Wi-Fi Protected Access (WPA) in einem Cisco Unified Wireless Network -Konfigurationsbeispiel

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen WPA- und WPA2-Unterstützung Netzwerkeinrichtung Konfigurieren der Geräte für den WPA2 Enterprise-Modus Konfigurieren des WLC für die RADIUS-Authentifizierung über einen externen RADIUS-Server WLAN für WPA2 Enterprise-Betriebsmodus konfigurieren Konfigurieren des RADIUS-Servers für die WPA2-Authentifizierung im Enterprise-Modus (EAP-FAST) Konfigurieren des Wireless-Clients für den WPA2 Enterprise-Betriebsmodus Konfigurieren der Geräte für den persönlichen WPA2-Modus Fehlerbehebung Zugehörige Informationen

Einleitung

In diesem Dokument wird die Konfiguration von Wi-Fi Protected Access (WPA) in einem Cisco Unified Wireless Network beschrieben.

Voraussetzungen

Anforderungen

Vergewissern Sie sich, dass Sie vor der Konfiguration über grundlegende Kenntnisse in diesen Themen verfügen:

- WPA
- Wireless LAN (WLAN) Sicherheitslösungen Hinweis: Weitere Informationen zu Cisco WLAN-Sicherheitslösungen finden Sie unter <u>Cisco Wireless LAN Security Overview (Cisco</u> zur <u>Wireless LAN-Sicherheit - Überblick</u>).

Verwendete Komponenten

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

- Cisco Lightweight Access Point der Serie 1000 (LAP)
- Cisco 4404 Wireless LAN Controller (WLC) mit Firmware 4.2.61.0
- Cisco 802.11a/b/g-Client-Adapter für Firmware 4.1
- Aironet Desktop Utility (ADU) für die Ausführung von Firmware 4.1
- Cisco Secure ACS Server Version 4.1

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</u> (Technische Tipps von Cisco zu Konventionen).

WPA- und WPA2-Unterstützung

Das Cisco Unified Wireless Network unterstützt die Wi-Fi Alliance-Zertifizierungen WPA und WPA2. WPA wurde 2003 von der Wi-Fi Alliance eingeführt. WPA2 wurde 2004 von der Wi-Fi Alliance eingeführt. Alle Produkte, die für WPA2 Wi-Fi zertifiziert sind, müssen mit Produkten kompatibel sein, die für WPA Wi-Fi zertifiziert sind.

WPA und WPA2 bieten Endbenutzern und Netzwerkadministratoren ein hohes Maß an Sicherheit, dass ihre Daten privat bleiben und der Zugriff auf ihre Netzwerke auf autorisierte Benutzer beschränkt wird. Beide verfügen über eine persönliche und eine unternehmensweite Arbeitsweise, die den unterschiedlichen Bedürfnissen der beiden Marktsegmente gerecht wird. Im Enterprise-Modus werden jeweils IEEE 802.1X und EAP für die Authentifizierung verwendet. Der persönliche Modus jedes Benutzers verwendet PSK (Pre-Shared Key) für die Authentifizierung. Cisco empfiehlt keinen persönlichen Modus für Unternehmens- oder Regierungsbereitstellungen, da ein PSK für die Benutzerauthentifizierung verwendet wird. PSK ist für Unternehmensumgebungen nicht sicher.

WPA behebt alle bekannten WEP-Schwachstellen in der ursprünglichen IEEE 802.11-Sicherheitsimplementierung und stellt damit eine sofortige Sicherheitslösung für WLANs sowohl in Umgebungen für kleine Büros und Heimbüros (SOHO) dar. WPA verwendet TKIP für die Verschlüsselung.

WPA2 ist die nächste Generation der Wi-Fi-Sicherheit. Es handelt sich um die interoperable Implementierung des ratifizierten IEEE 802.11i-Standards durch die Wi-Fi Alliance. Es implementiert den vom National Institute of Standards and Technology (NIST) empfohlenen AES-Verschlüsselungsalgorithmus unter Verwendung des Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). WPA2 vereinfacht die Einhaltung von FIPS 140-2 durch Behörden.

Vergleich der WPA- und WPA2-Modustypen

	WPA	WPA2
Enterprise-Modus (Unternehmen, Behörden, Bildungswesen)	 Authentifiz ierung: IEEE 802.1X/EA P Verschlüs selung: TKIP/MIC 	 Authentifiz ierung: IEEE 802.1X/E AP Verschlüs selung: AES- CCMP
Persönlicher Modus (SOHO, Home/Personal)	 Authentifiz ierung: PSK Verschlüs selung: TKIP/MIC 	 Authentifiz ierung: PSK Verschlüs selung: AES- CCMP

Im Enterprise-Betriebsmodus verwenden sowohl WPA als auch WPA2 802.1X/EAP für die Authentifizierung. 802.1X bietet WLANs eine starke gegenseitige Authentifizierung zwischen einem Client und einem Authentifizierungsserver. Darüber hinaus bietet 802.1X dynamische Verschlüsselungsschlüssel für einzelne Benutzer und Sitzungen. So entfallen der Verwaltungsaufwand und Sicherheitsprobleme im Zusammenhang mit statischen Verschlüsselungsschlüsseln.

