

WLC と Cisco Secure ACS を使用した SSID に基づく WLAN アクセス制限の設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[ネットワークのセットアップ](#)

[設定](#)

[WLC の設定](#)

[Cisco Secure ACS の設定](#)

[ワイヤレス クライアントの設定と確認](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[関連情報](#)

概要

このドキュメントでは、Service Set Identifier (SSID; サービス セット ID) に基づいて、WLAN へのアクセスをユーザごとに制限する設定例を説明します。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- Wireless LAN Controller (WLC; ワイヤレス LAN コントローラ) と Lightweight Access Point (LAP; Lightweight アクセス ポイント) の基本動作のための設定方法に関する知識
- Cisco Secure Access Control Server (ACS; アクセス コントロール サーバ) を設定する方法に関する基本的な知識
- Lightweight アクセス ポイント プロトコル (LWAPP) とワイヤレスのセキュリティ方式に関する知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ファームウェア 4.0 を実行する Cisco 2000 シリーズ WLC
- Cisco 1000 シリーズ LAP
- Cisco Secure ACS サーバ バージョン 3.2
- ファームウェア 2.6 を実行する Cisco 802.11a/b/g ワイヤレス クライアント アダプタ
- Cisco Aironet Desktop Utility (ADU) バージョン 2.6

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

背景説明

SSID ベースの WLAN アクセスを使用すると、WLAN に接続するために、ユーザが使用する SSID に基づいて認証されます。ユーザの認証には、Cisco Secure ACS サーバが使用されます。Cisco Secure ACS では、次の 2 つの段階で認証が行われます。

1. EAP Authentication
2. Cisco Secure ACS の Network Access Restriction (NAR; ネットワーク アクセス制限) に基づく SSID 認証

EAP および SSID ベースの認証に成功すると、ユーザは WLAN にアクセスでき、認証に失敗するとユーザは切断されます。

Cisco Secure ACS では NAR 機能を使用して、SSID に基づいてユーザ アクセスを制限します。NAR とは、ユーザがネットワークにアクセスできるようになる前に満たす必要がある条件の定義です。NAR は Cisco Secure ACS で作成されます。Cisco Secure ACS では、AAA クライアントから送信される属性からの情報を使用して、これらの条件を適用します。NAR を設定する方法はいくつかありますが、それらの方法はすべて AAA クライアントから送信される属性情報との照合に基づいています。そのため、効果的な NAR を導入するには、AAA クライアントから送信される属性の形式と内容を理解する必要があります。

NAR を設定すると、フィルタを許可条件または拒否条件のどちらとして動作させるかを選択できます。つまり、NAR では、AAA クライアントから送信される情報と NAR に格納されている情報の比較に基づいて、ネットワーク アクセスを許可するか拒否するかを指定します。ただし、NAR が動作するために十分な情報が取得できない場合、デフォルトではアクセスが拒否されます。

NAR は特定のユーザまたはユーザ グループに適用するように定義できます。詳細は、『[ネットワーク アクセス制限のホワイト ペーパー](#)』を参照してください。

Cisco Secure ACS では、次の 2 つのタイプの NAR フィルタをサポートしています。

1. **IP ベースのフィルタ** : IP ベースの NAR フィルタでは、エンド ユーザ クライアントと AAA クライアントの IP アドレスに基づいてアクセスを制限します。このタイプの NAR フィルタについては、『[IP ベースの NAR フィルタについて](#)』を参照してください。
2. **IP ベース以外のフィルタ** : IP ベース以外の NAR フィルタでは、AAA クライアントから送信された簡単な文字列の値の比較に基づいてアクセスを制限します。値には、Calling Line ID (CLID; 発信者番号)、Dialed Number Identification Service (DNIS; 着信番号情報サービ

ス) 番号、MAC アドレス、クライアントから送信されるその他の値などを使用できます。このタイプの NAR が動作するには、NAR の説明の値とクライアントから送信される値が、形式も含めて完全に一致する必要があります。たとえば、(217) 555-4534 と 217-555-4534 は一致しません。このタイプの NAR フィルタについては、「[IP ベース以外の NAR フィルタについて](#)」を参照してください。

このドキュメントでは、IP ベース以外のフィルタを使用して、SSID ベースの認証を実行します。IP ベース以外の NAR フィルタ (DNIS/CLI ベースの NAR フィルタ) は、許可または拒否されるコール/アクセスポイントの場所のリストです。このリストは、IP ベースの接続が確立されていないときに AAA クライアントの制限に使用できます。一般に、IP ベース以外の NAR 機能は、CLI 番号と DNIS 番号を使用します。DNIS/CLI フィールドの使用には例外があります。SSID 名を DNIS フィールドに入力して、SSID ベースの認証を実行できます。これは、WLC では DNIS 属性で SSID 名を RADIUS サーバに送信するためです。そのため、ユーザまたはグループに DNIS NAR を作成すると、ユーザごとの SSID 制限を作成できます。

RADIUS を使用する場合、次に示されている NAR フィールドでは次の値を使用します。

- [AAA client] : NAS-IP-address (属性 4) または、NAS-IP-address が存在しない場合は NAS-identifier (RADIUS 属性 32) が使用されます。
- [Port] : NAS-port (属性 5) または、NAS-port が存在しない場合は、NAS-port-ID (属性 87) が使用されます。
- CLI : calling-station-ID (属性 31) が使用されます。
- DNIS : called-station-ID (属性 30) が使用されます。

NAR の使用については、「[ネットワークアクセスの制限](#)」を参照してください。

WLC では DNIS 属性で SSID 名が送信されるため、ユーザごとの SSID 制限を作成できます。WLC の場合、NAR フィールドには次の値があります。

