

# Clean Access Agent に関する FAQ

## 目次

[はじめに](#)

[サポートされている機能](#)

[エラーメッセージ](#)

[その他](#)

[関連情報](#)

## 概要

このドキュメントでは、Cisco Clean Access Agent (旧名称 Perfigo SmartEnforcer) に関する FAQ に回答します。

製品名は変更されました。この表は古い名前と新しい名前の両方をリストしています。

旧名称	新名称
SmartManager	Clean Access Manager
SecureSmart Server	Clean Access Server
SmartEnforcer	Clean Access Agent
CleanMachinesAPI	Clean Access API

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

## サポートされている機能

Q. いずれのオペレーティング システムがサポートされているでしょうか。

A. エージェントは、次のオペレーティング システム上でサポートされています。

Windows プラットフォーム

- Windows 2000
- Windows XP
- Windows Vista
- Windows 7

Macintosh プラットフォーム

- Mac OS X 10.4.11 「Tiger」

- Mac OS X 10.5.8 「Leopard」
- Mac OS X 10.6.4 「Snow Leopard」

サポートされているブラウザおよび Java のバージョンの詳細については、『[Cisco NAC アプリケーション エージェント/OS/ブラウザのサポート マトリックス](#)』を参照してください。

## Q. カスタム API はサポートされていますか。

A. いいえ。

## Q. VMware または共有ドライバ上のエージェントはサポートされていますか。

A. VMware 上の NAC エージェントで、サポート対象またはサポート対象外となる環境を次に示します。

- **NAT モードの VMware** VMware NAT モードでは、すべての VM の IP および MAC が同一になるため、インバンドと OOB のいずれかを問わず、NAC エージェントはサポートされていません。したがって、認証およびポスチャのために、異なる VM を区別できません。
- **ブリッジモードの VMware (イメージ間の L2 分割、異なる IP/MAC アドレス)** インバンドモードでは、VM 用に一意の IP アドレスおよび MAC アドレスを取得できるため、NAC エージェントがサポートされています。OOB モードでは、スイッチポートあたりの MAC アドレスを 1 個に制限する必要があるため、OOB モードの場合、NAC エージェントはサポートされていません。OOB では、単一スイッチポート越しの複数 MAC アドレスはサポートされていません。( IP Phone とこの IP Phone に接続された PC はサポートされています )。

以上をまとめると、VMware 上の NAC エージェントは、次の場合にサポートされます。

- NAC がインバンド モード。
- VMware がブリッジ モード。

その他モードについては、いずれもサポート対象外です。

## Q. NAC 4.5 以降では、Trend Micro OfficeScan 10.x をサポートしていますか。

A. NAC では、バージョン 4.7.1 以降で Trend Micro OfficeScan 10.x をサポートしています。

## エラー メッセージ

Q. Cisco Clean Access エージェントから「SecureSmart is not available on the network」または「No SecureSmart Server found on the network」というエラーメッセージが表示されます。Cisco Clean Access Server をリブートしたところ、しばらくは回避できました。これはどのように解決すればよいですか。

A. このエラーは、Cisco Clean Access エージェントが、SWISS プロトコル ( UDP ポート 8905 を使用する暗号化通信 ) によって Cisco Clean Access Server と通信できないために発生しています。

