CHAPTER 7

Cisco NAC アプライアンスとの統合

この章では、次の内容について説明します。

通常のゲスト ユーザは、Web ブラウザを使用して認証の詳細を提供するキャプティブ ポータルを経由してネットワークへの認証を受けます。Cisco NAC アプライアンスにより、管理者はカスタマイズ可能なセキュアなゲスト ユーザ アクセス ポータルを提供できます。

Cisco NAC ゲスト サーバは、NAC アプライアンス API を使用して Clean Access Manager と統合されます。これは、ゲスト サーバが Cisco NAC アプライアンス マネージャ（別名 Clean Access Manager; CAM）と通信するために必要とする HTTPS ベースの API です。

Cisco NAC ゲスト サーバは、ゲスト ユーザに定義する特別なロールに割り当てられたローカル ユーザ アカウントとして、CAM でゲスト ユーザ アカウントを作成します。ゲスト サーバは、有効な新規アカウントを毎分作成し、期限切れになったアカウントを毎分削除します。アカウントが一時停止した場合、ゲスト サーバは、CAM のアカウントと、ログインしているネットワーク上のゲスト ユーザのアカウントの両方を削除します（ゲスト ユーザがログインしている場合）。

CAM は、RADIUS アカウンティング経由で Cisco NAC ゲスト サーバにアカウンティング情報を送信することもできます。この情報は、アクセス時間および IP アドレス別のゲストのレポートおよびトラッキングに使用されます。

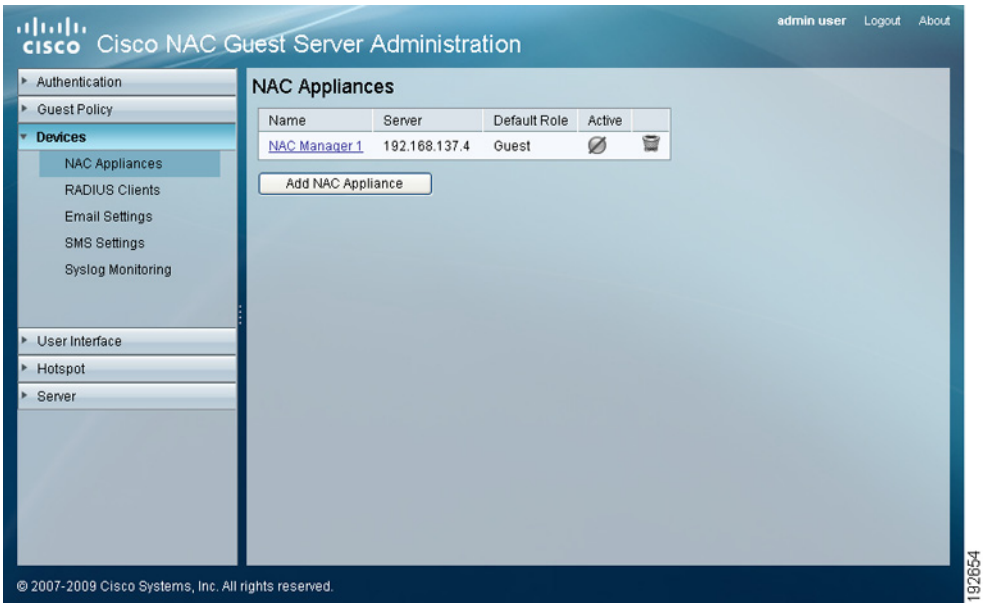
Cisco NAC ゲスト サーバには、複数の CAM を追加できます。アカウントをプロビジョニングすると、定義されているすべてのアクティブな CAM にアカウントが作成されます。

CAM エントリの追加

次の手順では、Cisco NAC ゲスト サーバと Cisco NAC アプライアンス マネージャが相互に通信できるように設定する方法について説明します。Cisco NAC ゲスト サーバがアカウントを作成する CAM ごとに、ゲスト サーバに API 情報を追加する必要があります。

ステップ 1　ゲスト サーバ管理インターフェイスの左側のメニューから、[Devices] > [NAC Appliances] を選択します（図 7-1 を参照）。

