Configuración de LDAP en Expressway para acceso Web, API y CLI

Contenido

Introducción

Este documento describe los pasos necesarios para habilitar el protocolo ligero de acceso a directorios (LDAP) en el servidor de Expressway y cómo habilitar el acceso de los grupos de administradores a través de la Web, la interfaz de programación de aplicaciones (API) y la interfaz de línea de comandos (CLI) a Expressway con los usuarios de dominio.

Colaboración de Jefferson Madriz y Elias Sevilla, Ingenieros del TAC de Cisco.

Prerequisites

Requirements

- Conocimientos básicos sobre Expressway.
- Configuración básica de Expressway ya realizada.
- Active Directory (AD) ya configurado.
- Reglas de firewall preparadas para permitir la comunicación entre Expressway y el servidor AD.

Componentes Utilizados

- Active Directory instalado en Windows Server 2016.
- Servidor de Expressway-C en la versión X14.0.3.

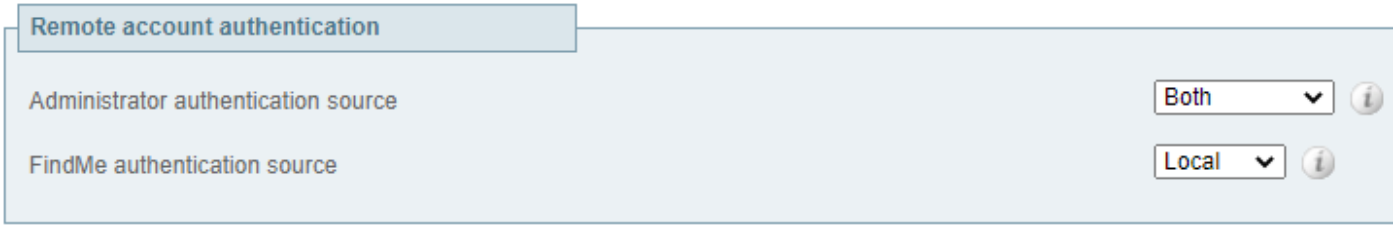
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Configuración de LDAP

La página de configuración de LDAP Usuarios > Configuración de LDAP se utiliza para configurar una conexión LDAP a un servicio de directorio remoto para la autenticación de cuenta de administrador.

- Autenticación de cuenta remota: Esta sección le permite habilitar o inhabilitar el uso de LDAP para autenticación de cuenta remota.



- Sólo local: Las credenciales se comprueban con una base de datos local almacenada en el sistema.
- Sólo remoto: Las credenciales se comprueban con un directorio de credenciales externo.
-Ambas: Las credenciales se comprueban primero con una base de datos local almacenada en el sistema y, a continuación, si no hay ninguna coincidencia con la cuenta, se utiliza en su lugar el directorio de credenciales externas.

- Configuración del servidor LDAP: esta sección especifica los detalles de conexión al servidor LDAP.

Resolución de dirección FQDN:

- registro SRV: búsqueda de registro de servicio (SRV) del servicio de nombres de dominio (DNS).
- Registro de dirección: Búsqueda de registros A o AAAA de DNS.
- Dirección IP: se introduce directamente como dirección IP.

Nota: Si utiliza registros SRV, asegúrese de que _ldap._tcp. Los registros utilizan el puerto LDAP estándar 389. Expressway no admite otros números de puerto para LDAP.

Nombre de host y dominio:

- Registro SRV: solo se requiere la parte del dominio de la dirección del servidor.
- Registro de dirección: introduzca el nombre de host y el dominio. A continuación, se combinan para proporcionar la dirección de servidor completa para la búsqueda de registros de direcciones DNS.
- Dirección IP: la dirección del servidor se introduce directamente como dirección IP.

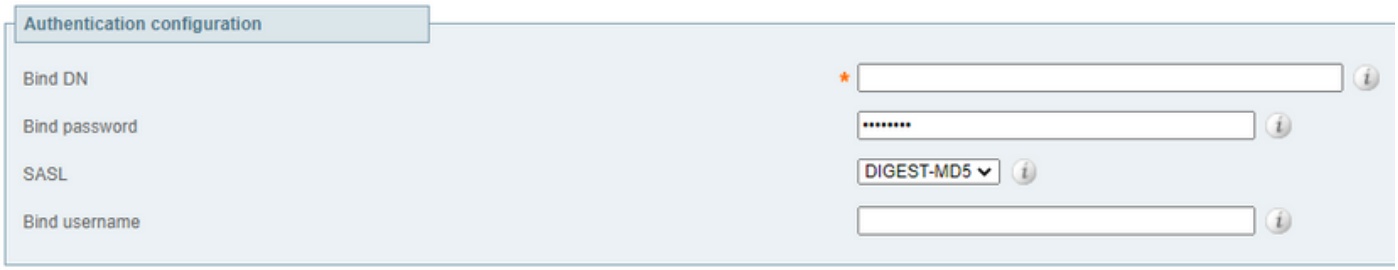
Puerto:

- El puerto IP a utilizar en el servidor LDAP.

