# Cisco Unified Wireless Network での Wi-Fi Protected Access (WPA)の設定例

### 内容

<u>概要</u> <u>前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>表記法</u> <u>WPA および WPA2 のサポート</u> <u>ネットワークのセットアップ</u> <u>WPA2 Enterprise モード向けのデバイスの設定</u> <u>MPA2 Enterprise モード向けの WLAN の設定</u> <u>WPA2 Enterprise 動作モード向けの WLAN の設定</u> <u>WPA2 Enterprise モード認証向けの RADIUS サーバの設定 (EAP-FAST)</u> <u>WPA2 Enterprise 動作モード向けのワイヤレス クライアントの設定</u> <u>WPA2 Personal モード向けのデバイスの設定</u> <u>トラブルシュート</u> 関連情報

### 概要

このドキュメントでは、Cisco Unified Wireless Network で Wi-Fi Protected Access(WPA)を設 定する方法について説明します。

# 前提条件

#### <u>要件</u>

この設定を開始する前に、次の項目に関する基本的な知識を必ず取得しておきます。

- WPA
- ワイヤレス LAN(WLAN)セキュリティ ソリューション注: Cisco WLANセキュリティソリ ューションの詳細については、『CiscoワイヤレスLANセキュリティの概要』を参照してくだ さい。

### <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。

• Cisco 1000 シリーズ Lightweight アクセス ポイント(LAP)

- •ファームウェア 4.2.61.0 が稼働する Cisco 4404 ワイヤレス LAN コントローラ(WLC)
- •ファームウェア 4.1 が稼働する Cisco 802.11a/b/g クライアント アダプタ
- •ファームウェア 4.1 が稼働する Aironet Desktop Utility (ADU)
- Cisco Secure ACS サーバ バージョン 4.1

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。

#### <u>表記法</u>

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。

### <u>WPA および WPA2 のサポート</u>

Cisco Unified Wireless Network は、Wi-Fi Alliance 認定の WPA および WPA2 をサポートしてい ます。WPA は 2003 年に Wi-Fi Alliance によって導入されました。WPA2 は 2004 年に Wi-Fi Alliance によって導入されました。WPA2 の Wi-Fi 認定を受けたすべての製品は、WPA の Wi-Fi 認定を受けた製品と相互運用できることが求められています。

WPA および WPA2 は、データが公開されないこと、およびネットワークへのアクセスが認可ユ ーザに限定されるということを、エンド ユーザおよびネットワーク管理者に対して高いレベルで 保証します。どちらの規格にも Personal 動作モードと Enterprise 動作モードがあり、これら 2 つの市場セグメント特有のニーズに応えます。これらは Enterprise モードでは、認証に IEEE 802.1X および EAP を使用します。これらは Personal モードでは、認証に事前共有キー (PSK)を使用します。Personal モードではユーザ認証に PSK を使用するため、ビジネスまた は官公庁への導入の場合、Cisco では Personal モードを推奨しません。企業環境では PSK は安 全ではありません。

WPA は、従来の IEEE 802.11 によるセキュリティ実装における WEP の既知のすべての脆弱性に 対処し、企業環境とスモール オフィス、ホーム オフィス(SOHO)環境の両方において、WLAN に即座に適用できるセキュリティ ソリューションです。WPA では暗号化に TKIP を使用します 。

WPA2 は次世代の Wi-Fi セキュリティ機能です。これは批准された IEEE 802.11i 標準を Wi-Fi Alliance と相互運用できるように実装したものです。WPA2 では、Counter Mode with Cipher Block Chaining Message Authentication Code Protocol(CCMP)を使用して、国立標準技術研究 所(NIST)が推奨する AES の暗号化アルゴリズムを実装しています。WPA2 によって、官公庁 の FIPS 140-2 への準拠が促進されます。

#### WPA モードと WPA2 モードのタイプの比較

	WPA	WPA2
	<ul> <li>認証</li> </ul>	<ul> <li>認証</li> </ul>
	: IEEE	: IEEE
Enterprise モード(ビジ	802.1X/E	802.1X/EA
ネス、官公庁、教育)	AP	Р
	• 暗号化	• 暗号化
	: TKIP/	: AES-

	MIC	CCMP
	<ul> <li>認証</li> </ul>	<ul> <li>認証</li> </ul>
Personal モード	: PSK	: PSK
(SOHO、家庭または個	● 暗号化	• 暗号化
人)	: TKIP/	: AES-
	MIC	CCMP

Enterprise 動作モードでは、WPA も WPA2 も両方とも認証に 802.1X/EAP を使用します。 802.1X により、WLAN でクライアントと認証サーバの間の高性能な相互認証が利用できます。 また、802.1X によってユーザ単位かつセッション単位の動的な暗号キーが提供されるため、静的 な暗号キーに伴う管理上の負担やセキュリティ上の問題がなくなります。

802.1X の場合、認証に使用されるログオン パスワードなどのクレデンシャルが平文で、つまり 暗号化されずにワイヤレス メディア経由で送信されることはありません。802.1X の認証タイプ はワイヤレス LAN に対して高性能な認証方式を提供しますが、標準的な 802.11 WEP 暗号化は ネットワーク攻撃に対して脆弱であるため、暗号化のためには 802.1X 以外に TKIP または AES が必要です。

いくつかの 802.1X 認証タイプが存在し、これらはそれぞれ認証の方式が異なりますが、クライ アントとアクセス ポイントの間の通信については同じフレームワークおよび EAP に依存してい ます。Cisco Aironet 製品では、他のどの WLAN 製品よりも多くの種類の 802.1X EAP 認証をサ ポートしています。サポートされるタイプには、次のものがあります。

