# Webverificatie met LDAP op Wireless LANcontrollers (WLC's) - configuratievoorbeeld

### Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten Achtergrondinformatie **Conventies** Web verificatieproces Configureren Netwerkdiagram Configuraties De LDAP-server configureren Gebruikers maken op de domeincontroller Een gebruikersdatabase maken onder een OE De gebruiker voor LDAP-toegang configureren **Anonymous Bind** Anonieme bindfunctie inschakelen op de Windows 2012 Essentials Server ANONIEME AANMELDTOEGANG verlenen aan de gebruiker Toestemming voor inhoudsopgave in doelgroep Geverifieerd bind Beheerdersrechten verlenen aan WLC-admin Gebruik LDP om de gebruikerskenmerken te identificeren WLC voor LDAP-server configureren Het WLAN voor webverificatie configureren Verifiëren Problemen oplossen

## Inleiding

Dit document beschrijft hoe u een draadloze LAN-controller (WLC) kunt instellen voor webverificatie. Het legt uit hoe een Lichtgewicht Directory Access Protocol (LDAP) server te configureren als de back-end database voor webverificatie om gebruikersreferenties op te halen en de gebruiker te verifiëren.

## Voorwaarden

#### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van de configuratie van Lichtgewicht access points (LAP's) en Cisco WLC's
- Kennis van controle en provisioning van Wireless Access Point Protocol (CAPWAP)
- Kennis van het instellen en configureren van Lichtgewicht Directory Access Protocol (LDAP), Active Directory en domeincontrollers

#### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 5508 WLC met firmwarerelease 8.2.100.0
- Cisco 1142 Series router
- Cisco 802.11a/b/g draadloze clientadapter.
- Microsoft Windows 2012 Essentials-server die de rol van de LDAP-server vervult

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

### Achtergrondinformatie

### Conventies

Raadpleeg <u>Cisco Technical Tips Conventions</u> (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

### Web verificatieproces

Web authenticatie is een Layer 3-beveiligingsfunctie die ervoor zorgt dat de controller IP-verkeer (behalve DHCP- en DNS-gerelateerde pakketten) van een bepaalde client verbiedt totdat die client correct een geldige gebruikersnaam en wachtwoord heeft opgegeven. Wanneer u webverificatie gebruikt om clients te verifiëren, moet u voor elke client een gebruikersnaam en wachtwoord definiëren. Vervolgens, wanneer de clients proberen zich aan te sluiten bij het draadloze LAN, moeten ze de gebruikersnaam en het wachtwoord invoeren wanneer dit wordt gevraagd door een inlogpagina.

Wanneer webverificatie is ingeschakeld (onder Layer 3 Security), ontvangen gebruikers af en toe een web-browser veiligheidswaarschuwing de eerste keer dat ze proberen om toegang te krijgen tot een URL.

**Tip**: Als u deze certificaatwaarschuwing wilt verwijderen, gaat u terug naar de volgende handleiding over het installeren van een betrouwbaar certificaat van een derde partij <u>http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/109597-csr-chained-certificates-wlc-00.html</u>

8	There is a problem with this website's security certificate.
	The security certificate presented by this website was not issued by a trusted certificate authority.
	Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
	We recommend that you close this webpage and do not continue to this website.
	Olick here to close this webpage.
	Solution to this website (not recommended).
	More information
	III. •

Nadat u op **Ja** klikt om verder te gaan (of meer bepaald **doorgaan naar deze website (niet aanbevolen)** voor Firefox-browser bijvoorbeeld), of als de browser van de client geen veiligheidswaarschuwing weergeeft, leidt het web-verificatiesysteem de client naar een inlogpagina, zoals in de afbeelding:

Login	

#### Welcome to the Cisco wireless network

Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work.

User Name		
Password	••••	
	Submit	

De standaardaanmeldpagina bevat een Cisco-logo en Cisco-specifieke tekst. U kunt ervoor kiezen om het web authenticatie systeem een van deze weer te geven:

- De standaardaanmeldpagina
- Een aangepaste versie van de standaardaanmeldpagina
- Een aangepaste inlogpagina die u op een externe webserver configureert

• Een aangepaste inlogpagina die u naar de controller downloadt

Wanneer u een geldige gebruikersnaam en wachtwoord invoert op de inlogpagina voor webverificatie en op **Indienen** klikt, wordt u geverifieerd op basis van de ingezonden referenties en een succesvolle verificatie van de backend-database (LDAP in dit geval). Het web authenticatie systeem toont vervolgens een succesvolle login pagina en leidt de geverifieerde client naar de gevraagde URL.

	Web Authentication
	Login Successful !
You	can now use all regular network services over the wireless network.
Pleas	e retain this small logout window in order to logoff when done. Note that you can always use the following URL to retrieve this page: <u>https://1.1.1.1/logout.html</u>
	Logout

De standaard succesvolle login pagina bevat een aanwijzer naar een virtuele gateway adres URL: <u>https://1.1.1/logout.html.</u> Het IP-adres dat u voor de virtuele interface van de controller instelt, dient als het omleidingsadres voor de inlogpagina.

Dit document legt uit hoe u de interne webpagina op de WLC kunt gebruiken voor webverificatie. In dit voorbeeld wordt een LDAP-server gebruikt als de back-end database voor webverificatie om gebruikersreferenties op te halen en de gebruiker te verifiëren.

### Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

**Opmerking: Gebruik de Command Lookup Tool** <u>(alleen voor geregistreerde klanten) voor</u> <u>meer informatie over de opdrachten die in deze sectie worden gebruikt.</u>

#### Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



### Configuraties

Voltooi de volgende stappen om deze setup met succes te implementeren:

- LDAP-server configureren.
- <u>Configureer WLC voor LDAP Server</u>.
- Configureer het WLAN voor webverificatie.

#### De LDAP-server configureren

De eerste stap is het configureren van de LDAP-server, die dient als een back-end database om gebruikersreferenties van de draadloze clients op te slaan. In dit voorbeeld wordt de Microsoft Windows 2012 Essentials-server gebruikt als LDAP-server.

De eerste stap in de configuratie van de LDAP-server is het maken van een gebruikersdatabase op de LDAP-server, zodat de WLC deze database kan bevragen om de gebruiker te verifiëren.

#### Gebruikers maken op de domeincontroller

Een Organisatorische Eenheid (OU) bevat meerdere groepen die verwijzingen naar persoonlijke vermeldingen in een PersonProfile dragen. Een persoon kan lid zijn van meerdere groepen. Alle objectklasse- en attribuutdefinities zijn standaard LDAP-schema. Elke groep bevat verwijzingen

(dn) voor elke persoon die tot deze groep behoort.

In dit voorbeeld wordt een nieuwe OU LDAP-USER gemaakt, en de gebruiker User1 wordt gemaakt onder deze OU. Wanneer u deze gebruiker configureert voor LDAP-toegang, kan de WLC deze LDAP-database bevragen voor gebruikersverificatie.

Het domein dat in dit voorbeeld wordt gebruikt is CISCOSYSTEMS.local.

#### Een gebruikersdatabase maken onder een OE

In deze paragraaf wordt uitgelegd hoe u een nieuwe OU in uw domein maakt en een nieuwe gebruiker maakt op deze OE.

- 1. Windows PowerShell openen en servermanager.exe typen
- 2. Klik in het venster Server Manager op **AD DS**. Klik vervolgens met de rechtermuisknop op uw servernaam om **Active Directory-gebruikers en -computers** te kiezen.
- Klik met de rechtermuisknop op uw domeinnaam, die in dit voorbeeld CISCOSYSTEMS.local is, en navigeer vervolgens naar Nieuw > Organisatorische Eenheid vanuit het contextmenu om een nieuwe OU te maken.

