CHAPTER 5

ホスト スキャンの設定

AnyConnect ポスチャ モジュールにより、AnyConnect Secure Mobility クライアントはホストにインストールされているオペレーティング システム、およびアンチウイルス、アンチスパイウェア、ファイアウォールの各ソフトウェアを識別できます。ホスト スキャン アプリケーションはポスチャ モジュールのコンポーネントに含まれる、こうした情報を収集するアプリケーションです。

適応型セキュリティ アプライアンス（ASA）では、オペレーティング システム、IP アドレス、レジストリ エントリ、ローカル証明書、ファイル名などのエンドポイント属性を評価するポリシーを作成できます。ポリシーの評価結果に基づいて、どのホストがセキュリティ アプライアンスへのリモート アクセス接続を確立できるかを制御できます。

AnyConnect 3.0 より、ホスト スキャン パッケージは AnyConnect Secure Mobility クライアントおよび Cisco Secure Desktop（CSD）の共有コンポーネントになっています。それ以前は、ホスト スキャン パッケージは CSD をインストールすることによってのみ利用可能になるコンポーネントの 1 つでした。

ホスト スキャン パッケージを CSD から分離したのは、CSD の一部として提供されていたときよりも、ユーザが頻繁にホスト スキャン サポート表を更新できるようにするためです。ホスト スキャンは、Dynamic Access Policies（DAPs）の割り当てに使用するアンチウイルス、アンチスパイウェア、ファイアウォールの各アプリケーションの製品名とバージョン情報を含む表をサポートします。シスコでは、ホスト スキャン パッケージにホスト スキャン アプリケーション、ホスト スキャン サポート表、および他のコンポーネントを含めて提供しています。

ポスチャ モジュールに同梱されたスタンドアロン ホスト スキャン パッケージとホスト スキャン パッケージが提供する機能は同じです。シスコでは、ホスト スキャン サポート表を簡単に更新できるように、別個のホスト スキャン パッケージを提供しています。

ホスト スキャン パッケージは、AnyConnect ポスチャ モジュール、CSD、スタンドアロン パッケージの 3 種類の方法で提供できるようになりました。AnyConnect ポスチャ モジュールには 2 つのタイプがあります。1 つ目のバージョンは、AnyConnect のインストールと一緒に ASA によってプッシュされます。もう 1 つのバージョンは、事前展開モジュールとして設定されます。事前展開モジュールは、ASA への初期接続を確立する前に、エンドポイントにインストールできます。

エンドポイントにインストールされたオペレーティング システム、およびアンチウイルス、アンチスパイウェア、ファイアウォールの各ソフトウェアを識別することに加え、ホスト スキャン パッケージによって、評価の実行、キーストローク ロガーの識別、およびエンドポイントで実行されるホスト エミュレーションと仮想マシンの検出を行うコンポーネントが提供されます。キーストローク ロガーの検出およびホスト エミュレーションと仮想マシンの検出は、CSD の機能でもありましたが、今ではホスト スキャン パッケージに組み込まれています。

それでも、ホスト スキャンは CSD の代わりにはなりません。キャッシュ クリーンナップや Secure Vault が必要なお客様は、ホスト スキャン パッケージの他に CSD をインストールして、有効にする必要があります。Secure Vault 機能の詳細については、CSD 設定ガイド（http://www.cisco.com/en/US/products/ps6742/products_installation_and_configuration_guides_list.html）を参照してください。

ASA の Adaptive Security Device Manager（ASDM）またはコマンドライン インターフェイスを使用して、ホスト スキャンをインストール、アンインストール、有効および無効にできます。Secure Desktop Manager ツールを ASDM で使用して、ポリシーを設定できます。

ポスチャ アセスメントおよび AnyConnect テレメトリ モジュールは、ホストにホスト スキャンがインストールされている必要があります。

この章の内容は、次のとおりです。

ホスト スキャン ワークフロー

以下のワークフローで説明するように、ホスト スキャンは ASA と連携して、企業ネットワークを保護します。

1. リモート デバイスでは、クライアントレス SSL VPN またはセキュリティ アプライアンスとの AnyConnect Client セッション確立が試行されます。
2. ASA はホスト スキャンをクライアントにダウンロードし、ASA とクライアントが同じバージョンのホスト スキャンを使用するようにします。
3. 評価は、リモート コンピュータについて次のチェックを行います。
   - オペレーティング システム
   - 指定するファイルの有無。
   - CSD 管理者が指定するレジストリ キーの有無。このチェックは、コンピュータが Microsoft Windows を実行している場合だけに適用されます。
   - CSD 管理者が指定するデジタル証明書の有無。このチェックについても、コンピュータが Microsoft Windows を実行している場合だけに適用されます。
   - CSD 管理者が指定する IP アドレスの範囲。
4. クライアントが評価を行っていると同時に、ホスト スキャンはそのエンドポイントの評価を行っており、アンチウイルス、ファイアウォール、アンチスパイウェアのバージョン情報を収集しています。同時に、Dynamic Access Policies で指定したレジストリ キー、ファイル、プロセスをスキャンしています。
5. 評価結果に応じて、次のいずれかのイベントが発生します。

- 評価が実行され、[Login Denied] エンド ノードで終了するシーケンスを経由する場合は、リモート コンピュータに「Login Denied」メッセージが表示されます。この場合、ASA とリモート デバイス間の対話は停止します。
- 評価により、ポリシー名がデバイスに割り当てられ、ポリシー名が ASA に報告されます。

6. ホスト スキャンは、評価後にリモート コンピュータが割り当てたポリシーの設定に基づいて、リモート コンピュータのキーストローク ロガーおよびホスト エミュレーションを確認します。
7. アンチウイルス、ファイアウォール、またはアンチスパイウェアは、保証があり、Advanced Endpoint Assessment ライセンスを保有している場合に修復されます。
8. ユーザがログインします。
9. 通常 ASA は、3. で収集した認証データ、さらに 4. で収集した設定済みのエンドポイント属性条件を使用します。この条件には、ポリシーおよびホスト スキャン結果などの値が入っており、ダイナミック アクセス ポリシーをセッションに適用できます。
10. ユーザ セッションが終了した後、ホスト スキャンが終了し、キャッシュ クリーナがクリーンアップ機能を実行します。

AnyConnect ポスチャ モジュールで有効になる機能

評価

評価は、ユーザが ASA に接続した後、かつログインする前に実行されます。この評価では、ファイル、デジタル証明書、OS、IP アドレス、および Microsoft Windows レジストリ キーについてリモート デバイスをチェックできます。

管理者とホスト スキャンのインターフェイスとなる Secure Desktop Manager では、評価モジュールを簡単に設定できるグラフィカル シーケンス エディタが提供されます。