Mit 802.1X werden die für die Authentifizierung verwendeten Anmeldeinformationen, z. B. Anmeldekennwörter, niemals unverschlüsselt oder unverschlüsselt über das Wireless-Medium übertragen. Während 802.1X-Authentifizierungstypen eine starke Authentifizierung für WLANs bieten, sind TKIP oder AES für die Verschlüsselung zusätzlich zu 802.1X erforderlich, da die standardmäßige 802.11-WEP-Verschlüsselung anfällig für Netzwerkangriffe ist.

Es gibt mehrere 802.1X-Authentifizierungstypen, die jeweils einen anderen Authentifizierungsansatz bieten und für die Kommunikation zwischen einem Client und einem Access Point auf demselben Framework und EAP basieren. Cisco Aironet-Produkte unterstützen mehr 802.1X-EAP-Authentifizierungstypen als alle anderen WLAN-Produkte. Folgende Typen werden unterstützt:

- <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-SIM (Subscriber Identity Module)

Ein weiterer Vorteil der 802.1X-Authentifizierung ist die zentrale Verwaltung für WLAN-Benutzergruppen, einschließlich richtlinienbasierter Schlüsselrotation, dynamischer Schlüsselzuweisung, dynamischer VLAN-Zuweisung und SSID-Einschränkung. Diese Funktionen sorgen für eine Rotation der Verschlüsselungsschlüssel.

Im Personal-Modus wird ein vorinstallierter Schlüssel (Passwort) für die Authentifizierung verwendet. Für den persönlichen Modus sind nur ein Access Point und ein Client-Gerät

erforderlich, während für den Enterprise-Modus in der Regel ein RADIUS oder ein anderer Authentifizierungsserver im Netzwerk erforderlich ist.

Dieses Dokument enthält Beispiele für die Konfiguration von WPA2 (Enterprise-Modus) und WPA2-PSK (Personal-Modus) in einem Cisco Unified Wireless-Netzwerk.

Netzwerkeinrichtung

In dieser Konfiguration sind ein Cisco 4404 WLC und ein Cisco LAP der Serie 1000 über einen Layer-2-Switch verbunden. Ein externer RADIUS-Server (Cisco Secure ACS) ist ebenfalls mit demselben Switch verbunden. Alle Geräte befinden sich im gleichen Subnetz. Der Access Point (LAP) wird zunächst beim Controller registriert. Es müssen zwei Wireless LANs erstellt werden, eines für den WPA2 Enterprise-Modus und das andere für den WPA2 Personal-Modus.

WPA2-Enterprise-Modus WLAN (SSID: WPA2-Enterprise) verwendet EAP-FAST für die Authentifizierung der Wireless-Clients und AES für die Verschlüsselung. Der Cisco Secure ACS-Server wird als externer RADIUS-Server für die Authentifizierung der Wireless-Clients verwendet.

WPA2-Personal-Modus WLAN (SSID: WPA2-PSK) verwendet WPA2-PSK für die Authentifizierung mit dem Pre-Shared Key "abcdefghijk".

Sie müssen die Geräte für diese Konfiguration konfigurieren:



WLC AP Manager IP address: Wireless Client IP address:	10.77.244.205 10.77.244.221
Cisco Secure ACS server IP address	10.77.244.196
Subnet Mask used in this example	255.255.255.224

Konfigurieren der Geräte für den WPA2 Enterprise-Modus

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

Führen Sie die folgenden Schritte aus, um die Geräte für den Betriebsmodus von WPA2 Enterprise zu konfigurieren:

- 1. <u>Konfigurieren des WLC für die RADIUS-Authentifizierung über einen externen RADIUS-</u> <u>Server</u>
- 2. Konfigurieren des WLAN für die WPA2-Authentifizierung im Enterprise-Modus (EAP-FAST)
- 3. Konfigurieren des Wireless-Clients für den WPA2-Enterprise-Modus

Konfigurieren des WLC für die RADIUS-Authentifizierung über einen externen RADIUS-Server

Der WLC muss konfiguriert werden, um die Benutzeranmeldeinformationen an einen externen RADIUS-Server weiterzuleiten. Der externe RADIUS-Server validiert dann die Benutzeranmeldeinformationen mithilfe von EAP-FAST und ermöglicht den Zugriff auf die Wireless-Clients.

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. Klicken Sie anschließend 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-NummerServerstatusIn diesem Dokument wird der ACS-Server mit der IP-Adresse 10.77.244.196 verwendet.

ahaha					Sage Co	nfiguration Ping	Logout Befresh
CISCO	MONITOR WLANS CONTRO	LLER WIRELESS S	ECURITY	MANAGEMENT	COMMANDS	нецр	
Security	RADIUS Authentication S	ervers > New				< Back	Apply
T AAA General	Server Index (Priority)	1					
	Server IPAddress	10.77.244.196		1			
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)	oustomers a	nd requires a key	wrap compliant	RADIUS server)	
Priority Order	Port Number	1812					
▶ 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	R Enable					
	Management	Enable					
	IPSec	Enable					

3. Klicken Sie auf Apply (Anwenden).

WLAN für WPA2 Enterprise-Betriebsmodus konfigurieren

Konfigurieren Sie anschließend das WLAN, das die Clients für die Verbindung mit dem Wireless-Netzwerk verwenden. Die WLAN-SSID für den WPA2-Enterprise-Modus lautet WPA2-Enterprise. In diesem Beispiel wird dieses WLAN der Verwaltungsschnittstelle zugewiesen.