次の原因が考えられます。

- ログ ファイルが増大しすぎた。

- Apache エントリによってログのサイズが 2 GB に達していないかどうかをチェックします。この問題は、バージョン 3.3.x 以降では修正されています。
- SS 証明書が無効です。Clean Access Server の証明書が無効であるか正しくない場合は、HTTPS 接続を適切に確立できません。証明書のポップアップの下部にあるチェックマークが 2 個 (一時証明書) または 3 個 (CA 署名付き証明書) であることを確認します。
- クライアントの時刻が正しくない。クライアント マシン上の時刻を原因としてサーバ証明書が信頼されない場合 (たとえば、クライアントに設定されている時刻がサーバの時刻よりも遅れている)、この設定によって証明書の時刻は、クライアントから見て将来の時刻になります。Clean Access Server 上の時刻をチェックし、タイム サーバに対する NTP プロトコルが許可されていることを確認します。
- クライアント マシンにネットワーク カードが複数枚搭載されている。クライアント マシンに複数のカードが搭載されていると、Windows で、誤ったカードを使用して情報を送信することがあります。この問題を回避するには、使用しないネットワーク カードを無効にします。
- 施行元 PC 上のキャッシュをクリアしてみます。コマンド プロンプトで `ipconfig` コマンドまたは `dnsflush` コマンドを発行します。または Internet Explorer で [Tools] > [Internet Options] > [Advanced] の下の [Check for server certificate revocation] をオフにします。
- ネットワーク接続が確立されていない。
- IP アドレスが適切であることを確認します。
- Cisco Clean Access エージェントの新規インストール後に、ローカル PC またはローカル マシンに問題があることがあります。
- PC をリブートします。Clean Access Server 上で `service perfigo restart` コマンドを発行します。
- Cisco Clean Access Server 上の宛先ポート 8905 がネットワーク ファイアウォールまたはパーソナル ファイアウォールによってブロックされている。
- ポート 8905 が開放されていることを確認します。
- サードパーティ製ソフトウェアによって、Cisco Clean Access エージェントが妨害されている。該当するソフトウェアを無効にして、Clean Access エージェントが動作するかどうか確認してみてください。
- パーソナル ファイアウォールをオフにするか、VPN ソフトウェアを無効にするか、スパム ブロッカーを無効にしてみてください。
- ソフトウェアの不具合が見つかり、Cisco Clean Access Server 3.2.6 で修正されています。
- Cisco Clean Access Manager および Cisco Clean Access Server を 3.2.6 にアップグレードしてください。

## Q. Cisco Clean Access エージェントのログイン時に、エラー メッセージ「Network Error」を受け取りました。なぜでしょうか。

A. Cisco Clean Access エージェントでは、HTTPS を使用して Cisco Clean Access Server と通信できない場合に、このエラーを表示します。複数の原因が考えられます。

- SS 証明書が無効です。Cisco Clean Access Server の証明書が無効であるか正しくない場合は、HTTPS 接続を適切に確立できません。証明書のポップアップの下部にあるチェックマークが 2 個 (一時証明書) または 3 個 (CA 署名付き証明書) であることを確認します。
- クライアントの時刻が正しくない。クライアント マシン上の時刻が原因で、クライアント マシンでは、サーバ証明書を信頼できません。たとえば、クライアントの時刻にサーバよりも遅れた時刻が設定されています。この結果、証明書の時刻がクライアントから見て将来になっています。Cisco Clean Access Server 上の時刻をチェックし、タイム サーバに対する

NTP プロトコルが許可されていることを確認します。

- クライアント マシンにネットワーク カードが複数枚搭載されている。クライアント マシンに複数のカードが搭載されていると、Windows で、誤ったカードを使用して情報を送信することがあります。この問題を回避するには、使用しないネットワーク カードを無効にします。
- サードパーティ製のソフトウェアによって、Cisco Clean Access エージェントおよび Cisco Clean Access Server の通信が妨害されています。Cisco VPN Client、CheckPoint® VPN クライアント、パーソナル ファイアウォールなどのソフトウェアが通信に影響しているおそれがあります。
- 該当するソフトウェアを無効にして、Cisco Clean Access エージェントが動作するかどうか確認してみてください。
- キャッシュをクリアします。コマンド プロンプトで `ipconfig /dnsflush` コマンドを発行するか、Internet Explorer の [Internet Options] > [Advanced] の下で [Check for server certificate revocation] をオフにします。

**Q. Windows アップデート中に Cisco Clean Access エージェントが出す「this update can not be performed for a non-administrator account」というエラー メッセージは何を意味していますか。**

