Konfigurationsbeispiel für EAP-Authentifizierung mit WLAN-Controllern (WLC)

Inhalt

Einführung

In diesem Dokument wird erläutert, wie der Wireless LAN Controller (WLC) für die EAP-Authentifizierung (Extensible Authentication Protocol) mit einem externen RADIUS-Server konfiguriert wird. In diesem Konfigurationsbeispiel wird der Cisco Secure Access Control Server (ACS) als externer RADIUS-Server verwendet, um die Benutzeranmeldeinformationen zu validieren.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Grundkenntnisse in der Konfiguration von Lightweight Access Points (APs) und Cisco WLCs.
- Grundkenntnisse des Lightweight AP Protocol (LWAPP).
- Kenntnisse zum Konfigurieren eines externen RADIUS-Servers wie Cisco Secure ACS.

Verwendete Komponenten

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

- Cisco Aironet Lightweight AP der Serie 1232AG
- Cisco WLC der Serie 4400 mit Firmware 5.1
- Cisco Secure ACS mit Version 4.1
- Cisco Aironet 802.11 a/b/g Client-Adapter
- Cisco Aironet Desktop Utility (ADU) für die Ausführung der Firmware 4.2

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).

Konfiguration

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

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten.

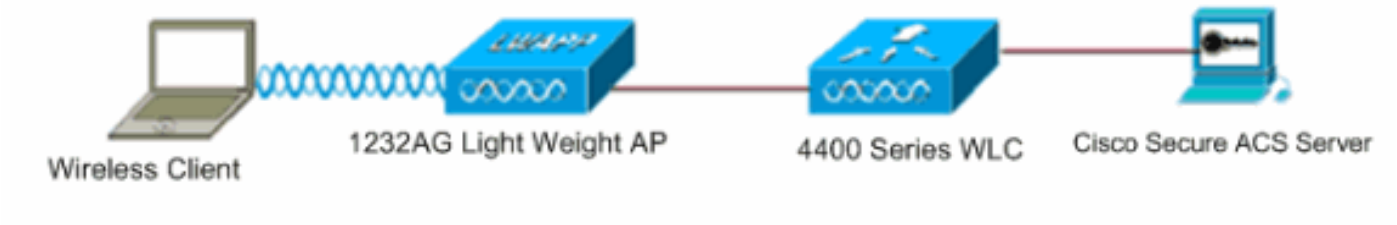
Gehen Sie wie folgt vor, um die Geräte für die EAP-Authentifizierung zu konfigurieren:

1. Konfigurieren Sie den WLC für den Basisbetrieb, und registrieren Sie die Lightweight APs beim Controller.
2. Konfigurieren Sie den WLC für die RADIUS-Authentifizierung über einen externen RADIUS-Server.
3. Konfigurieren Sie die WLAN-Parameter.
4. Konfigurieren Sie Cisco Secure ACS als externen RADIUS-Server, und erstellen Sie eine Benutzerdatenbank für die Authentifizierung von Clients.

Netzwerkdiagramm

In dieser Konfiguration werden ein Cisco 4400 WLC und ein Lightweight AP über einen Hub verbunden. Ein externer RADIUS-Server (Cisco Secure ACS) ist ebenfalls mit demselben Hub verbunden. Alle Geräte befinden sich im gleichen Subnetz. Der Access Point ist zunächst beim Controller registriert. Sie müssen WLC und AP für die LEAP-Authentifizierung (Lightweight Extensible Authentication Protocol) konfigurieren. Die Clients, die eine Verbindung zum AP

herstellen, verwenden die LEAP-Authentifizierung, um eine Verbindung zum AP herzustellen. Cisco Secure ACS wird für die RADIUS-Authentifizierung verwendet.



Konfigurieren des WLC für den Basisbetrieb und Registrieren der Lightweight APs für den Controller

Verwenden Sie den Assistenten für die Startkonfiguration in der Befehlszeilenschnittstelle (CLI), um den WLC für den Basisbetrieb zu konfigurieren. Alternativ können Sie auch die Benutzeroberfläche verwenden, um den WLC zu konfigurieren. In diesem Dokument wird die Konfiguration auf dem WLC mit dem Startup Configuration Wizard (Start-Konfigurationsassistent) in der CLI erläutert.

