ポスチャの設定

AnyConnect Secure Mobility Client は VPN ポスチャ（HostScan）モジュールおよび ISE ポスチャ モジュールを提供します。両方のモジュールにより、Cisco AnyConnect Secure Mobility Client で、ホストにインストールされたアンチウイルス、アンチスパイウェア、ファイアウォール ソフトウェアなどについてエンドポイントのコンプライアンスを評価できます。その後、エンドポイントがコンプライアンスに対応するまでネットワーク アクセスを制限したり、修復方法を確立できるようにローカル ユーザの権限を強化したりできます。

VPN ポスチャは、hostscan_version.pkg にバインドされています。これは、どのようなオペレーティング システム、アンチウイルス、アンチスパイウェア、およびソフトウェアがホストにインストールされているかを収集するアプリケーションです。ISE ポスチャは、ISE 制御ネットワークにアクセスするときに、AnyConnect と NAC Agent の両方を展開するのではなく、1 つのクライアントを展開します。ISE ポスチャは、AnyConnect 製品に（Web セキュリティやネットワーク アクセス マネージャなどと同じように）追加のセキュリティ コンポーネントとしてインストールできるモジュールです。リリース 3.x の AnyConnect バンドルの一部であった HostScan は、別個にインストールされるようになりました。

ISE ポスチャは、クライアント側評価を実行します。クライアントは、ヘッドエンドからポスチャ要件ポリシーを受信し、ポスチャ データ収集を実行し、結果をポリシーと比較し、評価結果をヘッドエンドに返します。エンドポイントがコンプライアンス対応かどうかを実際には ISE が判断する場合でも、ISE はエンドポイント独自のポリシー評価を利用します。

一方、HostScan はサーバ側評価を実行します。ASA がエンドポイント属性（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）のリストのみを要求し、これらが HostScan によって返されます。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。

（注） 2 つの異なるポスチャ エージェントを実行すると予期しない結果が生じる可能性があるため、HostScan と ISE ポスチャ エージェントの組み合わせは推奨されません。

次のポスチャチェックは、HostScan ではサポートされていますが、ISE ポスチャではサポートされていません。ホスト名、IP アドレス、MAC アドレス、ポート番号、OPSWAT バージョン、BIOS シリアル番号、および証明書フィールド属性です。

ISE ポスチャ モジュールの提供内容

ポスチャ チェック

ISE ポスチャ モジュールはポスチャ チェックの実行に OPSWAT v3 または v4 ライブラリを使用します。初回のポスチャ チェックでは、すべての必須要件への一致に失敗したエンドポイントがすべて非準拠と見なされます。その他のエンドポイントの許可ステータスは、ポスチャ不明または準拠（必須要件に合致）です。

（注） macOS 64 ビットの移行では、AnyConnect 4.6 ISE ポスチャ モジュールは古い OPSWAT v3 準拠モジュールと互換性がありません。

ポスチャ チェック フェーズでエラーが発生し、AnyConnect が続行可能な場合、ユーザに通知されますが、可能な場合はポスチャのチェックが続行されます。必須のポスチャ チェック中にエラーが発生した場合、チェックは失敗とマークされます。ネットワーク アクセスは、すべての必須要件が満たされている場合に許可されます。そうでない場合、ユーザはポスチャ プロセスをリスタートできます。

必要な修復

修復ウィンドウはバックグラウンドで実行されるため、ネットワーク アクティビティのアップデートはポップアップ表示されず、干渉や中断は発生しません。AnyConnect UI の ISE ポスチャ タイル部分で [詳細（Details）] をクリックして、検出された内容およびネットワークに参加する前に必要なアップデート内容を確認できます。必須の手動修復が存在する場合、修復ウィンドウが開き、対処が必要な項目が表示されます。このシステム スキャンのウィンドウに、アップデートの進捗状況、割り当てられたアップデート時間の残り時間、すべての要件のステータス、およびシステムの準拠状態が表示されます。

（注） 昇格された権限を必要とするアプリケーションは、管理者以外のユーザアカウントでのみ自動修復を使用します。管理者アカウントでは、修復を手動で実行する必要があります。

（注） 昇格権限を必要とするポスチャ チェックおよび修復は、サーバが信頼されている場合にのみ実行されます。

オプションのアップデートのみが残っている場合、[スキップ（Skip）] を選択して次の更新に進むことも、[すべてスキップ（Skip All）] を選択して残りの修復をすべて無視することも可能です。時間を節約するためにオプションの修復をスキップしても、ネットワーク アクセスは維持されます。

修復後（または修復が必要でない場合は要件チェック後）、アクセプタブル ユース ポリシーの通知を受け取る場合があります。この場合、ネットワーク アクセスのポリシーに同意する必要があり、同意しなかった場合はアクセスが制限されます。修復のこの部分では、AnyConnect UI のポスチャ タイル部分に、「システム スキャン：ネットワークのアクセプタブル ユース ポリシー（System Scan: Network Acceptable Use Policy）」と表示されます。

修復が完了すると、必須アップデートとしてリストされたチェック項目がすべて[完了（Done）] ステータスとなり、緑色のチェックボックスが表示されます。修復後、エージェントはISEにポスチャ結果を送信します。

パッチ管理チェックと修復

AnyConnect 4.x および Microsoft System Center Configuration Manager（SCCM）の統合により、パッチ管理チェックとパッチ管理修復が導入されました。エンドポイントで欠落している重要なパッチのステータスをチェックし、ソフトウェアパッチをトリガーするべきかどうか確認します。重要なパッチが Windows エンドポイントで欠落していない場合は、パッチ管理チェックは合格です。パッチ管理修復は、管理者レベルのユーザのみに対して、1つ以上の重要なパッチが Windows エンドポイントで欠落しているときにのみトリガーされます。

SCCM クライアントで、再起動前にインストールが行われるパッチをインストールすると、マシンが再起動するとすぐに、パッチのインストール ステータス（インストール完了または未インストール）がレポートされます。ただし、SCCM クライアントで、再起動後にインストールが開始されるパッチをインストールすると、パッチのステータスはすぐにはレポートされません。

AnyConnect コンプライアンス モジュールは、この時点で SCCM クライアントにステータスの提供を強制できません。ポスチャ モジュール クライアントがネイティブ API 要求を完了するためにかかる時間は、さまざまな動的 OS パラメータ（CPU 負荷、保留中のパッチの量、パッチ インストール後の再起動なしなど）と、ネットワークの要因（ポスチャ モジュール クライアントとサーバ間の接続と遅延）に依存します。SCCM クライアントが応答するまで待機する必要があるかもしれませんが、既知のパッチによる一部のテスト結果は約 10 分でした。

同様の動作は、Windows Server Update Services（WSUS）の検索 API でも見られ、応答時間は長めで、20 ～ 30 分かかることもあります。Windows アップデートは、Windows OS だけでなく、すべてのマイクロソフト製品（Microsoft Office など）についてパッチの不足がないかチェックします。

ISE のポリシー状態の設定方法については「Policy Conditions」を参照してください。またパッチ管理修復の詳細については「Patch Management Remediation」を参照してください。

