Beispiele für Wireless-Authentifizierungstypen in einem festkonfigurierten ISR

Inhalt

Einleitung

Dieses Dokument enthält ein Konfigurationsbeispiel, in dem erläutert wird, wie verschiedene Layer-2-Authentifizierungstypen auf einem integrierten Cisco Wireless-Router mit fester Konfiguration für Wireless-Verbindungen mit CLI-Befehlen konfiguriert werden.

Voraussetzungen

Anforderungen

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

- Grundkenntnisse der Konfiguration der Eckwerte des Cisco Integrated Services Routers (ISR)
- Kenntnisse der Konfiguration des 802.11a/b/g Wireless Client-Adapters mit dem Aironet Desktop Utility (ADU)

Verwendete Komponenten

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

- Cisco 877W ISR mit Cisco IOS® Softwareversion 12.3(8)YI1
- Laptop mit Aironet Desktop Utility Version 3.6
- 802.11 a/b/g Client-Adapter, der Firmware-Version 3.6 ausführt

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 in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Die Cisco Integrated Services Router mit fester Konfiguration unterstützen eine sichere, erschwingliche und benutzerfreundliche Wireless LAN-Lösung, die Mobilität und Flexibilität mit den von Netzwerkexperten benötigten Funktionen der Enterprise-Klasse kombiniert. Mit einem auf der Cisco IOS-Software basierenden Managementsystem fungieren die Cisco Router als Access Points und sind Wi-Fi-zertifizierte, IEEE 802.11a/b/g-konforme Wireless LAN-Transceiver.

Sie können die Router über die Befehlszeilenschnittstelle (CLI), das browserbasierte Managementsystem oder das Simple Network Management Protocol (SNMP) konfigurieren und überwachen. In diesem Dokument wird beschrieben, wie der ISR für die Wireless-Verbindung mit den CLI-Befehlen konfiguriert wird.

Konfigurieren

In diesem Beispiel wird veranschaulicht, wie diese Authentifizierungstypen auf einem Cisco Wireless Integrated Fixed Configuration Router mit CLI-Befehlen konfiguriert werden.

- Offene Authentifizierung
- 802.1x/EAP-Authentifizierung (Extensible Authentication Protocol)
- Wi-Fi Protected Access Pre-Shared Key (WPA-PSK)-Authentifizierung
- WPA-Authentifizierung (mit EAP)

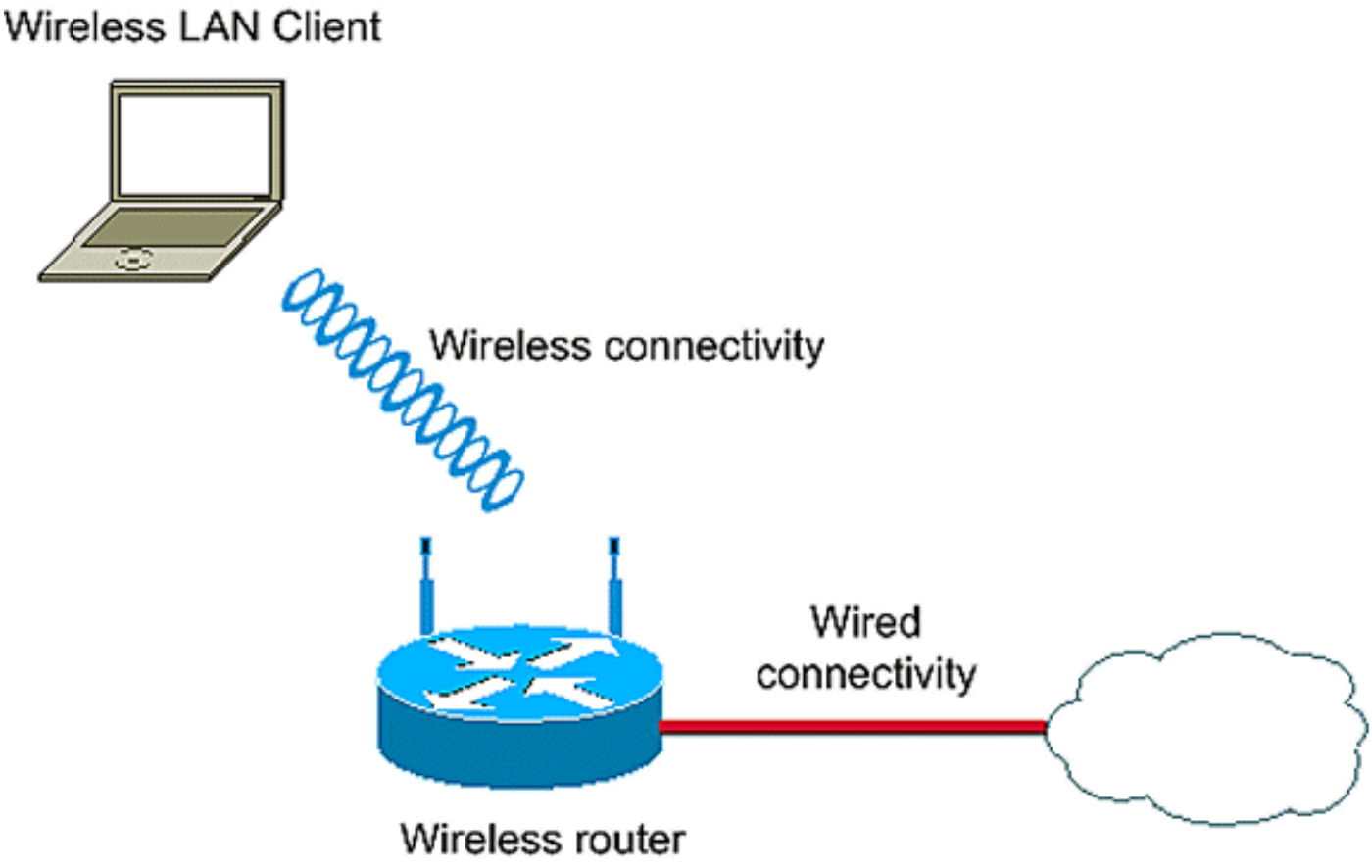
Hinweis: Dieses Dokument konzentriert sich nicht auf die gemeinsame Authentifizierung, da es sich um einen weniger sicheren Authentifizierungstyp handelt.

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 Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Bei dieser Konfiguration wird der lokale RADIUS-Server auf dem Wireless ISR zur Authentifizierung von Wireless-Clients mit 802.1x-Authentifizierung verwendet.

Konfigurieren der offenen Authentifizierung

Die offene Authentifizierung ist ein Nullauthentifizierungsalgorithmus. Der Access Point gewährt alle Authentifizierungsanfragen. Die offene Authentifizierung ermöglicht jedem Gerät den Zugriff auf das Netzwerk. Wenn im Netzwerk keine Verschlüsselung aktiviert ist, kann jedes Gerät, das die SSID des Access Points kennt, Zugriff auf das Netzwerk erhalten. Wenn die WEP-Verschlüsselung auf einem Access Point aktiviert ist, wird der WEP-Schlüssel selbst zu einem Mittel zur Zugriffskontrolle. Wenn ein Gerät nicht über den richtigen WEP-Schlüssel verfügt, obwohl die Authentifizierung erfolgreich ist, kann das Gerät keine Daten über den Access Point übertragen. Ebenso wenig können die vom Access Point gesendeten Daten entschlüsselt werden.

In dieser Beispielkonfiguration wird lediglich eine einfache offene Authentifizierung erklärt. Der WEP-Schlüssel kann obligatorisch oder optional gemacht werden. In diesem Beispiel wird der WEP-Schlüssel als optional konfiguriert, sodass jedes Gerät, das WEP nicht verwendet, auch authentifiziert und diesem AP zugeordnet werden kann.

Weitere Informationen finden Sie unter Authentifizierung öffnen.

In diesem Beispiel wird diese Konfiguration verwendet, um die offene Authentifizierung auf dem ISR zu konfigurieren.

- SSID-Name: "offen"
- VLAN 1
- Interner DHCP-Serverbereich: **10.1.0.0/16**

Hinweis: Zur Vereinfachung wird in diesem Beispiel keine Verschlüsselungstechnik für authentifizierte Clients verwendet.

Gehen Sie wie folgt vor:

1. Konfigurieren des Integrated Routing and Bridging (IRB) und Einrichten der Bridge Group
2. Konfigurieren der Bridged Virtual Interface (BVI)
3. Konfigurieren der SSID für die offene Authentifizierung
4. Konfigurieren des internen DHCP-Servers für die Wireless-Clients dieses VLAN

Konfigurieren des Integrated Routing and Bridging (IRB) und Einrichten der Bridge Group

Gehen Sie wie folgt vor:

1. **Aktivieren Sie IRB im Router.**Router<configure>**#Bridge-IRBHinweis:** Wenn alle Sicherheitstypen auf einem Router konfiguriert werden sollen, reicht es aus, IRB nur einmal global auf dem Router zu aktivieren. Sie muss nicht für jeden Authentifizierungstyp aktiviert werden.
2. **Definieren Sie eine Bridge-Gruppe.**In diesem Beispiel wird die Bridge-Gruppen-Nummer **1** verwendet.Router<configure>**#Bridge** ***1***
3. **Wählen Sie das Spanning Tree Protocol für die Bridge-Gruppe aus.**Hier wird das IEEE-

Spanning-Tree-Protokoll für diese Bridge-Gruppe konfiguriert.Router<configure>#**Bridge** *1-Protokollansicht*

4. **Aktivieren Sie eine BVI, um routingfähige Pakete zu akzeptieren und weiterzuleiten, die von der entsprechenden Bridge-Gruppe empfangen wurden.**In diesem Beispiel kann die BVI das IP-Paket akzeptieren und weiterleiten.router<configure>#**bridge** *1* **route** *ip*

Konfigurieren der Bridged Virtual Interface (BVI)

Gehen Sie wie folgt vor:

1. **Konfigurieren Sie die BVI.**Konfigurieren Sie die BVI, wenn Sie der BVI die entsprechende Nummer der Bridge-Gruppe zuweisen. Jede Bridge-Gruppe kann nur eine entsprechende BVI haben. In diesem Beispiel wird der BVI die Bridge-Gruppe Nr. 1 zugewiesen.router<configure>#**interface BVI** *<1>*
2. **Weisen Sie der BVI eine IP-Adresse zu.**router<config-if>#**ip address** *10.1.1.1 255.255.0.0*router<config-if>#**no shutdown**

Weitere Informationen zum Bridging finden Sie unter Configure Bridging.

Konfigurieren der SSID für die offene Authentifizierung

Gehen Sie wie folgt vor:

1. **Aktivieren der Funkschnittstelle**Um die Funkschnittstelle zu aktivieren, gehen Sie zum Konfigurationsmodus für die DOT11-Funkschnittstelle, und weisen Sie der Schnittstelle eine SSID zu.router<config>#**interface dot11radio0**router<config-if>#**no shutdown**router<config-if>#**ssid** *open*Der offene Authentifizierungstyp kann in Kombination mit der MAC-Adressauthentifizierung konfiguriert werden. In diesem Fall zwingt der Access Point alle Client-Geräte zur Authentifizierung der MAC-Adresse, bevor sie dem Netzwerk beitreten dürfen.Die offene Authentifizierung kann auch zusammen mit der EAP-Authentifizierung konfiguriert werden. Der Access Point zwingt alle Client-Geräte zur EAP-Authentifizierung, bevor sie dem Netzwerk beitreten dürfen. Geben Sie für den Listennamen die Authentifizierungsmethodenliste an.Ein für die EAP-Authentifizierung konfigurierter Access Point zwingt alle Client-Geräte, die eine Verbindung herstellen, zur EAP-Authentifizierung. Client-Geräte, die EAP nicht verwenden, können den Access Point nicht verwenden.
2. **Binden der SSID an ein VLAN.**Um die SSID auf dieser Schnittstelle zu aktivieren, binden Sie die SSID im SSID-Konfigurationsmodus an das VLAN.Router<config-ssid>**VLAN** *1*
3. **Konfigurieren Sie die SSID mit einer offenen Authentifizierung.**router<config-ssid>#**authentication open**
4. **Konfigurieren Sie die Funkschnittstelle für den WEP-Schlüssel optional.**router<config>#**encryption vlan** *1* **mode WEP optional**
5. **Aktivieren Sie VLAN auf der Funkschnittstelle.**router<config>#**interface Dot11Radio 0.1**router<config-subif>#**encapsulation dot1Q** *1*router<config-subif>#**bridge-group** *1*

Konfigurieren des internen DHCP-Servers für die Wireless-Clients dieses VLAN

Geben Sie diese Befehle im globalen Konfigurationsmodus ein, um den internen DHCP-Server für die Wireless-Clients dieses VLAN zu konfigurieren:

- **ip dhcp excluded-address 10.1.1.1 10.1.1.5**
- **ip dhcp pool** *offen*

Geben Sie im DHCP-Pool-Konfigurationsmodus die folgenden Befehle ein:

- **netzwerk** *10.1.0.0 255.255.0.0*
- **default-router** *10.1.1.1*

802.1x/EAP-Authentifizierung konfigurieren

Dieser Authentifizierungstyp bietet höchste Sicherheit für Ihr Wireless-Netzwerk. Mit dem Extensible Authentication Protocol (EAP), das für die Interaktion mit einem EAP-kompatiblen RADIUS-Server verwendet wird, unterstützt der Access Point ein Wireless-Client-Gerät und den RADIUS-Server bei der gegenseitigen Authentifizierung und der Ableitung eines dynamischen Unicast-WEP-Schlüssels. Der RADIUS-Server sendet den WEP-Schlüssel an den Access Point, der ihn für alle Unicast-Datensignale verwendet, die er an den Client sendet oder von diesem empfängt.

