ゲスト アクセスの設定

Cisco ISE ゲスト サービス

Cisco Identity Services Engine（ISE）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 サービスは次のページで設定します。

- ゲスト ポータル，（23 ページ）
- ゲスト タイプおよびユーザ ID グループ，（3 ページ）
- スポンサー ポータル，（42 ページ）
- スポンサー グループ，（45 ページ）

ISE コミュニティ リソース

ISE ゲストおよび 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 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、およびレポート機能を提供します。

管理ノード

エンドユーザ ポータルでユーザまたはデバイスに対して行う設定変更は、すべて管理ノードに書き込まれます。

ポリシー サービス ノード

エンドユーザ ポータルはポリシー サービス ノードで実行する必要があります。ここでは、ネットワーク アクセス、クライアント プロビジョニング、ゲスト サービス、ポスチャ、およびプロファイリングを含むすべてのセッション トラフィックが処理されます。ポリシー サービス ノードがノード グループに含まれる場合、ノードで障害が発生すると、他のノードが障害を検出し、保留中のセッションをリセットします。

モニタリング ノード

モニタリング ノードは、デバイス ポータル、スポンサー ポータル、およびゲスト ポータルでのエンドユーザおよびデバイスのアクティビティについて、データを収集、集約、およびレポートします。プライマリ モニタリング ノードで障害が発生した場合は、セカンダリ モニタリング ノードが自動的にプライマリ モニタリング ノードになります。

ゲスト アカウントとスポンサー アカウント

ゲスト サービスでは、さまざまなタイプのユーザ（ゲスト、スポンサー、および従業員）がサポートされています。管理者ポータルで、スポンサーのアクセス権限および機能サポートを定義します。これで、スポンサーはスポンサー ポータルにアクセスし、ゲスト アカウントを作成および管理します。

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。

ID ストア（Active Directory、LDAP、内部ユーザなど）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。

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、担当者、顧客、その他のユーザを表します。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 ポータルを使用して、承認ユーザ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。

ゲスト アカウント

ゲストとは、通常、ネットワークへのアクセスを必要とする承認ユーザ、担当者、顧客、その他の一時ユーザを表します。ただし、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。

ゲスト タイプおよびユーザ ID グループ

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：長い期間（最大 1 年）、ネットワークへのアクセスを必要とするユーザ。
- 日次：1 ～ 5 日間の短期間に、ネットワーク リソースへのアクセスを必要とするゲスト。
- 週次：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。

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 タイプを使用するに設定できます。また、

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日次ゲスト 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 ID グループを定義します。ユーザ ID グループは、[管理（Administration）] > [IDの管理（Identity Management）] > [グループ（Groups）] > [ユーザIDグループ（User Identity Groups）] で設定されます。特定のゲスト タイプの削除によってのみ、ゲストのユーザ ID グループを削除できます。

詳細については、以下を参照してください。

- ユーザ ID グループ
- ユーザ 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。ユーザが行った変更は、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適用されます。ログインしているゲストユーザには、ログアウトして再度ログインするまでこれらの変更は表示されません。また、ゲスト タイプを複製して、同じアクセス権限を持つ追加のゲスト タイプを作成できます。

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。

- [ゲスト タイプ名（Guest type name）]：このゲスト タイプを、デフォルトのゲスト タイプや作成したその他の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）]：このフィールドでは、サポート対象のすべての言語で、電子メールの件名、電子メール メッセージ、および SMS メッセージの内容を含む言語ファイルをエクスポートおよびインポートできます。これらの言語とコンテンツは、アカウントが期限切れになった旨の通知に使用され、このゲスト タイプに割り当てられているゲストに送信されます。新しいゲスト タイプを作成すると、ゲスト タイプを保存するまではこの機能は無効です。言語ファイルの編集の詳細については、ポータル言語のカスタマイズ を参照してください。
- [追加データの収集（Collect Additional Data）]：ゲストから追加の情報を収集するにはカスタム フィールドを選択します。

  カスタム フィールドは、[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）] で管理されます。
- **最大アクセス時間（Maximum Access Time）**

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

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

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

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

  値の範囲は 1 ～ 999 です。

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

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

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, （57 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 タイプが同時に実行できる最大ユーザ セッション数を入力します。
  - [ゲストが制限を超えた場合（When guest exceeds limit）]：[最大同時ログイン数（Maximum simultaneous logins）] を選択した場合は、その制限に到達した後にユーザが接続したときに実行するアクションも選択する必要があります。
    - 最も古い接続を切断（Disconnect the oldest connection）
    - [最も新しい接続を切断（Disconnect the newest connection）]：[エラーメッセージを示すポータルページにユーザをリダイレクトする（Redirect user to a portal page showing an error message）] をオプションで選択：特定の時間にわたってエラー メッセージが表示され、その後セッションが切断されてユーザがゲスト ポータルにリダイレクトされます。エラー メッセージが表示される時間は設定可能です。エラー ページの内容は、[メッセージ（Messages）] > [エラーメッセージ（Error Messages）] 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。
- [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。
- [ゲストに対しゲスト ポータルのバイパスを許可する（Allow guest to bypass the Guest portal）]：クレデンシャルを持つゲストのキャプティブ 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。

  この設定を有効にしない場合、ユーザは初めにクレデンシャルを持つゲストのキャプティブ ポータルを使用してログインしないと、ネットワークの他の部分にアクセスできません。

• アカウント有効期限通知

- [アカウント有効期限の __ 日前にアカウント有効期限通知を送信する（Send account expiration notification __ days before account expires）]：アカウントが期限切れになる前にゲストに通知を送信します。有効期限前の日数、時間数、または分数を指定します。
- [メッセージ表示原語（View messages in）]：電子メールまたは SMS 通知の表示言語を指定します。
- [電子メール（Email）]：アカウント有効期限通知を電子メールで送信します。
- [次のポータルのカスタマイズを使用する（Use customization from）]：選択したポータルに対して設定した同一のカスタマイズ内容をこのゲスト タイプのアカウント有効期限メールに適用します。
- [テキストのコピー元（Copy text from）]：別のゲスト タイプのアカウント有効期限メールに、作成した電子メール テキストを再利用します。
- テスト電子メールの送信先（Send test email to me at）
- [SMS]：アカウント有効期限通知を SMS で送信します。

  SMS の設定は、電子メール通知の設定と同一ですが、[テスト SMS の送信（Send test SMS to me）] の SMS ゲートウェイを選択する点が異なります。

- [スポンサー グループ（Sponsor Groups）]：このゲスト タイプを使用してゲスト 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。

次の作業

- 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。詳細については、スポンサー グループ, （45 ページ）を参照してください。
- 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。詳細については、アカウント登録ゲスト ポータルの作成, （35 ページ）を参照してください。

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。

ステップ 1 必要に応じて、次のいずれか 1 つまたは両方を実行します。

- [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 and Components）][> ゲスト タイプ（Guest Type）] を選択し、[スポンサー グループ（Sponsor Groups）] の特定のゲスト タイプを使用して、すべてのスポンサー グループを削除します。このアクションにより、すべてのスポンサーが新しいゲスト アカウントの作成に使用されることを効果的に回避できます。
- [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。特定のゲスト タイプを使用しているアカウント登録ゲスト ポータルを選択し、アカウント登録ゲストの割り当てゲスト タイプを変更します。

ステップ 2 [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

ゲスト アカウント属性の変更

ゲスト アカウントが作成されると、属性はゲスト タイプによってそのアカウントに設定されます。

ゲストタイプに変更を加えた場合、アクティブなゲストアカウントは、デフォルトのアクセス時刻、日付、期間など、更新されたゲスト タイプのすべての属性を引き受けます。それらは後で編集できます。さらに、元のゲスト タイプからカスタム フィールドが更新されたゲスト タイプにコピーされます。

