コンプライアンス

ポスチャ タイプ

次のポスチャエージェントは、Cisco ISE ポスチャポリシーをモニターおよび適用します。

- **[AnyConnect]**：AnyConnect エージェントを展開し、クライアントによるデータのやり取りが必要な Cisco ISE ポスチャポリシーを監視し、適用します。AnyConnect エージェントはクライアントに残ります。Cisco ISE での AnyConnect の使用に関する詳細については、「Cisco AnyConnect セキュアモビリティ （136 ページ）」を参照してください。

- **[AnyConnectステルス（AnyConnect Stealth）]**：ユーザーインターフェイスなしで、サービスとしてポスチャを実行します。エージェントはクライアント上に残ります。

  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）] ウィンドウにマッピングする場合、次の処理がサポートされます。

- AnyConnect はポスチャプロファイルを読み取り、必要なモードを設定することができます。
- AnyConnect は初回ポスチャ要求時に選択したモードに関する情報を Cisco ISE へ送信できます。
- Cisco ISE は、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）に基づいて正しいポリシーを照合します。

（注） AnyConnect ステルスモードを使用するには、AnyConnect バージョン 4.4 以降が必要です。

Cisco ISE での AnyConnect ステルスの設定の詳細については、AnyConnect ステルスモードのワークフローの設定 （97 ページ）を参照してください。

- [一時エージェントTemporal Agent]：クライアントが信頼できるネットワークにアクセスしようとすると、Cisco ISE は [クライアント プロビジョニング（Client Provisioning）] ポータルを開きます。ポータルから、エージェントをダウンロードしてインストールし、エージェントを実行するようにユーザーに指示が出されます。一時エージェントはコンプライアンスステータスを確認し、そのステータスを Cisco ISE に送信します。Cisco ISE は結果に基づいて動作します。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自体が削除されます。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。

  一時エージェントは、次の条件をサポートしていません。

  - 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ー 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
  - [ポスチャタイプ（Posture Types）]、[一時エージェント（Temporal Agent）]、[コンプライアンスモジュール（Compliance Module）]、[4.x 以降（4.x or later）] を使用して、ポスチャポリシーを設定します。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**として設定しないでください。
  - 一時エージェントの場合は、[要件（Requirements）] ウィンドウで [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、MacOS 向け一時エージェントを使用した VLAN 制御ポスチャをサポートしていません。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、VLAN が変更される前にユーザーの IP アドレスが解放されます。ユーザーが新しい VLAN に接続すると、クライアントは DHCP によって新しい IP アドレスを取

得します。新しいIPアドレスを認識するにはルート権限が必要ですが、一時エージェントはユーザー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。
- Cisco ISE での一時エージェントの設定の詳細については、Cisco Temporal Agent のワークフローの設定 （103 ページ）を参照してください。

- [AMP イネーブラ（AMP Enabler）]：AMP イネーブラによって、社内でローカルにホストされているサーバーからエンドポイントのサブセットに AMP for Endpoints ソフトウェアがプッシュされ、AMP サービスが既存のユーザーベースにインストールされます。AMP プロファイラについては、AMP イネーブラ プロファイルの設定 （117 ページ）を参照してください。
- [エージェントレスポスチャ（Agentless Posture）]：エージェントレスポスチャは、クライアントからのポスチャ情報を提供し、終了時に完全に削除します。エンドユーザーによる操作は不要です。一時エージェントとは異なり、エージェントレスポスチャは管理者ユーザーとしてクライアントに接続します。Cisco ISE でのエージェントレスポスチャの使用の詳細については、エージェントレスポスチャ （4 ページ）を参照してください。

[クライアントプロビジョニング（Client Provisioning）] ウィンドウ（**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアントプロビジョニング（Client Provisioning）] > [リソース（Resources）]**）と **[ポスチャ要件（Posture Requirements）]** ウィンドウ（**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [要件（Requirements）]**）でポスチャタイプを選択できます。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）] ウィンドウ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。

関連トピック

AnyConnect ステルスモードのワークフローの設定 （97 ページ）
Cisco Temporal Agent のワークフローの設定 （103 ページ）

エージェントレスポスチャ

エージェントレスポスチャは、クライアントからのポスチャ情報を提供し、完了時にそれ自体を完全に削除します。エンドユーザーによる操作は不要です。

要件

- クライアントは IP アドレスで到達可能であることが必要で、その IP アドレスは RADIUS アカウンティングで使用可能であることが必要です。IPv6 はサポートされていません。
- Windows クライアントと Mac クライアントが現在サポートされています。
  - Windows クライアントの場合、クライアントの PowerShell にアクセスするにはポート 5985 が開いている必要があります。PowerShell はバージョン 5.1 以降である必要があります。クライアントには、cURL バージョン 7.34 以降が必要です。

  - MacOS クライアントの場合、クライアントにアクセスするには SSH にアクセスするポート 22 が開いている必要があります。クライアントには、cURL バージョン 7.34 以降が必要です。

- シェルログイン用のクライアントログイン情報には、ローカル管理者権限が必要です。
- 設定手順の説明に従って、ポスチャフィードの更新を実行して最新のクライアントを取得します。
- エンドポイントでの証明書のインストールが失敗しないようにするため、次のエントリが sudoers ファイルで更新されていることを確認します。

```
<macadminusername> ALL = (ALL) NOPASSWD: /usr/bin/security, /usr/bin/osascript
```

- MacOS の場合、設定するユーザーアカウントは管理者のアカウントである必要があります。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [エンドポイントスクリプト（Endpoint Scripts）] > [ログイン設定（Login Configuration）] > [MAC ローカルユーザー（MAC Local User）]**の順に選択します。MacOS のエージェントレスポスチャは、より多くの権限が付与されているとしても、他のアカウントタイプでは機能しません。
- Microsoft からの更新により Windows クライアントのポート関連のアクティビティが変更された場合は、Windows クライアントのエージェントレスポスチャ設定ワークフローを再設定する必要がある場合があります。

サポートされているポスチャ条件

- ファイル条件（USER_DESKTOP および USER_PROFILE ファイルパスを使用する条件を除く）
- サービス条件（MacOS のシステムデーモンとデーモンまたはユーザーエージェントのチェックを除く）
- アプリケーション条件
- 外部データソース条件
- 複合条件
- マルウェア対策条件
- パッチ管理条件（Enabled および Up To Date 条件チェックを除く）
- ファイアウォール条件
- ディスク暗号化条件（暗号化ロケーションベースの条件チェックを除く）
- レジストリ条件（ルートキーとして HCSK を使用する条件を除く）

サポートされていないポスチャ条件

- 修復

- 猶予期間
- 定期的再評価
- 利用規定

サポート対象のクライアント オペレーティング システム

- Microsoft Windows のバージョン：10
- MacOS のバージョン：10.13、10.14、10.15

エージェントレス ポスチャのプロセスフロー

1. クライアントがネットワークに接続します。
2. Cisco ISE は、クライアントが使用する認証プロファイルでエージェントレスポスチャが有効になっているかどうかを検出します。
3. 有効になっている場合、Cisco ISE がエージェントレス ポスチャ ジョブ要求を Cisco ISE メッセージングキューに送信します。
4. Cisco ISE は、メッセージングキューからジョブを取得し、エージェントレス ポスチャ フローを開始します。
5. Cisco ISE が PowerShell または SSH を介してクライアントに接続します。
6. 証明書がクライアントの信頼できる認証局ストアにない場合、Cisco ISE が証明書をプッシュします。
7. Cisco ISE がクライアント プロビジョニング ポリシーを実行します。
8. Cisco ISE が、エージェントレスプラグインをクライアントにプッシュし、プラグインを起動します。
9. ポスチャ アセスメントがクライアントで実行され、ステータスが Cisco ISE に送信されます。
10. Cisco ISE が、クライアントからエージェントレスプラグインを削除します。ポスチャフローのログは、24 時間、またはクライアントがそれらのログを削除するまで、クライアントに残ります。

エージェントレスポスチャ設定

1. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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、**エージェントレスポスチャを使用して要件を特定する 1 つ以上のポスチャ要件を作成します。
2. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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、**そのポスチャ要件にエージェントレスポスチャを使用する 1 つ以上のサポートされ

ているポスチャポリシールールを作成します。使用する予定のルールを複製し、ポスチャタイプを [エージェントレス（Agentless）] に変更できます。

3. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authorization）] > [認証プロファイル（Authorization Profiles）] を選択し、**エージェントレスポスチャからの結果を評価する認証プロファイルを作成します。
   - 認証プロファイルでエージェントレスポスチャを有効にします。
   - このプロファイルは、エージェントレスポスチャにのみ使用します。他のポスチャタイプには使用しないでください。
   - エージェントレスポスチャには CWA とリダイレクト ACL は必要ありません。VLAN、DACL、または ACL をセグメンテーションルールの一部として使用できます。

4. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）] > [クライアント プロビジョニング（Client Provisioning）] に移動し、**クライアント プロビジョニング ポリシーを追加します。Cisco Agent の設定の場合は、設定したオペレーティングシステムのエージェントレスプラグインを選択します。Windows の場合、プラグインは CiscoAgentlessWindows 4.9.01095 です。MacOS の場合、プラグインは CiscoAgentlessOSX 4.9.01095 です。このルールが確認するポスチャ条件を選択します。Active Directory を使用している場合は、ポリシーで Active Directory グループを使用できます。

（注） MACOSX 10.14 バージョンと10.15 バージョンのエージェントレスポスチャ設定は、ポスチャフィードを更新するまで使用できません。ポスチャフィードを実行する前に、ポスチャフィードの URL を更新します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [設定（Settings）] > [ソフトウェアの更新（Software Updates）] > [ポスチャの更新（Posture Updates）]**の順に選択します。[ポスチャの更新（Posture Updates）] ウィンドウで、[フィードの URL の更新（Update Feed URL）] フィールドに URL（https://www.cisco.com/web/secure/spa/posture-update.xml）を入力し、[今すぐ更新（Update Now）] をクリックします。

5. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）] > [ポリシーセット（Policy Sets）] を選択し、**[認証ポリシー（Authorization Policy）] を展開します。次の 3 つの認証ポリシーを有効にし、設定します。
   - **Unknown_Compliance_Redirect**：結果をエージェントレスポスチャとして Network_Access_Authentication_Passed 条件と Compliance_Unknown_Devices 条件を設定します。
   - **NonCompliant_Devices_Redirect**：結果を DenyAccess として Network_Access_Authentication_Passed 条件と Non_Compliant_Devices 条件を設定します。
   - **Compliant_Devices_Access**：結果を PermitAccess として Network_Access_Authentication_Passed 条件と Compliant_Devices 条件を設定します。

6. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [設定（Settings）] > [エンドポイントスクリプト（Endpoint Scripts）] > [エンドポイントログインの設定（Endpoint Login Configuration）]** をクリックし、クライアントにログオンするためのクライアント資格情報を構成します。これらの同じログイン情報がエンドポイントスクリプトで使用されます。

7. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [設定（Settings）] > [エンドポイントスクリプト（Endpoint Scripts）] > [設定（Settings）] を選択し、**[OS 識別の最大再試行回数（Max retry attempts for OS identification）] と [OS 識別の再試行間の遅延（Delay between retries for OS identification）] を設定します。これらの設定によって、接続の問題をどれだけ迅速に確認できるかが決まります。たとえば、PowerShell ポートが開いていないというエラーがログに表示されるのは、再試行がすべては実行されなかった後のみです。

8. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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、**エージェントレスポスチャを設定します。

9. クライアントがエージェントレスポスチャに接続すると、ライブログでクライアントを確認できます。

デバッグおよびトラブルシューティング

次のデバッグログレベルを有効にします。

- インフラストラクチャ
- クライアント プロビジョニング
- ポスチャ（Posture）

デバッグログは *ise-psc.log* にあります

エージェントレスポスチャのトラブルシューティングは、次の場所にあります。

- Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[操作（Operations）] > [ライブログ（Live Logs）]**：[ポスチャステータス（Posture Status）] 列の下にある 3 つのドットをクリックすると、エージェントレスポスチャのトラブルシューティングが開きます。
- Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断（Diagnostics）] > [一般ツール（General Tools）]**

エージェントレスポスチャのトラブルシューティング

エージェントレス ポスチャ レポートは、エージェントレスポスチャが想定どおりに動作しない場合に使用する主要なトラブルシューティングツールです。このレポートには、スクリプト

アップロードの完了、スクリプトアップロードの失敗、スクリプト実行の完了などのイベントを含む、エージェントレスフローの段階が既知の失敗の理由（ある場合）とともに表示されます。

エージェントレスポスチャのトラブルシューティングには、次の2つの場所からアクセスできます。

- Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、[操作（Operations）] > [ライブログ（Live Logs）] を選択し、トラブルシューティングするクライアントの [ポスチャステータス（Posture Status）] 列にある縦に並んだ3つのドットをクリックします。
- Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断（Diagnostics）] > [一般ツール（General Tools）] > [エージェントレスポスチャのトラブルシューティング（Agentless Posture Troubleshooting）]**の順に選択します。

エージェントレスポスチャのトラブルシューティング ツールは、指定されたクライアントのエージェントレス ポスチャ アクティビティを収集します。[エージェントレス ポスチャ フロー（Agentless Posture Flow）] はポスチャを開始し、現在アクティブなクライアントと Cisco ISE 間のすべてのデータのやり取りを表示します。[クライアントログのみをダウンロード（Only Download Client Logs）] は、クライアントからの最大 24 時間分のポスチャフローを含むログを作成します。クライアントはいつでもログを削除できます。収集が完了したら、ログの ZIP ファイルをエクスポートできます。

レポート

Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、[操作（Operations）] > [レポート（Reports）] > [レポート（Reports）] > [エンドポイントとユーザー（Endpoints and Users）] > [エージェントレスポスチャ（Agentless Posture）] を選択すると、エージェントレスポスチャを実行したすべてのエンドポイントが表示されます。

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 サーバー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 AnyConnectWeb 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アセスメント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ー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、エンドユーザー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. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、[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）] ウィンドウ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。

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	[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 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。 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 （31 ページ）を参照してください。
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 Agent 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]：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ファイル。

フィールド名	使用上のガイドライン
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、ユーザー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。ユーザー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。この要件が欠けていると、Windows クライアントのエージェントは、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。
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。 エージェントユーザーとの通信に使用できるすべての修復タイプ用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エージェントユーザー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、エージェントユーザー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ーに提供されています。このシナリオでは、エージェント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 アセスメントの利用規定の設定 （25 ページ）
クライアントのポスチャ要件の作成 （91 ページ）

クライアントのタイマー設定

ユーザー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を設定し、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に対してすべてのタイマーを設定できます。

ただし、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）] 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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[ポスチャ（Posture）]** > **[全般設定（General Settings）]**の順に選択します。

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]**の順に選択します。

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

ポスチャアセスメント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。ユーザーはログイン 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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]**の順に選択します。

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

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 デバイスや iPod、iPhone、iPad などの Apple のデバイスが Cisco ISE 対応ネットワークに接続されている場合、これらのデバイスはデフォルトの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、エンドポイントがクライアント プロビジョニング ポータルにリダイレクトされている間、ポスチャのランタイム中に一致するクライアント プロビジョニング 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できます。

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]**の順に選択します。

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

ユーザーがネットワークにログインするたびにポスチャ アセスメントを実行したり、指定した間隔でポスチャ アセスメント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、ポスチャアセスメントに AnyConnect エージェントを使用するユーザー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

- ユーザー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。
- ユーザーは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）。
- ユーザーは 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、ユーザーにアクセス権が付与されます。
- ユーザーは 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）。
- ユーザーは 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、ユーザー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。同じユーザーセッションが使用されているため、ユーザーは引き続きネットワークに接続されています。
- 1 時間後、ユーザーはログオフします（セッションはユーザー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、ユーザーはログオンします。ポスチャ リースが期限切れになり、新しいユーザー 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 はモニターリング 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。

（注） PRA は、PSN フェールオーバー中はサポートされません。PSN フェールオーバー後、クライアントで再スキャンを有効にするか、ポスチャリースを有効にする必要があります。

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ー ID グループに各 PRA を設定できます。

始める前に

- 各定期的再評価（PRA）構成に、設定に割り当てられている一意のグループ、またはユーザー 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ー ID グループがないことを確認します。
- PRA 構成がユーザー 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* 以外のユーザー ID グループを反映するように、任意のユーザー ID グループで既存の PRA 設定を更新します。
  - ユーザー ID グループ「*Any*」の既存の PRA 設定を削除します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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、**[新規再評価の構成（New Reassessment Configuration）]** ウィンドウで値を変更します。

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）] ウィンドウのフィールドについて説明します。 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]** の順に選択します。

表 *2:* ポスチャのトラブルシューティングの設定

フィールド名	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	
[ユーザー名（Username）]	フィルタリング基準として使用するユーザー名を入力します。

フィールド名	使用上のガイドライン
MAC アドレス	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	
時刻	イベントの時刻
ステータス（Status）	ポスチャ ステータス
[ユーザー名（Username）]	イベントに関連付けられたユーザー名
MAC アドレス	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

ポスチャのトラブルシューティング ツール （105 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）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[ポスチャ（Posture）]** > **[全般設定（General Settings）]**の順に選択します。

これらの設定はポスチャのデフォルト設定であり、ポスチャプロファイルによって上書きできます。

全般的なポスチャの設定

- [修復タイマー（Remediation Timer）]：修復を開始する前に待機する時間を入力します。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）]：時間値を秒単位で入力します。デフォルト値は 3 秒です。有効な範囲は 2 ～ 30 秒です。
- [デフォルト ポスチャ ステータス（Default Posture Status）]：[準拠（Compliant）] または [非準拠（Noncompliant）] を選択します。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はこのステータスを想定します。
- [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。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。有効な範囲は 0 ～ 300 秒です。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。
- [エージェントレス ポスチャ クライアントのタイムアウト（Agentless posture client timeout）]：ポスチャチェックが失敗したと見なされるまでの待機時間を指定します。
- [毎回の実行後にエージェントレスプラグインを削除する（Remove Agentless Plugin after each run）]：この設定を有効にすると、エージェントレスポスチャの実行後にクライアントからエージェントが削除されます。新しいバージョンが使用可能になるまで、ダウンロードしたプラグインを再利用できるように、これを無効のままにしておくことを強くお勧めします。これを無効のままにすると、ネットワークトラフィックを削減できます。
- [ステルスモードでのアクセプタブル ユース ポリシー（Acceptable Use Policy in Stealth Mode）]：会社のネットワークの利用規約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

- [ユーザーがネットワークに接続するたびにポスチャアセスメントを行う（Perform posture assessment every time a user connects to the network）]：ユーザーがネットワークに接続するたびにポスチャアセスメントを開始するには、このオプションを選択します。
- [n 日おきにポスチャアセスメントを行う（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場合でも、指定された日数が経過したらポスチャアセスメントを開始するには、このオプションを選択します。
- [最後の既知のポスチャ準拠ステータスをキャッシュする（Cache Last Known Posture Compliant Status）]：ポスチャアセスメント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。
- [最後の既知のポスチャ準拠ステータス（Last Known Posture Compliant Status）]：この設定は、[最後の既知のポスチャ準拠ステータスをキャッシュする（Cache Last Known Posture Compliant Status）] をオンにした場合にのみ適用されます。Cisco ISE は、このフィールドに指定された時間、ポスチャアセスメント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

ポスチャ管理の設定 （9 ページ）
ポスチャのリース （15 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 （14 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、「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）] ウィンドウを使用して、Web から更新を動的にダウンロードできます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [更新（Updates）]**の順に選択します。

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 サーバー経由など）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）] ウィンドウの値を変更します。

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）] ウィンドウに、[ポスチャ更新（Posture Updates）] ウィンドウの [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。

Cisco ISE オフライン更新

このオフライン更新オプションを使用すると、Cisco ISE を使用してデバイスから Cisco.com にインターネット経由で直接アクセスできない場合、またはセキュリティポリシーによって許可されていない場合に、クライアントプロビジョニングおよびポスチャ更新をダウンロードできます。

オフラインのクライアント プロビジョニング リソースをアップロードするには、次の手順を実行します。

ステップ 1 https://software.cisco.com/download/home/283801620/type/283802505/release/3.0.0に進みます。

ステップ 2 ログインクレデンシャルを入力します。

ステップ 3 Cisco Identity Services Engine のダウンロードウィンドウに移動し、リリースを選択します。

次のオフライン インストール パッケージをダウンロードできます。

- **win_spw-**<*version*>**-isebundle.zip**：Windows 向けのオフライン SPW インストールパッケージ
- **mac-spw-**<*version*>**.zip**：Mac OS X 向けのオフライン SPW インストールパッケージ

- **compliancemodule-**<*version*>**-isebundle.zip**：オフライン コンプライアンス モジュール インストール パッケージ
- **macagent-**<*version*>**-isebundle.zip**：オフライン Mac エージェント インストール パッケージ
- **webagent-**<*version*>**-isebundle.zip**：オフライン Web エージェント インストール パッケージ

ステップ 4 [ダウンロード（Download）] または [カートに追加（Add to Cart）] のいずれかをクリックします。

ダウンロードしたインストールパッケージを Cisco ISE に追加する方法については、『Cisco Identity Services EngineAdministrator Guide』の「Add ClientProvisioning Resources from a Local Machine」のセクションを参照してください。

ポスチャ更新を使用して、ローカルシステムのアーカイブから Windows および Mac オペレーティングシステムのチェック、オペレーティングシステム情報、ウイルス対策とスパイウェア対策サポート表を更新できます。

