ワイヤレス LAN コントローラ スプラッシュ ペ ージ リダイレクトの設定例

内容

概要 前提条件 要件 使用するコンポーネント 表記法 背景説明 ネットワークのセットアップ 設定 ステップ1: Cisco Secure ACS サーバを使用して RADIUS 認証用の WLC を設定する。 ステップ2:管理部門および運用部門用の WLAN を設定する。 ステップ3: スプラッシュ ページ リダイレクト機能をサポートするように Cisco Secure ACS を設定する。 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、ワイヤレス LAN コントローラのスプラッシュ ページ リダイレクト機能 の設定方法を説明します。

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。

- LWAPP セキュリティ ソリューションに関する知識
- Cisco Secure ACS の設定方法に関する知識

<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 バージョン 5.0 が稼働している Cisco 4400 シリーズ ワイヤレス LAN コント ローラ(WLC) • Cisco 1232 シリーズ Lightweight アクセス ポイント(LAP)

- ファームウェア バージョン 4.1 が稼働している Cisco Aironet 802.a/b/g ワイヤレス クライア ント アダプタ
- バージョン 4.1 が稼働している Cisco Secure ACS サーバ
- ・サードパーティの外部 Web サーバ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、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>

背景説明

スプラッシュ ページ Web リダイレクトは、ワイヤレス LAN コントローラ バージョン 5.0 から 導入された機能です。この機能を使用すると、ユーザは 802.1x 認証の完了後に特定の Web ペー ジにリダイレクトされます。リダイレクトは、ユーザがブラウザ(デフォルトのホーム ページが 設定されている)を開いたとき、または URL へのアクセスを試行したときに実行されます。 Web ページへのリダイレクトが完了すると、ユーザはネットワークにフル アクセスできます。

Remote Authentication Dial-In User Service(RADIUS)サーバでリダイレクト ページを指定でき ます。RADIUS サーバは、802.1x 認証に成功した時点で、Cisco av-pair url-redirect RADIUS 属性 をワイヤレス LAN コントローラに返すように設定する必要があります。

スプラッシュ ページ Web リダイレクト機能は、802.1x または WPA/WPA2 レイヤ 2 セキュリティに対して設定されている WLAN でのみ利用できます。

<u>ネットワークのセットアップ</u>

この例では、Cisco 4404 WLC と Cisco 1232 シリーズ LAP がレイヤ 2 スイッチを介して接続されています。Cisco Secure ACS サーバ(外部 RADIUS サーバとして機能)も同じスイッチに接続されています。すべてのデバイスは同じサブネット内にあります。

最初に LAP をコントローラに登録します。2つのWLANを作成する必要があります。1つは**管理部** 門ユーザ用で、もう1つは**運用部門**ユーザ用です。どちらのワイヤレス LAN も WPA2/AES を使 用します(EAP-FAST が認証に使用されます)。どちらの WLAN も、ユーザを適切なホーム ペ ージ URL(外部 Web サーバ上)ヘリダイレクトするためにスプラッシュ ページ リダイレクト機 能を使用します。

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。



Cisco Secure ACS server

WLC Management IP address:	10.77.244.204
WLC AP Manager IP address:	10.77.244.205
Wireless Client IP address:	10.77.244.221

Cisco Secure ACS server IP address 10.77.244.196

Subnet Mask used in this example 255.255.255.224

次のセクションでは、この構成でデバイスを設定する方法を説明します。

<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。

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。

スプラッシュ ページ リダイレクト機能を使用するようにデバイスを設定するには、次の手順を実 行します。

- 1. <u>Cisco Secure ACS サーバを使用して RADIUS 認証用の WLC を設定する。</u>
- 2. 管理部門および運用部門用の WLAN を設定する。
- 3. <u>スプラッシュ ページ リダイレクト機能をサポートするように Cisco Secure ACS を設定す</u> <u>る。</u>

<u>ステップ 1 : Cisco Secure ACS サーバを使用して RADIUS 認証用の WLC を設定</u> <u>する。</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。

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] と [RADIUS Authentication] をクリックして、[RADIUS Authentication Servers] ページを表示します。
- 2. [New] をクリックして、RADIUS サーバを定義します。
- [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

