ダイナミックVLAN割り当てのRADIUSサーバと WLCの設定

内容

概要 前提条件 要件 <u>使用するコンポーネント</u> 表記法 RADIUS サーバによるダイナミック VLAN 割り当て 設定 ネットワーク図 コンフィギュレーション 設定手順 RADIUS サーバの設定 ダイナミック VLAN 割り当て用の Cisco Airespace VSA アトリビュートによる ACS の設定 複数の VLAN を使用するためのスイッチの設定 WLC の設定 Wireless Client Utility の設定 確認 トラブルシュート 関連情報

<u>概要</u>

このドキュメントでは、ダイナミック VLAN 割り当ての概念について説明します。このドキュメ ントでは、ワイヤレス LAN(WLAN)クライアントを特定の VLAN に動的に割り当てるようにワ イヤレス LAN コントローラ(WLC)および RADIUS サーバを設定する方法について説明します 。

前提条件

<u>要件</u>

この設定を行う前に、次の要件が満たされていることを確認します。

- •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
- Lightweight AP Protocol (LWAPP; Lightweight AP プロトコル)に関する基本的な知識がある

<u>使用するコンポーネント</u>

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 5.2 が稼動している Cisco 4400 WLC
- Cisco 1130 シリーズ LAP
- ファームウェア リリース 4.4 が稼動している Cisco 802.11a/b/g ワイヤレス クライアント ア ダプタ
- バージョン 4.4 が稼動している Cisco Aironet Desktop Utility (ADU)
- バージョン 4.1 が稼動している CiscoSecure Access Control Server (ACS)
- Cisco 2950 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、初期(デフォルト)設定の状態から起動しています 。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は、『<u>シスコ テクニカル ティップスの表記法』を参照してください。</u>

RADIUS サーバによるダイナミック VLAN 割り当て

一般的な WLAN システムでは、Service Set Identifier(SSID)(コントローラの用語では WLAN)に関連付けられたすべてのクライアントに適用されるスタティックなポリシーが各 WLAN に存在します。この方法は強力ですが、異なる QoS ポリシーやセキュリティ ポリシーを 継承するために各クライアントを異なる SSID に関連付ける必要があるので、さまざまな制約が あります。

一方、Cisco WLAN ソリューションでは、アイデンティティ ネットワーキングがサポートされて います。この場合、ネットワーク上で 1 つの SSID のみをアドバタイズすることにより、特定の ユーザはユーザ クレデンシャルに基づいて異なる QoS ポリシーやセキュリティ ポリシーを継承 できるようになります。

ダイナミック VLAN 割り当ては、ユーザが入力したクレデンシャルに基づいてワイヤレス ユーザ を特定の VLAN に割り当てる機能です。ユーザを特定のVLANに割り当てるこの作業は、 CiscoSecure ACSなどのRADIUS認証サーバによって処理されます。たとえば、この機能を利用 すると、キャンパス ネットワーク内を移動するワイヤレス ホストを同じ VLAN に割り当てるこ とができます。

したがって、クライアントがコントローラに登録済みの LAP への関連付けを試みると、LAP から RADIUS サーバにユーザのクレデンシャルが渡されて検証されます。認証に成功すると、 RADIUS サーバからユーザに特定の Internet Engineering Task Force(IETF)アトリビュートが 渡されます。これらの RADIUS アトリビュートにより、ワイヤレス クライアントに割り当てら れる VLAN ID が決定されます。ユーザはこの事前設定済みの VLAN ID に常に割り当てられるの で、クライアントの SSID(WLC の用語では WLAN)は無視されます。

VLAN ID の割り当てに使用される RADIUS ユーザ アトリビュートは次のとおりです。

• IETF 64(Tunnel Type): これを VLAN に設定します。

- IETF 65(Tunnel Medium Type):これを 802 に設定します。
- IETF 81(Tunnel Private Group ID): これを VLAN ID に設定します。

VLAN ID は 12 ビットで、1 ~ 4094 の値(両端を含む)を取ります。Tunnel-Private-Group-IDは 文字列型であるため、<u>RFC2868</u> でIEEE 802.1Xで使用するように定義されているため、VLAN IDの整数値は文字列としてエンコードされます。これらのトンネル アトリビュートが送信される 際には、Tag フィールドの値を設定する必要があります。

