Configurar LDAP no Expressway para acesso à Web, API e CLI

Contents

Introdução

Este documento descreve as etapas necessárias para ativar o Lightweight Diretory Access Protocol (LDAP) no servidor Expressway e como ativar o Administrator Groups para acessar via Web, Application Programming Interface (API) e Command Line Interface (CLI) para o Expressway com seus usuários de domínio.

Contribuição de Jefferson Madriz e Elias Sevilla, engenheiros do Cisco TAC.

Pré-requisitos

Requisitos

- Conhecimento básico sobre o Expressway.
- Configuração básica do Expressway já feita.
- Ative Diretory (AD) já configurado.
- Regras de firewall prontas, para permitir a comunicação entre o Expressway e o servidor AD.

Componentes Utilizados

- Ative Diretory instalado no Windows Server 2016.
- Servidor Expressway-C na versão X14.0.3.

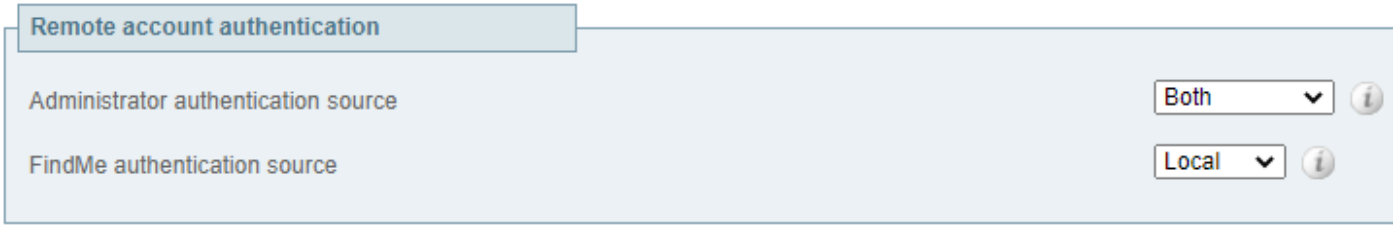
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Configuração LDAP

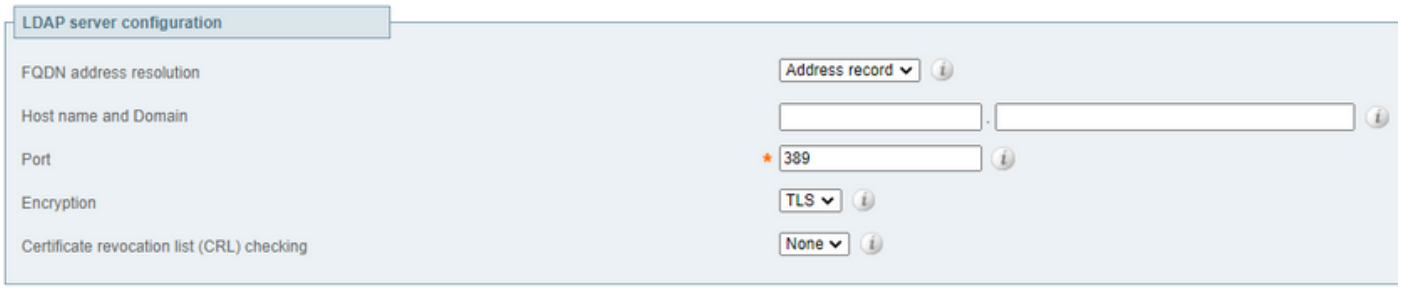
A página de configuração LDAP Users > LDAP configuration é usada para configurar uma conexão LDAP a um serviço de diretório remoto para autenticação de conta de administrador.

- Autenticação de conta remota: Esta seção permite habilitar ou desabilitar o uso de LDAP para autenticação de conta remota.



- Somente local: As credenciais são verificadas em relação a um banco de dados local armazenado no sistema.
- Somente remoto: As credenciais são verificadas em um diretório de credenciais externas.
-Ambos: As credenciais são verificadas primeiro em um banco de dados local armazenado no sistema e, em seguida, se não houver correspondência com a conta, o diretório de credenciais externas será usado.

- Configuração do servidor LDAP: esta seção especifica os detalhes da conexão com o servidor LDAP.



Resolução de endereço FQDN:

- Registro SRV: pesquisa de Registro de Serviço (SRV) do Domain Name Service (DNS).
- Registro de endereço: Pesquisa de registro DNS A ou AAAA.
- Endereço IP: digitado diretamente como um endereço IP.

Note: Se você usar registros SRV, certifique-se de que _ldap._tcp. Os registros usam a

---

porta LDAP padrão 389. O Expressway não oferece suporte a outros números de porta para LDAP.

Nome do host e domínio:

- Registro SRV: somente a parte Domínio do endereço do servidor é necessária.
- Registro de endereço: insira o Nome do host e o Domínio. Eles são combinados para fornecer o endereço completo do servidor para a pesquisa de registro de endereço DNS.
- Endereço IP: o endereço do servidor é inserido diretamente como um endereço IP.