- <u>Cisco LEAP</u>
- EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)
- EAP-Transport Layer Security (EAP-TLS)
- Protected Extensible Authentication Protocol ( PEAP )
- EAP-Tunneled TLS ( EAP-TTLS )
- EAP-Subscriber Identity Module (EAP-SIM)

802.1X 認証のもう 1 つのメリットは、WLAN ユーザ グループの集中管理で、これにはポリシー ベースのキー ローテーション、動的キー割り当て、動的 VLAN 割り当て、SSID 制限などがあり ます。これらの機能では、暗号キーがローテーションされます。

Personal 動作モードでは、認証に事前共有キー(パスワード)が使用されます。Personal モード では、アクセス ポイントおよびクライアント デバイスのみが必要ですが、Enterprise モードでは 通常、RADIUS サーバなどの認証サーバがネットワーク上に必要になります。

このドキュメントでは、Cisco Unified Wireless Network 上に WPA2(Enterprise モード)および WPA2-PSK(Personal モード)を設定する例を示します。

#### <u>ネットワークのセットアップ</u>

この構成では、Cisco 4404 WLC と Cisco 1000 Series LAP がレイヤ2スイッチを介して接続さ れています。外部 RADIUS サーバ(Cisco Secure ACS)も同じスイッチに接続します。すべて のデバイスは同じサブネット内にあります。アクセス ポイント(LAP)はコントローラに最初か ら登録されています。ワイヤレス LAN は、1 つを WPA2 Enterprise モード用に、もう 1 つを WPA2 Personal モード用に2つ作成する必要があります。

WPA2-EnterpriseモードのWLAN(SSID:WPA2-Enterprise)では、ワイヤレスクライアントの認証 にEAP-FASTを使用し、暗号化にAESを使用します。ワイヤレス クライアントの認証用の外部 RADIUS サーバとして、Cisco Secure ACS サーバを使用します。

WPA2-PersonalモードWLAN(SSID:WPA2-PSK)は、事前共有キー「abcdefghijk」を使用した認証 にWPA2-PSKを使用します。

この構成に合わせてデバイスを設定する必要があります。



# <u>WPA2 Enterprise モード向けのデバイスの設定</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。

WPA2 Enterprise 動作モード用にデバイスを設定するには、次の手順を実行します。

- 1. <u>外部 RADIUS サーバによる RADIUS 認証用の WLC の設定</u>
- 2. WPA2 Enterprise モード認証向けの WLAN の設定(EAP-FAST)
- 3. WPA2 Enterprise モード向けのワイヤレス クライアントの設定

#### <u>外部 RADIUS サーバによる RADIUS 認証用の WLC の設定</u>

ユーザ クレデンシャルを外部 RADIUS サーバに転送するには、WLC を設定する必要があります 。そうすると、外部 RADIUS サーバは、EAP-FAST を使用してユーザのクレデンシャルを検証し 、ワイヤレス クライアントにアクセス権を付与します。

外部 RADIUS サーバ用に WLC を設定するには、次の手順を実行します。

- 1. コントローラの GUI から [Security]、[RADIUS]、[Authentication] を選択して、[RADIUS Authentication Servers] ページを表示します。次に、[New] をクリックして、RADIUS サー バを定義します。
- 2. [RADIUS Authentication Servers] > [New] ページで RADIUS サーバのパラメータを定義しま す。次のパラメータがあります。RADIUS サーバの IP アドレス共有秘密ポート番号サーバ ステータスこのドキュメントでは、10.77.244.196 という IP アドレスを持つ ACS サーバを 使用しています。

		Sage Configuration   Ping   Logout   Befresh
CISCO	MONITOR WLANS CONT	ROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security	RADIUS Authentication	Servers > New <back apply<="" th=""></back>
- AAA General	Server Index (Priority)	1 .
▼ RADIUS Authentication	Server IPAddress	10.77.244.196
Accounting     TACACS+     LDAP	Shared Secret Format	ASCII -
Local Net Users MAC Filtering	Shared Secret	****
Disabled Clients User Login Policies AP Policies	Confirm Shared Secret	****
▶ Local EAP	Key Wrap	(Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Priority Order	Dout Number	1012
▶ Access Control Lists	Port Number	1012
Wireless Protection     Policies	Server Status	Enabled *
Web Auth	Support for RFC 3576	Enabled 💌
Advanced	Server Timeout	2 seconds
	Network User	☑ Enable
	Management	Enable
	IPSec	Enable

3. [Apply] をクリックします。

<u>WPA2 Enterprise 動作モード向けの WLAN の設定</u>

次に、クライアントがワイヤレス ネットワークに接続するために使用する WLAN を設定します 。WPA2 Enterprise モード用の WLAN SSID は、WPA2-Enterprise です。この例では、この WLAN を管理インターフェイスに割り当てます。

WLAN と関連するパラメータを設定するために、次の手順を実行します。

- 1. コントローラの GUI で [WLANs] をクリックして、[WLANs] ページを表示します。このペー ジには、コントローラに存在する WLAN の一覧が表示されます。
- 2. [New] をクリックして新規の WLAN を作成します。
- 3. [WLANs] > [New] ページで WLAN SSID 名とプロファイル名を入力します。次に、[Apply] をクリックします。この例では、SSID として **WPA2-Enterprise** を使用しています。

							Sa <u>v</u> e Co	onfiguration   Ping	Logout Befr
cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECORITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs >	New						< Back	Apply
WLANS	Туре		WLAN						
▶ Advanced	Profile Na	me	WPA2-Ent	erprise					
	WLAN SSI	D	WPA2-Ent	erprise					

- 4. 新しい WLAN を作成すると、新しい WLAN に対する [WLAN] > [Edit] ページが表示されま す。このページでは、その WLAN に固有のさまざまなパラメータを定義できます。これに は、全般ポリシー、セキュリティ ポリシー、QOS ポリシー、および高度なパラメータが含 まれます。
- 5. WLAN を有効にするには、[General Policies] で [Status] チェック ボックスをオンにします

