CHAPTER 17

パーソナル デバイスのサポート

この章では、従業員が企業ネットワーク上で自分のパーソナル デバイスを使用できるようにする方法に関する情報を提供します。

この章の内容は、次のとおりです。

- 「企業ネットワーク上のパーソナル デバイス」（P.17-1）
- 「パーソナル デバイス ポータル」（P.17-1）
- 「従業員アカウント」（P.17-3）
- 「ネイティブ サプリカントを使用したデバイス登録のサポート」（P.17-3）
- 「デバイス ポータルのサポート」（P.17-4）
- 「従業員が追加するパーソナル デバイスの管理」（P.17-7）
- 「ネイティブ サプリカントを使用したパーソナル デバイスの展開シナリオ」（P.17-8）

企業ネットワーク上のパーソナル デバイス

企業ネットワーク上でパーソナル デバイスをサポートする場合は、ユーザおよびそのデバイスを認証および許可することによってネットワーク サービスおよび企業データを保護する必要があります。Cisco ISE 拡張ライセンスでは、従業員が企業ネットワーク上でパーソナル デバイスをセキュアに使用できるために必要なツールを提供しています。

ユーザには、ネットワークにパーソナル デバイスを追加する方法が 2 つあります。ネイティブ サプリカントまたはデバイス ポータルを使用することです。ネイティブ サプリカント プロファイルを作成できます。それによって、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できるようにします。ネイティブ サプリカント プロファイルはすべてのデバイスでは使用できませんが、ユーザはデバイス ポータルを使用して、それらのデバイスを手動で追加できます。

パーソナル デバイス ポータル

Cisco ISE には、従業員が所有するパーソナル デバイスをサポートするいくつかの Web ベースのポータルがあります。

セルフプロビジョニング ポータル

従業員は、ネイティブ サプリカントを使用してパーソナル デバイスを登録するときにセルフプロビジョニング ポータルにアクセスします。従業員がパーソナル デバイスを使用して最初にネットワークへのアクセスを試みると、登録およびサプリカントのインストールの手順が自動的に示されます。デバイスを登録したら、デバイス ポータルを使用して管理できます。

関連項目

- 「ネイティブ サプリカントを使用したデバイス登録のサポート」（P.17-3）

デバイス ポータル

ネットワーク デバイスの中にはネイティブ サプリカントでサポートされていないものがあります。オペレーティング システムがサポートされていない場合や、デバイスに Web ブラウザがない場合（プリンタ、インターネット ラジオや他のデバイスなど）でも、これらのデバイスはネットワークにアクセスする必要があります。企業ネットワークにこれらのタイプのデバイスを追加するには、従業員はデバイス ポータルを使用する必要があります。

従業員は、デバイスの MAC アドレスを入力して、新しいデバイスを追加および管理できます。従業員がデバイス ポータルを使用してデバイスを追加すると、Cisco ISE は [エンドポイント（Endpoints）] ページに RegisteredDevices エンドポイント ID グループのメンバーとしてそのデバイスを追加します。デバイスは Cisco ISE の他のエンドポイントと同様にプロファイリングされ、ネットワークにアクセスするための登録プロセスに進みます。

従業員がネイティブ サプリカントまたはデバイス ポータルを使用してデバイスを登録したかどうかにかかわらず、すべての従業員はデバイス ポータルを使用してパーソナル デバイスを管理できます。

関連項目

- 「エンドユーザ Web ポータルの設定およびカスタマイズ」（P.15-1）
- 「デバイス ポータルのサポート」（P.17-4）
- 「ネイティブ サプリカントでサポートされるオペレーティング システム」（P.17-3）

ブラックリスト ポータル

従業員はデバイスを紛失したかどうかを示すことができます。それにより、そのデバイスはブラックリスト エンドポイント ID グループに追加され、他者がそのデバイスを使用して許可なくネットワークにアクセスすることができなくなります。ユーザがこれらのデバイスの 1 つを使用してネットワークに接続しようとすると、ブラックリスト ポータルにリダイレクトされます。デバイスが見つかった場合、従業員は、デバイスを再登録せずに再開し、ネットワークにアクセスできるようになります。

