CHAPTER 13

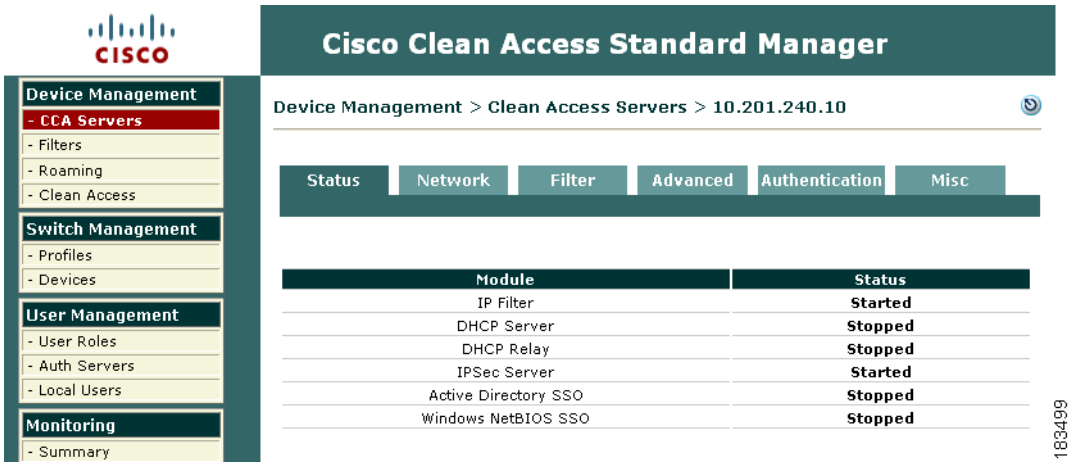
# CAS の管理

この章では、Clean Access Server（CAS）の管理について説明します。この章の内容は、次のとおりです。

# Status タブ

CAS 管理ページの **Status** タブには、CAS で稼働中のモジュールに関する高度なステータス情報が表示されます。

**図 13-1　CAS 管理ページの Status タブ**




- **IP Filter** — パケットを分析して、パケットが有効な認証済みユーザから送信されたことを保証する IP パケット フィルタ
- **DHCP Server** — CAS の内部 Dynamic Host Configuration Protocol（DHCP）サーバ
- **DHCP Relay** — クライアントと外部 DHCP サーバ間でアドレス要求および割り当てをリレーするモジュール
- **IPSec Server** — CAS とクライアント デバイス間でセキュアな、IP セキュリティベースのチャネルを確立するためのモジュール。モジュールは、クライアントとサーバ間で送受信されるデータの暗号化および暗号解除を実行します。
- **Active Directory SSO** — Active Directory Single Sign-On（SSO; シングル サインオン）をイネーブルにするモジュール。
- **Windows NetBIOS SSO** — 認証された Windows ユーザの Windows NetBIOS ログインをイネーブルにするモジュール。

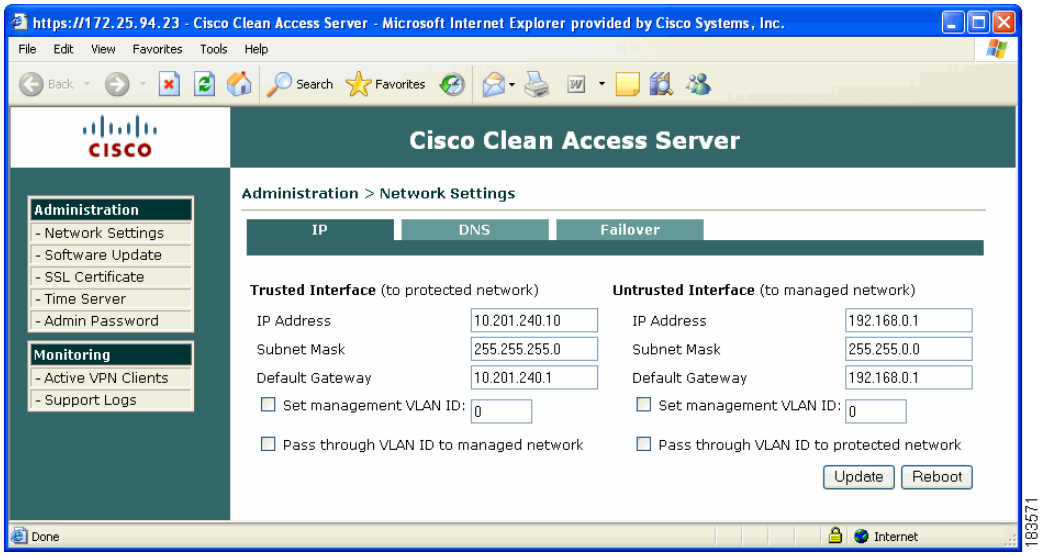
# CAS ダイレクト アクセス Web コンソール

CAM Web 管理コンソール（図 13-1）の CAS 管理ページは、CAS を設定する場合の主要インターフェイスです。ただし、CAS にはそれぞれ独自の Web 管理コンソールがあり、CAS の特定の管理およびモニタリング設定値を直接設定できます（図 13-2）。CAS ダイレクト アクセス Web コンソールは主に、CAS サポート ログをダウンロードする、または CAS ペアにハイ アベイラビリティを設定する場合に使用します。詳細は、第 14 章「ハイ アベイラビリティ（HA）の設定」を参照してください。CAS 管理ページを使用できない場合は、ダイレクト コンソール インターフェイスを使用して、CAS の SSL 証明書の管理や、システム アップグレードなどの他の機能を実行することもできます。

CAS のダイレクト アクセス Web 管理コンソールにアクセスする手順は、次のとおりです。

1. Web ブラウザを開き、URL/ アドレス フィールドに CAS の信頼できる（eth0）インターフェイスの IP アドレスを **https://<CAS_eth0_IP>/admin** の形式で入力します（例：`https://172.16.1.2/admin`）。
2. 一時証明書を受け入れて、ユーザ `admin`（デフォルト パスワードは `cisco123`）としてログインします。

**図 13-2　CAS ダイレクト アクセス Web 管理コンソール**




（注）

- CAS IP アドレスの先頭に「https://」を、末尾に「/admin」を付加してください。そうしないと、Web ログイン ユーザ用のリダイレクト ページが表示されます。
- セキュリティのために、CAS Web コンソールのデフォルト パスワードを変更することを推奨します。

CAS Web コンソールのほとんどすべての設定は、CAM Web 管理コンソールの CAS 管理ページで設定できます。例外は、**Failover**、**DHCP Failover**、**Admin Password**、および **Support Logs** です。CAS ダイレクト アクセス Web コンソールには、ローカル CAS 用の次の管理ページがあります。

- Network Settings（IP、DNS、Failover、DHCP Failover）
- Software Update

- SSL Certificates（Generate Temporary Certificate、Import Certificate、Export CSR/Private Key/Certificate）
- Time Server
- Admin Password

