ワイヤレス LAN コントローラ(WLC)上での LDAP を使用した Web 認証の設定例

内容

目次
<u>はじめに</u>
·····································
<u>要件</u> 。 <u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>表記法</u> ————————————————————————————————————
<u>Web 認証プロセス</u>
トレート <u>ネットワーク図</u>
<u>コンフィギュレーション</u>
<u>LDAP サーバの設定</u>
<u> ドメイン コントローラでのユーザの作成</u>
<u>OU でのユーザ データベースの作成</u>
<u>ユーザの LDAP アクセスの設定</u>
<u>匿名バインド</u>
<u>Windows 2012 Essentials Serverで匿名バインド機能を有効にする</u>
<u>ユーザへのANONYMOUS LOGONアクセス権の付与</u>
<u>OU での List Contents 権限の付与</u>
<u>認証されたバインド</u>
<u>WLC-adminへの管理者権限の付与</u>
<u>LDP を使用したユーザ属性の確認</u>
<u>LDAP サーバの WLC の設定</u>
Ⅰ <u>Web 認証用の WLAN の設定</u>
<u>トラブルシュート</u>
*

はじめに

このドキュメントでは、Web認証用にワイヤレスLANコントローラ(WLC)を設定する方法につい て説明します。ユーザクレデンシャルを取得してユーザを認証するために、Lightweight Directory Access Protocol(LDAP)サーバをWeb認証用のバックエンドデータベースとして設定する方法につ いて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ・ Lightweight アクセス ポイント(LAP)および Cisco WLC の設定に関する知識
- Control And Provisioning of Wireless Access Point Protocol(CAPWAP)に関する知識
- Lightweight Directory Access Protocol(LDAP)、Active Directory、およびドメインコントロー ラのセットアップ方法と設定方法に関する知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ・ファームウェア リリース 8.2.100.0 が稼働している Cisco 5508 WLC
- ・ Cisco 1142 シリーズ LAP
- Cisco 802.11a/b/gワイヤレスクライアントアダプタ
- ・ LDAPサーバの役割を実行するMicrosoft Windows 2012 Essentialsサーバ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在 的な影響について確実に理解しておく必要があります。

背景説明

表記法

ドキュメント表記の詳細については、『<u>シスコ テクニカル ティップスの表記法</u>』を参照してくだ さい。

Web 認証プロセス

Web認証は、有効なユーザ名とパスワードが正しく入力されるまで、特定のクライアントからの IPトラフィック(DHCPおよびDNS関連パケットを除く)をコントローラで拒否させるレイヤ3セ キュリティ機能です。Web 認証を使用してクライアントを認証する場合は、クライアントごとに ユーザ名とパスワードを定義する必要があります。次に、クライアントがワイヤレスLANに参加 しようとすると、ログインページでプロンプトが表示されたときにユーザ名とパスワードを入力 する必要があります。

Web 認証が(レイヤ 3 セキュリティ下で)有効になっている場合、ユーザが、最初にある URL にアクセスしようとした際に、Web ブラウザにセキュリティ警告が表示されることがあります。

▼ ヒン ール <u>http:/</u>	ト:この証明書の警告を削除するには、サードパーティの信頼できる証明書をインス する方法に関する次のガイドに戻ってください [/] /www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-
<u>contr</u>	ollers/109597-csr-chained-certificates-wic-00.html
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.
	Click here to close this webpage.
	Solution Continue to this website (not recommended).
	More information

.

Yesをクリックして続行するか(Firefoxブラウザなどのより正確なContinue to this website(推奨 されません))、またはクライアントのブラウザにセキュリティ警告が表示されない場合、Web認 証システムは図に示すようにログインページにクライアントをリダイレクトします。



デフォルトのログイン ページには、Cisco ロゴや Cisco 特有のテキストが表示されます。Web 認 証システムが次のいずれかを表示するように選択できます。

- ・ デフォルトのログイン ページ
- デフォルトのログインページの変更バージョン
- 外部の Web サーバに設定する、カスタマイズされたログイン ページ
- コントローラにダウンロードする、カスタマイズされたログイン ページ

Web認証のログインページで有効なユーザ名とパスワードを入力してSubmitをクリックすると、 送信されたクレデンシャル(この場合はLDAP)と、バックエンドデータベースからの正常な認 証に基づいて認証されます。その後、Web 認証システムは、ログインに成功したことを示す(ロ グイン成功)ページを表示し、認証されたクライアントを要求された URL ヘリダイレクトします 。



デフォルトのログイン成功ページには、仮想ゲートウェイアドレス URL(<u>https://1.1.1.1/logout.html</u>)へのポインタが含まれます。コントローラの仮想インターフェイ スに設定した IP アドレスは、ログイン ページのリダイレクト アドレスとして機能します。

このドキュメントでは、WLC 上の内部 Web ページを Web 認証用に使用する方法を説明します 。この例では、LDAPサーバをWeb認証用のバックエンドデータベースとして使用して、ユーザ クレデンシャルを取得し、ユーザを認証します。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供して います。

◆ 注:このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool(登録ユーザ専用)を参照してください。一部ツールについては、ゲスト登録のお客様 にはアクセスできない場合がありますことをご了承ください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



Wireless Client

コンフィギュレーション

この設定を実装するには、次の作業を実行します。

- <u>LDAP サーバの設定</u>
- <u>LDAP サーバの WLC の設定</u>
- ・ Web 認証用の WLAN の設定

LDAP サーバの設定

最初の手順では、LDAP サーバを設定します。LDAP サーバは、ワイヤレス クライアントのユー ザ クレデンシャルを格納するためのバックエンド データベースとして機能します。この例では、 LDAPサーバとしてMicrosoft Windows 2012 Essentialsサーバが使用されます。

LDAP サーバを設定する最初の手順として、LDAP サーバでユーザ データベースを作成します。 これにより、WLC はユーザ認証時にこのデータベースをクエリできます。

ドメイン コントローラでのユーザの作成

組織単位(OU)には、PersonProfile のパーソナル エントリへの参照を持つ複数のグループが含まれます。1 人で複数のグループのメンバになることができます。オブジェクト クラスと属性定義はすべて LDAP スキーマのデフォルトです。各グループには、そこに所属する各人への参照 (dn)が含まれます。

この例では新しい OU LDAP-USERS が作成され、この OU の中にユーザ User1 が作成されました。このユーザに対して LDAP アクセスを設定することで、WLC はユーザ認証でこの LDAP デ ータベースをクエリできます。

