

Einschränken des WLAN-Zugriffs auf der Basis der SSID mit WLC und Cisco Secure ACS - Konfigurationsbeispiel

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[Netzwerkeinrichtung](#)

[Konfiguration](#)

[Konfigurieren des WLC](#)

[Konfigurieren von Cisco Secure ACS](#)

[Konfigurieren des Wireless-Clients und Überprüfen](#)

[Fehlerbehebung](#)

[Befehle zur Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

Dieses Dokument enthält ein Konfigurationsbeispiel, um den benutzerspezifischen Zugriff auf ein WLAN auf Basis der Service Set Identifier (SSID) zu beschränken.

Voraussetzungen

Anforderungen

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

- Kenntnisse der Konfiguration von Wireless LAN Controller (WLC) und Lightweight Access Point (LAP) für den grundlegenden Betrieb
- Grundlegende Informationen zur Konfiguration des Cisco Secure Access Control Server (ACS)
- Kenntnis der LWAPP- (Lightweight Access Point Protocol) und Wireless-Sicherheitsmethoden

Verwendete Komponenten

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

- Cisco WLC der Serie 2000 mit Firmware 4.0
- Cisco LAP der Serie 1000
- Cisco Secure ACS Server Version 3.2
- Cisco 802.11a/b/g Wireless Client-Adapter, der Firmware 2.6 ausführt
- Cisco Aironet Desktop Utility (ADU) Version 2.6

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 \(Technische Tipps von Cisco zu Konventionen\)](#).

Hintergrundinformationen

Bei Verwendung eines SSID-basierten WLAN-Zugriffs können die Benutzer anhand der SSID authentifiziert werden, die sie für die Verbindung mit dem WLAN verwenden. Der Cisco Secure ACS-Server dient zur Authentifizierung der Benutzer. Die Authentifizierung erfolgt in zwei Phasen des Cisco Secure ACS:

1. EAP-Authentifizierung
2. SSID-Authentifizierung basierend auf Network Access Restrictions (NARs) auf Cisco Secure ACS

Wenn die EAP- und SSID-basierte Authentifizierung erfolgreich ist, kann der Benutzer auf das WLAN zugreifen, oder der Benutzer wird getrennt.

Cisco Secure ACS verwendet die Funktion "NARs", um den Benutzerzugriff auf Basis der SSID zu beschränken. Ein NAR ist eine Definition, die Sie in Cisco Secure ACS erstellen, in der zusätzliche Bedingungen definiert werden, die erfüllt sein müssen, bevor ein Benutzer auf das Netzwerk zugreifen kann. Cisco Secure ACS wendet diese Bedingungen mithilfe von Informationen aus Attributen an, die von Ihren AAA-Clients gesendet wurden. NARs können zwar auf verschiedene Weise eingerichtet werden, sie basieren jedoch alle auf übereinstimmenden Attributinformationen, die vom AAA-Client gesendet werden. Daher müssen Sie Format und Inhalt der Attribute, die Ihre AAA-Clients senden, verstehen, wenn Sie effektive NARs verwenden möchten.

Beim Einrichten eines NAR können Sie auswählen, ob der Filter positiv oder negativ funktioniert. Das heißt, im NAR geben Sie an, ob der Netzwerkzugriff zugelassen oder verweigert werden soll, basierend auf einem Vergleich der von AAA-Clients gesendeten Informationen mit den im NAR gespeicherten Informationen. Wenn ein NAR jedoch nicht auf ausreichende Informationen zum Betrieb stößt, wird standardmäßig der Zugriff verweigert.

Sie können einen NAR für einen bestimmten Benutzer oder eine bestimmte Benutzergruppe definieren und auf diesen anwenden. Weitere Informationen finden Sie im [Whitepaper zu Netzwerkzugriffsbeschränkungen](#).

Cisco Secure ACS unterstützt zwei Arten von NAR-Filtern:

1. **IP-basierte Filter** - IP-basierte NAR-Filter beschränken den Zugriff auf der Grundlage der IP-Adressen des Endbenutzer-Clients und des AAA-Clients. Weitere Informationen zu diesem NAR-Filtertyp finden Sie unter [About IP-based NAR Filters](#).
2. **Nicht IP-basierte Filter** - Nicht IP-basierte NAR-Filter beschränken den Zugriff auf Basis eines einfachen Zeichenfolgenvergleichs eines vom AAA-Client gesendeten Werts. Der Wert kann die CLI-Nummer (Call Line ID), die DNIS-Nummer (Dialed Number Identification Service), die MAC-Adresse oder ein anderer vom Client stammender Wert sein. Damit dieser NAR-Typ funktioniert, muss der Wert in der NAR-Beschreibung genau mit dem übereinstimmen, was vom Client gesendet wird, einschließlich des verwendeten Formats. Beispielsweise entspricht (217) 555-4534 nicht dem Wert 217-555-4534. Weitere Informationen zu diesem NAR-Filtertyp finden Sie [unter About Non-IP-based NAR Filters](#).

In diesem Dokument werden die nicht IP-basierten Filter für die SSID-basierte Authentifizierung verwendet. Ein Nicht-IP-basierter NAR-Filter (d. h. ein DNIS/CLI-basierter NAR-Filter) ist eine Liste zulässiger oder abgelehnter Anruf-/Zugriffspunkte, die Sie bei der Einschränkung eines AAA-Clients verwenden können, wenn Sie keine etablierte IP-basierte Verbindung haben. Die nicht IP-basierte NAR-Funktion verwendet im Allgemeinen die CLI-Nummer und die DNIS-Nummer. Bei der Verwendung der Felder DNIS/CLI gibt es Ausnahmen. Sie können den SSID-Namen in das DNIS-Feld eingeben und eine SSID-basierte Authentifizierung durchführen. Der Grund hierfür ist, dass der WLC das DNIS-Attribut, den SSID-Namen, an den RADIUS-Server sendet. Wenn Sie also DNIS NAR entweder im Benutzer oder in der Gruppe erstellen, können Sie SSID-Einschränkungen pro Benutzer erstellen.

Wenn Sie RADIUS verwenden, verwenden die hier aufgeführten NAR-Felder die folgenden Werte:

- **AAA-Client** - Die NAS-IP-Adresse (Attribut 4) oder, falls die NAS-IP-Adresse nicht vorhanden ist, der NAS-Identifizierer (RADIUS-Attribut 32) wird verwendet.
- **Port** - Der NAS-Port (Attribut 5) oder, falls der NAS-Port nicht vorhanden ist, die NAS-Port-ID (Attribut 87) wird verwendet.
- **CLI** - Die Calling-Station-ID (Attribut 31) wird verwendet.
- **DNIS** - Die called-station-ID (Attribut 30) wird verwendet.

Weitere Informationen zur Verwendung von NAR finden Sie unter [Netzwerkzugriffsbeschränkungen](#).

