ワイヤレス LAN コントローラ スプラッシュ ページ リダイレクトの設定例

内容

概要

このドキュメントでは、ワイヤレス LAN コントローラのスプラッシュ ページ リダイレクト機能の設定方法を説明します。

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。

- LWAPP セキュリティ ソリューションに関する知識
- Cisco Secure ACS の設定方法に関する知識

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 バージョン 5.0 が稼働している Cisco 4400 シリーズ ワイヤレス LAN コントローラ（WLC）

- Cisco 1232 シリーズ Lightweight アクセス ポイント（LAP）
- ファームウェア バージョン 4.1 が稼働している Cisco Aironet 802.a/b/g ワイヤレス クライアント アダプタ
- バージョン 4.1 が稼働している Cisco Secure ACS サーバ
- サードパーティの外部 Web サーバ

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

スプラッシュ ページ Web リダイレクトは、ワイヤレス LAN コントローラ バージョン 5.0 から導入された機能です。この機能を使用すると、ユーザは 802.1x 認証の完了後に特定の Web ページにリダイレクトされます。リダイレクトは、ユーザがブラウザ（デフォルトのホーム ページが設定されている）を開いたとき、または URL へのアクセスを試行したときに実行されます。Web ページへのリダイレクトが完了すると、ユーザはネットワークにフル アクセスできます。

Remote Authentication Dial-In User Service（RADIUS）サーバでリダイレクト ページを指定できます。RADIUS サーバは、802.1x 認証に成功した時点で、Cisco av-pair url-redirect RADIUS 属性をワイヤレス LAN コントローラに返すように設定する必要があります。

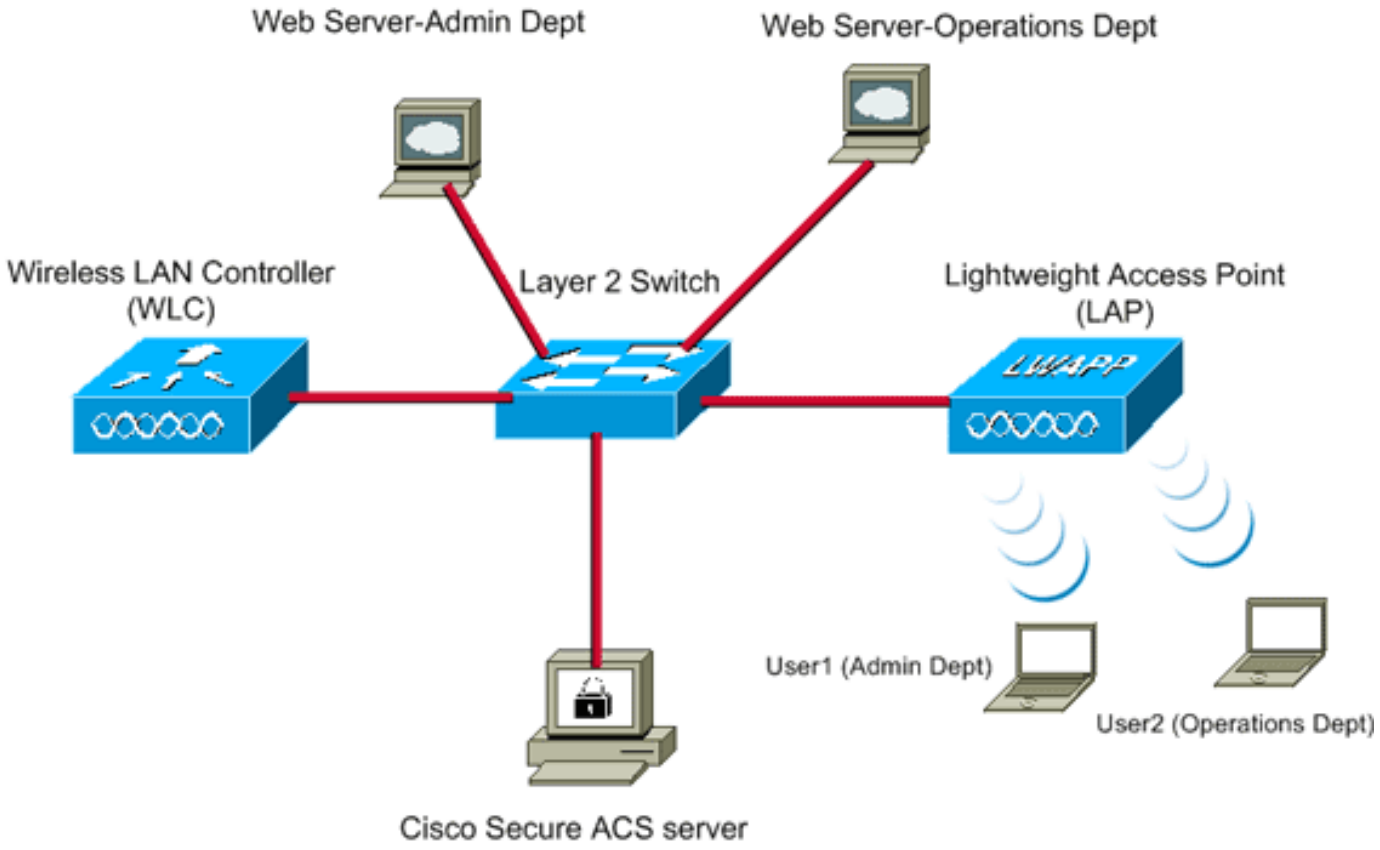
スプラッシュ ページ Web リダイレクト機能は、802.1x または WPA/WPA2 レイヤ 2 セキュリティに対して設定されている WLAN でのみ利用できます。

ネットワークのセットアップ

この例では、Cisco 4404 WLC と Cisco 1232 シリーズ LAP がレイヤ 2 スイッチを介して接続されています。Cisco Secure ACS サーバ（外部 RADIUS サーバとして機能）も同じスイッチに接続されています。すべてのデバイスは同じサブネット内にあります。

最初に LAP をコントローラに登録します。2つのWLANを作成する必要があります。1つは**管理部門**ユーザ用で、もう1つは**運用部門**ユーザ用です。どちらのワイヤレス LAN も WPA2/AES を使用します（EAP-FAST が認証に使用されます）。どちらの WLAN も、ユーザを適切なホーム ページ URL（外部 Web サーバ上）へリダイレクトするためにスプラッシュ ページ リダイレクト機能を使用します。

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。



WLC Management IP address:	10.77.244.204
WLC AP Manager IP address:	10.77.244.205
Wireless Client IP address:	10.77.244.221
Cisco Secure ACS server IP address	10.77.244.196
Subnet Mask used in this example	255.255.255.224

次のセクションでは、この構成でデバイスを設定する方法を説明します。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

スプラッシュ ページ リダイレクト機能を使用するようにデバイスを設定するには、次の手順を実行します。

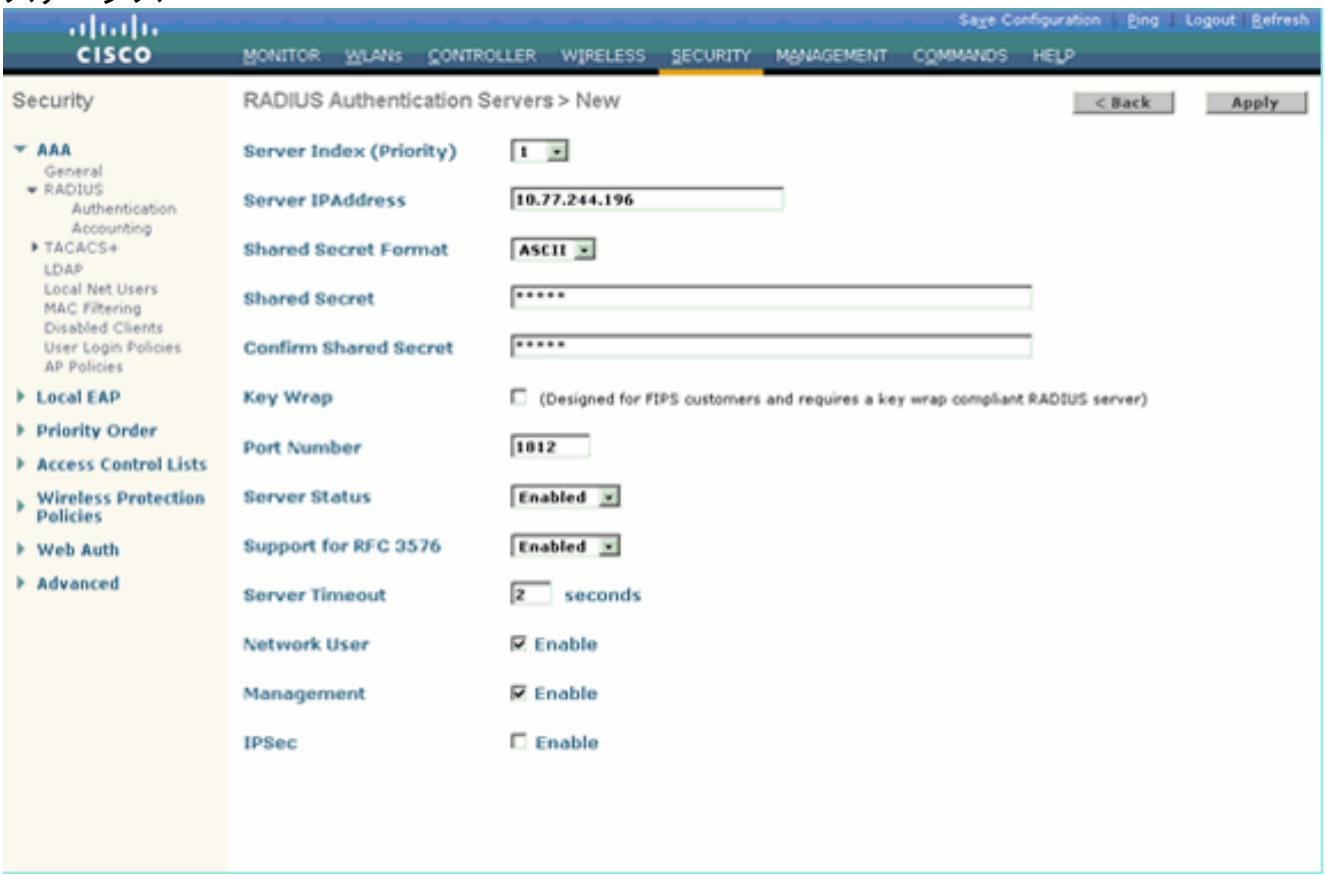
1. Cisco Secure ACS サーバを使用して RADIUS 認証用の WLC を設定する。
2. 管理部門および運用部門用の WLAN を設定する。
3. スプラッシュ ページ リダイレクト機能をサポートするように Cisco Secure ACS を設定する。

