



ゲストおよびセキュア Wi-Fi

- [Cisco ISE ゲスト サービス \(1 ページ\)](#)
- [ゲスト アカウントとスポンサー アカウント \(2 ページ\)](#)
- [ゲスト ポータル \(22 ページ\)](#)
- [スポンサー ポータル \(37 ページ\)](#)
- [ゲストとスポンサーのアクティビティのモニター \(55 ページ\)](#)
- [ゲスト アクセス Web 認証オプション \(57 ページ\)](#)
- [ゲスト ポータル設定 \(65 ページ\)](#)
- [スポンサー ポータル アプリケーションの設定 \(88 ページ\)](#)
- [ゲストおよびスポンサー ポータルのグローバル設定 \(97 ページ\)](#)
- [ゲスト タイプの設定 \(98 ページ\)](#)
- [スポンサー グループ設定 \(101 ページ\)](#)
- [エンドユーザー ポータル \(105 ページ\)](#)
- [エンドユーザー Web ポータルのカスタマイズ \(106 ページ\)](#)
- [ポータル コンテンツのタイプ \(108 ページ\)](#)
- [ポータルの基本的なカスタマイズ \(108 ページ\)](#)
- [ポータルの高度なカスタマイズ \(119 ページ\)](#)
- [ポータル言語のカスタマイズ \(140 ページ\)](#)
- [ゲスト通知、承認、およびエラー メッセージのカスタマイズ \(144 ページ\)](#)
- [ポータル ページのタイトル、コンテンツおよびラベルの文字数制限 \(149 ページ\)](#)
- [ポータルのカスタマイズ \(152 ページ\)](#)
- [ポータル言語ファイルの HTML サポート \(153 ページ\)](#)

Cisco ISE ゲスト サービス

Cisco Identity Services Engine (Cisco ISE) のゲストサービスを使用すると、ビジター、請負業者、コンサルタント、顧客などのゲストにセキュアなネットワークアクセスを提供することができます。Cisco ISE の基本ライセンスを持つゲストをサポートでき、会社のインフラストラクチャと機能の要件に応じて複数の展開オプションから選択できます。

Cisco ISE は、企業のネットワークおよび内部リソースとサービスへのゲストおよび従業員のオンボーディングを行う Web ベースのモバイル ポータルを提供します。

管理者ポータルで、ゲスト ポータルおよびスポンサー ポータルの作成と編集、ゲスト タイプの定義によるゲストアクセス権限の設定、ゲストアカウントの作成と管理のためのスポンサー権限の割り当てを行うことができます。

- [ゲスト ポータル \(22 ページ\)](#)
- [ゲスト タイプおよびユーザー ID グループ \(3 ページ\)](#)
- [スポンサー ポータル \(37 ページ\)](#)
- [スポンサー グループ \(39 ページ\)](#)

ISE コミュニティ リソース

ISE ゲストと Web 認証に関する ISE コミュニティリソースのリストについては、「[ISE Guest Access - ISE Guest and Web Authentication.](#)」を参照してください。

分散環境のエンドユーザーのゲスト ポータルとスポンサー ポータル

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

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

ゲスト アカウントとスポンサー アカウント

- **ゲストアカウント**: ゲストとは、通常、ネットワークへの一時アクセスを必要とする承認ユーザー、担当者、顧客、その他のユーザーを表します。いずれかのゲスト展開シナリオを使用して、従業員のネットワーク アクセスを許可する場合は、従業員用のゲストアカ

アカウントを使用することもできます。スポンサーポータルにアクセスして、スポンサーおよびアカウント登録ゲストによって作成されたゲストアカウントを表示できます。

- **スポンサーアカウント**：[スポンサー (Sponsor)]ポータルを使用して、承認ユーザー用の一時アカウントを作成し、企業ネットワークまたはインターネットにセキュアにアクセスできるようにします。ゲストアカウントを作成した後、スポンサーポータルを使用してそれらのアカウントを管理し、ゲストにアカウントの詳細を提供できます。

次のユーザーがゲストアカウントを作成できます。

- **スポンサー**：管理者ポータルで、ゲストアカウントを作成し管理する[スポンサー (Sponsor)]ポータルにアクセスできる、スポンサーのアクセス権限と機能のサポートを定義できます。
- **ゲスト**：ゲストは、アカウント登録ゲストポータルに自分自身を登録することによって、独自のアカウントを作成することもできます。これらのアカウント登録ゲストは、ポータル設定に基づいて、ログインクレデンシャルを受け取る前にスポンサーの承認が必要になる場合があります。

ゲストは、ホットスポットゲストポータルを使用してネットワークにアクセスすることもできます。このポータルでは、ゲストアカウントやユーザー名およびパスワードなどのログインクレデンシャルを作成する必要はありません。
- **従業員**：ID ストア (Active Directory、LDAP、内部ユーザーなど) に含まれている従業員は、クレデンシャルを持つゲストポータル (Sponsored-Guestポータルおよびアカウント登録ゲストポータル) が設定されている場合には、これを使用してアクセスすることもできます。

Bring Your Own Device (BYOD; 個人所有デバイス持ち込み) ワークフローを通じてオンボーディングされたデバイスは、ゲストデバイスとして扱われず、設定されているエンドポイント ID グループは変更されません。Bring Your Own Device (BYOD) の詳細については、「[個人所有デバイスの持ち込み \(BYOD\)](#)」を参照してください。

ゲストアカウントが作成されると、ゲストは Sponsored-Guestポータルを使用してネットワークにログインおよびアクセスできます。

ゲストタイプおよびユーザー ID グループ

各ゲストアカウントをゲストタイプに関連付ける必要があります。ゲストタイプを使用して、スポンサーは、ゲストアカウントに対して、さまざまなレベルのアクセス権や、さまざまなネットワーク接続時間を割り当てることができます。これらのゲストタイプは、特定のネットワークアクセスポリシーに関連付けられます。Cisco ISE には、次のデフォルトゲストタイプが含まれます。

- [担当者 (Contractor)]：長期間 (最大1年) にわたってネットワークへのアクセスを必要とするユーザー。
- [毎日 (Daily)]：1～5日間の短期間に、ネットワーク上のリソースへのアクセスを必要とするゲスト。

- [毎週 (Weekly)] : 2 ~ 3 週間の間、ネットワークへのアクセスを必要とするユーザー。

ゲストアカウントを作成する場合、特定のスポンサー グループを特定のゲストタイプを使用するように制限することができます。このようなグループのメンバーは、そのゲストタイプに指定された機能のみを持つゲストを作成できます。たとえば、スポンサー グループ ALL_ACCOUNTS は担当者ゲストタイプのみを使用するように設定でき、スポンサー グループ OWN_ACCOUNTS および GROUP_ACCOUNTS は日次または週次ゲストタイプを使用するように設定できます。通常、アカウント登録ゲストポータルを使用するアカウント登録ゲストは、1日のみのアクセスを必要とするため、これらのゲストには[毎日 (Daily)]のゲストタイプを割り当てることができます。

ゲストタイプは、ゲストのユーザー ID グループを定義します。

詳細については、以下を参照してください。

- [ユーザー ID グループ](#)
- [ユーザー ID グループの作成](#)

ゲストタイプの作成または編集

デフォルトのゲストタイプとデフォルトのアクセス権限や設定を編集できます。または、新しいゲストタイプを作成できます。ユーザーが行う変更は、この特定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適用されます。ログインしているゲストユーザーには、ログアウトして再度ログインするまで、これらの変更はわかりません。また、ゲストタイプを複製して、同じアクセス権限を持つゲストタイプを追加で作成することもできます。

各ゲストタイプに名前、説明、およびこのゲストタイプでゲストアカウントを作成できるスポンサーグループのリストがあります。ゲストタイプに対して、アカウント登録ゲストにのみ使用すること、(任意のスポンサーグループによる) ゲストアカウントの作成には使用しないこと、などを指定できます。

下記で説明するフィールドに入力します。

これら設定のナビゲーションパスは、[ゲストアクセス (Guest Access)] > [設定 (Configure)] > [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、ゲストタイプを作成できるスポンサーグループを指定できます。

フィールド名	使用上のガイドライン
ゲストタイプ名 (Guest type name)	デフォルトのゲストタイプおよび作成した別のタイプと区別できるこのゲストタイプの名前を入力します (1 ~ 256 文字)。

フィールド名	使用上のガイドライン
説明	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）を入力します（「アカウント登録ゲストに使用」、「ゲストアカウントの作成に使用禁止」など）。
言語ファイル（Language File）	このゲストタイプを使用してポータルに使用する言語ファイルをエクスポートまたはインポートします。
追加データの収集（Collect Additional Data）	<p>ゲストの追加情報を収集するにはカスタムフィールドを選択します。</p> <p>カスタムフィールドは、[ゲストアクセス（Guest Access）]>[設定（Settings）]>[カスタムフィールド（Custom Fields）]で管理されます。</p>
最大アクセス時間—アカウント有効期間の開始（Maximum Access Time—Account Duration Starts）	<p>[最初のログインから（From first login）]：アカウントの開始時刻は、ゲストユーザー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、終了時刻は指定された期間に相当します。ゲストユーザーはログインしなければ、アカウントがゲストアカウントの消去ポリシーによって削除されるまで、アカウントは初回ログイン待ち状態のままになります。アカウント登録されたり、スポンサーが作成したりしたユーザーアカウントは、ゲストユーザーがアカウントを作成してそのアカウントにログインしたときから開始となります。</p> <p>(注) [Allow access only on these days and times] を選択すると、ロケーションを使用して、これらの時間のコンテキストを確立します。[From First Login] アクセスがロケーションに基づかないようにするには、アクセス用の日付と時刻を設定しないでください。</p> <p>[From sponsor-specified date]：このゲストタイプのゲストがアクセスでき、ネットワークに接続され続けることができる、最大の日数、時間または分を 1 ~ 999 で指定します。</p> <p>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。</p>

フィールド名	使用上のガイドライン
<p>これらの曜日および時間のみアクセスを許可 (Allow access only on these days and times)</p>	<p>時間範囲を入力し、曜日を選択して、このゲストタイプがいつネットワークにアクセスできるかを指定します。このゲストタイプがこれらの時間パラメータを超えて接続を維持している場合、ログアウトされます。時間範囲は、このゲストタイプを使用してゲストに割り当てられた場所で定義されたタイムゾーンに基づきます。</p> <p>+ または - をクリックして、アクセス時間制限を増減します。</p>
<p>ゲストアカウントの消去ポリシーの設定 (Configure guest account Purge Policy)</p>	<p>エンドポイント消去ジョブをスケジュールできます。エンドポイントの消去スケジュールはデフォルトで有効になっており、Cisco ISE は 30 日以上経過したエンドポイントを削除します。詳細については、エンドポイントの消去の設定を参照してください。</p>
<p>ログイン オプション—最大同時ログイン数 (Login Options—Maximum simultaneous logins)</p>	<p>このゲストタイプが同時に実行できる最大ユーザーセッション数を入力します。</p>
<p>ゲストが制限を超えた場合 (When guest exceeds limit)</p>	<p>[最大同時ログイン数 (Maximum simultaneous logins)] を選択した場合は、その制限に到達した後にユーザー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。</p> <p>ゲストが制限を超えた場合：</p> <ul style="list-style-type: none"> • 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) • [Redirect user to a portal page showing an error message]：設定可能な期間、エラーメッセージが表示されます。その後、セッションが切断され、ユーザーはゲストポータルにリダイレクトされます。エラーページの内容は、[Messages] > [Error Messages] タブの [Portal Page Customization] ダイアログボックスで設定します。

フィールド名	使用上のガイドライン
<p>ゲストが登録可能な最大デバイス数 (Maximum devices guests can register)</p>	<p>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。</p> <p>ゲストユーザーが登録できるデバイスの最大数に達すると、次のいずれかの方法で続行できることを通知する通知が表示されます。</p> <ul style="list-style-type: none"> • デバイスリストから削除する登録済みデバイスを選択し、新しいデバイスを追加します。 • 新しいデバイスの登録に進みます。このシナリオでは、リストにある最も古い登録済みデバイスが自動的に登録解除されます。
<p>ゲストにゲストポータルをバイパスを許可する (Allow guest to bypass the Guest portal)</p>	<p>クレデンシャルを持つゲスト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ーに許可します。ゲストアカウントは、[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。</p> <p>この設定を有効にしない場合、ユーザー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。</p>
<p>アカウント期限切れ通知—アカウント期限切れの__日前にアカウント期限切れ通知を送信する (Account Expiration Notification—Send account expiration notification __ days before account expires)</p>	<p>ゲストの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。期限切れの何日前、何時間前、または何分前に通知するかを指定します。</p>
<p>メッセージの表示言語 (View messages in)</p>	<p>電子メールまたは SMS 通知の表示言語を指定します。</p>
<p>E メール</p>	<p>アカウントの失効通知に使用する手段としてメールを選択します。</p>
<p>次のカスタマイズを使用 (Use customization from)</p>	<p>別のポータルから電子メールのカスタマイズを選択します。</p>
<p>メッセージ</p>	<p>アカウントの有効期限通知に使用するテキストを入力します。</p>

フィールド名	使用上のガイドライン
テキストのコピー元 (Copy text from)	アカウントの期限切れ通知のために別のゲストタイプ用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)	自分の電子メール アドレスに送信することによって、電子メール通知が意図したとおりに表示されることを確認します。
SMS	アカウントの失効通知に使用する手段としてテキスト (SMS) を選択します。
メッセージ	アカウントの有効期限通知に使用するテキストを入力します。
テキストのコピー元 (Copy text from)	別のゲストタイプ用に作成したテキスト メッセージを再使用します。
テスト SMS の送信先 (Send test SMS to me at)	自分の携帯電話に送信することによって、テキスト通知が意図したとおりに表示されることを確認します。
これらのスポンサー グループはこのゲストタイプを作成できる (These sponsor groups can create this guest type)	このゲストタイプでゲストアカウントを作成できるスポンサーグループを選択します。 このゲストタイプの使用を無効にする場合は、いずれのスポンサーグループにも割り当てないでください。このゲストタイプの使用を中止するには、リストされたスポンサーグループを削除します。

次のタスク

- このゲストタイプを使用するスポンサーグループを作成または変更します。
- 該当する場合は、アカウント登録ゲストポータルで、このゲストタイプをアカウント登録ゲストに割り当てます。

ゲストタイプの無効化

ゲストアカウントで使用されているゲストタイプのうち、最後に残ったゲストタイプは削除できません。使用されているゲストタイプを削除するには、最初にそのゲストタイプが使用できなくなることを確認します。ゲストタイプをディセーブルにしても、そのゲストタイプで作成したゲストアカウントには影響しません。

次の手順で、ターゲットゲストタイプを準備および無効にする方法を説明します。

-
- ステップ 1** ターゲットゲストタイプを使用して、スポンサーがゲストを作成するのを許可しているスポンサーグループを識別します。[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [設定 (Configure)] > [ポータルとコンポーネント (Portals and Components)] > [スポンサーグループ (Sponsor Groups)] を選択し、各スポンサーグループを開いて、[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できます (This sponsor group can create accounts using these guest types)] リストを調べます。
- ステップ 2** ターゲットゲストタイプを割り当てるアカウント登録ポータルを識別します。[ワークセンター (Work Center)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲストポータル (Guest Portals)] を選択します。各アカウント登録ゲストポータルを開きます。ポータルが特定のゲストタイプを使用している場合、[Portal Settings] を展開し、[Employees using this portal as guests inherit login options from:] フィールドに割り当てられたゲストタイプを変更します。
- ステップ 3** 削除するゲストタイプを開き、前の手順で識別したすべてのスポンサーグループを削除します。この操作により、効果的に、すべてのスポンサーがこのゲストタイプの新しいゲストアカウントの作成を使用できなくなります。[ワークセンター (Work Center)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals and Components)] > [ゲストタイプ (Guest Type)] を選択します。
-

エンドポイントユーザーの最大同時ログイン数の設定

ゲストに許可される同時ログインの最大数を設定できます。

ユーザーがゲストポータルにログインし、正常に認証されると、ユーザーがすでにログインの最大数に達しているかどうかを確認するために、ユーザーの既存のログイン数がチェックされます。その場合、ゲストユーザーはエラーページにリダイレクトされます。エラーページが表示され、セッションが停止します。そのユーザーがインターネットに再度アクセスしようとすると、ユーザーの接続はゲストポータルのログインページにリダイレクトされます。

始める前に

このポータルの許可ポリシーで使用している許可プロファイルで [アクセスタイプ (Access Type)] が *Access_Accept* に設定されていることを確認します。[アクセスタイプ (Access Type)] が *Access_Reject* に設定されている場合は、最大同時ログイン数は機能しません。

-
- ステップ 1**
- [最大同時ログイン数 (Maximum simultaneous logins)] チェックボックスをオンにして、許可される同時ログインの最大数を入力します。
 - [ゲストが制限を超えた場合 (When guest exceeds limit)] の下で、[最も新しい接続を切断 (Disconnect the newest connection)] オプションをクリックします。
 - [エラーメッセージを表示するポータルページにユーザーをリダイレクトする (Redirect user to a portal page showing an error message)] チェックボックスをオンにします
- ステップ 2**
- [共通タスク (Common Tasks)] で、[Web リダイレクション (Web Redirection)] をオンにし、次の手順を実行します。
 - 最初のドロップダウンで、[中央集中Web認証 (Centralized Web Auth)] を選択します。

- 前提条件の一部として作成した **ACL** を入力します。
 - [値 (Value)] の場合、リダイレクト先のゲスト ポータルを選択します。
- b) [共通タスク (Common Tasks)] で下にスクロールし、[再認証 (Reauthentication)] チェックボックスをオンにして、次の手順を実行します。
- [タイマー (Timer)] に、ユーザーがゲストポータルにリダイレクトされる前にエラーページが表示される時間を入力します。
 - [再認証中に接続を維持 (Maintain Connectivity During Reauthentication)] で、[デフォルト (Default)] を選択します。

ステップ 3 [ポリシー (Policy)] > [ポリシーセット (Policy Sets)] を選択して、属性 `NetworkAccess.SessionLimitExceeded` が `true` の場合にユーザーがポータルにリダイレクトされるように、許可ポリシーを作成します。

次のタスク

[ポータルページのカスタマイズ (Portal Page Customization)] タブでエラーページのテキストをカスタマイズできます。[メッセージ (Messages)] > [エラーメッセージ (Error Messages)] を選択し、エラーメッセージキー `ui_max_login_sessions_exceeded_error` のテキストを変更します。

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

アクティブなまたは一時停止されたゲストアカウントがアカウント有効期間（スポンサーがアカウントを作成するときに定義）の終了に達すると、そのアカウントは失効します。ゲストアカウントが期限切れになった場合、影響を受けるゲストはネットワークにアクセスできません。スポンサーは、期限切れになったアカウントを、消去される前に延長することができます。ただし、アカウントが消去された場合、スポンサーは、新しいアカウントを作成する必要があります。

期限切れになったゲストアカウントが消去された場合、関連するエンドポイントおよびレポート情報とログイン情報は保持されます。

Cisco ISE は、デフォルトで 15 日ごとに期限切れになったゲストアカウントを自動的に消去します。[次回消去日 (Date of next purge)] は、次の消去の発生時期を示します。次のことも実行できます。

- X 日ごとに消去が行われるようにスケジュール設定します。最初の消去は X 日後の **消去の時刻** に行われ、その後消去は X 日ごとに行われます。
- X 週間ごとに特定の曜日に消去が行われるようにスケジュール設定します。最初の消去は次のその曜日の **消去の時刻** に行われ、その後消去は設定された週数おきにその曜日と時刻に行われます。たとえば、月曜日に、5 週間おきに木曜日に消去が行われるように設定したとします。次の消去は、今から 5 週間後の木曜日ではなく、その週の木曜日に行われます。

- [今すぐ消去 (Purge Now)] をクリックして、ただちに消去を行います。

消去が実行されるようにスケジュールされているときに Cisco ISE サーバーがダウンした場合は、消去は行われません。消去プロセスは、サーバーがその時点で動作していれば、次にスケジュールされている消去時刻に再度実行されます。

ステップ 1 [ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [設定 (Settings)] > [ゲストアカウント消去ポリシー (Guest Account Purge Policy)] を選択します。

ステップ 2

ステップ 3 次のオプションのいずれかを選択します。

- 期限切れのゲスト アカウント レコードを即時に消去するには、[今すぐ消去 (Purge Now)] をクリックします。
- 消去をスケジュールするには、[期限切れのゲスト アカウントの消去のスケジュール (Schedule purge of expired guest accounts)] をオンにします。

(注) 各消去の完了後に、[次回消去日 (Date of next purge)] が次にスケジュールされている消去に合わせてリセットされます。

ステップ 4 [経過後にポータルユーザー情報を期限切れにする (Expire portal-user information after)] で、ユーザーを期限切れにするための非アクティブ日数を指定します。この設定により、使用されていない LDAP および Active Directory アカウントが ISE データベースに無期限に残ることを防ぎます。

最初のログインが行われない場合、指定された期間の終了時にゲストアカウントが期限切れ状態になり、設定された消去ポリシーに基づいて消去されます。

また、期限切れになったゲストアカウントを消去する必要がある頻度 (日数または週数) を指定することもできます。[_ 週ごとに消去 (Purge occurs every _ weeks)] オプションを選択した場合は、期限切れのアカウントを消去する日時も指定できます。

ステップ 5 [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。

ゲスト アカウント作成用のカスタム フィールドの追加

ゲスト アクセスを提供する場合、名前、電子メールアドレス、電話番号以外の情報をゲストから収集する必要がある場合があります。Cisco ISE には、会社のニーズに固有の、ゲストに関する追加情報の収集に使用できるカスタム フィールドが用意されています。ゲスト タイプ およびアカウント登録ゲスト ポータルとスポンサー ポータルにカスタム フィールドを関連付けることができます。Cisco ISE はデフォルトのカスタム フィールドを提供しません。

次のタスク

目的のカスタム フィールドを含めることが可能です。

- そのゲスト タイプで作成されたアカウントにこの情報が含まれるようにゲスト タイプを定義する場合。「[ゲスト タイプの作成または編集](#)」を参照してください。
- ゲストアカウントの作成時にスポンサーが使用するスポンサーポータルを設定する場合。[スポンサーポータルのカスタマイズ \(50 ページ\)](#) を参照してください。
- アカウント登録ゲストポータルを使用してアカウント登録ゲストからの情報を要求する場合。[アカウント登録ゲストポータルの作成 \(32 ページ\)](#) を参照してください。

電子メールでの通知用の電子メールアドレスおよび SMTP サーバーの指定

Cisco ISE では、スポンサーおよびゲストに、情報と手順を通知する電子メールを送信できます。これらの電子メールでの通知を配信するように SMTP サーバーを設定できます。また、ゲストに通知を送信する電子メールアドレスを指定できます。



(注) ゲスト通知には、UTF-8 に互換性がある電子メールクライアントが必要です。

シングルクリックスポンサーの承認機能を使用するには、HTML 対応の電子メールクライアント（機能を有効にする）が必要です。

ゲストのロケーションおよび SSID の割り当て

ゲストロケーションはタイムゾーンの名前を定義し、ゲストにログインした時間関連設定を適用するために ISE によって使用されます。ゲストロケーションは、ゲストアカウントを作成するスポンサー、およびアカウント登録ゲストによってゲストアカウントに割り当てられます。デフォルトのゲストロケーションは San Jose です。他のゲストロケーションが追加されていない場合、すべてのアカウントにこのゲストロケーションが割り当てられます。1つ以上の新しいロケーションを作成しないと、San Jose のゲストロケーションは削除できません。すべてのゲストが San Jose と同じタイムゾーンにいる場合を除き、必要なタイムゾーンで少なくとも1つのゲストロケーションを作成します。



(注) ゲストアクセスの時間は、ゲストロケーションのタイムゾーンに基づきます。ゲストロケーションのタイムゾーンがシステムのタイムゾーンと一致しないと、ゲストユーザーはログインできなくなることがあります。この場合、ゲストユーザーには「認証に失敗しました (Authentication Failed)」エラーが表示されることがあります。デバッグレポートに「ゲストのアクティブ時間はまだ開始していません (Guest active time period not yet started)」というエラーメッセージが表示されることがあります。回避策として、[アカウントの管理 (Manage Accounts)] オプションを使用して、ゲストユーザーのローカルタイムゾーンに一致するようにゲストのアクセス開始時刻を調整できます。

ここで追加する SSID はスポンサー ポータルで使用できるため、スポンサーは接続する SSID をゲストに伝えることができます。

ゲスト ロケーションまたは SSID がスポンサー ポータルで設定されている場合、またはゲスト アカウントに割り当てられている場合は、削除できません。

ステップ 1 ゲストポータルおよびスポンサーポータルのゲストロケーションと SSID を追加、編集、または削除するには、[ワークセンター (Work Centers)] > [ポータルとコンポーネント (Portals & Components)] > [設定 (Settings)] > [ゲストロケーションおよび SSID (Guest Locations and SSIDs)] を選択します。

ステップ 2

ステップ 3 [ゲスト ロケーション (Guest Locations)] :

- a) サポートが必要な各タイムゾーンに対し、[ロケーション名 (Location name)] に入力し、ドロップダウンリストから [タイムゾーン (Time zone)] を選択します。
- b) [追加 (Add)] をクリックします。

(注) ゲスト ロケーションでは、場所の名前、タイムゾーンの名前、および GMT オフセットはスタティックであり、これらを変更できません。GMT オフセットは夏時間の変更によって変更されません。GMT オフセットは、リストに表示されているオフセットとは逆です。たとえば、*Etc/GMT+3* は実際には GMT-3 です。

(注) 初回ログインのゲスト タイプの場合、[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)] ページでアクセス時間制限を設定する場合にのみ、ゲスト ロケーション (タイムゾーン) を設定することを確認してください。

ステップ 4 [ゲスト SSID (Guest SSIDs)] :

- a) ゲスト ロケーションでゲストが使用できるネットワークの **SSID** 名を入力します。
- b) [Add] をクリックします。

ステップ 5 [Save] をクリックします。最後に保存した値に戻すには、[リセット (Reset)] をクリックします。

次のタスク

新しいゲスト ロケーションまたは SSID を追加すると、次のことが可能になります。

- スポンサーがゲストアカウントを作成するときに使用できる SSID を提供します。 [スポンサーポータルのポータル設定 \(89 ページ\)](#) を参照してください。
- スポンサーグループにゲストロケーションを追加して、ゲストアカウントの作成時にそのグループに割り当てられたスポンサーが使用できるようにします。 [スポンサーグループの設定 \(41 ページ\)](#) を参照してください。
- アカウント登録ゲストポータルを使用してアカウント登録ゲストに使用可能なゲストロケーションを割り当てます。 [アカウント登録ゲストポータルの作成 \(32 ページ\)](#) を参照してください。

- 既存のゲストアカウントの場合は、アカウントを手動で編集して SSID またはロケーションを追加します。

ゲストパスワードポリシーのルール

Cisco ISE には、ゲストユーザーパスワードについて次の組み込みルールがあります。

- ゲストパスワードポリシーは、スポンサーポータル、アカウント登録ポータル、CSV ファイルでアップロードされたアカウント、ERS API を使用して作成されたパスワード、およびユーザーが作成したパスワードに適用されます。
- ゲストパスワードポリシーに対する変更は、ゲストパスワードの期限が切れて変更が必要になるまで、既存のアカウントに影響しません。
- パスワードは大文字・小文字の区別をします。(Unable to authenticate using the domain name, user name, and password that you specified. Please check the values that you entered and try again. Passwords are case sensitive.)」
- 特殊文字 (<, >, /, スペース, カンマ, %) を使用することはできません。
- 最小長および最小必須文字数は、すべてのパスワードに適用されます。
- パスワードとユーザー名を同じにすることはできません。
- 新規パスワードと既存パスワードを同じにすることはできません。
- ゲストアカウントの期限切れとは異なり、ゲストはパスワードが期限切れになる前に通知を受信しません。ゲストパスワードが期限切れになった場合は、スポンサーがパスワードをランダムパスワードにリセットするか、ゲストが現在のログインクレデンシャルを使用してログインしてからパスワードを変更することができます。



(注) ゲストのデフォルトユーザー名は4文字の英字からなり、パスワードは4文字の数字からなります。短期間のゲストには、短く覚えやすいユーザー名とパスワードが適切です。必要に応じて ISE でユーザー名とパスワードの長さを変更できます。

ゲストパスワードポリシーと有効期限の設定

すべてのゲストポータルのパスワードポリシーを定義できます。ゲストパスワードポリシーは、すべてのゲストアカウントのパスワードの生成方法を決定します。パスワードはアルファベット、数字、特殊文字を組み合わせて作成することができます。また、ゲストパスワードが期限切れになるまでの日数を設定し、ゲストにパスワードのリセットを要求することができます。

ゲストパスワードポリシーは、スポンサーポータル、アカウント登録ポータル、CSV ファイルでアップロードされたアカウント、ERS API を使用して作成されたパスワード、およびユーザーが作成したパスワードに適用されます。

次のタスク

パスワード要件を提示するためのパスワードポリシーに関連したエラーメッセージをカスタマイズする必要があります。

1. [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [Sponsored-Guest ポータル (Sponsored-Guest Portals)] または [アカウント登録ゲストポータル (Self-Registered Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > [エラーメッセージ (Error Messages)] を選択します。
2. キーワード policy を検索します。

ゲスト ユーザー名ポリシーのルール

Cisco ISE には、ゲスト ユーザー名ポリシーについて次の組み込みルールがあります。

- ゲスト ユーザー名ポリシーに対する変更は、ゲスト アカウントの期限が切れて変更が必要になるまで、既存のアカウントに影響しません。
- 特殊文字 (<, >, /, スペース, カンマ, %) を使用することはできません。
- 最小長および最小必須文字数は、電子メールアドレスに基づいたユーザー名を含め、すべてのシステム生成ユーザー名に適用されます。
- パスワードとユーザー名を同じにすることはできません。

ゲスト ユーザー名ポリシーの設定

ゲストユーザー名の作成方法に関するルールを設定できます。生成されるユーザー名は、電子メールアドレスに基づいて、またはゲストの姓と名に基づいて作成できます。またスポンサーは、ランダムな数のゲストアカウントを作成し、複数のゲストを作成する場合、またはゲストの名前と電子メールアドレスが利用できない場合に時間を短縮することもできます。ランダムに生成されたゲストユーザー名は、アルファベット、数字、および特殊文字の組み合わせから成ります。これらの設定は、すべてのゲストに影響します。

次のタスク

ユーザー名要件を提示するためのユーザー名ポリシーに関連したエラーメッセージをカスタマイズする必要があります。

1. [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)] > [Sponsored-Guest ポータル (Sponsored-Guest Portal)]、[アカウント登録ゲストポータル (Self-Registered Guest Portals)]、[スポンサーポータル (Sponsor Portals)]、または [デバイスポータル (My Devices Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > [エラーメッセージ (Error Messages)] の順に選択します。
2. キーワード policy を検索します。

SMS プロバイダおよびサービス

SMS サービスは、クレデンシャルを持つゲスト ポータルを使用しているゲストに SMS 通知を送信します。SMS メッセージを送信する予定がある場合は、このサービスを有効にします。可能な限り、会社の経費を削減するために、無料の SMS サービス プロバイダを設定および提供します。

Cisco ISE は、加入者に無料の SMS サービスを提供するさまざまなセルラー サービス プロバイダをサポートします。Cisco ISE でサービス契約とアカウント クレデンシャルを設定せずに、これらのプロバイダを使用できます。セルラー サービス プロバイダには、ATT、Orange、Sprint、T-Mobile、Verizon があります。

また、無料の SMS サービスを提供するその他のセルラー サービス プロバイダ、または Click-A-Tell などのグローバル SMS サービス プロバイダも追加できます。デフォルトのグローバル SMS サービス プロバイダには、サービス契約が必要です。また、Cisco ISE のアカウント クレデンシャルを設定する必要があります。