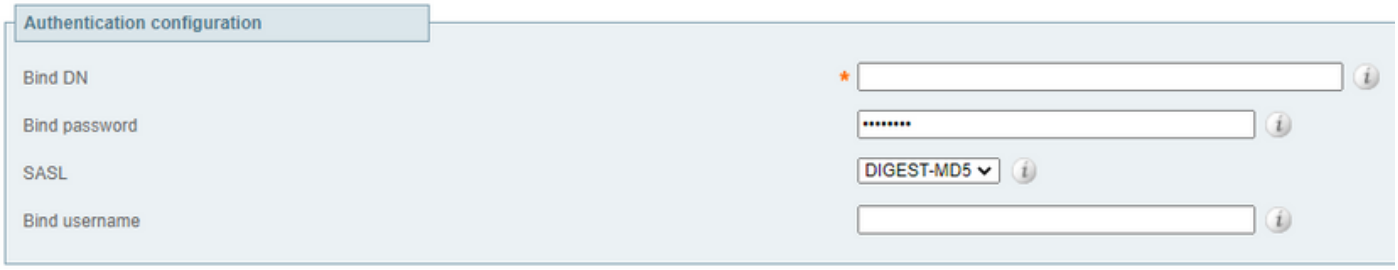
Porta:

- A porta IP a ser usada no servidor LDAP.

Criptografia:

- TLS: usa a criptografia TLS (Transport Layer Security) para a conexão ao servidor LDAP.
- Off: nenhuma criptografia é usada.

- Configuração de autenticação: esta seção especifica as credenciais de autenticação do Expressway a serem usadas para vincular ao servidor LDAP.



DN de vinculação: O DN (Distinguished Name - Nome Distinto), não diferencia maiúsculas de minúsculas, usado pelo Expressway para vincular-se ao servidor LDAP. É importante especificar o DN na ordem cn=, depois ou=, depois dc=

Note: A conta vinculada é geralmente uma conta somente leitura sem privilégios especiais.

Senha de vinculação: A senha (diferencia maiúsculas de minúsculas) usada pelo Expressway para vincular ao servidor LDAP.

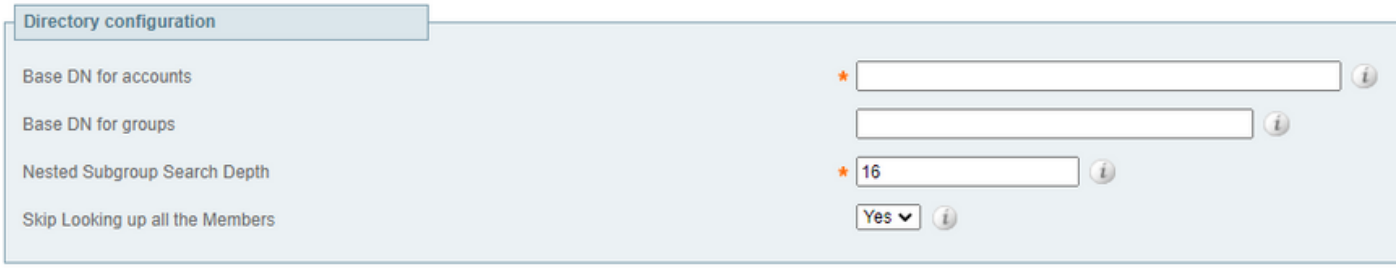
SASL: O mecanismo SASL (Simple Authentication and Security Layer) a ser usado para vincular ao servidor LDAP

- Nenhum: nenhum mecanismo é usado.
- DIGEST-MD5: o mecanismo DIGEST-MD5 é usado.

Associar nome de usuário: Nome de usuário da conta que o Expressway usa para fazer logon no servidor LDAP (diferencia maiúsculas de minúsculas).

- Configuração do diretório: Esta seção especifica os nomes distintos base a serem usados

para procurar por nomes de conta e de grupo.



DN Base para contas: A definição da Unidade Organizacional (OU) e do Controlador de Domínio (DC) do Nome Distinto em que uma pesquisa de contas de usuário começa na estrutura do banco de dados (não diferencia maiúsculas de minúsculas).

O DN base para contas e grupos deve estar no nível DC ou abaixo dele (inclua todos os valores dc= e ou=, se necessário). A autenticação LDAP não examina as contas sub DC, apenas os níveis de OU e CN (Common Nag, nome comum) mais baixos.

DN Base para grupos: A definição de OU e DC do Nome Distinto onde uma pesquisa por grupos deve começar na estrutura do banco de dados (não diferencia maiúsculas de minúsculas).

Se nenhum DN base para grupos for especificado, o DN base para contas será usado para grupos e contas.