Da der WLC das DNIS-Attribut und den SSID-Namen sendet, können Sie SSID-Einschränkungen pro Benutzer erstellen. Im Fall des WLC haben die NAR-Felder folgende Werte:

- **AAA-Client** - WLC-IP-Adresse
- **Port** -*
- **CLI** -*
- **DNIS** -*ssidname

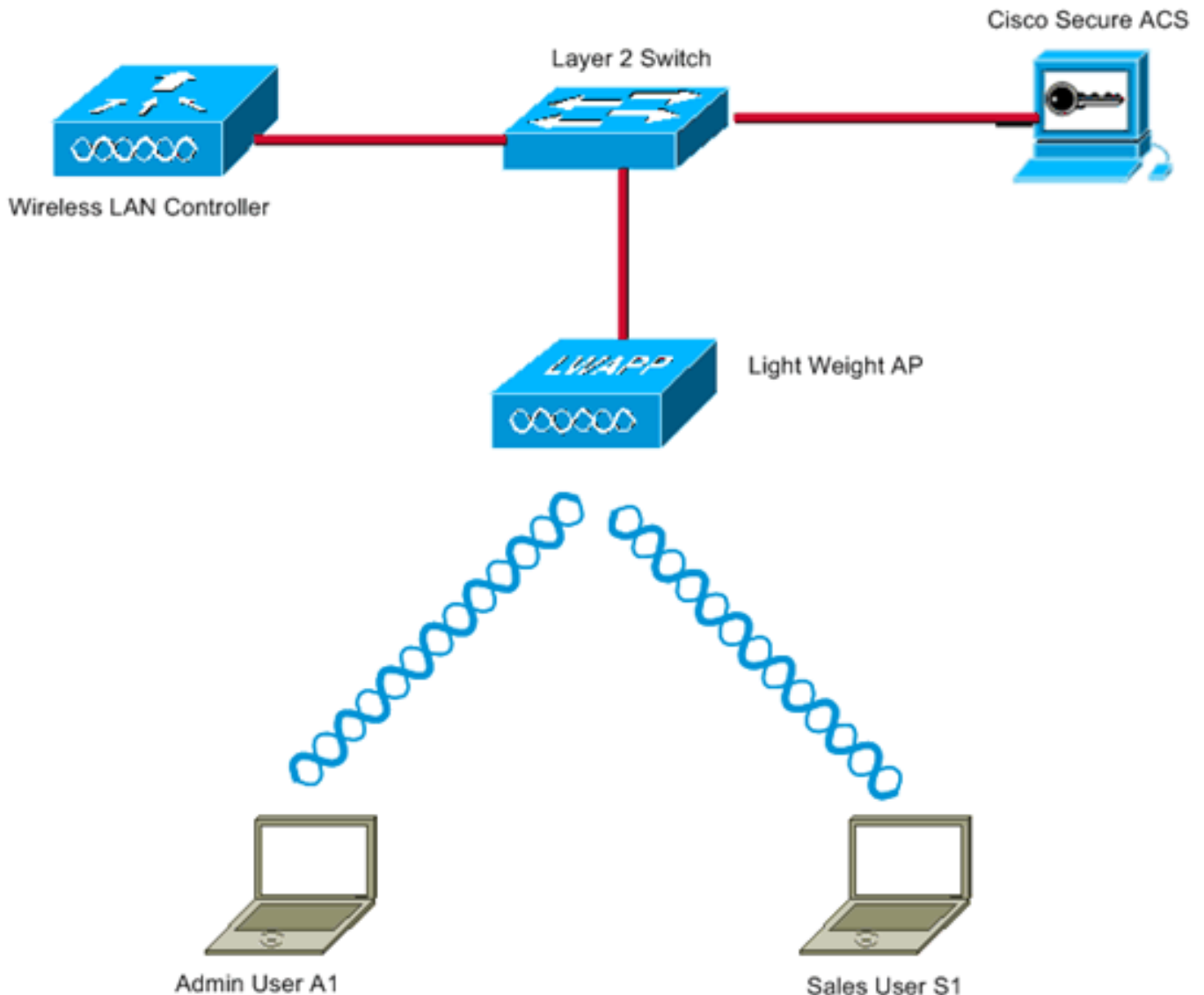
Im verbleibenden Teil dieses Dokuments finden Sie ein Konfigurationsbeispiel dazu, wie Sie dies erreichen können.

[Netzwerkeinrichtung](#)

In dieser Beispieleinrichtung ist WLC für die LAP registriert. Es werden zwei WLANs verwendet. Ein WLAN ist für die Benutzer der Admin-Abteilung und das andere für die Benutzer der

Vertriebsabteilung vorgesehen. Die Wireless-Clients A1 (Admin-Benutzer) und S1 (Sales-Benutzer) sind mit dem Wireless-Netzwerk verbunden. Sie müssen den WLC und den RADIUS-Server so konfigurieren, dass der Admin-Benutzer A1 nur auf den WLAN-Admin zugreifen kann und über eingeschränkten Zugriff auf den WLAN-Vertrieb verfügt. Der Vertriebsbenutzer S1 sollte auf den WLAN-Vertrieb zugreifen können und sollte über eingeschränkten Zugriff auf den WLAN-Admin verfügen. Alle Benutzer verwenden die LEAP-Authentifizierung als Layer-2-Authentifizierungsmethode.

Hinweis: In diesem Dokument wird davon ausgegangen, dass der WLC beim Controller registriert ist. Wenn Sie neu im WLC sind und nicht wissen, wie Sie den WLC für den Basisbetrieb konfigurieren, lesen Sie die Informationen zur [LAP-Registrierung \(Lightweight AP\) in einem Wireless LAN Controller \(WLC\)](#).