Weitere Informationen finden Sie unter EAP-Authentifizierung.

In diesem Beispiel wird diese Konfigurationseinrichtung verwendet:

- SSID-Name: **Sprung**
- VLAN 2
- Interner DHCP-Serverbereich: **10.2.0.0/16**

In diesem Beispiel wird die LEAP-Authentifizierung als Mechanismus zur Authentifizierung des Wireless-Clients verwendet.

Hinweis: Informationen zur Konfiguration von EAP-TLS finden Sie unter Cisco Secure ACS für Windows v3.2 mit EAP-TLS-Computerauthentifizierung.

Hinweis: Informationen zur Konfiguration von PEAP-MS-CHAPv2 finden Sie unter Konfigurieren der sicheren Cisco ACS für Windows v3.2 mit PEAP-MS-CHAPv2-Computerauthentifizierung.

Hinweis: Beachten Sie, dass bei der Konfiguration dieser EAP-Typen hauptsächlich Konfigurationsänderungen auf Client- und Authentifizierungsserverseite erforderlich sind. Die Konfiguration auf dem Wireless-Router oder dem Access Point ist für alle Authentifizierungstypen mehr oder weniger identisch.

Hinweis: Wie bereits erwähnt, verwendet diese Konfiguration den lokalen RADIUS-Server auf dem Wireless ISR zur Authentifizierung von Wireless-Clients mit 802.1x-Authentifizierung.

Gehen Sie wie folgt vor:

1. Konfigurieren des Integrated Routing and Bridging (IRB) und Einrichten der Bridge Group
2. Konfigurieren der Bridged Virtual Interface (BVI)
3. Konfigurieren des lokalen RADIUS-Servers für die EAP-Authentifizierung
4. Konfigurieren der SSID für die 802.1x/EAP-Authentifizierung
5. Konfigurieren des internen DHCP-Servers für die Wireless-Clients dieses VLAN

Konfigurieren des Integrated Routing and Bridging (IRB) und Einrichten der Bridge

Group

Gehen Sie wie folgt vor:

1. **Aktivieren Sie IRB im Router.**Router<configure>**#Bridge-IRBHinweis:** Wenn alle Sicherheitstypen auf einem Router konfiguriert werden sollen, reicht es aus, IRB nur einmal global auf dem Router zu aktivieren. Sie muss nicht für jeden Authentifizierungstyp aktiviert werden.
2. **Definieren Sie eine Bridge-Gruppe.**In diesem Beispiel wird die Bridge-Gruppe Nr. 2 verwendet.Router<configure>**#Bridge** ***2***
3. **Wählen Sie das Spanning Tree Protocol für die Bridge-Gruppe aus.**Hier wird das IEEE-Spanning-Tree-Protokoll für diese Bridge-Gruppe konfiguriert.Router<configure>**#Bridge** ***2-Protokollansicht***
4. **Wählen Sie das Spanning Tree Protocol für die Bridge-Gruppe aus.**Hier wird das IEEE-Spanning-Tree-Protokoll für diese Bridge-Gruppe konfiguriert.Router<configure>**#Bridge** ***2-Protokollansicht***
5. **Aktivieren Sie eine BVI, um routingfähige Pakete zu akzeptieren und weiterzuleiten, die von der entsprechenden Bridge-Gruppe empfangen werden.**In diesem Beispiel kann die BVI IP-Pakete akzeptieren und weiterleiten.Router<configure>**#Bridge** ***2*** **route** ***ip***

Konfigurieren der Bridged Virtual Interface (BVI)

Gehen Sie wie folgt vor:

1. **Konfigurieren Sie die BVI.**Konfigurieren Sie die BVI, wenn Sie der BVI die entsprechende Nummer der Bridge-Gruppe zuweisen. Jede Bridge-Gruppe kann nur über eine BVI des Korrespondenten verfügen. In diesem Beispiel wird der BVI die Bridge-Gruppe Nr. 2 zugewiesen.Router<configure>**#Interface BVI** ***<2>***
2. **Weisen Sie der BVI eine IP-Adresse zu.**router<config-if>**#ip address** ***10.2.1.1*** ***255.255.0.0***router<config-if>**#no shutdown**

Konfigurieren des lokalen RADIUS-Servers für die EAP-Authentifizierung

Wie bereits erwähnt, verwendet dieses Dokument den lokalen RADIUS-Server auf dem Wireless-fähigen Router für die EAP-Authentifizierung.

1. **Aktivieren Sie das Zugriffskontrollmodell für Authentifizierung, Autorisierung und Abrechnung (Authentication, Authorization, Accounting - AAA).**Router<configure>**#aaa new-model**
2. **Erstellen Sie eine Rad-Eap für die Servergruppe für den RADIUS-Server.**router<configure>**#aaa group server radius** ***rad-eap*** **server** ***10.2.1.1*** **auth-port** ***1812*** **acct-port** ***1813***
3. **Erstellen Sie eine Methodenliste eap_methods, die die Authentifizierungsmethode auflistet, die zum Authentifizieren des AAA-Anmeldebenutzers verwendet wird. Weisen Sie dieser Servergruppe die Methodenliste zu.**router<configure>**#aaa authentication login** ***eap_methods*** **group** ***rad-eap***
4. **Aktivieren Sie den Router als lokalen Authentifizierungsserver, und wechseln Sie in den Konfigurationsmodus für den Authentifizierer.**router<configure>**#radius-server local**
5. **Fügen Sie im Konfigurationsmodus Radius-Server den Router als AAA-Client des lokalen**

Authentifizierungsservers hinzu.router<config-radsrv>**#nas** *10.2.1.1*-Schlüssel *Cisco*
6. **Konfigurieren Sie** *user1* **auf dem lokalen Radius-Server.**router<config-radsrv>**#user** *user1* **password** *user1* **group** *rad-eap*
7. **Geben Sie den RADIUS-Server-Host an.**router<config-radsrv>**#radius-server host** *10.2.1.1* **auth-port** *1812* **acct-port** *1813* **key** *cisco***Hinweis:** Dieser Schlüssel muss mit dem Schlüssel übereinstimmen, der im **nas-**Befehl im Radius-Server-Konfigurationsmodus angegeben wurde.

Konfigurieren der SSID für die 802.1x/EAP-Authentifizierung

Die Konfiguration der Funkschnittstelle und der zugehörigen SSID für 802.1x/EAP umfasst die Konfiguration verschiedener Wireless-Parameter auf dem Router, darunter die SSID, der Verschlüsselungsmodus und der Authentifizierungstyp. In diesem Beispiel wird die SSID *Sprung* genannt.

1. **Aktivieren Sie die Funkschnittstelle.**Um die Funkschnittstelle zu aktivieren, wechseln Sie zum Konfigurationsmodus für die DOT11-Funkschnittstelle, und weisen Sie der Schnittstelle eine SSID zu.router<config>**#interface dot11radio0**router<config-if>**#no shutdown**router<config-if>**#ssid** *Leap*
2. **Binden der SSID an ein VLAN.**Um die SSID auf dieser Schnittstelle zu aktivieren, binden Sie die SSID im SSID-Konfigurationsmodus an das VLAN.router<config-ssid>**#vlan** *2*
3. **Konfigurieren Sie die SSID mit 802.1x/LEAP-Authentifizierung.**router<config-ssid>**#authentication network-eap** *eap_methods*
4. **Konfigurieren Sie die Funkschnittstelle für die dynamische Schlüsselverwaltung.**router<config>**#encryption vlan** *2* **mode ciphers wep40**
5. **Aktivieren Sie VLAN auf der Funkschnittstelle.**router<config>**#interface Dot11Radio 0.2**router<config-subif>**#encapsulation dot1Q** *2*router<config-subif>**#bridge-group** *2*

Konfigurieren des internen DHCP-Servers für die Wireless-Clients dieses VLAN

Geben Sie diese Befehle im globalen Konfigurationsmodus ein, um den internen DHCP-Server für die Wireless-Clients dieses VLAN zu konfigurieren:

- **ip dhcp excluded-address 10.2.1.1 10.2.1.5**
- **ip dhcp pool** *leapauth*

Geben Sie im DHCP-Pool-Konfigurationsmodus die folgenden Befehle ein:

- **netzwerk** *10.2.0.0 255.255.0.0*
- **default-router** *10.2.1.1*

WPA-Schlüsselverwaltung

Wi-Fi Protected Access ist eine standardbasierte, interoperable Sicherheitserweiterung, die den Datenschutz und die Zugriffskontrolle für aktuelle und zukünftige WLAN-Systeme erheblich erhöht.

Weitere Informationen finden Sie unter WPA-Schlüsselverwaltung.

WPA-Schlüsselverwaltung unterstützt zwei sich gegenseitig ausschließende Managementtypen:

WPA-Pre-Sshared Key (WPA-PSK) und WPA (mit EAP).

Konfigurieren von WPA-PSK

WPA-PSK wird in einem WLAN, in dem keine 802.1x-basierte Authentifizierung verfügbar ist, als Schlüsselverwaltungstyp verwendet. In solchen Netzwerken müssen Sie einen vorinstallierten Schlüssel auf dem Access Point konfigurieren. Sie können den vorinstallierten Schlüssel als ASCII- oder Hexadezimalzeichen eingeben. Wenn Sie den Schlüssel als ASCII-Zeichen eingeben, müssen Sie zwischen 8 und 63 Zeichen eingeben, und der Access Point erweitert den Schlüssel mit dem im kennwortbasierten Verschlüsselungsstandard (RFC2898) beschriebenen Prozess. Wenn Sie den Schlüssel als Hexadezimalzeichen eingeben, müssen Sie 64 Hexadezimalzeichen eingeben.