Nachdem der WLC zum ersten Mal gestartet wurde, wird er direkt in den Startup Configuration Wizard (Startup-Konfigurationsassistent) eingegeben. Konfigurieren Sie mithilfe des Konfigurationsassistenten die Grundeinstellungen. Sie können den Assistenten über die Kommandozeile oder die Benutzeroberfläche ausführen. Diese Ausgabe zeigt ein Beispiel für den Startup Configuration Wizard (Start-Konfigurationsassistent) in der CLI:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: WLC-1
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 10.77.244.204
Management Interface Netmask: 255.255.255.224
Management Interface Default Router: 10.77.244.220
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.77.244.220
AP Manager Interface IP Address: 10.77.244.205
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (10.77.244.220):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Test
Network Name (SSID): Cisco123
Allow Static IP Addresses [YES][no]: yes
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configuration saved!
Resetting system with new configuration..
```

Diese Parameter richten den WLC für den Basisbetrieb ein. In diesem Konfigurationsbeispiel verwendet der WLC als IP-Adresse der Verwaltungsschnittstelle 10.77.244.204 und

10.77.244.205 als IP-Adresse der AP-Manager-Schnittstelle.

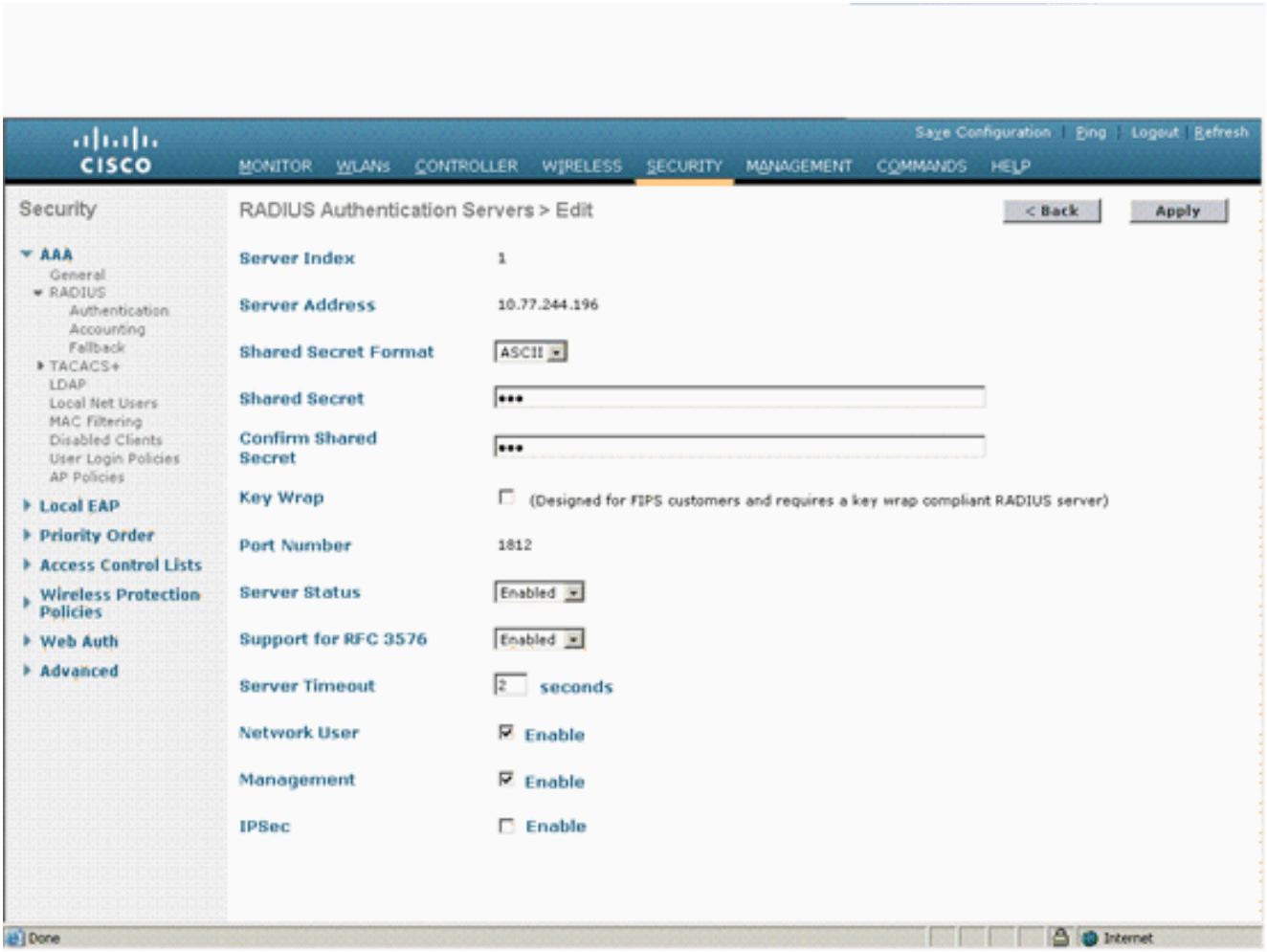
Bevor andere Funktionen auf den WLCs konfiguriert werden können, müssen die Lightweight APs beim WLC registriert werden. In diesem Dokument wird davon ausgegangen, dass der Lightweight Access Point beim WLC registriert ist. Weitere Informationen zur Registrierung von APs mit geringem Speicheraufkommen beim WLC finden Sie unter Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC).

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 und ermöglicht den Zugriff auf die Wireless-Clients.

Gehen Sie wie folgt vor, um den WLC für einen externen RADIUS-Server zu konfigurieren:

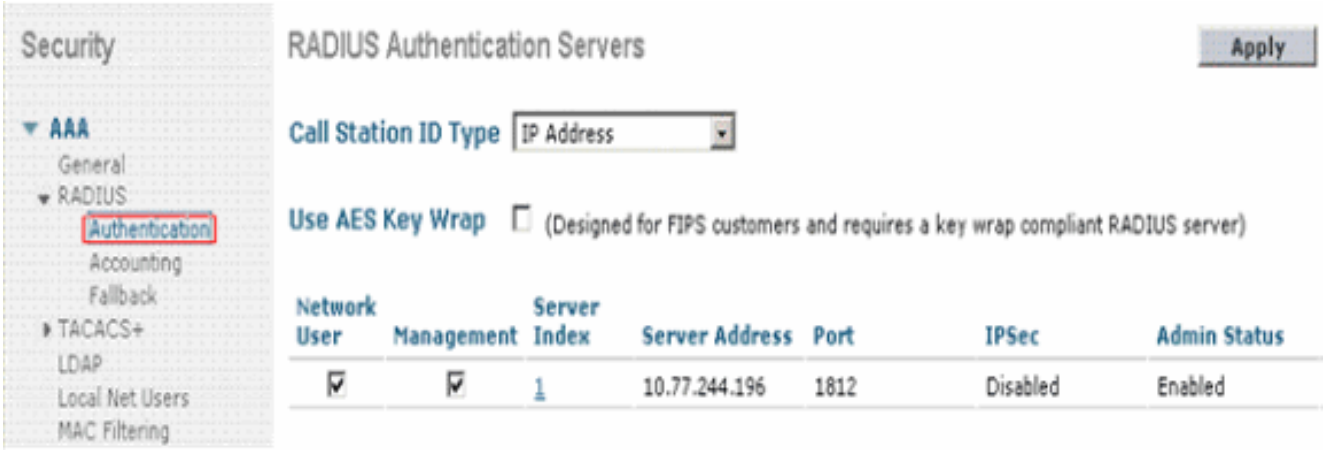
1. Wählen Sie **Sicherheit** und **RADIUS Authentication (RADIUS-Authentifizierung)** in der Benutzeroberfläche des Controllers aus, um die Seite RADIUS Authentication Servers (RADIUS-Authentifizierungsserver) anzuzeigen. Klicken Sie anschließend auf **Neu**, um einen RADIUS-Server zu definieren.



2. Definieren Sie die RADIUS-Serverparameter auf der Seite RADIUS Authentication Servers > New (RADIUS-Authentifizierungsserver > Neu). Zu diesen Parametern gehören die IP-Adresse des RADIUS-Servers, der Shared Secret, die Portnummer und der Serverstatus.Die

Kontrollkästchen für Netzwerkbenutzer und -verwaltung legen fest, ob die RADIUS-basierte Authentifizierung für die WLC-Verwaltung und die Netzwerkbenutzer gilt. In diesem Beispiel wird Cisco Secure ACS als RADIUS-Server mit der IP-Adresse 10.77.244.196 verwendet.

3. Radius-Server können jetzt vom WLC für die Authentifizierung verwendet werden. Der Radius-Server ist aufgelistet, wenn Sie **Security > Radius > Authentication** auswählen.



