ISE 2.0 ワイヤレス ゲスト セットアップ 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:2016 年 3 月

目次

このマニュアルについて

このガイドでは、すぐにゲスト アクセスを提供できるように 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。

このガイドの一部は、すでに設定されている WLC または ISE に使用できます。このガイドのフローには、基本的なセットアップを正しい順序で進めることができるよう、リセットされた（未構成の） ISE Web UI が利用可能な物理コントローラが必要です。

このガイドの対象読者は、ISE Express（WLC/ISE の廉価版ライセンス）の購入者ですが、クリーン インストールから ISE および WLC を設定するユーザも使用できます。

このガイドは、ISE 2.0 を対象としています。

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
- クレデンシャルを持つゲスト ポータルを使用したゲスト アクセス

サポートはどこで受けることができますか

このガイドを使用する汎用サポートについては、ローカル ISE ベンダー、シスコ アカウント チームまたは Cisco TAC にお問い合わせください。

ISE ワイヤレス ゲスト セットアップ ウィザードのサポートについては、ise-express@cisco.com までメールにてお問い合わせください。

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：Cisco Wireless Controller（WLC）および Identity Services Engine（ISE）のインストールおよび設定**：パート 1 では、**パート 2** での手順に進む前に WLC と ISE に対して行うインストール事前設定と設定アクティビティについて説明します。

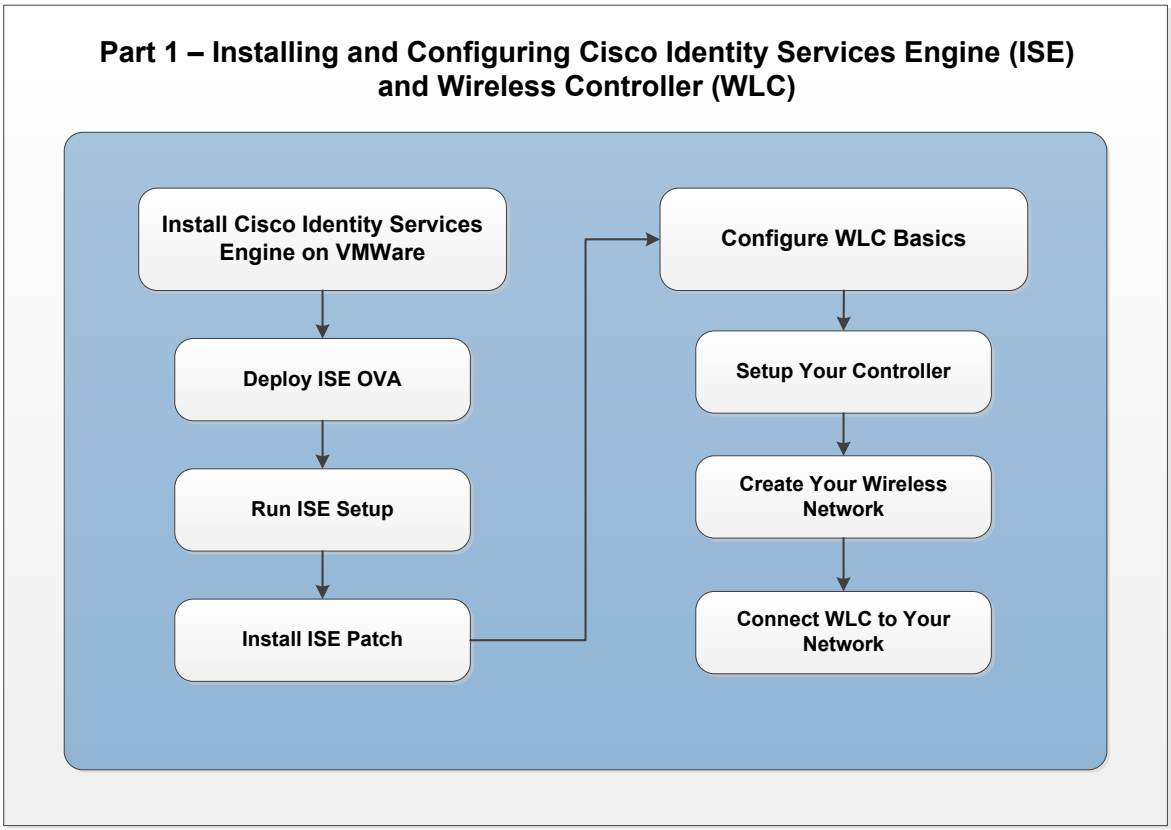

図 1 パート 1 のフロー - ISE および WLC のインストールおよび設定

- **パート 2:ゲスト アクセス用の WLC および ISE の設定**:パート 2 では、ISE を取得したシスコ ワイヤレスのゲスト アクセス用の追加の設定手順について説明します。

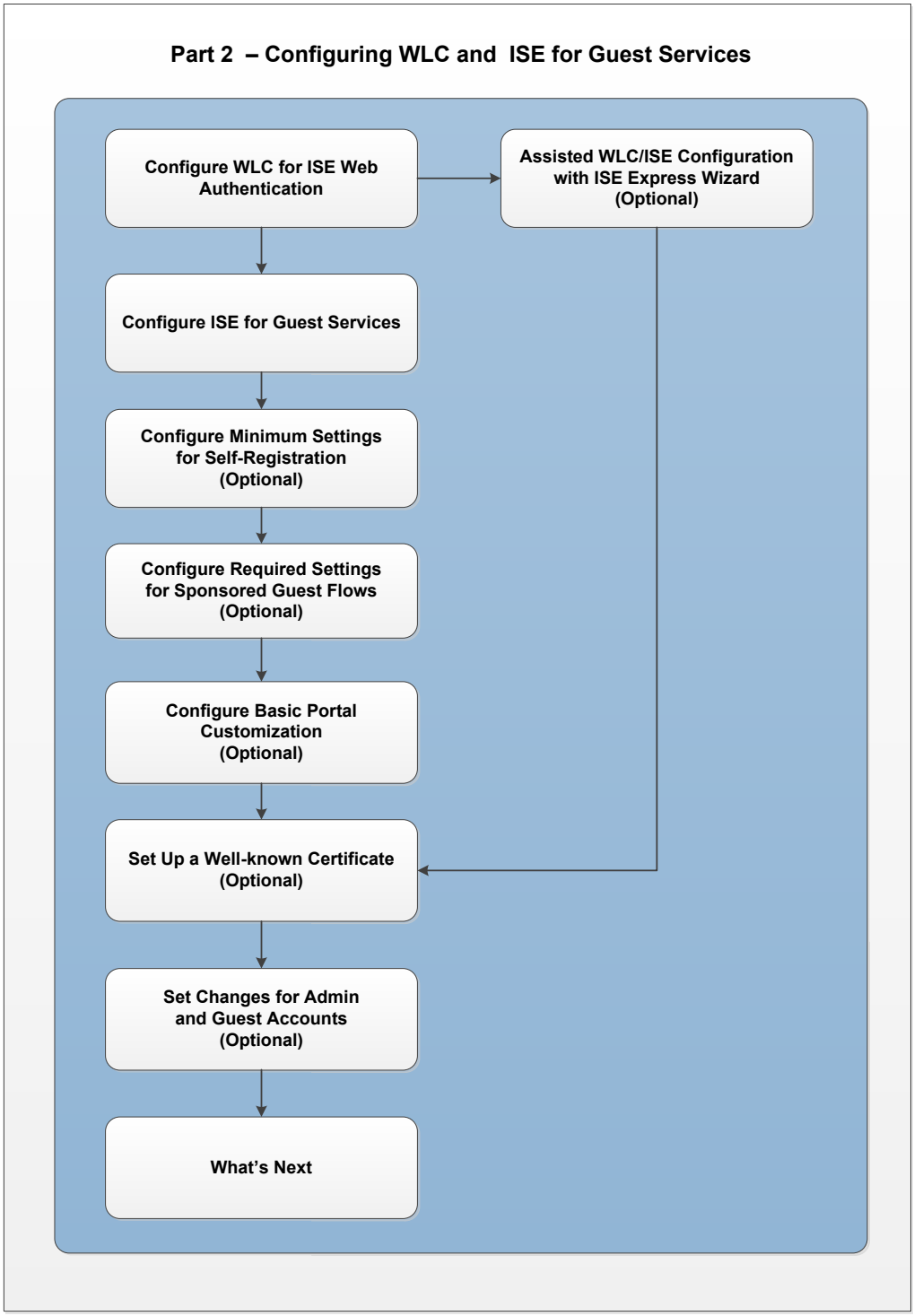

図 2 パート 2 のフロー - ゲスト サービス用の WLC および ISE の設定

要件

- サポートされる仮想環境
  - ESX (i) 5.x の VMware バージョン 8（デフォルト）
  - ESX (i) 6.x の VMware バージョン 11（デフォルト）
  - RHEL 7.0 の KVM（サポートされていますが、このガイドでは説明しません）
- 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 2.0
- 8.0.121.0 を実行する物理的シスコ ワイヤレス コントローラ（WLC）。最新情報については「ISE compatibility chart」を参照してください。
  - これは、ソリューションの設定完了後、このコードを実行したアップグレードが未実行である場合に、より簡単な方法として推奨されています。
- Microsoft Active Directory のスポンサー グループについては、『ISE Network Component Compatibility Guide』の「Supported External Identity Sources」の項を確認してください。

注:このガイドは、新しいワイヤレス コントローラのインストール専用です。新しいインストールでない場合は、コントローラのファクトリ リセットを実行します。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。それでも、このガイドを使用する場合は、WLAN および ACL 設定に必要な設定の参考として使用できます。

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、ゲスト アクセス 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。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

資格情報を持ったゲスト ポータルには、ゲストがアクセスするユーザ名とパスワードが必要です。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。この自己登録ポータルは、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、ネットワークに対する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。

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 ダウンロード ソフトウェア」をクリックします。

- ISE 2.0 の ISE VM OVA ファイル：Virtual SNS-3415
  - ISE-2.0.0.306-virtual-SNS3415.ova
- ISE 2.0 最新パッチ：このリリースの詳細については、リリース ノートを参照
  - 例：ise-patchbundle-2.0.0.306-Patch2-164765.SPA.x86_64.tar.gz
- ISE 2.0 ワイヤレス ゲスト セットアップ ウィザード（WLC および ISE の自動設定に推奨）
  - サポート対象：
    - Apple MAC OSX 10.9 以上
    - Microsoft Windows 7 以上

注：ISE パッチ（tar.gz）をダウンロードすると、OSX Safari などのいくつかの Web ブラウザでは、アーカイブの構造は維持されません。パッチをインストールする際にアーカイブの構造を維持するため、Firefox または Google Chrome のブラウザを使用することを推奨します。

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 [英語]

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、インストールおよび設定中に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。インストールと設定プロセス時に、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前と事前設定チェックリストの情報を記録している間に、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（内部サーバ）
- 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

表 1 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	• コントローラ システム名 • WLC で設定 • *例:WLC*	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	• WLC のネットワーク情報 • WLC および ISE で設定	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	• ネットワーク内の DHCP サーバ • WLC で設定	DHCP サーバの IP:_____
4	ゲスト SSID	• ゲストがアクセスするネットワークの名前 • WLC で設定 • *例:yourcompany-guest（企業名-ゲスト）*	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	• ゲスト用に使用される VLAN • WLC で設定 • *例:50*	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	• 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。 • WLC で設定	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:_____

番号	サービス	説明	情報をここに記録
7	DNS サーバの IP	• ネットワーク内の DNS サーバ • ISE で設定	DNS サーバの IP:_____
8	NTP サーバの IP	• ネットワーク内の NTP サーバ • ISE で設定	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	• ISE のネットワーク情報 • WLC および ISE で設定	ISE の IP:_____ サブネット マスク:_____ ゲートウェイ:_____
10	ISE のホスト名およびドメイン	• ISE サーバの名前とドメイン • ISE で設定 • DNS であること、それ以外はこのソリューションが動作しない	ISE のホスト名:_____ ISE ドメイン:_____
11	管理ネットワーク VLAN	• ESX (i) ホストで ISE および WLC が接続するネットワーク • WLC および ESX(i) ホストで設定 • *例:100*	管理ネットワーク VLAN:_____
12	共有秘密鍵	• 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。 • WLC および ISE で設定	共有秘密鍵:_____

VMware サーバへの Cisco ISE のインストールおよびセットアップ

ガイドのこのパートでは、VMware サーバで ISE ソフトウェアをインストールし、設定するタスクについて説明します。

図 3 に、このパートのタスクのワークフローを示します。このワークフローは、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。

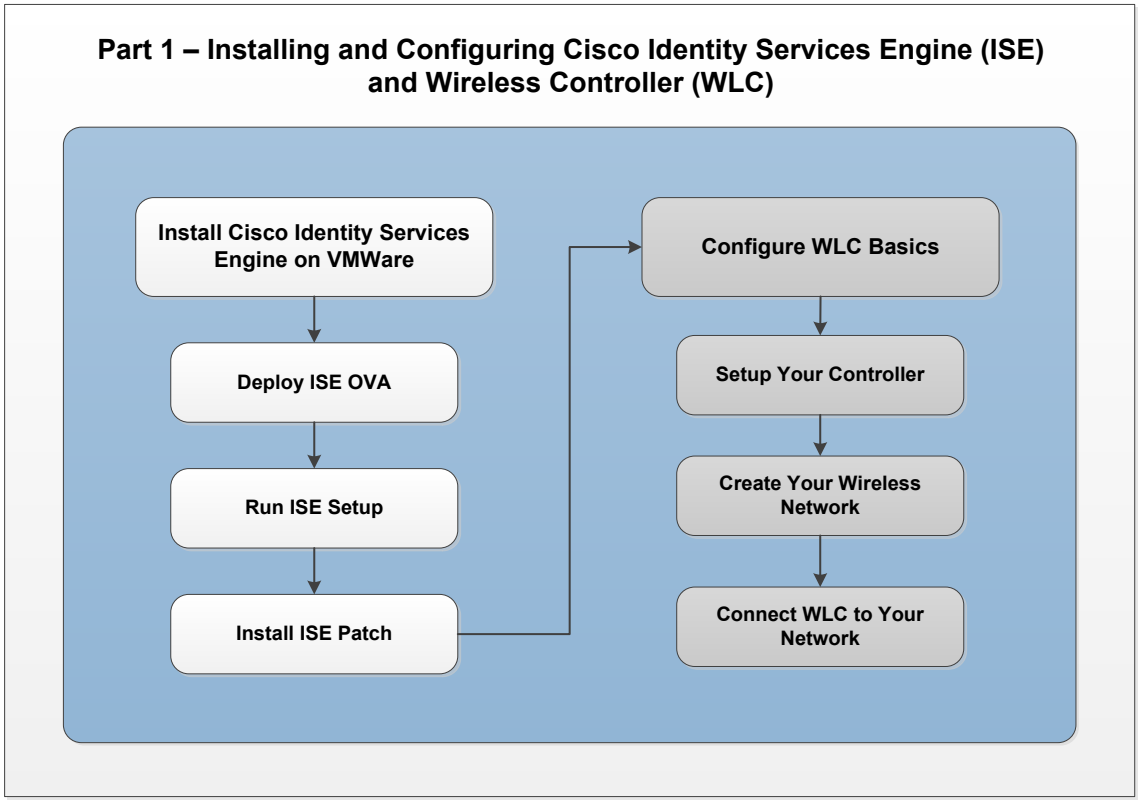

図 3 パート 1 フロー – WMWare への Cisco ISE のインストール

ISE OVA の仮想マシンとしての導入

OVA テンプレートを使用して仮想マシンに 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。前のタスク「Cisco ISE ソフトウェアのダウンロード」で、Cisco.com から OVA テンプレートをダウンロードしました。