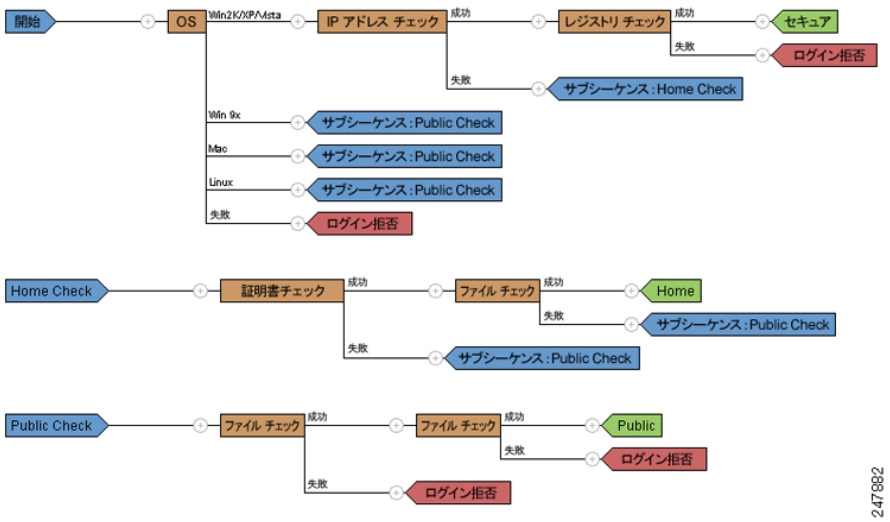
評価モジュールを設定するときに、ホスト スキャン管理者は「*シーケンス*」と呼ばれるノードのブランチを作成します。各シーケンスは [Start] ノードで始まり、続いてエンドポイント チェックが実行されます。チェックの結果により、別のエンドポイント チェックを実行するかどうか、またはエンド ノードでシーケンスを終了するかどうかを判定します。

エンドノードでは、「Login Denied」メッセージを表示するかどうか、ポリシーをデバイスに割り当てるかどうか、または「サブシーケンス」と呼ばれるセカンダリ チェックのセットを実行するかどうかを判定します。「*サブシーケンス*」は、シーケンスの連続で、通常、詳細なエンドポイント チェックとエンドノードで構成されます。この機能は、以下の処理を行う場合に便利です。

- 特定のケースで、チェックのシーケンスを再利用する。

- サブシーケンス名を使用して文書化するといった全体的な目的を持つ条件セットを作成する。
- グラフィカル シーケンス エディタが占める水平方向の領域を制限する。

図 5-1　　完全な評価の例



ポリシー

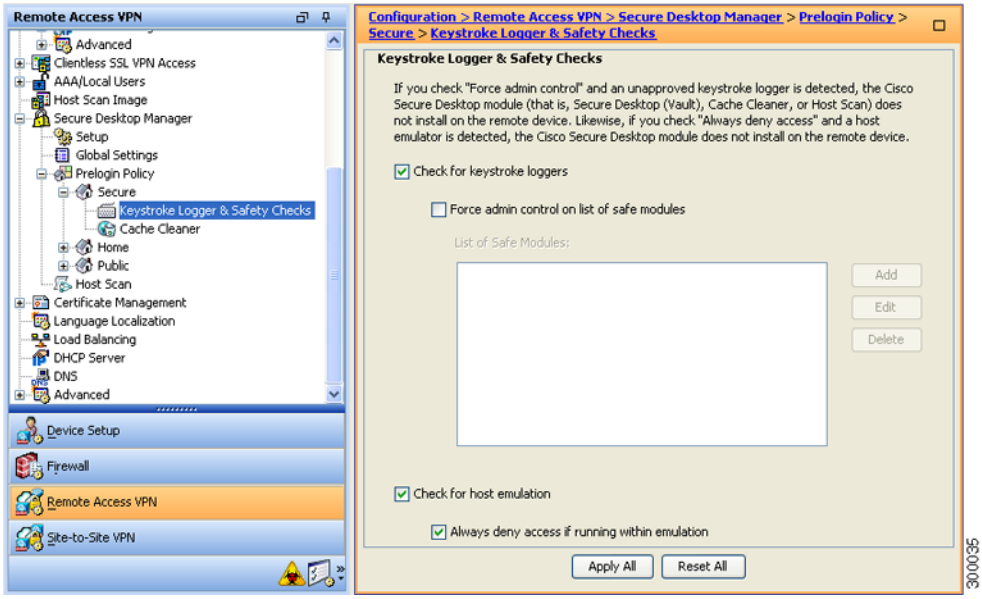
グラフィカル シーケンス エディタで設定された評価（図 5-1）のチェックの結果によって、評価が特定のポリシーに割り当てられるか、または拒否されるリモート アクセス接続となるかが判明します。

ポリシーを作成するたびに、Secure Desktop Manager によりポリシーにちなんだ名前が追加されます。ポリシーのメニューごとに、ポリシーに対して一意な設定を割り当てることができます。これらの設定により、ポリシーに割り当てられた条件に一致するリモート デバイス上にキーストローク ロガー検出、ホスト エミュレーション検出、またはキャッシュ クリーナがインストールされるかが決まります。管理者は通常、これらのモジュールを企業以外のコンピュータに割り当て、セッション終了後の企業データやファイルへのアクセスを防止します。

ホスト スキャンおよびポリシーの設定の詳細については、『*Cisco Secure Desktop Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators, Release 3.6*』の次の章を参照してください。

- Confirming Host Scan
- Tutorial: Assigning Criteria to Policies
- Details: Assigning Criteria to Policies

図 5-2　　ポリシー



キーストローク ロガー検出

ユーザが入力したキー入力を記録するプロセスまたはモジュールをスキャンするよう、選択したポリシーを設定して、疑わしいキー入力ロギング アプリケーションが存在する場合は、VPN アクセスを拒否できます。

デフォルトでは、キーストローク ロガー検出はすべてのポリシーで無効になっています。Secure Desktop Manager を使用して、キーストローク ロガー検出を有効または無効にできます。安全なキーストローク ロガーを指定するか、またはリモート コンピュータ上のキャッシュ クリーナまたはホスト スキャンを実行するための条件としてスキャンで識別されたキーストローク ロガーをリモート ユーザに対話的に承認させることができます。

有効にすると、キーストローク ロガー検出はキャッシュ クリーナまたはホスト スキャンとともにリモート コンピュータにダウンロードされます。ダウンロードが完了したキーストローク ロガー検出は、OS が Windows で、かつユーザが管理者権限を持っている場合に限り実行されます。

関連モジュールは、スキャンに問題がない場合、または、管理者がユーザに管理作業を割り当て、スキャンで識別されたアプリケーションをユーザが承認する場合に限り実行されます。

（注）　キーストローク ロガー検出は、エンドユーザが管理者権限でログインしている限り、ユーザ モードとカーネル モードの両方のロガーに適用されます。

キーストローク ロガー検出は、32 ビット版 Microsoft Windows OS 環境に限り実行できます。「キーストローク ロガー検出およびホスト エミュレーション検出対応オペレーティング システム」（P.5-6）を参照してください。

キーストローク ロガー検出では、潜在的に悪意のあるキーストローク ロガーのすべてを検出できない場合があります。ハードウェアのキー入力ロギング デバイスは検出されません。

ホスト エミュレーション検出

ポリシーのもう 1 つの機能であるホスト エミュレーション検出では、リモートの Microsoft Windows オペレーティング システムがバーチャライゼーション ソフトウェア上で実行されているかどうかを判断します。Secure Desktop Manager を使用して、この機能を有効または無効にできます。また、ホスト エミュレータが存在する場合にアクセスを拒否したり、ユーザに検出を報告し、続行するか終了するかの判断をユーザに委ねることができます。

デフォルトでは、ホスト エミュレーション検出はすべてのポリシーで無効になっています。この機能を有効にすると、Secure Desktop、Cache Cleaner、またはホスト スキャンと共にリモート コンピュータにダウンロードされます。ダウンロードが完了すると、まずホスト エミュレーション検出が実行され、キーストローク ロガー検出の実行が設定されている場合は同時に実行されます。続いて、次のいずれかの条件に当てはまる場合は、関連モジュールが実行されます。

