個人所有デバイスの持ち込み（BYOD）

企業ネットワークのパーソナル デバイス（BYOD）

企業ネットワーク上のパーソナルデバイスをサポートする場合は、ユーザー（従業員、請負業者、およびゲスト）とそのデバイスを認証および許可することで、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 は、従業員が企業ネットワーク上でパーソナル デバイスを安全に使用できるようにするために必要なツールを提供します。

ゲストは、ゲストポータルへのログイン時に、自動的に自分のデバイスを登録することができます。ゲストは、ゲストタイプに定義されている最大数まで追加デバイスを登録できます。これらのデバイスは、ポータル構成に基づいてエンドポイント ID グループに登録されます。

ゲストは、ネイティブ サプリカント プロビジョニング（Network Setup Assistant）を実行するか、またはデバイスを [デバイス（My Devices）] ポータルに追加して、パーソナル デバイスをネットワークに追加できます。オペレーティング システムに基づいて、使用する適切なネイティブ サプリカント プロビジョニング ウィザードを決定するネイティブ サプリカント プロファイルを作成できます。

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使用できるわけではないため、ユーザーはデバイス ポータルを使用してこれらのデバイスを手動で追加することができます。または、これらのデバイスを登録するように BYOD ルールを設定できます。

Cisco ISE コミュニティ リソース

分散環境のエンドユーザーのデバイス ポータル

Cisco ISE のエンドユーザー Web ポータルは、管理ペルソナ、ポリシー サービス ペルソナ、およびモニタリング ペルソナに基づき、設定、セッション サポート、およびレポート作成を提供します。

- [ポリシー管理ノード（PAN）（Policy Administration node (PAN)）]：ユーザー、デバイス、およびエンドユーザーポータルが PAN に書き込まれる構成の変更。
- [ポリシーサービスノード（PSN）（Policy Service node (PSN)）]：エンドユーザーポータルは PSN で実行する必要があります。ここでは、ネットワークアクセス、クライアントプロビジョニング、ゲストサービス、ポスチャ、およびプロファイリングを含むすべてのセッショントラフィックが処理されます。PSN がノードグループに含まれる場合、1 つのノードで障害が発生すると、他のノードが障害を検出し、保留中のセッションをリセットします。
- [モニタリングノード（MnT ノード）（Monitoring node (MnT node)）]：MnT ノードは、デバイスポータル、スポンサーポータル、およびゲストポータルでのエンドユーザーおよびデバイスのアクティビティについて、データを収集、集約、およびレポートします。プライマリ MnT ノードに障害が発生すると、セカンダリ MnT ノードが自動的にプライマリ MonT ノードになります。

デバイス ポータルのグローバル設定

Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータルの管理（Device Portal Management）] > [設定（Settings）]** を選択します。

BYOD ポータルおよびデバイス ポータルの次の一般設定を設定できます。

- [従業員が登録したデバイス（Employee Registered Devices）]：[従業員を制限（Restrict employees to）] に、従業員が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** デバイスに設定されています。
- [再試行 URL（Retry URL）]：デバイスを Cisco ISE にリダイレクトするために使用できる URL を [オンボードのための再試行 URL（Retry URL for onboarding）] に入力します。

これらの一般的な設定値を設定したら、これらの設定は会社に設定したすべて BYOD ポータルおよびデバイス ポータルに適用されます。

パーソナル デバイス ポータル

Cisco ISE では、従業員が所有するパーソナル デバイスをサポートするために複数の Web ベース ポータルが提供されています。これらのデバイスポータルは、ゲストポータルのフローまたはスポンサー ポータルのフローには関与しません。

- **ブロック済みリストポータル**：ブロックリストに掲載されており、ネットワークへのアクセスには使用できないパーソナルデバイスに関する情報が表示されます。
- **BYOD ポータル**：従業員がネイティブ サプリカント プロビジョニング機能を使用して自分のパーソナルデバイスを登録できるようにします。
- **証明書プロビジョニングポータル**：管理者や従業員が BYOD フローを通過できないデバイスについてユーザー証明書やデバイス証明書を要求できるようにします。
- **クライアント プロビジョニング ポータル**：コンプライアンスをチェックするポスチャエージェントを自分のデバイスにダウンロードするよう従業員に強制します。
- **MDM ポータル**：従業員が外部のモバイルデバイス管理（MDM）システムに自分のモバイルデバイスを登録できるようにします。
- **デバイスポータル**：従業員がパーソナルデバイス（ネイティブ サプリカント プロビジョニングをサポートしないデバイスを含む）を追加および登録し、管理できるようにします。

Cisco ISE には、事前定義済みのデフォルト ポータルのセットを含む複数のデバイス ポータルを Cisco ISE サーバーでホストする機能が用意されています。デフォルトのポータルテーマには、管理者ポータル（[管理（Administration）] > [デバイスポータル管理（Device Portal Management）]）を通じて管理できる標準的なシスコのブランディングが適用されています。組織に固有のイメージ、ロゴ、およびカスケーディング スタイル シート（CSS）ファイルをアップロードして、ポータルをさらにカスタマイズすることもできます。

デバイス ポータルへのアクセス

次のように、Cisco ISE GUI から任意のパーソナルデバイスポータルにアクセスできます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）]** を選択します。

ステップ 2 設定する特定のデバイス ポータルを選択します。

ブロックリスト ポータル

従業員は、このポータルに直接アクセスするのではなく、このポータルにリダイレクトされます。

従業員が自分のパーソナルデバイスを紛失したり、盗まれたりした場合、[デバイス（My Devices）] ポータルでデバイスのステータスを更新して、ブロック済みリストのエンドポイント ID グループにデバイスを追加できます。これにより、不正なネットワーク アクセスにデバイスが使用されることを防ぎます。誰か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、ブロック済みリストポータルにリダイレクトされ、デバイスのネットワークアクセスが拒否されることが通知されます。デバイスが見つかった場合、従業員はデバ

イス ポータルでデバイスを復元し、デバイスを再登録せずにネットワーク アクセスを回復できます。デバイスの盗難か紛失かによっては、デバイスをネットワークに接続する前に、追加のプロビジョニングが必要になる場合があります。

ブロック済みリストポータルのポート設定（デフォルトはポート8444）を設定できます。ポート番号を変更する場合は、別のエンドユーザーポータルで使用されていないことを確認してください。

ブロック済みリストポータルの設定については、ブロックリスト ポータルの編集 （17 ページ）を参照してください。

証明書プロビジョニング ポータル

従業員は、証明書プロビジョニング ポータルに直接アクセスできます。

証明書プロビジョニング ポータルでは、従業員はオンボーディング フローを通過できないデバイスについて証明書を要求することができます。たとえば、販売時点管理端末などのデバイスは、BYOD フローを通過できず、証明書を手動で発行する必要があります。証明書プロビジョニング ポータルで、権限のある一連のユーザーは、そのようなデバイスに対する証明書要求をアップロードし、キーペアを生成し（必要に応じて）、証明書をダウンロードできます。

従業員は、このポータルにアクセスして、1 つの証明書について要求を行うか、または CSV ファイルを使用して一括証明書要求を行うことができます。

ISE コミュニティ リソース

Cisco ISE 証明書プロビジョニングポータルの機能と構成については、「ISE 2.0: Certificate Provisioning Portal」を参照してください。

個人所有デバイスの持ち込みポータル

従業員は、このポータルに直接アクセスしません。

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、個人所有デバイスの持ち込み（BYOD）ポータルにリダイレクトされます。従業員がパーソナルデバイスを使用して初めてネットワークにアクセスを試みると、手動でNetwork Setup Assistant（NSA）ウィザードをダウンロードして起動するように求められ、ネイティブ サプリカントの登録およびインストールに進む場合があります。デバイスを登録すると、デバイス ポータルを使用して、それを管理できます。

NSA およびエージェントウィザードをダウンロードするための Web ブラウザとして Microsoft Edge 93 または Microsoft Edge 94 を使用している場合は、**リダイレクトされた URL** または**ダウンロードリンク**をコピーして新しいタブに貼り付け、キーボードの **Enter** を押します。

あるいは、Microsoft Edge 93 または Microsoft Edge 94 ブラウザで、**[ダウンロード（Download）] アイコン** > **[ダウンロードしたファイルを右クリック（right click on downloaded file）]** > **[ファイルの保持（Keep file）]** をクリックします。

