# Configuración del WLC con autenticación LDAP para las WLAN 802.1x y de autenticación web

# Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados Antecedentes** Antecedentes técnicos **Preguntas Frecuentes** Configurar Crear una WLAN que se base en un servidor LDAP para autenticar usuarios a través de 802.1x Diagrama de la red Crear WLAN que confía en el servidor LDAP para autenticar a los usuarios a través del portal web interno del WLC Diagrama de la red Utilice la herramienta LDP para configurar y solucionar problemas de LDAP Verificación Troubleshoot Información Relacionada

# Introducción

Este documento describe el procedimiento para configurar un WLC de AireOS para autenticar clientes con un servidor LDAP como la base de datos de usuarios.

# Prerequisites

# Requirements

Cisco recomienda conocer estos temas:

- Servidores de Microsoft Windows
- Directorio activo

### **Componentes Utilizados**

La información que contiene este documento se basa en estas versiones de software:

Software Cisco WLC 8.2.110.0

Microsoft Windows Server 2012 R2

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.

# Antecedentes

### Antecedentes técnicos

- LDAP es un protocolo utilizado para acceder a los servidores de directorio.
- Los servidores de directorio son bases de datos jerárquicas orientadas a objetos.
- Los objetos se organizan en contenedores como unidades organizativas (OU), grupos o contenedores predeterminados de Microsoft como CN=Usuarios.
- La parte más difícil de esta configuración es configurar los parámetros del servidor LDAP correctamente en el WLC.

Para obtener información más detallada sobre estos conceptos, consulte la sección Introducción de <u>Cómo configurar el Controlador de LAN Inalámbrica (WLC) para la autenticación del Protocolo ligero de acceso a directorios (LDAP)</u>.

### **Preguntas Frecuentes**

• ¿Qué nombre de usuario se debe utilizar para enlazar con el servidor LDAP?

Hay dos maneras de enlazar contra un servidor LDAP, Anonymous o Authenticated (consulte para comprender la diferencia entre ambos métodos).

Este nombre de usuario de enlace debe tener privilegios de administrador para poder consultar otros nombres de usuario/contraseñas.

• Si se autentica: ¿el nombre de usuario de enlace está dentro del mismo contenedor que todos los usuarios?

No: utilice todo el trazado. Por ejemplo:

# CN=Administrador,CN=Administradores de dominio,CN=Usuarios,DC=laboratorio,DC=cisco,DC=com

Sí: utilice sólo el nombre de usuario. Por ejemplo:

#### Administrador

- ¿Qué sucede si hay usuarios en diferentes contenedores? ¿Todos los usuarios de LDAP inalámbrico involucrados deben estar en el mismo contenedor?
- No, se puede especificar un DN base que incluya todos los contenedores necesarios.
  - ¿Qué atributos debe buscar el WLC?
- El WLC coincide con el atributo de usuario y el tipo de objeto especificados.

**Nota: sAMAccountName** distingue entre mayúsculas y minúsculas, pero person no lo hace. Por lo tanto, **sAMAccountName=RICARDO** y **sAMAccountName=ricardo** son iguales y funcionan, mientras que **samaccountname=RICARDO** y **samaccountname=ricardo** no.

 ¿Qué métodos de protocolo de autenticación extensible (EAP) se pueden utilizar?
 Sólo EAP-FAST, PEAP-GTC y EAP-TLS. Los suplicantes predeterminados de Android, iOS y MacOS funcionan con el protocolo de autenticación ampliable protegido (PEAP).

Para Windows, el administrador de acceso de red (NAM) de Anyconnect o el suplicante predeterminado de Windows con Cisco:PEAP se debe utilizar en adaptadores inalámbricos compatibles, como se muestra en la imagen.

Local-EAP Wireless Network Properties	×
Connection Security	
Security type: WPA2-Enterprise Encryption type: AES	•
Choose a network authentication method:	
Cisco: PEAP Settin Microsoft: Smart Card or other certificate Microsoft: Protected EAP (PEAP) Cisco: LEAP Cisco: EAP-FAST Intel: EAP-FAST Intel: EAP-TTLS Intel: EAP-AKA Advanced settings	does not work! works!
OK	Cancel

**Nota**: los <u>complementos EAP de Cisco</u> para Windows incluyen una versión de Open Secure Socket Layer (OpenSSL 0.9.8k) que se ve afectada por el Id. de error de Cisco <u>CSCva09670</u>, Cisco no tiene previsto publicar más versiones de los complementos EAP para Windows y recomienda a los clientes que utilicen AnyConnect Secure Mobility Client.