- ホストがエミュレータ（または、バーチャライゼーション ソフトウェア）上で実行されていない。
- アクセスを常に拒否するように設定しておらず、ユーザが検出されたホスト エミュレータを承認する。

「キーストローク ロガー検出およびホスト エミュレーション検出対応オペレーティング システム」（P.5-6）を参照してください。

キーストローク ロガー検出およびホスト エミュレーション検出対応オペレーティング システム

キーストローク ロガー検出およびホスト エミュレーション検出は、次のオペレーティング システムで動作します。

- x86（32 ビット）の Windows Vista SP1 および SP2

  SP1 または SP2 が適用されていない Windows Vista を実行しているコンピュータには KB935855 をインストールする必要があります。
- x86（32 ビット）の Windows XP SP2 および SP3

（注）　Secure Desktop、キーストローク ロガー検出およびホスト エミュレーション検出は Windows 7 には対応していません。

Cache Cleaner

Secure Desktop の代替機能となる Cache Cleaner は機能面で制限がありますが、多くのオペレーティング システムをサポートする柔軟性を備えています。Cache Cleaner では、クライアントレス SSL VPN または AnyConnect Client セッション終了時に、ブラウザ キャッシュから情報を削除しようとします。この情報には、入力されたパスワード、オートコンプリート テキスト、ブラウザでキャッシュされたファイル、セッション時に行われたブラウザ設定の変更、クッキーが含まれます。

Cache Cleaner は、Microsoft Windows、Apple Mac OS、Linux 上で実行されます。システム要件の詳細については、『Cisco Secure Desktop Release Notes』を参照してください。

これは、キャッシュ クリーナが導入され、エンドポイントがクライアントレス SSL VPN 接続を確立しようとする、または Web 起動を使用して AnyConnect を起動しようとする場合の一連のイベントです。

ステップ 1　ユーザがエンドポイントの URL をブラウザに入力すると、エンドポイントは ASA に接続されます。

ステップ 2　ホスト スキャンにより評価を行います。

ステップ 3　エンドポイントが評価を通過することが前提で、AnyConnect の認証が開始されます。ユーザはパスワードを入力するか、証明書を使用して認証します。

ステップ 4　[Clean the whole cache in addition to the current session cache (IE only)] を有効にしないで Internet Explorer を実行しているユーザ、または Safari や Firefox を実行しているユーザの場合、ユーザ認証の後、約 1 分間、キャッシュ クリーナによってブラウザのキャッシュのスナップショットが取られます。

ステップ 5　ユーザが操作すると、ブラウザは情報をキャッシュします。

ステップ 6　ユーザが VPN セッションからログアウトした場合：

- [Clean the whole cache in addition to the current session cache (IE only)] を有効にして Internet Explorer を実行しているユーザについては、キャッシュ クリーナによってブラウザのキャッシュ全体が削除されます。
- [Clean the whole cache in addition to the current session cache (IE only)] を有効にしないで Internet Explorer を実行しているユーザ、または Safari や Firefox を実行しているユーザの場合、キャッシュ クリーナはブラウザのすべてのキャッシュの削除を試行してから、そのキャッシュに対して取ったスナップショットを復元します。

  機密情報がコンピュータ上に復元されないようにするため、セッション終了後に手動でブラウザのキャッシュを消去し、ブラウザを閉じることをお勧めします。

（注）　キャッシュ クリーナを、[Clean the whole cache in addition to the current session cache (IE only)] オプションを有効にして設定することをお勧めします。

ホスト スキャン

ホスト スキャンは、ユーザが ASA に接続した後、かつログインする前に、リモート デバイス上にインストールされるパッケージです。ホスト スキャンは、CSD 管理者が設定する基本ホスト スキャン モジュール、エンドポイント アセスメントモジュール、Advanced Endpoint Assessment モジュールの任意の組み合わせで構成されます。ホスト スキャンは、Microsoft Windows、Apple Mac OS X、および Linux 上で実行されます。詳細な要件については、「システム要件」（P.5-11）を参照してください。

ホスト スキャン パッケージは、CSD とバンドルされて、スタンドアロン モジュールとして、また AnyConnect 3.0 クライアントのポスチャ モジュールの一部として提供されます。

基本ホスト スキャン機能

ホスト スキャンは、CSD またはホスト スキャン/CSD が ASA で有効にされている場合に、Cisco クライアントレス SSL VPN または AnyConnect クライアント セッションを確立するリモート デバイスのオペレーティング システムおよびサービス パックを自動的に識別します。

Secure Desktop Manager を使用して、特定のプロセス、ファイル、レジストリ キー、デジタル証明書、および IP アドレスについて、エンドポイントを検査するようにホスト スキャンを設定することもできます。Secure Desktop Manager は、ASA 上で Adaptive Security Device Manager（ASDM）と統合されます。

ホスト スキャンは、ユーザがコンピュータにログオンする前に、これらすべての検査を実行します。

ホスト スキャンは、オペレーティング システムとサービス パックの情報とともに、収集するように設定されたプロセス、ファイル、レジストリ キー、デジタル証明書、および IP アドレスをエンドポイントから収集した後、その情報を ASA に送信します。ASA では、その情報は、企業所有のコンピュータ、個人用コンピュータ、パブリック コンピュータを区別するために使用されます。情報は、評価にも使用できます。詳細については、「評価」（P.5-3）を参照してください。

また、ホスト スキャンは、設定した DAP エンドポイント条件と照合して評価するために、以下の追加の値を自動的に返します。

- Microsoft Windows、Mac OS、Linux のビルド
- Microsoft Windows が実行されている接続ホスト上でアクティブなリスニング ポート
- 接続ホスト上にインストールされている CSD コンポーネント
- Microsoft サポート技術情報（KB）番号

DAP および Lua 表現の詳細については、「Dynamic Access Policies との統合」（P.5-10）および、『*Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*』の第 7 章「Using Match Criteria to Configure Dynamic Access Policies」を参照してください。

エンドポイント アセスメント

ホスト スキャン拡張機能であるエンドポイント アセスメントでは、アンチウイルスとアンチスパイウェアのアプリケーション、関連する定義の更新、およびファイアウォールの大規模なコレクションについて、リモート コンピュータを検査します。この機能を使用して、ASA によって特定の DAP がセッションに割り当てられる前に、要件を満たすようにエンドポイント条件を組み合わせることができます。DAP の詳細については、『*Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*』の第 7 章「Using Match Criteria to Configure Dynamic Access Policies」を参照してください。

Advanced Endpoint Assessment：アンチウイルス、アンチスパイウェア、およびファイアウォールの修復

ASA にインストールされた **Advanced Endpoint Assessment** ライセンスを購入すると、以下のホスト スキャンの高度な機能を使用できます。

修復

Windows、Mac OS X、および Linux のデスクトップでは、アンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォール保護のソフトウェアで別のアプリケーションが修復を開始することを許可している場合に、Advanced Endpoint Assessment は、それらのソフトウェアに関するさまざまな修復を開始しようとします。