Network Setup Assistant（NSA）およびエージェントウィザードをダウンロードするために Web ブラウザとして Google Chrome 93 または Google Chrome 95 を使用している場合は、ダウンロード通知の [保持（Keep）] オプションをクリックして、システムに NSA および エージェント パッケージを保持してインストールします。

（注）

- BYOD フローは、デバイスが Network Access Manager（NAM）を使用してネットワークに接続すると、サポートされません。
- Android デバイスに BYOD フローを使用している場合は、WLAN 設定で Android 11 にアップグレードするか、[ブロードキャスト SSID（Broadcast SSID）] オプションを有効にします。

関連トピック

BYOD ポータルの作成 （20 ページ）
企業ネットワークのパーソナル デバイス（BYOD） （1 ページ）

クライアント プロビジョニング ポータル

従業員は、このポータルに直接アクセスするのではなく、このポータルにリダイレクトされます。

クライアント プロビジョニング システムでは、企業ネットワークにアクセスしようとしているデバイスのポスチャ評価および修復を行います。従業員がデバイスを使用してネットワークアクセスを要求したときに、クライアント プロビジョニング ポータルにルーティングして、最初にポスチャ エージェントをダウンロードするように要求できます。ポスチャ エージェントは、デバイスにアンチウイルス ソフトウェアがインストールされていることや、オペレーティング システムがサポートされていることの確認など、コンプライアンスに関するデバイスのスキャンを行います。

関連トピック

クライアント プロビジョニング ポータルの作成 （23 ページ）

モバイル デバイス管理ポータル

従業員は、このポータルに直接アクセスするのではなく、このポータルにリダイレクトされます。

数多くの会社で、従業員のモバイル デバイスを管理するために、モバイル デバイス管理（MDM）システムを使用しています。

Cisco ISE では外部 MDM システムとの統合が許可されており、従業員はこれを使用して、モバイルデバイスを登録し、企業ネットワークにアクセスすることができます。シスコでは、従業員がデバイスを登録し、ネットワークに接続するために使用できる外部 MDM インターフェイスを提供しています。

MDM ポータルを使用することで、従業員は外部 MDM システムに登録できます。

従業員は、デバイス ポータルを使用して、PIN コードでのデバイスのロック、工場出荷時のデフォルト設定へのデバイスのリセット、デバイス登録時にインストールされていたアプリケーションおよび設定の削除など、モバイル デバイスの管理を行うことができます。

Cisco ISE では、すべての外部 MDM システム用に単一の MDM ポータルを、または個々の MDM システムごとに 1 つのポータルを使用できます。

MDM サーバーを Cisco ISE とともに動作するように設定する方法については、MDM ポータルの作成 （25 ページ）を参照してください。

デバイス ポータル

従業員は、デバイス ポータルに直接アクセスできます。

ネットワーク アクセスが必要な一部のネットワーク デバイスは、ネイティブ サプリカント プロビジョニングでサポートされていないため、BYOD ポータルを使用して登録することができません。ただし、従業員は、オペレーティングシステムがサポートされていないか、または Web ブラウザが搭載されていないパーソナルデバイス（プリンタ、インターネットラジオ、その他のデバイスなど）を、[デバイス（My Devices）] ポータルを使用して追加および登録することができます。

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（My Devices）] ポータルを使用してデバイスを追加すると、Cisco ISE はそのデバイスを [登録済みデバイス（RegisteredDevices）] エンドポイント ID グループのメンバーとして [エンドポイント（Endpoints）] ウィンドウ（**[管理（Administration）] > [コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）]**）に追加します（別のエンドポイント ID グループに静的に割り当てられている場合を除く）。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 アクセスのための登録プロセスが行われます。

1 つのデバイスからの 2 つの MAC アドレスがユーザーにより [デバイス（My Devices）] ポータルに入力されると、それらが同じホスト名を持ち、Cisco ISE で 1 つのエントリとして統合されていることがプロファイリングによって設定されます。たとえば、ユーザーは有線および無線のアドレスでラップトップを登録します。そのデバイス上での削除などの操作は、両方のアドレスで機能します。

登録済みデバイスがポータルから削除されると、[デバイス登録ステータス（DeviceRegistrationStatus）] と [BYOD 登録状態（BYODRegistration）] の属性はそれぞれ [未登録（NotRegistered）] と [いいえ（No）] に変更されます。ただし、これらの属性は、従業員のデバイス登録時にのみ使用される BYOD 属性であるため、ゲスト（従業員以外）がクレデンシャルを持つゲストポータルの [ゲストデバイス登録（Guest Device Registration）] ウィンドウを使用してデバイスを登録した場合は、変更されずそのままになります。

従業員は、BYOD またはデバイス ポータルを使用して自分のデバイスを登録しているかどうかに関係なく、デバイス ポータルを使用してそれらを管理できます。

（注） 管理者ポータルがダウンしている場合、デバイス ポータルは使用できません。

エンドポイントが [コンテキストの可視性（Context Visibility）] からインポートされても、BYODユーザーアカウントに自動的にリンクされません。デバイスポータルに追加するには、通常の BYOD 登録プロセスに従う必要があります。

関連トピック

デバイス ポータルの作成 （27 ページ）

BYOD の展開オプションとステータス ワークフロー

パーソナルデバイスをサポートするBYOD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：シングル SSID の場合は、同じワイヤレス ローカル エリア ネットワーク（WLAN）が証明書の登録、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。1 つは登録およびプロビジョニングを提供し、もう 1 つ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のフローは、サポートされているパーソナルデバイスを利用する従業員を BYOD ポータルにリダイレクトしてこれらのデバイス情報を確認することによって、デバイスのタイプに関係なく、同様に開始します。プロセスはデバイス タイプに応じて分岐します。

Cisco ISE リリースを使用していて、シングルまたはデュアル SSID BYOD フローの場合、iOS デバイスを持つ BYOD ユーザーはエンタープライズ ネットワークに接続する前に、次の手順を実行する必要があります。

1. **[設定（Settings）]** > **[Safari]**の順に移動します。
2. **[履歴と Web サイトデータを消去（Clear History and Website Data）]** をタップします。

[管理（Administration）] > **[管理（Administration）]** > **[証明書（Certificate）]** > **[システム証明書（System Certificates）]** > **[デフォルト自己署名証明書（Default Self-Signed Certificate）]**ウィンドウの、BYOD 証明書の [サブジェクト代替名（Subject Alternative Name）] フィールドには、DNS 名と IP アドレスの両方を含める必要があります。

従業員がネットワークに接続する

1. Cisco ISE は、会社の Active Directory または会社の他の ID ストアを照合して従業員のクレデンシャルを認証し、認証ポリシーを提供します。
2. デバイスが BYOD 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（MAC address）] フィールドは事前に設定されています。ユーザーはデバイス名と説明を追加できます。

3. ネイティブサプリカント（MacOS、Windows、iOS、Android）が設定されますが、プロセスはデバイスによって異なります。

   • MacOS デバイスと Windows デバイス：従業員が BYOD ポータルで [登録（Register）] をクリックし、サプリカントプロビジョニング ウィザード（Network Setup Assistant）をダウンロードしてインストールします。このウィザードではサプリカントが設定され、EAP-TLS 証明書ベース認証に使用する証明書が（必要に応じて）提供されます。デバイスの MAC アドレスと従業員のユーザー名が発行済み証明書に組み込まれます。

   MacOS 10.15 以降では、ユーザーはサプリカントプロビジョニング ウィザード（SPW）のダウンロードを許可する必要があります。ユーザーのデバイスに、Cisco ISE サーバーからのダウンロードを許可または拒否するように求めるウィンドウが表示されます。

（注） Network Setup Assistant は、そのデバイスのユーザーが管理者権限を持っていない限り、Windows デバイスにダウンロードすることはできません。エンドユーザーに管理者権限を与えることができない場合は、BYOD フローを使用するのではなく、グループ ポリシー オブジェクト（GPO）を使用して証明書をユーザーのデバイスにプッシュします。

   • iOS デバイス：Cisco ISE ポリシーサーバーは Apple の iOS ワイヤレス機能を使用して新しいプロファイルを iOS デバイスに送信します。このプロファイルには次の情報が含まれます。

