CHAPTER 3

システムのセットアップ

Cisco NAC ゲスト サーバは、すべて HTTP または HTTPS による Web インターフェイスによって管理されます。初期インストール後、時間や SSL 証明書の設定など、アプライアンスおよび他のシステムに不可欠な設定を行う際、Web インターフェイスを利用したシステムのネットワーキング設定が利用できます。

この章の内容は、次のとおりです。

製品ライセンスのインストールと管理インターフェイスへのアクセス

Cisco NAC ゲスト サーバの Web 管理インターフェイスにアクセスする前に、製品ライセンスをインストールする必要があります。ライセンスは、アプライアンスに添付されている PAK の指示に従うか、https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet?FormId=146 で評価ライセンスの登録を行うことで取得できます。

（注） 評価ライセンスの詳細については、『*Cisco NAC Appliance Service Contract / Licensing Support*』を参照してください。

ここでは、次の内容について説明します。

Cisco NAC ゲスト サーバ ライセンスの取得とインストール

次の手順を使用して、Cisco NAC ゲスト サーバの FlexLM 製品ライセンス ファイルを取得してインストールできます。

ステップ 1　FlexLM のライセンスにより、購入する各ゲスト サーバの Product Authorization Key（PAK; プロダクト認証キー）を受信します。PAK は、パッケージに添付されている Software License Claim Certificate カードに粘着ラベルとして貼られています。

警告　**PAK は、Cisco NAC ゲスト サーバのライセンスではありません。PAK は、以下に説明されているように、Cisco NAC ゲスト サーバのライセンスを取得するために使用されます。**

ステップ 2　登録済み CCO ユーザとしてログインし、PAK Cisco Technical Support サイト（http://www.cisco.com/go/license）にあるカスタマー登録フォームに記入します。カスタマー登録時には、受信する各 PAK と Cisco NAC ゲスト サーバの eth0 MAC アドレスを送信します。

（注）　わかりやすいように、Cisco NAC ゲスト サーバ ライセンス フォーム（図 3-1 を参照）の上部には、ゲスト サーバ アプライアンスの MAC アドレスが表示されます。

警告　**カスタマー登録フォームに入力するゲスト サーバの eth0 の MAC アドレスは大文字でなければなりません（たとえば、16 進数の文字は大文字にする必要があります）。文字の間にコロン（「:」）を入力しないでください。**

ライセンス Web ページの指示に従って、正しい MAC アドレスを入力してください。

ステップ 3　**送信した PAK ごとにライセンス ファイルが生成されて、電子メールで送信されます。**

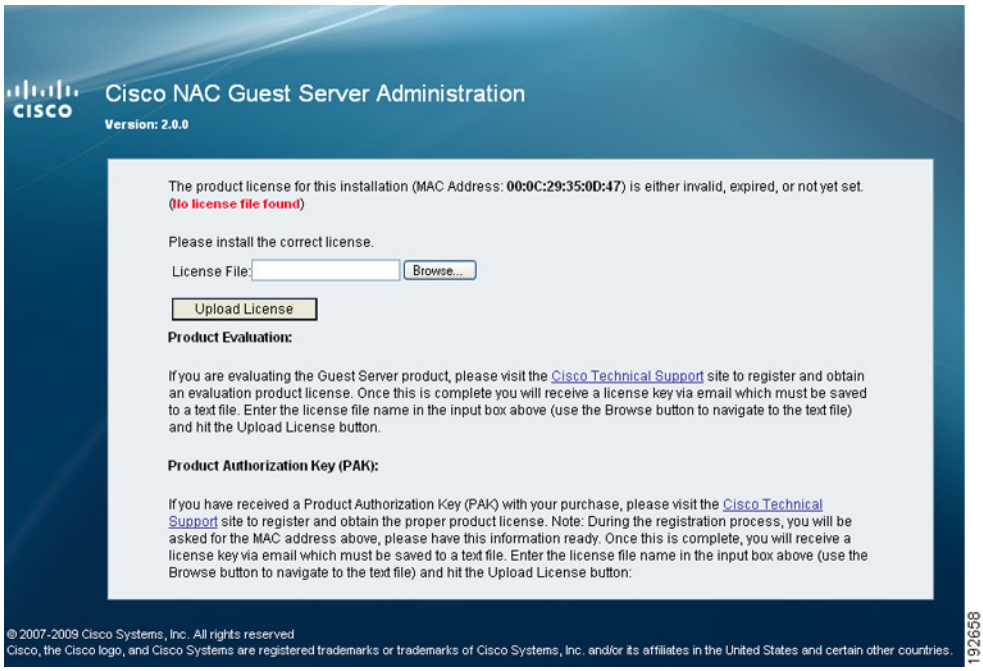
ステップ 4　受信した各ライセンス ファイルをディスクに保存します。

ステップ 5　コマンドラインにより設定した IP アドレスを URL（/admin を末尾に付加）として入力し、Cisco NAC ゲスト サーバ管理インターフェイスへの Web ブラウザを開きます。

- HTTP アクセスの場合は、**http://<guest_server_ip_address>/admin** を開きます。
- HTTPS アクセスの場合は、**https://<guest_server_ip_address>/admin** を開きます。

ステップ 6　Cisco NAC ゲスト サーバ ライセンス フォーム（図 3-1 を参照）で、[Browse] ボタンをクリックし、ライセンス ファイルを見つけます。

