Konfigurationsbeispiel für die Umleitung der Splash-Seite des Wireless LAN Controller

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Hintergrundinformationen Netzwerkeinrichtung Konfigurieren Schritt 1: Konfigurieren des WLC für die RADIUS-Authentifizierung über den Cisco Secure ACS-Server Schritt 2: Konfigurieren Sie die WLANs für die Abteilung Administration und Betrieb. Schritt 3: Konfigurieren Sie Cisco Secure ACS so, dass die Splash-Seitenumleitungsfunktion unterstützt wird. Überprüfung Fehlerbehebung Zugehörige Informationen

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Funktion zur Umleitung der Splash-Seite auf den Wireless LAN-Controllern konfigurieren.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind, bevor Sie diese Konfiguration ausprobieren:

- Kenntnisse der LWAPP-Sicherheitslösungen
- Informationen zur Konfiguration von Cisco Secure ACS

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Wireless LAN Controller (WLC) der Serie 4400 mit Firmware-Version 5.0
- Cisco Lightweight Access Point der Serie 1232 (LAP)
- Cisco Aironet 802.a/b/g Wireless Client Adapter für Firmware-Version 4.1
- Cisco Secure ACS Server mit Version 4.1
- Externer Webserver von Drittanbietern

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter <u>Cisco Technical Tips</u> <u>Conventions (Technische Tipps von Cisco zu Konventionen).</u>

Hintergrundinformationen

Splash Page Web Redirect ist eine Funktion, die mit dem Wireless LAN Controller Version 5.0 eingeführt wurde. Mit dieser Funktion wird der Benutzer auf eine bestimmte Webseite umgeleitet, nachdem die 802.1x-Authentifizierung abgeschlossen ist. Die Umleitung erfolgt, wenn der Benutzer einen Browser öffnet (konfiguriert mit einer Standard-Startseite) oder versucht, auf eine URL zuzugreifen. Nachdem die Umleitung auf die Webseite abgeschlossen ist, hat der Benutzer vollen Zugriff auf das Netzwerk.

Sie können die Umleitungsseite auf dem RADIUS-Server (Remote Authentication Dial-In User Service) angeben. Der RADIUS-Server muss so konfiguriert werden, dass das Cisco AV-pair urlredirect RADIUS-Attribut bei erfolgreicher 802.1x-Authentifizierung an den Wireless LAN Controller zurückgegeben wird.

Die Splash-Page-Webumleitungsfunktion ist nur für WLANs verfügbar, die für die 802.1x- oder WPA/WPA2-Layer-2-Sicherheit konfiguriert sind.

Netzwerkeinrichtung

In diesem Beispiel sind ein Cisco 4404 WLC und ein Cisco 1232 LAP über einen Layer-2-Switch verbunden. Der Cisco Secure ACS-Server (der als externer RADIUS-Server fungiert) ist ebenfalls mit demselben Switch verbunden. Alle Geräte befinden sich im gleichen Subnetz.

Die LAP wird zunächst für den Controller registriert. Sie müssen zwei WLANs erstellen: eines für die Benutzer der **Administratorabteilung** und eines für die Benutzer der **Betriebsabteilung**. Beide WLANs verwenden WPA2/AES (EAP-FAST wird für die Authentifizierung verwendet). Beide WLANs verwenden die Funktion "Splash Page Redirect" (Umleitung der Splash-Seite), um Benutzer an die entsprechenden URLs der Startseite (auf externen Webservern) umzuleiten.

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



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

Im nächsten Abschnitt wird erläutert, wie Sie die Geräte für dieses Setup konfigurieren.

Konfigurieren

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Hinweis: Verwenden Sie das <u>Tool für die Suche nach Befehlen (nur registrierte Kunden), um</u> weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Führen Sie die folgenden Schritte aus, um die Geräte für die Verwendung der Splash-Page-Umleitungsfunktion zu konfigurieren:

- 1. <u>Konfigurieren des WLC für die RADIUS-Authentifizierung über den Cisco Secure ACS-</u> <u>Server</u>
- 2. Konfigurieren Sie die WLANs für die Admin- und die Betriebsabteilung.
- 3. <u>Konfigurieren Sie Cisco Secure ACS so, dass die Funktion zum Umleiten von Splash-Seiten</u> <u>unterstützt wird.</u>

Schritt 1: Konfigurieren des WLC für die RADIUS-Authentifizierung über den Cisco Secure ACS-Server

Der WLC muss konfiguriert werden, um die Benutzeranmeldeinformationen an einen externen RADIUS-Server weiterzuleiten.

