

Configurar o WLC com a autenticação LDAP para 802.1x e Web-Auth WLANs

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Experiência técnica](#)

[Perguntas mais freqüentes](#)

[Configurar](#)

[Criar uma WLAN que dependa de um servidor LDAP para autenticar usuários por meio do 802.1x](#)

[Diagrama de Rede](#)

[Criar uma WLAN que depende do servidor LDAP para autenticar usuários através do portal interno da WLC na Web](#)

[Diagrama de Rede](#)

[Usar a ferramenta LDP para configurar e solucionar problemas do LDAP](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve o procedimento para configurar um AireOS WLC para autenticar clientes com um servidor LDAP como o banco de dados de usuários.

Prerequisites

Requirements

A Cisco recomenda o conhecimento destes tópicos:

- Servidores Microsoft Windows
- Diretório ativo

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Software Cisco WLC 8.2.110.0

- Microsoft Windows Server 2012 R2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Experiência técnica

- LDAP é um protocolo usado para acessar servidores de diretório.
- Os servidores de diretório são bancos de dados hierárquicos orientados a objetos.
- Os objetos são organizados em contêineres, como Unidades Organizacionais (OU), Grupos ou Contêineres Microsoft padrão como CN=Usuários.
- A parte mais difícil dessa configuração é configurar os parâmetros do servidor LDAP corretamente no WLC.

Para obter informações mais detalhadas sobre esses conceitos, consulte a seção [Introdução de Como configurar o Wireless Lan Controller \(WLC\) para autenticação LDAP](#).

Perguntas mais freqüentes

- Que nome de usuário deve ser usado para vincular-se ao servidor LDAP?

Há duas maneiras de vincular-se a um servidor LDAP: anônimo ou autenticado (consulte para compreender a diferença entre os dois métodos).

Esse nome de usuário de associação precisa ter privilégios de Administrador para poder consultar outros nomes de usuário/senhas.

- Se autenticado: o nome de usuário de vinculação está dentro do mesmo contêiner que todos os usuários?

Não: use todo o caminho. Por exemplo:

CN=Administrador,CN=Administradores de domínio,CN=Usuários,DC=labm,DC=cisco,DC=com

Sim: use apenas o nome de usuário. Por exemplo:

Administrador

- E se houver usuários em contêineres diferentes? Todos os usuários LDAP sem fio envolvidos precisam estar no mesmo contêiner?

Não, um DN base que inclui todos os contêineres necessários pode ser especificado.

- Quais atributos a WLC deve procurar?

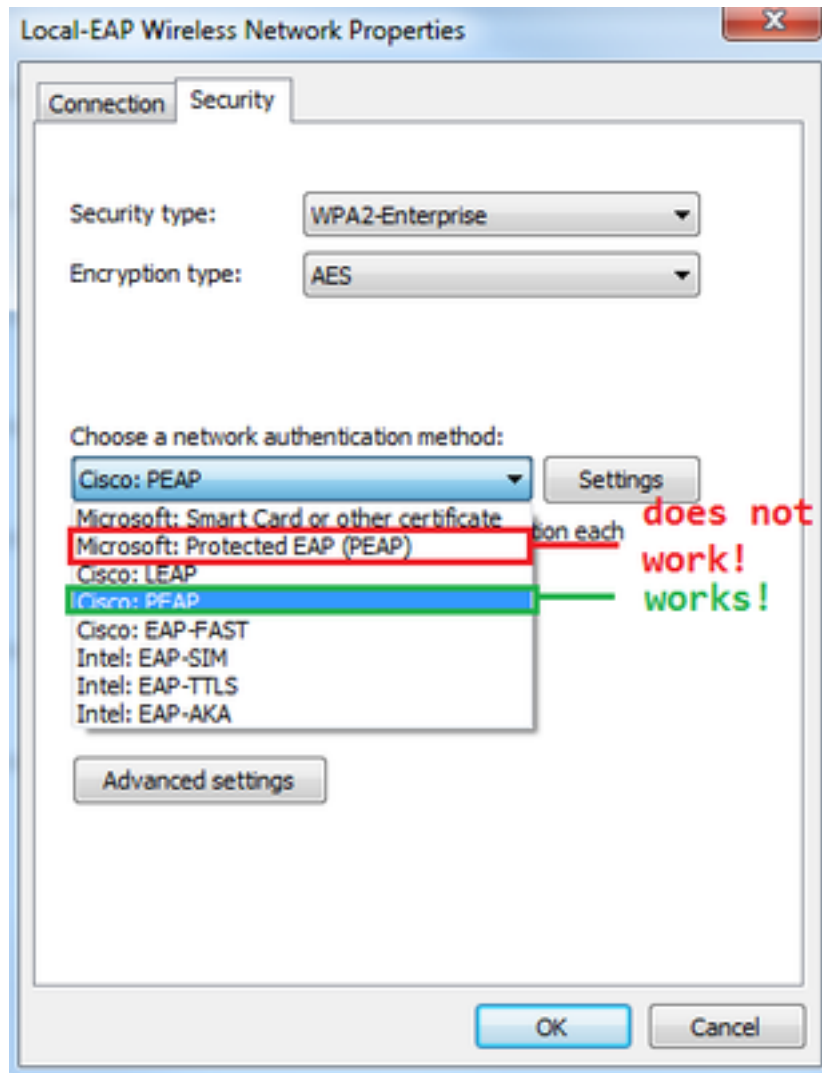
A WLC corresponde ao atributo de usuário e ao tipo de objeto especificados.

Observação: **sAMAccountName** diferencia maiúsculas de minúsculas, mas a pessoa não

diferencia. Portanto, **sAMAccountName=RICARDO** e **sAMAccountName=ricardo** são os mesmos e funcionam enquanto **samaccountname=RICARDO** e **samaccountname=ricardo** não.

- Quais métodos EAP (Extensible Authentication Protocol) podem ser usados?
EAP-FAST, PEAP-GTC e EAP-TLS apenas. Os suplicantes padrão Android, iOS e MacOS trabalham com o PEAP (Protected Extensible Authentication Protocol).

Para Windows, o Anyconnect Network Access Manager (NAM) ou o suplicante padrão do Windows com Cisco:PEAP deve ser usado em adaptadores sem fio suportados, como mostrado na imagem.



