CHAPTER 10

ローカルの Certified Devices と Floating Devices

この章では、Cisco NAC アプライアンスの実装の CAS レベルで設定可能なローカル設定について説明します。CAM Web コンソールでの Cisco NAC アプライアンスの設定の詳細については、『*Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.9*』を参照してください。この章の内容は、次のとおりです。

概要

ログイン ページ、Nessus スキャン プラグインの動作、Agent の要件、ユーザ ロールなど、Cisco NAC アプライアンスのほとんどの要素は、すべての CAS にグローバルに設定できます。ただし、特定の作業は、各 CAS にローカル レベルで実行することもできます。これらの要素は次のとおりです。

- 認証済みデバイスの削除

  ユーザ認証が行われ、デバイスがネットワーク スキャンに合格して脆弱性が検出されなかった場合や、Agent 要件を満たしている場合、各 CAS の Cisco NAC アプライアンス モジュールによって該当するデバイスが Certified Devices リストに**自動的に**追加されます。認証済みデバイスは、リストから削除されないかぎり、クリーンであると見なされます。指定時刻に、または指定した間隔で Certified Devices リストからデバイスを削除して、ネットワーク スキャンと Agent チェックを強制的に繰り返すことができます。Agent ユーザのデバイスは、ログインするたびに必ず、要件を満たしているかどうかスキャンされます。

- 免除デバイスの追加/削除

  免除デバイスは、ネットワーク スキャン（Nessus スキャン）による認証対象にならないデバイスです。デバイスを免除デバイスに指定して、ネットワーク スキャンを省略できるようにしたり、免除デバイスを削除して、Cisco NAC アプライアンス要件を満たすように強制することができます。免除デバイスの追加または削除は、常に**手動**で行います。

- フローティング デバイスの指定

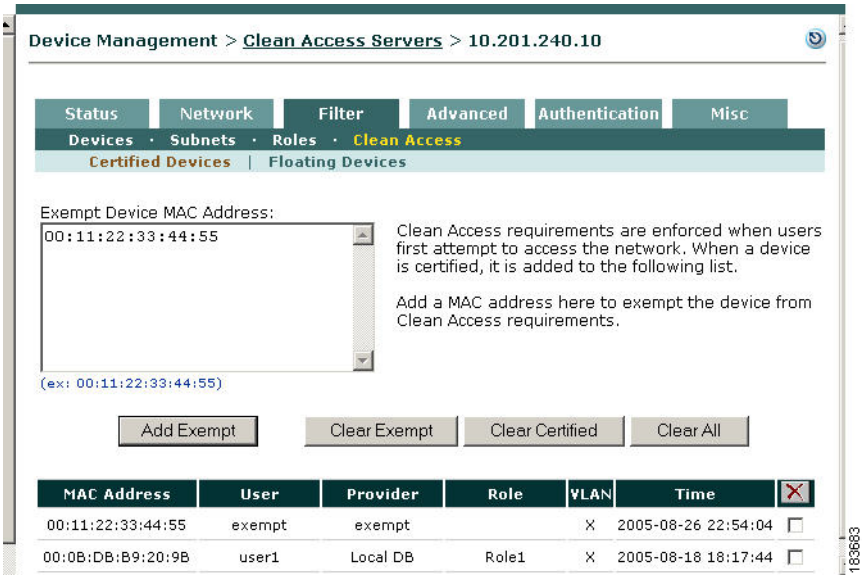
  フローティング デバイスにはログインごとに認証が必要で、1 回のユーザ セッションの間だけ認証が有効です。フローティング デバイスは常に手動で追加されます。

免除デバイスの追加

デバイスを免除デバイスとして指定するには、自動生成される Certified Devices リストに、そのデバイスを**手動で**追加します。デバイスがネットワーク スキャンに合格して脆弱性が検出されないか、Agent システム要件を満たしているか、その両方の場合に限り、Certified Devices リストにデバイスが追加されます。リストに追加されたデバイスはクリーンであると見なされため、その MAC アドレスが Certified Devices リストにある間は、認証プロセスを免除されます。実際に免除デバイスを追加すると、リストに追加しているデバイスがクリーンであるかどうかを認証する自動ネットワーク スキャン認証プロセスが省略されます。

ステップ 1　[Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Filter] > [Clean Access] > [Certified Devices] の順番に進みます。