この例で使用するドメインはCISCOSYSTEMS.localです。

OU でのユーザ データベースの作成

この項では、ドメインに新しい OU を作成し、この OU の中に新しいユーザを作成する手順を説 明します。

- 1. Windows PowerShellを開き、「servermanager.exe」と入力します。
- 2. Server Managerウィンドウで、AD DSをクリックします。次に、サーバ名を右クリックして、Active Directory Users and Computersを選択します。
- 3. ドメイン名(この例ではCISCOSYSTEMS.local)を右クリックし、コンテキストメニューから New > Organizational Unitに移動して新しいOUを作成します。

			Active Direc	tory Users	and Compute	ers	_ 🗆 X
File Action View H	Help						
🗢 🄿 🖄 🖬 📋	🖾 🙆 🔝 🖬 🔏 🗞	🛅 🍸 💆	38				
Active Directory Users	and Computers [WIN-A0\ Name	2	Туре 📩	Description			
Saved Queries	🛄 Bu	iltin	builtinDomain				
CISCOSYSTEMS.Io	Call Control	mnuterc	Container	Default con	tainer for up		
	Delegate Control	u	. Container	Default con	tainer for sec		
Domain (Find	e	. Container	Default con	tainer for ma		
ForeignSe	Change Domain	ata	Container	Default loca	ation for stor		
TPRS	Change Domain Controller		Container	Default con	tainer for un		
LostAndF	Raise domain functional level	ire	infrastructureU	Derugit con	tunier for up		
Managed	Operations Masters	u	lostAndFound	Default con	tainer for or		
Program System	New	•	Computer		fications co		
b 🗎 Users	All Tasks	•	Contact				
NTDS Qu	View	•	Group		tainer for do		
D IPM Dev	Refresh		InetOrgPerson				
	Export List		msImaging-PSP	5			
	Decention		MSMQ Queue A	lias			
	Properties		Organizational U	nit			
	Help		Printer				
			User				
			Shared Folder				
					1		
< III	>						
Create a new object							

4. 次の図に示すように、このOUに名前を割り当て、OKをクリックします。

New Object - Organizational Unit	x
Create in: CISCOSYSTEMS.local/	
Name:	
LDAP-USERS	
Protect container from accidental deletion	
OK Cancel Help	

これで、LDAP サーバに新しい OU LDAP-USERS が作成されました。次に、この OU にユーザ User1 を作成します。これを行うには、次の手順を実行します。

1. 作成した新しい OU を右クリックします。次の図に示すように、表示されたコンテキストメ ニューからLDAP-USERS> New > Userに移動して、新しいユーザを作成します。

					Active Directory Users and Computers	- 0 ×
File Action View	Help					
(* *) 🖄 📰 🐇		6		2 2 🗊 🝸 🔟 2		
Active Directory Us Saved Queries Saved Queries CISCOSYSTEM Salitin Salitin Computers Computers Salitin	sers and Com Nan S.local introllers unityPrincipali iervice Accour RC Delegate Contr	ne 101	Тут	Description	There are no items to show in this view.	
	Move					
	Find					
	All Tasks			Computer		
	View			Group		
	Cut Delete Rename Refresh Evenet List			InetOrgPerson msImaging-PSPs MSMQ Queue Alias Organizational Unit Printer		
	Properties			User		
	Help		-	Shared Folder		
< m						
Create a new object						
		4	21			▲ P 🙀 🕼 12:14 PM 12:17/2015

2. 次の例に示すように、ユーザ設定ページで必須フィールドに情報を入力します。この例では、[User logon name] フィールドに User1 が指定されています。

これは、クライアントを認証するために LDAP データベースで検証されるユーザ名です。 この例では、[First name] および [Full Name] フィールドに User1 が指定されています。 [Next] をクリックします。

Create in				
	: CISCOSYS	TEMS.local/LD/	AP-USERS	
First name:	User1	1	Initials:	
Last name:				
Full name:	User1			7
User logon name:				-
User1		@CISCOSY	STEMS.local	v
User logon name (pr	e-Windows 200			
CISCOSYSTEMS\		User1		
		< Back	Next >	Cancel

3. パスワードを入力し、確認のためのパスワードを入力します。[Password never expires] オ プションを選択して [Next] をクリックします。

	New Object - User	X
Create in: C	ISCOSYSTEMS.local/LDAP-USERS	
Password:	•••••	
Confirm password:	••••••	
 User must change pas User cannot change p Password never expire Account is disabled 	sword at next logon assword s	
	< Back Next > Car	ncel

4. [Finish] をクリックします。

新しいユーザ User1 が OU LDAP-USERS に作成されます。以下は、ユーザ クレデンシャ ルです。

- ユーザ名: User1
- パスワード: Laptop123

		New O	bject - I	Jser		
8	Create in:	CISCOSYSTE	MS.local/I	LDAP-USEF	IS	
When y	ou <mark>clic</mark> k Finish	the following ol	bject will be	e created:		
Full nan	ne: User1					^
User log	gon name: Use	r1@CISCOSYS	TEMS.loc	al		
The pa	ssword never e	xpires.				
						~
			Rack	Finis	b	Cancel
		L	Dack			Caricel

これで OU の中にユーザが作成されました。次に、このユーザの LDAP アクセスを設定します。

ユーザの LDAP アクセスの設定

AnonymousまたはAuthenticatedのいずれかを選択して、LDAPサーバのローカル認証バインド方 式を指定できます。Anonymous方式では、LDAPサーバへの匿名アクセスが許可されます。 Authenticated方式では、アクセスを保護するためにユーザ名とパスワードを入力する必要があり ます。デフォルトでは [Anonymous] になっています。

このセクションでは、匿名方式と認証方式の両方を設定する方法について説明します。

匿名バインド

注:匿名バインドの使用は推奨されません。匿名バインドを許可するLDAPサーバでは、クレデ ンシャル認証のタイプは必要ありません。攻撃者は、匿名バインドエントリを利用して、LDAPデ ィレクタ上のファイルを表示する可能性があります。

LDAPアクセス用に匿名ユーザを設定するには、このセクションの手順を実行します。

Windows 2012 Essentials Serverで匿名バインド機能を有効にする

サードパーティアプリケーション(この例ではWLC)がLDAP上のWindows 2012 ADにアクセス するには、Windows 2012で匿名バインド機能が有効になっている必要があります。デフォルトで は、Windows 2012 ドメイン コントローラでは匿名 LDAP 操作は許可されていません。匿名バイ ンド機能を有効にするには、次の手順を実行します。