Active Directory Users and Computers							
File Action View Help							
Active Directory Users and Computers [WIN-A0] Name Type Cescription							
Saved Queries							
4 [3] CISCOSYSTEMS.local Container Default container for up							
Builtin Delegate Control u Container Default container for sec							
Compute Find     E Container Default container for ma							
Change Domain tata Container Default location for stor							
Change Domain Controller     Container Builtin system settings							
LostAndF Raise domain functional level Container Default container for up							
Managed Operations Masters							
Program New Default container for of							
System							
Users All Tasks Contact							
NTDS Qu View → Group Group							
Refresh InetOrgPerson							
Export List msImaging-PSPs							
MSMQ Queue Alias							
Properties Organizational Unit							
Help Printer							
User							
Shared Folder							
Create a new object							

4. Wijs een naam toe aan deze OE en klik op OK, zoals in de afbeelding:

	New Object - Organizational Unit	x				
🧭 c	reate in: CISCOSYSTEMS.local/					
Name:						
LDAP-USER	LDAP-USERS					
	OK Cancel Help					

Nu de nieuwe OU LDAP-USER op de LDAP-server is gemaakt, is de volgende stap om **Gebruiker1** te maken onder deze OE. Voltooi de volgende stappen om dit te bereiken:

1. Klik met de rechtermuisknop op de nieuwe OE die wordt gemaakt. Navigeer naar LDAP-GEBRUIKERS> Nieuw > Gebruiker vanuit de resulterende contextmenu's om een nieuwe gebruiker te maken, zoals in de afbeelding:

						Active Directory Users and Computers	- 8 ×
File Action	View He	зlp					
🗢 🄶 🙍	1 4 🗅	🗙 🗊 🛛	0		<mark>% % 🗑 7</mark> 🗖 %		
Active Direct	tory Users a ueries /STEMS.locci in uputers aain Control gged Servic s P-USERS	al lers Principal: e Accour Delegate Con Move Find	ame atrol	Ty	pe Description	There are no items to show in this view.	
	All Tasks > All Tasks > View > Cut Delete Rename Refresh Export List Properties		•	Computer Contact Group InetOrgPerson msImaging-PSPs MSNQ Queue Alias Organizational Unit Printer User User			
< <u>m</u>		Help			Jaareu rouer		
Create a new obj	ject				12		
	2			-			<ul> <li>P 12:14 PM</li> <li>12/17/2015</li> </ul>

2. Vul op de pagina Instellen gebruiker de gewenste velden in zoals in dit voorbeeld. In dit voorbeeld is Gebruiker1 in het veld Gebruikersnaam vermeld.Dit is de gebruikersnaam die in de LDAP-database wordt geverifieerd om de client te verifiëren. Dit voorbeeld gebruikt Gebruiker1 in de velden Voornaam en Volledige naam. Klik op Next (Volgende).

Creat	e in: CISCOS'	YSTEMS.local/LDAP-USERS
First name:	User1	Initials:
Last name:		
Full name:	User1	
User logon name	-	
Uşer1		@CISCOSYSTEMS.local v
User logon name	(pre-Windows 2	2000):
CISCOSYSTEM	S/	User1

3. Voer een wachtwoord in en bevestig het wachtwoord. Kies de optie Wachtwoord verloopt

nooit en klik op Volgende.

Password:	•••••	
Confirm password:	•••••	
<ul> <li>User cannot change</li> <li>Password never exp</li> <li>Account is disabled</li> </ul>	e password pires	

4. Klik op Finish (Voltooien). Er wordt een nieuwe gebruiker User1 aangemaakt onder de OU LDAP-GEBRUIKERS. Dit zijn de gebruikersreferenties:gebruikersnaam: Gebruiker1wachtwoord: Notebook123

	: CISCOSYSTEMS.local/LDAP-US	SERS
Vhen you click Finis	sh, the following object will be created	l:
ull name: User1		<u>^</u>
Jser logon name: L	lser1@CISCOSYSTEMS.local	
The password neve	er expires.	
		~

gebruiker is gemaakt onder een OE, is de volgende stap om deze gebruiker te configureren voor LDAP-toegang.

#### De gebruiker voor LDAP-toegang configureren

U kunt kiezen tussen **Anonymous** of **Authenticated** om de lokale verificatiebindmethode voor de LDAP-server op te geven. De methode Anonymous biedt anonieme toegang tot de LDAP-server. De methode Authenticated vereist dat een gebruikersnaam en wachtwoord worden ingevoerd om de toegang te beveiligen. De standaardwaarde is anoniem.

Deze sectie legt uit hoe u zowel Anonieme als geverifieerde methoden kunt configureren.

#### **Anonymous Bind**

**Opmerking**: gebruik van Anonymous Bind wordt niet aanbevolen. Een LDAP-server die anoniem bind toestaat, vereist geen enkel type van gelimiteerde authenticatie. Een aanvaller kon gebruik maken van de Anonymous bind toegang om bestanden op de LDAP-regisseur te bekijken.

Voer de stappen in deze sectie uit om een anonieme gebruiker voor LDAP-toegang te configureren.

#### Anonieme bindfunctie inschakelen op de Windows 2012 Essentials Server

Voor toepassingen van derden (in ons geval WLC) om toegang te krijgen tot Windows 2012 AD op de LDAP, moet de functie Anonymous Bind zijn ingeschakeld op Windows 2012. Anonieme LDAP-bewerkingen zijn standaard niet toegestaan op Windows 2012 domeincontrollers. Voer deze stappen uit om de functie Anonymous Bind in te schakelen:

- 1. Start het gereedschap ADSI Bewerken door te typen: **ADSIEdit.msc** in Windows PowerShell. Deze tool maakt deel uit van de Windows 2012-ondersteuningstools.
- Breid in het venster ADSI Edit het rootdomein uit (Configuration [WIN-A0V2BU68LR9.CISCOSYSTEMS.local]).Ga naar CN=Services > CN=Windows NT > CN=Directory Service. Klik met de rechtermuisknop op de container CN=Directory Service en kies Eigenschappen in het contextmenu, zoals in de afbeelding:

2				ADSI Edit		- 0 X
File Action View Help						
🗢 🏟 🖄 📷 💥 🖾 🙆	🗟 🖪 📩					
📝 ADSI Edit		Name	Class	Distinguished Name	Actions	
Domain [WIN-A0V2BU68LF	R9.CISCOSYSTEMS.local]	CN=Directory Service	nTDSService	CN=Directory Service, CN=Windows NT, CN=Services, CN=Configuration, DC=CIS	CN=Windows N	▲ TI
Configuration (WiN-A0/2)     Che-Configuration, DC -     Che-Configuration, DC -     Che-DisplaySpecific     Che-DisplayS	SUGELR9.CISCOSYSTEMS.local] cISCOSYSTEMS_DC=local ts ICConfig ions infiguration Distribution Service pp Services Services Services 17 17 16 17	CN=Directory Service nTDSService	CN=Directory Service, CN=Windows NT, CN=Services, CN=Configuration, DC=CIS	CN=Windows h More Actions	۰ ۲	
CN=Sites CN=WellKnown	Move New Connection from Here					
	New	<b>&gt;</b>				
	Delete Rename Refresh					
	Properties					
	Help					
Opens the properties dialog box for	r the current selection.					
						▲ 🔀 🙀 🕼 1:07 PM 12/17/2015

3. In het venster van de Eigenschappen van de Dienst van CN=Directory, onder Attributen, klik de attributen van dsHeuristics onder het gebied van Attributen en kies Bewerken. Voer in het venster String Attribute Editor van deze eigenschap de waarde 000002 in; klik op Toepassen en OK, zoals in de afbeelding. De functie Anonymous Bind is ingeschakeld op de Windows 2012-server.Opmerking: het laatste (zevende) teken is het teken dat bepaalt hoe je kan binden aan LDAP-service. 0 (nul) of geen zevende teken betekent dat anonieme LDAP-bewerkingen zijn uitgeschakeld. Als u het zevende teken op 2 instelt, wordt de functie Anonymous Bind ingeschakeld.

operties	<u>? ×</u>	
butes		
ites		
that have values		
Syntax	Value 🔺	
Unicode String Unicode String UTC Coded Ti Unicode String Distinguished Octet String UTC Coded Ti Octet String UTC Coded Ti Unicode String Unicode String Integer	lab.wireless/Configuration       Directory Service       S/4/2008 12:38:09 PM <not set=""> <not set=""></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not>	String Attribute Editor       Ambute: dSHeuristics       Value:       Iteor       Iteor       Clear
	butes tes that have <u>values</u> Syntax Unicode String Unicode String Unicode String Distinguished Unicode String Distinguished Octet String UTC Coded TL Unicode String UTC Coded String UTC Coded String UTC Coded String UTC Coded String UTC Coded String Unicode String Integer	Operation     ? ×       butes     tes       that have yalues     Isb wireless/Configuration       Unicode String     Isb wireless/Configuration       Unicode String     Directory Service       UTC Coded Ti     9/4/2008 12:38:09 PM       Unicode String     (Not Seb)       UTC Coded Ti     (Not Seb)       Unicode String     (Not Seb)

#### ANONIEME AANMELDTOEGANG verlenen aan de gebruiker

De volgende stap is om ANONYMOUS LOGON toegang tot de gebruiker User1 te verlenen. Voltooi de volgende stappen om dit te bereiken:

- 1. Open Active Directory-gebruikers en -computers.
- 2. Zorg ervoor dat de optie Geavanceerde functies bekijken is ingeschakeld.
- 3. Navigeer naar de gebruiker Gebruiker1 en klik met de rechtermuisknop op deze gebruiker. Kies **Eigenschappen** in het contextmenu. Deze gebruiker wordt geïdentificeerd met de voornaam Gebruiker1.



