管理ユーザを認証するためのWLCとACSの設定

内容

はじめに

このドキュメントでは、AAAサーバがコントローラで管理ユーザを認証できるように、WLCとCisco Secure ACSを設定する方法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

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、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

表記法

表記法の詳細については、『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

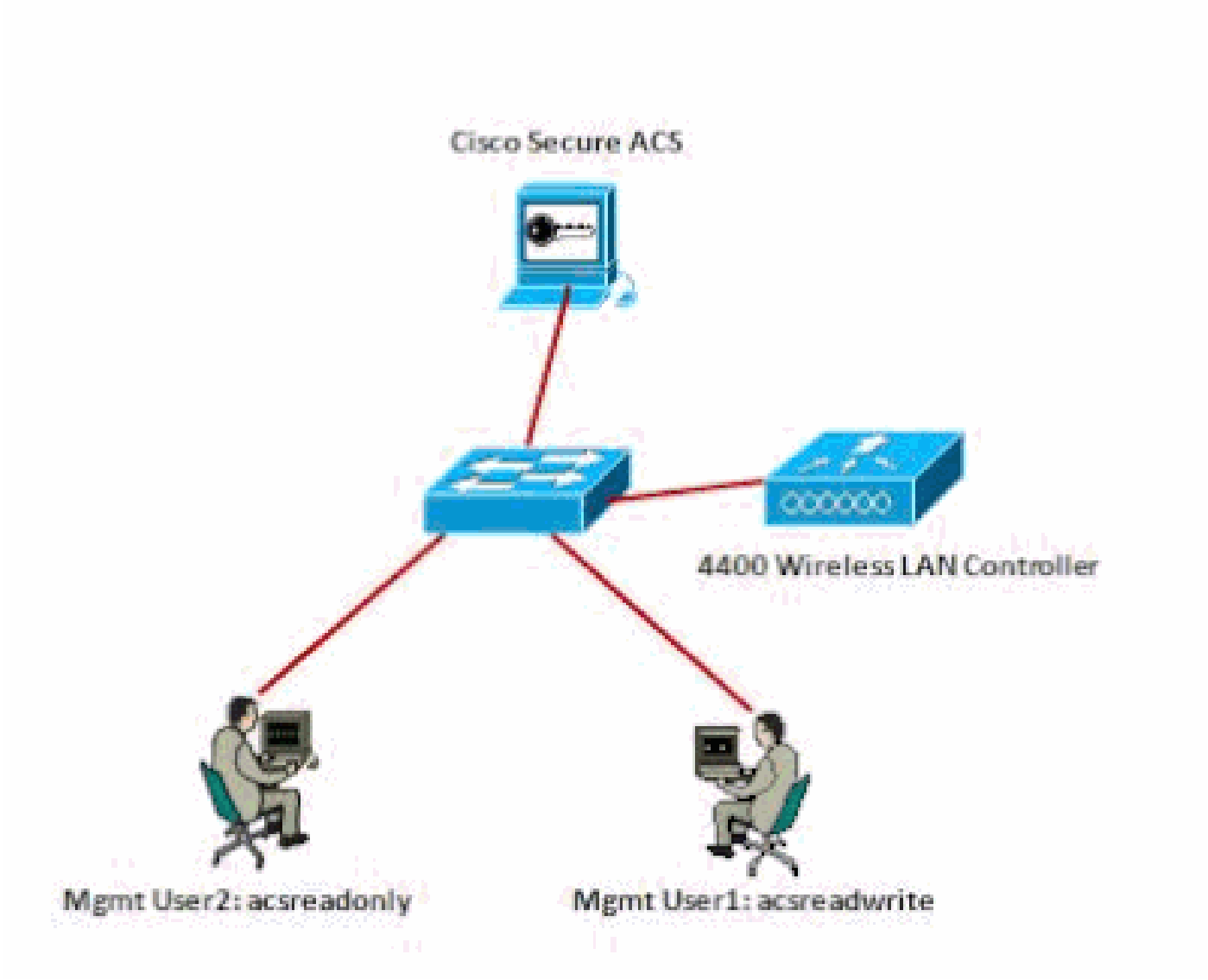
このドキュメントでは、認証、認可、アカウンティング(AAA)サーバがコントローラ上で管理ユーザを認証できるように、ワイヤレスLANコントローラ(WLC)とアクセスコントロールサーバ(Cisco Secure ACS)を設定する方法について説明します。また、Cisco Secure ACS RADIUSサーバから返されるベンダー固有属性(VSA)を使用して、さまざまな管理ユーザが異なる特権を受け取る方法についても説明します。

設定

このセクションでは、このドキュメントの目的に従って WLC および ACS を設定する方法について説明します。

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。



ネットワーク図

この設定例では、次のパラメータを使用します。

- Cisco Secure ACS の IP アドレス - 172.16.1.1/255.255.0.0
- コントローラの管理インターフェイスの IP アドレス - 172.16.1.30/255.255.0.0
- 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：asdf1234
- ACS で設定する 2 人のユーザのクレデンシャルは次のとおりです。
    - ユーザ名 - acsreadwrite

      パスワード - acsreadwrite
    - ユーザ名 - acsreadonly

      パスワード - acsreadonly

次の目的で WLC と Cisco Secure ACS を設定する必要があります。

- ユーザ名とパスワードに acsreadwrite を使用して WLC にログインするユーザに、WLC への完全な管理アクセス権を付与する。
- ユーザ名とパスワードに acsreadonly を使用して WLC にログインするユーザには、WLC への読み取り専用アクセス権を付与する。

