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

Inhalt

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 Cisco Wireless LAN Security Overview (Cisco zur Wireless LAN-Sicherheit - Überblick).

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 Cisco Technical Tips Conventions (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)	• Authentifizierung: IEEE 802.1X/EAP • Verschlüsselung: TKIP/MIC	• Authentifizierung: IEEE 802.1X/EAP • Verschlüsselung: AES-CCMP
Persönlicher Modus (SOHO, Home/Personal)	• Authentifizierung: PSK • Verschlüsselung: TKIP/MIC	• Authentifizierung: PSK • Verschlüsselung: 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:

- Cisco LEAP
- 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.

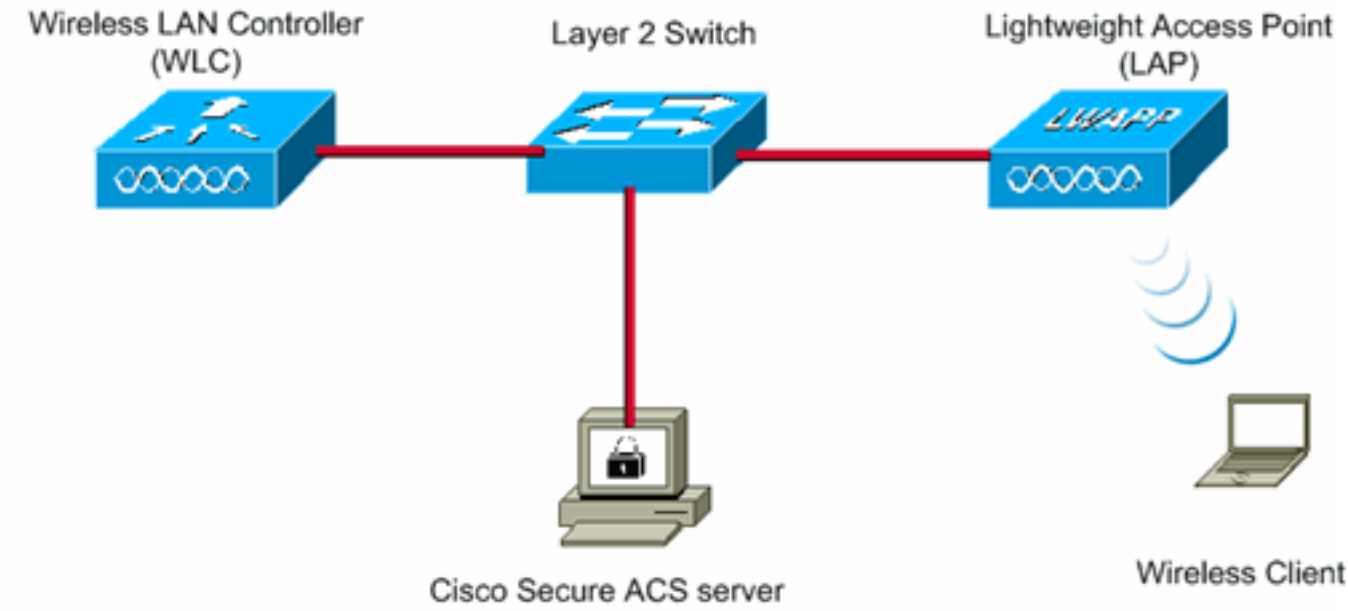
Netzwerkeinrichtung

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 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

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:

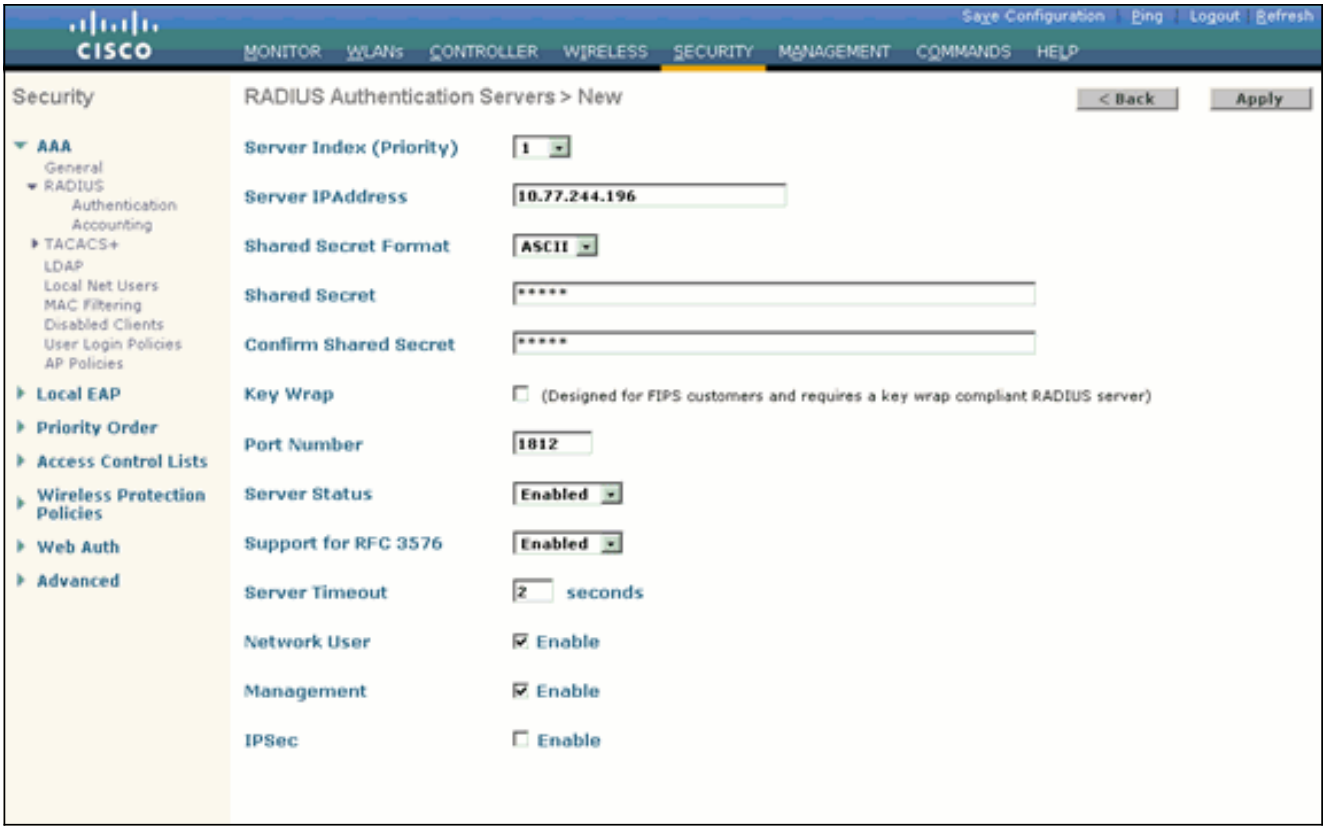
1. Konfigurieren des WLC für die RADIUS-Authentifizierung über einen externen RADIUS-Server
2. Konfigurieren des WLAN für die WPA2-Authentifizierung im Enterprise-Modus (EAP-FAST)
3. Konfigurieren des Wireless-Clients für den WPA2-Enterprise-Modus

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.
2. 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.



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.

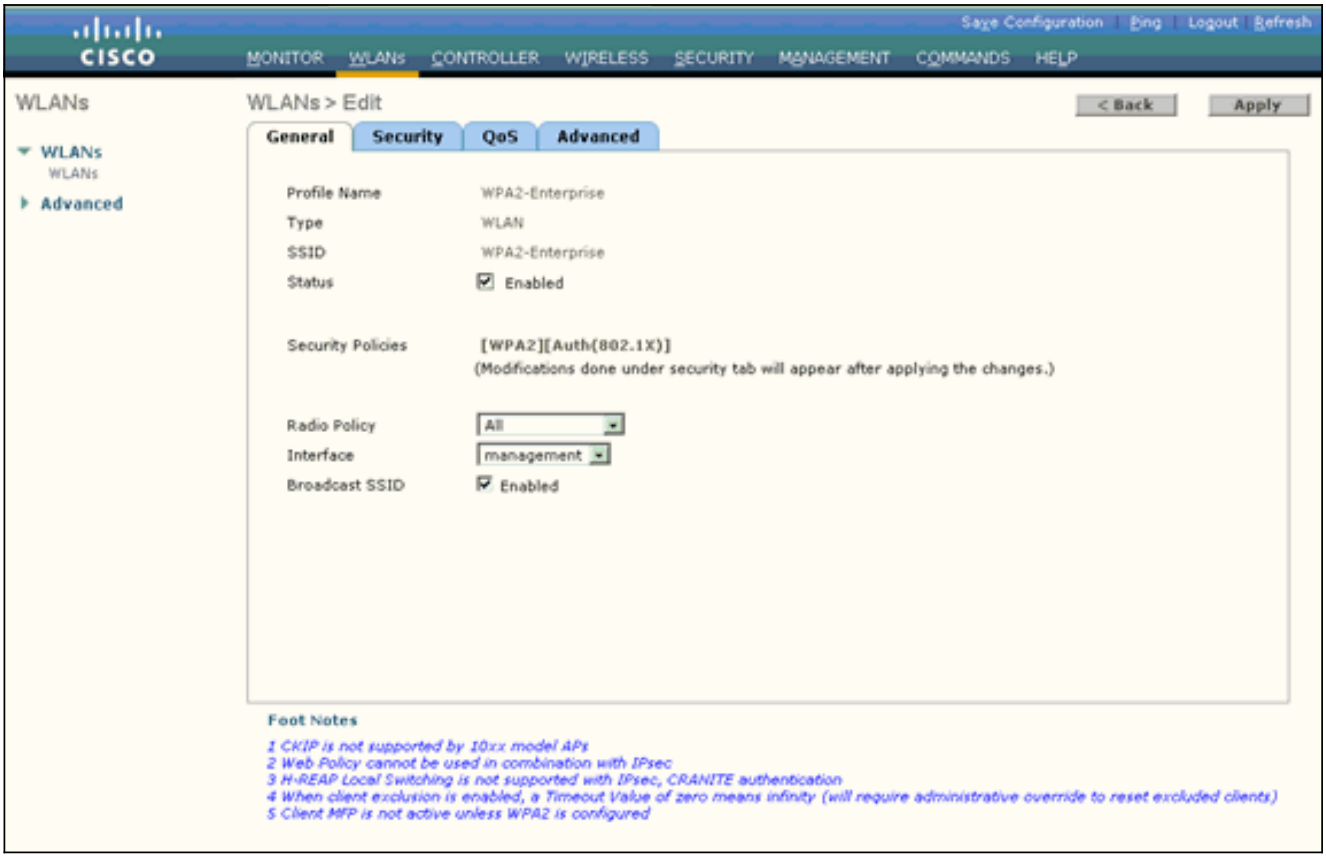
Gehen Sie wie folgt vor, um das WLAN und die zugehörigen Parameter zu konfigurieren:

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.
3. 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
verwendet.