図 3-1　Cisco NAC ゲスト サーバ ライセンス フォーム（例）



ステップ 7　[Upload License] をクリックし、ライセンスをインストールします。

Cisco NAC ゲスト サーバ管理インターフェイスへのアクセス

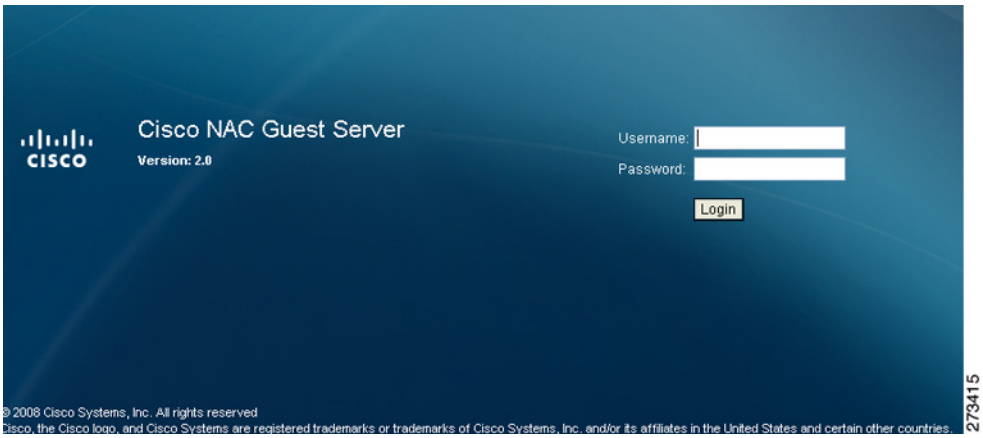
ステップ 1　ライセンスをインストールすると、admin のログインが自動的に表示されます。表示されない場合は、コマンドラインにより設定した IP アドレスを URL（/admin を末尾に付加）として入力することで、Cisco NAC ゲスト サーバ管理インターフェイスへの Web ブラウザを開きます。

- HTTP アクセスの場合は、**http://<guest_server_ip_address>/admin** を開きます。
- HTTPS アクセスの場合は、**https://<guest_server_ip_address>/admin** を開きます。

ステップ 2　Cisco NAC ゲスト サーバ管理インターフェイスが表示されます（図 3-2 を参照）。これは、アプライアンスの管理者インターフェイスです。

ステップ 3　admin ユーザとしてログインします。管理コンソールのデフォルトのユーザ名 / パスワードは、**admin**/**admin** です。

図 3-2　管理ログイン



（注）　セキュリティのために、SSL アクセスを設定し、デフォルトの admin ユーザ パスワードを変更することを推奨します。詳細については、「SSL 証明書の設定」（P.3-9）および「既存の admin アカウントの編集」（P.3-17）を参照してください。

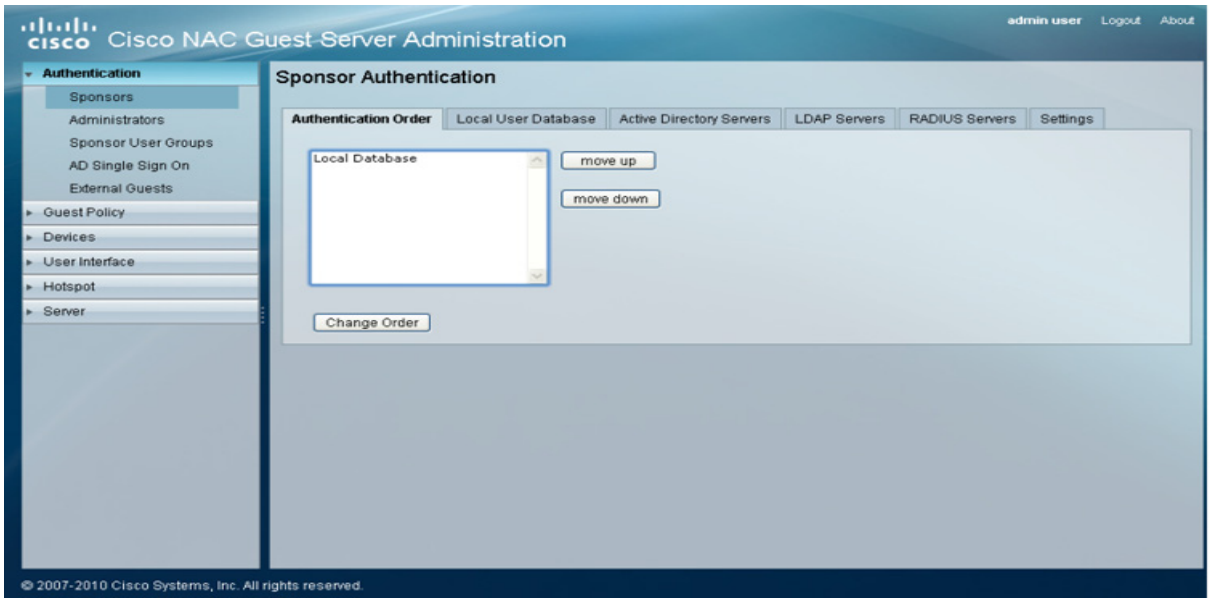
（注）　URL に「/admin」を付けずにゲスト サーバの IP アドレスを入力すると、スポンサーのインターフェイスが表示されます。詳細については、第 4 章「スポンサー認証の設定」を参照してください。

ネットワーク設定の構成

他の操作を実行する前に、残されたネットワーク設定を行います。これにより、あとでアプライアンスを再起動する必要性が減ります。

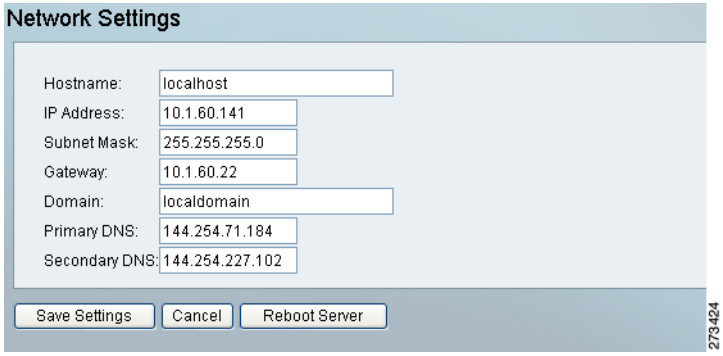
ステップ 1　管理インターフェイスにログインすると、ホームページには [Authentication] > [Sponsors] > [Authentication Order] ページ（図 3-3 を参照）がデフォルトで表示されます。