• ¿Por qué el WLC no puede encontrar a los usuarios?

Los usuarios dentro de un grupo no se pueden autenticar. Deben estar dentro de un contenedor predeterminado (CN) o una unidad organizativa (OU), como se muestra en la imagen.

	Name	Туре	Description
<u>.</u>	SofiaLabGroup	Group	will not work
20	SofiaLabOU	Organizational Unit	
	Users	Container	Default container for upgr

# Configurar

Existen diferentes escenarios en los que se puede emplear un servidor LDAP, ya sea con autenticación 802.1x o autenticación Web.

Para este procedimiento, sólo se deben autenticar los usuarios dentro de OU=SofiaLabOU.

Para aprender cómo utilizar la herramienta de Label Distribution Protocol (LDP), configure y resuelva problemas de LDAP, consulte la <u>Guía de Configuración LDAP de WLC</u>.

# Crear una WLAN que se base en un servidor LDAP para autenticar usuarios a través de 802.1x

#### Diagrama de la red

En este escenario, el LDAP-dot1x de WLAN utiliza un servidor LDAP para autenticar a los usuarios con el uso de 802.1x.



à	Server Manager	_ 0 ×
€ Server M	lanager • Dashboard	- ②   🎢 Manage Took View Help
Dashboard	WELCOME TO SERVER MANAGER	Active Directory Administrative Center Active Directory Domains and Trusts Active Directory Lightweight Directory Services Setup Wizard
Local Server     All Servers     All CS	1 Configure this local server	Active Directory Module for Windows PowerShell Active Directory Sites and Services Active Directory Users and Computers
AD DS	2 Add roles and features	ADSI Edit Certification Authority Component Services
DNS     File and Storage Services ▷	3     Add other servers to manage       WHATS NEW     4       Create a server group	Computer Management Defragment and Optimize Drives DHCP
Ko IIS ¶∖ NAP		UNS Event Viewer Group Policy Management

#### Create User: SofiaLab User1 Test User

Account	Account			•
Organization Member Of Password Settings Profile Policy Silo	ACCOUNT First name: Middle initials: Last name: Full name: Vise UN logon: Use SamAccountName o Password: Confirm password: Create in: DC=labm,DC=ciss Find in this column Labm	SofiaLab User1 Test User SofiaLab User1 (abm Vik User1 Find in this column Demain Controllers	Account expires:	
	Q N	Employees     ForeignScurityPrincipe     Guests     ListAndFound		?ו
	This object will be added	Managed Service Accol		Add Remove

#### Create User: SofiaLab User1 Test User

Create User:	SofiaLab User1	Test User				TASKS 🔻	SECTIONS 🔻
Account	Account			•			
Organization Member Of Password Settings Profile Policy Silo	First name: Middle initials: Last name: Full name: User UPN logon: User SamAccountName Io Password: Confirm password: Create in: OUI=SofiaLabOU, Protect from accidental Log on hours	SofiaLab User1 Test User SofiaLab User1 Test User Isbm DC=labm,DC=cisco,DC=com Chang deletion Log on to	e	ccount expires: assword options: ) User must change passwo ) Other password options ) Smart card is required ' Bassword never expired User cancel the context of the	Never C End of Grinteractive log on for interactive log on password		•
	Organization						
	Member Of		Select Groups	×			
	Filter Name SofiaLabGroup	P Active Director Primary Isbm-SofiaLab	Select this object type : Groups or Bulk in security principals From this location: labin cisco com Enter the object names to select ( <u>examples</u> ): Cotal abform of	Types			Add Remove
	This object will be added Directly Associated	t to the default Active Directory gro Password Settings Precedence	Advanced	2ancel			? 🗴 🔊

Paso 2. Cree un perfil EAP en el WLC con el método EAP deseado (utilice PEAP).