4. Klik op het tabblad **Beveiliging**, zoals in de afbeelding:

		User1	Proper	ties		? X		
Published C	ertificates	Member Of	Passwo	ord Replica	tion	Dial-in Object		
Remote	Desktop Se	ervices Profile	. (	COM+	At	tribute Editor		
General	Address	Account	Profile	Teleph	ones	Organization		
Security	Er	nvironment	Ses	sions	Re	emote control		
Group or u	ser names:							
Image: RAS and IAS Servers (CISCOSYSTEMS\RAS and IAS Servers)       ^         Image: Administrators (CISCOSYSTEMS\Administrators)       ^         Image: Account Operators (CISCOSYSTEMS\Account Operators)       ^         Image: Account Operators (CISCOSYSTEMS\Account Operators)       ^         Image: Pre-Windows 2000 Compatible Access (CISCOSYSTEMS\Pre-Wi)       Image: Pre-Windows 2000 Compatible Access (CISCOSYSTEMS\Pre-Wi)         Image: Pre-Windows Authorization Access Group (CISCOSYSTEMS\Window)       Image: Pre-Windows Authorization Access Group (CISCOSYSTEMS\Window)         Image: Pre-Windows Authorization Access Group (CISCOSYSTEMS\Terminal Serv)       Image: Pre-Windows Pre-Windows)         Image: Pre-Windows Authorization Access Group (CISCOSYSTEMS\Terminal Serv)       Image: Pre-Windows)         Image: Pre-Windows Authorization Access Group (CISCOSYSTEMS\Terminal Serv)       Image: Pre-Windows)         Image: Pre-Windows Authorization Access Group (CISCOSYSTEMS\Terminal Serv)       Image: Pre-Windows)         Image: Pre-Windows Authorization Access Group (CISCOSYSTEMS\Terminal Serv)       Image: Pre-Windows)         Image: Pre-Windows Authorization Access Group (CISCOSYSTEMS\Terminal Serv)       Image: Pre-Windows)         Image: Pre-Windows Authorization Access Group (CISCOSYSTEMS\Terminal Serv)       Image: Pre-Windows         Image: Pre-Windows Authorization Access Group (CISCOSYSTEMS\Terminal Serv)       Image: Pre-Windows								
Permission	s for ANON		ON	A	llow	Deny		
Full cont	trol							
Read					/			
Write								
Create a	all child obje	ects		L	_			
Delete a	all child obje	ects		L				
Allowed	to authenti	cate						
For special Advanced Learn abou	permission	s or advanced	l settings, missions	click		Advanced		
	0	ĸ	Cancel	Ap	ply	Help		

- 5. Klik op Add in het resulterende venster.
- 6. Voer onder het *vak* '*Voer* de *namen van de objecten in om het* dialoogvenster te *selecteren* en te bevestigen' de **ANONIEME AANMELDING in**, zoals wordt aangegeven in de afbeelding:

Select Users, Computers, Service Accou	nts, or Groups 🛛 ? 🗙
Select this object type:	
Users, Groups, or Built-in security principals	Object Types
From this location:	
CISCOSYSTEMS.local	Locations
Enter the object names to select (examples):	
ANONYMOUS LOGON	Check Names
Advanced	OK Cancel

7. In de ACL, merk op dat ANONYMOUS LOGON toegang tot sommige bezitsreeksen van de gebruiker heeft. Klik op **OK**. De ANONIEME LOGON-toegang wordt aan deze gebruiker verleend, zoals wordt getoond in de afbeelding:

		User1	Propert	ies		?	x
Published Certific	ates	Member Of	Passwor	d Replica	tion	Dial-in	Object
Remote Desk	top Se	rvices Profile	0	OM+	A	ttribute E	ditor
General Add	dress	Account	Teleph	ones	Orga	nization	
Security	En	vironment	Sess	ions	Re	emote co	ontrol
Group or user n	ames:						
SANONYMO	DUS LO	DGON					~
Serveryone							_
SELF							=
Authentica	ited Us	ers					
	lmins ((	CISCOSYSTE	MS\Domai	in Admins	6		
Cert Publis	hers (C	SCOSYSTEM	IS\Cert Pu	ublishers)	,		$\sim$
				Add		Remo	ve
Permissions for	ANON	YMOUS LOGO	DN .	A	llow	Der	ıy
Full control							^
Read				•	/		
Write							
Create all chi	ld obje	cts		L	_		
Delete all chi	ld obje	cts		L	_		
Allowed to all	Inentio	ate		L			$\sim$
For special pem Advanced.	nissions	s or advanced	settings, c	lick		Advanc	ed
Leam about ac	cess co	ontrol and pem	<u>iissions</u>				
	O	< C	ancel	Ap	ply		Help

#### Toestemming voor inhoudsopgave in doelgroep

De volgende stap is om tenminste de toestemming van de Inhoud van de Lijst te verlenen aan de ANONIEME LOGON op OU waarin de gebruiker wordt gevestigd. In dit voorbeeld bevindt Gebruiker1 zich op de OU LDAP-GEBRUIKERS. Voltooi de volgende stappen om dit te bereiken:

1. In Active Directory Gebruikers en Computers, klik met de rechtermuisknop op de OU LDAP-GEBRUIKERS en kies Eigenschappen, zoals in de afbeelding:

			Active Directory	Users and Computers		_ 0 X
File Action View Help						
🗢 🔿 📶 🦸 🗰 🔀 🖬 🖏 🗽 🏹 🖾	à,					
<ul> <li></li></ul>	Same Subser	Type User	Description		Ctivate Windows	
< III >					 	
Opens the properties dialog hox for the current selection.						

- 2. Klik op Beveiliging.
- 3. Klik op Add (Toevoegen). In het dialoogvenster dat nu wordt geopend, voert u ANONIEME AANMELDING in en bevestigt u het dialoogvenster, zoals in de afbeelding:

Select Users, Computers, Service Accounts, or Grou	ups ? X
Select this object type:	,
Users, Groups, or Built-in security principals	Object Types
From this location:	
CISCOSYSTEMS.local	Locations
Enter the object names to select (examples):	
ANONYMOUS LOGON	Check Names
Advanced OK	Cancel

#### Geverifieerd bind

Voer de stappen in deze sectie uit om een gebruiker voor lokale verificatie naar de LDAP-server te configureren.

- 1. Windows PowerShell openen en typen servermanager.exe
- 2. Klik in het venster Server Manager op AD DS. Klik vervolgens met de rechtermuisknop op de naam van uw server om te kiezen Active Directory Gebruikers en computers.

3. Klik met de rechtermuisknop op **Gebruikers**. Navigeer naar **Nieuw > Gebruiker** vanuit de resulterende contextmenu's om een nieuwe gebruiker te maken.

3	Active Directory Users and Computers	 x	
File Action View Help			
🗢 🔿 📶 🔏 📋 💥 🔂 😣	TT 浅 🐮 🛅 🍸 🚨 🐍		
<ul> <li>Active Directory Users and Computers [WIN-A0\</li> <li>Saved Queries</li> <li>GISCOSYSTEMS.local</li> <li>Builtin</li> <li>Computers</li> <li>Domain Controllers</li> <li>ForeignSecurityPrincipals</li> <li>LOAP-USERS</li> <li>LostAndFound</li> <li>Managed Service Accounts</li> <li>Program Data</li> <li>System</li> <li>User</li> <li>NTD</li> <li>Delegate Control</li> <li>TPM</li> <li>Find</li> <li>New</li> <li>All Tasks</li> <li>View</li> </ul>	Name         Type         Description           & Allowed RO         Security Group         Members in this group c           & Cert Publish         Security Group         Members of this group c           & Denied ROD         Security Group         Members in this group c           & DinsAdmins         Security Group         Members in this group c           & RAS and IAS         Security Group         DNX Administrators Gro           & WinRMRem         Security Group         Members of this group an           & WinRMRem         Security Group         Members of this group t           & Coneable D         Security Group         Members of this group t           & Domain Ad         Security Group         DNS clients who are per           & Domain Co         Security Group         All workstations and ser           & Domain Co         Security Group         All domain quests           Bomain Users         Security Group         All domain users           Computer         p         Members in this group c		
Refresh Export List Properties Help	InetOrgPerson P msImaging-PSPs P MSMQ Queue Alias P Printer P User p		
< III 2., Create a new object	Shared Folder p Members of this group		~

- 4. Vul op de pagina Instellen gebruiker de gewenste velden in zoals in dit voorbeeld. Dit voorbeeld heeft WLC-admin in het veld Gebruikersnaam. Dit is de gebruikersnaam die gebruikt moet worden voor lokale verificatie van de LDAP-server. Klik op Next (Volgende).
- 5. Voer een wachtwoord in en bevestig het wachtwoord. Kies de optie **Wachtwoord verloopt nooit** en klik op **Volgende**.
- Klik op Finish (Voltooien). Een nieuwe gebruiker WLC-admin wordt gemaakt onder de User container. Dit zijn de gebruikersreferenties:gebruikersnaam: WLC-adminwachtwoord: Admin123

#### Beheerdersrechten verlenen aan WLC-admin

Nu de lokale verificatiegebruiker is aangemaakt, moeten we de beheerder rechten toekennen. Voltooi de volgende stappen om dit te bereiken:

- 1. Open Active Directory-gebruikers en -computers.
- 2. Zorg ervoor dat de optie Geavanceerde functies bekijken is ingeschakeld.
- 3. Navigeer naar de gebruiker **WLC-admin** en klik er met de rechtermuisknop op. Kies **Eigenschappen** in het contextmenu, zoals in de afbeelding. Deze gebruiker wordt geïdentificeerd met de voornaam WLC-admin.

