

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

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuração LDAP](#)

[Como localizar o DN de base](#)

[Exemplo de configuração LDAP](#)

[Configuração de grupos do administrador](#)

[Opções de configuração de grupos do administrador no Expressway](#)

[Configuração do grupo de administradores no AD](#)

[Configuração do grupo de administradores no Expressway](#)

[Verificar](#)

Introdução

Este documento descreve as etapas necessárias para ativar o Lightweight Directory 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 Directory (AD) já configurado.
- Regras de firewall prontas, para permitir a comunicação entre o Expressway e o servidor AD.

Componentes Utilizados

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

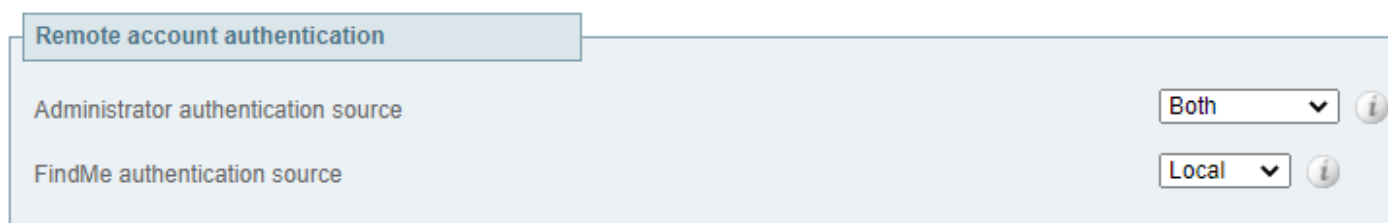
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer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



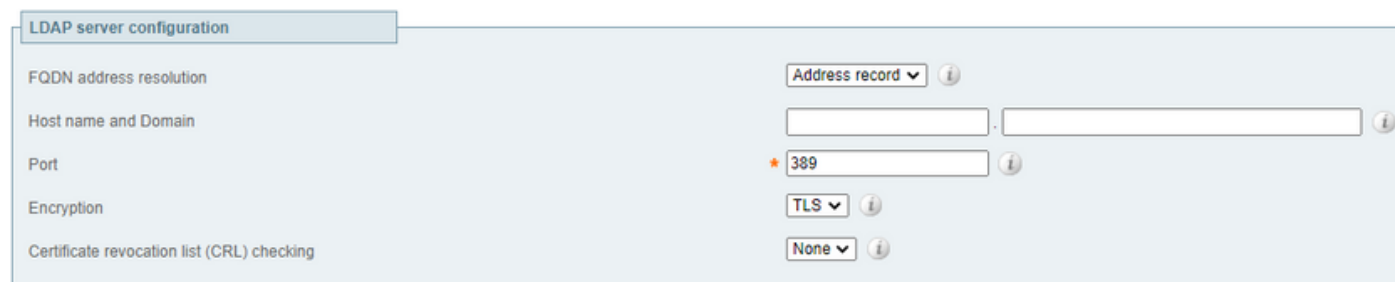
Remote account authentication

Administrator authentication source: Both

FindMe authentication source: Local

- 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.



LDAP server configuration

FQDN address resolution: Address record

Host name and Domain: [] . []

Port: 389

Encryption: TLS

Certificate revocation list (CRL) checking: None

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:

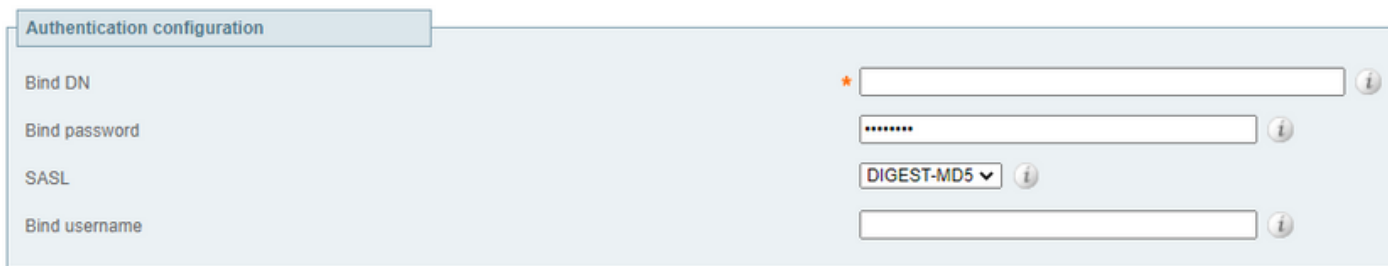
- Registro SRV: somente a parte Domínio do endereço do servidor é necessária.
- Registro de endereço: insira o Nome do host e o Domínio. Eles são combinados para fornecer o endereço completo do servidor para a pesquisa de registro de endereço DNS.
- Endereço IP: o endereço do servidor é inserido diretamente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