管理者ポータルを使用して、ブラックリスト ポータルのポート設定（デフォルトはポート 8444）を行うことができます。従業員は、このポータルに直接アクセスしません。

関連項目

- 「エンドユーザ Web ポータルの設定およびカスタマイズ」（P.15-1）

従業員アカウント

Cisco ISE に従業員または契約者を追加すると、ネットワーク上でパーソナル デバイスを使用することを許可できます。外部 ID ストアを使用してそれらを追加した場合でも、または内部ユーザ作成した場合でも、それらがネットワーク上でパーソナル デバイスを使用することを許可できます。

Cisco ISE では、ローカル データベースあるいは外部の Lightweight Directory Access Protocol（LDAP）または Microsoft Active Directory ID ストアによりユーザを認証します。

Cisco ISE には、内部ユーザの従業員ユーザ ID グループがあります。

関連項目

「ユーザの追加」（P.14-3）

ネイティブ サプリカントを使用したデバイス登録のサポート

Cisco ISE ネットワーク上でパーソナル デバイスをサポートするために、ネイティブ サプリカント プロファイルを作成できます。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。

従業員がパーソナル デバイスを使用して最初にネットワークへのアクセスを試みると、登録およびサプリカントの設定の手順が自動的に示されます。従業員がデバイスを登録したら、デバイス ポータルを使用してデバイスを管理できます。

- 「ネイティブ サプリカントでサポートされるオペレーティング システム」（P.17-3）
- 「従業員がネイティブ サプリカントを使用してパーソナル デバイスを登録できるようにする」（P.17-3）

ネイティブ サプリカントでサポートされるオペレーティング システム

ネイティブ サプリカントは、次のオペレーティング システムでサポートされます。

- Android (Amazon Kindle、B&N Nook を除く）
- Mac OS X（Apple Mac コンピュータの場合）
- Apple iOS デバイス（Apple iPod、iPhone および iPad）
- Microsoft Windows 7、Vista、および XP

従業員がネイティブ サプリカントを使用してパーソナル デバイスを登録できるようにする

セルフプロビジョニング フローを使用すると、従業員は、Windows、MacOS、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、ネットワークにデバイスを直接接続することができます。

この機能を有効にしない場合でも、従業員は、デバイス ポータルを使用してパーソナル デバイスを追加することができます。デフォルトでは、この機能はアップグレードしたときは無効になり、Cisco ISE の新規インストールを実行したときは有効になります。

はじめる前に

ネイティブ サプリカント プロファイルを作成する必要があります。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [マルチポータルの設定（Multi-Portal Configurations）] を選択します。

ステップ 2　ポータルを選択し、[編集（Edit）] をクリックします。

ステップ 3　[操作（Operations）] をクリックします。

ステップ 4　[セルフプロビジョニング フローの有効化（Enable Self-Provisioning Flow）] をオンにします。

関連項目

- 「ネイティブ サプリカント プロファイルの作成」（P.22-27）
- 「パーソナル デバイス登録動作の設定」（P.22-28）

デバイス ポータルのサポート

従業員は、パーソナル デバイスを登録および管理するためにデバイス ポータルを使用できます。デバイス ポータルには、ポータルの使用に関する支援を従業員に提供するオンライン ヘルプが含まれています。ただし、従業員がアクセスする前に、ポータルを準備するために行う必要があるいくつかの事柄があります。

