CHAPTER 22

クライアント プロビジョニングの設定

この章では、クライアント リソースのクライアント プロビジョニングをダウンロードして、Windows および MAC OS X クライアントのエージェント プロファイルとを独自のパーソナル デバイスのネイティブ サプリカント プロファイルを設定する Cisco ISE クライアント プロビジョニング機能について説明します。

クライアント プロビジョニング リソースのタイプ

クライアント プロビジョニング リソース ポリシーにより、クライアント デバイスにリソースをダウンロードしてインストールすることが可能になります。以下にアクセスし取り込む前に、これらのリソースが Cisco ISE にインストールされている必要があります：

- 永続的なエージェントおよび一時的なエージェント：

  - Windows および Mac OS X の Cisco ネットワーク アドミッション コントロール（NAC）エージェント
  - Cisco NAC Web Agent
- ネイティブ サプリカント プロファイル
- エージェント プロファイル
- ネイティブ サプリカント プロビジョニング/インストール ウィザード
- エージェント準拠モジュール
- エージェント カスタマイゼーション パッケージ

関連項目

- 「リモート ソースからのクライアント プロビジョニング リソースの追加」（P.22-3）
- 「ローカル マシンからのクライアント プロビジョニング リソースの追加」（P.22-3）
- 「クライアント プロビジョニング リソースの自動ダウンロード」（P.22-4）
- 「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」（P.22-30）

クライアント プロビジョニングの有効化と無効化

はじめる前に

クライアント プロビジョニング リソースを Cisco ISE にダウンロードできる適切なリモートの場所にアクセスできるようにするには、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。

ステップ 1　[管理（Administration）] > [システム（System）] > [設定（Settings）] > [クライアント プロビジョニング（Client Provisioning）] を選択します。

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、[有効（Enable）] または [無効（Disable）] を選択します。

ステップ 3　[保存（Save）] をクリックします。

Cisco ISE のこの機能を無効にすることを選択した場合、ネットワークにアクセスしようとするユーザは、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を受信します。

次の作業

次の項のガイドラインに従って、クライアント プロビジョニング機能をシステム全体にセット アップします。

- 「リモート ソースからのクライアント プロビジョニング リソースの追加」（P.22-3）
- 「ローカル マシンからのクライアント プロビジョニング リソースの追加」（P.22-3）
- 「クライアント プロビジョニング リソースの自動ダウンロード」（P.22-4）
- 「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」（P.22-30）

関連項目

- 「Cisco ISE でのプロキシ設定の指定」（P.5-3）

- 「リモート クライアントのプロビジョニング リソースをダウンロードできない」（P.G-13）

リモート ソース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.com などのリモート ソースからクライアント プロビジョニング リソースを追加できます。選択したリソースと使用可能なネットワーク帯域幅選択に応じて、新しい項目をダウンロードして、使用可能なクライアント プロビジョニング リソースの一覧を表示するのに、Cisco ISE は数秒または数分かかる場合があります。

はじめる前に

ネットワークのプロキシ設定が正しく設定されていることを確認し、適切なリモート ロケーションにアクセスして、クライアント プロビジョニング リソースを Cisco ISE にダウンロードできることを確認します。

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

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

ステップ 3　[ダウンロードしたリモート リソース（Downloaded 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リソースを 1 つ以上選択します。

ステップ 4　[保存（Save）] をクリックします。

次の作業

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。

関連項目

- 「Cisco ISE でのプロキシ設定の指定」（P.5-3）
- 「クライアント プロビジョニング リソースのタイプ」（P.22-1）
- 「ローカル マシンからのクライアント プロビジョニング リソースの追加」（P.22-3）
- 「クライアント プロビジョニング リソースの自動ダウンロード」（P.22-4）
- 「エージェント カスタマイゼーション ファイルの作成」（P.22-13）
- 「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」（P.22-30）
- 「リモート クライアントのプロビジョニング リソースをダウンロードできない」（P.G-13）

ローカル マシンからのクライアント プロビジョニング リソースの追加

ローカル マシンから既存のクライアント プロビジョニング リソースを追加できます（たとえば、Cisco.com からラップトップにダウンロードしたファイル）。

はじめる前に

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。古いサポートされていないリソース（たとえば、Cisco NAC Agent の古いバージョン）を使用すると、クライアント アクセスで重大な問題が発生する場合があります。詳細については、『*Cisco Identity Services Engine Network Component Compatibility, Release 1.2*』を参照してください。

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、『*Release Notes for the Cisco Identity Services Engine, Release 1.2*』の「Cisco ISE Offline Updates」の項を参照してください。

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

ステップ 2　[追加（Add）] > [ローカル ディスクからリソースを追加（Add resource from local disk）] を選択します。

ステップ 3　[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 4　検索ウィンドウでリソース ファイルを強調表示し、[保存（Save）] をクリックします。

次の作業

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。

関連項目

- 「Cisco ISE でのプロキシ設定の指定」（P.5-3）
- 「クライアント プロビジョニング リソースのタイプ」（P.22-1）
- 「リモート ソースからのクライアント プロビジョニング リソースの追加」（P.22-3）
- 「クライアント プロビジョニング リソースの自動ダウンロード」（P.22-4）
- 「エージェント カスタマイゼーション ファイルの作成」（P.22-13）
- 「エージェント プロファイル設定のガイドライン」（P.22-15）
- 「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」（P.22-30）

クライアント プロビジョニング リソースの自動ダウンロード

この機能は、Cisco からのすべての使用可能なソフトウェアをアップロードしますが、多くの項目が展開に適していない場合があります。

はじめる前に

クライアント プロビジョニング リソースを Cisco ISE にダウンロードできる適切なリモートの場所にアクセスできるようにするには、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。ネットワークで URL リダイレクト機能（プロキシ サーバ経由など）を制限しているために、デフォルトの URL へのアクセスに問題がある場合は、Cisco ISE で https://www.perfigo.com/ise/provisioning-update.xml を指定してください。

クライアント プロビジョニング リソースをダウンロードするデフォルトの URL は、https://www.cisco.com/web/secure/pmbu/provisioning-update.xml です。

シスコは、自動的なアップロードをせずに、可能な限り手動でリソースをアップロードすることを推奨します。

ステップ 1　[管理（Administration）] > [システム（System）] > [設定（Settings）] > [クライアント プロビジョニング（Client Provisioning）] を選択します。

ステップ 2　[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。

ステップ 3　[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。

ステップ 4　[保存（Save）] をクリックします。

次の作業

次の項のガイドラインに従って、クライアント プロビジョニング機能をシステム全体にセット アップします。

- 「リモート ソースからのクライアント プロビジョニング リソースの追加」（P.22-3）
- 「ローカル マシンからのクライアント プロビジョニング リソースの追加」（P.22-3）
- 「クライアント プロビジョニング リソースの自動ダウンロード」（P.22-4）
- 「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」（P.22-30）

関連項目

- 「Cisco ISE でのプロキシ設定の指定」（P.5-3）
- 「リモート クライアントのプロビジョニング リソースをダウンロードできない」（P.G-13）

クライアント ログイン セッションの基準

Cisco Identity Services Engine（ISE）では、内部ネットワークにユーザがアクセスするときに使用するログイン セッションのタイプを分類する場合に、次のようなさまざまな要素を調べます。

- クライアント マシンのオペレーティング システムおよびバージョン
- クライアント マシンのブラウザ タイプおよびバージョン
- ユーザが属するグループ
- （適用したディクショナリ属性に基づく）条件評価結果

Cisco ISE は、クライアント マシンを分類した後、クライアント プロビジョニング リソース ポリシーを使用して、適切なエージェント バージョン、アンチウイルスとアンチスパイウェアのベンダー サポートに対する最新のコンプライアンス モジュール、および（必要に応じて）正しいエージェント カスタマイゼーション パッケージとプロファイルで、クライアント マシンが設定されていることを確認します。

Cisco ISE エージェント

エージェントとは、Cisco ISE ネットワークにログインしているクライアント マシンに存在するアプリケーションです。エージェントは、クライアントがネットワークにログインしていない場合でもインストール後に永続的に留まることも（Cisco NAC Agent または Mac OS X エージェントなど）、一時的な

存在としてログイン セッション終了後は自身をクライアント マシンから削除することもできます（Cisco NAC Web Agent など）。いずれの場合も、エージェントはネットワークにログインし、適切なアクセス プロファイルを受け取り、クライアント マシンでポスチャ評価を実行してネットワークのコアにアクセスする前にネットワーク セキュリティ ガイドラインに従うようにします。

