CHAPTER 16

ゲストに許可されるネットワーク アクセスのサポート

この章では、ネットワーク ユーザ アクセスの管理、スポンサー アカウント、およびこれらのネットワーク ユーザに必要なポリシーの作成方法について説明します。

この章は、次の内容で構成されています。

Cisco ISE ゲスト サービス

Cisco Identity Services Engine（ISE）のゲスト サービスを使用すると、ゲスト、訪問者、契約者、コンサルタント、および顧客にセキュアなネットワーク アクセスを提供できます。基本および拡張の両方の Cisco ISE ライセンスを持つゲスト ユーザをサポートでき、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導入オプションから選択できます。

関連項目

- 「ゲスト展開シナリオ」（P.16-28）
- 第 7 章「Cisco ISE ライセンス」

ゲスト サービス エンドユーザ ポータル

Cisco ISE には、ネットワークへのゲスト アクセスを管理するための Web ベースのポータルが用意されています。

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。スポンサーは、スポンサー ポータルを使用して、許可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安全にアクセスするための一時アカウントを作成および管理できます。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。

関連項目

- 第 15 章「エンドユーザ Web ポータルの設定およびカスタマイズ」
- 「スポンサー ポータルの設定」（P.16-8）

ゲスト ポータル

会社の外部の人々がインターネットにアクセスするため企業のネットワークを使用しようとすると、ゲスト ポータルにルーティングされます。外部ユーザの内部ネットワークとサービスへの一時的なアクセスを識別し、許可するためにゲスト ポータルを使用できます。スポンサーは、許可した訪問者の一時的なユーザ名およびパスワードを作成できます。次に、訪問者はゲスト ポータルのログイン ページでこれらのクレデンシャルを入力することでネットワークにアクセスできます。

Cisco ISE では、異なる基準に基づいてゲストのアクセスを許可するために使用できる複数のゲスト ポータルを作成することができます。たとえば、毎日の訪問者に使用するポータルとは別の毎月の契約者用のゲスト ポータルを作成できます。モバイルで最適化されたゲスト ポータルのバージョンにモバイル ユーザをルーティングするオプションもあります。

関連項目

- 「ゲスト展開シナリオ」（P.16-28）
- 「ゲスト ポータルの設定」（P.16-11）

複数のゲスト ポータルのサポート

Cisco ISE には、Cisco ISE サーバで、事前定義された DefaultGuestPortal を含む複数のポータルをホストするための機能が備わっています。デフォルトのポータル テーマには、管理者ポータルからカスタマイズできる標準のシスコ ブランドが適用されています。また、組織に固有の HTML ページをアップロードすることによって、ポータルをカスタマイズすることもできます。

関連項目

- 「ゲスト ポータルの設定」（P.16-11）

モバイル ゲスト ポータル

Cisco ISE では、モバイルで最適化されたバージョンのゲスト ポータルを提供でき、これらのモバイル デバイスを使用してネットワークにアクセスするゲストに向上したユーザ エクスペリエンスが提供されます。これはオプションの機能なので、ゲスト ポータルの作成時に有効にする必要があります。

関連項目

「モバイルで最適化されたゲスト ポータルの提供」（P.16-11）

デバイス登録 Web 認証ポータル

デバイス登録 Web 認証（DRW）ポータルは、ゲストにユーザ名とパスワードの入力を要求しない代替ゲスト ポータルです。代わりに、Cisco ISE は、ワイヤレス LAN コントローラ（WLC）と連携して、ゲストのデバイスにネットワーク アクセスを直接付与します。

DRW ポータルをサポートする場合、Cisco ISE では、ゲストのデバイスを一元的に追跡できるようにするデフォルトのゲスト ID グループ GuestEndpoints が用意されています。

関連項目

- 「デバイス登録 WebAuth」（P.16-32）

クライアント プロビジョニング ポータル

クライアント プロビジョニング ポータルは、ゲスト ユーザにポスチャ評価および修復を提供します。ゲストがネットワーク アクセスを要求すると、クライアント プロビジョニング ポータルにゲストをルーティングし、最初にクライアント プロビジョニング エージェントをダウンロードするようにゲストに要求できます。

クライアント プロビジョニング ポータルは、中央 WebAuth（CWA）のゲスト展開のみで使用できます。このオプションを選択すると、ゲスト ログイン フローで CWA が実行され、利用規定とパスワード変更チェックの実行後に、ゲスト ポータルがクライアント プロビジョニングにリダイレクトされます。ポスチャ サブシステムでネットワーク アクセス デバイスに対して許可変更（CoA）が実行され、ポスチャの評価後にクライアント接続が再認証されます。

関連項目

- 「中央 WebAuth 対応の NAD のプロセス フロー」（P.16-28）
- 「クライアント プロビジョニングの設定」（P.22-1）

スポンサーおよびゲスト アカウントの管理

ゲスト サービスには、特別な 2 つのタイプのユーザ、ゲストとスポンサーが必要です。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のサポートを定義する必要があります。次に、スポンサーはスポンサー ポータルにアクセスして、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

ゲストは通常、許可されたビジター、契約者、顧客、またはネットワークへのアクセスが必要なその他の一時ユーザを表します。ただし、従業員がネットワークにアクセスできるようになるゲスト展開シナリオの 1 つを使用する場合は、従業員に対してもゲスト アカウントを使用できます。スポンサーだけがゲスト ユーザを作成でき、ゲスト ユーザのリストを表示するにはスポンサー ポータルにアクセスする必要があります。

ゲスト ロールおよび ID グループ

ゲスト ID グループは、ゲスト ロールによって定義されます。スポンサーがゲスト アカウントを作成すると、ゲスト ロールにアカウントを関連付ける必要があります。ゲスト ロールにより、スポンサーにゲスト アカウントへの異なるアクセス レベルの割り当てを許可します。これらのゲスト ロールは、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。たとえば、Cisco ISE には、次のデフォルトのゲスト ロールがあります。

- ゲスト：ユーザは、ネットワークの他の部分にアクセスする前に、最初にゲスト キャプティブ ポータルからログインする必要があります（中央集中 Web 認証（CWA）など）。
- ActivatedGuest：ユーザはゲスト ポータルをバイパスし、デバイス上のネイティブ サプリカントにクレデンシャルを提供することでネットワークにアクセスできます（IEEE 802.1X（dot1x）認証など）。

スポンサー アカウントで使用するために、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）]）。

関連項目

「ユーザ ID グループの作成」（P.14-5）

ゲスト ロールの設定

ゲスト ロールとして使用する新しい ID グループを作成する場合、それらに適用するデフォルトの動作を次から示す必要があります。ゲストまたはアクティブなゲスト。

はじめる前に

ゲストに使用する新しいユーザの ID グループを作成します。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [ゲスト ロールの設定（Guest Roles Configurationy）] を選択します。

ステップ 2　自分が作成した ID グループを選択します。

ステップ 3　[>] または [<] をクリックして ID グループを次のいずれかのグループに割り当てます。

- **ゲスト**：ユーザは、ネットワークの他の部分にアクセスする前に、最初にゲスト キャプティブ ポータルからログインする必要があります（中央集中 Web 認証（CWA）など）。
- **ActivatedGuest**：ユーザはゲスト ポータルをバイパスし、デバイス上のネイティブ サプリカントにクレデンシャルを提供することでネットワークにアクセスできます（IEEE 802.1X（dot1x）認証など）。

ステップ 4　[保存（Save）] をクリックします。

次の作業

このゲスト ロールを使用するには、スポンサー グループを作成または変更します。

関連項目

- 「ユーザ ID グループの作成」（P.14-5）
- 「スポンサー グループの作成」（P.16-6）

スポンサー アカウントおよび ID グループ

スポンサーは、スポンサー ポータルを使用してゲスト アカウントを作成できる内部ユーザの特殊なタイプです。他の内部ユーザと同様、Cisco ISE では、ローカル データベースあるいは外部の Lightweight Directory Access Protocol（LDAP）または Microsoft Active Directory ID ストアによりスポンサーを認証します。外部ソースを使用しない場合、Cisco ISE でユーザ アカウントを作成する必要があります（[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）]）。

次に、適切なスポンサー ID グループにユーザを割り当てる必要があります。スポンサー ID グループは、スポンサー ポータルを使用できるユーザを指定し、それらはスポンサー グループ ポリシーのデフォルトのスポンサー グループにデフォルトでマッピングされます。

Cisco ISE には、次のデフォルトのスポンサー ユーザ ID グループがあります。

- SponsorAllAccount
- SponsorGroupAccounts
- SponsorOwnAccounts

スポンサー アカウントで使用するために、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）]）。

関連項目

「ユーザの追加」（P.14-3）

「ユーザ ID グループの作成」（P.14-5）

スポンサー グループ

スポンサー グループ設定は、スポンサー ユーザの権限および設定を定義します。ポリシーは、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。

