

# 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](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[LDAPの設定](#)

[ベースDNの検索方法](#)

[LDAPの設定例](#)

[管理者グループの設定](#)

[Expresswayの管理者グループの設定オプション](#)

[ADでの管理者グループの設定](#)

[Expresswayでの管理者グループの設定](#)

[確認](#)

---

## 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。

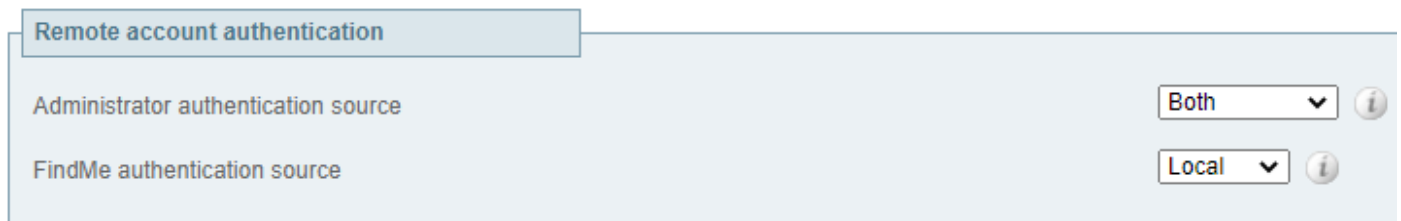
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 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。

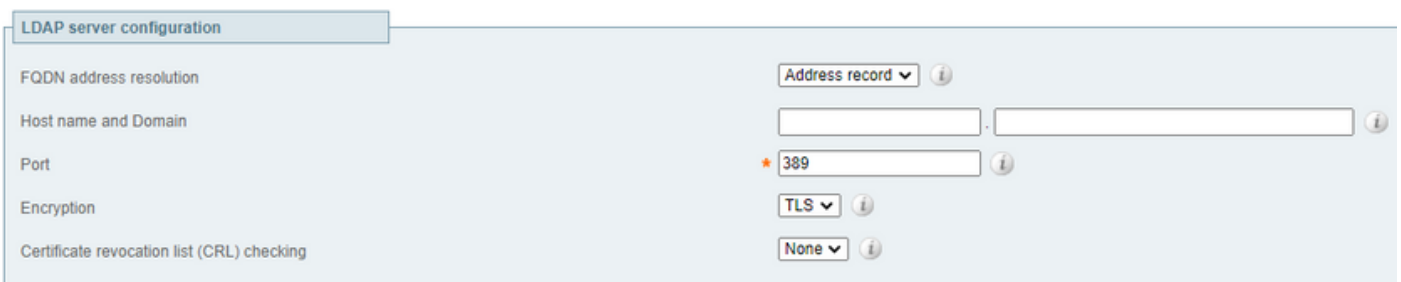
- ・ リモートアカウント認証：このセクションでは、リモートアカウント認証でのLDAPの使用を有効または無効にできます。



The screenshot shows the 'Remote account authentication' configuration section. It contains two rows of settings. The first row is 'Administrator authentication source' with a dropdown menu set to 'Both' and an information icon. The second row is 'FindMe authentication source' with a dropdown menu set to 'Local' and an information icon.

- 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。



The screenshot shows the 'LDAP server configuration' section. It contains several settings: 'FQDN address resolution' with a dropdown set to 'Address record'; 'Host name and Domain' with two text input fields; 'Port' with a text input field containing '389' and a red star icon; 'Encryption' with a dropdown set to 'TLS'; and 'Certificate revocation list (CRL) checking' with a dropdown set to 'None'. Each setting has an information icon.

#### 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：

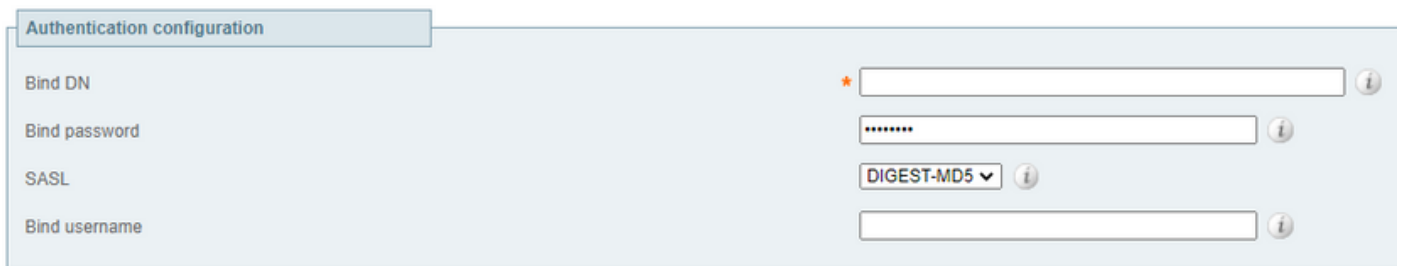
- SRVレコード：サーバアドレスのドメイン部分のみが必要です。
- アドレスレコード：ホスト名とドメインを入力します。次に、これらを組み合わせて、DNSアドレスレコードのルックアップに完全なサーバアドレスを提供します。
- IPアドレス：サーバアドレスはIPアドレスとして直接入力されます。