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.
- Geben Sie auf der Seite WLANs > New (WLANs > Neu) den WLAN-SSID-Namen und den Profilnamen ein. Klicken Sie anschließend auf Apply. In diesem Beispiel wird WPA2-Enterprise als SSID

ve	rw	er	١d	e	ŀ
10			i u		

						Sa <u>v</u> e Co	nfiguration Bing	Logout Befr
cisco	MONITOR WLA	Ns CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs > New	r					< Back	Apply
WLANS	Туре	WLAN						
▶ Advanced	Profile Name	WPA2-Ent	terprise					
	WLAN SSID	WPA2-En	terprise					

4. Nachdem Sie ein neues WLAN erstellt haben, 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.

- 5. Aktivieren Sie unter General Policies (Allgemeine Richtlinien) das Kontrollkästchen Status, um das WLAN zu
 - aktivieren.

alulu							Sage Co	onfiguration E	ing Logout <u>R</u> efresh
CISCO	MONITOR	WLANS Q	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs>	Edit						< Bac	k Apply
T WI AND	General	Security	Qo5	Advanced					
 ₩LANS WLANS > Advanced 	Profile Type SSID Status Securit Radio F Interfa Broado	y Policies folicy ce est SSID	WPA2-Er WLAN WPA2-Er Modifical (Modifical Manage R Enabl	Iterprise Iterprise led [Auth(802.1X isens done unde ment = ed)] r security tab	will appear after a	pplying the chan	ges.)	
	Foot Not 1 CKIP Is 2 Web Poi 3 H-REAP 4 When Cl 5 Client M	es hot supported hor cannot be Local Switchin ient exclusion IP is not active	by I0xx mod used in comb g is not suppo is enabled, a e unless WPA	el APx ination with IPs vted with IPsex Timeout Value 2 is configured	ec , CRANITE aut of zero means	hentication infinity (will requi	re administrative	override to rese	et excluded clients)

- 6. Wenn der Access Point die SSID in den Beacon-Frames übertragen soll, aktivieren Sie das Kontrollkästchen **Broadcast SSID**.
- 7. Klicken Sie auf die Registerkarte **Sicherheit**. Wählen Sie unter Layer 2 Security (Layer 2-Sicherheit) **WPA+WPA2 aus**.Dadurch wird die WPA-Authentifizierung für das WLAN aktiviert.

alialia	Sa <u>v</u> a Configuration <u>P</u> ing Logout	<u>R</u> efresh
WLANs	MONITOR WLANS CONTROLLER WIRELESS SECORITY MANAGEMENT COMMANDS HELP WLANS>Edit CBack A	pply
 WLANS WLANS Advanced 	General Security QoS Advanced Layer 2 Layer 3 AAA Servers Layer 2 Security WPA+WPA2 Image: Comparison of the security MAC Filtering Static WEP Parameters MAC Filtering Static WEP Parameters Static Key (Key Index = 0) Type Type Key Size Key Index Encryption Key Allow Shared Key Image: Comparison of the security Enabled	
	CKIP Parameters 4 002.11 Data Encryption Current Key: 0 bits CKIP Key (Key Index= 0) Key Size Key Index Inot set I Image: Second Secon	intx)

 Blättern Sie auf der Seite nach unten, um die WPA+WPA2-Parameter zu ändern. In diesem Beispiel sind die WPA2-Richtlinie und die AES-Verschlüsselung ausgewählt.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	Eng Logout Betresh
WLANS WLANS WLANS Advanced	WLANS > Edit General Security QoS Advanced Layer 2 Layer 3 AAA Servers 002.11 Data Encryption Current Key: 0 bits CKIP Key (Key Index= 0) Key Size Key Index Encryption Key NMMi Mode Enabled Key Permutation Enabled 802.11 Data Encryption Type Key Nermutation Enabled 802.11 Data Encryption Type WPA+WPA2 Parameters @ WEP WPA2 Policy @ WPA2 Policy @ WPA2 Encryption AES VPA2 Encryption AES VPA2 Policy @ VPA2 Encryption AES VPA B02.1X VPA2 Encryption AES VPA2 Encryption VPA2 State of the state	Back Apply

- 9. Wählen Sie unter Auth Key Mgmt (Authentifizierungstastenverwaltung) die Option **802.1x aus**.Dadurch wird WPA2 mit 802.1x/EAP-Authentifizierung und AES-Verschlüsselung für das WLAN aktiviert.
- 10. Klicken Sie auf die Registerkarte AAA-Server. Wählen Sie unter Authentication Servers

(Authentifizierungsserver) die entsprechende Server-IP-Adresse aus. In diesem Beispiel wird 10.77.244.196 als RADIUS-Server

verwendet.

11. Klicken Sie auf Apply (Anwenden). Hinweis: Dies ist die einzige EAP-Einstellung, die auf dem Controller für die EAP-Authentifizierung konfiguriert werden muss. Alle anderen für EAP-FAST spezifischen Konfigurationen müssen auf dem RADIUS-Server und den zu authentifizierenden Clients vorgenommen werden.

