RADIUS サーバによる Wireless LAN コントローラのロビー管理者の認証

内容

概要

このドキュメントでは、RADIUS サーバを使用したワイヤレス LAN コントローラ（WLC）のロビー管理者の認証に関連した設定手順について説明します。

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。

- WLC の基本パラメータの設定方法に関する知識
- Cisco Secure ACS などの RADIUS サーバの設定方法に関する知識
- WLC のゲスト ユーザの知識

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 7.0.216.0 が稼働する Cisco 4400 ワイヤレス LAN コントローラ。
- この設定では、ソフトウェア バージョン 4.1 が稼働する Cisco Secure ACS を RADIUS サーバとして使用します。

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

WLC のロビー アンバサダーとも呼ばれるロビー管理者は、ワイヤレス LAN コントローラ（WLC）上でゲスト ユーザ アカウントを作成して管理できます。 ロビー アンバサダーは、設定権限が制限されており、ゲスト アカウントの管理に使用される Web ページにしかアクセスできません。ロビー アンバサダーは、ゲスト ユーザ アカウントを利用できる時間を指定できます。指定した時間を経過すると、ゲスト ユーザ アカウントは、自動的に無効になります。

ゲスト ユーザの詳細については、「導入ガイド：シスコ ワイヤレス LAN コントローラを使用したシスコ ゲスト アクセス」を参照してください。

WLC 上でゲスト ユーザ アカウントを作成するには、ロビー管理者としてコントローラにログインする必要があります。このドキュメントでは、RADIUS サーバから返される属性に基づいてユーザがロビー管理者として WLC に対してどのように認証されるかについて説明します。

注：ロビー管理者の認証は、WLCでローカルに設定されたロビー管理者アカウントに基づいて実行することもできます。コントローラ上でロビー管理者アカウントをローカルに作成する方法については、「ロビー アンバサダー アカウントの作成」を参照してください。

設定

ここでは、このドキュメントの目的に従って WLC と Cisco Secure ACS を設定する方法について説明します。

設定

このドキュメントでは、次の構成を使用します。

- WLC の管理インターフェイス IP アドレスは 10.77.244.212/27 です。
- RADIUS サーバの IP アドレスは 10.77.244.197/27 です。
- アクセス ポイント（AP）と RADIUS サーバで使用される共有秘密キーは cisco123 です。
- RADIUS サーバで設定されたロビー管理者のユーザ名とパスワードはどちらも lobbyadmin です。

このドキュメントの設定例では、lobbyadmin というユーザ名とパスワードを使用してコントローラにログインするユーザにロビー管理者の役割を割り当てます。

WLC の設定

必要な WLC の設定を開始する前に、コントローラがバージョン 4.0.206.0 以降を実行していることを確認します。これは、ユーザ名が RADIUS データベースに保存されている場合にコントロー

ラの Web インターフェイスに LobbyAdmin ユーザの間違った Web ページが表示されるシスコバグ ID CSCsg89868（登録ユーザ専用）によるものです。LobbyAdmin は、LobbyAdmin インターフェイスではなく ReadOnly インターフェイスに表示されます。

このバグはWLCバージョン4.0.206.0で解決されています。したがって、コントローラのバージョンが4.0.206.0以降であることを確認してください。コントローラを適切なバージョンにアップグレードする方法については、「ワイヤレス LAN コントローラ（WLC）ソフトウェアのアップグレード」を参照してください。