Windows クライアント用 Cisco NAC Agent

Cisco NAC Agent には、クライアント マシンに対して、ポスチャ評価および修復を行う機能があります。

ユーザは Cisco NAC Agent（読み取り専用クライアント ソフトウェア）をダウンロードしてインストールし、ホストのレジストリ、プロセス、アプリケーション、およびサービスをチェックすることができます。Cisco NAC Agent を使用すると、Windows の更新またはアンチウイルスやアンチスパイウェアの定義の更新を実行したり、正規の修復プログラムを起動したり、Cisco ISE サーバにアップロードされたファイルを配布したり、ユーザがファイルをダウンロードしてシステムを修復できるように Web サイト リンクを Web サイトに配布したり、情報や手順を配布したりすることができます。

シスコは、最新の Windows ホット フィックスとパッチが Windows XP クライアントにインストールされ、Cisco NAC Agent が安全で暗号化された Cisco ISE との通信を確立できることが保障されることを推奨します（SSL over TCP など）。

Windows クライアント用 Cisco NAC Agent のアンインストール

NAC Agent は Windows クライアントの **C:\Program Files\Cisco\Cisco NAC Agent** にインストールされます。Agent は、次の方法でアンインストールできます。

- [Uninstall Cisco NAC Agent] デスクトップ アイコンのダブルクリック
- [Start Menu] > [Programs] > [Cisco Systems] > [Cisco Clean Access] > [Uninstall Cisco NAC Agent]
- [Start Menu] > [Control Panel] > [Add or Remove Programs] > [Cisco NAC Agent]

Windows 8 クライアントの Cisco NAC Agent をアンインストールするには、次を手順を実行します。

ステップ 1　メトロ モードに切替えます。

ステップ 2　[Cisco NAC Agent] タイルを右クリックします。

ステップ 3　画面下部にあるオプションから [アンインストール（Un-Install）] を選択します。

ステップ 4　システムが自動的にデスクトップ モードに切替わり、[追加/削除（Add/Remove）] コントロール パネルが開きます。

ステップ 5　[追加/削除（Add/Remove）] コントロール パネルで、次のいずれかの操作を行います。

- [Cisco NAC Agent] をダブル クリックします。
- [Cisco NAC Agent] を選択し、[アンインストール（Uninstall）] をクリックします。
- [Cisco NAC Agent] を右クリックし、[アンインストール（Uninstall）] を選択します。

関連項目

- 『*Cisco Identity Services Engine Network Component Compatibility, Release 1.2*』

Windows 8 メトロおよびメトロ アプリケーションのサポート：Toast 通知

[Toast 通知の有効化（Enable Toast Notification）] オプションは、Windows 8 を使用しているクライアントに対してのみ、Cisco NAC Agent Tray アイコンが用意されています。ユーザに関連する通知を送信するには、このオプションを有効します。

Cisco NAC Agent で、「修復で障害発生」や「ネットワーク アクセスの期限切れ」などのためにユーザがネットワーク アクセスを取得できなかったといような場合は、エージェントが次のような Toast 通知を表示します。

Network not available, Click "OK" to continue

詳細を取得するには、toast を選択すると、デスクトップ モードにリダイレクトされ、NAC Agent ダイアログが表示されます。

Toast 通知は、ネットワーク アクセスを取得するために実行する必要があるすべてのプラス推奨処置に対して表示されます。次に例を示します。

- ネットワーク受信ポリシーの場合は、「Click Accept to gain network access」という toast が表示されます。
- エージェント / コンプライアンス モジュールのアップグレードの場合は、「Click OK to Upgrade/Update」という toast が表示されます。
- 「user logged out」イベントでは、CAM でログオフの「Auto Close」オプションが有効でない場合に、toast 通知が表示されます。この toast により、ユーザがログアウトされており、ネットワークにアクセスするには再度ログインする必要があることが分かります。

Macintosh クライアント用 Cisco NAC Agent

Mac OS X Agent により、Macintosh クライアント マシンはポスチャ評価および修復を実行できます。

ユーザは Mac OS X Agent（読み取り専用クライアント ソフトウェア）をダウンロードしてインストールし、アンチウイルスおよびアンチスパイウェアの定義の更新をチェックすることができます。

Mac OS X Agent は、ユーザがログインすると、ユーザ ロールまたはオペレーティング システムに設定された要件を Cisco ISE サーバから取得し、必要なパッケージをチェックし、レポートを Cisco ISE サーバに送信します。クライアントに関する要件が満たされている場合、ユーザはネットワークにアクセスできます。要件が満たされていない場合、エージェントは満たされていない要件ごとに、ユーザにダイアログを表示します。ダイアログにより、クライアント マシンの要件を満たすための手順および対処法が提供されます。あるいは、指定された要件が満たされない場合は、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。

関連項目

- 『*Cisco Identity Services Engine Network Component Compatibility, Release 1.2*』

Macintosh クライアントの Cisco NAC Agent のアンインストール

次のアンインストール スクリプトを実行して、Mac OS X クライアントの NAC Agent をアンインストールできます。

ステップ 1　ナビゲータ ペインを開き、<*local drive ID*> > [Applications] に移動します。

ステップ 2　[CCAAgent] アイコンを強調表示して右クリックし、選択メニューを表示します。

ステップ 3　[パッケージ コンテンツの表示（Show Package Contents）] を選択し、[NacUninstall] をダブル クリックします。

ステップ 4　これで Mac OS X Agent はアンインストールされます。

Cisco NAC Web Agent

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

ユーザは Cisco NAC 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。Web Agent は Windows クライアントのみ使用可能で、Mac OS X クライアントは使用できません。

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

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

関連項目

- 『*Cisco Identity Services Engine Network Component Compatibility, Release 1.2*』

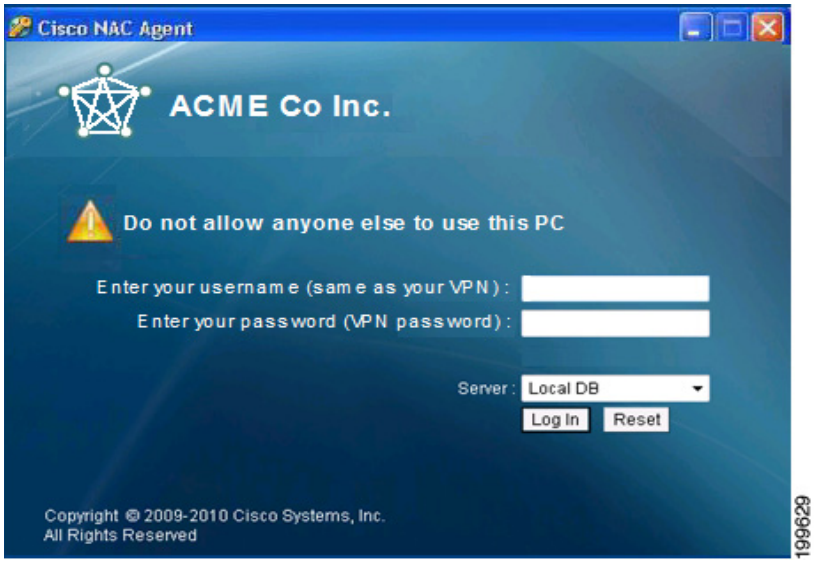
エージェント ログイン画面のカスタマイズ

Cisco NAC Agent ログイン画面に表示される要素をカスタマイズできます。これらの要素をカスタマイズすると、最後の .zip ファイル（Agent ログインのカスタマイゼーション パッケージ）パッケージの「updateFeed.xml」XML ディスクリプタ ファイルと組み合わせて、Cisco ISE にアップロードできます。

nac_login.xml ファイルを変更し、デフォルトの Cisco ロゴを「nac_logo.gif ファイル」という名前の .gif ファイル形式の自社ロゴに置き換え、「nacStrings_*xx*.xml」ファイルを 1 つ以上作成すると、Windows クライアント ユーザは Cisco NAC Agent を介してネットワークにアクセスできます。

図 22-1　Cisco NAC Agent ログイン：デフォルト画面

図 22-2　Cisco NAC Agent ログイン：サンプル カスタマイズ画面



関連項目

- 「カスタム nac_login.xml ファイル テンプレート」（P.22-10）
- 「カスタム企業 / 会社ロゴの使用」（P.22-10）
- 「カスタム nacStrings_xx.xml ファイル テンプレート」（P.22-11）
- 「UpdateFeed.xml ディスクリプタ ファイルのテンプレート」（P.22-12）
- 「エージェント カスタマイゼーション ファイルの作成」（P.22-13）
- 「エージェント XML ファイルのインストール ディレクトリ」（P.22-14）