エンドポイント コンプライアンスの再評価

エンドポイントがコンプライアンス対応と見なされ、ネットワーク アクセスが許可されると、管理者が設定した制御に基づいてエンドポイントを任意で定期的に再評価できます。パッシブ再評価ポスチャ チェックは、初期のポスチャ チェックとは異なります。失敗した場合、ユーザには修復するオプションが与えられます（管理者がそのように設定していた場合）。この構成設定では、1 つ以上の必須要件が満たされていない場合でも、ユーザが信頼ネットワーク アクセスを維持するかどうかを制御します。初期のポスチャ評価では、すべての必須要件が満たされていないと、エンドポイントはコンプライアンス非対応と見なされます。この機能はデフォルトでは無効であり、ユーザ ロールに対して有効になっている場合、ポスチャは 1 ～ 24 時間ごとに再評価されます。

管理者は、結果を [続行（Continue）]、[ログオフ（Logoff）]、または [修復（Remediate）] に設定し、適用や猶予時間など他のオプションを設定できます。

ISE の UI を使用すると、AnyConnect ポスチャ プロファイルに表示される情報メッセージを作成できます。ボタンのテキストとリンクは、カスタマイズも可能です。

非準拠デバイスの猶予期間

Cisco ISE の UI で猶予期間を設定することができます。これを設定すると、以前のポスチャ ステータスでは準拠していたが準拠しなくなったエンドポイントに、ネットワークへのアクセスを許可できるようになります。Cisco ISE は、以前に認識された良好な状態をキャッシュ内で探し、デバイスに猶予時間を提供します。猶予期間が終了すると、AnyConnect は再度ポスチャ チェックを行いますが、今回は修復を行いません。チェックの結果に基づいてエンドポイントの状態を準拠または非準拠と判断します。

（注） デバイスが猶予期間にあるがポスチャ ポリシーで更新されると、次のようになります。

- （猶予期間が延長された場合）、以前の猶予期間が経過するか、またはデバイスが Cisco ISE から削除されたときに、新しい猶予期間が適用されます。
- （猶予期間が短縮された場合）、デバイスが再びポスチャ フロー プロセスを通過した場合にのみ、新しい猶予期間がデバイスに適用されます。

猶予期間は、一時的なエージェント、ハードウェアのインベントリ、アプリケーションのモニタリングには適用されません。

ユーザが猶予期間にいる場合は、定期的な再評価（PRA）は適用されません。

（それぞれ異なる猶予期間を設定した）複数のポスチャ ポリシーにデバイスが一致する場合、それらの異なるポリシーで設定された最大の猶予期間がデバイスに与えられます。

デバイスが猶予期間に移行すると、アクセプタブル ユース ポリシー（AUP）は表示されません。

猶予期間は、ISE UI で **[ポリシー（Policy）] > [ポスチャ（Posture）] または [ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポスチャポリシー（Posture Policy）]** の順に移動して、AnyConnect ポスチャ プロファイルに設定します。有効な値は、日、時間、または分単位で指定します。デフォルトでは、この設定は無効です。

柔軟な通知

猶予期間の特定の割合が経過するまでカスタム通知ウィンドウの表示を遅らせるには、遅延通知のオプションを使用します。たとえば、ISE UI の [Delay Notification（遅延の通知）] フィールドが 50 % に設定され、設定されている猶予期間が 10 分の場合、AnyConnect ISE ポスチャは5分後にエンドポイントを再スキャンし、エンドポイントに違反があると検出した場合は通知ウィンドウを表示します。エンドポイントのステータスが準拠している場合、通知ウィンドウは表示されません。通知遅延期間が0 % に設定されている場合は、猶予期間の開始時に直ちに問題の解決を促すメッセージが表示されます。エンドポイントは、猶予期間の有効期限が切れるまで、アクセスが許可されます。

カスタム通知が ISE UI で設定されている場合にのみ、エンドポイントが準拠していないと AnyConnect UI に警告が表示されます。通知は、猶予期間の開始および猶予期間の開始後に準拠していないエンドポイントに対しても示されます。AnyConnect システム スキャン タイルにはすべてのポスチャ障害が強調表示され、[再度スキャン（Scan Again）] ボタンを押すと、ポスチャ ポリシーの再実行を強制して完全なネットワーク アクセスを維持できます。

（注） [再度スキャン（Scan Again）] オプションが表示されるようにするには、[再スキャンボタンを有効にする（Enable Rescan Button）] オプションを [有効（Enabled）] に設定する必要があります。

修復フローでは、問題を解決するまで基本的にアクセスがブロックされます。一時的なアクセスは、使用可能ではありません。猶予期間フローでは、遅延アクセスの取得により、問題を解決するための猶予期間が提供されます。柔軟な通知フローの[**ブラウザを起動**（Launch Browser）]オプションをクリックすると、サーバが信頼できる場合は、ブラウザを起動することができます。ブラウザ オプションでは、ポスチャ ポリシーへの準拠に関する詳細を取得できます。

シスコ テンポラル エージェント

シスコ テンポラル エージェントは、ユーザが信頼ネットワークにアクセスしているときにコンプライアンス ステータスを共有できるように、Windows または macOS 環境向けに設計されています。シスコ テンポラル エージェントの設定は、ISE UI で行います。シスコ テンポラル エージェントの実行ファイル .exe（Windows 用）または dmg（macOS 用）は、エンドポイントがインターネットへのアクセスを試行するたび、エンドポイントにダウンロードされます。ユーザは、ダウンロードした実行ファイルまたは dmg を実行し、コンプライアンス チェックを行う必要があります。これには、管理者権限は不要です。

UI が自動的に起動し、エンドポイントのコンプライアンスに問題がないか判断するチェックを開始します。コンプライアンス チェックが完了すると、ISE は、ISE UI でのポリシーの設定方法に基づいて必要なアクションを取れるようになります。

Windows では、実行ファイルは自己解凍されます。この解凍により、コンプライアンス チェックに必要なすべての dll およびその他のファイルが一時フォルダに保存されます。解凍されたファイルおよび実行ファイルは、コンプライアンス チェックの完了後、削除されます。ファイルおよび実行ファイルを完全に削除するには、ユーザが UI を終了する必要があります。

ISE UI での詳細な設定手順については、『*Cisco Identity Services Engine Administrator Guide, Release 2.3*』の「Cisco Temporal Agent Workflows」を参照してください。

シスコ テンポラル エージェントの制限事項

- macOS では、VLAN 制御のポスチャ環境は、ルート権限がないと更新アダプタ（DHCP 更新）プロセスが実行されないため、テンポラル エージェントについてはサポートされていません。テンポラル エージェントはユーザ プロセスとしてのみ実行できます。ACL 制御のポスチャ環境は、エンドポイントの IP を更新する必要がないため、サポートされています。
- 修復中にネットワーク インターフェイスが発生した場合、ユーザは、現在の UI を終了して手順全体をやり直す必要があります。
- macOS では、dmg ファイルは削除されません。
- テンポラル エージェント インストーラは、起動後、エンドポイントでの実行中にブラウザの背後に隠れてしまうことがあります。テンポラル エージェント アプリケーションでのヘルス情報の収集を続行するには、エンドユーザは、ブラウザを最小化する必要があります。この問題は、主に Windows 10 ユーザで発生します。理由は、これらのクライアントでは、高いセキュリティ条件で実行されるサードパーティ アプリケーションを許容するため、UAC モードが「高」に設定されていることです。

- エンドポイントでステルス モードが有効になっている場合は、テンポラル エージェントを使用できません。
- 次の状態は、シスコ テンポラル エージェントではサポートされていません。
  - サービス状態（macOS）：システム デーモンのチェック
  - サービス状態（macOS）：デーモンまたはユーザ エージェントのチェック
  - PM：Up to Date チェック
  - PM：有効化チェック
  - DE：暗号化の場所に基づくチェック