コンフィギュレーション

このドキュメントでは、次のコンフィギュレーションを使用します。

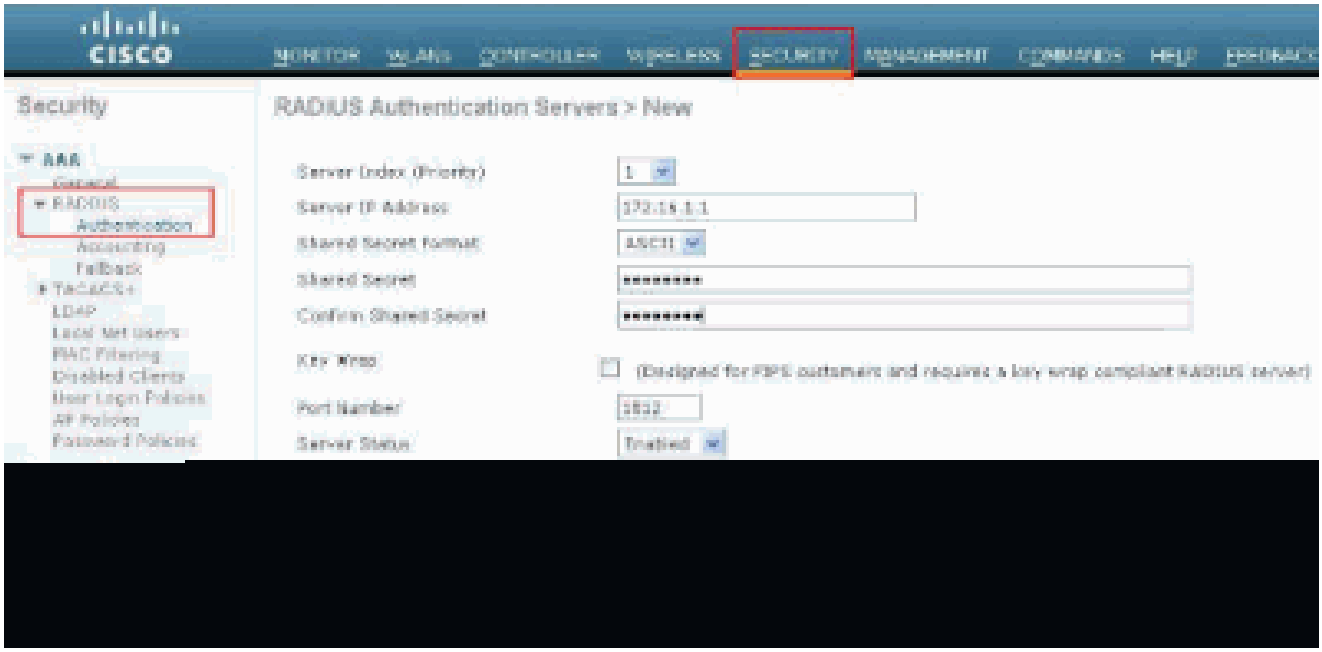
- WLC の設定
- Cisco Secure ACS の設定

WLC の設定

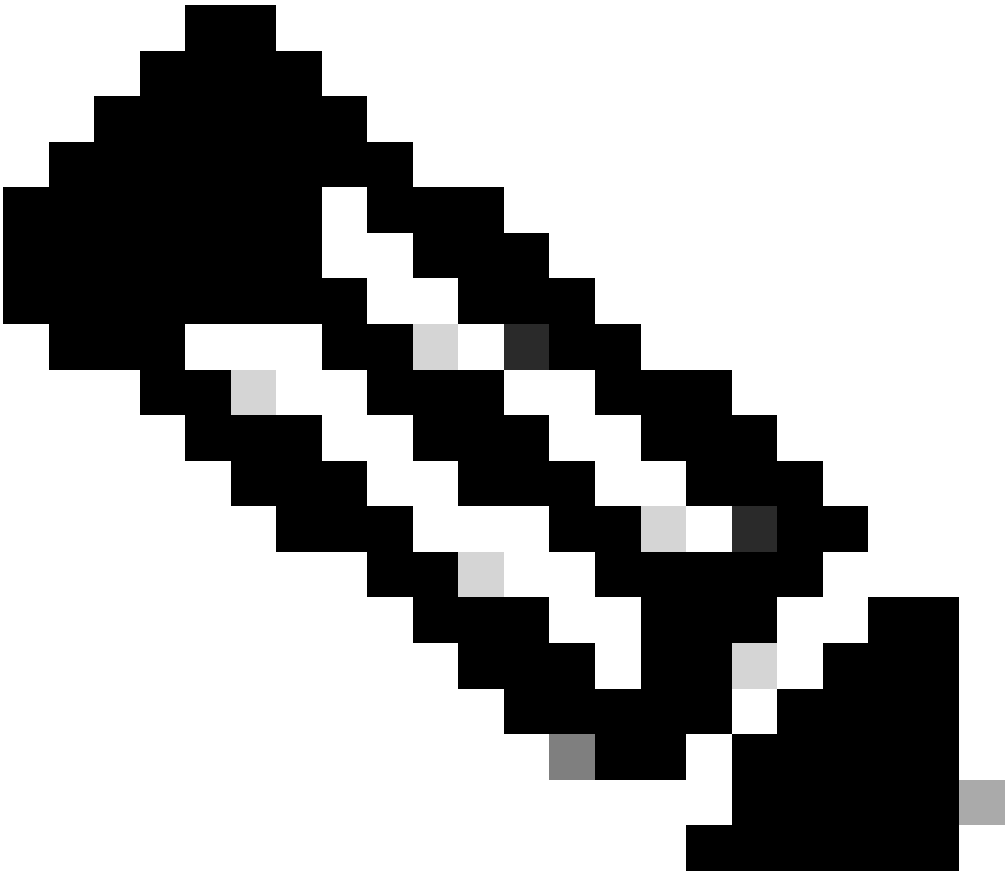
Cisco Secure ACS サーバによる管理を受け入れるように WLC を設定します。

RADIUSサーバと通信するようにWLCを設定するには、次の手順を実行します。

1. WLC GUI で [Security] をクリックします。 左側のメニューから、[RADIUS] > [Authentication] をクリックします。 [RADIUS Authentication servers] ページが表示されます新しい RADIUS サーバを追加するには、[New] をクリックします。[RADIUS Authentication Servers] > [New page] ページで、RADIUS サーバに固有のパラメータを入力します。次に例を示します。

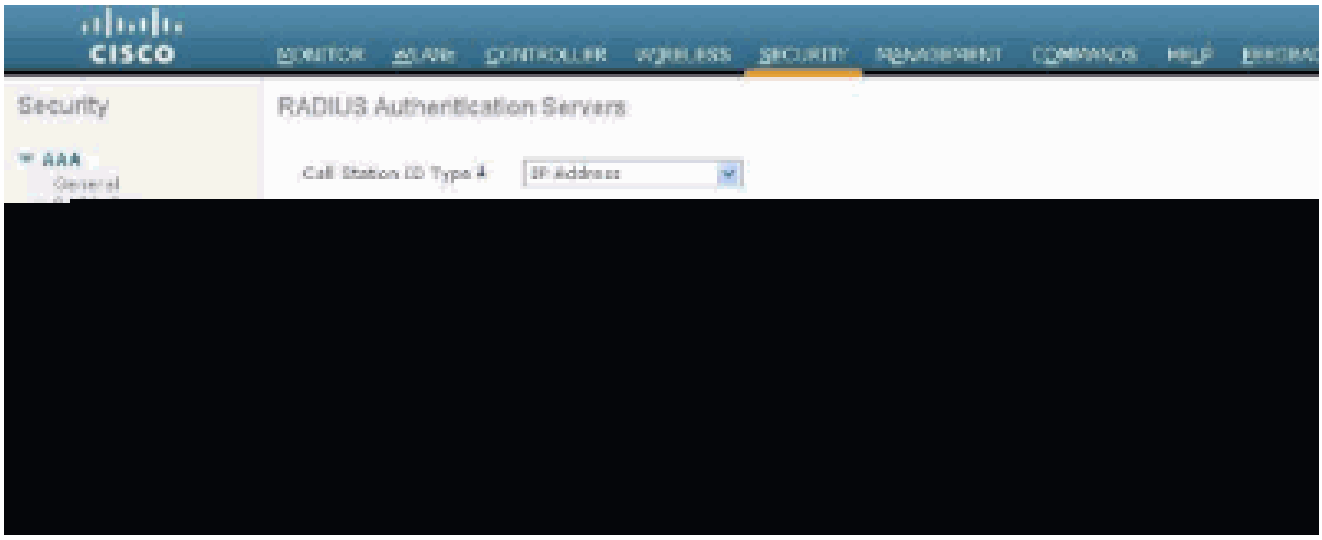


2. RADIUS サーバが WLC にログインするユーザを認証できるようにするには、[Management] オプション ボタンにチェックマークを付けます。



注：このページで設定されている共有秘密が、RADIUSサーバで設定されている共有秘密と一致していることを確認してください。その場合にだけ、WLC が RADIUS サーバと通信できます。

3. Cisco Secure ACS で管理できるように WLC が設定されているかどうかを確認します。これを実行するには、WLC の GUI から [Security] をクリックします。次のような GUI ウィンドウが表示されます。



RADIUS サーバ 172.16.1.1 の [Management] チェック ボックスにチェックマークが付いていることを確認します。これは、ACS が WLC 上で管理ユーザを認証できることを示しています。

Cisco Secure ACS の設定

ACS を設定するには、次の手順を実行します。

1. WLC を AAA クライアントとして RADIUS サーバに追加する
2. ユーザおよび RADIUS IETF アトリビュートを設定する
3. 読み取り/書き込みアクセス権を持つユーザを設定する
4. 読み取り専用アクセス権を持つユーザを設定する

WLC を AAA クライアントとして RADIUS サーバに追加する

WLCをAAAクライアントとしてCisco Secure ACSに追加するには、次の手順を実行します。

1. ACS の GUI で、[Network Configuration] をクリックします。
2. [AAA Clients] 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。

   この例では、次のように設定します。

   - AAA クライアントのホスト名 - WLC-4400
   - AAA クライアント（この例では WLC）の IP アドレス - 172.16.1.30/16
   - 共有秘密キー - asdf1234

Add AAA Clientウィンドウ

この共有秘密キーは、WLC 上で設定する共有秘密キーと同じにする必要があります。

4. [Authenticate Using] ドロップダウン メニューから [RADIUS (Cisco Airespace)] 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。

ユーザおよび RADIUS IETF アトリビュートを設定する

コントローラへのログインとコントローラの管理のためにRADIUSサーバを介してユーザ認証を行うようにするには、RADIUSデータベースにユーザを追加し、ユーザ権限に基づいてIETF RADIUS attributeService-Typesetに適切な値を設定する必要があります。

- ユーザに読み取り/書き込み権限を設定するには、Service-TypeAttributeをAdministrativeに設定します。
- ユーザに読み取り専用権限を設定するには、Service-TypeAttributeをNAS-Promptに設定します。