カスタム nac_login.xml ファイル テンプレート

Agent ログインのカスタマイゼーション パッケージに必要なファイルの 1 つであり、これにより Cisco NAC Agent ログイン ダイアログのロゴ、フィールド、メッセージ テキストをカスタマイズして、特定の Windows クライアントをネットワークのアクセス要件に合致させることができます。

適切な「nac_login.xml」ファイルを作成するには、次のテンプレートを使用します。

次の例では、カスタマイズしたテキストを太字で示しています。

```
<tr class="nacLoginMiddleSectionContainerInput">
   <td colspan="2">
      <fieldset width="100%" id="nacLoginCustomAlert"
                style="display:block" class="nacLoginAlertBox">
          <table width="100%">
             <tr>
                <td id="nacLoginCustomAlert.img" valign="top" width="32px">
                  <img src="./cues_icons/Status_warning_icon.png" align="absmiddle"
onload="cuesFixPNG(null,this)"></img>
                </td>
                <td id="nacLoginCustomAlert.content" class="nacLoginAlertText">
                  <cues:localize key="login.customalert"/>
                </td>
              </tr>
          </table>
       </fieldset>
    </td>
</tr>
<tr id="nacLoginRememberMe" style="visibility:hidden">
    <td>
       <cues:localize key="cd.nbsp"/>
    </td>
    <td class="cuesLoginField">
      <nobr>
      <input type="checkbox" alt="" title="" name="rememberme"
             id="rememberme" checked="true"/>
            <cues:localize key="login.remember_me"/>
      </nobr>
    </td>
</tr>
```

関連項目

- 「エージェント ログイン画面のカスタマイズ」（P.22-8）
- 「カスタム企業 / 会社ロゴの使用」（P.22-10）
- 「カスタム nacStrings_xx.xml ファイル テンプレート」（P.22-11）
- 「サンプル拡張 nacStrings_xx.xml ファイル」（P.22-12）
- 「UpdateFeed.xml ディスクリプタ ファイルのテンプレート」（P.22-12）
- 「エージェント カスタマイゼーション ファイルの作成」（P.22-13）
- 「エージェント XML ファイルのインストール ディレクトリ」（P.22-14）

カスタム企業 / 会社ロゴの使用

すべての Cisco NAC Agent 画面に表示されている Cisco ロゴを、自分の企業 / 企業ロゴの置き換えることができます。

はじめる前に

Agent ログインのカスタマイゼーション パッケージに必要なファイルの 1 つであり、これにより Cisco NAC Agent ログイン ダイアログのロゴ、フィールド、メッセージ テキストをカスタマイズして、特定の Windows クライアントをネットワークのアクセス要件に合致させることができます。

イメージが 67 x 40 ピクセルを超えない .gif ファイルであることを確認してください。イメージの名前が「nac_logo.gif」であることを確認してください。

関連項目

- 「エージェント ログイン画面のカスタマイズ」（P.22-8）
- 「カスタム nac_login.xml ファイル テンプレート」（P.22-10）
- 「カスタム nacStrings_xx.xml ファイル テンプレート」（P.22-11）
- 「サンプル拡張 nacStrings_xx.xml ファイル」（P.22-12）
- 「UpdateFeed.xml ディスクリプタ ファイルのテンプレート」（P.22-12）
- 「エージェント カスタマイゼーション ファイルの作成」（P.22-13）
- 「エージェント XML ファイルのインストール ディレクトリ」（P.22-14）

カスタム nacStrings_*xx*.xml ファイル テンプレート

Agent ログインのカスタマイゼーション パッケージに必要なファイルの 1 つであり、これにより Cisco NAC Agent ログイン ダイアログのロゴ、フィールド、メッセージ テキストをカスタマイズして、特定の Windows クライアントをネットワークのアクセス要件に合致させることができます。

次のテンプレートを使用して、1 つ以上の nacStrings_xx.xml ファイルを作成します。ここで、*xx* は特定言語の 2 文字の ID です。

次の例では、カスタマイズしたテキストを太字で示しています。

```
<cueslookup:name key="login.productname"> XYZ Co Inc. </cueslookup:name>
<cueslookup:name key="login.version">Version</cueslookup:name>
<cueslookup:name key="login.username"> Enter your username (same as your VPN)
</cueslookup:name>
<cueslookup:name key="login.password">Enter your password (VPN password)</cueslookup:name>
<cueslookup:name key="login.remember_me">Remember Me</cueslookup:name>
<cueslookup:name key="login.server">Server</cueslookup:name>
<cueslookup:name key="login.customalert">Do not allow anyone else to use this
PC</cueslookup:name>
<cueslookup:name key="login.Too many users using this account">This account is already
active on another device</cueslookup:name>
<cueslookup:name key="login.differentuser">Login as Different User</cueslookup:name>
<cueslookup:name key="login.removeoldest">Remove Oldest Login Session</cueslookup:name>
```

（注） カスタマイズしたテキストに使用できる文字数に制限はありません。ただし、カスタマイズされたログイン画面がクライアント上に表示された場合に、あまり大きな領域を必要としないように長さを制限することをシスコは推奨します。

関連項目

- 「エージェント ログイン画面のカスタマイズ」（P.22-8）
- 「カスタム nac_login.xml ファイル テンプレート」（P.22-10）
- 「カスタム企業/会社ロゴの使用」（P.22-10）
- 「サンプル拡張 nacStrings_xx.xml ファイル」（P.22-12）

サンプル拡張 nacStrings_*xx*.xml ファイル

```
<cueslookup:name key="dp.status.fullNetAccess">Full Network Access</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccess.verbose">Your device conforms with all the
security policies for this protected network</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccessWarn.verbose">Only optional requirements are
failing. It is recommended that you update your system at your earliest
convenience.</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.progress.verbose">Refreshing IP address. Please
Wait ...</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.complete.verbose">Refreshing IP address
succeeded.</cueslookup:name>
<cueslookup:name key="dp.status.vlanchange.progress.verbose">Connecting to protected
Network. Please Wait ...</cueslookup:name>
<cueslookup:name key="dp.status.guestNetAccess">Guest Network Access</cueslookup:name>
<cueslookup:name key="dp.status.noNetAccess">Network Access Denied</cueslookup:name>
<cueslookup:name key="dp.status.noNetAccess.verbose">There is at least one mandatory
requirement failing. You are required to update your system before you can access the
network.</cueslookup:name>
<cueslookup:name key="dp.status.rejectNetPolicy.verbose">Network Usage Terms and
Conditions are rejected. You will not be allowed to access the network.</cueslookup:name>
<cueslookup:name key="dp.status.RestrictedNetAccess">Restricted Network Access
granted.</cueslookup:name>
<cueslookup:name key="dp.status.RestrictedNetAccess.verbose">You have been granted
restricted network access because your device did not conform with all the security
policies for this protected network and you have opted to defer updating your system. It
is recommended that you update your system at your earliest convenience.</cueslookup:name>
<cueslookup:name key="dp.status.temporaryNetAccess">Temporary Network
Access</cueslookup:name>
<cueslookup:name key="dp.status.temporaryNetAccess.bepatient.verbose">Please be patient
while your system is checked against the network security policy.</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure">Performing
Re-assessment</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure.verbose">There is at least one
mandatory requirement failing. You are required to update your system otherwise your
network access will be restricted.</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure">Performing
Re-assessment</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure.verbose">Only optional requirements
are failing. It is recommended that you update your system at your earliest
convenience.</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout">Logged out</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout.verbose">Temporary Access to the network
has expired.</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated">Logged out</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated.verbose"> </cueslookup:name>
```

UpdateFeed.xml ディスクリプタ ファイルのテンプレート

Agent ログインのカスタマイゼーション パッケージに必要なファイルの 1 つであり、これにより Cisco NAC Agent ログイン ダイアログのロゴ、フィールド、メッセージ テキストをカスタマイズして、特定の Windows クライアントをネットワークのアクセス要件に合致させることができます。

Agent ログイン カスタマイゼーション パッケージを完了する前、適切な **updateFeed.xml** XML ディスクリプタ ファイルを構築する必要があります。カスタマイゼーション パッケージに必要な updateFeed.xml ファイルのセット アップには、次の例をテンプレートとして使用します。

```
<?xml version="1.0" encoding="utf-8"?>
<feed xmlns="http://www.w3.org/2005/Atom"
xmlns:update="http://www.cisco.com/cpm/update/1.0">
   <title>Provisioning Update</title>
   <updated>2011-12-21T12:00:00Z</updated>
   <id>https://www.cisco.com/web/secure/pmbu/provisioning-update.xml</id>
   <author>
      <name>Cisco Support</name>
      <email>support@cisco.com</email>
   </author>

   <!-- Custom Branding -->
      <entry>
         <id>http://foo.foo.com/foo/AgentCustomizationPackage/1/1/1/1</id> -- This id can
be anything, but should be unique within an ISE deployment
         <title>Agent Customization Package</title>
         <updated>2010-06-07T12:00:00Z</updated>
         <summary>This is the agent customization package </summary> - Can be anything
         <link rel="enclosure" type="application/zip" href="brand-windows.zip"
length="18884" />
         <update:type>AgentCustomizationPackage</update:type>
         <update:version>1.1.1.0</update:version> -- Important to have this as 4 digit
         <update:os>Win</update:os>
      </entry>
</feed>
```