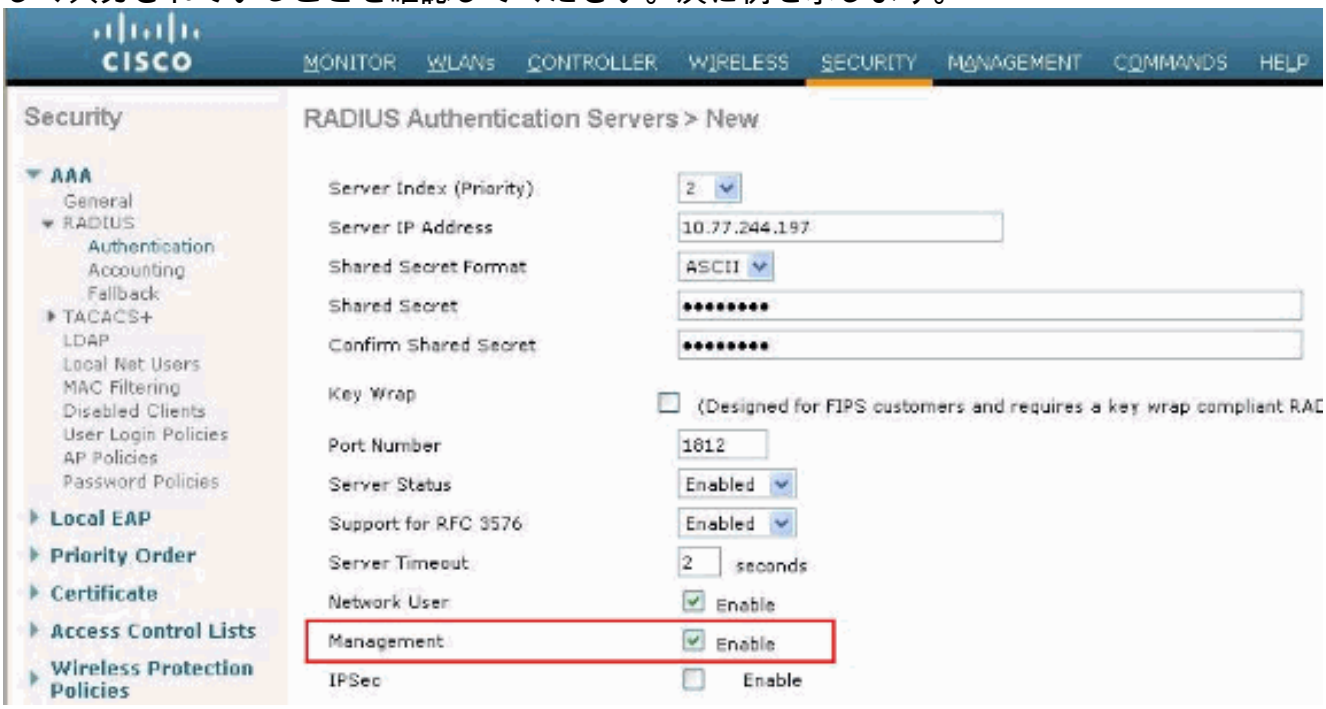
RADIUS サーバを使用してコントローラ管理認証を実行するには、コントローラ上で **Admin-auth-via-RADIUS フラグが有効になっていることを確認します。**これは **show radius summary コマンドの出力で確認できます。**

最初のステップは、コントローラ上で RADIUS サーバ情報を設定して、コントローラと RADIUS サーバ間のレイヤ 3 到達可能性を確立することです。

コントローラでの RADIUS サーバ情報の設定

次の手順を実行して、ACS に関する詳細で WLC を設定します。

1. WLC GUI から、[Security] **タブを選択し、ACS サーバの IP アドレスと共有秘密を設定します。**WLC が ACS と通信するためには、この共有秘密が ACS 上の共有秘密と一致している必要があります。**注：** ACS 共有秘密は大文字と小文字が区別されます。共有秘密情報が正しく入力されていることを確認してください。次に例を示します。



2. ステップ1の図に示すようにACSがWLCユーザを管理できるようにするには、[Management]チェックボックスをオンにします。次に、[Apply]をクリックします。
3. **ping コマンドを使用して、コントローラと設定した RADIUS サーバ間のレイヤ 3 到達可能性を確認します。**この ping オプションは、WLC GUI の [Security] > [RADIUS Authentication] **タブで設定された RADIUS サーバ ページでも使用できます。**次の図は、RADIUS サーバからの正常な ping 応答を示しています。したがって、コントローラと RADIUS サーバ間でレイヤ 3 到達可能性が使用できます。