スポンサーは、期限切れになる前にアカウント有効期間を延長することもできます。

エンドポイント ユーザの最大同時ログイン数の設定

ゲスト ユーザ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、ユーザの既存のログイン数がチェックされます。達していた場合、ゲスト ユーザはエラー ページにリダイレクトされます。ユーザがエラー ページを確認できる設定可能な期間が経過すると、セッションは終了します。ユーザがインターネットに再度アクセスしようとすると、そのユーザはゲスト ポータルのログイン ページにリダイレクトされます。

許可ポリシーで、属性 *Network Access.SessionLimitExceeded* に対する値をチェックし、セッションの最大数に達した場合に実行するアクションを設定します。

はじめる前に

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、最大ログイン数は機能しません。

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 タイプ（Guest Type）] の順に選択し、[ログイン オプション（Login Options）] の下で次の操作を実行します。

a) [最大同時ログイン数（Maximum simultaneous logins）] を有効にします。これは、デフォルトのゲスト タイプですでにイネーブルになっています。

b) [最も新しい接続を切断（Disconnect the newest connection）] を選択し、[エラーメッセージを示すポータルページにユーザをリダイレクトする（Redirect user to a portal page showing an error message）] を選択して、許可する同時ログインの最大数を選択します。

ステップ 2 [ポリシー（Policy）] > [結果（Results）] の順に選択し、許可プロファイルを作成します。

a) [共通タスク（Common Tasks）] で、[Webリダイレクション（Web Redirection）] を選択し、次の操作を実行します。

- 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）] では、任意のゲスト ポータルを選択します。

b) [再認証（Reauthentication）] を選択し、次の手順を実行します。

1. [タイマー（Timer）] に、ユーザがゲスト ポータルのログイン ページ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。
2. [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。

次の作業

[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するには、[メッセージ（Messages）][エラーメッセージ（ErrorMessages）] タブで、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ギング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）] の順に選択します。

ステップ 2 次のオプションのいずれかを選択します。

- 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 3 LDAP および Active Directory ユーザ用に Cisco ISE データベースに保持されているユーザに固有のポータル レコードが、非アクティブの状態で何日経過すると消去されるかを指定します。

ステップ 4 [経過後にポータル ユーザ情報を期限切れにする（Expire portal-user information after）] で、ユーザ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。

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。

ステップ 1 すべてのゲスト ポータルとスポンサー ポータルのカスタム フィールドを追加、編集、または削除するには、[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。

ステップ 2 [カスタム フィールド名（Custom Field Name）] に入力し、ドロップダウン リストからデータ タイプを選択し、カスタム フィールドに関する追加情報を提供するのに役立つヒント テキストを入力します。たとえば、Date of Birth と入力し、[Date-MDY] を選択して、日付形式に関するヒントとして MM/DD/YYYY を入力します。

ステップ 3 [追加（Add）] をクリックします。
カスタム フィールドがリストにアルファベット順またはソート順序のコンテキストで表示されます。

ステップ 4 [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。

（注） カスタム フィールドを削除すると、ゲスト タイプの [カスタム フィールド（Custom Fields）] リスト、およびアカウント登録ゲスト ポータルとスポンサー ポータルの設定で選択できなくなります。フィールドが使用されている場合、[削除（Delete）] は無効になります。

次の作業

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, （4 ページ）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。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, （35 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。

ステップ 1 電子メール設定を指定し、すべてのゲスト ポータルおよびスポンサー ポータルの SMTP サーバを設定するには、[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [設定（Settings）] > [ゲスト電子メールの設定（Guest Email Settings）] の順に選択します。

ステップ 2 [ゲストへの電子メール通知を有効にする（Enable email notifications to guests）] はデフォルトでオンになっています。この設定を無効にした場合、ゲストは、ゲスト ポータルとスポンサー ポータルの設定中に有効にした他の設定に関係なく、電子メールでの通知を受信しません。

ステップ 3 ゲストに電子メールでの通知を送信するために指定されている [デフォルトの送信元メールアドレス（Default “From” email address）] を入力します。たとえば、donotreply@*yourcompany*.com と入力します。

ステップ 4 次のいずれかを実行します。

- ゲストのアカウントを作成したスポンサーからの通知をゲストが受信するようにする場合は、[スポンサーの電子メール アドレスから通知を送信する（スポンサードの場合）（Send notifications from sponsor's email address (if sponsored)）] をオンにします。アカウント登録ゲストは、デフォルトの電子メール アドレスから通知を受信します。

- ゲストがスポンサードかアカウント登録かに関係なく通知を受信するようにする場合は、[常にデフォルトの電子メール アドレスから通知を送信する（Always send notifications from the default email address）] をオンにします。

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 [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 3 [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) [追加（Add）] をクリックします。

ステップ 4 [保存（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。

次の作業

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, （46 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, （35 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 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と小文字を区別します。
- 特殊文字 <、>、/、および % は使用できません。

- 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名とパスワードが適切です。必要に応じて ISE でユーザ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。

ステップ 1 [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）] を選択します。

ステップ 2 ゲスト パスワードの [最小パスワード長（Minimum password length）]（文字数）を入力します。

ステップ 3 パスワードの作成にゲストが使用できる各文字セットの文字を指定します。
[許可される文字数と最小値（Allowed Characters and Minimums）] で次のいずれか 1 つのオプションを選択して、ゲスト用のパスワード ポリシーを指定します。

- 各文字セットのすべての文字を使用します。
- 特定の文字の使用を防止するには、ドロップダウン メニューから [カスタム（Custom）] を選択し、その文字を事前定義済みの完全なセットから削除します。

ステップ 4 各セットから、使用する最小文字数を入力します。
4つの文字セットの必須文字数の合計が、全体の最小パスワード長を超えないようにする必要があります。

ステップ 5 [パスワードの有効期限（Password Expiration）] で、次のオプションのいずれかを選択します。

- 最初にログインしてからゲストがパスワードを変更する必要がある頻度（日数）を指定します。期限切れになる前にゲストがパスワードをリセットしないと、次回に元のログイン クレデンシャルを使用してネットワークにログインするときに、パスワードを変更するように促されます。

- パスワードを無期限に設定します。

ステップ 6 [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。

次の作業

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 ユーザ名ポリシーのルール

Cisco ISE には、ゲスト ユーザ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 <、>、/、および % は使用できません。
- 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名を含め、すべてのシステム生成ユーザ名に適用されます。
- パスワードとユーザ名を同じにすることはできません。

ゲスト ユーザ名ポリシーの設定

ゲスト ユーザ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。

ステップ 1 すべてのゲスト ポータルとスポンサー ポータルのゲスト ユーザ名ポリシーを定義するには、[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 ユーザ名ポリシー（Guest Username Policy）] の順に選択します。

ステップ 2 ゲスト ユーザ名の [ユーザ名の最小長（Minimum username length）]（文字数）を入力します。

ステップ 3 [既知のゲストのユーザ名基準（Username Criteria for Known Guests）] で次のいずれか 1 つのオプションを選択して、既知のゲストのユーザ名を作成するためのポリシーを指定します。

ステップ 4 [ランダムに生成されるユーザ名で使用できる文字（Characters Allowed in Randomly-Generated Usernames）] で次のいずれか1つのオプションを選択して、ゲストのランダムユーザ名を作成するためのポリシーを指定します。

- 各文字セットのすべての文字を使用します。
- 特定の文字の使用を防止するには、ドロップダウン メニューから [カスタム（Custom）] を選択し、その文字を事前定義済みの完全なセットから削除します。

ステップ 5 各セットから、使用する最小文字数を入力します。
3 つの文字セットからの合計文字数は、[ユーザ名の最小長（Minimum username length）] に指定されている数を超えないようにする必要があります。

ステップ 6 [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。

次の作業

ユーザ名要件を提示するためのユーザ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 プロバイダーおよびサービス

