



# ISE 高速インストール ガイド

セキュア アクセスを実現するハウツー ガイド シリーズ

作成者: Jason Kunst

日付: 2015 年 5 月

## 目次

このガイドについて.....	4
このガイドの使用方法 .....	4
要件 .....	5
ゲスト アクセス .....	6
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.....	6
クレデンシアルを持つゲスト ポータルを使用したゲスト アクセス.....	6
Cisco ISE ソフトウェアのダウンロード.....	7
計画.....	8
事前設定チェックリスト .....	8
WLC の基本設定.....	10
WLC への接続 .....	10
キャプティブ ポータルのバイパス設定 .....	14
トポロジの例.....	16
RADIUS 用の WLC の設定 .....	17
WLC での RADIUS 認証サーバの設定 .....	17
WLC での RADIUS アカウンティング サーバの設定 .....	18
中央 Web 認証(CWA)を使用するように WLC の設定を変更します .....	18
ゲストのリダイレクト用の ACL の設定およびアクセスの許可 .....	21
ゲスト デバイスを ISE ゲスト ポータルにリダイレクトするための ACL の設定 .....	21
認証後にインターネットへのゲスト アクセスを許可するための ACL の設定 .....	22
VMware でのインストールおよび設定 (ISE) .....	23
仮想マシンへの Cisco ISE のインストール.....	24
ISE OVA の仮想マシンとしての導入 .....	24
ISE のセットアップの実行 .....	24
ISE のパッチのインストール .....	25
ゲスト アクセス用の ISE の設定.....	26
ワイヤレス コントローラ(WLC)のネットワーク アクセス デバイス(NAD)としての設定 .....	26
認証ポリシーの設定 .....	27
ゲスト エンドポイントを ISE へリダイレクトする認証プロファイルの作成 .....	27
アクセスを認可するための認証プロファイルの作成 .....	28
ゲスト アクセス用の認証ポリシーの作成 .....	29

自己登録およびスポンサー ゲストのフローに必要な最小限の設定 (任意).....	31
ゲストのロケーションとタイム ゾーンの設定.....	31
該当のロケーションを使用するようにポータルを設定 .....	32
スポンサー ゲストのフローに必要な設定 (任意).....	33
スポンサー グループを設定します .....	33
Active Directory スポンサー グループ All_Accounts の設定 .....	34
スポンサー グループのロケーションの設定 .....	35
ISE スポンサー ポータルの FQDN ベースのアクセスの設定 .....	36
既知の証明書の設定 (任意) .....	37
証明書署名要求の作成と認証局への CSR の送信 .....	37
信頼された証明書ストアへの証明書のインポート .....	39
署名要求への CA 署名付き証明書のバインド.....	40
管理ポータルおよび EAP 認証で使用する証明書の編集 .....	41
ポータルで既知の証明書を使用するための設定 .....	42
ポータルの基本的なカスタマイズの設定 (任意) .....	43
次のステップ .....	45
付録 A: スイッチの設定 .....	46

## このガイドについて

このガイドでは、すぐにゲスト アクセスできるように Cisco Identity Services Engine (ISE) とシスコ ワイヤレス コントローラを設定するプロセスについて説明します。このガイドの手順に従うことにより、約 2 時間でユーザのゲスト アクセスをセットアップできます。

このガイドは ISE 1.3 を使用して作成されましたが、ISE 1.4 にも対応しています。

このガイドでサポートされるポータルには次の 2 種類があります。

- 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
- クレデンシアルを持つゲスト ポータルを使用したゲスト アクセス

## このガイドの使用方法

このガイドには、ISE とシスコ ワイヤレス コントローラ (WLC) を使用してワイヤレス ゲスト アクセスをインストールし、設定するために必要なアクティビティを説明する 2 つのパートがあります。

- **パート 1: シスコ ワイヤレス コントローラ (WLC) のインストールおよび設定:** パート 1 では、インストール前の事前設定および設定のアクティビティについて説明します。これらのアクティビティは、パート 2 に記載されたタスクを開始する前に完了しておく必要があります。
- **パート 2: VMware での Identity Services Engine (ISE) のインストールおよび設定:** パート 2 では、VMware サーバでの ISE ソフトウェアのインストールと設定、および WLC を使用したゲスト サービスの設定について説明します。

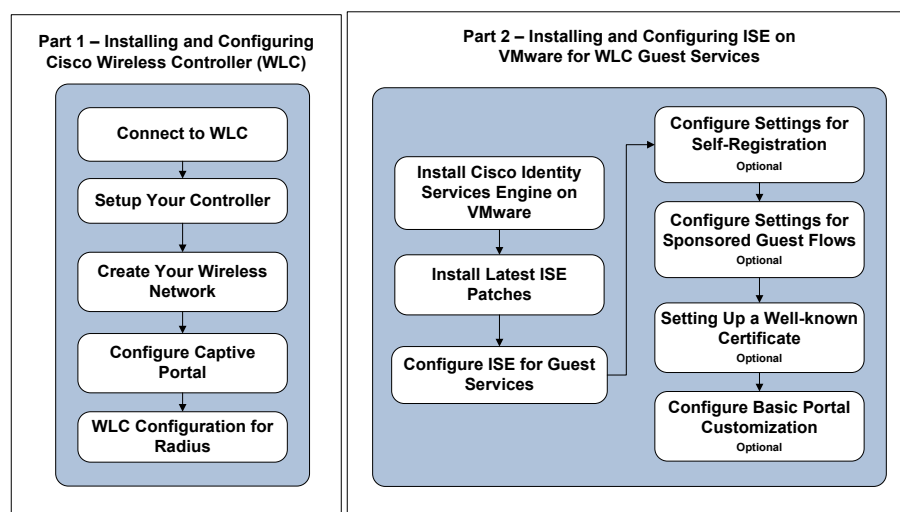


図 1. ゲスト サービスのための WLC を使用した ISE 高速インストールおよび設定プロセス

## 要件

- VMware ESX (i) 4.x 以上
- SNS-3415 アプライアンスとして実行される仮想マシン。「[VMware Appliance Specifications](#)」の表 2 を参照してください。
- 最新のパッチを適用した Cisco Identity Services Engine リリース 1.3 または 1.4
  - 既知の問題 ([CSCus55690](#)) への対応。この問題は、1.3 のパッチ 3 および 1.4 のパッチ 1 で解消されます。これらのパッチが入手可能になり次第、インストールすることを強くお勧めします。
  - **注:** デバイスは、消去された後であってもエンドポイント データベースからは除外されず、アクセス可能な状態が維持されます。
- 物理シスコワイヤレス コントローラ (WLC) 7.6.x または 8.x

**注:** このガイドは、新規インストールのみを対象にしています。新規のインストールでない場合は、コントローラを初期設定にリセットしてください。コントローラをリセットする手順については、コントローラのマニュアルを参照してください。

## ゲスト アクセス

社外の人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内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、さまざまなゲスト ポータルを介してネットワーク アクセスを提供することができます。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。

このガイドでサポートされるゲスト アクセス ポータルには、次の 2 種類があります。

- 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
- 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

### 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

ホットスポットゲスト ポータルを使用したゲスト アクセスとは、ゲストが接続する際にユーザ名とパスワードの確立を要求せずにネットワークにアクセスできるように設定するゲスト ポータルです。このタイプのゲスト アクセスは、個別のゲスト アカウントを管理するためのオーバーヘッドがありません。ゲストがネットワークに接続すると、ゲストは ISE のホットスポット ゲスト ポータルにリダイレクトされます。このポータルでゲストは、ネットワークや、最終的にはインターネットへアクセスできるように、アクセプタブル ユース ポリシー (AUP) に同意する必要があります。

### クレデンシャルを持つゲスト ポータルを使用したゲスト アクセス

クレデンシャルを持つゲスト ポータルを使用したゲスト アクセスによってネットワークにアクセスできますが、ゲストがアクセス権を取得するにはユーザ名とパスワードを所有していなければなりません。ゲストは自己登録ポータルを使用して、ゲストポータルへのログインに使用するアカウントを自分で作成できます。このポータルは、スポンサーによって作成されたクレデンシャルでも使用することができます。従業員またはロビー アンバサダーなどがスポンサーになれます。ネットワークに接続したゲストはポータルにリダイレクトされます。このポータルには、自己登録したクレデンシャルか、スポンサーが作成したクレデンシャルを使用してログインできます。ゲストはログインすると、ネットワークへの (最終的にはインターネットへの) アクセス権を得るためにアクセプタブル ユース ポリシー (AUP) に同意するよう求められる場合があります。スポンサー ゲストポータルを使用してアクセス権を設定することもできます。このポータルでは、ユーザはスポンサーによって作成されたクレデンシャルが必要です。

ゲスト ポータルおよび機能の詳細については、「[Cisco Guest Access](#)」を参照してください。

# Cisco ISE ソフトウェアのダウンロード

ISE ソフトウェアのダウンロードリンクから、最新の Cisco ISE ソフトウェアおよび ISE のパッチをダウンロードします。ダウンロード時間は、ネットワークの速度によって異なります。

## ソフトウェアのダウンロード

次のファイルをダウンロードできる Cisco ISE ソフトウェア ダウンロード ページにアクセスするには、「[Cisco ISE Download Software](#)」をクリックします。

- ISE 1.3 または 1.4 の ISE VM OVA ファイル: Virtual SNS-3415
  - 例: ISE-1.3.0.876-virtual-SNS3415-2.ova
- ISE 1.3 または 1.4 の最新のパッチ ファイル
  - 例: ise-patchbundle-1.3.0.876-Auto1-125229.x86\_64.tar.gz

**注:** ISE のパッチ (tar.gz) のダウンロード時、OSX Safari など、一部の Web ブラウザでは注意が必要です。パッチのインストール時にアーカイブの構造を維持する必要があり、そのためには、Firefox または Google Chrome ブラウザを使用します。

下記のリンクをクリックすると、Cisco ISE ソフトウェアのダウンロードについてのビデオを視聴できます。

- [ISE の概要および Cisco ISE ソフトウェアのダウンロードの方法](#)

## 計画

ISE および WLC のインストールおよび設定を開始する前に、ISE および WLC のインストールおよび設定で後から使用する情報を収集しておくことをお勧めします。サーバ情報を整理し、記録するのに役立つチェックリストを作成しました。設定プロセスにおけるインストール時に、必要に応じてこのチェックリストを参照してください。

**注:** ISE をインストールするにあたり、**事前設定チェックリスト**の情報を記録する際に次のサービスへのアクセス権があることを確認します。これらのサービスが使用できない場合、インストール プロセスは失敗する可能性があります。

- DNS
- NTP およびデフォルト ゲートウェイ

ご使用の **ESX** および **NTP ホスト**の時間が正しいことを確認します。サービスおよび証明書が正しく機能するためには、ホストの時間が同期されている必要があります。

## 事前設定チェックリスト

番号	サービス	説明	情報をここに記録
1	WLC システム名	<ul style="list-style-type: none"> <li>• WLC で設定されたコントローラのシステム名</li> <li>• 例: WLC</li> </ul>	WLC システム名: _____
2	ワイヤレス コントローラの IP、サブネット マスク、ゲートウェイ	<ul style="list-style-type: none"> <li>• WLC のネットワーク情報</li> </ul>	ワイヤレス コントローラの IP: _____ サブネット マスク: _____ ゲートウェイ: _____
3	DHCP サーバの IP	<ul style="list-style-type: none"> <li>• ネットワーク内の DHCP サーバ</li> <li>• WLC で設定</li> </ul>	DHCP サーバの IP: _____
4	ゲスト SSID (Guest SSID)	<ul style="list-style-type: none"> <li>• ゲストがアクセスするネットワークの名前</li> <li>• WLC で設定</li> <li>• 例: yourcompany-guest (企業名-ゲスト)</li> </ul>	ゲスト SSID: _____
5	ゲスト VLAN (任意) ゲスト用に管理ネットワークと同じネットワークを使用する場合不要です	<ul style="list-style-type: none"> <li>• ゲスト用に使用される VLAN</li> <li>• WLC で設定</li> <li>• 例: 50</li> </ul>	ゲスト VLAN: _____