RFC2868 のセクション 3.1 で述べられているように、 Tag フィールドは 1 オクテットの長さを 持ち、同じトンネルを参照する同じパケット内の属性をグループ化する手段を提供することを目 的としています。このフィールドで有効な値は、0x01 ~ 0x1F(両端を含む)です。Tag フィー ルドを使用しない場合は、このフィールドをゼロ(0x00)に設定する必要があります。 すべての RADIUS 属性の詳細は、RFC 2868 を参照してください。

<u>設定</u>

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。

<u>ネットワーク図</u>

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 172.16.1.1 です。
- •WLC の管理インターフェイス アドレスは 172.16.1.30 です。
- WLC の AP マネージャ インターフェイス アドレスは 172.16.1.31 です。
- DHCPサーバアドレス172.16.1.1は、LWAPPにIPアドレスを割り当てるために使用されます。コントローラの内部 DHCP サーバは、ワイヤレス クライアントに IP アドレスを割り当てる目的に使用されます。
- VLAN10 および VLAN11 は、この設定全体を通じて使用されます。RADIUS サーバにより user1 は VLAN10 に割り当てられ、user2 は VLAN11 に割り当てられるように設定されてい ます。注意:このドキュメントでは、user1に関連するすべての構成情報のみが表示されます 。user2に関するこのドキュメントで説明されている手順と同じ手順を実行してください。
- このドキュメントでは、セキュリティメカニズムとして 802.1x と LEAP を使用します。注
 :WLANを保護するために、EAP-FASTやEAP-TLS認証などの高度な認証方式を使用することを推奨します。このドキュメントでは、説明を簡単にするため、LEAP を使用しています

<u>コンフィギュレーション</u>

このドキュメントでは、設定を開始する前に LAP が WLC にすでに登録されていることが前提と なっています。詳細は、『<u>ワイヤレス LAN コントローラと Lightweight アクセス ポイントの基本</u> <u>設定例</u>』を参照してください。必要な登録手順については、『<u>ワイヤレス LAN コントローラ</u> <u>(WLC)への Lightweight AP (LAP)の登録</u>』を参照してください。

設定手順

o

この設定は、次の4つのカテゴリに分類されます。

- 1. <u>RADIUS サーバの設定</u>
- 2. <u>複数の VLAN を使用するためのスイッチの設定</u>
- 3. <u>WLC の設定</u>
- 4. Wireless Client Utility の設定

RADIUS サーバの設定

設定には次の手順が必要です。

- RADIUSサーバ上のAAAクライアントとしてのWLCの設定
- RADIUS サーバでのダイナミック VLAN 割り当てに使用するユーザと RADIUS (IETF) アト リビュートの設定

RADIUS サーバでの WLC の AAA クライアントの設定

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 の GUI で、[Network Configuration] をクリックします。
- 2. [AAA Clients] フィールドの下にある [Add Entry] セクションをクリックします。
- AAA クライアントの IP アドレスとキーを入力します。ここで入力する IP アドレスは、 WLC の管理インターフェイスの IP アドレスと一致している必要があります。ここで入力す るキーは、[セキュリティ] ウィンドウで WLC に対して設定されているキーと一致している 必要があります。これは AAA クライアント(WLC)と RADIUS サーバの間の通信で使用さ れる秘密キーです。
- 4. [Authenticate Using] フィールドで、認証タイプとして [RADIUS (Cisco Airespace)] を選択 します。

CISCO SYSTEMS	Network Configuration
and the still the s	Edit
User Setup	
Group Setup	Add AAA Client
Shared Profile Components	
Network Configuration	AAA Client Hostname WLC4400
System Configuration	AAA Client IP Address
Configuration	Shared Secret cisco
Administration Control	RADIUS Key Wrap
Databases	Key Encryption Key
noon Posture	Message Authenticator Code
Network Access Profiles	Key Input Format © ASCII ® Hexadecimal
Reports and Activity	Authenticate Using RADIUS (Cisco Airespace)
Documentation	□ Single Connect TACACS+ AAA Client (Record stop in accounting on failure)
·	Log Update/Watchdog Packets from this AAA Client
	Log RADIUS Tunneling Packets from this AAA Client
	Replace RADIUS Port info with Username from this AAA Client
	Match Framed-IP-Address with user IP address for accounting packets from this AAA Client
	Submit Submit + Apply Cancel

