CHAPTER 8

Cisco VPN コンセントレータとの統合

この章では、Clean Access Server（CAS）と Cisco VPN コンセントレータを統合するために必要な設定について説明します。この章の内容は、次のとおりです。

概要

Cisco NAC アプライアンスを使用すると、VPN コンセントレータまたはルータ（または複数のルータ）の後ろにインバンド CAS を配置できます。また、ユーザと CAS の間に 1 つまたは複数のルータがある場合、Clean Access Manager（CAM）と CAS が一意の IP アドレスによってユーザ セッションをトラッキングできるようにして、マルチホップ レイヤ 3 インバンド配置をサポートしています。1 つの CAS で L2 と L3 のユーザに両方対応することも可能です。レイヤ 2 接続されたユーザがいる場合、CAM/CAS は引き続きユーザの MAC（メディア アクセス制御）アドレスに基づいてユーザ セッションを管理します。

ユーザが L3 ホップに関して 1 つまたは複数ホップ以上離れている場合は、次の点に注意してください。

- ユーザ セッションは MAC アドレスではなく、一意の IP アドレスに基づいて確立されます。
- ユーザの IP アドレスが変更された場合は（ユーザとの VPN 接続が切断された場合など）、クライアントには Clean Access 認証プロセスを再実行する必要があります。
- クライアントと CAS が L3 ホップに関して 1 つまたは複数ホップ以上離れている場合に、クライアントが CAS を検出するには、最初に Clean Access Agent（CAA）をインストールし、CAS を介してダウンロードする必要があります。これにより、ユーザが CAS から L3 ホップに関して 1 つまたは複数ホップ以上離れている場合に、以降のログインに必要な CAM 情報がクライアントに提供されます。CAS からの直接ダウンロード以外の方法を使用して Agent を取得してインストールしても、必要な CAM 情報は Agent に提供されず、インストールされたこれらの Agent はマルチホップ L3 配置で稼働できません。
- Certified List は、MAC アドレスによって L2 および L3 VPN ユーザをトラッキングし、これらのユーザに Certified Devices Timer が適用されます。
- ネットワーク スキャナや CAA ログなど、その他のすべてのユーザ監査証跡は、マルチホップ L3 ユーザ用に保持されます。

- セッション タイマーは、マルチホップ L3 インバンド配置の場合も、L2（インバンドまたは Out-Of-Band［OOB; アウトオブバンド］）配置の場合と同様に機能します。

  マルチホップ L3 VPN コンセントレータ 統合構成で SSO（シングルサインオン）機能が設定されている場合は、CAS でユーザのセッションがタイムアウトになっても、そのユーザがまだ VPN コンセントレータにログインしたままであれば、ユーザ名 / パスワード提供しなくてもユーザ セッションが復元されます。
- ハートビート タイマーは、L3 配置では機能せず、アウトオブバンド配置には適用されません。

  ただし、CAS が VPN コンセントレータの背後にある最初のホップである場合、ハートビート タイマーは機能します。この場合、VPN コンセントレータは、自身の現在のトンネル クライアントの IP アドレスに対する ARP クエリーに応答するからです。

必要なトポロジーおよび設定は、大幅に簡素化されています。図 8-1 に、VPN コンセントレータと統合された Cisco NAC アプライアンス ネットワークを示します。図 8-2 に複数のアカウンティング サーバが使用されている場合の Cisco NAC アプライアンスとの「統合前の」VPN コンセントレータの構成、図 8-3 に「統合後の」構成を示します。CAS は VPN コンセントレータの単一の RADIUS アカウンティング サーバとして設定する必要があります。VPN コンセントレータがすでに 1 つまたは複数の RADIUS アカウンティング サーバ用に設定されている場合は、これらの設定をコンセントレータから CAS に転送する必要があります。

（注）　VPN コンセントレータでスプリット トンネリングを使用している場合、スプリット トンネルが、Discovery Host 用に使用されているネットワークへのアクセスを許可するようにしてください。Discovery Host が CAM IP アドレスと同じである場合、CAM を許可する必要があります。

SSO

CiscoNAC アプライアンスは VPN コンセントレータとともに導入できるだけでなく、SSO を介して Cisco VPN コンセントレータ ユーザに最適な操作性を提供します。VPN クライアントを介してログインするユーザは、Cisco NAC アプライアンスに再ログインする必要がありません。Cisco NAC アプライアンスは VPN ログイン、および任意の VPN ユーザ グループ / クラス属性を利用して、ユーザを特定のロールに対応付けます。

このレベルの統合を実現するには、RADIUS アカウンティング サーバと、RADIUS アカウンティング プロキシとして機能する CAS を使用します。Cisco NAC アプライアンスは、以下に対する SSO をサポートしています。

- Cisco VPN コンセントレータ
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco Airespace Wireless LAN コントローラ
- Cisco SSL VPN Client（Full Tunnel）
- Cisco VPN Client（IPSec）

（注）　CAA を VPN トンネル モードで機能させるには、CAS で「**Enable L3 support**」オプションをオンにする必要があります（**Device Management > Clean Access Servers > Manage [CAS_IP] > Network > IP**）。

（注）　CAS は、SSO を実現するため、Calling_Station_ID または Framed_IP_address RADIUS のいずれの属性からクライアントの IP アドレスを取得できます。SSO のための Cisco NAC アプライアンス RADIUS アカウンティング サポートには、Cisco Airespace Wireless LAN コントローラ が含まれています。Cisco NAC アプライアンスと SSO を連携させるには、Cisco Airespace Wireless LAN コントローラから Calling_Station_IP 属性をクライアントの IP アドレスとして送信する必要があります（逆に、Framed_IP_address 属性は VPN コンセントレータで使用されます）。「Active VPN Clients の表示」（p.8-17）も参照してください。