		Active Direct	tory Users and Compute	ers	 z x	5
File Action View Help	<b>F S S F 7</b>	7 🗾 🐍				
<ul> <li>Active Directory Users and Computers [WIN-A0\</li> <li>Saved Queries</li> <li>CISCOSYSTEMS.local</li> <li>Builtin</li> <li>Computers</li> <li>Domain Controllers</li> <li>ForeignSecurityPrincipals</li> <li>LDAP-USERS</li> <li>LostAndFound</li> <li>Managed Service Accounts</li> <li>Program Data</li> <li>System</li> <li>Users</li> <li>NTDS Quotas</li> <li>TPM Devices</li> </ul>	Name     Ty       State     Domain Gue     Set       Domain Users     Set       Domain Users     Set       Rough     RadallowAd     Set       RA_AllowAd     Set       RA_AllowSh     Set       RA_AllowSh     Set       RA_AllowSh     Set       RA_AllowSh     Set       Read-only D     Set       Read-only D     Set       Benterprise A     Set       Balfares     Us       SciscoTAC     Us       Guest     Us       Krbtyt     Us	ype  ccurity Group eccurity Grou eccurity	Description All domain guests All domain users Members in this group c Copy Add to a group Name Mappings Disable Account Reset Password Move Open Home Page Send Mail All Tasks ▶ Cut Delete Rename <b>Properties</b>			
< III >	& WLC-admin U	ser	нер			~
Opens the properties dialog box for the current select	ion.					

4. Klik op het tabblad Lid van, zoals in de afbeelding:

		WLC-adm	in Prope	erties		?	x		
Security	Er	vironment	Sessio	ons	Re	emote co	ontrol		
Remote Desi	top Se	ervices Profile	, CO	M+	A	ttribute E	Editor		
General Ad	dress	Account	Profile	Teleph	ones	Orga	nization		
Published Certific	cates	Member Of	Password	Replicat	tion	Dial-in	Object		
Member of:									
Name Active Directory Domain Services Folder									
Domain Users		CISCOSYSTE	MS.local/L	lsers					
Add	F	Remove							
Primary group:       Domain Users         Set Primary Group       There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.									
	0	к	ancel	Арр	oly		Help		

5. Klik op Add (Toevoegen). In het dialoogvenster dat nu wordt geopend, voert u Beheerders in en klikt u op OK, zoals in de afbeelding:

Select Groups	? X
Select this object type:	
Groups or Built-in security principals	Object Types
From this location:	
CISCOSYSTEMS.local	Locations
Enter the object names to select ( <u>examples</u> ):	
Administrators	Check Names
Advanced OK	Cancel

#### Gebruik LDP om de gebruikerskenmerken te identificeren

Dit GUI-gereedschap is een LDAP-client waarmee gebruikers bewerkingen kunnen uitvoeren, zoals verbinden, binden, zoeken, wijzigen, toevoegen of verwijderen, tegen elke LDAP- compatibele map, zoals Active Directory. LDP wordt gebruikt om objecten te bekijken die in Active Directory zijn opgeslagen, samen met hun metagegevens, zoals security descriptoren en replicatie metagegevens.

De LDP GUI-tool is inbegrepen wanneer u de Windows Server 2003 Support Tools van de product-CD installeert. In deze paragraaf wordt uitgelegd hoe u het LDP-hulpprogramma kunt gebruiken om de specifieke kenmerken te identificeren die aan de gebruiker User1 zijn gekoppeld. Sommige van deze eigenschappen worden gebruikt om de LDAP-serverconfiguratieparameters in de WLC in te vullen, zoals het type Gebruikerskenmerk en het type Gebruikersobject.

- 1. Open op de Windows 2012-server (zelfs op dezelfde LDAP-server) de Windows PowerShell en voer LDP in om toegang te krijgen tot de LDP-browser.
- Navigeer in het hoofdvenster van de LDP naar Connection > Connect en maak verbinding met de LDAP-server wanneer u het IP-adres van de LDAP-server invoert, zoals in de afbeelding wordt getoond.

1 2 2	Ldp	_ 🗆 X
Connection Browse View Options Utilities	Help	
Connect		
Bind Ctrl+B		
Disconnect		
New Ctrl+N		
Save		
Save As		
Exit		
Connect to specified server		

3. Nadat u verbinding hebt gemaakt met de LDAP-server, kiest u **Beeld** in het hoofdmenu en klikt u op **Boom**, zoals in de afbeelding:

							Idap://WIN-A0V2BU68LR9.CISCOSYSTEMS.Iocal/DC=CISCOSYSTEMS,DC=Iocal		×
Conne	ction	Browse	View	Options	Utilities	Help	•		
							defaultNamingContext: DC-CISCOSYSTEMS,DC-local; dmahControlFrunctionality: 5; domainCintonality: 5; domainCintonality: 5; dotServiceIAume: CIA=CINTS Settings,CN=WIN-A0V2BU68LR9,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=CISCOSYSTEMS,DC=local; forestFunctionality: 5; disServiceIAume: CIA=CINTS Settings,CN=WIN-A0V2BU68LR9,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=CISCOSYSTEMS,DC=local; forestFunctionality: 5; disServiceIAume: CISCOSYSTEMS,DC=local; CN=Configuration,DC=CISCOSYSTEMS,DC=local; DC=DomainNamingContext: D5=CISCOSYSTEMS,DC=local; CN=Configuration,DC=CISCOSYSTEMS,DC=local; DC=DomainNamingContext: D5=CISCOSYSTEMS,DC=local; CN=Configuration,DC=CISCOSYSTEMS,DC=local; colDomainNamingContext: D5=CISCOSYSTEMS,DC=local; serverName: CN=VIN-A0V2BU68LR9,CN=Servers,ON=Default-First-Site=Amme,CN=Sites,CN=Configuration,DC=CISCOSYSTEMS,DC=local; serverName: CN=VIN-A0V2BU68LR9,CN=Servers,ON=Default-First-Site=Amme,CN=Sites,CN=Configuration,DC=CISCOSYSTEMS,DC=local; serverName: CN=VIN-A0V2BU68LR9,CN=Servers,ON=Default-First-Site=Amme,CN=Sites,CN=Configuration,DC=CISCOSYSTEMS,DC=local; supportedContry: LD=AP_INTEG ); 12.840.113556.14.819 = (CATIVE_DIRECTORY_V61); 12.840.113556.14.819 = (CATIVE_DIRECTORY_V61); 12.840.113556.14.819 = (CATIVE_DIRECTORY_V61); 12.840.113556.14.819 = (CATIVE_DIRECTORY_V61); 12.840.113556.14.814 = (SORT); 12.840.113556.14.819 = (CARSYCC); 12.840.	28 = ( ; ; 2211 ge;	
Ready									T

4. Voer in het venster voor de resulterende boomweergave de **BaseDN** van de gebruiker in. In dit voorbeeld, Gebruiker1 wordt gevestigd onder de OU "LDAP-GEBRUIKERS" onder het domein CISCOSYSTEMS.local. Klik op **OK** zoals in de afbeelding wordt weergegeven:

8	Idap://WIN-A0V2BU68LR9.CISCOSYSTEMS.local/DC=CISCOSYSTEMS,DC=local	_		x	
Connection Browse View Options Utilities	Help				
	defaultNamingContext: DC=CISCOSYSTEMS_DC=local; domainControllerf-unctionality: 5; domainFunctionality: 5; domainFunctionality: 5; domainControllerf-unctionality: 5; highestColamet: CIN-NTDS Settings, CN=WIN-A0V2BU68LR9, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=CISCOSYSTEMS, DC=local forsesFunctionality: 5; bighestColamet: CISCOSYSTEMS_Docal; CM=Configuration, DC=CISCOSYSTEMS_DC=local; dspServiceName: CISCOSYSTEMS_Docal; CM=Configuration, DC=CISCOSYSTEMS_DC=local; CN=Schema, CN=Configuration, DC=CISCOSYSTEMS_DC=local; dspServiceName: CISCOSYSTEMS_Docal; CM=Configuration, DC=CISCOSYSTEMS_DC=local; rootDomainNamingContext: 0): DC=CISCOSYSTEMS_DC=local; DC=ForestDmsZones, DC=CISCOSYSTEMS_DC=local; schemaNamingContext: DC=CISCOSYSTEMS_DC=local; DC=ForestDmsZones, DC=CISCOSYSTEMS, DC=local; rootDomainNamingContext: DC=CISCOSYSTEMS_DC=local; schemaNamingContext: DC=CISCOSYSTEMS_DC=	; 1 = ( ); 1556.1. 302 = ( 14 = ( YNC_E ED); YNC_ED); axValF	4.528 EST ); X ); 1.4.22 lange;	= (	
Ready					