RADIUS サーバでのダイナミック VLAN 割り当てに使用するユーザと RADIUS(IETF)アトリビ ユートの設定

この手順では、RADIUS サーバのユーザと、それらのユーザに VLAN ID を割り当てるための RADIUS(IETF)アトリビュート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. ACS の GUI で、[User Setup] をクリックします。
- 2. [User Setup] ウィンドウで、[User] フィールドにユーザ名を入力し、[**Add/Edit**] をクリック します。

Cisco Systems	User Setup
	Select
User Setup	
Group Setup	User: User1
Shared Profile Components	Find Add/Edit
Network Configuration	List users beginning with letter/number:
System Configuration	<u>A B C D E F G H I J K L M</u> <u>N O P Q R S T U V W X Y Z</u>
Configuration	
Madministration Control	
Databases	Remove Dynamic Users
Posture Validation	
Network Access Profiles	Y Back to Help
Reports and Activity	
Online Documentation	

3. [Edit] ページで、図に示すように必要なユーザ情報を入力します。

CISCO SYSTEMS	User Setup
antilliterantillitera -	Edit
User Setup	User: User1
Shared Profile Components	Account Disabled
Network Configuration	Supplementary User Info
System Configuration	Real Name User1
Interface Configuration	Description User1
Administration Control	
External User Databases	User Setup 🤶
Posture Validation	Password Authentication:
Network Access Profiles	CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.)
Activity	Password •••••
Online Documentation	Confirm Password
	Separate (CHAP/MS-CHAP/ARAP)
	Password •••••••••
	Confirm Password
	When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

User Setup セクションで入力したパスワードと、ユーザ認証時にクライアント側で入力す るパスワードは一致している必要があります。

- 4. [Edit] ページを下にスクロールして、[IETF RADIUS Attributes] フィールドを探します。
- 5. [IETF RADIUS Attributes] フィールドで、3 つのトンネル アトリビュートの横にあるチェック ボックスにチェックマークを付け、図に示すようにアトリビュート値を設定します。

Cisco Systems	CISCO SYSTEMS User Setup						
	Failed attempts since login: 0	last successful					
User Setup	Reset current faile	d attempts count					
Group Setup	on submit						
Shared Profile Components							
Network Configuration	Download	able ACLs	়				
System Configuration	Assign IP ACL:	VPN_Access	•				
Configuration		0	-				
Administration Control		S Attributes	<u>.</u>				
- C External User	🗹 [064] Tunnel-Type						
90 Databases	Tag 1 🗾 Value	VLAN	-				
BBBB Posture Validation	Tag 2 💽 Value		-				
Network Access	🗹 [065] Tunnel-Medium-1	Туре					
Profiles	Tag 1	▼ Value 802					
Reports and Activity	Tag 2	▼ Value	•				
	🗹 (081) Tunnel-Private-G	Group-ID					
	Tag 1 💌 Va	lue 10					
	Tag 🛛 💌 Va	lue					
	<u></u>						

注: ACSサーバの初期設定では、IETF RADIUS属性が表示されない場合があります。IETF アトリビュートを有効にするために、ユーザ設定ウィンドウで [Interface Configuration] > [RADIUS (IETF)] の順に選択します。次に、アトリビュート 64、65、および 81 の [User] 列 と [Group] 列のチェック ボックスにチェックマークを付けます。



注:RADIUSサーバがクライアントを特定のVLANに動的に割り当てるため、RADIUSサーバ のIETF 81(Tunnel-Private-Group-ID)フィールドで設定されたVLAN-IDがWLCに上に上にに 存在します。RADIUS サーバでユーザごとの設定を有効にするために、[Interface Configuration] > [Advanced Options] の順に選択し、[Per User TACACS+/RADIUS] アトリビ ュート チェック ボックスをオンにします。また、認証プロトコルとして LEAP を使用する ので、図に示すように RADIUS サーバの [System Configuration] ウィンドウで LEAP が有効 になっていることを確認します。



