

使用WLC和Cisco Secure ACS配置示例根據SSID限制WLAN訪問

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[背景資訊](#)

[網路設定](#)

[設定](#)

[設定WLC](#)

[配置Cisco Secure ACS](#)

[配置無線客戶端並驗證](#)

[疑難排解](#)

[疑難排解指令](#)

[相關資訊](#)

簡介

本檔案將提供基於服務組識別碼(SSID)限制每使用者存取WLAN的組態範例。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 瞭解如何設定無線LAN控制器(WLC)和輕量型存取點(LAP)以達成基本操作
- 有關如何配置思科安全訪問控制伺服器(ACS)的基本知識
- 輕量型存取點通訊協定(LWAPP)和無線安全方法知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行韌體4.0的Cisco 2000系列WLC
- Cisco 1000系列LAP
- Cisco安全ACS伺服器版本3.2

- 執行韌體2.6的Cisco 802.11a/b/g無線使用者端配接器
- Cisco Aironet案頭公用程式(ADU)版本2.6

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

背景資訊

使用基於SSID的WLAN訪問時，可以根據使用者用於連線到WLAN的SSID對其進行身份驗證。Cisco Secure ACS伺服器用於對使用者進行身份驗證。身份驗證在Cisco Secure ACS上分兩個階段進行：

1. EAP身份驗證
2. Cisco Secure ACS上基於網路訪問限制(NAR)的SSID身份驗證

如果基於EAP和SSID的身份驗證成功，則允許使用者訪問WLAN，否則將取消使用者關聯。

Cisco Secure ACS使用NAR功能根據SSID限制使用者訪問。NAR是在思科安全ACS中設定的定義，其中定義了在使用者訪問網路之前必須滿足的其他條件。Cisco Secure ACS使用來自AAA客戶端傳送的屬性的資訊應用這些條件。雖然有多種方法可以設定NAR，但它們都基於AAA客戶端傳送的匹配屬性資訊。因此，如果要使用有效的NAR，您必須瞭解AAA客戶端傳送的屬性的格式和內容。

設定NAR時，您可以選擇過濾器是執行正值還是負值。也就是說，在NAR中，您根據從AAA客戶端傳送的資訊與NAR中儲存的資訊之間的比較來指定是允許還是拒絕網路訪問。但是，如果NAR沒有獲得足夠的資訊來運行，則預設設定為拒絕訪問。

您可以為特定使用者或使用者組定義NAR並將其應用於特定使用者或使用者組。有關詳細資訊，請參閱[網路訪問限制白皮書](#)。

Cisco Secure ACS支援兩種型別的NAR過濾器：

1. **基於IP的過濾器** — 基於IP的NAR過濾器根據終端使用者客戶端和AAA客戶端的IP地址限制訪問。有關此類NAR過濾器的詳細資訊，請參閱[關於基於IP的NAR過濾器](#)。
2. **非基於IP的過濾器** — 非基於IP的NAR過濾器基於從AAA客戶端傳送的值的簡單字串比較來限制訪問。該值可以是主叫線路ID(CLI)號碼、被叫號碼識別服務(DNIS)號碼、MAC地址或從客戶端發出的其他值。為了使此型別的NAR運行，NAR描述中的值必須與從客戶端傳送的内容完全匹配，包括所使用的任何格式。例如，(217)555-4534與217-555-4534不匹配。有關此型別的NAR過濾器的詳細資訊，請參閱[關於非基於IP的NAR過濾器](#)。

本文檔使用非IP過濾器執行基於SSID的身份驗證。非基於IP的NAR過濾器 (即基於DNIS/CLI的NAR過濾器) 是允許或拒絕的呼叫/接入點位置的清單，當您沒有已建立的基於IP的連線時，可以在AAA客戶端的限制中使用這些位置。非基於IP的NAR功能通常使用CLI編號和DNIS編號。DNIS/CLI欄位的使用存在異常。您可以在DNIS欄位中輸入SSID名稱，並執行基於SSID的身份驗證。這是因為WLC會將DNIS屬性 (SSID名稱) 傳送到RADIUS伺服器。因此，如果在使用者或組中構建DNIS NAR，則可以建立每使用者SSID限制。

如果使用RADIUS，此處列出的NAR欄位使用以下值：

- **AAA客戶端** — 使用NAS-IP-address (屬性4) 或NAS-IP-address (如果NAS-IP-address不存

在)，使用NAS-identifier (RADIUS屬性32)。

- **Port** — 使用NAS埠 (屬性5)，如果沒有NAS埠，則使用NAS埠ID (屬性87)。
- **CLI** — 使用呼叫站ID (屬性31)。
- **DNIS** — 使用被叫站ID (屬性30)。