ESX(i) 環境に ISE OVA を導入するには、次の手順に従います。

手順 1 **VMware vSphere** クライアントを起動します。
手順 2 **VMware ホスト**にログインします。
手順 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。
手順 4 [参照(Browse)] をクリックして OVA テンプレートを選択し、[次へ(Next)] をクリックします。
手順 5 [OVF テンプレート詳細(OVF Template Details)] ページの詳細を確認し、[次へ(Next)] をクリックします。
手順 6 一意に識別するために仮想マシンの名前を [名前とロケーション(Name and Location)] ページに入力し、[次へ(Next)] をクリックします。
手順 7 OVA をホストする**データストア**を選択します。
手順 8 [ディスクフォーマット(Disk Format)] ページの [シックプロビジョニング(Thick Provision)] オプション ボタンをクリックし、[次へ(Next)] をクリックします。

- Cisco ISE 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 Zeroed)] か [イーガーゼロ(Eager Zeroed)] を選択するよう要求されたら [レイジーゼロ(Lazy Zeroed)] を選択します。

手順 9 [完了準備(Ready to Complete)] ページの情報を確認します。
手順 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。
手順 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。

手順 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。

手順 2 本書の「事前設定チェックリスト」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、『*Cisco ISE 2.0 Administration Guide*』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、次の指示に従って最新のパッチをインストールします。

手順 1 ISE の管理 UI（http://iseapaddress）にログインします。

手順 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。

手順 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。

手順 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。

- 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。

手順 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、『*Cisco ISE 2.0 Administration Guide*』の「Installing a Software Patch」の項を参照してください

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［英語］
- Cisco WLAN リリース ノート［英語］

図 4 に表示されるフロー図は、WLC の基本を設定する際に使用するプロセスを示します。

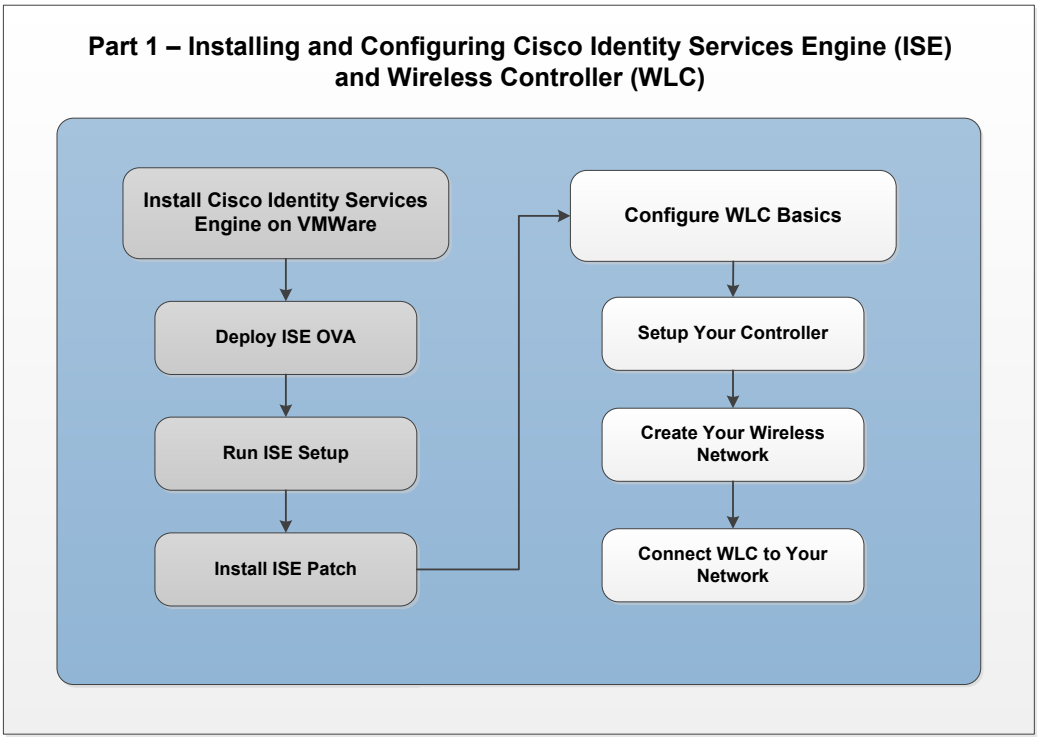

図 4 パート 1 フロー - WLC の基本設定

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、次の手順を実行します。

手順 1　**図 5** 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。

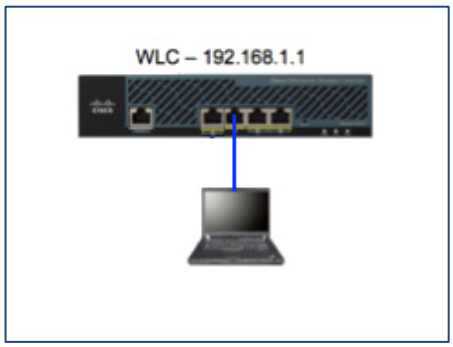

図 5 WLC へのラップトップの接続

- 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。

手順 2　Web ブラウザを開き、WLC セットアップ ウィザードにアクセスするには、「192.168.1.1」と入力します。

- 図 6 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。

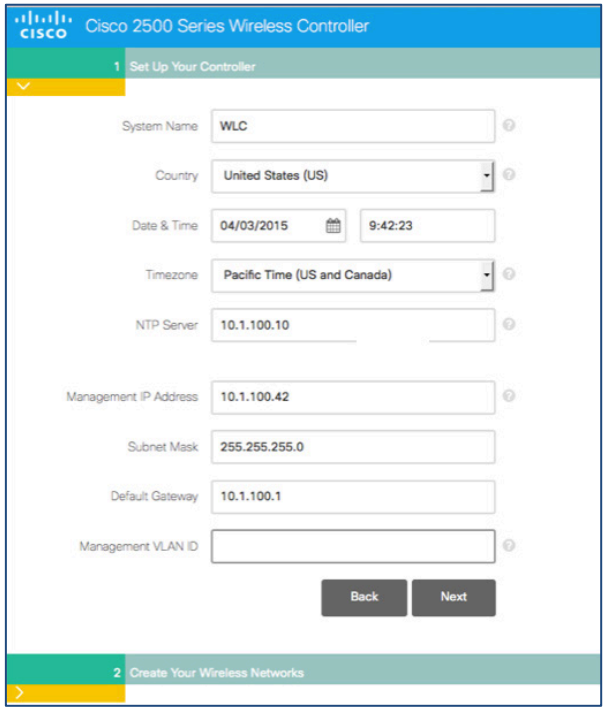

図 6 コントローラのセットアップ

手順 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**」の項で完了した「事前設定チェックリスト」を参照してください。

表 2 コントローラ フィールドの設定

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 Server）	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

フィールド	説明
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 Gateway）	WLC のデフォルト ゲートウェイ 事前チェックリストの項目番号：2
管理ネットワーク VLAN（Management Network 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

手順 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

手順 5　[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。

手順 6　図 7 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 7 ワイヤレス ネットワークの作成

表 3 ワイヤレス ネットワーク フィールドの作成

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（Security）	ドロップダウン メニューに表示されるオプションから、セキュリティ タイプ [Web での同意（Web Consent）] を選択します。 注：WPA では ISE ゲストはサポートされません。
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

手順 7 「事前設定チェックリスト」で用意した、**必要な情報**を入力します。

手順 8 [次へ（Next）] をクリックして続行します。

- 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。

ネットワークへの WLC の接続

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、**図 8** のトポロジ例をご覧ください。

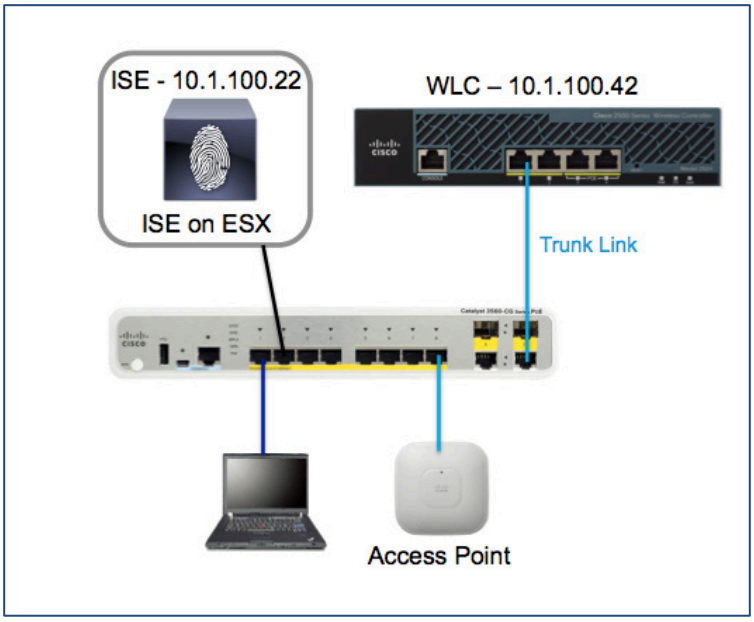

図 8 トポロジ例

図 8 の Cisco 3560G スイッチは、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：ワイヤレスの構成」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しなくなります。

手順 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。

手順 2 WLC の**ポート 1** を、スイッチのトランク **ポート 10** に接続します。スイッチのトランク ポートには、コントローラを管理しゲスト アクセスを提供するために、管理 VLAN（100）およびゲスト VLAN（50）を含める必要があります。

- 管理 PC を使用して、再度 WLC にアクセスできるようになります。（例：https://10.1.100.42）。

手順 3 コントローラのアクセス ポイント検出用のネットワークを設定します。

アクセス ポイントを設定するには、ワイヤレス コントローラを検出するようにネットワークを設定します。ネットワークにおける検出オプション設定の詳細については、ワイヤレス コントローラのマニュアルを参照してください。

http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configuration-guide/b_cg80/b_cg80_chapter_01100101.html#ID302

手順 4　ネットワークに必要な検出オプションを設定した後、**ポート 8** にアクセス ポイントを接続します。

注:　この時点で、すべてのクライアントからゲスト ワイヤレス ネットワーク（SSID）を参照できるはずです（事前設定チェックリストの項目番号：**4**）。これは、コントローラからの基本のスプラッシュ ページで、ISE ゲスト（Web Auth）ポータルを使用するための統合はまだされていません。

セットアップ ウィザードで処理された WLC および ISE の設定

WLC と ISE の基本インストールとセットアップが完了し、設定の残りのプロセス方法には 2 つのオプションがあります。

推奨されるパスは、このタスクを自動化するための ISE 2.0 ワイヤレス ゲスト セットアップ ウィザードを使用することです。ウィザードは、OS X および Windows で実行されます。必要なゲスト フローのシステムを接続して設定するのに必要な情報を要求されます。

事前にウィザードをダウンロードする必要があります。そうでない場合は、Cisco ISE ダウンロード ソフトウェアからダウンロードします。

ウィザードを使用して、**図 9** に示すようにガイドのほとんどを省略します。

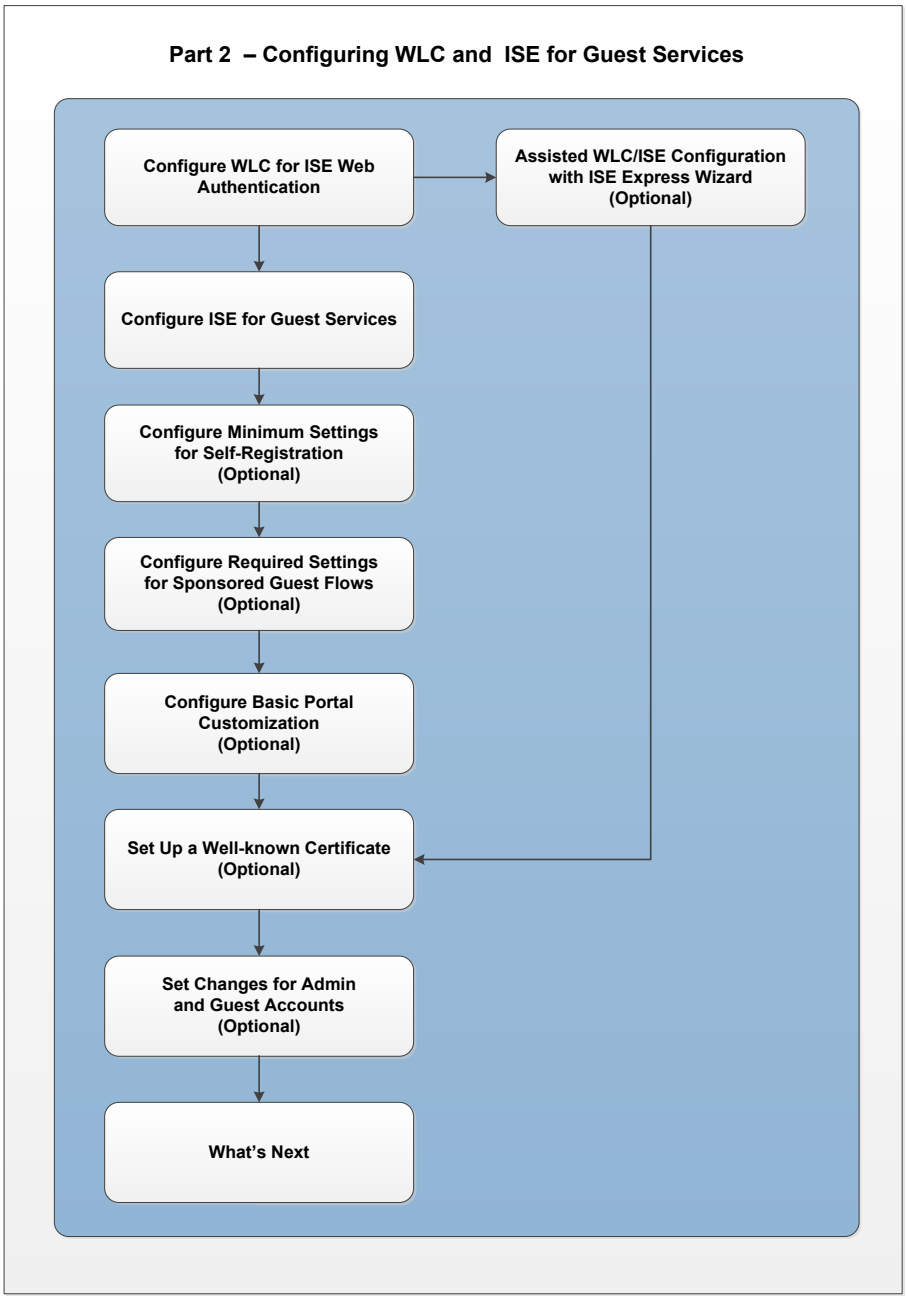

図 9 パート 2 フロー – ゲスト サービスの WLC と ISE の設定

注: ISE ワイヤレス ゲスト セットアップ ウィザードを介して実行した後は、このガイドの「ISE Web 認証用の WLC の設定」から「ポータルの基本的なカスタマイズの設定（任意）」までの項は参照専用です。「既知の証明書の設定（任意）」に進んでください。

手順 1 手動設定が必要な場合は、「*ISE Web 認証用の WLC の設定*」に進んでください。

図 10 では、ウィザードに開始する前の基本要件が表示されています。開発者にログを提供する必要がある場合、左下に [デバッグ ウィンドウ(Debug window)] オプションがあります。右下にビルド番号が表示されます。

