

Konfigurationsbeispiel für Wi-Fi Protected Access 2 (WPA 2)

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[WPA 2-Unterstützung für Cisco Aironet-Geräte](#)

[Konfiguration im Enterprise-Modus](#)

[Netzwerkeinrichtung](#)

[Konfigurieren des Access Points](#)

[CLI-Konfiguration](#)

[Konfigurieren des Client-Adapters](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Konfigurieren im persönlichen Modus](#)

[Netzwerkeinrichtung](#)

[Konfigurieren des Access Points](#)

[Konfigurieren des Client-Adapters](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument werden die Vorteile der Verwendung von Wi-Fi Protected Access 2 (WPA 2) in einem WLAN erläutert. Das Dokument enthält zwei Konfigurationsbeispiele zur Implementierung von WPA 2 in einem WLAN. Im ersten Beispiel wird die Konfiguration von WPA 2 im Enterprise-Modus und im zweiten Beispiel die Konfiguration von WPA 2 im Personal-Modus veranschaulicht.

Hinweis: WPA arbeitet mit Extensible Authentication Protocol (EAP) zusammen.

Voraussetzungen

Anforderungen

Vergewissern Sie sich, dass Sie vor dem Versuch dieser Konfiguration über grundlegende Kenntnisse dieser Themen verfügen:

- WPA
- WLAN-Sicherheitslösungen **Hinweis:** Informationen zu Cisco WLAN-Sicherheitslösungen finden Sie unter [Übersicht über die Cisco Aironet Wireless LAN-Sicherheit](#).

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Aironet 1310G Access Point (AP)/Bridge mit Cisco IOS® Software Release 12.3(2)JA
- Aironet 802.11a/b/g CB21AG Client-Adapter, der Firmware 2.5 ausführt
- Aironet Desktop Utility (ADU), das Firmware 2.5 ausführt

Hinweis: Die Client-Adaptersoftware Aironet CB21AG und PI21AG ist nicht mit anderen Aironet Client-Adaptersoftware kompatibel. Sie müssen die ADU mit CB21AG- und PI21AG-Karten verwenden und das Aironet Client Utility (ACU) für alle anderen Aironet Client-Adapter verwenden. Weitere Informationen zur Installation der CB21AG-Karte und der ADU finden Sie unter [Installieren des Client-Adapters](#).

Hinweis: Dieses Dokument verwendet einen Access Point/Bridge mit integrierter Antenne. Wenn Sie einen AP/Bridge verwenden, für den eine externe Antenne erforderlich ist, stellen Sie sicher, dass die Antennen mit dem Access Point/Bridge verbunden sind. Andernfalls kann der Access Point bzw. die Bridge keine Verbindung zum Wireless-Netzwerk herstellen. Bestimmte AP/Bridge-Modelle sind mit integrierten Antennen ausgestattet, während andere eine externe Antenne für den allgemeinen Betrieb benötigen. Informationen zu AP-/Bridge-Modellen, die mit internen oder externen Antennen ausgeliefert werden, finden Sie in der Bestellanleitung bzw. im Produkthandbuch des entsprechenden Geräts.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

WPA ist eine standardbasierte Sicherheitslösung der Wi-Fi Alliance, die die Schwachstellen in nativen WLANs behebt. WPA bietet verbesserten Datenschutz und erweiterte Zugriffskontrolle für WLAN-Systeme. WPA behebt alle bekannten Wired Equivalent Privacy (WEP)-Schwachstellen in der ursprünglichen IEEE 802.11-Sicherheitsimplementierung und bietet WLANs in Enterprise- und Small Office-, Home Office (SOHO)-Umgebungen eine sofortige Sicherheitslösung.

WPA 2 ist die nächste Generation der Wi-Fi-Sicherheit. WPA 2 ist die von der Wi-Fi Alliance kompatible Implementierung des ratifizierten IEEE 802.11i-Standards. WPA 2 implementiert den

vom National Institute of Standards and Technology (NIST) empfohlenen AES-Verschlüsselungsalgorithmus (Advanced Encryption Standard) unter Verwendung des Counter-Modus mit dem Cipher Block Chaining Message Authentication Code Protocol (CCMP). AES Counter Mode ist eine Blockchiffre, die 128-Bit-Datenblöcke gleichzeitig mit einem 128-Bit-Verschlüsselungsschlüssel verschlüsselt. Der CCMP-Algorithmus erstellt einen Nachrichtenintegritätscode (Message Integrity Code, MIC), der Datenursprungsauthentifizierung und Datenintegrität für den Wireless-Frame bietet.

Hinweis: CCMP wird auch als CBC-MAC bezeichnet.

WPA 2 bietet eine höhere Sicherheitsstufe als WPA, da AES eine stärkere Verschlüsselung als das Temporal Key Integrity Protocol (TKIP) bietet. TKIP ist der von WPA verwendete Verschlüsselungsalgorithmus. WPA 2 erstellt bei jeder Zuordnung neue Sitzungsschlüssel. Die Verschlüsselungsschlüssel, die für jeden Client im Netzwerk verwendet werden, sind eindeutig und spezifisch für diesen Client. Letztlich wird jedes Paket, das über die Luft gesendet wird, mit einem eindeutigen Schlüssel verschlüsselt. Die Sicherheit wird durch die Verwendung eines neuen und eindeutigen Verschlüsselungsschlüssels verbessert, da keine Schlüsselwiederverwendung möglich ist. WPA gilt weiterhin als sicher, und TKIP wurde nicht beschädigt. Cisco empfiehlt Kunden jedoch, so bald wie möglich auf WPA 2 umzusteigen.

WPA und WPA 2 unterstützen beide zwei Betriebsmodi:

- Enterprise-Modus
- Persönlicher Modus

In diesem Dokument wird die Implementierung dieser beiden Modi mit WPA 2 erläutert.

[WPA 2-Unterstützung für Cisco Aironet-Geräte](#)

WPA 2 wird auf diesem Gerät unterstützt:

- Aironet AP-Serie 1130AG und AP-Serie 1230AG
- Aironet AP der Serie 1100
- Aironet AP der Serie 1200
- Aironet AP der Serie 1300

Hinweis: Konfigurieren Sie diese APs mit 802.11g-Funkmodulen, und verwenden Sie die Cisco IOS Software Release 12.3(2)JA oder höher.

WPA 2 und AES werden ebenfalls unterstützt auf:

- Aironet-Funkmodule der Serie 1200 mit den Teilenummern AIR-RM21A und AIR-RM22A **Hinweis:** Das Funkmodul Aironet 1200 mit der Teilenummer AIR-RM20A unterstützt WPA 2 nicht.
- Aironet 802.11a/b/g Client-Adapter mit Firmware-Version 2.5

Hinweis: Produkte der Cisco Aironet Serie 350 unterstützen WPA 2 nicht, da ihre Funkmodule keine AES-Unterstützung bieten.

Hinweis: Cisco Aironet Wireless Bridges der Serie 1400 unterstützen WPA 2 oder AES nicht.

[Konfiguration im Enterprise-Modus](#)

Der Begriff **Enterprise-Modus** bezieht sich auf Produkte, die getestet wurden, um sowohl im Pre-Shared Key (PSK)- als auch im IEEE 802.1x-Betriebsmodus für die Authentifizierung interoperabel zu sein. 802.1x gilt als sicherer als jedes andere Legacy-Authentifizierungs-Framework, da es eine Vielzahl von Authentifizierungsmechanismen und stärkere Verschlüsselungsalgorithmen flexibel unterstützt. WPA2 führt im Enterprise-Modus die Authentifizierung in zwei Phasen durch. Die Konfiguration der offenen Authentifizierung erfolgt in der ersten Phase. Die zweite Phase ist die 802.1x-Authentifizierung mit einer der EAP-Methoden. AES stellt den Verschlüsselungsmechanismus bereit.

Im Enterprise-Modus authentifizieren sich Clients und Authentifizierungsserver gegenseitig mithilfe einer EAP-Authentifizierungsmethode, und Client und Server generieren einen paarweisen Master Key (PMK). Mit WPA 2 generiert der Server den PMK dynamisch und übergibt den PMK an den AP.

