# ACS 5.2およびWLCを使用したPEAPおよび EAP-FASTの設定

内容

はじめに <u>前提条件</u> 要件 使用するコンポーネント 表記法 設定 ネットワーク図 前提 設定手順 RADIUS サーバの設定 ネットワーク リソースの設定 ユーザの設定 ポリシー要素の定義 アクセス ポリシーの適用 WLC の設定 WLC での認証サーバの詳細設定 ダイナミック インターフェイス (VLAN)の設定 WLAN (SSID)の設定 無線クライアント ユーティリティの設定 PEAP-MSCHAPv2 (user1) EAP-FAST (user2) 確認 <u>user1(PEAP-MSCHAPv2)の検証</u> <u>user2(EAP-FAS</u>T)の検証 トラブルシュート トラブルシューティングのためのコマンド <u>関連</u>情報

## はじめに

このドキュメントでは、Access Control Server(ACS)5.2 などの外部 RADIUS サーバを使用し て拡張認証プロトコル(EAP)認証のためのワイヤレス LAN コントローラ(WLC)を設定する 方法について説明します。

## 前提条件

### 要件

この設定を行う前に、以下の要件を満たしていることを確認してください。

- WLC および Lightweight アクセス ポイント(LAP)に関する基本的な知識があること
- AAA サーバに関する実務的な知識があること
- ワイヤレス ネットワークとワイヤレスのセキュリティ問題に関する全般的な知識があること

### 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 7.0.220.0 が稼働している Cisco 5508 WLC
- ・ Cisco 3502 シリーズ LAP
- ・ Intel 6300-N ドライバ バージョン 14.3 対応の Microsoft Windows 7 ネイティブ サプリカン ト
- バージョン 5.2 が稼働している Cisco Secure ACS
- Cisco 3560 シリーズ スイッチ

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。

### 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。

## 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。



この図で使用されているコンポーネントの設定の詳細は、次のとおりです。

- ACS (RADIUS) サーバの IP アドレスは 192.168.150.24 です。
- WLC の管理インターフェイスおよび AP マネージャ インターフェイスのアドレスは 192.168.75.44 です。
- DHCP サーバのアドレスは 192.168.150.25 です。
- VLAN 253 がこの設定を通して使用されます。両方のユーザが同じ SSID "goa" に接続しま す。ただし、user1 は PEAP-MSCHAPv2 を使用して認証するように、user2 は EAP-FAST を使用して認証するように設定されます。
- ・ ユーザは VLAN 253 で割り当てられます。
  - VLAN 253:192.168.153.x/24。ゲートウェイ: 192.168.153.1
  - ◎ VLAN 75:192.168.75.x/24ゲートウェイ:192.168.75.1

### 前提

- ・ スイッチには、レイヤ 3 VLAN がすべて設定されています。
- DHCP サーバには DHCP スコーが割り当てられています。
- ネットワーク内すべてのデバイス間ではレイヤ3接続が確立しています。
- ・ LAP はでに WLC に登録されています。
- 各 VLAN は /24 マスクを使用しています。
- ACS 5.2 には自己署名証明書がインストールされています。

## 設定手順

この設定は、大きく次の3つに分類されます。

- 1. <u>RADIUS サーバの設定</u>
- 2. <u>WLC の設定</u>
- 3. <u>無線クライアント ユーティリティの設定</u>

## RADIUS サーバの設定

RADIUS サーバの設定は次の4つのステップで構成されます。

- 1. <u>ネットワーク リソースの設定</u>
- 2. <u>ユーザの設定</u>
- 3. ポリシー要素の定義
- 4. <u>アクセス ポリシーの適用</u>

ACS 5.x は、ポリシーベースのアクセス コントロール システムです。つまり、ACS 5.x では、 4.x バージョンで使用されていたグループベースのモデルの代わりに、ルールベース ポリシー モ デルが使用されています。

ACS 5.x のルールベース ポリシー モデルを使用すると、以前のグループベースの手法よりも強力 で柔軟なアクセス コントロールを実現できます。

以前のグループベース モデルでは、グループを使用してポリシーを定義していました。これは、 グループに次の 3 つのタイプの情報が結合されていたためです。

 識別情報:この情報は、AD グループまたは LDAP グループでのメンバーシップ、または ACS 内部ユーザの静的割り当てに基づいています。

- その他の制限または条件:時間制限、デバイス制限など。
- 許可: VLAN または Cisco IOS® の特権レベル。

ACS 5.x ポリシー モデルは、次の形式のルールに基づいています。

• If condition then result

たとえば、グループベース モデルに関して記述されている次の情報を使用します。

If identity-condition, restriction-condition then authorization-profile

これにより、ユーザがネットワークにアクセスするための条件だけでなく、特定の条件を満たす 場合に必要な承認レベルに基づいて、柔軟に制限できるようになります。

ネットワーク リソースの設定

ここでは、RADIUS サーバ上の WLC 用に AAA クライアントを設定します。

この手順では、WLC から RADIUS サーバにユーザ クレデンシャルを渡せるように、RADIUS サ ーバで AAA クライアントとして WLC を追加する方法について説明します。

次のステップを実行します。

1. ACS GUI から [Network Resources] > [Network Device Groups] > [Location] に移動し、 [Create] (最下部)をクリックします。

cisco Cisco Secure Ad	CS
► 🚭 My Workspace	Network Resources > Network Device Groups > Location
👻 🕼 Network Resources	Network Device Groups
<ul> <li>Network Device Groups</li> <li>Location</li> </ul>	Filter: • Match if: • Go •
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Image: Name         Description           Image: All Locations         All Locations
Big Users and Identity Stores	
► Sp Policy Elements	
► 🔂 Access Policies	
<ul> <li>Monitoring and Reports</li> </ul>	
🕞 🍓 System Administration	