有關NAR用法的詳細資訊，請參閱[網路訪問限制](#)。

由於WLC會傳入DNIS屬性和SSID名稱，因此您可以建立每個使用者的SSID限制。若是WLC，NAR欄位具有以下值：

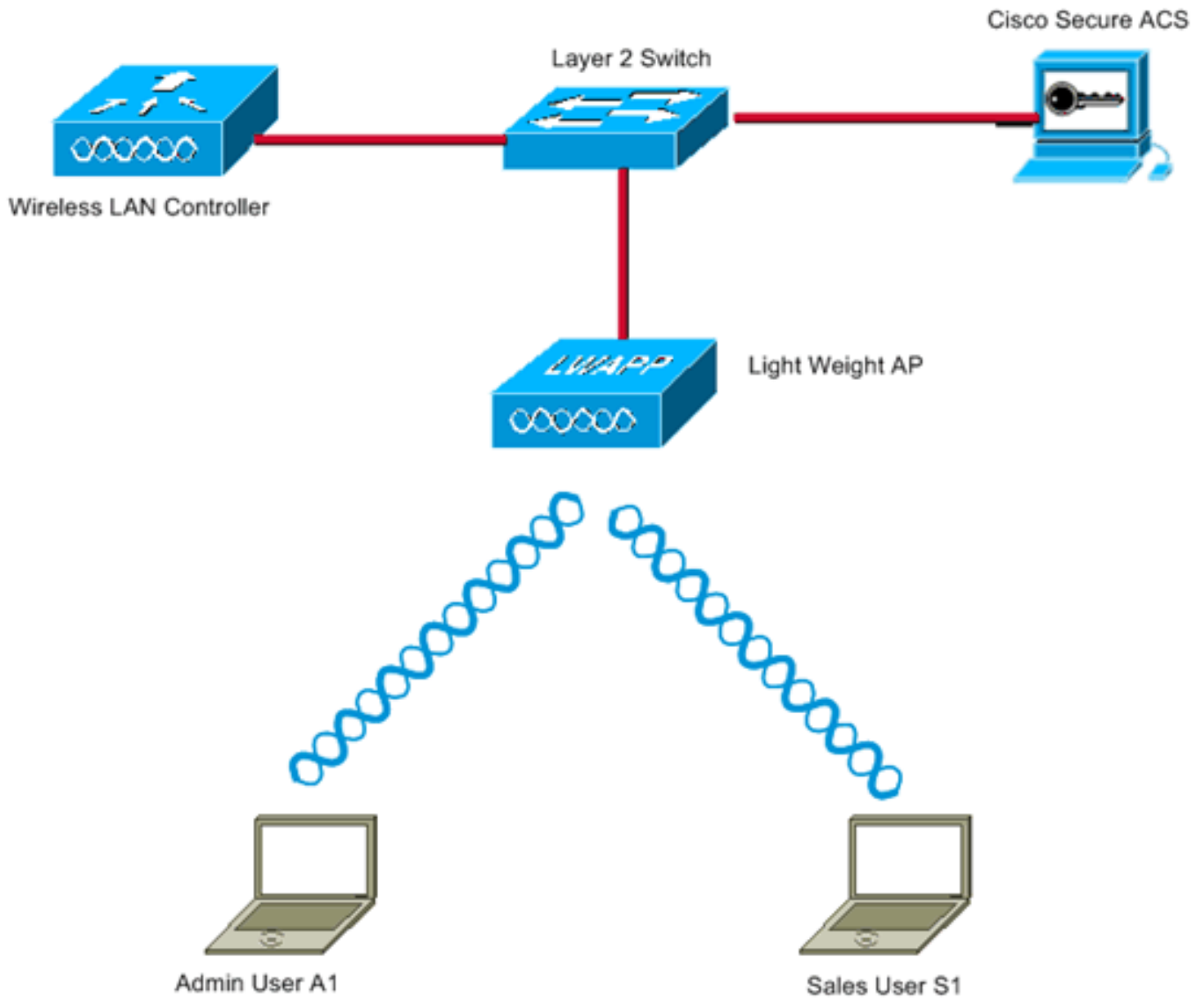
- **AAA客戶端** — WLC IP地址
- **埠**—*
- **CLI** —*
- **DNIS** -*ssidname

本文的其餘部分提供了有關如何完成此操作的配置示例。

[網路設定](#)

在此範例設定中，WLC已註冊到LAP。使用兩個WLAN。一個WLAN用於管理部門使用者，另一個WLAN用於銷售部門使用者。無線客戶端A1 (管理員使用者) 和S1 (銷售使用者) 連線到無線網路。您需要設定WLC和RADIUS伺服器，以使Admin使用者A1隻能存取WLAN **Admin**，且限制存取WLAN **Sales**的權利，而Sales使用者S1應該能夠存取WLAN **Sales**，且應該限制存取WLAN **Admin**。所有使用者都使用LEAP身份驗證作為第2層身份驗證方法。

注意：本檔案假設WLC已註冊到控制器。如果您不熟悉WLC，且不知道如何設定WLC以達成基本操作，請參閱[輕量AP\(LAP\)註冊到無線LAN控制器\(WLC\)](#)。



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

設定

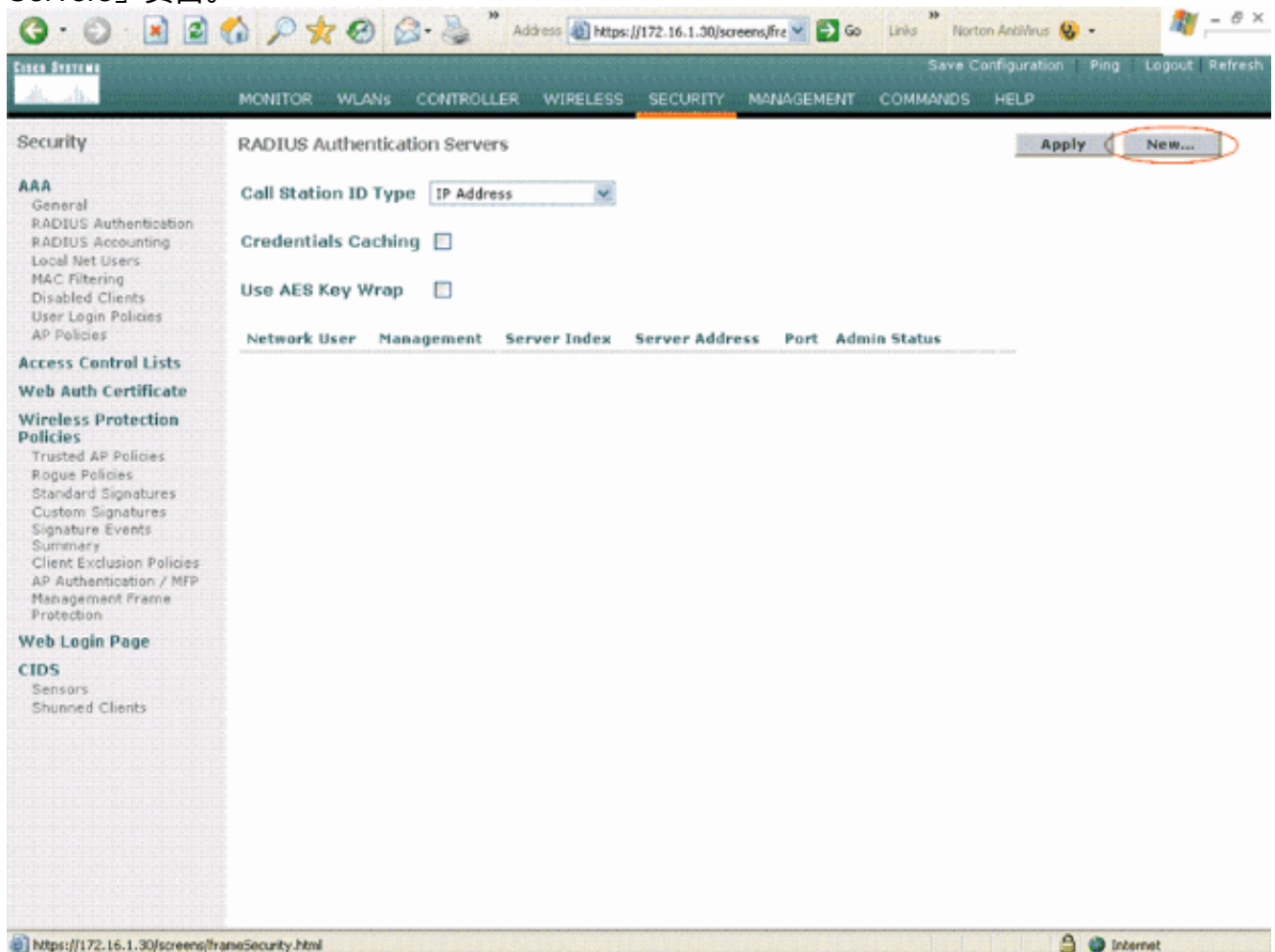
要為此設定配置裝置，您需要：

1. [為兩個WLAN和RADIUS伺服器配置WLC。](#)
2. [配置Cisco Secure ACS。](#)
3. [設定無線使用者端並進行驗證。](#)