System Configuration

	Cisco client initial message:
User Setup	PEAP session timeout (minutes): 120
Group Setup	Enable Fast Reconnect:
Shared Profile Components	EAP-FAST
Network Configuration	
System Configuration	Allow EAP-TLS
Interface Configuration	Select one or more of the following options:
Administration	Certificate CN comparison
External User Databases	EAP-TLS session timeout (minutes): 120
Posture Validation	
Network Access Profiles	LEAP Allow LEAP (For Aironet only)
Reports and Activity	EAP-MD5
Online Documentation	Allow EAP-MD5
	AP EAP request timeout (seconds): 20

<u>ダイナミック VLAN 割り当て用の Cisco Airespace VSA アトリビュートによる</u> <u>ACS の設定</u>

ACS の最新バージョンでは、Cisco Airespace [VSA (Vendor-Specific)] アトリビュートを使用し 、ACS のユーザ設定に基づいて、認証に成功したユーザを(VLAN ID ではなく)VLAN インター フェイス名に割り当てます。これを実現するには、このセクションで説明する手順を実行する必 要があります。

注:このセクションでは、ACS 4.1バージョンを使用してCisco Airespace VSA属性を設定します。

<u>Cisco Airespace VSA アトリビュート オプションを使用した ACS グループの設定</u>

次のステップを実行します。

- 1. ACS 4.1 の GUI で、ナビゲーション バーから [Interface Configuration] をクリックします。 次に、Cisco Airespace アトリビュート オプションを設定するために、[Interface Configuration] ページで **[RADIUS (Cisco Airespace)]**を選択します。
- 2. [RADIUS (Cisco Airespace)] ウィンドウで、[User Edit] ページで表示するために、[Aire-Interface-Name] の横の [User] チェック ボックス(必要に応じて [Group] チェック ボックス)をオンにします。次に [Submit] をクリックします。



- 3. user1 の Edit ページに移動します。
- 4. [User Edit] ページで、[Cisco Airespace RADIUS Attributes] セクションまで下にスクロール します。[Aire-Interface-Name] アトリビュートの横のチェック ボックスにチェックマークを 付け、ユーザ認証が成功した場合に割り当てるダイナミック インターフェイスの名前を指 定します。次の例では、ユーザを admin VLAN に割り当てています。

CISCO SYSTEMS	User Setup	
	L Date exceeds.	
User Setup Group Setup Shared Profile Components Network Configuration System Configuration	☐ Failed attempts excee 5 Failed attempts since login: 0 ☐ Reset current failed on submit	May 💌 24 2009 ed: last successful d attempts count
Interface Configuration	Download	able ACLs 🤶
Administration Control	Assign IP ACL:	VPN_Access
Posture Validation	Cisco Airespace R	ADIUS Attributes ?
Network Access Profiles	☑ [14179\005] Aire-Interfa	ice-Name
Reports and Activity	admin	
Documentation		

5. [Submit] をクリックします。

複数の VLAN を使用するためのスイッチの設定

複数の VLAN がスイッチを通過できるようにするには、次のコマンドを発行して、コントローラ に接続されたスイッチ ポートを設定する必要があります。

- 1. Switch(config-if)#switchport mode trunk
- 2. Switch(config-if)#switchport trunk encapsulation dot1q

注:デフォルトでは、ほとんどのスイッチはトランクポートを介してスイッチ上で作成されたす べてのVLANを許可します。

これらのコマンドは、Catalyst オペレーティング システム(CatOS)スイッチによって異なります。

スイッチに有線ネットワークが接続されている場合は、有線ネットワークに接続されたスイッチ ポートに対しても同じ設定を適用できます。これにより、有線ネットワークとワイヤレス ネット ワークの同じ VLAN 間での通信が可能になります。

注:このドキュメントでは、VLAN間通信については説明しません。これはこのドキュメントの

範囲外です。VLAN 間ルーティングを行うには、レイヤ 3 スイッチまたは VLAN およびトランキ ングが適切に設定された外部ルータが必要になります。VLAN 間ルーティングの設定に関して説 明しているドキュメントはいくつかあります。

<u>WLC の設定</u>

設定には次の手順が必要です。

- 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

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 サーバの [Network Configuration] > [AAA Clients] > [Add Entry] で設定されたキーと一致している必要があります。WLC のウィンドウ の例を次に示します。