図 3-3　管理ホームページ



ステップ 2　管理ホームページの左側のパネルから [Server] >[Network Settings] を選択し、[Network Settings] ページに移動します。このページには、Cisco NAC ゲスト サーバ アプライアンスで変更できるすべてのネットワーク設定が表示されます（図 3-4 を参照）。

図 3-4　ネットワーク設定



次のネットワーク設定を変更できます。

- [Hostname]：DNS で定義されたアプライアンスの名前を割り当てます（DNS サフィックスなし）。
- [IP Address]：アプライアンスの eth0 インターフェイスの IP アドレスを変更します。
- [Subnet Mask]：対応するサブネット マスクを入力します。
- [Gateway]：アプライアンスが接続されているネットワークのデフォルト ゲートウェイを変更します。
- [Domain]：組織のドメイン名を入力します（cisco.com など）。
- [Primary DNS]：プライマリ DNS サーバの IP アドレスを入力します。
- [Secondary DNS]：セカンダリ DNS サーバの IP アドレスを入力します。

ステップ 3　[Save Settings] ボタンをクリックして、行った変更を保存します。

ステップ 4　変更を保存したら、ゲスト サーバを再起動し、すべてのプロセスで正しい IP アドレスが使用されることを確認します。[Reboot Server] ボタンをクリックすると、再起動プロセスが 60 秒以内にゲスト サーバで開始されます。

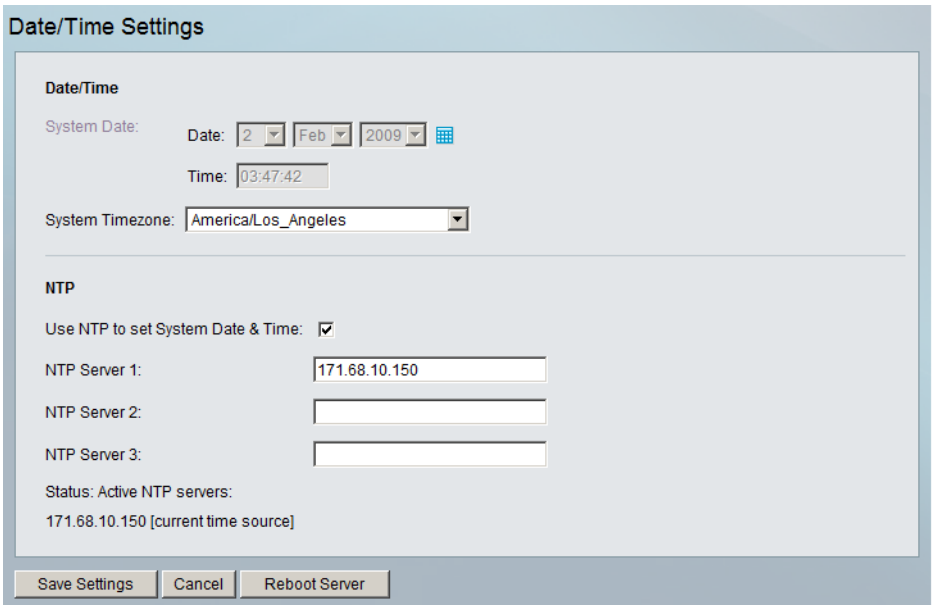
（注）　[Server] の設定を変更する場合は再起動が必要です。一度に複数の [Server] の設定を変更および保存してから再起動することができますが、その変更を適用するには、[Reboot Server] をクリックする必要があります。

日付と時刻の設定

Cisco NAC ゲスト サーバでは、正しい日付と時刻がきわめて重要です。ゲスト サーバは、アカウントが有効な期間に基づいてゲスト ユーザを認証します。ゲスト アカウントが正しい時刻に作成、削除されるためには、設定された時刻が正確である必要があります。可能であれば、ネットワーク タイム プロトコル（NTP）サーバを使用して、時刻と日付を同期することを推奨します。

ステップ 1　管理インターフェイスから、[Server] > [Date/Time Settings] を選択し、[Date/Time Settings] ページ（図 3-5 を参照）を表示します。

図 3-5　日付 / 時刻設定



ステップ 2　ゲスト サーバがある場所の正しい [System Date] と [System Time] を選択します。

ステップ 3　ゲスト サーバがある場所の正しい [System Timezone] を選択します。

ステップ 4　[Save Settings] ボタンをクリックして、システムのタイムゾーンを適用します。

（注）　システムのタイムゾーンを変更すると、サーバの日付と時刻が自動的に調整されます。

ステップ 5　ネットワーク上に使用可能な 1 台、2 台または 3 台の NTP サーバがある場合は、[Use NTP to set System Date & Time] チェックボックスをクリックします。

ステップ 6　表示されたフィールドに、使用可能な NTP サーバの IP アドレスを入力します。

ステップ 7　[Save Settings] ボタンをクリックして、変更を適用します。

（注）　NTP サーバを設定する場合、同期に時間がかかることがあります。NTP サーバの設定を保存する前に、NTP サーバに近い時刻を設定し、[Save Settings] ボタンをクリックして保存しておくと、同期が高速になります。

ステップ 8　新しい設定が有効になるように、[Reboot Server] ボタンをクリックして、NTP プロセスを再起動します。

（注）　サーバ設定を変更した場合は、システムを再起動する必要があります。一度に複数の [Server] の設定を変更および保存できますが、その変更を適用するには、[Reboot Server] をクリックする必要があります。