アンチウイルス：Advanced Endpoint Assessment 機能は、アンチウイルス ソフトウェアの次のコンポーネントを修復できます。

- [Force File System Protection]：アンチウイルス ソフトウェアが無効の場合に、Advanced Endpoint Assessment はこのコンポーネントを有効にできます。
- [Force Virus Definitions Update]：アンチウイルス定義が Advanced Endpoint Assessment 設定で定義された日数内に更新されていない場合、Advanced Endpoint Assessment はウイルス定義のアップデートを開始できます。

アンチスパイウェア：アンチスパイウェア定義が Advanced Endpoint Assessment 設定で定義された日数内に更新されていない場合、Advanced Endpoint Assessment はアンチスパイウェア定義のアップデートを開始できます。

パーソナル ファイアウォール：ファイアウォール設定およびルールが Advanced Endpoint Assessment の設定で定義された要件を満たしていない場合、Advanced Endpoint Assessment モジュールは、それらを再設定しようとします。

- ファイアウォールは、有効または無効にできます。
- アプリケーションを実行、または実行できないようにできます。

- ポートをブロックまたは開くことができます。

（注）　すべてのパーソナル ファイアウォールがこの機能をサポートしているわけではありません。

エンド ユーザがアンチウイルスまたはパーソナル ファイアウォールを無効にする場合、VPN 接続が正常に確立された後、Advanced Endpoint Assessment 機能は約 60 秒以内にそのアプリケーションを再度有効にしようとします。

Windows モバイル デバイスの Lua 表現

Windows モバイル デバイスについて、管理者は Dynamic Access Policies（DAPs）で Lua 表現を作成し、モバイル デバイス固有の属性についてポスチャ チェックを実施きるようになります。これらの Lua 表現の例については、『*Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*』の第 7 章「Using Match Criteria to Configure Dynamic Access Policies」を参照してください。

ホスト スキャン サポート表

ホスト スキャン サポート表に、ポリシーで使用するアンチウイルス、アンチスパイウェア、およびファイアウォールのアプリケーションの製品名およびバージョン情報が記載されます。ホスト スキャンおよびホスト スキャン サポート表はホスト スキャン パッケージで提供されます。

AnyConnect Secure Mobility Client のこのリリースでは、ホスト スキャン パッケージは Cisco Secure Desktop（CSD）とは別にアップロードできます。これは、CSD をインストールしなくてもホスト スキャンの機能を展開できること、また、最新のホスト スキャン パッケージに更新することで、ホスト スキャン サポート表を更新できることを意味します。

ホスト スキャン サポート表は、cisco.com（http://www.cisco.com/en/US/products/ps10884/products_device_support_tables_list.html）からダウンロードできます。

これらのサポート表は、Microsoft Excel、Microsoft Excel Viewer、または OpenOffice を使用して表示できます。Firefox、Chrome、および Safari などのブラウザは、最高のダウンロード エクスペリエンスを実現します。

ホスト スキャン用のアンチウイルス アプリケーションの設定

アンチウイルス アプリケーションが、ポスチャ モジュールやホスト スキャン パッケージを含む一部のアプリケーションの動作を誤って悪意のあるものと判断する場合があります。ポスチャ モジュールまたはホスト スキャン パッケージをインストールする前に、以下のホスト スキャン アプリケーションをアンチウイルス ソフトウェアの「ホワイトリスト」に設定するか、セキュリティ例外を設けます。

- cscan.exe
- ciscod.exe
- cstub.exe

Dynamic Access Policies との統合

ASA では、ホスト スキャンの機能が Dynamic Access Policies（DAP）に統合されます。設定に応じて、ASA では、DAP 割り当ての条件として、オプションの AAA 属性値と組み合わせたエンドポイント属性値が 1 つ以上使用されます。DAP のエンドポイント属性でサポートされるホスト スキャンの機能には、OS 検出、ポリシー、基本ホスト スキャン結果、およびエンドポイント アセスメントがあります。

（注） ホスト スキャンの機能を有効にするには、AnyConnect Premium ライセンスを ASA にインストールする必要があります。

管理者は、セッションに DAP を割り当てるために必要な条件を構成する属性を、単独で、または組み合わせて指定できます。DAP により、エンドポイント AAA 属性値に適したレベルでネットワーク アクセスが提供されます。設定したエンドポイント条件がすべて満たされたときに、ASA によって DAP が適用されます。

（注） ASDM を使用して ASA で DAP を設定する方法の詳細については、ご使用の ASDM バージョンの『Adaptive Security Device Manager (ASDM) Configuration Guide』で、「Configuring Dynamic Access Policies」の章をご覧ください。

ポスチャ モジュールとスタンドアロン ホスト スキャン パッケージの相違点

AnyConnect ポスチャ モジュールは、ASA を使用してエンドポイントに展開できます。または、エンドポイントが ASA への初期接続を行う前に、事前展開キットを使用してエンドポイントにインストールできます。

ポスチャ モジュールには、ホスト スキャン パッケージ、評価、キーストローク ロガー検出、ホスト エミュレーション検出、キャッシュ クリーナ、およびホスト スキャン アプリケーションで必要なその他のモジュールがいくつか含まれます。ポスチャ モジュールを展開することにより、エンドポイントのユーザが管理者ではなくても、ホスト スキャンは特権動作を実行できます。また、その他の AnyConnect モジュールをホスト スキャンを使用して開始することもできます。

スタンドアロン ホスト スキャン パッケージは、ホスト スキャン エンジン、評価モジュール、キーストローク ロガー検出、およびホスト エミュレーション検出を提供します。

AnyConnect ポスチャ モジュールの依存関係およびシステム要件

AnyConnect ポスチャ モジュールには、ホスト スキャン パッケージやその他のコンポーネントが含まれています。

依存関係

AnyConnect Secure Mobility Client をポスチャ モジュールとともに使用するには、最低でも次のような ASA コンポーネントが必要です。

- ASA 8.4
- ASDM 6.4

次の AnyConnect 機能は、ポスチャ モジュールをインストールする必要があります。

- ホスト スキャン
- SCEP 認証
- AnyConnect テレメトリ モジュール

ホスト スキャン、CSD、および AnyConnect Secure Mobility Client の相互運用性

注意　AnyConnect Secure Mobility Client、バージョン 3.0.x でホスト スキャンを展開する場合、AnyConnect Secure Mobility Client では、ホスト スキャンのバージョン番号は同じか、それ以降にする必要があります。

Cisco Secure Desktop（CSD）バージョン 3.5 以前を ASA で有効にしていて、展開している AnyConnect Secure Mobility Client 3.0.x のバージョンに一致するまたはそれ以降のホスト スキャン パッケージにアップグレードしない場合、評価は失敗し、ユーザは VPN セッションを確立できません。ASA は、ASA で有効にされているホスト スキャン パッケージに一致するように、エンドポイントのホスト スキャン パッケージを自動的にダウングレードするため、AnyConnect 3.0.x ポスチャ モジュールがエンドポイントに事前展開されていても、この問題は発生します。

AnyConnect 3.0.x は旧バージョンのホスト スキャンまたは CSD と互換性はありませんが、旧バージョンの AnyConnect は新しいバージョンのホスト スキャン パッケージと互換性があります。たとえば、CSD 3.6 以前および AnyConnect 2.5.6 以前を使用していてホスト スキャン イメージを 3.0.8 以降にアップグレードする場合、評価は成功します。