In diesem Beispiel wird diese Konfigurationseinrichtung verwendet:

- SSID-Name: **WPA-Shared**
- VLAN 3
- Interner DHCP-Serverbereich: **10.3.0.0/16**

Gehen Sie wie folgt vor:

1. Konfigurieren des Integrated Routing and Bridging (IRB) und Einrichten der Bridge Group
2. Konfigurieren der Bridged Virtual Interface (BVI)
3. Konfigurieren der SSID für die WPA-PSK-Authentifizierung
4. Konfigurieren des internen DHCP-Servers für die Wireless-Clients dieses VLAN

Konfigurieren des Integrated Routing and Bridging (IRB) und Einrichten der Bridge Group

Gehen Sie wie folgt vor:

1. **Aktivieren Sie IRB im Router.**Router<configure>**#Bridge-IRBHinweis:** Wenn alle Sicherheitstypen auf einem Router konfiguriert werden sollen, reicht es aus, IRB nur einmal global auf dem Router zu aktivieren. Sie muss nicht für jeden Authentifizierungstyp aktiviert werden.
2. **Definieren Sie eine Bridge-Gruppe.**In diesem Beispiel wird die Bridge-Group-Nummer **3** verwendet.Router<configure>**#Bridge *3***
3. **Wählen Sie das Spanning Tree Protocol für die Bridge-Gruppe aus.**Das IEEE-Spanning-Tree-Protokoll wird für diese Bridge-Gruppe konfiguriert.Router<configure>**#Bridge *3* Protocol *View***
4. **Aktivieren Sie eine BVI, um routingfähige Pakete zu akzeptieren und weiterzuleiten, die von der entsprechenden Bridge-Gruppe empfangen wurden.**In diesem Beispiel kann die BVI IP-Pakete akzeptieren und weiterleiten.router<configure>**#bridge *3* route *ip***

Konfigurieren der Bridged Virtual Interface (BVI)

Gehen Sie wie folgt vor:

1. **Konfigurieren Sie die BVI.**Konfigurieren Sie die BVI, wenn Sie der BVI die entsprechende

Nummer der Bridge-Gruppe zuweisen. Jede Bridge-Gruppe kann nur über eine BVI des Korrespondenten verfügen. In diesem Beispiel wird der BVI die Bridge-Gruppe Nr. 3 zugewiesen.Router<configure>**#Interface BVI *<2>***

2. **Weisen Sie der BVI eine IP-Adresse zu.**router<config-if>**#ip address *10.3.1.1 255.255.0.0***router<config-if>**#no shutdown**

Konfigurieren der SSID für die WPA-PSK-Authentifizierung

Gehen Sie wie folgt vor:

1. **Aktivieren Sie die Funkschnittstelle.**Um die Funkschnittstelle zu aktivieren, gehen Sie zum Konfigurationsmodus für die DOT11-Funkschnittstelle, und weisen Sie der Schnittstelle eine SSID zu.router<config>**#interface dot11radio0**router<config-if>**#no shutdown**router<config-if>**#ssid *wpa-shared***
2. **Um die Verwaltung des WPA-Schlüssels zu aktivieren, konfigurieren Sie zunächst den WPA-Verschlüsselungscode für die VLAN-Schnittstelle. In diesem Beispiel wird tkip als Verschlüsselungscode verwendet.**.Geben Sie diesen Befehl ein, um den Verwaltungstyp des WPA-Schlüssels für die Funkschnittstelle anzugeben.router<config>**#interface dot11radio0**router(config-if)**#verschlüsselung vlan *3* mode ciphers *tkip***
3. **Binden der SSID an ein VLAN.**Um die SSID auf dieser Schnittstelle zu aktivieren, binden Sie die SSID im SSID-Konfigurationsmodus an das VLAN.Router<config-ssid>**VLAN *3***
4. **Konfigurieren Sie die SSID mit der WPA-PSK-Authentifizierung.Sie müssen zuerst im SSID-Konfigurationsmodus die offene oder Netzwerk-EAP-Authentifizierung konfigurieren, um die Verwaltung des WPA-Schlüssels zu aktivieren. In diesem Beispiel wird die offene Authentifizierung konfiguriert.**router<config>**#interface dot11radio0**router<config-if>**#ssid *wpa-shared***router<config-ssid>**#authentication openAktivieren Sie jetzt das WPA-Schlüsselmanagement auf der SSID. Der Schlüsselverwaltungs-Chip tkip ist für dieses VLAN bereits konfiguriert.**router(config-if-ssid)**#authentication key-management wpaKonfigurieren Sie die WPA-PSK-Authentifizierung auf der SSID.**router(config-if-ssid)**#wpa-psk ascii *1234567890!— 1234567890 ist der Pre-Shared Key-Wert für diese SSID. Stellen Sie sicher, dass derselbe Schlüssel für diese SSID auf Clientseite angegeben ist.***
5. **Aktivieren Sie VLAN auf der Funkschnittstelle.**router<config>**#interface Dot11Radio 0.3**router<config-subif>**#encapsulation dot1Q *3***router<config-subif>**#bridge-group *3***

Konfigurieren des internen DHCP-Servers für die Wireless-Clients dieses VLAN

Geben Sie diese Befehle im globalen Konfigurationsmodus ein, um den internen DHCP-Server für die Wireless-Clients dieses VLAN zu konfigurieren:

- **ip dhcp excluded-address 10.3.1.1 10.3.1.5**
- **ip dhcp pool *wpa-psk***

Geben Sie im DHCP-Pool-Konfigurationsmodus die folgenden Befehle ein:

- **netzwerk *10.3.0.0 255.255.0.0***
- **default-router *10.3.1.1***

WPA-Authentifizierung (mit EAP) konfigurieren

Dies ist ein anderer Verwaltungstyp für einen WPA-Schlüssel. Dabei authentifizieren sich die Clients und der Authentifizierungsserver gegenseitig mit einer EAP-Authentifizierungsmethode, und der Client und der Server generieren einen paarweisen Master Key (PMK). Mit WPA generiert der Server den PMK dynamisch und leitet ihn an den Access Point weiter. Bei WPA-PSK konfigurieren Sie jedoch einen vorinstallierten Schlüssel sowohl auf dem Client als auch auf dem Access Point, und dieser vorinstallierte Schlüssel wird als PMK verwendet.

Weitere Informationen finden Sie unter WPA mit EAP-Authentifizierung .

In diesem Beispiel wird diese Konfigurationseinrichtung verwendet:

- SSID-Name: **wpa-dot1x**
- VLAN 4
- Interner DHCP-Serverbereich: **10.4.0.0/16**

Gehen Sie wie folgt vor:

1. Konfigurieren des Integrated Routing and Bridging (IRB) und Einrichten der Bridge Group
2. Konfigurieren der Bridged Virtual Interface (BVI)
3. Konfigurieren Sie den lokalen RADIUS-Server für die WPA-Authentifizierung.
4. Konfigurieren der SSID für WPA mit EAP-Authentifizierung
5. Konfigurieren des internen DHCP-Servers für die Wireless-Clients dieses VLAN

Konfigurieren des Integrated Routing and Bridging (IRB) und Einrichten der Bridge Group

Gehen Sie wie folgt vor:

1. **Aktivieren Sie IRB im Router.**Router<configure>**#Bridge-IRBHinweis:** Wenn alle Sicherheitstypen auf einem Router konfiguriert werden sollen, reicht es aus, IRB nur einmal global auf dem Router zu aktivieren. Sie muss nicht für jeden Authentifizierungstyp aktiviert werden.
2. **Definieren Sie eine Bridge-Gruppe.**In diesem Beispiel wird die Bridge-Group-Nummer **4** verwendet.Router<configure>**#Bridge *4***
3. **Wählen Sie das Spanning Tree-Protokoll für die Bridge-Gruppe aus.**Hier wird das IEEE-Spanning-Tree-Protokoll für diese Bridge-Gruppe konfiguriert.Router<configure>**#Bridge *4-Protokollansicht***
4. **Aktivieren Sie eine BVI, um die von der entsprechenden Bridge-Gruppe empfangenen routingfähigen Pakete zu akzeptieren und weiterzuleiten.**In diesem Beispiel kann die BVI IP-Pakete akzeptieren und weiterleiten.router<configure>**#bridge *4* route *ip***

Konfigurieren der Bridged Virtual Interface (BVI)

Gehen Sie wie folgt vor:

1. **Konfigurieren Sie die BVI.**Konfigurieren Sie die BVI, wenn Sie der BVI die entsprechende Nummer der Bridge-Gruppe zuweisen. Jede Bridge-Gruppe kann nur eine entsprechende BVI haben. In diesem Beispiel wird der BVI die Bridge-Gruppe Nr. 4 zugewiesen.router<configure>**#interface BVI *<4>***
2. **Weisen Sie der BVI eine IP-Adresse zu.**router<config-if>**#ip address *10.4.1.1***

*255.255.0.0*router<config-if>#**no shutdown**

Konfigurieren des lokalen RADIUS-Servers für die WPA-Authentifizierung

Das ausführliche Verfahren finden Sie im Abschnitt unter 802.1x/EAP Authentication.

Konfigurieren der SSID für WPA mit EAP-Authentifizierung

Gehen Sie wie folgt vor:

1. **Aktivieren Sie die Funkschnittstelle.**Um die Funkschnittstelle zu aktivieren, wechseln Sie zum Konfigurationsmodus für die DOT11-Funkschnittstelle, und weisen Sie der Schnittstelle eine SSID zu.router<config>**#interface dot11radio0**router<config-if>**#no shutdown**router<config-if>**#ssid *wpa-dot1x***
2. **Um die Verwaltung des WPA-Schlüssels zu aktivieren, konfigurieren Sie zunächst den WPA-Verschlüsselungscode für die VLAN-Schnittstelle. In diesem Beispiel wird tkip als Verschlüsselungscode verwendet.**.Geben Sie diesen Befehl ein, um den Verwaltungstyp des WPA-Schlüssels für die Funkschnittstelle anzugeben.router<config>**#interface dot11radio0**router(config-if)**#verschlüsselung vlan *4* mode ciphers *tkip***
3. **Binden der SSID an ein VLAN.**Um die SSID auf dieser Schnittstelle zu aktivieren, binden Sie die SSID im SSID-Konfigurationsmodus an das VLAN.**VLAN *4***
4. **Konfigurieren Sie die SSID mit der WPA-PSK-Authentifizierung.**Um die Funkschnittstelle für WPA mit EAP-Authentifizierung zu konfigurieren, konfigurieren Sie zunächst die zugeordnete SSID für Netzwerk-EAP.router<config>**#interface dot11radio0**router<config-if>**#ssid *wpa-shared***router<config-ssid>**#authentication network eap *eap_methods***
5. **Aktivieren Sie jetzt das WPA-Schlüsselmanagement auf der SSID. Der Schlüsselverwaltungs-Chip tkip ist für dieses VLAN bereits konfiguriert.**router(config-if-ssid)**#authentication key-management wpa**
6. **Aktivieren Sie VLAN auf der Funkschnittstelle.**router<config>**#interface Dot11Radio 0.4**router<config-subif>**#encapsulation dot1Q *4***router<config-subif>**#bridge-group *4***

Konfigurieren des internen DHCP-Servers für die Wireless-Clients dieses VLAN

Geben Sie diese Befehle im globalen Konfigurationsmodus ein, um den internen DHCP-Server für die Wireless-Clients dieses VLAN zu konfigurieren:

- **ip dhcp excluded-address 10.4.1.1 10.4.1.5**
- **ip dhcp pool *wpa-dot1shared***

Geben Sie im DHCP-Pool-Konfigurationsmodus die folgenden Befehle ein:

- **netzwerk *10.4.0.0 255.255.0.0***
- **default-router *10.4.1.1***

Konfigurieren des Wireless-Clients für die Authentifizierung

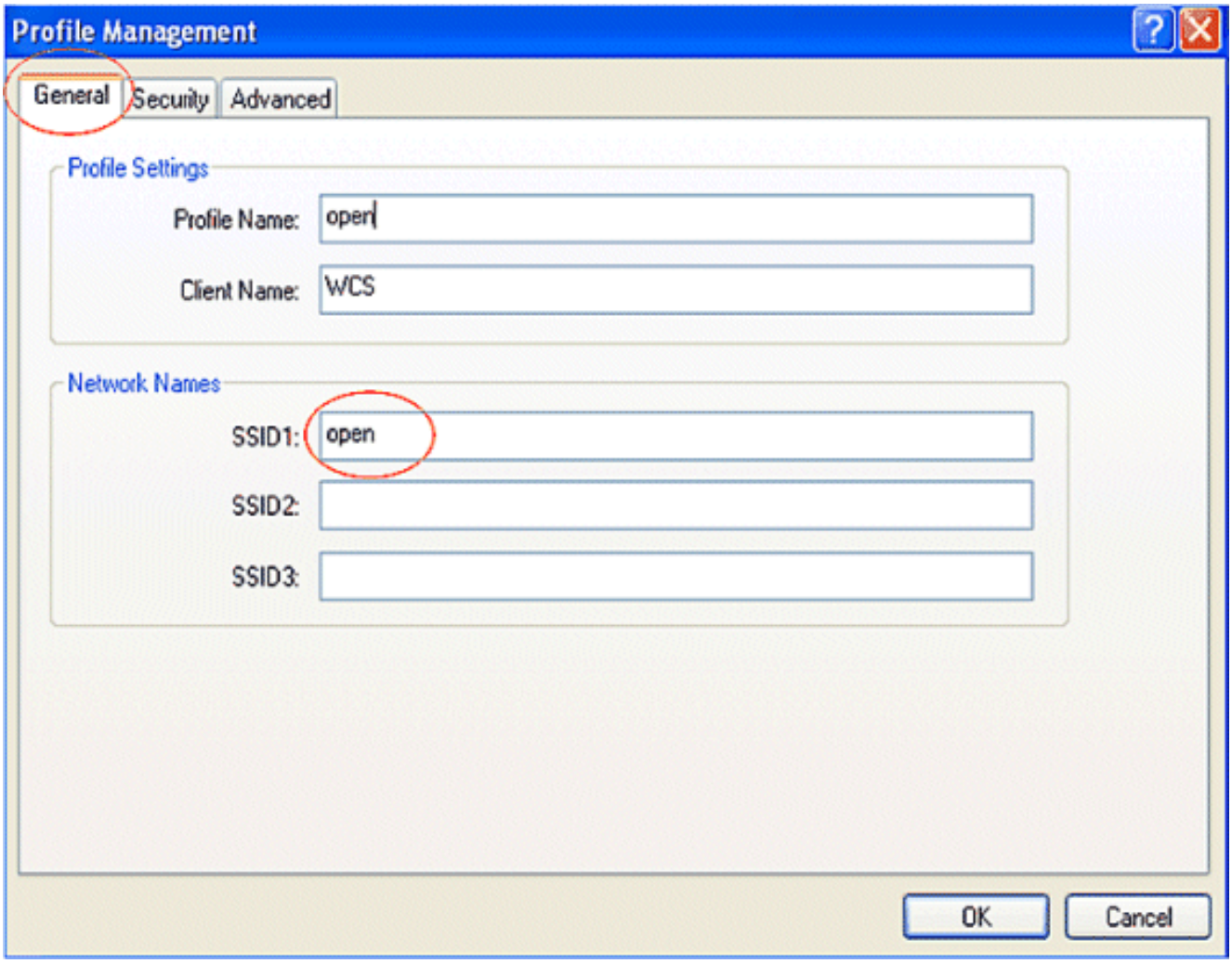
Nachdem Sie den ISR konfiguriert haben, konfigurieren Sie den Wireless-Client für verschiedene Authentifizierungstypen, sodass der Router diese Wireless-Clients authentifizieren und Zugriff auf

das WLAN-Netzwerk gewähren kann. In diesem Dokument wird das Cisco Aironet Desktop Utility (ADU) für die clientseitige Konfiguration verwendet.