Cifrado:

- TLS: utiliza el cifrado de Seguridad de la capa de transporte (TLS) para la conexión con el servidor LDAP.
- Desactivado: no se utiliza cifrado.

- Configuración de autenticación: esta sección especifica las credenciales de autenticación de Expressway que se utilizarán para enlazar con el servidor LDAP.



Enlazar DN: El nombre distinguido (DN), sin distinción de mayúsculas y minúsculas, que utiliza Expressway para enlazar con el servidor LDAP. Es importante especificar el DN en el orden cn=, luego ou= y luego dc=

Nota: La cuenta de enlace suele ser una cuenta de sólo lectura sin privilegios especiales.

Enlazar contraseña: La contraseña (distingue entre mayúsculas y minúsculas) que utiliza Expressway para enlazar con el servidor LDAP.

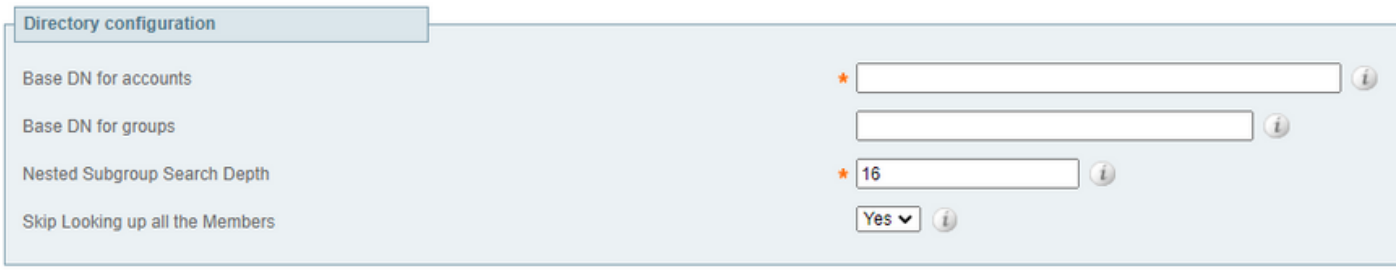
SASL: Mecanismo de autenticación simple y capa de seguridad (SASL) que se utiliza para enlazar con el servidor LDAP

- Ninguno: no se utiliza ningún mecanismo.
- DIGEST-MD5: se utiliza el mecanismo DIGEST-MD5.

Enlazar nombre de usuario: Nombre de usuario de la cuenta que utiliza Expressway para iniciar

sesión en el servidor LDAP (distingue entre mayúsculas y minúsculas).

- Configuración del directorio: En esta sección se especifican los nombres completos base que se utilizarán para buscar nombres de cuentas y grupos.



DN base para cuentas: la definición de unidad organizativa (OU) y controlador de dominio (DC) del nombre distinguido donde comienza una búsqueda de cuentas de usuario en la estructura de base de datos (no distingue entre mayúsculas y minúsculas).

El DN base para cuentas y grupos debe estar en el nivel DC o por debajo de él (incluya todos los valores dc= y ou= si es necesario). La autenticación LDAP no busca en las cuentas de DC secundarias, solo en los niveles OU y Nane común (CN) más bajos.

DN base para grupos: definición de OU y DC del nombre distinguido donde debe comenzar una búsqueda de grupos en la estructura de base de datos (no distingue entre mayúsculas y minúsculas).

Si no se especifica un DN base para los grupos, el DN base para las cuentas se utiliza tanto para los grupos como para las cuentas.

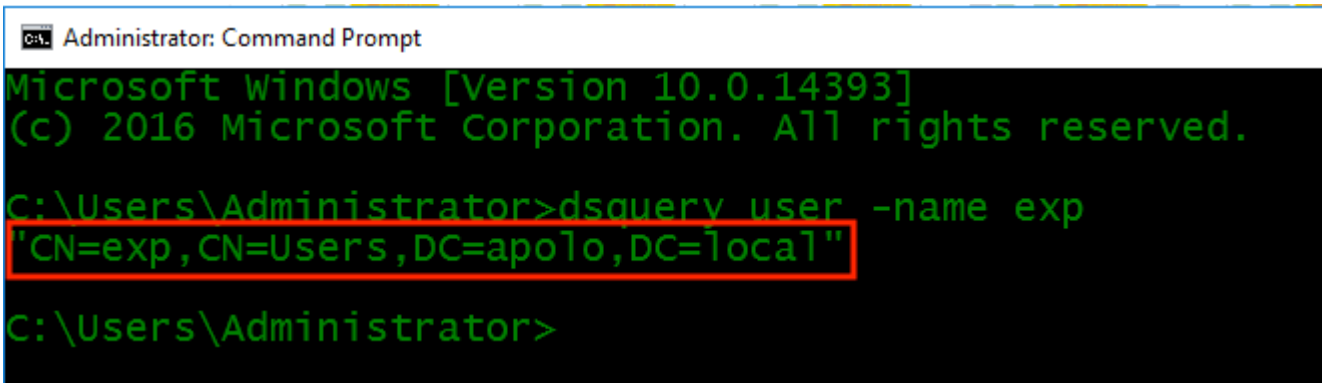
Profundidad de búsqueda de subgrupos anidados: se utiliza para limitar la profundidad de los grupos para la búsqueda LDAP.