オプション モードのポスチャ ポリシー拡張機能

必須の要件チェックの成否に関係なく、オプション モードで失敗した要件チェックの修復を実行できます。修復に関するメッセージは、AnyConnect ISE ポスチャ UI に表示され、失敗の内容と必要な修復アクションを確認することが可能です。

- オプション モードの手動修復：[システムスキャンのサマリー（System Scan Summary）] 画面には、条件が満たされない場合に修復が必要な可能性がある、オプション モードのステータスが表示されます。[開始（Start）] を手動でクリックして修復するか、[スキップ（Skip）] をクリックします。これらはオプションの要件にすぎないため、修復が失敗しても、エンドポイントはコンプライアンス対応です。[システム サマリー（System Summary）] に、スキップされたのか、失敗したのか、成功したのかが表示されます。
- オプション モードの自動修復：オプションのアップデートの適用時、[システム スキャン（System Scan）] タイルの表示内容を監視できます。修復は自動的に実行されるため、修復を開始するか確認されません。いずれかの自動修復が失敗すると、修復を試行できなかったというメッセージが表示されます。さらに、必要に応じて、修復アクションをスキップできます。

ハードウェア インベントリの可視性

ISE UI の [コンテキストの可視性（Context Visibility）] の下に、[エンドポイント（Endpoints）] > [ハードウェア（Hardware）] タブが追加されました。これは、エンドポイント ハードウェアの情報を短時間で収集、分析、および報告するのに役立ちます。メモリ容量が小さいエンドポイントの検出や、エンドポイントのBIOSモデル/バージョンの検出など、情報を収集することができます。検出結果に基づいて、メモリ容量を増やしたり、BIOS のバージョンをアップグレードしたり、資産の購入を計画する前に要件を評価したりすることができます。[メーカー使用状況（Manufacturers Utilization）] ダッシュレットには、Windows または macOS のエンドポイントのハードウェア インベントリの詳細が表示されます。[エンドポイント使用状況（Endpoint Utilizations）] ダッシュレットには、エンドポイントの CPU、メモリ、およびディスクの使用状況が表示されます。詳細については、『Cisco Identity Services Engine Administrator Guide, Release 2.3』の「The Hardware Tab」を参照してください。

ステルス モード

管理者は、AnyConnect UI タイルをエンド ユーザ クライアントに対して非表示にしている間に、ISE ポスチャを設定できます。ポップアップは表示されないので、ユーザによる設定を必要とするどのシナリオでも、デフォルトのアクションが実行されます。この機能は、Windows および Mac オペレーティング システムで使用できます。

『Cisco Identity Services Engine Administrator Guide』の「*Configure Posture Policies*」の項を参照してください。ここでは、クライアントレス状態を無効または有効にしてステルス モードを設定します。

ISE UI では、エンド ユーザにエラー通知が表示されるようにステルス モードで通知を有効にするよう設定できます。

ISE ポスチャ プロファイル エディタ（16 ページ）でプロファイルをマッピングし、AnyConnect 設定を ISE の [クライアント プロビジョニング（Client Provisioning）] ページにマッピングすると、AnyConnect は、ポスチャ プロファイルを読み込んで目的のモードに設定し、最初のポスチャ要求中に選択されたモードに関する情報を ISE に送信できます。モードと、ID グループ、OS、コンプライアンス モジュールなどのその他の要因に基づいて、Cisco ISE は適切なポリシーをマッチングします。

『Cisco Identity Services Engine Administrator Guide』でステルス モードの展開とその影響について参照してください。

ISE ポスチャでは、ステルス モードで次の機能を設定することはできません。

- すべての手動修復
- リンク修復
- ファイル修復
- WSUS 表示 UI 修復
- アクティブ化 GUI 修復
- AUP ポリシー

ポスチャ ポリシーの適用

エンドポイントにインストールされているソフトウェアの全体的な可視性を改善するために、シスコは次のポスチャ拡張機能を提供しました。

- エンドポイントのファイアウォール製品の状態をチェックして、その製品が実行されているかどうか確認できます。必要に応じて、ファイアウォールを有効にし、最初のポスチャ中や定期的な再評価（PRA）中にポリシーを適用できます。設定するには、『Cisco Identity Services Engine Configuration Guide』の「*Firewall Condition Settings*」の項を参照してください。
- 同様に、エンドポイントにインストールされているアプリケーションのクエリを実行できます。不要なアプリケーションが実行中またはインストールされている場合は、アプリ

ケーションを停止するか、不要なアプリケーションをアンインストールできます。設定するには、ISE UI で、『Cisco Identity Services Engine Configuration Guide』の「*Application Remediation*」の項を参照してください。

UDID 統合

AnyConnect は、デバイスにインストールされていると、AnyConnect のすべてのモジュール間で共有される独自の一意の ID（UDID）を持ちます。この UDID は、エンドポイントの ID であり、エンドポイント属性として保存されるため、MAC アドレスではなく特定のエンドポイントでのポスチャ制御が保証されます。その後は、UDID に基づいてエンドポイントをクエリすることができます。UDID は定数で、エンドポイントの状況（接続、アップグレード、アンインストールなど）に関係なく変化しません。ISE UI の [コンテキスト表示（Context Visibility）] ページ（**[コンテキスト表示（Context Visibility）] > [エンドポイント（Endpoints）] > [コンプライアンス（Compliance）]**）は、複数の NIC を持つエンドポイントについて、複数のエントリではなく 1 つのエントリを表示できます。

アプリケーション監視

ポスチャ クライアントは、動的な変化を監視し、ポリシー サーバに報告できるように、さまざまなエンドポイント属性を継続的に監視できます。ポスチャ ポリシーの設定に応じて、インストールされるアプリケーションや、アプリケーションが実行するアンチスパイウェア、アンチウイルス、アンチマルウェア、ファイアウォールなどのさまざまな属性を監視できます。アプリケーションの条件設定の詳細については、『Cisco Identity Services Engine Administrator Guide』の「*Continuous Endpoint Attribute Monitoring*」の項を参照してください。

USB ストレージ デバイス検出

USB 大容量ストレージ デバイスを Windows エンド ポイントに接続すると、ポスチャ クライアントはそのデバイスを検出し、ポスチャ ポリシー ブロックに応じて、デバイスをブロックしたり許可したりすることができます。エージェントは USB 検出を使用して、同じ ISE 制御ネットワークにある限り、継続的にエンドポイントをモニタします。この期間内に、条件に一致する USB デバイスを接続した場合、指定した修復アクションが実行されます。インシデントは、ポリシー サーバにも報告されます。

USB ストレージ検出は、OPSWAT v4 コンプライアンス モジュールに依存しています。[ワーク センター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [USB] で、ISE UI の定期再評価ポリシー（PRA）の USB チェックを設定する必要があります。

（注） チェックと修復は順番に実行されるため、その他のチェックの PRA 猶予時間を最小限の値に設定することによって、USB チェックの処理での遅延を防止できます。猶予時間は、[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [設定（Settings）] > [再評価設定（Reassessment Config）] の ISE UI で設定されます。