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。

- SponsorAllAccounts : Cisco ISE ネットワーク内のすべてのゲスト アカウントを管理できるスポンサー。
- SponsorGroupGrpAccounts : 同じスポンサー グループのスポンサー ユーザが作成したゲスト アカウントだけを管理できるスポンサー。
- SponsorGroupOwnAccounts : 自分が作成したゲスト アカウントだけを管理できるスポンサー。

スポンサー ポリシーを作成する際正しい ID グループとスポンサー グループの関連付けに役立つように、これらのスポンサー グループはデフォルト ユーザ ID グループと類似した名前を持っています。

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。

- スポンサーが作成したゲスト アカウントを他のスポンサーが表示することを制限できます。
- アカウントの作成、アカウントの変更、電子メールまたは SMS テキスト メッセージによるゲストへのアカウント詳細の送信など、さまざまな機能へのアクセスを制限できます。
- 設定が変更されている短期間にスポンサー グループがログインできないように、スポンサー グループの権限を設定できます。

関連項目

- 「スポンサー グループの作成」（P.16-6）
- 「スポンサー グループ ポリシーの作成」（P.16-7）
- 「スポンサー グループ設定」（P.A-52）

スポンサー グループの作成

Cisco ISE によって提供されているデフォルトのスポンサー グループに加えて、追加のスポンサー グループを作成できます。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [スポンサー グループ（Sponsor 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　次の各タブのフィールドを更新します。

- [一般（General）] : 新しいスポンサー グループの名前および説明を指定します。
- [許可レベル（Authorization Levels）] : アカウントの作成、通知の送信、およびアカウントの一時停止など、このグループのスポンサーで使用可能な機能を識別します。
- [ゲスト ロール（Guest Roles）] : スポンサーがゲスト ユーザを割り当てることができるゲスト ロールを選択します。
- [時間プロファイル（Time Profiles）] : スポンサーがゲスト アカウントで設定できる時間プロファイルを選択します。

ステップ 4　[送信（Submit）] をクリックします。

関連項目

- 「スポンサー グループ」（P.16-5）
- 「スポンサー グループ設定」（P.A-52）

スポンサー グループ ポリシー

スポンサー グループ ポリシーで、ユーザ ID グループをスポンサー グループに関連付けます。各スポンサー グループ ポリシーは、少なくとも 1 つの ID グループを含み、スポンサー グループを定義する他の属性条件も含むことができます。内部ユーザまたは外部 ID ストア（LDAP または Active Directory など）のユーザをスポンサー グループにマッピングできます。

内部ユーザをスポンサー グループにマップするには、スポンサー グループ ポリシーで使用される ID グループ ロールを割り当てます。ID グループ ロールとスポンサー グループ ポリシーの条件がどちらも内部ユーザに適合する場合は、そのスポンサー グループ ポリシーに関連付けられているスポンサー グループにユーザがマップされます。

外部ユーザをスポンサー ユーザとして識別するには、外部 ID ストアの属性がスポンサー グループ ポリシー内の条件に適合し、ローカル スポンサー グループに外部ユーザをマップできる必要があります。外部ユーザが持つ属性条件がスポンサー グループ ポリシーに定義されている場合、ユーザは、スポンサー グループ ポリシーで選択されたゲスト スポンサー グループに割り当てられます。

スポンサー グループ ポリシーの作成

スポンサー グループ ポリシーで、スポンサーがスポンサー ポータルにログインすると利用可能なアクセスと機能を決定する条件を指定します。

スポンサー グループ ポリシーは次から構成されます。

- 1 つ以上の ID グループ
- 1 つ以上の属性または条件

はじめる前に

スポンサー グループ ポリシーに既存の条件を適用できます。ポリシーを作成する前に、必要に応じて、追加の条件を定義します。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [スポンサー グループ ポリシー（Sponsor Group Policy）] を選択します。

ステップ 2　[操作（Action）] アイコンをクリックし、オプションを選択します。

ステップ 3　新しいポリシーの名前を入力します。

ステップ 4　ポリシーに関連付ける ID グループを選択します。

ステップ 5　（任意）次のいずれかのオプションを選択して追加条件を選択してください。

- [既存の条件をライブラリから選択（Select Existing Condition from Library）] を選択して、既存の単純、複合、または時刻と日付の条件を選択します
- [新しい条件の作成（Create New Condition）] を選択した、式ビルダーから属性、演算子、および値を選択します。

ステップ 6　対象のスポンサー グループ ポリシーに関連付けるスポンサー グループを選択します。

ステップ 7　[保存（Save）] をクリックします。

関連項目

- 「単純条件の作成」（P.18-2）
- 「複合条件の作成」（P.18-3）
- 「ユーザの追加」（P.14-3）
- 「スポンサー グループの作成」（P.16-6）

スポンサー グループへの Active Directory グループのマップ

外部 ID グループをスポンサー グループにマッピングできます。

はじめる前に

このタスクを開始する前に、Active Directory ID グループを設定する必要があります。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [スポンサー グループ ポリシー（Sponsor Group Policy）] を選択します。

ステップ 2　[操作（Action）] アイコンをクリックし、オプションを選択します。

ステップ 3　新しいポリシーの名前を入力します。

ステップ 4　内部グループとのグループ マッピングは存在しないため、ID グループとして [任意（Any）] を選択します。

ステップ 5　Active Directory ID ストアに対して作成した条件を選択します

ステップ 6　この AD 条件に関連づけるスポンサー グループを選択します。

ステップ 7　[保存（Save）] をクリックします。

関連項目

- 「外部 ID ソースとしての Active Directory」（P.14-9）
- 「Active Directory ユーザ グループの設定」（P.14-14）

スポンサー ポータルの設定

スポンサーがスポンサー ポータルにアクセスしてゲスト ユーザのアカウントを作成できるようになる前に、スポンサー ポータルでいくつかの設定を行う必要があります。

スポンサー ID ソース順序

スポンサー ID ソース順序は、スポンサーのログイン クレデンシャルとともに、スポンサー ポータルにアクセスするスポンサーを認証および許可するために使用されます。ID ストア順序では、スポンサー ユーザの認証を解決するために、どのストアにどのような順序でアクセスするかを定義し、ローカル Cisco ISE ID ストアと外部ストアを含めることができます。

Cisco ISE には、デフォルトの ID ストアである内部ユーザを含む、デフォルトのスポンサー ID ソース順序（Sponsor_Portal_Sequence）があります。

関連項目

- 「スポンサーの ID ソース順序の指定」（P.16-8）
- 「ID ソース順序の作成」（P.14-40）

スポンサーの ID ソース順序の指定

スポンサー ユーザがスポンサー ポータルにログインできるようにするには、すべてのスポンサー アカウントに使用する ID ソース順序を選択する必要があります。この順序は、スポンサーのログイン クレデンシャルとともに、スポンサー ポータルにアクセスするスポンサーを認証および許可するために使用されます。

はじめる前に

ID ソース順序を作成します。または、Cisco ISE に付属しているデフォルトの順序である Sponsor_Portal_Sequence を使用できます。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [スポンサー（Sponsor）] > [認証ソース（Authentication Source）] を選択します。

ステップ 2　[ID ストア順序（Identity Store Sequence）] ドロップダウン リストから ID ソース順序を選択します。

ステップ 3　[保存（Save）] をクリックします。

関連項目

- 「スポンサー ID ソース順序」（P.16-8）
- 「ID ソース順序」（P.14-39）
- 「ID ソース順序の作成」（P.14-40）

ゲスト通知のカスタマイズ

スポンサーがゲスト アカウントを作成すると、詳細を印刷、電子メール送信、または携帯電話で送信して、アカウントのクレデンシャルをゲスト ユーザに提供します。スポンサー グループの作成時に、スポンサーにこれらの通知の使用を許可するかどうかを決定します。

電子メール通知のカスタマイズ

アカウント詳細とともにゲストに送信される電子メールの件名と本文を指定することができます。

はじめる前に

通知が有効になるように SMTP サーバを設定し、電子メール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。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [スポンサー（Sponsor）] > [言語テンプレート（Language Template）] を選択します。

ステップ 2　ポリシーに適用する言語（たとえば、英語）をクリックします。

ステップ 3　[電子メール通知の設定（Configure Email Notification）] をクリックします。

ステップ 4　[件名（Subject）] フィールドに、電子メールの件名を入力します。

ステップ 5　書式を設定するための HTML タグを使用して、[レイアウト（Layout）] フィールドに電子メールの本文を入力します。

ステップ 6　[保存（Save）] をクリックします。

関連項目

- 「通知をサポートするように SMTP サーバを設定」（P.5-5）
- 「スポンサー グループの作成」（P.16-6）
- 「電子メール通知テンプレート」（P.D-1）