関連項目

- 「エージェント ログイン画面のカスタマイズ」（P.22-8）
- 「カスタム nac_login.xml ファイル テンプレート」（P.22-10）
- 「カスタム企業/会社ロゴの使用」（P.22-10）
- 「カスタム nacStrings_xx.xml ファイル テンプレート」（P.22-11）
- 「サンプル拡張 nacStrings_xx.xml ファイル」（P.22-12）
- 「エージェント カスタマイゼーション ファイルの作成」（P.22-13）
- 「エージェント XML ファイルのインストール ディレクトリ」（P.22-14）

エージェント カスタマイゼーション ファイルの作成

エージェントのカスタマイゼーション ファイルにより、Cisco NAC Agent ログイン ダイアログのロゴ、フィールド、メッセージをカスタマイズして、特定の Windows クライアントをネットワークのアクセス要件に合致させることができます。

XML ディスクリプタ ファイルを含む .zip ファイルとしてカスタマイゼーション パッケージを作成し、カスタマイズされたオプションから成るコンテンツを含む別の .zip ファイルを作成することができます。

ステップ 1　Agent ログイン カスタマイゼーション パッケージを構成するために必要なファイルを組み合わせます。

- カスタマイズされた nac_login.xml ファイル
- .gif ファイルとしてカスタマイズされた企業/会社のロゴ

- 1 つ以上のカスタマイズされた nacStrings_*xx*.xml ファイル
- カスタマイズされた updateFeed.xml ディスクリプタ ファイル

ステップ 2　完成したファイルを含む「brand-win.zip」と呼ばれる zip ファイルを作成します。たとえば Linux または UNIX 環境では、次のコマンドを実行します。

zip -r brand-win.zip nac_login.xml nac_logo.gif nacStrings_en.xml nacStrings_cy.xml nacStrings_el.xml

ステップ 3　適切な updateFeed.xml ディスクリプタ ファイルと上記で作成された .zip ファイルを含む「custom.zip」ファイルを作成します。たとえば Linux または UNIX 環境では、次のコマンドを実行します。

zip -r custom.zip updateFeed.xml brand-win.zip

ステップ 4　完成した「custom.zip」ファイルを、Cisco ISE にアップロードする場合にアクセスできるローカル マシン上に保存します。

関連項目

- 「エージェント ログイン画面のカスタマイズ」（P.22-8）
- 「カスタム nac_login.xml ファイル テンプレート」（P.22-10）
- 「カスタム企業/会社ロゴの使用」（P.22-10）
- 「カスタム nacStrings_xx.xml ファイル テンプレート」（P.22-11）
- 「サンプル拡張 nacStrings_xx.xml ファイル」（P.22-12）
- 「UpdateFeed.xml ディスクリプタ ファイルのテンプレート」（P.22-12）
- 「エージェント XML ファイルのインストール ディレクトリ」（P.22-14）

エージェント XML ファイルのインストール ディレクトリ

Cisco NAC Agent 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、これらの .xml ファイルは次のディレクトリにあります。

- nac_login.xml ファイルは「C:\Program Files\Cisco\Cisco NAC Agent\UI\nac_divs\login」ディレクトリにあります。
- nacStrings_xx.xml ファイルで、「xx」はロケールを示します。ファイルの全リストは「C:\Program Files\Cisco\Cisco NAC Agent\UI\cues_utility」ディレクトリにあります。

エージェントが別の場所にインストールされている場合には、ファイルは「<*Agent Installed path*>\Cisco\Cisco NAC Agent\UI\nac_divs\login」および「<*Agent Installed path*>\Cisco\Cisco NAC Agent\cues_utility」にあります。

関連項目

- 「エージェント ログイン画面のカスタマイズ」（P.22-8）
- 「カスタム nac_login.xml ファイル テンプレート」（P.22-10）
- 「カスタム企業/会社ロゴの使用」（P.22-10）
- 「カスタム nacStrings_xx.xml ファイル テンプレート」（P.22-11）
- 「サンプル拡張 nacStrings_xx.xml ファイル」（P.22-12）
- 「UpdateFeed.xml ディスクリプタ ファイルのテンプレート」（P.22-12）

- 「エージェント カスタマイゼーション ファイルの作成」（P.22-13）

エージェント プロファイル設定のガイドライン

シスコは、エージェント プロファイルを設定して、修復タイマー、ネットワーク遷移遅延タイマー、およびクライアント マシン上でログイン成功画面を制御するために使用するタイマー制御し、これらの設定がポリシーベースになるようにすることを推奨します。ただし、クライアント プロビジョニング ポリシーと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、[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）] 設定ページを使用して、同じ目的を達成できます。

ポリシー適用または他の方法でクライアント デバイスにエージェント プロファイルを設定してアップロードすると、そのエージェント プロファイルはクライアント上で維持され、他の何かに変更するまで、ログインおよび操作の動作に影響を及ぼします。したがって、エージェント プロファイルを Cisco ISE から削除しても、以前影響を受けたクライアントからその動作はなくなりません。ログインおよび操作の動作を変更するには、クライアント上の、既存のエージェント プロファイル パラメータの値を*上書き*する新しいエージェント プロファイルを定義し、これをポリシー適用によってアップロードする必要があります。

クライアントにあるものと異なるエージェント プロファイルが Cisco ISE にある場合（MD5 チェックサムを使用して判定）、Cisco ISE は、新しいエージェント プロファイルをクライアントにダウンロードします。Cisco ISE から送信されるエージェント カスタマイズ ファイルが異なる場合にも、Cisco ISE は新しいエージェント カスタマイズ ファイルをクライアントにダウンロードします。詳細については、を参照してください。

関連項目

- 「ポスチャ管理の設定」（P.23-5）
- 「エージェント カスタマイゼーション ファイルの作成」（P.22-13）

エージェント プロファイル パラメータおよび適用可能な値

エージェント設定パラメータは機能別にグループ化されます。

この項では、クライアント マシンにインストールされたエージェントのログイン、操作、およびログアウトの動作のカスタマイズに使用するエージェント プロファイル パラメータの説明、デフォルト値、および使用可能な範囲を示します。

表 22-1　複数の Active NIC を使用してクライアントの認証 VLAN 変更ディスカバリにアクセス

パラメータ	デフォルト値	有効な範囲	使用上のガイドライン
VLAN 検出間隔（Vlan detect interval）	0[1]、5 [2]	0、5 ～ 900	• 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 ICMP または ARP クエリを 5 秒ごとに送信します。 • 6 ～ 900：ICMP/ARP クエリが *x* 秒ごとに送信されます。
UI なしの VLAN 検出の有効化（Enable VLAN detect without UI?）	No	「Yes」または「No」で答えてください。	• **No**：VLAN 検出機能は無効です。 • **Yes**：VLAN 検出機能が有効です。 **（注）** この設定は Mac OS X のクライアントには適用されません。

1. Cisco NAC Windows エージェントの場合、デフォルト値は 0 です。デフォルトでは、認証 VLAN 変更機能へのアクセスは Windows に対して無効にされます。
2. 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、VlanDetectInterval を 5 秒として有効になっています。

表 22-2　エージェント ログイン/ログアウト ダイアログの動作のカスタマイズ

パラメータ	デフォルト値	有効な範囲	使用上のガイドライン
エージェントの終了の無効化（Disable Agent Exit?）	No	「Yes」または「No」で答えてください。	**Yes**：ユーザはシステム トレイ アイコンを使用してエージェントを停止できません。 **（注）** この設定は Mac OS X のクライアントには適用されません。
CRL チェックの許可（Allow CRL Checks?）	Yes	「Yes」または「No」で答えてください。	**No**：検出およびネゴシエーション時の証明書失効リスト（CRL）の確認をオフにします。 **（注）** この設定は Mac OS X のクライアントには適用されません。
アクセシビリティ モード（Accessibility mode?）	No	「Yes」または「No」で答えてください。	• 1：エージェントは Job Access with Speech（JAWS）画面リーダーと互換性があります。 • 0：エージェントは JAWS 画面リーダーとのやりとりはありません。 この機能を有効にすると、パフォーマンスがわずかながら影響を受ける可能性があります。JAWS 画面リーダーがインストールされていないクライアント マシンでこの機能をイネーブルにしても、Agent は正常に機能します。 **（注）** この設定は Mac OS X のクライアントには適用されません。