Omitir la búsqueda de todos los miembros: se utiliza para deshabilitar o habilitar la búsqueda de miembros de un grupo de administradores mientras se realiza el proceso de búsqueda de autenticación. El valor predeterminado es Yes - omitir la búsqueda de miembros.

Cómo encontrar el DN base

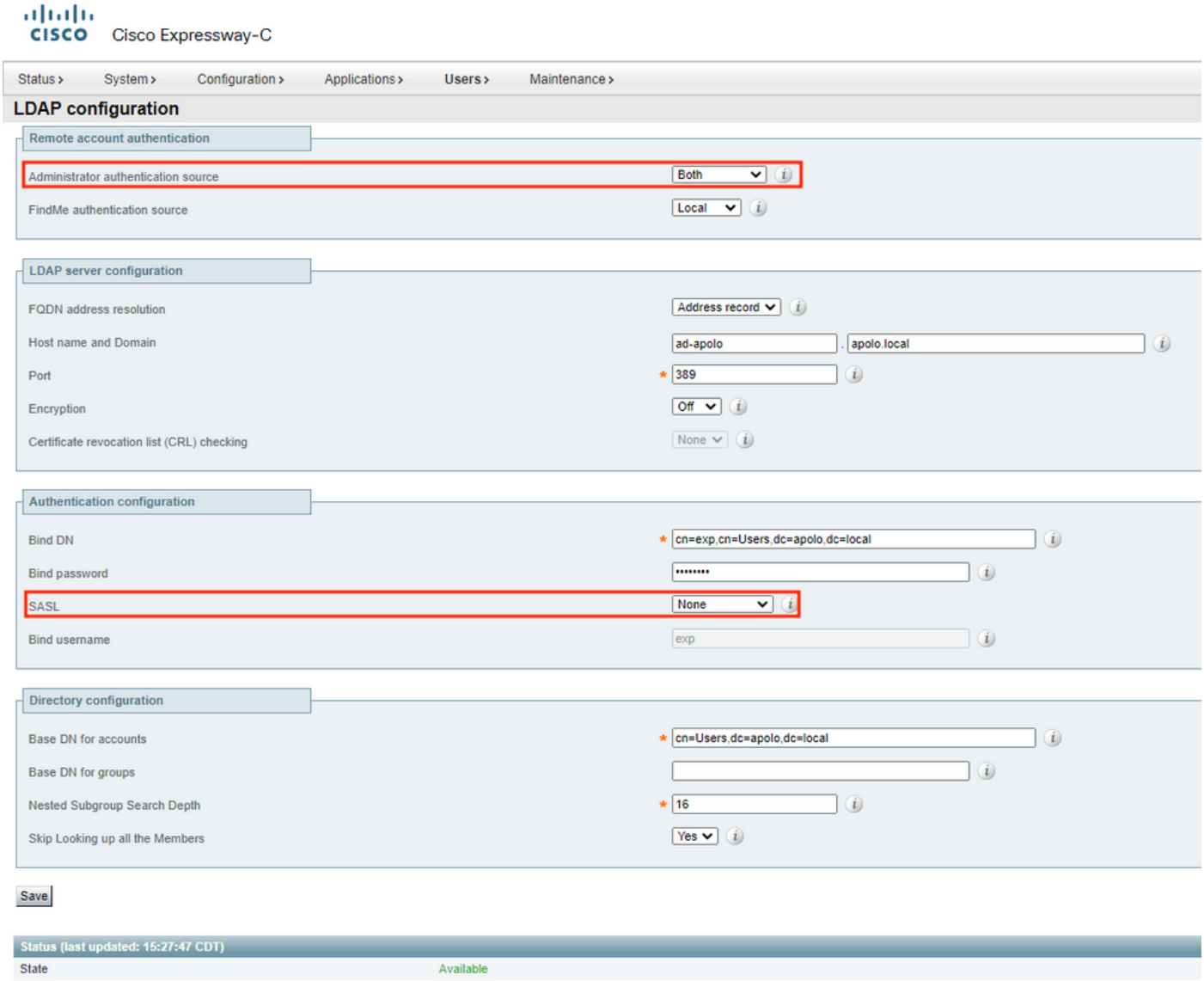
En el servidor de AD, abra el símbolo del sistema (CMD) como administrador y ejecute el comando: **dsquery user -name**

.



