

LDAP configureren op Expressway voor toegang tot web, API en CLI

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[LDAP-configuratie](#)

[Hoe de basis DN te vinden](#)

[Voorbeeld LDAP-configuratie](#)

[Configuratie van beheerdersgroepen](#)

[Configuratieopties voor beheerdersgroepen op Expressway](#)

[Beheerdersgroepconfiguratie op AD](#)

[Beheerdersgroepconfiguratie op Expressway](#)

[Verifiëren](#)

Inleiding

In dit document worden de stappen beschreven die nodig zijn om het Lightweight Directory Access Protocol (LDAP) op de Expressway-server in te schakelen en hoe beheerdersgroepen toegang kunnen krijgen via Web, Application Programming Interface (API) en Command Line Interface (CLI) tot Expressway met uw domeingebruikers.

Bijgedragen door Jefferson Madriz en Elias Sevilla, Cisco TAC Engineers.

Voorwaarden

Vereisten

- Kennis van Expressway.
- De basisconfiguratie van de Expressway is al voltooid.
- Active Directory (AD) is al geconfigureerd.
- Firewallregels klaar, zodat er communicatie tussen Expressway en AD-server mogelijk is.

Gebruikte componenten

- Active Directory geïnstalleerd op Windows Server 2016.
- Expressway-C-server op versie X14.0.3.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

LDAP-configuratie

De LDAP-configuratiepagina Gebruikers > LDAP-configuratie wordt gebruikt om een LDAP-verbinding met een externe directoryservice te configureren voor verificatie van de beheerdersaccount.

- Externe accountverificatie: Met deze sectie kunt u het gebruik van LDAP voor externe accountverificatie in- of uitschakelen.

The screenshot shows the 'Remote account authentication' section of a configuration interface. 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.

- Alleen lokaal: referenties worden geverifieerd aan de hand van een lokale database die op het systeem is opgeslagen.
- Alleen op afstand: referenties worden geverifieerd aan de hand van een externe directory met referenties.
- Beide: referenties worden eerst geverifieerd aan de hand van een lokale database die op het systeem is opgeslagen, en als er geen overeenkomst is met de account, wordt de externe directory voor referenties gebruikt.

- LDAP-serverconfiguratie: in deze sectie worden de verbidingsgegevens voor de LDAP-server gespecificeerd.

The screenshot shows the 'LDAP server configuration' section. It includes several fields: '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 field has an information icon to its right.

FQDN-adresresolutie:

- SRV-record: opzoeken van DNS-servicerecord (SRV).
- Adresrecord: opzoeken van DNS A- of AAAA-record.
- IP-adres: rechtstreeks ingevoerd als IP-adres.

 **Opmerking:** als u SRV-records gebruikt, moet u ervoor zorgen dat _ldap._tcp.-records de standaard LDAP-poort 389 gebruiken. De snelweg ondersteunt geen andere poortnummers voor LDAP.

Hostnaam en domein:

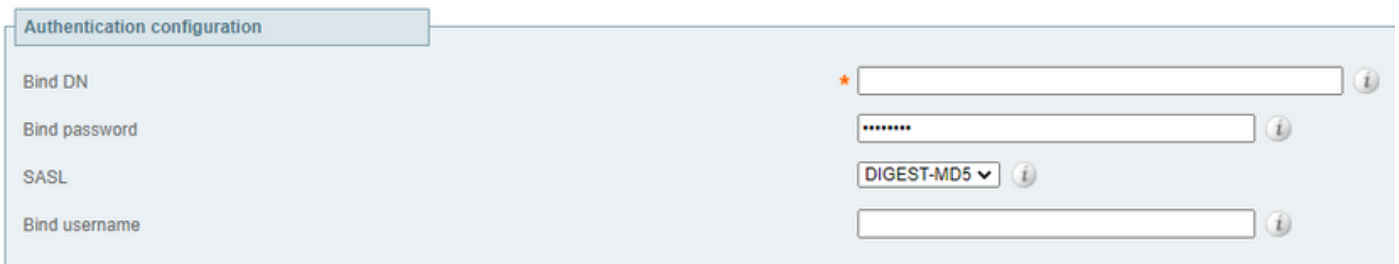
- SRV-record: alleen het domeingedeelte van het serveradres is vereist.
- Adresrecord: voer de hostnaam en het domein in. Deze worden vervolgens gecombineerd om het volledige serveradres voor het opzoeken van het DNS-adresrecord op te geven.
- IP-adres: het serveradres wordt rechtstreeks als IP-adres ingevoerd.