The screenshot shows the 'Authentication configuration' section of a web interface. It contains four fields: 'Bind DN' (with a red star icon), 'Bind password' (masked with dots), 'SASL' (a dropdown menu currently showing 'DIGEST-MD5'), and 'Bind username'. Each field has a small information icon to its right.

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.

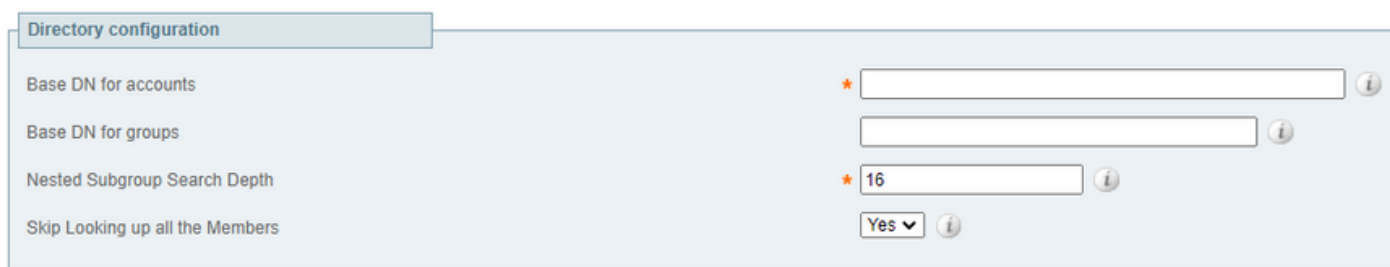
SASL: O mecanismo SASL (Simple Authentication and Security Layer) a ser usado para vincular ao servidor LDAP

- 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 login 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.



Directory configuration

Base DN for accounts *

Base DN for groups *

Nested Subgroup Search Depth 16

Skip Looking up all the Members Yes

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**

```
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>
```

Exemplo de configuração LDAP

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

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

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

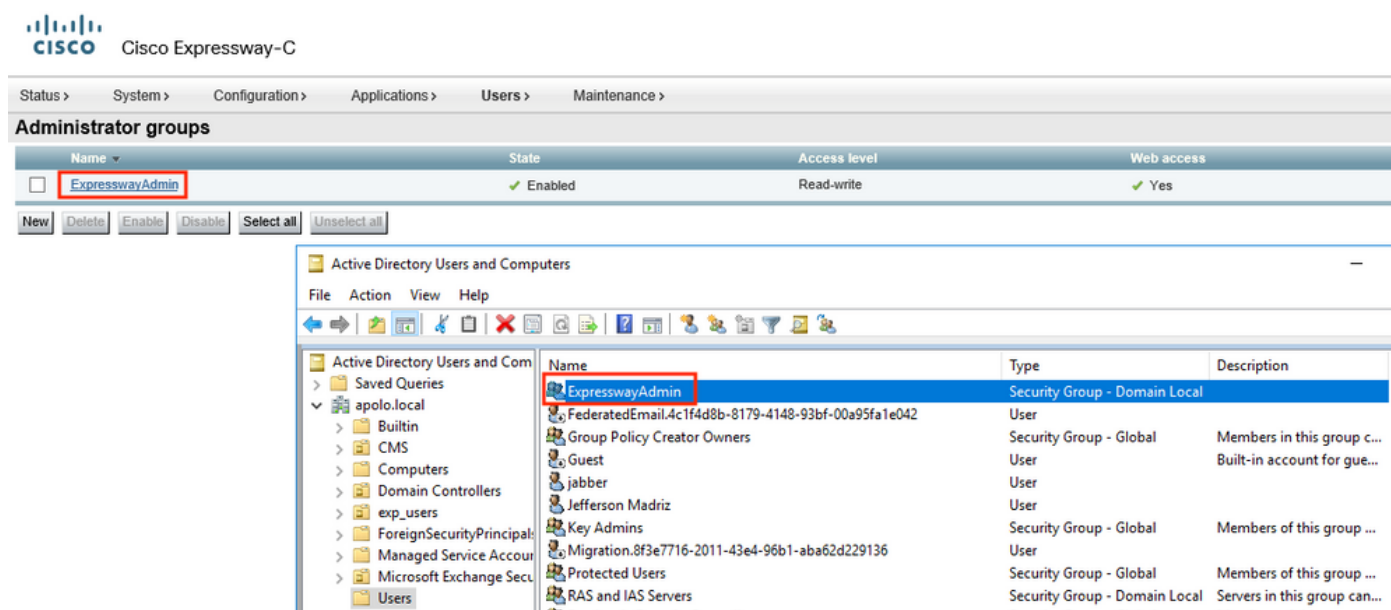
A página Grupos de administradores Usuários > Grupos de administradores lista todos os grupos de administradores que foram configurados no Expressway e permite adicionar, editar e excluir grupos.

