



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。

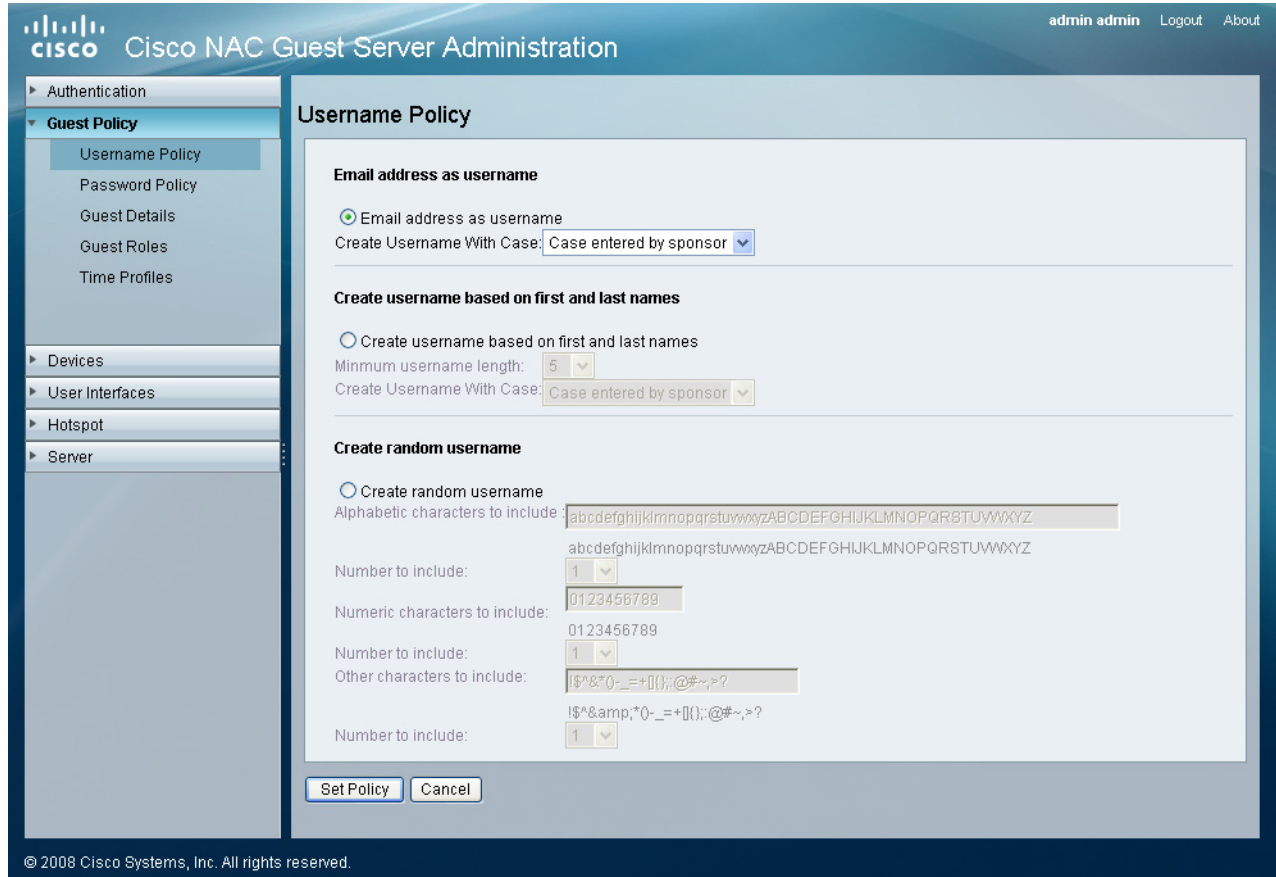
- [ユーザ名ポリシーの設定](#)
- [パスワードポリシーの設定](#)
- [ゲスト詳細ポリシーの設定](#)
- [ゲストロールの設定](#)
- [時間プロファイルの設定](#)

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の左側のメニューから、[Guest Policy] > [Username Policy] を選択します (図 6-1)。

図 6-1 ゲスト ユーザーポリシー



ステップ 2 ゲストアカウントのユーザー名の作成に関して、次の3つのユーザーポリシーのオプションのいずれかを選択します。

a. ユーザーポリシー 1 : Email address as username

ゲストの電子メールアドレスをユーザー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、ユーザー名を一意にします。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ー名の太文字小文字の表記を決定できます。

