



# ゲスト アクセスのユーザ インターフェイスのリファレンス

- [ゲスト ポータル設定 \(1 ページ\)](#)
- [スポンサー ポータル アプリケーションの設定 \(24 ページ\)](#)
- [グローバル設定 \(33 ページ\)](#)

## ゲスト ポータル設定

### ポータル ID 設定

これらの設定へのナビゲーションパスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータルまたはスポンサー ポータル (Guest Portals or Sponsor Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ゲスト ポータルおよびスポンサー ポータルの設定とカスタマイズ (Guest Portals or Sponsor Portals Settings and Customization)] です。

- **ポータル名 (Portal Name)** : このポータルにアクセスするための一意のポータル名を入力します。このポータル名を、その他のスポンサー、ゲスト、または非ゲストポータル (ブラックリスト、個人所有デバイス持ち込み (BYOD)、クライアントプロビジョニング、モバイルデバイス管理 (MDM)、またはデバイスの各ポータル) に使用しないでください。

この名前は、リダイレクションを選択するために、認証プロファイルポータルの選択に表示されます。これはポータルのリストに適用され、他のポータルとの間で簡単に識別できます。

- **説明 (Description)** : 任意項目です。
- **ポータルテスト URL (Portal test URL)** : [保存 (Save)] をクリックした後にリンクとして表示されるシステムにより生成された URL。ポータルをテストするために使用します。  
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。

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、ISEは最初のアクティブPSNを選択します。

- 言語ファイル (Language File) : 各ポータルタイプは、デフォルトで15種類の言語をサポートします。これらの言語は、個々のプロパティファイルとして使用できます。これらのファイルは、圧縮された単一の言語ファイル内にまとめてバンドルされています。ポータルで使用する圧縮言語ファイルをエクスポートまたはインポートします。圧縮言語ファイルには、ポータルのテキストを表示するために使用可能な個別の言語ファイルがすべて含まれています。

言語ファイルには、その言語のポータル全体のすべての文字列設定に加え、特定のブラウザのロケール設定 (例: フランス語の場合は `fr`、`fr-fr`、`fr-ca`) へのマッピングが含まれています。1つの言語ファイルには、翻訳およびローカリゼーションの目的に容易に使用できるように、サポートされるすべての言語が含まれています。

1つの言語用のブラウザロケール設定を変更した場合、変更内容は他のすべてのエンドユーザ Web ポータルに適用されます。たとえば、ホットスポット ゲスト ポータルの `French.properties` ブラウザロケールを `fr,fr-fr,fr-ca` から `fr,fr-fr` に変更すると、この変更内容がデバイスポータルにも適用されます。

[ポータルページのカスタマイズ (Portal Page Customizations) ] タブでいずれかのテキストをカスタマイズすると、警告アイコンが表示されます。警告メッセージは、ポータルのカスタマイズ時に1つの言語で行った変更をすべてのサポート対象の言語プロパティファイルにも追加する必要があることを通知します。ドロップダウンリストのオプションを使用して、手動で警告アイコンが表示されないようにします。また、警告アイコンは、更新された圧縮言語ファイルのインポート後に自動的に表示されなくなります。

## ホットスポット ゲスト ポータルのポータル設定

このページへのナビゲーションパスは、[ワークセンター (Work Centers) ] > [ゲストアクセス (Guest Access) ] > [ポータルとコンポーネント (Portals & Components) ] > [ゲストポータル (Guest Portals) ] > [作成、編集または複製 (Create, Edit or Duplicate) ] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings) ] > [ポータル設定 (Portal Settings) ] です。

- [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**



(注) 最適なパフォーマンスを得るには、ゲスト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、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ています。これが成功しない場合、おそらく、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、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ています。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ため、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ています。
- [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。
- エンドポイント ID グループ (Endpoint identity group)：ゲストのデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **GuestEndpoints** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、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。

従業員のデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **RegisteredDevices** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、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。

- \_\_日に達した場合にこの ID グループ内のエンドポイントを消去する (Purge endpoints in this identity group when they reach \_\_ days) : Cisco ISE データベースから消去されるまでの、ユーザのデバイスの登録からの日数を変更します。消去は毎日実行され、消去アクティビティは全体的な消去タイミングと同期されます。変更は、このエンドポイント ID グループ全体に適用されます。

その他のポリシー条件に基づいてエンドポイント消去ポリシーに変更が加えられた場合、この設定は使用できなくなります。

#### • 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。

## ホットスポット ゲスト ポータルの利用規定 (AUP) ページ設定

このページへのナビゲーションパスは、[ワークセンター (Work Centers) ]>[ゲスト アクセス (Guest Access) ]>[ポータルとコンポーネント (Portals & Components) ]>[ゲスト ポータル (Guest Portals) ]>[作成、編集または複製 (Create, Edit or Duplicate) ]>[ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings) ]>[利用規定 (AUP) ページ設定 (Acceptable Use Policy (AUP) Page Settings) ]です。

- [AUP ページを含める (Include an AUP page) ] : 会社のネットワーク使用諸条件を、別のページでユーザに表示します。
- [アクセスコードが必要 (Require an access code) ] : 複数のゲストがネットワークへのアクセスを獲得するために使用する必要があるログインクレデンシャルとして、アクセスコードを割り当てます。アクセスコードは、物理的に存在するゲストに対して指定される、主にローカルで認識されるコードです (ホワイトボードによって視覚的に、またはロビーアンバサダーにより口頭で)。これは、ネットワークにアクセスするために部外者に認知されることも使用されることもありません。

個別のゲストにログイン クレデンシャルとして提供されるユーザ名とパスワードに加えて、このオプションを使用できます。

- AUPの最後までスクロールが必要 (Require scrolling to end of AUP) : ユーザが AUP を完全に読んだことを確認します。[同意 (Accept) ] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。AUP がユーザに表示された場合に設定します。

ホットスポット ゲストポータルのフローを設定する場合、AUP アクセス コードはエンドポイント ID グループのデバイス登録によって異なります。つまり、[AUPの最後の受け入れとネットワークアクセス : EQUALSゲストフローの使用例 (AUP Last Acceptance and Network Access: Use Case EQUALS Guest Flow) ] フラグを使用することはできません。ユーザのセッションが接続時に NAD から削除されると、AUP ページが表示されますが、AUP アクセス コードを入力する必要はありません。

AUP アクセス コード ページは、MAC アドレスがホットスポット ポータルの設定に関連付けられたエンドポイント ID グループから削除された後のみ表示されます。エンドポイントは、Cisco ISE の [コンテキストの可視性 (Context Visibility) ] ページを介してデータベースから手動で削除するか、エンドポイント消去機能を使用し、エンドポイント消去ポリシーを設定して消去します。

## ホットスポット ポータルのポストアクセス バナー ページ設定

このページへのナビゲーションパスは、[ワーク センター (Work Centers) ] > [ゲスト アクセス (Guest Access) ] > [ポータルとコンポーネント (Portals & Components) ] > [ゲスト ポータル (Guest Portals) ] > [作成、編集または複製 (Create, Edit or Duplicate) ] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings) ] > [アクセス後のバナー ページ設定 (Post-Access Banner Page Settings) ] です。

この設定を使用して、ゲストにアクセスステータスおよび必要に応じてその他の追加アクションを通知します。

フィールド	使用上のガイドライン
アクセス後バナー ページを含める (Include a Post-Access Banner page)	ゲストが正常に認証された後、ネットワークアクセスを付与される前に追加情報を表示します。

## クレデンシャルを持つゲスト ポータルのポータル設定

このページへのナビゲーションパスは、[ワーク センター (Work Centers) ] > [ゲスト アクセス (Guest Access) ] > [ポータルとコンポーネント (Portals & Components) ] > [ゲスト ポータル (Guest Portals) ] > [作成、編集または複製 (Create, Edit or Duplicate) ] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings) ] > [ポータル設定 (Portal Settings) ] です。

- [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。

ポスト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**



---

(注) 最適なパフォーマンスを得るには、ゲスト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、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ています。これが成功しない場合、おそらく、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、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ています。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ため、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ています。
  - 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。
  - 認証方式（Authentication Method）IDソース順序（Identity source sequence）：ユーザ認証に使用する ID ソース順序（ISS）または ID プロバイダー（IdP）を選択します。ISS は、ユーザクレデンシャルを確認するために順番に検索される ID ストアのリストです。たとえば、内部ゲストユーザ、内部ユーザ、Active Directory、LDAP ディレクトリなどがあります。
- Cisco ISE には、スポンサーポータル Sponsor\_Portal\_Sequence 用のデフォルトのスポンサー ID ソース順序が含まれています。
- IdP を設定するには、[管理（Administration）]>[IDの管理（Identity Management）]>[外部IDソース（External Identity Sources）]>[SAML ID プロバイダー（SAML Id Providers）]の順に選択します。
- ID ソース順序を設定するには、[管理（Administration）]>[IDの管理（Identity Management）]>[IDソース順序（Identity Source Sequences）]の順に選択します。



- ゲストとしてこのポータルを使用する従業員のログイン オプションの継承元 (Employees using this portal as guests inherit login options from) : 従業員がこのポータルにログオンしたときに割り当てられるゲスト タイプを選択します。従業員のエンドポイント データは、そのゲスト タイプで属性 [エンドポイント ID グループにデバイス情報を保存する (Store device information in endpoint identity group) ] に設定されたエンドポイント ID グループに保存されます。関連付けられたゲスト タイプの他の属性は継承されません。
- 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。

## クレデンシャルを持つゲストポータルのログインページ設定

このページへのナビゲーションパスは、[ワークセンター (Work Centers) ] > [ゲストアクセス (Guest Access) ] > [ポータルとコンポーネント (Portals & Components) ] > [ゲストポータル (Guest Portals) ] > [作成、編集または複製 (Create, Edit or Duplicate) ] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings) ] > [ログインページの設定 (Login Page Settings) ] です。