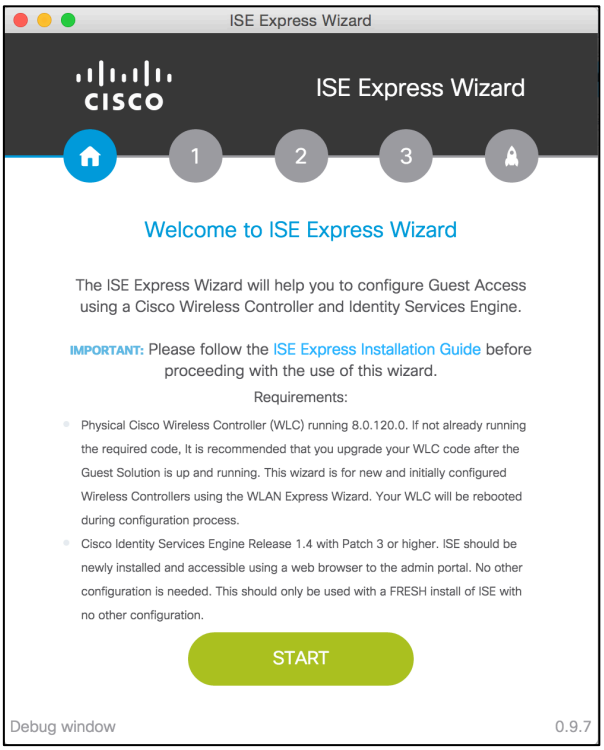

図 10 ISE ワイヤレス ゲスト セットアップ ウィザードの開始

手順 2 [開始(Start)] をクリックします。

図 8 では、ゲストに送信するポータル タイプ(ゲスト フロー)を選択します。これらのフローは、「*ゲスト アクセス*」の項ですでに説明しました。ポータルをカスタマイズする場合にも選択できます。

手順 3 チェックボックスをオンにして**ポータルのカスタマイズ(オプション)を有効**にし、使用したい**ゲスト フロー**を選択します。現時点でカスタマイズを行わない場合は、手順 5 にスキップします。ポータルは後で設定できます。詳細については、「*ポータルの基本的なカスタマイズの設定(任意)*」を参照してください。

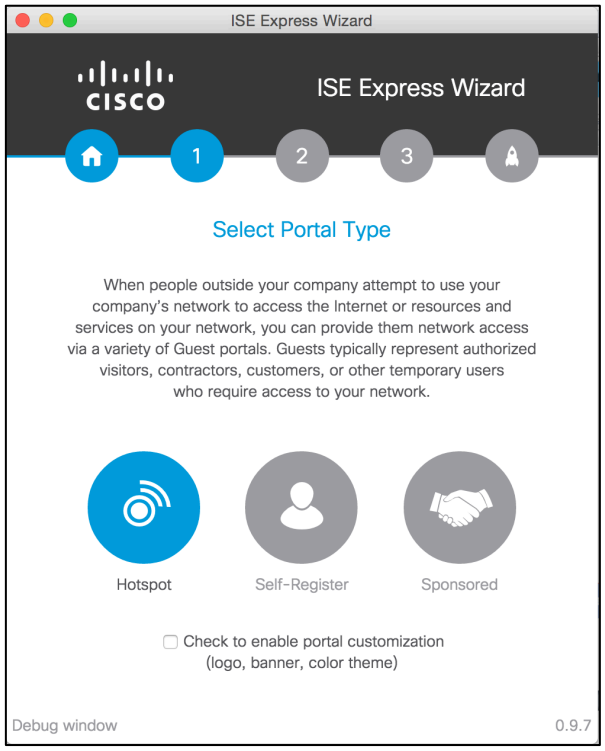

図 11 ポータル タイプの選択

手順 4　　図 **12** に示すように、**ロゴ**、**バナーをアップロードし**、**カラー テーマ**を選択して、[次へ(Next)] をクリックします。

注:　　このカスタマイズはフローのポータルのいずれかに対して行います(ゲストまたはスポンサー)。

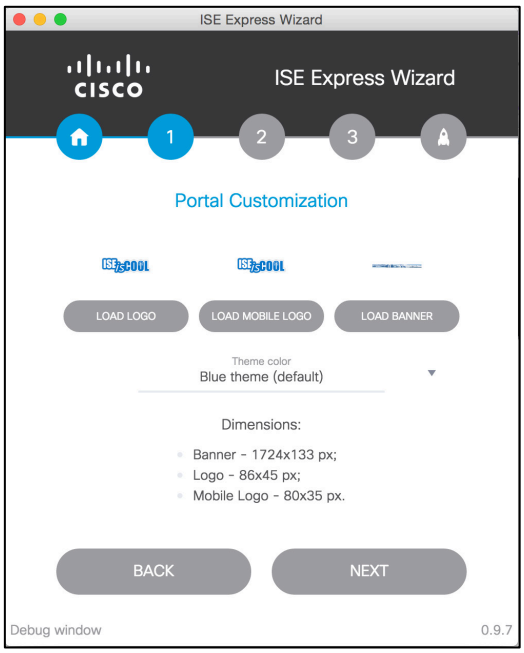

図 12 ポータルのカスタマイズ

手順 5 ワイヤレス コントローラの設定に必要な情報を入力します。この情報は、事前設定チェックリストを使用して計画段階で収集されました。完了したら、[次へ(Next)] をクリックします。

注: ゲートウェイ IP アドレスは、WLC 管理ネットワークのデフォルト ゲートウェイです。

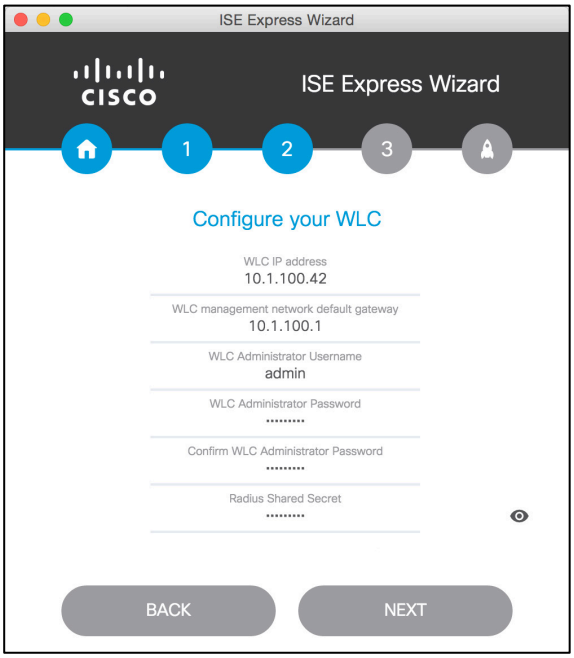

図 13 WLC の設定

手順 6 ウィザードは、ワイヤレス コントローラに接続して利用可能な WLAN のリストを取得します。WLAN Express 経由で実行中に設定したゲスト ネットワークを選択し、[次へ(Next)] をクリックします。

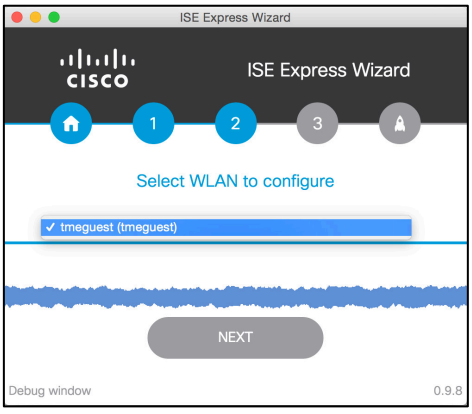

図 14 WLAN の選択

手順 7　**図 15** では、ウィザードから ISE を設定するのに必要な情報が求められます。この情報は事前設定チェックリストを使用して収集されました。必要な情報を入力した後、[次へ(Next)] をクリックします。

ゲストのロケーション/タイム ゾーン - ゲストの正しいタイム ゾーンを入力することは重要です。詳細については、またはウィザードの完了後より多くの場所を設定するには、「*ゲストのロケーションとタイム ゾーンの設定*」の項を参照してください。

スポンサー ソースの選択:スポンサーに使用するアイデンティティ ソースを選択するためのオプションもあります。ここでは、Active Directory のグループを使用するためのオプションを表示します。ISE にローカル ユーザを作成する選択をすることもできます。これらのオプションの詳細については、またはウィザードのセットアップが完了したときに別のスポンサーを追加するには、「*スポンサー アカウントの設定*」の項を参照してください。

注:　ここでは、Active Directory のグループを使用してスポンサー ゲストのフローを表示します。これは、ウィザードを完了した後に表示されるオプションのスーパーセット(最も詳細)です。

ホットスポットのフローでは、次のオプションが表示されず、自己登録フローにスポンサー ユーザのソースを設定するオプションはありません。

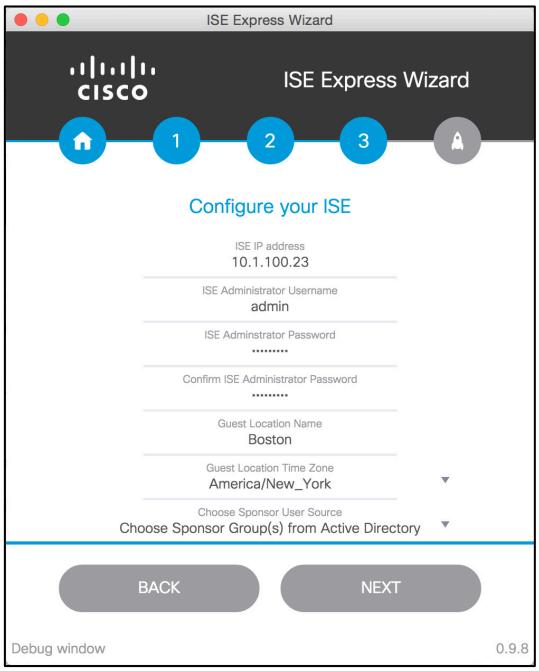

図 15 ISE の設定

手順 8　手順 7 で選択したオプションによって、スポンサー アカウントを設定する画面を表示するか、Active Directory を示します。ローカル アカウントは簡単な手順であるため、そのオプションは強調表示していません。ローカル アカウントを使用する場合は、手順 10 にスキップします。
図 16 に示すように、Active Directory オプションに進む場合は、次の情報を入力し、[次へ(Next)] をクリックします。

この情報はシンプルです。次を入力します。

- 参加ポイント名:ISE で作成されるドメイン接続の基本ラベル
- Active Directory ドメイン:スポンサーとして使用するグループが属するドメイン

- AD ユーザ名/パスワード

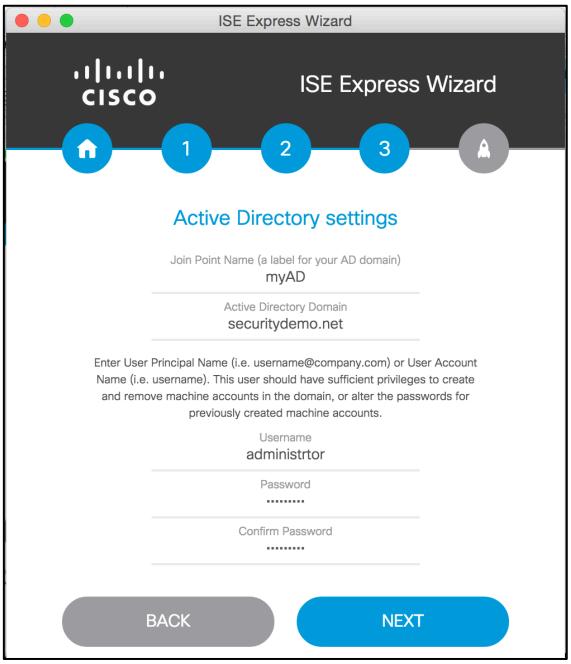

図 16 Active Directory 設定

手順 9 ウィザードは、ドメインに接続し、Active Directory のグループをすべてプルダウンします。スポンサー ゲスト アカウントにアクセスできるグループを 1 つ以上選択できます。アカウントを選択したら、[次へ(Next)] をクリックします。

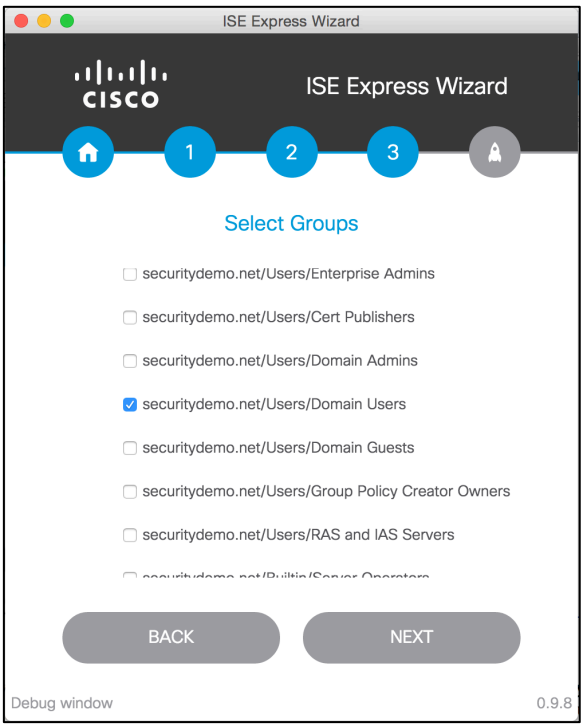

図 17 グループの選択

手順 10 この手順では、スポンサー ポータルの URL を設定します。この機能を使用する DNS には依存関係があります。DNS を設定していなくても、このオプションをここで設定し、DNS を後で設定できます。詳細については、「ISE スポンサー ポータルの FQDN ベースのアクセスの設定」の項を参照してください。

FQDN を入力するか、またはこれを後で行うためのオプションを選択します。
[開始(Start)] をクリックします。

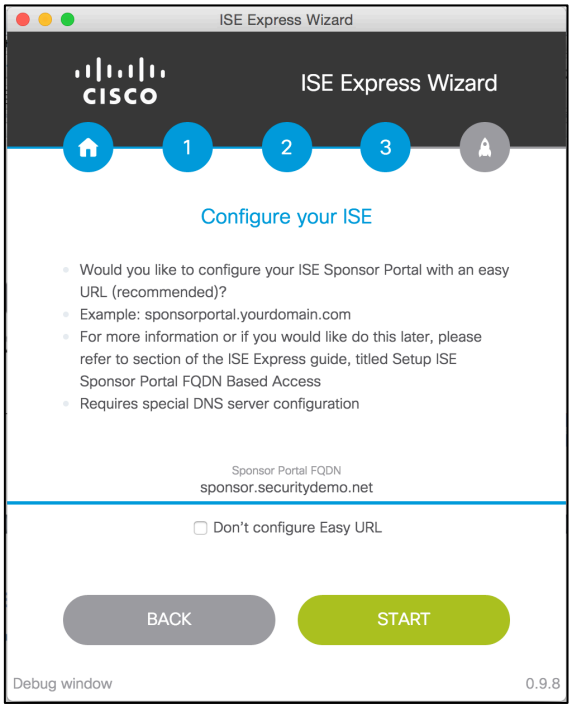

図 18 スポンサー ポータルの FQDN の設定

Apple デバイスのサポートには再起動を必要とする特別な設定が必要です。このオプションの詳細については、「キャプティブ ポータルのバイパス設定」の項を参照してください。