CAS ダイレクト アクセス コンソールの **Monitoring** モジュールには次のページがあります。

- Active VPN Clients
- Support Logs

（注）　ハイ アベイラビリティ CAS ペアの場合、CAS 管理ページまたは CAS ダイレクト アクセス Web コンソールによって HA プライマリ CAS で実行された CAS ネットワークの設定変更もまた、スタンバイ CAS ユニットでダイレクト アクセス Web コンソールによって繰り返す必要があります。これらの設定には、SSL 証明書、システム時刻、タイム ゾーン、DNS、またはサービス IP の更新が含まれます。詳細については、「IP フォーム」（p.5-9）および「ハイ アベイラビリティ設定の変更」（p.14-26）を参照してください。

# CAS SSL 証明書の管理

Cisco NAC アプライアンスの各要素は、Secure Socket Layer（SSL）接続を介してセキュアに通信します。Cisco NAC アプライアンスは SSL 接続を次の場合に使用します。

- Clean Access Manager（CAM）と CAS 間の接続
- CAM と、CAM Web 管理コンソールにアクセスしているブラウザ間の接続
- CAS と、CAS に接続しているエンドユーザ間の接続
- CAS と、CAS ダイレクト アクセス Web コンソールにアクセスしているブラウザ間の接続

インストール中に、CAM と CAS の両方の設定ユーティリティ スクリプトから、インストール中のサーバの一時 SSL 証明書を生成するように要求されます。対応する秘密鍵も、一時証明書を使用して生成されます。

運用配置の場合は、通常、**CAS** の一時証明書を Certificate Authority（CA）署名付き SSL 証明書で置き換える必要があります。CAS 証明書はエンド ユーザが参照できるためです。運用配置でない場合、CAS に一時証明書があれば、ネットワークにアクセスするユーザはログインするたびに、CAS からこの証明書を明示的に受け入れる必要があります。

（注）　システム ソフトウェアの Java バージョンの依存性により、Cisco Clean Access のみが SSL 証明書の 1024 ビットおよび 2048 ビットのキー長をサポートします。

CAM では、CA 署名付き証明書を使用する必要はありません。必要に応じて、一時証明書を引き続き使用できます。CAM の SSL 証明書の管理方法については、『*Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide, Release 4.1(1)*』を参照してください。

ここでは、CAS の SSL 証明書の管理方法について説明します。

- 一時証明書の生成（p.13-7）
- CSR/ 秘密鍵 / 証明書のエクスポート（p.13-9）
- 現在インストールされている秘密鍵および証明書の確認（p.13-10）
- 署名付き証明書のインポート（p.13-13）
- インポートのためにアップロードされた証明書ファイルの表示（p.13-15）
- 証明書に関する問題のトラブルシューティング（p.13-15）

（注）　CAM 用に購入された CA 署名付き証明書は、CAS では使用できません。CAS ごとに個別の証明書を購入する必要があります。

### SSL 証明書管理のための Web コンソール ページ

実際は、CAM SSL 証明書ファイルは CAM マシンに保持され、CAS SSL 証明書 ファイルは CAS マシンに保持されます。インストール後、CAM および CAS 証明書はそれぞれ次の Web コンソール ページから管理できます。

**CAM 証明書：**

- **Administration > CCA Manager > SSL Certificate**

**CAS 証明書：**

- CAS 管理ページ：**Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs**
- CAS ダイレクト アクセス コンソール：**Administration > SSL Certificate**

**（注）** CAS 管理ページが使用できない場合は、CAS ダイレクト アクセス コンソール インターフェイスを使用できます。詳細については、「CAS ダイレクト アクセス Web コンソール」（p.13-3）を参照してください。

CAS 管理ページおよび CAS ダイレクト アクセス コントロールには同じコントロールが配置されていて、次の SSL 証明書関連の操作を実行できます。

- 一時証明書（および対応する秘密鍵）の生成
- 現在の一時証明書に基づく PEM エンコード PKCS #10 Certificate Signing Request（CSR; 証明書署名要求）の生成
- 秘密鍵のインポートとエクスポート。エクスポート キー機能は、CSR のベースとなる秘密鍵のバックアップ コピーを保存する場合に使用します。CA 署名付き証明書が CA から戻されて、CAS にインポートされる場合は、この秘密鍵を併用する必要があります。

**（注）** ハイ アベイラビリティ CAS ペアの場合、CAS 管理ページまたは CAS ダイレクト アクセス Web コンソールによって HA プライマリ CAS で実行された CAS ネットワークの設定変更もまた、スタンバイ CAS ユニットでダイレクト アクセス Web コンソールによって繰り返す必要があります。これらの設定には、SSL 証明書、システム時刻、タイム ゾーン、DNS、またはサービス IP の更新が含まれます。詳細については、「CAS ダイレクト アクセス Web コンソール」（p.13-3）および「ハイ アベイラビリティ設定の変更」（p.14-26）を参照してください。

## CAS の新規インストールの一般的な手順

新規インストールの場合に CAS 証明書を管理する一般的な手順は、次のとおりです。

1. 時刻を同期します。

   CAM および CAS をインストールしたら、CAM および CAS の時刻を同期し、そのあとで CSR のベースとなる一時証明書を再生成します。詳細については、次の「システム時刻の同期」（p.13-18）を参照してください。

2. CAS の DNS 設定を確認します。

   CA 署名付き証明書にサーバの IP アドレスでなく DNS 名を使用する場合は、CAS 設定を検証し、一時証明書を再生成する必要があります。詳細は、「IP でなく DNS 名に対応した証明書が再生成される」（p.13-17）を参照してください。

3. 一時証明書の生成（p.13-7）

   一時証明書および秘密鍵は、CAS インストール中に自動的に生成されます。CAS の時刻または DNS 設定を変更する場合は、一時証明書および秘密鍵を再生成してから、CSR を作成します。

4. 保護またはバックアップのために、秘密鍵をローカル マシンにエクスポート（バックアップ）します。

   CSR を生成およびエクスポートする**前に**、必ず、現在の一時証明書に対応する秘密鍵をローカル ハード ドライブにバックアップして保護することを推奨します。See CSR/ 秘密鍵 / 証明書のエクスポート（p.13-9）

5. CSR をローカル マシンにエクスポート（保存）します。
   「CSR/ 秘密鍵 / 証明書のエクスポート」（p.13-9）を参照してください。

6. CSR ファイルを、信頼できる証明書の発行が許可された CA に送信します。
7. CA が署名し、証明書を戻したら、CA 署名付き証明書をサーバにインポートします。

   CA 署名付き証明書を CA から受信したら、PEM エンコード ファイルとして CAS 一時ストアにアップロードします。「署名付き証明書のインポート」（p.13-13）を参照してください。
8. 必要に応じて、必要な中間 CA 証明書をすべて、単一の PEM エンコード ファイルとして CAS 一時ストアにアップロードします。
9. **Verify and Install Uploaded Certificates** をクリックして、一時ストア内の証明書チェーンおよび秘密鍵全体を検証し、検証済み証明書を CAS にインストールします。
10. CAS にアクセスするクライアントとしてテストします。

（注）　インポートしている CA 署名付き証明書が CSR を生成した証明書であること、およびそれ以降別の一時証明書を生成していないことを確認します。新しい一時証明書を生成すると、新しい秘密 / 公開鍵の組み合わせが作成されます。また、（保護のため、および秘密鍵を使いやすくするために）署名用の CSR を生成する場合は、必ず秘密鍵を安全な場所にエクスポートし、保管してください。