Konfigurieren des RADIUS-Servers für die WPA2-Authentifizierung im Enterprise-Modus (EAP-FAST)

In diesem Beispiel wird Cisco Secure ACS als externer RADIUS-Server verwendet. Führen Sie die folgenden Schritte aus, um den RADIUS-Server für die EAP-FAST-Authentifizierung zu konfigurieren:

- 1. Erstellen einer Benutzerdatenbank zur Authentifizierung von Clients
- 2. <u>Hinzufügen des WLC als AAA-Client zum RADIUS-Server</u>
- Konfigurieren der EAP-FAST-Authentifizierung auf dem RADIUS-Server mit anonymer In-Band-PAC-Bereitstellung Hinweis: EAP-FAST kann entweder mit anonymer In-Band-PAC-Bereitstellung oder mit authentifizierter In-Band-PAC-Bereitstellung konfiguriert werden. In diesem Beispiel wird die anonyme In-Band-PAC-Bereitstellung verwendet. Ausführliche 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 externem RADIUS-Server.

Erstellen einer Benutzerdatenbank zur Authentifizierung von EAP-FAST-Clients

Führen Sie diese Schritte aus, um eine Benutzerdatenbank für EAP-FAST-Clients auf dem ACS zu erstellen. In diesem Beispiel werden der Benutzername und das Kennwort des EAP-FAST-Clients als User1 bzw. User1 konfiguriert.

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



 Konfigurieren Sie auf der Seite "User Setup Edit" (Benutzereinrichtung bearbeiten) 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.

ess [@] http://127.0.	0.1:1065/	
isco Svorems	User Setup	
adhaadha.	Edit	Help
User Setup	User: User1 (New User)	Account Disabled Deleting a Username
Setup SharedProfile Components	Account Disabled	Supplementary User Infe Password Authentikation Group to which the user is assigned
Network Configuration	Supplementary User Info 💡	Callback Client 3P. Address Assignment Advanced Settlings
System Configuration	Real Name Description	Network Access Restrictions Has Session Usage Destas Access Network
Interface Configuration		Account Unsets Devening adable AfLs Advanced TACACS+ Sections TACACS+ Control
Control External User Databases	User Setup	TACACS - Control Control TACACS - Control Parament TACACS - Outboard Parament TACACS - Outboard Parament TACACS - Solid Commund Authorization
Posture Validation	Password Authentication:	Command Authorization for Network Device Hanagement Applications TACACS + Unknown Services TIT RADIUS Attributes
Network Access Profiles	CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not	RADIUS Yeadar-Specific Attributes
Reports and Activity	Password •••••	Account Disabled Status
Documentation	Password	Safect the Account Disabled check bow to disable this account: clear the check box to enable the account.
	Separate (CHAP/MS-CHAP/ARAP) Dassword	[Back to Tep]
	Confirm	Deleting a Username The Delete botton area are solv when you are edition to existing over
	Submit Cancel	account not before appears and ding a new year account. To delete the current user account from the database, click Delete . When asked to

- 3. Wählen Sie **ACS Internal Database** aus dem Dropdown-Feld "Password Authentication" (Kennwortauthentifizierung) aus.
- 4. Konfigurieren Sie alle anderen erforderlichen Parameter, und klicken Sie auf Senden.

Hinzufügen des WLC als AAA-Client zum RADIUS-Server

Gehen Sie wie folgt vor, um den Controller als AAA-Client auf dem ACS-Server zu definieren:

- Klicken Sie in der ACS-GUI auf Network Configuration (Netzwerkkonfiguration). Klicken Sie im Abschnitt "AAA-Client hinzufügen" der Seite "Netzwerkkonfiguration" auf Eintrag hinzufügen, um den WLC als AAA-Client zum RADIUS-Server hinzuzufügen.
- Legen Sie auf der Seite AAA Client (AAA-Client) den Namen des WLC, die IP-Adresse, den gemeinsamen geheimen Schlüssel und die Authentifizierungsmethode (RADIUS/Cisco AirSpace) fest. Weitere Authentifizierungsserver, die nicht dem ACS angehören, finden Sie in der Dokumentation des Herstellers.

		5
lisco Systems	Network Configuration	2
User Setup	Edit	 Help AAA Clent Hestname.
Group Setup	Add AAA Client	AAA Gient IP Address Shared Secont Nativerk Device Group
Network	AAA Client Hostname WLC	BADUS Key Wrap Arthen Scatz Using Single Connect TACACS - AAA Client
System Configuration	AAA Client IP Address	Los Undats/Watchdog Packets from this AAA Client Log RADUS Tunneling Packets from this AAA Client
Interface Configuration	Shared Secret cisco	Replace RADIUS Part info with Username from this AAA Client Hatch Framed-IP-Address with user IP
Administration Centrol	RADIUS Key Wrap	addense for accounting packets from this AAA Client
External User Databases	Message Authenticator Code	AAA Client Hostname
Network Access	Key Input Format C ASCII @ Hexadecimal	The AAA Client Hostname is the name assigned to the AAA client.
Reports and Activity	Authenticate Using RADIUS (Cisco Airespace)	(back to Teo)
Online	Single Connect TACACS+ AAA Client (Record stop in accounting on failure)	AAA Client IP Address
- Conversion and	Log Update/Watchdog Packets from this AAA Client	The AAA Client IP Address is the IP address assigned to the
	Log RADIUS Tunneling Packets from this AAA Client	AAA client.
	Replace RADIUS Port info with Username from this AAA Client	If you want to designate more than one AAA client with a single
	\square Match Framed-IP-Address with user IP address for accounting packets from this AAA Client	AAA client entry in ACS, you can specify the IP address for each AAA client to be represented by this 4844 client entry. To

Hinweis: Der gemeinsam genutzte geheime Schlüssel, den Sie auf dem WLC und dem ACS-Server konfigurieren, muss übereinstimmen. Beim gemeinsamen geheimen Schlüssel wird zwischen Groß- und Kleinschreibung unterschieden.