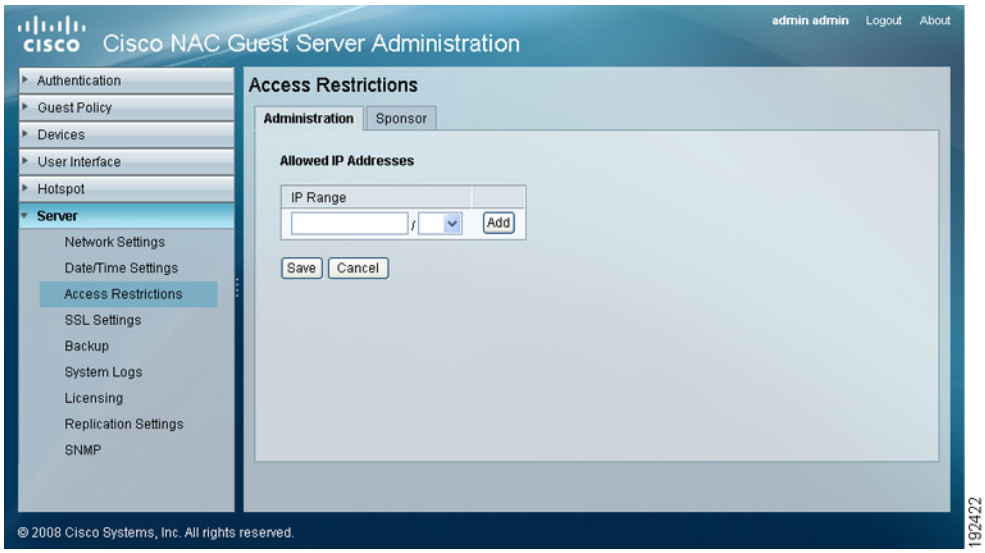
アクセス制限

いつでも管理インターフェイスおよびスポンサー インターフェイスに対しては特定の IP アドレス範囲だけにアクセスを制限するように、Cisco NAC ゲスト サーバを設定できます。

管理アクセス

ステップ 1　管理インターフェイスから、[Server] > [Access Restrictions] を選択し、[Administration] タブ（図 3-6 を参照）をクリックします。

図 3-6　アクセス制限（管理）



ステップ 2　[Allowed IP Addresses] フィールドに、ゲスト サーバ管理インターフェイスへのアクセスを許可する IP アドレスの範囲を入力し、ドロップダウン メニューを使用して CIDR サブネット範囲を適用します。

ステップ 3　[Add] をクリックして、アドレスをリストに追加します。

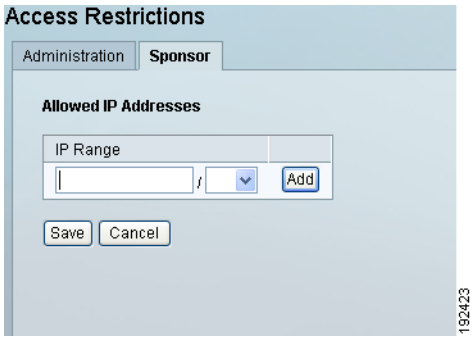
ステップ 4　[Save] をクリックして、変更を保存します。

（注）　IP Range フィールドをブランクのままにすると、必要な admin アカウント権限をユーザが持っている場合はすべての IP アドレスから管理インターフェイスにアクセスできます。

スポンサー アクセス

ステップ 1　管理インターフェイスから、[Server] > [Access Restrictions] を選択し、[Sponsor] タブ（図 3-7 を参照）をクリックします。

図 3-7　アクセス制限（スポンサー）



ステップ 2　スポンサー インターフェイスへのアクセスを許可する IP アドレスの範囲を入力し、ドロップダウン メニューを使用して CIDR サブネット範囲を適用します。

ステップ 3　続行するには [Save] をクリックします。

（注）　[IP Range] フィールドをブランクのままにすると、必要なスポンサー アカウント権限をユーザが持っている場合はすべての IP アドレスからスポンサー インターフェイスにアクセスできます。

（注）　サーバ設定を変更した場合は、システムを再起動する必要があります。一度に複数の [Server] の設定を変更および保存できますが、その変更を適用するには、[Reboot Server] をクリックする必要があります。

SSL 証明書の設定

スポンサーと管理者は HTTP または HTTPS を使用して Cisco NAC ゲスト サーバにアクセスできます。よりセキュアなアクセスのために、HTTPS の使用を推奨します。

ここでは、次の内容について説明します。

- HTTP または HTTPS を使用したゲスト サーバへのアクセス
- 一時証明書/CSR/秘密キーの生成
- 証明書ファイルのダウンロード
- 証明書ファイルのアップロード

HTTP または HTTPS を使用したゲスト サーバへのアクセス

スポンサーと管理者がポータルにアクセスする際、HTTP、HTTP と HTTPS の両方、または HTTPS だけを使用するのかを設定できます。

ステップ 1　管理インターフェイスの左側のパネルから、[Server] > [SSL Settings] を選択し、[SSL Settings] ページ（図 3-8 を参照）を表示します。

図 3-8　[SSL Settings] メイン ページ

ステップ 2　[SSL Settings] メイン ページには、次のオプションがあります。

- [Allow Only HTTPS]：選択されている場合、ゲスト サーバのスポンサー インターフェイスまたは管理インターフェイスに対する HTTPS アクセスだけが許可されます。
- [Allow Only HTTP]：選択されている場合、ゲスト サーバのスポンサー インターフェイスまたは管理インターフェイスに対する HTTP アクセスだけが許可されます。
- [Allow HTTPS and HTTP]：選択されている場合、ゲスト サーバのスポンサー インターフェイスまたは管理インターフェイスに対する HTTPS アクセスと HTTP アクセスの両方が許可されます。
- [Allow Only HTTPS (with HTTP Redirected to HTTPS)]：選択した場合、スポンサーと管理者は HTTPS および標準の HTTP によってポータルにアクセスできます。ただし、標準の HTTP 接続を使用した場合、スポンサーと管理者は HTTPS 経由でリダイレクトされます。

