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（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。

ISE コミュニティ リソース

How To: ISE and BYOD - Onboarding, Registering, and Provisioning

How To: ISE and BYOD - Using Certificates for Differentiated Access

分散環境のエンドユーザのデバイス ポータル

Cisco ISE のエンドユーザ 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。

- **管理ノード**：ユーザ、デバイス、およびエンドユーザ ポータルが管理ノードに書き込まれる構成の変更。
- **ポリシー サービス ノード**：エンドユーザ ポータルはポリシー サービス ノード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。ポリシー サービス ノードがノード 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**：モニタリング 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 モニタリング ノードで障害が発生した場合は、セカンダリ モニタリング ノードが自動的にプライマリ モニタリング ノードになります。

デバイス ポータルのグローバル設定

[ワーク センター（Work Centers）] > [BYOD] > [設定（Settings）] > [従業員が登録するデバイス（Employee Registered Devices）] または **[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。

- [従業員が登録するデバイス（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。

関連トピック

従業員が登録するパーソナル デバイス数の制限 （10 ページ）
BYOD 登録に再接続する URL の提供 （11 ページ）
分散環境のエンドユーザのデバイス ポータル （2 ページ）

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 フローまたはスポンサー ポータル フローには関与しません。

次のポータルを使用します。

- **ブラックリスト ポータル**：「ブラックリスト」に掲載されているためネットワーク 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を提供します。
- **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**：管理者および従業員が BYOD フローを通過できないデバイスについてユーザ/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、管理者ポータルからカスタマイズできる標準のシスコ ブランド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

ステップ 1 デバイス ポータルへのアクセスには、次のいずれかを実行します。

- **[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** をクリックします。[デバイス ポータルの設定およびカスタマイズ（Configure and Customize Device Portals）] ページには、サポートされるデバイス ポータルのリストが表示されます。
- **[管理（Administration）]** > **[デバイス ポータル管理（Device Portal Management）]** を選択します。ドロップダウン メニューにサポートされるデバイス ポータルが表示されます。

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。

ブラックリスト 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 ポータルでデバイスのステータスを更新して、ブラックリスト 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、ブラックリスト ポータルにリダイレクトされ、デバイスがネットワークへのアクセスを拒否す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 ポータルで使用されていないことを確認してください。

ブラックリスト ポータルの設定については、ブラックリスト ポータルの編集 （16 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

Identity Services Engine 証明書プロビジョニング ポータルの機能と設定については、「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。

（注） BYOD フローは、デバイスが AnyConnect 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。

関連トピック

BYOD ポータルの作成 （19 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 （22 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 サーバを 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（24 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、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 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 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 **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）] ページに追加します（別のエンドポイント ID グループに、すで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 アドレスがユーザによりデバイス ポータルに入力されると、それらが同じホスト名を持ち、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、デバイス登録状態属性と BYOD 登録状態属性は、それぞれ [未登録（NotRegistered）] および [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）] ページ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。

関連トピック

デバイス ポータルの作成 （26 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、証明書の登録、プロビジョニング、およびネットワーク アクセスに同じ WLAN が使用されます。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。

従業員がネットワークに接続する

1. **従業員のクレデンシャルが認証される**：Cisco ISE は、社内 Active Directory または社内の他の ID ストアと照合して従業員を認証し、許可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る**：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）] フィールドは自動的に事前設定されます。ユーザはデバイス名と説明を追加できます。
3. **ネイティブ サプリカントが設定される（MacOS、Windows、iOS、Android）**：ネイティブ サプリカントが設定されます。ただしこのプロセスはデバイスに応じて異なります。
   - MacOS および Windows デバイス：従業員が BYOD ポータルで [登録（Register）] 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（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名が発行済み証明書に組み込まれます。

     （注） Network Setup Assistant は、そのデバイスのユーザ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、GPO を使用して証明書をユーザのデバイスにプッシュします。

     （注） バージョン OSx 10.15 以降では、ユーザはサプリカント 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。ユーザのデバイスに、Cisco ISE サーバ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。

