LDAP auf Expressway für Web-, API- und CLI-Zugriff konfigurieren

Inhalt

Einleitung

In diesem Dokument werden die erforderlichen Schritte zum Aktivieren des Lightweight Directory Access Protocol (LDAP) auf dem Expressway-Server und zum Aktivieren von Administratorgruppen für den Zugriff auf Expressway für Domänenbenutzer über das Web, die API (Application Programming Interface) und die CLI (Command Line Interface) beschrieben.

Beitrag von Jefferson Madriz und Elias Sevilla, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

- Grundkenntnisse auf Expressway.
- Expressway-Basiskonfiguration bereits abgeschlossen.
- Active Directory (AD) ist bereits konfiguriert.
- Firewall-Regeln bereit, um die Kommunikation zwischen Expressway und AD-Server zu ermöglichen.

Verwendete Komponenten

- Active Directory wurde auf Windows Server 2016 installiert.
- Expressway-C Server auf Version X14.0.3.

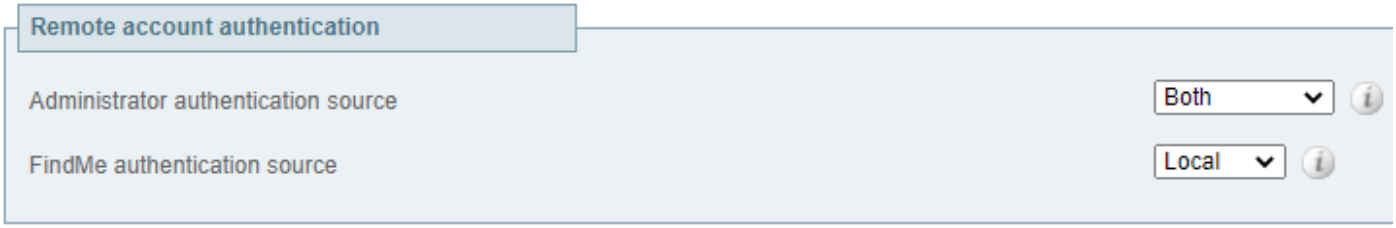
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

LDAP-Konfiguration

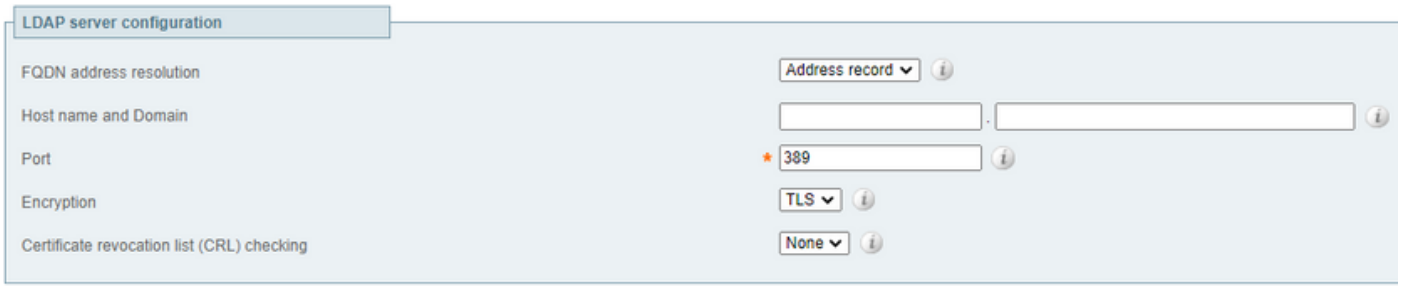
Die LDAP-Konfigurationsseite Benutzer > LDAP-Konfiguration wird verwendet, um eine LDAP-Verbindung mit einem Remote-Verzeichnisdienst für die Administrator-Kontoauthentifizierung zu konfigurieren.

- Remote-Kontoauthentifizierung: In diesem Abschnitt können Sie die Verwendung von LDAP für die Remote-Kontoauthentifizierung aktivieren oder deaktivieren.



- Nur lokal: Die Anmeldeinformationen werden mit einer lokalen Datenbank abgeglichen, die auf dem System gespeichert ist.
- Nur Remote: Die Anmeldeinformationen werden anhand eines externen Anmeldeinformationsverzeichnisses überprüft.
- Beides: Die Anmeldeinformationen werden zuerst mit einer lokalen Datenbank überprüft, die auf dem System gespeichert ist. Wenn keine Übereinstimmung mit dem Konto besteht, wird stattdessen das Verzeichnis der externen Anmeldeinformationen verwendet.

- LDAP-Serverkonfiguration: In diesem Abschnitt werden die Verbindungsdetails zum LDAP-Server angegeben.



Auflösung der FQDN-Adressen:

- SRV-Eintrag: Domain Name Service (DNS) Service Record (SRV)-Suche.
- Adressdatensatz: Suche nach DNS-A- oder AAAA-Datensätzen.
- IP-Adresse: direkt als IP-Adresse eingegeben werden.

Anmerkung: Wenn Sie SRV-Datensätze verwenden, stellen Sie sicher, dass _ldap.tcp. Datensätze verwenden den LDAP-Standardport 389. Andere Portnummern für LDAP werden von Expressway nicht unterstützt.