ISE UI で USB ストレージの検出を設定する手順については、「USB Mass Storage Check Workflow」を参照してください。

自動コンプライアンス

ポスチャ リースにより、ISE サーバは、ポスチャを完全にスキップし、簡単にシステムを準拠状態にすることができます。この機能により、ユーザは、自分のシステムが最近ポスチャされている場合に、ネットワーク間の切り替えによる遅延を感じることがありません。ISE ポスチャ エージェントは、単に、ISE サーバが検出されたすぐ後に、システムが準拠しているかどうかを示すステータス メッセージを UI に送信します。ISE の UI（[設定（Settings）] > [ポスチャ（Posture）] > [一般設定（General Settings）]）で、最初のコンプライアンス チェックの後にエンドポイントがポスチャ準拠と見なされる時間を指定できます。ユーザがある通信インターフェイスから別の通信インターフェイスに切り替えた場合でも、コンプライアンス ステータスは維持されることが予期されています。

（注） ポスチャ リースでは、ISE でセッションが有効な場合に、エンドポイントがポスチャ不明状態から準拠状態に移行することが予期されます。

VLAN のモニタリングと遷移

サイトによっては、異なる VLAN またはサブネットを使用して、企業グループおよびアクセス レベル用にネットワークを分割しています。ISE からの認可変更（CoA）では、VLAN の変更を指定します。変更は、セッション終了など管理者のアクションによって発生することもあります。有線接続中の VLAN 変更をサポートするには、ISE ポスチャ プロファイルに次の設定を行います。

- [VLAN 検出間隔（VLAN Detection Interval）]：エージェントが VLAN の遷移を検出する頻度およびモニタリングを無効にするかどうかを決定します。VLAN モニタリングは、この間隔が 0 以外の値に設定されている場合に有効になります。Mac OS X の場合、この値は 5 以上に設定します。

  VLAN モニタリングは Windows と Mac OS X の両方に実装されていますが、Mac では予期しない VLAN 変更を検出するためにのみ必要です。VPN が接続される場合、または acise（メインの AnyConnect ISE プロセス）が実行されていない場合は、自動的に無効になります。有効な値の範囲は 0 ～ 900 秒です。

- [エージェント IP 更新の有効化（Enable Agent IP Refresh）]：オフにすると、ISE はエージェントに [ネットワーク遷移遅延（Network Transition Delay）] 値を送信します。オンにすると、ISE はエージェントに DHCP リリースおよび更新の値を送信し、エージェントは IP 更新を行って最新の IP アドレスを取得します。

- [DHCP リリース遅延（DHCP release delay）] と [DHCP 更新遅延（DHCP renew delay）]：IP 更新および [エージェント IP 更新の有効化（Enable Agent IP Refresh）] 設定との相関で使用されます。[エージェント IP 更新の有効化（Enable Agent IP Refresh）] チェックボック

スをオンにし、この値が 0 でない場合、エージェントはリリース遅延秒数を待機し、IP アドレスを更新し、更新遅延秒数を待機します。VPN が接続されている場合、IP 更新は自動的に無効になります。4 連続でプローブがドロップされると、DHCP 更新がトリガーされます。

- [ネットワーク遷移遅延（Network Transition Delay）]：（[エージェント IP 更新の有効化（Enable Agent IP Refresh）] チェックボックスで）VLAN モニタリングがエージェントによって無効または有効にされた場合に使用されます。この遅延により、VLAN が使用されていない場合にはバッファが追加され、サーバからの正確なステータスを待機する十分な時間がエージェントに与えられます。ISE はエージェントにこの値を送信します。また、ISE UI のグローバル設定に [ネットワーク遷移遅延（Network Transition Delay）] 値を設定した場合、ISE ポスチャ プロファイル エディタの値でその値が上書きされます。

（注） ASA は VLAN 変更をサポートしないため、クライアントが ASA を介して ISE に接続されているときには、これらの設定は適用されません。

トラブルシューティング

ポスチャの完了後にエンドポイントデバイスがネットワークにアクセスできない場合は、次の点を確認してください。

- VLAN 変更は ISE UI で設定されていますか。
  - 設定されている場合、DHCP リリース遅延および更新遅延がプロファイルに設定されていますか。
  - どちらの設定も 0 の場合、[ネットワーク遷移遅延（Network Transition Delay）] がプロファイルに設定されていますか。

AnyConnect ISE フローを中断する操作

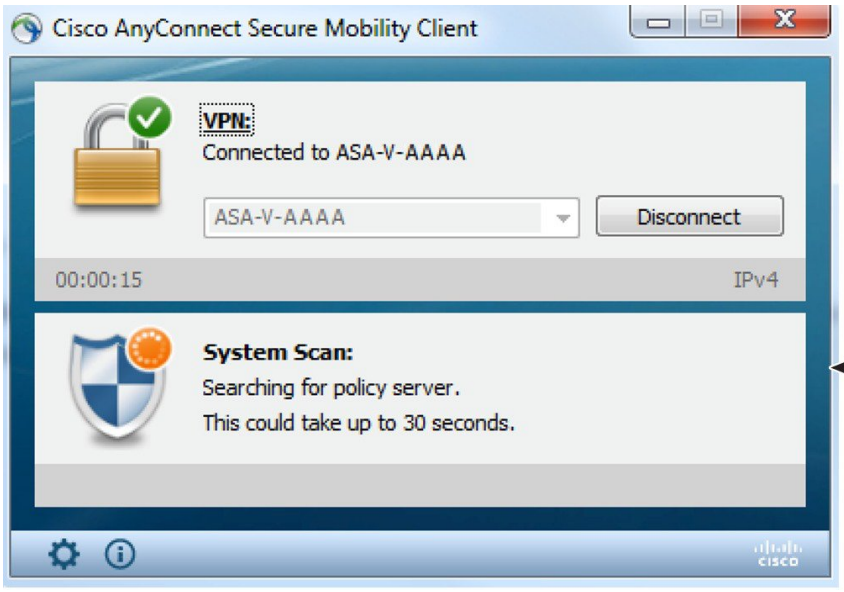
さまざまな理由から、AnyConnect ISE ポスチャ フローは最初のポスチャ再アセスメントまたはパッシブ再アセスメント中に中断されることがあります。

- ユーザが AnyConnect ISE をキャンセルする：ポスチャのチェックと修復の期間に、ユーザは AnyConnect ISE をキャンセルできます。UI にはキャンセルが進行中であることがただちに通知されますが、これはエンドポイントを問題のある状態にすることを回避するときにだけ発生します。サードパーティ ソフトウェアを使用している場合、キャンセル操作によってはリブートが必要な場合があります。キャンセル後、AnyConnect UI のポスチャ タイル部分には、準拠状態が示されます。
- 修復タイマーが期限切れになる：ポスチャ要件を満たすための管理者制御時間が終了しました。アセスメント レポートがヘッドエンドに送信されます。パッシブ再アセスメント時には、ユーザはネットワーク アクセスを保持し、ポスチャ アセスメントでは、必須要件すべてが満たされた場合にネットワーク アクセスが許可されます。