Observação: os [plug-ins Cisco EAP](#) para Windows incluem uma versão do Open Secure Socket Layer (OpenSSL 0.9.8k) que é afetada pela ID de bug da Cisco **CSCva09670**, a Cisco não planeja emitir mais nenhuma versão dos plug-ins EAP para Windows e recomenda que os clientes usem o AnyConnect Secure Mobility Client.

- Por que a WLC não consegue encontrar usuários?
Os usuários dentro de um grupo não podem ser autenticados. Eles precisam estar dentro de um CN (Default Container, contêiner padrão) ou de uma OU (Organizational Unit, unidade organizacional), como mostra a imagem.

Name	Type	Description
SofiaLabGroup	Group	Default container for upgr...
SofiaLabOU	Organizational Unit	
Users	Container	

will not work

Configurar

Há diferentes cenários nos quais um servidor LDAP pode ser empregado, com autenticação 802.1x ou autenticação da Web.

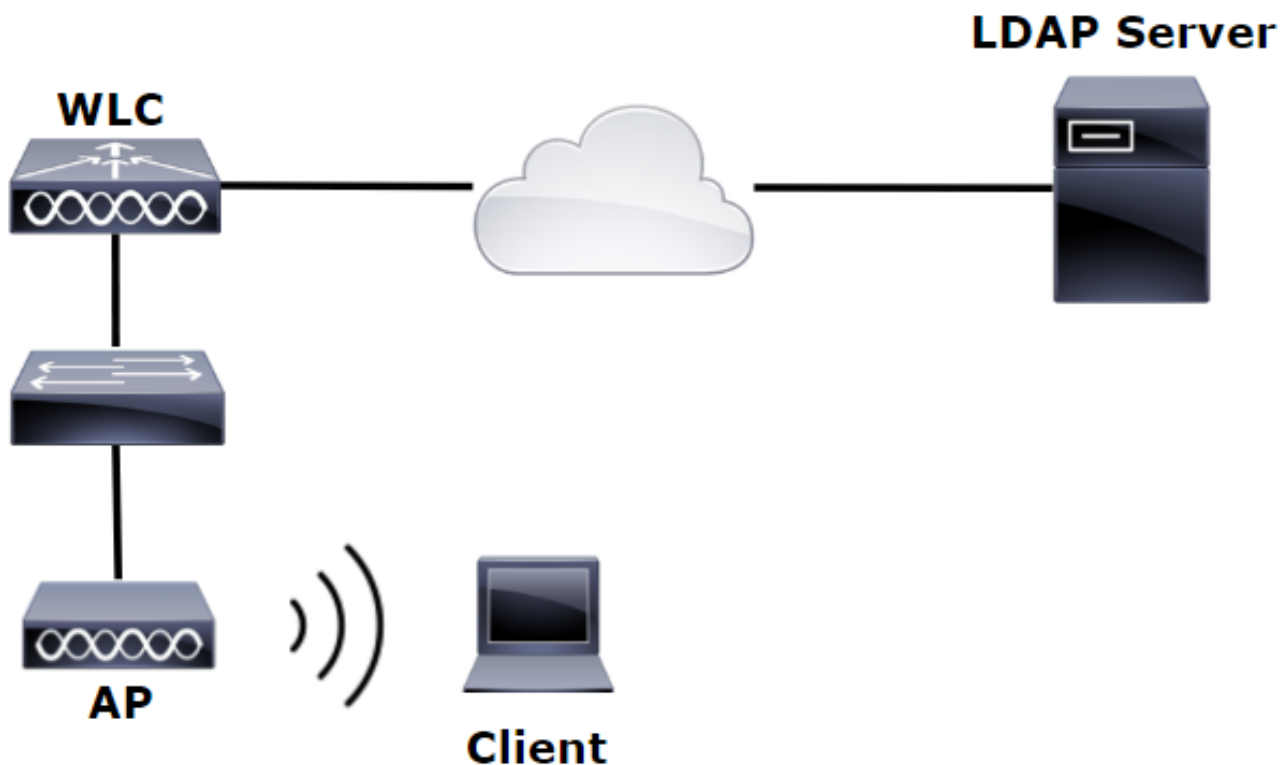
Para este procedimento, somente usuários dentro da OU=SofiaLabOU devem ser autenticados.

Para aprender a usar a ferramenta Label Distribution Protocol (LDP), configurar e solucionar problemas do LDAP, consulte o [Guia de Configuração LDAP da WLC](#).

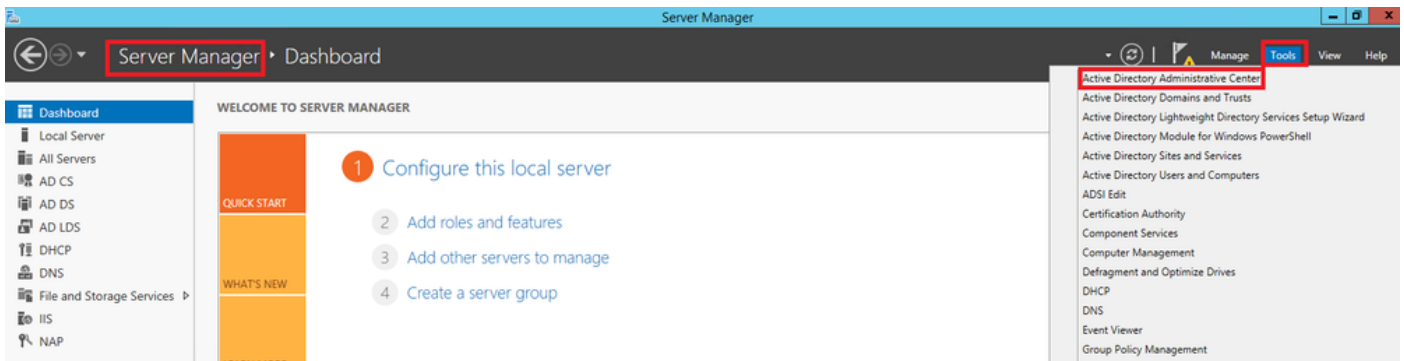
Criar uma WLAN que dependa de um servidor LDAP para autenticar usuários por meio do 802.1x