WLC Management Interface IP address : 172.16.1.30/16

WLC AP-Manager Interface IP address: 172.16.1.31/16

Cisco Secure ACS server IP address: 172.16.1.60/16

SSID for the Admin department users : Admin

SSID for Sales department users: Sales

Konfiguration

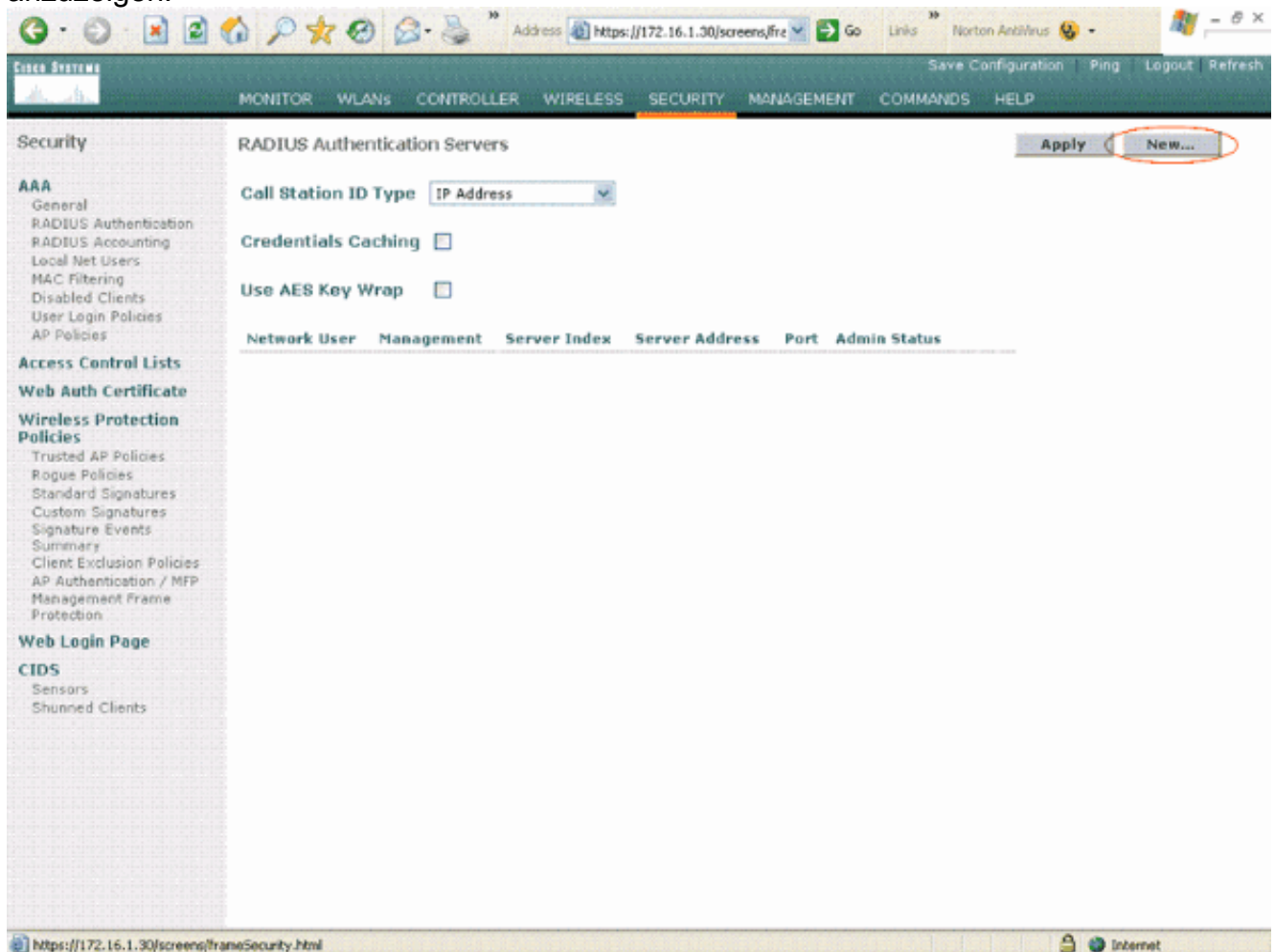
Um die Geräte für diese Konfiguration zu konfigurieren, müssen Sie:

1. [Konfigurieren Sie den WLC für die beiden WLANs und den RADIUS-Server.](#)
2. [Konfigurieren Sie den Cisco Secure ACS.](#)
3. [Konfigurieren Sie die Wireless-Clients, und überprüfen Sie.](#)

Konfigurieren des WLC

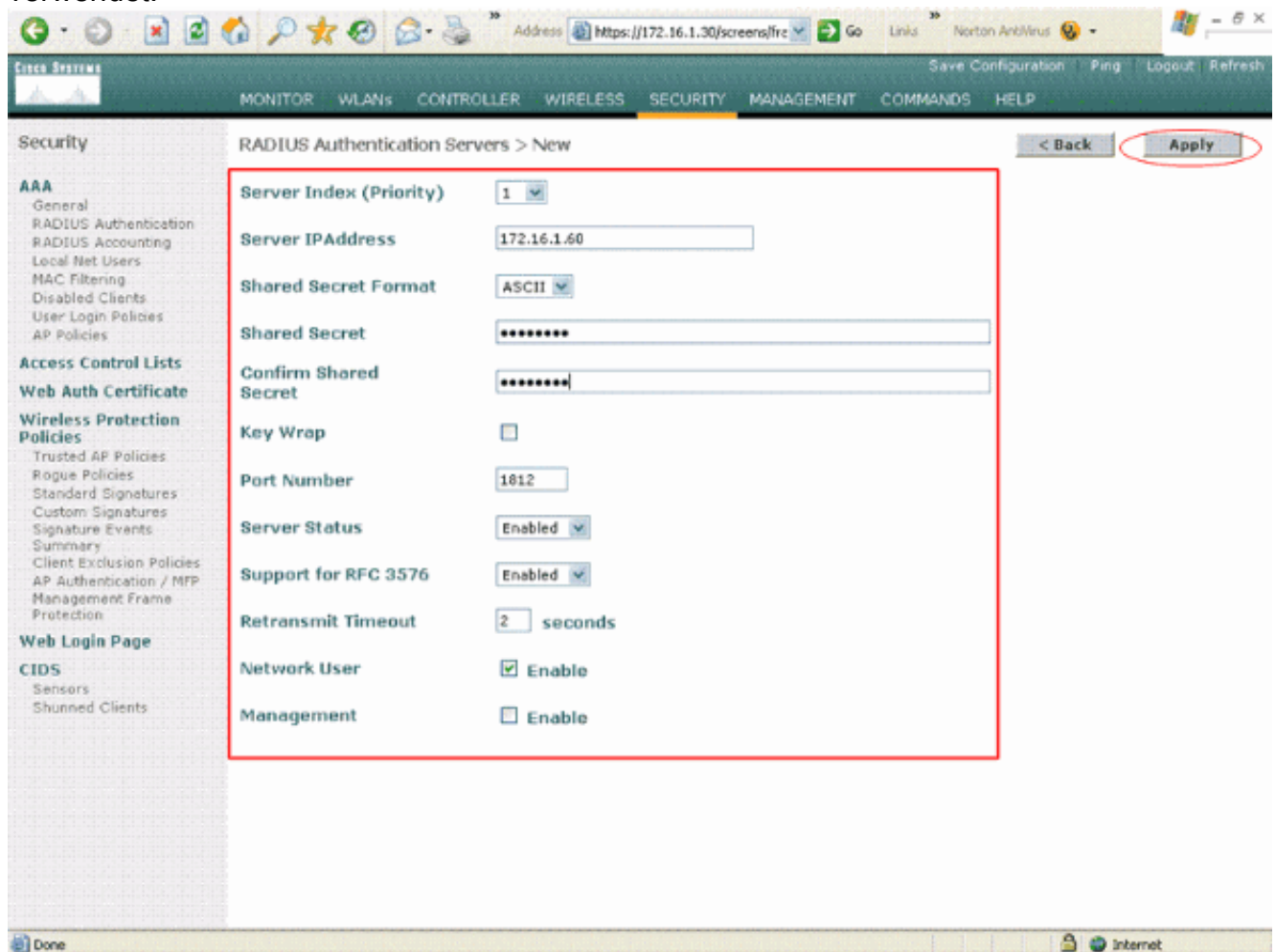
Führen Sie die folgenden Schritte aus, um den WLC für diese Einrichtung zu konfigurieren:

1. Der WLC muss so konfiguriert werden, dass die Benutzeranmeldeinformationen an einen externen RADIUS-Server weitergeleitet werden. Der externe RADIUS-Server (in diesem Fall Cisco Secure ACS) validiert dann die Benutzeranmeldeinformationen und ermöglicht den Zugriff auf die Wireless-Clients. Führen Sie diese Schritte aus: Wählen Sie **Security > RADIUS Authentication (Sicherheit > RADIUS-Authentifizierung)** in der Controller-GUI aus, um die Seite RADIUS Authentication Servers (RADIUS-Authentifizierungsserver) anzuzeigen.