図 10-1　　認証済みデバイス（ローカル）



ステップ 2　テキスト フィールドに、免除デバイスの MAC アドレスを入力します。複数のアドレスを区切るには、改行を使用します。

ステップ 3　[Add Exempt] をクリックします。

免除デバイスの削除

免除デバイスを削除すると、Certified Devices リストからそのデバイスが削除され、強制的に Nessus スキャンが適用されます。免除デバイスは手動でリストに追加されるので、削除も手動で行う必要があります。したがって、グローバルの Certified Devices Timer を使用して一定間隔で定期的にリストを消去しても、Certified Devices リスト上の免除デバイスは自動的には削除されません。

リストから免除デバイスを手動で削除する手順は、次のとおりです。

ステップ 1　[Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Filter] > [Clean Access] > [Certified Devices] の順番に進みます（図 10-1 を参照）。

ステップ 2　[Clear Exempt] をクリックします。この CAS のすべての免除デバイスがリストから削除されます。

認証済みデバイスの削除

デバイスは CAS によって Certified Devices リストに追加され、リストから削除されるまではクリーンであると見なされます。

認証済みデバイスをある CAS から別の CAS に移動した場合、そのデバイスが全 CAS に対してグローバルレベルで免除デバイスとして手動でリストに追加されていなければ、新しい CAS で再度 Nessus スキャンを受けなければなりません。したがって、ある CAS の要件を別の CAS より厳しくするといったことも可能です。

CAM には、認証元 CAS に従ってデバイス情報を格納する、中央の Certified Devices リストが保持されます。CAM は各 CAS の認証済みデバイスを該当する CAS にパブリッシュし、さらにすべての CAS にグローバルな免除デバイスをパブリッシュします。

デバイスの認証およびリストへの追加は CAS 単位でしか実行できませんが、認証済みデバイスの削除はすべての CAS にグローバルに実行したり、特定の CAS にローカルに実行することができます。認証済みデバイスを削除すると、そのデバイスに Cisco NAC アプライアンス スキャンと要件チェックを強制的に繰り返すことになります。

- グローバル レベル（自動）: [Certified Devices Timer] フォーム（[Device Management] > [Clean Access] > [Certified Devices] > [Timer]）を使用して、定期的にリストを削除できます。
- グローバル レベル（手動）: グローバル フォーム（[Device Management] > [Clean Access] > [Certified Devices]）を使用して、Certified Devices リストを手動で削除できます。
- ローカル レベル（手動）: ローカル フォーム（[Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Filter] > [Clean Access] > [Certified Devices]）を使用して、特定の CAS の認証済みデバイスを手動で削除できます。

（注）

- Certified Devices リストを手動または自動的に削除すると、ユーザはネットワークからログオフされます。
- [Monitoring] > [Online Users] > [View Online Users] でユーザを削除しても、Certified Devices リストからクライアントは削除されません。したがって、クリーンと見なされているクライアントデバイスは認証プロセスを強制されずに、ユーザは再度ログインできます。

特定の CAS のリストから手動でデバイスを削除する手順は、次のとおりです。

ステップ 1　[Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Filter] > [Clean Access] > [Certified Devices] の順番に進みます（図 10-1 を参照）。

ステップ 2　[Clear Exempt] をクリックして、（[Add Exempt] を使用して）手動で追加されたデバイスを削除します。

ステップ 3　[Clear Certified] をクリックして、Cisco NAC アプライアンス基準を満たした後にリストに追加されたデバイスを削除します。

ステップ 4　[Clear All] をクリックして、両方のタイプのデバイスを削除します。

ステップ 5　ユーザの MAC アドレスの横にあるチェックボックスをオンにし、[Kick Individual User] ボタンをクリックして、ユーザを個別に削除します。

（注）　ローカル リストに表示されるのは、特定の CAS に対応する認証済みデバイスだけです。すべての CAS の認証済みデバイスを表示するには、[Device Management] > [Clean Access] の順番に進みます。

フローティング デバイスの指定

フローティング デバイスの認証が有効なのは、1 回のユーザ セッションの間だけです。ユーザがログアウトすると、そのデバイスの次のユーザは再度認証を受けなければなりません。フローティング デバイスは、kiosk コンピュータや図書館で貸し出される無線カードなどの共用機器を管理する場合に便利です。