Diagrama de Rede

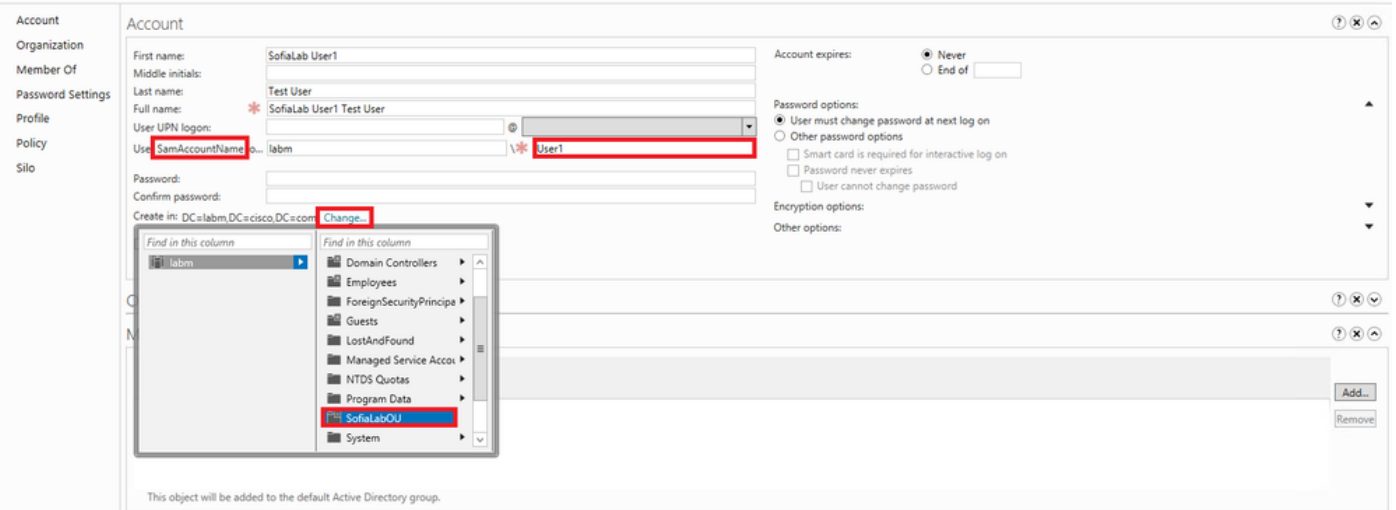
Neste cenário, o LDAP-dot1x da WLAN usa um servidor LDAP para autenticar os usuários com o uso de 802.1x.



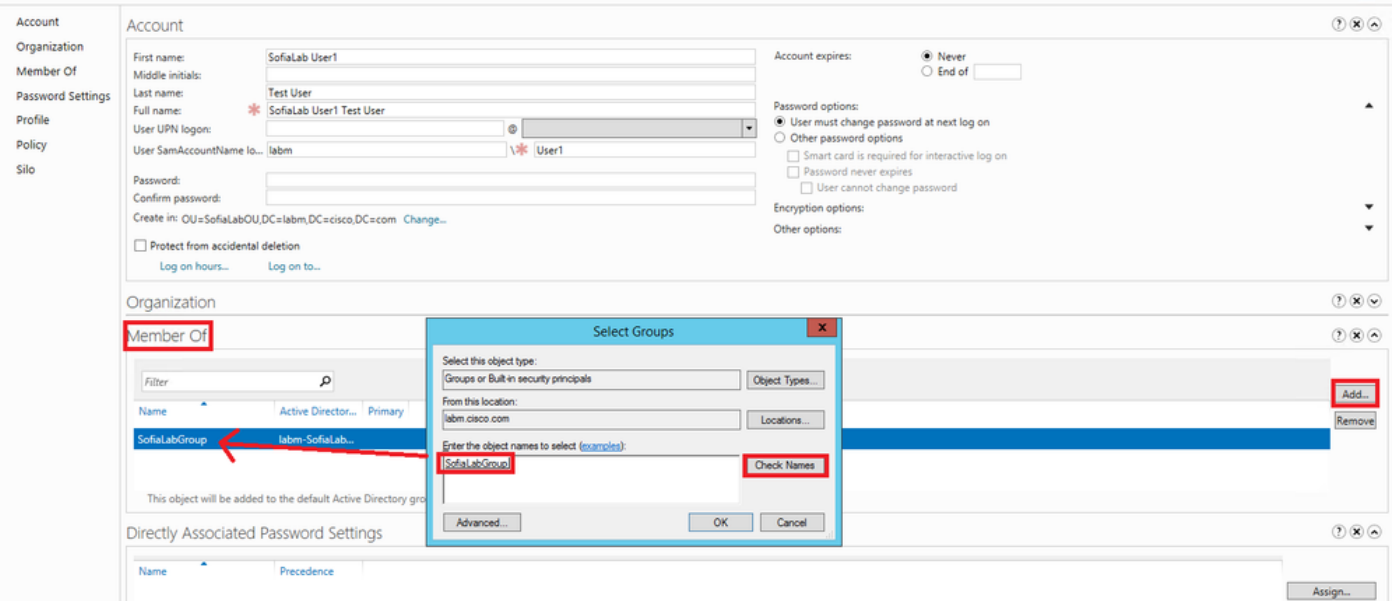
Etapa 1. Crie um usuário **User1** no servidor LDAP membro do SofiaLabOU e SofiaLabGroup.



Create User: SofiaLab User1 Test User



Create User: SofiaLab User1 Test User



Etapa 2. Crie um perfil EAP na WLC com o método EAP desejado (use PEAP).

Profile Name	LEAP	EAP-FAST	EAP-TLS	PEAP
Local-EAP-PEAP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Local-EAP-LEAP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

LEAP	Server Nothing	Client Username & Password
EAP-FAST	Server PAK	Client Username & Password
EAP-TLS	Server Certificate	Client Certificate
PEAP	Server Certificate	Client Username & Password

Etapa 3. Vincule a WLC ao servidor LDAP.