Führen Sie die folgenden Schritte aus, um den WLC für einen externen RADIUS-Server zu konfigurieren:

- 1. Wählen Sie **Sicherheit** und **RADIUS-Authentifizierung** in der Benutzeroberfläche des Controllers aus, um die Seite RADIUS-Authentifizierungsserver anzuzeigen.
- 2. Klicken Sie auf **Neu**, um einen RADIUS-Server zu definieren.
- Definieren Sie die RADIUS-Serverparameter auf der Seite RADIUS Authentication Servers > New (RADIUS-Authentifizierungsserver > Neu).Zu diesen Parametern gehören:IP-Adresse des RADIUS-ServersGemeinsamer SchlüsselPort-NummerServerstatus

ahaha					Sage Co	onfiguration \ Bing	Logout Befresh
cisco	MONITOR WLANS CONT	ROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	RADIUS Authentication	Servers > New				< 8ack	Apply
✓ AAA General	Server Index (Priority)	1					
RADIUS Authentication	Server IPAddress	10.77.244.196					
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 I	IPS customers	and requires a ke	y wrap complian	t RADIUS server)	
Priority Order	Port Number	1012					
Access Control Lists							
 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					

In diesem Dokument wird der ACS-Server mit der IP-Adresse 10.77.244.196 verwendet. 4. Klicken Sie auf **Apply** (Anwenden).

Schritt 2: Konfigurieren Sie die WLANs für die Abteilung Administration und Betrieb.

In diesem Schritt konfigurieren Sie die beiden WLANs (eines für die Admin-Abteilung und eines für die Operations-Abteilung), die die Clients für die Verbindung mit dem Wireless-Netzwerk verwenden.

Die WLAN-SSID für die Admin-Abteilung lautet *Admin*. Die WLAN-SSID für die Betriebsabteilung lautet "Operations" (Betrieb).

Verwenden Sie die EAP-FAST-Authentifizierung, um WPA2 als Layer-2-Sicherheitsmechanismus in beiden WLANs zu aktivieren, und die Webrichtlinie - Splash Page-Webumleitung als Layer-3-Sicherheitsmethode.

Gehen Sie wie folgt vor, um das WLAN und die zugehörigen Parameter zu konfigurieren:

- 1. Klicken Sie in der GUI des Controllers auf **WLANs**, um die Seite WLANs anzuzeigen.Auf dieser Seite werden die WLANs aufgelistet, die auf dem Controller vorhanden sind.
- 2. Klicken Sie auf Neu, um ein neues WLAN zu

erstellen.							Cause Co	affection Data	Longut Defeach
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Colour Ferresu
WLANs	WLANs>	New						< Back	Apply
WLANS	Туре		WLAN						
Advanced	Profile Na	me	Admin						
	WLAN SSI	D	Admin						

- 3. Geben Sie auf der Seite WLANs > New (WLAN > Neu) den WLAN-SSID-Namen und den Profilnamen ein.
- 4. Klicken Sie auf Apply (Anwenden).
- 5. Zunächst erstellen wir das WLAN für die Admin-Abteilung.Nach dem Erstellen eines neuen WLAN wird die Seite WLAN > Edit (WLAN > Bearbeiten) für das neue WLAN angezeigt. Auf dieser Seite können Sie verschiedene Parameter speziell für dieses WLAN definieren. Dies umfasst allgemeine Richtlinien, Sicherheitsrichtlinien, QoS-Richtlinien und erweiterte Parameter.
- 6. Aktivieren Sie unter General Policies (Allgemeine Richtlinien) das Kontrollkästchen **Status**, um das WLAN zu aktivieren.

cisco		<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	Saya C COMMANDS	onfiguration Eine HELP) Logout <u>R</u> efr
WLANS WLANS Havanced	WLANS > General Profile f Type SSID Status Security Radio P Interfac Broaded	Edit Secur Name y Policies volicy ce est SSID	ity QoS Admin WLAN Admin I Enable Splash- (Modificati All admin I Enable	Advanced ed Page-Web-Ri ons done unde	edirect[WPA2 r security tab	?][Auth(802.1X)] will appear after a] pplying the chan	ges.)	Apply