SMS テキスト メッセージ通知のカスタマイズ

Short Message Service（SMS）ゲートウェイ、およびアカウント詳細とともにゲストに送信される SMS テキスト メッセージの件名と本文を指定することができます。

はじめる前に

- 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目的で使用される SMTP サーバを設定します。
- 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 ゲートウェイのアカウントが必要です。Cisco ISE はテキスト メッセージを電子メール メッセージとしてゲートウェイに送信し、その後そのメッセージは SMS を経由して指定されたユーザに転送されます。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [スポンサー（Sponsor）] > [言語テンプレート（Language Template）] を選択します。

ステップ 2　ポリシーを適用する言語をクリックします。

ステップ 3　[SMS テキスト通知の設定（Configure SMS Text Notification）] をクリックします。

ステップ 4　[件名（Subject）] フィールドに、テキスト メッセージの件名を入力します。

ステップ 5　[宛先（Destination）] フィールドに、サードパーティ SMS ゲートウェイのアドレスを入力します。

ステップ 6　書式を設定するための HTML タグを使用して、[レイアウト（Layout）] フィールドにテキスト本文を入力します。

ステップ 7　[保存（Save）] をクリックします。

関連項目

- 「通知をサポートするように SMTP サーバを設定」（P.5-5）
- 「スポンサー グループの作成」（P.16-6）
- 「SMS テキスト メッセージ通知テンプレート」（P.D-2）

印刷通知のカスタマイズ

アカウント詳細とともにゲストに対して印刷されるページ ヘッダーとページの本文を指定することができます。

はじめる前に

印刷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。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [スポンサー（Sponsor）] > [言語テンプレート（Language Template）] を選択します。

ステップ 2　ポリシーに適用する言語（たとえば、英語）をクリックします。

ステップ 3　[印刷通知の設定（Configure Print Notification）] をクリックします。

ステップ 4　[ページ ヘッダー（Page Header）] フィールドにタイトルを入力します。

ステップ 5　書式を設定するための HTML タグを使用して、[レイアウト（Layout）] フィールドに印刷の本文を入力します。

ステップ 6　[保存（Save）] をクリックします。

関連項目

- 「スポンサー グループの作成」（P.16-6）
- 「印刷通知テンプレート」（P.D-3）

ゲスト ポータルの設定

ゲストがゲスト ポータルを使用してネットワークにアクセスできるようにする前にゲスト ポータルの設定を行う必要があります。すべてのゲスト ポータルにグローバルに適用される設定もあれば、ポータルごとに個別に設定する必要がある設定もあります。

新しいゲスト ポータルの追加

新しいゲスト ポータルを追加するか、または既存のゲスト ポータルを編集できます。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [マルチポータルの設定（Multi-Portal Configurations）] 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　次の各タブのフィールドを更新します。

- [一般（General）] : ポータルの名前と説明を入力し、ポータル タイプを選択します。
- [操作（Operations）] : 特定のポータルのカスタマイズを有効にします
- [カスタマイズ（Customization）] : ローカライズされたコンテンツを含むゲスト ポータルを表示する言語テンプレートを選択します
- [ファイル アップロード（File Upload）] : カスタム HTML ファイルをアップロードするように要求するポータル タイプを選択した場合にのみ表示されます。
- [ファイル マッピング（File Mapping）] : 特定のゲスト ページ用にアップロードした HTML ファイルを識別し、選択します。カスタム HTML ファイルをアップロードするように要求するポータル タイプを選択した場合にのみ表示されます。
- [認証（Authentication）] : ゲスト ログイン中にユーザを認証する方法を示します。

ステップ 4　[送信（Submit）] をクリックします。

関連項目

- 「マルチポータルの設定」（P.A-62）
- 「C シスコ ISE 認証ポリシー」（P.19-1）
- 「簡易認証ポリシーの設定」（P.19-23）
- 「ルール ベースの認証ポリシーの設定」（P.19-23）

モバイルで最適化されたゲスト ポータルの提供

モバイル ユーザがモバイルで最適化されたゲスト ポータルのバージョンにアクセスできるようにできます。

はじめる前に

ポータル ゲストを作成するか、または DefaultGuestPortal を変更します。この設定は、各ゲスト ポータルに固有です。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [マルチポータルの設定（Multi-Portal Configuration）] を選択します。

ステップ 2　ゲスト ポータルをオンにして更新し、[編集（Edit）] をクリックします。

ステップ 3　[操作（Operations）] タブをクリックします。

ステップ 4　[モバイル ポータルの有効化（Enable Mobile Portal）] をオンにします。

ステップ 5　[保存（Save）] をクリックします。

関連項目

- 「新しいゲスト ポータルの追加」（P.16-11）
- 「マルチポータルの設定」（P.A-62）
- 「Web ポータルのイメージおよびカラー スキームのカスタマイズ」（P.15-6）

カスタマイズされたゲスト ポータル

ゲスト ポータルのカスタマイズに使用できる 2 つのオプションがあります。

- [管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [一般（General）] > [ポータル テーマ（Portal Theme）] を選択して、すべてのゲスト、スポンサー、およびデバイス ポータルに同じカスタム カラー スキーム、バナー、およびロゴを適用します。（詳細については、「Web ポータルのイメージおよびカラー スキームのカスタマイズ」（P.15-6）を参照してください）。
- ゲスト ポータルのルックアンドフィールを完全に制御できるカスタム HTML ページを作成します。

  カスタム html ファイルを作成した場合、それらの変更はゲスト ポータルにのみ適用されます。その他のポータルでは、ポータル テーマで定義された設定が使用されます。ポータル間でルックアンドフィールをさらに同期するには、ポータル テーマにもカスタム ロゴとバナーをアップロードしてください。

関連項目

- 「ゲスト ポータル用のカスタム ページのサンプル HTML」（P.D-3）
- 「ゲスト ポータルのカスタム HTML ファイルの作成」（P.16-14）
- 「ゲスト ポータルの HTML ファイルのアップロード」（P.16-15）
- 「ゲスト ポータル ページへの HTML ファイルのマッピング」（P.16-15）

カスタム ゲスト ポータルに必要な HTML ページ

完全にカスタマイズされたゲスト ポータルをサポートするには、サポートする機能に基づいて HTML ページの最小セットを提供する必要があります。

- [ログイン（Login）] ページ：必須

- [正常ゲスト ログイン（Successful Guest Login）] ページ：必須
- [エラー（Error）] ページ：必須
- [アクセプタブル ユース ポリシー（Acceptable Use Policy）] ページ：ゲストにアクセプタブル ユース ポリシーを確認するように要求する場合のみ必須。
- [パスワードの変更（Change Password）] ページ：ゲストが初めてサイン インするときにパスワードを変更するように要求する場合のみ必須。
- [アカウント登録（Self-Registration）] ページ：ゲストが自分のアカウントを作成する（セルフ サービス）のを許可する場合のみ必須。
- [アカウント登録結果（Self-Registration Result）] ページ：ゲストが自分のアカウントを作成する（セルフ サービス）のを許可する場合のみ必須。
- [デバイスの登録（Device Registration）] ページ：ゲスト ユーザのデバイスの登録をサポートしている場合のみ必須。

関連項目

- 「ゲストへのパスワードの変更要求」（P.16-17）
- 「ゲストのアクセプタブル ユース ポリシーの必要性」（P.16-20）
- 「ゲストがデバイスを追加することの許可」（P.16-23）
- 「ゲストがアカウントを作成することの許可」（P.16-23）

ゲスト ポータルで使用されるカスタマイズした HTML ページの順序

カスタマイズした HTML ページの順序および表示は、Cisco ISE 管理で有効になっている機能によって異なります。次に順序の例をいくつか示します。

- 基本順序
  - [ログイン（Login）] ページ（必須）> [正常ゲスト ログイン（Successful Guest Login）] ページ（必須）
  - [ログイン（Login）] ページ（必須）> [パスワードの変更（Change Password）] ページ > [正常ゲスト ログイン（Successful Guest Login）] ページ（必須）
- デバイス登録順序
  - [ログイン（Login）] ページ（必須）> [デバイスの登録（Device Registration）] ページ > [正常ゲスト ログイン（Successful Guest Login）] ページ（必須）
  - [ログイン（Login）] ページ（必須）> [パスワードの変更（Change Password）] ページ > [デバイスの登録（Device Registration）] ページ > [正常ゲスト ログイン（Successful Guest Login）] ページ（必須）
- アクセプタブル ユース ポリシー順序
  - [ログイン（Login）] ページ（必須）> [アクセプタブル ユース ポリシー（Acceptable Use Policy）] ページ > [正常ゲスト ログイン（Successful Guest Login）] ページ（必須）
  - [ログイン（Login）] ページ（必須）> [アクセプタブル ユース ポリシー（Acceptable Use Policy）] ページ > [パスワードの変更（Change Password）] ページ > [正常ゲスト ログイン（Successful Guest Login）] ページ（必須）
  - [ログイン（Login）] ページ（必須）> [アクセプタブル ユース ポリシー（Acceptable Use Policy）] ページ > [パスワードの変更（Change Password）] ページ > [デバイスの登録（Device Registration）] ページ > [正常ゲスト ログイン（Successful Guest Login）] ページ（必須）