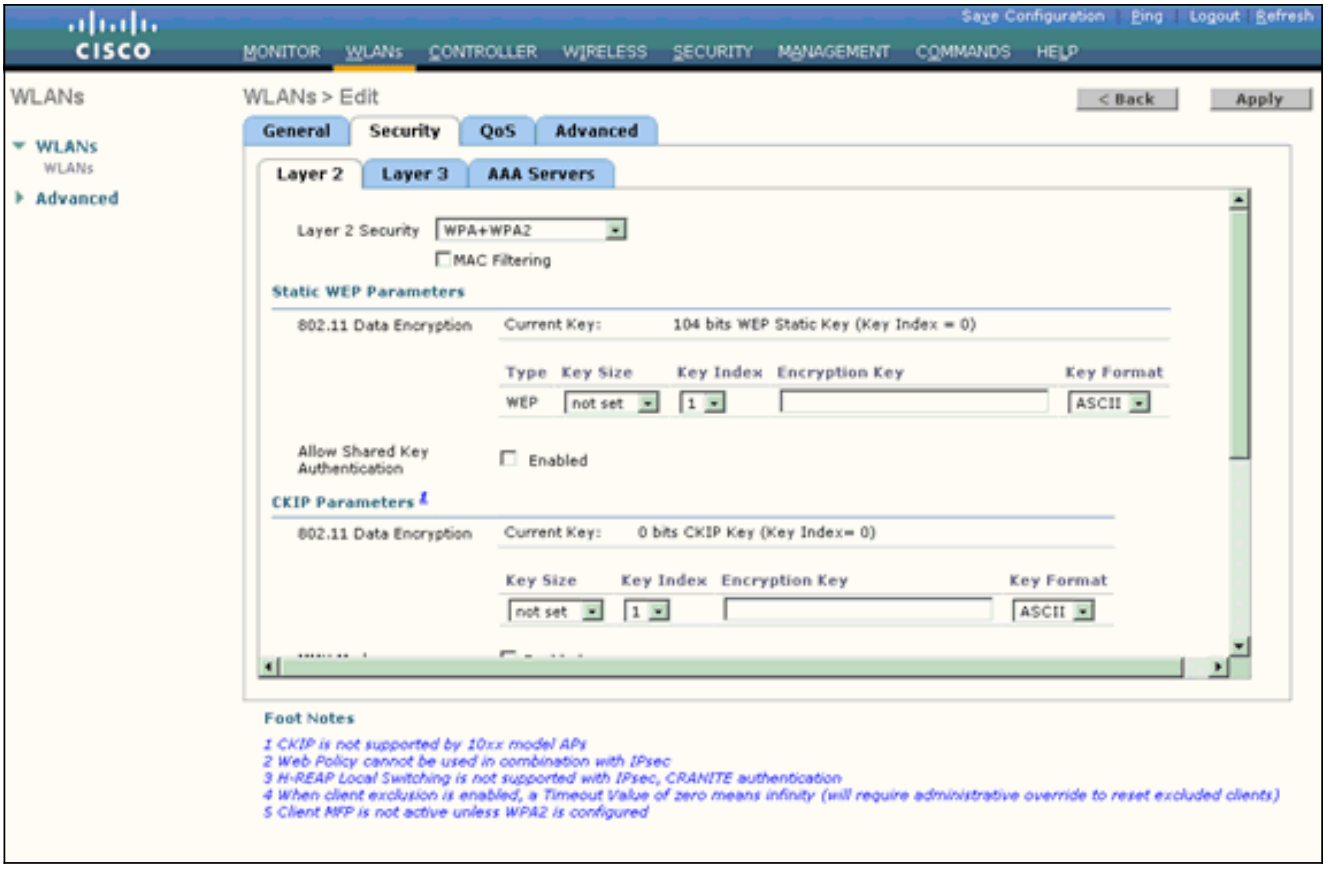
4. Nachdem Sie ein neues WLAN erstellt haben, wird die Seite **WLAN > Edit** (WLAN > Bearbeiten) für das neue WLAN angezeigt. Auf dieser Seite können Sie verschiedene

Parameter speziell für dieses WLAN definieren. Dies umfasst allgemeine Richtlinien, Sicherheitsrichtlinien, QoS-Richtlinien und erweiterte Parameter.

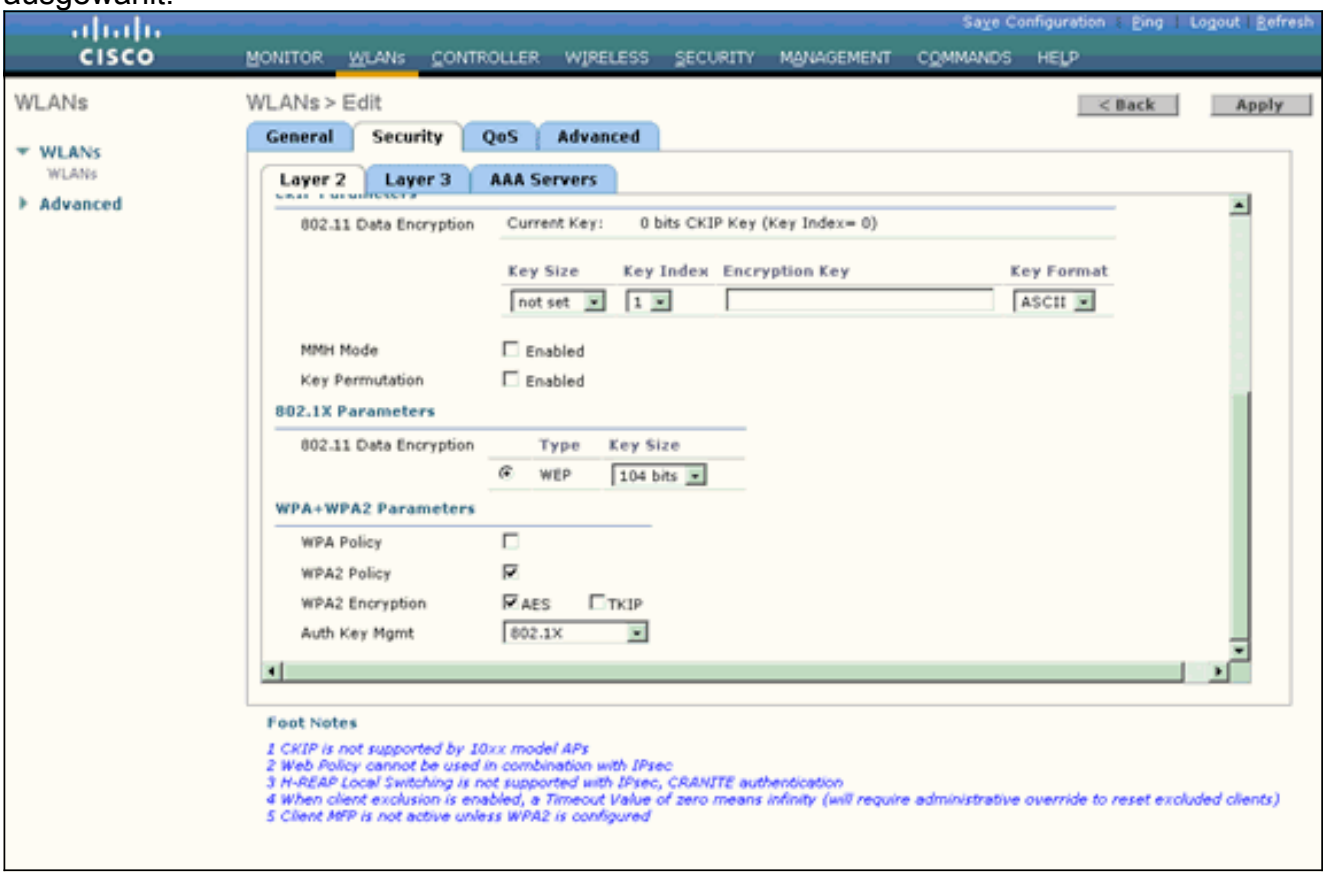
5. Aktivieren Sie unter General Policies (Allgemeine Richtlinien) das Kontrollkästchen **Status**, um das WLAN zu aktivieren.



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 2 Security (Layer 2-Sicherheit) **WPA+WPA2 aus**.Dadurch wird die WPA-Authentifizierung für das WLAN aktiviert.

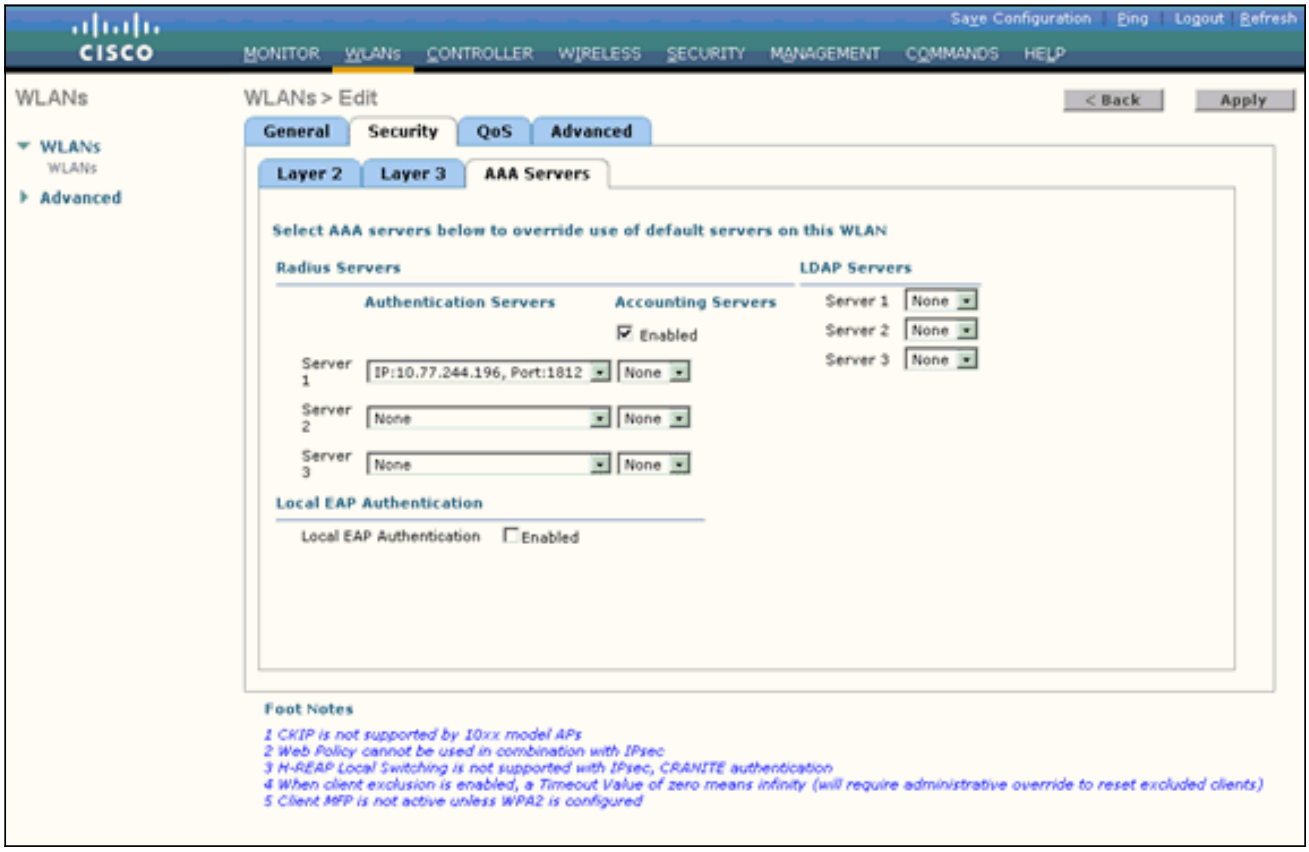


8. Blättern Sie auf der Seite nach unten, um die **WPA+WPA2-Parameter** zu ändern.In diesem Beispiel sind die WPA2-Richtlinie und die AES-Verschlüsselung ausgewählt.