- 7. Klicken Sie auf die Registerkarte Sicherheit und dann auf die Registerkarte Layer 2.
- 8. Wählen Sie **WPA+WPA2** aus der Dropdown-Liste "Layer 2 Security" (Layer 2-Sicherheit) aus.In diesem Schritt wird die WPA-Authentifizierung für das WLAN aktiviert.
- 9. Aktivieren Sie unter WPA+WPA2-Parameter die Kontrollkästchen WPA2-Richtlinie und AES-Verschlüsselung

verschliusselui	<u>y.</u>						
alialia					Saye Co	infiguration Eing	Logout Refre
CISCO	MONITOR WLANS CONT	TROLLER WIRELESS	SECORITY	MANAGEMENT	COMMANDS	нецр	
WLANs	WLANs > Edit					< Back	Apply
T WI AND	General Security	QoS Advanced					
WLANS	Layer 2 Layer 3	AAA Servers					
Advanced							
	Layer 2 Security WP	A+WPA2					
	E MA	AC Filtering					
	WPA+WPA2 Parameters						
	WPA Policy						
	WPA2 Folicy						
	Auth Key Mamt	802.1X					
	L						

- Wählen Sie 802.1x aus der Dropdown-Liste "Auth Key Mgmt" (Schlüsselverwaltung für Authentifizierung) aus. Diese Option aktiviert WPA2 mit 802.1x/EAP-Authentifizierung und AES-Verschlüsselung für das WLAN.
- 11. Klicken Sie auf die Registerkarte "Layer 3 Security".
- 12. Aktivieren Sie das Kontrollkästchen Webrichtlinie, und klicken Sie dann auf das Optionsfeld Splash Page Web Redirect (Webumleitung für Splash-Seite). Mit dieser Option wird die Splash Page Web Redirect-Funktion aktiviert.

					Sa <u>v</u> e Co	onfiguration Ping	Logout <u>R</u> efre
CISCO	MONITOR WLANS CONTRO	LLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANS WLANS MLANS Advanced	WLANS > Edit General Security Q Layer 2 Layer 3 / Layer 3 Security None Web Policy 2 Authentication Passthrough Conditional Web Redir Preauthentication ACL None	oS Advanced AAA Servers Total AAA Servers				< Back	Apply

- 13. Klicken Sie auf die Registerkarte AAA-Server.
- 14. Wählen Sie unter Authentication Servers (Authentifizierungsserver) in der Dropdown-Liste Server 1 die entsprechende Server-IP-Adresse

aus.								
cisco		<u>w</u> lans <u>c</u> on	TROLLER WIREL	ESS <u>S</u> ECURITY	MANAGEMENT	Sa <u>v</u> a Co C <u>O</u> MMANDS	onfiguration Ping HELP	Logout <u>R</u> ef
WLANS WLANS MLANS Advanced	WLANS > E General Layer 2 Select AA Radius 5 Server 3 Server 3 Local EA Local EA Local EA	A servers bel ervers Authenticat [19:10.77.24 [None [None P Authenticat] EAP Authenticat Cation prior th user	QoS Advance AAA Servers ow to override us ion Servers 4.196, Port:1812 u v on on Enabled ity order for	e of default serve Accounting Serve I Enabled None I None I	ers on this WLAN LDAP Server ers Server 1 Server 2 Server 3	None × None ×	< Back	Apply

In diesem Beispiel wird 10.77.244.196 als RADIUS-Server verwendet.

- 15. Klicken Sie auf Apply (Anwenden).
- 16. Wiederholen Sie die Schritte 2 bis 15, um das WLAN für die Betriebsabteilung zu erstellen. Auf der Seite WLANs werden die beiden von Ihnen erstellten WLANs aufgeführt.

					Sa <u>v</u> e C	onfiguration <u>P</u> ing	Logout <u>R</u> efresh
cisco	MONITOR WLANS C	ONTROLLER WIREL	ESS SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs						New
WLANS WLANS	Profile Name	Туре	WLAN SSID		Admin Status	Security Policies	
Advanced	Admin	WLAN	Admin		Enabled	[WPA2][Auth(802.17	()], Splash-Page
	Operations	WLAN	Operations		Enabled	[WPA2][Auth(802.1>	()], Splash-Page

Beachten Sie, dass die Sicherheitsrichtlinien die Umleitung der Splash-Seite enthalten.

Schritt 3: Konfigurieren Sie Cisco Secure ACS so, dass die Splash-Seitenumleitungsfunktion unterstützt wird.