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。



The screenshot shows the 'Authentication configuration' section of a web interface. It contains four input fields: 'Bind DN' (with a red asterisk), 'Bind password' (masked with dots), 'SASL' (a dropdown menu currently showing 'DIGEST-MD5'), and 'Bind username'. Each field has a small circular information icon (i) to its right.

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。

---

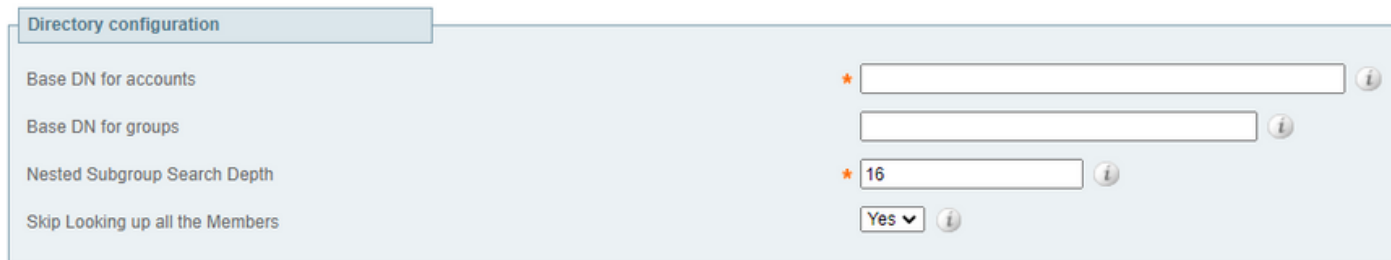
バインドパスワード：ExpresswayがLDAPサーバにバインドするために使用するパスワード（大文字と小文字が区別されます）。

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 )。

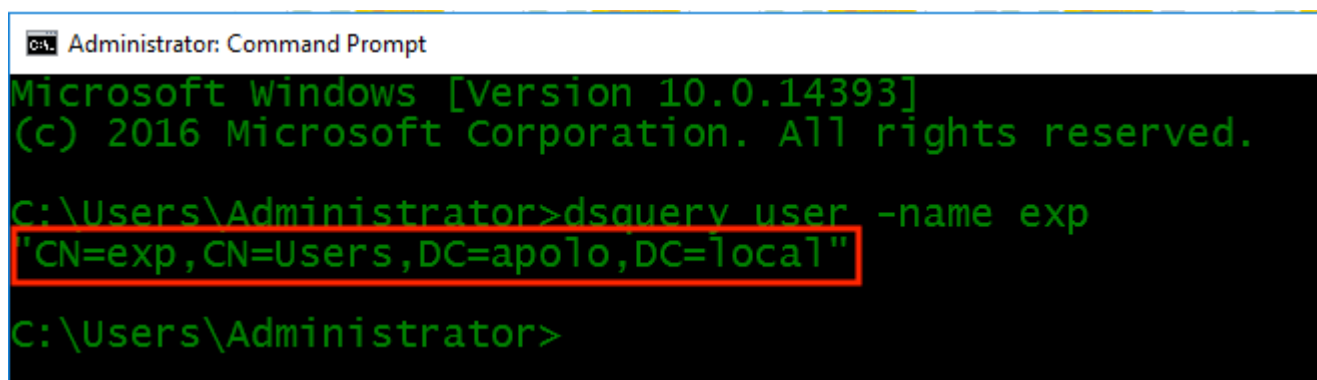
グループのベースDNが指定されていない場合は、アカウントのベースDNがグループとアカウントの両方に使用されます。

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。



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>dsquery user -name exp
'CN=exp,CN=Users,DC=apolo,DC=local'