- [アクセスコードが必要 (Require an access code) ] : 複数のゲストがネットワークへのアクセスを獲得するために使用する必要があるログインクレデンシャルとして、アクセスコードを割り当てます。アクセスコードは、物理的に存在するゲストに対して指定される、主にローカルで認識されるコードです (ホワイトボードによって視覚的に、またはロビーアンバサダーにより口頭で)。これは、ネットワークにアクセスするために部外者に認知されることも使用されることもありません。

個別のゲストにログインクレデンシャルとして提供されるユーザ名とパスワードに加えて、このオプションを使用できます。

- [頻度制限までの最大ログイン試行失敗数 (Maximum failed login attempts before rate limiting) ] : Cisco ISE がアカウントのスロットルを開始するまでの単一のブラウザセッションからのログイン試行失敗回数を指定します。これにより、アカウントのロックアウト

トは起きません。スロットル率は、[頻度制限時のログイン試行間隔 (Time between login attempts when rate limiting)] で設定されます。

- [頻度制限時のログイン試行間隔 (Time between login attempts when rate limiting)] : [頻度制限までの最大ログイン試行失敗数 (Maximum failed login attempts before rate limiting)] で定義された回数のログインの失敗後に、ユーザが再度ログインを試行するまでに待機する必要がある時間 (スロットル率) を分単位で設定します。
- [AUPを含める (Include an AUP)] : フローに利用規約ページを追加します。AUP をページに追加したり、別のページへのリンクを設定することができます。これを追加すると、右側のフローの画像が変わります。
  - [同意が必要 (require acceptance)] : フローを続行する前に、ユーザが AUP に同意するように強制します。
- [ゲストに自分自身のアカウントの作成を許可 (Allow guests to create their own accounts)] : このポータルの [ログイン (Login)] ページで、ゲストが自身を登録するためのオプションが提供されます。このオプションが選択されていない場合は、スポンサーがゲストアカウントを作成します。これを有効にすることで、このページのタブが有効になり、[アカウント登録ページの設定 (Self-Registration Page Settings)] および [アカウント登録成功ページの設定 (Self-Registration Success Page Settings)] を設定できます。

ゲストがこのオプションを選択した場合、自身のゲストアカウントを作成するために必要な情報を入力できるアカウント登録フォームが示されます。
- [ソーシャルログインを許可 (Allow Social Login)] : このポータルのユーザのログインクレデンシャルを取得するためにソーシャルメディアサイトを使用します。このオプションをチェックすると、次の設定が表示されます。
  - [ソーシャルログイン後に登録フォームを表示 (Show registration form after social login)] : これにより、ユーザは Facebook によって提供される情報を変更できます。
  - [ゲストの承認が必要 (Require guests to be approved)] : スポンサーがアカウントを承認する必要があることをユーザに通知し、ログイン用のクレデンシャルを送信します。
- [ゲストにログイン後のパスワード変更を許可 (Allow guests to change password after login)] : ゲストが正常に認証され、AUP に同意した後に、ゲストに必要なに応じてパスワードを変更することを許可します。ゲストが自分のパスワードを変更した場合、スポンサーはゲストにログインクレデンシャル情報を提供できません。スポンサーは、ゲストのパスワードをランダムパスワードにリセットすることだけが可能です。
- [ログインに次の ID プロバイダ ゲストポータルの使用を許可 (Allow the following identity-provider guest portal to be used for login)] : このオプションをオンにし、SAML Id ID プロバイダを選択すると、その SAML ID のリンクがこのポータルに追加されます。このサブポータルは、ユーザが証明書を提供している SAML IDP のように見えるように設定できます。

- [ソーシャルログインを許可 (Allow social login) ]: このポータルはすべて、ユーザログインにソーシャルメディアタイプを使用します。この項目を選択すると、設定したソーシャルメディアタイプをドロップダウンで選択できます。ソーシャルログインの設定の詳細については、『』の「アカウント登録ゲストのソーシャルログイン」のセクション [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。
- [ソーシャルログイン後にゲストフォームを表示 (Show guest form after social login) ]: このオプションを選択すると、ログオン画面がスキップされます。

## アカウント登録ページの設定

このページへのナビゲーションパスは、[ワークセンター (Work Centers) ]>[ゲストアクセス (Guest Access) ]>[ポータルとコンポーネント (Portal & Components) ]>[ゲストポータル (Guest Portals) ]>[作成、編集または複製 (Create, Edit or Duplicate) ]>[ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings) ]>[アカウント登録ページの設定 (Self-Registration Page Settings) ]です。これらの設定を使用して、ゲストが自身を登録し、提供する必要がある情報をアカウント登録フォームで指定できるようにします。

- [アカウント登録ゲストに割り当てるゲストタイプ (Assign self-registered guests to guest type) ]: このポータルを使用するすべてのアカウント登録ゲストに割り当てられるゲストタイプを選択します。
- [アカウントの有効期間 (Account valid for) ]: アカウントの有効期間を、日、時間、または分で指定します。この期間を超過した場合、管理者またはスポンサーがスポンサーポータルでアカウント有効期間を延長した場合を除き、アカウントは失効します。
- [アカウント登録に登録コードを必要とする (Require a registration code for self registration) ]: アカウント登録ゲストがアカウント登録フォームを正常に送信するために入力する必要があるコードを割り当てます。部外者がシステムにアクセスすることを防ぐために、アクセスコードと同様に、登録コードはオフラインで提供されます。
- [含めるフィールド (Fields to include) ]: アカウント登録ページ上で、アカウント登録フォームに表示するフィールドのチェックボックスをオンにします。その後、ゲストがこのフォームを送信してゲストアカウントを受信するために入力が必要であるフィールドのチェックボックスをオンにします。アカウント登録ゲストから重要な情報を収集するために、[SMS サービス プロバイダー (SMS Service Provider) ] および [訪問先担当者 (Person being Visited) ] フィールドを必須にすることができます。
  - [場所 (Location) ]: アカウント登録のゲストが定義済みリストを使用して登録時に選択できる場所を入力します。これにより、これらのゲストの有効なアクセス時間として自動的に関連するタイムゾーンが割り当てられます。場所の名前は、選択時に混乱を回避するために具体的なものを使用します (たとえば、ボストン オフィス、500 Park Ave New York、シンガポールなど) 。

ゲストアクセスを時間で制限する予定の場合は、その時間を設定するときにタイムゾーンを使用します。アクセス時間が制御されたゲスト全員がサンノゼのタイムゾーンにいる場合を除き、各自のロケールのタイムゾーンを作成します。場所が1つだけである場合は、その場所がデフォルトの場所として自動的に割り当てられ、ポータル

ではこのフィールドがゲストに対して表示されません。また、[場所 (Location)] は、[含むフィールド (Fields to include)] のリスト内で無効になります。

- [SMS サービス プロバイダー (SMS Service Provider)] : アカウント登録フォームに SMS プロバイダーを表示して、アカウント登録ゲストが自分の SMS プロバイダーを選択できるようにします。これで、会社の経費を最小化するために、ゲストの SMS サービスを使用して SMS 通知を送信できるようになります。ゲストが使用できる SMS プロバイダーを1つだけ選択した場合は、このフィールドはアカウント登録フォームに表示されません。
- [訪問先担当者 (Person being Visited)] : これはテキストフィールドであるため、このフィールドを使用する場合には、ゲストに対し、このフィールドに入力する情報について説明してください。
- [カスタム フィールド (Custom Fields)] : アカウント登録ゲストから追加のデータを収集するために作成したカスタムフィールドを選択します。その後、ゲストがアカウント登録フォームを送信してゲストアカウントを受信するために入力が必要であるフィールドのチェックボックスをオンにします。これらのフィールドは名前のアルファベット順に表示されます。これらのフィールドは、カスタムフィールドを追加するため、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [設定 (Settings)] > [カスタム フィールド (Custom Fields)] で作成します。
- [AUP を含む (Include an AUP)] : 会社のネットワーク使用の諸条件を、現在ユーザに表示されるページ上のテキストとして、または AUP テキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。
  - [同意が必要 (Require acceptance)] : ユーザが AUP を最後まで読んだことを確認します。これにより、アカウント登録ページの [同意する (Accept)] ボタンが設定されます。AUP を [ページ (as on page)] として設定する場合は、ユーザが AUP の終わりまでスクロールするまで [同意する (Accept)] ボタンを無効にすることもできます。
- [次の電子メールアドレスを持つゲストのみを許可 (Only allow guests with an email address from)] : アカウント登録ゲストが電子メールアドレスを作成するときに [電子メールアドレス (Email Address)] で使用できるドメイン (例 : cisco.com) の許可されたリストを指定します。

このフィールドを空白のままにすると、[次の電子メールアドレスを持つゲストを許可しない (Do not allow guests with email address from)] にリストされているドメイン以外のすべての電子メールアドレスが有効になります。
- [次の電子メールアドレスを持つゲストを許可しない (Do not allow guests with email address from)] : アカウント登録ゲストが電子メールアドレスを作成するときに [電子メールアドレス (Email Address)] に使用できないドメイン (例 : czgtgj.com) のブロックされたリストを指定します。
- [アカウント登録ゲストが承認される必要がある (Require self-registered guests to be approved)] : このポータルを使用するアカウント登録ゲストは、ゲストのクレデンシャル

を受信する前にスポンサーによる承認が必要であることを指定します。このオプションをクリックすると、スポンサーがアカウント登録ゲストを承認する方法に関する追加のオプションが表示されます。