     • 発行済み証明書（設定されている場合）には iOS デバイスの MAC アドレスと従業員のユーザー名が組み込まれます。

     • 802.1X 認証の EAP-TLS の使用を強制できる Wi-Fi サプリカント プロファイル。追加のプロファイルをエンドポイントデバイスにインストールして、Over-The-Air（OTA）通信を保護できます。

   [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）] チェックボックスをオンにするのは、実際の Wi-Fi ネットワークが非表示の場合に限ります。そうしないと、特にシングル SSID フロー（同じ Wi-Fi ネットワークまたは SSID がオンボーディングと接続の両方に使用されている）の特定の iOS デバイスに対して Wi-Fi ネットワーク設定が適切にプロビジョニングされない場合があります。

   • Android デバイス：Cisco ISE は、従業員に Google Play ストアから Network Setup Assistant（NSA）をダウンロードするように要求し、ルーティングします。アプリケーションのインストール後に、従業員は NSA を開いてセットアップウィザードを開始できます。このウィザードでは、サプリカントの設定と、デバイスの設定に使用される発行済み証明書が生成されます。

4. ユーザーがオンボーディングフローを完了すると、Cisco ISE は認可変更（CoA）を開始します。これにより、MacOS、Windows、および Android デバイスはセキュアな 802.1X ネットワークに再接続します。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、ウィザードは iOS ユーザーに手動で新しいネットワークに接続するように要求します。

サプリカントを使用しない BYOD フローを設定できます。詳細については、Cisco ISE コミュニティリソースに関するドキュメント [英語] を参照してください。

（注） このフローでは、Mac のランダム化は有効ではありません。

Android 10 は新しい接続プロファイルが作成されるたびにランダムな MAC アドレスを生成するため、BYOD フローが Android クライアントで動作するためには、デフォルトルールを変更して、認証プロファイルから *BYOD_is_Registered* および *MAC_in_SAN* 条件を削除する必要があります。

BYOD セッション エンドポイント属性

エンドポイント属性 *BYODRegistration* の状態は、BYOD フローにおいて次の状態に変化します。

- *Unknown*：デバイスは BYOD フローを完了していません。
- *Yes*：デバイスは BYOD フローを通過し、登録されました。
- *No*：デバイスは BYOD フローを完了しましたが、登録されていません。つまり、デバイスは削除されています。

デバイス登録ステータスのエンドポイント属性

エンドポイント属性 *DeviceRegistrationStatus* の状態は、デバイス登録中に次の状態に変化します。

- *Registered*：デバイスは BYOD フローを完了し、登録されました。この属性が Pending から Registered になるまでに 20 分の遅れがあります。
- *Pending*：デバイスは BYOD フローを完了し、登録されています。ただし、Cisco ISE はネットワーク上でそれを認識していません。
- *Not Registered*：デバイスは BYOD フローを完了していません。*Not Registered* は、*DeviceRegistrationStatus* 属性のデフォルトの状態です。
- *Stolen*：ユーザーが [デバイス（My Devices）] ポータルにログインし、現在オンボーディングされているデバイスを Stolen としてマークしました。次のようになります。
  - 証明書とプロファイルをプロビジョニングしてデバイスのオンボーディングが行われた場合、Cisco ISE はそのデバイスに対してプロビジョニングされた証明書を失効さ

せ、デバイスの MAC アドレスを ブロック済みリストのエンドポイント ID グループに割り当てます。そのデバイスはネットワークにアクセスできなくなります。

- （証明書は含めず）プロファイルのみをプロビジョニングしてデバイスのオンボーディングが行われた場合、Cisco ISE はそのデバイスを ブロック済みリストのエンドポイント ID グループに割り当てます。この状況に対応する認証ポリシーを作成していない場合は、デバイスは引き続きネットワークにアクセスできます。たとえば、**エンドポイント ID グループがブロック済みリストであり、BYOD_is_Registered の場合は DenyAccess となります。**

管理者は、さまざまなデバイスに対してネットワークアクセスを無効にするアクション（証明書の削除や失効など）を実行します。

ユーザーが盗まれたデバイスを復元すると、ステータスは *Not Registered* に戻ります。ユーザーはそのデバイスを削除してからもう一度追加する必要があります。これにより、オンボーディングプロセスが開始されます。

- *Lost*：ユーザーが [デバイス（My Devices）] ポータルにログオンし、現在オンボーディングされているデバイスを *Lost* としてマークしたため、次のアクションが実行されます。
  - そのデバイスは ブロック済みリストの ID グループに割り当てられます。
  - デバイスに対してプロビジョニングされた証明書は失効します。
  - デバイスのステータスが *Lost* に更新されます。
  - *BYODRegistration* ステータスが *No* に更新されます。

紛失デバイスをブロックする許可ポリシーを作成していない場合、紛失デバイスは引き続きネットワークにアクセスできます。ルールで ブロック済みリストの ID グループまたはルールで *endpoint:BYODRegistration* 属性を使用できます。たとえば、**エンドポイント ID グループがブロック済みリストで EndPoints:BYODRegistrations が No の場合は BYOD** になります。きめ細かなアクセスを設定するには、*NetworkAccess:EAPAuthenticationMethod Equals PEAP or EAP-TLS or EAP-FAST" , InternalUser:IdentityGroup Equals <<group>>* をルールの IF 部分に追加することもできます。

従業員が登録するパーソナル デバイス数の制限

従業員が 1 ～ 999 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。従業員がパーソナルデバイスの登録に使用したポータルに関係なく、この設定では、すべてのポータルにわたって登録されるデバイスの最大数を定義します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [設定（Settings）] > [従業員が登録するデバイス（Employee Registered Devices）]** を選択します。

ステップ 2 [従業員を制限（Restrict employees to）] に、従業員が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** 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。設定の更新を保存しない場合は、[リセット（Reset）]をクリックして、最後に保存した値に戻します。

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

ネイティブ サプリカント プロファイルを作成して、Cisco ISE ネットワークでパーソナル デバイスをサポートできます。ユーザーの許可要件に関連付けるプロファイルに基づいて、Cisco ISE はネットワークにアクセスするユーザーのパーソナル デバイスをセットアップ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ます。

従業員がパーソナルデバイスを使用して初めてネットワークへのアクセスを試みると、登録とサプリカントの設定の手順が自動的に示されます。デバイスを登録した後、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 サプリカントがサポートす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）
- MacOS（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、8（RT を除く）、Vista、および 10

クレデンシャルを持つゲスト ポータルを使用したパーソナル デバイスの登録を従業員に許可

クレデンシャルを持つゲスト ポータルを利用している従業員は、自分のパーソナル デバイスを登録できます。BYOD ポータルによって提供されるセルフ プロビジョニング フローにより、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できます。

始める前に

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Center）] > [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）]** を選択します。

ステップ 2 従業員がネイティブ サプリカントを使用して自分のデバイスを登録するために使用できるクレデンシャルを持つゲスト ポータルを選択し、[編集（Edit）] をクリックします。

ステップ 3 [ポータルの動作とフロー設定（Portal Behavior and Flow Settings）] タブをクリックします。

ステップ 4 [BYOD 設定（BYOD Settings）] で [従業員にネットワークでのパーソナルデバイスの使用を許可する（Allow employees to use personal devices on the network）] チェックボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。

BYOD 登録に再接続する URL の提供

BYOD ポータルを使用してパーソナル デバイスを登録中に問題が発生した従業員に、登録プロセスへの再接続を可能にする情報を提供できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [設定（Settings）] > [再試行 URL（Retry URL）]** を選択します。

ステップ 2 [オンボードのための再試行 URL（Retry URL for onboarding）] フィールドに、デバイスを Cisco ISE にリダイレクトするために使用できる URL を入力します。

登録プロセス中にデバイスに問題が発生した場合、デバイスはインターネットに自動的に再接続しようとします。この時点で、このフィールドに入力した URL を使用してデバイスが Cisco ISE にリダイレクトされ、オンボーディングプロセスが再開されます。デフォルト値は 192.0.2.123 です。