RADIUS サーバの設定

次の手順を実行して、RADIUS サーバを設定します。

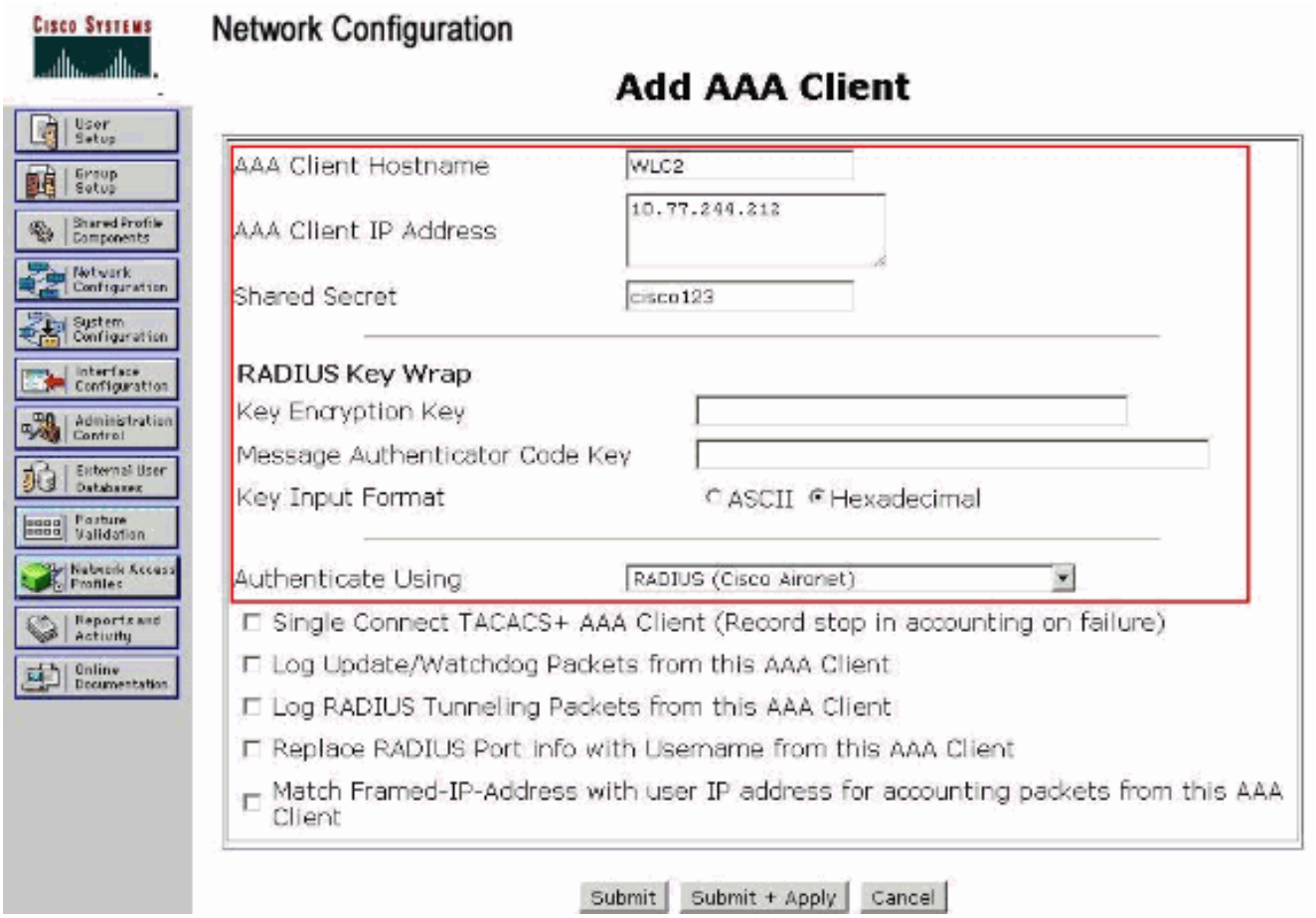
1. WLC を AAA クライアントとして RADIUS サーバに追加する
2. 口ビー管理者に適切な RADIUS IETF Service-Type 属性を設定する

WLC を AAA クライアントとして RADIUS サーバに追加する

次の手順を実行して、RADIUS サーバに WLC を AAA クライアントとして追加します。前述したように、このドキュメントでは ACS を RADIUS サーバとして使用します。この設定では、任意の RADIUS サーバを使用できます。

次の手順を実行して、WLC を AAA クライアントとして ACS に追加します。

1. ACS GUI で、[Network Configuration] **タブを選択します。**
2. AAA Clients の下で **[Add Entry]** をクリックします。
3. [Add AAA Client] ウィンドウで、WLC のホスト名、WLC の IP アドレス、および共有秘密キーを入力します。ステップ 5 の図を参照してください。
4. Authenticate Using ドロップダウン メニューから、RADIUS (Cisco Aironet) を選択します。
5. 設定を保存するには、**Submit + Restart** をクリックします。