Hostname und Domäne:

- SRV-Eintrag: Nur der Domänenteil der Serveradresse ist erforderlich.
- Adressdatensatz: Geben Sie den Hostnamen und die Domäne ein. Diese werden dann kombiniert, um die vollständige Serveradresse für die Suche nach DNS-Adressdatensätzen bereitzustellen.
- IP-Adresse: Die Serveradresse wird direkt als IP-Adresse eingegeben.

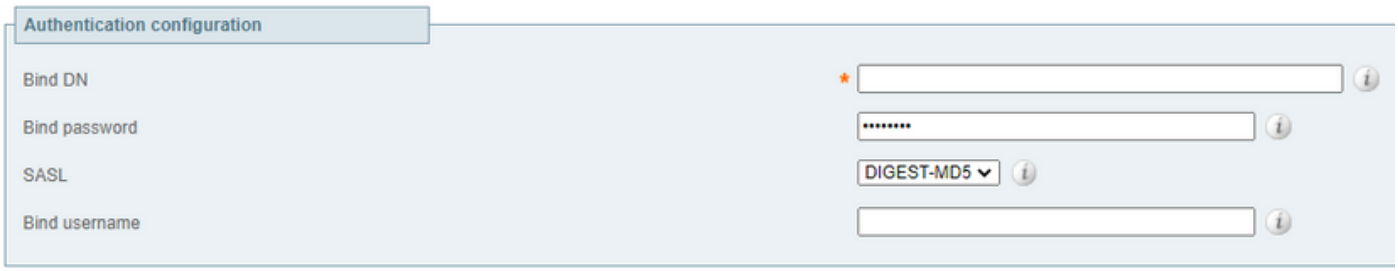
Anschluss:

- Der IP-Port für den LDAP-Server.

Verschlüsselung:

- TLS: verwendet TLS-Verschlüsselung (Transport Layer Security) für die Verbindung mit dem LDAP-Server.
- Off (Deaktiviert): wird keine Verschlüsselung verwendet.

- Authentifizierungskonfiguration: In diesem Abschnitt werden die Anmeldeinformationen für die Expressway-Authentifizierung angegeben, die für die Anbindung an den LDAP-Server verwendet werden sollen.



Bind-DN: Der Distinguished Name (DN), unabhängig von der Groß-/Kleinschreibung, wird von Expressway für die Anbindung an den LDAP-Server verwendet. Es ist wichtig, den DN in der Reihenfolge cn=, dann ou= und dann dc= anzugeben.

Anmerkung: Das Bind-Konto ist in der Regel ein schreibgeschütztes Konto ohne besondere Berechtigungen.

Bind-Passwort: Das Passwort (Groß- und Kleinschreibung beachten), das von Expressway für die Anbindung an den LDAP-Server verwendet wird.

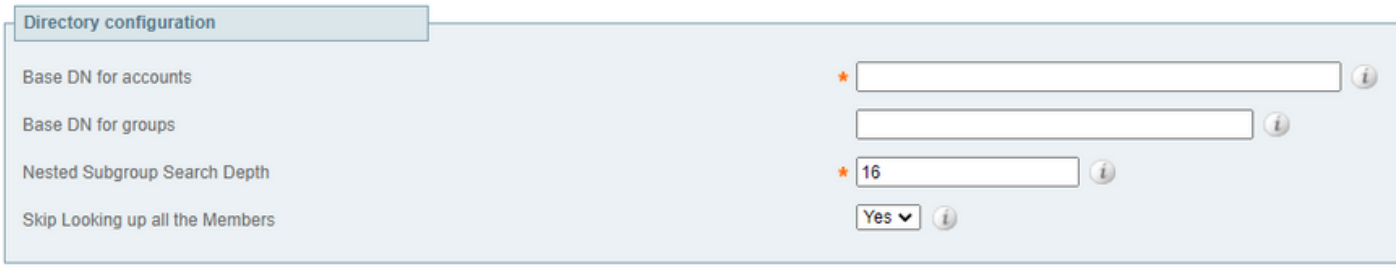
SASL: Der SASL-Mechanismus (Simple Authentication and Security Layer) für die Anbindung an den LDAP-Server

- None: wird kein Mechanismus verwendet.

- DIGEST-MD5: wird der DIGEST-MD5-Mechanismus verwendet.

Bind-Benutzername: Benutzername des Kontos, das der Expressway für die Anmeldung beim LDAP-Server verwendet (Groß- und Kleinschreibung beachten).

- Verzeichniskonfiguration: In diesem Abschnitt werden die wichtigsten DNs für die Suche nach Konto- und Gruppennamen angegeben.



Basis-DN für Konten: Die Definition der Organisationseinheit (OU) und des Domänencontrollers (DC) des Distinguished Name, bei der die Suche nach Benutzerkonten in der Datenbankstruktur beginnt (Groß-/Kleinschreibung wird nicht berücksichtigt).

Die Basis-DN für Konten und Gruppen muss auf oder unter der DC-Ebene liegen (ggf. alle dc=-Werte und ou=-Werte einschließen). Die LDAP-Authentifizierung bezieht sich nicht auf Sub-DC-Konten, sondern nur auf niedrigere OU- und CN-Ebenen.