関連項目

「デバイス ポータル」（P.17-2）

従業員認証に使用する ID ストア順序の指定

従業員がデバイス ポータルにログインできるようにするには、管理者が ID ストア順序を指定する必要があります。この順序は従業員のログイン クレデンシャルとともに、その従業員を認証してデバイス ポータルへのアクセスを許可するのに使用されます。Cisco ISE には、従業員のデフォルトの ID ストア順序 MyDevices_Portal_Sequence があります。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [デバイス（My Devices）] > [認証ソース（Authentication Source）] を選択します。

ステップ 2　[ID ストア順序（Identity Store Sequence）] ドロップダウン リストから、ID ストア順序を選択します。

ステップ 3　[保存（Save）] をクリックします。

関連項目

- 「デバイス ポータルの設定」（P.A-60）
- 「ID ソース順序の作成」（P.14-40）

デバイス ポータルの有効化

デフォルトでは、デバイス ポータルは有効になっています。無効にした場合、ユーザがその URL に移動しようとしたときに、カスタマイズ可能なエラー メッセージでポータルが使用できないことを通知します。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [デバイス（My Devices）] > [ポータル設定（Portal Configuration）] を選択します。

ステップ 2　[デバイス ポータルの有効化（Enable My Devices Portal）] チェックボックスをオフにします。

ステップ 3　[保存（Save）] をクリックします。

関連項目

「デバイス ポータルの設定」（P.A-60）

従業員のアクセプタブル ユース ポリシーの実装

デバイス ポータルを使用するときに、従業員がアクセプタブル ユース ポリシーを承認するように要求できます。

従業員のアクセプタブル ユース ポリシーのカスタマイズ

従業員にアクセプタブル ユース ポリシーを承認するように要求する場合、会社のポリシーを反映するようにテンプレートを更新する必要があります。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [デバイス（My Devices）] > [言語テンプレート（Language Template）] を選択します。

ステップ 2　ポリシーを適用する言語をクリックします。

ステップ 3　[利用規定ページの設定（Configure Acceptable Use Policy Page）] をクリックし、会社のポリシーに従うようにタイトルとテキストを更新します。

ステップ 4　[保存（Save）] をクリックします。

関連項目

- 「従業員のアクセプタブル ユース ポリシーの要求」（P.17-5）
- 「デバイス ポータルの言語テンプレートの設定」（P.A-59）

従業員のアクセプタブル ユース ポリシーの要求

デバイス ポータルのログイン ページおよびデバイス登録ページにアクセプタブル ユース ポリシーを表示できます。

はじめる前に

アクセプタブル ユース ポリシーを会社のポリシーで更新します。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [デバイス（My Devices）] > [ポータル設定（Portal Configuration）] を選択します。

ステップ 2　[利用規定リンクの有効化（Enable the Acceptable Use Policy Link）] チェックボックスをオンにします。

ステップ 3　[保存（Save）] をクリックします。

関連項目

- 「従業員のアクセプタブル ユース ポリシーのカスタマイズ」（P.17-5）
- 「デバイス ポータルの設定」（P.A-60）

従業員が登録するパーソナル デバイスの制限

従業員が 1 ～ 100 のパーソナル デバイスを登録できるようにすることができます。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [デバイス（My Devices）] > [ポータル設定（Portal Configuration）] を選択します。

ステップ 2　従業員が [デバイス管理（Device Management）] フィールドで登録できるデバイスの最大数を入力します。デフォルトでは、この値は 5 つのデバイスに設定されています。

ステップ 3　[保存（Save）] をクリックします。

関連項目

「デバイス ポータルの設定」（P.A-60）

ヘルプ デスク連絡先詳細のカスタマイズ

この設定により、デバイス ポータルのログイン ページおよびメイン ページにある連絡先リンクに関連付けられた電子メール アドレスと電話番号をカスタマイズすることができます。

はじめる前に

連絡先リンク名を変更する場合は、デバイス言語テンプレート設定（[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [デバイス（My Devices）] > [言語テンプレート（Language Template）] > [その他の項目の設定（Configure Miscellaneous Items）]）で名前を更新する必要があります。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [デバイス（My Devices）] > [ポータル設定（Portal Configuration）] を選択します。