- アカウント登録順序
  - [ログイン（Login）] ページ（必須）> [アカウント登録（Self-Registration）] ページ > [アカウント登録結果（Self-Registration Result）] ページ > [正常ゲスト ログイン（Successful Guest Login）] ページ（必須）

関連項目

- 「ゲストへのパスワードの変更要求」（P.16-17）
- 「ゲストのアクセプタブル ユース ポリシーの必要性」（P.16-20）
- 「ゲストがデバイスを追加することの許可」（P.16-23）
- 「ゲストがアカウントを作成することの許可」（P.16-23）

ゲスト ポータルのカスタム HTML ファイルの作成

カスタム HTML ページをゲスト ポータルに使用するには、手動でコード化する必要があります。独自の HTML ページを使用した場合、詳細ポリシー、言語テンプレート、およびポータル テーマは適用されません。したがって、これらの機能が重要になる場合は、独自に HTML コードを記述して類似の機能を提供するか、代わりに標準ポータル テーマ ページを使用する必要があります。

はじめる前に

シスコ提供の HTML ページに精通してください（「ゲスト ポータル用のカスタム ページのサンプル HTML」（P.D-3）を参照）。最低でも、ログイン、正常ゲスト、およびエラーのページ ファイルを作成する必要があります。

ステップ 1　HTML またはテキスト編集アプリケーションを開きます。

ステップ 2　シスコ提供のサンプル HTML ページを参照として使用して、カスタム HTML コードを入力します。

ステップ 3　ページごとに別個の HTML ファイルを作成して保存します。

- [ログイン（Login）] ページ（必須）
- [正常ゲスト ログイン（Successful Guest Login）] ページ（必須）
- [エラー（Error）] ページ（必須）
- [アクセプタブル ユース ポリシー（Acceptable Use Policy）] ページ
- [パスワードの変更（Change Password）] ページ
- [アカウント登録（Self-Registration）] ページ
- [アカウント登録結果（Self-Registration Result）] ページ
- [デバイスの登録（Device Registration）] ページ

次の作業

HTML ページを作成したら、Cisco ISE にアップロードし、適切なゲスト ポータル ページにマッピングします。

関連項目

- 「ゲスト ポータル用のカスタム ページのサンプル HTML」（P.D-3）
- 「ゲスト ポータルの HTML ファイルのアップロード」（P.16-15）
- 「ゲスト ポータル ページへの HTML ファイルのマッピング」（P.16-15）

ゲスト ポータルの HTML ファイルのアップロード

ゲスト ポータルを完全にカスタマイズするには、HTML ファイルをアップロードします。

はじめる前に

カスタム HTML ファイルを作成する必要があります。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [マルチポータルの設定（Multi-Portal Configurations）] を選択します。

ステップ 2　これらのポータル タイプのいずれかを選択します。

- **カスタム デフォルト ポータル**
- **カスタム デバイス Web 認証ポータル**

ステップ 3　[ファイル アップロード（File Upload）] タブをクリックします。

ステップ 4　[ファイルの更新（Update File）] をクリックして、各 HTML ファイルを選択してアップロードします。

ステップ 5　[送信（Submit）] をクリックします。

関連項目

- 「ゲスト ポータル用のカスタム ページのサンプル HTML」（P.D-3）
- 「ゲスト ポータルのカスタム HTML ファイルの作成」（P.16-14）
- 「ゲスト ポータル ページへの HTML ファイルのマッピング」（P.16-15）

ゲスト ポータル ページへの HTML ファイルのマッピング

カスタム HTML ファイルをアップロードしたら、ゲスト ポータルの該当するページにマッピングする必要があります。

はじめる前に

カスタム HTML ファイルを作成およびアップロードする必要があります。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [マルチポータルの設定（Multi-Portal Configurations）] を選択します。

ステップ 2　これらのポータル タイプのいずれかを選択します。

- **カスタム デフォルト ポータル**
- **カスタム デバイス Web 認証ポータル**

ステップ 3　[ファイル マッピング（File Mapping）] タブをクリックします。

ステップ 4　ドロップダウン メニューをクリックして、アップロードした HTML ページを該当するファイルに割り当てます。

ステップ 5　[送信（Submit）] をクリックします。

- 「ゲスト ポータル用のカスタム ページのサンプル HTML」（P.D-3）

- 「ゲスト ポータルのカスタム HTML ファイルの作成」（P.16-14）
- 「ゲスト ポータルの HTML ファイルのアップロード」（P.16-15）

ゲスト ユーザ名およびパスワード ポリシーの設定

ゲスト アカウントのユーザ名とパスワード ポリシーを設定する必要があります。

名前または電子メール アカウントに基づくゲスト ユーザ名ポリシーの設定

ゲスト ユーザ名は、電子メール アドレスまたはゲストの姓名に基づいて作成することができます。これは、すべてのゲスト ポータルに適用されるグローバル設定ですが、変更は既存のアカウントには影響しません。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [ユーザ名ポリシー（Username Policy）] 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。

- **電子メール アドレスからユーザ名を作成します**
- **名と姓からユーザ名を作成します**

ステップ 3　ゲスト ユーザ名の最小長を入力します。有効な指定範囲は 1 ～ 20 です。

ステップ 4　[保存（Save）] をクリックします。

関連項目

- 「ゲスト ユーザ名ポリシーの設定」（P.A-68）

ランダム ゲスト アカウントのユーザ名ポリシーの設定

ゲスト ユーザ名は、アルファベット、数字、特殊文字をランダムに組み合わせて作成することができます。ランダム ゲスト ユーザ名ポリシーは、スポンサーがランダム アカウントを作成するときに使用されます。これは、すべてのゲスト ポータルに適用されるグローバル設定ですが、変更は既存のアカウントには影響しません。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [ユーザ名ポリシー（Username Policy）] を選択します。

ステップ 2　ランダム ユーザ名を生成するために使用される文字を入力します。

ステップ 3　各文字のセットから使用する最小数を入力します。

ステップ 4　[保存（Save）] をクリックします。

関連項目

- 「ゲスト ユーザ名ポリシーの設定」（P.A-68）

ゲスト パスワード ポリシーの設定

ゲスト パスワード ポリシーでは、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 ポリシーは、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。

これは、すべてのゲスト ポータルに適用されるグローバル設定です。ただし、ゲスト パスワード ポリシーに対する変更は、ゲスト ユーザ 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。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [パスワード ポリシー（Password Policy）] を選択します。

ステップ 2　使用できるアルファベット、数字、特殊文字を入力します。

ステップ 3　各文字のセットから使用する最小数を入力します。

ステップ 4　[保存（Save）] をクリックします。

ゲスト パスワードの有効期限の設定

ゲスト パスワードの有効期限が切れ、パスワードをリセットするようにゲストに要求するまでの日数を設定できます。これは、すべてのゲスト ポータルに適用されるグローバル設定です。

はじめる前に

このオプションを使用するには、失効時にゲストにパスワードを変更するように要求するオプションも設定する必要があります。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [ポータル ポリシー（Portal Policy）] を選択します。

ステップ 2　[ゲスト パスワードの有効期限（Guest Password Expiration）] フィールドに日数を入力します。

ステップ 3　[保存（Save）] をクリックします。

関連項目

- 「ゲストへのパスワードの変更要求」（P.16-17）
- 「ゲスト ポータル ポリシーの設定」（P.A-66）

ゲストへのパスワードの変更要求

ゲスト ユーザの初期アカウント クレデンシャルがスポンサーによって作成された後に、ゲスト ユーザにパスワードの変更を許可するか、または要求できます。ゲスト ユーザがパスワードを変更した場合に、ログイン クレデンシャルが失われていたらスポンサーはそれらをゲストに提供できません。スポンサーは、新しいゲスト アカウントを作成する必要があります。

ゲストがパスワードを変更できるようにするか、または失効時および最初のログイン時にパスワードを変更することを要求できます。

はじめる前に

ポータル ゲストを作成するか、または DefaultGuestPortal を変更します。この設定は、各ゲスト ポータルに固有です。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [マルチポータルの設定（Multi-Portal Configuration）] を選択します。