- [承認要求電子メール送信先 (Email approval request to) ] : 次のいずれかを選択します。
  - [下に示すスポンサーの電子メールアドレス (sponsor email addresses listed below) ] : 承認者として指名されたスポンサーの1つ以上の電子メールアドレス、またはすべてのゲストの承認要求の送信先となるメールソフトウェアを入力します。電子メールアドレスが無効な場合、承認は失敗します。
  - [訪問先担当者 (person being visited) ] : [スポンサーに承認用クレデンシャルの入力を求める (Require sponsor to provide credentials for authentication) ] フィールドが表示され、[含むフィールド (Fields to include) ] の [必須 (Required) ] オプションが有効になります (以前は無効だった場合)。これらのフィールドはアカウント登録フォームに表示され、アカウント登録ゲストからこの情報を要求します。電子メールアドレスが無効な場合、承認は失敗します。
- [承認/拒否のリンクの設定 (Approve/Deny Link Settings) ] : このセクションでは次の内容を設定できます。
  - [リンクの有効期間 (Links are valid for) ] : アカウント承認リンクの有効期間を設定できます。
  - [スポンサーに承認用クレデンシャルの入力を求める (Require sponsor to provide credentials for authentication) ] : このセクションの設定でスポンサーによるアカウント承認用のクレデンシャルの入力が必須ではない場合にも、スポンサーにこの情報を入力させるには、このフィールドをオンにします。このフィールドは、[アカウント登録ゲストが承認される必要がある (Require self-registered guests to be approved) ] が [訪問先担当者 (person being visited) ] に設定されている場合にだけ表示されます。
  - [承認権限を検証するためスポンサーがスポンサーポータルと照合される (Sponsor is matched to a Sponsor Portal to verify approval privileges) ] : [詳細 > (Details >) ] をクリックして、スポンサーが有効なシステムユーザであり、スポンサーグループのメンバーであり、そのスポンサーグループのメンバーにアカウント承認権限があることを確認するために検索されるポータルを選択します。各スポンサーポータルには、スポンサーを識別するために使用される ID ソース シーケンスがあります。ポータルはリストされている順序で使用されます。リストの1番目のポータルは、スポンサーポータルで使用されているスタイルとカスタマイズ内容を決定します。
- [登録の送信後のゲストの誘導先 (After registration submission, direct guest to) ] : 登録の正常完了後にアカウント登録ゲストを誘導する場所を選択します。
  - [アカウント登録成功 (Self-Registration Success) ] ページ : アカウント登録に成功したゲストを [アカウント登録成功 (Self-Registration Success) ] ページに誘導します。こ

のページには、[アカウント登録成功ページ設定 (Self Registration Success Page Settings)] で指定したフィールドとメッセージが表示されます。

すべての情報を表示することが望ましくない場合があります。システムはアカウントの承認待ち（このページで有効になっている場合）であるか、またはこのページで指定された許可されたリストのドメインおよびブロックされているリストのドメインに基づいて電子メールアドレスまたは電話番号にログインクレデンシャルを提供する可能性があるためです。

[アカウント登録成功ページの設定 (Self Registration Success Page Settings)] で [ゲストのアカウント登録成功ページからの直接ログインを許可する (Allow guests to log in directly from the Self-Registration Success page)] を有効にした場合、アカウント登録に成功したゲストはこのページから直接ログインすることができます。これが有効になっていない場合、ゲストは [アカウント登録成功 (Self-Registration Success)] ページが表示された後にポータルログインページに誘導されます。

- [ログインクレデンシャルを取得する方法の手順を含むログインページ (Login page with instructions about how to obtain login credentials)] : アカウント登録に成功したゲストをポータルログインページに再び誘導し、「ゲストクレデンシャルが電子メール、SMS、または印刷物で提供されるのを待ってからログインに進んでください。」などのメッセージを表示します。

デフォルトメッセージをカスタマイズするには、[ポータルページのカスタマイズ (Portal Page Customization)] タブをクリックして、[アカウント登録ページ設定 (Self Registration Page Settings)] を選択します。

システムはアカウントの承認待ち（このページで有効になっている場合）であるか、またはこのページで指定された許可されたリスト、ブロックされているリストのドメインに基づいて電子メールアドレスまたは電話番号にログインクレデンシャルを提供する可能性があります。

- [URL] : アカウント登録に成功したゲストを、アカウントクレデンシャルの提供を待機している間に、指定された URL に誘導します。

システムはアカウントの承認待ち（このページで有効になっている場合）であるか、またはこのページで指定された許可されたリスト、ブロックされているリストのドメインに基づいて電子メールアドレスまたは電話番号にログインクレデンシャルを提供する可能性があります。

- [クレデンシャル通知自動送信手段 (Send credential notification automatically using)] :

- [電子メール (Email)] : アカウント登録に成功したゲストがログインクレデンシャルを受信する手段のオプションとして電子メールを選択します。このオプションを選択した場合、[電子メールアドレス (Email address)] が [含めるフィールド (Fields to include)] のリストで必須フィールドになり、このオプションを無効にできなくなります。
- [SMS] : アカウント登録に成功したゲストがログインクレデンシャルを受信する手段のオプションとして SMS を選択します。このオプションを選択した場合、[SMS サー

ビспロバイダー (SMS Service Provider) ]が[含めるフィールド (Fields to include) ]のリストで必須フィールドになり、このオプションを無効にできなくなります。

## アカウント登録成功ページの設定

このページへのナビゲーションパスは、[ワークセンター (Work Centers) ]>[ゲストアクセス (Guest Access) ]>[ポータルとコンポーネント (Portal s& Components) ]>[ゲストポータル (Guest Portals) ]>[作成、編集または複製 (Create, Edit or Duplicate) ]>[ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings) ]>[アカウント登録成功ページ設定 (Self Registration Success Page Settings) ]です。これらの設定を使用して、正常にアカウント登録したゲストに、ネットワークへのアクセスを獲得するために必要なクレデンシャルを通知します。

フィールド	使用上のガイドライン
アカウント登録の成功ページにこの情報を含める (Include this information on the Self-Registration Success page)	<p>[アカウント登録成功 (Self-Registration Success) ]ページで正常に登録されたゲストに表示されるフィールドのチェックボックスをオンにします。</p> <p>スポンサーによるゲストの承認が必要ない場合は、[ユーザ名 (Username) ]と[パスワード (Password) ]のチェックボックスをオンにして、ゲストにこれらのクレデンシャルを表示します。スポンサーの承認が必要な場合、クレデンシャルはゲストが承認された後のみ提供されるため、これらのフィールドを無効にします。</p>
ゲストは次の手段で情報を自分に送信できる (Allow guest to send information to self using)	<p>正常にアカウント登録したゲストが自分自身にクレデンシャル情報を送信するためのオプションのチェックボックスをオンにします。[印刷 (Print) ]、[電子メール (Email) ]、または[SMS]。</p>
AUP をページに含める/AUP をリンクとして含める (Include an AUP (on page/as link))	<p>会社のネットワーク使用の諸条件を、現在ユーザに表示されるページ上のテキストとして、またはAUPテキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。</p>

フィールド	使用上のガイドライン
同意が必要 (Require acceptance)	ユーザのアカウントが完全に有効になる前に、ユーザはAUPに同意する必要があります。[ログイン (Login)] ボタンは、ユーザがAUPを受け入れない場合は有効になりません。ユーザがAUPに同意しない場合、ネットワークにアクセスできません。
AUPの最後までスクロールが必要 (Require scrolling to end of AUP)	このフィールドは、[ページ上のAUP (AUP on page)] オプションを選択した場合のみ表示されます。  ユーザがAUPを最後まで読んだことを確認します。[同意 (Accept)] ボタンは、ユーザがAUPの最後までスクロールするとアクティブになります。
ゲストをアカウント登録の成功ページから直接ログインできるようにする (Allow guests to log in directly from the Self-Registration Success page)	[アカウント登録の成功 (Self-Registration Success)] ページ下部に[ログイン (Login)] ボタンを表示します。これにより、ゲストはログインページをバイパスし、自動的にログインクレデンシャルをポータルに提供して、ポータルフローの次のページ (たとえばAUPページ) を表示できるようになります。

## クレデンシャルを持つゲストポータルの利用規定 (AUP) ページ設定

このページへのナビゲーションパスは、[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲストポータル (Guest Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [利用規定 (AUP) ページ設定 (Acceptable Use Policy (AUP) Page Settings)] です。

- [AUP ページを含める (Include an AUP page)] : 会社のネットワーク使用諸条件を、別のページでユーザに表示します。
- [従業員に別のAUPを使用する (Use different AUP for employees)] : 従業員専用で別のAUPおよびネットワーク使用諸条件を表示します。このオプションを選択すると、[従業員用のAUPをスキップ (Skip AUP for employees)] は選択できません。
- [従業員用のAUPをスキップ (Skip AUP for employees)] : 従業員は、ネットワークにアクセスする前にAUPに同意する必要はありません。このオプションを選択すると、[従業員に別のAUPを使用する (Use different AUP for employees)] は選択できません。
- [AUPの最後までスクロールが必要 (Require scrolling to end of AUP)] : [AUPをページに含める (Include an AUP on page)] を有効にした場合のみ、このオプションが表示されます。



ユーザが AUP を最後まで読んだことを確認します。[同意 (Accept)] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。AUP がユーザに表示された場合に設定します。

- [初回のログインのみ (On first login only)] : ユーザが初めてネットワークまたはポータルにログインしたときに AUP を表示します。
- [ログインごと (On every login)] : ユーザがネットワークまたはポータルにログインするごとに、AUP を表示します。
- [\_\_ 日ごと (初回のログインから) (Every \_\_ days (starting at first login))] : ネットワークやポータルにユーザが初めてログインした後は、AUP を定期的に表示します。

## クレデンシャルを持つゲストポータルへのゲストによるパスワード変更の設定

### ゲストのパスワード変更設定 (Guest Change Password Settings)

このページへのナビゲーションパスは、[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲストポータル (Guest Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ゲストによるパスワード変更設定 (Guest Change Password Settings)] です。

- [ゲストにログイン後のパスワード変更を許可 (Allow guests to change password after login)] : ゲストが正常に認証され、AUP に同意した後に、ゲストに必要なに応じてパスワードを変更することを許可します。ゲストが自分のパスワードを変更した場合、スポンサーはゲストにログインクレデンシャル情報を提供できません。スポンサーは、ゲストのパスワードをランダムパスワードにリセットすることだけが可能です。