ı. cısco	MONITOR MEANS CONT	Sage Configuration Eng Logout Befresh ROLLER WIRELESS <u>B</u> ECURITY MANAGEMENT COMMANDS HELP
Security	RADIUS Authentication	Servers>New <back apply<="" td=""></back>
AAA General RADIUS Authentication Accounting Peliback TACACS+ LDAP Local Net Users MAC Fittering Disabled Clients User Login Policies AP Policies	Server Index (Priority) Server IP Address Shared Secret Format Shared Secret Confirm Shared Secret Key Wrap Port Number	1 Image: Constraint of the second
► Local EAP	Server Status	Enabled
Priority Order	Support for RFC 3576	Enabled .
▶ Certificate	Server Timeout	2 seconds
Access Control Lists	Network User	Enable
 Wireless Protection Policies Web Auth 	Management IPSec	Enable
Advanced		

<u>ダイナミック インターフェイス (VLAN)の設定</u>

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。こ のドキュメントですでに説明したように、RADIUS サーバの Tunnel-Private-Group ID 属性で指定 された VLAN ID が WLC 内にも存在している必要があります。

この例では、user1 の Tunnel-Private-Group ID は RADIUS サーバ上で 10 (VLAN =10) に設定さ

れています。user1 の [User Setup] ウィンドウの <u>[IETF RADIUS Attributes]</u> セクションを参照し てください。

この例では、WLC でも同じダイナミック インターフェイス(VLAN=10)が設定されていること を確認できます。ダイナミック インターフェイスの設定は、コントローラの GUI の Controller > Interfaces ウィンドウで行います。

 cisco	MONITOR WLANS C	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	Saya Co COMMANDS	nfiguration Bing HELP	Logout Befresh
Controller	Interfaces > New						< Back	Apply
General Inventory Interfaces	Interface Name Vian VLAN Id 10	10						
Multicast Network Routes								
 Internal DHCP Server Mobility Management 								
Ports NTP								
CDP Advanced								

- 1. このウィンドウで **[Apply]**をクリックします。このダイナミック インターフェイス(この例 では VLAN 10)の [Edit] ウィンドウが開きます。
- 2. 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

cisco	MONITOR WLANS C	ONTROLLER WIRELESS	SECURITY	MANAGEMENT	Saye C COMMANDS	nifiguration Bing . HELP	togout Bef
Controller	Interfaces > Edit					< Back	Apply
General Inventory	Concert Information						
Interfaces	General Information						
Multicast	Interface Name	vian10					
Network Routes	MAC Address	00:0b:85:48:53:c0					
Internal DHCP Server Mobility Management	Configuration						
Ports	Guest Lan						
NTP	Quarantine						
CDP	Quarantine Vlan Id	0					
Advanced	Physical Information						
	Port Number	1		-			
	Backup Port	0					
	Active Port	0					
	Enable Dynamic AP Man	agement 🔲					
	Interface Address						
	VLAN Identifier	10		_			
	IP Address	172.18.1.10]				
	Netmask	255.255.0.0]				
	Gateway	172.18.1.30]				
	DHCP Information						
	Primary DHCP Server	172.16.1.30					
	Secondary DHCP Server						

注:このドキュメントではコントローラの内部DHCPサーバを使用するため、このウィンド ウのプライマリDHCPサーバフィールドはWLC自体の管理インターフェイスを指しています 。ワイヤレス クライアントに対する DHCP サーバとしては、外部 DHCP サーバ、ルータ、 または RADIUS サーバ自体を使用することもできます。その場合、プライマリ DHCP サー バのフィールドには、DHCP サーバとして使用するデバイスの IP アドレスを指定します。 詳細については、DHCP サーバのマニュアルを参照してください。

 [Apply] をクリックします。これで WLC にダイナミック インターフェイスが設定されます 。同様の方法で、WLC に複数のダイナミック インターフェイスを設定することもできます 。ただし、クライアントに割り当てる特定の VLAN の VLAN ID が RADIUS サーバ内にも存 在している必要があります。

<u>WLAN(SSID)の設定</u>

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] > [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 VLAN10 を使用しています。

cisco	MONITOR	WLANS		WIRELESS	SECURITY	MONAGEMENT	C <u>O</u> MMANDS	HELP	rollon Beren
WLANs	WLANs > I	New						< Back	Apply
WLANS WLANS	Туре		WLAN						
+ Advanced	Profile Nan	ne	VLAN	10					
	SSID		VLAN	10					
	ID		3	3					