- アカウント登録ゲストがアカウント登録フォームで無料 SMS サービス プロバイダを選択すると、SMS 通知がログイン クレデンシャルとともに無料で送信されます。SMS サービス プロバイダを選択しない場合は、会社が契約したデフォルトのグローバル SMS サービス プロバイダが SMS 通知を送信します。
- 自分が作成したゲスト アカウントに対してスポンサーが SMS 通知を送信できるようにする場合は、スポンサー ポータルをカスタマイズして、使用できる適切な SMS サービス プロバイダをすべて選択します。スポンサー ポータル用の SMS サービス プロバイダを選択しない場合は、会社が契約したデフォルトのグローバル SMS サービス プロバイダが SMS サービスを提供します。

SMS プロバイダは、Cisco ISE の SMS ゲートウェイとして設定されます。Cisco ISE からの電子メールは SMS ゲートウェイにより SMS に変換されます。SMS ゲートウェイはプロキシ サーバーの背後に配置できます。

ゲストに SMS 通知を送信するための SMS ゲートウェイの設定

次のことができるようにするには、Cisco ISE で SMS ゲートウェイを設定する必要があります。

- ログイン クレデンシャルおよびパスワードリセット手順に関する SMS 通知をスポンサーがゲストに手動で送信します。
- ゲストが、自分自身の登録に成功した後、自分のログイン資格情報が含まれた SMS 通知を自動的に受信します。
- ゲスト アカウントの期限が切れる前に実行するアクションに関する SMS 通知をゲストが自動的に受信します。

情報をフィールドに入力するときは、[USERNAME]、[PASSWORD]、[PROVIDER_ID] など、[] 内のすべてのテキストを、SMS プロバイダのアカウントに固有の情報で更新する必要があります。

始める前に

[SMS 電子メールゲートウェイ (SMS Email Gateway)] オプションに使用するデフォルト SMTP サーバーを設定します。

次のタスク

新しい SMS ゲートウェイを追加すると、次のことが可能になります。

- 期限切れのアカウントに関する SMS 通知をゲストに送信するときに、SMS サービス プロバイダーを選択します。「[ゲスト タイプの作成または編集](#)」を参照してください。
- [アカウント登録 (Self-Registration)] フォームでアカウント登録ゲストに示される選択肢として、SMS プロバイダーのうちのどれを表示するかを指定します。[アカウント登録ゲスト ポータルの作成 \(32 ページ\)](#) を参照してください。

アカウント登録ゲストのソーシャルログイン

ゲストは、ゲストポータルにユーザー名とパスワードを入力する代わりに、アカウント登録ゲストでクレデンシャルを提供する方法としてソーシャルメディアプロバイダーを選択できます。これを有効にするには、ソーシャルメディアサイトを外部 ID ソースとして設定し、ユーザーがその外部 ID (ソーシャルメディアプロバイダー) を使用できるようにするポータルを設定します。Cisco ISE のソーシャルメディアログインに関する追加情報は、次を参照してください。<https://community.cisco.com/t5/security-documents/how-to-configure-amp-use-a-facebook-social-media-login-on-ise/ta-p/3609532>

ソーシャルメディアで認証した後、ゲストはソーシャルメディアサイトから取得した情報を編集できます。ソーシャルメディアのクレデンシャルが使用されているにもかかわらず、ソーシャルメディアサイトは、ユーザーがそのサイトの情報を使用してログインしたことを認識していません。ISE は引き続き、ソーシャルメディアサイトから取得された情報を今後の追跡のために内部的に使用します。

ユーザーがソーシャルメディアサイトから取得した情報を変更しないようにゲストポータルを設定したり、登録フォームの表示を抑制することもできます。

ソーシャルログインゲストフロー

ログインフローは、ポータル設定を行う方法によって異なります。ソーシャルメディアのログインは、ユーザー登録なし、ユーザー登録あり、またはユーザー登録とスポンサー承認ありで設定できます。

1. ユーザーはアカウント登録ポータルに接続し、ソーシャルメディアを使用してログインすることを選択します。アクセスコードを設定した場合、ユーザーはログインページにアクセスコードも入力する必要があります。
2. ユーザーは認証のためにソーシャルメディアサイトにリダイレクトされます。ユーザーは、ソーシャルメディアサイトの基本的なプロフィール情報の使用を承認する必要があります。

3. ソーシャルメディアサイトへのログインが成功すると、ISE はユーザーに関する追加情報をソーシャルメディアサイトから取得します。Cisco ISE はソーシャルメディア情報を使用してユーザーをログオンします。
4. ログイン後、設定に応じて、ユーザーは AUP を受け入れなくてはならない場合があります。
5. ログイン フローの次のアクションは設定によって異なります。
 - 登録なし：登録はバックグラウンドで行われます。Facebook はログイン用にユーザーのデバイスのトークンを Cisco ISE に提供します。
 - 登録あり：ユーザーには、ソーシャルメディアプロバイダーからの情報が事前に入力された登録フォームを完了するよう指示されます。これにより、ユーザーは不足している情報を修正および追加し、ログインのために更新された情報を提出することができます。登録フォームの設定で登録コードを設定した場合、ユーザーは登録コードも入力する必要があります。
 - 登録およびスポンサー承認あり：ユーザーにソーシャルメディア提供の情報を更新させることに加えて、ユーザーはスポンサーの承認を待たなければならないという通知を受けます。スポンサーは、アカウントの承認または拒否を要求する電子メールを受け取ります。スポンサーがアカウントを承認すると、Cisco ISE はユーザーにアクセス権を電子メール送信します。ユーザーはゲストポータルに接続し、ソーシャルメディア トークンで自動的にログインします。
6. 登録が成功します。ユーザーは [登録フォーム設定 (Registration Form Settings)] の [アカウント登録のためゲストフォームを送信後にゲストを次の場所に誘導する (After submitting the guest form for self-registration, direct guest to)] に設定されているオプションに誘導されます。ユーザーのアカウントは、ポータルのゲストタイプ用に設定されたエンドポイント ID グループに追加されます。
7. ゲストアカウントが期限切れになるか、またはユーザーがネットワークから切断するまで、ユーザーはアクセス権を持ちます。

アカウントの有効期限が切れた場合、ユーザーのログインを許可する唯一の方法は、アカウントを再アクティブ化することです（そうでない場合は、アカウントを削除します）。ユーザーはログインフローを再度実行する必要があります。

ユーザーがネットワークから切断して再接続した場合、Cisco ISE の処理は認証ルールによって異なります。ユーザーが次のような認証を取得した場合：

```
rule if guestendpoint then permit access
```

ユーザーがエンドポイントグループにまだ存在する場合、ユーザーはログオンページにリダイレクトされます。ユーザーがまだ有効なトークンを持っている場合は、自動的にログインします。持っていない場合は、登録をやり直す必要があります。

ユーザーが現在はエンドポイントグループに所属していない場合、ユーザーはゲストページにリダイレクトされ、登録をやり直します。

ソーシャルログインアカウントの期間

アカウント再認証は接続方法によって異なります。

- 802.1x の場合、デフォルトの許可ルールでは、

```
if guestendpoint then permit access
```

ユーザーデバイスがスリープ状態になった場合、または別の建物にローミングした場合に、ゲストが再接続できるようにします。ユーザーが再接続すると、そのユーザーはゲストページにリダイレクトされ、トークンを使用して自動ログインするか、または再度登録を開始します。

- MAB では、再接続するたびにユーザーはゲストポータルにリダイレクトされ、ソーシャルメディアを再度クリックする必要があります。Cisco ISE にそのユーザーのアカウントのトークン（ゲストアカウントの有効期限が切れていない）がまだある場合は、ソーシャルメディアプロバイダーに接続する必要はなく、ログインが即座に成功します。

すべての再接続が別のソーシャルログインにリダイレクトされないようにするには、デバイスを記憶し、アカウントが期限切れになるまでアクセスを許可する許可ルールを設定できます。アカウントが期限切れになると、そのアカウントはエンドポイントグループから削除され、フローはゲストリダイレクトのルールにリダイレクトされます。次に例を示します。

```
if wireless_mab and guest endpoint then permit access
```

```
if wireless_mab then redirect to self-registration social media portal
```

レポートとユーザー トラッキング

Cisco ISE ライブログと Facebook

- **Authentication Identity Store** : Cisco ISE のソーシャルメディアアプリケーションで作成したアプリケーションの名前です。
- **Facebook username** : Facebook によって報告されたユーザー名です。ユーザーが登録時にユーザー名を変更できるようにする場合、Cisco ISE によって報告される名前はソーシャルメディアのユーザー名です。
- **SocialMediaIdentifier** : ここでは、

```
https://facebook.com/<number>
```

number はソーシャルメディアユーザーを識別します。

[ISE レポート (ISE Reports)] : ゲストユーザー名は、ソーシャルメディアサイトのユーザー名です。

[Facebook 分析 (Facebook Analytics)] : Facebook の分析を使用して、Facebook のソーシャルログインを通じてゲストネットワークを使用しているユーザーを確認することができます。

[ワイヤレスと Facebook (Wireless and Facebook)] : ワイヤレスコントローラの [ユーザー名 (User Name)] は、ライブログの **SocialMediaIdentifier** と同じ一意の Facebook ID です。ワイ

ヤレス UI の設定を表示するには、[モニター (Monitor)] > [クライアント (Clients)] > [詳細 (Detail)] を選択し、[ユーザー名 (User Name)] フィールドを確認します。

ソーシャルメディアで認証されたゲストのブロック

個々のソーシャルメディアユーザーをブロックする許可ルールを作成することができます。これは、トークンが期限切れになっていない場合に Facebook を認証に使用する際に便利です。次の例は、Facebook ユーザー名を使用してブロックされた Wi-Fi 接続のゲストユーザーを示します。

図 1: Facebook ユーザー名を使用してブロックされた Wi-Fi 接続のゲストユーザー



Cisco ISE のソーシャルログインの設定については、[ソーシャルログインの設定 \(20 ページ\)](#) を参照してください。

ソーシャルログインの設定

始める前に

Cisco ISE が接続できるようにソーシャルメディアサイトを設定します。現在は Facebook のみがサポートされています。

Cisco ISE が Facebook にアクセスできるように、次の HTTPS 443 URL が NAD を介して開かれていることを確認します。

facebook.co
akamaihd.net
akamai.co
fbcdn.net



(注) Facebook のソーシャルログイン URL は HTTPS です。すべての NAD が HTTPS URL へのリダイレクションをサポートしているわけではありません。<https://communities.cisco.com/thread/79494?start=0&tstart=0&mobileredirect=true>を参照してください。

ステップ 1 Facebook で、Facebook アプリケーションを作成します。

- a) <https://developers.facebook.com> にログオンし、開発者としてサインアップします。
- b) ヘッダーで [アプリ (Apps)] を選択し、[新しいアプリの追加 (Add a New App)] をクリックします。

ステップ 2 タイプが [Web] の新しい [製品 (Product)]、[Facebook ログイン (Facebook Login)] を追加します。[設定 (Settings)] をクリックして次の値を設定します。

- [クライアント OAuth ログイン (Client OAuth Login)] : [いいえ (NO)]
- [Web OAuth ログイン (Web OAuth Login)] : [はい (YES)]
- [Web OAuth の再認証を強制 (Force Web OAuth Reauthentication)] : [いいえ (NO)]
- [組み込みブラウザ OAuth ログイン (Embedded Browser OAuth Login)] : [いいえ (NO)]
- [有効な OAuth リダイレクト URI (Valid OAuth redirect URIs)] : ISE から自動リダイレクト URL を追加します
- [デバイスからログイン (Login from Devices)] : [いいえ (NO)]

ステップ 3 [アプリレビュー (App Review)] をクリックして、[アプリは現在実行中でパブリックで利用可能です (Your app is currently live and available to the public)] に [はい (Yes)] を選択します。

ステップ 4 ISE で、[管理 (Administration)] > [ID 管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [ソーシャルログイン (Social Login)] に移動して [追加 (Add)] をクリックし、新しいソーシャルログインの外部 ID ソースを作成します。

- [タイプ (Type)] : ソーシャルログインプロバイダーのタイプを選択します。Facebook が現在のところ唯一の選択肢です。
- [アプリケーション ID (App ID)] : Facebook アプリケーションからアプリケーション ID を入力します。
- [アプリケーションシークレット (App Secret)] : Facebook アプリケーションからアプリケーションシークレットを入力します。

ステップ 5 Cisco ISE で、アカウント登録ポータルでの [ソーシャルメディアのログイン (Social Media Login)] を有効にします。ポータルページで、[ポータルとページの設定 (Portal & Page Settings)] > [ログインページの設定 (Login Page Settings)] を選択し、[ソーシャルログインの許可 (Allow Social Login)] チェックボックスをオンにし、次の詳細を入力します。

- [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、ユーザーは 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ーに通知し、ログイン用のクレデンシャルを送信します。

ステップ 6 [管理 (Administration)] > [外部 ID ソース (External Identity Sources)] を選択し、[Facebook ログイン (Facebook Login)] ウィンドウを選択して Facebook の外部 ID ソースを編集します。これによりリダイレクト URI が作成され、これを Facebook アプリケーションに追加します。

ステップ 7 Facebook で、前のステップの URI を Facebook アプリケーションに追加します。

次のタスク

Facebook では、アプリに関するデータを表示できます。このデータには、Facebook ソーシャルログインでのゲストアクティビティが表示されます。

ゲストポータル

企業の訪問者が企業のネットワークを使用してインターネットまたはネットワーク上のリソースおよびサービスにアクセスしようとしている場合、ゲストポータルを使用してネットワークアクセスを提供することができます。設定すると、従業員はゲストポータルを使用して会社のネットワークにアクセスできます。

3 つのデフォルトのゲストポータルがあります。

- [ホットスポットゲストポータル (Hotspot Guest portal)] : ネットワークアクセスはログイン情報を必要とせずに許可されます。通常、ネットワークアクセスを許可する前にユーザーポリシーの認可 (AUP) が承認される必要があります。

Wireless Setup では、ホットスポットポータルとアカウント登録ポータルでのアクセスコードログオンの要求がサポートされています。

- [Sponsored-Guest ポータル (Sponsored-Guest portal)] : ゲストのアカウントを作成したスポンサーによりネットワークアクセスが許可され、ゲストにログイン情報が提供されます。
- [アカウント登録ゲストポータル (Self-Registered Guest portal)] : ゲストは各自のアカウントのログイン情報を作成できます。ネットワークアクセスが付与される前に、スポンサー承認が必要となることがあります。

Cisco ISE は、事前に定義されたデフォルトポータルなど、複数のゲストポータルをホストすることができます。

ゲストポータルでのクレデンシャル

Cisco ISE では、ゲストにさまざまなタイプのクレデンシャルを使用したログインを要求することによって、保護されたネットワークアクセスを提供します。ゲストがこれらのクレデンシャルの1つまたは組み合わせを使用してログインすることを要求できます。

- [ユーザー名 (MAC Local User)]: 必須。エンドユーザーポータル (ホットスポットゲストポータルを除く) を使用するすべてのゲストに適用され、ユーザー名ポリシーから取得されます。ユーザー名ポリシーはシステムによって生成されたユーザー名のみ適用され、ゲストAPIプログラミングインターフェイスまたはアカウント登録プロセスを使用して指定されたユーザー名には適用されません。[ワークセンター (Work Centers)]>[ゲストアクセス (Guest Access)]>[設定 (Settings)]>[ゲストユーザー名ポリシー (Guest Username Policy)]で、ユーザー名に適用するポリシーを設定できます。ゲストは、電子メール、SMS、または印刷形式で、ユーザー名の通知を受け取ることができます。
- [パスワード (Password)]: 必須。エンドユーザーポータル (ホットスポットゲストポータルを除く) を使用するすべてのゲストに適用され、パスワードポリシーから取得されます。[ワークセンター (Work Centers)]>[ゲストアクセス (Guest Access)]>[設定 (Settings)]>[ゲストパスワードポリシー (Guest Password Policy)]で、パスワードに適用するポリシーを設定できます。ゲストは、電子メール、SMS、または印刷形式で、パスワードの通知を受け取ることができます。
- [アクセスコード (Access code)]: オプション。ホットスポットゲストポータルおよびクレデンシャルを持つゲストポータルを使用するゲストに適用されます。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)。ネットワークにアクセスするために、屋外にいる誰かに知られたり使用されたりすることはありません。アクセスコードの設定を有効にした場合、次のようになります。
 - スポンサー付きゲストは、[ログイン (Login)]ページで (ユーザー名およびパスワードとともに) これを入力するよう求められます。
 - ホットスポットゲストポータルを使用するゲストは、[利用規定 (Acceptable Use Policy (AUP))]ページでこれを入力するよう求められます。
- [登録コード (Registration code)]: オプション。アカウント登録ゲストに適用され、アカウント登録ゲストに提供される方法においてアクセスコードと似ています。登録コード設定が有効な場合、アカウント登録ゲストはアカウント登録フォームでこれを入力するよう求められます。

ユーザー名とパスワードは、社内のスポンサーが (スポンサー付きゲストに対して) 提供できます。または、ゲストが自分自身を登録してこれらのクレデンシャルを取得できるように、クレデンシャルを持つゲストポータルを設定できます。

関連トピック

[ゲストタイプおよびユーザーIDグループ \(3 ページ\)](#)

ホットスポット ゲスト ポータルを使用したゲスト アクセス

Cisco ISE にはネットワーク アクセス機能があり、その機能には「ホットスポット」が含まれています。これは、アクセスポイントで、ゲストはこれを使用してログインにクレデンシャルを必要とすることなくインターネットにアクセスできます。ゲストがコンピュータまたは Web ブラウザを搭載した任意のデバイスでホットスポット ネットワークに接続して、Web サイトに接続しようとする、自動的にホットスポット ゲスト ポータルにリダイレクトされます。この機能では、有線接続と無線接続 (Wi-Fi) の両方がサポートされます。

ホットスポット ゲスト ポータルは代替となるゲスト ポータルで、これを使用すると、ゲストにユーザー名とパスワードを要求することなく、ネットワーク アクセスを提供することができます。代わりに、ゲストデバイスにネットワークアクセスを直接提供するために、Cisco ISE はネットワークアクセスデバイス (NAD) およびデバイス登録 Web 認証 (デバイス登録 WebAuth) とともに動作します。場合によって、ゲストは、アクセスコードを使用してログインするよう要求されることがあります。通常、これは社内に物理的に存在しているゲストにローカルに提供されるコードです。

ホットスポット ゲスト ポータルをサポートしている場合：

- ホットスポット ゲスト ポータルの設定に基づいて、ゲスト アクセスの条件を満たしている場合、ゲストにネットワーク アクセスが付与されます。
- Cisco ISE によってデフォルトのゲスト ID グループ `GuestEndpoints` が提供され、これを使用して、ゲストデバイスを一元的に追跡できます。

クレデンシャルを持つゲスト ポータルを使用したゲスト アクセス

クレデンシャルを持つゲスト ポータルを使用して、外部ユーザーの内部ネットワークおよびサービスと、インターネットへの一時アクセスを識別し許可することができます。スポンサーは、ポータルの [ログイン (Login)] ページでこれらのクレデンシャルを入力することによって、ネットワークにアクセスできる承認ユーザーの一時的なユーザー名およびパスワードを作成できます。

次のように取得したユーザー名とパスワードを使用してゲストがログインできるように、クレデンシャルを持つゲスト ポータルを設定できます。

- スポンサーから付与されます。このゲストフローでは、ゲストは、社内に入って個人のゲストアカウントで設定されたとき、ロビー アンバサダーなどのスポンサーによるグリーンディングを受け取ります。
- オプションの登録コードまたはアクセスコードを使用して自分自身を登録した後に付与されます。このゲストフローでは、ゲストは人間の介入なしでインターネットにアクセスでき、これらのゲストにコンプライアンスに使用可能な一意の識別子があることが Cisco ISE によって保証されます。
- オプションの登録コードまたはアクセスコードを使用して自分自身を登録した後に付与されます。ただし、ゲストアカウントの要求がスポンサーによって承認された後のみです。

このゲストフローでは、ゲストにネットワークへのアクセスが提供されますが、追加のスクリーニング レベルが実行された後でのみ提供されます。

また、ログイン時にユーザーに新しいパスワードを入力するよう強制できます。

Cisco ISE では、複数のクレデンシャルを持つゲスト ポータルを作成し、これを使用してさまざまな基準に基づいてゲストアクセスを許可することができます。たとえば、日次訪問者に使用されるポータルとは別の、月次担当者向けのポータルを設定できます。

クレデンシャルを持つゲスト ポータルを使用した従業員アクセス

従業員は、そのポータルに設定された ID ソース順序でクレデンシャルにアクセスできれば、従業員クレデンシャルを使用してサインインすることによって、クレデンシャルを持つゲストポータルを使用してネットワークにアクセスすることもできます。

ゲスト デバイスのコンプライアンス

ゲストおよび非ゲストがクレデンシャルを持つゲストポータルを介してネットワークにアクセスした場合、アクセスを許可する前に、そのデバイスのコンプライアンスをチェックすることができます。ゲストおよびゲスト以外を[クライアントプロビジョニング (Client Provisioning)] ウィンドウ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要求することができます。このエージェントは、ポスチャプロファイルを確認し、デバイスが準拠しているかどうかを検証します。これは、クレデンシャルを持つゲストポータルで、[ゲストデバイスのコンプライアンス設定 (Guest Device Compliance Settings)] のオプションを有効にすることで実行できます。これによって、[クライアントプロビジョニング (Client Provisioning)] ウィンドウがゲストフローの一部として表示されます。



(注) ゲストフローのクライアントポスチャアセスメントは、テンポラルエージェントのみをサポートしています。

クライアントプロビジョニングサービスでは、ゲストのポスチャ評価および修復が提供されます。クライアントプロビジョニングポータルは、中央 Web 認証 (CWA) のゲスト展開でのみ使用できます。ゲストログインフローによって CWA が実行され、クレデンシャルを持つゲストポータルは、利用規定やパスワード変更のチェックを実行した後、クライアントプロビジョニングポータルにリダイレクトされます。いったんポスチャが評価されると、ポスチャサブシステムはネットワークアクセスデバイスに対して許可変更 (CoA) を実行し、クライアント再接続を再認証します。

ゲスト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。

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。

さまざまなゲストポータルの設定に関連するタスクについては、この表を参照してください。

タスク	ホットスポットゲストポータル	Sponsored-Guest ポータル	アカウント登録ゲストポータル
ポリシーサービスの有効化 (27 ページ)	必須	必須	必須
ゲストポータルの証明書の追加 (27 ページ)	必須	必須	必須
外部 ID ソースの作成 (27 ページ)	N/A	必須	必須
ID ソース順序の作成 (29 ページ)	N/A	必須	必須
エンドポイント ID グループの作成	必須	不要 (ゲストタイプによって定義される)	不要 (ゲストタイプによって定義される)
ホットスポットゲストポータルの作成 (30 ページ)	必須 (Required)	N/A	N/A
Sponsored-Guest ポータルの作成 (31 ページ)	N/A	必須	N/A
アカウント登録ゲストポータルの作成 (32 ページ)	N/A	N/A	必須
ポータルの許可 (34 ページ)	必須	必須	必須
ゲストポータルのカスタマイズ (36 ページ)	オプション	オプション	オプション

ポリシー サービスの有効化

Cisco ISE エンドユーザー Web ポータルをサポートするには、ホストするノードでポータルポリシーサービスを有効にする必要があります。

- ステップ 1 [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)] チェックボックスをオンにします。
- ステップ 4 [セッションサービスの有効化 (Enable Session Services)] チェックボックスをオンにします。
- ステップ 5 [Save] をクリックします。

ゲスト ポータルの証明書の追加

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

外部 ID ソースの作成

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



- (注) 認証済みユーザー ID を受信して共有できるようにするパッシブ ID サービスを使用するには、[その他のパッシブ ID サービスプロバイダ](#)を参照してください。

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 ソースとして Active Directory に接続する場合。詳細については、[外部 ID ソースとしての Active Directory](#)を参照してください。
- LDAP : LDAP ID ソースを追加する場合。詳細については、[LDAP](#)を参照してください。
- RADIUS トークン (RADIUS Token) : RADIUS トークンサーバーを追加する場合。詳細については、[RADIUS トークン ID ソース](#)を参照してください。
- RSA SecurID : RSA SecurID サーバーを追加する場合。詳細については、[RSA ID ソース](#)を参照してください。

- SAML IDプロバイダー (SAML Id Providers) : Oracle Access Manager などの ID プロバイダー (IdP) を追加する場合。詳細については、[外部 ID ソースとしての SAMLv2 ID プロバイダー](#)を参照してください。
- [ソーシャルログイン (Social Login)] : Facebook などのソーシャルログインを外部 ID ソースとして追加する場合。詳細については、[アカウント登録ゲストのソーシャルログイン \(17 ページ\)](#) を参照してください。

認証用の SAML IDP ポータルにリダイレクトするためのゲストポータルの設定

ゲストポータルを設定して、ユーザーが認証のために SAML IDP ポータルにリダイレクトされるようにすることができます。

ゲストポータルで [ログインに次の ID プロバイダー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)] オプションを設定することで、そのポータルで新しいログイン エリアが有効になります。ユーザーがそのログイン オプションを選択した場合、代替 ID ポータルにリダイレクトされてから (表示されません) 、認証のために SAML IDP ログオン ポータルにリダイレクトされます。

たとえば、ゲストポータルには従業員ログインのためのリンクがあります。既存のポータルにログインする代わりに、ユーザーは従業員ログオンリンクをクリックし、SAML IDP シングル サインオン ポータルにリダイレクトされます。従業員はこの SAML IDP による最後のログオンからのトークンを使用して再接続されるか、その SAML サイトでログインします。これにより、同じポータルでシングル SSID からゲストと従業員の両方を扱うことができます。

次の手順は、SAML IDP を認証用に使用するように設定されている別のポータルを呼び出すゲストポータルを設定する方法を示しています。

- ステップ 1** 外部 ID ソースを設定します。詳細については、[外部 ID ソースとしての SAMLv2 ID プロバイダー](#)を参照してください。
- ステップ 2** SAML プロバイダーのゲストポータルを作成します。ポータル設定で [認証方式 (Authentication method)] を SAML プロバイダーに設定します。ユーザーにはこのポータルは表示されず、これは単にユーザーを SAML IDP ログオン ページにつなぐためのプレースホルダです。次に説明するように、他のポータルをこのサブポータルにリダイレクトするように設定できます。
- ステップ 3** 作成したばかりの SAML プロバイダー ポータルのゲストポータルにリダイレクトするためのオプションを備えたゲストポータルを作成します。これはメインポータルで、サブポータルにリダイレクトします。SAML プロバイダーに見えるように、このポータルの外観をカスタマイズする場合があります。
 - a) メインポータルの [ログイン ページの設定 (Login Page Settings)] で、[ログインに次の ID プロバイダー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)] にマークを付けます。
 - b) SAML プロバイダーと使用するために設定したゲストポータルを選択します。

ID ソース順序の作成

始める前に

Cisco ISE に外部 ID ソースを設定していることを確認します。

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

ゲストユーザーがローカル WebAuth を使用して認証できるようにするには、ゲストポータル認証ソースと ID ソース順序の両方に同じ ID ストアが含まれるように設定する必要があります。

-
- ステップ 1 [管理 (Administration)] > [ID 管理 (Identity Management)] > [ID ソース順序 (Identity Source Sequences)] > [追加 (Add)] を選択します。
 - ステップ 2 ID ソース順序の名前を入力します。また、任意で説明を入力できます。
 - ステップ 3 [証明書認証プロファイル (Certificate Authentication Profile)] チェックボックスをオンにし、証明書ベースの認証のための証明書認証プロファイルを選択します。
 - ステップ 4 [選択済み (Selected)] リストフィールドの ID ソース順序に含めるデータベースを選択します。
 - ステップ 5 Cisco ISE がデータベースを検索する順序に [選択済み (Selected)] リストフィールドのデータベースを並べ替えます。
 - ステップ 6 選択したアイデンティティストアに認証のためにアクセスできない場合は、[高度な検索リスト (Advanced Search List)] 領域で次のいずれかのオプションを選択します。
 - [順序内の他のストアにアクセスせず、AuthenticationStatus 属性を ProcessError に設定 (Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError)]
 - [ユーザーが見つからなかったとして処理し、順序内の次のストアに進む (Treat as if the user was not found and proceed to the next store in the sequence)]

Cisco ISE では、要求の処理中にこれらの ID ソースが順番に検索されます。[選択済み (Selected)] リストフィールドに Cisco ISE が ID ソースを検索する順序で ID ソースが表示されていることを確認します。
 - ステップ 7 [送信 (Submit)] をクリックして ID ソース順序を作成すると、その後この ID ソース順序をポリシーで使用できます。
-

エンドポイント ID グループの作成

Cisco ISE では、検出したエンドポイントを、対応するエンドポイント ID グループにグループ化します。Cisco ISE では、システム定義された複数のエンドポイントの ID グループが事前に用意されています。[エンドポイント ID グループ (Endpoint Identity Groups)] ウィンドウでは、追加のエンドポイント ID グループも作成できます。作成したエンドポイント ID グループを編集または削除できます。システムで定義されたエンドポイント ID グループの説明のみを編集できます。これらのグループの名前を編集または削除することはできません。

-
- ステップ 1** [管理 (Administration)] > [ID 管理 (Identity Management)] > [グループ (Groups)] > [エンドポイント ID グループ (Endpoint Identity Groups)] を選択します。
- ステップ 2** [Add] をクリックします。
- ステップ 3** 作成するエンドポイント ID グループの [名前 (Name)] に入力します (エンドポイント ID グループの名前にはスペースを入れないでください)。
- ステップ 4** 作成するエンドポイント ID グループの [説明 (Description)] に入力します。
- ステップ 5** [親グループ (Parent Group)] ドロップダウン リストをクリックして、新しく作成したエンドポイント ID グループを関連付けるエンドポイント ID グループを選択します。
- ステップ 6** [Submit] をクリックします。
-

ホットスポット ゲスト ポータルの作成

ホットスポット ゲスト ポータルを提供して、ゲストが、ログインにユーザー名とパスワードを要求されずにネットワークに接続できるようにすることができます。ログイン時にアクセスコードが必要な場合があります。

新しいホットスポット ゲスト 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ホットスポット ゲスト 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、ゲストフロー図のグラフィカルフローに反映されます。AUP 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、ゲスト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、次に有効なページがゲストに表示されます。

[認証成功の設定 (Authentication Success Settings)] を除くすべてのページ設定は、任意です。

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。
- ゲストがホットスポットポータルのために接続する WLC が Cisco ISE でサポートされていることを確認します。お使いのバージョンの Cisco ISE の『[Identity Services Engine Network Component Compatibility](#)』ガイドを参照してください。

-
- ステップ 1** [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)] を選択します。
- ステップ 2** 新しいポータルを作成する場合は、[ゲストポータルの作成 (Create Guest Portal)] ダイアログボックスで、ポータルタイプとして [ホットスポット ゲスト ポータル (Hotspot Guest Portal)] を選択し、[続行 (Continue)] をクリックします。
- ステップ 3** ポータルの一意の [ポータル名 (Portal Name)] および [説明 (Description)] を指定します。

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

- ステップ 4** [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 5** [ポータルの設定 (Portal Settings)] でポート、イーサネット インターフェイス、証明書グループ タグ、エンドポイント ID グループなどのデフォルト値を更新し、ポータル全体に適用する動作を定義します。
- ステップ 6** 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。
- [利用規定 (AUP) ページ設定 (Acceptable Use Policy (AUP) Page Settings)] : 利用規定に同意することをゲストに要求します。
 - [ポストログイン バナーページの設定 (Post-Login Banner Page Settings)] : 必要に応じて、ゲストにアクセス ステータスおよびその他の追加アクションを通知します。
 - [VLAN DHCPリリースページの設定 (VLAN DHCP Release Page Settings)] : ゲスト デバイスの IP アドレスをゲスト VLAN から解放し、ネットワークの他の VLAN にアクセスするように更新します。
 - [認証成功の設定 (Authentication Success Settings)] : 認証されたゲストに対する表示内容を指定します。
 - [サポート情報ページの設定 (Support Information Page Settings)] : 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を支援します。
- ステップ 7** [保存 (Save)] をクリックします。システム生成の URL がポータル テスト URL として表示されます。この URL を使用して、ポータルにアクセスし、テストすることができます。