9. Wählen Sie unter Auth Key Mgmt (Authentifizierungstastenverwaltung) die Option **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)

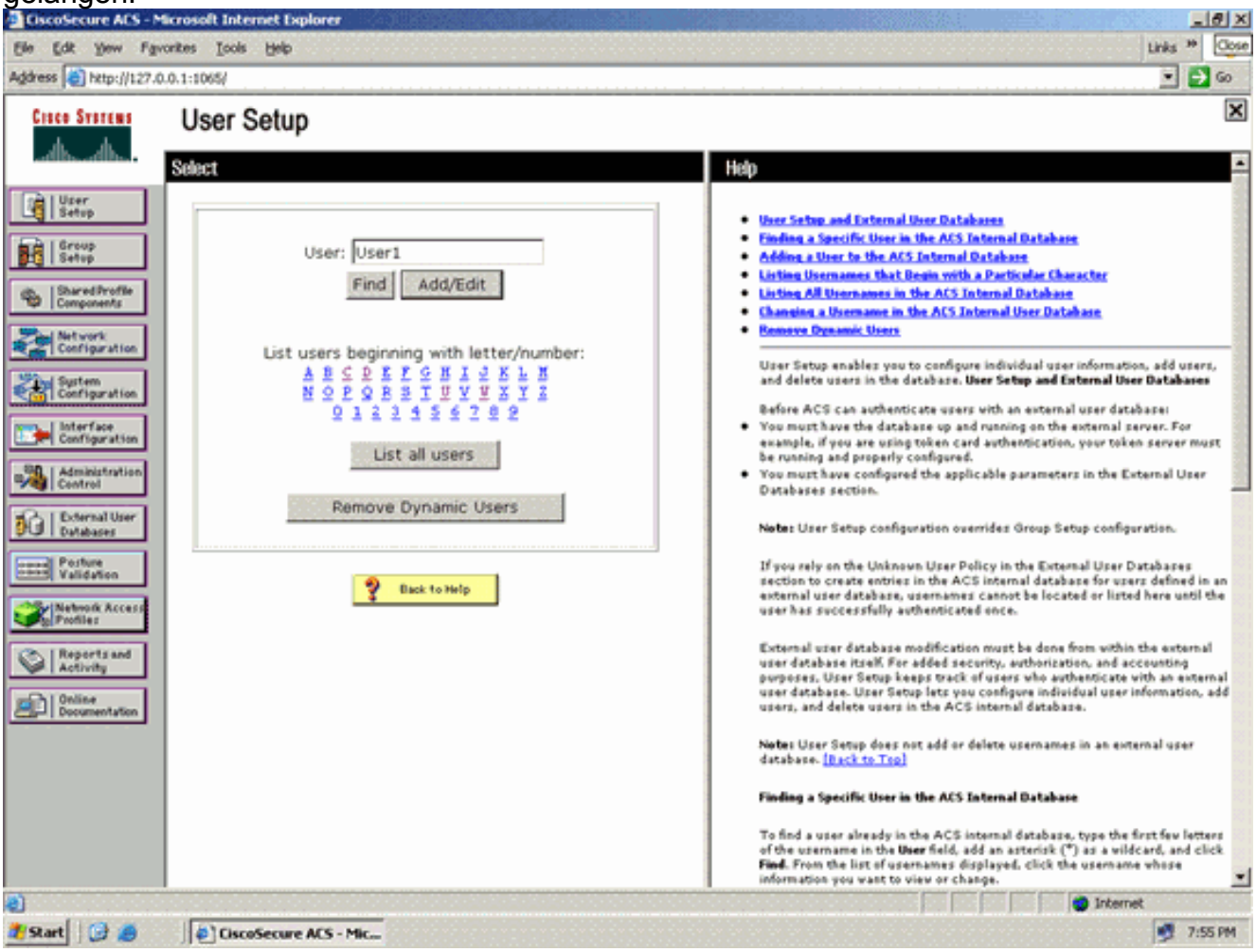
In diesem Beispiel wird Cisco Secure ACS als externer RADIUS-Server verwendet. Führen Sie die folgenden Schritte aus, um den RADIUS-Server für die EAP-FAST-Authentifizierung zu konfigurieren:

1. Erstellen einer Benutzerdatenbank zur Authentifizierung von Clients
2. Hinzufügen des WLC als AAA-Client zum RADIUS-Server
3. 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.

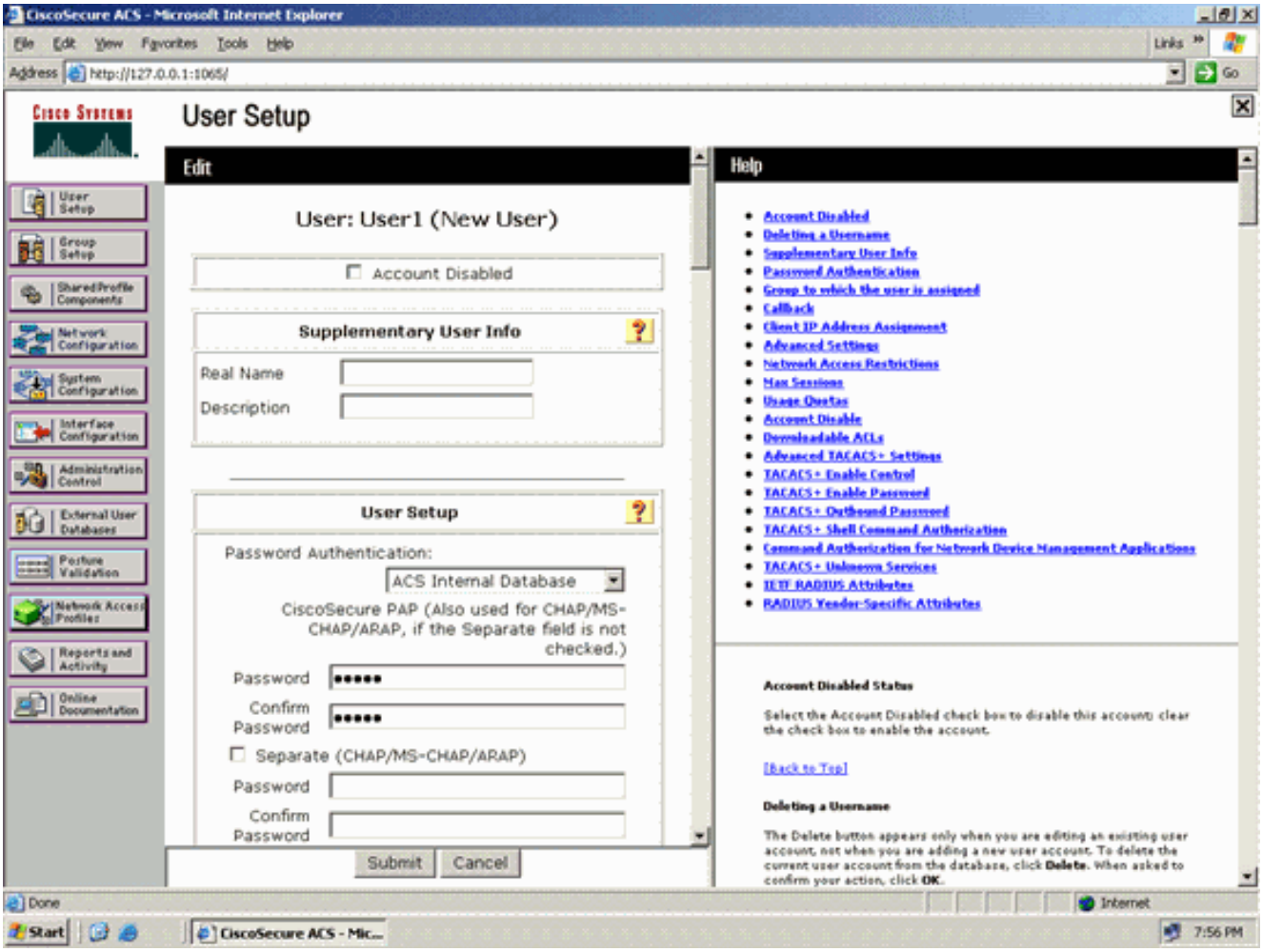
Erstellen einer Benutzerdatenbank zur Authentifizierung von EAP-FAST-Clients

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.

1. 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.



2. 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** für die Kennwortauthentifizierung
verwendet.

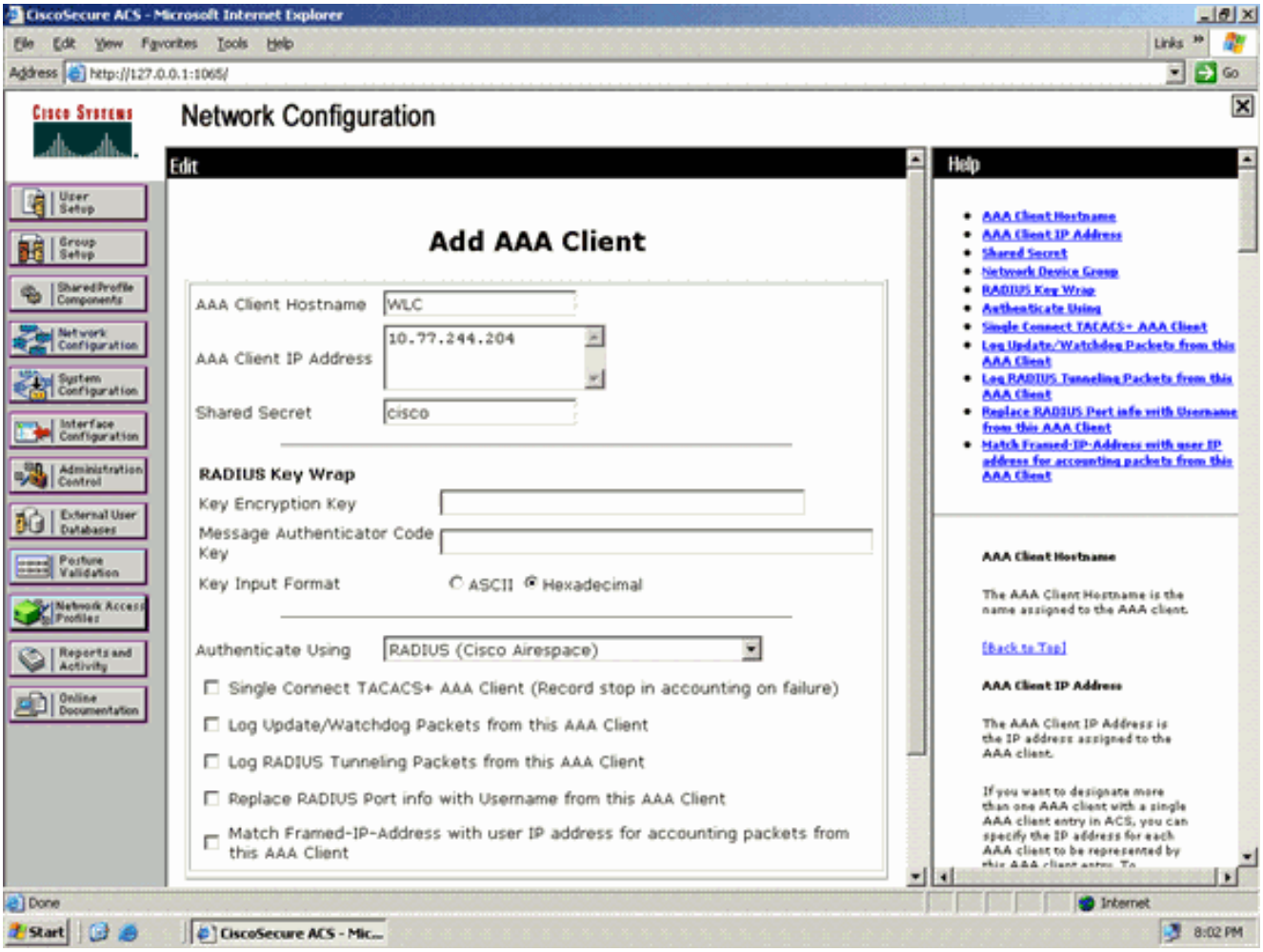


3. Wählen Sie **ACS Internal Database** aus dem Dropdown-Feld "Password Authentication" (Kennwortauthentifizierung) aus.
4. Konfigurieren Sie alle anderen erforderlichen Parameter, und klicken Sie auf **Senden**.

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:

1. 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.
2. 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.



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.

