

Expressway에서 웹, API 및 CLI 액세스를 위한 LDAP 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[LDAP 컨피그레이션](#)

[기본 DN을 찾는 방법](#)

[LDAP 컨피그레이션 예](#)

[관리자 그룹 컨피그레이션](#)

[Expressway의 관리자 그룹 컨피그레이션 옵션](#)

[AD의 관리자 그룹 컨피그레이션](#)

[Expressway의 관리자 그룹 컨피그레이션](#)

[다음을 확인합니다.](#)

소개

이 문서에서는 Expressway 서버에서 LDAP(Lightweight Directory Access Protocol)를 활성화하는 데 필요한 단계와 관리자 그룹이 도메인 사용자와 함께 웹, API(Application Programming Interface) 및 CLI(Command Line Interface)를 통해 Expressway에 액세스하는 방법에 대해 설명합니다.

기고자: Jefferson Madriz 및 Elias Sevilla, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

- Expressway에 대한 기본 지식
- Expressway 기본 컨피그레이션이 이미 완료되었습니다.
- AD(Active Directory)가 이미 구성되었습니다.
- Expressway와 AD 서버 간의 통신을 허용하는 방화벽 규칙이 준비되었습니다.

사용되는 구성 요소

- Windows Server 2016에 Active Directory가 설치되었습니다.
- 버전 X14.0.3의 Expressway-C 서버.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

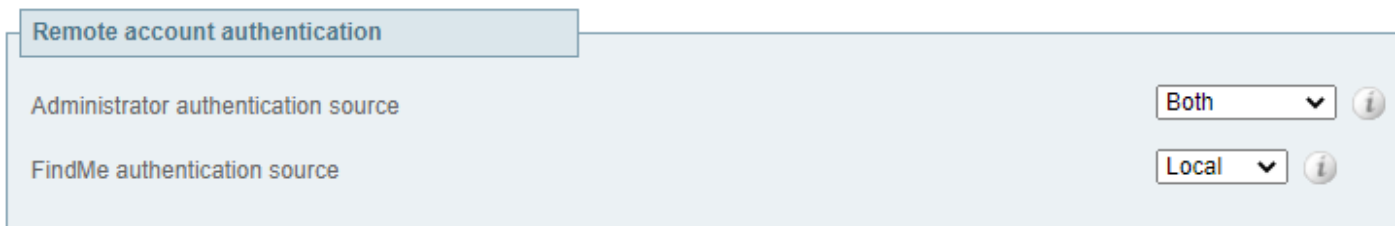
이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

LDAP 컨피그레이션

LDAP configuration(LDAP 컨피그레이션) 페이지 Users(사용자) > LDAP configuration(LDAP 컨피그레이션)은 관리자 계정 인증을 위해 원격 디렉토리 서비스에 대한 LDAP 연결을 구성하는 데 사용됩니다.

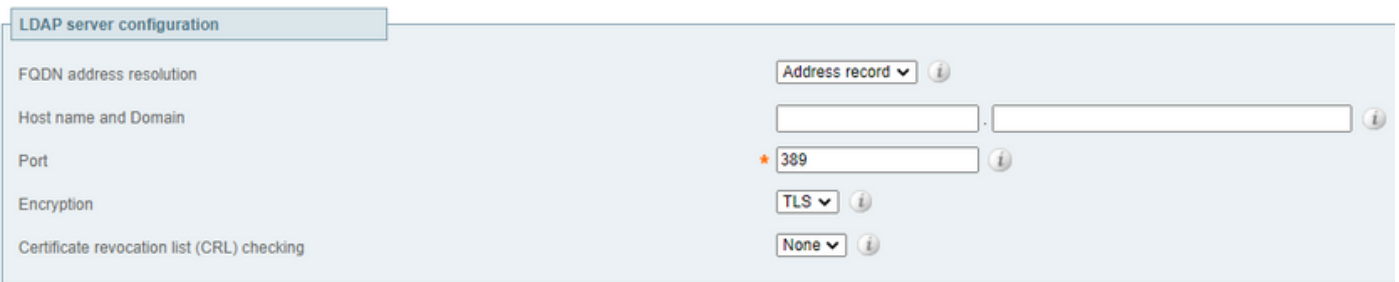
- 원격 계정 인증: 이 섹션에서는 원격 계정 인증에 LDAP를 사용하거나 사용하지 않도록 설정할 수 있습니다.