- ポスチャ チェック中のエラー：ポスチャ チェック フェーズでエラーが発生し、AnyConnect が続行可能な場合、ユーザに通知されますが、可能な場合はポスチャのチェックが続行されます。必須のポスチャ チェック中にエラーが発生した場合、チェックは失敗とマークされます。ネットワーク アクセスは、すべての必須要件が満たされている場合に許可されます。そうでない場合、ユーザはポスチャ プロセスをリスタートできます。
- 修復中のエラー：修復フェーズでエラーが発生し、AnyConnect ISE ポスチャが続行可能な場合は、ユーザに通知されます。失敗した修復ステップが必須のポスチャ要件と関連付けられている場合、AnyConnect ISE ポスチャは修復プロセスを停止します。失敗した修正ステップがオプションのポスチャの要件に関連付けられている場合は、次のステップに進んで ISE ポスチャ操作を終了しようとします。ネットワーク アクセスは、すべての必須要件が満たされている場合に許可されます。そうでない場合、ユーザはポスチャ プロセスをリスタートできます。
- デフォルト ゲートウェイの変更：デフォルト ゲートウェイに対する変更により、ユーザが信頼ネットワークへのアクセスを失う場合があります。これにより、ISE ポスチャは ISE の再検出を試みます。AnyConnect UI の ISE ポスチャ タイル部分では、再検出モードに入ると ISE ポスチャのステータスが表示されます。
- AnyConnect と ISE 間の接続の喪失：エンドポイントが準拠状態と見なされてネットワーク アクセスが許可された後に、さまざまなネットワーク シナリオが発生する可能性があります。エンドポイントがネットワーク接続を完全に失う場合があります。ISE がダウンする場合があります。ISE ポスチャが失敗する場合があります（セッション タイムアウト、手動リスタートなどによる）。ASA の背後の ISE が VPN トンネルを喪失する場合があります。
- ISE ポスチャを使用している場合、1 つの macOS エンドポイントに複数のコンソール ユーザをログインさせることはできません。

ISE ポスチャのステータス

AnyConnect ISE ポスチャが機能し、想定どおりにネットワーク アクセスをブロックしている場合に、AnyConnect UI の [ISE ポスチャ（ISE Posture）] タイルに [システム スキャン：ポリシー サーバを検索しています（System Scan: Searching for policy server）] と表示されます。Windows タスク マネージャまたは Mac OS X システム ログには、プロセスが実行中であると示される場合があります。サービスが実行されていない場合は、AnyConnect UI の [ISE ポスチャ（ISE Posture）] タイルに [システム スキャン：サービスは使用できません（System Scan: Service is unavailable）] と表示されます。



ネットワークを変更すると、検出フェーズが開始されます。AnyConnect ISE ポスチャの場合、プライマリ インターフェイスのデフォルト ルートが変更された場合、エージェントが検出プロセスに戻ります。たとえば、WiFi およびプライマリ LAN が接続された場合、エージェントは検出をリスタートします。同様に、WiFi およびプライマリ LAN が接続されたものの、その後、WiFi の接続が解除された場合、エージェントは検出をリスタートしません。

また、「システム スキャン」後、AnyConnect UI の [ISE ポスチャ（ISE Posture）] タイルに次のステータス メッセージが表示される場合があります。

- [限定的または接続なし（Limited or no connectivity）]：接続がないため検出は発生していません。AnyConnect ISE ポスチャ エージェントは、ネットワーク上の不正なエンドポイントで検出を実行している可能性があります。
- [システム スキャンは現在の WiFi では不要（System scan not required on current WiFi）]：セキュアでない WiFi が検出されたため検出は発生していません。AnyConnect ISE ポスチャ エージェントは、LAN、ワイヤレス（802.1X 認証が使用されている場合）、および VPN でのみ検出を開始します。WiFi がセキュアでないか、またはエージェント プロファイルで OperateOnNonDot1XWireless を 1 に設定してこの機能を無効にしています。
- [不正なポリシー サーバ（Unauthorized policy server）]：ネットワーク アクセスが制限されているか存在しないため、ホストが ISE ネットワークのサーバ名ルールに一致していません。
- [AnyConnect ダウンローダが更新を実行しています…（The AnyConnect Downloader is performing update...）]：ダウンローダが呼び出され、パッケージ バージョンを比較し、AnyConnect 設定をダウンロードし、必要なアップグレードを行います。
- [システムをスキャンしています...（Scanning System...）]：アンチウイルス/アンチスパイウェアのセキュリティ製品のスキャンが開始されました。このプロセス中にネットワークが変更された場合、エージェントはログ ファイルの生成プロセスをリサイクルし、ステータスは [検出されたポリシー サーバなし（No policy server detected）] に戻ります。

- [AnyConnect スキャンのバイパス（Bypassing AnyConnect scan）]：ネットワークは、Cisco NAC Agent を使用するように設定されています。
- [ユーザによってキャンセルされた信頼できないポリシー サーバ（Untrusted Policy Server Cancelled by the user）]：AnyConnect UI の [システム スキャン プリファレンス（System Scan Preferences）] タブで信頼できないサーバへの接続のブロックを解除すると、ポップアップ ウィンドウに AnyConnect ダウンローダのセキュリティ警告が表示されます。この警告ページで [接続のキャンセル（Cancel Connection）] をクリックすると、[ISE ポスチャ（ISE Posture）] タイルがこのステータスに変わります。
- [ネットワークの利用規定（Network Acceptable Use Policy）]：ネットワークへのアクセスには、アクセプタブル ユース ポリシーを確認し、受け入れる必要があります。ポリシーを拒否すると、ネットワーク アクセスが制限される可能性があります。
- [ネットワーク設定の更新（Updating Network Settings）]：ISE UI の [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）] では、ネットワーク遷移間で発生させる遅延の秒数を指定できます。
- [コンプライアンス非対応。更新時間の期限が切れました。（Not Compliant. Update time expired.）]：修復のために設定された時間の期限が切れました。
- [コンプライアンス対応。ネットワーク アクセスが許可されています。（Compliant. Network access allowed.）]：修復が完了しました。[システム スキャン（System Scan）] > [スキャン概要（Scan Summary）] にも、ステータスが完了と示されます。
- [検出されたポリシー サーバなし（No policy server detected）]：ISE ネットワークが見つかりません。30 秒後、エージェントによるプローブは低下します。デフォルトのネットワーク アクセスが有効になります。

ポスチャとマルチホーミング

AnyConnect ISE ポスチャ モジュールは、マルチホーミングをサポートしていません。これは、そのようなシナリオの動作が定義されていないためです。たとえば、メディアが有線からワイヤレスに変更された後で有線に戻ると、エンドポイントが実際には有線接続でリダイレクトされている場合でも、ユーザには ISE ポスチャ モジュールに準拠したポスチャ ステータスが表示されることがあります。

エンドポイントの同時ユーザ

AnyConnect ISE は、複数のユーザが同時にエンドポイントにログインしてネットワーク接続を共有した場合、個別のポスチャ評価をサポートしません。最初に AnyConnect ISE を実行したユーザが正常にポスチャされ、エンドポイントに信頼ネットワーク アクセスが許可されると、エンドポイントの他のすべてのユーザがネットワーク アクセスを継承します。これを防ぐため、管理者はエンドポイントに同時ユーザを許可する機能を無効にできます。

ポスチャ モジュールのロギング

ISE ポスチャの場合、イベントはネイティブ オペレーティング システムのイベント ログ（Windows イベント ログ ビューアまたは Mac OS X システム ログ）に記録されます。

VPN ポスチャ（HostScan）の場合、エラーおよび警告は syslog（Windows 以外の場合）とイベント ビューア（Windows の場合）に送信されます。使用可能なすべてのメッセージがログ ファイルに記録されます。

VPN ポスチャ（HostScan）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、および起動メカニズム（Web 起動または AnyConnect）に基づいて、次の 3 つのログに出力します。

- cstub.log：AnyConnect Web 起動が使用された場合にログを取り込みます。
- libcsd.log：VPN ポスチャ 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ます。
- cscan.log：スキャニング実行可能ファイル（cscan.exe）によって作成される、VPN ポスチャのメインのログです。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ます。