## クレデンシャルを持つゲストポータルへのゲストデバイス登録の設定

### ゲストデバイス登録設定 (Guest Device Registration Settings)

このページへのナビゲーションパスは、[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲストポータル (Guest Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ゲストデバイス登録設定 (Guest Device Registration Settings)] です。

これらの設定を使用して、ゲストがログインしたら Cisco ISE がゲストのデバイスを自動的に登録するようにするか、ゲストがログイン後に手動で自身のデバイスを登録することを許可できます。

各ゲストタイプの最大デバイス数は、[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲストタイプ (Guest Types)] で指定されます。

- [ゲストのデバイスを自動登録 (Automatically register guest devices)] : ゲストがこのポータルにアクセスするデバイスのエンドポイントを自動的に作成します。エンドポイントは、このポータルに指定されたエンドポイント ID グループに追加され、。

許可ルールの作成が可能になり、該当 ID グループ内のエンドポイントへのアクセスが許可されます。そのため、Web 認証は不要になります。

登録済みデバイスの最大数に到達すると、システムは自動的に最初の登録デバイスを削除し、ゲストがログインしようとしているデバイスを登録し、このことをゲストに通知します。[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲストタイプ (Guest Types)] を選択し、ゲストが登録できるデバイスの最大数を変更します。

- [ゲストにデバイスの登録を許可 (Allow guests to register devices)] : ゲストは、名前、説明、および MAC アドレスを入力して、自分のデバイスを手動で登録できます。MAC アドレスはエンドポイント ID グループに関連付けられます。

登録済みデバイスの最大数に到達した場合に別のデバイスを登録できるようにするには、ゲストは少なくとも 1 個のデバイスを削除する必要があります。

## クレデンシャルを持つゲスト ポータルの BYOD 設定

このページへのナビゲーションパスは、[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲストポータル (Guest Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [BYOD 設定 (BYOD Settings)] です。

この設定を使用して、従業員などゲスト以外の個人所有デバイスの持ち込み (BYOD) 機能を有効にし、クレデンシャルを持つゲストポータルを使用して企業ネットワークにアクセスできるようにします。

フィールド	使用上のガイドライン
従業員がネットワークでパーソナルデバイスを使用することを許可する (Allow employees to use personal devices on the network)	このポータルに [従業員の個人所有デバイス (BYOD) の登録 (Employee Bring Your Own Device (BYOD) Registration)] ページを追加して、従業員がデバイス登録プロセスを実行できるようにして、場合によってはネイティブサプリカントおよび証明書のプロビジョニングを実行できるようにします。これは、従業員のパーソナルデバイスタイプ (iOS、Android、RT またはモバイルを除く Windows、OSX など) のクライアントプロビジョニングの設定に応じて異なります。

フィールド	使用上のガイドライン
エンドポイント ID グループ (Endpoint Identity Group)	<p>ゲストのデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する <b>GuestEndpoints</b> のエンドポイント ID グループを提供します。デフォルトを使用しない場合、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。</p>
従業員にゲストアクセスの選択のみを許可する (Allow employees to choose to get guest access only)	<p>従業員をゲストネットワークにアクセスさせて、企業ネットワークへのアクセスに必要なことがある追加のプロビジョニングおよび登録を避けます。</p>
登録時にデバイス ID フィールドを表示する (Display Device ID field during registration)	<p>登録プロセス中に、デバイス ID をユーザに表示します。これは、デバイス ID が事前設定されており、BYOD ポータルを使用しているときに変更できない場合も含まれます。</p>
元の URL (Originating URL)	<p>ネットワークへの認証に成功すると、可能な場合はユーザのブラウザを、ユーザがアクセスしようとしていた元の Web サイトにリダイレクトします。リダイレクトできない場合は、認証成功ページが表示されます。リダイレクト URL が NAD のアクセスコントロールリストとその NAD の ISE で設定された許可プロファイルにより、PSN のポート 8443 で動作することを確認します。</p> <p>Windows、MAC、および Android デバイスの場合、制御はプロビジョニングを実行するセルフプロビジョニングウィザードアプリケーションに渡されます。そのため、これらのデバイスは元の URL にリダイレクトされません。ただし、iOS (dot1X) およびサポート対象外のデバイス (ネットワークアクセスが許可されている) では、この URL にリダイレクトされます。</p>
成功ページ (Success page)	<p>デバイスの登録が成功したことを示すページを表示します。</p>
URL	<p>ネットワークへの認証に成功すると、ユーザのブラウザを指定された URL (会社の Web サイトなど) にリダイレクトします。</p>

## クレデンシャルを持つゲストポータルのポストログインバナーページ設定

このページへのナビゲーションパスは、[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲストポータルまたはスポンサーポータル (Guest Portals or Sponsor Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ポストログインバナーページ設定 (Post-Login Banner Page Settings)] です。

これらの設定を使用して、正常なログイン後にユーザ（状況に応じてゲスト、スポンサーまたは従業員）に追加情報を通知します。

フィールド	使用上のガイドライン
ポストログインバナーページを含める (Include a Post-Login Banner page)	ユーザが正常にログインした後、ネットワークアクセスを付与される前に追加情報を表示します。

## 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のコンプライアンス設定

このページへのナビゲーションパスは、[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲストポータル (Guest Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ゲストデバイスのコンプライアンス設定 (Guest Device Compliance Settings)] です。これらの設定を使用して、ネットワークにアクセスするためにデバイスのクライアントプロビジョニングを実行するようゲストおよびゲストポータルを使用する従業員に要求します。

- [ゲストデバイスコンプライアンスが必要 (Require guest device compliance)]: ゲストをポスチャージェントのダウンロードを要求する[クライアントプロビジョニング (Client Provisioning)] ページにリダイレクトします。これにより、ウイルス対策ソフトウェアのチェックなど、ゲストのポスチャポリシーを設定するゲストフローにクライアントプロビジョニングが追加されます。

ゲストが、ネットワークへのアクセスにクレデンシャルを持つゲストポータルを使用している従業員の場合:

- [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)] が有効になっている場合、従業員はBYODフローにリダイレクトされ、クライアントのプロビジョニングは実行されません。
- [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)] および [従業員にゲストアクセスの選択のみを許可する (Allow employees to choose to get guest access)] が有効になっている場合、従業員はBYODフローにリダイレクトされ、クライアントのプロビジョニングは実行されません。

only) ]が有効になっていて、従業員がゲストアクセスを選択する場合、[クライアントプロビジョニング (Client Provisioning) ] ページにルーティングされます。

## ゲストポータルの VLAN DHCP リリース ページ設定

このページへのナビゲーションパスは、[ワークセンター (Work Centers) ]>[ゲストアクセス (Guest Access) ]>[ポータルとコンポーネント (Portal s& Components) ]>[ゲストポータル (Guest Portals) ]>[作成、編集または複製 (Create, Edit or Duplicate) ]>[ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings) ]>[VLAN DHCP リリース ページの設定 (VLAN DHCP Release Page Settings) ]です。

- [VLAN DHCP リリースを有効にする (Enable VLAN DHCP release) ] : 有線環境と無線環境の両方で VLAN が変更された後、Windows デバイスのゲストの IP アドレスを更新します。

これは、ネットワーク アクセスでゲスト VLAN が新しい VLAN に変更されたときに、最終的な許可処理時の中央 WebAuth (CWA) フローに影響します。ゲストの古い IP アドレスは VLAN の変更の前にリリースされる必要があります、ゲストが新しい VLAN に接続するときに新しいゲスト IP アドレスが DHCP を介して要求される必要があります。IP アドレスのリリースと更新操作は、DirectX コントロールを使用する Internet Explorer ブラウザのみでサポートされています。

VLAN DHCP リリース オプションは、モバイルデバイスでは動作しません。代わりに、ゲストが IP アドレスを手動でリセットする必要があります。この方法はデバイスによって異なります。たとえば、Apple iOS デバイスでは、ゲストは Wi-Fi ネットワークを選択して、[リースを更新 (Renew Lease) ] ボタンをクリックできます。

- [リリースを\_\_秒遅延 (Delay to release \_\_ seconds) ] : リリース遅延時間を入力します。リリースは、アプレットをダウンロードした直後から、Cisco ISE サーバが CoA 要求を再認証するよう NAD に指示するまでの間に行う必要があるため、この時間は短くすることを推奨します。
- [CoA を\_\_秒遅延 (Delay to CoA \_\_ seconds) ] : Cisco ISE が CoA の実行を遅延する時間を入力します。十分な時間を指定して (ガイドラインとしてデフォルト値を使用)、アプレットによるクライアント上での IP リリースのダウンロードと実行を可能にします。
- [更新を\_\_秒遅延 (Delay to renew \_\_ seconds) ] : 更新を遅延する値を入力します。この時間は IP リリース値に追加され、コントロールがダウンロードされるまで計時が開始されません。十分な時間を指定して (ガイドラインとしてデフォルト値を使用)、CoA の処理を可能にし、新しい VLAN アクセスが付与されるようにします。

## ゲストポータルの認証成功の設定

このページへのナビゲーションパスは、[ワークセンター (Work Centers) ]>[ゲストアクセス (Guest Access) ]>[ポータルとコンポーネント (Portals & Components) ]>[ゲストポータル (Guest Portals) ]>[作成、編集または複製 (Create, Edit or Duplicate) ]>[ポータルの動作

およびフローの設定 (Portal Behavior and Flow Settings) ] > [認証成功の設定 (Authentication Success Settings) ] です。

これらの設定では、ユーザ (状況に応じてゲスト、スポンサーまたは従業員) に認証の成功が通知されるか、または URL が表示されます。[認証されたらゲストに次を表示: (Once authenticated, take guest to:)] で、次のフィールドを設定します。