オフライン更新の場合は、アーカイブファイルのバージョンが設定ファイルのバージョンと一致していることを確認します。Cisco ISE を設定した後にオフラインでポスチャ更新を使用し、ポスチャポリシーサービスの動的更新を有効にします。

オフラインのポスチャ更新をダウンロードするには、次のようにします。

ステップ 1 https://www.cisco.com/web/secure/spa/posture-offline.htmlに進みます。

ステップ 2 ローカルシステムに **posture-offline.zip** ファイルを保存します。このファイルを使用すると、Windows および Mac オペレーティングシステムのオペレーティングシステム情報、チェック、ルール、ウイルス対策とスパイウェア対策サポート表が更新されます。

ステップ 3 [管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）]の順に選択します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、

ステップ 4 矢印をクリックすると、ポスチャの設定が表示されます。

ステップ 5 [更新（Updates）] をクリックします。
[ポスチャ更新（Posture Updates）] ウィンドウが表示されます。

ステップ 6 [オフライン（Offline）] オプションをクリックします。

ステップ 7 [参照（Browse）] をクリックし、システムのローカルフォルダからアーカイブファイル（posture-offline.zip）を検索します。

（注） [更新するファイル（File to Update）] フィールドは必須フィールドです。適切なファイルを含むアーカイブファイル（.zip）を 1 つだけ選択できます。.zip、.tar、.gz 以外のアーカイブファイルはサポートされていません。

ステップ 8 [今すぐ更新（Update Now）] をクリックします。

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [更新（Updates）]**の順に選択します。

ステップ 2 [ポスチャ更新（Posture Updates）] ウィンドウで [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 [アクセプタブルユースポリシー構成（Acceptable Use Policy Configurations）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [アクセプタブルユースポリシー（Acceptable Use Policy）]** です。

表 *3 :* ポスチャ *AUP* の設定

フィールド名	使用上のガイドライン
構成名	ユーザーが作成する AUP 設定の名前を入力します。
設定の説明（Configuration Description）	ユーザーが作成する AUP 設定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
エージェントユーザーへの AUP の表示（Windows の場合のみ）	選択した場合、認証およびポスチャアセスメントが成功すると、ネットワークのネットワーク使用の利用規約へのリンクがユーザーに表示されます。
[AUP メッセージの URL を使用（Use URL for AUP message）]	選択した場合、AUP メッセージの URL を [AUP URL] フィールド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）]	選択した場合、場所を参照し、ジップ形式のファイルをアップロードします。このファイルには、最上位レベルに index.html を含める必要があります。 .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	ユーザーが認証およびポスチャアセスメントに成功した際にアクセスする AUP の URL を入力します。
AUP ファイル（AUP File）	ファイルを参照し、Cisco ISE サーバーにアップロードします。これは zip 形式のファイルで、最上位レベルに index.html ファイルを含める必要があります。

フィールド名	使用上のガイドライン
ユーザー ID グループの選択（Select User Identity Groups）	AUP 構成の一意のユーザー ID グループまたはユーザー 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。 • 2 つの設定が共通のユーザー ID グループを持つことはできません。 • ユーザー 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。 • ユーザー ID グループ「Any」を使用して AUP 構成を作成した場合、一意のユーザー ID グループ、または複数のユーザー ID グループを使用して他の AUP 構成を作成することはできません。Any 以外のユーザー ID グループを使用して AUP 構成を作成するには、最初にユーザー ID グループ「Any」を使用した既存の AUP 構成を削除するか、ユーザー ID グループ「Any」を使用した既存の AUP 構成を一意のユーザー ID グループまたは複数のユーザーの 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ー ID グループを一覧表示します。

関連トピック

ポスチャ アセスメントの利用規定の設定 （25 ページ）

ポスチャ アセスメントの利用規定の設定

ログインし、クライアントのポスチャ アセスメントが成功すると、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。ユーザーがリンクをクリックすると、ネットワーク使用の利用規約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、一意のユーザー ID グループ、またはユーザー 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ー 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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [アクセプタブルユースポリシー（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 **[アクセプタブルユースポリシー構成（New Acceptable Use Policy Configuration）]** ウィンドウで値を変更します。

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。

ユーザー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上のレジストリ 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どうかを確認する条件。

（注） プロセスがインストールされ実行されている場合、ユーザーは準拠します。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、エンドユーザーは準拠します。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、エンドユーザーは準拠しません。

- 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どうかを確認する条件。
- 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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]**の順に選択します。

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。
- ウイルス対策複合条件：1 つ以上の AV 条件、または AV 複合条件が含まれます。
- スパイウェア対策複合条件：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。

複合ポスチャ条件の作成

ポスチャ アセスメントと検証のポスチャ 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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]**の順に選択します。

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。

ディクショナリ複合条件の設定

表 *4:* 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ー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

複合ポスチャ条件 （27 ページ）
複合ポスチャ条件の作成 （28 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）]ウィンドウ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）] ウィンドウには、ウイルス対策とスパイウェア対策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。ユーザー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、エージェントは新しいアンチウイルスおよびアンチスパイウェア ライブラリを受け取ります。これは、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。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確認します。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および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 ISE Compatibility Guide』の 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。

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 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 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 *5 : 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

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
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。

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]**の順に選択します。

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 （63 ページ）
パッチ管理修復の追加 （88 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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]**の順に選択します。

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）] ウィンドウで、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

次の表に、[ファイル条件（File Conditions）] ウィンドウのフィールドの説明を示します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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 *6 :* 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	**MacOS** での使用ガイドライン	**Linux OS** 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。	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。	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 MacOS を選択します。	ファイル条件が適用される Linux OS を選択します。次のオプションを使用できます。 • **Ubuntu** • **18.04** • **20.04** • **Red Hat** • **7.5** • **7.9** • **8.1** • **8.2** • **8.3** • **SuSE** • **12.3** • **12.4** • **12.5** • **15.0** • **15.1** • **15.2**

フィールド名	**Windows OS** での使用ガイドライン	**MacOS**での使用ガイドライン	**Linux OS** での使用ガイドライン
ファイル タイプ（File Type）	次のいずれかのオプションを選択します。 • [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。	次のいずれかのオプションを選択します。 • [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。	次のいずれかのオプションを選択します。 • [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。

フィールド名	**Windows OS** での使用ガイドライン	**MacOS** での使用ガイドライン	**Linux OS** での使用ガイドライン
データ型と演算子（**Data Type and Operator**）	NA		NA

フィールド名	Windows OS での使用ガイドライン	MacOSでの使用ガイドライン	Linux OS での使用ガイドライン
		（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	

フィールド名	**Windows OS** での使用ガイドライン	**MacOS** での使用ガイドライン	**Linux OS** での使用ガイドライン
		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。	
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（BuildVersionStampAsNumber など）を入力します。	NA

フィールド名	**Windows OS** での使用ガイドライン	**MacOS**での使用ガイドライン	**Linux OS** での使用ガイドライン
ファイル パス（**File Path**）		次のいずれかのオプションを選択します。 • 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。	次のいずれかのオプションを選択します。 • 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	MacOS での使用ガイドライン	Linux OS での使用ガイドライン
	次のいずれかのオプションを選択します。 • 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：		

フィールド名	**Windows OS** での使用ガイドライン	**MacOS**での使用ガイドライン	**Linux OS** での使用ガイドライン
	指定したファイルが Windows ユーザー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 ユーザーのローカル プロファイル ディレクトリにあるかど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。

フィールド名	**Windows OS** での使用ガイドライン	**MacOS** での使用ガイドライン	**Linux OS** での使用ガイドライン
ファイル演算子	[File Operator] オプションは、[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** • [Within]：最後の n 日。有効な範囲は 1 ～ 300 です。 **FileExistence** • **Exists** • **DoesNotExist** **FileVersion** • **EarlierThan** • **LaterThan** • **EqualTo**	[File Operator] オプションは、[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** • [Within]：最後の n 日。有効な範囲は 1 ～ 300 です。 **FileExistence** • **Exists** • **DoesNotExist**	[File Operator] オプションは、[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** • [Within]：最後の n 日。有効な範囲は 1 ～ 300 です。 **FileExistence** • **Exists** • **DoesNotExist**
ファイルの **CRC** データ（**File CRC Data**）	（[File Type] として [CRC32] を選択した場合のみ使用可能） 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。	（[File Type] として [CRC32] を選択した場合のみ使用可能） 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。	（[File Type] として [CRC32] を選択した場合のみ使用可能） 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。

フィールド名	Windows OS での使用ガイドライン	MacOS での使用ガイドライン	Linux OS での使用ガイドライン
ファイルのSHA-256データ（File SHA-256 Data）	（[File Type] として [SHA-256] を選択した場合のみ使用可能）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。	（[File Type] として [SHA-256] を選択した場合のみ使用可能）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。	（[File Type] として [SHA-256] を選択した場合のみ使用可能）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）	（[File Type] として [FileDate] を選択した場合のみ使用可能）クライアントシステムの日付と時刻を、mm/dd/yyyy 形式と hh:mm:ss 形式で入力します。	（[File Type] として [FileDate] を選択した場合のみ使用可能）クライアントシステムの日付と時刻を、mm/dd/yyyy 形式と hh:mm:ss 形式で入力します。	（[File Type] として [FileDate] を選択した場合のみ使用可能）クライアントシステムの日付と時刻を、mm/dd/yyyy 形式と 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 （26 ページ）
複合ポスチャ条件 （27 ページ）
ポスチャ条件の作成 （100 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 MacOS のデフォルトのファイアウォール条件を提示します。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（Description）	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 MacOS 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。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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 *7:* 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 （26 ページ）
複合ポスチャ条件 （27 ページ）

継続的なエンドポイント属性モニターリング

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ーします。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ーします。この機能をオンまたはオフにできます。また、データのモニター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。AnyConnect は初回ポスチャ時に、実行中のアプリケーションと搭載アプリケーションの一覧を報告します。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ーに送信します。サーバー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得られます。

次の表に、[アプリケーション条件（Application Conditions）] ウィンドウのフィールドを示します。このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして、**[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）]**の順に選択します。

フィールド名	使用上のガイドライン
名前（Name）	アプリケーションの条件の名前を入力します。
説明（Description）	アプリケーション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	アプリケーション条件が適用されるオペレーティングシステムを選択します。次のオプションを使用できます。 • **Windows** • **Mac OSX** • **Linux**
コンプライアンス モジュール	次のいずれかのオプションを選択します。 • **4.x 以降** • **3.x 以前** • **任意のバージョン（Any Version）**
次を確認（**Check By**）	次のいずれかのオプションを選択します。 • [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。 • [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。 （注） Linux OS の場合は、[Process] オプションのみが表示されます。
プロセス名	（[Check By] オプションで [Process] を選択した場合のみ使用可能）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**）	（[Check By] オプションで [Process] を選択した場合のみ使用可能）次のいずれかを選択します。 • [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。 • [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。