SMS サービスは、ユーザおよびスポンサーが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 通知を送信する場合に必要となります。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 プロバイダー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 プロバイダーをサポートします。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ーを使用できます。セルラー サービス プロバイダーには、ATT、Orange、Sprint、TMobile、Verizon などがあります。

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 プロバイダー、または Click-A-Tell などのグローバル SMS サービス プロバイダーも追加できます。デフォルトのグローバル SMS サービス プロバイダーには、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 プロバイダーを選択すると、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 プロバイダー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 プロバイダーが SMS 通知の送信に使用されます。
- 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、スポンサーが使用できる適切な SMS サービス プロバイダーをすべて選択する必要があります。スポンサー ポータル用の SMS サービス プロバイダー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 プロバイダーが SMS サービスを提供します。

SMS プロバイダーは、ISE の SMS ゲートウェイとして設定されます。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 サーバの背後に配置できます。

関連トピック

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, （17 ページ）
SMS ゲートウェイ設定（SMS Gateway Settings）

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 プロバイダーのアカウントに固有の情報で更新する必要があります。

はじめる前に

[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 サーバを設定します。

ステップ 1 [管理（Administration）]>[システム（System）]>[設定（Settings）]>[SMS ゲートウェイ（SMS Gateway）] を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [SMS ゲートウェイ プロバイダー名（SMS Gateway Provider Name）] を入力します。

ステップ 4 [プロバイダー インターフェイス タイプ（Provider Interface Type）] を選択し、必要な情報を入力します。

- [SMS 電子メール ゲートウェイ（SMS Email Gateway）]：電子メール サーバ経由で SMS を送信する場合。
- [SMS HTTP API]：HTTP API を介して SMS を送信する場合（GET または POST 方式）。

SMS 電子メール ゲートウェイおよび SMS HTTP API ゲートウェイの設定に関する詳細については、SMS ゲートウェイ設定（SMS Gateway Settings）を参照してください。

ステップ 5 [長いメッセージを複数に分割する（Break up long message into multiple parts）] をオンにして、Cisco ISE で 140 バイトを超えるメッセージを複数のメッセージに分割できるようにします。
ほとんどの SMS プロバイダーは、長い SMS メッセージを自動的に複数に分割します。MMS メッセージは SMS メッセージよりも長くなる可能性があります。

ステップ 6 [送信（Submit）] をクリックします。

次の作業

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, （4 ページ）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, （35 ページ）を参照してください。
- 情報が使用可能なゲストのゲスト アカウントを作成するときにスポンサーが使用できる、SMS サービス プロバイダーを提供します。スポンサー グループの設定, （46 ページ）を参照してください。

自己登録ゲストのソーシャル ログイン

ゲストは、ゲスト ポータルにユーザ名とパスワードを入力する代わりに、自己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。ISE のソーシャル メディア ログインに関する追加情報は、こちらをご覧ください。 https://communities.cisco.com/docs/DOC-73960

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、ポータル設定を構成する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、ユーザ登録なし、ユーザ登録あり、またはユーザ登録とスポンサー承認ありで設定できます。

1. ユーザ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。ユーザは、ソーシャル メディア サイトの基本的なプロファイ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。ISE はソーシャル メディア情報を使用してユーザをログオンします。
4. ログイン後、設定に応じて、ユーザは 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：登録は裏側で行われます。Facebook はログイン用にユーザのデバイスのトークンを ISE に提供します。
   - 登録あり：ユーザには、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、ISEはユーザにアクセス権を電子メール送信します。ユーザはゲスト 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。ユーザは、アカウント自己登録用のゲスト フォームを送信した後、登録フォームの設定に誘導されます。ユーザのアカウントは、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、またはユーザがネットワークから切断するまで、ユーザ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。

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

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

ユーザがエンドポイント グループにまだ存在する場合、ユーザはログオン ページにリダイレクトされます。ユーザ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。