- 元の URL (Originating URL) : ネットワークへの認証に成功すると、可能な場合はユーザのブラウザを、ユーザがアクセスしようとしていた元の Web サイトにリダイレクトします。リダイレクトできない場合は、認証成功ページが表示されます。リダイレクト URL が NAD のアクセス コントロール リストとその NAD の ISE で設定された許可プロファイルにより、PSN のポート 8443 で動作することを確認します。

Windows、MAC、および Android デバイスの場合、制御はプロビジョニングを実行するセルフプロビジョニング ウィザード アプリケーションに渡されます。そのため、これらのデバイスは元の URL にリダイレクトされません。ただし、iOS (dotIX) およびサポート対象外のデバイス (ネットワーク アクセスが許可されている) では、この URL にリダイレクトされます。

- 認証の成功ページ (Authentication Success page) : ユーザの認証に成功した通知。
- URL : ネットワークへの認証に成功すると、ユーザのブラウザを指定された URL (会社の Web サイトなど) にリダイレクトします。



(注) 認証後に外部 URL にゲストをリダイレクトする場合、URL アドレスを解決して、セッションがリダイレクトされるまでに遅延が生じることがあります。リダイレクト URL が NAD のアクセス コントロール リストとその NAD の ISE で設定された許可プロファイルにより、PSN のポート 8443 で動作することを確認します。

## ゲストポータルをサポート情報ページの設定

このページへのナビゲーションパスは、[ワークセンター (Work Centers) ] > [ゲストアクセス (Guest Access) ] > [ポータルとコンポーネント (Portals & Components) ] > [ゲストポータル (Guest Portals) ] > [作成、編集または複製 (Create, Edit or Duplicate) ] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings) ] > [サポート情報ページの設定 (Support Information Page Settings) ] です。

これらの設定を使用して、ヘルプデスクがユーザ (状況に応じてゲスト、スポンサーまたは従業員) が体験したアクセスの問題をトラブルシューティングするために使用できる情報を表示します。

フィールド	使用上のガイドライン
サポート情報ページを含める (Include a Support Information Page)	該当ポータルのすべての有効なページ上で、問い合わせ先などの情報へのリンクを表示します。

フィールド	使用上のガイドライン
MAC アドレス	[サポート情報 (Support Information) ] ページにデバイスの MAC アドレスを含めます。
IP アドレス	[サポート情報 (Support Information) ] ページにデバイスの IP アドレスを含めます。
ブラウザのユーザエージェント (Browser user agent)	[サポート情報 (Support Information) ] ページに、要求の発信元のユーザエージェントの製品名とバージョン、レイアウトエンジン、バージョンなど、ブラウザの詳細を含めます。
ポリシー サーバ (Policy server)	[サポート情報 (Support Information) ] ページに、このポータルを提供している ISE ポリシーサービス ノード (PSN) の IP アドレスを含めます。
障害コード (Failure code)	可能な場合は、ログメッセージカタログ内の対応する番号を含めます。メッセージカタログにアクセスしてこれを表示するには、[管理 (Administration) ]>[システム (System) ]>[ロギング (Logging) ]>[メッセージカタログ (Message Catalog) ] に移動します。
フィールドを隠す (Hide field)	含める情報が存在しない場合、[サポート情報 (Support Information) ] ページ上の該当するフィールドラベルを表示しません。たとえば、障害コードが不明であるために空白である場合、[障害コード (Failure code) ] は、選択されている場合でも表示されません。
値のないラベルを表示 (Display label with no value)	含める情報が存在しない場合でも、選択されているすべてのフィールドのラベルを [サポート情報 (Support Information) ] ページに表示します。たとえば、障害コードが不明な場合、[障害コード (Failure code) ] は空白であっても表示されます。
デフォルト値でラベルを表示 (Display label with default value)	[サポート情報 (Support Information) ] ページ上の選択されているフィールドに含まれる情報が存在しない場合、このテキストがこれらのすべてのフィールドに表示されます。たとえば、このフィールドに「Not Available」と入力した場合に障害コード不明が不明な場合は、[障害コード (Failure code) ] に [使用できません (Not Available) ] と表示されます。

# スポンサー ポータル アプリケーションの設定

## ポータル ID 設定

これらの設定へのナビゲーションパスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータルまたはスポンサー ポータル (Guest Portals or Sponsor Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ゲスト ポータルおよびスポンサー ポータルの設定とカスタマイズ (Guest Portals or Sponsor Portals Settings and Customization)] です。

- ポータル名 (Portal Name) : このポータルにアクセスするための一意のポータル名を入力します。このポータル名を、その他のスポンサー、ゲスト、または非ゲストポータル (ブラックリスト、個人所有デバイス持ち込み (BYOD)、クライアントプロビジョニング、モバイルデバイス管理 (MDM)、またはデバイスの各ポータル) に使用しないでください。

この名前は、リダイレクションを選択するために、認証プロファイルポータルの選択に表示されます。これはポータルのリストに適用され、他のポータルとの間で簡単に識別できます。

- 説明 (Description) : 任意項目です。
- ポータルテスト URL (Portal test URL) : [保存 (Save)] をクリックした後にリンクとして表示されるシステムにより生成された URL。ポータルをテストするために使用します。  
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、ISE は最初のアクティブ PSN を選択します。

- 言語ファイル (Language File) : 各ポータルタイプは、デフォルトで 15 種類の言語をサポートします。これらの言語は、個々のプロパティファイルとして使用できます。これらのファイルは、圧縮された単一の言語ファイル内にまとめてバンドルされています。ポータルで使用する圧縮言語ファイルをエクスポートまたはインポートします。圧縮言語ファイルには、ポータルのテキストを表示するために使用可能な個別の言語ファイルがすべて含まれています。



言語ファイルには、その言語のポータル全体のすべての文字列設定に加え、特定のブラウザのロケール設定（例：フランス語の場合は `fr`、`fr-fr`、`fr-ca`）へのマッピングが含まれています。1つの言語ファイルには、翻訳およびローカリゼーションの目的に容易に使用できるように、サポートされるすべての言語が含まれています。

1つの言語用のブラウザ ロケール設定を変更した場合、変更内容は他のすべてのエンドユーザ Web ポータルに適用されます。たとえば、ホットスポット ゲストポータルの `French.properties` ブラウザロケールを `fr,fr-fr,fr-ca` から `fr,fr-fr` に変更すると、この変更内容がデバイスポータルにも適用されます。

[ポータルページのカスタマイズ (Portal Page Customizations)] タブでいずれかのテキストをカスタマイズすると、警告アイコンが表示されます。警告メッセージは、ポータルのカスタマイズ時に1つの言語で行った変更をすべてのサポート対象の言語プロパティファイルにも追加する必要があることを通知します。ドロップダウンリストのオプションを使用して、手動で警告アイコンが表示されないようにします。また、警告アイコンは、更新された圧縮言語ファイルのインポート後に自動的に表示されなくなります。

## スポンサー ポータルのポータル設定

これらの設定を設定して、ポータルを特定し、すべてのポータルページで使用する言語ファイルを選択します。

- [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**



(注) 最適なパフォーマンスを得るには、ゲスト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、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ています。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、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ています。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ため、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ています。

- [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。
- [完全修飾ドメイン名 (FQDN) (Fully Qualified Domain Name (FQDN)) ] : スポンサーまたはデバイス ポータルに対応する1つの固有のFQDNまたはホスト名を入力します。たとえば、**sponsorportal.yourcompany.com**、**sponsor** と入力することで、ユーザはブラウザにこれらのいずれかを入力すると、スポンサーポータルが表示されます。カンマを使用して名前を区切りますが、エントリ間にスペースを挿入しないでください。

デフォルトのFQDNを変更する場合は、次を実行します。

- DNS を更新して、新しいURLのFQDNが有効なポリシー サービス ノード (PSN) のIPアドレスに解決するようにします。PSNのプールを提供するロードバランサの仮想IPアドレスを指定することもできます。
- 名前の不一致による証明書の警告メッセージを回避するために、Cisco ISE PSNのローカルサーバ証明書のサブジェクト代替名 (SAN) 属性に、カスタマイズされたURLのFQDNまたはワイルドカードを含めます。
- 認証方式 (Authentication Method) IDソース順序 (Identity source sequence) : ユーザ認証に使用するIDソース順序 (ISS) またはIDプロバイダー (IdP) を選択します。ISSは、ユーザクレデンシャルを確認するために順番に検索されるIDストアのリストです。たとえば、内部ゲストユーザ、内部ユーザ、Active Directory、LDAPディレクトリなどがあります。

Cisco ISEには、スポンサーポータル Sponsor\_Portal\_Sequence 用のデフォルトのスポンサーIDソース順序が含まれています。

IdPを設定するには、[管理 (Administration) ]>[IDの管理 (Identity Management) ]>[外部IDソース (External Identity Sources) ]>[SAML ID プロバイダー (SAML Id Providers) ]の順に選択します。

IDソース順序を設定するには、[管理 (Administration) ]>[IDの管理 (Identity Management) ]>[IDソース順序 (Identity Source Sequences) ]の順に選択します。

- [アイドル タイムアウト (Idle timeout) ]: ポータルでアクティビティがない場合にユーザをログアウトするまでに Cisco ISE が待機する時間 (分) を入力します。有効な範囲は 1 ~ 30 分です。
- [Kerberosを許可する (Allow Kerberos) ]: スポンサー ポータルへアクセスするためのスポンサーの認証に Kerberos を使用します。ブラウザが ISE との SSL 接続を確立した後、セキュア トンネル内で Kerberos SSO が実行されます。



(注) Kerberos 認証には、同じドメイン内に存在する次の項目が必要です。

- スポンサーの PC
- ISE PSN
- このスポンサー ポータルに設定された FQDN



(注) ゲスト ポータルの Kerberos 認証はサポートされていません。

#### • 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。

## スポンサー ポータルのログイン設定

### スポンサー ポータルのログイン ページ設定

このページへのナビゲーションパスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Sponsor Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ログイン ページの設定 (Login Page Settings)] です。