ポスチャ モジュールのログ ファイルと場所

ISE ポスチャの場合、イベントはインストールされた AnyConnect バージョンの独自のサブフォルダに含まれているため、AnyConnect イベントの他の部分から容易に分離できます。各ビューアでは、キーワードの検索およびフィルタリングが可能です。Web Agent イベントは、標準のアプリケーション ログに書き込まれます。

トラブルシューティングのために、ISE ポスチャ要件ポリシーとアセスメント レポートがイベント ログではなく、エンドポイントの別の難解化されたファイルに記録されます。一部のログ ファイル サイズ（aciseposture など）は、管理者がプロファイルに設定できますが、UI ログ サイズは事前に定義されています。

プロセスが異常終了したときは、他の AnyConnect モジュールと同じように、常にミニ ダンプ ファイルが生成されます。

VPN ポスチャ（HostScan）の場合、ファイルはユーザのホーム フォルダの次のディレクトリにあります。

- （Windows 以外）：.cisco/hostscan/log
- （Windows）：C:\Users\<user_name>\AppData\Local\Cisco HostScan\log\cscan.log

ISE ポスチャ プロファイル エディタ

管理者は、ポスチャプロファイルを作成し、ISE にアップロードするために、このスタンドアロンエディタを使用することを選択できます。それ以外の場合、組み込みのポスチャ プロファイル エディタが ISE UI の [ポリシー要素（Policy Elements）] に設定されます。AnyConnect コンフィギュレーション エディタが ISE で起動すると、AnyConnect ソフトウェアおよび関連するモジュール、プロファイル、OPSWAT、およびカスタマイズを備えた AnyConnect 設定が作成されます。ASA の ISE ポスチャ用のスタンドアロン プロファイル エディタには、次のパラメータが含まれています。

- **エージェントの動作**
  - [署名チェックの有効化（Enable signature check）]：オンにすると、エージェントによって実行される前に実行可能ファイルの署名チェックが有効になります。
  - [ログ ファイル サイズ（Log file size）]：エージェント ログ ファイルの最大サイズ。有効な値は 5 ～ 200 MB です。
  - [修復タイマー（Remediation timer）]：コンプライアンス非対応とタグ付けされるまでにユーザが修復に割くことができる時間。有効な値は 1 ～ 300 分です。
  - [エージェント ログ トレースの有効化（Enable agent log trace）]：エージェントでのデバッグ ログを有効にします。
  - [非 802.1X ワイヤレス ネットワークでの動作（Operate on non-802.1X wireless networks）]：オンにすると、エージェントは非 802.1X ワイヤレス ネットワークで動作できます。
  - [ステルス モードを有効にする（Enable Stealth Mode）]：ユーザによる設定を行わなくてもポスチャをサービスとして実行できるステルス モードを有効にするかどうかを選択します。
  - [通知によるステルスを有効にする（Enable Stealth With Notification）]：ステルス モードの通知が有効に設定されている場合、エンド ユーザは、AnyConnect ステルス モードが非準拠の状態にある、ネットワーク アクセスが制限されている、到達不能なサーバなどがあるなどの場合でも通知メッセージを受け取ります。
  - [再スキャンボタンを有効にする（Enable Rescan Button）]：障害発生後、手動修復後、ポスチャの動作不能時（など）に、ポスチャ（またはディスカバリ）を再起動する場合は、このボタンを有効にして、[システムスキャン（System Scan）] タイルに **[再度スキャン（Scan Again）]** の選択が表示されるようにします。このオプションは、ISE ポスチャ プロファイルで表示または非表示にできます。**[再度スキャン（Scan Again）]** をクリックすると、ディスカバリが起動し、ポスチャ フロー全体が開始されます。

（注） [再度スキャン（Scan Again）] がタイルに表示されるのは、ポスチャ プロファイルで EnableRescan タグを 1 に設定している場合だけです。0 に設定すると、[再度スキャン（Scan Again）] ボタンが表示されるのは、それが（このオプションよりも先に）表示されていた場合だけです。

（注） ISE 側でプロファイルの変更が発生すると、次回ディスカバリが起動されるときに、その変更が AnyConnect タイルに反映されます。

- [UACポップアップを無効にする（Disable UAC Popup）]：ポリシー検証中に Windows ユーザ アカウント制御（UAC）ポップアップが表示されるかどうかを決定します。デフォルト値（オフ）では、エンドユーザは引き続き接続時に管理者権限を求められます。有効にすると、ポリシーの検証中に Windows ユーザ アカウント制御（UAC）プロンプトが表示されません。UACプロンプトをオフにすることによって、AnyConnect ポスチャは「管理者として実行（Run as administrator）」ではなく、特権昇格のシステム プロセスを使用します。UAC プロンプトを無効にする前に、ユーザにローカル管理者権限があるデバイスでポスチャ ポリシーを検証します。
- [バックオフ タイマーの制限（Backoff Timer Limit）]：AnyConnect が ISE 検出のプローブを送信する最長時間を入力します。プローブによりトラフィックが増えるため、ネットワークの負荷にならない値を選択してください。
- [定期プローブ間隔（Periodic Probe Interval）]：バックオフ タイマーの制限を超えた後の検出プローブの間隔を指定します。AnyConnect は、有効な ISE サーバが見つかるまで、指定された間隔で定期的なプローブを送信します。デフォルトでは 30 分で、プローブは、初回プローブの完了後、30 分間隔で継続的に送信されます。値を 0 に設定すると、定期的なプローブがディセーブルになります。

• IP アドレスの変更

最適なユーザ エクスペリエンスのため、次の値を推奨値に設定してください。

- [VLAN 検出間隔（VLAN detection interval）]：クライアント IP アドレスを更新する前にエージェントが VLAN 変更の検出を試みる間隔。有効な範囲は 0 ～ 900 秒で、推奨値は 5 秒です。
- [ping または ARP（Ping or ARP）]：IP アドレスの変更を検出する方法。推奨設定は ARP です。
- [ping の最大タイムアウト（Maximum timeout for ping）]：1 ～ 10 秒の ping タイムアウト。

- [エージェント IP 更新の有効化（Enable agent IP refresh）]：VLAN 変更の検出を有効にする場合にオンにします。
- [DHCP 更新遅延（DHCP renew delay）]：IP 更新後にエージェントが待機する秒数。[エージェント IP 更新の有効化（Enable Agent IP Refresh）] を有効にしたときに、この値を設定します。この値が 0 ではない場合、エージェントはこの予期される遷移中に IP を更新します。更新中に VPN が検出された場合、更新は無効です。有効な値は 0 ～ 60 秒で、推奨値は 5 秒です。
- [DHCP リリース遅延（DHCP release delay）]：エージェントによる IP 更新を遅延させる秒数。[エージェント IP 更新の有効化（Enable Agent IP Refresh）] を有効にしたときに、この値を設定します。この値が 0 ではない場合、エージェントはこの予期される遷移中に IP を更新します。更新中に VPN が検出された場合、更新は無効です。有効な値は 0 ～ 60 秒で、推奨値は 5 秒です。
- [ネットワーク遷移遅延（Network transition delay）]：計画された IP 変更を待機できるようにエージェントがネットワーク モニタリングを一時停止する期間（秒単位）。推奨値は 5 秒です。