認証要件から免除されないデバイスは、MAC アドレスで指定することもできます。これは、非信頼（管理対象）ネットワークからマルチユーザ トラフィックをチャネリングするダイヤルアップ ルータなど、マルチユーザ デバイスの場合に役立ちます。この場合、CAS は信頼ネットワークのトラフィック送信元アドレスとして、そのデバイスの MAC アドレスだけを認識します。そのデバイスがフローティング デバイスとして設定されていない場合は、最初のユーザが認証されたあとに、別のユーザは意図せずに認証を免除されます。認証されないフローティング デバイスとしてルータの MAC アドレスを設定すれば、そのデバイスを通じてネットワークにアクセスする各ユーザは、脆弱性と要件に適合しているかどうかが個別に評価されます。

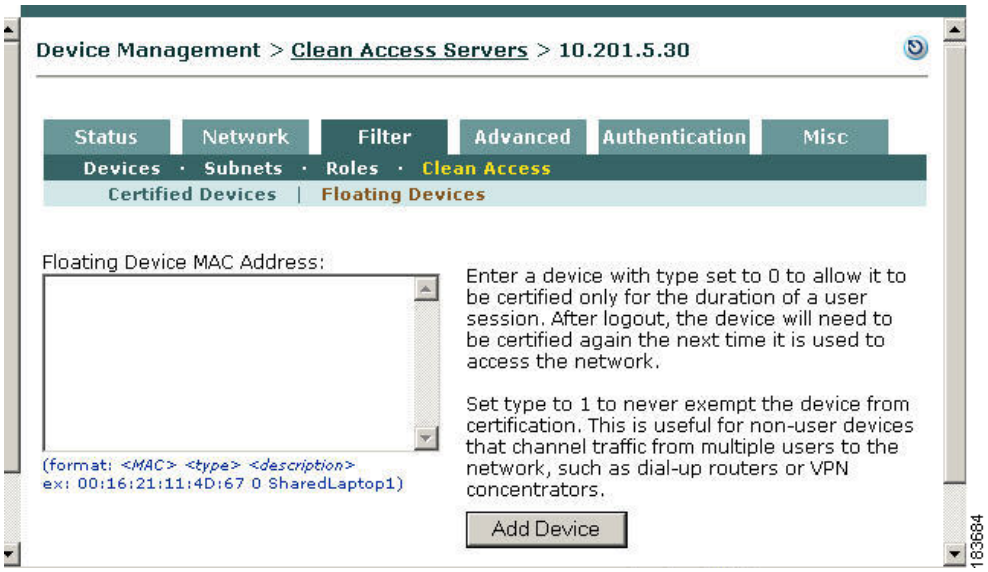
この場合、ユーザは IP アドレスで区別されるため、ユーザごとに異なる IP アドレスを設定する必要があります。ルータが Network Address Translation（NAT; ネットワーク アドレス変換）サービスを実行する場合、CAM はユーザを区別できず、最初のユーザだけが認証されます。

「フローティング デバイスとしての VPN コンセントレータの追加」（P.6-10）も参照してください。

ローカル フローティング デバイスを指定する手順は、次のとおりです。

ステップ 1　[Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Filter] > [Clean Access] > [Floating Devices] の順番に進みます。

図 10-2　　フローティング デバイス（ローカル）



ステップ 2　フローティング デバイスを次の形式の MAC アドレスで指定します。

<MAC> <type> <description>

上記で

- *MAC* はデバイスの MAC アドレスです（`00:16:21:23:4D:00` などの標準 16 進 MAC アドレス形式）。
- *type* は、次のいずれかです。

  0：セッション範囲での認証の場合

  1：そのデバイスを認証済みとは見なさない場合
- *description* は、そのデバイスの説明です（任意）。

各要素の区切りにはスペースを入力し、複数のエントリ間の区切りには改行を使用します。例：

```
00:16:21:23:4D:00 0 LibCard1
00:16:34:21:4C:00 0 LibCard2
00:16:11:12:4A:00 1 Router1
```

ステップ 3　[Add Device] をクリックして、設定値を保存します。

ステップ 4　フローティング MAC アドレスを削除する場合は、そのアドレスの横にある [Delete] アイコンをクリックします。