CHAPTER 6

ゲスト ポリシーの設定

一般的な組織では、ユーザ名のフォーマット、長さ、パスワードの複雑さなど、内部ユーザや内部システム向けのアカウント作成に関するポリシーが定められています。Cisco NAC ゲスト サーバにより、ゲスト ユーザ名およびパスワードの作成ポリシーを組織のポリシーに適合するように設定したり、ゲスト アカウント独自のポリシーを作成したりすることができます。

ゲスト詳細ポリシーを使用して、Cisco NAC ゲスト サーバ上で特定のゲスト ユーザ情報を定義することもできます。

Cisco NAC ゲスト サーバによって、ゲストに対してさまざまなロールを設定できます。ゲスト ロールを使用すると、さまざまなゲスト アカウントに対してさまざまなレベルのアクセスを提供できます（たとえば、さまざまなゲスト ロールを Clean Access Manager ロールにマッピングしたり、さまざまな RADIUS 属性を割り当てたり、特定の IP アドレスの範囲からのゲストだけにアクセスを許可するなど）。

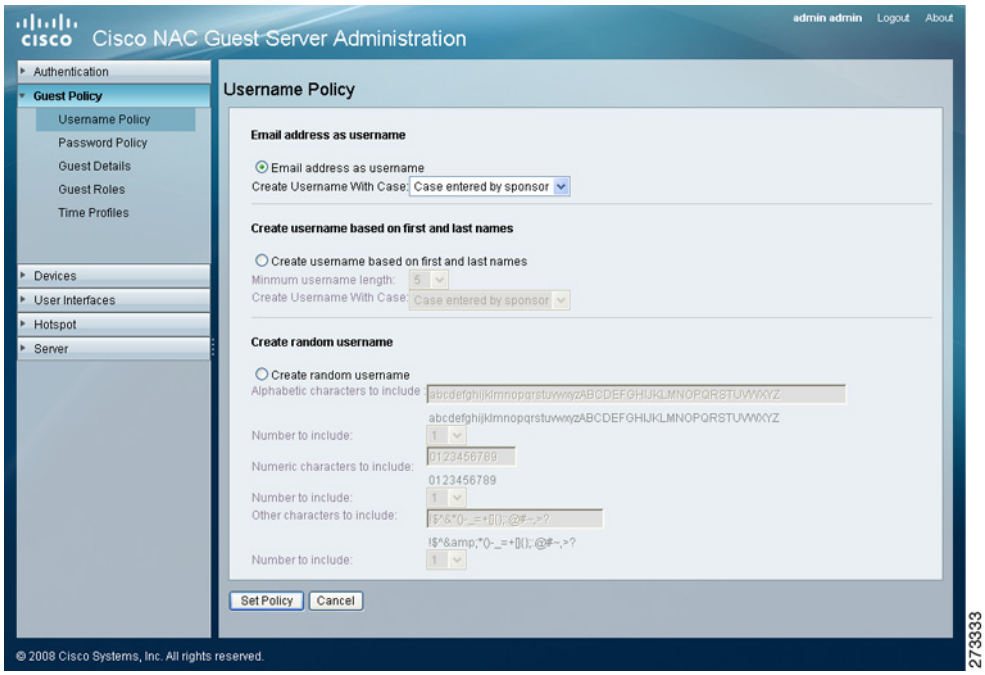
この章では、次の内容について説明します。

ユーザ名ポリシーの設定

ユーザ名ポリシーでは、すべてのゲスト アカウントのユーザ名の作成方法を決定します。

ステップ 1 管理インターフェイスから、[Guest Policy] > [Username Policy] を選択します（図 6-1 を参照）。

図 6-1　　ゲスト ユーザ名ポリシー



ステップ 2　ゲスト アカウントのユーザ名の作成に関して、次のユーザ名ポリシーのオプションのいずれかを選択します。

a. ユーザ名ポリシー 1：Email address as username

ゲストの電子メール アドレスをユーザ名として使用します。同一電子メール アドレスを持つ重複するアカウントがある場合、電子メール アドレスの最後にランダムな番号を追加し、ユーザ名を一意にします。重複するアカウントとは同一の電子メール アドレスを持つアカウントを意味し、有効な期間が重複しています。

[Create Username With Case] オプションを使用して、スポンサーによって作成されたゲスト ユーザ名の大文字小文字の表記を決定できます。

- [Case entered by sponsor]：ユーザ名の大文字小文字の設定をスポンサーによる設定のままにします。
- [UPPERCASE]：ユーザ名が、スポンサーによって設定された後に、強制的に大文字にされます。
- [lowercase]：ユーザ名が、スポンサーによって設定された後に、強制的に小文字にされます。

b. ユーザ名ポリシー 2：Create username based on first and last names

ゲストの名前と姓を組み合わせることにより、ユーザ名を作成します。このユーザ名の [Minimum username length] を 1 ～ 20 文字に設定できます（デフォルトは 10）。最小文字数未満のユーザ名は、ランダムな数字を加えて最小文字数以上にします。

[Create Username With Case] オプションを使用して、スポンサーによって作成されたゲスト ユーザ名の大文字小文字の表記を決定できます。

- [Case entered by sponsor]：ユーザ名の大文字小文字の設定をスポンサーによる設定のままにします。
- [UPPERCASE]：ユーザ名が、スポンサーによって設定された後に、強制的に大文字にされます。
- [lowercase]：ユーザ名が、スポンサーによって設定された後に、強制的に小文字にされます。

c. ユーザ名ポリシー 3 - Create random username

アルファベット、数字、特殊文字のランダムな組み合わせにより、ユーザ名を作成します。各文字のセットから名前に含める文字を入力して、使用するランダムな文字と数字を生成します。