ユーザがもはやエンドポイント グループに属していない場合、ユーザはゲスト 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
  ```

  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。再接続すると、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、ユーザは再接続するたびにゲスト 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。ISE にそのユーザ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 トラッキング

ISE ライブ ログと Facebook

- **認証 ID ストア**：ISE のソーシャル メディア アプリで作成したアプリケーションの名前です。
- **Facebook のユーザ名**：Facebook によって報告されたユーザ名です。ユーザが登録時にユーザ名を変更できるようにする場合、ISE によって報告される名前はソーシャル メディアのユーザ名です。

- **SocialMediaIdentifier**：ここでの
  `https://facebook.com/<number>`
  number はソーシャル メディア ユーザを識別します。

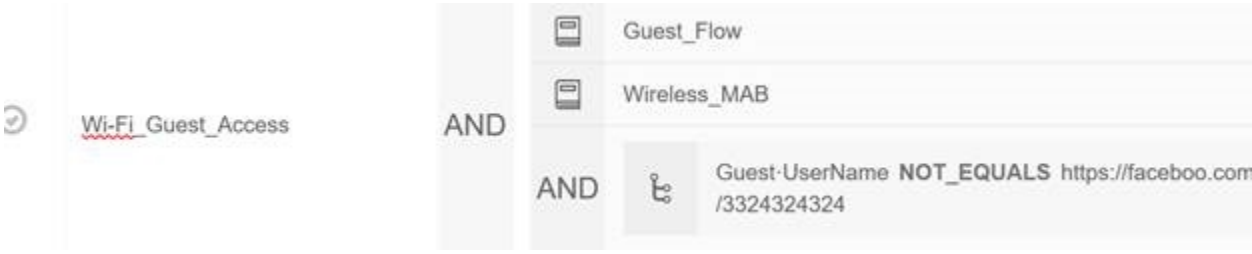
ISE レポート：ゲスト ユーザ名は、ソーシャル メディア サイトのユーザ名です。

Facebook 分析：Facebook の分析を使用して、Facebook のソーシャル ログオンを通じてゲスト ネットワークを使用しているユーザを確認することができます。

ワイヤレスと Facebook：ワイヤレス コントローラの [ユーザ名（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（Monitor）]>[クライアント（Clients）]>[詳細（Detail）] に移動し、[ユーザ名（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 ユーザ名を使用してブロックされた Wi-Fi 接続のゲスト ユーザを示します。



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, （21 ページ） を参照してください。

ソーシャル ログインの設定

はじめる前に

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。

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) 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）] を選択します。

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、以下を設定します。

- [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）]

a) 保存します。

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）] で [はい（Yes）] を選択します。

ステップ 4 ISE で、[管理（Administration）] > [ID の管理（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）] をクリックして、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 ID（App ID）] : Facebook アプリケーションからアプリ ID を入力します。
- [アプリ秘密（App Secret）] : Facebook アプリケーションからアプリ秘密を入力します。

ステップ 5 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を有効にします。ポータル ページで、[ポータルおよびページの設定（Portal & Page Settings）]>[ログイン ページの設定（Login Page Settings）] に移動して、[ソーシャル ログインを許可（Allow Social Login）] をオンにします。すると、さらに多くの設定が表示されます。

- [ソーシャル ログイン後に登録フォームを表示（Show registration form after social login）] : これにより、ユーザは Facebook によって提供される情報を変更できます。

- [ゲストの承認が必要（Require guests to be approved）]：スポンサーがアカウントを承認する必要があることをユーザに通知し、ログイン用のクレデンシャルを送信します。

ステップ 6 [管理（Administration）] > [外部 ID ソース（External Identity Sources）] に移動し、[Facebook ログイン（Facebook Login）] ページを選択し、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。

次の作業

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：ネットワーク アクセスはクレデンシャル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 ポリシーの認可（AUP）が承認される必要があります。
- Sponsored-Guest ポータル：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 クレデンシャルが提供されます。
- アカウント登録ゲスト ポータル：ゲストは各自のアカウント クレデンシャルを作成できます。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。

デフォルトのポータルテーマには、管理者ポータルからカスタマイズできる標準のシスコブランドが適用されています。

Wireless Setup には独自のデフォルト テーマ（CSS）があります。ロゴ、バナー、背景画像、色、フォントなどの基本的な設定の一部を変更できます。ISE では、他の設定を変更することでポータルをさらにカスタマイズでき、高度なカスタマイズを行うこともできます。

ゲスト ポータルのクレデンシャル

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。

- ユーザ名：必須。エンドユーザ 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、ユーザ名ポリシーから取得されます。ユーザ名ポリシーはシステムによって生成されたユーザ名のみに適用され、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 ユーザ名ポリシー（Guest Username Policy）] で、ユーザ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、ユーザ名の通知を受け取ることができます。
- パスワード：必須。エンドユーザ 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：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：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

ユーザ認証ポリシーの設定
ゲスト タイプおよびユーザ 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と、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、ゲスト アカウントを管理する必要性が軽減されます。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の一時的なユーザ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テ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。ゲストおよび非ゲストを [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 プロファイルをチェックし、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）] ページがゲスト フローの一部として表示されます。

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, （28 ページ）	必須（Required）	必須（Required）	必須（Required）
ゲスト ポータルの証明書の追加, （28 ページ）	必須（Required）	必須（Required）	必須（Required）
外部 ID ソースの作成, （28 ページ）	N/A	必須（Required）	必須（Required）
ID ソース順序の作成, （30 ページ）	N/A	必須（Required）	必須（Required）
エンドポイント ID グループの作成	必須（Required）	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, （31 ページ）	必須（Required）	N/A	N/A
Sponsored-Guest ポータルの作成, （33 ページ）	N/A	必須（Required）	N/A
アカウント登録ゲスト ポータルの作成, （35 ページ）	N/A	N/A	必須（Required）
ポータルの許可, （40 ページ）	必須（Required）	必須（Required）	必須（Required）
ゲスト ポータルのカスタマイズ, （42 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 Web ポータルをサポートするには、ホストするノードでポータル ポリシー サービスを有効にする必要があります。

ステップ 1 [管理（Administration）] > [システム（System）] > [展開（Deployment）] を選択します。
ステップ 2 ノードをクリックして、[編集（Edit）] をクリックします。
ステップ 3 [全般設定（General Settings）] タブで、[ポリシー サービス（Policy Service）] をオンにします。
ステップ 4 [セッション サービスの有効化（Enable Session Services）] オプションをオンにします。
ステップ 5 [保存（Save）] をクリックします。

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 Web ポータルに使用されるデフォルトの証明書グループ タグは [デフォルト ポータル証明書グループ（Default Portal Certificate Group）] です。

ステップ 1 [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）] を選択します。
ステップ 2 システム証明書を追加し、ポータルに使用する証明書グループ タグに割り当てます。
この証明書グループ タグは、ポータルを作成または編集するときに選択できるようになります。
ステップ 3 [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）] > [作成または編集（Create or Edit）] > [ポータル設定（Portal Settings）] の順に選択します。
ステップ 4 新しく追加された証明書に関連付けられた [証明書グループ タグ（Certificate group tag）] ドロップダウン リストから特定の証明書グループ タグを選択します。

外部 ID ソースの作成

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

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

ステップ 1 [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（詳細は 外部 ID ソースとしての Active Directory を参照）。
- [LDAP]：LDAP ID ソースを追加する場合（詳細は LDAP を参照）。
- [RADIUS トークン（RADIUS Token）]：RADIUS トークン サーバを追加する場合（詳細は RADIUS トークン ID ソース を参照）。
- [RSA SecurID]：RSA SecurID サーバを追加する場合（詳細は RSA ID ソース を参照）。
- [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（詳細は 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, （29 ページ） を参照）。
- [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（を参照）。 自己登録ゲストのソーシャル ログイン, （18 ページ）

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 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）] 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る場合があります。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、『ISE Administrators Guide』の「SAMLv2 Identity Provider as an External Identity Source」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。ユーザにはこのポータルは表示されず、これは単にユーザを 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もあります。

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 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

はじめる前に

Cisco ISE に外部 ID ソースを設定していることを確認します。

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