ステップ 1：Cisco Secure ACS サーバを使用して RADIUS 認証用の WLC を設定する。

ユーザ クレデンシャルを外部 RADIUS サーバに転送するには、WLC を設定する必要があります。

外部 RADIUS サーバ用に 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] と [RADIUS Authentication] をクリックして、[RADIUS Authentication Servers] ページを表示します。
2. [New] をクリックして、RADIUS サーバを定義します。
3. [RADIUS Authentication Servers] > [New] ページで RADIUS サーバのパラメータを定義します。次のパラメータがあります。RADIUS サーバの IP アドレス共有秘密ポート番号サーバ ステータス



このドキュメントでは、10.77.244.196 という IP アドレスを持つ ACS サーバを使用しています。

4. [Apply] をクリックします。

ステップ 2：管理部門および運用部門用の WLAN を設定する。

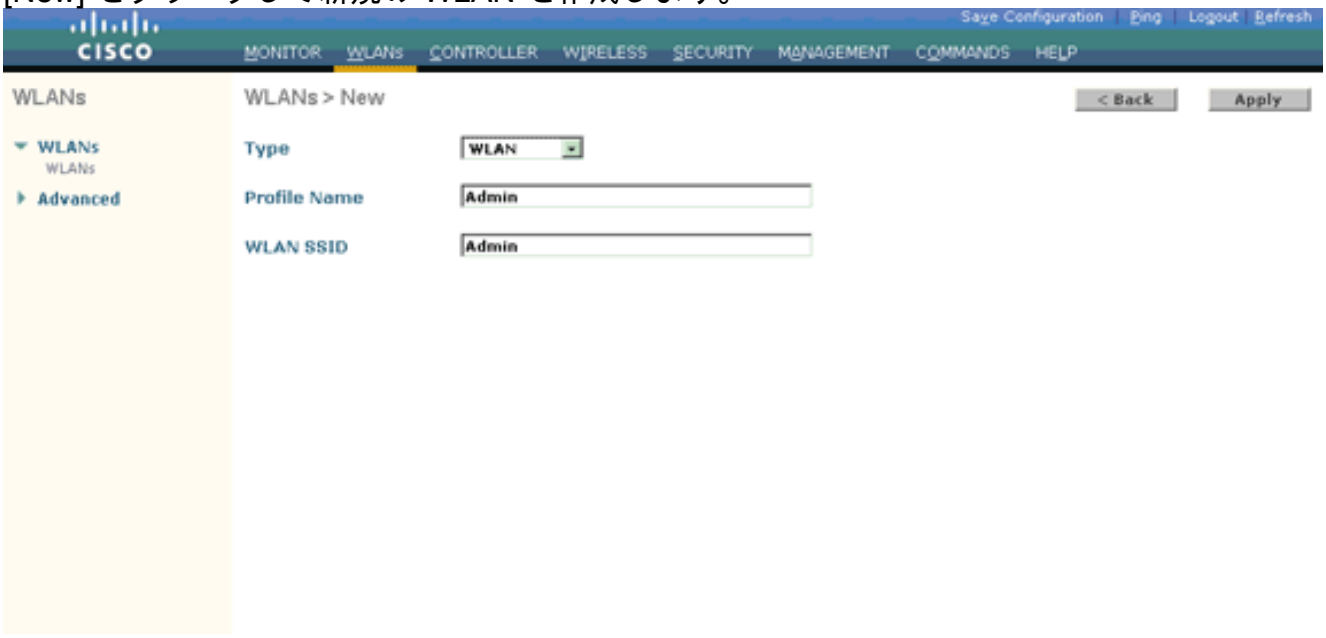
この手順では、クライアントがワイヤレス ネットワークに接続するために使用する 2 つの WLAN（1 つは管理部門用、もう 1 つは運用部門用）を設定します。

管理部門用の WLAN SSID は *Admin* です。運用部門用の WLAN SSID は Operations です。

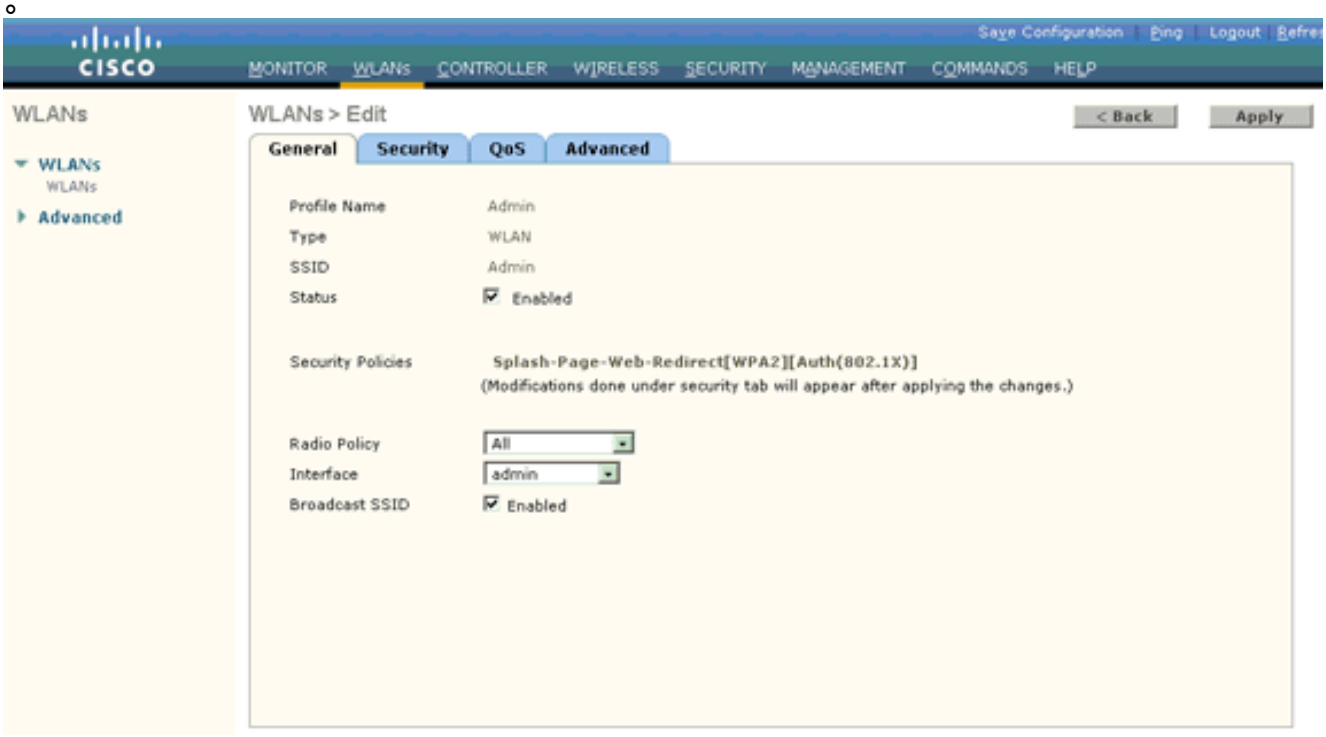
両方の WLAN と Web ポリシーで WPA2 をレイヤ 2 セキュリティ メカニズムとして有効にし、スプラッシュ ページ Web リダイレクト機能をレイヤ 3 セキュリティ方式として有効にするために、EAP-FAST 認証を使用します。

WLAN と関連するパラメータを設定するために、次の手順を実行します。

1. コントローラの GUI で [WLANs] をクリックして、[WLANs] ページを表示します。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. [New] をクリックして新規の WLAN を作成します。