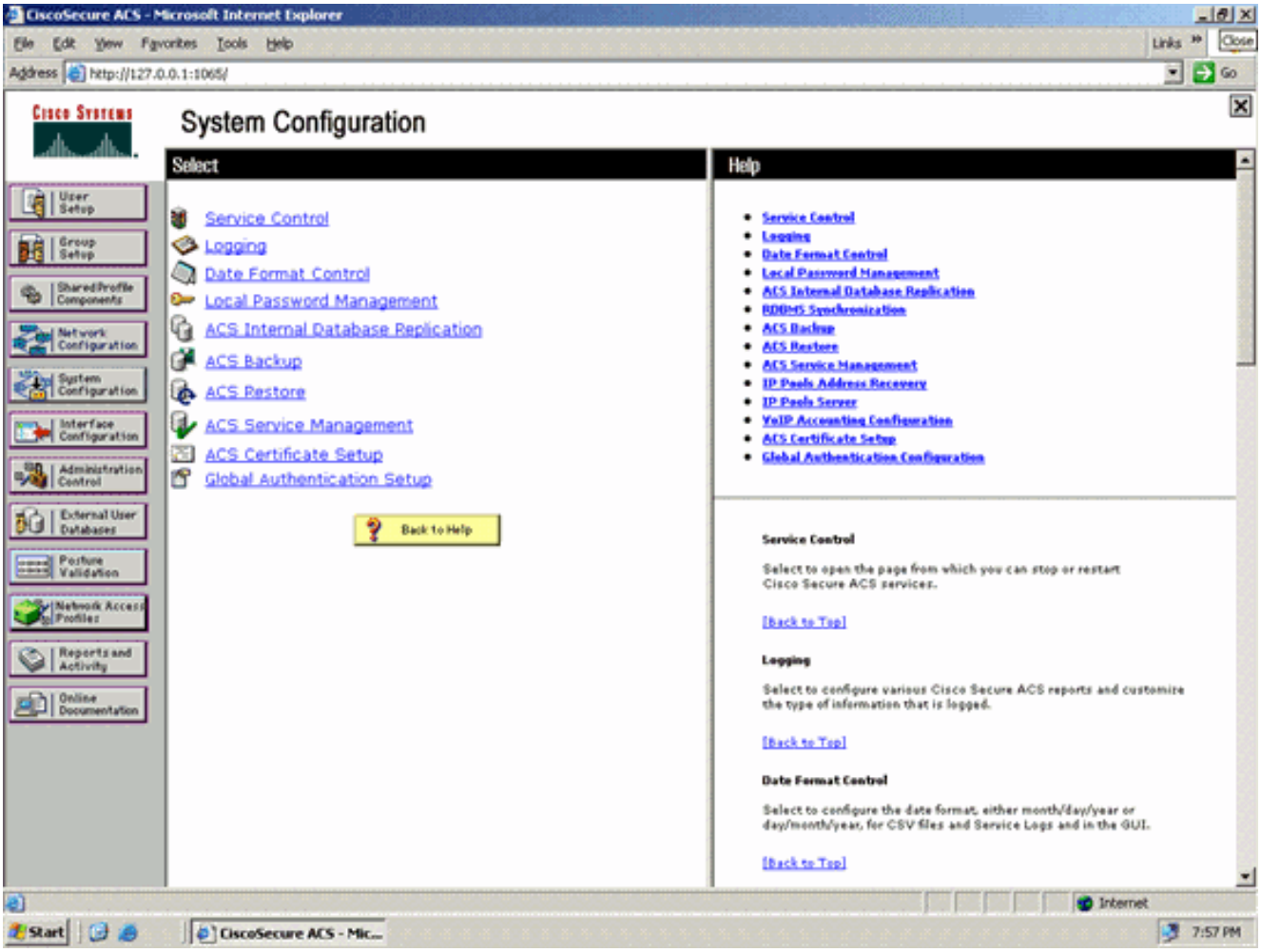
Anschließend erfordert der ACS eine EAP-MS-CHAPv2-Authentifizierung des Benutzers. Bei erfolgreicher Benutzerauthentifizierung erstellt der ACS einen Diffie-Hellman-Tunnel mit dem Endbenutzer-Client. Der ACS generiert eine PAC für den Benutzer und sendet diese zusammen mit Informationen über diesen ACS 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

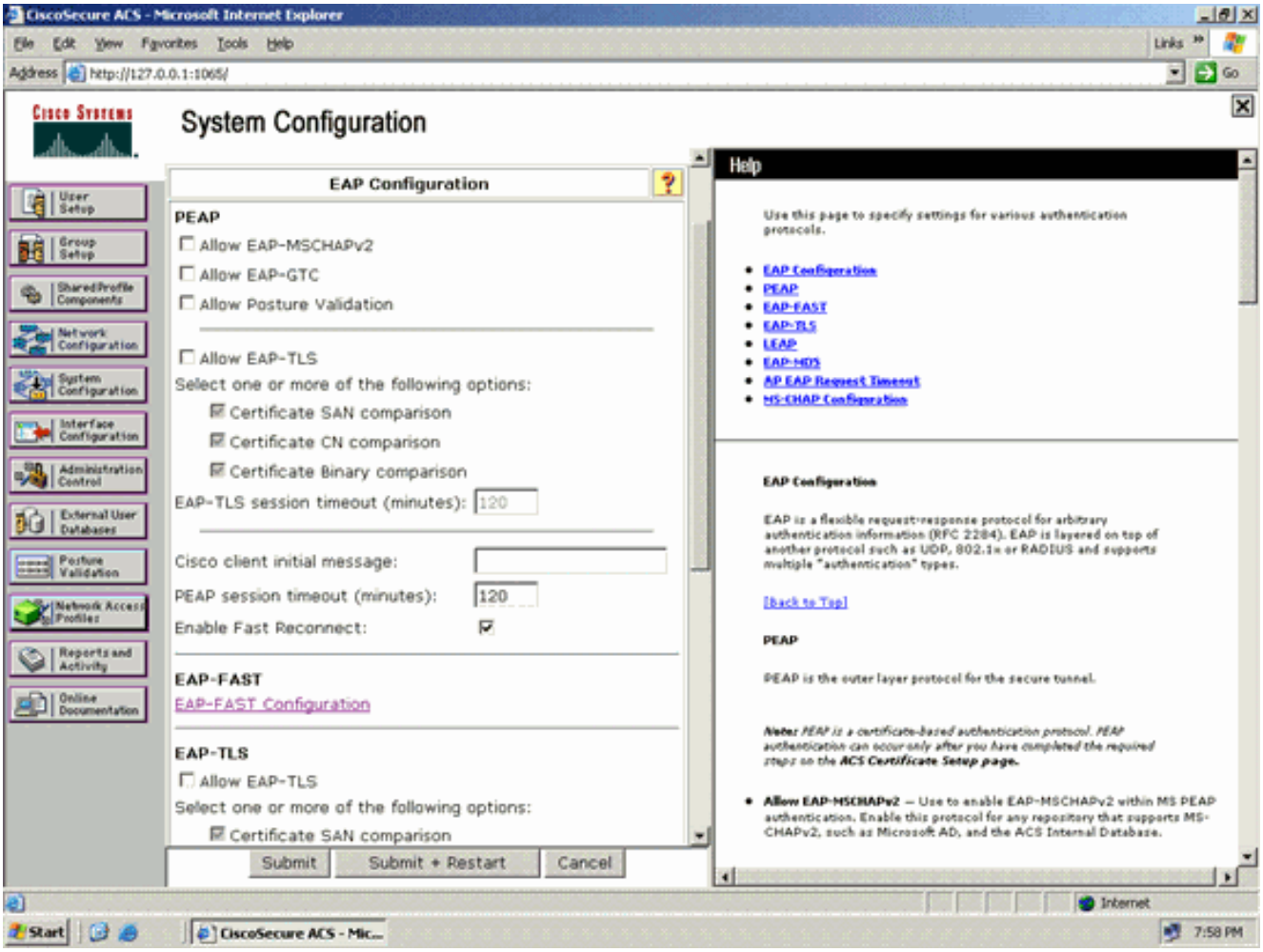
Kennwort zu verwenden. Daher können im Tunnel nur MS-CHAP-Anmeldeinformationen verwendet werden. MS-CHAPv2 wird verwendet, um die Identität des Peers zu überprüfen und eine PAC für weitere Authentifizierungssitzungen zu empfangen (EAP-MS-CHAP wird nur als interne Methode verwendet).

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

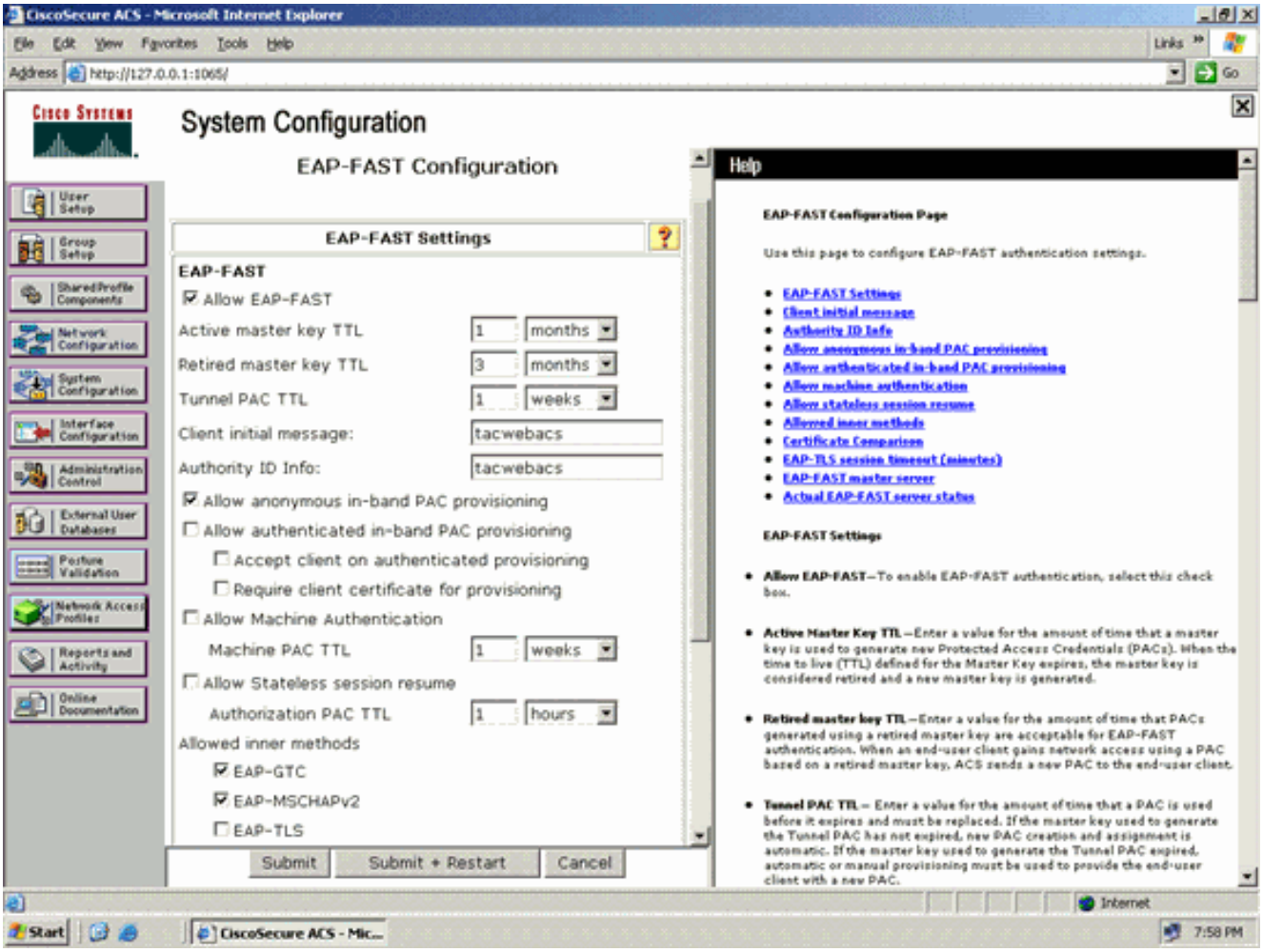
1. Klicken Sie in der RADIUS-Server-GUI auf **Systemkonfiguration**. Wählen Sie auf der Seite "System Configuration" die Option **Global Authentication Setup aus**.



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



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



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.