č							
					Sage Co	nfiguration Eng	Logout Refresh
CISCO	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs > Edit					< Back	Apply
	General Securit	0oS Advanced					
WLANS WLANS	Seller ar Securit	y gos noranced					
k Advanced	Profile Name	WPA2-Enterprise					
, Nordinced	Туре	WLAN					
	SSID	WPA2-Enterprise					
	Status	Enabled					
	Security Policies	[WPA2][Auth(802.1X]	1				
	accord reaction	(Modifications done under	r security tab wi	il appear after ap	plying the chang	es.)	
	Radio Policy	Al					
	Interface	management 💌					
	Broadcast SSID	Enabled					
	East Nates						
	I CKIR is not supported	d hu they model dite					
	2 Web Policy cannot be	used in combination with IPse	NC				
	4 When client exclusion	ng is not supported with IPsec, n is enabled, a Timeout Value o	of zero means in	nfinity (will requir	e administrative	override to reset exclu	vded clients)
	S Client MFP is not acti	ve unless WPA2 is configured					

- 6. AP にビーコン フレームで SSID をブロードキャストさせる場合は、[Broadcast SSID] にチェックボックスをオンにします。
- 7. [Security] タブをクリックします。[Layer 2 Security] で、[WPA+WPA2] を選択します。これ により、WLAN に対して WPA 認証が有効になります。

ahaha	Sage Configuration   Eing   Logout   Befresh
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANS	WLANs > Edit < Back Apply General Security QoS Advanced
Advanced	Layer 2 Layer 3 AAA Servers Layer 2 Security WPA+WPA2  MAC Filtering Static WEP Parameters B02.11 Data Encryption Current Key: 104 bits WEP Static Key (Key Index = 0)  Type Key Size Key Index Encryption Key Key Format WEP Port set In International ASCILIENT
	Allow Shared Key Authentication Enabled CKIP Parameters 1 802.11 Data Encryption Current Key: 0 bits CKIP Key (Key Index= 0) Key Size Key Index Encryption Key Key Format
	Implement     ASCII      ASSCII      ASCII      AS

8. [WPA+WPA2 Parameters] を変更するために、ページを下にスクロールします。この例では 、[WPA2 Policy] および [AES] 暗号化が選択されています。

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANS WLANS WLANS Advanced	WLANS > Edit       < Back

- 9. [Auth Key Mgmt] で [802.1x] を選択します。これで、802.1x/EAP 認証と AES 暗号化を使用 する WPA2 が WLAN に対して有効になります。
- 10. [AAA Servers] タブを選択します。[Authentication Servers] から、適切なサーバ IP アドレ スを選択します。この例では、10.77.244.196 が RADIUS サーバとして使用されます。

		and the second secon	Save Configuration   Eing   Logout   Befresh
cisco	MONITOR WLANS CONTROLLER WIRELESS	SECURITY MANAGEMENT COM	IMANDS HELP
WLANS WLANS WLANS Advanced	WLANS > Edit         General       Security       QoS       Advanced         Layer 2       Layer 3       AAA Servers         Select AAA servers below to override use of d       Radius Servers         Authentication Servers       Acco         Server       Authentication Servers       Acco         Server       IP:10.77.244.196, Port:1812       None         Server       None       None         Server       None       None         Server       None       None         Local EAP Authentication       Enabled         Local EAP Authentication       Enabled         Foot Notes       2 Web Policy cannot be used in combination with IPsec, 4 When olderd evaluation is enabled, a Timeout Value of 5 Cheat MPP is not active unless WPA2 is configured	efault servers on this WLAN LDAP Servers unting Servers Server 1 Non abled Server 2 Non a  Server 3 Non a a a a a a a a a a a a a a a a a a a	e  e  e  e  e  e  e  e  e  e  e  e  e  e

11. [Apply] をクリックします。**注:**これは、EAP認証用にコントローラで設定する必要がある 唯一のEAP設定です。EAP-FAST に固有なその他すべての設定は、RADIUS サーバおよび 認証が必要なクライアントで行う必要があります。

<u>WPA2 Enterprise モード認証向けの RADIUS サーバの設定(EAP-FAST)</u>

この例では、外部 RADIUS サーバとして Cisco Secure ACS サーバを使用しています。RADIUS サーバの EAP-FAST 認証を設定するには、次の手順を実行します。

- 1. <u>クライアント認証用のユーザ データベースの作成</u>
- 2. <u>AAA クライアントとしての WLC の RADIUS サーバへの追加</u>
- 3. <u>匿名インバンド PAC プロビジョニングによる RADIUS サーバへの EAP-FAST 認証の設定</u> 注: EAP-FASTは、匿名インバンドPACプロビジョニングまたは認証済みインバンドPACプ ロビジョニングのいずれかで設定できます。この例では匿名インバンド PAC プロビジョニ ングを使用します。EAP-FAST を匿名インバンド PAC プロビジョニングおよび認証済みイ ンバンド PAC プロビジョニングで設定することについての詳細な情報および設定例につい ては『ワイヤレス LAN コントローラおよび外部 RADIUS サーバを使用する EAP-FAST 認 証の設定例』を参照してください。

EAP-FAST クライアント認証用のユーザ データベースの作成

ACS で EAP-FAST クライアント用のユーザ データベースを作成するには、次の手順を実行します。この例では、EAP-FAST クライアントのユーザ名およびパスワードをそれぞれ User1、 User1 に設定します。

1. ナビゲーション バーの ACS GUI から、[User Setup] を選択します。新しいワイヤレス ユー ザを作成し、[Add/Edit] をクリックして、このユーザの編集ページに移動します。