表 22-2　エージェント ログイン/ログアウト ダイアログの動作のカスタマイズ （続き）

パラメータ	デフォルト値	有効な範囲	使用上のガイドライン
署名のチェック（Check signature?）	No	「Yes」または「No」で答えてください。	署名のチェック設定により、Windows が実行可能ファイルを起動する前にファイルを信頼できるかどうかを判断するためにエージェントが使用する、デジタル署名が検索されます。詳細については、「プログラム起動修復の追加」（P.23-17）を参照してください。 **（注）** この設定は Mac OS X のクライアントには適用されません。
概要画面のバイパス（Bypass summary screen）	Yes	「Yes」または「No」で答えてください。	エージェントの要件に自動修復を採用している場合、この設定によって、エージェント ポスチャ評価の概要画面をスキップして自動修復の最初の機能に直接進むことにより、エージェント セッション ダイアログを自動化することができます。この手順を回避すると、エージェント ログインおよび修復セッション中のユーザ対話が削減、または完全になくなります。 **（注）** この設定は Mac OS X のクライアントには適用されません。

表 22-3　クライアント側 MAC アドレスおよびエージェント Discovery Host の管理

パラメータ	デフォルト値	有効な範囲	使用上のガイドライン
MAC 例外リスト（MAC Exception list）	—	有効な MAC アドレス	この設定で 1 つまたは複数の MAC アドレスを指定すると、エージェントは、ログインと認証の間、ネットワーク経由で不要な MAC アドレスが送信されることを防ぐために、これらの MAC アドレスを Cisco ISE にアドバタイズしません。指定するテキスト文字列は、コロンを含む、カンマで区切られた MAC アドレスのリストでなければなりません。次に例を示します。 `AA:BB:CC:DD:EE:FF,11:22:33:44:55:66` **（注）** この設定は Mac OS X のクライアントには適用されません。
Discovery host	—	IP アドレスまたは完全修飾ドメイン名（FQDN）	この設定では、レイヤ 3 配置で Cisco ISE に接続するためにエージェントが使用する Discovery Host のアドレスまたは解決可能なドメイン名を指定します。

表 22-3　クライアント側 MAC アドレスおよびエージェント Discovery Host の管理 （続き）

パラメータ	デフォルト値	有効な範囲	使用上のガイドライン
Discovery host が編集可能か（Discovery host editable?）	Yes	「Yes」または「No」で答えてください。	**Yes**：（デフォルト値）ユーザが [エージェントのプロパティ（**Agent Properties**）] ダイアログボックスの [ホストの検索（Discovery Host）] フィールドにカスタム値を指定できます。 **No**：ユーザがクライアント マシンの [Discovery Host] フィールドの値を変更できません。 **（注）** この設定は Mac OS X のクライアントには適用されません。
サーバ名ルール（Server name rules）	—	FQDN	このパラメータは、関連する Cisco ISE ノードのカンマ区切り名から構成されます。エージェントは、このリストの名前を使用して、Cisco ISE アクセス ポイントを許可します。このリストが空の場合、許可は実行されません。いずれの名前も見つからない場合、エラーが報告されます。 サーバ名は FQDN 名である必要があります。類似の文字で構成される Cisco ISE ノード名を指定するには、ワイルドカード文字（アスタリスク [*****]）使用できます。たとえば、***.cisco.com** は、Cisco.com ドメインのすべてのサーバと一致します。 **（注）** この設定は Mac OS X のクライアントには適用されません。
生成された MAC（Generated MAC）	—	有効な MAC アドレス	このパラメータは、クライアント マシンでの Evolution-Data Optimized（EVDO）接続をサポートします。クライアント マシンにアクティブなネットワーク インターフェイス カード（NIC）がない場合、エージェントはシステム上にダミーの MAC アドレスを作成します。 **（注）** この設定は Mac OS X のクライアントには適用されません。

表 22-4　エージェント ローカリゼーション設定の指定

パラメータ	デフォルト値	有効な範囲	使用上のガイドライン
言語情報（Language Info）	OS の設定（「**default**」）	—	• **default**：エージェントは、クライアント オペレーティング システムのロケール設定を使用します。 • この設定が、サポートされている言語の ID、略称、または正式名称の場合、Agent は自動的に、クライアント マシンの Agent ダイアログをローカライズされたテキストで表示します。表 22-5 を参照してください。「サポートされる言語」。 **（注）** この設定は Mac OS X のクライアントには適用されません。

表 22-5　サポートされる言語

言語	ID	略称	正式名称
英語（米国）	1033	en	英語
カタロニア語	1027	ca	カタロニア語（スペイン）
簡体字中国語	2052	zh_cn	中国語（簡体字）
繁体字中国語	1028	zh_tw	中国語（繁体字）
チェコ語	1029	cs	チェコ語
デンマーク語	1030	da	デンマーク語
オランダ語	1043	nl	オランダ語（標準）
フィンランド語	1035	fi	フィンランド語
フランス語	1036	fr	フランス語
フランス語（カナダ）	3084	fr-ca	フランス語（カナダ）
ドイツ語	1031	de	ドイツ語
ハンガリー語	1038	hu	ハンガリー語
イタリア語	1040	it	イタリア語
日本語	1041	ja	日本語
韓国語	1042	ko	韓国語
ノルウェー語	1044	No	ノルウェー語
ポーランド語	1045	pl	ポーランド語
ポルトガル語	2070	pt	ポルトガル語
ロシア語	1049	ru	ロシア語
セルビア語（ラテン）	2074	sr	セルビア語（ラテン）
セルビア語（キリル）	3098	src	セルビア語（キリル）
スペイン語	1034	es	スペイン語（従来型）
スウェーデン語	1053	sv	スウェーデン語
トルコ語	1055	tr	トルコ語

表 22-6　レポートおよびログ表示設定

パラメータ	デフォルト値	有効な範囲	使用上のガイドライン
ポスチャ レポート フィルタ（Posture Report Filter）	displayFailed	—	このパラメータは、クライアント マシンでポスチャ評価が行われたときにユーザに表示される結果のレベルとタイプを制御します。 • **displayAll**：[エージェント（Agent）] ダイアログの [詳細を表示（Show Details）] をクリックすると、クライアント ポスチャ評価レポートにすべての結果が表示されます。 • **displayFailed**：（デフォルト値）[エージェント（Agent）] ダイアログの [詳細を表示（Show Details）] をクリックすると、クライアント ポスチャ評価レポートは修復エラーだけを表示します。 **（注）** この設定は Mac OS X のクライアントには適用されません。
ログ ファイル サイズ（MB 単位）（Log file size in MB）	5	0 以上	この設定では、クライアント マシン上のエージェント ログ ファイルのファイル サイズ（メガバイト単位）を指定します。 • 0：エージェントは、クライアント マシン上のユーザ セッションに関するログインまたは操作情報を記録しません。 • 他の整数：エージェント レコードは指定されたメガバイト数までログインおよびセッション情報を記録します。[1]

1. エージェント ログ ファイルは、クライアント マシンのディレクトリに記録、保存されます。1 回目のエージェント ログイン セッションの後、2 つのファイルがディレクトリ内に置かれます。1 つは前回のログイン セッションからのバックアップ ファイルで、もう 1 つは現在のセッションのログインおよび操作の情報を含む新しいファイルです。現在のエージェント セッションのログ ファイルが大きくなり、指定されたファイル サイズを超えると、エージェントのログインおよび操作情報の最初の部分が自動的にディレクトリ内のバックアップ ファイルになり、エージェントは引き続き最新のエントリを現在のセッション ファイルに記録していきます。

表 22-7　クライアント マシン接続確認の繰り返し

パラメータ	デフォルト値	有効な範囲	使用上のガイドライン
検出の再試行（Detect Retries）	3	0 以上	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）ポーリングが失敗した場合、クライアント IP アドレスの更新の前に、この設定はエージェントが *x* 回再試行するよう設定します。

表 22-7　クライアント マシン接続確認の繰り返し （続き）

パラメータ	デフォルト値	有効な範囲	使用上のガイドライン
ping ARP	0	0 ～ 2	• 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 がダウンした場合は）ARP を使用してポーリング
ping の最大タイムアウト（Max Timeout for Ping）	1	1 ～ 10	ICMP を使用してポーリングし、*x* 秒内に応答がない場合は、ICMP ポーリング失敗を宣言します。