ステップ 2　[電子メール アドレス（Email Address）] および [電話番号（Phone Number）] フィールドにヘルプ デスクの連絡先情報を入力します。

ステップ 3　[保存（Save）] をクリックします。

関連項目：

「デバイス ポータルの設定」（P.A-60）
「デバイス ポータルの言語テンプレートの設定」（P.A-59）

従業員が追加するパーソナル デバイスの管理

従業員がネイティブ サプリカントを使用してデバイスを登録するか、またはデバイス ポータルにデバイスを追加すると、エンドポイント リストに表示されます。従業員はデバイスを削除して、自分のアカウントからデバイスの関連付けを解除できますが、デバイスは Cisco ISE データベースに残っています。この結果、従業員は、これらのデバイスを使用する際発生するエラーを解決するときに支援を必要とする場合があります。

従業員が追加するデバイスの表示

エンドポイントの一覧ページに表示される [ポータル ユーザ（Portal User）] フィールドを使用して、特定の従業員が追加したデバイスを検索できます。これは、特定のユーザが登録したデバイスを削除する必要がある場合に便利です。デフォルトでは、このフィールドは表示されないので、検索する前に最初に有効にする必要があります。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [エンドポイント（Endpoints）] を選択します。

ステップ 2　[設定（Settings）] アイコンをクリックし、[カラム（Columns）] を選択します。

ステップ 3　[ポータル ユーザ（Portal User）] を選択して、エンドポイントの一覧にこの情報を表示します。

ステップ 4　[表示（Show）] ドロップダウン リストをクリックし、[クイック フィルタ（Quick Filter）] を選択します。

ステップ 5　特定のユーザに割り当てられたエンドポイントだけを表示するには、[ポータル ユーザ（Portal User）] フィールドにユーザの名前を入力します。

関連項目

「リスト ページのデータのフィルタリング」（P.2-8）

登録済みエンドポイント レポート

[登録済みエンドポイント レポート（Registered Endpoints report）] には、デバイス登録ポータルから登録されたエンドポイントに関する情報が表示されます。（サプリカント プロビジョニング統計情報および関連データについては、「クライアント プロビジョニング レポートの表示」（P.22-32）を参照してください）。

エンドポイント データベースに対するクエリーを実行して、RegisteredDevices エンドポイント ID グループに割り当て済みのエンドポイントの情報を取得することができます。また、PortalUser 属性がヌル以外の値に設定されている特定のユーザについてレポートを生成することもできます。

[登録済みエンドポイント レポート（Registered Endpoints Report）] には、特定のユーザによって指定の期間内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表示されます。

ステップ 1　Cisco ISE ユーザ インターフェイスにログインします。

ステップ 2　[操作（Operations）] > [レポート（Reports）] > [カタログ（Catalog）] を選択します。

ステップ 3　[レポート（Reports）] ナビゲーション ペインの [デバイス（My Devices）] をクリックします。

ステップ 4　[登録済みエンドポイント（Registered Endpoints）] を選択します。

ステップ 5　[実行（Run）] をクリックします。

ユーザ、登録済みデバイスの MAC アドレス、ID グループ、エンドポイント ポリシーに対するクエリーを実行して、レポートを生成することができます。

デバイスをデバイス ポータルに追加するときのエラー

従業員が追加しようとしているデバイスが、すでに他の従業員によって追加されて Cisco ISE のエンドポイント データベースに存在する場合は、そのデバイスの追加はできません。

従業員がネイティブ サプリカントをサポートするデバイスを追加しようとする場合は、代わりにそれを使用することを推奨します。その登録プロセスでは、元の登録が上書きされ、新しいユーザに所有権が切り替わります。

デバイスが MAC 認証バイパス（MAB）のデバイス（プリンタなど）の場合、デバイスの所有権を解決し、適宜、新しい所有者がデバイスを正常に追加できるようにエンドポイント データベースからそのデバイスを削除する必要があります。