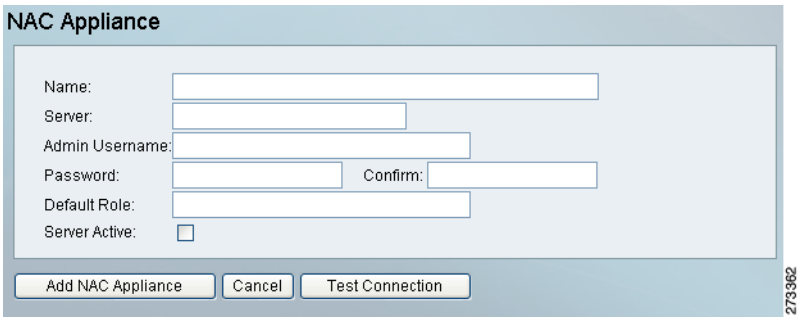
図 7-1　Cisco NAC アプライアンス



ステップ 2　[Add NAC Appliance] ボタンをクリックします。

ステップ 3　[NAC Appliance Details] ページで、次の設定を入力します（図 7-2 を参照）。

図 7-2　CAM の追加



- [Name]：CAM を説明する名前を入力します。
- [Server]：CAM の DNS 名または IP アドレスを入力します。
- [Admin Username]：CAM に対する Full-Control API 権限を持つ admin ユーザ名を入力します。
- [Password]：アカウントのパスワードを入力します。
- [Confirm Password]：パスワードを再度入力し、パスワードが一致していることを確認します。
- [Default Role]：ゲスト ユーザに割り当てる CAM での User ロールの名称を入力します。これは、CAM に設定された User ロール名と大文字、小文字を含めて正確に一致している必要があります。
- [Server Active]：Cisco NAC ゲスト サーバが CAM にアカウントをプロビジョニングするようにゲスト サーバをアクティブ ステータスに設定するには、このチェックボックスをオンにします。このフィールドをオフのままにすると、ゲスト サーバのプロビジョニングがディセーブルになります。

ステップ 4　[Add NAC Appliance] ボタンをクリックします。

ステップ 5　[Test Connection] ボタンをクリックし、これらの設定が正しく機能していることを確認します。

ステップ 6　CAM 管理コンソールで [Monitoring] > [Event Logs] に移動し、アカウント nacguest_test が正常に作成され、削除されたことを確認します。

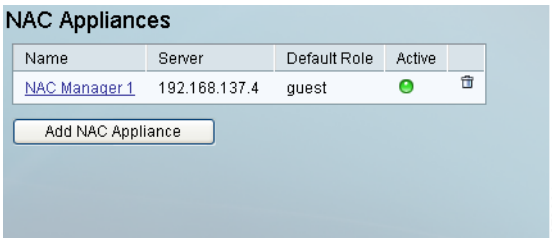
（注）　CAM は、自動的に **Default** ゲスト ロールに追加され、ここで指定したロール名を使用してプロビジョニングするように設定されます。このロールに CAM を追加しない場合は、エントリを手動で削除する必要があります。

CAM エントリの編集

次の手順では、CAM の既存のエントリを編集する方法について説明します。

ステップ 1　ゲスト サーバ管理インターフェイスの左側のメニューから、[Devices] > [NAC Appliances] を選択します（図 7-3 を参照）。