図 19 で、[OK] をクリックして、先へ進みます。

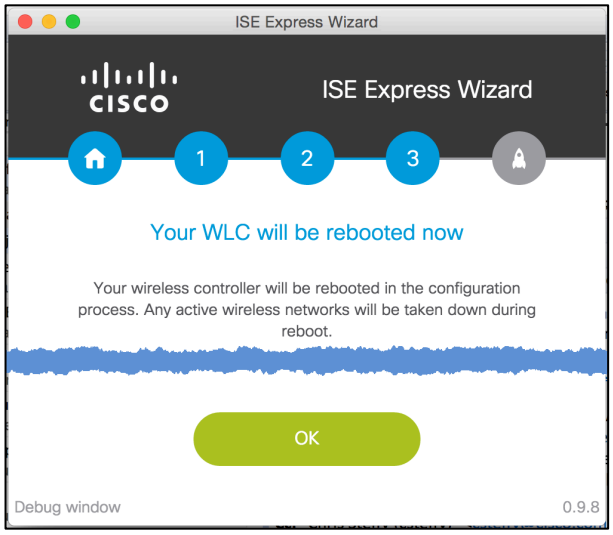

図 19 キャプティブ ポータルのバイパス構成の再起動

図 20 に示すように、ワイヤレス コントローラおよび ISE の両方を設定し、各コンポーネントの状態のアクティブ ステータスを示します。

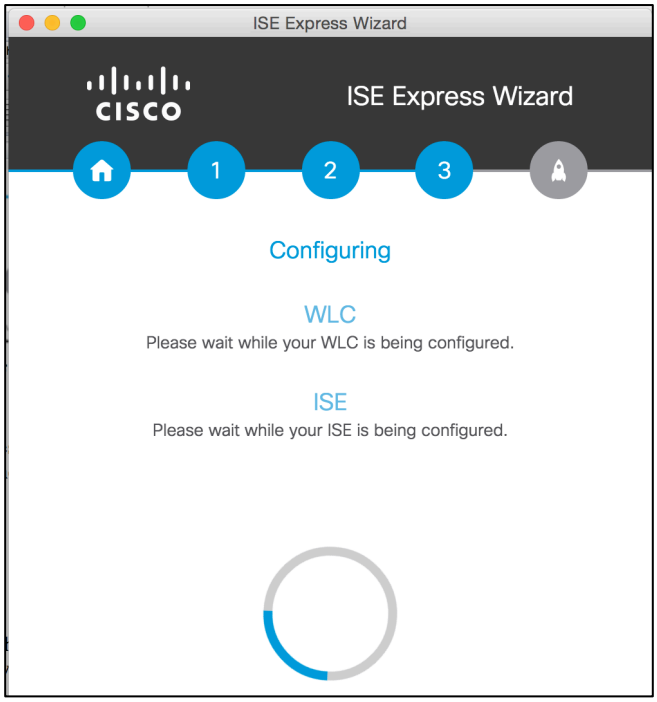

図 20 設定

ウィザードで WLC と ISE を設定すると、**図 21** に示すように最終ステータスの画面が表示されます。この画面には次の情報があります。

- SSID：クライアントの接続先の名前。
- ゲスト ポータルにリンクします。ポータルがどのように表示されるかを参照するためにこれを使用できます。ユーザが実際のデバイスから参照するように、ポータルを完全にテストするために使用することもできます。
- スポンサー フローの場合、設定する際にスポンサー ポータルと簡単な URL（FQDN）にもリンクを提供します。

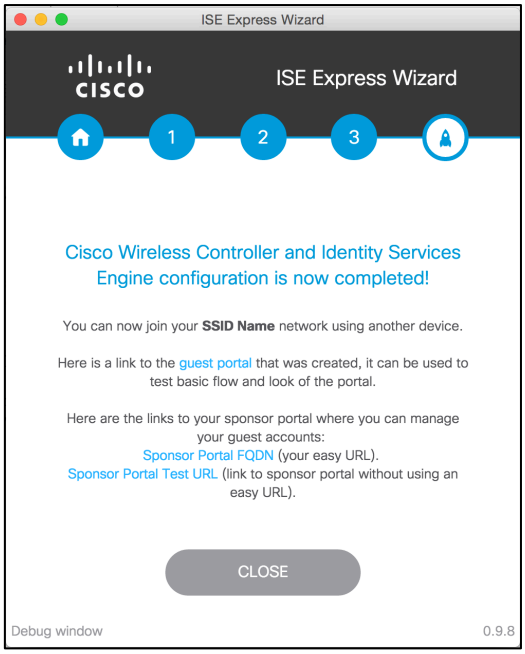

図 21 完了された設定

手順 11 [閉じる（Close）] をクリックします。

注： システム設定が完了すると、両方の設定をリセットして新たに開始しない限り、WLC または ISE への接続にこのツールは使用できません。設定を変更するか、またはシステム全体について知る必要がある場合は、ドキュメントの残りを参照します。

ウィザードを使用して設定を完了しました。この後の「ISE Web 認証用の WLC の設定」から「ポータルの基本的なカスタマイズの設定（任意）」までの項は参照専用です。「既知の証明書の設定（任意）」の項に進んでください。

ISE Web 認証用の WLC の設定

この項では、WLC で必要なセキュリティ設定を設定して ISE を使用します。RADIUS NAC は、ISE が認可変更（COA）要求を送信し、ユーザがネットワークを認証してアクセスできるようにします。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。たとえば、Portal 認証のために ISE にリダイレクトすると、クライアントは認証されてネットワークへのアクセスが許可されます。

図 22 に表示されるフロー図は、ISE Web 認証用に WLC を設定するときに使用するプロセスを示します。

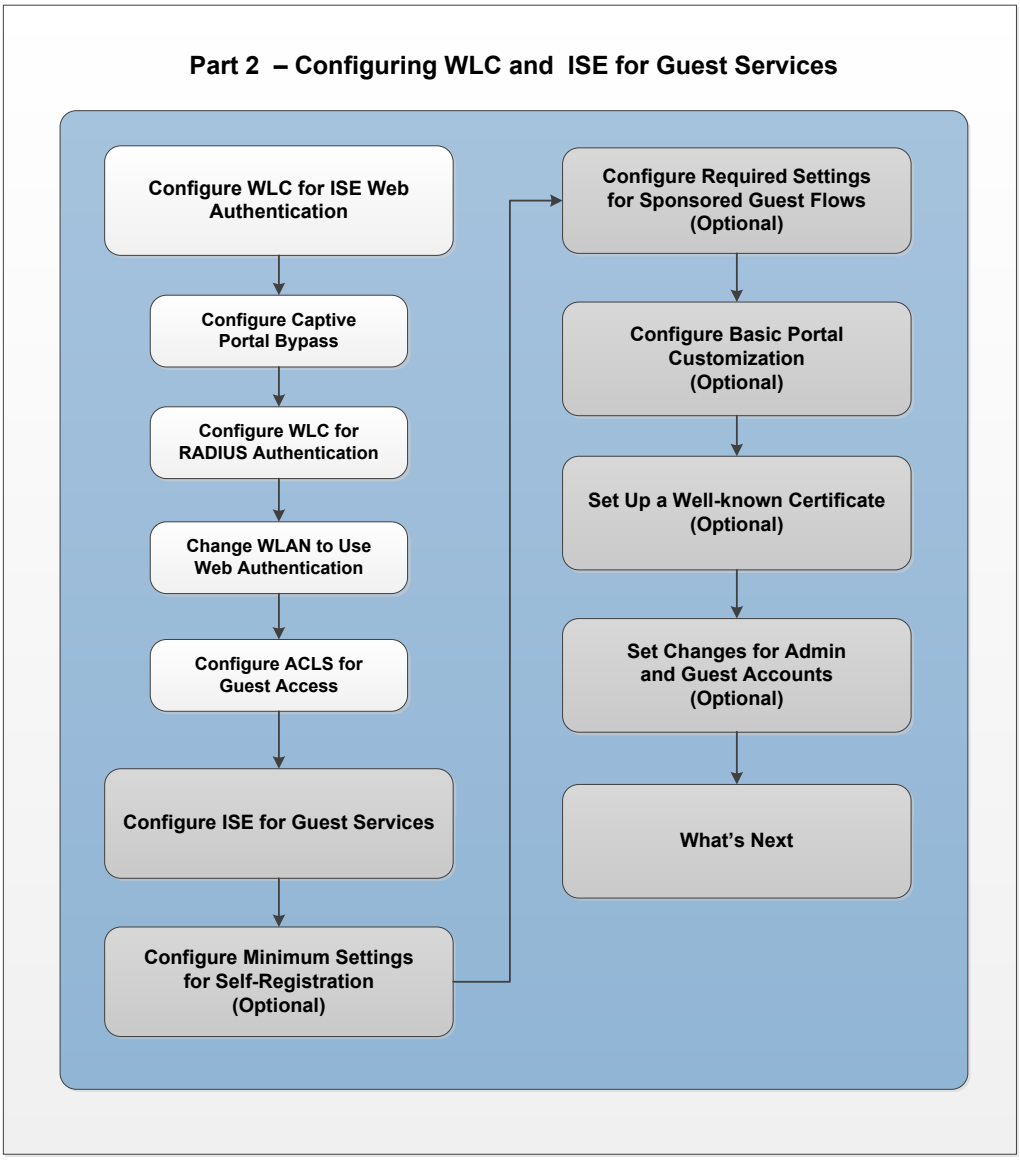

図 22 パート 2 フロー - ISE Web 認証用 WLC の設定

キャプティブ ポータルのバイパス設定

Cisco Identity Services Engine ソフトウェアのゲスト アクセスは、さまざまなクライアントや Web ブラウザでサポートされています。Cisco ISE ゲスト アクセスおよび Apple（iOS および OS X クライアント）を持つコントローラを使用するには、キャプティブ ポータル バイパス設定プロセスを完了する必要があります。

- キャプティブ ポータル バイパスのコマンドの使用に関する詳細については、ISE の使用しているバージョンの『*Cisco Wireless Controller Configuration Guide*』の「Configuring Captive Bypassing」を参照してください。

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。

手順 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。

注:コンソールまたは Telnet を使用して接続することもできます。

手順 2 コントローラの CLI にログインします。

手順 3 次のコマンドを入力します。

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

- コントローラから再起動するよう指示されます。

手順 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
```

手順 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   ..................Enable
```

手順 6 コントローラへの SSH セッションを閉じます。

WLC での RADIUS 認証サーバの設定

RADIUS 認証サーバとして ISE を設定するには、次の手順に従います。

手順 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。

手順 2 **図 23** 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。

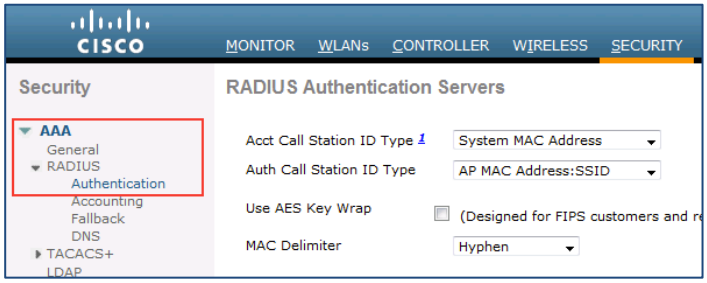

図 23 RADIUS 認証サーバ

手順 3　[新規(New)]をクリックします。

- **図 24** に示すように、RADIUS 認証サーバの画面が表示されます。

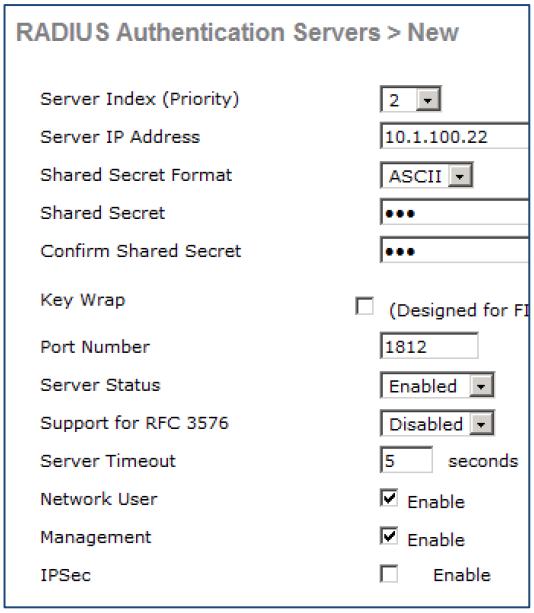

図 24 [RADIUS 認証サーバ(Radius Authentication Servers)] > [新規(New)]

手順 4　**ISE の IP アドレス**および**共有秘密鍵**を入力します。
手順 5　**RFC 3576** に対するサポートを有効にします。
手順 6　サーバのタイムアウトを **5 秒**に変更します。
手順 7　[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。

手順 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。
手順 2　**図 25** 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。

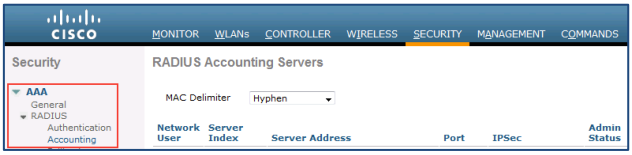

図 25 RADIUS アカウンティング サーバ

手順 3　[新規(New)]をクリックします。

- 図 26 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。

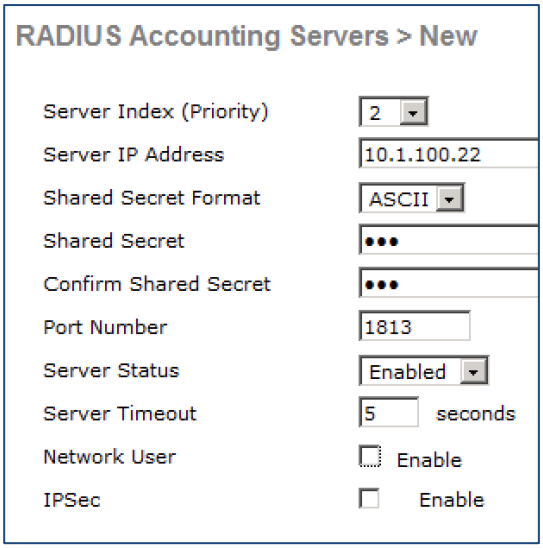

図 26 [RADIUS アカウンティングサーバ(Radius Accounting Servers)] > [新規(New)]

手順 4　**ISE の IP アドレス**および**共有秘密鍵**を入力します。
手順 5　サーバのタイムアウトを **5 秒**に変更します。
手順 6　[ネットワーク ユーザ(Network User)] チェックボックスをオフにします。
手順 7　[適用(Apply)] をクリックします。

ISE の Web 認証を使用するように WLAN の設定を変更

ISE の Web 認証に RADIUS NAC 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。

手順 1　[WLAN(WLANs)] を選択します。
手順 2　[ゲスト SSID(Guest SSID)] を選択します。

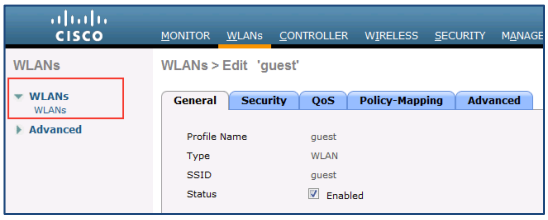

図 27 WLAN

手順 3 [セキュリティ(Security)] タブをクリックします。
手順 4 [レイヤ 2(Layer 2)] タブをクリックします

- **図 28** に示すように、[レイヤ 2(Layer 2)] の [セキュリティ(Security)] タブ オプションが表示されます。

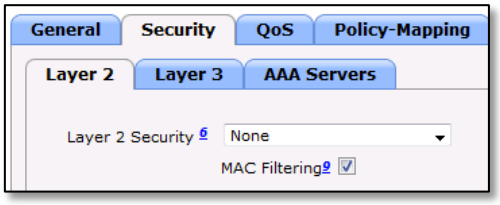

図 28 [セキュリティ(Security)] > [レイヤ 2(Layer 2)]

手順 5 レイヤ 2 セキュリティに対して、[なし(None)] を選択します。
手順 6 [MAC フィルタリング(MAC Filtering)] を有効にします。
手順 7 [レイヤ 3(Layer 3)] タブをクリックします。

- **図 29** に示すように、[レイヤ 3(Layer 3)] の [セキュリティ(Security)] タブ オプションが表示されます。

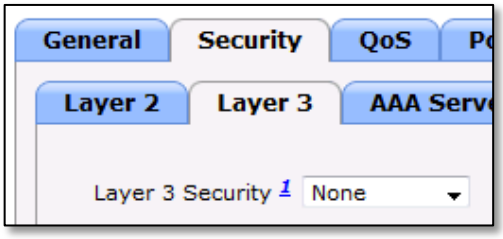

図 29 [セキュリティ(Security)] > [レイヤ 3(Layer 3)]