ステップ 2　ゲスト ポータルをオンにして更新し、[編集（Edit）] をクリックします。

ステップ 3　[操作（Operations）] タブをクリックします。

ステップ 4　次のいずれかまたは両方のオプションをオンにします。

- **ゲスト ユーザがパスワードを変更できるようにします（Allow guest users to change password）**
- **失効時および初回ログイン時にゲスト ユーザにパスワードの変更を要求します（Require guest users to change password at expiration and first login）**

ステップ 5　[保存（Save）] をクリックします。

関連項目

- 「新しいゲスト ポータルの追加」（P.16-11）
- 「マルチポータルの設定」（P.A-62）

ログインの最大失敗試行回数の指定

ゲスト アカウントが中断され、スポンサーにアカウントを再開するように要求する前に、試行される失敗ログインの最大数を設定できます。これは、すべてのゲスト ポータルに適用されるグローバル設定です。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [ポータル ポリシー（Portal Policy）] を選択します。

ステップ 2　[最大ログイン失敗（Maximum Login Failures）] フィールドに値を入力します。

ステップ 3　[保存（Save）] をクリックします。

関連項目

「ゲスト ポータル ポリシーの設定」（P.A-66）

ゲスト機能の定義

ゲスト ポータルに必要な情報と使用可能なパラメータを指定できます。

ゲスト アカウントに必要なデータの指定

詳細ポリシーでは、ゲスト アカウントを作成するために必要なデータを指定します。スポンサーが新しいゲスト アカウントを作成したとき、またはゲストが自らを登録したときに表示されるフィールド（名前、会社、電子メール、および電話など）を定義する必要があります。これは、すべてのゲスト ポータルに適用されるグローバル設定です。

はじめる前に

独自の HTML ページをアップロードしてカスタム ポータルを作成した場合、カスタム HTML コードには詳細ポリシーは適用されません。したがって、この機能が重要になる場合は、独自に HTML コードを記述して類似の機能を提供するか、代わりに標準ポータル ページを使用する必要があります。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [詳細ポリシー（Details Policy）] を選択します。

ステップ 2　各フィールドが必須、オプション、または未使用であるかどうかを指定します。

ステップ 3　[保存（Save）] をクリックします。

次の作業

これらのフィールド名を完全にカスタマイズできます。たとえば、任意指定のデータ フィールドの名前を会社で一般的に使用されるフィールドに変更する場合、ゲスト ポータル上に表示するテキストを変更できます。詳細については、「ポータルの UI フィールドおよびエラー メッセージのカスタマイズ」（P.15-5）を参照してください。

ゲスト 1 人あたりのサポートされるデバイスの数の制限

各ゲストに登録できるデバイスの数を制限できます。

これは、すべてのゲスト ポータルに適用されるグローバル設定です。現在ゲスト アカウントに登録されているデバイスの最大数未満にこの値を設定できますが、この変更は既存の登録済みデバイスには影響しません。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [ポータル ポリシー（Portal Policy）] を選択します。

ステップ 2　[デバイス登録ポータル制限（Device Registration Portal Limit）] フィールドに値を入力します。

ステップ 3　[保存（Save）] をクリックします。

関連項目

「ゲスト ポータル ポリシーの設定」（P.A-66）

1 つアクティブなネットワーク セッションへのゲストの制限

ゲストがネットワークに接続できるデバイスは一度に 1 つだけと制限できます。ゲストが 2 番めのデバイスで接続しようとすると、現在接続されているデバイスはネットワークから自動的に接続解除されます。

これは、すべてのゲスト ポータルに適用されるグローバル設定です。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [ポータル ポリシー（Portal Policy）] を選択します。

ステップ 2　[1 人のユーザあたり 1 つのゲスト セッションを許可（Allow only one guest session per user）] オプションをオンにします。

ステップ 3　[保存（Save）] をクリックします。

関連項目

「ゲスト ポータル ポリシーの設定」（P.A-66）

「ゲスト デバイスはネットワーク アクセスを失ったままである」（P.G-33）

ゲストのアクセプタブル ユース ポリシーの必要性

ゲストがアカウントを完全に有効にするために受け入れる必要があるアクセプタブル ユース ポリシーを表示できます。ゲストがポリシーを受け入れない場合、ネットワーク アクセスできません。

はじめる前に

ゲスト ポータルを作成するか、または既存のものを使用します。アクセプタブル ユース ポリシーは、各ゲスト ポータルに固有です。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [マルチポータルの設定（Multi-Portal Configuration）] を選択します。

ステップ 2　ゲスト ポータルをオンにして更新し、[編集（Edit）] をクリックします。

ステップ 3　[操作（Operations）] タブをクリックします。

ステップ 4　次のオプションのいずれかを選択して、ゲスト ユーザがアクセプタブル ユース ポリシーに同意するかどうかを決定します。

- 未使用
- 初回ログイン
- ログインごと

ステップ 5　[保存（Save）] をクリックします。

関連項目

「マルチポータルの設定」（P.A-62）

ゲストのアクセプタブル ユース ポリシーのカスタマイズ

ゲストにアクセプタブル ユース ポリシーを承認するように要求する場合、会社のポリシーを反映するようにテンプレートを更新する必要があります。これは、すべてのゲスト ポータルに影響を与えるグローバル変更です。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [言語テンプレート（Language Template）] を選択します。

ステップ 2　ポリシーを適用する言語をクリックします。

ステップ 3　[利用規定ページの設定（Configure Acceptable Use Policy Page）] をクリックし、会社のポリシーに従うようにタイトルとテキストを更新します。

ステップ 4　[保存（Save）] をクリックします。

関連項目

「マルチポータルの設定」（P.A-62）

新しいゲスト時間プロファイルの作成

ゲスト アカウントの作成時にスポンサーが使用できるカスタム ゲスト時間プロファイルを作成できます。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [時間プロファイル（Time Profiles）] 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　時間プロファイルに名前と説明を割り当てます。この名前は、スポンサーがゲスト アカウントを作成するときに表示されます。

ステップ 4　時間制限に使用するタイム ゾーンを選択します。

ステップ 5　アカウント タイプおよび期間を選択します。

ステップ 6　制限時間に対して曜日および「から」と「まで」の時間を入力して、これらの時間にゲスト ユーザがネットワークにアクセスできないようにするか、ゲスト ユーザをログアウトさせます。

ステップ 7　[設定（Settings）] アイコンをクリックして追加の制限を追加します。

ステップ 8　[送信（Submit）] をクリックします。

関連項目

- 「ゲスト時間プロファイルの設定」（P.A-67）
- 「デフォルトのゲスト時間プロファイル」（P.16-21）

デフォルトのゲスト時間プロファイル

時間プロファイルでは、さまざまなレベルの時間がさまざまなゲスト アカウントにアクセスできるようにします。スポンサーはアカウントの作成時に時間プロファイルをゲストに割り当てる必要がありますが、時間プロファイルを変更することはできません。ただし、それらをカスタマイズし、特定のスポンサー グループが使用できる時間プロファイルを指定することはできます。Cisco ISE 1.2 から、時間プロファイルは、スポンサー ポータルの*アカウント期間*と呼ばれます。

Cisco ISE 1.2 には、以前使用できたプロファイルと置き換わる次のデフォルトのプロファイルがあります。

- DefaultFirstLoginEight：アカウントは、ゲスト ユーザが最初に正常にゲスト ポータルにログインしたときから開始する 8 時間利用できます。これは DefaultFirstLogin 時間プロファイルと置き換わります。
- DefaultEightHours：アカウントは、スポンサーが最初にアカウントを作成したときから開始する 8 時間利用できます。これは DefaultOneHour 時間プロファイルと置き換わります。
- DefaultStartEnd：スポンサーは、ネットワーク アクセスを開始および停止する日付および時刻を指定できます。

Cisco ISE 1.2 にアップグレードする場合は、古い時間プロファイルはまだ使用可能ですが、使用しない場合はそれらを削除できます。古い時間プロファイルがスポンサー グループに割り当てられている場合は、削除する前にアラート メッセージが表示されます。Cisco ISE 1.2 の新規インストールを実行した場合、新しい時間プロファイルだけが表示されます。

関連項目

- 「ゲスト時間プロファイルの設定」（P.A-67）
- 「新しいゲスト時間プロファイルの作成」（P.16-21）

ゲスト ユーザのポスチャの有効化

中央 WebAuth（CWA）のゲスト展開を使用してゲスト ポータルを実装している場合は、ウイルス保護ソフトウェアのチェックなど、ゲスト ユーザのポスチャ ポリシーを有効にできます。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [マルチポータルの設定（Multi-Portal Configurations）] 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　[操作（Operations）] タブをクリックします。