3. Klicken Sie auf Senden+Anwenden.

Konfigurieren der EAP-FAST-Authentifizierung auf dem RADIUS-Server mit anonymer In-Band-PAC-Bereitstellung

Anonyme In-Band-Bereitstellung

Dies ist eine der beiden In-Band-Bereitstellungsmethoden, bei der der ACS eine gesicherte Verbindung mit dem Endbenutzer-Client herstellt, um dem Client eine neue PAC bereitzustellen. Diese Option ermöglicht einen anonymen TLS-Handshake zwischen dem Endbenutzer-Client und dem ACS.

Diese Methode wird in einem Authenticated Diffie-HellmanKey Agreement Protocol (ADHP)-Tunnel ausgeführt, bevor der Peer den ACS-Server authentifiziert.

Anschließend erfordert der ACS eine EAP-MS-CHAPv2-Authentifizierung des Benutzers. Bei erfolgreicher Benutzerauthentifizierung erstellt der ACS einen Diffie-Hellman-Tunnel mit dem Endbenutzer-Client. Der ACS generiert eine PAC für den Benutzer und sendet diese zusammen mit Informationen über diesen ACS an den Endbenutzer-Client in diesem Tunnel. Bei dieser Bereitstellungsmethode wird EAP-MSCHAPv2 als Authentifizierungsmethode in Phase Null und EAP-GTC in Phase zwei verwendet.

Da ein nicht authentifizierter Server bereitgestellt wird, ist es nicht möglich, ein unverschlüsseltes

Kennwort zu verwenden. Daher können im Tunnel nur MS-CHAP-Anmeldeinformationen verwendet werden. MS-CHAPv2 wird verwendet, um die Identität des Peers zu überprüfen und eine PAC für weitere Authentifizierungssitzungen zu empfangen (EAP-MS-CHAP wird nur als interne Methode verwendet).

Führen Sie die folgenden Schritte aus, um die EAP-FAST-Authentifizierung auf dem RADIUS-Server für die anonyme In-Band-Bereitstellung zu konfigurieren:

1. Klicken Sie in der RADIUS-Server-GUI auf **Systemkonfiguration**. Wählen Sie auf der Seite "System Configuration" die Option **Global Authentication Setup**

aus.		
ElscoSecure ACS -	Microsoft Internet Explorer	 1984 * 000
Address http://127.	0.0.1:1065/	• •
Address Antropy Provided Address Party Party Provided Address Party Pa	ACS Service Management ACS Service Management	Help Service Control Leopins Date Format Control Cost of Description Date Format Control Cost of Description Date Format Control Cost of Description Date Format Control Cost of Description Date Format Control Date Format Control
Posture Posture Panidedion Prodies Prodies Reports and Activity Documentation		Service Control Select to open the page from which you can stop or restart Cisco Secure ACS services. Iback to Top! Select to configure various Cisco Secure ACS reports and customize the type of information that is logged. [Back to Top] 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 Top]
1 Sant G	D Chron Service ACS - Mir	Thermet
a start	I COCOSCUPE WC2 - LUC	13 Lorm

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

ElscoSecure ACS -	Microsoft Internet Explorer	() ()
Address a http://127	0.0.1:1065/	• D 00
Cisco Systems	System Configuration	×
Ch Ultra	EAP Configuration	2 Help
Setup Setup Setup SharedShoff Configuration SuredShoff Configuration SuredShoff Configuration SuredShoff Sured SuredShoff SuredShoff	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 Binary comparison E Certificate Binary comparison EAP-TLS session timeout (minutes): 120 Cisco client initial message: PEAP session timeout (minutes): 120 Enable Fast Reconnect:	Use this page to specify settings for various authentication protocols. • EAP Configuration • PEAP • EAP-BAST • CAP-BS • EAP-BS • EAP-BS • EAP-BS • EAP-BS • EAP-BS • EAP-BS • EAP-BS • EAP Configuration EAP is a flexible request-response protocol for arbitrary authentication information (NFC 2284). EAP is layered on tap of another protocol such as UDP, DC2.1m or RADEUS and supports multiple "authentication" types. EAP to Tap]
Contemports and Activity Online Documentation	EAP-FAST EAP-FAST Configuration	PEAP is the outer layer protocol for the secure tunnel.
	EAP-TLS	Alexer AEAP is a cartificate-based authentication protocol. AEAP authentication can occur only after you have completed the required steps so 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- CHAPv2, such as Microsoft AD, and the ACS Internal Database.
	Submit Submit + Restart Cancel	1
		Internet
Start 10 8	Uscosecure ACS - Mic	7:58 PM