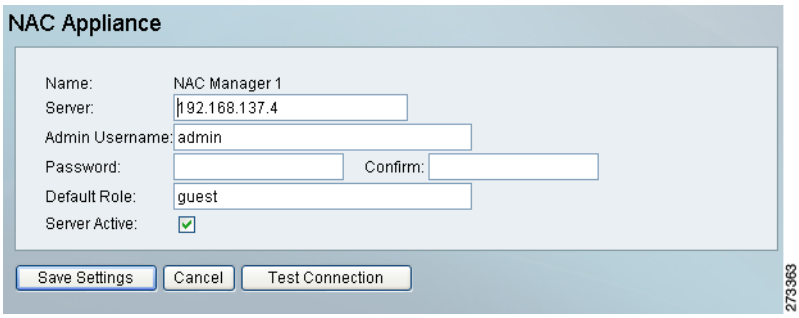
図 7-3　Cisco NAC アプライアンスのリスト



ステップ 2　リストの下線付き NAC アプライアンス名をクリックして編集します。

ステップ 3　[NAC Appliance Settings] ページで、次の設定を入力します（図 7-4 を参照）。

図 7-4　CAM の編集



- [Server] : CAM の DNS 名または IP アドレスを入力します。
- [Admin Username] : CAM に対する API 権限を持つ admin ユーザ名を入力します。
- [Password] : アカウントのパスワードを入力します。
- [Confirm Password] : パスワードを再度入力し、パスワードが一致していることを確認します。
- [Default Role] : ゲスト ユーザに割り当てる CAM での User ロールの名称を入力します。これは、CAM に設定された User ロール名と大文字、小文字を含めて正確に一致している必要があります。
- [Server Active] : Cisco NAC ゲスト サーバが CAM にアカウントをプロビジョニングするようにゲスト サーバをアクティブ ステータスに設定するには、このチェックボックスをオンにします。このフィールドをオフのままにすると、ゲスト サーバのプロビジョニングがディセーブルになります。

ステップ 4　[Save Settings] ボタンをクリックします。

ステップ 5　[Test Connection] ボタンをクリックし、これらの設定が正しく機能していることを確認します。

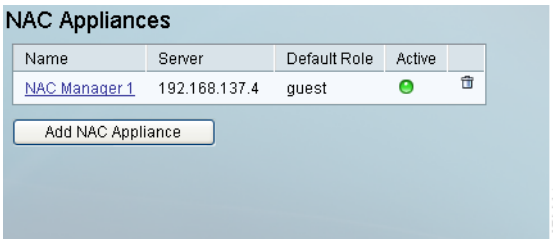
ステップ 6　CAM 管理コンソールで [Monitoring] > [Event Logs] に移動し、アカウント nacguest_test が正常に作成され、削除されたことを確認します。

CAM エントリの削除

次の手順では、NAC アプライアンス（CAM）のエントリを削除する方法について説明します。

ステップ 1　ゲスト サーバ管理インターフェイスの左側のメニューから、[Devices] > [NAC Appliances] を選択します（図 7-5 を参照）。

図 7-5　Cisco NAC アプライアンスのリスト



ステップ 2　リストから削除する Cisco NAC アプライアンスを選択し、アクティブなフィールドの右側にあるゴミ箱アイコンをクリックします。プロンプトに従って削除を確認します。

ステップ 3　NAC ゲスト サーバ データベースから、NAC アプライアンスで作成されたアカウントのレコードを削除するかどうかを確認するメッセージが表示されます。NAC アプライアンスを後で追加する場合は、プロビジョニング レコードが必要になる場合があります。

警告　**NAC アプライアンスを削除する場合は、CAM で作成されるゲスト アカウントを手動で管理する必要があります。**

レポートのための CAM の設定

レポートが実行されているときに Cisco NAC ゲスト サーバがゲスト ユーザの詳細を正しく表示するには、CAM がゲスト サーバに RADIUS アカウンティング情報を送信するように設定する必要があります。さらに、CAM はその情報を正しくフォーマットする必要があります。

（注）　CAM にアクセスして CAM で設定を行う方法の詳細については、該当する『*Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide*』を参照してください。