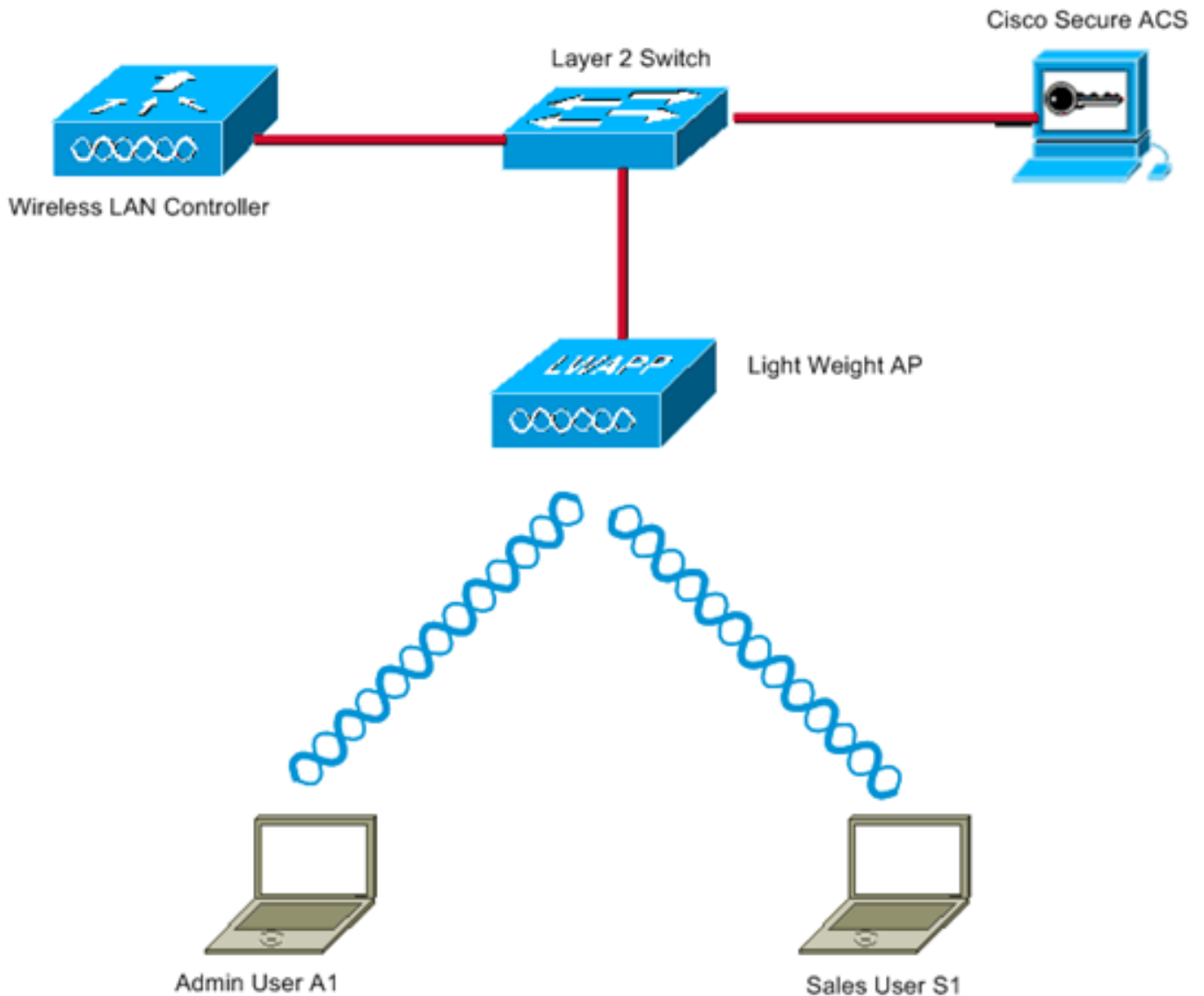
- AAA client : WLC IP アドレス
- port : *
- CLI : *
- DNIS : *ssid 名

これ以降のドキュメントでは、これを実行するための設定例を示します。

[ネットワークのセットアップ](#)

この設定例では、WLC は LAP に登録されています。2 つの WLAN が使用されています。1 つの WLAN は管理部門のユーザ用で、もう 1 つの WLAN は営業部門のユーザ用です。ワイヤレスクライアント A1 (管理部門ユーザ) と S1 (営業部門ユーザ) はワイヤレスネットワークに接続します。管理部門ユーザ A1 は WLAN Admin にのみアクセスでき、WLAN Sales へのアクセスを制限されるようにし、営業部門ユーザ S1 は WLAN Sales にはアクセスできるが、WLAN Admin へのアクセスは制限されるように、WLC と RADIUS サーバを設定する必要があります。すべてのユーザはレイヤ 2 認証方式として LEAP 認証を使用します。

注: このドキュメントでは、WLC がコントローラに登録されていることを前提としています。WLC を初めて使用し、WLC の基本操作の設定方法が分からない場合は、『[ワイヤレス LAN コントローラ \(WLC\) への Lightweight AP \(LAP\) の登録](#)』を参照してください。