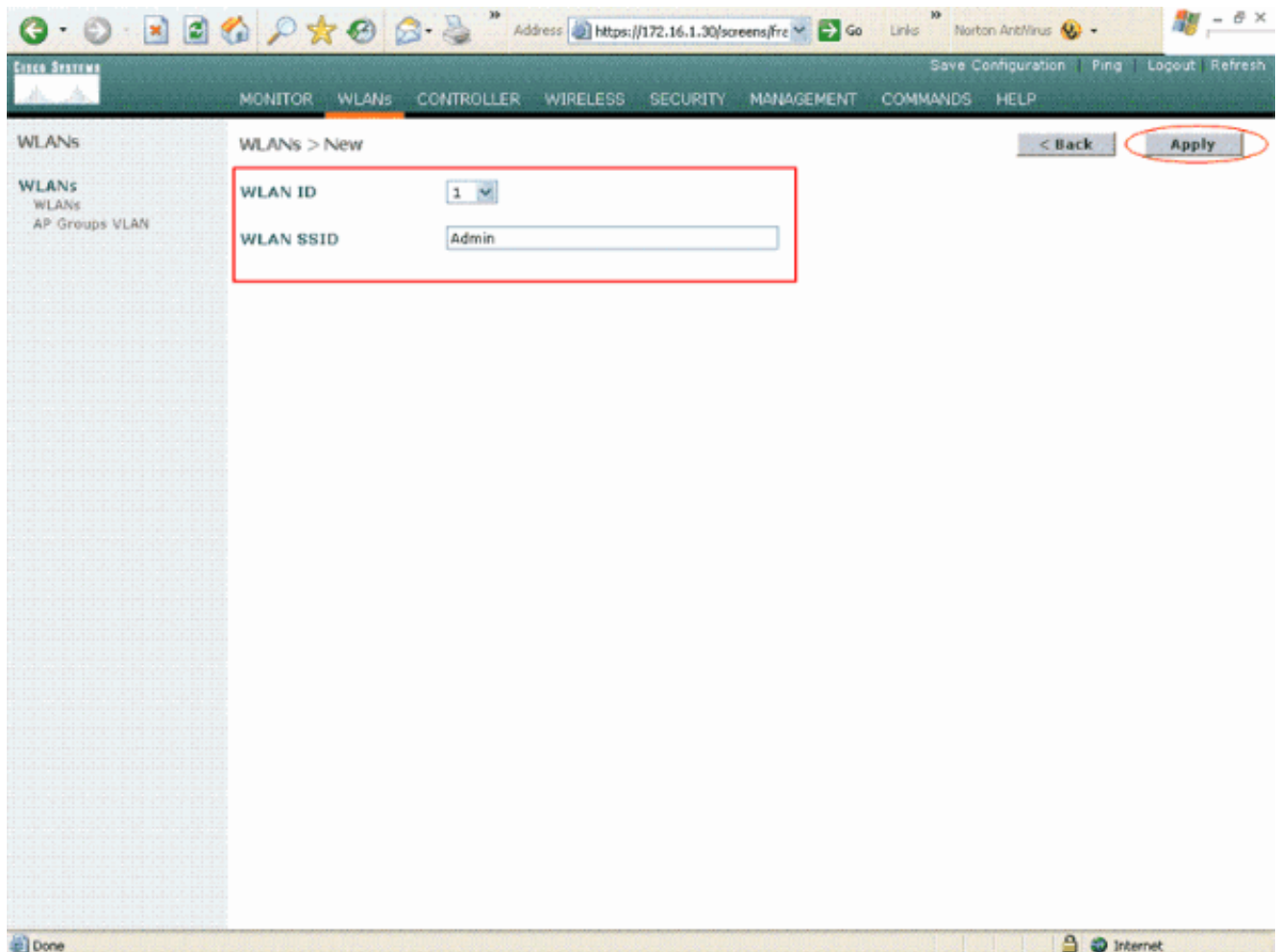
Klicken Sie auf **Neu**, um die RADIUS-Serverparameter zu definieren. Zu diesen Parametern gehören die IP-Adresse des RADIUS-Servers, der Shared Secret, die Portnummer und der Serverstatus. Die Kontrollkästchen für Netzwerkbenutzer und -verwaltung legen fest, ob die RADIUS-basierte Authentifizierung für Verwaltungs- und Netzwerkbenutzer gilt. In diesem Beispiel wird Cisco Secure ACS als RADIUS-Server mit der IP-Adresse 172.16.1.60

verwendet.



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

2. Konfigurieren Sie ein WLAN für die Admin-Abteilung mit SSID **Admin** und das andere WLAN für die Sales-Abteilung mit SSID **Sales**. Gehen Sie wie folgt vor, um dies zu tun: Klicken Sie in der Controller-GUI auf **WLANs**, um ein WLAN zu erstellen. Das Fenster WLANs wird angezeigt. In diesem Fenster werden die auf dem Controller konfigurierten WLANs aufgeführt. Klicken Sie auf **Neu**, um ein neues WLAN zu konfigurieren. In diesem Beispiel wird ein WLAN mit dem Namen **Admin** für die Admin-Abteilung erstellt, und die WLAN-ID lautet 1. Klicken Sie auf **Apply** (Anwenden).



Legen Sie im Fenster **WLAN > Edit** (WLAN > Bearbeiten) die für das WLAN spezifischen Parameter fest: Wählen Sie im Kontextmenü für die Layer-2-Sicherheit die Option **802.1x aus**. Standardmäßig ist die Layer-2-Sicherheitsoption 802.1x. Dadurch wird die 802.1x/EAP-Authentifizierung für das WLAN aktiviert. Aktivieren Sie unter "Allgemeine Richtlinien" das Kontrollkästchen **AAA override**. Wenn AAA Override aktiviert ist und ein Client im Konflikt stehende AAA- und Controller-WLAN-Authentifizierungsparameter aufweist, wird die Client-Authentifizierung vom AAA-Server durchgeführt. Wählen Sie im Dropdown-Menü unter RADIUS Servers den entsprechenden RADIUS-Server aus. Die anderen Parameter können je nach Anforderung des WLAN-Netzwerks geändert werden. Klicken Sie auf **Apply** (Anwenden).

The screenshot displays the Cisco Systems WLAN configuration interface. The page is titled "WLANs > Edit" and shows various configuration options for a WLAN with ID 1 and SSID "Admin". The "General Policies" section includes settings for Radio Policy (All), Admin Status (Enabled), Session Timeout (1800), QoS (Silver), WMM Policy (Disabled), 7920 Phone Support, Broadcast SSID (Enabled), Aironet IE (Enabled), Allow AAA Override (Enabled), Client Exclusion (Enabled), DHCP Server (Override), DHCP Addr. Assignment (Required), Interface Name (management), MFP Version Required (1), MFP Signature Generation (Global MFP Disabled), and H-REAP Local Switching. The "Security Policies" section shows Layer 2 Security set to 802.1X and Layer 3 Security set to None. The "Radius Servers" section shows a single server with IP 172.16.1.60 and Port 1812. Red circles highlight the "Apply" button, "Admin Status", "Allow AAA Override", "Layer 2 Security", and the Radius Server configuration.