- 1. Windows PowerShellでADSIEdit.mscと入力して、ADSI編集ツールを起動します。このツー ルは、Windows 2012サポートツールの一部です。
- 2. ADSI Editウィンドウで、ルートドメイン(Configuration [WIN-A0V2BU68LR9.CISCOSYSTEMS.local])を展開します。

CN=Services > CN=Windows NT > CN=Directory Serviceの順に移動します。図に示すよう に、CN=Directory Serviceコンテナを右クリックし、コンテキストメニューから Propertiesを選択します。

2				ADSI Edit		- 0 ×
File Action View Help						
🗢 🏘 🙇 📷 🗶 🖾 🤅	» 🛛 💼					
2 ADSI Edit		Name	Class	Distinguished Name	7	Actions
Domain [WIN-A0V2BU68LR	R9.CISCOSYSTEMS.local]	CN=Directory Service	nTDSService	CN= Directory Service, CN= Windows NT, CN= Services, CN= Configuration, DC= CIS		CN=Windows NT
A Configuration [WIN-A0V2B	BU68LR9.CISCOSYSTEMS.local]					More Actions
A CN=Configuration, DC=	ECISCOSYSTEMS, DC Elocal					Hole Actions
CN=Extended-Right	5					
CN=ForestUpdates						
CN=LostAndFound	Config					
CN=NIDS Quotas						
CN=Physical Locati	ons					
a 🔛 CNii Services						
CN=Claims Con	figuration					
CN=Group Key I	Distribution Service					
CN=MsmqServi	ces					
CN=NetServices						
CN=Public Key !	Services					
CN=RMAS A CN=Windows N	IT					
CN=Dire-***	n Canica					
CN=Sites	Move					
CN=WellKnown	New Connection from Here					
	New	*				
	Delete					
	Rename					
-	Refresh					
L	Properties					
	Help					
Opens the properties dialog box for	r the current selection.	25			(h)	
						- 107 PM

 [CN=Directory Service Properties] ウィンドウで [Attribute] フィールドの下にある [dsHeuristics] 属性をクリックし、[Edit] を選択します。この属性のString Attribute Editorウ ィンドウで、値0000002を入力し、図に示すようにApplyとOKをクリックします。Windows 2012 サーバで匿名バインド機能が有効になりました。

◆ 注:最後(7番目)の文字は、LDAPサービスへのバインド方法を制御するものです。 0(ゼロ)または7文字目がない場合は、匿名LDAP操作が無効になります。7番目の文 字を2に設定すると、匿名バインド機能が有効になります。

 Show mandatory attributes Show optional attributes Show only attributes 	butes tes that have <u>v</u> alues			
Attribute canonicalName cr createTimeStamp description directReports displayName distinguishedName distinguishedName distinguishedName dSASignature dSCorePropagationD dSHeuristics extensionName flags	Synkax Unicode String Unicode String UTC Coded Ti Unicode String Distinguished Unicode String Distinguished Octet String UTC Coded Ti Unicode String Unicode String Integer	Value lab.wireless/Configuration Directory Service 9/4/2008 12:38:09 PM <not <not="" cn="Directory" s<="" seb="" service,cn="" th=""><th>String Attribute Editor Ambute: dSHeuristics Value: COUDD2 Clear</th><th>OK Cancel</th></not>	String Attribute Editor Ambute: dSHeuristics Value: COUDD2 Clear	OK Cancel

ユーザへのANONYMOUS LOGONアクセス権の付与

次に、ANONYMOUS LOGON アクセス権限をユーザ User1 に付与します。これを行うには、次の手順を実行します。

- 1. [Active Directory Users and Computers] を開きます。
- 2. View Advanced Featuresにチェックマークが付いていることを確認します。
- 3. ユーザ User1 にナビゲートして右クリックします。コンテキスト メニューから [Properties] を選択します。このユーザは、名User1で識別されます。



4. 図に示すように、Securityタブをクリックします。

		User1	Propert	ies		?)	
Published Ce	rtificates	Member Of	Passwor	d Replica	tion I	Dial-in Objec	
Remote [rvices Profile	C	OM+	At	tribute Editor		
General	Address	Account	Profile	Teleph	ones	Organization	
Security	En	vironment	Sess	sions	Re	mote control	
Group or us	er names:						
Administrators (CISCOSYSTEMS\Administrators) Administrators (CISCOSYSTEMS\Administrators) Account Operators (CISCOSYSTEMS\Account Operators) Pre-Windows 2000 Compatible Access (CISCOSYSTEMS\Pre-Wi Windows Authorization Access Group (CISCOSYSTEMS\Window Terminal Server License Servers (CISCOSYSTEMS\Terminal Serv							
Permissions	for ANON	YMOUS LOGO	DN	Add A	llow	Remove Deny	
Full contr	ol						
Kead Write							
Create al	child obie	cts		L			
Delete al	l child obje	cts		Г			
Allowed t	o authentio	ate					
For special permissions or advanced settings, click Advanced.							
Leam abou	t access co	ontrol and pem	nissions				
	0	< C	ancel	Ap	ply	Help	

5. 表示されるウィンドウで [Add] をクリックします。

6. 図に示すように、[Enter the object names to select] ボックスにANONYMOUS LOGONと入

カし、ダイアログを確認します。

Select Users, Computers, Service Accounts, or Grou	ıps	?	x
Select this object type:			
Users, Groups, or Built-in security principals	Obje	ect Typ	pes
From this location:			
CISCOSYSTEMS.local	Lo	cation	IS
Enter the object names to select (examples):			
ANONYMOUS LOGON	Che	ck Na	ames
Advanced OK		Can	cel

7. ACL で ANONYMOUS LOGON がユーザの一部のプロパティ セットにアクセスできること がわかります。[OK] をクリックします。図に示すように、ANONYMOUS LOGONアクセス 権限がこのユーザに付与されます。

		User1	Properti	ies		? X
Published Ce	rtificates	Member Of	Password	d Replica	tion I	Dial-in Object
Remote D	esktop Se	rvices Profile	C	DM+	At	tribute Editor
General	Address	Account	Profile	Teleph	ones	Organization
Security	En	vironment	Sess	ions	Re	mote control
Group or us	er names:					
& ANON	YMOUS LO	DGON				~
Reveryo	ne					_
SELF						_
	iticated Us -M	ers				
Bononii Shori	n Admins ((CISCOSYSTE	MS\Domai	n Admins)	
🦉 🧟 Cert Pu	ublishers (C	ISCOSYSTEM	IS\Cert Pu	ublishers)	·	~
-						<u> </u>
				Add		Remove
Permissions	for ANON	YMOUS LOGO	N	А	low	Deny
Full contr	ol					
Read				٩	/	
Write						
Create all	child obje	cts				
Delete all	child obje	cts		L		
Allowed t	o authentic	ate				님 ㅋ
For special	permissions	or advanced	settings, c	lick		Advanced
Advanced.						
Leam about	access co	ontrol and pem	nissions			
	Oł	< C	ancel	Ар	ply	Help