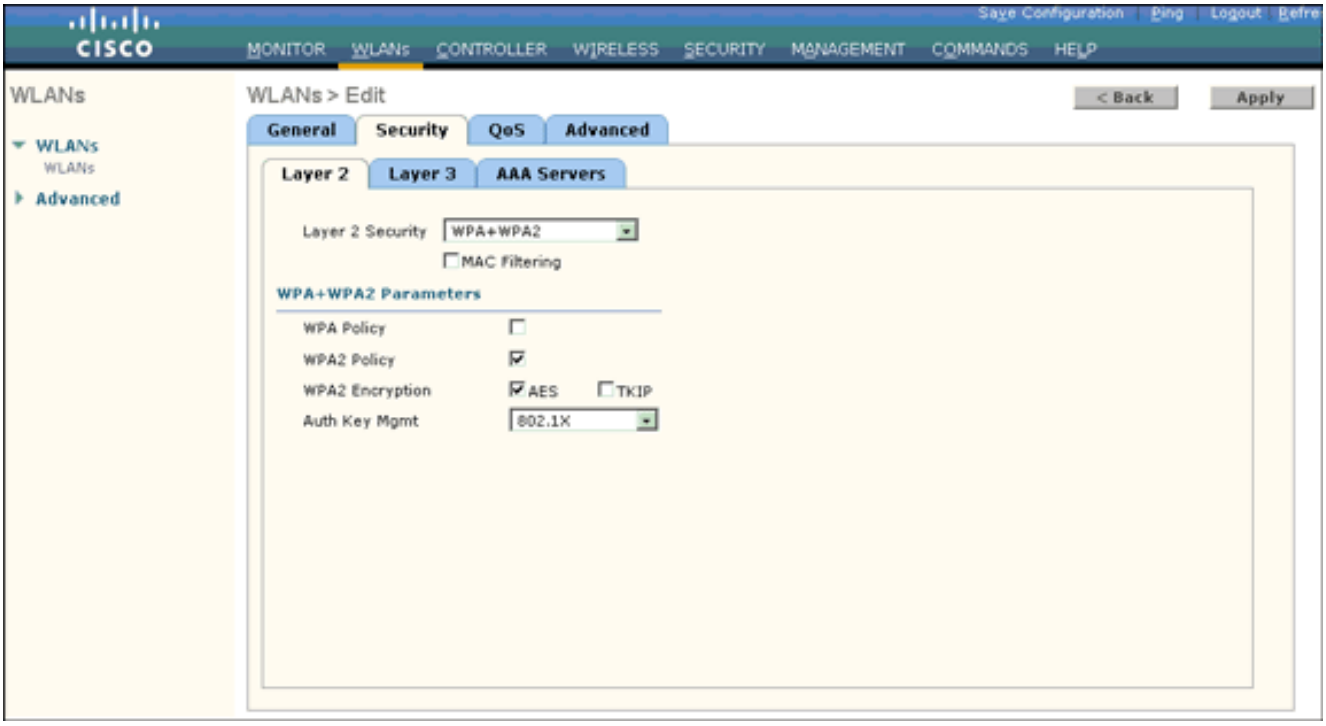


3. [WLANs] > [New] ページで、WLAN SSID 名とプロファイル名を入力します。
4. [Apply] をクリックします。
5. 最初に、管理部門の WLAN を作成します。新しい WLAN を作成すると、新しい WLAN に対する [WLAN] > [Edit] ページが表示されます。このページでは、その WLAN に固有のさまざまなパラメータを定義できます。このようなパラメータには、汎用ポリシー、セキュリティ ポリシー、QoS ポリシー、および詳細設定のパラメータがあります。
6. WLAN を有効にするには、[General Policies] で [Status] チェック ボックスをオンにします。

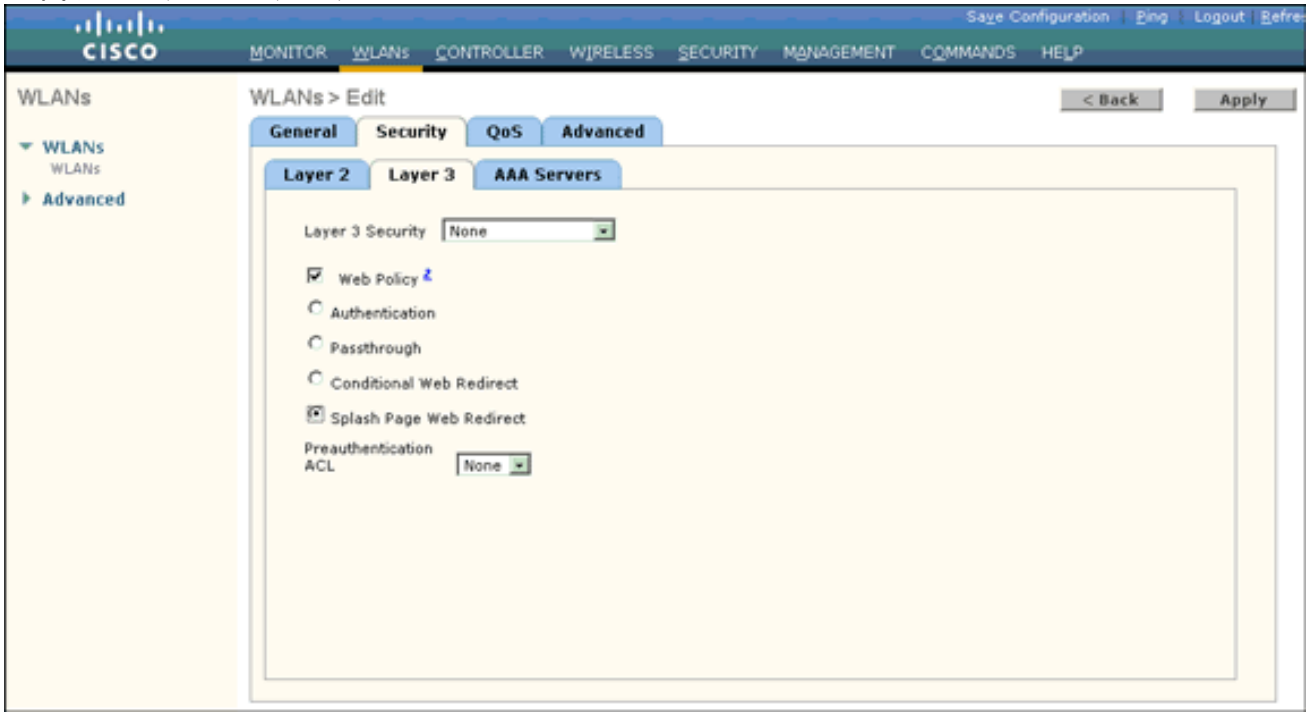


7. [Security] タブをクリックし、さらに [Layer 2] タブをクリックします。
8. [Layer 2 Security] ドロップダウン リストから [WPA+WPA2] を選択します。これにより、WLAN に対して WPA 認証が有効になります。

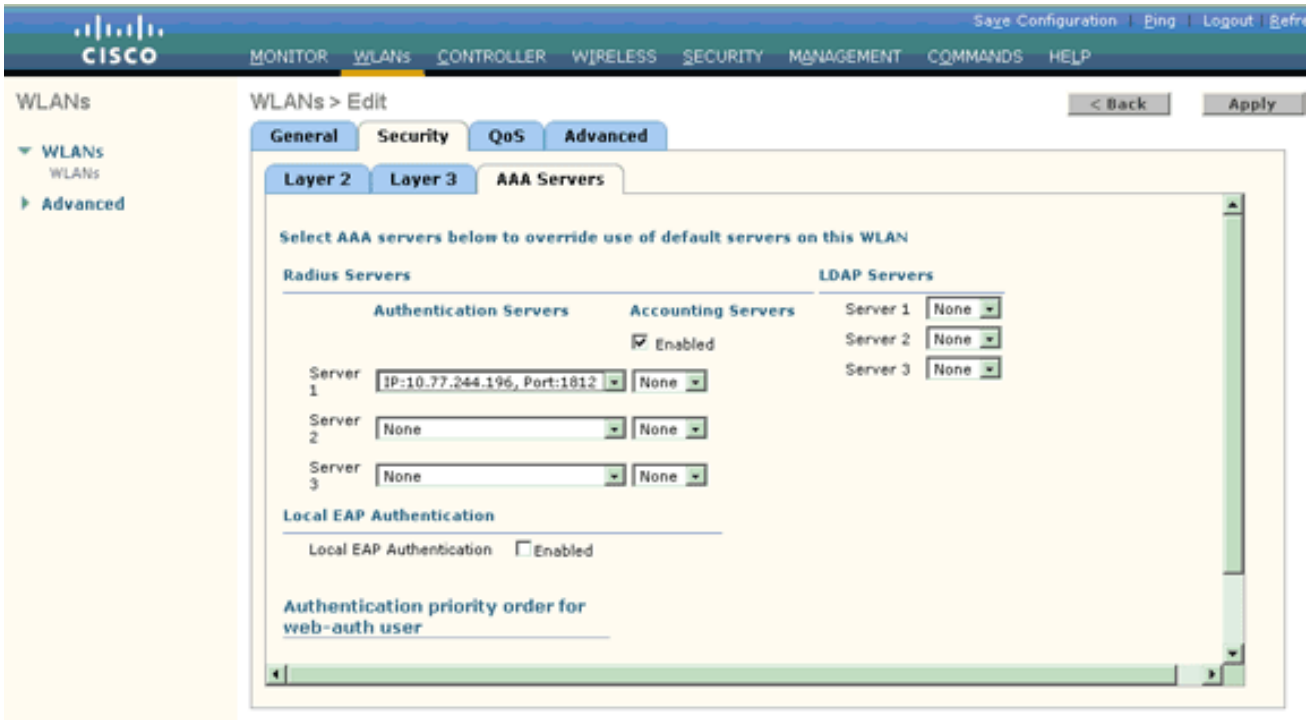
9. [WPA+WPA2 Parameters] の下で、[WPA2 Policy] および [AES Encryption] チェック ボックスをオンにします。