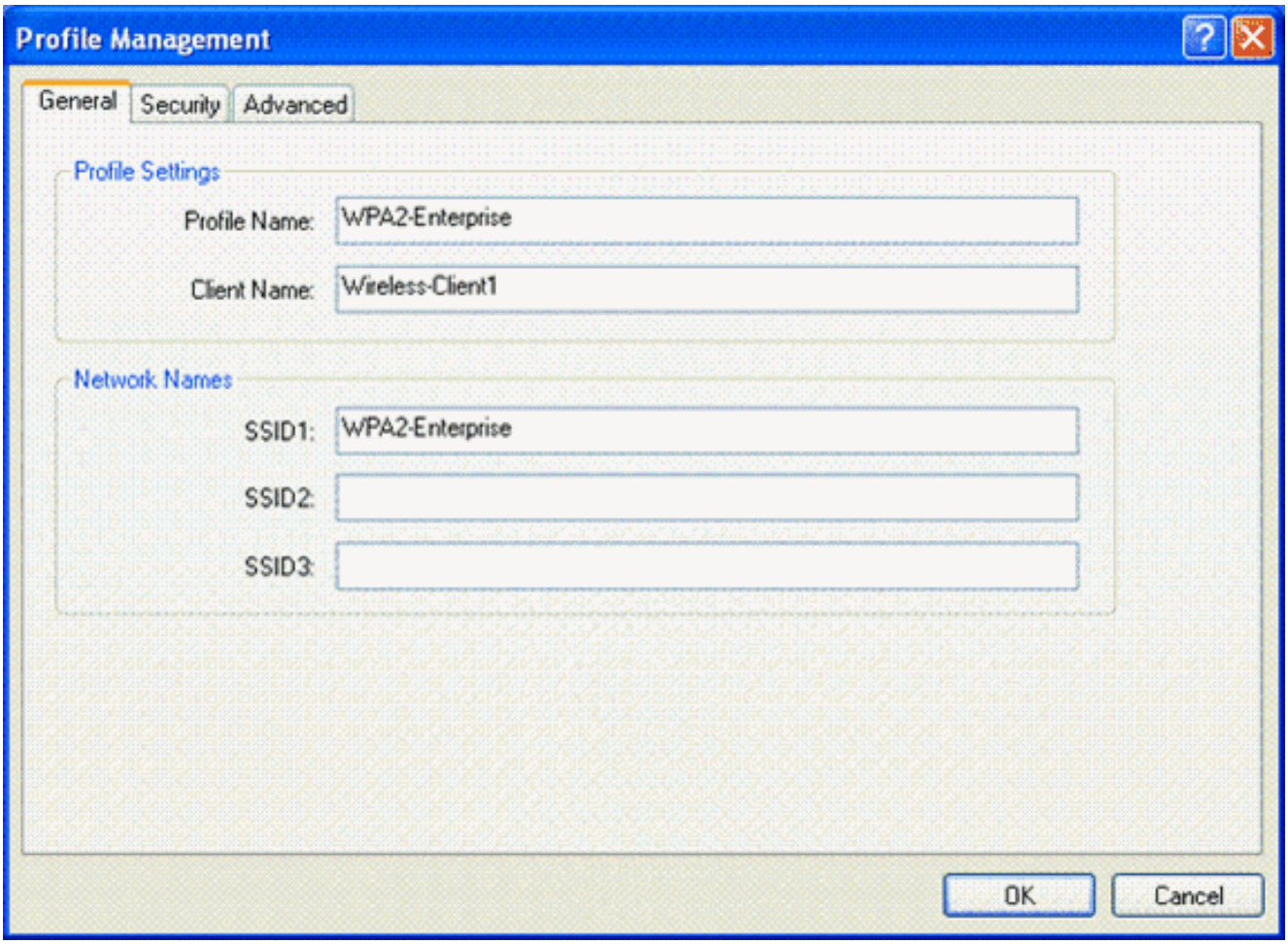
Konfigurieren des Wireless-Clients für den WPA2 Enterprise-Betriebsmodus

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

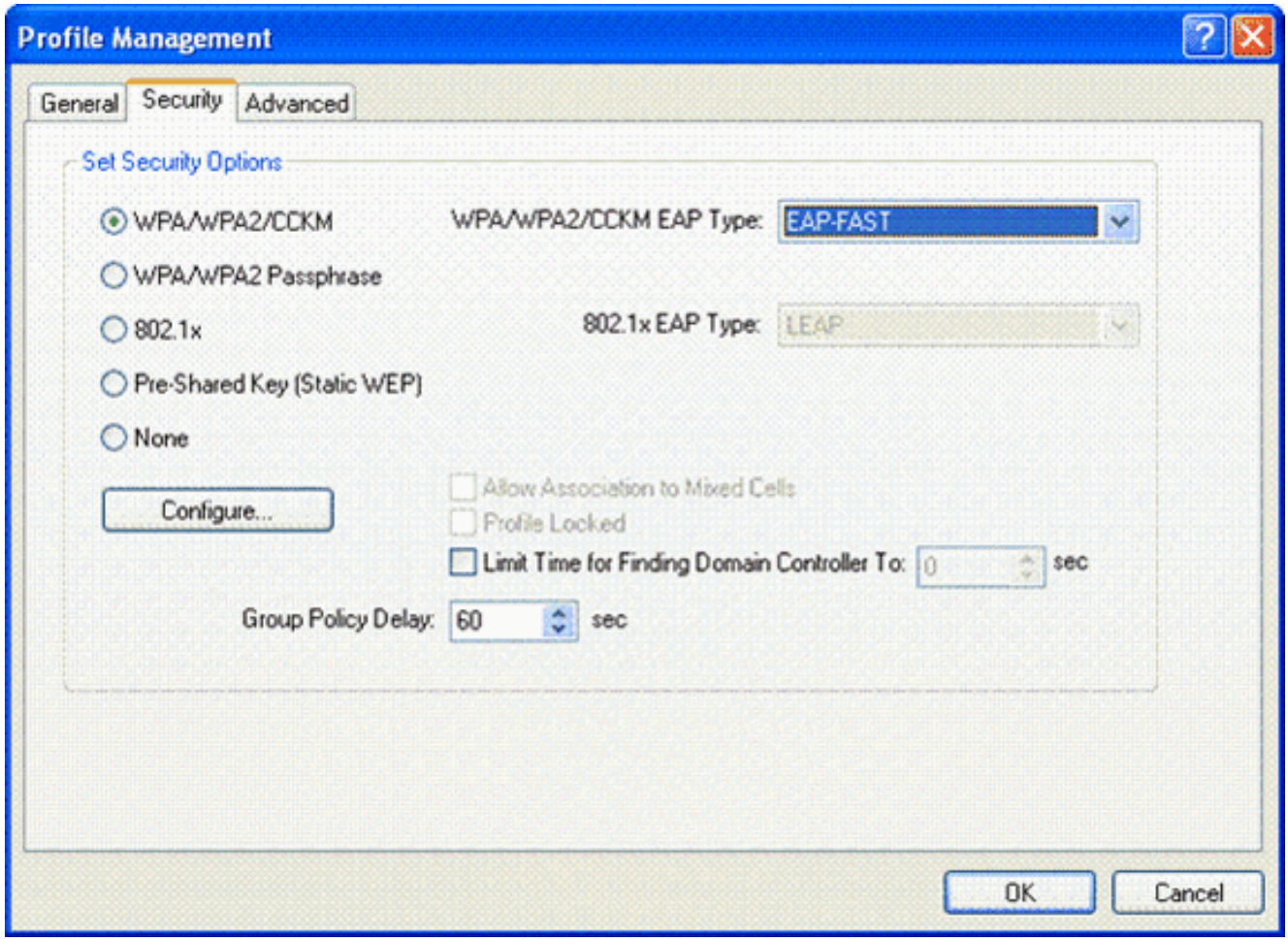
Führen Sie diese Schritte aus, um den Wireless-Client für den WPA2 Enterprise-Modus zu

konfigurieren.

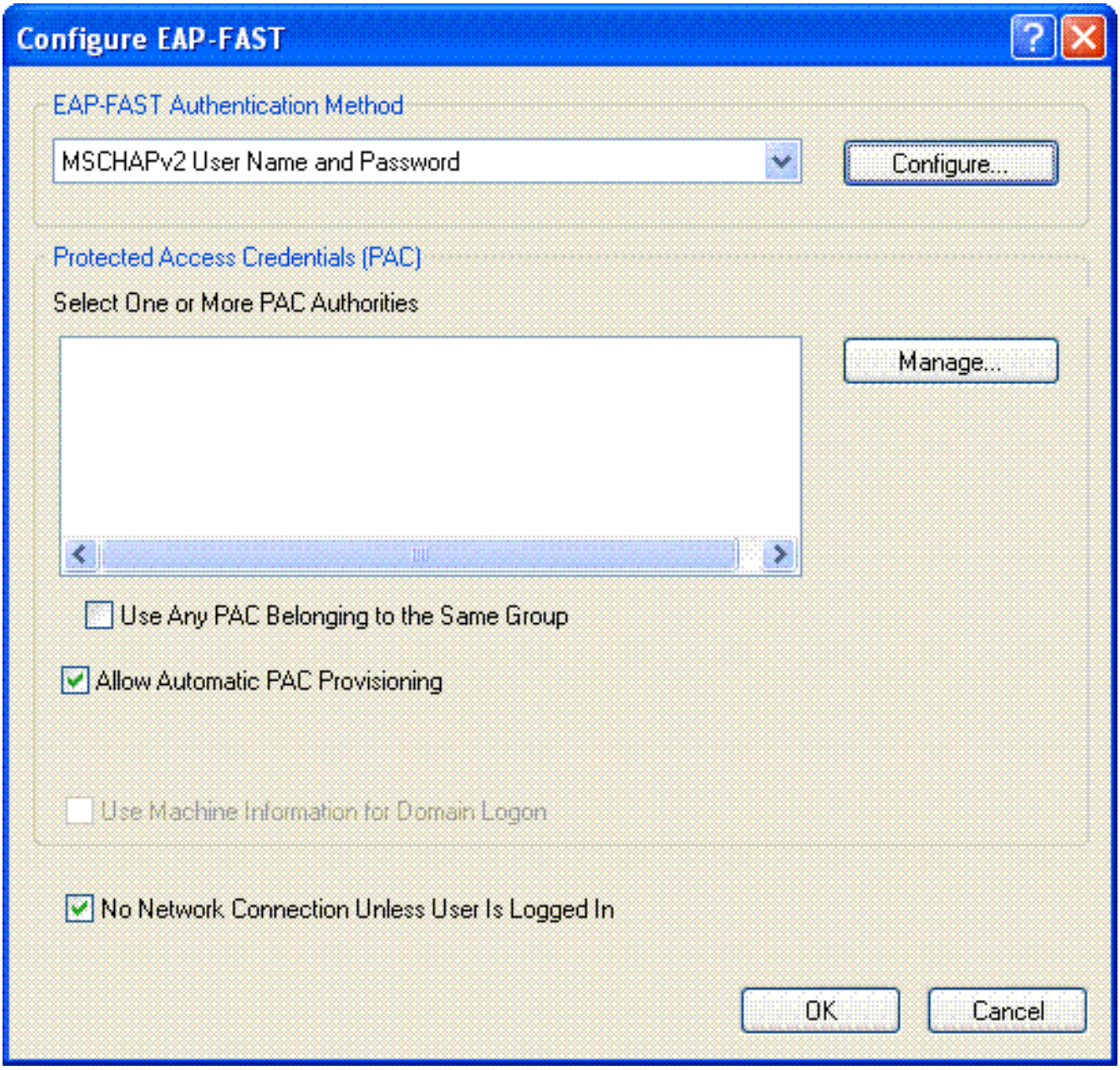
1. Klicken Sie im Fenster von Aironet Desktop Utility auf **Profile Management > New,** um ein Profil für den WPA2-Enterprise WLAN-Benutzer zu erstellen.Wie bereits erwähnt, verwendet dieses Dokument den WLAN/SSID-Namen als **WPA2-Enterprise** für den Wireless-Client.
2. Klicken Sie im Fenster Profilverwaltung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