The image 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.

- 로컬 전용: 자격 증명은 시스템에 저장된 로컬 데이터베이스에 대해 검증됩니다.
- 원격 전용: 자격 증명은 외부 자격 증명 디렉토리에서 확인됩니다.
- 둘 다 자격 증명은 시스템에 저장된 로컬 데이터베이스에 대해 먼저 확인되며, 계정과 일치하지 않는 경우 외부 자격 증명 디렉토리가 대신 사용됩니다.

- LDAP 서버 구성: 이 섹션에서는 LDAP 서버에 대한 연결 세부 정보를 지정합니다.



The image shows the 'LDAP server configuration' section. It includes 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 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 주소 확인:

- SRV 레코드: DNS(Domain Name Service) 서비스 레코드(SRV) 조회
- 주소 레코드: DNS A 또는 AAAA 레코드 조회.
- IP 주소: IP 주소로 직접 입력했습니다.



참고: SRV 레코드를 사용하는 경우 _ldap._tcp를 확인합니다. 레코드는 표준 LDAP 포트 389를 사용합니다. Expressway는 LDAP에 대해 다른 포트 번호를 지원하지 않습니다.

호스트 이름 및 도메인:

- SRV 레코드: 서버 주소의 Domain 부분만 필요합니다.

- 주소 레코드: 호스트 이름 및 도메인을 입력합니다. 그런 다음 DNS 주소 레코드 조회를 위한 전체 서버 주소를 제공하기 위해 이들을 결합합니다.
- IP 주소: 서버 주소는 IP 주소로 직접 입력됩니다.

포트:

- LDAP 서버에서 사용할 IP 포트.

암호화:

- TLS: 여기서는 LDAP 서버 연결에 TLS(Transport Layer Security) 암호화를 사용합니다.
- 끄기: 암호화가 사용되지 않습니다.
- 인증 구성: 이 섹션에서는 LDAP 서버에 바인딩하는 데 사용할 Expressway의 인증 자격 증명을 지정합니다.

The screenshot shows the 'Authentication configuration' section. It contains four fields: 'Bind DN' with a red asterisk, 'Bind password' with masked characters, 'SASL' with a dropdown menu set to 'DIGEST-MD5', and 'Bind username'. Each field has an information icon (i) to its right.

바인드 DN: 대/소문자를 구분하지 않는 DN(Distinguished Name). Expressway에서 LDAP 서버에 바인딩하는 데 사용됩니다. cn=, ou=, dc= 순서로 DN을 지정하는 것이 중요합니다



참고: 바인드 계정은 일반적으로 특별한 권한이 없는 읽기 전용 계정입니다.

바인딩 암호: Expressway에서 LDAP 서버에 바인딩하기 위해 사용하는 비밀번호(대/소문자 구분).

SASL: LDAP 서버에 바인딩하는 데 사용할 SASL(Simple Authentication and Security Layer) 메커니즘

- None: 메커니즘이 사용되지 않습니다.
- 다이제스트-MD5: digest-MD5 메커니즘이 사용됩니다.

바인드 사용자 이름: Expressway에서 LDAP 서버에 로그인하는 데 사용하는 계정의 사용자 이름입니다(대/소문자 구분).

- 디렉터리 구성: 이 섹션에서는 계정 및 그룹 이름을 검색하는 데 사용할 기본 고유 이름을 지정합니다.