Ejemplo de Configuración LDAP

El origen de autenticación del administrador se establece en Both y SASL se establece en None en este ejemplo.



Verificar estado LDAP

Validar el estado de conexión del servidor LDAP:

- Disponible: No se muestran mensajes de error
- Error: Se muestran mensajes de error. Mensajes de error LDAP

Configuración de grupos de administradores

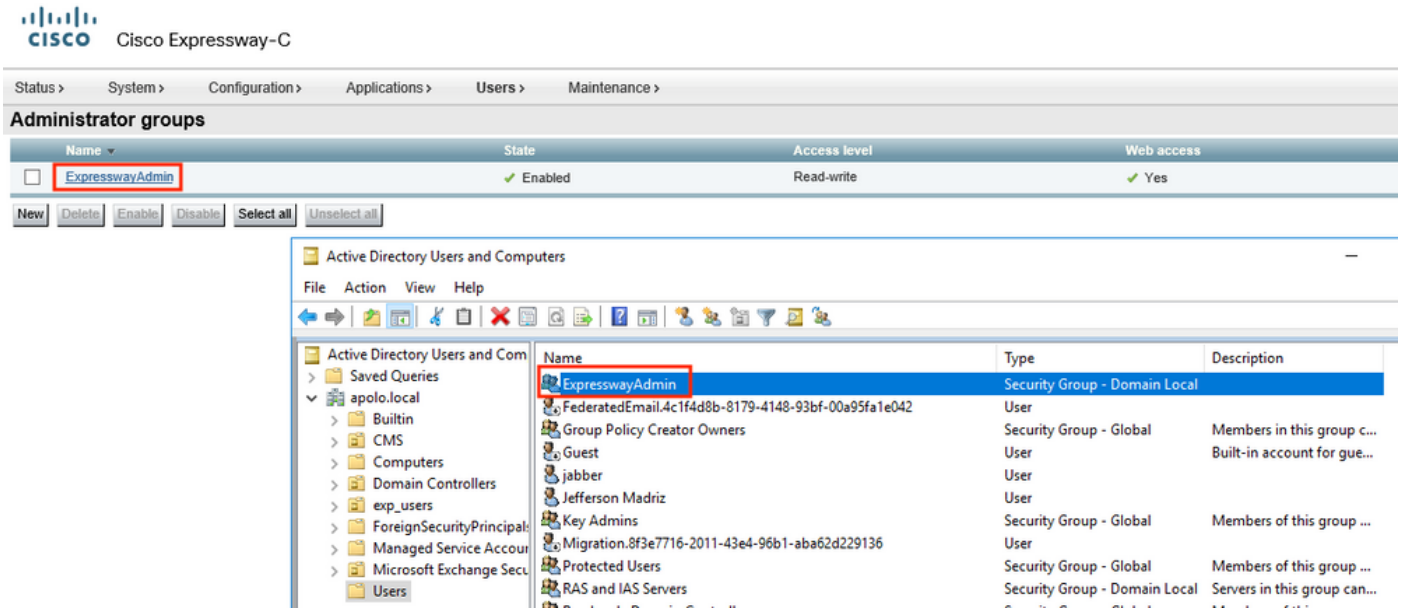
La página Grupos de administradores Usuarios > Grupos de administradores muestra todos los grupos de administradores que se han configurado en Expressway y le permite agregar, editar y eliminar grupos.

Nota: Los grupos de administradores sólo se aplican si la autenticación de cuenta remota mediante LDAP está habilitada.

Al iniciar sesión en la interfaz web de Expressway, las credenciales se autentican en el servicio de directorio remoto y se le asignan los derechos de acceso asociados con el grupo al que pertenece.

Opciones de configuración de grupos de administradores en Expressway

Nombre: El nombre del grupo de administradores. Los nombres de grupo definidos en Expressway deben coincidir con los nombres de grupo que se han configurado en el servicio de directorio remoto para administrar el acceso de administrador a Expressway.



Nivel de acceso:

- Lectura-escritura Permite ver y modificar toda la información de configuración. Esto proporciona los mismos derechos que la cuenta de administrador predeterminada.
- Sólo-Lectura: Permite que la información de estado y configuración se visualice únicamente y no se modifique. Algunas páginas, como la página Actualizar, están bloqueadas para cuentas de solo lectura.
- Auditor: Permite acceder únicamente a las páginas Event Log (Registro de eventos), Configuration Log (Registro de configuración), Network Log (Registro de red), Alarms and

Overview (Alarmas).
- Ninguno: No se permite el acceso

Acceso web: Determina si los miembros de este grupo pueden iniciar sesión en el sistema con la interfaz web.