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。

Sponsored-Guest ポータルの作成

Sponsored-Guest ポータルを提供して、指定されたスポンサーがゲストにアクセスを許可できるようにすることができます。

新しい Sponsored-Guest 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、任意の Sponsored-Guest 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、ゲストフロー図のグラフィカルフローに反映されます。AUP 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、ゲスト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、次に有効なページがゲストに表示されます。

次のすべてのページ設定によって、ゲスト用の利用規定 (AUP) を表示し、その同意を要求することができます。

- ログイン ページの設定 (Login Page Settings)
- 利用規定 (AUP) ページ設定 (Acceptable Use Policy (AUP) Page Settings)

- BYOD 設定 (BYOD Settings)

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 ソース、および ID ソース順序が設定されていることを確認します。

次のタスク



(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。

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。

アカウント登録ゲスト ポータルの作成

アカウント登録ゲストポータルを提供して、ゲストが自分自身を登録し、自分のアカウントを作成して、ネットワークにアクセスできるようにすることができます。これらのアカウントに対しては、その後も、アクセスを許可する前に、スポンサーによる承認を要求できます。

新しいアカウント登録ゲスト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アカウント登録ゲスト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、ゲストフロー図のグラフィカルフローに反映されます。AUP 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、ゲスト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、次に有効なページがゲストに表示されます。

次のすべてのページ設定によって、ゲスト用の利用規定 (AUP) を表示し、その同意を要求することができます。

- ログイン ページの設定 (Login Page Settings)
- アカウント登録ページの設定 (Self-Registration Page Settings)
- アカウント登録成功ページの設定 (Self-Registration Success Page Settings)
- 利用規定 (AUP) ページ設定 (Acceptable Use Policy (AUP) Page Settings)
- BYOD 設定 (BYOD Settings)

始める前に

このポータルに必要な証明書、外部 ID ソース、および ID ソース順序が設定されていることを確認します。

次のタスク



- (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。

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。

スポンサーによるアカウント登録のアカウントの承認

登録済みゲストがアカウントの承認を要求するように設定すると、Cisco ISE は、アカウントの承認のために電子メールを承認者に送信します。承認者は、訪問先担当者またはスポンサーユーザーのいずれかです。

承認者がスポンサーの場合、アカウントを拒否または承認するリンクを含めるように電子メールを設定できます。承認リンクには、承認をスポンサーの電子メールアドレスに関連付けるトークンが含まれています。スポンサーに認証を要求できます。これにより、トークンは無視されます。トークンはタイムアウトすることもあります。タイムアウトすると、スポンサーは、アカウントを承認する前に認証を受ける必要があります。

アカウント承認オプションは、自己登録ポータルの [登録フォームの設定 (Registration Form Settings)] で設定します。この機能は、シングルクリック スポンサー承認とも呼ばれます。

スポンサーが電子メールを開いて承認リンクをクリックすると実行されるアクションは、承認者の設定に応じて異なります。

[承認要求電子メール送信先 (Email approval request to)] が次のいずれかに設定されている場合について説明します。

• [訪問先担当者 (person being visited)]

- また、ゲストアカウントに認証が不要な場合は、1 回のクリックでアカウントが承認されます。
- ゲストアカウントに承認が必要な場合は、スポンサーにスポンサーポータルが表示されます。このポータルでは、アカウントの承認前にスポンサーがクレデンシャルを入力する必要があります。

- [下に示すスポンサーの電子メールアドレス (Sponsor email addresses listed below)] : Cisco ISE は、指定されるすべての電子メールアドレスに電子メールを送信します。これらのスポンサーのいずれかが承認リンクまたは拒否リンクをクリックすると、スポンサーポータルが表示されます。そのスポンサーがクレデンシャルを入力し、確認されます。スポン

サーが所属するスポンサー グループで、スポンサーによるゲスト アカウントの承認が許可されている場合、スポンサーはアカウントを承認できます。クレデンシャルが失敗すると、Cisco ISE は、スポンサーポータルにログインしてアカウントを手動で承認するようスポンサーに通知します。

説明

- 前のバージョンの Cisco ISE からデータベースをアップグレードまたは復元する場合は、承認または拒否のリンクを手動で挿入する必要があります。アカウント登録ゲストポータルを開き、[ポータルページのカスタマイズ (Portal Page Customizations)] タブを選択します。下方向にスクロールし、[承認要求の電子メール (Approval Request Email)] ウィンドウを選択します。そのウィンドウの **電子メール本文** セクションで [承認/拒否のリンクを挿入する (Insert Approve/Deny Links)] をクリックします。
- Active Directory および LDAP で認証するスポンサー ポータルのみがサポートされています。スポンサーがマッピングするスポンサー グループには、スポンサーが属する Active Directory グループが含まれている必要があります。
- スポンサーのリストがある場合、最初のポータルが、スポンサーがログインするポータルではない場合でも、最初のポータルのカスタマイズ内容が使用されます。
- スポンサーは、承認リンクと拒否リンクを使用するために、HTM 対応の電子メールクライアントを使用する必要があります。
- スポンサーの電子メールアドレスが有効なスポンサー用ではない場合、承認電子メールは送信されません。

シングルクリック スポンサーの承認の詳細については、Cisco ISE コミュニティリソースの『[ISE Single Click Sponsor Approval FAQ](#)』を参照してください。このドキュメントには、プロセス全体を説明するビデオへのリンクも含まれています。

アカウント承認メール リンクの設定

ネットワークにアクセスする前に、アカウント登録ゲストの承認を要求できます。Cisco ISE は、訪問先担当者の電子メールアドレスを使用して、承認者に通知します。承認者は、訪問先担当者またはスポンサーのいずれかです。承認の詳細については、[スポンサーによるアカウント登録のアカウントの承認 \(33 ページ\)](#) を参照してください。

ポータルの許可

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

始める前に

ポータルを許可する前にポータルを作成する必要があります。

ステップ 1 ポータルの特別な許可プロファイルを設定します。

ステップ 2 プロファイルの許可ポリシー ルールを作成します。

許可プロファイルの作成

各ポータルには、特別な許可プロファイルを設定する必要があります。

始める前に

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

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。

ホットスポット ポータルおよび MDM ポータル用の許可ポリシー ルールの作成

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

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

ip:port : IP アドレスとポート番号

PortalID : 一意のポータル名

ホットスポット ゲスト ポータル :

`https://ip:port/guestportal/gateway?sessionID=SessionIdValue&portal=PortalID&action=cwa&type=drw`

モバイルデバイス管理 (MDM) ポータル :

`https://ip:port/mdmportal/gateway?sessionID=SessionIdValue&portal=PortalID&action=mdm`

ステップ 1 [ポリシー (Policy)] > [ポリシーセット (Policy Sets)][ポリシー (Policy)] > [ポリシーセット (Policy Sets)] を選択して、[標準 (Standard)] ポリシーで新しい認証ポリシー規約を作成します。

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

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

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



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

ゲストポータルのカスタマイズ

ポータルの外観およびユーザー（必要に応じてゲスト、スポンサー、または従業員）エクスペリエンスをカスタマイズするには、ポータルテーマをカスタマイズし、ポータルページの UI 要素を変更して、ユーザーに表示されるエラーメッセージと通知を編集します。ポータルのカスタマイズの詳細については、[エンドユーザー Web ポータルのカスタマイズ \(106 ページ\)](#) を参照してください。

定期的な AUP 受け入れの設定

[ポリシー (Policy)] > [ポリシーセット (Policy Sets)] を選択し、AUP の期限が切れた場合にゲストユーザーをログイン情報を持つポータルにリダイレクトする新しい認証ルールをリストの上部に作成します。LastAUPAcceptanceHours を目的の最大時間と比較するために条件 (LastAUPAcceptanceHours > 8 など) を使用します。時間の範囲 1 ~ 999 をチェックできます。

次のタスク

エンドポイントが AUP 設定を受信したことを確認するには、次の手順を実行します。

- 1.
2. AUP が最後に受け入れられた時刻を確認するエンドポイントをクリックします (AUPAcceptedTime)。

定期的な AUP の強制

ポリシーで LastAUPAcceptance を使用して、AUP を承認することをユーザーに強制できます。

```
If LastAUPAcceptance >= 24: Hotspot Redirect
If LastAUPAcceptance < 24: PermitAccess
If Wireless_MAB: Hotspot Redirect
```

この例では、24 時間ごとにホットスポットポータルに AUP を強制する方法を示します。

1. ユーザーが 24 時間以上前に AUP を承認済みの場合、AUP を受け入れる（初めからやり直す）必要があります。
2. ユーザーが 24 時間前以内に AUP を承認済みの場合、セッションを続行します。
3. ネットワーク (MAB) への最初のアクセス時は AUP を承認する必要があります。

クレデンシャルを持つポータルでは、そのポータルの AUP が有効であれば同じ規則を使用できます。



- (注)
- エンドポイントへのゲスト AUP ページの通信を確立するには、次に示すとおり、ゲストポータルのリダイレクト認証ルールに LastAUPAcceptanceHours 条件を追加します。
 If AUP <= "X hours": Add in the Permit Access Rule
 If AUP > "X hours": Add in the Redirection Rule
 - 新規ユーザーは、LastAUPAcceptanceHours 条件なしでリダイレクト認証ルールを設定できません。

ゲストユーザー情報を保存

この機能により、Cisco ISE はレポートとログに MAC アドレスではなくゲストのユーザー名を表示できます。

ゲストが初回認証されると、ユーザーのデバイスの MAC アドレスがエンドポイントグループに保存され、レポートでユーザー名が使用されます。ユーザーが切断され、ネットワークに再接続された場合、MAC アドレスはすでにエンドポイントグループに存在するため、ユーザーは再びログイン（認証）する必要はありません。この場合、ユーザー名は利用できないため、レポートとログには MAC アドレスが使用されます。

Cisco ISE はポータルユーザー ID を保持し、これを一部のレポートで使用します。この機能を無効にするには、**[Guest] > [Settings] > [Logging]** に移動します。この機能は新規インストール時にデフォルトで有効になっています。

[アカウントを記憶する (Remember Me)] のロギングの問題に関する詳細については、Cisco ISE コミュニティのリソースの『[ISE 2.3+ Remember Me guest using guest endpoint group logging display](#)』を参照してください。

[アカウントを記憶する (Remember Me)] の設定に関する詳細については、『Cisco ISE Guest Access Deployment』のガイドを参照してください。 <https://communities.cisco.com/docs/DOC-77590>

各リリースでサポートされるレポート方法に関する詳細については、該当するリリースのリリース ノートを参照してください。

スポンサー ポータル

スポンサー ポータルは、Cisco ISE ゲスト サービスの主要コンポーネントの 1 つです。スポンサー ポータルを使用して、スポンサーは承認ユーザー用の一時アカウントを作成および管理し、企業ネットワークまたはインターネットにセキュアにアクセスできるようにします。ゲストアカウントを作成した後、スポンサーは、スポンサーポータルを使用して、印刷、電子メール送信、または携帯電話による送信を行ってゲストにアカウントの詳細を提供することもでき

まず、アカウント登録ゲストに企業ネットワークへのアクセス権を提供する前に、スポンサーはゲスト アカウントを承認するように電子メールで要求されることがあります。

スポンサー ポータルでのゲスト アカウントの管理

スポンサー ポータルのログオンのフロー

スポンサー グループにより、スポンサー ユーザーに割り当てられる権限のセットが指定されます。スポンサーがスポンサー ポータルにログインすると、次の処理が行われます。

1. ISE がスポンサーのクレデンシャルを検証します。
2. スポンサーの認証が成功すると、Cisco ISE は使用可能なすべてのスポンサーグループを検索して、スポンサーが属するスポンサーグループを見つけます。次の両方の条件を満たしている場合は、スポンサーがスポンサー グループに一致しているか、属しています。
 - スポンサーは、設定されているいずれかのメンバー グループのメンバーである。
 - [その他の条件 (Other Conditions)] を使用している場合は、そのスポンサーについてすべての条件が `true` である。
3. スポンサーがスポンサー グループに属している場合、スポンサーはそのグループの権限を取得します。スポンサーは複数のスポンサー グループに属することができます。この場合、属しているすべてのグループの権限が組み合わせられます。スポンサーがどのスポンサー グループにも属していない場合、スポンサー ポータルへのログインは失敗します。

スポンサー グループとその権限は、スポンサー ポータルから独立しています。スポンサーがログインするスポンサー ポータルに関係なく、スポンサー グループの照合には同一アルゴリズムが使用されます。

スポンサー ポータルの使用

スポンサー ポータルを使用して、承認された訪問者が企業ネットワークまたはインターネットにセキュアにアクセスできるようにする一時ゲスト アカウントを作成します。ゲスト アカウントを作成したら、スポンサー ポータルを使用してこれらのアカウントを管理し、アカウントの詳細情報をゲストに提供することができます。

スポンサー ポータルでは、スポンサーが新しいゲスト アカウントを個別に作成するか、またはファイルからユーザー グループをインポートすることができます。



-
- (注) Active Directory などの外部 ID ストアから承認された ISE 管理者は、スポンサー グループに所属できません。ただし、内部管理者アカウント (デフォルトの「admin」アカウントなど) はスポンサー グループに含めることができます。
-

スポンサー ポータルを開く方法はいくつかあります。

- [管理者 (Administrators)] コンソールで、[アカウントの管理 (Manage Accounts)] リンクを使用します。[管理者 (Administrators)] コンソールで、[ゲストアクセス (Guest Access)] をクリックしてから、[アカウントの管理 (Manage Accounts)] をクリックします。[アカウントの管理 (Manage Accounts)] をクリックすると、ALL_ACCOUNTS にアクセスできるデフォルトのスポンサーグループに割り当てられます。新しいゲストアカウントを作成できますが、ゲストに対して通知することはできません。これは、ゲストからのアカウントアクティブ化要求を受信するための電子メールアドレスがないためです。同じ権限を持ち、スポンサーポータルにログインしてこれらのアカウントを検索するスポンサーは、通知を送信できます。

このステップでは、[スポンサー (Sponsor)] ポータルの [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] ウィンドウで設定した FQDN が DNS サーバーに存在している必要があります。

NAT ファイアウォールを介してスポンサーポータルにアクセスしている場合、接続はポート 9002 を使用します。

- [管理者 (Administrators)] コンソールの [スポンサーポータル (Sponsor Portal)] 設定ウィンドウから、次の操作を実行します。[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)] をクリックしてスポンサーポータルを開き、[説明 (Description)] フィールドの右側にある [ポータルテスト URL (Portal Test URL)] リンクをクリックします。
- ブラウザで、スポンサーポータルの [ポータル設定 (Portal Settings)] ウィンドウで設定した URL (FQDN) を開きます。この URL (FQDN) は DNS サーバーで定義されている必要があります。

次の作業

スポンサーポータルの使用法については、お使いのバージョンの ISE の『Sponsor Portal User Guide』 (<https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html>) を参照してください。

スポンサー アカウントの管理

スポンサーは、スポンサーポータルからゲストユーザーアカウントを作成および管理する組織の従業員または請負業者となります。Cisco ISE は、ローカルデータベースあるいは外部の Lightweight Directory Access Protocol (LDAP) 、Microsoft Active Directory、または SAML ID ストア経由でスポンサーを認証します。外部ソースを使用しない場合、スポンサー用の内部ユーザーアカウントを作成する必要があります。

スポンサー グループ

スポンサーグループは、スポンサーポータルの使用時にスポンサーに付与される権限を制御します。スポンサーがスポンサーグループのメンバーである場合、スポンサーにはグループに定義されている権限が付与されます。

スポンサーは、次の**両方**が当てはまる場合にスポンサーグループのメンバーであると見なされます。

■ スポンサー アカウントの作成およびスポンサー グループへの割り当て

1. スポンサーが、スポンサー グループで定義されているメンバー グループの少なくとも 1 つに属している。メンバー グループは、ユーザー ID グループか、Active Directory などの外部 ID ソースから選択されたグループです。
2. スポンサーが、スポンサーグループで指定されているすべてのその他の条件を満たしている。オプションのその他の条件は、ディクショナリ属性で定義される条件です。これらの条件は、許可ポリシーで使用されるものと動作が似ています。

スポンサーは、複数のスポンサーグループのメンバーにすることができます。その場合、スポンサーにはそれらすべてのグループから次のように組み合わせられた権限が付与されます。

- いずれかのグループで有効になっている場合、「ゲストのアカウントの削除」などの個々の権限が付与されます。
- スポンサーは、任意のグループでゲスト タイプを使用してゲストを作成できます。
- スポンサーは、任意のグループの場所にゲストを作成できます。
- バッチ サイズ制限などの数値は、グループの最大値が使用されます。

スポンサーがいずれかのスポンサーグループのメンバーでない場合、そのスポンサーはスポンサー ポータルにログインできません。

- ALL_ACCOUNTS : スポンサーは、すべてのゲストアカウントを管理できます。
- GROUP_ACCOUNTS : スポンサーは、同じスポンサーグループのスポンサーが作成したゲストアカウントを管理できます。
- OWN_ACCOUNTS : スポンサーは、作成したゲストアカウントのみを管理できます。

特定のスポンサーグループで使用可能な機能をカスタマイズでき、それによりスポンサーポータルの機能を制限または拡張できます。

■ スポンサー アカウントの作成およびスポンサー グループへの割り当て

内部スポンサー ユーザー アカウントを作成し、スポンサー ポータルを使用できるスポンサーを指定するには、次の手順を実行します。

ステップ 1 (注) デフォルトのスポンサー グループには、デフォルトの ID グループ Guest_Portal_Sequence が割り当てられています。

ステップ 2 [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)] > [作成、編集または複製 (Create, Edit or Duplicate)] を選択し、Cisco ISE GUI で [メニュー (Menu)] アイコン (☰) をクリックして選択します。[メンバー (Members)] をクリックします。スポンサーユーザー ID グループをスポンサーグループにマッピングします。

次のタスク

スポンサーで使用するために、追加で組織に固有のユーザー ID グループを作成することもできます。[管理 (Administration)] > [ID の管理 (Identity Management)] > [グループ (Groups)] > [ユーザー ID グループ (User Identity Groups)] を選択します。

スポンサー グループの設定

シスコはデフォルトのスポンサー グループを提供します。デフォルト オプションを使用しない場合、新しいスポンサー グループを作成するか、またはデフォルトのスポンサー グループを編集して設定を変更できます。スポンサーグループを複製して、同じ設定と権限を持つスポンサー グループをさらに作成することもできます。

スポンサーグループを無効にすることができます。無効になったグループのメンバーはスポンサー ポータルにログインできなくなります。Cisco ISE によって提供されているデフォルトのスポンサー グループ以外のスポンサー グループを削除できます。

ステップ 1 [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 and Components)] > [スポンサーグループ (Sponsor Groups)] > [作成、編集または複製 (Create, Edit or Duplicate)] を選択します。

ステップ 2 [スポンサーグループ名 (Sponsor group name)] と [説明 (Description)] に入力します。

ステップ 3 [一致基準 (Match Criteria)] セクションに次の詳細を入力します。

- [メンバーグループ (Member Groups)] : [メンバー (Members)] をクリックして1つ以上のユーザー (ID) グループと外部 ID ソースグループを選択し、それらのグループを追加します。ユーザーがこのスポンサー グループのメンバーになるためには、少なくとも1つの設定済みグループに属している必要があります。
- [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め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。内部ユーザー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ー 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ーだけがこのスポンサー グループに所属できます。
 - Active Directory インスタンスの ExternalGroups 属性を使用して条件を作成するには、一致させるスポンサー ユーザーの AD 「プライマリ グループ」を選択します。たとえば、ユーザーの名前が Smith の場合は *ADI:LastName EQUALS Smith* になります。

1 つ以上の設定されたメンバー グループとの一致に加えて、スポンサーはここで作成するすべての条件に一致する必要があります。認証しているスポンサーユーザーが複数のスポンサー グループの一致基準を満たす場合には、そのユーザーには次のようにアクセス許可が付与されます。

- ゲストのアカウントの削除などの個々の権限は、一致するグループのいずれかで有効になっている場合に付与されます。
- スポンサーは、一致するグループのいずれかのゲストタイプを使用してゲストを作成することができます。
- スポンサーは、一致するグループのいずれかのゲストタイプを使用してゲストを作成することができます。
- スポンサーは、一致するグループのいずれかの場所でゲストを作成することができます。
- バッチサイズ制限などの数値については、一致するグループの最も大きな値が使用されます。

[メンバーグループ (Member Groups)] のみが指定されている一致基準、または [その他の条件 (Other Conditions)] のみが指定されている一致基準を作成できます。[その他の条件 (Other Conditions)] のみを指定する場合、スポンサーグループのスポンサーのメンバーシップは、一致するディクショナリ属性のみに基づいて決定されます。

ステップ 4 このスポンサーグループに基づいてスポンサーが作成できるゲストタイプを指定するには、[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)] をクリックして、1 つ以上のゲストタイプを選択します。

[次の場所にゲストタイプを作成 (Create Guest Types at)] の下のリンクをクリックして、このスポンサーグループに割り当てるゲストタイプをさらに作成できます。新しいゲストタイプを作成した後、その新しいゲストタイプを選択するには、スポンサーグループを保存して閉じ、再度開いてください。

ステップ 5 [ゲストが訪問するロケーションを選択 (Select the locations that guests will be visiting)] を使用して、ゲストアカウントの作成時にスポンサーグループのスポンサーが選択できるロケーション (ゲストの時間帯の設定に使用) を指定します。

[次の場所にゲストロケーションを設定 (Configure guest locations at)] の下のリンクをクリックして、ゲストロケーションを追加することで、選択できるロケーションをさらに追加できます。新しいゲストロケーションを作成した後、その新しいゲストロケーションを選択するには、スポンサーグループを保存して閉じ、再度開いてください。

これによって、ゲストが他のロケーションからログインできなくなることはありません。

ステップ 6 スポンサーがユーザーの作成後に [通知 (Notify)] をクリックする操作を行わずにすむようにするには、[自動ゲスト通知 (Automatic guest notification)] の下の [電子メールアドレスが使用可能な場合はアカウント作成時にゲストに電子メールを自動的に送信する (Automatically email guests upon account creation if email address is available)] をオンにします。これにより、電子メールが送信されたことを示すウィンドウが表示されます。また、このオプションをオンにすると、[ゲスト通知は自動送信されました (Guest notifications are sent automatically)] というヘッダーがスポンサーポータルに追加されます。

ステップ 7 [スポンサー作成可能 (Sponsor Can Create)] で、このグループ内のスポンサーがゲストアカウントを作成するために使用できるオプションを設定します。

- [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))]: スポンサーが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るようにします。

このオプションが有効になっている場合、[インポート (Import)] オプションが [スポンサー (Sponsor)] ポータルの [アカウントの作成 (Create Accounts)] ウィンドウに表示されます。[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複数のランダムゲストアカウントを作成するか、または、または複数のアカウントをすばやく作成することができるようにします。

このオプションが有効になっている場合、[ランダム (Random)] オプションが [スポンサー (Sponsor)] 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。

- [デフォルトユーザー名プレフィックス (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ー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ー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 (Enabled)] : スポンサーは、[スポンサー (Sponsor)] 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 (Not enabled)] : スポンサーは [スポンサー (Sponsor)] 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。

ユーザー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ー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 ポータルでユーザー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ー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。

ステップ 8 [スポンサーが管理可能 (Sponsor Can Manage)] で、このスポンサー グループのメンバーが表示および管理できるゲスト アカウントを制限できます。

- [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。

ステップ 9 [スポンサーの権限 (Sponsor Can)]で、このスポンサー グループのメンバーに、ゲストのパスワードおよびアカウントに関連する追加の権限を提供できます。

- [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)]: このオプションをオンにすると、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)] ウィンドウとゲストの詳細に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、ユーザー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。
- [ゲストアカウントの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ー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。この機能では、スポンサーの ID ソースで電子メール属性が適切に設定されている必要もあります。

- [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。

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

スポンサー アカウント作成のためのアカウント コンテンツの設定

ゲストとスポンサーが新しいゲストアカウントの作成時に指定する必要があるユーザーデータのタイプを設定できます。ISE アカウントを識別するために必要なフィールドがありますが、その他のフィールドを削除し、独自のカスタム フィールドを追加することができます。

スポンサーによるアカウント作成用のフィールドを設定するには、次の手順に従います。

1. [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)] を選択し、スポンサーポータルを編集します。
2. [ポータル ページのカスタマイズ (Portal Page Customization)] タブを選択します。
3. 下にスクロールして [既知のゲストのアカウント作成 (Create Account for Known Guests)] を選択します。
4. 右側の [プレビュー (Preview)] 表示で [設定 (Settings)] を選択します。

これらの設定により、スポンサー ポータルでのゲストアカウントの作成時に表示される、ゲストアカウントに必要なフィールドが決定します。この設定は、ゲストタイプ [既知 (Known)]、[ランダム (Random)]、および [インポート (Imported)] に適用されます。新しいユーザーをインポートするためにスポンサーがダウンロードするテンプレートは動的に作成されるので、[既知のゲスト (Known Guests)] で設定したフィールドだけが含まれます。

アカウントのユーザー名とパスワードのインポート

スポンサーはユーザー名とパスワードをインポートできますが、スポンサーが CSV テンプレートをダウンロードするときにはこれらの行がテンプレートに追加されません。スポンサーはこ

これらのヘッダーを追加できます。ISE が列を認識できるように、ヘッダーの名前が正しく設定されている必要があります。

- [ユーザー名 (Username)] : *User Name* または *UserName* です。
- [パスワード (Password)] : **password** である必要があります。

スポンサー ポータルの特別な設定

次の設定は、[インポートされたゲストにアカウントを作成 (Create Account for Imported Guests)] ページ、[ポータルページのカスタマイズ (Portal Page Customizations)] タブ、スポンサー ポータルで一意です。

- [スポンサーによるゲストクレデンシャルの電子メールのコピーを許可 (Allow sponsor to be copied in Guest Credentials email)] : このオプションを有効にすると、インポートされたゲストに正常に送信されるゲストクレデンシャルの各電子メールがスポンサーにも送信されます。デフォルトでは、電子メールはスポンサーに送信されません。
- [スポンサーによるサマリーの電子メールの受信を許可 (Allow sponsor to receive summary email)] : スポンサーがユーザーリストをインポートすると、ISE はインポートされたすべてのユーザーを含むサマリーの電子メールを1つ送信します。このオプションをオフにすると、スポンサーはインポートされたユーザーごとにそれぞれ電子メールを受信します。

スポンサー ポータル フローの設定

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。

会社の営業所やその小売の場所にさまざまなブランディングがある場合、会社にさまざまな製品ブランドがある場合、または市役所が火災、警察、およびその他の部門で異なるテーマのポータルを必要とする場合は、複数のスポンサー ポータルを作成することもできます。

これらは、スポンサー ポータルの設定に関連するタスクです。

始める前に

[スポンサー グループの設定 \(41 ページ\)](#) の説明に従い、サイトの既存のスポンサー グループを設定または編集します。

-
- ステップ1 [ポリシー サービスの有効化 \(47 ページ\)](#)。
 - ステップ2 [ゲスト サービスの証明書の追加 \(47 ページ\)](#)。
 - ステップ3 [外部 ID ソースの作成 \(47 ページ\)](#)。

- ステップ4 ID ソース順序の作成 (48 ページ)。
- ステップ5 スポンサー ポータルの作成 (49 ページ)。
- ステップ6 (任意) スポンサー ポータルのカスタマイズ (50 ページ)。

ポリシー サービスの有効化

Cisco ISE エンドユーザー Web ポータルをサポートするには、ホストするノードでポータルポリシーサービスを有効にする必要があります。

-
- ステップ1 [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)] チェックボックスをオンにします。
- ステップ4 [セッションサービスの有効化 (Enable Session Services)] チェックボックスをオンにします。
- ステップ5 [Save] をクリックします。

ゲスト サービスの証明書の追加

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

外部 ID ソースの作成

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



(注) 認証済みユーザー ID を受信して共有できるようにするパッシブ ID サービスを使用するには、[その他のパッシブ ID サービス プロバイダ](#)を参照してください。

- 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 ソースとして Active Directory に接続する場合。詳細については、[外部 ID ソースとしての Active Directory](#)を参照してください。

- LDAP : LDAP ID ソースを追加する場合。詳細については、[LDAP](#)を参照してください。
- RADIUS トークン (RADIUS Token) : RADIUS トークンサーバーを追加する場合。詳細については、[RADIUS トークン ID ソース](#)を参照してください。
- RSA SecurID : RSA SecurID サーバーを追加する場合。詳細については、[RSA ID ソース](#)を参照してください。
- SAML IDプロバイダー (SAML Id Providers) : Oracle Access Manager などの ID プロバイダー (IdP) を追加する場合。詳細については、[外部 ID ソースとしての SAMLv2 ID プロバイダー](#)を参照してください。
- [ソーシャルログイン (Social Login)] : Facebook などのソーシャルログインを外部 ID ソースとして追加する場合。詳細については、[アカウント登録ゲストのソーシャルログイン \(17 ページ\)](#) を参照してください。

ID ソース順序の作成

始める前に

Cisco ISE に外部 ID ソースを設定していることを確認します。

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

ゲストユーザーがローカル WebAuth を使用して認証できるようにするには、ゲストポータル認証ソースと ID ソース順序の両方に同じ ID ストアが含まれるように設定する必要があります。

ステップ 1 [管理 (Administration)] > [ID 管理 (Identity Management)] > [ID ソース順序 (Identity Source Sequences)] > [追加 (Add)] を選択します。

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

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

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

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

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

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

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

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

スポンサー ポータルの作成

スポンサーポータルを提供して、ネットワークに接続してインターネットと内部リソースおよびサービスにアクセスするゲストのアカウントをスポンサーが作成、管理、および承認できるようにすることができます。

Cisco ISE では、別のポータルを作成する必要なく使用できるデフォルトのスポンサーポータルが用意されています。ただし、新しいスポンサー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。デフォルトのスポンサーポータル以外のすべてのポータルを削除できます。IPv6 は、スポンサーポータルのログインではサポートされていません。

[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 (Page Settings)] で行った変更は、スポンサーフロー図のグラフィカルフローに反映されます。[AUP] 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、スポンサーはポータルでそれを確認します。無効にした場合は、そのページがフローから削除され、次に有効にされたページがスポンサーに表示されます。

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 ソース、および ID ソース順序が設定されていることを確認します。

-
- ステップ1** [スポンサーポータルのポータル設定 \(89 ページ\)](#) の説明に従って、[ポータル設定 (Portal Settings)] ページを設定します。
ここで使用するポータル名が他のエンドユーザーポータルに使用されていないことを確認します。
 - ステップ2** [スポンサーポータルのログイン設定 \(92 ページ\)](#) の説明に従って、[ログイン設定 (Login Settings)] ページを設定します。
 - ステップ3** [スポンサーポータルの利用規定 \(AUP\) 設定 \(93 ページ\)](#) の説明に従って、[利用規定 (AUP) ページ設定 (Acceptable Use Policy (AUP) Page Settings)] ページを設定します。
 - ステップ4** [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 \(94 ページ\)](#) の説明に従って、[スポンサー変更パスワード設定 (Sponsor Change Password Settings)] オプションを設定します。
 - ステップ5** [スポンサーポータルのポストログインバナー設定 \(94 ページ\)](#) の説明に従って、[ポストログインバナーページ設定 (Post-Login Banner Page Settings)] ページを設定します。
 - ステップ6** ポータルをカスタマイズする場合は、[スポンサーポータルアプリケーション設定 (Sponsor Portal Application Settings)] をクリックします。
 - ステップ7** [Save] をクリックします。
-



- (注) LDAP と SAML GuestID ストアを ID ストアとして使用してスポンサーポータルにログインする場合は、スポンサーの電子メールアドレスを使用してログインすることを推奨します。スポンサー ID でログインすると、承認されたユーザーが表示できない場合があります。

スポンサー ポータルのカスタマイズ

ポータルの外観およびユーザー エクスペリエンスをカスタマイズするには、ポータル テーマをカスタマイズし、ポータル ページの UI 要素を変更して、ユーザーに表示されるエラーメッセージと通知を編集します。ポータルのカスタマイズの詳細については、[エンドユーザー Web ポータルのカスタマイズ \(106 ページ\)](#) を参照してください。