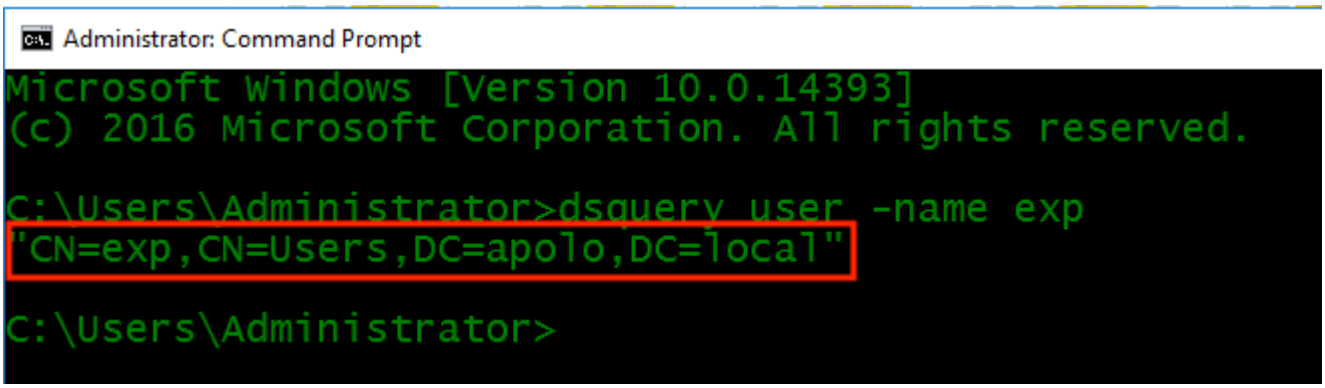
Profundidade de pesquisa de subgrupo aninhado: usada para limitar a profundidade de grupos para a pesquisa LDAP.

Ignorar pesquisa de todos os membros: usado para desabilitar ou habilitar a pesquisa de membros de um grupo de administradores enquanto o processo de pesquisa de autenticação é feito. O padrão é Sim - ignorar a pesquisa de membro.

Como localizar o DN de base

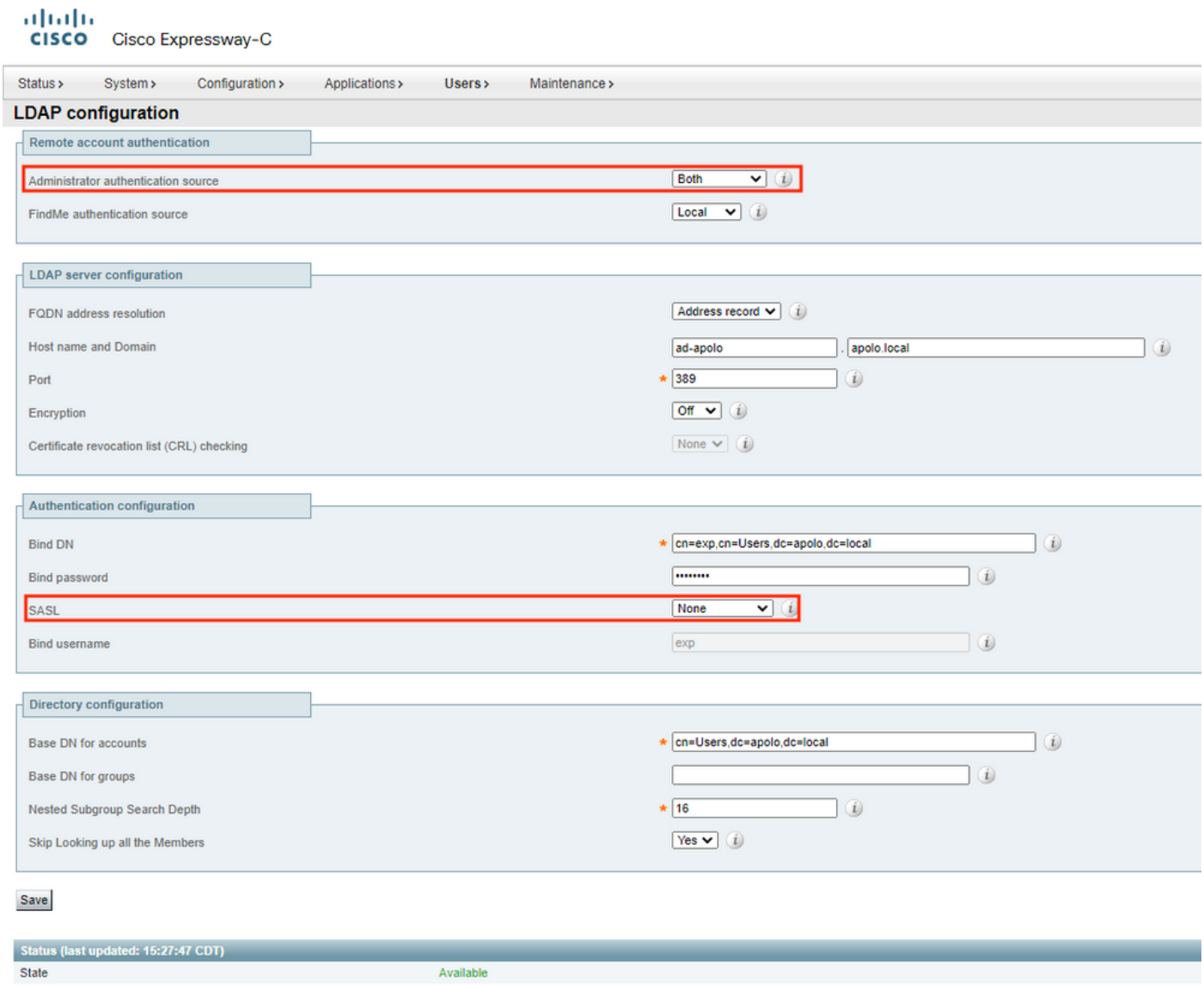
No servidor do AD, abra o Prompt de Comando (CMD) como administrador e execute o comando: **dsquery user -name**