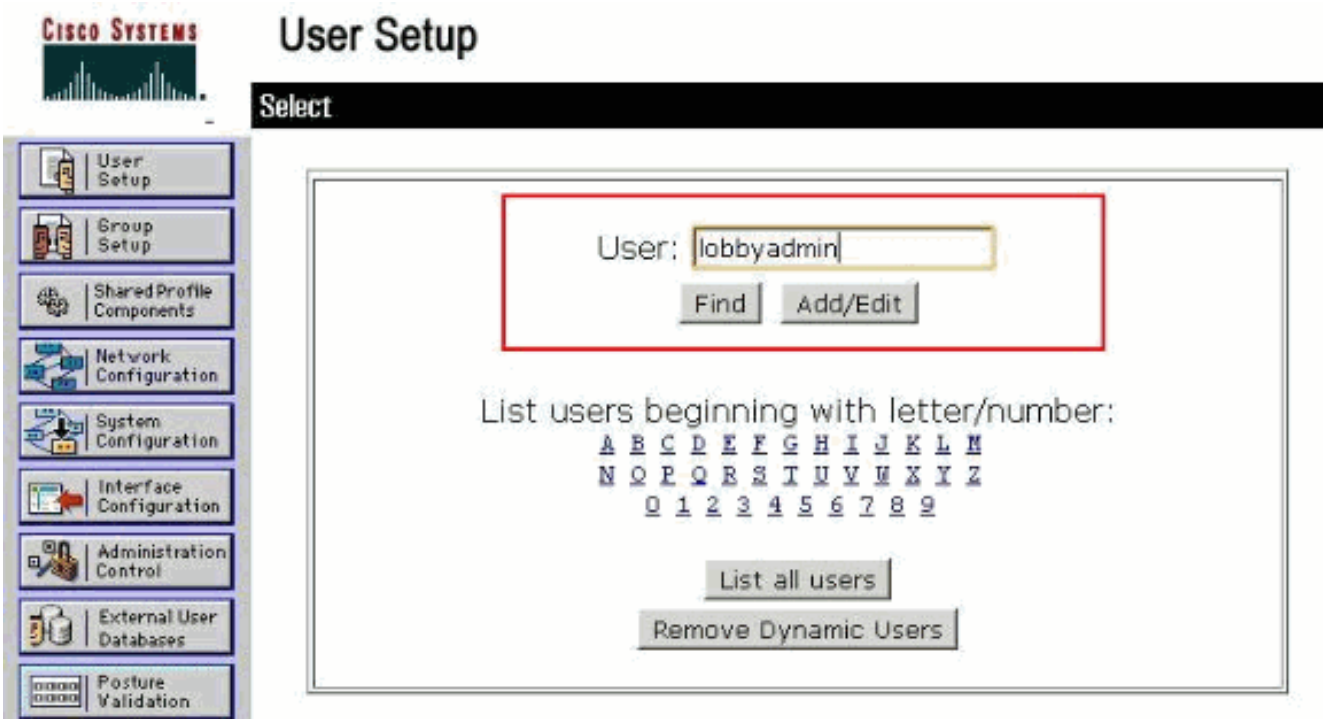


ロビー管理者に適切な RADIUS IETF Service-Type 属性を設定する

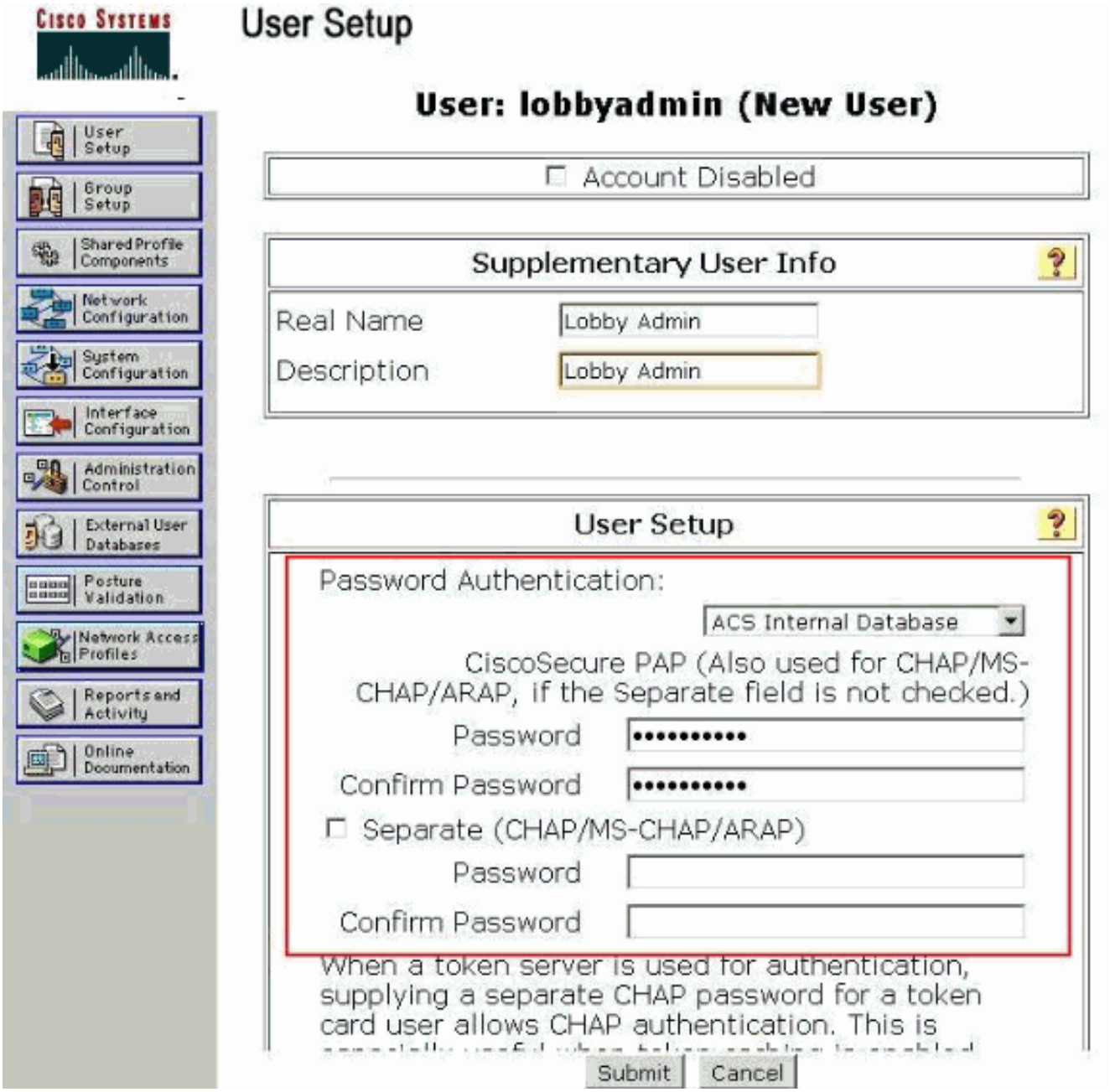
RADIUS サーバ経由でコントローラの管理ユーザをロビー管理者として認証するには、IETF RADIUS Service-Type 属性を [Callback Administrative] に設定した RADIUS データベースにユーザを追加する必要があります。この属性は、コントローラ上で特定のユーザにロビー管理者の役割を割り当てます。

