コンプライアンス

- ポスチャ サービス （2 ページ）
- ポスチャ管理の設定 （9 ページ）
- ポスチャの全般設定 （18 ページ）
- Cisco ISE へのポスチャ更新のダウンロード （20 ページ）
- ポスチャの利用規定の構成設定 （21 ページ）
- ポスチャ評価の利用規定の設定 （24 ページ）
- ポスチャ条件 （24 ページ）
- 単純ポスチャ条件 （24 ページ）
- 単純ポスチャ条件の作成 （25 ページ）
- 複合ポスチャ条件 （26 ページ）
- Windows クライアントでの自動アップデートを有効にするための事前定義の条件 （27 ページ）
- 事前設定済みアンチウイルスおよびアンチスパイウェア条件 （28 ページ）
- アンチウイルスとアンチスパイウェア サポート表 （28 ページ）
- インライン ポスチャ ノード （29 ページ）
- コンプライアンス モジュール （30 ページ）
- ポスチャ コンプライアンスのチェック （32 ページ）
- 複合ポスチャ条件の作成 （32 ページ）
- パッチ管理条件の作成 （33 ページ）
- ディスク暗号化条件の作成 （34 ページ）
- ポスチャ条件の設定 （34 ページ）
- ポスチャ ポリシーの設定 （68 ページ）
- AnyConnect のワークフローの設定 （71 ページ）
- 証明書ベースの条件のための前提条件 （71 ページ）
- デフォルトのポスチャ ポリシー （73 ページ）
- クライアント ポスチャ評価 （74 ページ）
- ポスチャ評価オプション （74 ページ）
- ポスチャ修復オプション （76 ページ）
- ポスチャのカスタム条件 （77 ページ）

- ポスチャ エンドポイントのカスタム属性 （77 ページ）
- エンドポイント カスタム属性を使用したポスチャ ポリシーの作成 （78 ページ）
- カスタム ポスチャ修復アクション （79 ページ）
- ポスチャ評価要件 （83 ページ）
- ポスチャ再評価の構成設定 （85 ページ）
- ポスチャのカスタム権限 （87 ページ）
- 標準許可ポリシーの設定 （88 ページ）
- ポスチャとネットワーク ドライブ マッピングのベスト プラクティス （89 ページ）
- AnyConnect ステルス モードのワークフローの設定 （89 ページ）
- AnyConnect ステルス モード通知の有効化 （94 ページ）
- Cisco Temporal Agent のワークフローの設定 （94 ページ）
- ポスチャのトラブルシューティング ツール （97 ページ）
- Cisco ISE でのクライアント プロビジョニングの設定 （97 ページ）
- クライアント プロビジョニン リソース （98 ページ）
- ネイティブ サプリカント プロファイルの作成 （102 ページ）
- 各種ネットワークでの URL リダイレクトなしでのクライアント プロビジョニング （104 ページ）
- AMP イネーブラ プロファイルの設定 （106 ページ）
- **Cisco ISE の Chromebook デバイスのオンボーディングのサポート** （111 ページ）
- Cisco AnyConnect セキュア モビリティ （124 ページ）
- Cisco Web Agent （131 ページ）
- クライアント プロビジョニング リソース ポリシーの設定 （131 ページ）
- クライアント プロビジョニング レポート （134 ページ）
- クライアント プロビジョニング イベント ログ （135 ページ）
- クライアント プロビジョニング ポータルのポータル設定 （135 ページ）
- クライアントプロビジョニング ポータルの言語ファイルの HTML サポート （139ページ）

ポスチャ サービス

ポスチャは、Cisco Identity Services Engine（Cisco ISE）のサービスです。ポスチャを使用すると、ネットワークに接続する前に、エンドポイントのコンプライアンス（ポスチャとも呼ばれる）をチェックできます。AnyConnect ISE ポスチャ エージェントなどのポスチャ エージェントは、エンドポイントで実行されます。クライアントプロビジョニングは、エンドポイントが適切なポスチャ エージェントを受信できるようにします。

Cisco ISE の ISE ポスチャ エージェントでは、以前のユーザと完全に切断されていないため、ネイティブ サプリカントを使用する場合は Windows のユーザの簡易切り替え機能がサポートされません。新しいユーザが送信されると、古いユーザのプロセスとセッション ID がエージェントによってハングされるため、新しいポスチャ セッションが開始できません。Microsoft のセキュリティ ポリシーに従い、ユーザの簡易切り替え機能を無効にすることを推奨します。

（注） ISE では、セッション制御は複数のノードで行われます。

MnT ノードでは、セッションは次の場合に削除されます。

- アカウンティングの開始があるのにアカウンティングの停止（古いセッション）がない場合、セッションは 5 日以内に削除されます。
- アカウンティングの停止後にアカウンティングの開始がある場合、セッションは数時間以内に削除されます。
- アカウンティングの開始または停止がない場合、セッションは数時間以内に削除されます。

PSN ノードでは、セッションは次の場合に削除されます。

- アカウンティングの停止を受信した場合。
- セッションキャッシュが消去された場合、特に多くのセッションがある場合、またはPSNをリロードした場合。

リダイレクトのないポスチャをマルチノード展開で使用し、セッションを適切に管理しないと、ポスチャ機能に影響する可能性があります。

ISE コミュニティ リソース

Configure ISE 2.1 and AnyConnect 4.3 Posture USB Check

How To Configure Posture with AnyConnect Compliance Module and ISE 2.0

ポスチャ サービスのコンポーネント

Cisco ISE ポスチャ サービスには、主にポスチャ管理サービスとポスチャ ランタイム サービスが含まれます。

ポスチャ管理サービス

Cisco ISE に APeX ライセンスをインストールしていない場合、ポスチャ管理サービス オプションは管理者ポータルから使用できません。

管理サービスは、ポスチャ サービス用に設定された要件および許可ポリシーに関連付けられた、ポスチャ固有のカスタム条件および修復アクションに対するバックエンドサポートを提供します。

ポスチャ ランタイム サービス

ポスチャ ランタイム サービスでは、ポスチャ評価およびクライアントの修復のためにクライアント エージェントと Cisco ISE サーバの間で実行されるすべての相互作用をカプセル化します。

ポスチャ ランタイム サービスは検出フェーズから開始します。エンドポイント セッションは、エンドポイントが 802.1x 認証に成功した後に作成されます。クライアント エージェントは、次の順序で各種の方式によって検出パケットを送信して Cisco ISE ノードへの接続を試行します。

1. HTTP 経由で Cisco ISE サーバのポート 80 へ（設定されている場合）
2. HTTPS 経由で Cisco ISE サーバのポート 8905 へ（設定されている場合）
3. HTTP 経由でデフォルト ゲートウェイのポート 80 へ
4. HTTPS 経由でポート 8905 からそれぞれ前にアクセスしたサーバへ
5. HTTP 経由で enroll.cisco.com のポート 80 へ

ポスチャ フェーズは、利用規定（存在する場合）が受け入れられると開始されます。Cisco ISE ノードはクライアント エージェントにポスチャ ドメインのポスチャ トークンを発行します。ポスチャ トークンにより、エンドポイントではポスチャ プロセスを再度実行せずにネットワークに再接続できます。これには、エージェント GUID、利用規定のステータス、エンドポイントのオペレーティング システム情報などの情報が含まれています。

ポスチャ フェーズで使用されるメッセージは、NEA PB/PA 形式（RFC5792）です。

ポスチャ タイプ

Cisco ISE ポスチャ ポリシーを監視および適用するために使用できる 3 つのポスチャ タイプがあります。

- AnyConnect：AnyConnect エージェントを展開し、クライアントとのやりとりが必要な Cisco ISE ポスチャ ポリシーを監視し、適用します。
- AnyConnect Stealth：ユーザの操作なしで、サービスとしてポスチャを実行します。
- Temporal Agent：クライアント上で実行するように Cisco ISE GUI で設定できる一時実行可能ファイル。クライアントが信頼ネットワークにアクセスしようとすると、Cisco ISE は、ユーザがクライアント上で実行する必要のある実行可能ファイルをプッシュします。Termporal Agent は、コンプライアンス ステータスを再び検査し、そのステータスを Cisco ISE に送信します。Cisco ISE は結果に基づいて必要なアクションを実行します。コンプライアンス処理が完了すると、クライアントから一時エージェントが削除されます。一時エージェントは、カスタム修復をサポートしていません。デフォルトの修復では、メッセージ テキストのみがサポートされます。

（注）

- [ポスチャ タイプ（Posture Types）] を [Temporal Agent]、[コンプライアンス モジュール（Compliance Module）] を [4.x 以降（4.x or later）] として、ポスチャ ポリシーを設定できます。このようなポリシーの修復と要件を作成する際は、コンプライアンス モジュールを「3.x 以前」または「任意のバージョン」に変更しないように注意してください。
- Termporal Agent の場合は、[要件（Requirements）] ページで [インストール（Installation）] チェック タイプを含むパッチ管理条件のみを表示できます。
- Cisco ISE は、Mac OSX 向け Temporal Agent を使用した VLAN 制御ポスチャ環境をサポートしていません。これは、ネットワーク アクセスを既存の VLAN から新しい VLAN に変更するときに、VLAN の変更前にユーザの IP アドレスを解放し、ユーザが新しい VLAN に接続するときに新しい IP アドレスを DHCP 経由で要求する必要があるためです。これにはルート権限が必要ですが、Temporal Agent はユーザ プロセスとして実行します。

  Cisco ISE は、エンドポイント IP アドレスの更新を必要としない ACL 制御のポスチャ環境をサポートしています。

Temporal Agent によってサポートされない条件：

- サービス条件 MAC：システム デーモン チェック
- サービス条件 MAC：デーモンまたはユーザ エージェント チェック
- PM：最新チェック
- PM：有効化チェック
- DE：暗号化チェック

[クライアント プロビジョニング（Client Provisioning）] ページ（[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]）と [ポスチャ要件（Posture Requirements）] ページ（[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [要件（Requirements）]）に、ポスチャ タイプが含まれており、推奨されるベスト プラクティスは、[クライアント プロビジョニング（Client Provisioning）] ページでポスチャ プロファイルをプロビジョニングすることです。

ポスチャ要件で AnyConnect ステルス ポスチャ タイプを選択すると、一部の条件、修復、または条件内の属性が無効になります（灰色表示）。たとえば、手動修復ではクライアント側のやりとりが必要となるため、AnyConnect ステルス要件を有効にすると、[手動修復タイプ（Manual Remediation Type）] が無効になります（灰色表示）。

AnyConnect ステルス モードの展開で、ポスチャ プロファイルを AnyConnect 設定にマッピングし、Anyconnect設定を[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場合、次の処理がサポートされます。

- AnyConnect によるポスチャ プロファイルの読み取りと必要なモードの設定
- 初回ポスチャ要求における AnyConnect による選択したモードに関する情報の Cisco ISE への送信
- Cisco ISEによるモードおよびその他の要因（ID グループ、OS、コンプライアンス モジュールなど）に基づく正しいポリシーの照合。

（注） AnyConnect バージョン 4.4 以降では、ステルス モードでの Cisco ISE ポスチャがサポートされています。

関連トピック

AnyConnect ステルス モードのワークフローの設定 （89 ページ）
Cisco Temporal Agent のワークフローの設定 （94 ページ）

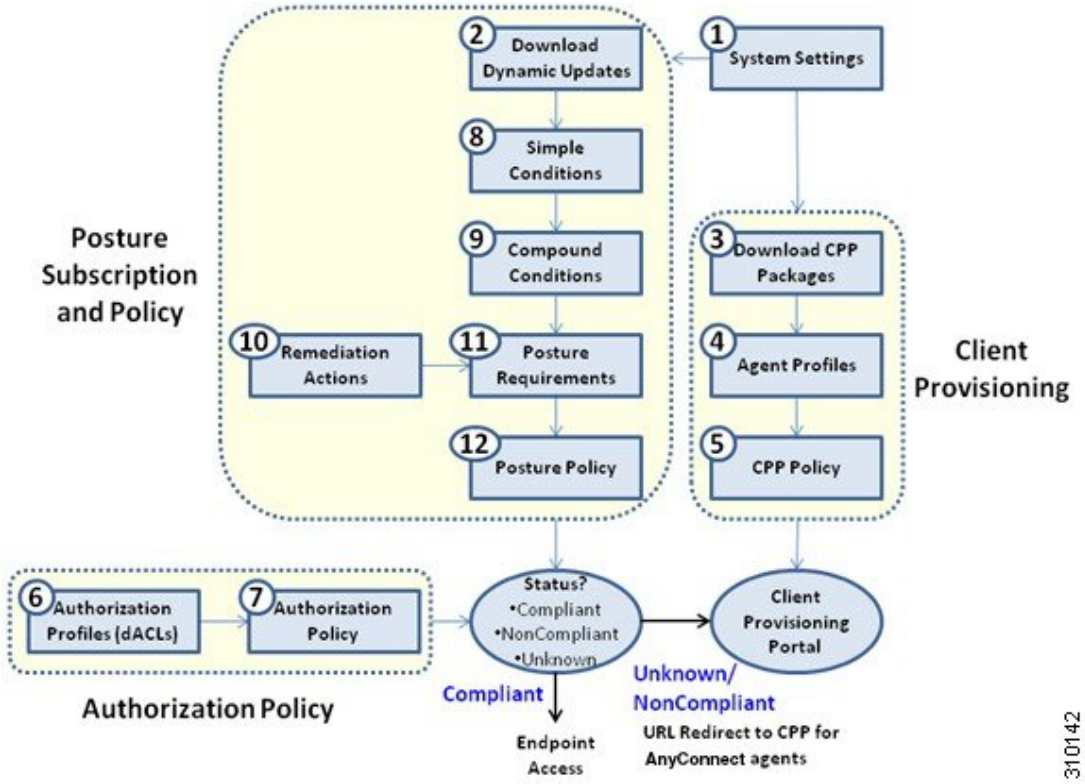
Cisco ISE ポスチャ エージェント

ポスチャ エージェントとは、Cisco ISE ネットワークにログインしているクライアント マシンに存在するアプリケーションです。クライアントがネットワークにログインしていない場合でも、エージェントは永続的にすることができ（AnyConnect と同様）、インストール後もクライアント マシンに残ります。エージェントは一時的にすることもでき（ や Windows および Mac OS 向けの Cisco Temporal Agent と同様）、ログイン セッション終了後にクライアント マシンから削除されます。いずれの場合も、エージェントはネットワークにログインし、適切なアクセスプロファイルを受け取り、クライアントマシンでポスチャ評価を実行してネットワークのコアにアクセスする前にネットワーク セキュリティ ガイドラインに従うようにします。

（注） Windows 向けの Cisco Temporal Agent は、クライアント プロビジョニング ポータルをサポートし、URL リダイレクションを使用します。

ポスチャおよびクライアントプロビジョニングポリシーワークフロー

図 *1 : Cisco ISE* のポスチャおよびクライアント プロビジョニング ポリシー ワークフロー



ポスチャ検出のステージ1では、すべてのディスカバリプローブが、ポスチャエージェントによって同時に実行されます。タイムアウト値は5秒です。ステージ2には2つのディスカバリプローブが含まれています。これにより、ポスチャモジュールはPSNへの接続を確立できます。このPSNへの接続は、リダイレクションがサポートされていない環境での認証をサポートしています。ステージ2では、すべてのプローブが連続しています。ステージ2に障害が発生した場合、ポスチャエージェントは再度ステージ1を試行します。このサイクルは30秒間継続します。その後、「ポリシーサーバが検出されません」と表示されます。この状態は、ディスカバリプローブがトリガーされるまで続きます。

ポスチャ サービス ライセンス

Cisco ISEは、Baseライセンス、Plusライセンス、APeXライセンスの3種類のライセンスを提供します。プライマリ PANで APeXライセンスをインストールしないと、ポスチャ要求はCisco ISEで実行されません。Cisco ISEのポスチャ サービスは、1つのノードまたは複数のノードで実行できます。

ポスチャ サービス展開

Cisco ISE は、スタンドアロン環境（単一ノード）または分散環境（複数ノード）に展開できます。

スタンドアロン Cisco ISE 展開では、単一のノードをすべての管理サービス、モニタリングとトラブルシューティング サービス、およびポリシー実行時サービスに設定できます。

分散 Cisco ISE 展開では、各ノードを、管理サービス、モニタリングとトラブルシューティング サービス、およびポリシー実行時サービスの Cisco ISE ノードとして設定できます。管理サービスを実行しているノードは、Cisco ISE 展開内のプライマリ ノードです。他のサービスを実行している他のノードは、互いのバックアップ サービス用に設定できるセカンダリ ノードです。

Cisco ISE でのポスチャ セッション サービスの有効化

始める前に

- クライアントから受信したすべてのポスチャ要求に対応するには、Cisco ISE でセッション サービスを有効にし、拡張ライセンス パッケージをインストールする必要があります。
- 分散展開に複数のノードを登録している場合は、登録したすべてのノードがプライマリ ノードとは別に [展開ノード（Deployment Nodes）] ページに表示されます。各ノードを Cisco ISE ノード（管理ペルソナ、ポリシー サービス ペルソナ、およびモニタリング ペルソナ）として設定できます。
- ポスチャ サービスは、ポリシー サービス ペルソナを担当する Cisco ISE ノードでのみ実行され、分散展開で管理ペルソナとモニタリング ペルソナを担当する Cisco ISE ノードでは実行されません。

ステップ 1 **[管理（Administration）] > [システム（System）] > [展開（Deployment）] > [展開（Deployment）]** を選択します。

ステップ 2 [展開ノード（Deployment Nodes）] ウィンドウから Cisco ISE ノードを選択します。

ステップ 3 [編集（Edit）] をクリックします。

ステップ 4 [全般設定（General Settings）] タブで [ポリシーサービス（Policy Service）] チェックボックスをオンにします。

[ポリシー サービス（Policy Service）] チェックボックスがオフになっている場合は、セッション サービスとプロファイリング サービスの両方のチェックボックスが無効になります。

ステップ 5 ポリシーサービス ペルソナでネットワーク アクセス、ポスチャ、ゲスト、およびクライアント プロビジョニングのセッション サービスを実行するには、[セッション サービスの有効化（Enable Session Services）] チェックボックスをオンにします。セッション サービスを停止するには、このチェックボックスをオフにします。

ステップ 6 [保存（Save）] をクリックします。

ポスチャ評価レポートの実行

ポスチャの詳細な評価を実行して、ポスチャ評価中に使用されるポスチャ ポリシーに対するクライアントのコンプライアンスの詳細なステータスを生成できます。

ステップ 1 **[操作（Operations）] > [レポート（Reports）] > [ISE レポート（ISE Reports）] > [エンドポイントとユーザ（Endpoints and Users）] > [ポスチャの詳細な評価（Posture Detail Assessment）]** を選択します。

ステップ 2 [時間範囲（Time Range）] ドロップダウン リストから特定の期間を選択します。

ステップ 3 [実行（Run）] をクリックして、選択した期間中にアクティブだったすべてのエンド ポイントの概要を表示します。

ポスチャ管理の設定

ポスチャ サービス用の管理者ポータルをグローバルに設定できます。シスコから Web 経由で自動的に Cisco ISE サーバに更新をダウンロードできます。また、オフラインで、後で、Cisco ISE を手動で更新することもできます。さらに、クライアントに AnyConnect、NAC Agent、Web Agent などのエージェントがインストールされていると、クライアントにポスチャ評価および修復サービスが提供されます。クライアント エージェントは、Cisco ISE に対してクライアントのコンプライアンス ステータスを定期的に更新します。ログインおよびポスチャの要件評価が正常に完了した後、ネットワーク使用の利用規約への準拠をエンドユーザに求めるリンクが示されたダイアログがクライアント エージェントに表示されます。このリンクを使用して、エンドユーザがネットワークへのアクセス権を取得する前に同意する、企業ネットワークのネットワーク使用情報を定義できます。

クライアントのポスチャ要件

ポスチャの要件を作成するには、次の手順を実行します。

1. [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [要件（Requirements）] を選択します。
2. 要件行の末尾にある [編集（Edit）] ドロップダウンリストから、[新しい要件の挿入（Insert New Requirement）] を選択します。
3. 必要な詳細を入力し、[完了（Done）] をクリックします。

次の表に、[クライアントのポスチャ要件（Client Posture Requirements）] ページのフィールドを示します。

表 *1:* ポスチャ要件

フィールド名	使用上のガイドライン
[名前（Name）]	要件の名前を入力します。
オペレーティング システム	オペレーティング システムを選択します。 プラス記号 [+] をクリックして、複数のオペレーティング システムをポリシーに関連付けます。 マイナス記号 [-] をクリックして、ポリシーからオペレーティング システムを削除します。
コンプライアンス モジュール	[準拠モジュール（Compliance Module）] ドロップダウンリストから必要な準拠モジュールを選択します。 • 4.x 以降（4.x or Later）：マルウェア対策、ディスク暗号化、Patch Management、および USB の各種条件をサポートします。 • 3.x 以前（3.x or Earlier）：ウイルス対策、スパイウェア対策、ディスク暗号化、およびパッチ管理の各種条件をサポートします • すべてのバージョン（Any Version）：ファイル、サービス、レジストリ、アプリケーション、および複合の各種条件をサポートします。 コンプライアンスモジュールの詳細については、コンプライアンス モジュール （30 ページ）を参照してください。

フィールド名	使用上のガイドライン
ポスチャタイプ	[ポスチャタイプ（Posture Type）] ドロップダウンリストから、必要なポスチャタイプを選択します。 • [AnyConnect]：AnyConnect エージェントを展開し、クライアントとのやり取りが必要な Cisco ISE ポリシーを監視し、適用します。 • [AnyConnect ステルス（AnyConnect Stealth）]：AnyConnect エージェントを展開し、クライアントとやり取りしない Cisco ISE ポスチャポリシーを監視し、適用します。 • [Temporal Agent]：コンプライアンス ステータスを確認するためにクライアント上で実行される一時実行可能ファイル。
条件（Conditions）	リストから条件を選択します。 [操作（Action）] アイコンをクリックして、ユーザ定義の条件を作成して、要件に関連付けることもできます。ユーザ定義の条件を作成中に関連する親オペレーティング システムは編集できません。 pr_WSUSRule は、Windows Server Update Services（WSUS）修復が関連付けられているポスチャ要件で使用される、ダミーの複合条件です。関連 WSUS 修復アクションは、重大度レベル オプションを使用して Windows Updates を検証するように設定する必要があります。この要件が失敗すると、Windows クライアントにインストールされている NAC Agent は、WSUS 修復で定義した重大度レベルに基づいて WSUS 修復アクションを適用します。 pr_WSUSRule は複合条件のリストページには表示できません。条件ウィジェットからのみ pr_WSUSRule を選択できます。

フィールド名	使用上のガイドライン
修復アクション（Remediation Actions）	リストから修復を選択します。 修復アクションを作成して、要件に関連付けることもできます。 Agentユーザとの通信に使用できるすべての修復タイプのテキスト ボックスがあります。修復アクションに加えて、クライアントの非準拠に関してメッセージで Agent ユーザと通信することができます。 [メッセージ テキストのみ（Message Text Only）] オプションで Agent ユーザに非準拠について通知します。また、詳細情報を得るためにヘルプ デスクに連絡したり、クライアントを手動で修復したりするオプションの手順がユーザに提供されています。このシナリオでは、NAC Agentは修復アクションをトリガーしません。

関連トピック

ポスチャ評価の利用規定の設定 （24 ページ）
クライアントのポスチャ要件の作成 （85 ページ）

クライアントのタイマー設定

ユーザが修復するためのタイマー、あるステータスから別のステータスに移行するためのタイマー、およびログイン成功画面を制御するためのタイマーをセットアップできます。

エージェントプロファイルを設定して、修復タイマー、ネットワーク遷移遅延タイマー、およびクライアントマシン上でログイン成功画面を制御するために使用するタイマー制御し、これらの設定がポリシーベースになるようにすることを推奨します。**[AnyConnect ポスチャプロファイル（AnyConnect Posture Profile）]** ウィンドウ（**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアントのプロビジョニング（Client Provisioning）] > [リソース（Resources）] > [追加（Add）] > [AnyConnect ポスチャプロファイル（AnyConnect Posture Profile）]** のクライアントのプロビジョニングリソースのエージェントのすべてのタイマーを設定できます。

しかし、クライアント プロビジョニング ポリシーに一致するように設定されたエージェントプロファイルがない場合、[全般設定（General Settings）] の設定ウィンドウ（**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]**）の設定を使用できます。

指定した時間内で修復するためのクライアントの修復タイマーの設定

指定した時間内にクライアントを修復するためのタイマーを設定できます。最初の評価時にクライアントが設定されたポスチャ ポリシーを満たすことに失敗した場合、エージェントは修復タイマーに設定された時間内にクライアントが修復するのを待ちます。クライアントがこの指定時間内の修復に失敗すると、クライアント エージェントはポスチャ ランタイム サービスにレポートを送信します。その後、クライアントは非準拠ステートに移行されます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]** を選択します。

ステップ 2 [修復タイマー（Remediation Timer）] フィールドに、分単位で時間の値を入力します。

デフォルト値は 4 分です。有効な範囲は 1 ～ 300 分です。

ステップ 3 [保存（Save）] をクリックします。

クライアントの遷移のためのネットワーク遷移遅延タイマーの設定

ネットワーク遷移遅延タイマーを使用して、指定した時間内に、クライアントがある状態から別の状態に遷移するためのタイマーを設定できます。これは、許可変更（CoA）が完了するために必要となります。ポスチャの成功時と失敗時にクライアントが新しい VLAN の IP アドレスを取得するための時間がかかる場合は、より長い遅延時間が必要になることがあります。クライアントが正常にポスチャされると、Cisco ISE は、ネットワーク遷移遅延タイマーで指定された時間内に未知から準拠モードへ移行することを許可します。ポスチャに失敗すると、Cisco ISE は、タイマーで指定された時間内にクライアントが未知から非準拠モードへ移行することを許可します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]** を選択します。

ステップ 2 [ネットワーク遷移遅延（Network Transition Delay）] フィールドに時間値を秒単位で入力します。

デフォルト値は 3 秒です。有効な値の範囲は 2 ～ 30 秒です。

ステップ 3 [保存（Save）] をクリックします。

ログイン成功ウィンドウを自動的に閉じる設定

ポスチャ評価が正常に完了した後、クライアント エージェントは一時的なネットワーク アクセス画面を表示します。ユーザはログイン ウィンドウで [OK] ボタンをクリックして、この画面を閉じる必要があります。指定した時間の経過後にこのログイン画面を自動的に閉じるタイマーを設定できます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]** を選択します。

ステップ 2 [経過後にログイン成功画面を自動的に閉じる（Automatically Close Login Success Screen After）] チェックボックスをオンにします。

ステップ 3 [経過後にログイン成功画面を自動的に閉じる（Automatically Close Login Success Screen After）] チェックボックスの横のフィールドに時間値を秒単位で入力します。

有効な値の範囲は 0 ～ 300 秒です。時間をゼロに設定すると、AnyConnect はログイン成功画面を表示しません。

ステップ 4 [保存（Save）] をクリックします。

非エージェント デバイスへのポスチャ ステータスの設定

Linux または iDevice などの非エージェント デバイスで実行されるエンドポイントのポスチャ ステータスを設定できます。Android デバイスおよび iPod、iPhone、iPad などの Apple の iDevice が Cisco ISE 対応ネットワークに接続する場合、これらのデバイスはデフォルト ポスチャ ステータスの設定を引き継ぎます。

これらの設定は、ポスチャのランタイム中に一致するポリシーが見つからない場合、Windows および Macintosh オペレーティング システムで実行されるエンドポイントにも適用されます。

始める前に

エンドポイントにポリシーを適用するには、対応するクライアント プロビジョニング ポリシー（エージェントのインストール パッケージ）を設定する必要があります。そうしないと、エンドポイントのポスチャ ステータスは自動的にデフォルト設定が反映されます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]** を選択します。

ステップ 2 [デフォルトポスチャステータス（Default Posture Status）] ドロップダウン リストから、オプションに [準拠（Compliant）] または [非準拠（Noncompliant）] を選択します。

ステップ 3 [保存（Save）] をクリックします。

ポスチャのリース

ユーザがネットワークにログインするたびにポスチャ評価を実行したり、指定した間隔でポスチャ評価を実行したりするよう Cisco ISE を設定できます。有効な範囲は 1 ～ 365 日です。

この設定は、ポスチャ評価に AnyConnect エージェントを使用するユーザだけに適用されます。

ポスチャ リースがアクティブな場合、Cisco ISE は最新の既知のポスチャを使用しますが、コンプライアンスの確認のためにエンドポイントに接続しません。ただし、ポスチャ リースが期限切れになると、Cisco ISE はエンドポイントの再認証またはポスチャ再評価を自動的にトリガーしません。同じセッションが使用されているため、エンドポイントは同じコンプライアンス状態のままになります。エンドポイントが再認証されると、ポスチャが実行され、ポスチャ リース時間がリセットされます。

使用例のシナリオ

- ユーザはエンドポイントにログオンし、1 日に設定されているポスチャ リースにポスチャ準拠させます。
- ユーザは4時間後にエンドポイントからログオフします（この時点で、ポスチャ リースは 20 時間残っています）。
- ユーザは 1 時間後に再度ログオンします。この時点で、ポスチャ リースは 19 時間残っています。最新の既知のポスチャ状態は準拠状態でした。したがって、エンドポイントでポスチャが実行されることなく、ユーザにアクセス権が付与されます。
- ユーザは 4 時間後にログオフします（この時点で、ポスチャ リースは 15 時間残っています）。
- ユーザは 14 時間後にログオンします。ポスチャ リースは 1 時間残っています。最新の既知のポスチャ状態は準拠状態でした。エンドポイントでポスチャが実行されることなく、ユーザにアクセス権が付与されます。
- 1 時間後、ポスチャ リースは期限切れになります。同じユーザ セッションが使用されているため、ユーザは引き続きネットワークに接続されています。
- 1 時間後、ユーザはログオフします（セッションはユーザに関連付けられていますが、マシンには関連付けられていないため、マシンはネットワーク上に留まることができます）。
- 1 時間後、ユーザはログオンします。ポスチャ リースが期限切れになり、新しいユーザ セッションが開始されるため、マシンはポスチャ アセスメントを実行し、その結果が Cisco ISE に送信され、ポスチャ リース時間が 1 日にリセットされます（この使用例の場合）。

定期的再評価

定期的再評価（PRA）は、コンプライアンスについてすでに適切にポスチャされているクライアントにのみ実行できます。PRA は、クライアントがネットワーク上で準拠していない場合には実行されません。

PRA は、エンドポイントが準拠ステートになっている場合にのみ有効であり、適用可能です。ポリシー サービス ノードは関連するポリシーを調べ、設定で定義されているクライアント ロールに応じて要件をコンパイルし、PRA を適用します。PRA 設定の一致が見つかった場合、ポリシー サービス ノードは、クライアントの PRA 設定で定義されている PRA 属性を使用して、クライアント エージェントに応答してから、CoA 要求を発行します。クライアント エージェントは、設定に指定された間隔に基づいて定期的に PRA 要求を送信します。PRA が成功した場合、または、PRA 設定に指定されているアクションが続行になっている場合、クライアント

は準拠ステートのままになります。クライアントが PRA を満たしていない場合、準拠ステートから非準拠ステートに移行します。

PostureStatus 属性は、ポスチャ再評価要求の場合でも、PRA 要求で現在のポスチャ ステータスを不明ではなく準拠と示します。PostureStatus はモニタリング レポートでも更新されます。

ポスチャのリースが有効期限内の場合、アクセス コントロール リスト（ACL）に基づいてエンドポイントが準拠し、PRA が開始されます。PRA が失敗すると、エンドポイントが非準拠になり、ポスチャのリースがリセットされます。