Port:

- De IP-poort die op de LDAP-server moet worden gebruikt.

Codering:

- TLS: maakt gebruik van Transport Layer Security (TLS)-codering voor de verbinding met de LDAP-server.
- Uit: er wordt geen encryptie gebruikt.
- Verificatieconfiguratie: in deze sectie worden de verificatiereferenties van de Expressway opgegeven die moeten worden gebruikt om te binden aan de LDAP-server.



Bind DN: De Distinguished Name (DN), hoofdletterongevoelig, wordt door de Expressway gebruikt om te binden aan de LDAP-server. Het is belangrijk om de DN op te geven in de volgorde cn=, dan ou=, dan dc=

 **Opmerking:** Het bindingsaccount is meestal een alleen-lezen account zonder speciale privileges.

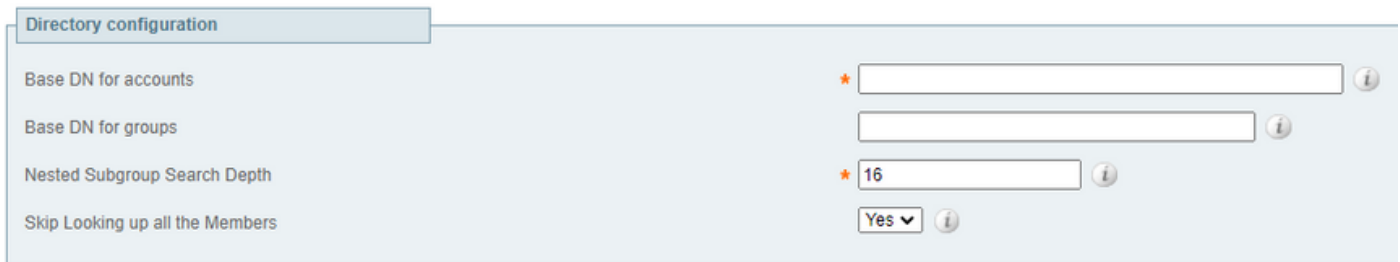
Bindingswachtwoord: Het wachtwoord (hoofdlettergevoelig) dat door de Expressway wordt gebruikt om te binden aan de LDAP-server.

SASL: Het SASL-mechanisme (Simple Authentication and Security Layer) dat u kunt gebruiken om te binden aan de LDAP-server

- Geen: er wordt geen mechanisme gebruikt.
- DIGEST-MD5: het DIGEST-MD5-mechanisme wordt gebruikt.

Bind gebruikersnaam: Gebruikersnaam van het account dat de Expressway gebruikt om in te loggen op de LDAP-server (hoofdlettergevoelig).

- Directoryconfiguratie: In deze sectie worden de basis-namen opgegeven die moeten worden gebruikt voor het zoeken naar account- en groepsnamen.



The screenshot shows a 'Directory configuration' window with the following fields:

- Base DN for accounts:** A text input field with a red asterisk and an information icon.
- Base DN for groups:** A text input field with an information icon.
- Nested Subgroup Search Depth:** A numeric input field with a red asterisk, containing the value '16', and an information icon.
- Skip Looking up all the Members:** A dropdown menu currently set to 'Yes' and an information icon.

Basis-DN voor accounts: de definitie van de Organizational Unit (OU) en Domain Controller (DC) van de Distinguished Name waarbij een zoekopdracht naar gebruikersaccounts begint in de databasestructuur (hoofdletterongevoelig).

De basis-DN voor accounts en groepen moet op of onder het DC-niveau liggen (neem indien nodig alle dc= waarden en ou= waarden op). LDAP-authenticatie kijkt niet naar sub-DC-accounts, alleen lagere OU- en Common Name (CN)-niveaus.

Basis-DN voor groepen: de OU- en DC-definitie van de Distinguished Name waarbij in de databasestructuur moet worden gezocht naar groepen (hoofdletterongevoelig).

Als er geen basis-DN voor groepen is opgegeven, wordt de basis-DN voor accounts gebruikt voor zowel groepen als accounts.