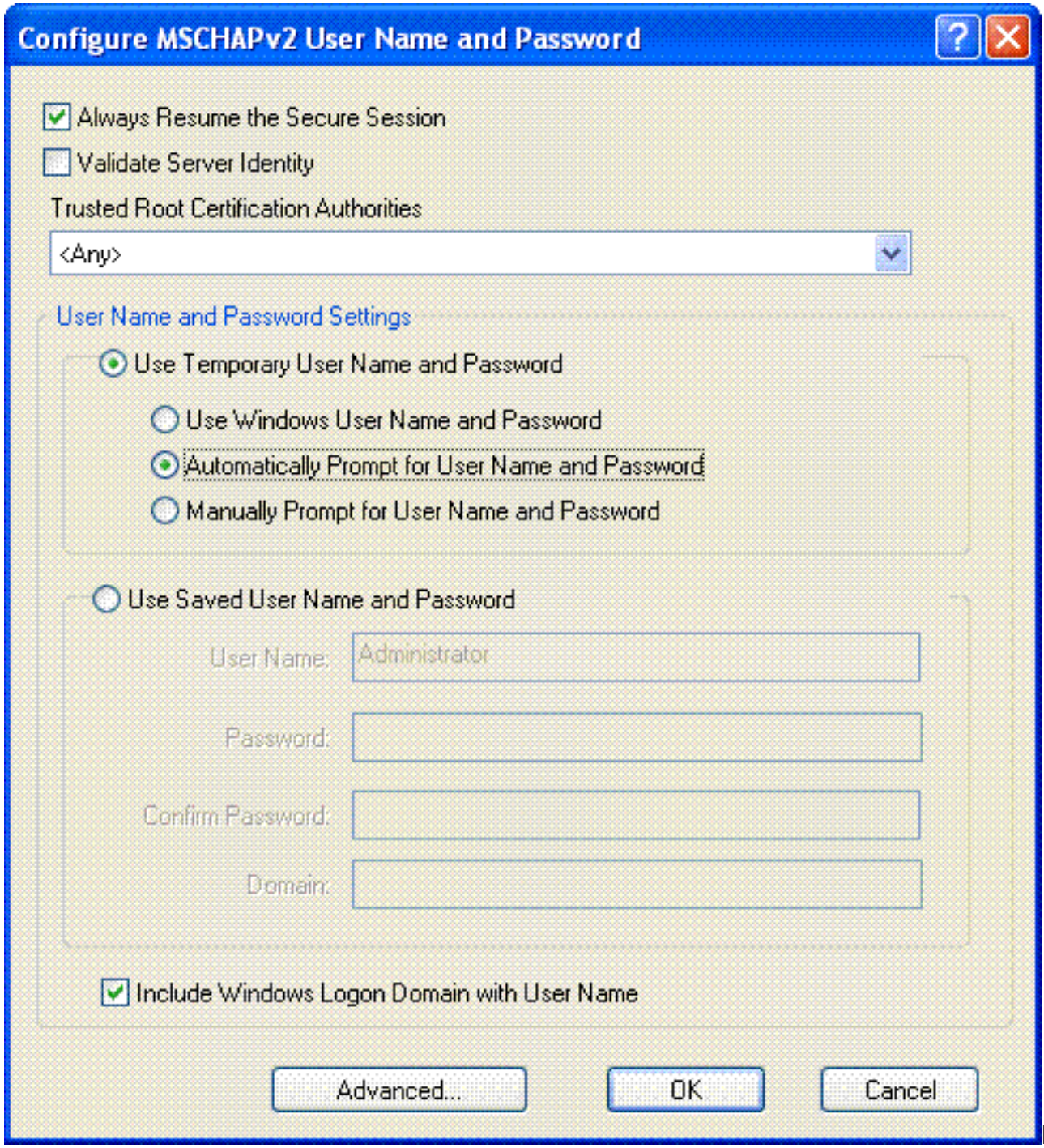
3. Klicken Sie auf die Registerkarte **Sicherheit**, und wählen Sie **WPA/WPA2/CCKM** aus, um den WPA2-Betriebsmodus zu aktivieren. Wählen Sie unter WPA/WPA2/CCKM EAP Type die Option **EAP-FAST aus**. Klicken Sie auf **Konfigurieren**, um die EAP-FAST-Einstellung zu konfigurieren.



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.



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**.



D
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.

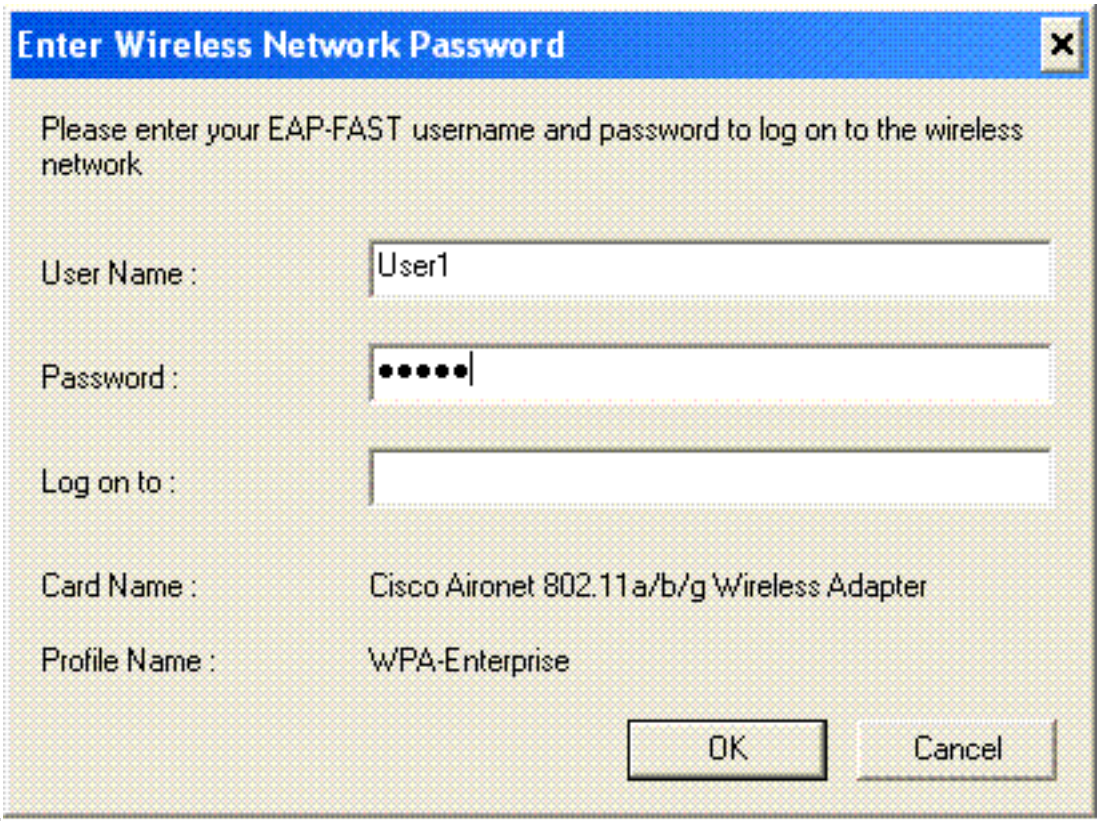
7. Klicken Sie auf **OK**.

Betriebsmodus von WPA2 Enterprise überprüfen

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

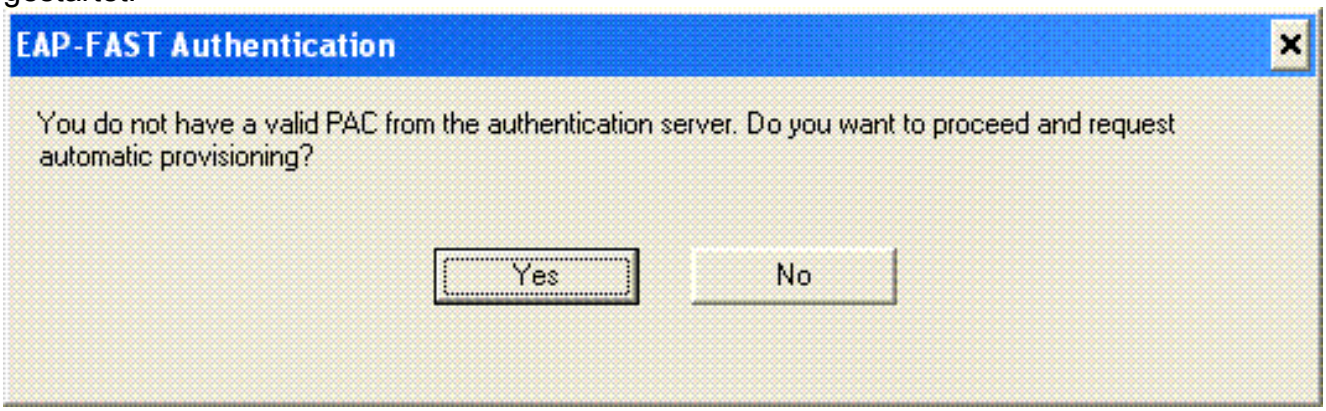
1. Wählen Sie im Fenster "Aironet Desktop Utility" das Profil **WPA2-Enterprise aus,** und klicken Sie auf **Activate (Aktivieren)**, um das Profil des Wireless-Clients zu aktivieren.
2. Wenn Sie MS-CHAP ver2 als Authentifizierung aktiviert haben, fordert der Client die Eingabe

von Benutzername und Kennwort

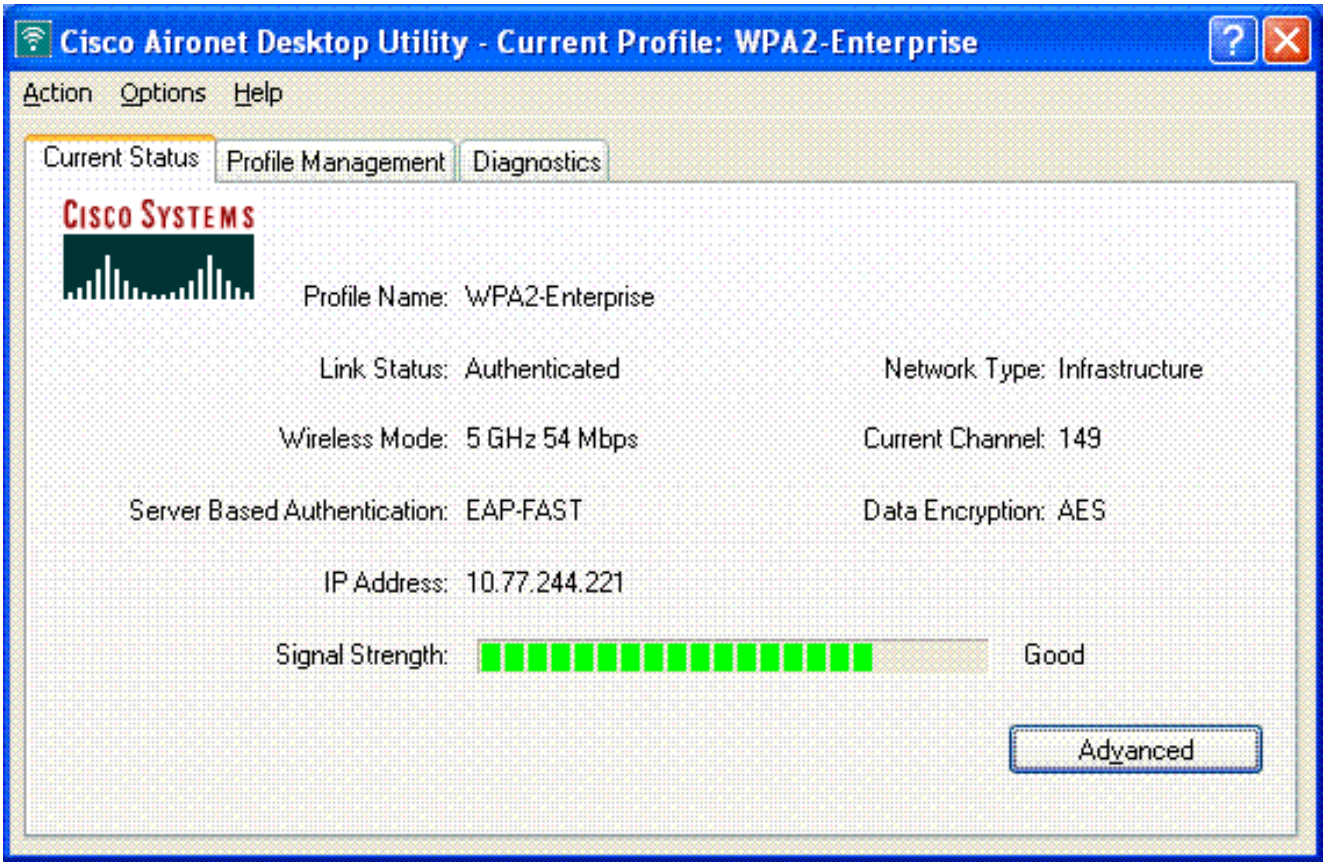


an.

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.