2. 必要なフィールドを追加して [Submit] をクリックします。

Device Group -	Seneral	
o Name:	LAB	
Description:	LAB Devices	
o Parent:	All Locations	Select
Required field	lds	

次の確認画面が表示されます。

cisco Cisco Secure A	CS
My Workspace     Metwork Resources     Network Device Groups	Network Resources > Network Device Groups > Location           Network Device Groups           Filter:
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	□     Name     ▲     Description       □     ▼ <u>All Locations</u> All Locations
Bers and Identity Stores     Solution Policy Elements	LAB LAB Devices
Access Policies     Monitoring and Reports	
System Administration	

3. [Device Type] > [Create] をクリックします。

cisco Cisco Secure A	CS	
► 🚭 My Workspace	Network Resources > Network Device Groups > Device Type > Create	
	Device Group - General         O Name:       5508         Description:       Wireless LAN Controller         O Parent:       All Device Types         O = Required fields	Select
Users and Identity Stores		
Policy Elements		
Access Policies		
<ul> <li>Monitoring and Reports</li> </ul>		
<ul> <li>System Administration</li> </ul>		

4. [Submit] をクリックします。次の確認画面が表示されます。

cisco	Cisco Secure A	CS		-	-		
→ 😚 M	y Workspace	Netwo	rk R	Resources > N	letwork	Device Groups > Device Type	
- 👘 N	etwork Resources	Net	wo	rk Device Gr	oups		
▼ Netwo Loca	ork Device Groups ation	Filt	er.	[	•	Natch if.	Go 🔻
Netw	ork Devices and AAA Clients	1		Name		Description	
Extern	al RADIUS Servers			All Device	Types	All Device Types	
+ 💕 U	sers and Identity Stores			5508		Wireless LAN Controller	
• 💫 P	olicy Elements						
• 🔂 A	cess Policies						
► 🗊 M	onitoring and Reports						
🕨 🍓 S	stem Administration						

- 5. [Network Resources] > [Network Devices and AAA Clients] に移動します。
- 6. [Create] をクリックして、次のように詳細を入力します。

+ 🔂 My Workspace	Network Resources > Net	work Devices and AAA Clerks > Create			
Lea Network Resources     Network Device Groups     Location     Device Type     Network Devices and AMAChents     Default Network Device     External RADIUS Servers	o Name. WL Description Wr Network Device Gro Location Device Type	C-5508 eless LAN Controller All Locations:LAB All Device Types:5508	Salect		
Busers and Identity Stores     Policy Elements     C. Access Pulicies     Monitoring and Reports	IP Address © Single IP Ad 9 IP: 192 168 75	PAddress C IP Range(s) 75.44		Authentication Options  TACACS+  RADUS  Authentication Options  TACACS+  Casest Cisco  Cisco	
<ul> <li>System Administration</li> </ul>	• - Required fields			CoAlport (1700 Enable KeyWiap Key Encryption Key: Message Authenticator Code Key: Key Input Format C ABCII C HEXADECIMAL	

7. [Submit] をクリックします。次の確認画面が表示されます。

iller.		<ul> <li>Match it.</li> </ul>	-	G0 🔻	
-	Name 🔺	IP / Mask	NDG:Location	NDG:Device Type	Description
	WLC-5508	192.168.75.44/32	All Locations:LAB	All Device Types:5508	Wireless LAN Controller

## ユーザの設定

ここでは、ACS 上のローカル ユーザを作成します。両方のユーザ(user1 と user2)が "Wireless Users" というグループに割り当てられます。

1. [Users and Identity Stores] > [Identity Groups] > [Create] に移動します。

cisco Cisco Secure A	cs
» ⊕ My Workspace	Users and identity Stores > Identity Groups > Create
In Network Resources	
Users and Identity Stores     Identity Groups     Internal Identity Stores     Users     Hosts     External Identity Stores     LDAP     Active Directory     RSA SecurID Token Servers     RADIUS Identity Servers     Certificate Authorities     Certificate Authorities     Certificate Authorities     Certificate Authorities     Certificate Authorities     Certificate Authentication Profile     Identty Store Sequences     SQ: Policy Elements	General       Wireless Users         Description:       Wireless Users authenticating over wireless         Parent       All Groups         Select       Select         Parent       Frequired tields

2. [Submit] をクリックすると、次のようなページが表示されます。

cisco Cisco Secure Ad	CS
▶ 🖓 My Workspace	Users and identity Stores > identity Groups
► 🔚 Network Resources	Identity Groups
Users and Identity Stores	Filter: 💌 Match it: 💌 Go 🔝
<ul> <li>Internal Identity Stores</li> <li>Users</li> </ul>	Name   Description
+ External identity Stores	All Groups Identity Group Root     Wireless Users authenticating over wireless
Active Directory	
RSA SecuriD Token Servers RADIUS Identity Servers Certificate Authorities Certificate Authorities	
Identity Store Sequences	
Policy Elements	

3. ユーザの user1 と user2 を作成して、それらを "Wireless Users" グループに割り当てます。

a. [Users and Identity Stores] > [Identity Groups] > [Users] > [Create] をクリックします。



b. 同様に、user2 を作成します。

	cisco Cisco Secure A	CS
	<ul> <li>My Workspace</li> </ul>	Users and Identity Stores > Internal Identity Stores > Users > Create
	In the sources	
	🗸 🎬 Users and identity Stores	G Name: Juser? Status: Enabled T @
	Identity Groups	Description: FAPFAST user
	<ul> <li>Internal Identity Stores</li> </ul>	Identity Group: All Groups Wireless Lisers     Select
	Hosts External identity Stores Certificate Authorities Certificate Authorities Identity Store Sequences	Password Information Password must • Contain 4 - 32 characters
	Policy Elements	Password:     Acceleration
ł	Access Policies	Password:
	Monitoring and Reports	Change password on next login
	System Administration	User Information There are no additional identity attributes defined for user records - Required fields