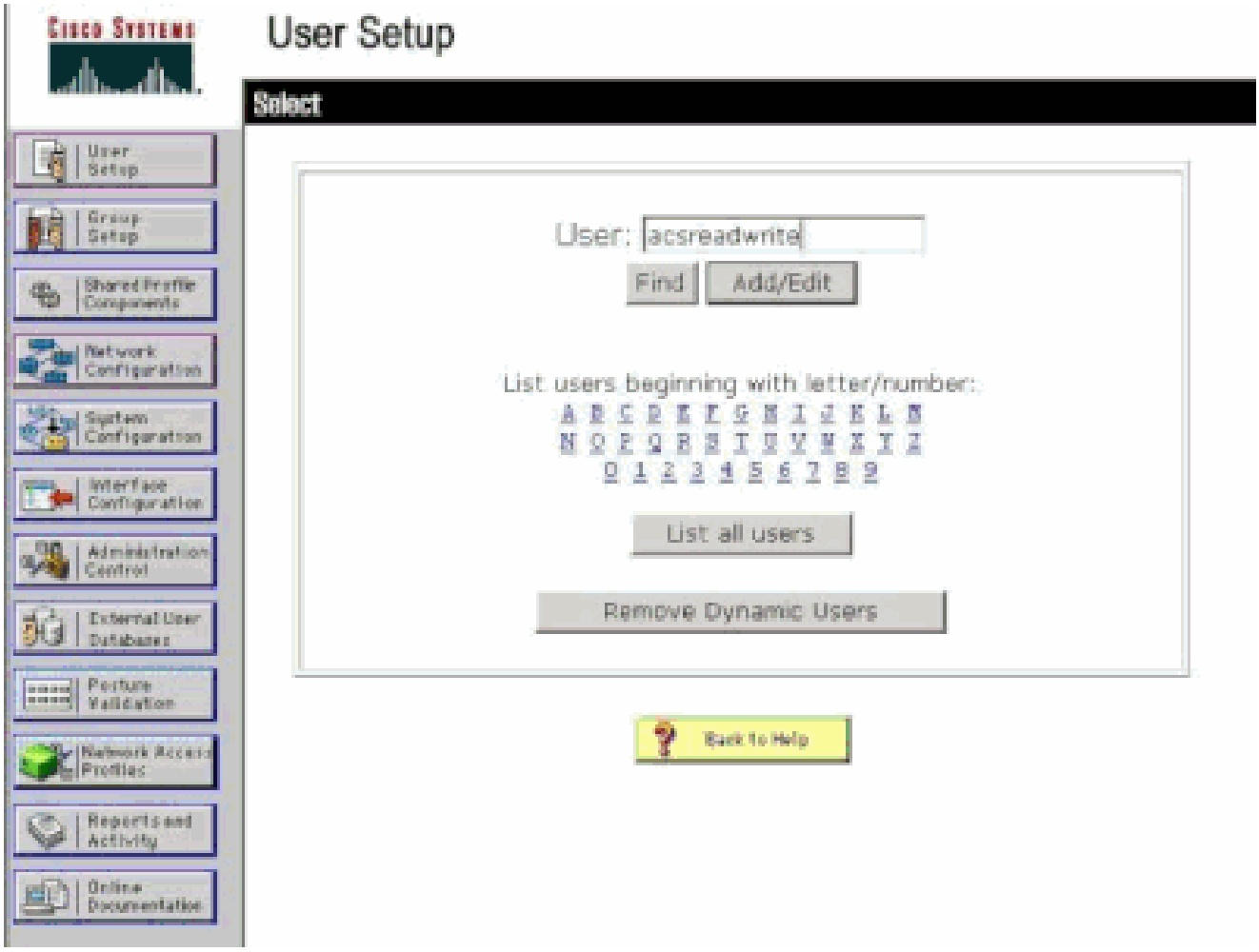
読み取り/書き込みアクセス権を持つユーザを設定する

最初の例は、WLC への完全なアクセス権を持つユーザの設定を示しています。このユーザがコントローラにログインしようとすると、RADIUS サーバは認証を行って、このユーザに完全な管理アクセス権を付与します。

この例で使用するユーザ名とパスワードは acsreadwrite です。

Cisco Secure ACS で次の手順を実行します。

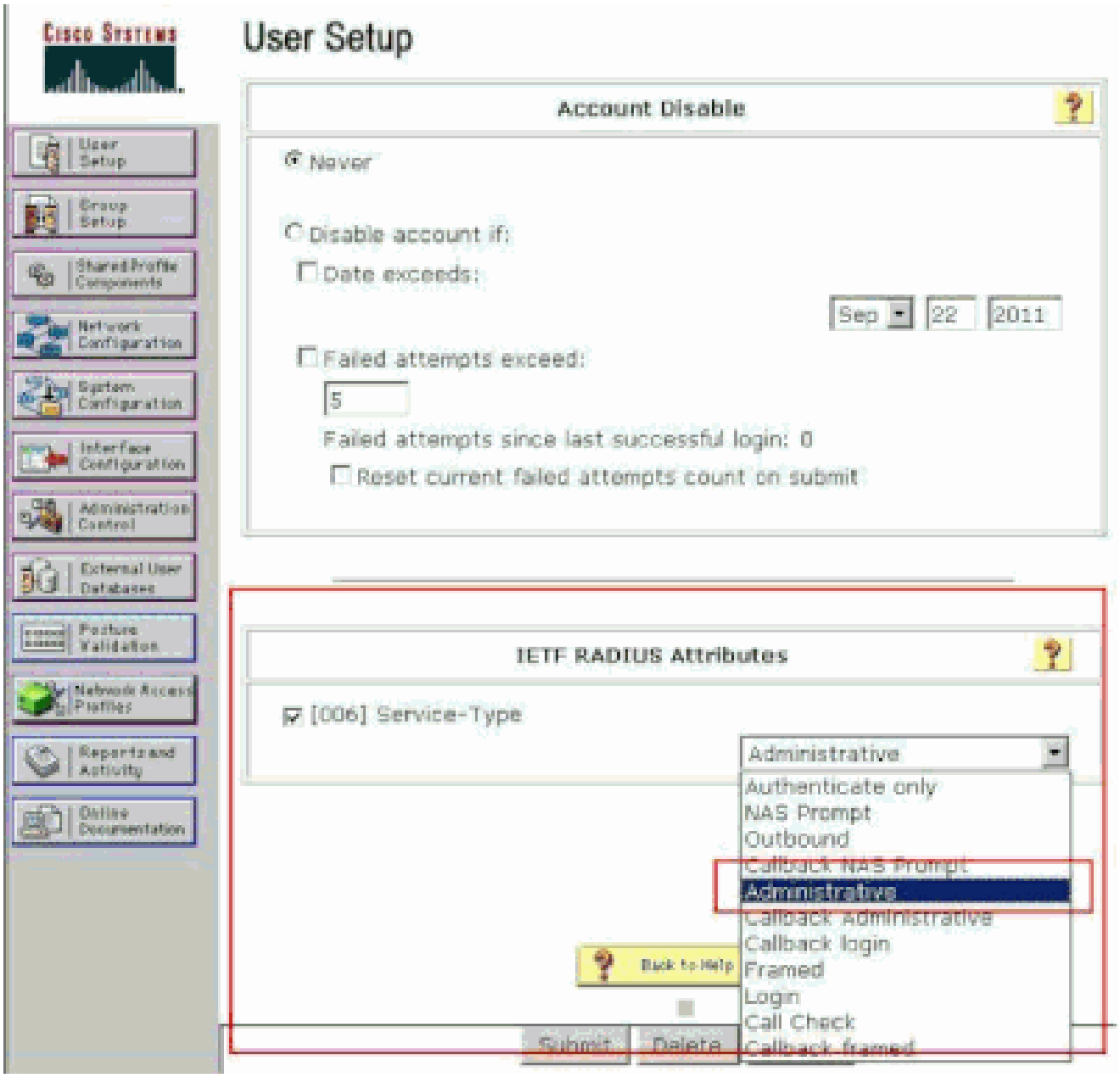
1. ACS の GUI で、[User Setup] をクリックします。
2. 次の例に示すように、ACS に追加するユーザ名を入力します。



User Setupウィンドウ

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。
5. 下にスクロールして [IETF RADIUS Attributes] の設定に移動し、[Service-Type] アトリビュートにチェックマークを付けます。
6. この例では、ユーザ acsreadwrite に完全なアクセス権を与える必要があるので、[Service-Type] プルダウン メニューから [Administrative] を選択し、[Submit] をクリックします。