システム要件

ポスチャ モジュールは、次のいずれかのプラットフォームにインストールできます。

- Windows XP（x86 版、および x64 環境で動作する x86 版）
- Windows Vista（x86 版、および x64 環境で動作する x86 版）
- Windows 7（x86 版、および x64 環境で動作する x86 版）
- Mac OS X 10.5、10.6、10.7 および 10.8（32 ビット版、および 64 ビット環境で動作する 32 ビット版）
- Linux（32 ビット版、および 64 ビット環境で動作する 32 ビット版）

（注）　ホスト スキャンは、32 ビット アプリケーションで、コア 32 ビット ライブラリを 64 ビット版 Linux オペレーティング システムにインストールする必要があります。ホスト スキャンは、インストールされた時点で、これらの 32 ビット ライブラリを提供しません。まだプロビジョニングしていない場合、お客様は自分で 32 ビット ライブラリをエンドポイントにインストールする必要があります。

- Windows Mobile

ライセンシング

ポスチャ モジュールには、次の AnyConnect ライセンシング要件があります。

- 基本ホスト スキャン、エンドポイント アセスメント、Advanced Endpoint Assessment などのホスト スキャンに同梱されたすべての機能に AnyConnect Premium ライセンスが必要です。
- Advanced Endpoint Assessment ライセンスは、以下の機能が必要とする追加のライセンスです。
  - 修復
  - モバイル デバイス管理

Advanced Endpoint Assessment をサポートするためのアクティベーション キーの入力

Advanced Endpoint Assessment には、Endpoint Assessment 機能のすべてが含まれており、バージョン要件を満たすために非準拠のコンピュータのアップデートを試行するように設定できます。次の手順に従い、Advanced Endpoint Assessment をサポートするために、シスコからキーを取得したら、ASDM を使用してキーのアクティベーションを行います。

ステップ 1　[Configuration] > [Device Management] > [Licensing] > [Activation Key] を選択します。

ステップ 2　[New Activation Key] フィールドにキーを入力します。

ステップ 3　[Update Activation Key] をクリックします。

ステップ 4　[File] > [Save Running Configuration to Flash] を選択します。

[Advanced Endpoint Assessment] エントリが表示され、[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Host Scan] ペインの [Host Scan Extensions] 領域内の [Configure] ボタンがアクティブになります。[Host Scan] ペインは、CSD が有効になっている場合に限りアクセスできます。

ホスト スキャン パッケージ

ASA へのホスト スキャン パッケージは次のいずれかの方法でロードできます。

- **hostscan-*version*-k9.pkg** は、スタンドアロン パッケージとしてアップロードできます。
- **anyconnect-win-*version*-k9.pkg** は、AnyConnect Secure Mobility パッケージをアップロードすることによって、アップロードできます。

- **csd_version-k9.pkg** は、Cisco Secure Desktop をアップロードすることによって、アップロードできます。

表 5-1　ASA にロードするホスト スキャン パッケージ

ファイル	説明
hostscan-*version*-k9.pkg	このファイルには、ホスト スキャン イメージ、ホスト スキャン サポート表、評価モジュール、キャッシュ クリーナ、キーストローク ロガー検出、ホスト エミュレーション検出が含まれています。
anyconnect-win-*version*-k9.pkg	このパッケージには、hostscan-*version*-k9.pkg ファイルなど、すべての AnyConnect Secure Mobility Client 機能が含まれています。
csd_*version*-k9.pkg	このファイルには、ホスト スキャン ソフトウェア、またホスト スキャン サポート表、Secure Desktop（Vault）、キャッシュ クリーナ、キーストローク ロガー検出、およびホスト エミュレーション検出などのすべての Cisco Secure Desktop 機能が含まれています。

複数のホスト スキャン イメージが ASA にロードされている場合に有効になるホスト スキャン イメージ

ホスト スキャン イメージは、ホスト スキャン パッケージに同梱されます。このイメージは、スタンドアロン ホスト スキャン パッケージ、完全な AnyConnect Secure Mobility Client パッケージ、および Cisco Secure Desktop からエンドポイントに展開できます。ASA にインストールしたライセンスの内容によっては、ASA にこれらのすべてのパッケージをロードできます。その場合、ASA は最初にホスト スキャン イメージとして指定したイメージを有効にし、イメージを指定していない場合は、Cisco Secure Desktop からホスト スキャン機能を有効にします。「ホスト スキャンのインストールまたはアップグレード」（P.5-15）を参照してください。

ホスト スキャン パッケージをアンインストールすると、ASA はそのホスト スキャン イメージを有効にできなくなります。

以下のシナリオは、複数ロードされた場合に、ASA が配布するホスト スキャン パッケージについて説明します。

- ASA にスタンドアロン ホスト スキャン パッケージをインストールし、それをホスト スキャン イメージとして指定して、CSD/hostscan を有効にしている場合、ASA はスタンドアロン ホスト スキャン パッケージを配布します。
- ASA にスタンドアロン ホスト スキャン パッケージをインストールして、それをホスト スキャン イメージとして指定し、また ASA に CSD イメージをインストールして、CSD/hostscan を有効にしている場合、ASA はスタンドアロン ホスト スキャン イメージを配布します。
- ASA にホスト スキャン イメージをインストールしたが、それを有効にはせず、また ASA に CSD イメージをインストールして、CSD/hostscan を有効にしている場合、ホスト スキャン イメージがアンインストールされていないため、ASA はスタンドアロン ホスト スキャン イメージを配布します。
- AnyConnect Secure Mobility Client パッケージを ASA にインストールし、それをホスト スキャン イメージと指定した場合、ホスト スキャン イメージはそのパッケージから配布されます。

- ASA に AnyConnect Secure Mobility Client パッケージ ファイルをインストールしたが、それをホスト スキャン イメージとして指定しない場合、ASA はその AnyConnect パッケージに関連付けられたホスト スキャン パッケージを配布しません。ASA は、CSD が有効であることを前提に、インストール済みのホスト スキャン パッケージまたは CSD パッケージを配布します。

AnyConnect ポスチャ モジュールおよびホスト スキャンの展開

ポスチャ モジュールおよびホスト スキャンには 2 種類の展開シナリオがあります。

事前展開：事前展開方式を使用する場合、エンドポイントが ASA への接続を確立しようとする前に、AnyConnect クライアントおよびポスチャ モジュールをインストールします。事前展開ポスチャ モジュール パッケージには、ポスチャ属性の収集に使用できるあらゆるコンポーネント、ライブラリ、サポート表、また「AnyConnect ポスチャ モジュールで有効になる機能」（P.5-3）に記載の機能を提供するアプリケーションが入っています。ASA にインストールされた同じバージョンの AnyConnect クライアントとポスチャ モジュールをエンドポイントに事前展開する場合、エンドポイントが ASA に接続するときに、追加のポスチャ モジュール ファイルは ASA からプッシュダウンされません。

Web 展開：Web 展開方式を使用する場合、エンドポイントが ASA に接続するときに ASA は AnyConnect クライアントとポスチャ モジュールをエンドポイントにプッシュダウンします。可能な限り短時間かつ効率的にダウンロードを実行するために、ASA は必須のポスチャ モジュール ファイルのみをダウンロードします。