Basis-DN für Gruppen: Die OU- und DC-Definition des Distinguished Name, bei der eine Suche nach Gruppen in der Datenbankstruktur beginnen muss (Groß-/Kleinschreibung wird nicht berücksichtigt).

Wenn kein Basis-DN für Gruppen angegeben ist, wird der Basis-DN für Konten sowohl für Gruppen als auch für Konten verwendet.

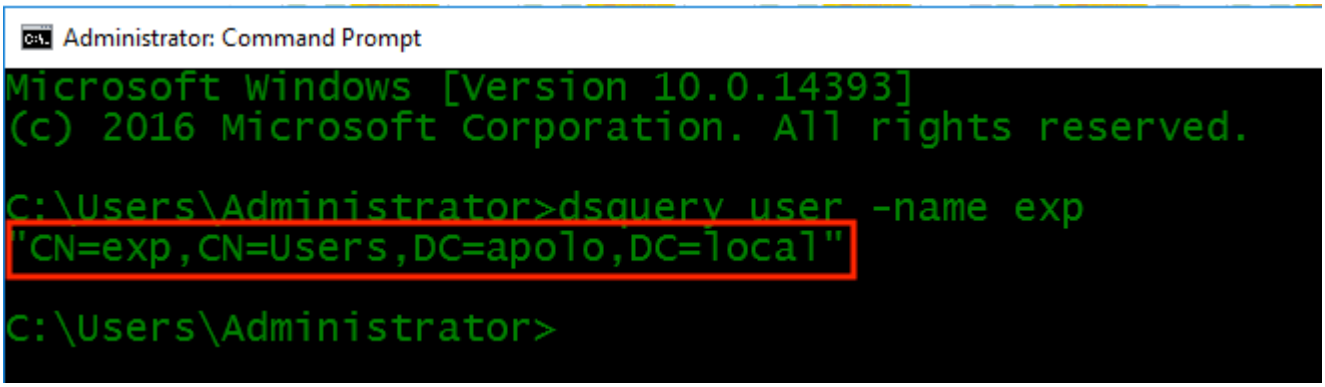
Verschachtelte Untergruppen-Suchtiefe: Wird verwendet, um die Tiefe der Gruppen für die LDAP-Suche einzuschränken.

Suche nach allen Mitgliedern überspringen: Wird verwendet, um die Suche nach Mitgliedern einer Administratorgruppe zu deaktivieren oder zu aktivieren, während der Authentifizierungs-Suchprozess durchgeführt wird. Der Standardwert ist "Ja". Die Suche nach Mitgliedern wird übersprungen.

So suchen Sie nach Basis-DN

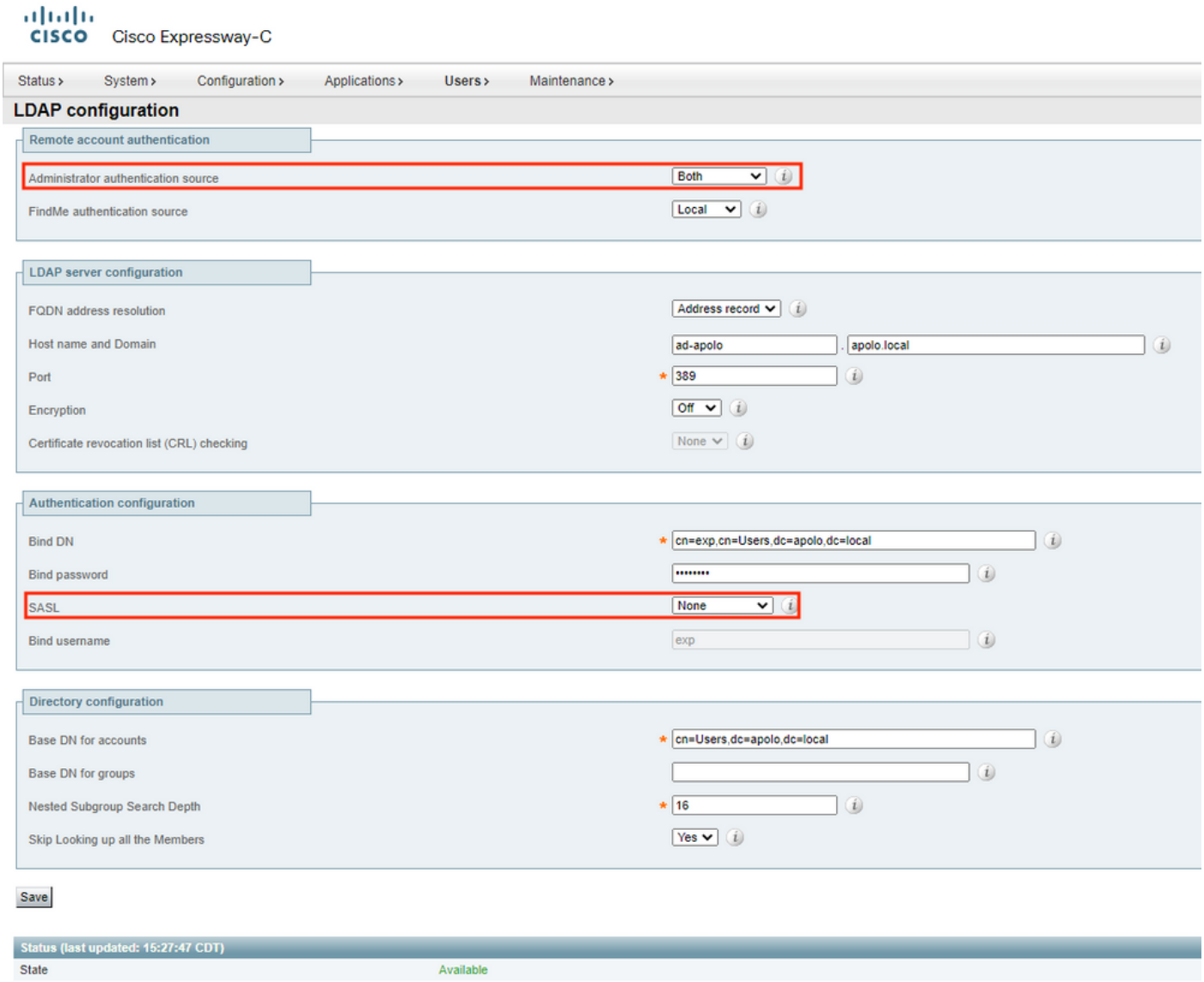
Öffnen Sie auf dem AD-Server die Eingabeaufforderung (CMD) als Administrator, und führen Sie den folgenden Befehl aus: **dsquery user -name**