   これで、このユーザに WLC への読み取り/書き込みアクセス権が与えられます。



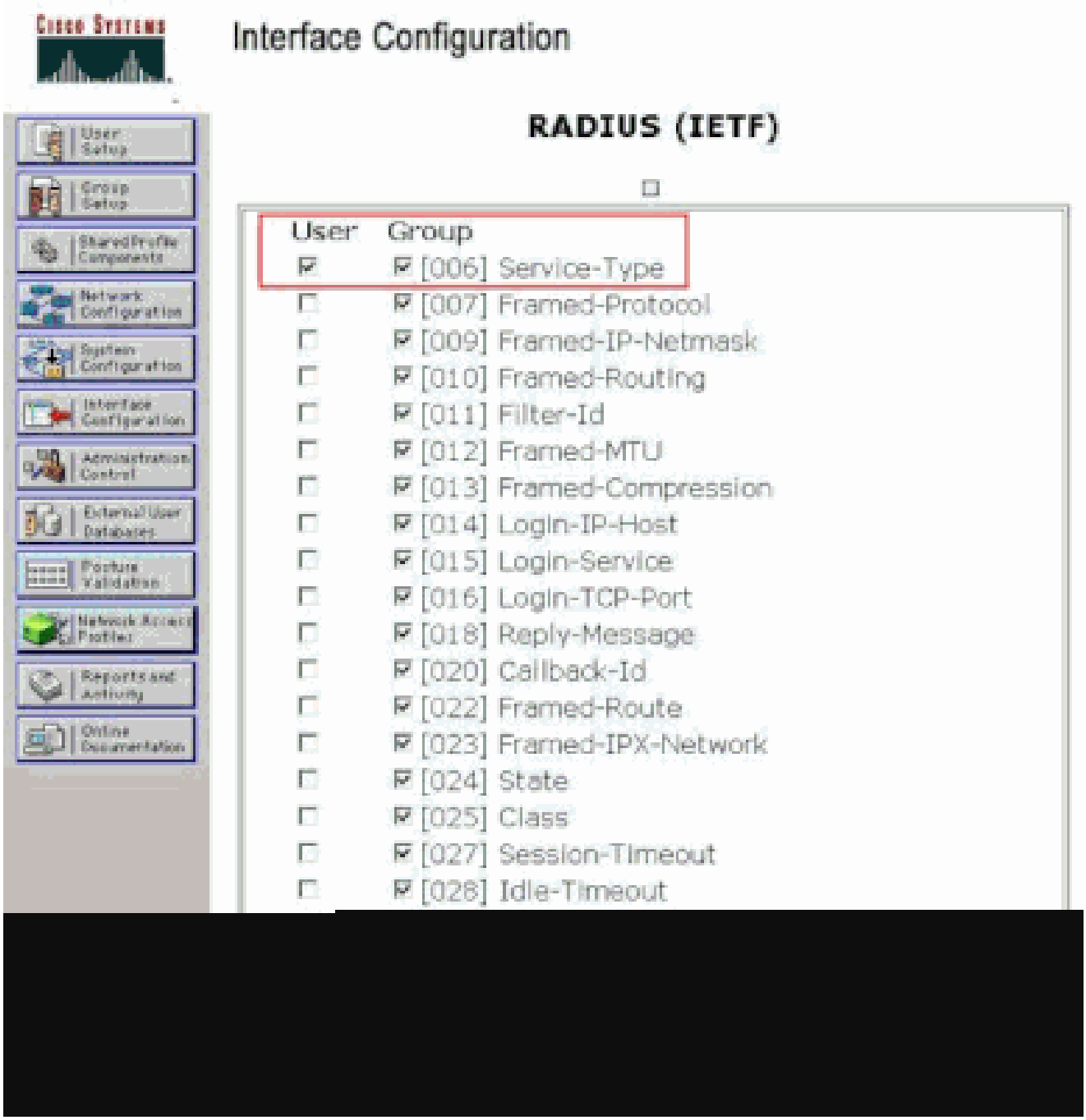
ETF RADIUSアトリビュートの設定

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このアトリビュートが表示されるようにします。

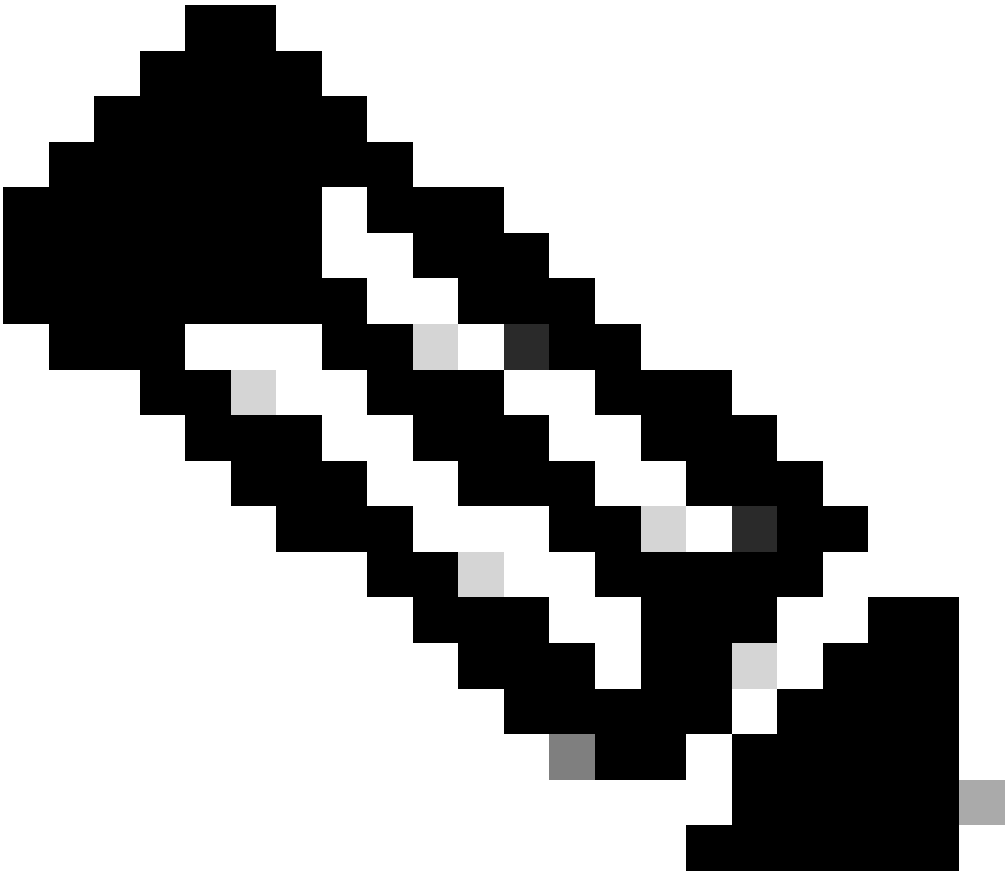
1. ACS の GUI から、IETF アトリビュートを有効にするために、[User Configuration] ウィンドウで [Interface Configuration] > [RADIUS (IETF)] の順に選択します。

   RADIUS (IETF) の設定ページが表示されます。

2. 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。



RADIUS(IETF)設定ページ



注：この例では、ユーザごとの認証を指定します。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、グループ設定でこのアトリビュートが表示されるように、[Group] チェック ボックスにチェックマークを付けます。 グループ単位で認証を行う場合は、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特権を与えるようにグループ設定の IETF アトリビュートを設定する必要もあります。グループの設定と管理の詳細については、『グループ管理』を参照してください。

読み取り専用アクセス権を持つユーザを設定する

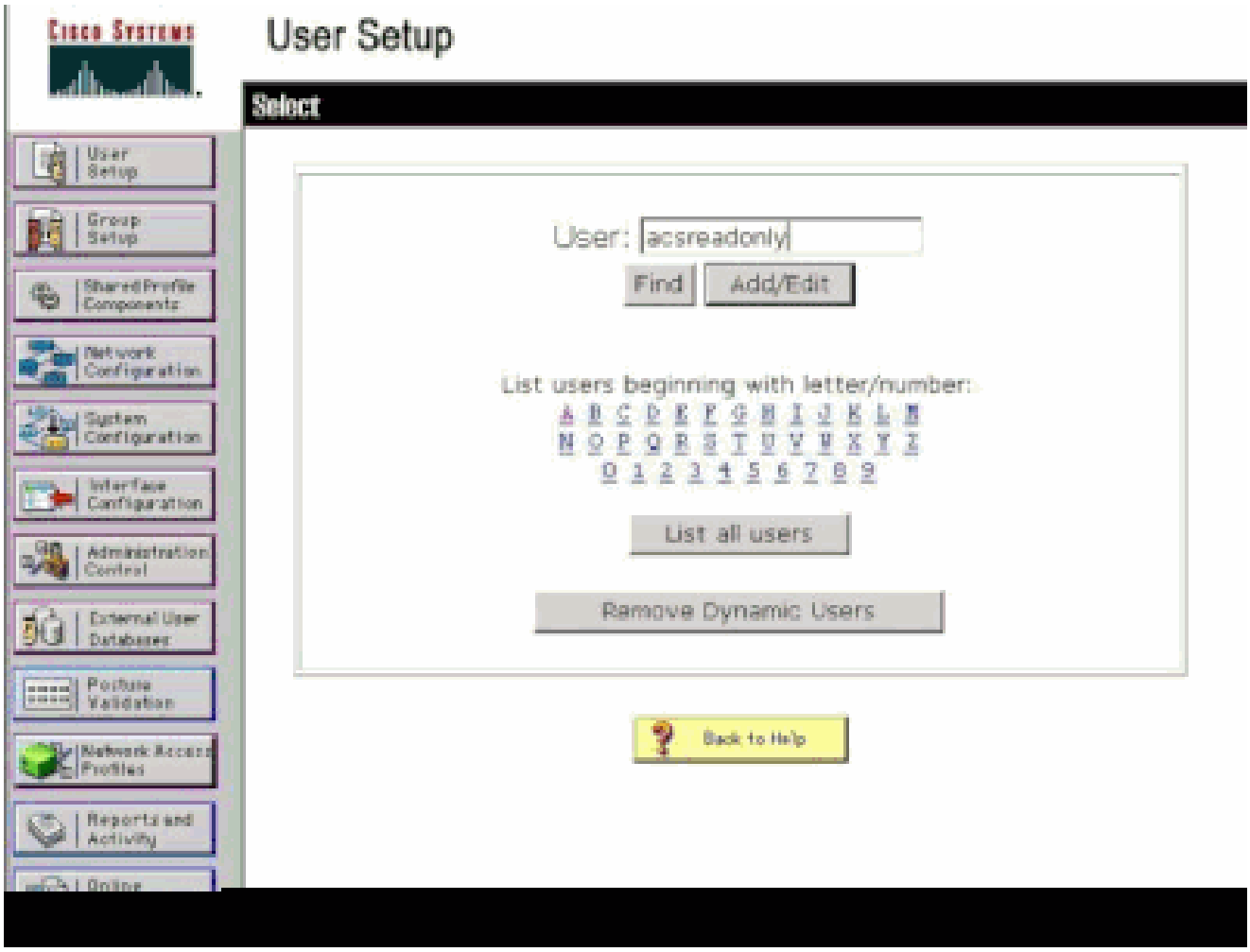
次の例は、WLC への読み取り専用アクセス権を持つユーザの設定を示しています。このユーザがコントローラにログインしようとすると、RADIUS サーバは認証を行って、このユーザに読み取り専用のアクセス権を付与します。

