ISE バージョン 1.3 の自己登録したゲスト ポータルの設定例

目次

概要

Cisco Identity Services Engine （ ISE ）バージョン 1.3 にネットワークリソースへのアクセス権を得るときゲストユーザ自己レジスタを可能にする自己によって登録されているゲスト ポータルと呼ばれるゲスト ポータルの新型があります。 このポータルは複数の機能を設定し、カスタマイズすることを可能にします。 このドキュメントでは、この機能の設定とトラブルシューティングの方法を説明します。

前提条件

要件

ISE 構成の経験と、次のトピックに関する基本的な知識があることが推奨されます。

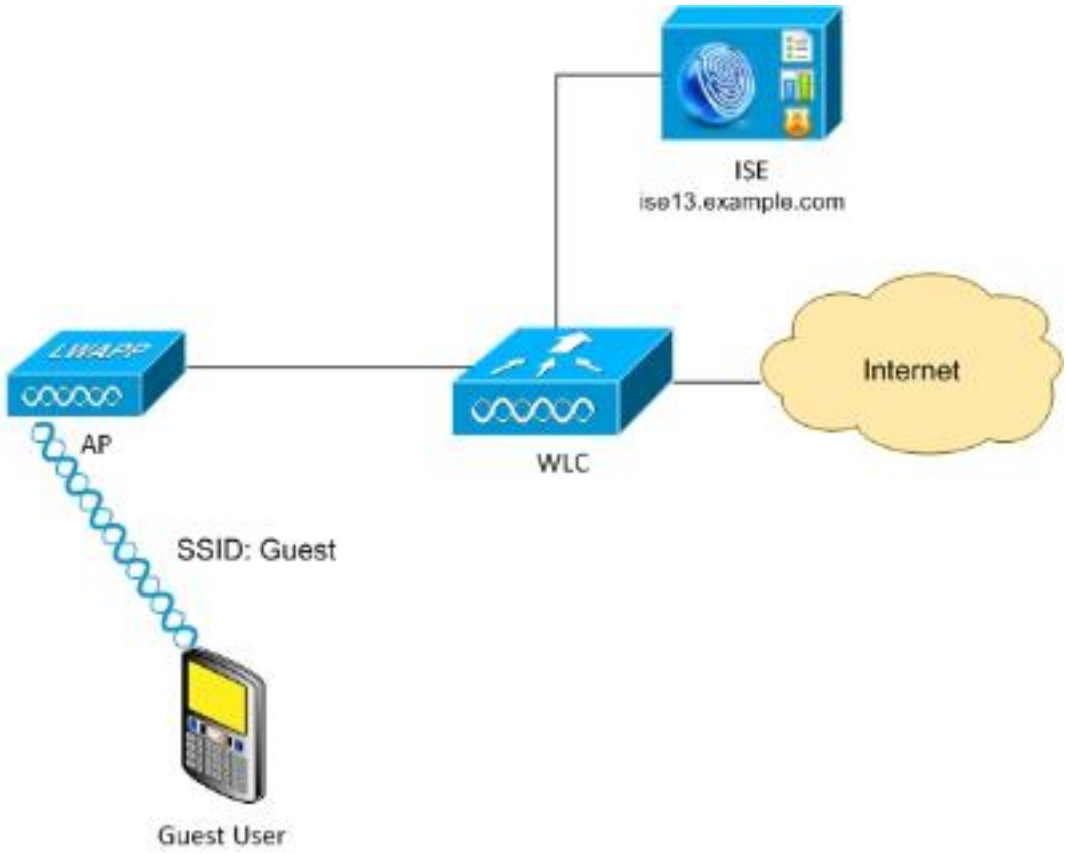
- ISE の導入およびゲスト フロー
- ワイヤレス LAN コントローラ（WLC）の設定

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Microsoft Windows 7
- Cisco WLC バージョン 7.6 以降
- ISE ソフトウェア、バージョン 3.1 および それ 以降

トポロジとフロー



このシナリオは自己登録を行うときゲストユーザ向けに利用可能な複数のオプションを示します。

一般的なフローはここにあります:

ステップ 1：ゲスト ユーザがサービス セット識別子（SSID）：ゲスト。 これは、認証に ISE を使用する MAC フィルタリングが設定されたオープン ネットワークです。 この認証はゲスト自己によって登録されているポータルに ISE の第 2 承認規則および許可プロファイル リダイレクトを一致させます。 ISE から、2 つの cisco-av-pairs を使用した RADIUS Access-Accept が返されます。

- url-redirect-acl（リダイレクトする必要があるトラフィック、および WLC でローカルに定義されたアクセス コントロール リスト（ACL）の名前）
- url-redirect（そのトラフィックのリダイレクト先 - ISE）

ステップ 2： ゲストユーザは ISE にリダイレクトされます。 信任状ログインを提供しなさいよりもむしろ、ユーザは"Donot have a account"を クリックする。 ユーザはそのアカウントが作成することができるページにリダイレクトされます。 オプションの秘密登録コードはだれがその秘密の値を知っているか民を住まわせる自己登録特権を制限するためイネーブルになるであるかもしれません。 アカウントが作成された後、ユーザは提供された信任状（ユーザ名 および パスワード）で、それらの信任状と ログオンします。

ステップ 3. ISE は WLC に許可（CoA）の RADIUS 変更を再認証します送信 します。 WLC は承認だけ属性の RADIUS Access-Request を送信 するときユーザを再認証します。 ISE はインターネットだけへのアクセスを提供する WLC でローカルで定義される Access-Accept および Airespace ACL と応答します（ゲストユーザ向けの最終的なアクセスは承認ポリシーによって異なります）。

EAP セッションが要求元と ISE の間にあるので Extensible Authentication Protocol（EAP）セッションのために、再認証を誘発するために ISE が終わる CoA を送信 する必要があることに注目して下さい。 しかし MAB（MAC フィルタリング）のために、CoA Reauthenticate 十分です; 無線クライアントを非 associate/de 認証する必要がありません。

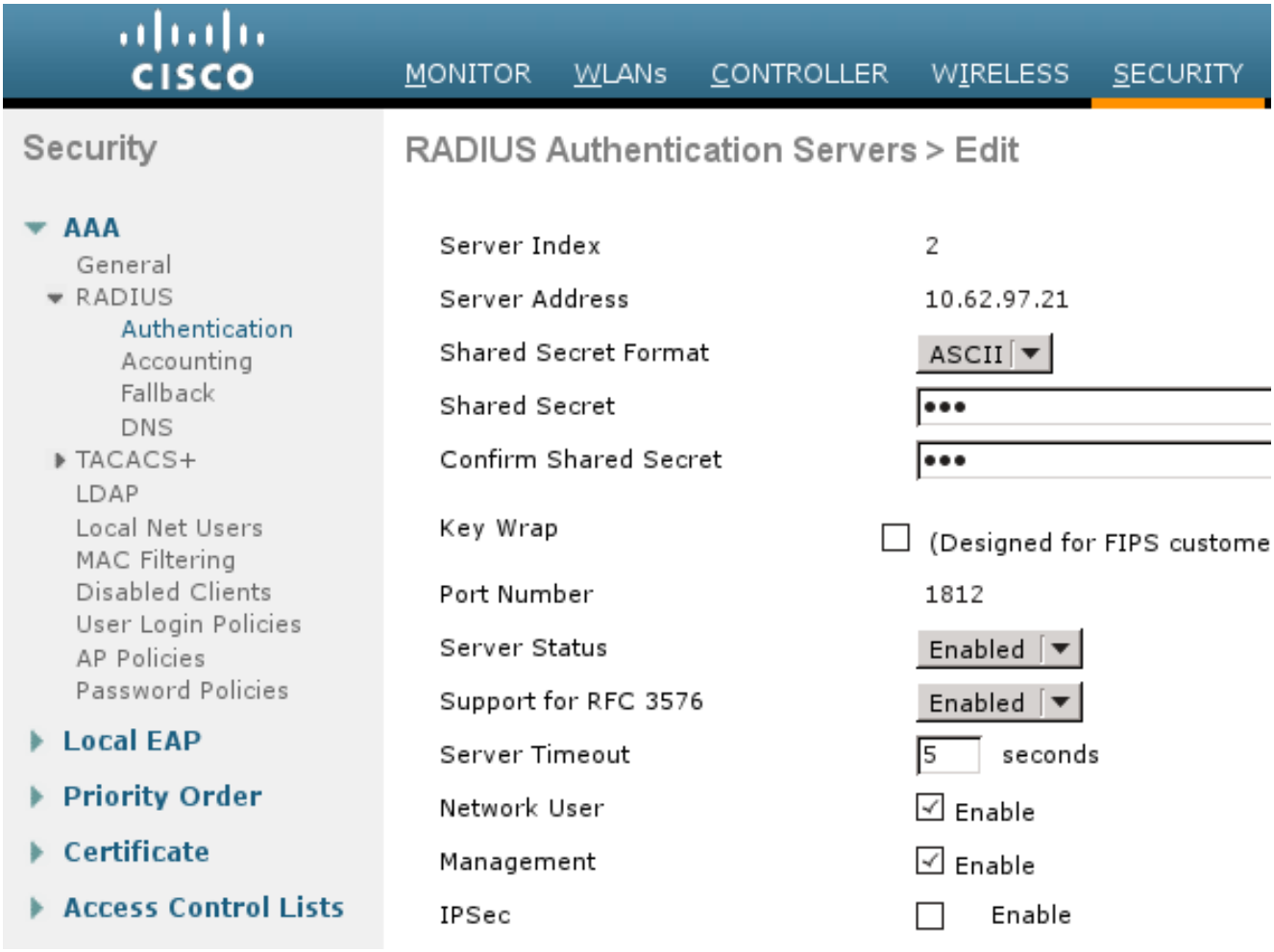
ステップ 4 ゲストユーザはネットワークへのアクセスを望みました。

ポスチャのような複数の追加機能はあなた自身のデバイス（BYOD）をイネーブルになります持って来、（説明されていた以降）。

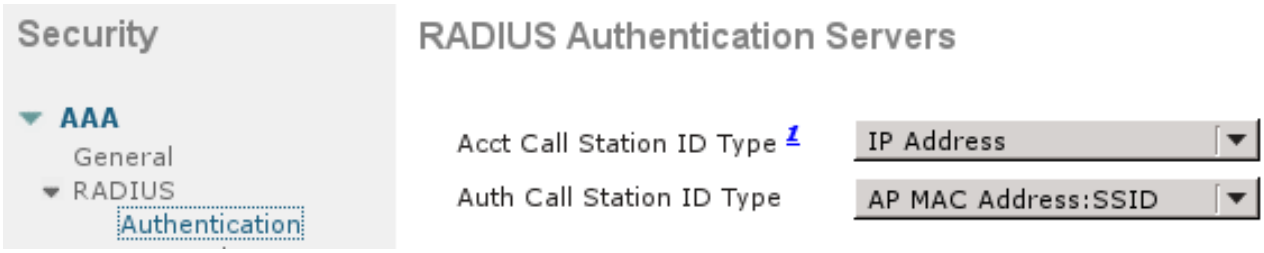
設定

WLC

1. 認証とアカウンティングのために新しい RADIUS サーバを追加します。 RADIUS CoA（RFC 3576）を有効にするため、[Security] > [AAA] > [Radius] > [Authentication] に移動します。



