

ワイヤレス LAN コントローラおよび Cisco Secure ACS を使ったユーザごとの ACL 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](#)

[ネットワーク図](#)

[設定](#)

[ワイヤレス LAN コントローラの設定](#)

[ワイヤレス ユーザ用の VLAN の作成](#)

[Cisco Secure ACS で認証する WLC の設定](#)

[ワイヤレス ユーザ用の新規 WLAN の作成](#)

[ユーザに対する ACL の定義](#)

[Cisco Secure ACS サーバの設定](#)

[Cisco Secure ACS 上の AAA クライアントとしてのワイヤレス LAN コントローラの設定](#)

[Cisco Secure ACS 上でのユーザおよびユーザ プロファイルの設定](#)

[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ヒント](#)

[関連情報](#)

概要

このドキュメントでは、WLC のアクセス コントロール リスト (ACL) を作成し、RADIUS 認証に応じてユーザに適用する方法の例を示します。

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。

- Cisco Secure ACS サーバを設定してワイヤレス クライアントを認証する方法についての基本的な知識

- Cisco Aironet Lightweight アクセス ポイント (LAP) および Cisco Wireless LAN Controller (WLC) の設定についての知識
- Cisco Unified Wireless Security ソリューションについての知識

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。

- バージョン 5.0.148.0 が稼働する Cisco 4400 シリーズ Wireless LAN Controller
- Cisco Aironet 1231 シリーズ Lightweight アクセス ポイント (LAP)
- バージョン 3.6 が稼働する Cisco Aironet 802.11 a/b/g Cisco Wireless LAN クライアント アダプタ
- Cisco Aironet Desktop Utility バージョン 3.6
- Cisco Secure ACS サーバ バージョン 4.1
- IOS® バージョン 12.4(11)T が稼働する Cisco 2800 シリーズ サービス統合型ルータ
- バージョン 12.0(5)WC3b が稼働する Cisco Catalyst 2900XL シリーズ スイッチ

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については、『[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

ユーザごとのアクセス コントロール リスト (ACL) は、シスコのアイデンティティ ネットワーキングの一部です。Cisco Wireless LAN ソリューションは、アイデンティティ ネットワーキングをサポートします。それによって、ネットワークが単一の SSID をアダプタイズできる一方、特定のユーザが、ユーザ プロファイルに基づいて異なるポリシーを継承することができるようになります。

ユーザごとの ACL 機能を使用すると、ワイヤレス LAN コントローラ上で設定された ACL を RADIUS 認証に基づいてユーザに適用することができます。これは、Airespace-ACL-Name Vendor Specific Attribute (VSA) で実現されます。

この属性は、クライアントに適用される ACL 名を示します。RADIUS Access Accept に ACL 属性が指定されている場合、システムでは認証後に ACL-Name がクライアント ステーションに適用されます。これは、インターフェイスに割り当てられた ACL を上書きします。インターフェイスに割り当てられた ACL を無視し、新しい ACL を適用するということです。

ACL-Name 属性形式の要約を次に示します。フィールドは左から右に伝送されます。

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1			
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+			
Type	Length	Vendor-Id	

```

+++++
Vendor-Id (cont.)      | Vendor type  | Vendor length |
+++++
|      ACL Name...
+++++
• Type - 26 for Vendor-Specific
• Length - >7
• Vendor-Id - 14179
• Vendor type - 6
• Vendor length - >0
• Value - A string that includes the name of the ACL to use for the client.
      The string is case sensitive.

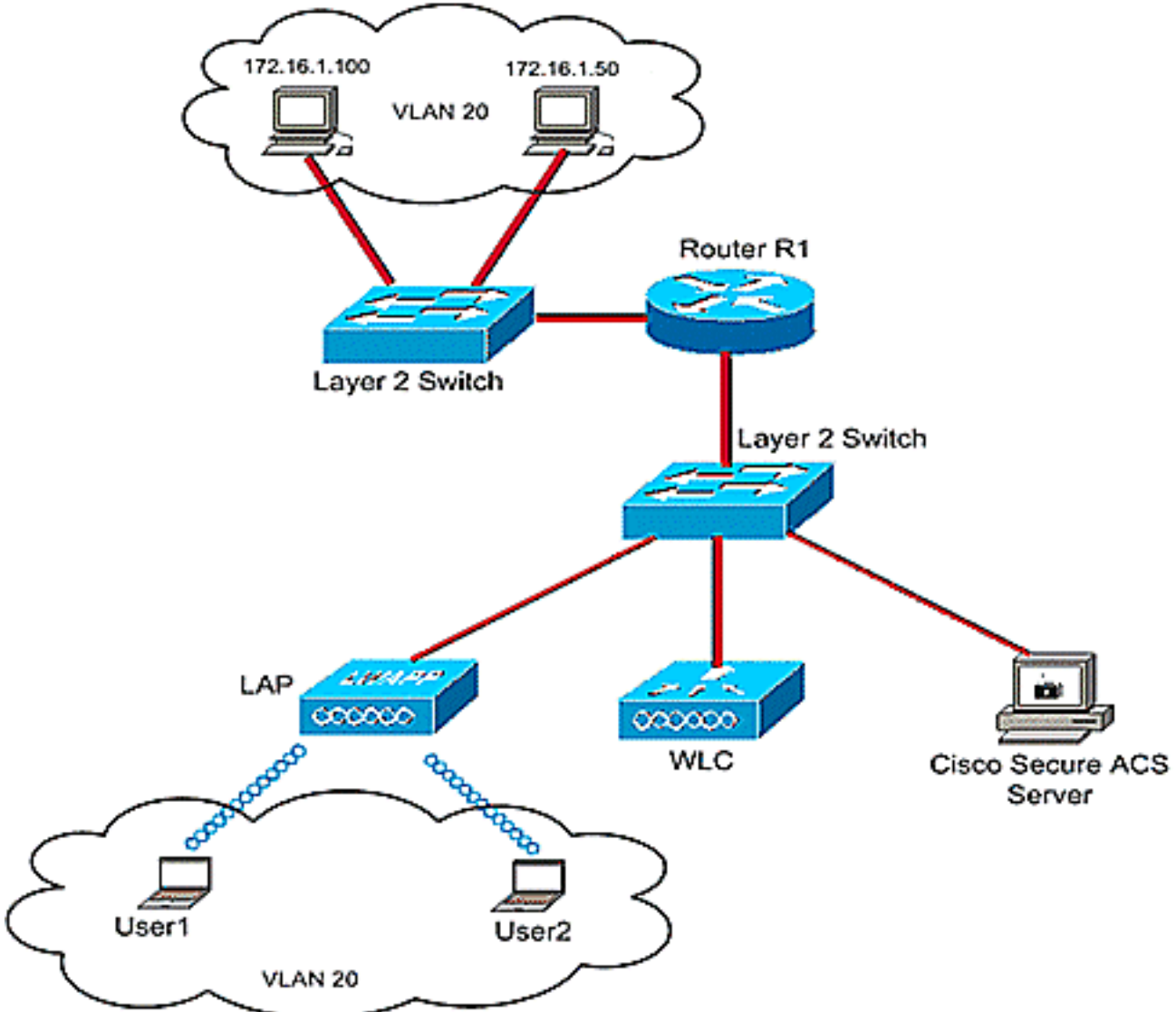
```

Cisco Unified Wireless Network Identity Networking の詳細については、ドキュメント『[セキュリティソリューションの設定](#)』の「Identity ネットワーキングの設定」の項を参照してください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。

このセットアップでは、ワイヤレス LAN コントローラ WLC および LAP を使用して、Department A および Department B のユーザにワイヤレス サービスが提供されます。ワイヤレスユーザはすべて Office-VLAN という VLAN 内に存在し、ネットワークへのアクセスに Office という共通の WLAN (SSID) を使用します。



ワイヤレス ユーザの認証には、Cisco Secure ACS サーバが使用されます。ユーザの認証には EAP 認証が使用されます。WLC、LAP、および Cisco Secure ACS サーバは、次のように Layer 2 Switch に接続されます。

Router R1 は、次のように、Layer 2 Switch 経由で有線側に接続されます。Router R1 は、DHCP サーバとしても機能し、サブネット 172.16.0.0/16 からのワイヤレス クライアントに IP アドレスを提供します。

次の状態になるようにデバイスを設定する必要があります。

Department A からの User1 はサーバ 172.16.1.100 にだけアクセスできる

Department B からの User2 はサーバ 172.16.1.50 にだけアクセスできる

これを実現するには、WLC に 2 つの ACL を作成する必要があります。1 つは User1 用、もう 1 つは User2 用です。ACL を作成したら、ワイヤレスユーザの認証が成功したら、ACL 名属性を WLC に返すように Cisco Secure ACS サーバを設定する必要があります。WLC はユーザに ACL を適用し、その結果ネットワークへの接続はユーザ プロファイルによって制限されます。

注：このドキュメントでは、ユーザの認証に LEAP 認証を使用します。Cisco LEAP には、ディクシヨナリ攻撃に対する脆弱性が存在します。リアルタイム ネットワークでは、EAP FAST のような、よりセキュアな認証方法を使用する必要があります。このドキュメントは、ユーザごとの ACL 機能の設定方法を説明することが目的であるため、ここでは単純化のために LEAP を使用しています。

次のセクションは、このセットアップを設定するためのステップごとの手順を説明しています。

設定

ユーザごとの ACL を設定する前に、WLC の基本動作を設定し、さらに WLC に LAP を登録する必要があります。このドキュメントでは、基本動作用に WLC が設定されており、WLC に LAP が登録されていることを前提としています。WLC で LAP との基本動作を初めて設定する場合は、[Wireless LAN Controller \(WLC \) への Lightweight AP \(LAP \) の登録](#)を参照してください。

LAP が登録されたら、次の手順を実行し、このセットアップ用のデバイスを設定します。

1. [ワイヤレス LAN コントローラを設定します。](#)
2. [Cisco Secure ACS サーバを設定します。](#)
3. [設定を確認します。](#)