- Case entered by sponsor : ユーザー名の太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 : ユーザー名が、スポンサーによって設定された後に、強制的に太文字にされます。
- lowercase : ユーザー名が、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. ユーザーポリシー 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、ユーザー名を作成します。このユーザー名の [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ー名は、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きい文字小文字の表記を決定できます。

- Case entered by sponsor : ユーザ名の大きい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、強制的に大きい文字にされます。
- 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を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の左側のメニューから [Guest Policy] > [Password Policy] を選択します (図 6-2)。

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数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 により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の左側のメニューから、[Guest Policy] > [Guest Details] を選択します (図 6-3)。

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が、スポンサーはフィールドに入力し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るようになります（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）。

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よう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の左側のメニューから、[Guest Policy] > [Guest Roles] を選択します (図 6-4)。

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) 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](#)

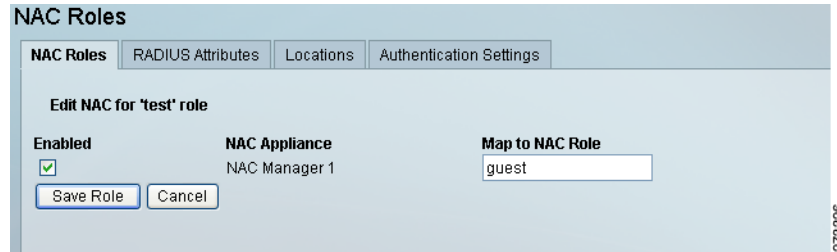
NAC ロールの編集

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 のどのロール名が使用されるかを指定できます。

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)。

図 6-8 RADIUS 属性

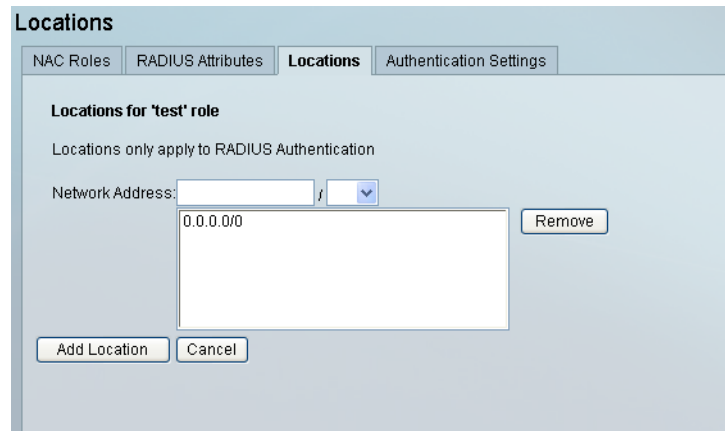
- ステップ 3** 各 [Attribute] と [Value] の組み合わせを入力し、[Add] ボタンをクリックします。
- ステップ 4** 送信される属性を並べ替える必要がある場合は、[Move up] ボタンと [Move down] ボタンを使用します。
- ステップ 5** RADIUS 属性を保存する場合は、[Save Role] ボタンをクリックします。

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** ページの上部から [Locations] を選択します (図 6-9)。

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 ページの上部から [Authentication Settings] を選択します (図 6-10)。

図 6-10 認証の設定

Authentications settings

Guest Roles | RADIUS Attributes | Locations | **Authentication Settings**

Authentications settings for 'Default' role

Maximum Concurrent Connections:
Leave blank for unlimited

Maximum Failed Authentications:
Leave blank for unlimited

Allow Password Change:

Require Password Change:

- ステップ 3** このロールのゲストが、表示されたフィールドで作成できる [Maximum Concurrent Connections] の数と [Maximum Failed Authentications] の数を入力します。数を制限しない場合は、フィールドを空のままにしておきます。
- ステップ 4** ゲストがパスワードを変更できるようにする場合は、[Allow Password Change] チェックボックスをオンにします。
- ステップ 5** ゲストに強制的にパスワードを変更させる場合は、[Require Password Change] チェックボックスをオンにします。
- ステップ 6** [Save] ボタンをクリックして変更を保存します。

時間プロフィールの設定

時間プロフィールでは、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ィールを割り当てることができます。