In diesem Abschnitt wird die Konfiguration erläutert, die für die Implementierung von WPA 2 im Enterprise-Modus erforderlich ist.

[Netzwerkeinrichtung](#)

In dieser Konfiguration authentifiziert ein Aironet 1310G AP/Bridge, der das Cisco Lightweight Extensible Authentication Protocol (LEAP) ausführt, einen Benutzer mit einem WPA 2-kompatiblen Client-Adapter. Die Schlüsselverwaltung erfolgt über WPA 2, auf dem die AES-CCMP-Verschlüsselung konfiguriert ist. Der AP ist als lokaler RADIUS-Server konfiguriert, auf dem die LEAP-Authentifizierung ausgeführt wird. Sie müssen den Client-Adapter und den Access Point konfigurieren, um diese Konfiguration zu implementieren. Die Abschnitte [Konfigurieren des Access Points](#) und [Konfigurieren des Client-Adapters](#) zeigen die Konfiguration des Access Points und des Client-Adapters.

[Konfigurieren des Access Points](#)

Gehen Sie wie folgt vor, um den Access Point mithilfe der Benutzeroberfläche zu konfigurieren:

1. Konfigurieren Sie den Access Point als lokalen RADIUS-Server, auf dem die LEAP-Authentifizierung ausgeführt wird. Wählen Sie im Menü links **Security > Server Manager** aus, und definieren Sie die IP-Adresse, die Ports und den gemeinsamen geheimen Schlüssel des RADIUS-Servers. Da der Access Point bei dieser Konfiguration als lokaler RADIUS-Server konfiguriert wird, verwenden Sie die IP-Adresse des Access Points. Verwenden Sie die Ports 1812 und 1813 für den lokalen RADIUS-Serverbetrieb. Legen Sie im Bereich Default Server Priorities (Standardserverprioritäten) die standardmäßige EAP-Authentifizierungspriorität als 10.0.0.1 fest. **Hinweis:** 10.0.0.1 ist der lokale RADIUS-Server.

Cisco Aironet 1300 Series Wireless Bridge

SERVER MANAGER GLOBAL PROPERTIES

Hostname bridge bridge uptime is 7 minutes

Security: Server Manager

Backup RADIUS Server

Backup RADIUS Server: (Hostname or IP Address)
 Shared Secret:

Apply Delete Cancel

Corporate Servers

Current Server List

10.0.0.1

Server: (Hostname or IP Address)
 Shared Secret:

Delete

Authentication Port (optional): (0-65536)
 Accounting Port (optional): (0-65536)

Apply Cancel

Default Server Priorities

EAP Authentication MAC Authentication Accounting

Priority 1: Priority 1: Priority 1:

2. Wählen Sie im Menü links **Security > Encryption Manager** aus, und führen Sie die folgenden Schritte aus: Wählen Sie im Menü Cipher die Option **AES CCMP**. Diese Option aktiviert die AES-Verschlüsselung unter Verwendung des Zählermodus mit CBC-MAC.

Cisco Aironet 1300 Series Wireless Bridge

Hostname bridge bridge uptime is 5 minutes

Security: Encryption Manager

Encryption Modes

None

WEP Encryption

Cisco Compliant TKIP Features: Enable Message Integrity Check (MIC)
 Enable Per Packet Keying (PPK)

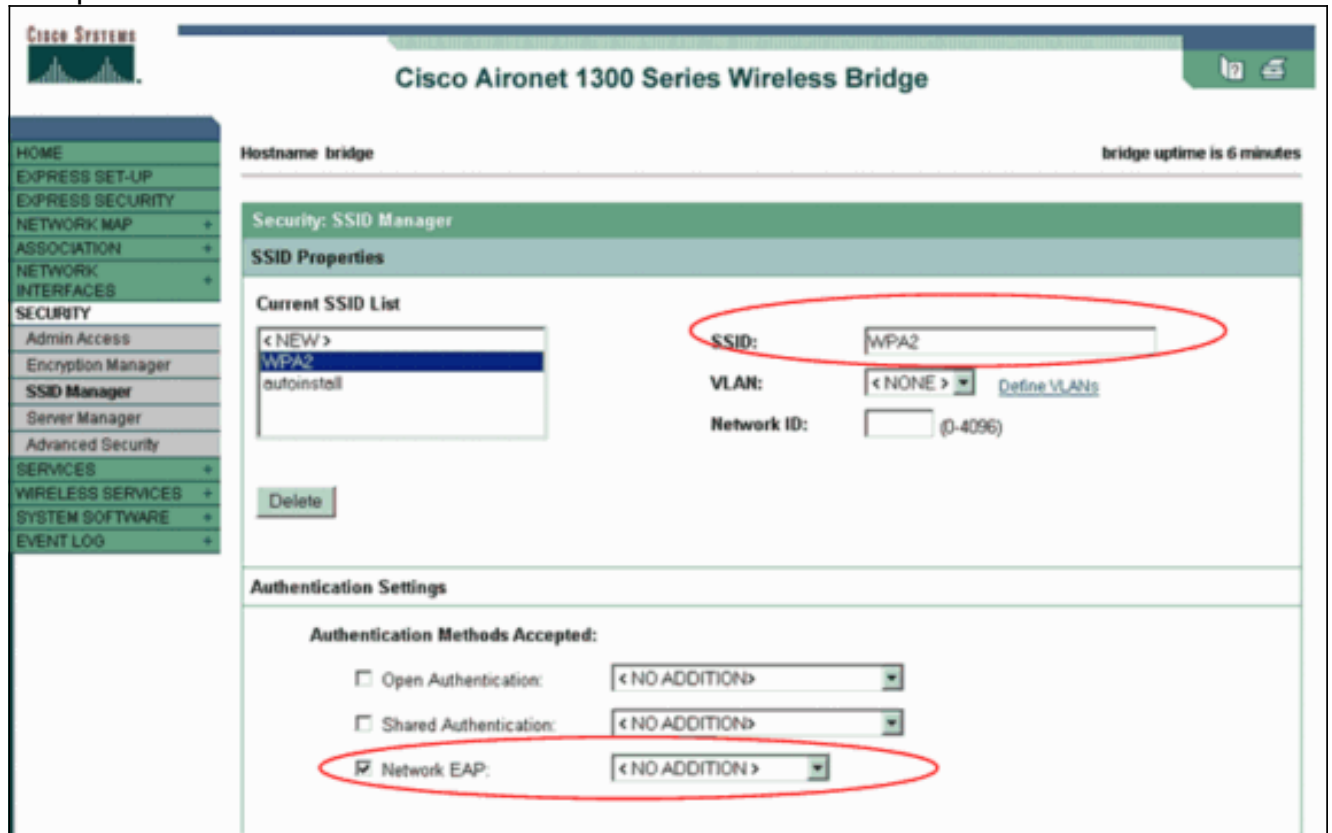
Cipher

Encryption Keys

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input type="radio"/>	<input type="text"/>	<input type="text" value="128 bit"/>
Encryption Key 2:	<input checked="" type="radio"/>	<input type="text"/>	<input type="text" value="128 bit"/>
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	<input type="text" value="128 bit"/>
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	<input type="text" value="128 bit"/>

Klicken Sie auf **Übernehmen**.

3. Wählen Sie **Security > SSID Manager (Sicherheit > SSID-Manager)**, und erstellen Sie einen neuen Service Set Identifier (SSID) für die Verwendung mit WPA 2. Aktivieren Sie das Kontrollkästchen **Network EAP** im Bereich Authentifizierungsmethoden akzeptiert.



