Web、API、およびCLIアクセス用のExpresswayでのLDAPの設定

内容

はじめに

このドキュメントでは、ExpresswayサーバでLightweight Directory Access Protocol(LDAP)をイネーブルにするために必要な手順と、管理者グループがWeb、アプリケーションプログラミングインターフェイス(API)、およびコマンドラインインターフェイス(CLI)を介してExpresswayにドメインユーザでアクセスできるようにする方法について説明します。

著者：Cisco TACエンジニア、Jefferson MadrizおよびElias Sevilla

前提条件

要件

- Expresswayの基礎知識
- Expresswayの基本設定はすでに完了しています。
- Active Directory(AD)は既に構成されています。
- ExpresswayとADサーバ間の通信を許可するためのファイアウォールルールの準備ができました。

使用するコンポーネント

- Active DirectoryはWindow Server 2016にインストールされています。
- バージョンX14.0.3のExpressway-Cサーバ。

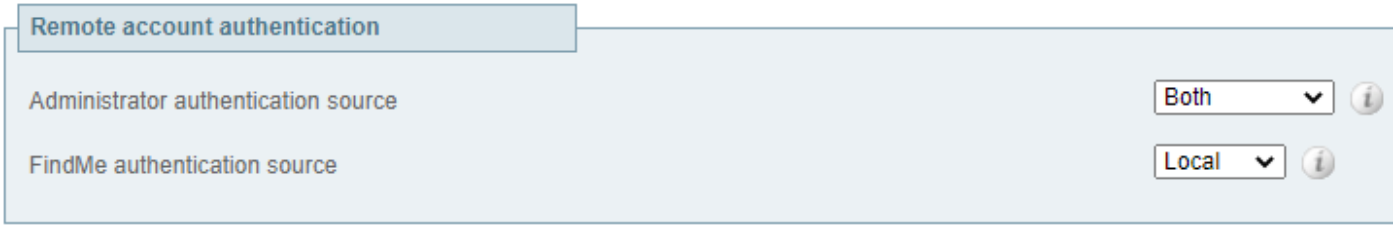
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

LDAPの設定

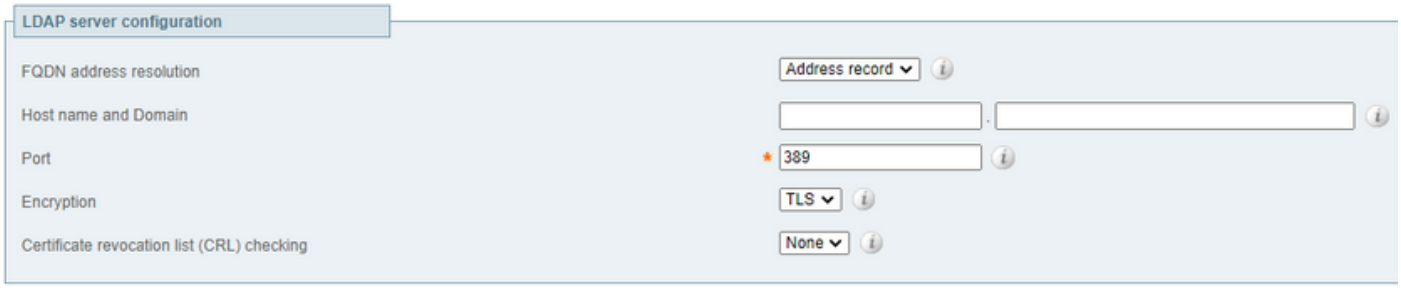
管理者アカウント認証用のリモートディレクトリサービスへのLDAP接続を設定するには、LDAP設定ページのUsers > LDAP configurationを使用します。

- リモートアカウント認証：このセクションでは、リモートアカウント認証でのLDAPの使用を有効または無効にできます。



- ローカルのみ：クレデンシャルは、システムに保存されているローカルデータベースに対して検証されます。
- リモートのみ：クレデンシャルは外部のクレデンシャルディレクトリに対して検証されます。
- 両方：クレデンシャルは、最初にシステムに保存されているローカルデータベースに対して確認され、アカウントと一致するものが見つからない場合は、代わりに外部クレデンシャルディレクトリが使用されます。

- LDAPサーバ設定：このセクションでは、LDAPサーバへの接続の詳細を指定します。



FQDNアドレス解決：

- SRVレコード：ドメインネームサービス(DNS)サービスレコード(SRV)ルックアップ。
- アドレスレコード：DNS AまたはAAAAレコードのルックアップ。
- IPアドレス：IPアドレスとして直接入力されます。

注：SRVレコードを使用する場合は、_ldap._tcp.レコードで標準のLDAPポート389が使用されていることを確認します。Expresswayでは、LDAPの他のポート番号はサポートされて