.



LDAP-Konfigurationsbeispiel

Die Administrator-Authentifizierungsquelle ist in diesem Beispiel auf Both (Beide) und SASL auf None (Keine) festgelegt.



LDAP-Status überprüfen

Verbindungsstatus des LDAP-Servers überprüfen:

- Verfügbar: Es werden keine Fehlermeldungen angezeigt
- Fehlgeschlagen: Fehlermeldungen werden angezeigt. LDAP-Fehlermeldungen

Konfiguration von Administratorgruppen

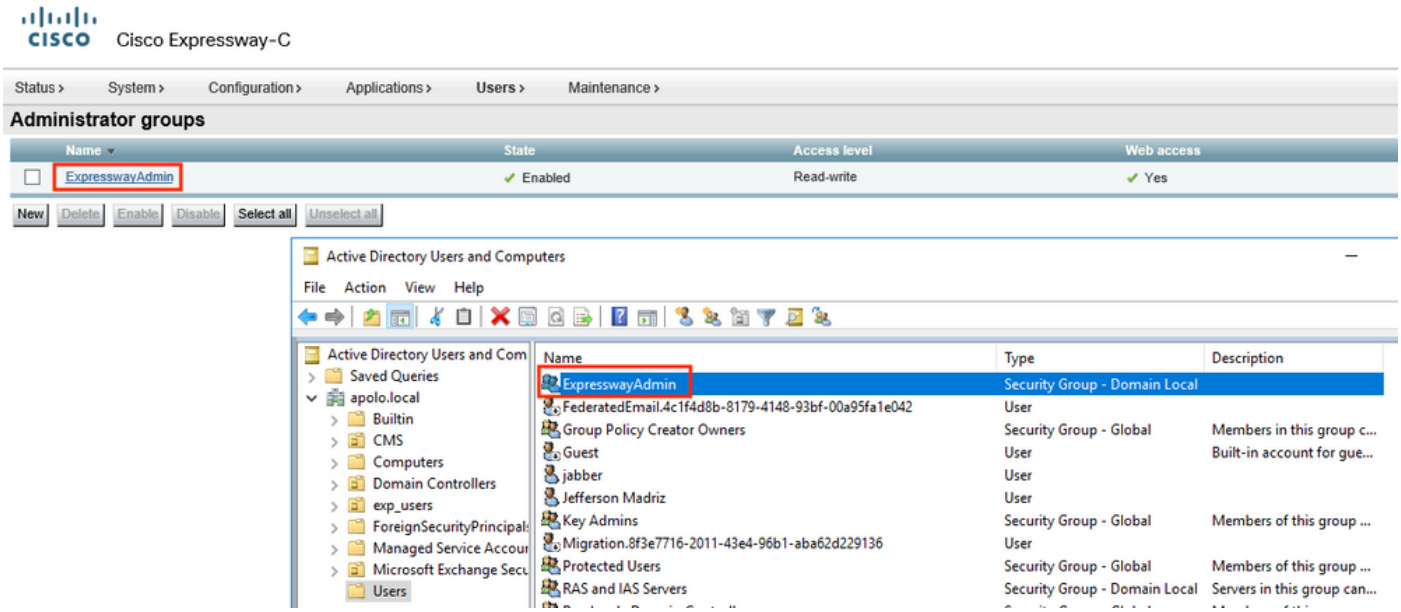
Die Seite Administratorgruppen Benutzer > Administratorgruppen listet alle Administratorgruppen auf, die auf dem Expressway konfiguriert wurden, und ermöglicht das Hinzufügen, Bearbeiten und Löschen von Gruppen.

Anmerkung: Administratorgruppen gelten nur, wenn Remote Account Authentication Using LDAP aktiviert ist.