定期的再評価の設定

コンプライアンスに対してすでに正常にポスチャされているクライアントだけの定期的な再評価を設定できます。システムで定義されているユーザ ID グループに各 PRA を設定できます。

始める前に

- 各 PRA 設定に、一意のグループ、または設定に割り当てられているユーザ ID グループの一意の組み合わせがあることを確認します。
- 2 つの一意のロールである role_test_1 および role_test_2 を PRA 設定に割り当てることができます。論理演算子とこれら 2 つのロールを組み合わせ、2 つのロールの一意の組み合わせとして PRA 設定に割り当てることができます。たとえば、role_test_1 OR role_test_2 とします。
- 2 つの PRA 設定に共通のユーザ ID グループがないことを確認します。
- PRA 設定がユーザ ID グループ「Any」にすでに存在する場合、次のことを実行しないと、他の PRA 設定を作成できません。
  - *Any* 以外のユーザ ID グループを反映するように、任意のユーザ ID グループで既存の PRA 設定を更新します。
  - ユーザ ID グループ「*Any*」の既存の PRA 設定を削除します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [再評価（Reassessments）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 新しい PRA を作成するには、[新規再評価の設定（New Reassessment Configuration）] ページで値を変更します。

ステップ 4 [送信（Submit）] をクリックして、PRA 設定を作成します。

ポスチャのトラブルシューティングの設定

次の表では、ネットワーク内のポスチャ問題の検出と解決に使用する [ポスチャのトラブルシューティング（Posture troubleshooting）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [ポスチャのトラブルシューティング（Posture Troubleshooting）]** です。

表 *2:* ポスチャのトラブルシューティングの設定

オプション	使用上のガイドライン
トラブルシューティングが必要なポスチャ イベントの検索と選択	
[ユーザ名（Username）]	フィルタリング基準として使用するユーザ名を入力します。
MAC アドレス（MAC Address）	フィルタリング基準として使用する MAC アドレスを、xx-xx-xx-xx-xx-xx 形式で入力します。
ポスチャ ステータス（Posture Status）	フィルタリング基準として使用する認証ステータスを選択します。
失敗の理由（Failure Reason）	失敗理由を入力するか、または [選択（Select）] をクリックしてリストから失敗理由を選択します。失敗理由をクリアするには、[クリア（Clear）] をクリックします。
時間範囲（Time Range）	時間範囲を選択します。この時間範囲に作成された RADIUS 認証レコードが使用されます。
開始日時：（Start Date-Time:）	（[時間範囲（Time Range）] として [カスタム（Custom）] を選択した場合にのみ使用可能）開始日時を入力するか、またはカレンダ アイコンをクリックして開始日時を選択します。日付は *mm/dd/yyyy* 形式、時刻は *hh:mm* 形式である必要があります。
終了日時：（End Date-Time:）	（[時間範囲（Time Range）] として [カスタム（Custom）] を選択した場合にのみ使用可能）終了日時を入力するか、またはカレンダ アイコンをクリックして終了日時を選択します。日付は *mm/dd/yyyy* 形式、時刻は *hh:mm* 形式である必要があります。
レコード数の取得（Fetch Number of Records）	表示するレコードの数を選択します。10、20、50、100、200、または 500 を選択できます。
検索結果	

オプション	使用上のガイドライン
時刻（Time）	イベントの時刻
ステータス（Status）	ポスチャ ステータス
[ユーザ名（Username）]	イベントに関連付けられたユーザ名
MAC アドレス（MAC Address）	システムの MAC アドレス
失敗の理由（Failure Reason）	イベントの障害理由

関連トピック

エンドポイント ポスチャの障害のトラブルシューティング
ポスチャのトラブルシューティング ツール （97 ページ）

ポスチャの全般設定

次の表では、修復時間およびポスチャ ステータスなどの一般的なポスチャ設定を行うために使用できる [ポスチャの全般設定（Posture General Settings）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[ポスチャ（Posture）]** > **[全般設定（General Settings）]** です。

表 *3:* ポスチャの全般設定

フィールド	使用上のガイドライン
修復タイマー（Remediation Timer）	分単位で時間値を入力します。デフォルト値は 4 分です。有効な範囲は 1 ～ 300 分です。
ネットワーク遷移遅延（Network Transition Delay）	秒単位で時間値を入力します。デフォルト値は 3 秒です。有効な値の範囲は 2 ～ 30 秒です。
デフォルトのポスチャ ステータス（Default Posture Status）	準拠または非準拠を選択します。Linux のような非エージェント デバイスは、ネットワークに接続している間、このステータスを想定します。

フィールド	使用上のガイドライン
一定時間（秒）経過後にログイン成功画面を自動的に閉じる（Automatically Close Login Success Screen After）	このチェックボックスをオンにすると、指定された時間後に、ログイン成功画面が自動的に閉じます。 チェックボックスの隣のフィールドに、時間値を秒単位で入力します。 0 ～ 300 秒にログイン画面が自動的に閉じるようにタイマーを設定できます。時間をゼロに設定した場合は、クライアント上のエージェントはログイン成功画面を表示しません。
連続モニタリング間隔（Continuous Monitoring Interval）	AnyConnect がモニタリング データの送信を開始するまでの時間間隔を指定します。アプリケーション条件の場合アプリケーションおよびハードウェア条件の場合、デフォルト値は 5 分です。
ステルス モードでの利用規約（Acceptable Use Policy in Stealth Mode）	会社のネットワーク使用条件が満たされていない場合、ステルス モードで [ブロック（Block）] を選択して、クライアントを非準拠ポスチャ ステータスに移行します。
ポスチャのリース	
ユーザがネットワークに接続するたびにポスチャ評価を行う（Perform posture assessment every time a user connects to the network）	ユーザがネットワークに接続するたびにポスチャ評価を開始するには、このオプションを選択します。
n 日おきにポスチャ評価を行う（Perform posture assessment every n days）	クライアントがすでにポスチャ準拠であるものの、指定された日数が経過したら、ポスチャ評価を開始する場合は、このオプションを選択します。
最後の既知の良い状態をキャッシュする（Cache Last Known Good State）	ポスチャ評価の結果をキャッシュするには、Cisco ISE のこのチェックボックスをオンにします。デフォルトでは、このフィールドは無効です。
最後の既知の良い状態（Last Known Good State）	[最後の既知の良い状態をキャッシュする（Cache Last Known Good State）] チェックボックスをオンにしている場合のみ該当します。Cisco ISE は、このフィールドに指定した期間にわたり、ポスチャ評価の結果をキャッシュします。有効な値は、1 ～ 30 日、1 ～ 720 時間、または 1 ～ 43200 分です。

関連トピック

ポスチャ サービス （2 ページ）
ポスチャ管理の設定 （9 ページ）
ポスチャのリース （14 ページ）
Cisco ISE でのポスチャ セッション サービスの有効化 （8 ページ）
指定した時間内で修復するためのクライアントの修復タイマーの設定 （13 ページ）
クライアントの遷移のためのネットワーク遷移遅延タイマーの設定 （13 ページ）
ログイン成功ウィンドウを自動的に閉じる設定 （13 ページ）
非エージェント デバイスへのポスチャ ステータスの設定 （14 ページ）

Cisco ISE へのポスチャ更新のダウンロード

ポスチャ更新には、Windows および Macintosh オペレーティング システムの両方のアンチウイルスとアンチスパイウェアの一連の事前定義済みのチェック、ルール、サポート表、およびシスコでサポートされるオペレーティング システム情報が含まれます。また、ローカル ファイル システムの更新の最新のアーカイブを含むファイルから Cisco ISE をオフラインで更新することもできます。

ネットワークに Cisco ISE を初めて展開する場合は、Web からポスチャ更新をダウンロードできます。通常、このプロセスには約 20 分かかります。初回ダウンロード後に、差分更新が自動的にダウンロードされるように Cisco ISE を設定できます。

Cisco ISE では、初回ポスチャ更新時に 1 回のみ、デフォルトのポスチャ ポリシー、要件、および修復を作成します。それらを削除した場合、Cisco ISE は後続の手動またはスケジュールされた更新中にこれらを再作成しません。

始める前に

ポスチャ リソースを Cisco ISE にダウンロードできる適切なリモート ロケーションにアクセスできるようにするには、5-2 ページの「Cisco ISE でのプロキシ設定の指定」の説明に従ってネットワークにプロキシが正しく設定されていることを確認する必要がある場合があります。

[ポスチャ更新（Posture Update）] ページを使用して、Web から更新を動的にダウンロードできます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [更新（Updates）]** を選択します。

ステップ 2 [Web] オプションを選択して、更新を動的にダウンロードします。

ステップ 3 [デフォルトに設定（Set to Default）] をクリックして、[フィードURLの更新（Update Feed URL）] フィールドにシスコのデフォルト値を設定します。

ネットワークで URL リダイレクション機能（プロキシ サーバ経由など）を制限しているために、上記の URL へのアクセスに問題がある場合は、Cisco ISE で関連トピックの代替 URL を指定してください。

ステップ 4 [ポスチャ更新（Posture Updates）] ページの値を変更します。

ステップ 5 シスコからの更新をダウンロードするには、[今すぐ更新（Update Now）] をクリックします。

更新された後、[ポスチャ更新（Posture Updates）] ページに、[ポスチャ更新（Posture Updates）] ページの [更新情報（Update Information）] セクションの更新の確認として現在のシスコ更新のバージョン情報が表示されます。

ステップ 6 [はい（Yes）] をクリックして続行します。

ポスチャ更新の自動ダウンロード

最初の更新後に、更新を確認し、自動的にダウンロードするようにCisco ISEを設定できます。

始める前に

- 最初にポスチャ更新をダウンロードして、更新を確認し、自動的にダウンロードするように Cisco ISE を設定しておく必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [更新（Updates）]** を選択します。

ステップ 2 [ポスチャ更新（Posture Updates）] ページで [初期遅延から開始される更新の自動確認（Automatically check for updates starting from initial delay）] チェックボックスをオンにします。

ステップ 3 初期遅延時間を hh:mm:ss の形式で入力します。

Cisco ISE は、初期遅延時間の終了後に確認を開始します。

ステップ 4 時間間隔を時間単位で入力します。

Cisco ISE は初期遅延時間から指定した間隔で、展開に更新をダウンロードします。

ステップ 5 [保存（Save）] をクリックします。

ポスチャの利用規定の構成設定

次の表では、ポスチャのアクセプタブルユースポリシーを設定するために使用できるポスチャの [利用規定設定（Acceptable Use Policy Configurations）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [利用規定（Acceptable Use Policy）]** です。

表 *4:* ポスチャ *AUP* の設定

フィールド	使用上のガイドライン
構成名	ユーザが作成する AUP 設定の名前を入力します。
設定の説明（Configuration Description）	ユーザが作成する AUP 設定の説明を入力します。
エージェントユーザへの AUP の表示（Windows の場合のみ）	オンにした場合、[エージェントユーザへの AUP の表示（Show AUP to Agent users）] チェックボックスはユーザ（Windows のみ）にネットワークの利用規約へのリンクを表示し、それをクリックすると、認証およびポスチャ評価が成功したときに AUP が表示されます。
AUP メッセージの URL を使用（Use URL for AUP message）オプション ボタン	選択した場合、認証およびポスチャ評価が成功したときにクライアントがアクセスする必要がある AUP メッセージへの URL を AUP URL に入力する必要があります。
AUP メッセージのファイルを使用（Use file for AUP message）オプション ボタン	選択した場合、場所を参照し、トップ レベルに index.html を含む AUP ファイルにジップ形式のファイルをアップロードします。 .zip ファイルには、index.html ファイルに加えて、他のファイルおよびサブディレクトリを含めることができます。これらのファイルは、HTML タグを使用して相互に参照できます。
AUP URL	クライアントは認証およびポスチャ評価が成功したときにアクセスする必要がある AUP への URL を入力します。
AUP ファイル（AUP File）	[AUP ファイル（AUP File）] で、ファイルを参照し、Cisco ISE サーバにアップロードします。これは zip 形式のファイルで、zip 形式のファイルではトップ レベルに index.html ファイルを含める必要があります。

フィールド	使用上のガイドライン
ユーザ ID グループの選択（Select User Identity Groups）	[ユーザ ID グループの選択（Select User Identity Groups）] ドロップダウン リストで、AUP 設定の一意のユーザ ID グループまたはユーザ ID グループの一意の組み合わせを選択します。 AUP 設定を作成する場合は、次の点に注意してください。 • ポスチャ AUP は、ゲスト フローには適用できません。 • 各設定には、一意のユーザ ID グループ、またはユーザ ID グループの一意の組み合わせが必要です。 • 2 つの設定が共通のユーザ ID グループを持つことはできません。 • ユーザ ID グループ「Any」で AUP 設定を作成する場合は、まず他のすべての AUP 設定を削除します。 • ユーザ ID グループ「Any」を使用して AUP 設定を作成した場合、一意のユーザ ID グループ、または複数のユーザ ID グループを使用して他の AUP 設定を作成することはできません。Any 以外のユーザ ID グループを使用して AUP 設定を作成するには、最初にユーザ ID グループ「Any」を使用した既存の AUP 設定を削除するか、ユーザ ID グループ「Any」を使用した既存の AUP 設定を一意のユーザ ID グループまたは複数のユーザの ID グループを使用して更新します。
利用規定設定 - 設定リスト（Acceptable use policy configurations—Configurations list）	既存の AUP 設定と AUP 設定に関連付けられたエンドユーザ ID グループを一覧表示します。

関連トピック

ポスチャ サービス （2 ページ）
ポスチャ評価の利用規定の設定 （24 ページ）

ポスチャ評価の利用規定の設定

ログインし、クライアントのポスチャ評価が成功すると、クライアントエージェントにより一時的なネットワークアクセス画面が表示されます。この画面には、利用規定（AUP）へのリンクが含まれています。ユーザがリンクをクリックすると、ネットワーク利用条件を表示するページにリダイレクトされます。その条件を読み、同意する必要があります。

各利用規定設定には、一意のユーザ ID グループ、またはユーザ ID グループの一意の組み合わせが必要です。Cisco ISE は最初に一致したユーザ ID グループの AUP を見つけ、AUP を表示するクライアント エージェントと通信します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [利用規定（Acceptable Use Policy）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [新規利用規定設定（New Acceptable Use Policy Configuration）] ページで値を変更します。

ステップ 4 [送信（Submit）] をクリックします。

ポスチャ条件

ポスチャ条件は次の単純条件のいずれかになります。ファイル、レジストリ、アプリケーション、サービス、またはディクショナリ条件。これらの単純条件のうちの 1 つ以上の条件によって複合条件が形成され、複合条件はポスチャ要件と関連付けることができます。

ネットワークに Cisco ISE を初めて展開する場合は、Web からポスチャ更新をダウンロードできます。このプロセスは、初期ポスチャ更新と呼ばれます。

初期ポスチャ更新の後、Cisco ISE はシスコ定義の単純および複合条件も作成します。シスコ定義の単純条件はプレフィクスとして pc_ が付けられ、複合条件はプレフィクスとして pr_ が付けられています。

ダイナミック ポスチャ更新の結果としてシスコ定義の条件を Web を介してダウンロードするように Cisco ISE を設定することもできます。シスコ定義のポスチャ条件を削除または編集することはできません。

ユーザ定義の条件やシスコ定義の条件には、単純条件と複合条件の両方が含まれます。

単純ポスチャ条件

[ポスチャナビゲーション（Posture Navigation）] ペインを使用して、次の単純条件を管理できます。

- ファイル条件：ファイルの存在、ファイルの日付、およびクライアントのファイル バージョンを確認する条件。
- レジストリ条件：レジストリ キーの存在またはクライアントのレジストリ キーの値を確認する条件。
- アプリケーション条件：アプリケーションまたはプロセスがクライアント上で実行されているかまたは実行されていないかを確認する条件。

（注） プロセスがインストールされ実行されている場合、ユーザは準拠します。ただし、アプリケーション条件が逆ロジックで動作している場合は、アプリケーションがインストールされておらず実行されていなくも、エンドユーザは準拠します。アプリケーションがインストールされ実行されている場合、エンドユーザは準拠しません。

- サービス条件：サービスがクライアント上で実行されているかまたは実行されていないかを確認する条件。
- ディクショナリ条件：ディクショナリ属性と値を確認する条件。
- USB 条件：USB マス ストレージ デバイスの有無をチェックする条件。

単純ポスチャ条件の作成

ポスチャ ポリシーまたは他の複合条件で使用できる、ファイル、レジストリ、アプリケーション、サービス、およびディクショナリ単純条件を作成できます。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）]** を選択します。

ステップ 2 [ファイル（File）]、[レジストリ（Registry）]、[アプリケーション（Application）]、[サービス（Service）]、または [ディクショナリ単純条件（Dictionary Simple Condition）] のいずれかを選択します。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 フィールドに適切な値を入力します。

ステップ 5 [送信（Submit）] をクリックします。

複合ポスチャ条件

複合条件は、1つ以上の単純条件、または複合条件で構成されます。ポスチャ ポリシーを定義する場合、次の複合条件を使用できます。

- 複合条件：1 つ以上の単純条件、またはタイプがファイル、レジストリ、アプリケーション、またはサービス条件の複合条件が含まれます
- アンチウイルス複合条件：1 つ以上の AV 条件、または AV 複合条件が含まれます
- アンチスパイウェア複合条件：1 つ以上の AS 条件、または AS 複合条件が含まれます
- ディクショナリ複合条件：1 つ以上のディクショナリ単純条件またはディクショナリ複合条件が含まれます
- マルウェア対策条件：1 つ以上の AM 条件が含まれます

ディクショナリ複合条件の設定

次の表に、[ディクショナリ複合条件（Dictionary Compound Conditions）] ウィンドウのフィールドを示します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）]**>**[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** > **[ディクショナリ複合条件（Dictionary Compound Conditions）]** です。

表 *5:* ディクショナリ複合条件の設定

フィールド名	使用上のガイドライン
[名前（Name）]	作成するディクショナリ複合条件の名前を入力します。
説明	作成するディクショナリ複合条件の説明を入力します。
既存の条件をライブラリから選択（Select Existing Condition from Library）	ポリシー要素ライブラリから事前定義済みの条件を選択して式を定義するか、または後のステップでアドホック属性/値のペアを式に追加します。
条件名（Condition Name）	ポリシー要素ライブラリからすでに作成しているディクショナリ単純条件を選択します。
式（Expression）	[条件名（Condition Name）] ドロップダウンリストでの選択に基づいて式が更新されます。

フィールド名	使用上のガイドライン
AND または OR 演算子（AND or OR operator）	ライブラリから追加できるディクショナリ単純条件を論理的に組み合わせるには、ANDまたはOR 演算子を選択します。 次の操作を行うには、[操作（Action）]アイコンをクリックします。 • 属性/値の追加（Add Attribute/Value） • ライブラリから条件を追加（Add Condition from Library） • 削除（Delete）
新しい条件の作成（高度なオプション）（Create New Condition (Advance Option)）	さまざまなシステムディクショナリまたはユーザ定義ディクショナリから属性を選択します。 後のステップで事前定義された条件をポリシー要素ライブラリから追加することもできます。
条件名（Condition Name）	すでに作成したディクショナリ単純条件を選択します。
式（Expression）	[式（Expression）] ドロップダウン リストから、ディクショナリ単純条件を作成できます。
演算子	属性に値を関連付ける演算子を選択します。
値	ディクショナリ属性に関連付ける値を入力するか、またはドロップダウン リストから値を選択します。

関連トピック

ディクショナリおよびディクショナリ属性
単純条件と複合条件
複合ポスチャ条件 （26 ページ）
複合ポスチャ条件の作成 （32 ページ）

Windows クライアントでの自動アップデートを有効にするための事前定義の条件

pr_AutoUpdateCheck_Rule はシスコによって事前定義された条件であり、[複合条件（Compound Conditions）]ページにダウンロードされます。この条件を使用すると、Windows クライアント上で自動アップデート機能が有効になっているかどうかを確認することができます。Windows

クライアントがこの要件を満たさない場合、ネットワークアクセスコントロール（NAC）エージェントによって、Windowsクライアントの自動アップデート機能が強制的に有効になります（修復）。この修復後、Windowsクライアントはポスチャ準拠になります。自動アップデート機能がWindowsクライアント上で有効になっていない場合は、ポスチャポリシーで関連付けたWindows Update修復でWindows管理者設定を上書きします。

事前設定済みアンチウイルスおよびアンチスパイウェア条件

Cisco ISEの[AV複合条件（AV Compound Condition）]および[AS複合条件（AS Compound Condition）]ページには、アンチウイルスとアンチスパイウェアの事前設定済みの複合条件がロードされます。これらの条件は、WindowsおよびMacintoshオペレーティングシステムのアンチウイルスおよびアンチスパイウェアサポート表で定義されます。これらの複合条件では、指定されたアンチウイルスとアンチスパイウェア製品がすべてのクライアント上に存在するかどうかを確認できます。Cisco ISEで新しいアンチウイルスとアンチスパイウェアの複合条件を作成することもできます。

アンチウイルスとアンチスパイウェア サポート表

Cisco ISEは、各ベンダー製品の最新バージョンおよび定義ファイルの日付を提供するアンチウイルスとアンチスパイウェアサポート表を使用します。ユーザは頻繁にアンチウイルスとアンチスパイウェアサポート表をポーリングする必要があります。アンチウイルスとアンチスパイウェアのベンダーはアンチウイルスとアンチスパイウェア定義ファイルを頻繁に更新するため、各ベンダー製品の最新バージョンおよび定義ファイルの日付を検索します。

新しいアンチウイルスとアンチスパイウェアのベンダー、製品、リリースのサポートを反映するようにアンチウイルスとアンチスパイウェア サポート表が更新されるたびに、NAC Agentは新しいアンチウイルスとアンチスパイウェア ライブラリを受け取ります。これは、NAC Agentがより新しい追加機能をサポートするのに役立ちます。NAC Agentがこのサポート情報を取得すると、定期的に更新されるse-checks.xmlファイル（se-templates.tar.gzアーカイブでse-rules.xmlファイルとともに公開される）で最新の定義情報をチェックし、クライアントがポスチャポリシーに準拠しているかどうかを決定します。特定のアンチウイルスまたはアンチスパイウェア製品のアンチウイルスとアンチスパイウェアライブラリによってサポートされている機能に応じて、適切な要件がNAC Agentに送信され、ポスチャ検証中にクライアント上でそれらの存在、および特定のアンチウイルスおよびアンチスパイウェア製品のステータスが検証されます。

ISEポスチャエージェントでサポートされているウイルス対策およびマルウェア対策製品の詳細については、Cisco.comにあるCisco AnyConnect ISEポスチャのサポート表を参照してください。

マルウェア対策のポスチャ条件を作成する際に、コンプライアンスモジュールの最小バージョンを確認できます。ポスチャフィードが更新されたら、[ワークセンター（Work Centers）]>

[ポスチャ（Posture）]>[ポリシー要素（Policy Elements）]>[マルウェア対策条件（Anti-Malware Condition）]を選択し、[オペレーティングシステム（Operating System）]と[ベンダー（Vendor）]を選択してサポート表を表示します。

（注） マルウェア対策のエンドポイントセキュリティ ソリューション（FireEye、Cisco AMP、Sophos など）の一部には、それぞれの集中型サービスへネットワークを通じてアクセスしないと機能しないものがあります。このような製品の場合、AnyConnect ISE の章 (または OESIS ライブラリ) は、エンドポイントがインターネットに接続されていることを想定しています。このようなエンドポイントについては、これらのオンラインエージェントのための事前ポスチャ（オフライン検出が有効になっていない場合）時にインターネットアクセスを許可することを推奨します。このような場合には、署名定義の条件が適用されないことがあります。

インライン ポスチャ ノード

インライン ポスチャ ノードは、ネットワーク上のワイヤレス LAN コントローラ（WLC）および VPN コンセントレータなどのネットワーク アクセス デバイスの背後にある、ゲートキーピング ノードです。インライン ポスチャ ノードにより、ユーザが認証され、アクセス権が与えられた後にアクセス ポリシーが適用され、WLC または VPN で処理できない許可変更（CoA）要求が処理されます。Cisco ISE では、プライマリ ロールまたはセカンダリ ロールを担当できるインライン ポスチャ ノードを 2 つ使用してハイ アベイラビリティを実現できます。

インライン ポスチャ ノードは、専用ノードである必要があります。このノードはインライン ポスチャ サービス専用である必要があり、他の Cisco ISE サービスと同時に実行することはできません。同様に、そのサービスの特性のため、インライン ポスチャ ノードはどのペルソナも担当することができません。たとえば、Cisco ISE ネットワークの管理サービスを提供する管理ノード、ネットワーク アクセス サービス、ポスチャ サービス、プロファイル サービス、およびゲスト サービスを提供するポリシー サービス ノード、またはモニタリング サービスおよびトラブルシューティング サービスを提供するモニタリング ノードとして稼働することはできません。

インライン ポスチャのペルソナは Cisco ISE 3495 プラットフォームではサポートされません。インライン ポスチャのペルソナは、サポートされるプラットフォームである Cisco ISE 3315、Cisco ISE 3355、Cisco ISE 3395、または Cisco ISE 3415 のいずれかにインストールしてください。

インライン ポスチャ ノードの Web ベースのユーザ インターフェイスにアクセスすることはできません。これは、PAN からのみ設定できます。

インライン ポスチャ ノードのインストール

Cisco.com からインライン ポスチャ ISO（IPN ISO）イメージをダウンロードし、サポートされているプラットフォームのいずれかにインストールします。次に、コマンドライン インター

フェイス（CLI）を使用して証明書を設定する必要があります。これで、管理者ポータルからこのノードを登録できます。

（注） リリース 1.31.4 用の別個のインライン ポスチャ ISO イメージはありません。1.2 IPN ISO イメージを使用して、インライン ポスチャ ノードをインストールおよび設定します。

インライン ポスチャ アプリケーションをインストールして設定した後、インライン ポスチャ ノードを登録するには、証明書を設定する必要があります。詳細については、『Cisco Identity Services Engine Hardware Installation Guide』を参照してください。

インライン ポスチャ ノードの登録

登録時にノードのタイプ（Cisco ISE またはインライン ポスチャ）を決定することを推奨します。後でノードタイプを変更する場合は、ノードを展開から登録解除し、スタンドアロン ノードで Cisco ISE を再起動してから、そのノードを登録する必要があります。

始める前に

- プライマリ ノードの証明書信頼リスト（CTL）に、登録するセカンダリ ノードの HTTPS 証明書を検証するための適切な認証局（CA）証明書があることを確認します。
- セカンダリ ノードをプライマリ ノードに登録した後、セカンダリ ノードで HTTPS 証明書を変更する場合は、プライマリ ノードの CTL に適切な CA 証明書をインポートする必要があります。

ステップ 1 PAN にログインします。

ステップ 2 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

ステップ 3 左側のナビゲーション ペインで、[展開（Deployment）] をクリックします。

ステップ 4 **[登録（Register）] > [インライン ポスチャ ノードの登録（Register an Inline Posture Node）]** を選択して、セカンダリ インライン ポスチャ ノードを登録します。

コンプライアンス モジュール

コンプライアンス モジュールには、ベンダー名、製品バージョン、製品名、および Cisco ISE のポスチャ条件をサポートする OPSWAT が提供する属性などのフィールドのリストが含まれています。

ベンダーは頻繁に製品バージョンや定義ファイルの日付を更新するので、頻繁にアップデートのコンプライアンス モジュールをポーリングすることで、各ベンダーの製品の最新バージョンおよび定義ファイルの日付を調べる必要があります。新しいベンダー、製品、およびリリース

のサポートを反映してコンプライアンス モジュールが更新されるたびに、AnyConnect のエージェントは新しいライブラリを受信します。これは、AnyConnect のエージェントがより新しい追加機能をサポートするのに役立ちます。AnyConnect のエージェントがこのサポート情報を取得すると、定期的に更新される se-checks.xml ファイル（se-templates.tar.gz アーカイブで se-rules.xml ファイルとともに公開される）で最新の定義情報をチェックし、クライアントがポスチャ ポリシーに準拠しているかどうかを決定します。特定のアンチウイルス、アンチスパイウェア、マルウェア対策、ディスク暗号化またはパッチ管理製品のライブラリによってサポートされている機能に応じて、適切な要件が AnyConnect エージェントに送信され、ポスチャ検証中にクライアント上でそれらの存在、およびクライアントでの特定の製品のステータスが検証されます。

コンプライアンス モジュールは、Cisco.com で入手可能です。

次の表に、ISE ポスチャ ポリシーをサポートするまたはしない OPSWAT API バージョンを示します。バージョン 3 および 4 をサポートするエージェントごとに異なるポリシー ルールがあります。

表 *6 : OPSWAT API* バージョン

ポスチャ条件	コンプライアンス モジュールのバージョン
OPSWAT	
アンチウイルス	3.x 以前
スパイウェア対策	3.x 以前
マルウェア対策	4.x 以降
ディスク暗号化	3.x 以前および 4.x 以降
パッチ管理	3.x 以前および 4.x 以降
USB	4.x 以降
非 OPSWAT	
ファイル（File）	すべてのバージョン
Application	すべてのバージョン
複合	すべてのバージョン
レジストリ	すべてのバージョン
サービス	すべてのバージョン

（注）
- 上記のバージョンのいずれかがインストールされた可能性のあるクライアントを予測して、バージョン 3.x 以前およびバージョン 4.x 以降用に別個のポスチャ ポリシーを作成する必要があります。
- OESIS バージョン 4 のサポートはコンプライアンス モジュール 4.x および Cisco AnyConnect 4.3 以降に提供されます。しかし、AnyConnect 4.3 は OESIS バージョン 3 とバージョン 4 のポリシーの両方をサポートします。
- バージョン 4 コンプライアンス モジュールは、ISE 2.1 以降でサポートされています。

ポスチャ コンプライアンスのチェック

ステップ 1 Cisco ISE にログインし、ダッシュボードにアクセスします。

ステップ 2 [ポスチャ コンプライアンス（Posture Compliance）] ダッシュレットで、カーソルを積み上げ棒またはスパークラインに合わせます。

ツール チップに詳細情報が示されます。

ステップ 3 データ カテゴリを展開すると、詳細を参照できます。

ステップ 4 [ポスチャ コンプライアンス（Posture Compliance）] ダッシュレットを大きくします。

詳細なリアルタイム レポートが表示されます。

（注） [コンテキストの可視性（Context Visibility ）] ウィンドウにポスチャ コンプライアンス レポートを表示できます。[コンテキストの可視性（Context Visibility ）] > [エンドポイント（Endpoints）] > [コンプライアンス（Compliance）] に移動します。このウィンドウには、コンプライアンス ステータス、場所、エンドポイント、およびカテゴリ別のアプリケーションに基づいてさまざまなチャートが表示されます。

アクティブなセッションがないエンドポイントのポスチャ ステータスが表示される場合があります。たとえば、エンドポイントの最新の既知のポスチャ ステータスが準拠の場合、エンドポイントセッションが終了していても、エンドポイントで次の更新を受信するまで、[コンテキストの可視性（Context Visibility）] ウィンドウのステータスは準拠のままになります。ポスチャ ステータスは、このエンドポイントが削除または消去されるまで、[コンテキストの可視性（Context Visibility）] ウィンドウで保持されます。

複合ポスチャ条件の作成

ポスチャ評価と検証のポスチャ ポリシーで使用できる複合条件を作成できます。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** > **[複合条件（Compound Conditions）]** > **[追加（Add）]** を選択します。

ステップ 2 フィールドに適切な値を入力します。

ステップ 3 条件を検証するために [式の確認（Validate Expression）] をクリックします。

ステップ 4 [送信（Submit）] をクリックします。

パッチ管理条件の作成

選択したベンダーのパッチ管理製品のステータスを確認するポリシーを作成できます。

たとえば、Microsoft System Center Configuration Manager（SCCM）、クライアント バージョン 4.x ソフトウェア製品がエンドポイントにインストールされているかどうかを確認する条件を作成できます。