Geneste subgroepzoekdiepte: Wordt gebruikt om de diepte van groepen voor de LDAP-zoekopdracht te beperken.

Alle leden niet opzoeken: Wordt gebruikt om het opzoeken van leden van een beheerdersgroep uit te schakelen of in te schakelen terwijl het verificatieproces wordt uitgevoerd. De standaard is Ja - sla het opzoeken van het lid over.

Hoe de basis DN te vinden

Open op een AD-server de opdrachtprompt (CMD) als beheerder en voer de opdracht: **dsquery user -name** uit.

```
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>
```

Voorbeeld LDAP-configuratie

De bron voor de verificatie van de beheerder is ingesteld op Both en SASL is ingesteld op None in dit voorbeeld.

The screenshot shows the Cisco Expressway-C configuration interface. The top navigation bar includes Status, System, Configuration, Applications, Users, and Maintenance. The main section is titled 'LDAP configuration' and is divided into four tabs: Remote account authentication, LDAP server configuration, Authentication configuration, and Directory configuration. The 'Remote account authentication' tab is active, showing 'Administrator authentication source' set to 'Both' and 'FindMe authentication source' set to 'Local'. The 'LDAP server configuration' tab is also visible, showing 'FQDN address resolution' set to 'Address record', 'Host name and Domain' set to 'ad-apolo.apolo.local', 'Port' set to '389', 'Encryption' set to 'Off', and 'Certificate revocation list (CRL) checking' set to 'None'. The 'Authentication configuration' tab is active, showing 'Bind DN' set to 'cn=exp,cn=Users,dc=apolo,dc=local', 'Bind password' set to '*****', 'SASL' set to 'None', and 'Bind username' set to 'exp'. The 'Directory configuration' tab is also visible, showing 'Base DN for accounts' set to 'cn=Users,dc=apolo,dc=local', 'Base DN for groups' set to an empty field, 'Nested Subgroup Search Depth' set to '16', and 'Skip Looking up all the Members' set to 'Yes'. A 'Save' button is located at the bottom left. The status bar at the bottom indicates 'Status (last updated: 15:27:47 CDT)' and 'State Available'.

LDAP-status verifiëren

De verbindingstatus van de LDAP-server valideren:

- Beschikbaar: er worden geen foutmeldingen weergegeven
- Mislukt: er worden foutmeldingen weergegeven. [LDAP-foutberichten](#)

Configuratie van beheerdersgroepen

De pagina Beheerdersgroepen Gebruikers > Beheerdersgroepen geeft alle beheerdersgroepen weer die op de snelweg zijn geconfigureerd en laat u groepen toevoegen, bewerken en verwijderen.

 Opmerking: beheerdersgroepen zijn alleen van toepassing als Externe accountverificatie met LDAP is ingeschakeld.

Wanneer u zich aanmeldt bij de Expressway-webinterface, worden uw referenties geverifieerd aan de hand van de externe directoryservice en krijgt u de toegangsrechten toegewezen die zijn gekoppeld aan de groep waartoe u behoort.

Configuratieopties voor beheerdersgroepen op Expressway

Naam: De naam van de beheerdersgroep. De groepsnamen die in de Expressway zijn gedefinieerd, moeten overeenkomen met de groepsnamen die in de externe directoryservice zijn ingesteld om de beheerderstoegang tot deze Expressway te beheren.

 Cisco Expressway-C

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

Administrator groups

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

New Delete Enable Disable Select all Unselect all

Active Directory Users and Computers

File Action View Help

Active Directory Users and Com

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...

Toegangsniveau:

- Read-write: Hiermee kunnen alle configuratiegegevens worden bekeken en gewijzigd. Dit biedt dezelfde rechten als de standaard beheerdersaccount.
- Alleen-lezen: hiermee kunnen status- en configuratiegegevens alleen worden bekeken en niet worden gewijzigd. Sommige pagina's, zoals de Upgrade-pagina, zijn geblokkeerd voor alleen-lezen accounts.
- Auditor: geeft alleen toegang tot het eventlog, configuratielog, netwerklog, alarmen en overzichtspagina's.

- Geen: geen toegang toegestaan

Webtoegang: Bepaalt of leden van deze groep met de webinterface op het systeem mogen inloggen.