   - iOS デバイス：Cisco ISE ポリシー サーバは 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。

- Android デバイス：Cisco ISE は、従業員に Google Play ストアから Cisco 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. **認可変更が発行される**：ユーザがオンボーディング フローを通過すると、Cisco ISE は認可変更（CoA）を開始します。これにより、MacOS X、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。

（注） サプリカントを使用しない BYOD フローを設定できます。Cisco ISE コミュニティの資料（https://supportforums.cisco.com/blog/12705471/ise-byod-registration-only-without-native-supplicant-or-certificate-provisioning）を参照してください。

（注） [ターゲットネットワークが非表示になっている場合に有効にする（Enable if Target Network is Hidden）] チェック ボックスをオンにするのは、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/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。

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*：デバイスが BYOD フローを通過していません。
- *Yes*：デバイスは BYOD フローを通過し、登録されました。
- *No*：デバイスが BYOD フローを通過しましたが、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 フローを通過し、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フローを通過し、登録されました。ただし、ISEはネットワーク上でこのデバイスを認識していません。
- *Not Registered*：デバイスがBYODフローを通過していません。これは、この属性のデフォルト状態です。
- *Stolen*：ユーザがデバイス 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。この状況が発生した場合は次のような処理が行われます。
  - 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、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 **ブラックリスト**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、ISE はそのデバイスを **ブラックリスト** 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許可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、**IF Endpoint Identity Group is Blacklist AND BYOD_is_Registered THEN 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）を行います。

  ユーザ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*：ユーザがデバイス 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 としてマークしました。これにより、次のアクションが実行されます。
  - そのデバイスは **ブラックリスト** 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」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 **ブラックリスト** ID グループまたは *endpoint:BYODRegistration* 属性を使用できます。たとえば、**IF Endpoint Identity Group is Blacklist AND EndPoints:BYODRegistrations Equals No THEN BYOD** と指定できます。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 **[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。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）
- 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、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 **[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 [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] タブおよび [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）] をオンにします。

ステップ 4 [保存（Save）] をクリックし、[閉じる（Close）] 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 **[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 IP アドレスを変更するか、またはデバイスを 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。

登録プロセス中に従業員の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、ここに入力する IP アドレスまたはドメイン名がデバイスを Cisco ISE にリダイレクトし、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 1.1.1.1 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	ブラックリスト 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 （13 ページ）	必須（Required）	必須（Required）	必須（Required）	必須（Required）	必須（Required）
デバイス ポータルへの証明書の追加 （14 ページ）	必須（Required）	必須（Required）	必須（Required）	必須（Required）	必須（Required）
外部 ID ソースの作成 （14 ページ）	不要	不要	不要	不要	必須（Required）
ID ソース順序の作成 （15 ページ）	不要	不要	不要	不要	必須（Required）
エンドポイント ID グループの作成 （16 ページ）	不要	必須（Required）	不要	必須（Required）	必須（Required）

タスク	ブラックリスト 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
ブラックリスト ポータルの編集（16 ページ）	必須（Required）	N/A	N/A	N/A	N/A
BYOD ポータルの作成（19 ページ）	N/A	必須（Required）	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（22 ページ）	N/A	N/A	必須（Required）	N/A	N/A
MDM ポータルの作成（24 ページ）	N/A	N/A	N/A	必須（Required）	N/A
デバイス ポータルの作成（26 ページ）	N/A	N/A	N/A	N/A	必須（Required）
許可プロファイルの作成（27 ページ）	N/A	必須（Required）	必須（Required）	必須（Required）	不要
デバイス ポータルのカスタマイズ（28 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 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 **[管理（Administration）]** > **[システム（System）]** > **[展開（Deployment）]** を選択します。
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）] をオンにします。
ステップ 4 [セッション サービスの有効化（Enable Session Services）] オプションをオンにします。

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 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。

（注） BYOD は、3 つ以上の証明書チェーンをサポートしていません。

ステップ 1 **[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 **[管理（Administration）] > [デバイス ポータル管理（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。