The screenshot shows the 'Directory configuration' section. It contains four fields: 'Base DN for accounts' with a red asterisk, 'Base DN for groups', 'Nested Subgroup Search Depth' with a value of 16, and 'Skip Looking up all the Members' with a dropdown menu set to 'Yes'. Each field has an information icon (i) to its right.

어카운트의 기본 DN: 데이터베이스 구조에서 사용자 어카운트 검색이 시작되는 DN의 OU(Organizational Unit) 및 DC(Domain Controller) 정의입니다(대/소문자 구분 안 함).

어카운트 및 그룹의 기본 DN은 DC 레벨 이하여야 합니다(필요한 경우 모든 dc= 값 및 ou= 값 포함). LDAP 인증은 하위 DC 계정을 고려하지 않으며 OU 및 CN(Common Name) 레벨만 낮춥니다.

그룹의 기본 DN: 데이터베이스 구조에서 그룹을 검색해야 하는 DN의 OU 및 DC 정의입니다(대/소문자 구분 안 함).

그룹에 대한 Base DN을 지정하지 않으면 Base DN for accounts가 그룹 및 어카운트 모두에 사용됩니다.

중첩된 하위 그룹 검색 깊이: LDAP 검색을 위한 그룹 깊이를 제한하는 데 사용됩니다.

모든 구성원 조회 건너뛰기: 인증 검색 프로세스가 진행되는 동안 관리자 그룹의 구성원 조회를 비활성화하거나 활성화하는 데 사용됩니다. 기본값은 Yes - 멤버 조회를 건너뜁니다.