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

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

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

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

ステップ 4 [選択済み（Selected）] リスト ボックスの ID ソース順序に含めるデータベースを選択します。

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

ステップ 6 [高度な検索リスト（Advanced Search List）] 領域で、次のいずれかのオプションを選択します。

- [順序内の他のストアにアクセスせず、AuthenticationStatus 属性を ProcessError に設定（Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError）]：最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が検索を中止する場合。
- [ユーザが見つからなかったとして処理し、順序内の次のストアに進む（Treat as if the user was not found and proceed to the next store in the sequence）]：最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が順序内の他の選択された ID ソースの検索を続行する場合。

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

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

エンドポイント ID グループの作成

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

ステップ 1 [管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [エンドポイント ID グループ（Endpoint Identity Groups）] を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 作成するエンドポイント ID グループの名前を入力します（エンドポイント ID グループの名前にスペースを入れないでください）。

ステップ 4 作成するエンドポイント ID グループの説明を入力します。

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

ステップ 6 [送信（Submit）] をクリックします。

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。

はじめる前に

- 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 ISE でサポートされていることを確認します。リリースの『**Cisco Identity Services Engine Network Component Compatibility**』ガイド（http://www.cisco.com/c/en/us/td/docs/security/ise/2-1/compatibility/ise_sdt.html など）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）] の順に選択します。

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 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。

次の作業

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）

はじめる前に

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 [ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [設定（Configure）] > [ゲスト ポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] の順に選択します。

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 [Sponsored-Guest ポータル（Sponsored-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 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、ID ソース順序、認証方式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。

- [ログイン ページの設定（Login Page Settings）]：ゲスト クレデンシャルおよびログイン ガイドラインを指定します。[ゲストが自分のアカウントを作成することを許可する（Allow guests to create their accounts）] オプションを選択した場合、ユーザは独自のゲスト アカウントを作成できます。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 アカウントを作成する必要があります。

  （注） [認証方式（Authentication Method）] フィールドで ID プロバイダー IdP）を選択している場合は、[ログインページ設定（Login Page Settings）] オプションは無効です。

- [利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）]：別の AUP ページを追加し、クレデンシャルを持つゲスト ポータルを使用する従業員を含むゲスト用の利用規定の動作を定義します。

- [従業員のパスワード変更の設定（Employee Change Password Settings）]：ゲストに、初めてログインした後にパスワードを変更するように指示します。

- [ゲスト デバイス登録の設定（Guest Device Registration Settings）]：Cisco ISE に自動的にゲスト デバイスが登録されるようにするか、またはゲストが手動でこれらのデバイスを登録できるページを表示するかどうかを選択します。

- [BYOD 設定（BYOD Settings）]：従業員が自分のパーソナル デバイスを使用してネットワークにアクセスすることを許可します。

- [ポストログイン バナーページの設定（Post-Login Banner Page Settings）]：ネットワーク アクセスを許可する前にゲストに追加情報を通知します。

- [ゲスト デバイスのコンプライアンス設定（Guest Device Compliance Settings）]：ゲストを [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し、最初にポスチャ エージェントをダウンロードするように要求します。

- [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。

次の作業

（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。

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）

はじめる前に

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。

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）] の順に選択します。

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 [アカウント登録ゲスト ポータル（Self-Registered 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 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、ID ソース シーケンス、認証方式、およびこのポータルの動作を定義するその他の設定のデフォルト値を更新します。
ポータル設定フィールドの詳細については、クレデンシャルを持つゲスト ポータルのポータル設定を参照してください。

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。

- [ログイン ページの設定（Login Page Settings）]：ゲスト クレデンシャルおよびログイン ガイドラインを指定します。詳細については、クレデンシャルを持つゲスト ポータルのログイン ページ設定を参照してください。
- [アカウント登録成功ページの設定（Self-Registration Success Page Settings）]：アカウント登録が成功したゲストに対して [アカウント登録成功（Self-Registration Success）] ページに表示される情報、および Cisco ISE 登録されたゲストのゲスト エクスペリエンスを指定します。
- [アカウント登録ページの設定（Self-Registration Page Settings）]：ゲストが [アカウント登録（Self-Registration）] フォームを送信した後のゲスト エクスペリエンス以外に、アカウント登録ゲストが読み取る情報、および [アカウント登録（Self-Registration）] フォームに入力する必要がある情報を指定します。
- [利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）]：別の AUP ページを追加し、クレデンシャルを持つゲスト ポータルを使用する従業員を含むゲスト用の利用規定の動作を定義します。詳細については、クレデンシャルを持つゲスト ポータルの利用規定（AUP）ページ設定を参照してください。
- [従業員のパスワード変更の設定（Employee Change Password Settings）]：ゲストに、初めてログインした後にパスワードを変更するように指示します。

- [ゲスト デバイス登録の設定（Guest Device Registration Settings）]：Cisco ISE に自動的にゲスト デバイスが登録されるようにするか、またはゲストが手動でこれらのデバイスを登録できるページを表示するかどうかを選択します。
- [BYOD 設定（BYOD Settings）]：従業員が自分のパーソナル デバイスを使用してネットワークにアクセスすることを許可します。詳細については、クレデンシャルを持つゲスト ポータルの BYOD 設定を参照してください。詳細については、クレデンシャルを持つゲスト ポータルの BYOD 設定を参照してください。
- [ポストログイン バナー ページ設定（Post-Login Banner Page Settings）]：ユーザが正常にログインした後、ネットワーク アクセスを付与される前に追加情報を表示します。
- [ゲスト デバイスのコンプライアンス設定（Guest Device Compliance Settings）]：ポスチャ アセスメントのためにゲストを [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。詳細については、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を参照してください。
- [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。詳細については、クレデンシャルを持つゲスト ポータルの BYOD 設定を参照してください。
- 認証成功の設定（Authentication Success Settings）：認証後のゲストの宛先を指定します。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。詳細については、ゲスト ポータルの認証成功の設定を参照してください。
- [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。

次の作業

（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。

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。

電子メールによるアカウント登録のアカウントの承認

登録ゲストにはアカウントの承認が必要であると設定されている場合、[アカウント登録ページの設定（Self-Registration Page Settings）] で設定されているスポンサーに対して電子メールが送信されます。このメールには、アカウントを拒否または承認するためのリンクが含まれています。

（注）

古いバージョンの Cisco ISE から Cisco ISE 2.2 に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/拒否のリンクを手動で挿入する必要があります。承認/拒否のリンクを手動で挿入するには、次の手順に従います。

1. [アカウント登録ゲスト ポータル（Self-Registered Guest Portal）] を選択します。
2. [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。
3. [承認要求の電子メール（Approval Request Email）] セクションで [承認/拒否のリンクを挿入する（Insert Approve/Deny link）] をクリックします。

承認/拒否リンクを含む承認要求の電子メールの設定については、アカウント承認メール リンクの設定，（39 ページ）を参照してください。

たとえば、スポンサーが電子メールを開いて [承認（Approve）] リンクをクリックすると実行されるアクションは、承認者の設定方法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）]