スポンサー アカウント作成のためのアカウント コンテンツの設定

ゲストとスポンサーが新しいゲスト アカウントの作成時に指定する必要があるユーザー データのタイプを設定できます。ISE アカウントを識別するために必要なフィールドがありますが、その他のフィールドを削除し、独自のカスタム フィールドを追加することができます。

スポンサーによるアカウント作成用のフィールドを設定するには、次の手順に従います。

1. [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)] を選択し、スポンサーポータルを編集します。
2. [ポータル ページのカスタマイズ (Portal Page Customization)] タブを選択します。
3. 下にスクロールして [既知のゲストのアカウント作成 (Create Account for Known Guests)] を選択します。

右側の [プレビュー (Preview)] 表示で [設定 (Settings)] を選択します。これらの設定により、スポンサーポータルでのゲストアカウントの作成時に表示される、ゲストアカウントに必要なフィールドが決定します。

この設定は、ゲスト タイプ [既知 (Known)]、[ランダム (Random)]、および [インポート (Imported)] に適用されます。新しいユーザーをインポートするためにスポンサーがダウンロードするテンプレートは動的に作成されるので、[既知のゲスト (Known Guests)] で設定したフィールドだけが含まれます。

スポンサーによるアカウントのユーザー名とパスワードのインポート

スポンサーはユーザー名とパスワードをインポートできますが、スポンサーがテンプレートをダウンロードするときにはこれらの行はテンプレートに追加されません。スポンサーはこれらのヘッダーを追加できます。Cisco ISE が列を認識できるように、ヘッダーの名前が正しく設定されている必要があります。

- [ユーザー名 (Username)] : **User Name** または **UserName** です。
- [パスワード (Password)] : パスワードです。

スポンサーに対して使用可能な時間設定項目の設定

スポンサーは新しいゲストアカウントを作成するときに、アカウントがアクティブである期間を設定します。スポンサーが使用できるオプションを設定して、スポンサーがアカウントの期間と、開始時刻および終了時刻を設定できるようにすることができます。これらのオプションはゲストタイプ別に設定されます。スポンサーに対し、[アクセス情報 (Access Information)] というヘッダーの下に結果が表示されます。

スポンサーポータルアカウント期間オプションを制御する [ゲストタイプ (Guest Type)] 設定は、[最大アクセス時間 (Maximum Access Time)] ヘッダーの下にあります。この設定について次に説明します。

- [最初のログインから (From first login)] : スポンサーポータルには、最初のログイン後にアカウントがアクティブ化されている期間が表示されます。

Access Information

Duration:*

Days (Maximum:365)

FromFirst Login

Create

ゲストタイプ設定の [最大アカウント期間 (Maximum Account Duration)] により、スポンサーがその期間に対して入力できる値が決定されます。

- [スポンサーが指定した日付から (From sponsor-specified date) (該当する場合はアカウント登録の日付)] : スポンサーは、期間を [営業日の終わり (End of business day)] として設定するか、または [営業日の終わり (End of business day)] フィールドをオフにして、期間、開始時刻、および終了時刻を設定するかを選択できます。

Access Information End of business day

23:59

Duration:*

90

Days (Maximum:365)

From Date (yyyy-mm-dd) *

2017-02-08

From Time *

10:52

To Date (yyyy-mm-dd) *

2017-05-09

To Time *

11:52

Create

期間と有効な日付を制御するゲストタイプ設定は、[アクセスを許可する日付と時刻 (Allow access only on these days and times)]ヘッダーの下にあります。

- 選択した曜日により、スポンサーのカレンダーで選択できる日付が制限されます。
- 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。

スポンサー ポータルの Kerberos 認証

Cisco ISE を設定して、Windows にログオンしているスポンサーユーザーの [スポンサー (Sponsor)]ポータルへのアクセスの認証に Kerberos を使用できます。このプロセスは、Kerberos チケットでログインしているスポンサー ユーザーの Active Directory クレデンシャルを使用します。ブラウザが Cisco ISE との SSL 接続を確立した後、セキュアなトンネル内で Kerberos SSO が実行されます。

次の項目は同じ Active Directory ドメインに存在する必要があります。

- 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

この要件は、Microsoft では Active Directory フォレスト間の双方向の信頼での Kerberos SSO がサポートされていないため必要です。

スポンサー ユーザーは、Windows にログオンする必要があります。

ゲスト ポータルの Kerberos 認証はサポートされていません。

Kerberos の設定

[スポンサー (Sponsor)] ポータルで Kerberos を有効にするには、[スポンサー設定とカスタマイズ (Sponsor Settings and Customization)] ウィンドウで [Kerberos SSO を許可する (Allow Kerberos SSO)] チェックボックスをオンにします。

スポンサーのブラウザも正しく設定されていなければなりません。次のセクションでは、各ブラウザを手動で設定する方法を説明します。



(注) Active Directory のユーザー名とユーザープリンシパル名が一致している必要があります。SSO は、ユーザーのセッションを識別するユーザープリンシパル名によって決まります。

ブラウザからスポンサーポータル FQDN を使用してスポンサーポータルにアクセスしている間、Cisco ISE は設定されたスポンサーポータル FQDN ではなく PSN FQDN に要求をリダイレクトします。

たとえば、スポンサーポータルの FQDN が `sponsor.example.com` で PSN の FQDN が `psn.example.com` の場合、ブラウザから `https://sponsor.example.com` にアクセスしようとするとき、
`https://ise.example.com:8445/sponsorportal/PortalSetup.action?portal=b7e7d773-7bb3-442b-a50b-42837c12248a` にリダイレクトされます。

この動作は、[Kerberos SSO を許可 (Allow Kerberos SSO)] オプションを有効にしているときのみ発生します。

Firefox を手動で設定するには

1. アドレス バーに `about:config` と入力します。
2. 表示される警告は無視し、クリックして続行します。
3. 検索バーで `negotiate` を検索します。
4. `network.negotiate-auth.delegation-uris` と `network.negotiate-auth.trusted-uris` に FQDN を追加します。各属性の URL の一覧はコンマで区切られます。
5. タブを閉じます。ブラウザが使用可になり、再起動は必要ありません。

Internet Explorer を手動で設定するには

1. 右上の歯車をクリックし、[インターネットオプション (Internet Options)] を選択します。
2. [セキュリティ (Security)] タブをクリックします。
3. [ローカルイントラネット (Local Intranet)] をクリックします。
4. [サイト (Sites)] をクリックし、[詳細設定 (Advanced)] をクリックします。
5. 文字列に `<mydomain>.com` を追加します (`<mydomain>` はスポンサー ポータル FQDN のワールドカード)、または FQDN を入力します。
6. [閉じる (Close)] をクリックし、[OK] をクリックします。

7. [Advanced] タブをクリックします。
8. [セキュリティ (Security)] セクションまで下方向にスクロールし、[統合 Windows 認証を有効にする (Enable Integrated Windows Authentication)] チェックボックスをオンにします。
9. コンピュータを再起動します。

Chrome は Internet Explorer から設定を取得します

トラブルシューティング

- コマンドプロンプトで `set user` を実行し、マシンが適切な AD ドメインに連結されていることを確認します。
- コマンドプロンプトで `klist` を実行し、キャッシュされた Kerberos チケットとホスト名の一覧を表示します。
- SPNEGO トークンデータを見ます。NTLM パスワードベースのトークン文字列は、Kerberos トークン文字列よりもはるかに短く、正しいトークン文字列は 1 行に収まりません。
- `kerberos` フィルタを使用して Wireshark を使用し、存在する場合は Kerberos 要求をキャプチャします。



- (注) Kerberos SSO オプションを有効にすると、ユーザーは、Kerberos SSO が正しく機能するノード FQDN でスポンサー ポータルにアクセスする必要があります。スポンサー ポータルでポータル FQDN が設定されている場合、ユーザーがポータル FQDN に接続すると、そのノード FQDN によってこのポータルにリダイレクトされます。

スポンサーがスポンサー ポータルにログインできない

問題

次のエラー メッセージは、スポンサーがスポンサー ポータルにログインしようとしたときに表示されます。

"Invalid username or password. Please try again."

原因

- スポンサーが無効なクレデンシャルを入力しました。
- スポンサーは、ユーザーレコードがデータベース (内部ユーザーまたは Active Directory) にないため無効です。
- スポンサーが属するスポンサー グループは無効です。

- スポンサーのユーザー アカウントがアクティブな/有効なスポンサー グループのメンバーではありません。これは、スポンサー ユーザーの ID グループがいずれのスポンサー グループのメンバーでもないことを意味します。
- スポンサーの内部ユーザー アカウントは無効（一時停止中）です。

ソリューション

- ユーザーのクレデンシャルを確認します。
- スポンサー グループを有効にします。
- ユーザー アカウントが無効になっている場合は復元します。
- スポンサー ユーザーの ID グループをスポンサー グループのメンバーとして追加します。

ゲストとスポンサーのアクティビティのモニター

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

オン デマンドまたはスケジュール ベースでこれらのレポートを実行できます。

-
- ステップ 1** [操作 (Operations)] > [レポート (Reports)] > [レポート (Reports)] を選択します。
 - ステップ 2** [ゲスト (Guest)] または [エンドポイントとユーザー (Endpoints and Users)] を選択して、さまざまなゲスト、スポンサー、およびエンドポイント関連のレポートを表示します。
 - ステップ 3** [フィルタ (Filters)] ドロップダウンリストを使用して検索するデータを選択します。
 - ステップ 4** データを表示する [時間範囲 (Time Range)] を選択します。
 - ステップ 5** [Run] をクリックします。
-

メトリック ダッシュボード

Cisco ISE では、Cisco ISE ホーム ページに表示されるメトリック ダッシュボードで、ネットワークの [認証されたゲスト (Authenticated Guests)] と [アクティブ エンドポイント (Active Endpoints)] を一目で確認できます。



-
- (注) ホットスポットフローの場合は、[Authenticated Guests] ダッシュレットにエンドポイントが表示されません。
-

AUP 受け入れステータス レポート

レポートを使用して、特定の期間のすべての許可および拒否された AUP 接続を追跡できます。

ゲスト アカウンティング レポート

ゲスト アカウンティング レポートは、指定された期間のゲスト ログイン履歴を表示します。このレポートは次の手順で利用できます。[操作 (Operations)] > [レポート (Reports)] > [ゲスト (Guest)] > [ゲスト アカウンティング (Guest Accounting)]

プライマリゲストレポート

プライマリゲストレポートは、さまざまなレポートからのデータを単一のビューへ結合して、複数の異なるレポートソースからデータをエクスポートできるようにします。データカラムをさらに追加したり、表示またはエクスポートしないデータカラムを削除したりできます。このレポートへのナビゲーションパスは、次のとおりです。[操作 (Operations)] > [レポート (Reports)] > [レポート (Reports)] > [ゲスト (Guest)] > [プライマリゲストレポート (Primary Guest Report)]。

このレポートはすべてのゲスト アクティビティを収集し、ゲストユーザーがアクセスした Web サイトに関する詳細を提供します。このレポートをセキュリティ監査の目的で使用して、ゲストユーザーがいつネットワークにアクセスして、何を行ったかを確認できます。アクセスした Web サイトの URL などのゲストのインターネット アクティビティを表示するには、初めに次の操作を行う必要があります。

- ゲスト トラフィックで使用するファイアウォールで次のオプションを有効にします。
 - HTTP トラフィックを検査し、Cisco ISE モニタリング ノードにデータを送信します。Cisco ISE はゲスト アクティビティ レポートに対して IP アドレスおよびアクセスした URL だけを必要とするため、可能な場合は、この情報だけが含まれるようにデータを制限します。
 - Cisco ISE モニタリング ノードに syslog を送信します。

スポンサーのログインおよび監査レポート

スポンサー ログインおよび監査レポートは、次を追跡する統合レポートです。

- スポンサー ポータルでのスポンサーによるログイン アクティビティ。
- スポンサー ポータルでスポンサーが実行したゲスト関連の操作。

ゲストおよびスポンサー ポータルの監査ロギング

ゲスト ポータルおよびスポンサー ポータルで特定のアクションが実行されると、基礎となる監査システムに監査ログ メッセージが送信されます。これらのメッセージを表示するには、**show logging application localStore/iseLocalStore.log** コマンドを使用します。

これらのメッセージを **syslog** によってモニタリング/トラブルシューティング システムおよびログ コレクタに送信するように設定することができます。モニタリング サブシステムによって、適切なスポンサー、デバイス監査ログ、およびゲストのアクティビティログにこの情報が示されます。

ゲスト ログイン フローは、ゲスト ログインが成功したか失敗したかにかかわらず、監査ログに記録されます。

ゲスト アクセス Web 認証オプション

Cisco ISE ゲスト サービスと Web 認証サービスでは、セキュアなゲストアクセスを有効にするための複数の展開オプションがサポートされています。ローカルまたは中央 Web 認証とデバイス登録 Web 認証を使用した有線または無線のゲスト接続を提供することができます。

- [中央 Web 認証 (Central WebAuth)] : すべてのゲスト ポータルに適用されます。有線および無線の両方の接続要求に対して、中央 Cisco ISE RADIUS サーバーを介した Web 認証を使用します。ゲストは、ホットスポット ゲスト ポータルでオプションのアクセス コードを入力するか、クレデンシャルを持つゲストポータルでユーザー名とパスワードを入力することにより、後で認証されます。



(注) リダイレクト時に、ブラウザが複数のタブを開いていると、Cisco ISE はすべてのタブにリダイレクトします。ユーザーはポータルにログインできますが、Cisco ISE はセッションを承認できず、ユーザーはアクセスに失敗します。この問題を回避するには、ユーザーがブラウザ上で 1 つを除くすべてのタブを閉じる必要があります。

- [ローカル Web 認証 (ローカル WebAuth)] : クレデンシャルを持つ [ゲスト (Guest)] ポータルに適用されます。ゲストは、有線接続の場合はスイッチに接続し、ワイヤレス接続の場合はワイヤレス LAN コントローラ (WLC) に接続します。ネットワークアクセスデバイス (NAD) は、認証用の Web ページにゲストを転送します。ゲストは、認証のために、クレデンシャルを持つゲスト ポータルでユーザー名とパスワードを入力します。
- [デバイス登録 Web 認証 (デバイス登録 WebAuth)] : ホットスポット ゲスト ポータルにのみ適用されます。Cisco ISE は、Web 認証の前にゲストデバイスを登録して承認します。ゲストが有線またはワイヤレス NAD に接続すると、ゲストはホットスポット ゲストポータルに転送されます。ゲストは、クレデンシャル (ユーザー名とパスワード) を入力せずにネットワークにアクセスします。

ISE Community Resource

ゲスト アクセスを提供するように Cisco ISE と Cisco ワイヤレス コントローラを設定する方法については、『[ISE Guest Access Prescriptive Deployment Guide](#)』を参照してください。

ISE のテクニカルノート『[ISE Wireless Guest Setup Guide & Wizard](#)』も参照してください。

中央 WebAuth プロセス対応の NAD

このシナリオでは、ネットワーク アクセス デバイス (NAD) で、不明なエンドポイント接続から Cisco ISE RADIUS サーバーへの新しい認証要求を作成します。これで、エンドポイントは Cisco ISE への URL-redirect を受け取ります。



- (注) webauth-vrf-aware コマンドは、IOS XE 3.7E、IOS 15.2(4)E 以降のバージョンでのみサポートされています。その他のスイッチでは、Virtual Route Forwarding (VRF) 環境での WebAuth URL リダイレクトはサポートされていません。このような場合、回避策として、トラフィックを VRF に戻すためのルートをグローバルルーティングテーブルに追加できます。

ゲストデバイスが NAD に接続されている場合、ゲストサービスのインタラクションは、ゲストポータルの中核 WebAuth のログインにつながる MAC 認証バイパス (MAB) 要求の形式を取ります。無線と有線の両方のネットワーク アクセス デバイスに適用される後続の中核 Web 認証 (中央 WebAuth) プロセスの概要は、次のとおりです。

1. ゲストデバイスは、有線接続によって NAD に接続します。ゲストデバイス上に 802.1X サプリカントはありません。
2. MAB のサービス タイプを扱う認証ポリシーにより、MAB が引き続き失敗し、中央 WebAuth ユーザー インターフェイスの URL-redirect を含む制限付きネットワーク プロファイルが返されます。
3. NAD は、Cisco ISE RADIUS サーバーに対して MAB 要求を認証するように設定されています。
4. Cisco ISE RADIUS サーバーで MAB 要求が処理されますが、ゲストデバイスのエンドポイントが見つかりません。

この MAB の失敗により、制限付きネットワーク プロファイルが適用され、プロファイル内の URL-redirect 値が access-accept で NAD に返されます。この機能をサポートするには、許可ポリシーが存在し、適切な有線または無線 MAB (複合条件下で) と、任意で「Session:Posture Status=Unknown」条件が備わっていることを確認します。NAD では、この値に基づいて、デフォルトポート 8443 のすべてのゲスト HTTPS トラフィックが URL-redirect 値にリダイレクトされます。

この場合の標準の URL 値は次のとおりです。

`https://ip:port/guestportal/gateway?sessionId=NetworkSessionId&portal=<PortalID>&action=cwa`

5. ゲストデバイスが、Web ブラウザから URL をリダイレクトするための HTTP 要求を開始します。
6. NAD により、最初の `access-accept` から返された `URL-redirect` 値に要求がリダイレクトされます。
7. CWA をアクションとしたゲートウェイ URL 値は、ゲスト ポータル ログインページにリダイレクトされます。
8. ゲストはログイン クレデンシヤルを入力してログイン フォームを送信します。
9. ゲスト サーバーはログイン クレデンシヤルを認証します。
10. フローのタイプに応じて、次の処理が実行されます。
 - クライアントプロビジョニングを実行するようにゲストポータルが設定されていない非ポストチャフロー（これ以上の検証がない認証）の場合、ゲストサーバーは CoA を NAD に送信します。この CoA により、NAD は Cisco ISE RADIUS サーバーを使用してゲストデバイスを再認証します。設定されたネットワークアクセスとともに新しい `access-accept` が NAD に返されます。クライアントプロビジョニングが未設定で、VLAN を変更する必要がある場合、ゲストポータルで VLAN IP の更新が行われます。ゲストはログインクレデンシヤルを再入力する必要はありません。初回ログイン時に入力したユーザー名とパスワードが自動的に使用されます。
 - クライアントプロビジョニングを実行するようにゲストポータルが設定されているポストチャフローの場合、ゲストデバイスの Web ブラウザに、ポストチャエージェントのインストールおよびコンプライアンスのための [クライアントプロビジョニング (Client Provisioning)] ページが表示されます。（必要に応じて、クライアントプロビジョニングリソースポリシーに「`NetworkAccess:UseCase=GuestFlow`」条件を含めることもできます）。

Linux 向けのクライアントプロビジョニングやポストチャエージェントは存在しないため、ゲストポータルはクライアントプロビジョニングポータルにリダイレクトされ、クライアントプロビジョニングポータルは元のゲスト認証サブレットにリダイレクトされます。この認証サブレットで、必要に応じて IP リリース/更新が行われてから、CoA が実行されます。

クライアントプロビジョニングポータルへのリダイレクションを使用して、クライアントプロビジョニングサービスはゲストデバイスに非永続的 Web エージェントをダウンロードし、デバイスのポストチャチェックを実行します必要に応じて、ポストチャポリシーに「`NetworkAccess:UseCase=GuestFlow`」条件を含めることもできます。

ゲストデバイスが非準拠の場合、「`NetworkAccess:UseCase=GuestFlow`」条件および「`Session:Posture Status=NonCompliant`」条件を備えた許可ポリシーが設定済みであることを確認してください。

ゲストデバイスが準拠している場合は、設定した許可ポリシーに「`NetworkAccess:UseCase=GuestFlow`」条件および「`Session:Posture Status=Compliant`」条件が含まれていることを確認してください。ここから、クライアントプロビジョニングサービスによって NAD に対して CoA が発行されます。この CoA により、NAD は Cisco ISE RADIUS サー

バーを使用してゲストを再認証します。設定されたネットワーク アクセスとともに新しい access-accept が NAD に返されます。



(注) 「NetworkAccess: UseCase=GuestFlow」は、ゲストとしてログインする Active Directory および LDAP ユーザーにも適用できます。

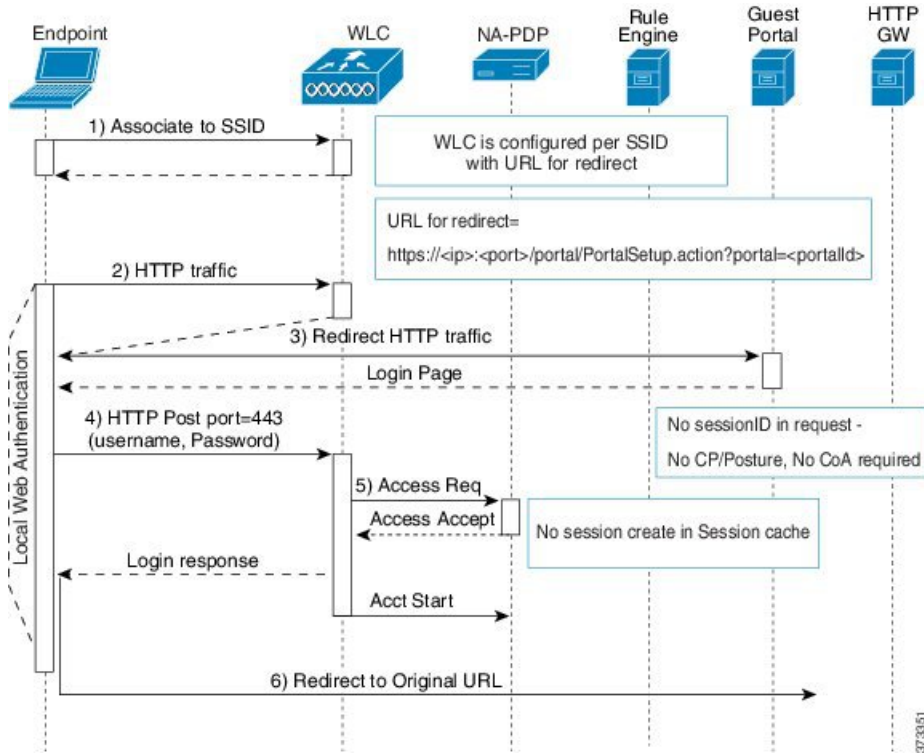
ローカル WebAuth プロセス対応のワイヤレス LAN コントローラ

このシナリオでは、ゲストがログインすると、ワイヤレス LAN コントローラ (WLC) に転送されます。その後、WLC はゲストをゲストポータルにリダイレクトします。ゲストポータルでは、ログインクレデンシャルの入力を求められ、必要に応じて利用規定 (AUP) の受け入れやパスワードの変更を実行することもできます。

完了したら、ゲストデバイスのブラウザは WLC にリダイレクトされ、POST 経由でログインクレデンシャルが提供されます。

WLC は、Cisco ISE RADIUS サーバー経由でゲストのログイン処理を行うことができます。その処理が完了したら、WLC はゲストデバイスのブラウザを元の URL の宛先にリダイレクトします。ゲストポータルの元の URL リダイレクトをサポートするためのワイヤレス LAN コントローラ (WLC) とネットワークアクセスデバイス (NAD) の要件は、リリース IOS-XE 3.6.0.E および 15.2(2)E が動作する WLC 5760 および Cisco Catalyst 3850、3650、2000、3000、および 4000 シリーズ アクセス スイッチです。

図 2: ローカル WebAuth 対応 WLC の Non-Posture フロー



ローカル WebAuth プロセス対応の有線 NAD

このシナリオでは、ゲストポータルにより、ゲストのログイン要求がスイッチ（有線 NAD）にリダイレクトされます。ログイン要求は、スイッチにポストされる HTTPS URL の形式になり、ログインクレデンシャルが含まれます。スイッチにゲストログイン要求が届くと、設定済みの Cisco ISE RADIUS サーバーを使用してゲストの認証が行われます。

1. Cisco ISE により、HTML リダイレクトを含む `login.html` ファイルを NAD にアップロードするよう要求されます。HTTPS 要求が発生すると、この `login.html` ファイルがゲストデバイスのブラウザに返されます。
2. ゲストデバイスのブラウザがゲストポータルにリダイレクトされます。ここで、ゲストのログインクレデンシャルが入力されます。
3. 利用規定（AUP）とパスワード変更が処理された後（両方ともオプションです）、ゲストポータルにより、ログインクレデンシャルをポストするゲストデバイスのブラウザが NAD にリダイレクトされます。
4. NAD により、Cisco ISE RADIUS サーバーに対して RADIUS 要求が発行され、ゲストの認証と許可が行われます。

Login.html ページに必要な IP アドレスおよびポートの値

login.html ページの次の HTML コードで、IP アドレスとポートの値を Cisco ISE ポリシー サービス ノードと同じ値に変更する必要があります。デフォルトポートは 8443 ですが、この値を変更できます。そのため、スイッチに割り当てた値が Cisco ISE の設定と一致していることを確認してください。

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
<head>
<title>ISE Guest Portal</title>
<meta Http-Equiv="Cache-Control" Content="no-cache">
<meta Http-Equiv="Pragma" Content="no-cache">
<meta Http-Equiv="Expires" Content="0">
<meta http-equiv="content-type" content="text/html; charset=UTF-8">

<meta http-equiv="REFRESH"
content="0;url=https://ip:port/portal/PortalSetup.action?switch_url=wired">

</HEAD>
<BODY>

<center>
Redirecting ... Login
<br>
<br>
<a href="https://ip:port/portal/PortalSetup.action?switch_url=wired">ISE Guest Portal</a>
</center>

</BODY>
</HTML>
```

カスタム ログイン ページはパブリック Web フォームであるため、次のガイドラインに従ってください。

- ログインフォームは、ユーザーによるユーザー名とパスワードの入力を受け付け、これらを **uname** および **pwd** として示す必要があります。
- カスタム ログイン ページは、ページタイムアウト、暗号化されたパスワード、冗長送信の防止など、Web フォームに対するベストプラクティスに従う必要があります。

NAD での HTTPS サーバーの有効化

Web ベース認証を使用するには、**ip http secure-server** コマンドを使用してスイッチ内で HTTPS サーバーを有効にする必要があります。

NAD 上でのカスタマイズされた認証プロキシ Web ページのサポート

成功、失効、失敗に関するカスタム ページを NAD にアップロードできます。Cisco ISE では特定のカスタマイズは必要ないため、NAD に付属する標準の設定手順を使用して、これらのページを作成できます。

NAD の Web 認証の設定

デフォルトの HTML ページをカスタム ファイルで置き換えて、NAD における Web 認証を完了する必要があります。

始める前に

Web ベースの認証中、スイッチのデフォルト HTML ページの代わりに使用する 4 つの代替 HTML ページを作成します。

ステップ 1 カスタム認証プロキシ Web ページを使用するように指定するには、最初にカスタム HTML ファイルをスイッチのフラッシュ メモリに格納します。スイッチのフラッシュ メモリに HTML ファイルをコピーするには、スイッチで次のコマンドを実行します。

copy tftp/ftp flash

ステップ 2 スイッチに HTML ファイルをコピーした後、グローバル コンフィギュレーション モードで次のコマンドを実行します。

ip admission proxy http login page file device:login-filename	スイッチのメモリ ファイル システム内で、デフォルトのログインページの代わりに使用するカスタム HTML ファイルの場所を指定します。device: はフラッシュ メモリです。
ip admission proxy http success page file device:success-filename	デフォルトのログイン成功ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
ip admission proxy http failure page file device:fail-filename	デフォルトのログイン失敗ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
ip admission proxy http login expired page file device:expired-filename	デフォルトのログイン失効ページの代わりに使用するカスタム HTML ファイルの場所を指定します。

ステップ 3 スイッチによって提供されるガイドラインに従って、カスタマイズされた認証プロキシ Web ページを設定します。

ステップ 4 次の例に示すように、カスタム認証プロキシ Web ページの設定を確認します。

```
Switch# show ip admission configuration
Authentication proxy webpage
  Login page           : flash:login.htm
  Success page        : flash:success.htm
  Fail Page           : flash:fail.htm
  Login expired Page  : flash:expired.htm

