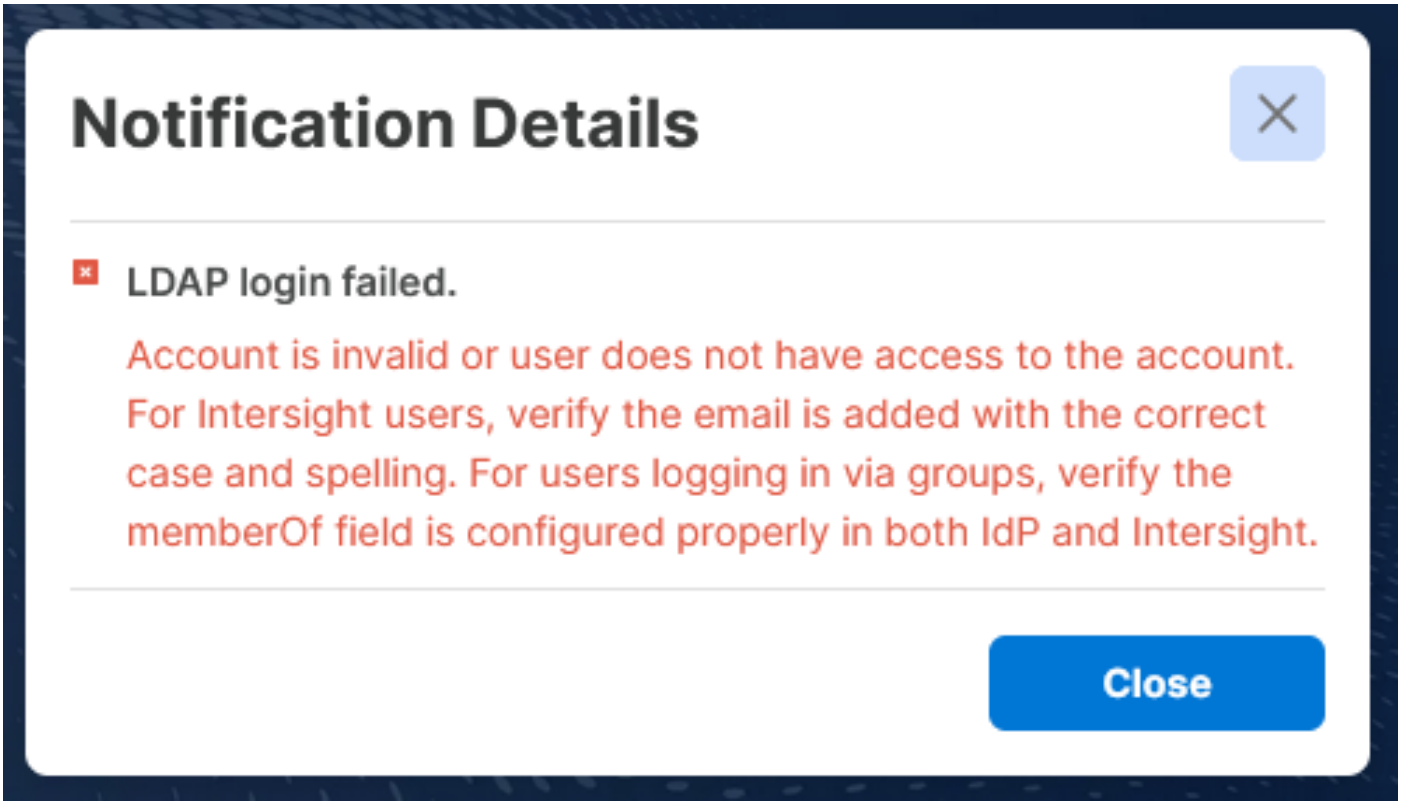


誤ったバインドデータに関するエラーメッセージ

このエラーは、バインドデータが正しくないことを意味します。

1. BindDNを確認します。
2. LDAP設定で設定されているバインドパスワードを確認します。

Error 3.ユーザが見つかりません

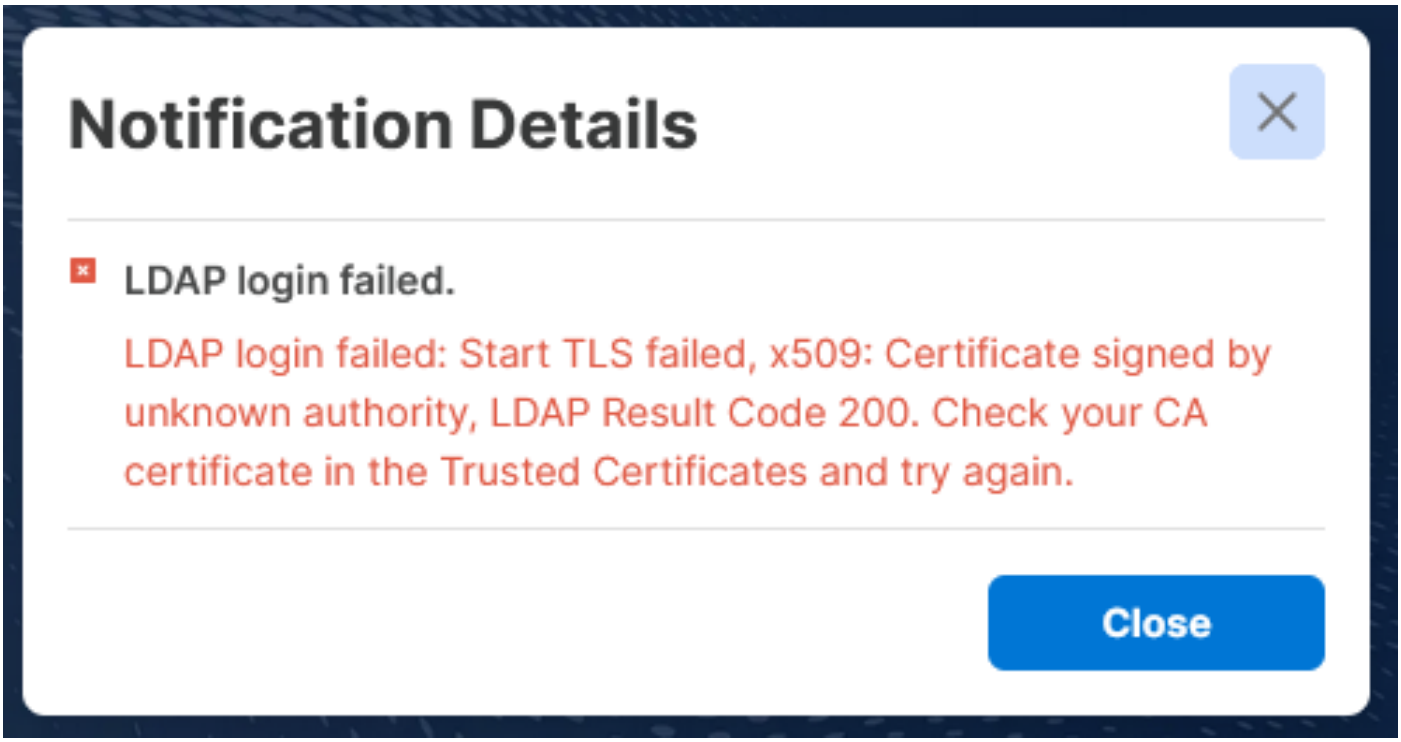


ユーザが見つからないというエラーメッセージ

これは、LDAPサーバでの検索で、許可されたユーザが返されない場合にトリガーされます。次の設定が正しいことを確認します。

1. BaseDNにチェックマークを付けます。ユーザの検索に使用されるパラメータが正しくありません。
2. Group AttributeがmemberOfではなくmemberに設定されていることを確認します。
3. Groups設定のGroup Name in Identity Providerが正しいことを確認します。これは、グループを介して許可が提供される場合にのみ適用されます。
4. ユーザの電子メールが、ユーザのAD設定のmailフィールドで正しく設定されていることを確認します。これは、個々のユーザに認可が提供される場合にのみ適用されます。