.



Exemplo de configuração LDAP

A origem da autenticação do administrador está definida como Both e SASL está definida como None neste exemplo.



Verificar status LDAP

Validar o status da conexão do servidor LDAP:

- Disponível: Nenhuma mensagem de erro é exibida
- Falha: Mensagens de erro são exibidas. Mensagens de erro LDAP

Configuração de grupos do administrador

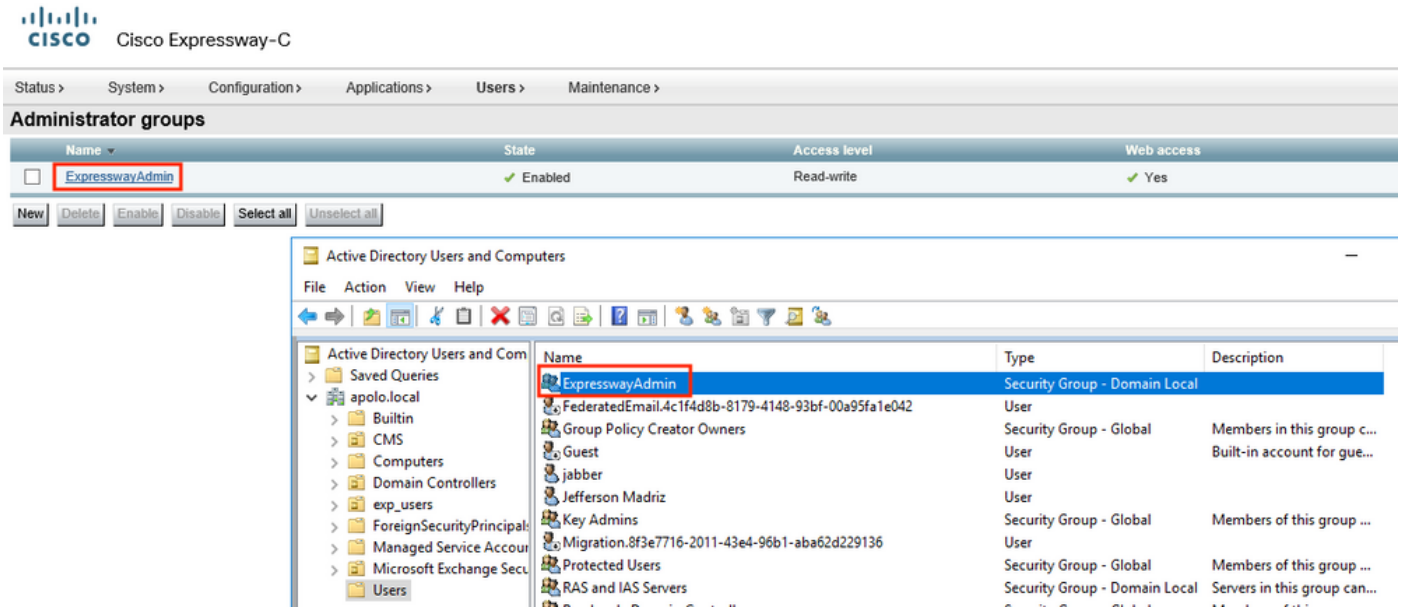
A página Grupos de administradores Usuários > Grupos de administradores lista todos os grupos de administradores que foram configurados no Expressway e permite adicionar, editar e excluir grupos.

Note: Os grupos de administradores só se aplicam se a opção Autenticação de conta remota usando LDAP estiver habilitada.

Quando você faz login na interface da Web do Expressway, suas credenciais são autenticadas no serviço de diretório remoto e você recebe os direitos de acesso associados ao grupo ao qual você pertence.

Opções de configuração de grupos do administrador no Expressway

Nome: O nome do grupo de administradores. Os nomes de grupos definidos no Expressway devem corresponder aos nomes de grupos que foram configurados no serviço de diretório remoto para gerenciar o acesso de administrador a este Expressway.