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

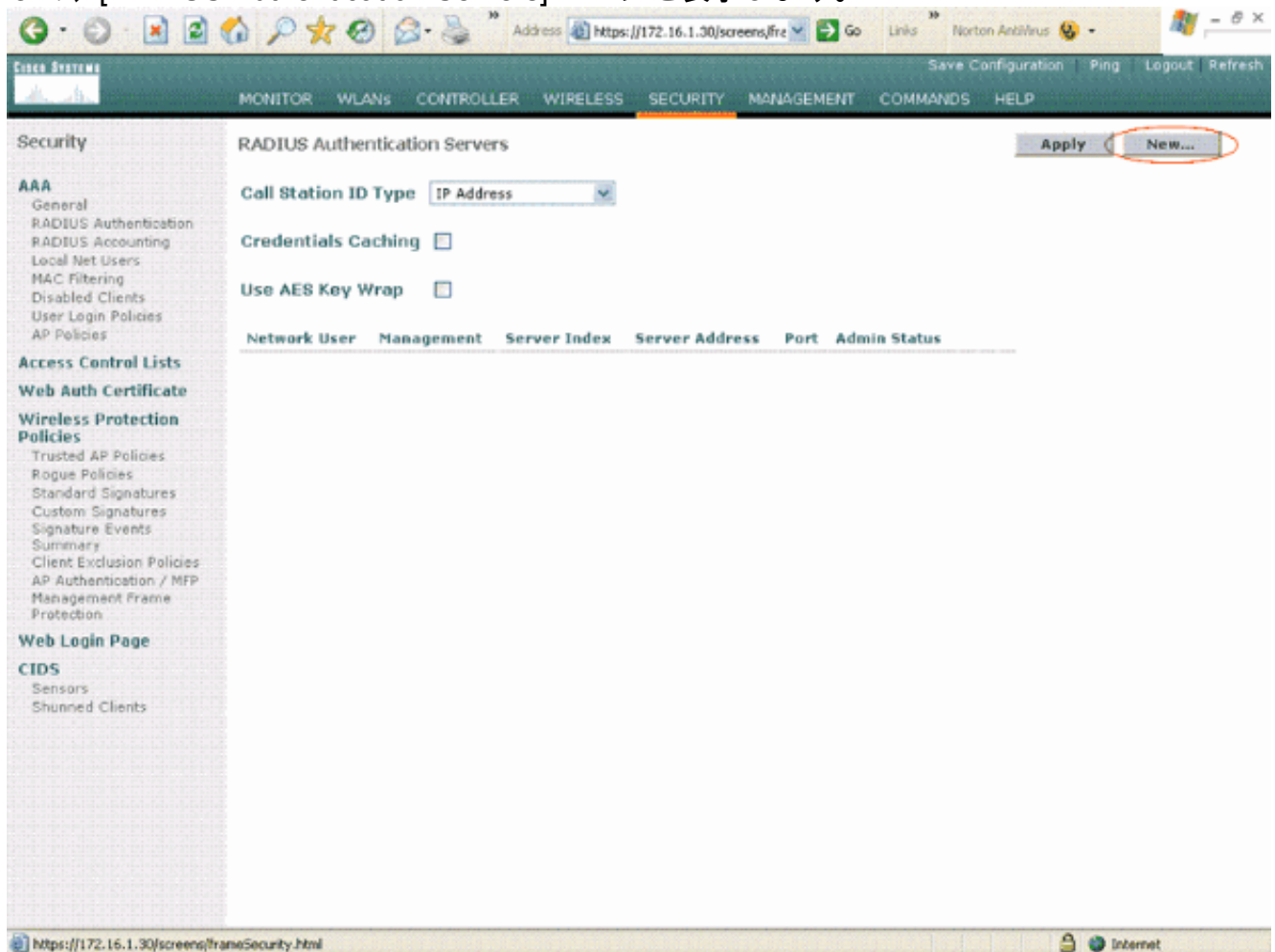
この設定用にデバイスを設定するには、次の手順を実行します。

1. [2つのWLANとRADIUSサーバ用のWLCを設定します。](#)
2. [Cisco Secure ACSを設定します。](#)
3. [ワイヤレスクライアントを設定して確認します。](#)

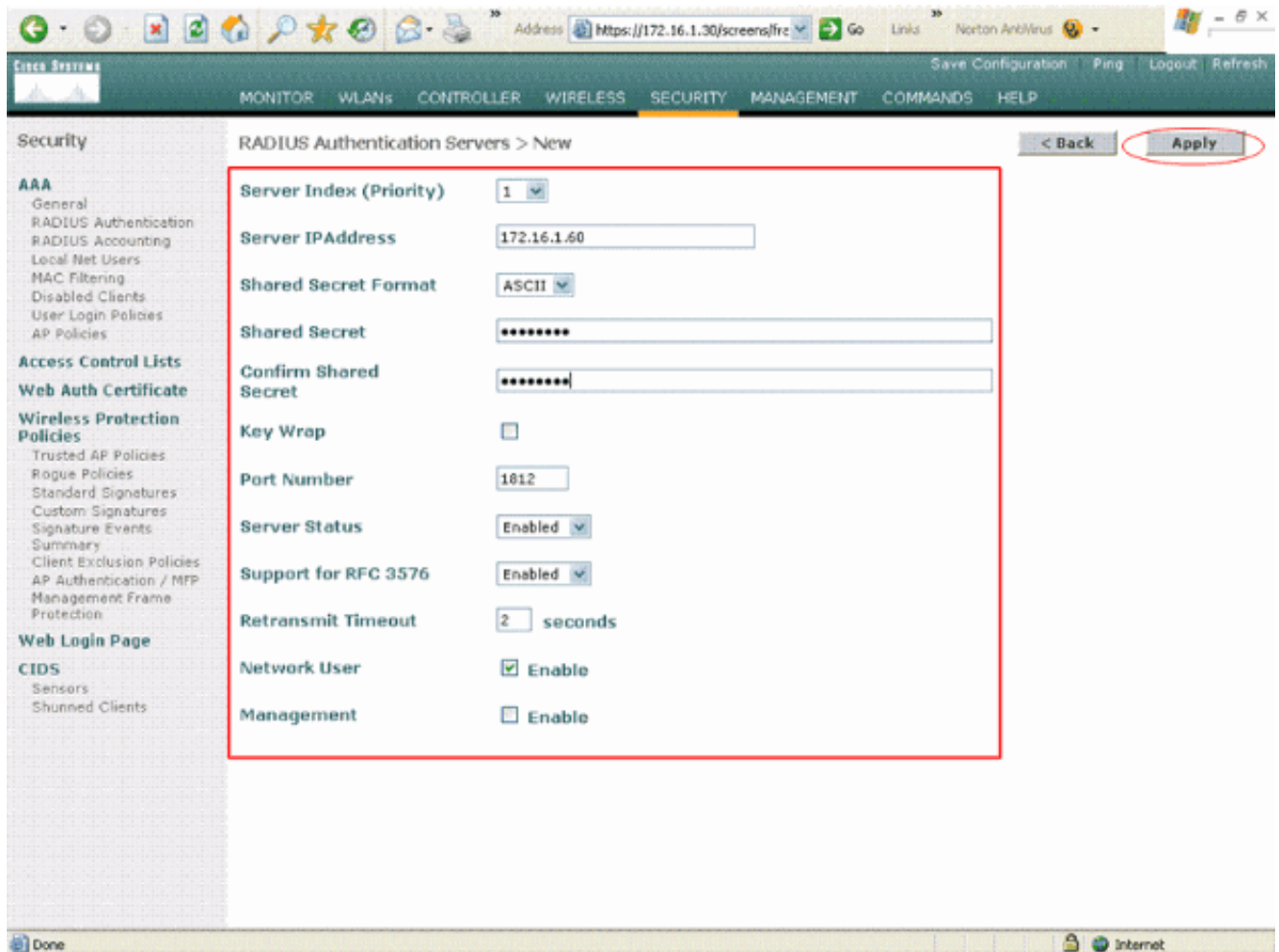
WLCの設定

このセットアップのためにWLCを設定するには、次の手順を実行します。

1. ユーザ クレデンシャルを外部 RADIUS サーバに転送するように WLC を設定する必要があります。設定すると、外部 RADIUS サーバ (この場合は Cisco Secure ACS) は、ユーザ クレデンシャルを検証し、ワイヤレス クライアントにアクセス権を付与します。次のステップを実行します。コントローラの GUI から [Security] > [RADIUS Authentication] の順に選択して、[RADIUS Authentication Servers] ページを表示します。