ステップ 3 [保存（Save）] をクリックします。

設定の更新を保存しない場合は、[リセット（Reset）] をクリックして、最後に保存した値に戻します。

デバイス ポータルの設定タスク

デフォルト ポータルと、証明書、エンドポイント ID グループ、ID ソース順序、ポータル テーマ、イメージ、および Cisco ISE によって提供されるその他の詳細などのデフォルト設定を使用できます。デフォルト設定を使用しない場合は、新しいポータルを作成するか、必要性に合うように既存の設定を編集する必要があります。同じ設定で複数のポータルを作成する場合は、ポータルを複製できます。

新しいポータルを作成したり、デフォルト ポータルを編集した後は、ポータルの使用を承認する必要があります。いったんポータルの使用を承認すると、後続の設定変更はただちに有効になります。

デバイス ポータルを使用するための許可は必要ありません。

ポータルを削除する場合は、関連付けられている許可ポリシー ルールおよび許可プロファイルを先に削除するか、別のポータルを使用するように変更する必要があります。

この表を使用して、異なるデバイス ポータルの設定に関連するタスクを確認できます。

タスク	ブロックリスト ポータル	BYOD ポータル	クライアント プロビジョニング ポータル	MDM ポータル	デバイス ポータル
ポリシー サービスの有効化（14 ページ）	必須	必須	必須	必須	必須
デバイス ポータルへの証明書の追加（14 ページ）	必須	必須	必須	必須	必須
外部 ID ソースの作成（15 ページ）	不要	不要	不要	不要	必須
ID ソース順序の作成（16 ページ）	不要	不要	不要	不要	必須
エンドポイント ID グループの作成（16 ページ）	不要	必須	不要	必須	必須
ブロックリスト ポータルの編集	必須	N/A	N/A	N/A	N/A
BYOD ポータルの作成（20 ページ）	N/A	必須	N/A	N/A	N/A
クライアント プロビジョニング ポータルの作成（23 ページ）	N/A	N/A	必須	N/A	N/A
MDM ポータルの作成（25 ページ）	N/A	N/A	N/A	必須	N/A
デバイス ポータルの作成（27 ページ）	N/A	N/A	N/A	N/A	必須

タスク	ブロックリスト ポータル	BYOD ポータル	クライアント プロビジョニング ポータル	MDM ポータル	デバイス ポータル
許可プロファイルの作成（28 ページ）	N/A	必須	必須	必須	不要
デバイス ポータルのカスタマイズ（30 ページ）	オプション	オプション	オプション	オプション	オプション

ポリシー サービスの有効化

Cisco ISE エンドユーザー Web ポータルをサポートするには、ホストするノードでポータルポリシーサービスを有効に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（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [展開（Deployment）]** の順に選択します。

ステップ 2 ノードをクリックして、[編集（Edit）] をクリックします。

ステップ 3 [全般設定（General Settings）] タブで [ポリシーサービス（Policy Service）] トグルボタンを有効にします。

ステップ 4 [セッションサービスの有効化（Enable Session Services）] チェックボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。

デバイス ポータルへの証明書の追加

デフォルトの証明書を使用しない場合は、有効な証明書を追加して、証明書グループ タグに割り当てることができます。すべてのエンドユーザー Web ポータルに使用されるデフォルトの証明書グループタグは [デフォルトポータル証明書グループ（Default Portal Certificate Group）] です。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。

ステップ 2 システム証明書を追加し、ポータルに使用する証明書グループ タグに割り当てます。

この証明書グループ タグは、ポータルを作成または編集するときに選択できるようになります。

ステップ 3 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータルの管理（Device Portal Management）] >（任意のポータル）> [作成または編集（Create or Edit）] > [ポータル設定（Portal Settings）]** を選択します。

ステップ 4 新しく追加された証明書に関連付けられた [証明書グループ タグ（Certificate Group Tag）] ドロップダウン リストから特定の証明書グループ タグを選択します。

（注）
- BYOD は長さが 3 つの証明書を超える証明書チェーンをサポートしていません。
- BYOD オンボーディング時に、iOS デバイスに対して証明書が 2 回発行されます。

外部 ID ソースの作成

Cisco ISE では、Active Directory、LDAP、RADIUS トークン、RSA SecurID サーバーなどの外部 ID ソースに接続して、認証/許可のユーザー情報を取得できます。外部 ID ソースには、証明書ベースの認証に必要な証明書認証プロファイルも含まれています。

（注） 認証済みユーザー ID を受信して共有できるようにするパッシブ ID サービスを使用するには、その他の パッシブ ID サービス プロバイダー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（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）]** を選択します。

ステップ 2 次のオプションのいずれかを選択します。

- 証明書認証プロファイル（Certificate Authentication Profile）：証明書ベースの認証の場合。
- Active Directory：外部 ID ソースとして Active Directory に接続する場合。詳細については、外部 ID ソースとしての Active Directoryを参照してください。
- LDAP：LDAP ID ソースを追加する場合。詳細については、LDAPを参照してください。
- RADIUS トークン（RADIUS Token）：RADIUS トークン サーバーを追加する場合。詳細については、RADIUS トークン ID ソースを参照してください。
- RSA SecurID：RSA SecurID サーバーを追加する場合。詳細については、RSA ID ソースを参照してください。
- SAML IDプロバイダー（SAML Id Providers）：Oracle Access Manager などの ID プロバイダー（IdP）を追加する場合。詳細については、外部 ID ソースとしての SAMLv2 ID プロバイダーを参照してください。
- ソーシャルログイン（Social Login）：Facebook などのソーシャルログインを外部 ID ソースとして追加する場合。詳細については、アカウント登録ゲストのソーシャル ログインを参照してください。

ID ソース順序の作成

始める前に

Cisco ISE に外部 ID ソースを設定していることを確認します。

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ゲストユーザーがローカル WebAuth を使用して認証できるようにするには、ゲストポータル認証ソースと ID ソース順序の両方に同じ ID ストアが含まれるように設定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（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）] > [追加（Add）]** を選択します。

ステップ 2 ID ソース順序の名前を入力します。また、任意で説明を入力できます。

ステップ 3 [証明書認証プロファイル（Certificate Authentication Profile）] チェックボックスをオンにし、証明書ベースの認証のための証明書認証プロファイルを選択します。

ステップ 4 [選択済み（Selected）] リストフィールドの ID ソース順序に含めるデータベースを選択します。

ステップ 5 Cisco ISE がデータ ベースを検索する順序に [選択済み（Selected）] リストフィールドのデータベースを並べ替えます。

ステップ 6 選択したアイデンティティストアに認証のためにアクセスできない場合は、[高度な検索リスト（Advanced Search List）] 領域で次のいずれかのオプションを選択します。

- [順序内の他のストアにアクセスせず、AuthenticationStatus属性をProcessErrorに設定（Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError）]
- [ユーザーが見つからなかったとして処理し、順序内の次のストアに進む（Treat as if the user was not found and proceed to the next store in the sequence）]

  Cisco ISE では、要求の処理中にこれらの ID ソースが順番に検索されます。[選択済み（Selected）] リストフィールドに Cisco ISE が ID ソースを検索する順序で ID ソースが表示されていることを確認します。

ステップ 7 [送信（Submit）] をクリックして ID ソース順序を作成すると、その後この ID ソース順序をポリシーで使用できます。

エンドポイント ID グループの作成

Cisco ISE では、検出したエンドポイントを、対応するエンドポイント ID グループにグループ化します。Cisco ISE では、システム定義された複数のエンドポイントの ID グループが事前に用意されています。[エンドポイントIDグループ（Endpoint Identity Groups）] ウィンドウでは、追加のエンドポイント ID グループも作成できます。作成したエンドポイント ID グループを編

集または削除できます。システムで定義されたエンドポイント ID グループの説明のみを編集できます。これらのグループの名前を編集または削除することはできません。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [グループ（Groups）] > [エンドポイント ID グループ（Endpoint Identity Groups）]** 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 作成するエンドポイント ID グループの [名前（Name）] に入力します（エンドポイント ID グループの名前にはスペースを入れないでください）。

ステップ 4 作成するエンドポイント ID グループの [説明（Description）] に入力します。

ステップ 5 [親グループ（Parent Group）] ドロップダウン リストをクリックして、新しく作成したエンドポイント ID グループを関連付けるエンドポイント ID グループを選択します。