2. [User Setup] の [Edit] ページで、この例に示すように、[Real Name]、[Description]、 [Password] を設定します。このドキュメントでは、[Password Authentication] オプションで [ACS Internal Database] を使用しています。

ress a http://127.0	0.0.1:1065/	
Cisco Systems	User Setun	······
de de		
	Edit	Help
User Setup Group Setup	User: User1 (New User)	Account Disabled     Deleting a Username     Supplementary User Info
Shared Profile Components	Account Disabled	Passwerd Arthentickten     Grang to which the user is assigned     Callback
Network Configuration	Supplementary User Info 🤶	Cleart IP Address Assignment     Advanced Settings     Network Access Restrictions
System Configuration	Description	Han Seation     Usede Quetas     Account Disable
Administration Centrel		Advanced TACACS+ Settings     TACACS+ Control     TACACS+ Enable Deserved
External User	User Setup ?	TACACS - Outboard Parameted     TACACS - Shell Command Authoritation
Porture Validation	Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not chacked.)	Command Authentication for Network Device Management Applications     TACACS - Unknown Services     ILTT RADIUS Attributes     RADIUS Yeader-Specific Attributes
Online Documentation	Password •••••	Account Disabled Status Select the Account Disabled check box to disable this account: clear
	Password	the check box to enable the account.
	Password	[Back to Tep]
	Confirm Password Submit Cancel	Deleting a Username The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click Delete. When asked to

- 3. [Password Authentication] ドロップダウン ボックスから [ACS Internal Database] を選択し ます。
- 4. その他の必須パラメータをすべて設定して [Submit] をクリックします。

#### AAA クライアントとしての WLC の RADIUS サーバへの追加

ACS サーバでコントローラを AAA クライアントとして定義するには、次の手順を実行します。

- 1. ACS の GUI で [Network Configuration] をクリックします。[Network Configuration] ページ の [Add AAA client] セクションで、[Add Entry] をクリックして、AAA クライアントとして WLC を RADIUS サーバに追加します。
- 2. [AAA Client] ページで、WLC の名前、IP アドレス、共有秘密、および認証方式(RADIUS または Cisco Airespace)を定義します。ACS 以外の他の認証サーバについては、メーカー のマニュアルを参照してください。

Cisco Systems	Network Configuration	X
alls alls	Ph	Ti Holo
User Setup Setup Setup Setup Setup Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration	AAA Client Hostname WLC AAA Client IP Address 10.77.244.204 AAA Client IP Address Cisco Shared Secret Cisco RADIUS Key Wrap Key Encryption Key Message Authenticator Code Key Key Input Format C ASCII @ Hexadecimal	AAA Cleant Hostname     Anthenticate Units     Sonds Connect TACAS:- AAA Cleant     Sonds Connect TACAS:- AAA Cleant     Les Undats.'Watchdes Packets from this     AAA Cleant     Can RADIUS Transeling Packets from this     AAA Cleant     Match Framed IP-Address with user IP     address for accounting packets from this     AAA Cleant     Match Framed IP-Address with user IP     address for accounting packets from this     AAA Cleant     Match Framed IP-Address with user IP     address for accounting packets from this     AAA Cleant     The AAA Cleant     The AAA Cleant
Contine Documentation	Autoenticate Using [RADIUS (Cisco Airespace)      Single Connect TACACS+ AAA Client (Record stop in accounting on failure)      Lon Undate/Watchdon Packets from this AAA Client	AAA Client IP Address The AAA Client IP Address is
	Log RADIUS Tunneling Packets from this AAA Client	the IP address assigned to the AAA client.
	Replace RADIUS Port info with Username from this AAA Client     Match Framed-IP-Address with user IP address for accounting packets from	If you want to designate more than one AAA client with a single AAA client entry in ACS, you can specify the IP address for each

**注**:WLCとACSサーバで設定する共有秘密キーは一致している必要があります。共有秘密 では、大文字と小文字が区別されます。

3. [Submit+Apply] をクリックします。

#### <u>匿名インバンド PAC プロビジョニングによる RADIUS サーバへの EAP-FAST 認証の設定</u>

#### 匿名インバンド プロビジョニング

これは、2 つのインバンド プロビジョニング方式の 1 つです。これにより、ACS は、クライアン トに新しい PAC を提供するために、エンドユーザ クライアントとセキュア接続を確立します。 このオプションでは、エンドユーザ クライアントと ACS の間で匿名の TLS ハンドシェイクが可 能になります。

この方式は、ピアが ACS サーバを認証する前に、Authenticated Diffie-HellmanKey Agreement Protocol (ADHP) トンネル内で機能します。

ACS では、ユーザの EAP-MS-CHAPv2 認証が必要です。ユーザ認証が成功すると、ACS はエンドユーザ クライアントとの Diffie-Hellman トンネルを確立します。ACS はユーザ用の PAC を生成し、この ACS に関する情報とともにこのトンネル内でエンドユーザ クライアントに送信します。このプロビジョニング方式は、認証方式としてフェーズ 0 で EAP-MSCHAPv2、フェーズ 2 で EAP-GTC を使用します。

非認証サーバがプロビジョニングされるため、プレーン テキスト パスワードは使用できません。 そのため、トンネル内では MS-CHAP クレデンシャルだけを使用できます。MS-CHAPv2 は、そ の後の認証セッションのためにピアの ID をプローブし、PAC を受け取るときに使用されます (EAP-MS-CHAP は内部方式としてのみ使用されます)。 RADIUS サーバ内で匿名インバンド プロビジョニング用に EAP-FAST 認証を設定するには、次の手順を実行します。