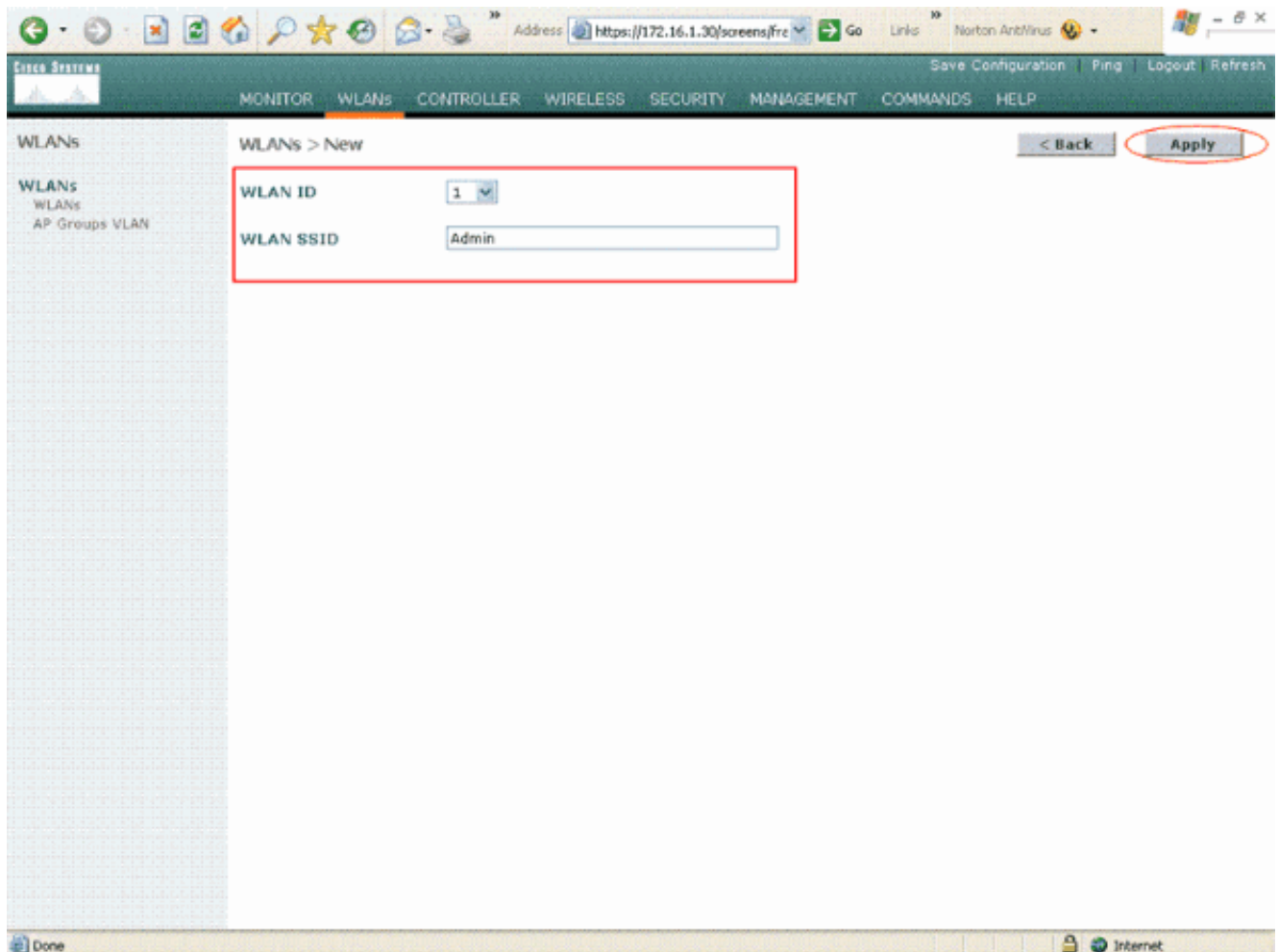


RADIUS サーバ パラメータを定義するには、[New] をクリックします。RADIUS サーバ IP アドレス、共有秘密、ポート番号、サーバステータスなどのパラメータがあります。[Network User] チェックボックスと [Management] チェックボックスでは、管理ユーザとネットワーク ユーザに RADIUS ベースの認証を適用するかどうかを指定します。この例では、Cisco Secure ACS を IP アドレスが 172.16.1.60 である RADIUS サーバとして使用します。



[Apply] をクリックします。

2. SSID が **Admin** である WLAN を管理部門用に 1 つ設定し、SSID が **Sales** である WLAN を営業部門用にもう 1 つ設定します。これを行うには、次の手順を実行します。WLAN を作成するために、コントローラの GUI で [WLANs] をクリックします。WLANs ウィンドウが表示されます。このウィンドウには、コントローラに設定されている WLAN の一覧が表示されます。新しい WLAN を設定するために [New] をクリックします。この例では、管理部門に **Admin** という名前の WLAN を作成し、WLAN ID は 1 です。[Apply] をクリックします。



[WLAN] > [Edit] ウィンドウで、WLAN に固有のパラメータを定義します。[Layer 2 Security] プルダウン メニューから、[802.1x] を選択します。デフォルトでは、レイヤ 2 セキュリティ オプションは 802.1x です。これで、この WLAN の 802.1x/EAP 認証がイネーブルになります。[General Policies] で、[AAA Override] ボックスをクリックします。[AAA Override] がイネーブルになっていて、クライアントの AAA とコントローラの WLAN の認証パラメータが競合する場合、クライアント認証は AAA サーバで実行されます。[RADIUS Servers] のプルダウン メニューから、適切な RADIUS サーバを選択します。WLAN ネットワークの要件に基づいて、その他のパラメータを変更できます。[Apply] をクリックします。