ステップ 4　[ゲスト ユーザは、ポスチャ クライアントをダウンロードする必要があります（Guest users should download the posture client）] オプションをオンにします。

ステップ 5　[送信（Submit）] をクリックします。

関連項目

- 「セルフプロビジョニング ポータル」（P.17-2）
- 「エンドユーザ ポータルに対するイーサネット インターフェイスの指定」（P.15-3）
- 「マルチポータルの設定」（P.A-62）

ゲストの ID ソース順序の指定

ゲスト ユーザがスポンサー ポータルにログインできるようにするには、各ゲスト ポータルに使用する ID ソース順序を選択する必要があります。この順序は、ゲストのログイン クレデンシャルとともに、ネットワークにアクセスするゲストを認証および許可するために使用されます。

順序でチェックされる複数の認証ソースを設定でき、複数のストアにユーザが存在するか、または同じフローで従業員および従来のゲストの組み合わせを使用する場合に便利です。

はじめる前に

- ID ソース順序を作成するか、または Cisco ISE に付属しているデフォルトの Guest_Portal_Sequence を使用できます。
- ゲスト ポータルを作成するか、または既存のものを使用します。この設定は、各ゲスト ポータルに固有です。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [マルチポータルの設定（Multi-Portal Configuration）] を選択します。

ステップ 2　ゲスト ポータルをオンにして更新し、[編集（Edit）] をクリックします。

ステップ 3　[認証（Authentication）] タブをクリックします。

ステップ 4　適切な ID ソース順序を選択します。

ステップ 5　[保存（Save）] をクリックします。

関連項目

「マルチポータルの設定」（P.A-62）

ゲスト ユーザが自分のアカウントを作成することおよびデバイスを追加することの許可

スポンサーは通常、ゲスト ユーザのログイン クレデンシャルを作成しますが、このロールをバイパスし、ゲストがセルフ サービスとアカウントの登録を使用して自分のアカウントを作成できるようにすることができます。

ゲストがアカウントを作成することの許可

ユーザがゲスト ポータルにリダイレクトされたときに、自分のアカウントを作成できるようにすることができます。

はじめる前に

ゲスト ポータルを作成し、ゲスト ロールおよび時間プロファイルを設定します。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [マルチポータルの設定（Multi-Portal Configuration）] を選択します。

ステップ 2　ゲスト ポータルをオンにして更新し、[編集（Edit）] をクリックします。

ステップ 3　[操作（Operations）] タブをクリックします。

ステップ 4　[ゲスト ユーザにアカウント登録を許可する必要があります（Guest users should be allowed to do self service）] 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。

関連項目

- 「マルチポータルの設定」（P.A-62）
- 「アカウント登録でのゲスト ロールの設定」（P.16-24）
- 「アカウント登録での時間プロファイルの設定」（P.16-24）

ゲストがデバイスを追加することの許可

ゲストがスポンサーによって作成されたクレデンシャルを使用してサイン インしているか、または自分で登録することによって作成されたクレデンシャルを使用してサイン インしているかにかかわらず、ゲストがデバイスを追加できるようにすることができます。

はじめる前に

ゲスト ポータルを作成するか、または既存のものを使用します。この設定は、各ゲスト ポータルに固有です。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [マルチポータルの設定（Multi-Portal Configuration）] を選択します。

ステップ 2　ゲスト ポータルをオンにして更新し、[編集（Edit）] をクリックします。

ステップ 3　[操作（Operations）] タブをクリックします。

ステップ 4　[ゲスト ユーザにデバイス登録を許可する必要があります（uest users should be allowed to do device registration）] 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。

関連項目

「マルチポータルの設定」（P.A-62）

アカウント登録でのゲスト ロールの設定

アカウント登録にゲスト ユーザに割り当てるデフォルトのゲスト ロールを選択する必要があります。ゲスト ロールは、ゲストがネットワークに対して持っているアクセスのタイプを変更するために認可ポリシーによって使用され、また、

- システムに定義されたポリシーに基づいて、関連する ID グループにゲスト ユーザを関連付けます
- ユーザがアクティブなゲストとして扱われるかどうかを制御します

これは、すべてのゲスト ポータルに適用されるグローバル設定です。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [ポータル ポリシー（Portal Policy）] を選択します。

ステップ 2　[アカウント登録ゲスト ロール（Self Registration Guest Role）] フィールドで、デフォルトのゲスト ロールを選択します。

ステップ 3　[保存（Save）] をクリックします。

関連項目

- 「ゲスト ポータル ポリシーの設定」（P.A-66）
- 「ゲストがアカウントを作成することの許可」（P.16-23）

アカウント登録での時間プロファイルの設定

アカウント登録後にゲスト ユーザに割り当てるデフォルトの時間プロファイルを選択します。時間プロファイルは、ゲストがネットワークに登録およびアクセスできる期間を決定します。使用できるのは、CreateTime タイプと FirstLogin タイプの時間プロファイルのみです。アカウント登録でのゲスト ユーザ アカウントの作成時には、どちらも FromCreation アカウントとして扱われます。

これは、すべてのゲスト ポータルに適用されるグローバル設定です。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [ポータル ポリシー（Portal Policy）] を選択します。

ステップ 2　[アカウント登録時間プロファイル（Self Registration Time Profile）] フィールドで、選択した時間プロファイルを選択します。

ステップ 3　[保存（Save）] をクリックします。

関連項目

- 「ゲスト ポータル ポリシーの設定」（P.A-66）
- 「ゲストがアカウントを作成することの許可」（P.16-23）

スポンサーとゲストのアクティビティのモニタリング

Cisco ISE では、次の方法を使用して、スポンサーとゲストのアクティビティを表示およびモニタできます。

- 「中断されたゲスト アカウントと期限切れのゲスト アカウント」（P.16-25）
- 「期限切れのゲスト アカウントの消去」（P.16-26）
- 「メトリック メーター」（P.16-26）
- 「ゲスト アクティビティ レポート」（P.16-26）
- 「ゲスト アカウンティング レポート」（P.16-27）
- 「ゲスト スポンサー概要」（P.16-27）
- 「ゲストおよびスポンサー ポータルでの監査ロギング」（P.16-27）

中断されたゲスト アカウントと期限切れのゲスト アカウント

ゲスト アカウントが中断されるか、または期限切れになると、適用されたゲスト ユーザはネットワークにアクセスできません。

ゲスト アカウントは、2 つの方法で中断できます。

- ゲストはログイン試行の最大回数に達しています（[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [ゲスト（Guest）] > [ポータル ポリシー（Portal Policy）] で定義）。
- スポンサーは、スポンサー ポータルからアカウントを手動で中断しました。

ゲスト アカウントがアカウント期間（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。

スポンサーは、中断されたアカウントおよび期限切れのアカウントを再アクティブ化または再開できます。ただし、期限切れのアカウントは、設定した基準（[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [一般（General）] > [消去（Purge）] ）に基づいて自動的に消去されます。アカウントが消去されたら、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。

期限切れのゲスト アカウントの消去

Cisco ISE は 15 日ごとに期限切れのゲスト アカウントを自動的に消去しますが、次の状況で設定を変更できます。

- 消去の実行が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、スケジュールされた次回の消去時刻にサーバが実行されていない限り、消去は再実行されません。
- システムにより、消去を実行する時間かどうか確認するために 15 分ごとにチェックされます。したがって、この自動プロセスとスケジュールされた消去のタイミングによって、消去の開始に最大 15 分の遅延が生じる可能性があります。

スケジュールされた消去を待つことなく、ただちに期限切れのゲスト ユーザ アカウントを強制的に消去できます。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [一般（General）] > [消去（Purge）] 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。

- [期限切れのゲスト アカウントの消去設定の有効化（Enable purge settings for expired guest accounts）] チェックボックスをオンにし、消去をスケジュールし、消去が行われる日の頻度と時間を指定します。
- 期限切れのゲスト ユーザ レコードをすぐに消去にするには、[今すぐ消去（Purge Now）] をクリックします。

ステップ 3　[保存（Save）] をクリックします。

関連項目

- 「ゲスト消去の設定」（P.A-57）

メトリック メーター

Cisco ISE のダッシュボードに表示されるメトリック メーターを見ると、ネットワークにおけるアクティブ ゲストを一目で把握できます。

ゲスト アクティビティ レポート

ゲスト アクティビティ レポートは、ゲスト ユーザがアクセスしている Web サイトに関する詳細を提供します。このレポートは、セキュリティ監査の目的で使用し、ゲスト ユーザがネットワークにアクセスした時間、およびそこで行った操作を示すことができます。このレポートは、[操作（Operations）] > [レポート（Reports）] > [エンドポイントとユーザ（Endpoints and Users）] > [ゲスト アクティビティ（Guest Activity）] で使用できます。