  - ゲスト アカウントに認証が**不要**な場合、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、スポンサーに対し、スポンサー ポータルの特別なページが表示されます。このページでは、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）]：指定されるすべての電子メールアドレスに承認リンクが電子メールで送信されます。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。スポンサーは、検証済みのクレデンシャルを提供します。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、アカウントは承認されます。クレデンシャルが失敗すると、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指示がスポンサーに対して示されます。

説明

- Active Directory と LDAP を使用するスポンサー ポータルだけがサポートされています。
- [訪問先担当者（person being visited）] を選択した場合、アカウント登録ゲストがそのフィールドに入力する内容は、スポンサーの電子メールアドレスでなければなりません。アカウント登録ポータルをカスタマイズし、そのフィールド名を「スポンサーの電子メール アドレ

ス」のような名前に変更することを推奨します。ゲストの訪問先担当者を取得するため、必要に応じて新しいフィールドを作成できます。ユーザが [登録（Register）] ボタンをクリックすると、ISE により、訪問先担当者が有効なスポンサーであり、電子メール アドレスがあることが確認されます。ISE が ID ソースでそのスポンサーの電子メール アドレスを見つけることができない場合、ISE はエラー メッセージを表示し、アカウント登録が失敗します。

- スポンサーのリストが設定されている場合、1 番目のポータルが、スポンサーがログインするポータルではない場合でも、1 番目のポータルのカスタマイズ内容が使用されます。

アカウント承認メール リンクの設定

アカウント登録ゲストを承認するための承認リンクをスポンサーに電子メールで送信する方法の詳細については、電子メールによるアカウント登録のアカウントの承認, （38 ページ）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（Guest）] > [設定（Configure）] > [ゲスト ポータル（Guest Portals）] に移動し、メール アカウント承認リンクを設定するアカウント登録ポータルを選択します。

ステップ 2 [アカウント登録ページの設定（Self Registration Page Settings）] タブを展開します。

ステップ 3 3.[アカウント登録ゲストの承認が必要である（Require self-registered guests to be approved）] をオンにします。これにより、[承認/拒否のリンクの設定（Approve/Deny Link Settings）] セクションがタブ エリアの下部に表示されます。また、[承認要求メール（Approval Request Email）] の電子メール設定に、承認リンクと拒否リンクが取り込まれます。
[アカウント登録ページの設定（Self Registration Page Settings）] を選択すると表示されるすべてのフィールドを以下に示します。

- [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。詳細については、電子メールによるアカウント登録のアカウントの承認, （38 ページ）を参照してください。
  - [承認要求電子メール送信先（Email approval request to）]：次のいずれかを選択します。
    - [下に示すスポンサーの電子メールアドレス（sponsor email addresses listed below）]：承認者として指名されたスポンサーの 1 つ以上の電子メール アドレス、またはすべてのゲストの承認要求の送信先となるメール ソフトウェアを入力します。
    - [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。
  - [承認/拒否のリンクの設定（Approve/Deny Link Settings）]：このセクションでは次の内容を設定できます。

- [リンクの有効期間（Links are valid for）]：アカウント承認リンクの有効期間を設定できます。
- [スポンサーに承認用クレデンシャルの入力を求める（Require sponsor to provide credentials for authentication ）]：このセクションの設定でスポンサーによるアカウント承認用のクレデンシャルの入力が必須ではない場合にも、スポンサーにこの情報を入力させるには、このフィールドをオンにします。このフィールドは、[アカウント登録ゲストが承認される必要がある（Require self-registered guests to be approved）] が [訪問先担当者（person being visited）] に設定されている場合にだけ表示されます。
- [承認権限を検証するためスポンサーがスポンサー ポータルと照合される（Sponsor is matched to a Sponsor Portal to verify approval privileges）]：[詳細 >（Details >）] をクリックして、スポンサーが有効なシステム ユーザであり、スポンサー グループのメンバーであり、そのスポンサー グループのメンバーにアカウント承認権限があることを確認するために検索されるポータルを選択します。各スポンサー ポータルには、スポンサーを識別するために使用される ID ソース シーケンスがあります。ポータルはリストされている順序で使用されます。リストの 1 番目のポータルは、スポンサー ポータルで使用されているスタイルとカスタマイズ内容を決定します。

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。

はじめる前に

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。

はじめる前に

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

ステップ 1 [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [許可プロファイル（Authorization Profiles）] を選択します。

ステップ 2 使用を許可するポータル名を使用して許可プロファイルを作成します。

次の作業

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

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

ip:port = IP アドレスとポート番号

PortalID = 一意のポータル名

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

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

ステップ 1 [ポリシー（Policy）] > [ポリシー セット（Policy Sets）] を選択して、[標準（Standard）] ポリシーで新しい許可ポリシー ルールを作成します。

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

（注） ホットスポット ゲスト ポータルは、Termination CoA だけを発行するため、ゲスト許可ポリシーの検証条件の 1 つとして [Network Access:UseCase EQUALS Guest Flow] を使用しないでください。代わりに、エンドポイントが属する ID グループに照合して検証を行います。次の例を参考にしてください。

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

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

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

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）] を参照し、AUP の期限が切れた場合にゲスト ユーザをクレデンシャルを持つポータルにリダイレクトする新しい許可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には条件を使用します（たとえば LastAUPAcceptanceHours > 8）。時間の範囲 8 ～ 999 をチェックできます。

次の作業

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. [管理（Administration）] > [ID（Identities）] > [エンドポイント（EndPoints）] を選択します。
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*）。

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す。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、スポンサーユーザに割り当てることができる権限のセットが指定されます。スポンサー ユーザがスポンサー ポータルにログインすると、次の処理が行われます。

1. ISE がユーザのクレデンシャルを検証します。
2. ユーザの認証が成功すると、次にそのスポンサー ユーザに一致するスポンサー グループ、つまりそのユーザが属するスポンサーグループを見つけるため、使用可能なすべてのスポンサーグループが検索されます。次の両方の条件を満たしている場合は、ユーザがスポンサーグループに一致しているか、属しています。
   - ユーザは、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、そのユーザについてすべての条件が true である。
3. スポンサー ユーザがスポンサー グループに属している場合、スポンサー ユーザはそのグループの権限を取得します。ユーザ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。ユーザがどのスポンサー 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適用されます。

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 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す。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せん。

スポンサー ポータルを開く方法はいくつかあります。

- 管理者コンソールで [アカウントの管理（Manage Accounts）] リンクを使用する：管理者コンソールで [ゲスト アクセス（Guest Access）] をクリックし、[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 アクティベーション リクエスト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 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）] ページで設定した FQDN が DNS サーバに存在している必要があります。

- 管理者コンソールのスポンサー ポータル設定ページから、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、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）] ページで設定した URL（FQDN）を開きます。この URL（FQDN）は DNS サーバで定義されている必要があります。

次の作業

スポンサー ポータルの使い方については、『Sponsor Portal User Guide for Cisco Identity Services Engine』（http://www.cisco.com/c/en/us/td/docs/security/ise/2-2/sponsor_guide/b_spons_SponsorPortlUserGuide_22.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 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 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

各スポンサーは、スポンサー グループに属します。スポンサー グループ設定では、そのグループ内のスポンサーの権限と設定が定義されます。Cisco ISE には、次のデフォルトのスポンサー グループがあります。

- 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、自分が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。次に例を示します。

- スポンサーが 1 回の操作で複数のゲスト アカウントを作成することを許可できます。
- スポンサーが作成したゲストアカウントを他のスポンサーが管理することを制限できます。
- ゲスト パスワードをスポンサーが表示することを制限できます。
- アカウント登録ゲストからの要求を承認または拒否する権限をスポンサーに付与できます。
- スポンサーがゲスト アカウントを削除、一時停止、および回復することを許可できます。
- スポンサー グループを無効にして、スポンサー ポータルにメンバーがログインすることを防ぐことができます。

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。

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 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さ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、自分が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。次に例を示します。

関連トピック

スポンサー ポータル, （42 ページ）

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 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 [管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）] を選択します。適切なユーザ ID グループに内部スポンサー ユーザ アカウントを割り当てます。