この例で使用するユーザ名とパスワードは acsreadonly です。

Cisco Secure ACS で次の手順を実行します。

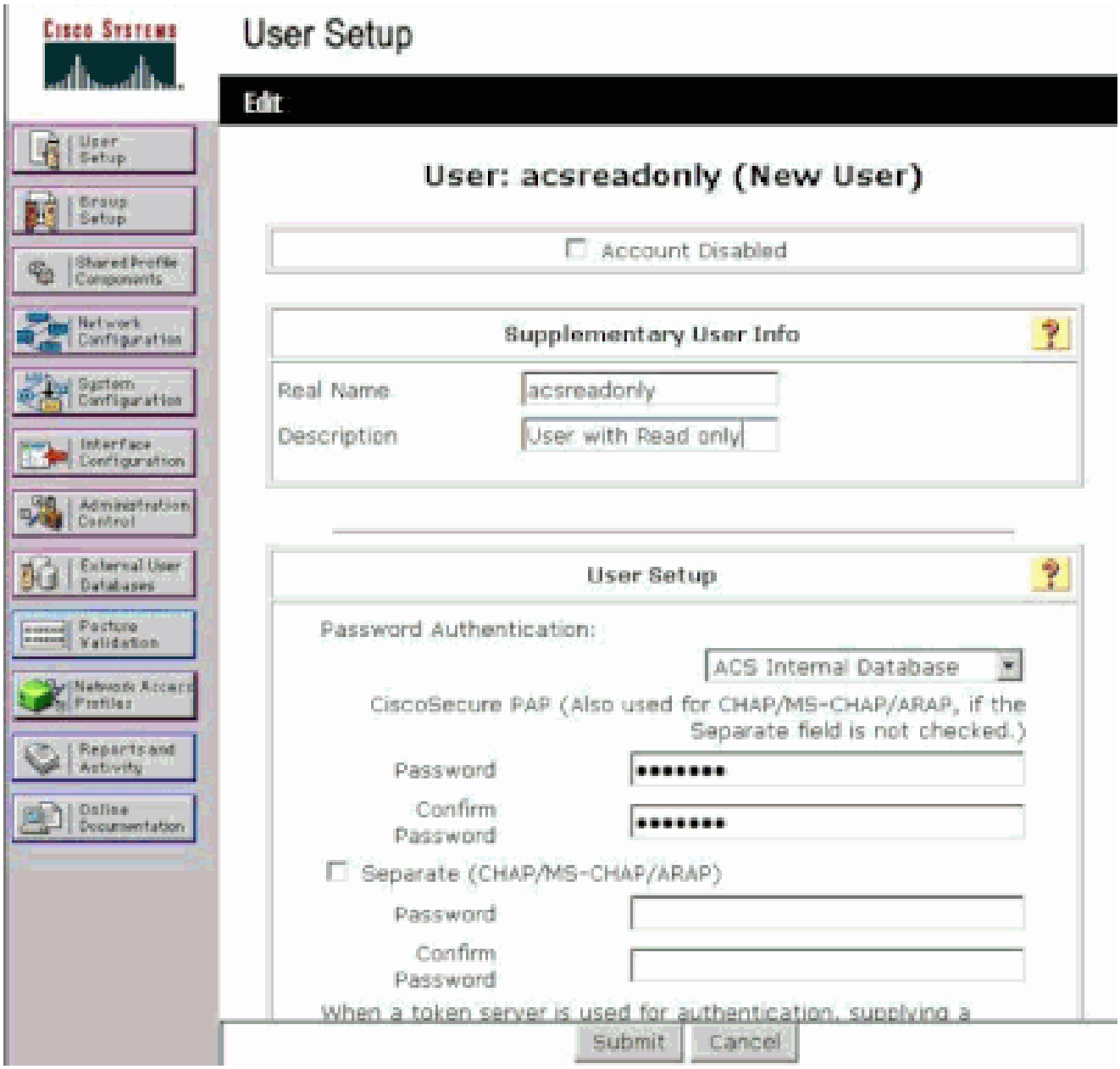
1. ACS の GUI で、[User Setup] をクリックします。

2. ACS に追加するユーザ名を入力し、[Add/Edit] をクリックして [User Edit] ページに移動します。



ユーザ名の追加

3. このユーザの Real Name、Description、および Password を入力します。次に例を示します。

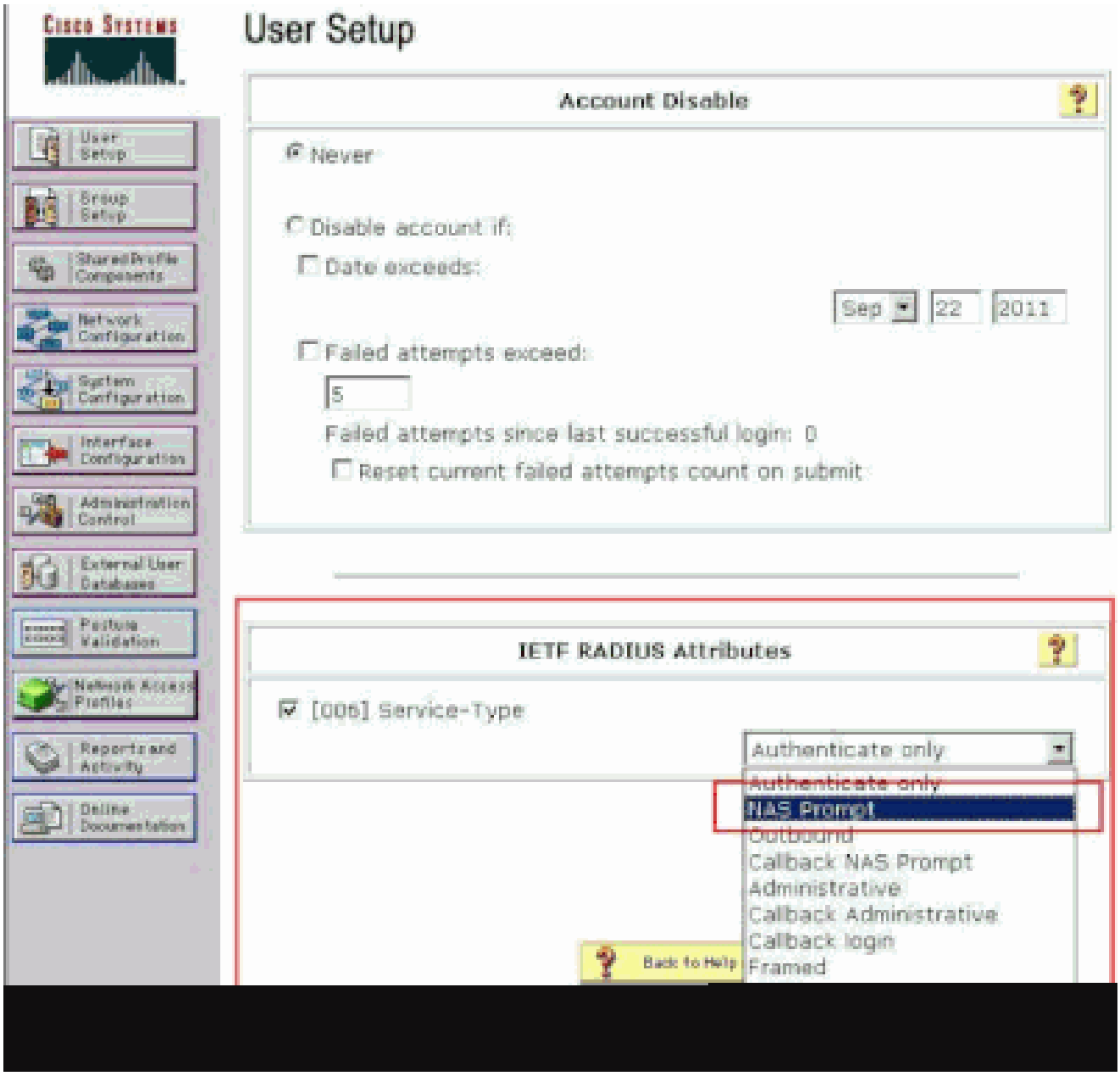


追加したユーザの実名、説明、およびパスワードを入力します

4. 下にスクロールして [IETF RADIUS Attributes] の設定に移動し、[Service-Type] アトリビュートにチェックマークを付けます。