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

EiscoSecure AES - M	Skrosoft Internet Explorer	<u>-101 ×</u>
Ele Edt Yew Fav	ronites Iools Help	Lirks 🤲 🦓
Address http://127.0	0.0.1:1065/	💌 🛃 Go
Cinco Syntems	System Configuration	×
and to have to have a	EAP-FAST Configuration	- Help
User Setup		EAP-FAST Configuration Page
Group	EAP-FAST Settings	?
R Setup	EAP-FAST	Use this page to configure EAP-FAST authentication settings.
SharedProfile Components	R Allow EAP-FAST	EAP-EAST Settings
Markey I Markawark	Active master key TTI	Client initial message Authority ID Infe
Configuration	Pathod seater hay TT	 Allow anonymous in-band PAC previsioning
Sustem	Retired master key TTL 3 months	Allow as then ticated in-band PAC previsioning Allow machine as then tication
Con Consideration	Tunnel PAC TTL 1 weeks	Allow stateless session resume.
Configuration	Client initial message: tacwebacs	Allowed inser methods Certificate Comparison
	Authority ID Info: tacwebacs	 EAP-TLS session timeout (minutes)
Centrel	Allow approximates in-band BAC provisioning	CAPTAST master server Actual EAP-FAST server status
Deternal User	Allow authenticated in-band PAC provisioning	
	Accept cleat on withoutinated provisioning	EAP-FAST Settings
Validation	Descript client on addienticated provisioning	Allow EAP-FAST-To enable EAP-FAST authentication, select this check
Network Access	C cleve Machine Authentication	bes.
S Promet	La allow machine Authentication	Active Master Key TTL-Enter a value for the amount of time that a master
Activity	Machine PAC TTL 1 Weeks	time to live (TTL) defined for the Master Key expires, the master key is
and 1 Online	C Allow Stateless session resume	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
	Allowed inner methods	generated using a retired master key are acceptable for EAP-PAST authentication. When an end-user client gains network access using a PAC
	EAP-GTC	based on a retired master key, ACS sends a new PAC to the end-user client.
	EAP-MSCHAPv2	Tunnel PAC TR - Enter a value for the amount of time that a PAC is used
	EAP-TLS	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
	Submit Submit + Restart Cancel	automatic. If the master key used to generate the Tunnel PAC expired, automatic or manual provisioning must be used to provide the end-user clinest with a new DAC.
2)		internet
🍠 Start 🛛 🔂 🥭	CiscoSecure ACS - Mic	👮 7:58 PM

- 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.Weitere Informationen zu aktiven und zurückgezogenen Hauptschlüsseln finden Sie unter Hauptschlüssel. Weitere Informationen finden Sie auch unter Hauptschlüssel und PAC-TTLs.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. Allowed inner methods (Zugelassene interne Methoden) Diese Option bestimmt, 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.

Konfigurieren des Wireless-Clients für den WPA2 Enterprise-Betriebsmodus

Im nächsten Schritt wird der Wireless-Client für den WPA2 Enterprise-Betriebsmodus konfiguriert.

Führen Sie diese Schritte aus, um den Wireless-Client für den WPA2 Enterprise-Modus zu

konfigurieren.

- Klicken Sie im Fenster von Aironet Desktop Utility auf Profile Management > New, um ein Profil f
 ür den WPA2-Enterprise WLAN-Benutzer zu erstellen.Wie bereits erwähnt, verwendet dieses Dokument den WLAN/SSID-Namen als WPA2-Enterprise f
 ür den Wireless-Client.
- Klicken Sie im Fenster Profilverwaltung auf die Registerkarte Allgemein, und konfigurieren Sie Profilname, Client-Name und SSID-Namen wie in diesem Beispiel gezeigt. Klicken Sie dann auf

JK		
Profile Management		2 🔀
General Security Advance	be	
Profile Settings Profile Name:	WPA2-Enterprise	
Client Name:	Wireless-Client1	
Network Names		
SSID1:	WPA2-Enterprise	
SSID2:		
SSID3:		
		OK Cancel

 Klicken Sie auf die Registerkarte Sicherheit, und wählen Sie WPA/WPA2/CCKM aus, um den WPA2-Betriebsmodus zu aktivieren. Wählen Sie unter WPA/WPA2/CCKM EAP Type die Option EAP-FAST aus. Klicken Sie auf Konfigurieren, um die EAP-FAST-Einstellung zu konfigurieren.

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	
	OK C	ancel

4. Aktivieren Sie im Fenster Configure EAP-FAST (EAP-FAST konfigurieren) das Kontrollkästchen Allow Automatic PAC Provisioning (Automatische PAC-Bereitstellung zulassen). Wenn Sie die anonyme PAC-Bereitstellung konfigurieren möchten, wird EAP-MS-CHAP als einzige interne Methode in Phase Null verwendet.

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

- 5. Wählen Sie im Dropdown-Feld EAP-FAST Authentication Method den Benutzernamen und das Kennwort für MSCHAPv2 als Authentifizierungsmethode aus. Klicken Sie auf **Configure** (Konfigurieren).
- 6. Wählen Sie im Fenster MSCHAPv2-Benutzername und -Kennwort konfigurieren die entsprechenden Einstellungen für Benutzername und Kennwort aus. In diesem Beispiel wird Automatically Prompt (Automatisch nach Benutzername und Kennwort fragen) ausgewählt.

ted Root Certification Au	uthorities
ηγ>	×
er Name and Password S	ettings
 Use Temporary Use 	r Name and Password
O Use Windows I	User Name and Password
 Automatically F 	rompt for User Name and Password
O Manually Prom	pt for User Name and Password
🔘 Use Saved User Nar	me and Password
User Name:	Administrator
Password:	
Password: Confirm Password:	
Password: Confirm Password: Domain:	
Password: Confirm Password: Domain:	

erselbe Benutzername und dasselbe Kennwort sollten im ACS registriert werden. Wie bereits erwähnt, wird in diesem Beispiel User1 bzw. User1 als Benutzername und Kennwort verwendet. Beachten Sie außerdem, dass es sich um eine anonyme In-Band-Bereitstellung handelt. Daher kann der Client das Serverzertifikat nicht validieren. Stellen Sie sicher, dass das Kontrollkästchen Serveridentität überprüfen deaktiviert ist.