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
```

```
Authentication Proxy Auditing is disabled  
Max Login attempts per user is 5
```

デバイス登録 WebAuth プロセス

デバイス登録 Web 認証（デバイス登録 WebAuth）およびホットスポット ゲスト ポータルを使用すると、ユーザー名とパスワードを要求しないで、プライベートネットワークへの接続をゲスト デバイスに許可できます。

このシナリオでは、ゲストは無線接続でネットワークに接続します。デバイス登録 WebAuth プロセス フローの例については、[図 3: ワイヤレス デバイス登録 Web 認証フロー](#)を参照してください。

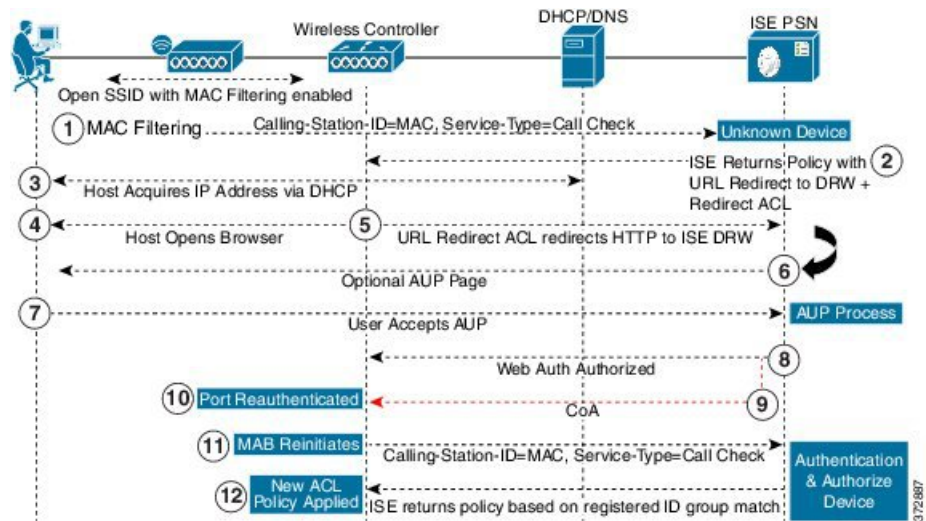
後続のデバイス登録 WebAuth プロセスの概要を次に説明します。無線接続と有線接続の両方で同様のプロセスとなります。

1. ネットワーク アクセス デバイス（NAD）がホットスポット ゲスト ポータルにリダイレクトを送信します。
2. ゲスト デバイスの MAC アドレスがいずれのエンドポイント ID グループにも含まれていないか、利用規定（AUP） accepted 属性が true に設定されていない場合、Cisco ISE は許可プロファイルに指定された URL リダイレクションを使用して応答します。
3. ゲストが何らかの URL にアクセスしようとする、URL リダイレクションによって AUP ページ（有効な場合）が示されます。
 - ゲストが AUP を受け入れると、デバイスの MAC アドレスに関連付けられたエンドポイントが、設定されたエンドポイント ID グループに割り当てられます。ゲストによる AUP の受け入れを追跡できるよう、この時点で、このエンドポイントの AUP accepted 属性は true に設定されます。
 - ゲストが AUP を受け入れない場合、または、エンドポイントの作成中や更新中などにエラーが発生した場合、エラー メッセージが表示されます。
4. ホットスポット ゲスト ポータルの設定に基づいて、追加情報を含むポスト アクセス バナー ページが表示される場合があります（有効な場合）。
5. エンドポイントが作成または更新された後、許可変更（CoA）終了が NAD に送信されます。
6. CoA の後、NAD は MAC 認証バイパス（MAB）の新しい要求でゲスト接続を再認証します。新規認証では、エンドポイントとそれに関連付けられているエンドポイント ID グループが検索され、設定されているアクセスが NAD に返されます。
7. ホットスポット ゲスト ポータルの設定に基づいて、ゲストは、アクセスを要求した URL、管理者が指定したカスタム URL、または認証の成功ページに誘導されます。

有線とワイヤレスのどちらの場合も、CoA タイプは Termination CoA です。VLAN DHCP リリース（および更新）を実行するようにホットスポットゲストポータルを設定し、それによって、有線と無線の両方の CoA タイプを許可変更に変更再許可できます。

VLAN DHCP リリースのサポートは、Windows デバイスのみで使用可能です。モバイルデバイスでは利用できません。登録するデバイスがモバイルで、[VLAN DHCP リリース (VLAN DHCP Release)] オプションが有効の場合、ゲストは手動で IP アドレスを更新することを要求されます。モバイルデバイスのユーザーの場合は、VLAN を使用するよりも、WLC でアクセスコントロールリスト (ACL) を使用することを推奨します。

図 3: ワイヤレス デバイス登録 Web 認証フロー



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、次のとおりです。[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)] を選択します。

- [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 (Blacklist)]、[個人所有デバイス持ち込み (BYOD) (Bring Your Own Device (BYOD))]、[クライアントプロビジョニング (Client Provisioning)]、[モバイルデバイス管理 (MDM) (Mobile Device Management (MDM))]、または [デバイス (My Devices)] 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)] : オプションです。
- [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。



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

- [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、特定のブラウザロケール設定へのマッピングと、その言語でのポータル全体のすべての文字列設定が含まれています。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ー 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)] > [ポータル動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ポータル設定 (Portal Settings)] 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 (Blacklist)] ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このウィンドウで変更を加えるまで維持されます。このウィンドウを変更する場合は、この制限に従うようにポート設定を更新します。

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

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

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

- スポンサーポータルを例として使用した有効な組み合わせを次に示します。
 - スポンサーポータル : ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイスポータル : ポート **8443**、インターフェイス **0**、証明書グループ **A**
 - スポンサーポータル : ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイスポータル : ポート **8445**、インターフェイス **0**、証明書グループ **B**
 - [スポンサー (Sponsor)] 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 (Blacklist)] 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 (Sponsor)] 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 (Blacklist)] ポータル : ポート **8444**、インターフェイス **0**、証明書グループ **A**



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

- [使用可能インターフェイス (Allowed Interfaces)] : PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネットインターフェイスを設定する必要があります。

これらのインターフェイスは、ポリシーサービスがオンになっているすべての PSN (VM ベースを含む) で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

- イーサネットインターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
- ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため必須です。
- ポータルの証明書のサブジェクト名またはサブジェクトの代替名はインターフェイス IP アドレスに解決する必要があります。
- ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリインターフェイスの IP アドレスを FQDN にマッピングします。これは、証明書のサブジェクト名、またはサブジェクトの代替名と一致させるために使用されます。
- ボンディングされた NIC のみが選択されている場合は、PSN はポータルの設定時に、最初にボンディングインターフェイスの設定を試みます。これが成功しない場合、おそらく、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
- NIC チーミングまたはボンディングは、ハイアベイラビリティ (耐障害性) を実現するために 2 つの個別の NIC を設定できる設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC が [ポータル設定 (Portal Settings)] に基づいてポータルに選択されます。物理 NIC と対応するボンディングされた NIC の両方が設定されている場合は、PSN がポータルを設定しようとする、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せん。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 データベースからデバイスが消去されるまでの日数を指定します。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。ブラウザのロケールの言語が Cisco ISE でサポートされていない場合は、[フォールバック言語 (Fallback Language)] が言語ポータルとして使用されます。
- [フォールバック言語 (Fallback Language)]: ブラウザロケールから言語を取得できない場合、またはブラウザロケール言語が Cisco ISE でサポートされていない場合に使用する言語を選択します。
- [常に使用 (Always Use)]: ポータルに使用する表示言語を選択します。この設定は、ユーザーの [ブラウザのロケールを使用する (User Browser Locale)] オプションを上書きします。

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)]>[アクセプタブルユースポリシー (AUP) ページ設定 (Acceptable Use Policy (AUP) Page Settings)]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ーに表示します。

- [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ー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) : ユーザーが AUP を完全に読んだことを確認します。[同意 (Accept)] ボタンは、ユーザーが 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 がユーザー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。

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にのみ表示されます。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

これらの設定へのナビゲーションパスは、次のとおりです。[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)] 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 (Blacklist)] ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このウィンドウで変更を加えるまで維持されます。このウィンドウを変更する場合は、この制限に従うようにポート設定を更新します。

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

ポス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 (Sponsor)] 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 (Blacklist)] 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 (Sponsor)] 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 (Blacklist)] ポータル : ポート **8444**、インターフェイス **0**、証明書グループ **A**



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

- [使用可能インターフェイス (Allowed Interfaces)] : PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネットインターフェイスを設定する必要があります。

これらのインターフェイスは、ポリシーサービスがオンになっているすべての PSN (VM ベースを含む) で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

- イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
- ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため必須です。
- ポータルの証明書のサブジェクト名またはサブジェクトの代替名はインターフェイス IP アドレスに解決する必要があります。
- ISE CLI で **ip host x.x.x.yyy.domain.com** を設定して、セカンダリインターフェイスの IP アドレスを FQDN にマッピングします。これは、証明書のサブジェクト名、またはサブジェクトの代替名と一致させるために使用されます。
- ボンディングされた NIC のみが選択されている場合は、PSN はポータルの設定時に、最初にボンディングインターフェイスの設定を試みます。これが成功しない場合、おそらく、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 チューニングまたはボンディングは、ハイアベイラビリティ (耐障害性) を実現するために 2 つの個別の NIC を設定できる 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC が [ポータル設定 (Portal Settings)] に基づいてポータルに選択されます。物理 NIC と対応するボンディングされた NIC の両方が設定されている場合は、PSN がポータルを設定しようとする、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ます。
- ポータルの証明書のサブジェクト名またはサブジェクトの代替名はインターフェイス IP アドレスに解決する必要があります。
- [認証方式 (AuthenticationMethod)] : ユーザー認証に使用する ID ソース順序 (ISS) または ID プロバイダー (IdP) を選択します。ID ソース順序は、ユーザー 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。

Cisco ISE には、スポンサーポータル Sponsor_Portal_Sequence 用のデフォルトの 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 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 管理 (Identity Management)] > [ID ソース順序 (Identity Source Sequences)] を選択します。

• 表示言語

- [ブラウザのロケールを使用する (Use Browser Locale)] : クライアントブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザのロケールの言語が Cisco ISE でサポートされていない場合は、[フォールバック言語 (Fallback Language)] が言語ポータルとして使用されます。
- [フォールバック言語 (Fallback Language)] : ブラウザロケールから言語を取得できない場合、またはブラウザロケール言語が Cisco ISE でサポートされていない場合に使用する言語を選択します。
- [常に使用 (Always Use)] : ポータルに使用する表示言語を選択します。この設定は、ユーザーの [ブラウザのロケールを使用する (User Browser Locale)] オプションを上書きします。

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)] を選択します。

- [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ー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。

- [レート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。

- [レート制限時のログイン試行間隔 (Time Between Login Attempts when Rate Limiting)] : [レート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、ユーザー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)] : フローにアクセプタブルユース ポリシー ウィンドウを追加します。AUP をウィンドウに追加したり、別のウィンドウへのリンクを設定することができます。
- [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。

- [ゲストにパスワードのリセットを許可 (Allow Guests to Recover the Password)] : このオプションは、アカウント登録ゲストに対し、ゲストポータルの [パスワードのリセット (Reset Password)] ボタンを有効にします。有効なアカウントを持つアカウント登録ゲストがログインポータルに接続し、パスワードを忘れた場合は、[パスワードのリセット (Reset Password)] をクリックできます。これにより、ゲストは自分の電話番号または電子メール (いずれかを登録に使用) を入力できるアカウント登録ウィンドウに戻ります。
- [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ーのログイン 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、ユーザーは 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ーに通知し、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、ゲストが必要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。



(注) ゲストポータルからログインした内部ユーザーは、パスワードをリセットできません。

- [ログインに次の ID プロバイダー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 プロバイダーを選択すると、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、ユーザー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、ユーザーログインにソーシャルメディアタイプを使用します。ソーシャルログインの設定の詳細については、[アカウント登録ゲストのソーシャルログイン \(17 ページ\)](#) を参照してください。

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、次のとおりです。[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 (Portal & Components)]> [ゲストポータル (Guest Portals)]> [作成、編集または複製 (Create, Edit or Duplicate)]> [ポータルの動作とフローの設定 (Portal Behavior and Flow Settings)]> [アカウント登録ページの設定 (Self-Registration Page Settings)]。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。

- [ゲストタイプへのアカウント登録ゲストの割り当て (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の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須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、[含めるフィールド (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す。そのため、このフィールドを使用する場合には、このフィールドに入力する情報についてゲストに説明してください。
- [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。追加のカスタムフィールドを追加するには、[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)] でこれらのフィールドを作成します。
- [AUP を含める (Include an AUP)] : 会社のネットワークの使用についての諸条件を、現在ユーザー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)] : ユーザーが 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、ユーザーが 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) のブロック済み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。
 - [アカウント登録したゲストにスポンサーの承認後に自動ログインを許可 (Allow guests to login automatically from self-registration after sponsor's approval)] : アカウント登録ゲストは、スポンサーの承認後に自動的にログインします。
 - [承認要求電子メール送信先 (Email approval request to)] :
 - [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、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、[含めるフィールド (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/拒否リンクの設定 (Approve/Deny Link Settings)] :
 - [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 ユーザーであり、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)] ウィンドウに誘導します。このウィンドウには、[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 (このウィンドウで有効になっている場合) であるか、またはこのウィンドウ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ウィンドウ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)] ウィンドウが表示された後にポータルログイン ウィンドウに誘導されます。

- [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ウィンドウに再び誘導し、「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。(Please wait for your guest credentials to be delivered either via email, SMS, or print format and proceed with logging in)」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 (このウィンドウで有効になっている場合) であるか、またはこのウィンドウ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 (このウィンドウで有効になっている場合) であるか、またはこのウィンドウ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ヤ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 サービスプロバイダー (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、次のとおりです。[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)] > [ポータルの動作とフローの設定 (Portal Behavior and Flow Settings)] > [アカウント登録成功ページ設定 (Self Registration Success Page Settings)]。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ヤルを通知します。

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)	[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。 スポンサーによるゲストの承認が必要ない場合は、[ユーザー名 (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ヤルを表示します。スポンサーの承認が必要な場合、クレデンシヤルはゲストが承認された後に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。
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)	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ヤ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]。
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))	会社のネットワーク使用の諸条件を、現在ユーザーに表示されているウィンドウ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。

フィールド	使用上のガイドライン
[同意が必要 (Require Acceptance)]	ユーザーのアカウントが完全に有効になる前に、ユーザーはAUPに同意する必要があります。[ログイン (Login)]ボタンは、ユーザーがAUPを受け入れない場合は有効になりません。ユーザーが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。 ユーザーがAUPを最後まで読んだことを確認します。[同意 (Accept)]ボタンは、ユーザーがAUPの最後までスクロールすると有効になります。
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

- [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ーに表示します。
- [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)] を有効にした場合にのみ、このオプションが表示されます。

ユーザーが AUP を最後まで読んだことを確認します。[同意 (Accept)] ボタンは、ユーザーが 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 がユーザー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)]: ユーザー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)]: ユーザー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ー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、次のとおりです。[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)]。

- [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。



(注) ゲストポータルからログインした内部ユーザーは、パスワードをリセットできません。

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)]> [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 [BYOD の登録 (BYOD Registration)] ウィンドウを追加して、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ブ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、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 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。</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 をユーザーに表示します。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ーのブラウザを、ユーザー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。使用できない場合は、[認証成功 (Authentication Success)] ウィンドウが表示されます。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 Cisco ISE で設定された認証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、ユーザー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、次のとおりです。[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)] > [ポータルの動作とフローの設定 (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)]。

これらの設定を使用して、正常なログイン後にユーザー（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)	ユーザー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、次のとおりです。[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)] > [ポータルの動作とフローの設定 (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)]。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)] : ゲストをポスチャエ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、次のとおりです。[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)]を選択します。

- [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 サーバーが 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、ユーザー (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ーのブラウザを、ユーザー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。使用できない場合は、[認証成功 (Authentication Success)] ウィンドウが表示されます。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 (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。

- [認証の成功 (Authentication Success)] ページ : ユーザー認証成功の通知。
- URL : ネットワークへの認証に成功すると、ユーザー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、次のとおりです。[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)] > [ポータルの動作とフローの設定 (Portal Behavior and Flow Settings)] > [サポート情報ページの設定 (Support Information Page Settings)]。

これらの設定を使用して、ヘルプデスクがユーザー (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 (Contact Us)] 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 Address	[サポート情報 (Support Information)] ウィンドウにデバイスのMACアドレスを含めます。
IP Address	[サポート情報 (Support Information)] ウィンドウにデバイスのIPアドレスを含めます。
ブラウザ ユーザー エージェント	[サポート情報 (Support Information)] ページに、要求の発信元の製品名とバージョン、レイアウトエンジン、ユーザーエージェントのバージョンなど、ブラウザの詳細を含めます。
ポリシー サーバー	[サポート情報 (Support Information)] ウィンドウに、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)] を選択します。
[フィールドを非表示にする (Hide Field)]	含める情報が存在しない場合、[サポート情報 (Support Information)] ウィンドウ上の該当するフィールドの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)] ウィンドウに表示します。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)]	含める情報が存在しない場合、[サポート情報 (Support Information)] ウィンドウ上の選択されているすべてのフィールドにこのテキストが表示されます。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、次のとおりです。[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)] を選択します。

- [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 (Blacklist)]、[個人所有デバイス持ち込み (BYOD) (Bring Your Own Device (BYOD))]、[クライアントプロビジョニング (Client Provisioning)]、[モバイルデバイス管理 (MDM) (Mobile Device Management (MDM))]、または [デバイス (My Devices)] 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)] : オプションです。
- [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。



Note

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

- [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、特定のブラウザロケール設定へのマッピングと、その言語でのポータル全体のすべての文字列設定が含まれています。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ー 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 (Blacklist)] ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このウィンドウで変更を加えるまで維持されます。このウィンドウを変更する場合は、この制限に従うようにポート設定を更新します。

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

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

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

- スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
 - スポンサー ポータル : ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル : ポート **8443**、インターフェイス **0**、証明書グループ **A**
 - スポンサー ポータル : ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル : ポート **8445**、インターフェイス **0**、証明書グループ **B**

- [スポンサー (Sponsor)]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 (Blacklist)]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 (Sponsor)]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 (Blacklist)]ポータル : ポート **8444**、インターフェイス **0**、証明書グループ **A**



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

- [使用可能インターフェイス (Allowed Interfaces)] : PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。

これらのインターフェイスは、ポリシーサービスがオンになっているすべての PSN (VM ベースを含む) で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

- イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
- ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため必須です。
- ポータルの証明書のサブジェクト名またはサブジェクトの代替名はインターフェイス IP アドレスに解決する必要があります。
- ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリインターフェイスの IP アドレスを FQDN にマッピングします。これは、証明書のサブジェクト名、またはサブジェクトの代替名と一致させるために使用されます。
- ボンディングされた NIC のみが選択されている場合は、PSN はポータルの設定時に、最初にボンディングインターフェイスの設定を試みます。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記

録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。

- NIC チューニングまたはボンディングは、ハイアベイラビリティ（耐障害性）を実現するために 2 つの個別の NIC を設定できる 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC が [ポータル設定 (Portal Settings)] に基づいてポータルに選択されます。物理 NIC と対応するボンディングされた NIC の両方が設定されている場合は、PSN がポータルを設定しようとする、最初にボンディング インターフェイスへ接続しようとする。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する。
 - [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 (Sponsor)] ポータルまたは [デバイス (MyDevices)] ポータルの固有の FQDN またはホスト名を 1 つの以上入力します。たとえば、**sponsorportal.yourcompany.com, sponsor** と入力することで、ユーザーはブラウザにこれらのいずれかを入力すると、が表示されます。カンマを使用して名前を区切りませんが、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 のローカルサーバー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。[Kerberos SSO を許可 (Allow Kerberos SSO)] オプションがスポンサーポータルで有効になっている場合は、ポータルで使用されるローカルサーバー証明書の SAN 属性に Cisco ISE PSN の FQDN またはワイルドカードを含める必要があります。
 - [認証方式 (AuthenticationMethod)] : ユーザー認証に使用する ID ソース順序 (ISS) または ID プロバイダー (IdP) を選択します。ID ソース順序は、ユーザー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。

Cisco ISE には、スポンサーポータル Sponsor_Portal_Sequence 用のデフォルトの 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 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 管理 (Identity Management)] > [ID ソース順序 (Identity Source Sequences)] を選択します。

- [アイドルタイムアウト (Idle Timeout)] : ポータルにアクティビティがない場合にユーザー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。

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。ブラウザのロケールの言語が Cisco ISE でサポートされていない場合は、[フォールバック言語 (Fallback Language)] が言語ポータルとして使用されます。
- [フォールバック言語 (Fallback Language)] : ブラウザロケールから言語を取得できない場合、またはブラウザロケール言語が Cisco ISE でサポートされていない場合に使用する言語を選択します。
- [常に使用 (Always Use)] : ポータルに使用する表示言語を選択します。この設定は、ユーザーの [ブラウザのロケールを使用する (User Browser Locale)] オプションを上書きします。
- [ス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。

- [レート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。
- [レート制限時のログイン試行間隔 (Time Between Login Attempts when Rate Limiting)] : [レート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、ユーザー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)] : フローにアクセプタブルユース ポリシー ウィンドウを追加します。AUP をウィンドウに追加したり、別のウィンドウへのリンクを設定することができます。

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、次のとおりです。[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 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)]> [アクセプタブルユース ポリシー (AUP) ページ設定 (Acceptable Use Policy (AUP) Page Settings)]。

これらの設定を使用して、ユーザー (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 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ーに表示します。
AUP の最後までスクロールが必要 (Require scrolling to end of AUP)	ユーザーが AUP を最後まで読んだことを確認します。[同意 (Accept)] ボタンは、ユーザーが AUP の最後までスクロールすると有効になります。
[初回ログイン時のみ (On First Login only)]	ユーザー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)]	ユーザー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))]	ユーザー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

スポンサーポータルを使用してスポンサーのパスワード要件を設定するには、[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)] > [ポータルの動作とフローの設定 (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)] 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ー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、次のとおりです。[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 (Portal s & 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)] > [ポータルの動作とフローの設定 (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)]。

これらの設定を使用して、正常なログイン後にユーザー (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)	ユーザー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 ポータルの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、次のとおりです。[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 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)]。

これらの設定を使用して、ヘルプデスクがユーザー（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 (Contact Us)] などの情報へのリンクを表示します。
MAC Address	[サポート情報 (Support Information)] ウィンドウにデバイスの MAC アドレスを含めます。
IP Address	[サポート情報 (Support Information)] ウィンドウにデバイスの IP アドレスを含めます。
ブラウザ ユーザー エージェント	[サポート情報 (Support Information)] ページに、要求の発信元の製品名とバージョン、レイアウトエンジン、ユーザーエージェントのバージョンなど、ブラウザの詳細を含めます。
ポリシー サーバー	[サポート情報 (Support Information)] ウィンドウに、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)] を選択します。
[フィールドを非表示にする (Hide Field)]	含める情報が存在しない場合、[サポート情報 (Support Information)] ウィンドウ上の該当するフィールドの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)] ウィンドウに表示します。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。

フィールド	使用上のガイドライン
[デフォルト値でラベルを表示 (Display Label with Default Value)]	含める情報が存在しない場合、[サポート情報 (Support Information)]ウィンドウ上の選択されているすべてのフィールドにこのテキストが表示されます。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ー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。

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、およびユーザー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 サーバーおよび 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したら、特定の [**ゲスト (Guest)**] ポータルと [**スポンサー (Sponsor)**] 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を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 \(10 ページ\)](#) を参照してください。
- [**カスタムフィールド (Custom Fields)**] : ユーザー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 \(11 ページ\)](#) 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 サーバーの指定 \(12 ページ\)](#) を参照してください。
- [**ゲストのロケーションと 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 \(12 ページ\)](#) を参照してください。
- [**ゲストユーザー名ポリシー (Guest Username Policy)**] : ゲストユーザー名の作成方法を設定します。詳細については、[ゲストユーザー名ポリシーの設定 \(15 ページ\)](#) および [ゲストパスワードポリシーのルール \(14 ページ\)](#) 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 (Guest)**] ポータルと [**スポンサー (Sponsor)**] 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 \(14 ページ\)](#) を参照してください。
- [**ロギング (Logging)**] : ゲストユーザーは、デバイスの MAC アドレスで追跡されます。ゲストユーザーがレポートに表示される場合、ユーザー名は MAC アドレスです。このオプションを選択すると、ユーザー名として MAC アドレスではなく、ポータルユーザー

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、[ゲストユーザー情報を保存 \(37 ページ\)](#) 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。
- [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 \(140 ページ\)](#) 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)] オプションをクリックして、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)

- [アカウント有効期間の開始 (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、ゲストユーザー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。ゲストユーザー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ーのアカウントは、ユーザー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。

- [最大アカウント有効期間 (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 分ごとに行われるため、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 \(51 ページ\)](#) 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ーが同時に実行できる最大ユーザー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ー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ーをリダイレクトする (Redirect user to a portal page showing an error message)] を選択する場合、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ー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)] ウィンドウの [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)] : ログイン情報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) サプリカントまたは 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ーに許可します。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、ユーザー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。
- [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、次のとおりです。[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)] > [スポンサーグループ (Sponsor Groups)]。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 (Sponsor)] 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)] をクリックし、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、使用可能なユーザー 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め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。内部ユーザー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ー 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ー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 (Sponsor)]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)]>[ページのカスタマイズ (Page Customization)]>[アカウントの作成 (Create Accounts)]>[ゲストタイプ (Guest Types)]>[設定 (Settings)]を選択します。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)] : アカウントを作成中にゲストに割り当てることができるロケーションを選択します。これは、これらのゲストアカウントの有効なタイムゾーンを定義し、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。これにより、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))] : スポンサーが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るようになります。

このオプションが有効になっている場合、[インポート (Import)]オプションが[スポンサー (Sponsor)]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のみで使用可能です (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になっている場合、[ランダム (Random)] オプションが [スポンサー (Sponsor)] ポータルの [アカウントの作成 (Create Accounts)] ページに表示されません。

- [デフォルトユーザー名プレフィックス (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ー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ー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 (Enabled)]: スポンサーは、[スポンサー (Sponsor)] 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 (Not enabled)]: スポンサーは [スポンサー (Sponsor)] 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。

ユーザー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ー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ー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ー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)]: スポンサーが作成されている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る日数を指定します。

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ドレスに基づいて、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)]: このオプションをオンにすると、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)]ウィンドウとゲストの詳細に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、ユーザー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。
- [ゲストアカウントの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ー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。この機能では、スポンサーの ID ソースで電子メール属性が適切に設定されている必要もあります。
- [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。

エンドユーザー ポータル

Cisco ISE では、Web ベースのポータルをエンドユーザーの 3 つのプライマリ セットに対して提供しています。

- ゲストポータル (ホットスポットと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一時的にアクセスする必要があるゲスト。
- スポンサー ポータルを使用してゲスト アカウントを作成および管理できるスポンサーとして指定されている従業員。
- 個人所有デバイスの持ち込み (BYOD) 、モバイルデバイス管理 (MDM) 、デバイスポータルなどのさまざまな非ゲストポータルを使用して、企業ネットワークでパーソナルデバイスを使用している従業員。

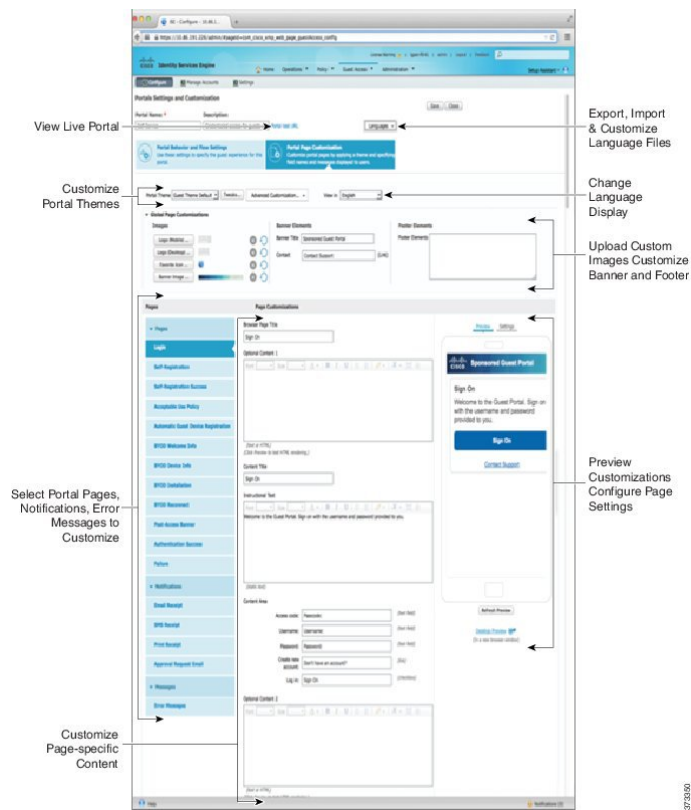
エンドユーザー Web ポータルのカスタマイズ

さらにポータルを編集、複製、作成できます。ポータルの外観を完全にカスタマイズし、その結果として、ポータルのエクスペリエンスをカスタマイズすることもできます。他のポータルへの影響なく、各ポータルを個別にカスタマイズできます。

ポータル全体またはポータルの特定のページに適用される、次のようなポータルインターフェイスのさまざまな側面をカスタマイズできます。

- テーマ、イメージ、色、バナー、およびフッター
- ポータルテキスト、エラーメッセージ、および通知の表示に使用される言語
- タイトル、コンテンツ、手順、およびフィールドとボタンのラベル
- 電子メール、SMS、およびプリンタでゲストに送信される通知（アカウント登録ゲストポータルとスポンサーポータルにのみ該当）
- ユーザーに表示されるエラーメッセージと情報メッセージ
- アカウント登録ゲストポータルとスポンサーポータルの場合は、カスタムフィールドを作成して必要に応じた固有のゲスト情報を収集できます。

図 4: カスタマイズ用のポータルページのレイアウト



ISE コミュニティ リソース

Web ポータルのカスタマイズの詳細については、「[ISE Portal Builder](#)」および「[HowTo: ISE Web Portal Customization Options](#)」を参照してください。

カスタマイズ方法

エンドユーザーのポータルページをカスタマイズする方法は複数あり、それぞれ異なるレベルの知識が必要です。

- **基本**：ポータルの [カスタマイズ (Customization)] ページを変更できます。
 - バナーとロゴのアップロード
 - 一部の色の変更 (ボタンを除く)
 - 画面のテキスト、およびポータル全体で使用される言語の変更
- **中間**
 - ミニエディタを使用した HTML および Javascript の追加。



(注) ミニエディタに HTML を入力する前に、[HTML] アイコンをクリックします。

- jQuery mobile theme roller を使用したすべてのページ要素の色の変更
- **[Advanced]**
 - プロパティおよび CSS ファイルの手動による変更。

ポータルをカスタマイズした後、それを複製して (同じタイプの) 複数のポータルを作成できます。たとえば、1つの業務エンティティのホットスポットゲストポータルをカスタマイズした場合、それを複製し、少し変更して他の業務エンティティのカスタムホットスポットゲストポータルを作成することができます。

ミニエディタを使用してポータルをカスタマイズするためのヒント

- ミニエディタのボックス内のワードが長いと、ポータルの画面領域のスクロールがオフになる場合があります。HTML 段落属性 `style="word-wrap: break-word"` を使用して改行します。次に例を示します。

```
<p style="word-wrap:break-word">
```

```
thisisaverylonglineoftextthatwillexceedthewidthoftheplacethatyouwanttoputitsousethisstructure
```