Im nächsten Schritt wird der RADIUS-Server für diese Funktion konfiguriert. Der RADIUS-Server muss eine EAP-FAST-Authentifizierung durchführen, um die Client-Anmeldeinformationen zu validieren und den Benutzer bei erfolgreicher Authentifizierung an die URL (auf dem externen Webserver) umzuleiten, die im Cisco av-pair *url-redirect*-RADIUS-Attribut angegeben ist.

Konfigurieren von Cisco Secure ACS für die EAP-FAST-Authentifizierung

Hinweis: In diesem Dokument wird davon ausgegangen, dass der Wireless LAN Controller dem Cisco Secure ACS als AAA-Client hinzugefügt wurde.

Führen Sie die folgenden Schritte aus, um die EAP-FAST-Authentifizierung auf dem RADIUS-Server zu konfigurieren:

1. Klicken Sie in der RADIUS-Server-GUI auf **Systemkonfiguration**, und wählen Sie dann auf der Seite "Systemkonfiguration" die Option **Globale Authentifizierungseinrichtung** aus.

CiscoSecure ACS - Microsoft Internet Explorer	×.91
Ele Edit Yew Favorites Icols Help	Links ** Close
Address a http://127.0.0.1:1065/	• 🔁 😡
System Configura	ation
Select User Setup Group Group Bared/hoffe Date Format Control ACS Internal Databar Configuration Settor Settor Mater Face Configuration ACS Service Manage ACS Service Manage ACS Service Manage ACS Configuration ACS Continuates ACS Continuation ACS Continuates Actinuates Actinuates <th>Help A Service (setted) Leaster Cate Fernal Control Cate Fernal Control Cate Fernal Control Excel Parameter Cate Fernal Control Excel Parameter</th>	Help A Service (setted) Leaster Cate Fernal Control Cate Fernal Control Cate Fernal Control Excel Parameter Cate Fernal Control Excel Parameter
Porture Porture Validation	Back to Help Service Cootbol Select to open the page from which you can stop or restart Cisco Secure ACS services. Reck to Tap! Legging Select to configure various Cisco Secure ACS reports and customize the type of information that is logged. Back to Tap! Date Format Cootbol Select to configure the date format, either month/day/year or day/month/year, for CSV files and Service Logs and in the GUI. Select to Tap!
8	internet
🖏 Start 🔄 🧶 Gisco Secure ACS - Mic.	- J 7:57 PM

2. Klicken Sie auf der Seite "Global Authentication" auf **EAP-FAST Configuration**, um zur Seite mit den EAP-FAST-Einstellungen zu gelangen.

le Edit Yew Fa	vonites Iools Help	Links 🀲 🥂
tress) http://127.	0.0.1:1065/	
Crees Systems	System Configuration	×
ab Litrar	EAP Configuration	P Help
Group Setup	PEAP Allow EAP-MSCHAPv2	Use this page to specify settings for various authentication protocols. • CAP Configuration • PEAP
Network Configuration System Configuration	Allow Posture Validation Allow EAP-TLS Select one or more of the following options:	EAP_FAST EAP_DIS EAP_DIS EAP_DIS EAP_DID AP_EAP_DID AP_EAP_DID SOLAP_Configuration
Administration Control	EXP-TLS session timeout (minutes): 120	EAP Configuration
Dafabases Posture Validation Notices Profiles	Cisco client initial message: PEAP session timeout (minutes): 120 Enable Fast Reconnect:	authentication information (RFC 2204), EAP is layered on top of another protocol such as UOP, 002.1x or RADIUS and supports multiple "authentication" types. [Back to Top]
operts and octivity nline ocumentation	EAP-FAST EAP-FAST Configuration	PEAP is the outer layer protocol for the secure tunnel.
	EAP-TLS Allow EAP-TLS Select one or more of the following options:	Notes: FAP is a contribute-based authentication protocol. FAP authentication can occur only after you have completed the required stops on the ACS Certificate Setup page. Allows EAP-MSCHAPv2 — Use to enable EAP-MSCHAPv2 within MS PEAP authentication Enable this external for any
	Certificate SAN comparison Submit Submit + Restart Cancel	CHAPv2, such as Microsoft AD, and the ACS Internal Database.
dia c	(T2	internet

3. Aktivieren Sie auf der Seite "EAP-FAST Settings" das Kontrollkästchen Allow EAP-FAST, um EAP-FAST auf dem RADIUS-Server zu aktivieren.