WLANs > Edit

WLAN ID: 1
WLAN SSID: Admin

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

同様に、営業部門のWLANを作成するには、手順bとcを繰り返します。スクリーンショットを次に示します。

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

Cisco Secure ACS の設定

Cisco Secure ACS サーバで、次の操作を実行します。













1. WLC を AAA クライアントとして設定します。
2. User データベースを作成し、SSID ベースの認証用に NAR を定義します。
3. EAP 認証をイネーブルにします。

Cisco Secure ACS で次の手順を実行します。

1. ACS サーバでコントローラを AAA クライアントとして定義するには、ACS GUI から [Network Configuration] をクリックします。AAA クライアントで、[Add Entry] をクリックします。


The screenshot shows the Cisco Secure ACS Network Configuration page. The left sidebar contains a navigation menu with the following items: User Setup, Group Setup, Shared Profile Components, Network Configuration (highlighted), System Configuration, Interface Configuration, Administration Control, External User Databases, Feature Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled 'Network Configuration' and features a 'Select' dropdown menu. Below this, there are two tables: 'AAA Clients' and 'AAA Servers'. The 'AAA Clients' table is currently empty, displaying 'None Defined'. The 'AAA Servers' table contains one entry: 'tsweb-laptop' with an IP address of '127.0.0.1' and a type of 'CiscoSecure ACS'. Both tables have 'Add Entry' and 'Search' buttons. At the bottom of the page, there is a 'Back to Help' button.

2. [Network Configuration] ページが表示されたら、WLC の名前、IP アドレス、共有秘密鍵、および認証方式 (RADIUS Cisco Airespace) を定義します。

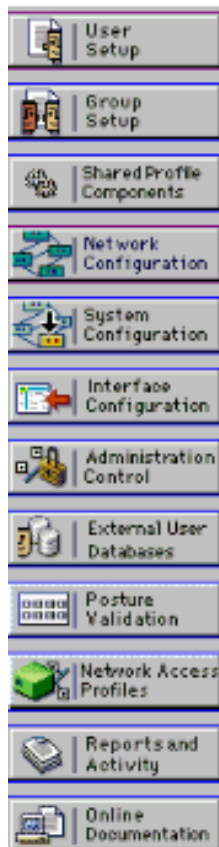
-  User Setup
-  Group Setup
-  Shared Profile Components
-  Network Configuration
-  System Configuration
-  Interface Configuration
-  Administration Control
-  External User Databases
-  Posture Validation
-  Network Access Profiles
-  Reports and Activity
-  Online Documentation

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. ACS GUI から [User Setup] をクリックし、ユーザ名を入力して、[Add/Edit] をクリックします。この例では、ユーザは A1 です。
4. [User Setup] ページが表示されたら、ユーザに固有のすべてのパラメータを定義します。LEAP 認証にはユーザ名、パスワード、補足ユーザ情報のパラメータが必要なため、この例ではこれらの値が設定されています。



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:

- [User Setup] ページの [Network Access Restrictions] セクションまで下にスクロールします。
 [User Interface of DNIS/CLI Access Restriction] で、[Permitted Calling/ Point of Access Locations] を選択し、次のパラメータを定義します。**AAA client** : WLC IP アドレス (この例では 172.16.1.30) **Port** : *CLI : *DNIS : *ssid 名
- DNIS 属性は、ユーザがアクセスを許可される SSID を定義します。WLC は SSID を DNIS 属性で RADIUS サーバに送信します。Admin という名前の WLAN にのみユーザがアクセスする必要がある場合は、DNIS フィールドに「*Admin」と入力します。これにより、ユーザには Admin という名前の WLAN にのみアクセス権が与えられます。[Enter] をクリックします。注 : SSIDの前には必ず*を付ける必要があります。これは必須です。

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

7. [Submit] をクリックします。
8. 同様に、営業部門のユーザを作成します。次にスクリーンショットを示します。



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. データベースにさらにユーザを追加するには、同じ手順を繰り返します。注：デフォルトでは、すべてのユーザがデフォルトグループの下にグループ化されます。特定のユーザを別のグループに割り当てるには、『[Cisco Secure ACS for Windows Server 3.2 ユーザガイド](#)』の「[ユーザグループ管理](#)」セクションを参照してください。注：[User Setup] ウィンドウに [Network Access Restrictions] セクションが表示されない場合、このオプションがイネーブルになっていない可能性があります。ユーザの [Network Access Restrictions] をイネーブルにするには、ACS GUI から [Interfaces] > [Advanced Options] の順に選択し、[User-Level Network Access Restrictions] を選択して [Submit] をクリックします。これにより、NAR がイネーブルになり、[User Setup] ウィンドウに表示されます。



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:

enter

Submit
Cancel

10. EAP 認証をイネーブルにするには、目的の EAP 認証方法を実行するように認証サーバが設定されていることを確認するために [System Configuration] と [Global Authentication Setup] をクリックします。[EAP Configuration] の設定で、適切な EAP 方式を選択します。この例では、LEAP 認証を使用しています。設定が終了したら、[Submit] をクリックします。