詳細については、「CAS/CAM の SSO の設定」（p.8-10）を参照してください。

図 8-1　Cisco NAC アプライアンスと統合された VPN コンセントレータ

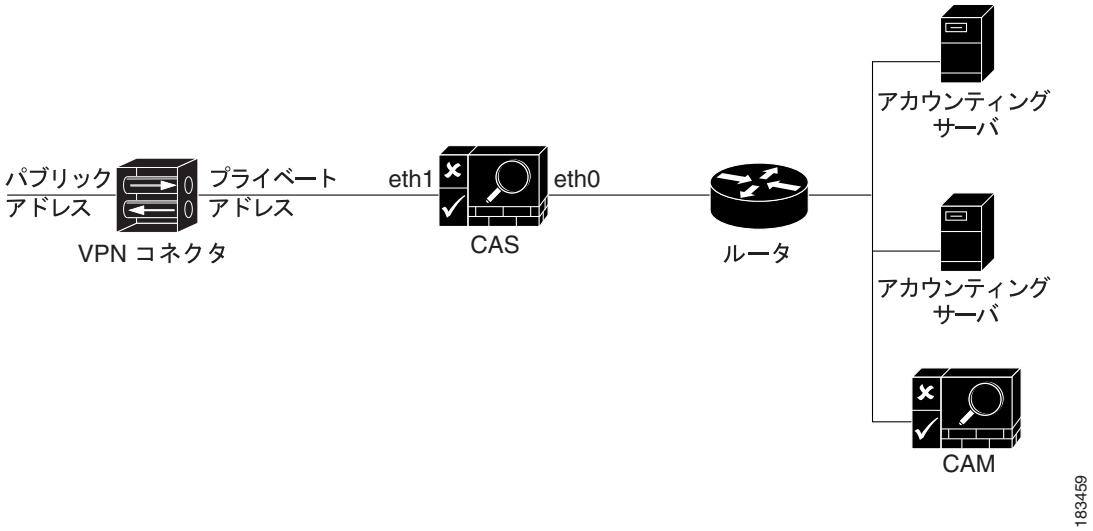


図 8-2　Clean Access との統合前の VPN コンセントレータ

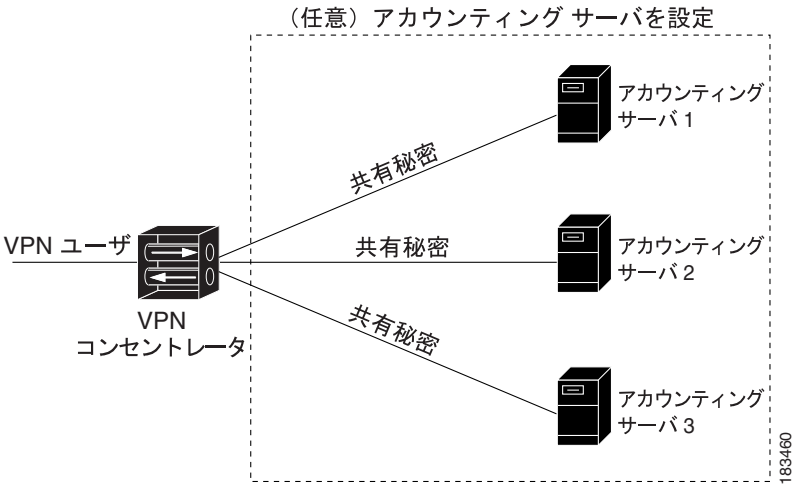
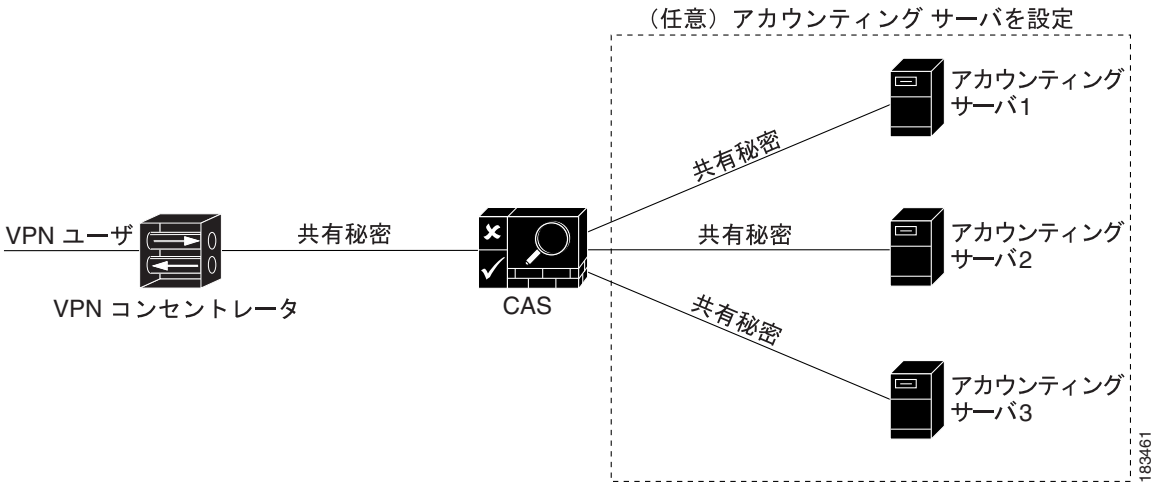


図 8-3　Clean Access との統合後の VPN コンセントレータ



VPN コンセントレータとの統合のための Clean Access の設定

VPN コンセントレータと連携するように Cisco NAC アプライアンスを設定するには、次の手順が必要です。

ステップ 1　デフォルト ログイン ページの追加

ステップ 2　VPN ユーザに対するユーザ ロールおよび Clean Access 要件の設定

ステップ 3　CAS での L3 サポートのイネーブル化

ステップ 4　Discovery Host の確認

ステップ 5　CAS への VPN コンセントレータの追加

ステップ 6　CAS を VPN コンセントレータの RADIUS アカウンティング サーバに設定

ステップ 7　CAS へのアカウンティング サーバの追加

ステップ 8　VPN コンセントレータとアカウンティング サーバのマッピング

ステップ 9　（任意）認証サーバ マッピング規則の作成

ステップ 10　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

ステップ 11　CAS/CAM の SSO の設定

ステップ 12　Cisco VPN SSO の CAM での（任意）認証サーバ マッピング規則の作成

ステップ 13　CAA および VPN コンセントレータと SSO としてのテスト

ステップ 14　Active VPN Clients の表示（トラブルシューティング用）

デフォルト ログイン ページの追加

CAA によるユーザの認証を可能にするには、Web ログイン ユーザと CAA ユーザの両方のためのログイン ページをシステムに追加する必要があります。デフォルトのユーザ ログイン ページを迅速に追加するには、**Administration > User Pages > Login Page > Add | Add** を選択します。ログイン ページの設定オプションの詳細については、『*Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide, Release 4.1(1)*』を参照してください。