OU での List Contents 権限の付与

次に、ユーザが含まれている OU で ANONYMOUS LOGON に List Contents 権限を付与します。 この例では、User1はOU LDAP-USERSにあります。これを行うには、次の手順を実行します。

1. 次の図に示すように、Active Directory Users and ComputersでOU LDAP-USERSを右クリ

ックし、Propertiesを選択します。

Re detail Veer Help Anthe Charged Kentral (WMH A028/MBB 65 C6C003TBL65.Kg) Be detailed in the second seco	8	Active Directory Users and Computers	- 0 X
Image: Control of the second secon	File Action View Help		
Ante Type Sector Sector Sector Sector Depende Cetor Deter Cetor	♦ ♦ 2 10 ¥ 1 × 10 0 0 2 11 3 2 2 7 2	8	
	Active Directory Users and Computers (WN-ADV2BU68LR9.CISCOSYSTEMS.M) Saved Queries) CISCOSYSTEMS.Iceal) Computers) Computers) Computers) Computers) Computers) Delegate Control) Delegate Control Properties Help	Name Type Description Buse1 User	tivate Windows.
Opens the properties dialog has for the surrent selection	Opens the properties dialog how for the current selection		

- 2. [Security] をクリックします。
- 3. [Add] をクリックします。開くダイアログで、ANONYMOUS LOGONと入力し、図に示すようにダイアログを確認します。

Select Users, Computers, Service Accounts, or Grou	ps	?	x
Select this object type:			
Users, Groups, or Built-in security principals	Obje	ect Typ	pes
From this location:			
CISCOSYSTEMS.local	Lo	cation	IS
Enter the object names to select (<u>examples</u>):			
ANONYMOUS LOGON	Che	eck Na	ames
Advanced OK		Can	cel

認証されたバインド

LDAPサーバへのローカル認証用にユーザを設定するには、この項の手順を実行します。

- 1. Windows PowerShellを開き、次のように入力します servermanager.exeファイル
- 2. Server Managerウィンドウで、AD DSをクリックします。サーバ名を右クリックして選択 します [Active Directory Users and Computers] の順に選択します。
- 3. [Users] を右クリックします。表示されたコンテキストメニューからNew > Userの順に移動 し、新しいユーザを作成します。

3	Active Directory Users and Computers	_ 🗆 X
File Action View Help		
🗢 🔿 📶 🔏 🖬 🔀 🖬 🖬	🗖 🔁 🐮 🗑 🝸 🚨 🍇	
 Active Directory Users and Computers [WIN-A0" Saved Queries CISCOSYSTEMS.local Builtin Computers Computers CorregnSecurityPrincipals LDAP-USERS LostAndFound Managed Service Accounts Program Data System User Inth Delegate Control TPM Find 	Name Type Description Allowed RO Security Group Members in this group c Allowed RO Security Group Members of this group Denied ROD Security Group Members of this group c Denied ROD Security Group Members of this group c Denied ROD Security Group DNS Administrators Gro RAS and IAS Security Group Servers in this group can NinRMRem Security Group Members of this group t Donabled D Security Group Members of this group t Donabled P Security Group DNS clients who are per Domain Ad Security Group Designated administrato Domain Co Security Group All domain controllers i Domain Co Security Group All domain guests Domain Users Security Group All domain users Members in this group c Members in this group c	E
All Tasks View Refresh Export List Properties Help < III	Contact p Group p InetOrgPerson p Instagging-PSPs p MSMQ Queue Alias p Printer p Shared Folder p Members of this group P	~
Create a new object		

- 4. 次の例に示すように、ユーザ設定ページで必須フィールドに情報を入力します。この例では 、User logon nameフィールドにWLC-adminが設定されています。これは、LDAPサーバへ のローカル認証に使用されるユーザ名です。[Next] をクリックします。
- 5. パスワードを入力し、確認のためのパスワードを入力します。[Password never expires] オ プションを選択して [Next] をクリックします。
- 6. [Finish] をクリックします。

新しいユーザWLC-adminがUsersコンテナの下に作成されます。以下は、ユーザ クレデン シャルです。

- ユーザ名:WLC-admin
- パスワード: Admin123

WLC-adminへの管理者権限の付与

ローカル認証ユーザが作成されたので、管理者権限を付与する必要があります。これを行うには 、次の手順を実行します。

- 1. [Active Directory Users and Computers] を開きます。
- 2. View Advanced Featuresにチェックマークが付いていることを確認します。
- 3. ユーザWLC-adminに移動して右クリックします。次の図に示すように、コンテキストメニ ューからPropertiesを選択します。このユーザは、名WLC-adminで識別されます。

8	Active D	irectory Users and Compute	ers	- 🗆 X
File Action View Help Image: Active Directory Users and Computers [WIN-AD] Image: Active Directory Users and Computers [WIN-AD]	Di 🐮 🐮 🐨 🔽 🞉	Description		
 Saved Queries 	Domain Gue Security Grou Domain Users Security Grou Group Polic Security Grou RA_AllowAd Security Grou RA_AllowCo Security Grou RA_AllowHo Security Grou RA_AllowHo Security Grou RA_AllowHo Security Grou RA_AllowHo Security Grou	p All domain guests p All domain users p Members in this group c p p p Copy		
 Managed service Accounts Porgram Data System Users NTDS Quotas TPM Devices 	RA_AllowNe Security Grouting Grouti	Add to a group Name Mappings Disable Account Reset Password Move Open Home Page Send Mail All Tasks ► Cut Delete Rename Froperties Help		Ξ
Opens the properties dialog box for the current selection	ion.			~

4. 図に示すように、[Member Of] タブをクリックします。

WLC-admin Properties

)

?