次のような画面が表示されます。

	ACS	id Identity Store	s × internal identity Sto	rea > Uaera			
Network Resources	Inter	Internal Users					
<ul> <li>Users and Identity Stores</li> <li>Identity Groups</li> </ul>	Fitter		Match it:	💌 G0 🗢			
Internal Identity Stores	Г	Status	User Name	<ul> <li>Identity Group</li> </ul>	Description		
Users		0	user1	All Groups:Wireless Users	PEAP:mschapv2 users		
External Identity Stores	П	0	user2	All Groups:Wireless Users	EAPFAST user		
Certificate Authorities Certificate Authentication Profile Identity Store Sequences							
Q Policy Elements							

ポリシー要素の定義

[Permit Access] が設定されていることを確認します。

cisco Cisco Secure A	CS
<ul> <li>My Workspace</li> </ul>	Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles
Network Resources	Authorization Profiles
Users and Identity Stores	Filter Match It Go V
👻 🎭 Policy Elements	
Session Conditions     Authorization and Permissions	Permit Access
Network Access     Authorization Profiles	
Device Administration     Named Permission Objects	
Access Policies	
► 🔝 Monitoring and Reports	
🛛 🍇 System Administration	

アクセス ポリシーの適用

ここでは、使用する認証方式とルールの設定方法を選択します。これまでのステップに基づいて ルールを作成します。

次のステップを実行します。

1. Access Policies > Access Services > Default Network Access > Edit: "Default Network Access"の順に選択します。

cisco Cisco Secure A	CS
+ 🛞 My Workspace	Access Policies > Access Services > Default Network Access > Edit "Default Network Access"
B Network Resources	
Users and Identity Stores	General Allowed Protocols
► Sp. Policy Elements	Name: Default Network Access
👻 🌉 Access Policies	Description: Default Network Access Service
Access Services     Service Selection Rules	Service Type : Network Access
O Dafault Device Admin	Policy Structure
🕨 🤮 Default Network Access	Identity
► 2º deleteme	Group Mapping
Monitoring and Reports	Authorization
🕞 🍓 System Administration	

2. ワイヤレス クライアントを認証する EAP 方式を選択します。この例では、PEAP-MSCHAPv2 と EAP-FAST を使用します。

cisco Cisco Secure A	CS
🖌 🧭 My Workspace	Access Palicies > Access Services > Default Network Access > Edit: "Default Network Access"
Network Resources	
B Users and Identity Stores	General Allowed Protocols
► Sp Policy Elements	Process Host Lookup
- 🏨 Access Policies	Authentication Protocols
Access Services     El Service Selection Rules     O Default Device Admin	Allow PAP/ASCII     Allow CHAP
Identity	► I Allow MS-CHAPv1
Authorization	► I Allow MS-CHAPv2
Monitoring and Reports     Reserve Administration	Allow EAP-MD5
	► MINW EAP-TLS
	► Allow LEAP
	► Allow PEAP
	► 🕅 Allow EAP-FAST
	Preferred EAP protocol LEAP

• 🐁 Access Policies	► Allow LEAP
Access Services     El Service Selection Rules     @ Default Device Admin     @ Default Network Access     Idently     Authorization     @ deleteme     @ Monitoring and Reports     @ System Administration	<ul> <li>✓ Allow PEAP</li> <li>PEAP Inner Methods</li> <li>✓ Allow EAP-MS-CHAPv2</li> <li>✓ Allow Password Change Retries: 1</li> <li>✓ Allow EAP-GTC</li> <li>✓ Allow Password Change Retries: 1</li> </ul>
	<ul> <li>Now EAP-FAST</li> <li>EAP-FAST Inner Methods</li> <li>Allow EAP-MS-CHAPV2</li> <li>Allow Password Change Retries: 3</li> <li>Allow EAP-GTC</li> <li>Allow TLS-Renegotiation</li> <li>Use PACs DontUse PACs</li> <li>Tunnel PAC Time To Live: 90 Days v</li> <li>Proactive PAC update will occur after 10 % of PAC Time To Live has expired</li> <li>Allow Authenticated in-Band PAC Provisioning</li> <li>Server Returns Access Accept After Authenticsted Provisioning</li> <li>Barver Returns Access Accept After Authenticsted Provisioning</li> <li>Allow Machine Authentication</li> <li>Machine PAC Time To Live: 1 Weeks v</li> <li>Enable Stateless Bession Resume</li> <li>Authorization PAC Time To Live: 1 Hours v</li> </ul>

- 3. [Submit] をクリックします。
- 4. 選択した Identity グループを確認します。この例では、ACS 上に作成した [Internal Users] を使用し、変更を保存します。

Nanced Options							
entication failed R	eject 🔻						
notfound R	eject 💌						
ess failed D	rop 💌						
	r not found Received The Receiv	r not found Reject cess failed Drop For authentications using PEAP.	r not found Reject ress failed Drop For authentications using PEAR, LEAP, EAP	r not found Reject ress failed Drop For authentications using PEAP, LEAP, EAP-FAST or RADIL	r not found Reject ress failed Drop  For authentications using PEAR LEAP, EAP-FAST or RADIUS MSCHAP it i	r not found Reject ress failed Drop For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP it is not possib	r not found Reject ress failed Drop For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP it is not possible to continue