 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.



The screenshot displays the Cisco Expressway web interface. At the top, the navigation bar includes 'Status', 'System', 'Configuration', 'Applications', 'Users', and 'Maintenance'. The 'Users' section is active, showing 'Administrator groups'. A table lists the groups, with 'ExpresswayAdmin' highlighted. Below the table, a window titled 'Active Directory Users and Computers' is open, showing a list of groups in the 'Users' container. The 'ExpresswayAdmin' group is highlighted in this list as well.

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...

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 login no sistema com a interface da Web.

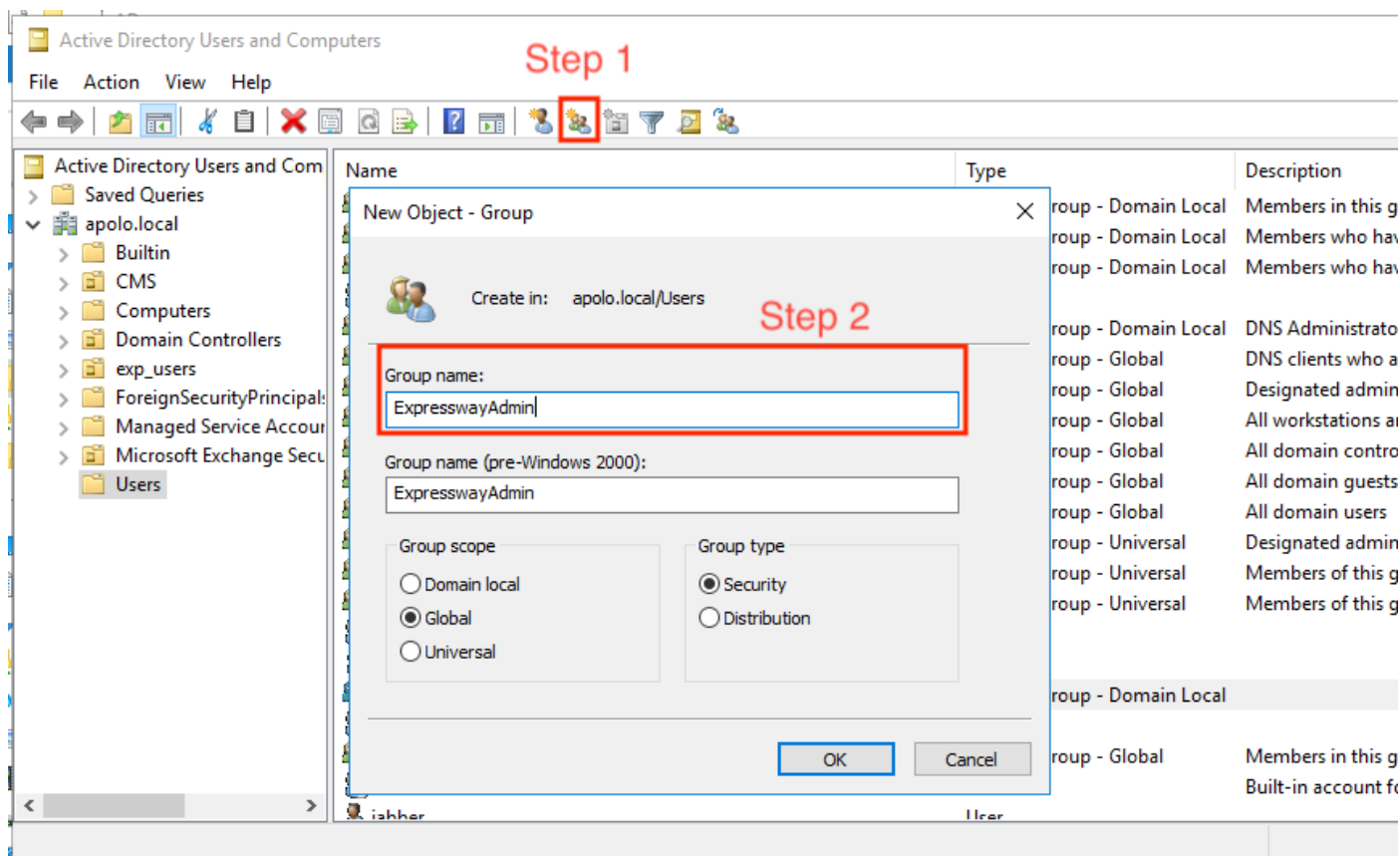
Acesso à API: Determina se os membros deste grupo têm permissão para acessar o status e a configuração do sistema com a API.