10. [Auth Key Mgmt] ドロップダウン リストから **802.1x** を選択します。このオプションにより、WLAN に対して 802.1x/EAP を使用した WPA2 認証と AES 暗号化が有効になります。
11. [Layer 3] タブをクリックします。
12. [Web Policy] チェック ボックスをオンにして、[Splash Page Web Redirect] オプション ボタンをクリックします。このオプションによって、スプラッシュ ページ Web リダイレクト機能が有効になります。



13. [AAA Servers] タブを選択します。
14. [Authentication Servers] の下で、[Server 1] ドロップダウン リストから適切なサーバの IP アドレスを選択します。



この例では、10.77.244.196 が RADIUS サーバとして使用されます。

15. [Apply] をクリックします。
16. 手順 2 ~ 15 を繰り返して、運用部門の WLAN を作成します。[WLANs] ページに作成した 2 つの WLAN が一覧表示されます。

セキュリティ ポリシーにスプラッシュ ページ リダイレクトが含まれていることがわかります。

ステップ 3：スプラッシュ ページ リダイレクト機能をサポートするように Cisco Secure ACS を設定する。

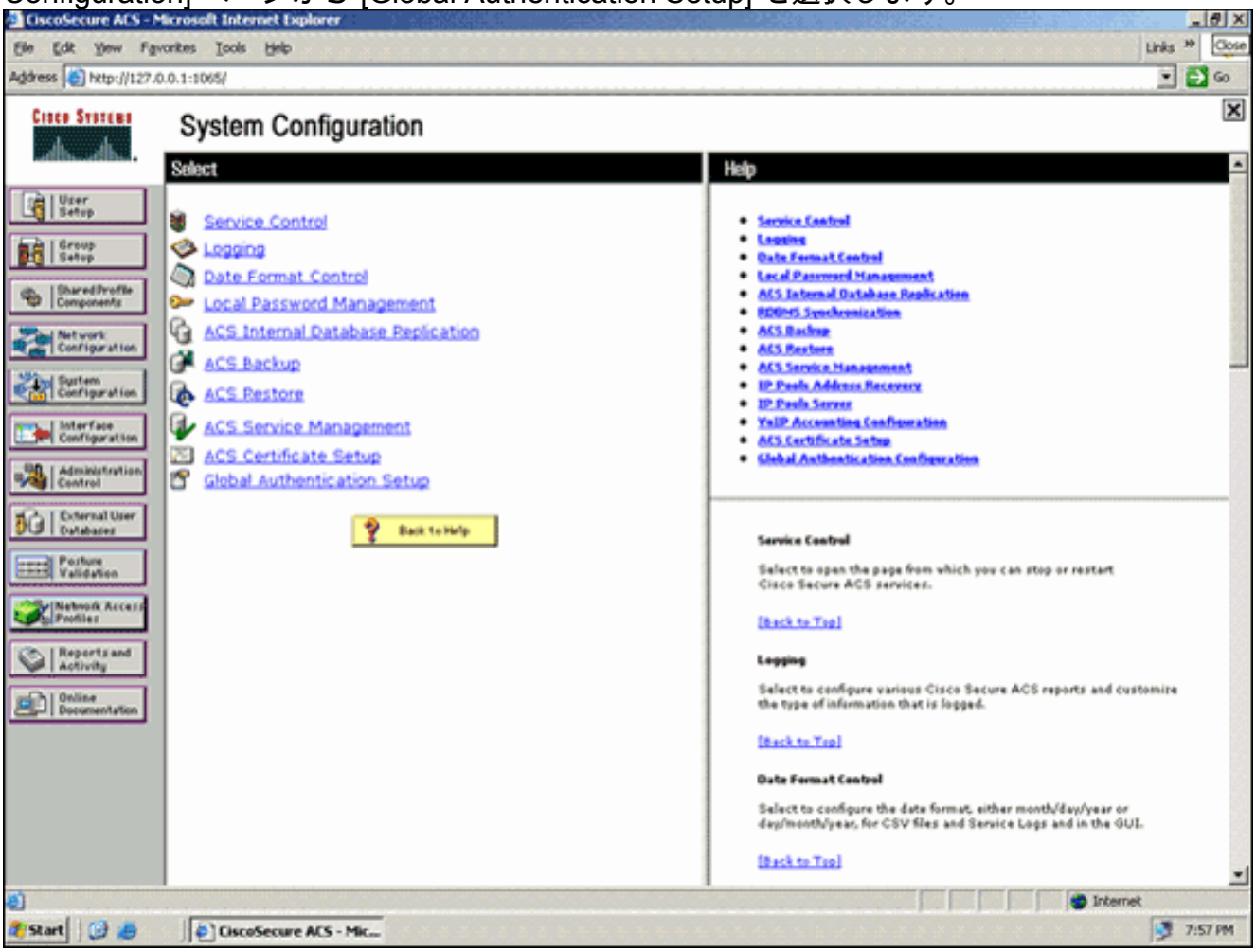
次の手順では、この機能に対応するように RADIUS サーバを設定します。RADIUS サーバは、クライアント クレデンシャルを検証するために EAP-FAST 認証を実行し、認証が成功した時点で、Cisco av-pair *url-redirect RADIUS 属性で指定された URL（外部 Web サーバ上）にユーザをリダイレクトする必要があります。*

Cisco Secure ACS を EAP-FAST 認証対応に設定する

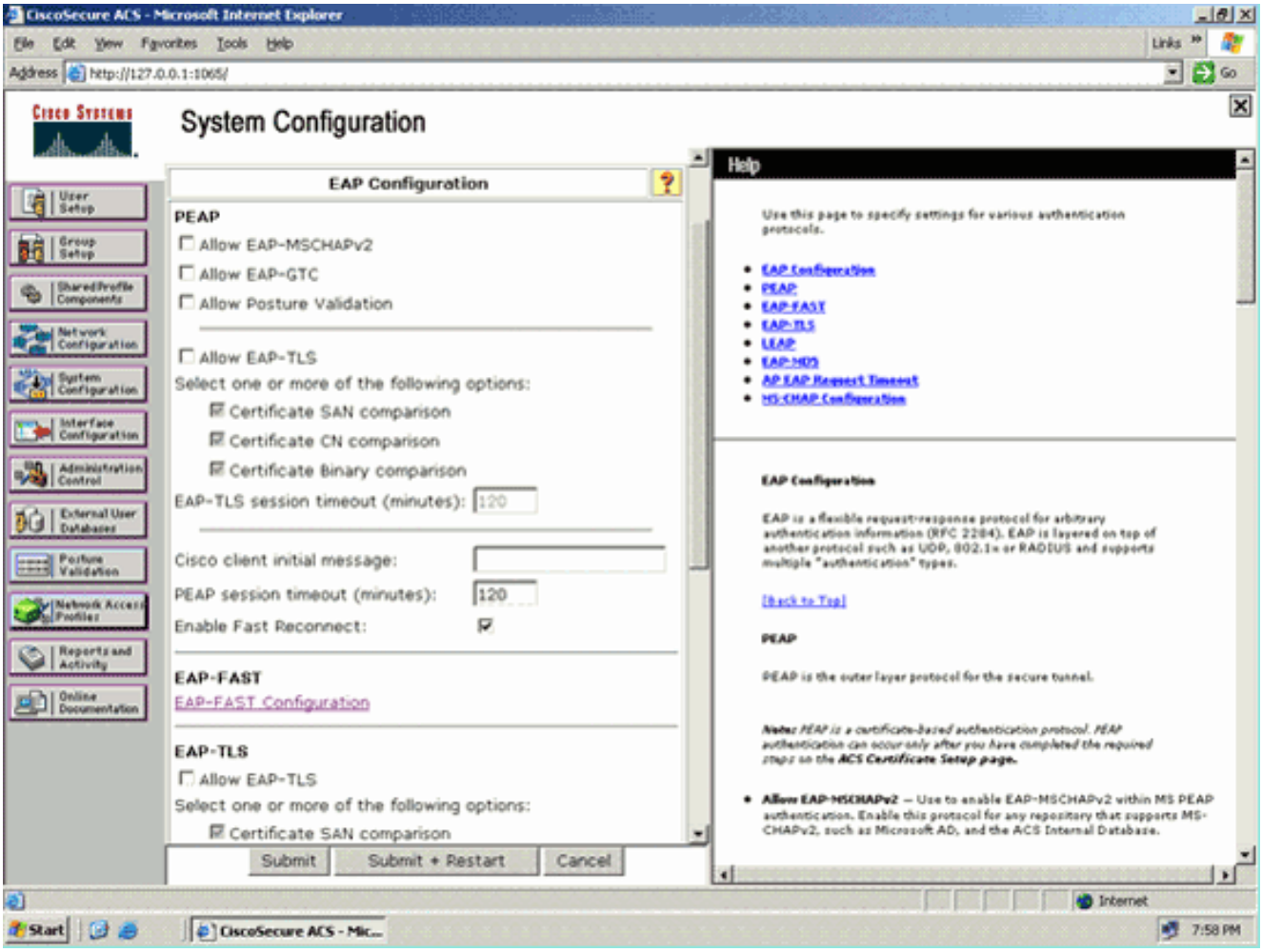
注：このドキュメントでは、ワイヤレスLANコントローラ(WLC)がAAAクライアントとしてCisco Secure ACSに追加されていることを前提としています。