6	ゲストネットワークの IP アドレス、サブネット マスク、ゲートウェイ	<ul style="list-style-type: none"> <li>• コントローラがゲストと通信するために、ゲストネットワークの IP アドレスが必要です</li> <li>• WLC で設定</li> </ul>	ゲスト ネットワークの IP: _____ サブネット マスク: _____ ゲートウェイ: _____
7	DNS サーバの IP	<ul style="list-style-type: none"> <li>• ネットワーク内の DNS サーバ</li> <li>• ISE で設定</li> </ul>	DNS サーバの IP: _____
8	NTP サーバの IP	<ul style="list-style-type: none"> <li>• ネットワーク内の NTP サーバ</li> <li>• ISE で設定</li> </ul>	NTP サーバの IP: _____
9	ISE の IP、サブネット マスク、およびゲートウェイ	<ul style="list-style-type: none"> <li>• ISE のネットワーク情報</li> <li>• ISE で設定</li> </ul>	ISE の IP: _____ サブネット マスク: _____ ゲートウェイ: _____
10	ISE のホスト名	<ul style="list-style-type: none"> <li>• ISE サーバの名前</li> <li>• ISE で設定</li> <li>• 例: <i>yourdomain.com</i> (ユーザのドメイン.com)</li> </ul>	ISE のホスト名: _____
11	管理ネットワーク VLAN	<ul style="list-style-type: none"> <li>• ESX (i) ホストで ISE および WLC が接続するネットワーク</li> <li>• WLC および ESX(i) ホストで設定</li> <li>• 例: 100</li> </ul>	管理 ネットワーク VLAN: _____
12	共有秘密鍵 (Shared Secret)	<ul style="list-style-type: none"> <li>• これは、RADIUS チャネルを保護するために ISE と WLC 間の通信で共有されるパスワードです。</li> <li>• WLC および ISE で設定</li> </ul>	共有秘密鍵: _____

## WLC の基本設定

シスコワイヤレス LAN コントローラは複数の方法で設定できます。このガイドでは、WLAN 高速セットアップを使用します。WLAN 高速セットアップと WLC の設定の詳細については、次のリンクのいずれかを選択してください。

- [WLAN 高速セットアップについてのビデオ](#)
- [Cisco WLAN リリースノート](#)

## WLC への接続

シスコワイヤレス ゲスト サービスを構成するすべてのコンポーネントを接続する前に、まず、ご使用のラップトップ (コンピュータ) と WLC 間の通信を確立する必要があります。最初にラップトップと WLC 間の通信を確立すると、ハードウェアのセットアップとソフトウェアのインストール手順を完了できるようになります。

### コントローラのセットアップ

WLC に接続するには、次の手順に従います。

**ステップ 1** 図 1 に示すように、**管理用ラップトップ**を WLC の**ポート 2** に接続します。



図 2. ラップトップと WLC との接続

ラップトップはサブネット 192.168.1.0/24 から IP アドレスを取得します。

**ステップ 2** ブラウザを開き、アドレス バーに <https://192.168.1.1> と入力して、WLC の管理ユーザ インターフェイスにアクセスします。

図 2 に示すように WLC の管理ユーザ インターフェイスが表示されます。

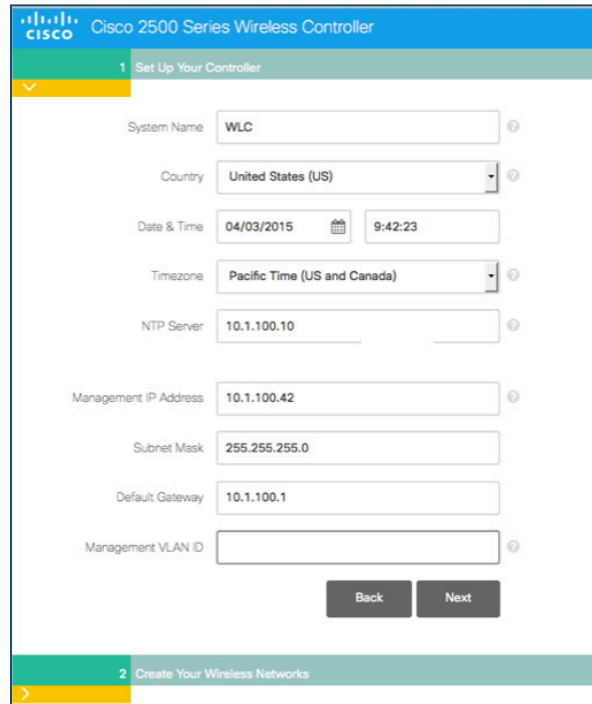


図 3. WLC:[コントローラのセットアップ (Set Up Your Controller)] タブ

**ステップ 3** コントローラを管理するためのクレデンシャルを入力します。「計画」の項で完成させた「事前設定チェックリスト」を参照してください。

表 1. ワイヤレス LAN コントローラのウィザード

フィールド	説明
システム名 (System Name)	WLC システム名 事前チェックリストの項目番号 : 1
国 (Country)	現在の国の場所
日付と時刻 (Date & time)	現在の日付と時刻
タイムゾーン (Timezone)	ドロップダウン メニューからタイムゾーンを選択します
NTP サーバ	NTP サーバの IP アドレス 事前チェックリストの項目番号 : 8
管理 IP アドレス (Management IP Address)	ワイヤレス コントローラを管理するための IP アドレス 事前チェックリストの項目番号 : 2
サブネット マスク (Subnet Mask)	WLC のサブネット マスク 事前チェックリストの項目番号 : 2
デフォルト ゲートウェイ (Default)	WLC のデフォルト ゲートウェイ

フィールド	説明
Gateway)	事前チェックリストの項目番号 : 2
管理ネットワーク VLAN	管理ネットワーク VLAN 事前チェックリストの項目番号 : 11

**ステップ 4** [次へ (Next)] をクリックして続行します。

次に、ワイヤレス ネットワークを作成する必要があります。

## ワイヤレス ネットワークの作成

**ステップ 1** [従業員用ネットワーク (Employee Network)] を選択解除するには、[X] をクリックします。

**注:** 従業員 (内部ユーザ) 用のワイヤレス dot1x ネットワークの設定については、このガイドでは取り扱いません。

**ステップ 2** 図 3 に示すように、[ゲストネットワーク (Guest Network)] の横のチェックマークをクリックします。

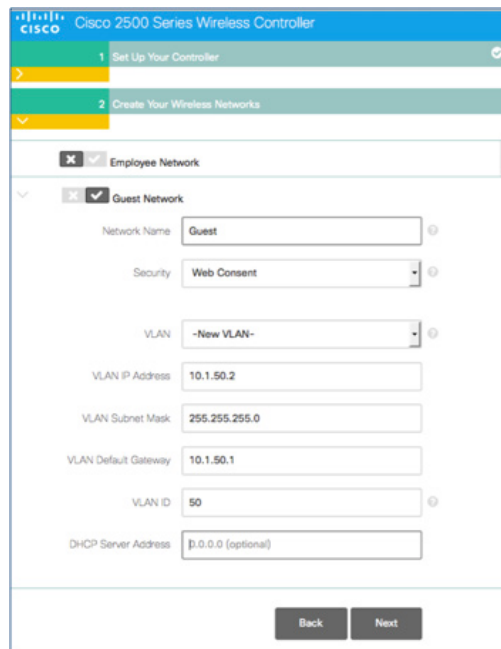


図 4. WLC: [ワイヤレスネットワークの作成 (Create Your Wireless Network)] タブ

表 2. [ワイヤレスネットワークの作成 (Create Your Wireless Network)] タブのフィールド

フィールド	説明
ネットワーク名 (Network Name)	ゲスト用のワイヤレス ネットワーク (SSID) 事前チェックリストの項目番号 : 4
セキュリティ	ドロップダウン メニューに表示されるオプションから、セキュリ

フィールド	説明
	ティタイプ [Web での同意 (Web Consent)] を選択します。
VLAN	ドロップダウン メニューに表示されるオプションから、VLAN [新しい VLAN (New VLAN)] を選択します。
VLAN IP アドレス (VLAN IP Address)	ゲスト ネットワークの IP アドレス 事前チェックリストの項目番号: 6
VLAN サブネット マスク (VLAN Subnet Mask)	VLAN のサブネット マスクの IP アドレス 事前チェックリストの項目番号: 6
VLAN デフォルト ゲートウェイ (VLAN Default Gateway)	デフォルト ゲートウェイの IP アドレス 事前チェックリストの項目番号: 6
VLAN ID (任意)	VLAN の ID (任意。管理ネットワークを使用する場合は不要) 事前チェックリストの項目番号: 5
DHCP サーバ アドレス (DHCP Server Address)	DHCP サーバの IP アドレス 事前チェックリストの項目番号: 3

**ステップ 3** 計画段階で用意した、**必要な情報**を入力します。

**ステップ 4** [次へ (Next)] をクリックして続行します。

図 5 に示すように、確認画面が表示され WLC の変更を適用するかどうか確認されます。[OK] をクリックするとシステムが再起動することが通知されます。

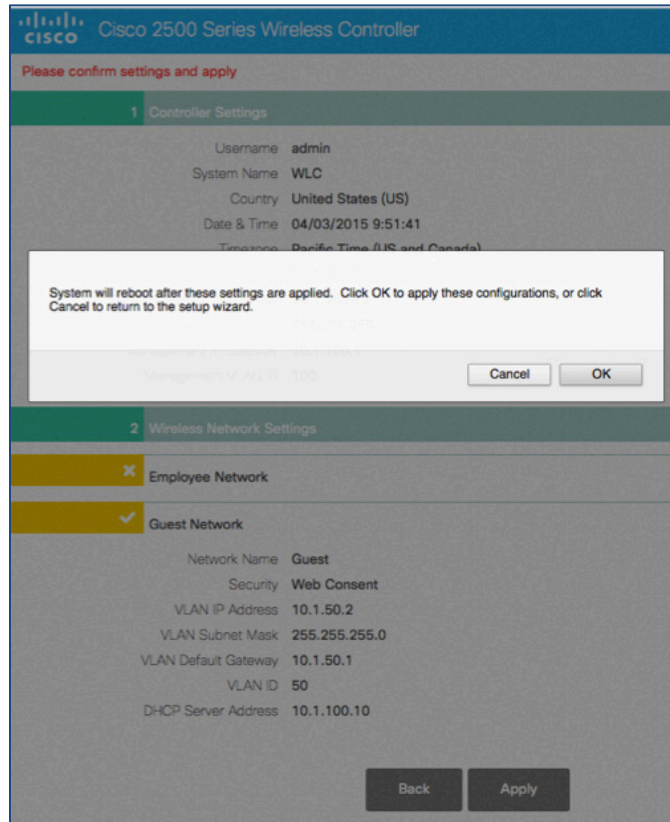


図 5. WLC:ワイヤレス ネットワークを作成するかどうかの確認

## キャプティブ ポータルのバイパス設定

Cisco Identity Services Engine ソフトウェアは、さまざまな Web ブラウザでサポートされます。Apple の Safari Web ブラウザから Cisco ISE ゲスト アクセスを利用してコントローラを使用するには、ISE ゲスト サービスのインストールと設定を行う前に、キャプティブ ポータルのバイパス設定プロセスを完了しておく必要があります。

キャプティブ ポータルのバイパスを設定するには、次の手順に従います。

- ステップ 1.** Putty などの SSH クライアントを使用して、ワイヤレス コントローラの IP アドレスに接続します。
- ステップ 2.** コントローラの CLI にログインします。
- ステップ 3.** 次のコマンドを入力します。

```
config network web-auth captive-bypass enable
```

コントローラがリブートします。

- ステップ 4.** CLI に再度ログインし、次のコマンドを使用してステータスを表示します。

```
show network summary
```

ステップ 5. 最後のページで、次の行を見つけます。

ヒント:スペースキーを 2 回押すと、最後のページに移動します。

```
Web Auth Captive-Bypass ..... 有効(Enable)
```

ステップ 6. SSH セッションを閉じ、Web ブラウザを使用して WLC に再接続します。

Captive Portal Bypass コマンドの詳細な使用方法については、「[Configuring Captive Bypassing](#)」から、ご使用の環境に応じた特定のコードのリリースを参照してください。