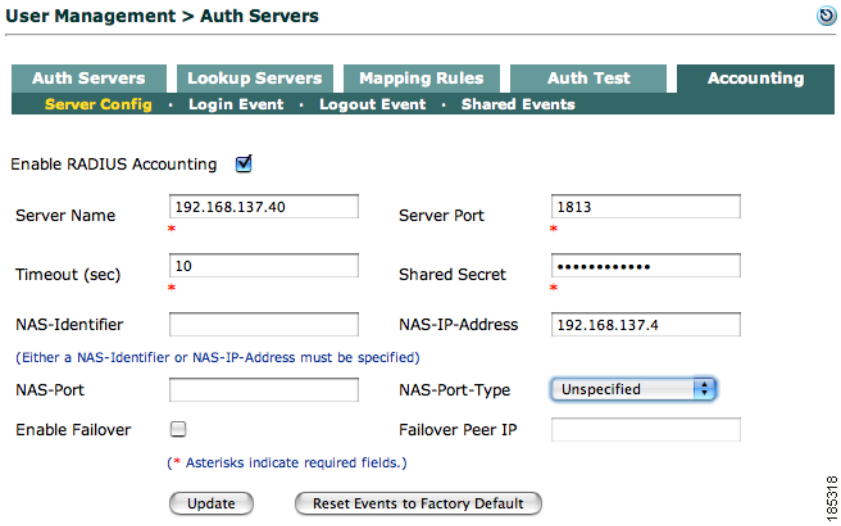
RADIUS アカウンティング サーバの追加

ステップ 1　適切なパスワードをもつ admin ユーザとして、CAM Web コンソールにログインします（デフォルトのユーザ名 / パスワードは **admin**/**cisco123**）。

（注）　編集権限をもつすべての CAM admin ユーザがこの設定を行うことができます。

ステップ 2　[User Management] > [Auth Servers] > [Accounting] > [Server Config] に移動します。

図 7-6　RADIUS アカウンティング サーバの設定



ステップ 3　[Enable RADIUS Accounting] のチェックボックスをクリックし、次のフィールドを設定します。

- [Server Name] : Cisco NAC ゲスト サーバの IP アドレスを入力します。
- [Server Port] : ポートとして 1813 を入力します。
- [Timeout (sec)] : タイムアウトの値を入力します。一般的には 10 秒が適切です。
- [Shared Secret] : Cisco NAC ゲスト サーバで使用する共有秘密を入力します。これは、「RADIUS クライアントの追加」（P.8-2）で説明されているように、CAM を RADIUS クライアントとしてゲスト サーバに追加するときにゲスト サーバで設定した共有秘密に一致している必要があります。両方の共有秘密が同一であることを確認します。
- [NAS-IP-Address] : CAM 自身のアドレスを NAS-IP-Address として入力します。

ステップ 4　[Update] ボタンをクリックします。

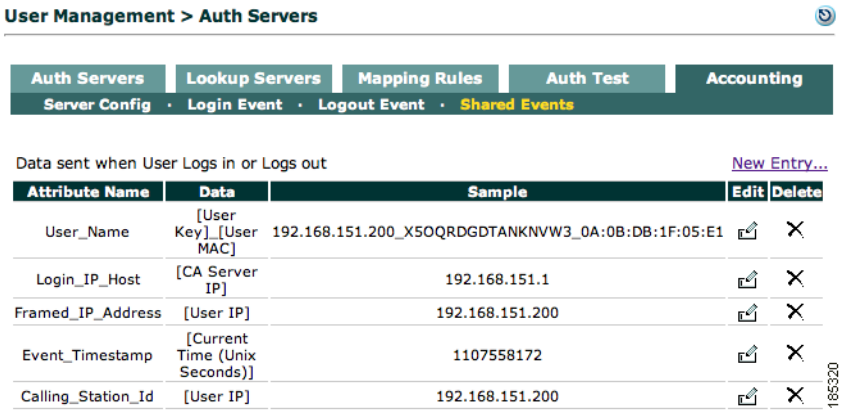
RADIUS アカウンティング データをフォーマットするための CAM の設定

CAM は、多くの異なる属性を RADIUS アカウンティング パケットに付加するように設定することにより、属性自体をさまざまな方法でフォーマットすることができます。Cisco NAC ゲスト サーバが認識できるような特定のフォーマットで属性情報を送信するように、CAM を設定する必要があります。

（注）　詳細については、該当する『*Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide*』の「RADIUS Accounting」の項を参照してください。

ステップ 1　CAM 管理コンソールにログインし、[User Management] > [Auth Servers] > [Accounting] > [Shared Events] に移動します（図 7-7 を参照）。