RADIUS サーバに EAP-FAST 認証を設定するには、次の手順を実行します。

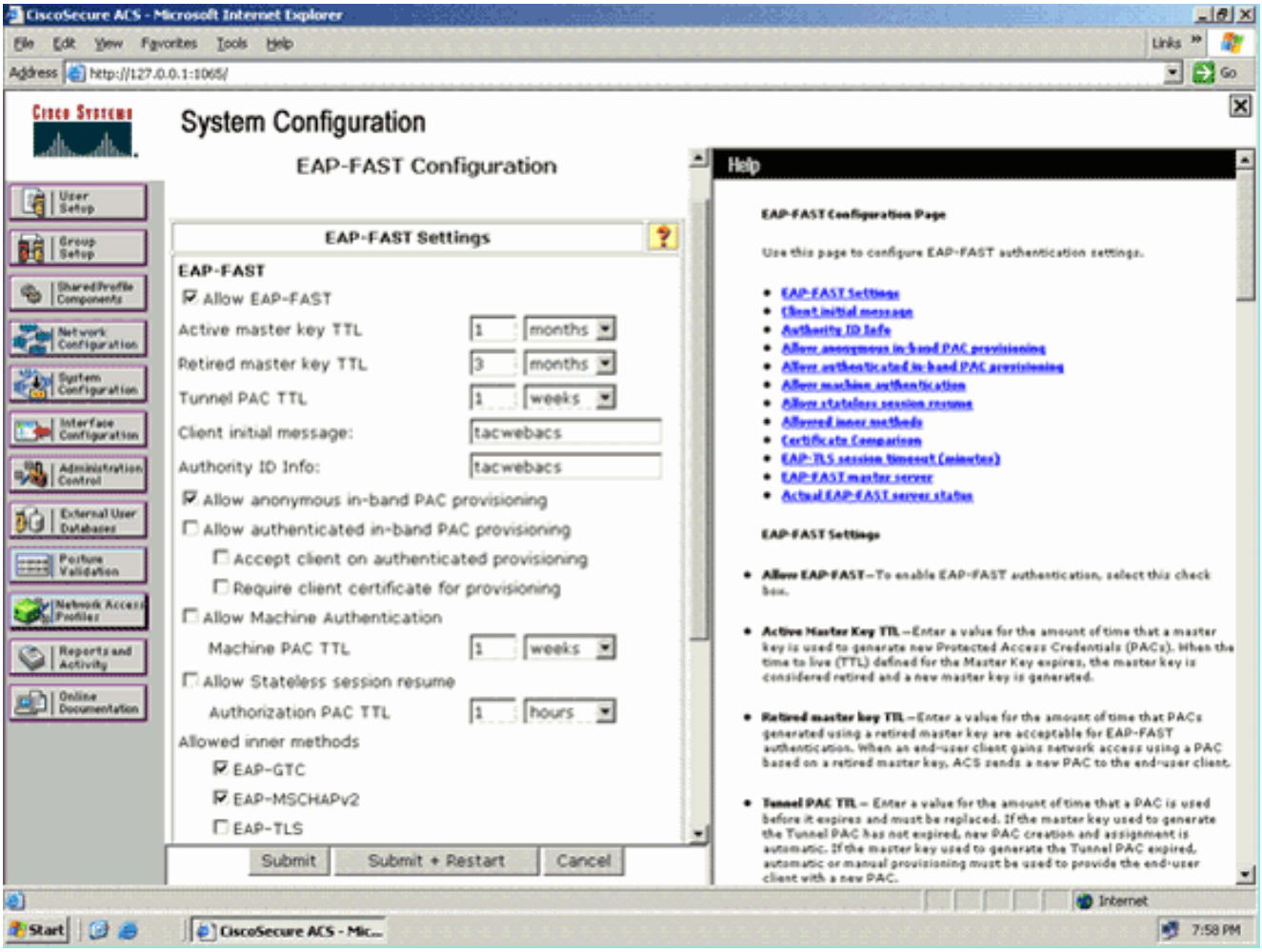
1. RADIUS サーバ GUI で [System Configuration] をクリックし、さらに [System Configuration] ページから [Global Authentication Setup] を選択します。



2. [Global Authentication setup] ページで [EAP-FAST Configuration] をクリックし、EAP-FAST 設定のページに進みます。



3. [EAP-FAST Settings] ページで、[Allow EAP-FAST] チェック ボックスをオンにして、RADIUS サーバの EAP-FAST を有効にします。



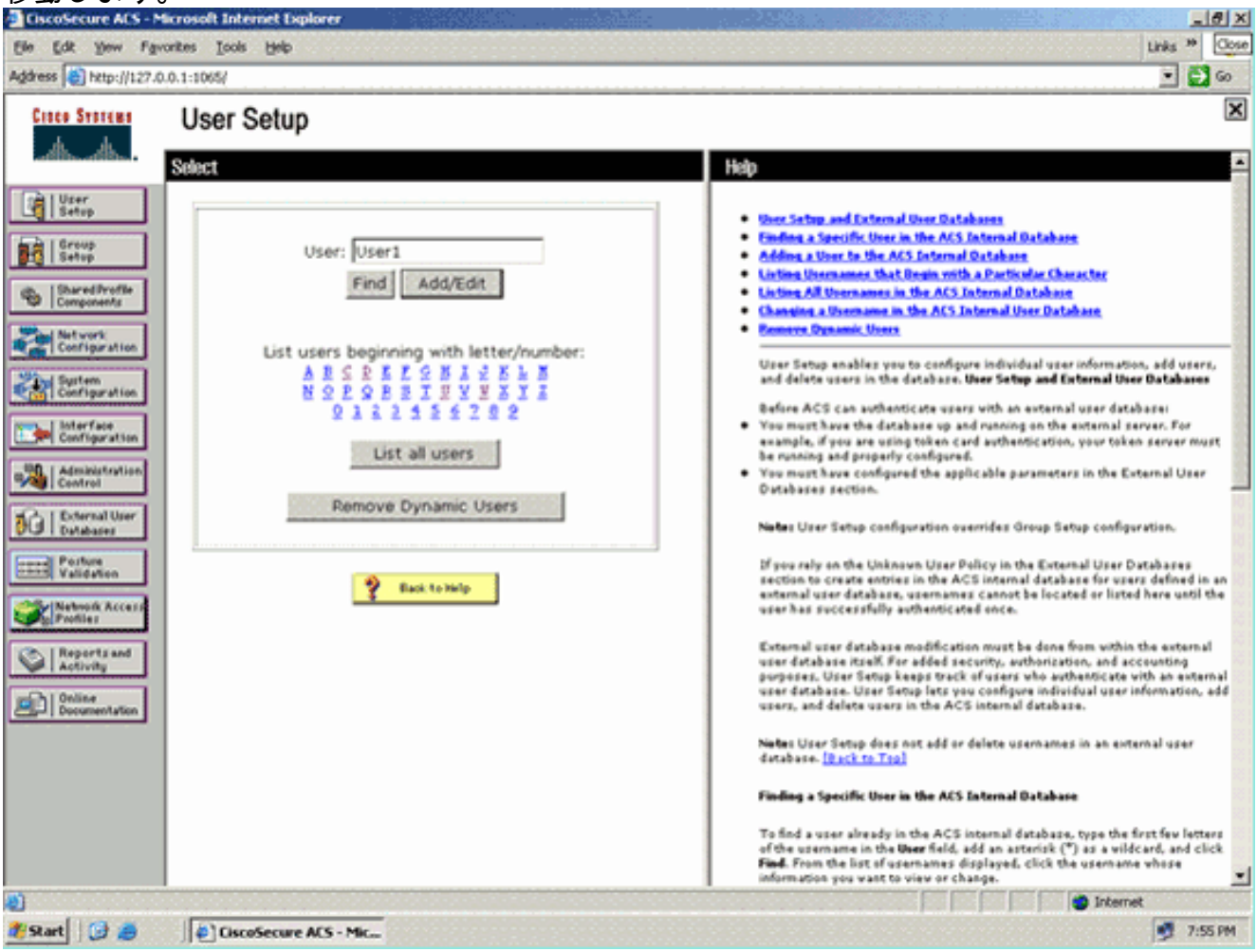
4. アクティブおよびリタイア マスター キーの TTL（存続可能時間）の値を目的に合わせて設定するか、この例で示すようにデフォルト値に設定します。[Authority ID Info] フィールドは、この ACS サーバのテキスト ID を表し、認証先の ACS サーバをエンド ユーザが判別するために使用できます。このフィールドの入力は必須です。[Client initial display message] フィールドは、EAP-FAST クライアントを使用して認証するユーザに送信するメッセージを指定します。最大長は 40 文字です。ユーザに初期メッセージが示されるのは、エンドユーザ クライアントがその表示をサポートしている場合だけです。
5. ACS で匿名インバンド PAC プロビジョニングを実行する場合、[Allow anonymous in-band PAC provisioning] チェックボックスをオンにします。
6. [Allowed inner methods] オプションでは、EAP-FAST TLS トンネル内で実行できる内部 EAP 方式を決定します。匿名インバンド プロビジョニングを実行する場合は、下位互換性を確保するために EAP-GTC と EAP-MS-CHAP を有効にする必要があります。[Allow anonymous in-band PAC provisioning] を選択する場合は、EAP-MS-CHAP（フェーズ 0）および EAP-GTC（フェーズ 2）を選択する必要があります。
7. [Submit] をクリックします。**注：**匿名インバンドPACプロビジョニングと認証済みインバンドプロビジョニングを使用してEAP FASTを設定する方法の詳細と例については、『ワイヤレスLANコントローラおよび外部RADIUSサーバを使用したEAP-FAST認証の設定例』を参照してください。