```
</p>
```

- HTML または javascript を使用してポータル ページをカスタマイズする場合は、必ず有効な構文を使用してください。Cisco ISE は、ミニエディタに入力したタグやコードを検証しません。無効な構文が原因でポータル フロー時に問題が発生する場合があります。

ポータルコンテンツのタイプ

Cisco ISE では、「そのまま」使用するか、または新しいカスタム ファイルを作成するためのモデルとして既存の CSS ファイルを使用することでカスタマイズできる、ポータルテーマのデフォルトセットが提供されます。ただし、カスタマイズされた CSS ファイルを使用しないでポータルの外観を変更することもできます。

たとえば、独自の企業ロゴやバナーイメージを使用する場合は、単にこれらの新しいイメージ ファイルをアップロードして使用することができます。ポータルのさまざまな要素および領域の色を変更することによって、デフォルトのカラースキームをカスタマイズできます。カスタム変更時に、カスタム変更を表示する言語を選択することもできます。

ロゴおよびバナーを置き換えるための画像を設計するときは、画像のサイズを次のピクセルサイズに可能な限り近づけてください。

バナー	1724 X 133
デスクトップのロゴ	86 X 45
モバイルのロゴ	80 X 35

ISE はポータルに合わせて画像のサイズを変更しますが、画像が小さすぎるとサイズ変更後に正しく表示されない場合があります。

高度なカスタマイズ（ページレイアウトの変更、ポータル ページへのビデオ クリップや広告の追加など）を行うには、独自のカスタム CSS ファイルを使用できます。

特定のポータルでのこのようなタイプの変更は、そのポータルのすべてのページにグローバルに適用されます。ページレイアウトの変更は、ポータル内にグローバルに、または特定の 1 ページのみに適用することができます。

ポータル ページのタイトル、コンテンツ、およびラベル

エンドユーザー Web ポータル ページでゲストに表示されるタイトル、テキスト ボックス、手順、フィールドとボタンのラベル、その他の視覚要素をカスタマイズすることができます。ページをカスタマイズするときには、ページ設定を動的に編集することができます。

これらの変更は、カスタマイズしている特定のページにのみ適用されます。

ポータルの基本的なカスタマイズ

ニーズに最適な事前定義済みテーマを選択し、デフォルト設定のほとんどを使用します。その後、次のような基本的なカスタマイズが可能です。

- [ポータルテーマカラーの変更 \(109 ページ\)](#)
- [ポータルアイコン、イメージ、およびロゴの変更 \(110 ページ\)](#)
- [ポータルバナーおよびフッター要素の更新 \(111 ページ\)](#)
- [ポータル表示言語の変更 \(110 ページ\)](#)
- [タイトル、手順、ボタン、およびラベルテキストの変更 \(112 ページ\)](#)
- [テキストボックスの内容のフォーマットおよびスタイル \(112 ページ\)](#)



ヒント 更新するときに、[カスタマイズの参照 \(118 ページ\)](#) を行うことができます。

ポータルテーマカラーの変更

デフォルトポータルテーマのデフォルトカラースキームをカスタマイズして、ポータルさまざまな要素と領域の色を変更できます。これらの変更は、カスタマイズしているポータル全体に適用されます。

ポータル色を変更する場合は、次のことに注意してください。

- このオプションを使用して、このポータルで使用するためにインポートしたカスタムポータルテーマのカラースキームを変更することはできません。その色の設定を変更するには、カスタムテーマ CSS ファイルを編集する必要があります。
- ポータルテーマカラーを変更した後で、[ポータルテーマ (Portal Theme)] ドロップダウンメニューから別のポータルテーマを選択した場合、元のポータルテーマの変更は失われ、デフォルトカラーに戻ります。
- 変更済みのカラースキームを使用してポータルテーマカラーを調整し、保存する前に色をリセットした場合、カラースキームはデフォルトカラーに戻り、前の変更はすべて失われます。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、[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)] > [設定 (Configure)] > [ゲストポータル (Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサーポータルの場合、[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 (Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [ポータルテーマ (Portal Theme)] ドロップダウンリストからデフォルトテーマの 1 つを選択します。

ステップ3 [調整 (Tweaks)] をクリックして、選択したデフォルト ポータル テーマの色の設定の一部を上書きします。

- a) バナーとページ背景、テキスト、およびラベルの色の設定を変更します。
- b) テーマのデフォルト カラー スキームに戻す場合は、[色のリセット (Reset Colors)] をクリックします。
- c) [プレビュー (Preview)] で色の変更を確認する場合は、[OK] をクリックします。

ステップ4 [Save] をクリックします。

ポータルの表示言語の変更

カスタム変更を加えるときに、変更内容を表示する言語を選択できます。この変更は、カスタマイズしているポータル全体に適用されます。

ステップ1 次のポータルに移動します。

- [スポンサー (Sponsor)] ポータルの場合、[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)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > [グローバルなカスタマイズ (Global Customization)] を選択します。
- デバイスポータルの場合、[管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > [グローバルなカスタマイズ (Global Customization)] を選択します。

ステップ2 [表示 (View In)] ドロップダウンリストから、ページをカスタマイズするときにテキストを表示する言語を選択します。

ドロップダウンリストには、特定のポータルに関連付けられた言語ファイルにあるすべての言語が含まれています。

次のタスク

ポータルページをカスタマイズするときに選択した言語に加えた変更が、サポート対象のすべての言語プロパティ ファイルで更新されていることを確認します。

ポータルのアイコン、イメージ、およびロゴの変更

独自の企業ロゴ、アイコン、およびバナー イメージを使用する場合は、カスタム イメージをアップロードするだけで既存のイメージを置き換えることができます。サポートされている画像形式は、.gif、.jpg、.jpeg、.png です。これらの変更は、カスタマイズしているポータル全体に適用されます。

始める前に

ポータルのはなり（たとえば、アドバタイズメント）にイメージを含めるには、そのイメージがある外部サーバーにアクセスできる必要があります。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、[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)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサーポータルの場合、[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)] > [設定 (Configure)] > [スポンサーポータル (Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイスポータルの場合、[管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [イメージ (Images)] で、ロゴ、アイコン、イメージのボタンをクリックし、カスタムイメージをアップロードします。

ステップ 3 [Save] をクリックします。

ポータルのはなりおよびフッター要素の更新

ポータルのはなりページののはなりおよびフッターセクションに表示される情報をカスタマイズできます。これらの変更は、カスタマイズしているポータル全体に適用されます。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、[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)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサーポータルの場合、[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 (Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイスポータルの場合、[管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 各ポータル ページに表示される [はなり タイトル (Banner title)] を変更します。

ステップ 3 ポータルを使用するゲスト用に次のリンクを含めます。

- [ヘルプ (Help)] : オンラインヘルプ (スポンサーおよびデバイス ポータルにのみ提供します)。

- [連絡先 (Contact)]: テクニカルサポート (このことができるようにするには、[サポート情報 (Support Information)] ページを設定します)。

ステップ 4 各ポータル ページの下部に表示される [フッター要素 (Footer Elements)] に利用規約または著作権表示を追加します。

ステップ 5 [Save] をクリックします。

タイトル、手順、ボタン、およびラベルテキストの変更

ポータルに表示されるすべてのテキストを更新できます。カスタマイズするページの各 UI 要素に、入力できる文字数の最小範囲および最大範囲があります。テキストブロックの一部が使用可能な場合、ミニエディタを使用して表示スタイルをテキストに適用できます。これらの変更は、カスタマイズしている特定のポータルページにだけ適用されます。これらのページ要素は、電子メール、SMS、印刷通知ごとに異なります。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、[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)] > [設定 (Configure)] > [ゲストポータル (Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサーポータルの場合、[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 (Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイスポータルの場合、[管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [ページ (Pages)] で、変更するページを選択します。

ステップ 3 [ページのカスタマイズ (Page Customizations)] で、表示された UI 要素を更新します。すべてのページに [ブラウザ ページタイトル (Browser Page Title)]、[コンテンツ タイトル (Content Title)]、[説明テキスト (Instructional Text)]、[コンテンツ (Content)]、および 2 つの [任意のコンテンツ (Optional Content)] の各テキストブロックが含まれています。[コンテンツ (Content)] 領域のフィールドはすべてのページに固有です。

テキスト ボックスの内容のフォーマットおよびスタイル

テキストの基本的な書式設定を行うには、[説明テキスト (Instructional Text)]、[オプションの内容 1 (Optional Content 1)]、および [オプションの内容 2 (Optional Content 2)] テキストボックスにあるミニエディタを使用します。これらの変更は、カスタマイズしている特定のポータル ページにだけ適用されます。

[全画面表示の切り替え (Toggle Full Screen)] ボタンを使用して、作業しているテキスト ボックスのサイズを拡大および縮小します。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、[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)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサーポータルの場合、[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 (Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイスポータルの場合、[管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [ページ (Pages)] で、変更するページを選択します。

ステップ 3 [ページのカスタマイズ (Page Customizations)] の、[説明テキスト (Instructional Text)] および [オプションの内容 (Optional Content)] テキスト ボックスで、次の操作を実行できます。

- テキストのフォント、色、サイズを変更します。
- テキストに太字、イタリック体、下線のスタイルを設定します。
- 箇条書きおよび番号付きリストを作成します。

(注) ミニエディタを使用してフォーマットしたテキストに適用された HTML タグを見るために [HTML ソースの切り替え (Toggle HTML Source)] ボタンを使用できます。[HTML ソース (HTML Source)] ビューでテキストを編集する場合は、[ポータルページのカスタマイズ (Portal Page Customization)] ウィンドウで変更を保存する前に、[HTML ソースの切り替え (Toggle HTML Source)] ボタンをもう一度クリックします。

ポータル ページのカスタマイズ用の変数

これらのポータル ページテキスト ボックスへのナビゲーションパス:

- ゲストポータルの場合、[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)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > [ページ (Pages)] を選択します。
- スポンサーポータルの場合、[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 (Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > [ページ (Pages)] の順に選択します。

- デバイスポータルの場合、[管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > ページ を選択します。

ポータルユーザー (ゲスト、スポンサーおよび従業員) に表示される情報の一貫性を維持するために、ポータルコンテンツおよびゲスト通知用のテンプレートを作成するときにこれらの変数を使用します。[説明テキスト (Instructional Text)]、[オプション コンテンツ 1 (Optional Content 1)]、および [オプション コンテンツ 2 (Optional Content 2)] テキスト ボックスで、各ポータルのテキストを次に示す変数名と置き換えます。

表 1: ゲストポータルの変数のリスト

表示名	変数名による代替
アクセスコード 電子メール、テキストまたは印刷物の通知を使用して、ゲストにアクセスコードを提供するために使用します。	ui_access_code
BYOD IOS SSID デュアルSSIDフローに入った後にデバイスが接続する必要があるネットワークを指定するために使用します。	ui_byod_success_ios_ssid
クライアントプロビジョニングエージェントのタイプ (Client Provisioning Agent Type) クライアントプロビジョニングポリシーに現在設定されているエージェントを指定するために使用します。	ui_client_provision_agent_type
クライアントプロビジョニングエージェントの URL (Client Provisioning Agent URL) ポスチャエージェントのダウンロードURLを指定するために使用します。	ui_client_provision_agent_url

表示名	変数名による代替
<p>クライアントプロビジョニングエージェントインストール分数 (Client Provisioning agent install minutes)</p> <p>ゲストに、[クライアントプロビジョニング (Client Provisioning)] ウィンドウでインストール手順を完了する必要がある制限時間 (修復タイマーにより設定) を通知するために使用します。タイマーが時間切れになる前にゲストがインストール手順を完了しなかった場合、ゲストはブラウザ ページをリフレッシュして、ログインプロセスをやり直す必要があります。</p>	ui_client_provision_install_agent_mins
会社	ui_company
電子メールアドレス (Email address)	ui_email_address
終了日時 (End date and time)	ui_end_date_time
名 (First name)	ui_first_name
姓 (Last name)	ui_last_name
ロケーション名	ui_location_name
最大登録デバイス数 (Maximum registered devices)	ui_max_reg_devices
最大同時ログイン数 (Maximum simultaneous logins)	ui_max_siml_login
[パスワード (Password)]	ui_password
訪問先担当者 (電子メール) (Person being visited (email))	ui_person_visited
電話番号 (Phone number)	ui_phone_number
訪問の理由 (Reason for visit)	ui_reason_visit
SMS プロバイダー (SMS Provider)	ui_sms_provider
<p>SSID</p> <p>ゲストがネットワークに接続するために使用できるワイヤレス ネットワークを指定するために使用します。</p>	ui_ssid

表示名	変数名による代替
開始日時 (Start date and time)	ui_start_date_time
残り時間 (Time left)	ui_time_left
[ユーザー名 (Username)]	ui_user_name

表 2: スポンサー ポータルの変数のリスト

表示名	変数名による代替
ゲスト - 会社 (Guest - Company)	ui_guest_company
ゲスト - 電子メールアドレス (Guest - Email address)	ui_guest_email_address
ゲスト - 終了日時 (Guest - End date and time)	ui_guest_end_date_time
ゲスト - 名 (Guest - First name)	ui_guest_first_name
ゲスト - 姓 (Guest - Last name)	ui_guest_last_name
ゲスト - ロケーション名 (Guest - Location name)	ui_guest_location_name
ゲスト - 最大登録デバイス数 (Guest - Maximum registered devices)	ui_guest_max_reg_devices
ゲスト - 最大同時ログイン数 (Guest - Maximum simultaneous logins)	ui_guest_max_siml_login
ゲスト - パスワード (Guest - Password)	ui_guest_password
ゲスト - 訪問先担当者 (電子メール) (Guest - Person being visited (email))	ui_guest_person_visited
ゲスト - 電話番号 (Guest - Phone number)	ui_guest_phone_number
ゲスト - 訪問の理由 (Guest - Reason for visit)	ui_guest_reason_visit
ゲスト - SMS プロバイダー (Guest - SMS Provider)	ui_guest_sms_provider
ゲスト - SSID (Guest - SSID) ゲストがネットワークに接続するために使用できるワイヤレス ネットワークを指定するために使用します。	ui_guest_ssid
ゲスト - 開始日時 (Guest - Start date and time)	ui_guest_start_date_time

表示名	変数名による代替
ゲスト - 残り時間 (Guest - Time left)	ui_guest_time_left
ゲスト - ユーザー名 (Guest - Username)	ui_guest_user_name
[ユーザー名 (Username)] ポータルにログインしたユーザーのユーザー名を指定するために使用します。	ui_sponsor_user_name
[ゲストアクセス情報 (Guest Access Information)] ウィンドウに [これ以降 (From)] を表示するために使用します。	ui_from_label
[ゲストアクセス情報 (Guest Access Information)] ウィンドウに [初回ログイン (First Login)] を表示するために使用します。	ui_first_login_text
初回ログイン時にアクセス時間が開始すると、ゲスト アカウントの通知メッセージを表示するために使用します。	ui_notification_first_login_text
電子メール通知のアカウントの有効期間を示す動変数。	ui_access_duration
利用できなくなったアカウントを表示する動変数。[開始/終了 (Start-End)] アカウントでは日付は終了日で、[初回ログインから (From-First-Login)] アカウントでは日付はアカウントの作成日に消去期間日数を足したものです。	ui_account_purge_date
ゲスト ユーザーが少なくとも一度以前ログインしたことがある場合、スポンサーが、ゲストのタイプを [初回ログインから (From-First-Login)] から [開始/終了 (Start-End)] に変更、または逆に変更することを制限するために使用します。一般的なスポンサー ポータル メッセージに表示されます。	ui_guest_type_change_ffl_startend_not_allowed_error ui_guest_type_change_startend_ffl_not_allowed_error

表 3: MDM ポータルの変数のリスト

表示名	変数名による代替
MDM - ベンダー名 (MDM - Vendor Name)	ui_mdm_vendor_name

表 4: デバイス ポータルの変数のリスト

表示名	変数名による代替
デバイス - ログイン失敗の頻度制限 (MyDevices - Login Failure Rate Limit)	\$user_login_failure_rate_limit\$
デバイス - 最大登録デバイス数 (MyDevices - Max Devices to Register)	ui_max_register_devices
デバイス - ユーザー名 (MyDevices - User Name) ポータルにログインしたユーザーのユーザー名を指定するために使用します。	\$session_username\$

カスタマイズの参照

カスタマイズがポータルユーザー（ゲスト、スポンサー、従業員）にどのように表示されるかを確認できます。

ステップ 1 [ポータルテストURL (Portal test URL)] をクリックして、変更を表示します。

ステップ 2 (オプション) 変更がさまざまなデバイスでどのように表示されるかを動的に確認するには、[プレビュー (Preview)] をクリックします。

- モバイルデバイス: [プレビュー (Preview)] で変更を表示します。
- デスクトップデバイス: [プレビュー (Preview)] をクリックし、[デスクトッププレビュー (Desktop Preview)] をクリックします。

変更が表示されない場合は、[プレビューのリフレッシュ (Refresh Preview)] をクリックします。表示されるポータルは、変更を確認するためのものです。ボタンをクリックしたり、データを入力したりすることはできません。

- (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。複数の PSN がある場合、Cisco ISE は最初のアクティブ PSN を選択します。

カスタム ポータル ファイル

カスタム ポータル ファイル メニューでは、ISE サーバーに独自のファイルをアップロードすることができ、(管理者ポータルを除く) ユーザーがアクセスできるすべてのポータルのカス

カスタマイズに使用できます。アップロードしたファイルは PSN に保存され、すべての PSN に同期されます。

サポートされるファイルタイプは次のとおりです。

- .png、.gif、.jpg、.jpeg、.ico : 背景、お知らせ、および広告用
- .htm、.html、.js、.json、.css、.m4a、.m4v、.mp3、.mp4、.mpeg、.ogg、.wav : 高度なカスタマイズ用（ポータルビルダーなど）

ファイルのサイズは限定されます：

- ファイルあたり 20 MB
- すべてのファイルの合計が 200 MB

ファイルのリストのパス列には、このサーバー上のファイルの URL が表示されます。この URL は、ミニエディタ外部でそのファイルを参照する場合に使用できます。イメージファイルの場合、リンクをクリックすると、新しいウィンドウが開き、イメージが表示されます。

アップロードされたファイルは、[ポータルページのカスタマイズ (Portal Page Customization)] の下にあるミニエディタで、管理者用ポータルを除くすべてのポータルタイプにより参照できます。ミニエディタにファイルを挿入するには、ツールバーの [ファイルを挿入 (insert file)] ボタンをクリックします。[HTML ソース (HTML Source)] ビューに切り替えます。挿入されたファイルが適切な HTML タグで囲まれていることがわかります。

テストのために、表示可能なアップロードファイルを ISE の外部からブラウザで表示することもできます。URL は `https://ise_ip:8443/portal/customFiles/filename` です。

ポータル的高度なカスタマイズ

Cisco ISE から提供されるデフォルトのポータルテーマの 1 つを使用しない場合、ニーズに合わせてポータルをカスタマイズできます。そのためには、CSS および Javascript ファイルと jQuery Mobile ThemeRoller アプリケーションの使用経験が必要です。

デフォルトのポータルテーマを変更することはできませんが、次の操作を実行できます。

- [ポータルのデフォルトテーマ CSS ファイルのエクスポート \(125 ページ\)](#)、カスタムポータルテーマを作成する基本として使用できます。
- [カスタムポータルテーマ CSS ファイルの作成 \(126 ページ\)](#)、デフォルトのポータルテーマを編集し、新規ファイルとして保存することによって可能になります。
- [カスタムポータルテーマ CSS ファイルのインポート \(138 ページ\)](#)、ポータルに適用できます。

専門知識と要件に基づいて、さまざまなタイプの高度なカスタマイズを実行できます。事前定義済み変数を使用して、表示される情報の整合性の実現、ポータルページへのアドバタイズメントの追加、HTML、CSS、および Javascript コードを使用した内容のカスタマイズ、ポータルページのレイアウト変更が可能になります。

ポータルを変更するには、各ポータルの [ポータルページのカスタマイズ (Portal Page Customization)] タブのコンテンツボックスに HTML、CSS、および Javascript を追加します。このドキュメントでは、HTML と CSS を使用したカスタマイズの例について説明します。Javascript を使用した例は、ISE コミュニティ (<http://cs.co/ise-community>) で紹介されています。さらに多くの HTML、CSS、および Javascript の例については、ISE コミュニティ <https://community.cisco.com/t5/security-documents/how-to-ise-web-portal-customization-options/ta-p/3619042> を参照してください。



(注) TAC では、Javascript での Cisco ISE ポータルのカスタマイズをサポートしていません。Javascript でのカスタマイズに関する問題が発生した場合は、ISE コミュニティ <https://community.cisco.com/t5/identity-services-engine-ise/bd-p/5301j-disc-ise> に質問を投稿してください。

高度なポータル カスタマイズの有効化

Cisco ISE では、エンドユーザー ポータルに表示されるコンテンツをカスタマイズすることができます。[ポータルページのカスタマイズ (Portal Page Customization)] にリストされているさまざまなページのテキストボックスには HTML、CSS、および Javascript コードを入力できます。

- ステップ 1 [管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [設定 (Settings)] > [ポータルのカスタマイズ (Portal Customization)] を選択します。
- ステップ 2 [HTML を使用したポータルのカスタマイズの有効化 (Enable portal customization with HTML)] がデフォルトでオンになっていることを確認します。この設定によって、[説明テキスト (Instructional Text)]、[オプションの内容 1 (Optional Content 1)] フィールドと [オプションの内容 2 (Optional Content 2)] フィールドに HTML タグを含めることができます。
- ステップ 3 [HTML および JavaScript によるポータルのカスタマイズを有効化 (Enable Portal Customization with HTML and JavaScript)] をオンにします。高度な JavaScript カスタマイズには、<script> tags in the [説明テキスト (Instructional Text)]、[オプションの内容 1 (Optional Content 1)]、および [オプションの内容 2 (Optional Content 2)] フィールド。

ポータル テーマと構造 CSS ファイル

CSS ファイルの使用に関する経験がある場合、デフォルトのポータル テーマ CSS ファイルをカスタマイズして、ポータルプレゼンテーションを変更し、ページレイアウト、色、フォントなどの要素を操作できます。CSS ファイルをカスタマイズすると、プレゼンテーションの特性の指定における柔軟性と制御が向上し、複数のページでフォーマットを共有することが可能になり、構造化されたコンテンツの複雑さと繰り返しが削減されます。

Cisco ISE エンドユーザー ポータルは、種類が異なる 2 つの CSS ファイル (structure.css および theme.css) を使用します。ポータルテーマごとに独自の theme.css ファイルがありますが、ポー

タルタイプにつき `structure.css` ファイルは1つのみです（例：ゲストポータルの場合は `guest.structure.css`、スポンサーポータルの場合は `sponsor.structure.css`、デバイスポータルの場合は `mydevices.structure.css`）。

`structure.css` では、ページレイアウトと構造のスタイルを指定しています。これには各ページの要素の位置が定義され、jQuery Mobile 構造のスタイルも含まれています。`structure.css` ファイルは表示のみ可能で、編集することはできません。ただし、`theme.css` ファイル内のページレイアウトを変更し、これらのファイルをポータルにインポートして適用すると、最新の変更が `structure.css` のスタイルよりも優先されます。

`theme.css` ファイルは、フォント、ボタンの色、ヘッダーの背景などのスタイルを指定します。`theme.css` ファイルをエクスポートし、テーマ設定を変更してインポートし、ポータルのカスタムテーマとして使用できます。`theme.css` ファイルに対するページレイアウトスタイルの変更は、`structure.css` ファイルで定義されるスタイルよりも優先されます。

シスコが提供するデフォルトのポータル `theme.css` ファイルは変更できません。ただし、ファイル内の設定を編集して、新しいカスタム `theme.css` ファイルに保存できます。カスタム `theme.css` ファイルをさらに編集することはできますが、Cisco ISE に再度インポートする場合は、最初に使用されていたのと同じテーマ名にしてください。同じ `theme.css` ファイルに2つの異なるテーマ名を使用することはできません。

たとえば、デフォルトの `green theme.css` ファイルを使用して新しいカスタム `blue theme.css` ファイルを作成し、`Blue` と名付けることができます。その後、`blue theme.css` ファイルを編集できますが、これを再度インポートする場合は、同じテーマ名の `Blue` を再利用する必要があります。Cisco ISE はファイル名やその名前とテーマ名の一意性の関係を確認するため、そのファイルを `Red` という名前にすることはできません。ただし、`blue theme.css` ファイルを編集し、`red theme.css` として保存し、新規ファイルをインポートして `Red` と名付けることは可能です。

jQuery Mobile によるテーマカラーの変更

シスコのエンドユーザーポータルのカラースキームは、jQuery ThemeRoller と互換性があります。ThemeRoller Web サイトを使用して、ポータル全体の色を簡単に編集できます。

ThemeRoller の色の「見本」には独自のカラースキームがあります。それらのスキームによって、主要 UI 要素（ツールバー、コンテンツブロック、ボタン、リスト項目、フォントのテキストシャドウなど）の色、テクスチャ、フォントの設定が定義されます。さらに、ボタンのさまざまな操作状態（通常時、マウスオーバー時、押された時）の設定も定義されます。

シスコでは、次の3つの見本が使用されます。

- スイッチ A：デフォルトのスイッチ。
- スイッチ B：強調する要素を定義します（例：[承認 (Accept)] ボタンなど）。
- スイッチ C：重要な要素を定義します（例：アラート、エラーメッセージ、無効な入力フィールド、削除ボタンなど）。

スイッチを新たに追加して適用する場合は、そのスイッチを使用する要素を含む HTML コードを（オプションコンテンツなどに）追加しない限り、追加したスイッチを適用できません。

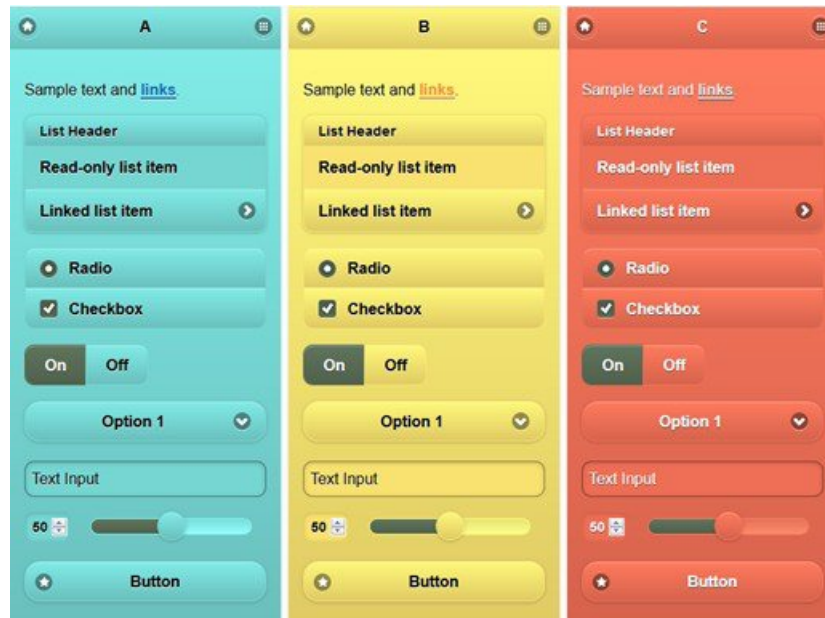
シスコ提供のデフォルトの CSS ファイルを編集するか、またはデフォルトのテーマに定義されている CSS クラスおよび構造に基づいて新しいファイルを作成するには、[jQuery Mobile ThemeRoller \(リリース 1.3.2\)](#) の必要なバージョンを使用してください。

jQuery Mobile ThemeRoller のスウォッチおよびテーマの詳細情報については、『[Creating a Custom Theme with ThemeRoller](#)』の「[Theming Overview](#)」を参照してください。jQuery Mobile ThemeRoller のオンライン ヘルプを使用して、カスタム テーマをダウンロード、インポート、および共有する方法を学習します。

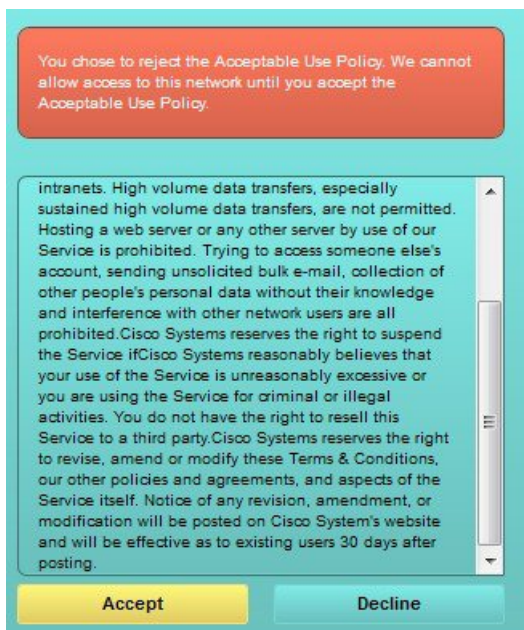
HTML、CSS、および Javascript コードを使用して、ポータルページに表示されるテキストおよびコンテンツをカスタマイズする方法のチュートリアルについては、[Codecademy](#) にアクセスしてください。

シスコの見本を示すテーマの例

見本がどのように使用されるかを示すために、ゲストポータルのデフォルトテーマが色の違いを示すように ThemeRoller で編集されました。



次の画面は、ユーザー（見本B）からのアクションを取るボタンとともにゲストポータルのログインエラー（見本C）を示し、画面の残りは見本Aです。



jQuery Mobile によるテーマ カラーの変更

始める前に

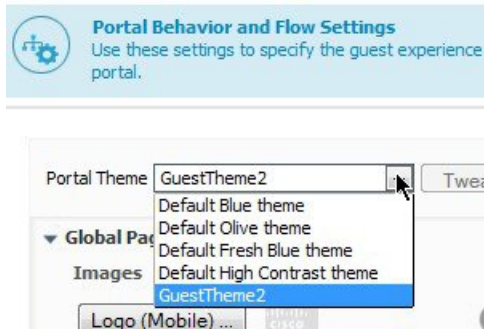
jQuery Mobile ThemeRoller のバージョン 1.3.2 を使用していることを確認します。ご使用のバージョンが次のように画面の左上隅に表示されます。



- ステップ 1 ポータルで **[構成 (Configuration)]** タブをクリックして、ポータルから変更する既存のテーマをエクスポートします。
- ステップ 2 **[高度なカスタマイズ (Advanced Customization)]** > **[テーマのエクスポート/インポート (Export/Import Themes)]** を選択します。
- ステップ 3 **[カスタムテーマ (Custom Theming)]** ダイアログで、更新するテーマをエクスポートします。
- ステップ 4 テキスト エディタでそのテーマを開き、すべてを選択してコピーします。
- ステップ 5 jQuery Web サイトの **[テーマのインポート (Import Theme)]** フィールドにテキスト (CSS) を貼り付けます。
- ステップ 6 jQuery Mobil Web ベースのアプリケーションで変更を行います。
- ステップ 7 jQuery Web サイトから更新されたテーマをエクスポートします (エクスポート形式は zip)。
- ステップ 8 更新されたテーマを解凍し、テーマフォルダ内の更新されたテーマを PC に展開します。テーマの名前は、jQuery Web サイトで指定した名前です。

ステップ 9 ポータル構成ページの [カスタムテーマ (Custom Theming)] ダイアログで、展開した CSS テーマファイルをポータルにインポートします。

[ポータル構成 (Portal Configuration)] ウィンドウの [ポータルテーマ (Portal Theme)] ドロップダウンをクリックすることで、古いテーマと新しいテーマを切替えることができます。



ロケーションに基づくカスタマイズ

ゲストアカウントが作成されるときに、それらをロケーションに関連付けて Service Set Identifier (SSID) 属性を指定することができます。ロケーションと SSID のどちらも、CSS クラスとして使用することができます。これを使用すると、ゲストのロケーションと SSID に基づいて、それぞれ異なる CSS スタイルをポータルページに適用できます。

次に例を示します。

- **ゲスト ロケーション** : ロケーションとして *San Jose* または *Boston* を持つアカウント付きゲストがクレデンシャルを持つゲストポータルにログインした場合、**guest-location-san-jose** または **guest-location-boston** のいずれかのクラスをすべてのポータルページで使用できます。
- **ゲスト SSID** : *Coffee Shop Wireless* という名前の SSID の場合、すべてのポータルページで **guest-ssid-coffee-shop-wireless** という CSS クラスを使用できます。この SSID は、ゲストアカウントに指定した SSID であり、ログイン時にゲストが接続した SSID ではありません。



(注) この情報は、クレデンシャルを持つゲストポータルにのみ、ゲストがログインした後に適用されます。

スイッチやワイヤレス LAN コントローラ (WLC) などのデバイスをネットワークに追加するときに、ロケーションも指定できます。このロケーションも CSS クラスとして使用ことができ、これを使用すると、ネットワークデバイスのロケーションに応じて、それぞれ異なる CSS スタイルをポータルページに適用できます。

たとえば、WLC が *Seattle* に割り当てられ、ゲストが Seattle-WLC から Cisco ISE にリダイレクトされた場合、すべてのポータル ページで **device-location-my-locations-usa-seattle** という CSS クラスを使用できます。

関連トピック

[ゲスト ロケーションに基づいたグリーティングのカスタマイズ](#) (133 ページ)

ユーザー デバイス タイプに基づくカスタマイズ

Cisco ISE は、クライアント デバイスのタイプ (ゲスト、スポンサー、または従業員) を検出し、企業のネットワークまたはエンドユーザー Web ポータル (ゲスト、スポンサーおよびデバイス) にアクセスします。タイプは、モバイル デバイス (Android、iOS など) またはデスクトップ デバイス (Windows、MacOS など) のいずれかとして検出されます。デバイス タイプは、CSS クラスとして利用できます。このクラスは、ユーザーのデバイス タイプに基づいてポータル ページに異なる CSS スタイルを適用するために使用できます。

ユーザーは Cisco ISE のエンドユーザー Web ポータルにログインすると、それらのポータル ページで **cisco-ise-mobile** クラスまたは **cisco-ise-desktop** クラスを使用できます。

関連トピック

[ユーザー デバイス タイプに基づいたグリーティングのカスタマイズ](#) (134 ページ)

ポータルのデフォルト テーマ CSS ファイルのエクスポート

シスコが提供するデフォルトのポータルテーマをダウンロードし、ニーズに合わせてカスタマイズできます。それを高度なカスタマイズを実行するための基本として使用できます。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、[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)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > [ページ (Pages)] を選択します。
- スポンサーポータルの場合、[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 (Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > [ページ (Pages)] の順に選択します。
- デバイスポータルの場合、[管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > ページ を選択します。

ステップ 2 [高度なカスタマイズ (Advanced Customization)] ドロップダウン リストから [テーマのエクスポート/インポート (Export/Import Themes)] を選択します。

ステップ 3 [カスタム テーマ (Custom Theming)] ダイアログボックスで、ドロップダウン リストを使用してカスタマイズするテーマを選択します。

ステップ 4 [テーマ CSS のエクスポート (Export Theme CSS)]をクリックして、カスタマイズするデフォルトの *theme.css* ファイルをダウンロードします。

ステップ 5 [保存 (Save)]をクリックしてファイルをデスクトップに保存します。

カスタム ポータル テーマ CSS ファイルの作成

カスタム ポータルテーマを作成するには、既存のデフォルト ポータルテーマをカスタマイズして、新規ポータルの *theme.css* ファイルに変更を保存します。デフォルト テーマの設定および見本を変更して、選択したポータルへのグローバルな変更を行うことができます。

始める前に

- カスタマイズするポータルから *theme.css* ファイルをデスクトップにダウンロードします。
- このタスクには、HTML、CSS、および Javascript コードの使用経験が必要です。
- jQuery Mobile ThemeRoller のリリース 1.3.2 を使用します。

ステップ 1 ダウンロードしたポータルの *theme.css* ファイルのコンテンツを jQuery Mobile ThemeRoller ツールにインポートします。

ヒント 変更時に、[カスタマイズの参照 \(139 ページ\)](#) を行うことができます。

ステップ 2 (任意) [ポータル コンテンツに組み込まれたリンク \(127 ページ\)](#)

ステップ 3 (任意) [動的なテキスト更新の変数の挿入 \(127 ページ\)](#)

ステップ 4 (任意) [テキストをフォーマットし、リンクを含めるソース コードの使用 \(129 ページ\)](#)

ステップ 5 (任意) [アダプティブメントとしてのイメージの追加 \(130 ページ\)](#)

ステップ 6 (任意) [ゲスト ロケーションに基づいたグリーティングのカスタマイズ \(133 ページ\)](#)

ステップ 7 (任意) [ユーザー デバイス タイプに基づいたグリーティングのカスタマイズ \(134 ページ\)](#)

ステップ 8 (任意) [カラーセルアダプティブングの設定 \(131 ページ\)](#)

ステップ 9 (任意) [ポータル ページのレイアウトの変更 \(135 ページ\)](#)

ステップ 10 カスタマイズされたファイルを新しい *theme.css* ファイルとして保存します。

(注) デフォルト CSS テーマファイルに編集内容を保存することはできません。編集を使用して新しいカスタム ファイルを作成することのみができます。

ステップ 11 新しい *theme.css* ファイルは、準備を整えた後、Cisco ISE にインポートできます。

ポータルコンテンツに組み込まれたリンク

リンクを追加して、ゲストがポータルページからさまざまな Web サイトにアクセスできるようことができます。これらの変更は、カスタマイズしている特定のポータルページにだけ適用されます。

[全画面表示の切り替え (Toggle Full Screen)] オプションを使用して、作業しているフィールドのサイズを拡大および縮小します。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、[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 and Components)] > [ゲストポータル (Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサーポータルの場合、[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 and Components)] > [スポンサーポータル (Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] の順に選択します。
- デバイスポータルの場合、[管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- [証明書プロビジョニング (Certificate Provisioning)] ポータルの場合、[管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)] > [証明書プロビジョニング (Certificate Provisioning)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [ページ (Pages)] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ (Page Customizations)] で、[オプションの内容 (Optional Content)] テキストブロックで提供されるミニエディタを使用して、ポータルページへのリンクを追加します。

ステップ 4 [リンクの作成 (Create Link)] ボタンをクリックします。
[リンクのプロパティ (Link Properties)] ダイアログボックスが表示されます。

ステップ 5 [URL] の [説明 (Description)] ウィンドウに、ハイパーリンクする **URL** およびテキストを入力します。

リンクが正しく機能するように、URL にプロトコル識別子を含めます。たとえば、www.cisco.com ではなく http://www.cisco.com を使用します。

ステップ 6 [設定 (Set)] をクリックし、[保存 (Save)] をクリックします。

ミニエディタを使用してフォーマットしたテキストに適用された HTML タグを見るために [HTML ソースの切り替え (Toggle HTML Source)] オプションを使用できます。

動的なテキスト更新の変数の挿入

内容を動的に更新する事前定義済みの変数 (\$variable\$) を代わりに使用することによって、ポータルに表示されるテキストのテンプレートを作成することもできます。これにより、ゲスト

トに表示するテキストと情報の一貫性が維持されます。これらの変更は、カスタマイズしている特定のポータル ページにだけ適用されます。

[全画面表示の切り替え (Toggle Full Screen)] オプションを使用して、作業しているフィールドのサイズを拡大および縮小します。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、[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 and Components)]>[ゲストポータル (Guest Portals)]>[編集 (Edit)]>[ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサーポータルの場合、[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 and Components)]>[スポンサーポータル (Guest Portals)]>[編集 (Edit)]>[ポータルページのカスタマイズ (Portal Page Customization)] の順に選択します。
- デバイスポータルの場合、[管理 (Administration)]>[デバイスポータル管理 (Device Portal Management)]> (任意のポータル) >[編集 (Edit)]>[ポータルページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [ページ (Pages)] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ (Page Customizations)] で、[説明テキスト (Instructional Text)]、[オプションの内容 1 (Optional Content 1)]、および [オプションの内容 2 (Optional Content 2)] フィールドで提供されるミニエディタを使用して、ポータルページのテキストテンプレートを作成します。

たとえば、複数のゲスト用に単一の初期メッセージテンプレートを作成し、正常にログインしてネットワークに接続した後にゲストに表示するメッセージをカスタマイズできます。

ステップ 4 通常どおりに情報をフィールドに入力します。

たとえば、ポータル用の初期メッセージを入力することができます。