TASKS V SECTIONS V

ababa								Sa <u>v</u> e Configuratio	n   <u>P</u> ing	Logout   <u>R</u> efree
cisco		MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	SECURI	TY MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK
Security	^	Local EA	P Profile	S				Ne	w	Apply
General		Profile Nar	me		LEAP	EAP-FAST	EAP-TLS	PEAP		
Authentication		Local-EAP-P	EAP					<b>~</b>		
Accounting Fallback		Local-EAP-L	.EAP		✓					
DNS TACACS+ LDAP Local Net Users										
MAC Filtering		LE/	AP	Server	Nothing	- I	Client Usern	ame & Pass	word	
User Login Policies		EA	P-FAST	Server	РАК	i	Client Usern	ame & Pass	word	
AP Policies		EA	P-TLS	Server	Certifi	cate	Client Certi	ficate		
Password Policies     Tocal EAP		PE	AP	Server	Certifi	cate	Client Usern	ame & Pass	word	
General Profiles EAP-FAST Parameters										
Authentication Priority										

Paso 3. Enlace el WLC con el servidor LDAP.

**Sugerencia**: Si el nombre de usuario de enlace no está en el DN base de usuario, debe escribir la ruta completa al usuario **Admin** tal y como se muestra en la imagen. De lo contrario, simplemente puede introducir **Administrator**.

ululu cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY M	1 <u>a</u> nagement c <u>o</u> mm	1ANDS HELI	P FEEDBACK	Sa <u>v</u> e Configuration   <u>P</u> ing	Logout <u>R</u> efre
Security	LDAP Servers > New					< Back	Apply
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> <li>DNS</li> <li>TACACS+</li> <li>LDAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> <li>AP Policies</li> <li>Paccal EAP</li> <li>Priority Order</li> <li>Certificate</li> <li>Access Control</li> </ul>	Server Index (Priority) Server IP Address Port Number Simple Bind Bind Username Bind Password Confirm Bind Password User Base DN User Attribute User Object Type Secure Mode(via TLS) Server Timeout Enable Server Status	1 V 10.88.173.121 389 Authenticated V CN=Administrator,CN=Users,D CN=Administrator,CN=Users,D CU=SofiaLabOU,DC=labm,DC= SAMAccountName Person Disabled V 2 seconds Enabled V	C=labm,DC= Adm	nin pri	vileges required Where are we going t What Attribute are w	to look for use we looking for?	ers?
<ul> <li>Wireless Protection Policies</li> <li>Web Auth TrustSec SXP Local Policies</li> <li>Advanced</li> </ul>					Warning: LDAP can only be use EAP-TLS methods	ed with EAP-FAST, PEAP-GTC an	d

Paso 4. Establezca el Orden de autenticación para establecer en Usuarios internos + LDAP o LDAP solamente.

،، ،،، ،، cısco		MONITOR	<u>w</u> lans	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u>
Security	^	Priority C	rder > L	ocal-Auth			
<ul> <li>▼ AAA</li> <li>General</li> <li>▼ RADIUS</li> <li>Authentication</li> </ul>		User Cred	lentials				
Accounting Fallback DNS TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies		Not Used	>	Order Used F	CAL	Up Down	]
<ul> <li>Local EAP</li> <li>General</li> <li>Profiles</li> <li>EAP-FAST Parameters</li> <li>Authentication Priority</li> </ul>						-	

#### Paso 5. Cree la WLAN LDAP-dot1x.

cisco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	WLANs								
WLANs	Current Fil	ter: No	ne [ <u>Char</u>	ige Filter] [Clea	r Filter]		Cr	eate New	♥ Go
Advanced	WLAN	ID Type	Profile Name	WLAN SSID	Admin Status	Security Policie	5		

uluili. cisco	Monitor Wlans Controller Wireless Security Management Commands Help Feedback
WLANs	WLANs > Edit 'LDAP-dot1x'
WLANS	General Security QoS Policy-Mapping Advanced
▶ 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     Image: Comparison of the sector of the sec

Paso 6. Establezca el método de seguridad L2 en WPA2 + 802.1x y establezca la seguridad L3 en none (ninguno).