## トポロジの例

本書に記載されているシナリオと設定についてさらにご理解いただくために、次のトポロジ例をご覧ください。

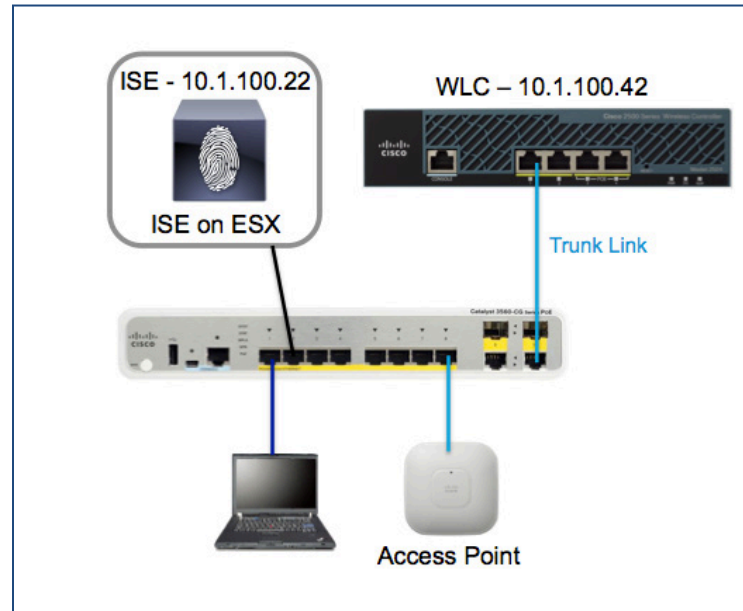


図 6. トポロジの例

トポロジ例の Cisco 3560G スイッチ (図 6) は、基本的にすべてのコンポーネントを接続しています。スイッチのすべてのポートは VLAN 100 へのアクセス用に設定されます。ただし、**ポート 10** をトランクポートとして設定する必要があります。

スイッチの設定の詳細については「付録 A」を参照してください。

**注:** WLC の再起動後、管理機能は VLAN 100 (例: 10.1.100.42) 上で稼働し、古い IP アドレス経由では応答なくなります。

**ステップ 1** WLC のポート 2 から管理用のラップトップを外し、スイッチのポート 1 に接続します。

**ステップ 2** WLC のポート 1 を、スイッチのトランクポートに接続します。

スイッチを使用することで WLC にアクセスできます。(例: <https://10.1.100.42>)。



## RADIUS 用の WLC の設定

この項では、WLC と ISE を機能させるのに必要なセキュリティ設定について説明します。RADIUS NAC を使用すると、ISE が認可変更 (COA) 要求を送信できるようになります。この要求は、ユーザがすでに認証されており、ネットワークにアクセスできることを示します。つまり、新しいセッションを開かなくても ISE がクライアントの状態を随時変更できるようになります。クライアントの状態を、ポータル認証のために ISE にリダイレクトされている状態から切り替え、認証が完了したら、そのクライアントの状態を変更して、ネットワークへのアクセス (例: インターネット) を許可します。

### WLC での RADIUS 認証サーバの設定

RADIUS 認証サーバを設定するには、次の手順に従います。

**ステップ 1** ワイヤレス LAN コントローラ (WLC) サーバの GUI にログインします。

**ステップ 2** 図 7 に示すように、左側のメニューから、[セキュリティ (Security)] > [AAA] > [RADIUS] > [認証 (Authentication)] の順に選択します。

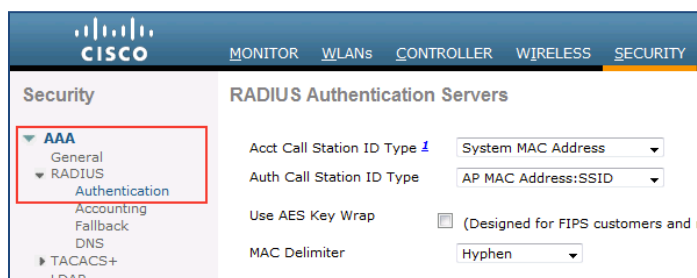


図 7. Radius 認証サーバ

**ステップ 3** [新規 (New)] をクリックします。

図 8 に示すように、RADIUS 認証サーバの画面が表示されます。

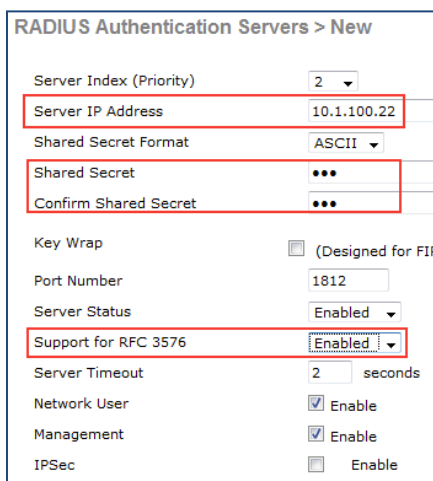


図 8. Radius 認証サーバ: 編集

**ステップ 4** ISE の IP アドレスおよび共有秘密鍵を入力します。

**ステップ 5** RFC 3576 に対するサポートを有効にします。

**ステップ 6** [適用 (Apply)] をクリックします。

## WLC での RADIUS アカウンティング サーバの設定

RADIUS アカウンティング サーバを設定するには、次の手順に従います。

**ステップ 1** ワイヤレス LAN コントローラ (WLC) サーバの GUI にログインします。

**ステップ 2** 図 9 に示すように、左側のメニューから、[セキュリティ (Security)] > [AAA] > [RADIUS] > [アカウンティング (Accounting)] の順に選択します。

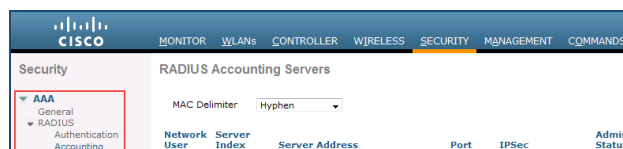


図 9. Radius アカウンティングサーバ

**ステップ 3** [新規 (New)] をクリックします。

図 10 に示すように、RADIUS アカウンティング サーバの画面が表示されます。

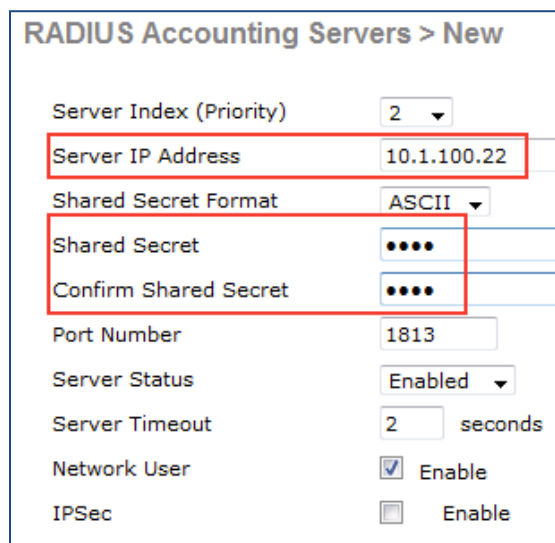


図 10. Radius アカウンティングサーバ: 編集

**ステップ 4** ISE の IP アドレスおよび共有秘密鍵を入力します。

**ステップ 5** [適用 (Apply)] をクリックします。

## 中央 Web 認証 (CWA) を使用するように WLC の設定を変更します

CWA を使用するように WLC の設定を変更するには、次の手順に従います。

**ステップ 1** [WLAN (WLANs)] を選択します。

**ステップ 2** [ゲスト SSID (Guest SSID)] を選択します。

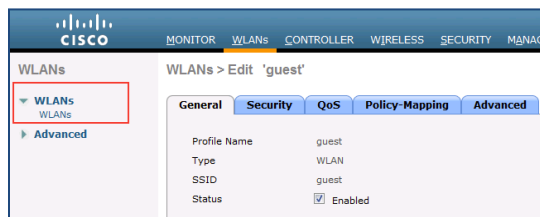


図 11. WLAN

**ステップ 3** [セキュリティ] タブを選択します。

**ステップ 4** [レイヤ 2 (Layer 2)] タブをクリックします

図 12 に示すように、[レイヤ 2 セキュリティ (Layer 3 Security)] タブ オプションが表示されます。

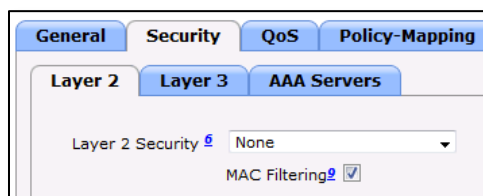


図 12. レイヤ 2 セキュリティ

**ステップ 5** レイヤ 2 セキュリティに対して、[なし (None)] を選択します。

**ステップ 6** [MAC フィルタリング (MAC Filtering)] を有効にします。

**ステップ 7** [レイヤ 3 (Layer 3)] タブをクリックします。

図 13 に示すように、[レイヤ 3 セキュリティ (Layer 3 Security)] タブ オプションが表示されます。

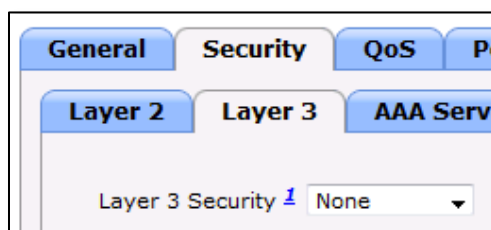


図 13. レイヤ 3 セキュリティ

**ステップ 8** [なし (None)] を選択します。

**ステップ 9** [AAA サーバ (AAA Servers)] を選択します。

図 14 に示すように、[AAA サーバ (AAA Servers)] のオプションが表示されます。

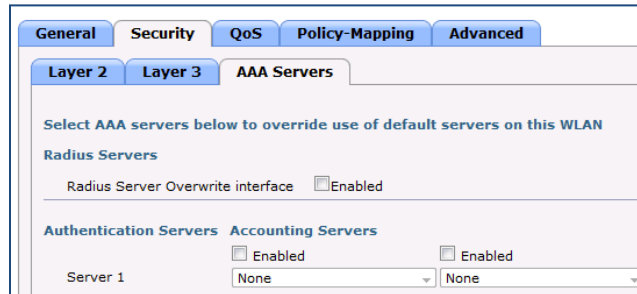


図 14. AAA サーバのセキュリティ

**ステップ 10** 図 15 に示すように、[サーバ 1 (Server 1)] ラベルで、[認証サーバ (Authentication Servers)] と [アカウンティングサーバ (Accounting Servers)] に対して ISE サーバの IP を有効にします。

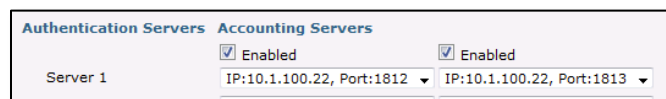


図 15. AAA サーバのセキュリティ

**ステップ 11** [詳細設定 (Advanced)] タブをクリックします。

**ステップ 12** 図 16 に示すように、[詳細設定 (Advanced)] タブ オプションが表示されます。

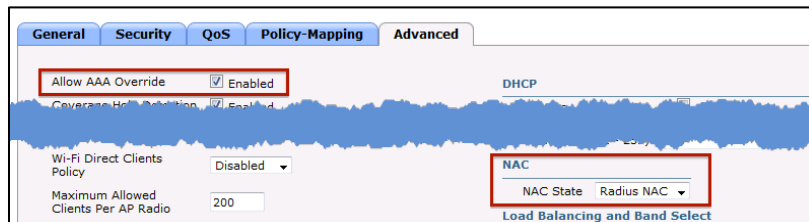


図 16. [詳細設定 (Advanced)] タブ オプション

**ステップ 13** [AAA オーバーライドを許可 (Allow AAA Override)] を有効にします。

**ステップ 14** [NAC の状態 (NAC State)] で、ドロップダウン メニューを使用して [RADIUS NAC] を選択します。

**ステップ 15** [適用 (Apply)] をクリックします。

## ゲストのリダイレクト用の ACL の設定およびアクセスの許可

この項では、WLC で ACL を設定する方法について説明します。目的は、ゲストクライアントがゲスト サービスへアクセスできるように ACL を設定することです。

### ゲスト デバイスを ISE ゲスト ポータルにリダイレクトするための ACL の設定

**ステップ 1** WLC の GUI に移動し、[セキュリティ(Security)] > [アクセスコントロールリスト(Access Control Lists)] > [アクセスコントロールリスト(Access Control Lists)] を選択します。

図 17 に示すように、[アクセスコントロールリスト(Access Control Lists)] ページが表示されます。このページには、WLC で設定されている ACL が一覧表示されます。また、このページでは、任意の ACL を編集または削除できます。