（注）　ユーザ名の全体の長さは、含まれる文字数の合計により決定されます。

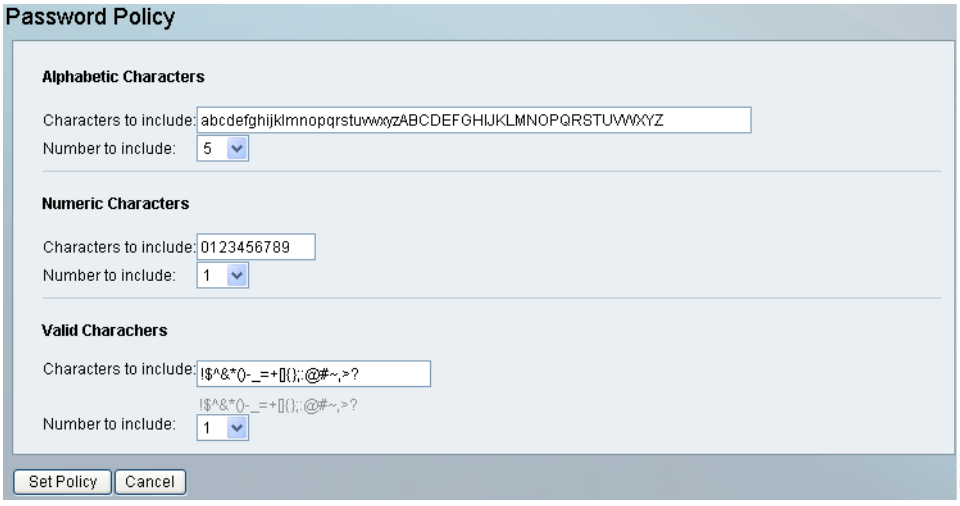
ステップ 3　終了したら、[Save] をクリックしてユーザ名ポリシーを適用します。

パスワード ポリシーの設定

パスワード ポリシーでは、すべてのゲスト アカウントのパスワードの作成方法を決定します。

ステップ 1　管理インターフェイスから、[Guest Policy] > [Password Policy] を選択します（図 6-2 を参照）。

図 6-2　パスワード ポリシー



ステップ 2　[Alphabetic Characters] セクションで、パスワードで使用する文字と文字数を入力します。

ステップ 3　[Numeric Characters] セクションで、パスワードで使用する数字と文字数を入力します。

ステップ 4　[Other Characters] セクションで、パスワードで使用する特殊文字と文字数を入力します。

注意　[Other Characters] フィールドのパスワードには、**!$^&*()-_=+[]{};:@#~,>?** だけを使用します。次の文字は、Clean Access Manager API で**サポートされていない**ため [Other Characters] フィールドでは**使用しないでください**。
£ % < ¬ ` ' \ |。

ステップ 5　[Save] ボタンをクリックして、設定を保存します。

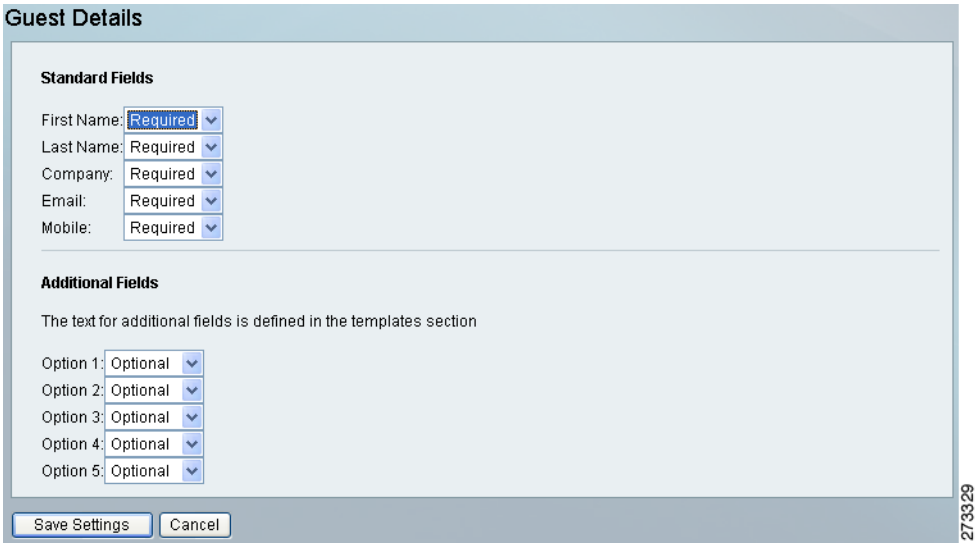
（注）　パスワードの全体の長さは、含まれる文字数の合計により決定されます。それぞれのフィールド（アルファベット、数字、特殊文字）で、0 ～ 20 字を選択できます。

ゲスト詳細ポリシーの設定

ゲスト詳細ポリシーでは、スポンサーがゲスト アカウントを作成するために入力する必要があるデータを決定します。

ステップ 1　管理インターフェイスから、[Guest Policy] > [Guest Details] を選択します（図 6-3 を参照）。

図 6-3　ゲスト詳細ポリシー



ステップ 2　各要件に対して 3 つの設定のいずれかを指定できます。

- [Required]：フィールドが [Required] に設定されている場合、そのフィールドは [Create Guest Account] ページに表示され、スポンサーによる入力が必須になります。
- [Optional]：フィールドが [Optional] に設定されている場合、そのフィールドは [Create Guest Account] ページに表示されます。ただし、スポンサーは、フィールドに入力が行われないように選択できます。
- [Unused]：フィールドが [Unused] に設定されている場合、そのフィールドは [Create Guest Account] ページに表示されず、どのような値も要求されません。