- [頻度制限までの最大ログイン試行失敗数 (Maximum failed login attempts before rate limiting)] : Cisco ISE がアカウントのスロットルを開始するまでの単一のブラウザセッションからのログイン試行失敗回数を指定します。これにより、アカウントのロックアウトは起きません。スロットル率は、[頻度制限時のログイン試行間隔 (Time between login attempts when rate limiting)] で設定されます。
- [頻度制限時のログイン試行間隔 (Time between login attempts when rate limiting)] : [頻度制限までの最大ログイン試行失敗数 (Maximum failed login attempts before rate limiting)] で定義された回数のログインの失敗後に、ユーザが再度ログインを試行するまでに待機する必要がある時間 (スロットル率) を分単位で設定します。
- [AUPを含める (Include an AUP)] : フローに利用規約ページを追加します。AUP をページに追加したり、別のページへのリンクを設定することができます。これを追加すると、右側のフローの画像が変わります。
  - [同意が必要 (require acceptance)] : フローを続行する前に、ユーザが AUP に同意するように強制します。

## スポンサー ポータルの利用規定 (AUP) 設定

このページへのナビゲーションパスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Sponsor Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [利用規定 (AUP) ページ設定 (Acceptable Use Policy (AUP) Page Settings)] です。

これらの設定を使用して、ユーザ (状況に応じてゲスト、スポンサーまたは従業員) に対して AUP エクスペリエンスを定義します。

フィールド	使用上のガイドライン
AUP ページを含める (Include an AUP page)	会社のネットワーク使用諸条件を、別のページでユーザに表示します。
AUP の最後までスクロールが必要 (Require scrolling to end of AUP)	ユーザが AUP を最後まで読んだことを確認します。[同意 (Accept)] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。

フィールド	使用上のガイドライン
初回のログインのみ (On first login only)	ユーザがネットワークまたはポータルに初めてログインしたときのみ、AUPを表示します。
ログインごと (On every login)	ユーザがネットワークまたはポータルにログインするごとに、AUPを表示します。
__日ごと (初回のログインから) (Every __ days (starting at first login))	ユーザがネットワークまたはポータルに初めてログインした後に、定期的にAUPを表示します。

## スポンサー ポータルのスポンサーのパスワード変更設定

このページへのナビゲーションパスは、[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサーポータル (Sponsor Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [スポンサーによるパスワード変更設定 (Sponsor Change Password Settings)] です。これらの設定により、スポンサーポータルを使用するスポンサーのパスワード要件が定義されます。

すべてのユーザのパスワードポリシーを設定するには、[管理 (Administration)] > [IDの管理 (Identity Management)] > [設定 (Settings)] > [ユーザパスワードポリシー (User Password Policy)] を選択します。

フィールド	使用上のガイドライン
スポンサーは自身のパスワードを変更可能 (Allow sponsors to change their own passwords)	スポンサーは、スポンサーポータルにログインした後、自身のパスワードを変更できます。このオプションは、スポンサーが内部ユーザデータベースの一部である場合にだけ、[パスワードの変更 (Change Password)] ページを表示します。

## スポンサー ポータルのポストログインバナー設定

このページへのナビゲーションパスは、[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲストポータルまたはスポンサーポータル (Guest Portals or Sponsor Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ポストログインバナーページ設定 (Post-Login Banner Page Settings)] です。

これらの設定を使用して、正常なログイン後にユーザ（状況に応じてゲスト、スポンサーまたは従業員）に追加情報を通知します。

フィールド	使用上のガイドライン
ポストログインバナー ページを含める (Include a Post-Login Banner page)	ユーザが正常にログインした後、ネットワークアクセスを付与される前に追加情報を表示します。

## スポンサーポータルをサポート情報ページの設定

このページへのナビゲーションパスは、[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサーポータル (Sponsor Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [サポート情報ページの設定 (Support Information Page Settings)] です。

これらの設定を使用して、ヘルプデスクがユーザ（状況に応じてゲスト、スポンサーまたは従業員）が体験したアクセスの問題をトラブルシューティングするために使用できる情報を表示します。

フィールド	使用上のガイドライン
サポート情報ページを含める (Include a Support Information Page)	該当ポータルのすべての有効なページ上で、 <b>問い合わせ先</b> などの情報へのリンクを表示します。
MAC アドレス	[サポート情報 (Support Information)] ページにデバイスの MAC アドレスを含めます。
IP アドレス	[サポート情報 (Support Information)] ページにデバイスの IP アドレスを含めます。
ブラウザのユーザエージェント (Browser user agent)	[サポート情報 (Support Information)] ページに、要求の発信元のユーザエージェントの製品名とバージョン、レイアウトエンジン、バージョンなど、ブラウザの詳細を含めます。
ポリシー サーバ (Policy server)	[サポート情報 (Support Information)] ページに、このポータルを提供している ISE ポリシーサービス ノード (PSN) の IP アドレスを含めます。

フィールド	使用上のガイドライン
障害コード (Failure code)	可能な場合は、ログメッセージカタログ内の対応する番号を含めます。メッセージカタログにアクセスしてこれを表示するには、[管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [メッセージカタログ (Message Catalog)] に移動します。
フィールドを隠す (Hide field)	含める情報が存在しない場合、[サポート情報 (Support Information)] ページ上の該当するフィールドラベルを表示しません。たとえば、障害コードが不明であるために空白である場合、[障害コード (Failure code)] は、選択されている場合でも表示されません。
値のないラベルを表示 (Display label with no value)	含める情報が存在しない場合でも、選択されているすべてのフィールドのラベルを[サポート情報 (Support Information)] ページに表示します。たとえば、障害コードが不明な場合、[障害コード (Failure code)] は空白であっても表示されます。
デフォルト値でラベルを表示 (Display label with default value)	[サポート情報 (Support Information)] ページ上の選択されているフィールドに含まれる情報が存在しない場合、このテキストがこれらのすべてのフィールドに表示されます。たとえば、このフィールドに「Not Available」と入力した場合に障害コード不明が不明な場合は、[障害コード (Failure code)] に [使用できません (Not Available)] と表示されます。

## スポンサーポータルへのゲストへの通知のカスタマイズ

これらの設定へのナビゲーションパスは、[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサーポータル (Sponsor Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルページのカスタマイズ (Portal Page Customization)] > [ゲストへの通知 (Notify Guests)] です。

[ページのカスタマイズ (Page Customizations)] で、スポンサーがスポンサーポータルからゲストに送信する通知に表示される、メッセージ、タイトル、コンテンツ、手順、およびフィールドやボタンのラベルをカスタマイズできます。

[設定 (Settings)] では、スポンサーが電子メールまたはSMSを使用してゲストにユーザ名とパスワードを個別に送信できるかどうかを指定できます。また、ヘルプデスクがアクセスの間



題をトラブルシューティングするために使用できる情報を提供するために、スポンサーがゲストに [サポート情報 (Support Information)] ページを表示できるかどうかを指定できます。

## スポンサー ポータルのカスタマイズの管理と承認

これらの設定へのナビゲーションパスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Sponsor Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [管理と承認 (Manage and Approve)] です。

[ページのカスタマイズ (Page Customizations)] で、スポンサー ポータルの [管理と承認 (Manage and Approve)] タブに表示される、メッセージ、タイトル、コンテンツ、手順、およびフィールドやボタンのラベルをカスタマイズできます。

これらには、アカウント (登録済みおよび保留) の概要および詳細ビュー、スポンサーがゲストアカウントに対して実行する編集、拡張、一時停止などの操作に基づいて表示されるポップアップ ダイアログ、さらに汎用ポータルやアカウント アクション メッセージが含まれています。

## グローバル設定

### ゲストおよびスポンサー ポータルのグローバル設定

[ゲスト アクセス (Guest Access)] > [設定 (Settings)] を選択します。Cisco ISE 内のゲストポータル、スポンサー ポータル、ゲスト タイプ、およびスポンサー グループに適用される、次の一般設定を設定できます。

- ゲスト アカウントの消去、およびユーザ名とパスワードの生成のポリシー。
- 電子メールおよび SMS 通知をゲスト アカウントとスポンサーに送信するときに使用する SMTP サーバおよび SMS ゲートウェイ。
- アカウント登録ゲスト ポータルを使用したゲスト アカウントの作成およびゲストの登録時に選択する場所、タイムゾーン、SSID およびカスタム フィールド。

これらのグローバル設定を指定すると、特定のゲスト ポータルとスポンサー ポータル、ゲスト タイプおよびスポンサー グループの設定時にそれらが必要に応じて使用できます。

[ポータル設定 (Portal settings)] ページには、次のタブがあります。

- [ゲストアカウントの消去ポリシー (Guest Account Purge Policy)] : 期限が切れたゲストアカウントを消去する時期をスケジューリングします。詳細については、[期限切れのゲストアカウントを消去するスケジューリング設定](#)を参照してください。

- [カスタムフィールド (Custom Fields) ]: ユーザから追加情報を取得するためにゲストポータルで使用するカスタム フィールドを追加します。詳細については、[ゲストアカウント作成用のカスタム フィールドの追加](#)を参照してください。
- [ゲスト電子メールの設定 (Guest Email Settings) ]: アカウントの変更をゲストに電子メール通知するかどうかを決定します。詳細については、[電子メールでの通知用の電子メールアドレスおよび SMTP サーバの指定](#)を参照してください。
- [ゲストのロケーションおよびSSID (Guest Locations and SSIDs) ]: ロケーションと、ゲストがそのロケーションで使用できるネットワークのサービス セット識別子 (SSID) を設定します。詳細については、[ゲストのロケーションおよび SSID の割り当て](#)を参照してください。
- [ゲストユーザ名ポリシー (Guest Username Policy) ]: ゲスト ユーザ名の作成方法を設定します。詳細については、[ゲスト ユーザ名ポリシーの設定](#)および[ゲストパスワードポリシーのルール](#)を参照してください。
- [ゲストパスワードポリシー (Guest Password Policy) ]: すべてのゲストポータルとスポンサーポータルのゲストパスワードポリシーを定義します。詳細については、[ゲストパスワードポリシーと有効期限の設定](#)を参照してください。
- [ロギング (Logging) ]: ゲストユーザは、デバイスの MAC アドレスで追跡されます。ゲストユーザがレポートに表示される場合、ユーザ名は MAC アドレスです。このオプションを選択すると、ユーザ名として MAC アドレスではなく、ポータル ユーザ ID がレポートに表示されます。このオプションの詳細については、[ゲストユーザ情報を保存](#)を参照してください。