A. 管理者以外の Clean Access エージェントでは、Windows アップデートを実行できないという問題です。管理者以外で Windows Server Update Services ( WSUS ) を起動するには、エージェント スタブが必要です。スタブ サービスは、admin ではないユーザに対して、次の機能をサポートするために必要です。

- エージェントのダウンロードとインストール
- エージェントのアップグレード
- 実行可能ファイルの起動
- WSUS アップデートの起動
- 認証 VLAN 変更設定へのアクセス
- IP 更新の実行

**Q. 「This client version is old and not compatible. Please login from web browser to see the download link for the new version」というエラー メッセージを Cisco Clean Access エージェントが出す場合、何を意味するのでしょうか。**

A. Clean Access のエージェントとサーバのバージョンが異なることが問題です。Clean Access エージェントのバージョンをサーバと合わせてみてください。

**Q. Windows 98 システムをフレッシュ インストールしました。Cisco Clean Access エージェント クライアント 3.2.0 をこのマシンにインストールすると、インストーラをアップデートするように要求されます。ただし、Cisco Clean Access エージェントがインストーラをアップデートするように試みるとすぐ `instmsi c` 得て下さい: `Windows \ Files\Content.IE5\KXERWHYB\InstMSIA[2].exe` エラーメッセージ。これはどのように解決すればよいですか。**

A. フルバージョンの Cisco Clean Access エージェント 3.1.3 または 3.2.0 ( 5 Mb 超 ) をインストールします。

**Q. Cisco Clean Access エージェントを Cisco Clean Access Server にアップロードしましたが、Cisco Clean Access Server によってパブリッシュされません。「Checking for the uploaded SmartEnforcer client file.... SmartEnforcer client file not found.」というエラーメッセージが表示されます。これはどのように解決すればよいですか。**

A. .zip ファイルではなく、.exe ファイルをアップロードします。アップロードする前に、zip フォルダから .exe ファイルを必ず抽出解凍してください。元の .exe ファイルの名前を変更しない必要もあります。

**Q. Cisco Clean Access エージェントにログインしようとする「Access to network is blocked by the administrator」というエラーメッセージが表示されるのはなぜでしょうか。**

A. 有線ネットワークとワイヤレスネットワークを同時に使用しているときに、このエラーメッセージが出ることがあります。ネットワークとワイヤレスネットワークのいずれかのみを使用すると、この問題が解決することがあります。CCA バージョン 4.1.3 の使用も試してください。この問題の解決に役立つことがあります。

**Q. NAC アプライアンスのアップグレード後に「Warning: The current Trusted Certificate Authority 'www.perfigo.com' is suited for lab environments only. Cisco recommends importing a third-party Certificate Authority. Please check your Clean Access Server(s) and standby Clean Access Manager for similar messages.」というエラーメッセージが表示されるのはなぜでしょうか。**

A. このエラーメッセージの原因は、Perfigo 証明書にあります。この問題は、信頼できる CA のリストから Perfigo CA を削除することにより解決できます。

**Q. 「Revocation information for the security certificate for this site is not available. Do you want to proceed」というエラーメッセージが Cisco Clean Access エージェントに出る場合、何を意味するのでしょうか。**

A. この問題の原因は、セキュリティ証明書の失効情報を参照できないことにあります。この問題には 2 つの解決策があります。解決策を以下に示します。

1. CA 署名付き CAS SSL 証明書を使用する場合は、証明書の [CRL Distribution Points] フィールドを確認し ( 中間 CA またはルート CA )、Unauthenticated、Temporary、Quarantine のロールの許可ホスト ポリシーに URL ホストを追加します。これにより、ログイン時にエージェントで CRL をフェッチできます。
2. この問題を解決するには、インターネット ブラウザで次の手順を実行します。クライアントシステムの信頼できるルートストアに証明書をインポートします。[Tools] > [Internet Options] > [Advanced] タブ > [Security] セクションを選択し、[Check for server certificate revocation (requires restart)] のチェックマークを外します。開いているブラウザを閉じ、新しくブラウザを開いて変更を有効にします。