このドキュメントでは、ロビー管理者の例としてユーザ lobbyadmin を使用します。このユーザを設定するには、ACS 上で次の手順を実行します。

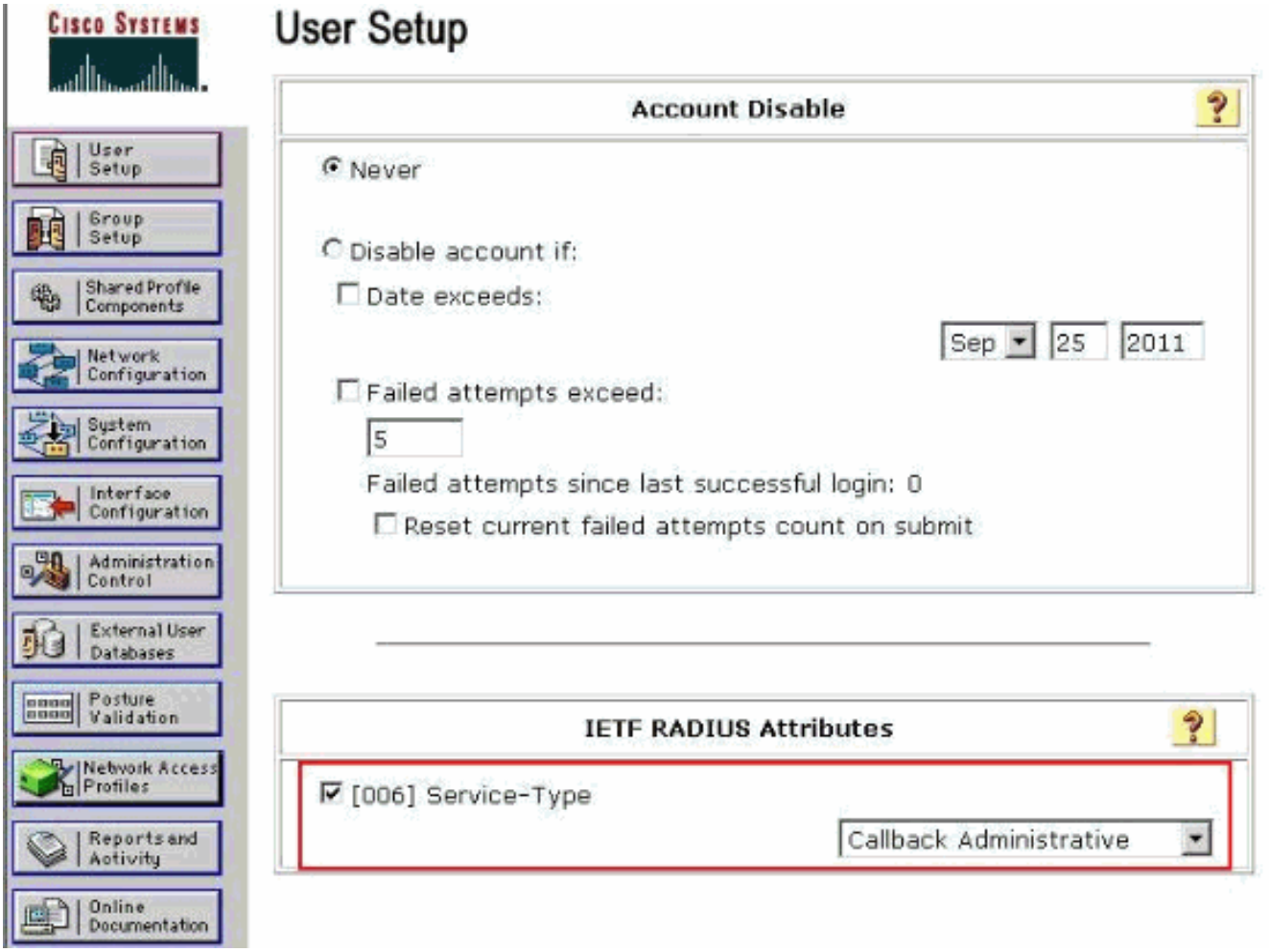
1. ACS GUI で、[User Setup] **タブを選択します。**
2. 次の例に示すように、ACS に追加するユーザ名を入力します。