-  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

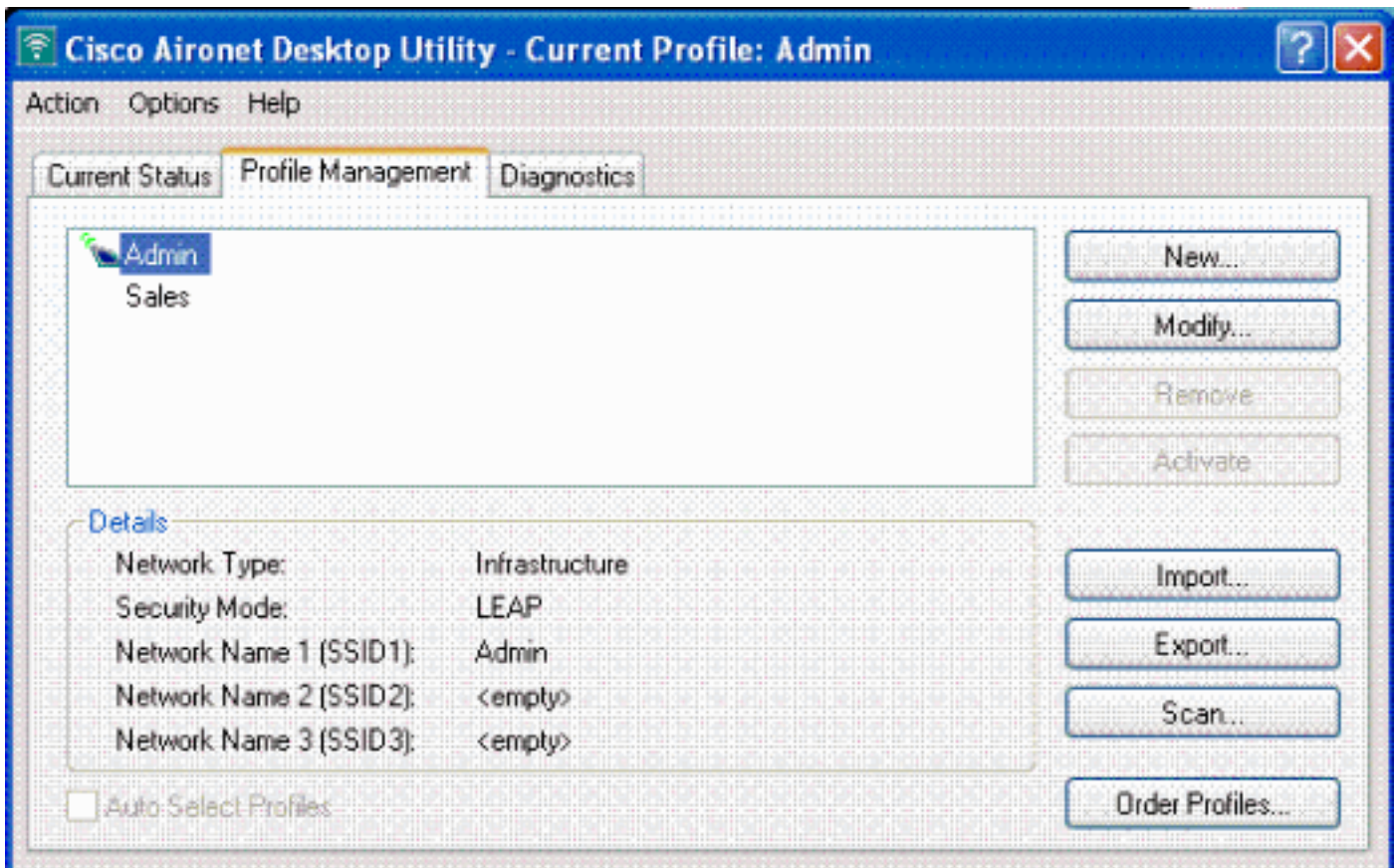
Submit
Submit + Restart
Cancel

ワイヤレスクライアントの設定と確認

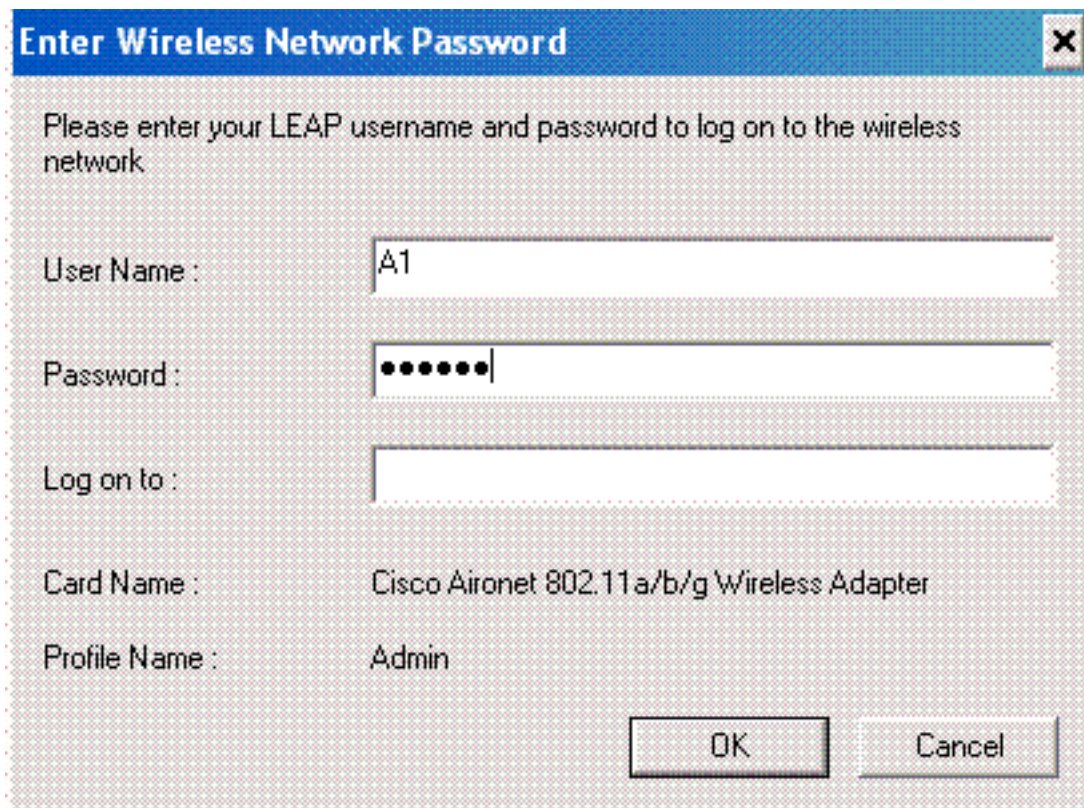
ここでは、設定が正常に機能しているかどうかを確認します。LEAP 認証を使用してワイヤレスクライアントと LAP を関連付けて、設定が目的のとおり動作することを確認します。