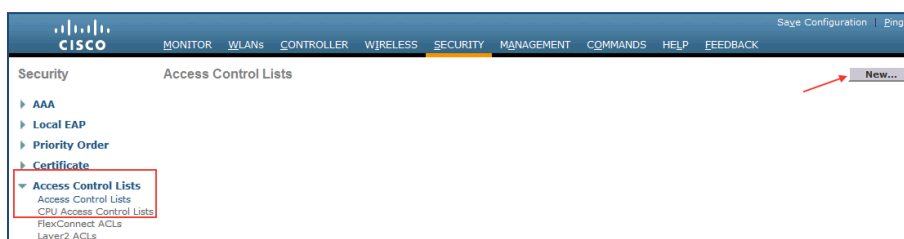


図 17. アクセス コントロール リスト

**ステップ 2** [新規(New)] ボタンをクリックして、新しい ACL を作成します。

**ステップ 3** 図 18 に示すように、名前に **GUESTREDIRECT** と入力します。

**ステップ 4** ACL のルールを作成するには、[編集(Edit)] をクリックします。

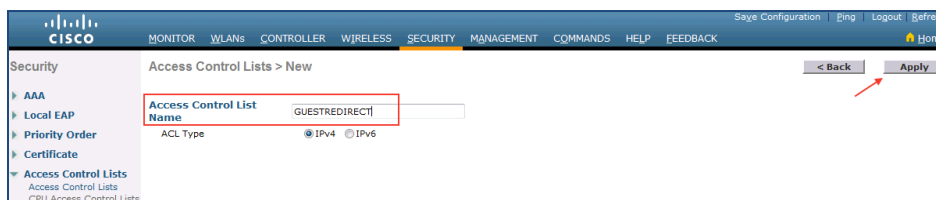


図 18. アクセス コントロール リスト

**ステップ 5** [適用(Apply)] ボタンをクリックします

図 19 に示すように、[アクセスコントロールリスト(Access Control Lists)] の編集ページが表示されます。

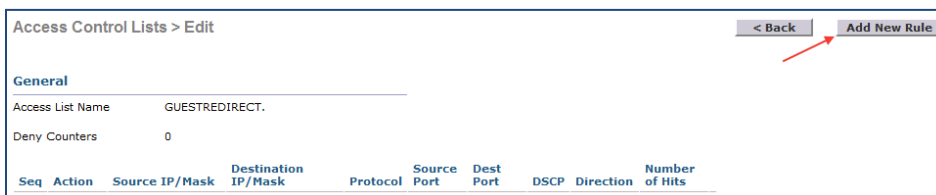


図 19. アクセス コントロール リストの編集ページ

**ステップ 6** [新規ルール of 追加 (Add New Rule)] ボタンをクリックします。

**ステップ 7** [アクセスコントロールリスト (Access Control Lists)] > [ルール (Rules)] ページが表示されます。

**ステップ 8** 図 20 に示すように、ルールを設定します。

**注:** 10.1.100.22 は ISE の IP アドレスです (ご使用の ISE の IP アドレスを使用します)。

General										
Access List Name		GUESTREDIRECT								
Deny Counters		0								
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Outbound	0	
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	0	
3	Permit	0.0.0.0 / 0.0.0.0	10.1.100.22 / 255.255.255.255	Any	Any	Any	Any	Inbound	0	
4	Permit	10.1.100.22 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	0	

図 20. ACL ルールのエントリ

## 認証後にインターネットへのゲスト アクセスを許可するための ACL の設定

**ステップ 1** WLC のウィザードにより、**guest-acl** という名前で ACL が作成されています。

**ステップ 2** [guest-acl] ACL をクリックします。

**ステップ 3** シーケンス 2 の後に、次の 2 つの新規ルールを追加します。この順序に従うことが非常に重要です。

- 送信元 ISE IP へのアクセスで any を許可します。
- 宛先 ISE IP へのアクセスで any を許可します。

図 21 に、シーケンス 2 の後に追加された 2 つの新規ルールを示します。

General										
Access List Name		guest-acl								
Deny Counters		0								
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0	
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0	
3	Permit	0.0.0.0 / 0.0.0.0	10.1.100.22 / 255.255.255.255	Any	Any	Any	Any	Any	0	
4	Permit	10.1.100.22 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0	

図 21. 新規ルールのエントリ

**注:** 10.1.100.22 は ISE サーバの IP アドレスです。新規ルールには、ご使用の ISE IP アドレスを使用します。

これで、Cisco Identity Services Engine と WLC のゲスト サービス プロセスの最初のパート (シスコ ワイヤレス コントローラ (WLC) のインストールおよび設定) は終了です。

## VMware でのインストールおよび設定 (ISE)

ここでは、VMware サーバでの ISE ソフトウェアのインストールおよび設定に関連するタスクについて説明します。

図 7 に、このパートで説明するタスクのワークフローを示します。このワークフローのアクティビティは、ISE を使用したゲストサービスを正常に導入するために必要なタスクを示しています。

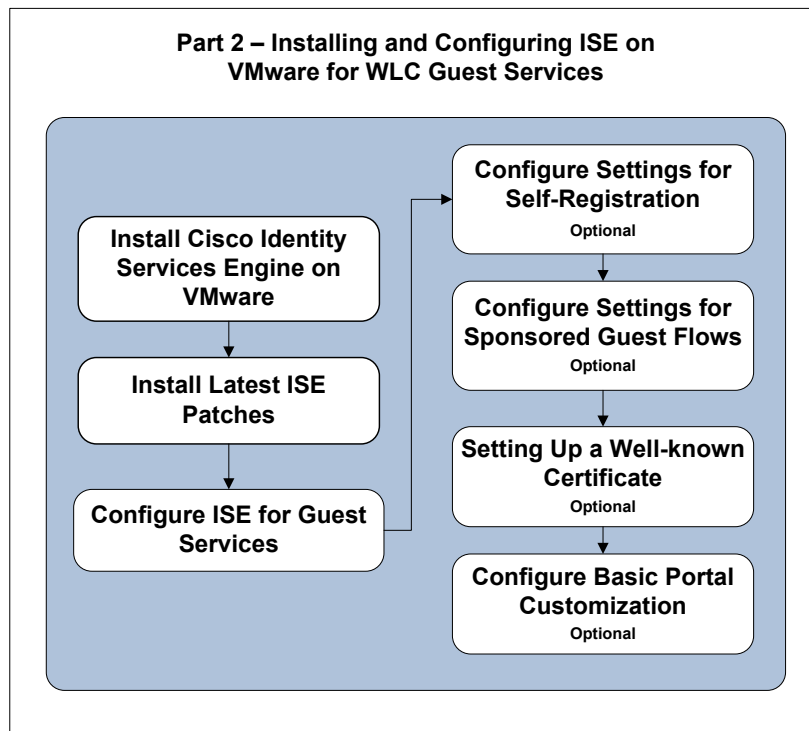


図 22. VMware でのインストールおよび設定 (ISE)

## 仮想マシンへの Cisco ISE のインストール

OVA テンプレートを 사용하여仮想マシンに Cisco ISE ソフトウェアをインストールし、展開することができます。OVA テンプレートは前の手順で Cisco.com からダウンロードしてあります。

### ISE OVA の仮想マシンとしての導入

ESX(i) 5.x を使用して ESX(i) 環境に ISE OVA を導入するには、次の手順に従います。

- ステップ 1** VMware vSphere クライアントを起動します。
- ステップ 2** VMware ホストにログインします。
- ステップ 3** VMware vSphere クライアントから [ファイル (File)] > [OVF テンプレートの導入 (Deploy OVF Template)] を選択します。
- ステップ 4** [Browse] をクリックして OVA テンプレートを選択し、[Next] をクリックします。
- ステップ 5** [OVF Template Details] ページの詳細を確認し、[Next] をクリックします。
- ステップ 6** 一意に識別するために仮想マシンの名前を [Name and Location] ページに入力し、[Next] をクリックします。
- ステップ 7** OVA をホストするデータストアを選択します。
- ステップ 8** [Disk Format] ページの [Thick Provision] オプション ボタンをクリックし、[Next] をクリックします。

Cisco ISE リリース 1.3 は、シック プロビジョニングとシン プロビジョニングの両方をサポートします。ただし、パフォーマンスを高めるためにシック プロビジョニングを選択することをお勧めします。シン プロビジョニングを選択した場合は、最初のディスク拡張中に、より多くのディスク領域が必要なアップグレード、バックアップと復元、デバッグ ロギングなどの操作に影響が出ることがあります。

**注:** [レイジーゼロ (Lazy Zero)] か [イーガーゼロ (Eager Zero)] を選択するよう要求されたら [レイジーゼロ (Lazy Zero)] を選択します。

- ステップ 9** [Ready to Complete] ページの情報を確認します。
- ステップ 10** [導入後に電源をオンにする (Power on after deployment)] チェックボックスをオンにします。
- ステップ 11** [終了 (Finish)] をクリックします。

### ISE のセットアップの実行

この項では、vSphere コンソールのコマンドライン インターフェイス (CLI) を使用して ISE 仮想マシンをセットアップします。インストール プロセスが終了すると、仮想マシンは自動的に再起動されます。仮想マシンが再起動すると、システムプロンプトが表示されます。

- ステップ 1** システム プロンプトで `setup` と入力し、Enter を押します。

セットアップ ウィザードが表示され、ウィザードに従って初期設定を実行します。

- ステップ 2** 本書の事前設定の計画の項で収集した情報を使用して、セットアップ ウィザードの質問に対応します。



下記の例は、**setup** コマンドの出力例を示します。

```
localhost login: setup
Press 'Ctrl-C' to abort setup
Enter hostname[]: ise
Enter IP address[]: 10.1.100.22
Enter IP default netmask[]: 255.255.255.0
Enter IP default gateway[]: 10.1.100.1
Enter default DNS domain[]: yourdomain.com
Enter primary nameserver[]: 172.16.168.183
Add/Edit another nameserver? Y/N : n
Enter primary NTP server[time.nist.gov]:
Add/Edit secondary NTP server? Y/N : n
Enter system timezone[UTC] :
Enter username[admin]:
Enter password:
Enter password again:
Bringing up network interface...
Pinging the gateway...
Pinging the primary nameserver...
Do not use 'Ctrl-C' from this point on...
Appliance is configured
```

インストールに関する情報および詳細については、管理ガイドの「[Installing Cisco ISE Software on a VMware System](#)」の項を参照してください。

## ISE のパッチのインストール

ISE 仮想マシンをセットアップしたら、最新のパッチをインストールする次の指示に従ってシステムにパッチを適用します。

- ステップ 1** ISE の管理 UI (<http://iseapaddress>) にログインします。
- ステップ 2** [管理 (Administration)] > [システム (System)] > [メンテナンス (Maintenance)] > [パッチ管理 (Patch Management)] > [インストール (Install)] の順に選択します。
- ステップ 3** [参照 (Browse)] をクリックし、Cisco.com からダウンロードしたパッチを選択します。
- ステップ 4** [インストール (Install)] をクリックしてパッチをインストールします。

プライマリ管理ノードでのパッチのインストールが完了すると、Cisco ISE から自動的にログアウトされます。再びログインできるようになるまで数分間待つ必要があります。

**注:** パッチ インストールの進行中、[パッチ管理 (Patch Management)] ページ上の機能のうち使用できるのは [ノードステータスを表示 (Show Node Status)] のみです。

- ステップ 5** [パッチのインストール (Patch Installation)] ページに戻るには、[管理 (Administration)] > [システム (System)] > [メンテナンス (Maintenance)] > [パッチ管理 (Patch Management)] の順に移動します。

ISE のパッチの詳細については、『ISE 1.3 Administration Guide』の「[Installing a Software Patch](#)」の項を参照してください。

## ゲスト アクセス用の ISE の設定

### ワイヤレス コントローラ(WLC)のネットワーク アクセス デバイス(NAD)としての設定

**ステップ 1** ISE の管理 UI にログインします。

**ステップ 2** [管理 (Administration)] > [ネットワークリソース (Network Resources)] > [ネットワークデバイス (Network Devices)] に移動します。

**ステップ 3** 図 23 に示すように、[追加 (Add)] を選択します。

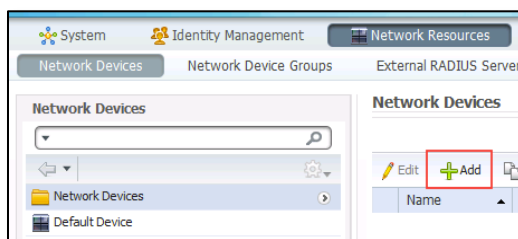


図 23. ISE のネットワークデバイス: デバイスの追加

図 24 に示すように、[ネットワークデバイス (Network Devices)] の編集ページが表示されます。

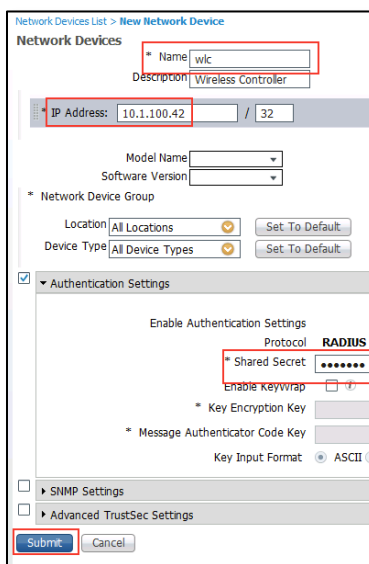


図 24. ネットワーク デバイス

**ステップ 4** デバイス名を入力します。

**ステップ 5** デバイスの IP アドレスを入力します。

**ステップ 6** [認証の設定 (Authentication Settings)] を有効にします。

**ステップ 7** [共有秘密鍵 (Shared Secret)] を入力します (事前チェックリストの項目番号: 12)。

**ステップ 8** [送信 (Submit)] をクリックします。

## 認証ポリシーの設定

認証ポリシーでは、Cisco ISE が通信に使用する、許可されるプロトコルおよび ID ソースまたは ID ソース順序を静的に定義できます。Cisco ISE では、デフォルトで、ゲスト アクセス用の事前構成済みの使用可能な認証ポリシーが用意されています。