（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）] の順に選択し、[メンバー（Members）] をクリックします。スポンサー ユーザ ID グループをスポンサー グループにマッピングします。

次の作業

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 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 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）] の順に選択します。

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（Matching Criteria）]：このセクションの設定により、スポンサーがこのグループのメンバーかどうかが判別されます。

- メンバー グループ（Member Groups）：メンバーをクリックして 1 つ以上のユーザ（ID）グループおよび外部 ID ソースのグループを選択し、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 グループに含まれるためにスポンサーが満たす必要がある条件を 1 つ以上構築します。Active Directory、LDAP、SAML、ODBC の ID ストアからの認証属性を使用できますが、RADIUS トークンまたは RSA SecurID ストアは使用できません。内部ユーザ属性も使用できます。条件には、属性、演算子、値があります。
  - ディクショナリ属性 *Name* を使用して条件を作成するには、ID グループ名の前にユーザ ID グループを付けます。次に例を示します。

    InternalUser:Name EQUALS bsmith

    この場合、「bsmith」という名前の内部ユーザだけがこのスポンサー グループに所属できます。
  - 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 ユーザの AD「プライマリ グループ」を選択します。たとえば、ユーザの名前が Smith の場合は *AD1: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 グループに基づくスポンサーによって作成できるゲスト 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）] でボックス内をクリックして、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)）：スポンサーは、ファイルから姓名などのゲストの詳細をインポートすることによって、複数のゲスト アカウントを作成できます。

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

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

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

- [ゲストへの複数のゲスト アカウントの割り当て（ランダム）（Multiple guest accounts to be assigned to any guests (Random)）]：スポンサーが、未知のゲストのプレースホルダとして複数のランダム 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である場合、[ランダム（Random）] ボタンがスポンサー ポータルの [アカウントの作成（Create Accounts）] ページに表示されます。

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

  ユーザ名プレフィックスを指定しないか、またはスポンサーにユーザ名プレフィックスの指定を許可しない場合、スポンサーはスポンサー ポータルでユーザ名プレフィックスを割り当てることができません。
- スポンサーにユーザ名プレフィックスの指定を許可（Allow sponsor to specify a username prefix）：このスポンサー グループが複数のアカウントを同時に作成できる場合、単一のインポート操作で作成可能なゲスト アカウントの数を指定します。

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

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（View guests' 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、そのパスワードを表示できます。

ゲストがパスワードを変更した場合、スポンサーは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しない限り、そのパスワードを表示できません。

（注） このオプションがスポンサー グループで無効になっている場合、そのグループのメンバーは、管理しているゲスト アカウントのログイン クレデンシャル（ゲスト パスワード）に関する電子メールおよび SMS 通知を送信できません。

- ゲストのクレデンシャルを含む SMS 通知の送信（Send SMS notifications with guests' credentials）：スポンサーは、自分が管理できるゲスト アカウントについて、アカウントの詳細とログイン クレデンシャルとともにゲストに SMS（テキスト）通知を送信できます。
- ゲスト アカウント パスワードのリセット（Reset guest account passwords）：スポンサーは、自分が管理できるゲスト アカウントについて、そのパスワードを Cisco ISE によって生成されたランダムなパスワードにリセットできます。
- ゲストのアカウントの延長（Extend guests' accounts）：スポンサーは、自分が管理できるゲスト アカウントについて、その有効期限を延長できます。スポンサーは、アカウントの有効期限に関してゲストに送信される電子メール通知に自動的にコピーされます。
- ゲストのアカウントの削除（Delete guests' accounts）：スポンサーは、自分が管理できるゲスト アカウントについて、アカウントを削除し、ゲストが企業のネットワークにアクセスすることを防ぐことができます。
- ゲストのアカウントの一時停止（Suspend guests' accounts）：スポンサーは、自分が管理できるゲスト アカウントについて、アカウントを一時停止してゲストが一時的にログインすることを防ぐことができます。

  また、このアクションは、許可変更（CoA）終了を発行して、一時停止されていたゲストをネットワークから排除できます。

  - スポンサーに理由の入力を求める（Require sponsor to provide a reason）：ゲスト アカウントの一時停止に対する説明の入力をスポンサーに求めます。

- アカウント登録ゲストからの要求の承認および表示（Approve and view requests from self-registering guests）：このスポンサー グループに含まれているスポンサーは、（承認が必要な）アカウント登録ゲストからのすべての保留中のアカウント要求を表示するか、アクセス先の担当者としてユーザがスポンサーの電子メール アドレスを入力した要求のみを表示できます。この機能では、アカウント登録ゲストによって使用されるポータルで [アカウント登録ゲストが承認される必要がある（Require self-registered guests to be approved）] にマークが付けられていて、スポンサーの電子メールが連絡先の担当者としてリストされている必要があります。

  - [保留中のすべてのアカウント（Any pending accounts）]：このグループに所属するスポンサーは、他のスポンサーによって作成されたアカウントを承認およびレビューします。
  - [このスポンサーに割り当てられている保留中のアカウントのみ（Only pending accounts assigned to this sponsor）]：このグループに所属するスポンサーは、スポンサー自身が作成したアカウントだけを表示および承認できます。

- プログラムによるインターフェイス（Guest REST API）を使用した Cisco ISE ゲスト アカウントへのアクセス（Access Cisco ISE guest accounts using the programmatic interface (Guest REST API)）：スポン

サーは、自分が管理できるゲスト アカウントについて、Guest REST API プログラミング インターフェイスを使用してゲスト アカウントにアクセスできます。

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. ISE で [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名とパスワードのインポート

スポンサーはユーザ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。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 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。

はじめる前に

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, （52 ページ）。
ステップ 2 ゲスト サービスの証明書の追加, （53 ページ）.
ステップ 3 外部 ID ソースの作成, （53 ページ）.
ステップ 4 ID ソース順序の作成, （54 ページ）.
ステップ 5 スポンサー ポータルの作成, （55 ページ）.
ステップ 6 （任意） c_CustomizingSponsorPortals.xml。

ポリシー サービスの有効化

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

ステップ 1 [管理（Administration）] > [システム（System）] > [展開（Deployment）] を選択します。
ステップ 2 ノードをクリックして、[編集（Edit）] をクリックします。
ステップ 3 [全般設定（General Settings）] タブで、[ポリシー サービス（Policy Service）] をオンにします。
ステップ 4 [セッション サービスの有効化（Enable Session Services）] オプションをオンにします。
ステップ 5 [保存（Save）] をクリックします。

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 Web ポータルに使用されるデフォルトの証明書グループ タグは [デフォルト ポータル証明書グループ（Default Portal Certificate Group）] です。

ステップ 1 [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）] を選択します。

ステップ 2 システム証明書を追加し、ポータルに使用する証明書グループ タグに割り当てます。
この証明書グループ タグは、ポータルを作成または編集するときに選択できるようになります。

ステップ 3 [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）] > [作成または編集（Create or Edit）] > [ポータル設定（Portal Settings）] を選択します。

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

外部 ID ソースの作成

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

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

ステップ 1 [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（詳細は 外部 ID ソースとしての Active Directory を参照）。
- [LDAP]：LDAP ID ソースを追加する場合（詳細は LDAP を参照）。
- [RADIUSトークン（RADIUS Token）]：RADIUS トークン サーバを追加する場合（詳細は RADIUS トークン ID ソース を参照）。
- [RSA SecurID]：RSA SecurID サーバを追加する場合（詳細は RSA ID ソース を参照）。

- [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（詳細は 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，（29 ページ） を参照）。
- [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（を参照）。 自己登録ゲストのソーシャル ログイン，（18 ページ）

ID ソース順序の作成

はじめる前に

Cisco ISE に外部 ID ソースを設定していることを確認します。

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

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

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

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

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

ステップ 4 [選択済み（Selected）] リスト ボックスの ID ソース順序に含めるデータベースを選択します。

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

ステップ 6 [高度な検索リスト（Advanced Search List）] 領域で、次のいずれかのオプションを選択します。

- [順序内の他のストアにアクセスせず、AuthenticationStatus 属性を ProcessError に設定（Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError）]：最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が検索を中止する場合。