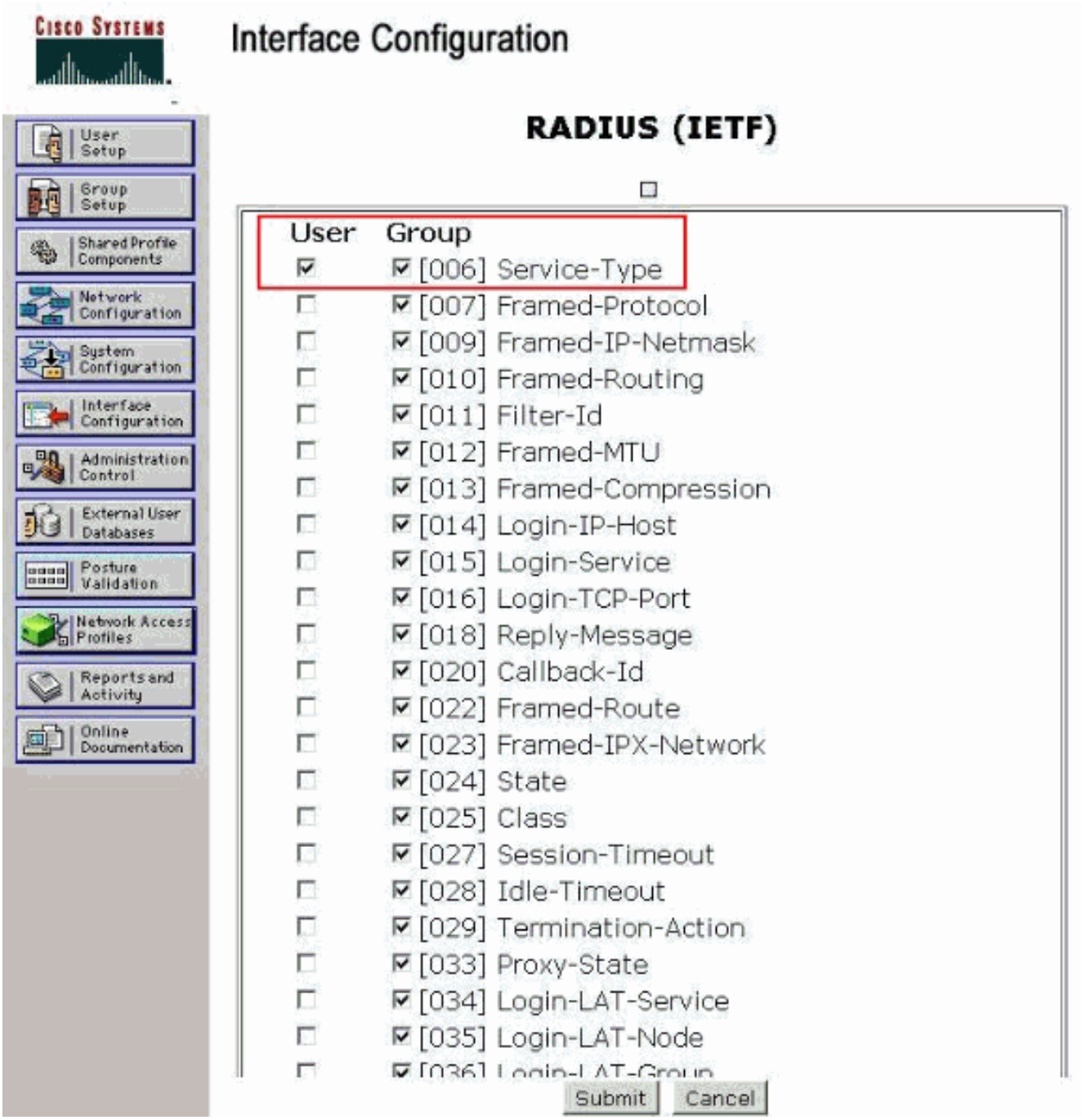
3. Add/Edit をクリックして、User Edit ページに移動します。
4. [User Edit] ページで、このユーザの [Real Name]、[Description]、および [Password] の詳細を入力します。この例では、使用するユーザ名とパスワードがどちらも lobbyadmin です。



5. [IETF RADIUS Attributes] 設定までスクロールダウンして、[Service-Type Attribute] **チェック ボックスをオンにします。**
6. [Service-Type] プルダウン メニューから [Callback Administrative] **を選択して、[Submit] をクリックします。**これがこのユーザに**ロビー管理者の役割を割り当てる属性です。**



場合によっては、この Service-Type アトリビュートがユーザ設定で表示されないことがあります。その場合は、次の手順を実行してそれが表示されるようにします。ACS の GUI から、IETF アトリビュートを有効にするために、[User Configuration] ウィンドウで [Interface Configuration] > [RADIUS (IETF)] の順に選択します。[RADIUS (IETF) Settings] ページが表示されます。RADIUS (IETF) の設定ページでは、ユーザ設定やグループ設定で表示する必要がある IETF アトリビュートを指定できます。この設定では、[User] カラムで [Service-Type] **にチェックマークを付けて、[Submit] をクリックします。**次に例を示します。