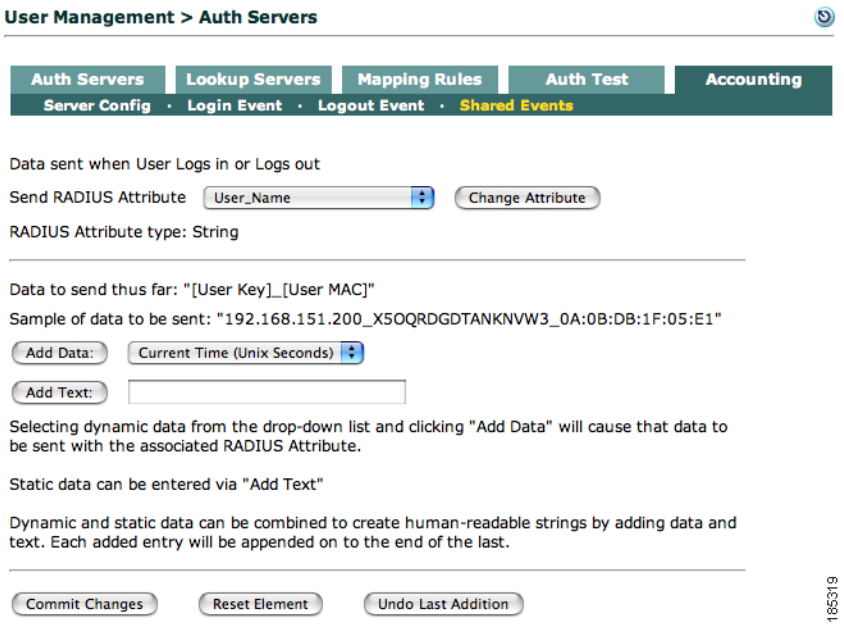
図 7-7　共有イベント



ステップ 2　[Shared Events] ページで、User_Name 属性エントリの右側にある [Edit] ボタンをクリックします。

ステップ 3　[Edit User_Name Attribute] ページ（図 7-8 を参照）で、[Reset Element] ボタンをクリックし、既存のサンプル データ フォーマットを削除します。

図 7-8　ユーザ名属性の編集



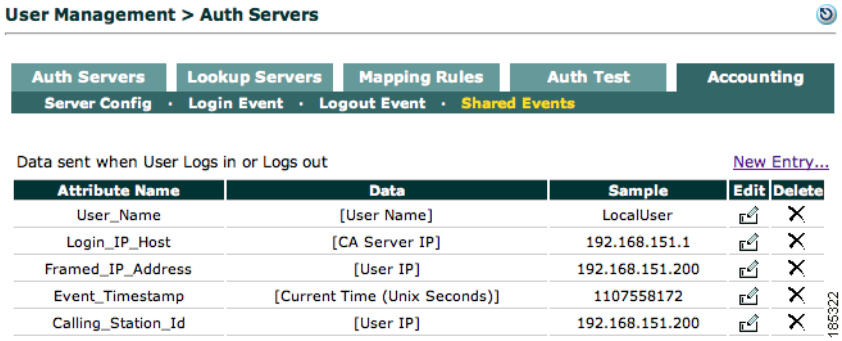
ステップ 4　[Add Data] ドロップダウン メニューから [User Name] を選択します。

ステップ 5　[Add Data] ボタンをクリックします。

ステップ 6　[Commit Changes] ボタンをクリックします。

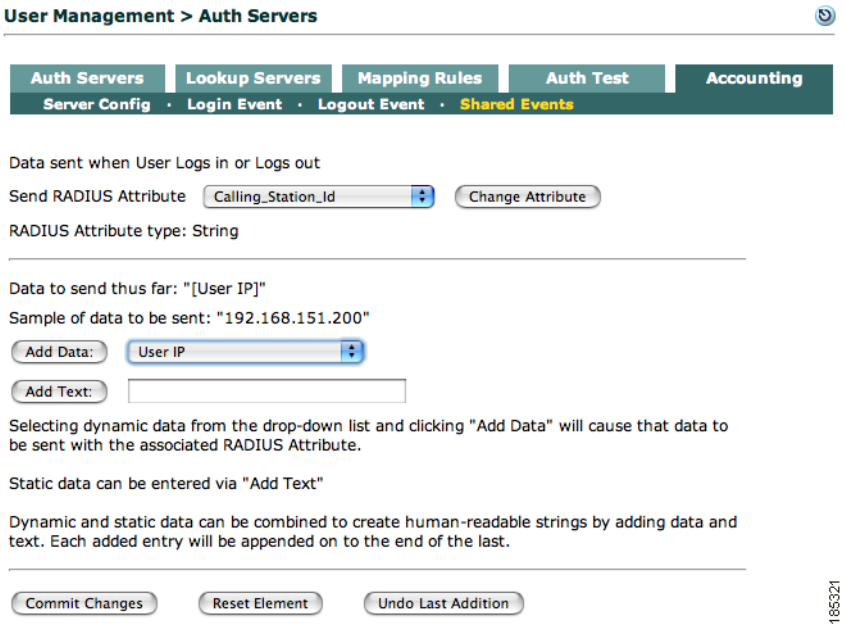
ステップ 7　メインの [Shared Events] リストのページが再び表示されます（図 7-9 を参照）。[Data] カラムに [User_Name] がリスト表示されていることを確認します。