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.

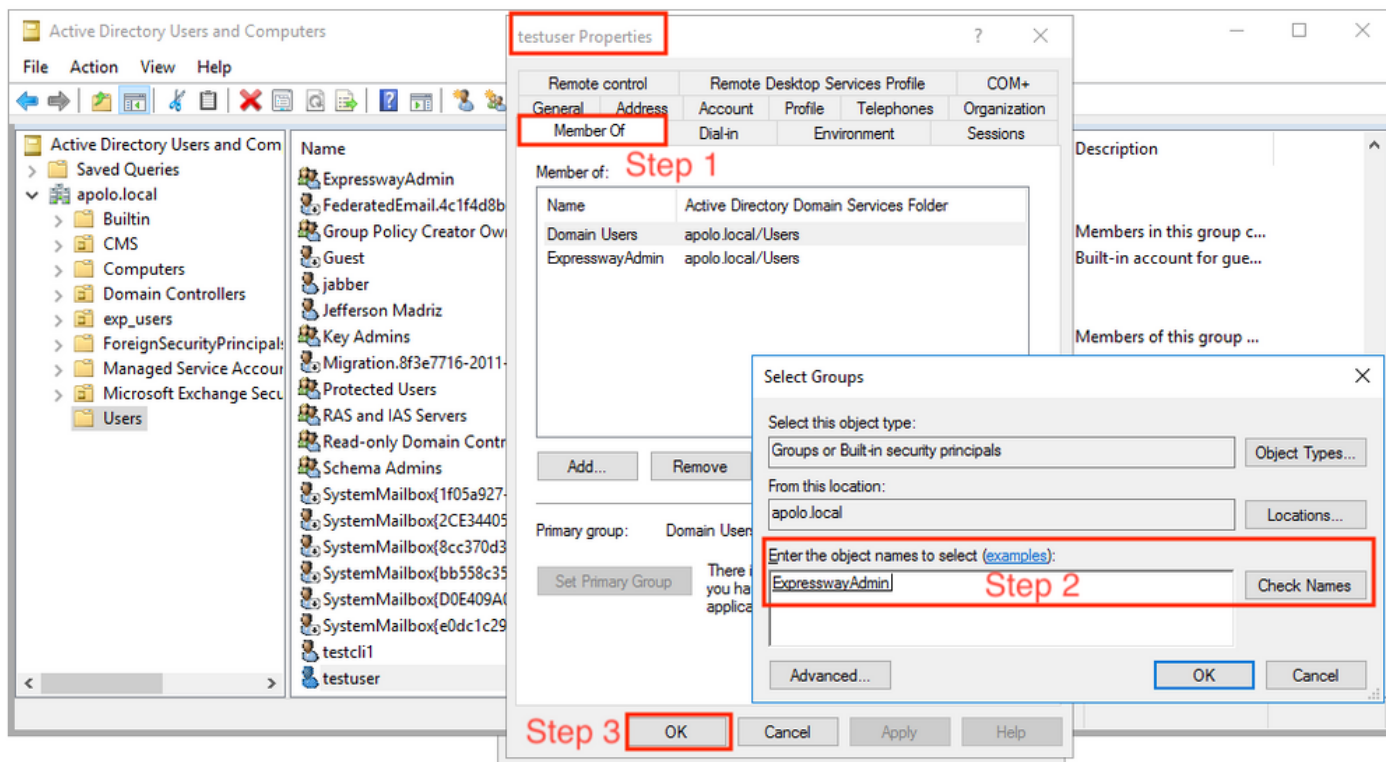
Configuração do grupo de administradores no AD