### デフォルトの認証ポリシーの表示

事前定義済みのデフォルトの認証ポリシーを表示するには、次の手順に従います。

**ステップ 1** ISE の管理 UI にログインします。

**ステップ 2** [ポリシー (Policy)] > [認証 (Authentication)] に移動します。

図 25 に示すように、[デフォルトの認証ポリシー (Default Authentication Policy)] ページが表示されます。

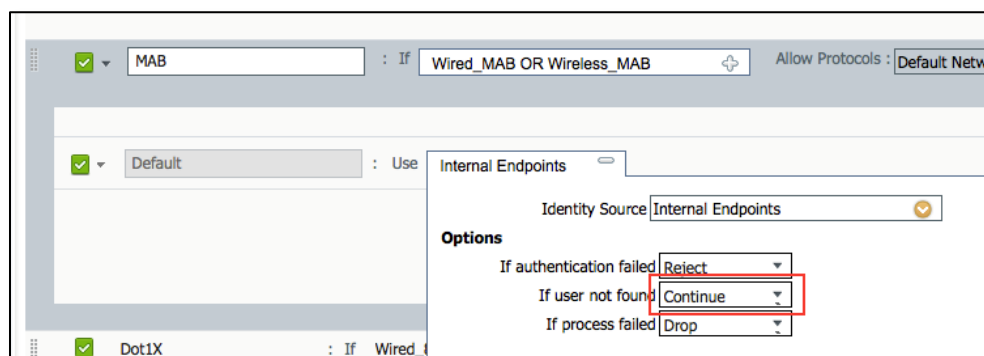


図 25. デフォルトの認証ポリシー

デフォルトの認証ポリシーでは、未知の内部エンドポイントの **MAB** は [続行 (Continue)] に設定されています。これにより、(未知)のゲスト エンドポイントが認証を続行でき、このエンドポイントのゲスト ポータルへのリダイレクトが許可されます。

## ゲスト エンドポイントを ISE へリダイレクトする認証プロファイルの作成

エンドポイントがネットワークに初めてアクセスする場合、エンドポイントを認証のためにゲスト ポータルへリダイレクトする必要があります。リダイレクトするには認証プロファイルが必要です。

**ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] に移動します。

**ステップ 2** [認証 (Authorization)] を展開し、[認証プロファイル (Authorization Profiles)] をクリックします。

**ステップ 3** [追加 (Add)] をクリックします。

**ステップ 4** 次の情報を入力します。

- [名前 (Name)]: Guest Redirect
- [Web リダイレクト (Web Redirection)] をオンにし、**リダイレクトの種類**を選択: [ホットスポット (Hotspot)] または [集中型 Web 認証 (Centralized Web Authentication)] (自己登録またはスポンサー ゲストのフローで使用)。

- [ACL]:この ACL は大文字と小文字を区別し、WLC で設定された名前と一致する必要があります。「ゲストのリダイレクト用の ACL の設定およびアクセスの許可」の項での設定に従い、GUESTREDIRECT を使用します。
- 値:適切なデフォルト ポータル([ホットスポット (Hotspot)], [自己登録 (Self-Registration)], または [スポンサー (Sponsored)]) を選択します。

**ステップ 5** [送信 (Submit)] をクリックします。

## リダイレクト用のホットスポット プロファイルの例

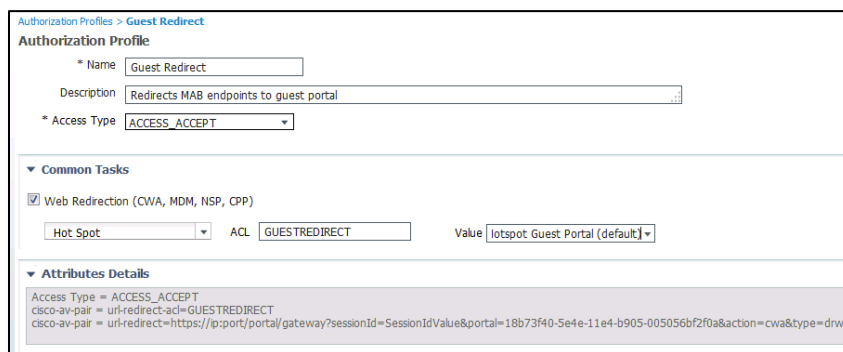


図 26. 認証プロファイル:リダイレクト用のホットスポット プロファイル

## クレデンシャルを持つリダイレクトの例

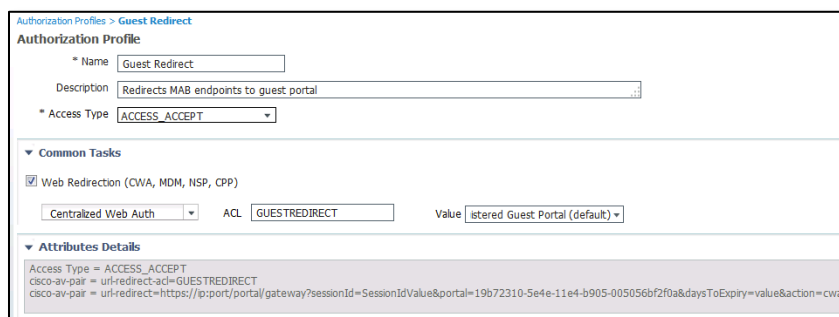


図 27. 認証プロファイル:クレデンシャルを持つリダイレクト

## アクセスを認可するための認証プロファイルの作成

この項では、ユーザ/デバイスが認証された後にネットワークにアクセスできるように、新規認証プロファイルを作成します。

アクセスを認可するための認証プロファイルを作成するには、次の手順に従います。

- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] に移動します。
- ステップ 2** [認証 (Authorization)] を展開し、[認証プロファイル (Authorization Profiles)] をクリックします。
- ステップ 3** [追加 (Add)] をクリックします。

図 28 に示すように、[新規の認証プロファイル (New Authorization Profile)] 画面が表示されます。

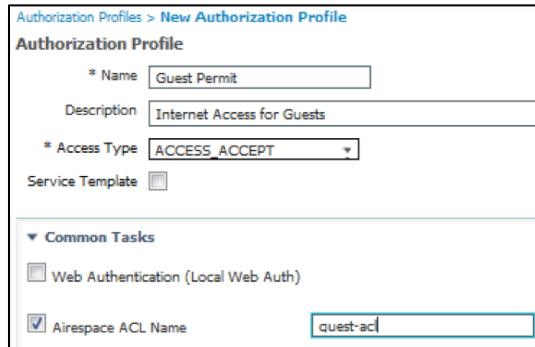


図 28. 新規の認証プロファイル

**ステップ 4** 図に示すように、次の情報を入力します。

- [名前 (Name)]: Guest Permit
- [説明 (Description)]: ゲスト用インターネット アクセス
- [Airespace ACL 名 (Airespace ACL Name)] をオンにし、guest-acl と入力

**注:** この ACL は大文字と小文字を区別し、WLC での定義に正確に一致する必要があります。この ACL は、「ゲストのリダイレクト用の ACL の設定およびアクセスの許可」の項ですでに作成済みです。

**ステップ 5** [送信 (Submit)] をクリックします。

## ゲスト アクセス用の認証ポリシーの作成

ゲスト ポータルへリダイレクトさせるために必要な認証ルールを作成します。認証ルールを作成することにより、デバイスまたはユーザは認証されると、エンドポイントのグループに応じて簡単にアクセスできるようになります。

**ステップ 1** [ポリシー (Policy)] > [認証 (Authorization)] に移動します。

**ステップ 2** [デフォルト (Default)] ルール行の [編集 (Edit)] の横にある矢印をクリックします。

**ステップ 3** 新規ルールをその上に挿入します。

**ステップ 4** 図 29 に示すように、これまでの設定に合う 2 つの新規ルールを追加します。

<input checked="" type="checkbox"/>	Guest Permit	if GuestEndpoints AND Wireless_MAB	then Guest_Permit	Edit   ▼
<input checked="" type="checkbox"/>	Guest Redirect	if Wireless_MAB	then Guest Redirect	Edit   ▼
<input checked="" type="checkbox"/>	Default	if no matches, then	DenyAccess	Edit   ▼

図 29. 認証ポリシー: 新規ルールの追加

**ステップ 5** 最初のリダイレクト ルールを作成します。

**ステップ 6** ルールの名前: **Guest Redirect**

**ステップ 7** Wireless\_MAB の場合、[Condition (条件)] > [Compound Condition (複合条件)] を選択します。

**ステップ 8** 認証プロファイル [標準 (Standard)] > [Guest Redirect] を選択します。

**ステップ 9** [完了 (Done)] をクリックします。

**ステップ 10** 別のルールを **Guest Permit** ルールの上に挿入します。

**ステップ 11** ルールの名前: **Guest Permit**

**ステップ 12** GuestEndpoint かつ Wireless\_MAB の場合に選択します。

**ステップ 13** [Guest Permit] プロファイルを選択します。

**ステップ 14** [完了 (Done)] をクリックします。

**ステップ 15** [保存 (Save)] をクリックします。

ユーザが、AUP(ホットスポット)に同意するかクレデンシャル ポータルにログインすると、任意のポータル タイプの設定フローがページに表示されます。AUP がいずれかのフローで同意されると、デバイスが **GuestEndpoints** に登録され、他にリダイレクトされることなくアクセスが 30 日間許可されます。30 日後、デバイスは **GuestEndpoints** グループから消去され、このフローが繰り返されます。

この完了した手順は、ポータルが稼働するのに必須の手順です。

ゲスト アクセスにホットスポット ポータルを使用している場合は、「**既知の証明書の設定**」の項までスキップできます。

自己登録またはスポンサー ポータルを使用している場合は、さらに設定が必要です。次の項「**自己登録およびスポンサーゲストのフローに必要な設定**」に進んでください。

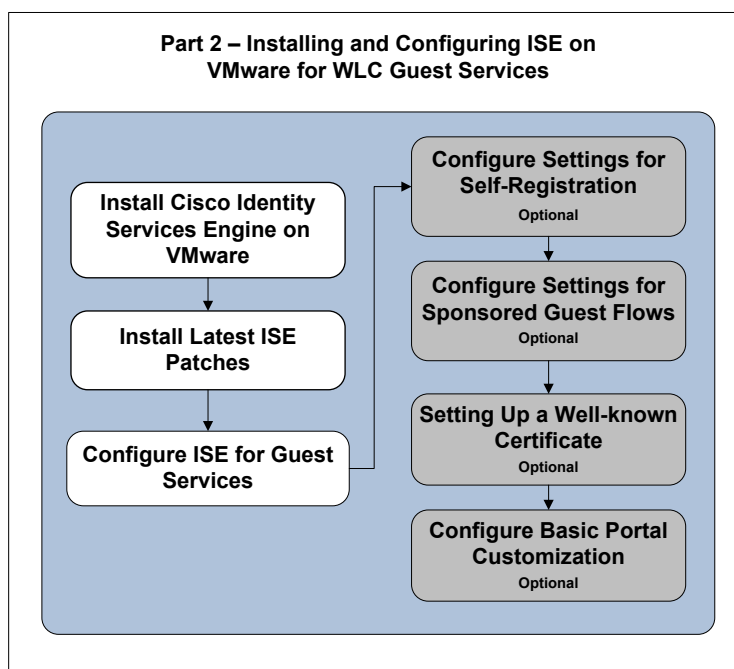


図 30. パート 2: WLC ゲスト サービス用の VMware での ISE のインストールおよび設定

# 自己登録およびスポンサー ゲストのフローに必要な最小限の設定(任意)

## ゲストのロケーションとタイムゾーンの設定

これらの設定は、自己登録およびスポンサー ゲストのフローをサポートするのに必要です。ゲストがネットワークにアクセスするロケーションを設定して、アカウントが有効化された際にスポンサーがタイムゾーンを簡単に選択できるようにすることが必要です。ロケーションを設定しない場合、アカウントが正しい時刻に有効化されません。