5. De linkerkant van de LDP browser toont de gehele boom die onder de gespecificeerde BaseDN verschijnt (OU=LDAP-GEBRUIKERS, dc=CISCOSYSTEMS, dc=local). Breid de structuur uit om de gebruiker te vinden.Gebruiker1. Deze gebruiker kan worden geïdentificeerd met de GN-waarde die de voornaam van de gebruiker vertegenwoordigt. In dit voorbeeld is het CN=User1. Dubbelklik op CN=User1. In het rechterdeelvenster van de LDP-browser worden alle kenmerken van Gebruiker1 weergegeven, zoals in de afbeelding:

	Idap://WIN-A0V2BU68LR9.CISCOSYSTEMS.local/DC=CISCOSYSTEMS,DC=Iocal	_ 🗆 X
Connection Browse View Options Utilities H	telp	
Connection Browse View Options Utilities F 	<pre>telp</pre>	<u></u>
	sAMACcountrype: 05306388 = ( NORMAL_USER_ACCOUNT ); userAccountContro 0x10200 = ( NORMAL_ACCOUNT   DONT_EXPIRE_PASSWD ); userAccountContro: 0x10200 = ( NORMAL_ACCOUNT   DONT_EXPIRE_PASSWD ); userAccountContro: 0x10200 = ( NORMAL_ACCOUNT   DONT_EXPIRE_PASSWD ); userAccountrype: 0x10200 = ( NORMAL_ACCOUNT   DONT_EXPIRE_PASSWD ); whenChanged: 12/24/2015 1:10:15 PM E. Europe Standard Time; whenCreated: 12/24/2015 1:19:15 PM E. Europe Standard Time;	=
< III > Ready		×

- 6. Wanneer u de WLC voor de LDAP-server configureert, voert u in het veld Gebruikerskenmerken de naam van het kenmerk in in de gebruikersrecord die de gebruikersnaam bevat. Van deze LDP-uitvoer kunt u zien dat sAMAaccountName een kenmerk is dat de gebruikersnaam "User1" bevat, dus voer het kenmerk sAMAaccountName in dat overeenkomt met het veld Gebruikerskenmerken op de WLC.
- 7. Wanneer u de WLC voor de LDAP-server configureert, voert u in het veld User Object Type de waarde in van het kenmerk LDAP objectType dat de record als gebruiker identificeert. Vaak hebben gebruikersrecords verschillende waarden voor het objectType-kenmerk, waarvan sommige uniek zijn voor de gebruiker en sommige met andere objecttypes worden

gedeeld. In de LDP-uitvoer is CN=Person een waarde die de record als een gebruiker identificeert, dus specificeer **Persoon** als het kenmerk User Object Type op de WLC.De volgende stap is het configureren van de WLC voor de LDAP-server.

#### WLC voor LDAP-server configureren

Nu de LDAP server is geconfigureerd, is de volgende stap om de WLC te configureren met details van de LDAP server. Voltooi deze stappen op de WLC GUI:

**Opmerking**:Dit document gaat ervan uit dat de WLC is geconfigureerd voor basisbediening en dat de LAP's zijn geregistreerd in de WLC. Als u een nieuwe gebruiker bent die de WLC voor basisbediening met LAP's wilt instellen, raadpleegt u <u>Lichtgewicht AP (LAP)-registratie</u> <u>naar een draadloze LAN-controller (WLC)</u>.

1. Kies op de pagina Security van de WLC AAA > LDAP in het taakvenster aan de linkerkant om naar de configuratiepagina van de LDAP-server te

gaan.										
ululu cisco	MONITOR	WLANS CONTROL	LER WIRELESS	SECURITY	MANAGEMENT	COMMANDS HELP	FEEDBA	ск		ng   Lo <u>q</u> out   <u>R</u> efresh
Security	LDAP Ser	vers								New
▼ AAA General ▼ RADIUS	Server Index	Server Address(1	pv4/Ipv6)		Port	Server	State	Secure Mode(via TLS)	Bind	
Authentication	1	172.16.16.200			389	Enabled		Disabled	Authenticated	
Fallback DNS Downloaded AVP TACACS+ LOAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	E									
▶ Local EAP										
Advanced EAP										
Priority Order										
▶ Certificate										

Klik op **Nieuw** om een LDAP-server toe te voegen. De pagina LDAP Servers > New verschijnt.

2. Geef in de pagina Bewerken LDAP-servers de details van de LDAP-server op, zoals het IPadres van LDAP-server, het poortnummer, de serverstatus inschakelen enzovoort.Kies een nummer uit de vervolgkeuzelijst Server Index (Priority) om de prioriteitsvolgorde van deze server te specificeren in vergelijking met andere geconfigureerde LDAP-servers. U kunt maximaal zeventien servers configureren. Als de controller de eerste server niet kan bereiken, probeert het de tweede server in de lijst enzovoort. Voer in het veld IP-adres van de LDAP-server in. Voer het TCP-poortnummer van de LDAP-server in het veld Port Number. Het geldige bereik loopt van 1 tot 65535 en de standaardwaarde is 389.voor de Eenvoudige bind, gebruikten wij Voor authentiek verklaard, voor de bind gebruikersbenaming die de plaats van de admin WLC gebruiker is die zal worden gebruikt om tot de server LDAP en zijn wachtwoord toegang te hebbenVoer in het veld User Base DN de voorname naam (DN) van de substructuur in op de LDAP-server die een lijst van alle gebruikers bevat. Bijvoorbeeld, ou=organisationele eenheid, .ou=volgende organisatorische eenheid, en o=corporation.com. Als de boom die gebruikers bevat de basis DN is, ga o=corporation.com of dc=corporation, dc=com in.In dit voorbeeld, wordt de gebruiker gevestigd onder de Organisatorische Eenheid (OU) LDAP-GEBRUIKERS, die, beurtelings, als deel van het lab wireless domein wordt gecreëerd.De gebruikersbasis-DN moet het volledige pad aangeven waar de gebruikersinformatie (gebruikersreferenties volgens de EAP-FAST-verificatiemethode) zich

bevindt. In dit voorbeeld, wordt de gebruiker gevestigd onder de basis DN OU=LDAP-GEBRUIKERS, DC=CISCOSYSTEMS, DC=local.Voer in het veld Gebruikerskenmerken de naam van het attribuut in in de gebruikersrecord die de gebruikersnaam bevat. Voer in het veld Gebruikersobjecttype de waarde in van het kenmerk LDAP objectType dat de record als gebruiker identificeert. Vaak hebben gebruikersrecords verschillende waarden voor het objectType-kenmerk, waarvan sommige uniek zijn voor de gebruiker en sommige worden gedeeld met andere objecttypesU kunt de waarde van deze twee velden uit uw directory server verkrijgen met het LDAP browser hulpprogramma dat als onderdeel van de Windows 2012 support tools komt. Deze Microsoft LDAP browser tool wordt LDP genoemd. Met behulp van deze tool kunt u de velden Gebruikersbasis-DN, Gebruikerskenmerk en Gebruikersobjecttype van deze specifieke gebruiker kennen. Gedetailleerde informatie over het gebruik van LDP om deze gebruikerspecifieke kenmerken te kennen, wordt besproken in het gedeelte Gebruikerskenmerken gebruiken om de sectie Gebruikerskenmerken van dit document te identificeren. Voer in het veld Server Time-out het aantal seconden in tussen heruitzendingen. Het geldige bereik is 2 tot 30 seconden en de standaardwaarde is 2 seconden.Schakel het selectievakje Serverstatus inschakelen in om deze LDAP-server in te schakelen of uit om deze uit te schakelen. De standaardwaarde is uitgeschakeld.Klik op **Toepassen** om de wijzigingen te doorvoeren. Dit is een voorbeeld dat al met deze informatie is

#### geconfigureerd:

սիսիս							Sa <u>v</u> e Configuration   <u>P</u> ing   Logout	<u>R</u> efresh
CISCO	MONITOR WLANS CONTROLLER	WIRELESS SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK	0	Home
Security	LDAP Servers > Edit						< Back Ap	ply
<ul> <li>AAA         <ul> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> <li>DNS</li> <li>Downloaded AVP</li> </ul> </li> <li>TACACS+</li> <li>LOAP</li> <li>Local Net Users</li> <li>AP Policies</li> <li>Password Policies</li> <li>Local EAP</li> <li>Advanced EAP</li> <li>Priority Order</li> </ul>	Server Index Server Address(Ipv4/Ipv6) Port Number Simple Bind Bind Username Bind Password Confirm Bind Password User Base DN User Base DN User Attribute User Object Type Secure Mode(via TLS) Server Timeout Enable Server Status	1 172:16.16.200 389 Authenticated CN=WLC-ADMIN,CN=Users CN=Users,DC=CISCOSYST sAMAccountName Person Disabled Enabled Enabled V	,DC=CISCOSYSTEM	S,C				
Certificate								