時間プロフィールを作成したら、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ィー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ィー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、「[時間プロフィールの割り当て](#)」(P.5-14)を参照してください。



(注)

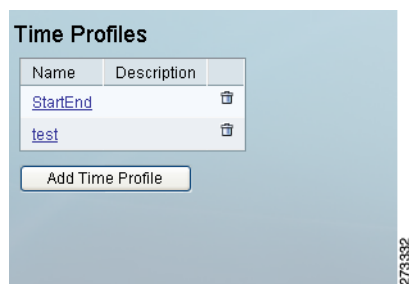
Cisco NAC ゲスト サーバ Version 2.0 は、Cisco NAC アプライアンスと共に使用される場合に開始/終了プロフィールだけをサポートします。

時間プロフィールの追加

次の手順で、ゲスト ロールに新しい時間プロフィールを追加できます。

- 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 6-11)。

図 6-11 時間プロフィール



- 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ィールを追加します。
- ステップ 3** [Add Time Profile] ページ (図 6-12) から、新しい時間プロフィールの [Name] と [Description] を入力します。

図 6-12 [Add Time Profile] ページ

ステップ 4 [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。
- **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 5 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。
- **Time Used** : スポンサーがゲストのログインできる有効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。

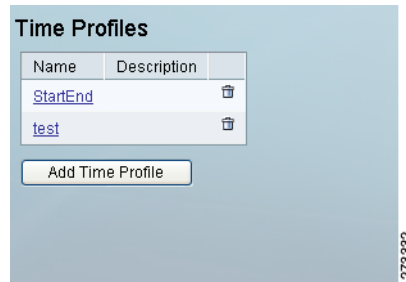
ステップ 6 時間プロファイルを作成すると、[Restrictions] セクションに **Account Restrictions** を実装できます。ドロップダウンメニューを使用して、ゲストアクセスの制限を開始および終了する日付と時刻を選択します。時間の条件の設定を完了したら、[Add] をクリックして、次の制限を作成します。

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。

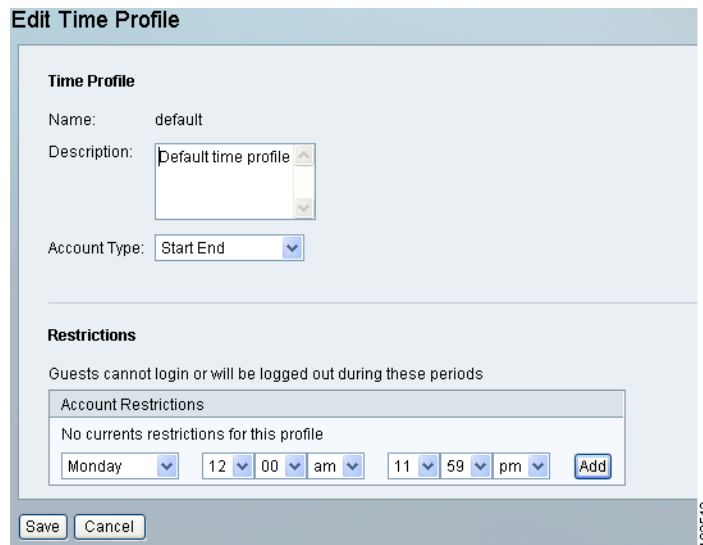
図 6-13 時間プロファイルの編集



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)。

ステップ 3 [Edit Time Profile] ページ (図 6-14) 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 [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。
- **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 5 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。

- **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。

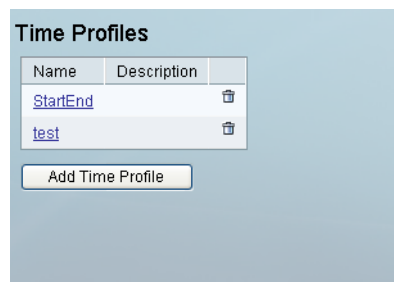
ステップ 6 時間プロファイルを作成すると、[Restrictions] セクションに **Account Restrictions** を実装できます。ドロップダウンメニューを使用して、ゲストアクセスの制限を開始および終了する日付と時刻を選択します。時間の条件の設定を完了したら、[Add] をクリックして、次の制限を作成します。

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) 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 クリックして削除を確認します。