注：この例では、ユーザごとに認証を指定します。ユーザが属するグループ単位で認証を行うこともできます。その場合は、[Group] **チェック ボックスをオンにして、この属性がグループ設定に表示されるようにします。注：認証がグループベースの場合**は、特定のグループにユーザを割り当て、そのグループのユーザにアクセス権限を付与するようにグループ設定IETF属性を設定する必要があります。グループの設定方法と管理方法の詳細については、「ユーザ グループの管理」を参照してください。

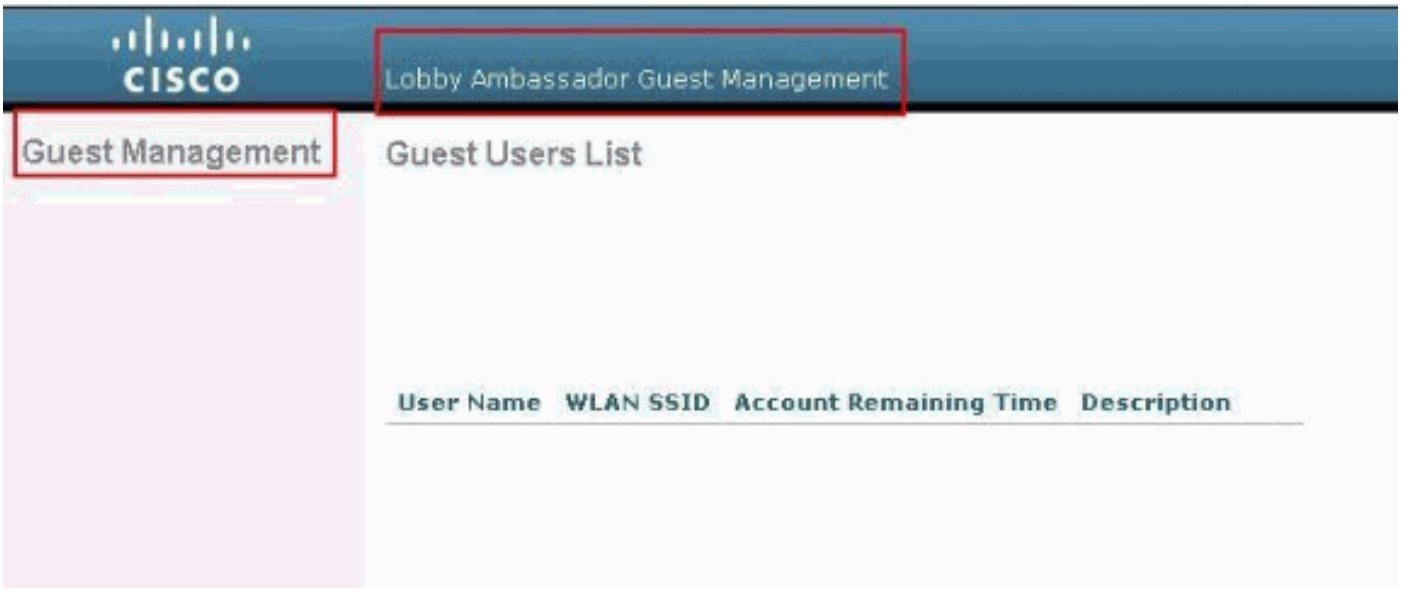
確認

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。

設定が正しく機能するかどうかを確認するには、GUI (HTTP/HTTPS) モードで WLC にアクセスします。

注：ロビーアンバサーはコントローラのCLIインターフェイスにアクセスできないため、コントローラのGUIからのみゲストユーザアカウントを作成できます。

ログイン プロンプトが表示されたら、ACS 上で設定したようにユーザ名とパスワードを入力します。設定が正しければ、**ロビー管理者**として WLC に認証されます。次の例は、認証が成功してからロビー管理者の GUI がどのように表示されるかを示しています。