Hinweis: Verwenden Sie diese Richtlinien, wenn Sie den Authentifizierungstyp auf der Funkschnittstelle konfigurieren: Cisco Clients - Verwenden Sie Network EAP. Drittanbieter-Clients (die Cisco Compatible Extensions [CCX]-konforme Produkte enthalten) - Verwenden Sie die Open Authentication mit EAP. Eine Kombination aus Cisco Clients und Clients von Drittanbietern - Wählen Sie Network EAP und Open Authentication with EAP. Blättern Sie im Fenster Security SSID Manager nach unten zum Bereich Authenticated Key Management (Authentifiziertes Schlüsselmanagement), und führen Sie die folgenden Schritte aus: Wählen Sie im Menü Key Management (Schlüsselverwaltung) die Option **Obligatorisch aus**. Aktivieren Sie das Kontrollkästchen **WPA** rechts. Klicken Sie auf **Übernehmen**. **Hinweis:** Die Definition von VLANs ist optional. Wenn Sie VLANs definieren, werden Client-Geräte, die mit der Verwendung dieser SSID verknüpft sind, in das VLAN gruppiert. Weitere Informationen zur Implementierung von VLANs finden Sie unter [Konfigurieren von VLANs](#).

Authenticated Key Management

Key Management: CCCKM WPA

WPA Pre-shared Key: ASCII Hexadecimal

Accounting Settings

Enable Accounting

Accounting Server Priorities:

Use Defaults [Define Defaults](#)

Customize

Priority 1:

Priority 2:

Priority 3:

General Settings

Advertise Extended Capabilities of this SSID

Advertise Wireless Provisioning Services (WPS) Support

Advertise this SSID as a Secondary Broadcast SSID

Enable IP Redirection on this SSID

IP Address:

IP Filter (optional): [Define Filter](#)

4. Wählen Sie **Security > Local Radius Server**, und führen Sie die folgenden Schritte aus: Klicken Sie auf die Registerkarte **Allgemeine Einrichtung** oben im Fenster. Aktivieren Sie das Kontrollkästchen **LEAP**, und klicken Sie auf **Übernehmen**. Legen Sie im Bereich Network Access Servers (Netzwerkzugriffsserver) die IP-Adresse und den gemeinsamen geheimen Schlüssel des RADIUS-Servers fest. Verwenden Sie für den lokalen RADIUS-Server die IP-Adresse des AP.

The screenshot shows the configuration interface for a Cisco Aironet 1300 Series Wireless Bridge. The page is titled "Cisco Aironet 1300 Series Wireless Bridge" and has three tabs: "STATISTICS", "GENERAL SET-UP", and "EAP-FAST SET-UP". The "GENERAL SET-UP" tab is active. The page shows the "Local Radius Server Authentication Settings" section, where the "Enable Authentication Protocols" are listed: "EAP FAST" (unchecked), "LEAP" (checked and circled in red), and "MAC" (unchecked). Below this, the "Current Network Access Servers" section is visible, showing a list of servers with a "Delete" button. A "Network Access Server" field is circled in red and contains the IP address "10.0.0.1". The "Shared Secret" field is also circled in red. The page includes a sidebar with navigation options like "HOME", "EXPRESS SET-UP", "SECURITY", and "SERVICES".

Klicken Sie auf **Übernehmen**.

5. Blättern Sie im Fenster "Allgemeine Einrichtung" nach unten zum Bereich Individuelle Benutzer, und definieren Sie die einzelnen Benutzer. Die Definition der Benutzergruppen ist optional.

The screenshot shows a configuration interface with two main sections: 'Individual Users' and 'User Groups'.

Individual Users:

- Current Users:** A list containing '<NEW>' and 'user1'. A 'Delete' button is below the list.
- Username:** 'user1' (circled in red).
- Password:** A masked field with a radio button for 'Text' and a selected radio button for 'NT Hash'.
- Confirm Password:** An empty text field.
- Group Name:** '<NONE >'.
- MAC Authentication Only
- Buttons: 'Apply' and 'Cancel'.

User Groups:

- Current User Groups:** A list containing '<NEW>'. A 'Delete' button is below the list.
- Group Name:** An empty text field.
- Session Timeout (optional):** An empty text field with '(1-4294967295 sec)' to its right.
- Failed Authentications before Lockout (optional):** An empty text field with '(1-4294967295)' to its right.
- Lockout (optional):** Radio buttons for 'Infinite' and 'Interval' (selected). The 'Interval' option has an empty text field and '(1-4294967295 sec)' to its right.
- VLAN ID (optional):** An empty text field.
- SSID (optional):** An empty text field with an 'Add' button to its right.
- Buttons: 'Delete'.

Diese Konfiguration definiert einen Benutzer mit dem Namen "user1" und einem Kennwort. Außerdem wählt die Konfiguration NT-Hash als Kennwort aus. Nach Abschluss des Verfahrens in diesem Abschnitt kann der Access Point Authentifizierungsanforderungen von Clients akzeptieren. Im nächsten Schritt wird der Client-Adapter konfiguriert.