cisco		<u>W</u> LANs <u>C</u> ON	TROLLER W	VIRELESS	SECURITY	MANAGEN
WLANs	WLANs >	Edit 'LDA	P-dot1x'			
WLANs     WLANs	General	Security	QoS Po	olicy-Mappi	ing Adv	anced
Advanced	Layer 2	Layer 3	AAA Serve	ers		
	Layer 2	2 Security 🕯 🛛 🛛	/PA+WPA2	~		
	Fast Tran	MA	C Filtering	]		
	Fast Trans	ition 🗌				
	Protected	l Management	Disabled	$\checkmark$		
	WPA+WP	A2 Parameter	s			
	WPA Po	olicy Policy				
	WPA2	Encryption	AES			
	Authentic	ation Key Man	agement			
	ССКМ	. <u> </u>	nable			
	PSK	1X 🗆	nable			
	FT PSK		Enable			
	WPA gt	tk-randomize St	Di	isable 🗸		

Paso 7. Habilite la autenticación EAP local y asegúrese de que las opciones Servidores de autenticación y Servidores de cuentas estén inhabilitadas y que LDAP esté habilitado.

cisco	MONITOR WLANS C	ONTROLLER	W <u>I</u> RELESS <u>S</u> ECU	RITY M <u>a</u> nao	GEMENT C <u>O</u> MMANDS	HELP FEEDBA	ACK
WLANs	WLANs > Edit 'Ll	DAP-dot1x'					
WLANs WLANs	General Security	/ QoS I	Policy-Mapping	Advanced			
Advanced	Layer 2 Layer	3 AAA Ser	vers				
	Select AAA servers b	elow to overrid	e use of default se	vers on this V	VLAN		
	Radius Servers						
	Radius Server Over	write interface	Enabled				
	Authentication Serve	ers Accounting	Servers		E	AP Parameters	
		Enabled		Enabled		Enable	
	Server 1	None	~	None	$\sim$		
	Server 2	None	~	None	$\sim$		
	Server 3	None	$\sim$	None	$\sim$		
	Server 4	None	~	None	$\sim$		
	Server 5	None	~	None	$\sim$		
	Server 6	None	~	None	$\sim$		
	Radius Server Accou	nting					
	Interim Update						
	LDAP Servers						
	Server 1 IP:10.8	8.173.121, Port:3	389 🗸				
	Server 2 None		~				
	Server 3 None		~				
	Local EAP Authentica	ation					
	Local EAP Authentic	cation 🗹 Enabl	ed				
	EAP Profile Name	Local-E	AP-PEAP 🗸				
	Authentication pr	iority order f	or web-auth use	r			
	Not Use	ed			Order Used For Authe	ntication	
			>		LOCAL RADIUS	Up	]

El resto de los parámetros se pueden dejar en los valores predeterminados.

#### Notas:

Utilice la herramienta LDP para confirmar los parámetros de configuración. La base de búsqueda no puede ser un grupo (como SofiaLabGroup). PEAP-GTC o Cisco:PEAP deben utilizarse en lugar de Microsoft:PEAP en el solicitante si se trata de un equipo con Windows. Microsoft:PEAP funciona de forma predeterminada con MacOS/iOS/Android.

# Crear WLAN que confía en el servidor LDAP para autenticar a los usuarios a través del portal web interno del WLC

#### Diagrama de la red

En este escenario, el LDAP-Web de WLAN utiliza un servidor LDAP para autenticar a los usuarios con el portal Web interno del WLC.

# LDAP Server



Asegúrese de que los pasos 1. a 4. se han tomado del ejemplo anterior. A partir de ahí, la configuración de WLAN se establece de manera diferente.

Paso 1. Cree un usuario **User1** en el miembro del servidor LDAP de OU SofiaLabOU y el grupo SofiaLabGroup.

Paso 2. Cree un perfil EAP en el WLC con el método EAP deseado (utilice PEAP).

Paso 3. Enlace el WLC con el servidor LDAP.

Paso 4. Establezca el Orden de autenticación en Usuarios internos + LDAP.