このエラーメッセージを解消する別の回避策があります。次のディレクトリの NACAgentCFG.xml ファイルに <AllowCRLChecks>0</AllowCRLChecks> を追加できます。  
C:\ProgramFiles\Cisco\Cisco NAC Agent

注: この問題が原因で、Cisco Clean Access エージェントは、「Network Error SSL Certificate

Rev Failed 12057」というエラーメッセージを生成します。

詳細は、次のドキュメントを参照してください。

- 『[Cisco NAC アプライアンスバージョン 4.7\(2\) リリースノート](#)』の「[Windows Vista および Windows 7 : IE 7 および IE 8 の証明書失効リスト](#)」
- 『[エージェントログインおよびクライアント ポスチャ評価のための Cisco NAC アプライアンスの設定](#)』の「[Cisco NAC エージェント XML 設定ファイルの設定](#)」

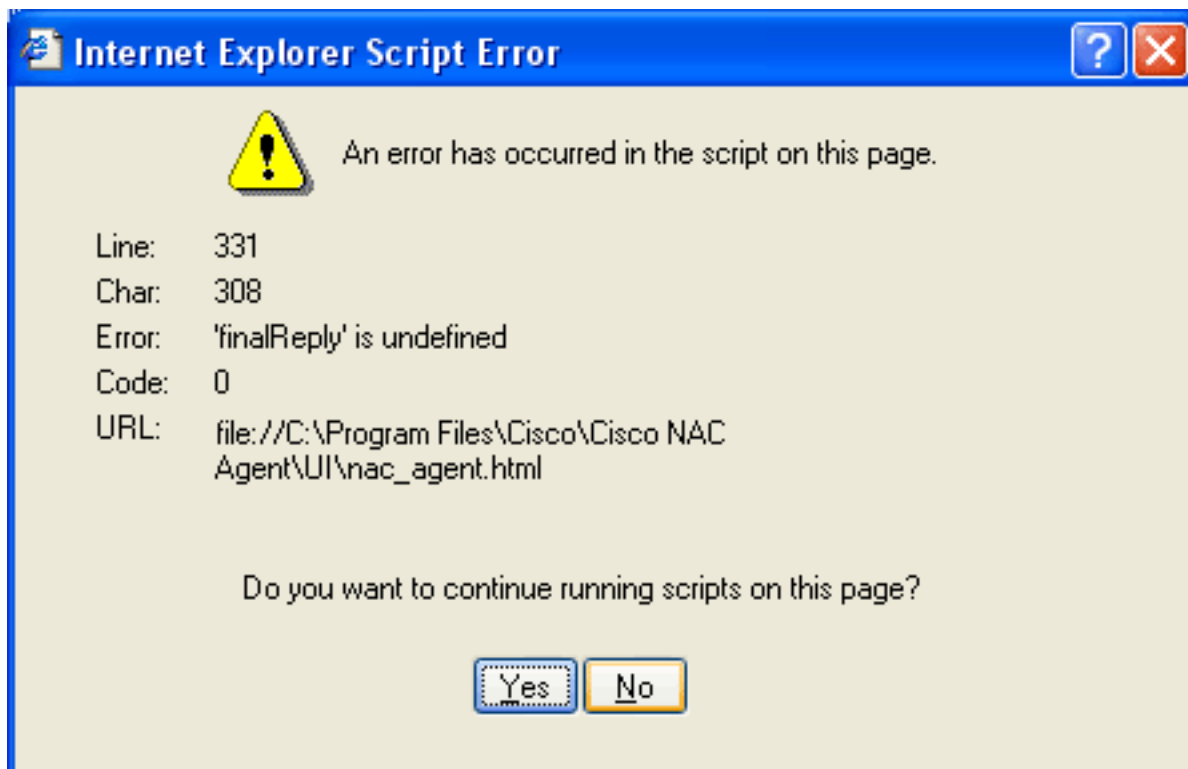
**Q. Windows 7 マシン上で Web エージェントを起動すると、エラーメッセージコード 3 を出して失敗します。この問題を解決するにはどうすればよいですか。**