（注）　HTTP から HTTPS へのリダイレクトは、API アクセスではサポートされていません。

ステップ 3　選択したら、[Save Settings] ボタンをクリックします。

（注）　[Server] の設定を変更する場合は再起動が必要です。一度に複数の [Server] の設定を変更および保存してから再起動することができますが、その変更を適用するには、[Reboot Server] をクリックする必要があります。

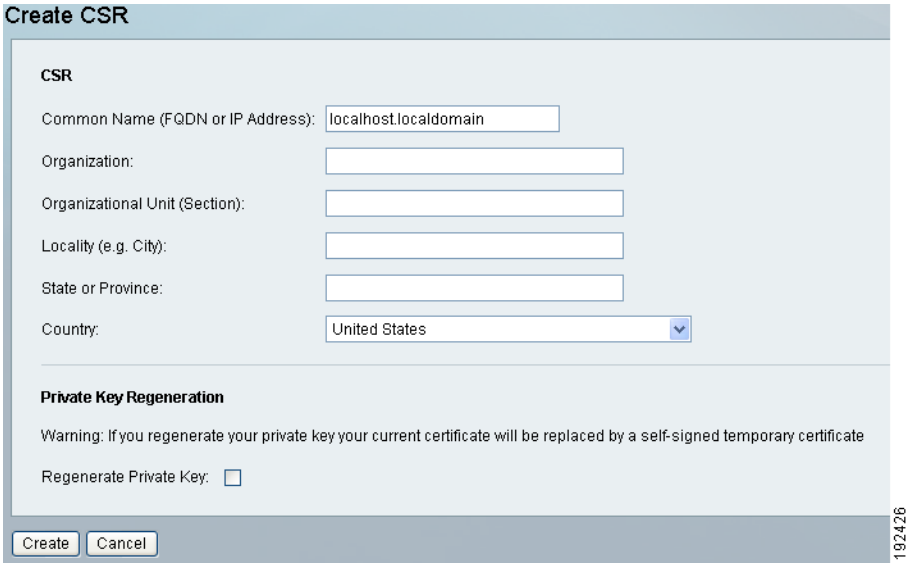
一時証明書/CSR/秘密キーの生成

Cisco NAC ゲスト サーバは、デフォルトの証明書がインストールされた状態で出荷されます。HTTPS を使用する場合、新しい一時証明書と秘密キーを生成することを強く推奨します。これらの生成を行うとき、Certificate Authority（CA；認証局）署名付き証明書を取得するために使用できる Certificate Signing Request（CSR；証明書署名要求）も生成されます。

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、[Server] > [SSL Settings] を選択し、[Create CSR] リンクをページの中央部分（図 3-9 を参照）でクリックすると、Create CSR フォーム（図 3-10 を参照）が表示されます。

図 3-9　CSR

図 3-10　CSR の生成



ステップ 2　Create CSR フォームに、一時証明書と CSR の詳細を入力します。

- [Common Name (FQDN or IP Address)]：Cisco NAC ゲスト サーバの IP アドレス、またはゲスト サーバの Fully Qualified Domain Name（FQDN；完全修飾ドメイン名）。FQDN は DNS で正しく解決する必要があります。
- [Organization]：組織または会社の名前。
- [Organizational Unit (Section)]：デバイスを所有する部門または部署の名前。
- [Locality (e.g. City)]：サーバが配置されている都市。
- [State or Province]：サーバが配置されている州。
- [Country]：該当する国をドロップダウン メニューから選択します。

ステップ 3　[Regenerate Private Key] チェックボックスは任意の選択項目で、既存の秘密キーに問題があると思われる場合に使用します。秘密キーを再生成すると、現在の証明書は無効になり、新しい秘密キーと CSR を使用して新しい自己署名付き一時証明書が生成されます。秘密キーを再生成する場合は、このオプションを選択します。

ステップ 4　[Create] をクリックします。

ステップ 5　[Certificate Signing Request] ページが再び表示されます（図 3-9 を参照）。秘密キーを再生成することを選択すると、サーバを再起動するように要求されます。新しい証明書と秘密キーを使用するには、サーバを再起動する必要があります。

ステップ 6　[Create Temporary Certificate from CSR] オプションと [Download CSR] オプションが使用できるようになります（図 3-11 を参照）。

図 3-11　Create CSR と Download CSR

ステップ 7　[Create Temporary Certificate from CSR] を選択すると、前もって要求される CSR（ステップ 1 ～ 4 で作成）から一時証明書が生成されます。

ステップ 8　CSR をダウンロードするには、[Download CSR] オプション（図 3-11）をクリックします。CSR を CA に送信し、応答として CA 署名付き証明書を取得したら、「証明書ファイルのアップロード」（P.3-14）の手順に従って、その証明書をアップロードできます。

ステップ 9　新しい一時証明書を使用するには、Web サーバ プロセスを再起動する必要があります。[Reboot Server] ボタンをクリックします（図 3-8 を参照）。

（注）　[Server] の設定を変更する場合は再起動が必要です。一度に複数の [Server] の設定を変更および保存してから再起動することができますが、その変更を適用するには、[Reboot Server] をクリックする必要があります。

ヒント　中間 CA によって発行された SSL 証明書をインストールする場合は、CLI の手順を実行する必要があります。この手順に関するガイダンスを受け取るには、Cisco TAC に連絡してください。

CLI を使用した自己署名 SSL 証明書の生成

管理者が NAC ゲスト サーバに関連しない SSL 証明書をインストールしようとすると、「The Current Private Key does not Correspond to the Current Certificate」というエラー メッセージが表示されます。

[Reboot Server] オプションをクリックすると、無効な証明書がアップロードされ、GUI にアクセスできなくなります。この問題を回避するには、CLI を使用して自己署名 SSL 証明書を生成し、インストールします。これにより、ユーザが GUI にアクセスできるようになります。

CLI を使用して自己署名 SSL 証明書を生成するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、キーおよび証明書ファイルを生成します。

```
openssl req -new -key /etc/pki/tls/private/localhost.key -nodes -x509 -days 365 -out
/etc/pki/tls/certs/localhost.crt
```