Dica: se o nome de usuário de vinculação não estiver no DN de base do usuário, você terá que gravar o caminho inteiro para o **usuário Admin** como mostrado na imagem. Caso contrário, basta digitar **Administrator**.

Admin privileges required

Where are we going to look for users?

What Attribute are we looking for?

Message from webpage
Warning: LDAP can only be used with EAP-FAST, PEAP-GTC and EAP-TLS methods

Etapa 4. Defina a Ordem de autenticação a ser definida como Usuários internos + LDAP ou LDAP apenas.

The screenshot shows the Cisco Security configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', and 'SECURITY' (highlighted with a red box). The left sidebar shows the 'Security' menu with 'AAA' expanded to 'TACACS+' and 'Local EAP' expanded to 'Authentication Priority' (highlighted with a red box). The main content area is titled 'Priority Order > Local-Auth' and 'User Credentials'. It features two columns: 'Not Used' and 'Order Used For Authentication'. The 'Order Used For Authentication' column contains a box labeled 'LOCAL' and 'LDAP' (highlighted with a red box). Navigation buttons '>' and '<' are between the columns, and 'Up' and 'Down' buttons are to the right.

Etapa 5. Crie a WLAN LDAP-dot1x.

The screenshot shows the Cisco WLANs configuration interface. The top navigation bar includes 'MONITOR', 'WLANs' (highlighted with a red box), 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar shows the 'WLANs' menu with 'WLANs' (highlighted with a red box) and 'Advanced'. The main content area is titled 'WLANs' and shows 'Current Filter: None' with links for '[Change Filter]' and '[Clear Filter]'. A 'Create New' button with a dropdown arrow and a 'Go' button are highlighted with a red box. Below is a table header with columns: 'WLAN ID', 'Type', 'Profile Name', 'WLAN SSID', 'Admin Status', and 'Security Policies'.

CISCO

MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs

WLANs > Edit 'LDAP-dot1x'

General Security QoS Policy-Mapping Advanced

Profile Name LDAP-dot1x

Type WLAN

SSID LDAP-dot1x

Status Enabled

Security Policies [WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy All

Interface/Interface Group(G) vlan2562

Multicast Vlan Feature Enabled

Broadcast SSID Enabled

NAS-ID none

Etapa 6. Defina o método de segurança de L2 como WPA2 + 802.1x e defina a segurança de L3 como nenhum.

CISCO

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEM

WLANs

WLANs > Edit 'LDAP-dot1x'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security WPA+WPA2

MAC Filtering

Fast Transition

Fast Transition

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy

WPA2 Policy

WPA2 Encryption AES TKIP

Authentication Key Management

802.1X Enable

CCKM Enable

PSK Enable

FT 802.1X Enable

FT PSK Enable

WPA gtk-randomize State Disable

Passo 7. Habilite a autenticação EAP local e verifique se as opções Servidores de autenticação e Servidores de contabilização estão desabilitadas e se o LDAP está habilitado.

The screenshot shows the Cisco WLC configuration interface for the WLAN 'LDAP-dot1x'. The 'Security' tab is selected, and the 'AAA Servers' sub-tab is active. The configuration is as follows:

- Authentication Servers:** All six servers (Server 1 to Server 6) have their 'Enabled' checkboxes unchecked.
- Accounting Servers:** All six servers (Server 1 to Server 6) have their 'Enabled' checkboxes unchecked.
- RADIUS Server Accounting:** The 'Interim Update' checkbox is unchecked.
- LDAP Servers:** Server 1 is configured with 'IP:10.88.173.121, Port:389'. Servers 2 and 3 are set to 'None'.
- Local EAP Authentication:** The 'Local EAP Authentication' checkbox is checked (Enabled), and the 'EAP Profile Name' is set to 'Local-EAP-PEAP'.
- Authentication priority order for web-auth user:** The order is LOCAL, RADIUS, and LDAP.

Todas as outras configurações podem ser deixadas como padrão.

Notas:

Use a ferramenta LDP para confirmar os parâmetros de configuração.

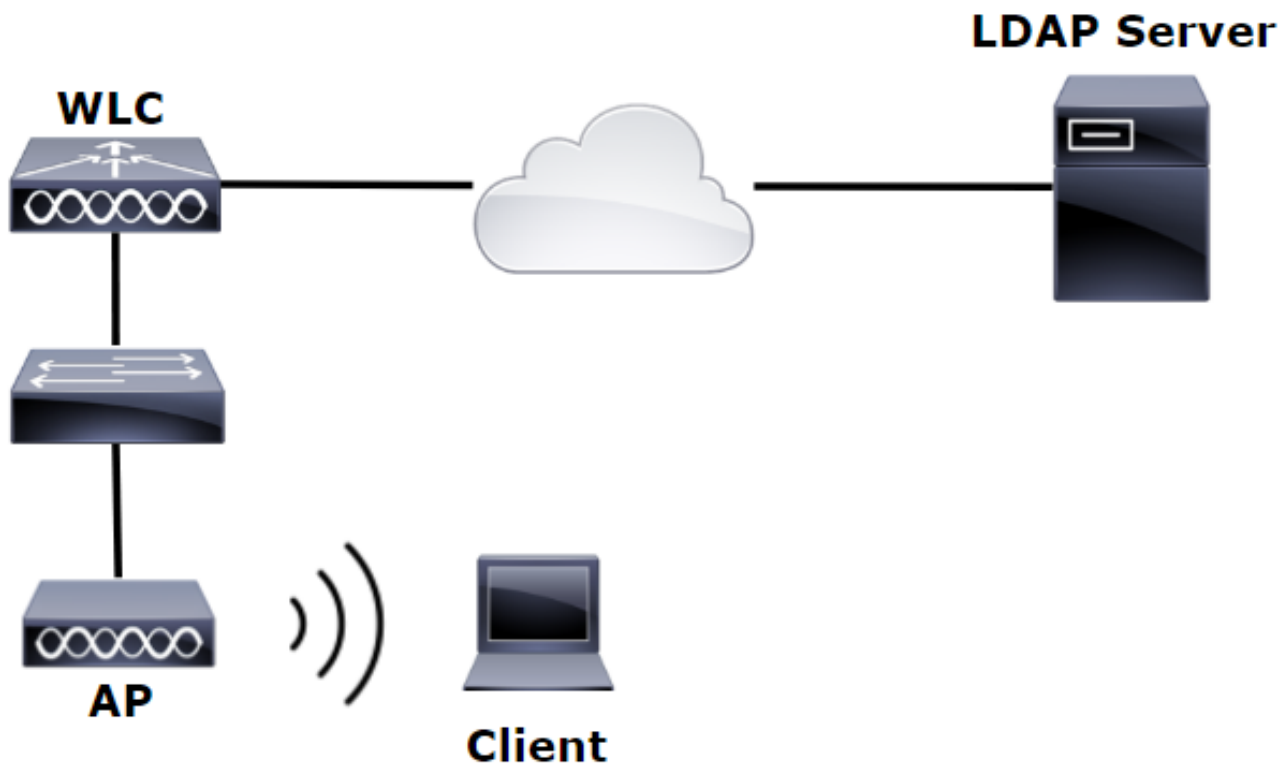
A base de pesquisa não pode ser um grupo (como SofiaLabGroup).