注：ロビー管理者には、ゲストユーザ管理以外のオプションがないことがわかります。

CLI モードからそれを確認するには、読み取り/書き込み管理者としてコントローラに Telnet します。コントローラの CLI で **debug aaa all enable コマンドを発行します。**

```
(Cisco Controller) >debug aaa all enable

(Cisco Controller) >
*aaaQueueReader: Aug 26 18:07:35.072: ReProcessAuthentication previous proto 28,
 next proto 20001
*aaaQueueReader: Aug 26 18:07:35.072: AuthenticationRequest: 0x3081f7dc
*aaaQueueReader: Aug 26 18:07:35.072:   Callback.....................................0x10756dd0
*aaaQueueReader: Aug 26 18:07:35.072:   protocolType.................................0x00020001
*aaaQueueReader: Aug 26 18:07:35.072:
proxyState.....................................00:00:00:40:
00:00-00:00
*aaaQueueReader: Aug 26 18:07:35.072:   Packet contains 5 AVPs (not shown)
*aaaQueueReader: Aug 26 18:07:35.072: apfVapRadiusInfoGet: WLAN(0) dynamic int attributes
srcAddr:
0x0, gw:0x0, mask:0x0, vlan:0, dpPort:0, srcPort:0
*aaaQueueReader: Aug 26 18:07:35.073: 00:00:00:40:00:00 Successful transmission of
Authentication
Packet (id 39) to 10.77.244.212:1812, proxy state 00:00:00:40:00:00-00:01
*aaaQueueReader: Aug 26 18:07:35.073: 00000000: 01 27 00 47 00 00 00 00  00 00 00 00 00 00 00 00
.'.G............
*aaaQueueReader: Aug 26 18:07:35.073: 00000010: 00 00 00 00 01 0c 6c 6f  62 62 79 61 64 6d 69 6e
......lobbyadmin
*aaaQueueReader: Aug 26 18:07:35.073: 00000020: 02 12 5f 5b 5c 12 c5 c8  52 d3 3f 4f 4f 8e 9d 38
 .._[\...R.?OO..8
*aaaQueueReader: Aug 26 18:07:35.073: 00000030: 42 91 06 06 00 00 00 07  04 06 0a 4e b1 1a 20 09
B.........N....
*aaaQueueReader: Aug 26 18:07:35.073: 00000040: 57 4c 43 34 34 30 30 WLC4400
*radiusTransportThread: Aug 26 18:07:35.080: 00000000: 02 27 00 40 7e 04 6d 533d ed 79 9c b6 99
d1
f8  .'.@~.mS=.y.....
*radiusTransportThread: Aug 26 18:07:35.080: 00000010: d0 5a 8f 4f 08 06 ff ffff ff 06 06 00 00
00
```

```
0b  .Z.O...........
*radiusTransportThread: Aug 26 18:07:35.080: 00000020: 19 20 43 41 43 53 3a 302f 61 65 32 36 2f
61
34  ..CACS:0/ae26/a4
*radiusTransportThread: Aug 26 18:07:35.080: 00000030: 65 62 31 31 61 2f 6c 6f62 62 79 61 64 6d
69
6e  eb11a/lobbyadmin
*radiusTransportThread: Aug 26 18:07:35.080: ****Enter processIncomingMessages: response code=2
*radiusTransportThread: Aug 26 18:07:35.080: ****Enter processRadiusResponse: response code=2
*radiusTransportThread: Aug 26 18:07:35.080: 00:00:00:40:00:00 Access-Accept received from
RADIUS
server 10.77.244.212 for mobile 00:00:00:40:00:00 receiveId = 0
*radiusTransportThread: Aug 26 18:07:35.080: AuthorizationResponse: 0x13c73d50
*radiusTransportThread: Aug 26 18:07:35.080:    structureSize.............................118
*radiusTransportThread: Aug 26 18:07:35.080:    resultCode................................0
*radiusTransportThread: Aug 26 18:07:35.080:
protocolUsed.............................0x00000001
*radiusTransportThread: Aug 26 18:07:35.080:
proxyState...............................00:00:00:40:00:00-00:00
*radiusTransportThread: Aug 26 18:07:35.080:    Packet contains 3 AVPs:
*radiusTransportThread: Aug 26 18:07:35.080:        AVP[01] Framed-IP-
Address.....................0xffffffff (-1) (4 bytes)
*radiusTransportThread: Aug 26 18:07:35.080:        AVP[02] Service-
Type.............................0x0000000b (11) (4 bytes)
*radiusTransportThread: Aug 26 18:07:35.080:        AVP[03]
Class.....................................
CACS:0/ae26/a4eb11a/lobbyadmin (30 bytes)
*emWeb: Aug 26 18:07:35.084: Authentication succeeded for lobbyadmin
```

この出力で強調表示されている情報で、service-type 属性 11（Callback Administrative）が ACS サーバからコントローラに渡され、ユーザがロビー管理者としてログインしていることを確認できます。

次のコマンドが役に立つ場合があります。

- **debug aaa details enable**
- **debug aaa events enable**
- **debug aaa packets enable**

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。

トラブルシュート

ロビー アンバサダー権限でコントローラにログインした場合は、絶対に期限切れにならないアカウントである、有効期間値が **"0" のゲスト ユーザ アカウントを作成することができません。**このような状況では、「`Lifetime value cannot be 0`

これは、主にWLCバージョン4.0で見られるCisco Bug ID CSCsf32392(登録ユーザ専用)が原因です。このバグはWLCバージョン4.1で解決されています。

関連情報

- コントローラ上で管理ユーザの RADIUS サーバ認証を行うための設定例
- Cisco Unified Wireless Network TACACS+ の設定
- Cisco Wireless LAN Controller コンフィギュレーション ガイド Software Release 4.0：ユー

ザ アカウントの管理

- Wireless LAN Controller での ACL の設定例
- Wireless LAN Controller (WLC) に関する FAQ
- 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
- ワイヤレス LAN コントローラを使用した外部 Web 認証の設定例
- ワイヤレス LAN コントローラの Web 認証の設定例
- WLC を使用したゲスト WLAN と内部 WLAN の設定例
- テクニカル サポートとドキュメント – Cisco Systems