Nível de acesso:

- Leitura-gravação: Permite que todas as informações de configuração sejam visualizadas e alteradas. Isso fornece os mesmos direitos que a conta de administrador padrão.
- Somente leitura: Permite que as informações de status e configuração sejam visualizadas apenas e não alteradas. Algumas páginas, como a página Atualizar, são bloqueadas para contas somente leitura.
- Auditor: Permite acesso somente às páginas Log de eventos, Log de configuração, Log de rede, Alarmes e Visão geral .
- Nenhum: Nenhum acesso é permitido

Acesso à Web: Determina se os membros desse grupo têm permissão para fazer logon no sistema com a interface da Web.

Acesso à API: Determina se os membros deste grupo têm permissão para acessar o status e a configuração do sistema com a API.

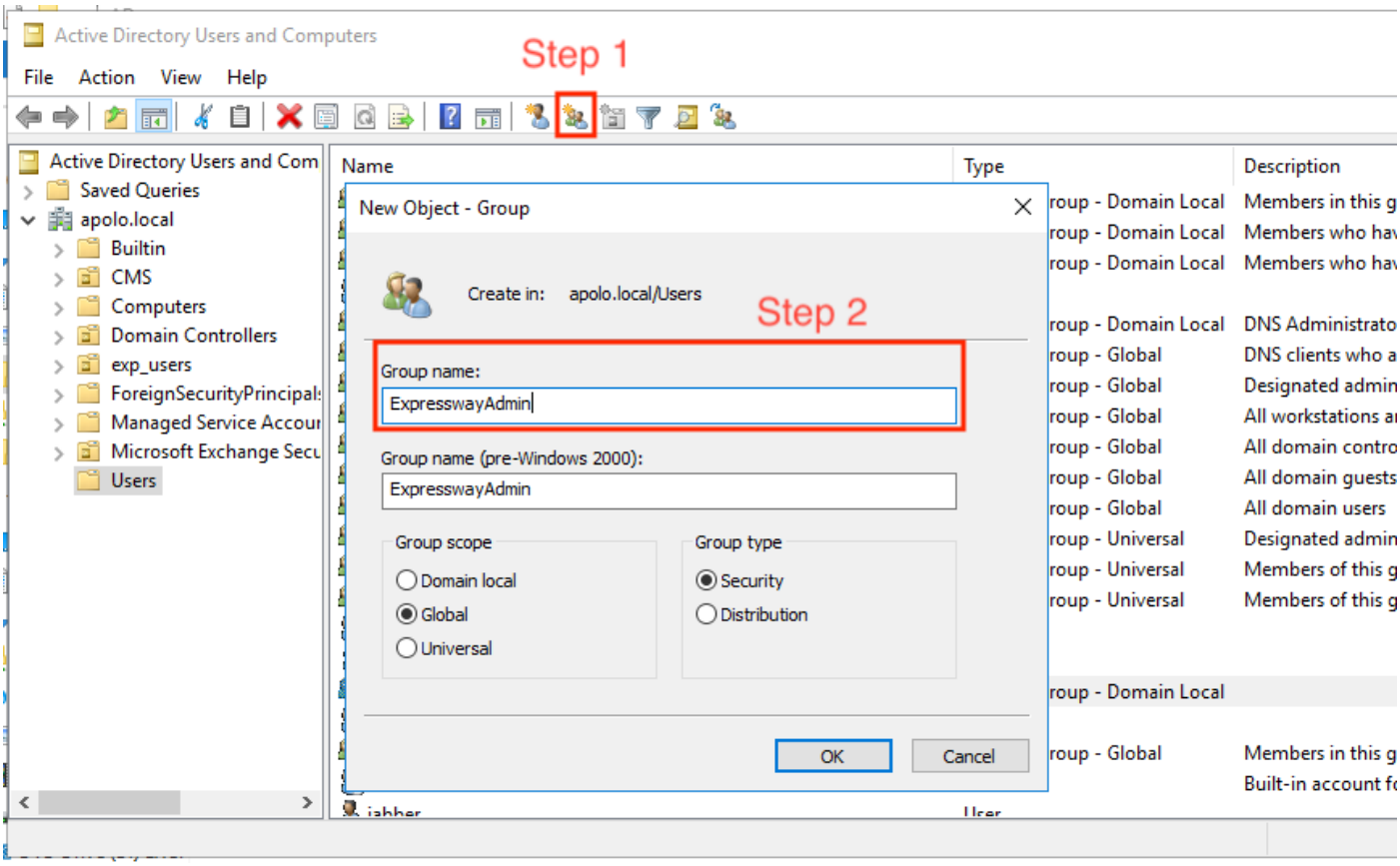
Acesso CLI: Determina se os membros deste grupo têm permissão para acessar o sistema via CLI.

Estado: Indica se o grupo está ativado ou desativado.