表 22-8　追加の SWISS ディスカバリのカスタマイズ

パラメータ	デフォルト値	有効な範囲	使用上のガイドライン
Swiss タイムアウト（Swiss timeout）	1	1 以上	• 1：エージェントは、設計どおりに SWISS ディスカバリを実行し、追加の UDP 応答パケット遅延タイムアウト値は使用されません。 • 1 よりも大きい整数：エージェントは、追加番号の秒数だけ Cisco ISE からの SWISS UDP 検出応答パケットを待ってから、別のディスカバリ パケットを送信します。エージェントは、このアクションを実行して、ネットワークで応答パケットの遅延が発生していないことを確認します。（Swiss タイムアウトは UDP SWISS タイムアウトでのみ機能します） **（注）** この設定は Mac OS X のクライアントには適用されません。
L3 Swiss 遅延の無効化（Disable L3 Swiss Delay?）	No	「Yes」または「No」で答えてください。	この設定が Yes の場合、エージェントはレイヤ 3 検出パケットの転送間隔を長くする機能を無効にします。したがって、レイヤ 3 検出パケットはレイヤ 2 パケットと同様に、5 秒ごとに送信され続けます。デフォルト設定は no です。 **（注）** この設定は Mac OS X のクライアントには適用されません。

表 22-9　HTTP 検出のカスタマイズ

パラメータ	デフォルト値	有効な範囲	説明または動作
Http 検出のタイムアウト（Http discovery timeout）	30	0、3 以上	• Windows：Http 検出のタイムアウトは、エージェントからの HTTPS 検出が Cisco ISE からの応答を待機する時間で、デフォルトで 30 秒に設定されています。指定された時間内に応答がないと、検出プロセスはタイムアウトになります。有効な範囲は 3 秒以上です。1 または 2 の値を入力すると、自動的に 3 がパラメータ値に設定されます。 • Mac OS X：シスコは Mac OS X クライアント マシン エージェント プロファイルには、この値を 5 秒に設定することを推奨します。 この値が 0 に設定されている場合は、デフォルトのクライアント マシンのオペレーティング システムのタイムアウト設定が使用されます。
Http タイムアウト（Http timeout）	120	0、3 以上	Http タイムアウトは、エージェントからの HTTP 要求が応答を待機する時間で、デフォルトで 120 秒に設定されています。指定時間内に応答がない場合は、要求時間と検出プロセス時間は期限切れになります。有効な範囲は 3 秒以上です。（1 または 2 の値を入力すると、自動的に 3 がパラメータ値に設定されます） この値が 0 に設定されている場合は、デフォルトのクライアント マシンのオペレーティング システムのタイムアウト設定が使用されます。

表 22-10　修復タイムアウトのカスタマイズ

パラメータ	デフォルト値	有効な範囲	使用上のガイドライン
修復タイマー（Remediation timer）	4	1 ～ 300	クライアント マシンで失敗したポスチャ評価チェックをユーザが何分以内に修復することが必要であるかを指定します。この分数を経過すると、ログイン プロセスを再び実行する必要があります。
ネットワーク遷移遅延（Network Transition Delay）	3	2 ～ 30	エージェントがネットワーク遷移（IP アドレスの変更）を待機する必要がある秒数を指定します。これが経過すると、修復タイマーのカウントダウンが開始されます。 **（注）** 「Enable Agent IP refresh after VLAN change」オプションを使用する場合、Cisco ISE は Windows エージェント プロファイルに使用する「Network transition delay」設定の代わりに、（下記のように）「DHCP release delay」および「DHCP renew delay」設定を送信します。「Enable Agent IP refresh after VLAN change」オプションを使用しない場合、Cisco ISE はこの *2* つではなく、「Network transition delay」タイマー設定をクライアント マシンに送信します。

表 22-11　ユーザのログアウトまたはシャットダウンでのエージェント ダイアログの動作

パラメータ	デフォルト値	有効な範囲	使用上のガイドライン
ログイン画面の自動クローズの有効化（Enable auto close login screen?）	No	「Yes」または「No」で答えてください。	クライアント マシン ユーザがログイン クレデンシャルを入力するエージェント ログイン ダイアログを認証後に自動的に閉じるかどうかを決定できます。
<*x*> 秒後にログイン画面を自動的に閉じる（Auto close login screen after <x> sec）	0	0 ～ 300	クライアント マシンでユーザ クレデンシャルを認証した後、エージェントが自動的に閉じるまでに待機する秒数を指定します。

表 22-12　クライアント マシンの IP アドレスの動作設定

パラメータ	デフォルト値	有効な範囲	使用上のガイドライン
VLAN 変更後にエージェント IP 更新を有効化	No	「Yes」または「No」で答えてください。	**注意** シスコは、ネイティブ Windows、Cisco Secure Services Client、または AnyConnect サプリカントを介してネットワークにアクセスする Windows クライアント マシンに対してこのオプションを有効にすることは推奨しません。 切り替え後またはそれぞれの切り替えポートでクライアントのログイン セッションの VLAN を WLC が変更した後にクライアント マシンが IP アドレスを更新する必要があるかどうかを指定します。 ポスチャを備えた MAB に対して有線と無線の両方の環境で Windows クライアント IP アドレスを更新するには、[VLAN 変更後にエージェント IP 更新を有効化（Enable agent IP refresh after VLAN change）] パラメータをオンにします。 割り当てられた VLAN を変更したときに Mac OS X クライアント IP アドレスが更新されるようにするために、有線と無線の両方の環境でネイティブ Mac OS X サプリカントを介してネットワークにアクセスする Mac OS X クライアント マシンに対してこのパラメータが必要です。 **（注）** 「Enable Agent IP refresh after VLAN change」オプションを使用する場合、Cisco ISE は Windows エージェント プロファイルに使用する「Network transition delay」設定の代わりに、（下記のように）「DHCP release delay」および「DHCP renew delay」設定を送信します。「Enable Agent IP refresh after VLAN change」オプションを使用しない場合は、Cisco ISE は *この 2 つ*ではなく、「Network transition delay」タイマー設定をクライアント マシンに送信します。
DHCP 更新遅延（DHCP renew delay）	0	0 ～ 60	ネットワーク DHCP サーバから新しい IP アドレスを要求しようとする前にクライアント マシンが待機する秒数。
DHCP リリース遅延（DHCP release delay）	0	0 ～ 60	現在の IP アドレスをリリースする前にクライアント マシンが待機する秒数。

プロファイル作成機能を使用して生成された XML ファイルの例

```
<?xml version="1.0" ?>
```

```
<cfg>
   <VlanDetectInterval>0</VlanDetectInterval>
   <RetryDetection>3</RetryDetection>
   <PingArp>0</PingArp>
   <PingMaxTimeout>1</PingMaxTimeout>
   <EnableVlanDetectWithoutUI>0</EnableVlanDetectWithoutUI>
   <SignatureCheck>0</SignatureCheck>
   <DisableExit>0</DisableExit>
   <PostureReportFilter>displayFailed</PostureReportFilter>
   <BypassSummaryScreen>1</BypassSummaryScreen>
   <LogFileSize>5</LogFileSize>
   <DiscoveryHost></DiscoveryHost>
   <DiscoveryHostEditable>1</DiscoveryHostEditable>
   <Locale>default</Locale>
   <AccessibilityMode>0</AccessibilityMode>
   <SwissTimeout>1</SwissTimeout>
   <HttpDiscoveryTimeout>30</HttpDiscoveryTimeout>
   <HttpTimeout>120</HttpTimeout>
   <ExceptionMACList></ExceptionMACList>
   <GeneratedMAC></GeneratedMAC>
   <AllowCRLChecks>1</AllowCRLChecks>
   <DisableL3SwissDelay>0</DisableL3SwissDelay>
   <ServerNameRules></ServerNameRules>
</cfg>
```

（注） このファイルには、2 つの静的（つまり、ユーザまたは Cisco ISE 管理者が編集できない）「AgentCfgVersion」パラメータおよび「AgentBrandVersion」パラメータも含まれています。これらのパラメータは、クライアントでエージェント プロファイルおよびエージェント カスタマイズ ファイルの現在のバージョンをそれぞれ識別するために使用されます。

Windows エージェントのプロファイルの作成

Cisco ISE で、保護されたネットワークにログインした場合の Windows クライアントの動作方法を指定するエージェント プロファイルを設定できます。パラメータを 1 つ以上設定して既存のエージェント プロファイルとマージすると、新しい（未定義）パラメータはマージされた値に従って設定されますが、エージェント プロファイルの既存のパラメータの設定は維持されます。

はじめる前に

Windows エージェント プロファイルを作成する前に、Cisco ISE にエージェント ソフトウェアをアップロードすることを推奨します:

- 「リモート ソースからのクライアント プロビジョニング リソースの追加」（P.22-3）
- 「ローカル マシンからのクライアント プロビジョニング リソースの追加」（P.22-3）
- 「クライアント プロビジョニング リソースの自動ダウンロード」（P.22-4）

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

ステップ 2　[追加（Add）] > [ISE ポスチャ エージェント プロファイル（ISE Posture Agent Profile）] を選択します。

ステップ 3　Windows エージェント プロファイルの名前を指定します。

ステップ 4　パラメータの値を指定し、必要に応じてこれらの設定を既存のプロファイル設定とマージするかまたは上書きするかを指定し、Windows クライアント マシン エージェントの動作を適切に設定します。

ステップ 5　[送信（Submit）] をクリックします。

次の作業

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、1 つ以上のエージェント プロファイル オプションを設定すると、リソース ポリシーの設定を開始できます。

関連項目

- 「エージェント プロファイル設定のガイドライン」（P.22-15）
- 「エージェント プロファイル パラメータおよび適用可能な値」（P.22-15）
- 「プロファイル作成機能を使用して生成された XML ファイルの例」（P.22-24）
- 「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」（P.22-30）

Mac OS X エージェント プロファイルの作成

Cisco ISE で、保護されたネットワークにログインした場合の Mac OS X クライアントの動作方法を指定するエージェント プロファイルを設定できます。パラメータを 1 つ以上設定して既存のエージェント プロファイルとマージすると、新しい（未定義）パラメータはマージされた値に従って設定されますが、エージェント プロファイルの既存のパラメータの設定は維持されます。

Mac OS X クライアント マシン用の設定に使用できるパラメータは、Windows クライアント マシン用に使用できるもののサブセットのみです。「Mac プラットフォーム：適用外」という注釈があるパラメータの設定は Mac OS X クライアントのエージェント動作に影響しないため、それらの設定は指定しないことを推奨します。

はじめる前に

Mac OS X エージェント プロファイルを作成する前に、Cisco ISE にエージェント ソフトウェアをアップロードすることを推奨します:

- 「リモート ソースからのクライアント プロビジョニング リソースの追加」（P.22-3）
- 「ローカル マシンからのクライアント プロビジョニング リソースの追加」（P.22-3）
- 「クライアント プロビジョニング リソースの自動ダウンロード」（P.22-4）

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

ステップ 2　[追加（Add）] > [ISE ポスチャ エージェント プロファイル（ISE Posture Agent Profile）] を選択します。

ステップ 3　エージェント プロファイルの名前を指定します。

ステップ 4　パラメータの値を指定し、必要に応じてこれらの設定を既存のプロファイル設定とマージするかまたは上書きするかを指定し、Mac OS X クライアント マシン エージェントの動作を適切に設定します。

ステップ 5　[送信（Submit）] をクリックします。

次の作業

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、1 つ以上のエージェント プロファイル オプションを設定すると、リソース ポリシーの設定を開始できます。

関連項目

- 「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」（P.22-30）
- 「エージェント プロファイル設定のガイドライン」（P.22-15）
- 「エージェント プロファイル パラメータおよび適用可能な値」（P.22-15）
- 「プロファイル作成機能を使用して生成された XML ファイルの例」（P.22-24）

ネイティブ サプリカント プロファイルの作成

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

はじめる前に

- リモート デバイス登録に TLS デバイス プロトコルを使用しようとしている場合、「Simple Certificate Enrollment Protocol プロファイル」（P.8-31）の説明に従って、少なくとも 1 つの Simple Certificate Enrollment Protocol（SCEP）プロファイルを設定してください。
- TCP ポート 8909 および UDP ポート 8909 を開き、Cisco NAC Agent、Cisco NAC 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てください。ポートの使用法の詳細については、『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*』の付録「Cisco ISE Appliance Ports Reference」を参照してください。

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

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

ステップ 3　エージェント プロファイルの [名前（Name）] を指定します。

ステップ 4　（任意）[ネイティブ サプリカント プロファイル（Native Supplicant Profile）] の説明を [説明（Description）] に入力します。

ステップ 5　このプロファイルの [オペレーティング システム（Operating System）] を選択します。

ステップ 6　このプロファイルの有線または無線の接続タイプ（あるいは両方）に適切なオプションを有効にします。無線接続オプションを有効にした場合は、デバイス SSID と無線セキュリティ タイプ（WPA2-Enterprise または WPA エンタープライズのどちらか）も指定するようにします。

ステップ 7　デバイス プロファイルの [許可されるプロトコル（Allowed Protocol）] を選択します。

ステップ 8　このプロファイルに対して他の [任意の設定（Optional Settings）] を適切に有効または無効にします。

ステップ 9　[送信（Submit）] をクリックします。

次の作業

「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。

関連項目

- 「エージェント プロファイル設定のガイドライン」（P.22-15）
- 「複数のゲスト ポータルのサポート」（P.16-2）

許可されたプロトコルの設定

表 22-13　許可されたプロトコルの設定

パラメータ	説明
TLS	TLS プロトコルを使用して最高レベルのデバイス登録セキュリティを提供します。TLS の方法を指定した場合、Cisco ISE は、デバイスの証明書用に [証明書署名要求（Certificate Signing Request）] を生成し、SCEP 要求を適切な認証登録局に転送します。SCEP 認証局に接続を設定する方法の詳細については、「Simple Certificate Enrollment Protocol プロファイル」（P.8-31）を参照してください。
PEAP	通常、PEAP では、ユーザはネットワークにログインするときにアクセス クレデンシャルを入力でき、代わりに標準登録証明書を受け取ります。
EAP-FAST	Apple iOS および Mac OS X デバイスへの接続には EAP-FAST を使用します。接続は、通常、証明書タイプおよびその有無から独立して行われます。 **（注）** iPhone および iPad での Apple iOS のデフォルト動作のため、Cisco ISE は、*単一の* Service Set Identifier（SSID）を介して接続している場合、ネイティブ サプリカント プロファイルでの EAP-FAST プロトコルの使用をサポートしていません。Cisco ISE ネットワークにログインするとき、iOS ベースのデバイスは、デバイスにインストールされたサプリカント プロビジョニング プロファイルが EAP-FAST プロトコルを指定している場合でも、デフォルトで PEAP-MSCHAPv2 プロトコルを使用して自動的にネゴシエーションします。デュアル SSID 環境では、iOS ベースのデバイスはこの制約を受けません。

パーソナル デバイス登録動作の設定

この機能を使用して、Cisco ISE がネイティブ サプリカント プロビジョニング ウィザードをインストールできないパーソナル デバイスを介したユーザ ログイン セッションを Cisco ISE が処理する方法を指定します（Research In Motion の Blackberry デバイスなど）。

ステップ 1　[管理（Administration）] > [システム（System）] > [設定（Settings）] > [クライアント プロビジョニング（Client Provisioning）] を選択します。

ステップ 2　[ネイティブ サプリカント プロビジョニング ポリシーを使用できない（Native Supplicant Provisioning Policy Unavailable）] ドロップダウン リストから、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。
- [定義済みの許可ポリシーの適用（Apply Defined Authorization Policy）] : ユーザは、標準認証および（ネイティブ サプリカント プロビジョニング プロセスではない）許可ポリシーを適用して Cisco ISE ネットワークへのアクセスを試みる必要があります。このオプションを有効にすると、ユーザ デバイスに対して、ユーザの ID に適用されたすべてのクライアント プロビジョニング ポリシーに従った標準登録が行われます。Cisco ISE ネットワークにアクセスするためにユーザのデバイスが証明書を必要とする場合は、15 章の「End_User Web ポータルのセットアップとカスタマイズ」の「カスタム言語テンプレートの追加」の説明に従って、カスタマイズ可能なユーザ提示テキスト フィールドを使用して有効な証明書を取得して適用する方法もユーザに詳細に指示する必要があります。

ステップ 3　[保存（Save）] をクリックします。

次の作業

「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。

関連項目

- 「複数のゲスト ポータルのサポート」（P.16-2）
- 「カスタム言語テンプレートの追加」（P.15-5）

Cisco NAC Agent MSI インストーラを使用したクライアント マシンのプロビジョニング

ネットワークとの一致に必要な適切なエージェント プロファイル情報を含むエージェント設定 XML ファイル（**NACAgentCFG.xml** という名前）とともに、MSI インストーラをディレクトリに、または MSI インストーラの zip バージョンをクライアント マシン上に置くことができます。

ステップ 1　**nacagentsetup-win.msi** または **nacagentsetup-win.zip** インストーラ ファイルを Cisco Software Download サイト（http://software.cisco.com/download/navigator.shtml）からダウンロードします。

ステップ 2　**nacagentsetup-win.msi** ファイルをクライアント マシン上の特定のディレクトリに置きます（たとえば、C:\temp\nacagentsetup-win.msi）。