A. エラーコード 3 は、エージェントがダウンロードされた一方で、インストールされていないことを示すメッセージです。次の回避策があります。

1. UAC ( ユーザ アカウント制御 ) が有効化されていることを確認します。
2. Internet Explorer が管理者モードで実行されていることを確認します。
3. 一部の Active X 機能が失敗していないかどうかを確認し、IE と Active X のすべてのアクセス許可をデフォルトにリセットしてみます。
4. 他のいずれかのアンチウイルス ( AV ) ソフトウェアによって、一時ディレクトリから IE の実行可能ファイルを起動できなくなっていないかどうかを確認します。

**Q. NAC エージェントが起動を試行したときに、Internet Explorer スクリプトエラーが出ます。この問題を解決するにはどうすればよいですか。**

A. 次のエラーメッセージが表示されます。



この問題を解決するには、次の手順を実行します。

1. Cisco NAC エージェントをシステムからアンインストールします。

2. C:\Program Files\Cisco\Cisco NAC Agent ディレクトリを手動で削除します。
3. 次の URL から *regrserv32a.exe* をダウンロードします。  
<http://support.microsoft.com/kb/267279>
4. *regrserv32a.exe* を実行します。アプリケーションがローカル コンピュータに解凍されます。
5. コマンド プロンプトを開き、*regrserv32.exe* アプリケーションを解凍したディレクトリに移動します。
6. *regsvr32.exe msxml3.dll* を実行します。登録が成功したことを示すダイアログ ボックスが表示されます。
7. Cisco NAC エージェントをインストールします。
8. Cisco NAC エージェントが正常に開始されていることを確認します。

## その他

**Q. MAC クライアントが「Page Not Found」ページにリダイレクトされない問題を修正するには、どうすればよいですか。**

A. *.local* で終わるドメイン名を使用していないことを確認します。MAC では、マルチキャスト DNS 用の専用 DNS 名としてこのドメイン名を扱います。そのため、解決要求が DNS サーバに送信されません。

**Q. Clean Access エージェントが McAfee によってブロックされる場合、何が起きていますか。**

A. McAfee で *webagent* セットアップ プログラム (*webagentsetup-win.exe*) をトロイの木馬と見なし、Clean Access エージェントをブロックすることが問題です。この問題の回避策の 1 つは、クライアントのダウンロード方法を変更して ActiveX アプレットを外し、Java コンポーネントだけを使用することです。これは UserPages を使用して CAM で **ログイン ページ-編集します-Web クライアント (ActiveX/アプレット) - Java アプレットだけを設定** することができます。または、Firefox (推奨) を初めとする任意のブラウザを使用することもできます。

**Q. ポート 8905 を送信元ポートとして接続する場合、Cisco Clean Access Server では、いずれの宛先と通信しようとしていますか。**

A. Cisco Clean Access エージェントでは、UDP ポート 8905 を使用する暗号化通信による SWISS プロトコルを介して Cisco Clean Access Server と通信します。

**Q. SSH アクセスを Cisco Clean Access Server に限定するにはどうすればよいですか。**

A. */etc/ssh/sshd\_config* ファイルに変更を加えて、次のような行を追加します。

```
ListenAddress IP_address_of_where_you_want_ssh_to_allow_connections
```