（注） Cisco ISE および AnyConnect のサポート対象バージョンは次のとおりです。

- Cisco ISE バージョン 1.4 以降
- AnyConnect バージョン 4.1 以降

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** > **[パッチ管理条件（Patch Management Condition）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [名前（Name）] フィールドに条件名を入力し、[説明（Description）] フィールドにその説明を入力します。

ステップ 4 [オペレーティングシステム（Operating System）] ドロップダウン フィールドから、適切なオペレーティング システムを選択します。

ステップ 5 ドロップダウン リストから [コンプライアンスモジュール（Compliance Module）] を選択します。

ステップ 6 ドロップダウン リストから [ベンダー名（Vendor Name）] を選択します。

ステップ 7 [チェックタイプ（Check Type）] を選択します。

ステップ 8 [インストール済みパッチの確認（Check Patches Installed）] ドロップダウン リストから適切なパッチを選択します。

ステップ 9 [送信（Submit）] をクリックします。

関連トピック

パッチ管理条件の設定 （61 ページ）
パッチ管理修復の追加 （80 ページ）

ディスク暗号化条件の作成

エンドポイントが指定されたデータ暗号化ソフトウェアに準拠しているかどうかを確認するポリシーを作成できます。

たとえば、C: ドライブがエンド ポイントで暗号化されているかどうかを確認する条件を作成できます。C: ドライブが暗号化されていない場合、エンド ポイントはコンプライアンス違反通知を受信し、ISE はメッセージをログに記録します。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。AnyConnect ISE ポスチャ エージェントを使用している場合にのみ、ポスチャ要件とディスク暗号化条件を関連付けることができます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ディスク暗号化条件（Disk Encryption Condition）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ディスク暗号化条件（Disk Encryption Condition）] ページで、フィールドに適切な値を入力します。

ステップ 4 [送信（Submit）] をクリックします。

ポスチャ条件の設定

ここでは、ポスチャに使用される単純条件および複合条件について説明します。

ファイル条件の設定

次の表では、[ファイル条件（File Conditions）] ウィンドウのフィールドについて説明します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ファイル条件（File Conditions）]** です。

表 *7:* ファイル条件の設定

フィールド名	**Windows OS** での使用ガイドライン	**Mac OS X** での使用ガイドライン
名前（**Name**）	ファイル条件の名前を入力します。	ファイル条件の名前を入力します。
説明	ファイル条件の説明を入力します。	ファイル条件の説明を入力します。
オペレーティング システム（**Operating System**）	ファイル条件が適用される Windows オペレーティング システムを選択します。	ファイル条件が適用される Mac OS X を選択します。
ファイル タイプ（**File Type**）	次のいずれか 1 つの事前定義済み設定を選択します。 • FileDate：特定のファイル作成日またはファイル更新日のファイルがシステムに存在するかどうかをチェックします。 • FileExistence：システムにファイルが存在するかどうかをチェックします。 • FileVersion：特定のバージョンのファイルがシステムに存在するかどうかをチェックします。 • CRC32：チェックサム関数を使用してファイルのデータ整合性をチェックします。 • SHA-256：ハッシュ関数を使用してファイルのデータ整合性をチェックします。	次のいずれか 1 つの事前定義済み設定を選択します。 • FileDate：特定のファイル作成日またはファイル更新日のファイルがシステムに存在するかどうかをチェックします。 • FileExistence：システムにファイルが存在するかどうかをチェックします。 • CRC32：チェックサム関数を使用してファイルのデータ整合性をチェックします。 • SHA-256：ハッシュ関数を使用してファイルのデータ整合性をチェックします。 • PropertyList：loginwindow.plist などの plist ファイルのプロパティ値をチェックします。

フィールド名	**Windows OS** での使用ガイドライン	**Mac OS X** での使用ガイドライン
データ型と演算子（Data Type and Operator）	NA	（ファイル タイプとして [PropertyList] を選択した場合に限り使用可能）plist ファイル内で検索するデータ型またはキーの値を選択します。各データ型には、一連の演算子が含まれています。 • 未指定（Unspecified）：指定したキーの存在をチェックします。 演算子（Exists、DoesNotExist）を入力します。 • 番号（Number）：指定した番号データ型のキーをチェックします。 演算子（equals、does not equal、greater than、less than、greater than または equal to、less than または equal to）と値を入力します。 • 文字列（String）：指定した文字列データ型のキーをチェックします。 演算子（equals、does not equal、equals (ignore case)、starts with、does not start with、contains、does not contain、ends with、does not end with）と値を入力します。 • バージョン（Version）：バージョン文字列で指定したキーの値をチェックします。 演算子（earlier than、later than、same as）と値を入力します。

フィールド名	**Windows OS** での使用ガイドライン	**Mac OS X** での使用ガイドライン
プロパティ名	NA	（ファイル タイプとして [PropertyList] を選択した場合に限り使用可能）キーの名前（たとえば BuildVersionStampAsNumber）を入力します。

フィールド名	**Windows OS** での使用ガイドライン	**Mac OS X** での使用ガイドライン
ファイル パス（**File Path**）		次のいずれか 1 つの事前定義済み設定を選択します。 • ルート（Root）：ルート（/）ディレクトリ内のファイルをチェックします。 ファイルのパスを入力します。 • ホーム（Home）：ホーム（~）ディレクトリ内のファイルをチェックします。 ファイルのパスを入力します。

フィールド名	Windows OS での使用ガイドライン	Mac OS X での使用ガイドライン
	次のいずれか 1 つの事前定義済み設定を選択します。 • ABSOLUTE_PATH：ファイルの完全修飾パスのファイルをチェックします。 例：C:\<directory>\file name。その他の設定では、ファイル名のみを入力します。 • SYSTEM_32：C:\WINDOWS\system32 ディレクトリ内のファイルをチェックします。ファイル名を入力します。 • SYSTEM_DRIVE：C:\ ドライブ内のファイルをチェックします。ファイル名を入力します。 • SYSTEM_PROGRAMS：C:\Program Files 内のファイルをチェックします。ファイル名を入力します。 • SYSTEM_ROOT：Windows システムのルートパス内のファイルをチェックします。ファイル名を入力します。 • USER_DESKTOP：指定したファイルが Windows ユーザのデスクトップにあるかどうかをチェックします。ファイル名を入力します。 • USER_PROFILE：ファイルが Windows ユーザのローカル プロファイル ディレクトリにあるかど	

フィールド名	**Windows OS** での使用ガイドライン	**Mac OS X** での使用ガイドライン
	うかをチェックします。ファイルのパスを入力します。	
ファイル日付タイプ（File Date Type）	（ファイル タイプとして [FileDate] を選択した場合に限り使用可能）[作成日（Creation Date）] または [変更日（Modification Date）] を選択します。	（ファイル タイプとして [FileDate] を選択した場合に限り使用可能）[作成日（Creation Date）] または [変更日（Modification Date）] を選択します。
ファイル演算子	[ファイル演算子（File Operator）] オプションは、[ファイル タイプ（File Type）] で選択した設定に応じて変化します。次の設定を適切に選択します。 FileDate • EarlierThan • LaterThan • EqualTo • 内部（Within）：最後の *n* 日数。有効な値は、1 ～ 300 日です） FileExistence • Exists • DoesNotExist FileVersion • EarlierThan • LaterThan • EqualTo	[ファイル演算子（File Operator）] オプションは、[ファイル タイプ（File Type）] で選択した設定に応じて変化します。次の設定を適切に選択します。 FileDate • EarlierThan • LaterThan • EqualTo • 内部（Within）：最後の *n* 日数。有効な値は、1 ～ 300 日です） FileExistence • Exists • DoesNotExist

フィールド名	Windows OS での使用ガイドライン	Mac OS X での使用ガイドライン
ファイルの CRC データ（File CRC Data）	（ファイル タイプとして [CRC32] を選択した場合に限り使用可能）チェックサムの値（たとえば 0x3c37fec3）を入力してファイルの整合性をチェックできます。チェックサム値は 16 進数の整数 0x で始まる必要があります。	（ファイル タイプとして [CRC32] を選択した場合に限り使用可能）チェックサムの値（たとえば 0x3c37fec3）を入力してファイルの整合性をチェックできます。チェックサム値は 16 進数の整数 0x で始まる必要があります。
ファイルのSHA-256データ（File SHA-256 Data）	（ファイル タイプとして [SHA-256] を選択した場合に限り使用可能）64 バイトの 16 進数のハッシュ値を入力してファイルの整合性をチェックできます。	（ファイル タイプとして [SHA-256] を選択した場合に限り使用可能）64 バイトの 16 進数のハッシュ値を入力してファイルの整合性をチェックできます。
日付および時刻（Date and Time）	（ファイル タイプとして **FileDate** を選択した場合に限り使用可能）クライアント システムの日付と時刻を、mm/dd/yyyy および hh:mm:ss 形式で入力します。	（ファイル タイプとして **FileDate** を選択した場合に限り使用可能）クライアント システムの日付と時刻を、mm/dd/yyyy および hh:mm:ss 形式で入力します。

関連トピック

単純ポスチャ条件 （24 ページ）
複合ポスチャ条件 （26 ページ）
ポスチャ条件の作成 （92 ページ）

ファイアウォール条件の設定

ファイアウォール条件により、特定のファイアウォール製品がエンドポイントで稼働しているかどうかがチェックされます。サポートされているファイアウォール製品のリストは、OPSWAT サポート チャートに基づいています。初回ポスチャと定期的再評価（PRA）の実行中にポリシーを適用できます。

Cisco ISE は、Windows および Mac OS のデフォルトのファイアウォール条件を提供します。これらの条件は、デフォルトで無効になっています。

フィールド名	使用上のガイドライン
名前（Name）	ファイアウォール条件の名前を入力します。
説明	ファイアウォール条件の説明を入力します。

フィールド名	使用上のガイドライン
コンプライアンス モジュール	必要なコンプライアンス モジュールを選択します。 • 4.x 以降 • 3.x 以降 • 任意のバージョン（Any Version）
オペレーティング システム	必要なファイアウォール製品がエンドポイントにインストールされているかどうかを確認します。Windows OS または Mac OSX を選択できます。
ベンダー	ドロップダウン リストからベンダー名を選択します。ベンダーのファイアウォール製品とそれらのチェック タイプが取得され、[選択したベンダーの製品（Products for Selected Vendor）]テーブルに表示されます。テーブル内のリストは、選択したオペレーティング システムによって変わります。
チェック タイプ（**Check Type**）	[有効（Enabled）]：特定のファイアウォールがエンドポイントで稼働しているかどうかをチェックします。ベンダーの製品が選択したチェック タイプをサポートしているかどうかを [選択したベンダーの製品（Products for Selected Vendor）] リストを参照することで確認します。

レジストリ条件の設定

次の表では、[レジストリ条件（Registry Conditions）] ウィンドウのフィールドについて説明します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）]>[ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [レジストリ条件（Registry Conditions）]** です。

表 *8*: レジストリ条件の設定

フィールド名	使用上のガイドライン
名前（**Name**）	レジストリ条件の名前を入力します。
説明	レジストリ条件の説明を入力します。

フィールド名	使用上のガイドライン
レジストリ タイプ（**Registry Type**）	レジストリ タイプとして事前定義済み設定の 1 つを選択します。
レジストリ ルート キー（**Registry Root Key**）	レジストリ ルート キーとして事前定義済み設定の 1 つを選択します。
サブ キー（**Sub Key**）	レジストリ ルート キーに指定されたパスのレジストリ キーをチェックするには、バックスラッシュ（「\」）なしでサブ キーを入力します。 たとえば、SOFTWARE\Symantec\Norton AntiVirus\version によって、次のパスのキーがチェックされます。 HKLM\SOFTWARE\Symantec\NortonAntiVirus\version
値の名前（**Value Name**）	（[レジストリ タイプ（Registry Type）] として [RegistryValue] または [RegistryValueDefault] を選択した場合にのみ使用可能） [RegistryValue] をチェックするレジストリ キー値の名前を入力します。 これは [RegistryValueDefault] のデフォルト フィールドです。
値データ型（**Value Data Type**）	（[レジストリ タイプ（Registry Type）] として [RegistryValue] または [RegistryValueDefault] を選択した場合にのみ使用可能）次の設定の 1 つを選択します。 • [未指定（Unspecified）]：レジストリ キー値があるかどうかをチェックします。このオプションは、[RegistryValue] の場合にのみ使用できます。 • [数字（Number）]：レジストリ キー値の指定された数字をチェックします • [文字列（String）]：レジストリ キー値の文字列をチェックします • [バージョン（Version）]：レジストリ キー値のバージョンをチェックします
値演算子（**Value Operator**）	設定を適切に選択します。

フィールド名	使用上のガイドライン
値データ	（[レジストリ タイプ（Registry Type）] として [RegistryValue] または [RegistryValueDefault] を選択した場合にのみ使用可能）[値データ型（Value Data Type）] で選択したデータ型に応じてレジストリ キーの値を入力します。
オペレーティング システム	レジストリ条件を適用する必要のあるオペレーティング システムを選択します。

関連トピック

単純ポスチャ条件 （24 ページ）
複合ポスチャ条件 （26 ページ）

アプリケーション条件の設定

次の表に、[アプリケーション条件（Application Conditions）] ページのフィールドを示します。このページへのナビゲーション パスは、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [アプリケーション条件（Application Conditions）]** です。

表 *9:* アプリケーション条件の設定

フィールド	使用上のガイドライン
[名前（Name）]	アプリケーションの条件の名前を入力します。
説明	アプリケーションの状態の説明を入力します。
オペレーティング システム（Operating System）	アプリケーション条件が適用される Windows OS または MAC OSX を選択します。
プロセス名	調べるアプリケーションの名前を入力します。
アプリケーション演算子（Application Operator）	調べるステータスを選択します。

関連トピック

単純ポスチャ条件 （24 ページ）
複合ポスチャ条件 （26 ページ）

継続的なエンドポイント属性モニタリング

ポスチャ アセスメントの実行中に動的な変更が確認されるようにするため、AnyConnect エージェントを使用してさまざまなエンドポイント属性を継続的にモニタします。これによりエン

ドポイントの全体的な可視性が向上し、動作に基づいてポスチャ ポリシーを作成できるようになります。AnyConnect エージェントは、エンドポイントにインストールされ実行されているアプリケーションをモニタします。この機能をオンまたはオフにできます。また、データのモニタ頻度を設定できます。デフォルトでは、データは5分間隔で収集され、データベースに保存されます。初回ポスチャでは、AnyConnectがすべての実行中アプリケーションとインストールされているアプリケーションのリストを報告します。初回ポスチャの後に、AnyConnectエージェントはX分間隔でアプリケーションをスキャンし、最終スキャンでの差異をサーバに送信します。サーバはすべての実行中アプリケーションとインストールされているアプリケーションのリストを表示します。

アプリケーション条件の設定

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に対するアプリケーション条件クエリ。これにより、エンドポイントで配信されているソフトウェアの集約された可視性を確認できます。たとえば、この情報に基づいてポリシーを作成し、デスクトップ チームと協力してソフトウェア ライセンスの数を減らすことができます。

次の表に、[アプリケーション条件（Application Conditions）]ページのフィールドを示します。このページへのナビゲーション パスは **[ワーク センター（Work Centers）]** > **[ポスチャ（Posture）]** > **[ポリシー要素（Policy Elements）]** > **[アプリケーション条件（Application Condition）]** > **[追加（Add）]** です。

フィールド名	使用上のガイドライン
名前（Name）	アプリケーション条件の名前を入力します。
説明	アプリケーション条件の説明を入力します。
オペレーティング システム	アプリケーション条件が適用される Windows OS または MAC OSX を選択します。
コンプライアンス モジュール	OESIS バージョン 4.x 以降、3.x 以前、またはすべてのバージョンのサポート。
次を確認（Check By）	次のいずれかを実行します。 • [プロセス（Process）] : エンドポイントでプロセスが実行されているかどうかを確認するには、このオプションをオンにします。 • [アプリケーション（Application）] : エンドポイントでアプリケーションが実行されているかどうかを確認するには、このオプションをオンにします。

フィールド名	使用上のガイドライン
プロセス名	（[次を確認（Check By）] オプションで [プロセス（Process）] を選択した場合に使用可能）必要なプロセス名を入力します。
アプリケーション演算子（**Application Operator**）	（[次を確認（Check By）] オプションで [プロセス（Process）] を選択した場合に使用可能）次のいずれかを選択します。 • [実行中（Running）]：エンドポイントでアプリケーションが実行されているかどうかを確認するには、このオプションを選択します。 • [実行されていない（Not Running）]：エンドポイントでアプリケーションが実行されていないかどうかを確認するには、このオプションをオンにします。
アプリケーションの状態（**Application State**）	（[次を確認（Check By）] オプションで [アプリケーション（Application）] を選択した場合に使用可能）次のいずれかを選択します。 • [インストール済み（Installed）]：クライアントのシステムに悪質なアプリケーションがインストールされているかどうかを調べるには、このオプションをオンにします。 悪意のあるアプリケーションがある場合は、修復アクションがトリガーされます。 • [実行中（Running）]：エンドポイントでアプリケーションが実行されているかどうかを確認するには、このオプションをオンにします。

フィールド名	使用上のガイドライン
次をプロビジョニング（**Provision By**）	（[次を確認（Check By）] オプションで [アプリケーション（Application）] を選択した場合に使用可能）次のいずれかを選択します。 • [すべて（Everything）] : [ブラウザ（Browser）]、[パッチ管理（Patch Management）] など、リストされているすべてのカテゴリを選択できます。 • [名前（Name）] : 1 つ以上のカテゴリを選択します。 たとえば [ブラウザ（Browser）] カテゴリを選択すると、[ベンダー（Vendor）] ドロップダウン リストに対応するベンダーが表示されます。 • [カテゴリ（Category）] : 1 つ以上のカテゴリ（[マルウェア対策（Anti-Malware）]、[バックアップ（Backup）]、[ブラウザ（Browser）]、[データストレージ（Data Storage）] など）をオンにできます。 （注） カテゴリは OPSWAT ライブラリから動的に更新されます。

[コンテキストの可視性（Context Visibility）] > **[エンドポイント（Endpoints）]** > **[コンプライアンス（Compliance）]** ウィンドウで、各エンドポイントでインストールされているアプリケーションと実行中のアプリケーションの数を確認できます。

[ホーム（Home）] > **[概要（Summary）]** > **[コンプライアンス（Compliance）]** ウィンドウに、ポスチャアセスメント対象であり準拠しているエンドポイントのパーセンテージが表示されます。

サービス条件の設定

次の表では、[サービス条件（Service Conditions）] ウィンドウのフィールドについて説明します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** > **[サービス条件（Service Condition）]** です。

表 *10* : サービス条件の設定

フィールド名	使用上のガイドライン
名前（**Name**）	サービス条件の名前を入力します。

フィールド名	使用上のガイドライン
説明	サービス条件の説明を入力します。
オペレーティング システム（**Operating Systems**）	サービス条件を適用する必要のあるオペレーティングシステムを選択します。Windows OSまたはMac OSXのさまざまなバージョンを選択できます。
サービス名（**Service Name**）	ルートとして動作するデーモンまたはユーザエージェントサービスの名前を入力します（たとえばcom.apple.geod）。AnyConnectエージェントは、コマンド **sudo launchctl list** を使用してサービス条件を確認します。
サービス タイプ	クライアントのコンプライアンスを確実にするためにAnyConnectが調べる必要があるタイプ オブ サービスを選択します。 • [デーモン（Daemon）]：マルウェアに対するクライアントデバイスのスキャンなど、指定したサービスがクライアントのデーモンサービスの指定されたリストにあるかどうかをチェックします。 • [ユーザエージェント（User Agent）]：マルウェアが検出された場合に実行するサービスなど、指定したサービスがクライアントのユーザサービスの指定されたリストにあるかどうかをチェックします。 • [デーモンまたはユーザエージェント（Daemon or User Agent）]：指定したサービスがデーモンまたはユーザエージェントのサービスリストにあるかどうかをチェックします。

フィールド名	使用上のガイドライン
サービス オペレータ（Service Operator）	クライアントでチェックするサービス ステータスを選択します。 • [Windows OS]：サービスが [実行している（Running）] か、または [実行していない（Not Running）] かをチェックします。 • [Mac OSX]：サービスが [ロード済み（Loaded）] か、[ロードされていない（Not Loaded）] か、[ロード済みで実行している（Loaded and Running）] か、[終了コード付きでロード済み（Loaded with Exit Code）] か、[ロード済みで実行しているまたは終了コードが付いている（Loaded & running or with Exit code）] かどうかをチェックします。

関連トピック

単純ポスチャ条件 （24 ページ）
複合ポスチャ条件 （26 ページ）

ポスチャ複合条件の設定

次の表に、[複合条件（Compound Conditions）] ウィンドウのフィールドを示します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** > **[複合条件（Compound Conditions）]** です。

表 *11* : ポスチャ複合条件の設定

フィールド名	使用上のガイドライン
名前（Name）	作成する複合条件の名前を入力します。
説明	作成する複合条件の説明を入力します。
オペレーティング システム	1 つ以上の Windows オペレーティング システムを選択します。これにより、条件が適用される Windows オペレーティング システムを関連付けることができます。
カッコ ( )（Parentheses ( )）	ファイル、レジストリ、アプリケーション、サービス条件という単純な条件タイプから 2 つの単純条件を組み合わせるには、カッコをクリックします。

フィールド名	使用上のガイドライン
（&）：AND 演算子（AND 演算子には「&」を使用します）	複合条件内には AND 演算子（アンパサンド（&））を使用できます。たとえば、**Condition1 & Condition2** と入力します。
（|）：OR 演算子（OR 演算子には「|」を使用します）	複合条件内には OR 演算子（縦線「|」）を使用できます。たとえば、**Condition1 & Condition2** と入力します。
（!）：NOT 演算子（NOT 演算子には「!」を使用します）	複合条件内には NOT 演算子（感嘆符（!））を使用できます。たとえば、**Condition1 & Condition2** と入力します。
単純条件	ファイル、レジストリ、アプリケーション、サービス条件という単純条件のリストから選択します。 また、オブジェクト セレクタからファイル、レジストリ、アプリケーション、サービス条件という単純条件を作成できます。 ファイル、レジストリ、アプリケーション、サービス条件という単純条件を作成するには、[操作（Action）] ボタンのクイック ピッカー（下向き矢印）をクリックします。

関連トピック

ポスチャ条件 （24 ページ）
複合ポスチャ条件の作成 （32 ページ）

ウイルス対策条件の設定

次の表では、[ウイルス対策条件（Anti-Virus Condition）] ウィンドウのフィールドについて説明します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ウイルス対策条件（Anti-Virus Condition）]** です。

表 *12 :* ウイルス対策条件の設定

フィールド名	使用上のガイドライン
名前（Name）	作成するウイルス対策条件の名前を入力します。
説明	作成するウイルス対策条件の説明を入力します。

フィールド名	使用上のガイドライン
オペレーティング システム	オペレーティング システムを選択して、クライアント上のアンチウイルス プログラムのインストールをチェックするか、または条件が適用される最新のアンチウイルス定義ファイルの更新をチェックします。
ベンダー	ドロップダウン リストからベンダーを選択します。ベンダーを選択すると、アンチウイルス製品およびバージョンが取得され、[選択したベンダーの製品（Products for Selected Vendor）] テーブルに表示されます。
チェック タイプ（**Check Type**）	クライアント上でインストールをチェックするか、または最新の定義ファイルの更新をチェックするかを選択します。
インストール	クライアント上のアンチウイルス プログラムのインストールのみをチェックする場合に選択します。
定義（**Definition**）	クライアント上のアンチウイルス製品の、最新の定義ファイルの更新のみをチェックする場合に選択します。
最新の AV 定義ファイルのバージョンに対してチェックします（使用可能な場合）（**Check against latest AV definition file version, if available**）	（[定義（Definition）] チェック タイプを選択した場合にのみ使用可能）クライアントのアンチウイルス定義ファイルのバージョンをチェックする場合に選択します。Cisco ISE でのポスチャ更新の結果として、最新のアンチウイルス定義ファイルのバージョンを使用できるときには、そのバージョンに対するチェックが行われます。それ以外の場合、このオプションを使用すると、クライアント上の定義ファイルの日付を、Cisco ISE の最新の定義ファイルの日付に対してチェックできます。

フィールド名	使用上のガイドライン
ウイルス定義ファイルを（有効）にすることを許可する（**Allow virus definition file to be (Enabled)**）	（定義チェック タイプを選択した場合のみ使用可能）アンチウイルス定義ファイルのバージョンと、クライアント上の最新のアンチウイルス定義ファイルの日付をチェックする場合に選択します。最新の定義ファイルの日付が、製品の最新のアンチウイルス定義ファイルの日付または現在のシステム日付から、次のフィールド（[より古い日数（days older than）] フィールド）で定義した日数よりも古いことは許容されません。 オフにした場合、[最新の AV 定義ファイルのバージョンに対してチェックします（使用可能な場合）。（Check against latest AV definition file version, if available.）] オプションを使用してアンチウイルス定義ファイルのバージョンのみをチェックすることができます。
より古い日数（**Days Older Than**）	クライアント上の最新のアンチウイルス定義ファイルの日付が、製品の最新のアンチウイルス定義ファイルの日付または現在のシステム日付よりも何日古いことが許容されるかを定義します。デフォルト値は 0 です。
最新のファイルの日付（**Latest File Date**）	[より古い日数（days older than）] クライアント上のアンチウイルス定義ファイルの日付をチェックすることを選択します。この日付は、フィールドで定義した日数だけ古いことが許容されます。 日数をデフォルト値（0）に設定する場合、クライアント上のアンチウイルス定義ファイルの日付が、製品の最新のアンチウイルス定義ファイルの日付よりも古いことは許容されません。
現在のシステム日付（**Current System Date**）	[より古い日数（days older than）] クライアント上のアンチウイルス定義ファイルの日付をチェックすることを選択します。この日付は、フィールドで定義した日数だけ古いことが許容されます。 日数をデフォルト値（0）に設定する場合、クライアント上のアンチウイルス定義ファイルの日付が、現在のシステム日付よりも古いことは許容されません。

フィールド名	使用上のガイドライン
選択したベンダーの製品（Products for Selected Vendor）	テーブルからアンチウイルス製品を選択します。[新しいアンチウイルス条件（New Anti-virus Compound Condition）] ページで選択したベンダーに基づいて、テーブルは、アンチウイルス製品およびバージョン、提供する修復のサポート、最新の定義ファイルの日付とバージョンに関する情報を取得します。 テーブルから製品を選択すると、アンチウイルス プログラムのインストールをチェックしたり、最新のアンチウイルス定義ファイルの日付および最新バージョンをチェックしたりできます。

関連トピック

複合ポスチャ条件 （26 ページ）
事前設定済みアンチウイルスおよびアンチスパイウェア条件 （28 ページ）
アンチウイルスとアンチスパイウェア サポート表 （28 ページ）

アンチスパイウェア複合条件の設定

次の表に、[AS複合条件（AS Compound Conditions）] ウィンドウのフィールドを示します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[AS複合条件（AS Compound Condition）]** です。

表 *13*：アンチスパイウェア複合条件の設定

フィールド名	使用上のガイドライン
名前（Name）	作成するアンチスパイウェア複合条件の名前を入力します。
説明	作成するアンチスパイウェア複合条件の説明を入力します。
オペレーティング システム（Operating System）	オペレーティング システムを選択すると、クライアント上のアンチスパイウェア プログラムのインストールをチェックするか、または条件が適用される最新のアンチスパイウェア定義ファイルの更新をチェックすることができます。

フィールド名	使用上のガイドライン
Vendor	ドロップダウン リストからベンダーを選択します。ベンダーを選択すると、アンチスパイウェア製品およびバージョンが取得され、[選択したベンダーの製品（Products for Selected Vendor）] テーブルに表示されます。
チェック タイプ（**Check Type**）	クライアント上でインストールをチェックするか、または最新の定義ファイルの更新をチェックするか、いずれかのタイプを選択します。
インストール	クライアント上のアンチスパイウェア プログラムのインストールのみをチェックする場合に選択します。
定義（**Definition**）	クライアント上のアンチスパイウェア製品の、最新の定義ファイルの更新のみをチェックする場合に選択します。
ウイルス定義ファイルを（有効）にすることを許可する（**Allow Virus Definition File to be (Enabled)**）	このチェックボックスは、アンチスパイウェア定義チェック タイプを作成するときはオンにし、アンチスパイウェア インストール チェック タイプを作成するときはオフにします。 オンにすると、その選択により、クライアント上のアンチスパイウェア定義ファイルのバージョンおよび最新のアンチスパイウェア定義ファイルの日付をチェックできます。最新の定義ファイルの日付が、現在のシステム日付から、[より古い日数（days older than）] フィールドで定義した日数より古いことは許容されません。 オフの場合、その選択により、[ウイルス定義ファイルを（有効）にすることを許可する（Allow virus definition file to be (Enabled)）] チェックボックスがオフのときに、アンチスパイウェア定義ファイルのバージョンのみをチェックすることができます。
より古い日数（**Days Older Than**）	クライアント上の最新のアンチスパイウェア定義ファイルの日付が、現在のシステム日付よりも何日古いことが許容されるかを定義します。デフォルト値は 0 です。

フィールド名	使用上のガイドライン
現在のシステム日付（**Current System Date**）	[より古い日数（days older than）] クライアント上のアンチスパイウェア定義ファイルの日付をチェックすることを選択します。この日付は、フィールドで定義した日数だけ古いことが許容されます。 日数をデフォルト値（0）に設定する場合、クライアント上のアンチスパイウェア定義ファイルの日付が、現在のシステム日付よりも古いことは許容されません。
選択したベンダーの製品（**Products for Selected Vendor**）	テーブルからアンチスパイウェア製品を選択します。[新しいアンチスパイウェア複合条件（New Anti-spyware Compound Condition）] ページで選択したベンダーに基づいて、テーブルは、アンチスパイウェア製品およびバージョン、提供する修復のサポート、最新の定義ファイルの日付とバージョンに関する情報を取得します。 テーブルから製品を選択すると、アンチスパイウェア プログラムのインストールをチェックしたり、最新のアンチスパイウェア定義ファイルの日付および最新バージョンをチェックしたりできます。

関連トピック

複合ポスチャ条件 （26 ページ）
事前設定済みアンチウイルスおよびアンチスパイウェア条件 （28 ページ）
アンチウイルスとアンチスパイウェア サポート表 （28 ページ）

マルウェア対策条件の設定

マルウェア対策条件はスパイウェア対策条件とウイルス対策条件の組み合わせで、OESIS バージョン 4.x 以降のコンプライアンス モジュールでサポートされています。次の表では、[マルウェア対策条件（Antimalware Conditions）] ウィンドウのフィールドについて説明します。ナビゲーションパスは、**[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）] > [マルウェア対策（Antimalware）]** です。また、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [マルウェア対策条件（Antimalware Condition）]** ウィンドウでもこのオプションにアクセスできます。

（注） 最新の定義が適用されるようにインストールしたマルウェア対策製品を手動で1回以上更新することをお勧めします。更新しないと、マルウェア対策定義のAnyConnectを使用したポスチャチェックが失敗します。

表 *14 :* マルウェア対策条件の設定

フィールド名	使用上のガイドライン
名前（**Name**）	マルウェア対策条件の名前を入力します。
説明	マルウェア対策条件の説明を入力します。
コンプライアンス モジュール	OESIS バージョン 4.x 以降のサポート。
オペレーティング システム（**Operating System**）	オペレーティング システムを選択して、クライアント上のマルウェア対策プログラムのインストールをチェックするか、または条件が適用される最新のマルウェア対策定義ファイルの更新をチェックします。MAC と Windows OS の両方をサポートしています。
Vendor	ドロップダウン リストからベンダーを選択します。選択したベンダーのマルウェア対策製品、バージョン、最新の定義日、最新の定義バージョン、最小コンプライアンス モジュール バージョンが [選択したベンダーの製品（Products for Selected Vendor）] テーブルに表示されます。
チェック タイプ（**Check Type**）	クライアント上でインストールをチェックするか、または最新の定義ファイルの更新をチェックするかを選択します。
インストール	クライアント上のマルウェア対策プログラムのインストールのみをチェックする場合に選択します。
定義（**Definition**）	クライアント上のマルウェア対策製品の、最新の定義ファイルの更新のみをチェックする場合に選択します。