アカウンティングでも同様の設定があります。 また、[Called Station ID] 属性で SSID を送信するように WLC を設定することが推奨されます。これにより、ISE は SSID に基づいて柔軟なルールを設定できます。

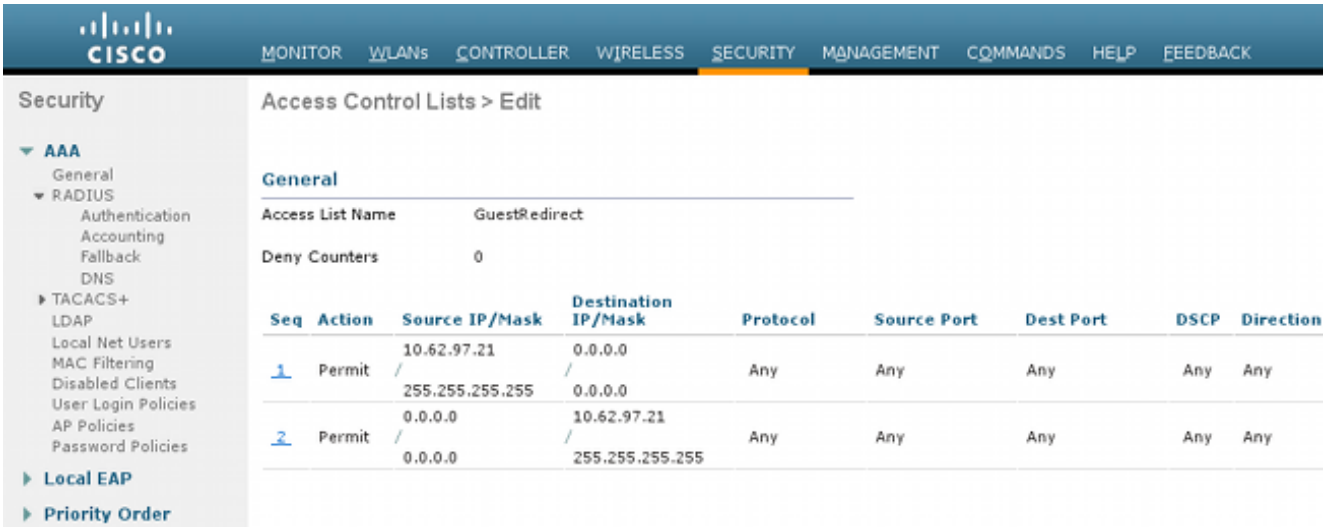


2. WLAN タブの下で、Wireless LAN （ WLAN ）ゲストを作成し、正しいインターフェイスを設定して下さい。 MAC フィルタリングで Layer2 セキュリティを [None] に設定します。 セキュリティ/認証、許可、アカウンティング（ AAA ）サーバで、認証およびアカウンティング両方に ISE IP アドレスを選択して下さい。 [Advanced] タブで [AAA Override] を有効にし、[Network Admission Control (NAC) State] を [RADIUS NAC] に設定します（ CoA サポート）。

3. [Security] > [Access Control Lists] > [Access Control Lists] の順に移動し、2 つのアクセス リストを作成します。

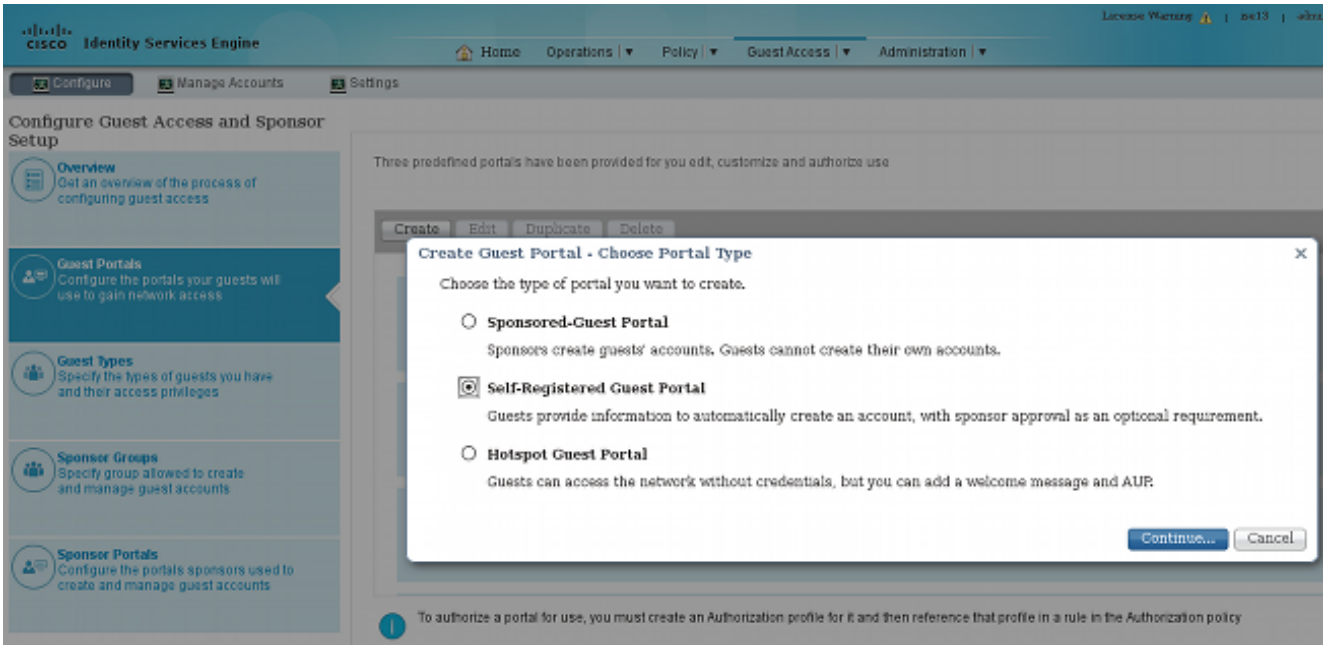
   リダイレクトするべきではないし、他のトラフィックをすべてリダイレクトする割り当てトラフィック GuestRedirect、Internet：社内ネットワークについては拒否され、その他のすべてのネットワークについては許可されます。

GuestRedirect ACL（リダイレクションから ISE に出入するトラフィックを除く必要）のための例はここにあります:



ISE

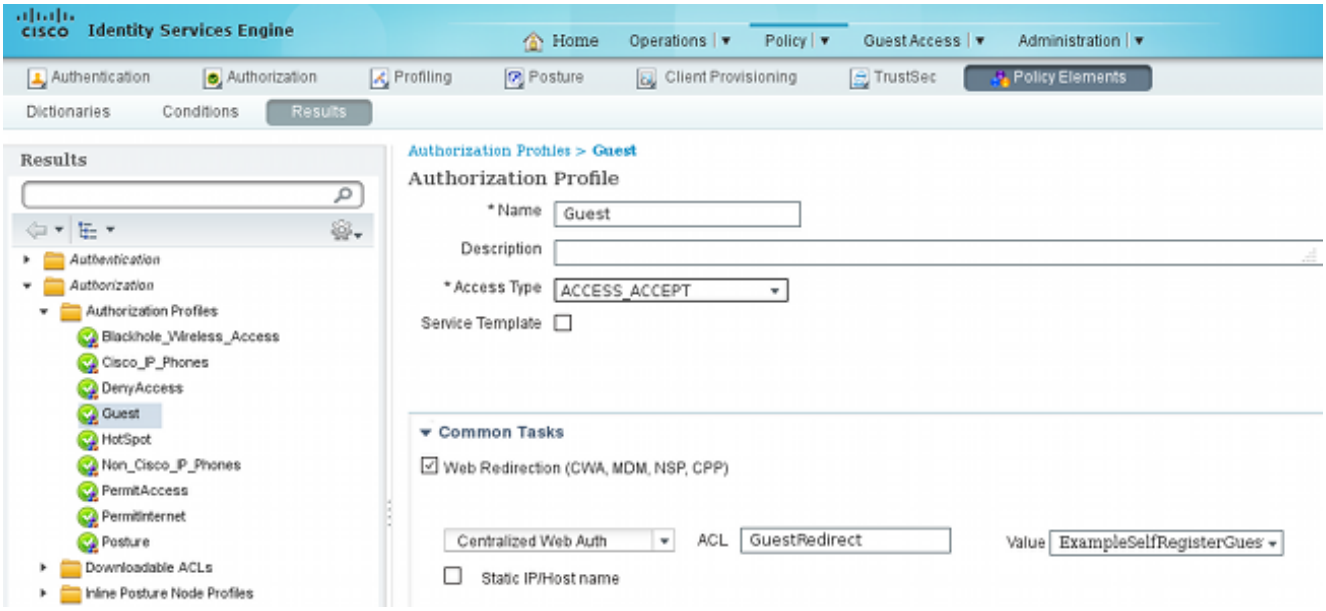
1. **ゲスト アクセス**へのナビゲートは **> > ゲスト ポータル設定し**、新しい門脈型を、自己によって登録されているゲスト ポータル作成します:



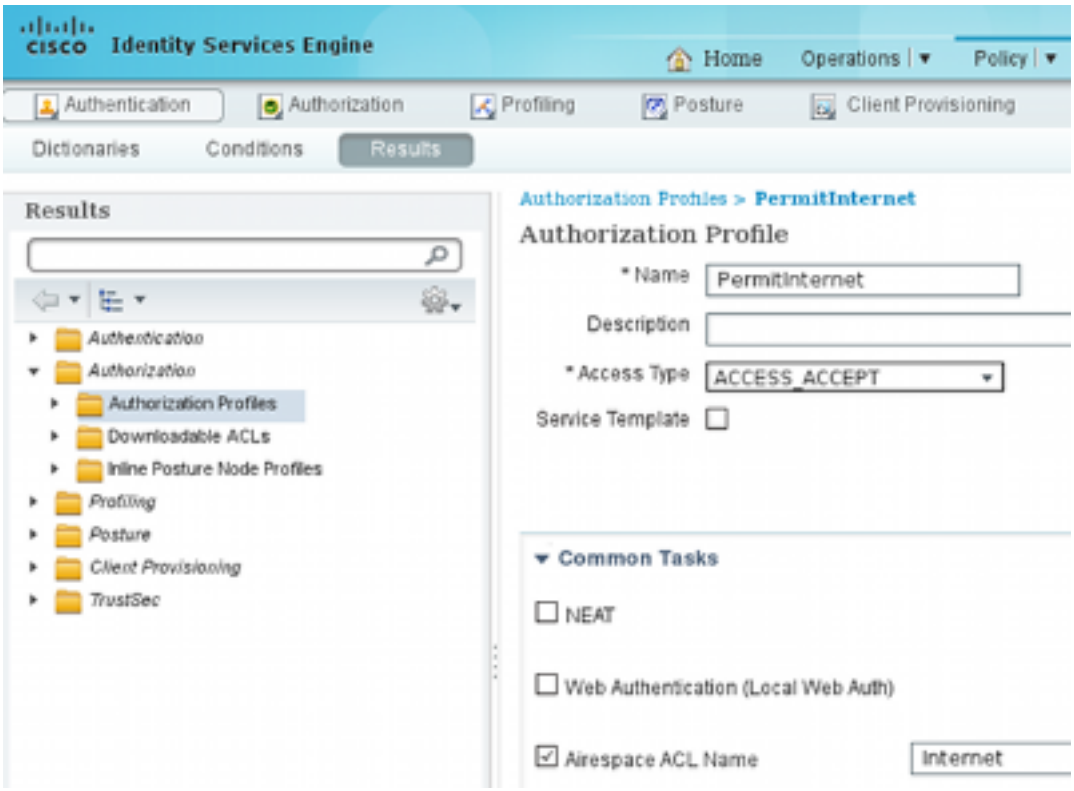
2. 認証プロファイルで参照されるポータル名を選択します。 ディフォルトするために他の設定すべてを行って下さい。 門脈ページ カスタマイゼーションの下で、示されるすべてのページはカスタマイズすることができます。

3. 許可プロファイルを設定して下さい:

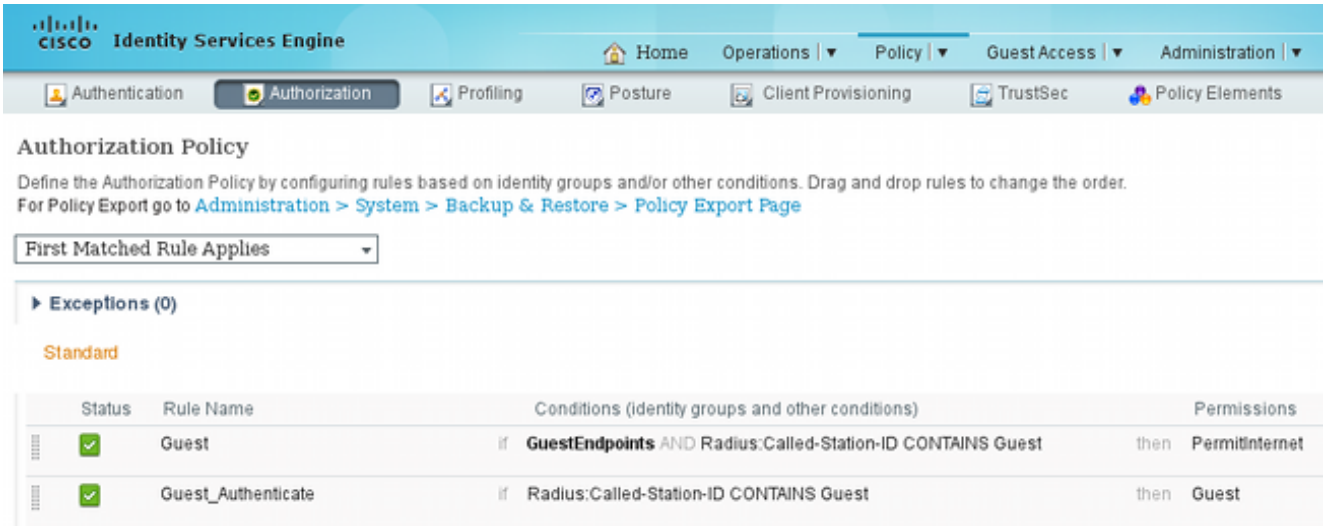
   ゲスト（ゲスト門脈名前および ACL GuestRedirect へのリダイレクションと）



PermitInternet（Airespace ACL 等号インターネットと）



4. 認可ルールを確認するために、[Policy] > [Authorization] に移動します。 ISE で壊れる MAC 認証バイパス（MAB）アクセス（見つけられない MAC アドレス）認証のためのバージョン 1.3 はデフォルトで続きます（拒否されない）。 これはデフォルトの認証ルールで何でも変更する必要がないのでゲスト ポータルに非常に役立ちます。



ゲスト SSID に関連付ける新規 ユーザはまだあらゆる識別グループの一部でない。 こういうわけで彼らは正しいゲスト ポータルにそれらをリダイレクトするのにゲスト許可プロファイルを使用する第 2 ルールを一致する。

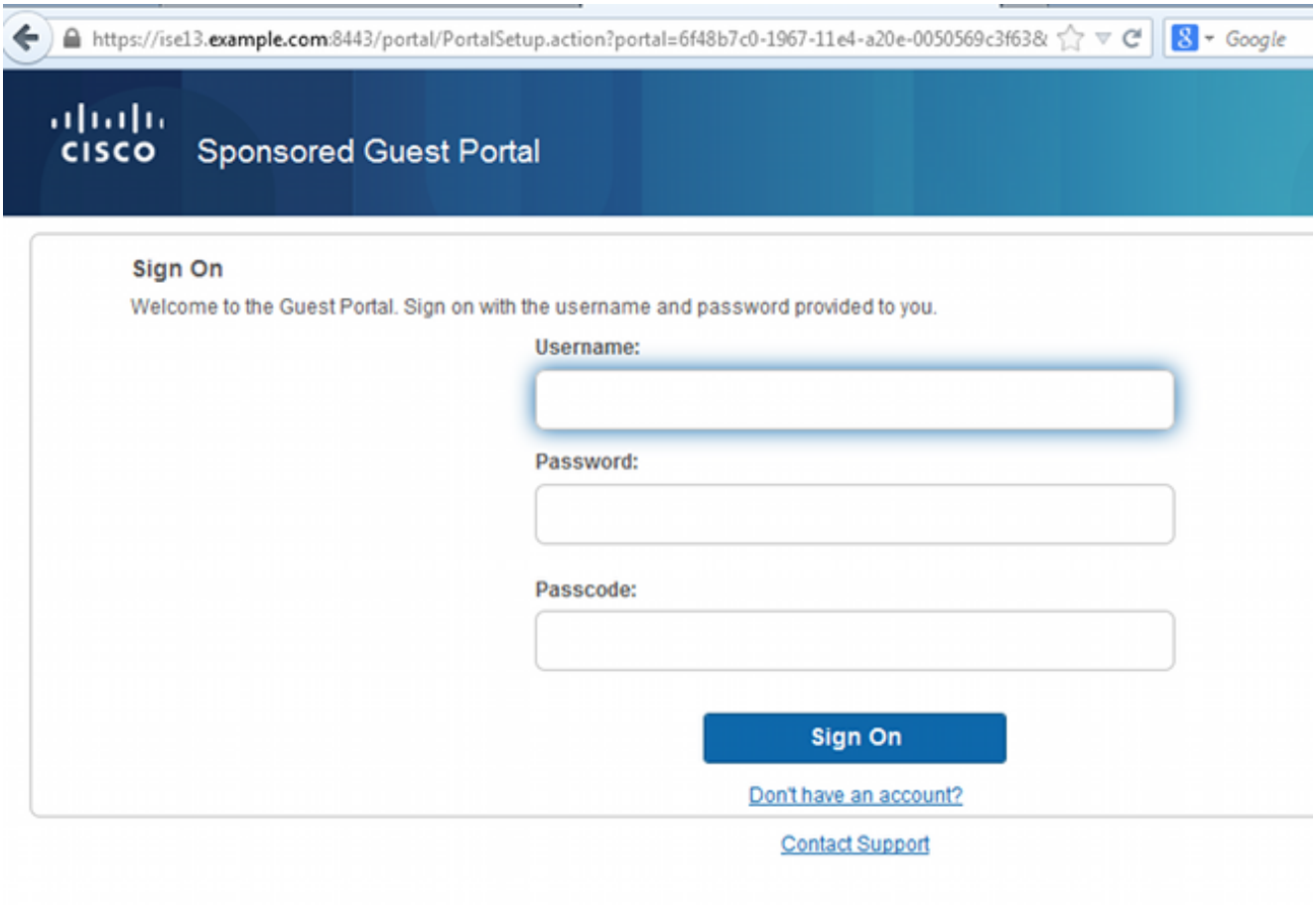
ユーザがアカウントを作成した、正常にログオンする後、ISE は RADIUS CoA を送信 し、WLC は再認証を行います。 今回、最初のルールは許可プロファイル PermitInternet と共に一致し、WLC で適用される ACL 名前を戻します。

5. [Administration] > [Network Resources] > [Network Devices] で WLC をネットワーク アクセス デバイスとして追加します。