3. [Apply] をクリックして WLAN SSID10 の [Edit] ウィンドウに移動します。

WLANs WLANs	General Security	QoS Advanced	
Advanced	Profile Name	VLAN10	
	Туре	WLAN	
	SSID	VLAN10	
	Status	P Enabled	
	Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)	
	Radio Policy	Al	
	Interface	management -	
	Broadcast SSID	P Enabled	

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT	Sage Configuration Bing Logout B C <u>O</u> MMANDS HELP
WLANs	WLANs > Edit	< Back Apply
WLANS WLANS	General Security QoS Advanced	
▶ Advanced	Layer 2 Layer 3 AAA Servers	
	Layer 2 Security ² 802.1X MAC Filtering	
	802.1X Parameters	
	802.11 Data Encryption Type Key Size	
	WEP 104 bits	

		J. J

通常、ワイヤレス LAN コントローラでは、WLAN に属する特定のユーザが特定の VLAN に 割り当てられるように、各 WLAN が特定の VLAN(SSID)にマッピングされます。通常、 このマッピングは [WLAN SSID] ウィンドウの [Interface Name] フィールドで行います。

cisco	MONITOR WLAN: CONTROLLER WIRELESS SECURIT	Y MANAGEMENT COMMANDS HELP					
LANs	WLANs > Edit <back apr<="" td=""></back>						
WLANS WLANS	General Security QoS Advanced						
Advanced	Layer 2 Layer 3 AAA Servers						
	Select AAA servers below to override use of default servers on this WLAN						
	Radius Servers	LDAP Servers					
	Authentication Servers Accounting Server	ers Server 1 None - Server 2 None -					
	Server 1 IP:172.16.1.1, Port:1812 • None •	Server 3 None -					
	Server 2 None None K						
	Server 3 None None None						
	Local EAP Authentication						
	Local EAP Authentication Enabled						
	Authentication priority order for web-auth user						
	(IRADIUS						

この例では、認証の成功後にワイヤレス クライアントを特定の VLAN に割り当てるタスク は RADIUS サーバによって処理されます。WLAN は WLC 上で特定のダイナミック インタ ーフェイスにマッピングされている必要はありません。WLC で WLAN がダイナミック イン ターフェイスにマッピングされている場合でも、RADIUS サーバはこのマッピングを無視し 、その WLAN からアクセスしているユーザを、RADIUS サーバでそのユーザの [Tunnel-Group-Private-ID] フィールドに指定されている VLAN に割り当てます。

- 4. WLC の設定を RADIUS サーバで無視するために、[Allow AAA Override] チェック ボックス をオンにします。
- 5. 設定されている WLAN(SSID)ごとにコントローラで Allow AAA Override を有効にします
 - o

cisco	MONITOR WLANS CONTROLLER WIRELESS SECU	Sage Configuration Eing Logout Be RITY MANAGEMENT C <u>O</u> MMANDS HELP
WLANS	WLANs > Edit	< Back Apply
WLANs	General Security QoS Advanced	
Advanced	Allow AAA Override	DHCP
	Coverage Hole Detection F Enabled Enable Session Timeout F 1800	DHCP Server 🗖 Override
	Aironet IE Rabled	DHCP Addr. Assignment Required Management Frame Protection (MFP)
	Diagnostic Channel Enabled	Infrastructure MFP 🔽 (Global MFP Disabled)
	P2P Blocking Action Disabled	MFP Client Protection & Optional -
	Client Exclusion 4 F Enabled 60	DTIM Period (in beacon intervals) (secs)
	HREAP	802.11a/n (1 - 255) 1
	H-REAP Local Switching 2 Enabled Learn Client IP Address 1 IZ Enabled	802.11b/g/n (1 - 255) 1 NAC
		State 🗖 Enabled