いません。

ホスト名とドメイン：

- SRVレコード：サーバアドレスのドメイン部分のみが必要です。
- アドレスレコード：ホスト名とドメインを入力します。次に、これらを組み合わせて、DNSアドレスレコードのルックアップに完全なサーバアドレスを提供します。
- IPアドレス：サーバアドレスはIPアドレスとして直接入力されます。

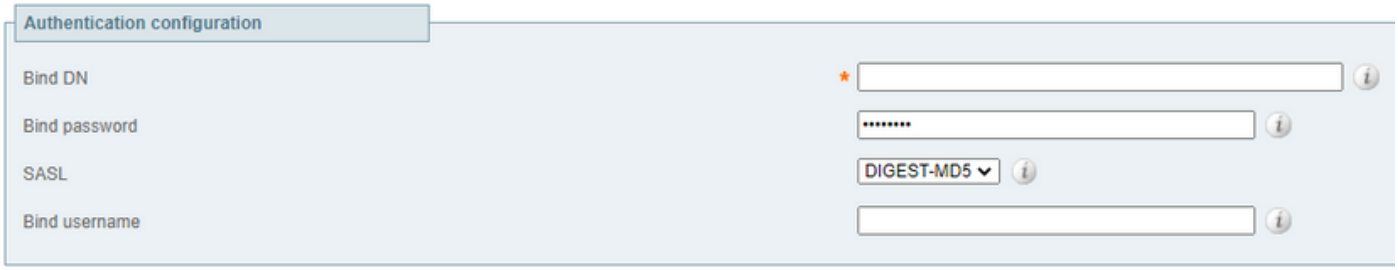
Port：

- LDAPサーバで使用するIPポート。

暗号化：

- TLS:LDAPサーバへの接続にTransport Layer Security(TLS)暗号化を使用します。
- オフ：暗号化は使用されません。

- 認証設定：このセクションでは、LDAPサーバへのバインドに使用するExpresswayの認証資格情報を指定します。



バインドDN:大文字小文字を区別しない、ExpresswayがLDAPサーバにバインドするために使用する識別名(DN)。DNはcn=、ou=、dc=の順に指定することが重要です

注：バインドアカウントは通常、特別な権限のない読み取り専用アカウントです。

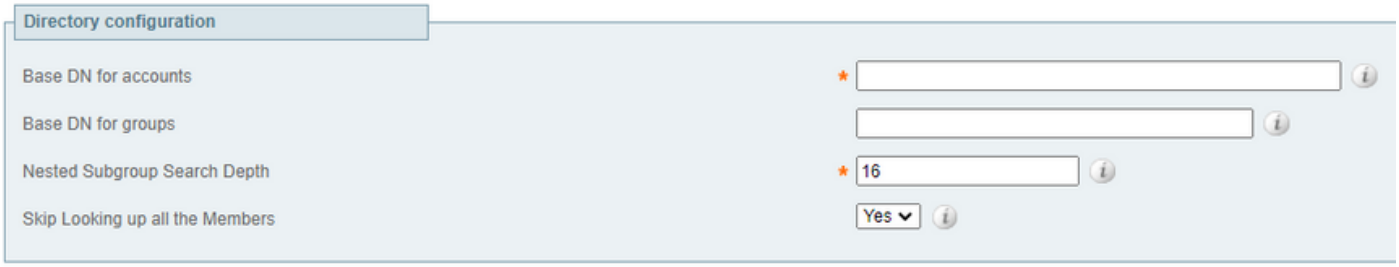
バインドパスワード：ExpresswayがLDAPサーバにバインドするために使用するパスワード（大文字と小文字が区別されます）。

SASL:LDAPサーバへのバインドに使用するSimple Authentication and Security Layer(SASL)メカニズム

- [なし]:メカニズムは使用されません。
- DIGEST-MD5:DIGEST-MD5メカニズムが使用されます。

バインドユーザ名：ExpresswayがLDAPサーバへのログインに使用するアカウントのユーザ名（大文字と小文字が区別されます）。

- ディレクトリ構成：このセクションでは、アカウント名とグループ名の検索に使用するベース識別名を指定します。



アカウントのベースDN:データベース構造でユーザーアカウントの検索が開始される、識別名の組織単位(OU)およびドメインコントローラ(DC)の定義（大文字と小文字は区別されません）。

勘定科目とグループのベースDNは、DCレベルかその下にある必要があります（必要に応じて、すべてのdc=値とou=値を含めます）。 LDAP認証はサブDCアカウントを参照せず、低いOUレベルと共通ネイン(CN)レベルのみを参照します。