外部 ID ソースの作成

Cisco ISE では、Active Directory、LDAP、RADIUS トークン、RSA SecurID サーバなどの外部 ID ソースに接続して、認証/許可のユーザ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 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、を参照してくださいその他の パッシブ ID サービス プロバイダー。

ステップ 1 **[管理（Administration）] > [ID の管理（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 ソースである Active Directory に接続する場合。 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 プロバイダを参照してください。
- **ソーシャル ログイン**：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。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 **[管理（Administration）] > [ID の管理（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 ボックスの 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）] リストのデータベースを並べ替えます。

ステップ 6 [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）]：最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が検索を中止する場合。
- [ユーザ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）]：最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が順序内の他の選択された ID ソースの検索を続行する場合。

  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）] ページで追加のエンドポイント ID グループを作成することもできます。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したり、これらのグループを削除したりすることはできません。

ステップ 1 **[管理（Administration）] > [ID の管理（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 グループの名前を入力します（エンドポイント ID グループの名前に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 グループの説明を入力します。

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。

ブラックリスト ポータルの編集

Cisco ISE では、Cisco ISE でブラ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ラックリスト 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。新しいブラ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 **[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [ブラックリスト ポータル（Blacklist 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 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 ポータルで使用する言語ファイルをエクスポートおよびインポートするには、[言語（Languages）] メニューを使用します。

ステップ 4 [ポータルの設定（Portal Settings）] で証明書グループ タグ、言語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、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合は、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（マイ デバイスなど）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**、およびブラックリスト 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**、およびブラックリスト 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**

- [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とサブジェクトの代替名はインターフェイス IP 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 IP 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と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：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスを設定しようとします。これが成功しない場合、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、高可用性（耐障害性）のために 2 つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
  - 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンドセットアップがなかったことが原因である可能性があるので、PSN は物理インターフェイスでポータルを開始しようとします。

- [証明書グループ タグ（Certificate group tag）]：ポータルの HTTPS トラフィックに使用する証明書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 ロケールの言語が ISE でサポートされていない場合は、フォールバック言語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 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、ユーザのブラウザのロケール オプションを上書きします。

[スポンサーに使用可能な SSID（SSIDs available to sponsors）]：ゲストの訪問にあたり、スポンサーが正しい接続先ネットワークとしてゲストに通知できる、ネットワークの名前または SSID（セッション サービス識別子）を入力します。

ステップ 5 [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パ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 6 [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

個人所有デバイスの持ち込み（BYOD）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設定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。

[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] タブのページ設定に加えた変更は、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）] ページなどのページを有効にすると、そのページ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。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 **[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [BYOD ポータル（BYOD Portals）] > [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 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 メニューを使用して、ポータルで使用する言語ファイルをエクスポートおよびインポートします。

ステップ 4 [ポータルの設定（Portal Settings）] でポート、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 5 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、[サポート情報ページの設定（Support Information Page Settings）] を更新します。

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、プロビジョニング プロセス時に次のページに表示される [コンテンツ領域（Content Area）] メッセージ テキストをカスタマイズします。

- [BYOD ウェルカム（BYOD Welcome）] ページ：
  - [デバイス設定が必要（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。

- [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。

- [BYOD デバイス情報（BYOD Device Information）] ページ：
  - [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。
  - [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。

- [BYOD インストール（BYOD Installation）] ページ：
  - [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。
  - [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。
  - [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。

- [BYOD 成功（BYOD Success）] ページ：
  - [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。
  - [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。
  - [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。

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。

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：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：自分自身にのみ証明書を生成できます。

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（ネットワーク アクセス ユーザ）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 ユーザを作成し、それからユーザ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 ユーザは、このポータルにアクセスできます。

証明書プロビジョニング ポータルにアクセスするための管理者アカウントを作成するには、次の手順を実行します。

1. 内部ユーザを追加します（[管理（Administration）] > [IDの管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）] > [追加（Add）]）。
2. ユーザをスーパー管理グループまたは ERS 管理グループに追加します（[管理（Administration）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理ユーザ（Admin Users）] > [追加（Add）] > [既存のネットワークアクセスユーザから選択（Select from existing network access user）]）。これでユーザが内部ネットワーク アクセス ユーザとスーパー管理ユーザまたは ERS 管理ユーザの両方になりました。