Wenn Sie sich bei der Expressway-Webschnittstelle anmelden, werden Ihre Anmeldeinformationen mithilfe des Remoteverzeichnisdiensts authentifiziert, und Ihnen werden die Zugriffsrechte zugewiesen, die der Gruppe zugeordnet sind, der Sie angehören.

Konfigurationsoptionen für Administratorgruppen auf Expressway

Name: Der Name der Administratorgruppe. Die in Expressway definierten Gruppennamen müssen mit den Gruppennamen übereinstimmen, die im Remoteverzeichnisdienst eingerichtet wurden, um den Administratorzugriff auf diesen Expressway zu verwalten.



Zugriffsebene:

- Lese-/Schreibzugriff: Ermöglicht das Anzeigen und Ändern aller Konfigurationsdaten. Dadurch werden die gleichen Rechte wie für das Standardadmin-Konto bereitgestellt.
- Schreibgeschützt: Ermöglicht das Anzeigen von Status- und Konfigurationsinformationen ohne Änderungen. Einige Seiten, z. B. die Seite "Aktualisierung", sind für schreibgeschützte Konten gesperrt.
- Auditor: Zugriff nur auf die Seiten Event Log (Ereignisprotokoll), Configuration Log (Konfigurationsprotokoll), Network Log (Netzwerkprotokoll), Alarms und Overview

(Übersicht)
- None: Kein Zugriff zulässig

Webzugriff: Bestimmt, ob Mitglieder dieser Gruppe sich mit der Webschnittstelle beim System anmelden dürfen.

API-Zugriff: Bestimmt, ob Mitglieder dieser Gruppe über die API auf den Systemstatus und die Konfiguration zugreifen dürfen.

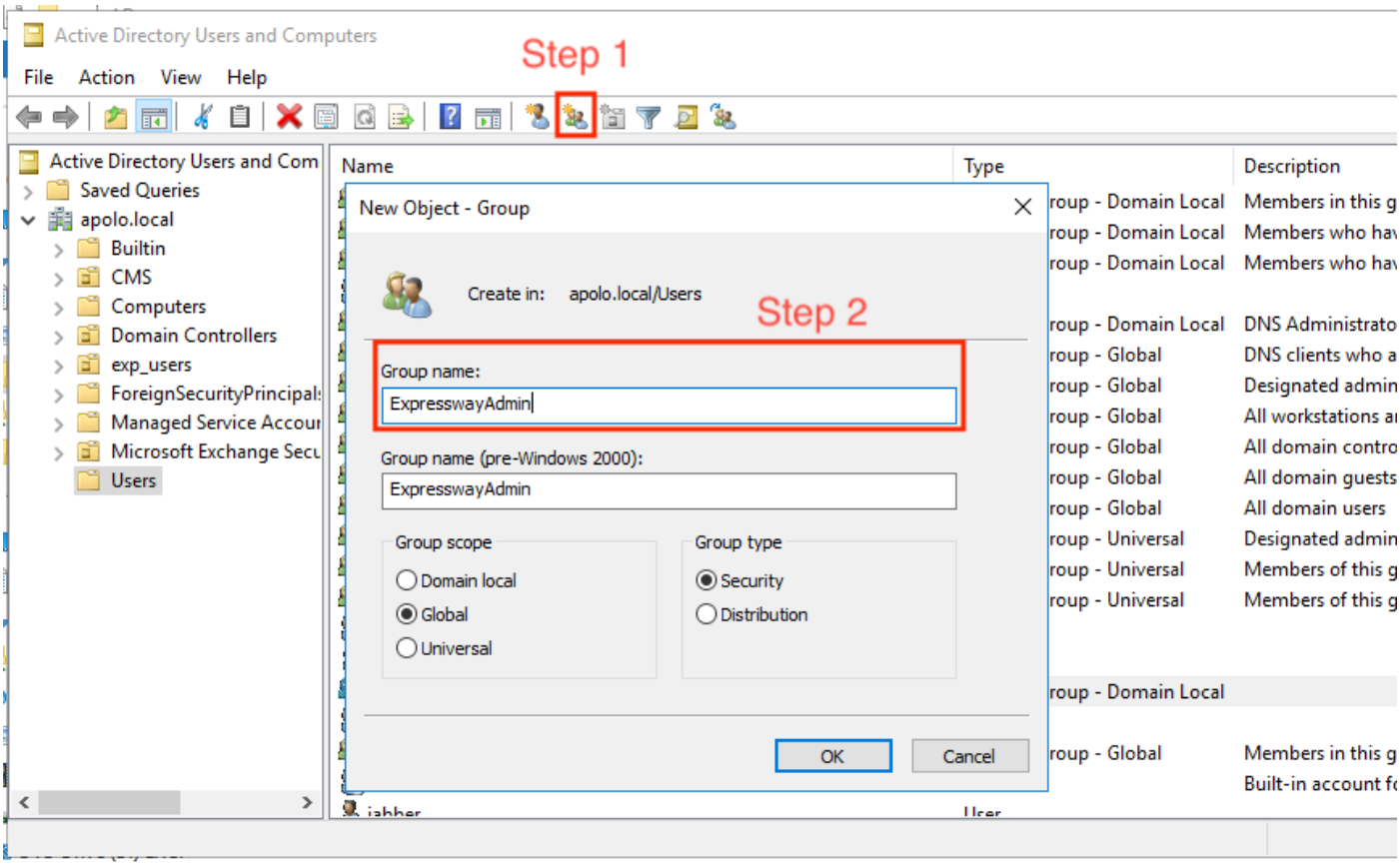
CLI-Zugriff: Bestimmt, ob Mitglieder dieser Gruppe über die CLI auf das System zugreifen dürfen.