Paso 5. Cree la WLAN LDAP-Web como se muestra en las imágenes.

cisco	Monitor <u>w</u> lans <u>c</u> ontroller w <u>i</u> reless <u>s</u> ecurity m <u>a</u> nagement c <u>o</u> mmands he <u>l</u> p <u>f</u> eedback
WLANs	WLANs
WLANs	Current Filter: None [Change Filter] [Clear Filter] Create New V Go
Advanced	UKAN ID Type Profile Name WLAN SSID Admin Status Security Policies

،،ا،،،ا،، cısco	MONITOR WLANS CONTROLL	ER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'LDAP-Web	)'
WLANS	General Security Qo	S Policy-Mapping Advanced
Advanced	Profile Name	LDAP-Web
	Туре	WLAN
	SSID	LDAP-Web
	Status	C 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

Paso 6. Establezca la seguridad L2 en none y la seguridad L3 en Web Policy -Authenticationcomo se muestra en las imágenes.

cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY M <u>A</u> NAGEMENT C <u>O</u> MMANDS HELP <u>F</u> EEDBACK
WLANs	WLANs > Edit 'LDAP-Web'
<ul> <li>WLANs</li> <li>Advanced</li> </ul>	General       Security       Qos       Policy-Mapping       Advanced         Layer 2       Layer 3       AAA Servers         Layer 2       Security       None       MAC Filtering         Fast Transition       Fast Transition       Fast Transition

،،ا،،،ا،، cısco	Monitor <u>w</u> lans <u>c</u> ontroller w <u>i</u> reless <u>s</u> ecurity m <u>a</u> nagement c <u>o</u> mmands he <u>l</u> p <u>f</u> eedback
WLANs	WLANs > Edit 'LDAP-Web'
WLANS	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 3 Security 1 Web Policy Authentication Authentication Conditional Web Redirect Splash Page Web Redirect On MAC Filter failure19 Preauthentication ACL IPv4 None IPv6 None WebAuth FlexAcl None Sleeping Client Enable Over-ride Global Config29 Enable Web Auth type Internal

Paso 7. Establezca el orden de prioridad de autenticación para que web-auth utilice LDAP y asegúrese de que las opciones Servidores de autenticación y Servidores de cuentas estén inhabilitadas.

،،ا،،،ا،، cısco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY M <u>A</u> NAGEMENT C <u>O</u> MMANDS HELP <u>F</u> EEDBACK						
WLANs	WLANs > Edit 'LDAP-Web'						
WLANS	General Security QoS Policy-Mapping Advanced						
Advanced	Layer 2 Layer 3 AAA Servers						
	Select AAA servers below to override use of default servers on this WLAN RADIUS Servers RADIUS Server Overwrite interface						
	Authentication Servers Accounting Servers						
	Enabled Enabled						
	Server 1 None V None V						
	Server 2 None   None						
	Server 3 None V None V						
	Server 4 None V None						
	Server 5 None V None V						
	Server 6 None V None V						
	RADIUS Server Accounting						
	Interim Update						
	LDAP Servers						
	Server 1 IP:10.88.173.121, Port:389 V						
	Server 2 None						
	Server 3 None V						
	Local EAP Authentication						
	Local EAP Authentication Enabled						
	Authentication priority order for web-auth user						
	Not Used Order Used For Authentication						
	RADIUS A Up V C						

El resto de los parámetros se pueden dejar en los valores predeterminados.

# Utilice la herramienta LDP para configurar y solucionar problemas de LDAP

Paso 1. Abra la herramienta LDP en el servidor LDAP o en un host con conectividad (el puerto TCP 389 debe estar permitido al servidor).

Start	]	Search Everywhere v
Server Manager	Windows PowerShell	ldp
This PC	Task Manager	

Paso 2. Navegue hasta Conexión > Enlazar, inicie sesión con un usuario administrador y

seleccione el botón de opción Enlazar con credenciales.

onnection Bro	owse View Oj
Bind Disconnect	Ctrl+B
New Save Save As	Ctrl+N
Exit	

Paso 3. Navegue hasta Ver > Árbol y seleccione Aceptar en el DN base.

· 🏠	ldap:	//WIN-4BD4NV0J3NK.labm.cisco.com/DC=labm,DC=cisc	o,DC=com
Connection Browse View Options U	Itilities Help	Tree View	X
Tree	Ctrl+T	Tree view	
Enterprise Cor	nfiguration	2 DV -	
✓ Status Bar		BaseDN:	Y
Set Font		Cancel	ОК

Paso 4. Expanda el árbol para ver la estructura y buscar el DN de base de búsqueda. Tenga en cuenta que puede ser cualquier tipo de contenedor excepto Grupos. Puede ser el dominio completo, una OU específica o un CN como CN=Users.