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:



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:

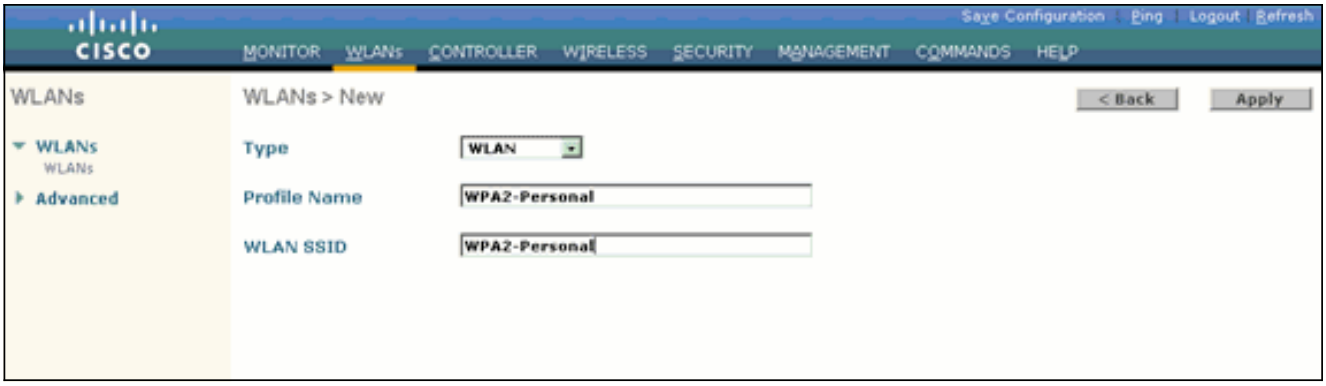
1. WLAN für die WPA2 Personal Mode-Authentifizierung konfigurieren
2. Konfigurieren des Wireless-Clients für den persönlichen WPA2-Modus

Konfigurieren des WLAN für den persönlichen WPA2-Modus

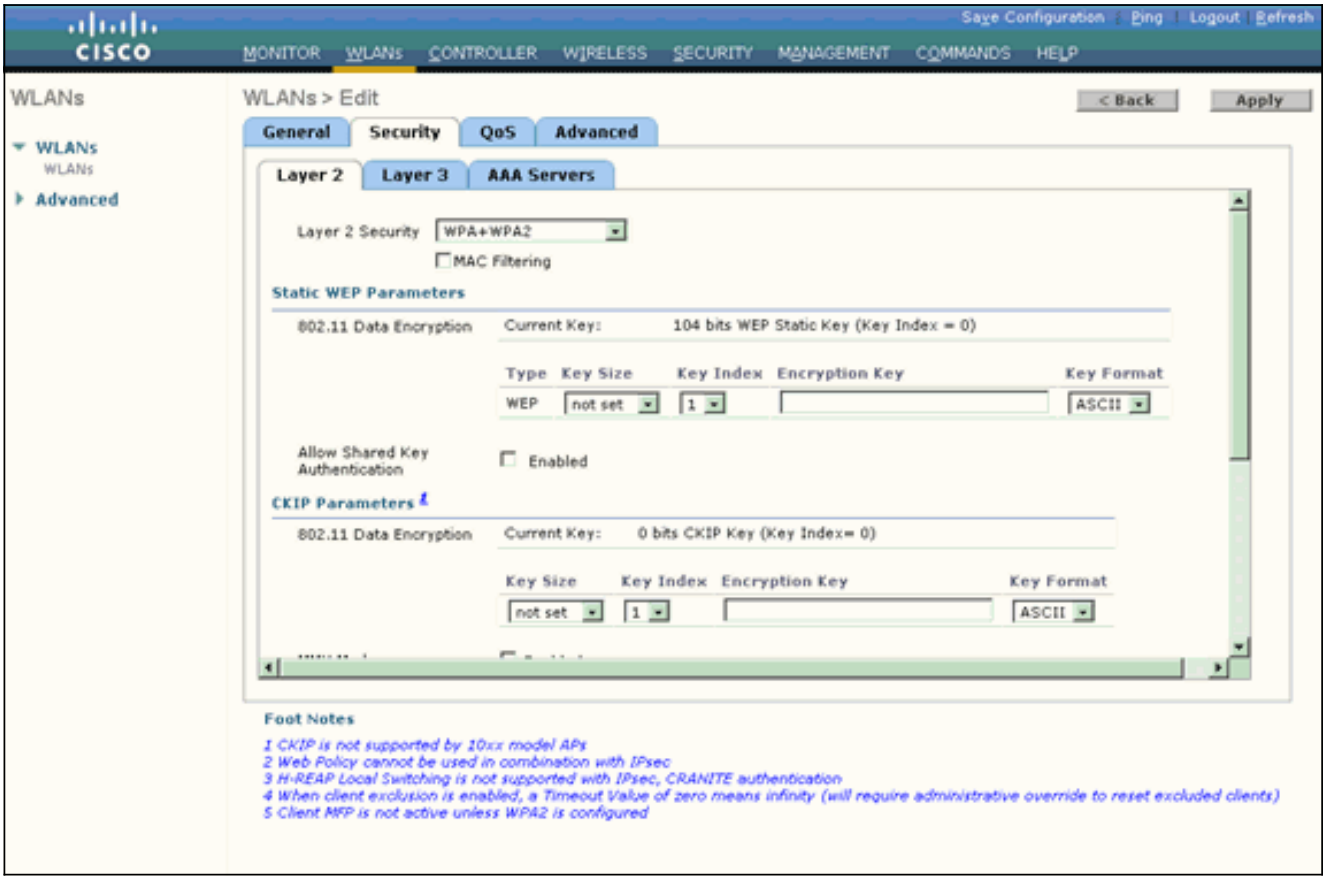
Sie müssen das WLAN konfigurieren, das die Clients für die Verbindung mit dem Wireless-Netzwerk verwenden. Die WLAN-SSID für den WPA2 Personal-Modus ist WPA2-Personal. In diesem Beispiel wird dieses WLAN der Verwaltungsschnittstelle zugewiesen.

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

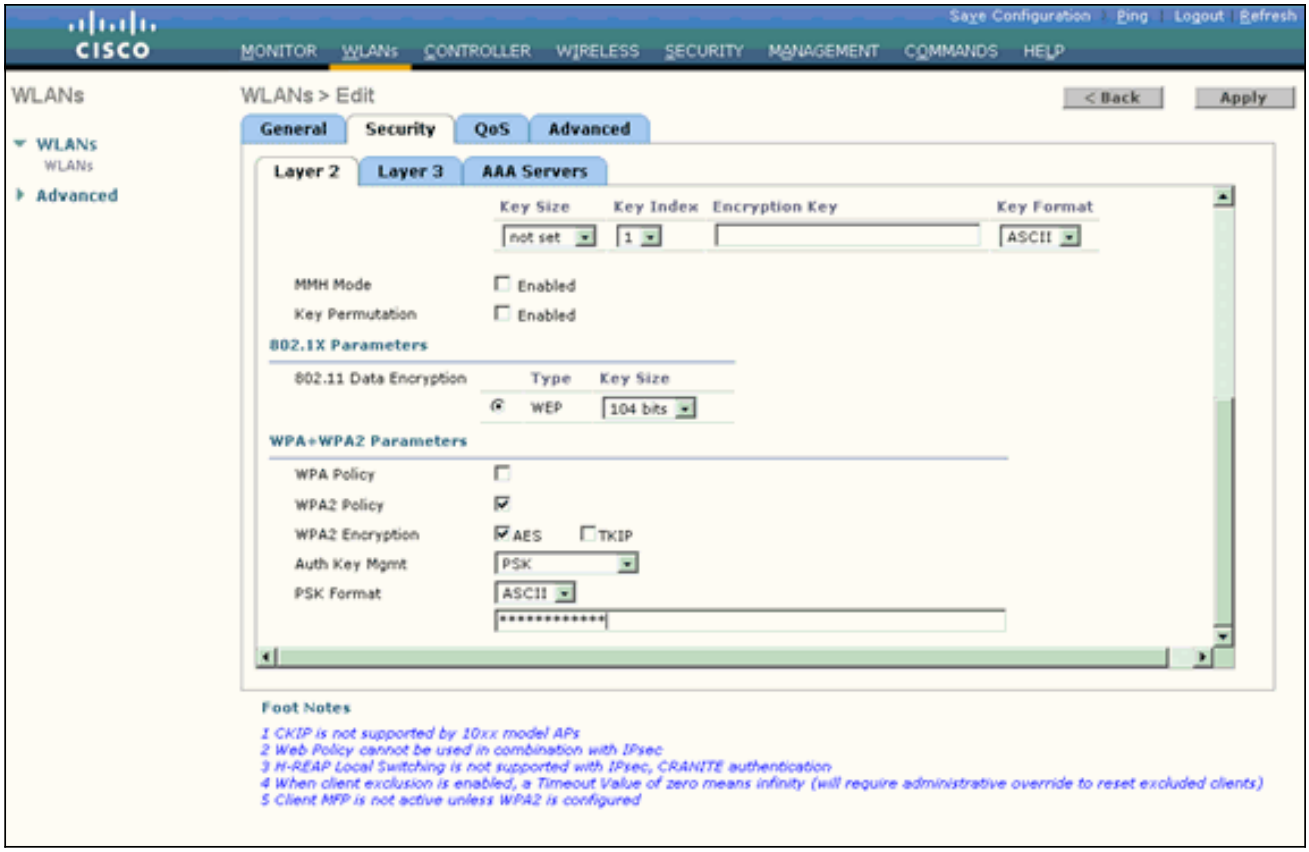
1. Klicken Sie in der GUI des Controllers auf **WLANs**, um die Seite WLANs anzuzeigen.Auf dieser Seite werden die WLANs aufgelistet, die auf dem Controller vorhanden sind.
2. Klicken Sie auf **Neu**, um ein neues WLAN zu erstellen.
3. Geben Sie auf der Seite WLANs > New (WLAN > Neu) den WLAN-SSID-Namen, den Profilnamen und die WLAN-ID ein. Klicken Sie anschließend auf **Apply**.In diesem Beispiel wird **WPA2-Personal** als SSID
verwendet.



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.



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.



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

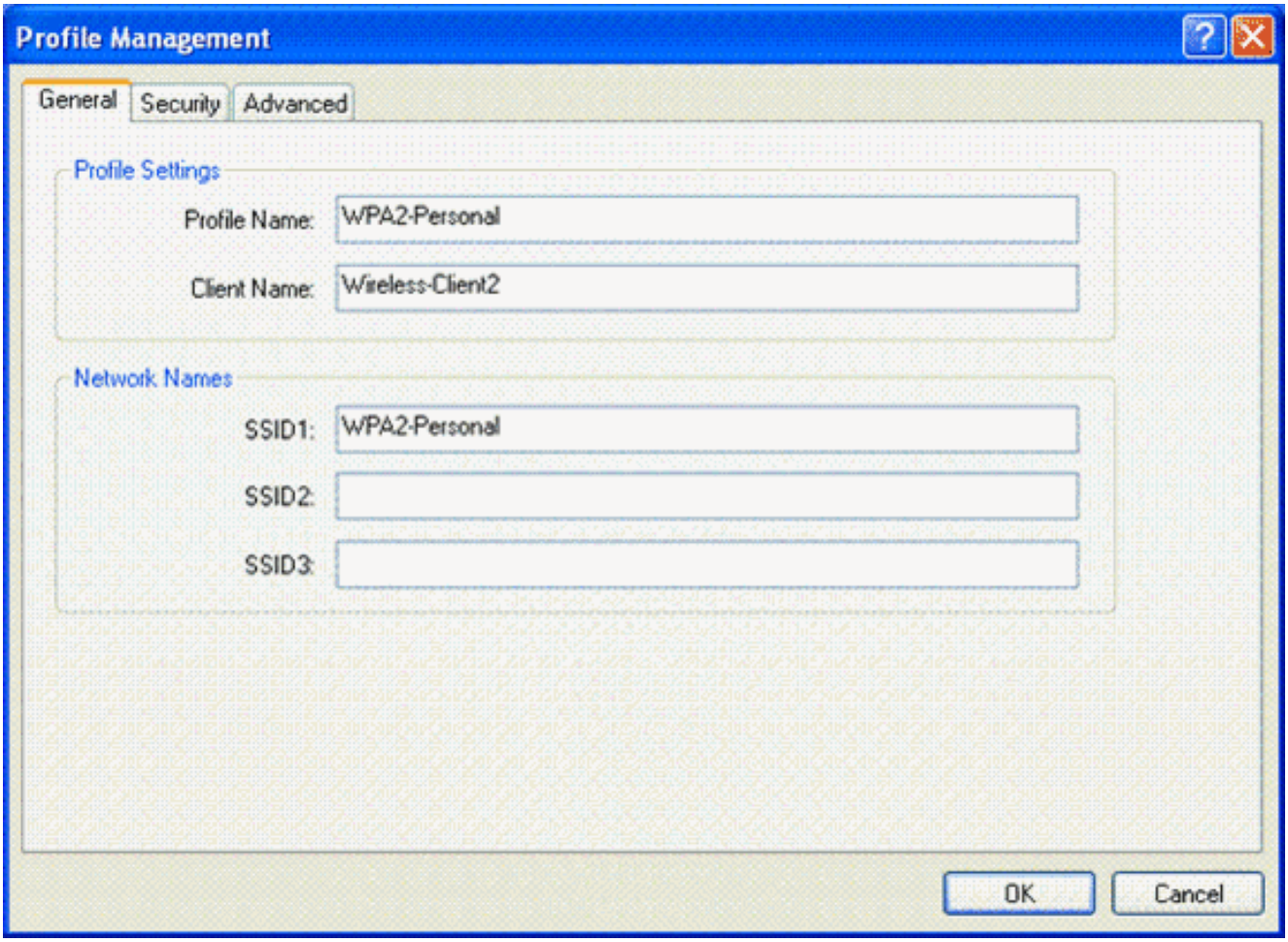
11. Klicken Sie auf **Apply** (Anwenden).