手順 8 [なし(None)] を選択します。
手順 9 [AAA サーバ(AAA Servers)] を選択します。

- **図 30** 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。

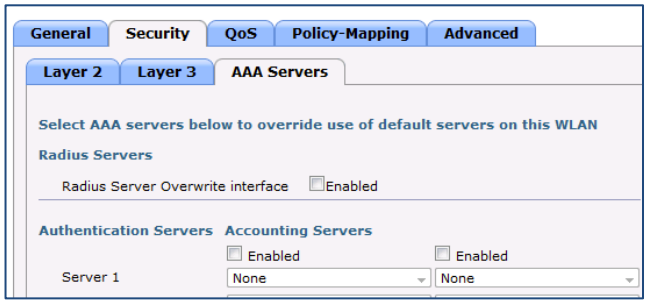

図 30 [セキュリティ(Security)] > [AAA サーバ(AAA Servers)]

手順 10　図 **31** に示すように、[サーバ 1（Server 1）] ラベルで、**認証サーバとアカウンティング サーバ**に対して ISE サーバの IP を選択して有効にします。

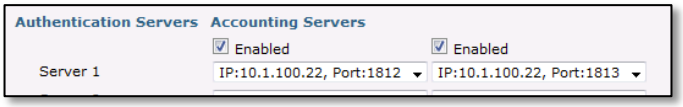

図 31 [セキュリティ（Security）] > [AAA サーバ（AAA Servers）]

手順 11　[詳細設定（Advanced）] タブをクリックします。

手順 12　図 **32** 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。

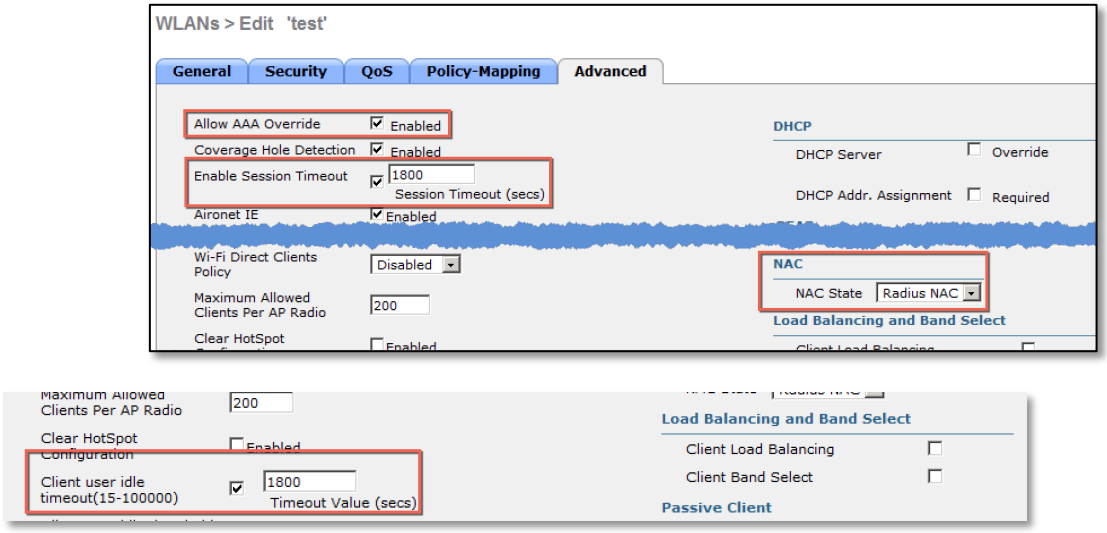

図 32 [詳細設定（Advanced）]

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

手順 14　[インターフェイス ACL をオーバーライド（Override Interface ACL）] に [なし（None）] を選択します。

手順 15　[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。

手順 16　[クライアント ユーザ アイドル タイムアウト（Client User Idle Timeout）] を有効にし、**1800 秒**に設定します。

手順 17　[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

手順 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 33** 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。

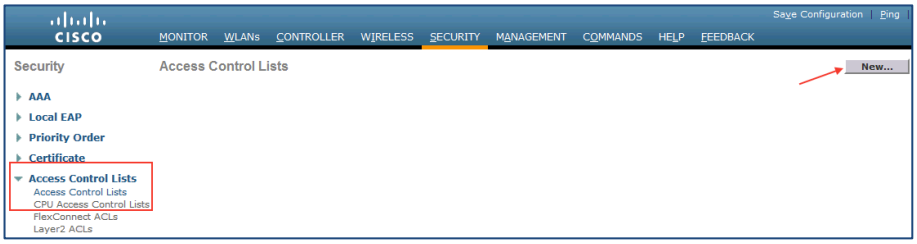

図 33 [セキュリティ(Security)] > [アクセスコントロールリスト(Access Control Lists)]

手順 2 [新規(New)] をクリックして、新しい ACL を作成します。

手順 3 **図 34** に示すように、名前に **guest-redirect** と入力します。

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

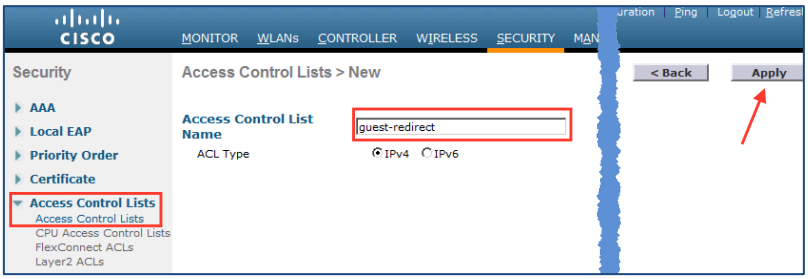

図 34 [アクセスコントロールリスト(Access Control Lists)]

手順 5 [適用(Apply)] をクリックします。

- メイン リストが表示されます。新しい ACL をクリックすると、**図 35** のように表示されます。

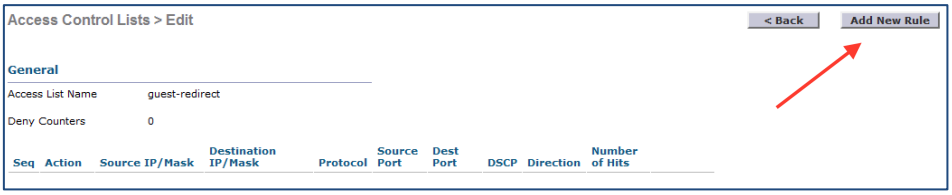

図 35 [アクセスコントロールリスト(Access Control Lists)] > [編集(Edit)]

手順 6 [新しいルールの追加(Add New Rule)] をクリックします。
手順 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。
手順 8 **図 36** 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)。

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	Inbound	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Outbound	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 36 ゲスト リダイレクション用の ACL 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

手順 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。**[guest-acl]** ACL をクリックします。
手順 2 **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。

注:次の手順を順番に実行することは非常に重要です。

- **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 37** 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。
  - 以下の ACL は WLAN Express で作成されたすべての ACL ではなく、追加の ACE をどこに挿入する必要があるかを示すための、ほんの一部であることに注意してください。

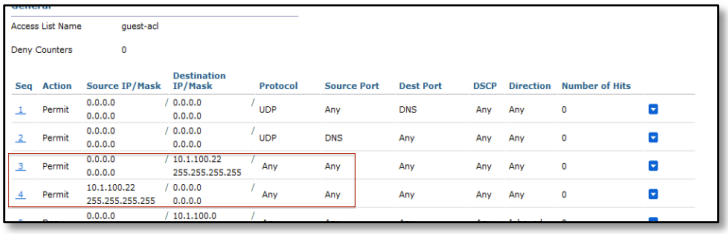

図 37 Guest Permit 用の ACL エントリ

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。

ゲスト アクセス用の ISE の設定

ワイヤレス コントローラを ISE Web 認証を使用するように設定したため、ISE に必要な手順を実行する必要があります。

図 38 に表示されるフロー図は、ゲスト サービス用設定 ISE のプロセスを示します。

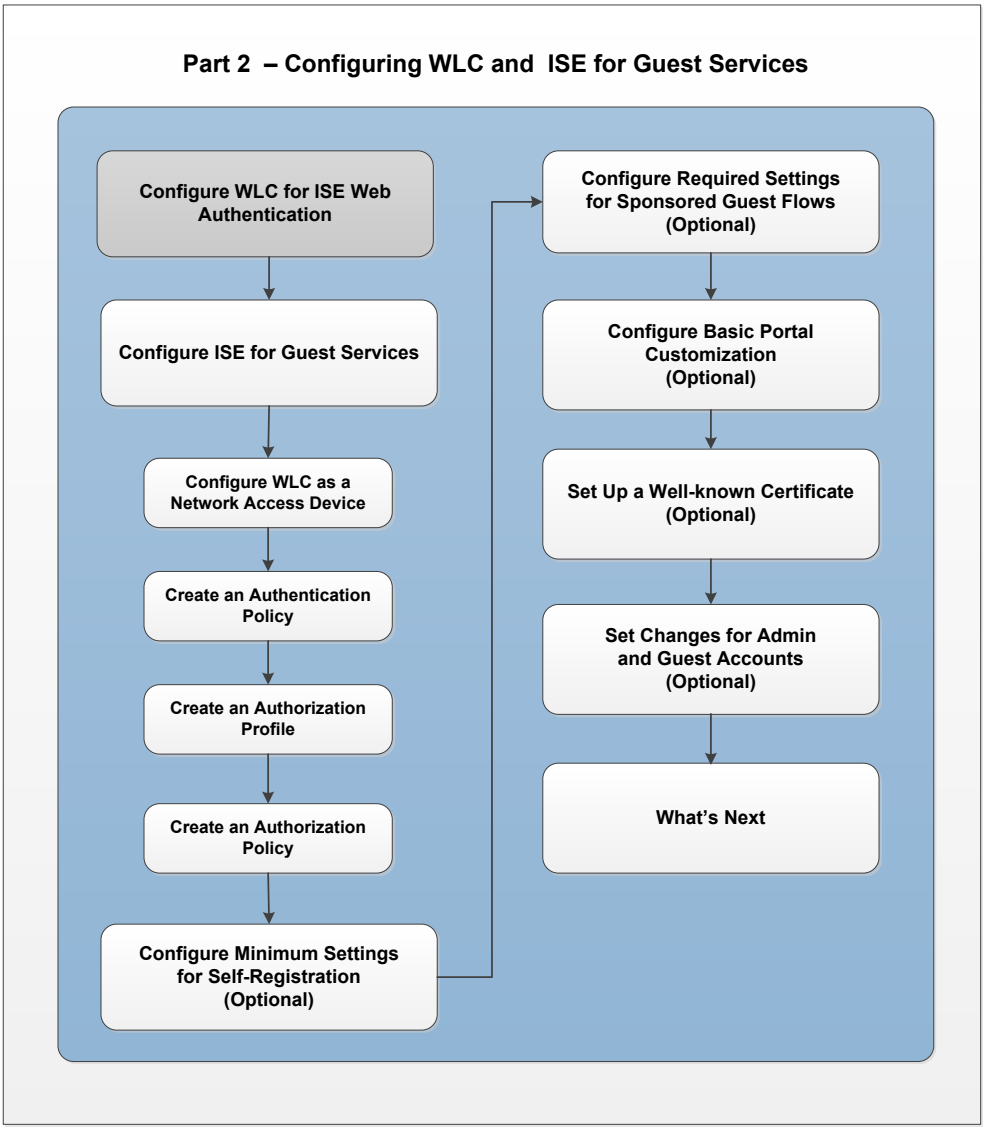

図 38 パート 2 フロー - ゲスト サービス用 ISE の設定

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

手順 1　**ISE の管理 UI** にログインします。

手順 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。

手順 3　**図 39** に示すように、[追加（Add）] を選択します。

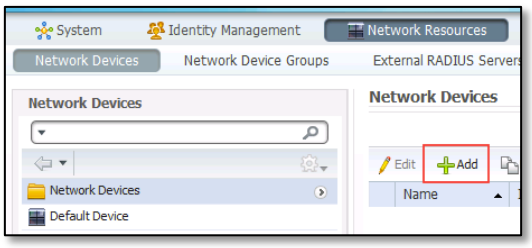

図 39 ネットワーク デバイスの追加

- **図 40** 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。

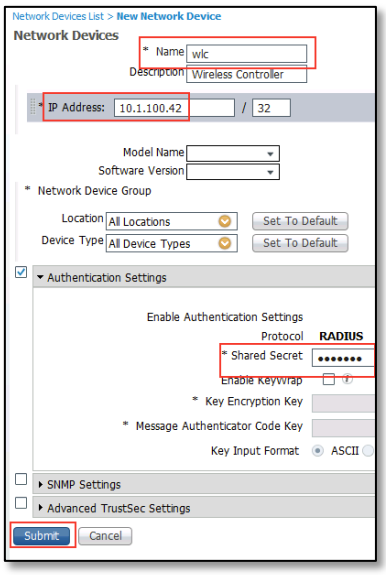

図 40 新しいネットワーク デバイスの追加

手順 4　**デバイス名**を入力します。

手順 5　**デバイスの IP アドレス**を入力します。

手順 6　[認証の設定（Authentication Settings）] を有効にします。

手順 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）。

手順 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。

手順 1 ISE の管理 UI にログインします。
手順 2 [ポリシー(Policy)] > [認証(Authentication)] に移動します。

- **図 41** 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。

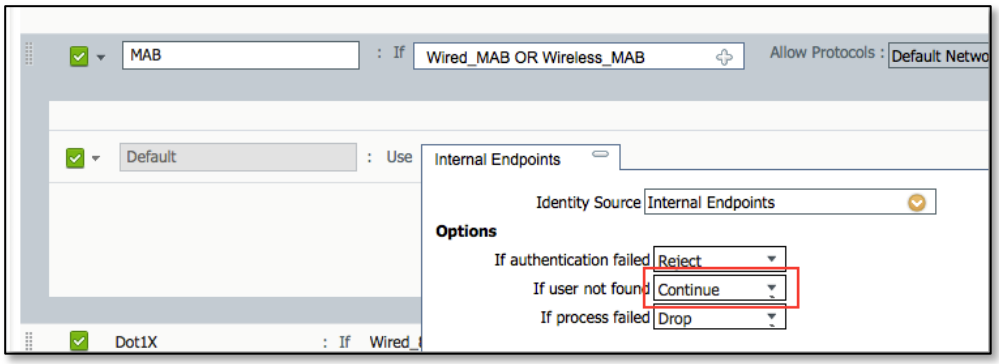

図 41 デフォルトの認証ポリシー

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

エンドポイントは、初めてネットワークにアクセスする際、MAB でユーザ認証され、認証用のゲスト ポータルにリダイレクトされる必要があります。ISE 2.0 には Cisco_WebAuth と呼ばれる組み込みプロファイルが付属しています。ゲストのインストールを使用するために、これを変更します。

手順 1 [ポリシー(Policy)] > [ポリシー要素(Policy Elements)] > [結果(Results)] に移動します。
手順 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。
手順 3 [Cisco_WebAuth] を選択します。
手順 4 セットアップの作業用にプロファイルを変更します。

- [Web リダイレクト(Web Redirection)] の下で、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、guest-redirect を使用します。