Configuração do grupo de administradores no AD

1. Crie um novo Grupo de Objetos, na pasta em que deseja armazenar os usuários.

2. Atribua um nome ao Nome do Grupo.

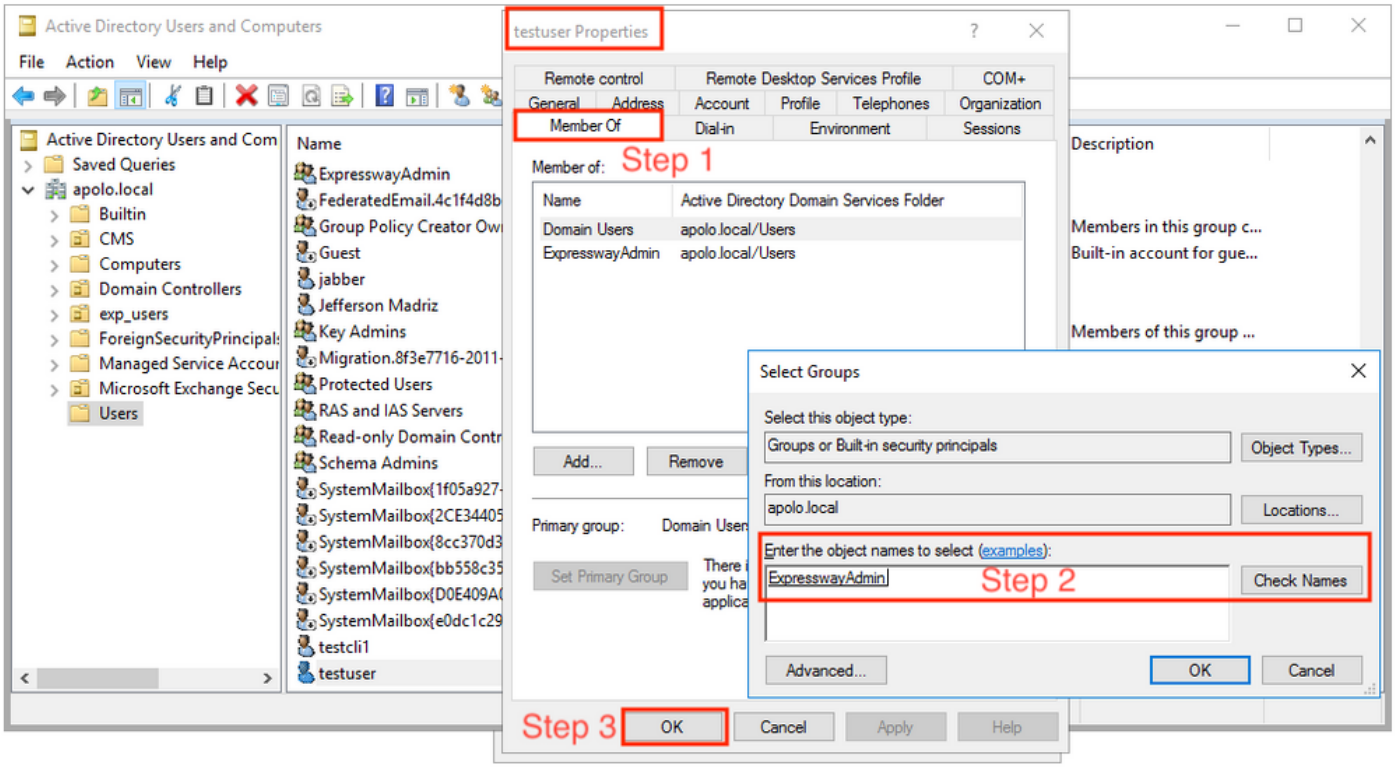


Atribua o grupo configurado aos usuários que precisam acessar o Expressways via Web, API ou CLI. Nesse caso, o usuário é testuser.