CiscoSecure ACS - N	ticrosoft Internet Explorer	
te gat yew rg	vontes Loos Hep	Unis " 4
lavess lel yetb:1(12) y	0.0.1:1065/	
Cisco Systems	System Configuration	I
db.db.		
	EAP-FAST Configuration	⊐ Hap
User Setup		EAP-FAST Configuration Page
A Group	EAP-FAST Settings	?
Setup	FAP-FAST	Use this page to configure EAP-FAST authentication settings.
Shared Profile	R Allow EAP-EAST	EAP-EAST Settings
Tempering		 Clent initial measure
Configuration	Active master key TTL	Antherity ID Lefe Allow approximate in band PAC previousing
1 forder	Retired master key TTL 3 months 💌	 Allow as then ticated in-band PAC previatening
Configuration	Tunnel PAC TTL	Allers machine authentication
Interface		Allowed inner methods
Configuration	Client initial message: tacwebacs	Certificate Comparison
Administration	Authority ID Info: tacwebacs	CAP-ILS session timeset (minutes) EAP-FAST marker server
Centres	R Allow anonymous in-band PAC provisioning	Actual EAP-EAST server states
External User Databases	Allow authenticated in-band PAC provisioning	TAD FAST Letting
Porture	Eleccent client on authenticated provisioning	
Validation	Desuite client certificate for equivieries	Allow EAP-FAST-To enable EAP-FAST authentication, select this check
Network Access	E Require client certificate for provisioning	bes.
p[Profile	L Allow Machine Authentication	Active Haster Key TR Enter a value for the amount of time that a master
Reports and	Machine PAC TTL 1 weeks	key is used to generate new Protected Access Credentials (PACs). When the time to live (TTL) defined for the Master Key expires, the master key is
	C Allow Stateless session resume	considered retired and a new master key is generated.
Documentation	Authorization PAC TTL 1 hours	 Retired master key TRL-Enter a value for the amount of time that PACs
	Allowed inner methods	generated using a retired master key are acceptable for EAP-FAST
	EAP-GTC	authentication, when an end-user client gains network access using a PAC based on a retired master key, ACS zends a new PAC to the end-user client
	R FAD MCCHADIO	
	R EAP-MSCHAPV2	 Tunnel PAC TIL = 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
	D EAP-TLS	the Tunnel PAC has not expired, new PAC creation and assignment is
	Submit Submit + Restart Cancel	automatic or manual provisioning must be used to provide the end-user
		COUNT WITH & MAY PAC.
100		

- 4. Konfigurieren Sie die TTL-Werte (Time-to-Live) des Master-Schlüssels "Aktiv/Abgesetzt" nach Bedarf, oder legen Sie den Standardwert fest, wie in diesem Beispiel gezeigt.Das Feld "Authority ID Info" (Autoritäts-ID-Informationen) stellt die Textidentität dieses ACS-Servers dar, über die ein Endbenutzer bestimmen kann, für welchen ACS-Server die Authentifizierung erfolgen soll. Das Ausfüllen dieses Feldes ist obligatorisch.Das Feld für die anfängliche Client-Anzeige gibt eine Nachricht an, die an Benutzer gesendet werden soll, die sich mit einem EAP-FAST-Client authentifizieren. Die maximale Länge beträgt 40 Zeichen. Die ursprüngliche Nachricht wird dem Benutzer nur angezeigt, wenn der Endbenutzer-Client die Anzeige unterstützt.
- 5. Wenn der ACS eine anonyme In-Band-PAC-Bereitstellung durchführen soll, aktivieren Sie das Kontrollkästchen Anonyme In-Band-PAC-Bereitstellung zulassen.
- 6. Die Option Allowed inner methods legt fest, welche internen EAP-Methoden im EAP-FAST TLS-Tunnel ausgeführt werden können. Für die anonyme In-Band-Bereitstellung müssen Sie EAP-GTC und EAP-MS-CHAP aus Gründen der Abwärtskompatibilität aktivieren. Wenn Sie Anonyme In-Band-PAC-Bereitstellung zulassen auswählen, müssen Sie EAP-MS-CHAP (Phase Null) und EAP-GTC (Phase Zwei) auswählen.
- 7. Klicken Sie auf **Senden.Hinweis:** Detaillierte Informationen und Beispiele zur Konfiguration von EAP FAST mit anonymer In-Band-PAC-Bereitstellung und authentifizierter In-Band-Bereitstellung finden Sie unter Konfigurationsbeispiel für EAP-FAST-Authentifizierung mit Wireless LAN-Controllern und externen RADIUS-Servern.