次に、例を示します。

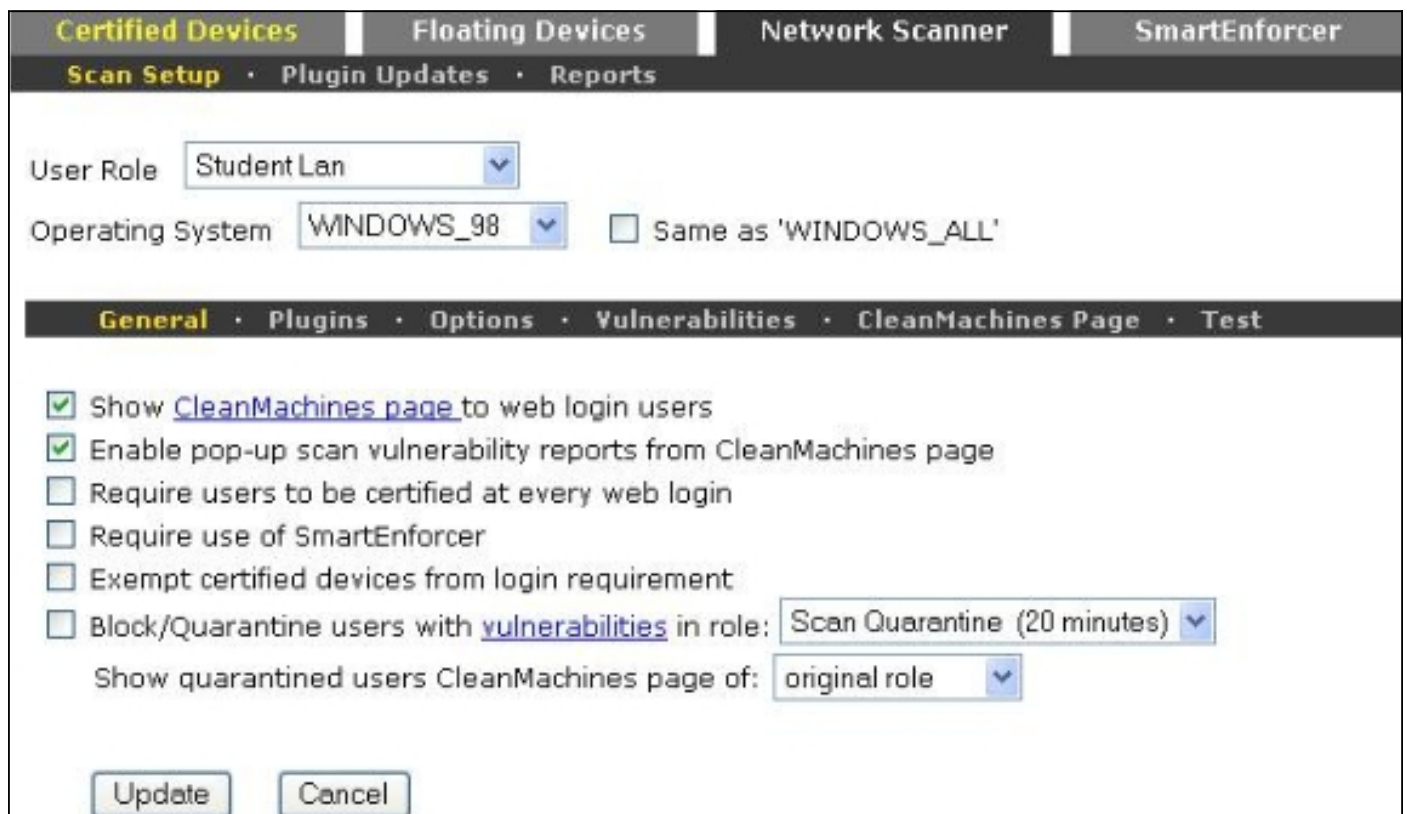
```
ListenAddress 192.168.151.60
```



service sshd restart コマンドを発行して SSHD プロセスを再起動します。

Q. Windows 98/95 で、Clean Access エージェントを無効にするにはどうすればよいですか。

A. [CleanMachines] の下で [Windows All] のチェックを外し、各 OS の [Require Use of Clean Access Agent] を個別に選択します。



The screenshot shows the SmartEnforcer configuration interface. At the top, there are tabs for 'Certified Devices', 'Floating Devices', 'Network Scanner', and 'SmartEnforcer'. Below these are sub-tabs for 'Scan Setup', 'Plugin Updates', and 'Reports'. The 'User Role' is set to 'Student Lan' and the 'Operating System' is set to 'WINDOWS\_98'. There is a checkbox for 'Same as 'WINDOWS\_ALL'' which is unchecked. Below this is a navigation bar with tabs for 'General', 'Plugins', 'Options', 'Vulnerabilities', 'CleanMachines Page', and 'Test'. The 'CleanMachines Page' tab is selected. The settings for this page are as follows:

- Show [CleanMachines page](#) to web login users
- Enable pop-up scan vulnerability reports from CleanMachines page
- Require users to be certified at every web login
- Require use of SmartEnforcer
- Exempt certified devices from login requirement
- Block/Quarantine users with [vulnerabilities](#) in role: Scan Quarantine (20 minutes)
- Show quarantined users CleanMachines page of: original role

At the bottom, there are 'Update' and 'Cancel' buttons.