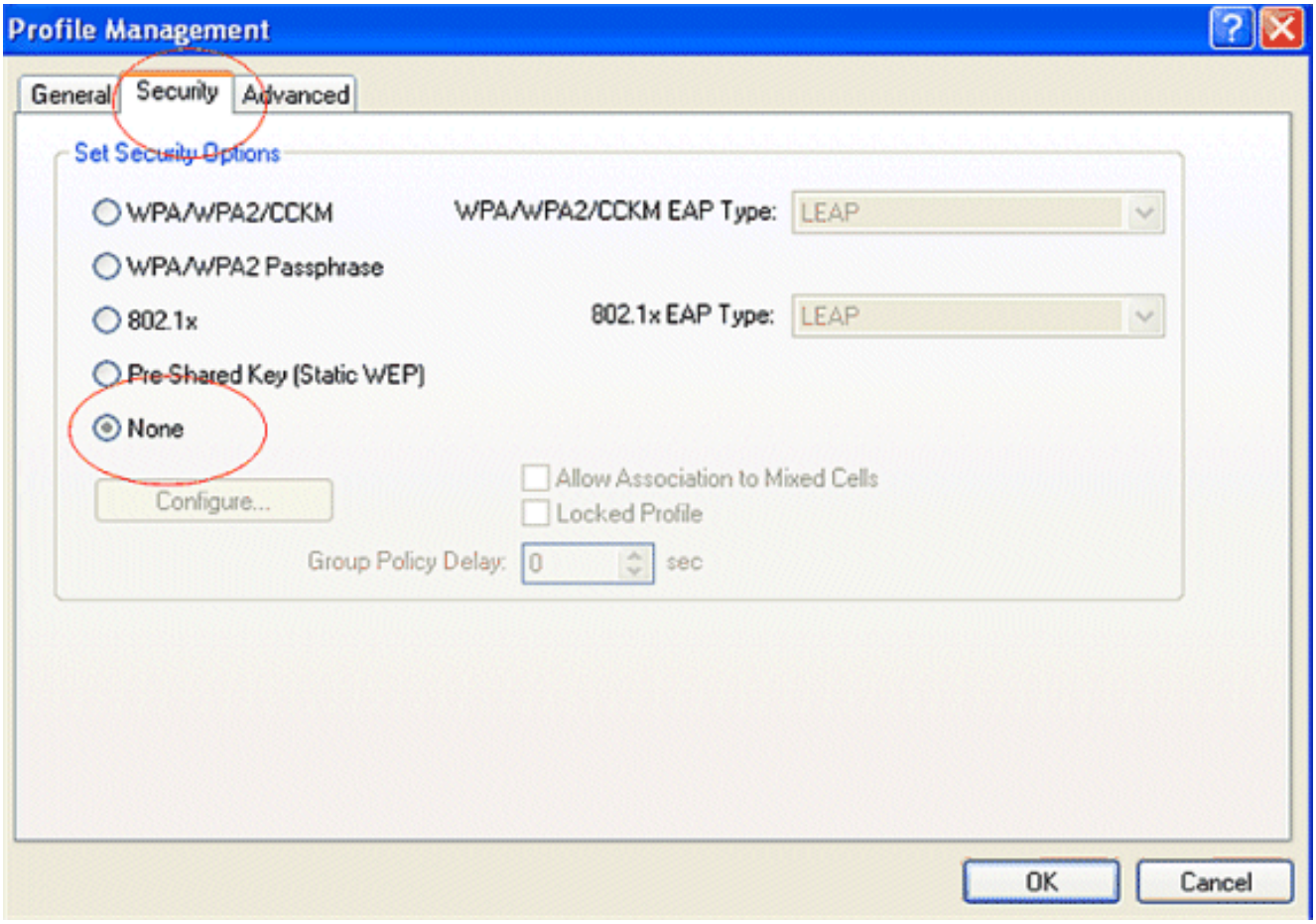
Konfigurieren des Wireless-Clients für die offene Authentifizierung

Führen Sie diese Schritte aus:

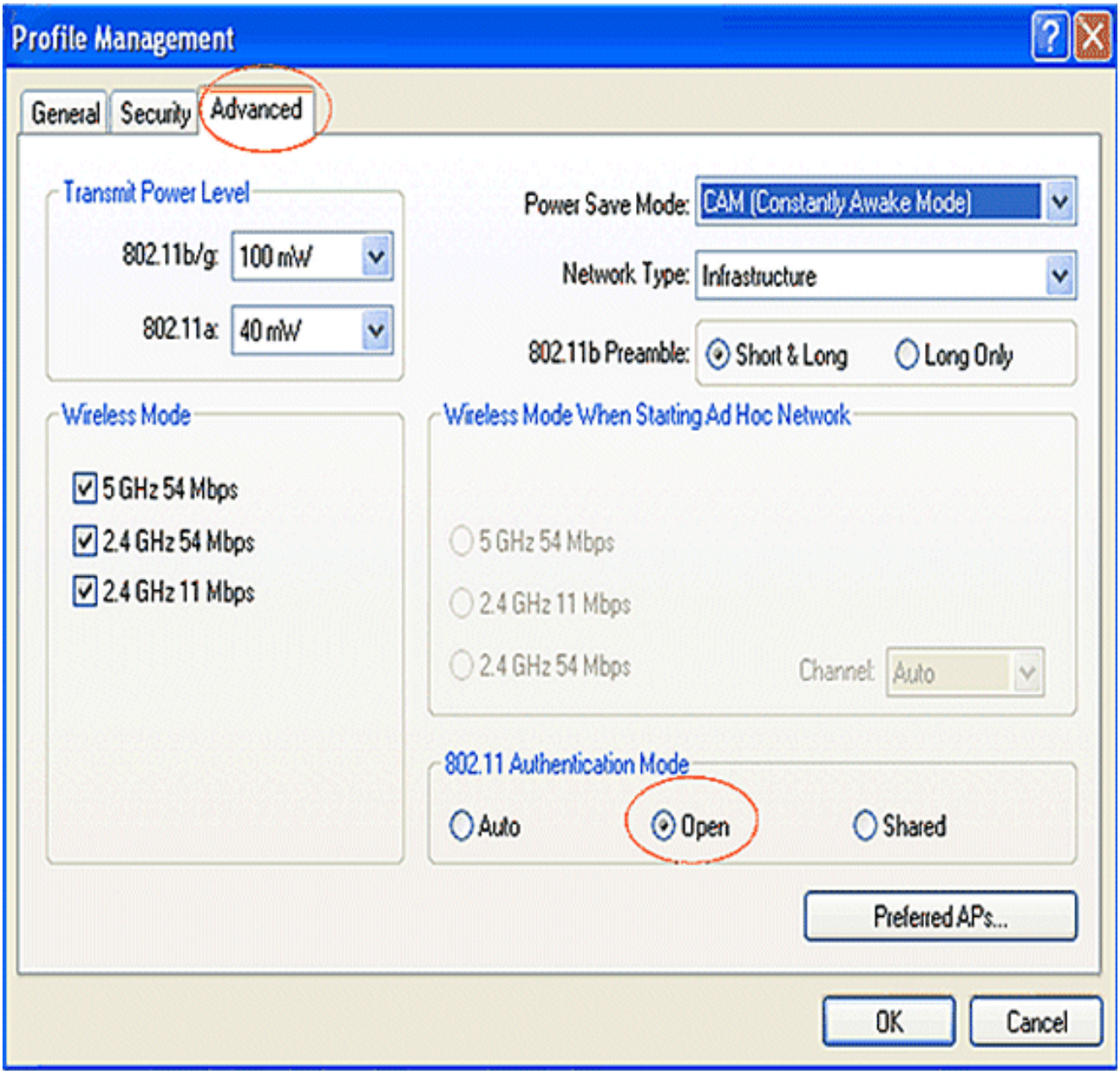
1. Klicken Sie im Fenster Profilverwaltung auf der ADU auf **Neu**, um ein neues Profil zu erstellen.Es wird ein neues Fenster angezeigt, in dem Sie die Konfiguration für die offene Authentifizierung festlegen können. Geben Sie auf der Registerkarte **Allgemein** den Profilnamen und die SSID ein, die der Client-Adapter verwendet.In diesem Beispiel sind der Profilname und die SSID **offen**.**Hinweis:** Der SSID muss mit der SSID übereinstimmen, die Sie für die offene Authentifizierung auf dem ISR konfiguriert haben.



2. Klicken Sie auf die Registerkarte **Sicherheit**, und belassen Sie die Sicherheitsoption als **Keine** für WEP-Verschlüsselung. Da in diesem Beispiel WEP als optional verwendet wird, ermöglicht es das Festlegen dieser Option auf None dem Client, erfolgreich eine Verbindung zum WLAN-Netzwerk herzustellen und mit diesem zu kommunizieren.Klicken Sie auf **OK**

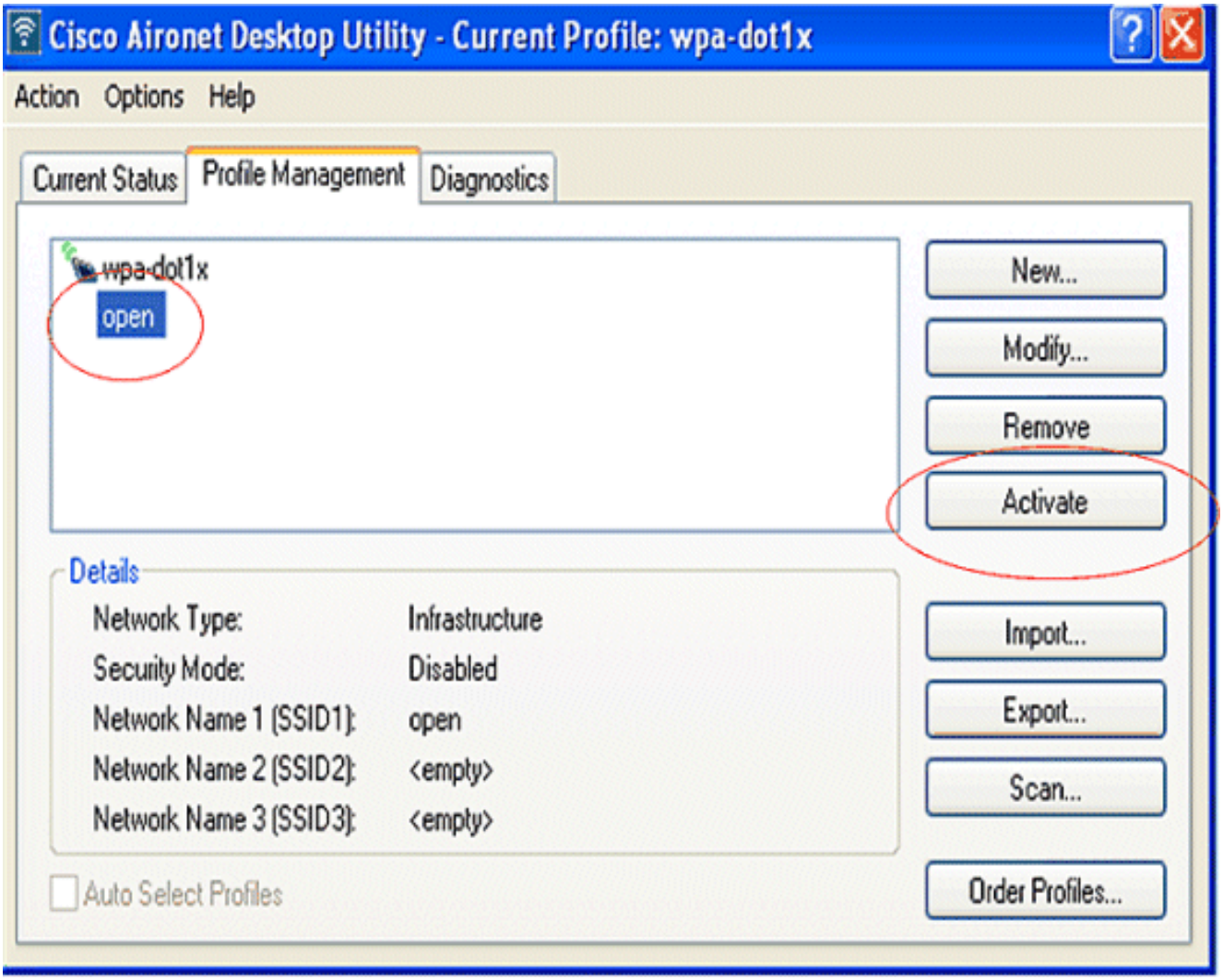


3. Wählen Sie **auf** der Registerkarte **Profilverwaltung** das **Fenster Erweitert aus**, und legen Sie den 802.11-Authentifizierungsmodus für die offene Authentifizierung als **offen** fest.