PEAP-GTC ou Cisco:PEAP devem ser usados em vez de Microsoft:PEAP no solicitante, se for uma máquina com Windows. Microsoft:O PEAP funciona por padrão com MacOS/iOS/Android.

Criar uma WLAN que depende do servidor LDAP para autenticar usuários através do portal interno da WLC na Web

Diagrama de Rede

Neste cenário, WLAN LDAP-Web usa um servidor LDAP para autenticar os usuários com o Portal Web da WLC interno.



Verifique se as Etapas 1 a 4 foram retiradas do exemplo anterior. A partir daí, a configuração da WLAN é definida de forma diferente.

Etapa 1. Crie um usuário **User1** no membro do servidor LDAP da OU SofiaLabOU e do Grupo SofiaLabGroup.

Etapa 2. Crie um perfil EAP na WLC com o método EAP desejado (use PEAP).

Etapa 3. Vincule a WLC ao servidor LDAP.

Etapa 4. Defina a Ordem de autenticação a ser definida como Usuários internos + LDAP.

Etapa 5. Crie a WLAN LDAP-Web conforme mostrado nas imagens.



The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar shows 'WLANs' with sub-items 'WLANs' and 'Advanced'. The main content area is titled 'WLANs > Edit 'LDAP-Web'' and has tabs for 'General', 'Security', 'QoS', 'Policy-Mapping', and 'Advanced'. The 'General' tab is active, showing the following configuration:

Profile Name	LDAP-Web
Type	WLAN
SSID	LDAP-Web
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	vlan2562
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
NAS-ID	none

Etapa 6. Defina a segurança de L2 como none e a segurança de L3 como política da Web - autenticação como mostrado nas imagens.

The screenshot shows the Cisco WLAN configuration interface, specifically the 'Security' tab for 'LDAP-Web'. The 'Security' tab is active, and the 'Layer 2' sub-tab is selected. The configuration for Layer 2 is as follows:

Layer 2 Security	None
MAC Filtering	<input type="checkbox"/>
Fast Transition	<input type="checkbox"/>

The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar shows 'WLANs' with sub-items 'WLANs' and 'Advanced'. The main content area is titled 'WLANs > Edit 'LDAP-Web''. It features several tabs: 'General', 'Security', 'QoS', 'Policy-Mapping', and 'Advanced'. Under the 'Security' tab, there are sub-tabs for 'Layer 2', 'Layer 3', and 'AAA Servers'. The 'Layer 3' sub-tab is active, showing 'Layer 3 Security' set to 'Web Policy'. Below this, the 'Authentication' radio button is selected. Other options include 'Passthrough', 'Conditional Web Redirect', 'Splash Page Web Redirect', and 'On MAC Filter failure'. There are also dropdown menus for 'Preauthentication ACL' (IPv4: None, IPv6: None, WebAuth FlexAcl: None) and a checkbox for 'Sleeping Client' (disabled). At the bottom, the 'Over-ride Global Config' checkbox is checked and enabled, and the 'Web Auth type' is set to 'Internal'. Red boxes highlight the 'Security' tab, 'Layer 3' sub-tab, 'Web Policy' dropdown, 'Authentication' radio button, and the 'Over-ride Global Config' and 'Web Auth type' section.

Passo 7. Defina a ordem de prioridade de Autenticação para que a autenticação da Web use LDAP e verifique se as opções Servidores de Autenticação e Servidores de Contabilização estão desabilitadas.

The screenshot shows the Cisco configuration interface for a WLAN named 'LDAP-Web'. The 'Security' tab is selected, and the 'AAA Servers' sub-tab is active. The configuration includes:

- RADIUS Servers:** A checkbox for 'RADIUS Server Overwrite interface' is checked (Enabled).
- Authentication Servers:** A checkbox for 'Enabled' is checked.
- Accounting Servers:** A checkbox for 'Enabled' is checked.
- RADIUS Server Accounting:** An 'Interim Update' checkbox is unchecked.
- LDAP Servers:** 'Server 1' is configured with 'IP:10.88.173.121, Port:389'. Servers 2 and 3 are set to 'None'.
- Local EAP Authentication:** A checkbox for 'Enabled' is unchecked.
- Authentication priority order for web-auth user:** A list shows 'RADIUS' as 'Not Used' and 'LDAP' as 'Order Used For Authentication'. The 'LDAP' entry is highlighted in the search results.

Todas as outras configurações podem ser deixadas como padrão.