기본 DN을 찾는 방법

AD 서버에서 관리자로 명령 프롬프트(CMD)를 열고 다음 명령을 실행합니다. **dsquery user -name**

```
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 컨피그레이션 예

이 예에서는 관리자 인증 소스가 Both로 설정되고 SASL이 None으로 설정됩니다.



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 ⓘ

Save

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

State Available

LDAP 상태 확인

LDAP 서버 연결 상태를 확인합니다.

- 사용 가능: 오류 메시지가 표시되지 않음
- 실패: 오류 메시지가 표시됩니다. [LDAP 오류 메시지](#)

관리자 그룹 컨피그레이션

Administrator groups(관리자 그룹) 페이지 Users(사용자) > Administrator groups(관리자 그룹)에는 Expressway에 구성된 모든 관리자 그룹이 나열되며, 이를 통해 그룹을 추가, 편집 및 삭제할 수 있습니다.

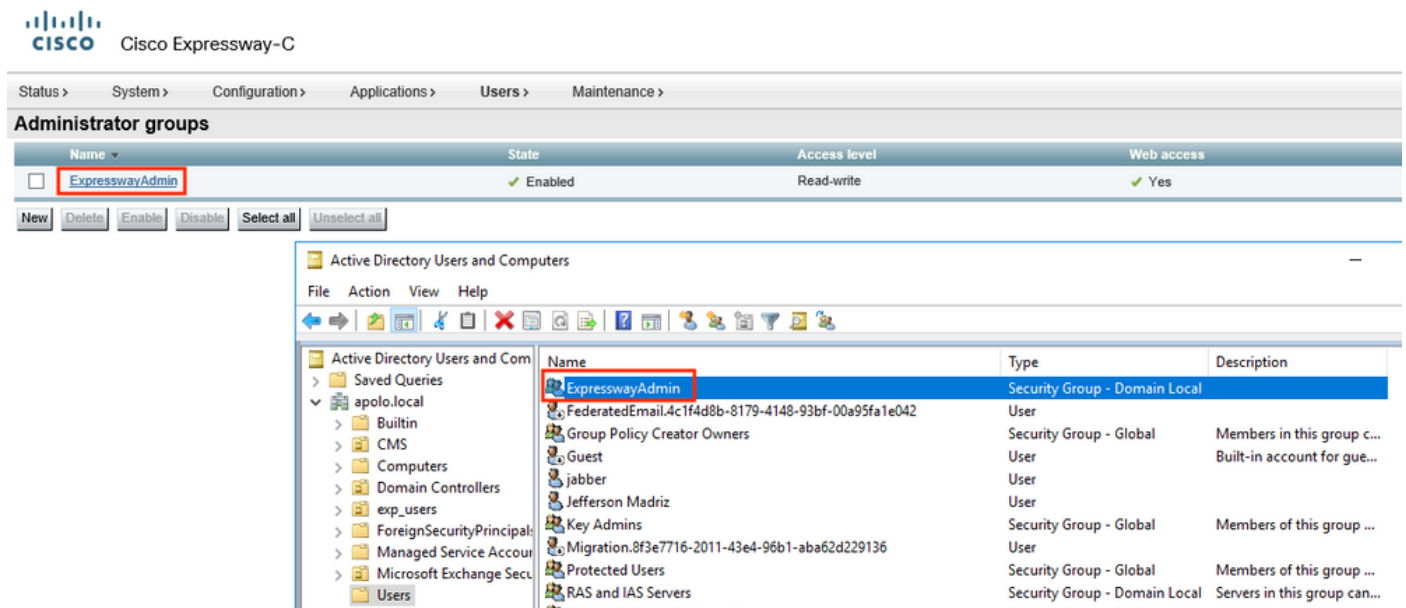


참고: 관리자 그룹은 LDAP를 사용하는 원격 계정 인증이 활성화된 경우에만 적용됩니다.

Expressway 웹 인터페이스에 로그인하면 자격 증명이 원격 디렉터리 서비스에 대해 인증되고 사용자가 속한 그룹과 연결된 액세스 권한이 할당됩니다.