注：このドキュメントでは、ワイヤレス側で必要な設定について説明します。有線側が設定されていることを前提としています。

ワイヤレス LAN コントローラの設定

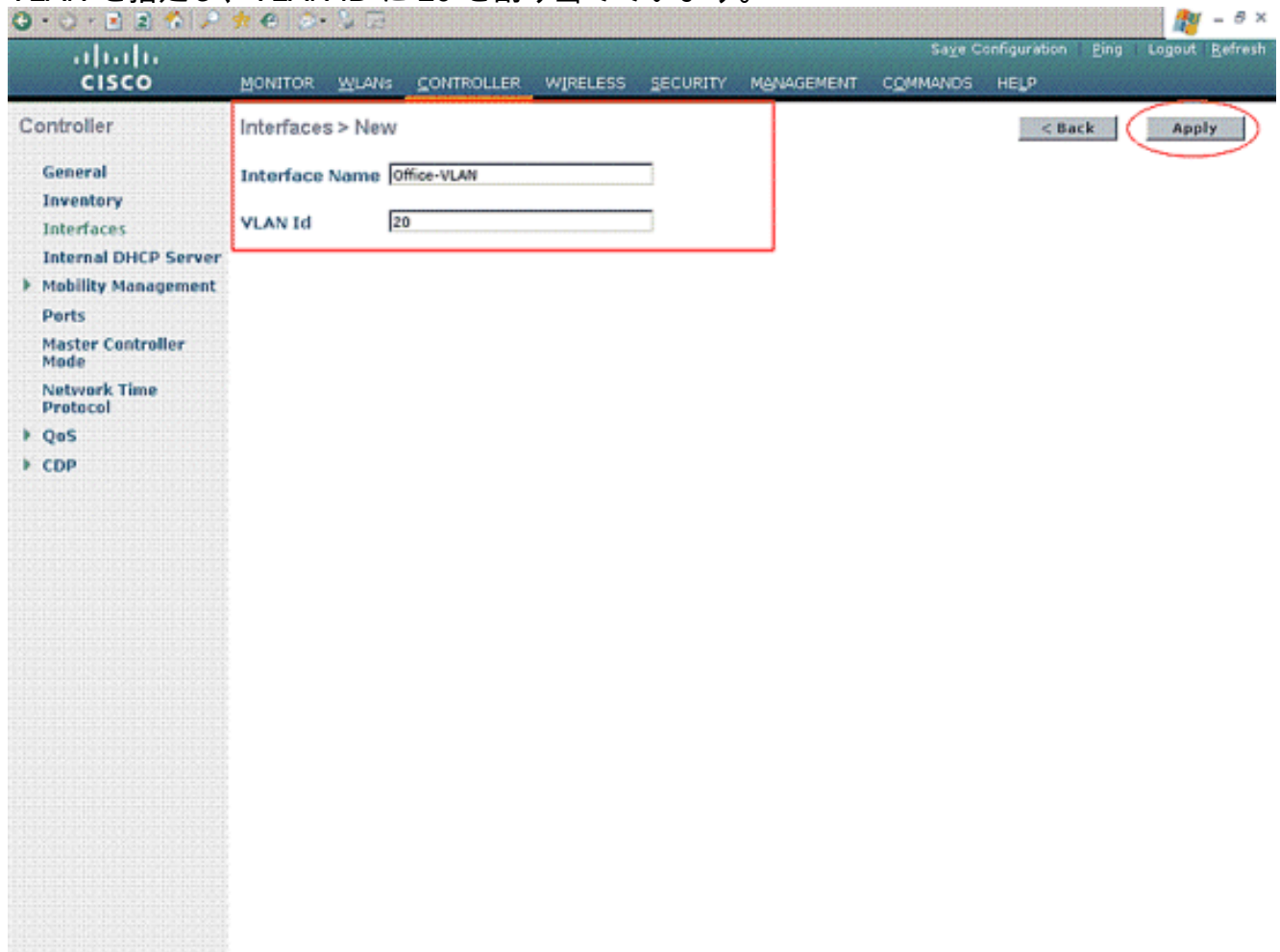
ワイヤレス LAN コントローラで次を実行する必要があります。

- [ワイヤレス ユーザ用の VLAN の作成。](#)
- [Cisco Secure ACS でワイヤレス ユーザを認証する WLC の設定。](#)
- [ワイヤレス ユーザ用の新規 WLAN の作成。](#)
- [ワイヤレス ユーザに対する ACL の定義。](#)

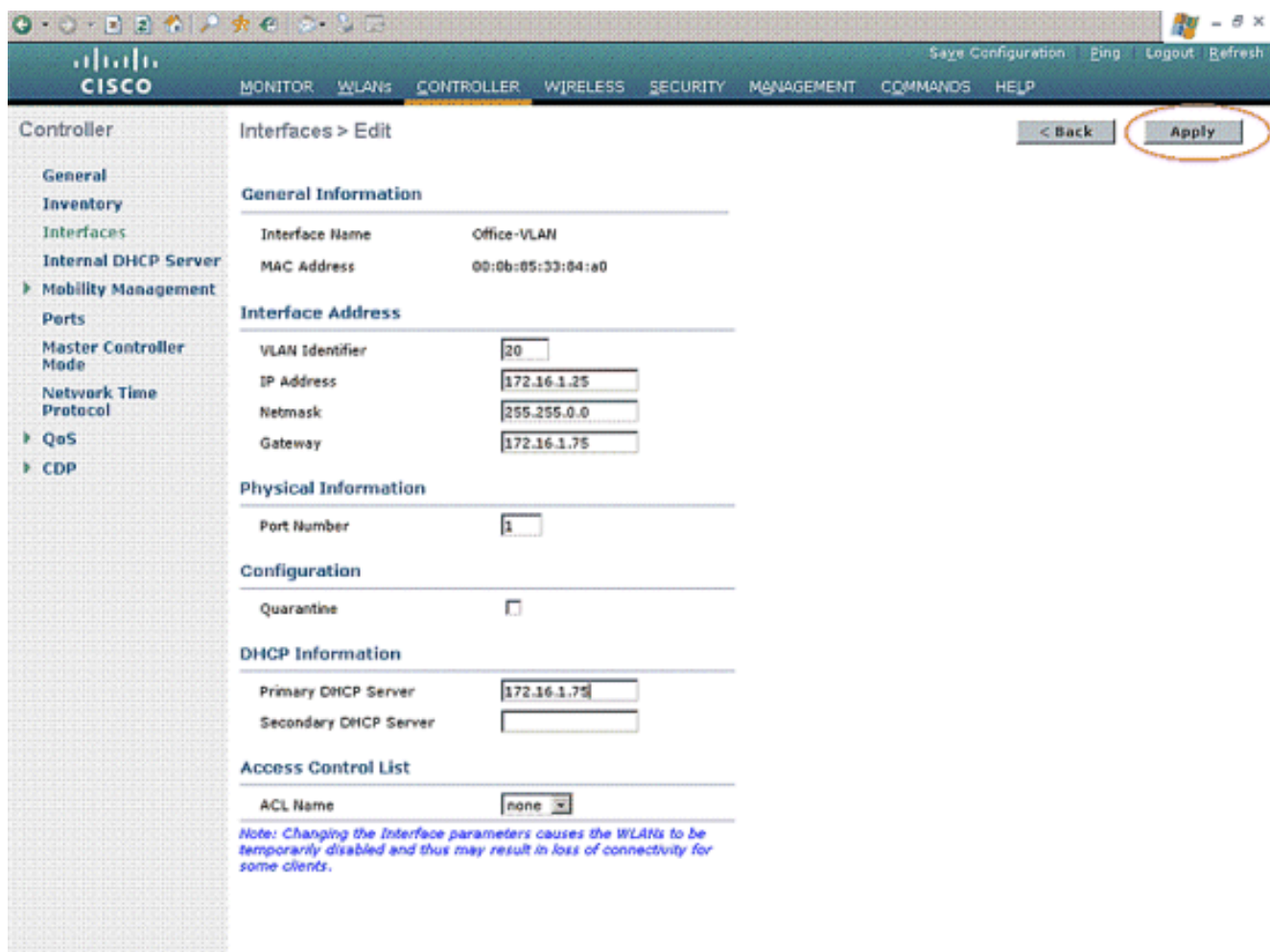
ワイヤレス ユーザ用の VLAN の作成

ワイヤレス ユーザ用の VLAN を作成するには、次の手順を実行します。

1. WLC の GUI に移動し、[Controller] > [Interfaces] の順に選択します。[Interfaces] 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インターフェイスの一覧が表示されます。
2. 新しいダイナミック インターフェイスを作成するには、[New] をクリックします。
3. [Interfaces] > [New] ウィンドウで、インターフェイス名と VLAN ID を入力します。次に [Apply] をクリックします。この例では、ダイナミック インターフェイスの名前に Office-VLAN を指定し、VLAN ID に 20 を割り当てています。



4. [Interfaces] > [Edit] ウィンドウで、ダイナミック インターフェイスの IP アドレス、サブネット マスク、デフォルト ゲートウェイを入力します。ダイナミック インターフェイスを WLC の物理ポートに割り当て、DHCP サーバの IP アドレスを入力します。次に [Apply] をクリックします。



この例では、Office-VLAN インターフェイスに次のパラメータを使用しています。

Office-VLAN

IP address: 172.16.1.25

Netmask: 255.255.0.0

Default gateway: 172.16.1.75 (sub-interface on Router R1)