ステップ 6 [送信（Submit）] をクリックします。

ブロックリスト ポータルの編集

Cisco ISE では、Cisco ISE でブロックリストに登録されている、紛失したり、盗難にあったりしたデバイスが企業のネットワークへのアクセスを試行した場合に、情報が表示される単一のブロックリストポータルが提供されます。

デフォルトのポータル設定を編集し、ポータルについて表示されるデフォルトのメッセージをカスタマイズすることのみができます。新しいブロックリストポータルを作成することはできず、デフォルトポータルを複製または削除することもできません。

始める前に

このポータルで使用するために、必要な証明書が設定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（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [ブロックリストポータル（Blocked List Portal）] > [編集（Edit）]** を選択します。

ステップ 2 ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。

ここで使用するポータル名が他のエンドユーザー ポータルに使用されていないことを確認します。

ステップ 3 [言語ファイル（Language File）] ドロップダウンリストから、ポータルで使用する言語ファイルをインポートまたはエクスポートする目的のアクションを選択します。

ステップ 4 [ポータルテストURL（Portal test URL）] リンクをクリックすると、このポータルの URL を表示する新しいブラウザタブが開きます。ポリシーサービスを含むポリシーサービスノード（PSN）をオンにする必要があります。ポリシーサービスがオンになっていない場合、PSN は管理者用ポータルのみを表示します。

（注） テストポータルはRADIUSセッションをサポートしていないため、すべてのポータルに対するポータルフローの全体は表示されません。BYODおよびクライアント プロビジョニングはRADIUSセッションに依存するポータルの例です。たとえば、外部URLへのリダイレクションは機能しません。複数の PSN がある場合、Cisco ISE は最初のアクティブ PSN を選択します。

ステップ 5 [ポータル設定（Portal Settings）] を展開します。ポート、証明書グループタグ、エンドポイントID グループなどのデフォルト値を更新し、ポータル全体に適用する動作を定義します。

- [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、ブロックリストポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このウィンドウで変更を加えるまで維持されます。このウィンドウを変更する場合は、この制限に従うようにポート設定を更新します。

  ゲストポータルに非ゲストポータル（[デバイス（My Devices）] など）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

  ポスチャ評価と修復についてのみ、クライアント プロビジョニング ポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲストポータルへの割り当てと同じポートを使用します。

  同じ HTTPS ポートに割り当てられたポータルは、同じギガビット イーサネット インターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループ タグを使用する必要があります。次に例を示します。

  - スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブロック済みリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
  - 無効な組み合わせには次が含まれます。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：**8443**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブロック済みリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**

  （注） 最適なパフォーマンスを得るには、ゲストサービスにインターフェイス 0 を使用することを推奨します。[ポータル設定（Portal Settings）] ではインターフェイス 0 のみを設定できます。または、CLI コマンド **ip host** を使用して、ホスト名またはFQDNをインターフェイス 0 の IP アドレスにマッピングすることもできます。

- [使用可能インターフェイス（Allowed Interfaces）]：PANがポータルの実行に使用できるPSNインターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポート

を探します。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。

これらの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すべての PSN（VM ベースを含む）で使用可能である必要があります。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、必須要件です。

- イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用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またはサブジェクトの代替名はインターフェイス IP アドレスに解決する必要があります。
- ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリインターフェイスの IP アドレスを FQDN にマッピングします。これは、証明書のサブジェクト名、またはサブジェクトの代替名と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、おそらくは、そのPSNでボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
- NIC チーミングまたはボンディングは、ハイアベイラビリティ（耐障害性）を実現するために 2 つの個別の NIC を設定できる 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（Portal Settings）] に基づいてポータルに選択されます。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は、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を指定する証明書グループタグを選択します。
- **表示言語**
  - [ブラウザのロケールを使用する（Use Browser Locale）]：クライアントブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザのロケールの言語が Cisco ISE でサポートされていない場合は、[フォールバック言語（Fallback Language）] が言語ポータルとして使用されます。
  - [フォールバック言語（Fallback Language）]：ブラウザロケールから言語を取得できない場合、またはブラウザロケール言語が Cisco ISE でサポートされていない場合に使用する言語を選択します。

- [常に使用（Always Use）]：ポータルに使用する表示言語を選択します。この設定は、ユーザーの [ブラウザのロケールを使用する（User Browser Locale）] オプションを上書きします。

ステップ 6 [ポータル ページのカスタマイズ（Portal Page Customization）] タブで、許可されていないデバイスがネットワークへのアクセスの取得を試行した場合にポータルに表示されるページタイトルおよびメッセージテキストをカスタマイズします。

ステップ 7 [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

BYOD ポータルの作成

Bring Your Own Device（BYOD; 個人所有デバイス持ち込み）ポータルを提供して、ネットワークへのアクセスの許可の前に登録とサプリカント構成を行うことができるように、従業員が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。

新しいBYODポータルを作成するか、既存のものを編集または複製できます。Cisco ISEによって提供されているデフォルトのポータルを含むすべての BYOD ポータルを削除できます。

[ポータルの動作とフローの設定（Portal Behavior and Flow Settings）] タブのしたにある [ポータルとページの設定（Portal & Page Settings）] に加えた変更は、デバイスポータルフロー図のグラフィカル フローに反映されます。[サポート情報（Support Information）] ウィンドウなどのウィンドウを有効にすると、そのウィンドウがフローに表示され、従業員はポータルで使用できるようになります。ウィンドウを無効にすると、フローから削除されます。

始める前に

このポータル内で使用するために、必要な証明書とエンドポイント ID グループが設定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（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [BYOD] > [作成（Create）]** を選択します。

ステップ 2 ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。

ここで使用するポータル名が他のエンドユーザーポータルに使用されていないことを確認します。

ステップ 3 [言語ファイル（Language File）] ドロップダウンリストから、ポータルで使用する言語ファイルをインポートまたはエクスポートする目的のアクションを選択します。

ステップ 4 [ポータルの動作とフロー設定（Portal Behavior and Flow Settings）] タブをクリックします。

ステップ 5 [ポータル設定（Portal Settings）] を展開します。ポート、証明書グループタグ、エンドポイント ID グループなどのデフォルト値を更新し、ポータル全体に適用する動作を定義します。

ステップ 6 [サポート情報ページの設定（Support Information Page Settings）] を展開します。ネットワークアクセスの問題のトラブルシューティングのためにヘルプデスクが使用する情報を従業員が提供するのに役立つように、ここで必要な情報を更新します。

ステップ 7 [ポータルページのカスタマイズ（Portal Page Customizations）] タブをクリックします。次のエンドユーザーポータル ウィンドウをカスタマイズするには、[ページのカスタマイズ（Page Customizations）] 領域までスクロールします。左側のメニューにある [ページ（Pages）] にリストされている対応するオプションをクリックして、カスタマイズするポータルウィンドウを選択します。

- **[BYOD ようこそ（BYOD Welcome）]**：
  - **[デバイス構成が必要（Device Configuration Required）]**：デバイスが BYOD ポータルに初めてリダイレクトされ、証明書のプロビジョニングが必要な場合、表示される内容を入力します。
  - **[証明書の更新が必要（Certificate Needs Renewal）]**：前の証明書が更新される必要がある場合、表示される内容を入力します。
- **[BYOD デバイス情報（BYOD Device Information）]**：
  - **[最大デバイス数に到達（Maximum Devices Reached）]**：従業員が登録できるデバイスの最大数に到達した場合、表示される内容を入力します。
  - **[必要なデバイス情報（Required Device Information）]**：従業員がデバイスを登録できるようにするために必要なデバイス情報を要求している場合、表示される内容を入力します。
- **[BYOD インストール（BYOD Installation）]**：
  - **[デスクトップインストール（Desktop Installation）]**：デスクトップデバイス用のインストール情報を提供する場合、表示される内容を入力します。
  - **[iOS インストール（iOS Installation）]**：iOS モバイルデバイス用のインストールの指示を提供する場合、表示される内容を入力します。
  - **[Android インストール（Android Installation）]**：Android モバイルデバイス用のインストールの指示を提供する場合、表示される内容を入力します。
- **[BYOD成功（BYOD Success）]**：
  - **[成功（Success）]**：デバイスが設定され、自動的にネットワークに接続される場合、表示される内容を入力します。
  - **[成功：手動手順（Success: Manual Instructions）]**：デバイスが正常に設定され、従業員がネットワークに手動で接続する必要がある場合、表示される内容を入力します。
  - **[成功：サポート対象外のデバイス（Success: Unsupported Device）]**：サポート対象外のデバイスがネットワークに接続できる場合、表示される内容を入力します。