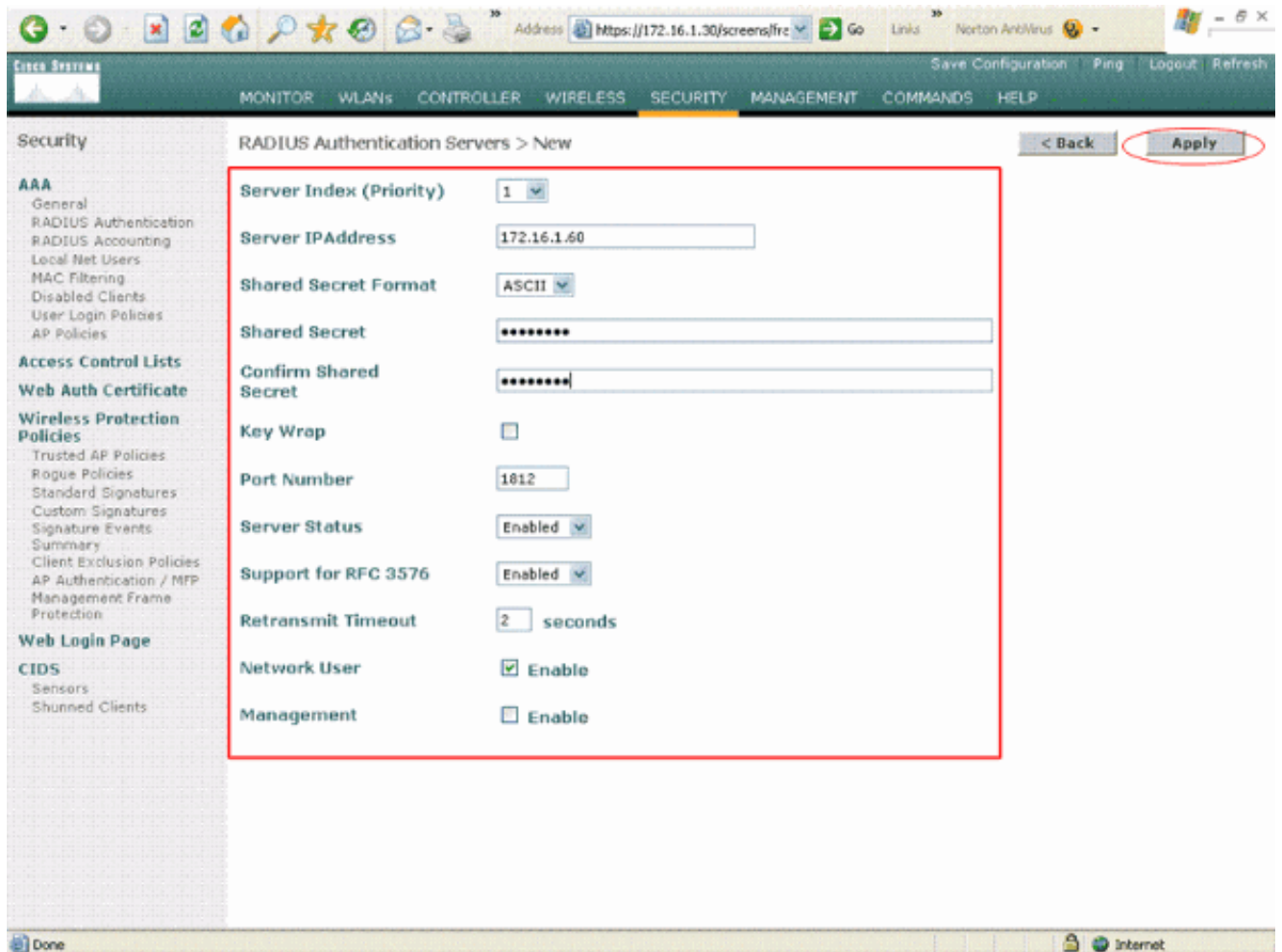
設定WLC

完成以下步驟，以便為此設定設定WLC:

1. 需要設定WLC以將使用者認證轉送到外部RADIUS伺服器。外部RADIUS伺服器 (此案例為思科安全ACS) 然後驗證使用者認證並提供對無線使用者端的存取許可權。請完成以下步驟：從控制器GUI中選擇**Security > RADIUS Authentication**，以顯示「RADIUS Authentication Servers」頁面。