エンドポイントが再接続すると、必須のポスチャ モジュール ファイルにより、エンドポイント アセスメントの実施に必要なその他のライブラリまたはファイルが判断され、それらのファイルが ASA から取得されます。たとえば、ポスチャ モジュールは、Norton アンチウイルスのあるバージョンがエンドポイントで実行されているために、すべての Norton アンチウイルス ソフトウェアのホスト スキャン サポート表を取得する場合があります。ポスチャ モジュールは必要とする追加ファイルを取得した後、エンドポイント アセスメントを実行し、ASA に属性を転送します。エンドポイント属性がダイナミック アクセス ポリシー（DAP）のルールを十分に満たすことを前提に、ASA はエンドポイントを接続させることができます。DAP を満たしたら、ASA は残りのポスチャ モジュールをエンドポイントにプッシュするかどうか設定できます。

ポスチャ モジュール全体をエンドポイントに Web 展開しない場合、制限付き Web 展開を実施できます。この場合、エンドポイントにはポスチャ ファイルが 1 つだけダウンロードされ、エンドポイント アセスメントの実施に必要なホスト スキャン ライブラリのみ要求されます。このシナリオでは、非常に短い時間で ASA からエンドポイントにダウンロードできますが、Advanced Endpoint Assessment を実行する機能やアンチウイルス、アンチスパイウェア、またはファイアウォールの修復タスクを実行する機能は使用できなくなります。

AnyConnect ポスチャ モジュールの事前展開

ポスチャ モジュールを事前展開する場合、AnyConnect クライアントが初めて ASA に接続する前に、エンドポイントにモジュールをインストールします。

ポスチャ モジュールをインストールする前に、AnyConnect Secure Mobility Client をエンドポイントにインストールする必要があります。Web 展開方式および事前展開方式を使用して、AnyConnect Secure Mobility Client およびポスチャ モジュールをインストールする手順については、第 2 章「AnyConnect Secure Mobility Client の展開」を参照してください。

表 5-2 に、ポスチャ モジュール事前展開キットを一覧表示します。

表 5-2　ポスチャ モジュール事前展開キット

ファイル	説明
Windows	anyconnect-posture-win-*version*-pre-deploy-k9.msi
Linux	anyconnect-linux-*version*-posture-k9.tar.gz
Mac OS X	anyconnect-macosx-posture-i386-*version*-i386-k9.dmg

ASA 上でのホスト スキャンのインストールと有効化

次のタスクでは、ASA 上でのホスト スキャンのインストールと有効化について説明します。

- ホスト スキャン エンジン最新版アップデートのダウンロード
- ホスト スキャンのインストールまたはアップグレード
- ASA でホスト スキャンを有効または無効にする
- ホスト スキャンのアンインストール
- AnyConnect ポスチャ モジュールのグループ ポリシーへの割り当て

ホスト スキャン エンジン最新版アップデートのダウンロード

Cisco Host Scan Engine の最新版アップデートをダウンロードするには、Cisco.com にユーザ登録する必要があります。

ステップ 1　Cisco VPN クライアント ツールのソフトウェア ダウンロード エリアに移動するには、このリンクをクリックします。

http://www.cisco.com/cisco/software/release.html?mdfid=282414594&flowid=4470&softwareid=282364364&release=Engine%20Updates&relind=AVAILABLE&rellifecycle=&reltype=latest

ステップ 2　製品ディレクトリ ツリーの [Latest Releases] を展開します。

ステップ 3　[Engine Updates] をクリックします。

ステップ 4　右のカラムで、最新版の **hostscan_3.0.xxxx-k9.pkg** を見つけ、[Download Now] をクリックします。

ステップ 5　cisco.com のクレデンシャルを入力し、[Login] をクリックします。

ステップ 6　[Proceed with Download] をクリックします。

ステップ 7　エンド ユーザ ライセンス契約書を読み、[Agree] をクリックします。

ステップ 8　ダウンロード マネージャ オプションを選択し、[download] リンクをクリックしてダウンロードを行います。

ホスト スキャンのインストールまたはアップグレード

次の手順を使用して、ASA 上で新しいホスト スキャン イメージをアップロードまたはアップグレードし、有効にすることができます。イメージを使用して AnyConnect のホスト スキャン機能を有効にするか、Cisco Secure Desktop（CSD）の既存の展開についてホスト スキャン サポート表をアップグレードします。

フィールドに、スタンドアロンのホスト スキャン パッケージ、または AnyConnect セキュア モビリティ クライアント パッケージのバージョン 3.0 以降を指定することができます。

以前に CSD イメージを ASA にアップロードしていた場合は、指定するホスト スキャン イメージによって、CSD パッケージに同梱されていた既存のホスト スキャン ファイルがアップグレードまたはダウングレードされます。

ホスト スキャンをインストールまたはアップグレードした後に、セキュリティ アプライアンスを再起動する必要はありませんが、ASDM の Secure Desktop Manager ツールにアクセスするには、Adaptive Security Device Manager（ASDM）を終了して再起動する必要があります。

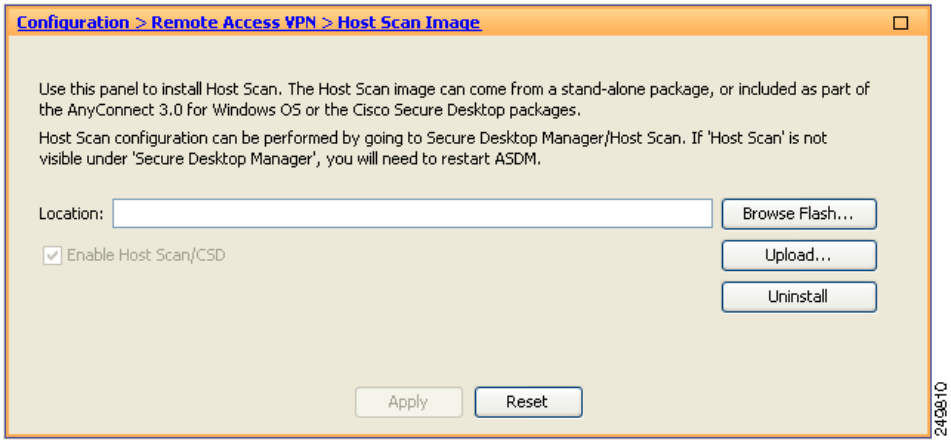
（注）　ホスト スキャンには、AnyConnect Secure Mobility Client Premium ライセンスが必要です。

ステップ 1　「ホスト スキャン エンジン最新版アップデートのダウンロード」（P.5-15）を使用して、最新版のホスト スキャン パッケージをダウンロードします。

（注）　ソフトウェアをダウンロードするには、Cisco.com のアカウントでログインする必要があります。

ステップ 2　ASDM を開き、[Configuration] > [Remote Access VPN] > [Host Scan Image] の順に選択します。[Host Scan Image] パネル（図 5-3）が開きます。

図 5-3　[Host Scan Image] パネル



ステップ 3　[Upload] をクリックして、ご使用のコンピュータから ASA 上のドライブにホスト スキャン パッケージのコピーを転送する準備をします。

ステップ 4　[Upload Image] ダイアログボックスで、[Browse Local Files] をクリックしてローカル コンピュータのホスト スキャン パッケージを検索します。

ステップ 5　ステップ 1 でダウンロードした **hostscan_*version*.pkg** ファイルまたは **anyconnect-win-*version*-k9.pkg** ファイルを選択し、[Select] をクリックします。[Local File Path] フィールドおよび [Flash File System Path] フィールドで選択したファイルのパスには、ホスト スキャン パッケージのアップロード先パスが反映されます。ASA に複数のフラッシュ ドライブがある場合は、別のフラッシュ ドライブを示すように [Flash File System Path] を編集できます。