フィールド名	使用上のガイドライン
アプリケーションの状態（**Application State**）	（[Check By] オプションで [Application] を選択した場合のみ使用可能）次のいずれかのオプションを選択します。 • [Installed]：クライアント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確認するには、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。 • [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。
次をプロビジョニング（**Provision By**）	（[Check By] オプションで [Application] を選択した場合のみ使用可能）次のいずれかのオプションを選択します。 • [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。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]**の順に選択します。

表 *8*: 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。
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MacOS 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ー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。

フィールド名	使用上のガイドライン
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。 • [ユーザーエージェント（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ー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ーエージェント（Daemon or User Agent）]：指定したサービスがデーモンまたはユーザー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。
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 （26 ページ）
複合ポスチャ条件 （27 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。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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 *9:* 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（Description）	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。
（&）：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 （26 ページ）
複合ポスチャ条件の作成 （28 ページ）

ウイルス対策条件の設定

Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]**の順に選択します。

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。
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、クライアント上のウイルス対策プログラムのインストールを確認するか、または条件が適用される最新のウイルス対策定義ファイルの更新を確認します。
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。

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。

（注） [ベースライン条件（Baseline Condition）] または [高度な条件（Advance Condition）] のいずれかから、各ウイルス対策製品に対して 1 つの条件のみを設定できます。

ベースライン条件

フィールド名	ガイドライン
最小バージョン	（オペレーティングシステムとベンダーを更新する場合にのみ使用可能）ドロップダウンリストからウイルス対策の最小バージョンを選択します。 このチェックにより、ネットワーク上のすべてのエンドポイントにネットワークポリシーが適用され、ウイルス対策の最小バージョンに準拠します。
最大バージョン	ウイルス対策の最大バージョンは、ポスチャフィードを更新すると自動的に改訂されます。
最小準拠モジュールバージョン	最小準拠モジュールバージョンは AnyConnect から更新されます。

高度な条件

フィールド名	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	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。

関連トピック

複合ポスチャ条件 （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 （30 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 （30 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。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[AS 複合条件（AS Compound Condition）]**の順に選択します。

表 *10 :* 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（Description）	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、クライアント上のスパイ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スパイウェア対策定義ファイルの更新をチェックすることができます。
ベンダー（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。

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)**）	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。
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。

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 （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 （30 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 （30 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。

このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして、**[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）]**の順に選択します。

（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 チェックが失敗する場合があります。

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。

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（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確認するか、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確認します。。Windows、MacOS、およびLinuxオペレーティングシステムをサポートしています。
ベンダー（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 [Products for Selected Vendor] テーブルに表示されます。
チェック タイプ（Check Type）	次のいずれかのオプションを選択します。 • [Install]：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確認する場合にこのオプションを選択します。 • [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確認する場合にこのオプションを選択します。
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）	（[Definition] チェックタイプを選択した場合のみ使用可能）クライアント上のマルウェア対策定義ファイルのバージョンを確認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 [Latest Definition Date] または [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、[Current System Date] フィールドを使用する必要があります。

フィールド名	使用上のガイドライン
[Allow Virus Definition File to be]	（[Definition] 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確認する場合にこのオプションを選択します。最新の定義ファイルの日付を [Days Older Than] フィールドで定義した値よりも前にすることはできません。 オフにした場合、Cisco ISE では [Check against latest AV definition file version] オプションを使用する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を、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前にできる日数を定義します。デフォルト値は 0 です。
最新のファイルの日付（**Latest File Date**）	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前にできる日数を定義するには、このオプションを選択します。 日数をデフォルト値に設定する場合、クライアント上のマルウェア対策定義ファイルの日付を、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前にすることは許容されません。 このチェックは、選択した製品の [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、[Current System Date] フィールドを使用する必要があります。

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**）	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現在のシステム日付よりも前にできる日数を定義するには、このオプションを選択します。 日数をデフォルト値に設定すると、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前にすることはできません。

関連トピック

複合ポスチャ条件 （27 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。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]** の順に選択します。

表 *11* : 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（**Description**）	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

単純ポスチャ条件 （26 ページ）
単純ポスチャ条件の作成 （27 ページ）

ディクショナリ複合条件の設定

表 *12 :* 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。
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ー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。

フィールド名	使用上のガイドライン
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

複合ポスチャ条件 （27 ページ）
複合ポスチャ条件の作成 （28 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。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[Policy]** > **[Policy Elements]** > **[Conditions]** > **[Posture]** > **[Patch Management Conditions]** です。

表 *13* : 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（**Description**）	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確認するか、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確認します。Windows、MacOS、または Linux OS 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**）	[Vendor Name] ドロップダウンリストからベンダーを選択します。選択したベンダーとパッチ管理製品およびそれらのサポート対象のバージョンに基づいて、チェックタイプ、最小対応モジュールのサポートの詳細が [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
	次のいずれかのオプションを選択します。 • [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、[Requirements] ウィンドウで [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。 [Vendor Name] フィールド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、[Products for Selected Vendor] ドロップダウンリストをクリックします。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 [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 以降と AnyConnect 4.5 以降に適用）[Patch Management condition with SCCM] で [Up To Date] チェックタイプを選択すると、Cisco ISE は次の動作を行いま

フィールド名	使用上のガイドライン
	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）	（[Up To Date] チェックタイプを選択した場合のみ使用可能）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。次のいずれかのオプションを選択します。 • [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。 • [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。 • [Moderate, Important, and 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。 • [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

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。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、[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 *14* : 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 MacOS 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、MacOS 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MacOS 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）] は無効になります。 （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。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [USB]**の順に選択します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]**

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

表 *15 : 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

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	Windows
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 （26 ページ）

ハードウェア属性条件の設定

Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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に定義されたチェック。
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

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 アセスメント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） 「エンドポイントポリシー」と「論理プロファイル」の両方が **[ポリシー（Policy）]** > **[ポスチャ（Posture）]** の [その他の条件（Other Conditions）] で設定されている場合、プロファイラポリシー評価は機能しません。

（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。
- 猶予期間は Linux エージェントではサポートされません。
- （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

- アクセプタブル ユース ポリシー（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 （137 ページ）を参照してください。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）]** > **[ポスチャ（Posture）]** または **[ワークセンター（Work Centers）]** > **[ポスチャ（Posture）]** > **[ポスチャポリシー（Posture Policy）]** の順に選択します。

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 ー 90 日
- 1 ー 2,160 時間
- 1 ー 129,600 分

デフォルトでは、この設定は無効です。

（注） ポスチャアセスメント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ー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。

ユーザー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、パッチ管理、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。

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 認証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。

ステップ 11 AnyConnect をダウンロードして起動します。

a) SSID に接続します。
b) 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。
c) [開始（Start）] をクリックします。これにより、AnyConnect エージェント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。
d) [ここに初めて来ました（This Is My First Time Here）] をクリックします。

e) **[AnyConnect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 AnyConnect）]** を選択します。

f) Windows または MacOS 用の Cisco Anyconnect の .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、MacOS の場合は .dmg ファイルをダブルクリックして、アプリケーションを実行します。

（注） Cisco ISE は、AnyConnect ポスチャフローの AnyConnect の ARM64 バージョンをサポートしていません。クライアント プロビジョニング ポリシーで AnyConnect の ARM64 バージョンを使用しないでください。使用すると、クライアント側で障害が発生する可能性があります。この問題が原因で AnyConnect が正常に動作していない場合は、クライアントを再起動します。

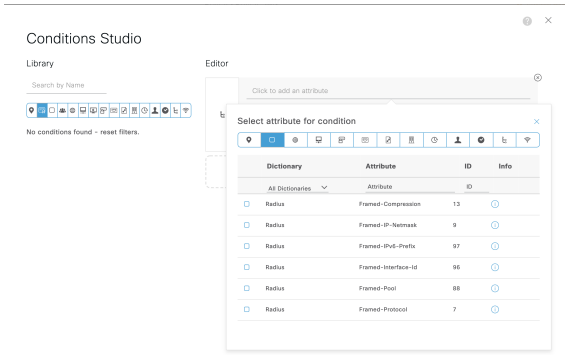
証明書ベースの条件のための前提条件

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のいずれか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認証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 *1 : Cisco* のプロビジョニング ポリシー

図 *2:* 条件スタジオ



（注） ISE サーバー証明書は、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、サーバーが信頼されていない場合は機能しません。

- Windows OS：サーバー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：サーバー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、ポスチャポリシーとプロファイルの作成を容易にする、事前に設定されたポスチャポリシー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。次に、デフォルトのいくつかのデフォルトのポスチャポリシーを示します。

ルール名	説明（Description）	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

ルール名	説明（Description）	要件
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
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 アセスメント

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、エンタープライズ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、ユーザー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 アセスメント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 アセスメントオプション

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

表 *16 :* ポスチャ アセスメントオプション

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）	—	—

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
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
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	—	—	—

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
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 Cisco ISE ポスチャエージェント、および Windows の Web エージェントでサポートされている修復オプション（ポスチャ条件）のリストを示します。

表 *17*：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	—
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。

ユーザー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 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許可またはブロック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) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、 > [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) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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 （103 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. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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。

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）] ウィンドウには、すべてのウイルス対策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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）]**の順に選択します。

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 Remediation）] ウィンドウで値を変更します。

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）] ウィンドウには、すべてのウイルス対策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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）]**の順に選択します。

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）]** ウィンドウで値を変更します。

ステップ 6 **[送信（Submit）]** をクリックします。

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）] ウィンドウでは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）] ウィンドウには、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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[ポスチャ（Posture）]**の順に選択します。

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）] ウィンドウで値を変更します。

ステップ 7 **[送信（Submit）]** をクリックします。

スクリプト修復の追加

ポスチャ修復スクリプトを作成して Cisco ISE にアップロードし、エンドポイントのコンプライアンス違反の問題を解決できます。

始める前に

- ポスチャポリシーを取得するための信頼を確立します。詳細については、「スクリプト条件を実行するために信頼を確立する （85 ページ）」を参照してください。
- スクリプトをダウンロードします。詳細については、「スクリプトのダウンロード （87 ページ）」を参照してください。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[ポスチャ（Posture）]**の順に選択します。

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 [スクリプト修復（Script 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 スクリプトの [名前（Name）] と [説明（Description）] に入力します。

ステップ 6 対応するドロップダウンリストから [オペレーティングシステム（Operating System）] と [修復タイプ（Remediation Type）] を選択します。

[Windows] オペレーティングシステムを選択した場合は、[スクリプトタイプ（Script Type）] と [Windows PowerShell 実行ポリシー（Windows PowerShell Execution）] フィールドが表示されます。対応するオプションボタンをクリックして、必要なスクリプトタイプと実行ポリシーを選択します。

ステップ 7 [修復タイプ（Remediation Type）] ドロップダウンリストから、[自動（Automatic）] または [手動（Manual）] を選択します。

（注）
- Linux エージェントでは、自動修復のみがサポートされます。手動修復はサポートされていません。
- Linux エージェントでは、シェルスクリプトのみがサポートされます。