Status: Gibt an, ob die Gruppe aktiviert oder deaktiviert ist.

Konfiguration der Administratorgruppe auf AD

1. Erstellen Sie eine neue Objektgruppe in dem Ordner, in dem Sie die Benutzer speichern möchten.

2. Weisen Sie dem Gruppennamen einen Namen zu.



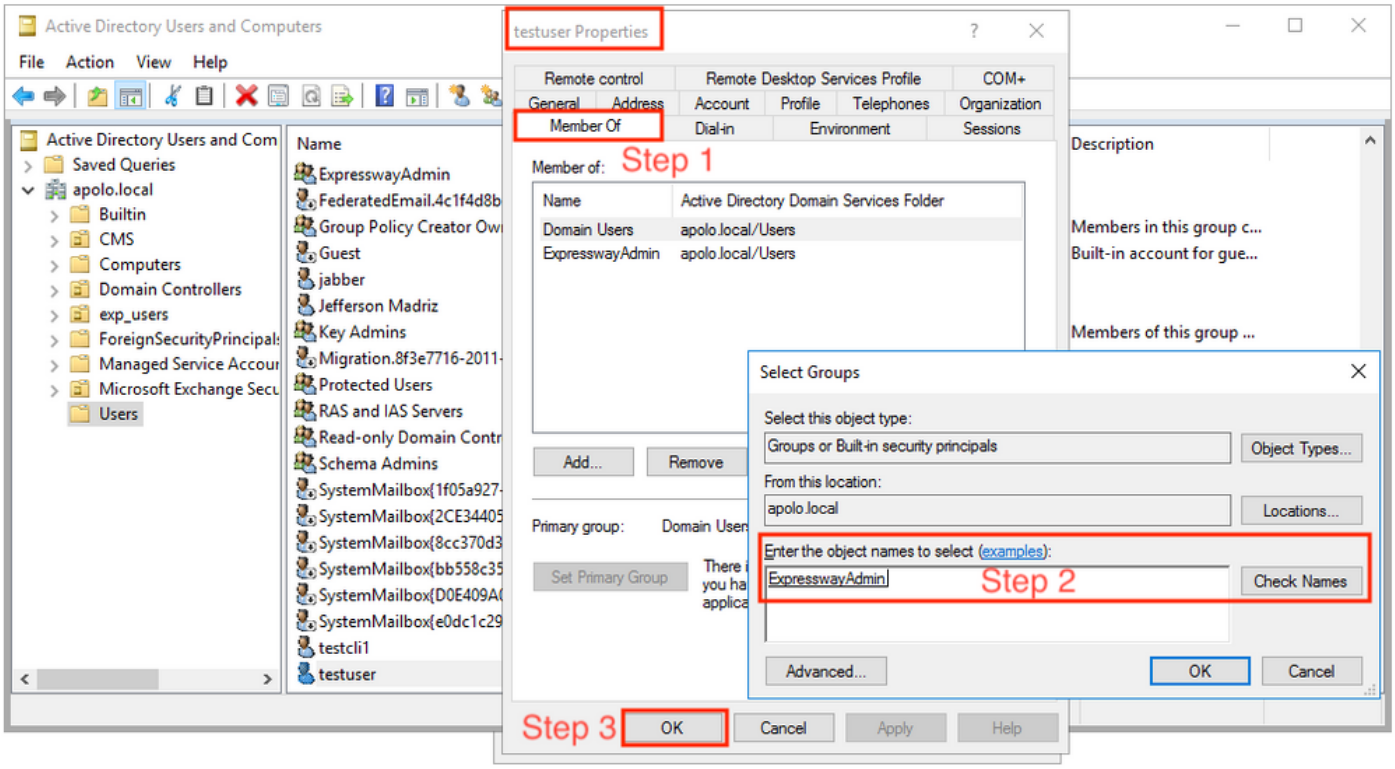
Weisen Sie die konfigurierte Gruppe dem oder den Benutzern zu, die über Web, API oder CLI auf Expressways zugreifen müssen. In diesem Fall ist der Benutzer testuser.