In ähnlicher Weise wiederholen Sie die Schritte b und c, um ein WLAN für die Vertriebsabteilung zu erstellen. Hier sind die Screenshots.

Cisco Systems | Save Configuration | Ping | Logout | Refresh

MONITOR | **WLANs** | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP

WLANs > New

WLAN ID: 2

WLAN SSID: Sales

< Back | **Apply**

WLANs

WLANs

AP Groups VLAN

Done | Internet

Cisco Systems | Save Configuration | Ping | Logout | Refresh

MONITOR | **WLANs** | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP

WLANs > Edit

WLAN ID: 2

WLAN SSID: Sales

General Policies

Radio Policy: All

Admin Status: Enabled

Session Timeout (secs): 1800

Quality of Service (QoS): Silver (best effort)

WMM Policy: Disabled

7920 Phone Support: Client CAC Limit AP CAC Limit

Broadcast SSID: Enabled

Aironet IE: Enabled

Allow AAA Override: Enabled

Client Exclusion: Enabled ** 60 Timeout Value (secs)

DHCP Server: Override

DHCP Addr. Assignment: Required

Interface Name: management

MFP Version Required: 1

MFP Signature Generation: (Global MFP Disabled)

H-REAP Local Switching:

* H-REAP Local Switching not supported with IPSEC, L2TP, PPTP, CRANITE and FORTRESS authentications.

Security Policies

Layer 2 Security: 802.1X

MAC Filtering

Layer 3 Security: None

Web Policy *

* Web Policy cannot be used in combination with IPsec and L2TP.

** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)

*** CKIP is not supported by 10xx APs

Radius Servers

Authentication Servers | Accounting Servers

Server 1: IP:172.16.1.60, Port:1812 | none

Done | Internet

Konfigurieren von Cisco Secure ACS

Auf dem Cisco Secure ACS-Server müssen Sie:

1. Konfigurieren Sie den WLC als AAA-Client.
2. Erstellen Sie die Benutzerdatenbank und definieren Sie NAR für die SSID-basierte Authentifizierung.
3. Aktivieren Sie die EAP-Authentifizierung.

Gehen Sie wie folgt vor:

1. Um den Controller als AAA-Client auf dem ACS-Server zu definieren, klicken Sie in der ACS-GUI auf **Netzwerkkonfiguration**. Klicken Sie unter AAA-Clients auf **Add Entry (Eintrag hinzufügen)**.

CISCO SYSTEMS Network Configuration

Select

AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
None Defined		

Add Entry Search













AAA Servers

AAA Server Name	AAA Server IP Address	AAA Server Type
tswab-laptop	127.0.0.1	CiscoSecure ACS

Add Entry Search


Back to Help

2. 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).

-  User Setup
-  Group Setup
-  Shared Profile Components
-  Network Configuration
-  System Configuration
-  Interface Configuration
-  Administration Control
-  External User Databases
-  Posture Validation
-  Network Access Profiles
-  Reports and Activity
-  Online Documentation

Add AAA Client

AAA Client Hostname	<input type="text" value="WLC"/>
AAA Client IP Address	<input type="text" value="172.16.1.30"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="RADIUS (Cisco Airespace)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	

 [Back to Help](#)

3. Klicken Sie in der ACS-GUI auf **User Setup** (Benutzereinrichtung), geben Sie den Benutzernamen ein, und klicken Sie auf **Hinzufügen/Bearbeiten**. In diesem Beispiel ist der Benutzer A1.
4. 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 für die LEAP-Authentifizierung benötigen.

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

User: A1 (New User)

Account Disabled

Supplementary User Info

Real Name

Description

User Setup

Password Authentication:

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

5. Blättern Sie auf der Seite für die Benutzereinrichtung nach unten, bis der Abschnitt Netzwerkzugriffsbeschränkungen angezeigt wird. Wählen Sie unter "User Interface of DNIS/CLI Access Restriction" (Benutzerschnittstelle der Zugriffseinschränkung für DNIS/CLI) die Option **Permitted Calling/Point of Access Locations (Zulässige Anrufe/Zugangspunkte) aus**, und definieren Sie folgende Parameter:**AAA-Client** - WLC-IP-Adresse (in unserem Beispiel 172.16.1.30)**Port** -*CLI -*DNIS -*ssidname
6. Das DNIS-Attribut definiert die SSID, auf die der Benutzer zugreifen darf. Der WLC sendet die SSID im DNIS-Attribut an den RADIUS-Server. Wenn der Benutzer nur auf das WLAN mit dem Namen Admin zugreifen muss, geben Sie ***Admin** für das Feld DNIS ein. Dadurch wird sichergestellt, dass der Benutzer nur auf das WLAN Admin zugreifen kann. Klicken Sie auf **Eingabe.Hinweis**: Der SSID sollte immer * vorangestellt werden. Es ist obligatorisch.

Advanced Settings

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

Network Access Restrictions (NAR) ?

Per User Defined Network Access Restrictions

Define IP-based access restrictions

Table Defines: Permitted Calling/Point of Access Locations

AAA Client	Port	Address
remove		

AAA Client: All AAA Clients

Port:

Address:

enter

Define CLI/DNIS-based access restrictions

Table Defines: Permitted Calling/Point of Access Locations

AAA Client	Port	CLI	DNIS
remove			

AAA Client: WLC

Port:

CLI:

DNIS:

enter

Submit
Cancel

7. Klicken Sie auf **Senden**.

8. Erstellen Sie entsprechend einen Benutzer für den Benutzer der Vertriebsabteilung. Hier sind die Screenshots.



User Setup

Edit

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

User: S1 (New User)

Account Disabled

Supplementary User Info

Real Name
Description

User Setup

Password Authentication:

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

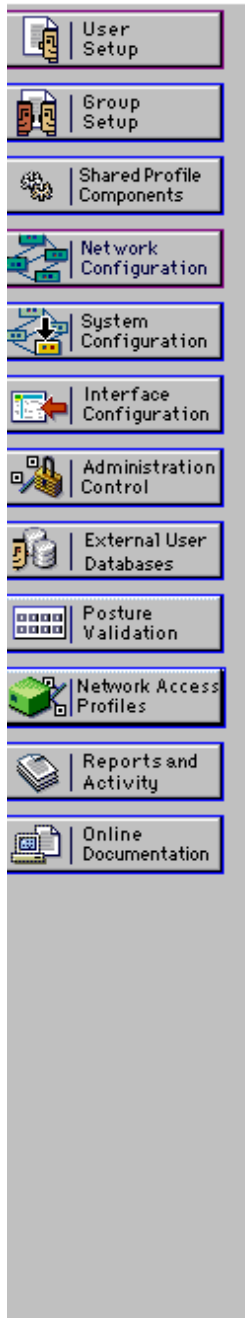
Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:



Network Access Restrictions (NAR) ?