- **ポスチャ プロトコル**
  - [ホストの検索（Discovery host）]：エージェントが接続できるサーバ。スタンドアロン プロファイル エディタでは、1 つのホストのみを入力します。
  - [サーバ名ルール（Server name rules）]：エージェントが接続できるサーバを定義する、ワイルドカード対応のカンマで区切られた名前のリスト（.cisco.com など）。
  - [Call Home リスト（Call Home List）]：ロード バランシング、ルックアップのモニタリングとトラブルシューティングに使用する FQDN、またはそのノードでデフォルトのポリシー サービス ノード（PSN）にマップする DNS の FQDN（複数シナリオの場合）を入力します。これを設定すると、ルックアップのモニタリングとトラブルシューティングついての最初のプローブは Call Home に送信されます。リダイレクト ネットワークから非リダイレクト ネットワークに移行するときにこれを設定する必要があります。
  - [PRA 再送信時間（PRA retransmission time）]：パッシブ再評価の通信障害が発生した場合に、このエージェントが再試行する間隔を指定します。有効な値の範囲は 60 ～ 3600 秒です。

[詳細（Advanced）] パネル

AnyConnect Secure Mobility Client UI の [詳細（Advanced）] パネルは、コンポーネントの統計情報、ユーザ プリファレンス、およびコンポーネント固有のその他の情報を表示するための各コンポーネントの領域です。AnyConnect システム トレイで、[すべてのコンポーネントの詳細ウィンドウ（Advanced Window for all components）] アイコンをクリックすると、新しい [システム スキャン（System Scan）] セクションに次のタブが含まれます。

（注） macOS では、これらの統計情報、ユーザ設定、メッセージ履歴などは、[統計情報（Statistics）] ウィンドウの下に表示されます。プリファレンスは、[プリファレンス（Preferences）] ウィンドウに表示され、Windows のようなタブの向きではありません。

- [プリファレンス（Preferences）]：信頼できないサーバへの接続をブロックできます。ダウンローダのプロセス中に、証明書が信頼できず検証されていない ISE サーバに対して、「信頼できないサーバをブロックしました（Untrusted Server Blocked）」というメッセージを受信します。ブロッキングを無効にすると、AnyConnect は悪意がある可能性があるネットワーク デバイスへの接続をブロックしなくなります。
- [統計情報（Statistics）]：現在の ISE ポスチャ ステータス（準拠または未準拠）、OPSWAT のバージョン情報、アクセプタブル ユース ポリシーのステータス、ポスチャの最新の実行タイム スタンプ、不足要件、およびトラブルシューティングの目的で表示するのに十分重要であると考えられるその他の統計情報を提供します。
- [セキュリティ製品（Security Products）]：システムにインストールされているマルウェア対策製品のリストにアクセスします。
- [スキャンの概要（Scan Summary）]：管理者がユーザに対して表示するように設定したポスチャ項目をユーザが確認できるようにします。たとえば、設定されている場合、ユーザはシステム上にポスチャされたすべての項目を表示したり、ポスチャ チェックに失敗して修復が必要な項目のみを表示したりすることができます。
- [メッセージ履歴（Message History）]：コンポーネントについて、システム トレイに送信されたすべてのステータス メッセージの履歴を表示します。この履歴は、トラブルシューティングに役立ちます。

VPN ポスチャ（HostScan）モジュールの提供内容

HostScan

HostScan 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。HostScan は、基本モジュール、Endpoint Assessment モジュール、および Advanced Endpoint Assessment モジュールで構成されています。

（注） AnyConnect リリース 3.x では、このパッケージは hostscan_version.pkg ファイルにバンドルされ、HostScan が機能するためには ASA の HostScan イメージ下で更新されて有効化される必要がありました。現在は、独立したインストールです。

基本的機能

HostScan は自動的に Cisco クライアントレス SSL VPN または AnyConnect VPN クライアント セッションを確立しているリモート デバイスのオペレーティング システムとサービス パック を識別します。

特定のプロセス、ファイル、およびレジストリ キーについて、エンドポイントを検査するように HostScan を設定することもできます。HostScan は、トンネルが完全に確立される前にこれらのすべての検査を実行し、この情報を ASA に送信して、会社所有、個人用、および公共のコンピュータを識別します。この情報は、評価にも使用できます。

（注） ログイン前の評価および証明書情報の返送は実行できません。HostScan は認証方式ではありません。HotScan は、接続しようとしているデバイスの内容を検証するチェックを実行するだけです。

また、HostScan 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、次の追加の値を自動的に返します。

- Microsoft Windows、Mac OS、および Linux オペレーティング システム
- Microsoft サポート技術情報（KB）番号
- デバイス エンドポイント属性タイプ（ホスト名、MAC アドレス、BIOS シリアル番号、ポート番号（レガシー属性）、TCP/UDP ポート番号、プライバシー保護、およびエンドポイント アセスメント（OPSWAT）のバージョンなど）。

（注） HostScan は Windows クライアント システム上の Microsoft のソフトウェア アップデートに関するサービス リリース（GDR）の情報を収集します。サービス リリースには複数のホットフィックスが含まれます。サービス リリース エンドポイント属性は、ホット フィックスではなく、DAP ルールに使用されます。

エンドポイント アセスメント

エンドポイント アセスメントは、HostScan の拡張機能であり、多くの種類の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について、リモート コンピュータを検査します。ASA によって特定のダイナミック アクセス ポリシー（DAP）がセッションに割り当てられる前に、この機能を使用して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。

詳細については、適切なバージョンの『Cisco ASA Series VPN Configuration Guide』の「*Dynamic Access Policies*」の項を参照してください。

Advanced Endpoint Assessment：マルウェア対策およびファイアウォールの修復

Windows、macOS、および Linux のデスクトップでは、マルウェア対策およびパーソナル 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。

マルウェア対策：Advanced Endpoint Assessment は、マルウェア対策ソフトウェアの以下のコンポーネントを修復しようとします。

- ファイル システム保護の強制：マルウェア対策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します。
- ウイルス定義更新の強制：Advanced Endpoint Assessment の設定で定義された日数の間、マルウェア対策定義が更新されなかった場合に、Advanced Endpoint Assessment はウイルス定義の更新を開始しようとします。

パーソナル ファイアウォール：Advanced Endpoint Assessment モジュールでは、ファイアウォールを有効または無効にすることができます。

HostScan バージョン 4.4 は、パーソナル ファイアウォールを使用するアプリケーションとポートのブロックまたは許可をサポートしていません。

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

HostScan 用のアンチマルウェア アプリケーションの設定

VPN ポスチャ（HostScan）モジュールをインストールする前に、アンチマルウェア ソフトウェアを「ホワイトリスト」に設定するか、または、次の各アプリケーションについてセキュリティ例外を作成します。アンチマルウェア アプリケーションは、これらのアプリケーションの動作を悪意があるものと誤って認識する場合があります。

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

ダイナミック アクセス ポリシーとの統合

ASA では、HostScan の機能がダイナミック アクセス ポリシー（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 HostScan の機能には、OS 検出、ポリシー、基本結果、およびエンドポイント アセスメントがあります。

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。

『Cisco ASA Series VPN Configuration Guide』の「*Configure Dynamic Access Policies*」の項を参照してください。

DAP の BIOS シリアル番号

VPN ポスチャ（HostScan）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、その BIOS シリアル番号に基づいて ASA への VPN 接続を許可または拒否できます。

DAP エンドポイント属性としての BIOS の指定

手順

ステップ 1 ASDM にログインします。

ステップ 2 **[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）]** または **[クライアントレス SSL VPN アクセス（Clientless SSL VPN Access）] > [ダイナミック アクセス ポリシー（Dynamic Access Policies）]** を選択します。