ステップ 6　[Upload File] をクリックします。ASDM によって、ファイルのコピーがフラッシュ カードに転送されます。[Information] ダイアログボックスには、次のメッセージが表示されます。

```
File has been uploaded to flash successfully.
```

ステップ 7　[OK] をクリックします。

ステップ 8　[Use Uploaded Image] ダイアログで [OK] をクリックして、現行イメージとしてアップロードしたホスト スキャン パッケージ ファイルを使用します。

ステップ 9　[Enable Host Scan/CSD] がオンになっていない場合はオンにします。

ステップ 10　[Apply] をクリックします。

（注）　ASA 上で AnyConnect Essentials が有効になっている場合、ホスト スキャンと CSD は AnyConnect Essentials と組み合わせて動作しないというメッセージが表示されます。AnyConnect Essentials を**無効**にするか、**保持**するかを選択します。

ステップ 11　[Save] をクリックします。

ASA でホスト スキャンを有効または無効にする

ASDM を使用して初めてホスト スキャン イメージをインストールまたはアップグレードする場合は、手順の一部としてそのイメージを有効にします。「ASA 上でのホスト スキャンのインストールと有効化」（P.5-15）を参照してください。

それ以外の場合、ASDM を使用してホスト スキャン イメージを有効または無効にするには、次の手順を実行します。

ステップ 1　ASDM を開き、[Configuration] > [Remote Access VPN] > [Host Scan Image] の順に選択します。[Host Scan Image] パネル（図 5-3）が開きます。

ステップ 2　[Enable Host Scan/CSD] をオンにしてホスト スキャンを有効にするか、または [Enable Host Scan/CSD] をオフにしてホスト スキャンを無効にします。

ステップ 3　[Apply] をクリックします。

ステップ 4　[Save] をクリックします。

ASA 上での CSD の有効化または無効化

Cisco Secure Desktop（CSD）を有効にすると、CSD 設定ファイルおよび data.xml がフラッシュ デバイスから実行コンフィギュレーションにロードされます。CSD を無効にしても、CSD 設定は変更されません。

次の手順に従い、ASDM を使用して CSD を有効または無効にします。

ステップ 1　[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Setup] を選択します。

ASDM によって、[Setup] ペインが開きます（図 5-3）。

（注）　[Secure Desktop Image] フィールドに現在インストールされているイメージ（およびバージョン）が表示されます。[Enable Secure Desktop] チェックボックスは、CSD が有効になっているかどうかを示します。

ステップ 2　[Enable Secure Desktop] をオンにして CSD を有効にするか、[Enable Secure Desktop] をオフにして CSD を無効にします。

ステップ 3　[ASDM] を閉じます。次のメッセージがウィンドウに表示されます。

```
The configuration has been modified. Do you want to save the running configuration to
flash memory?
```

ステップ 4　[Save] をクリックします。ASDM は設定を保存して閉じます。

ホスト スキャンおよび CSD のアップグレードとダウングレード

パッケージがスタンドアロン ホスト スキャン パッケージ、AnyConnect Secure Mobility Client に同梱されたパッケージ、または Cisco Secure Desktop に同梱されたパッケージのいずれであっても、ASA は、有効なホスト スキャン パッケージを自動的にエンドポイントに配布します。エンドポイントに古いバージョンのホスト スキャン パッケージがインストールされている場合、エンドポイントのそのパッケージはアップグレードされます。エンドポイントに新しいバージョンのホスト スキャン パッケージがある場合、エンドポイントのそのパッケージはダウングレードされます。

ASA で有効にされたホスト スキャン イメージの判別

ASDM を開き、[Configuration] > [Remote Access VPN] > [Host Scan Image] の順に選択します。

[Host Scan Image Location] フィールドにホスト スキャン イメージが指定されており、[Enable HostScan/CSD] ボックスがオンになっている場合は、そのイメージのバージョンが ASA で使用されるホスト スキャン バージョンとなります。

[Host Scan Image] フィールドが空で、[Enable HostScan/CSD] ボックスがオンになっている場合は、[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] を選択します。[Secure Desktop Image Location] フィールドの CSD のバージョンが、ASA で使用されるホスト スキャン バージョンとなります。

ホスト スキャンのアンインストール

ホスト スキャン パッケージのアンインストール

ホスト スキャン パッケージをアンインストールすると、ASDM インターフェイス上のビューから削除されます。これにより、ホスト スキャンまたは CSD が有効の場合でも ASA によるホスト スキャン パッケージの展開が回避されます。ホスト スキャンをアンインストールしても、フラッシュ ドライブのホスト スキャン パッケージは削除されません。

セキュリティ アプライアンスのホスト スキャンをアンインストールするには、次の手順を使用します。

ステップ 1　ASDM を開き、[Configuration] > [Remote Access VPN] > [Host Scan Image] の順に選択します。

ステップ 2　[Host Scan Image] ペインで [Uninstall] をクリックします。ASDM では、[Location] テキスト ボックスのテキストが削除されます。

ステップ 3　[Save] をクリックします。

ASA からの CSD のアンインストール

Cisco Secure Desktop（CSD）をアンインストールすると、**フラッシュ カード上のデスクトップ ディレクトリから CSD 設定ファイルである data.xml が削除されます**。このファイルを保存する場合は、CSD をアンインストールする前に、別の名前を使用してファイルをコピーするか、ワークステーションにダウンロードします。

セキュリティ アプライアンスの CSD をアンインストールするには、次の手順を使用します。

ステップ 1　ASDM を開き、[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Setup] を選択します。

ASDM によって、[Setup] ペインが開きます（図 5-3）。

ステップ 2　[Uninstall] をクリックします。

次のメッセージが確認ウィンドウに表示されます。

```
Do you want to delete disk0:/csd_<n>.<n>.*.pkg and all CSD data files?
```

ステップ 3　[Yes] をクリックします。

ASDM によって、[Location] テキスト ボックスからテキストが削除され、[Setup] の下にある [Secure Desktop Manager] メニュー オプションが削除されます。

ステップ 4　[ASDM] を閉じます。次のメッセージがウィンドウに表示されます。

```
The configuration has been modified. Do you want to save the running configuration to
flash memory?
```

ステップ 5　[Save] をクリックします。ASDM は設定を保存して閉じます。

AnyConnect ポスチャ モジュールのグループ ポリシーへの割り当て

ステップ 1　ASDM を開き、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] の順に選択します。

ステップ 2　[Group Policies] パネルで [Add] をクリックして新規グループ ポリシーを作成するか、またはホスト スキャン パッケージを割り当てるグループ ポリシーを選択し、[Edit] をクリックします。

ステップ 3　[Edit Internal Group Policy] パネルで、左側の [Advanced] ナビゲーション ツリーを展開し、[AnyConnect Client] を選択します。

ステップ 4　[Optional Client Modules to Download Inherit] チェックボックスをオフにします。

ステップ 5　[Optional Client Modules to Download] ドロップダウン メニューで [AnyConnect Posture Module] をオンにし、[OK] をクリックします。

ステップ 6　[OK] をクリックします。

ホスト スキャン ロギング

ホスト スキャンは、Windows プラットフォームの場合イベント ビューアに、また Windows プラットフォーム以外の場合 syslog にログを記録します。イベント ビューアでは、すべてのログは、独自の「Cisco AnyConnect Secure Mobility Client Posture」フォルダに保存されます。