					Save Co	efouration - Pine L	Logout Refres
cisco	MONITOR WLANS CONT	OLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	неџр	
Security	RADIUS Authentication	Servers > New				< Back	Apply
AAA -	Server Index (Priority)	1					
RADIUS Authentication	Server IPAddress	10.77.244.196					
Accounting TACACS+	Shared Secret Format	ASCII 💌					
LDAP Local Net Users MAC Filtering	Shared Secret	•••••					
Disabled Clients User Login Policies AP Policies	Confirm Shared Secret	•••••					
Local EAP	Key Wrap	(Designed for I	IPS customers	and requires a ke	y wrap complian	RADIUS server)	
Priority Order	Port Number	1012					
Wireless Protection	Server Status	Enabled 💌					
Web Auth	Support for RFC 3576	Enabled 💌					
Advanced	Server Timeout	2 seconds					
	Network User	🗵 Enable					
	Management	🗵 Enable					
	IPSec	Enable					
このドキュメン	トブけ 1077 04	1 106 2 112	יד מו	ミレフをは		サーバを庙	田レプい

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。

4. [Apply] をクリックします。

<u>ステップ2:管理部門および運用部門用のWLANを設定する。</u>

この手順では、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 2 つの WLAN(1 つは管理部門用、もう 1 つは運用部門用)を設定します。

管理部門用の WLAN SSID は Admin です。運用部門用の WLAN SSID は Operations です。

両方の WLAN と Web ポリシーで WPA2 をレイヤ 2 セキュリティ メカニズムとして有効にし、 スプラッシュ ページ Web リダイレクト機能をレイヤ 3 セキュリティ方式として有効にするため に、EAP-FAST 認証を使用します。 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。

cisco	MONITOR	WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs>	New						< Back	Apply
VLANs	Туре		WLAN						
Advanced	Profile Na	me	Admin						
	WLAN SSI	ID	Admin						

- 3. [WLANs] > [New] ページで、WLAN SSID 名とプロファイル名を入力します。
- 4. [Apply] をクリックします。

0

- 5. 最初に、管理部門の WLAN を作成します。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。このようなパラメータには、汎用ポリシー、セキュリテ ィ ポリシー、QoS ポリシー、および詳細設定のパラメータがあります。
- 6. 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

cisco		LANS <u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	Saye Co C <u>O</u> MMANDS	HELP	Logout <u>R</u> efre
WLANS WLANS WLANS Advanced	WLANS > Ed General Profile Nam Type SSID Status Security Po Radio Polic; Interface Broadcast S	it Security QoS Marin WLAN Admin E Enable Micies Splash- (Modificat Y All admin SSID I Enable	Advanced ed Page-Web-Ri ions done unde	edirect[WPA2 r security tab	2][Auth(802.1X)] will appear after a] pplying the chan	ges.)	Apply

- 7. [Security] タブをクリックし、さらに [Layer 2] タブをクリックします。
- 8. [Layer 2 Security] ドロップダウン リストから [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。

9. [WPA+WPA2 Parameters] の下で、[WPA2 Policy] および [AES Encryption] チェック ボック スをオンにします。

				107 DB 108	Sa <u>v</u> e Co	nfiguration	eing Logout Befn
CISCO	MONITOR WLANS COM	TROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	нецр	_
WLANS WLANS WLANS > Advanced	WLANS > Edit General Security Layer 2 Layer 3 Layer 2 Security Wi WPA+WPA2 Parameter WPA Policy WPA2 Policy WPA2 Encryption Auth Key Mgmt	QoS Advanced AAA Servers VA+WPA2 x IAC Filtering S VA+WPA2 x IAC Filtering S VA+WPA2 x IAC Filtering S VA+WPA2 x IAC Filtering S VA+WPA2 x IAC Filtering S				< Back	Apply
	-						

- 10. [Auth Key Mgmt] ドロップダウン リストから **802.1x** を選択します。このオプションにより、WLAN に対して 802.1x/EAP を使用した WPA2 認証と AES 暗号化が有効になります。
- 11. [Layer 3] タブをクリックします。
- 12. [Web Policy] チェック ボックスをオンにして、[Splash Page Web Redirect] オプション ボ タンをクリックします。このオプションによって、スプラッシュ ページ Web リダイレク ト機能が有効になります。