詳細については、「証明書に関する問題のトラブルシューティング」（p.13-15）も参照してください。

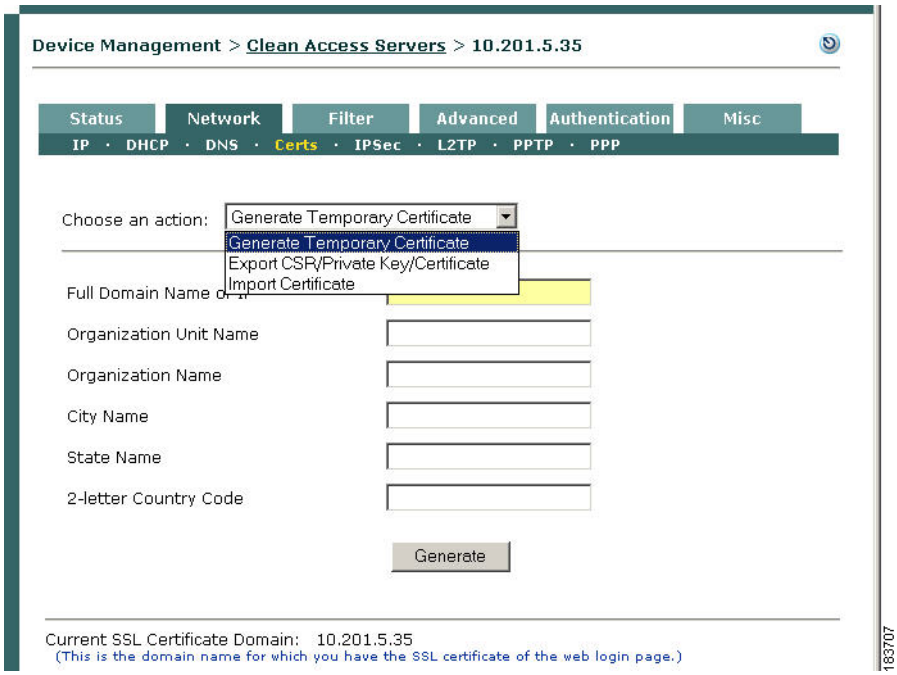
## 一時証明書の生成

次に、CAS の新しい一時証明書の生成手順を示します。CAS に一時証明書があれば、ネットワークにアクセスするユーザはログインするたびに、CAS からこの証明書を明示的に受け入れる必要があります。一時証明書を生成すると、CA への送信に適した CSR を生成できます。詳細については、「IP でなく DNS 名に対応した証明書が再生成される」（p.13-17）を参照してください。

**証明書を生成する手順は、次のとおりです。**

1. **Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs** の順番に進みます。
2. **Choose an action** ドロップダウン メニューで、**Generate Temporary Certificate** をまだ選択していなければ、選択します。

**図 13-3　Certs — Generate Temporary Certificate**




3. フォームのフィールドに適切な値を入力します。
   - **Full Domain Name or IP** — 証明書を適用する CAS の完全修飾ドメイン名または IP アドレス。次の例を参考にしてください。`caserver.<your_domain_name>`
   - **Organization Unit Name** — 企業内の単位名（適用可能な場合）
   - **Organization Name** — 企業の正式名称
   - **City Name** — 企業の正式な所在都市
   - **State Name** — 企業の正式な所在国（フルネーム）
   - **2-letter Country Code** — 2 文字の ISO フォーマット国別コード（英国は GB、米国は US など）
4. 終了したら、**Generate** をクリックします。これで、新しい一時証明書および新しい秘密鍵が生成されます。

（注）　各フォームの下部にある **Current SSL Certificate Domain: <IP or domain name>** フィールドには、表示された Web コンソール ページにアクセスするために使用されている、現在の SSL 証明書の IP アドレスまたはドメイン名が表示されます。たとえば、CAS の SSL 証明書管理ページにアクセスしている場合は、該当する CAS の SSL 証明書に記載されたドメイン名または IP アドレスが表示されます。CAM の SSL 証明書管理ページにアクセスしている場合は、CAM の SSL 証明書に記載されたドメイン名 /IP が表示されます。

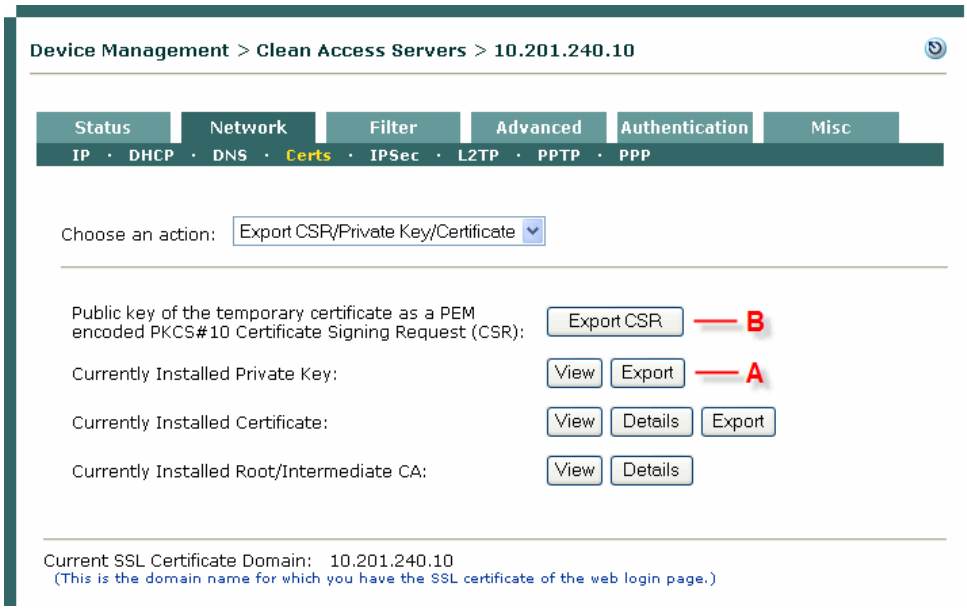
## CSR/ 秘密鍵 / 証明書のエクスポート

CSR をエクスポートすると、CA への送信に適した PEM エンコード PKCS#10 フォーマットの CSR が生成されます。CSR は、キーストア データベースに現在格納されている一時証明書および秘密鍵に基づきます。

**証明書要求を作成する手順は、次のとおりです。**

1. **Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs** の順番に進みます（図 13-4）。
2. **Choose an action** ドロップダウン メニューで、**Export CSR/Private Key/Certificate** を選択します。

**図 13-4　Certs — Export CSR/Private Key/Certificate**




3. Export CSR/Private Key/Certificate フォームの **Currently Installed Private Key**（A）の **Export** ボタンをクリックして、要求の生成に使用する秘密鍵のバックアップを作成します。ファイルを保存するか、または開くように要求されます（「エクスポートしたファイルのファイル名」[p.13-10] を参照）。ファイルは安全な場所に保存します。

（注）　Cisco Clean Access のみが SSL 証明書の 1024 ビットおよび 2048 ビットのキー長をサポートします。

4. **Export CSR**（B）をクリックします。CAS の CSR ファイルが生成され、ダウンロードに使用できるようになります（「エクスポートしたファイルのファイル名」[p.13-10] を参照）。