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。

- **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。

手順 5 [保存(Save)] 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

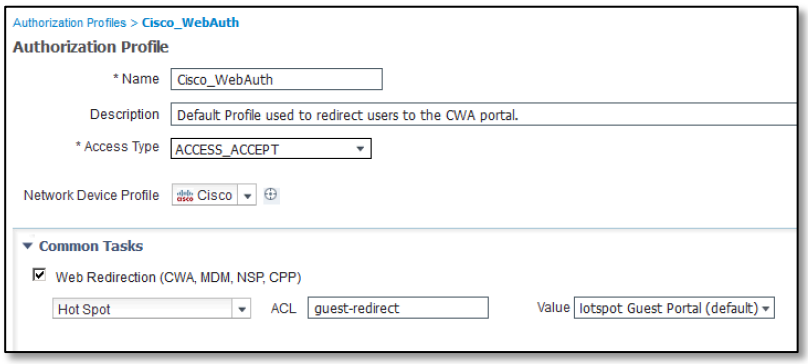

図 42 ホットスポットの認証プロファイル

クレデンシャルを持つリダイレクトの例

図 43 クレデンシャルを持つリダイレクト用認証プロファイル

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。

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

手順 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。

手順 3　[追加(Add)] をクリックします。

- 新しい認証プロファイルの画面が表示されます。

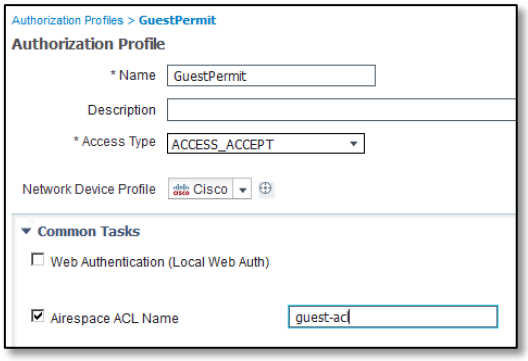

図 44 Guest Permit 用の認証プロファイル

手順 4　**図 44** 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されました。

手順 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。ISE 2.0 には組み込みルールが含まれていて、これをセットアップで使用するように変更します。

手順 1　[ポリシー(Policy)] > [認証(Authorization)] に移動します。
手順 2　[Wi-Fi_Redirect_to_Guest_Login] ルール行の [編集(Edit)] をクリックします。
手順 3　行の左側の [状態(Status)] をクリックし、プルダウンして [有効(Enabled)] に変更します。
手順 4　[完了(Done)] をクリックします。
手順 5　[Wi-Fi_Redirect_to_Guest_Login] ルール行の [編集(Edit)] の横にある矢印をクリックします。
手順 6　**新規ルールをその上に**挿入します。
手順 7　**図 45** に示すように、これまでの設定に合う新規ルールを追加します。

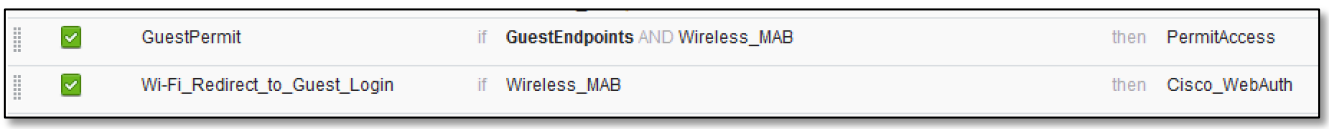

図 45 認証ポリシーのルール

手順 8　2 つ目の許可ルールを作成します。

手順 9　ルールに **GuestPermit** という名前を付けます。
手順 10　**GuestEndpoint** かつ **Wireless_MAB** の場合に選択します。
手順 11　[GuestPermit] 認証プロファイルを選択します。
手順 12　[完了(Done)] をクリックします。
手順 13　[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。

キー ポイント:前述で使用される設定はエンドポイント グループに基づいている簡易認証です。ユーザまたはデバイスがネットワークに入ります。AUP (ホットスポット)を受け入れるか、デバイスが GuestEndpoints に登録されているいくつかのクレデンシャル(資格情報を持ったフロー)を入力します。その後、そのエンドポイント グループに基づいてアクセスできるようになります。デバイスを手動で削除するか、または 30 日間のマーク(デフォルト設定)を通過するまで、ユーザまたはデバイスが AUP を受け入れるため、またはポータルに再度ログインするためのリダイレクトはされません。

消去日を変更する場合は、__ 日に到達したときに、この ID グループの設定の消去エンドポイントを設定します。

- ホットスポットのフローは、「Portal Settings for Hotspot Guest Portals」で設定されています。
- 資格情報を持ったフローは、ゲスト タイプを使用して実行されます。「Create or Edit Guest Types」を参照してください。

資格情報を持ったゲスト フローのネットワークへのアクセス許可の別のオプションは、ゲスト フローまたはゲスト タイプの認証ルールに基づいてネットワークにアクセスできるようにすることです。この設定は、ゲスト タイプの設定でユーザを制限することができます。例:最大アカウント有効期間、日時のみへのアクセス許可、最大同時ログインなど。「Create or Edit Guest Types」で説明しています。

このため、新しいネットワーク セッションになるたびにユーザがポータルにログインする必要があります。たとえば、WLC ユーザのアイドル タイムアウト値(デフォルトは 180 秒)で設定するときに、ユーザはデバイスを利用してスリープ、再開して、新しいワイヤレス セッション ID を取得します。

この設定は、資格情報を持つフロー専用です。
図 46 に表示される最初の例は、あらゆるタイプのゲストもゲスト フローによってネットワークに許可する単純な方式です。このフローは内蔵されていますが、ゲスト許可の認証プロファイルを使用する Wi-Fi_Guest_access のアクセス許可を変更します。
図 47 に表示される 2 番めの例は、ゲスト タイプによって、アクセス権を付与します。契約者には、通常のゲストに比べ、特別なアクセス権があります。

✓	Wi-Fi_Guest_Access	if	(GuestType_Daily (default) OR GuestType_Weekly (default) OR GuestType_Contractor (default)) AND (Guest_Flow AND Wireless_MAB)	then	GuestPermit AND Guests
✓	Wi-Fi_Redirect_to_Guest_Login	if	Wireless_MAB	then	Cisco_WebAuth
✓	Basic_Authenticated_Access	if	Network_Access_Authentication_Passed	then	PermitAccess
✓	Default	if no matches, then	DenyAccess		

図 46 基本のゲスト フロー用認証ルール

☑	GuestPermit	if	**GuestType_Contractor (default)** AND Network Access:UseCase EQUALS Guest Flow	then	ContractorPermit
☑	GuestPermit_copy	if	**GuestType_Daily (default)** AND Network Access:UseCase EQUALS Guest Flow	then	GuestPermit
☑	GuestRedirect	if	Wireless_MAB	then	GuestRedirect

図 47 ゲスト タイプ別の認証ルール

ポータルが稼働するのに必須の手順を完了しました。

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、「ポータルの基本的なカスタマイズの設定（任意）」の項までスキップできます。

自己登録またはスポンサー フロー（資格情報を持つゲスト アクセス）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最小限の設定」に進んでください。

図 48 は、資格情報を持ったゲスト フローを設定するのに使用するプロセスを示します。

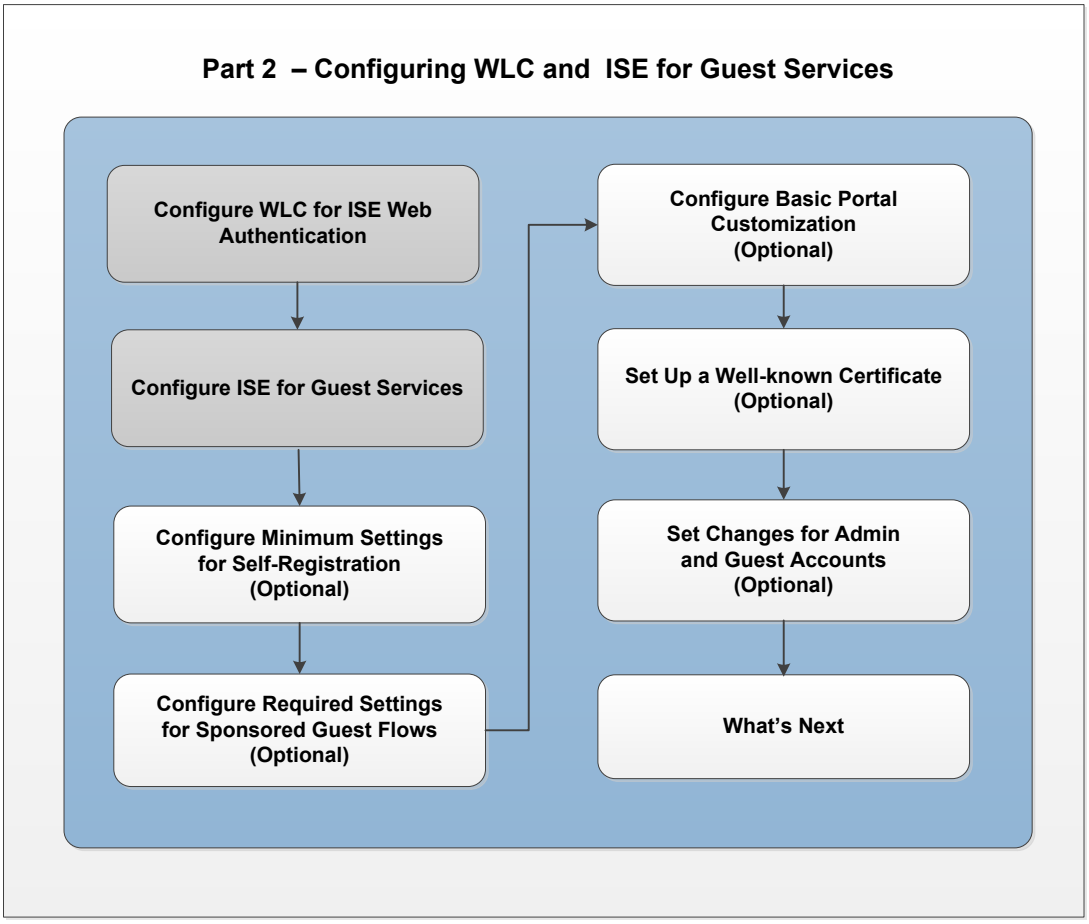

図 48 資格情報を持ったアクセスの ISE の設定

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

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。必要な設定は、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です。

注:これはとても重要です。ロケーションを設定しない場合、アカウントは正しい時刻に有効化されません。ユーザはログインできなくなります。

また、ISE サーバの時間が正しいことを確認する必要があります。使用しているブラウザよりも数分速いだけの場合、自己登録またはスポンサー フローを使用して作成されたアカウントで動作を開始するのに数分かかることがあります。

ゲスト ポータルを使用しているエンド ユーザに表示されるメッセージは、「認証に失敗しました(Authentication failed)」です。

ISE の [運用(Operations)] > [認証(Authentications)] で、アカウントがまだアクティブでないことを示すエントリの詳細が表示されます。

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 つだけ設定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 タイム ゾーンの導入は、ISE に構築されているサンノゼのロケーションを使用できます。このタイム ゾーンが許容範囲内の場合、「スポンサー ゲストのフローに必要な設定」の項にスキップします。

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、アドミニストレータ ガイドの「Assign Guest Locations and SSIDs」を参照してください。

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。

手順 1 [ゲスト アクセス(Guest Access)] > [設定(Settings)] > [ゲスト ロケーションと SSID(Guest Locations and SSIDs)] の順に選択します。

手順 2 **図 49** 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。

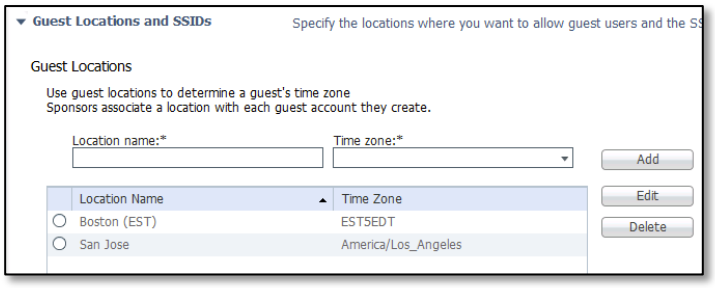

図 49 ゲストのロケーションの設定

手順 3 **ロケーション名およびタイム ゾーン**を入力します。例：EST5EDT を使用するボストン（EST）またはアメリカ/ニューヨーク。

注：サンノゼのロケーションは削除しないでください。

手順 4 [追加（Add）] をクリックします。

手順 5 [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（自己登録）

この新しく追加されたロケーションを使用するには、自己登録ポータルを設定する必要があります。自己登録を使用していない場合、以下の「スポンサー ゲストのフローに必要な設定」の項にスキップしてください。それ以外は、「既知の証明書の設定（任意）」の項を続けてください。

注：デフォルトのサンノゼ（PST 時間）が許容範囲内の場合は、この項をスキップしても構いません。

手順 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。

手順 2 自己登録したゲスト ポータルを選択します。

手順 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。

手順 4 **図 50** に示すように、自己登録ページの設定の [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。

手順 5 [追加（Add）] をクリックします。

手順 6 [送信（Submit）] をクリックします。

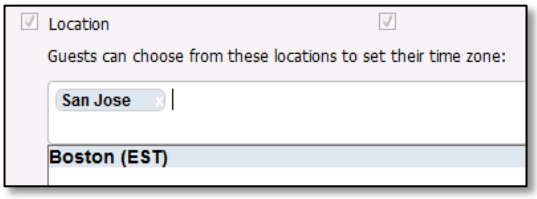

図 50 ゲスト ポータルの選択ロケーション

スポンサー ゲストのフローに必要な設定

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（任意）」の項に移動してください。

スポンサー アカウントの設定

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 と統合する場合は、「Active Directory のスポンサー アカウントの使用」の項に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。

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

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 グループを含む 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。

手順 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。
手順 2 [Active Directory] を選択します。
手順 3 **図 51** に示すように、[追加（Add）] をクリックします。

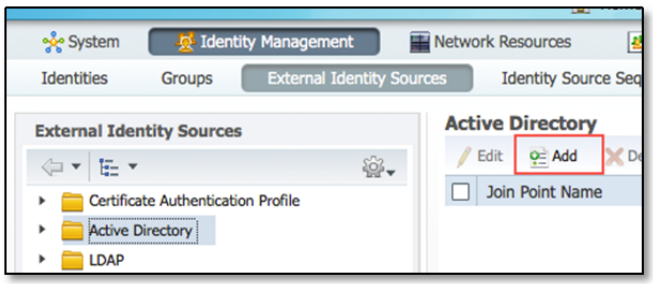

図 51 Active Directory 参加ポイントの追加

手順 4　図 **52** に示すように、参加ポイント名および Active Directory ドメインを入力します。

手順 5　[送信（Submit）] をクリックします。

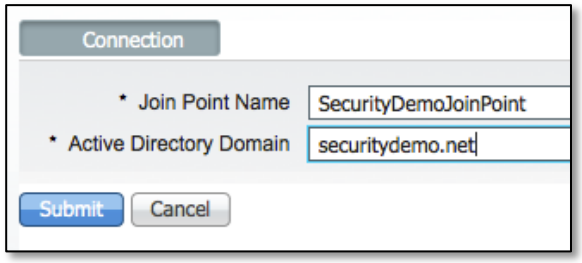

図 52 参加ポイント接続の設定

手順 6　「Active Directory ドメインにすべての ISE ノードを参加させますか（Would you like to Join all ISE Nodes to the Active Directory Domain）」というメッセージが表示されたら、[はい（Yes）] をクリックします。

手順 7　ドメインに参加するためのクレデンシャルを入力するように求められます。これには、組織ユニットの指定も含まれます（任意）。要求される内容の詳細については情報ボタンを参照してください。