Expressway의 관리자 그룹 컨피그레이션 옵션

이름: 관리자 그룹의 이름입니다. Expressway에 정의된 그룹 이름은 이 Expressway에 대한 관리자 액세스를 관리하기 위해 원격 디렉터리 서비스에 설정된 그룹 이름과 일치해야 합니다.



The image shows the Cisco Expressway-C web interface and a Windows Active Directory Users and Computers window. In the Expressway interface, the 'Administrator groups' table shows a group named 'ExpresswayAdmin' with state 'Enabled', access level 'Read-write', and web access 'Yes'. In the Active Directory window, the 'ExpresswayAdmin' group 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...

액세스 수준:

- 읽기/쓰기: 모든 컨피그레이션 정보를 보고 변경할 수 있습니다. 기본 관리자 계정과 동일한 권한을 제공합니다.
- 읽기 전용: 상태 및 컨피그레이션 정보를 볼 수만 있고 변경할 수는 없습니다. Upgrade(업그레이드) 페이지와 같은 일부 페이지는 읽기 전용 계정으로 차단됩니다.
- 감사: Event Log(이벤트 로그), Configuration Log(컨피그레이션 로그), Network Log(네트워크 로그), Alarms(경보) 및 Overview(개요) 페이지에만 액세스할 수 있습니다.
- None: 액세스가 허용되지 않음

웹 액세스: 이 그룹의 구성원이 웹 인터페이스를 사용하여 시스템에 로그인할 수 있는지 여부를 결정합니다.

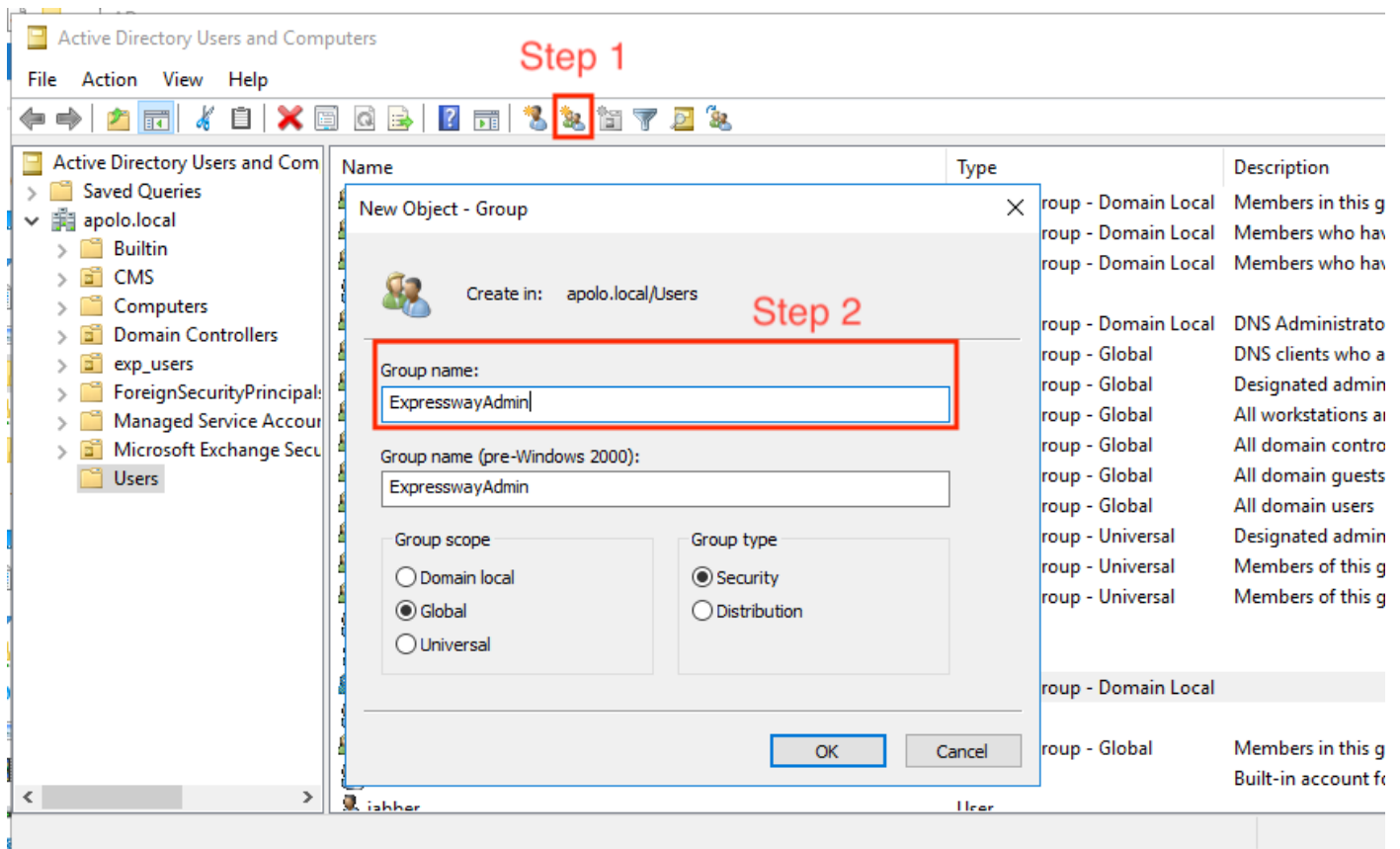
API 액세스: 이 그룹의 구성원이 API를 사용하여 시스템의 상태 및 구성에 액세스할 수 있는지 여부를 결정합니다.

CLI 액세스: 이 그룹의 구성원이 CLI를 통해 시스템에 액세스할 수 있는지 여부를 결정합니다.

상태: 그룹이 활성화되었는지 또는 비활성화되었는지를 나타냅니다.

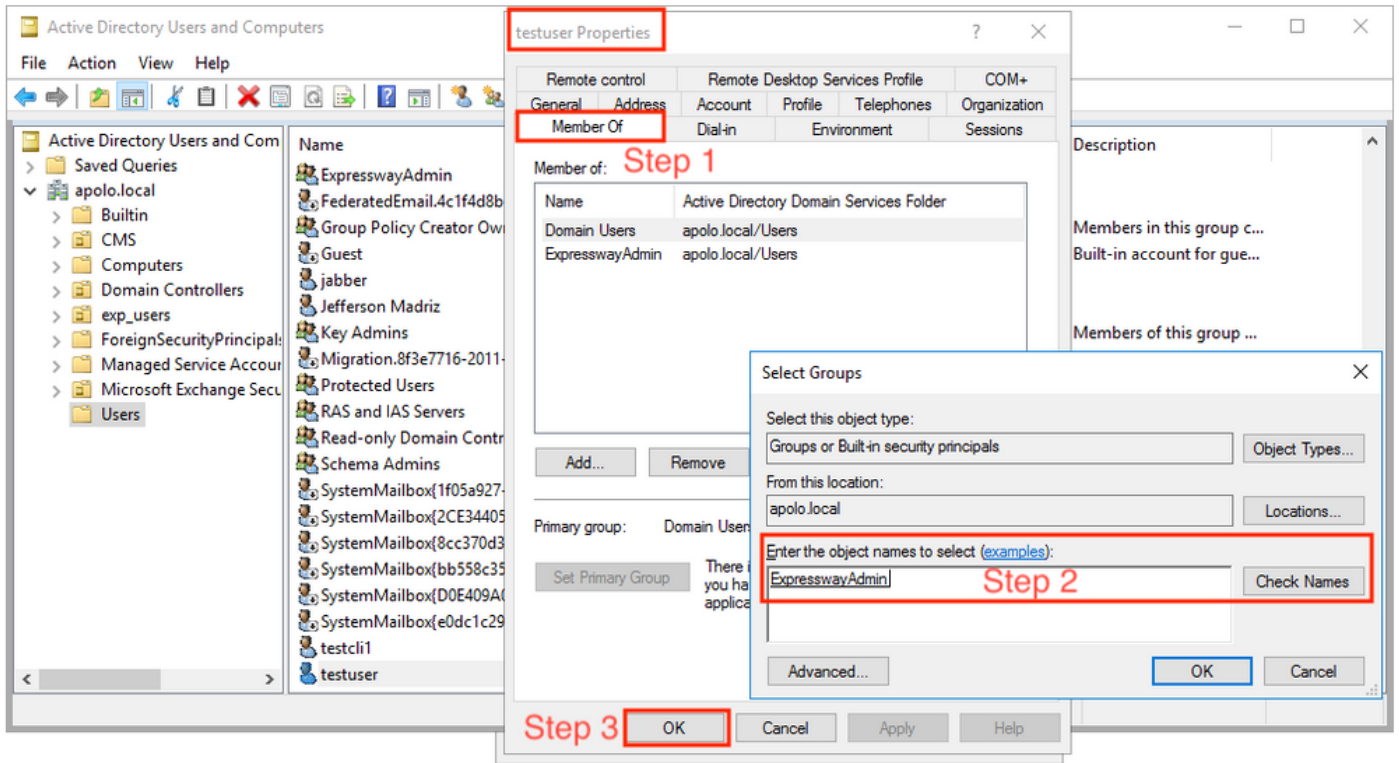
AD의 관리자 그룹 컨피그레이션

1. 사용자를 저장할 폴더에 새 객체 그룹을 생성합니다.
2. 그룹명을 지정합니다.

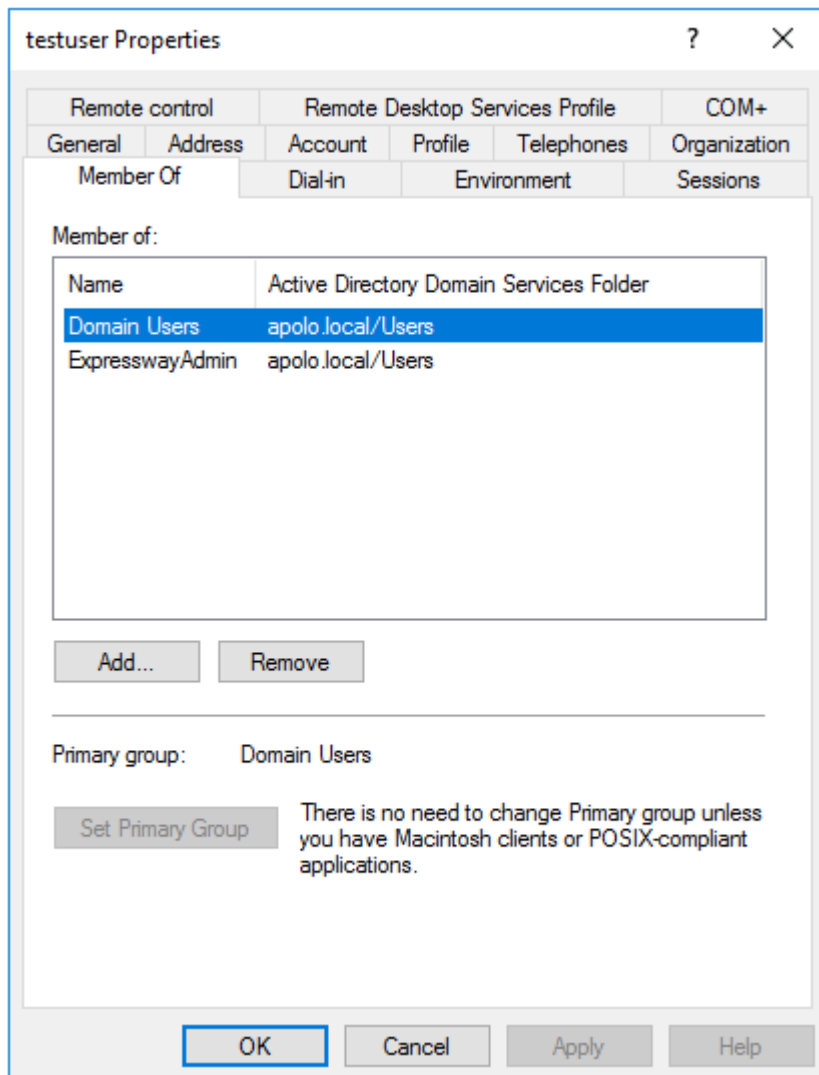


웹, API 또는 CLI를 통해 Expressway에 액세스해야 하는 사용자에게 구성된 그룹을 할당합니다. 이 경우 사용자는 testuser입니다.

1. 사용자 등록 정보를 열고 구성원 탭으로 이동한 다음 추가를 선택합니다
2. 이전에 생성된 그룹명을 검색합니다.
3. 그런 다음 확인을 선택합니다.