フィールド名	使用上のガイドライン
最新の AV 定義ファイルのバージョンに対してチェックします（使用可能な場合）（**Check Against Latest AV Definition File Version, if Available**）	（[定義（Definition）] チェック タイプを選択した場合にのみ使用可能）クライアントのマルウェア対策定義ファイルのバージョンをチェックする場合に選択します。Cisco ISE でのポスチャ更新の結果として、最新のマルウェア対策定義ファイルのバージョンを使用できるときには、そのバージョンに対するチェックが行われます。それ以外の場合、このオプションを使用すると、クライアント上の定義ファイルの日付を、Cisco ISE の最新の定義ファイルの日付に対してチェックできます。 このチェックは、選択した製品の [最新の定義日（Latest Definition Date）] または [最新の定義バージョン（Latest Definition Version）] フィールドの Cisco ISE に値が記載されている場合にのみ機能します。そうでない場合は、[現在のシステム日付（Current System Date）] フィールドを使用する必要があります。
ウイルス定義ファイルを（有効）にすることを許可する（**Allow Virus Definition File to be (Enabled)**）	（定義チェック タイプを選択した場合のみ使用可能）マルウェア対策定義ファイルのバージョンと、クライアント上の最新のマルウェア対策定義ファイルの日付をチェックする場合に選択します。最新の定義ファイルの日付が、製品の最新のマルウェア対策定義ファイルの日付または現在のシステム日付から、次のフィールド（[より古い日数（days older than）] フィールド）で定義した日数よりも古いことは許容されません。 オフにした場合、[最新の AV 定義ファイルのバージョンに対してチェックします（使用可能な場合）。（Check against latest AV definition file version, if available.）] オプションを使用してマルウェア対策定義ファイルのバージョンのみをチェックすることができます。
より古い日数（**Days Older Than**）	クライアント上の最新のマルウェア対策定義ファイルの日付が、製品の最新のマルウェア対策定義ファイルの日付または現在のシステム日付よりも何日古いことが許容されるかを定義します。デフォルト値は 0 です。

フィールド名	使用上のガイドライン
最新のファイルの日付（**Latest File Date**）	クライアント上のマルウェア対策定義ファイルの日付をチェックすることを選択します。この日付は、[より古い日数（days older than）] フィールドで定義した日数だけ古いことが許容されます。 日数をデフォルト値（0）に設定する場合、クライアント上のマルウェア対策定義ファイルの日付が、製品の最新のマルウェア対策定義ファイルの日付よりも古いことは許容されません。 このチェックは、選択した製品の [最新の定義日（Latest Definition Date）] フィールドの Cisco ISE に値が記載されている場合にのみ機能します。そうでない場合は、[現在のシステム日付（Current System Date）] フィールドを使用する必要があります。
現在のシステム日付（**Current System Date**）	クライアント上のマルウェア対策定義ファイルの日付をチェックすることを選択します。この日付は、[より古い日数（days older than）] フィールドで定義した日数だけ古いことが許容されます。 日数をデフォルト値（0）に設定する場合、クライアント上のマルウェア対策定義ファイルの日付が、現在のシステム日付よりも古いことは許容されません。
選択したベンダーの製品（**Products for Selected Vendor**）	テーブルからマルウェア対策製品を選択します。[新しいマルウェア対策条件（New Antimalware Condition）] ページで選択したベンダーに基づいて、テーブルは、マルウェア対策製品およびバージョン、提供する修復のサポート、最新の定義ファイルの日付とバージョンに関する情報を取得します。 テーブルから製品を選択すると、マルウェア対策プログラムのインストールをチェックしたり、最新のマルウェア対策定義ファイルの日付および最新バージョンをチェックしたりできます。

関連トピック

複合ポスチャ条件 （26 ページ）

ディクショナリ単純条件の設定

次の表に、[ディクショナリ単純条件（Dictionary Simple Conditions）] ウィンドウのフィールドを示します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ディクショナリ単純条件（Dictionary Simple Conditions）]** です。

表 *15*：ディクショナリ単純条件の設定

フィールド名	使用上のガイドライン
[名前（Name）]	作成するディクショナリ単純条件の名前を入力します。
説明	作成するディクショナリ単純条件の説明を入力します。
属性（Attribute）	ディクショナリから属性を選択します。
演算子	選択した属性に値を関連付ける演算子を選択します。
値	ディクショナリ属性に関連付ける値を入力するか、またはドロップダウン リストから事前定義済みの値を選択します。

関連トピック

ディクショナリおよびディクショナリ属性
単純条件と複合条件
単純ポスチャ条件 （24 ページ）
単純ポスチャ条件の作成 （25 ページ）

ディクショナリ複合条件の設定

次の表に、[ディクショナリ複合条件（Dictionary Compound Conditions）] ウィンドウのフィールドを示します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）]>[ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ディクショナリ複合条件（Dictionary Compound Conditions）]** です。

表 *16*：ディクショナリ複合条件の設定

フィールド名	使用上のガイドライン
[名前（Name）]	作成するディクショナリ複合条件の名前を入力します。

フィールド名	使用上のガイドライン
説明	作成するディクショナリ複合条件の説明を入力します。
既存の条件をライブラリから選択（**Select Existing Condition from Library**）	ポリシー要素ライブラリから事前定義済みの条件を選択して式を定義するか、または後のステップでアドホック属性/値のペアを式に追加します。
条件名（**Condition Name**）	ポリシー要素ライブラリからすでに作成しているディクショナリ単純条件を選択します。
式（**Expression**）	[条件名（Condition Name）] ドロップダウンリストでの選択に基づいて式が更新されます。
AND または OR 演算子（**AND or OR operator**）	ライブラリから追加できるディクショナリ単純条件を論理的に組み合わせるには、AND または OR 演算子を選択します。 次の操作を行うには、[操作（Action）] アイコンをクリックします。 • 属性/値の追加（Add Attribute/Value） • ライブラリから条件を追加（Add Condition from Library） • 削除（Delete）
新しい条件の作成（高度なオプション）（**Create New Condition (Advance Option)**）	さまざまなシステムディクショナリまたはユーザ定義ディクショナリから属性を選択します。 後のステップで事前定義された条件をポリシー要素ライブラリから追加することもできます。
条件名（**Condition Name**）	すでに作成したディクショナリ単純条件を選択します。
式（**Expression**）	[式（Expression）] ドロップダウン リストから、ディクショナリ単純条件を作成できます。
演算子	属性に値を関連付ける演算子を選択します。
値	ディクショナリ属性に関連付ける値を入力するか、またはドロップダウン リストから値を選択します。

関連トピック

ディクショナリおよびディクショナリ属性

単純条件と複合条件
複合ポスチャ条件 （26 ページ）
複合ポスチャ条件の作成 （32 ページ）

パッチ管理条件の設定

次の表に、[パッチ管理条件（Patch Management Conditions）] ウィンドウのフィールドを示します。ナビゲーションパスは、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [パッチ管理条件（Patch Management Conditions）]** です。

表 *17* : パッチ管理条件

フィールド名	使用上のガイドライン
名前（Name）	パッチ管理条件の名前を入力します。
説明	パッチ管理条件の説明を入力します。
オペレーティング システム	オペレーティング システムを選択して、エンドポイント上のパッチ管理ソフトウェアのインストールをチェックするか、または条件が適用される最新のパッチ管理定義ファイルの更新をチェックします。Windows OS または Mac OSX を選択できます。また、パッチ管理条件を作成する複数のオペレーティング システムのバージョンを選択することもできます。
ベンダー名（Vendor Name）	ドロップダウン リストからベンダー名を選択します。ベンダーのパッチ管理製品とそれらのサポート対象バージョン、チェック タイプ、および最小対応モジュールのサポートが取得され、[選択したベンダーの製品（Products for Selected Vendor）] テーブルに表示されます。テーブル内のリストは、選択したオペレーティング システムによって変わります。

フィールド名	使用上のガイドライン
チェック タイプ（**Check Type**）	

フィールド名	使用上のガイドライン
	次のオプションのいずれかを選択します。 • [インストール（Installation）]：選択した製品がエンドポイントにインストールされているかどうかを確認します。 このチェック タイプは、すべてのベンダーでサポートされています。 （注） Cisco Temporal Agent の場合は、[要件（Requirements）]ページで[インストール（Installation）] チェック タイプを含むパッチ管理条件のみを表示できます。 • [有効（Enabled）]：選択した製品がエンドポイントで有効かどうかを確認します。ベンダーの製品が選択したチェック タイプをサポートしているかどうかを[選択したベンダーの製品（Products for Selected Vendor）]リストを参照することで確認します。 • [最新（Up to Date）]：選択した製品に欠けているパッチがないかどうかを確認します。ベンダーの製品が選択したチェック タイプをサポートしているかどうかを[選択したベンダーの製品（Products for Selected Vendor）] リストを参照することで確認します。 [ベンダー名（Vendor Name）] で指定したベンダーがサポートする製品のリストを表示するには、[選択したベンダーの製品（Products for Selected Vendor）] ドロップダウン矢印をクリックします。たとえば、製品 1 と 製品 2 の 2 つの製品を持つベンダーA を選択したとします。製品 1 は [有効（Enabled）] オプションをサポートしているが、製品 2 はサポートしていない場合があります。または、製品1がチェック タイプのいずれもサポートしていない場合は、グレー表示されます。 （注） （Cisco ISE 2.3 以降および AnyConnect 4.5 以上に適用されます）SCCM のパッチ管理条件で [最新（Up to Date）] チェック タイプを

フィールド名	使用上のガイドライン
	選択すると、Cisco ISE は次の動作を行います 1. Microsoft API を使用して、指定された重大度レベルの現在のセキュリティ パッチを確認します。 2. その欠落しているセキュリティ パッチに対するパッチ管理修復をトリガーします。
インストール済みパッチの確認（Check Patches Installed）	（[最新（Up To Date）] チェック タイプを選択している場合にのみ使用可能。）欠落しているパッチの重大度レベルを設定し、重大度に基づいて展開することができます。次の重大度レベルのいずれかを選択します。 • [クリティカルのみ（Critical Only）]：クリティカルなソフトウェアパッチが展開内のエンドポイントにインストールされているかどうかを確認します。 • [重要およびクリティカル（Important and Critical）]：重要かつクリティカルなソフトウェアパッチが展開内のエンドポイントにインストールされているかどうかを確認します。 • [中程度、重要およびクリティカル（Moderate, Important, & Critical）]：中程度、重要およびクリティカルなソフトウェアパッチが展開内のエンドポイントにインストールされているかどうかを確認します。 • [低程度からクリティカルまで（Low To Critical）]：低程度、中程度、重要、およびクリティカルなソフトウェアパッチが展開内のエンドポイントにインストールされているかどうかを確認します。 • [すべて（All）]：すべての重大度レベルの欠落しているパッチをインストールします。

関連トピック

ソフトウェア パッチのインストール
ソフトウェア パッチのロールバック
パッチのインストールおよびロールバックの変更の表示
パッチ管理条件の作成 （33 ページ）

ディスク暗号化条件の設定

次の表では、[ディスク暗号化条件（Disk Encryption Condition）] ウィンドウのフィールドについて説明します。ナビゲーションパスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ディスク暗号化条件（Disk Encryption Condition）] です。

表 *18* : ディスク暗号化条件の設定

フィールド名	使用上のガイドライン
名前（**Name**）	作成するディスク暗号化条件の名前を入力します。
説明	ディスク暗号化条件の説明を入力します。
オペレーティング システム	ディスクを暗号化のためにチェックするエンドポイントのオペレーティング システムを選択します。Windows OS または Mac OSX を選択できます。また、ディスク暗号化条件を作成するための複数のバージョンのオペレーティング システムを選択することもできます。
ベンダー名（**Vendor Name**）	ドロップダウン リストからベンダー名を選択します。ベンダーのデータ暗号化製品およびそれらのサポート対象バージョン、暗号化状態チェック、および最小対応モジュールサポートが取得され、[選択したベンダーの製品（Products for Selected Vendor）] テーブルに表示されますテーブル内のリストは、選択したオペレーティング システムによって変わります。

フィールド名	使用上のガイドライン
[所在地（Location）]	オプションが [選択したベンダーの製品（Products for Selected Vendor）] セクションでオンになっている場合にのみ有効です。次のオプションのいずれかを選択します。 • [特定のロケーション（Specific Location）]：指定したディスクドライブがエンドポイントで暗号化されているか（たとえば Windows OS の場合は C:）、または指定したボリュームラベルが暗号化されているか（たとえば、Mac OSX の場合は Mackintosh HD）を確認します。 • [システムロケーション（System Location）]：デフォルトの Windows OS のシステムドライブまたは Mac OSX のハードドライブがエンドポイントで暗号化されているかを確認します。 • [すべての内部ドライブ（All Internal Drives）]：内部のドライブを確認します。マウントおよび暗号化されたすべてのハードディスクと、すべての内部パーティションが含まれます。読み取りのみのドライブ、システム リカバリ ディスク/パーティション、ブート パーティション、ネットワーク パーティション、およびエンドポイント外のさまざまな物理ディスク ドライブ（USB およびサンダーボルトを介して接続されたディスク ドライブを含むがこれに限定されない）は除外されます。検証済みの暗号化ソフトウェア製品には次のものがあります。 • Bit-locker-6.x/10.x • Windows 7 上の Checkpoint 80.x

フィールド名	使用上のガイドライン
暗号化状態（Encryption State）	[暗号化状態（Encryption State）] チェックボックスは、選択した製品が暗号化状態チェックをサポートしていない場合はディセーブルになっています。リピータは、チェックボックスがオンになっている場合のみ表示されます。[完全に暗号化済み（Fully Encrypted）] オプションを選択して、クライアントのディスクドライブが完全に暗号化されているかどうかを確認できます。 たとえば TrendMicro に対し条件を作成し、2 つのベンダー（一方のベンダーの [暗号化状態（Encryption State）] は「はい（Yes）」でもう一方の [暗号化状態（Encryption State）] は「いいえ（No）」）を選択した場合、ベンダーの暗号化状態の一方が「いいえ（No）」になっているので [暗号化状態（Encryption State）] はディセーブルになります。 （注） リピータをクリックすることで追加のロケーションを追加でき、各ロケーション間の関係は論理 AND 演算子です。

関連トピック

ディスク暗号化条件の作成 （34 ページ）

USB 条件の設定

次の表では、[USB条件（USB Condition）] ウィンドウのフィールドについて説明します。ナビゲーションパスは、**[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [USB]** です。また、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [USB条件（USB Condition）]** ウィンドウに移動することもできます。

USB チェックは事前定義された条件で、Windows OS のみをサポートしています。

表 *19 : USB* 条件の設定

フィールド名	使用上のガイドライン
名前（Name）	USB_Check
説明	シスコの事前定義チェック
オペレーティング システム	Windows

フィールド名	使用上のガイドライン
コンプライアンス モジュール	バージョン 4.x 以降向けの、ISE のポスチャ準拠モジュールの表示専用フィールドのサポート。

関連トピック

単純ポスチャ条件 （24 ページ）

ハードウェア属性条件の設定

[ポリシー（Policy）]>[ポリシー要素（Policy Elements）]>[ハードウェア属性条件（Hardware Attributes Condition）] を選択して、[ハードウェア属性条件（Hardware Attributes Condition）] ウィンドウにアクセスします。次の表では、[ハードウェア属性条件（Hardware Attributes Condition）] ウィンドウのフィールドについて説明します。

フィールド名	使用上のガイドライン
名前（**Name**）	Hardware_Attributes_Check：条件に割り当てられたデフォルトの名前。
説明	クライアントからハードウェア属性を収集するシスコの事前定義済みチェック。
オペレーティング システム	Windows すべてまたは Mac OS
コンプライアンス モジュール	4.x 以降

関連トピック

ハードウェア ダッシュボード

ポスチャ外部データ ソース条件

エンドポイント UDID と外部データ ソースが一致する条件を設定できます。現在、Active Directory のみがサポートされています。ポスチャ エージェントで必要な、UDID を Active Directory に送信するスクリプトは、ISE に含まれていません。

ポスチャ ポリシーの設定

ポスチャ ポリシーは 1 つ以上の ID グループおよびオペレーティング システムに関連付けられたポスチャ要件の集合です。ディクショナリ属性は、デバイスの異なるポリシーを定義する、ID グループおよびオペレーティング システムと組み合わされたオプションの条件です。

Cisco ISE には、適合しないデバイスの猶予時間を設定するオプションが用意されています。デバイスが適合していないことが判明した場合、Cisco ISE はポスチャ評価結果キャッシュ内

で以前の正常な状態を検索し、デバイスに猶予時間を与えます。デバイスには、猶予期間中にネットワークへのアクセス権が付与されます。分、時、または日単位（最大 30 日）で猶予期間を設定できます。

詳細については、『ISE Posture Prescriptive Deployment Guide』の「Posture Policy」の項を参照してください。

（注）

- 猶予期間が延長または短縮されると、デバイスがポスチャ フローを再び通過した場合（たとえば、[遅延通知（Delayed Notification）] オプションが有効で、[再スキャン（Re-Scan）] オプションが選択されている場合、デバイスとネットワークの切断や再接続が行われます）、新しい猶予期間および遅延通知が適用されます。
- 猶予期間は Temporal Agent には適用されません。
- （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なると、アクセプタブル ユース ポリシー（AUP）は表示されません。

始める前に

- AUP について理解している必要があります。
- 定期的再評価（PRA）について理解している必要があります。
- AnyConnect エージェント 4.7 以降を使用して、コンプライアンス関連の通知を表示する必要があります。AnyConnect エージェントの設定に関する詳細については、AnyConnect 設定の作成 （125 ページ）を参照してください。

ステップ 1 **[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）]** を選択します。

ステップ 2 ドロップダウンの矢印を使用して新しいポリシーを追加します。

ステップ 3 プロファイルを編集するには、ポリシーをダブルクリックするか、または行の末尾にある [編集（Edit）] をクリックします。

ステップ 4 [ルールステータス（Rule Status）] ドロップダウン リストで [有効（Enabled）] または [無効（Disabled）] を選択します。

ステップ 5 [ポリシーオプション（Policy Options）] でドロップダウンを選択し、[猶予期間の設定（Grace Period Settings）] を分単位、時間単位、日単位で指定します。

有効な値は次のとおりです。

- 1 ～ 30 日
- 1 ～ 720 時間

- 1 ～ 43200 分

デフォルトでは、この設定は無効です。

（注） ポスチャ評価の結果が適合しない場合でも、デバイスが以前に準拠しており、キャッシュの期限がまだ切れていなければ、[猶予期間の設定（Grace Period Settings）] で指定された時間にわたり、デバイスにアクセス権が付与されます。

ステップ 6 （オプション）[遅延通知（Delayed Notification）] という名前のスライダをドラッグし、猶予期間の特定の割合が過ぎるまで、猶予期間プロンプトがユーザに遅れて表示されるようにします。たとえば、通知遅延期間が 50 % に設定され、設定されている猶予期間が 10 分の場合、Cisco ISE は 5 分後にポスチャ ステータスをチェックし、エンドポイントが準拠していないと判断した場合は猶予期間通知を表示します。エンドポイントのステータスが準拠している場合、猶予期間通知は表示されません。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。ただし、エンドポイントは、猶予期間の有効期限が切れるまで、アクセス権が付与されます。このフィールドのデフォルト値は 0% です。有効な範囲は 0 ～ 95% です。

ステップ 7 [ルール名（Rule Name）] フィールドに、ポリシーの名前を入力します。

（注） 予期しない結果を回避するためのベストプラクティスは、各要件でポスチャ ポリシーを個別のルールとして設定することです。

ステップ 8 [IDグループ（Identity Groups）] 列から任意の ID グループを選択します。

ユーザまたはエンドポイントの ID グループに基づいて、ポスチャ ポリシーを作成することができます。

ステップ 9 [オペレーティングシステム（Operating Systems）] 列からオペレーティング システムを選択します。

ステップ 10 [準拠モジュール（Compliance Module）] 列から必要な準拠モジュールを選択します。

- 4.x 以降（4.x or Later）：マルウェア対策、ディスク暗号化、Patch Management、および USB の各種条件をサポートします。
- 3.x 以前（3.x or Earlier）：ウイルス対策、スパイウェア対策、ディスク暗号化、および Patch Management の各種条件をサポートします
- すべてのバージョン（Any Version）：ファイル、サービス、レジストリ、アプリケーション、および複合の各種条件をサポートします。

ステップ 11 [ポスチャタイプ（Posture Type）] 列から、[ポスチャタイプ（Posture Type）] を選択します。

- [AnyConnect]：AnyConnect エージェントを展開し、クライアントとのやりとりが必要な Cisco ISE ポリシーを監視し、適用します。
- [AnyConnect ステルス（AnyConnect Stealth）]：AnyConnect エージェントを展開し、クライアントとやりとりしない Cisco ISE ポスチャ ポリシーを監視し、適用します。
- [Temporal Agent]：準拠のステータスを確認するためにクライアント上で実行される一時実行可能ファイル。

ステップ 12 [その他の条件（Other Conditions）] では、1 つ以上のディクショナリ属性を追加し、単純条件または複合条件としてディクショナリに保存できます。

（注） [ポスチャポリシー（Posture Policy）] ウィンドウで作成したディクショナリ単純条件とディクショナリ複合条件は、許可ポリシーを設定するときには表示されません。

ステップ 13 [要件（Requirements）] フィールドに要件を指定します。

ステップ 14 [保存（Save）] をクリックします。

AnyConnect のワークフローの設定

AnyConnect エージェントを設定するには、Cisco ISE で次の手順を実行します。

ステップ 1 AnyConnect エージェントプロファイルを作成します。

ステップ 2 AnyConnect パッケージの AnyConnect 設定を作成します。

ステップ 3 クライアント プロビジョニング ポリシーを作成します。

ステップ 4 （任意）カスタムポスチャを作成します。

ステップ 5 （任意）カスタム修復アクションを作成します。

ステップ 6 （任意）カスタムポスチャの要件を作成します。

ステップ 7 ポスチャポリシーを作成します。

ステップ 8 クライアント プロビジョニング ポリシーを設定します。

ステップ 9 認可プロファイルを作成します。

ステップ 10 認証ポリシーを設定します。

証明書ベースの条件のための前提条件

クライアント プロビジョニングおよびポスチャ ポリシーのルールに、証明書の属性に基づく条件を含めることができます。クライアント プロビジョニングまたはポスチャ ポリシーにおける証明書ベースの条件では、同じ証明書属性に基づいて一致する許可ポリシー ルールが存在することが前提条件になります。

たとえば、図に示されているように同じ属性を使用する必要があります。[発行者 - 共通名（Issuer – Common Name）] 属性が、クライアント プロビジョニングまたはポスチャと許可ポリシーの両方で使用されています。

図 *2 : Cisco* のプロビジョニング ポリシー

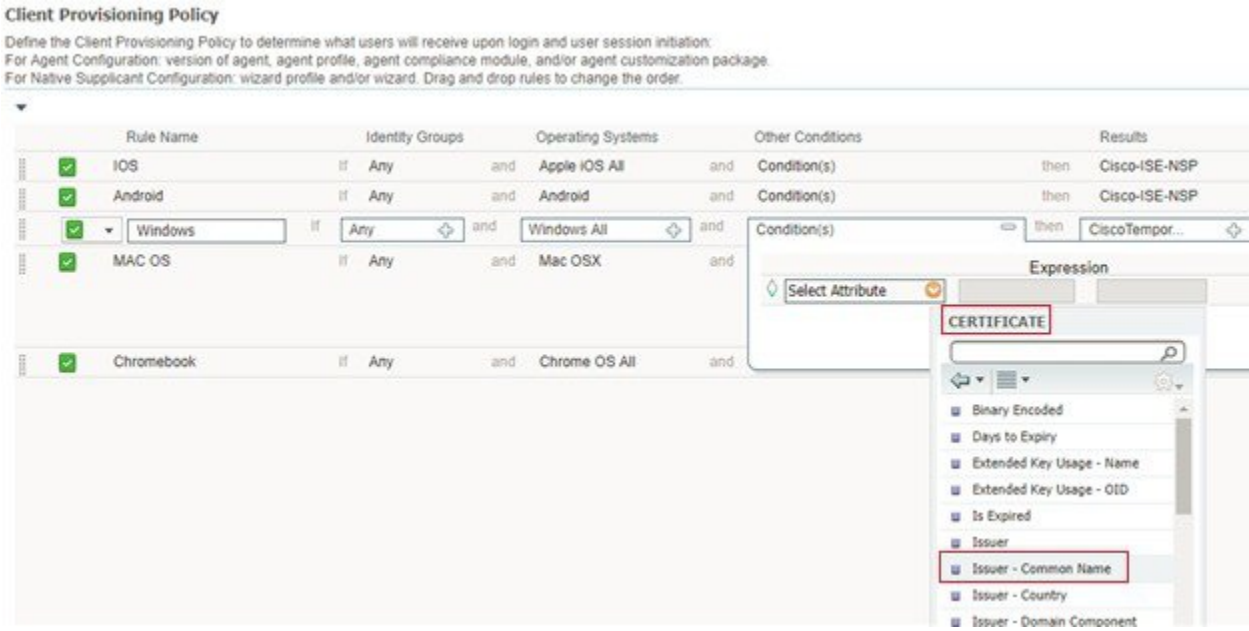
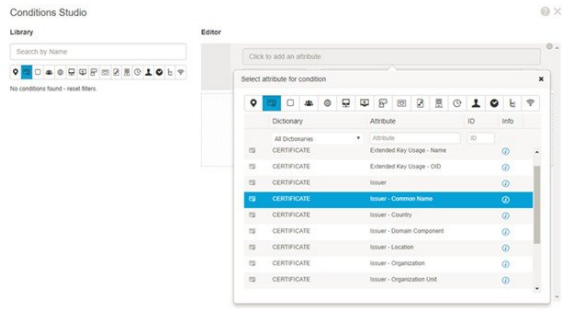


図 *3 : [*条件スタジオ（***Conditions Studio***）*]*



（注） ISE サーバ証明書は、AnyConnect 4.6 MR2 以降のシステム証明書ストアで信頼できる必要があります。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ない場合は機能しません。

- Windows OS：サーバ証明書をシステム証明書ストアに追加する必要があります。
- MAC OS：サーバ証明書をシステム キーチェーンに追加する必要があります。コマンドライン ユーティリティを使用して証明書を信頼することをお勧めします。キーチェーン アクセス アプリケーションを使用してシステム キーチェーンに証明書を追加しても、ログイン キーチェーンにすでに存在する場合は機能しないことがあります。

デフォルトのポスチャ ポリシー

Cisco ISE ソフトウェアには、ポスチャ ポリシーおよびプロファイルの作成を容易にする、事前設定されたポスチャ ポリシー（[ポリシー（Policy）]>[ポスチャ（Posture）]）が多数用意されています。これらのポリシーは、デフォルトで無効になっています。要件に基づいて、これらのポリシーを有効にできます。以下は、デフォルトのポスチャ ポリシーの一部です。

ルール名（**Rule Name**）	説明	要件
Default_Antimalware_Policy_Mac	エンドポイントに、サポートされているベンダーのマルウェア対策ソフトウェア（AnyConnect で認識されているもの）がインストールされ、デバイスで実行されているかどうかを確認します。	Any_AM_Installation
Default_Antimalware_Policy_Win	エンドポイントに、サポートされているベンダーのマルウェア対策ソフトウェア（AnyConnect で認識されているもの）がインストールされ、デバイスで実行されているかどうかを確認します。	Any_AM_Installation_Win
Default_AppVis_Policy_Mac	情報を収集し、特定のエンドポイントにインストールされているすべてのアプリケーションを報告します。	Default_AppVis_Requirement_Mac
Default_AppVis_Policy_Win	情報を収集し、特定のエンドポイントにインストールされているすべてのアプリケーションを報告します。	Default_AppVis_Requirement_Win
Default_Firewall_Policy_Mac	エンドポイントに、サポートされているベンダーのファイアウォール プログラム（AnyConnect で認識されているもの）がインストールされているかどうかを確認します。	Default_Firewall_Requirement_Mac

ルール名（**Rule Name**）	説明	要件
Default_Firewall_Policy_Win	エンドポイントに、サポートされているベンダーのファイアウォール プログラム（AnyConnect で認識されているもの）がインストールされているかどうかを確認します。	Default_Firewall_Requirement_Win
Default_USB_Block_Win	エンドポイント デバイスに USB ストレージ デバイスが接続されていないことを確認します。	USB_Block

クライアント ポスチャ評価

Cisco ISE を使用すると、適用されたネットワーク セキュリティ対策の適切さと効果を維持するために、保護されたネットワークにアクセスする任意のクライアントマシンに対してセキュリティ機能を検証し、そのメンテナンスを行うことができます。Cisco ISE 管理者は、クライアントマシンで最新のセキュリティ設定またはアプリケーションを使用できるよう設計されたポスチャ ポリシーを使用することによって、どのクライアント マシンでも、企業ネットワークへのアクセスについて定義されたセキュリティ標準を満たし、その状態を継続することを保証できます。ポスチャ コンプライアンス レポートによって、ユーザがログインしたとき、および定期的再評価が行われるたびに、クライアントマシンのコンプライアンス レベルのスナップショットが Cisco ISE に提供されます。

ポスチャ評価およびコンプライアンスは、Cisco ISE で提供される次のいずれかのエージェント タイプを使用して行われます。

- AnyConnect ISE Agent：Windows または Mac OS X クライアントにインストールできる永続的なエージェントであり、ポスチャ コンプライアンス機能を実行します。
- Cisco Temporal Agent：コンプライアンス ステータスを確認するためにクライアント上で実行される一時実行可能ファイル。エージェントは、ログインセッションが終了した後にクライアント マシンから削除されます。デフォルトでは、エージェントは Cisco ISE ISO イメージに存在し、インストール中に Cisco ISE にアップロードされます。

ポスチャ評価オプション

次の表に、Windows および Macintosh の ISE Posture Agent、および Windows の Web Agent でサポートされるポスチャ評価（ポスチャ条件）オプションのリストを示します。

表 *20 :* ポスチャ評価オプション

Windows 用 ISE ポスチャ エージェント	Windows 用 Cisco Temporal エージェント	Macintosh OS X 用 ISE ポスチャ エージェント	Macintosh OS X 用 Cisco Temporal エージェント
オペレーティング システム/サービス パック/ホットフィックス	—	—	—
サービス チェック	サービス チェック（Temporal エージェント 4.5 および ISE 2.3）	サービス チェック（AC 4.1 および ISE 1.4）	デーモン チェックはサポートされていません
レジストリ チェック	レジストリ チェック（Temporal エージェント 4.5 および ISE 2.3）	—	—
ファイル チェック	ファイル チェック（Temporal エージェント 4.5 および ISE 2.3）	ファイル チェック（AC 4.1 および ISE 1.4）	ファイル チェック（Temporal エージェント 4.5 および ISE 2.3）
アプリケーション チェック	アプリケーション チェック（Temporal エージェント 4.5 および ISE 2.3）	アプリケーション チェック（AC 4.1 および ISE 1.4）	アプリケーション チェック（Temporal エージェント 4.5 および ISE 2.3）
アンチウイルスのインストール	マルウェア対策のインストール	アンチウイルスのインストール	マルウェア対策のインストール
アンチウイルス バージョン/アンチウイルス定義日	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます	アンチウイルス バージョン/アンチウイルス定義日	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます
アンチスパイウェアのインストール	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます	アンチスパイウェアのインストール	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます

Windows 用 ISE ポスチャ エージェント	Windows 用 Cisco Temporal エージェント	Macintosh OS X 用 ISE ポスチャ エージェント	Macintosh OS X 用 Cisco Temporal エージェント
アンチスパイウェア バージョン/アンチスパイウェア定義日	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます	アンチスパイウェア バージョン/アンチスパイウェア定義日	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます
パッチ管理チェック（AC 4.1 および ISE 1.4）	パッチ管理のインストールのみチェック	パッチ管理チェック（AC 4.1 および ISE 1.4）	—
実行中の Windows Update	—	—	—
Windows Update の設定	—	—	—
WSUS のコンプライアンス設定	—	—	—

ポスチャ修復オプション

次の表に、Windows および Macintosh の ISE Posture Agent、および Windows の Web Agent でサポートされる修復オプション（ポスチャ条件）のリストを示します。

表 *21* : ポスチャ修復オプション

ISE ポスチャ エージェント Windows	ISE ポスチャ エージェント Macintosh OS X
メッセージ テキスト（ローカル チェック）	メッセージ テキスト（ローカル チェック）
URL リンク（リンク分散）	URL リンク（リンク分散）
ファイル配布	—
プログラム起動	—
アンチウイルス定義更新	アンチウイルス ライブ更新
アンチスパイウェア定義更新	アンチスパイウェア ライブ更新
パッチ管理修復（AC 4.1 および ISE 1.4）	—
Windows Update	—

ISE ポスチャ エージェント Windows	ISE ポスチャ エージェント Macintosh OS X
WSUS	—

ISE Community Resource
Cisco ISE and SCCM integration Reference Guide

ポスチャのカスタム条件

ポスチャ条件は次の単純条件のいずれかになります。ファイル、レジストリ、アプリケーション、サービス、またはディクショナリ条件。これらの単純条件のうちの1つ以上の条件によって複合条件が形成され、複合条件はポスチャ要件と関連付けることができます。

最初のポスチャ更新の後に、Cisco ISE もシスコ定義の単純条件と複合条件を作成します。シスコ定義の単純条件では pc_ as が使用され、複合条件では pr_ as が使用されます。

ユーザ定義の条件またはシスコ定義の条件には、単純条件と複合条件の両方が含まれます。

ポスチャ サービスは、アンチウイルスおよびアンチスパイウェア（AV/AS）複合条件に基づいた内部チェックを使用します。このため、ポスチャ レポートは、作成した正確な AV/AS 複合条件名を反映しません。レポートには、AV/AS 複合条件の内部チェックの名前だけが表示されます。

たとえば、任意のベンダーおよび製品をチェックする「MyCondition_AV_Check」という名前の AV 複合条件を作成した場合、ポスチャ レポートには、条件名として、「MyCondition_AV_Check」ではなく、内部チェック「av_def_ANY」が表示されます。

ポスチャ エンドポイントのカスタム属性

ポスチャ エンドポイントのカスタム属性を使用して、クライアント プロビジョニングおよびポスチャ ポリシーを作成できます。最大100個のエンドポイントのカスタム属性を作成できます。以下のタイプのエンドポイント カスタム属性がサポートされています：Int、String、Long、Boolean、Float、IP、および Date。

エンドポイント カスタム属性は、特定の属性に基づいてデバイスをホワイトリスト登録またはブラックリスト登録するために使用することも、ポスチャまたはクライアント プロビジョニング ポリシーに基づいて特定の権限を割り当てるために使用することもできます。

エンドポイント カスタム属性を使用したポスチャ ポリシーの作成

エンドポイント カスタム属性を使用してポスチャ ポリシーを作成するには、次の手順を実行します。

ステップ 1 エンドポイント カスタム属性を作成します。

a) **[管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] > [エンドポイント カスタム属性（Endpoint Custom Attributes）]** の順に選択します。

b) [エンドポイント カスタム属性（Endpoint Custom Attributes）] 領域に、[属性名（Attribute Name）]（たとえば、deviceType）と [データ型（Data Type）]（たとえば、String）を入力します。

c) [保存（Save）] をクリックします。

ステップ 2 カスタム属性に値を割り当てます。

a) [コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] の順に選択します。

b) カスタム属性値を割り当てます。

- 必要な MAC アドレスのチェックボックスをオンにし、[編集（Edit）] をクリックします。
- または、必要なMACアドレスをクリックし、[エンドポイント（Endpoints）]ページで[編集（Edit）] をクリックします。

c) 作成したカスタム属性が、[エンドポイントの編集（Edit Endpoint）] ダイアログボックスの [カスタム属性（Custom Attributes）] 領域に表示されていることを確認します。

d) [編集（Edit）] をクリックし、必要な属性値を入力します（たとえば、deviceType = Apple-iPhone）。

e) [保存（Save）] をクリックします。

ステップ 3 カスタム属性と値を使用してポスチャ ポリシーを作成します。

a) [ワーク センター（Work Centers）] > [ポスチャ（Posture）] > [ポスチャ ポリシー（Posture Policy）] を選択します。

b) 必要なポリシーを作成します。[その他の条件（Other Conditions）] をクリックしてカスタム属性を選択し、必要なディクショナリを選択します（たとえば、ステップ 1 で作成したカスタム属性である [エンドポイント（Endpoints）] > [deviceType] を選択します）。詳細については、Cisco Temporal Agent のワークフローの設定 （94 ページ） を参照してください。

c) [保存（Save）] をクリックします。

エンドポイント カスタム属性を使用してクライアント プロビジョニング ポリシーを作成するには、次の手順を実行します。

1. [ワーク センター（Work Centers）] > [ポスチャ（Posture）] > [クライアント プロビジョニング（Client Provisioning）] > [クライアント プロビジョニング ポリシー（Client Provisioning Policy）] を選択します。

2. 必要なポリシーを作成します。
   - 必要なルールを作成します（たとえば、Rule Name=WindowsAll, if Identity Groups=Any and Operating Systems=Windows All and Other Conditions=Conditions, then Results=AC_Win_44117）。
   - [その他の条件（Other Conditions）] をクリックして必要なディクショナリを選択して、カスタム属性を選択します。

カスタム ポスチャ修復アクション

カスタムポスチャ修復アクションは、ファイル、リンク、アンチウイルスまたはアンチスパイウェア定義の更新、プログラムの起動、Windows Update、Windows Server Update Services（WSUS）の修復タイプです。

ファイル修復の追加

ファイル修復により、クライアントはコンプライアンスに必要なファイルのバージョンをダウンロードできます。クライアントエージェントは、コンプライアンスのためにクライアントが必要とするファイルを使用してエンドポイントを修復します。

[ファイル修復（File Remediations）] ページでファイル修復をフィルタリング、表示、追加、または削除することはできますが、ファイル修復を編集することはできません。[ファイル修復（File Remediations）] ページには、すべてのファイル修復がそれらの名前と説明、および修復に必要なファイルとともに表示されます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] >** [ポスチャ（Posture）] を選択します。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [ファイル修復（File Remediation）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [名前（Name）] フィールドに名前を入力し、[説明（Description）] フィールドにファイル修復の説明を入力します。

ステップ 6 [新規ファイル修復（New File Remediation）] ページで値を変更します。

ステップ 7 [送信（Submit）] をクリックします。

リンク修復の追加

リンク修復により、クライアントは修復ページまたはリソースにアクセスするための URL をクリックできます。クライアントエージェントはリンクを使用してブラウザを開き、クライアントはコンプライアンスのために自身を修復できます。

[リンク修復（Link Remediation）]ページには、すべてのリンク修復がそれらの名前と説明、および修復のモードとともに表示されます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > [ポスチャ（Posture）] を選択します。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [リンク修復（Link Remediation）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [新規リンク修復（New Link Remediation）] ページで値を変更します。

ステップ 6 [送信（Submit）] をクリックします。

パッチ管理修復の追加

パッチ管理修復を作成して、修復後にコンプライアンスのために最新のファイル定義でクライアントを更新できます。

[パッチ管理修復（Patch Management Remediation）]ページには、修復タイプ、パッチ管理ベンダーの名前、およびさまざまな修復オプションが表示されます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > [ポスチャ（Posture）] を選択します。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [パッチ管理修復（Patch Management Remediation）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [パッチ管理修復（Patch Management Remediation）] ページで値を変更します。

ステップ 6 [送信（Submit）] をクリックして、[パッチ管理修復（Patch Management Remediation）] ページに修復アクションを追加します。

関連トピック

パッチ管理修復

アンチウイルス修復の追加

アンチウイルス修復を作成して、修復後にコンプライアンスのために最新のファイル定義でクライアントを更新できます。

[AV 修復（AV Remediations）] ページには、すべてのアンチウイルス修復がそれらの名前と説明、および修復のモードとともに表示されます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > [ポスチャ（Posture）] を選択します。
ステップ 2 [修復アクション（Remediation Actions）] をクリックします。
ステップ 3 [AV 修復（AV Remediation）] をクリックします。
ステップ 4 [追加（Add）] をクリックします。
ステップ 5 [新規 AV 修復（New AV Remediation）] ページで値を変更します。
ステップ 6 [送信（Submit）] をクリックします。

アンチスパイウェア修復の追加

アンチスパイウェア修復を作成して、修復後にコンプライアンスのために最新のファイル定義でクライアントを更新できます。

[AS 修復（AS Remediations）] ページには、すべてのアンチウイルス修復がそれらの名前と説明、および修復のモードとともに表示されます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > [ポスチャ（Posture）] を選択します。
ステップ 2 [修復アクション（Remediation Actions）] をクリックします。
ステップ 3 [AS 修復（AS Remediations）] をクリックします。
ステップ 4 [追加（Add）] をクリックします。
ステップ 5 [新規 AS 修復（New AS Remediations）] ページで値を変更します。
ステップ 6 [送信（Submit）] をクリックします。

関連トピック

アンチスパイウェア修復

プログラム修復起動の追加

コンプライアンスのために、クライアントエージェントが 1 つ以上のアプリケーションを起動してクライアントを修復するプログラム修復起動を作成できます。

[プログラム修復起動（Launch Program Remediations）] ページには、すべてのプログラム修復起動がそれらの名前と説明、および修復のモードとともに表示されます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > [ポスチャ（Posture）] を選択します。
ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [プログラム起動修復（Launch Program Remediation）] をクリックします。
ステップ 4 [追加（Add）] をクリックします。
ステップ 5 [新規プログラム修復起動（New Launch Program Remediation）] ページで値を変更します。
ステップ 6 [送信（Submit）] をクリックします。

プログラム修復起動のトラブルシューティング

問題

プログラム修復起動を使用して、アプリケーションを修復として起動すると、アプリケーションは正常に開始されます（Windows Task Manager で観察されます）が、アプリケーション UI は表示されません。

ソリューション

プログラム起動 UI アプリケーションはシステム権限で実行され、[インタラクティブサービス検出（ISD）（Interactive Service Detection (ISD)）] ウィンドウに表示されます。プログラム起動 UI アプリケーションを表示するには、次の OS で ISD をイネーブルにする必要があります。

- Windows Vista：ISD はデフォルトで停止状態になっています。services.msc で ISD サービスを起動して、ISD をイネーブルにします。
- Windows 7：ISD サービスはデフォルトでイネーブルになっています。
- Windows 8/8.1：レジストリ \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows で「NoInteractiveServices」を 1 から 0 に変更することで ISD をイネーブルにします。

Windows Update 修復の追加

[Windows Update 修復（Windows update remediations）] ページには、すべての Windows Update 修復がそれらの名前と説明、および修復のモードとともに表示されます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > > **[ポスチャ（Posture）]** を選択します。
ステップ 2 [修復アクション（Remediation Actions）] をクリックします。
ステップ 3 [Windows Update 修復（Windows Update Remediation）] をクリックします。
ステップ 4 [追加（Add）] をクリックします。
ステップ 5 [新規 Windows Update 修復（New Windows Update Remediation）] ページで値を変更します。
ステップ 6 [送信（Submit）] をクリックします。

Windows Server Update Services 修復の追加

コンプライアンスのためにローカルに管理されているか、または Microsoft で管理されている WSUS サーバから最新の WSUS 更新を受信するように Windows クライアントを設定できます。Windows Server Update Services（WSUS）修復は、ローカルに管理されている WSUS サーバまたは Microsoft で管理されている WSUS サーバから最新の Windows サービス パック、ホットフィックス、およびパッチをインストールします。

クライアント エージェントをローカルの WSUS Agent と統合して、エンドポイントの WSUS 更新が最新かどうかをチェックする WSUS 修復を作成できます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > [ポスチャ（Posture）] を選択します。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [Windows Server Update Service 修復（Windows Server Update Services Remediation）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [新規 Windows Server Update Service 修復（New Windows Server Update Services Remediation）] ページで値を変更します。

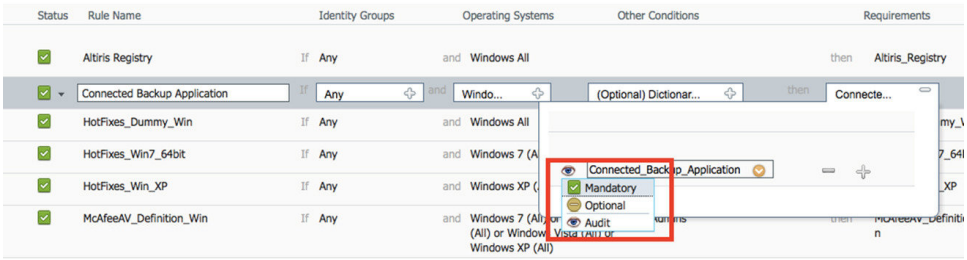
ステップ 6 [送信（Submit）] をクリックします。

ポスチャ評価要件

ポスチャ要件は、ロールおよびオペレーティング システムとリンクできる修復アクションを伴う一連の複合条件です。ネットワークに接続しているすべてのクライアントは、ネットワークで適合ホストになるためにはポスチャ評価中に必須要件を満たす必要があります。

ポスチャ ポリシー要件は、ポスチャ ポリシーの必須、オプション、または監査タイプに設定できます。要件がオプションで、クライアントがこれらの要件を満たさない場合、クライアントにはエンドポイントのポスチャ評価中に続行するオプションがあります。

図 *4*：ポスチャ ポリシーの要件タイプ



必須要件

ポリシーの評価時に、エージェントはポスチャ ポリシーに定義されている必須要件を満たすことができないクライアントに修復オプションを提供します。エンドユーザは、修復タイマー設定で指定された時間内に要件を満たすように修復する必要があります。

たとえば、絶対パス内にC:\temp\text.fileがあるかをチェックするために、ユーザ定義の条件を含む必須要件を指定したとします。ファイルがない場合、必須要件は失敗し、ユーザは [非準拠（Non-Compliant）] 状態になります。

オプション要件

ポリシーの評価時に、クライアントがポスチャ ポリシーに指定されたオプション要件を満たすことができない場合に、エージェントは続行するためのオプションをクライアントに提供します。エンドユーザは、指定されたオプション要件をスキップすることができます。

たとえば、Calc.exeなどのクライアントマシンで実行するアプリケーションをチェックするために、ユーザ定義の条件を含むオプション要件を指定したとします。クライアントが条件を満たすことができない場合、オプション要件がスキップされ、エンドユーザが[準拠（Compliant）] 状態になるように、さらに続行するためのオプションがエージェントによって促されます。

監査要件

監査要件は内部用に指定され、エージェントはポリシー評価時の合格または失敗のステータスに関係なく、メッセージやエンドユーザからの入力を促しません。

たとえば、エンドユーザにアンチウイルス プログラムの最新バージョンがあるかどうかを確認するために、必須のポリシー条件を作成中だとします。ポリシー条件として実際に適用する前に非準拠のエンドユーザを見つける場合は、その条件を監査要件として指定できます。

可視性要件

ポリシー評価の間に、エージェントが可視性要件のコンプライアンス データを 5 ～ 10 分ごとにレポートします。

非準拠ステートでスタックしたクライアント システム

クライアント マシンが必須要件を修復できない場合、ポスチャ ステータスは「非準拠」に変更され、エージェント セッションは隔離されます。クライアント マシンを「非準拠」状態から移行するには、エージェントがクライアントマシン上でポスチャ評価を再び開始するようにポスチャ セッションを再起動する必要があります。次のようにポスチャ セッションを再起動できます。

- 802.1X 環境での有線およびワイヤレス許可変更（CoA）：
  - [新しい許可プロファイル（New Authorization Profiles）] ページで新しい許可プロファイルを作成するときに、特定の許可ポリシーの再認証タイマーを設定できます。詳細については、20-11 ページの「ダウンロード可能 ACL の権限の設定」の項を参照してください。

- 有線ユーザは、ネットワークの接続を切断して再接続すると、隔離状態から移行できます。ワイヤレス環境では、ユーザは、ワイヤレス LAN コントローラ（WLC）から切断し、ユーザのアイドルタイムアウト時間が過ぎるまで待機してから、ネットワークへの再接続を試行する必要があります。

- VPN 環境：VPN トンネルを切断し、再接続します。

クライアントのポスチャ要件の作成

[要件（Requirements）] ページでは、ユーザ定義の条件とシスコ定義の条件、および修復アクションを関連付けて要件を作成できます。[要件（Requirements）] ページで作成および保存されたユーザ定義の条件および修復アクションは、それぞれのリスト ページに表示されます。

始める前に

- ポスチャの利用規定（AUP）について理解している必要があります。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [要件（Requirements）]** を選択します。

ステップ 2 [要件（Requirements）] ページに値を入力します。

ステップ 3 読み取り専用モードでポスチャ要件を保存するには、[完了（Done）] をクリックします。

ステップ 4 [保存（Save）] をクリックします。

ポスチャ再評価の構成設定

次の表では、ポスチャ再評価の設定に使用できる [ポスチャ再評価設定（Posture Reassessment Configurations）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [再評価（Reassessments）]** です。

表 *22* : ポスチャ再評価の構成設定

フィールド	使用上のガイドライン
構成名	PRA 設定の名前を入力します。
設定の説明（Configuration Description）	PRA 設定の説明を入力します。
再評価適用を使用?（Use Reassessment Enforcement?）	ユーザ ID グループの PRA 設定を適用するには、チェックボックスをオンにします。

フィールド	使用上のガイドライン
適用タイプ（Enforcement Type）	適用する次のアクションを選択します。 • [続行（Continue）]：ユーザはポスチャ要件に関係なくクライアントを修復できるようにユーザ介入なしの特権アクセスが引き続き提供されます。 • [ログオフ（Logoff）]：クライアントが非準拠の場合、ユーザを強制的にネットワークからログオフします。 クライアントが再度ログインしたときのコンプライアンス ステータスは不明です。 • [修復（Remediate）]：クライアントが非準拠の場合、エージェントは修復のために指定の期間待機します。 クライアントが修復された後、エージェントはポリシーサービス ノードにPRA レポートを送信します。修復がクライアントで無視された場合、エージェントはクライアントにネットワークからログオフすることを強制するために、ポリシーサービス ノードにログオフ要求を送信します。 ポスチャ要件が [必須（mandatory）] に設定されている場合、RADIUS セッションはPRA 障害アクションの結果としてクリアされ、クライアントを再びポスチャするには新しい RADIUS セッションを開始する必要があります。 ポスチャ要件が [任意（Optional）] に設定されている場合、クライアント上のエージェントではユーザがエージェントから [続行（Continue）] オプションをクリックできます。ユーザは、制限なしで現在のネットワークにとどまることができます。
インターバル（Interval	最初のログイン成功後にクライアントで PRA を開始する間隔を分単位で入力します。 デフォルト値は 240 分です。最小値は 60 分、最大値は 1440 分です。

フィールド	使用上のガイドライン
猶予時間（Grace time）	クライアントが修復を完了することのできる時間間隔を分単位で入力します。猶予時間をゼロにすることはできません。また、PRA 間隔より大きくする必要があります。デフォルトの最小間隔（5 分）から最小 PRA 間隔までの範囲にすることができます。 最小値は 5 分、最大値は 60 分です。 （注） 猶予時間は、クライアントがポスチャの再評価に失敗した後、適用タイプが修復アクションに設定されている場合にだけ有効です。
ユーザ ID グループの選択（Select User Identity Groups）	PRA設定に対して一意のグループまたはグループの一意の組み合わせを選択します。
PRA の設定（PRA configurations）	既存の PRA 設定と PRA 設定に関連付けられたユーザ ID グループを表示します。

関連トピック

ポスチャのリース （14 ページ）
定期的再評価 （15 ページ）
ポスチャ評価オプション
ポスチャ修復オプション （76 ページ）
ポスチャのカスタム条件 （77 ページ）
カスタム ポスチャ修復アクション （79 ページ）
定期的再評価の設定 （16 ページ）

ポスチャのカスタム権限

カスタム権限は、Cisco ISE で定義する標準許可プロファイルです。標準許可プロファイルは、エンドポイントの一致するコンプライアンス ステータスに基づいてアクセス権を設定します。ポスチャ サービスでは、ポスチャは大きく不明プロファイル、準拠プロファイル、および非準拠プロファイルに分類されます。ポスチャ ポリシーおよびポスチャ要件によって、エンドポイントのコンプライアンス ステータスが決まります。

VLAN、DACL および他の属性値ペアの異なるセットを持つことができるエンドポイントの不明、準拠、および非準拠のポスチャ ステータスに対して 3 つの異なる許可プロファイルを作成する必要があります。これらのプロファイルは、3 つの異なる許可ポリシーに関連付けることができます。これらの許可ポリシーを区別するために、Session:PostureStatus 属性を他の条件とともに使用できます。

不明プロファイル

エンドポイントに一致するポスチャ ポリシーが定義されていない場合、そのエンドポイントのポスチャ コンプライアンス ステータスは不明に設定されることがあります。不明のポスチャ コンプライアンス ステータスは、一致するポスチャ ポリシーが有効であるが、エンドポイントに対してポスチャ評価がまだ行われておらず、従ってクライアント エージェントによってコンプライアンス レポートが提供されていないエンドポイントにも適用できます。

準拠プロファイル

エンドポイントに一致するポスチャ ポリシーが定義されている場合、そのエンドポイントのポスチャ コンプライアンス ステータスは準拠に設定されます。ポスチャ評価が行われると、エンドポイントは、一致するポスチャ ポリシー内に定義されているすべての必須要件を満たします。準拠とポスチャされているエンドポイントには、ネットワークに対する特権ネットワーク アクセスを付与できます。

非準拠プロファイル

エンドポイントのポスチャ コンプライアンス ステータスが非準拠に設定されるのは、そのエンドポイントに対して一致するポスチャ ポリシーが定義されているが、ポスチャ評価の実行中にすべての必須要件を満たすことができない場合です。非準拠としてポスチャされたエンドポイントは、修復アクションを含むポスチャ要件に一致し、自らを修復するために修復リソースへ制限付きのネットワーク アクセスが付与される必要があります。

標準許可ポリシーの設定

[許可ポリシー（Authorization Policy）] ページでは、標準許可ポリシーと例外許可ポリシーの 2 種類の許可ポリシーを定義できます。ポスチャに固有の標準許可ポリシーは、エンドポイントのコンプライアンス ステータスに基づいて、ポリシー決定を行うために使用されます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー セット（Policy Sets）]** を選択します。

ステップ 2 [ビュー（View）] 列で、対応するデフォルトポリシーに隣接する矢印アイコンをクリックします。

ステップ 3 [アクション（Actions）] 列で、歯車アイコンをクリックし、ドロップダウン リストから新しい認証ポリシーを選択します
[ポリシーセット（Policy Sets）] テーブルに新しい行が表示されます。

ステップ 4 着信サービス名を入力します。

ステップ 5 [条件（Conditions）] 列から、（+）記号をクリックします。

ステップ 6 [条件スタジオ（Conditions Studio）] ページで必要な条件を作成します。[エディタ（Editor）] セクションで、[クリックして属性を追加する（Click To Add an Attribute）] テキスト ボックスをクリックし、必要なディクショナリと属性を選択します。

ライブラリ条件を [クリックして属性を追加する（Click To Add An Attribute）] テキスト ボックスにドラッグ アンド ドロップできます。

ステップ 7 [使用（Use）] をクリックして、読み取り専用モードで新しい標準許可ポリシーを作成します。
ステップ 8 [保存（Save）] をクリックします。

ポスチャとネットワーク ドライブ マッピングのベスト プラクティス

Windows エンドポイントのポスチャ アセスメント実行中に、エンドポイント ユーザがデスクトップへのアクセスするときに遅延が生じることがあります。これは、Windows でユーザがデスクトップにアクセスできるようにする前に、ファイル サーバのドライブ文字のマッピングを復元しようとすることが原因で発生する場合があります。ポスチャ実行中の遅延を防ぐためのベスト プラクティスを次に示します。

- ファイル サーバ ドライブ文字をマッピングするときには AD にアクセスする必要があるため、エンドポイントは Active Directory サーバにアクセスできる必要があります。（AnyConnect ISE ポスチャ エージェントを使用した）ポスチャがトリガーされると、AD へのアクセスがブロックされ、これが原因でログインが遅延します。ポスチャが完了する前に、ポスチャ修復 ACL を使用して AD サーバへのアクセスを提供します。
- ポスチャ完了までのログイン スクリプトの遅延を設定し、その後 Persistence 属性を NO に設定する必要があります。Windows はログイン中にすべてのネットワーク ドライブへの再接続を試行しますが、AnyConnect ISE ポスチャ エージェントが完全なネットワーク アクセスを得るまでは、この操作を完了できません。

AnyConnect ステルス モードのワークフローの設定

ステルス モードでの AnyConnect の設定プロセスには、一連の手順があります。Cisco ISE で次の手順を実行する必要があります。

ステップ 1 AnyConnect エージェント プロファイルを作成します。「AnyConnect エージェント プロファイルの作成」を参照してください。
ステップ 2 AnyConnect パッケージの AnyConnect 設定を作成します。「AnyConnect パッケージの AnyConnect 設定の作成」を参照してください。
ステップ 3 Cisco ISE でオープン DNS プロファイルをアップロードします。「Cisco ISE へのオープン DNS プロファイルのアップロード」を参照してください。
ステップ 4 クライアント プロビジョニング ポリシーを作成します。「クライアント プロビジョニング ポリシーの作成」を参照してください。
ステップ 5 ポスチャ条件を作成します。「ポスチャ条件の作成」を参照してください。
ステップ 6 ポスチャ修復を作成します。「ポスチャ修復の作成」を参照してください。

ステップ 7 クライアントレスモードでポスチャ要件を作成します。「ステルス モードでのポスチャ要件の作成」を参照してください。

ステップ 8 ポスチャ ポリシーを作成します。「ポスチャ ポリシーの作成」を参照してください。

ステップ 9 認証プロファイルを設定します。

a) **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可（Authorization）]** > **[許可プロファイル（Authorization Profiles）]** を選択します。

b) [追加（Add）] をクリックして、プロファイルの [名前（Name）] に入力します。

c) [共通タスク（Common Tasks）] で、[Web リダイレクション（CWA、MDM、NSP、CPP）（Web Redirection (CWA, MDM, NSP, CPP)）] を有効にし、ドロップダウンリストから [クライアント プロビジョニング（ポスチャ）（Client provisioning (Posture)）] を選択し、リダイレクト [ACL] の名前を入力して、[クライアント プロビジョニング ポータル（Client Provisioning Portal）] 値を選択します。新しいクライアント プロビジョニング ポータルは、**[ワークセンター（Work Centers）]** > **[ポスチャ（Posture）]** > **[クライアント プロビジョニング（Client Provisioning）]** > **[クライアント プロビジョニング ポータル（Client Provisioning Portal）]** で編集または作成できます。

ステップ 10 許可ポリシーを設定します。

a) **[ポリシー（Policy）]** > **[ポリシーセット（Policy Sets）]** を選択します。

b) [>] をクリックして [認可ポリシー（Authorization Policy）] を選択し、[+] アイコンをクリックして **Session:Posture Status EQUALS Unknown** と以前に設定した認証プロファイルが備わっている新しいルールを作成します。

c) 以前のルールの上に、**Session:Posture Status EQUALS NonCompliant** 条件を備えた新しい認証ルールと、**Session:Posture Status EQUALS Compliant** 条件を備えた別の新しい認証ルールを作成します。

AnyConnect エージェント プロファイルの作成

始める前に

Mac および Windows OS 用の AnyConnect Cisco パッケージおよび AnyConnect 準拠モジュールをアップロードする必要があります。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[クライアントプロビジョニング（Client Provisioning）]** > **[リソース（Resources）]** ページを選択します。

ステップ 2 [追加（Add）] ドロップダウンリストから、**[AnyConnect ポスチャプロファイル（AnyConnect Posture Profile）]**を選択します。

ステップ 3 [ポスチャ エージェント プロファイルの設定（Posture Agent Profile Settings）] ドロップダウンリストから [AnyConnect] を選択します。

ステップ 4 [名前（Name）] フィールドに、目的の名前（たとえば、AC_Agent_Profile）を入力します。

ステップ 5 [エージェントの動作（Agent Behavior）] セクションでは、[ステルス モード（Stealth Mode）] パラメータで[クライアントレス（Clientless）][有効（Enabled）] を選択します。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

AnyConnect パッケージの AnyConnect 設定を作成する必要があります。

AnyConnect パッケージの AnyConnect 設定の作成

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** ページに移動します。

ステップ 2 [追加（Add）] ドロップダウン リストから、[AnyConnect 設定（AnyConnect Configuration）] を選択します。

ステップ 3 [AnyConnect パッケージの選択（Select AnyConnect Package）] ドロップダウン リストから、必要な AnyConnect パッケージを選択します（AnyConnectDesktopWindows 4.4.117.0 など）。

ステップ 4 [設定名（Configuration Name）] テキスト ボックスに、必要な名前を入力します（AC_Win_44117 など）。

ステップ 5 [コンプライアンス モジュール（Compliance Module）] ドロップダウン リストで、必要なコンプライアンス モジュールを選択します（AnyConnectComplianceModuleWindows 4.2.437.0 など）。

ステップ 6 [AnyConnect モジュール選択（AnyConnect Module Selection）] セクションで、[ISE ポスチャ（ISE Posture）] と [ネットワーク アクセス マネージャ（Network Access Manager）] のチェック ボックスにマークを付けます。

ステップ 7 [プロファイル選択（Profile Selection）] セクションの [ISE ポスチャ（ISE Posture）] ドロップダウン リストで、AnyConnect エージェント プロファイルを選択します（AC_Agent_Profile など）。

ステップ 8 [ネットワーク アクセス マネージャ（Network Access Manager）] ドロップダウン リストから、必要な AnyConnect エージェント プロファイルを選択します（AC_Agent_Profile など）。

次のタスク

クライアントにプッシュされるオープン DNS プロファイルをアップロードする必要があります。

Cisco ISE へのオープン DNS プロファイルのアップロード

オープン DNS プロファイルがクライアントにプッシュされます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** ページに移動します。

ステップ 2 [追加（Add）] ドロップダウン リストから、[ローカル ディスクのエージェント リソース（Agent Resources From Local Disk）] を選択します。

ステップ 3 [カテゴリ（Category）] ドロップダウン リストから [顧客作成のパッケージ（Customer Created Packages）] を選択します。

ステップ 4 [タイプ（Type）] ドロップダウン リストから、[AnyConnect プロファイル（AnyConnect Profile）] を選択します。

ステップ 5 [名前（Name）] テキスト ボックスに、目的の名前（たとえば、OpenDNS）を入力します。

ステップ 6 [参照（Browse）] をクリックして、ローカル ディスクから JSON ファイルを見つけます。

ステップ 7 [送信（Submit）] をクリックします。

次のタスク

クライアント プロビジョニング ポリシーを作成する必要があります。

クライアント プロビジョニング ポリシーの作成

ステップ 1 **[ポリシー（Policy）]** > **[クライアント プロビジョニング（Client Provisioning）]** ページに移動します。