ユーザ ロールおよび Clean Access 要件の設定

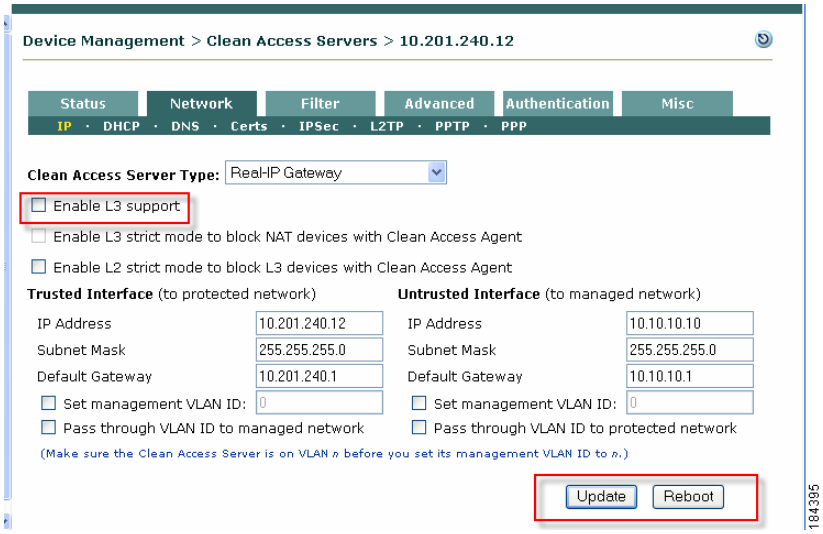
VPN ユーザに Clean Access プロセスを適用するには、Clean Access 要件とともにユーザ ロールを設定する必要があります。設定の詳細については、『*Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide, Release 4.1(1)*』を参照してください。

CAS での L3 サポートのイネーブル化

CAA を VPN トンネル モードで機能させるには、CAS の IP フォームで「**Enable L3 support**」オプションをオンにする必要があります。

1. **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Network > IP** の順番に進みます。

図 8-4　CAS Network タブ — Enable L3 Support



2. **Clean Access Server Type**、**Trusted Interface**、および **Untrusted Interface** 設定は正しく設定されている必要があります（CAS を追加した時点以降）。
3. **Enable L3 support** のチェックボックスをクリックします。
4. **Update** をクリックします。
5. **Reboot** をクリックします。

（注）

- L3 機能のイネーブル化 / ディセーブル化は、デフォルトでディセーブルです。有効にするには、CAS の **Update** および **Reboot** を実行する必要があります。**Update** を実行すると、次にリブートするまで、変更された設定が Web コンソールに維持されます。**Reboot** を実行すると、CAS のプロセスが起動します。
- L3 および L2 strict オプションは同時に使用できません。一方のオプションをイネーブルにすると、他方のオプションがディセーブルになります。

「L3 サポートのイネーブル化」（p.5-13）も参照してください。

Discovery Host の確認

CAA で VPN または L3 配置の CAS を検出できるようにするには、Discovery Host をイネーブルにする必要があります。デフォルトでは、Discovery Host フィールドは CAM の IP アドレスに設定されています。VPN コンセントレータは、ユーザと CAS の間のルータとして機能するので、Agent は UDP 8096 検出パケットを CAS のネットワークに向けるために、Discovery Host を使用します。CAS は、これらのパケットを使用して CAA がアクティブであることを認識し、CAM に到達するまえにパケットを廃棄します。Agent をクライアント マシンに配布およびインストールする前に、CAM で Discovery Host フィールドを設定する必要があります。

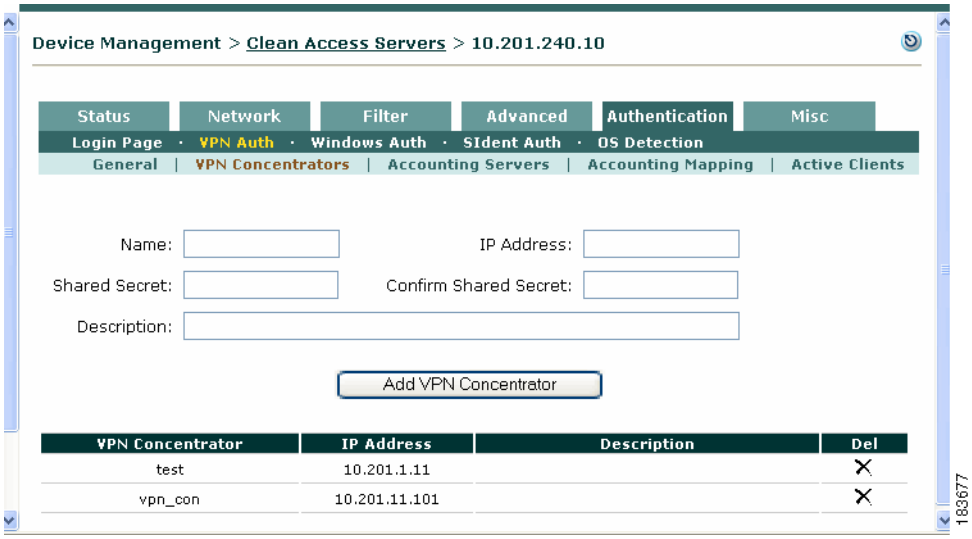
1. **Device Management > Clean Access > Clean Access Agent > Distribution** の順番に進みます。
2. **Discovery Host** フィールドの IP アドレスが、CAM の IP アドレス（デフォルト）、または CAS を経由してトラフィックをルーティング / 転送する必要がある信頼できるネットワーク IP アドレスであることを確認します。
3. **Discovery Host** を変更した場合は、**Update** ボタンをクリックします。