- MSI インストーラを直接クライアントにコピーする場合は、クライアント マシンから Cisco NAC Agent をインストールする際のインストール元となるディレクトリに、**nacagentsetup-win.msi** ファイルを置きます。
- **nacagentsetup-win.zip** インストーラを使用する場合は、クライアント マシンから Cisco NAC Agent をインストールする際のインストール元となるディレクトリに、zip ファイルの内容を抽出します。

ステップ 3　Agent 設定 XML ファイルを、Cisco NAC Agent MSI パッケージと同じディレクトリに置きます。

Cisco ISE に接続しない場合は、すでに正常にプロビジョニングされたクライアントから **NACAgentCFG.xml** ファイルをコピーできます。ファイルは、**C:\Program Files\Cisco\Cisco NAC Agent\NACAgentCFG.xml** にあります。

Agent 設定 XML ファイルが MSI インストーラ パッケージと同じディレクトリに存在していれば、インストール プロセスによって Agent 設定 XML ファイルは自動的に適切な Cisco NAC Agent アプリケーション ディレクトリに置かれるため、エージェントは最初に起動されたとき、正しいレイヤ 3 ネットワーク上の場所をポイントすることができます。

ステップ 4　クライアント マシンでコマンド プロンプトを開き、次のように入力してインストールを実行します。

```
msiexec.exe /i NACAgentSetup-win.msi /qn /l*v c:\temp\agent-install.log
```

（`/qn` 修飾子は、Cisco NAC Agent を完全にサイレントでインストールします。`/l*v` は、インストール セッションを冗長モードで記録します。）

ステップ 5　Altiris/SMS を使用して MSI インストーラを分散する場合は、エージェントのカスタマイゼーション ファイルを「%TEMP%/CCAA」ディレクトリの「brand」という名前のサブディレクトリに置きます。Cisco NAC Agent がクライアントにインストールされるとき、このカスタマイズは Agent に適用されます。カスタマイズを削除するには、カスタマイズ ファイルなしの MSI を送信します。

関連項目

- 「プロファイル作成機能を使用して生成された XML ファイルの例」（P.22-24）
- 「Windows エージェントのプロファイルの作成」（P.22-25）

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

エージェント準拠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それを上書きします。

はじめる前に

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には、次のトピックに従って、システム全体のクライアント プロビジョニング機能を設定済みであることを確認します。

- 「Cisco ISE でのプロキシ設定の指定」（P.5-3）
- 「リモート ソースからのクライアント プロビジョニング リソースの追加」（P.22-3）
- 「ローカル マシンからのクライアント プロビジョニング リソースの追加」（P.22-3）
- 「クライアント プロビジョニング リソースの自動ダウンロード」（P.22-4）

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

ステップ 2　動作のドロップダウン リストから [有効（Enable）]、[無効（Disable）]、または [モニタ（Monitor）] を選択します。

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

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

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

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

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

「Android」、「Mac iOS」、「Mac OS X」などのように単一オペレーティング システムを指定することも、「Windows XP（All）」または「Windows 7（All）」などのように多数のクライアント マシンのオペレーティング システムを包括的に指定することもできます。

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 マシンに対して、前のトピックで定義した分類に基づいて、クライアント マシンで使用可能にし、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、またはプロファイルを指定します。

a. [エージェント（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 [アップグレードは必須か（Is Upgrade Mandatory）] オプションを有効または無効にして、適切に指定します。

（注）　[アップグレードは必須か（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。Agent プロファイル、コンプライアンス モジュール、および Agent カスタマイズ パッケージの更新は常に必須です。

b. [プロファイル（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。

c. [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。

（注）　ポリシー設定プロセスを使用し、[操作（Action）] アイコンをクリックし、ドロップダウン リストから [リソースのダウンロード（Download Resource）] または [リソースのアップロード（Upload Resource）] をクリックして、これら 3 つのリソース タイプに対してエージェント リソースを「すぐに」ダウンロードすることもできます。これにより、[リモート リソースのダウンロード（Downloaded Remote Resources）] または [手動リソース アップロード（Manual Resource Upload）] ダイアログボックスが開き、そこから「リモート リソースからのクライアント プロビジョニング リソースの追加」と「ローカル マシンからのクライアント プロビジョニング リソースの追加」の項の説明のように 1 つ以上のリソースを Cisco ISE にダウンロードすることができます。

d. [エージェント カスタマイズ パッケージ（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。

ステップ 8　パーソナル デバイスに対して、上記で定義した分類に基づいて、登録したパーソナル 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 サプリカント設定を指定します。

a. 特定の [設定ウィザード（Configuration Wizard）] を選択して、これらのパーソナル デバイスに配布します。

b. 指定されたパーソナル デバイス タイプに適用可能な [ウィザード プロファイル（Wizard Profile）] を指定します。

ステップ 9　[保存（Save）] をクリックします。

次の作業

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

関連項目

- 第 23 章「クライアント ポスチャ ポリシーの設定」

クライアント プロビジョニング レポートの表示

Cisco ISE のモニタリングおよびトラブルシューティング機能にアクセスし、ユーザ ログイン セッションの成功または失敗の全体のトレンドをチェックし、特定の期間にネットワークにログインしたクライアント マシンの数およびタイプに関する統計情報を収集し、また、クライアント プロビジョニング リソースでの最近の設定変更をチェックすることができます。

関連項目

- 「クライアント プロビジョニング要求の表示」（P.22-32）
- 「クライアント アクセス セッションの表示」（P.22-32）
- 「クライアント プロビジョニング リソースの設定変更の表示」（P.22-32）
- 「サプリカント プロビジョニング要求の表示」（P.22-33）
- 「クライアント プロビジョニング イベント ログの表示」（P.22-33）

クライアント プロビジョニング要求の表示

[操作（Operations）] > [レポート（Reports）] > [ISE レポート（ISE Reports）] > [エンドポイントおよびユーザ（Endpoints and Users）] > [クライアント プロビジョニング（Client Provisioning）] ページには、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。[実行（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。

クライアント アクセス セッションの表示

[操作（Operations）] > [レポート（Reports）] > [カタログ（Catalog）] > [ユーザ（User）] > [一意のユーザ（Unique Users）] ページには、特定の期間に起動された既知の特定のクライアント アクセス セッションに関する統計情報が表示されます。[実行（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。

クライアント プロビジョニング リソースの設定変更の表示

[操作（Operations）] > [レポート（Reports）] > [カタログ（Catalog）] > [サーバ インスタンス（Server Instance）] > [サーバ設定監査（Server Configuration Audit）] ページには、最近のクライアント プロビジョニング リソースの設定変更に関する情報が表示されます。[実行（Run）] を選択していずれかのプリセット期間を指定すると、指定した期間内に行われた Cisco ISE のクライアント プロビジョニング リソースの設定変更（たとえば、新しくアップロードされたエージェント バージョン）が表示されます。

サプリカント プロビジョニング要求の表示

[操作（Operations）] > [レポート（Reports）] > [カタログ（Catalog）] > [ユーザ（User）] > [サプリカント プロビジョニング（Supplicant Provisioning）] ウィンドウには、最近の成功および失敗したユーザ デバイス登録およびサプリカント プロビジョニング要求に関する情報が表示されます。[実行（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、ユーザ ID、IP アドレス、MAC アドレス、サーバ、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 ログの表示

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。クライアント プロビジョニングおよびポスチャの監査メッセージおよび診断のロギング エントリをコンパイルして表示できます。

関連項目

- 第 11 章「ロギング」

Cisco NAC Agent ログの収集

Cisco NAC Agent for Windows で、[エージェント トレイ（Agent Tray）] アイコンを右クリックし、[ログ パッケージ（Log Package）] をクリックして、サポート パッケージを実行し、ログを収集します。

Cisco NAC Agent for Mac OS X で、[ツール（Tools）] メニューで [エージェント（Agent）] アイコンを右クリックして、[サポート ログの収集（Collect Support Logs）] オプションをクリックして、エージェントのログとサポート情報を収集します。収集された情報は、ZIP ファイルとして提供されます。ユーザは、ファイルの場所とファイル名を選択して、ファイルを保存できます。デフォルトでは、ファイルは *CiscoSupportReport.zip* というファイル名でデスクトップに保存されます。

エージェントがクラッシュまたはハングした場合は、**CCAAgentLogPackager.app** を実行してログを収集することができます。このファイルは **/Applications/CCAAgent.app** で入手できます。[CCAAgent.app] を右クリックして、[パッケージ コンテンツの表示（Show Package Contents）] を選択し、[CCAAgentLogPackager] をダブルクリックして、サポート情報を収集します。