Security	Er	vironment	Sessi	ons	Re	mote co	ontrol
Remote	Desktop Se	ervices Profile	, cc)M+	At	tribute E	Editor
General	Address	Account	Profile	Teleph	iones	Orga	nization
Published C	ertificates	Member Of	Password	l Replica	tion	Dial-in	Object
Member of	- -		-				
Name		Active Directo	ry Domain	Services	s Folder	-	
Domain U	Users	CISCOSYSTE	MS.local/U	Users			
Add	. F	Remove					
Primary gro	oup: D	omain Users					
Set Prin	nary Group	There is no you have I application	o need to c Macintosh Is.	hange P	rimary (POSI)	group ur (-compli	nless ant
	0	к	ancel	Ар	ply		Help

5. [Add] をクリックします。開くダイアログで、Administratorsと入力し、次の図に示すように OKをクリックします。

...

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

LDP を使用したユーザ属性の確認

この GUI ツールは、ユーザがすべての LDAP 互換ディレクトリ(Active Directory など)に対し て接続、バインド、検索、変更、追加、削除などの操作を実行できるようにする LDAP クライア ントです。LDP では、Active Directory に格納されているオブジェクトとそのメタデータ(セキュ リティ記述子やレプリケーション メタデータなど)を表示できます。

LDP GUI ツールは、製品 CD から Windows Server 2003 Support Tools をインストールするとイ ンストールされます。ここでは、LDP ユーティリティを使用してユーザ User1 に関連付けられて いる特定の属性を確認する方法について説明します。一部の属性は、WLC で LDAP サーバ設定 パラメータ(ユーザ属性タイプ、ユーザ オブジェクトタイプなど)の値を入力するときに使用さ れます。

- 1. Windows 2012サーバ(同じLDAPサーバ上でも)で、Windows PowerShellを開き、LDPと 入力してLDPブラウザにアクセスしますを参照。
- 2. 図に示すように、LDPメインウィンドウでConnection > Connectの順に選択し、LDAPサー バのIPアドレスを入力してLDAPサーバに接続します。

22				Ldp	_ 0	
Connection Browse	View (ptions	Utilities	Help		
Connect]				
Bind	Ctrl+B					
Disconnect						
New	Ctrl+N					
Save						
Save As		-				
Exit						

3. LDAPサーバに接続したら、次の図に示すように、メインメニューからViewを選択し、 Treeをクリックします。

Idap://WIN-A0V2BU68LR9.CISCOSYSTEMS.local/DC=CISCOSYSTEMS,DC=local	Ŀ	. 🗖		x
Connection Browse View Options Utilities Heip Connection Browse View Options Utilities Heip Connection Browse View Options Utilities Heip Connection Browse View Options Utilities Heip Connection Browse View Options Utilities Heip Connection Browse View Options Utilities GenutlammicContest: 0::0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:	DC=local; IS,DC=local; IS,DC=local; V61_R2); 1840.113556 IS,01.41339 = 9 = (VLVRE(ISS6.14.802 0.14.11374 = 19.11974 = RCYCLED = (DRSYNC 2.2840.11355 izze; Conn; MaxV/	(QUEST = (QUEST); 56.1.4: alRang	28 = []); ;; ;2211 ge;	
Ready				

4. 表示される [Tree View] ウィンドウで、ユーザの BaseDN を入力します。この例では、 User1はドメインCISCOSYSTEMS.localのOU「LDAP-USERS」に含まれています。次の図 に示すように、OKをクリックします。

	Idap://WIN-A0V2BU68LR9.CISCOSYSTEMS.local/DC=CISCOSYSTEMS,DC=local	-		X	
Connection Browse View Options Utilities	Help				
	defaultNamingContext: DC-CISCOSYSTEMS,DC-local; dmainfortollerFunctionalty: 5; domainFunctionalty: 5; domainFunctionalty: 5; highestCommittedUSN: 16585; isGlobalCatalogReady: TRUE; isSynchronized: TRUE; isSynchroized: TRUE; isSynchisSynchronized: TRUE; isSynchronized: TRUE; is	cal; 1 = (); 1556.1.4 302 = (14 = (20); 2556.1 44 = (20); 200 = (20); 20; 200 = (20); 200 = (20); 200; 200; 200; 200; 200; 200; 200;	4.528 - (ST); (4.221 ange;	=(=	
Ready		-	_	_	4

5. LDPブラウザの左側には、指定したBaseDN(OU=LDAP-USERS, dc=CISCOSYSTEMS, dc=local)の下にツリー全体が表示されます。ツリーを展開してユーザ User1 を見つけます 。このユーザは、ユーザの名前を表す CN 値で識別されます。この例では CN=User1 です 。CN=User1 をダブルクリックします。図に示すように、LDPブラウザの右側のペインに、 User1に関連付けられているすべての属性が表示されます。

8	Idap://WIN-A0V2BU68LR9.CISCOSYSTEMS.local/DC=CISCOSYSTEMS,DC=local	_ _ ×
Connection Browse View Options Utilities	Help	
E OULDAP-USERS.DC=CISCOSYSTEMS,DC=CISCOSYST CULDAP-USERS.DC=CISCOSYSTEMS,DC=CISCOSYST No children	<pre>Trep Expanding base 'CN=User1,OU=LDAP-USERS,DC=CISCOSYSTEMS,DC=local Getting 1 entries: Dh: CN=User1,OU=LDAP-USERS,DC=CISCOSYSTEMS,DC=local accountExprises: 9223372038654775807 (never); badPwsdCount: 0; co: User1; codePage: 0; countryCode: 0; displayMame: User1; distinguishedName: CN=User1.OU=LDAP-USERS,DC=CISCOSYSTEMS,DC=local; disCorePropagationData (3): 12/24/2015 1:34:53 PM E. Europe Standard Time; 12/24/2015 1:20:39 PM E. Europe Standard Time; 0x0 = (), 0x0 = (); givenName: User1; instanceType: 0x4 = (WRITE); lastLogort 0 (never); lastLogort 0 (never); lastLogort 0 (never); lastLogort 0 (never); lastLogort 0 (never); lastLogort 0 (never); logorCount: 0; name: User1; objectClategory: CN=Person, CN=Schema,CN=Configuration,DC=CISCOSYSTEMS,DC=local; objectClategory: CN=Person, CN=Schema,CN=CONFIGURATION; primaryGroupD: 513 = (GROUP,RD_USERS); pwdLastSet: 12242/2015 1:19:16 PM E. Europe Standard Time; sAMAccountTyme: 805306386 4: (NORMAL_USER_ACCOUNT); userAncountControl to Cu200 = 4 (NORMAL_ACCOUNT); userAncountControl to Cu200 = 4 (NORMAL_A</pre>	R R R R R R R R R R R R R R R R R R R
	whenCreated: 12/24/2015 1:19:15 PM E. Europe Standard Time;	
Paadu 2	1	Y
neauy		