詳細については、「CAA の VPN/L3 アクセス」（p.5-14）、および『*Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide, Release 4.1(1)*』の「Configuring Agent Distribution/Installation」を参照してください。

CAS への VPN コンセントレータの追加

1. **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Authentication > VPN Auth > VPN Concentrators** の順番に進みます。

図 8-5　VPN コンセントレータを追加します。



2. **Name** に、コンセントレータの名前を入力します。
3. **IP Address** に、コンセントレータのプライベート IP アドレスを入力します。
4. **Shared Secret** に、CAS と VPN コンセントレータ間の共有秘密を入力します。コンセントレータ自体にも、同じ秘密を設定する必要があります。
5. **Confirm Shared Secret** フィールドに秘密を再入力します。
6. （任意）**Description** に説明を入力します。
7. **Add VPN Concentrator** をクリックします。

CAS を VPN コンセントレータの RADIUS アカウンティング サーバに設定

CAS を VPN コンセントレータの RADIUS アカウンティング サーバに設定します（たとえば、VPN 3000 シリーズでは、Configuration > System > Servers > Accounting で実行します）。あとで CAS に転送するために、各アカウンティング サーバの設定を記録することを推奨します。CAS は VPN コンセントレータの唯一のアカウンティング サーバでなければなりません。VPN コンセントレータには CAS の信頼できる側の IP アドレス、および CAS と同じ共有秘密を持つように設定する必要があります。

詳細については、次のような該当する製品マニュアルを参照してください。

http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/tsd_products_support_series_home.html

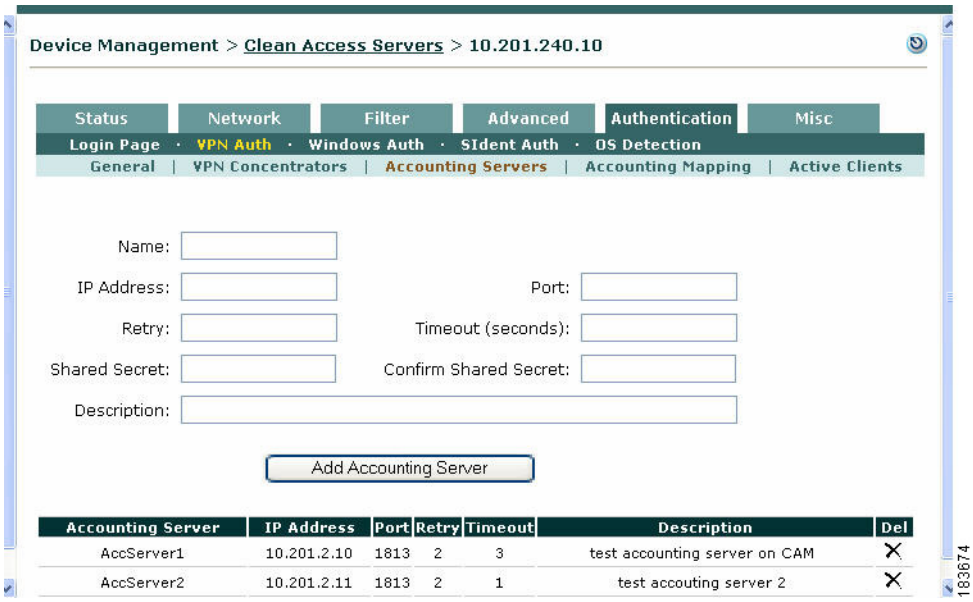
http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html

CAS へのアカウンティング サーバの追加

VPN コンセントレータがアカウンティング サーバと連携するように設定されている場合、アカウンティング サーバの情報を CAS に転送する必要があります。CAS は代わりにこれらのアソシエーションを保持します。

1. **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Authentication > VPN Auth > Accounting Servers** の順番に進みます。

図 8-6　アカウンティング サーバの追加



2. **Name** に、アカウンティング サーバの名前を入力します。
3. **IP Address** に、アカウンティング サーバの IP アドレスを入力します。
4. **Port** に、アカウンティング サーバのポートを入力します（通常は 1813）。
5. **Retry** に、アカウンティング サーバの再試行回数を入力します。これにより、指定した Timeout 内に応答がない場合に、要求を再試行する回数が指定されます。たとえば、Retry が 2 で、Timeout が 3（秒）の場合、CAS がリスト内の次のアカウンティング サーバに要求を送信するまでに 6 秒かかります。