ステップ 8 [間隔（Interval）] と [再試行回数（Retry Count）] に値を入力します。有効な範囲は 0 ～ 999 です。

ステップ 9 [アップロードするファイル（File To Upload）] の隣にある [ファイルの選択（Choose File）] をクリックし、ローカルシステムからアップロードするスクリプトを選択します。

ステップ 10 スクリプトを管理者として実行するには、[管理者/ルート（Administrator/Root）] オプションボタンをクリックします。ログインユーザーとしてスクリプトを実行するには、[ログインユーザー（Logged-in User）] オプションボタンをクリックします。

ステップ 11 **[送信（Submit）]** をクリックします。

ステップ 12 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[操作（Operations）]** > **[レポート（Reports）]** > **[エンドポイントとユーザー（Endpoints and Users）]** > **[ポスチャスクリプト修復（Posture Script Remediation）]** を選択し、修復スクリプトの実行ステータスを確認します。

次のいずれかのステータスが表示されます。

- 修復スクリプトの実行に成功しました。
- 修復が試行され、スクリプトは失敗して終了しました。
- 修復は試行されませんでした（デフォルト）。
- 修復の試行に失敗しました。含まれているポリシーが改ざんされている可能性があるため、スクリプトの整合性チェックに失敗しました。
- 修復の試行に失敗しました。クライアントがスクリプトのダウンロードに失敗しました。
- 修復の試行に失敗しました。スクリプトが破損しているか、改ざんされている可能性があるため、スクリプトの整合性テストに失敗しました。
- 修復の試行に失敗しました。スクリプトは実行されましたが、時間内に終了しませんでした（タイムアウト）。
- 修復の試行に失敗しました。一般的な内部システム障害が発生しました。
- 修復の試行に失敗しました。スクリプトタイプがサポートされていません。
- 修復の試行に失敗しました。スクリプトの起動に失敗しました。
- 証明書の検証に失敗しました。クライアントが、Cisco ISE よって提示されたサーバー証明書を検証できませんでした。

スクリプト条件を実行するために信頼を確立する

エンドポイントでスクリプトを実行し、Cisco ISE サーバーが侵害されていないことを確認するには、信頼を確立する必要があります。Cisco ISE 環境では、1 つ以上の PSN を設定できま

す。すべての PSN には有効な証明書チェーンがあります。証明書チェーンは任意の証明書で始まり、中間証明書またはルート CA 証明書が続きます。フィンガープリントの検証では、証明書チェーン内のすべての証明書を使用できます。

AnyConnectLocalPolicy のプロファイルエディタの証明書チェーン内に任意の証明書の SHA-256 フィンガープリントを設定できます。たとえば、次のコマンドは、input.cer という名前の証明書の SHA-256 フィンガープリントを生成します

```
openssl x509 -inform DER -in <input.cer> -out <output.crt>
openssl x509 -in <output.crt> -fingerprint -noout -sha256
```

次に、出力の例を示します。

```
openssl x509 -in 535-pos.crt -fingerprint -noout -sha256
SHA256
Fingerprint=B9:42:7F:85:09:18:30:40:06:0B:DB:9C:48:36:F0:60:90:75:AB:D3:E9:83:AB:1A:BF:01:8F:6E:F0:11:9A:B5
```

次の例は、AnyConnectLocalPolicy.xml の新しいタグを示しています。

```
<TrustedISECertFingerprints>
<fingerprint>
<algorithm>SHA-256</algorithm>
<hash>B9:42:7F:85:09:18:30:40:06:0B:DB:9C:48:36:F0:60:90:75:AB:D3:E9:83:AB:1A:BF:01:8F:6E:F0:11:9A:B5</hash>
</fingerprint>
</TrustedISECertFingerprints>
```

（注） SHA-256 フィンガープリントは、コロンの有無にかかわらず追加できます。次のいずれかの形式でフィンガープリントを追加できます。
`B9:42:7F:85:09:18:30:40:06:0B:DB:9C:48:36:F0:60:90:75:AB:D3:E9:83:AB:1A:BF:01:8F:6E:F0:11:9A:B5` または `B9427F8509183040060BDB9C4836F0609075ABD3E983AB1ABF018F6EF0119AB5`。フィンガープリントでは大文字と小文字は区別されません。

エージェントは、Cisco ISE 証明書のフィンガープリントと信頼できる証明書のフィンガープリント（AnyConnectLocalPolicy.xml に存在）を照合します。エンドポイントに有効な証明書フィンガープリントがない場合、スクリプトはエンドポイントで実行されません。

（注） AnyConnectLocalPolicy.xml でフィンガープリントが設定されている場合、すべてのフローの Cisco ISE 信頼を検証するためにそれらのフィンガープリントが使用されます。証明書が信頼できない場合、またはフィンガープリントの不一致がある場合、エラーメッセージは表示されません。ただし、次のエラーメッセージが [ポスチャスクリプト条件（Posture Script Condition）] レポートに含まれています（[操作（Operations）] > [レポート（Reports）] > [エンドポイントとユーザー（Endpoints and Users）]）。

条件スクリプト証明書の検証に失敗しました。クライアントが、Cisco ISE よって提示されたサーバー証明書を検証できませんでした。

スクリプトのダウンロード

ポスチャチェックが失敗し、関連する修復アクションがトリガーされると、AnyConnect はポスチャポリシーで設定された HTTPS URL からスクリプトをダウンロードします。スクリプトをダウンロードするには、次の条件を満たしている必要があります。

- 信頼できるフィンガープリントが AnyConnectLocalPolicy.xml に存在している。
- HTTPS URL によって提示されるフィンガープリントが、AnyConnectLocalPolicy.xml に存在している信頼できる証明書フィンガープリントと一致している。

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）]**の順に選択します。

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。

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ウィンドウ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）] ウィンドウには、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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）]**の順に選択します。

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）] ウィンドウで値を変更します。

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）] ウィンドウには、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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）]**の順に選択します。

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）] ウィンドウで値を変更します。

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）] ウィンドウに修復アクションを追加します。

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 サーバーから最新の 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 サーバーまたは Microsoft で管理されている WSUS サーバーから最新の 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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[ポスチャ（Posture）]**の順に選択します。

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）] ウィンドウの値を変更します。

ステップ 6 **[送信（Submit）]** をクリックします。

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]** ウィンドウで値を変更します。

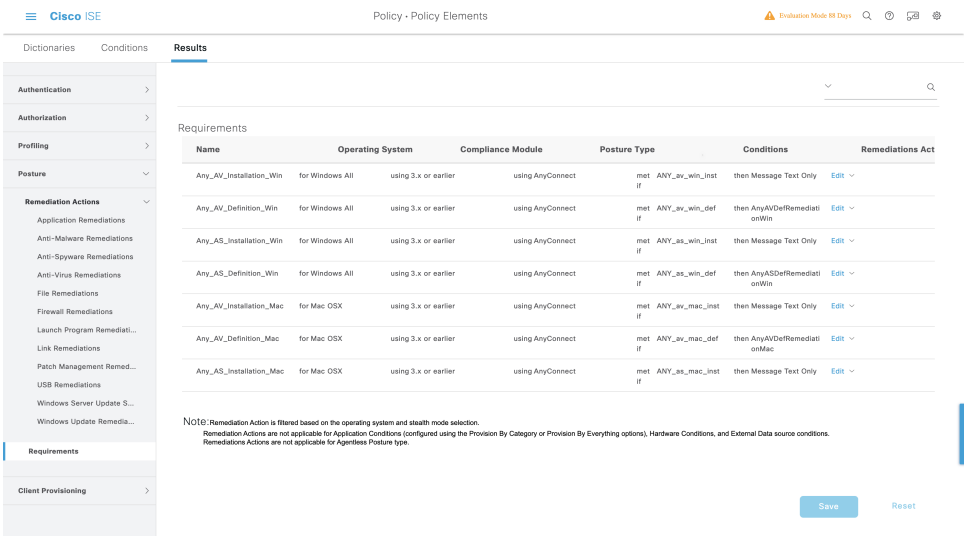
ステップ 6 **[送信（Submit）]** をクリックします。

ポスチャ アセスメント要件

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 アセスメント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 アセスメント中に続行するオプションがあります。

図 *3:* 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。エンドユーザーは、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、ユーザー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、ユーザーは [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。エンドユーザーは、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、ユーザー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、エンドユーザーが [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ーからの入力を促しません。

たとえば、エンドユーザー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ーを見つける場合は、その条件を監査要件として指定できます。

可視性要件

ポリシーの評価時に、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 分ごとに報告します。

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 アセスメント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。

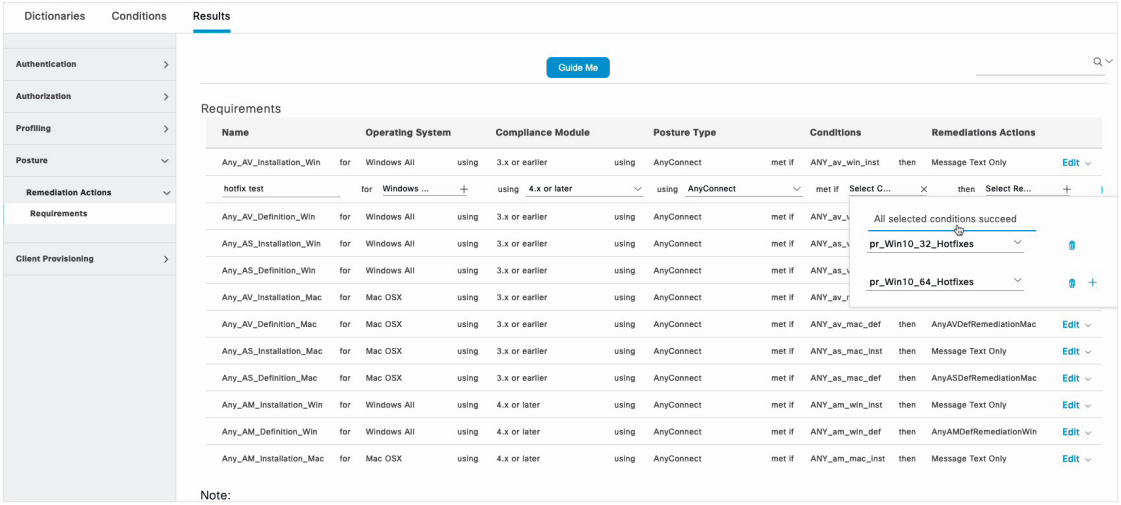
- 802.1X 環境での有線およびワイヤレス許可変更（CoA）：
  - [新しい許可プロファイル（New Authorization Profiles）] ウィンドウで新しい許可プロファイルを作成するときに、特定の許可ポリシーの再認証タイマーを設定できます。
  - 有線ユーザーは、ネットワークの接続を切断して再接続すると、隔離状態から移行できます。ワイヤレス環境では、ユーザーは、ワイヤレス LAN コントローラ（WLC）から切断し、ユーザーのアイドルタイムアウト時間が過ぎるまで待機してから、ネットワークへの再接続を試行する必要があります。
- VPN 環境：VPN トンネルを切断し、再接続します。