							Sa <u>v</u> e Co	onfiguration Eing	Logout Befre
CISCO	MONITOR	WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANS WLANS WLANS Advanced	WLANS> General Layer C p C c C p C c Prea ACL	Edit Secur 2 Laye or 3 Security Web Policy i Authenticatio Conditional 1 Splash Page authenticatio	ity QoS er 3 AAA Su None 2 web Redirect Web Redirect None 💌	Advanced ervers	SECONTIN			< Back	Apply

- 13. [AAA Servers] タブを選択します。
- 14. [Authentication Servers] の下で、[Server 1] ドロップダウン リストから適切なサーバの IP アドレスを選択します。

	Save Configuration Ping Log	out i <u>B</u> ef
WLANS WLANS WLANS WLANS Advanced	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP WLANS > Edit ////////////////////////////////////	

この例では、10.77.244.196 が RADIUS サーバとして使用されます。

- 15. [Apply] をクリックします。
- 16. 手順 2 ~ 15 を繰り返して、運用部門の WLAN を作成します。[WLANs] ページに作成した 2 つの WLAN が一覧表示されます。

					Sage Co	onfiguration Ping	Logout <u>R</u> efresh
CISCO	MONITOR WLANS CONTROLL	ER WIREL	ESS SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs						New
VLANs WLANs	Profile Name	Туре	WLAN SSID		Admin Status	Security Policies	
Advanced	Admin	WLAN	Admin		Enabled	[WPA2][Auth(802.1X)], Splash-Page
	Operations	WLAN	Operations		Enabled	[WPA2][Auth(802.1X], Splash-Page
セキュリティ ポ	リシーにスプラッシ	ノユ ペー	-ジ リダイ	レクトカ	「含まれて	ていることだ	がわかり

セキュリティ ポリシーにスプラッシュ ページ リダイレクトが含まれていることがわかり ます。

<u>ステップ 3:スプラッシュ ページ リダイレクト機能をサポートするように Cisco</u> <u>Secure ACS を設定する。</u>

次の手順では、この機能に対応するように RADIUS サーバを設定します。RADIUS サーバは、ク ライアント クレデンシャルを検証するために EAP-FAST 認証を実行し、認証が成功した時点で 、Cisco av-pair *url-redirect RADIUS 属性で指定された URL(外部 Web サーバ上)にユーザをリ* ダイレクトする必要があります。

Cisco Secure ACS を EAP-FAST 認証対応に設定する

注:このドキュメントでは、ワイヤレスLANコントローラ(WLC)がAAAクライアントとしてCisco Secure ACSに追加されていることを前提としています。 RADIUS サーバに 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 GUI で [System Configuration] をクリックし、さらに [System Configuration] ページから [Global Authentication Setup] を選択します。

In Edit View E	Microsoft Internet Explorer	
ddress bitp://127	2.0.0.1:1065/	- Do
ie Edt yew Fr gdress in http://127 Citco States in http://127 Citco States in http://127 Citco States in http://127 in http://12	growtes Lood 20.0.1:1005/ Service Control Servi	Help
		<u>[Back to Troj]</u> Date Format Control
		Select to configure the date format, either month/day/year or day/month/year, for CSV files and Service Logs and in the GUI.
		(Back to Teo)

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。

- Lating of the	.0.0.1:1065/	• 🔂 👳
en Sverens dada.	System Configuration	Σ
liter 1	EAP Configuration	P Help
Steep Broop Setup Shared Profile Components Network Configuration System Configuration Interface Configuration Administration	PEAP Allow EAP-MSCHAPv2 Allow EAP-GTC Allow Posture Validation Allow EAP-TLS Select one or more of the following options: E Certificate SAN comparison E Certificate CN comparison E Certificate Binary comparison	Use this page to specify settings for various authentication protocols. • EAP Configuration • PSAP • EAP FASIS • E
Control External User Databases Posture Validation Network Access Profiles Reports and	EAP-TLS session timeout (minutes): 120 Cisco client initial message: PEAP session timeout (minutes): 120 Enable Fast Reconnect:	EAP Configuration EAP is a flexible request-response protocol for arbitrary authentic ation information (RFC 2284), EAP is layered on top of another protocol such as UOP, 002.1x or RADDUS and supports multiple "authentication" types. [back to Top] PEAP
ine omentation	EAP-FAST EAP-FAST Configuration	PEAP is the outer layer protocol for the secure tunnel.
	EAP-TLS III Allow EAP-TLS Select one or more of the following options:	authentication can occur only after you have completed the required steps on the ACS Certificate Setup page. Allow EAP-MSCHAPv2 — Use to anable EAP-MSCHAPv2 within MS PEAP authentication. Enable this protocol for any repository that supports MS-