RFC 3576 wird auf dem RADIUS-Server Cisco CNS Access Registrar (CAR) unterstützt, jedoch nicht auf Cisco Secure ACS Server Version 4.0 und früheren Versionen.Sie können auch die lokale RADIUS-Serverfunktion verwenden, um Benutzer zu authentifizieren. Der lokale RADIUS-Server wurde mit Code der Version 4.1.171.0 eingeführt. WLCs, die ältere Versionen ausführen, verfügen nicht über die Funktion für den lokalen Radius. Lokaler EAP ist eine Authentifizierungsmethode, mit der Benutzer und Wireless-Clients lokal authentifiziert werden können. Sie ist für die Verwendung in Außenstellen ausgelegt, die die Verbindung zu Wireless-Clients aufrechterhalten möchten, wenn das Backend-System ausfällt oder der externe Authentifizierungsserver ausfällt. Der lokale EAP ruft Benutzeranmeldeinformationen aus der lokalen Benutzerdatenbank oder der LDAP-Backend-Datenbank ab, um Benutzer zu authentifizieren. Der lokale EAP unterstützt LEAP, EAP-FAST mit PACs, EAP-FAST mit Zertifikaten und EAP-TLS-Authentifizierung zwischen dem Controller und den Wireless-Clients.Der lokale EAP ist als Backup-Authentifizierungssystem konzipiert. Wenn RADIUS-Server auf dem Controller konfiguriert sind, versucht der Controller zunächst, die Wireless-Clients mit den RADIUS-Servern zu authentifizieren. Lokale EAP wird nur dann versucht, wenn keine RADIUS-Server gefunden werden, entweder weil die RADIUS-Server das Zeitlimit überschritten haben oder keine RADIUS-Server konfiguriert wurden.Weitere Informationen zur Konfiguration des lokalen EAP auf Wireless LAN-Controllern mit EAP-FAST und LDAP-Server finden Sie im Konfigurationsbeispiel für die lokale EAP-Authentifizierung auf Wireless LAN-Controllern.

WLAN-Parameter konfigurieren

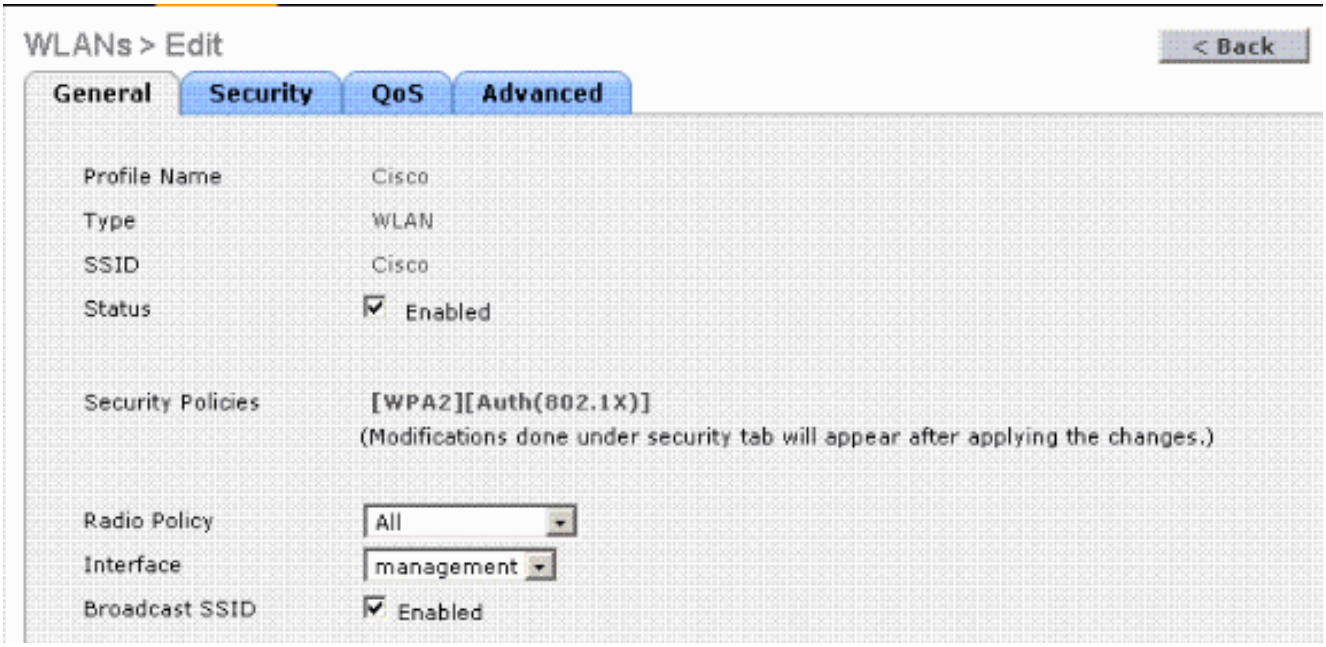
Konfigurieren Sie anschließend das WLAN, über das die Clients eine Verbindung zum Wireless-Netzwerk herstellen. Wenn Sie die Basisparameter für den WLC konfiguriert haben, haben Sie auch die SSID für das WLAN konfiguriert. Sie können diese SSID für das WLAN verwenden oder eine neue SSID erstellen. In diesem Beispiel erstellen Sie eine neue SSID.

Hinweis: Auf dem Controller können bis zu 16 WLANs konfiguriert werden. Die Cisco WLAN-Lösung kann bis zu 16 WLANs für Lightweight APs verwalten. Jedem WLAN können eindeutige Sicherheitsrichtlinien zugewiesen werden. Lightweight APs übertragen alle aktiven WLAN-SSIDs der Cisco WLAN-Lösung und setzen die Richtlinien durch, die Sie für jedes WLAN festlegen.

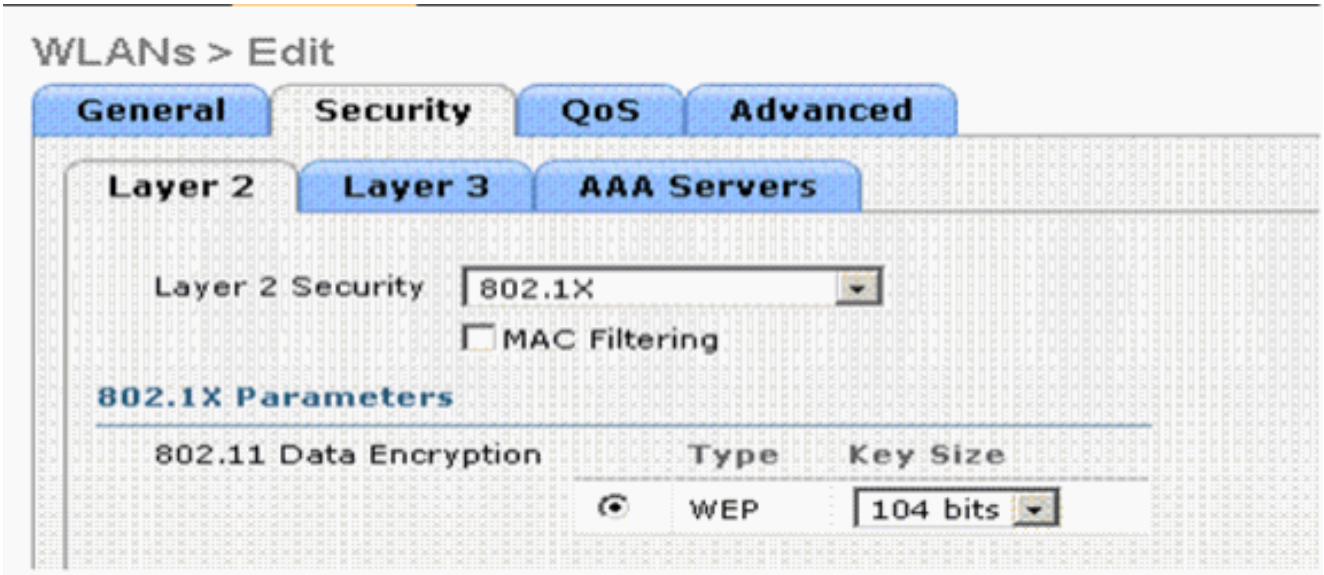
Gehen Sie wie folgt vor, um ein neues WLAN und die zugehörigen Parameter zu konfigurieren:

1. Klicken Sie in der Benutzeroberfläche des Controllers auf **WLANs**, um die Seite WLANs anzuzeigen.Auf dieser Seite werden die WLANs aufgelistet, die auf dem Controller vorhanden sind.
2. Wählen Sie **Neu**, um ein neues WLAN zu erstellen. Geben Sie den Profilnamen und die WLAN-SSID für das WLAN ein, und klicken Sie auf **Apply**. In diesem Beispiel wird Cisco als SSID
verwendet.

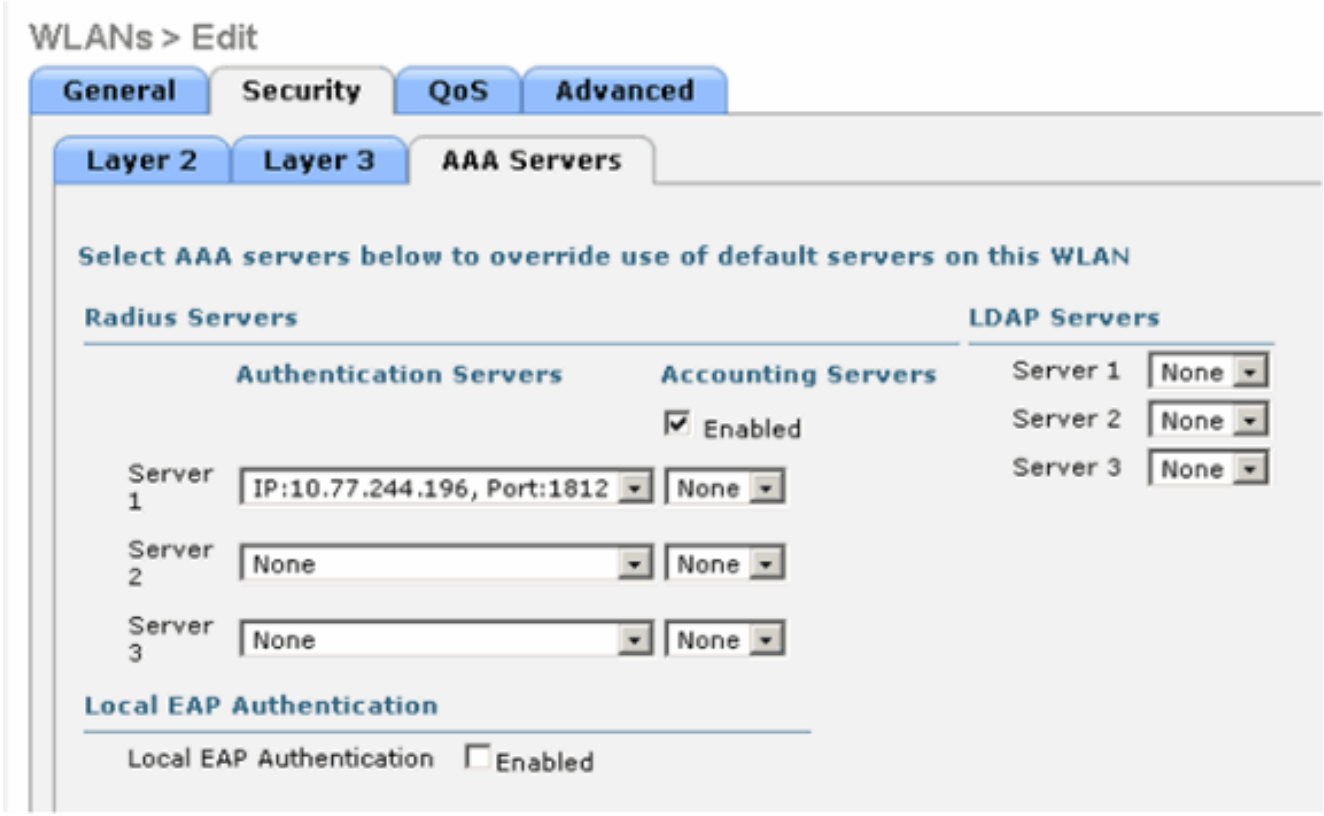
3. Sobald Sie ein neues WLAN erstellt haben, wird die Seite WLAN > Edit (WLAN > Bearbeiten) für das neue WLAN angezeigt. Auf dieser Seite können Sie verschiedene Parameter für dieses WLAN definieren, die allgemeine Richtlinien, Sicherheitsrichtlinien, QoS-Richtlinien und andere erweiterte Parameter