他のユーザ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するには、証明書プロビジョニング ポータルの設定を行います（[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ポータル（Certificate Provisioning Portal）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [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 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ポータル（Certificate Provisioning Portal）] > [作成（Create）]** の順に選択します。

ここで使用するポータル名が他のエンドユーザ 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）] メニューを使用して、ポータルで使用する言語ファイルをエクスポートおよびインポートします。

ステップ 4 [ポータルの設定（Portal Settings）] で証明書グループ タグ、言語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 5 [ポータルページのカスタマイズ（Portal Page Customization）] タブで、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 6 [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 コンプライアンスを確認する Cisco AnyConnect ポスチャ コンポーネントまたは を従業員がダウンロードできるようにすることができます。

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（ネットワーク アクセス ユーザ）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 ユーザを作成し、それからユーザ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 ユーザは、このポータルにアクセスできます。

クライアント プロビジョニング ポータルにアクセスするための管理者アカウントを作成するには、次の手順を実行します。

1. 内部ユーザを追加します（[管理（Administration）] > [IDの管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）] > [追加（Add）]）。
2. ユーザをスーパー管理グループまたは ERS 管理グループに追加します（[管理（Administration）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理ユーザ（Admin Users）] > [追加（Add）] > [既存のネットワークアクセスユーザから選択（Select from existing network access user）]）。これでユーザが内部ネットワーク アクセス ユーザとスーパー管理ユーザまたは ERS 管理ユーザの両方になりました。

他のユーザ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するには、クライアント プロビジョニング ポータルの設定を行います（[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）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [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 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が、ポータルにアクセスできるようになります。

[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] タブのページ設定に加えた変更は、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）] ページなどのページを有効にすると、そのページ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。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 **[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [クライアント プロビジョニング ポータル（Client Provisioning Portals）] > [作成、編集または複製（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 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 メニューを使用して、ポータルで使用する言語ファイルをエクスポートおよびインポートします。

ステップ 4 [ポータルの設定（Portal Settings）] でポート、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 5 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、[サポート情報ページの設定（Support Information Page Settings）] を更新します。

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、プロビジョニング プロセス時にクライアント プロビジョニング ポータルに表示される [コンテンツ領域（Content Area）] メッセージ テキストをカスタマイズします。

a) [クライアント プロビジョニング（Client Provisioning）] ページ：

- [確認、スキャン、および準拠（Checking, Scanning and 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。
- [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。

b) [クライアント プロビジョニング（エージェントが見つかりませんでいた）（Client Provisioning (Agent Not Found)）] ページ：

- [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。
- [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の、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。

- [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の、手動で Java プラグインをダウンロードし、インストールする方法の手順。
- [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の、ポスチャ エージェントを開始する方法の手順。これにより、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る。

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。

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 （28 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。

[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] タブのページ設定に加えた変更は、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）] ページなどのページを有効にすると、そのページ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。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 **[管理（Administration）]** > **[デバイス ポータル管理（Device Portal Management）]** > **[MDM ポータル（MDM Portals）]** > **[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 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 メニューを使用して、ポータルで使用する言語ファイルをエクスポートおよびインポートします。

ステップ 4 [ポータルの設定（Portal Settings）] でポート、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 5 特定のページのそれぞれに適用される次の設定を更新してください。

- [従業員のモバイル デバイス管理の設定（Employee Mobile Device Management Settings）] では、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。
- 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 デスクによって使用される情報をゲストが提供するのに役立つように、[サポート情報ページの設定（Support Information Page Settings）] を更新します。

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、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。
- [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。
- [続行（Continue）]：接続に問題がある場合に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。
- [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。

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。

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 （27 ページ）
- デバイス ポータルのカスタマイズ （28 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。