グループのベースDN:グループの検索をデータベース構造で開始する必要がある識別名(DN)のOUおよびDC定義（大文字と小文字は区別されません）。

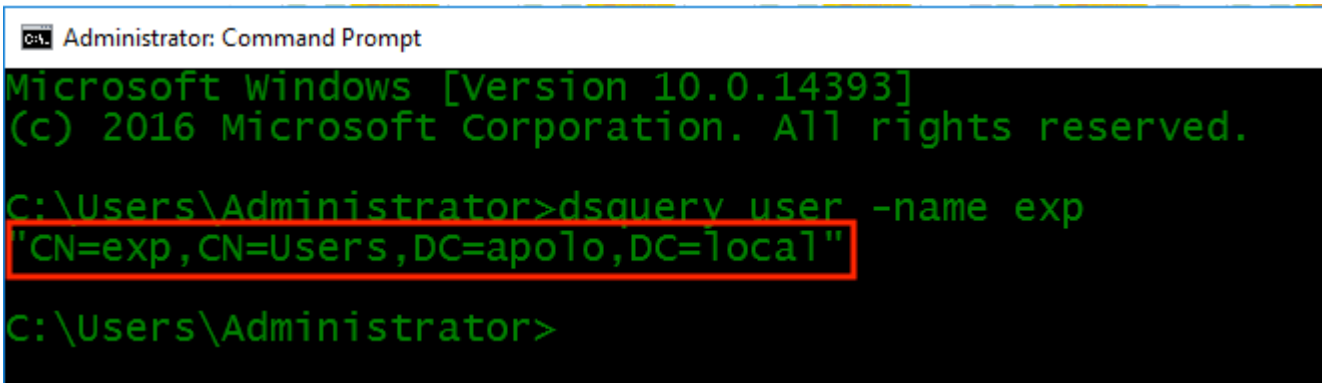
グループのベースDNが指定されていない場合は、アカウントのベースDNがグループとアカウントの両方に使用されます。

Nested subgroup search depth:LDAP検索のグループの深さを制限するために使用されます。

すべてのメンバーの検索をスキップする：認証検索プロセスの実行中に、管理者グループのメンバー検索を無効または有効にするために使用します。デフォルトはYesで、メンバの検索はスキップされます。