5. 許可プロファイルを確認するには、[Access Policies] > [Access Services] > [Default Network

Access] > [Authorization] に移動します。

ユーザのネットワークに対するアクセス条件や、認証後に許可する許可プロファイル(属性 )をカスタマイズできます。この精度は ACS 5.x でしか利用できません。この例では、 [Location]、[Device Type]、[Protocol]、[Identity Group]、[]EAP Authentication Method] を選 択します。



- 6. [OK] をクリックして変更を保存します。
- 7. 次に、ルールを作成します。ルールが定義されていない場合、クライアントは条件なしでア クセスが許可されます。

[Create] > [Rule-1] をクリックします。このルールは、グループ "Wireless Users" 内のユー ザ向けです。

Access Policies > Access Services > Defi	ault Network Access > Aufhorization				
Standard Policy Exception Policy					
Network Access Authorization Pc*	less .				-
Fiter: Status	Cisco Secure ACS - Mosilla Firefox				×
5	192168150.24 https://2921681	150.24/acsadmin/Policy	InputAction.do		슈
1 Status Frame NE			-		
No data to display	General				
	Name: Rule-1	Status: Enabled	- 0		
	The Customize bu policy conditions a Conditions	tton in the lower rig and results are avai	ht area of the policy rules screen con able here for use in policy rules.	trois which	
	MDG:Location:	in	All Locations LAB	Select	
	NDG:Device Type:	in	All Device Types 5500	Select	
	Protocol:	match	Radus	Select	
	Identity Group:	in	- All Groups Wireless Users	Select	
	Eap Authentication Method:	-ANY-			
	Results Authorization Profiles: Permit Access Select Deselect		You may select multiple authorization pro defined in multiple profiles will use the va profile defined.	files. Attributes lue from the first	
" E Dstaat Fr	OK Cancel			He	<u> </u>
Create  • Duplicate  • Edit	Delete A Move to V			Custe	mize Hit Count

8. 変更を保存します。 次のような画面が表示されます。

	VCC639 All	thorization Policy					
iter. St	atus	- Mate	chit Equals 🔹 Enat	led - Ci	ear Filter Go 🐨		
Status	Name	NDG:Location	NDG Device Type	Condition Protocol	identity Group	Esp Authentication Method	Results Authorization Profi
	Rule-1	in All Locations:LAB	In All Device Types 5508	match Radius	in All Groups:Wireless Users	-4117-	Permit Access
Default	_	If no rules defined or r	no enabled rule matches.				Permit Access

条件と一致しないユーザを拒否する場合は、デフォルト ルールを "deny access" に編集します。

9. 次に、サービス選択ルールを定義します。このページは、着信要求に適用するサービスを決

定する単純なポリシーまたはルールベースのポリシーを設定する場合に使用します。この例 では、ルールベースのポリシーを使用しています。

A	Coess P	olicies >	Access 5	iervices >	Service Selection	Ruies					
	Servic	e Sele	ction Poli	ey -	die based reso	I SERVICION					
	Filter	Statu	s 💌	Natch it	Equals 💌	Enabled	👻 Clear i	iter 🛛 Go 🛛 🗢			
			Status	Name	Protocol	Conditions		Res Service	ulta	Hit Count	
	1		8	Rule-1	match Radius			Default Netw	vork Access	0	
	2		8	Rule-2	match Tacacs			Default Devi	ce Admin	0	

## WLC の設定

設定には次の手順が必要です。

- 1. WLC での認証サーバの詳細設定
- 2. <u>ダイナミック インターフェイス (VLAN)の設定</u>
- 3. WLAN (SSID)の設定

WLC での認証サーバの詳細設定

WLC と RADIUS サーバの間でクライアントの認証やその他のトランザクションを行えるように、WLC を設定する必要があります。

次のステップを実行します。

- 1. コントローラの GUI で、[Security] をクリックします。
- 2. RADIUS サーバの IP アドレスと、RADIUS サーバと WLC の間で使用する共有秘密キーを 入力します。

この共有秘密キーは、RADIUS サーバに設定されたキーと一致している必要があります。

cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Security	RADIUS Authenti	cation Server	s > New					
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication Accounting Falback</li> <li>TACACS+ LDAP</li> <li>Local Net Users</li> <li>MAC Fitering</li> <li>Disabled Cliente</li> <li>User Login Policies</li> <li>AP Policies</li> <li>Pasword Policies</li> </ul>	Server Index (Priorit Server IP Address Shared Secret Form Shared Secret Confirm Shared Sec Key Wrap Port Number Server Status	ty) et ret	1 x 192.168.150.2 ASCII x  (Designed for 1012 Cnabled x	r FIPS custom	ers and requires a	key wrap compl	iant RADI	US server)
Local EAP	Support for RFC 357	6	Enabled -					
Priority Order	Server Timeout		2 aecond	la				
Certificate	Network User		🗷 Enable					
Access Control Lists	Management		🖻 Enable					
Wireless Protection     Policies	IPSec		Enable					
Web Auth								
Advanced								

ダイナミック インターフェイス (VLAN)の設定

この手順では、WLC でダイナミック インターフェイスを設定する方法について説明します。

次のステップを実行します。

1. ダイナミック インターフェイスは [Controller] > [Interfaces] ウィンドウのコントローラ GUI で設定します。

ControllerInterfaces > NewGeneralInterface NameInventoryInterface NameInterfacesInterfacesInterface GroupsNutticastNetwork RoutesInternal DHCP ServerMobility ManagementPortsNTPCOPAdvanced