- [ユーザが見つからなかったとして処理し、順序内の次のストアに進む（Treat as if the user was not found and proceed to the next store in the sequence）]：最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が順序内の他の選択された ID ソースの検索を続行する場合。

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

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

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。

[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。

はじめる前に

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 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 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 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 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 ゲスト パスワード ポリシーと有効期限の設定, （14 ページ） と ゲスト パスワード ポリシーのルール, （13 ページ） の説明に従って、[スポンサーのパスワード変更設定（Sponsor Change Password Settings）] ページを設定します。

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 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 [スポンサーポータルアプリケーションの設定（Sponsor Portal Application Settings）] では、ポータルをカスタマイズする場合は [ポータルのカスタマイズ（Portal Customization）] タブを参照します。

ステップ 7 [保存（Save）] をクリックします。

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

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. ISE で [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名とパスワードのインポート

スポンサーはユーザ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。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。

- **ユーザ名**：User Name または UserName のいずれかを指定します。
- [パスワード（Password）]：password である必要があります。

スポンサーに対して使用可能な時間設定項目の設定

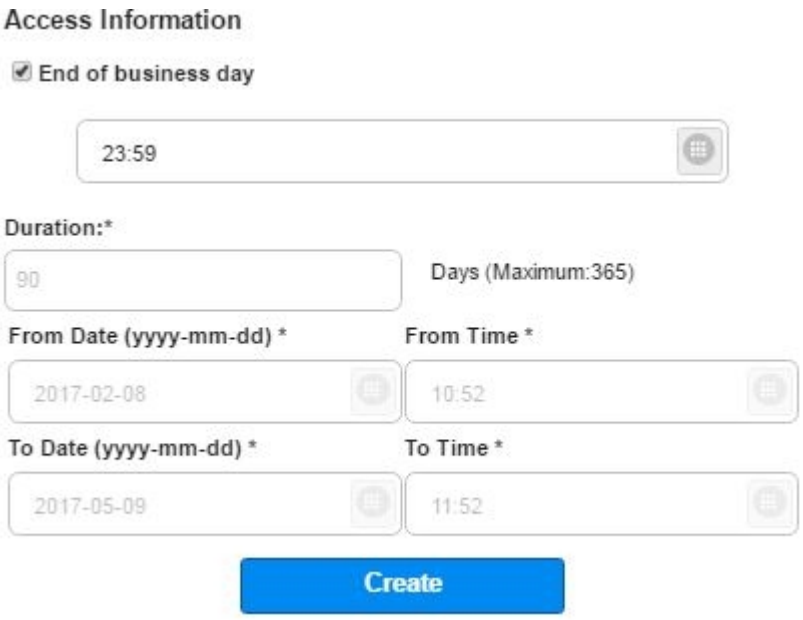
スポンサーは新しいゲスト アカウントを作成するときに、アカウントがアクティブである期間を設定します。スポンサーが使用できるオプションを設定して、スポンサーがアカウントの期間と、開始時刻および終了時刻を設定できるようにすることができます。これらのオプションはゲスト タイプ別に設定されます。スポンサーに対し、[アクセス情報（Access Information）] というヘッダーの下に結果が表示されます。

スポンサーのポータル 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。

- [初回ログインから（From-First-Login）]：スポンサー ポータルには [期間（Duration）] フィールドが表示され、その下に [初回ログインから（From-First-Login）] が表示されます。

  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と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。



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 レコードがデータベース（内部ユーザまたは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 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 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 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

Cisco ISE は、エンドポイントおよびユーザ管理情報、およびゲストとスポンサーのアクティビティを参照できるさまざまなレポートとログを提供します。Cisco ISE 1.2 レポートの一部は廃止されましたが、情報は他のレポートで表示できます。

オン デマンドまたはスケジュール ベースでこれらのレポートを実行できます。

ステップ 1 [操作（Operations）] > [レポート（Reports）] を選択します。

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

ステップ 3 レポートを選択し、[フィルタ（Filters）] ドロップダウン リストを使用して、検索するデータを選択します。
ユーザ名、ポータル名、デバイス名、エンドポイント ID グループ、および他のデータについてフィルタを使用できます。

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

ステップ 5 [実行（Run）] をクリックします。

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、[認証されたゲスト（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

AUP 受け入れステータス レポートには、すべてのゲスト ポータルからの、ゲストによる利用規定（AUP）の受け入れのステータスが示されます。このレポートは、[操作（Operations）] > [レポート（Reports）] > [ゲスト アクセス レポート（Guest Access Reports）] > [AUP 受け入れステータス（AUP Acceptance Status）] から使用できます。

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、[操作（Operations）] > [レポート（Reports）] > [ゲスト アクセス レポート（Guest Access Reports）] > [ゲスト アカウンティング（Guest Accounting）] で利用できます。

マスター ゲスト レポート

マスターゲスト 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。このレポートは、[操作（Operations）] > [レポート（Reports）] > [ゲスト アクセス レポート（Guest Access Reports）] > [マスター ゲスト（Master Guest）] で利用できます。このレポートには、非推奨のゲスト アクティビティ レポートに含まれていた情報も含まれるようになりました。

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。

- 成功した認証のロギング カテゴリを有効にします。[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギング カテゴリ（Logging Categories）] を選択して、[成功した認証（Passed authentications）] を選択します。
- 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。

このレポートは、[操作（Operations）]>[レポート（Reports）]>[ゲスト アクセス レポート（Guest Access Reports）]>[スポンサー ログインおよび監査（Sponsor Login and Audit）] で使用できます。

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。デフォルトでは、これらのメッセージは、/opt/CSCOcpm/logs/localStore/iseLocalStore.log ファイルに記録されます。

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 では、Cisco ISE ゲスト サービスと Web 認証サービスを使用したセキュアなゲスト 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。Web 認証は、有線および無線の両方の接続要求に対して、中央 Cisco ISE RADIUS サーバによって実行されます。ゲスト デバイスの認証は、ゲストが、ホットスポット ゲスト ポータルで任意のアクセス コードを入力し、クレデンシャルを持つゲスト ポータルでユーザ名とパスワードを入力した後、実行されます。
- 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 ポータルに適用されます。ゲストへのWebページの提供は、有線接続の場合にはスイッチなどのネットワーク アクセス デバイス（NAD）で、無線接続の場合にはワイヤレス LAN コントローラ（WLC）によって、ローカルに実行されます。ゲストデバイスの認証は、ゲストが、クレデンシャルを持つゲスト ポータルでユーザ名とパスワードを入力した後、実行されます。
- 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。Web認証は、Cisco ISEによってデバイスが登録され、使用が許可された後、

実行されます。ゲストは、有線または無線接続で（ユーザ名またはパスワードを入力しないで）ネットワークにアクセスできるホットスポット ゲスト ポータルに誘導されます。

ISE コミュニティ リソース

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、「How-To_93_ISE_20_Wireless_Guest_Setup_Guide」を参照してください。

ISE テクニカル ノートも参照してください。http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html

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 ポータルの中央 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央 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 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 クレデンシャルを入力してログイン フォームを送信します。

9 ゲスト サーバはログイン クレデンシャルを認証します。

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 サーバは CoA を NAD に送信します。この CoA により、NAD は Cisco ISE RADIUS サーバを使用してゲスト 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 クレデンシャ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チャ フローの場合、ゲスト デバイスの Web ブラウザに、ポスチャ 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ーブレットにリダイレクトされます。この認証サーブレットで、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、デバイスのポスチャ チェックを実行します（必要に応じて、ポスチャ 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（AD）および LDAP ユーザにも適用できます。

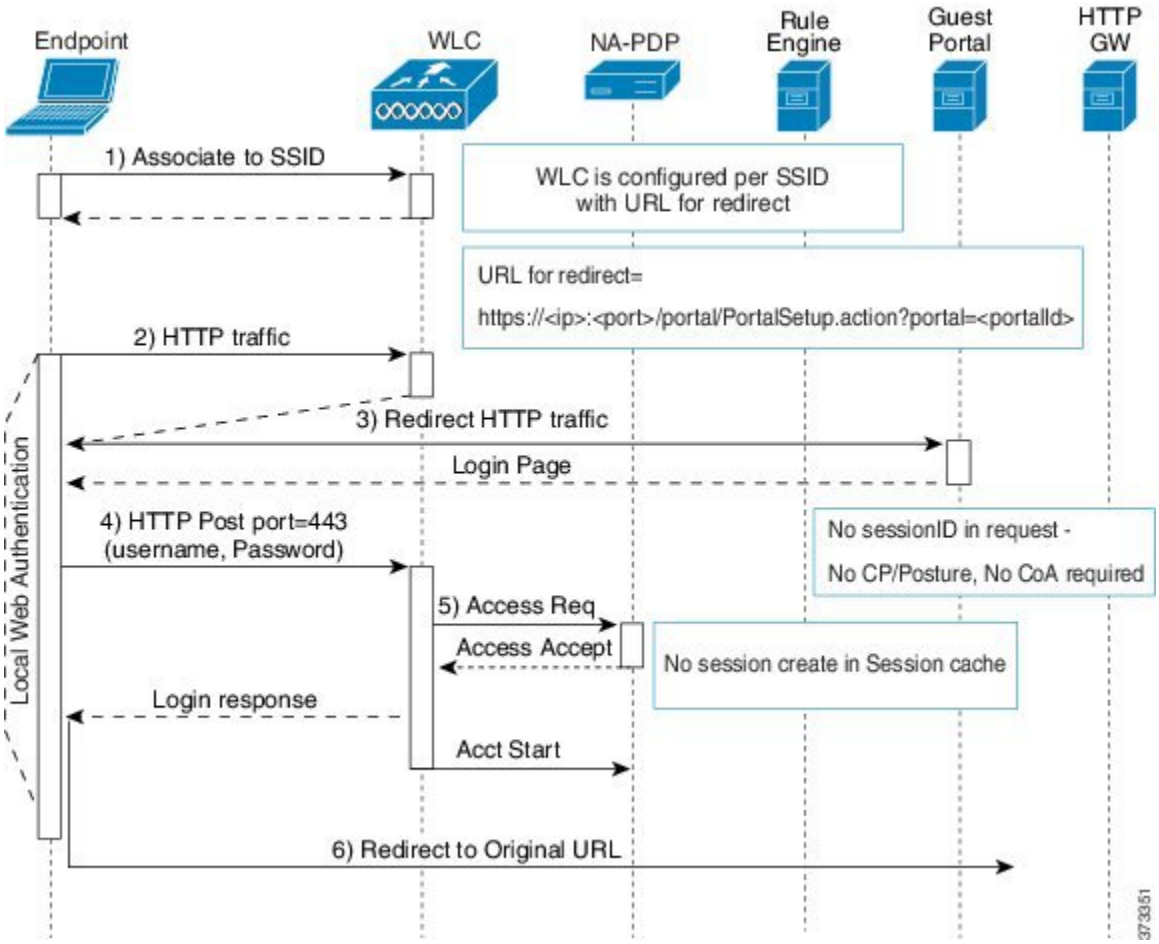
ローカル WebAuth プロセス対応のワイヤレス LAN コントローラ

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 *1*：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=ISO-8859-1">

<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、ユーザによるユーザ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、パスワード非表示、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。

はじめる前に

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。

a.	**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。
b.	**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。
c.	**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。
d.	**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 2：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と、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再許可できます。

VLAN DHCP リリースのサポートは、デスクトップ デバイスの Mac OS と Windows でのみ使用可能です。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 *2*：ワイヤレス デバイス登録 *Web* 認証フロー