3. Nu de details over de LDAP server op WLC worden gevormd, is de volgende stap een WLAN voor webverificatie te vormen.

#### Het WLAN voor webverificatie configureren

De eerste stap is het maken van een WLAN voor de gebruikers. Voer de volgende stappen uit:

- 1. Klik op **WLAN's** vanuit de controller-GUI om een WLAN te maken.Het WLAN-venster verschijnt. Dit venster toont de WLAN's die op de controller zijn geconfigureerd.
- Klik op Nieuw om een nieuw WLAN te configureren. In dit voorbeeld, wordt WLAN genoemd Web-

Auth.

cisco		ANs		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK
WLANs	WLANs > New								
✓ WLANS WLANS	Type Profile Name		WLAN	▼ TEST					
▶ Advanced	SSID ID		LDAP-1	rest •					

- 3. Klik op Apply (Toepassen).
- 4. Definieer in het venster WLAN > Bewerken de parameters die specifiek zijn voor het WLAN.

սիսիս			Saye Configuration   Ping   Logout   Refresh
WLANs	WLANs > Edit 'LDAP-T	INCILLER WIRELESS SECORITY MEMAGEMENT COMMANDS HELP EEEDBACK EST'	< Back Apply
WLANs     WLANs	General Security	QoS Policy-Mapping Advanced	
Advanced	Profile Name	LDAP-TEST	
	Type	WLAN	
	Status	V Enabled	
	Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)	=
	Radio Policy Interface/Interface		
	Group(G)	management •	
	Multicast Vian Feature Broadcast SSID	Enabled	
	NAS-ID	none	

Controleer het aanvinkvakje Status om het WLAN in te schakelen.Voor WLAN, kies de aangewezen interface van het veld van de interfacenaam.Dit voorbeeld brengt de beheerinterface in kaart die met de WLAN-webautorisatie verbindt.

 Klik op het tabblad Beveiliging. Selecteer in het veld Layer 3 Security het selectievakje Web Policy en kies de optie

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK	Save Configuration   <u>P</u> ing   Logout   <u>R</u> efresh n <u>H</u> ome
WLANs	WLANs > Edit 'LDAP-TEST'	< Back Apply
<ul> <li>WLANS WLANS</li> <li>Advanced</li> </ul>	General       Security       QoS       Policy-Mapping       Advanced         Layer 2       Layer 3       AAA Servers         Layer 3 Security 1       Web Policy •       •         • Authentication       •       •         • Passthrough       •       Conditional Web Redirect         • On MAC Filter failure <sup>42</sup> •       •         Preauthentication ACL       IPv6       None •       WebAuth FlexAcl       None •         Sleeping Client       Enable       •       •       •       •	

Deze optie is gekozen omdat web authenticatie wordt gebruikt om de draadloze clients te verifiëren. Schakel het aanvinkvakje **Override Global Config in** om per configuratie van WLAN-webverificatie de taak in te schakelen. Kies het gewenste type webverificatie in het vervolgkeuzemenu Type webautorisatie. In dit voorbeeld wordt interne webverificatie gebruikt.**Opmerking**: webverificatie wordt niet ondersteund met 802.1x-verificatie. Dit

betekent dat u geen 802.1x of WPA/WPA2 met 802.1x kunt kiezen als Layer 2-beveiliging wanneer u webverificatie gebruikt. Web verificatie wordt ondersteund met alle andere Layer 2 security parameters.

6. Klik op het tabblad **AAA-servers**. Kies de geconfigureerde LDAP-server in het keuzemenu van de LDAP-server. Als u een lokale database of RADIUS-server gebruikt, kunt u de verificatieprioriteit instellen onder de *prioriteitsvolgorde voor verificatie van het web-auth* gebruikersveld.



7. Klik op **Apply** (Toepassen).**Opmerking**: in dit voorbeeld worden Layer 2 Security methoden om gebruikers te verifiëren niet gebruikt, dus kies **Geen** in het veld Layer 2 Security.

### Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Om deze instelling te controleren, sluit u een draadloze client aan en controleert u of de configuratie werkt zoals verwacht.

De draadloze client komt omhoog, en de gebruiker voert de URL, zoals <u>www.yahoo.com</u>, in de webbrowser in. Omdat de gebruiker niet is geverifieerd, wordt de gebruiker door de WLC omgeleid naar de interne web login URL.

De gebruiker wordt gevraagd om de gebruikersreferenties. Nadat de gebruiker de gebruikersnaam en het wachtwoord heeft ingevoerd, neemt de inlogpagina de inloggegevens van de gebruiker in en stuurt deze, na het indienen, het verzoek terug naar het action\_URL-voorbeeld <a href="http://1.1.1.1/login.html">http://1.1.1.1/login.html</a> van de WLC-webserver. Dit wordt geleverd als een invoerparameter voor de klant om URL om te leiden, waarbij 1.1.1.1 het Virtual Interface Address op de switch is.

De WLC authenticeert de gebruiker tegen de LDAP gebruikersdatabase. Na succesvolle verificatie stuurt de WLC-webserver de gebruiker door naar de geconfigureerde doorverwijzing-URL of naar de URL waarmee de client is gestart, zoals <u>www.yahoo.com.</u>

•	III	
	More information	
	Secontinue to this website (not recommended).	
	Click here to close this webpage.	
	We recommend that you close this webpage and do not continue to this website.	
	Security certificate problems may indicate an attempt to fool you or intercept any data you server.	end to the
	The security certificate presented by this website was not issued by a trusted certificate author	rity.
8	There is a problem with this website's security certificate.	
125		

#### Welcome to the Cisco wireless network

E.

Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and putyour air space to work.

Uper Hame	User1
Password	•••••
	Submit

🐴 https://1.1.1.1 - Logout - Micros 🔳 🗖 🔀
File Edit View Favorites Tools Help 🛛
🕝 Back 🔹 🕑 - 💽 🛃 🏠 🤺
Web Authentication
Login Successful !
You can now use all regular network services over the wireless network.
Please retain this small logout window in order to logoff when done. Note that you can always use the following URL to retrieve this page: <u>https://1.1.1.1/logout.html</u>
Logout
🙆 Dor 🔒 🔮 Internet

### Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Gebruik deze opdrachten om problemen met uw configuratie op te lossen:

- debug mac addr <client-MAC-adres xx:xx:xx:xx:xx:xx:xx</li>
- · debug aaa all enable
- debug pem state enable
- debug pem gebeurtenissen activeren
- debug DHCP bericht activeren
- debug DHCP-pakket inschakelen

Dit is een voorbeelduitvoer van de opdrachten debug mac addr cc:fa:00:f7:32:35

#### debug aaa Idap activeren

(Cisco\_Controller) >\*pemReceiveTask: Dec 24 03:45:23.089: cc:fa:00:f7:32:35 Sent an XID frame \*apfMsConnTask\_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Processing assoc-req station:cc:fa:00:f7:32:35 AP:00:23:eb:e5:04:10-01 thread:18ec9330 \*apfMsConnTask\_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Association received from mobile on BSSID 00:23:eb:e5:04:1f AP AP1142-1 \*apfMsConnTask\_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Global 200 Clients are allowed to AP