Per User Defined Network Access Restrictions

Define IP-based access restrictions

Table Defines: Permitted Calling/Point of Access Locations

AAA Client	Port	Address

remove

AAA Client: All AAA Clients

Port:

Address:

enter

Define CLI/DNIS-based access restrictions

Table Defines: Permitted Calling/Point of Access Locations

AAA Client	Port	CLI	DNIS

remove

AAA Client: WLC

Port: *

CLI: *

DNIS: *Sales

enter

Submit
Cancel

9. Wiederholen Sie den gleichen Vorgang, um der Datenbank weitere Benutzer hinzuzufügen. **Hinweis:** Standardmäßig sind alle Benutzer der Standardgruppe zugeordnet. Wenn Sie bestimmte Benutzer verschiedenen Gruppen zuweisen möchten, lesen Sie den Abschnitt [Benutzergruppenverwaltung](#) im [Benutzerhandbuch für Cisco Secure ACS für Windows Server 3.2](#). **Hinweis:** Wenn der Abschnitt "Network Access Restrictions" (Netzwerkzugriffsbeschränkungen) im Fenster "User Setup" (Benutzereinrichtung) nicht angezeigt wird, ist er möglicherweise nicht aktiviert. Um die Netzwerkzugriffsbeschränkungen für Benutzer zu aktivieren, wählen Sie in der ACS-GUI **Interfaces > Advanced Options** (Schnittstellen > Erweiterte Optionen) aus, wählen Sie **User-Level Network Access Restrictions (Netzwerkzugriffsbeschränkungen auf Benutzerebene)** aus, und klicken Sie auf **Submit (Senden)**. Dies aktiviert das NAR und wird im Fenster User Setup (Benutzereinrichtung) angezeigt.



Interface Configuration

Edit

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

Advanced Options

Note: Only the selected options will appear in the user interface.

- Per-user TACACS+/RADIUS Attributes
- User-Level Shared Network Access Restrictions
- User-Level Network Access Restrictions
- User-Level Downloadable ACLs
- Default Time-of-Day / Day-of-Week Specification
- Group-Level Shared Network Access Restrictions
- Group-Level Network Access Restrictions
- Group-Level Downloadable ACLs
- Group-Level Password Aging
- Network Access Filtering
- Max Sessions
- Usage Quotas
- Distributed System Settings
- Remote Logging
- ACS internal database Replication
- RDBMS Synchronization
- IP Pools
- Network Device Groups
- Voice-over-IP (VoIP) Group Settings
- Voice-over-IP (VoIP) Accounting Configuration
- ODBC Logging

Submit

Cancel

Advanced Settings

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

Network Access Restrictions (NAR) ?

Per User Defined Network Access Restrictions

Define IP-based access restrictions

Table Defines : Permitted Calling/Point of Access Locations

AAA Client	Port	Address
remove		

AAA Client All AAA Clients

Port

Address

enter

Define CLI/DNIS-based access restrictions

Table Defines : Permitted Calling/Point of Access Locations

AAA Client	Port	CLI	DNIS
remove			

AAA Client WLC

Port *













CLI *

DNIS *Admin

enter

Submit
Cancel

10. Um die EAP-Authentifizierung zu aktivieren, klicken Sie auf **Systemkonfiguration** und **Global Authentication 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**.

-  User Setup
-  Group Setup
-  Shared Profile Components
-  Network Configuration
-  System Configuration
-  Interface Configuration
-  Administration Control
-  External User Databases
-  Posture Validation
-  Network Access Profiles
-  Reports and Activity
-  Online Documentation

Global Authentication Setup

?

EAP Configuration

PEAP

Allow EAP-MSCHAPv2

Allow EAP-GTC

Allow Posture Validation

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

EAP-FAST

[EAP-FAST Configuration](#)

EAP-TLS

Allow EAP-TLS

Select one or more of the following options:

Certificate SAN comparison

Certificate CN comparison

Certificate Binary comparison

EAP-TLS session timeout (minutes):

LEAP

Allow LEAP (For Aironet only)