Konfigurieren Sie die Benutzerdatenbank und definieren Sie das RADIUS-Attribut url-redirect.

In diesem Beispiel werden der Benutzername und das Kennwort des Wireless-Clients als User1 bzw. User1 konfiguriert.

Gehen Sie wie folgt vor, um eine Benutzerdatenbank zu erstellen:

- 1. Wählen Sie in der Navigationsleiste in der ACS-GUI die Option **User Setup** (Benutzereinrichtung).
- 2. Erstellen Sie einen neuen Wireless-Benutzer, und klicken Sie dann auf **Hinzufügen/Bearbeiten**, um zur Bearbeitungsseite dieses Benutzers zu gelangen.

Cisco Systems	User Setup	2
Uter Setop	State User: User1 Find Add/Edit List users beginning with letter/number: ABSENT VENT NSESTING NSESTING NSESTING List all users Remove Dynamic Users	Experimental State of State Sta
Porture Validation	Pack to Yelp	If you rely on the Unknown User Policy in the External User Databases section to create entries in the ACS internal database for wars defined in an external user database modification must be located or listed here until the user has successfully authenticated once. External user database modification must be done from within the external user database Itself. For added security, authorization, and accounting purposes. User Setup keeps track of users who authenticate with an enternal user database. User Setup late you configure individual user information, add users, and delete users in the ACS internal database. Notes User Setup does not add or delete usernames in an external user database. [Bigth to Too] Finding a Specific User is the ACS Internal Database To find a user already in the ACS Internal Database. To find a user already in the ACS Internal Database.

 Konfigurieren Sie auf der Seite zur Bearbeitung der Benutzereinrichtung den Namen und die Beschreibung sowie die Kennworteinstellungen, wie in diesem Beispiel gezeigt. In diesem Dokument wird die interne ACS-Datenbank f
ür die Kennwortauthentifizierung verwendet.

8 http://127	.0.0.1:1065/	
e Statens	User Setup	<u> </u>
k. dk.	Edit	Help
User Setup Group Setup	User: User1 (New User)	Account Disabled Ordetime a Username Sapplementary User Info Eastroard Asthentic Atten
Dared Profile Components Network Configuration Digitien Configuration	Supplementary User Info Real Name Description	Comp. In which, the user is assigned Calibach Client, UP. Advance, Assignment Advanced Sections Nutrends Access Restrictions Man Section Man Section Man Section Access Restrictions
Administration Control External User Databases	User Setup ?	Oremitability ACLs Advanced JACAGS - Snttlinan DACAGS - Looking Control JACAGS - Looking Control IACAGS - Looking Assessed IACAGS - Shell Command Anthesization Cammand Anthesization for Network Device, Nanagement Auglication
Following Access Profiles Reports and	ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.)	MAACS - Unknown Services INTERABIUS Attributes RADEUS Yeader Specific Attributes
Doline Documentation	Password •••••	Account Disabled Status Select the Account Disabled check box to disable this account: clear the check box to enable the account.
	Separate (CHAP/MS-CHAP/ARAP) Password Confirm	(Back to Tap) Defeting 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 current user account from the database, click Belete . When asked to confirm your action, click DK .

- 4. Blättern Sie auf der Seite nach unten, um die RADIUS-Attribute zu ändern.
- 5. Aktivieren Sie das Kontrollkästchen [009\001] cisco-av-pair.
- 6. Geben Sie diese Cisco av-pairs im [009\001] cisco-av-pair-Bearbeitungsfeld ein, um die URL anzugeben, an die der Benutzer umgeleitet wird:url-redirect=http://10.77.244.196/Admin-Login.html