Acceso a API: Determina si los miembros de este grupo tienen permiso para acceder al estado y la configuración del sistema con la API.

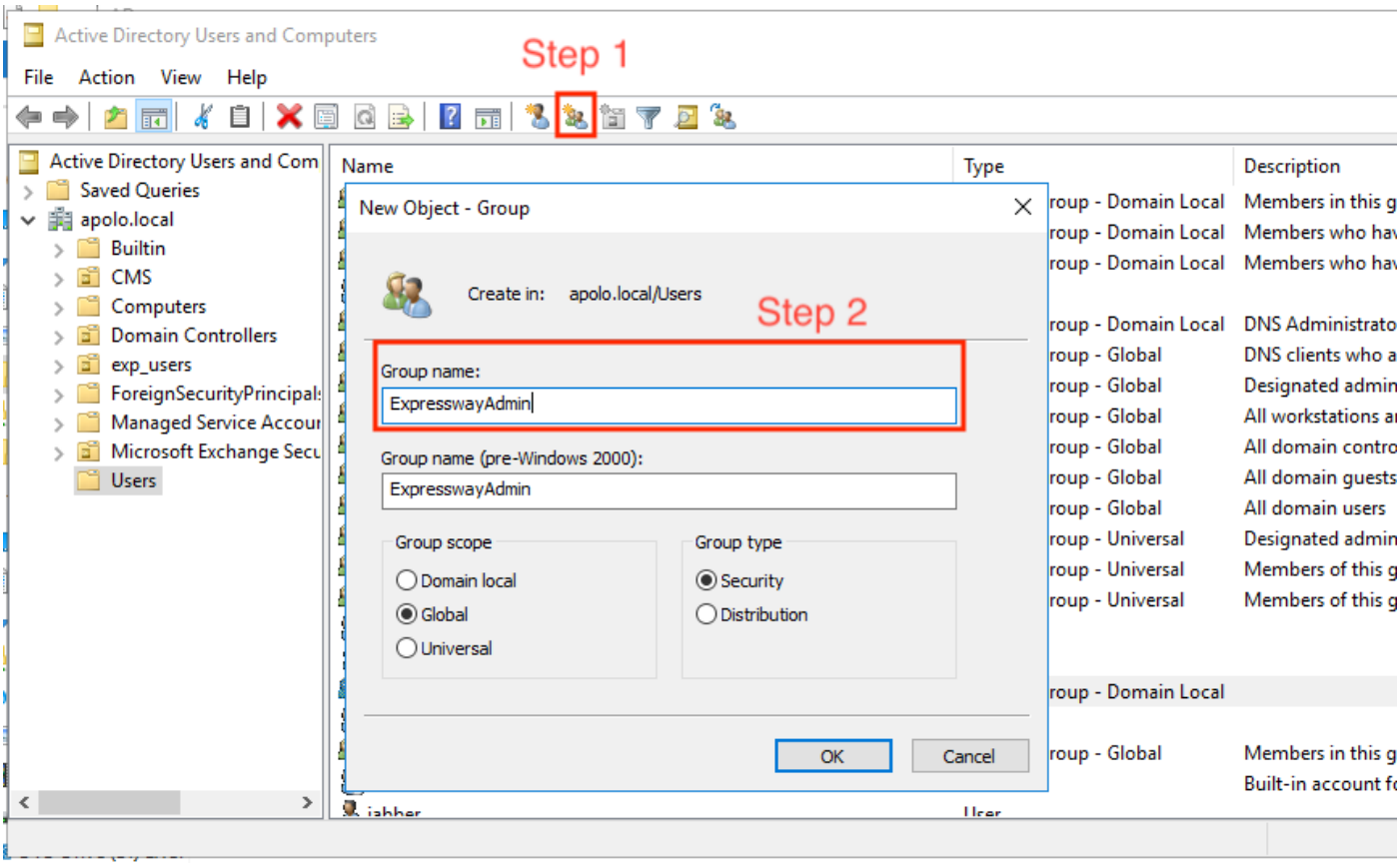
Acceso CLI: Determina si los miembros de este grupo tienen permiso para acceder al sistema a través de CLI.

Estado: Indica si el grupo está activado o desactivado.