（注）　この手順では、現在インストールされている（一時）証明書および秘密鍵のペアに基づいて、証明書要求が生成されます。これらが、CA に送信する CSR に対応した証明書および秘密鍵であることを確認してください。

5. **Save** をクリックして、CSR ファイルをハード ドライブに保存します（または、証明書要求フォームに記入する準備ができたら、**Open** をクリックしてテキスト エディタ内ですぐに開きます。CSR ファイルを使用して、CA に対して証明書を要求します。証明書をオーダーすると、CSR ファイルの内容を オーダー フォームの CSR フィールドにコピー アンド ペーストするように要求されることがあります。
6. CA から CA 署名付き証明書を受信したら、CAS にインポートできます（「署名付き証明書のインポート」[p.13-13] を参照）。
CA 署名付き証明書をインポートすると、CA 署名付き証明書が「Currently Installed Certificate」になります。また、あとでこの証明書のバックアップにアクセスする必要がある場合は、**Export** をクリックして、いつでも **Currently Installed Certificate** をエクスポートすることもできます。

（注）　各フォームの下部にある **Current SSL Certificate Domain: <IP or domain name>** フィールドには、表示された Web コンソール ページにアクセスするために使用されている、現在の SSL 証明書の IP アドレスまたはドメイン名が表示されます。たとえば、CAS の SSL 証明書管理ページにアクセスしている場合は、該当する CAS の SSL 証明書に記載されたドメイン名または IP アドレスが表示されます。CAM の SSL 証明書管理ページにアクセスしている場合は、CAM の SSL 証明書に記載されたドメイン名 /IP が表示されます。

### エクスポートしたファイルのファイル名

CAS からエクスポートできる SSL 証明書ファイルのファイル名は、次のとおりです。

| ファイル名[1] | 説明 |
|---|---|
| secsmart_csr.pem | CAS の CSR |
| secsmart_key.pem | CAS の Currently Installed Private Key |
| secsmart_crt.cer [2] | CAS の Currently Installed Certificate |

1. リリース 3.6.0.1 以前のファイル名拡張子は、.pem でなく .csr です。
2. リリース 3.6(1) の場合のみ、ファイル名は secsmart_crt.pem です。

## 現在インストールされている秘密鍵および証明書の確認

次のファイルを検証するには、**Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs | Export CSR/Private Key/Certificate**（図 13-4）でこれらを表示します。

- Currently Installed Private Key
- Currently Installed Certificate
- Currently Installed Certificate Details
- Currently Installed Root/Intermediate CA Certificate
- Currently Installed Root/Intermediate CA Certificate Details

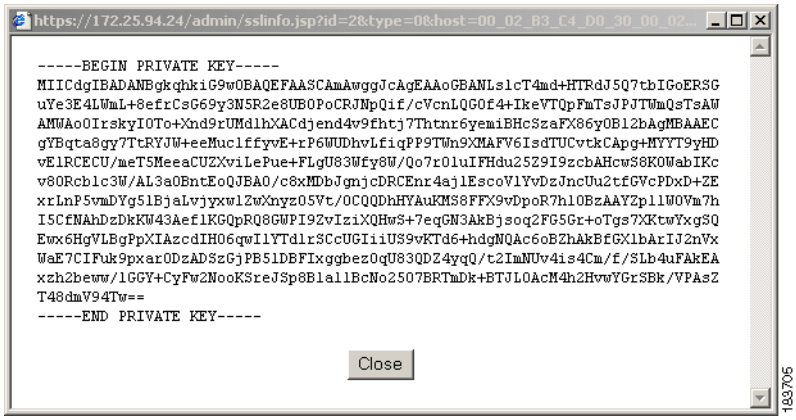
（注）　証明書ファイルを表示するには、Web コンソール セッションに現在ログインしている必要があります。

CAS で特定のファイルが現在インストールされていない場合（エクスポート）、またはアップロードされていない場合（インポート）に、**View** または **Details** ボタンをクリックすると、ダイアログ メッセージ [`Unable to read certificate from Clean Access Server`] が表示されます。たとえば、

CAS に一時証明書のみが存在する場合、Import および Export フォームでそれぞれ「Root/Intermediate CA」または「Currently Installed Root/Intermediate CA」の View/Details ボタンをクリックすると、このメッセージが表示されます。

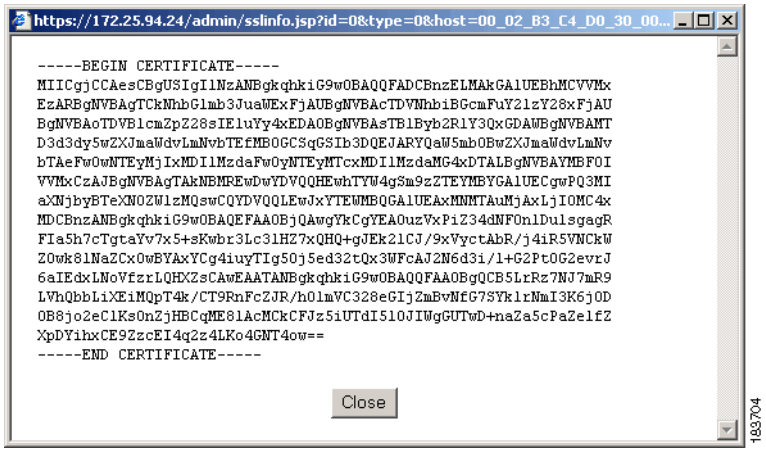
「**Currently Installed Private Key**」の **View** をクリックすると、図 13-5 に示されたダイアログが表示されます（BEGIN PRIVATE KEY/END PRIVATE KEY）。

**図 13-5　Currently Installed Private Key の表示**




「**Currently Installed Certificate**」の **View** をクリックすると、図 13-6 に示されたダイアログが起動します（BEGIN CERTIFICATE / END CERTIFICATE）。

**図 13-6　Currently Installed Certificate の表示**




「**Currently Installed Certificate**」の **Details** をクリックすると、図 13-7 に示されたダイアログが表示されます（「Certificate」）。**Currently Installed Certificate Details** フォームでは、一時証明書または CA 署名付き証明書があるかどうかを簡単に確認できます。確認する必要がある最も重要なフィールドは、次のとおりです。