C:\Users\Administrator>
```

## 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。

Status > System > Configuration > Applications > Users > Maintenance >

### LDAP configuration

Remote account authentication

Administrator authentication source: Both ⓘ

FindMe authentication source: Local ⓘ

LDAP server configuration

FQDN address resolution: Address record ⓘ

Host name and Domain: ad-apollo . apollo.local ⓘ

Port: 389 ⓘ

Encryption: Off ⓘ

Certificate revocation list (CRL) checking: None ⓘ

Authentication configuration

Bind DN: \* cn=exp,cn=Users,dc=apollo,dc=local ⓘ

Bind password: ..... ⓘ

SASL: None ⓘ

Bind username: exp ⓘ

Directory configuration

Base DN for accounts: \* cn=Users,dc=apollo,dc=local ⓘ

Base DN for groups: ..... ⓘ

Nested Subgroup Search Depth: \* 16 ⓘ

Skip Looking up all the Members: Yes ⓘ

Status (last updated: 15:27:47 CDT)

State: Available

## 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。

The screenshot shows the Cisco Expressway-C web interface and a Windows Active Directory console. In the Expressway interface, the 'Administrator groups' table lists 'ExpresswayAdmin' with state 'Enabled', access level 'Read-write', and web access 'Yes'. Below the table are buttons for 'New', 'Delete', 'Enable', 'Disable', 'Select all', and 'Unselect all'. The Active Directory console shows a tree view with 'Users' selected, and a list of users and groups. 'ExpresswayAdmin' is highlighted in the list, showing it is a 'Security Group - Domain Local'.