6. LDAP サーバに WLC を設定するときには、[User Attribute] フィールドに、ユーザ名を含む ユーザ レコードの属性の名前を入力します。この LDP の出力から、sAMAccountName が ユーザ名「User1」を含む属性の 1 つであることがわかります。そこで、WLC の [User Attribute] フィールドに対応する sAMAccountName 属性を入力します。

7. LDAP サーバに WLC を設定するときには、[User Object Type] フィールドに、レコードを

ユーザとして識別する LDAP objectType 属性の値を入力します。多くの場合、ユーザ レコ ードには objectType 属性の値が複数あり、そのうちのいくつかはユーザに固有であり、ま た、いくつかは他のオブジェクト タイプと共有されています。LDP 出力の CN=Person は レコードをユーザとして識別する値の 1 つです。そこで、WLC の User Object Type 属性と して Person を指定します。

次に LDAP サーバの WLC を設定します。

LDAP サーバの WLC の設定

ここまでで LDAP サーバが設定されました。次に LDAP サーバの詳細を使用して WLC を設定し ます。WLC の GUI から次の手順を実行します。

◆ 注:このドキュメントでは、WLCが基本動作用に設定され、LAPがWLCに登録されている ことを前提としています。WLC で LAP との基本動作を初めて設定する場合は、「<u>Wireless</u> LAN Controller (WLC) への Lightweight AP (LAP)の登録」を参照してください。

1. WLC の [Security] ページの左側にあるタスク ペインで [AAA] > [LDAP] を選択し、LDAP サ ーバ設定ページに進みます。

ahaha				-	-		-				Sage Go	nfiguration E	ing Logout <u>R</u> efresh
CISCO	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACI	ĸ			🔒 <u>H</u> ome
Security • AAA General • RADIUS	LDAP Se	rvers											New
	Server Index	Server	Address(Ipv	/lpv6)		Port		Server St	tate	Secure Mode(via TLS)	Bind		
Authentication	1	172.16	.16.200			389		Enabled		Disabled	Authenticated		
Fallback DNS Downloaded AVP TACACS+ Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	III												
Local EAP													
Advanced EAP													
Priority Order													
▶ Certificate													

LDAP サーバを追加するには、[New] をクリックします。[LDAP Servers > New] ページが表示されます。

- 2. [LDAP Servers Edit] ページで LDAP サーバの詳細(LDAP サーバの IP アドレス、ポート番号、サーバ有効化ステータスなど)を指定します。
 - [Server Index (Priority)] ドロップダウン ボックスから番号を選択し、その他の設定済 みの LDAP サーバト関連したこのサーバの優先順位を指定します。サーバは最大 17 個まで設定できます。コントローラが最初のサーバに接続できない場合、リスト内の 2 番目のサーバへの接続を試行する、というようになります。
 - [Server IP Address] フィールドに LDAP サーバの IP アドレスを入力します。
 - [Port Number] フィールドに LDAP サーバの TCP ポート番号を入力します。有効な範囲は1~65535 で、デフォルト値は389 です。

- ・簡易バインドでは、バインドユーザ名にAuthenticatedを使用しました。これは、 LDAPサーバとそのパスワードへのアクセスに使用されるWLC管理ユーザの場所です
- [User Base DN] フィールドに、すべてのユーザのリストを含む LDAP サーバ内のサブ ツリーの識別名(DN)を入力します。たとえば、ou=organizational unit, .ou=next organizational unit および o=corporation.com などです。ユーザを含むツリーがベース DN である場合、o=corporation.com または dc=corporation、dc=com と入力します。

この例ではユーザは組織単位(OU)LDAP-USERS に含まれています。この組織単位 は lab.wireless ドメインの一部として作成されています。

ユーザ ベース DN は、ユーザ情報(EAP-FAST 認証方式に基づくユーザ クレデンシャル)が保存されている場所のフル パスを指している必要があります。この例では、 ユーザはベースDN OU=LDAP-USERS, DC=CISCOSYSTEMS, DC=localの下にありま す。

• [User Attribute] フィールドに、ユーザ名を含むユーザ レコード内の属性の名前を入力 します。

[User Object Type] フィールドに、対象のレコードをユーザとして特定する LDAP objectType 属性の値を入力します。多くの場合、ユーザ レコードには objectType 属 性の値が複数あり、そのうちのいくつかはユーザに固有であり、また、いくつかは他 のオブジェクト タイプと共有されています。

これらの2つのフィールドの値は、Windows 2012サポートツールの一部として提供さ れているLDAPブラウザユーティリティを使用して、ディレクトリサーバから取得で きます。この Microsoft LDAP ブラウザ ツールは LDP と呼ばれます。このツールを使 用して、特定ユーザの [User Base DN]、[User Attribute]、および [User Object Type] フィールドの値を確認できます。LDP を使用したユーザ固有属性の確認方法の詳細に ついては、このドキュメントの「LDP を使用したユーザ属性の確認」を参照してくだ さい。

- [Server Timeout] フィールドに再送信の間隔(秒数)を入力します。有効な範囲は 2
 ~ 30 秒であり、デフォルト値は 2 秒です。
- [Enable Server Status] チェック ボックスをオンにしてこの LDAP サーバを有効にす るか、チェックマークをオフにして無効にします。デフォルト値は無効です。
- [Apply] をクリックして、変更を確定します。上記の情報を使用した設定の例を次に示します。

cisco	MONITOR WLANS CONTROL	LER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK	Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efrest ntermation <u>Ping Logout Refrest</u>
Security	LDAP Servers > Edit		< Back Apply
AAA General Caneral Caneral Authentication Accounting Fallback DNS Downloaded AVP TACACS+ LOAP LOAI Net Users MAC Filtering Disabled Clients User Login Policies AP Policies AP Policies Aevanced EAP Advanced EAP Prointly Order Certificate	Server Index Server Address(Ipv4/Ipv6) 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	1 172.16.16.200 389 Authenticated ▼ CN=WLC-ADMIN_CN=Users,DC=CISCOSYSTEMS,C *** *** CN=Users,DC=CISCOSYSTEMS,DC=LOCAL SAMAccountName Person Disabled ▼ 2 seconds Enabled ▼	

3. これで LDAP サーバに関する詳細が WLC に設定されました。次に、WLAN を Web 認証用 に設定します。

Web 認証用の WLAN の設定

最初の手順では、ユーザの WLAN を作成します。次のステップを実行します。

1. WLAN を作成するために、コントローラの GUI で [WLANs] をクリックします。

[WLANs] ウィンドウが表示されます。このウィンドウには、コントローラに設定されてい る WLAN の一覧が表示されます。

2. 新しい WLAN を設定するために [New] をクリックします。

この例では、WLAN の名前を Web-Auth としています。

cisco		WLANS		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	WLANs >	New							
 WLANs WLANs Advanced 	Type Profile Na SSID ID	me	WLAN LDAP- LDAP- 11	▼ TEST TEST					