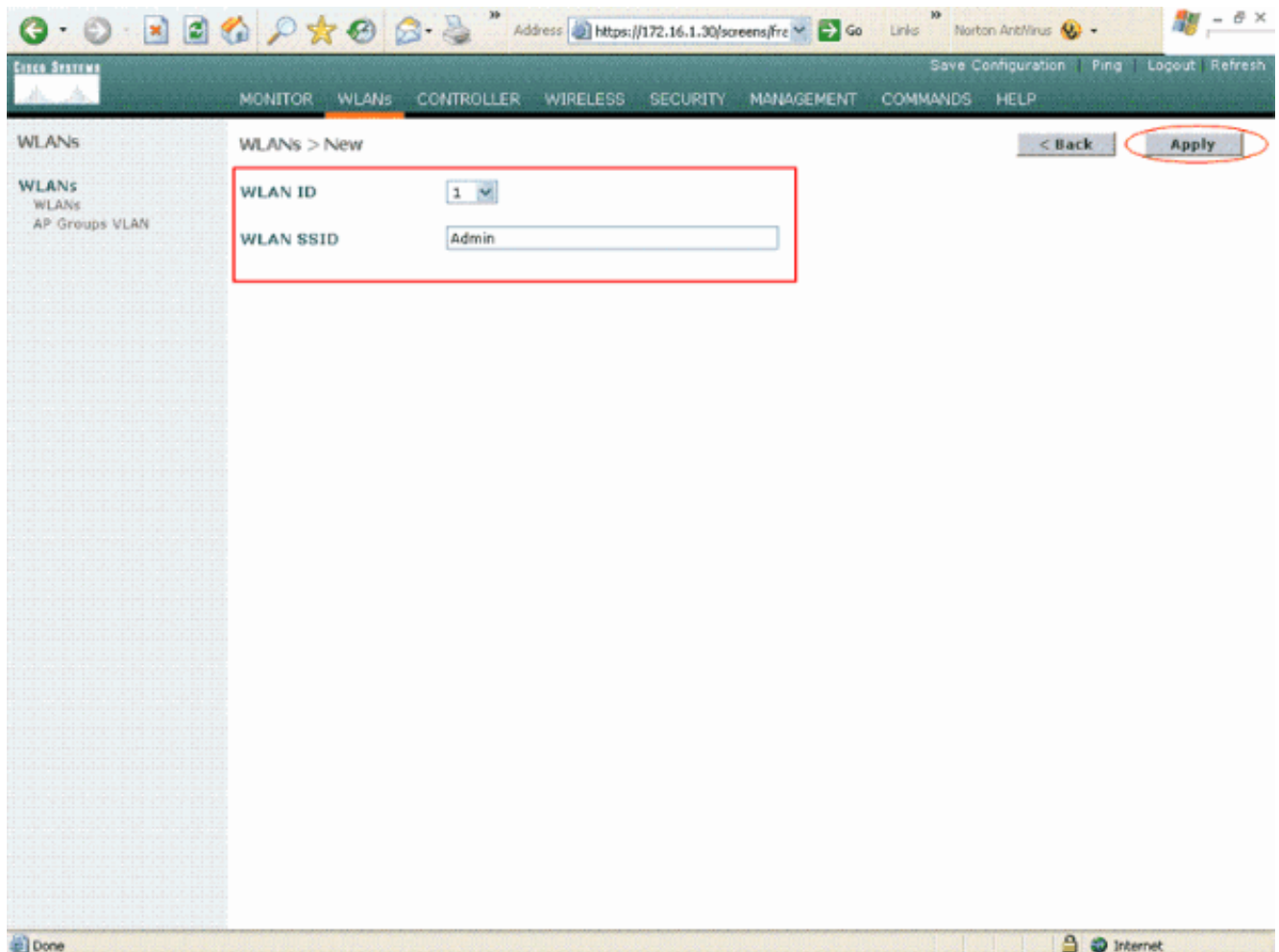


按一下「New」以定義RADIUS伺服器引數。這些引數包括RADIUS伺服器IP地址、共用金鑰、埠號和伺服器狀態。Network User和Management覈取方塊確定基於RADIUS的身份驗證是否適用於管理和網路使用者。此示例使用Cisco Secure ACS作為IP地址為172.16.1.60的RADIUS伺服器。