ステップ 3　[Save] ボタンをクリックして、ゲスト詳細ポリシーを保存します。

（注）　ゲスト アカウントを作成するときに、スポンサーに入力を求める任意の追加情報を追加するために使用できる 5 つの [Additional Fields] があります。これらは [Guest Details] ページに [Option 1] から [Option 5] として記述されます。これらのフィールドを使用する場合は、「ユーザ インターフェイス テンプレート」（P.11-1）での説明に従って、テンプレートの編集によってスポンサーに対して表示されるテキストをカスタマイズすることを推奨します。

ゲスト ロールの設定

ゲスト ロールは、さまざまなゲスト アカウントへのさまざまなアクセスのレベルを与える方法を提供します。たとえば、Clean Access Manager ロールへのさまざまなゲスト ロールのマップ、異なる RADIUS 属性の割り当て、または特定の IP アドレス範囲からのみのゲストへのアクセスの許可を実行できます。

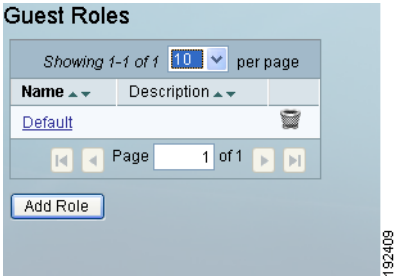
ゲスト ロールが作成されると、そのグループ内のスポンサーが適切なロールにおけるアカウントをプロビジョニングできるように許可するために、ユーザ グループを変更する必要があります。スポンサーによるさまざまなゲスト ロールの割り当て方法については、「ゲスト ロールの割り当て」（P.5-13）を参照してください。

ゲスト ロールの追加

次の手順を使用して新しいゲスト ロールを追加できます。

ステップ 1　管理インターフェイスから、[Guest Policy] > [Guest Roles] を選択します（図 6-4 を参照）。

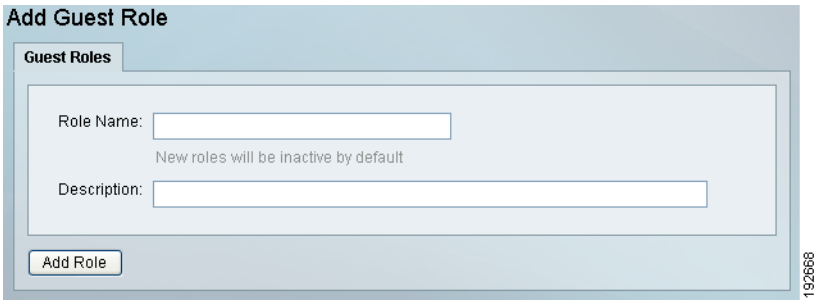
図 6-4　ゲスト ロール



ステップ 2　[Add Role] ボタンをクリックして新しいゲスト ロールを追加します。

ステップ 3　[Add Guest Role] ページ（図 6-5 を参照）から、新しいゲスト ロールの名前を入力します。

図 6-5　新しいゲスト ロールの追加



ステップ 4　表示されるフィールドにロール名と説明を入力します。

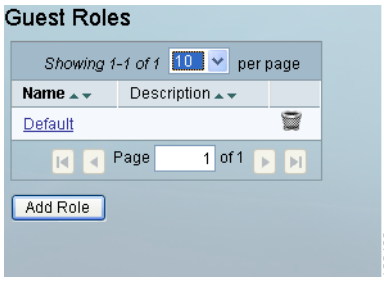
ステップ 5　[Add Role] ボタンをクリックして、ゲスト ロールを追加します。ここで、「ゲスト ロールの編集」（P.6-6）の説明に従って、新しいゲスト ロールの設定を編集できます。

ゲスト ロールの編集

次の手順で、ゲスト ロールの編集方法を説明します。

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、[Guest Policy] > [Guest Roles] を選択します。

図 6-6　ゲスト ロールの編集



ステップ 2　編集するロールを選択し、そのロールの下線付きの名前（図 6-6 を参照）をクリックして、[NAC Roles] の編集画面を表示します。次の属性を編集できます。

- NAC ロールの編集
- RADIUS 属性の編集
- ロケーションの編集
- 認証の設定の編集

NAC ロールの編集

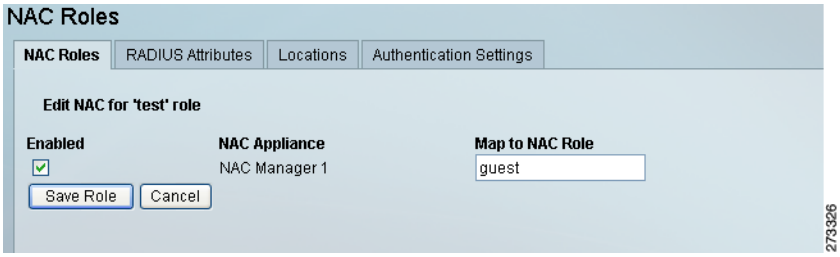
各ロールに対して、どの Clean Access Manager に対してゲスト アカウントがプロビジョニングされるか、およびその Clean Access Manager が使用されるロール名を指定できます。

デフォルトでは、どの Clean Access Manager も選択されておらず、表示されるロールは関連する Cisco NAC Appliance 設定からコピーされます。詳細については、第 7 章「Cisco NAC アプライアンスとの統合」を参照してください。

ステップ 1　管理インターフェイスから、[Guest Policy] > [Guest Roles] を選択し、編集するロールの下線付きの名前をクリックします。

ステップ 2　ページの上部から [NAC Roles] を選択します。

図 6-7　NAC ロール



ステップ 3　Cisco NAC アプライアンスごとに、このゲスト ロールが Clean Access Manager に対してプロビジョニングされた状態でアカウントを作成する場合は、[Enabled] ボックスをオンにします。

ステップ 4　Cisco NAC アプライアンスごとに、ゲスト アカウントを作成する Cisco NAC アプライアンスのロールに対応する [Map to NAC Role] フィールドにロールを入力します。