1. Öffnen Sie die Benutzereigenschaften, navigieren Sie zur Registerkarte Mitglied von,Wählen

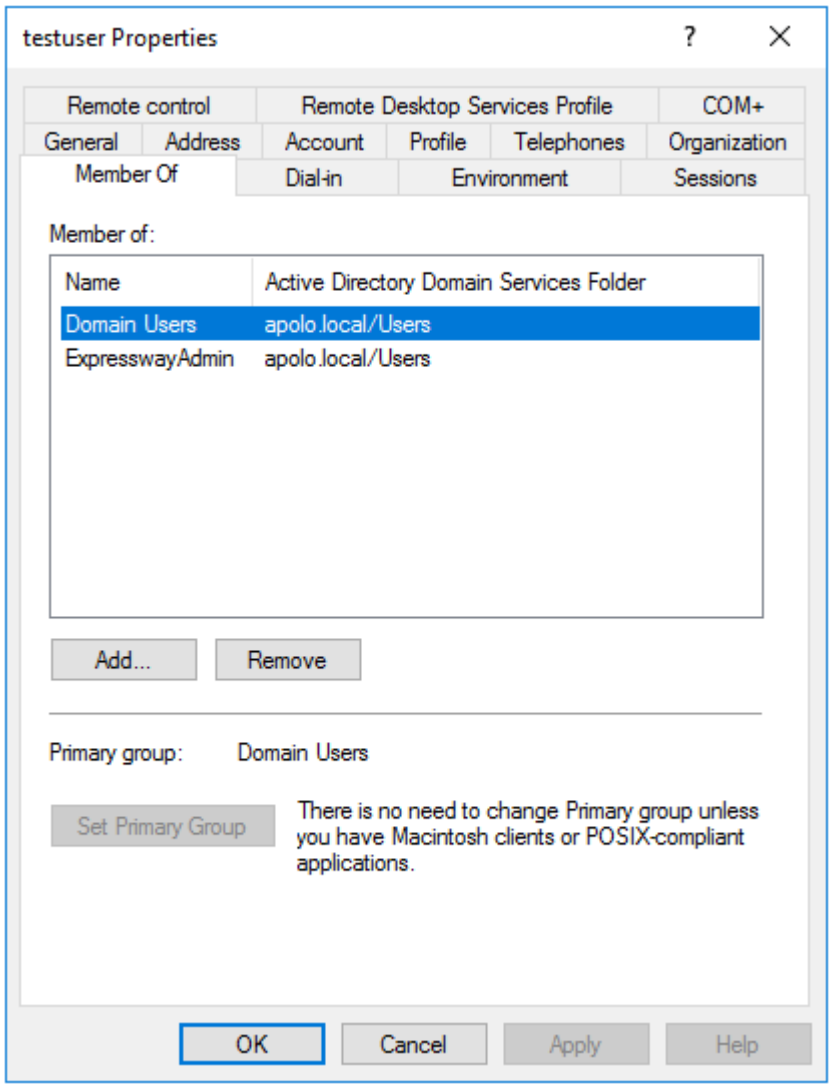
Sie Hinzufügen

2. Suchen Sie nach dem zuvor erstellten Gruppennamen.

3. Wählen Sie dann OK.



Zu diesem Zeitpunkt ist der Benutzer Mitglied von Domain Users und ExpresswayAdmin.

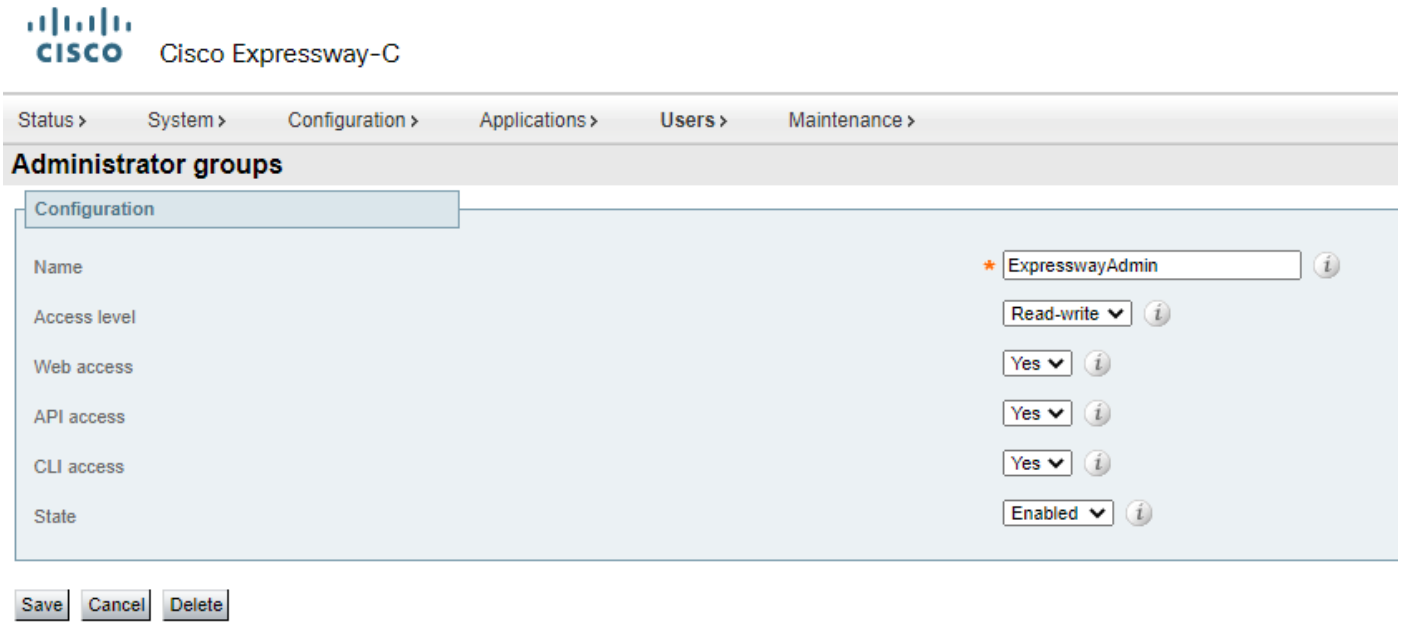


Konfiguration der Administratorgruppe auf Expressway

Sobald die Konfiguration abgeschlossen ist, navigieren Sie auf Expressway zu Users > Administrator groups, und wählen Sie New