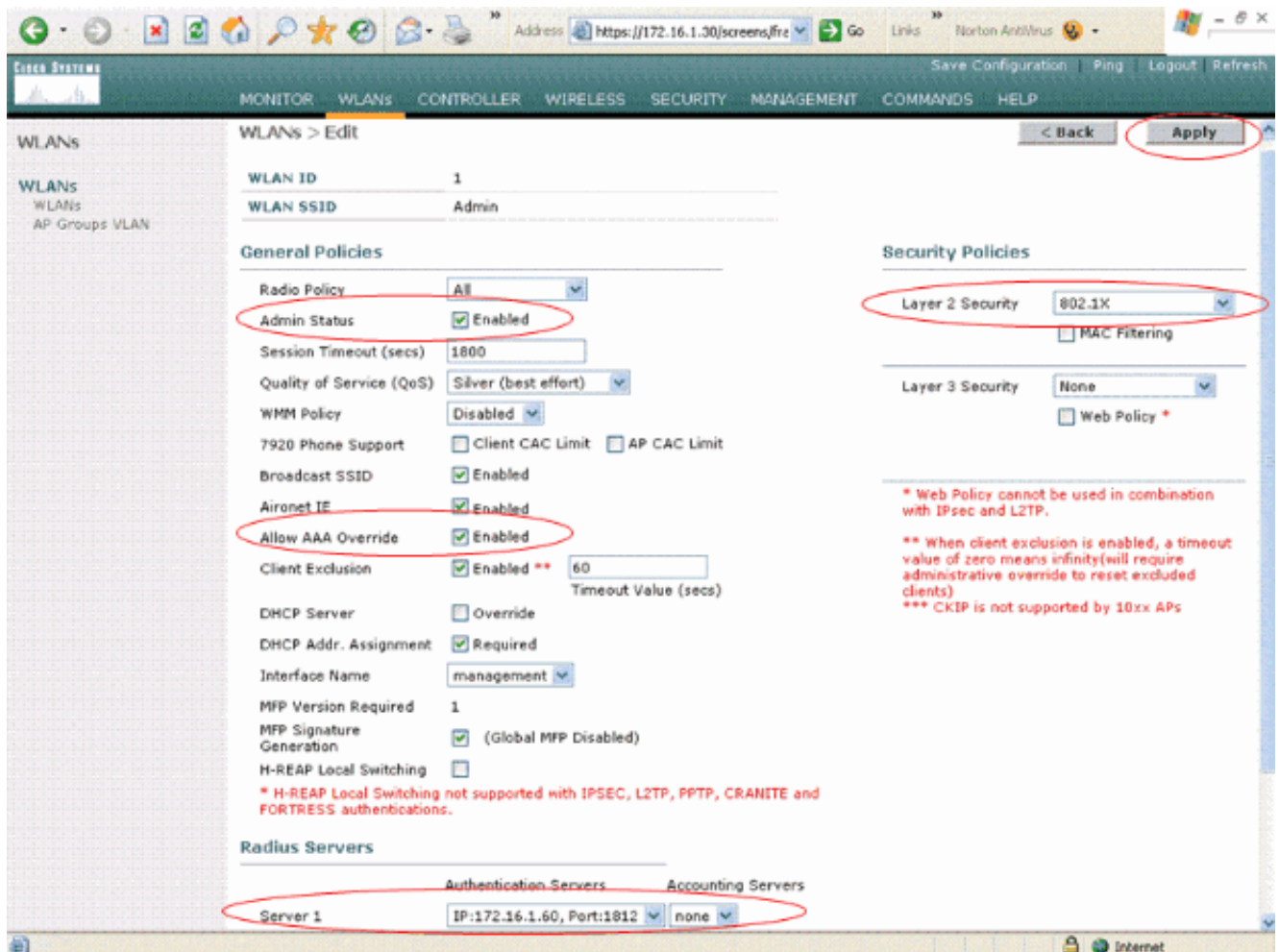


按一下「Apply」。

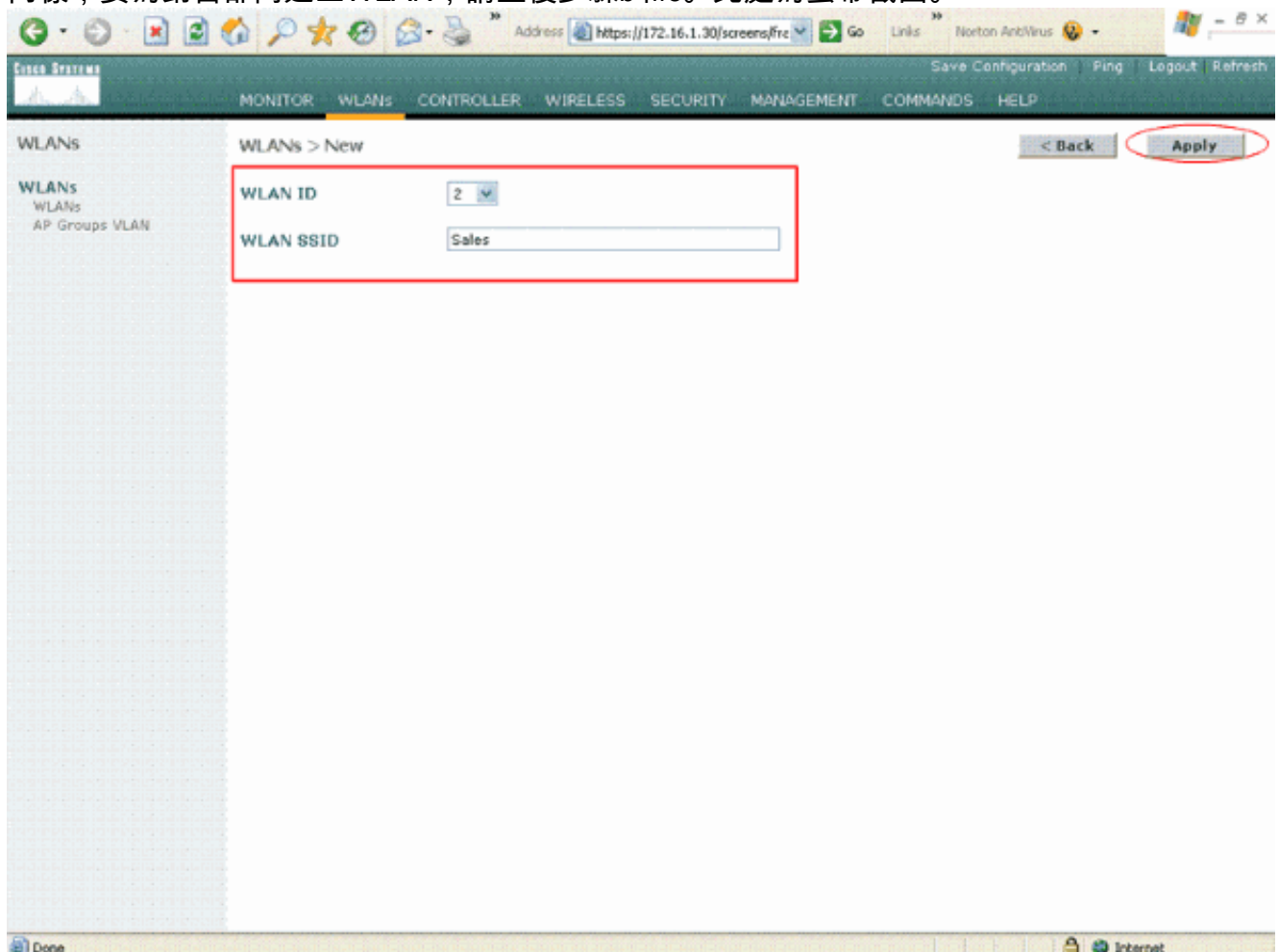
2. 為管理員部門配置一個WLAN(SSID **Admin**)，為銷售部門配置另一個WLAN(SSID **Sales**)。完成以下步驟即可完成此操作：在控制器GUI上按一下「**WLANs**」以建立WLAN。出現WLANs視窗。此視窗列出控制器上設定的WLAN。按一下**New**以設定新的WLAN。此示例為管理部門建立一個名為**Admin**的WLAN，WLAN ID為1。按一下**Apply**。