Konfigurieren des Wireless-Clients für den persönlichen WPA2-Modus

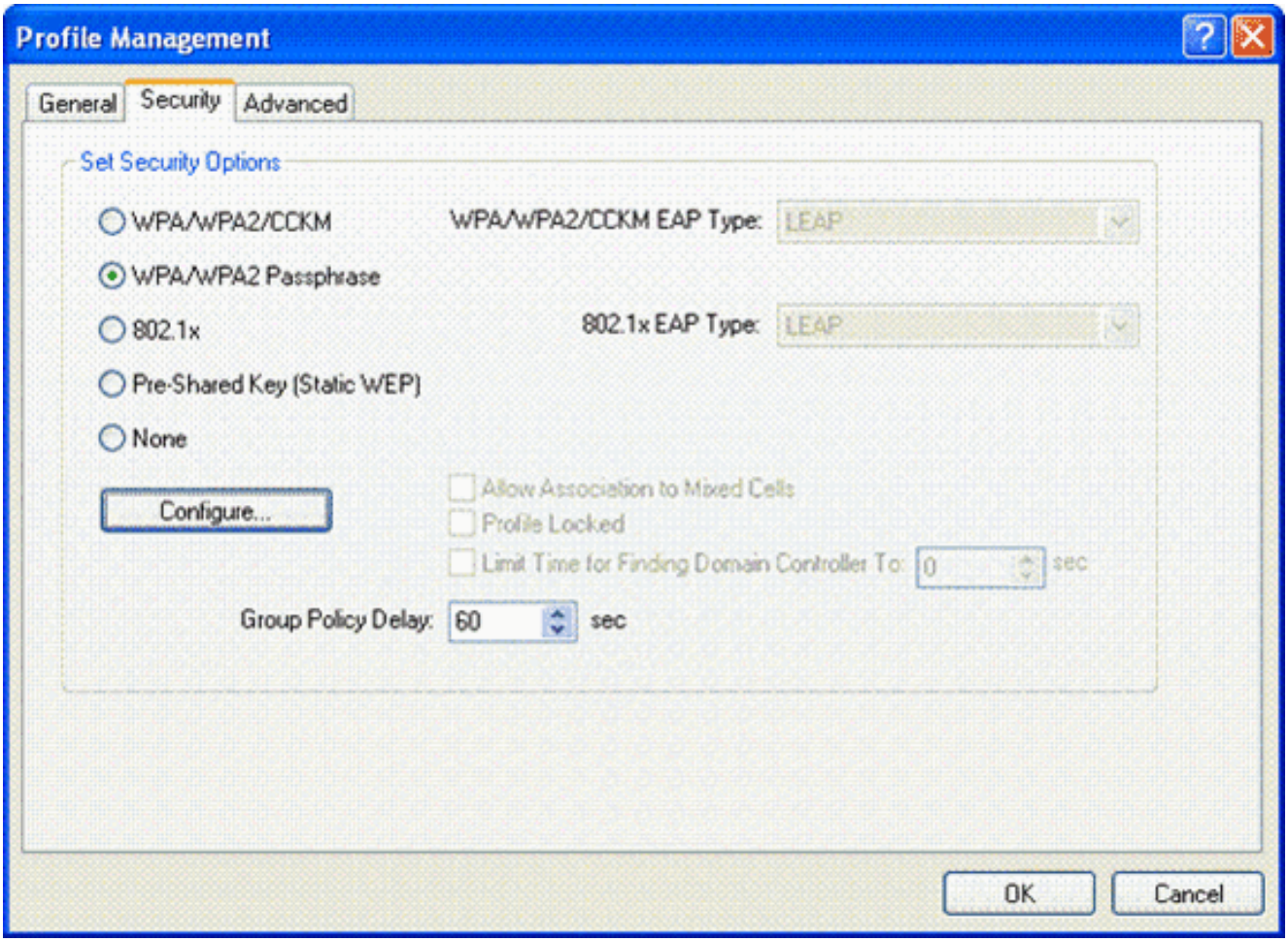
Der nächste Schritt besteht darin, den Wireless-Client für den WPA2-Personal-Betriebsmodus zu konfigurieren.

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

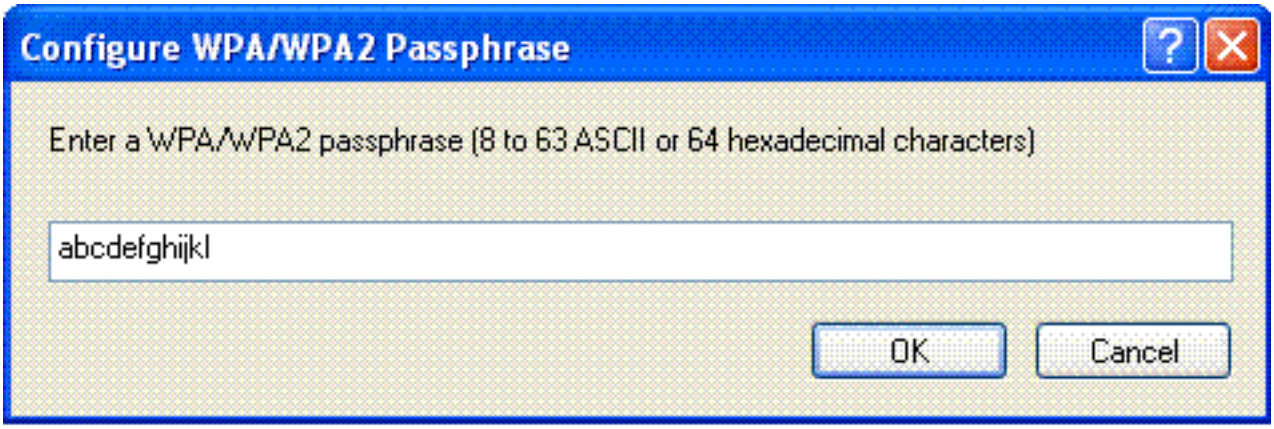
1. Klicken Sie im Fenster von Aironet Desktop Utility auf **Profile Management > New,** um ein Profil für WPA2-PSK-WLAN-Benutzer zu erstellen.
2. Klicken Sie im Fenster Profilverwaltung auf die Registerkarte **Allgemein,** und konfigurieren Sie Profilname, Client-Name und SSID-Namen wie in diesem Beispiel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



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.



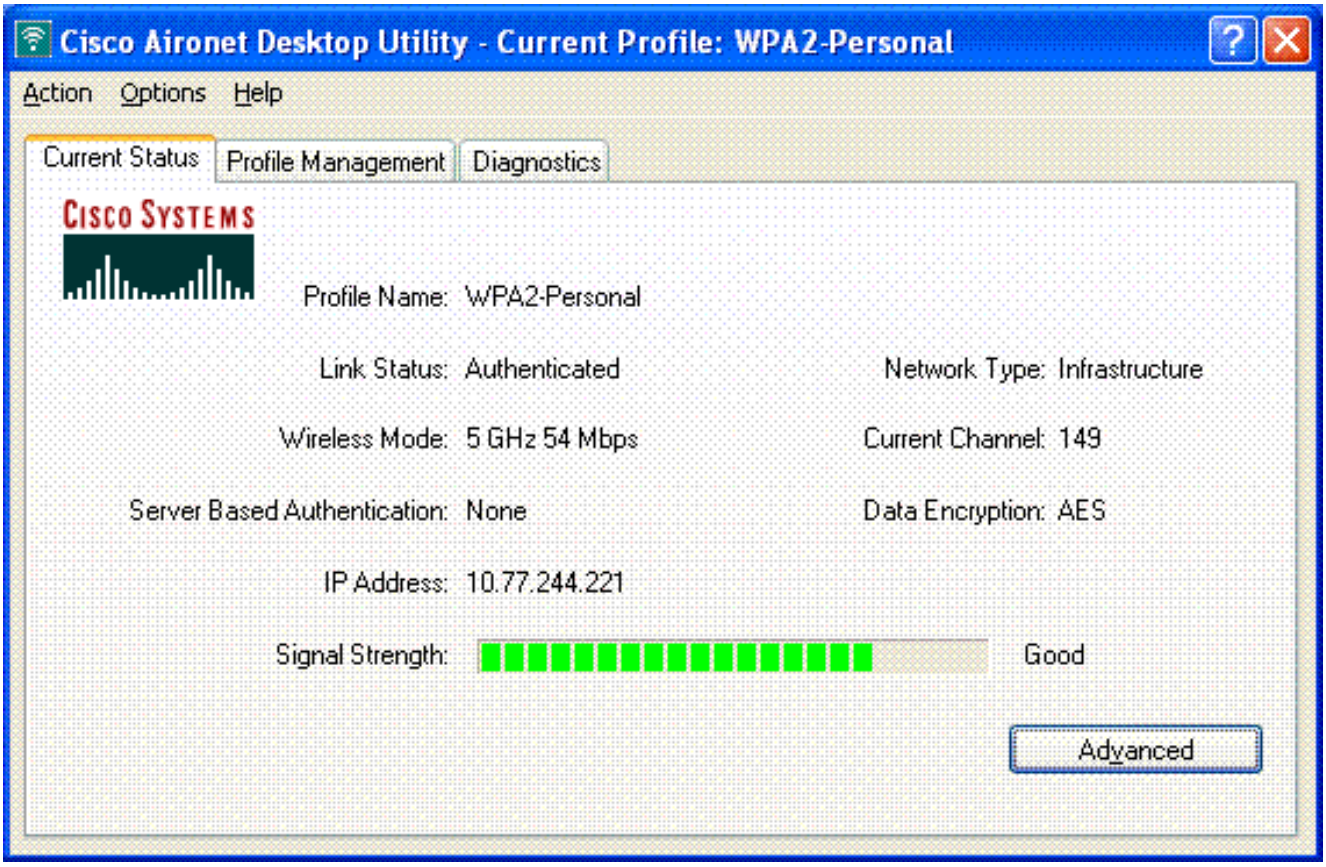
4. Geben Sie den vorinstallierten Schlüssel ein, und klicken Sie auf **OK**.



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:



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 Wichtige Informationen zu Debug-Befehlen, 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
.....
.....
.....
.....

Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Received EAP Response from
```

mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 43)
Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 **Processing Access-Challenge for mobile 00:40:96:af:3e:93**
Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 **Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20)**
Wed Feb 20 14:20:01 2007: 00:40:96:af:3e:93 **Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43)**
Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -0
Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3689 seconds on AP 00:0b:85:91:c3:c0
Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -1
Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3696 seconds on AP 00:0b:85:91:c3:c0
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 22)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received Identity Response (count=3) from mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===> 19 for STA 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 19)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 3)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 21)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 22)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 23)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 23, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for

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

```
tation 00:40:96:af:3e:93 (RSN 0)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP-Success to
mobile 00:40:96:af:3e:93 (EAP Id 25)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending default RC4 key to
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending Key-Mapping RC4 key to
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Auth Success while in
Authenticating state for mobile 00:40:96:af:3e:93
```

- **debug dot1x packet enable**: 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 externen RADIUS-Servers
- EAP-Authentifizierung mit WLAN-Controllern (WLC) - Konfigurationsbeispiel
- Übersicht über die WPA-Konfiguration
- Support für Wireless-Produkte
- 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.