enthalten.



Wählen Sie im Dropdown-Menü die entsprechende Schnittstelle aus. Die anderen Parameter können je nach Anforderung des WLAN-Netzwerks geändert werden.Aktivieren Sie das Feld **Status** unter Allgemeine Richtlinien, um das WLAN zu aktivieren.
4. Klicken Sie auf die Registerkarte **Sicherheit** und wählen Sie **Layer-2-Sicherheit aus**. Wählen Sie im Dropdown-Menü für Layer-2-Sicherheit die Option **802.1x aus**. Wählen Sie in den 802.1x-Parametern die WEP-Schlüsselgröße aus. In diesem Beispiel wird der 128-Bit-WEP-Schlüssel verwendet, der den 104-Bit-WEP-Schlüssel plus den 24-Bit-Initialisierungsvektor darstellt.



5. Wählen Sie die Registerkarte **AAA-Server aus**. Wählen Sie im Dropdown-Menü Authentication Servers (RADIUS) (Authentifizierungsserver (RADIUS)) den entsprechenden RADIUS-Server aus. Dieser Server wird zur Authentifizierung der Wireless-Clients verwendet.



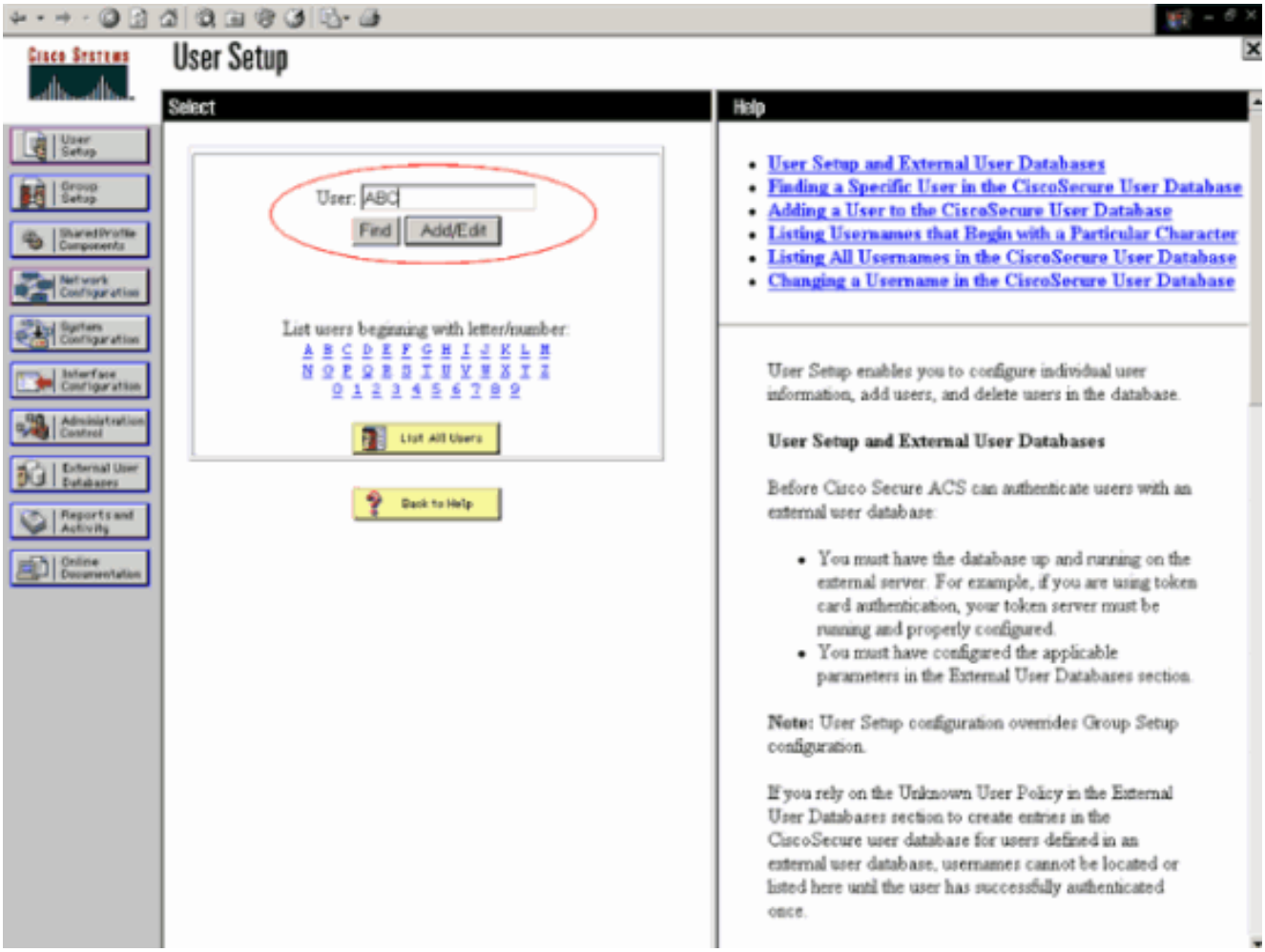
6. Klicken Sie auf **Apply**, um die Konfiguration zu speichern.

Konfigurieren von Cisco Secure ACS als externem RADIUS-Server und Erstellen einer Benutzerdatenbank für Authentifizierungs-Clients

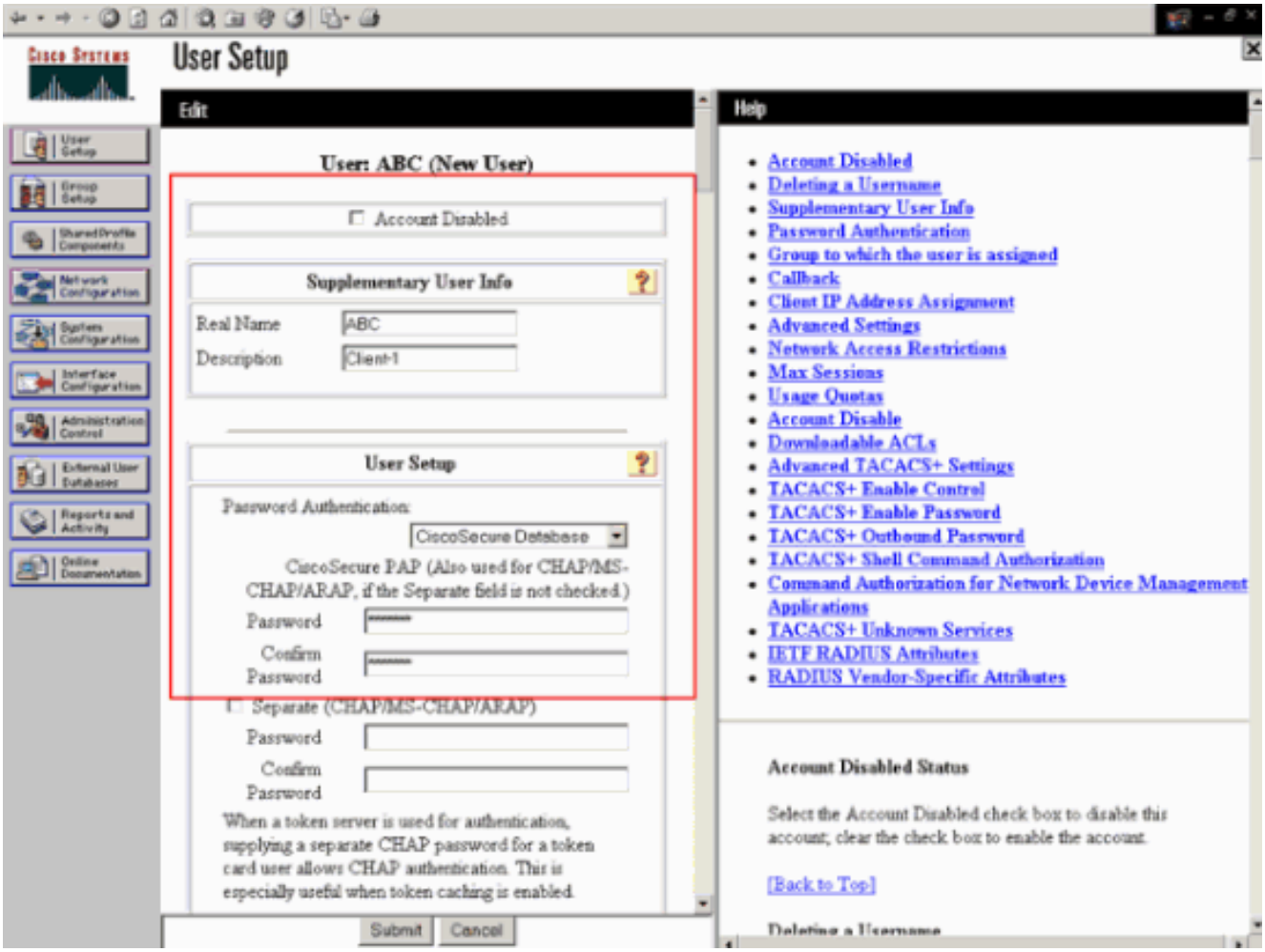
Gehen Sie wie folgt vor, um eine Benutzerdatenbank zu erstellen und die EAP-Authentifizierung auf dem Cisco Secure ACS zu aktivieren:

1. Wählen Sie **User Setup** (Benutzereinrichtung) aus der ACS-GUI aus, geben Sie den Benutzernamen ein, und klicken Sie auf **Hinzufügen/Bearbeiten**. In diesem Beispiel ist der Benutzer

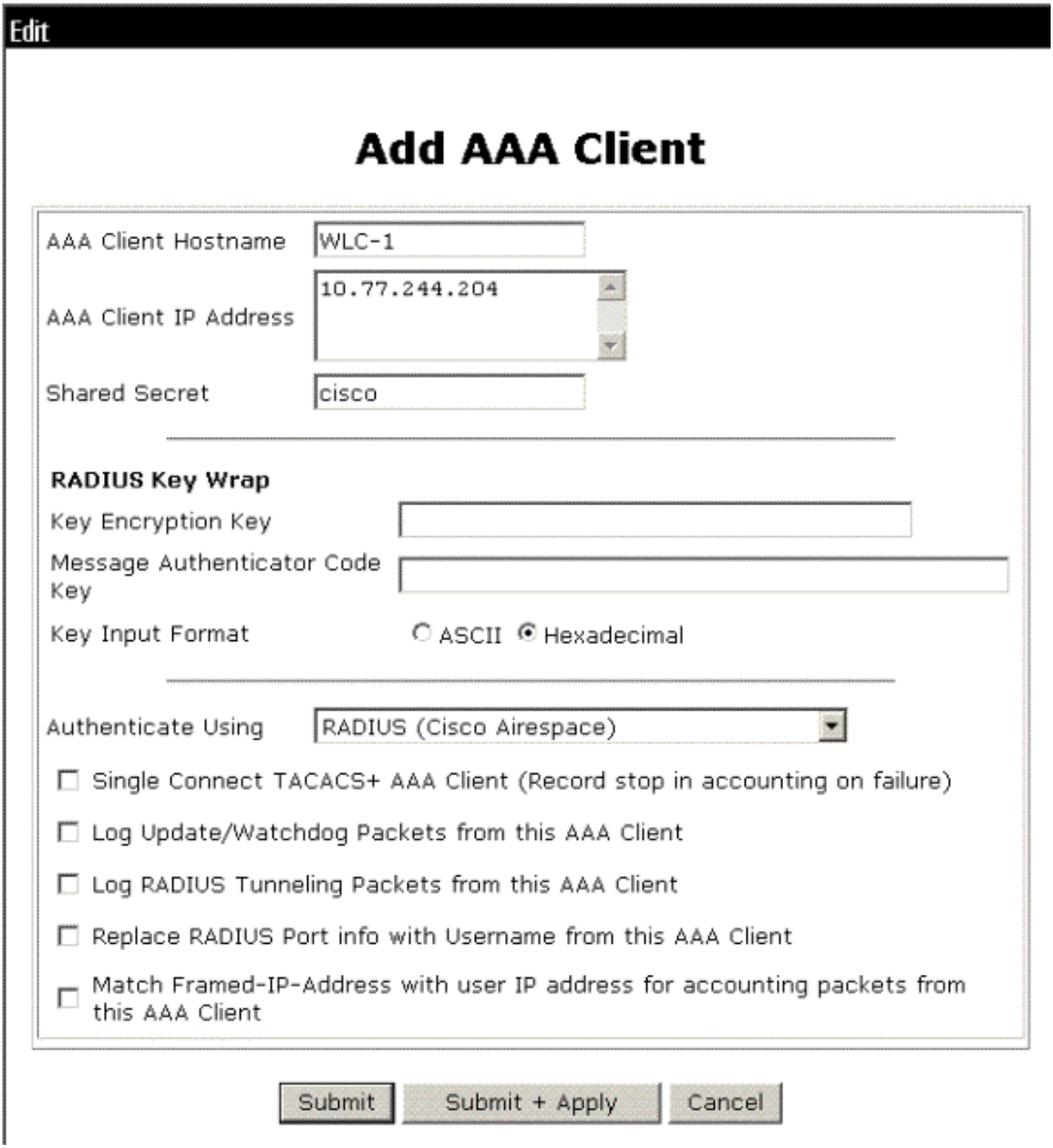
ABC.



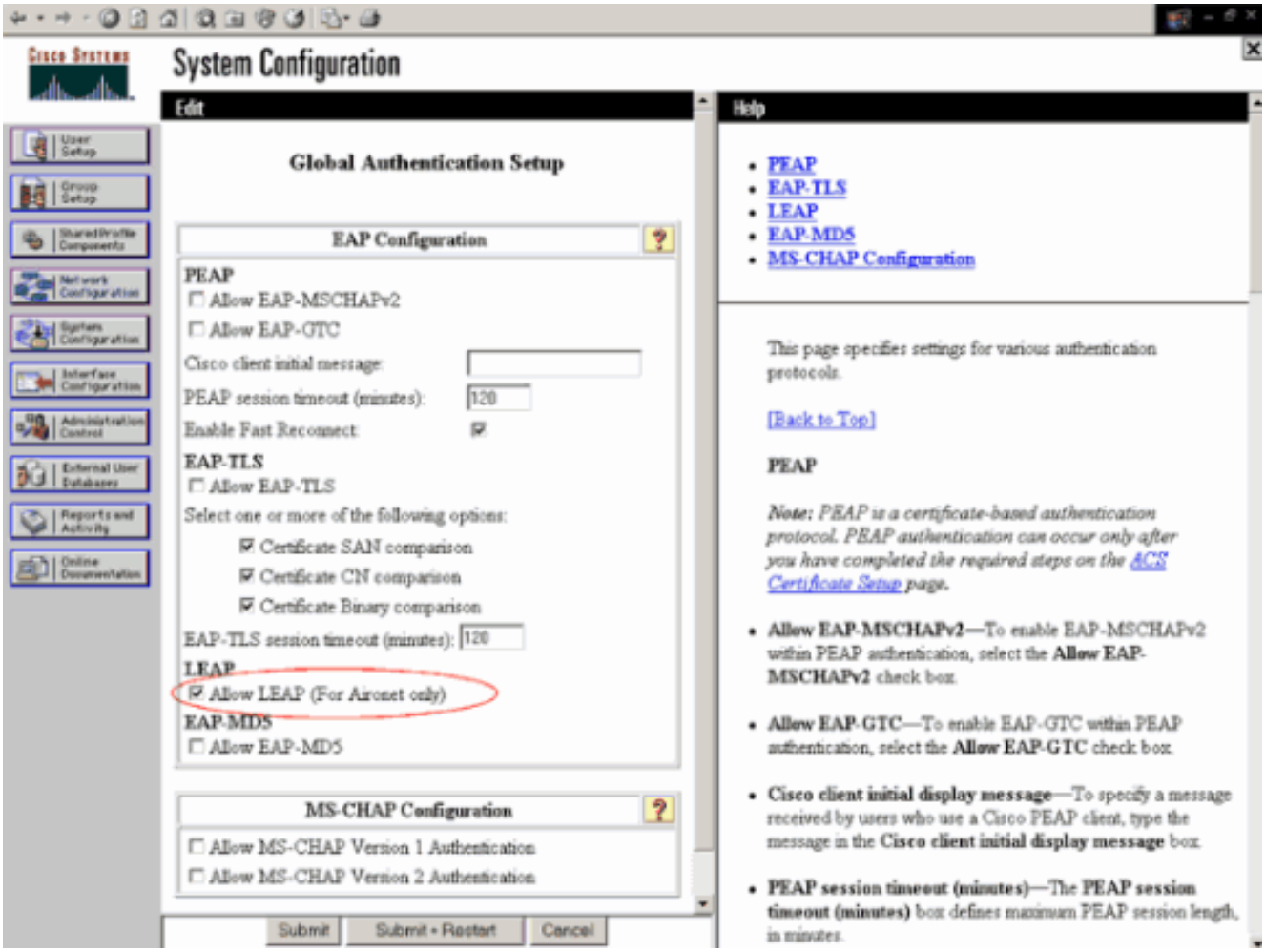
2. Wenn die Seite User Setup (Benutzereinrichtung) angezeigt wird, definieren Sie alle für den Benutzer spezifischen Parameter. In diesem Beispiel werden Benutzername, Kennwort und zusätzliche Benutzerinformationen konfiguriert, da Sie diese Parameter nur für die EAP-Authentifizierung benötigen.Klicken Sie auf **Senden**, und wiederholen Sie den gleichen Vorgang, um der Datenbank weitere Benutzer hinzuzufügen. Standardmäßig werden alle Benutzer in der Standardgruppe gruppiert und erhalten die gleiche Richtlinie wie für die Gruppe. Weitere Informationen zum Zuweisen bestimmter Benutzer zu verschiedenen Gruppen finden Sie im Benutzerhandbuch für Cisco Secure ACS für Windows Server 3.2 im Bereich für die Verwaltung von Benutzergruppen.



3. Definieren Sie den Controller als AAA-Client auf dem ACS-Server. Klicken Sie in der ACS-GUI auf **Netzwerkkonfiguration**.Wenn die Seite "Network Configuration" (Netzwerkkonfiguration) angezeigt wird, definieren Sie den Namen des WLC, die IP-Adresse, den gemeinsamen geheimen Schlüssel und die Authentifizierungsmethode (RADIUS Cisco Air). Informationen zu anderen Nicht-ACS-Authentifizierungsservern finden Sie in der Dokumentation des Herstellers.**Hinweis:** Der gemeinsam verwendete geheime Schlüssel, den Sie auf dem WLC und dem ACS-Server konfigurieren, muss übereinstimmen. Beim gemeinsamen geheimen Schlüssel wird die Groß- und Kleinschreibung beachtet.