ステップ 3 [ダイナミック アクセス ポリシーの設定（Configure Dynamic Access Policies）] パネルで、[追加（Add）] または [編集（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 [追加（Add）] をクリックします。

ステップ 5 [エンドポイント属性タイプ（Endpoint Attribute Type）] フィールドで、[デバイス（Device）] を選択します。

ステップ 6 [BIOS シリアル番号（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 シリアル番号（BIOS Serial Number）] フィールドに BIOS 番号を入力します。[OK] をクリックし、[エンドポイント属性（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 7 [OK] をクリックして、[ダイナミック アクセス ポリシーの編集（Edit Dynamic Access Policy）] への変更を保存します。

ステップ 8 [適用（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 9 [保存（Save）] をクリックします。

BIOS シリアル番号の取得方法

- Windows：http://support.microsoft.com/kb/558124

- Mac OS X：http://support.apple.com/kb/ht1529
- Linux：このコマンドを使用してください。

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

ASA で有効にされたホスト スキャン イメージの判別

ASDM を開いて [設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ホスト スキャン イメージ（HostScan Image）] を選択します。

HostScan のアップグレード

AnyConnect および HostScan を手動で（msiexec を使用して）アップグレードする場合は、必ず、AnyConnect を最初にアップグレードして、その後に HostScan をアップグレードしてください。

OPSWAT サポート

AnyConnect の VPN（HostScan）ポスチャ モジュールも ISE ポスチャ モジュールも、OPSWAT フレームワークを使用して、エンドポイントを保護します。

クライアントとヘッドエンドの両方を伴うこのフレームワークは、エンドポイント上のサードパーティ アプリケーションを評価するのに役立ちます。クライアントとヘッドエンドで使用されている OPSWAT のバージョンは、一致する必要があります。ポスチャ方式ごとに、サポート表が用意されています。使用される OPSWAT バージョンによって認識されるアプリケーションのリストに、製品およびバージョン情報を記載しています。

ヘッドエンド（ASA または ISE）とエンドポイント（VPN ポスチャまたは ISE ポスチャ）との間にバージョン番号の不一致があるときは、ヘッドエンドのバージョンに合わせて、OPSWAT 準拠モジュールがアップグレードまたはダウングレードされます。これらのアップグレード/ダウングレードは必須であり、ヘッドエンドへの接続が確立されるとすぐにエンドユーザの介入なしで自動的に実行されます。

VPN HostScan ポスチャ OPSWAT サポート

「HostScan サポート表」は、ASA ヘッドエンドで動作する AnyConnect に HostScan ポスチャを提供する HostScan パッケージ バージョンに対応しています。

HostScan は、AnyConnect メジャー リリースおよびメンテナンス リリースと連携するようにバージョン管理されます。ASDM で HostScan パッケージを設定するときに、HostScan バージョンを指定します。[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [セキュアデスクトップマネージャ（Secure Desktop Manager）] > [ホストスキャンイメージ（Host Scan Image）] の順に選択してください。

VPN HostScan ポスチャのガイドライン：

- HostScan 4.3.x までの全バージョンが OPSWAT v2 を使用します。HostScan 4.6x 以降は、OPSWAT v4 を使用します。OPSWAT v3 は、HostScan のどのバージョンでもサポートされていません。
- AnyConnect 4.4.x および 4.5.x は、HostScan バージョン 4.3.05017 以降をサポートしています。HostScan には、4.4.x や 4.5.x バージョンはありません。
- AnyConnect 4.6.x は、HostScan 4.3.05050（およびそれ以降の 4.3.x バージョン）と、4.6.x バージョンをサポートしています。
- AnyConnect 4.7.x は、HostScan 4.3.05050（およびそれ以降の 4.3.x バージョン）と、4.7.x バージョンをサポートしています。
- 基盤となる OPSWAT バージョンの変更に伴い、移行プロセスを完了して HostScan 4.3.x から 4.6.x 以降にアップグレードする必要があります。4.6.x 以降の HostScan イメージをロードして移行を開始するときには、ASDM 7.9.2 以降と HostScan バージョン 4.3.05050（またはそれ以降の 4.3.x バージョン）がヘッドエンドにインストールされている必要があります。

HostScan 4.3.05017 以降で使用される OPSWAT バージョンについては、次の表で詳しく説明します。互換性のある AnyConnect リリース、ASA/ASDM ヘッドエンド要件、および有効なダウングレード/アップグレード操作も記載して、VPN/HostScan ポスチャのために連携する製品の関係を示します。

OPSWAT バージョン	サポートされている HostScan バージョン	AnyConnect の互換性のあるバージョン	ASA/ASDM ヘッドエンドの必要なバージョン	ダウングレード/アップグレード操作
v2	4.3.05017 から 4.3.05050 まで	AnyConnect 4.4.x および 4.5x	AnyConnect をサポートするすべてのリリース。	以前の任意の 4.3.x HostScan リリースにダウングレードします。 以降の任意の 4.3.x HostScan リリースにアップグレードします。
	4.3.05050 およびそれ以降のすべての 4.3.x バージョン。	AnyConnect 4.4.x、4.5.x、および 4.6.x	AnyConnect をサポートするすべてのリリース。	以前の任意の 4.3.x HostScan リリースにダウングレードします。 以降の任意の 4.3.x HostScan リリースにアップグレードします。 （注） 任意の 4.6.x HostScan リリースにアップグレードするには、移行プロセスが必要です。 移行プロセスでは、HostScan 4.3.05050（またはそれ以降の 4.3.x バージョン）がヘッドエンドにインストールされている必要があります。

OPSWAT バージョン	サポートされている HostScan バージョン	AnyConnect の互換性のあるバージョン	ASA/ASDM ヘッドエンドの必要なバージョン	ダウングレード/アップグレード操作
v4	4.6.x	AnyConnect 4.4.x、4.5.x、および 4.6.x	ASDM 7.9.2 以降で AnyConnect をサポートするすべての ASA リリース。	以前の任意の 4.6.x バージョンにダウングレードします。 移行元の 4.3.x HS リリースへのダウングレードに必要なフォールバック プロセス。 以降の任意のリリースにアップグレードします。
	4.7.x	AnyConnect 4.4.x、4.5.x、4.6.x、および 4.7.x	ASDM 7.9.2 以降で AnyConnect をサポートするすべての ASA リリース。	以前の任意の 4.7.x バージョンにダウングレードします。 移行元の 4.3.x HS リリースへのダウングレードに必要なフォールバック プロセス。 以降の任意のリリースにアップグレードします。

ISE ポスチャ OPSWAT サポート

「Cisco AnyConnect エージェント準拠モジュール」は、ISE ポスチャ モジュール用です。

ISE エージェント準拠モジュールのバージョンには、基盤となる OPSWAT バージョンが反映されています。ISE ポスチャでは、OPSWAT バイナリは別個のインストーラにパッケージ化されています。OPSWAT ライブラリをローカル ファイル システムから ISE ヘッドエンドに手動でロードしたり、ISE 更新フィード URL を使用して直接取得するように ISE を設定したりできます。

AnyConnect リリース 4.3 以降を ISE 2.1 以降とともに使用したときは、ISE 準拠モジュールに OPSWAT v3 または v4 のどちらを使用するか選択できます。アンチマルウェアの設定は、[ワーク センター（Work Centers）] > [ポスチャ（Posture）] > [ポスチャ要素（Posture Elements）] > [条件（Conditions）] > [アンチマルウェア（Antimalware）] の ISE UI で行います。