| Name            | State   | Access level | Web access |
|-----------------|---------|--------------|------------|
| ExpresswayAdmin | Enabled | Read-write   | Yes        |

| Name                                                | Type                          | Description                  |
|-----------------------------------------------------|-------------------------------|------------------------------|
| ExpresswayAdmin                                     | Security Group - Domain Local |                              |
| FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042 | User                          |                              |
| Group Policy Creator Owners                         | Security Group - Global       | Members in this group c...   |
| Guest                                               | User                          | Built-in account for gue...  |
| jabber                                              | User                          |                              |
| Jefferson Madriz                                    | User                          |                              |
| Key Admins                                          | Security Group - Global       | Members of this group ...    |
| Migration.8f3e7716-2011-43e4-96b1-aba62d229136      | User                          |                              |
| Protected Users                                     | Security Group - Global       | Members of this group ...    |
| RAS and IAS Servers                                 | Security Group - Domain Local | Servers in this group can... |

### 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。

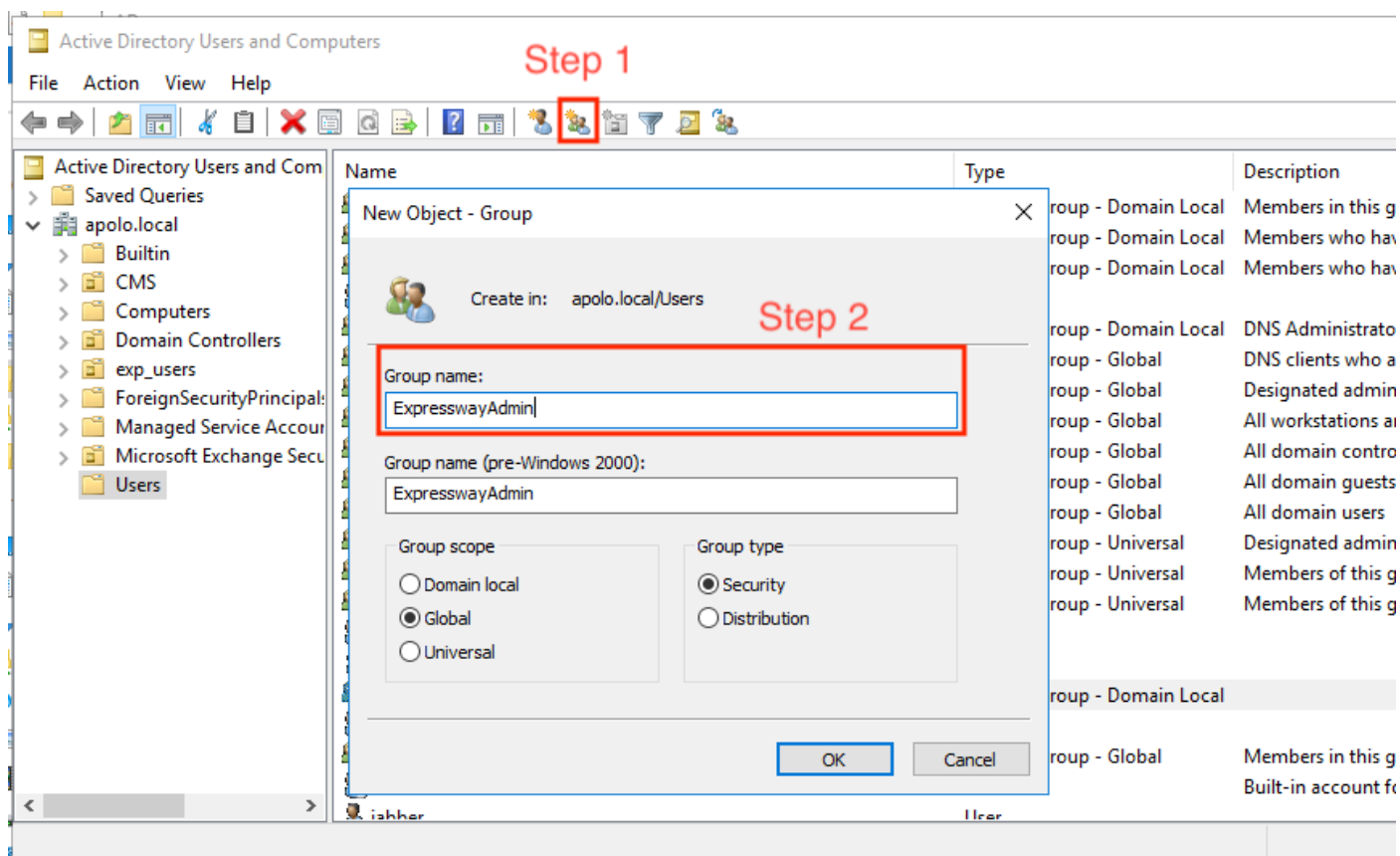
APIアクセス：このグループのメンバーがAPIを使用してシステムのステータスと設定にアクセスできるかどうかを決定します。

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。

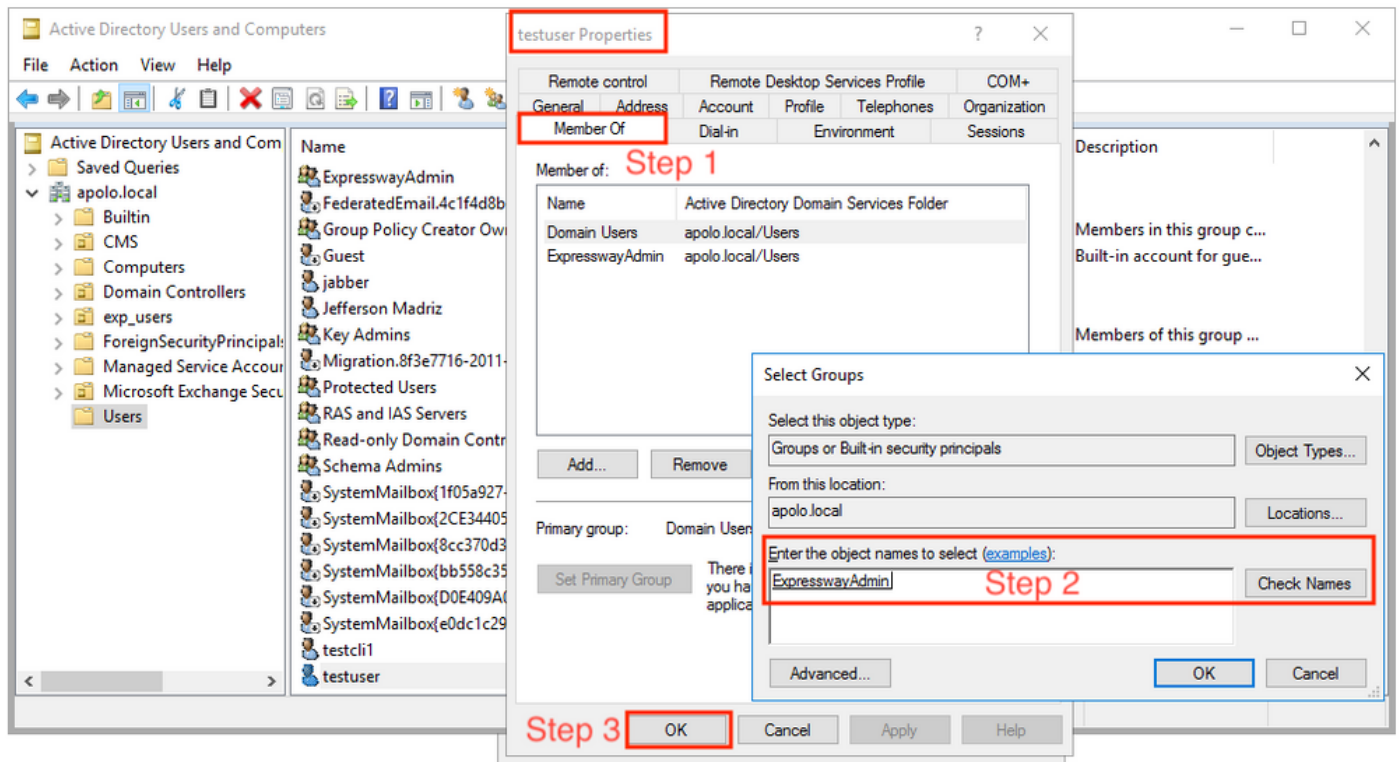
## ADでの管理者グループの設定

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。

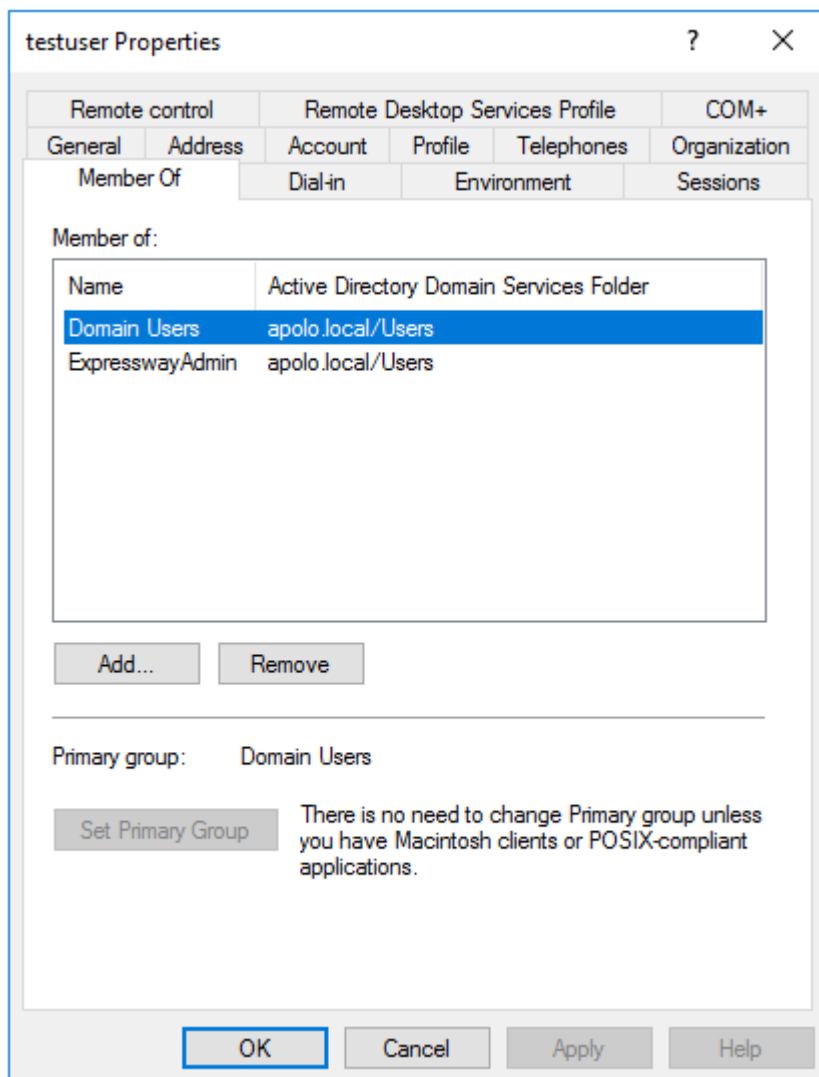


Web、API、またはCLIを介してExpresswayにアクセスする必要があるユーザに、設定したグループを割り当てます。この例では、ユーザはtestuserです。

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。

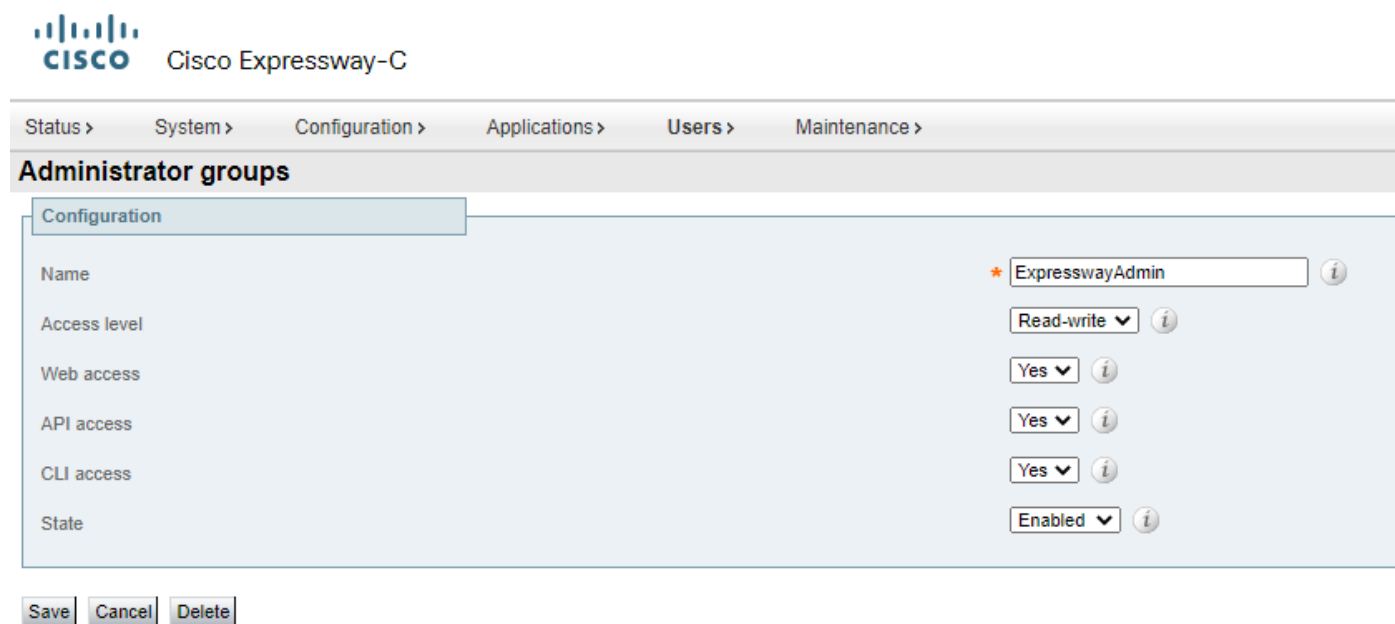


## Expresswayでの管理者グループの設定

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。



The screenshot shows the Cisco Expressway-C web interface. At the top is the Cisco logo and the text "Cisco Expressway-C". Below this is a navigation bar with tabs: Status >, System >, Configuration >, Applications >, Users >, and Maintenance >. The "Users >" tab is selected, and the page title is "Administrator groups". Under this title, there is a "Configuration" section. It contains several fields: "Name" (set to ExpresswayAdmin), "Access level" (set to Read-write), "Web access" (set to Yes), "API access" (set to Yes), "CLI access" (set to Yes), and "State" (set to Enabled). Each field has an information icon (i) to its right. At the bottom of the configuration section are three buttons: Save, Cancel, and Delete.

[Save] を選択します。

| Administrator groups                     |           |              |            |            |            |
|------------------------------------------|-----------|--------------|------------|------------|------------|
| Name                                     | State     | Access level | Web access | API access | CLI access |
| <input type="checkbox"/> ExpresswayAdmin | ✓ Enabled | Read-write   | ✓ Yes      | ✓ Yes      | ✓ Yes      |

## 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。

Administrator login

Username

testuser

Password

.....

Login

これは、Status > Event logで確認できます。

Status > System > Configuration > Applications Users > Maintenance >

Event Log

You are here: [Status](#)

Filter

Contains all of the words:

more options

Filter

Reset

Configure log settings | Download this page

1 2 3 4 5 6 ... Last | Next

Go to page 

Go

Results

2021-10-20T12:56:44.135-05:00

php: web: User="testuser" Event="Admin Session Start" Src-ip="10.15.13.30" Src-port="64705" UTCtime="2021-10-20 17:56:44"

2021-10-20T12:56:44.131-05:00

taa-chkpasswd: Event="pam" Module="pam\_unix(taa-chkpasswd-webadmin:session)" Level="INFO" Detail="session opened for user testuser by (uid=2)" UTCtime="2021-10-20 17:56:44"

## 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。