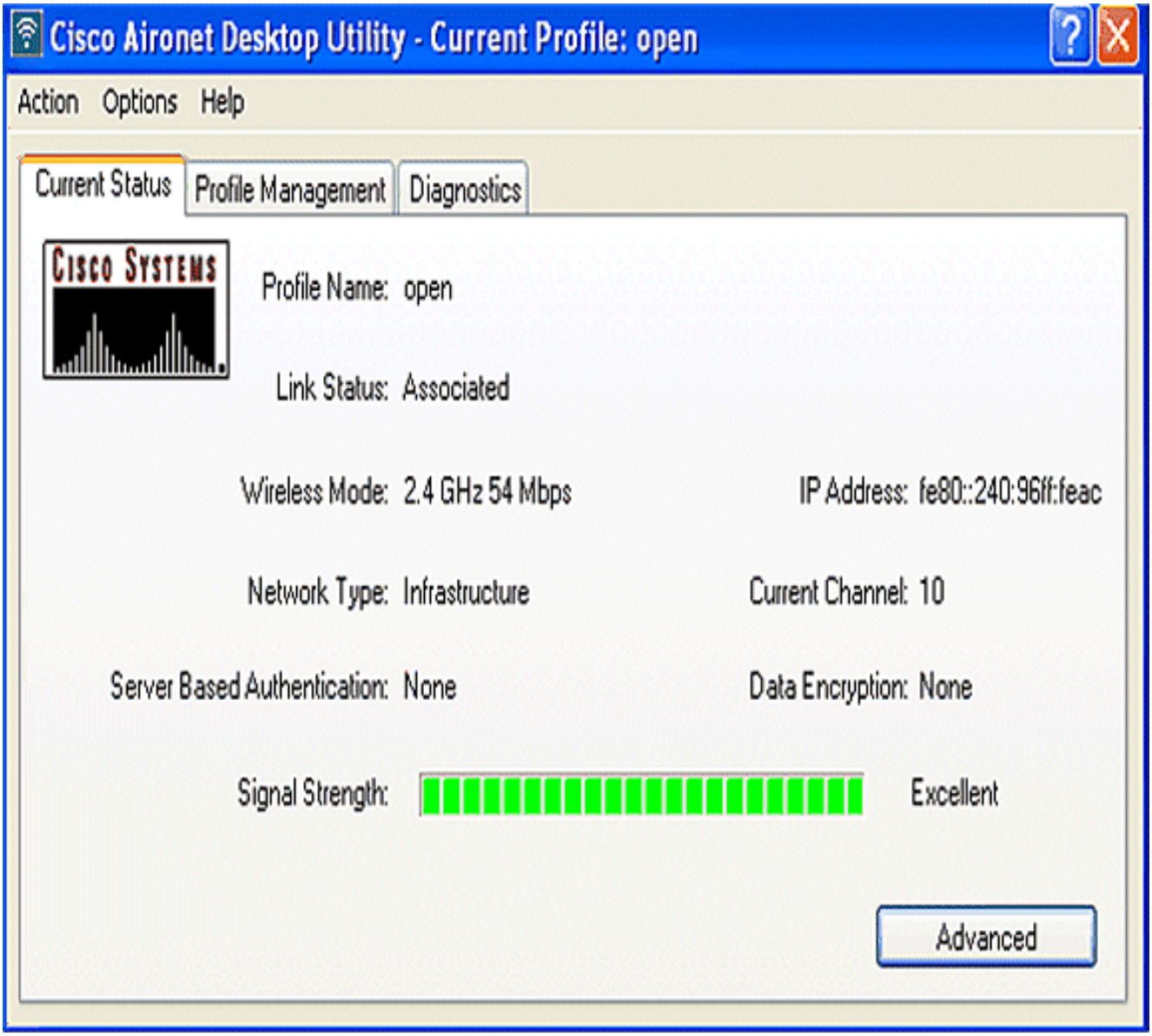


In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

1. Nachdem das Clientprofil erstellt wurde, klicken Sie unter der Registerkarte "Profilverwaltung" auf **Aktivieren**, um das Profil zu aktivieren.



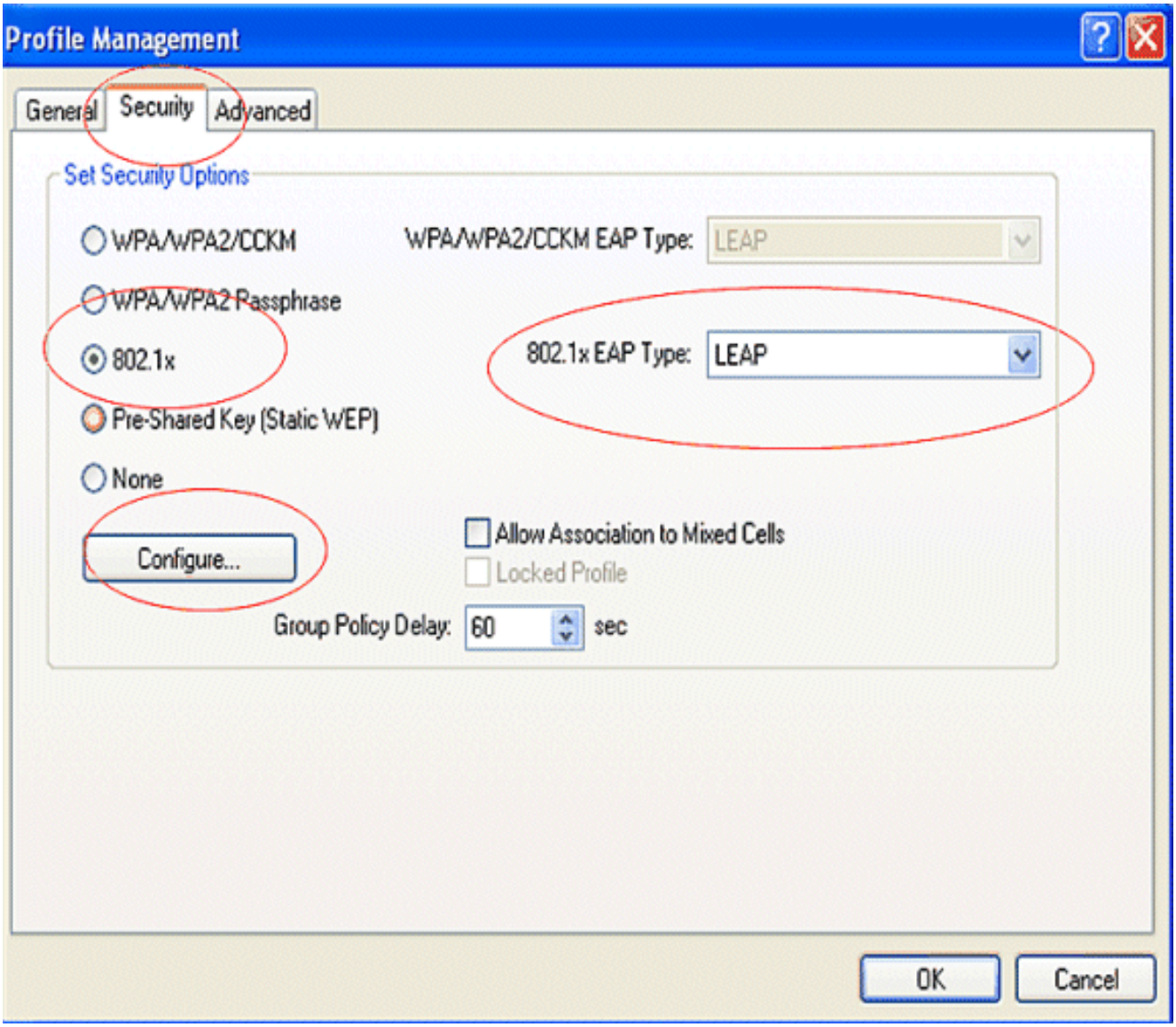
2. Überprüfen Sie den ADU-Status auf eine erfolgreiche Authentifizierung.



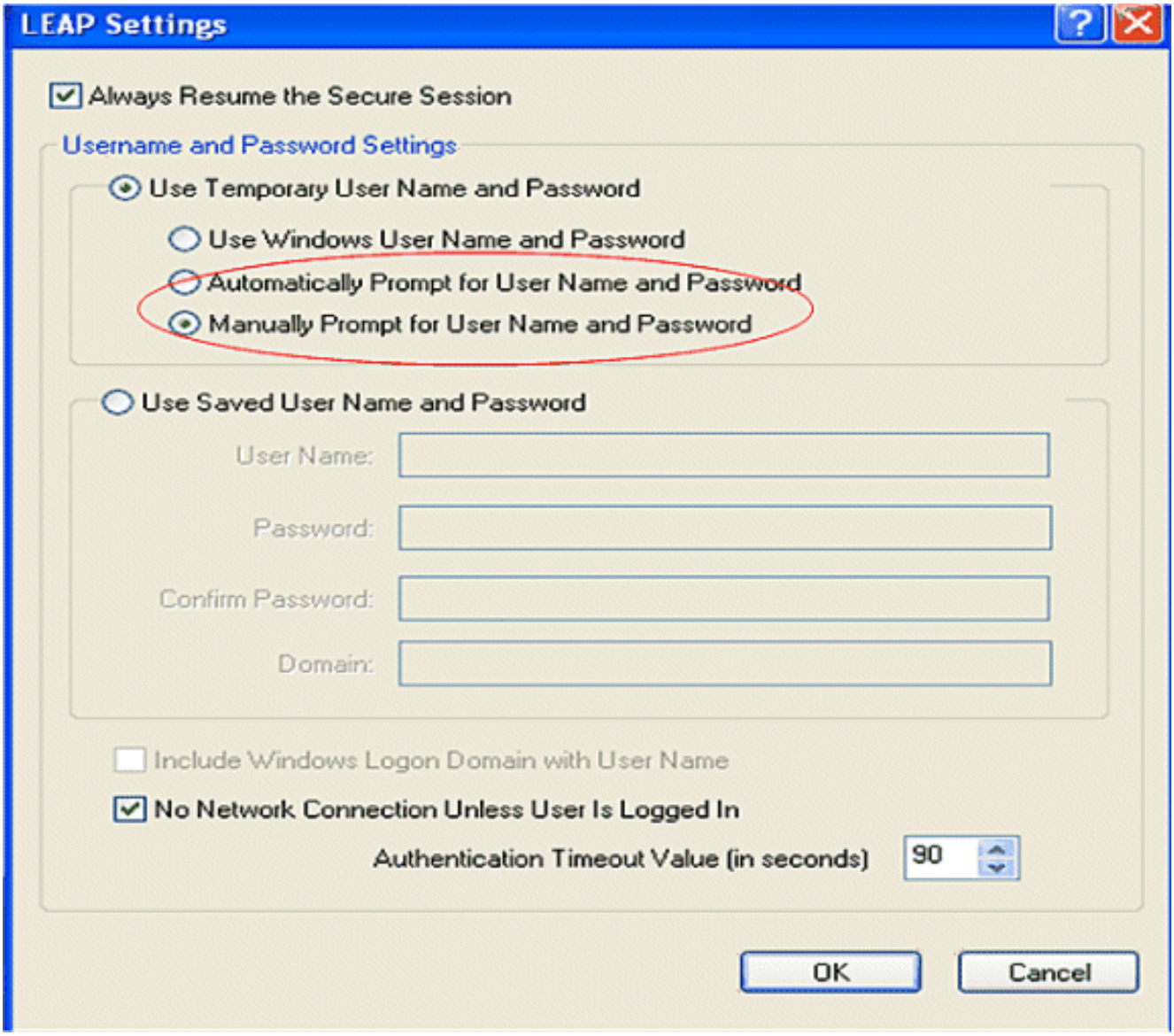
Konfigurieren des Wireless-Clients für die 802.1x/EAP-Authentifizierung