ポータルおよびスポンサー グループでロケーションが 1 つだけ使用されるように設定されている場合、利便性のために、ゲストおよびスポンサーにロケーションを選択するためのオプションは表示されません。

PST 時間での導入の場合は、システムに組み込まれているサンノゼのロケーションを使用できるため、「スポンサー ゲストのフローに必要な設定」の項までスキップしてください。

デフォルトのサンノゼ ロケーションの名前は変更できません。このロケーションは、使用するよう選択しなければ表示されないため、削除する必要はありません。

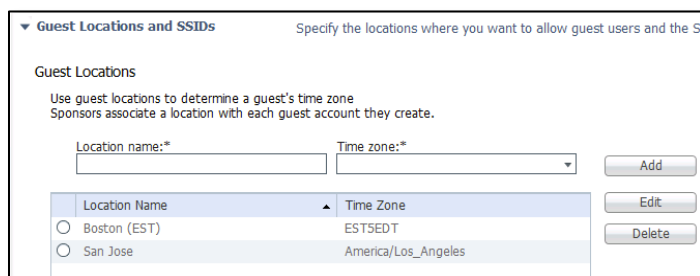
ロケーションおよび SSID の詳細については、[こちら](#)をクリックして、本ガイドの対応する項にアクセスしてください。

ゲストのロケーションとタイムゾーンを設定するには、次の手順に従います。

**ステップ 1** [ゲストアクセス (Guest Access)] > [設定 (Settings)] に移動します。

**ステップ 2** [ゲストのロケーションと SSID (Guest Locations and SSIDs)] を展開します。

**ステップ 3** 図 31 に示すように、[ゲストのロケーションと SSID (Guest Locations and SSIDs)] ページが表示されます。



Location Name	Time Zone
<input type="radio"/> Boston (EST)	EST5EDT
<input type="radio"/> San Jose	America/Los_Angeles

図 31.

**ステップ 4** ロケーション名およびタイムゾーンを入力します。例: ボストン (EST) で EST5EDT を使用。

**注:** サンノゼのロケーションはそのままにしておきます。

**ステップ 5** [追加 (Add)] をクリックします。

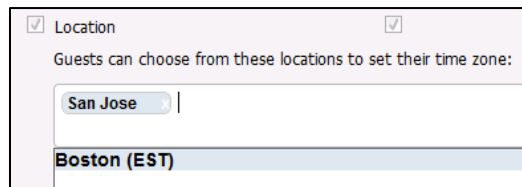
**ステップ 6** [保存 (Save)] をクリックします。

## 該当のロケーションを使用するようにポータルを設定

この新しく追加されたロケーションを使用するには、ポータルを設定する必要があります。

**注:** デフォルトのサンノゼ (PST 時間) を使用すればよい場合は、この項はスキップしてください。

- ステップ 1** [ゲストアクセス (Guest Access)] > [設定 (Configure)] > [ゲストポータル (Guest Portals)] に移動します。
- ステップ 2** 使用しているポータルを選択します (自己登録またはスポンサー ゲスト ポータル)。
- ステップ 3** [ポータルの設定およびログインページの設定 (Portal Settings and Login page settings)] を折りたたみます。
- ステップ 4** 図 32 に示すように、ページ設定の [ロケーション (Location)] に、作成したロケーションが追加されます。
- ステップ 5** [追加 (Add)] をクリックします。
- ステップ 6** [送信 (Submit)] をクリックします。



Location

Guests can choose from these locations to set their time zone:

San Jose

Boston (EST)

図 32. ゲストポータル:ロケーション



## スポンサー ゲストのフローに必要な設定(任意)

スポンサー ゲストをサポートするには、次の手順が必要です。自己登録のみを使用する場合は設定が完了しているため、このプロセスをスキップして、「**既知の証明書の設定**」の項に移動してください。

### スポンサー グループを設定します

内部アカウントを作成するか、ISE を Active Directory と統合することにより、スポンサーを設定します。Active Directory と統合している場合は、「**Active Directory のスポンサー アカウントの使用**」の項までスキップしてください。

内部アカウントを作成するには、次の手順に従います。

- ステップ 1** [管理 (Administration)] > [ID の管理 (Identity Management)] > [ID (Identities)] > [ユーザ (Users)] の順に移動します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** [スポンサー (Sponsor)] の情報を入力します。
- ステップ 4** [ユーザグループ (User Groups)] で [すべてのアカウント (ALL\_ACCOUNTS)] (デフォルト) を選択します。
- ステップ 5** [送信 (Submit)] をクリックします。
- ステップ 6** 「**スポンサー グループのロケーションの設定**」にスキップします。

### Active Directory のスポンサー アカウントの使用

次の 2 つの項は、ご使用のゲストアクセスシステムが、スポンサー グループが存在する Active Directory サーバと統合されている場合だけ必要です。ISE で作成したスポンサー アカウント(前の項で作成)を使用する予定であり、かつ、それらのアカウントを AD と統合しない場合は、この後の「**スポンサー グループのロケーションの設定**」までスキップできます。

詳細については、『ISE Configuration Guide』の「[Active Directory as an External Identity Source](#)」を参照してください。

Active Directory からスポンサー アカウントを作成するには、次の手順に従います。

- ステップ 1** [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] に移動します。
- ステップ 2** [Active Directory] を選択します。
- ステップ 3** 図 33 に示すように、[追加 (Add)] をクリックします。

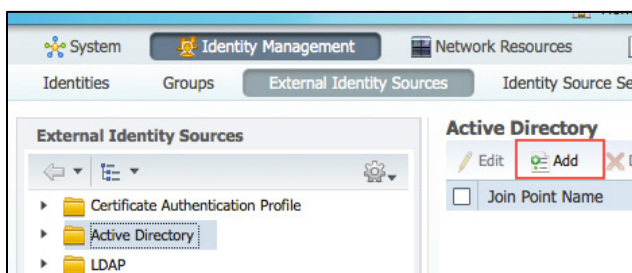


図 33. ID の管理: 外部 ID ソース

- ステップ 4** 接続ポイントの名前を入力します。

**ステップ 5** ADドメインを入力します。

**ステップ 6** [送信 (Submit)] をクリックします。

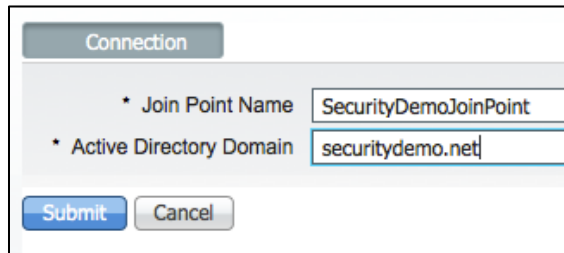


図 34. Active Directory

**ステップ 7** [グループ (Groups)] タブをクリックします。

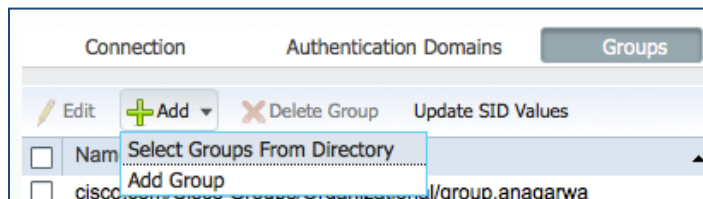


図 35. [グループ (Groups)] タブ

**ステップ 8** [追加 (Add)] をクリックし、[ディレクトリのグループを選択 (Select Groups from Directory)] を選択します。

**ステップ 9** グループを選択したら、ページ下部の [OK] をクリックします。

**ステップ 10** ページ下部の [保存 (Save)] をクリックします。

## Active Directory スポンサー グループ All\_Accounts の設定

次の手順は、スポンサーまたは従業員を含むグループを、スポンサー グループに関連付ける方法を示します。この例では、ドメイン ユーザを使用します。

**ステップ 1** [ゲストアクセス (Guest Access)] > [設定 (Configure)] に移動します。

**ステップ 2** [スポンサーグループ (Sponsor Groups)] > [ALL\_ACCOUNTS] をクリックします。

図 36 に示すように、[スポンサーグループ (Sponsor Group)] ページが表示されます。

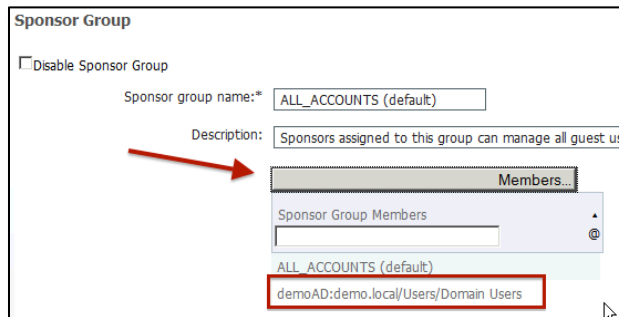


図 36. [スポンサーグループ (Sponsor Group)] ページ

**ステップ 3** [メンバー (Member)] をクリックし、図 37 に示すように、[選択されたユーザグループ (Selected User Groups)] 領域にドメイン ユーザを移動します。

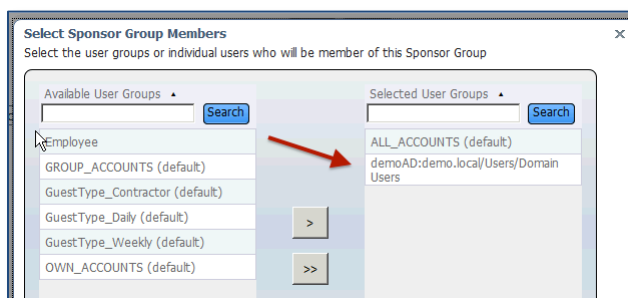


図 37. 選択されたユーザグループ

**ステップ 4** [OK] をクリックします。

## スポンサーグループのロケーションの設定

スポンサーがゲストアカウントを作成する際に、使用する正しい場所を設定することが重要です。サンノゼのロケーションを使用すればよい場合は、この項をスキップできます。それ以外の場合は、新規ロケーションを追加します。

**ステップ 1** 図 38 に示すように、スポンサーが使用するロケーションを、[ゲストがアクセスするロケーションを選択 (Select the locations that guests will be visiting)] セクションから選択します。

**ステップ 2** 必要のないロケーションを削除します。

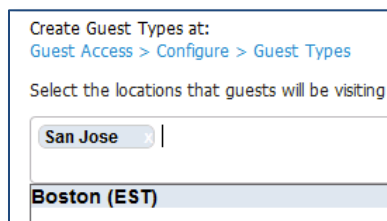


図 38. [ゲストがアクセスするロケーションを選択 (Select the locations that guests will be visiting)] ペイン

**ステップ 3** ページの最上部までスクロールし、[保存 (Save)] をクリックします。

**ステップ 4** [閉じる (Close)] をクリックします。

## ISE スポンサー ポータルの FQDN ベースのアクセスの設定

スポンサー ポータルを使用すると、スポンサーは、ゲスト、訪問者、契約者、コンサルタント、またはお客様が HTTP または HTTPS ログインを実行してネットワークにアクセスできるように、一時的なアカウントを作成できます。ネットワークは企業ネットワークでも、またはインターネットにアクセスしてもかまいません。

特別な設定をせずに ISE 管理 UI からスポンサー ポータルにアクセスする方法が 2 通りあります。

- [アカウントの管理(Manage Accounts)] ボタン:これは管理者用です。
- ポータル テスト URL:この URL はスポンサーに送信できるので、スポンサーが簡単にサイトをブックマークできます:(デフォルト)

スポンサーに簡単なスポンサー ポータルの URL を提供することをお勧めします。例:

<http://sponsorportal.yourcompany.com>

ISE スポンサー ポータルをセットアップするには、次の手順に従います。

**ステップ 1** [ゲストアクセス(Guest Access)] > [設定(Configure)] > [スポンサーポータル(Sponsor Portals)] に移動します。

**ステップ 2** [デフォルトのスポンサーポータル(default Sponsor portal)] をクリックすると、図 39 に示すように、[ポータル設定(Portal Settings)] ペインが表示されます。

**ステップ 3** [ポータル設定(Portal Settings)] で、[完全修飾ドメイン名(FQDN) (Fully Qualified Domain Name (FQDN))] セクションを見つけて、「sponsorportal.yourcompany.com」と入力します。