Configuración del grupo de administradores en AD

1. Cree un nuevo grupo de objetos, en la carpeta en la que desea almacenar los usuarios.

2. Asigne un nombre al nombre del grupo.

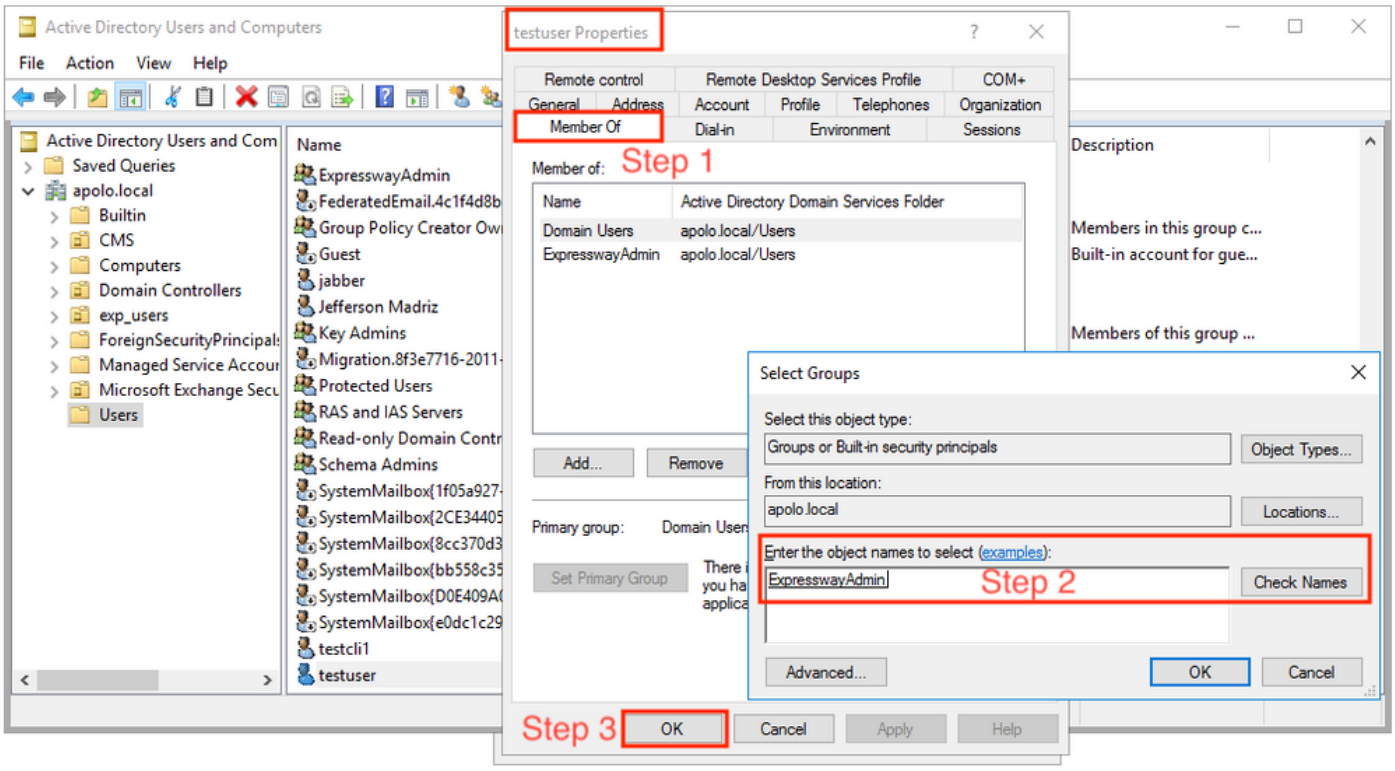


Asigne el grupo configurado al usuario o usuarios que necesitan acceder a Expressway a través de la Web, la API o la CLI. En este caso, el usuario es testuser.

