CHAPTER 8

RADIUS クライアントの設定

この章では、次の内容について説明します。

概要

Remote Authentication Dial In User Service（RADIUS）は、AAA（認証、許可、およびアカウント管理）プロトコルです。Cisco NAC ゲスト サーバは、RADIUS プロトコルを使用して、Cisco Wireless LAN コントローラなどの RADIUS 対応ネットワーク エンフォースメント デバイスを介してログインするゲストを認証し、監査します。

Cisco NAC アプライアンスは、「第 7 章「Cisco NAC アプライアンスとの統合」」で説明されているように、独自の API と特殊な方法を用いてアカウントの作成とユーザの認証を行います。しかし、RADIUS アカウンティングを使用してユーザのアクティビティを記録するため、RADIUS クライアントとして設定する必要があります。

ゲストが Wireless LAN コントローラなどの RADIUS クライアントに対する認証を受ける場合、RADIUS クライアントは RADIUS 認証を使用し、Cisco NAC ゲスト サーバにユーザ認証が有効かどうかを確認します。ゲスト認証が有効な場合、Cisco NAC ゲスト サーバは、そのユーザが有効であることを示すメッセージと、ユーザ セッションが期限切れになるまでの残りの時間を記したメッセージを返信します。RADIUS クライアントは、セッション タイムアウト属性に従って、ゲスト アカウントの期限が切れたときにゲストを削除する必要があります。

（注） Cisco Wireless LAN コントローラは特に AAA オーバーライドを可能にするように特別な設定をする必要があります。これにより、Cisco NAC ゲスト サーバから返されたセッション タイムアウト属性に従うことができます。

認証に加えて、RADIUS クライアント デバイスは、セッションの開始時刻や終了時刻、ユーザの IP アドレスなどの詳細を Cisco NAC ゲスト サーバに報告します。この情報は、RADIUS アカウンティング プロトコルにより転送されます。

ヒント　Cisco NAC ゲスト サーバと RADIUS クライアント間にファイアウォールがある場合、UDP ポート 1812 または 1645（RADIUS 認証）および UDP ポート 1813 または 1646（RADIUS アカウンティング）からのトラフィックが通過できるように設定する必要があります。

（注）　Cisco NAC ゲスト サーバの RADIUS コンポーネントに変更を加えるたびに、[Restart] ボタンを押して RADIUS サービスを再起動し、変更をアクティブにする必要があります。

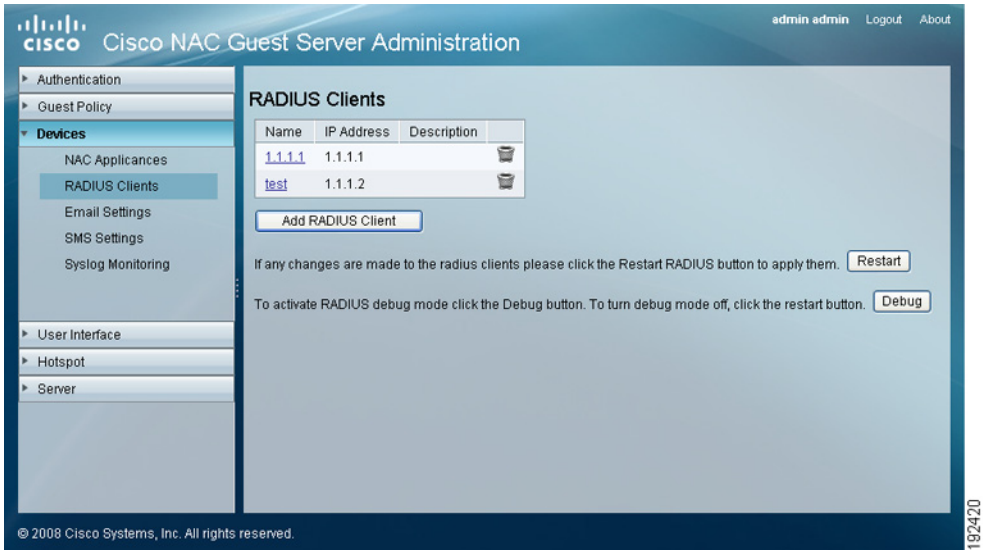
（注）　[Devices] > [RADIUS Clients] の下にある [Debug] ボタンをクリックすると、RADIUS サーバがデバッグ モードで有効になります。これにより、詳細なデバッグ情報が [Server] > [System Logs] > [Support Log] の下に表示されます。詳細については、「サポート ログ」（P.15-8）を参照してください。