Führen Sie diese Schritte aus:

1. Klicken Sie im Fenster Profilverwaltung auf der ADU auf **Neu**, um ein neues Profil zu erstellen.Es wird ein neues Fenster angezeigt, in dem Sie die Konfiguration für die offene Authentifizierung festlegen können. Geben Sie auf der Registerkarte **Allgemein** den Profilnamen und die SSID ein, die der Client-Adapter verwendet.In diesem Beispiel sind der Profilname und die SSID ein **Sprung**.
2. Klicken Sie unter **Profilverwaltung** auf die Registerkarte **Sicherheit**, legen Sie die Sicherheitsoption als 802.1x fest, und wählen Sie den entsprechenden EAP-Typ aus. In diesem Dokument wird LEAP als EAP-Typ für die Authentifizierung verwendet. Klicken Sie jetzt auf **Konfigurieren**, um die LEAP-Einstellungen für Benutzername und Kennwort zu konfigurieren.**Hinweis:** Hinweis: Die SSID muss mit der SSID übereinstimmen, die Sie auf dem ISR für die 802.1x-/EAP-Authentifizierung konfiguriert haben.

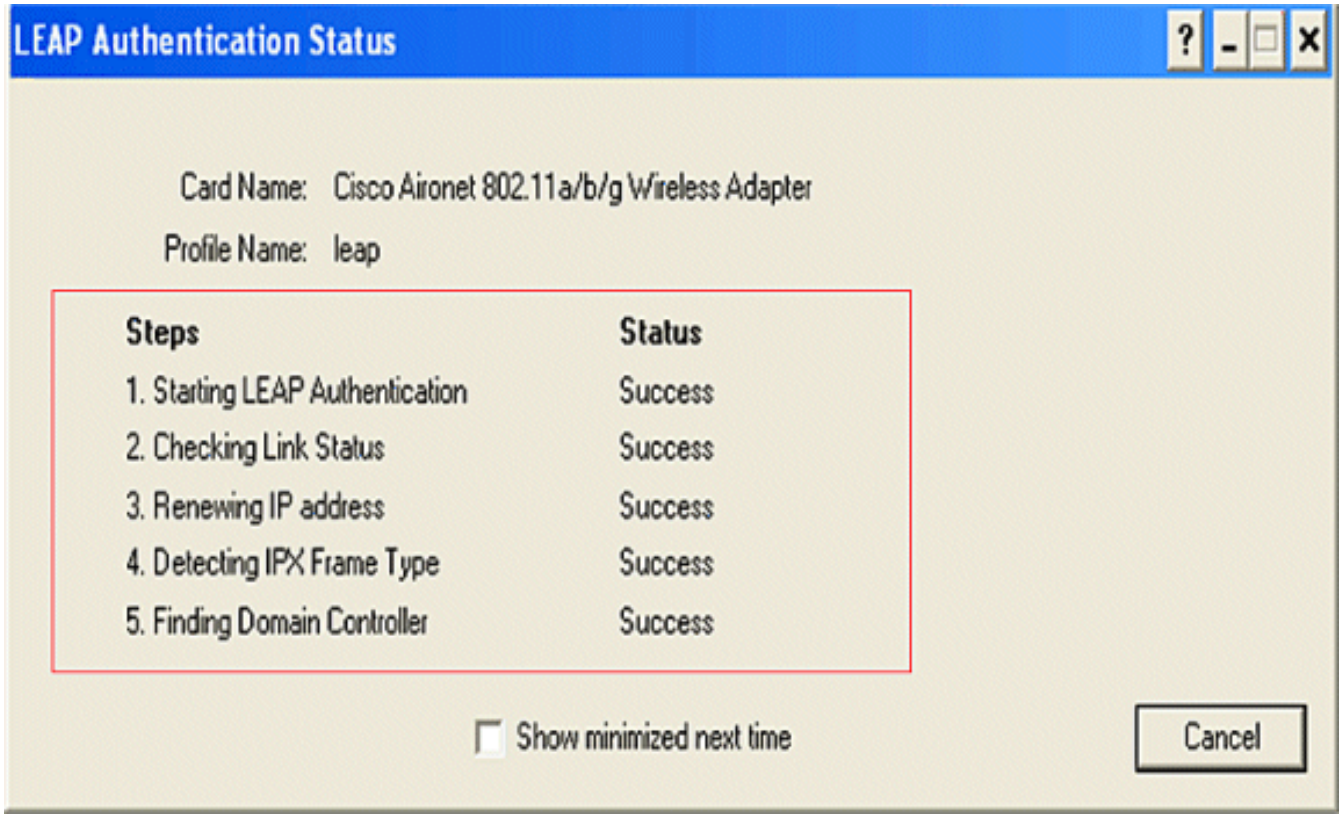


3. Unter den Einstellungen für Benutzername und Kennwort wird in diesem Beispiel die Option **Manuelle Aufforderung zur Eingabe von Benutzername und Kennwort** ausgewählt, sodass der Client aufgefordert wird, den korrekten Benutzernamen und das richtige Kennwort einzugeben, während der Client versucht, eine Verbindung zum Netzwerk herzustellen. Klicken Sie auf
OK.



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

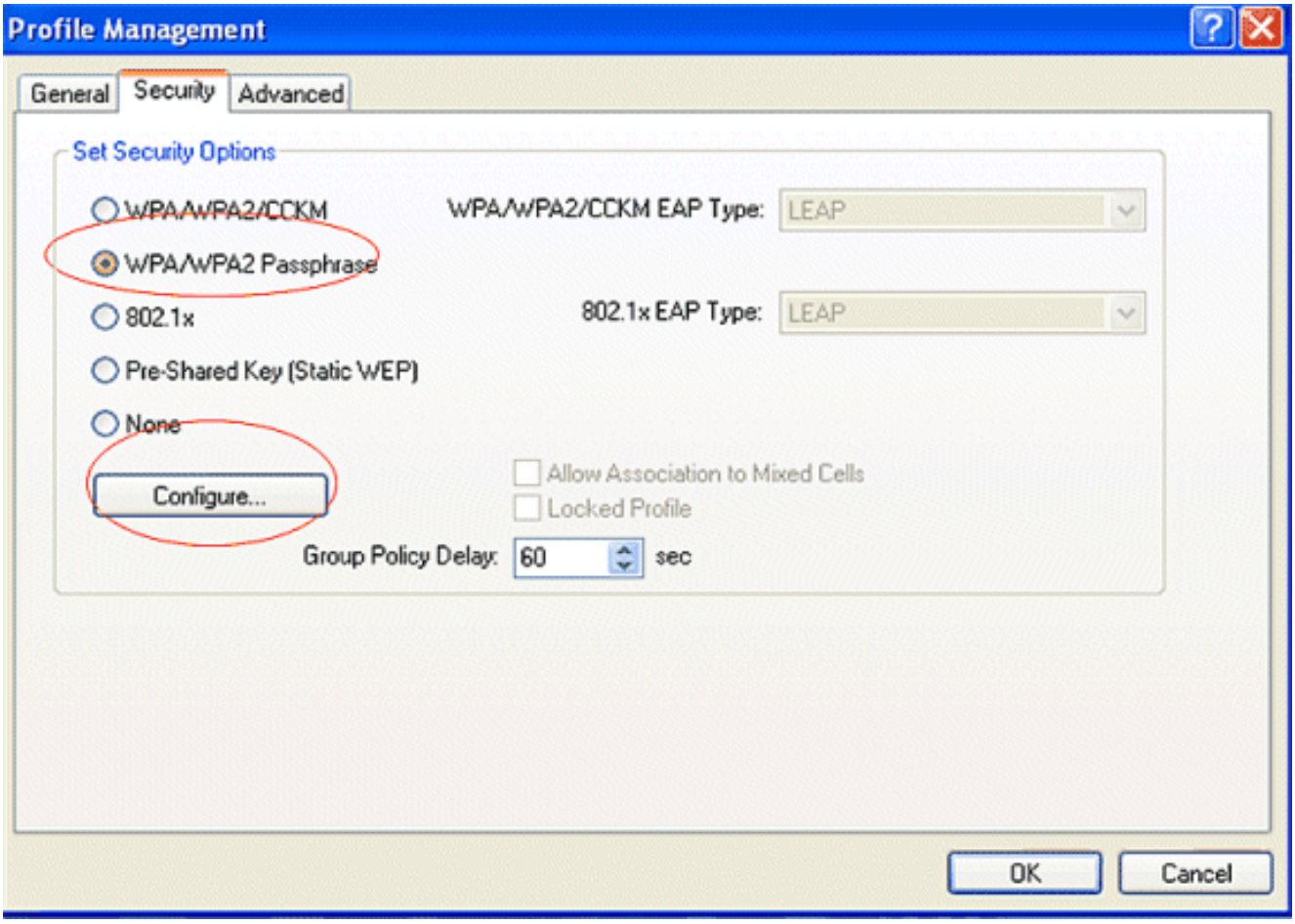
- Nachdem das Clientprofil erstellt wurde, klicken Sie auf der Registerkarte **Profilverwaltung** auf **Aktivieren**, um den Profilsprung **zu** aktivieren. Sie werden aufgefordert, den Benutzernamen und das Kennwort für den **Sprung einzugeben**. In diesem Beispiel werden der Benutzername und das Kennwort **user1** verwendet. Klicken Sie auf **OK**.
- Sie können die erfolgreiche Authentifizierung des Clients beobachten und eine IP-Adresse vom DHCP-Server erhalten, der auf dem Router konfiguriert
  wurde.



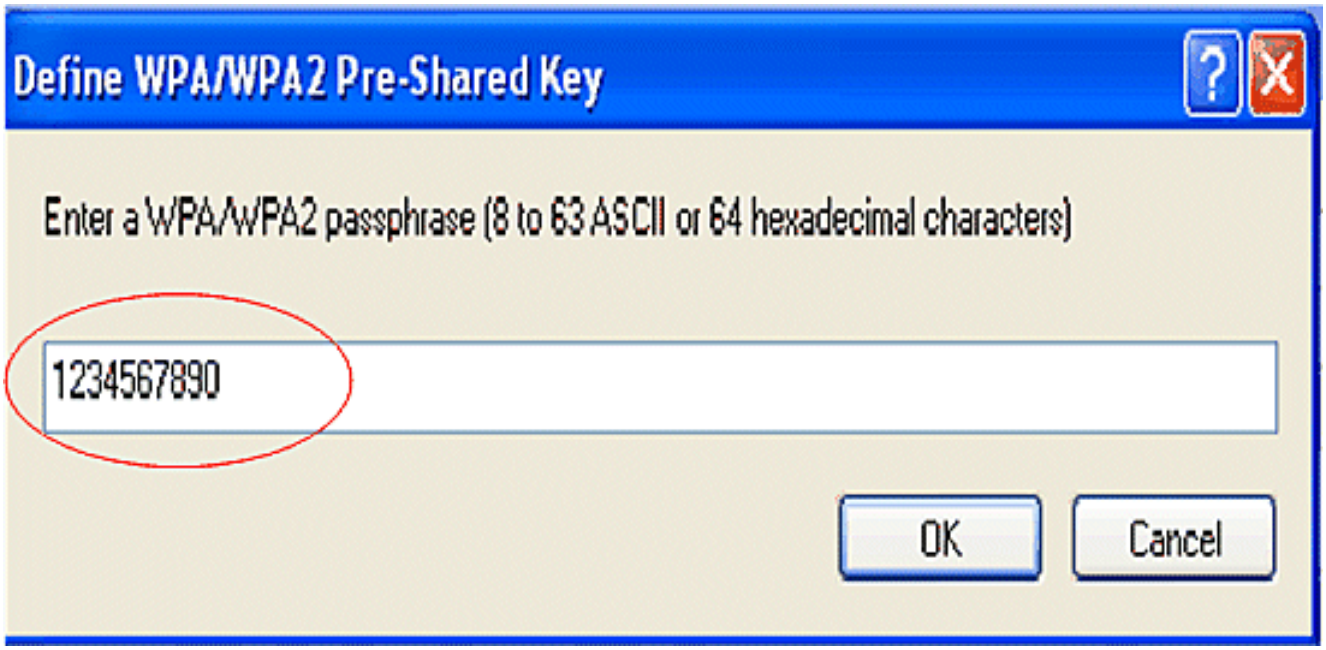
Konfigurieren des Wireless-Clients für die WPA-PSK-Authentifizierung

Führen Sie diese Schritte aus:

1. Klicken Sie im Fenster Profilverwaltung auf der ADU auf **Neu**, um ein neues Profil zu erstellen.Es wird ein neues Fenster angezeigt, in dem Sie die Konfiguration für die offene Authentifizierung festlegen können. Geben Sie auf der Registerkarte **Allgemein** den **Profilnamen** und die **SSID ein**, die der Client-Adapter verwendet.In diesem Beispiel sind der Profilname und die SSID **wpa-shared**.**Hinweis:** Die SSID muss mit der SSID übereinstimmen, die Sie auf dem ISR für die WPA-PSK-Authentifizierung konfiguriert haben.
2. Klicken Sie unter **Profilverwaltung** auf die Registerkarte **Sicherheit**, und legen Sie die Sicherheitsoption als **WPA/WPA2-Passphrase fest**. Klicken Sie jetzt auf **Konfigurieren**, um die WPA-Passphrase zu
konfigurieren.