注：このドキュメントでは、クライアントプロファイルが LEAP 認証用に設定されていることを前提としています。802.11 a/b/g ワイヤレスクライアントアダプタを LEAP 認証用に設定する方法については、「[EAP 認証の使用方法](#)」を参照してください。

注：ADUからは、2つのクライアントプロファイルが設定されていることがわかります。1つは SSID が **Admin** に設定されている管理部門ユーザ用であり、もう1つのプロファイルは SSID が **Sales** に設定されている営業部門ユーザ用です。両方のプロファイルは LEAP 認証用に設定されています。



管理部門のワイヤレス ユーザのプロファイルをアクティブにすると、ユーザは LEAP 認証のためのユーザ名とパスワードの入力を求められます。以下が一例です。

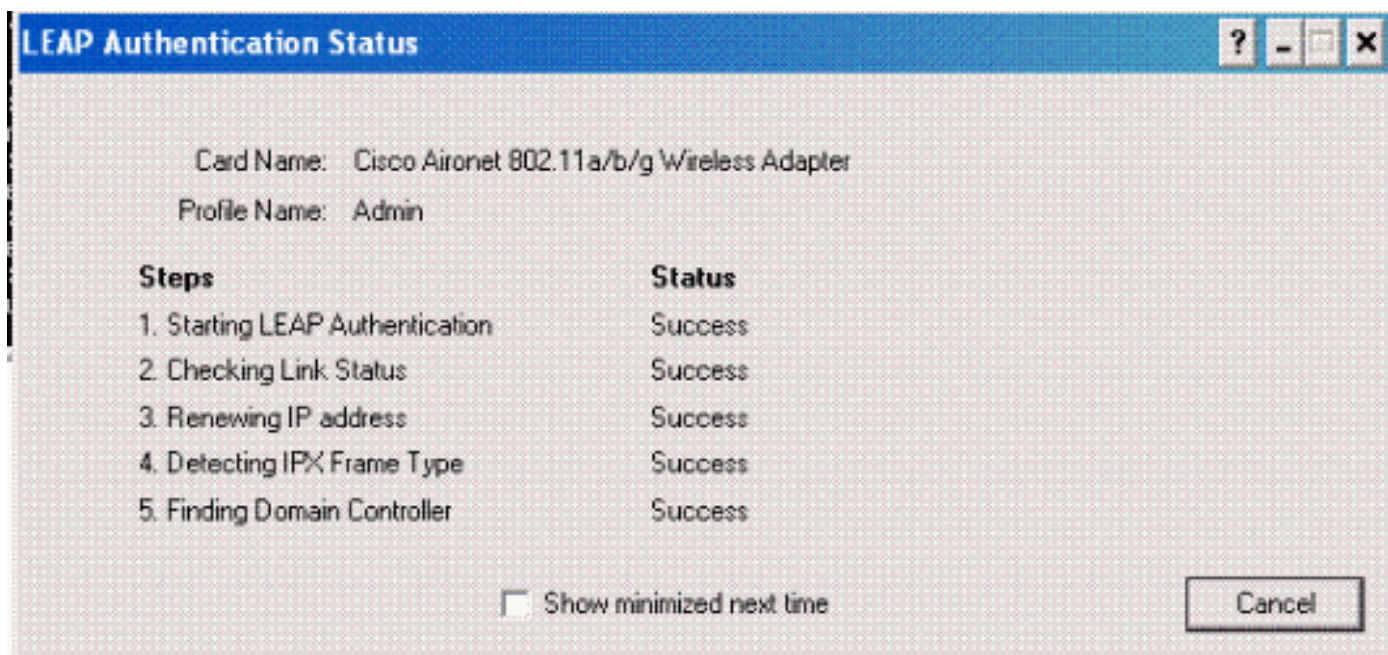


クレデンシャルを検証するため、最初に LAP、続いて WLC からユーザ クレデンシャルが外部 RADIUS サーバ (Cisco Secure ACS) に渡されます。WLC は DNIS 属性 (SSID 名) が含まれるクレデンシャルを、検証用に RADIUS サーバに送信します。

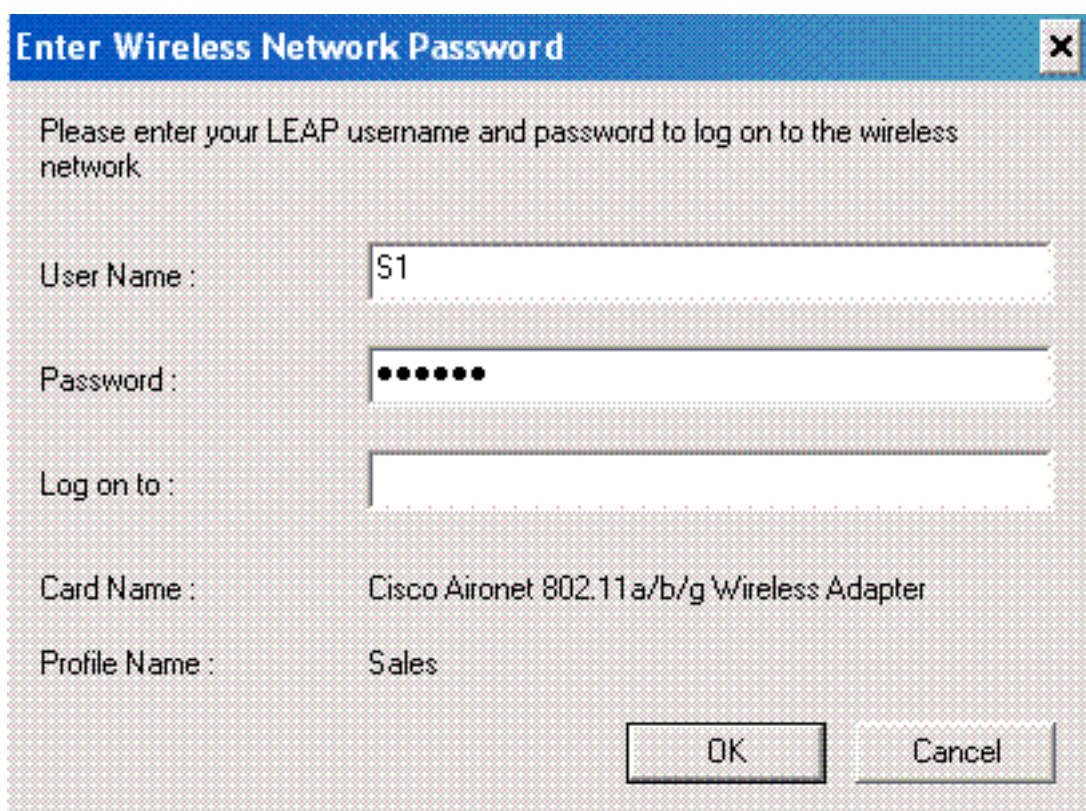
RADIUS サーバはデータをユーザ データベース (および NAR) と比較してユーザ クレデンシヤ