ステップ 8 [保存（Save）] をクリックして、さらに [閉じる（Close）] をクリックします。

次のタスク

ポータルを使用するには、そのポータルを許可する必要があります。ポータルを使用できるように許可する前または後に、ポータルをカスタマイズすることもできます。

クライアント プロビジョニング ポータルの作成

Cisco ISE では証明書プロビジョニング ポータルが提供され、そこではオンボーディング フローを通過できないデバイスについて証明書を要求することができます。たとえば、販売時点管理端末などのデバイスがあります。1つの証明書について要求を行うか、またはCSVファイルを使用して一括証明書要求を行うことができます。

デフォルトのポータル設定を編集し、ポータルに表示されるメッセージをカスタマイズすることができます。また、証明書プロビジョニング ポータルを作成、複製、および削除することもできます。

証明書プロビジョニング ポータルにアクセスできるユーザーには 2 つのタイプがあります。

- 管理者権限を持つ内部または外部のユーザー：自分自身と他人に対し証明書を生成できます。
- 他のすべてのユーザー：自身の証明書のみを生成できます。

スーパー管理ロールまたは ERS 管理ロールを割り当てられたユーザー（ネットワーク アクセスユーザー）はこのポータルにアクセスでき、他人のために証明書を要求できます。ただし、新しい内部管理ユーザーを作成し、スーパー管理ロールまたは ERS 管理ロールを割り当てると、内部管理ユーザーはこのポータルにアクセスできません。最初にネットワーク アクセス ユーザーを作成し、それからユーザーをスーパー管理グループまたは ERS 管理グループに追加する必要があります。スーパー管理グループまたは ERS 管理グループに追加されている既存のネットワーク アクセス ユーザーは、このポータルにアクセスできます。

他のユーザーがポータルにアクセスして自身の証明書を生成できるようにするには、[証明書プロビジョニングポータルの設定（Certificate Provisioning Portal Settings）] を設定します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [証明書プロビジョニング（Certificate Provisioning）] > [編集（Edit）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）]**。[認証方式（Authentication Method）] で適切な ID ソースまたは ID ソース順序を選択し、[承認済みグループの設定（Configure Authorized Groups）] でユーザー グループを選択します。選択したグループに属するすべてのユーザーが、ポータルにアクセスし、自分自身の証明書を生成できるようになります。

始める前に

このポータルで使用するために、必要な証明書が設定されていることを確認します。

ステップ 1 **[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [証明書プロビジョニング（Certificate Provisioning）]** > [作成（Create）]Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。。

ここで使用するポータル名が他のエンドユーザー ポータルに使用されていないことを確認します。

ステップ 2 ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。

ステップ 3 [言語ファイル（Language File）] ドロップダウンリストから、ポータルで使用する言語ファイルをインポートまたはエクスポートする目的のアクションを選択します。

ステップ 4 [ポータルの動作とフロー設定（Portal Behavior and Flow Settings）] タブをクリックします。

ステップ 5 [ポータル設定（Portal Settings）] を展開します。ポート、証明書グループタグ、エンドポイント ID グループなどのデフォルト値を更新し、ポータル全体に適用する動作を定義します。

ステップ 6 [ポータルページのカスタマイズ（Portal Page Customizations）] タブをクリックします。ポータルに表示されるページのタイトルとメッセージのテキストをカスタマイズします。

ステップ 7 [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

クライアント プロビジョニング ポータルの作成

クライアント プロビジョニング ポータルを提供して、ネットワークへのアクセスを許可する前に、デバイスのポスチャ遵守を確認する エージェントのポスチャコンポーネント を従業員がダウンロードできるようにすることが可能です。

新しいクライアント プロビジョニング ポータルを作成するか、既存のものを編集または複製できます。Cisco ISE によって提供されているデフォルトのポータルを含むすべてのクライアント プロビジョニング ポータルを削除できます。

スーパー管理ロールまたは ERS 管理ロールを割り当てられたユーザー（ネットワーク アクセス ユーザー）はこのポータルにアクセスできます。ただし、新しい内部管理ユーザーを作成し、スーパー管理ロールまたはERS管理ロールを割り当てると、内部管理ユーザーはこのポータルにアクセスできません。最初にネットワーク アクセス ユーザーを作成し、それからユーザーをスーパー管理グループまたは ERS 管理グループに追加する必要があります。スーパー管理グループまたは ERS 管理グループに追加されている既存のネットワーク アクセス ユーザーは、このポータルにアクセスできます。

他のユーザーがポータルにアクセスして自身の証明書を生成できるようにするには、[証明書プロビジョニングポータルの設定（Certificate Provisioning Portal Settings）] を設定します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[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（Client Provisioning）] > [編集（Edit）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）]** です。[認証方式（Authentication Method）] で適切な ID ソースまたは ID ソース順序を選択し、[承認済みグループの設定（Configure Authorized Groups）] でユーザー グループを選択します。選択したグループに属するすべてのユーザーが、ポータルにアクセスし、自分自身の証明書を生成できるようになります。

[ポータルの動作とフローの設定（Portal Behavior and Flow Settings）] タブのしたにある [ポータルとページの設定（Portal & Page Settings）] に加えた変更は、デバイスポータルフロー図のグラフィカル フローに反映されます。[サポート情報（Support Information）] ウィンドウなどのウィンドウを有効にすると、そのウィンドウがフローに表示され、従業員はポータルで使用できるようになります。ウィンドウを無効にすると、フローから削除されます。

始める前に

このポータルで使用するために設定されている必要な証明書とクライアントプロビジョニングポリシーが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（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータルの管理（Device Portal Management）] > [クライアントプロビジョニング（Client Provisioning）] > [作成（Create）** を選択します。

ステップ 2 ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。

ここで使用するポータル名が他のエンドユーザーポータルに使用されていないことを確認します。

ステップ 3 [言語ファイル（Language File）] ドロップダウンリストから、ポータルで使用する言語ファイルをインポートまたはエクスポートする目的のアクションを選択します。

ステップ 4 [ポータルの動作とフロー設定（Portal Behavior and Flow Settings）] タブをクリックします。

ステップ 5 [ポータル設定（Portal Settings）] を展開します。ポート、証明書グループタグ、エンドポイント ID グループなどのデフォルト値を更新し、ポータル全体に適用する動作を定義します。

ステップ 6 [サポート情報ページの設定（Support Information Page Settings）] を展開します。ネットワークアクセスの問題のトラブルシューティングのためにヘルプデスクが使用する情報を従業員が提供するのに役立つように、ここで必要な情報を更新します。

ステップ 7 [ポータルページのカスタマイズ（Portal Page Customizations）] タブをクリックします。次のエンドユーザーポータル ウィンドウをカスタマイズするには、[ページのカスタマイズ（Page Customizations）] 領域までスクロールします。左側のメニューにある [ページ（Pages）] にリストされている対応するオプションをクリックして、カスタマイズするポータルウィンドウを選択します。

- **[クライアントプロビジョニングポータル（Client Provisioning Portals）]**：
  - **[不明なエージェント（Agent Unknown）]**：エージェントが不明な場合に表示される内容を入力します。
  - **[確認（Checking）]、[スキャン（Scanning）]、[準拠（Compliant）]**：ポスチャエージェントが正常にインストールされ、デバイスがポスチャ要件に準拠していることを確認、スキャン、および検証する場合に表示される内容を入力します。
  - **[非準拠（Non-compliant）]**:ポスチャエージェントが、デバイスがポスチャ要件に準拠していないと判断した場合に表示される内容を入力します。
- **[クライアントプロビジョニング（エージェント未検出）（Client Provisioning (Agent Not Found)）]**：
  - **[エージェントが見つかりませんでした（Agent Not Found）]**：ポスチャエージェントがデバイスで検出されない場合に表示される内容を入力します。
  - **[手動インストールの手順（Manual Installation Instructions）]**：デバイスに Java または Active X ソフトウェアがインストールされていない場合に表示される内容、ポスチャエージェントを手動でダウンロードし、インストールする方法の手順を入力します。
  - **[インストール、Java/ActiveX なし（Install, No Java/ActiveX）]**：デバイスに Java または Active X ソフトウェアがインストールされていない場合に表示される内容、手動で Java プラグインをダウンロードしてインストールする方法の手順を入力します。