デバイス ポータルから削除されたデバイスはエンドポイント データベースに残っている

従業員がデバイス ポータルからデバイスを削除すると、そのデバイスは登録済みデバイスのリストから削除されますが、そのデバイスは Cisco ISE エンドポイント データベースに残っており、RegisteredDevices エンドポイント ID グループ内に表示されます。[エンドポイント（Endpoints）] ページ（[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [エンドポイント（Endpoints）]）からそのデバイスを完全に削除できます。

ネイティブ サプリカントを使用したパーソナル デバイスの展開シナリオ

ネイティブ サプリカントを使用してパーソナル デバイスをサポートする展開フローは、次の要因によって若干異なります。

- シングルまたはデュアル SSID：1 つの SSID を使用すると、同じ WLAN が証明書登録、プロビジョニング、およびネットワーク アクセスに使用されます。デュアル SSID 展開では、2 つの SSID があります。一方は登録およびプロビジョニングを提供し、他方はセキュアなネットワーク アクセスを提供します。
- Windows、MacOS、iOS、または Android デバイス：ネイティブ サプリカント フローは、デバイス タイプに関係なく同様に、サポートされているパーソナル デバイスを使用している従業員をセルフプロビジョニング ポータルにリダイレクトしてデバイス情報を確認することから開始します。この時点からは、プロセスは、デバイス タイプによって異なります。

従業員がネットワークに接続する

- シングル SSID：従業員は、企業のユーザ名とパスワードを入力して、デバイスを 802.1x SSID に接続します。
- デュアル SSID：従業員は、オープン ゲスト プロビジョニング SSID に接続し、ゲスト ポータルにリダイレクトされ、標準ゲスト ポータルでユーザ クレデンシャルを入力します。

従業員のクレデンシャルが認証される

Cisco ISE は、企業の Active Directory または他の企業の ID ストアに対してユーザを認証し、認可ポリシーを提供します。

デバイスがセルフプロビジョニング ポータルにリダイレクトされる

デバイスは、セルフプロビジョニング ポータルにリダイレクトされます。デバイスの MAC アドレスは自動的に事前に設定されていますが、従業員が確認して、説明を追加できます。

ネイティブ サプリカントが設定される（MacOS、Windows、iOS）

ネイティブ サプリカントが設定されます。プロセスはデバイスによって異なります。

- MacOS および Windows デバイス：ユーザは、セルフプロビジョニング ポータルで [登録（Register）] ボタンをクリックして、サプリカント プロビジョニング ウィザードをダウンロードしてインストールします。サプリカント プロビジョニング ウィザードは、サプリカントを設定し、証明書を提供します（必要な場合）。
- IOS デバイス：Cisco ISE ポリシー サーバは、Apple iOS の無線通信を使用して、次を含む新しいプロファイルを iPad に送信します。
  - （設定されている場合）iPad の MAC アドレスと従業員の Active Directory ユーザ名が埋め込まれた発行済み証明書
  - 802.1X 認証の EAP-MSCHAPv2 または EAP-TLS の使用を強制する Wi-Fi サプリカント プロファイル
- Android デバイス：ユーザは Cisco ISE プロンプトをダウンロードするように求められ、従業員が Google Play から Cisco Network Setup Assistant をダウンロードするように導きます。アプリケーションのインストール後、従業員はそれを開き、セットアップ ウィザードを開始します。それにより、認証パラメータが生成され、デバイス証明書の証明書要求（必要な場合）が開始されます。

許可変更の発行

Cisco ISE は許可変更（CoA）を開始し、MacOS X、Windows、および Android デバイスをセキュアな dot1x ネットワークに接続します。シングル SSID の場合、iOS デバイスも自動的に接続されますが、デュアル SSID の場合、手動で新しいネットワークに接続するようウィザードのプロンプトが表示されます。