4. Klicken Sie auf **Systemkonfiguration** und **Globales Authentifizierungs-Setup**, um sicherzustellen, dass der Authentifizierungsserver so konfiguriert ist, dass er die gewünschte EAP-Authentifizierungsmethode ausführt. Wählen Sie unter den EAP-Konfigurationseinstellungen die entsprechende EAP-Methode aus. In diesem Beispiel wird die LEAP-Authentifizierung verwendet. Klicken Sie abschließend auf **Senden**.

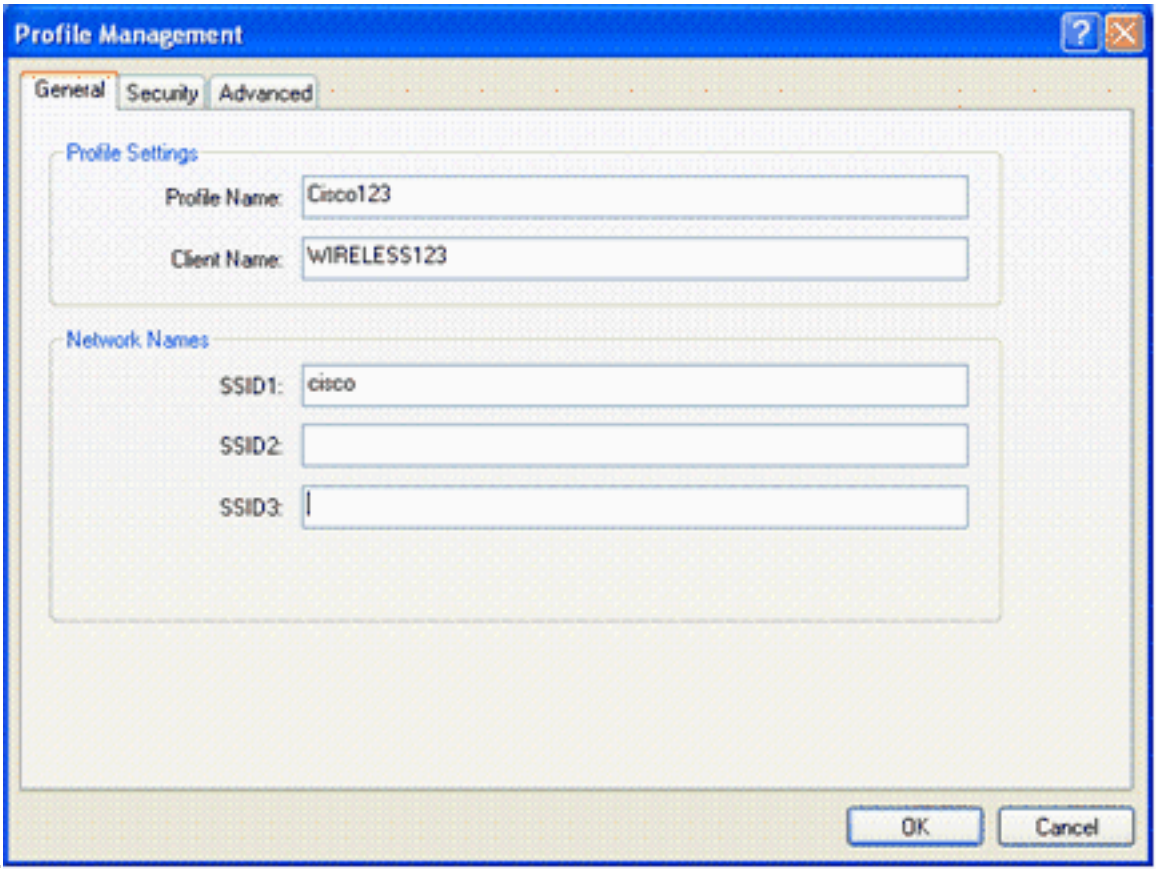


Konfigurieren des Clients

Der Client sollte auch für den entsprechenden EAP-Typ konfiguriert werden. Der Client schlägt dem Server während des EAP-Verhandlungsprozesses den EAP-Typ vor. Wenn der Server diesen EAP-Typ unterstützt, bestätigt er den EAP-Typ. Wenn der EAP-Typ nicht unterstützt wird, sendet er eine Negative-Bestätigung, und der Client handelt erneut mit einer anderen EAP-Methode aus. Dieser Prozess wird fortgesetzt, bis ein unterstützter EAP-Typ ausgehandelt wird. In diesem Beispiel wird LEAP als EAP-Typ verwendet.

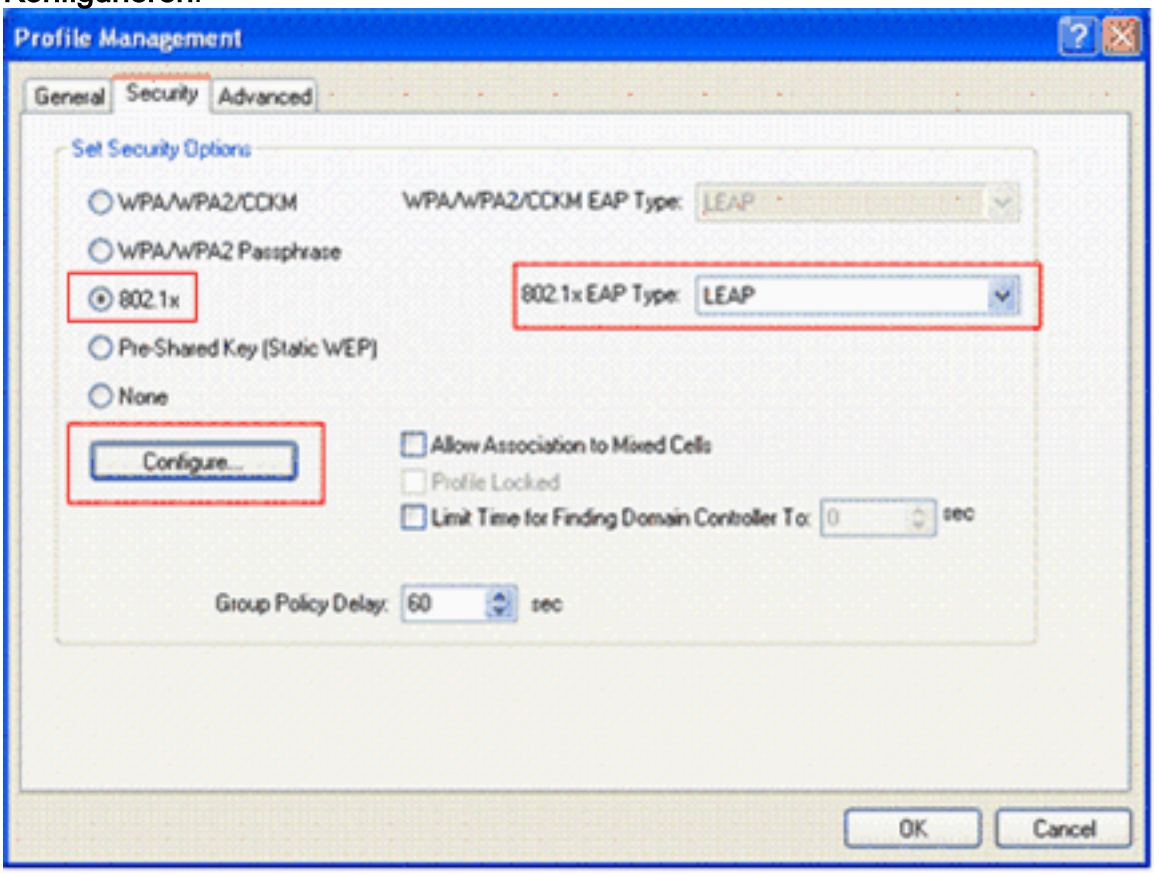
Führen Sie diese Schritte aus, um LEAP auf dem Client mit dem Aironet Desktop Utility zu konfigurieren.

1. Doppelklicken Sie auf das Symbol **Aironet Utility**, um es zu öffnen.
2. Klicken Sie auf die Registerkarte **Profilverwaltung**.
3. Klicken Sie auf ein Profil, und wählen Sie **Ändern aus**.
4. Wählen Sie auf der Registerkarte Allgemein einen *Profilnamen aus*. Geben Sie die **SSID** des WLAN

ein. 

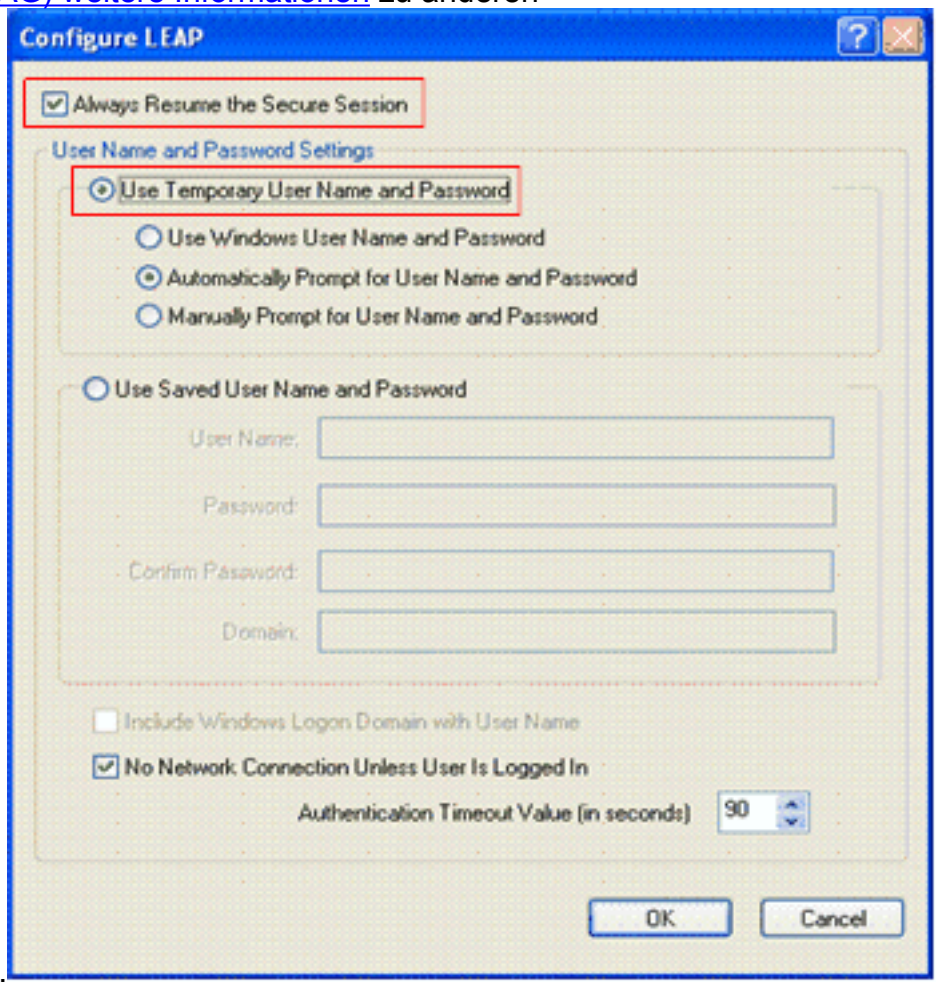
Hinweis: Bei der SSID wird die Groß- und Kleinschreibung beachtet, und sie muss genau mit der auf dem WLC konfigurierten SSID übereinstimmen.

5. Wählen Sie auf der Registerkarte **Sicherheit** die Option *802.1x aus*. Wählen Sie den EAP-Typ als **LEAP aus** und klicken Sie auf **Konfigurieren**.



6. Wählen Sie **Temporärer Benutzername und temporäres Kennwort verwenden aus**, um Sie bei jedem Neustart des Computers zur Eingabe der Benutzeranmeldeinformationen

aufzufordern.Wählen Sie eine der drei Optionen aus, die hier angegeben sind. In diesem Beispiel wird die **automatische Aufforderung zur Eingabe von Benutzername und Kennwort** verwendet. Sie müssen zusätzlich zum *Windows-Benutzernamen und -Kennwort* vor der Anmeldung bei Fenstern die *LEAP*-Benutzeranmeldeinformationen eingeben.Aktivieren Sie das Kontrollkästchen **Immer die sichere Sitzung fortsetzen** am oberen Fensterrand, wenn die LEAP-Komponente immer versuchen soll, die vorherige Sitzung wiederaufzunehmen, ohne dass Sie aufgefordert werden müssen, Ihre Anmeldeinformationen erneut einzugeben, wenn der Client-Adapter rommt und dem Netzwerk erneut zugeordnet wird.**Hinweis:** Im Abschnitt Konfigurieren des Client-Adapters finden Sie im Dokument Installations- und Konfigurationsanleitung für Cisco Aironet 802.11a/b/g Wireless LAN Client Adapter (CB21AG und PI21AG) weitere Informationen zu anderen Optionen.



7. Auf der Registerkarte **Erweitert** können Sie die Präambel-, Aironet- und andere 802.11-Optionen wie Stromversorgung, Frequenz usw. konfigurieren.