ステップ 2　次のように、証明書要求に組み込まれる適切な情報を入力します。

```
Country Name (2 letter code) [GB]:
State or Province Name (full name) [Berkshire]:
Locality Name (eg, city) [Newbury]:
Organization Name (eg, company) [My Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:
Email Address []:
```

ステップ 3　次のコマンドを入力して、証明書およびキーのコピーを Postgres に提供します。

```
cp /etc/pki/tls/certs/localhost.crt /var/lib/pgsql/data/server.crt
chmod 600 /var/lib/pgsql/data/server.crt
chown postgres:postgres /var/lib/pgsql/data/server.crt

cp /etc/pki/tls/private/localhost.key /var/lib/pgsql/data/server.key
chmod 600 /var/lib/pgsql/data/server.key
chown postgres:postgres /var/lib/pgsql/data/server.key
```

ステップ 4　サーバをリブートします。

サーバをリブートすると、GUI にアクセスできます。

証明書ファイルのダウンロード

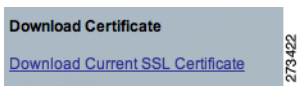
証明書のダウンロード

証明書と秘密キーをバックアップすることを強く推奨します。証明書は、安全な場所に手動でバックアップするために、管理インターフェイスからダウンロードできます。

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、[Server] > [SSL Settings] を選択します。

ステップ 2　[Download Current SSL Certificate] をページの [Download Certificate] セクション（図 3-12 を参照）から選択します。

図 3-12　証明書ファイルのダウンロード



ステップ 3　SSL 証明書を安全なバックアップ場所に保存します。

秘密キーのダウンロード

秘密キーを取得するには、ゲスト サーバへの SFTP 接続を使用する必要があります。Windows プラットフォームの場合、http://winscp.net から無償の SFTP クライアントを入手できます。

ステップ 1　Cisco NAC ゲスト サーバへの SFTP 接続を開きます。認証のクレデンシャルはコマンドラインと同じです。root ユーザ名と初期セットアップでこのアカウントに割り当てたパスワードを使用してログインします。

ステップ 2　**/etc/pki/tls/private/localhost.key** ファイルをダウンロードし、安全なバックアップ場所に保存します。

証明書ファイルのアップロード

Cisco NAC ゲスト サーバは、証明書ファイルをゲスト サーバ アプライアンスにインポートおよびアップロードする方法を提供します。[Upload Certificates] オプションを使用すると、CA 署名付き証明書のインストールまたは以前バックアップされた Base 64 PEM 形式の証明書ファイルの復元を行うことができます。

（注）　Base 64 PEM 形式の証明書ファイルをアップロードする必要があります。

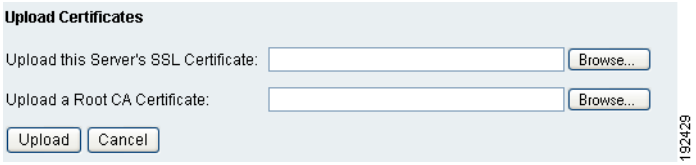
証明書ファイルは、バックアップ プロセスの一部としてバックアップされません。「証明書ファイルのダウンロード」（P.3-13）で説明されているように、手動でバックアップする必要があります。

ワイルドカード証明書はサポートされていません。

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、[Server] > [SSL Settings] を選択します。

ステップ 2　ページの下部に [Upload Certificates] セクション（図 3-13 を参照）が表示されます。

図 3-13　証明書ファイルのアップロード



ステップ 3　[Browse] ボタンをクリックし、アップロードする SSL 証明書ファイルまたはルート CA 証明書ファイルを見つけて、[Upload] ボタンをクリックします。

警告　**証明書をアップロードする場合、インストールされている秘密キーと一致する必要があります。**

ステップ 4　新しいサーバ SSL 証明書をアップロードする場合、その証明書を有効にするために、サーバを再起動するように要求されます。

（注）　[Server] の設定を変更する場合は再起動が必要です。一度に複数の [Server] の設定を変更および保存してから再起動することができますが、その変更を適用するには、[Reboot Server] をクリックする必要があります。

秘密キーのアップロード

秘密キーをアップロードするには、ゲスト サーバへの SFTP 接続を使用する必要があります。Windows プラットフォームの場合、http://winscp.net から無償の SFTP クライアントを入手できます。

ステップ 1　Cisco NAC ゲスト サーバへの SFTP 接続を開きます。認証のクレデンシャルはコマンドラインと同じです。root ユーザ名と初期セットアップでこのアカウントに割り当てたパスワードを使用してログインします。

ステップ 2　キーを /etc/pki/tls/private/localhost.key ファイルにアップロードします。

ステップ 3　root が所有し、644 の権限を持つように、所有権とファイルの権限を変更します。

```
chown root:root /etc/pki/tls/private/localhost.key
chmod 644 /etc/pki/tls/private/localhost.key
```

ステップ 4　新しいキーを /var/lib/pgsql/data/server.key にコピーします。

```
cp /etc/pki/tls/private/localhost.key /var/lib/pgsql/data/server.key
```

ステップ 5　postgres が所有し、700 の権限を持つように、所有権とファイルの権限を変更します。

```
chown postgres:postgres /var/lib/pgsql/data/server.key
chmod 700 /var/lib/pgsql/data/server.key
```

警告　**サーバまたはサーバ証明書が無効になる可能性があるため、説明した方法に従ってサーバ秘密キーで直接作業する前に、PKI に関する詳細な知識を持つことを強く推奨します。**

管理者認証の設定

Cisco NAC ゲスト サーバには、「admin」という 1 つのデフォルト管理者アカウントがあります。また、外部の RADIUS サーバに対して管理者を認証するように、Cisco NAC ゲスト サーバを設定することもできます。[Authentication] メニューの下にある [Admin Accounts] ページでは、追加の管理者アカウントを作成、編集、および削除することができます。