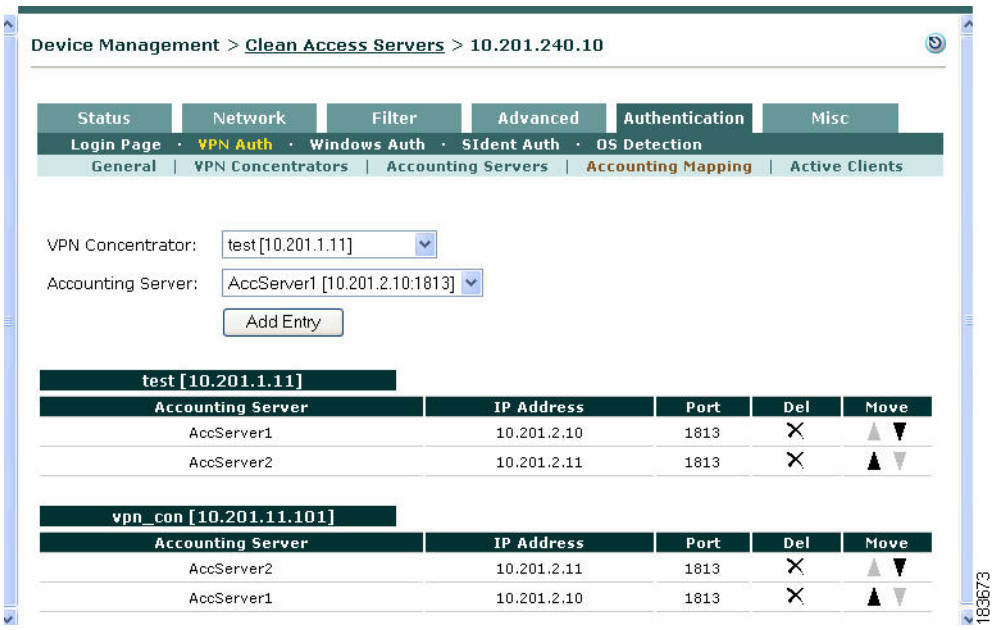
6. **Timeout** に、アカウンティング サーバのタイムアウトを入力します（秒単位）。これにより、応答がない場合に、アカウンティング サーバに要求を再試行するまでの CAS の待機時間が指定されます。
7. **Shared Secret** に、CAS と アカウンティング サーバ間の共有秘密を入力します。VPN コンセントレータから設定を転送したり、新しい秘密を作成したりできますが、アカウンティング サーバ自体に同じ秘密を設定する必要があります。
8. **Confirm Shared Secret** フィールドに秘密を再入力します。
9. （任意）**Description** に説明を入力します。
10. **Add Accounting Server** をクリックします。

VPN コンセントレータとアカウンティング サーバのマッピング

複数の VPN コンセントレータと複数のアカウンティング サーバを管理する場合は、VPN コンセントレータと一連のアカウンティング サーバを対応付けるマッピングを作成できます。このようにすると、CAS はアカウンティング サーバに到達できない場合に、リスト内の次のサーバに処理を継続できます。

1. **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Authentication > VPN Auth > Accounting Mapping** の順番に進みます。

図 8-7　Accounting Mapping



2. ドロップダウン メニューで **VPN Concentrator** を選択します。CAS に追加されたすべての VPN コンセントレータが表示されます。
3. ドロップダウン メニューで **Accounting Server** を選択します。CAS に設定されたすべてのアカウンティング サーバが表示されます。
4. **Add Entry** ボタンをクリックして、マッピングを追加します。下のリストに、名前、IP アドレス、およびポートを基準として各 VPN コンセントレータに対応付けられたアカウンティング サーバがすべて表示されます。

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

一般に、CAS はクライアントと同じサブネット上にないため、クライアントがシステムにログインしたときに、CAS はクライアントの IP アドレスに関する MAC 情報を取得しません。ユーザと CAS（すべての Server Type）間に VPN コンセントレータがある場合、VPN コンセントレータはクライアント IP アドレスに対してプロキシ ARP を実行するため、CAS は新しい各クライアント IP アドレスとともに、VPN コンセントレータの MAC アドレスを認識します。VPN コンセントレータがフローティング デバイスとして設定されていない場合は、Clean Access に最初のユーザ ログインを実行するだけで、Clean Access 要件を満たすことができます。したがって、管理者は **Device Management > Clean Access > Certified Devices > Add Floating Device** を実行して、ルータ /VPN コンセントレータの MAC アドレスを Floating Device リストに追加する必要があります（エントリ例：00:16:21:11:4D:67 1 vpn_concentrator）。詳細については、『*Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide, Release 4.1(1)*』の「Add Floating Devices」を参照してください。

CAS/CAM の SSO の設定

SSO を使用すると、ユーザは VPN クライアントを介して 1 回ログインするだけで、Clean Access プロセスに進むことができます。SSO を実行するために、Cisco NAC アプライアンスは VPN コンセントレータ / 無線コントローラから RADIUS アカウンティング情報を取得してユーザ認証を行い、この情報を使用してユーザをユーザ ロールに対応付けます。これにより、ユーザは CAS にログインしなくても、Clean Access プロセスに直接進むことができます。SSO は、次のように CAS と CAM の両方に設定されます。

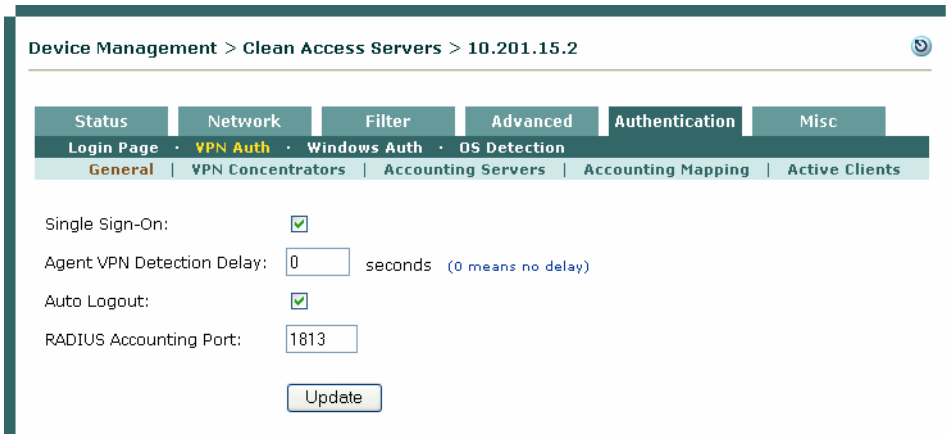
RADIUS アカウンティング パケットから必要とされる最も重要な属性は、User_name、Framed_IP_address、Calling_Station_ID です。ユーザが CAS で SSO に条件付けされるには、Framed_IP_address または Calling_Station_ID 属性（クライアントの IP アドレスのために送信）が RADIUS アカウンティング メッセージに記述されていなければなりません。

（注）　SSO のための RADIUS アカウンティング サポートには、Cisco Airespace Wireless LAN コントローラが含まれています。Cisco NAC アプライアンスと SSO を連携させるには、Cisco Airespace Wireless LAN コントローラから Calling_Station_IP 属性をクライアントの IP アドレスとして送信する必要があります（逆に、Framed_IP_address 属性は VPN コンセントレータで使用されます）。