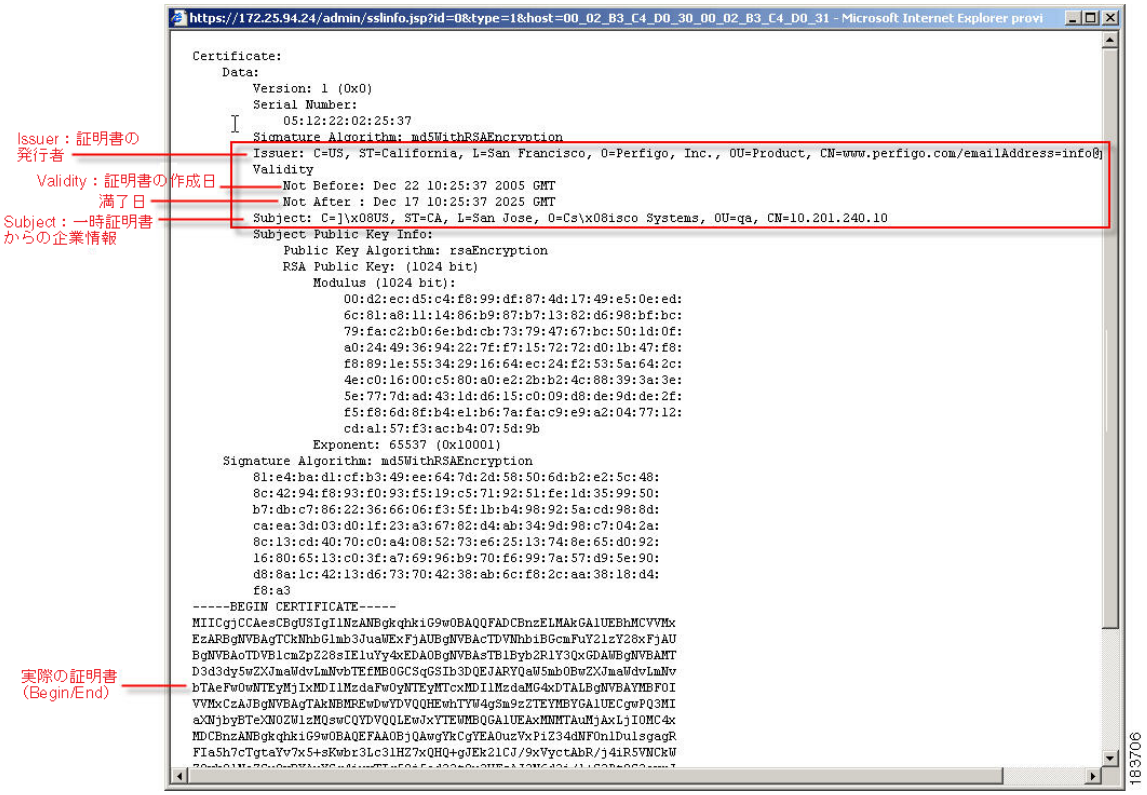
- **Issuer** — 現在の証明書への署名者。インストール中に生成された一時証明書には、Issuer 情報が含まれます（図 13-7 を参照）。

- **Validity** — 証明書の作成日（「Not Before:」）および満了日（「Not After」）

（注）　CAS に設定された時刻は、CAM の SSL 証明書に設定された作成日 / 満了日の範囲に収まっていなければなりません。ユーザ マシンに設定された時刻は、CAS の SSL 証明書に設定された作成日 / 満了日の範囲に収まっていなければなりません。

- **Subject** — 一時証明書を生成したときに入力されたサーバおよび企業情報
- **Begin Certificate/End Certificate** — ここには実際の証明書が表示されます。この証明書は、「Currently Installed Certificate」の **View** をクリックした場合に表示される情報と同じです。

**図 13-7　Currently Installed Certificate Details の表示（一時証明書の例）**




「**Currently Installed Root/Intermediate CA Certificate**」の **View** または **Details** をクリックすると、CAS にインストールしたルートまたは中間証明書に対する同様なダイアログが起動します。

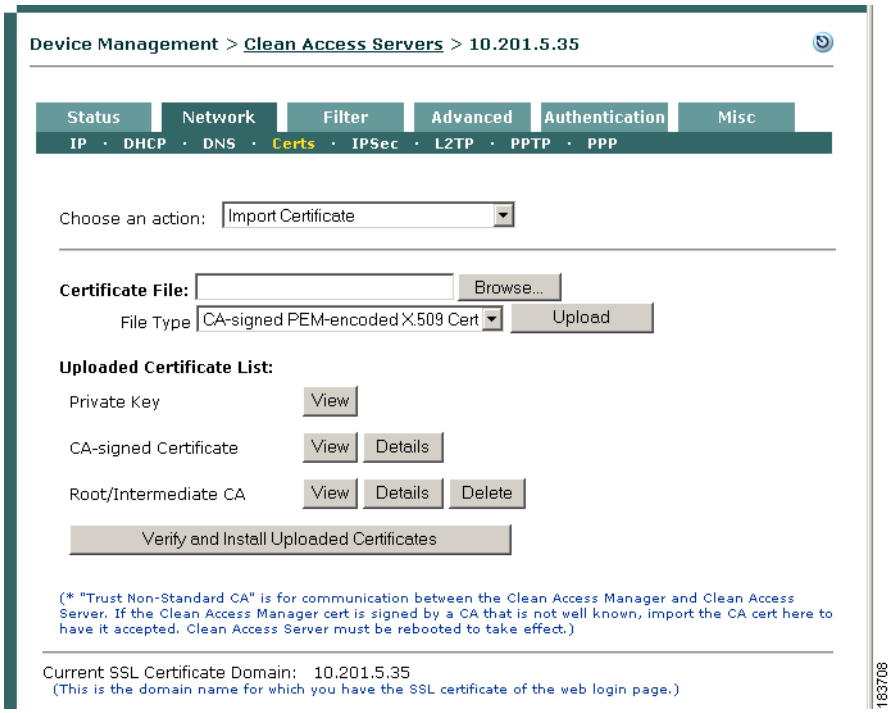
# 署名付き証明書のインポート

CAS の CA 署名付き PEM エンコード X.509 証明書を受信したら、ここの説明に従って、この証明書を CAS にインポートできます。作業を開始する前に、ルートおよび CA 署名付き証明書ファイルがアクセス可能なファイル ディレクトリに格納されているか確認してください。中間 CA が必要な CA を使用している場合は、これらのファイルが存在していて、アクセス可能であることも確認してください。

**CA 署名付き証明書のインポート手順は、次のとおりです。**

1. **Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs** の順番に進みます（図 13-8）。
2. **Choose an action** ドロップ ダウン メニューで、**Import Certificate** を選択します。

**図 13-8　Certs — Import Certificate**




3. **Certificate File** フィールドの横にある **Browse** ボタンをクリックして、ディレクトリ システムの証明書ファイルを特定します。

（注）　ファイルをインポートする場合は、ファイル名にスペースが含まれていないか確認してください（下線は使用できます）。

4. ドロップダウン メニューで、**File Type** を選択します。
   - **CA-signed PEM-encoded X.509 Cert** — PEM エンコード CA 署名付き証明書をアップロードする場合に選択します。

- **Root/Intermediate CA** — PEM エンコード中間 CA 証明書またはルート証明書をアップロードする場合に選択します。チェーン証明書（複数の中間 CA ファイル）をインストールする手順は、次のとおりです。

  **a.** 証明書チェーンが異なるファイル フォーマット（.p7b など）を使用する場合、まずチェーンを PEM フォーマットに変換する必要があります。

  **b.** ルートおよび中間証明書情報を 1 つのファイルにコピー アンド ペーストしてから、中間 CA PEM エンコード ファイルとして CAS にアップロードします。

（注）　CAS にアップロードできる中間 CA ファイルは 1 つのみで、PEM フォーマットでなければなりません。

- **Private Key** — CAS の秘密鍵を（バックアップから）アップロードする必要がある場合に選択します。通常、この処理が必要なのは、現在の秘密鍵が、CA 署名付き証明書のベースとなる元の CSR の作成に使用された秘密鍵と一致しない場合のみです。
- **Trust Non-Standard CA** — CAS で、CAM と 非標準機関によって署名された CAS 間の通信に必要な証明書をアップロードする場合は、このオプションを選択します。たとえば、CAS に対して VeriSign から発行された CA 署名付き証明書以外に、ユーザの所属機関（大学など）によって署名された CAM 用の非標準証明書が存在する場合があります。CAM 証明書が不明な CA によって署名されている場合は、**Trust Non-Standard CA** オプションを使用してこの CA 証明書をインポートし、受け入れます。この証明書を有効にするには、CAS をリブートする必要があります。