図 7-9　ユーザ名が変更された共有イベント



ステップ 8　ページの右側にある [New Entry...] リンクをクリックし、属性を追加します（図 7-9 を参照）。

図 7-10　Calling Station Id 属性の追加



ステップ 9　New Shared Events 属性フォーム（図 7-10 を参照）で、[Send RADIUS Attributes] ドロップダウン メニューから [Calling_Station_Id] を選択します。

ステップ 10　[Change Attribute] ボタンをクリックします。

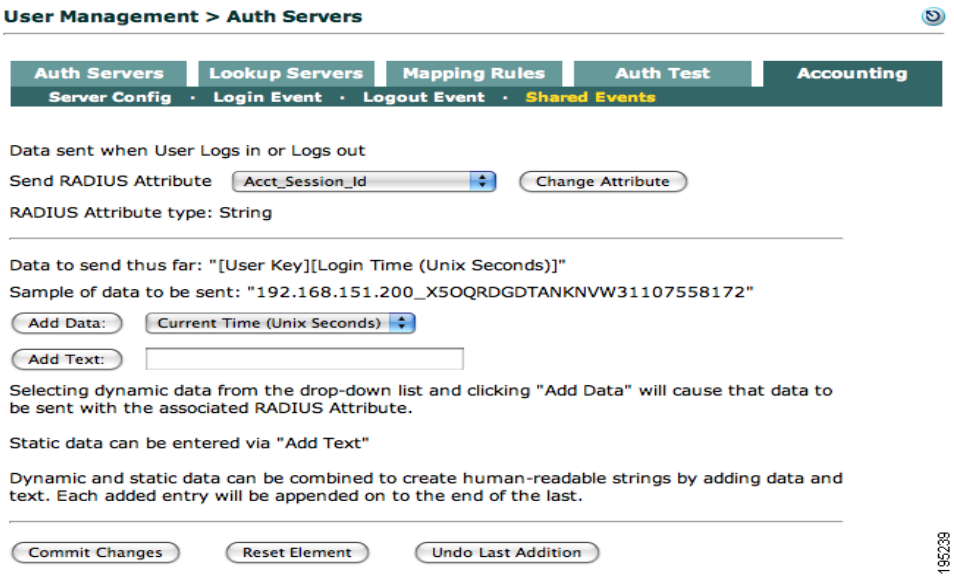
ステップ 11　[Add Data] ドロップダウン メニューから [User IP] を選択します。

ステップ 12　[Add Data] ボタンをクリックします。

ステップ 13　[Commit Changes] をクリックします。

ステップ 14　ページの右側にある [New Entry] リンクをクリックし（図 7-9 を参照）、属性を追加します（図 7-11 を参照）。

図 7-11　追加属性



ステップ 15　New Shared Events 属性フォーム（図 7-11 を参照）で、[Send RADIUS Attributes] ドロップダウン メニューから [Acct_Session_Id] を選択します。

ステップ 16　[Change Attribute] ボタンをクリックします。

ステップ 17　[Add Data] ドロップダウン メニューから [User Key] を選択します。

ステップ 18　[Add Data] ボタンをクリックします。

ステップ 19　[Add Data] ドロップダウン メニューから [Login Time] を選択します。

ステップ 20　[Add Data] ボタンをクリックします。

ステップ 21　[Commit Changes] をクリックします。

（注）　第 8 章「RADIUS クライアントの設定」の手順に従って、CAM を RADIUS クライアントとして追加します。