クライアントのポスチャ要件の作成

[要件（Requirements）] ウィンドウでは、ユーザー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）] ウィンドウで作成および保存されたユーザー定義の条件および修復アクションは、それぞれのリストウィンドウに表示されます。

（注） 環境内のすべての Windows 10 ホットフィックスを検証するポスチャ要件を作成するには、要件の [条件（Conditions）] 領域に pr_Win10_32_Hotfixes と pr_Win10_64_Hotfixes の両方を含めるように設定する必要があります。条件の上部で、[選択したすべての条件が成功する（All selected conditions succeed）] が選択されていることを確認します。設定が成功すると、**pr_Win10_32_Hotfixes と pr_Win10_64_Hotfixes** が表示されます。エンドポイントの検証済み条件の詳細を表示するには、メインメニューから**[運用（Operations）]**>**[レポート（Reports）]**>**[レポート（Reports）]**>**[エンドポイントとユーザー（Endpoints and Users）]**>**[エンドポイントによるポスチャアセスメント（Posture Assessment by Endpoints）]**を選択します。エンドポイントをクリックして、対応するポスチャの詳細を表示します。

図 *4 : Windows 10* でのポスチャ要件の検証



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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[ポスチャ（Posture）]** > **[要件（Requirements）]**の順に選択します。

ステップ 2 [要件（Requirements）] ウィンドウに値を入力します。

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 [ポスチャ再評価構成（Posture Reassessment Configurations）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして、**[管理（Administration）]**>**[システム（System）]**>**[設定（Settings）]**>**[ポスチャ（Posture）]**>**[再評価（Reassessments）]** です。

表 *18 :* ポスチャ再評価の構成設定

フィールド名	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?）	ユーザー 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。

フィールド名	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）]：ユーザー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ー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、ユーザー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ー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。ユーザーは、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。

フィールド名	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。
ユーザー 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ー 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 （15 ページ）
定期的再評価 （16 ページ）
ポスチャ アセスメントオプション （78 ページ）
ポスチャ修復オプション （80 ページ）
ポスチャのカスタム条件 （80 ページ）
カスタム ポスチャ修復アクション （82 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 つの異なる認証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 アセスメント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。

（注） すべてのシスコのネットワーク アクセス デバイスに、リダイレクトベースのポスチャを使用することを推奨します。

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 アセスメントが行われると、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 アセスメント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

[認証ポリシー（Authorization Policy）] ウィンドウでは、標準認証ポリシーと例外認証ポリシーの2種類の認証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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）]** > **[ポリシーセット（Policy Sets）]**の順に選択します。

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 ユーザー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 でユーザー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 サーバー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 サーバー 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 サーバー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 サーバー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) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [認証プロファイル（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) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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 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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]** の順に選択します。

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]**の順に選択します。

ステップ 2 **[追加（Add）]** ドロップダウンリストから、**[AnyConnectの設定（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。

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。

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。

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）]** チェックボックスをオンにします。

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。

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。

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]**の順に選択します。

ステップ 2 [追加（Add）] ドロップダウン リストから、[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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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。

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]** の順に選択します。

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]**の順に選択します。

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]**の順に選択します。

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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、if Identity Groups=Any and Operating Systems=Windows 7(All) and Compliance Module=4.x or later and Posture Type=AnyConnect Stealth then Requirements=win7Req です。

（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 サーバーで特定ユーザー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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、[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) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可（Authorization）]** > **[認証プロファイル（Authorization Profiles）]**の順に選択します。

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) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）]** > **[ポリシーセット（Policy Sets）]**の順に選択します。

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]** の順に選択します。

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[ポスチャ（Posture）]** > **[要件（Requirements）]**の順に選択します。

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）]** > **[ポスチャ（Posture）]**の順に選択します。

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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。

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 MacOS 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、MacOS 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。

ユーザー名、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。

エンドポイント ログイン クレデンシャルの設定

[エンドポイントログイン設定（Endpoint Login Configuration）] ウィンドウでは、Cisco ISE がクライアントにログインできるようにログインクレデンシャルを設定します。このウィンドウで設定されたログインクレデンシャルは、次の Cisco ISE 機能で使用されます。

Cisco ISE の GUIで、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[エンドポイントスクリプト（Endpoint Scripts）]** > **[設定（Settings）]** を選択します。

次のタブが表示されます。

- [Windows ドメインユーザー（Windows Domain User）]：Cisco ISE が SSH 経由でクライアントにログインするために使用する必要があるドメインクレデンシャルを設定します。[+（Plus）] アイコンをクリックして、必要な数の Windows ログインを入力します。ドメインごとに、[ドメイン（Domain）]、[ユーザー名（Username）]、および [パスワード（Password）] の各フィールドに必要な値を入力します。ドメインクレデンシャルを設定すると、[Windows ローカルユーザー（Windows Local User）] タブで設定されたローカルユーザー クレデンシャルは無視されます。
- [Windows ローカルユーザー（Windows Local User）]：Cisco ISE が SSH 経由でクライアントにアクセスするために使用するローカルアカウントを設定します。このローカルアカウントで、PowerShell と PowerShell をリモートで実行できる必要があります。
- [MAC ローカルユーザー（MAC Local User）]：Cisco ISE が SSH 経由でクライアントにアクセスするために使用するローカルアカウントを設定します。このローカルアカウントで、PowerShell と PowerShell をリモートで実行できる必要があります。[ユーザー名（Username）] フィールドに、ローカルアカウントのアカウント名を入力します。Mac OS アカウント名を表示するには、端末で次のコマンドを実行します。

```
whoami
```

エンドポイント設定

このページでは、エンドポイントスクリプトとエージェントレスポスチャのオプションを設定します。

- [ISEへのエンドポイントスクリプト実行ログのアップロード（Upload endpoint script execution logs to ISE）]：デフォルトで有効になっている場合、エンドポイントスクリプトを Cisco ISE にアップロードできます。これを無効にすると、エンドポイントスクリプトが無効になり、エンドポイントスクリプトをアップロードまたは実行できなくなります。
- [エンドポイントスクリプト実行の冗長ロギング（Endpoint script execution verbose logging）]：デバッグの冗長ロギングを有効にします。

- [エンドポイントプロセッサのバッチサイズ（Endpoints processor batch size）]：ネットワークの負荷とシステムのパフォーマンスに対応するように調整できます。
- **MAC の同時エンドポイント処理**
- **Windows の同時エンドポイント処理**
- **OS 識別の最大再試行回数**
- **OS 識別の再試行間の遅延（ミリ秒）**
- **エンドポイントページネーションのバッチサイズ**
- **エンドポイントのログ保持期間（日）**
- **接続タイムアウト（秒）**
- **接続の最大再試行回数**
- [Powershell接続のポート番号（Port Number for Powershell）]：非標準のポート番号を使用するには。これを変更します。
- [SSH接続のポート番号（Port Number for SSH Connection）]：非標準のポート番号を使用するには、これを変更します。

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、ユーザーがクライアント 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。Linux クライアント、 Windows クライアント、Mac OS X クライアント、および Linux クライアント、と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ーには、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トしている場合は、プロキシがクライアントにそのリモートの場所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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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（Software 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（Enable Provisioning）] 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 [自動ダウンロードの有効化（Enable Automatic Download）] ドロップダウン リストから、[有効（Enable）] を選択します。

フィードのダウンロードには、使用可能なすべてのクライアント プロビジョニング リソースが含まれます。これらのリソースの一部は、展開に関係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）]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 デバイスのクライアントプロビジョニング リソースがない場合は、次のいずれかのオプションを選択します。

- [ネットワークアクセスの許可（Allow Network Access）]：ユーザーは、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。
- [定義済みの認証ポリシーの適用（Apply Defined Authorization Policy）]：ユーザーは、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）認証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、ユーザー デバイスに対して、ユーザーの 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。ユーザーのデバイスがCisco ISE ネットワークにアクセスするための証明書を必要とする場合、ユーザーに表示されるカスタマイズ可能なテキストフィールドを使用して、有効な証明書を取得し、適用する方法を説明する詳細指示をユーザーに提供する必要があります。

ステップ 6 [保存（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。

Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]**。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[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 （107 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 （111 ページ） 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、ご使用のバージョンの AnyConnect の『AnyConnect Administrators Guide』（https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-installation-and-configuration-guides-list.html）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 （146 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 （107 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 （109 ページ）
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 （111 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 （112 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

Cisco Web エージェント、AnyConnect Windows、MacOS、および Linux クライアントの場合は、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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、 **[Policy]** > **[Policy Elements]** > **[Results]** > **[Client Provisioning]** > **[Resources]**。

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 [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。

Linux エージェントをインストールする際は、次の点に注意してください。

- 自己署名証明書を使用している場合：
  - ISE 証明書を Linux エージェントにコピーするには、SSH エージェントを有効にする必要があります。
    - RHEL の場合
      1. Cisco ISE の GUI から証明書をエクスポートします。
      2. <certificate>.pem を /etc/pki/ca-trust/source/anchors/ にコピーし、ファイルの名前を <certificate>.crt に変更します。
      3. コマンド **sudo update-ca-trust extract** を実行します。
      4. /etc/pki/tls/certs/ への移動
      5. コマンド **openssl x509 -in ca-bundle.crt -text -noout** を実行します。
    - Ubuntu の場合は、次の手順を実行します。
      1. Cisco ISE の GUI から証明書をエクスポートします。
      2. <certificate>.pem を /usr/local/share/ca-certificates/ に移動し、名前を <certificate>.crt に変更します。
      3. コマンド **sudo update-ca-certificates** を実行します。

         CA 証明書が正しくインストールされているかどうかを確認するには、/etc/ssl/certs/ca-certificates.crt に移動し、このファイルに証明書あることを確認します。

（注） ISE 証明書が信頼できる CA によって発行されている場合、証明書をインポートする必要はありません。

- dot1x リダイレクトフローまたは非リダイレクトフローを開始します。

- RHEL を使用している場合は、yum がサブスクリプション マネージャで更新されていることを確認します。Ubuntu を使用している場合は、apt-get を更新します。

  Linux エージェントのシステム要件の詳細については、『Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.9』を参照してください。

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、「Cisco ISE Release Notes」の「Cisco ISE Offline Updates」の項を参照してください。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]**の順に選択します。

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 [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。

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

ステップ 5 [送信（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 カスタマイゼーションおよび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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]**の順に選択します。

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 [顧客作成のパッケージ（Customer Created Packages）] を選択します。

ステップ 4 AnyConnect リソースの名前と説明を入力します。

ステップ 5 [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 6 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 7 [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、ユーザー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。ユーザーがサインインすると、Cisco ISE は、ユーザー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、ユーザー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、有線接続ユーザーと無線接続ユーザーは、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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]**の順に選択します。

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 ネイティブ サプリカント プロファイルの設定 （113 ページ）で説明されている手順を使用して、プロファイルを作成します。