\*apfMsConnTask\_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Max Client Trap Threshold: 0 cur: 1 \*apfMsConnTask\_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Rf profile 600 Clients are allowed to AP wlan \*apfMsConnTask\_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 override for default ap group, marking intgrp NULL \*apfMsConnTask\_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying Interface policy on Mobile, role Local. Ms NAC State 2 Quarantine Vlan 0 Access Vlan 16 \*apfMsConnTask\_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Re-applying interface policy for client \*apfMsConnTask\_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Changing IPv4 ACL 'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf\_policy.c:2699) \*apfMsConnTask\_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Changing IPv6 ACL 'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf\_policy.c:2720) \*apfMsConnTask\_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 apfApplyWlanPolicy: Apply WLAN Policy over PMIPv6 Client Mobility Type, Tunnel User - 0 \*apfMsConnTask\_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 In processSsidIE:6246 setting Central switched to TRUE \*apfMsConnTask\_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 In processSsidIE:6249 apVapId = 1 and Split Acl Id = 65535 \*apfMsConnTask\_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying site-specific Local Bridging override for station cc:fa:00:f7:32:35 - vapId 1, site 'default-group', interface 'management' \*apfMsConnTask\_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying Local Bridging Interface Policy for station cc:fa:00:f7:32:35 - vlan 16, interface id 0, interface 'management' \*apfMsConnTask\_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 processSsidIE statusCode is 0 and status is 0 \*apfMsConnTask\_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 processSsidIE ssid\_done\_flag is 0 finish\_flag is 0 \*apfMsConnTask\_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 STA - rates (3): 24 164 48 0 0 0 0 0 0 0 0 0 0 0 0 0 \*apfMsConnTask\_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 suppRates statusCode is 0 and gotSuppRatesElement is 1 \*apfMsConnTask\_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 AID 2 in Assoc Req from flex AP 00:23:eb:e5:04:10 is same as in mscb cc:fa:00:f7:32:35 \*apfMsConnTask\_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 apfMs1xStateDec \*apfMsConnTask\_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Change state to START (0) last state WEBAUTH\_REQD (8) \*apfMsConnTask\_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 pemApfAddMobileStation2: APF\_MS\_PEM\_WAIT\_L2\_AUTH\_COMPLETE = 0. \*apfMsConnTask\_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 START (0) Initializing policy \*apfMsConnTask\_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 START (0) Change state to AUTHCHECK (2) last state START (0) \*apfMsConnTask\_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4) last state AUTHCHECK (2) \*pemReceiveTask: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 Removed NPU entry. \*apfMsConnTask\_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Not Using WMM Compliance code qosCap 00 \*apfMsConnTask\_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 00:23:eb:e5:04:10 vapId 1 apVapId 1 flex-acl-name: \*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 L2AUTHCOMPLETE (4) Change state to WEBAUTH\_REQD (8) last state L2AUTHCOMPLETE (4) \*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) pemApfAddMobileStation2 3802, Adding TMP rule \*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Adding Fast Path rule

type = Airespace AP Client - ACL passthru

#### radio

on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0 IPv4 ACL I \*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Fast Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206, IntfId = 0 Local Bridging Vlan = 16, Local Bridging intf id = 0\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Fast Path rule (contd...) AVC Ratelimit: AppID = 0 , AppAction = 4, AppToken = 15206 AverageRate = 0, BurstRate = 0\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Fast Path rule (contd...) AVC Ratelimit: AppID = 0 , AppAction = 4, AppToken = 15206 AverageRate = 0, BurstRate = 0\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Fast Path rule (contd...) AVC Ratelimit: AppID = 0 ,AppAction = 4, AppToken = 15206 AverageRate = 0, BurstRate = 0\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255) \*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) pemApfAddMobileStation2 3911, Adding TMP rule \*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Replacing Fast Path rule type = Airespace AP Client - ACL passthru on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0 IPv4 AC \*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Fast Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206, IntfId = 0 Local Bridging Vlan = 16, Local Bridging intf id = 0 \*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Fast Path rule (contd...) AVC Ratelimit: AppID = 0 ,AppAction = 4, AppToken = 15206 AverageRate = 0, BurstRate = 0\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Fast Path rule (contd...) AVC Ratelimit: AppID = 0 ,AppAction = 4, AppToken = 15206 AverageRate = 0, BurstRate = 0\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Fast Path rule (contd...) AVC Ratelimit: AppID = 0 , AppAction = 4, AppToken = 15206 AverageRate = 0, BurstRate = 0\*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255) \*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2 (apf\_policy.c:359) Changing state for mobile cc:fa:00:f7:32:35 on AP 00:23:eb:e5:04:10 from Associated to Associated \*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2:session timeout forstation cc:fa:00:f7:32:35 - Session Tout 1800, apfMsTimeOut '1800' and sessionTimerRunning flag is 1 \*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Scheduling deletion of Mobile Station: (callerId: 49) in 1800 seconds \*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Func: apfPemAddUser2, Ms Timeout = 1800, Session Timeout = 1800 \*apfMsConnTask\_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Sending assoc-resp with status 0 station:cc:fa:00:f7:32:35 AP:00:23:eb:e5:04:10-01 on apVapId 1 \*apfMsConnTask\_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 Sending Assoc Response to station on BSSID 00:23:eb:e5:04:1f (status 0) ApVapId 1 Slot 1 \*apfMsConnTask\_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 apfProcessAssocReq (apf\_80211.c:10187) Changing state for mobile cc:fa:00:f7:32:35 on AP 00:23:eb:e5:04:10 from Associated to Associated

\*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 2,

dtlFlags 0x0 \*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 Sent an XID frame \*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 2, dtlFlags 0x0 \*pemReceiveTask: Dec 24 03:45:43.558: cc:fa:00:f7:32:35 Sent an XID frame \*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP received op BOOTREQUEST (1) (len 322, vlan 16, port 1, encap 0xec03, xid 0x62743488) \*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype Off:ff:ff:ff:ff:ff \*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block settings: dhcpServer: 172.16.16.25, dhcpNetmask: 255.255.254.0, dhcpGateway: 172.16.16.1, dhcpRelay: 172.16.16.25 VLAN: 16 \*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25 mscbVapLocalNetMask= 255.255.254.0 mscbdhcpRelay=172.16.16.25 \*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25 (local address 172.16.16.25, gateway 172.16.16.25, VLAN 16, port 1) \*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block settings: dhcpServer: 172.16.16.25, dhcpNetmask: 255.255.254.0, dhcpGateway: 172.16.16.1, dhcpRelay: 172.16.16.25 VLAN: 16 \*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE \*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block settings: dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0, dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25 VLAN: 16 \*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25 mscbVapLocalNetMask= 255.255.254.0 mscbdhcpRelay=172.16.16.25 \*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25 (local address 172.16.16.25, gateway 172.16.16.25, VLAN 16, port 1) \*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP transmitting DHCP DISCOVER (1) \*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1 \*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP xid: 0x62743488 (1651782792), secs: 0, flags: 0 \*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP chaddr: cc:fa:00:f7:32:35 \*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0 \*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP siaddr: 0.0.0.0, giaddr: 172.16.16.25 \*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block settings: dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0, dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25 VLAN: 16 \*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE \*DHCP Proxy Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP received op BOOTREPLY (2) (len 572, vlan 0, port 0, encap 0x0, xid 0x62743488) \*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP sending REPLY to STA (len 418, port 1, vlan 16) \*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP transmitting DHCP OFFER (2) \*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0 \*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP xid: 0x62743488 (1651782792), secs: 0, flags: 0 \*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP chaddr: cc:fa:00:f7:32:35 \*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP ciaddr: 0.0.0.0, yiaddr: 172.16.16.122 \*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0 \*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP server id: 1.1.1.1 rcvd server id: 172.16.16.25 \*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP received op BOOTREQUEST (1) (len 334, vlan 16, port 1, encap 0xec03, xid 0x62743488) \*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype

Off:ff:ff:ff:ff

\*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block settings:

dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,

dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25 VLAN: 16 \*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25 mscbVapLocalNetMask= 255.255.254.0 mscbdhcpRelay=172.16.16.25 \*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25 (local address 172.16.16.25, gateway 172.16.16.25, VLAN 16, port 1) \*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP transmitting DHCP REQUEST (3) \*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1 \*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP xid: 0x62743488 (1651782792), secs: 0, flags: 0 \*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP chaddr: cc:fa:00:f7:32:35 \*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0 \*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP siaddr: 0.0.0.0, giaddr: 172.16.16.25 \*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP requested ip: 172.16.16.122 \*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP server id: 172.16.16.25 rcvd server id: 1.1.1.1 \*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block settings: dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0, dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25 VLAN: 16 \*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE \*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP received op BOOTREPLY (2) (len 572, vlan 0, port 0, encap 0x0, xid 0x62743488) \*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP setting server from ACK (mscb=0x40e64b88 ip=0xac10107a)(server 172.16.16.25, yiaddr 172.16.16.122) \*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP sending REPLY to STA (len 418, port 1, vlan 16) \*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP transmitting DHCP ACK (5) \*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0 \*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP xid: 0x62743488 (1651782792), secs: 0, flags: 0 \*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP chaddr: cc:fa:00:f7:32:35 \*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP ciaddr: 0.0.0.0, yiaddr: 172.16.16.122 \*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0 \*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP server id: 1.1.1.1 rcvd server id: 172.16.16.25 \*ewmwebWebauth1: Dec 24 03:46:01.222: cc:fa:00:f7:32:35 Username entry (User1) created for mobile, length = 7\*ewmwebWebauth1: Dec 24 03:46:01.222: cc:fa:00:f7:32:35 Username entry (User1) created in mscb for mobile, length = 7\*aaaQueueReader: Dec 24 03:46:01.222: AuthenticationRequest: 0x2b6bdc3c \*aaaQueueReader: Dec 24 03:46:01.222: proxyState.....CC:FA:00:F7:32:35-00:00 \*aaaQueueReader: Dec 24 03:46:01.222: Packet contains 15 AVPs (not shown) \*LDAP DB Task 1: Dec 24 03:46:01.222: ldapTask [1] received msg 'REQUEST' (2) in state 'IDLE' (1)\*LDAP DB Task 1: Dec 24 03:46:01.222: LDAP server 1 changed state to INIT