```
Welcome to our company's Guest portal,
```

ステップ 5 テキストの代わりに変数を使用する箇所では、[変数の挿入 (Insert Variable)] ボタンをクリックします。変数のリストがポップアップメニューに表示されます。

ステップ 6 テキストの代わりに使用する変数を選択します。

たとえば、初期メッセージに各ゲストの名を表示する [名 (Firstname)] を選択します。変数 `ui_first_name` がカーソル位置に挿入されます。

```
Welcome to our company's Guest portal,$ui_first_name$.
```

これは John という名のゲストのポータルの初期ページに表示される初期メッセージです。当社のゲストポータルへようこそ、John (Welcome to our company's Guest portal, John) 。

ステップ 7 テキスト ボックスに情報を入力し終えるまで、必要に応じて続けて変数のリストを使用します。

ステップ 8 [保存 (Save)] をクリックします。

ミニエディタを使用してフォーマットしたテキストに適用された HTML タグを見るために [HTML ソースの切り替え (Toggle HTML Source)] オプションを使用できます。

テキストをフォーマットし、リンクを含めるソースコードの使用

ミニエディタのフォーマットとプレーンテキスト付きリンクアイコンの使用に加えて、HTML、CSS、および Javascript コードを使用して、ポータルページに表示されるテキストをカスタマイズすることもできます。これらの変更は、カスタマイズしている特定のポータルページにだけ適用されます。

[全画面表示の切り替え (Toggle Full Screen)] オプションを使用して、作業しているテキストボックスのサイズを拡大および縮小します。

始める前に

[管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [設定 (Settings)] > [ポータルのカスタマイズ (Portal Customization)] で [HTML を使用したポータルのカスタマイズの有効化 (Enable portal customization with HTML)] がデフォルトで有効になっていることを確認します。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、[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)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサーポータルの場合、[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 (Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイスポータルの場合、[管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [ページ (Pages)] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ (Page Customizations)] で、[説明テキスト (Instructional Text)]、[オプションコンテンツ1 (Optional Content 1)]、および [オプションコンテンツ2 (Optional Content 2)] の各フィールドで提供されるミニエディタを使用して、ソースコードを入力および表示します。

ステップ 4 [HTML ソースの切り替え (Toggle HTML Source)] をクリックします。

ステップ 5 ソースコードを入力します。

たとえば、テキストに下線を引くには、次のように入力します。

```
<p style="text-decoration:underline;">Welcome to Cisco!</p>
```

たとえば、HTML コードを使用してリンクを含めるには、次のように入力します。

```
<a href="http://www.cisco.com">Cisco</a>
```

重要 外部 URL を HTML コードで挿入する場合は、「http」または「https」を含む絶対 (全体的な) URL パスを入力することを確認します。

ステップ 6 [Save] をクリックします。

関連トピック

[高度なポータル カスタマイズの有効化 \(120 ページ\)](#)

アドバタイズメントとしてのイメージの追加

ポータルページの特定の領域に表示されるイメージおよびアドバタイズメントを含めることができます。

[全画面表示の切り替え (Toggle Full Screen)] オプションを使用して、作業しているテキストボックスのサイズを拡大および縮小します。

始める前に

[管理 (Administration)] > [システム (System)] > [管理アクセス (Admin Access)] > [設定 (Settings)] > [ポータルのカスタマイズ (Portal Customization)] で [HTMLを使用したポータルのカスタマイズの有効化 (Enable portal customization with HTML)] が有効になっていることを確認します。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、[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)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサーポータルの場合、[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 (Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイスポータルの場合、[管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [ページ (Pages)] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ (Page Customizations)] で、[説明テキスト (Instructional Text)]、[オプションコンテンツ1 (Optional Content 1)]、および [オプションコンテンツ2 (Optional Content 2)] の各フィールドで提供されるミニエディタを使用して、ソースコードを入力および表示します。

ステップ 4 [HTML ソースの切り替え (Toggle HTML Source)] をクリックします。

ステップ 5 ソースコードを入力します。

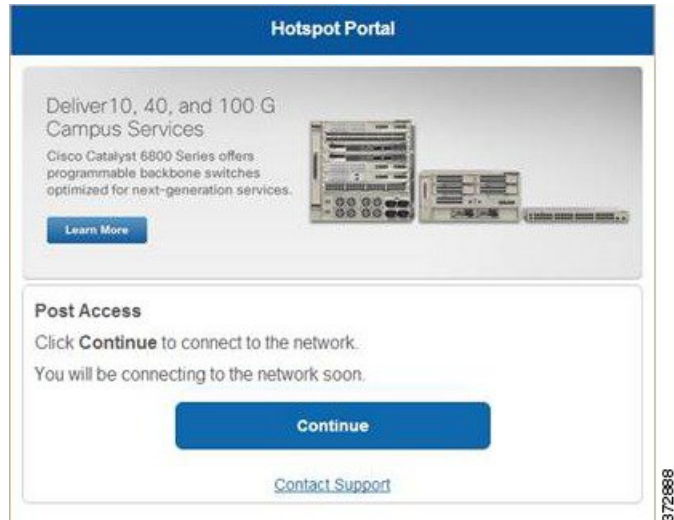
たとえば、ホットスポットゲストポータルポストアクセスバナーに HTML コードを使用して製品アドバタイズメントおよびそのイメージを含めるには、このコードを [ポストアクセスバナー (Post-Access Banner)] ページの [任意のコンテンツ 1 (Optional Content 1)] テキストボックスに入力します。

```
<p style="text-decoration:underline;">Optimized for 10/40/100 Campus Services!</p>

```

- (注) 外部 URL を HTML コードで挿入する場合は、「http」または「https」を含む絶対（全体的な）URL パスを入力することを確認します。

図 5: アドバタイズメントのサンプルイメージ



ステップ 6 [Save] をクリックします。

カルーセル アドバタイジングの設定

カルーセルアドバタイジングは、複数の製品イメージまたは説明テキストが表示され、バナー内で循環して繰り返されるアドバタイズメントの形式です。ゲスト ポータルでカルーセルアドバタイジングを使用して、複数の関連製品や、会社が提供するさまざまな製品を宣伝します。

[全画面表示の切り替え (Toggle Full Screen)] オプションを使用して、作業しているテキストボックスのサイズを拡大および縮小します。

始める前に

[管理 (Administration)]>[システム (System)]>[管理者アクセス (Admin Access)]>[設定 (Settings)]> [ポータルのカスタマイズ (Portal Customization)] を選択し、[HTML と Javascript を使用したポータルのカスタマイズの有効化 (Enable portal customization with HTML and Javascript)] をオンにします。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、[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)]> [編集 (Edit)]> [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。

- スポンサーポータルの場合、[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 (Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイスポータルの場合、[管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [ページ (Pages)] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ (Page Customizations)] で、[説明テキスト (Instructional Text)]、[オプションコンテンツ1 (Optional Content 1)]、および [オプションコンテンツ2 (Optional Content 2)] の各フィールドで提供されるミニエディタを使用して、ソースコードを入力および表示します。

ステップ 4 [HTML ソースの切り替え (Toggle HTML Source)] をクリックします。

ステップ 5 ソースコードを入力します。

たとえば、ゲストポータルで製品イメージを使用してカラーセルアドバタイジングを導入するには、[ポストアクセスバナー (Post-Access Banner)] (ホットスポットポータルの場合) または [ポストログインバナー (Post Login Banner)] (ログイン情報を持つゲストポータルの場合) ウィンドウの [任意のコンテンツ1 (Optional Content 1)] フィールドに次の HTML および Javascript コードを入力します。

```
<script>
var currentIndex = 0;
setInterval(changeBanner, 5000);

function changeBanner(){
var bannersArray = ["<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq/
n21v1DrawerContainer.img.jpg/1379452035953.jpg' width='100%' />",
"<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq_0/
n21v1DrawerContainer.img.jpg/1400748629549.jpg' width='100%' />",
"<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq_1/
n21v1DrawerContainer.img.jpg/1376556883237.jpg' width='100%' />"
];
var div = document.getElementById("image-ads");
if(div){
    currentIndex = (currentIndex<2) ? (currentIndex+1) : 0;
    div.innerHTML = bannersArray[currentIndex];
}
}
</script>
<style>
.grey{
color: black;
background-color: lightgrey;
}
</style>
<div class="grey" id="image-ads">
<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq/
n21v1DrawerContainer.img.jpg/1379452035953.jpg' />
</div>
```

たとえば、ゲストポータルでテキスト製品説明を使用してカラーセルアドバタイジングを導入するには、[ポストアクセスバナー (Post-Access Banner)] (ホットスポットポータルの場合) または [ポストログイン

ンバナー (Post Login Banner)] (ログイン情報を持つゲストポータルの場合) ウィンドウの [任意のコンテンツ2 (Optional Content 2)] フィールドに次の HTML および Javascript コードを入力します。

```
<script>
var currentIndex = 0;
setInterval(changeBanner, 2000);

function changeBanner(){
var bannersArray = ["Optimize branch services on a single platform while delivering an optimal
application experience across branch and WAN infrastructure", "Transform your Network Edge to
deliver high-performance, highly secure, and reliable services to unite campus, data center,
and branch networks", "Differentiate your service portfolio and increase revenues by delivering
end-to-end scalable solutions and subscriber-aware services"];

var colorsArray = ["grey", "blue", "green"];
var div = document.getElementById("text-ads");
if(div){
    currentIndex = (currentIndex<2) ? (currentIndex+1) : 0;
    div.innerHTML = bannersArray[currentIndex];
    div.className = colorsArray[currentIndex];
}
}
</script>
<style>
.grey{
color: black;
background-color: lightgrey;
}
.blue{
color: black;
background-color: lightblue;
}
.green{
color: black;
background-color: lightgreen;
}
</style>
<div class="grey" id="text-ads">
Optimize branch services on a single platform while delivering an optimal application
experience across branch and WAN infrastructure
</div>
```

(注) 外部 URL を HTML コードで挿入する場合は、「http」または「https」を含む絶対 (全体的な) URL パスを入力する必要があります。

ステップ 6 [Save] をクリックします。

ゲスト ロケーションに基づいたグリーティングのカスタマイズ

次の例に、ゲストがクレデンシャルを持つゲストポータル (ホットスポットではない) にログインした後に表示される正常なログインメッセージを、ゲストタイプに設定されたロケーションに基づいてカスタマイズする方法を示します。

[全画面表示の切り替え (Toggle Full Screen)] オプションを使用して、作業しているフィールドのサイズを拡大および縮小します。

ステップ 1 次のポータルのいずれかに移動します。

- ゲストポータルの場合、[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)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサーポータルの場合、[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 (Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [ページ (Pages)] で、[認証成功 (Authentication Success)] をクリックします。

ステップ 3 [ページのカスタマイズ (Page Customizations)] で、[任意のコンテンツ1 (Optional Content 1)] フィールドで提供されるミニエディタを使用して、HTML ソースコードを入力および表示します。

ステップ 4 [HTML ソースの切り替え (Toggle HTML Source)] をクリックします。

ステップ 5 ソースコードを入力します。

たとえば、ロケーションベースのグリーティングを含めるには、[任意のコンテンツ1 (Optional Content 1)] に次のコードを入力します。

```
<style>
  .custom-greeting {
    display: none;
  }
  .guest-location-san-jose .custom-san-jose-greeting {
    display: block;
  }
  .guest-location-boston .custom-boston-greeting {
    display: block;
  }
</style>
<div class="custom-greeting custom-san-jose-greeting">
  Welcome to The Golden State!
</div>
<div class="custom-greeting custom-boston-greeting">
  Welcome to The Bay State!
</div>
```

正常なログイン後に、特定のロケーションに応じて異なるメッセージがゲストに表示されます。

ユーザー デバイス タイプに基づいたグリーティングのカスタマイズ

ユーザーが Cisco ISE エンドユーザー Web ポータル (ゲスト、スポンサーおよびデバイス) のいずれかにログインした後に、ユーザーに送信するグリーティングを、クライアントデバイス タイプ (モバイルまたはデスクトップ) に基づいてカスタマイズできます。

[全画面表示の切り替え (Toggle Full Screen)] オプションを使用して、作業しているフィールドのサイズを拡大および縮小します。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、[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)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサーポータルの場合、[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 (Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイスポータルの場合、[管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [ページ (Pages)] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ (Page Customizations)] で、[オプションコンテンツ 1 (Optional Content 1)] フィールドで提供されるミニエディタを使用して、HTML ソースコードを入力および表示します。

ステップ 4 [HTML ソースの切り替え (Toggle HTML Source)] をクリックします。

ステップ 5 ソースコードを入力します。

たとえば、[AUP] ページでデバイスタイプベースのメッセージを含めるには、[AUP] ウィンドウの [オプションコンテンツ 1 (Optional Content 1)] フィールドにこの値を入力します。

```
<style>
  .custom-greeting {
    display: none;
  }
  .cisco-ise-desktop .custom-desktop-greeting {
    display: block;
  }
  .cisco-ise-mobile .custom-mobile-greeting {
    display: block;
  }
</style>
<div class="custom-greeting custom-mobile-greeting">
  Try our New Dark French Roast! Perfect on the Go!
</div>
<div class="custom-greeting custom-desktop-greeting">
  We brought back our Triple Chocolate Muffin!
  Grab a seat and dig in!
</div>
```

ユーザーがネットワークまたはポータルへのアクセスを取得するために使用したデバイスに応じて、[AUP] ページに異なるグリーティングが表示されます。

ポータル ページのレイアウトの変更

ページの全体的なレイアウトを操作できます。たとえば、追加情報や情報へのリンクを提供するサイドバーを AUP ページに追加できます。

ステップ 1 作成し、ポータルに適用するカスタム *theme.css* ファイルの末尾に次の CSS コードを追加します。これにより、AUP ページのレイアウトが変更されます。[任意のコンテンツ 1 (Optional Content 1)] フィールドは、デスクトップおよびモバイルデバイスモードでサイドバーとして表示されます。

```
#page-aup .cisco-ise-optional-content-1 {
    margin-bottom: 5px;
}
@media all and ( min-width: 60em ) {
    #page-aup .cisco-ise-optional-content-1 {
        float: left;
        margin-right: 5px;
        width: 150px;
    }
    #page-aup .cisco-ise-main-content {
        float: left;
        width: 800px;
    }
    #page-aup .cisco-ise-main-content h1,
    #page-aup .cisco-ise-main-content p {
        margin-right: auto;
        margin-left: -200px;
    }
}
```

次に、ポータルの AUP ウィンドウの [任意のコンテンツ1 (Optional Content 1)] フィールドで HTML コードを使用して、リンクを追加できます。

ステップ 2 次のポータルに移動します。

- ゲストポータルの場合、[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)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサーポータルの場合、[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)] > [スポンサーポータル (Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイスポータルの場合、[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 3 [ページ (Pages)] で、サイドバーを追加するページを選択します。

ステップ 4 [ページのカスタマイズ (Page Customizations)] で、[任意のコンテンツ1 (Optional Content 1)] フィールドで提供されるミニエディタを使用して、ソースコードを入力および表示します。

ステップ 5 [HTML ソースの切り替え (Toggle HTML Source)] をクリックします。

ステップ 6 ソースコードを入力します。

たとえば、AUP ウィンドウにサイドバーを含めるには、AUP ウィンドウの [任意のコンテンツ1 (Optional Content 1)] フィールドにこのコードを入力します。