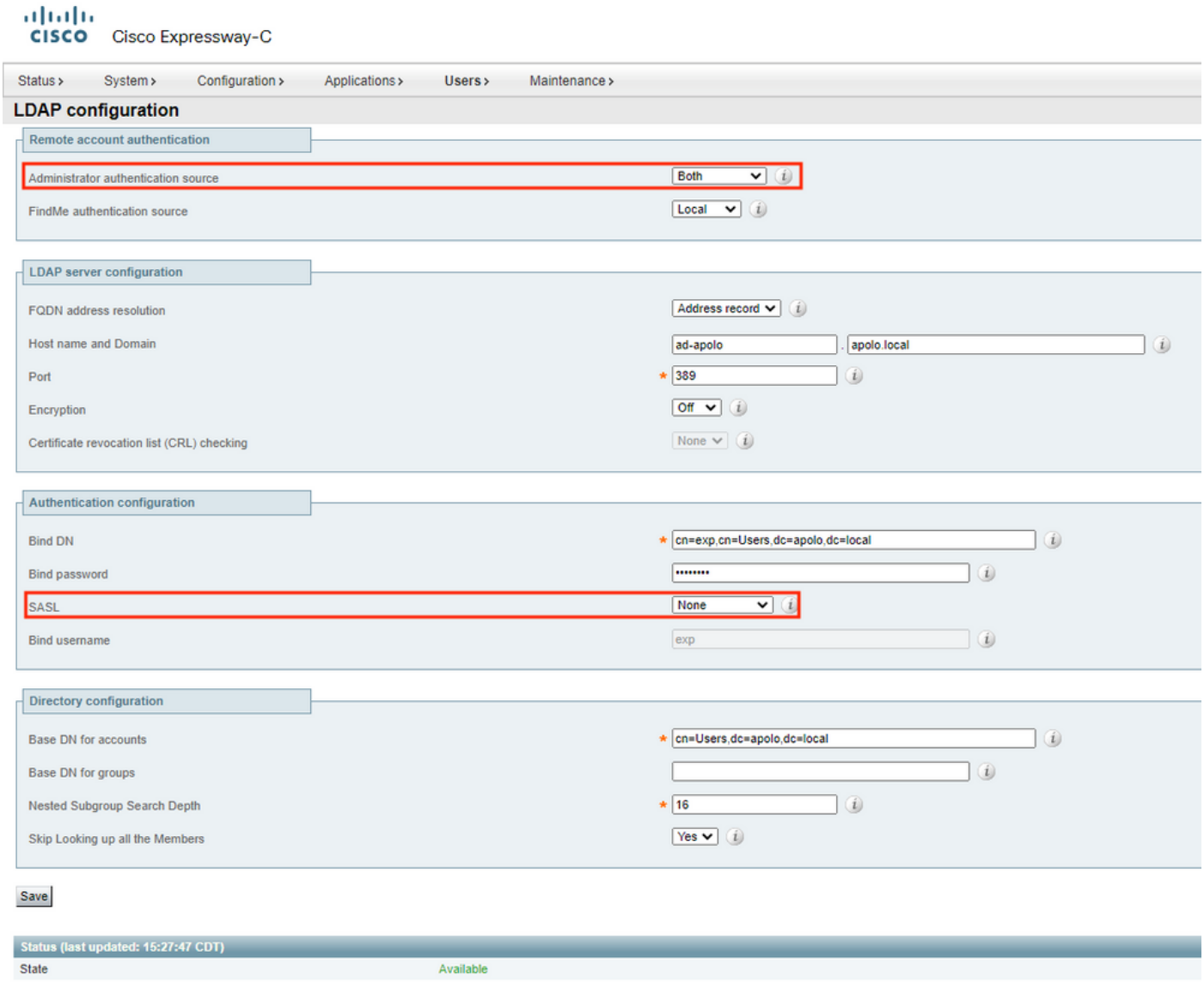
ベースDNの検索方法

ADサーバで、管理者としてコマンドプロンプト(CMD)を開き、コマンド**dsquery user -name <Known username>**を実行します。



LDAPの設定例

この例では、Administrator authentication sourceがBothに設定されており、SASLがNoneに設定されています。



LDAPステータスの確認

LDAPサーバの接続状態を確認します。

- Available：エラーメッセージは表示されません
- Failed：エラーメッセージが表示されます。 LDAPエラーメッセージ

管理者グループの設定

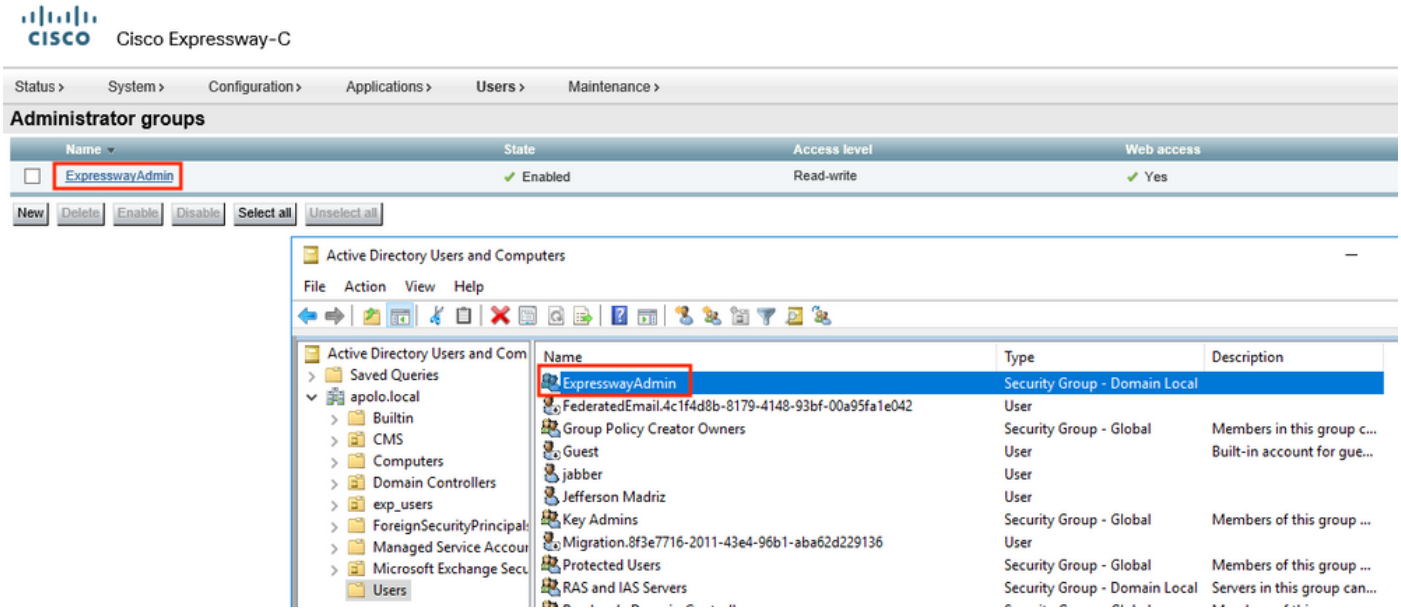
管理者グループページのユーザ>管理者グループには、Expresswayで設定されているすべての管理者グループがリストされ、グループを追加、編集、削除できます。

注：管理者グループは、LDAPを使用したリモートアカウント認証が有効になっている場合にのみ適用されます。

Expressway Webインターフェイスにログインすると、クレデンシャルがリモートディレクトリサービスに対して認証され、所属するグループに関連付けられているアクセス権が割り当てられます。

Expresswayの管理者グループの設定オプション

名前：管理者グループの名前。 Expresswayで定義されたグループ名は、このExpresswayへの管理者アクセスを管理するためにリモートディレクトリサービスで設定されたグループ名と一致する必要があります。



アクセス レベル:

- 読み取り/書き込み：すべての設定情報の表示と変更を許可します。これにより、デフォルトの管理者アカウントと同じ権限が付与されます。
- 読み取り専用：ステータスと設定情報の表示のみを許可し、変更は許可しません。アップグレードページなどの一部のページは、読み取り専用アカウントに対してブロックされています。
- Auditor:Event Log、Configuration Log、Network Log、Alarms、およびOverviewの各ページにのみアクセスできます。
- [なし]:アクセスは許可されません

Webアクセス：このグループのメンバーがWebインターフェイスを使用してシステムにログインできるかどうかを決定します。

APIアクセス：このグループのメンバーがAPIを使用してシステムのステータスと設定にアクセスできるかどうかを決定します。

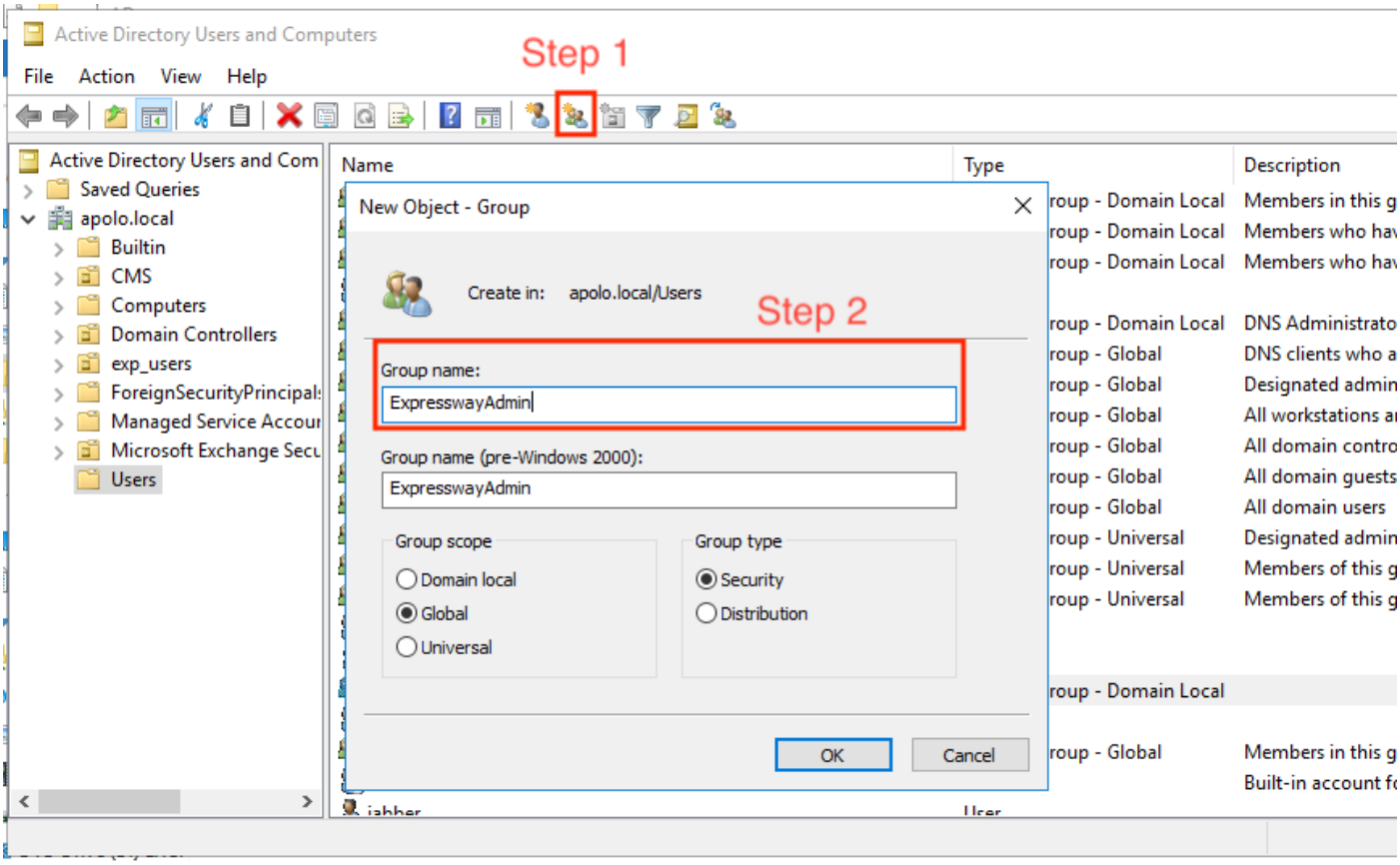
CLIアクセス：このグループのメンバーがCLI経由でシステムにアクセスできるかどうかを決定します。