Port on WLC: 1

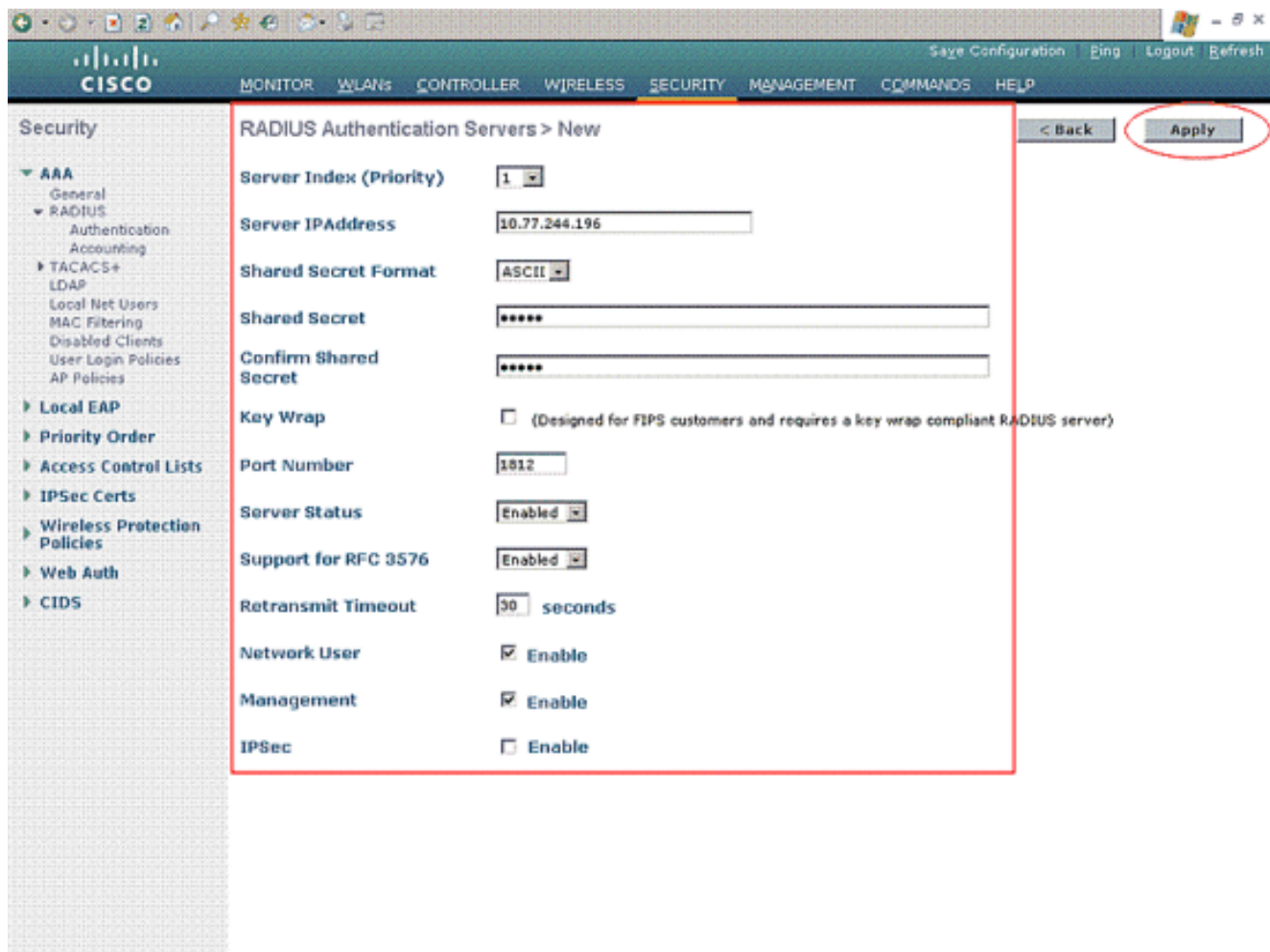
DHCP server: 172.16.1.75

[Cisco Secure ACS で認証する WLC の設定](#)

ユーザ クレデンシャルを外部 RADIUS サーバ (この例では、Cisco Secure ACS) に転送するには WLC を設定する必要があります。RADIUS サーバはユーザ クレデンシャルを検証し、ワイヤレス ユーザの認証に成功したら、ACL 名前属性を WLC に返します。

RADIUS サーバを使用するように WLC を設定するには、次の手順を実行します。

1. コントローラの GUI から [Security]、[RADIUS]、[Authentication] を選択して、[RADIUS Authentication Servers] ページを表示します。次に、[New] をクリックして、RADIUS サーバを定義します。
2. [RADIUS Authentication Servers] > [New] ページで RADIUS サーバのパラメータを定義します。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。

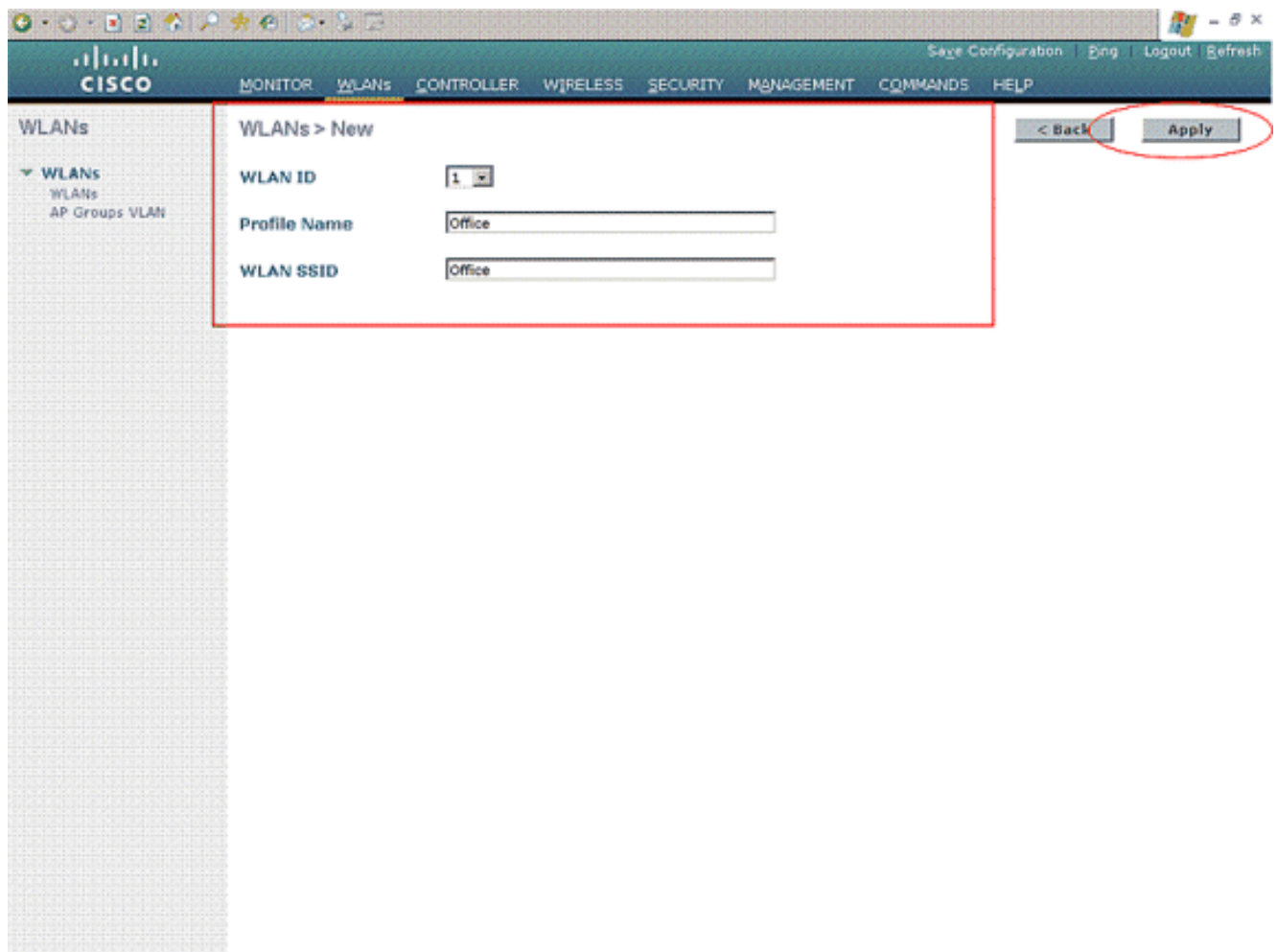


3. [Network User] チェックボックスと [Management] チェックボックスでは、管理ユーザとネットワークユーザに RADIUS ベースの認証を適用するかどうかを指定します。この例では、IPアドレス10.77.244.196のRADIUSサーバとしてCisco Secure ACSを使用しています。[Apply]をクリックします。

ワイヤレスユーザ用の新規 WLAN の作成

次に、ワイヤレスユーザが接続できる WLAN を作成する必要があります。新しい WLAN を作成するには、次の手順を実行します。

1. ワイヤレス LAN コントローラの GUI で [WLANs] をクリックします。このページには、コントローラに存在する WLAN の一覧が表示されます。
2. 新しい WLAN を作成するには、[New] をクリックします。WLAN の WLAN ID、プロファイル名、WLAN SSID を入力し、[Apply] をクリックします。この設定では、WLAN Office を作成します。



3. 新しい WLAN を作成すると、新しい WLAN に対する [WLAN] > [Edit] ページが表示されます。このページでは、General Policies、Security、QOS、Advanced パラメータなど、その WLAN に固有のさまざまなパラメータを定義できます。

The screenshot shows the Cisco WLAN configuration page. The 'WLAN Status' checkbox is checked and circled in red. The 'Interface' dropdown menu is set to 'office-vlan' and also circled in red. The 'Apply' button in the top right corner is circled in red. The 'Security' tab is selected, and the 'Security Policies' are set to '[WPA2][Auth(802.1X)]'. The 'Radio Policy' is set to 'All' and 'Broadcast SSID' is checked and enabled.

WLAN を有効にするには、[General Policies] の下の [WLAN Status] にチェックマークを入れます。プルダウン メニューから適切なインターフェイスを選択します。この例では、インターフェイス Office-vlan を使用します。このページの他のパラメータは、WLAN ネットワークの要件に基づいて変更できます。

4. [Security] タブを選択します。[Layer 2 Security] プルダウン メニューから [802.1x] を選択します (LEAP 認証であるため)。802.1x パラメータで適切な WEP キーのサイズを選択します。

The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'WLANs > Edit' page has tabs for 'General', 'Security', 'QoS', and 'Advanced'. Under the 'Security' tab, there are sub-tabs for 'Layer 2', 'Layer 3', and 'AAA Servers'. The 'Layer 2 Security' dropdown is set to '802.1X', and the 'MAC Filtering' checkbox is unchecked. Below this, the '802.1X Parameters' section has a table for '802.11 Data Encryption' with columns for 'Type' and 'Key Size'. The 'Type' is set to 'WEP' and the 'Key Size' is '104 bits'. Both the '802.1X' dropdown and the 'WEP' and '104 bits' selections are circled in red. At the bottom, there are 'Foot Notes' with five items:

- 1 CKIP is not supported by 10xx model APs
- 3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication
- 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 5 Client MFP is not active unless WPA2 is configured