RADIUS クライアントの追加

ステップ 1　管理インターフェイスの左側のメニューから、[Devices] > [RADIUS Clients] を選択します。

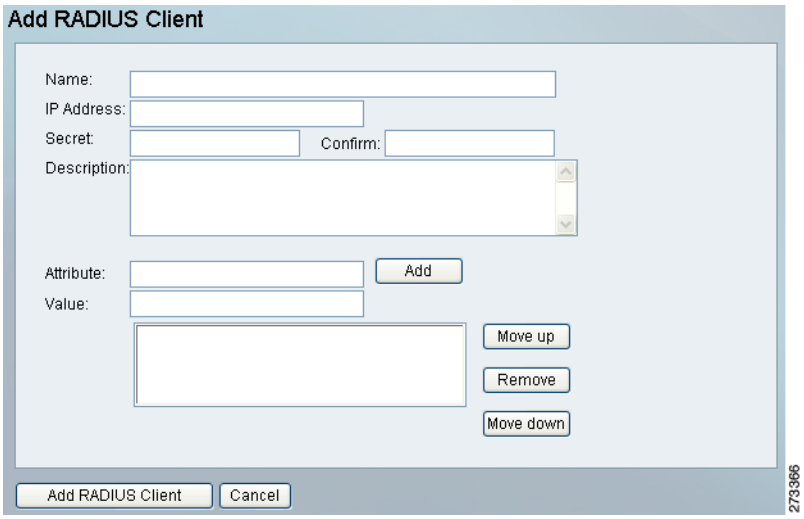
ステップ 2　[RADIUS Clients] ページ（図 8-1 を参照）で、[Add RADIUS Client] ボタンをクリックし、RADIUS クライアントを追加します。

図 8-1　RADIUS Clients



ステップ 3　[Add RADIUS Client] ページ（図 8-2 を参照）で、[Name] に RADIUS クライアントを説明する名前を入力します。

図 8-2　Add RADIUS Client



ステップ 4　[IP Address] に、RADIUS クライアントの IP アドレスを入力します。これは、RADIUS 要求が発生する IP アドレスと一致している必要があります。

ステップ 5　[Secret] に、RADIUS クライアントの共有秘密を入力します。これは、RADIUS クライアントの設定で指定された共有秘密と一致している必要があります。

ステップ 6　[Confirm] フィールドに共有秘密を再入力します。

ステップ 7　[Description] にクライアントおよびその他の必要な情報を入力します。

ステップ 8　認証が成功したときに RADIUS クライアントで追加の属性が送信されるようにする場合は、[Attribute] フィールドと [Value] フィールドに属性名と値を入力し、[Add] ボタンをクリックします。必要な数の属性を入力できます。

- 属性を削除する場合は、テーブルから属性を選択し、[Remove] ボタンをクリックします。
- [Move up] および [Move down] ボタンを使用して、RADIUS Accept メッセージで送信されるときの RADIUS 属性の順序を変更します。

ステップ 9　完了したら、[Add RADIUS Client] ボタンをクリックします。

ステップ 10　管理インターフェイスから、[Devices] >[RADIUS Clients] を選択します（図 8-1 を参照）。

ステップ 11　[Restart] ボタンをクリックして、RADIUS サービスを再起動し、変更を有効にします。

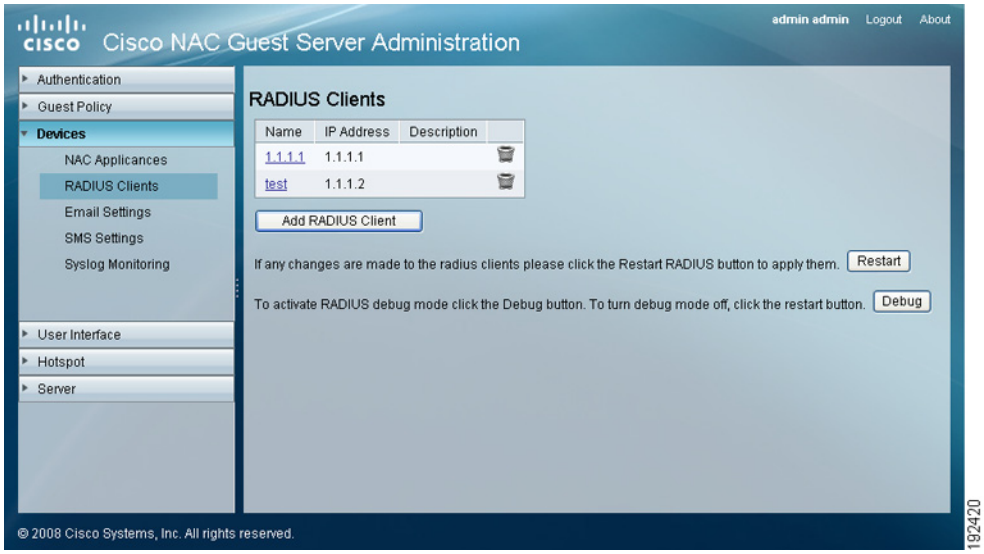
（注）　NAC ゲスト サーバは、RADIUS 認証の PAP だけをサポートしています。