2. [APPLY] をクリックします。

0

このダイナミック インターフェイス(この例では VLAN 253)の [Edit] ウィンドウが開きます。

3. このダイナミック インターフェイスの IP アドレスとデフォルト ゲートウェイを入力します

uluilu cisco	MONITOR WLANS		WIRELESS	<u>s</u> ecurity	MANAGEMENT
Controller	Interfaces > Edit				
General Inventory Interfaces	General Information	n			-
Interface Groups	Interface Name	vlan253	/		
Multicast Network Routes	NAC Address	00:24:9	7:09:03;cf		
) Internal DHCP Server	Guest Lan	F			
Mobility Management	Quarantine				
► NTP	Querentine Vien Id	0			
CDP     Advanced	Physical Informatio	n			
	The interface is attach Enable Dynamic AP Management	ed to a LAG.			
	Interface Address				
	VLAN Identifier	253			
	IP Address	192.168.15	3.81		
	Netmask	255.255.25	5.0		
	Gateway	192.168.15	3.1		
	DHCP Information				_
	Primary DHCP Server	1	92,100,150,25		
	Secondary DHCP Serv	/er			
	Access Control List				_
	ACL Name	-	one 🔄		
	Note: Changing the Inter temporarily disabled and some clients.				

- 4. [APPLY] をクリックします。
- 5. 設定したインターフェイスは、次のようになります。

uhuhu cisco	MONITOR	<u>W</u> LANs		WIRELESS	<u>s</u> ecurity	MANAGEMENT		s help	FEEDBACK	
Controller General Inventory	Interfaces	s Name	1	/LAN Identifier	192.168.75	s Interfac	е Туре Dy	mamic AP I	Management	
Interfaces Interface Groups Multicast Network Routes	service-por virtual vlan253	±	1	N/A. N/A 253	0.0.0.0 1.1.1.1 192.168.15	Static Static 3.81 Dynamic	No No Di	t Supported t Supported sabled		•
<ul> <li>Internal DHCP Server</li> <li>Mobility Management Ports</li> </ul>										
<ul> <li>NTP</li> <li>CDP</li> <li>Advanced</li> </ul>										

WLAN (SSID)の設定

この手順では、WLC で WLAN を設定する方法について説明します。

次のステップを実行します。

- 1. 新規の WLAN を作成するには、コントローラの GUI で [WLANs] > [Create New] の順に選 択します。新規の WLAN のウィンドウが表示されます。
- 2. WLAN ID と WLAN SSID 情報を入力します。

WLAN SSID には任意の名前を入力できます。この例では、WLAN SSID として goa を使用 しています。

uhuhu cisco	MONITOR	<u>W</u> LANs		W]RELE5S	SECURITY	MANAGEMENT	COMMAND5
WLANS	WLANs >	New					
<ul> <li>WLANS</li> <li>Advanced</li> </ul>	Type Profile Ne SSID ID	917716	WLAN goo goo 1	•			

3. [Apply] をクリックして、WLAN goa の [Edit] ウィンドウに移動します。

cisco			WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
WLANs	WLANs > Edit 'ge	ba'					
WLANS WLANS	General Secur	ity QoS	Advanced				
<ul> <li>Advanced</li> <li>AP Groups</li> </ul>	Profile Name Type SSID Status Security Policies Radio Policy Interface/Interfac Group(G) Multicast Man Feat Broadcast SSID	goa WLAN goa [WPA2]] (Modificati All ture ⊂ Inable P Inable	ed Auth(802.1X ons done under U	+ CCKM)] r security tab (	will appear after ap	oplying the chang	yes.)

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY
WLANs	WLANs > Edit 'goa'
WLANS WLANS	General Security QoS Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Løyer 2 Security VPA+WPA2 -
	WPA+WPA2 Parameters
	WPA Policy
	WPA2 Policy R WPA2 Encryption RAES TRIP
	Auth Key Mgmt 802.1X+CCKN .

Ivanced	
rs	
de use of default servers on this WLAN	
	LDAP Servers
Enabled	Server 1 None -
Authentication Servers Accounting Servers	Server 2 None 💌
Trabled Trabled	Server 3 None 💌
IP:192.168.150.24, Port:1812 Vone V	
None v None v	
None × None ×	
1	
•	
Order Used For Authentication	
	Ivanced srs de use of default servers on this WLAN Cnabled The block of the fault servers on this WLAN Cnabled For Authentication Servers V Dnabled V Dnabled TP:192.168.150.24, Port:1812 × None × None × None × None × None × Order Used For Authentication

### WLANs > Edit 'goa'

Allow AAA Override Enabled	DHCP
Coverage Hole Detection 🛛 Enabled	DHCP Server Override
Enable Session Timeout	-
Aironet IE Renabled	DHCP Addr. Assignment P Required
Diagnostic Channel Enabled	Management Frame Protection (MFP)
IPv6 Enable 2	and cliest perturbin # Dirabled a
Override Interface ACL None -	HER CHERCEPTOLECION - TO BEDIEC
P2P Blocking Action Disabled -	DTIM Period (in beacon intervals)
Client Exclusion <sup>2</sup> Enabled	802.11a/n (1 - 255) 1
Maximum Allowed	802.11b/g/n (1 - 255) 1
Cliente =	NAC
Static IP Tunneling 😰 🗌 Enabled	NAC State None -
Channel Scanning Defer	Load Balancing and Band Select
Scan Defer Priority 0 1 2 3 4 5 6 7	Client Load Balancing
	Client Band Select
Scan Defer Time(msecs) 100	

## 無線クライアント ユーティリティの設定

PEAP-MSCHAPv2 (user1)