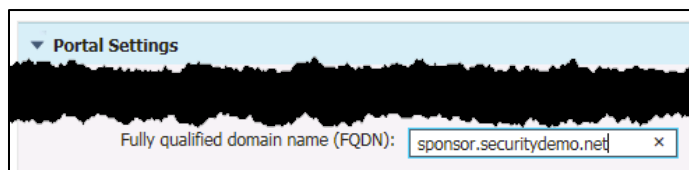


図 39. ポータル設定(Portal Settings)

**ステップ 4** 最上部までスクロールし、[保存(Save)] をクリックします。

この FQDN が確実に ISE IP アドレスに解決されるように、DNS を更新する必要があります。これは、sponsorportal.yourcompany.com が yourise.yourcompany.com をポイントする CNAME エイリアスを使用することで実現できる場合があります。

詳細については、『ISE 1.3 Portal User Guide』の「[Support Guest](#)」の項を参照してください。

## 既知の証明書の設定(任意)

この項の情報は、ISE 1.3 を使用して作成されました。既知の証明書の設定に関するリリース 1.4 ワークフローは少し異なる可能性があります。

この項では、ゲスト アクセス用のシステムを稼働させる必要はありません。この手順は任意ですが、実施することを強くお勧めします。ユーザが Web ブラウザから、ゲスト、スポンサー、または管理者ポータルに接続した場合に、無効な証明書を受け入れる必要がないようにするには、既知の認証局によって署名された ISE サーバ用の証明書を使用する必要があります。

現時点ではこの項をスキップする場合、最低限の設定については完了しているため、「次のステップ」の項に進むことができます。

このガイドで推奨されるタイプの証明書を完全にサポートするベンダーとしては SSL.com がありますが、他にも利用できるベンダーがあります。

**注:** 証明書のタイプは、証明書プロバイダーによって異なる名前で呼ばれる場合があります。SAN フィールドに何が必要かは、多くの場合、該当の会社に問い合わせるか、それらの会社のオンライン Web チャットを使用すれば確認できます。その際、CN= フィールドは FQDN で、SAN フィールドにはワイルドカードと FQDN の両方を含む証明書を必要としていると伝えます。

ワイルドカード証明書および証明書全般の詳細については、次のマニュアルを参照してください。

- 『ISE Administrator Guide』: [「Wildcard Certificate Support in Cisco ISE」](#)
- Moving Packets の記事: [「When SSL Certificates Go Wild」](#)
- Aaron Woland の Network World ブログ: [「Wildcard certificates and how to use with ISE」](#)

次のプロセスで取り上げる手順は、SAN でワイルドカードが使用されている、SSL.com (Comodo の下位) のユニファイドコミュニケーション証明書(UCC)の設定例を示しています。

## 証明書署名要求の作成と認証局への CSR の送信

**ステップ 1** [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書署名要求 (Certificate Signing Requests)] の順に移動します。

**ステップ 2** 図 40 に示すように、CSR を生成するための値を入力します。

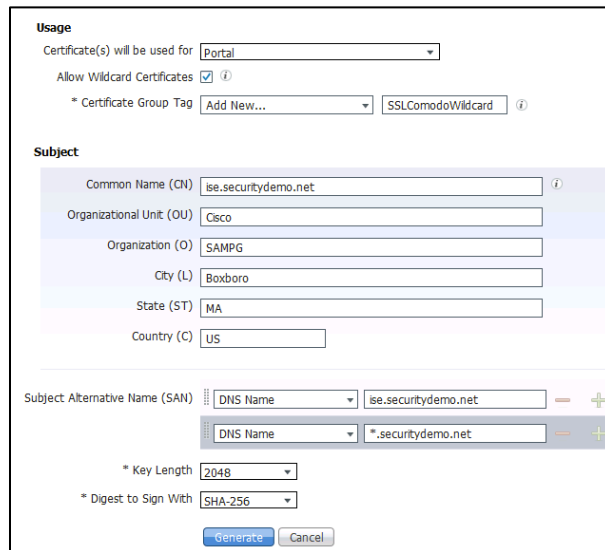


図 40. 証明書署名要求

### 使用方法

- [証明書の用途 (Certificate(s) will be used for)]: ポータル (Portal)
- [ワイルドカードの証明書を許可 (Allow Wildcard Certificates)]: オン
- [証明書グループタグ (Certificate Group Tag)]: [新規追加 (Add New)]: 名前を指定: 例、SSLComodoWildcard

### Subject

- [共通名 (Common name)]: yourdomain.com
- サブジェクトの他のセクションを、ユーザの組織に応じた情報に置き換えます。
- [サブジェクトの代替名 (SAN) (Subject Alternative Name (SAN))]=  
SAN DNS 名 1 = yourise.yourcompany.com  
SAN DNS 名 2 = \*.yourcompany.com
- 最後の 2 つのフィールドはデフォルトのままにします。

**ステップ 3** [Generate (生成)] をクリックして CSR を生成します。図 41 に示すように、CSR が生成されます。

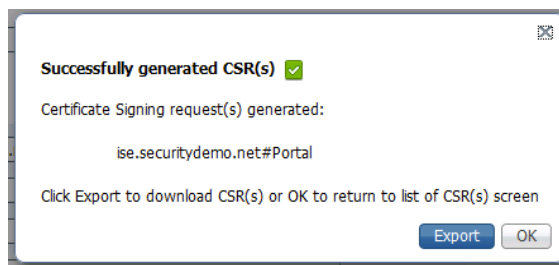


図 41. 正常に生成された CSR

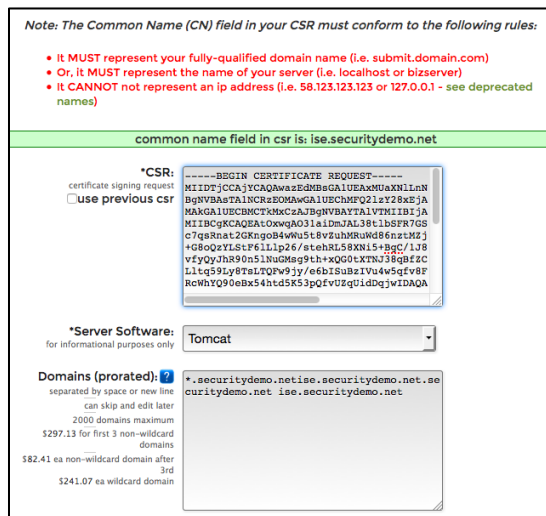
**ステップ 4** [エクスポート (Export)] をクリックしてファイルを保存します。

**ステップ 5** テキスト エディタでこのファイルを開きます。

**ステップ 6** 「----- BEGIN CERTIFICATE REQUEST-----」から「-----END CERTIFICATE REQUEST-----」までのすべてのテキストをコピーします。

**ステップ 7** 選択した CA の証明書要求に、この CSR の内容を貼ってください。

図 41 は、SSL.com のポータルを示します。



Note: The Common Name (CN) field in your CSR must conform to the following rules:

- It MUST represent your fully-qualified domain name (i.e. submit.domain.com)
- Or, it MUST represent the name of your server (i.e. localhost or bizserver)
- It CANNOT represent an ip address (i.e. 56.123.123.123 or 127.0.0.1 - see deprecated names)

common name field in csr is: ise.securitydemo.net

\*CSR:  
 use previous csr  
 -----BEGIN CERTIFICATE REQUEST-----  
 MIIDTjCCAjYCAQAwazEOMBcGA1UEAxM1LnN  
 BpVYBwTALINCRzEOMBcGA1UEChMQ21yZ2E5JA  
 NkKGA1UECMCTMkKCAzAjBgNVBAYTAlVTMIBIjA  
 MIIBCgKCAQEAtOxwqA031eIdmJAL38t1bSFR7GS  
 c7qsRnat2GKngob4wWu5t8vZuhMRuWd86ztMZj  
 +G8oQzYLSrF611p26/istehh2:59XN15+8gC/1J8  
 vfyQyJhR9On51NuGmsq9th+XQG0+XTN338qBf2C  
 Lltq59Ly8TatLQFw9jy/e6b1SuBzTVu4w5qfv8F  
 RcWhY090eBx54htd5K53pQfvUZq1dDqjwIDAQA

\*Server Software:  
 for informational purposes only  
 Tomcat

Domains (prorated):  
 separated by space or new line  
 can skip and edit later  
 2000 domains maximum  
 \$297.13 for first 3 non-wildcard  
 domains  
 \$82.41 ea non-wildcard domain after  
 3rd  
 \$241.07 ea wildcard domain

\*.securitydemo.net ise.securitydemo.net.se  
 curitydemo.net ise.securitydemo.net

図 42. SSL.com のポータル

**ステップ 8** 署名済みの証明書をダウンロードします。

**注:** CA によっては、署名付き証明書が電子メールで送信される場合があります。ダウンロードされたファイルまたは電子メールの添付ファイルの多くは zip ファイル形式で、新規に署名された証明書と CA のパブリック署名証明書が含まれています。これらの証明書は Cisco ISE の信頼された証明書ストアに追加する必要があります。デジタル署名証明書、ルート CA 証明書、および他の中間 CA 証明書(該当する場合)を、クライアントブラウザを開いているローカルシステムに保存します。これらの証明書は次の項でインポートします。

## 信頼された証明書ストアへの証明書のインポート

この項では、クライアントとサーバ間の通信が信頼されるために必要な証明書をインポートします。ISE は通信時、クライアントに対してサーバ証明書とともにルート証明書および中間証明書(必要に応じて)を提示します。

**注:** すべてのプロバイダーで中間証明書のインストールが必要なわけではありません。中間証明書は下位 CA から提供されます。たとえば SSL.com を使用する場合、SSL.com は Comodo の下位 CA になります。Comodo は AddTrust ルート CA の下位 CA です。したがって、この例では、ルート証明書に加えて、この 2 つの下位 CA の証明書もインポートします。

この 3 つの証明書をすべてインポートするには、次の手順に従います。

**ステップ 1** [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [信頼された証明書 (Trusted Certificates)] の順に移動します。

**ステップ 2** [インポート (Import)] をクリックします。

- ルート CA: AddTrustExternalCARoot.crt
- 下位 CA: SSLcomDVCA\_2.crt
- 下位 CA: USERTrustRSAAddTrustCA.crt



**ステップ 3** 図 43 に示すように、[証明書ストアに新規証明書をインポート (Import a new Certificate into the Certificate Store)] ペインが表示されます。

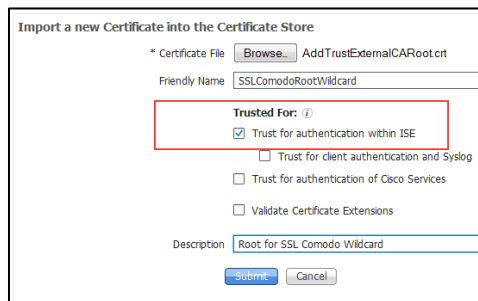


図 43. [証明書ストアに新規証明書をインポート (Import a new Certificate into the Certificate Store)] ペイン

**ステップ 4** 以下の証明書をインポートするには、次の手順 (4 ~ 9) に従います。

- ルート CA: AddTrustExternalCARoot.crt
- 下位 CA: SSLcomDVCA\_2.crt
- 下位 CA: USERTrustRSAAddTrustCA.crt

**ステップ 5** [参照 (Browse)] をクリックして、ルート CA 証明書を選択します。

**ステップ 6** わかりやすい名前を入力します。

**ステップ 7** CA によって返されたルート証明書を選択します。

**ステップ 8** [信頼の目的 (Trusted for)] ラベルの下の [ISE での認証のために信頼する (Trust for Authentication within ISE)] をクリックします。

**ステップ 9** 説明を入力します。

**ステップ 10** [送信 (Submit)] をクリックします。

## 署名要求への CA 署名付き証明書のバインド

これで、CA から返されたデジタル署名付き証明書を受け取り、CA 証明書のインポートが完了しました。次の手順は、CA が署名した証明書を ISE からの CSR にバインドすることです。バインドすることで、CSR の生成に使用された証明書と秘密鍵とのペアが作成されます。