3. [APPLY] をクリックします。

4. [WLAN] > [Edit] ウィンドウで、WLAN 固有のパラメータを定義します。

cisco	MONITOR WLANS CO	TROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDB	Save Configuration Bing Logout Befresh ACK A Home
WLANs	WLANs > Edit 'LDAP-1	EST	< Back Apply
WLANS WLANS	General Security	QoS Policy-Mapping Advanced	
▶ Advanced	Profile Name	LDAP-TEST	
	Туре	WLAN	
	SSID	LDAP-TEST	
	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)	management 👻	
	Multicast Vlan Feature	Enabled	
	Broadcast SSID	C Enabled	
	NAS-ID	none	

- [Status] チェックボックスをオンにしてこの WLAN を有効にします。
- WLAN に対し、[Interface Name] フィールドから適切なインターフェイスを選択します。

この例では、WLAN Web-Auth に接続する管理インターフェイスを割り当てています。

5. [Security] タブをクリックします。[Layer 3 Security] フィールドで、[Web Policy] チェック ボックスをオンにして、[Authentication] オプションを選択します。

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK	Sa <u>v</u> e Configuration Eing Logout <u>R</u> efresh A <u>H</u> ome
CISCO WLANS VLANS VLANS Advanced	MONITOR WLANS CONTROLLER WRELESS SECURITY MAAAGEMENT COMMANDS HELP FEEDBACK WLANS > Edit 'LDAP-TEST' General Security QoS Policy-Mapping Advanced Layer 2 Layer 3 AAA Servers Layer 3 AAA Servers Layer 3 Security 4 Web Policy Image: Conditional Web Redirect Ocnditional Web Redirect Image: On MAC Filter failure#2 Preauthentication ACL IPv4 None • IPv6 None • WebAuth FlexAcl None • Sleeping Client Enable Over-ride Global Configit# Enable Enable	E Back Apply

Web 認証を使用してワイヤレス クライアントを認証するため、このオプションを選択しま す。[Override Global Config] チェックボックスをオンにして、各 WLAN の Web 認証設定を 有効にします。[Web Auth type] ドロップダウン メニューから適切な Web 認証の種類を選 択します。この例では、内部 Web 認証を使用します。

▶ 注:Web認証は802.1x認証ではサポートされていません。これは、Web 認証を使用す る場合、レイヤ 2 セキュリティとして、802.1x または 802.1x を使用する WPA/WPA2 を選択できないことを意味します。その他のすべてのレイヤ 2 セキュリ ティ パラメータを使用した Web 認証がサポートされます。 [AAA Servers] タブを選択します。LDAP サーバのプルダウン メニューから設定した LDAP サーバを選択します。ローカル データベースまたは RADIUS サーバを使用している場合は 、[Authentication priority order for web-auth user] フィールドで認証のプライオリティを設 定できます。

cisco	MONITOR WUANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK	Saye Configuration Ping Logout Befresh n Home
WLANs	WLANs > Edit 'LDAP-TEST'	< Back Apply
WLANs WLANs	General Security QoS Policy-Mapping Advanced	
Advanced	Layer 2 Layer 3 AAA Servers	
	Interim Update	^
	Server 1 IP:172.16.16.200, Port:389 Server 2 None	=
	Server 3 None	
	Local EAP Authentication	
	Local EAP Authentication	
	Authentication priority order for web-auth user	E
	Not Used Order Used For Authentication	
	LOCAL A RADIUS V C Down	
	ш	•

7. [APPLY] をクリックします。

Signature State St

確認

ここでは、設定が正常に機能しているかどうかを確認します。

このセットアップを検証するために、ワイヤレス クライアントを接続し、設定が想定どおりに動 作するかどうかを確認します。

ワイヤレス クライアントが起動したら、Web ブラウザに URL(www.yahoo.com など)を入力し ます。ユーザが認証されていないため、WLC はそのユーザを内部 Web ログイン URL にリダイ レクトします。

ユーザ クレデンシャルの入力が求められます。ユーザがユーザ名とパスワードを送信すると、ロ グイン ページ側がユーザ クレデンシャルの入力を受け取り、WLC Web サーバの action_URL(http://1.1.1.1/login.html など)に入力を送信するとともに要求を戻します。これが入 カパラメータとしてカスタマーのリダイレクト URL に提供されます。ここで、1.1.1.1 は、スイ ッチの仮想インターフェイス アドレスです。

WLC は LDAP ユーザ データベースに照合してユーザを認証します。認証が成功すると、WLC Webサーバは、設定されたリダイレクトURLまたはクライアントが開始されたURLにユーザを転 送します。次に例を示します <u>www.yahoo.com にアクセスしてください。</u>

	More information	
	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 send server.	to the
	The security certificate presented by this website was not issued by a trusted certificate authority.	
8	There is a problem with this website's security certificate.	

O Image: Contract of the second second

Welcome to the Cisco wireless network

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

Oper Harpe	User1	
Password		
	Submit	



トラブルシュート

このセクションでは、設定のトラブルシューティングに役立つ情報を紹介します。

設定のトラブルシューティングを行うために、次のコマンドを使用できます。

- debug mac addr <client-MAC-address xx:xx:xx:xx:xx:xx:xx
- debug aaa all enable
- · debug pem state enable
- · debug pem events enable
- · debug dhcp message enable
- · debug dhcp packet enable

次に、debug mac addr cc:fa:00:f7:32:35コマンドの出力例を示します

debug aaa ldap enable

(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 *apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Association received from mobile on BSSID 00:2 *apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Global 200 Clients are allowed to AP radio *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 *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying Interface policy on Mobile, role Loca *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 A *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Changing IPv6 A *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 apfApplyWlanPolicy: Apply WLAN Policy over PMI *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 In processSsidIE:6246 setting Central switched *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 In processSsidIE:6249 apVapId = 1 and Split Ac *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying site-specific Local Bridging override *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying Local Bridging Interface Policy for s *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 *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 *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 suppRates statusCode is 0 and gotSuppRatesEle *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 AID 2 in Assoc Reg from flex AP 00:23:eb:e5:04 *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 *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 pemApfAddMobileStation2: APF_MS_PEM_WAIT_L2_AU *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 AUTHCH *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 AUTHCHECK (2) Change state to L2 *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 mobil *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 L2AUTHCOMPLETE (4) Change state