状態：グループが有効か無効かを示します。

ADでの管理者グループの設定

1. ユーザを保存するフォルダに、新しいオブジェクトグループを作成します。

2.グループ名に名前を割り当てます。

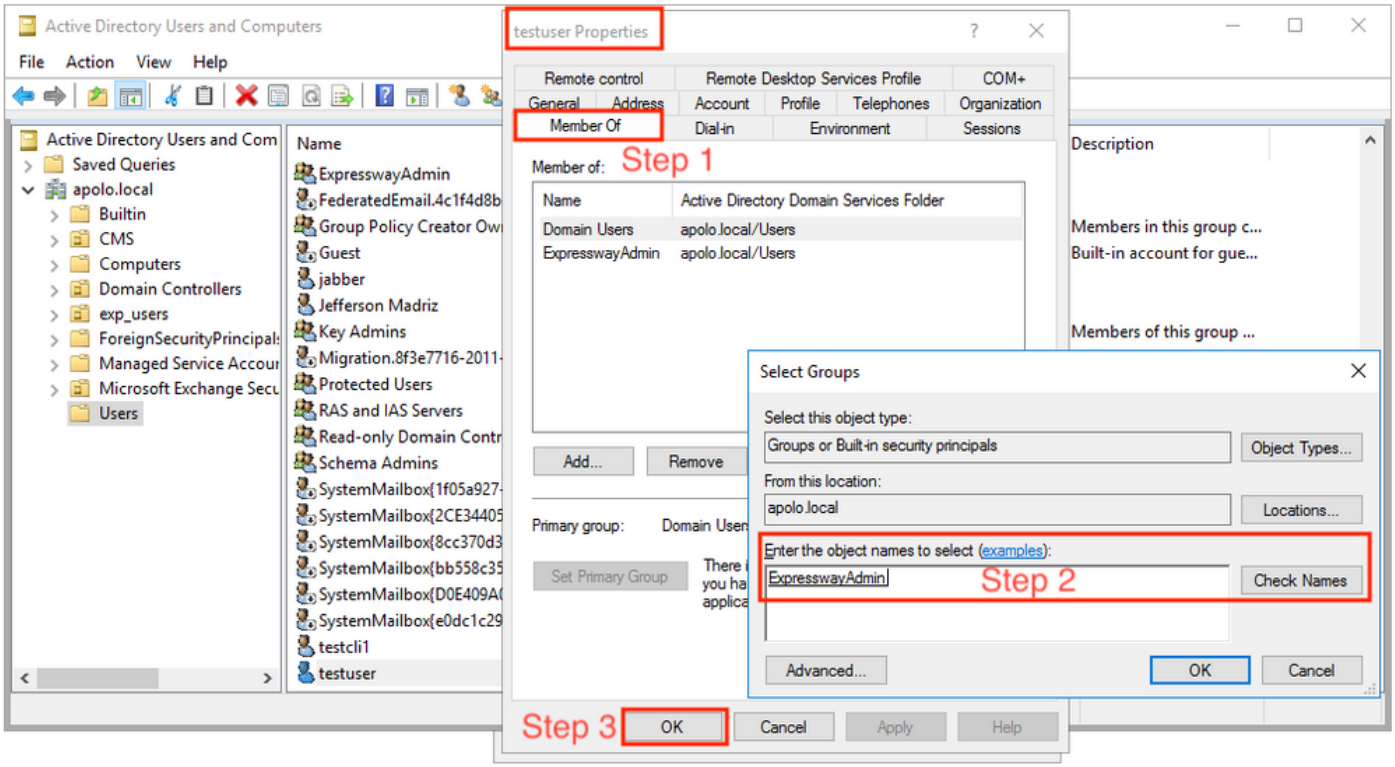


Web、API、またはCLIを介してExpresswayにアクセスする必要があるユーザに、設定したグループを割り当てます。この例では、ユーザはtestuserです。