- **[エージェントインストール済み（Agent Installed）]**：ポスチャエージェントがデバイスで検出された場合に表示される内容、ポスチャエージェントを開始する方法の手順を入力します。ポスチャエージェントにより、デバイスがポスチャ要件に準拠するかどうかが確認されます。

ステップ 8 [保存（Save）] をクリックして、さらに [閉じる（Close）] をクリックします。

次のタスク

ポータルを使用するには、そのポータルを許可する必要があります。ポータルを使用できるように許可する前または後に、ポータルをカスタマイズすることもできます。

関連トピック

ポータルの許可

デバイス ポータルのカスタマイズ （30 ページ）

MDM ポータルの作成

モバイル デバイス管理（MDM）ポータルを提供して、従業員が、企業ネットワークでの使用のために登録されたモバイル デバイスを管理できるようにすることができます。

新しい MDM ポータルを作成するか、既存のものを編集または複製できます。すべての MDM システムに対して 1 つの MDM ポータルを設定できます。または、各システムに対し 1 つのポータルを作成できます。Cisco ISE によって提供されているデフォルトのポータルを含むすべての MDM ポータルを削除できます。デフォルトのポータルは、サードパーティの MDM プロバイダー用です。

新しいMDMポータルを作成するか、既存のものを編集または複製できます。Cisco ISEによって提供されているデフォルトのポータルを含むすべての MDM ポータルを削除できます。デフォルトのポータルは、サードパーティの MDM プロバイダー用です。

[ポータルの動作とフローの設定（Portal Behavior and Flow Settings）] タブのしたにある [ポータルとページの設定（Portal & Page Settings）] に加えた変更は、デバイスポータルフロー図のグラフィカル フローに反映されます。[サポート情報（Support Information）] ウィンドウなどのウィンドウを有効にすると、そのウィンドウがフローに表示され、従業員はポータルで使用できるようになります。ウィンドウを無効にすると、フローから削除されます。

始める前に

このポータルで使用するために、必要な証明書とエンドポイント ID グループが設定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（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **[モバイルデバイス管理（Mobile Device Management）]** > **[作成、編集または複製（Create, Edit or Duplicate）]** を選択します。

ステップ 2 ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。

ここで使用するポータル名が他のエンドユーザーポータルに使用されていないことを確認します。

ステップ 3 [言語ファイル（Language File）] ドロップダウンリストから、ポータルで使用する言語ファイルをインポートまたはエクスポートする目的のアクションを選択します。

ステップ 4 [ポータルの動作とフロー設定（Portal Behavior and Flow Settings）] タブをクリックします。

ステップ 5 [ポータル設定（Portal Settings）] を展開します。ポート、証明書グループタグ、エンドポイント ID グループなどのデフォルト値を更新し、ポータル全体に適用する動作を定義します。

ステップ 6 [従業員のモバイルデバイス管理設定（Employee Mobile Device Management Settings）] を展開します。サードパーティの MDM プロバイダーを設定するために提供されているリンクにアクセスし、MDM ポータルを使用して従業員の受信ポリシーによる動作を定義します。

ステップ 7 [サポート情報ページの設定（Support Information Page Settings）] を展開します。ネットワークアクセスの問題のトラブルシューティングのためにヘルプデスクが使用する情報を従業員が提供するのに役立つように、ここで必要な情報を更新します。

ステップ 8 [ポータルページのカスタマイズ（Portal Page Customizations）] タブをクリックします。

ステップ 9 デバイス登録プロセス時に MDM ポータルに表示される [コンテンツ領域（Content Area）] メッセージをカスタマイズします。

- **[到達不能（Unreachable）]**：選択された MDM システムにアクセスできない場合に表示される内容を入力します。
- **[非準拠（Non-compliant）]**：登録されるデバイスが MDM システムの要件に準拠していない場合に表示される内容を入力します。
- **[続行（Continue）]**：接続に問題があるケースで、デバイスがネットワークへの接続を試行する必要がある場合に表示される内容を入力します。
- **[登録（Enroll）]**：デバイスが MDM エージェントを必要とし、かつそのデバイスを MDM システムに登録する必要がある場合に表示される内容を入力します。

ステップ 10 [保存（Save）] をクリックして、さらに [閉じる（Close）] をクリックします。

次のタスク

ポータルを使用するには、そのポータルを許可する必要があります。ポータルを使用できるように許可する前または後に、ポータルをカスタマイズすることもできます。また、次のトピックを参照してください。

- デバイス ポータルへの証明書の追加 （14 ページ）
- エンドポイント ID グループの作成 （16 ページ）
- 許可プロファイルの作成 （28 ページ）
- デバイス ポータルのカスタマイズ （30 ページ）

デバイス ポータルの作成

デバイス ポータルを提供して、従業員が、ネイティブ サプリカントをサポートせず、個人所有デバイスの持ち込み（BYOD）を使用して追加できないパーソナルデバイスを追加および登録できるようにすることができます。デバイス ポータルを使用して、いずれかのポータルを使用して追加されたすべてのデバイスを管理できます。

新しいデバイス ポータルを作成するか、既存のものを編集または複製できます。Cisco ISE によって提供されているデフォルトのポータルを含むすべてのデバイス ポータルを削除できます。

[ポータルの動作とフローの設定（Portal Behavior and Flow Settings）] タブのしたにある [ポータルとページの設定（Portal & Page Settings）] に加えた変更は、デバイスポータルフロー図のグラフィカル フローに反映されます。[サポート情報（Support Information）] ウィンドウなどのウィンドウを有効にすると、そのウィンドウがフローに表示され、従業員はポータルで使用できるようになります。ウィンドウを無効にすると、フローから削除されます。

始める前に

このポータルで使用するために、必要な証明書、外部 ID ストア、ID ソース順序、およびエンドポイント ID グループが設定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（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **[デバイス（My Devices）]** > **[作成（Create）]** を選択します。

ステップ 2 ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。

ここで使用するポータル名が他のエンドユーザーポータルに使用されていないことを確認します。

ステップ 3 [言語ファイル（Language File）] ドロップダウンリストから、ポータルで使用する言語ファイルをインポートまたはエクスポートする目的のアクションを選択します。

ステップ 4 [ポータルの動作とフロー設定（Portal Behavior and Flow Settings）] タブをクリックします。

ステップ 5 ポート、証明書グループタグ、エンドポイントIDグループなどのデフォルト値を更新して、ポータル全体に適用する動作を定義するには、[ポータルの設定（Portal Settings）] を展開します。

ステップ 6 従業員のログイン情報およびログインガイドラインを指定するには、[ログインページの設定（Login Page Settings）] を展開します。

ステップ 7 別の AUP ページを追加し、従業員のアクセプタブル ユース ポリシーの動作を定義するには、[アクセプタブルユースポリシー（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）] を展開します。

ステップ 8 ポータルへのログイン後に、従業員に追加情報を通知するには、[ポストログインバナーページの設定（Post-Login Banner Page Settings）] を展開します。

ステップ 9 従業員の自身のパスワードの変更を許可するには、[従業員のパスワード変更の設定（Employee Change Password Settings）] を展開します。このオプションは、従業員が内部ユーザーデータベースの一部である場合にのみ有効になります。

ステップ 10 [ポータル ページのカスタマイズ（Portal Page Customization）] タブで、登録および管理時にデバイス ポータルに表示される次の情報をカスタマイズします。

- タイトル、コンテンツ、フィールド、およびボタン ラベル
- **エラーメッセージ**および**通知メッセージ**

ステップ 11 [保存（Save）] をクリックして、さらに [閉じる（Close）] をクリックします。

次のタスク

ポータルの外観を変更する場合は、ポータルをカスタマイズできます。

関連トピック

デバイス ポータルのカスタマイズ （30 ページ）
デバイス ポータル （6 ページ）
従業員が追加したデバイスの表示 （30 ページ）

許可プロファイルの作成

ポータルを許可するときは、ネットワーク アクセス用のネットワーク許可プロファイルおよびルールを設定します。

始める前に

ポータルを許可する前にポータルを作成する必要があります。

ステップ 1 ポータルの特別な許可プロファイルを設定します。
ステップ 2 プロファイルの許可ポリシー ルールを作成します。

許可プロファイルの作成

各ポータルには、特別な許可プロファイルを設定する必要があります。

始める前に

デフォルトのポータルを使用しない場合は、許可プロファイルとポータル名を関連付けることができるように、最初にポータルを作成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（☰）をクリックして次を選択します。**[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）]** を選択します。
ステップ 2 使用を許可するポータル名を使用して許可プロファイルを作成します。