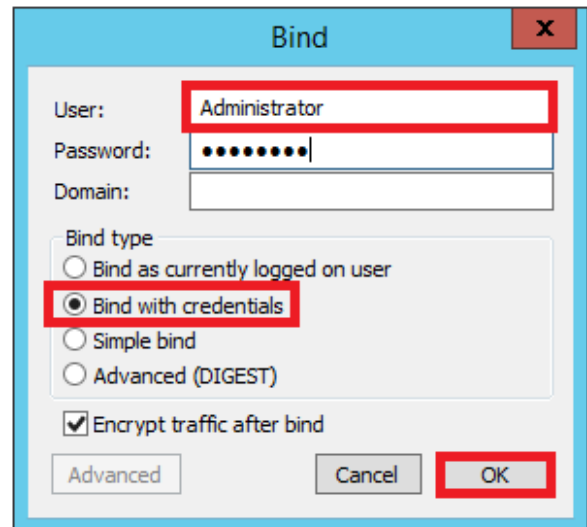
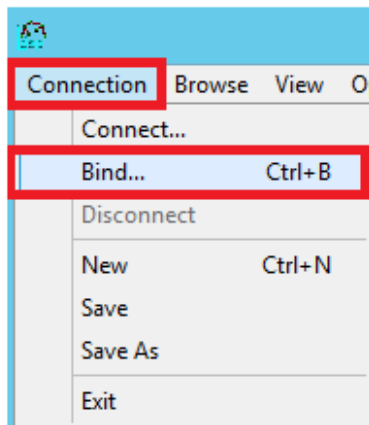
Usar a ferramenta LDP para configurar e solucionar problemas do LDAP

Etapa 1. Abra a ferramenta LDP no servidor LDAP ou em um host com conectividade (a porta TCP 389 deve ser permitida para o servidor).

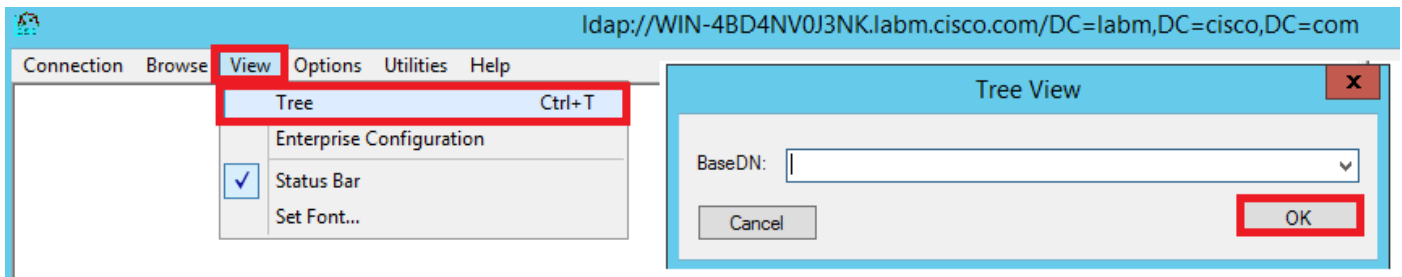
The screenshot shows the Windows Start menu search interface. The search bar contains the text 'ldp'. The search results show a single entry for 'ldp' with a red box highlighting the search results area.

Etapa 2. Navegue até **Connection > Bind**, efetue login com um usuário Admin e selecione o botão

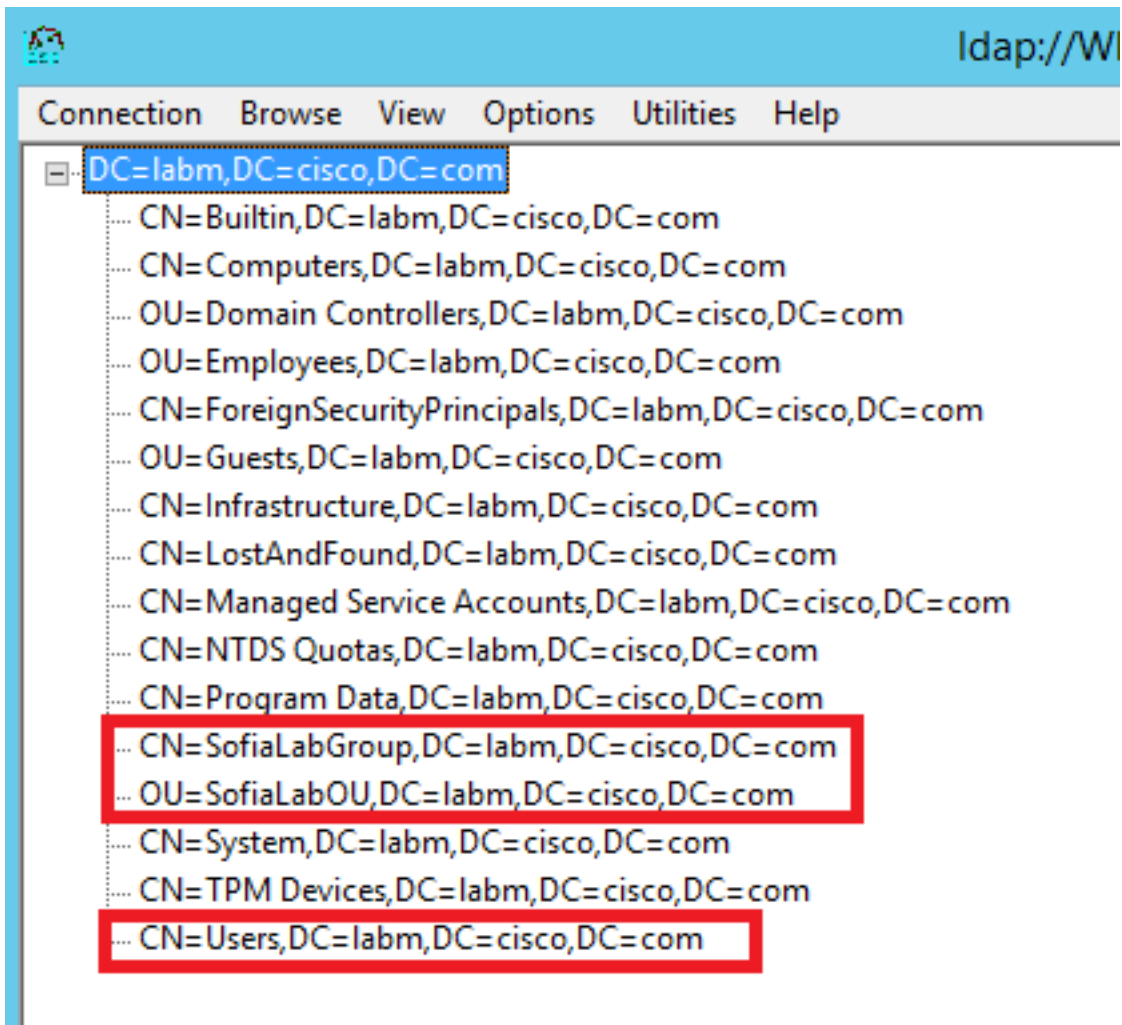
de opção **Bind with credentials**.