CLI-Konfiguration

Access Point

```
ap#show running-config
Building configuration...
.
.
.
aaa new-model !--- This command reinitializes the
authentication, !--- authorization and accounting
functions. !! aaa group server radius rad_eap
server 10.0.0.1 auth-port 1812 acct-port 1813
!--- A server group for RADIUS is created called
"rad_eap" !--- that uses the server at 10.0.0.1 on ports
1812 and 1813. . . . aaa authentication login
eap_methods group rad_eap
!--- Authentication [user validation] is to be done for
!--- users in a group called "eap_methods" who use
server group "rad_eap". . . . ! bridge irb ! interface
```

```

Dot11Radio0 no ip address no ip route-cache !
encryption vlan 1 key 1 size 128bit
    12345678901234567890123456 transmit-key
    !---This step is optional !--- This value seeds the
    initial key for use with !--- broadcast
    [255.255.255.255] traffic. If more than one VLAN is !---
    used, then keys must be set for each VLAN. encryption
vlan 1 mode wep mandatory
    !--- This defines the policy for the use of Wired
    Equivalent Privacy (WEP). !--- If more than one VLAN is
    used, !--- the policy must be set to mandatory for each
    VLAN. broadcast-key vlan 1 change 300
    !--- You can also enable Broadcast Key Rotation for
    each vlan and Specify the time after which Brodacst key
    is changed. If it is disabled Broadcast Key is still
    used but not changed. ssid cisco vlan 1
    !--- Create a SSID Assign a vlan to this SSID
authentication open eap eap_methods
    authentication network-eap eap_methods
    !--- Expect that users who attach to SSID "cisco" !---
    request authentication with the type 128 Open EAP and
    Network EAP authentication !--- bit set in the headers
    of those requests, and group those users into !--- a
    group called "eap_methods." ! speed basic-1.0 basic-2.0
    basic-5.5 basic-11.0 rts threshold 2312 channel 2437
    station-role root bridge-group 1 bridge-group 1
    subscriber-loop-control bridge-group 1 block-unknown-
    source no bridge-group 1 source-learning no bridge-group
    1 unicast-flooding bridge-group 1 spanning-disabled . .
    . interface FastEthernet0 no ip address no ip route-
    cache duplex auto speed auto bridge-group 1 no bridge-
    group 1 source-learning bridge-group 1 spanning-disabled
    ! interface BVI1 ip address 10.0.0.1 255.255.255.0 !---
    The address of this unit. no ip route-cache ! ip
    default-gateway 10.77.244.194 ip http server ip http
    help-path
    http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
    lp/eag/ivory/1100 ip radius source-interface BVI1 snmp-
    server community cable RO snmp-server enable traps tty
radius-server local
    !--- Engages the Local RADIUS Server feature. nas
10.0.0.1 key shared_secret
    !--- Identifies itself as a RADIUS server, reiterates !-
    -- "localness" and defines the key between the server
    (itself) and the access point(itself). ! group testuser
    !--- Groups are optional. ! user user1 nhash password1
    group testuser
    !--- Individual user user user2 nhash password2 group
    testuser
    !--- Individual user !--- These individual users
    comprise the Local Database ! radius-server host
10.0.0.1 auth-port 1812 acct-port
    1813 key shared_secret
    !--- Defines where the RADIUS server is and the key
    between !--- the access point (itself) and the server.
    radius-server retransmit 3 radius-server attribute 32
    include-in-access-req format %h radius-server
    authorization permit missing Service-Type radius-server
    vsa send accounting bridge 1 route ip ! ! line con 0
    line vty 5 15 ! end

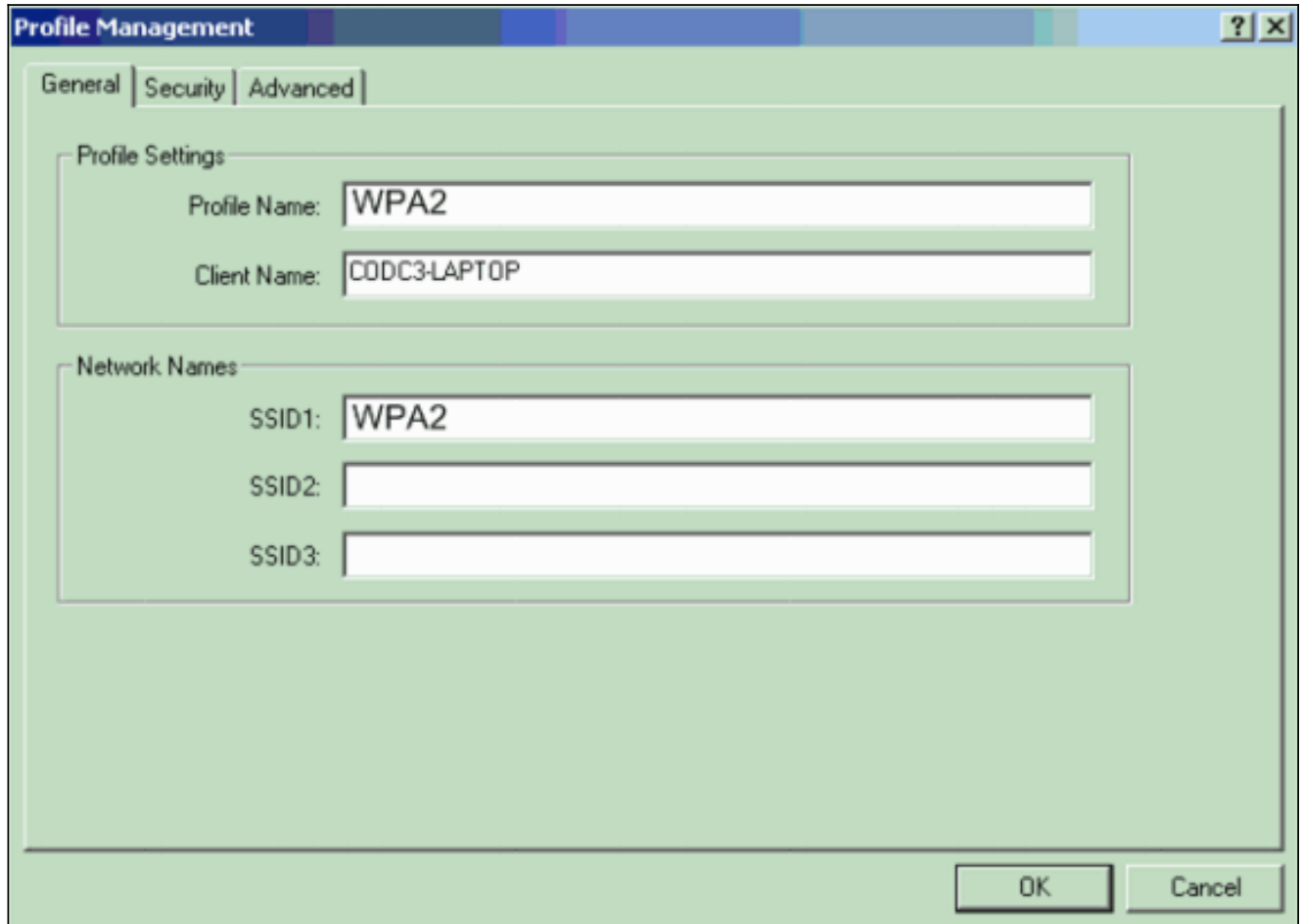
```

Konfigurieren des Client-Adapters

Gehen Sie wie folgt vor:

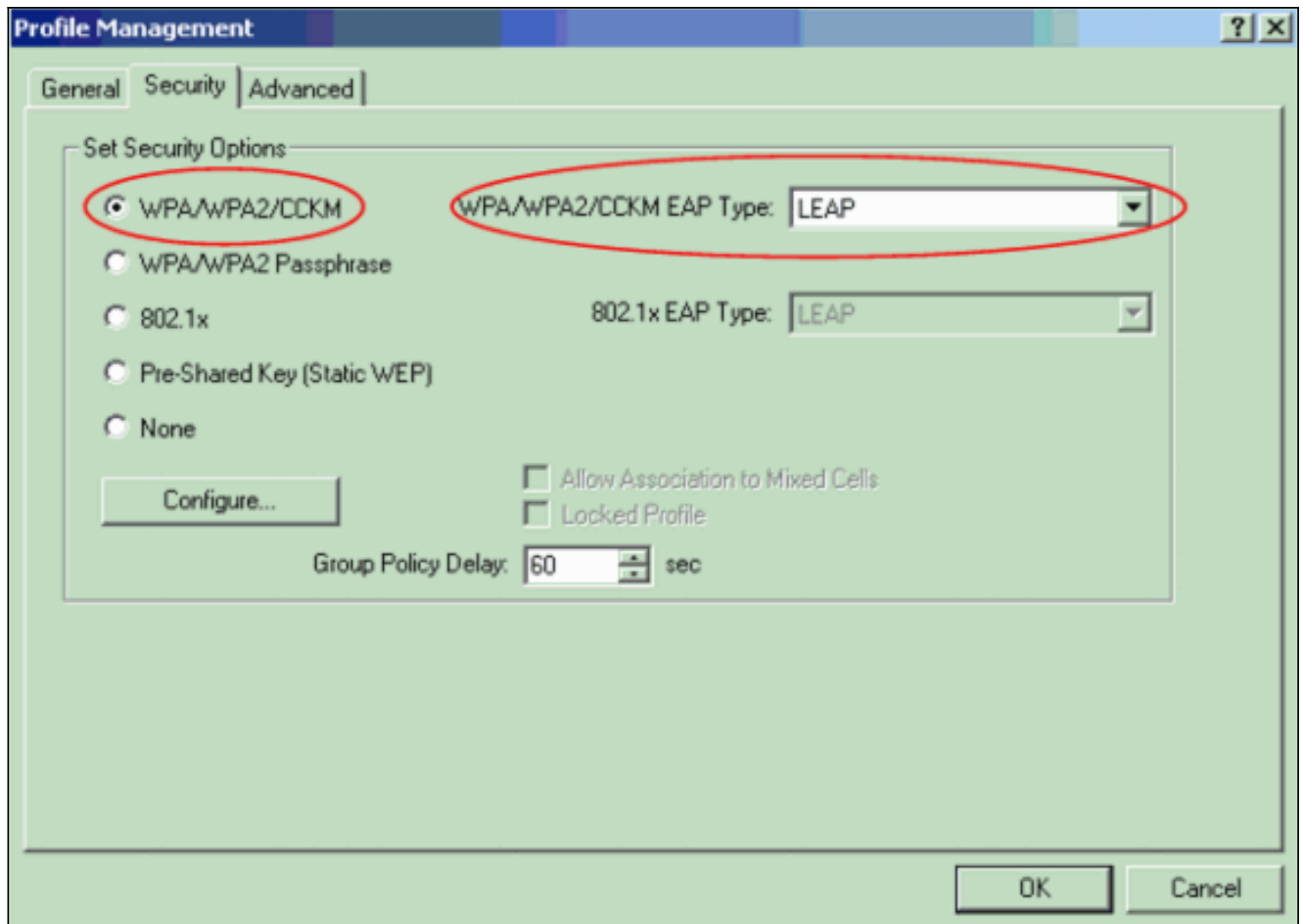
Hinweis: Dieses Dokument verwendet einen Aironet 802.11a/b/g Client Adapter, der Firmware 2.5 ausführt, und erläutert die Konfiguration des Client-Adapters mit ADU Version 2.5.