8. Klicken Sie auf **OK**. Der Client versucht nun, die konfigurierten Parameter zuzuordnen.

Überprüfung

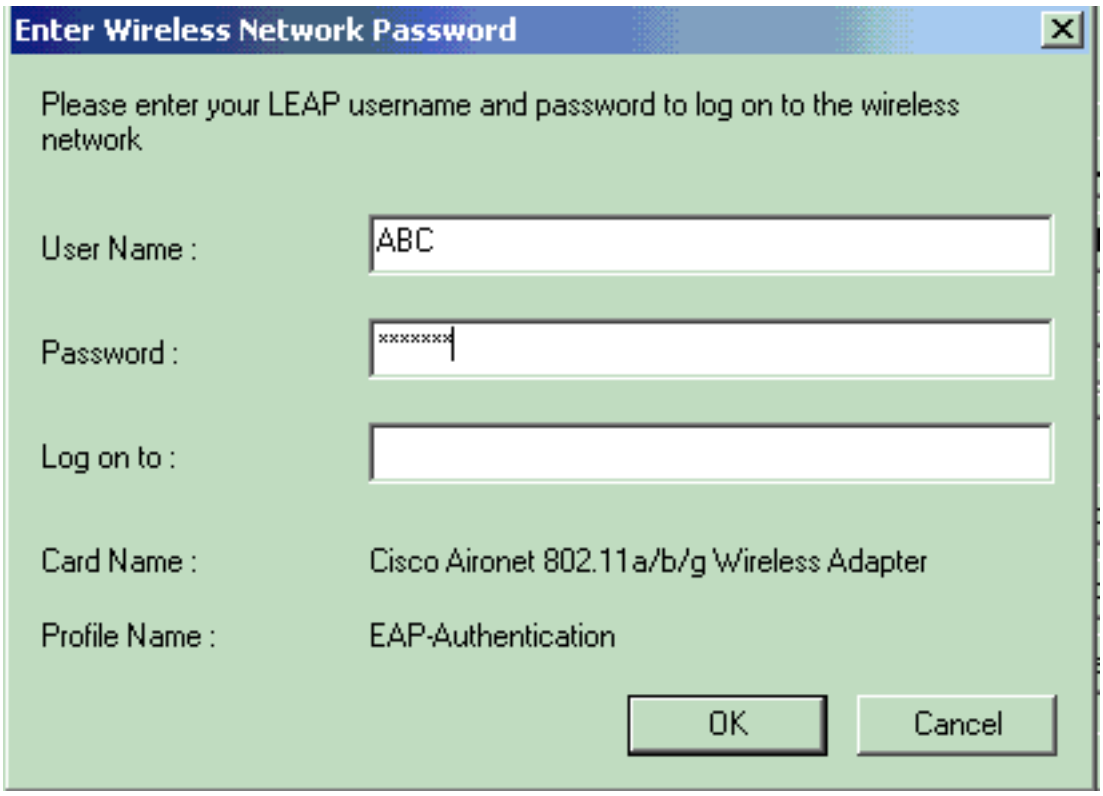
In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Versuchen Sie, mithilfe der LEAP-Authentifizierung einen Wireless-Client mit dem Lightweight AP zu verknüpfen, um zu überprüfen, ob die Konfiguration wie erwartet funktioniert.

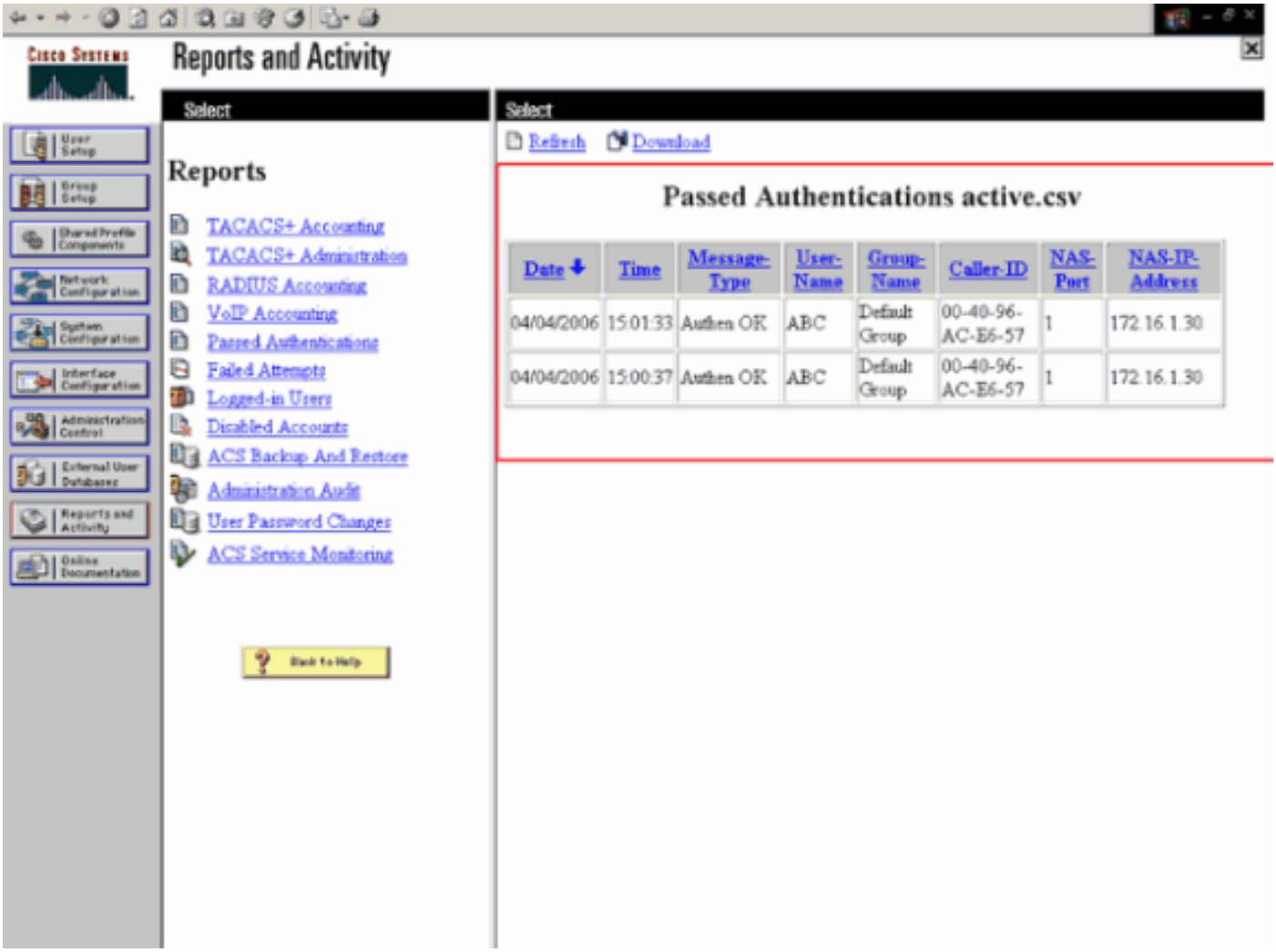
Hinweis: In diesem Dokument wird davon ausgegangen, dass das Clientprofil für die LEAP-Authentifizierung konfiguriert ist. Weitere Informationen zur Konfiguration des 802.11a/b/g-Wireless-Client-Adapters für die LEAP-Authentifizierung finden Sie unter Verwenden der EAP-

Authentifizierung.

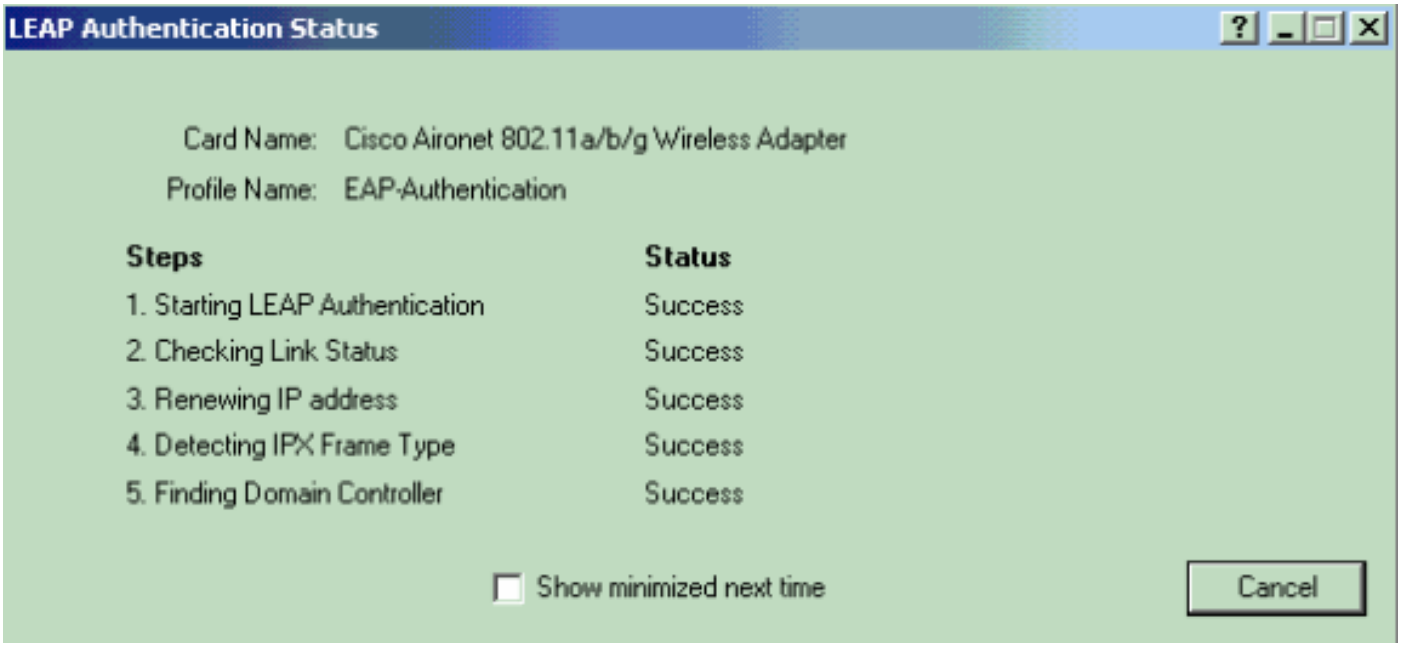
Wenn das Profil für den Wireless-Client aktiviert ist, wird der Benutzer aufgefordert, den Benutzernamen/das Kennwort für die LEAP-Authentifizierung einzugeben. Hier ein Beispiel:



Der Lightweight Access Point und anschließend der WLC übergeben die Benutzeranmeldeinformationen an den externen RADIUS-Server (Cisco Secure ACS), um die Anmeldeinformationen zu validieren. Der RADIUS-Server vergleicht die Daten mit der Benutzerdatenbank und ermöglicht den Zugriff auf den Wireless-Client, wenn die Benutzeranmeldeinformationen gültig sind, um die Benutzeranmeldeinformationen zu überprüfen. Der Bericht über die ausgegebene Authentifizierung auf dem ACS-Server zeigt, dass der Client die RADIUS-Authentifizierung bestanden hat. Hier ein Beispiel:



Nach erfolgreicher RADIUS-Authentifizierung ordnet der Wireless-Client dem Lightweight AP zu.

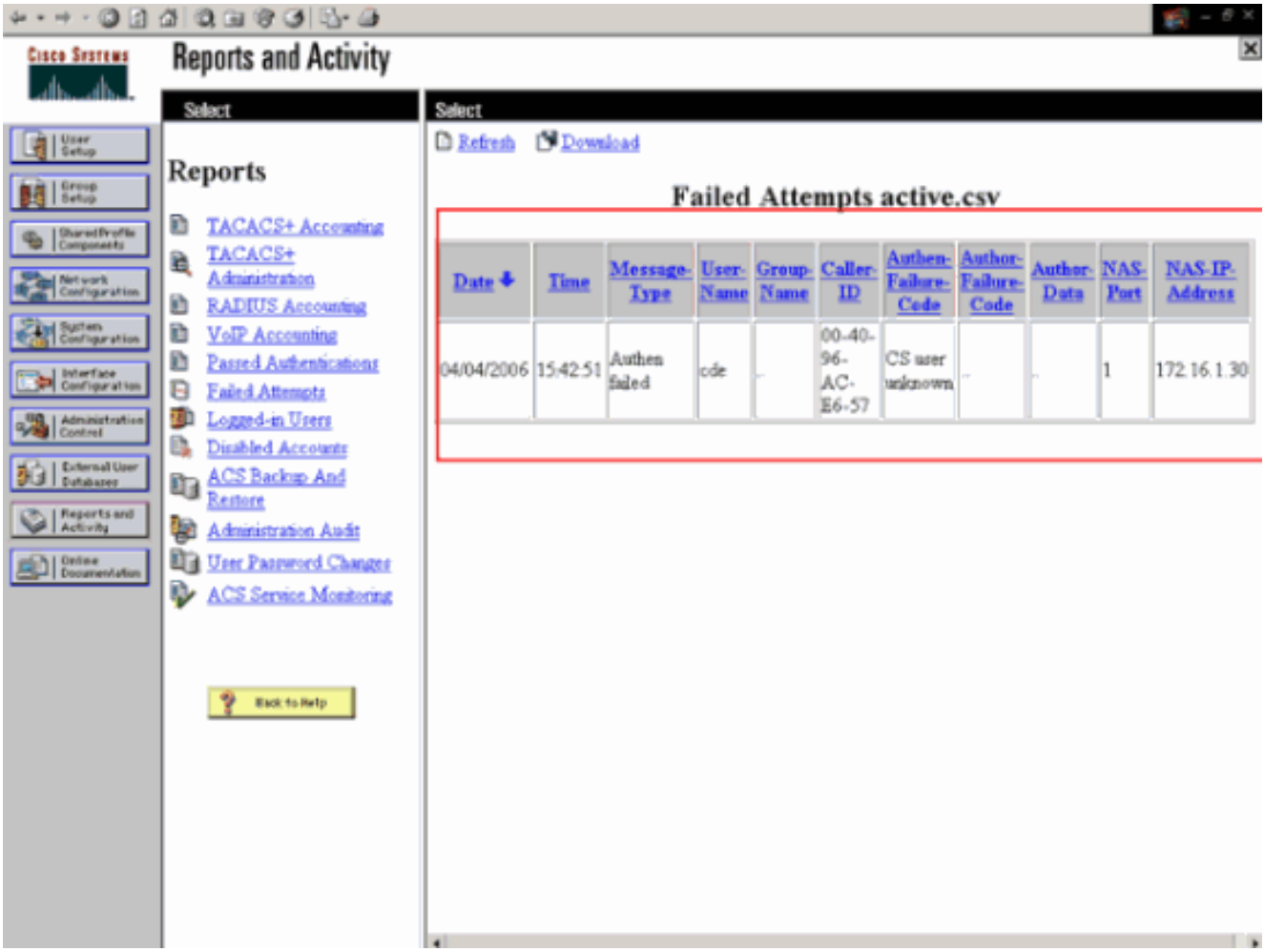


Dies kann auch auf der Registerkarte **Monitor** der WLC-GUI überprüft werden. Wählen Sie **Monitor > Clients** aus, und überprüfen Sie die MAC-Adresse des Clients.

Fehlerbehebung

Gehen Sie wie folgt vor, um die Fehlerbehebung für die Konfigurationen durchzuführen:

1. Verwenden Sie den Befehl **debug lwapp events enable**, um zu überprüfen, ob der Access Point beim WLC registriert.
2. Überprüfen Sie, ob der RADIUS-Server die Authentifizierungsanfrage vom Wireless-Client empfängt und validiert. Überprüfen Sie die NAS-IP-Adresse, das Datum und die Uhrzeit, um festzustellen, ob der WLC den Radius-Server erreichen konnte.Überprüfen Sie dazu die Berichte "Erfolgreiche Authentifizierung" und "Fehlgeschlagene Versuche" auf dem ACS-Server. Diese Berichte stehen unter "Berichte und Aktivitäten" auf dem ACS-Server zur Verfügung. Im folgenden Beispiel schlägt die RADIUS-Serverauthentifizierung fehl:



Hinweis: Informationen zur Fehlerbehebung und zum Abrufen von Debuginformationen für Cisco Secure ACS für Windows finden Sie unter Abrufen von Version- und AAA-Debuginformationen für Cisco Secure ACS.

3. Sie können diese **Debug-**Befehle auch zur Fehlerbehebung bei der AAA-Authentifizierung verwenden:**debug aaa all enable**: Konfiguriert das Debuggen aller AAA-Meldungen.**debug dot1x packet enable**: Aktiviert das Debuggen aller dot1x-Pakete.Im Folgenden finden Sie eine Beispielausgabe des Befehls **debug 802.1x aaa enable**:

```
(Cisco Controller) >debug dot1x aaa enable

*Sep 23 15:15:43.792: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31)
    index=1
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30)
    index=2
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32)
    index=5
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=11
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 AAA EAP Packet created request =
    0x1533a288.. !!!!
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Sending EAP Attribute (code=2, length=8,
    id=2) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.794: 00000000: 02 02 00 08 01 41 42 43
    .....ABC
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 [BE-req] Sending auth request to
    'RADIUS' (proto 0x140001)
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Interim
    Response'
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 AAA Message 'Interim Response' received
    for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 Received EAP Attribute (code=1,
    length=19,id=3, dot1xcb->id = 2) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.799: 00000000: 01 03 00 13 11 01 00 08  42 3a 8e d1 18 24 e8 9f
    ........B:...
*Sep 23 15:15:43.799: 00000010: 41 42 43
    ABC
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile
    00:40:96:ac:dd:05
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31)
    index=1
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30)
    index=2
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32)
    index=5
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_RAD_STATE(24) index=11
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=12
```

```
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 AAA EAP Packet created request =
    0x1533a288.. !!!!
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Sending EAP Attribute (code=2,
    length=35, id=3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.902: 00000000: 02 03 00 23 11 01 00 18  83 f1 5b 32 cf 65 04 ed
    ...#......[2.e..
*Sep 23 15:15:43.902: 00000010: da c8 4f 95 b4 2e 35 ac  c0 6b bd fa 57 50 f3 13
    ..O...5..k..WP..
*Sep 23 15:15:43.904: 00000020: 41 42 43
    ABC
*Sep 23 15:15:43.904: 00:40:96:ac:dd:05 [BE-req] Sending auth request to
    'RADIUS' (proto 0x140001)
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Interim
    Response'
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 AAA Message 'Interim Response' received
    for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 Received EAP Attribute (code=3,
    length=4,id=3, dot1xcb->id = 3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.907: 00000000: 03 03 00 04
    ....
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile
    00:40:96:ac:dd:05
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31)
    index=1
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30)
    index=2
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32)
    index=5
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_RAD_STATE(24) index=11
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=12
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 AAA EAP Packet created request =
    0x1533a288.. !!!!
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Sending EAP Attribute (code=1,
    length=19, id=3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.915: 00000000: 01 03 00 13 11 01 00 08  29 23 be 84 e1 6c d6 ae
    ........)#...l..
*Sep 23 15:15:43.915: 00000010: 41 42 43
    ABC
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 [BE-req] Sending auth request to
    'RADIUS' (proto 0x140001)
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Success'
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 AAA Message 'Success' received for
    mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[0]: attribute 8,
    vendorId 0, valueLen 4
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[1]: attribute 79,
    vendorId 0, valueLen 35
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 Received EAP Attribute (code=2,
    length=35,id=3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.918: 00000000: 02 03 00 23 11 01 00 18  03 66 2c 6a b3 a6 c3 4c
    ...#.....f,j...L
*Sep 23 15:15:43.918: 00000010: 98 ac 69 f0 1b e8 8f a2  29 eb 56 d6 92 ce 60 a6
    ..i.....).V...`.
*Sep 23 15:15:43.918: 00000020: 41 42 43
```