EAP-MD5

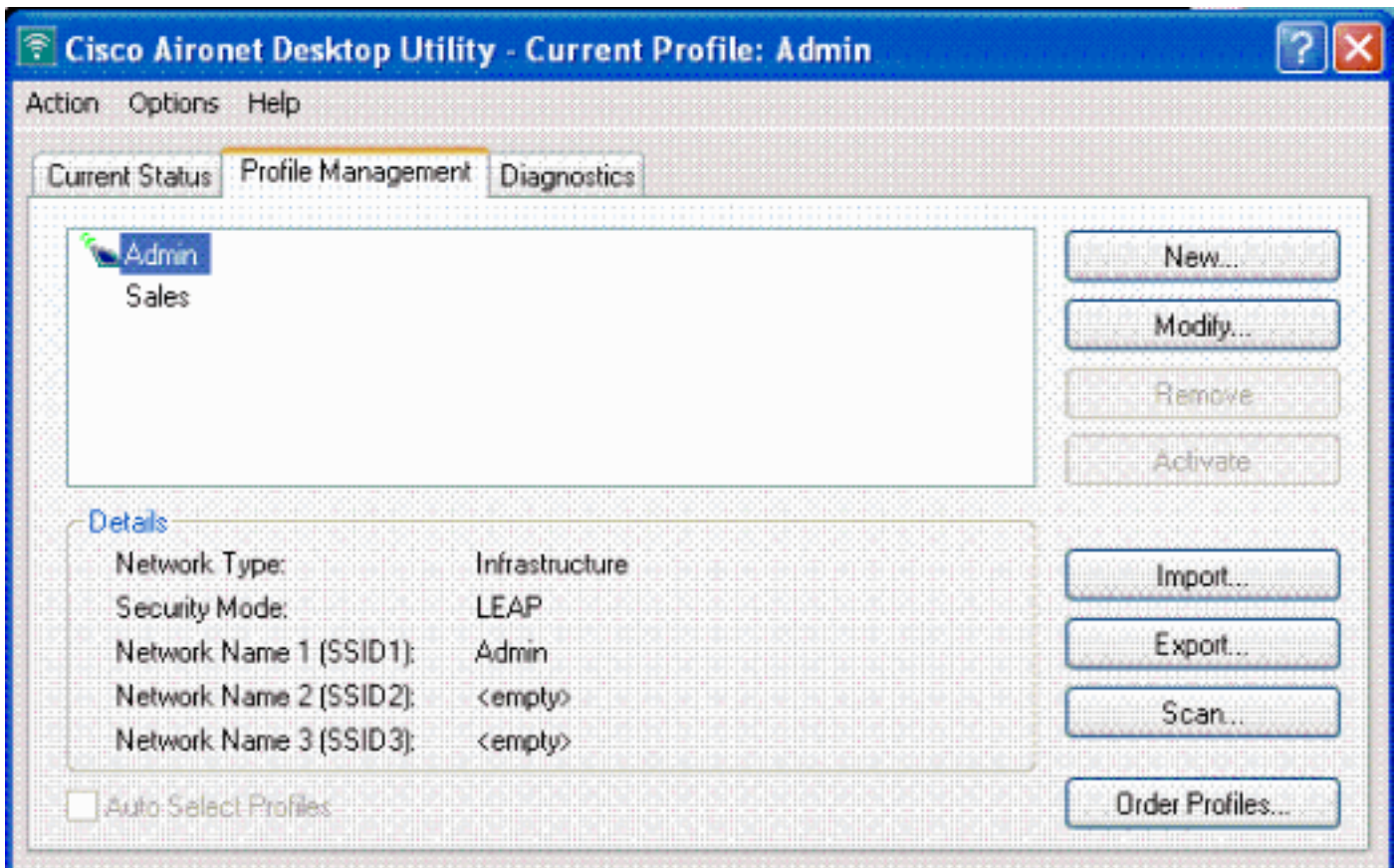
Submit
Submit + Restart
Cancel

Konfigurieren des Wireless-Clients und Überprüfen

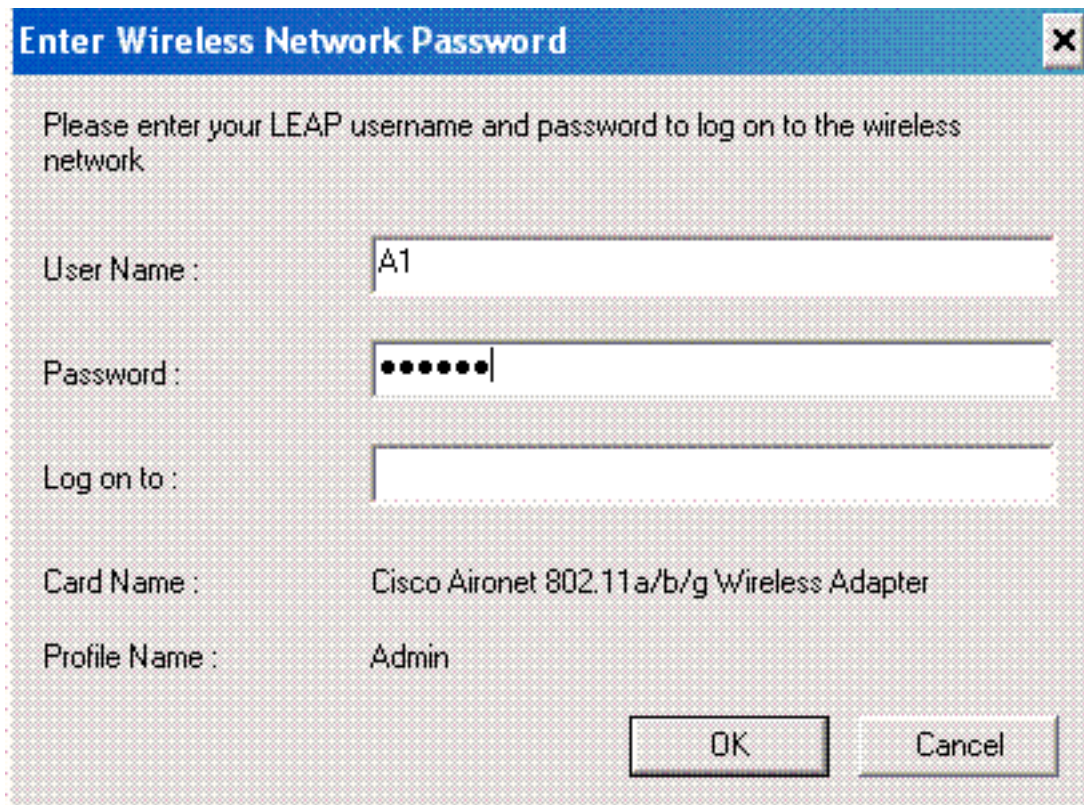
In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert. Versuchen Sie, mithilfe der LEAP-Authentifizierung einen Wireless-Client mit der LAP zu verknüpfen, um zu überprüfen, ob die Konfiguration wie erwartet funktioniert.

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](#).

Hinweis: Auf der ADU sehen Sie, dass Sie zwei Clientprofile konfiguriert haben. Eines für die Benutzer der Admin-Abteilung mit SSID **Admin** und das andere Profil für die Benutzer der Vertriebsabteilung mit SSID **Sales**. Beide Profile sind für die LEAP-Authentifizierung konfiguriert.



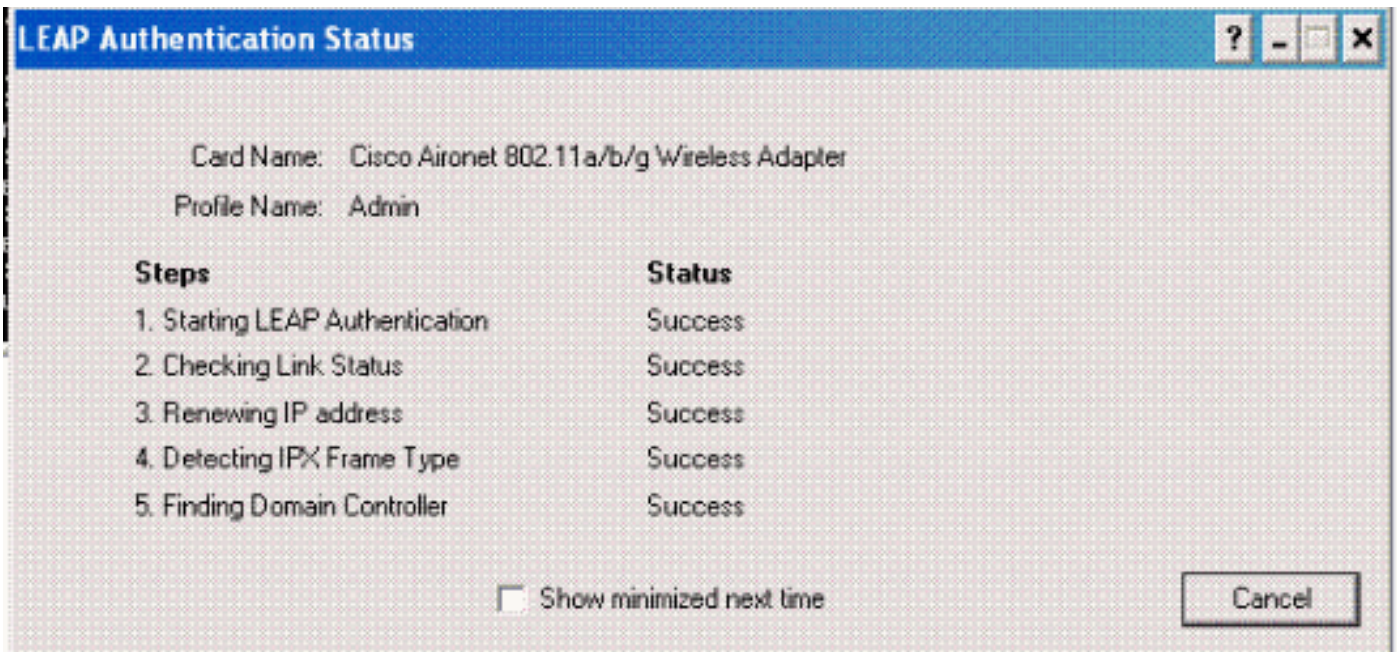
Wenn das Profil des Wireless-Benutzers aus der Admin-Abteilung aktiviert ist, wird der Benutzer aufgefordert, den Benutzernamen/das Kennwort für die LEAP-Authentifizierung einzugeben. Hier ein Beispiel:



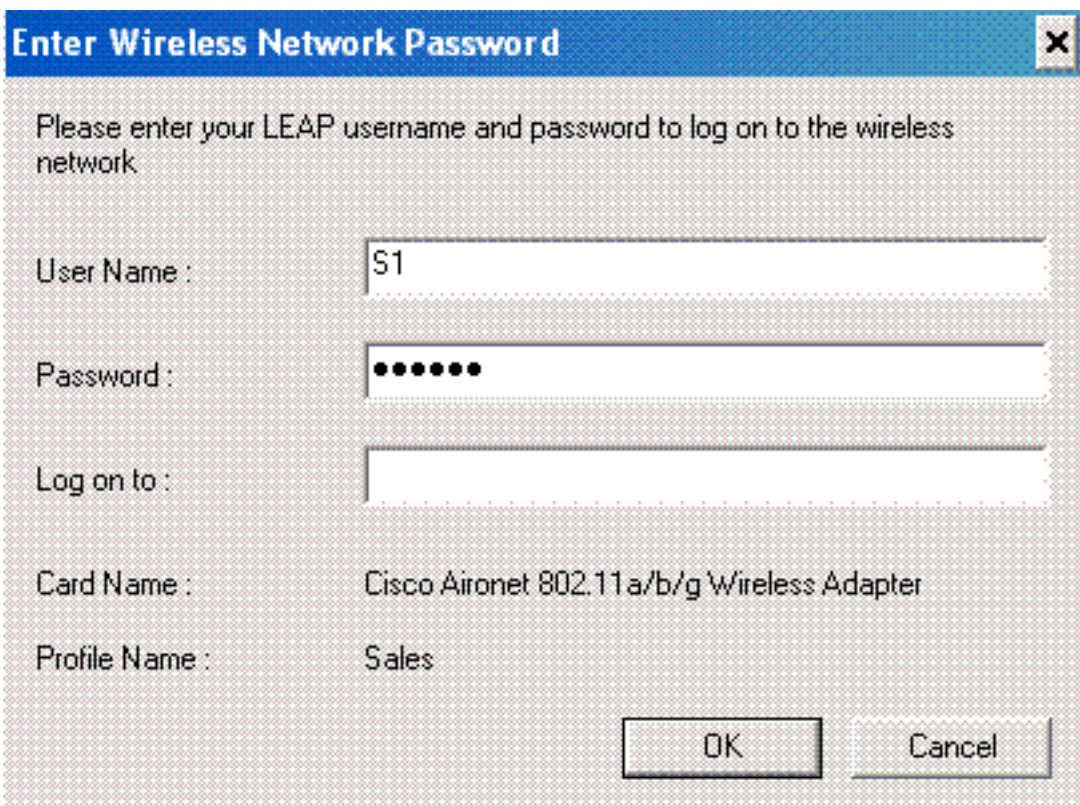
Die LAP und anschließend der WLC geben die Benutzeranmeldeinformationen an den externen RADIUS-Server (Cisco Secure ACS) weiter, um die Anmeldeinformationen zu validieren. Der WLC übergibt die Anmeldeinformationen einschließlich des DNIS-Attributs (SSID-Name) zur Validierung an den RADIUS-Server.

Der RADIUS-Server überprüft die Benutzeranmeldeinformationen, indem er die Daten mit der Benutzerdatenbank (und den NARs) vergleicht und bei Gültigkeit der Benutzeranmeldeinformationen Zugriff auf den Wireless-Client gewährt.

Nach erfolgreicher RADIUS-Authentifizierung ordnet der Wireless-Client der LAP zu.



Wenn ein Benutzer aus der Vertriebsabteilung das Vertriebsprofil aktiviert, wird der Benutzer vom RADIUS-Server anhand des LEAP-Benutzernamens/Kennworts und der SSID authentifiziert.



Der Bericht über die vergebene Authentifizierung auf dem ACS-Server zeigt, dass der Client die RADIUS-Authentifizierung (EAP-Authentifizierung und SSID-Authentifizierung) bestanden hat. Hier ein Beispiel:

Reports and Activity

Select

Passed Authentications active.csv Refresh Download

Regular Expression Start Date & Time End Date & Time Rows per Page

Apply Filter Clear Filter

Filtering is not applied.

Date ↓	Time	Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port	NAS-IP-Address	Network Access Profile Name	Shared BAC	Downloadable ACL	System-Posture-Token	Application-Posture-Token	Reason	EAP Type	EAP Type Name
10/11/2006	14:48:40	Authen OK	S1	Default Group	00-40-9E-9E-57	1	172.16.1.30	(Default)	17	LEAP
10/11/2006	14:47:05	Authen OK	A1	Default Group	00-40-9E-9E-57	1	172.16.1.30	(Default)	17	LEAP

Wenn der Sales User jetzt versucht, auf die **Admin-SSID** zuzugreifen, verweigert der RADIUS-Server dem Benutzer den Zugriff auf das WLAN. Hier ein Beispiel:



Auf diese Weise kann der Zugriff für Benutzer auf Basis der SSID eingeschränkt werden. In einer N-Unternehmensumgebung können alle Benutzer, die einer bestimmten Abteilung angehören, in einer einzigen Gruppe zusammengefasst werden. Der Zugriff auf das WLAN kann auf der Grundlage der SSID bereitgestellt werden, die sie verwenden, wie in diesem Dokument erläutert.

Fehlerbehebung

Befehle zur Fehlerbehebung

Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe** des Befehls **show** anzuzeigen.

Hinweis: Beachten Sie [vor der](#) Verwendung von **Debug**-Befehlen die [Informationen](#) zu [Debug-Befehlen](#).

- **debug dot1x aaa enable:** Aktiviert das Debuggen von 802.1x-AAA-Interaktionen.
- **debug dot1x packet enable:** Aktiviert das Debuggen aller dot1x-Pakete.

- **debug aaa all enable**: Konfiguriert das Debuggen aller AAA-Meldungen.

Sie können zur Fehlerbehebung auch den Bericht für die Authentifizierung nach bestandener Authentifizierung und den Bericht für fehlgeschlagene Authentifizierung auf dem Cisco Secure ACS-Server verwenden. Diese Berichte werden im Fenster **Berichte und Aktivität** in der ACS-GUI angezeigt.

Zugehörige Informationen

- [Konfigurationsbeispiel für EAP-Authentifizierung mit WLAN-Controllern \(WLC\)](#)
- [Konfigurationsbeispiel für die Webauthentifizierung des Wireless LAN-Controllers](#)
- [Konfigurationsbeispiel für AP-Gruppen-VLANs mit Wireless LAN-Controllern](#)
- [Wireless-Support-Seite](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)