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

Address http://127.0	0.0.1:1065/	· 63 a
Crace Systems	System Configuration	
حقالته حقاقه	EAP-FAST Configuration	- Help
User Setup	2	EAP-FAST Configuration Page
Group Setup	EAP-FAST Settings	Use this page to configure EAP-FAST authentication settings.
Shared Profile Components	R Allow EAP-FAST	EAP-EAST Settlese Clean bitted message
Network Configuration	Active master key TTL 1 months	Authority ID Infe Allow anonymous inclued DAC previousing
Configuration	Tunnel PAC TTL 1 weeks	Aliver, and then the start for band PAC previousning Aliver, machine, section, file stars Aliver, statistics, section, resume
Configuration	Client initial message: tacwebacs	Allerred inner methods Certificate Comparison
Administration Control	Authority ID Info: tacwebacs	• EAP-TLS service timest (admetes) • EAP-TLS restore to the server • Actual EAP-EAST server status
Diternal User Databases	Allow authenticated in-band PAC provisioning	EAP-FAST Settings
Porture Validation	Accept client on authenticated provisioning Require client certificate for provisioning	Allow EAP-FAST-To enable EAP-FAST authentication, select this check box.
Reports and Activity	Allow Machine Authentication Machine PAC TTL Weeks Machine Stateless session resume	 Active Haster Key TIL – Enter a value for the amount of time that a master key is used to generate new Protected Access Credentials (PACs). When the time to live (TTL) defined for the Master Key aspires, the master key is considered retired and a new master key is generated.
Documentation	Authorization PAC TTL 1 hours	 Retired master key TIL – Enter a value for the amount of time that PACs generated using a retired master key are acceptable for EAP-FAST authentication. When an end-user client gains network access using a PAC based on a retired master key. ACS sends a new PAC to the endruser client.
	EAP-MSCHAPv2	 Tennel PAC TR. – Enter a value for the amount of time that a PAC is used before it expires and must be replaced. If the master key used to generate the Tunnel PAC has not expired, new PAC creation and assignment is automatic. If the master key used to generate the Tunnel PAC expired, automatic or manual provisioning must be used to provide the end-user client with a new PAC.

- 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。[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] オプションでは、EAP-FAST TLS トンネル内で実行できる内部 EAP 方式を決定します。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。
- 7. [Submit] をクリックします。注:匿名インバンドPACプロビジョニングと認証済みインバン ドプロビジョニングを使用してEAP FASTを設定する方法の詳細と例については、『<u>ワイヤ</u> レスLANコントローラおよび外部RADIUSサーバを使用したEAP-FAST認証の設定例』を参 照してください。
- ユーザ データベースを設定し、url-redirect RADIUS 属性を定義する

この例では、ワイヤレス クライアントのユーザ名とパスワードをそれぞれ、User1 および User1 として設定します。

次の手順を実行して、ユーザ データベースを作成します。

- 1. ナビゲーションバーの ACS GUI から [User Setup] を選択します。
- 2. 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。



3. [User Setup] の [Edit] ページで、この例に示すように、[Real Name] と [Description]、さら に [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。