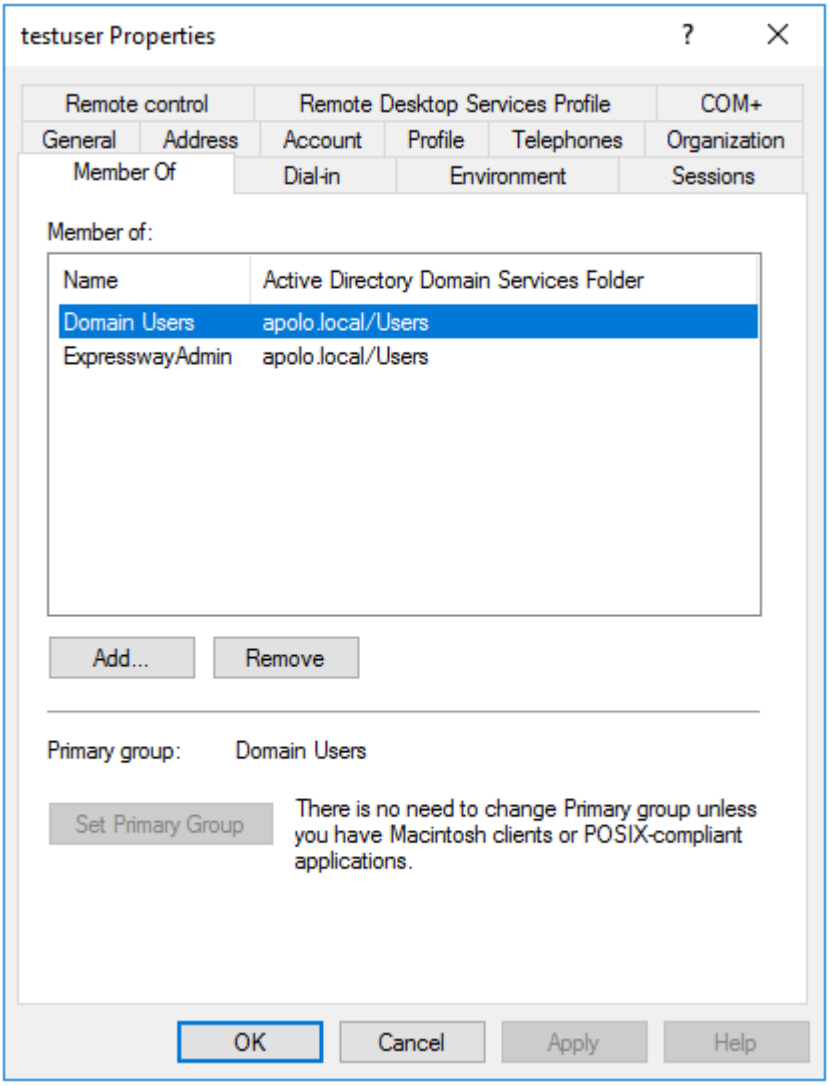
1. Abra las propiedades del usuario, acceda a la pestaña Miembro de, seleccione Agregar

2. Busque el nombre de grupo creado anteriormente.

3. Luego seleccione OK.



En este momento, el usuario es miembro de Domain Users y ExpresswayAdmin.

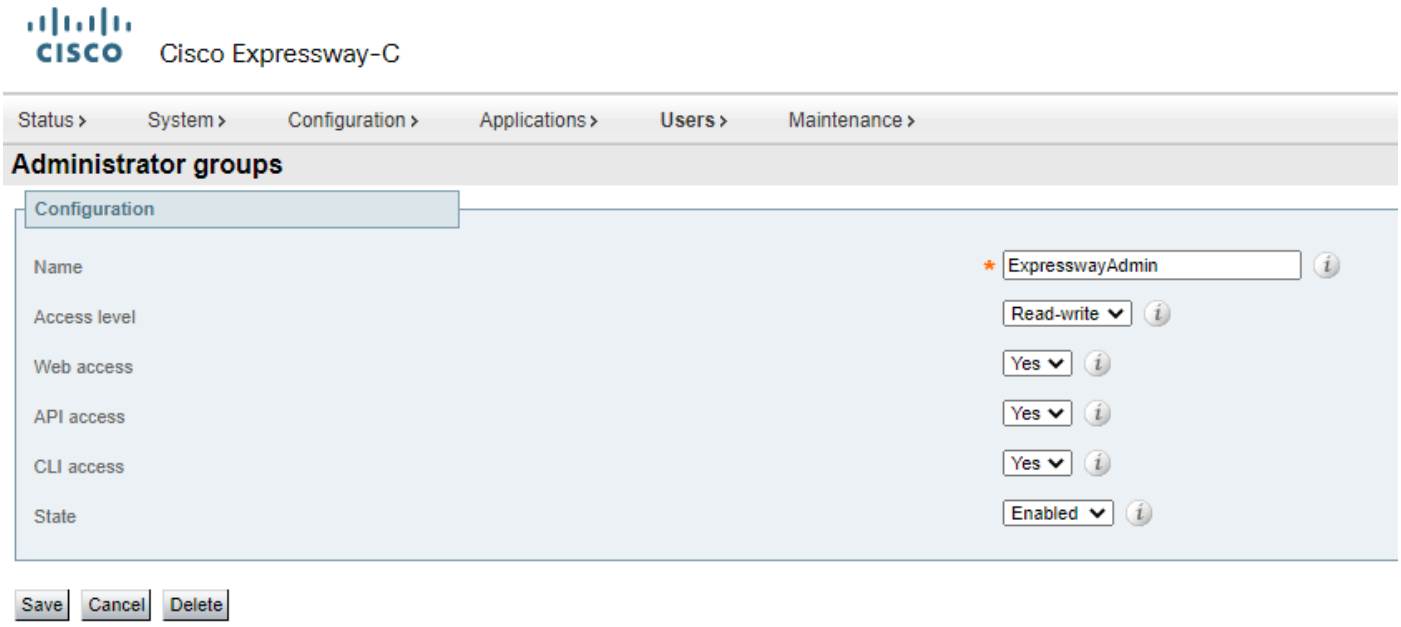


Configuración del grupo de administradores en Expressway

Una vez finalizada la configuración, en Expressway, navegue hasta Usuarios > Grupos de administradores, seleccione Nuevo

Nombre: debe coincidir con el nombre de grupo configurado y asociado con el usuario LDAP que necesita acceder a Expressway. En este ejemplo, el nombre del grupo es ExpresswayAdmin, por lo que el nuevo nombre del grupo de administradores es ExpresswayAdmin.