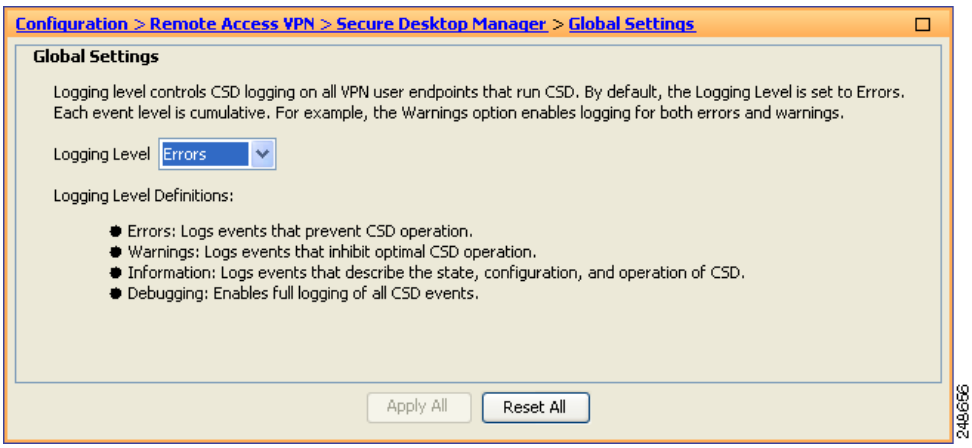
すべてのポスチャ モジュール コンポーネントのロギング レベルの設定

デフォルトでは、ポスチャ モジュール コンポーネントは、「エラー」の重大度レベル イベントを記録します。以下の手順を使用して、ポスチャ モジュールのすべてのコンポーネントのロギング重大度レベルを変更します。

ポスチャ モジュールは、ユーザのホーム フォルダに cscan.log ファイルをインストールします。cscan.log ファイルには、最後の VPN セッションからのエントリだけが表示されます。ユーザが ASA に接続するたびに、ホスト スキャンでは新しいロギング データでこのファイルのエントリを上書きします。

ポスチャのロギング レベルを表示または変更するには、次の手順に従います。

ステップ 1　ASDM インターフェイスから、[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Global Settings] を選択します。[Global Settings] パネルが開きます。



ステップ 2　ペイン内の [Logging Level Definitions] を参考に、[Logging Level] を設定します。

ステップ 3　実行コンフィギュレーションに加えられた変更を保存するには、[Apply All] をクリックします。

（注）　特定の接続プロファイルに対してホスト スキャンが無効になっている場合、その接続プロファイルを使用しているユーザにはホスト スキャンのロギングは実行されません。

ポスチャ モジュールのログ ファイルと場所

ポスチャ モジュール コンポーネントは、オペレーティング システム、特権レベル、権限レベル、起動メカニズム（Web 起動または AnyConnect）に基づいて、次に示す最大 3 つのログを出力します。

- cstub.log：AnyConnect Web 起動が使用されると、ロギングをキャプチャします。
- libcsd.log：ホスト スキャン API を使用する AnyConnect スレッドによって作成されます。ログ レベル設定に応じて、このログにデバッグのエントリが入力される場合があります。
- cscan.log：スキャン実行ファイル（cscan.exe）により作成される、ポスチャおよびホスト スキャンのメイン ログです。ログ レベル設定に応じて、このログにデバッグのエントリが入力される場合があります。

ポスチャ モジュールは、これらのログ ファイルをユーザのホーム フォルダに配置します。場所は、オペレーティング システムおよび VPN 方式によって異なります。

Cisco Technical Assistant Center（TAC）は、必要な場合に、これらのログ ファイルを使用して問題をデバッグします。お客様がこれらのファイルを確認する必要はありません。Cisco TAC では、これらのログ ファイルを必要とする場合に、DART バンドルを使用してそれらのファイルを提供するようにお客様に依頼することがあります。DART ユーティリティは、必要なすべての AnyConnect 設定とログ ファイルを収集し、圧縮ファイルに保存して TAC に送信します。DART の詳細については、「DART を使用したトラブルシューティング情報の収集」（P.13-4）を参照してください。

BIOS シリアル番号の DAP での使用

ホスト スキャンは、ホストの BIOS シリアル番号を取得できます。ダイナミック アクセス ポリシー（DAP）を使用して、その BIOS シリアル番号に基づいて ASA への VPN 接続を可能または回避できます。

DAP エンドポイント属性としての BIOS の指定

ステップ 1　ASDM にログオンします。

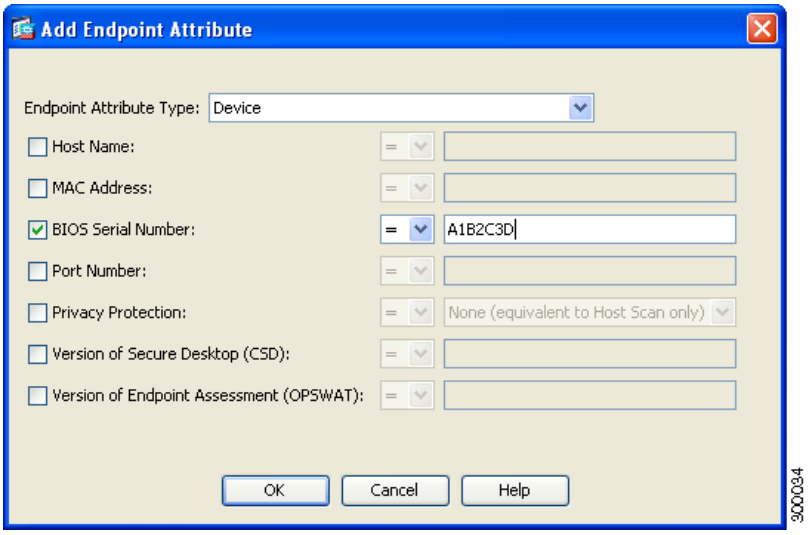
ステップ 2　[Configuration] > [Remote Access VPN] > [Network (Client) Access] を選択するか、[Clientless SSL VPN Access] > [Dynamic Access Policies] を選択します。

ステップ 3　[Configure Dynamic Access Policies] パネルで、[Add] または [Edit] をクリックして、BIOS を DAP エンドポイント属性として設定します。

ステップ 4　エンドポイント ID 表の右にある [Add] をクリックします。

ステップ 5　[Endpoint Attribute Type] フィールドで [Device] を選択します。

ステップ 6　[BIOS Serial Number] チェックボックスをオンにし、[=]（等しい）または [!=]（等しくない）を選択して、[BIOS Serial Number] フィールドに BIOS 番号を入力します。



ステップ 7　[OK] をクリックし、[Endpoint Attribute] ダイアログボックスでの変更を保存します。

ステップ 8　[OK] をクリックして、[Edit Dynamic Access Policy] への変更を保存します。

ステップ 9　[Apply] をクリックして、ダイナミック アクセス ポリシーへの変更を保存します。

ステップ 10　[Save] をクリックします。

BIOS シリアル番号の取得方法

次のリソースでは、さまざまなエンドポイントの BIOS シリアル番号の取得方法について説明しています。

- Windows：http://support.microsoft.com/kb/558124
- Mac OS X：http://support.apple.com/kb/ht1529
- Linux：次のコマンドを使用します。

```
/usr/bin/hal-get-property --udi /org/freedesktop/Hal/devices/computer --key
system.hardware.serial
```