ここでは、次の内容について説明します。

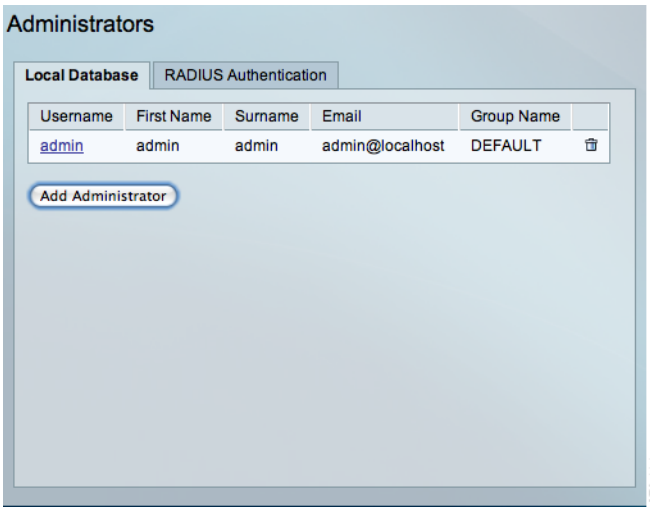
- 新しい admin アカウントの追加
- 既存の admin アカウントの編集
- 既存の admin アカウントの削除
- admin セッション タイムアウト
- 管理者認証用の RADIUS の設定

新しい admin アカウントの追加

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、[Authentication] > [Administrators] を選択します。

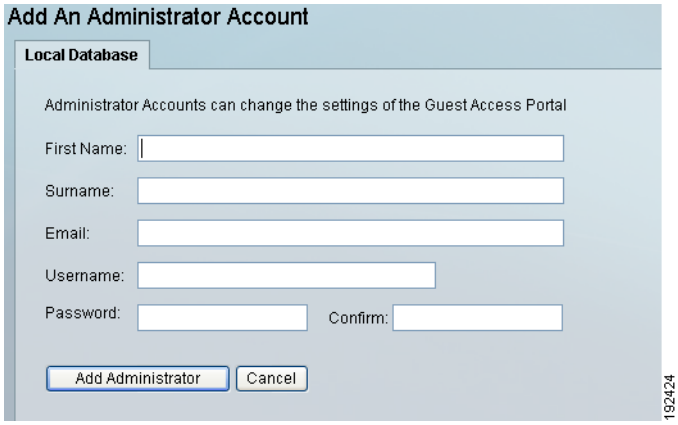
ステップ 2　[Administrators] ページの [Local Database] タブ（図 3-14 を参照）で、[Add Administrator] ボタンをクリックします。

図 3-14　管理者アカウント



ステップ 3　[Add Administrator] ページ（図 3-15 を参照）で、すべての admin ユーザのクレデンシャルを入力します。

図 3-15　admin ユーザの追加



- [First Name] : admin ユーザの名を入力します。
- [Surname] : admin ユーザの姓を入力します。
- [Email Address] : admin ユーザの電子メール アドレスを入力します。
- [Username] : admin アカウントのユーザ名を入力します。
- [Password] : admin アカウントのパスワードを入力します。
- [Confirm] : admin アカウントのパスワードを再入力します。

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

- エラーがある場合、アカウントは追加されず、ページの上部にエラー メッセージが表示されます。
- 正常に追加された場合、ページの上部に成功のメッセージが表示され、admin アカウントをさらに追加できます。

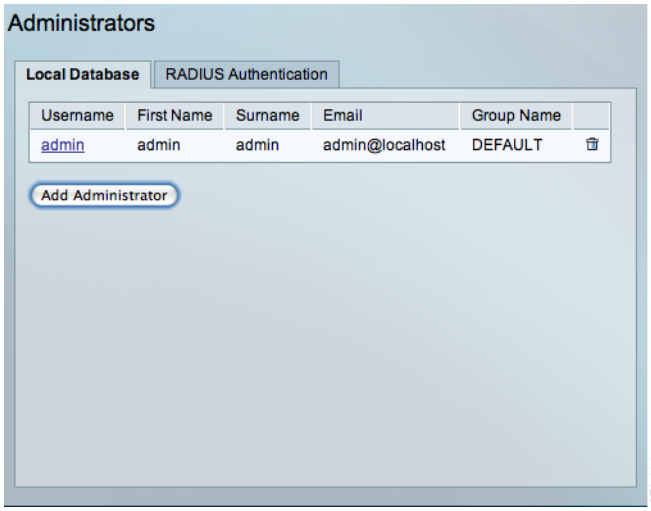
既存の admin アカウントの編集

すでに作成された admin アカウントの設定を変更できます。

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、[Authentication] > [Administrators] を選択します。

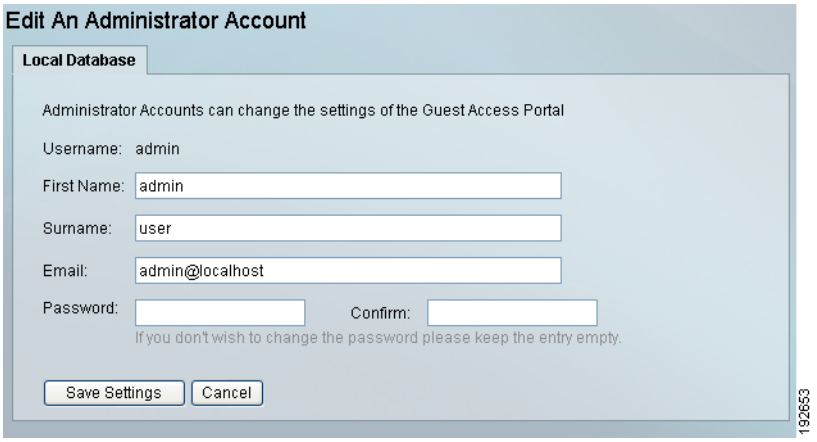
ステップ 2　[Administrators] ページの [Local Database] タブ（図 3-16 を参照）で、リストのユーザ名をクリックします。