**ステップ 1** [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書署名要求 (Certificate Signing Requests)] の順に移動します。

**ステップ 2** 署名要求のエントリを選択します。

**ステップ 3** 図 44 に示すように、[証明書のバインド (Bind Certificate)] をクリックします。

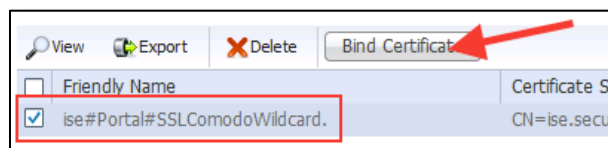


図 44. 証明書のバインド



- ステップ 4** [参照 (Browse)] をクリックし、CA 署名付き証明書を選択します。
- ステップ 5** 証明書のフレンドリ名を指定します。
- ステップ 6** サブジェクトの CN またはサブジェクト代替名の DNS 名にワイルドカード文字のアスタリスク (\*) を含む証明書をバインドするには、[ワイルドカード証明書の許可 (Allow Wildcard Certificates)] チェックボックスをオンにします。
- ステップ 7** その他のオプションは自動的に設定されます。
- ステップ 8** 図 45 に示すように [送信 (Submit)] をクリックして、CA 署名付き証明書をバインドします。

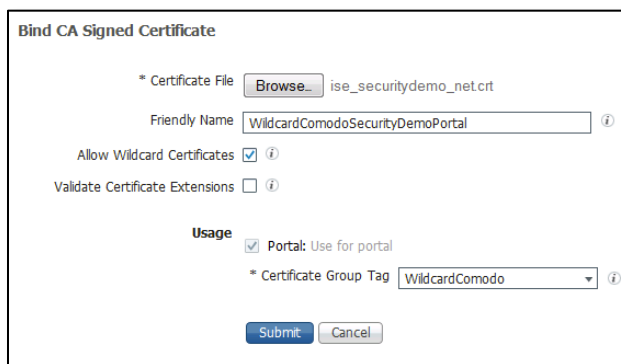


図 45. 署名付き証明書のバインド

## 管理ポータルおよび EAP 認証で使用する証明書の編集

この手順は任意です。ユーザ エクスペリエンスを高めるため (ユーザに対して自己署名証明書のインストールや信頼が要求されなくなります) や、将来の dot1x クライアントへの拡張のために、ISE の管理ポータルにアクセスする際にも既知の証明書を使用する場合は、次の手順に従います。バインド操作を実行した後、証明書を再度編集して、使用方法を更新する必要があります。

管理ポータルおよび EAP 認証で使用する証明書を編集するには次の手順に従います。

- 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)] の順に移動します。
- ステップ 2** 図 46 に示すように、新規にインポートした証明書の SSLComodoWizard を編集します。

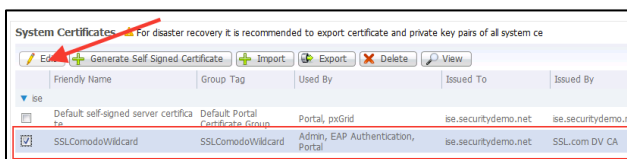


図 46. [システム証明書 (System Certificates)] ペイン

- ステップ 3** 図 47 に示すように [EAP の認証および管理 (EAP Authentication and Admin)] のボックスをオンにして、使用方法のオプションを編集します。

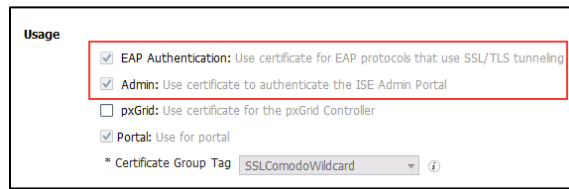


図 47. [使用方法 (Usage)] ペイン

**ステップ 4** [送信 (Submit)] をクリックします。

ISE システムが再起動します。

ISE での既知の証明書の設定が完了しました。

証明書の設定の詳細については、『ISE 1.3 Administration Guide』の「[Managing Certificates](#)」の項を参照してください。

## ポータルで既知の証明書を使用するための設定

既知の証明書の設定が終了したので、その証明書をゲスト ポータルに割り当てて、ゲスト デバイスと通信するときに使用されるようにする必要があります。この変更は、設定した他のすべてのポータルに影響します。スポンサー ポータルを使用している場合このアクションによりスポンサー ポータルも更新されるため、スポンサー ポータルを更新する必要はありません。

**ステップ 5** ISE の管理ポータルにログインします。

**ステップ 6** [ゲストアクセス (Guest Access)] > [設定 (Configure)] > [ゲストポータル (Guest Portals)] に移動します。

**ステップ 7** 使用するデフォルトのゲスト ポータル ([ホットスポット (Hotspot)], [自己登録 (Self-Registered)], または [スポンサー (Sponsored)]) をクリックします。

**ステップ 8** 図 48 に示すように、既知の証明書についての設定手順で設定した [証明書グループタグ (Certificate group tag)] を [ポータル設定 (Portal Settings)] ペインのドロップダウン メニューから選択します。

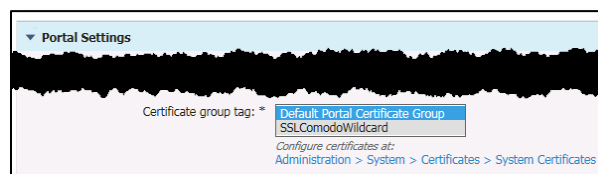


図 48. [ポータル設定 (Portal Settings)] ペイン

**ステップ 9** ページの最上部までスクロールし、[保存 (Save)] をクリックします。

**ステップ 10** 「同じポートのすべてのポータルの証明書を変更しますか。(Do you want to change the certificate for all the portals on the same port?)」と表示されたら、[OK] を押して続行します。

**ステップ 11** ページ最上部にある [閉じる (Close)] をクリックします。

## ポータルの基本的なカスタマイズの設定(任意)

この項では、ゲスト アクセス用のシステムを稼働させる必要はありません。これは、新規ゲスト ポータルの基本的なカスタマイズ オプションに関する理解を深めるための任意の手順です。

ゲスト ポータルをカスタマイズするには、次の手順に従います。

- ステップ 1** [ゲストアクセス (Guest Access)] → [設定 (Configure)] → [ゲストポータル (Guest Portals)] をクリックします。  
**ステップ 2** 使用しているポータル ([ホットスポット (Hotspot)], [自己登録 (Self-Registered)], または [スポンサー (Sponsored)]) をクリックし、そのポータルを編集します。

図 49 に示すように、アクティブなポータルには緑の円に囲まれたチェックが表示されます。

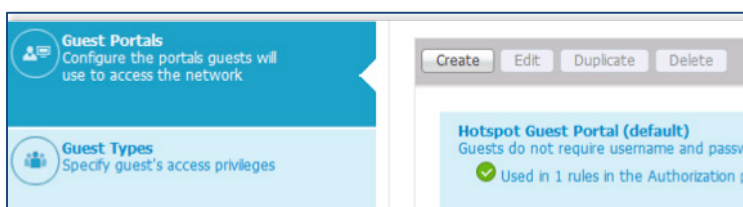


図 49. ホットスポット ゲスト ポータル

- ステップ 3** 図 50 に示すように、ページ最上部にある [ページのカスタマイズ (Page Customization)] セクションをクリックします。

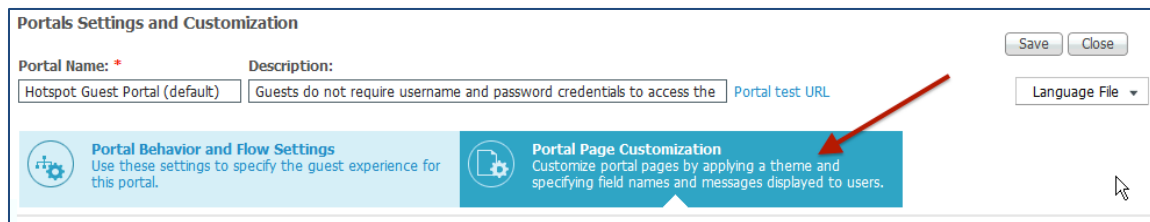


図 50. [ポータルの設定およびカスタマイズ (Portals Settings and Customization)] ページ

ISE 1.3 では、実施した基本的なカスタマイズが製品にすぐに反映されます。そのため変更の内容をリアルタイムで簡単に確認できます。カスタマイズに関する詳細はここでは記載ませんが、まずはページの最上部にあるロゴ、バナー、主要なテキスト要素などが変更できることをご確認ください。複数用意されている組み込みのテーマ カラーを選択することもできます。

- ステップ 4** ポータルのテーマ カラーを変更するには、組み込みのポータルのテーマを使用するか、図 51 に示すように [調整 (Tweaks)] を使用して色を変更します。

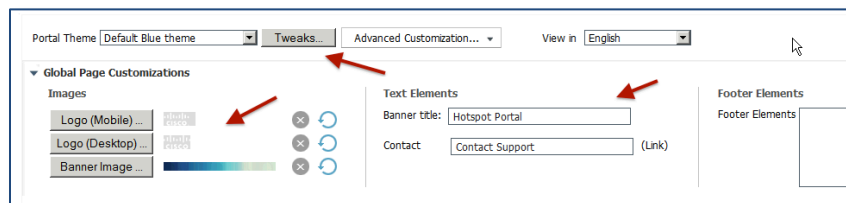


図 51. ページのカスタマイズ オプション

**ステップ 5** ポータルで使用するロゴやバナーをアップロードできます。

このメイン セクションの下では全体的なルックアンドフィールを調整できます。また、各ページに移動することもできます。ページの左側に表示されるオプションは、ポータルの設定とポータルのタイプに応じて異なります。ページのさまざまな領域のテキストを調整できます。

ポータルへの変更を表示するミニプレビューもあります。

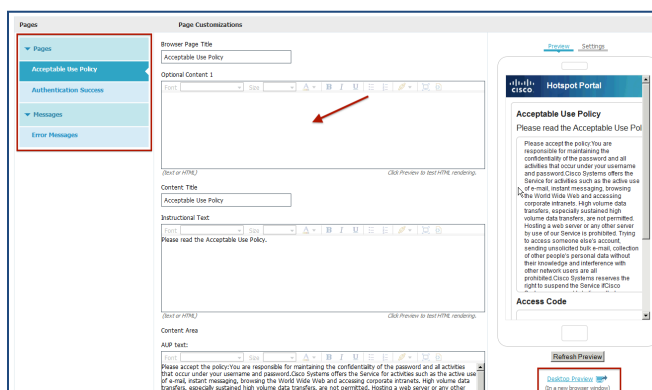


図 52. ポータルのカスタマイズ:ミニ プレビュー

**ステップ 6** 基本的なカスタマイズが完了したら、ミニプレビューの右下にあるオプションをクリックして、デスクトッププレビュー（ページの最上部にあるポータルテスト URL と同じ）を確認します。

**注:** ページ上部にあるポータルテスト URL 使用して、実際のクライアントを使用せずに、ユーザが体験する完全なフローをテストすることもできます。

**ステップ 7** デスクトッププレビュー ブラウザ ウィンドウを閉じます。

**ステップ 8** ページ最上部にある [閉じる (Close)] をクリックします (図 53 を参照)。

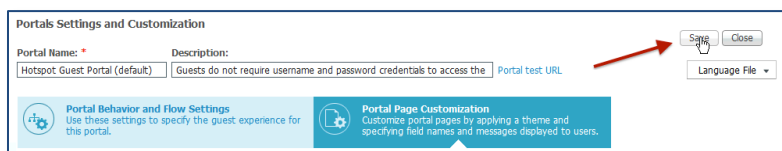


図 53. ポータル ページのカスタマイズを保存

ゲストのカスタマイズの詳細については、管理者ガイドの「[Customize End-User Web Portals](#)」の項を参照してください。

ISE 1.3 を使用した Cisco Wireless Guest Access のインストールが完了しました。

---

## 次のステップ

---

設定オプションの詳細については、<http://www.cisco.com/go/ise> にある Cisco ISE の資料を参照してください。

## 付録 A: スイッチの設定

スイッチの設定ファイルの例を次に示します。

```
hostname 3560CG
!
vlan 50
 name GUEST
!
vlan 100
 name Mgmt
!
interface GigabitEthernet0/1
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/2
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/3
 switchport access vlan 50
 switchport mode access
!
interface GigabitEthernet0/4
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/5
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/6
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/7
 switchport access vlan 90
 switchport mode access
!
interface GigabitEthernet0/8
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/9
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Vlan50
 ip address 10.1.50.1 255.255.255.0
 ip helper-address 10.1.100.10
!
interface Vlan100
 ip address 10.1.100.1 255.255.25
```