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 den WPA2-Enterprise-Modus festlegen können. Geben Sie auf der Registerkarte Allgemein den Profilnamen und die SSID ein, die der Client-Adapter verwendet. In diesem Beispiel sind der Profilename und die SSID WPA2: **Hinweis:** Die SSID muss mit der SSID übereinstimmen, die Sie auf dem Access Point für WPA 2 konfiguriert haben.



The screenshot shows a 'Profile Management' dialog box with three tabs: 'General', 'Security', and 'Advanced'. The 'General' tab is active. It contains two sections: 'Profile Settings' and 'Network Names'. In 'Profile Settings', 'Profile Name' is 'WPA2' and 'Client Name' is 'CODC3-LAPTOP'. In 'Network Names', 'SSID1' is 'WPA2', 'SSID2' is empty, and 'SSID3' is empty. At the bottom right are 'OK' and 'Cancel' buttons.

2. Klicken Sie auf die Registerkarte **Sicherheit**, klicken Sie auf **WPA/WPA2/CCKM**, und wählen Sie **LEAP** im Menü WPA/WPA2/CCKM EAP Type (WPA/WPA2/CCKM-EAP-Typ) aus. Diese Aktion aktiviert entweder WPA oder WPA 2, je nachdem, was Sie auf dem AP konfigurieren.



3. Klicken Sie auf **Konfigurieren**, um LEAP-Einstellungen zu definieren.
4. Wählen Sie je nach Anforderungen die entsprechenden Einstellungen für Benutzername und Kennwort aus, und klicken Sie auf **OK**. Bei dieser Konfiguration wird die Option Automatische Aufforderung zur Eingabe von Benutzername und Kennwort ausgewählt. Mit dieser Option können Sie den Benutzernamen und das Kennwort manuell eingeben, wenn die LEAP-Authentifizierung erfolgt.

LEAP Settings [?] [X]

Always Resume the Secure Session

Username and Password Settings

Use Temporary User Name and Password

Use Windows User Name and Password

Automatically Prompt for User Name and Password

Manually Prompt for User Name and Password

Use Saved User Name and Password

User Name:

Password:

Confirm Password:

Domain:

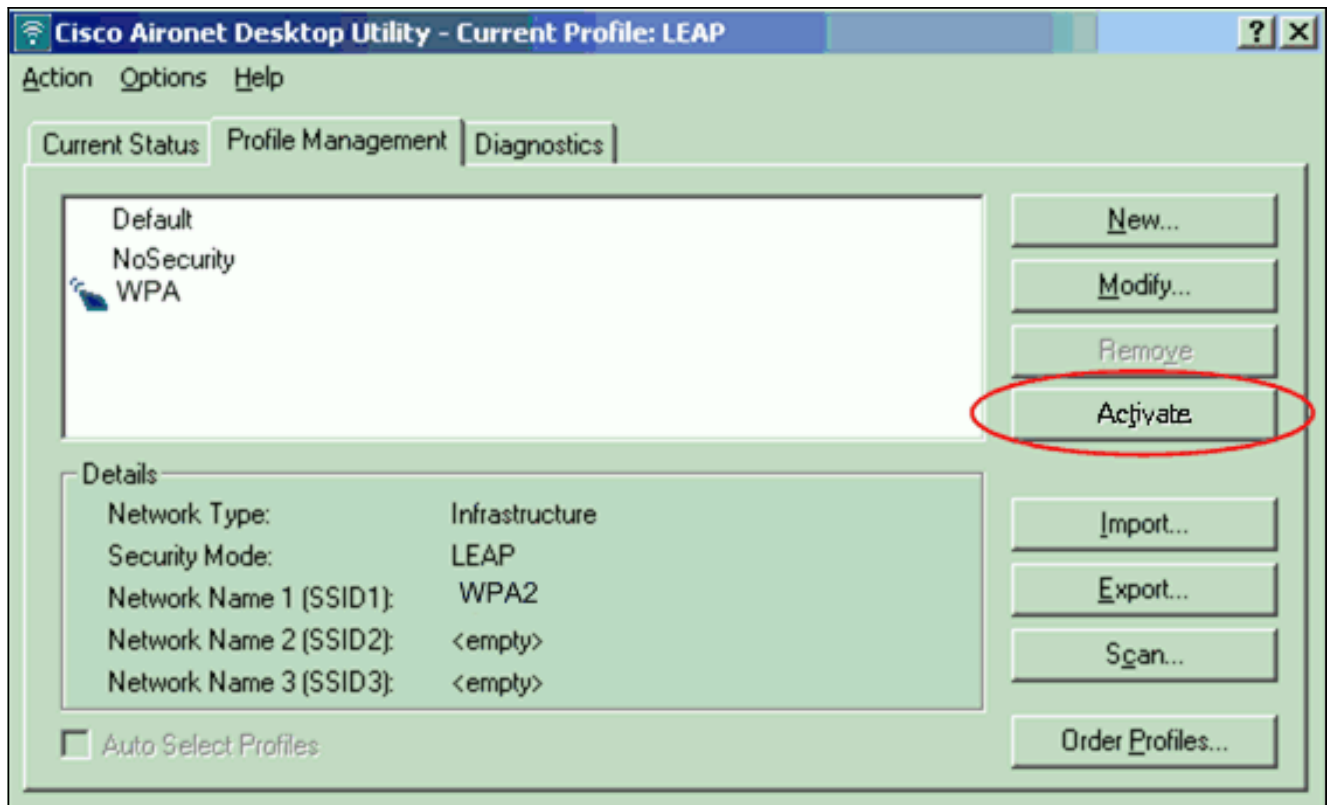
Include Windows Logon Domain with User Name

No Network Connection Unless User Is Logged In

Authentication Timeout Value (in seconds)

OK Cancel

5. Klicken Sie auf **OK**, um das Fenster Profilverwaltung zu schließen.
6. Klicken Sie auf **Aktivieren**, um dieses Profil auf dem Client-Adapter zu aktivieren.



Hinweis: Wenn Sie zur Konfiguration des Client-Adapters die Microsoft Wireless Zero Configuration (WZC) verwenden, ist WPA 2 standardmäßig nicht mit WZC verfügbar. Damit WZC-fähige Clients WPA 2 ausführen können, müssen Sie eine Hotfix für Microsoft Windows XP installieren. Informationen zur Installation finden Sie im [Microsoft Download Center - Update for Windows XP \(KB893357\)](#). Nach der Installation des Hotfix können Sie WPA 2 mit WZC konfigurieren.

Überprüfen

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

1. Wenn das Fenster Enter Wireless Network Password (Wireless-Netzwerkkenwort eingeben) angezeigt wird, geben Sie den Benutzernamen und das Kennwort

Enter Wireless Network Password

Please enter your LEAP username and password to log on to the wireless network

User Name : user1

Password : xxxxxxxx

Log on to :

Card Name : Cisco Aironet 802.11 a/b/g Wireless Adapter

Profile Name : WPA2

OK Cancel

ein. Das nächste Fenster lautet LEAP Authentication Status (LEAP-Authentifizierungsstatus). In dieser Phase werden die Benutzeranmeldeinformationen für den lokalen RADIUS-Server überprüft.

- Überprüfen Sie den Bereich Status, um das Ergebnis der Authentifizierung anzuzeigen.