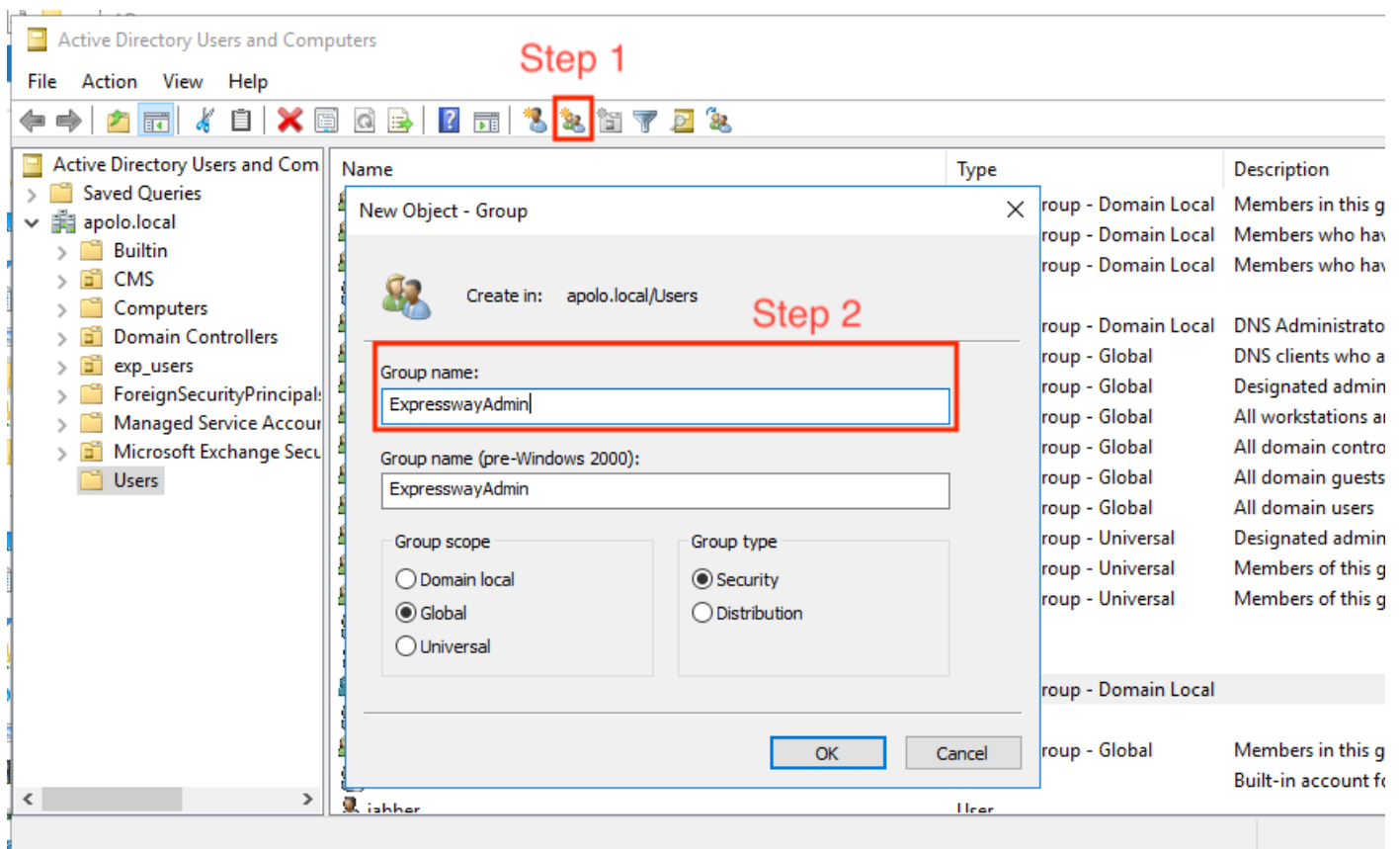
API-toegang: Bepaalt of leden van deze groep toegang hebben tot de status en configuratie van het systeem met de API.

CLI-toegang: Bepaalt of leden van deze groep toegang hebben tot het systeem via CLI.

Status: Geeft aan of de groep is ingeschakeld of uitgeschakeld.