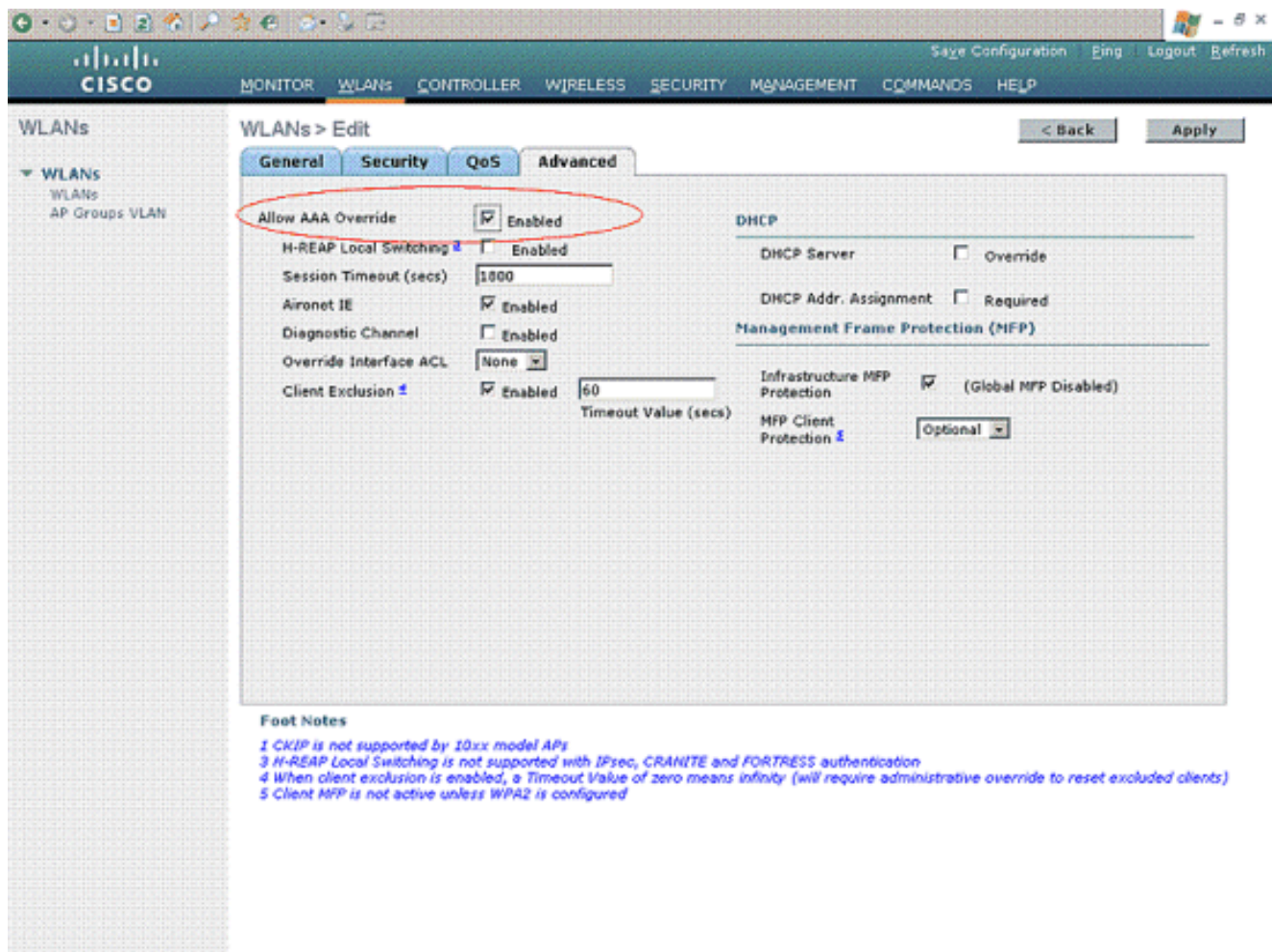
5. [Security] タブで、[AAA Servers] サブタブを選択します。ワイヤレスクライアントを認証するために使用される AAA サーバを選択します。この例では、ワイヤレスクライアントを認証するために ACS サーバ 10.77.244.1966 を使用します。

The screenshot shows the Cisco configuration page for WLANs. The 'WLANs > Edit' page has the 'Advanced' tab selected. Under 'AAA Servers', the 'Radius Servers' section is expanded. 'Server 1' is configured with 'IP:10.77.244.196, Port:1812' and 'None' for the accounting server. The 'Local EAP Authentication' section is also visible with the 'enabled' checkbox unchecked.

Foot Notes

- 1 CKIP is not supported by 10xx model APs
- 3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication
- 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 5 Client MFP is not active unless WPA2 is configured

6. [Advanced] タブを選択します。ワイヤレス LAN 上の AAA をからユーザ ポリシーのオーバーライドを設定するには、[Allow AAA Override] を選択します。



AAA オーバーライドが有効になっていて、クライアントで AAA と Cisco Wireless LAN Controller のワイヤレス LAN 認証パラメータが競合している場合、クライアント認証は AAA サーバによって行われます。この認証の一環として、オペレーティング システムはクライアントを、デフォルトの Cisco Wireless LAN ソリューションのワイヤレス LAN VLAN から、Cisco Wireless LAN Controller のインターフェイス設定で事前定義され、AAA サーバによって返された VLAN に移動します (MAC フィルタリング、802.1X、および WPA 動作が設定されている場合のみ)。すべてのケースで、Cisco Wireless LAN Controller のインターフェイス設定で事前定義されている限り、オペレーティング システムは、AAA サーバで指定された QoS、DSCP、802.1p 優先順位タグ値および ACL も使用します。

7. ネットワークの要件に応じてその他のパラメータを選択します。[Apply] をクリックします。

ユーザに対する ACL の定義

このセットアップに対して 2 つの ACL を作成する必要があります。

- ACL1 : User1 をサーバ 172.16.1.100 にだけアクセスさせるためのもの
- ACL2 : User2 をサーバ 172.16.1.50 にだけアクセスさせるためのもの

WLC 上で ACL を設定するには、次の手順を実行します。

1. WLC GUI で、[Security] > [Access Control Lists] の順に選択します。[Access Control Lists] ページが表示されます。このページには、WLC に設定されている ACL の一覧が表示されます。任意の ACL を編集または削除することもできます。新しい ACL を作成するには、[New] をクリックします。
2. このページで新しい ACL を作成することができます。ACL の名前を入力し、[Apply] をクリ

ックします。ACL が作成されたら、この ACL のルールを作成するために [Edit] をクリックします。

3. User1 はサーバ 172.16.1.100 にだけアクセスする必要があり、他のすべてのデバイスに対するアクセスは拒否されます。このためには、次のルールを定義する必要があります。ワイヤレス LAN コントローラ上で ACL を設定する方法の詳細は、[ワイヤレス LAN コントローラ上に ACL を設定する例を参照してください](#)。

The screenshot shows the Cisco WLC configuration interface for 'Access Control Lists > Edit'. The 'General' tab is selected, and the 'Access List Name' is 'User1'. A table of rules is displayed, with two rules highlighted in a red box:

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	172.16.0.0 / 255.255.0.0	172.16.1.100 / 255.255.255.255	Any	Any	Any	Any	Inbound
2	Permit	172.16.1.100 / 255.255.255.255	172.16.0.0 / 255.255.0.0	Any	Any	Any	Any	Outbound

4. 同様に、User2 に対して ACL を作成する必要があります。これにより、User2 はサーバ 172.16.1.50 にだけアクセスすることができます。これは User2 に必要な ACL です。

Security

Access Control Lists > Edit

General

Access List Name: User2

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	172.16.0.0 / 255.255.0.0	172.16.1.50 / 255.255.255.255	Any	Any	Any	Any	Inbound
2	Permit	172.16.1.50 / 255.255.255.255	172.16.0.0 / 255.255.0.0	Any	Any	Any	Any	Outbound

これで、このセットアップのワイヤレス LAN コントローラが設定されました。次の手順では、Cisco Secure Access Control サーバに対して、ワイヤレス クライアントを認証し、認証に成功した場合には ACL Name 属性を WLC に返すように設定します。

Cisco Secure ACS サーバの設定

Cisco Secure ACS がワイヤレス クライアントを認証できるようにするには、次の手順を実行する必要があります。

- [Cisco Secure ACS 上の AAA クライアントとしてワイヤレス LAN コントローラを設定します。](#)
- [Cisco Secure ACS 上でユーザおよびユーザ プロファイルを設定します。](#)

Cisco Secure ACS 上の AAA クライアントとしてのワイヤレス LAN コントローラの設定

ワイヤレス LAN コントローラを Cisco Secure ACS 上の AAA クライアントとして設定するには次の手順を実行します。

1. [Network Configuration] > [Add AAA client] をクリックします。[Add AAA Client] ページが表示されます。このページでは、WLC システム名、管理インターフェイス IP アドレス、共有秘密、および **Radius Airespace** を使用した認証を定義します。以下が一例です。

Network Configuration

Add AAA Client

AAA Client Hostname:

AAA Client IP Address:

Shared Secret:

RADIUS Key Wrap

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format: ASCII Hexadecimal

Authenticate Using:

Single Connect TACACS+ AAA Client (Record stop in accounting on failure)

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

Replace RADIUS Port info with Username from this AAA Client

Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

Help

- AAA Client Hostname
- AAA Client IP Address
- Shared Secret
- Network Device Group
- RADIUS Key Wrap
- Authenticate Using
- Single Connect TACACS+ AAA Client
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client
- Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

[\[Back to Top\]](#)

AAA Client IP Address

The AAA Client IP Address is the IP address assigned to the AAA client.

If you want to designate more than one AAA client with a single AAA client entry in ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press Enter.

You can use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1

注：Cisco Secure ACSに設定されている共有秘密は、[RADIUS Authentication Servers] > [New]でWLCに設定されている共有秘密と一致する必要があります。

2. [Submit+Apply] をクリックします。

Cisco Secure ACS 上でのユーザおよびユーザ プロファイルの設定

Cisco Secure ACS 上でユーザを設定するには次の手順を実行する必要があります。

1. ACS GUI から [User Setup] を選択し、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 User1 です。

Select

User:

List users beginning with letter/number:

A	B	C	D	E	F	G	H	I	J	K	L		
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9				

Help

- [User Setup and External User Databases](#)
- [Finding a Specific User in the ACS Internal Database](#)
- [Adding a User to the ACS Internal Database](#)
- [Listing Usernames that Begin with a Particular Character](#)
- [Listing All Usernames in the ACS Internal Database](#)
- [Changing a Username in the ACS Internal User Database](#)
- [Remove Dynamic Users](#)

User Setup enables you to configure individual user information, add users, and delete users in the database. **User Setup and External User Databases**

Before ACS can authenticate users with an external user database:

- You must have the database up and running on the external server. For example, if you are using token card authentication, your token server must be running and properly configured.
- You must have configured the applicable parameters in the External User Databases section.