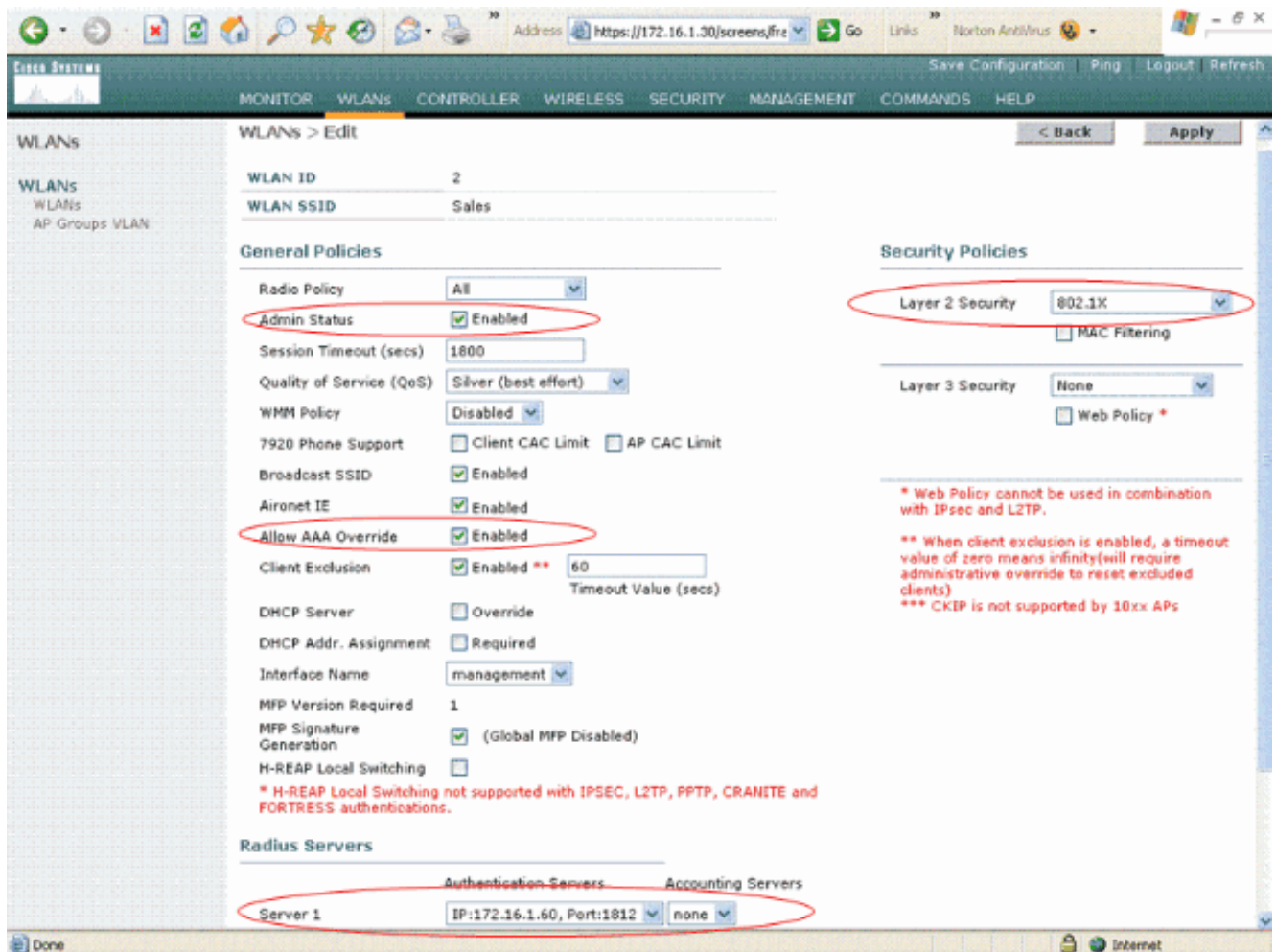


在「WLAN > Edit」視窗中，定義特定於WLAN的引數：從Layer 2 Security下拉選單中選擇802.1x。預設情況下，第2層安全選項為802.1x。這將為WLAN啟用802.1x/EAP身份驗證。在常規策略下，選中AAA override框。如果啟用AAA覆蓋，且客戶端的AAA和控制器WLAN身份驗證引數發生衝突，則客戶端身份驗證由AAA伺服器執行。從「RADIUS伺服器」下的下拉選單中選擇適當的RADIUS伺服器。其它引數可以根據WLAN網路的要求進行修改。按一下「Apply」。



同樣，要為銷售部門建立WLAN，請重複步驟b和c。此處為螢幕截圖。





配置Cisco Secure ACS

在Cisco Secure ACS伺服器上，您需要：

1. 將WLC配置為AAA客戶端。
2. 建立使用者資料庫並為基於SSID的身份驗證定義NAR。
3. 啟用EAP身份驗證。

在Cisco Secure ACS上完成以下步驟：

1. 若要將控制器定義為ACS伺服器上的AAA客戶端，請在ACS GUI上按一下**Network Configuration**。在AAA客戶端下，按一下**Add Entry**。



Network Configuration

Select

- 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

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

- 顯示「網路組態」頁面時，定義WLC的名稱、IP位址、共用密碼和驗證方法(RADIUS Cisco Airespace)。

- 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

- 在ACS GUI中按一下**User Setup**，輸入使用者名稱，然後按一下**Add/Edit**。在此範例中，使用者為A1。
- 出現「使用者設定」頁時，定義特定於使用者的所有引數。在本示例中，由於您需要這些引數進行LEAP身份驗證，因此配置使用者名稱、密碼和附加使用者資訊。

- 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. 向下滾動「使用者設定」頁面，直到看到網路訪問限制部分。在DNIS/CLI Access Restriction (DNIS/CLI訪問限制) 的使用者介面下，選擇**Permitted Calling/Point of Access Locations**，並定義以下引數：**AAA使用者端** — WLC IP位址 (在我們的範例中為 172.16.1.30) 埠—*CLI—*DNIS -*ssidname
6. DNIS屬性定義允許使用者訪問的SSID。WLC將DNIS屬性中的SSID傳送到RADIUS伺服器。如果使用者只需要訪問名為Admin的WLAN，請在DNIS欄位中輸入*Admin。這可確保使用者只能訪問名為Admin的WLAN。按一下「Enter」。註：SSID的前面應始終為*。」這是強制性的。

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. 按一下「Submit」。

8. 同樣，為銷售部門使用者建立一個使用者。這是螢幕截圖。



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:

- 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: *Sales

enter

Submit
Cancel

9. 重複相同的過程，向資料庫新增更多使用者。**注意：**預設情況下，所有使用者都分組在預設組下。如果要將特定使用者分配給不同的組，請參閱[適用於Windows Server 3.2的Cisco Secure ACS使用手冊](#)的**使用者組管理**部分。**附註：**如果在「使用者設定」視窗中未看到「網路訪問限制」部分，則可能是因為未啟用該部分。要為使用者啟用「網路訪問限制」，請從ACS GUI中選擇**Interfaces > Advanced Options**，選擇**User-Level Network Access Restrictions**，然後按一下**Submit**。這將啟用NAR並顯示在「使用者設定」視窗中。



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. 要啟用EAP身份驗證，請按一下**System Configuration**和**Global Authentication Setup**，以確保身份驗證伺服器配置為執行所需的EAP身份驗證方法。在EAP配置設定下，選擇適當的EAP方法。此示例使用LEAP身份驗證。完成後按一下**Submit**。