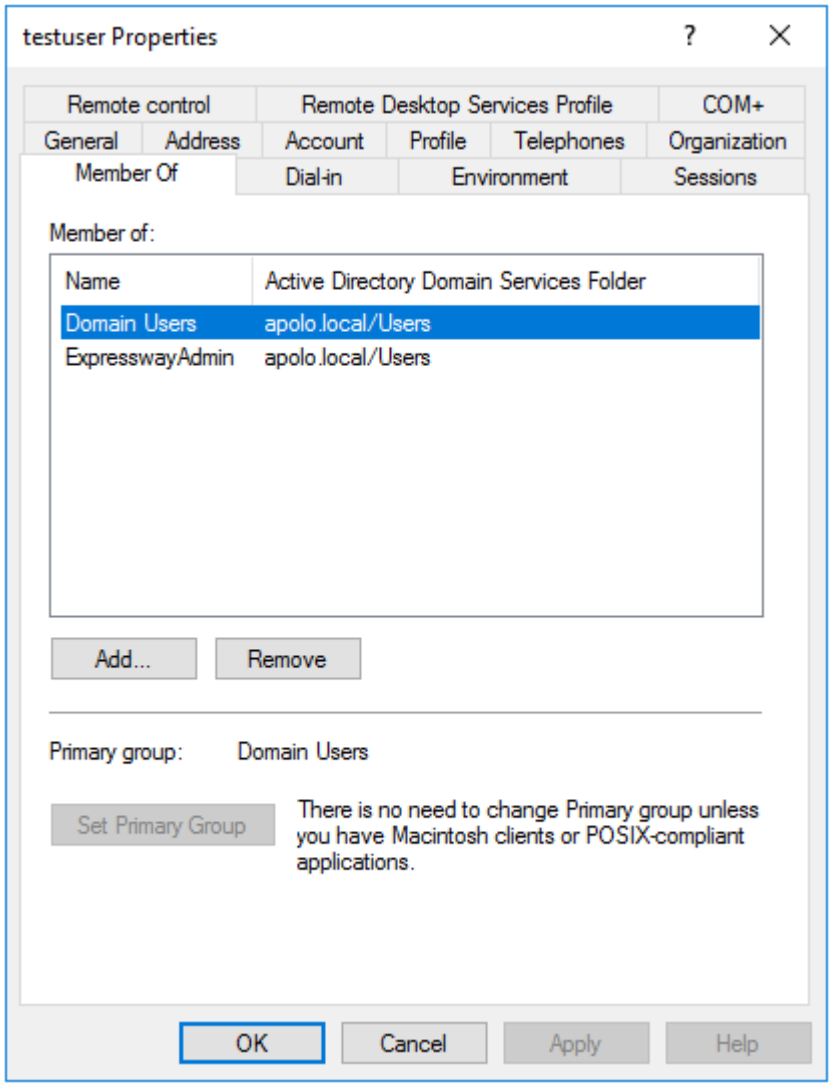
1. Abra as propriedades do usuário, navegue até a guia Membro de, selecione Adicionar

2. Procure o Nome do Grupo criado antes.

3. Em seguida, selecione OK.



Neste ponto, o usuário é membro de Domain Users e ExpresswayAdmin.

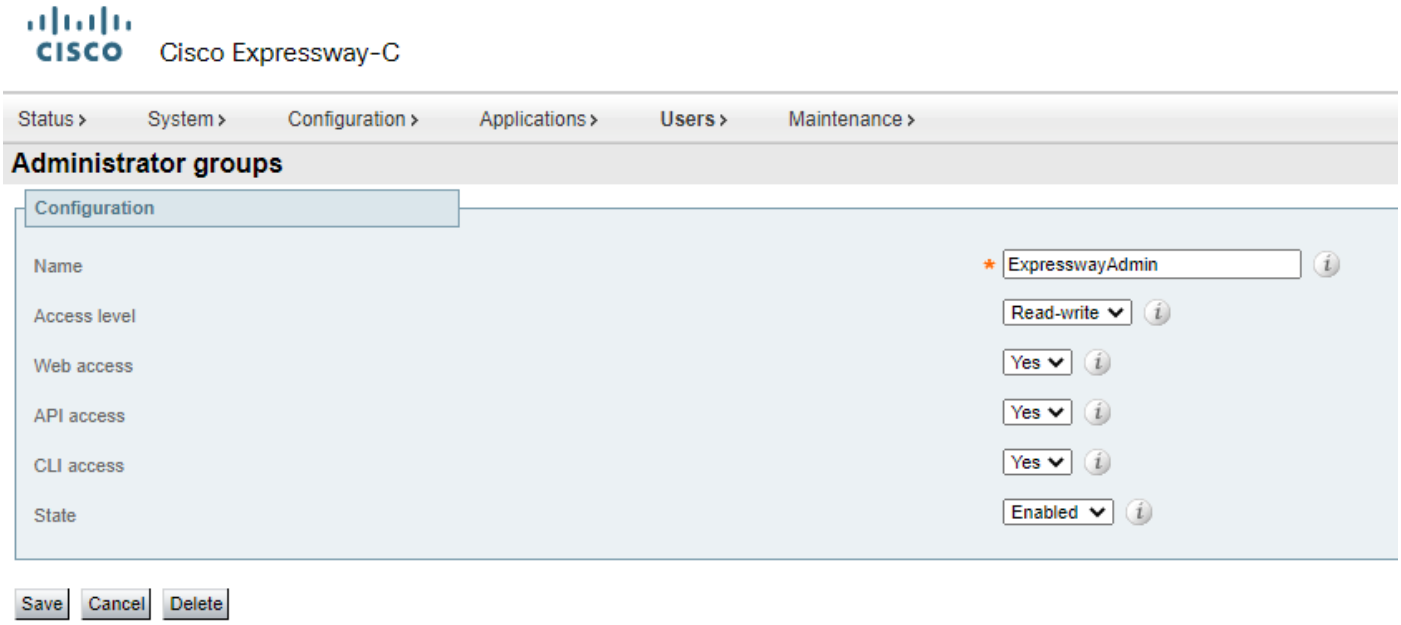


Configuração do grupo de administradores no Expressway

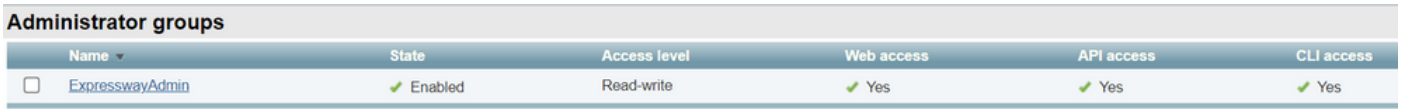
Depois que a configuração estiver concluída, no Expressway, navegue para Users > Administrator groups, selecione New