テスト クライアントでは、Intel 6300-N ドライバ バージョン 14.3 対応の Microsoft Windows 7 ネ イティブ サプリカントを使用します。テストでは、ベンダーから最新のドライバを取得して使用 することを推奨します。

次の手順を実行して、Windows Zero Config (WZC)のプロファイルを作成します。

- 1. [Control Panel] > [Network and Internet] > [Manage Wireless Networks] に移動します。
- 2. [Add] タブをクリックします。
- 3. [Manually create a network profile] をクリックします。

How do	o you want to add a network?
\$	Manually create a network profile This creates a new network profile or locates an existing network and saves a profile for the network on your computer. You need to know the network name (SSID) and security key (if applicable).
4	Create an ad hoc network This creates a temporary network for sharing files or an Internet connection

4. WLC で設定したとおりに詳細を追加します。

注:SSIDでは大文字と小文字が区別されます。

5. [Next] をクリックします。

Network name:	goa	
Security type:	WPA2-Enterprise	
Encryption type:	AES 👻	
Security Key:	Hide characters	
Start this connect	tion automatically	
Connect even if	the network is not broadcasting	

6. [Change connection settings] をクリックして設定を再度確認します。

Manually connect to a wireless network	
Successfully added goa	
Change connection settings Open the connection properties so that I can change the settings.	
	Close

7. PEAP が有効になっていることを確認します。

goa Wireless Network Pr	operties	23	
Connection Security			
	[		
Security type:	WPA2-Enterprise		
Encryption type:	AES 👻		
Choose a network aut	hentication method:		
Microsoft: Protected E	EAP (PEAP) 🔻 Settings		
Remember my credentials for this connection each			
time I'm logged on			
Advanced settings			
	OK	ncel	

goa Wireless Network Properties	x
Connection	
Security type: WPA2-Enterprise	
Encryption type: AES -	
Choose a network authentication method: Microsoft: Protected EAP (PEAP) Settings Remember my credentials for this connector code time I'm logged on Advanced settings	
OK Canc	el

8. この例では、サーバ証明書は検証しません。このチェックボックスをオンにしても接続できない場合は、機能を無効にしてから再度テストしてみてください。

Protected EAP Properties
When connecting:
Validate server certificate
Connect to these servers:
Trusted Root Certification Authorities:
AAA Certificate Services
C AddTrust External CA Root
Class 3 Public Primary Certification Authority
Class 3 Public Primary Certification Authority
DigiCert Assured ID Root CA
DigiCert High Assurance EV Root CA
Do not prompt user to authorize new servers or trusted certification authorities.
Select Authentication Method:
Configure
Enable Fast Reconnect
Enforce Network Access Protection
Disconnect if server does not present cryptobinding ILV
Enable Identity Privacy
OK Cancel

9. ほかにも、Windows クレデンシャルでログインできます。ただし、この例ではその方法を

用いません。[OK] をクリックします。



10. [Advanced settings] をクリックしてユーザ名とパスワードを設定します。

Connection Security	
Security type: WPA2-Enterprise   Encryption type: AES	
Choose a network authentication method: Microsoft: Protected EAP (PEAP) ▼ Settings Remember my credentials for this connection each time I'm logged on	
Advanced settings	
OK Cance	

Advanced settings
802.1X settings 802.11 settings
Specify authentication mode:
User authentication    Save credentials
Delete credentials for all users
Enable single sign on for this network
Perform immediately before user logon
Perform immediately after user logon
Maximum delay (seconds): 10
Allow additional dialogs to be displayed during single sign on
This network uses separate virtual LANs for machine and user authentication
OK Cancel

Saving your credential when you're not logge	s allows your comp d on (for example,	uter to co to downlo	nnect to t ad updat	he network es).
user1	d on (for example,			es).
user1				
user1				
	•			

これで、クライアント ユーティリティで接続する準備が整いました。

EAP-FAST (user2)

テスト クライアントでは、Intel 6300-N ドライバ バージョン 14.3 対応の Microsoft Windows 7 ネ イティブ サプリカントを使用します。テストでは、ベンダーから最新のドライバを取得して使用 することを推奨します。

次の手順を実行して WZC でプロファイルを作成します。

- 1. [Control Panel] > [Network and Internet] > [Manage Wireless Networks] に移動します。
- 2. [Add] タブをクリックします。
- 3. [Manually create a network profile] をクリックします。





4. WLC で設定したとおりに詳細を追加します。

注:SSIDでは大文字と小文字が区別されます。

5. [Next] をクリックします。

Network anno		
Network name:	goa	
Security type:	WPA2-Enterprise 🔻	
Encryption type:	AES 💌	
Security Key:	Hide characters	
Start this connec	ction automatically	
Connect even if	the network is not broadcasting	
Warning: If you	select this option, your computer's privacy might be at risk.	

6. [Change connection settings] をクリックして設定を再度確認します。

Manually connect to a wireless network	
Successfully added goa	
Change connection settings Open the connection properties so that I can change the settings.	
	Close

7. EAP-FAST が有効になっていることを確認します。

注:デフォルトでは、WZCの認証方式はEAP-FASTではありません。サードパーティ ベン ダーからユーティリティをダウンロードする必要があります。この例では、Intel カードを 使用するため、システムに Intel PROSet がインストールされています。

goa Wireless Network Pr	operties	
Connection Security		
Security type: Encryption type:	WPA2-Enterprise   AES	
Choose a network aut Cisco: EAP-FAST Microsoft: Smart Card Microsoft: Protected B Cisco: LEAP Cisco: PEAP Cisco: PEAP Cisco: EAP-FAST Intel: EAP-SIM Intel: EAP-SIM Intel: EAP-AKA Advanced settings	hentication method: I or other certificate AP (PEAP) I n each	
<u>.</u>	ОК Са	ncel

goa Wireless Network Properties	23
Connection	
Security type: WPA2-Enterprise   Encryption type: AES	
Choose a network authentication method: Cisco: EAP-FAST Settings Remember my credentials for this connection each time I'm logged on	
Advanced settings	
OK Car	ncel