## ゲストタイプの設定

これらの設定のナビゲーションパスは、[ワークセンター (Work Centers) ]>[ゲストアクセス (Guest Access) ]>[ポータルとコンポーネント (Portals & Components) ]>[ゲストタイプ (Guest Types) ]です。これらの設定を使用して、ネットワークにアクセスできるゲストのタイプおよびそのアクセス権限を作成します。また、このタイプのゲストを作成できるスポンサーグループを指定できます。

- [ゲストタイプ名 (Guest type name) ]: このゲストタイプを他のゲストタイプと区別する名前 (1 ~ 256 文字) を指定します。
- [説明 (Description) ]: このゲストタイプの推奨される使用方法に関する追加情報 (最大 2000 文字) を指定します。たとえば、アカウント登録ゲスト用。ゲストアカウントの作成に使用しない、など。
- [言語ファイル (Language File) ]: このフィールドでは、サポート対象のすべての言語で、電子メールの件名、電子メールメッセージ、および SMS メッセージの内容を含む言語ファイルをエクスポートおよびインポートできます。これらの言語とコンテンツは、アカウントが期限切れになった旨の通知に使用され、このゲストタイプに割り当てられているゲストに送信されます。新しいゲストタイプを作成すると、ゲストタイプを保存するまでは

この機能は無効です。言語ファイルの編集の詳細については、[ポータル言語のカスタマイズ](#)を参照してください。

- [追加データを収集 (Collect Additional Data) ] : [カスタムフィールド... (Custom Fields...)] ボタンをクリックして、このゲストタイプを使用しているゲストから追加データを収集するために使用するカスタム フィールドを選択します。

カスタム フィールドを管理するには、[ワークセンター (Work Centers) ]>[ゲストアクセス (Guest Access) ]>[設定 (Settings) ]>[カスタムフィールド (Custom Fields) ]を選択します。

- **最大アクセス時間 (Maximum Access Time)**

- [アカウント期間の開始 (Account duration starts) ] : [最初のログインから (From first login) ]を選択した場合、アカウントの開始時間は、ゲストユーザがゲストポータルに最初にログインしたときに開始され、終了時間は指定された期間に相当します。ゲストユーザがログインしなければ、アカウントがゲストアカウント消去ポリシーによって削除されるまで、アカウントはAwaiting first login状態のままになります。

値は、1 から 999 日、時間、または分です。

アカウント登録ユーザのアカウントは、ユーザがアカウントを作成し、自分のアカウントにログオンしたときに開始されます。

[スポンサーが指定した日付から (From sponsor-specified date) ]を選択した場合は、このゲストタイプのゲストがネットワークにアクセスして接続を保持できる最大日数、時間数、または分数を入力します。

この設定を変更した場合、変更内容はこのゲストタイプを使用して作成された既存のゲストアカウントには適用されません。

- [最大アカウント期間 (Maximum account duration) ] : このゲストタイプが割り当てられているゲストがログインできる期間 (日数、時間数、または分数) を入力します。




---

(注) アカウント消去ポリシーにより期限切れのゲストアカウントが確認され、期限切れ通知が送信されます。このポリシーは 20 分ごとに実行されるため、アカウント期間を 20 分未満に設定すると、アカウントの消去前に期限切れ通知が送信されることがあります。

---

[アクセスを許可する日付と時刻 (Allow access only on these days and times) ] オプションを使用して、このゲストタイプのゲストにアクセスを提供する期間や曜日を指定できます。

- 選択した曜日によって、スポンサーのカレンダーで選択できる日付へのアクセスが制限されます。
- スポンサーが期間と日付を選択すると、スポンサーポータルで最大アカウント期間が適用されます。

ここで設定するアクセス時刻の設定は、ゲストアカウントの作成時にスポンサーポータルで使用できる時刻設定に影響します。詳細については、[スポンサーに対して使用可能な時間設定項目の設定](#)を参照してください。

#### • ログインオプション

- [最大同時ログイン数 (Maximum simultaneous logins) ] : このゲストタイプに割り当てられたユーザが同時に実行できる最大ユーザセッション数を入力します。
- [ゲストが制限を超えた場合 (When guest exceeds limit) ] : [最大同時ログイン数 (Maximum simultaneous logins) ] を選択した場合は、その最大ログイン数に到達した後でユーザが接続したときに実行するアクションも選択する必要があります。

##### • 最も古い接続を切断 (Disconnect the oldest connection)

- [最も新しい接続を切断 (Disconnect the newest connection) ] : [エラーメッセージを示すポータルページにユーザをリダイレクトする (Redirect user to a portal page showing an error message) ] をオプションで選択 : 特定の時間にわたってエラーメッセージが表示され、その後セッションが切断されてユーザがゲストポータルにリダイレクトされます。エラーメッセージが表示される時間は設定可能です。エラーページの内容は、[メッセージ (Messages) ] > [エラーメッセージ (Error Messages) ] ページの [ポータルページのカスタマイズ (Portal Page Customization) ] ダイアログで設定します。
  - [ゲストが登録できるデバイスの最大数 (Maximum devices guests can register) ] : 各ゲストに登録できるデバイスの最大数を入力します。そのゲストタイプのゲストに登録済みの値より小さい値を最大数として設定できます。この値は、新しく作成されたゲストアカウントにのみ適用されます。新しいデバイスを追加し、最大数に達すると、最も古いデバイスが切断されます。
  - [ゲストデバイス登録のためのエンドポイントIDグループ (Endpoint identity group for guest device registration) ] : ゲストのデバイスに割り当てるエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **GuestEndpoints** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、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。
  - [ゲストに対しゲストポータルのバイパスを許可する (Allow guest to bypass the Guest portal) ] : クレデンシャルを持つゲストタイプのキャプティブポータル (Web 認証ページ) をバイパスし、有線およびワイヤレス (dot1x) サブリカントまたは VPN クライアントに認証情報を提供することでネットワークにアクセスすることをユーザに許可します。ゲストアカウントは、AUP が必要な場合でも、[初期ログインを待機 (Awaiting Initial Login) ] 状態と AUP ページをバイパスして [アクティブ (Active) ] 状態になります。
- この設定を有効にしない場合、ユーザは初めにクレデンシャルを持つゲストのキャプティブポータルを使用してログインしないと、ネットワークの他の部分にアクセスできません。

#### • アカウント有効期限通知

- [アカウント有効期限の \_\_ 日前にアカウント有効期限通知を送信する (Send account expiration notification \_\_ days before account expires) ] : アカウントが期限切れになる前にゲストに通知を送信します。有効期限前の日数、時間数、または分数を指定します。
- [メッセージ表示原語 (View messages in) ] : 電子メールまたは SMS 通知の表示言語を指定します。
- [電子メール (Email) ] : アカウント有効期限通知を電子メールで送信します。
- [次のポータルのカスタマイズを使用する (Use customization from) ] : 選択したポータルに対して設定した同一のカスタマイズ内容をこのゲストタイプのアカウント有効期限メールに適用します。
- [テキストのコピー元 (Copy text from) ] : 別のゲスト タイプのアカウント有効期限メールに、作成した電子メール テキストを再利用します。
- **テスト電子メールの送信先 (Send test email to me at)**
- [SMS] : アカウント有効期限通知を SMS で送信します。  
SMS の設定は、電子メール通知の設定と同一ですが、[テスト SMS の送信 (Send test SMS to me) ] の SMS ゲートウェイを選択する点が異なります。
- [スポンサーグループ (Sponsor Groups) ] : このゲスト タイプを使用してメンバーがゲストアカウントを作成できるスポンサー グループを指定します。このゲスト タイプにアクセスできないようにするスポンサー グループは削除します。

## スポンサー グループ設定

これらの設定のナビゲーションパスは、[ワーク センター (Work Centers) ]>[ゲスト アクセス (Guest Access) ]>[ポータルとコンポーネント (Portals & Components) ]>[スポンサー グループ (Sponsor Groups) ]です。スポンサー グループにメンバーを追加したり、ゲスト タイプおよびロケーション特権を定義したり、ゲストアカウントの作成と管理に関連する権限を設定したりする場合に、これらの設定を使用します。

- [スポンサー グループの無効化 (Disable Sponsor Group) ] : このスポンサー グループのメンバーがスポンサー ポータルにアクセスできないようにします。  
たとえば、管理者ポータルで設定を変更している間、スポンサーが一時的にスポンサーポータルにログインできないようにします。あるいは、再びアクティブ化する必要があるまで、年次会議のスポンサーシップゲストなど、頻繁には発生しないアクティビティに関するスポンサー グループを無効にします。
- **スポンサーグループ名 (Sponsor group name)** : 一意の名前を入力します (1 ~ 256 文字) 。
- **[説明 (Description) ]** : このスポンサー グループで使用されるゲスト タイプなどの有益な情報を入力します (最大 2000 文字) 。

- [ゲストタイプの設定 (Configure Guest Types)] : 必要とするゲストタイプが使用可能でない場合は、[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲストタイプ (Guest Types)] の順にクリックし、新しいゲストタイプを作成するか、または既存のゲストタイプを編集します。