ステップ 2 必要なルールを作成します（たとえば、Rule Name=WindowsAll, if Identity Groups=Any and Operating Systems=Windows All and Other Conditions=Conditions, then Results=AC_Win_44117）。

次のタスク

ポスチャ条件を作成する必要があります。

ポスチャ条件の作成

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** > **[ファイル条件（File Condition）]** の順に移動します。

ステップ 2 必要な名前を入力します（filechk など）。

ステップ 3 [オペレーティング システム（Operating Systems）] ドロップダウン リストから、[Windows 7（すべて）（Windows 7 (All)）] を選択します。

ステップ 4 [ファイル タイプ（File Type）] ドロップダウン リストから、[FileExistence] を選択します。

ステップ 5 [ファイル パス（File Path）] ドロップダウン リストから、[ABSOLUTE_PATH C:\test.txt] を選択します。

ステップ 6 [ファイル演算子（File Operator）] ドロップダウン リストから、[DoesNotExist] を選択します。

次のタスク

ポスチャ修復を作成する必要があります。

ポスチャ修復の作成

ファイル条件により、test.txtファイルがエンドポイントに存在するかどうかが確認されます。存在しない場合の修復は、USB ポートをブロックし、USB デバイスを使用したファイルのインストールを防止することです。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [修復アクション（Remediation Actions）] > [USB 修復（USB Remediations）]** ページに移動します。

ステップ 2 必要な名前を入力します（clientless_mode_block など）。

ステップ 3 [送信（Submit）] をクリックします。

次のタスク

ポスチャ要件を作成する必要があります。

ステルス モードでのポスチャ要件の作成

[要件（Requirements）] ページから修復アクションを作成する際は、ステルス モードに適した次の修復だけが表示されます：[マルウェア対策（Anti-Malware）]、[プログラム起動（Launch Program）]、[パッチ管理（Patch Management）]、[USB]、[Windows Server Update Services]、および [Windows Update]。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** ページに移動します。

ステップ 2 ポスチャの必須要件を作成します（たとえば、Name=win7Req for Operating Systems=Windows7(All) using Compliance Module=4.x or later using Posture Type=AnyConnect Stealth met if Condition=filechk then Remediation Actions=clientless_mode_block）。

次のタスク

ポスチャ ポリシーを作成する必要があります。

ポスチャ ポリシーの作成

始める前に

ポスチャ ポリシーの要件およびポリシーがクライアントレス モードで作成されていることを確認してください。

ステップ 1 **[ポリシー（Policy）] > [ポスチャ（Posture）]** を選択します。

ステップ 2 必要なルールを作成します。たとえば、Identity Groups=Any and Operating Systems=Windows 7(All) および Compliance Module=4.x or late および Posture Type=AnyConnect Stealth の場合、Requirements=win7Req となります。

（注） URL リダイレクションのないクライアント プロビジョニングの場合、ネットワーク アクセスまたはRADIUS に固有の属性を使用して条件を設定しても条件は機能せず、Cisco ISE サーバで特定ユーザのセッション情報が使用可能ではないことが原因で、クライアント プロビジョニング ポリシーの照合が失敗することがあります。ただし、Cisco ISE では外部で追加された ID グループに対して条件を設定できます。

AnyConnect ステルス モード通知の有効化

Cisco ISE では AnyConnect ステルス モード展開に対し、いくつかの新しい障害の発生通知を提供します。ステルス モードでの障害の発生通知を有効にすると、有線、ワイヤレスまたはVPN 接続で問題を特定できます。ステルス モードでの通知を有効にするには、次のようにします。

（注） AnyConnect バージョン 4.5.0.3040 以降は、ステルスモードでの通知をサポートします。

始める前に

ステルス モードで AnyConnect を設定します。

ステップ 1 [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）] を選択します。

ステップ 2 [追加（Add）] > **[AnyConnect ISEポスチャプロファイル（AnyConnect ISE Posture Profile）]** を選択します。

ステップ 3 [カテゴリの選択（Select a Category）] ドロップダウン リストから [AnyConnect] を選択します。

ステップ 4 [エージェントの動作（Agent Behavior）] セクションで、[ステルスモードで通知を有効にする（Enable notifications in stealth mode）] オプションに [有効（Enabled）] を選択します。

Cisco Temporal Agent のワークフローの設定

Cisco temporal agent を設定するプロセスには、一連の手順があります。Cisco ISE で次の手順を実行する必要があります。

ステップ 1 ポスチャ条件の作成

ステップ 2 ポスチャ要件の作成

ステップ 3 ポスチャ ポリシーの作成

ステップ 4 クライアント プロビジョニング ポリシーの設定

ステップ 5 認証プロファイルを設定します。

a) **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可（Authorization）]** > **[許可プロファイル（Authorization Profiles）]** を選択します。

b) [追加（Add）] をクリックして、プロファイルの [名前（Name）] に入力します。

c) [共通タスク（Common Tasks）] で、[Web リダイレクション（CWA、MDM、NSP、CPP）（Web Redirection (CWA, MDM, NSP, CPP)）] を有効にし、ドロップダウンリストから [クライアント プロビジョニング（ポスチャ）（Client provisioning (Posture)）] を選択し、リダイレクト [ACL] の名前を入力して、[クライアントプロビジョニング ポータル（Client Provisioning Portal）] 値を選択します。新しいクライアント プロビジョニング ポータルは、**[ワークセンター（Work Centers）]** > **[ポスチャ（Posture）]** > **[クライアント プロビジョニング（Client Provisioning）]** > **[クライアント プロビジョニング ポータル（Client Provisioning Portal）]** で編集または作成できます。

ステップ 6 許可ポリシーを設定します。

a) **[ポリシー（Policy）]** > **[ポリシーセット（Policy Sets）]** を選択します。

b) [>] をクリックして [認可ポリシー（Authorization Policy）] を選択し、[+] アイコンをクリックして **Session:Posture Status EQUALS Unknown** と以前に設定した認証プロファイルが備わっている新しいルールを作成します。

c) 以前のルールの上に、**Session:Posture Status EQUALS NonCompliant** 条件を備えた新しい認証ルールと、**Session:Posture Status EQUALS Compliant** 条件を備えた別の新しい認証ルールを作成します。

ステップ 7 Cisco Temporal Agent のダウンロードと起動

ポスチャ条件の作成

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** > **[ファイル条件（File Condition）]** の順に移動します。

ステップ 2 必要な名前を入力します（filecondwin など）。

ステップ 3 [オペレーティング システム（Operating Systems）] ドロップダウン リストから、[Windows 7（すべて）（Windows 7 (All)）] を選択します。

ステップ 4 [ファイル タイプ（File Type）] ドロップダウン リストから、[FileExistence] を選択します。

ステップ 5 [ファイル パス（File Path）] ドロップダウン リストから、[ABSOLUTE_PATH C:\test.txt] を選択します。

ステップ 6 [ファイル演算子（File Operator）] ドロップダウン リストから、[DoesNotExist] を選択します。

ポスチャ要件の作成

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [要件（Requirements）]** を選択します。

ステップ 2 [編集（Edit）] ドロップダウンリストから、[新しい要件の挿入（Insert New Requirement）] を選択します。

ステップ 3 [名前（Name）]、[オペレーティング システム（Operating Systems）]、および [コンプライアンス モジュール（Compliance Module）] を入力します（たとえば、Name filereqwin、Operating Systems Windows All、Compliance Module 4.x or later）。

ステップ 4 [ポスチャ タイプ（Posture Type）] ドロップダウンで、[Temporal Agent] を選択します。

ステップ 5 必要な条件（たとえば、filecondwin）を選択します。

（注） Cisco Temporal Agent の場合は、[要件（Requirements）] ページで [インストール（Installation）] チェック タイプを含むパッチ管理条件のみを表示できます。

ステップ 6 [メッセージ テキストのみ（Message Text Only）] 修復アクションを選択します。

（注） 一時エージェントは、AnyConnect 4.x 以降でサポートされています。

ポスチャ ポリシーの作成

ステップ 1 **[ポリシー（Policy）] > [ポスチャ（Posture）]** を選択します。

ステップ 2 必要なルールを作成します（たとえば、Name=filepolicywin、Identity Groups=Any、Operating Systems=Windows All、Compliance Module=4.x or later、Posture Type=Temporal Agent、および Requirements=filereqwin）。

クライアント プロビジョニング ポリシーの設定

ステップ 1 **[ポリシー（Policy）] > [クライアント プロビジョニング（Client Provisioning）]** を選択します。

ステップ 2 必要なルールを作成します（たとえば、Rule Name=Win、Identity Groups=Any、Operating Systems=Windows All、Other Conditions=Conditions、Results=CiscoTemporalAgentWindows4.5）。

Cisco Temporal Agent のダウンロードと起動

ステップ 1 SSID に接続します。

ステップ 2 ブラウザを起動すると、クライアント プロビジョニング ポータルにリダイレクトされます。

ステップ 3 [開始（Start）] をクリックします。これにより、Cisco Temporal Agent がインストールされ、動作しているかどうかがチェックされます。

ステップ 4 [ここに初めて来ました（This Is My First Time Here）] をクリックします。

ステップ 5 [Cisco Temporal Agent をダウンロードして起動するにはここをクリック（Click Here to Download and Launch Cisco Temporal Agent）] を選択します。

ステップ 6 Windows または Mac OSX 用の Cisco Temporal Agent .exe または .dmg ファイルをそれぞれ保存します。Windows の場合は .exe ファイルを実行し、Mac OSX の場合は .dmg ファイルをダブルクリックして、acisetempagent アプリケーションを実行します。
Cisco Temporal Agent はクライアントをスキャンし、結果（非準拠を示す赤い十字マークなど）を表示します。

ポスチャのトラブルシューティング ツール

[ポスチャのトラブルシューティング（Posture Troubleshooting）] ツールは、ポスチャ チェック エラーの原因を見つけ、次のことを識別するのに役立ちます。

- どのエンドポイントがポスチャに成功し、どのエンドポイントが成功しなかったか。
- エンドポイントがポスチャに失敗した場合、ポスチャ プロセスのどの手順が失敗したか。
- どの必須および任意のチェックが成功および失敗したか。

ユーザ名、MAC アドレス、ポスチャ ステータスなどのパラメータに基づいて要求をフィルタリングすることによって、この情報を特定します。

Cisco ISE でのクライアント プロビジョニングの設定

クライアントプロビジョニングを有効にして、ユーザがクライアントプロビジョニング リソースをダウンロードし、エージェント プロファイルを設定できるようにします。Windows クライアント、Mac OS X クライアント、およびパーソナル デバイスのネイティブ サプリカント プロファイルのエージェント プロファイルを設定できます。クライアント プロビジョニングを無効にすると、ネットワークにアクセスしようとするユーザには、クライアントプロビジョニング リソースをダウンロードできないことを示す警告メッセージが表示されます。

始める前に

プロキシを使用していて、クライアント プロビジョニング リソースをリモート システムでホスティングしている場合は、プロキシがクライアントにそのリモート ロケーションへのアクセスを許可していることを確認します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [クライアント プロビジョニング（Client Provisioning）]** または **[ワーク センター（Work Centers）] > [ポスチャ（Posture）] > [設定**

（**Settings**）]>[ソフトウェア アップデート（**oftware Updates**）]>[クライアント プロビジョニング（**Client Provisioning**）] の順に選択します。

ステップ 2 [プロビジョニングの有効化（Provision Enable）] ドロップダウン リストから、**Enable** または **Disable** を選択します。

ステップ 3 **Enable Automatic Download** ドロップダウン リストから、**Enable** を選択します。

フィードのダウンロードには、すべての使用可能なクライアント プロビジョニング リソースが含まれています。これらのリソースの一部は、展開に関連していない場合があります。シスコでは、このオプションを設定する代わりに可能な限りリソースを手動でダウンロードすることを推奨します。

ステップ 4 [フィード URL の更新（Update Feed URL）] : [フィード URL の更新（Update Feed URL）] テキスト ボックスに、Cisco ISE で検索するシステム アップデートの URL を指定します。たとえば、クライアント プロビジョニング リソースをダウンロードするためのデフォルト URL は https://www.cisco.com/web/secure/spa/provisioning-update.xml. です。

ステップ 5 [ネイティブ サプリカント プロビジョニング ポリシーを使用できない（Native Supplicant Provisioning Policy Unavailable）] : デバイスに対するクライアント プロビジョニング リソースがない場合は、ここでフローの進め方を決定します。

- **Allow Network Access**：ユーザは、ネイティブ サプリカント ウィザードをインストールおよび起動せずに、デバイスをネットワークに登録することを許可されます。
- **Apply Defined Authorization Policy**：ユーザは、標準認証および（ネイティブ サプリカント プロビジョニング プロセスではない）許可ポリシーを適用して Cisco ISE ネットワークへのアクセスを試みる必要があります。このオプションを有効にすると、ユーザ デバイスに対して、ユーザの ID に適用されたすべてのクライアント プロビジョニング ポリシーに従った標準登録が行われます。Cisco ISE ネットワークにアクセスするためにユーザのデバイスが証明書を必要とする場合は、第 15 章の「End_User Web ポータルのセットアップとカスタマイズ」の「カスタム言語テンプレートの追加」の項の説明に従って、カスタマイズ可能なユーザ提示テキスト フィールドを使用して有効な証明書を取得して適用する方法もユーザに詳細に指示する必要があります。

ステップ 6 **Save** をクリックします。

次のタスク

クライアント プロビジョニング リソース ポリシーを設定します。

クライアント プロビジョニン リソース

クライアント プロビジョニング リソースは、エンドポイントがネットワークに接続した後にエンドポイントにダウンロードされます。クライアント プロビジョニング リソースは、デスクトップの場合はコンプライアンスとポスチャ エージェントで構成され、電話およびタブレットの場合はネイティブ サプリカント プロファイルで構成されます。クライアント プロビジョニング ポリシーによって、これらのプロビジョニング リソースがエンドポイントに割り当てられ、ネットワーク セッションが開始します。

クライアント プロビジョニング リソースは、**[ポリシー要素（Policy Elements）]** > **[結果（Results）]**>**[クライアントプロビジョニング（Client Provisioning）]**>**[リソース（Resources）]** にリストされます。次のリソース タイプは、[追加（Add）] ボタンをクリックすることでリストに追加できます。

- [Ciscoサイトのエージェントリソース（Agent resources from Cisco Site）]：クライアント プロビジョニング ポリシーで使用できるようにする [NAC]、[AnyConnect] および [サプリカントプロビジョニング（Supplicant Provisioning）] ウィザードを選択します。シスコは、新しいリソースを追加したり既存のリソースを更新することで、定期的にこのリソースのリストを更新します。すべてのシスコのリソースおよびリソースの更新を自動的にダウンロードするようにISEを設定することもできます。詳細については、Cisco ISE でのクライアント プロビジョニングの設定 （97 ページ） を参照してください。
- [ローカルディスクのエージェントリソース（Agent resources from local disk）]：ISE にアップロードする PC 上のリソースを選択します。ローカル マシンからのシスコ提供のクライアント プロビジョニング リソースの追加 （100 ページ） を参照してください。
- [AnyConnect設定（AnyConnect Configuration）]：クライアント プロビジョニングで使用できるようにする AnyConnect PC クライアントを選択します。詳細については、「AnyConnect 設定の作成」を参照してください。
- [ネイティブサプリカントプロファイル（Native Supplicant Profile）]：ネットワークの設定が含まれている電話とタブレット用のサプリカントプロファイルを設定します。詳細については、「ネイティブ サプリカント プロファイルの作成」を参照してください。
- [AnyConnect ISE ポスチャプロファイル（AnyConnect ISE Posture Profile）]：エージェント XML プロファイルを作成および配布しない場合は、 AnyConnect ISE ポスチャを設定します。AnyConnect ISE ポスチャ エージェントおよび ISE ポスチャ プロファイル エディタの詳細については、お使いのバージョンの AnyConnect（https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-installation-and-configuration-guides-list.html）の『AnyConnect Administrators Guide』を参照してください。

クライアント プロビジョニング リソースを作成した後、エンドポイントにクライアント プロビジョニング リソースを適用するクライアント プロビジョニング ポリシーを作成します。クライアント プロビジョニング リソース ポリシーの設定 （131 ページ） を参照してください。

関連トピック

Cisco ISE でのクライアント プロビジョニングの設定 （97 ページ）
シスコからのクライアント プロビジョニング リソースの追加 （100 ページ）
クライアント プロビジョニング リソースの自動ダウンロード
ローカル マシンからのシスコ提供のクライアント プロビジョニング リソースの追加 （100 ページ）
ローカル マシンからの AnyConnect 用の顧客作成リソースの追加 （101 ページ）

シスコからのクライアント プロビジョニング リソースの追加

Windows クライアントおよび MAC OS x クライアント用の AnyConnectと Cisco Web エージェントのためにCisco.comからクライアントプロビジョニング リソースを追加できます。選択したリソースおよび利用できるネットワーク帯域幅によっては、Cisco ISE にクライアント プロビジョニング リソースをダウンロードするのに数分かかることがあります。

始める前に

- Cisco ISE で正しいプロキシ設定が設定されていることを確認します。
- Cisco ISE でクライアント プロビジョニングを有効にします。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** を選択します。

ステップ 2 **[追加（Add）] > [Cisco サイトのエージェント リソース（Agent resources from Cisco site）]** を選択します。

ステップ 3 [ダウンロード リモート リソース（Download Remote Resources）] ダイアログボックスで選択可能なリストから必要なクライアント プロビジョニング リソースを 1 つ以上選択します。

ステップ 4 **Save** をクリックします。

次のタスク

Cisco ISE に正常にクライアント プロビジョニング リソースを追加したら、クライアント プロビジョニング リソース ポリシーの設定を開始します。

ローカル マシンからのシスコ提供のクライアント プロビジョニング リソースの追加

シスコから以前にダウンロードしたクライアント プロビジョニング リソースをローカルディスクから追加できます。

始める前に

Cisco ISE には、必ず現行のサポートされているリソースのみをアップロードしてください。サポートされていない古いリソースでは、クライアントアクセスに重大な問題が発生する可能性があります。

Cisco.com からリソースファイルを手動でダウンロードする場合は、リリースノートの「Cisco ISE Offline Updates」の項を参照してください。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** を選択します。

ステップ 2 **[追加（Add）]** > **[ローカル ディスクのエージェント リソース（Agent resources from local disk）]** を選択します。

ステップ 3 [カテゴリ（Category）] ドロップダウンから [シスコ提供パッケージ（Cisco Provided Packages）] を選択します。

ステップ 4 **Browse** をクリックし、Cisco ISE にダウンロードするリソース ファイルがあるローカル マシン上のディレクトリに移動します。

以前に Cisco からローカルマシンにダウンロードした AnyConnect、Cisco NAC Agent、または Cisco Web エージェントのリソースを追加できます。

ステップ 5 **Submit** をクリックします。

次のタスク

Cisco ISE に正常にクライアント プロビジョニング リソースを追加したら、クライアント プロビジョニング リソース ポリシーの設定できます。

ローカル マシンからの AnyConnect 用の顧客作成リソースの追加

AnyConnect カスタマイズ パッケージ、AnyConnect ローカリゼーション パッケージ、AnyConnect プロファイルなどの顧客作成リソースをローカル マシンから Cisco ISE に追加します。

始める前に

AnyConnect の顧客作成リソースがローカル ディスクに zip 形式のファイルで使用可能であることを確認します。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[クライアント プロビジョニング（Client provisioning）]** > **[リソース（Resources）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ローカル ディスクのエージェント リソース（Agent Resources from local disk）] を選択します。

ステップ 4 [カテゴリ（Category）] ドロップダウンから [顧客作成のパッケージ（Customer Created Packages）] を選択します。

ステップ 5 AnyConnect リソースの名前と説明を入力します。

ステップ 6 [参照（Browse）] をクリックし、Cisco ISE にダウンロードするリソース ファイルがあるローカル マシン上のディレクトリに移動します。

ステップ 7 Cisco ISE にアップロードする次の AnyConnect リソースを選択します。

- AnyConnect カスタマイゼーション バンドル
- AnyConnect ローカリゼーション バンドル
- AnyConnect プロファイル
- 高度なマルウェア防御（AMP）イネーブラ プロファイル

ステップ 8 [送信（Submit）] をクリックします。

[アップロードされた AnyConnect リソース（Uploaded AnyConnect Resources）] 表に、Cisco ISE に追加する AnyConnect リソースが表示されます。

次のタスク

AnyConnect エージェント プロファイルの作成

ネイティブ サプリカント プロファイルの作成

ネイティブ サプリカント プロファイルを作成して、ユーザが独自のデバイスを Cisco ISE ネットワークに含めることができます。ユーザがサインインすると、Cisco ISE は、ユーザの承認要件に関連付けられたプロファイルを使用して、必要なサプリカント プロビジョニング ウィザードを選択します。ウィザードは、ユーザのパーソナルデバイスを起動して設定し、ネットワークにアクセスします。

（注） プロビジョニング ウィザードは、アクティブなインターフェイスのみを設定します。このため、有線接続ユーザと無線接続ユーザは、どちらもアクティブになっている場合を除き、両方のインターフェイスにはプロビジョニングされません。

始める前に

- TCP ポート 8905 を開き、Cisco AnyConnect Agent、Cisco Web Agent、およびサプリカント プロビジョニング ウィザードのインストールを有効にします。ポートの使用法の詳細については、『*Cisco Identity Services Engine Hardware Installation Guide*』の付録「Cisco ISE Appliance Ports Reference」を参照してください。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** を選択します。

ステップ 2 **[追加（Add）] > [ネイティブ サプリカント プロファイル（Native Supplicant Profile）]** を選択します。

ステップ 3 に示す説明を使用して、プロファイルを作成します。 ネイティブ サプリカント プロファイルの設定 （103 ページ）

次のタスク

「複数ゲスト ポータルのサポート」の項の説明に従って、従業員が自分のパーソナル デバイスをネットワークに直接接続できるようにセルフ プロビジョニング機能を有効にします。

ネイティブ サプリカント プロファイルの設定

[ポリシー（Policy）] > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[クライアント プロビジョニング リソース（Client Provisioning Resources）]** の順に選択し、ネイティブ サプリカント プロファイルを追加すると、次の設定が表示されます。

- [名前（Name）]：作成するネイティブ サプリカント プロファイルの名前。このプロファイルを適用するオペレーティング システムを選択します。各プロファイルは、ISE がクライアントのネイティブ サプリカントに適用するネットワーク接続の設定を定義します。

ワイヤレス プロファイル

1 つ以上のワイヤレス プロファイルを設定します。クライアントで使用可能にする SSID ごとに 1 つを設定します。

- [SSID名（SSID Name）]：クライアントが接続する SSID の名前。
- [プロキシ自動コンフィギュレーションファイルのURL（Proxy Auto-Config File URL）]：サプリカントのネットワーク設定を取得するためにクライアントがプロキシに接続する場合は、そのプロキシ サーバへの URL を入力します。
- **プロキシホスト/IP（Proxy Host/IP）**
- **プロキシ ポート（Proxy Port）**
- [セキュリティ（Security）]：WPA または WPA2 を使用するようにクライアントを設定します。
- [許可されているプロトコル（Allowed Procotol）]：クライアントが認証サーバに接続するのに使用するプロトコルを設定します（PEAP または EAP-TLS）。
- [証明書テンプレート（Certificate Template）]：TLS の場合は、**[管理（Administration）]** > **[システム証明書（System Certificates）]** > **[認証局（Certificate Authority）]** > **[証明書テンプレート（Certificate Templates）]** で定義された証明書テンプレートのいずれかを選択します。

オプション設定は、「オプション設定：*Windows* の場合」の項で説明します。

iOS 設定

- **ターゲットネットワークが非表示になっている場合に有効にする（Enable if target network is hidden）**

有線プロファイル

- [許可されているプロトコル（Allowed Protocol）]：クライアントが認証サーバに接続するのに使用するプロトコルを設定します（PEAP または EAP-TLS）。
- [証明書テンプレート（Certificate Template）]：TLS の場合は、[管理（Administration）][システム証明書（System Certificates）][認証局（Certificate Authority）][証明書テンプレート（Certificate Templates）] で定義された証明書テンプレートのいずれかを選択します。

オプション設定：Windows の場合

[オプション（Optional）] を展開すると、Windows クライアントの場合は次のフィールドも使用できます。

- [認証モード（Authentication Mode）]：許可のクレデンシャルとして、[ユーザ（User）]、[マシン（Machine）] またはその両方を使用するかを決定します。
- [自動的にログイン名とパスワード（およびもしあればドメイン）を使用する（Automatically use logon name and password (and domain if any)）]：認証モードで [ユーザ（User）] を選択すると、ユーザにプロンプトを表示することなくログインおよびパスワードを使用します（その情報が使用できる場合）。
- [高速再接続を有効にする（Enable Fast Reconnect）]：セッションの再開機能が PEAP プロトコル オプションで有効な場合（これは、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[プロトコル（Protocols）]** > **[PEAP]** で設定されます）、PEAP セッションはユーザ クレデンシャルをチェックすることなく再開できます。
- [隔離チェックを有効にする（Enable Quarantine Checks）]：クライアントが隔離されたかどうかを確認します。
- [サーバが暗号化バインドTLVを示さない場合に切断する（Disconnect if server does not present cryptobinding TLV）]：暗号化バインド TLV がネットワーク接続でサポートされていない場合に切断します。
- [新規サーバまたは信頼できる証明機関の承認をユーザに求めない（Do not prompt user to authorize new servers or trusted certification authorities）]：自動的にユーザ証明書を受け入れ、ユーザにプロンプトを表示しません。
- [ネットワークが名前（SSID）をブロードキャストしていなくても接続する（Connect even if the network is not broadcasting its name (SSID)）]：ワイヤレス プロファイルの場合のみ。

各種ネットワークでの URL リダイレクトなしでのクライアント プロビジョニング

URL リダイレクトなしのクライアント プロビジョニングは、サードパーティの NAC で CoA がサポートされていない場合に必要です。クライアント プロビジョニングは、URL リダイレクトの有無にかかわらず実行できます。

（注） URL リダイレクションを使用するクライアント プロビジョニングの場合、クライアント マシンにプロキシ設定が構成されている場合は、ブラウザ設定の例外リストに Cisco ISE を追加してください。この設定は、URL リダイレクションを使用するすべてのフロー、BYOD、MDM、ゲスト、およびポスチャに適用されます。たとえば、Windows マシンでは、次の手順を実行します。

1. コントロール パネルから、[Internet Properties] をクリックします。
2. [Connections] タブを選択します。
3. [LAN settings] をクリックします。
4. [プロキシ サーバー] 領域から、[Advanced] をクリックします。
5. [Exceptions] ボックスに Cisco ISE ノードの IP アドレスを入力します。
6. [OK] をクリックします。

各種ネットワークでリダイレクトなしでエンドポイントをプロビジョニングする手順を次に示します。

Dot1X EAP-TLS

1. プロビジョニングされた認証を使用して Cisco ISE ネットワークに接続する
2. ブラウザ ウィンドウを開き、プロビジョニング URL（provisioning.cisco.com）を入力する。
3. 内部ユーザ、AD、LDAP、または SAML を介して CP ポータルにログインする。

   AnyConnect がポスチャを実行する。エンドポイントがポスチャ コンプライアンスに基づいて正しいネットワークに移動する。

Dot1X PEAP

1. NSP 経由でユーザ名とパスワードを使用して Cisco ISE ネットワークに接続する
2. ブラウザ ウィンドウを開き、プロビジョニング URL（provisioning.cisco.com）を入力する。
3. 内部ユーザ、AD、LDAP、または SAML を介して CP ポータルにログインする

   AnyConnect がポスチャを実行する。エンドポイントがポスチャ コンプライアンスに基づいて正しいネットワークに移動する。

MAB（有線ネットワーク）

1. Cisco ISE ネットワークに接続する。
2. ブラウザ ウィンドウを開き、プロビジョニング URL（provisioning.cisco.com）を入力する。
3. 内部ユーザ、AD、LDAP、または SAML を介して CP ポータルにログインする。

   AnyConnect がポスチャを実行する。エンドポイントがポスチャ コンプライアンスに基づいて正しいネットワークに移動する。

MAB（ワイヤレス ネットワーク）

1. Cisco ISE ネットワークに接続する
2. ブラウザ ウィンドウを開き、プロビジョニング URL（provisioning.cisco.com）を入力する。
3. 内部ユーザ、AD、LDAP、または SAML を介して CP ポータルにログインする。

   AnyConnect がポスチャを実行する。ポスチャはワイヤレス 802.1X の場合にのみ開始する。

AMP イネーブラ プロファイルの設定

次の表に、[高度なマルウェア防御（AMP）イネーブラプロファイル（Advanced Malware Protection (AMP) Enabler Profile）] ページのフィールドを示します。ナビゲーション パスは、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** です。

[追加（Add）] ドロップダウン矢印をクリックし、[AMPイネーブラプロファイル（AMP Enabler Profile）] を選択します。

表 23 : [AMPイネーブラプロファイル（AMP Enabler Profile）] ページ

フィールド	使用上のガイドライン
[名前（Name）]	ユーザが作成する AMP イネーブラ プロファイルの名前を入力します。
説明	AMPイネーブラ プロファイルの説明を入力します。

フィールド	使用上のガイドライン
AMPイネーブラのインストール（Install AMP Enabler）	• **Windows インストーラ**：Windows OS ソフトウェアの AMP をホストするローカル サーバの URL を指定します。AnyConnect モジュールはこの URL を使用して、エンドポイントに .exe ファイルをダウンロードします。ファイル サイズは約 25 MB です。 • **Mac インストーラ**：Mac OSX ソフトウェアの AMP をホストするローカル サーバの URL を指定します。AnyConnect モジュールはこの URL を使用して、エンドポイントに .pkg ファイルをダウンロードします。ファイル サイズは約 6 MB です。 [オン（Check）] ボタンは、サーバと通信を行って URL が有効かどうかを確認します。URL が有効の場合は、「ファイルが見つかりました（File found）」メッセージが表示され、有効でない場合はエラー メッセージが表示されます。
AMPイネーブラのアンインストール（Uninstall AMP Enabler）	エンドポイントからエンドポイント ソフトウェアの AMP をアンインストールします。
開始メニューへの追加（Add to Start Menu）	エンドポイント ソフトウェアの AMP がエンドポイントにインストールされた後、エンドポイントの [開始（Start）] メニューにエンドポイント ソフトウェアの AMP のショートカットを追加します。
デスクトップへの追加（Add to Desktop）	エンドポイント ソフトウェアの AMP がエンドポイントにインストールされた後、エンドポイントのデスクトップにエンドポイント ソフトウェアの AMP のショートカットを追加します。
コンテキストメニューへの追加（Add to Context Menu）	エンドポイント ソフトウェアの AMP がエンドポイントにインストールされた後、エンドポイントの右クリック コンテキスト メニューに [今すぐスキャン（Scan Now）] オプションを追加します。