8. [Allow automatic PAC provisioning] をオンにして、[Validate server certificate] がオフになっ ていることを確認します。

EAP-FAST Properties
Connection User Credentials Authentication About
Use anonymous outer identity anonymous Use Protected Access Credentials (PAC) Allow automatic PAC provisioning
PAC Authority:          None       Import
Validate server certificate
Trusted Root Certificate Authority         AAA Certificate Services         AddTrust External CA Root         Class 3 Public Primary Certification Authority         Class 3 Public Primary Certification Authority         DigiCert Assured ID Root CA         DigiCert High Assurance EV Root CA         DST Root CA X3
OK Cancel Help

9. [User Credentials] タブをクリックして、user2 のクレデンシャルを入力します。ほかにも、 Windows クレデンシャルでログインできます。ただし、この例ではその方法を用いません 。

EAP-FA	ST Properties		? X
Conn	ection User Credentia	Authentication About	
	Use certificate on th	is computer	
	Use one-time passw	ord	
	Use Windows userna	ame and password	
	Prompt automatically	y for username and password	
	Use saved username	and password	
	Username:	user2	
	Password:	•••••	
	Confirm password:		
		V	
		OK Cancel	Help

10. [OK] をクリックします。

EAP-FAST Properties	? ×
Connection User Credentials Authentication About	
Select authentication method:	
Any method 🔹	Configure
Enable Fast Reconnect	
Enable Posture validation	
ОК Са	ncel Help

これで、クライアントユーティリティで user2 に接続する準備が整いました。

注:user2が認証を試みると、RADIUSサーバはPACを送信します。PAC を受け入れて認証を完 了します。



## 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。

<u>Output Interpreter Tool</u>(OIT)(<u>登録</u>ユーザ専用)では、特定の show コマンドがサポートされ ています。OIT を使用して show コマンド出力の解析を表示します。

user1(PEAP-MSCHAPv2)の検証

WLC GUI から [Monitor] > [Clients] に移動して MAC アドレスを選択します。

### Clients > Detail

#### **Client Properties**

MAC Address	00:24:d7:ae:f1:98	
IP Address	192.168.153.107	
Client Type	Regular	
User Neme	user1	
Port Number	13	
Interface	vian253	
VLAN ID	253	
CCX Version	CCXv4	
E2E Version	E2Ev1	
Mobility Role	Local	
Mobility Peer IP Address	N/A	
Policy Manager State	RUN	
Management Frame Protection	No	
UpTime (Sec)	12	
Power Save Mode	OFF	
Current TxRateSet		
Data RateSet	6.0,9.0,12.0,18.0,24.0,3 0	6.0,45.0,54.

### **AP Properties**

AP Address	2c:3f:38:c1:3c:f0
AP Name	3502e
AIP Type	902.11an
WLAN Profile	904
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Pol Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Nat Implemented
Re-authentication timeout	86365
Remaining Re-authentication timeout	0
WEP State	WEP Enable

### Security Information

Security Policy Completed	Yes
Policy Type	REN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	PEAP
SNMP NAC State	Access
Redius NAC State	RUN

WLC RADIUS のステータス:

### <#root>

(Cisco Controller) >

show radius auth statistics

Authentication Servers:
Server Index 1
Server Address 192.168.150.24
Msg Round Trip Time 1 (msec)
First Requests 8
Retry Requests 0
Accept Responses 1
Reject Responses 0
Challenge Responses7
Malformed Msgs 0
Bad Authenticator Msgs0

Pending Requests	0
Timeout Requests	0
Unknowntype Msgs	0
Other Drops	0

ACS ログ:

- 1. 次の手順を実行してヒット カウントを表示します。
  - a. 認証から 15 分以内にログを確認するときは、必ずヒット カウントを更新してください。

0	ngië re	sun selec	non 🦷 F	lule based result selection			
iervi	ce Sele	ection Pol	ley				
Filter	: Stat.	18 -	Match if:	Equals - Enabled	- Clear Filter	Go 🔻	
		Statue	Name	Condition	3	Results Service	Hit Cou
1		0	Bule-1	match Radius		Default Network Access	1
2	Г	0	Rule-2	match Tacaca		Default Device Admin	0

b. 同じページの最下部に [Hit Count] のタブがあります。

etwork /	access Authorization F	Policy					
ilter: St	atus	<ul> <li>Match if: Equals</li> </ul>	<ul> <li>Enabled</li> </ul>	▼ Clear Filter Go ▼			
lame	NDG:Location	NDG:Device Type	Conditi Protocol	ons Identity Group	Eap Authentication Method	Results Authorization Profiles	HitCo
ule-1	in All Locations LAB	in All Device Types:5508	match Radius	in All Groups:Wireless Users	-ANY-	Permit Access	1

2. [Monitoring and Reports] をクリックすると、新たにポップアップ ウィンドウが表示されま す。[Authentications] – [Radius] – [Today] に移動します。このほか、どのサービス選択ルー ルが適用されたかについては、[Details] をクリックすると確認できます。