ユーザ データベースを設定し、*url-redirect* RADIUS 属性を定義する

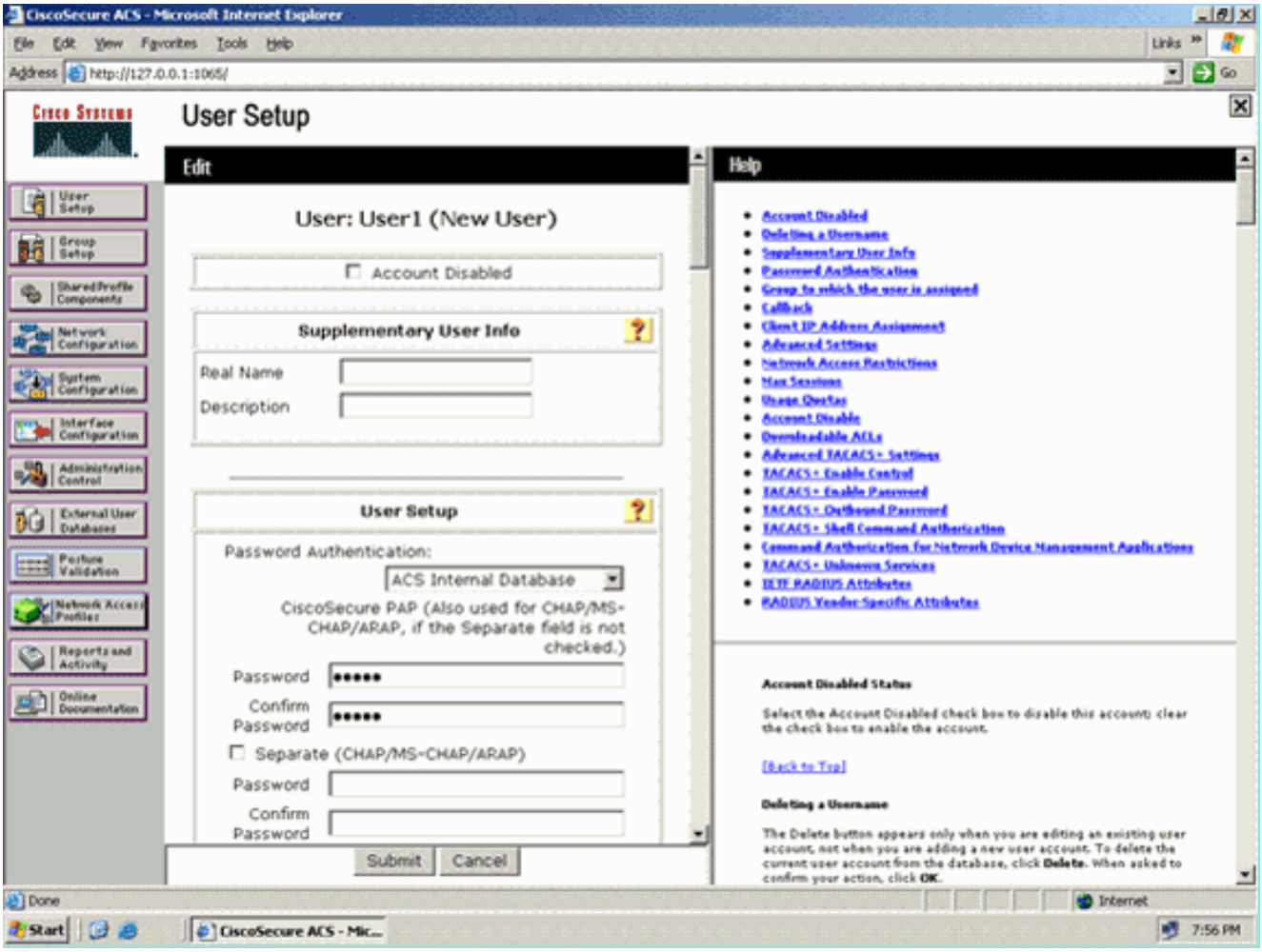
この例では、ワイヤレス クライアントのユーザ名とパスワードをそれぞれ、User1 および User1 として設定します。

次の手順を実行して、ユーザ データベースを作成します。

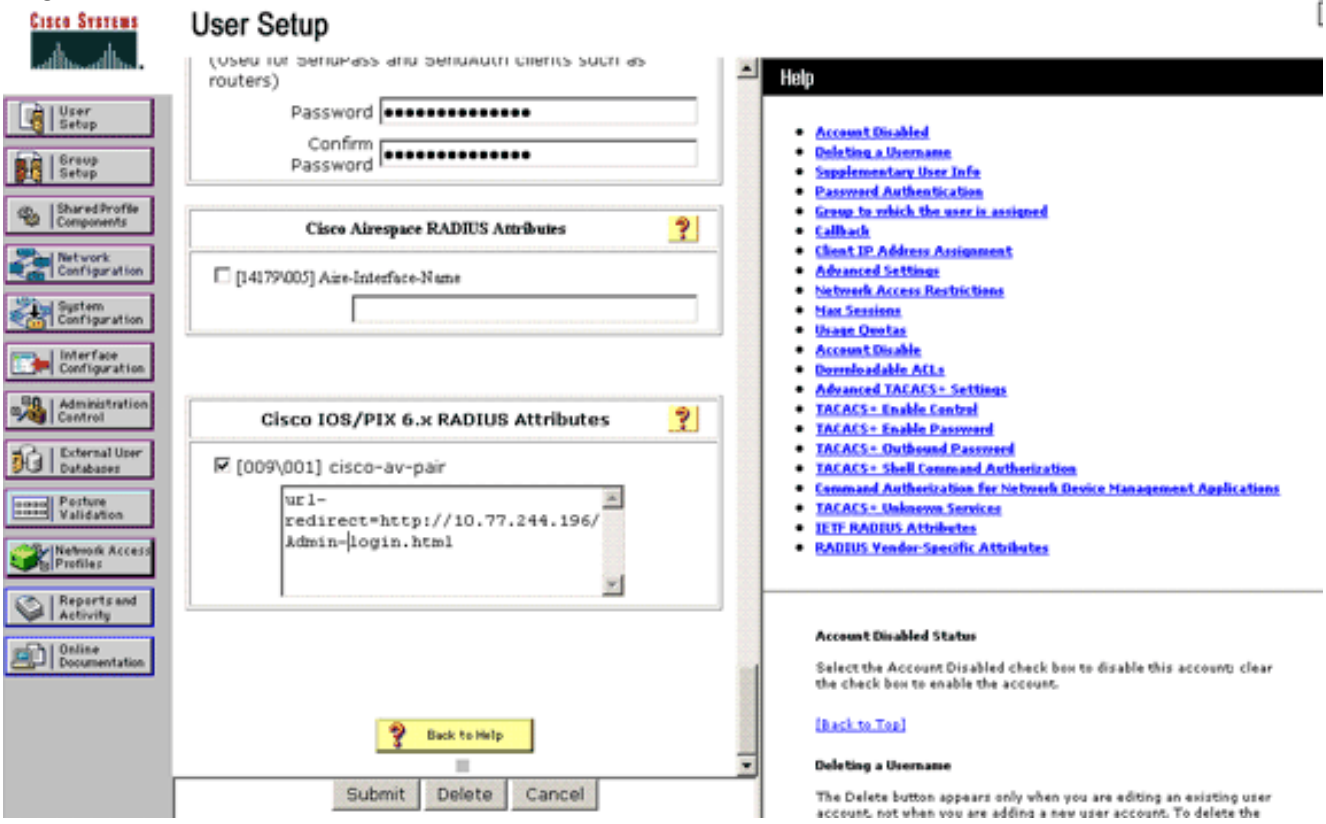
1. ナビゲーションバーの ACS GUI から [User Setup] を選択します。
2. 新しいワイヤレス ユーザを作成し、[Add/Edit] をクリックして、このユーザの編集ページに移動します。



3. [User Setup] の [Edit] ページで、この例に示すように、[Real Name] と [Description]、さらに [Password] を設定します。このドキュメントでは、[Password Authentication] オプションで [ACS Internal Database] を使用しています。



4. RADIUS 属性を変更するため、ページをスクロール ダウンします。
5. [[009\001] cisco-av-pair] チェックボックスをオンにします。
6. [[009\001] cisco-av-pair] 編集ボックスに、次の Cisco av-pairs を入力し、ユーザのリダイレクト先の URL を指定します。url-redirect=http://10.77.244.196/Admin-Login.html