-  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

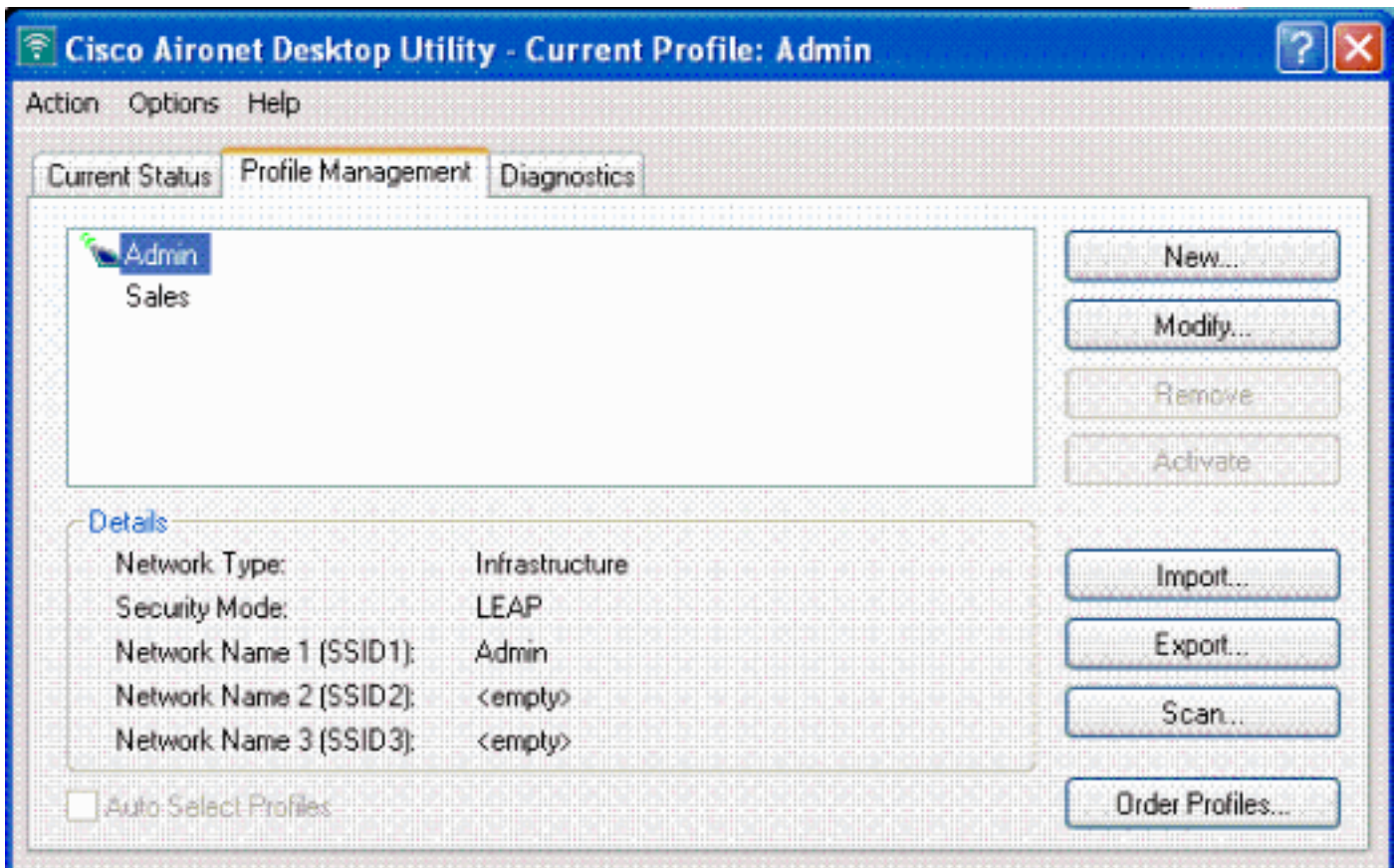
配置無線客戶端並驗證

使用本節內容，確認您的組態是否正常運作。嘗試使用LEAP身份驗證將無線客戶端與LAP關聯以驗證配置是否按預期工作。

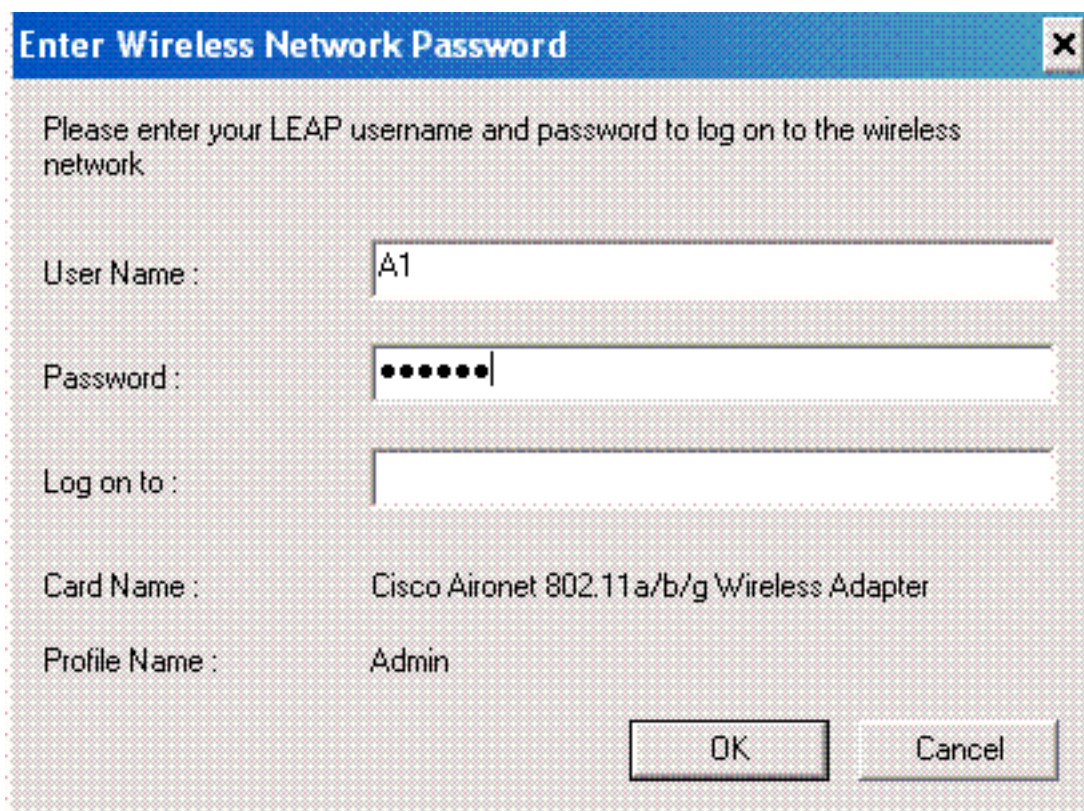
注意：本文檔假定客戶端配置檔案已配置為LEAP身份驗證。有關如何為LEAP身份驗證配置802.11 a/b/g無線客戶端介面卡的資訊，請參閱[使用EAP身份驗證](#)。

注意：從ADU中，您可以看到您已配置了兩個客戶端配置檔案。一個用於具有SSID **Admin**的管理部門使用者，另一個用於具有SSID **Sales**的銷售部門使用者。兩個配置檔案均配置為LEAP身份驗證

。



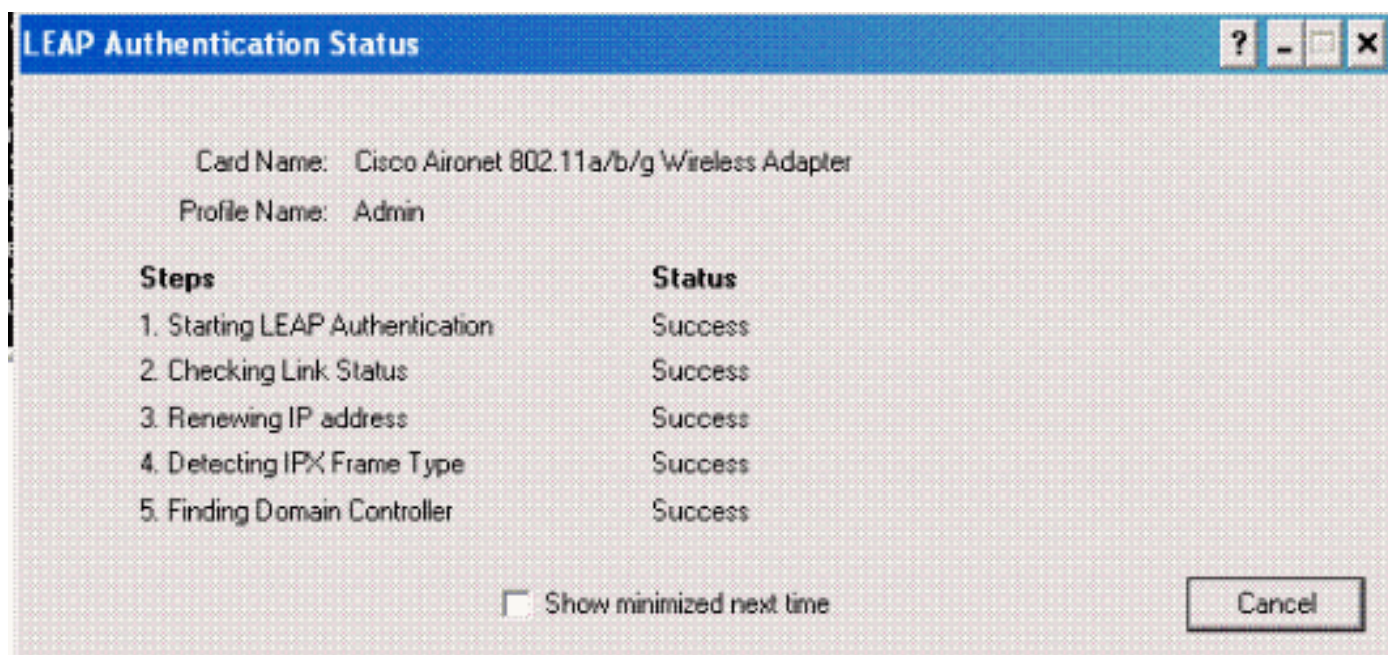
啟用管理部門的無線使用者配置檔案時，會要求使用者提供用於LEAP身份驗證的使用者名稱/密碼。以下是範例：