LEAP Authentication Status

Card Name: Cisco Aironet 802.11 a/b/g Wireless Adapter

Profile Name: WPA2

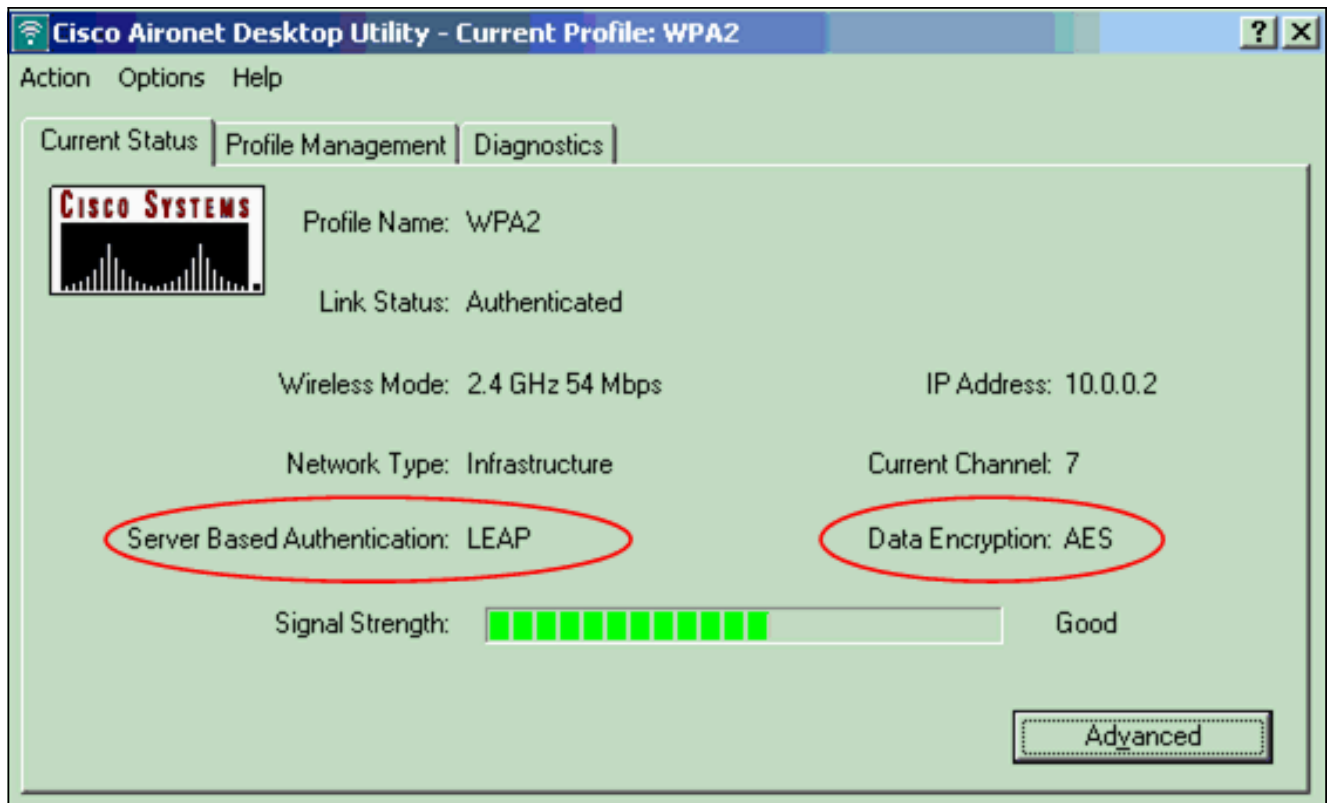
Steps	Status
1. Starting LEAP Authentication	Success
2. Checking Link Status	Success
3. Renewing IP address	Success
4. Detecting IPX Frame Type	Success
5. Finding Domain Controller	Success

Show minimized next time

Cancel

Wenn die Authentifizierung erfolgreich ist, stellt der Client eine Verbindung zum Wireless LAN her.

- Überprüfen Sie den aktuellen ADU-Status, um zu überprüfen, ob der Client die AES-Verschlüsselung und die LEAP-Authentifizierung verwendet. Dies zeigt, dass Sie WPA 2 mit LEAP-Authentifizierung und AES-Verschlüsselung im WLAN implementiert haben.



4. Überprüfen Sie das Ereignisprotokoll AP/Bridge, um zu überprüfen, ob der Client mit WPA 2 erfolgreich authentifiziert wurde.



Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Konfigurieren im persönlichen Modus

Der Begriff **persönlicher Modus** bezieht sich auf Produkte, die im PSK-only-Modus für die

Authentifizierung als interoperabel getestet wurden. Dieser Modus erfordert die manuelle Konfiguration eines PSK auf dem Access Point und den Clients. PSK authentifiziert Benutzer über ein Kennwort oder einen Identifikationscode auf der Client-Station und dem AP. Es ist kein Authentifizierungsserver erforderlich. Ein Client kann nur dann auf das Netzwerk zugreifen, wenn das Client-Kennwort mit dem AP-Kennwort übereinstimmt. Das Passwort enthält auch das Schlüsselmaterial, das TKIP oder AES zum Generieren eines Verschlüsselungsschlüssels für die Verschlüsselung der Datenpakete verwendet. Der Personal-Modus ist auf SOHO-Umgebungen ausgerichtet und gilt nicht als sicher für Unternehmensumgebungen. Dieser Abschnitt enthält die Konfiguration, die Sie benötigen, um WPA 2 im persönlichen Betriebsmodus zu implementieren.

Netzwerkeinrichtung

Bei dieser Konfiguration authentifiziert sich ein Benutzer mit einem WPA 2-kompatiblen Client-Adapter an einem Aironet 1310G AP/Bridge. Die Schlüsselverwaltung erfolgt bei Verwendung von WPA 2 PSK, wobei die AES-CCMP-Verschlüsselung konfiguriert wird. Die Abschnitte [Konfigurieren des Access Points](#) und [Konfigurieren des Client-Adapters](#) zeigen die Konfiguration des Access Points und des Client-Adapters.

Konfigurieren des Access Points

Gehen Sie wie folgt vor:

1. Wählen Sie im Menü links **Security > Encryption Manager** aus, und führen Sie die folgenden Schritte aus: Wählen Sie im Menü Cipher die Option **AES CCMP**. Diese Option aktiviert die AES-Verschlüsselung unter Verwendung des Zählermodus mit CCMP.

The screenshot shows the configuration interface for a Cisco Aironet 1300 Series Wireless Bridge. The page title is "Cisco Aironet 1300 Series Wireless Bridge". The hostname is "bridge" and the bridge uptime is 5 minutes. The left sidebar shows the navigation menu with "Security" expanded and "Encryption Manager" selected. The main content area is titled "Security: Encryption Manager" and shows the "Encryption Modes" section. The "Cipher" option is selected, and the dropdown menu shows "AES CCMP". Below this, there are checkboxes for "Cisco Compliant TKIP Features": "Enable Message Integrity Check (MIC)" and "Enable Per Packet Keying (PPK)". The "Encryption Keys" section contains a table with four keys, each with a "Transmit Key" radio button and a "Key Size" dropdown menu set to "128 bit".

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 2:	<input checked="" type="radio"/>	<input type="text"/>	128 bit
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	128 bit

Klicken Sie auf **Übernehmen**.

2. Wählen Sie **Security > SSID Manager (Sicherheit > SSID-Manager)**, und erstellen Sie eine

neue SSID für die Verwendung mit WPA 2. Aktivieren Sie das Kontrollkästchen **Authentifizierung** öffnen.

The screenshot displays the configuration interface for a Cisco Aironet 1300 Series Wireless Bridge. The page title is "Cisco Aironet 1300 Series Wireless Bridge". The hostname is "bridge" and the uptime is "7 minutes". The left sidebar shows the navigation menu with "SSID Manager" selected. The main content area is titled "Security: SSID Manager" and "SSID Properties". Under "Current SSID List", there is a list with entries: "< NEW >", "WPA2PSK", and "tsunami". The "WPA2PSK" entry is selected. To the right, the "SSID:" field contains "WPA2PSK", the "VLAN:" field is set to "< NONE >", and the "Network ID:" field is empty. Below the list is a "Delete" button. The "Authentication Settings" section is titled "Authentication Methods Accepted:" and shows three options: "Open Authentication" (checked), "Shared Authentication" (unchecked), and "Network EAP" (unchecked). The "Open Authentication" option is selected in a dropdown menu.