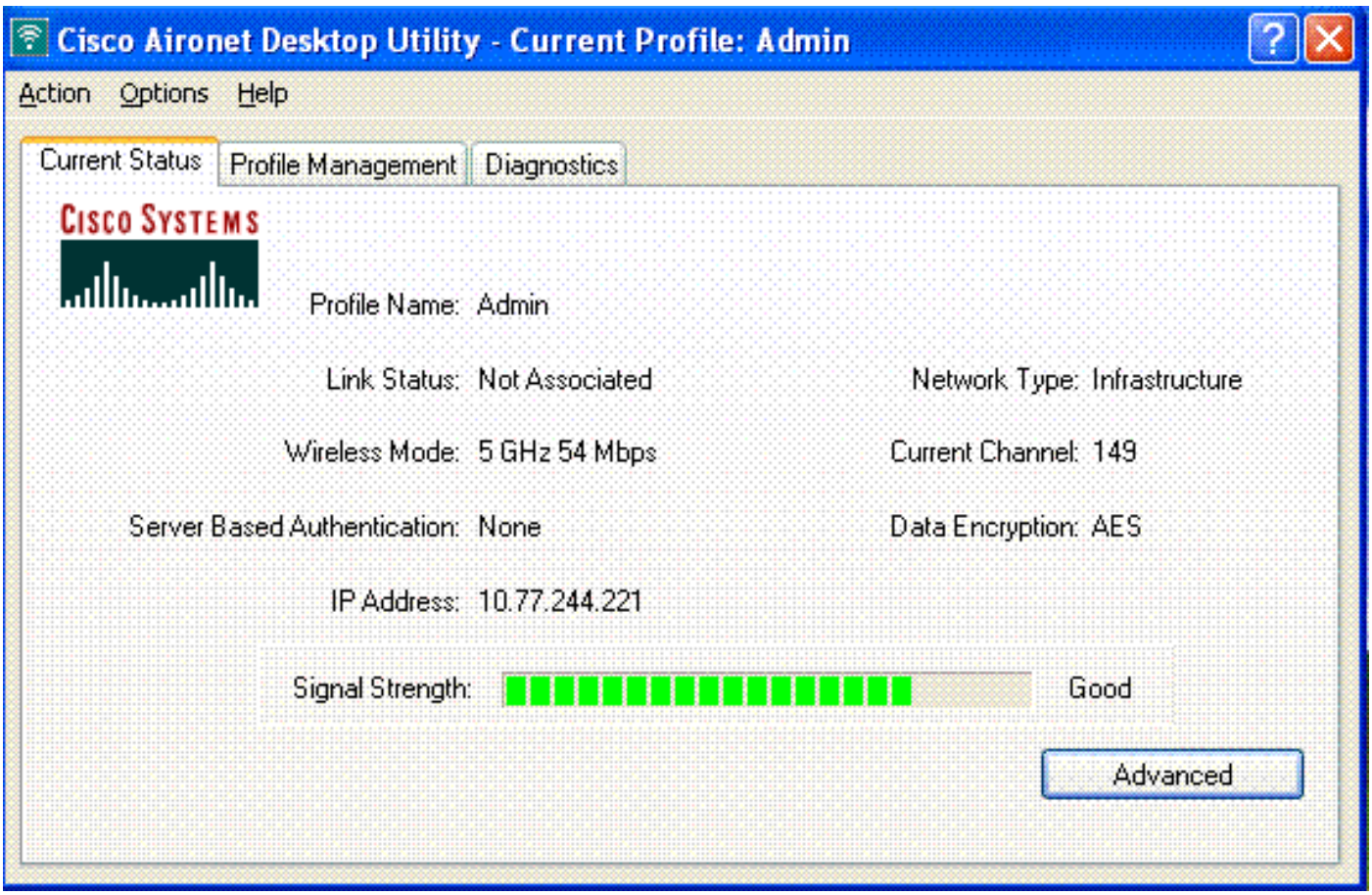
これは、管理部門ユーザのホーム ページです。

7. [Submit] をクリックします。
8. この手順を繰り返し、User2 (運用部門ユーザ) を追加します。
9. 手順 1 ~ 6 を繰り返し、より多くの管理部門ユーザと運用部門ユーザをデータベースに追加します。**注：**RADIUS属性は、Cisco Secure ACSのユーザレベルまたはグループレベルで設定できます。