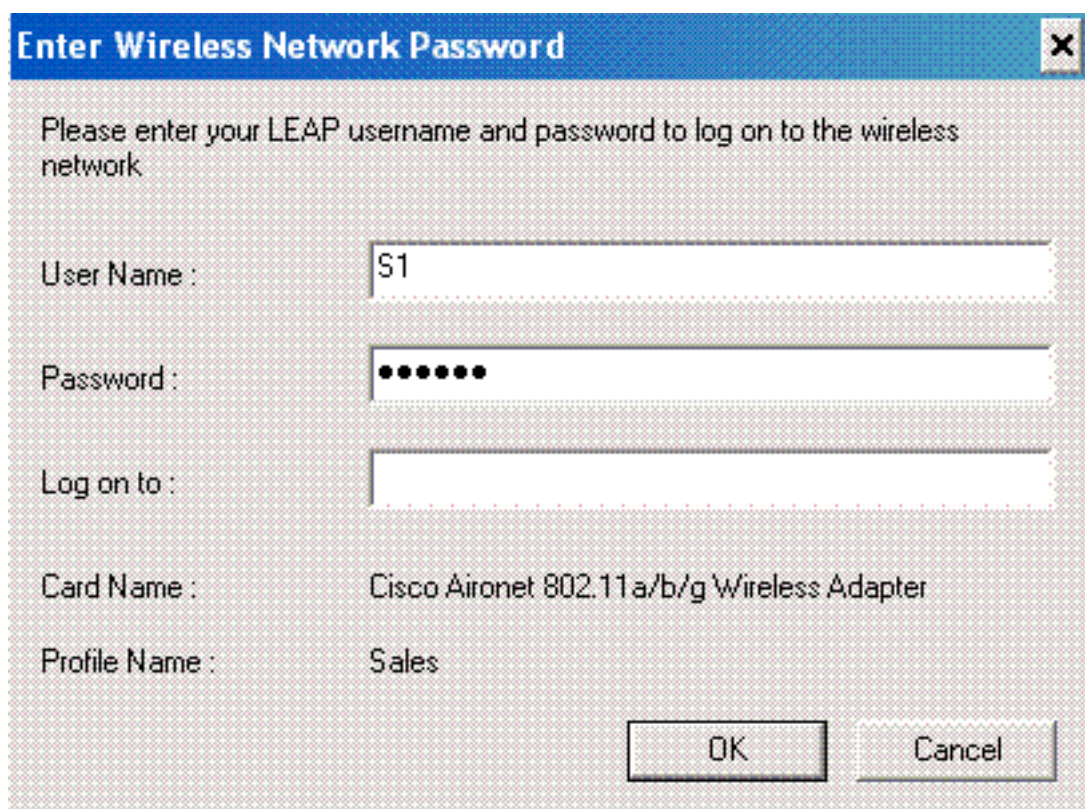
LAP和WLC將使用者憑證傳遞至外部RADIUS伺服器(Cisco Secure ACS)以驗證憑證。WLC會將包括DNIS屬性 (SSID名稱) 在內的憑證傳遞到RADIUS伺服器以進行驗證。

RADIUS伺服器會透過比較資料與使用者資料庫 (和NAR) 來驗證使用者認證，並在使用者認證有效時提供無線使用者端的存取許可權。

RADIUS驗證成功後，無線客戶端會與LAP關聯。



同樣，當銷售部門的使用者啟用銷售配置檔案時，RADIUS伺服器會根據LEAP使用者名稱/密碼和SSID對該使用者進行身份驗證。



ACS伺服器上的Passed Authentication報告顯示客戶端已通過RADIUS身份驗證（EAP身份驗證和SSID身份驗證）。以下是範例：

Reports and Activity

Select

Passed Authentications active.csv Refresh Download

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

mm/dd/yyyy, hh:mm:ss mm/dd/yyyy, hh:mm:ss 50

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-AC-E6-57	1	172.16.1.30	(Default)	17	LEAP
10/11/2006	14:47:05	Authen OK	A1	Default Group	00-40-9E-AC-E6-57	1	172.16.1.30	(Default)	17	LEAP

現在，如果銷售使用者嘗試訪問Admin SSID，RADIUS伺服器將拒絕使用者訪問WLAN。以下是範例：



這樣可以根據SSID限制使用者的訪問。在企業環境中，屬於特定部門的所有使用者可分為單個組，並且可以根據他們使用的SSID提供對WLAN的訪問許可權，如本文檔所述。

疑難排解

疑難排解指令

[輸出直譯器工具](#) (僅供已註冊客戶使用) (OIT) 支援某些show命令。使用OIT檢視show命令輸出的分析。

附註：使用 debug 指令之前，請先參閱[有關 Debug 指令的重要資訊](#)。

- debug dot1x aaa enable — 啟用802.1x AAA互動的調試。
- debug dot1x packet enable — 啟用所有dot1x資料包的調試。
- debug aaa all enable — 配置所有AAA消息的調試。

您還可以使用Cisco Secure ACS伺服器上的Passed Authentication報告和Failed Authentication報告

排除配置故障。這些報告位於ACS GUI上的**Reports and Activity**視窗中。

[相關資訊](#)

- [使用WLAN控制器\(WLC\)的EAP驗證組態範例](#)
- [無線 LAN 控制器 Web 驗證組態範例](#)
- [使用無線LAN控制器的AP組VLAN配置示例](#)
- [無線支援頁面](#)
- [技術支援與文件 - Cisco Systems](#)