CiscoSecure ACS - N	Microsoft Internet Explorer	_l∂ ×
Ele Edt Yew Fg	vonites Iools Help	Links 🇯 🤔
Address a http://127.0	0.0.1:1065/	۵ 🔁 🗉
Crace Systems	User Setup	×
als. db.		
[Dune]	Edit	Hep
Setup	User: User1 (New User)	Account Disabled
Group Setup		Onleting a Username Supplementary User Info
db. Shared/roffe	Account Disabled	Password Asthentication Coup to which the over is assigned
"OP Components		Callback
Configuration	Supplementary User Info	Advanced Settline
Sustem Configuration	Real Name	Contreads Access Restorctions Mail Session
mm. Listerface	Description	Georgent, Desting Georgent, Disable
Configuration		Overnikadable AELs Advanced TACACS - Sattings
Administration Control		TACACS - Enable Control TACACS - Enable Personnel
The External User	User Setup ?	TACACS - Dutbeend Password
Cont Parking	Password Authentication:	Command Authorization for Network Device Nanagement Applications
Validation	ACS Internal Database	LACACS - Unknewn Services LET RADIUS Attolectes
Network Access Profiles	CiscoSecure PAP (Also used for CHAP/MS- CHAP/APAP, if the Separate field is not	BADUS Yeadar Specific Attributes
Reports and	checked.)	
-Ch L Online	Password •••••	Account Disabled Status
Documentation	Confirm Password	Select the Account Disabled check box to disable this account clear the check how to apply the account.
	Separate (CHAP/MS-CHAP/ARAP)	
	Password	[Back to Traj
	Confirm	Deleting a Username
	Password Submit Cancel	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
	Concer	confirm your action, click OK.
Done Cone	Distance Mit Ma	j j j j 🕐 Internet
start 10 8	I Charlen AC - Mic.	1.20 MM

- 4. RADIUS 属性を変更するため、ページをスクロール ダウンします。
- 5. [[009\001] cisco-av-pair] チェックボックスをオンにします。
- 6. [[009\001] cisco-av-pair] 編集ボックスに、次の Cisco av-pairs を入力し、ユーザのリダイレ クト先の URL を指定します。url-redirect=http://10.77.244.196/Admin-

e

Lo	gi	n	.	h	r	n	l

Cisco Systems	User Setup	l
	(useu iur senueass anu senukuun cherus such as routers)	Help
User Setup	Password	Account Disabled
Group Setup	Password	Onleting a Uvername Supplementary Uver Infe
Shared Profile Components	Cisco Airespace RADIUS Attributes	Password Authentication Group to which the user is assigned Callback
Network Configuration	[14179/005] Aire-Interface-Nume	Cleat IP Address Assignment Advanced Settings
System Configuration		Network Access Restrictions Harr Seasons Harr Deples
Configuration		Account Disable Downloadable ACLs
Administration Centrel	Cisco IOS/PIX 6.x RADIUS Attributes	Advanced TACACS- Settings TACACS- Enable Control TACACS- Enable Control TACACS- Enable Remained
Dicternal Uper Databases	R [009\001] cisco-av-pair	TACACS- Outbeand Passwerd TACACS- Shell Command Authorization
Posture Validation	ur1- redirect=http://10.77.244.196/	Command Authorization for Network Device Management Applications TACACS-: Unknown Services
Network Access Profiles	Admin-login.html	BADEUS Vendor-Specific Attributes
Reports and Activity		
and a l Online		Account Disabled Status
Documentation		Select the Account Disabled check box to disable this account clear the check box to enable the account.
	P Back to Help	[Back.to.Top]
		Deleting a Username
	Submit Delete Cancel	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

これは、管理部門ユーザのホームページです。

- 7. [Submit] をクリックします。
- 8. この手順を繰り返し、User2(運用部門ユーザ)を追加します。
- 9. 手順1~6を繰り返し、より多くの管理部門ユーザと運用部門ユーザをデータベースに追加 します。注:RADIUS属性は、Cisco Secure ACSのユーザレベルまたはグループレベルで設 定できます。

<u>確認</u>

設定を検証するため、管理部門と運用部門の WLAN クライアントをそれぞれ適切な WLAN にア ソシエーションします。

ユーザが管理部門からワイヤレス LAN Admin に接続している場合には、802.1x クレデンシャル (この例の場合は EAP-FAST クレデンシャル)の入力がユーザに求められます。ユーザがクレデ ンシャルを入力すると、WLC がそれらのクレデンシャルを Cisco Secure ACS サーバに渡します 。Cisco Secure ACS サーバはユーザのクレデンシャルをデータベースに照合して検証し、認証に 成功した時点で、url-redirect 属性をワイヤレス LAN コントローラに返します。この段階で認証は 完了です。