Note: User Setup configuration overrides Group Setup configuration.

If you rely on the Unknown User Policy in the External User Databases section to create entries in the ACS internal database for users defined in an external user database, usernames cannot be located or listed here until the user has successfully authenticated once.

External user database modification must be done from within the external user database itself. For added security, authorization, and accounting purposes, User Setup keeps track of users who authenticate with an external user database. User Setup lets you configure individual user information, add users, and delete users in the ACS internal database.

Note: User Setup does not add or delete usernames in an external user database. [Back to Top](#)

Finding a Specific User in the ACS Internal Database

To find a user already in the ACS internal database, type the first few letters of the username in the User field, add an asterisk (*) as a wildcard, and click **Find**. From the list of usernames displayed, click the username whose information you want to view or change.

[Back to Top](#)

Adding a User to the ACS Internal Database

To add a new user or edit a configuration for an existing user, type a username

2. [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。この例では、ユーザ名、パスワード、補足ユーザ情報、および RADIUS 属性を設定します。これらのパラメータは EAP 認証でのみ必要となるものです。

User Setup

User: UserA (New User)

Account Disabled

Supplementary User Info

Real Name: User 1

Description:

User Setup

Password Authentication:

ACS Internal Database

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:

Submit Cancel

Help

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IEEE RADIUS Attributes
- RADIUS Vendor-Specific Attributes

Account Disabled Status

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[Back to Top](#)

Deleting a Username

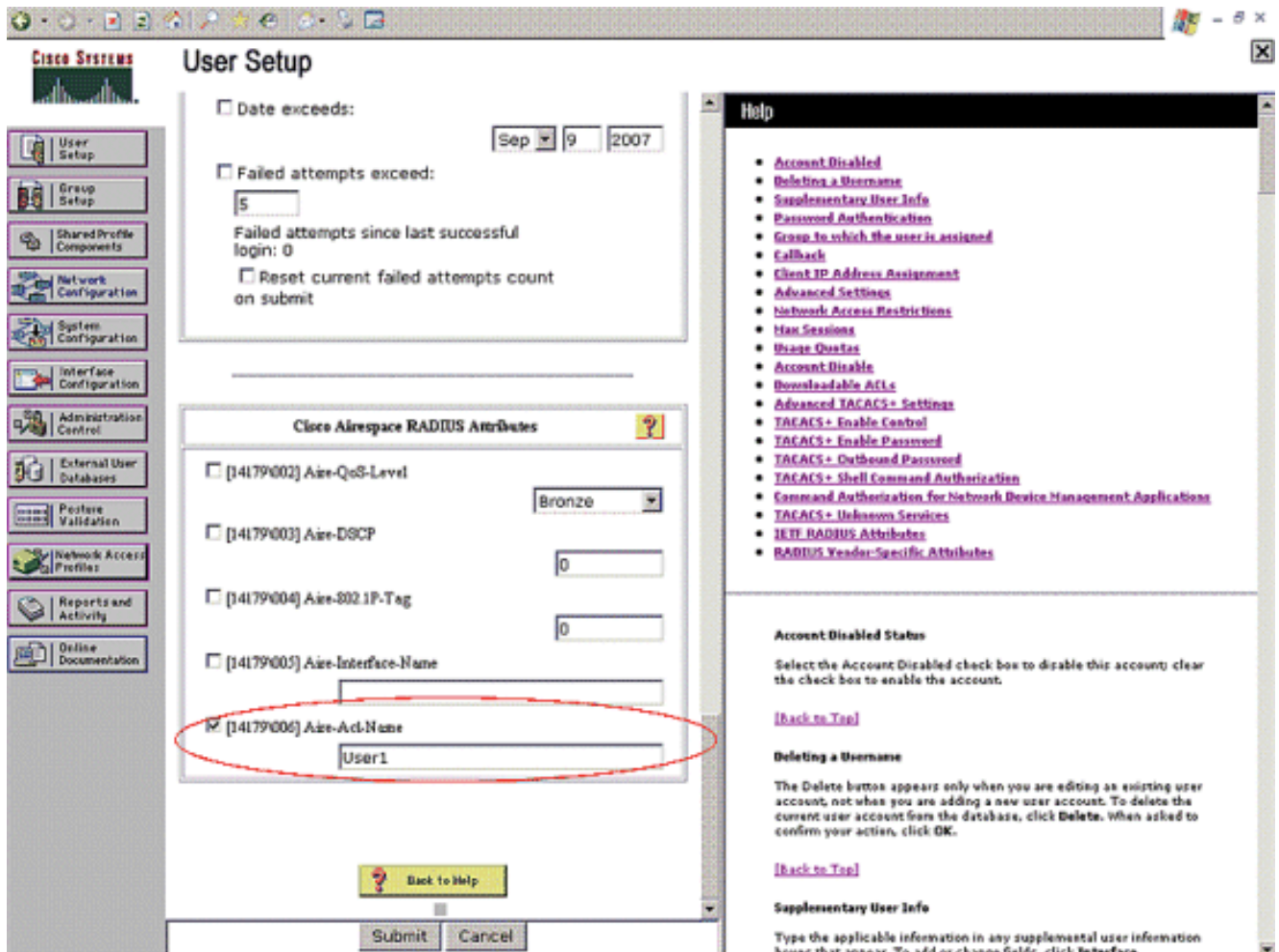
The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click **Delete**. When asked to confirm your action, click **OK**.

[Back to Top](#)