次のタスク

新しく作成される許可プロファイルを使用するポータル許可ポリシー ルールを作成する必要があります。

許可ポリシー ルールの作成

ユーザー（ゲスト、スポンサー、従業員）のアクセス要求への応答に使用するポータルのリダイレクション URL を設定するには、そのポータル用の許可ポリシー ルールを定義します。

url-redirect は、ポータル タイプに基づいて次の形式になります。

ip:port ：IP アドレスとポート番号

PortalID：一意のポータル名

ホットスポット ゲスト ポータル：
https://*ip:port*/guestportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=cwa&type=drw

モバイル デバイス管理（MDM）ポータル：
https://*ip:port*/mdmportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=mdm

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]**> **[ポリシーセット（Policy Sets）]** を選択して、[標準（Standard）] ポリシーで新しい認証ポリシールールを作成します。

ステップ 2 [条件（Conditions）] には、ポータルの検証に使用するエンドポイント ID グループを選択します。たとえば、ホットスポット ゲスト ポータルの場合は、デフォルトの [GuestEndpoints] エンドポイント ID グループを選択し、MDM、ポータルの場合は、デフォルトの [RegisteredDevices] エンドポイント ID グループを選択します。

（注） Reauthenticate および Terminate CoA タイプは、ホットスポット ゲスト ポータルでサポートされています。ホットスポット ゲスト ポータルで Reauthentication CoA タイプが選択されている場合のみ、ホットスポットゲスト認証ポリシーの検証条件の 1 つとして [ネットワークアクセス：ユースケースEQUALSゲストフロー（Network Access:UseCase EQUALS Guest Flow）] を使用できます。

ステップ 3 [権限（Permissions）] には、作成したポータル許可プロファイルを選択します。

（注） RADIUS.Calling-Station-ID など、MAC オプションが有効になっているディクショナリ属性を使用して許可条件を作成する場合は、さまざまな MAC 形式をサポートするために Mac 演算子（Mac_equals など）を使用する必要があります。

デバイス ポータルのカスタマイズ

ポータルの外観およびユーザー（必要に応じてゲスト、スポンサー、または従業員）エクスペリエンスをカスタマイズするには、ポータルテーマをカスタマイズし、ポータルページの UI 要素を変更して、ユーザーに表示されるエラーメッセージと通知を編集します。ポータルのカスタマイズの詳細については、 エンドユーザー Web ポータルのカスタマイズを参照してください。

従業員が追加するパーソナル デバイスの管理

従業員が Bring Your Own Device（BYOD; 個人所有デバイス持ち込み）またはデバイスポータルを使用してデバイスを登録すると、登録済みデバイスは[エンドポイント（Endpoints）]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を切り離すことができますが、デバイスは Cisco ISE データベースに残ります。この結果、従業員は、デバイスの使用時に発生するエラーの解決に管理者の支援を必要とする場合があります。

従業員が追加したデバイスの表示

[エンドポイント（Endpoints）] リストページに表示される [ポータルユーザー（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特定できます。これは、特定のユーザーが登録したデバイスを削除する必要がある場合に役立つことがあります。デフォルトでは、このフィールドは表示されないため、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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[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）]** を選択します。

ステップ 2 エンドポイントリストの右上隅でダッシュレットの下にある [設定（Settings）] アイコンをクリックします。

ステップ 3 [ポータルユーザー（Portal User）] チェックボックスをオンにして、[ポータルユーザー（Portal User）] トグルボタンを有効にして、エンドポイントリストにこの情報を表示します。

ステップ 4 [実行（Go）] をクリックします。

ステップ 5 [フィルタ（Filter）] 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 6 [ポータル ユーザー（Portal User）] フィールドにユーザーの名前を入力して、その特定のユーザーに割り当てられたエンドポイントのみを表示します。

デバイスをデバイス ポータルに追加するときのエラー

従業員は、別の従業員がすでに追加したサービスを追加することはできません。デバイスは引き続きエンドポイント データベースに含まれます。

Cisco ISE データベースにすでに存在しているデバイスを従業員が追加しようとした場合：

- デバイスがネイティブサプリカントのプロビジョニングをサポートしている場合は、BYOD ポータルからデバイスを追加することを推奨します。この場合、デバイスがネットワークに最初に追加されたときに作成された登録詳細がすべて上書きされます。
- デバイスがプリンタなどのMAC認証バイパス（MAB）デバイスである場合は、デバイスの所有権を最初に解決する必要があります。必要に応じて、管理者のポータルを使用してエンドポイントデータベースからデバイスを削除できます。これにより、新しい所有者は、マイデバイスポータルを使用して正常にデバイスを追加できます。

（注） 管理者ポータルがダウンしている場合、デバイス ポータルは使用できません。

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（My Devices）] ポータルからデバイスを削除すると、そのデバイスは従業員の登録済みデバイスのリストから削除されますが、Cisco ISE エンドポイントデータベースには残っており、[エンドポイント（Endpoints）] のリストに表示されます。

[エンドポイント（Endpoints）] ウィンドウからデバイスを完全に削除できます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[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）]** です。

従業員が登録するパーソナル デバイス数の制限

従業員が 1 ～ 999 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。従業員がパーソナルデバイスの登録に使用したポータルに関係なく、この設定では、すべてのポータルにわたって登録されるデバイスの最大数を定義します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [設定（Settings）] > [従業員が登録するデバイス（Employee Registered Devices）]** を選択します。

ステップ 2 [従業員を制限（Restrict employees to）] に、従業員が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** 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。設定の更新を保存しない場合は、[リセット（Reset）] をクリックして、最後に保存した値に戻します。

デバイスポータルおよびエンドポイントアクティビティのモニター

Cisco ISE は、エンドポイントおよびユーザー管理情報、およびゲストとスポンサーのアクティビティを参照できるさまざまなレポートとログを提供します。

オン デマンドまたはスケジュール ベースでこれらのレポートを実行できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]** > **[レポート（Reports）]** > **[レポート（Reports）]**。

ステップ 2 [ゲスト（Guest）] または [エンドポイントとユーザー（Endpoints and Users）] を選択して、さまざまなゲスト、スポンサー、およびエンドポイント関連のレポートを表示します。

ステップ 3 [フィルタ（Filters）] ドロップダウンリストを使用して検索するデータを選択します。

ステップ 4 データを表示する [時間範囲（Time Range）] を選択します。

ステップ 5 [実行（Run）] をクリックします。

デバイス ログインおよび監査レポート

[デバイスログインと監査（My Devices Login and Audit）] レポートは、次を追跡する統合レポートです。

- [デバイス（My Devices）] ポータルでの従業員によるログイン アクティビティ。
- [デバイス（My Devices）] ポータルで従業員が実行したデバイス関連の操作。

このレポートは、**[操作（Operations）]** > **[レポート（Reports）]** > **[レポート（Reports）]** > **[ゲスト（Guest）]** > **[デバイスログインと監査（My Devices Login and Audit）]** で使用できます。

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（Registered Endpoints）] のレポートには、従業員によって登録されたすべてのエンドポイントに関する情報が表示されます。このレポートは、**[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）]** > **[登録済みエンドポイント（Registered Endpoints）]** で使用できます。[ID（Identity）]、[エンドポイント ID（Endpoint ID）]、[ID グループ（Identity Group）]、[エンドポイントプロファイル（Endpoint Profile）] などの属性でフィルタ処理してレポートを生成できます。

[登録済みデバイス（Registered Devices）] エンドポイント ID グループに割り当てられているエンドポイントについて、エンドポイントデータベースに照会できます。また、[ポータルユー

ザー（Portal User）] 属性がヌル以外の値に設定されている特定のユーザーについては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（Registered Endpoints）] のレポートには、特定のユーザー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。

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。