🖻 Cisco Aironet Desk	top Utility - Cur	rent Profile: Admir	1	? 🗙
Action Options Help				
Current Status Profile M	anagement Diagno	ostics		
CISCO SYSTEMS				
IlluIllu. _{Pr}	rofile Name: Admin			
1	Link Status: Not Ass	sociated	Network Type: Infrastructure	
Wire	eless Mode: 5 GHz !	54 Mbps	Current Channel: 149	
Server Based Aut	hentication: None		Data Encryption: AES	
	IP Address: 10.77.2	44.221		
Sig	nal Strength: 📲		Good	
			Advanced	

ユーザが Web ブラウザを開くと、ユーザは管理部門のホーム ページの URL ヘリダイレクトされ ます(この URL は cisco-av-pair 属性を介して WLC に返されます)。ユーザは、リダイレクト後 、ネットワークにフル アクセスできます。次にスクリーンショットを示します。



ユーザが運用部門から WLAN Operations に接続した場合も同様に一連のイベントが発生します

o

🛜 Cisco Aironet Desktop Utilit	y - Current Profile: Operatio	ns ? 🔀
Action Options Help		
Current Status Profile Management	Diagnostics	
CISCO SYSTEMS		
utiliutiliu. Profile Name:	Operations	
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



<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。

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。

設定のトラブルシューティングを行うために、次のコマンドを使用することができます。

show wlan wlan_id:特定の WLAN の Web リダイレクト機能のステータスを表示します。以下が一例です。

WLAN Identifier	1
Profile Name	Admin
Network Name (SSID)	Admin
Web Based Authentication	Disabled
Web-Passthrough	Disabled
Conditional Web Redirect	Disabled
Splash-Page Web Redirect	Enabled

 debug dot1x events enable: 802.1x パケット メッセージのデバッグを有効にします。以下が 一例です。

Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP Request from AAA to mobile 00:40:96:ac:dd:05 (EAP Id 16)

- Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAPOL EAPPKT from mobile 00:40:96:ac:dd:05
- Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAP Response from mobile 00:40:96:ac:dd:05 (EAP Id 16, EAP Type 43)
- Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Processing Access-Challenge for mobile 00:40:96:ac:dd:05
- Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Setting re-auth timeout to 1800
 seconds, got from WLAN config.

Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Station 00:40:96:ac:dd:05

```
setting dot1x reauth timeout = 1800
 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Creating a new PMK Cache Entry
     for station 00:40:96:ac:dd:05 (RSN 2)
 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Adding BSSID 00:1c:58:05:e9:cf
     to PMKID cache for station 00:40:96:ac:dd:05
 Fri Feb 29 10:27:16 2008: New PMKID: (16)
 Fri Feb 29 10:27:16 2008:
                              [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca
     fb fa 8e 3c
 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Disabling re-auth since PMK
     lifetime can take care of same.
 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP-Success to mobile
     00:40:96:ac:dd:05 (EAP Id 17)
 Fri Feb 29 10:27:16 2008: Including PMKID in M1 (16)
                              [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca
 Fri Feb 29 10:27:16 2008:
     fb fa 8e 3c
 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAPOL-Key Message to
     mobile 00:40:96:ac:dd:05
     state INITPMK (message 1), replay counter 00.00.00.00.00.00.00
 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received Auth Success while
     in Authenticating state for mobile 00:40:96:ac:dd:05
• 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。以下が一
 例です。
 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
     Authentication Packet (id 103) to 10.77.244.196:1812, proxy state
     00:40:96:ac:dd:05-00:00
 Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=11
 Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=11
 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Challenge received from
     RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
     Authentication Packet (id 104) to 10.77.244.196:1812, proxy state
     00:40:96:ac:dd:05-00:00
 Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=2
 Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=2
 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Accept received from
     RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 AAA Override Url-Redirect
     'http://10.77.244.196/Admin-login.html' set
 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Applying new AAA override for
     station 00:40:96:ac:dd:05
 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Override values for station
     00:40:96:ac:dd:05
        source: 4, valid bits: 0x0
```

source: 4, valid bits: 0x0
qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
vlanIfName: '', aclName: '

関連情報

- <u>Cisco Wireless LAN Controller コンフィギュレーション ガイド、リリース 5.0</u>
- ・ワイヤレス LAN コントローラの Web 認証の設定例
- <u>ワイヤレス LAN コントローラを使用した外部 Web 認証の設定例</u>
- ・<u>ワイヤレスに関するサポート ページ</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。