```
    ABC
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[2]: attribute 1,
    vendorId 9, valueLen 16
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[3]: attribute 25,
    vendorId 0, valueLen 21
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[4]: attribute 80,
    vendorId 0, valueLen 16
```

Hinweis: Einige der Zeilen in der Debugausgabe wurden aufgrund von Platzhalterbeschränkungen eingeschlossen.

4. Überwachen Sie die Protokolle im WLC, um zu überprüfen, ob der RADIUS-Server die Benutzeranmeldeinformationen empfängt. Klicken Sie auf **Monitor**, um die Protokolle der WLC-GUI zu überprüfen. Klicken Sie im Menü auf der linken Seite auf **Statistics (Statistik),** und klicken Sie in der Liste der Optionen auf **Radius-Server**.Dies ist sehr wichtig, da der RADIUS-Server in einigen Fällen niemals die Anmeldeinformationen des Benutzers erhält, wenn die RADIUS-Serverkonfiguration auf dem WLC falsch ist.So werden die Protokolle im WLC angezeigt, wenn die RADIUS-Parameter falsch konfiguriert sind:

Sie können den Befehl **show wlan summary** verwenden, um zu erkennen, welche Ihrer WLANs RADIUS-Serverauthentifizierung verwenden. Anschließend können Sie den Befehl **show client summary** anzeigen, um festzustellen, welche MAC-Adressen (Clients) in RADIUS-WLANs erfolgreich authentifiziert wurden. Sie können dies auch mit den von Cisco Secure ACS begangenen Versuchen oder fehlgeschlagenen Protokollen korrelieren.

Tipps zur Fehlerbehebung

- Überprüfen Sie auf dem Controller, ob der RADIUS-Server im `aktiven` Zustand ist und sich nicht im `Standby-Modus` oder `deaktiviert` befindet.
- Verwenden Sie den Befehl **ping**, um zu überprüfen, ob der Radius-Server vom WLC aus erreichbar ist.
- Überprüfen Sie, ob der RADIUS-Server im Dropdown-Menü des WLAN (SSID) ausgewählt ist.
- Wenn Sie WPA verwenden, müssen Sie das neueste Microsoft WPA-Hotfix für Windows XP SP2 installieren. Außerdem sollten Sie den Treiber für Ihre Client-Komponente auf die neueste aktualisieren.
- Wenn Sie PEAP ausführen, z. B. Zertifikate mit XP, SP2, bei denen die Karten vom Microsoft Wireless-0-Dienstprogramm verwaltet werden, müssen Sie den KB885453-Patch von Microsoft erhalten.Wenn Sie die konfigurationsfreie Windows/Client-Komponente verwenden, deaktivieren Sie **Schnelle Wiederverbindung aktivieren**. Sie können dies tun, wenn Sie **Drahtlose Netzwerkeigenschaften > Drahtlose Netzwerke > Bevorzugte Netzwerke**

auswählen. Wählen Sie dann **SSID > Eigenschaften > Öffnen > WEP > Authentication > EAP type > PEAP > Properties > Enable Fast Reconnect aus**. Sie finden dann am Ende des Fensters die Option zum Aktivieren oder Deaktivieren.

- Wenn Sie Intel 2200 oder 2915 Karten besitzen, lesen Sie die Aussagen auf der Intel Website über die bekannten Probleme mit den Karten:Intel® PRO/Wireless 2200BG NetzwerkschnittstelleIntel® PRO/Wireless 2915ABG NetzwerkschnittstelleLaden Sie die aktuellsten Intel Treiber herunter, um Probleme zu vermeiden. Sie können Intel Treiber unter http://downloadcenter.intel.com/ herunterladen.
- Wenn die aggressive Failover-Funktion in WLC aktiviert ist, ist der WLC zu aggressiv, um den AAA-Server als `nicht antworten` zu markieren. Dies sollte jedoch nicht getan werden, da der AAA-Server möglicherweise nicht nur auf diesen Client reagiert, wenn Sie stummschalten. Es kann eine Antwort auf andere gültige Clients mit gültigen Zertifikaten sein. Der WLC kann jedoch trotzdem den AAA-Server als `nicht antworten` und `nicht funktionsfähig` markieren.Um dies zu vermeiden, deaktivieren Sie die Funktion für aggressive Ausfallsicherung. Führen Sie dazu den Befehl **Config RADIUS Aggressive-Failover Disable** (**aggressives Failover-Deaktivierung** im Konfigurationsradius der Benutzeroberfläche des Controllers aus. Wenn diese Option deaktiviert ist, wird der Controller nur dann zum nächsten AAA-Server umgeleitet, wenn drei aufeinander folgende Clients keine Antwort vom RADIUS-Server erhalten.

Bearbeiten von EAP-Timern

Während der 802.1x-Authentifizierung wird dem Benutzer möglicherweise der `DOT1X-1-MAX_EAPOL_KEY_RETRANS_FOR_MOBILE angezeigt: MAX EAPOL-Key M1-Neuübertragungen für mobile xx:xx:xx:xx:xx:xx` Fehlermeldung `erreicht`.

Diese Fehlermeldungen weisen darauf hin, dass der Client während der 802.1x-Schlüsselverhandlung (WPA) nicht rechtzeitig auf den Controller geantwortet hat. Der Controller legt einen Timer für eine Antwort während der Schlüsselverhandlung fest. Wenn Sie diese Meldung sehen, liegt sie in der Regel an einem Problem mit der Komponente. Stellen Sie sicher, dass Sie die aktuellsten Versionen der Client-Treiber und -Firmware ausführen. Auf dem WLC gibt es einige EAP-Timer, die Sie bearbeiten können, um die Client-Authentifizierung zu unterstützen. Zu diesen EAP-Timern gehören:

```
EAP-Identity-Request Timeout
EAP-Identity-Request Max Retries
EAP-Request Timeout (seconds)
EAP-Request Max Retries
EAPOL-Key Timeout
EAPOL-Key Max Retries
```

Bevor Sie diese Werte ändern können, müssen Sie wissen, was sie tun und wie sich deren Änderung auf das Netzwerk auswirkt:

- **Timeout für EAP-Identitätsanforderung:**Dieser Timer beeinflusst, wie lange Sie zwischen EAP-Identitätsanforderungen warten. Standardmäßig ist dies eine Sekunde (4.1 und niedriger) und 30 Sekunden (4.2 und höher). Der Grund dafür war, dass einige Clients, Handhelds, Telefone, Scanner usw. schwer genug reagierten. Geräte wie Laptops erfordern in der Regel keine Manipulation dieser Werte. Der verfügbare Wert liegt zwischen 1 und 120.Was passiert also, wenn dieses Attribut auf einen Wert von 30 festgelegt ist? Wenn der Client die erste

Verbindung herstellt, sendet er einen EAPOL Start an das Netzwerk, und der WLC sendet ein EAP-Paket, in dem die Identität des Benutzers oder Rechners angefordert wird. Wenn der WLC die Identitätsantwort nicht erhält, sendet er 30 Sekunden nach dem ersten Identitätsantrag eine weitere Identitätsanforderung. Dies geschieht bei der Erstverbindung und beim Roaming des Clients.Was passiert, wenn wir diesen Timer erhöhen? Wenn alles gut ist, gibt es keine Auswirkungen. Wenn jedoch ein Problem im Netzwerk vorliegt (einschließlich Client-Problemen, AP-Problemen oder RF-Problemen), kann dies zu Verzögerungen bei der Netzwerkverbindung führen. Wenn Sie beispielsweise den Timer auf den Maximalwert von 120 Sekunden festlegen, wartet der WLC zwischen Identitätsanforderungen 2 Minuten. Wenn der Client Roaming nutzt und die Antwort nicht beim WLC eingeht, haben wir mindestens einen Ausfall von zwei Minuten für diesen Client erstellt.Empfehlungen für diesen Timer sind *5*. Derzeit gibt es keinen Grund, diesen Timer auf seinen maximalen Wert zu setzen.

- **EAP-Identity-Request Max-Wiederholungen:**Der Wert Max Retries ist die Anzahl der Male, in denen der WLC die Identitätsanforderung an den Client sendet, bevor der Eintrag aus dem MSCB entfernt wird. Sobald der Max Retries erreicht ist, sendet der WLC einen De-Authentication-Frame an den Client, wodurch der EAP-Prozess neu gestartet werden muss. Der verfügbare Wert liegt zwischen 1 und 20. Als Nächstes werden wir uns das genauer ansehen.Die Einstellung Max Retries (Maximale Wiederholung) funktioniert mit der Identity Timeout (Identitätszeitüberschreitung). Wenn Sie Ihren Identity Timeout auf 120 eingestellt haben und Ihre Max Retries auf 20, wie lange dauert es 2400 (oder 120 * 20). Das bedeutet, dass es 40 Minuten dauern würde, bis der Client entfernt wird und der EAP-Prozess wieder gestartet wird. Wenn Sie das Identity Timeout auf 5 festlegen, mit einem Wert für die maximale Wiederholung von 12, dann dauert es 60 (oder 5 x 12). Im Gegensatz zum vorherigen Beispiel dauert es eine Minute bis der Client entfernt ist und muss EAP neu starten.Die Empfehlungen für die Max Retries sind *12*.
- **EAPOL-Schlüssel-Timeout:**Der Standardwert für das EAPOL-Key-Timeout ist 1 Sekunde oder 1.000 Millisekunden. Das bedeutet, dass der Access Point beim Austausch der EAPOL-Schlüssel zwischen dem Access Point und dem Client den Schlüssel sendet und standardmäßig bis zu 1 Sekunde wartet, bis der Client antwortet. Nach dem Warten auf den definierten Zeitwert überträgt der Access Point den Schlüssel erneut. Sie können den **Befehl config advanced eap eapol-key-timeout *<time>*** verwenden, um diese Einstellung zu ändern. Die verfügbaren Werte in 6.0 liegen zwischen 200 und 5.000 Millisekunden, während bei Codes vor 6.0 Werte zwischen 1 und 5 Sekunden möglich sind. Wenn Sie einen Client haben, der nicht auf einen Schlüsselversuch reagiert, können Sie bei einer Verlängerung der Timer mehr Zeit für eine Antwort haben. Dies kann jedoch auch die Zeit verlängern, die der WLC/AP benötigt, um den Client zu deauthentifizieren, damit der gesamte 802.1x-Prozess neu beginnt.
- **EAPOL-Schlüssel Max. Wiederholungen:**Der Standardwert für den Wert "EAPOL-Key Max Retries" ist 2. Dies bedeutet, dass wir den ursprünglichen Schlüsselversuch an den Client zweimal wiederholen. Diese Einstellung kann mit dem **Befehl config advanced eap eapol-key-retries *<retries>*** geändert werden. Die verfügbaren Werte liegen zwischen 0 und 4 Wiederholungen. Wenn der Standardwert für das EAPOL-Key-Timeout (d. h. 1 Sekunde) und der Standardwert für den EAPOL-Key Retry (2) verwendet wird, läuft der Vorgang wie folgt ab, wenn ein Client nicht auf den ersten Schlüsselversuch reagiert:Der Access Point sendet einen Schlüsselversuch an den Client.Sie wartet eine Sekunde auf eine Antwort.Wenn keine Antwort erfolgt, wird der erste EAPOL-Key Retry verschickt.Sie wartet eine Sekunde auf eine Antwort.Wenn keine Antwort erfolgt, wird der zweite EAPOL-Key Retry verschickt.Wenn der Client immer noch keine Antwort gibt und der Wiederholungswert erreicht wird, wird der Client deauthentifiziert. Wie beim EAPOL-Key-Timeout kann auch hier eine Verlängerung des

EAPOL-Key-Wiederholungswerts unter Umständen von Vorteil sein. Die Einstellung auf das Maximum kann jedoch wieder schädlich sein, da die deauthentifizierte Nachricht verlängert wird.

Extrahieren der Paketdatei vom ACS RADIUS-Server zur Fehlerbehebung

Wenn Sie ACS als externen Radius-Server verwenden, können Sie mit diesem Abschnitt eine Fehlerbehebung für Ihre Konfiguration durchführen. Die Datei package.cab ist eine Zip-Datei, die alle notwendigen Dateien enthält, um ACS effizient zu beheben. Sie können das Dienstprogramm CSSupport.exe verwenden, um die Datei package.cab zu erstellen, oder Sie können die Dateien manuell erfassen.

Weitere Informationen zum Erstellen und Extrahieren der Paketdatei aus dem WCS finden Sie im Abschnitt Erstellen einer Datei "package.cab" *unter Abrufen von Version- und AAA-Debuginformationen für Cisco Secure ACS für Windows*.

Zugehörige Informationen

- Konfigurationsbeispiel für WLAN-Controller-Failover für Lightweight Access Points
- Software-Upgrade für Wireless LAN Controller
- Cisco Wireless LAN Controller - Befehlsreferenz
- Technischer Support und Dokumentation für Cisco Systeme