組み込みプロファイル エディタを使用した AMP イネーブラ プロファイルの作成

ISE 埋め込みプロファイル エディタまたはスタンドアロン エディタを使用して、AMP イネーブラ プロファイルを作成できます。

ISE 埋め込みプロファイル エディタを使用して AMP イネーブル プロファイルを作成するには、次の手順を実行します。

始める前に

- SOURCEfire ポータルからエンドポイント ソフトウェアの AMP をダウンロードし、ローカル サーバでホスティングします。
- [管理（Administration）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] に移動して、エンドポイント ソフトウェアの AMP をホストするサーバの証明書を ISE 証明書ストアにインポートします。
- [AMPイネーブラ（AMP Enabler）] オプションが [AnyConnect設定（AnyConnect Configuration）] ページ（[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアントプロビジョニング（Client provisioning）] > [リソース（Resources）] > [追加（Add）] > [AnyConnect設定（AnyConnect Configuration）] > [AnyConnectパッケージの選択（Select AnyConnect Package）]）の [AnyConnectモジュール選択（AnyConnect Module Selection）] および [プロファイル選択（Profile Selection）] セクションで選択されていることを確認します。
- SOURCEfire ポータルにログインして、エンドポイント グループのポリシーを作成し、エンドポイント ソフトウェアの AMP をダウンロードする必要があります。ソフトウェアには、選択したポリシーが事前設定されています。2 つのイメージ、すなわち Windows OS の場合はエンドポイント ソフトウェアの AMP、Mac OSX の場合はエンドポイント ソフトウェアの AMP の再頒布可能なバージョンをダウンロードする必要があります。ダウンロードされたソフトウェアは、エンタープライズネットワークからアクセスできるサーバでホストされます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョン（Client Provision）] > [リソース（Resources）]** を選択します。

ステップ 2 [追加（Add）] ドロップダウンをクリックします。

ステップ 3 [AMPイネーブラプロファイル（AMP Enabler Profile）] を選択して、新しい AMP イネーブラ プロファイルを作成します。

ステップ 4 フィールドに適切な値を入力します。

ステップ 5 [送信（Submit）] をクリックして、プロファイルを [リソース（Resources）] ページに保存します。

スタンドアロン エディタを使用した AMP イネーブラ プロファイルの作成

AnyConnect スタンドアロンエディタを使用して、AMP イネーブラ プロファイルを作成するには、次の手順を実行します。

始める前に

AnyConnect 4.1 スタンドアロン エディタを使用して、XML 形式のプロファイルをアップロードして AMP イネーブラ プロファイルを作成できます。

- Cisco.com から Windows および Mac OS の AnyConnect スタンドアロン プロファイル エディタをダウンロードします。
- スタンドアロン プロファイル エディタを起動し、[AMPイネーブラプロファイルの設定（AMP Enabler Profile Settings）]AMP イネーブラ プロファイルの設定 （106 ページ）で指定されているようにフィールドに入力します。
- プロファイルを XML ファイルとしてローカル ディスクに保存します。
- [AMPイネーブラ（AMP Enabler）] オプションが [AnyConnect設定（AnyConnect Configuration）] ページ（[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアントプロビジョニング（Client provisioning）] > [リソース（Resources）] > [追加（Add）] > [AnyConnect設定（AnyConnect Configuration）] > [AnyConnectパッケージの選択（Select AnyConnect Package）]）の [AnyConnectモジュール選択（AnyConnect Module Selection）] および [プロファイル選択（Profile Selection）] セクションで選択されていることを確認します。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client provisioning）] > [リソース（Resources）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ローカルディスクのエージェントリソース（Agent resources from local disk）] を選択します。

ステップ 4 [カテゴリ（Category）] ドロップダウンから [顧客作成のパッケージ（Customer Created Packages）] を選択します。

ステップ 5 [タイプ（Type）] ドロップダウンから [AMPイネーブラプロファイル（AMP Enabler Profile）] を選択します。

ステップ 6 [名前（Name）] と [説明（Description）] に入力します。

ステップ 7 [参照（Browse）] をクリックして、ローカル ディスクから保存済みプロファイル（XML ファイル）を選択します。次に、カスタマイズされたインストール ファイルの例を示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<FAProfile xsi:noNamespaceSchemaLocation="FAProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <FAConfiguration>
 <Install>
 <WindowsConnectorLocation>
https://fa_webserver/ACFA_Mac_FireAMPSetup.exe
```

```
</WindowsConnectorLocation>
 <MacConnectorLocation>
https://fa_webserver/ACFA_Mac_FireAMPSetup.exe
</MacConnectorLocation>
 <StartMenu>true</StartMenu>
 <DesktopIcon>false</DesktopIcon>
 <ContextIcon>true</ContextIcon>
 </Install>
 </FAConfiguration>
</FAProfile>
```

次に、カスタマイズされたアンインストール ファイルの例を示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<FAProfile xsi:noNamespaceSchemaLocation="FAProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <FAConfiguration>
 <Uninstall>
 </Uninstall>
 </FAConfiguration>
</FAProfile>
```

ステップ 8 [送信（Submit）] をクリックします。
新しく作成された AMP イネーブラ プロファイルが [リソース（Resources）] ページに表示されます。

一般的な AMP イネーブラ インストール エラーのトラブルシューティング

[Windowsインストーラ（Windows Installer）] または [MACインストーラ（MAC Installer）] テキスト ボックスに SOURCEfire URL を入力して [オン（Check）] をクリックすると、次のエラーのいずれかが発生する場合があります。

- エラー メッセージ：「MacまたはWindowsのインストーラファイルを含むサーバの証明書がISEによって信頼されていません。（The certificate for the server containing the Mac/Windows installer file is not trusted by ISE.）信頼証明書を [管理（Administration）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] に追加します。（Add a trust certificate to **Administration** > **Certificates** > **Trusted Certificates**.）」

  このエラー メッセージは、Cisco ISE 証明書ストアに SOURCEfire の信頼できる証明書をインポートしていない場合に表示されます。SOURCEfire の信頼できる証明書を入手し、Cisco ISE の信頼できる証明書ストア（[管理（Administration）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]）にインポートします。

- エラー メッセージ：「インストーラファイルがこの場所で見つかりません。接続の問題である可能性があります。（The installer file is not found at this location, this may be due to a connection issue.）有効なパスを [インストーラ（Installer）] テキスト ボックスに入力するか、または接続を確認します。（Enter a valid path in the Installer text box or check your connection.）」

  このエラー メッセージは、エンドポイント ソフトウェアの AMP をホストしているサーバがダウンした場合、または [Windowsインストーラ（Windows Installer）] または [MACインストーラ（MAC Installer）] テキスト ボックスに入力ミスがある場合に表示されます。

- エラー メッセージ：「[Windowsインストーラ（Windows Installer）]または[MACインストーラ（MAC Installer）]テキスト ボックスに有効なURLが含まれていません。（The Windows/Mac installer text box does not contain a valid URL.）」

  このエラー メッセージは、構文的に正しくないURL形式を入力した場合に表示されます。

Cisco ISE の Chromebook デバイスのオンボーディングのサポート

Chromebookデバイスは他のデバイス（Apple、Windows、Android）とは異なり管理型デバイス（Google ドメインによって管理）で、オンボーディング サポートが制限されています。Cisco ISE はネットワークでの Chromebook デバイスのオンボーディングをサポートしています。オンボーディングとは、Cisco ISE による認証の後にネットワークに安全に接続できるように、エンドポイントに必要な設定とファイルを配送するプロセスのことです。このプロセスには、証明書のプロビジョニングやネイティブ サプリカントのプロビジョニングが含まれています。ただし、Chromebookデバイスでは、証明書のプロビジョニングのみが実行できます。ネイティブ サプリカントのプロビジョニングは、Google 管理コンソールで実行されます。

管理されていない Chromebook デバイスは、安全なネットワークへのオンボーディングができません。

Chromebook オンボーディング プロセスに関与するエンティティは次のとおりです。

- Google 管理者
- ISE 管理者
- Chromebook ユーザ/デバイス
- Google 管理コンソール（Google 管理者が管理）

Google 管理者：

- 次のライセンスの安全性を確保します。
  1. Google 管理コンソール設定のための Google Apps 管理者ライセンス。URL：https://admin.google.com。Google管理コンソールを使用して、管理者は組織内の人間のための Google サービスを管理できます。
  2. Chromebook のデバイス管理ライセンス。URL：https://support.google.com/chrome/a/answer/2717664?hl=en。Chromebook のデバイス管理ライセンスは、特定の Chromebook デバイスに対して設定を行い、ポリシーを適用するために使用されます。ユーザアクセスの制御、機能のカスタマイズ、ネットワークアクセスの設定などのためのデバイス設定への Google 管理者アクセス権を提供します。
- Googleデバイス ライセンスによるChromebookデバイスのプロビジョニングと登録を促進します。

- Google 管理コンソールを通じて Chromebook デバイスを管理します。
- 各 Chromebook ユーザの Wi-Fi ネットワーク設定のセットアップと管理を行います。
- Chromebook デバイスでアプリケーションの設定と強制されている拡張機能のインストールを行い、Chromebook デバイスを管理します。Chromebook デバイスのオンボーディングには、Chromebook デバイスに Cisco Network Setup Assistant 拡張機能がインストールされている必要があります。これにより、Chromebook デバイスが Cisco ISE に接続し、ISE 証明書をインストールできるようになります。証明書のインストールの操作は管理対象デバイスにのみ許可されるため、この拡張機能は強制的にインストールされます。
- サーバの検証と安全な接続を実現するために、Cisco ISE 証明書が Google 管理コンソールにインストールされていることを確認します。Google 管理者が、証明書がデバイスに対して生成されるか、ユーザに対して生成されるかを決定します。Cisco ISE には次のオプションがあります。
  - Chromebook デバイスを共有しない単一のユーザ用に証明書を生成します。
  - 複数のユーザで共有される Chromebook デバイス用に証明書を生成します。必要な追加設定については、「Google 管理コンソールでのネットワークの設定と拡張機能の強制」セクションの手順 5 を参照してください。

  ISE が Chromebook デバイスで証明書のプロビジョニングを実行するために信頼され、EAP-TLS 証明書ベースの認証が許可されるように、Google 管理者が ISE サーバ証明書をインストールします。Google Chrome バージョン 37 以降は、Chromebook デバイスの証明書ベースの認証をサポートしています。Google 管理者は Google 管理コンソールで ISE プロビジョニング アプリケーションをロードし、ISE から証明書を取得するために Chromebook デバイスで使用できるようにする必要があります。
- 推奨される Google ホスト名が、SSL の安全な接続のために WLC で設定された ACL 定義リストのホワイト リストにあることを確認します。Google サポート ページの推奨されるホスト名のホワイト リストを参照してください。

ISE 管理者：

- 証明書テンプレートの構造を含む、Chromebook OS のネイティブ サプリカント プロファイルを定義します。
- Chromebook ユーザの Cisco ISE で必要な認証ルールとクライアント プロビジョニング ポリシーを作成します。

Chromebook ユーザ：

- Chromebook デバイスを消去し、Google ドメインに登録して、Google 管理者によって定義された適用ポリシーを保護します。
- Chromebook デバイス ポリシーと、Google 管理コンソールによってインストールされた、強制されている Cisco Network Setup Assistant 拡張機能を受信します。
- Google 管理者によって定義されているとおりにプロビジョニングされた SSID に接続して、ブラウザを開いて BYOD ページを表示し、オンボーディング プロセスを開始します。
- Cisco Network Setup Assistant が Chromebook デバイスにクライアント証明書をインストールし、これによりデバイスが EAP-TLS 証明書ベースの認証を行えるようになります。

Google 管理コンソール：

Google 管理コンソールは Chromebook デバイス管理をサポートし、安全なネットワークの設定と、Chromebook への Cisco Network Setup Assistant 証明書管理拡張機能のプッシュができます。この拡張機能は SCEP 要求を Cisco ISE に送信し、クライアント証明書をインストールして、安全な接続とネットワークへのアクセスを可能にします。

共有環境での Chromebook デバイスの使用のベスト プラクティス

Chromebook デバイスが学校や図書館などの共有環境で使用される場合、Chromebook デバイスはさまざまなユーザによって共有されます。シスコが推奨するベストプラクティスの一部は、次のとおりです。

- 特定のユーザ（学生または教授）の名前で Chromebook デバイスをオンボーディングする場合、ユーザの名前が証明書の [件名（Subject）] フィールドの [共通名（CN）（Common Name (CN)）] に入力されます。また、共有 Chromebook がその特定のユーザの My Devices ポータルに表示されます。そのため、共有デバイスではオンボーディング時に共有クレデンシャルを使用し、特定のユーザの My Devices ポータルのリストにのみデバイスが表示されるようにすることを推奨します。共有アカウントは、個別のアカウントとして管理者または教授が管理し、共有デバイスを制御することができます。
- ISE 管理者は、共有 Chromebook デバイス用のカスタム証明書テンプレートを作成し、ポリシーで使用することができます。たとえば、[件名-共通名（CN）（Subject-Common Name (CN)）] 値に一致する標準の証明書テンプレートを使用する代わりに、証明書の名前（chrome-shared-grp1 など）を指定して同じ名前を Chromebook デバイスに割り当てることができます。ポリシーは、Chromebook デバイスへのアクセスを許可または拒否するために、名前で一致させるように設計できます。
- ISE 管理者は、（アクセスが制限される必要があるデバイスの）Chromebook オンボーディングを経る必要があるすべての Chromebook デバイスの MAC アドレスを備えたエンドポイント グループを作成することができます。認証ルールは、デバイス タイプ Chromebook とともにこれを呼び出す必要があります。これにより、アクセスが NSP にリダイレクトされます。

Chromebook オンボーディング プロセス

Chromebook オンボーディング プロセスは、次の一連のステップを実行します。

ステップ 1 Google 管理コンソールでのネットワークの設定と拡張機能の強制 。
ステップ 2 Chromebook オンボーディングのための ISE の設定。
ステップ 3 Chromebook デバイスのワイプ。
ステップ 4 Google 管理コンソールへの Chromebook の登録。
ステップ 5 BYOD オンボーディング用の Cisco ISE ネットワークへの Chromebook の接続。

Google 管理コンソールでのネットワークの設定と拡張機能の強制

Google 管理者は、次の手順を実行します。

ステップ 1 Google 管理コンソールにログインします。

a) ブラウザで URL https://admin.google.com を入力します。
b) 必要なユーザ名とパスワードを入力します。
c) [Welcome to Admin Console] ページで、[Device Management] をクリックします。
d) [デバイス管理（Device Management）] ページで、[ネットワーク（Network）] をクリックします。

ステップ 2 管理対象デバイスの Wi-Fi ネットワークをセットアップします。

a) [ネットワーク（Networks）] ページで、[Wi-Fi] をクリックします。
b) [Add Wi-Fi] をクリックして、必要な SSID を追加します。詳細については、「Google 管理コンソール：Wi-Fi ネットワーク設定」を参照してください。

MAB フローについては、2 つの SSID を作成し、1 つをオープン ネットワーク用、もう 1 つを証明書認証用にします。ユーザがオープン ネットワークに接続すると、Cisco ISE ACL は、認証のために、ユーザをクレデンシャルを持つゲスト ポータルにリダイレクトします。認証が成功すると、ACL はユーザを BYOD ポータルにリダイレクトします。

ISE 証明書が中間 CA によって発行された場合は、ルート CA ではなく、中間証明書を「サーバ認証局」にマッピングする必要があります。

c) [追加（Add）] をクリックします。

ステップ 3 強制拡張機能を作成します。

a) [デバイス管理（Device Management）] ページの [デバイス設定（Device Settings）] 領域で、[Chrome管理（Chrome Management）] をクリックします
b) [User Settings] をクリックします。
c) 下にスクロールして、[アプリケーションと拡張機能（Apps and Extensions）] セクションの [強制的にインストールされたアプリケーションと拡張機能（Force-Installed Apps and Extensions）] オプションで、[強制的にインストールされたアプリケーションの管理（Manage Force-Installed Apps）] をクリックします。

ステップ 4 強制拡張機能をインストールします。

a) [強制的にインストールされたアプリケーションと拡張機能（Force-Installed Apps and Extensions）] ページで、[Chromeウェブストア（Chrome Web Store）] をクリックします。
b) [検索（Search）] テキスト ボックスに「Cisco Network Setup Assistant」と入力して、拡張機能を見つけます。

Chromebook デバイスの Cisco Network Setup Assistant 拡張機能は、Cisco ISE の証明書を要求し、Chromebook デバイスに ISE の証明書をインストールします。証明書のインストールは管理対象デバイスに対してのみ許可されるため、この拡張機能は、強制的にインストールされるように設定する必要があります。登録プロセス中にこの拡張機能がインストールされていない場合は、Cisco ISE の証明書をインストールすることはできません。

拡張機能でサポートされている言語の詳細については、「Cisco ISE 国際化およびローカリゼーション」を参照してください。

c) [Add] をクリックして、強制的にアプリをインストールします。
d) [保存（Save）] をクリックします。

ステップ 5 （オプション）複数のユーザに共有されている Chromebook デバイスに証明書をインストールするには、コンフィギュレーション ファイルを定義します。

a) メモ帳ファイルに次のコードをコピー アンド ペーストして、ローカル ディスクに保存します。

```
{
  "certType": {
    "Value": "system"
  }
}
```

b) **[Device Management]** > **[Chromebook Management]** > **[App Management]** の順に選択します。
c) [Cisco Network Setup Assistant] 拡張機能をクリックします。
d) [User Settings] をクリックし、ドメインを選択します。
e) [設定ファイルのアップロード（Upload Configuration File）] をクリックし、ローカルディスクに保存した .txt ファイルを選択します。

（注） Cisco Network Setup Assistant で複数のユーザが共有するデバイスの証明書を作成するには、このメモ帳ファイルを Google 管理コンソールに追加する必要があります。追加しないと、Cisco NSA はシングル ユーザ用の証明書を作成します。

f) [保存（Save）] をクリックします。

ステップ 6 （オプション）Chromebook を共有しないシングル ユーザの証明書をインストールします。

a) **[Device Management]** > **[Network]** > **[Certificates]** の順に選択します。
b) [Certificates] セクションで、[Add Certificate] をクリックして、Cisco ISE の証明書ファイルをアップロードします。

次のタスク

Chromebook オンボーディングのための ISE の設定

Chromebook オンボーディングのための ISE の設定

始める前に

ISE 管理者は、[ポリシー（Policy）]>[ポリシー セット（Policy Sets）] ページで必要なポリシーを作成する必要があります。

認証ポリシーの例を次に示します。

Rule Name: Full_Access_After_Onboarding, Conditions: If RegisteredDevices AND Wireless_802.1x AND Endpoints:BYODRegistration EQUALS Yes AND Certificate: Subject Alternative Name Equals

RadiusCalling-Station-ID AND Network Access: EAP-Authentication EQUALS EAP-TLS Then CompliantNetworkAccess.

CompliantNetworkAccess は、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[Authorization（認証）]** > **[認証プロファイル（Authorization Profiles）]** ページで設定されている認証結果です。

ステップ 1 Cisco ISE でネイティブ サプリカント プロファイル（NSP）を設定します。

a) **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** の順に選択します。

b) **[クライアント プロビジョニング（Client Provisioning）]** > **[リソース（Resources）]** の順にクリックします。

Chromebook デバイスが新規 Cisco ISE インストールの [クライアント プロビジョニング（Client Provisioning）] ページに表示されます。ただし、アップグレードの場合は、[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [更新（Updates）] ページからポスチャの更新プログラムをダウンロードする必要があります。

c) **[追加（Add）]** > **[ネイティブ サプリカント プロファイル（Native Supplicant Profile）]** の順にクリックします。

d) [名前（Name）] と [説明（Description）] に入力します。

e) **[オペレーティング システム（Operating System）]** フィールドで、**[Chrome OS すべて（Chrome OS All）]** を選択します。

f) **[証明書テンプレート（Certificate Template）]** フィールドで、必要な証明書テンプレートを選択します。

g) [送信（Submit）] をクリックします。SSID が Google 管理コンソールからプロビジョニングされていて、ネイティブ サプリカント プロビジョニング フローからではないことを確認します。

ステップ 2 [クライアント プロビジョニング（Client Provisioning）] ページで NSP をマッピングします。

a) [ポリシー（Policy）] > [クライアント プロビジョニング（Client Provisioning）] の順に選択します。

b) 結果を定義します。

- クライアント プロビジョニング ポリシーの [結果（Results）] で組み込みのネイティブ サプリカント設定（Cisco-ISE-Chrome-NSP）を選択します。
- または、新しいルールを作成し、Chromebook デバイス用に作成された [結果（Result）] が選択されていることを確認します。

Chromebook デバイスのワイプ

Chromebook デバイスは、Google 管理コンソールが Google 管理者により設定された後でワイプされる必要があります。Chromebook ユーザはデバイスをワイプする必要があり、これは拡張を強制し、ネットワークを設定する一度だけの処理です。詳細については、次の URL https://support.google.com/chrome/a/answer/1360642を参照してください。

Chromebook ユーザは次の手順を実行します。

ステップ 1 **Esc + Refresh + Power** キーの組み合わせを押します。画面に黄色い感嘆符（!）が表示されます。

ステップ 2 開発モードを開始するには、**Ctrl + D** キーの組み合わせを押してから、**Enter** キーを押します。画面に赤い感嘆符が表示されます。

ステップ 3 **Ctrl + D** キーの組み合わせを押します。Chromebook はローカルデータを削除して、初期状態に戻ります。この削除には約 15 分かかります。

ステップ 4 移行が完了したら、**Space** キーを押してから **Enter** キーを押して、確認モードに戻ります。

ステップ 5 サインインする前に Chromebook を登録します。

次のタスク

Google 管理コンソールに Chromebook を登録します。

Google 管理コンソールへの Chromebook の登録

Chromebook のデバイスをプロビジョニングするには、Chromebook ユーザは最初に Google 管理コンソールページに登録し、デバイスポリシーおよび強制拡張を受信する必要があります。

ステップ 1 Chromebook のデバイスの電源を入れ、サインオン画面が表示されるまで、画面上の指示に従います。まだサインインしないでください。

ステップ 2 Chromebook のデバイスにサインインする前に、**Ctrl + Alt + E** のキーの組み合わせを押します。[エンタープライズ登録（Enterprise Enrolment）] 画面が表示されます。

ステップ 3 E メールアドレスを入力し、[次へ（Next）] をクリックします。
次のメッセージが表示されます：「デバイスは企業管理用に正しく登録されています（Your device has successfully been enrolled for enterprise management.）」。

ステップ 4 [完了（Done）] をクリックします。

ステップ 5 Google 管理のようこそレターからのユーザ名とパスワード、または登録資格があるアカウントの既存の Google アプリケーション ユーザのユーザ名とパスワードを入力します。

ステップ 6 [デバイスの登録（Enroll Device）] をクリックします。デバイスが正常に登録されると、確認メッセージが表示されます。

Chromebook の登録の処理は一度だけであることに注意してください。

BYOD オンボーディング用の Cisco ISE ネットワークへの Chromebook の接続

デュアル SSID 用の手順：EAP-TLS プロトコルを使用して 802.x ネットワークに接続する場合、Chromebook ユーザは次の手順を実行します。

（注） デュアル SSID を使用している場合：802.x PEAP から EAP-TLS ネットワークに接続するときは、ネットワーク サプリカント（Web ブラウザではなく）にクレデンシャルを入力して、ネットワークに接続してください。

ステップ 1 Chromebook で [設定（Settings）] をクリックします。

ステップ 2 [インターネット接続（Internet Connection）] セクションで、[Wi-Fi ネットワークをプロビジョニングする（Provisioning Wi-Fi Network）] をクリックしてから、該当するネットワークをクリックします。

ステップ 3 クレデンシャルを持つゲスト ポータルが開きます。

1. [サインオン（Sign On）] ページで、[ユーザ名（Username）] と [パスワード（Password）] を入力します。
2. [サインオン（Sign-on）] をクリックします。

ステップ 4 BYOD のウェルカム ページで、[開始（Start）] をクリックします。

ステップ 5 [デバイス情報（Device Information）] フィールドにデバイスの名前と説明を入力します。たとえば、「パーソナル デバイス：学校で使用するジェーンの Chromebook、または共有デバイス：ライブラリ Chromebook #1 または教室 1 Chromebook #1」と入力します。

ステップ 6 [続行（Continue）] をクリックします。

ステップ 7 [Cisco Network Setup Assistant] ダイアログ ボックスで [はい（Yes）] をクリックして、セキュアなネットワークにアクセスするための証明書をインストールします。

Google 管理者がセキュアな Wi-Fi を設定した場合、ネットワーク接続は自動的に行われます。そうでない場合は、使用可能なネットワークのリストからセキュアな SSID を選択します。

すでにドメインに登録され、Cisco Network Setup Assistant の拡張を取得済みの Chromebook ユーザは、自動更新を待たずに、拡張を更新できます。次の手順を実行して、拡張を手動で更新します。

1. Chromebook で、ブラウザを開き、次の URL を入力してください。**chrome://Extensions**
2. [開発者モード（Developer Mode）] チェック ボックスをオンにします。
3. [今すぐ拡張を更新（Update Extensions Now）] をクリックします。
4. Cisco Network Setup Assistant の拡張バージョンが 2.1.0.35 以上であることを確認します。

Google 管理コンソール：Wi-Fi ネットワーク設定

Wi-Fi ネットワークの設定を使用して、顧客ネットワークの SSID を設定するか、または証明書属性（EAP-TLS 用）を使用して証明書を照合します。証明書が Chromebook にインストールされるときに、Google管理設定と同期されます。接続は、定義された証明書属性のいずれかが SSID 設定と一致したときのみ確立されます。

以下に、EAP-TLS、PEAPおよびオープン ネットワーク フローに特有な必須フィールドを示します。これらは、Google 管理コンソール ページで各 Chromebook ユーザに対し、Wi-Fi ネットワークを設定するようにGoogle管理者が設定します。（[デバイス管理（Device Administration）] > [ネットワーク（Network ）] > [Wi-Fi] > [Wi-Fi の追加（Add Wi-Fi）]）。

フィールド	EAP-TLS	PEAP	オープン（Open）
[名前（Name）]	ネットワーク接続の名前を入力します。	ネットワーク接続の名前を入力します。	ネットワーク接続の名前を入力します。
サービスセット識別子（SSID）	SSID（たとえば、tls_ssid）を入力します。	SSID（たとえば、tls_ssid）を入力します。	SSID（たとえば、tls_ssid）を入力します。
この SSID はブロードキャストされません	オプションを選択します。	オプションを選択します。	オプションを選択します。
自動的に接続	オプションを選択します。	オプションを選択します。	オプションを選択します。
セキュリティ タイプ	WPA/WPA2 Enterprise（802.1x）	WPA/WPA2 Enterprise（802.1x）	オープン（Open）
Extensible Authentication Protocol	EAP-TLS	PEAP	—
内部プロトコル	—	• 自動（Automatic） • MSCHAP v2（オプションを選択） • MD5 • PAP • MSCHAP • GTC	—
外部 ID	—	—	—

フィールド	EAP-TLS	PEAP	オープン（Open）
[ユーザ名（Username）]	必要に応じて、固定値を設定するか、またはユーザログインから変数を使用します：${LOGIN_ ID} または ${LOGIN_EMAIL}。	ISE（内部 ISE ユーザ / AD / その他の ISE ID）とパスワードフィールドに対し認証する PEAP クレデンシャルを入力します。	—
サーバ認証局（Server Certificate Authority）	ISE 証明書を選択します（[デバイス管理（Device Administration）] > [ネットワーク（Network ）] > [証明書（Certificates）] からインポートされます）。	ISE 証明書を選択します（[デバイス管理（Device Administration）] > [ネットワーク（Network ）] > [証明書（Certificates）] からインポートされます）。	—
プラットフォームによるこの Wi-Fi ネットワークへのアクセス制限	• モバイル デバイスを選択します。 • Chromebooks を選択します。	• モバイル デバイスを選択します。 • Chromebooks を選択します。	—
クライアントの登録 URL	登録されていないユーザに対して Chromebook デバイスのブラウザがリダイレクトされる先の URL を入力します。未登録のユーザをリダイレクトするために、ワイヤレス LAN コントローラの ACL を設定します。	—	—

フィールド	EAP-TLS	PEAP	オープン（Open）
発行者パターン	証明書属性。少なくとも1つの属性を、インストールされた証明書属性に一致する、発行者パターンまたはサブジェクトパターンから選択してください。証明書を受け入れるように Chromebook デバイスに一致する証明書属性を指定します。 • 共通名：証明書のサブジェクトフィールド、またはノードのFQDNと一致している必要がある証明書のサブジェクトフィールドのワイルドカード ドメインを参照します。 • 地域：証明書のサブジェクトに関連するテスト地域（市）を参照してください。 • 組織：証明書のサブジェクトに関連する組織名を参照します。 • 組織単位：証明書のサブジェクトに関連する組織単位の名前を参照します。	—	—

フィールド	EAP-TLS	PEAP	オープン（Open）
サブジェクトパターン	証明書属性。少なくとも1つの属性を、インストールされた証明書属性に一致する、発行者パターンまたはサブジェクトパターンから選択してください。証明書を受け入れるように Chromebook デバイスに一致する証明書属性を指定します。 • 共通名：証明書のサブジェクトフィールド、またはノードのFQDNと一致している必要がある証明書のサブジェクトフィールドのワイルドカード ドメインを参照します。 • 地域：証明書のサブジェクトに関連するテスト地域（市）を参照してください。 • 組織：証明書のサブジェクトに関連する組織名を参照します。 • 組織単位：証明書のサブジェクトに関連する組織単位の名前を参照します。	—	—

フィールド	EAP-TLS	PEAP	オープン（Open）
プロキシの設定	• インターネットへの直接接続（選択済み） • 手動でのプロキシ設定 • 自動でのプロキシ設定	• インターネットへの直接接続（選択済み） • 手動でのプロキシ設定 • 自動でのプロキシ設定	—
ネットワークの適用	By User	By User	—

Cisco ISE での Chromebook デバイス アクティビティのモニタ

Cisco ISE は Chromebook のデバイスの認証と認可に関する情報を表示するさまざまなレポートとログを提供します。オン デマンドまたは定期的にこれらのレポートを実行できます。[操作（Operations）] > [RADIUS] > [ライブ ログ（Live Logs）] ページで、認証方法（たとえば、802.1x）と認証プロトコル（たとえば、EAP-TLS）を表示することができます。また、[ワークセンター（Work Center）] > [ネットワーク アクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）] ページに移動して、Chromebook デバイスとして分類されたエンドポイントの数も識別できます。

オンボーディング中の Chromebook デバイスのトラブルシューティング

このセクションでは、Chromebook デバイスのオンボーディング中に発生する可能性のある問題について説明します。

- エラー：webstore から拡張をインストールできない：webstore から拡張をインストールできません。これは、ネットワーク管理者によって Chromebook デバイスに自動的にインストールされます。
- エラー：証明書のインストールを完了したが、セキュアなネットワークに接続できない：管理コンソールで、インストールした証明書が定義された発行者とサブジェクトの属性パターンと一致していることを確認します。以下からインストールされた証明書に関する情報を得ることができます。chrome://settings/certificates
- エラー：Chromebook でセキュアなネットワークに手動で接続しようとして、「ネットワーク証明書の取得（Obtain Network Certificate）」のエラー メッセージが表示される：[新しい証明書の取得（Get New Certificate）] をクリックしてブラウザを開き、証明書をインストールする ISE BYOD にリダイレクトされます。ただし、セキュアなネットワークに接続できない場合は、管理コンソールで、インストールされた証明書が定義された発行者とサブジェクトの属性パターンと一致していることを確認します。

- エラー：[新しい証明書の取得（Get New Certificate）] をクリックしたが、www.cisco.com に転送される：ユーザはISEにリダイレクトされ、証明書のインストールプロセスを開始するために、プロビジョニングするSSIDに接続する必要があります。適切なアクセス リストがこのネットワーク用に定義されていることを確認します。
- エラー：エラーメッセージ「管理対象デバイスのみがこの拡張を使用できます。ヘルプデスクまたはネットワーク管理者にお問い合わせください（Only managed devices can use this extension. Contact helpdesk or network administrator）」が表示される：Chromebookは管理対象デバイスであり、デバイスで証明書をインストールするには、拡張は、Chrome OS APIにアクセスするために強制インストールとして設定する必要があります。拡張は、Google Webストアからダウンロードして手動でインストールすることもできますが、登録されていないChromebookユーザは証明書をインストールすることはできません。