このレポートを使用するには、最初に次の手順を実行する必要があります。

- Passed Authentication ロギング カテゴリを有効にします。[管理（Administration）] > [ロギング（Logging）] > [ロギング カテゴリ（Logging Categories）] を選択し、[成功した認証（Passed Authentications）] を選択します。
- ゲスト トラフィックに使用するファイアウォール上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 IP アドレスとアクセスされた URL だけを要求するので、可能な場合は、この情報をだけを含むようにデータを制限します。
- Cisco ISE モニタリング ノードに syslogs を送信します。

関連項目

- 「レポート」（P.26-1）
- Cisco ネットワークでのゲスト トラフィックの統合された URL ロギングおよびレポートの設定

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。ActivatedGuest またはゲスト ID グループに割り当てられたすべてのユーザがこのレポートに表示されます。このレポートは、[操作（Operations）] > [レポート（Reports）] > [エンドポイントとユーザ（Endpoints and Users）] > [ゲスト アカウンティング（Guest Accounting）] で使用できます。

関連項目

「レポート」（P.26-1）

ゲスト スポンサー概要

ゲスト スポンサー概要レポートは、各スポンサーによって作成されたすべてのゲスト ユーザを表示し、アカウント登録でのゲスト ユーザの数も示します。ゲスト ユーザの詳細を表示するには、スポンサーの名前をクリックします。このレポートは、[操作（Operations）] > [レポート（Reports）] > [エンドポイントとユーザ（Endpoints and Users）] > [ゲスト スポンサー概要（Guest Sponsor Summary）] で使用できます。

関連項目

「レポート」（P.26-1）

ゲストおよびスポンサー ポータルでの監査ロギング

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 ツールおよびログ 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、スポンサーとゲストのアクティビティ ログが提示されます。

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。

関連項目

第 25 章「モニタリングおよびトラブルシューティング」

ゲスト展開シナリオ

Cisco ISE では、セキュアなゲスト アクセスを可能にするいくつかの展開オプションがサポートされます。有線またはワイヤレスのゲスト接続、およびローカルまたは中央 Web 認証を提供できます。

中央 WebAuth 対応の NAD のプロセス フロー

このシナリオは、ワイヤレスと有線のどちらのネットワーク アクセス デバイスにも当てはまります。このシナリオでは、ゲスト ユーザのクレデンシャルが Cisco ISE セッション キャッシュに追加され、ネットワーク アクセス デバイス（NAD）を使用して許可変更（CoA）が要求されます。NAD を通じて、Cisco ISE サーバに対して新規許可要求が行われます。セッション キャッシュ属性を使用して、ゲスト ユーザが完全に認証および許可されます。

（注）　WLC では、中央 WebAuth 用の CoA がサポートされていますので（7.2 以降）、NAD は、同じ設定方式を使用して有線またはワイヤレスで Cisco ISE ネットワークに接続することができます。

クライアントのデバイスを NAD に接続している場合は、ゲスト サービス インタラクションにより MAC 認証バイパス（MAB）要求が失敗し、その結果としてゲスト ポータルの中央 WebAuth ログインが開始されます。

次に、MAB の失敗によってトリガーされる中央 WebAuth プロセスの各ステップを示します。

1. クライアントは、有線接続によって NAD に接続します。クライアント上に 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. MAB 要求を Cisco ISE RADIUS サーバにポストするよう NAD が設定されます。
4. クライアント デバイスが再接続され、NAD により MAB 要求が開始されます。
5. Cisco ISE サーバで MAB 要求が処理されますが、クライアント マシン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、適切な「NetworkAccess:UseCase=Hostlookup」条件および「Session:Posture Status=Unknown」条件を含む許可ポリシーが存在することを確認してください。NAD では、この値に基づいて、ポート 8443 のすべてのクライアント 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 URL 値は次のとおりです。https://ip:port/guestportal/gateway?sessionId=NetworkSessionId&action=cwa。
6. クライアントは、クライアント ブラウザを使用して、任意の URL に対する HTTP または HTTPS 要求を開始します。
7. 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。
8. 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。
9. クライアントは、ユーザ名とパスワードを入力し、ログイン フォームを送信します。
10. ゲスト アクション サーバで、指定されたユーザ クレデンシャルの認証が行われます。
11. クレデンシャルが有効な場合は、ゲスト アクション サーバによってユーザ名とパスワードがローカル セッション キャッシュに格納されます。

12. Non-Posture フロー（追加検証のない認証）の場合は、次のことが当てはまります。

    ゲスト ポータルがクライアント プロビジョニングを実行するように設定されていない場合は、ゲスト アクション サーバによって API 呼び出しを通じて CoA が NAD に送信されます。この CoA により、NAD は RADIUS サーバを使用してクライアントの再認証を行います。この再認証では、セッション キャッシュに格納されているユーザ クレデンシャルが利用されます。新しい access-accept が、設定されたネットワーク アクセスとともに 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 が使用されている場合は、ゲスト ポータルで VLAN IP の更新が行われます。

    ユーザは、このプロセスで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名前とパスワードが自動的に使用されます。

13. Posture フローの場合は、次のことが当てはまります。

    ゲスト ポータルがクライアント プロビジョニングを実行するように設定されていて、ゲスト アクションによってクライアント ブラウザがクライアント プロビジョニング URL にリダイレクトされます。（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 プロビジョニングにリダイレクトされ、クライアント プロビジョニング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。

    a. クライアント プロビジョニング URL にリダイレクトされると、クライアント プロビジョニング サブシステムによって非永続 Web エージェントがクライアント マシンにダウンロードされ、クライアント マシンのポスチャ チェックが実行されます。（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）。

    b. クライアント マシンが準拠していない場合は、設定した許可ポリシーに「NetworkAccess:UseCase=GuestFlow」条件および「Session:Posture Status=NonCompliant」条件が含まれていることを確認してください。

    c. クライアント マシン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 RADIUS サーバを使用してクライアントの再認証を行います。この再認証では、セッション キャッシュに格納されているユーザ クレデンシャルが利用されます。新しい access-accept が、設定されたネットワーク アクセスとともに NAD に返されます。

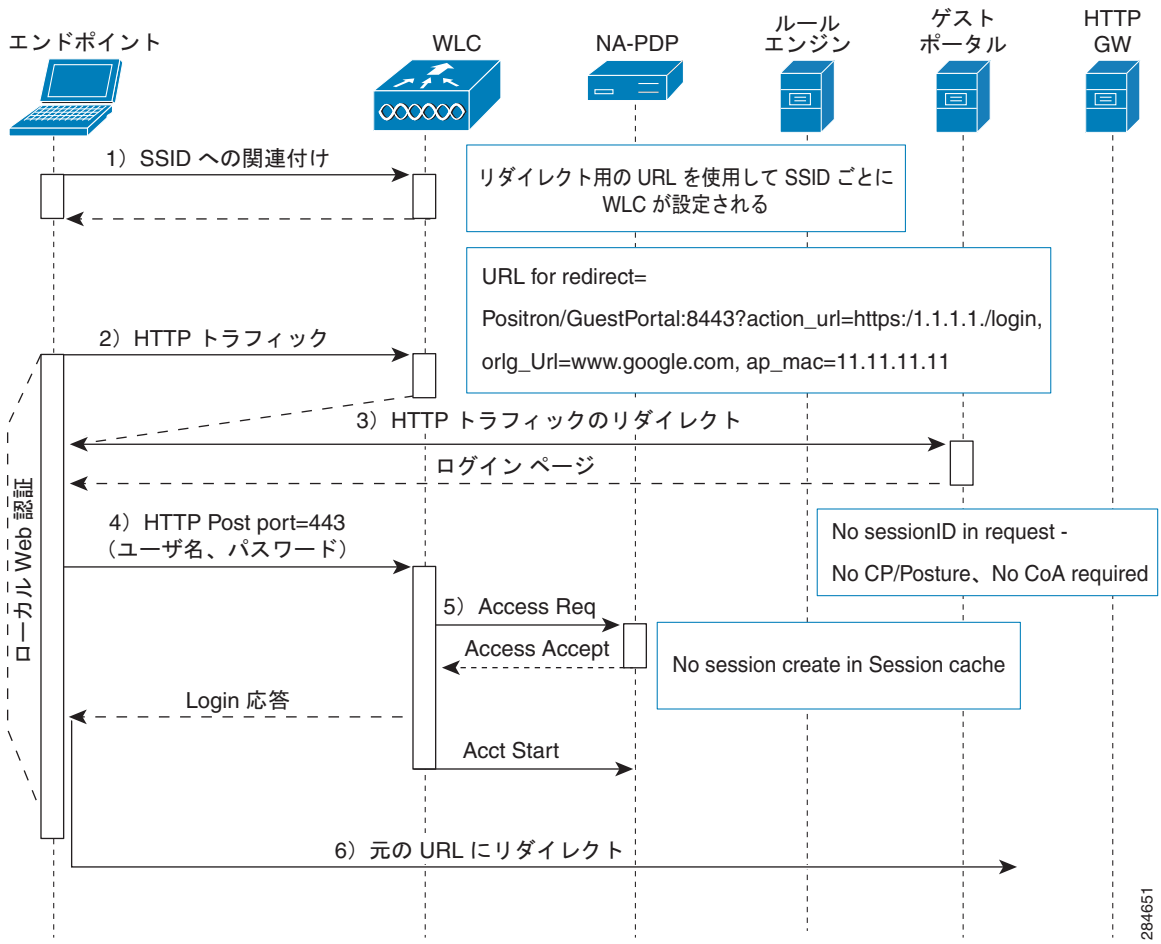
（注）「NetworkAccess:UseCase=GuestFlow」は、ゲスト ユーザとしてログインしている Active Directory ユーザおよび LDAP ユーザに適用されます。