5. **Upload** をクリックして、CAS の一時ストアに証明書ファイルをアップロードします。
6. **Verify and Install Uploaded Certificates** をクリックして、一時ストア内の証明書チェーンおよび秘密鍵全体を検証し、検証済み証明書ファイルを CAS 内の正しい場所にインストールします。失われているファイルがある場合は、アップロードする必要があるファイルを示すエラーが表示されます。たとえば、使用している CA で中間 CA 証明書が必要な場合は、この証明書を CAS 一時ストアにアップロードして、証明書チェーンを検証し、CAS にインストールします。

（注）　CAM および CAS は検証できない証明書チェーンをインストールしません。1 つのファイルに複数の証明書を含める場合は、デリミタ（Begin/End Certificate）が必要です。ただし、これらのファイルはインストール前に一時ストア内で検証されるため、特定の順番で証明書ファイルをアップロードする必要はありません。

7. リスト内の既存の CAS のルート / 中間 CA 証明書をアップロードしようとすると、**Verify and Install Uploaded Certificates** ボタンをクリックしたあとに、[this intermediate CA is not necessary] というエラーメッセージが表示されます。重複ファイルを削除するには、**Delete** をクリックして、アップロードされた **Root/Intermediate CA** を削除する必要があります。

（注）　各フォームの下部にある **Current SSL Certificate Domain: <IP or domain name>** フィールドには、表示された Web コンソール ページにアクセスするために使用されている、現在の SSL 証明書の IP アドレスまたはドメイン名が表示されます。たとえば、CAS の SSL 証明書管理ページにアクセスしている場合は、該当する CAS の SSL 証明書に記載されたドメイン名または IP アドレスが表示されます。CAM の SSL 証明書管理ページにアクセスしている場合は、CAM の SSL 証明書に記載されたドメイン名 /IP が表示されます。

## インポートのためにアップロードされた証明書ファイルの表示

次のように CAS にインポートするために一時ストアにアップロードされた証明書ファイルを確認するには、**Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs | Import Certificate**（図 13-4）を使用します。

- Uploaded Private Key
- Uploaded CA-Signed Certificate
- Uploaded CA-Signed Certificate Details
- Uploaded Root/Intermediate CA Certificate
- Uploaded Root/Intermediate CA Certificate Details

（注）　証明書ファイルを表示するには、Web コンソール セッションに現在ログインしている必要があります。

CAS で特定のファイルが現在インストールされていない場合（エクスポート）、またはアップロードされていない場合（インポート）に、**View** または **Details** ボタンをクリックすると、ダイアログ メッセージ [`Unable to read certificate from Clean Access Server`] が表示されます。たとえば、CAS に一時証明書のみが存在する場合、Import および Export フォームでそれぞれ「Root/Intermediate CA」または「Currently Installed Root/Intermediate CA」の View/Details ボタンをクリックすると、このメッセージが表示されます。

## 証明書に関する問題のトラブルシューティング

Cisco NAC アプライアンス証明書の管理中に、証明書チェーン内の SSL 証明書が一致しないなどの問題が発生することがあります。SSL 証明書の一般的な問題は、時間によるもの（CAM および CAS のクロックが同期していない場合、認証に失敗する）、IP によるもの（不正なインターフェイスに対して証明書が作成される）、情報によるもの（不正な、または入力ミスの証明書情報がインポートされる）などです。ここでは、次の内容について説明します。

- CAS が CAM とのセキュアな接続を確立できない
- CAS 内の秘密鍵が CA 署名付き証明書と一致しない
- IP でなく DNS 名に対応した証明書が再生成される
- 証明書関連ファイル

### CAS が CAM とのセキュアな接続を確立できない

ログインを試行したクライアントが [Clean Access Server could not establish a secure connection to the Clean Access Manager at <IPaddress or domain>] というエラー メッセージを受け取った場合（図 13-9 を参照）は、通常、次のいずれかの問題が発生しています。

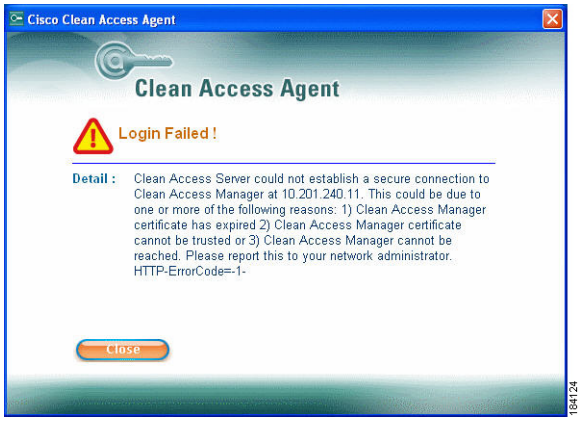
- CAM と CAS 間の時差が 5 分を超えています。
- IP アドレスが無効です。
- ドメイン名が無効です。
- CAM に到達できません。

CAM および CAS に設定された時刻の差は、5 分以内でなければなりません。この問題を解決する手順は、次のとおりです。

1. まず、CAM および CAS の時刻を正しく設定します（「システム時刻の同期」[p.13-18] を参照）。

2. 正しい IP アドレスまたはドメインを使用して、CAS 上で証明書を再生成します。
3. CAS をリブートします。
4. 正しい IP アドレスまたはドメインを使用して、CAM 上で証明書を再生成します。
5. CAM をリブートします。

**図 13-9　トラブルシューティング：「CAS が CAM とのセキュアな接続を確立できない」**




（注）　CAS で **nslookup** および **date** を実行し、CAS の DNS および TIME 設定が正しい場合、CAS の CA 証明書ファイルが破損している可能性があります。この場合は、/usr/java/j2sdk1.4/lib/security/cacerts の既存の CA 証明書をバックアップしてから、/perfigo/common/conf/cacerts のファイルで上書きし、CAS で「service perfigo restart」を実行することを推奨します。

（注）　クライアントのエラー メッセージが [Clean Access Server is not properly configured, please report to your administrator] の場合は、通常、証明書に関する問題ではなく、デフォルト ユーザ ログイン ページが CAM に追加されていません。詳細については、『*Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide, Release 4.1(1)*』の「Add Default Login Page」を参照してください。

## CAS 内の秘密鍵が CA 署名付き証明書と一致しない

この問題は、新しい一時証明書が生成されたにもかかわらず、古い一時証明書および秘密鍵ペアから生成された CSR に対応する CA 署名付き証明書が戻された場合に発生することがあります。

たとえば、管理者は CSR を生成し、秘密鍵をバックアップしてから、CSR を VeriSign などの CA に送信します。

CSR が送信されたあとに、別の管理者が一時証明書を再生成します。CA 署名付き証明書が CA から戻された場合、CA 証明書のベースとなる秘密鍵は、CAS 内の秘密鍵と一致しません。