Paso 5. Expanda SofiaLabOU para ver qué usuarios están dentro de ella. Existe el usuario User1 que se creó anteriormente.



ı. cısco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT	Sage Configuration Ping Logout Bet COMMANDS HELP FEEDBACK
Security	LDAP Servers > New		< Back Apply
<ul> <li>AAA</li> <li>General</li> <li>RADUS</li> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> <li>DNS</li> <li>TACACS+</li> <li>LDAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> <li>AP Policies</li> <li>Porrity Order</li> <li>Certificate</li> <li>Access Control</li> <li>Lists</li> <li>Wireless Protection</li> <li>Policies</li> <li>Web Auth</li> <li>TrustSec SXP</li> <li>Local Policies</li> <li>Advanced</li> </ul>	Server Index (Priority) Server IP Address Port Number Simple Bind Bind Username Bind Password Confirm Bind Password User Base DN User Attribute User Object Type Secure Mode(via TLS) Server Timeout Enable Server Status	1       ▼         10.88.173.121         389         Authenticated ✓         CN=Administrator,CN=Users,DC=labm,DC=         ••••••••         ••••••••         ••••••••         •••••••         ©U=SofiaLabOU,DC=labm,DC=cisco,DC=com         sAMAccountName         Person         Disabled ✓         2       seconds         Enabled ✓	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 OK Cancel

Paso 7. Los grupos como SofiaLabGroup no se pueden utilizar como DN de búsqueda. Expanda el grupo y busque los usuarios que se encuentran en su interior, donde debe estar el User1 creado anteriormentecomo se muestra.

E Active	Directory Administrative	ve Center + labm (local) +		- 🗵   Manage Help
Active Directory <	labm (local) (16)			Tasks
E TE Overview SofiaLabOU Users Dynamic Access Control Authentication Global Search	Filter         P           Name         Type           Builtin         builtin           Computers         Contair           Domain Controllers         Organia           Employees         Organia           ForeignSecurityPrincipals         Contair           Guests         Organia	B R R R R R R R R R R R R R R R R R R R	UP Group Group name: * SofaLabGroup Group (SamAccountNam* SofaLabGroup Group type: Group scope: © Security O Domain local O bistribution © Global	TASKS V SECTIONS V () (2) (2) (2) (2) (2) (2) (2) (2) (2) (
	Infrastructure infrastm     LostAndFound lostAnc     Managed Service Accounts Contain     NTDS Quotas msDS-6     Program Data Contain     Contain     Sofialab@roup Group	structureUpdate Extensions indFound ainer S-QuotaContainer ainer p	Protect from accidental deletion     O Universal     Managed By     Member Of	080 080
	SofiaLabOU Organizati System Container TPM Devices msTPM-In Users Container SofiaLabGroup	nizational Unit ainer M-InformationObjectsC ainer	Members       Filter       Name       Active Directory Domain Services Folder       Sofialab User1 Test User       Iabm-SofialabOU-Sofialab User1 Test User	Add
	E-mail: Managed by:	<ul> <li>More Information</li> </ul>		OK Cancel

El usuario 1 estaba allí, pero LDP no pudo encontrarlo. Significa que el WLC no puede hacerlo también y que es porqué los grupos no se soportan como un DN de la base de búsqueda.

# Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

```
(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

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

(cisco-controller) >debug client <mac address=""></mac>	
(cisco-controller) >debug aaa ldap enable	
(cisco-controller) >show ldap statistics	
Server Index Server statistics:	. 1
Initialized OK	0
Initialization failed	0
Initialization retries	0
Closed OK	0
Request statistics:	
Received	0
Sent	0
ОК	0
Success	0
Authentication failed	0
Server not found	0
No received attributes	0
No passed username	0
Not connected to conver	0
	0
	0
Ketries	U

# Información Relacionada

- Guía de Configuración de LDAP WLC 8.2
- <u>Cómo configurar el controlador de LAN inalámbrica (WLC) para la autenticación del protocolo</u> ligero de acceso a directorios (LDAP) - por Vinay Sharma
- Ejemplo de Configuración de Autenticación Web Usando LDAP en Controladores LAN Inalámbricos (WLCs) - por Yahya Jaber y Ayman Alfares
- Soporte Técnico y Documentación Cisco Systems

#### 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).