ローカル WebAuth 対応のワイヤレス LAN コントローラ

このシナリオでは、ユーザがログインすると、ワイヤレス LAN コントローラ（WLC）に転送されます。その後、WLC により、このゲスト ポータルにリダイレクトされ、ユーザ名とパスワードの入力を求められます。必要に応じて、アクセプト ユース ポリシー（AUP）と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、ユーザのブラウザは再ログインのために元の WLC にリダイレクトされます。

WLC では、RADIUS によってユーザ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、クライアント ブラウザが WLC から元の宛先にリダイレクトされます。このプロセス フローの例については、図 16-1 を参照してください。

図 16-1　ローカル WebAuth の Non-Posture フロー



ローカル WebAuth 対応の有線 NAD

このシナリオでは、ゲスト ユーザ ログイン ポータルにより、ゲスト ユーザのログイン要求がスイッチ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、その一部としてユーザ クレデンシャルが含まれます。スイッチにユーザ ログイン要求が届くと、Cisco ISE RADIUS サーバ実装を指す設定済みの RADIUS サーバを使用してユーザの認証が行われます。

次に、ローカル WebAuth 対応の有線 NAD プロセスの各ステップを示します。

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 がクライアント ブラウザに返されます。
2. その後、クライアント ブラウザが Cisco ISE ゲスト ポータルにリダイレクトされます。ここから、ユーザのクレデンシャルが送信されます。
3. AUP とパスワード変更が処理された後（マルチポータル設定で指定されている場合）、ゲスト ポータルにより、ユーザ クレデンシャルをポストするクライアント ブラウザが NAD にリダイレクトされます。
4. NAD により、Cisco ISE に対して RADIUS 要求が発行され、ユーザ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、スイッチに割り当てる値が Cisco ISE の設定に一致するように、この値を変更できます。

```
<!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/guestportal/portal.jsp?switch_url=wired">

</HEAD>
<BODY>

<center>
Redirecting ... Login
<br>
<br>
<a href="https://ip:port/guestportal/portal.jsp?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 で有効な HTTPS サーバ

Web ベース認証を使用するには、**http secure-server** コマンドを使用して、スイッチで 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 にアップロードすることができます。Cisco ISE では特定のカスタマイゼーションは必要ないので、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 における 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

デバイス登録 Web 認証（DRW）を使用すると、ゲスト アカウント クレデンシャルを必要とせずにゲストのデバイスがネットワークに接続できるようにします。

デバイス登録 Web 認証プロセス

このシナリオでは、ゲスト ユーザがネットワークに接続するときに、初回の MAB 要求を Cisco ISE ノードに送信するワイヤレス接続を使用します。ユーザの MAC アドレスがエンドポイント ID ストアに含まれていない場合、または AUP accepted 属性が true に設定されていない場合、Cisco ISE は URL リダイレクション許可プロファイルを使用して応答します。ユーザが URL に移動しようとすると、URL リダイレクションによって AUP 受け入れページが表示されます。

次に、デバイス登録 WebAuth プロセスの各ステップを示します。

1. ゲスト ユーザは、ワイヤレス接続を使用してネットワークに接続します。このユーザの MAC アドレスは、エンドポイント ID ストアに含まれておらず、AUP accepted 属性も true に設定されていないため、ユーザは URL リダイレクション許可プロファイルを受け取ります。ゲスト ユーザが URL に移動しようとすると、URL リダイレクションによって AUP 受け入れページが表示されます。
2. ゲスト ユーザが AUP を受け入れると、ユーザの MAC アドレスがエンドポイント ID ストアに新しいエンドポイントとして登録されます（エンドポイントがまだ存在しないと仮定）。ユーザが AUP を受け入れたことを追跡できるよう、新しいエンドポイントの AUP accepted 属性は true に設定されます。その後、管理者は、[Web ポータル管理（Web Portal Management）] の [マルチポータルの設定（Multi-Portal Configurations）] ページでエンドポイント ID グループを選択し、エンドポイントに割り当てることができます。
3. ゲストのエンドポイントがエンドポイント ID ストアにすでに存在する場合は、既存のエンドポイントの AUP accepted 属性が true に設定されます。エンドポイント ID グループは、[Web ポータル管理（Web Portal Management）] の [マルチポータルの設定（Multi-Portal Configurations）] ページで選択した値に自動的に変更されます。
4. ユーザが AUP を受け入れないか、エンドポイントの作成時にエラーが発生した場合は、エラーページが表示されます。
5. エンドポイントが作成または更新されると、成功ページが表示され、その後に CoA 終了が NAD/WLC に送信されます。
6. CoA の後、NAD/WLC により、新しい MAB 要求を使用してユーザの接続が再認証されます。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/WLC に返されます。

（注） 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 IP のリリースおよび更新を実行して有線とワイヤレスの両方の CoA タイプを Change of Auth に再認証するように、デバイス登録認証（DRW）を設定することができます。

デバイス登録 WebAuth のゲスト ポータルの作成

デバイス登録 WebAuth（DRW）を設定できます。

ステップ 1　[管理（Administration）] > [Web ポータル管理（Web Portal Management）] > [設定（Settings）] > [マルチポータルの設定（Multi-Portal Configurations）] を選択します。

ステップ 2　[名前（Name）] フィールドに一意の名前を入力します。このポータル名は、許可プロファイルで返される URL-redirect 値で使用し、要求処理用のポータルとして指定する必要があります。

ステップ 3　次のいずれかを選択します。

- **デバイス Web 認証ポータル**：Cisco ISE によって提供される標準 HTML ページを使用します

- **カスタム デバイス Web 認証ポータル**：カスタマイズした HTML ページとイメージをアップロードします

ステップ 4　[エンドポイント ID グループ（Endpoint Identity Group）] オプションから [GuestEndpoints] を選択します。Cisco ISE では、DRW ポータルで使用するためにこのデフォルトの ID グループが用意されています。

ステップ 5　[送信（Submit）] をクリックします。

次の作業

「DRW 許可プロファイルの作成」（P.16-34）

関連項目

「Cisco ISE 許可プロファイル」（P.20-1）

DRW 許可プロファイルの作成

デバイス登録 WebAuth を使用するには、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

最初に DRW ゲスト ポータルを作成して、許可プロファイルを設定するときにその名前を使用できるようにします。

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　以前作成した DRW ゲスト ポータルの名前を使用して、許可プロファイルを作成します。

次の作業

「DRW 許可ポリシー ルールの作成」（P.16-34）

関連項目

「Cisco ISE 許可プロファイル」（P.20-1）

DRW 許可ポリシー ルールの作成

ゲスト ユーザがアクセプト ユース ポリシーを確認すると、Cisco ISE はエンドポイントを作成し、内部エンドポイント ID ストアに登録されます。エンドポイントは、MAC アドレスを使用して作成され、AUP accepted 属性が true に設定されます。

ステップ 1　[ポリシー（Policy）] > [許可（Authorization）] > [標準（Standard）] を選択して、新しい許可ポリシーを作成します。

ステップ 2　条件として [GuestEndpoints] エンドポイント ID グループを選択します。

ステップ 3　権限として DRW 許可プロファイルを選択します。

この設定により、初回の MAB 要求が許可ポリシー ルールに適合する場合に、URL-redirect cisco av pair が WLC に返されるようになります。URL-redirect は次の形式になります。

ip:port = それぞれ IP アドレスとポート番号

DRWPortal = 一意のポータル名

https://*ip:port*/guestportal/gateway?sessionID=SessionIdValue&portal=*DRWPortal*&action=cwa

---

関連項目

「許可ポリシーの設定」（P.20-8）