CAS での SSO の設定

ステップ 1　**Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Authentication > VPN Auth > General** の順番に進みます。

図 8-8　一般的な設定（SSO/Logout/RADIUS Accounting Port）



ステップ 2　**Single Sign-On** のチェックボックスをクリックして、CAS で VPN SSO をイネーブルにします。

ステップ 3　**Agent VPN Detection Delay** 値の時間（秒単位）を入力します。この値は、CAS がリモート ユーザに認証ダイアログで SWISS UDP 検出パケットを送信するように指示するまでの待機時間を指定します。

このオプションでは、すでに提供しているログイン クレデンシャルについて指示する前に、VPN 経由で接続されているユーザの更新情報を CAS が受信する時間が確保されます。指定の待機時間内に CAS が接続状態を学習した場合、自動的に VPN SSO 機能に引き渡されます。VPN 経由でのユーザ接続が行われていないという通知のないまま指定の待機時間が経過した場合、CAS によりログイン クレデンシャルを入力するよう求められます。

（注）「0」を入力すると、ユーザのアクティブな VPN 接続に関する CAM からの応答は待機せず、SWISS UDP 検出パケットを受信するとログイン クレデンシャルを入力するよう求められます。

ステップ 4　ログアウト時に Clean Access ユーザの VPN セッションを自動的に終了するには、**Auto-Logout** のチェックボックスをクリックします。

ステップ 5　デフォルト ポート（1813）のままにするか、あるいは **RADIUS Accounting Port** 用の新しいポートを設定します。

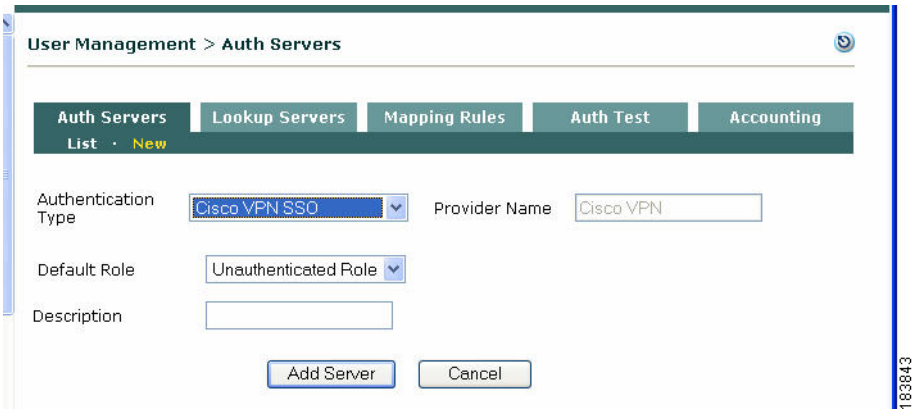
ステップ 6　**Update** をクリックします。

CAM での SSO の設定

Cisco NAC アプライアンス VPN コンセントレータとの統合を設定する場合に SSO をサポートするには、Cisco VPN SSO の認証元を CAM に追加する必要があります。

1. **User Management > Auth Servers > New** の順番に進みます。

図 8-9　新しい認証サーバの追加（CAM）



2. **Authentication Type** ドロップダウン メニューで、**Cisco VPN SSO** を選択します。
3. **Provider Name** はデフォルトで **Cisco VPN** に設定されています。
4. **Default Role** ドロップダウン メニューで、Clean Access プロセスのために VPN クライアント ユーザに割り当てるユーザ ロールを選択します。
5. オプションの **Description** に、認証サーバ リスト内で VPN コンセントレータを識別する説明を入力します。
6. **Add Server** をクリックします。

User Management > Auth Servers > List of Servers に新しい Cisco VPN SSO 認証サーバが表示されます。

- 設定値を変更する場合は、その認証サーバの横にある **Edit** ボタンをクリックします。
- 認証サーバの横にある **Mapping** ボタンをクリックして、Cisco VPN SSO に対する RADIUS 属性ベース マッピング規則を設定します。

詳細については、『*Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide, Release 4.1(1)*』を参照してください。

（任意）認証サーバ マッピング規則の作成

Cisco VPN SSO タイプの場合、VPN コンセントレータから渡される RADIUS 認証サーバ属性に基づくマッピング規則を作成し、ユーザをロールにマッピングできます。次の RADIUS 属性を使用すると、Cisco VPN SSO マッピング規則を設定できます。

- Class
- Framed_IP_Address
- NAS_IP_Address
- NAS_Port
- NAS_Port_Type

- User_Name
- Tunnel_Client_Endpoint
- Service_Type
- Framed_Protocol
- Acct_Authentic

マッピング規則は CAM Web 管理コンソールで設定します（**User Management > Auth Servers > Mapping Rules**）。設定の詳細については、『*Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide, Release 4.1(1)*』の「User Management: Configuring Auth Servers」を参照してください。

CAA および VPN コンセントレータと SSO

CAA はマルチホップ L3 配置、および Agent からの VPN/L3 アクセスをサポートします。Agent は以下の処理を実行します。

1. クライアント ネットワーク上で CAS（L2 配置）を検索します。検索されない場合は、次の処理を実行します。
2. CAM に検出パケットを送信して、CAS を検出しようとします。これにより、CAS が複数ホップ分離れている場合（マルチホップ配置）でも、検出パケットは CAS を通過するため、CAS はこれらのパケットを代行受信して、Agent に応答します。

クライアントが L3 ホップに関して 1 つまたは複数ホップ以上離れている場合に CAS を検出するには、最初にクライアントが CAS から Agent をダウンロードする必要があります。次の 2 つの方法でダウンロードできます。

- Download Clean Access Agent Web ページ（Web ログインを使用）
- 4.1.1.00 以上の Agent へのクライアント自動アップグレード。このためには、クライアントに 3.5.1 以上の Agent がすでにインストールされていなければなりません。