ステップ 5　[Save Role] ボタンをクリックします。

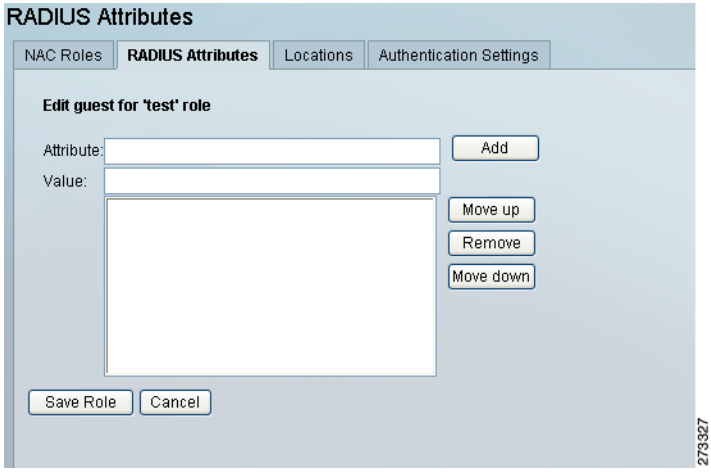
RADIUS 属性の編集

ゲストが Cisco Wireless LAN Controller などの RADIUS クライアント デバイスを使用して認証を行う場合は、正常な認証に対して送信される追加の RADIUS 属性を各ロールに対して指定できます。

ステップ 1　管理インターフェイスから、[Guest Policy] > [Guest Roles] を選択し、編集するロールの下線付きの名前をクリックします。

ステップ 2　ページの上部から [RADIUS Attributes] を選択します（図 6-8 を参照）。

図 6-8　RADIUS 属性



ステップ 3　各 [Attribute] と [Value] の組み合わせを入力し、[Add] ボタンをクリックします。

ステップ 4　送信される属性を並べ替える必要がある場合は、[Move up] ボタンと [Move down] ボタンを使用します。

ステップ 5　[Save Role] ボタンをクリックして、RADIUS 属性を保存します。

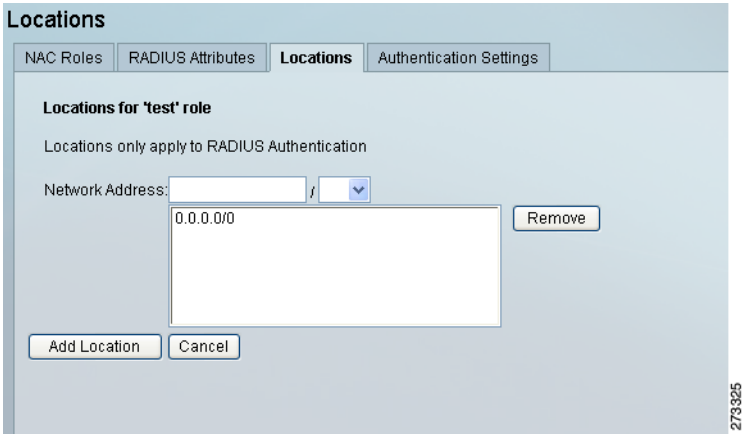
ロケーションの編集

Cisco Wireless LAN Controller などの RADIUS クライアント デバイスを使用してゲストが認証する場合、どの IP アドレスの範囲からゲストが各ロールに対する認証を行うことを許可されるかを指定できます。これによって、特定のロールに割り当てられているゲストが指定するロケーションからだけログインできるように、ロケーションに基づいてロールを指定できます。

ステップ 1　管理インターフェイスから、[Guest Policy] > [Guest Roles] を選択し、編集するロールの下線付きの名前をクリックします。

ステップ 2　[Locations] タブをクリックします（図 6-9 を参照）。

図 6-9　　ロケーション



ステップ 3　各 [Network Address] を入力し、ドロップダウン メニューから適切なプレフィックスの長さを選択します。有効なネットワーク アドレスだけが受け入れられます。ホスト アドレスは /32 プレフィックスの長さを使用して指定する必要があります。

ステップ 4　[Add Location] ボタンをクリックしてネットワーク アドレスを追加します。

（注）　ロールを追加すると、ロケーション 0.0.0.0/0 が自動的に追加されます。これは、ロールがどの IP アドレスからも有効であることを意味します。他の IP アドレスの範囲を制限する場合は、このアドレスを削除する必要があります。

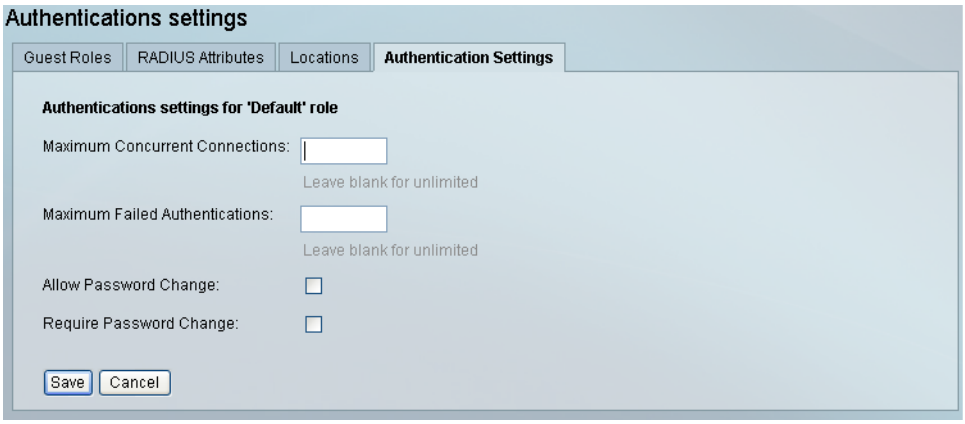
（注）　ロケーションは、Cisco Wireless LAN Controller などの RADIUS クライアントを通して認証するユーザだけに適用されます。