RADIUS クライアントの編集

ステップ 1　管理インターフェイスの左側のメニューから、[Devices] > [RADIUS Clients] を選択します。

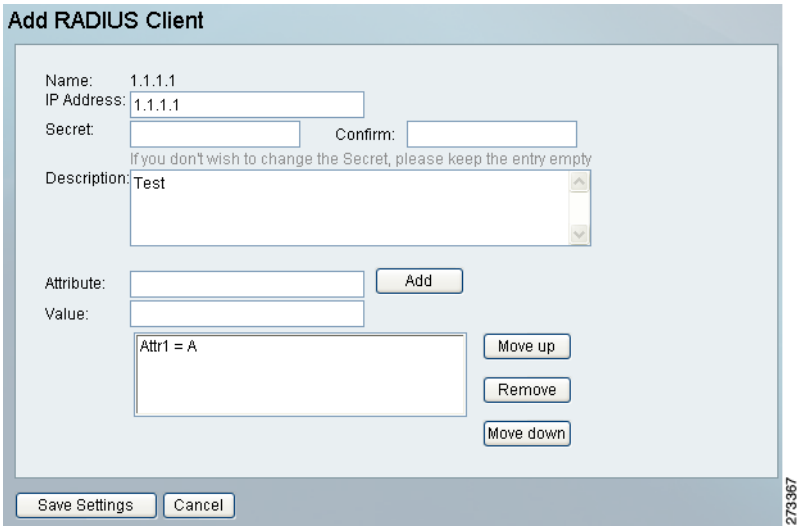
ステップ 2　[RADIUS Clients] ページ（図 8-3 を参照）で、リストから編集する RADIUS クライアントを選択し、そのクライアントの下線の付いた名前をクリックします。

図 8-3　RADIUS Clients のリスト



ステップ 3　[Edit RADIUS Client] ページ（図 8-4 を参照）で、RADIUS クライアントの [IP Address] を編集します。

図 8-4　Edit RADIUS Client



ステップ 4　[Secret] フィールドと [Confirm] フィールドでクライアントと Cisco NAC ゲスト サーバ間で使用されている共有秘密を編集します。

ステップ 5　[Description] に、必要な変更を加えます。

ステップ 6　認証が成功したときに NAC ゲスト サーバで追加の RADIUS 属性が RADIUS Client に送信されるようにする場合は、[Attribute] フィールドと [Value] フィールドに属性名と値を入力し、[Add] ボタンをクリックします。必要な数の属性を入力できます。属性を削除する場合は、テーブルから属性を選択し、[Remove] ボタンをクリックします。

ステップ 7　[Save Settings] をクリックします。

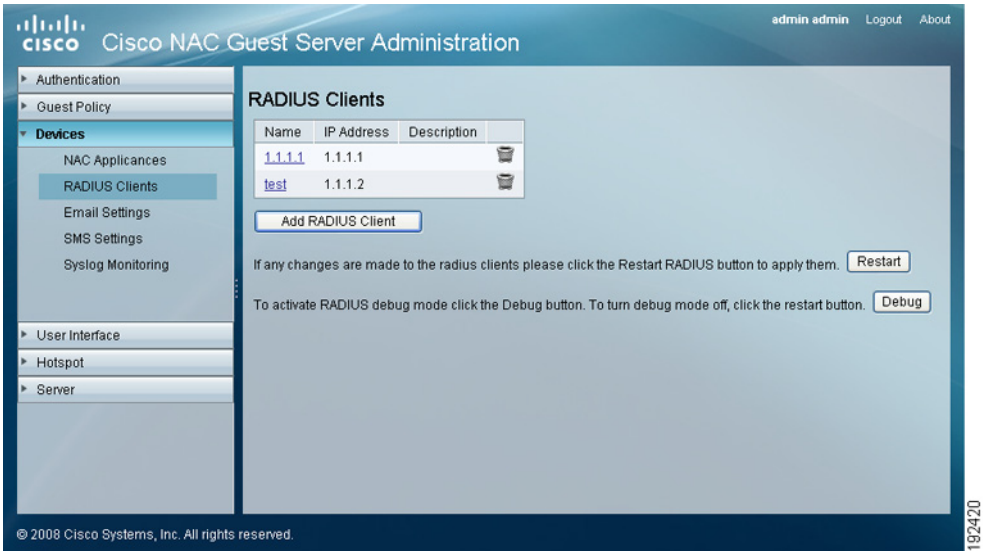
ステップ 8　管理インターフェイスの左側のメニューから、[Devices] > [RADIUS Clients] を選択します（図 8-1 を参照）。

ステップ 9　[Restart] ボタンをクリックして、RADIUS サービスを再起動し、変更を有効にします。

RADIUS クライアントの削除

ステップ 1　管理インターフェイスの左側のメニューから、[Devices] > [RADIUS Clients] を選択します。

図 8-5　RADIUS Clients のリスト



ステップ 2　[RADIUS Clients] ページ（図 8-5 を参照）で、リスト内の RADIUS クライアントの下線の付いた名前をクリックして編集します。

ステップ 3　エントリの右側にあるゴミ箱アイコンをクリックしてエントリを削除し、アクションを確認します。

ステップ 4　管理インターフェイスの左側のメニューから、[Devices] > [RADIUS Clients] を選択します（図 8-1 を参照）。

ステップ 5　[Restart] ボタンをクリックして、RADIUS サービスを再起動し、変更を有効にします。

（注）　RADIUS コンポーネントに変更を加えるたびに、RADIUS サービスを再起動して変更をアクティブにする必要があります。