[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] タブのページ設定に加えた変更は、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）] ページなどのページを有効にすると、そのページ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。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 **[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [デバイス ポータル（My Devices Portals）] > [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 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 メニューを使用して、ポータルで使用する言語ファイルをエクスポートおよびインポートします。

ステップ 4 [ポータルの設定（Portal Settings）] でポート、証明書グループ タグ、ID ソース順序、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 5 特定のページのそれぞれに適用される次の設定を更新してください。

- [ログイン ページの設定（Login Page Settings）]：従業員クレデンシャルおよびログイン ガイドラインを指定します。
- [利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）]：別の AUP ページを追加し、従業員の利用規定の動作を定義します。
- [ポストログイン バナーページの設定（Post-Login Banner Page Settings）]：ポータルへのログイン後に、従業員に追加情報を通知します。
- [従業員のパスワード変更の設定（Employee Change Password Settings）]：従業員の自身のパスワードの変更を許可します。このオプションは、従業員が内部ユーザ 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 6 [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 7 [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

次のタスク

ポートルの外観を変更する場合は、ポートルをカスタマイズできます。参照先

関連トピック

デバイス ポータルのカスタマイズ （28 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 （29 ページ）

許可プロファイルの作成

ポート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

ポートルを許可する前にポートルを作成する必要があります。

ステップ 1 ポート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

各ポートルには、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

デフォルトのポートルを使用しない場合は、許可プロファイルとポートル名を関連付けることができるように、最初にポートルを作成する必要があります。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [許可プロファイル（Authorization Profiles）]** を選択します。
ステップ 2 使用を許可するポート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（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 **[ポリシー（Policy）]** > **[ポリシー セット（Policy Sets）]** を選択して、[標準（Standard）] ポリシーで新しい許可ポリシー 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） ホットスポット ゲスト ポータルは、Termination CoA だけを発行するため、ゲスト許可ポリシーの検証条件の 1 つとして [Network Access:UseCase EQUALS Guest Flow] を使用しないでください。代わりに、エンドポイントが属する ID グループに照合して検証を行います。次の例を参考にしてください。

- "GuestEndpoint" + Wireless MAB の場合は Permit Access
- Wireless MAB の場合は HotSpot Redirect

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。

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（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 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

従業員が個人所有デバイスの持ち込み（BYOD）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、デバイスはエンドポイント 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（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 **[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 [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（Endpoints）] リストに情報を表示します。

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 [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て、その特定のユーザ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：

- さらに、デバイスがネイティブ サプリカント プロビジョニングをサポートしている場合、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、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、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 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 データベースに残っており、エンドポイント リストに表示されます。

[エンドポイント（Endpoints）] ページからデバイスを完全に削除するには、**[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。

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 **[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

Cisco ISE は、エンドポイントおよびユーザ管理情報、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。Cisco ISE 1.2 レポートの一部は廃止されましたが、情報は他のレポートで表示できます。

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 **[操作（Operations）]** > **[レポート（Reports）]** を選択します。

ステップ 2 レポート セレクタで、[ゲスト アクセス レポート（Guest Access Reports）] および [エンドポイントとユーザ（Endpoints and Users）] 選択を展開し、さまざまなゲスト、スポンサー、およびエンドポイントに関するレポートを表示します。

ステップ 3 レポートを選択し、[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。

ユーザ名、ポータル名、デバイス名、エンドポイント ID グループ、および他のデータについてフィルタを使用できます。

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 ログインおよび監査レポートは、次のものを追跡する統合レポートです。

- デバイス 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 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）] > [ゲスト アクセス レポート（Guest Access Reports）] > [デバイス ログインおよび監査レポート（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 レポート（Registered Endpoints report）] 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）] > [エンドポイントとユーザ（Endpoints and Users）] > [登録済みエンドポイント（Registered Endpoints）]** で使用できます。ID、エンドポイント ID、アイデンティティ プロファイルなどに対してクエリーを実行し、レポートを生成できます。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の詳細については、クライアント プロビジョニング レポートの表示に関する説明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、[ポータル ユーザ（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。