認証の設定の編集

ステップ 1　管理インターフェイスから、[Guest Policy] > [Guest Roles] を選択し、編集するロールの下線付きの名前をクリックします。

ステップ 2　[Authentication Settings] タブをクリックします（図 6-10 を参照）。

図 6-10　認証設定



ステップ 3　このロールのゲストの [Maximum Concurrent Connections] の数を入力します。これは、ゲスト アカウントが関連付けを許可された同時接続の最大数を設定します。接続数および認証数を無制限にするには、このフィールドは空白のままにします。

ステップ 4　このロールのゲストの [Maximum Failed Authentications] の数を入力します。これは、アカウントが一時停止される前に、ゲストに許可される認証失敗の最大試行回数を設定します。接続数および認証数を無制限にするには、このフィールドは空白のままにします。

ステップ 5　ゲストがパスワードを変更できるようにするには、[Allow Password Change] チェックボックスをオンにします。パスワード変更ウィジェットを使用するには、このオプションをオンにします。

ステップ 6　最初のログイン時に、パスワードの変更をゲストに強制するには、[Require Password Change] チェックボックスをオンにします。このオプションは、ゲスト ログインを許可するすべてのウィジェット（ログイン、セルフ サービス、請求）に適用され、ゲスト サーバにログインする前に、ゲストにパスワードの変更を強制します。ページにパスワード変更を含めるには、次のスクリプトを追加します。

```
<html>
<head>
</head>
<body>
<script type="text/javascript"
src="/sites/js/ngs_password.js"></script>
</body>
</html>"
```

ステップ 7　[Save] ボタンをクリックして変更を保存します。詳細については、「パスワード変更ページの作成（WLC およびスイッチ）」（P.12-27）を参照してください。

時間プロファイルの設定

時間プロファイルでは、さまざまなレベルの時間がさまざまなゲスト アカウントにアクセスできるようにします。たとえば、週末ではなく特定の営業日の間にゲストのアクセスを許可する時間プロファイルを割り当てることができます。

時間プロファイルを作成したら、スポンサー ユーザ グループに含まれるスポンサーが作成された適切な時間プロファイルにアカウントをプロビジョニングできるように、そのグループを変更する必要があります。スポンサーがさまざまな時間プロファイルを割り当てることができるようにする方法の詳細については、「時間プロファイルの割り当て」（P.5-15）を参照してください。

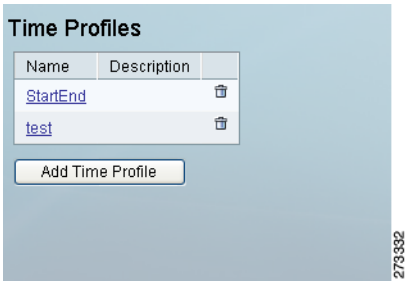
（注）　Cisco NAC ゲスト サーバ バージョン 2.0 以降は、Cisco NAC アプライアンスと共に使用される場合に、開始/終了プロファイルおよび作成からのプロファイルだけをサポートしています。

時間プロファイルの追加

次の手順を使用して、ゲスト ロールに新しい時間プロファイルを追加できます。

ステップ 1　管理インターフェイスから、[Guest Policy] > [Time Profiles] を選択します（図 6-11 を参照）。

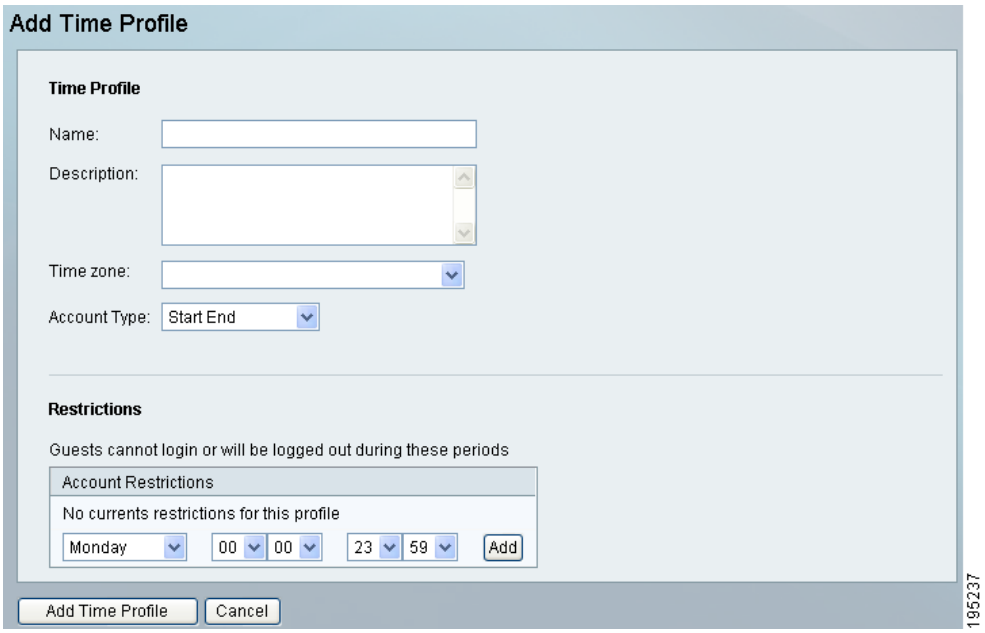
図 6-11　時間プロファイル



ステップ 2　[Add Time Profile] ボタンをクリックして新しい時間プロファイルを追加します。

ステップ 3　[Add Time Profile] ページ（図 6-12 を参照）から、新しい時間プロファイルの [Name] と [Description] を入力します。