\*LDAP DB Task 1: Dec 24 03:46:01.223: LDAP\_OPT\_REFERRALS = -1 \*LDAP DB Task 1: Dec 24 03:46:01.223: ldapInitAndBind [1] called lcapi\_init (rc = 0 - Success) \*LDAP DB Task 1: Dec 24 03:46:01.225: ldapInitAndBind [1] configured Method Authenticated lcapi\_bind (rc = 0 - Success) \*LDAP DB Task 1: Dec 24 03:46:01.225: LDAP server 1 changed state to CONNECTED \*LDAP DB Task 1: Dec 24 03:46:01.225: disabled LDAP\_OPT\_REFERRALS \*LDAP DB Task 1: Dec 24 03:46:01.225: LDAP\_CLIENT: UID Search (base=CN=Users,DC=CISCOSYSTEMS,DC=local, pattern=(&(objectclass=Person)(sAMAccountName=User1))) \*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP\_CLIENT: ldap\_search\_ext\_s returns 0 -5 \*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP\_CLIENT: Returned 2 msgs including 0 references \*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP\_CLIENT: Returned msg 1 type 0x64 \*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP\_CLIENT: Received 1 attributes in search entry msg \*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP\_CLIENT: Returned msg 2 type 0x65 \*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP\_CLIENT : No matched DN \*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP\_CLIENT : Check result error 0 rc 1013 \*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP\_CLIENT: Received no referrals in search result msg \*LDAP DB Task 1: Dec 24 03:46:01.226: ldapAuthRequest [1] 172.16.16.200 - 389 called lcapi\_query base="CN=Users,DC=CISCOSYSTEMS,DC=local" type="Person" attr="sAMAccountName" user="User1" (rc = 0 - Success) \*LDAP DB Task 1: Dec 24 03:46:01.226: Attempting user bind with username CN=User1, CN=Users, DC=CISCOSYSTEMS, DC=local \*LDAP DB Task 1: Dec 24 03:46:01.228: LDAP ATTR> dn = CN=User1,CN=Users,DC=CISCOSYSTEMS,DC=local (size 45) \*LDAP DB Task 1: Dec 24 03:46:01.228: Handling LDAP response Success \*LDAP DB Task 1: Dec 24 03:46:01.228: Authenticated bind : Closing the binded session \*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_REQD (8) Change state to WEBAUTH\_NOL3SEC (14) last state WEBAUTH\_REQD (8) \*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 apfMsRunStateInc \*LDAP DB Task 1: Dec 24 03:46:01.228: ldapClose [1] called lcapi\_close (rc = 0 - Success) \*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH\_NOL3SEC (14) Change state to RUN (20) last state WEBAUTH\_NOL3SEC (14) \*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 Stopping deletion of Mobile Station: (callerId: 74) \*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 Setting Session Timeout to 1800 sec starting session timer for the mobile \*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Reached PLUMBFASTPATH: from line 6972 \*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Replacing Fast Path rule type = Airespace AP Client on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0 IPv4 ACL ID = 255, IPv6 ACL ID \*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206, IntfId = 0 Local Bridging Vlan = 16, Local Bridging intf id = 0\*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule (contd...) AVC Ratelimit: AppID = 0 , AppAction = 4, AppToken = 15206 AverageRate = 0, BurstRate = 0\*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule (contd...) AVC Ratelimit: AppID = 0 , AppAction = 4, AppToken = 15206 AverageRate = 0, BurstRate = 0\*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule (contd...) AVC Ratelimit: AppID = 0 , AppAction = 4, AppToken = 15206 AverageRate = 0, BurstRate = 0\*ewmwebWebauth1: Dec 24 03:46:01.229: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Successfully

plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)

\*pemReceiveTask: Dec 24 03:46:01.229: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 1,
dtlFlags 0x0

(Cisco Controller) >show client detail cc:fa:00:f'	7:32:35
Client MAC Address	cc:fa:00:f7:32:35
Client Username	User1
AP MAC Address	00:23:eb:e5:04:10
AP Name	AP1142-1
AP radio slot Id	1
Client State	Associated
Client User Group	Heer1
Client NAC OOR State	
Wirelegg IAN Id	1
Wireless LAN Id	
Wireless LAN Network Name (SSID)	
Wireless LAN Profile Name	LDAP-TEST
Hotspot (802.11u)	Not Supported
BSSID	00:23:eb:e5:04:1f
Connected For	37 secs
Channel	36
IP Address	172.16.16.122
Gateway Address	172.16.16.1
Netmask	255.255.254.0
Association Id	2
Authentication Algorithm	Open System
Reason Code	1
Status Code	0
More or (g)uit current module or <ctrl-z> to abo</ctrl-z>	ort
Session Timeout	1800
Client CCX version	No CCX support
	Silver
Ave data Pata	0
Avy uata kate	0
Burst data Rate	0
Avg Real time data Rate	0
Burst Real Time data Rate	0
802.1P Priority Tag	disabled
CTS Security Group Tag	Not Applicable
KTS CAC Capability	No
Qos Map Capability	No
WMM Support	Enabled
APSD ACs	BK BE VI VO
Current Rate	m7
Supported Rates	12.0,18.0,24.0
Mobility State	Local
Mobility Move Count	0
	37

Policy Type..... N/A Encryption Cipher..... None Protected Management Frame ..... No Management Frame Protection..... No EAP Type..... Unknown FlexConnect Data Switching..... Central FlexConnect Dhcp Status..... Central FlexConnect Vlan Based Central Switching..... No FlexConnect Authentication..... Central FlexConnect Central Association..... No Interface..... management Quarantine VLAN..... 0 --More or (q)uit current module or <ctrl-z> to abort Access VLAN..... 16 Local Bridging VLAN..... 16 Client Capabilities: CF Pollable..... Not implemented CF Poll Request..... Not implemented Short Preamble..... Not implemented PBCC..... Not implemented Channel Agility..... Not implemented Listen Interval..... 10 Fast BSS Transition..... Not implemented 11v BSS Transition..... Not implemented Client Wifi Direct Capabilities: WFD capable..... No Manged WFD capable..... No Cross Connection Capable..... No Support Concurrent Operation..... No Fast BSS Transition Details: Client Statistics: Number of Bytes Received..... 16853 Number of Bytes Sent..... 31839 Total Number of Bytes Sent..... 31839 Total Number of Bytes Recv..... 16853 Number of Bytes Sent (last 90s)..... 31839 --More or (q)uit current module or <ctrl-z> to abort Number of Bytes Recv (last 90s)..... 16853 Number of Packets Received..... 146 Number of Interim-Update Sent..... 0 Number of EAP Id Request Msg Timeouts..... 0 Number of EAP Id Request Msg Failures..... 0 Number of EAP Request Msg Timeouts..... 0 Number of EAP Request Msg Failures..... 0 Number of EAP Key Msg Timeouts..... 0 Number of EAP Key Msg Failures..... 0 Number of Data Retries..... 2 Number of RTS Retries..... 0 Number of Duplicate Received Packets..... 0 Number of Decrypt Failed Packets..... 0 Number of Mic Failured Packets..... 0 Number of Mic Missing Packets..... 0 Number of RA Packets Dropped..... 0 Number of Policy Errors..... 0 Radio Signal Strength Indicator..... -48 dBm Signal to Noise Ratio..... 41 dB Client Rate Limiting Statistics: Number of Data Packets Received..... 0 Number of Data Rx Packets Dropped..... 0

--More or (q)uit current module or <ctrl-z> to abort Number of Data Bytes Received..... 0 Number of Data Rx Bytes Dropped..... 0 Number of Realtime Packets Received..... 0 Number of Realtime Rx Packets Dropped..... 0 Number of Realtime Bytes Received..... 0 Number of Realtime Rx Bytes Dropped..... 0 Number of Data Packets Sent..... 0 Number of Data Tx Packets Dropped..... 0 Number of Data Bytes Sent..... 0 Number of Data Tx Bytes Dropped..... 0 Number of Realtime Packets Sent..... 0 Number of Realtime Tx Packets Dropped..... 0 Number of Realtime Bytes Sent..... 0 Number of Realtime Tx Bytes Dropped..... 0 Nearby AP Statistics: AP1142-1(slot 0) antenna0: 25 secs ago..... -37 dBm antennal: 25 secs ago..... -37 dBm AP1142-1(slot 1) antenna0: 25 secs ago..... -44 dBm antennal: 25 secs ago..... -57 dBm DNS Server details: DNS server IP ..... 0.0.0.0 --More or (q)uit current module or <ctrl-z> to abort DNS server IP ..... 0.0.0.0 Assisted Roaming Prediction List details:

Client Dhcp Required: False

#### Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.