1. Crie um novo Grupo de Objetos, na pasta em que deseja armazenar os usuários.
2. Atribua um nome ao Nome do Grupo.

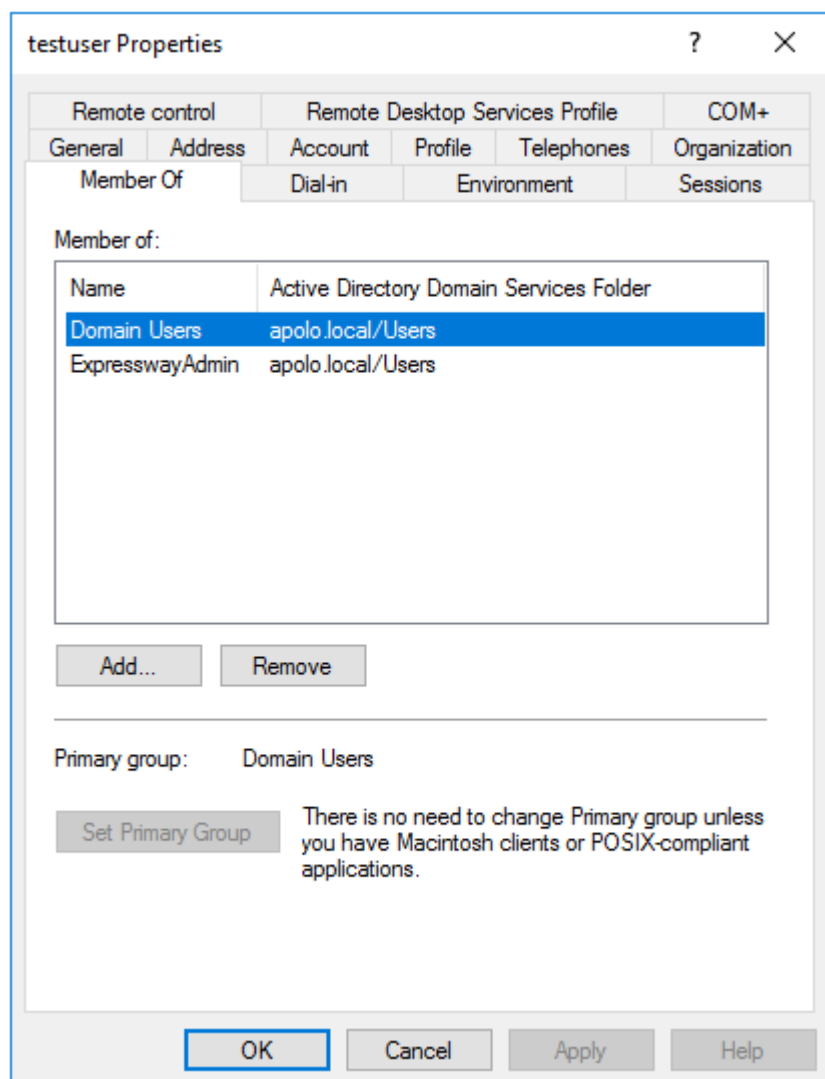


Atribua o grupo configurado aos usuários que precisam acessar o Expressways via Web, API ou CLI. Nesse caso, o usuário é testuser.