7. Klicken Sie auf OK.

Betriebsmodus von WPA2 Enterprise überprüfen

Führen Sie die folgenden Schritte aus, um zu überprüfen, ob die WPA2 Enterprise-Moduskonfiguration ordnungsgemäß funktioniert:

- 1. Wählen Sie im Fenster "Aironet Desktop Utility" das Profil **WPA2-Enterprise aus,** und klicken Sie auf **Activate (Aktivieren)**, um das Profil des Wireless-Clients zu aktivieren.
- 2. Wenn Sie MS-CHAP ver2 als Authentifizierung aktiviert haben, fordert der Client die Eingabe

von Benutzername und Kennwort

network	Ar THOT decinance and passificita to log on to the Micloss
User Name :	User1
Password :	••••
Log on to :	
Card Name :	Cisco Aironet 802.11a/b/g Wireless Adapter
Profile Name :	WPA-Enterprise

3. Während der EAP-FAST-Verarbeitung des Benutzers werden Sie vom Client aufgefordert, PAC vom RADIUS-Server anzufordern. Wenn Sie auf **Ja** klicken, wird die PAC-Bereitstellung gestartet.

EAP-FAST Authentication	×
You do not have a valid PAC from the authentication server. Do you want to proceed and request automatic provisioning?	
Yes No	

4. Nach der erfolgreichen PAC-Bereitstellung in Phase Null folgen Phase eins und zwei, und es findet eine erfolgreiche Authentifizierung statt.Nach erfolgreicher Authentifizierung wird der Wireless Client dem WLAN WPA2-Enterprise zugeordnet. Hier der Screenshot:

😤 Cisco Aironet Desktop Utility	y - Current Profile: WP	A2-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

Sie können auch überprüfen, ob der RADIUS-Server die Authentifizierungsanforderung vom Wireless-Client empfängt und validiert. Überprüfen Sie dazu die Berichte "Bestanden Authentifizierungen" und "Fehlgeschlagene Versuche" auf dem ACS-Server. Diese Berichte stehen unter "Berichte und Aktivitäten" auf dem ACS-Server zur Verfügung.

Konfigurieren der Geräte für den persönlichen WPA2-Modus

Führen Sie die folgenden Schritte aus, um die Geräte für den Betriebsmodus von WPA2-Personal zu konfigurieren:

- 1. WLAN für die WPA2 Personal Mode-Authentifizierung konfigurieren
- 2. Konfigurieren des Wireless-Clients für den persönlichen WPA2-Modus

Konfigurieren des WLAN für den persönlichen WPA2-Modus

Sie müssen das WLAN konfigurieren, das die Clients für die Verbindung mit dem Wireless-Netzwerk verwenden. Die WLAN-SSID für den WPA2 Personal-Modus ist WPA2-Personal. In diesem Beispiel wird dieses WLAN der Verwaltungsschnittstelle zugewiesen.

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.
- Geben Sie auf der Seite WLANs > New (WLAN > Neu) den WLAN-SSID-Namen, den Profilnamen und die WLAN-ID ein. Klicken Sie anschließend auf Apply. In diesem Beispiel wird WPA2-Personal als SSID verwendet.

						Sa <u>x</u> e Co	onfiguration <u>P</u> in	ig Logout <u>R</u> efresh
cisco	MONITOR WLAN	s <u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs > New						< Back	Apply
WLANS WLANS	Туре	WLAN	×					
▶ Advanced	Profile Name	WPA2-Pe	rsonal					
	WLAN SSID	WPA2-Pe	rsonal					

- 4. Nachdem Sie ein neues WLAN erstellt haben, 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.
- 5. Aktivieren Sie unter General Policies (Allgemeine Richtlinien) das Kontrollkästchen **Status**, um das WLAN zu aktivieren.
- 6. Wenn der Access Point die SSID in den Beacon-Frames übertragen soll, aktivieren Sie das Kontrollkästchen **Broadcast SSID**.
- 7. Klicken Sie auf die Registerkarte **Sicherheit**. Wählen Sie unter Layer Security (Layer-Sicherheit) **WPA+WPA2 aus**.Dadurch wird die WPA-Authentifizierung für das WLAN aktiviert.