1. RADIUS サーバの GUI で [System Configuration] をクリックします。[System Configuration] ページで、[Global Authentication Setup] を選択します。

Ele Edit Yew I	Fgvorites Iools Help	Links	* 00
Address Address http://12	27.0.0.1:1065/		60
Crace Systems	System Configuration		2
User Setup Setup Salared Profile Components Surved Profile Configuration Surtwork Configuration Surtwork Configuration Configuration Configuration Configuration	Select     Hep       Service Control     - Service Control       Logging     Date Format Control       Date Format Control     - Lessins       Local Password Management     - AdS Internal Database Replication       ACS Internal Database Replication     - AdS Internal Database Replication       ACS Restore     - AdS Internal Configuration       ACS Restore     - DPade Address Receivery       ACS Service Management     - AdS Internal Configuration       ACS Service Management     - AdS Internal Configuration       ACS Service Management     - AdS Internal Configuration       ACS Certificate Setup     - Gibbal Authentication Setup	tion h talista	
Porfuse Validation Natwork Access Profiles Reports and Activity Documentation	Select to open the page from w Ciscos ACS pervices. Iback to Tupi Legging Select to configure various Cis the type of information that is i Iback to Tupi Date Fermat Control Select to configure the date for day/month/year, for CSV files [Back to Tup]	chich you can stop or restant sco Secure ACS reports and customice legged. rmat, either month/day/year or and Service Logs and in the GUI.	

2. [Global Authentication setup] ページで [EAP-FAST Configuration] をクリックし、EAP-FAST 設定のページに進みます。

ElscoSecure AES - M	ficrosoft Internet Explorer	
ddress 🙆 http://127.0	contes [sous Bep 0.0.1:1065/	unes ** 📲
Crace Systems	System Configuration	
Uter Setup Croup Dared Profile Components Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration	EAP Configuration  PEAP  Allow EAP-MSCHAPv2 Allow EAP-GTC Allow Posture Validation  Allow EAP-TLS Select one or more of the following options:  Certificate SAN comparison  Certificate CN comparison  EAP-TLS session timeout (minutes):  120	Use this page to specify settings for various authentication protocols. • CAP Configuration • CAP-Configuration • CAP-CAST • CAP-TAST • CAP-TAST
Velidation Velidation Reports and Activity Online Documentation	PEAP session timeout (minutes): 120 Enable Fast Reconnect: EAP-FAST EAP-FAST EAP-TLS F Allow EAP-TLS Select one or more of the following options: F Certificate SAN comparison Submit Submit + Restart Cancel	[back to Top]         PEAP         PEAP is the outer layer protocol for the secure tunnel.         Andrew AEAP is a cartificate-based authentication protocol. AEAP authentication on accurate after you have completed the required steps so the ACS Certificate Setup page.         • Allow EAP-HSENAPu2 - Use to anable EAP-MSCHAPu2 within MS PEAP authentication. Enable this protocol for any repository that supports MS-CHAPu2, such as Microsoft AD, and the ACS Internal Database.
2) 2 Start   🕑 🦽	CiscoSecure ACS - Mic	Internet     7:58 PM

3. [EAP-FAST Settings] ページから、[Allow EAP-FAST] チェックボックスをオンにして、 RADIUS サーバで EAP-FAST を有効にします。

CiscoSecure ACS - M	Scrosoft Internet Explorer			>
address bate-//1.22 /	Nonzes Toos Geb		uns "	
educes in under the				
Cisco Systems	System Configuration		12	<u>.</u>
حظائم حظائم	EAP-FAST Configuration	Help		
A I Uper				
Lag   Setup		EAP-I	FAST Configuration Page	
Group Setup	EAP-FAST Settings	<b>2</b> Use 6	his page to configure EAP-FAST authentication settings.	
	EAP-FAST			
Components	R Allow EAP-FAST	•	P-FAST Settings	-
Start National	Active master key TTL 1 months		ent initial message	
Configuration		• •	low anonymous in-band PAC previsioning	
Pind System	Retired master key TTL 3 months 🖻		few authenticated in-band PAC provisioning	
Configuration	Tunnel PAC TTL 1 weeks 💌		low machine authentication	
www.listerface	er a fabili	- 1	loved inner methods	
Configuration	Client initial message: tacwebacs	• •	rtificate Comparison	
Administration	Authority ID Info: tacwebacs		IP-TLS session timeout (minutes)	
Control	R Allow anonymous in-band PAC provisioning	• •	tual EAP-FAST server status	
Databases	Allow authenticated in-band PAC provisioning	EAD-I	EAST Settings	
Partice	E accept client on authenticated provisioning			
Validation	Dequire client on the interactive provisioning	Allow	EAP-FAST-To enable EAP-FAST authentication, select this check	
Network Access	C Require client certificate for provisioning	box.		
B Profiler	LI Allow Machine Authentication	Activ	e Master Key TTL-Enter a value for the amount of time that a master	
C Reports and	Machine PAC TTL 1 weeks	key is time t	s used to generate new Protected Access Credentials (PACs). When the to live (TTL) defined for the Master Key expires, the master key is	
- Di Antonio	Allow Stateless session resume	consi	dered retired and a new master key is generated.	
Documentation	Authorization PAC TTL 1 hours	• Retire	ed master key TIL-Enter a value for the amount of time that PACs	
	Allowed inner methods	gener	uted using a retired master key are acceptable for EAP-FAST	
	EAP-GTC	based	d on a retired master key, ACS sends a new PAC to the end-user client.	
	EAP-MSCHAPv2		<b>J DAT TR</b> - Farme a value for the amount of time that a DAC is used	
	DEAD-TIS	befor	e it expires and must be replaced. If the master key used to generate	
	L/EAP-ILD	the To autor	unnel PAC has not expired, new PAC creation and assignment is natic. If the master key used to generate the Tunnel PAC expired.	
	Submit Submit + Restart Cancel	autor	natic or manual provisioning must be used to provide the end-user with a new PAC.	
3)			Internet	
🐮 Start 🔂 🥭	CiscoSecure ACS - Mic		🝠 7:58 PM	1