AAA Override を有効にしていて、クライアントの AAA とコントローラの WLAN の認証パ ラメータが競合する場合は、クライアント認証は AAA (RADIUS)サーバで実行されます。 この認証の一環として、オペレーティング システムにより、AAA サーバから返された VLAN にクライアントが移動されます。これはコントローラ インターフェイス設定で事前に 定義されています。たとえば、VLAN 2 に割り当てられた管理インターフェイスが企業 WLAN でメインとして使用されていて、AAA Override により VLAN 100 へのリダイレクト が返された場合は、VLAN 100 が割り当てられている物理ポートが使用できない場合でも、 オペレーティング システムにより、すべてのクライアント通信が VLAN 100 にリダイレク トされます。AAA Override を無効にすると、コントローラの認証パラメータ設定がすべて のクライアント認証においてデフォルトで使用され、コントローラ WLAN にクライアント 固有の認証パラメータがない場合は、AAA サーバのみによって認証が実行されます。

<u>Wireless Client Utility の設定</u>

このドキュメントでは、ユーザ プロファイルを設定するためのクライアント ユーティリティとし て ADU を使用します。さらに、この設定では認証プロトコルとして LEAP を使用します。この セクションで説明するとおりに ADU を設定してください。

新規のプロファイルを作成するには、ADU のメニューバーで [Profile Management] > [New] の順 に選択します。

例のクライアントは、SSID VLAN10の一部として設定されています。次の図は、クライアントに ユーザプロファイルを設定する方法を示しています。

Cisco Aironet Desktop Utility - Current Profile:	Default 🛛 💽
Current Status Profile Management Diagnostics	
Default LAP	<u>N</u> ew
Ext.Web	Modily
	Remove
	Activate
Details	
Network Type: Security Mode:	Import
Network Name 1 (SSID1):	Export
Network Name 2 (SSID2):	Scan.
Network Name 3 (SSID3):	
Auto Select Profiles	Order Profiles

Profile N	anagemer	nt		? 🛛
General	Security 4	Advance	a]	
~ Profil	e Settings			
	Profile	Name:	vlan10	
	Client	Name:	wcs	
Netw	ork Names		·····	
		SSID1:	vlan10	
		SSID2:		
		SSID3:		
	* * * *			
				Cancel

Security Onlines				
) WPA/WPA2/C	CKM WPA	/WPA2/CCKM EA	AP Type: LEAP	
802.1v		802.1× EA	P Type: LEAP	 ~
Pre-Shared Ke	(Static WEP)			
Configure		Allow Associa	ation to Mixed Cells	
	Group Policy Delay.	60 🛟 se	c	

<u>確認</u>

ADU で設定したユーザ プロファイルをアクティブにします。設定に基づいて、ユーザ名とパス ワードの入力を求められます。ADU に対して Windows ユーザ名とパスワードを認証に使用する ように指示することもできます。クライアントが認証を受けるためのオプションはいくつか用意 されています。これらのオプションは、作成したユーザ プロファイルの [Security] > [Configure] タブで設定できます。

上の例では、RADIUS サーバで指定されているとおりに、user1 は VLAN10 に割り当てられます。

この例では、クライアントの認証と RADIUS サーバによる VLAN への割り当てを実行するために 、クライアント側からの次のユーザ名とパスワードを使用します。

• ユーザ名 = user1

パスワード = user1

この例は、SSID VLAN10 がどのようにユーザ名とパスワードの入力を求められるかを示しています。この例では、ユーザ名とパスワードがすでに入力されています。

Current Status		
Default		New
Ext.Web		Modify
Vian10		Remove
ter Wireless N	etwork Password X	Activate
TELWOIK		Import
Jser Name :	user1	Export Scan
Jser Name : Password :	user1	Export Scan Order Profiles
Jser Name : Password : .og on to :	user1 •••••	Export Scan Order Profiles
Jser Name : Password : .og on to : Card Name :	user1 ••••• Cisco Aironet 802.11a/b/g Wireless Adapter	Export Scan Order Profiles

認証と確認に成功すると、成功のステータス メッセージが返されます。

次に、送信された RADIUS アトリビュートに従ってクライアントが適切な VLAN に割り当てられ たことを確認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. コントローラの GUI で、[Wireless] > [AP] の順に選択します。
- 2. [Access Points (APs)] ウィンドウの左隅にある [Clients] をクリックします。クライアントの 統計情報が表示されます。

cisco	MONITOR Y	MLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Eing 1	Logout	t Fet	esh
Monitor	Clients								Entrie	s 1 - 4	of 4	
Summary	Current Filter	,	None	Change Filte	r] (Show All)							
Access Points												
Statistics	Client MAC A	Addr /	AP Name		WLAN	Profile	Protocol	Status	Auth	Port	WGB	
♦ CDP	00:21:5c:09:0	08:dd	P1130		Unknow	wh.	802.11a	Probing	No	2	No	
Rogues	00:21:50:50:3	Sailf /	MP1130		VLAN1)	802.11g	Associated	Yes	2	No	
Clients												
Multicast												