- alaha-					Sage Co	onfiguration (<u>P</u> ing	Logout Befresh
CISCO	MONITOR WLANS CONTR	OLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs > Edit					< Back	Apply
- 101 4514	General Security	QoS Advanced					
WLANS	Layer 2 Layer 3	AAA Servers					
Advanced	Layer 2 Security WPA4	Current Key: Type Key Size WEP not set	104 bits WEI Key Index	P Static Key (Key 1 Encryption Key	ndex = 0)	Key Format	
	Allow Shared Key Authentication	Enabled					
	802.11 Data Encryption	Current Key: 0 8	its CKIP Key ((Key Index= 0)			
		Key Size Key not set 💌 1	Index Encr	yption Key	ĸ	ey Format ASCII 💌	
							_ <u>×</u>
	Foot Notes I CKIP is not supported by 10 2 Web Policy cannot be used 3 H-REAP Local Switching is in 4 When client exclusion is end 5 Client MFP is not active unle	hix model APs in combination with IPsec of supported with IPsec ibled, a Timeout Value iss WPA2 is configured	ic , CRANITE aut of zero means	hentication infinity (will requir	e administrative	override to reset e	xcluded clients)

- 8. Blättern Sie auf der Seite nach unten, um die WPA+WPA2-Parameter zu ändern. In diesem Beispiel sind die WPA2-Richtlinie und die AES-Verschlüsselung ausgewählt.
- 9. Wählen Sie unter Auth Key Mgmt (Authentifizierungstastenverwaltung) die Option **PSK** aus, um WPA2-PSK zu aktivieren.
- 10. Geben Sie den vorinstallierten Schlüssel wie dargestellt in das entsprechende Feld ein.

cisco	Sage Configuration) Bing Logout Befree MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	h
WLANS WLANS WLANS WLANS Advanced	Saye Configuration Engl Logout Befree MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP WLANS > Edit Apply General Security QoS Advanced Layer 2 Layer 3 AAA Servers Apply General Security QoS Advanced Apply General Security QoS Advanced	
	2 Web Policy cannot be used in combination with IPsec. 3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication 4 Wiben 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	

Hinweis: Der auf dem WLC verwendete vorinstallierte Schlüssel muss mit dem auf den Wireless-Clients konfigurierten Schlüssel übereinstimmen.

11. Klicken Sie auf Apply (Anwenden).

Konfigurieren des Wireless-Clients für den persönlichen WPA2-Modus

Der nächste Schritt besteht darin, den Wireless-Client für den WPA2-Personal-Betriebsmodus zu konfigurieren.

Führen Sie die folgenden Schritte aus, um den Wireless-Client für den WPA2-Personal-Modus zu konfigurieren:

- 1. Klicken Sie im Fenster von Aironet Desktop Utility auf **Profile Management > New,** um ein Profil für WPA2-PSK-WLAN-Benutzer zu erstellen.
- Klicken Sie im Fenster Profilverwaltung auf die Registerkarte Allgemein, und konfigurieren Sie Profilname, Client-Name und SSID-Namen wie in diesem Beispiel gezeigt. Klicken Sie dann auf OK.

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

3. Klicken Sie auf die Registerkarte **Sicherheit**, und wählen Sie **WPA/WPA2-Passphrase aus**, um den WPA2-PSK-Betriebsmodus zu aktivieren. Klicken Sie auf **Configure** (Konfigurieren), um den vorinstallierten WPA-PSK-Schlüssel zu konfigurieren.

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

4. Geben Sie den vorinstallierten Schlüssel ein, und klicken Sie auf OK

Configure WPA/WPA2 Passphrase	,
Enter a WPA/WPA2 passphrase (8 to 63	ASCII or 64 hexadecimal characters)
abcdefghijkl	
	OK Cancel

Betriebsmodus von WPA2-Personal überprüfen

Führen Sie die folgenden Schritte aus, um zu überprüfen, ob die WPA2-Enterprise-Moduskonfiguration ordnungsgemäß funktioniert:

- 1. Wählen Sie im Fenster von Aironet Desktop Utility das Profil **WPA2-Personal aus,** und klicken Sie auf **Activate (Aktivieren)**, um das Wireless-Client-Profil zu aktivieren.
- 2. Sobald das Profil aktiviert wurde, wird der Wireless-Client nach erfolgreicher Authentifizierung mit dem WLAN verknüpft.Hier der Screenshot:

🖻 Cisco Aironet Desktop Utility - Current Profile: WPA2-Personal 🛛 🔹 🛛					
Action Options Help					
Current Status Profile Management	Diagnostics				
CISCO SYSTEMS					
nullinIllin Profile Name:	WPA2-Personal				
Link Status:	Authenticated	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			

Fehlerbehebung

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

Die folgenden **Debug**-Befehle sind für die Fehlerbehebung der Konfiguration hilfreich:

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

 debug dot1x events enable: Aktiviert das Debuggen aller dot1x-Ereignisse. Nachfolgend finden Sie ein Beispiel für eine Debug-Ausgabe, die auf einer erfolgreichen Authentifizierung basiert: Hinweis: Einige der Zeilen aus dieser Ausgabe wurden aufgrund von Platzbeschränkungen in zweite Zeilen verschoben.

```
(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
```

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: Aktiviert das Debuggen von 802.1x-Paketnachrichten.
- debug aaa events enable Aktiviert die Debug-Ausgabe aller aaa-Ereignisse.

Zugehörige Informationen

- WPA2 Wi-Fi Protected Access 2
- EAP-FAST-Authentifizierung mit Wireless LAN-Controllern und Konfigurationsbeispiel eines <u>externen RADIUS-Servers</u>
- EAP-Authentifizierung mit WLAN-Controllern (WLC) Konfigurationsbeispiel
- <u>Übersicht über die WPA-Konfiguration</u>
- Support für Wireless-Produkte
- <u>Technischer Support und Dokumentation für Cisco Systeme</u>

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.