- 4. アクティブおよびリタイア マスター キーの TTL(存続可能時間)の値を目的に合わせて設定するか、この例で示すようにデフォルト値に設定します。アクティブおよびリタイア マスター キーについては、「マスター キー」を参照してください。また、詳細については、「マスター キーおよび PAC TTLs」を参照してください。[Authority ID Info] フィールドは、この ACS サーバのテキスト ID を表し、認証先の ACS サーバをエンド ユーザが判別するために使用できます。このフィールドの入力は必須です。[Client initial display message] フィールドは、EAP-FAST クライアントを使用して認証するユーザに送信するメッセージを指定します。最大長は 40 文字です。ユーザに初期メッセージが示されるのは、エンドユーザ クライアントがその表示をサポートしている場合だけです。
- 5. ACS で匿名インバンド PAC プロビジョニングを実行する場合、[Allow anonymous in-band PAC provisioning] チェックボックスをオンにします。
- [Allowed inner methods]: このオプションにより、EAP-FAST TLS トンネル内で実行できる 内部 EAP 方式が決まります。 匿名インバンド プロビジョニングを実行する場合は、下位互 換性を確保するために EAP-GTC と EAP-MS-CHAP を有効にする必要があります。 [Allow anonymous in-band PAC provisioning] を選択する場合は、EAP-MS-CHAP(フェーズ0)お よび EAP-GTC(フェーズ2)を選択する必要があります。

#### WPA2 Enterprise 動作モード向けのワイヤレス クライアントの設定

次の手順では、WPA2 Enterprise 動作モード用にワイヤレス クライアントを設定します。

WPA2 Enterprise モード用にワイヤレス クライアントを設定するには、次の手順を実行します。

1. [Aironet Desktop Utility] ウィンドウで、[Profile Management] > [New] をクリックして、 WPA2-Enterprise WLAN ユーザのプロファイルを作成します。すでに説明したように、この ドキュメントでは、ワイヤレス クライアントの WLAN/SSID 名として **WPA2-Enterprise** を 使用します。

2. [Profile Management] ウィンドウの [General] タブをクリックし、この例に示すように、プロファイル名、クライアント名、および SSID 名を設定します。次に、[OK] をクリックします。

rofile Management		? 🔈
General Security Advance	be	
Profile Settings		
Profile Name:	WPA2-Enterprise	
Client Name:	Wireless-Client1	
Network Names		
SSID1:	WPA2-Enterprise	
SSID2:		
SSID3:		
<u>.</u>		
	ОК	Cancel

3. [Security] タブをクリックし、[WPA/WPA2/CCKM] を選択して WPA2 動作モードを有効に します。[WPA/WPA2/CCKM EAP Type] で、[EAP-FAST] を選択します。[Configure] をクリ ックして、EAP-FAST を設定します。

Profile Management		? 🗙
General Security Advanced		
- Set Security Options		
⊙ WPA/WPA2/CCKM	WPA/WPA2/CCKM EAP Type: EAP-FAST	
○ WPA/WPA2 Passphrase		
○ 802.1x	802.1x EAP Type: LEAP	
O Pre-Shared Key (Static WEP)		
◯ None		
Configure	Allow Association to Mixed Cells	
	Limit Time for Finding Domain Controller To: 0 0 sec	
Group Policy Delay:	60 🗢 sec	
	ОК	ancel

4. [Configure EAP-FAST] ウィンドウから、[Allow Automatic PAC Provisioning] チェック ボッ クスをオンにします。匿名 PAC プロビジョニングを設定する場合、EAP-MS-CHAP は、フ ェーズ 0 の内部方式だけで使用されます。

Configure EAP-FAST	? 🔀
EAP-FAST Authentication Method	
MSCHAPv2 User Name and Password	Configure
Protected Access Credentials (PAC)	
Select One or More PAC Authorities	
	Manage
	>
Use Any PAC Belonging to the Same Group	
Allow Automatic BAC Provisioning	
Use Machine Information for Domain Logon	
	1
No Network Connection Unless User Is Logged In	
	OK Cancel

- 5. [EAP-FAST Authentication Method] ドロップダウン ボックスから、認証方式として [MSCHAPv2 User Name and Password] を選択します。[Configure] をクリックします。
- 6. [Configure MSCHAPv2 User Name and Password] ウィンドウから、適切なユーザ名とパス ワード設定を選択します。この例では、[Automatically Prompt for User Name and Password] を選択しています。

:Any>			~
Jser Name and Password S	ettings		
Use Temporary Use	Name and Password		
O Use Windows I	Jser Name and Passw	ord	
	rompt for User Name a	nd Password	
Manually Promp	ot for User Name and F	assword	
O Use Saved User Nar	ne and Password		
User Name:	Administrator		
Provinced			
r-asswurd.	L		
Confirm Password:			
Domain:			

- しユーザ名およひハスワードを ACS に登録する必要があります。すでに説明したように、 この例ではユーザ名およびパスワードとしてそれぞれ User1、User1 を使用します。また、 これは匿名インバンド プロビジョニングであることに注意してください。そのため、クラ イアントは、サーバ証明書を確認できません。[Validate Server Identity] チェックボックスが オフになっていることを確認します。
- 7. [OK] をクリックします。

#### <u>WPA2 Enterprise 動作モードの確認</u>

WPA2 Enterprise 動作モード設定が正しく機能するかどうかを確認するには、次の手順を実行します。

- 1. [Aironet Desktop Utility] ウィンドウで、[WPA2-Enterprise] プロファイルを選択して [Activate] をクリックし、ワイヤレス クライアント プロファイルをアクティブ化します。
- 2. MS-CHAP ver2 認証を有効にしている場合、ユーザ名およびパスワードを求めるプロンプト