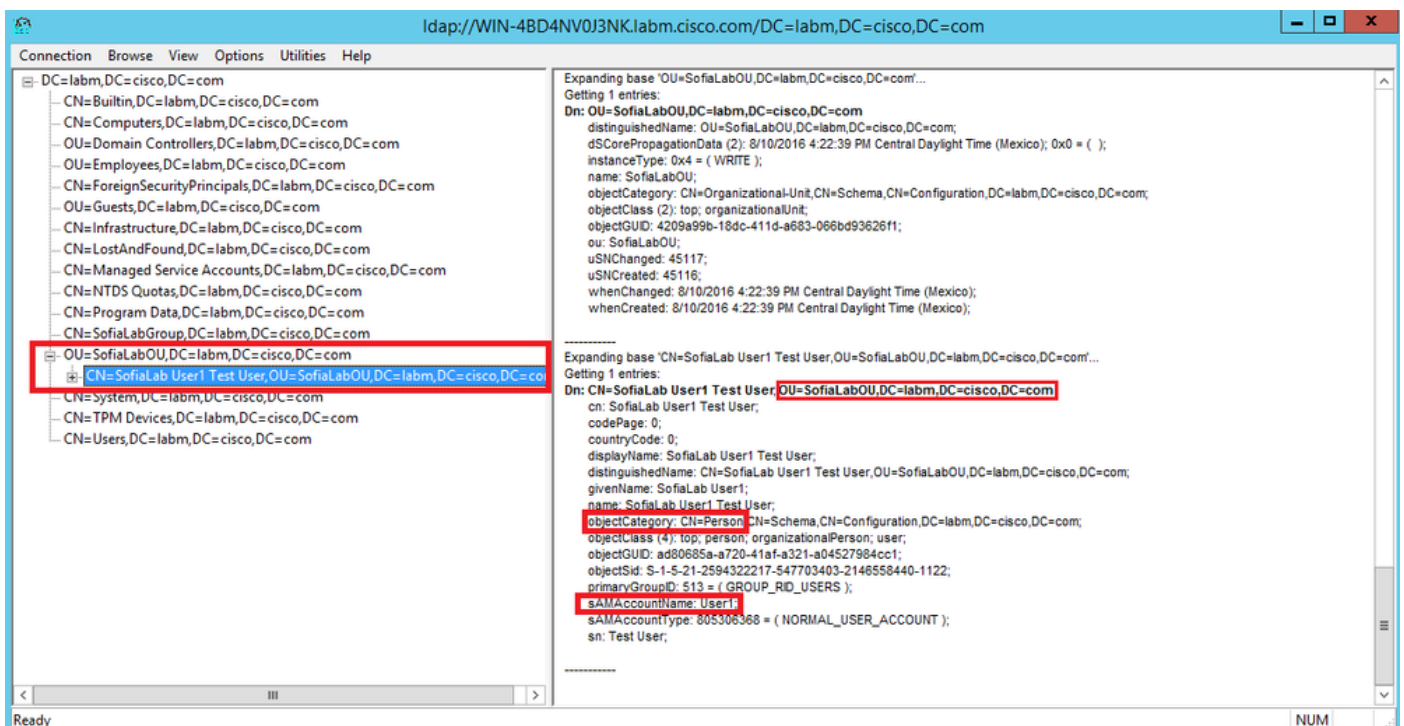
Etapa 3. Navegue até **View > Tree** e selecione **OK** no DN base.



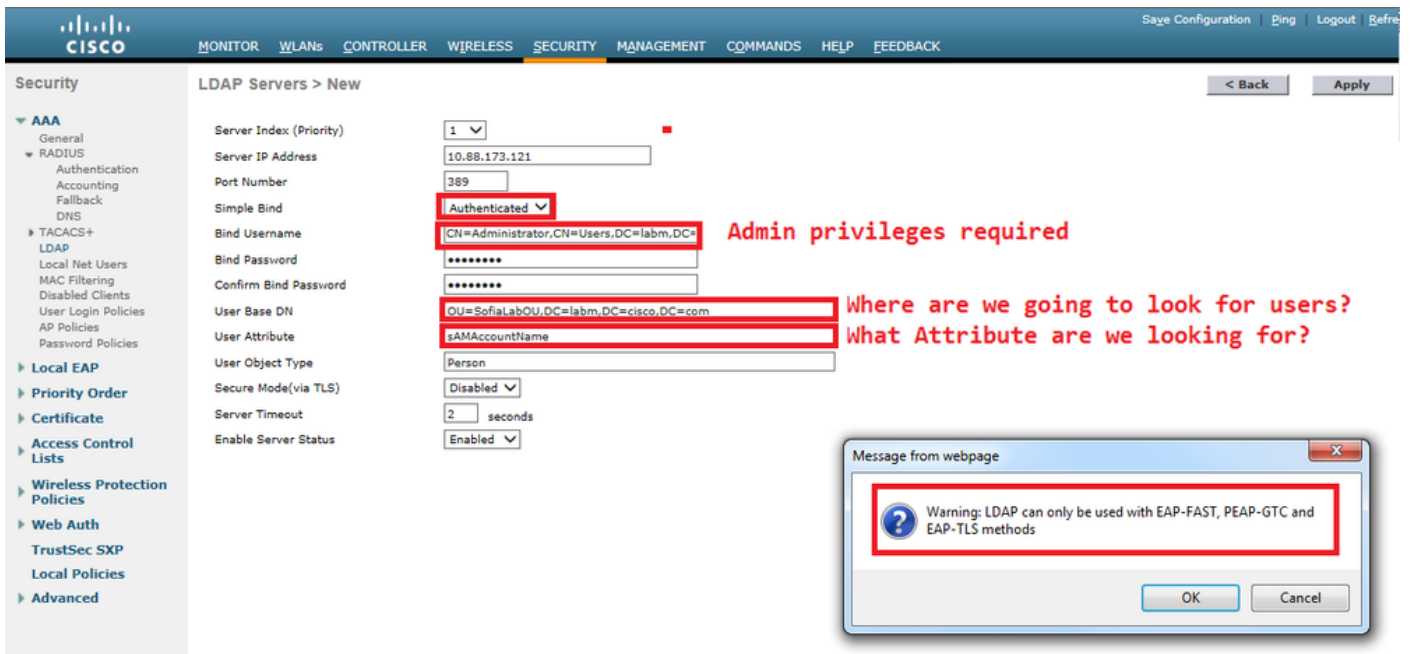
Etapa 4. Expanda a árvore para exibir a estrutura e procurar o DN de base de pesquisa. Considere que pode ser qualquer tipo de contêiner, exceto Grupos. Pode ser o domínio inteiro, uma OU específica ou um CN como CN=Users.