이 시점에서 사용자는 Domain Users 및 ExpresswayAdmin의 멤버입니다.

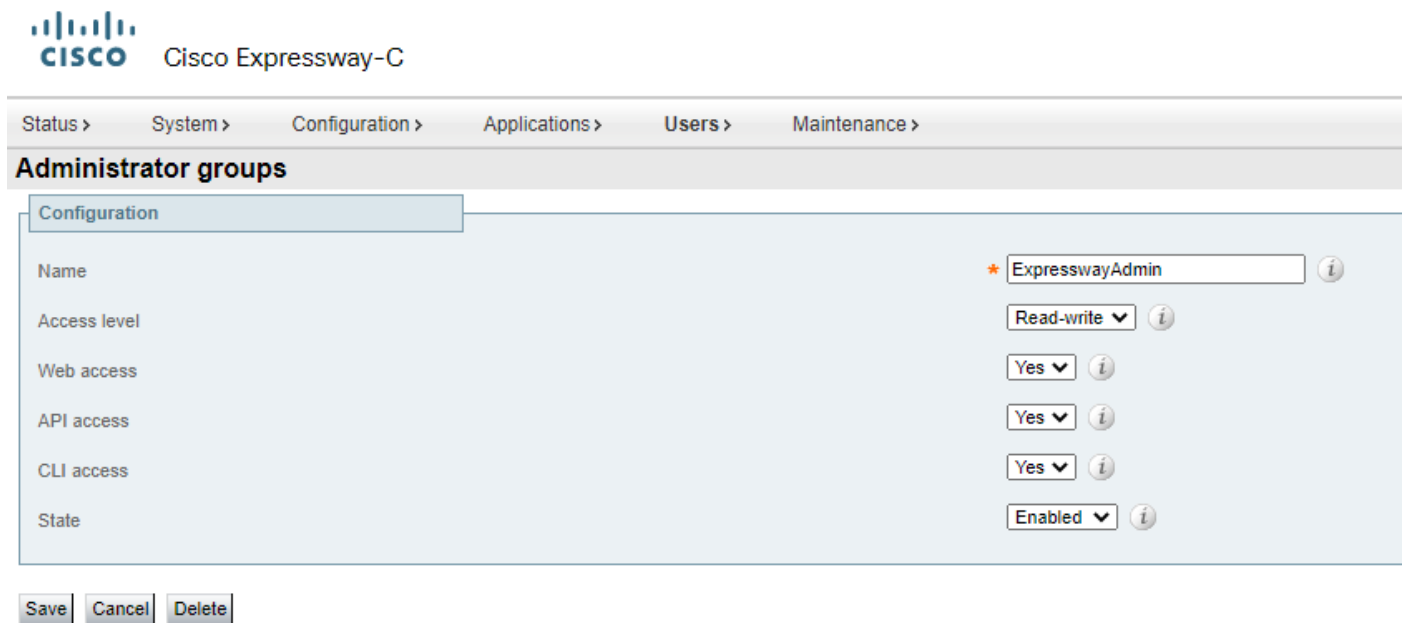


Expressway의 관리자 그룹 컨피그레이션

컨피그레이션이 완료되면 Expressway에서 Users(사용자) > Administrator groups(관리자 그룹)로 이동하고 New(새로 만들기)를 선택합니다

Name(이름): Expressway에 액세스해야 하는 LDAP 사용자가 구성되고 연결된 그룹 이름과 일치해야 합니다. 이 예에서 그룹 이름은 ExpresswayAdmin이므로 새 관리자 그룹 이름은 ExpresswayAdmin입니다.

이 그룹에는 사용 가능한 모든 권한 및 액세스 권한이 있습니다.



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 "Administrator groups" page is displayed. On the left, there is a "Configuration" tab. The main area contains a form for configuring the "ExpresswayAdmin" group. The form fields are: Name (text box with "ExpresswayAdmin"), Access level (dropdown menu with "Read-write"), Web access (dropdown menu with "Yes"), API access (dropdown menu with "Yes"), CLI access (dropdown menu with "Yes"), and State (dropdown menu with "Enabled"). Each dropdown menu has an information icon (i) to its right. At the bottom of the form are three buttons: Save, Cancel, and Delete.

저장을 선택합니다.

Administrator groups					
Name ▾	State	Access level	Web access	API access	CLI access
☐ ExpresswayAdmin	✔ Enabled	Read-write	✔ Yes	✔ Yes	✔ Yes

다음을 확인합니다.

로그아웃하고 관리자 그룹이 연결된 LDAP 사용자로 웹을 통해 액세스를 시도합니다. 이 예에서 사용자가 생성한 것은 testuser입니다.

Administrator login

Username

testuser

Password

.....

Login

이는 Status(상태) > Event log(이벤트 로그)를 통해 확인할 수 있습니다.

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"

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.