Nome: deve corresponder ao nome do grupo configurado e associado ao usuário LDAP que precisa acessar o Expressway. Neste exemplo, o nome do grupo é ExpresswayAdmin, então o novo nome do grupo de administradores é ExpresswayAdmin.

Este grupo tem todas as permissões e acesso disponíveis.

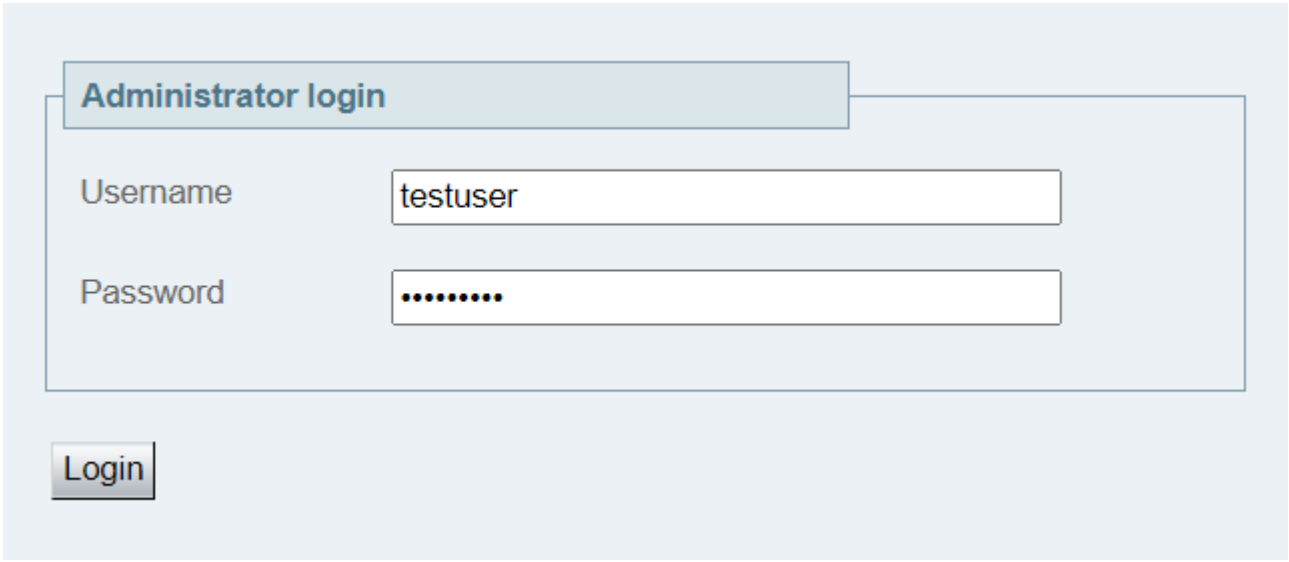


Selecione Save.

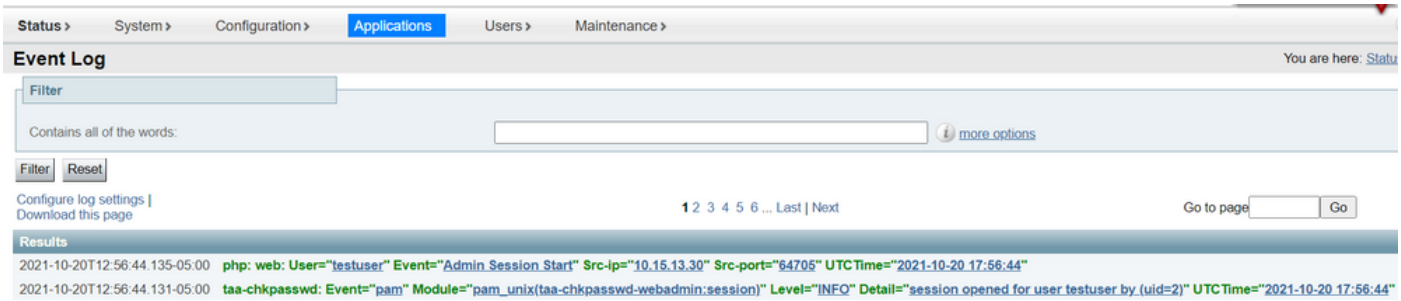


Verificar

Faça logoff e tente acessar via Web com o usuário LDAP que tem o Grupo de administradores associado. Neste exemplo, o usuário criado é testuser.



Isso pode ser confirmado via Status > Event log:



Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.