図 3-16　編集対象の admin ユーザ



ステップ 3　[Edit Administrator] ページ（図 3-17 を参照）で、ユーザのクレデンシャルを編集します。

図 3-17　admin アカウントの編集



- [First Name] : admin ユーザの名を編集します。
- [Surname] : admin ユーザの姓を編集します。
- [Email Address] : admin ユーザの電子メール アドレスを編集します。
- [Password] : admin アカウントのパスワードを編集します。
- [Confirm] : admin アカウントのパスワードを編集します。

（注）　強力なパスワードを使用することを推奨します。それには、辞書にあるような単語は使わず、6 文字以上とし、5 種類以上の文字を含めるようにします。

（注）　[Password] フィールドと [Repeat Password] フィールドを空にすると、既存のパスワードが維持されます。

ステップ 4　[Save Settings] ボタンをクリックします。

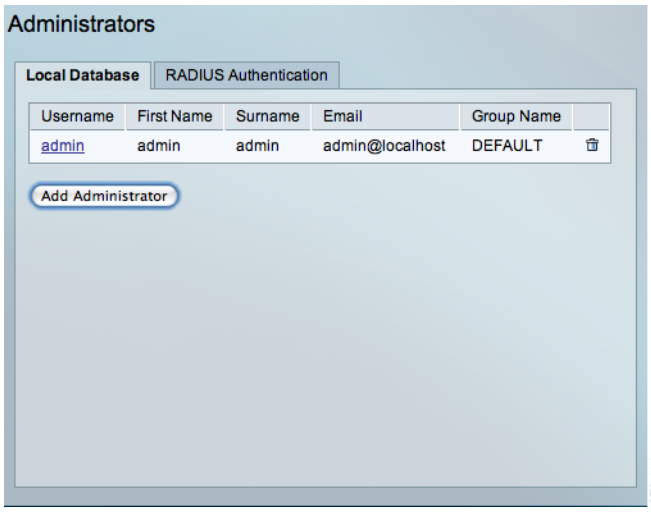
- エラーがある場合、アカウントは変更されず、ページの上部にエラー メッセージが表示されます。
- 正常に変更された場合、ページの上部に成功のメッセージが表示され、同じ admin アカウントをさらに変更できます。

既存の admin アカウントの削除

既存の admin アカウントを管理インターフェイスから削除できます。

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、[Authentication] > [Administrators] を選択します。

図 3-18　削除する admin アカウントの選択



ステップ 2　[Admin Accounts] ページ（図 3-18 を参照）で、削除するユーザ エントリの端にあるゴミ箱の形をしたアイコンをクリックします。

ステップ 3　プロンプトが表示されたら、[OK] をクリックしてユーザを削除するか、または [Cancel] をクリックして削除をキャンセルします。正常に削除された場合、ページの上部に成功のメッセージが表示されます。

admin セッション タイムアウト

スポンサー インターフェイスに対して定義したセッション タイムアウトは、管理インターフェイスにも適用されます。詳細については、「セッション タイムアウト」（P.4-20）を参照してください。

管理者認証用の RADIUS の設定

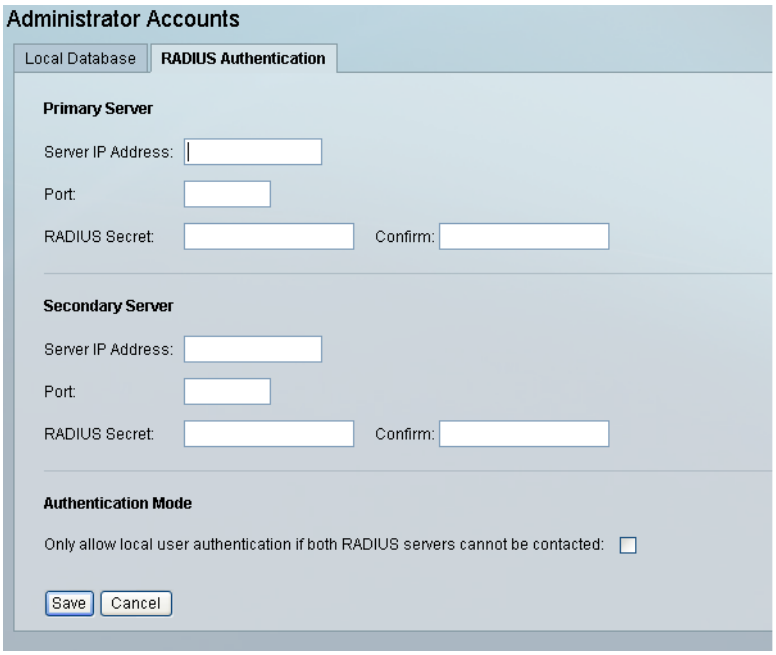
（注）　Cisco NAC ゲスト サーバは、正常に認証された admin ユーザに対してだけアクセスを許可します。RADIUS サーバは、6（administrative）に設定された IETF Service-Type 属性を返します。

ローカル管理者アカウントを設定する代わりに、RADIUS を介して RADIUS サーバに対して認証するように admin ユーザを設定することもできます。管理者認証用に RADIUS 認証を設定するには、次の手順を実行します。

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

ステップ 2　[RADIUS Authentication] タブをクリックします（図 3-19 を参照）。

図 3-19　管理者の 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　両方の RADIUS サーバに接続できない場合に Local Admin アカウントが許可されるようにするには、[Authentication Mode] チェックボックスをオンにします。このオプションをオフにすると、認証がいずれかの RADIUS サーバで拒否された場合に Local Admin アカウントが許可されます。

ステップ 9　[Save] ボタンをクリックして、管理者の RADIUS の設定を保存します。