  登録されていないChromebookデバイスは、ユーザがドメインユーザ グループに属する場合に証明書を保護できます。拡張はデバイスのドメインユーザを追跡します。ただし、ドメイン ユーザは登録されていないデバイスのユーザ単位の認証キーを生成できます。
- エラー：Google の管理コンソールで SSID が接続された順番が不明：
  - いくつかの SSID（PEAP、および EAP-TLS）が Google の管理コンソールで設定された場合、証明書がインストールされ、属性が一致すると、Chrome OS は SSID が設定された順序にかかわらず、証明書ベースの認証を使用して SSID に自動的に接続します。
  - 2つのEAP-TLS SSIDが同じ属性で一致した場合、接続は、信号強度や他のネットワーク レベルの信号などの、ユーザまたは管理者で制御できないその他の要因に依存します。
  - 複数のEAP-TLSの証明書がChromebookデバイスにインストールされ、そのすべてが管理コンソールで設定された証明書パターンと一致した場合、一番新しい証明書が接続に使用されます。

Cisco AnyConnect セキュア モビリティ

Cisco ISE は、Cisco ISE ポスチャ要件の AnyConnect で統合モジュールを使用します。

（注） Cisco AnyConnect は CWA フローをサポートしていません。[ワークセンター（Work Centers）] の [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）][設定（Configure）]>[ゲストポータル（Guest Portals）] >[作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ゲストデバイスのコンプライアンス設定（Guest Device Compliance Settings）] ページの [ゲスト デバイス コンプライアンスが必要（Require guest device compliance）] フィールドを使用してゲストポータルから AnyConnect をプロビジョニングすることはできません。代わりに、クライアント プロビジョニング ポータルで AnyConnect をプロビジョニングします。この方法を使用すると、許可権限で設定されているようにリダイレクションが実行されます。

（注） ネットワークのメディアを切り替えるときに、AnyConnect ISE ポスチャモジュールが変更後のネットワークを検出し、クライアントを再評価するように、デフォルトのゲートウェイを変更する必要があります。

Cisco ISE を AnyConnect エージェントと統合すると、Cisco ISE は次のように機能します。

- AnyConnect のバージョン 4.0 および以降のリリースを展開するためのステージングサーバとして機能する
- Cisco ISE ポスチャ要件の AnyConnect ポスチャコンポーネントとやり取りする
- AnyConnect プロファイル、カスタマイズおよび言語パッケージ、および Windows と Mac OS X の各オペレーティングシステムの OPSWAT のライブラリ更新の展開をサポートする
- AnyConnect およびレガシー エージェントを同時にサポートします

AnyConnect 設定の作成

AnyConnect 設定には、AnyConnect ソフトウェアおよび関連するコンフィギュレーション ファイルが含まれます。この設定は、ユーザがクライアントで AnyConnect リソースをダウンロードしてインストールできるクライアントプロビジョニングポリシーで使用できます。AnyConnect を展開するために ISE および ASA を使用した場合、設定は両方のヘッドエンドで一致する必要があります。

（注） VPN に接続するときに ISE ポスチャ モジュールをプッシュするには、シスコの Adaptive Security Device Manager（ASDM）GUI ツールを使用する Cisco 適応型セキュリティ アプライアンス（ASA）を使用して AnyConnect エージェントをインストールすることをお勧めします。ASA は、VPN ダウンローダを使用してインストールを行います。ダウンロードでは、ISE ポスチャ プロファイルは ASA によってプッシュされ、後続のプロファイルのプロビジョニングに必要なホスト検出が利用可能になってから、ISE ポスチャ モジュールが ISE に接続します。その一方、ISE では、ISE ポスチャ モジュールは ISE が検出された後にのみプロファイルを取得し、これがエラーの原因になることがあります。したがって、VPN に接続するとき ASA を ISE ポスチャ モジュールにプッシュすることを推奨します。

始める前に

AnyConnect 設定オブジェクトを設定する前に、次の手順を実行する必要があります。

1. Cisco ソフトウェアのダウンロードページから AnyConnect ヘッドエンド展開パッケージとコンプライアンスモジュールをダウンロードします。
2. これらのリソースを Cisco ISE にアップロードします（ローカル マシンからのシスコ提供のクライアント プロビジョニング リソースの追加 （100 ページ）を参照）。
3. （任意）カスタマイズおよびローカライズのバンドルを追加します（ローカルマシンからの AnyConnect 用の顧客作成リソースの追加 （101 ページ）を参照）。
4. AnyConnect のポスチャ エージェント プロファイルを設定します（ポスチャ エージェント プロファイルの作成 （127 ページ）を参照）。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョン（Client Provision）] > [リソース（Resources）]** を選択します。

ステップ 2 [追加（Add）] をクリックして、AnyConnect 設定を作成します。

ステップ 3 [AnyConnect 設定（AnyConnect Configuration）] を選択します。

ステップ 4 以前にアップロードした AnyConnect パッケージを選択します。たとえば、AnyConnectDesktopWindows xxx.x.xxxxx.x を選択します。

ステップ 5 現在の AnyConnect 設定の名前を入力します。たとえば、AC Config xxx.x.xxxxx.x とします。

ステップ 6 以前にアップロードしたコンプライアンス モジュールを選択します。たとえば、AnyConnectComplianceModulewindows x.x.xxxx.x を選択します。

ステップ 7 1 つ以上の AnyConnect モジュールのチェックボックスをオンにします。たとえば、ISE ポスチャ、VPN、ネットワーク アクセス マネージャ、Web セキュリティ、AMP イネーブラ、ASA ポスチャ、Start Before Log on（Windows OS のみ）、Diagnostic and Reporting Tool の中から、1 つ以上のモジュールを選択します。

（注） [AnyConnect モジュール選択（AnyConnect Module Selection）] で VPN モジュールをオフにしても、プロビジョニングされたクライアントの VPN タイルは無効になりません。AnyConnect GUI の VPN タイルを無効にするには、VPNDisable_ServiceProfile.xml を設定する必要があります。AnyConnect がデフォルトの場所にインストールされているシステムでは、このファイルは C:\Program Files\Cisco にあります。AnyConnect が別の場所にインストールされている場合、このファイルは <AnyConnect がインストールされているパス>\Cisco にあります。

ステップ 8 選択した AnyConnect モジュール用の AnyConnect プロファイルを選択します。たとえば、ISE ポスチャ、VPN、NAM および Web セキュリティを選択します。

ステップ 9 AnyConnect カスタマイズ バンドルおよびローカリゼーション バンドルを選択します。

ステップ 10 [送信（Submit）] をクリックします。

ポスチャ エージェント プロファイルの作成

AnyConnect ポスチャのエージェント プロファイルを作成するには、次の手順を実行します。このプロファイルでは、ポスチャ プロトコルのエージェントの動作を定義するパラメータを指定できます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [AnyConnect ポスチャプロファイル（AnyConnect Posture Profile）] を選択します。

ステップ 4 プロファイルの [名前（Name）] に入力します。

ステップ 5 次のパラメータを設定します。

- Cisco ISE ポスチャ エージェントの動作
- クライアント IP アドレスの変更
- Cisco ISE ポスチャ プロトコル

ステップ 6 [送信（Submit）] をクリックします。

クライアント IP アドレスのリフレッシュ設定

次の表に、VLAN の変更後に IP アドレスをリフレッシュするようにクライアントのパラメータを設定できる [NAC AnyConnect ポスチャ プロファイル（NAC AnyConnect Posture Profile）] ページのフィールドを示します。このページへのナビゲーションパスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）] > [追加（Add）] > [NAC または AnyConnect

ポスチャプロファイル（NAC or AnyConnect Posture Profile）][NAC または AnyConnect ポスチャプロファイル（NAC or AnyConnect Posture Profile）] です。

フィールド	デフォルト値（Default Value）	使用上のガイドライン
VLAN 検出間隔（VLAN detection interval）	0、5	この設定は、エージェントが VLAN 変更をチェックする間隔です。 Mac OS X エージェントの場合、デフォルト値は 5 です。Mac OS X のデフォルトでは、認証 VLAN 変更機能へのアクセスは、VlanDetectInteval を 5 秒として有効になっています。有効な範囲は 5 ～ 900 秒です。 0：認証 VLAN 変更機能へのアクセスは無効化されます。 1 ～ 5：エージェントはインターネット制御メッセージ プロトコル（ICMP）またはアドレス解決プロトコル（ARP）クエリーを 5 秒ごとに送信します。 6 ～ 900：ICMP/ARP クエリーが x 秒ごとに送信されます。
UI なしの VLAN 検出の有効化（Enable VLAN detection without UI）（Mac OS X クライアントには適用できません）	なし	この設定は、ユーザがログインしていないときでも VLAN 検出を有効または無効にします。 No：VLAN 検出機能は無効です。 Yes：VLAN 検出機能が有効です。

フィールド	デフォルト値（Default Value）	使用上のガイドライン
再試行検出数（Retry detection count）	3	インターネット制御メッセージプロトコル（ICMP）またはアドレス解決プロトコル（ARP）ポーリングが失敗する場合、この設定で、クライアント IP アドレスをリフレッシュする前に x 回再試行するようにエージェントを設定します。
Ping または ARP（Ping or ARP）	[0] 有効な範囲は 0 ～ 2 です。	この設定は、クライアント IP アドレスの変更を検出するために使用する方式を指定します。 0：ICMP を使用してポーリング 1：ARP を使用してポーリング 2：最初に ICMP を使用し、（ICMP が失敗した場合は）ARP を使用してポーリング
ping の最大タイムアウト（Maximum timeout for ping）	1 有効な値の範囲は 1 ～ 10 秒です。	ICMP を使用してポーリングし、指定した時間内に応答がない場合は、ICMP ポーリングの失敗を宣言します。
エージェント IP のリフレッシュの有効化（Enable agent IP refresh）	Yes（デフォルト）	この設定は、スイッチ（または WLC）が各スイッチポートでクライアントのログインセッション用 VLAN を変更した後にクライアント マシンが IP アドレスをリフレッシュするかどうかを指定します。
DHCP 更新遅延（DHCP renew delay）	[0] 有効な値の範囲は 0 ～ 60 秒です。	この設定は、ネットワーク DHCP サーバからの新しい IP アドレスの要求を試行する前に、クライアント マシンが待機するように指定します。

フィールド	デフォルト値（Default Value）	使用上のガイドライン
DHCP リリース遅延（DHCP release delay）	[0] 有効な値の範囲は 0 ～ 60 秒です。	この設定は、現在の IP アドレスをリリースする前にクライアント マシンが待機するように指定します。

（注） パラメータ値は、既存のエージェントプロファイル設定とマージするか、または上書きして、Windows および Mac OS X クライアントで適切に IP アドレスがリフレッシュされるように設定します。

ポスチャ プロトコル設定

次の表に、Cisco ISE で AnyConnect のポスチャプロトコル設定を設定できる [AnyConnectのポスチャプロファイル（NAC or AnyConnect Posture Profile）] ページのフィールドを示します。Anyconnect のポスチャ プロトコル設定のその他のフィールドについては、お使いのバージョンの AnyConnect の『Cisco AnyConnect Secure Mobility Client Administrator Guide』を参照してください。

フィールド	デフォルト値（Default Value）	使用上のガイドライン
[Call Home リスト（Call Home List）]	—	IP アドレスとポートをコロンで結んだカンマ区切りリストを入力します。
[バックオフ タイマー（Back-off Timer）]	30 秒	この設定により、Anyconnect エージェントは最大時間制限に達するまでディスカバリ パケットを送信することで、ディスカバリ ターゲット（リダイレクション ターゲットおよび以前に接続していた PSN）に継続的に到達できます。有効な値の範囲は 10 ～ 600 秒です。

継続的なエンドポイント属性モニタリング

ポスチャ アセスメントの実行中に動的な変更が確認されるようにするため、AnyConnect エージェントを使用してさまざまなエンドポイント属性を継続的にモニタします。これによりエンドポイントの全体的な可視性が向上し、動作に基づいてポスチャ ポリシーを作成できるようになります。AnyConnect エージェントは、エンドポイントにインストールされ実行されている

アプリケーションをモニタします。この機能をオンまたはオフにできます。また、データのモニタ頻度を設定できます。デフォルトでは、データは5分間隔で収集され、データベースに保存されます。初回ポスチャでは、AnyConnectがすべての実行中アプリケーションとインストールされているアプリケーションのリストを報告します。初回ポスチャの後に、AnyConnectエージェントはX分間隔でアプリケーションをスキャンし、最終スキャンでの差異をサーバに送信します。サーバはすべての実行中アプリケーションとインストールされているアプリケーションのリストを表示します。

Cisco Web Agent

Cisco Web Agent では、クライアント マシンのための一時的なポスチャ評価を提供します。

ユーザは Cisco Web Agent 実行ファイルを起動することができ、ActiveX コントロールまたは Java アプレットによって、クライアント マシンの一時ディレクトリに Web Agent ファイルがインストールされます。

Cisco Web Agent は、ユーザがログインすると、ユーザ ロールまたはオペレーティング システムに設定された要件を Cisco ISE サーバから取得し、必要なパッケージのホスト レジストリ、プロセス、アプリケーション、およびサービスをチェックし、レポートを Cisco ISE サーバに送信します。クライアントマシンに関する要件が満たされている場合、ユーザはネットワークにアクセスできます。要件が満たされていない場合、Web Agent は満たされていない要件ごとに、ユーザにダイアログを表示します。ダイアログにより、クライアントマシンの要件を満たすための手順および対処法が提供されます。あるいは、指定された要件が満たされない場合は、ユーザ ログイン ロールの要件を満たすようにクライアント システムの修復試行中は制限付きのネットワーク アクセスを受け入れるという選択もできます。

（注） ActiveX は 32 ビット版の Internet Explorer でのみサポートされます。Firefox Web ブラウザまたは 64 ビット版の Internet Explorer のバージョンでは、ActiveX をインストールできません。

クライアント プロビジョニング リソース ポリシーの設定

クライアントの場合、どのユーザがリソース（エージェント、エージェント コンプライアンス モジュール、エージェント カスタマイズ パッケージ/プロファイル）のどのバージョン（または複数のバージョン）をログイン時およびユーザ セッション開始時に Cisco ISE から受信するかは、クライアント プロビジョニング リソース ポリシーによって決定されます。

AnyConnectの場合、クライアント プロビジョニング リソース ページからリソースを選択し、クライアント プロビジョニング ポリシー ページで使用できる AnyConnect 設定を作成することができます。AnyConnect 設定は、AnyConnect ソフトウェアとそのさまざまなコンフィギュレーション ファイルとの関連付けであり、これらのファイルには、Windows および Mac OS X

クライアントの AnyConnect バイナリ パッケージ、コンプライアンス モジュール、モジュール プロファイル、AnyConnect のカスタマイズおよび言語パッケージなどがあります。

始める前に

- 有効なクライアント プロビジョニング リソース ポリシーを作成する前に、Cisco ISE にリソースを追加したことを確認します。エージェント コンプライアンス モジュールをダウンロードすると、システムで使用している既存のモジュールがあれば常にそれが上書きされます。
- クライアント プロビジョニング ポリシーで使用されているネイティブのサプリカント プロファイルをチェックして、ワイヤレス SSID が正しいことを確認します。iOS デバイスの場合、接続対象ネットワークが非表示の場合は、[iOSの設定（iOS Settings）] エリアで [ターゲットネットワークが非表示になっている場合に有効にする（Enable if target network is hidden）] チェック ボックスをオンにします。
- 証明書属性に基づく条件を含むクライアント プロビジョニング ルールについては、「証明書ベースの条件のための前提条件」のセクションを参照してください。

ステップ 1 **[ポリシー（Policy）]** > **[クライアント プロビジョニング（Client Provisioning）]** を選択します。

ステップ 2 動作のドロップダウン リストから **Enable**、**Disable**、または **Monitor** を選択します。

- **Enable**：ユーザがネットワークにログインし、クライアントプロビジョニングポリシーのガイドラインに従っている場合に、Cisco ISE がこのポリシーを使用して、クライアントプロビジョニング機能を果たすようにします。
- **Disable**：Cisco ISE は、指定されたリソース ポリシーを使用せずにクライアント プロビジョニング機能を果たします。
- **Monitor**：ポリシーを無効にし、クライアント プロビジョニング セッション要求を監視し、Cisco ISE が [モニタ対象（Monitored）] のポリシーに基づいて起動しようとした回数を確認します。

ステップ 3 [ルール名（Rule Name）] テキスト ボックスに、新しいリソース ポリシーの名前を入力します。

ステップ 4 Cisco ISE にログインするユーザが属する ID グループを 1 つ以上指定します。

設定した既存の ID グループのリストから、あらゆる ID タイプを指定することも、1 つ以上のグループを選択することもできます。

ステップ 5 [オペレーティング システム（Operating Systems）] フィールドを使用して、ユーザが Cisco ISE にログインする際に使用するクライアント マシンまたはデバイスで動作している 1 つ以上のオペレーティング システムを指定します。

[Android]、[Mac iOS]、[Mac OS X] などの単一のオペレーティング システムや、[Windows XP（すべて）（Windows XP (All)）] や [Windows 7（すべて）（Windows 7 (All)）] など、複数のクライアント マシン オペレーティング システムに対応する包括的なオペレーティング システムの指定を選択できます。

（注） Cisco ISE GUI のクライアント プロビジョニング ポリシー ページに、MAC OS 10.6/10.7/10.8 を選択できるオプションがありますが、これらのバージョンは AnyConnect ではサポートされていません。

ステップ 6 [その他の条件（Other Conditions）] フィールドで、この特定のリソース ポリシー用に作成する新しい式を指定します。

ステップ 7 クライアント マシンの場合は、[エージェント設定（Agent Configuration）] を使用して、クライアント マシンで利用可能にし、プロビジョニングするエージェント タイプ、コンプライアンス モジュール、エージェント カスタマイズ パッケージ/プロファイルを指定します。

クライアントマシンでエージェントがポップアップできるようにするには、クライアントプロビジョニングの URL を許可ポリシーに含める必要があります。これにより、ランダムなクライアントからの要求が回避され、適切なリダイレクト URL を持つクライアントのみがポスチャ評価を要求できるようになります。

ステップ 8 **Save** をクリックします。

次のタスク

1 つ以上のクライアント プロビジョニング リソース ポリシーを正常に設定したら、ログイン中にクライアント マシンのポスチャ評価を実行するように Cisco ISE の設定を開始できます。

クライアント プロビジョニング ポリシーの Cisco ISE ポスチャ エージェントの設定

クライアントマシンについては、エージェントタイプ、コンプライアンスモジュール、エージェント カスタマイズ パッケージ/プロファイルを、ユーザがクライアントマシンにダウンロードおよびインストールできるように設定します。

始める前に

Cisco ISE の AnyConnect のクライアント プロビジョニング リソースを追加している必要があります。

ステップ 1 **Agent** ドロップダウン リストから使用可能なエージェントを選択し、ここで定義したエージェントのアップグレード（ダウンロード）がクライアント マシンに対して必須かどうかを、**Is Upgrade Mandatory** オプションを必要に応じて有効または無効にすることによって指定します。

Is Upgrade Mandatory 設定は、エージェントのダウンロードにのみ適用されます。エージェント プロファイル、コンプライアンス モジュール、およびエージェント カスタマイズ パッケージの更新は常に必須です。

ステップ 2 **Profile** ドロップダウン リストから既存のエージェント プロファイルを選択します。

ステップ 3 **Compliance Module** ドロップダウン リストを使用して使用可能なコンプライアンス モジュールを選択し、クライアント マシンにダウンロードします。

ステップ 4 **Agent Customization Package** ドロップダウン リストから、クライアント マシンに使用可能なエージェント カスタマイズ パッケージを選択します。

パーソナル デバイスのネイティブ サプリカントの設定

従業員は、Windows、Mac OS、iOS、および Android デバイスで使用可能なネイティブ サプリカントを使用して、ネットワークに自分のパーソナルデバイスを直接接続できます。パーソナル デバイスに関して、登録されているパーソナル デバイスで使用可能にし、プロビジョニングするネイティブ サプリカントの設定を指定します。

始める前に

ユーザがログインするとき、そのユーザの許可要件と関連付けるプロファイルに基づいて、Cisco ISE が、ユーザのパーソナル デバイスを設定するために必要なサプリカント プロビジョニング ウィザードを提供して、ネットワークにアクセスするように、ネイティブ サプリカント プロファイルを作成します。

ステップ 1 **[ポリシー（Policy）] > [クライアント プロビジョニング（Client Provisioning）]** を選択します。

ステップ 2 動作のドロップダウン リストから **Enable**、**Disable**、または **Monitor** を選択します。

ステップ 3 [ルール名（Rule Name）] テキスト ボックスに、新しいリソース ポリシーの名前を入力します。

ステップ 4 次を指定します。

- [ID グループ（Identity Groups）] フィールドを使用して、Cisco ISE にログインするユーザが属する ID グループを 1 つ以上指定します。
- [オペレーティング システム（Operating System）] フィールドを使用して、ユーザが Cisco ISE にログインする際に使用するパーソナル デバイスで動作している 1 つ以上のオペレーティング システムを指定します。
- [その他の条件（Other Conditions）] フィールドを使用して、この特定のリソース ポリシー用に作成する新しい式を指定します。

ステップ 5 パーソナル デバイスの場合、[ネイティブサプリカントの設定（Native Supplicant Configuration）] を使用し、特定の**Configuration Wizard**を選択して、パーソナル デバイスに配信します。

ステップ 6 指定されたパーソナル デバイス タイプに適用可能な **Wizard Profile** を指定します。

ステップ 7 [保存（Save）] をクリックします。

クライアント プロビジョニング レポート

Cisco ISE のモニタリングおよびトラブルシューティング機能にアクセスし、ユーザ ログイン セッションの成功または失敗の全体のトレンドをチェックし、特定の期間にネットワークにロ

グインしたクライアントマシンの数およびタイプに関する統計情報を収集し、また、クライアント プロビジョニング リソースでの最近の設定変更をチェックすることができます。

クライアント プロビジョニングの要求

[操作（Operations）] > [レポート（Reports）] > [ISE レポート（ISE Reports）] > [エンドポイントおよびユーザ（Endpoints and Users）] > [クライアント プロビジョニング（Client Provisioning）] レポートには、クライアント プロビジョニング要求の成功および失敗に関する統計情報が表示されます。**Run** を選択していずれかのプリセット期間を指定すると、Cisco ISE によってデータベースが調べられ、生成されたクライアント プロビジョニング データが表示されます。

サプリカント プロビジョニングの要求

[操作（Operations）] > [レポート（Reports）] > [ISE レポート（ISE Reports）] > [エンドポイントおよびユーザ（Endpoints and Users）] > [サプリカント プロビジョニング（Supplicant Provisioning）] ウィンドウには、最近の成功および失敗したユーザ デバイス登録およびサプリカント プロビジョニング要求に関する情報が表示されます。**Run** を選択していずれかのプリセット期間を指定すると、Cisco ISE によってデータベースが調べられ、生成されたサプリカント プロビジョニング データが表示されます。

サプリカント プロビジョニング レポートは、特定の期間にデバイス登録ポータルから登録されたエンドポイントのリストに関する情報が提供されます。これには、ログイン日時、ID（ユーザ ID）、IP アドレス、MAC アドレス（エンドポイント ID）、サーバ プロファイル、エンドポイント オペレーティング システム、SPW バージョン、障害理由（ある場合）、登録のステータスなどのデータが含まれます。

クライアント プロビジョニング イベント ログ

クライアントの動作の問題の診断に役立つイベント ログ エントリを検索できます。たとえば、ネットワーク上のクライアント マシンがログイン時にクライアント プロビジョニング リソースの更新を取得できないという問題の原因を特定する必要がある場合があります。ポスチャおよびクライアント プロビジョニングの監査、ポスチャおよびクライアント プロビジョニングの診断のロギング エントリを使用できます。

クライアントプロビジョニングポータルのポータル設定

これらの設定へのナビゲーション パスは、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [クライアント プロビジョニング ポータル（Client Provisioning Portals）] > [作成、編集、複製または削除（Create, Edit, Duplicate, or Delete）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]** です。

ポータル設定

- HTTPS ポート（HTTPS Port）：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合、この制限に従うようにポート設定を変更する必要があります。
- 使用可能インターフェイス（Allowed interfaces）：ポータルを実行できる PSN インターフェイスを選択します。PSN で使用可能なインターフェイスを備えた PSN のみがポータルを作成できます。物理およびボンディングされたインターフェイスの任意の組み合わせを設定できます。これは PSN 全体の設定です。すべてのポータルはこれらのインターフェイスでのみ動作し、このインターフェイス設定はすべての PSN に適用されます。
  - 異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。
  - ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名とサブジェクトの代替名は、インターフェイス IP に解決される必要があります。
  - ISE CLI の ip host x.x.x.x yyy.domain.com をセカンダリ インターフェイス IP と FQDN をマッピングするように設定します。これは証明書のサブジェクト名/サブジェクトの代替名を一致させるために使用されます。
  - ボンディングされた NIC のみが選択されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスを設定しようとします。これが成功しない場合、その PSN にボンド セットがなかったことが原因である可能性があるので、PSN はエラーを記録して終了します。物理インターフェイスでポータルを開始しようとはしません。
  - **NIC チーミング**またはボンディングは、高可用性（耐障害性）のために 2 つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
    - 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSN は物理インターフェイスでポータルを開始しようとします。
- 証明書グループ タグ（Certificate group tag）：ポータルの HTTPS トラフィックに使用する証明書グループのグループ タグを選択します。

- [認証方式（Authentication Method）]：ユーザ認証に使用する ID ソース順序（ISS）または ID プロバイダー（IdP）を選択します。ISS は、ユーザ クレデンシャルを確認するために順番に検索される ID ストアのリストです。たとえば、内部ゲスト ユーザ、内部ユーザ、Active Directory、LDAP などがあります。

  Cisco ISE には、クライアント プロビジョニング ポータル用のデフォルトのクライアント プロビジョニング ID ソース順序 Certificate_Portal_Sequence が含まれています。

- 完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）：クライアント プロビジョニング ポータル用に少なくとも 1 つの一意の FQDN、ホスト名、またはその両方を入力します。たとえば、「provisionportal.yourcompany.com」と入力した場合、ユーザはこれらのいずれかをブラウザに入力して証明書プロビジョニング ポータルに到達できます。

  - DNS を更新して、新しい URL の FQDN が有効なポリシー サービス ノード（PSN）の IP アドレスに確実に解決するようにします。PSN のプールを提供するロード バランサの仮想 IP アドレスを指定することもできます。

  - 名前の不一致による証明書の警告メッセージを回避するために、Cisco ISE PSN のローカル サーバ証明書のサブジェクト代替名（SAN）属性に、カスタマイズされた URL の FQDN またはワイルドカードを含めます。

（注） URL リダイレクトなしのクライアント プロビジョニングの場合、[完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）] フィールドに入力するポータル名は、DNS 設定で設定されている必要があります。URL リダイレクトなしのクライアント プロビジョニングを有効にするため、この URL をユーザに通知する必要があります。

- アイドル タイムアウト（Idle timeout）：ポータルでアクティビティがない場合にユーザをログアウトするまでに Cisco ISE が待機する時間（分）を入力します。有効な範囲は 1 ～ 30 分です。

（注） クライアント プロビジョニング ポータルではポート番号と証明書を定義できます。これにより、ホストはクライアント プロビジョニングとポスチャに同じ証明書をダウンロードすることを許可します。ポータル証明書が正式な認証局により署名されている場合、セキュリティ警告は表示されません。自己署名証明書の場合、ポータルと Cisco AnyConnect Posture コンポーネントの両方でセキュリティ警告を受け取ります。

ログイン ページの設定（Login Page Settings）

- [ログインの有効化（Enable Login）]：クライアント プロビジョニング ポータルのログイン手順を有効にするには、このチェック ボックスを選択します

- [頻度制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）]：単一のブラウザ セッションからのログイン試行失敗回数を指定します。この回数を超過すると、Cisco ISE はログイン試行を実行できる頻度を意図的に低下させて、追加のログイン試行を防ぎます。ログイン失敗がこの回数に達した後のログイン試行の間隔は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で指定されます。
- [頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）]：[頻度制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）] で定義された回数のログインの失敗後に、ユーザが再度ログインを試行するまでに待機する必要がある時間を分単位で設定します。
- [AUP をページに含める/AUP をリンクとして含める（Include an AUP (on page/as link)）]：会社のネットワーク使用の諸条件を、現在ユーザに表示されるページ上のテキストとして、または AUP テキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。
- [同意が必要（Require acceptance）]：ポータルにアクセスする前にユーザが AUP を受け入れることを要求します。[ログイン（Login）] ボタンは、ユーザが AUP を受け入れない場合は有効になりません。AUP を受け入れないユーザは、ポータルにアクセスできません。
- [AUP の最後までのスクロールが必要（Require scrolling to end of AUP）]：[AUP をページに含める（Include an AUP on page）] を有効にした場合にのみ、このオプションが表示されます。ユーザが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。

利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）

- [AUP を含める（Include an AUP）]：会社のネットワーク使用諸条件を、別のページでユーザに表示します。
- [AUP の最後までのスクロールが必要（Require scrolling to end of AUP）]：ユーザが AUP を完全に読んだことを確認します。[同意（Accept）] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。
- [初回のログインのみ（On first login only）]：ユーザがネットワークまたはポータルに初めてログインしたときのみ、AUP を表示します。
- [ログインごと（On every login）]：ユーザがネットワークまたはポータルにログインするごとに、AUP を表示します。
- [_ 日ごと（初回のログインから）（Every _____ days (starting at first login)）]：ネットワークやポータルにユーザが初めてログインした後は、AUP を定期的に表示します。

ポストログイン バナー ページ設定（Post-Login Banner Page Settings）

[ポストログイン バナー ページを含める（Include a Post-Login Banner page）]：ユーザが正常にログインした後、ネットワーク アクセスを付与される前に追加情報を表示します。

パスワード変更設定（Change Password Settings）

[内部ユーザに自身のパスワードの変更を許可する（Allow internal users to change their own passwords）]：従業員がクライアントプロビジョニング ポータルにログインして、自分のパスワードを変更できるようにします。これは、アカウントが Cisco ISE データベース保存されている従業員に適用され、Active Directory や LDAP などの外部データベースに保存されている場合には適用されません。

関連トピック

クライアント プロビジョニング ポータル
クライアント プロビジョニング ポータルの作成
クライアント プロビジョニング ポータルの言語ファイルの HTML サポート

クライアントプロビジョニングポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト（Instructional Text）]、[コンテンツ（Content）]、[任意のコンテンツ 1（Optional Content 1）]、および [任意のコンテンツ 2（Optional Content 2）] テキスト ボックスへのナビゲーション パスは、**[管理（Administration）]** > **[デバイス ポータル管理（Device Portal Management）]** > **[クライアント プロビジョニング ポータル（Client Provisioning Portals）]** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** > **[ページ（Pages）]** です。テキスト ボックスのミニ エディタの [HTML ソースの表示（View HTML Source）] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。

（注） これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.guest.ui_client_provision_agent_installed_instructions_without_java_message
- key.guest.ui_contact_instruction_message
- key.guest.ui_success_message
- key.guest.ui_client_provision_unable_to_detect_message
- key.guest.ui_client_provision_instruction_message
- key.guest.ui_client_provision_agent_installation_message
- key.guest.ui_client_provision_posture_agent_check_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_client_provision_agent_installation_instructions_with_no_java_message
- key.guest.ui_success_instruction_message

- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_contact_optional_content_1
- key.guest.ui_client_provision_posture_check_compliant_message
- key.guest.ui_client_provision_optional_content_2
- key.guest.ui_client_provision_optional_content_1
- key.guest.ui_error_optional_content_2
- key.guest.ui_error_optional_content_1
- key.guest.ui_client_provision_posture_check_non_compliant_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_client_provision_posture_agent_scan_message