Error 4.誤った証明書

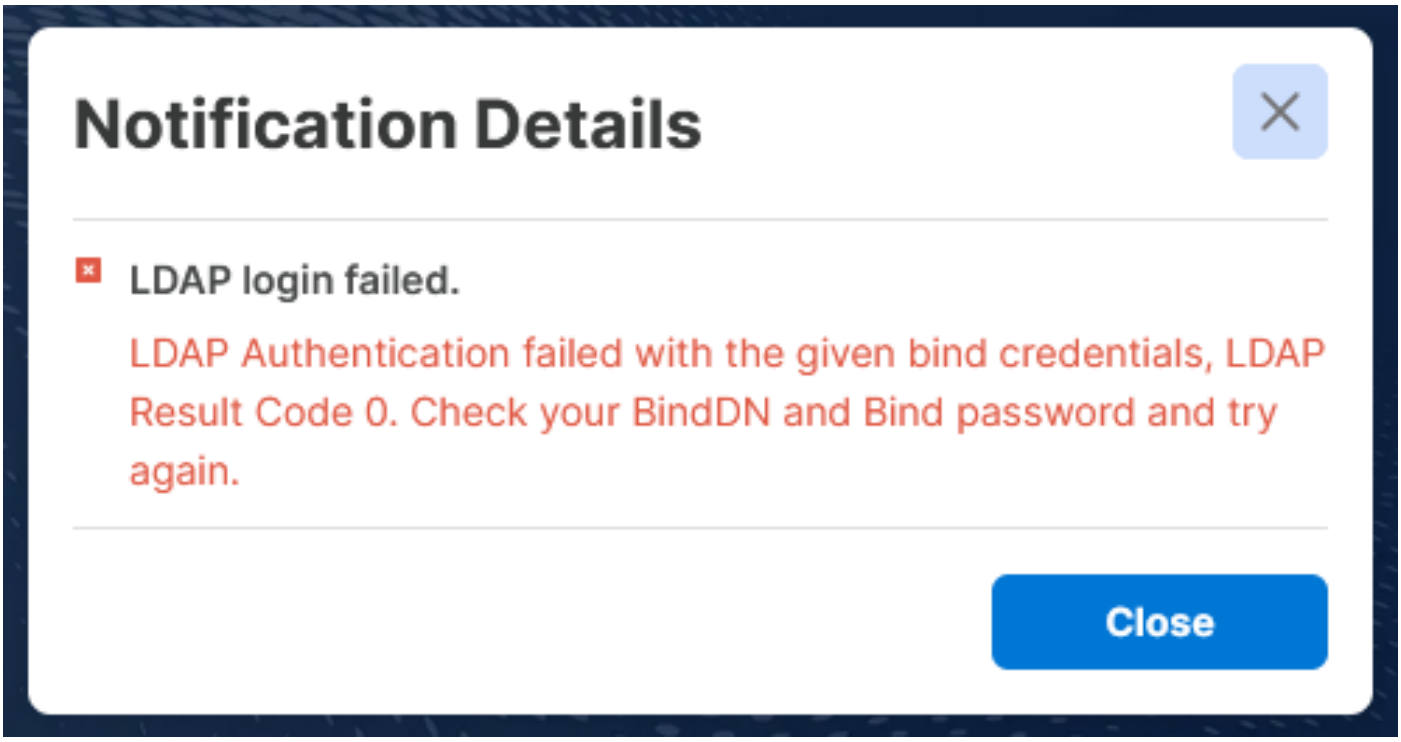


誤った証明書のエラーメッセージ

暗号化LDAPが有効な場合：

1. 証明書が設定され、正しい完全な証明書が含まれていることを確認します。

Error 5.暗号化の有効化がセキュアポートで使用されている



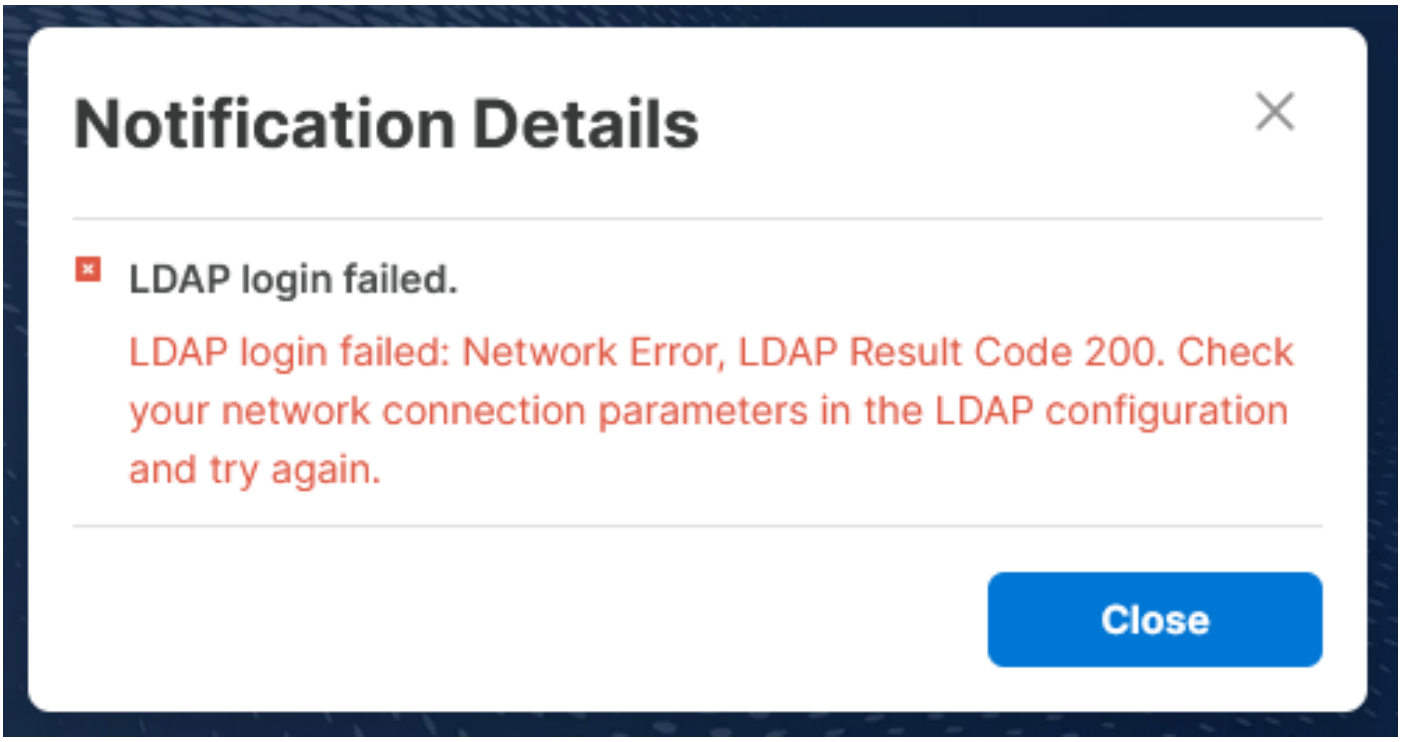
Enable Encryption is Disabledのエラーメッセージ

このエラーは、Enable Encryptionが有効になっていないにもかかわらず、セキュアLDAPのポー

トが設定されている場合に表示されます。

1. 暗号化が有効になっていない場合は、ポート389を使用していることを確認してください。

Error 6.接続パラメータが正しくありません



誤ったポートのエラーメッセージ

このエラーは、LDAPサーバへの接続が正常に確立できなかったことを意味します。確認してください。

1. DNSサーバは、LDAPサーバのホスト名を正しいIPに解決する必要があります。
2. IntersightアプライアンスはLDAPサーバに到達できる。
3. ポート389が暗号化されていないLDAPに使用されていること、636または3269がセキュアLDAP(LDAPS)に使用されていること、およびその他のポートがTLSに使用されていること（暗号化を有効にして証明書をセットアップする）を確認します。

関連情報

- Cisco Intersight仮想アプライアンスとLDAPの統合（ビデオ）
- Intersightアプライアンスでの LDAP設定
- Intersightのロールと権限
- UCSMでのLDAPの設定例

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。