Beheerdersgroepconfiguratie op AD

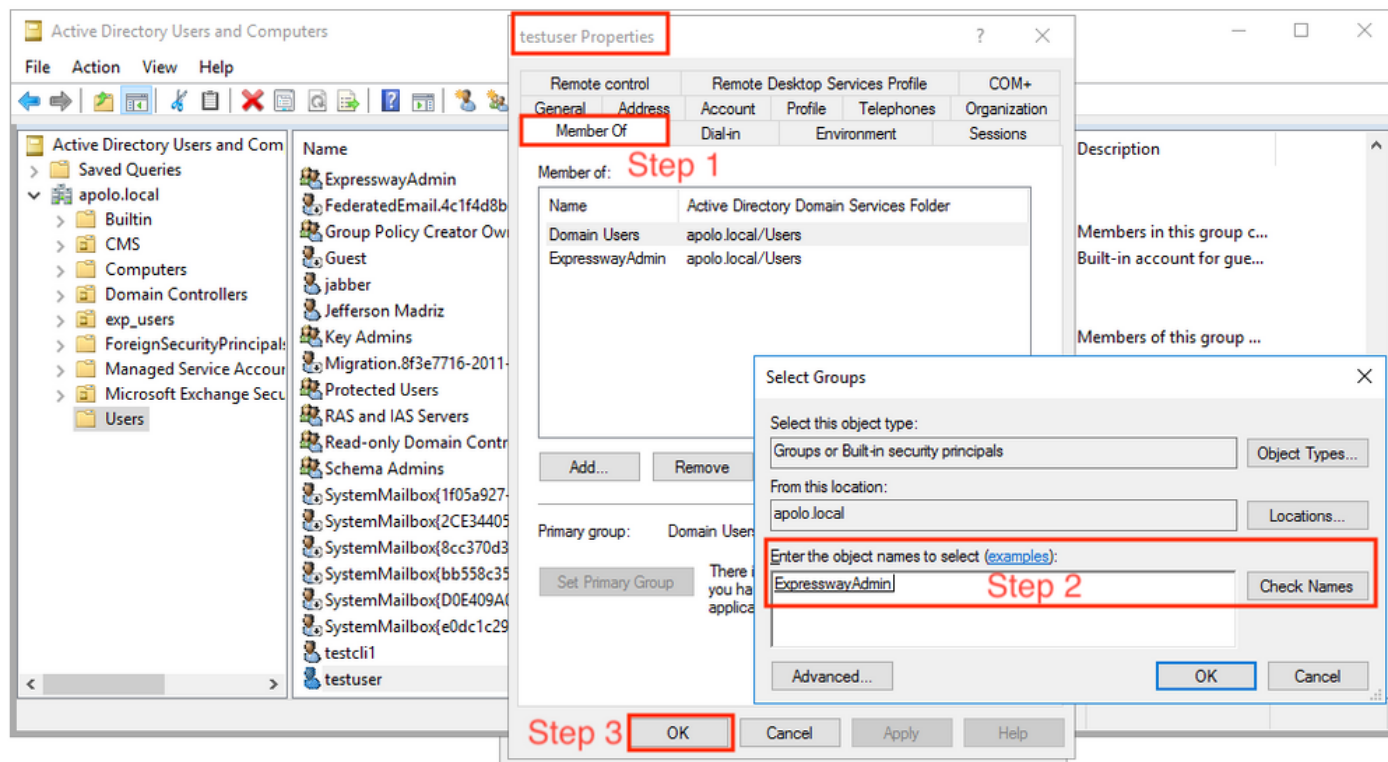
1. Maak een nieuwe objectgroep, in de map die u wilt opslaan van de gebruikers.
2. Wijs een naam toe aan de groepsnaam.