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) pemApfAddMobile *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Adding Fast Pat type = Airespace AP Client - ACL passthru 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 *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Successfully pl *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) pemApfAddMobile *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Replacing Fast 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 *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Successfully pl *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2 (apf_policy.c:359) Changing sta *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2:session timeout forstation cc:f *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Scheduling deletion of Mobile Station: (calle *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Func: apfPemAddUser2, Ms Timeout = 1800, Sessi *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Sending assoc-resp with status 0 station:cc:fa *apfMsConnTask_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 Sending Assoc Response to station on BSSID 00: *apfMsConnTask_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 apfProcessAssocReg (apf_80211.c:10187) Changin *pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 2, dtlFla *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, dtlFla *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,vla *DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype 0ff:ff:ff:ff: *DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block settin 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 mscbVapLoc *DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25 (local a *DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block settin 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 settin 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 mscbVapLoc *DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25 (local a *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 xid: 0x62743488 (1651782792), secs: 0, *DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP *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 settin 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 *DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP sending REPLY to STA (len 418, port 1, vl *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 *DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP xid: 0x62743488 (1651782792), secs: 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 server id: 1.1.1.1 rcvd server id: 172 *DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP *DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP received op BOOTREQUEST (1) (len 334,vla *DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype Off:ff:ff:ff: *DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block settin 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 mscbVapLoc *DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25 (local a *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 *DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP xid: 0x62743488 (1651782792), secs: 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 i *DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block settin 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 *DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP setting server from ACK (mscb=0x40e64b88 *DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP sending REPLY to STA (len 418, port 1, vl *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 *DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP xid: 0x62743488 (1651782792), secs: 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 *ewmwebWebauth1: Dec 24 03:46:01.222: cc:fa:00:f7:32:35 Username entry (User1) created for mobile, leng *ewmwebWebauth1: Dec 24 03:46:01.222: cc:fa:00:f7:32:35 Username entry (User1) created in mscb for mobi *aaaQueueReader: Dec 24 03:46:01.222: AuthenticationRequest: 0x2b6bdc3c *aaaQueueReader: Dec 24 03:46:01.222: Callback.....0x12088c50 *aaaQueueReader: Dec 24 03:46:01.222: protocolType.....0x0000002 *aaaQueueReader: Dec 24 03:46:01.222: proxyState.....CC:FA:00:F7:32:35-*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 (r

*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, *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=" *LDAP DB Task 1: Dec 24 03:46:01.226: Attempting user bind with username CN=User1,CN=Users,DC=CISCOSYST *LDAP DB Task 1: Dec 24 03:46:01.228: LDAP ATTR> dn = CN=User1,CN=Users,DC=CISCOSYSTEMS,DC=local (size *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 *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 *ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 Stopping deletion of Mobile Station: (callerId: *ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 Setting Session Timeout to 1800 sec - starting *ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Reached PLUMBFASTPATH: f *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... *ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule (contd... *ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule (contd... *ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule (contd... *ewmwebWebauth1: Dec 24 03:46:01.229: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Successfully plumbed mob *pemReceiveTask: Dec 24 03:46:01.229: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 1, dtlFla

(Cisco_Controller) >show client detail cc:fa:00:f7:32:35	
Client MAC Addressc:fa:00:f7:32:3	5
Client UsernameUser1	
AP MAC Address00:23:eb:e5:04:1	0
AP Name AP1142-1	
AP radio slot Id 1	
Client State Associated	
Client User GroupUser1	
Client NAC OOB State	
Wireless LAN Id 1	
Wireless LAN Network Name (SSID) LDAP-TEST	
Wireless LAN Profile Name	
Hotspot (802.11u) Not Supported	
BSSID00:23:eb:e5:04:1	.f
Connected For	
Channel	
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 (q)uit current module or <ctrl-z> to ab</ctrl-z>	ort
Session Timeout	1800
Client CCX version	No CCX support
QoS Level	Silver
Avg data Rate	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
Security Policy Completed	Yes
Policy Manager State	RUN
Audit Session ID	ac1010190000005567b69f8
AAA Role Type	none
Local Policy Applied	none
IPv4 ACL Name	none
More or (g)uit current module or <ctrl-z> to abo</ctrl-z>	ort
FlexConnect ACL Applied Status	Unavailable
IPv4 ACL Applied Status	Unavailable
IPv6 ACL Name	none
IPv6 ACL Applied Status	Unavailable
Layer2 ACL Name	none
Laver2 ACL Applied Status	Unavailable
Client Type	SimpleIP
mDNS Status	Enabled
mDNS Profile Name	default-mdns-profile
No. of mDNS Services Advertised	0
Policy Type	N/A
Encryption Cipher	None
Protected Management Frame	No
Management Frame Protection	No
	Unknown
FlexConnect Data Switching	Central
FlexConnect Dhcp Status	Central
FlexConnect Vlan Based Central Switching	No
FlexConnect Authentication	Central
FlexConnect Central Association	No
Interface	management
VI AN	16
Quarantine VI AN	0
	0
More or (a)uit current module or <ctrl-z> to abo</ctrl-z>	ort
Arress VI AN	16
Local Bridging VLAN	16
Client Canabilities.	10
CE Polloble	Not implemented
CE Poll Poquest	Not implemented
Chart Draamble	Not implemented
	Not implemented
FDUL	Not impremented

Channel Agility	Not implemented
East RSS Transition	Not implemented
11v RSS Transition	Not implemented
Client Wifi Direct Capabilities:	Not impremented
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 (a)uit current module or <ctrl-z> to abo</ctrl-z>	ort
Number of Rytes Recy (last 90s)	16853
Number of Packets Received	146
Number of Packets Sent	92
Number of Interim-Undate Sent	0
Number of FAP Id Request Msg Timeouts	0
Number of EAP Id Request Msg Filleouts	0
Number of EAP Request Msg Tarrates	0
Number of EAP Request Msg Finicouts	0
Number of FAP 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 abo</ctrl-z>	ort
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	U
Number of Realtime Ix Bytes Dropped	U
Nearby AP Statistics:	
AT1142 - 1(SIOT U)	27 dBm
antennau: 25 secs ago	- 57 UBM
antennat: 25 Secs ago	-37 UBM
$AT \pm \pm \pm 2 \pm 1 \pm 1$	

antenna0: 25 secs ago..... -44 dBm antenna1: 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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。