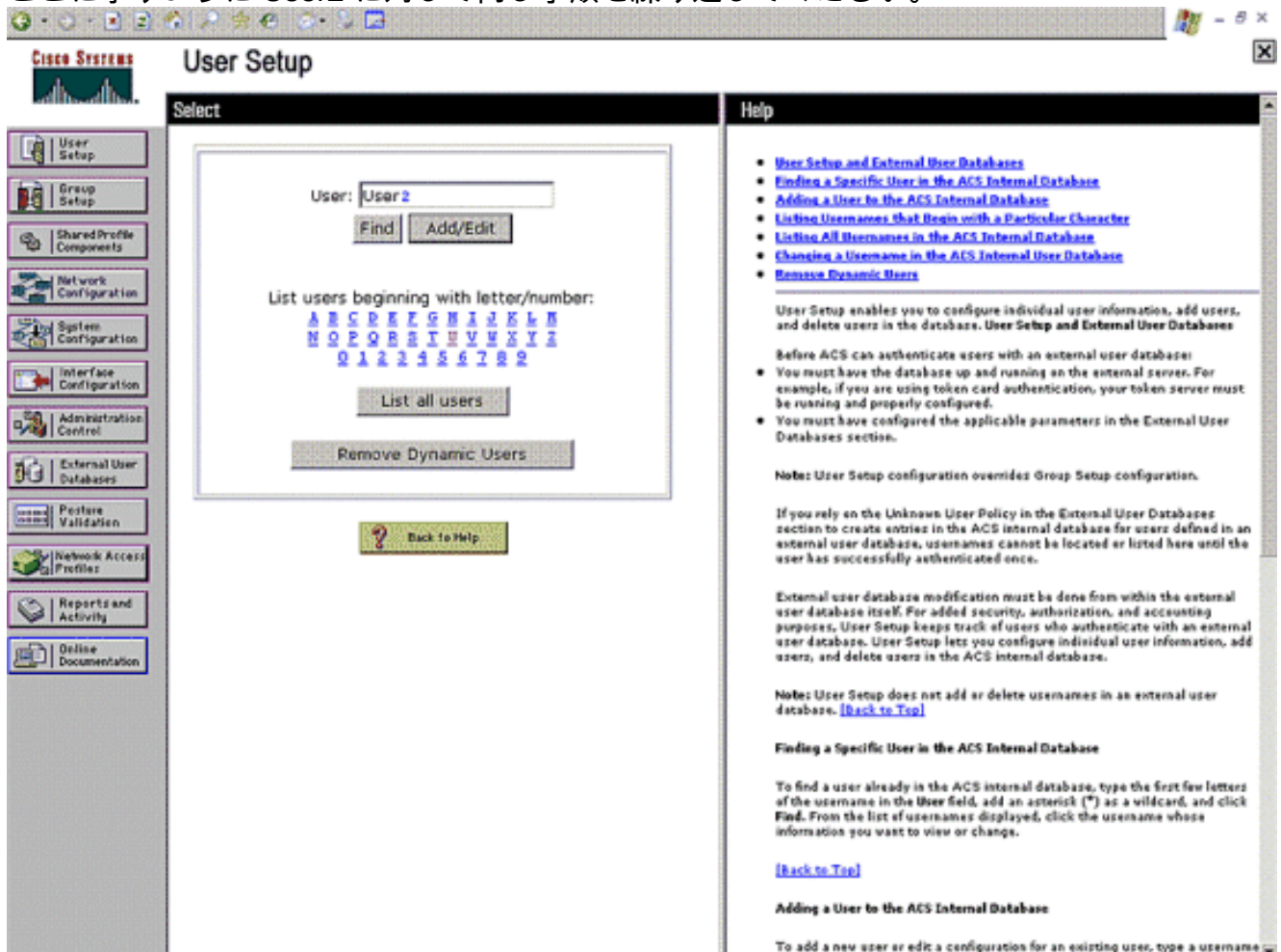
Supplementary User Info

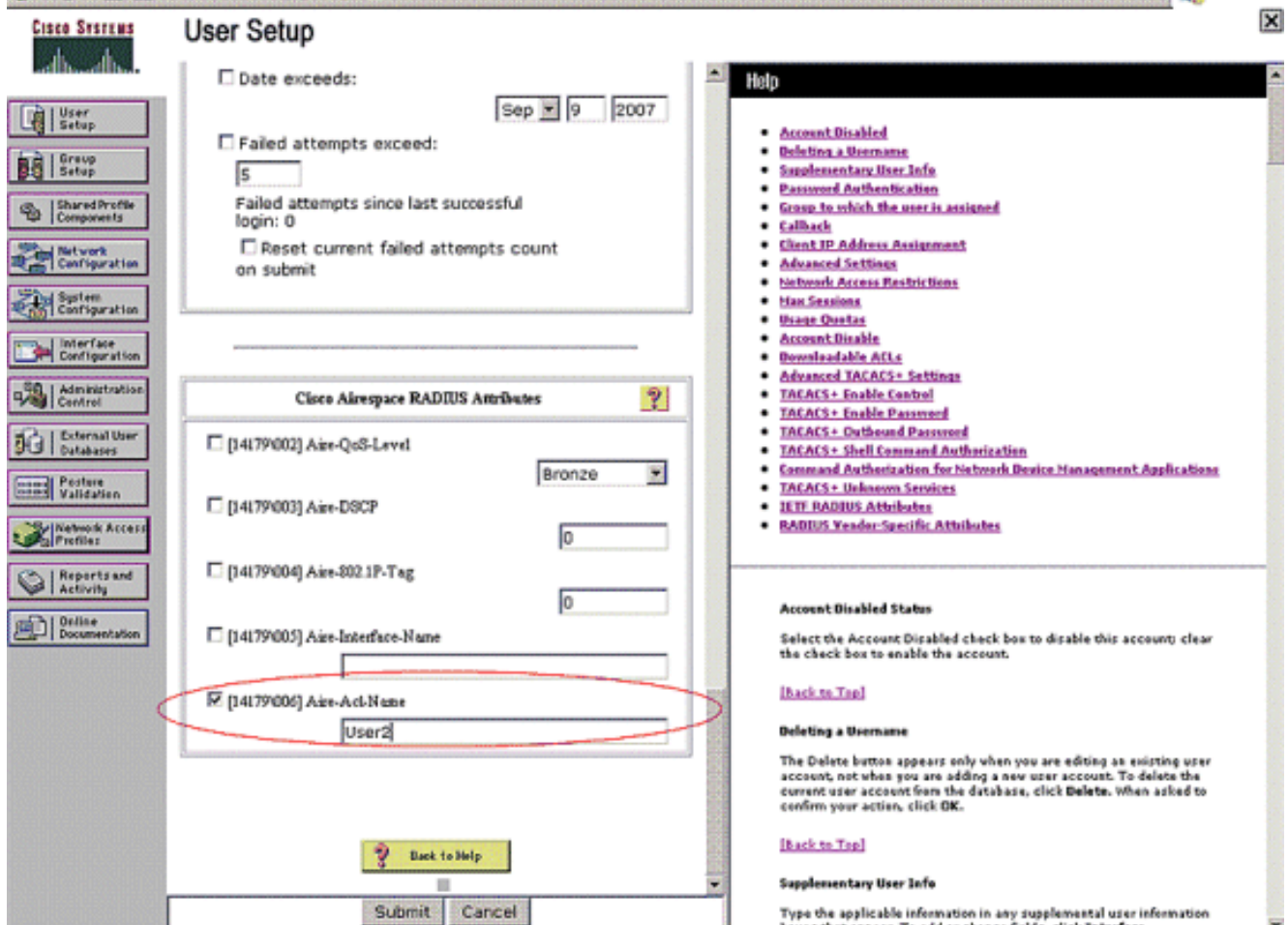
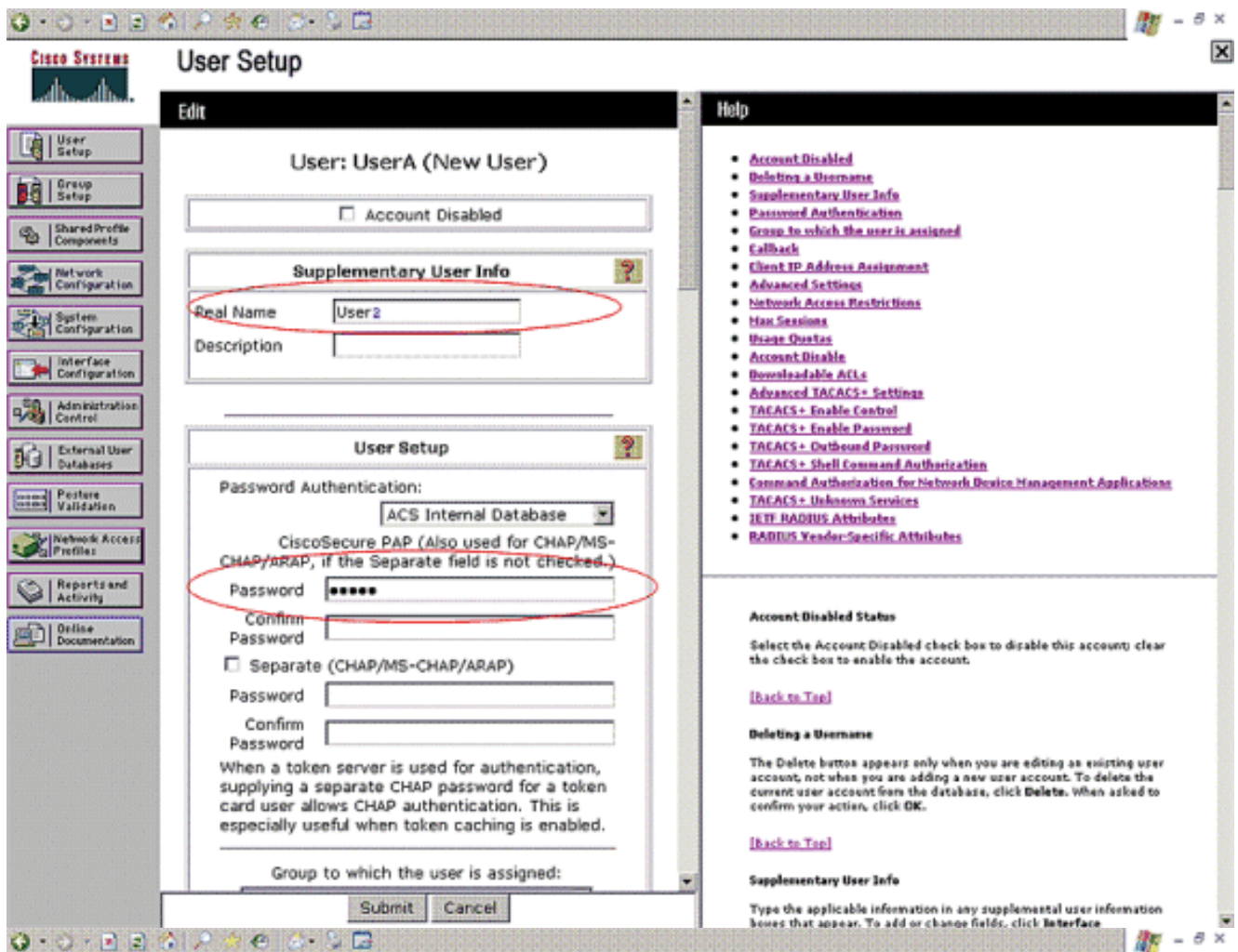
Type the applicable information in any supplemental user information boxes that appear. To add or change fields, click **Interface**

ユーザに固有の Cisco Airespace RADIUS 属性が表示されるまで下にスクロールします。
[Aire-ACL-Name] をクリックして、認証成功が戻ってきた際に、ACS が ACL 名を WLC に返せるようにします。User1 用に WLC 上で ACL User1 を作成します。ACL の名前を User1 として入力します。



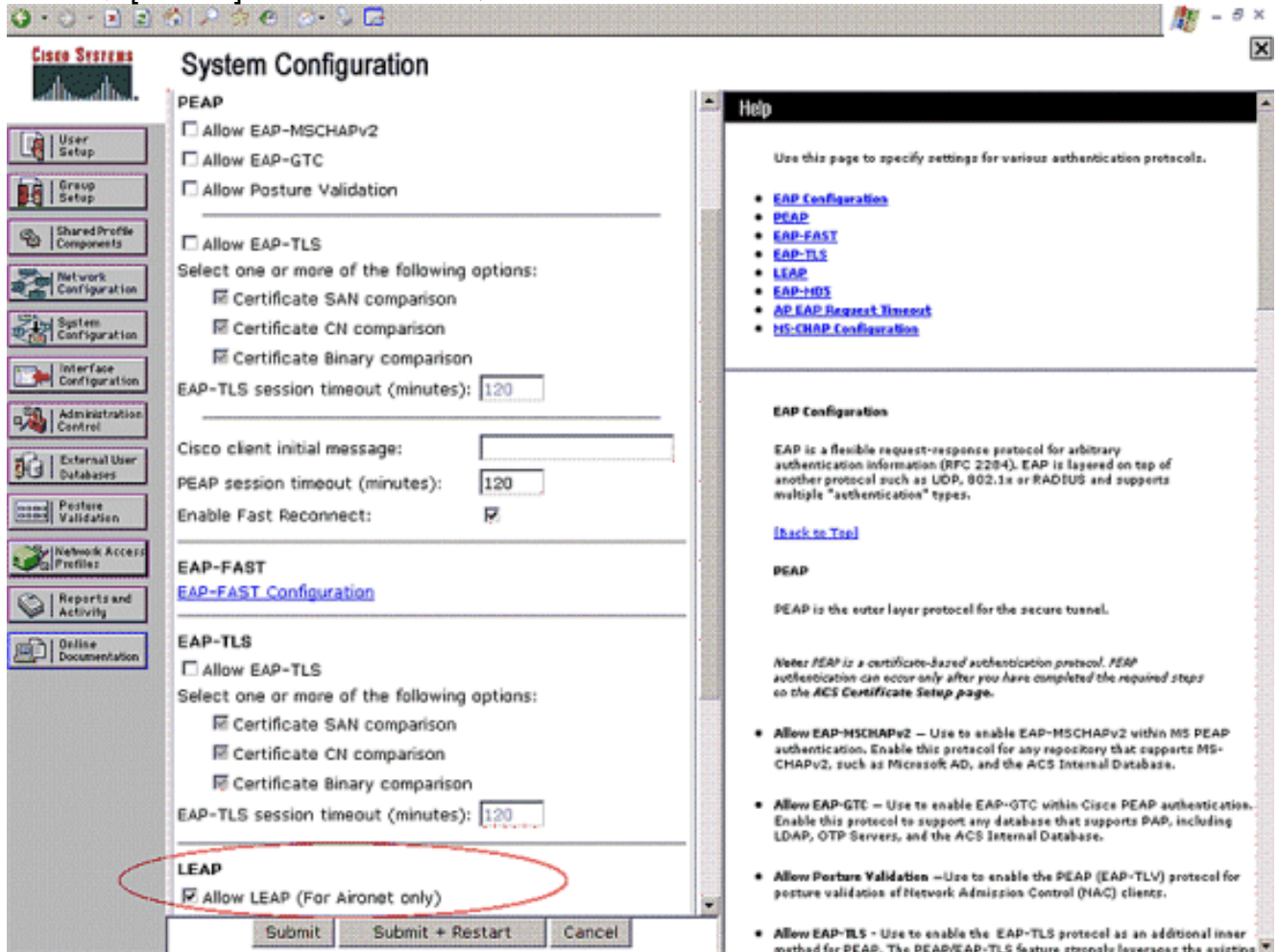
3. ここに示すように User2 に対して同じ手順を繰り返してください。





4. 意図した 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には

、[System Configuration]、[Global Authentication Setup] をクリックします。EAP の設定で、適切な EAP 方法を選択します。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。