5. この例では、ユーザ acsreadonly に読み取り専用アクセス権を与える必要があるので、[Service-Type] プルダウン メニューから [NAS Prompt] を選択し、[Submit] をクリックします。

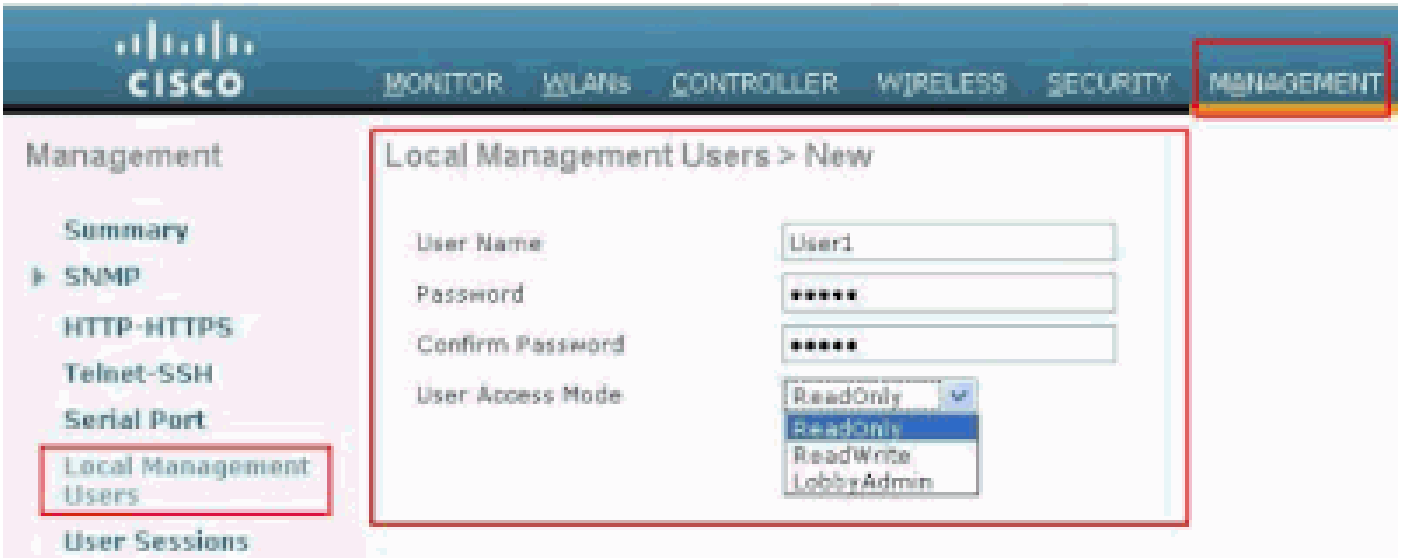
   これで、このユーザに WLC への読み取り専用アクセス権が与えられます。



Service-Type属性の確認

RADIUS サーバによる管理に加えてローカルで WLC を管理する方法

WLC 上でローカルに管理ユーザを設定することもできます。これを実行するには、コントローラの GUI から [Management] > [Local Management Users] の順に選択します。



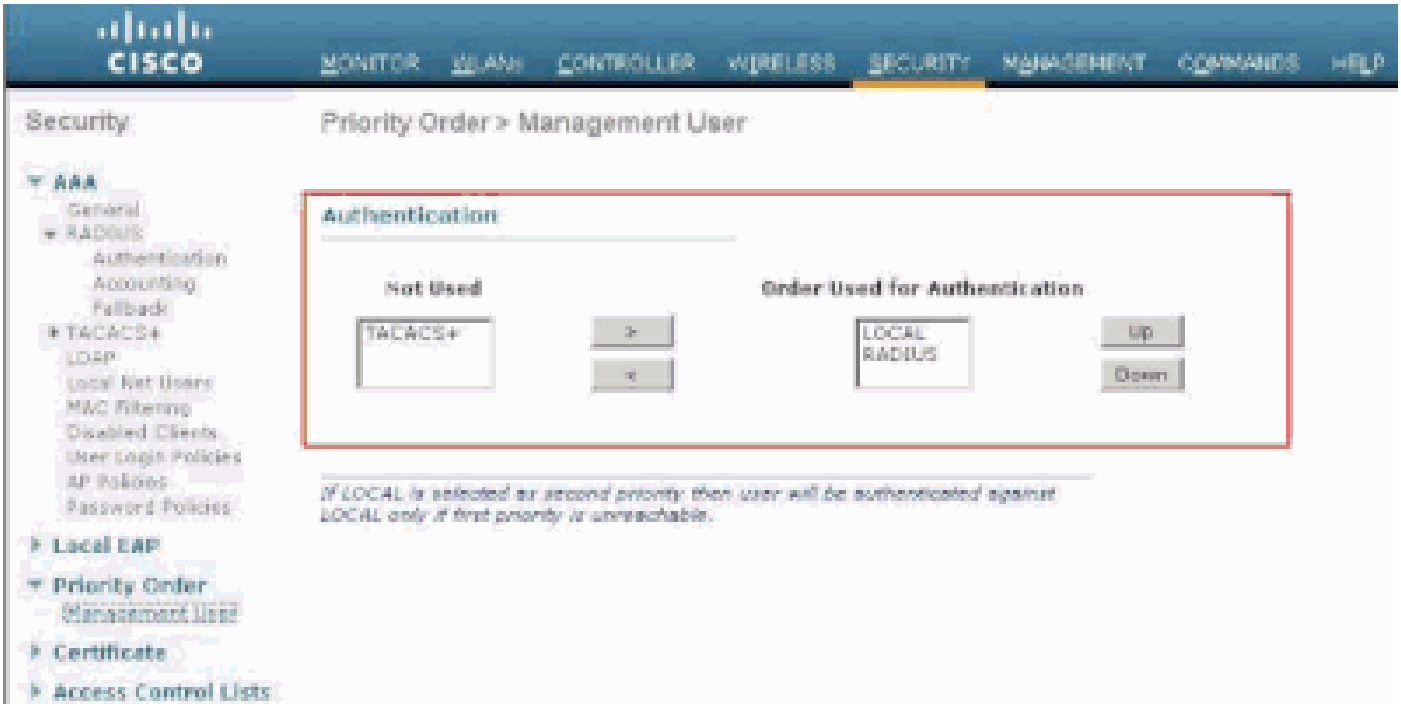
WLCでの管理ユーザのローカル設定

WLC で、[Management] チェック ボックスにチェックマークが付いている RADIUS サーバだけでなく、ローカルにも管理ユーザが設定されていると仮定します。このようなシナリオでは、ユーザが WLC にログインしようとすると、デフォルトでは WLC は次のように動作します。

1. WLC は、まずローカルで定義されている管理ユーザを探します。このユーザがローカルのリストに存在すれば、WLC はこのユーザを認証します。このユーザがローカルに存在しなければ、WLC は RADIUS サーバを検索します。

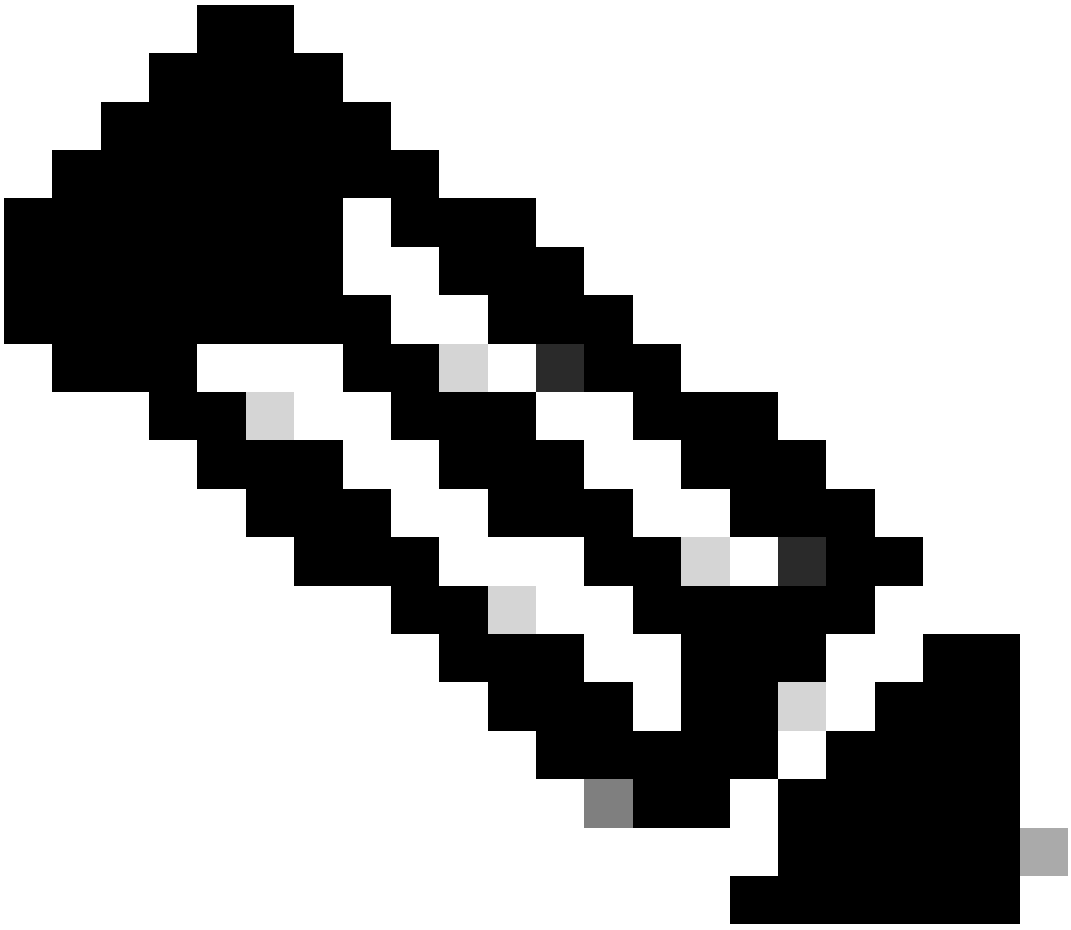
2. 同じユーザがローカルにも RADIUS サーバにも存在し、アクセス特権が異なる場合は、ローカルで指定されている特権でユーザを認証します。つまり、WLC のローカル設定は RADIUS サーバ上の設定より常に優先されます。