図 6-12　[Add Time Profile] ページ



ステップ 4　[Timezone] ドロップダウン メニューから、Account Restrictions が適用されるタイムゾーンを指定します。

（注）　[Timezone] 機能は、バージョン 2.0.1 以降からのみ使用できます。バージョン 2.0.0 では、アカウントの制限は、サーバ設定の日付/時刻設定で設定されたタイムゾーンによって決まります。

ステップ 5　[Account Type] ドロップダウン メニューから、次の定義済みのオプションのいずれかを選択できます。

- [Start End]：スポンサーがアカウント有効期間の開始時間と終了時間を定義できるようにします。
- [From First Login]：スポンサーが最初のログインからのゲストのアクセス時間の長さを定義できるようにします。
- [From Creation]：スポンサーが、アカウント作成時点からのゲスト アクセスの時間長を定義できるようになります。

（注）　[From Creation] オプションは、バージョン 2.0.1 以降でのみ使用可能です。

- [Time Used]：スポンサーがゲストのログインできる期間を作成できるようにします。たとえば、アカウントを 2 時間にわたって有効にして、最初のログインから 24 時間以内の任意の時間にわたって使用できるようにすることができます。

ステップ 6　選択したアカウントの種類に応じて、次のフィールドに有効期間を入力します。

- [Start End]：スポンサーがアカウント有効期間の開始時間と終了時間を定義できるようにします。これにより、有効期間が不要になります。
- [From First Login]：スポンサーが最初のログインからのゲストのアクセス時間の長さを定義できるようにします。日単位の有効期間が必要です。
- [From Creation]：スポンサーが、アカウント作成時点からのゲスト アクセスの時間長を定義できるようになります。

（注）　[From Creation] オプションは、バージョン 2.0.1 以降でのみ使用可能です。

- [Time Used]：スポンサーがゲストのログインできる期間を作成できるようにします。たとえば、アカウントを 2 時間にわたって有効にして、最初のログインから 24 時間以内の任意の時間にわたって使用できるようにすることができます。スポンサーがゲスト アカウントを割り当てることができる長さ、およびゲスト アカウントを終了する必要がある時間の枠を指定する必要があります。
- [Save] ボタンをクリックして保存します。

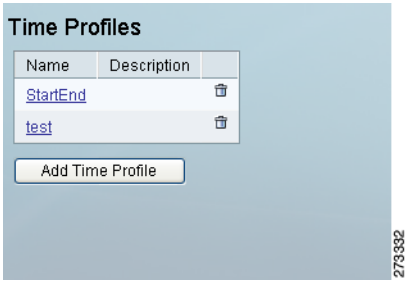
ステップ 7　時間プロファイルを作成すると、[Restrictions] セクションに Account Restrictions を実装できます。ドロップダウン メニューを使用して、ゲスト アクセスの制限を開始および終了する日付と時刻を選択します。時間の条件の設定を完了したら、[Add] をクリックして、次の制限を作成します。

時間プロファイルの編集

次の手順で、時間プロファイルを編集する方法を説明します。

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、[Guest Policy] > [Time Profiles] を選択します。

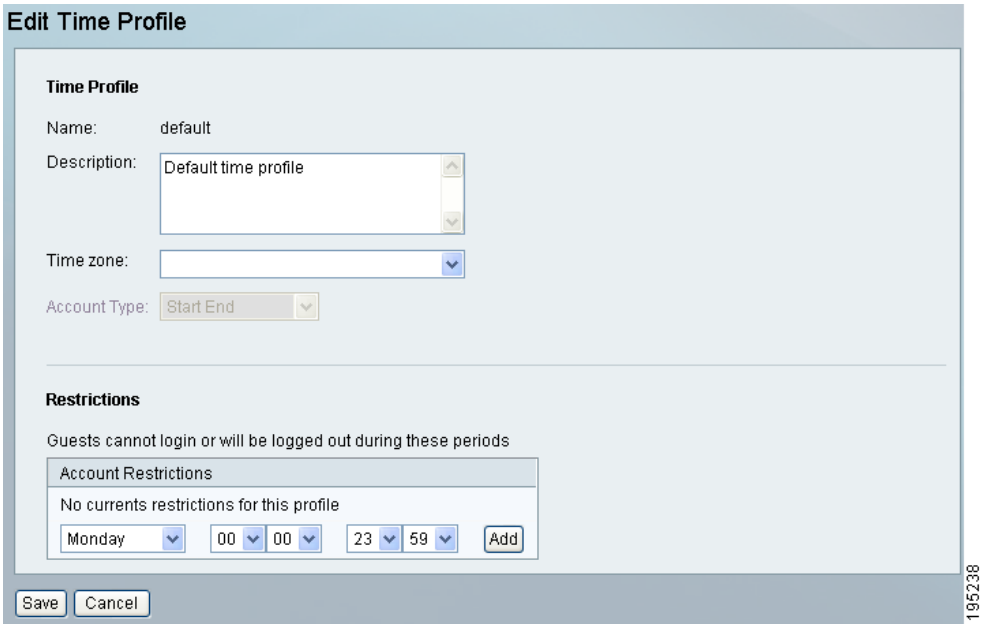
図 6-13　時間プロファイルの編集



ステップ 2　編集する時間プロファイルを選択し、そのロールの下線の付いた名前をクリックします（図 6-13 を参照）。

ステップ 3　[Edit Time Profile] ページ（図 6-14 を参照）から、そのプロファイルの [Name] と [Description] を編集できます。

図 6-14　時間プロファイルの編集



ステップ 4　[Timezone] ドロップダウン メニューから、Account Restrictions が適用されるタイムゾーンを指定します。

（注）　[Timezone] 機能は、バージョン 2.0.1 以降からのみ使用できます。バージョン 2.0.0 では、アカウントの制限は、サーバ設定の日付 / 時刻設定で設定されたタイムゾーンによって決まります。