Blättern Sie nach unten zum Thema Sicherheit: Das Fenster SSID Manager wird in den Bereich für die Verwaltung authentifizierter Schlüssel verschoben. Gehen Sie wie folgt vor: Wählen Sie im Menü Key Management (Schlüsselverwaltung) die Option **Obligatorisch aus**. Aktivieren Sie das Kontrollkästchen **WPA** rechts.

Authenticated Key Management

Key Management: CCKM WPA

WPA Pre-shared Key: ASCII Hexadecimal

Accounting Settings

Enable Accounting

Accounting Server Priorities:

Use Defaults [Define Defaults](#)

Customize

Priority 1:

Priority 2:

Priority 3:

General Settings

Advertise Extended Capabilities of this SSID

Advertise Wireless Provisioning Services (WPS) Support

Advertise this SSID as a Secondary Broadcast SSID

Enable IP Redirection on this SSID

IP Address:

IP Filter (optional): [Define Filter](#)

Geben Sie den WPA PSK-Schlüssel für den geheimen Schlüssel oder den WPA PSK-Passphrase-Schlüssel ein. Dieser Schlüssel muss mit dem WPA PSK-Schlüssel übereinstimmen, den Sie auf dem Client-Adapter konfigurieren. Klicken Sie auf **Übernehmen**.

Der Access Point kann nun Authentifizierungsanforderungen von den Wireless-Clients empfangen.

[Konfigurieren des Client-Adapters](#)

Gehen Sie wie folgt vor:

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 den WPA 2 PSK-Betriebsmodus festlegen können. Geben Sie auf der Registerkarte Allgemein den Profilnamen und die SSID ein, die der Client-Adapter verwendet. In diesem Beispiel lautet der Profilname WPA2-PSK und die SSID WPA2PSK: **Hinweis:** Die SSID muss mit der SSID übereinstimmen, die Sie auf dem Access Point für das WPA 2 PSK konfiguriert haben.

The image shows a screenshot of a Windows dialog box titled "Profile Management". The dialog has three tabs: "General", "Security", and "Advanced". The "Security" tab is currently selected. Inside the dialog, there are two main sections: "Profile Settings" and "Network Names".

Profile Settings:

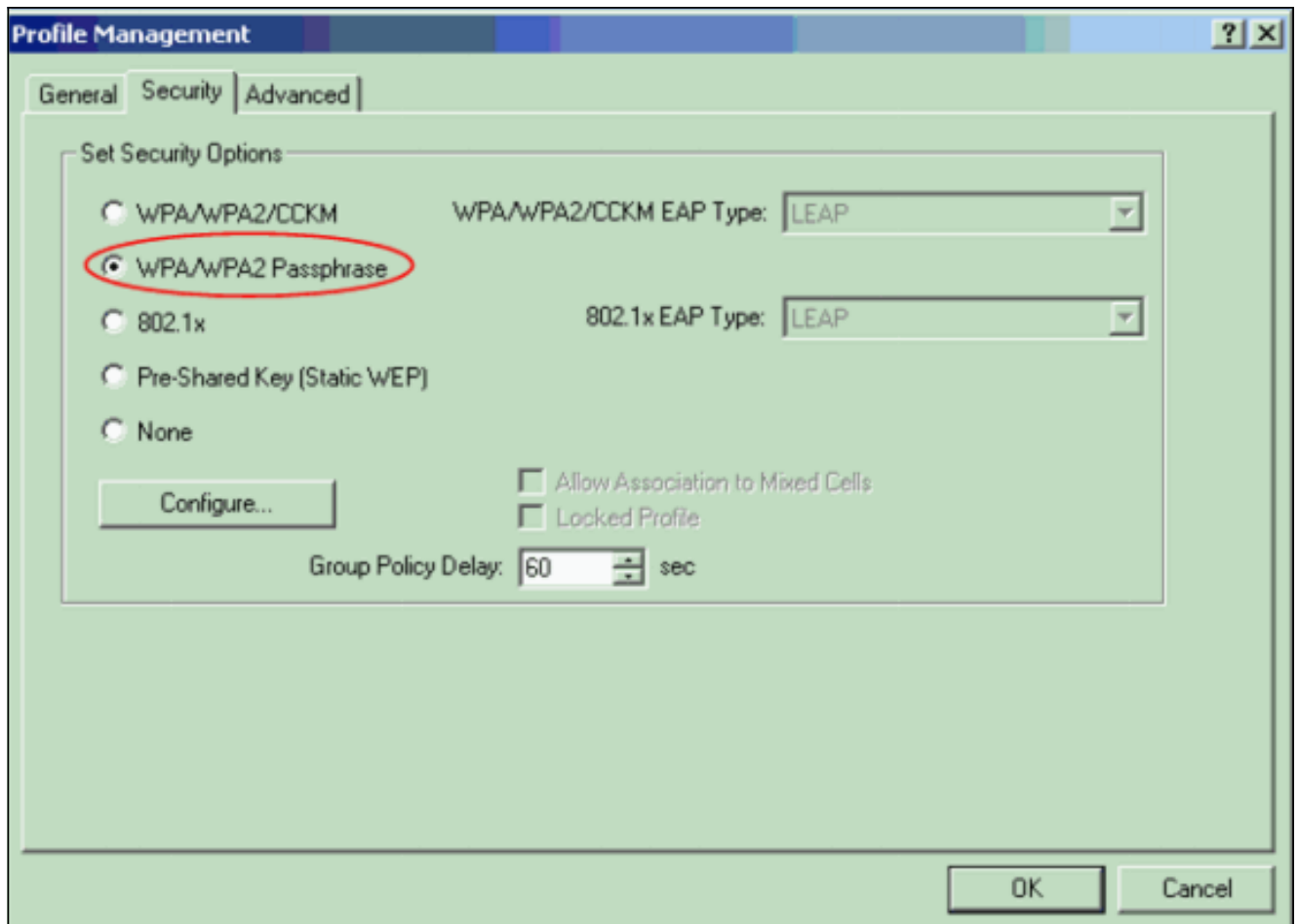
- Profile Name: WPA2-PSK
- Client Name: CODC3-LAPTOP

Network Names:

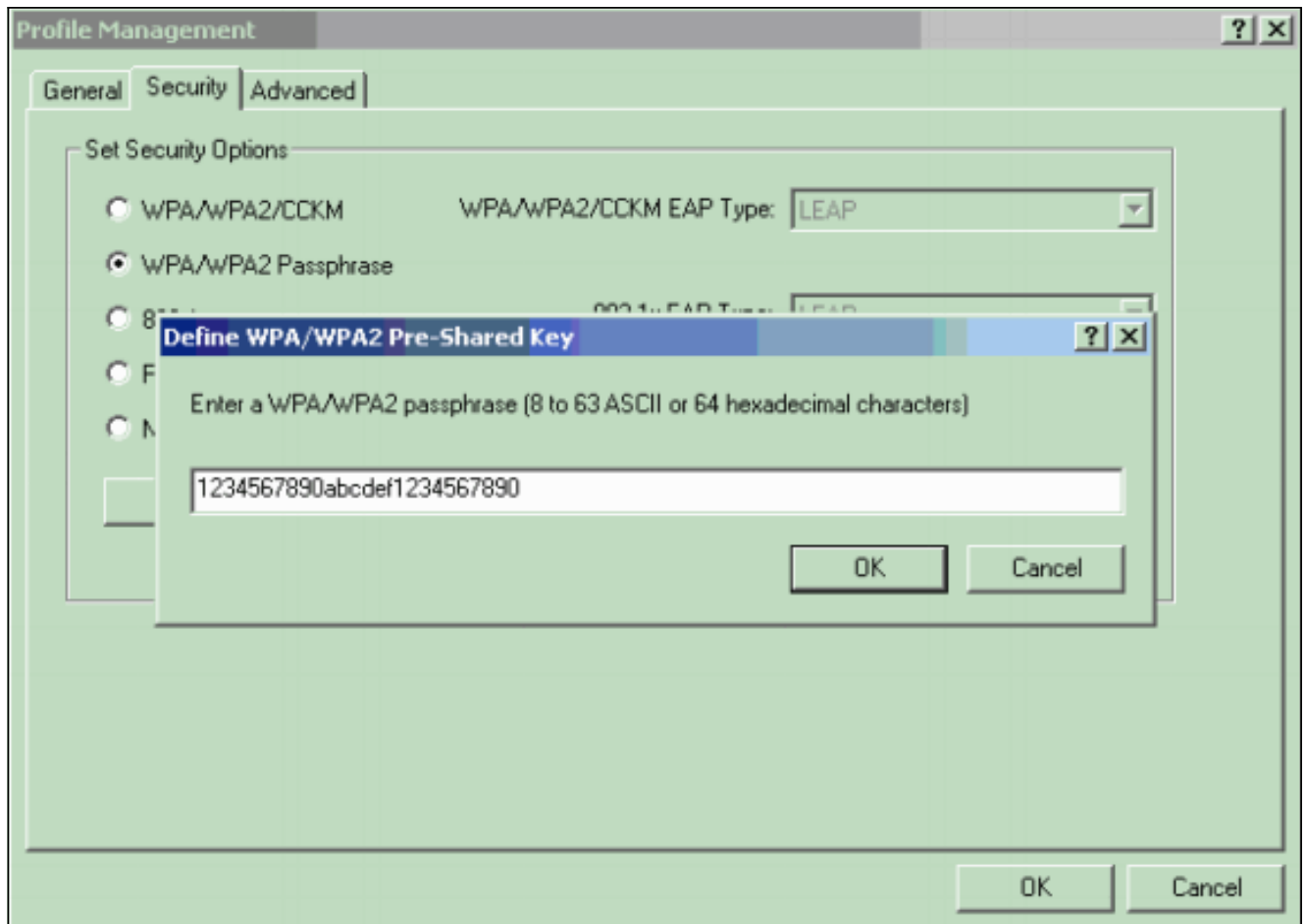
- SSID1: WPA2PSK
- SSID2: (empty)
- SSID3: (empty)

At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

2. Klicken Sie auf die Registerkarte **Sicherheit** und anschließend auf **WPA/WPA2-Passphrase**. Diese Aktion aktiviert entweder WPA PSK oder WPA 2 PSK, je nachdem, was Sie auf dem AP konfigurieren.



3. Klicken Sie auf **Konfigurieren**. Das Fenster Vorinstallierten Schlüssel für WPA/WPA2 definieren wird angezeigt.
4. Rufen Sie die WPA/WPA2-Passphrase von Ihrem Systemadministrator ab, und geben Sie die Passphrase in das Feld WPA/WPA2-Passphrase ein. Rufen Sie die Passphrase für den AP in einem Infrastrukturnetzwerk oder die Passphrase für andere Clients in einem Ad-hoc-Netzwerk ab. Verwenden Sie diese Richtlinien, um eine Passphrase einzugeben: WPA/WPA2-Passphrasen müssen zwischen 8 und 63 ASCII-Textzeichen oder 64 Hexadezimalzeichen enthalten. Die WPA/WPA2-Passphrase des Client-Adapters muss mit der Passphrase des AP übereinstimmen, mit dem Sie kommunizieren möchten.



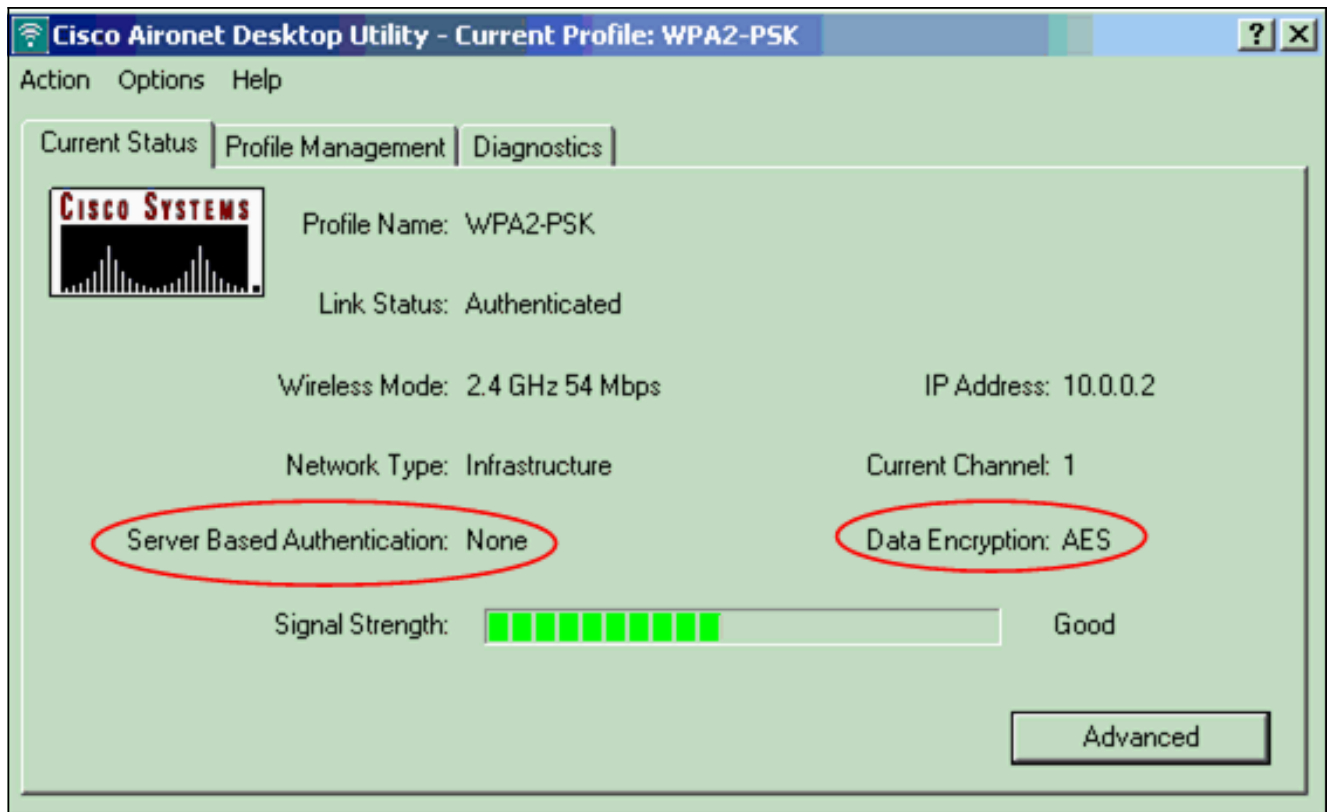
5. Klicken Sie auf **OK**, um die Passphrase zu speichern und zum Fenster Profilverwaltung zurückzukehren.

Überprüfen

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

Nach Aktivierung des WPA 2 PSK-Profiles authentifiziert der WAP den Client anhand der WPA 2-Passphrase (PSK) und ermöglicht den Zugriff auf das WLAN.

1. Überprüfen Sie den aktuellen ADU-Status, um die erfolgreiche Authentifizierung zu überprüfen. Dieses Fenster enthält ein Beispiel. Das Fenster zeigt an, dass die verwendete Verschlüsselung AES ist und dass keine serverbasierte Authentifizierung erfolgt:



- Überprüfen Sie das AP/Bridge-Ereignisprotokoll, um sicherzustellen, dass der Client erfolgreich mit dem WPA2 PSK-Authentifizierungsmodus authentifiziert wurde.



Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- [Konfigurieren von Cipher-Suiten und WEP](#)
- [Konfigurieren von Authentifizierungstypen](#)
- [Übersicht über die WPA-Konfiguration](#)
- [WPA2 - Wi-Fi Protected Access 2](#)
- [Was ist der gemischte WPA-Modus, und wie wird er in meinem AP konfiguriert?](#)
- [Wireless-Support-Seite](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)