がクライアントに表示されます。

Enter Wireless N	etwork Password	×
Please enter your E/ network	AP-FAST username and password to log on to the wireless	
User Name :	User1	
Password :	•••••	]
Log on to :		
Card Name :	Cisco Aironet 802.11a/b/g Wireless Adapter	
Profile Name :	WPA-Enterprise	
	OK Cancel	

3. ユーザの EAP-FAST 処理中、RADIUS サーバから PAC を要求するように、クライアントに より求められます。[YES] をクリックすると、PAC プロビジョニングが開始します。

EAP-FAST Authenti	ation	×
You do not have a vali automatic provisioning?	PAC from the authentication server. Do y	ou want to proceed and request
	Yes No	) 

4. フェーズ 0 で PAC プロビジョニングに成功した後、フェーズ 1 および 2 が実行され、認証 手順が正常に実行されます。認証に成功すると、ワイヤレス クライアントは WLAN WPA2-Enterprise に関連付けられます。次にスクリーンショットを示します。

😤 Cisco Aironet Desktop Utility	y - Current Profile	: WPA2-Enterprise 🛛 🖓 🔀
Action Options Help		
Current Status Profile Management	Diagnostics	
CISCO SYSTEMS		
Profile Name:	WPA2-Enterprise	
Link Status:	Authenticated	Network Type: Infrastructure
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 149
Server Based Authentication:	EAP-FAST	Data Encryption: AES
IP Address:	10.77.244.221	
Signal Strength:		Good
		Advanced

また、RADIUS サーバがワイヤレス クライアントから認証要求を受信して検証するかどう かも確認できます。そのためには、ACS サーバで Passed Authentications レポートと Failed Attempts レポートを調べます。これらのレポートは、ACS サーバの [Reports and Activities] で見ることができます。

# <u>WPA2 Personal モード向けのデバイスの設定</u>

WPA2-Persona動作モード用にデバイスを設定するには、次の手順を実行します。

- 1. WPA2 Personal モード認証向けの WLAN の設定
- 2. WPA2 Personal モード向けのワイヤレス クライアントの設定

<u>WPA2 Personal 動作モード向けの WLAN の設定</u>

クライアントがワイヤレス ネットワークに接続するために使用する WLAN を設定する必要があ ります。WPA2 Personal モード用の WLAN SSID は、WPA2-Personal です。この例では、この WLAN を管理インターフェイスに割り当てます。

WLAN と関連するパラメータを設定するために、次の手順を実行します。

- 1. コントローラの GUI で [WLANs] をクリックして、[WLANs] ページを表示します。このペー ジには、コントローラに存在する WLAN の一覧が表示されます。
- 2. [New] をクリックして新規の WLAN を作成します。
- 3. [WLANs] > [New] ページで WLAN SSID 名、プロファイル名、および WLAN ID を入力しま す。次に、[Apply] をクリックします。この例では、SSID として **WPA2-Personal** を使用し ています。

						Sa <u>v</u> e Co	onfiguration <u>P</u> ing	Logout <u>B</u> efresh
CISCO	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs > New						< Back	Apply
WLANS	Туре	WLAN	×					
▶ Advanced	Profile Name	WPA2-Per	sonal					
	WLAN SSID	WPA2-Per	sonal					

- 4. 新しい WLAN を作成すると、新しい WLAN に対する [WLAN] > [Edit] ページが表示されま す。このページでは、その WLAN に固有のさまざまなパラメータを定義できます。これに は、全般ポリシー、セキュリティ ポリシー、QOS ポリシー、および高度なパラメータが含 まれます。
- 5. WLAN を有効にするには、[General Policies] で [Status] チェック ボックスをオンにします。
- 6. AP にビーコン フレームで SSID をブロードキャストさせる場合は、[Broadcast SSID] にチェックボックスをオンにします。
- 7. [Security] タブをクリックします。[Layer 2 Security] で、[WPA+WPA2] を選択します。これ により、WLAN に対して WPA 認証が有効になります。

	saže roundnages ( Fud ) rođoni ( Fi
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
ANs	WLANs > Edit < Back App
	General Security QoS Advanced
WLANS	Laver 2 Laver 3 A66 Servers
dvanced	
	Layer 2 Security WPA+WPA2
	MAC Filtering
	Static WEP Parameters
	802.11 Data Encryption Current Key: 104 bits WEP Static Key (Key Index = 0)
	Type Key Size Key Index Enzyntion Key Key Enzynt
	WEP ANT AT THE ACCULATION
	Allow Shared Key Enabled
	EVID Durantees I
	PO2 11 Data Encryption Current Key: 0 bits CK10 Key (Key Indexe 0)
	Key Size Key Index Encryption Key Key Format
	not set 🔹 1 💌 🛛 ASCII 💌
	Foot Notes
	1 CKIP is not supported by 10xx model APs
	2 Web Policy cannot be used in combination with IPsec 3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
	4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients 5 Client MPP is not active unless WPA2 is configured

8. [WPA+WPA2 Parameters] を変更するために、ページを下にスクロールします。この例では、[WPA2 Policy] および [AES] 暗号化が選択されています。

9. [Auth Key Mgmt] で [PSK] を選択して、WPA2-PSK を有効にします。

10. 以下に示す適切なフィールドに事前共有キーを入力します。

cisco	MONITOR WLANS CONTRO	LLER WIRELESS SECURITY MANAGEMENT	Sage Configuration   Bing   Logout   Befresh
WLANS WLANS	WLANs > Edit General Security Qu	as Servers	< Back Apply
▶ Advanced	MMH Mode Key Permutation 802.1X Parameters 802.11 Data Encryption	Key Size Key Index Encryption Key not set I Enabled Enabled Type Key Size WEP 104 bits	Key Format
	WPA+WPA2 Parameters WPA Policy WPA2 Policy WPA2 Encryption Auth Key Mgmt PSK Format	ASCII	 
	Foot Notes I CRIP is not supported by 10x 2 Web Policy cannot be used in 3 H-REAP Local Switching is not 4 When client exclusion is enable 5 Client MFP is not active unless	r model APs combination with IPsec supported with IPsec, CRANITE authentication led, a Timeout Value of zero means infinity (will require WPA2 is configured	administrative override to reset excluded clients)