The screenshot shows the Cisco System Configuration interface. On the left is a navigation menu with options like 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, and Online Documentation. The main content area is titled 'System Configuration' and contains sections for PEAP, EAP-FAST, EAP-TLS, and LEAP. The LEAP section is circled in red and shows the checkbox 'Allow LEAP (For Aironet only)' checked. Below the LEAP section are buttons for 'Submit', 'Submit + Restart', and 'Cancel'. On the right, a 'Help' window is open, displaying information about EAP Configuration, including a list of links for EAP-Configuration, PEAP, EAP-FAST, EAP-TLS, LEAP, EAP-TLS, AP EAP Request Timeout, and MS-CHAP Configuration. The help text explains that EAP is a flexible request-response protocol for arbitrary authentication information (RFC 2284) and is layered on top of another protocol such as UDP, 802.1x or RADIUS and supports multiple "authentication" types.

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。

設定が意図したとおりに動作することを確認するには、LEAP 認証を使用して、ワイヤレスクライアントと Lightweight AP の関連付けを試みます。

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の詳細は、[EAP 認証の使用方法を参照してください](#)。

ワイヤレスクライアント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。これは、User1 が LAP への認証を試行した場合に発生します。

Enter Wireless Network Password [X]

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

User Name :

Password :

Log on to :

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

Profile Name : Office

Lightweight AP および続いて WLC が、クレデンシャルを検証するために、ユーザのクレデンシャルを外部 RADIUS サーバ (Cisco Secure ACS) に渡します。RADIUS サーバは、データをユーザ データベースと比較し、認証に成功したら、ユーザに設定された ACL 名を WLC に返します。この場合、ACL User1 が WLC に返されます。

Cisco Aironet Desktop Utility - Current Profile: Office-TSWEB [?] [X]

Action Options Help

Current Status Profile Management Diagnostics

CISCO SYSTEMS

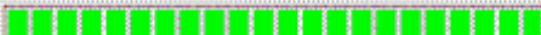
Profile Name: Office-TSWEB

Link Status: Authenticated Network Type: Infrastructure

Wireless Mode: 5 GHz 54 Mbps Current Channel: 64

Server Based Authentication: LEAP Data Encryption: WEP

IP Address: 172.16.0.14

Signal Strength:  Excellent

ワイヤレスLANコントローラ(WLC)はこのACLをUser1に適用します。このping出力は、User1がサーバ172.16.1.100にのみアクセスでき、他のデバイスにはアクセスできないことを示します。

```
D:\Documents and Settings\Administrator>ping 172.16.1.100
```

```
Pinging 172.16.1.100 with 32 bytes of data:
```

```
Reply from 172.16.1.100: bytes=32 time=3ms TTL=255
```

```
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
```

```
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
```

```
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
```

```
Ping statistics for 172.16.1.100:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 1ms, Maximum = 3ms, Average = 1ms
```

```
D:\Documents and Settings\Administrator>ping 172.16.1.50
```

```
Pinging 172.16.1.50 with 32 bytes of data:
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Ping statistics for 172.16.1.50:
```

```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

同様に、User2 が WLAN へのアクセスを試行した場合、認証に成功したら、RADIUS サーバは ACL User2 を WLC に返します。

Enter Wireless Network Password

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

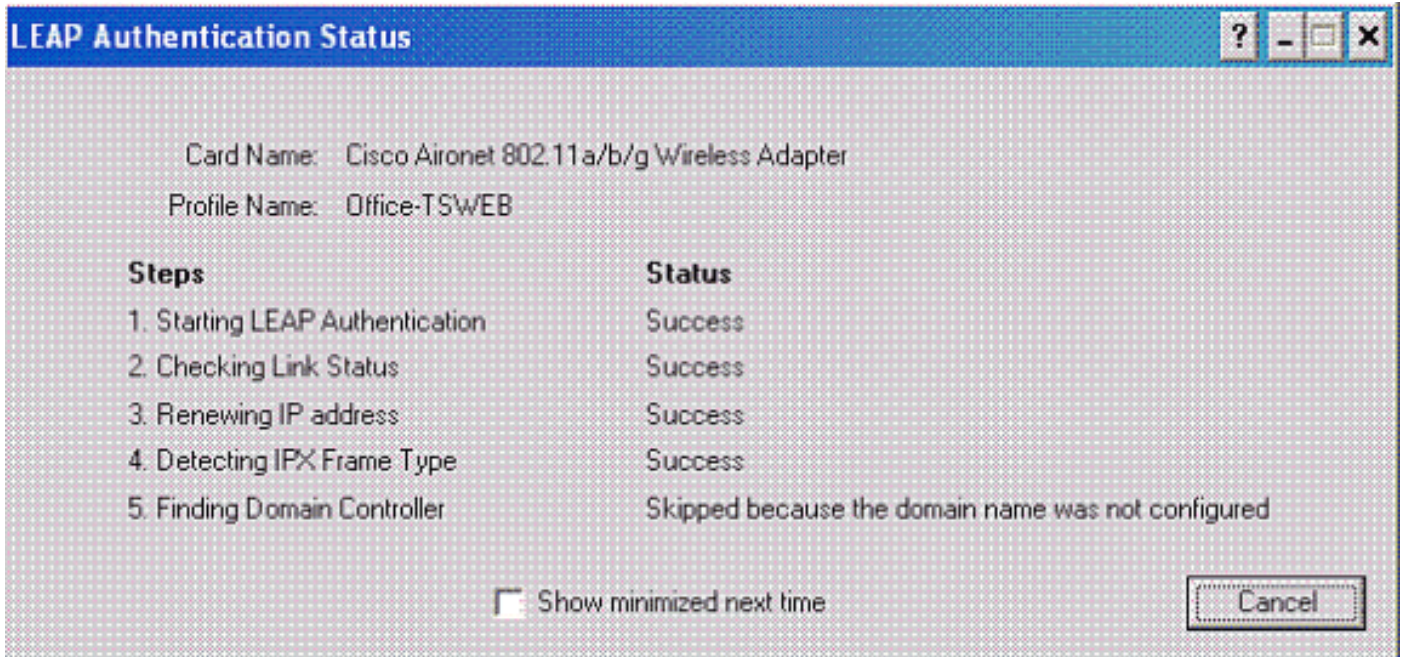
User Name :

Password :

Log on to :

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

Profile Name : Office



ワイヤレスLANコントローラ(WLC)はこのACLをUser2に適用します。このping出力は、User2がサーバ172.16.1.50にのみアクセスでき、他のデバイスにはアクセスできないことを示します。

```
D:\Documents and Settings\Administrator>ping 172.16.1.50
```

```
Pinging 172.16.1.50 with 32 bytes of data:
```

```
Reply from 172.16.1.50: bytes=32 time=3ms TTL=255
Reply from 172.16.1.50: bytes=32 time=18ms TTL=255
Reply from 172.16.1.50: bytes=32 time=1ms TTL=255
Reply from 172.16.1.50: bytes=32 time=1ms TTL=255
```

```
Ping statistics for 172.16.1.50:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 18ms, Average = 5ms
```

```
D:\Documents and Settings\Administrator>ping 172.16.1.100
```

```
Pinging 172.16.1.100 with 32 bytes of data:
```

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

```
Ping statistics for 172.16.1.100:
```

```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

ワイヤレス LAN コントローラで、AAA 認証のトラブルシューティングに次のデバッグ コマンドを使用することもできます。

- 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。
- debug dot1x packet enable : すべてのdot1xパケットのデバッグを有効にします
- debug client <MAC Address> : ワイヤレス クライアント デバッグを有効にします。

次に debug aaa all enable コマンドの例を示します。

注 : 出力の一部の行は、スペースの制約により2行目に移動しています。

```
Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xb1ab104
Thu Aug 16 14:42:54 2007:      Callback.....0x85ed228
Thu Aug 16 14:42:54 2007:      protocolType.....0x00140001
Thu Aug 16 14:42:54 2007:      proxyState.....00:40:96:AF:3E:93-03:01
Thu Aug 16 14:42:54 2007:      Packet contains 16 AVPs (not shown)
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Successful transmission of Authentication Packet
(id 1) to 10.77.244.196:1812, proxy state 00:40:96:af:3e:93-00:00
Thu Aug 16 14:42:54 2007: 00000000: 01 01 00 d0 2d 34 f5 99  b4 19 27 28 eb 5f 35 9c
....-4....'(_5.
Thu Aug 16 14:42:54 2007: 00000010: 8f a9 00 dd 01 07 75 73  65 72 31 1f 13 30 30 2d
.....user1..00-
Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46  2d 33 45 2d 39 33 1e 20
40-96-AF-3E-93..
Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35  2d 35 42 2d 46 42 2d 44
00-0B-85-5B-FB-D
Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65  2d 54 53 57 45 42 05 06
0:Office-TSWEB..
Thu Aug 16 14:42:54 2007: 00000050: 00 00 00 01 04 06 0a 4d  f4 d2 20 05 77 6c 63 1a
.....M....wlc.
Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00  00 00 01 06 06 00 00 00
...7c.....
Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d  06 00 00 00 13 40 06 00
.....=.....@..
Thu Aug 16 14:42:54 2007: 00000080: 00 00 0d 41 06 00 00 00  06 51 04 32 30 4f 27 02
...A.....Q.200'.
Thu Aug 16 14:42:54 2007: 00000090: 01 00 25 11 01 00 18 1d  87 9d 0b f9 dd e5 39 0d
..%......9.
Thu Aug 16 14:42:54 2007: 000000a0: 2e 82 eb 17 c6 23 b7 96  dc c3 55 ff 7c 51 4e 75
.....#.U.|QNu
Thu Aug 16 14:42:54 2007: 000000b0: 73 65 72 31 18 0a 53 56  43 3d 30 2e 31 3b 50 12
ser1..SVC=0.1;P.
Thu Aug 16 14:42:54 2007: 000000c0: 1a d5 3b 35 5e 93 11 c0  c6 2f 5e f5 65 e9 3e 2d
..;5^..../^e.>-
Thu Aug 16 14:42:54 2007: 00000000: 0b 01 00 36 8c 31 6a b4  27 e6 d4 0e 1b 8e 5d 19
...6.1j.'.....].
Thu Aug 16 14:42:54 2007: 00000010: 60 1c c2 16 4f 06 03 01  00 04 18 0a 53 56 43 3d
...O.....SVC=
Thu Aug 16 14:42:54 2007: 00000020: 30 2e 31 3b 50 12 6c fb  90 ec 48 9b fb d7 ce ca
0.1;P.l...H.....
Thu Aug 16 14:42:54 2007: 00000030: 3b 64 93 10 fe 09          ;d...
Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=11
Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=11
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Access-Challenge received from RADIUS server
10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3
Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800
Thu Aug 16 14:42:54 2007:      structureSize.....104
Thu Aug 16 14:42:54 2007:      resultCode.....255
Thu Aug 16 14:42:54 2007:      protocolUsed.....0x00000001
Thu Aug 16 14:42:54 2007:      proxyState.....
00:40:96:AF:3E:93-03:01
Thu Aug 16 14:42:54 2007:      Packet contains 3 AVPs (not shown)
```


Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xb1ab104
Thu Aug 16 14:42:54 2007: Callback.....0x85ed228
Thu Aug 16 14:42:54 2007: protocolType.....0x00140001
Thu Aug 16 14:42:54 2007: proxyState.....
00:40:96:AF:3E:93-03:02
Thu Aug 16 14:42:54 2007: Packet contains 16 AVPs (not shown)
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Successful transmission of Authentication Packet (id 2) to 10.77.244.196:1812,
proxy state 00:40:96:af:3e:93-00:00
Thu Aug 16 14:42:54 2007: 00000000: 01 02 00 c0 38 b6 b2 20 ff 5b f2 16 64 df 02 61
....8....[.d..a
Thu Aug 16 14:42:54 2007: 00000010: cf f5 93 4b 01 07 75 73 65 72 31 1f 13 30 30 2d
...K..User1..00-
Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46 2d 33 45 2d 39 33 1e 20
40-96-AF-3E-93..
Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35 2d 35 42 2d 46 42 2d 44
00-0B-85-5B-FB-D
Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65 2d 54 53 57 45 42 05 06
0:Office..
Thu Aug 16 14:42:54 2007: 00000050: 00 00 00 01 04 06 0a 4d f4 d2 20 05 77 6c 63 1a
.....M....wlc.
Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00 00 00 01 06 06 00 00 00
...7c.....
Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d 06 00 00 00 13 40 06 00
.....=.....@..
Thu Aug 16 14:42:54 2007: 00000080: 00 00 0d 41 06 00 00 00 06 51 04 32 30 4f 17 01
...A.....Q.200..
Thu Aug 16 14:42:54 2007: 00000090: 01 00 15 11 01 00 08 0f 14 05 65 1b 28 61 c9 75
.....e.(a.u
Thu Aug 16 14:42:54 2007: 000000a0: 73 65 72 31 18 0a 53 56 43 3d 30 2e 31 3b 50 12
ser1..SVC=0.1;P.
Thu Aug 16 14:42:54 2007: 000000b0: 05 ba 6b af fe a4 b0 d1 a2 94 f8 39 80 ca 3c 96
..k.....9.<.
Thu Aug 16 14:42:54 2007: 00000000: 02 02 00 ce c9 3d 5d c8 6c 07 8e fb 58 84 8d f6
.....=].l...X...
Thu Aug 16 14:42:54 2007: 00000010: 33 6d 93 21 08 06 ff ff ff ff 4f 27 02 01 00 25
3m.!.....O'...%
Thu Aug 16 14:42:54 2007: 00000020: 11 01 00 18 e5 e5 31 1e 33 b5 4e 69 90 e7 84 25
.....1.3.Ni...%
Thu Aug 16 14:42:54 2007: 00000030: 42 a9 20 ac 84 33 9f 87 ca dc c9 b3 75 73 65 72
B....3.....user
Thu Aug 16 14:42:54 2007: 00000040: 31 1a 3b 00 00 00 09 01 35 6c 65 61 70 3a 73 65
1.;.....5leap:se
Thu Aug 16 14:42:54 2007: 00000050: 73 73 69 6f 6e 2d 6b 65 79 3d 29 80 1d 2c 1c 85
ssion-key=)....
Thu Aug 16 14:42:54 2007: 00000060: db 1c 29 7e 40 8a b8 93 69 2a 55 d2 e5 46 89 8b
..)~@...i*U..F..
Thu Aug 16 14:42:54 2007: 00000070: 2c 3b 65 49 3e 44 cf 7e 95 29 47 54 1a 1f 00 00
;;eI>D.~.)GT....
Thu Aug 16 14:42:54 2007: 00000080: 00 09 01 19 61 75 74 68 2d 61 6c 67 6f 2d 74 79
....auth-algo-ty
Thu Aug 16 14:42:54 2007: 00000090: 70 65 3d 65 61 70 2d 6c 65 61 70 1a 0d 00 00 37
pe=eap-leap....7
Thu Aug 16 14:42:54 2007: 000000a0: 63 06 07 55 73 65 72 31 19 14 43 41 43 53 3a 30
c..User1..CACS:0
Thu Aug 16 14:42:54 2007: 000000b0: 2f 39 2f 61 34 64 66 34 64 32 2f 31 50 12 9a 71
/9/a4df4d2/1P..q
Thu Aug 16 14:42:54 2007: 000000c0: 09 99 7d 74 89 ad af e5 c8 b1 71 94 97 d1
..}t.....q...
Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=2
Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=2
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93

Access-Accept received from RADIUS server

10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3

```

Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800
Thu Aug 16 14:42:54 2007:      structureSize.....236
Thu Aug 16 14:42:54 2007:      resultCode.....0
Thu Aug 16 14:42:54 2007:      protocolUsed.....0x0
0000001
Thu Aug 16 14:42:54 2007:      proxyState.....00:
40:96:AF:3E:93-03:02
Thu Aug 16 14:42:54 2007: Packet contains 6 AVPs:
Thu Aug 16 14:42:54 2007: AVP[01] Framed-IP-Address.....0xffffffff (-1)
(4 bytes)
Thu Aug 16 14:42:54 2007: AVP[02] EAP-Message.....DATA (37 bytes)
Thu Aug 16 14:42:54 2007: AVP[03] Cisco / LEAP-Session-Key...DATA (16 bytes)
Thu Aug 16 14:42:54 2007: AVP[04] Airespace / ACL-Name.....User1 (5 bytes)
Thu Aug 16 14:42:54 2007: AVP[05] Class.....CACs:0/9/a4df4d2/1
(18 bytes)
Thu Aug 16 14:42:54 2007: AVP[06] Message-Authenticator.....DATA (16 bytes)
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Applying new AAA override
for station 00:40:96:af:3e:93
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Override values
for station 00:40:96:af:3e:93
source: 4, valid bits: 0x400
qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
dataAvgC: -1, rTAVgC: -1, dataBurstC: -1, rTimeBurstC: -1
vlanIfName: '',
aclName:User1
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Inserting new RADIUS override into chain for station 00:40:96:af:3e:93

```

show wlan summary コマンドを組み合わせることで、どの WLAN で RADIUS サーバ認証が使用されているかがわかります。その後、show client summary コマンドを使用すると、RADIUS WLAN での認証に成功した MAC アドレス (クライアント) がわかります。また、この情報を、Cisco Secure ACS の成功した試行または失敗した試行のログと関連させることもできます。

正しく設定したことを確認するために、ワイヤレスクライアントを使用して ACL 設定をテストすることを推奨します。正しく動作しない場合は、ACL Web ページで ACL を確認し、ACL に対する変更がコントローラのインターフェイスに適用されたことを確認してください。

設定は、次の show コマンドを使用して確認することもできます。

- **show acl summary** : コントローラ上に設定されている ACL を表示するには、show acl summary コマンドを使用します。

以下が一例です。

```
(Cisco Controller) >show acl summary
```

ACL Name	Applied
User1	Yes
User2	Yes

- **show acl detailed <ACL_Name>** : 設定された ACL の詳細情報を表示します。以下が一例です。注 : 出力の一部の行は、スペースの制約により2行目に移動しています。

```
Cisco Controller) >show acl detailed User1
```

		Source		Destination	
	Source Port	Dir	Dest Port		
I	Prot	Range	Range	DSCP	Action
1	In	172.16.0.0/255.255.0.0			172.16.1.100/255.255.255.255
	Any	0-65535	0-65535	Any	Permit
2	Out	172.16.1.100/255.255.255.255			172.16.0.0/255.255.0.0
	Any	0-65535	0-65535	Any	Permit

(Cisco Controller) >show acl detailed User2

		Source		Destination	
	Source Port	Dir	Dest Port		
I	Prot	Range	Range	DSCP	Action
1	In	172.16.0.0/255.255.0.0			172.16.1.50/255.255.255.255
	Any	0-65535	0-65535	Any	Permit
2	Out	172.16.1.50/255.255.255.255			172.16.0.0/255.255.0.0
	Any	0-65535	0-65535	Any	Permit

- **show client detail <MAC Address of the client>** : ワイヤレス クライアントに関する詳細情報を表示します。

[トラブルシューティングのヒント](#)

トラブルシューティングには、次のヒントを使用します。

- コントローラで、RADIUS サーバがアクティブ状態であり、スタンバイや無効状態ではないことを確認します。
- コントローラの WLAN (SSID) のドロップダウン メニューで RADIUS サーバが選択されていることを確認します。
- RADIUS サーバがワイヤレス クライアントから認証要求を受信して検証するかどうかを確認します。
- そのためには、ACS サーバで Passed Authentications レポートと Failed Attempts レポートを調べます。これらのレポートは、ACS サーバの [Reports and Activities] で見ることができます。

[関連情報](#)

- [ワイヤレス LAN コントローラの ACL : ルール、制約事項、および例](#)
- [Wireless LAN Controller での ACL の設定例](#)
- [無線 LAN コントローラ \(WLC \) を使用した MAC フィルタの設定例](#)
- [Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 5.2](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)