Q. リンクアップトラップまたは MAC 通知トラップの送信後に、SNMPv3 を実行しているエッジスイッチがコントローラによって適切にポーリングされません。SNMPv3 を実行しているスイッチ上のポートに接続しているエンドポイントの検出は、NAC Profiler の NetMap によるスイッチの次回定期ポーリングまで遅延します。これは、なぜですか。

A. この問題は、Cisco Bug ID [CSCta25695](#) (登録ユーザ専用) に関連しています。詳細は、このバグを参照してください。

Q. NAC アプライアンスで Perfigo からの証明書を使用するとなぜ問題があるのですか。

A. Perfigo からの証明書を使用したときに問題が生じる原因は、使用する Cisco NAC アプライアンスのバージョンにある場合があります。Cisco NAC アプライアンス リリース 4.7(0) の .ISO イメージおよびアップグレード イメージには、www.perfigo.com 認証局 (CA) は含まれなくなりました。ネットワークで www.perfigo.com CA を使用する必要がある管理者は、リリース 4.7(0) のインストールまたはアップグレードの後で、この CA をローカル マシンから手動でインポートする必要があります。

CAM と CAS の間に最初のセキュア通信チャネルを確立するためには、各アプライアンスからもう一方のアプライアンスの信頼できるストアにルート証明書をインポートして、CAM が CAS の



( および CAS が CAM の ) 証明書を信頼できるようにする必要があります。

**Q. Windows 7 マシンの場合に、Cisco Clean Access の AV チェックが失敗します。この問題を解決するにはどうすればよいですか。**

A. この問題は、Windows 7 OS の下で、要件規則で選択された規則が正しくないために発生します。Windows 7 の既存の要件の下ですべての要件規則を選択します。

**Q. AVG 10 がインストールされていても、NAC では、ワークステーションにアンチウイルスがインストールされていないとして、ネットワークアクセスを拒否します。この問題の原因は何ですか。**

A. AVG 10 は、まだ NAC 上でサポートされていません。この拡張についての詳細は、Cisco Bug ID [CSCtj89340](#) ( [登録ユーザ専用](#) ) を参照してください。

**Q. NAC の背後にある Nortel IP Phone に DHCP 要求を渡すことができますか。**

A. はい。NAC の背後にある Nortel IP Phone に DHCP 要求を渡すことができます。詳細については、『[NAC の背後にある Nortel IP Phone](#)』を参照してください。

## 関連情報

- [Clean Access Manager FAQ](#)
- [Cisco Clean Access Manager FAQ 2](#)
- [Cisco Clean Access Server FAQ](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)