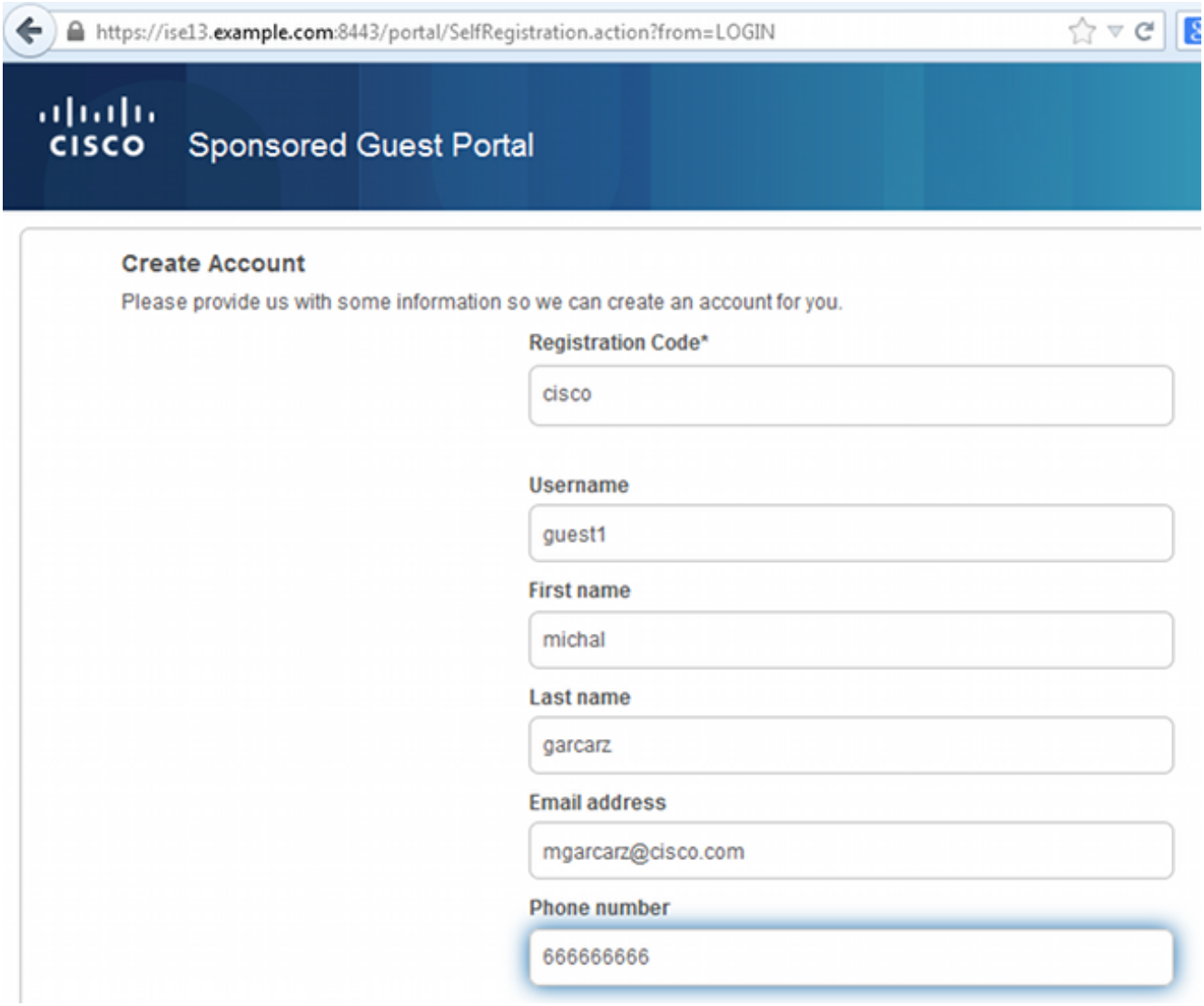
確認

このセクションでは、設定が正常に機能していることを確認します。

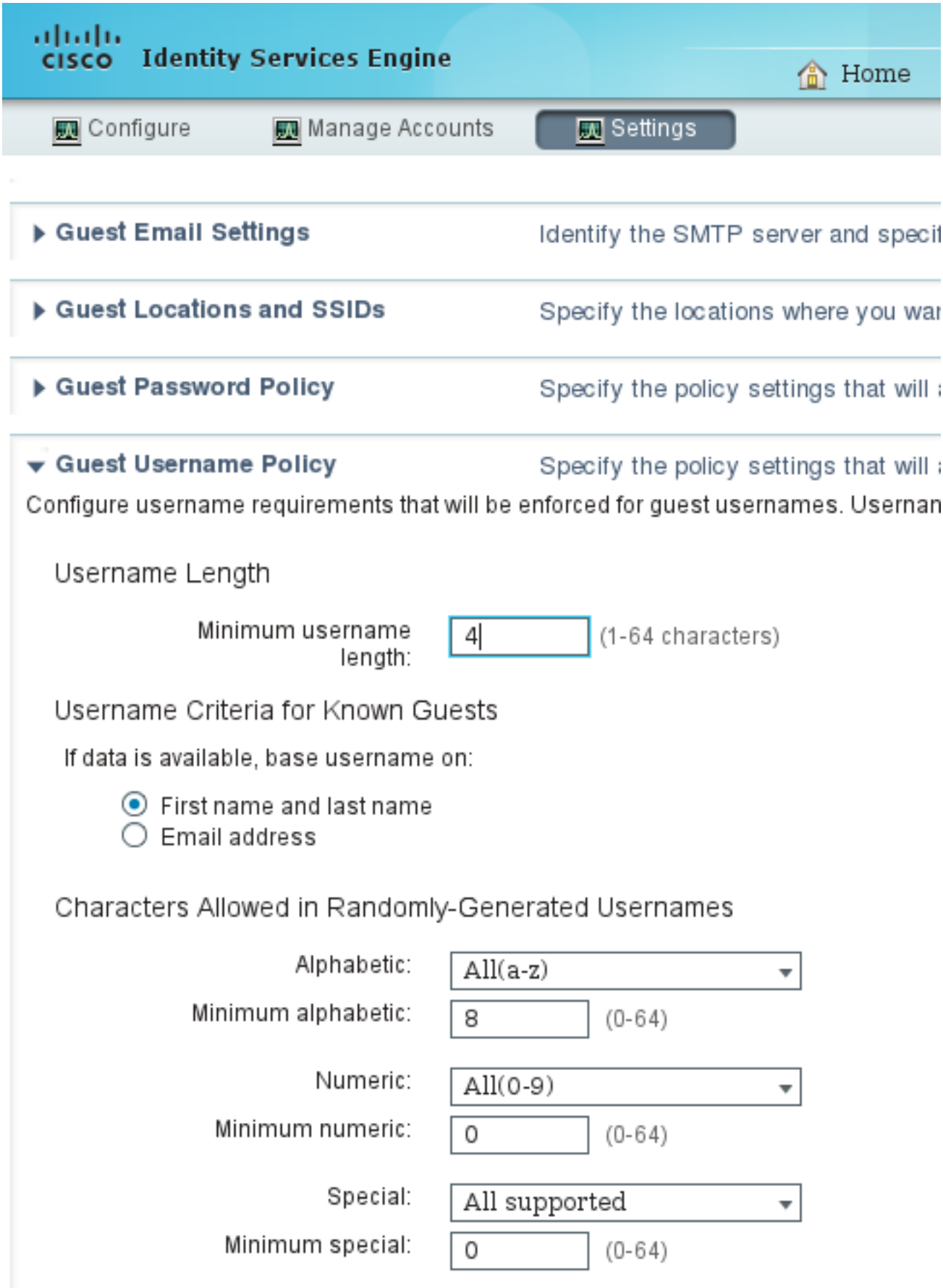
1. ゲスト SSID と関連付けた、URL をタイプする後、そしてログイン ページにリダイレクトされます:



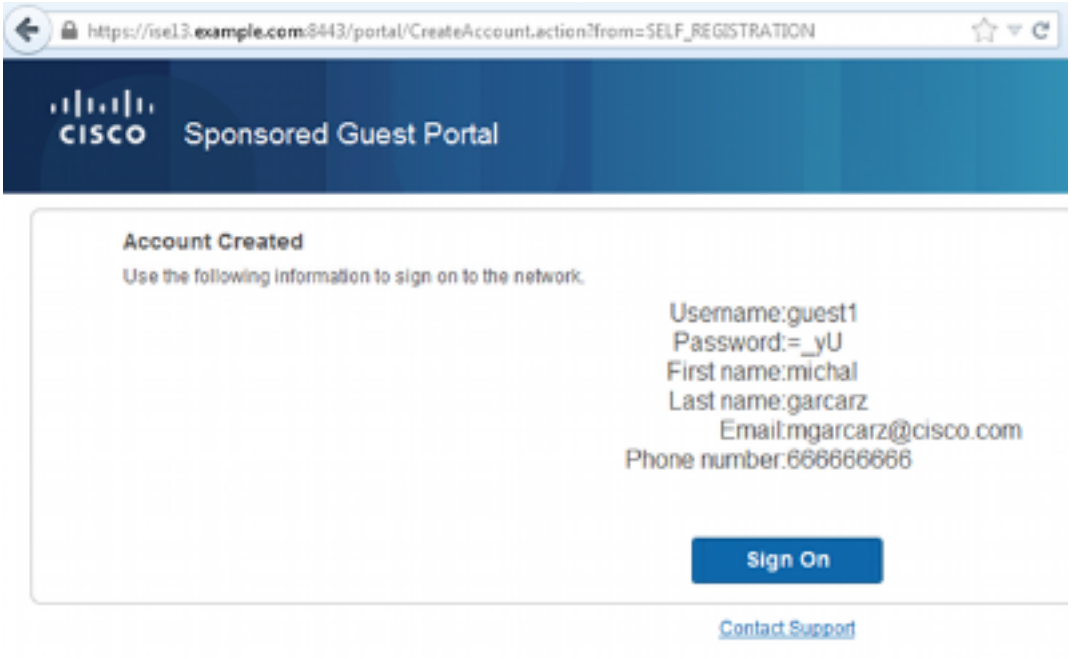
2. 信任状がまだあっていないので、**持っていませんアカウントを**選択して下さい**か。** オプション。 New ページ アカウントの作成ディスプレイを可能にする。 登録コード オプションがゲスト門脈設定の下でイネーブルになっていた場合、正しい 許可の個人だけ自己レジスタを与えられるように) その秘密の値が必要となります (これはします。



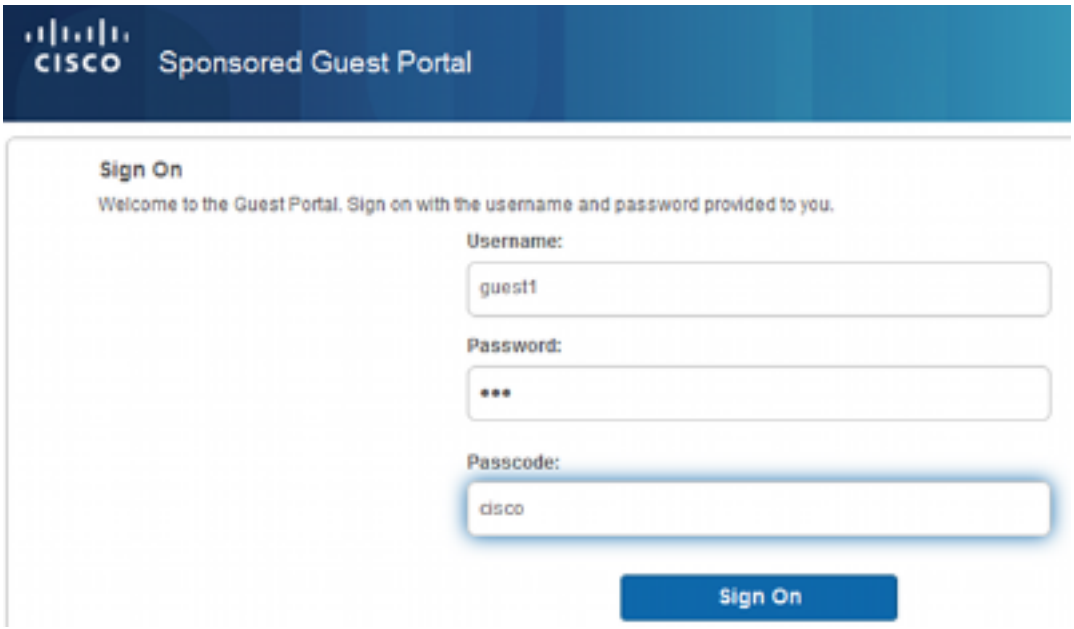
3. パスワードまたはユーザポリシーに問題がある場合、**ゲスト アクセス > 設定 > ゲスト パスワード ポリシーまたはゲスト アクセス > 設定 > ゲスト ユーザ名 ポリシー**に設定を変更するためにナビゲート して下さい。 次に例を示します。