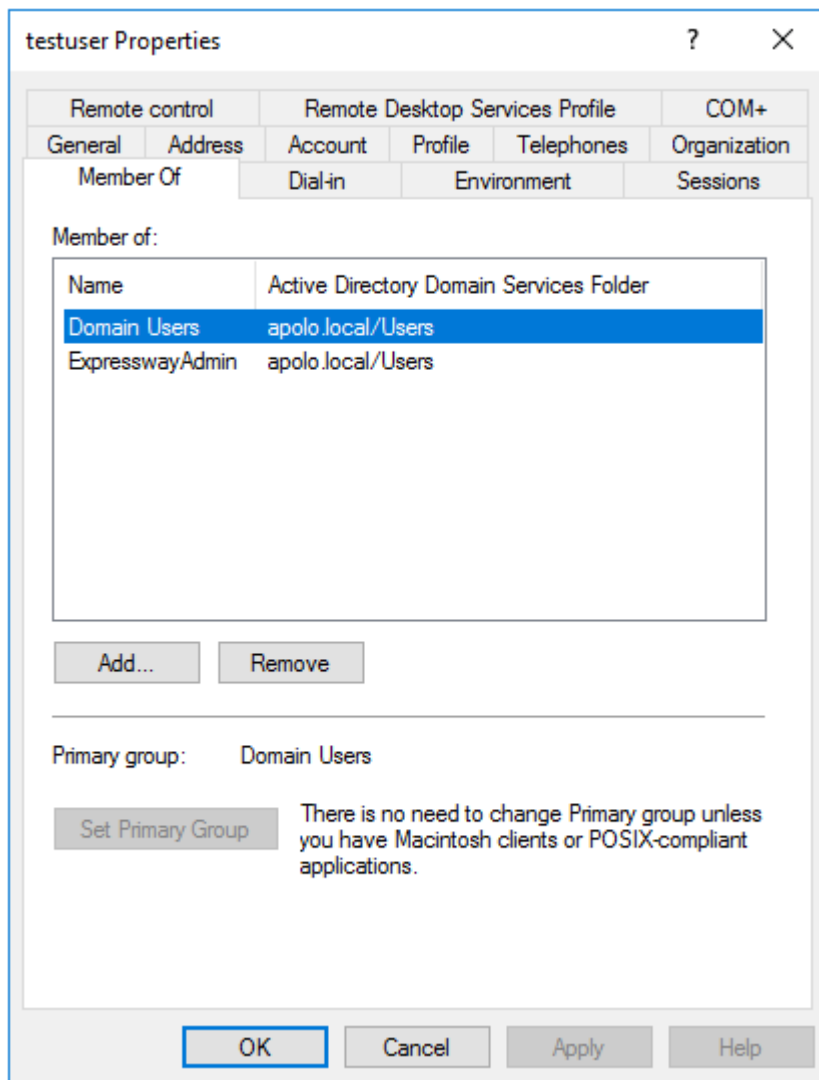
Wijs de groep die is geconfigureerd toe aan de gebruiker of gebruikers die toegang moeten krijgen tot Expressways via Web, API of CLI. In dit geval is de gebruiker een testgebruiker.

1. Open de gebruikerseigenschappen, ga naar het tabblad Lid van, selecteer Toevoegen
2. Zoek naar de eerder gemaakte groepsnaam.

3. Selecteer vervolgens OK.



Op dit moment is de gebruiker lid van Domeingebruikers en ExpresswayAdmin.



Beheerdersgroepconfiguratie op Expressway

Zodra de configuratie is voltooid, navigeert u op Expressway naar Gebruikers > Beheerdersgroepen, selecteert u Nieuw

Naam: moet overeenkomen met groepsnaam en configureren gekoppeld aan de LDAP-gebruiker die toegang moet krijgen tot de snelweg. In dit voorbeeld is de groepsnaam ExpresswayAdmin, dus de nieuwe naam van de beheerdersgroep is ExpresswayAdmin.

Deze groep heeft alle rechten en toegang beschikbaar.

[Status >](#) [System >](#) [Configuration >](#) [Applications >](#) [Users >](#) [Maintenance >](#)**Administrator groups****Configuration**

Name

* ExpresswayAdmin

Access level

Read-write

Web access

Yes

API access

Yes

CLI access

Yes

State

Enabled

Selecteer Opslaan.

Administrator groups

Name	State	Access level	Web access	API access	CLI access
☐ ExpresswayAdmin	✓ Enabled	Read-write	✓ Yes	✓ Yes	✓ Yes

Verifiëren

Log uit en probeer toegang te krijgen via het web met de LDAP-gebruiker waaraan de beheerdersgroep is gekoppeld. In dit voorbeeld is de aangemaakte gebruiker testgebruiker.

Administrator login

Username

testuser

Password

••••••••

Dit kan worden bevestigd via Status > Eventlogboek:

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"

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.