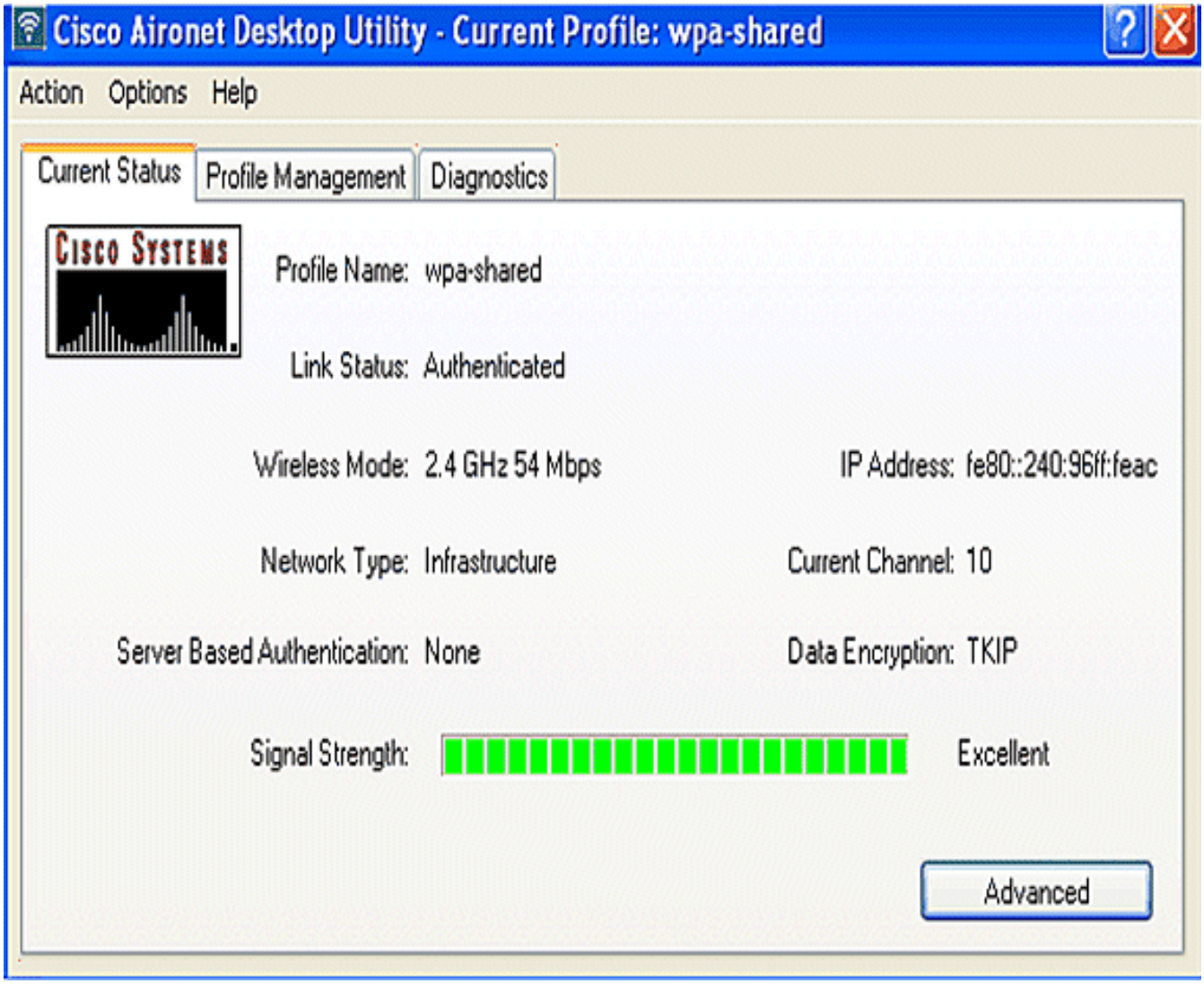


3. Definieren eines WPA Pre-Shared Key. Der Schlüssel muss 8 bis 63 ASCII-Zeichen lang sein. Klicken Sie auf **OK**.



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

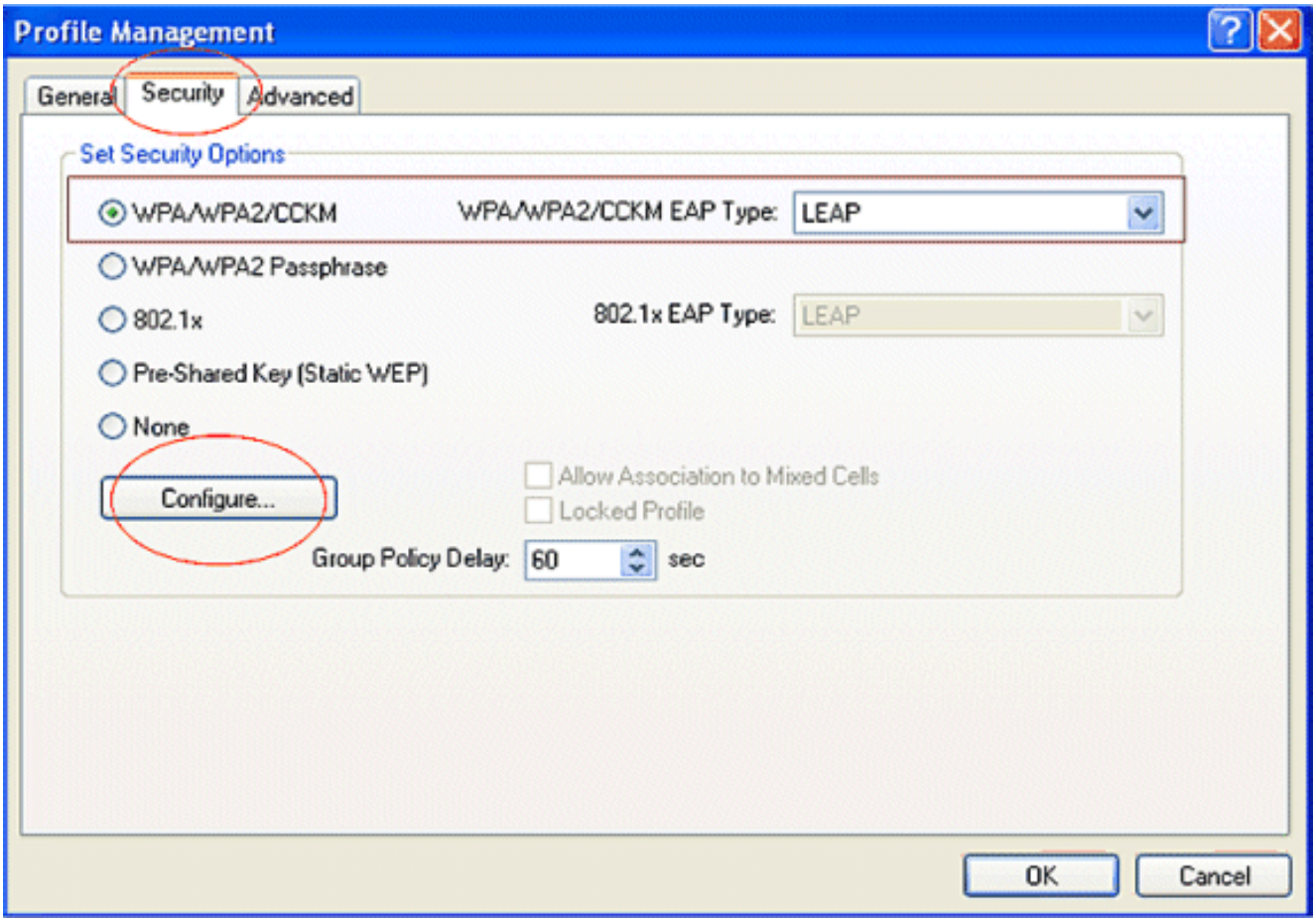
- Nachdem das Clientprofil erstellt wurde, klicken Sie auf der Registerkarte **Profilverwaltung** auf **Aktivieren**, um das Profil **wpa-shared** zu aktivieren.
- Überprüfen Sie die ADU auf eine erfolgreiche Authentifizierung.



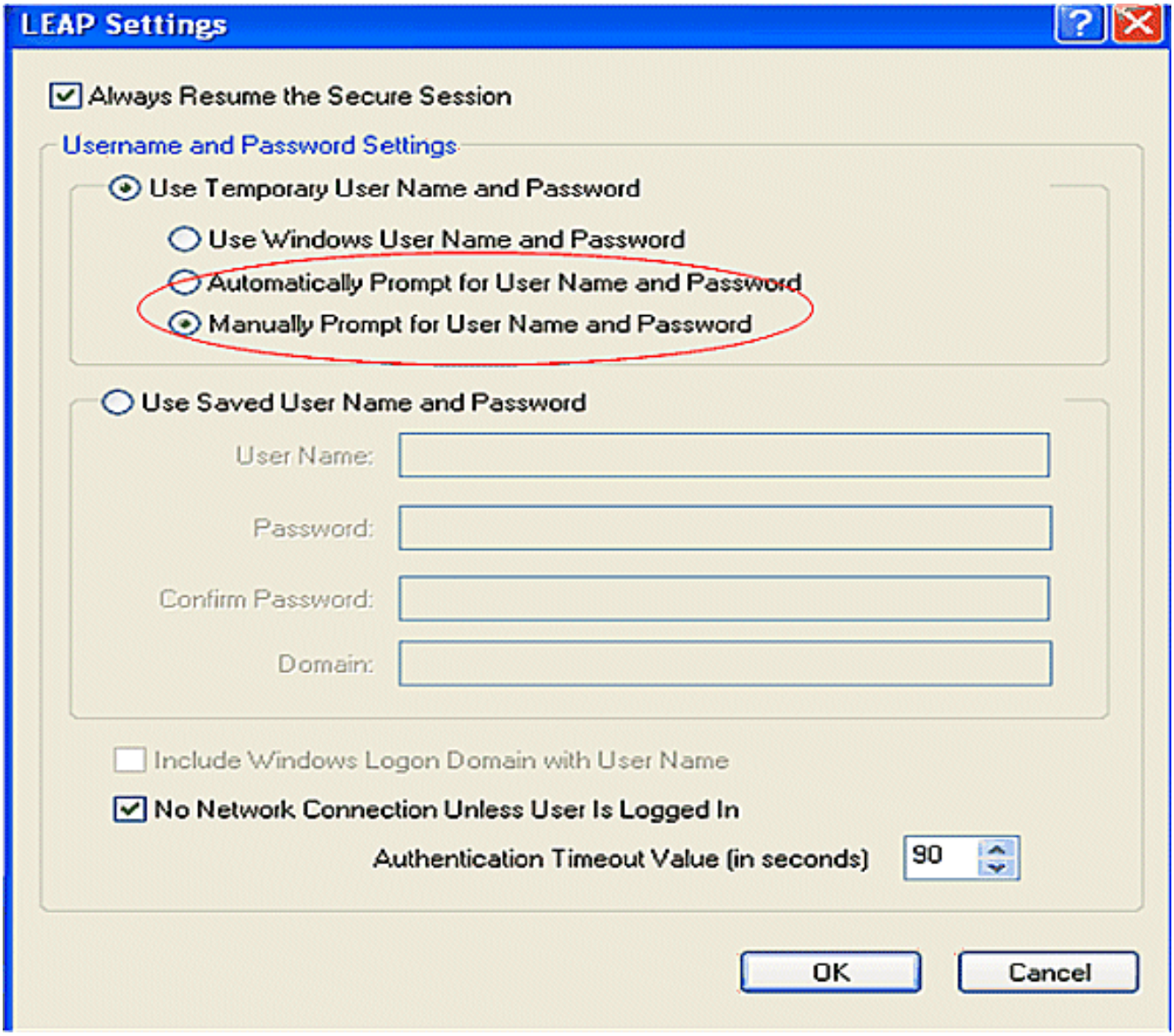
Konfigurieren des Wireless-Clients für die WPA-Authentifizierung (mit EAP)