3. このクライアントの IP アドレスや、このクライアントが割り当てられている VLAN などの 詳細を確認するには、[Details] をクリックします。この例では、クライアント user1 の詳細 が表示されています。

cisco	MONITOR WLANS CONT	ROLLER WIRELESS SECUR	ITY MANAGEMENT COMM	Saye Configuration <u>B</u> ing Logout <u>B</u> efre AANDS HELP
Monitor	Clients > Detail		< Back	Apply Link Test Remove
Access Points	Client Properties		AP Properties	
Statistics	MAC Address	00:21:50:50:3a:1f	AP Address	00:15:c7:ab:55:90
➤ CDP	IP Address	17.18.1.35	AP Name	AP1130
Rogues	Client Type	Regular	AP Type	802-11g
Clients	User Name	User1	WLAN Profile	VLAN10
Multicast	Port Number	2	Status	Associated
	Interface	vlan10	Association ID	1
	VLAN ID	10	802.11 Authentication	Open System
	CCX Version	CCXv4	Reason Code	0
	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	Implemented
	Mirror Mode	Disable -	PBCC	Not Implemented
	Management Frame Protection	No	Channel Agility	Not Implemented
	Convrite Information		Timeout	1800
			WEP State	WEP Disable
	Security Policy Completed	Yes		
	Policy Type	802.1X		
	Encryption Cipher	WEP (104 bits)		
	EAP Type	LEAP		
	NAC State	Access		

このウィンドウでは、RADIUS サーバに設定された RADIUS アトリビュートに従って、こ のクライアントが VLAN10 に割り当てられたかどうかを確認できます。注:ダイナミック VLAN割り当てがCisco Airespace VSA属性の設定に基づいている場合は、クライアントの詳 細ページでは、この例に従ってインターフェイス名がadminとして表示されます。 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。

 debug aaa events enable:このコマンドを使用すると、コントローラを介して RADIUS アト リビュートがクライアントに正常に転送されたことを確認できます。 デバッグ出力に次の部 分が含まれている場合は、RADIUS アトリビュートの転送に成功したことを意味しています

```
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[0]:
attribute 64, vendorId 0, valueLen 4
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[1]:
attribute 65, vendorId 0, valueLen 4
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[2]:
attribute 81, vendorId 0, valueLen 3
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[3]:
attribute 79, vendorId 0, valueLen 32
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Received EAP Attribute
(code=2, length=32,id=0) for mobile 00:40:96:ac:e6:57
Fri Jan 20 02:25:08 2006: 00000000: 02 00 00 20 11 01 00 18
4a 27 65 69 6d e4 05 f5
.....J'eim...00000010: d0 98 0c cb 1a 0c 8a 3c
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[4]:
attribute 1, vendorId 9, valueLen 16
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[5]:
attribute 25, vendorId 0, valueLen 28
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[6]:
attribute 80, vendorId 0, valueLen 16
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-Type 16777229
should be 13 for STA 00:40:96:ac:e6:57
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-Medium-Type 16777222
```

should be 6 for STA 00:40:96:ac:e6:57
Fri Jan 20 02:30:00 2006: 00:40:96:ac:e6:57 Station 00:40:96:ac:e6:57
setting dot1x reauth timeout = 1800

• 次のコマンドも使用できます。debug dot1x aaa enabledebug aaa packets enable

<u>トラブルシュート</u>

現在、この設定に関する特定のトラブルシューティング情報はありません。

注:ダイナミックVLAN割り当ては、WLCからのWeb認証では機能しません。

関連情報

- <u>RADIUS サーバとの EAP 認証</u>
- <u>Cisco LEAP</u>
- <u>Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 4.0</u>
- ・<u>テクニカル サポートとドキュメント Cisco Systems</u>