管理ユーザの認証の順序は WLC で変更できます。これを実行するには、WLC の [Security] ページから [Priority Order] > [Management User] をクリックします。 このページから、認証の順序を指定できます。次に例を示します。



Management User Selection" />

Priority Order > Management User Selection



注：2番目の優先順位としてLOCALを選択した場合、最初の優先順位として定義された方式(RADIUS/TACACS)が到達不能である場合にのみ、この方式を使用してユーザが認証されます。

確認

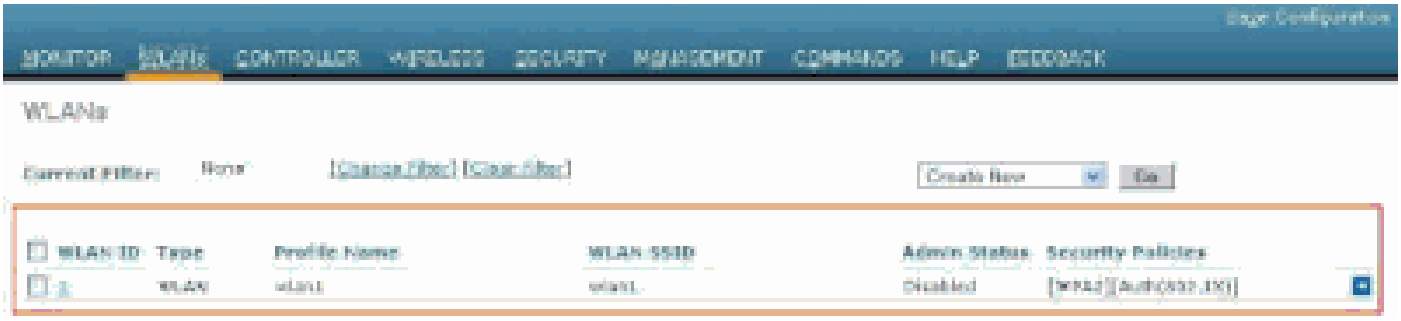
設定が正しく機能するかどうかを確認するには、CLI または GUI (HTTP/HTTPS) モードで WLC にアクセスします。ログイン プロンプトが表示されたら、Cisco Secure ACS で設定したユーザ名とパスワードを入力します。

設定が正しければ、認証に成功して WLC にログインできます。

また、ACS で指定したとおりのアクセス制限がユーザに適用されているかどうかを確認することもできます。これを確認するには、HTTP または HTTPS を使用して WLC の GUI にアクセスし

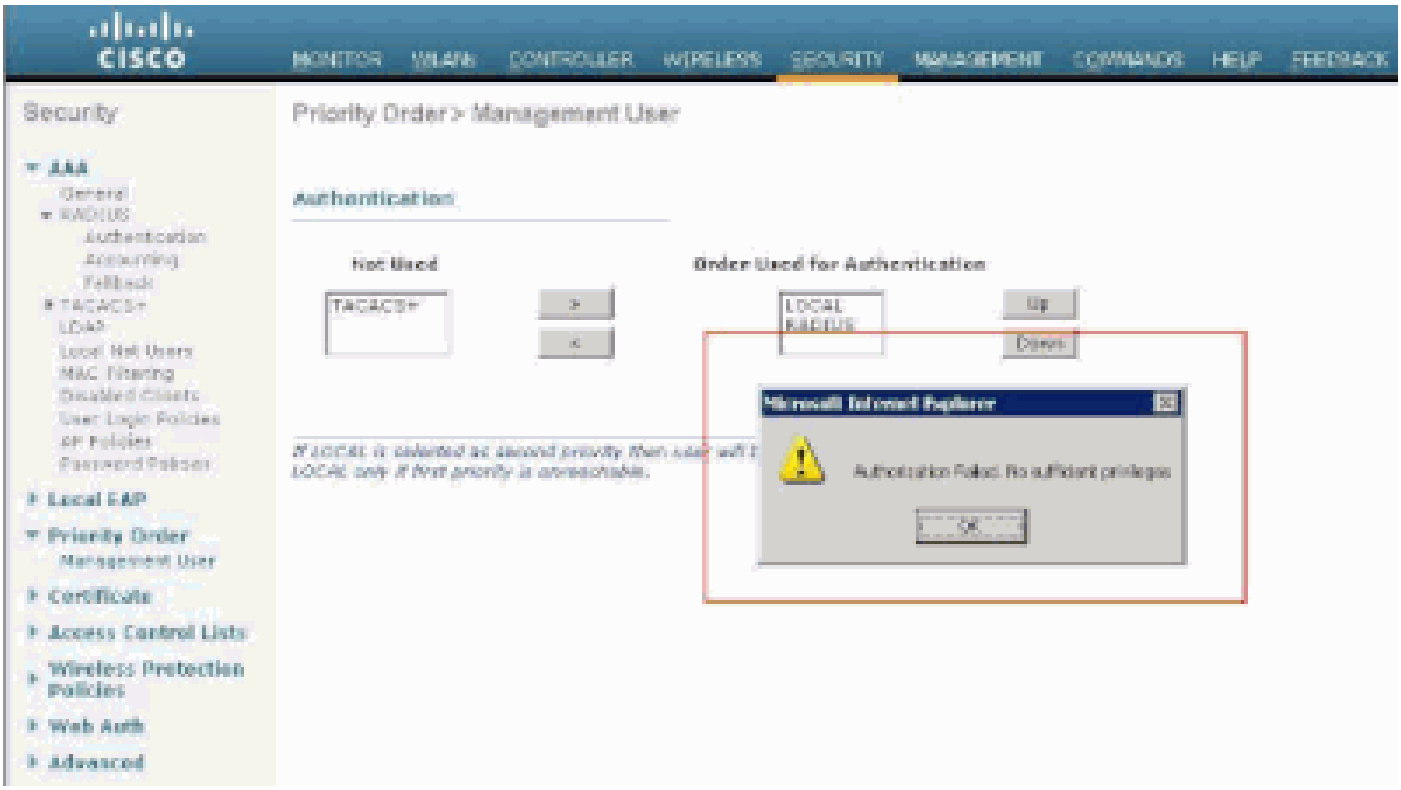
ます (HTTP または HTTPS を使用できるように WLC が設定されていることを確認してください)。

ACS で読み取り/書き込みアクセス権を与えられたユーザは、WLC で設定可能な特権を持っています。たとえば、読み取り/書き込みユーザは、WLC の WLANs ページで新しい WLAN を作成する特権を持っています。次に例を示します。