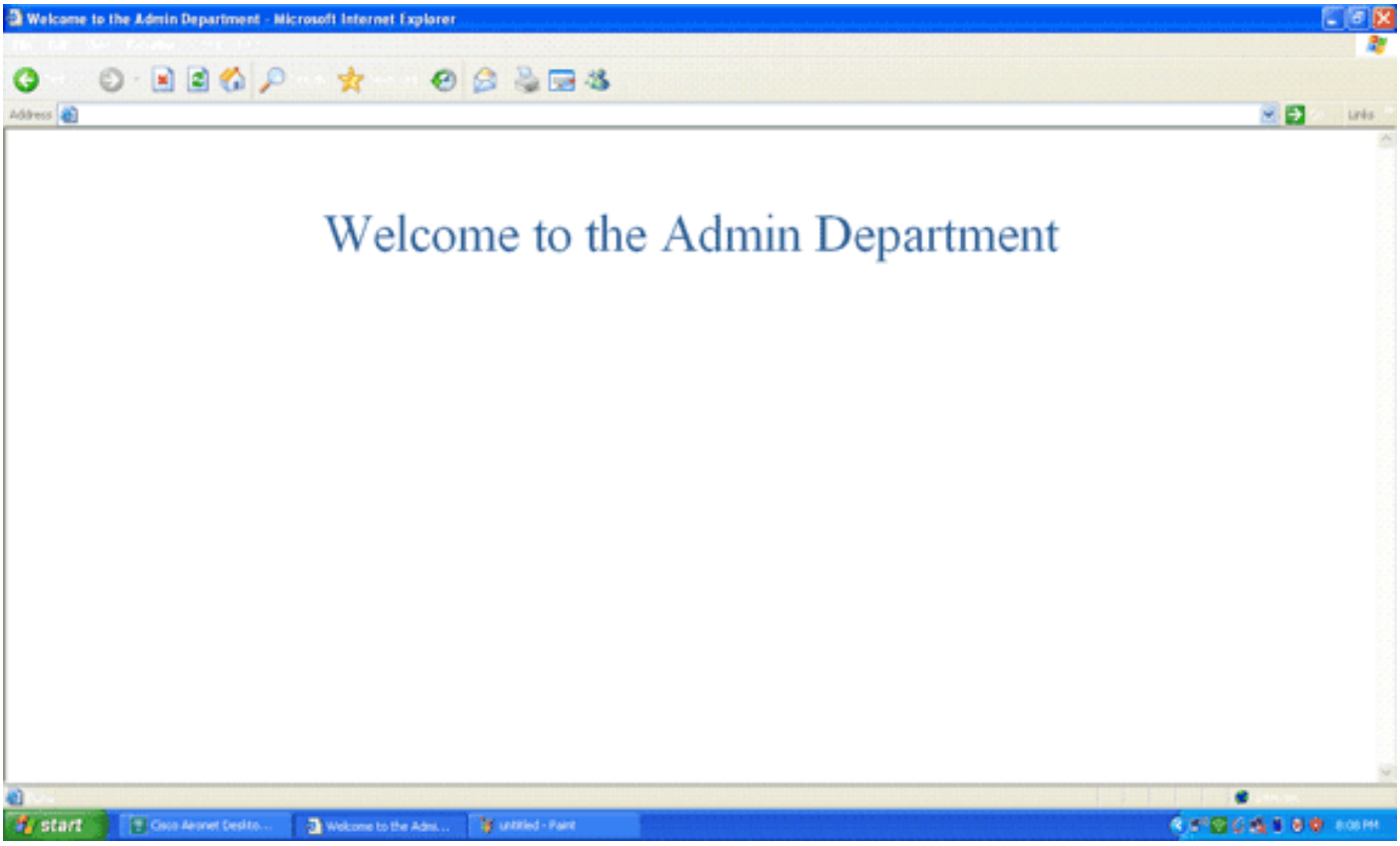
確認

設定を検証するため、管理部門と運用部門の WLAN クライアントをそれぞれ適切な WLAN にアソシエーションします。

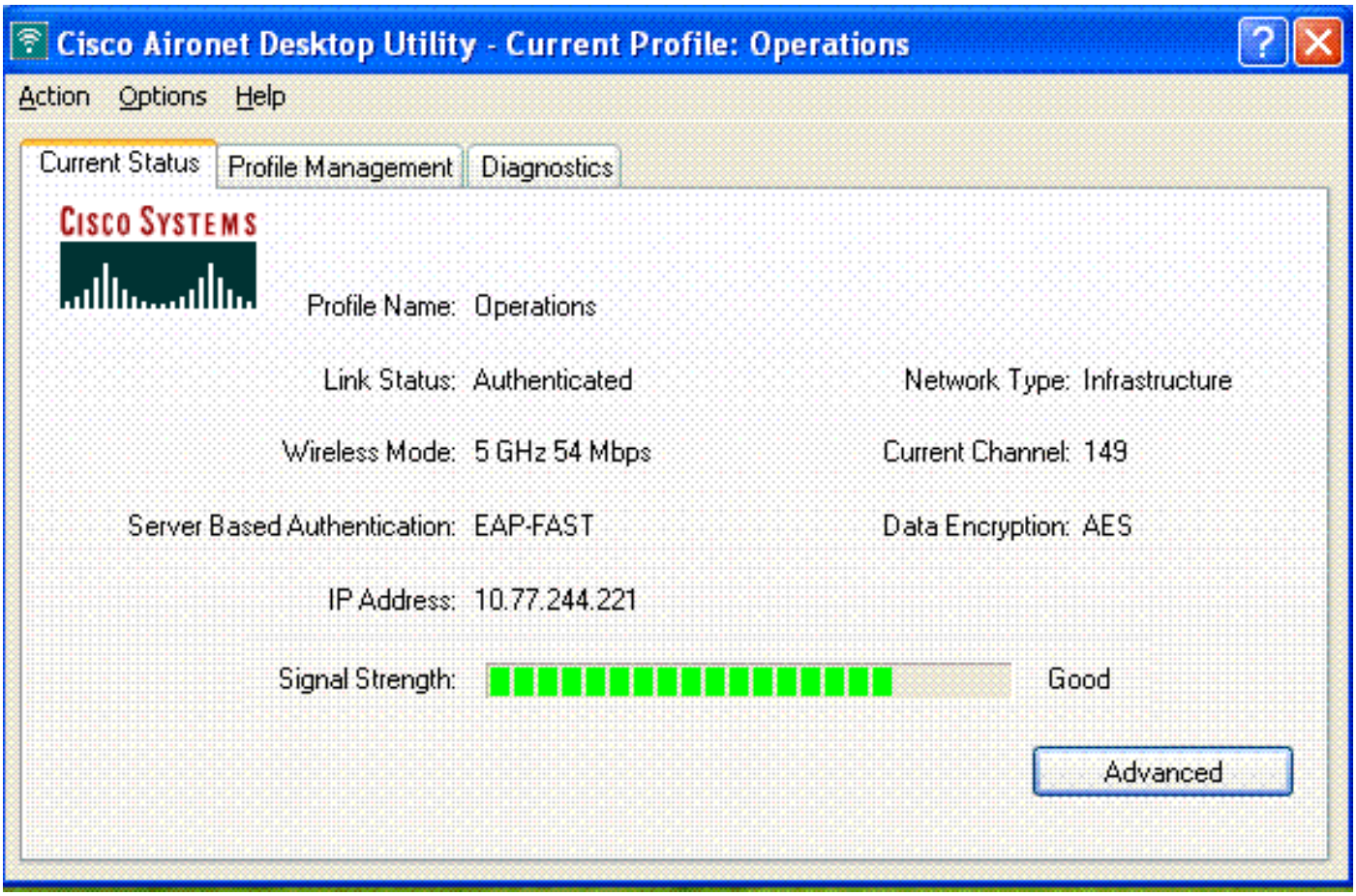
ユーザが管理部門からワイヤレス LAN Admin に接続している場合には、802.1x クレデンシャル (この例の場合は EAP-FAST クレデンシャル) の入力がユーザに求められます。ユーザがクレデンシャルを入力すると、WLC がそれらのクレデンシャルを Cisco Secure ACS サーバに渡します。Cisco Secure ACS サーバはユーザのクレデンシャルをデータベースに照合して検証し、認証に成功した時点で、url-redirect 属性をワイヤレス LAN コントローラに返します。この段階で認証は完了です。

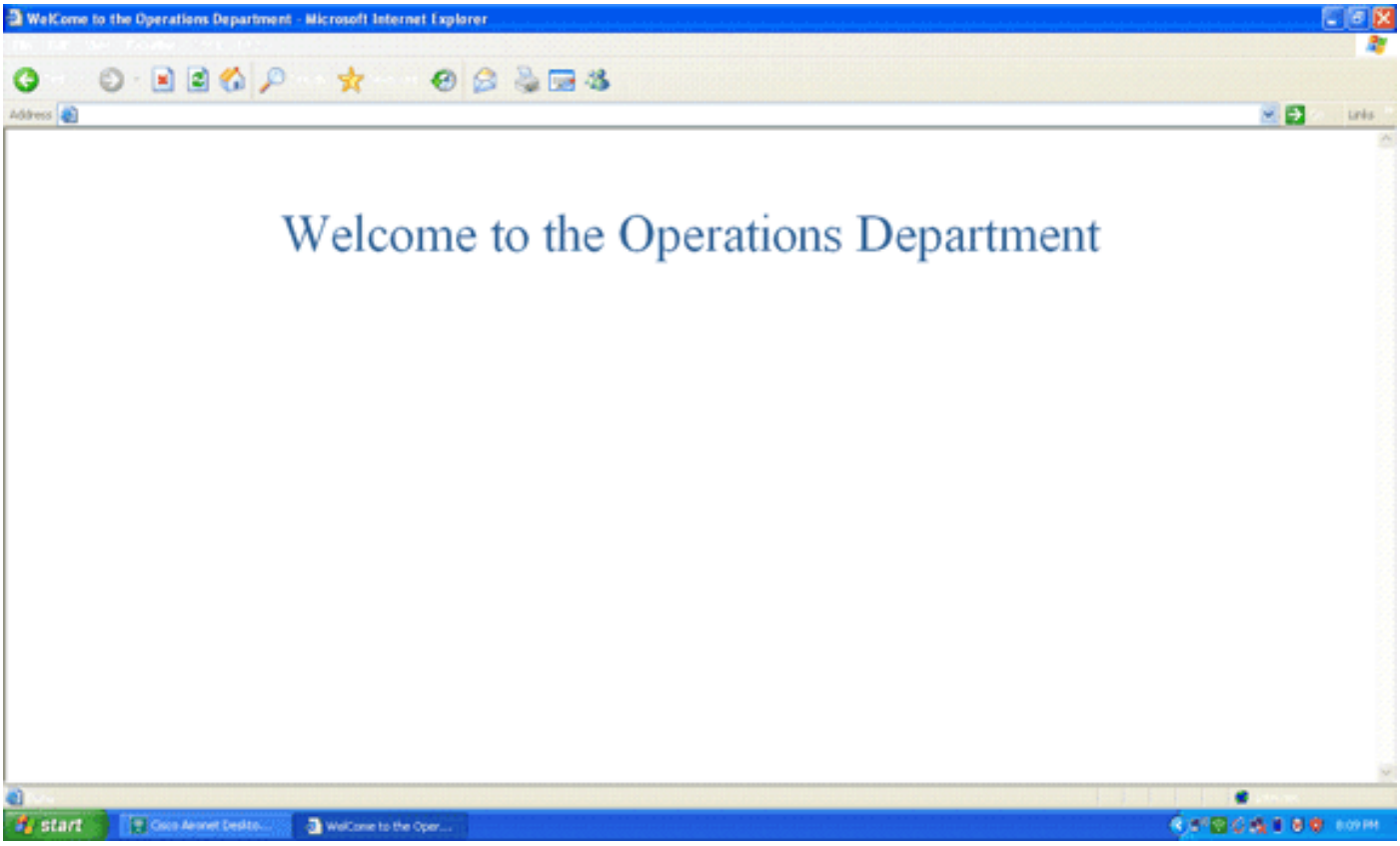


ユーザが Web ブラウザを開くと、ユーザは管理部門のホーム ページの URL へリダイレクトされます (この URL は cisco-av-pair 属性を介して WLC に返されます)。ユーザは、リダイレクト後、ネットワークにフル アクセスできます。次にスクリーンショットを示します。



ユーザが運用部門から WLAN Operations に接続した場合も同様に一連のイベントが発生します。





トラブルシュート

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。

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。

設定のトラブルシューティングを行うために、次のコマンドを使用することができます。

- **show wlan wlan_id**：特定の WLAN の Web リダイレクト機能のステータスを表示します。以下が一例です。

```
WLAN Identifier.................................. 1
Profile Name..................................... Admin
Network Name (SSID).............................. Admin
...
Web Based Authentication......................... Disabled
Web-Passthrough.................................. Disabled
Conditional Web Redirect......................... Disabled
Splash-Page Web Redirect......................... Enabled
```

- **debug dot1x events enable**：802.1x パケット メッセージのデバッグを有効にします。以下が一例です。

```
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP Request from AAA to
    mobile 00:40:96:ac:dd:05 (EAP Id 16)
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAPOL EAPPKT from
    mobile 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAP Response from
    mobile 00:40:96:ac:dd:05 (EAP Id 16, EAP Type 43)
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Processing Access-Challenge for
    mobile 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Setting re-auth timeout to 1800
    seconds, got from WLAN config.
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Station 00:40:96:ac:dd:05
```

```
    setting dot1x reauth timeout = 1800
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Creating a new PMK Cache Entry
    for station 00:40:96:ac:dd:05 (RSN 2)
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Adding BSSID 00:1c:58:05:e9:cf
    to PMKID cache for station 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: New PMKID: (16)
Fri Feb 29 10:27:16 2008:      [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca
    fb fa 8e 3c
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Disabling re-auth since PMK
    lifetime can take care of same.
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP-Success to mobile
    00:40:96:ac:dd:05 (EAP Id 17)
Fri Feb 29 10:27:16 2008: Including PMKID in M1  (16)
Fri Feb 29 10:27:16 2008:      [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca
    fb fa 8e 3c
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAPOL-Key Message to
    mobile 00:40:96:ac:dd:05
    state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received Auth Success while
    in Authenticating state for mobile 00:40:96:ac:dd:05
```

- **debug aaa events enable**：すべての aaa イベントのデバッグ出力を有効にします。以下が一例です。

```
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
    Authentication Packet (id 103) to 10.77.244.196:1812, proxy state
    00:40:96:ac:dd:05-00:00
Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=11
Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=11
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Challenge received from
    RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
    Authentication Packet (id 104) to 10.77.244.196:1812, proxy state
    00:40:96:ac:dd:05-00:00
Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=2
Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=2
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Accept received from
    RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 AAA Override Url-Redirect
    'http://10.77.244.196/Admin-login.html' set
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Applying new AAA override for
    station 00:40:96:ac:dd:05
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Override values for station
    00:40:96:ac:dd:05
       source: 4, valid bits: 0x0
       qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
       dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
       vlanIfName: '', aclName: '
```

関連情報

- Cisco Wireless LAN Controller コンフィギュレーション ガイド、リリース 5.0
- 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外部 Web 認証の設定例
- 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。