Name: muss mit dem konfigurierten Gruppennamen übereinstimmen und mit dem LDAP-Benutzer verknüpft sein, der auf den Expressway zugreifen muss. In diesem Beispiel lautet der Gruppenname ExpresswayAdmin, der neue Administratorgruppenname lautet also ExpresswayAdmin.

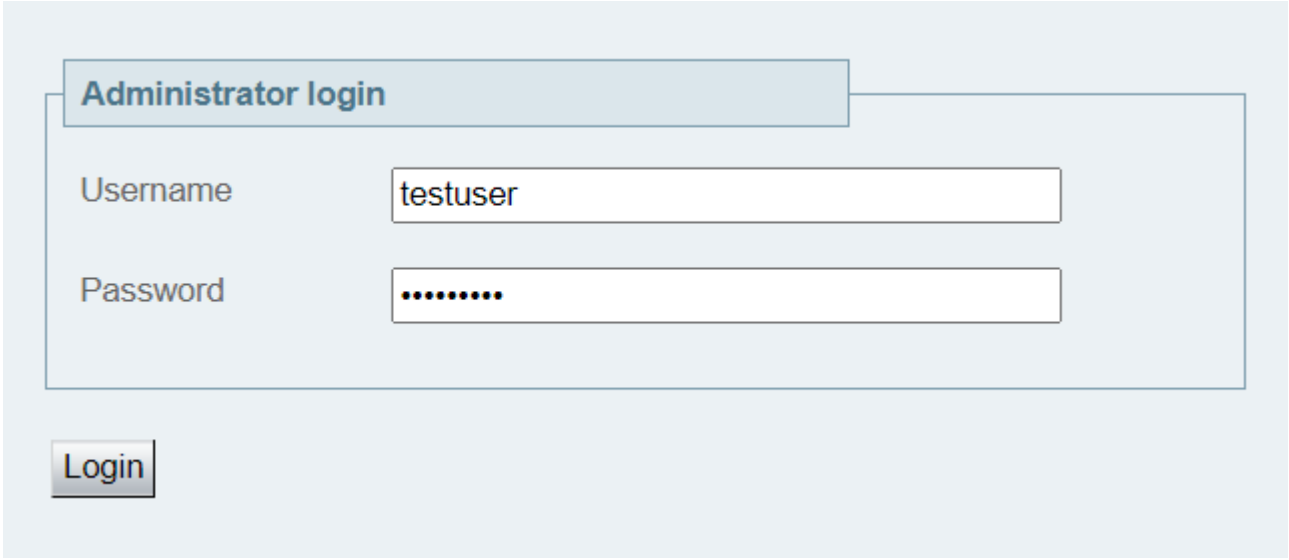
Für diese Gruppe sind alle Berechtigungen und alle Zugriffsrechte verfügbar.



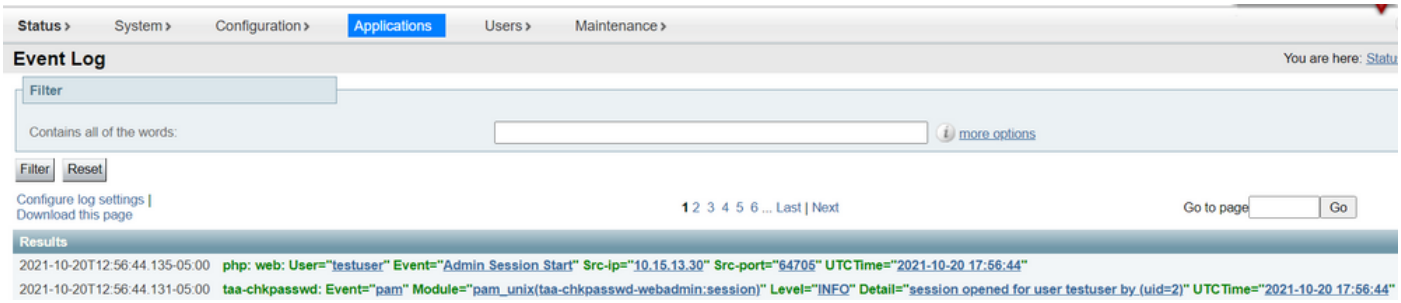
Wählen Sie Speichern aus.

Überprüfung

Melden Sie sich ab, und versuchen Sie, über das Internet auf den LDAP-Benutzer zuzugreifen, dem die Administratorgruppe zugeordnet ist. In diesem Beispiel ist der erstellte Benutzer testuser.



Dies kann über Status > Event log (Ereignisprotokoll) bestätigt werden:


Status › System › Configuration › Applications Users › Maintenance ›
Event Log
You are here: Statu
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"

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.