この問題を解決するには、古い秘密鍵を再インポートしてから、CA 署名付き証明書をインストールします。

## IP でなく DNS 名に対応した証明書が再生成される

サーバの IP アドレスでなく DNS 名に基づいて証明書を再作成する場合は、次のようにします。

- インポートしている CA 署名付き証明書が CSR を生成した証明書であること、およびそれ以降別の一時証明書を生成していないことを確認します。新しい一時証明書を生成すると、新しい秘密 / 公開鍵の組み合わせが作成されます。また、（秘密鍵を使いやすくするために）署名用の CSR を生成する場合は、必ず秘密鍵をエクスポートし、保管してください。
- 特定の CA 署名付き証明書をインポートすると、CA 署名付き証明書への署名に使用されるルート証明書（CA のルート証明書）をインポートする必要があること、または場合によっては中間ルート証明書をインポートしなければならないことを通知する警告が表示されることがあります。
- DNS サーバに DNS エントリがあることを確認します。
- CAS 内の DNS アドレスが正しいことを確認します（「ネットワークの DNS サーバの設定」[p.5-16] を参照）。
- ハイ アベイラビリティ（フェールオーバー）構成の場合、サービス IP の DNS 名を使用します（仮想 DNS）。
- 新しい証明書を生成したり、CA 署名付き証明書をインポートしたら、リブートすることを推奨します。
- 使用している DNS ベース証明書が CA 署名付きでない場合は、証明書を受け入れるように促すプロンプトが表示されます。

## 証明書関連ファイル

表 13-1 に、トラブルシューティング用の、CAS の証明書関連ファイルを示します。たとえば、CA 証明書 / 秘密鍵の組み合わせが一致しないために管理コンソールに到達できない場合、CAS のファイル システム内にあるこれらのファイルを直接変更しなければならないことがあります。

**表 13-1　CAS の証明書関連ファイル**

| ファイル | 説明 |
|---|---|
| /root/.tomcat.key | 秘密鍵 |
| /root/.tomcat.crt | 証明書 |
| /root/.tomcat.csr | CSR |
| /root/.chain.crt | 中間証明書 |
| /perfigo/common/conf/perfigo-ca-bundle.crt | ルート CA バンドル |

# システム時刻の同期

ロギングおよびその他の時間依存タスク（SSL 証明書の生成など）のために、CAM および CAS の時刻は正確に同期する必要があります。**Time** フォームを使用すると、CAS の時刻を設定したり、CAS OS（オペレーティング システム）のタイム ゾーン設定を変更することができます。

CAM および CAS をインストールしたら、CAM および CAS の時刻を同期し、そのあとで CSR のベースとなる一時証明書を再生成する必要があります。このための最も簡単な方法は、タイム サーバと時刻を自動的に同期することです（**Sync Current Time** ボタン）。

（注）　CAS に設定された時刻は、CAM の SSL 証明書に設定された作成日 / 満了日の範囲に収まっていなければなりません。ユーザ マシンに設定された時刻は、CAS の SSL 証明書に設定された作成日 / 満了日の範囲に収まっていなければなりません。

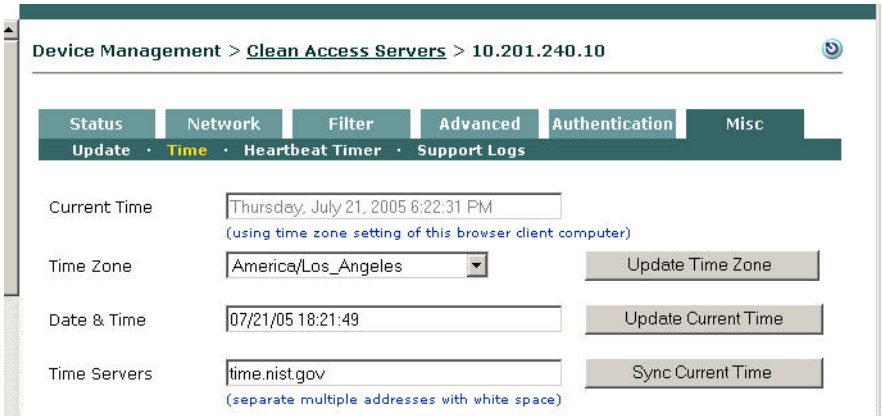
（注）　ハイ アベイラビリティ CAS ペアの場合、CAS 管理ページまたは CAS ダイレクト アクセス Web コンソールによって HA プライマリ CAS で実行された CAS ネットワークの設定変更もまた、スタンバイ CAS ユニットでダイレクト アクセス Web コンソールによって繰り返す必要があります。これらの設定には、SSL 証明書、システム時刻、タイム ゾーン、DNS、またはサービス IP の更新が含まれます。詳細については、「CAS ダイレクト アクセス Web コンソール」（p.13-3）および「ハイ アベイラビリティ設定の変更」（p.14-26）を参照してください。

CAM の時刻を変更するには、**Administration > CCA Manager > System Time** を使用します。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。

**現在時刻を表示する手順は、次のとおりです。**

1. **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Time** の順番に進みます。
2. CAS のシステム時刻は **Current Time** フィールドに表示されます。

**図 13-10　Time フォーム**



システム時刻は、手動で新しい時刻を入力して調整したり、外部タイム サーバから同期して自動的に調整することができます。

### 手動でシステム時刻を変更する手順は、次のとおりです。

**Misc** タブの **Time** フォームで、次のいずれかを実行します。

- **Date & Time** フィールドに時刻を入力し、**Update Current Time** をクリックします。時刻は *mm*/*dd*/*yy hh*:*ss* PM/AM の形式で入力する必要があります。
- **Sync Current Time** ボタンをクリックして、**Time Servers** フィールドに表示されたタイム サーバを使用して時刻を更新させます。

### タイム サーバと自動的に同期する手順は、次のとおりです。

デフォルト タイム サーバは、**time.nist.gov** にある National Institute of Standards and Technology（NIST）で管理されたサーバです。別のタイム サーバを指定する手順は、次のとおりです。

1. **Misc** タブの **Time** フォームの **Time Servers** フィールドに、サーバの URL を入力します。指定したサーバは、NIST 標準フォーマットの時刻を提供する必要があります。複数のサーバを区切るには、スペースを使用します。
2. **Update Current Time** をクリックします。

複数のタイム サーバを指定した場合、CAS は同期中にリストの最初のサーバと接続を試みます。このサーバを使用できる場合は、そこから時刻が更新されます。このサーバが使用できない場合、CAS は目的のサーバに到達するまで、次のサーバを順に試みます。

CAS は、設定された NTP サーバと時刻を定期的な間隔で自動的に同期します。

### サーバ システム時刻のタイム ゾーンを変更する手順は、次のとおりです。

1. **Misc** タブの **Time** フォームの **Time Zone** ドロップダウン メニューで、新しいタイム ゾーンを選択します。
2. **Update Time Zone** をクリックします。

# サポート ログとログレベルの設定

CAS の **Support Logs** ページは、カスタマーの問題に対して TAC のサポートを容易にするためのものです。管理者は **Support Logs** ページ上で、さまざまなシステム ログ（開いているファイル、開いているハンドル、パッケージの情報など）を 1 つの tarball に結合し、サポート事例に追加するために TAC に送信できます。管理者はカスタマーのサポート要求を送信する場合に、これらのサポート ログをダウンロードする必要があります。