ステップ 5　[Account Type] ドロップダウン メニューから 3 つの定義済みのオプションのいずれかを選択できます。

- [Start End]：スポンサーがアカウント有効期間の開始時間と終了時間を定義できるようにします。
- [From First Login]：スポンサーが最初のログインからのゲストのアクセス時間の長さを定義できるようにします。
- [From Creation]：スポンサーが、アカウント作成時点からのゲスト アクセスの時間長を定義できるようになります。

（注）　[From Creation] オプションは、バージョン 2.0.1 以降でのみ使用可能です。

- [Time Used]：スポンサーがゲストのログインできる期間を作成できるようにします。たとえば、アカウントを 2 時間にわたって有効にして、最初のログインから 24 時間以内の任意の時間にわたって使用できるようにすることができます。

ステップ 6　選択したアカウントの種類に応じて、次のフィールドに有効期間を入力します。

- [Start End]：スポンサーがアカウント有効期間の開始時間と終了時間を定義できるようにします。これにより、有効期間が不要になります。
- [From First Login]：スポンサーが最初のログインからのゲストのアクセス時間の長さを定義できるようにします。日単位の有効期間が必要です。
- [From Creation]：スポンサーが、アカウント作成時点からのゲスト アクセスの時間長を定義できるようになります。

（注）　[From Creation] オプションは、バージョン 2.0.1 以降でのみ使用可能です。

- [Time Used]：スポンサーがゲストのログインできる期間を作成できるようにします。たとえば、アカウントを 2 時間にわたって有効にして、最初のログインから 24 時間以内の任意の時間にわたって使用できるようにすることができます。スポンサーがゲスト アカウントを割り当てることができる長さ、およびゲスト アカウントを終了する必要がある時間の枠を指定する必要があります。
- [Save] ボタンをクリックして保存します。

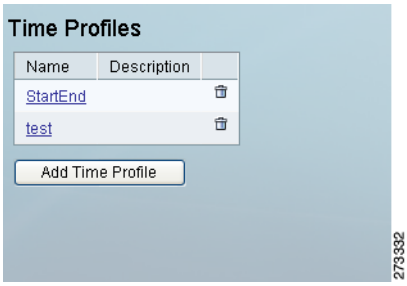
ステップ 7　時間プロファイルを作成すると、[Restrictions] セクションに Account Restrictions を実装できます。ドロップダウン メニューを使用して、ゲスト アクセスの制限を開始および終了する日付と時刻を選択します。時間の条件の設定を完了したら、[Add] をクリックして、次の制限を作成します。

時間プロファイルの削除

次の手順で、時間プロファイルを削除する方法を説明します。

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、[Guest Policy] > [Time Profiles] を選択します。

図 6-15　時間プロファイルの削除



ステップ 2　[Time Profiles] ページ（図 6-15 を参照）から削除するプロファイルを選択し、ゴミ箱アイコンをクリックします。

ステップ 3　プロンプトに従って削除を確認します。

（注）　ゲスト アカウントの作成に一度も使用されていない時間プロファイルだけを削除できます。使用された時間プロファイルは、監査目的で必要になるため削除できません。

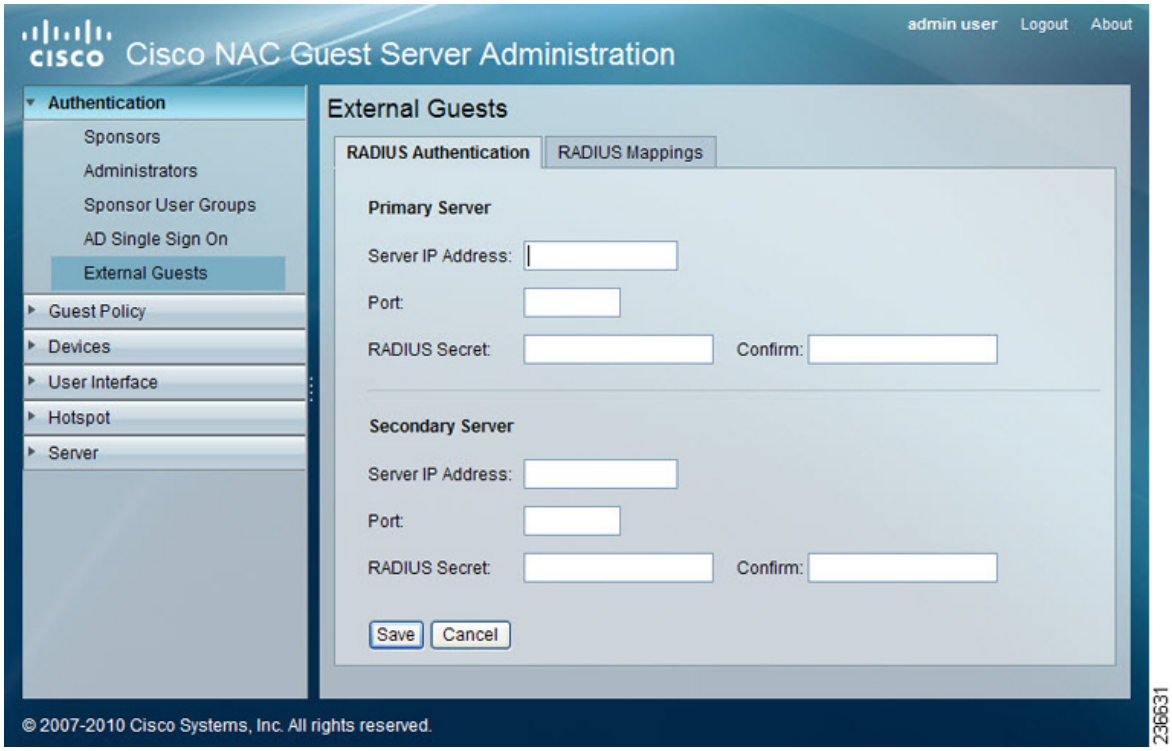
外部ゲスト認証

RADIUS 認証では、既存の RADIUS ユーザ アカウントを使用し、Cisco NAC ゲスト サーバに対してゲスト ユーザを認証します。ゲストは、ゲスト サーバを認証するために、別のユーザ名とパスワードのセットを覚えておく必要がなくなります。また、ローカル ゲスト アカウントの作成にスポンサーの関与が必要ないため、RADIUS 認証により、ゲストは、すばやくロールアウトして独自のゲスト アクセスを作成することもできます。