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

Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）] > [ネイティブサプリカントプロファイル（Native Supplicant Profile）]**。以下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を入力します。
- [オペレーティングシステム（Operating System）]：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ドロップダウンリストから選択します。

各プロファイルでは、Cisco 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

クライアントで使用可能にする SSID ごとにワイヤレスプロファイルを 1 つ設定します。

- [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ーの URL を入力します。
- [プロキシホスト/IP（Proxy Host/IP）]：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ーのホスト/IP を入力します。
- [プロキシポート（Proxy Port）]：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ーのポートを入力します。
- [セキュリティ（Security）]：[WPA] または [WPA2] を選択します。
- [許可されたプロトコル（Allowed Procotol）]：[PEAP] または [EAP-TLS] を選択します。
- [証明書テンプレート（Certificate Template）]：TLS の場合は、いずれかの証明書テンプレートを選択します。証明書テンプレートは、**[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）]** で定義されています。

オプションの設定

[オプション（Optional）] を展開すると、次のフィールドが表示されます。

Windows の設定

- [認証モード（Authentication Mode）]：認証のためのログイン情報として、[ユーザー（User）]、[マシン（Machine）]、または両方を選択します。
- [新規サーバーまたは信頼された証明機関の承認をユーザーに求めない（Do not prompt user to authorize new servers or trusted certification authorities）]：このオプションを有効にすると、ユーザーは承認を求められません。ユーザー証明書は自動的に受け入れられます。
- [接続に別のユーザー名を使用（Use a different user name for the connection）]：ワイヤレスプロファイルにのみ適用されます。接続に別のユーザー名を使用します。
- [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にのみ適用されます。SSID がブロードキャストされていない場合でも、ネットワークに接続します。

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は有効にする（Enable if target network is hidden）]：ターゲットネットワークが非表示になっている場合は、このチェックボックスをオンにします。

Android の設定

- [証明書登録プロトコル（Certificate Enrollment Protocol）]：いすれかのオプションボタンをクリックして、証明書登録プロトコル（[Enrollment over Secure Transport（EST）] または [Simple Certificate Enrollment Protocol（SCEP）]）を選択します。EST プロトコルを選択し

た場合、Cisco ISE は、証明書の発行時に Android ユーザーに対して追加のパスワードの入力を要求します。

有線プロファイル

- [許可されたプロトコル（Allowed Procotol）]：[PEAP] または [EAP-TLS] を選択します。
- [証明書テンプレート（Certificate Template）]：TLS の場合は、いずれかの証明書テンプレートを選択します。証明書テンプレートは、**[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）]** で定義されています。

オプションの設定

[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）]：認証のためのログイン情報として、[ユーザー（User）]、[マシン（Machine）]、または両方を選択します。
- [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（Authentication Mode）] で [ユーザー（User）] を選択すると、ユーザー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情報が使用されます（これらの情報が使用可能な場合）。
- [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になっている場合（これは、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[プロトコル（Protocols）]** > **[PEAP]** で設定）、PEAP セッションはユーザー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。
- [サーバーが暗号化バインド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。
- [新規サーバーまたは信頼できる証明機関の承認をユーザーに求めない（Do not prompt user to authorize new servers or trusted certification authorities）]：自動的にユーザー証明書を受け入れ、ユーザーにプロンプトを表示しません。

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、[詳細設定（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. 内部ユーザー、AD、LDAP、または SAML を介して CP ポータルにログインする。

   AnyConnect がポスチャを実行します。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 経由でユーザー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. 内部ユーザー、AD、LDAP、または SAML を介して CP ポータルにログインする

   AnyConnect がポスチャを実行します。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. 内部ユーザー、AD、LDAP、または SAML を介して CP ポータルにログインする。

   AnyConnect がポスチャを実行します。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. 内部ユーザー、AD、LDAP、または SAML を介して CP ポータルにログインする。

   AnyConnect がポスチャを実行します。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、[Cisco Advanced Malware Protection（AMP）イネーブラプロファイル（Advanced Malware Protection (AMP) Enabler Profile）] 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、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、 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 *19 : [AMPイネーブラプロファイル（AMP Enabler Profile）] ページ*

フィールド名	使用上のガイドライン
名前（**Name**）	ユーザーが作成する 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。

フィールド名	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 Installer）]：Windows OS ソフトウェアの AMP をホストするローカルサーバーの 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 Installer）]：MacOS ソフトウェアの AMP をホストするローカルサーバーの 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、サーバーと通信を行って 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

Cisco 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。

Cisco ISE 埋め込みプロファイルエディタを使用して AMP 有効化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 サーバーでホスティングします。
- エンドポイントのソフトウェアの AMP をホストするサーバーの証明書を ISE 証明書ストアにインポートします。[管理（Administration）]Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、 > [証明書（Certificates）] > **[信頼できる証明書（Trusted Certificates）]**の順に選択します。
- [AMPイネーブラ（AMP Enabler）] オプションが **[AnyConnect設定（AnyConnect Configuration）]** 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モジュールの選択（AnyConnect Module Selection）]** および[プロファイルの選択（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、MacOS の場合はエンドポイントソフトウェアの AMP の再配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ーでホストされます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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 Provision）]** > **[リソース（Resources）]**の順に選択します。

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 （117 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）]** 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モジュールの選択（AnyConnect Module Selection）]** および[プロファイルの選択（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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]**の順に選択します。

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ーの証明書が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ーがダウンした場合、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 ユーザー/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。ユーザーアクセスの制御、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 ユーザーの 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。
- サーバー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、ユーザー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ー用に証明書を生成します。
  - 複数のユーザーで共有される 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 サーバー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 定義リストで許可されていることを確認します。Google サポートページの推奨および許可されているホスト名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 ユーザーの 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 ユーザー：

- 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ー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。

- 特定のユーザー（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、ユーザーの名前が証明書の [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ーの 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、特定のユーザーの 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。
- Cisco 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。
- Cisco 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 オンボーディング用の Cisco 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) 必要なユーザー名とパスワードを入力します。
c) [管理コンソールへようこそ（Welcome to Admin Console）] ウィンドウで、[デバイス管理（Device Management）] をクリックします。
d) [デバイス管理（Device Management）] ウィンドウで、[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。ユーザーがオープン ネットワークに接続すると、Cisco ISE ACL は、認証のために、ユーザー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 はユーザーを 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「サーバー認証局」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）] ウィンドウの [デバイス設定（Device Settings）] の下にある [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）] ウィンドウで、[Chrome Web 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）複数のユーザーに共有されている 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 で複数のユーザー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 ユーザー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 ユーザー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) [証明書（Certificates）] ウィンドウで、[証明書の追加（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 オンボードのための Cisco ISE の設定

Chromebook オンボーディング用の Cisco ISE の設定

始める前に

Cisco ISE 管理者は、必要なポリシーを作成する必要があります。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**(ポリシー（Policy）]** > **[ポリシーセット（Policy Sets）]** ウィンドウを選択します。

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、設定された認証結果です。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可（Authorization）]** > **[認証プロファイル（Authorization Profiles）]** ウィンドウを選択します。

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) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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。

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、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。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）][システム（System）][設定（Settings）][ポスチャ（Posture）][更新（Updates）]** ウィンドウを選択します。

b) **[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。

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

d) **[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。

e) **[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。

f) [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) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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。

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 ユーザー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 ユーザー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 ユーザーは最初に 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ー名とパスワード、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 ユーザーのユーザー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 ユーザー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、[ユーザー名（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 ユーザーは、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 ユーザーに対し、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	—

フィールド	EAP-TLS	PEAP	オープン（Open）
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	—	—	—
[ユーザー名（Username）]	必要に応じて、固定値を設定するか、またはユーザー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 ユーザー / 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。	—
サーバー認証局（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。	—

フィールド	EAP-TLS	PEAP	オープン（Open）
クライアントの登録 URL	登録されていないユーザーに対して 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。未登録のユーザー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ー

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。認証方式（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。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[操作（Operations）]** > **[RADIUS]** > **[ライブログ（Live Logs）]** ウィンドウを選択します。また、Chromebook デバイスとして分類されるエンドポイントの数を特定することもできます。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ワークセンター（Work Centers）]** > **[ネットワークアクセス（Network Access）]** > **[ID（Identities）]** > **[エンドポイント（Endpoints）]** ウィンドウを選択します。

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：ユーザーは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 ユーザー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、ユーザーがドメインユーザー 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ーを追跡します。ただし、ドメインユーザーは登録されていないデバイスのユーザー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、ユーザー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 Cisco AnyConnect で統合モジュールを使用します。

（注） 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）][ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] >[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）]** ウィンドウの **[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。

Cisco ISE を Cisco 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。

- Cisco AnyConnect 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ーとして機能する
- 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
- Cisco AnyConnect プロファイル、カスタマイズおよび言語パッケージ、ならびに 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
- Cisco AnyConnect およびレガシーエージェントを同時にサポートする

（注） ネットワークのメディアを切り替えるときに、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。

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、ユーザーがクライアントで 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。ISE と ASA の両方を使用して AnyConnect を展開する場合は、両方のヘッドエンドで設定が一致している必要があります。

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。

（注） Cisco ISE が ASA と統合されている場合は、ASA でアカウンティングモードが [シングル（Single）] に設定されていることを確認します。アカウンティングデータは、シングルモードでは 1 つのアカウンティングサーバーにのみ送信されます。

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 （111 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 （112 ページ）を参照）。
4. AnyConnect 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 （139 ページ）を参照）。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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 Provision）]** > **[リソース（Resources）]** の順に選択します。

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の設定（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。例：AnyConnectDesktopWindows xxx.x.xxxxx.x.