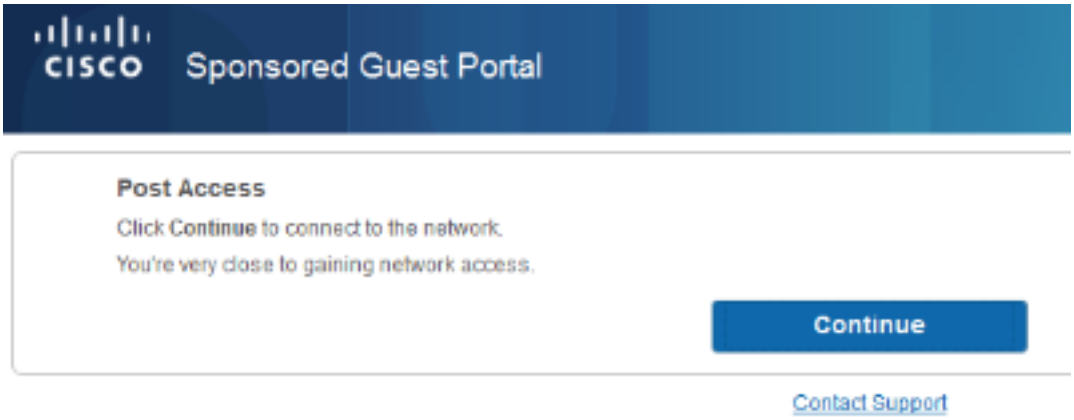
4. 正常なアカウントの作成の後で、信任状（ゲスト パスワード ポリシーによって生成されるパスワード）が表示されます:



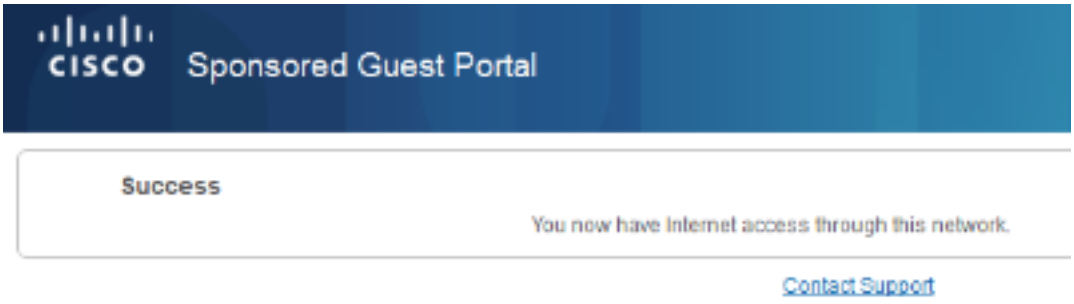
5. **サインを**クリックし、信任状を提供して下さい（ゲスト ポータルの下で追加アクセス パスコードがもし設定するなら必要となるかもしれません; これはログインにパスワードを知っている）人だけ可能にするもう一つのセキュリティ機構です。



6. 正常な場合、オプションの Acceptable Use Policy （AUP）は示されるかもしれません（もし設定するならゲスト ポータルの下で）。 ポスト アクセス ページ（また設定可能な下ゲスト ポータル）はまた表示するかもしれません。



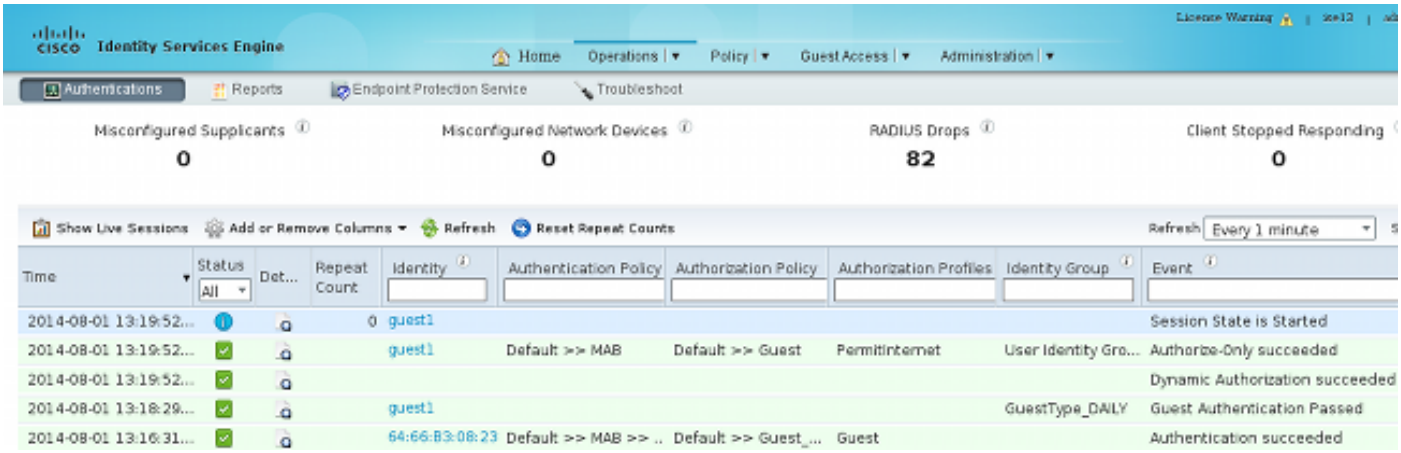
最後のページはアクセスが認められたことを確認します:



トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

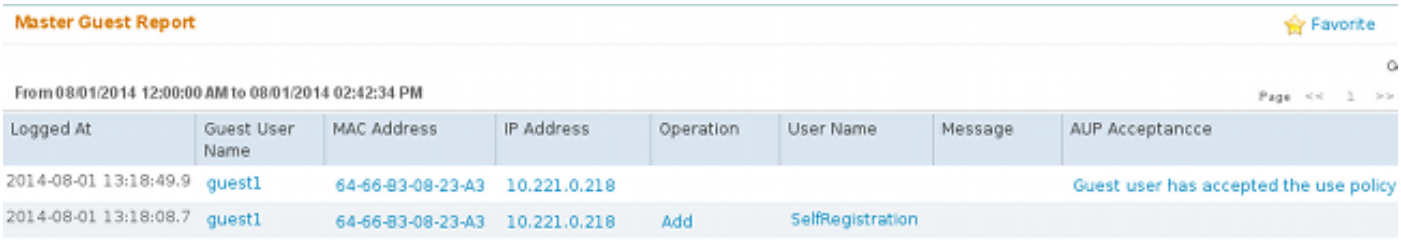
この段階では、ISE はこれらのログを示します:



ここで、フローを示します。

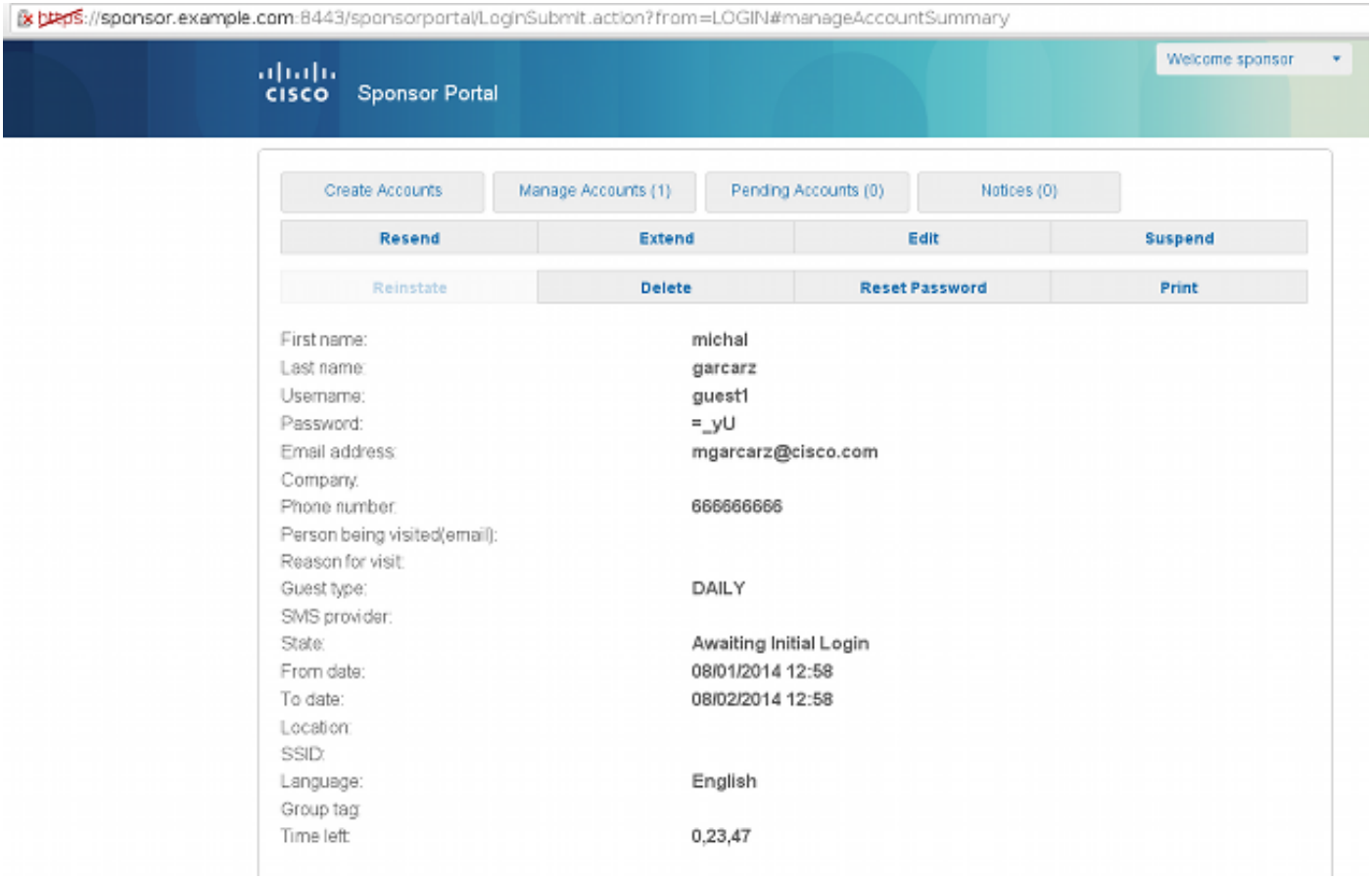
- ゲストユーザは第 2 承認規則（Guest_Authenticate）に出会い、ゲストにリダイレクトされます（「Auhentication」は成功しました）。
- ゲストは自己登録のためにリダイレクトされます。 正常にログオンが（新しく作成されたアカウントと）、ISE WLC（「成功する」動的許可）によって確認される CoA を送信 した後再認証して下さい。
- WLC は承認だけ属性と再認証を行い、ACL 名前は戻ります（「成功する」承認だけ）。 ゲ