WLCで設定可能な特権

読み取り専用特権を持つユーザがコントローラの設定を変更しようとすると、次のメッセージが表示されます。



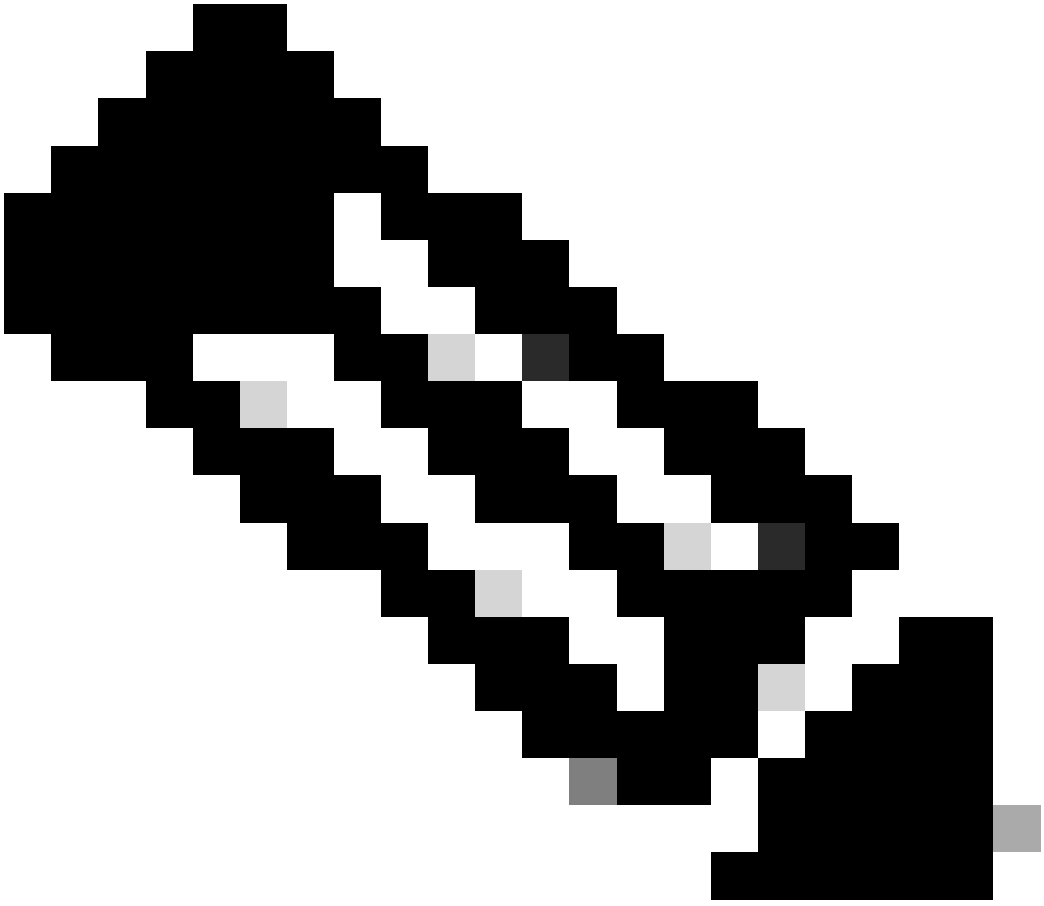
読み取り専用アクセス権を持つコントローラを変更できない

このアクセス制限は、WLC の CLI でも検証できます。次に出力例を示します。

```
<#root>

(Cisco Controller) >

?
```

```
debug           Manages system debug options.
help            Help
linktest        Perform a link test to a specified MAC address.
logout          Exit this session. Any unsaved changes are lost.
show            Display switch options and settings.

(Cisco Controller) >config

Incorrect usage.  Use the '?' or <TAB> key to list commands.
```

次の出力例に示すように、コントローラCLIの?には、現在のユーザが使用できるコマンドのリストが表示されます。また、この出力例に**config** コマンドが含まれていないことにも注意してください。これは、読み取り専用ユーザが WLC 上で設定を行う特権を持たないことを示しています。反対に、読み取り/書き込みユーザは、コントローラ上で (GUI および CLI モードで) 設定を行う特権を持っています。



注：RADIUSサーバでWLCユーザを認証した後でも、ページ間を移動しながらブラウズすると、毎回HTTP[S]サーバによってクライアントが完全に認証されます。各ページで認証プロンプトが表示されない理由は、ブラウザのキャッシュにクレデンシャルが保存されて自動的に送信されるためです。

トラブルシュート

コントローラがACSを介して管理ユーザを認証し、認証が正常に完了し(access-accept)、コントローラに認可エラーが表示されない場合があります。しかし、ユーザには再度認証のプロンプトが表示されます。

このような場合、**debug aaa events enable** コマンドだけでは、何が間違っていて、なぜユーザがWLCにログインできないのかを把握できません。コントローラが再び認証プロンプトを表示するだけです。

この問題の原因としては、ACS でユーザ名とパスワードが正しく設定されていたとしても、特定のユーザやグループの Service-Type アトリビュートを渡すように ACS が設定されていないことが考えられます。

debug aaa events enable

コマンドの出力は、AAAサーバから**access-accept**が送り返されているにもかかわらず、ユーザが必要な属性（Service-Type属性など）を持っていないことを示しているわけではありません。**debug aaa events enable** コマンドの出力例を次に示します。

<#root>

(Cisco Controller) >

debug aaa events enable

```
Mon Aug 13 20:14:33 2011: AuthenticationRequest: 0xa449a8c

Mon Aug 13 20:14:33 2011: Callback.....................................0x8250c40

Mon Aug 13 20:14:33 2011: protocolType.................................0x00020001

Mon Aug 13 20:14:33 2011: proxyState....................1A:00:00:00:00:00-00:00
```

```
Mon Aug 13 20:14:33 2011: Packet contains 5 AVPs (not shown)

Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Successful transmission of
Authentication Packet (id 8) to 172.16.1.1:1812, proxy state
1a:00:00:00:00:00-00:00

Mon Aug 13 20:14:33 2011: ****Enter processIncomingMessages: response code=2

Mon Aug 13 20:14:33 2011: ****Enter processRadiusResponse: response code=2
```

Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Access-Accept received from RADIUS server 172.16.1.1 for mobile 1a:00:00:00:00:00 receiveId = 0

```
Mon Aug 13 20:14:33 2011: AuthorizationResponse: 0x9802520

Mon Aug 13 20:14:33 2011: structureSize.............................28

Mon Aug 13 20:14:33 2011: resultCode.................................0

Mon Aug 13 20:14:33 2011: protocolUsed.............................0x00000001

Mon Aug 13 20:14:33 2011: proxyState.....................1A:00:00:00:00:00-00:00

Mon Aug 13 20:14:33 2011: Packet contains 0 AVPs:
```

最初の**debug aaa events enable** コマンドの出力例では、RADIUSサーバからAccess-Acceptを受信しているにもかかわらず、WLCにService-Typeアトリビュートが渡されていないことがわかります。これは、ACS 上でこのアトリビュートがこのユーザに対して設定されていないことが原因です。

Cisco Secure ACS はユーザ認証の後で Service-Type アトリビュートを返すように設定する必要があります。Service-Type属性値は、**ユーザ権限**に基づいて、**Administrative** または**NAS-Prompt** に設定する必要があります。

2番目の例も、**debug aaa events enable**コマンドの出力を示しています。ただし、今回は ACS 上で Service-Type アトリビュートが [Administrative] に設定されています。

```
    <#root>

(Cisco Controller)>
```

debug aaa events enable

Mon Aug 13 20:17:02 2011: AuthenticationRequest: 0xa449f1c

Mon Aug 13 20:17:02 2011: Callback.....0x8250c40

Mon Aug 13 20:17:02 2011: protocolType.....0x00020001

Mon Aug 13 20:17:02 2011: proxyState.....1D:00:00:00:00:00-00:00

Mon Aug 13 20:17:02 2011: Packet contains 5 AVPs (not shown)

Mon Aug 13 20:17:02 2011: 1d:00:00:00:00:00 Successful transmission of
Authentication Packet (id 11) to 172.16.1.1:1812, proxy state
1d:00:00:00:00:00-00:00

Mon Aug 13 20:17:02 2011: ****Enter processIncomingMessages: response code=2

Mon Aug 13 20:17:02 2011: ****Enter processRadiusResponse: response code=2

**Mon Aug 13 20:17:02 2011: 1d:00:00:00:00:00 Access-Accept received
from RADIUS server 172.16.1.1 for mobile 1d:00:00:00:00:00 receiveId = 0**

Mon Aug 13 20:17:02 2011: AuthorizationResponse: 0x9802520

Mon Aug 13 20:17:02 2011: structureSize.....100

Mon Aug 13 20:17:02 2011: resultCode.....0

Mon Aug 13 20:17:02 2011: protocolUsed.....0x00000001

Mon Aug 13 20:17:02 2011: proxyState.....1D:00:00:00:00:00-00:00

Mon Aug 13 20:17:02 2011: Packet contains 2 AVPs:

Mon Aug 13 20:17:02 2011: AVP[01] Service-Type.....0x00000006 (6) (4 bytes)

Mon Aug 13 20:17:02 2011: AVP[02] Class.....
CISCOACS:000d1b9f/ac100128/acsserver (36 bytes)

上記の出力例では、Service-TypeアトリビュートがWLCに渡されていることが確認できます。

関連情報

- **ワイヤレスLANコントローラの設定 – コンフィギュレーションガイド**
- **ワイヤレスLANコントローラでのVLANの設定**
- **ダイナミックVLAN割り当て用のRADIUSサーバおよびWLCの設定**
- **ワイヤレス LAN コントローラおよび Lightweight アクセスポイントの基本設定**
- **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**
- **シスコのテクニカルサポートとダウンロード**

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。