```
<ul data-role="listview">
  <li>Rent a Car</li>
  <li>Top 10 Hotels</li>
  <li>Free Massage</li>
  <li>Zumba Classes</li>
</ul>
```


図 6: サンプル AUP ページのサイドバーのビュー (デスクトップ デバイス)

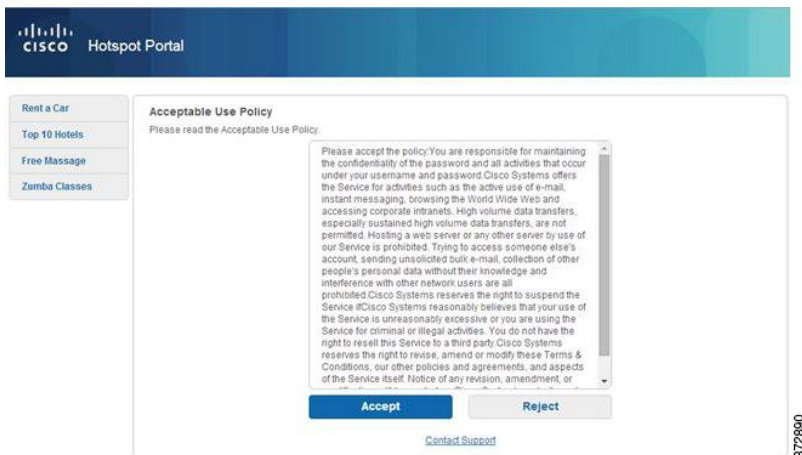
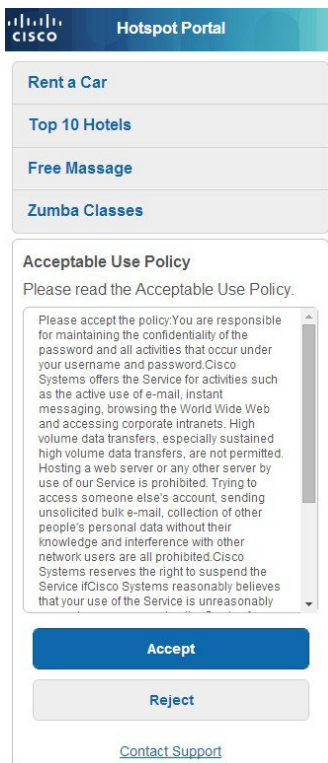


図 7: サンプル AUP ページのサイドバーのビュー (モバイル デバイス)



ステップ 7 [保存 (Save)] をクリックします。

次のタスク

[任意のコンテンツ (Optional Content)] フィールドに別のテキストまたは HTML コードを入力して、他のページをカスタマイズできます。

カスタム ポータル テーマ CSS ファイルのインポート

作成したカスタム *theme.css* ファイルをアップロードし、エンドユーザー ポータルに適用できます。これらの変更は、カスタマイズしているポータル全体に適用されます。

カスタム *theme.css* ファイルを編集し、Cisco ISE に再度インポートする場合は、最初に使用したテーマ名を使用するように注意してください。同じ *theme.css* ファイルに 2 つの異なるテーマ名を使用することはできません。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、[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)] > [設定 (Configure)] > [ゲストポータル (Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサーポータルの場合、[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 (Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイスポータルの場合、[管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [高度なカスタマイズ (Advanced Customization)] ドロップダウン リストから [テーマのエクスポート/インポート (Export/Import Themes)] を選択します。

ステップ 3 [カスタム テーマ (Custom Theming)] ダイアログボックスで、新しい *theme.css* ファイルを検索するには、[参照 (Browse)] をクリックします。

ステップ 4 新しいファイルの [テーマ名 (Theme Name)] を入力します。

ステップ 5 [保存 (Save)] をクリックします。

次のタスク

カスタマイズするポータルにこのカスタム ポータル テーマを適用できます。

1. ポータル全体に適用する更新されたテーマを [ポータルテーマ (Portal Themes)] ドロップダウン リストから選択します。
2. [Save] をクリックします。

カスタム ポータル テーマの削除

Cisco ISE にインポートしたカスタム ポータル テーマは、いずれかのポータルで使用されていない場合に削除できます。Cisco ISE によって提供されているデフォルトのテーマを削除することはできません。

始める前に

他のポータルで使用されているポータル テーマを削除することはできません。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、[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)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサーポータルの場合、[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 (Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイスポータルの場合、[管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [高度なカスタマイズ (Advanced Customization)] ドロップダウンリストから [テーマの削除 (Delete Themes)] を選択します。

ステップ 3 [テーマ名 (Theme Name)] ドロップダウン リストから削除するポータル テーマを選択します。

ステップ 4 [削除 (Delete)] をクリックし、[保存 (Save)] をクリックします。

カスタマイズの参照

カスタマイズがポータルユーザー (ゲスト、スポンサー、従業員) にどのように表示されるかを確認できます。

ステップ 1 [ポータルテスト URL (Portal test URL)] をクリックして、変更を表示します。

ステップ 2 (オプション) 変更がさまざまなデバイスでどのように表示されるかを動的に確認するには、[プレビュー (Preview)] をクリックします。

- モバイルデバイス : [プレビュー (Preview)] で変更を表示します。
- デスクトップデバイス : [プレビュー (Preview)] をクリックし、[デスクトッププレビュー (Desktop Preview)] をクリックします。

変更が表示されない場合は、[プレビューのリフレッシュ (Refresh Preview)] をクリックします。表示されるポータルは、変更を確認するためのものです。ボタンをクリックしたり、データを入力したりすることはできません。

- (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。複数の PSN がある場合、Cisco ISE は最初のアクティブ PSN を選択します。

ポータル言語のカスタマイズ

ゲスト、スポンサー、デバイスおよびクライアントプロビジョニングの各ポータルは、サポートされているすべての言語およびロケールにローカライズされています。ローカライズには、テキストラベル、メッセージ、フィールド名およびボタンラベルが含まれます。クライアントブラウザが Cisco ISE テンプレートにマッピングされていないロケールを要求した場合、ポータルは英語のテンプレートを使用して内容を表示します。

管理者ポータルを使用して、各言語のゲスト、スポンサー、デバイスの各ポータルで使用されるフィールドを個別に変更できます。また、言語を追加することも可能です。現在、クライアントプロビジョニングポータルについては、これらのフィールドはカスタマイズできません。

デフォルトでは、各タイプのポータルでは 15 言語がサポートされています。**[ポータルページのカスタマイズ (Portal Page Customization)]** ウィンドウで、ポータルで使用する言語を選択し、オプションで選択した言語でページのコンテンツを更新します。ある言語に合わせてページのフォントとコンテンツを変更しても、他の言語へこの変更は反映されません。**[ポータルページのカスタマイズ (Portal Page Customization)]** ウィンドウで行った変更は、次回に言語ファイルをエクスポートするときに組み込まれます。

サポート対象の言語は次のとおりです。

- 中国語（簡体字）
- 中国語（繁体字）
- チェコ語
- オランダ語
- 英語
- フランス語
- ドイツ語
- ハンガリー語
- イタリア語
- 日本語
- 韓国語
- ポーランド語

- ポルトガル語
- ロシア語
- スペイン語

ポータルで使用する言語の編集

1. 編集するポータルを開きます。
2. [ポータルページのカスタマイズ (Portal Page Customization)] タブで、[表示 (view in)] ドロップダウンから、編集する言語を選択します。
3. 必要に応じてコンテンツ、ヘッダー、フォントを変更します。
4. ポータル構成を保存し、更新する他の言語でこのフローを繰り返します。

言語ファイルを編集するには

各 [ポータルページのカスタマイズ (Portal Page Customization)] ウィンドウでは言語ファイルも提供されます。言語ファイルとは、属性ファイルが含まれている ZIP です。これらの属性ファイルは、ポータルフローの一部であるテキストやヘッダーのカスタマイズには使用できませんが、[ポータルページのカスタマイズ (Portal Page Customization)] ウィンドウのカスタマイズには使用できません。

言語ファイルには、特定のブラウザロケール設定へのマッピングと、その言語でのポータル全体のすべての文字列設定が含まれています。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ー 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。

zip 形式の言語ファイルをエクスポートし、新規言語の追加や不要な既存言語の削除などを行って更新することができます。

言語ファイルの更更新手順については、次を参照してください。

- [言語ファイルのエクスポート \(141 ページ\)](#)
- [言語ファイルでの言語の追加または削除 \(142 ページ\)](#)
- [更新された言語ファイルのインポート \(143 ページ\)](#)

言語ファイルのエクスポート

各ポータルタイプに使用できる言語ファイルをエクスポートして、そのファイルで指定された既存の値を編集およびカスタマイズし、言語を追加または削除できます。



(注) 言語プロパティファイル内の一部のディクショナリ キーだけが値 (テキスト) で HTML をサポートしています。

ステップ1 次のポータルに移動します。

- ゲストポータルの場合、[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)] > [編集 (Edit)] を選択します。
- [スポンサー (Sponsor)] ポータルの場合、[ワークセンター (Work Centers)] > [設定 (Configure)] > [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)] > [編集 (Edit)] を選択します。
- [デバイス (Device)] ポータルの場合、[管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] を選択します。

ステップ2 [言語ファイル (Language File)] をクリックし、ドロップダウンリストから [エクスポート (Export)] を選択します。

ステップ3 zip 形式の言語ファイルをデスクトップに保存します。

言語ファイルでの言語の追加または削除

ポータルタイプに使用したい言語が言語ファイルにない場合は、新しい言語プロパティファイルを作成し、zip 形式の言語ファイルに追加できます。不要な言語がある場合、その言語プロパティファイルを削除できます。

始める前に

言語プロパティファイルを追加または削除するには、各ポータルタイプで使用可能な zip 形式の言語ファイルをエクスポートします。

ステップ1 UTF-8 を表示するエディタ (Notepad ++ など) を使用して、言語を追加または削除するポータルタイプ用の定義済み言語ファイルを開きます。

複数のポータルタイプの言語を追加または削除するには、該当するすべてのポータルプロパティファイルを使用します。

ステップ2 新しい言語を追加するには、既存の言語プロパティファイルを他のファイルと同じ命名規則を使用する新しい言語プロパティファイルとして zip 形式の言語ファイルに保存します。たとえば、新しい日本語の言語プロパティファイルを作成するには、ファイルを `Japanese.properties` (`LanguageName.properties`) として保存します。

ステップ3 新しい言語プロパティファイルの最初の行にブラウザロケール値を指定して、ブラウザロケールに新しい言語を関連付けます。たとえば、`LocaleKeys=ja,ja-jp` (`LocaleKeys=browser locale value`) を `Japanese.properties` ファイルの最初の行に入力する必要があります。

ステップ4 新しい言語プロパティ ファイルでディクショナリ キーのすべての値（テキスト）を更新します。

ディクショナリキーは変更できません。それらの値のみを更新できます。

(注) 一部のディクショナリ キーだけが、値（テキスト）に HTML をサポートしています。

次のタスク

1. すべてのプロパティ ファイル（新規および既存）を zip 形式で圧縮し、新しい zip 形式の言語ファイルを作成します。フォルダやディレクトリは含めないでください。



(注) Mac を使用する場合は、ZIP ファイルを抽出すると、DS ストアが生成されます。編集後に言語ファイルを圧縮する場合は、DS ストアに ZIP を含めないでください。DS ストアの抽出方法については、<https://superuser.com/questions/198569/compressing-folders-on-a-mac-without-the-ds-store> を参照してください。

2. zip 形式の言語ファイルには新しい名前または元の名前を使用します。
3. エクスポート元の特定のポータルに zip 形式の言語ファイルをインポートします。

更新された言語ファイルのインポート

言語プロパティ ファイルを追加または削除したり、既存のプロパティ ファイルのテキストを更新してカスタマイズした編集済み言語ファイルをインポートできます。



(注) Word ファイルからカスタマイズした内容をコピーして貼り付けることはできません。代わりに [ファイル (File)] > [名前を付けて保存 (Save As)] を選択し、Word ファイルを HTML 形式で保存します。その後、この HTML ファイルからカスタマイズした内容をコピーして貼り付けることができます。

ステップ1 次のポータルに移動します。

- [ゲスト (Guest)] ポータルの場合、[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)] > [編集 (Edit)] を選択します。
- [スポンサー (Sponsor)] ポータルの場合、[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)] > [編集 (Edit)] を選択します。
- [デバイス (Device)] ポータルの場合、[管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] を選択します。

- ステップ2 [言語ファイル (Language)] をクリックし、ドロップダウン リストから [インポート (Import)] を選択します。
- ステップ3 デスクトップを参照して新しい zip 形式の言語ファイルを見つけます。
- ステップ4 エクスポートしたポータル タイプに再度インポートします。

次のタスク

変更したテキストまたは追加した新しい言語を表示するには、[表示 (View In)] ドロップダウン リストから特定の言語を選択します。

ゲスト通知、承認、およびエラーメッセージのカスタマイズ

各ポータルで内で、ゲストが電子メール、SMS テキスト メッセージ、および印刷物で通知を受け取る方法をカスタマイズできます。これらの通知を使用して、次の場合にログインクレデンシャルを電子メール送信、テキスト送信、または印刷します。

- ゲストがアカウント登録ゲストポータルを使用し、自分自身の登録に成功した場合。
- スポンサーがゲストアカウントを作成し、ゲストに詳細を提供する場合。スポンサーグループ作成時にスポンサーによる SMS 通知の使用を許可するかどうかを指定できます。これらの機能を利用できる場合は、常に電子メール通知および印刷通知を使用できます。

ネットワークにアクセスしようとするアカウント登録ゲストを承認するよう要求するスポンサー宛電子メール通知をカスタマイズすることもできます。また、ゲストとスポンサーに表示されるデフォルトのエラーメッセージをカスタマイズできます。

電子メールでの通知のカスタマイズ

電子メールでゲストに送信される情報をカスタマイズできます。

始める前に

- 電子メールでの通知を有効にするように SMTP サーバーを設定します。[管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [SMTP サーバー (SMTP Server)] を選択します。
- ゲストへの電子メールでの通知のサポートを設定します。[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [設定 (Settings)] > [ゲスト電子メールの設定 (Guest Email Settings)] を選択します。[ゲストへの電子メール通知を有効にする (Enable email notifications to guests)] をオンにします。
- [管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [設定 (Settings)] > [ポータルのカスタマイズ (Portal Customization)] で [HTML を使用

したポータルのカスタマイズの有効化 (Enable portal customization with HTML)] がデフォルトで有効になっていることを確認します。

-
- ステップ 1** アカウント登録スポンサーポータルの場合、[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)]>[編集 (Edit)]>[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)]>[電子メール通知 (Email Notification)] を選択します。
- ステップ 2** [グローバル ページのカスタマイズ (Global Page Customizations)] で指定されたデフォルトの [ロゴ (電子メール) (Logo (Email))] を変更できます。
- ステップ 3** [件名 (Subject)] および [電子メール本文 (Email body)] を指定します。電子メール メッセージに含まれる、ゲストアカウント情報を指定するには、事前定義済みの変数を使用します。テキストをカスタマイズするには、ミニエディタと HTML タグを使用します。
- ステップ 4** [設定 (Settings)] では、次のことが可能です。
- 異なる電子メールで [ユーザー名とパスワードを個別に送信する (Send username and password separately)]。このオプションを選択すると、ユーザー名電子メール通知とパスワード電子メール通知をカスタマイズするための 2 つのタブが [ページの カスタマイズ (Page Customizations)] に表示されます。
 - 電子メール アドレスへの [テスト電子メールの送信 (Send Test Email)]。すべてのデバイスでカスタマイズをプレビューし、適切に表示されることを確認します。
- ステップ 5** [保存 (Save)] をクリックし、[閉じる (Close)] をクリックします。
-

SMS テキスト メッセージ通知のカスタマイズ

SMS テキスト メッセージでゲストに送信される情報をカスタマイズできます。

始める前に

- SMS ゲートウェイに電子メールを送信して、SMS テキスト メッセージを配信するために使用される SMTP サーバーを設定します。[管理 (Administration)]>[システム (System)]>[設定 (Settings)]>[SMTP サーバー (SMTP Server)] を選択します。
- SMS テキスト通知をサポートするようにスポンサー グループを設定します。
- サードパーティ SMS ゲートウェイでアカウントを設定します。[管理 (Administration)]>[システム (Systems)]>[設定 (Settings)]>[SMS ゲートウェイ (SMS Gateway)] を選択します。Cisco ISE では、テキスト メッセージが電子メールとしてゲートウェイに送信され、SMS プロバイダー経由で指定したユーザーにメッセージが転送されます。
- [管理 (Administration)]>[システム (System)]>[管理者アクセス (Admin Access)]>[設定 (Settings)]>[ポータルのカスタマイズ (Portal Customization)] で [HTML を使用したポータルのカスタマイズの有効化 (Enable portal customization with HTML)] がデフォルトで有効になっていることを確認します。

ステップ 1 アカウント登録ゲストポータルおよびスポンサーポータルの場合は、[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)] > [ゲストポータルまたはスポンサーポータル (Guest or Sponsor Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > [SMS 受信または SMS 通知 (SMS Receipt or SMS Notification)] を選択します。

ステップ 2 [メッセージテキスト (Message Text)] をカスタマイズするには、ミニエディタと HTML タグを使用します。SMS テキストメッセージに含まれる、ゲストアカウント情報を指定するには、事前定義済みの変数を使用します。

ステップ 3 [設定 (Settings)] では、次のことが可能です。

- 異なるテキストメッセージで [ユーザー名とパスワードを個別に送信する (Send username and password separately)]。このオプションを選択すると、**ユーザー名メッセージ**と**パスワードメッセージ**をカスタマイズするための 2 つのタブが [ページのカスタマイズ (Page Customizations)] に表示されます。
- 携帯電話への [テストメッセージの送信 (Send Test Message)]。カスタマイズをプレビューし、情報が適切に表示されることを確認します。サポートされる電話番号の形式には、+1 ###-###-####、###-###-####、(###) ###-####、#####、1##### などがあります。

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。

印刷通知のカスタマイズ

ゲスト用に印刷される情報をカスタマイズできます。



(注) 各ポータル内では、印刷通知ロゴは、電子メール通知ロゴの設定から継承されます。

始める前に

[管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [設定 (Settings)] > [ポータルのカスタマイズ (Portal Customization)] で [HTML を使用したポータルのカスタマイズの有効化 (Enable portal customization with HTML)] がデフォルトで有効になっていることを確認します。

ステップ 1 [アカウント登録ゲスト (Self-Registered Guest)] ポータルと [スポンサー (Sponsor)] ポータルの場合は、[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)] > [ゲストポータルまたはスポンサーポータル (Guest or Sponsor Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > [印刷受け取りまたは印刷通知 (Print Receipt or Print Notification)] を選択します。

ステップ 2 [印刷説明テキスト (Print Introduction Text)] を指定します。電子メールメッセージに含まれる、ゲストアカウント情報を指定するには、事前定義済みの変数を使用します。テキストをカスタマイズするには、ミニエディタと HTML タグを使用します。

- ステップ 3** サムネールで、または [印刷プレビュー (Print Preview)] をクリックして、カスタマイズをプレビューします。サムネールでは、HTML のカスタマイズを表示できません。
[印刷プレビュー (Print Preview)] オプションを選択した場合、アカウントの詳細を印刷できるウィンドウが表示され、そこで適切に表示されることを確認します。
- 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。

承認要求の電子メールでの通知のカスタマイズ

アカウント登録ゲストのアカウントが作成され、そのゲストがログインクレデンシャルを取得する前に、アカウント登録ゲストを承認するようスポンサーに要求できます。電子メールでスポンサーに送信される、承認を要求する情報をカスタマイズできます。この通知は、ネットワークアクセスを許可する前にアカウント登録ゲストポータルを使用するアカウント登録ゲストを承認する必要があると指定した場合にのみ表示されます。

始める前に

- 電子メールでの通知を有効にするように SMTP サーバーを設定します。[管理 (Administration)] > [システム (Systems)] > [設定 (Settings)] > [SMTP サーバー (SMTP Server)] を選択します。
- ゲストへの電子メールでの通知のサポートを設定します。[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [設定 (Settings)] > [ゲスト電子メールの設定 (Guest Email Settings)] を選択します。[ゲストへの電子メール通知を有効にする (Enable email notifications to guests)] をオンにします。
- スポンサーに自己登録アカウントの要求を承認させるには、[ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] タブの [アカウント登録ページの設定 (Self-Registration Page Settings)] 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)] をオンにします。それによって、[ポータルページのカスタマイズ (Portal Page Customization)] の [通知 (Notifications)] の下の [承認要求の電子メール (Approval Request Email)] タブが有効になり、スポンサーに送られる電子メールをカスタマイズできます。

ステップ 1 [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)] > [設定 (Configure)] > [アカウント登録ゲストポータル (Self-Registered Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > [承認要求電子メール (Approval Request Email)] を選択します。ここでは次を実行できます。

ステップ 2 次の手順を実行します。

- a) [グローバルページのカスタマイズ (Global Page Customizations)] で指定されたデフォルトの [ロゴ (Logo)] を変更します。
- b) [件名 (Subject)] および [電子メール本文 (Email body)] を指定します。電子メールメッセージに含まれる、ゲストアカウント情報を指定するには、事前定義済みの変数を使用します。テキストをカスタマイズするには、ミニエディタと HTML タグを使用します。たとえば、リクエスト承認の電子メール

ルにスポンサーポータルへのリンクを含めるには、[リンクを作成 (Create a Link)] をクリックして、スポンサーポータルに FQDN を追加します。

- c) [テスト電子メールの送信 (Send Test Email)] を使用してすべてのデバイスでカスタマイズをプレビューし、適切に表示されることを確認します。
- d) [保存 (Save)] をクリックし、[閉じる (Close)] をクリックします。

ステップ 3 スポンサーが送信する承認電子メールの内容をカスタマイズします。

- a) [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)] を選択します。
- b) [ポータルページのカスタマイズ (Portal Page Customizations)] をクリックします。
- c) [電子メール通知 (Email Notification)] タブをクリックし、詳細を入力します。

エラーメッセージの編集

ゲスト、スポンサー、および従業員に表示される [失敗 (Failure)] ページに表示されるエラーメッセージを完全にカスタマイズできます。[失敗 (Failure)] ページは、[ブラックリスト (Black)] ポータルを除くすべてのエンドユーザー Web ポータルで利用可能です。

ステップ 1 次のいずれかを実行します。

- [ゲスト (Guest)] ポータルの場合は、[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)] > [ゲストポータル (Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > [メッセージ (Messages)] > [エラーメッセージ (Error Messages)] を選択します。
- [スポンサー (Sponsor)] ポータルの場合は、[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)] > [スポンサーポータル (Sponsor Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > [メッセージ (Messages)] > [エラーメッセージ (Error Messages)] を選択します。
- [デバイス (Device)] ポータルの場合は、[管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > [メッセージ (Messages)] > [エラーメッセージ (Error Messages)] を選択します。

ステップ 2 [表示言語 (View In)] ドロップダウンから、メッセージのカスタマイズ時にテキストを表示する言語を選択します。

このドロップダウンリストには、特定のポータルに関連付けられた言語ファイルのすべての言語が含まれています。ポータルページのカスタマイズ時に行った変更でサポート対象の言語プロパティファイルを更新します。

ステップ 3 エラーメッセージテキストを更新します。特定のエラーメッセージを検索するには、エラーメッセージに関連付けられた AUP を検索する **aup** などのキーワードを入力します。

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。

ポータルページのタイトル、コンテンツおよびラベルの文字数制限

[ポータルページのカスタマイズ (Portal Page Customization)] タブのタイトル、テキストボックス、手順、フィールド、ボタンラベル、およびその他の視覚的な要素に入力できる文字数には上限および下限があります。

ポータルページのタイトル、コンテンツおよびラベルの文字数制限

ポータルページの UI 要素へのナビゲーションパスは、次のとおりです。

- ゲストポータルの場合、[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)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > [ページ (Pages)] を選択します。
- スポンサーポータルの場合、[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 (Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > [ページ (Pages)] の順に選択します。
- デバイスポータルの場合、[管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > ページ を選択します。

タイトル、テキストボックス、手順、フィールドとボタンのラベル、およびカスタマイズしているポータルページのその他のビジュアル要素のコンテンツを入力する際に、この情報を使用します。これらの更新は、カスタマイズしている特定のページにのみ適用されます。



(注) シングルバイト文字とマルチバイト文字のどちらを入力するかにかかわらず、識別される最大文字数のみをフィールドに入力できます。マルチバイト文字は文字数制限には影響しません。

フィールドのカテゴリ	フィールド	フィールドラベル：最小文字数	フィールドラベル：最大文字数	フィールドの入力値：最小文字数	フィールドの入力値：最大文字数
共通のページ要素	バナータイトル				256
	フッター要素			[0]	2000

フィールドのカテゴリ	フィールド	フィールドラベル：最小文字数	フィールドラベル：最大文字数	フィールドの入力値：最小文字数	フィールドの入力値：最大文字数
	ブラウザページのタイトル			[0]	256
	説明テキスト			[0]	2000
	コンテンツタイトル			[0]	256
	オプションコンテンツ 1			[0]	2000
	オプションコンテンツ 2			[0]	2000
	ボタンラベル	[0]	64		
	チェックボックスラベル	[0]	64		
	タブラベル	[0]	64		
	リンクラベル	[0]	256		
AUP	AUP テキスト			0	50,000
メッセージテキスト	メッセージテキスト (ページに表示)			[0]	2000
	メッセージテキスト (ポップアップウィンドウに表示)			[0]	256

フィールドの カテゴリ	フィールド	フィールド ラベル：最 小文字数	フィールドラ ベル：最大文字数	フィールドの入力 値：最小文字数	フィールドの入力 値：最大文字数
フィー ルドラ ベル	すべての フィールド ラベル	[0]	256		
フィー ルド入 力（一 般）	一般的な フィールド 入力（次の 特別な場合 を参照）			[0]	256
フィー ルド入 力（特 別な場 合）	[アクセス コード （Access Code）] フィールド			1	20
	[登録コード （Registration Code）] フィールド			1	20
	[ユーザー名 （Username）] フィールド			1	64
	[パスワード （Password）] フィールド			1	256
	[電話番号 （Phone Number）] フィールド			[0]	64
	[デバイス ID （Device ID）] フィー ルド			12	17

ポータルのカスタマイズ

エンドユーザー Web ポータルおよびゲストエクスペリエンスの外観をカスタマイズできます。カスケーディングスタイルシート (CSS) 言語と Javascript の使用経験がある場合、ポータルページのレイアウトを変更することで、jQuery Mobile ThemeRoller アプリケーションを使用してポータルのテーマをカスタマイズできます。

必要なポータルページから CSS テーマまたは言語プロパティをエクスポートすることで、すべてのフィールドを表示できます。詳細については、「[ポータルのデフォルトテーマ CSS ファイルのエクスポート](#)」を参照してください。

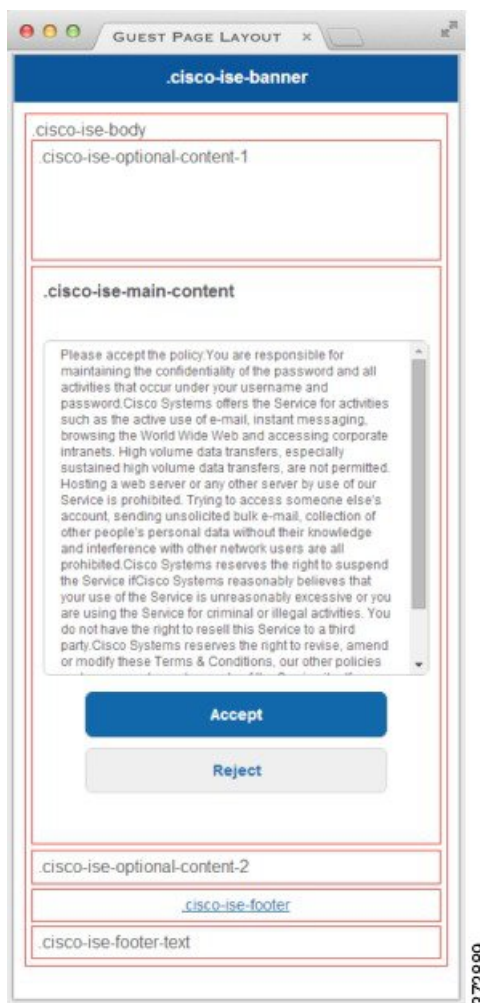
エンドユーザー ポータルのページレイアウトの CSS クラスと説明

Cisco ISE エンドユーザー Web ポータルのページレイアウトを定義および変更するには、次の CSS クラスを使用します。

CSS クラス名	説明
cisco-ise-banner	ロゴ、バナーイメージ、およびバナーテキストが含まれます。 スポンサーポータルおよびデバイスポータルでは、このクラスにコンテキストメニューをアクティブ化できるボタンも含まれます。たとえば、このメニューで [ログアウト (Log Out)]、[パスワードの変更 (Change Password)]などのオプションが含まれるポップアップウィンドウを表示できます。
cisco-ise-body	バナーの一部ではないすべてのページの要素が含まれます。
cisco-ise-optional-content-1	デフォルトでは空です。テキスト、リンク、および HTML コードと JavaScript コードを追加できます。
cisco-ise-main-content	説明テキスト、操作ボタン、および cisco-ise-footer コンテナなど、ポータルページのメインコンテンツが含まれます。
cisco-ise-optional-content-2	デフォルトでは空です。テキスト、リンク、および HTML コードと JavaScript コードを追加できます。
cisco-ise-footer	フッターの一部です。 サポートへの問い合わせ や オンラインヘルプ などのリンクのプレースホルダーです。

CSS クラス名	説明
cisco-ise-footer-text	デフォルトでは空です。著作権表示または免責事項など、ポータルページの下部に表示するもののプレースホルダーです。

図 8: エンドユーザー ポータルのページ レイアウトで使用される CSS クラス



ポータル言語ファイルの HTML サポート

各ポータルの圧縮済み言語ファイルには、そのポータルのデフォルト言語プロパティファイルが含まれます。各プロパティファイルには、ポータルに表示される内容を定義するディクショナリ キーが含まれます。

[説明テキスト (Instructional Text)]、[コンテンツ (Content)]、[オプションコンテンツ 1 (Optional Content 1)]、[オプションコンテンツ 2 (Optional Content 2)] の各フィールドの内

容など、ポータルに表示されるテキストをカスタマイズすることができます。これらのフィールドには、デフォルトのコンテンツがあるものと空白のものがあります。

これらのフィールドに関連付けられたディクショナリキーの一部でのみ、その値（テキスト）で HTML がサポートされます。

ブラックリストポータル言語ファイルの HTML サポート

このポータルの [説明テキスト (Instructional Text)]、[コンテンツ (Content)]、[オプションコンテンツ 1 (Optional Content 1)]、および [オプションコンテンツ 2 (Optional Content 2)] テキストボックスへのナビゲーションパスは次のとおりです。[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)]>[ポータルページのカスタマイズ (Portal Page Customization)]>ページ。ミニエディタの [HTML ソースの表示 (View HTML Source)] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。



Note これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.blacklist.ui_reject_message

個人所有デバイスの持ち込みポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト (Instructional Text)]、[コンテンツ (Content)]、[オプションコンテンツ 1 (Optional Content 1)]、および [オプションコンテンツ 2 (Optional Content 2)] テキストボックスへのナビゲーションパスは、次のとおりです。[管理 (Administration)]>[デバイスポータル管理 (Device Portal Management)]>[BYOD ポータル (BYOD Portals)]>[編集 (Edit)]>[ポータルページのカスタマイズ (Portal Page Customization)]>[ページ (Pages)]。ミニエディタの [HTML ソースの表示 (View HTML Source)] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。



(注) これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.guest.ui_contact_instruction_message
- key.guest.ui_byod_welcome_optional_content_1
- key.guest.ui_byod_welcome_optional_content_2

- key.guest.ui_byod_reg_limit_message
- key.guest.ui_byod_reg_content_message
- key.guest.ui_byod_success_manual_reconnect_message
- key.guest.ui_byod_install_winmac_instruction_message
- key.guest.ui_byod_install_optional_content_1
- key.guest.ui_byod_reg_optional_content_2
- key.guest.ui_byod_install_optional_content_2
- key.guest.ui_byod_reg_optional_content_1
- key.guest.ui_byod_reg_instruction_message
- key.guest.ui_byod_welcome_aup_text
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_byod_install_ios_instruction_message
- key.guest.ui_byod_welcome_instruction_message
- key.guest.ui_error_optional_content_2
- key.guest.ui_error_optional_content_1
- key.guest.ui_byod_welcome_renew_cert_message
- key.guest.ui_byod_install_android_instruction_message
- key.guest.ui_byod_install_instruction_message
- key.guest.ui_byod_welcome_config_device_message
- key.guest.ui_byod_success_message
- key.guest.ui_byod_success_unsupported_device_message
- key.guest.ui_byod_success_optional_content_1
- key.guest.ui_byod_success_optional_content_2
- key.guest.ui_error_instruction_message

証明書プロビジョニング ポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト (Instructional Text)]、[コンテンツ (Content)]、[オプションコンテンツ 1 (Optional Content 1)]、および [オプションコンテンツ 2 (Optional Content 2)] テキストボックスへのナビゲーションパスは、次のとおりです。 [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)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal

Page Customization]>[**ページ (Pages)**]。ミニエディタの [HTML ソースの表示 (View HTML Source)] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。



(注) これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.manualcertprov.ui_login_instruction_message
- key.manualcertprov.ui_aup_instruction_message
- key.manualcertprov.ui_changepwd_instruction_message
- key.manualcertprov.ui_post_access_instruction_message
- key.manualcertprov.ui_status_csv_invalid_instruction_message
- key.manualcertprov.ui_login_optional_content_1
- key.manualcertprov.ui_login_optional_content_2
- key.manualcertprov.ui_aup_optional_content_1
- key.manualcertprov.ui_aup_optional_content_2
- key.manualcertprov.ui_changepwd_optional_content_1
- key.manualcertprov.ui_changepwd_optional_content_2
- key.manualcertprov.ui_post_access_optional_content_1
- key.manualcertprov.ui_post_access_optional_content_2
- key.manualcertprov.ui_landing_instruction_message
- key.manualcertprov.ui_status_page_single_generated_content
- key.manualcertprov.ui_status_generated_content

クライアントプロビジョニングポータル言語ファイルの HTML サポート

このポータルの [説明テキスト (Instructional Text)]、[コンテンツ (Content)]、[オプションコンテンツ 1 (Optional Content 1)]、および [オプションコンテンツ 2 (Optional Content 2)] テキストボックスへのナビゲーションパスは、次のとおりです。[**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ポータル (Client Provisioning Portals)**]>[**編集 (Edit)**]>[**ポータルページのカスタマイズ (Portal Page Customization)**]>[**ページ (Pages)**]。ミニエディタの [HTML ソースの表示 (View HTML Source)] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。



(注) これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.guest.ui_client_provision_agent_installed_instructions_without_java_message
- key.guest.ui_contact_instruction_message
- key.guest.ui_success_message
- key.guest.ui_client_provision_unable_to_detect_message
- key.guest.ui_client_provision_instruction_message
- key.guest.ui_client_provision_agent_installation_message
- key.guest.ui_client_provision_posture_agent_check_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_client_provision_agent_installation_instructions_with_no_java_message
- key.guest.ui_success_instruction_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_contact_optional_content_1
- key.guest.ui_client_provision_posture_check_compliant_message
- key.guest.ui_client_provision_optional_content_2
- key.guest.ui_client_provision_optional_content_1
- key.guest.ui_error_optional_content_2
- key.guest.ui_error_optional_content_1
- key.guest.ui_client_provision_posture_check_non_compliant_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_client_provision_posture_agent_scan_message

クレデンシャル ゲスト ポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト (Instructional Test)]、[コンテンツ (Content)]、[オプションコンテンツ 1 (Optional Content 1)]、および [オプションコンテンツ 2 (Optional Content 2)] テキストボックスへのナビゲーションパスは、次のとおりです。[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)]>[ゲストポータル (Guest Portals)]>[編集 (Edit)]>[ポータルページのカスタマイズ (Portal Page Customization)]>[ページ (Pages)]。ミニエディタの [HTML ソースの表示 (View HTML Source)] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。



(注) これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.guest.ui_contact_instruction_message
- key.guest.ui_login_optional_content_1
- key.guest.ui_login_optional_content_2
- key.guest.ui_client_provision_unable_to_detect_message
- key.guest.ui_client_provision_instruction_message
- key.guest.ui_device_reg_optional_content_2
- key.guest.ui_device_reg_optional_content_1
- key.guest.ui_byod_success_manual_reconnect_message
- key.guest.ui_byod_reg_optional_content_2
- key.guest.ui_byod_reg_optional_content_1
- key.guest.ui_client_provision_agent_installation_instructions_with_no_java_message
- key.guest.ui_success_instruction_message
- key.guest.ui_max_devices_instruction_message
- key.guest.ui_max_devices_optional_content_1
- key.guest.ui_self_reg_results_instruction_message
- key.guest.notification_credentials_email_body
- key.guest.ui_max_devices_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_byod_install_ios_instruction_message

- key.guest.ui_changepwd_instruction_message
- key.guest.ui_client_provision_posture_check_compliant_message
- key.guest.ui_aup_instruction_message
- key.guest.ui_changepwd_optional_content_2
- key.guest.ui_changepwd_optional_content_1
- key.guest.ui_self_reg_results_optional_content_2
- key.guest.ui_self_reg_results_optional_content_1
- key.guest.ui_device_reg_instruction_message
- key.guest.ui_byod_welcome_renew_cert_message
- key.guest.ui_vlan_execute_message
- key.guest.ui_byod_install_android_instruction_message
- key.guest.ui_client_provision_posture_check_non_compliant_message
- key.guest.ui_byod_install_instruction_message
- key.guest.ui_device_reg_max_reached_message
- key.guest.ui_byod_success_message
- key.guest.ui_byod_success_unsupported_device_message
- key.guest.ui_byod_success_optional_content_1
- key.guest.ui_byod_success_optional_content_2
- key.guest.ui_aup_employee_text
- key.guest.ui_client_provision_agent_installed_instructions_without_java_message
- key.guest.ui_success_message
- key.guest.ui_byod_welcome_optional_content_1
- key.guest.ui_byod_welcome_optional_content_2
- key.guest.ui_self_reg_optional_content_2
- key.guest.ui_self_reg_optional_content_1
- key.guest.ui_byod_reg_limit_message
- key.guest.notification_credentials_print_body
- key.guest.ui_byod_reg_content_message
- key.guest.ui_client_provision_agent_installation_message
- key.guest.ui_post_access_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_byod_install_winmac_instruction_message

- key.guest.ui_aup_guest_text
- key.guest.ui_byod_install_optional_content_1
- key.guest.ui_byod_install_optional_content_2
- key.guest.ui_byod_reg_instruction_message
- key.guest.ui_aup_optional_content_1
- key.guest.ui_aup_optional_content_2
- key.guest.ui_self_reg_aup_text
- key.guest.ui_login_instruction_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_self_reg_results_aup_text
- key.guest.ui_device_reg_register_message
- key.guest.ui_byod_welcome_instruction_message
- key.guest.ui_client_provision_optional_content_2
- key.guest.ui_self_reg_instruction_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_post_access_instruction_message
- key.guest.ui_post_access_optional_content_2
- key.guest.ui_post_access_optional_content_1
- key.guest.ui_byod_welcome_config_device_message
- key.guest.ui_client_provision_posture_agent_scan_message

ホットスポット ゲスト ポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト (Instructional Test)]、[コンテンツ (Content)]、[オプションコンテンツ 1 (Optional Content 1)]、および [オプションコンテンツ 2 (Optional Content 2)] テキストボックスへのナビゲーションパスは、次のとおりです。[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**)]>[ゲストポータル (**Guest Portals**)]>[編集 (**Edit**)]>[ポータルページのカスタマイズ (**Portal Page Customization**)]>[ページ (**Pages**)]。ミニエディタの [HTML ソースの表示 (View HTML Source)] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。



(注) これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.guest.ui_contact_instruction_message
- key.guest.ui_success_message
- key.guest.ui_post_access_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_success_instruction_message
- key.guest.ui_aup_optional_content_1
- key.guest.ui_aup_optional_content_2
- key.guest.ui_vlan_unsupported_error_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_aup_instruction_message
- key.guest.ui_aup_hotspot_text
- key.guest.ui_vlan_execute_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_post_access_instruction_message
- key.guest.ui_post_access_optional_content_2
- key.guest.ui_post_access_optional_content_1

モバイル デバイス管理ポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト (Instructional Text)]、[コンテンツ (Content)]、[オプションコンテンツ 1 (Optional Content 1)]、および [オプションコンテンツ 2 (Optional Content 2)] の各テキストボックスへのナビゲーションパスは、次のとおりです。[管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)] > [MDM ポータル (MDM Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > [ページ

(Pages)]。ミニエディタの [HTML ソースの表示 (View HTML Source)] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。

- key.mdm.ui_contact_instruction_message
- key.mdm.ui_mdm_enrollment_after_message
- key.mdm.ui_error_optional_content_2
- key.mdm.ui_error_optional_content_1
- key.mdm.ui_mdm_enroll_optional_content_1
- key.mdm.ui_mdm_enroll_optional_content_1
- key.mdm.ui_mdm_enroll_optional_content_2
- key.mdm.ui_mdm_enroll_instruction_message
- key.mdm.ui_error_instruction_message
- key.mdm.ui_mdm_enrollment_link_message
- key.mdm.ui_mdm_not_reachable_message
- key.mdm.ui_contact_optional_content_2
- key.mdm.ui_mdm_continue_message
- key.mdm.ui_contact_optional_content_1

デバイス ポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト (Instructional Text)]、[コンテンツ (Content)]、[任意のコンテンツ1 (Optional Content 1)]、および [任意のコンテンツ2 (Optional Content 2)] テキストボックスへのナビゲーションパスは、[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)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > [ページ (Pages)] です。ミニエディタの [HTML ソースの表示 (View HTML Source)] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。



(注) これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.mydevices.ui_add_optional_content_1
- key.mydevices.ui_add_optional_content_2

- key.mydevices.ui_post_access_instruction_message
- key.mydevices.ui_edit_instruction_message
- key.mydevices.ui_contact_optional_content_2
- key.mydevices.ui_contact_optional_content_1
- key.mydevices.ui_changepwd_optional_content_1
- key.mydevices.ui_changepwd_optional_content_2
- key.mydevices.ui_post_access_message
- key.mydevices.ui_home_instruction_message
- key.mydevices.ui_edit_optional_content_1
- key.mydevices.ui_edit_optional_content_2
- key.mydevices.ui_add_instruction_message
- key.mydevices.ui_post_access_optional_content_2
- key.mydevices.ui_post_access_optional_content_1
- key.mydevices.ui_error_instruction_message
- key.mydevices.ui_actions_instruction_message
- key.mydevices.ui_home_optional_content_2
- key.mydevices.ui_aup_optional_content_1
- key.mydevices.ui_aup_optional_content_2
- key.mydevices.ui_home_optional_content_1
- key.mydevices.ui_changepwd_instruction_message
- key.mydevices.ui_contact_instruction_message
- key.mydevices.ui_aup_employee_text
- key.mydevices.ui_login_optional_content_2
- key.mydevices.ui_login_optional_content_1
- key.mydevices.ui_login_instruction_message
- key.mydevices.ui_error_optional_content_1
- key.mydevices.ui_error_optional_content_2
- key.mydevices.ui_aup_instruction_message

スポンサー ポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト (Instructional Test)]、[コンテンツ (Content)]、[オプションコンテンツ 1 (Optional Content 1)]、および [オプションコンテンツ 2 (Optional Content 2)] テ

キストボックス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)]>[編集 (Edit)]>[ポータルページのカスタマイズ (Portal Page Customization)]>[ページ (Pages)]です。ミニエディタの [HTML ソースの表示 (View HTML Source)] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。



(注) これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.sponsor.ui_aup_instruction_message
- key.sponsor.ui_create_random_instruction_message
- key.sponsor.ui_home_instruction_message
- key.sponsor.ui_post_access_instruction_message
- key.sponsor.notification_credentials_print_body
- key.sponsor.ui_aup_sponsor_text
- key.sponsor.ui_create_accounts_access_info_instruction_message
- key.sponsor.ui_login_instruction_message
- key.sponsor.notification_credentials_email_body
- key.sponsor.ui_create_known_instruction_message
- key.sponsor.ui_create_import_instruction_message
- key.sponsor.ui_suspend_account_instruction_message
- key.sponsor.ui_post_access_message
- key.sponsor.ui_login_optional_content_2
- key.sponsor.ui_login_optional_content_1
- key.sponsor.notification_credentials_email_password_body
- key.sponsor.ui_contact_optional_content_2
- key.sponsor.ui_contact_optional_content_1
- key.sponsor.ui_login_aup_text
- key.sponsor.ui_changepwd_instruction_message
- key.sponsor.ui_create_accounts_guest_type_instruction_message
- key.sponsor.ui_changepwd_optional_content_1
- key.sponsor.ui_changepwd_optional_content_2
- key.sponsor.notification_credentials_email_username_body

- key.sponsor.ui_aup_optional_content_1
- key.sponsor.ui_aup_optional_content_2
- key.sponsor.ui_post_access_optional_content_1
- key.sponsor.ui_post_access_optional_content_2
- key.sponsor.ui_contact_instruction_message

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。