ステップ 1　管理インターフェイスから、[Authentication] > [External Guests] を選択します。

ステップ 2　[RADIUS Authentication] タブをクリックします（図 6-16 を参照）。

図 6-16　RADIUS 認証



ステップ 3　プライマリ RADIUS サーバの [Server IP Address] を入力します。

ステップ 4　そのサーバで RADIUS 認証を実行する [Port] を入力します（デフォルトは 1645 または 1812 です）。

ステップ 5　[RADIUS Secret] フィールドに、RADIUS サーバと NAC ゲスト サーバの間で使用される共有秘密を入力します。

ステップ 6　秘密が正しく設定されていることを確認します。

ステップ 7　セカンダリ RADIUS サーバの詳細を入力します。これらの詳細は、NAC ゲスト サーバがプライマリ RADIUS サーバから応答を受信しなかった場合に使用されます。これらのフィールドは任意です。

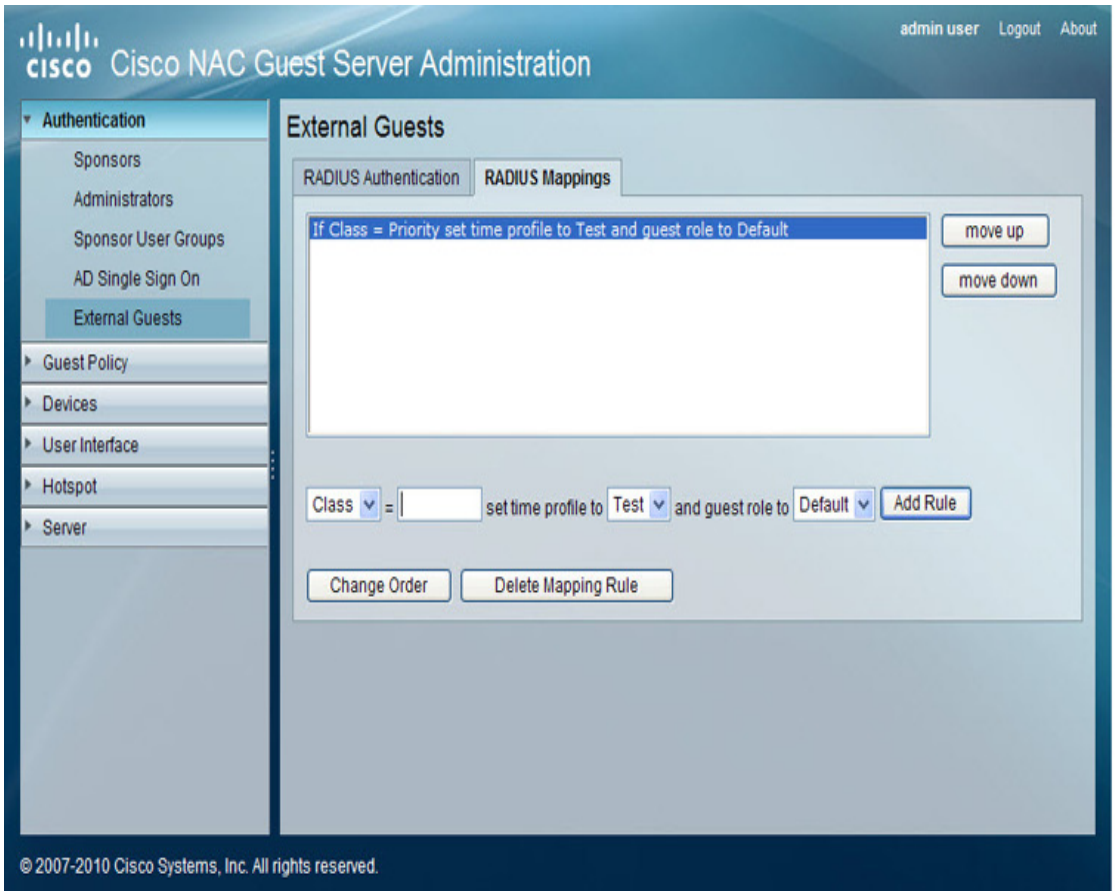
ステップ 8　[Save] をクリックして、管理者の RADIUS の設定を保存します。

ここで、必要な RADIUS マッピングを入力できます。

ステップ 1　管理インターフェイスから、[Authentication] > [External Guests] を選択します。

ステップ 2　[RADIUS Mappings] タブをクリックします（図 6-17 を参照）。

図 6-17　RADIUS マッピング



ステップ 3　空のフィールド、および事前定義されたテキストがあるドロップ ダウン メニューを使用して、RADIUS マッピングを入力できます。ドロップ ダウン メニュー内のテキストは、NAC ゲスト サーバの管理者によって事前に作成されている時間プロファイルおよびゲスト ロールに関連しています。

（注）　外部ゲスト認証は、[From First Login] 時間プロファイルだけをサポートしています。

ステップ 4　ルールが作成されたら、[Add Rule] ボタンをクリックして適用します。

ステップ 5　ルールの順序は、ルールを選択および強調表示し、[move up] ボタンおよび [move down] ボタンをクリックして変更できます。[Change Order] ボタンをクリックして変更を適用します。