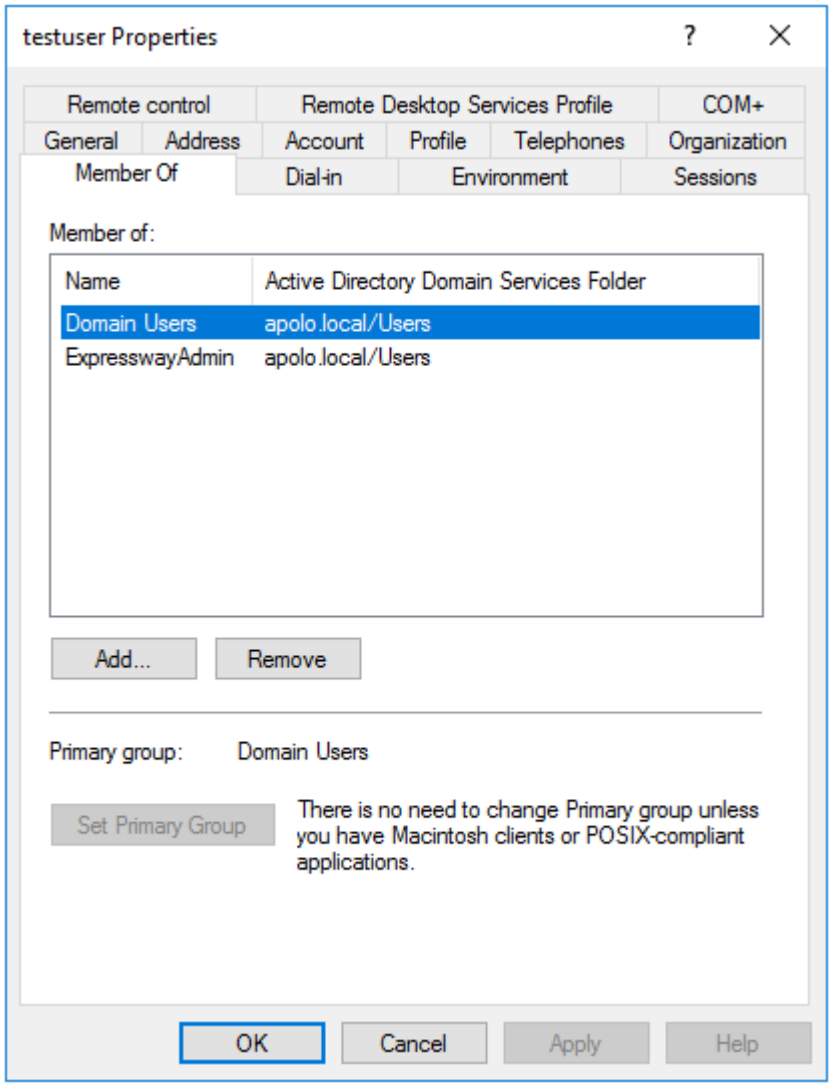
1.ユーザーのプロパティを開き、「Member Of」タブに移動して、「追加」を選択します

2.以前に作成されたグループ名を検索します。

3. 次にOKを選択します。



この時点で、ユーザはDomain UsersとExpresswayAdminのメンバです。

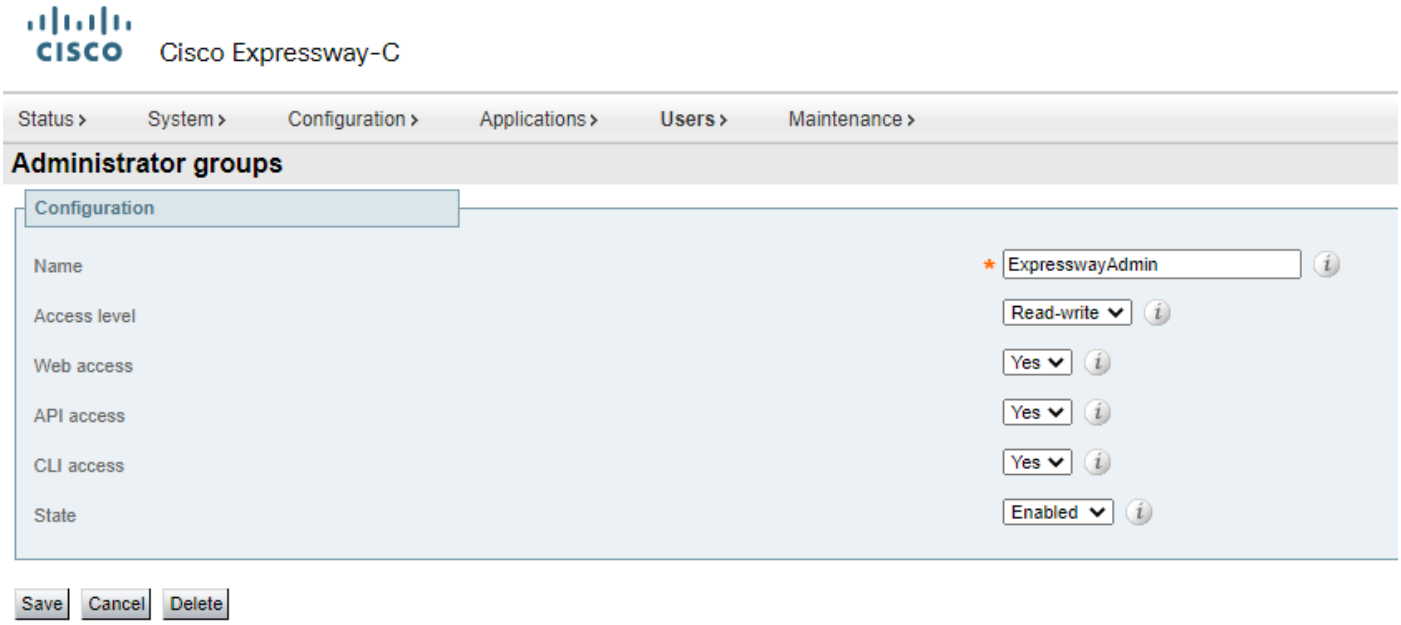


Expresswayでの管理者グループの設定

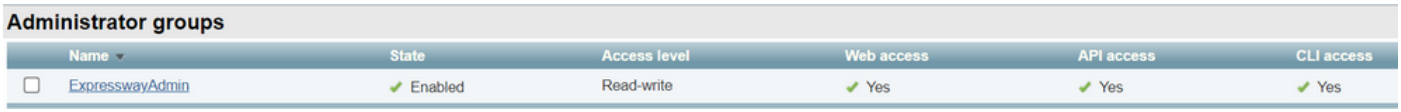
設定が完了したら、ExpresswayでUsers > Administrator groupsの順に移動し、Newを選択します。