- **一致基準**

- **メンバー (Members)** : [スポンサーグループメンバーの選択 (Select Sponsor Group Members)] ボックスを表示する場合にクリックします。ここでは、使用可能なユーザIDグループを (内部および外部のIDストアから) 選択し、このスポンサーグループのメンバーとして追加できます。
  - **スポンサーグループメンバー (Sponsor Group Members)** : 選択したスポンサーグループのリストを検索およびフィルタリングし、含めないグループを削除します。
- **その他の条件 (Other conditions)** : [新しい条件の作成 (Create New Condition)] をクリックして、このスポンサーグループに含まれるためにスポンサーが満たす必要がある条件を1つ以上構築します。Active Directory、LDAP、SAML、ODBCのIDストアからの認証属性を使用できますが、RADIUS トークンまたはRSA SecurID ストアは使用できません。内部ユーザ属性も使用できます。条件には、属性、演算子、値があります。
  - ディクショナリ属性 *Name* を使用して条件を作成するには、IDグループ名の前にユーザIDグループを付けます。次に例を示します。

*InternalUser:Name EQUALS bsmith*

この場合、「bsmith」という名前の内部ユーザだけがこのスポンサーグループに所属できます。

- このスポンサーグループはこれらのゲストタイプを使用してアカウントを作成可能 (This sponsor group can create accounts using these guest types) : このスポンサーグループのメンバーがゲストアカウントの作成時に使用できるゲストタイプを指定します。有効にするスポンサーグループには、使用できる少なくとも1つのゲストタイプが設定されている必要があります。

このスポンサーグループに1つのゲストタイプのみを割り当てる場合、それが使用可能な唯一の有効なゲストであるため、スポンサーポータルに表示しないことを選択できます。[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサーポータル (Sponsor Portal)] > [ページカスタマイズ (Page Customization)] > [アカウントの作成 (Create Accounts)] > [ゲストタイプ (Guest Types)] > [設定 (Settings)] の順に選択します。このオプションを有効にするには、[スポンサーで1つのみ使用できる場合はゲストタイプを非表示 (Hide guest type if only one is available to sponsor)] をオンにします。

- **ゲストがアクセスするロケーションを選択 (Select the locations that guests will be visiting)** : このグループのスポンサーがアカウントの作成時にゲストに割り当てることができるさま

さまざまなロケーションを選択します。このことは、これらのゲストアカウントの有効な時間帯を定義し、有効なアクセス時間などゲストに適用するすべての時間パラメータを指定する場合に役立ちます。このことによって、ゲストが他のロケーションからネットワークに接続できなくなることはありません。

有効にするスポンサーグループには、使用できる少なくとも1つのロケーションが設定されている必要があります。

このスポンサーグループに1つのロケーションのみを割り当てると、それが、メンバーが作成するゲストアカウントの唯一の有効な時間帯になります。デフォルトでは、スポンサーポータルに表示されません。

### スポンサーが作成可能 (Sponsor Can Create)

- 特定のゲストに割り当てられた複数のゲストアカウント (インポート) (Multiple guest accounts assigned to specific guests (Import)) : スポンサーは、ファイルから姓名などのゲストの詳細をインポートすることによって、複数のゲストアカウントを作成できます。

このオプションが有効である場合、[インポート (Import)] ボタンがスポンサーポータルの [アカウントの作成 (Create Accounts)] ページに表示されます。[インポート (Import)] オプションは、Internet Explorer、Firefox、Safari などのデスクトップブラウザだけで使用可能です (モバイルは不可)

- バッチ処理の制限 (Limit to batch of) : このスポンサーグループが複数のアカウントを同時に作成できる場合、単一のインポート操作で作成可能なゲストアカウントの数を指定します。

スポンサーは最大 10,000 個のアカウントを作成できますが、潜在的なパフォーマンスの問題があるため、作成するアカウントの数を制限することを推奨します。

- ゲストへの複数のゲストアカウントの割り当て (ランダム) (Multiple guest accounts to be assigned to any guests (Random)) : スポンサーが、未知のゲストのプレースホルダとして、または複数のアカウントをすばやく作成する必要がある場合に複数のランダムゲストアカウントを作成できるようにします。

このオプションが有効である場合、[ランダム (Random)] ボタンがスポンサーポータルの [アカウントの作成 (Create Accounts)] ページに表示されます。

- デフォルトユーザ名プレフィックス (Default username prefix) : スポンサーが複数のランダムなゲストアカウントを作成する場合に使用できるユーザ名プレフィックスを指定します。指定した場合、このプレフィックスはランダムなゲストアカウントを作成するときにスポンサーポータルに表示されます。また、[スポンサーにユーザ名プレフィックスの指定を許可 (Allow sponsor to specify a username prefix)] の設定により、次のようになります。

- 有効 : スポンサーは、スポンサーポータルでデフォルトのプレフィックスを編集できます。
- 無効 : スポンサーは、スポンサーポータルでデフォルトのプレフィックスを編集できません。

ユーザ名プレフィックスを指定しないか、またはスポンサーにユーザ名プレフィックスの指定を許可しない場合、スポンサーはスポンサーポータルでユーザ名プレフィックスを割り当てることができません。

- スポンサーにユーザ名プレフィックスの指定を許可 (Allow sponsor to specify a username prefix) : このスポンサーグループが複数のアカウントを同時に作成できる場合、単一のインポート操作で作成可能なゲストアカウントの数を指定します。

スポンサーは最大 10,000 個のアカウントを作成できますが、潜在的なパフォーマンスの問題があるため、作成するアカウントの数を制限することを推奨します。

- 開始日を\_\_日後より遅くすることはできない (Start date can be no more than \_\_ days into the future) : 有効にして日数を指定すると、作成した複数のゲストアカウントの開始日をこの日数以内に設定する必要があります。

### スポンサーが管理可能 (Sponsor Can Manage)

- スポンサーが作成したアカウントのみ (Only accounts sponsor has created) : このグループのスポンサーは、スポンサーの電子メールアカウントに基づいて、スポンサーが作成したゲストアカウントのみを表示および管理できます。
- このスポンサーグループのメンバーによって作成されたアカウント (Accounts created by members of this sponsor group) : このグループのスポンサーは、このスポンサーグループ内のスポンサーが作成したゲストアカウントを表示および管理できます。
- すべてのゲストアカウント (All guest accounts) : スポンサーはすべての保留中のゲストアカウントを表示および管理できます。



- (注) [アカウント登録ゲストからの要求の承認および表示 (Approve and view requests from self-registering guests)] にマークを付けて、[スポンサーが可能 (Sponsor Can)] の下で [このスポンサーに割り当てられた保留中のアカウントのみ (Only pending accounts assigned to this sponsor)] オプションを使用していない限り、グループメンバーシップにかかわらず、すべてのスポンサーがすべての保留中のアカウントを表示できます。

### スポンサーが可能 (Sponsor Can)

- ゲストの連絡先情報 (電子メール、電話番号) の更新 (Update guests' contact information (email, Phone Number)) : スポンサーは、自分が管理できるゲストアカウントについて、ゲストの連絡先情報を変更できます。
- ゲストのパスワードの表示/印刷 (View/print guests' passwords) : これをオンにすると、スポンサーはゲストのパスワードを印刷することができます。スポンサーは [アカウントの管理 (Manage Accounts)] ページおよびゲストの詳細で、ゲストのパスワードを表示できます。これがオフの場合、スポンサーはパスワードを印刷できませんが、ユーザは電子メールまたは SMS (設定済みの場合) を介してパスワードを取得できます。



- ゲストのクレデンシャルを含む SMS 通知の送信 (Send SMS notifications with guests' credentials) : スポンサーは、自分が管理できるゲストアカウントについて、アカウントの詳細とログインクレデンシャルとともにゲストに SMS (テキスト) 通知を送信できます。
  - ゲストアカウントパスワードのリセット (Reset guest account passwords) : スポンサーは、自分が管理できるゲストアカウントについて、そのパスワードを Cisco ISE によって生成されたランダムなパスワードにリセットできます。
  - ゲストのアカウントの延長 (Extend guests' accounts) : スポンサーは、自分が管理できるゲストアカウントについて、その有効期限を延長できます。スポンサーは、アカウントの有効期限に関してゲストに送信される電子メール通知に自動的にコピーされます。
  - ゲストのアカウントの削除 (Delete guests' accounts) : スポンサーは、自分が管理できるゲストアカウントについて、アカウントを削除し、ゲストが企業のネットワークにアクセスすることを防ぐことができます。
  - ゲストのアカウントの一時停止 (Suspend guests' accounts) : スポンサーは、自分が管理できるゲストアカウントについて、アカウントを一時停止してゲストが一時的にログインすることを防ぐことができます。
- また、このアクションは、許可変更 (CoA) 終了を発行して、一時停止されていたゲストをネットワークから排除できます。
- スポンサーに理由の入力を求める (Require sponsor to provide a reason) : ゲストアカウントの一時停止に対する説明の入力をスポンサーに求めます。
- アカウント登録ゲストからの要求の承認および表示 (Approve and view requests from self-registering guests) : このスポンサーグループに含まれているスポンサーは、(承認が必要な) アカウント登録ゲストからのすべての保留中のアカウント要求を表示するか、アクセス先の担当者としてユーザがスポンサーの電子メールアドレスを入力した要求のみを表示できます。この機能では、アカウント登録ゲストによって使用されるポータルで [アカウント登録ゲストが承認される必要がある (Require self-registered guests to be approved)] にマークが付けられていて、スポンサーの電子メールが連絡先の担当者としてリストされている必要があります。
    - [保留中のすべてのアカウント (Any pending accounts)] : このグループに所属するスポンサーは、他のスポンサーによって作成されたアカウントを承認およびレビューします。
    - [このスポンサーに割り当てられている保留中のアカウントのみ (Only pending accounts assigned to this sponsor)] : このグループに所属するスポンサーは、スポンサー自身が作成したアカウントだけを表示および承認できます。
  - プログラムによるインターフェイス (Guest REST API) を使用した Cisco ISE ゲストアカウントへのアクセス (Access Cisco ISE guest accounts using the programmatic interface (Guest REST API)) : スポンサーは、自分が管理できるゲストアカウントについて、Guest REST API プログラミングインターフェイスを使用してゲストアカウントにアクセスできます。