**注**:WLCで使用される事前共有キーは、ワイヤレスクライアントで設定されているものと 一致する必要があります。

11. [Apply] をクリックします。

WPA2 Personal モード向けのワイヤレス クライアントの設定

次の手順では、WPA2-Personal 動作モード用にワイヤレス クライアントを設定します。

WPA2-Personal モード用にワイヤレス クライアントを設定するには、次の手順を実行します。

- 1. [Aironet Desktop Utility] ウィンドウで、[Profile Management] > [New] をクリックして、 WPA2-PSK WLAN ユーザのプロファイルを作成します。
- 2. [Profile Management] ウィンドウの [General] タブをクリックし、この例に示すように、プロファイル名、クライアント名、および SSID 名を設定します。次に、[OK] をクリックします。

Profile Management		?×
General Security Advance	ed	
Profile Settings		
Profile Name:	WPA2-Personal	
Client Name:	Wireless-Client2	
Network Names		
SSID1:	WPA2-Personal	
SSID2.		
SSID3:		
	ОК	Cancel

3. [Security] タブをクリックし、[WPA/WPA2 Passphrase] を選択して WPA2-PSK 動作モード を有効にします。[Configure] をクリックして、WPA-PSK 事前共有キーを設定します。

Profile Management			? 🔀
General Security Advanced			
- Set Security Options			
O WPA/WPA2/CCKM	WPA/WPA2/CCKM EAP Type:	LEAP	
WPA/WPA2 Passphrase			
O 802.1x	802.1x EAP Type:	LEAP	
O Pre-Shared Key (Static WEP)			
◯ None			
Configure	Allow Association to Mixed Ce Profile Locked	ella	
	Limit Time for Finding Domain	Controller To: 0 🔅 se	c
Group Policy Delay:	60 😂 sec		
		OK	Cancel

4. 事前共有キーを入力して、[OK] をクリックします。

Configure WPA/WPA2 Passphrase	2×
Enter a WPA/WPA2 passphrase (8 to 63 ASCII or 64 hexadecimal characters)	
abcdefghijkl	
Cance	1

#### <u>WPA2-Personal 動作モードの確認</u>

WPA2-Enterprise 動作モード設定が正しく機能するかどうかを確認するには、次の手順を実行します。

- 1. [Aironet Desktop Utility] ウィンドウで、[WPA2-Personal] プロファイルを選択して [Activate] をクリックし、ワイヤレス クライアント プロファイルをアクティブ化します。
- 2. プロファイルがアクティブになると、ワイヤレス クライアントは認証に成功後、WLAN に 関連付けられます。次にスクリーンショットを示します。

🖻 Cisco Aironet Desktop Utility	y - Current Profile: WPA2-P	ersonal		<u>?</u> ×
Action Options Help				
Current Status Profile Management	Diagnostics			
<mark>Cisco Systems</mark>				
nullunnullun Profile Name:	WPA2-Personal			
Link Status:	Authenticated	Network T	ype: Infrastructure	
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 149		
Server Based Authentication:	None	Data Encryption: AES		
IP Address:	10.77.244.221			
Signal Strength:			Good	
			Advanced	
			<b>6</b>	

# <u>トラブルシュート</u>

ここでは、設定のトラブルシューティングに使用できる情報を示します。

次に示す debug コマンドは、設定のトラブルシューティングに役立ちます。

#### 注:<u>debug</u> 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。

• debug dot1x events enable: すべての dot1x イベントのデバッグを有効にします。これは、 正常な認証に基づくデバッグ出力の例です。**注:この**出力の一部の行は、スペースの制約に より2行目に移動されています。 (Cisco Controller)>debug dot1x events enable Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP -Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93 Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 2) Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAP Response packet with mismatching id (currentid=2, eapid=1) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received Identity Response (count=2) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 43) Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:01 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43) Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -0 Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3689 seconds on AP 00:0b:85:91:c3:c0 Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -1 Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3696 seconds on AP 00:0b:85:91:c3:c0 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received Identity Response (count=3) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===> 19 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 19) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 3) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 21) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from

mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 23) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 23, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 26) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 26, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 27) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 27, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Reject for mobile00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Failure to mobile 00:4096:af:3e:93 (EAP Id 27) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Setting quiet timer for 5 seconds for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 2) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Identity Response (count=2) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 2 ===> 20 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 3) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to

mobile 00:40:96:af:3e:93 (EAP Id 21) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===> 24 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Accept for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Creating a new PMK Cache Entry for tation 00:40:96:af:3e:93 (RSN 0) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP-Success to mobile 00:40:96:af:3e:93 (EAP Id 25) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending default RC4 key to mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending Key-Mapping RC4 key to mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Auth Success while in Authenticating state for mobile 00:40:96:af:3e:93

- debug dot1x packet enable: 802.1x パケット メッセージのデバッグを有効にします。
- debug aaa events enable: すべての aaa イベントのデバッグ出力を有効にします。

### <u>関連情報</u>

- WPA2 Wi-Fi Protected Access 2
- ワイヤレス LAN コントローラおよび外部 RADIUS サーバを使用する EAP-FAST 認証の設定
   例
- EAP 認証と WLAN コントローラ(WLC)の設定例
- WPA 設定の概要
- ・<u>ワイヤレス製品に関するサポート</u>
- <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。