CAM Web コンソールと CAS ダイレクト アクセス Web コンソールの **Support Logs** ページ（図 13-11）では、/perfigo/logs のトラブルシューティング目的で、記録されたログの詳細なレベルを設定する Web ページ コントロールを提供します。この Web コントロールは、トラブルシューティング時に CLI **`loglevel`** コマンドおよびパラメータを使用したシステム情報の収集に代わるものです。

通常の操作では、ログ レベルは必ずデフォルト設定です（Severe）。特定のトラブルシューティング時間の間、一般的にはカスタマー サポート /TAC エンジニアの要求により、ログ レベルは一時的にのみ変更されます。大半の場合、設定は特定の間隔で「Severe」から「All」に切り替えられ、データが収集されたあとで「Severe」にリセットされます。CAM/CAS をリブートする、または **`service perfigo restart`** コマンドを実行すると、ログ レベルはデフォルトの設定に戻ります（Severe）。

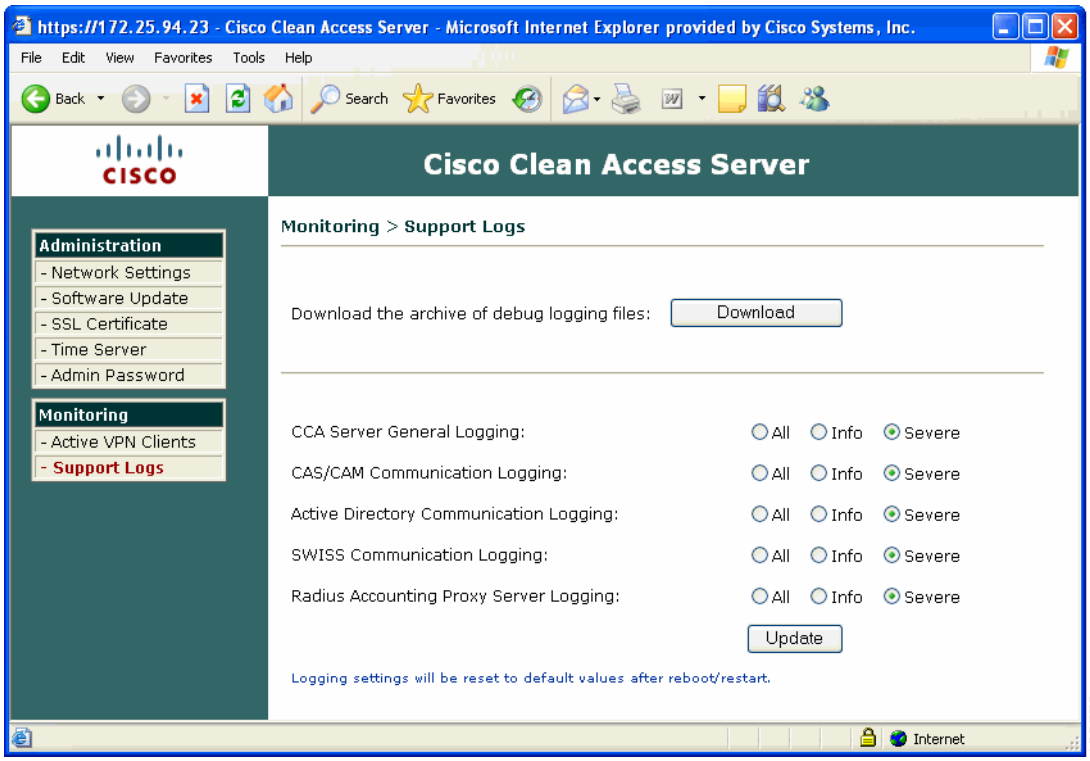
**注意**　ログ レベルの設定を永久に「All」または「Info」にしないでください。設定すると、ログ ファイルが急激に大きくなります。

**CAS サポート ログをダウンロードする手順は、次のとおりです。**

**（注）**　メモリ使用率を最適化する場合、CAS サポート ログ ページは「Monitoring」の CAS ダイレクト アクセス コンソールでのみ使用できます（CAS 管理ページからは使用できません）。

1. URL/ アドレスとして **https://<CAS_eth0_IP>/admin** を使用するブラウザから CAS ダイレクト アクセス コンソールを開きます。
2. **Monitoring > Support Logs** の順番に進みます（図 13-11）。

図 13-11　CAS サポート ログ




3. **Download** ボタンをクリックして、**cas_logs.<cas-ip-address>.tar.gz**　ファイルをローカル コンピュータにダウンロードします。
4. この .tar.gz ファイルをカスタマー サポート要求とともに送信します。

（注）　CAM の圧縮済みサポート ログ ファイルを取得するには、**Administration > CCA Manager > Support Logs** の順番に進みます。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。

**CAS ログのログ レベルを変更する手順は、次のとおりです。**

1. CAS ダイレクト Web コンソール（**https://<CAS_eth0_IP>/admin**）を開きます。
2. **Monitoring > Support Logs** の順番に進みます。
3. 変更する CAS ログ カテゴリを選択します。
   - **CCA Server General Logging**：このカテゴリには、次のほかの 3 つのカテゴリには含まれていない、この CAS の一般的なロギング イベントが含まれます。たとえば、ログインする（CAM へ要求を送信する必要がある）ユーザは、ここでロギングされます。
   - **CAS/CAM Communication Logging**：このカテゴリには関連ログの大半が含まれます（この CAS に特有の CAM/CAS 設定または通信エラー）。たとえば、この CAS へ情報をパブリッシュする CAM の試みが失敗した場合、イベントはここでロギングされます。
   - **SWISS Communication Logging**：このカテゴリには、この CAS と Clean Access Agent の間で送信された SWISS（専用の通信プロトコル）パケットに関連したログ イベントが含まれます。
   - **Radius Accounting Proxy Server Logging**：このカテゴリには、Cisco VPN Server と統合された場合に、この CAS の SSO に関連する RADIUS アカウンティング ログ イベントが含まれます。

4. ログのカテゴリのログレベルの設定をクリックします。
   - **All**：これは最低のログレベルです。すべてのイベントと詳細が記録されています。
   - **Info**：Severe ログレベルよりも詳しい情報を提供します。たとえば、ユーザが正常にログインすると、Info メッセージがロギングされます。
   - **Severe**：これは、システムのデフォルトのロギング レベルです。システムに次のような重大なエラーが発生した場合にのみ、ログ イベントが /perfigo/logs に書き込まれます。

     - CAM が CAS に接続できない。

     - CAM と CAS が通信できない。

（注） CAS を検出するため、CAA は、L2 ユーザの UDP ポート 8905 および L3 ユーザ 8906 ポートで SWISS（専用の CAS-Agent 通信プロトコル）パケットを送信します。CAS は、UDP ポート 8905 とポート 8906 で必ず受信し、デフォルトではトラフィックをポート 8905 で受け入れます。L3 サポートがイネーブル化されていない場合、CAS は UDP ポート 8906 でトラフィックをドロップします。Agent は 5 秒ごとに SWISS を検出します。