いずれの方法でも、Agent は CAM の IP アドレスを取得して、トラフィックを L3 ネットワーク経由で CAM/CAS に送信することができます。この方法でインストールされた Agent は、L3/VPN コンセントレータ配置でも、正規の L2 配置でも使用できます。詳細については、「L3 サポートのイネーブル化」（p.5-13）を参照してください。

（注）　VPN コンセントレータ SSO 配置の場合に、Agent を CAS からダウンロードせずにほかの方法でダウンロードすると、Agent は CAM の実行時 IP 情報を取得できないため、ポップアップが自動表示されず、クライアントがスキャンされません。

以下の点に注意してください。

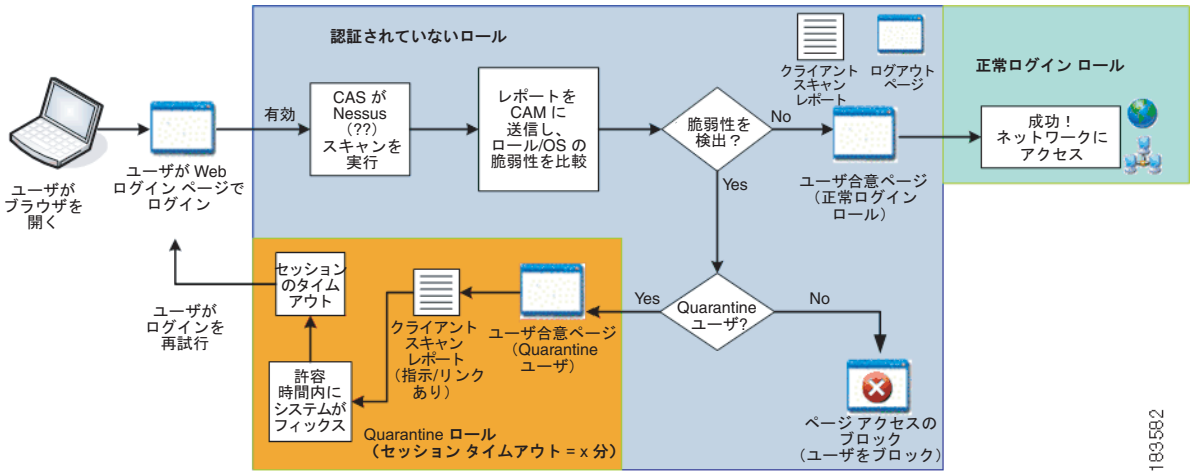
- VPN 接続上にとどまっている間に Agent をアンインストールしても、接続は終了しません。
- 3.5.0 以前のバージョンの Agent がすでにインストールされている場合、または Agent が CAS 以外の方法でインストールされている場合は、Web ログインを実行して CAS から直接最新の Agent セットアップ ファイルをダウンロードし、Agent を再インストールして、L3 機能を取得する必要があります。

CAA L3 VPN コンセントレータのユーザ操作

1. VPN クライアントで、Cisco NAC アプライアンス用に設定された VPN コンセントレータの VPN 接続エントリをダブルクリックします。
2. VPN Client | User Authentication ダイアログにユーザとしてログインします。
3. ログインしたらブラウザを開いて、イントラネットまたはエクストラネット サイトの順番に進みます。

図 8-10 に、CAA および SSO を使用している VPN ユーザに関する Clean Access プロセスを示します。VPN 接続を介して、CAA の初期ダウンロードを実行する必要があります。

図 8-10　SSO を使用する VPN ユーザの場合の CAA



SSO を使用した場合、CAA は自動ログインとスキャンを実行します（図 8-11 と図 8-12 を参照）。

図 8-11　Agent 自動ログイン（SSO）

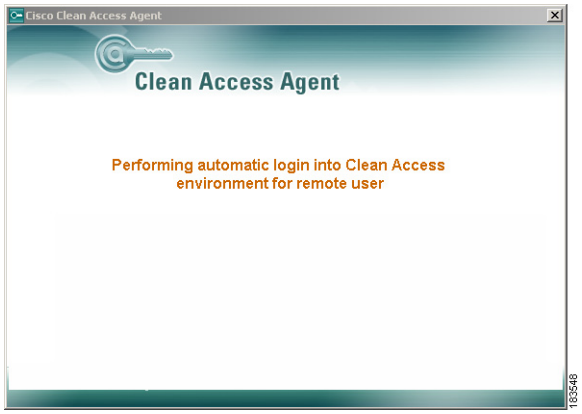
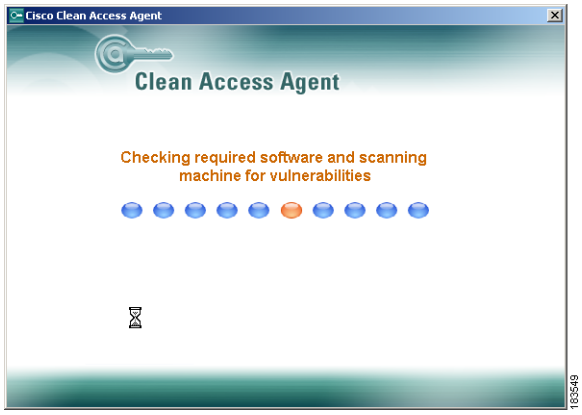
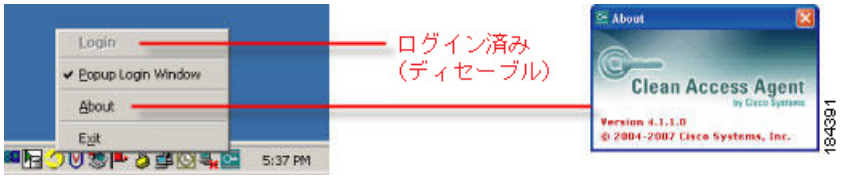


図 8-12　CAA のスキャン



タスクバー メニューの「Login」オプションは Agent に対してディセーブルです（図 8-13）。

図 8-13　システムトレイ アイコンおよびログイン ステータス



（注）　Web ログインは常に L2 または L3 モードで機能します。L3 機能はディセーブルにできません。

Active VPN Clients の表示

Active VPN Clients ページには、VPN SSO によって CAS に通知された IP アドレスが一覧表示されます。このページはトラブルシューティング用のもので、CAS 管理ページと CAS ダイレクト アクセス コンソールの両方で利用できます。Active VPN Clients ページに表示されるのは、CAS が有効な RADIUS アカウンティング START パケットを受信したユーザのリストです。