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.

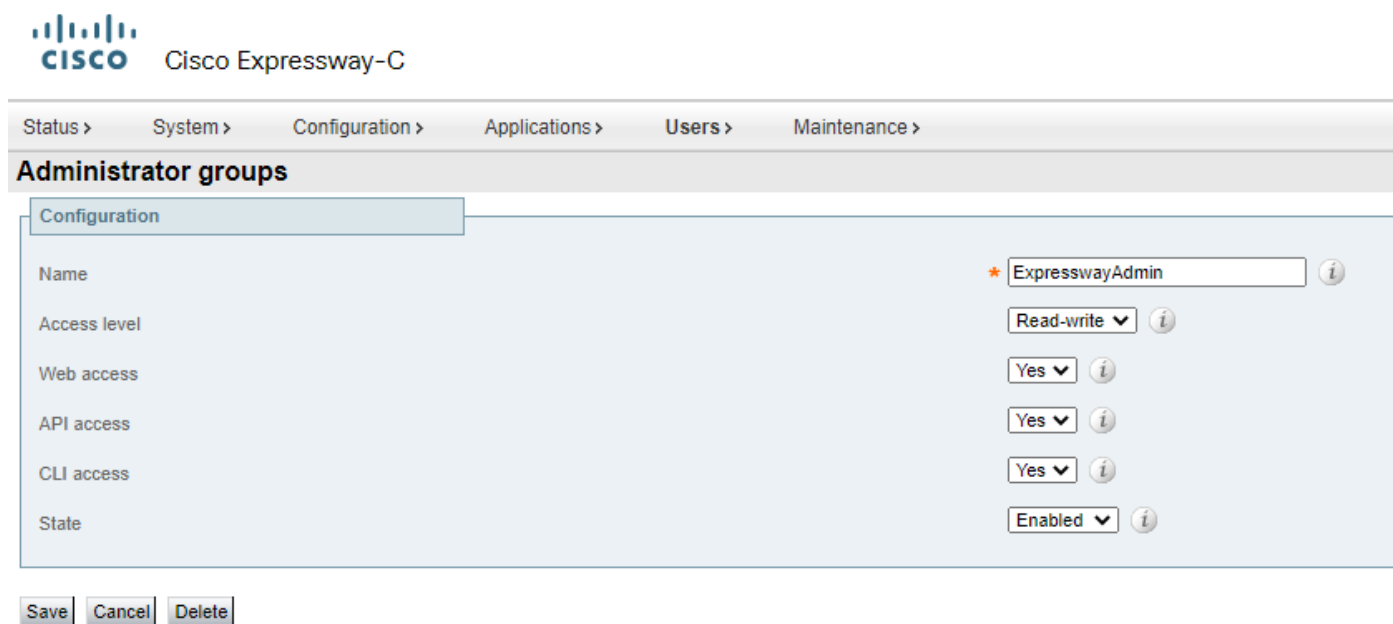


Configuração do grupo de administradores no Expressway

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.



The screenshot shows the Cisco Expressway-C web interface. At the top, there's a navigation bar with tabs: Status >, System >, Configuration >, Applications >, Users >, and Maintenance >. Below this, the 'Administrator groups' section is active. A 'Configuration' tab is selected, showing a form for a new administrator group. The form fields are: Name (set to 'ExpresswayAdmin'), Access level (set to 'Read-write'), Web access (set to 'Yes'), API access (set to 'Yes'), CLI access (set to 'Yes'), and State (set to 'Enabled'). Each field has an information icon (i) to its right. At the bottom of the form are three buttons: Save, Cancel, and Delete.

Selecione Save.

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

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.

Administrator login

Username

testuser

Password

.....

Login

Isso pode ser confirmado via Status > Event log:

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"

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.