ルを検証し、ユーザ クレデンシャルが有効であれば常に、ワイヤレス クライアントにアクセス権を付与します。

RADIUS 認証に成功すると、ワイヤレス クライアントは LAP と関連付けられます。



同様に、営業部門のユーザが営業のプロファイルをアクティブにすると、ユーザは RADIUS サーバによって LEAP のユーザ名とパスワードおよび SSID に基づいて認証されます。



ACS サーバ上の [Passed Authentication] レポートには、クライアントが RADIUS 認証 (EAP 認証と SSID 認証) をパスしたことが示されます。以下が一例です。

Reports and Activity

Select

Passed Authentications active.csv Refresh Download

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

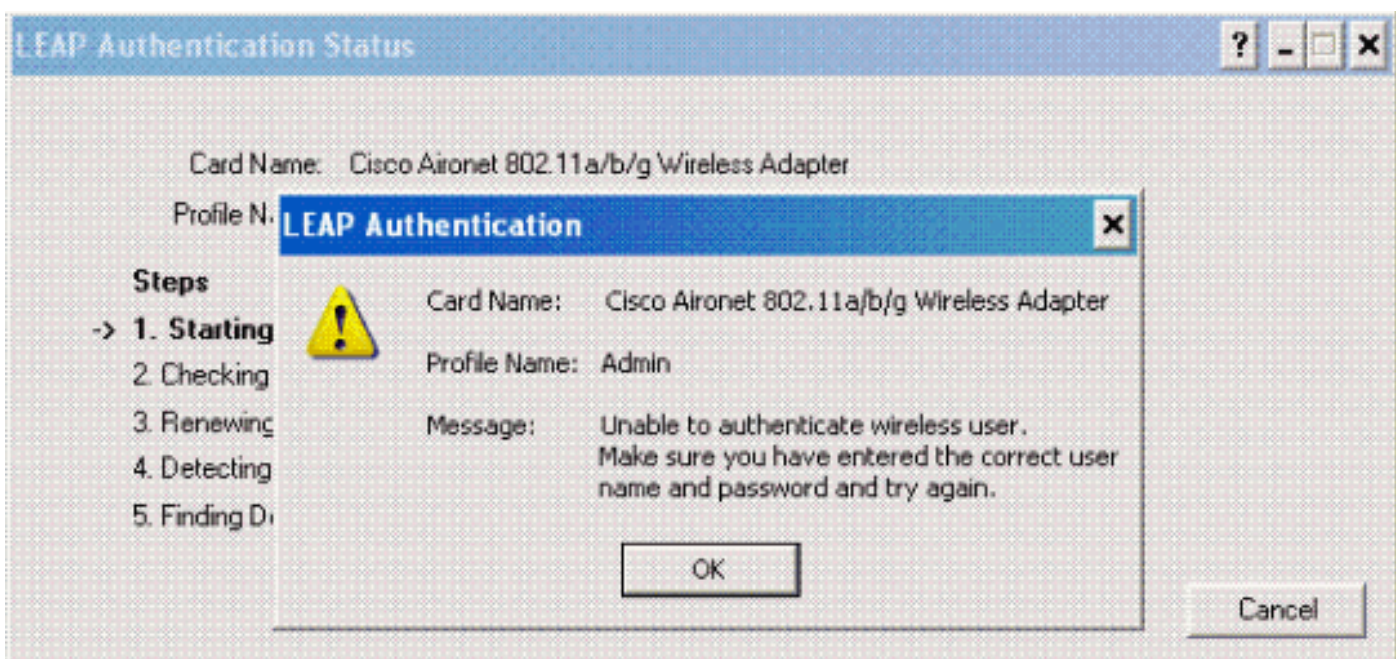
mm/dd/yyyy, hh:mm:ss mm/dd/yyyy, hh:mm:ss 50

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	00-40-95-AC-E6-57	1	172.16.1.30	(Default)	17	LEAP
10/11/2006	14:47:05	Authen OK	A1	Default Group	00-40-95-AC-E6-57	1	172.16.1.30	(Default)	17	LEAP

ここで、営業ユーザが Admin SSID にアクセスしようとする、RADIUS サーバはその WLAN へのユーザ アクセスを拒否します。以下が一例です。



このようにして、SSID に基づいてユーザ アクセスが制限されます。エンタープライズ環境では、特定の部署に所属するすべてのユーザを 1 つのグループにグループ化でき、このドキュメントで説明されているように、使用する SSID に基づいて WLAN へのアクセス権を付与できます。

トラブルシューティング

トラブルシューティングのためのコマンド

[アウトプット インタープリタ ツール \(登録ユーザ専用\) \(OIT\)](#) は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

注: [debug](#) コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

- `debug dot1x aaa enable` : 802.1x AAA のインタラクションのデバッグをイネーブルにします。
- `debug dot1x packet enable` : すべての dot1x パケットのデバッグをイネーブルにします。

- **debug aaa all enable** : すべての AAA メッセージのデバッグを設定します。

また、Cisco Secure ACS サーバで [Passed Authentication] レポートと [Failed Authentication] レポートを使用して、設定をトラブルシューティングできます。これらのレポートは、ACS GUI の [Reports and Activities] ウィンドウにあります。

[関連情報](#)

- [EAP 認証と WLAN コントローラ \(WLC \) の設定例](#)
- [ワイヤレス LAN コントローラの Web 認証の設定例](#)
- [ワイヤレス LAN コントローラを使用した AP グループ VLAN の設定例](#)
- [ワイヤレスに関するサポート ページ](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。