注:ドメイン クレデンシャルは ISE によって保存されません。これはマシン アカウントの初期接続を設定するために 1 回使用します。

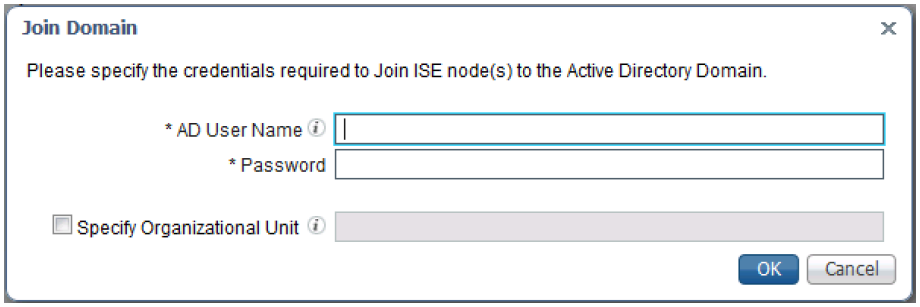

図 53 AD ドメインの参加

手順 8　図 **54** に示すように成功メッセージが表示されます。[閉じる（Close）] をクリックします。

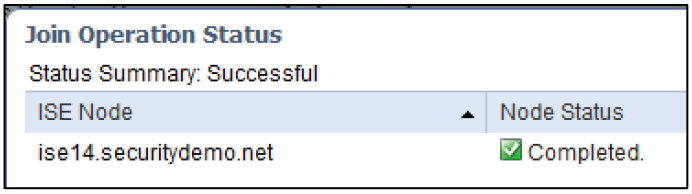

図 54 操作ステータスの参加

手順 9　[グループ（Groups）] タブをクリックします。

手順 10　図 **55** に示すように、[追加（Add）] をクリックして、[ディレクトリからグループを選択（Select Groups From Directory）] を選択します。

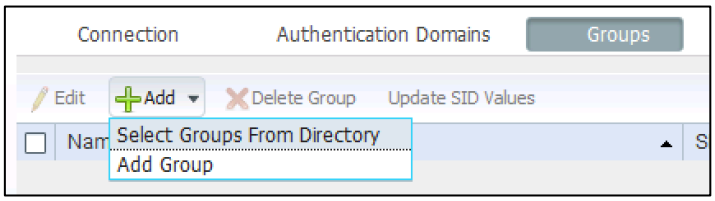

図 55 AD からグループの選択

手順 11　図 **56** に示すように、[グループを取得（Retrieve Groups）] をクリックします。

手順 12　ゲストのスポンサーになるユーザを含むグループを選択した後、ページ下部の [OK] をクリックします。

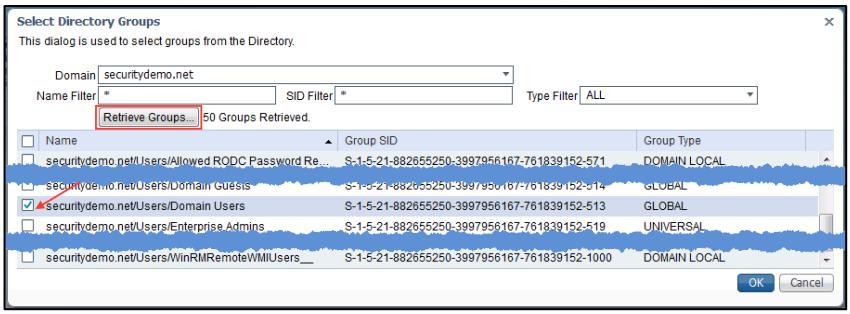

図 56 Directory Groups の選択

手順 13　グループを選択すると、画面は**図 57** のようになります。この [グループ（Groups）] ページ下部の [保存（Save）] をクリックします。

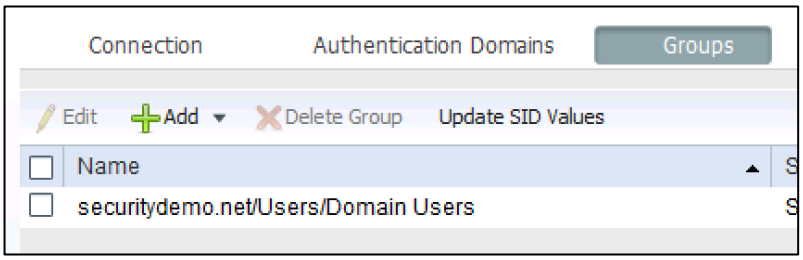

図 57 グループ

スポンサー グループに割り当てる場合に使用できる Active Directory グループのセットアップが完了しました。

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。

手順 1 [ゲスト アクセス(Guest Access)] > [設定(Configure)] > [スポンサー グループ(Sponsor Groups)] > [ALL_ACCOUNTS] の順に移動します。

- **図 58** 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。

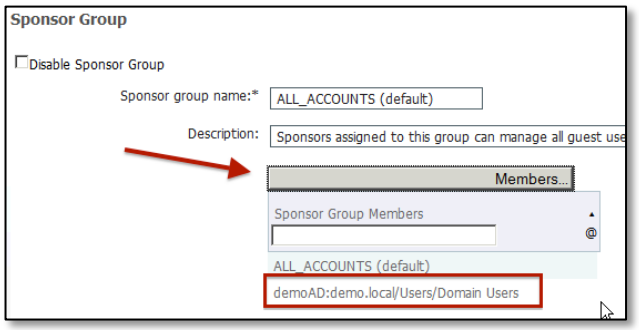

図 58 スポンサー グループ メンバーの選択

手順 2 [メンバー(Member)] をクリックし、図 36 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。

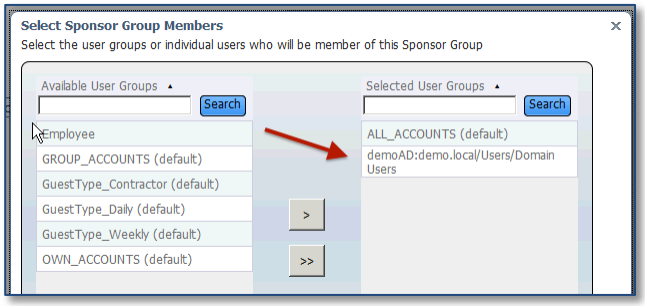

図 59 スポンサー グループ メンバーの選択

手順 3 [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してよい場合は、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。

手順 1 **図 60** 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)] の項から選択します。

手順 2　必要のないロケーションを削除します。

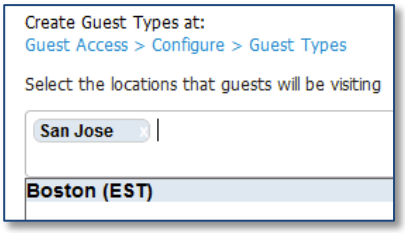

図 60 ゲスト タイプのロケーションの選択

手順 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。
手順 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(Portal Test 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(**これはデフォルトです**)

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

複雑な URL または簡単な URL にアクセスする方法を表示するには、次の手順を実行します。

手順 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。
手順 2　[スポンサーポータル(デフォルト)(Sponsor Portal (default))] をクリックすると、**図 61** に示すように [ポータル設定(Portal Settings)] ペインが表示されます。

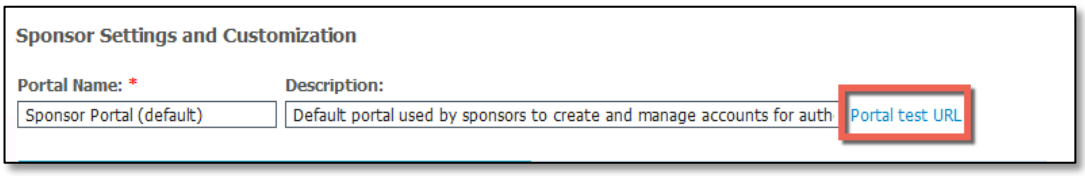

図 61 スポンサー設定

手順 3　[ポータルテスト URL(Portal test URL)] をクリックすると、新しいブラウザ ウィンドウが開きます。

注:これは、FQDN ポータル名について次の手順に進まなければ、スポンサーへの送信が必要になる URL 例です。
「https://ise.securitydemo.net:8443/sponsorportal/PortalSetup.action?portal=28981f50-e96e-11e4-a30a-005056bf01c9」

手順 4　[ポータルテスト URL（Portal Test URL）] ウィンドウを閉じます。

手順 5　[ポータル設定（Portal Settings）] で、**図 62** で示すように [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。

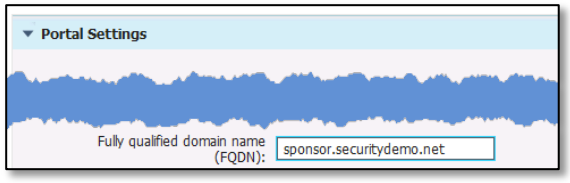

図 62 [ポータル設定（Portal Settings）] > [FQDN]

手順 6　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** 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。

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。ポータルをカスタマイズする必要がない場合は、「既知の証明書の設定（任意）」の項に進んでください。

ゲストのカスタマイズの詳細については、アドミニストレータ ガイドの「Customize End-User Web Portals」の項と設計ガイドのサイトで「**HowTo: ISE Web Portal Customization Options**」を参照してください。

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。

手順 1　[ゲスト アクセス（Guest Access）] > [設定（Configure）] > [ゲストポータル（Guest Portals）] の順にクリックします。

手順 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 63** 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。

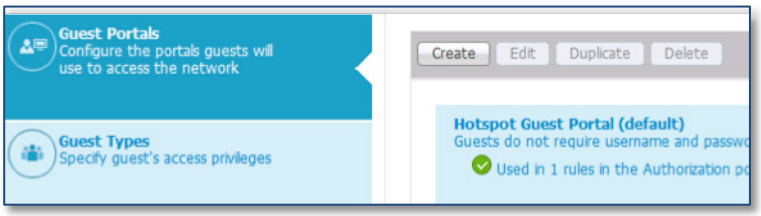

図 63 アクティブなホットスポット ポータル

手順 3　**図 64** 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）] の項をクリックします。

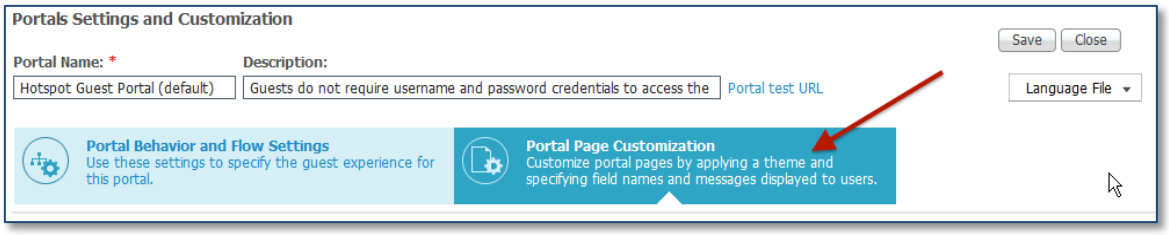

図 64 [ポータルページのカスタマイズ（Portal Page Customization）]

- ISE 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しませんが、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。

手順 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 65** に示すように [調整(Tweaks)] を使用して色を変更します。

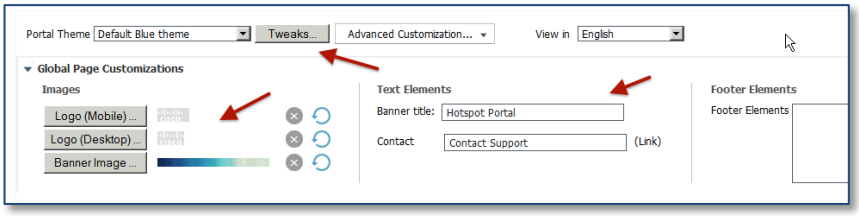

図 65 ページのカスタマイズ オプション

手順 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 UI のメイン セクションの下で、全体的なルック アンド フィールを調整できます。また、各ページも調整できます。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。

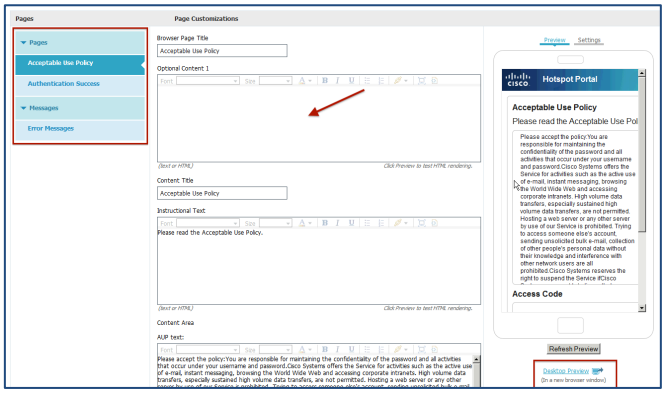

図 66 ポータル カスタマイゼーション ミニ エディタおよびプレビュー

手順 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** を使用して、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。

手順 7 デスクトップ プレビュー ブラウザ ウィドウを閉じます。

手順 8 ページ最上部にある [保存(Save)] をクリックします。**図 67** を参照してください。

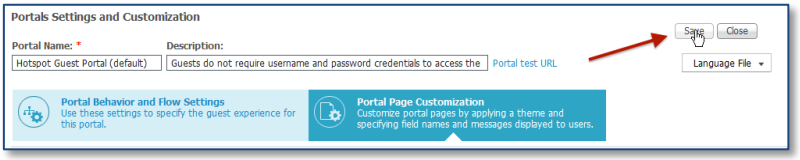

図 67 カスタマイズの保存

ゲスト ポータルの基本的なカスタマイズが完了しました。スポンサー ゲスト アクセスを使用すると、スポンサー ポータルで同じことを行うことができます。これを行うには、[ゲストアクセス(Guest Access)] > [設定(Configure)] > [スポンサーポータル(Sponsor Portals)] > [デフォルトポータルの選択(Select the default portal)] に移動し、ゲスト ポータルをカスタマイズするために使用したのと同じ手順に従います。

次の項「既知の証明書の設定(任意)」に進むか、「次のステップ」にスキップできます。

既知の証明書の設定（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が、強く推奨します。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。

ここでこの項をスキップして、「次のステップ」の項に進むことができます。最小設定を行いました。

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」
- Aaron Woland のハウツーガイド：「HowTo: Implement Cisco ISE and Server Side Certificates」

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

手順 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。

手順 2 [証明書署名要求（CSR）の生成（Generate Certificate Signing Requests (CSR)）] をクリックします。

手順 3 **図 68** に示すように、**CSR** を生成するための**値**を入力します。

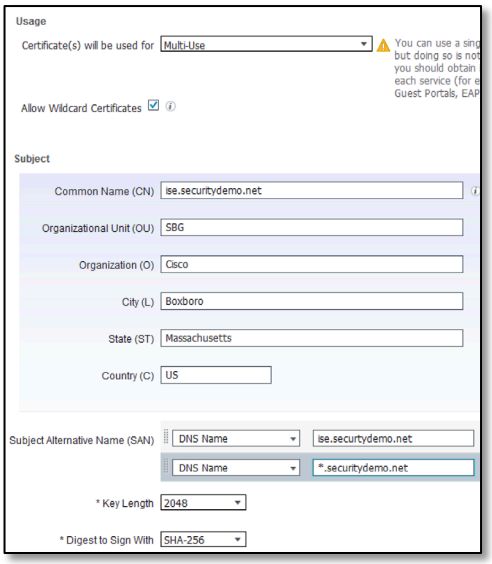

図 68 CSR を生成する情報の入力

使用方法（Usage）

- [証明書の用途（Certificate(s) will be used for）]：[複数使用（Multi-Use）]
- [ワイルドカードの証明書を許可（Allow Wildcard Certificates）]：**オン**

サブジェクト（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。

手順 4　[Generate（生成）] をクリックして CSR を生成します。**図 69** に示すように、CSR が生成されます。

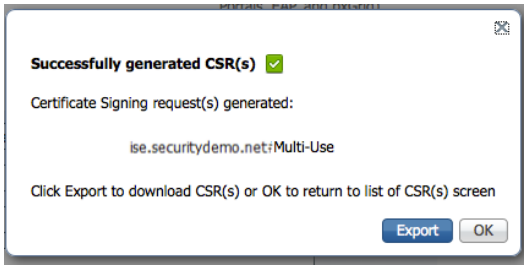

図 69 正常に生成された CSR

手順 5　[エクスポート（Export）] をクリックしてファイルを保存します。

手順 6　テキスト エディタでこの**ファイル**を開きます。

手順 7　「---- 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。

手順 8　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 70 に SSL.com ポータルを示します。