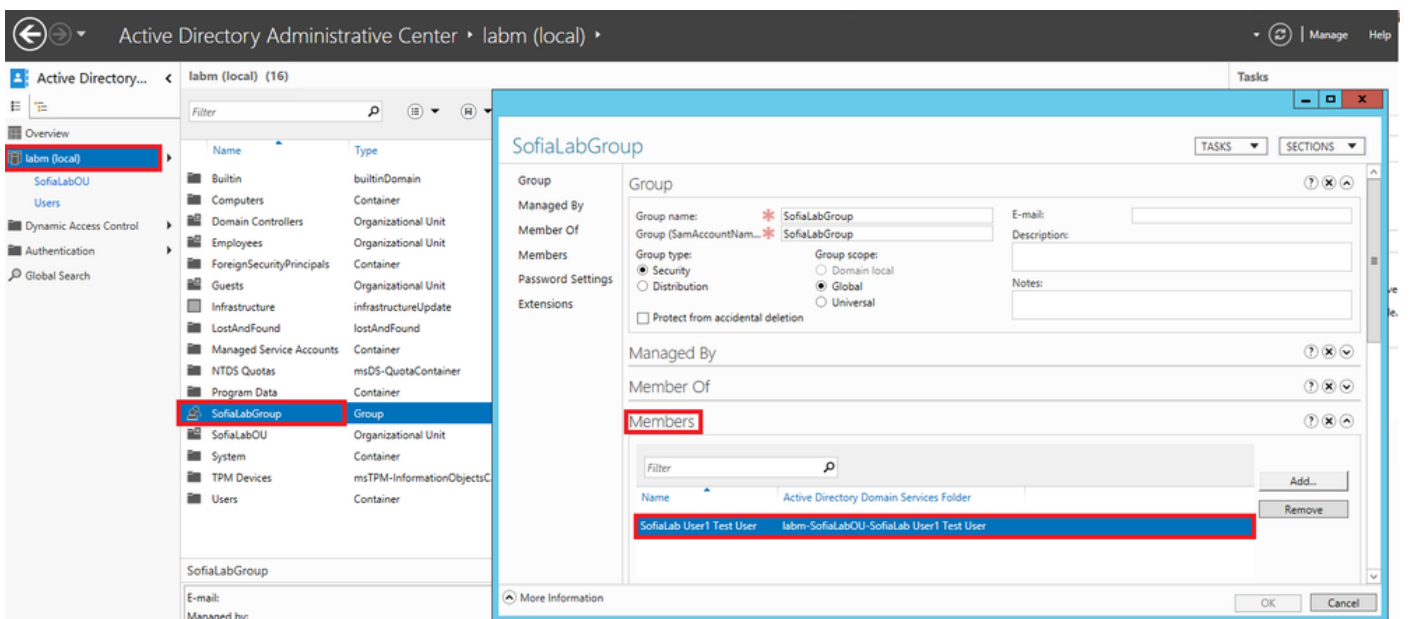
Etapa 5. Expanda SofiaLabOU para ver quais usuários estão dentro dele. Existe o User1 que foi criado antes.



Etapa 6. Tudo o que é necessário para configurar o LDAP.



Passo 7. Grupos como SofiaLabGroup não podem ser usados como um DN de pesquisa. Expanda o grupo e procure os usuários dentro dele, onde o User1 criado anteriormente deve estar como mostrado.



O User1 estava lá, mas o LDP não conseguiu encontrá-lo. Isso significa que a WLC não pode fazer isso também e é por isso que os grupos não são suportados como um DN de base de pesquisa.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

```
(cisco-controller) >show ldap summary
```

```
Idx Server Address Port Enabled Secure
```

```
-----  
1 10.88.173.121 389 Yes No
```

```
(cisco-controller) >show ldap 1
```

```
Server Index..... 1  
Address..... 10.88.173.121  
Port..... 389  
Server State..... Enabled  
User DN..... OU=SofiaLabOU,DC=labm,DC=cisco,DC=com  
User Attribute..... sAMAccountName  
User Type..... Person  
Retransmit Timeout..... 2 seconds  
Secure (via TLS)..... Disabled  
Bind Method ..... Authenticated  
Bind Username..... CN=Administrator,CN=Domain  
Admins,CN=Users,DC=labm,DC=cisco,DC=com
```

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

```
(cisco-controller) >debug client <MAC Address>
```

```
(cisco-controller) >debug aaa ldap enable
```

```
(cisco-controller) >show ldap statistics
```

```
Server Index..... 1  
Server statistics:  
Initialized OK..... 0  
Initialization failed..... 0  
Initialization retries..... 0  
Closed OK..... 0  
Request statistics:  
Received..... 0  
Sent..... 0  
OK..... 0  
Success..... 0  
Authentication failed..... 0  
Server not found..... 0  
No received attributes..... 0  
No passed username..... 0  
Not connected to server..... 0  
Internal error..... 0  
Retries..... 0
```

Informações Relacionadas

- [Guia de configuração do LDAP - WLC 8.2](#)
- [Como configurar a controladora Wireless Lan \(WLC\) para autenticação LDAP - por Vinay Sharma](#)
- [Exemplo de configuração de autenticação da Web usando LDAP em controladoras Wireless](#)

[LAN \(WLCs\) - por Yahya Jaber e Ayman Alfares](#)

- [Suporte Técnico e Documentação - Cisco Systems](#)

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.