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。例：AnyConnectComplianceModulewindows x.x.xxxx.x

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 カスタマイゼーション 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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）] ウィンドウのフィールドを示します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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ポスチャプロファイル（AnyConnect Posture Profile）]**。

フィールド名	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、ユーザー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。
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。

フィールド名	デフォルト値（Default Value）	使用上のガイドライン
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 サーバーからの新しい 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。
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、AnyConnect のポスチャプロトコル設定を設定できる [AnyConnectポスチャプロファイル（AnyConnect Agent Posture Profile）] ウィンドウのフィールドを示します。詳細については、ご使用のバージョンの AnyConnect の『Cisco AnyConnect Secure Mobility Client Administrator Guide』を参照してください。

フィールド名	デフォルト値（Default Value）	使用上のガイドライン
[PRA 再送信時間（PRA Retransmission Time）]	120 秒	パッシブ再アセスメントで通信障害がある場合のエージェントの再試行期間です。
[再送遅延（Retransmission Delay）]	60 秒	再試行までの待機時間（秒）。
[再送の制限（Retransmission Limit）]	4	メッセージに対して許可される再試行回数。
[ホストの検出（Discovery Host）]	—	NAD を介してルーティングされる任意の IP アドレスまたは FQDN を入力します。NAD はその HTTP トラフィックを検出し、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します。
[バックアップサーバーリストの検出（Discovery Backup Server List）]	—	ドロップダウンリストから PSN を選択します。AnyConnect は、このサーバーリストをプローブして、ポスチャを実行する必要がある PSN ノードを見つけます。PSN を選択しない場合、ノードグループまたはクラスタ内のすべての PSN がバックアップサーバーリストとして AnyConnect に送信されます。
サーバ名ルール（Server Name Rules）	—	エージェントが接続できるサーバーを定義する、ワイルドカード対応のカンマで区切られた名前のリスト。
[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。

フィールド名	デフォルト値（Default Value）	使用上のガイドライン
[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。有効な範囲は 10 ～ 600 秒です。

継続的なエンドポイント属性モニターリング

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ーします。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ーします。この機能をオンまたはオフにできます。また、データのモニター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。AnyConnect は初回ポスチャ時に、実行中のアプリケーションと搭載アプリケーションの一覧を報告します。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ーに送信します。サーバー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。

双方向ポスチャフロー

ネットワーク設定の変更により、Cisco ISE がクライアントまたはエンドポイントを「保留（Pending）」状態に移行する場合があります。ただし、AnyConnectはこの変更を検出できず、クライアントまたはエンドポイントを「準拠（Compliant）」状態で維持します。したがって、ポスチャステータスに不一致があり、理想的には、このシナリオで正しいポスチャステータスを取得するために Cisco ISE がプローブされる必要があります。指定された間隔で Cisco ISE をプローブするように AnyConnect を設定することで、これを実行できます。それにより、Cisco ISEでクライアントまたはエンドポイントのポスチャステータスが保留状態の場合、プローブによってクライアントまたはエンドポイントが保留状態のままになるのを防ぐことができます。

双方向ポスチャフローは、Windows、Linux、および MacOS クライアントでサポートされます。

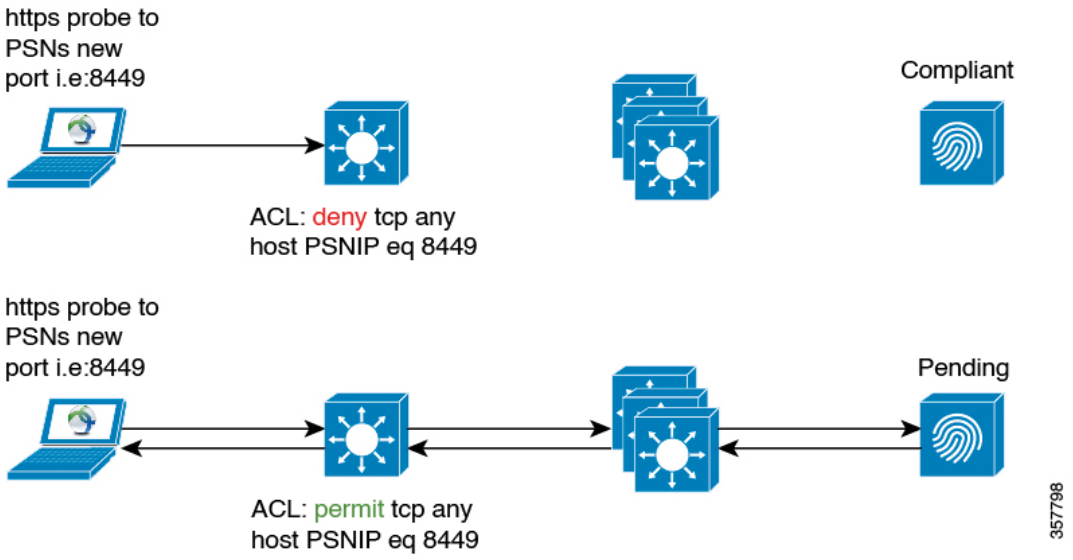
双方向ポスチャフローには、次の手順が含まれます。

1. クライアントがネットワークへの接続を試行します。

2. PSN がポスチャフローを実行します。クライアントがポスチャポリシーに準拠している場合、エンドポイントは準拠状態に移行します。
3. AnyConnect エージェントが、Cisco ISE から [ポスチャプロービングバックアップリスト（Posture Probing Backup List）] および [ポスチャ状態同期間隔（Posture State Synchronization Interval）] の設定の詳細を受信します。
4. AnyConnect エージェントが、指定された間隔で Cisco ISE のプローブを開始します。

   たとえば、Cisco ISE はポスチャステータスを [保留（Pending）] と表示し、AnyConnect はポスチャステータスを [準拠（Compliant）] と表示します。AnyConnect が Cisco ISE をプローブし、新しい状態を学習すると、再評価がトリガーされます。

図 5 : 双方向ポスチャフロー



（注） 何らかの理由でクライアントのステータスが「**保留（Pending）**」に移行した場合、AnyConnect エージェントはクライアントからプローブ要求を受け取ります。これにより、正しいクライアント状態を調べて Cisco ISE から受信し、クライアントを正しい状態に移行します。

双方向ポスチャフローの設定

ステップ 1 **[AnyConnectポスチャプロファイル（AnyConnect Posture Profile）]** で **[ポスチャプロービングバックアップリスト（Posture Probing Backup List）]** と **[ポスチャ状態同期間隔（Posture State Synchronization Interval）]** を設定します。手順は次のとおりです。

a) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、[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。

b) **[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。

c) [エージェントの動作（Agent Behavior）] 領域で、次の設定を行います。

- **[ポスチャプロービングバックアップリスト（Posture Probing Backup List）]**：AnyConnect がエンドポイントのポスチャ コンプライアンス ステータスをプローブする必要がある PSN を選択します。最大 6 つの PSN を選択できます。

  AnyConnect は、これらの PSN にプローブを送信して、エンドポイントのポスチャ コンプライアンス ステータスがまだ有効かどうかを確認します。PSN を選択しない場合、接続された PSN と任意の 2 台のバックアップサーバーがポスチャ状態同期のバックアップとして使用されます。

- **[ポスチャ状態同期間隔（Posture State Synchronization Interval）]**：AnyConnect がポスチャステータスを Cisco ISE と同期する頻度を定義します。有効な範囲は 0 ～ 300 です。0 を入力すると、ポスチャ状態同期プローブが無効になります。この値が 0 より大きい場合は、ポスチャ状態同期ポートを準拠認証プロファイルに対してブロックする必要があります。

ステップ 2 ポート 8449 を双方向通信用に設定します。手順は次のとおりです。

a) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、[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）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] を選択します。

b) [ポータル設定（Portal Settings）] をクリックします。

c) [双方向ポート（Bidirectional Port）] フィールドで、ポート 8449 が双方向通信用に設定されていることを確認します。

デフォルトでは、ポート 8449 は双方向通信に使用されます。

ステップ 3 クライアント ポスチャ ステータスが準拠している場合、ポスチャ状態同期プローブが Cisco ISE に到達しないように ACL を設定します。手順は次のとおりです。

a) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [ダウンロード可能 ACL（Downloadable ACLs）] を選択します。

b) ACL を設定します。

保留状態のクライアントのみが、双方向ポートを介して設定済みの PSN に到達できることを確認します。これにより、準拠状態のクライアントからの不要なトラフィックが回避されます。次に、ACL の例を示します。

```
deny tcp any host <ip address> eq 8449
deny tcp any host <ip address> eq 8449
deny tcp any host <ip address> eq 8449
permit ip any any
```

ACL が設定されていない場合、Cisco ISE ダッシュボードで、ポスチャ設定検出アラームがトリガーされます。ACL は、問題のあるポリシー セットでのみ設定する必要があります。このアラームの主な目的は、Cisco ISE への大量のトラフィックを防ぐことです。

（注） クライアントが保留状態のときに、対応するポートの通信がファイアウォールによってブロックされないようにします。

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 アセスメントを提供します。

ユーザーは 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、ユーザーがログインすると、ユーザー 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 サーバーから取得し、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 サーバーに送信します。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、ユーザー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、ユーザー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、ユーザー 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、クライアント プロビジョニング リソースのポリシーによって、ログイン時とユーザーセッション開始時にどのユーザーがどのバージョンのリソース（エージェント、エージェント対応モジュール、およびエージェント カスタマイゼーション パッケージまたはプロファイル）を Cisco ISE から受信するかが決まります。

AnyConnect の場合、[クライアント プロビジョニング リソース（Client Provisioning Resources）] ウィンドウからリソースを選択して、[クライアント プロビジョニング ポリシー（Client Provisioning Policy）] ウィンドウで使用できる AnyConnect 設定を作成できます。AnyConnect

設定では、AnyConnect ソフトウェアと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を指定します。ファイルには、 Windows クライアント、MacOS クライアント、および Linux 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、カスタマイズパッケージ、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非表示時にイネーブルにする（Enable if target network is hidden）] チェックボックスをオンにします。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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。

ステップ 2 [Behavior] ドロップダウンリストから、次のオプションのいずれかを選択します。

- [有効化（Enable）] : ユーザー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。
- [無効化（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。
- [モニター（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「モニター対象」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ーが属する 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、[Any] 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、ユーザーが 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。

（注） Cisco ISE の GUI の **[クライアント プロビジョニング（Client Provisioning）]** ウィンドウには MacOS 10.6、10.7、および 10.8 を選択するオプションはありますが、AnyConnect はこれらのバージョンをサポートしていません。

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）] オプションを使用して、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、および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 URL を認証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 アセスメントを要求できるようになります。

ステップ 8 [保存（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アセスメントを実行するように 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、ユーザー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

ユーザーがログインするとき、そのユーザー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、ユーザー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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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ーが属する 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、ユーザーが 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 のモニター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、ユーザー 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ー（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ー（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ー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（ユーザー ID）、IP アドレス、MAC アドレス（エンドポイント ID）、サーバー 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

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[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）]** を選択します。

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、**[ブロック済みリスト（Blocked List）]** 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は、PSN はポータルの設定時に、最初にボンディング インターフェイスの設定を試みます。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）]：ユーザー認証に使用する ID ソース順序（ISS）または ID プロバイダ（IdP）を選択します。ISS は、ユーザー 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 ユーザー、内部ユーザー、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、ユーザー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 サーバー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 をユーザーに通知する必要があります。

- [アイドルタイムアウト（Idle Timeout）]：ポータルにアクティビティがない場合にユーザー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 ポスチャ 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

- [レート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）]：**[レート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、ユーザー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契約条件を、現在ユーザー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ーが AUP を受け入れることを要求します。[ログイン（Login）] ボタンは、ユーザーが 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ーは、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。ユーザーが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザーが 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の契約条件を、別のページでユーザーに表示します。
- [AUP の最後までのスクロールが必要（Require scrolling to end of AUP）]：ユーザーが AUP を完全に読んだことを確認します。[同意（Accept）] ボタンは、ユーザーが 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）]：ユーザー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）]：ユーザー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ー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）]：ユーザー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）

[内部ユーザー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。

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

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[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）]**を選択します。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

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。