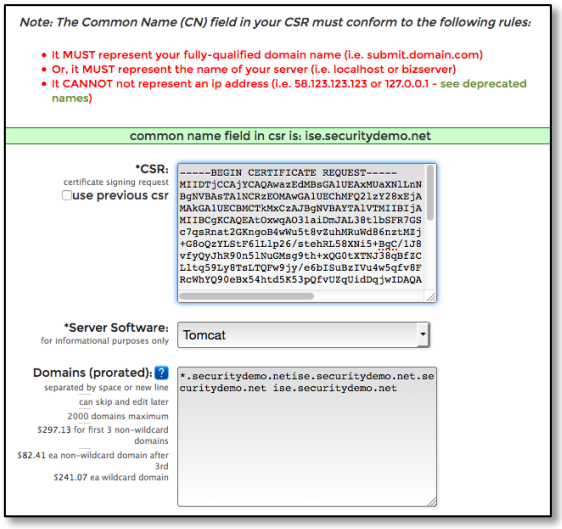

図 70 SSL.com ポータル

手順 9　**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。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。

信頼できる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。

手順 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。

手順 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

手順 3 図 71 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 71 ストアへの新しい証明書のインポート

手順 4 次の証明書をインポートするには、次の手順を使用してください。

- **ルート CA**:AddTrustExternalCARoot.crt
- **下位 CA**:SSLcomDVCA_2.crt
- **下位 CA**:USERTrustRSAAddTrustCA.crt

手順 5 [参照(Browse)] をクリックして、**ルート CA 証明書**を選択します。
手順 6 **わかりやすい名前**を入力します。
手順 7 CA によって**返されたルート証明書**を選択します。
手順 8 [信頼の目的:(Trusted For:)] で、[ISE での認証のために信頼する(Trust for Authentication within ISE)] および [クライアント認証および Syslog のために信頼する(Trust for client authentication and Syslog)] のボックスをオンにします。
手順 9 [証明書の拡張の検証(Validate Certificate Extensions)] を選択することも推奨します。
手順 10 **説明**を入力します。
手順 11 [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とり、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キーとのペアが作成されます。

手順 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。
手順 2 **署名要求**のエントリを選択します。
手順 3 図 72 に示すように、[証明書のバインド(Bind Certificate)] をクリックします。

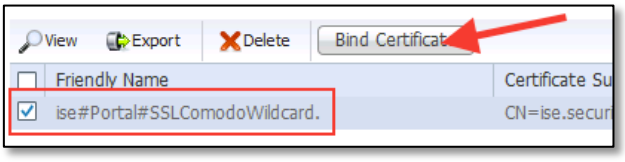

図 72 バインドする証明書の選択

手順 4 [参照(Browse)] をクリックし、CA 署名付き証明書を選択します。

手順 5 証明書の**わかりやすい名前**を指定します。

手順 6 [使用方法(Usage)] で、次のオプションをオンにします。[管理(Admin)]、[EAP認証(EAP Authentication)]、[ポータル(Portal)]

手順 7 [ポータルグループタグ(Portal Group Tag)] では、[デフォルトのポータル証明書グループ(Default Portal Certificate Group)] を選択します。

手順 8 **図 73** 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。

[送信(Submit)] をクリックすると、システムが再起動され、最大で 5 分間使用できなくなります。

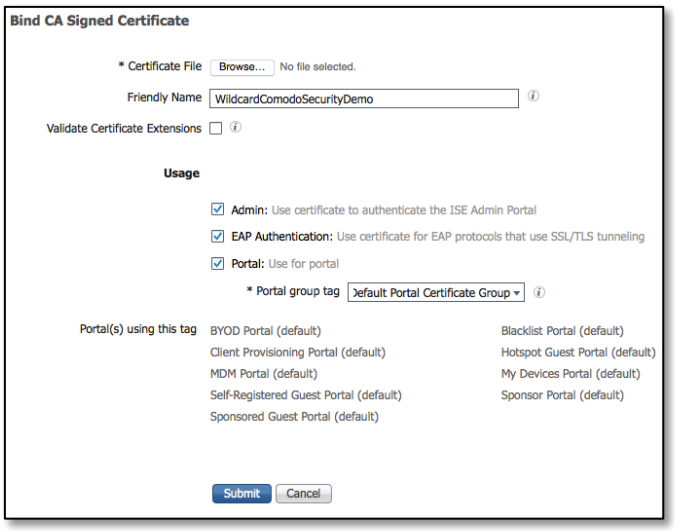

図 73 署名付き証明書のバインド

ISE 2.0 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、『*Cisco ISE 2.0 Administration Guide*』の「Managing Certificates」の項を参照してください。

管理者およびゲスト アカウントの変更の設定（任意）

システムが起動したら、次のアカウントのデフォルト設定を変更することを推奨します。

- ロックアウトを回避するために管理者アカウントのパスワード ポリシーをよく読んでおいてください。
- ユーザが管理とログインをより簡単にできるようにするゲストのデフォルト ユーザ名とパスワードの要件を設定します。

管理者パスワード ポリシーの習得

ISE を設定する場合の一般的な問題は、一定期間使用しない場合、管理者アカウントの設定を変更するのを忘れて最終的にシステムからロックアウトされることです。それらを理解し、システムに一定期間アクセスしない場合は、ロックされないように、要件について把握しておくことを推奨します。

[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [パスワードポリシー（Password Policy）] に移動します。

必要に応じて設定を変更します。たとえば、パスワード ライフタイムは**期限切れの行のチェックボックスをオフにするか、または拡張**します。

ゲスト アカウント要件の変更

個別に、ISE ゲスト ソリューションには、非常に困難なパスワードの設定があります。これらのパスワードは、長くて複雑なため記憶するだけでなく、書き留めておくのも困難です。ユーザ エクスペリエンスをより良くするためにこれらの設定を変更できます。また、デバイスによっては、文字「O、l」と数字「0、1」の違いを理解しづらいため、ユーザが認証を失敗する原因になります。文字数を減らして簡単にしつつ、少し混ぜあわせて複雑にしておくこともできます。

手順 1 [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）] の順に選択して、ポリシーごとに、**図 74** に示すように更新します。

手順 2 [ユーザ名の最小長（Minimum username length）] を **4** に変更します。

手順 3 [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）] の下を次のように変更します。

- 英字
  - 「l」および「O」を削除する
  - 最小を 3 に変更する

- 数値
  - 「1」および「0」を削除する
  - 最小を 3 に変更する

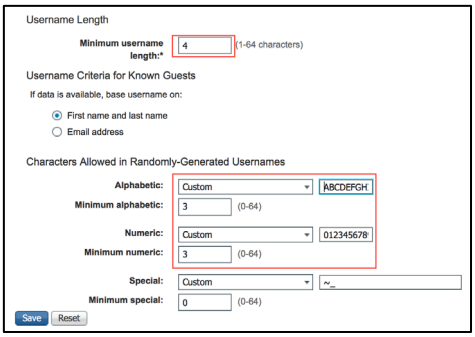

図 74 ユーザ名のポリシー

手順 4 [保存(Save)] をクリックします。

手順 5 [ゲスト パスワード ポリシー(Guest Password Policy)] に移動して、**図 75** に示すように変更します。

- パスワードの長さ:4 に設定する
- 小文字、大文字の最小数:0 に設定する
- 最小値:4 に設定する
- 最小特殊文字数:0 に設定する

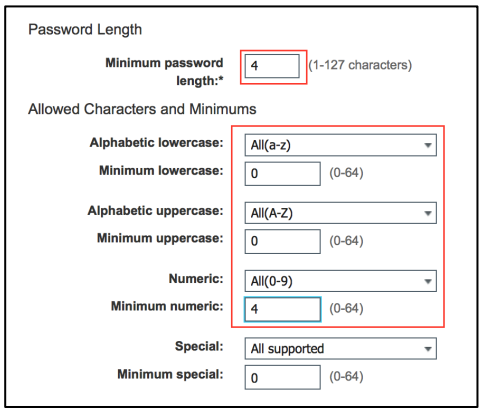

図 75 パスワード ポリシー

手順 6 [保存(Save)] をクリックします。

次のステップ

ISE サーバを設定したら、機能していることを検証するために次を実行する必要があります。

ホット スポット ゲスト フローの場合

手順 1 **ゲスト SSID** に接続します。
手順 2 **ホットスポット ポータル**にログインします。

自己登録ゲスト フローの場合

手順 1 **ゲスト SSID** に接続します。
手順 2 [アカウントを持っていない（Don't have an Account）] をクリックし、ゲスト アカウントを作成します。
手順 3 **自己登録ポータル**にログインします。

スポンサー ゲスト フローの場合

手順 1 内部ネットワークでマシンを使用して、**スポンサー ポータル** http://sponsorportal.yourdomain.com に接続するか、またはスポンサー ポータル アクセスのポータル テストの URL を使用します。これについては、「ISE スポンサー ポータルの FQDN ベースのアクセスの設定」で説明しています。
手順 2 **スポンサー アカウント**を使用してログインします。
手順 3 **ゲスト アカウント**を作成します。
手順 4 別のクライアントを使用して、**ゲスト SSID** に接続します。
手順 5 **新しく作成されたゲスト アカウント**を使用してログインします。

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。

ワイヤレス コントローラの一般的な推奨構成については、「How-to:Universal WLC Config」を参照してください。

付録 A:ワイヤレスの構成

WLAN Express セットアップ実行後、ISE ワイヤレス ゲスト セットアップ ウィザードがワイヤレス システムに追加するコマンドを次に示します。

```
'config network web-auth captive-bypass enable'
'reset system'

—REBOOT—

'config radius auth add 1 {ISE IP} 1812 ascii {RADIUS SECRET}',
'config radius auth disable 1',
'config radius auth retransmit-timeout 1 5',
'config radius auth rfc3576 enable 1',
'config radius auth network 1 enable',
'config radius auth management 1 disable',
'config radius auth enable 1',
'config radius acct add 1 {ISE IP} 1813 ascii {RADIUS SECRET}',
'config radius acct disable 1',
'config radius acct retransmit-timeout 1 5',
'config radius acct network 1 enable',
'config radius acct enable 1',
'config acl create guest-redirect',
'config acl rule add guest-redirect 1',
'config acl rule destination port range guest-redirect 1 0 65535',
'config acl rule action guest-redirect 1 permit',
'config acl rule source port range guest-redirect 1 53 53',
'config acl rule direction guest-redirect 1 out',
'config acl rule protocol guest-redirect 1 17',
'config acl rule add guest-redirect 2',
'config acl rule destination port range guest-redirect 2 53 53',
'config acl rule action guest-redirect 2 permit',
'config acl rule source port range guest-redirect 2 0 65535',
'config acl rule direction guest-redirect 2 in',
'config acl rule protocol guest-redirect 2 17',
'config acl rule add guest-redirect 3',
'config acl rule destination port range guest-redirect 3 0 65535',
'config acl rule destination address guest-redirect 3 {ISE IP} 255.255.255.255',
'config acl rule action guest-redirect 3 permit',
'config acl rule source port range guest-redirect 3 0 65535',
'config acl rule add guest-redirect 4',
'config acl rule destination port range guest-redirect 4 0 65535',
'config acl rule action guest-redirect 4 permit',
'config acl rule source port range guest-redirect 4 0 65535',
'config acl rule source address guest-redirect 4 {ISE IP} 255.255.255.255',
'config acl rule add guest-redirect 65',
'config acl rule destination port range guest-redirect 65 0 65535',
'config acl rule source port range guest-redirect 65 0 65535',
'config acl apply guest-redirect',
'config acl create guest-acl',
'config acl rule add guest-acl 1',
'config acl rule destination port range guest-acl 1 53 53',
'config acl rule action guest-acl 1 permit',
'config acl rule source port range guest-acl 1 0 65535',
'config acl rule protocol guest-acl 1 17',
'config acl rule add guest-acl 2',
'config acl rule destination port range guest-acl 2 0 65535',
'config acl rule action guest-acl 2 permit',
```

```
'config acl rule source port range guest-acl 2 53 53',
'config acl rule protocol guest-acl 2 17',
'config acl rule add guest-acl 3',
'config acl rule destination port range guest-acl 3 0 65535',
'config acl rule destination address guest-acl 3 {ISE IP} 255.255.255.255',
'config acl rule action guest-acl 3 permit',
'config acl rule source port range guest-acl 3 0 65535',
'config acl rule add guest-acl 4',
'config acl rule destination port range guest-acl 4 0 65535',
'config acl rule action guest-acl 4 permit',
'config acl rule source port range guest-acl 4 0 65535',
'config acl rule source address guest-acl 4 {ISE IP} 255.255.255.255',
'config acl rule add guest-acl 5',
'config acl rule destination port range guest-acl 5 0 65535',
'config acl rule destination address guest-acl 5 {GATEWAY IP} 255.255.255.255',
'config acl rule action guest-acl 5 permit',
'config acl rule source port range guest-acl 5 0 65535',
'config acl rule add guest-acl 65',
'config acl rule destination port range guest-acl 65 0 65535',
'config acl rule source port range guest-acl 65 0 65535',
'config acl apply guest-acl',
'config wlan disable {WLAN ID}',
'config wlan exclusionlist {WLAN ID} 60',
'config wlan flexconnect local-switching {WLAN ID} disable',
'config wlan security wpa akm 802.1x disable {WLAN ID}',
'config wlan security wpa wpa2 ciphers aes disable {WLAN ID}',
'config wlan security wpa wpa2 disable {WLAN ID}',
'config wlan security wpa disable {WLAN ID}',
'config wlan security web-auth server-precedence {WLAN ID} local radius ldap',
'config wlan security web-auth disable {WLAN ID}',
'config wlan security web-passthrough disable {WLAN ID}',
'config wlan aaa-override enable {WLAN ID}',
'config wlan mac-filtering enable {WLAN ID}',
'config wlan broadcast-ssid enable {WLAN ID}',
'config wlan session-timeout {WLAN ID} 1800',
'config wlan mfp client enable {WLAN ID}',
'config wlan radius_server auth add {WLAN ID} 1',
'config wlan radius_server acct add {WLAN ID} 1',
'config wlan wmm allow {WLAN ID}',
'config wlan nac radius enable {WLAN ID}',
'config wlan acl {WLAN ID} none',
'config wlan ipv6 acl {WLAN ID} none',
'config wlan radius_server acct interim-update 0 {WLAN ID}',
'config wlan radius_server acct interim-update enable {WLAN ID}',
'config wlan ccx AironetIeSupport disable {WLAN ID}',
'config wlan profiling radius all enable {WLAN ID}',
'config wlan enable {WLAN ID}',
'save config'
```

Guest-acl screenshot example:

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	10.1.100.37 / 255.255.255.255	Any	Any	Any	Any	Any	0	
4	Permit	10.1.100.37 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0	
5	Permit	0.0.0.0 / 0.0.0.0	10.1.100.1 / 255.255.255.255	Any	Any	Any	Any	Any	0	
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0	
7	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0	
8	Deny	0.0.0.0 / 0.0.0.0	10.1.100.0 / 255.255.255.0	Any	Any	Any	Any	Inbound	0	
9	Deny	10.1.100.0 / 255.255.255.0	10.1.20.0 / 255.255.255.0	Any	Any	Any	Any	Any	0	
10	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	0	
11	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	0	
12	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0	
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0	

付録 B: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
!
vlan 90
 name access-points
!
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 90
 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 Vlan90
 ip address 10.1.90.1 255.255.255.0
 ip helper-address 10.1.100.10
!
interface Vlan100
 ip address 10.1.100.1 255.255.255.0
```