Führen Sie diese Schritte aus:

1. Klicken Sie im Fenster Profilverwaltung auf der ADU auf **Neu**, um ein neues Profil zu erstellen.Es wird ein neues Fenster angezeigt, in dem Sie die Konfiguration für die offene Authentifizierung festlegen können. Geben Sie auf der Registerkarte **Allgemein** den Profilnamen und die SSID ein, die der Client-Adapter verwendet.In diesem Beispiel sind der Profilname und die SSID **wpa-dot1x**.**Hinweis:** Die SSID muss mit der SSID übereinstimmen, die Sie auf dem ISR für die WPA-Authentifizierung (mit EAP) konfiguriert haben.
2. Klicken Sie unter **Profilverwaltung** auf die Registerkarte **Security** (Sicherheit), legen Sie die Sicherheitsoption als **WPA/WPA2/CCKM fest**, und wählen Sie den entsprechenden WPA/WPA2/CCKM-EAP-Typ aus. In diesem Dokument wird LEAP als EAP-Typ für die Authentifizierung verwendet. Klicken Sie jetzt auf **Konfigurieren**, um die LEAP-Einstellungen für Benutzername und Kennwort zu konfigurieren.

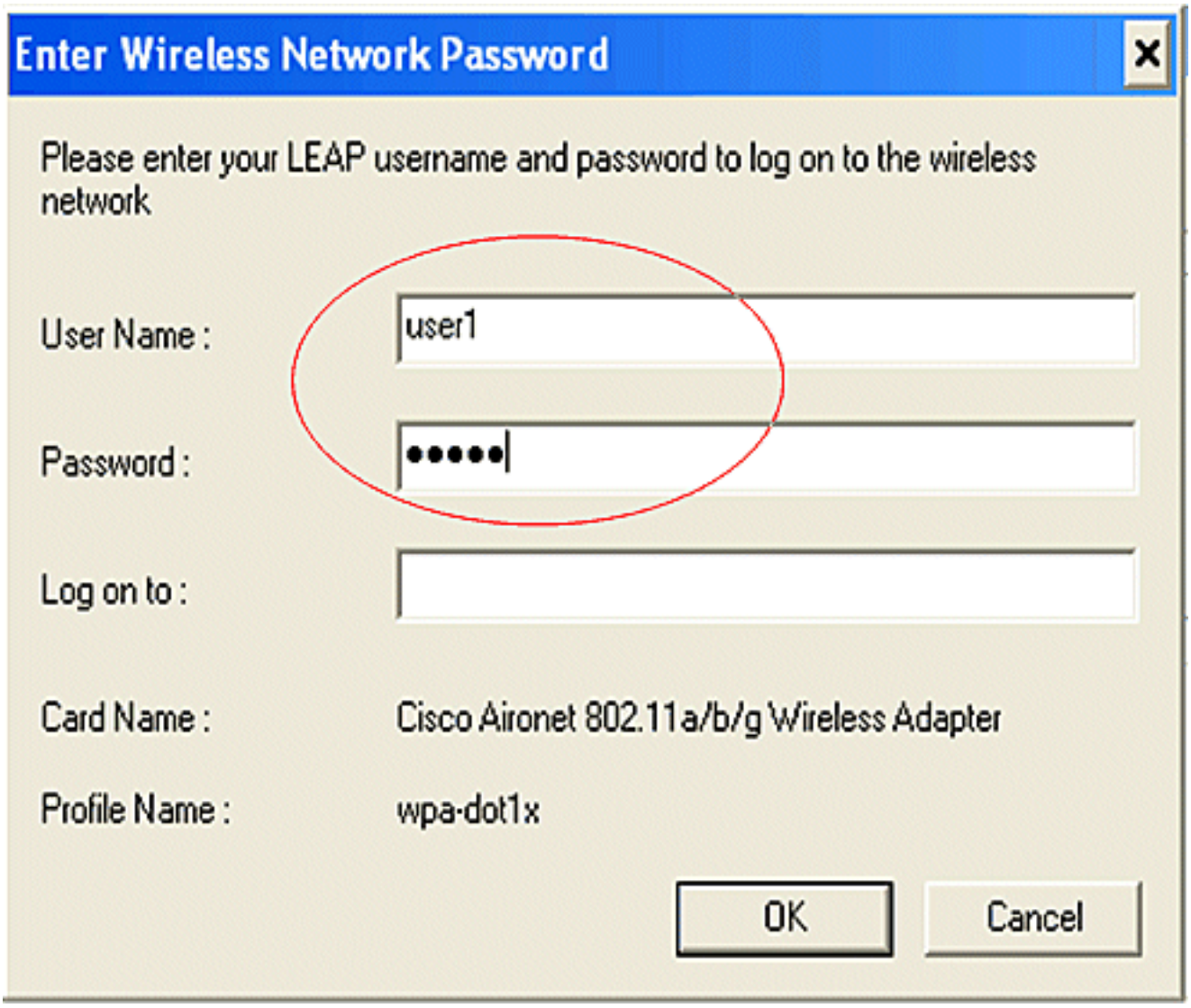


3. Im Bereich "Username and Password Settings" (Einstellungen für Benutzername und Kennwort) wird in diesem Beispiel die **manuelle Aufforderung zur Eingabe von Benutzername und Kennwort** ausgewählt, sodass der Client aufgefordert wird, den korrekten Benutzernamen und das richtige Kennwort einzugeben, während der Client versucht, eine Verbindung zum Netzwerk herzustellen. Klicken Sie auf **OK**.

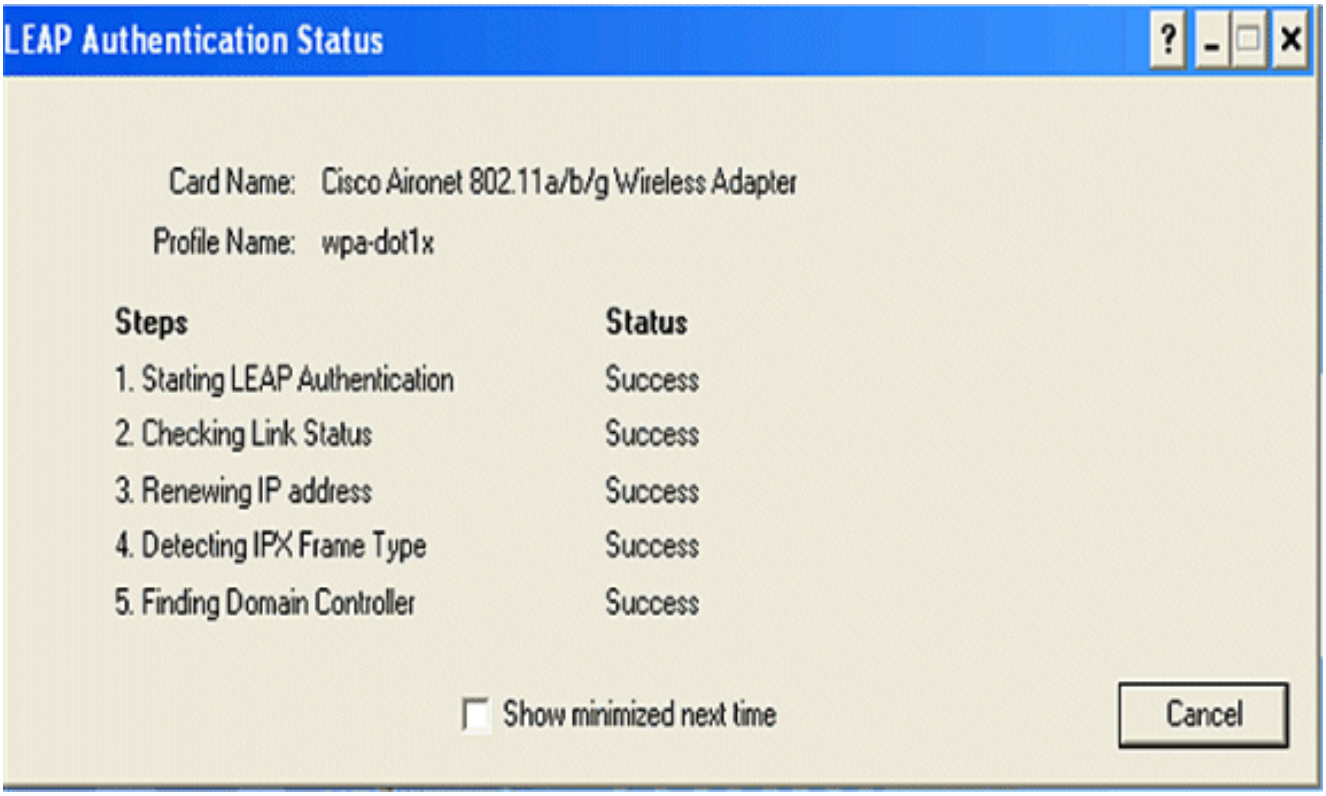


In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

1. Nachdem das Clientprofil erstellt wurde, klicken Sie auf der Registerkarte "Profilverwaltung" auf **Aktivieren**, um das Profil **wpa-dot1x** zu aktivieren. Sie werden zur Eingabe des LEAP-Benutzernamens und -Kennworts aufgefordert. In diesem Beispiel werden Benutzername und Kennwort als **user1** verwendet. Klicken Sie auf **OK**.



2. Sie können beobachten, wie der Client sich erfolgreich authentifiziert.



Der Befehl **show dot1 associated** (**dot1-Zuordnungen anzeigen**) in der Router-CLI zeigt

vollständige Details zum Client-Zuordnungsstatus an. Hier ein Beispiel.

Router**#show dot1-Zuordnungen**

```
802.11 Client Stations on Dot11Radio0:

SSID [leap] :

MAC Address    IP address      Device        Name            Parent         State
0040.96ac.e657 10.3.0.2        CB21AG/PI21AG WCS             self         EAP-Assoc

SSID [open] :

SSID [pre-shared] : DISABLED, not associated with a configured VLAN

SSID [wpa-dot1x] :

SSID [wpa-shared] :


Others:  (not related to any ssid)
```

Fehlerbehebung

Befehle zur Fehlerbehebung

Sie können diese Debugbefehle verwenden, um Konfigurationsfehler zu beheben.

- **debug dot11 aaa authentication all** - Aktiviert das Debuggen von MAC- und EAP-Authentifizierungspaketen.
- **debug radius authentication**: Zeigt die RADIUS-Verhandlungen zwischen Server und Client an.
- **debug radius local-server pakets**: Zeigt den Inhalt der gesendeten und empfangenen RADIUS-Pakete an.
- **debug radius local-server client**: Zeigt Fehlermeldungen über fehlgeschlagene Client-Authentifizierungen an.

Zugehörige Informationen

- Konfigurationsbeispiele für die Authentifizierung auf Wireless LAN-Controllern
- Konfigurieren von VLANs auf Access Points
- Konfigurationsbeispiel für 1800 ISR Wireless-Router mit internem DHCP und offener Authentifizierung
- Konfigurationsleitfaden für Cisco Wireless ISR und HWIC Access Points
- Konfigurationsbeispiel für Wireless LAN-Verbindungen mit einem ISR mit WEP Encryption und LEAP Authentication
- Technischer Support und Dokumentation für Cisco Systeme
- Konfigurieren von Authentifizierungstypen
- Konfigurationsbeispiel für Wireless LAN-Verbindungen mit einem ISR mit WEP-Verschlüsselung und LEAP-Authentifizierung