Name：設定されているグループ名と一致し、Expresswayにアクセスする必要があるLDAPユーザに関連付けられている必要があります。この例では、グループ名はExpresswayAdminであるため、新しい管理者グループ名はExpresswayAdminです。

このグループには、使用可能なすべての権限とアクセス権があります。

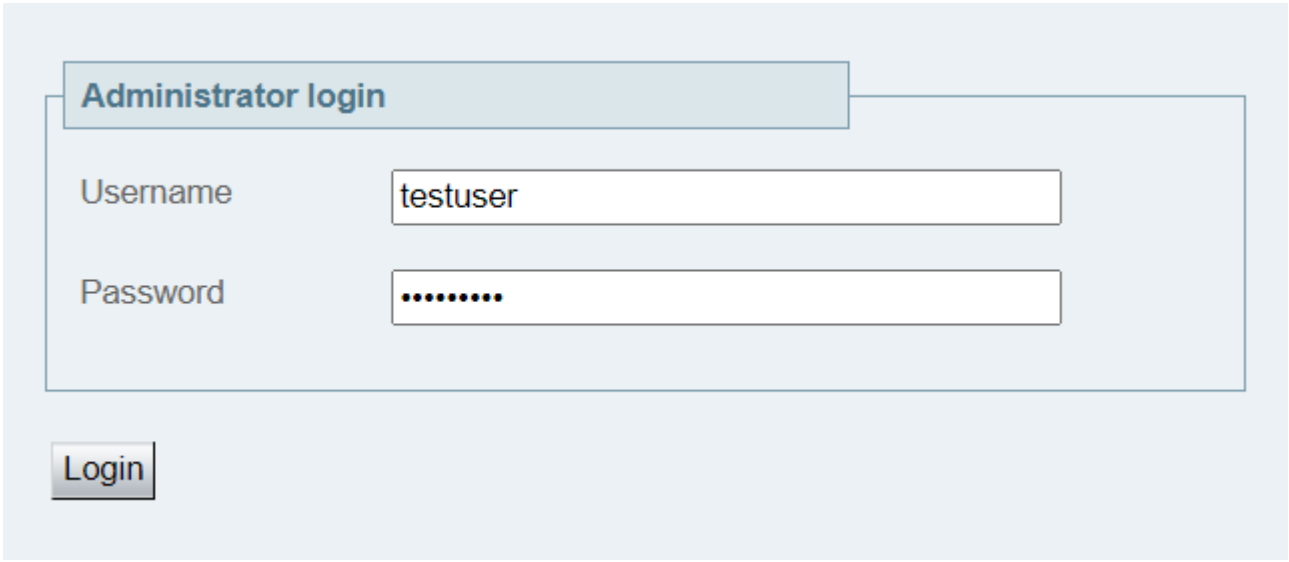


[Save] を選択します。

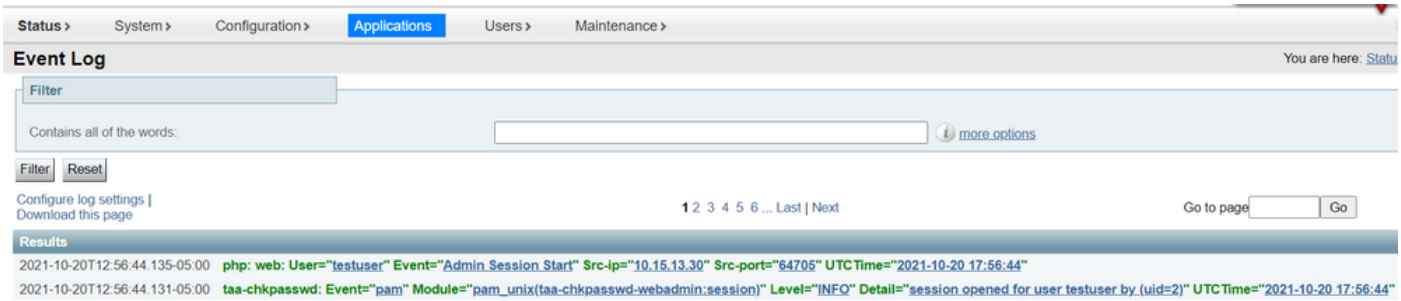


確認

ログアウトし、管理者グループが関連付けられているLDAPユーザで、Web経由でのアクセスを試みます。この例で作成するユーザはtestuserです。



これは、Status > Event logで確認できます。



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。