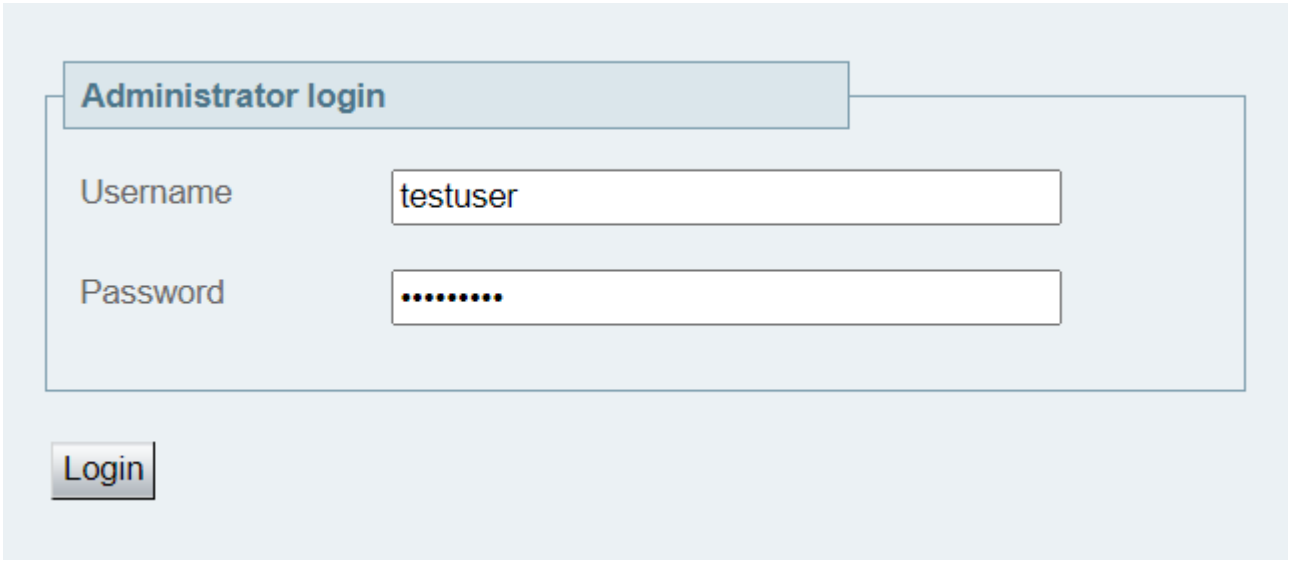
Este grupo tiene todos los permisos y acceso disponibles.



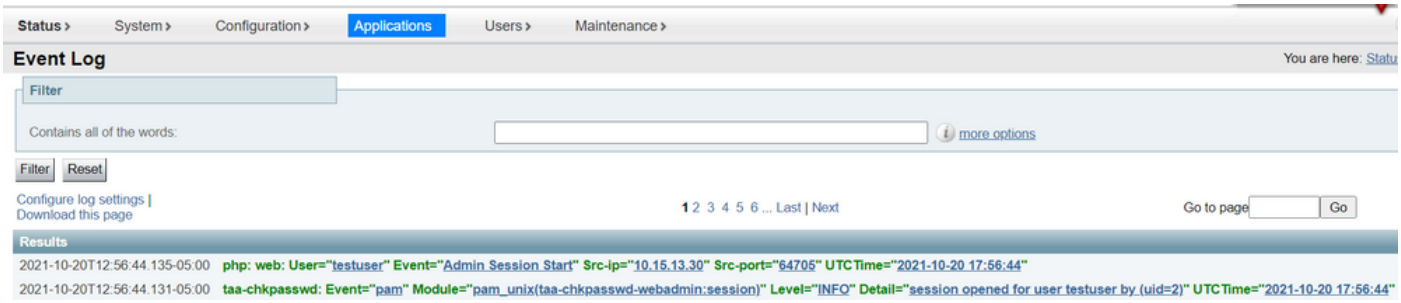
Seleccione Guardar.

Verificación

Cierre la sesión e intente acceder a través de la Web con el usuario LDAP que tiene el grupo de administradores asociado. En este ejemplo, el usuario creado es testuser.



Esto se puede confirmar a través de Status > Event log:


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"

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).