그 또 ㅋ											Launch Inter	nective Veneer
Showing Page	1 of 1					6	Colo Page: Ge					
AAA Protocol > RAD	IUS Authe	nticatio	n									
Authentication Status : Date :	Pass or Fail Jonuary 29,	2012 05:	40 PM -	January 29	2012 06:10 PM (1	Lost 30 Minutes (Lost Hour	H <u>Loot 12 Hours   Tedar   Yes</u>	tendey i Last 7 Do	(a   Last 30 Dava )			
Generated on January 2	9, 2012 6:10	42 PM 8	ST									
Reited	-Click for a	lataila	R -mau	sa over iten	n flor additional info	mater						
Logged At	RADIUS	S NAS Failure	Details	Usemane	MAC/IP Address	Access Service	Authentication Method	Network Device	NAS IP Address	NAS Port ID	CTS Security Group	ACS Instance
Jan 29,12 6:07 37.943	PM 🖌		<i>e</i>	uper1	00-24-d7-ae-f1-98	Default Notesrk Access	PEAP (EAP-MBCHAPv2)	WLC-5508	192.168.75.44			SALIL-ACS52

## user2(EAP-FAST)の検証

## WLC GUI から [Monitor] > [Clients] に移動して MAC アドレスを選択します。

Clients > Detail

Client Properties			AP Properties	
MAC Address	00r24rd7raerf1r98		AP Address	2013fr3810113crf0
1P Address	192.168.153.111		AP Name	3502e
Client Type	Regular		AP Type	002.11an
User Name	user2		WLAN Profile	goa
Port Number	13		Statue	Associated
Interface	vlan253		Association ID	1
VLAN ID	253		802.11 Authentication	Open System
CCX Version	CCXV4	•	Reason Code	1
E2E Version	E2Ev1		Status Code	0
Mobility Role	Local		CF Pollable	Not Implemented
Mobility Peer IP Address	N/A		CF Poll Request	Not Implemented
Policy Manager State	RUN		Short Preamble	Not Implemented
Management Frame Protection	No		PBCC	Not Implemented
UpTime (Sea)	29		Chennel Agility	Not Implemented
Power Save Mode	OFF		Re-authentication timeout	86392
Current TxRateSet	m15 6.0.9.0.12.0.18.0.24	1.0.36.0.48.0.54.	Remaining Re-authentication timeout	0
Data RateSet	0		WEP State	WEP Enable

### Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	EAP-FAST
SNMP NAC State	Access
Radius NAC State	RUN

### ACS ログ:

1. 次の手順を実行してヒット カウントを表示します。

a. 認証から 15 分以内にログを確認するときは、必ずヒット カウントを更新してください。

Filter:	State	JS <u>-</u>	Match It.	Equals 👻	Enabled -	Clear Filter	Go 🗢	
	Г	Status	Name	Protocol	Conditions		Results Service	Hit Cour
1		0	Rule-1	match Radius			Default Network Access	3
2		0	Rule-2	match Tacacs			Default Device Admin	0

b. 同じページの最下部に [Hit Count] のタブがあります。

Filter: Sta	atus						
		<ul> <li>Match if: Equals</li> </ul>	<ul> <li>Enabled</li> </ul>	▼ Clear Filter Go ▼			
Name	NDG:Location	NDG:Device Type	Conditi Protocol	ions Identity Group	Eap Authentication Method	Results Authorization Profiles	Hit Cou
Rule-1	in All Locations:LAB	in All Device Types:5508	match Radius	in All Groups: Wireless Users	-ANY-	Permit Access	2

2. [Monitoring and Reports] をクリックすると、新たにポップアップ ウィンドウが表示されま す。[Authentications] – [Radius] – [Today] に移動します。このほか、どのサービス選択ルー ルが適用されたかについては、[Details] をクリックすると確認できます。

-	9 10												Launch Interactive	Vewer
	Shi	owing Pe	ige 1	of 1		111111	rol reev	Head Look	I Get	io Page: Go				
AAA Pr	0000	ol > R/	DIUS	Auther	ticatio	n								
Authent Data : Generat	ticatio ted on ad	n Statu Januar	y 29, 2	s or Fail sary 39, 3 012 6:23	2012 06 17 PM I	S3 PM - EST	January 29, 3	2012 06:23 PM (La	at 20 Minutes ( <u>Last Hour</u> (L	<u>aari 12 Hours   Todar   Yesterdar  </u>	Last 7 Days (Last	(20 Days)		
	Logi	ped At		RACIUS Status	NAS Failure	Details	Usemane	MAC/IP Address	Access Service	Authentication Method	Natwork Device	NAS IP Address NAS Por	ID CTS Security Group	ACS IN
Jan 29	12 6	19:27.2	TO PM	*		14	upor2	90-24-d7-ap-f1-98	Default Network Access	EAP-FAST (EAP-MSCHWPv2)	WLC-5508	192.168.75.44		SALL-A
Jan 29	12 6	07:37.9	43 PM	*		4	user1	00-24-d7-ae-f1-95	Default Network Access	PEAP (EAP-MSCHAPV2)	WLC-5598	192 168 75.44		SALL-P

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。

### トラブルシューティングのためのコマンド

<u>Output Interpreter Tool</u>(OIT)(<u>登録</u>ユーザ専用)では、特定の show コマンドがサポートされ ています。OIT を使用して show コマンド出力の解析を表示します。

注: debug コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

1. 問題が発生した場合は、WLC で次のコマンドを発行します。

- debug client <mac add of the client>
- debug aaa all enable
- show client detail <mac addr> :ポリシー マネージャの状態を確認します。
- show radius auth statistics : 失敗の原因を確認します。
- debug disable-all:デバッグをオフにします。
- ・ clear stats radius auth all:WLC 上の RADIUS 統計情報を削除します。

2. ACS のログを確認して失敗の原因を探します。

## 関連情報

• <u>テクニカル サポートとドキュメント - Cisco Systems</u>

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。