CAS は、特定のクライアント マシンの有効な RADIUS アカウンティング START パケットを受信すると、これを Active VPN Clients のリストに追加します。

- クライアントがこのリストに表示されている場合、そのクライアントは SSO を実行できます。
- クライアントがこのリストに表示されていない場合、START パケットが CAS に到達していないか、形式が間違っていることが考えられます。

パケットのフォーマットとして重要な項目には、次のものがあります。

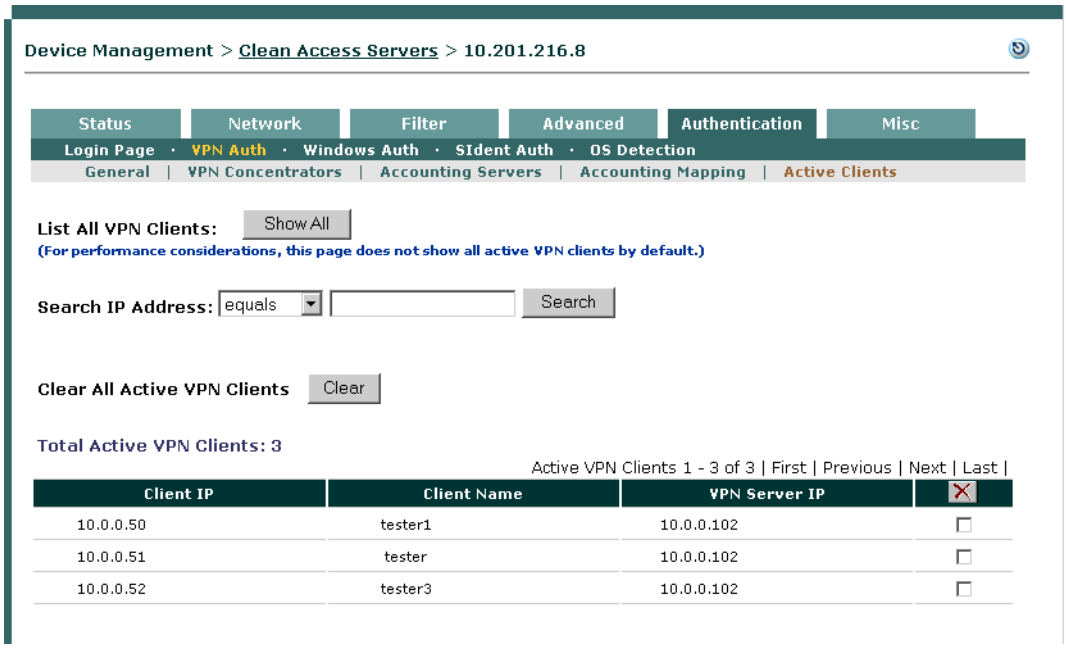
- Account-Status-type = 1（START パケットであることを示す）
- Calling-station-Id（エンド マシンの IP アドレスを示す）

ユーザがブラウズや CAA の実行を試みる場合、CAM/CAS は Active VPN Client の情報とマッピング規則を比較し、ユーザに割り当てるロールを決定します。

Active VPN Clients の表示

1. **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Authentication > VPN Auth > Active Clients** の順番に進みます。

図 8-14　Active Clients（VPN コンセントレータ）



2. **List All VPN Clients** の **Show All** をクリックしてすべて VPN クライアントを一覧表示するか、または **Search** を実行します。次のいずれかを実行するまでは、Active Clients ページは空白のままです。
   a. システム SSO テーブルのすべてのカレント IP/ ユーザ情報を表示するため、**Show All** をクリックします。

b. または、結果を表示するため、**Search IP Address** テキスト フィールドに IP アドレスを入力し、ドロップダウン メニューから演算子（**equals**、**starts with**、**ends with**、**contains**）を選択し、**Search** ボタンをクリックします。

3. ページ下部の表に、次の情報が読み込まれます。エントリは、クライアントの IP アドレス順にソートされます。
   - **Total Active VPN Clients** — SSO テーブル内で現在アクティブとなっている VPN クライアントの数を表示します。
   - **Client IP** — RADIUS アカウンティング パケットから受信したクライアント IP アドレス。
   - **Client Name** — RADIUS アカウンティング パケットから受信したクライアント名。
   - **VPN Server IP** — SSO に使用される Cisco VPN SSO 認証サーバの IP アドレス。

（注）　**Show All** をクリックするか、新しい検索を実行すると、ページが最新の SSO テーブルの情報に更新されます。

4. Active Client ページのエントリを削除するには、次のいずれかを実行します。
   a. **Clear All Active VPN Clients** の **Clear** ボタンをクリックしてすべて SSO テーブルのすべてのエントリを削除します。たとえば、VPN サーバのクラッシュにより VPN ユーザのセッションが終了した場合、CAS に RADIUS アカウンティング停止メッセージは送信されず、このユーザは、手動で削除するまでシステム SSO テーブルに残ります。Active VPN Clients ページのすべてのエントリを削除すると、新しい SSO テーブルでシステムが再起動されます。
   b. 個々のエントリのチェックボックスをクリックし、列の最上部にある **Delete** ボタンをクリックして、そのエントリを SSO テーブルから削除します。

（注）　**Clear** ボタンまたは **Delete** ボタンをクリックした場合、システムの現在の SSO クライアント テーブルからユーザが削除されるだけで、Online Users リストからは削除されません。

ヒント　アクティブな VPN クライアントは、CAS のダイレクト コンソール（https://<CAS_IP>/admin）で **Monitoring > Active VPN Clients** ページ（図 8-15）の順番に進み表示することもできます。

図 8-15　CAS ダイレクト アクセス コンソール — Active VPN Clients のモニタリング