Cisco Systems	User Setup	
allowed he	(Useu iur benuPass anu benuAurn cilenis sucri as routers)	Help
User Setup	Password •••••	
Graup Setup	Confirm Password	Color Constrained Color Constrained Supplementary User Info Presentary User Info
Shared Profile Components	Cisco Airespace RADIUS Attributes	Group to relich the user is assigned Callback Callback
Retwork Configuration	[141794005] Aire-Interface-Nume	Advanced Settings
System Configuration		Network Access Restrictions Has Sension
Configuration		Account Disable Downloadable ACLs
Administration Centrel	Cisco IOS/PIX 6.x RADIUS Attributes	Advanced TACACS+ Settings TACACS+ Enable Control TACACS+ Enable Password
Databases	[009\001] cisco-av-pair [009\001] [TACACS - Outbound Password TACACS - Shell Command Authorization
anna Pesture	ur1- 🛋	Command Authorization for Network Device Management Applications TACACS - Unknown Services
Const Validation	redirect=http://10.77.244.196/ Admin=login.html	IETF RADRUS Attributes RADRUS Vender-Secrific Attributes
Profiles	*	
S Reports and Activity		
Coline		Account Disabled Status
Cap- Counterration		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]
	11	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

Dies ist die Homepage der Benutzer der Administratorabteilung.

- 7. Klicken Sie auf **Senden**.
- 8. Wiederholen Sie dieses Verfahren, um Benutzer 2 (Betriebsabteilung) hinzuzufügen.
- 9. Wiederholen Sie die Schritte 1 bis 6, um der Datenbank weitere Benutzer der Admin-Abteilung und der Operations-Abteilung hinzuzufügen. **Hinweis:** Die RADIUS-Attribute können auf Benutzer- oder Gruppenebene in Cisco Secure ACS konfiguriert werden.

<u>Überprüfung</u>

Um die Konfiguration zu überprüfen, verbinden Sie einen WLAN-Client der Admin- und der Betriebsabteilung mit den entsprechenden WLANs.

Wenn ein Benutzer der Admin-Abteilung eine Verbindung zum Wireless LAN-Administrator herstellt, wird dieser zur Eingabe von 802.1x-Anmeldedaten aufgefordert (in unserem Fall EAP-FAST-Anmeldedaten). Sobald der Benutzer die Anmeldedaten eingegeben hat, übergibt der WLC diese an den Cisco Secure ACS Server. Der Cisco Secure ACS-Server überprüft die Anmeldeinformationen des Benutzers anhand der Datenbank und gibt bei erfolgreicher Authentifizierung das url-redirect-Attribut an den Wireless LAN Controller zurück. Die Authentifizierung ist zu diesem Zeitpunkt abgeschlossen.

😤 Cisco Aironet Desktop Utility	y - Current Profile: Admin		? 🗙
Action Options Help			
Current Status Profile Management	Diagnostics		<u> </u>
CISCO SYSTEMS			
Profile Name:	Admin		
Link Status:	Not Associated	Network Type: 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	

Wenn der Benutzer einen Webbrowser öffnet, wird er zur Homepage-URL der Admin-Abteilung umgeleitet. (Diese URL wird über das cisco-av-pair-Attribut an den WLC zurückgegeben.) Nach der Umleitung hat der Benutzer vollen Zugriff auf das Netzwerk. Hier sind die Screenshots:



Die gleichen Ereignisfolgen treten auf, wenn ein Benutzer der Betriebsabteilung eine Verbindung zum WLAN-Betrieb herstellt.

😤 Cisco Aironet Desktop Utility	y - Current Profile: Operatio	ns	? 🗙
Action Options Help			
Current Status Profile Management	Diagnostics		
CISCO SYSTEMS			
utilituutilitu 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	



Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Hinweis: Lesen Sie <u>Wichtige Informationen</u> zu <u>Debug-Befehlen</u>, bevor Sie **Debug-**Befehle verwenden.

Sie können die folgenden Befehle verwenden, um Fehler in Ihrer Konfiguration zu beheben.

 show wlan wlan_id: Zeigt den Status der Webumleitungsfunktionen f
ür ein bestimmtes WLAN an.Hier ein Beispiel:

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: Aktiviert das Debuggen von 802.1x-Paketnachrichten.Hier ein Beispiel:

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)
 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 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 - Aktiviert die Debug-Ausgabe aller aaa-Ereignisse. Hier ein Beispiel:

 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
        qosLevel: -1, dscp: 0xfffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
        dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
        vlanIfName: '', aclName: '
```

Zugehörige Informationen

- <u>Cisco Wireless LAN Controller Configuration Guide, Release 5.0</u>
- Konfigurationsbeispiel f
 ür Web-Authentifizierung des Wireless LAN-Controllers
- Konfigurationsbeispiel für externe Web-Authentifizierung mit Wireless LAN-Controllern
- <u>Seite zur Wireless-Unterstützung</u>
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.