ストは正しいネットワーク アクセス提供されます。
レポートはまた（**オペレーション > レポート > ISE は > ゲスト アクセス レポート > マスター Guest レポート報告します**）それを確認します:



スポンサー ユーザは（正しい特権と）ゲストユーザの現在のステータスを確認できます。

この例はアカウントが作成されるが、ユーザは決してログオンしことを確認しま（「最初のログイン」を待ちます）:



オプション設定

このフローの各ステージの場合、異なるオプションは設定することができます。 これすべては**ゲスト アクセス**のゲスト ポータルごとに **> 設定し、> ゲスト ポータル > PortalName > Edit > 門脈動作設定フローします**設定されます。 より重要な設定は下記のものを含んでいます:

自己登録設定

- ゲスト型-パスワード終止オプション、ログオン時間およびオプション（これは ISE バージョ

ンからの時間プロファイルおよびゲスト ロールの 1.2) か組み合わせですどの位アカウントであるアクティブ記述します
- 登録コード-有効な場合、暗号を知っているアカウントが作成されるときユーザだけ自己レジスタを与えられます (パスワードを提供しなければなりません)
- AUP - 自己登録の間に使用ポリシーを受け入れて下さい
- 承認するべきスポンサー/アクティブ化ゲスト アカウントのための要件

ログオン ゲスト設定

- アクセスコード-有効な場合、暗号を知っているゲストユーザだけログインに許可されます
- AUP - 自己登録の間に使用ポリシーを受け入れて下さい
- パスワード変更オプション

デバイス登録設定

- デフォルトで、デバイスは自動的に登録されています

ゲスト デバイス 準拠性設定

- フロー内のポスチャを可能に

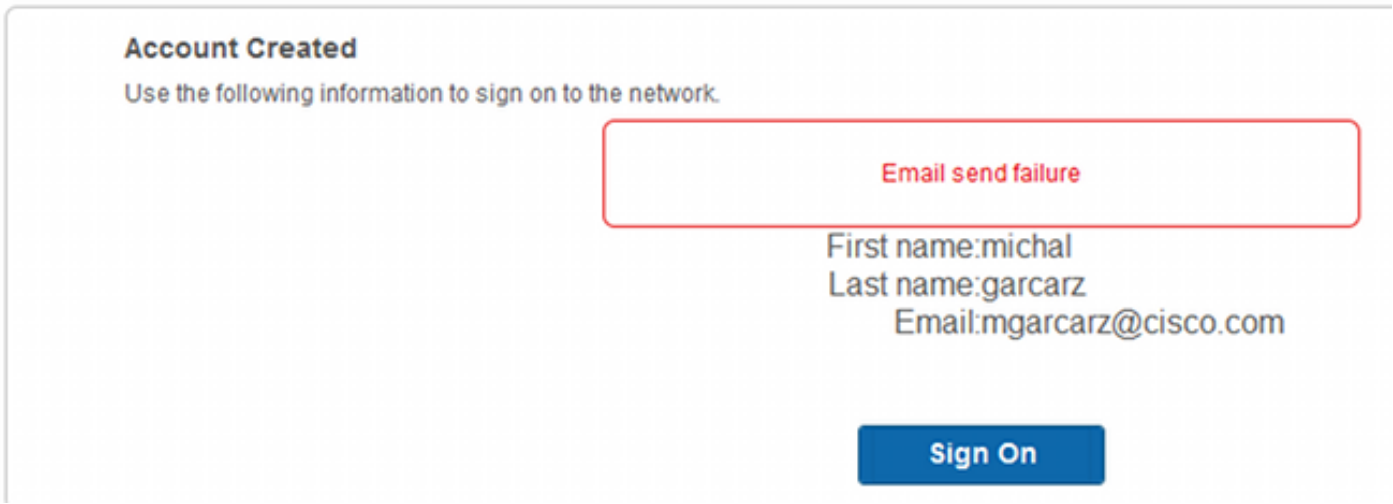
BYOD 設定

- 個人的なデバイスを登録するのにゲストとしてポータルを使用する企業ユーザを許可します

スポンサー公認アカウント

承認されたオプション**である Require によって自己登録されるゲストが**選択される場合、ゲストが作成するアカウントはスポンサーによって承認する必要があります。 この機能はスポンサーに通知を渡すためにメールを使用するかもしれません (ゲスト アカウント承認のために) :

メールからの通知からの Simple Mail Transfer Protocol (SMTP) サーバかデフォルトが設定されない場合、アカウントは作成されません:

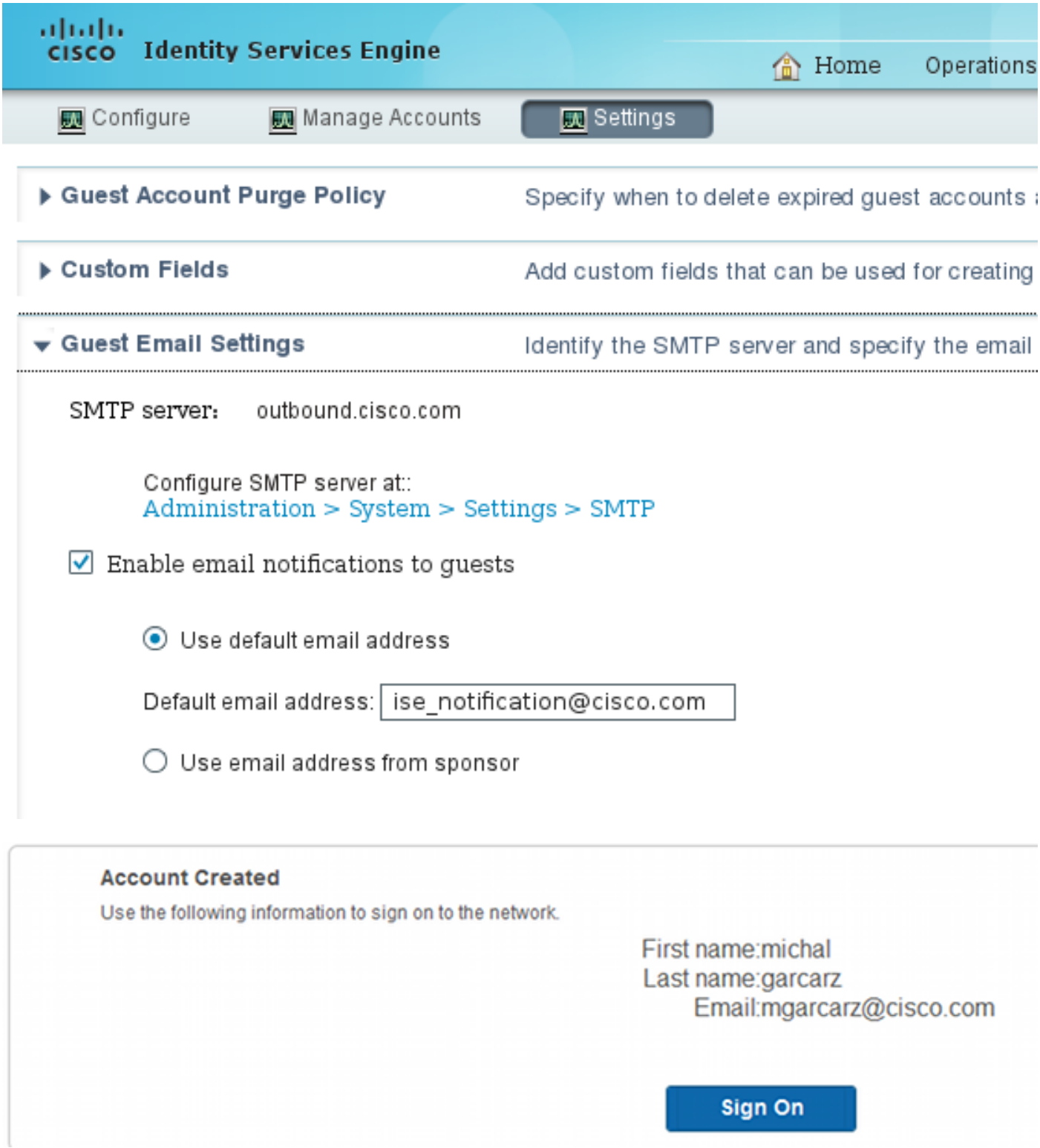


guest.log からの ログは通知に使用するアドレスからのグローバルの抜けていることを確認します

:

```
2014-08-01 22:35:24,271 ERROR  [http-bio-10.62.97.21-8443-exec-9][] guestaccess.
flowmanager.step.guest.SelfRegStepExecutor -:7AAF75982E0FCD594FE97DE2970D472F::-
Catch GuestAccessSystemException on sending email for approval: sendApproval
Notification: From address is null.  A global default From address can be
configured in global settings for SMTP server.
```

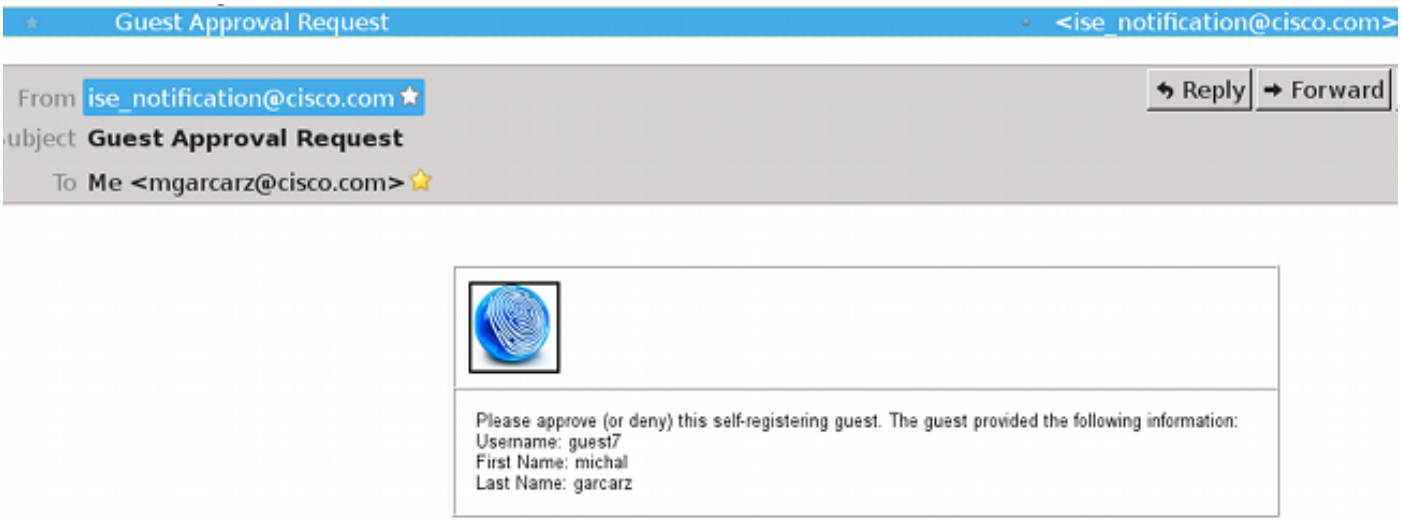
適切なメール設定があるとき、アカウントは作成されます:



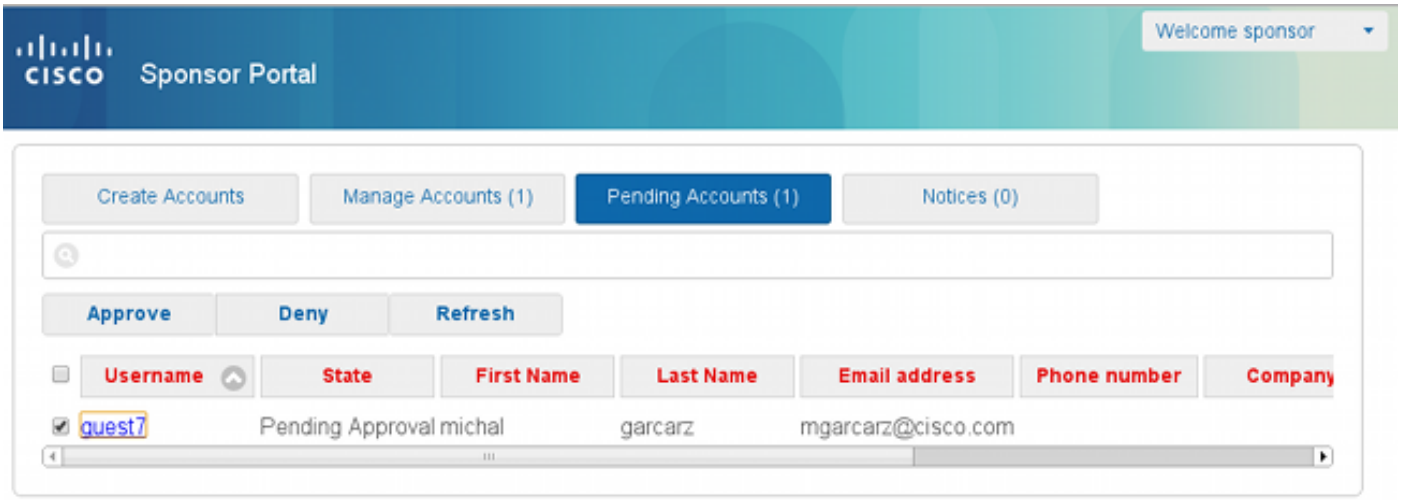
require によって自己登録されるゲストが承認されたオプション**であることを**可能にした後ユーザ名 および パスワード フィールドは**含**から自動的に自己**登録成功ページ** セクション**のこの情報**削除されます。 こういうわけで、スポンサー承認が必要なときアカウントが作成されたことを示す

ために、ゲストユーザ向けの信任状は Webページにこと提供情報デフォルトで表示されません。その代り（SMS）またはメールそれらは Short Message Services（SMS）によって渡す必要があります。 このオプションはセクション（マーク email/SMS）**を使用して承認に送信クレデンシャル通知**でイネーブルになっている必要があります。

通知 メールはスポンサーに渡されます:



スポンサーは門脈スポンサーにログイン し、アカウントを承認します:



ここから先は、ゲストユーザはログインに許可されます（メールか SMS によって受け取られて信任状が）。

要約すると、このフローで使用される 3 e メールアドレスがあります:

- 」アドレスからの通知「。 これは統計的に定義されか、またはスポンサー アカウントから奪取 され、アドレスからのとして両方のために使用されます: ゲストに（承認のために）およびクレデンシャル詳細後援するべき通知。 これは**ゲスト アクセス**の下で **> 設定します > 設定 > ゲスト メール設定**設定されます。

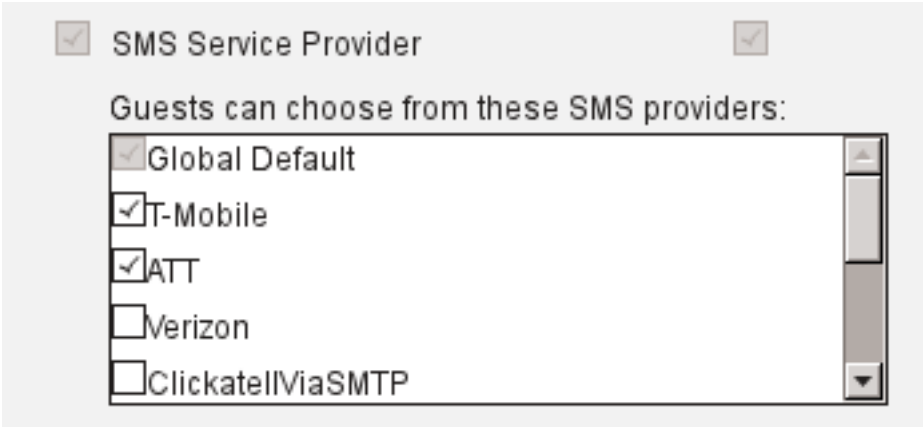
- アドレス指定するべき通知「」。 これは承認のためのアカウントを受け取ったことスポンサーを知らせるために使用されます。 これは**ゲスト アクセス**の下のゲスト ポータルで **> 設定します > ゲスト ポータル > 門脈名前 > > メール 承認要求に承認されるべき Require によって自己登録されるゲスト**設定されます。

- アドレス指定するべきゲスト「」。 これは登録の間にゲストユーザによって提供されます。 **メールを使用して承認に送信クレデンシャル通知が**選択される場合、クレデンシャル詳細（ユーザ名 および パスワード）が付いているメールはゲストに渡されます。

SMS によって信任状を渡して下さい

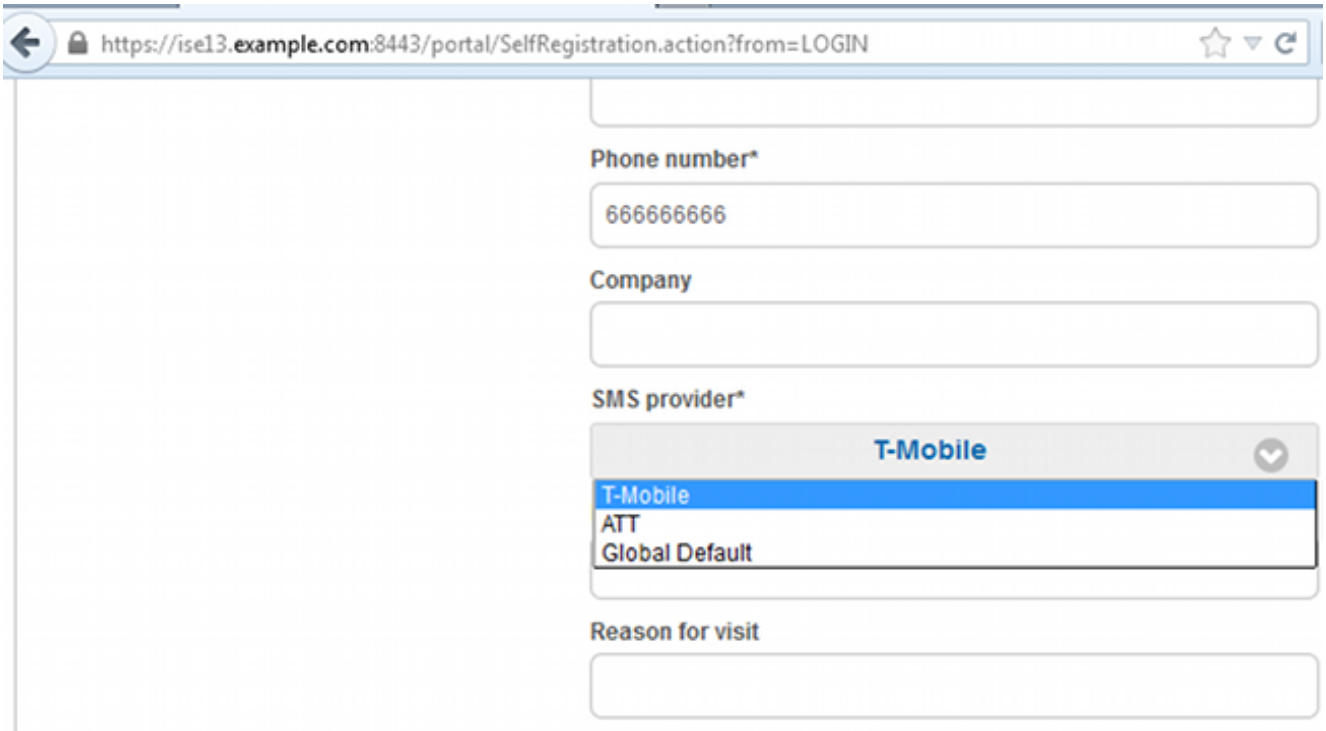
ゲスト信任状はまた SMS によって渡すことができます。 これらのオプションは設定する必要があります:

1. SMS サービス プロバイダーを選択して下さい:

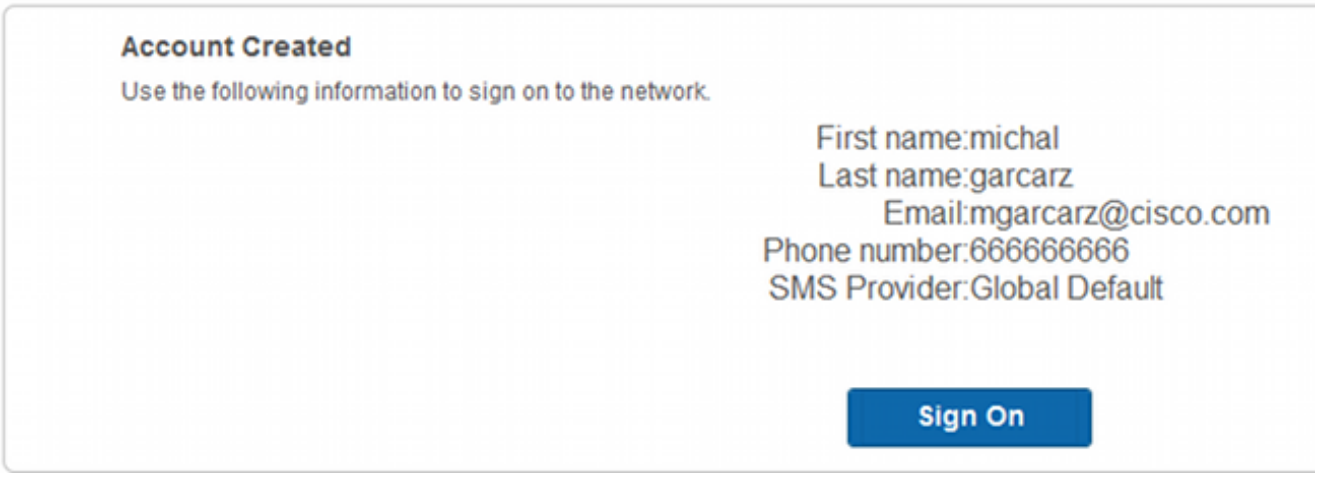


2. **承認に送信クレデンシャル通知をを使用して**チェックして下さい: **SMS** チェックボックス。

3. それから、ゲストユーザは彼がアカウントを作成するとき利用可能なプロバイダを選択するように頼まれます:



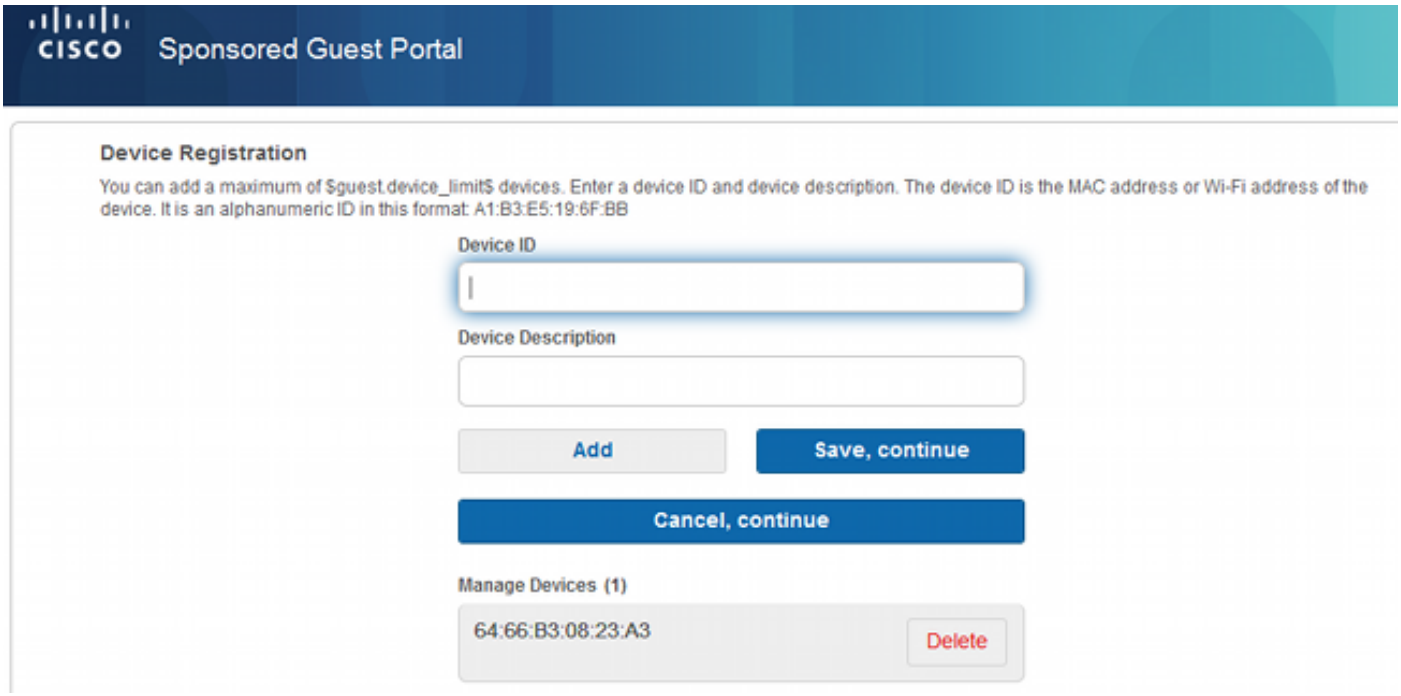
4. SMS は選択されたプロバイダおよび電話番号によって渡されます:



5. **Administration > システム > 設定 > SMS ゲートウェイ**の下で SMS プロバイダを設定できます。

デバイス登録

ゲストユーザが AUP をログオンした、受け入れる後**デバイス** オプションを**登録する割り当てゲストが**選択されれば、デバイスを登録できます:



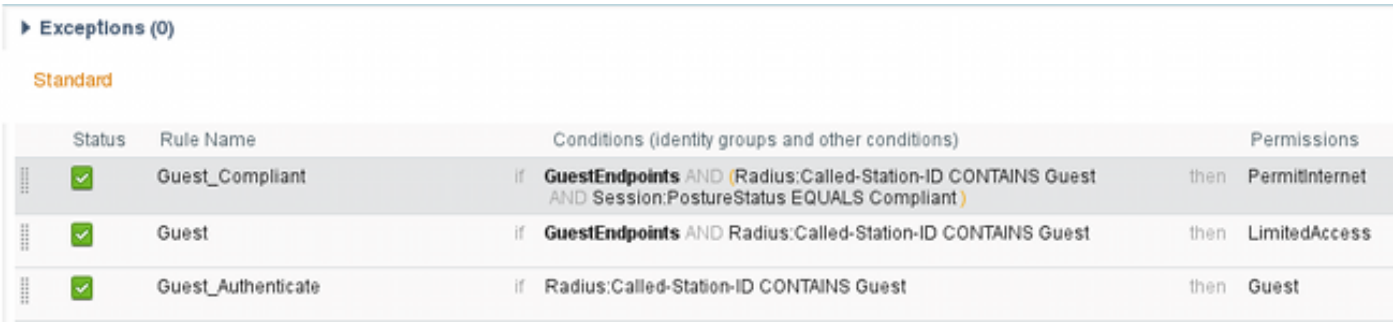
デバイスが既に自動的に追加されていたことに注意して下さい（Manage デバイス・リストにあります）。 これは**自動的にレジスタ ゲスト デバイスが**選択されたという理由によります。

ポスチャ

必要とゲスト デバイス 準拠性オプションが選択される場合、ゲストユーザはポスチャ（NAC/Web エージェント）を後彼らログイン行った、AUP を受け入れますエージェントによって提供されます（およびオプションでデバイス登録を行って下さい）。 ISE はどのエージェント

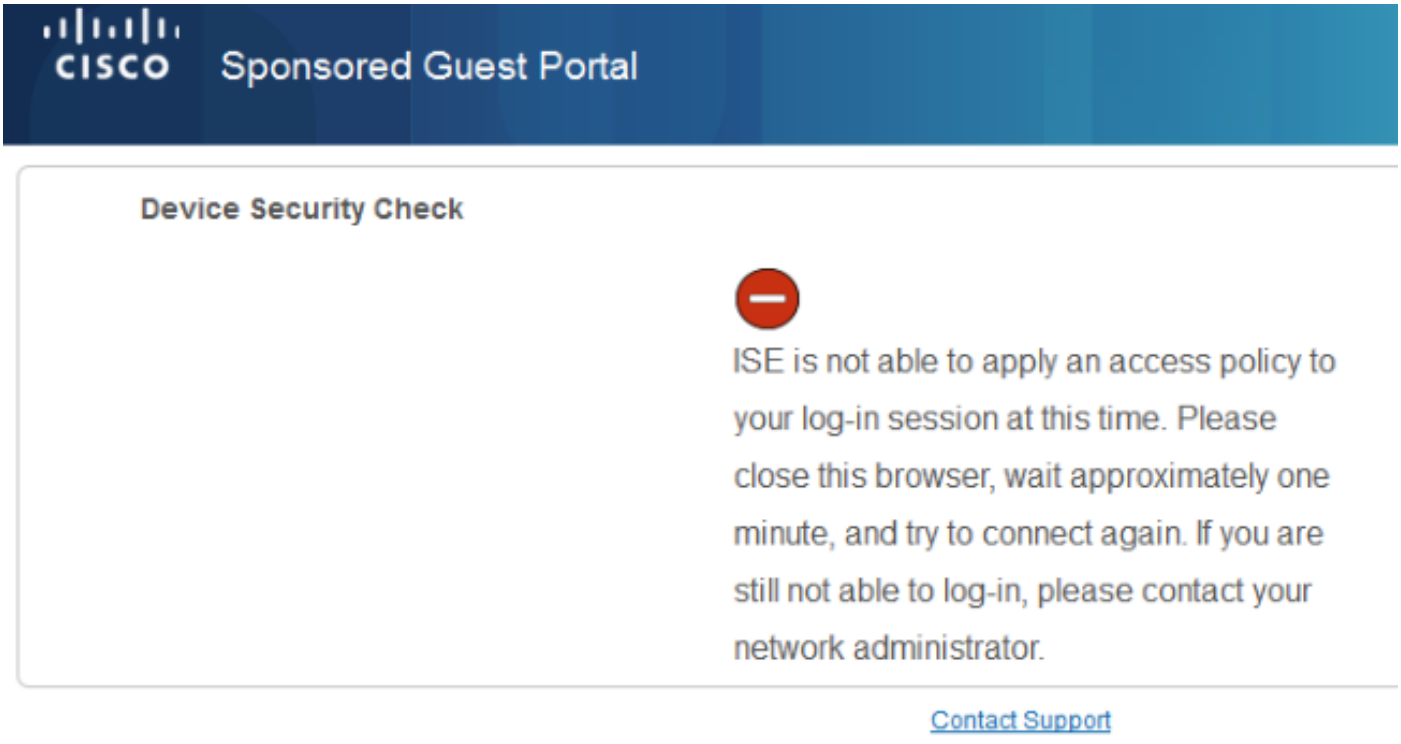
が提供する必要があるか決定するクライアント プロビジョニング ルールを処理します。 それからステーションで動作するエージェントはポスチャを (ポスチャ ルールによって) 行い、認証ステータスを変更するために CoA を再認証するもし必要なら送信 する ISE に結果を送ります。

可能性のある承認規則はこれに類似したに検知 するかもしれません:



自己レジスタ ゲスト ポータルに Guest_Authenticate ルール リダイレクトに出会う最初の新規 ユーザ。 ユーザ自己登録はログオンした、後、CoA は認証ステータスを変更し、ポスチャおよび治療を行うためにユーザは制限されたアクセスを与えられます。 NAC エージェントがおよび提供される後やっとステーションは対応もう一度しますインターネットへのアクセスを提供するために CoA 変更認証ステータスをです。

ポスチャにおける典型的な問題は正しいクライアント プロビジョニング ルールの欠如が含まれています:



これはまた guest.log ファイルを検査する場合確認することができます (1.3) ISE バージョンで新しい:

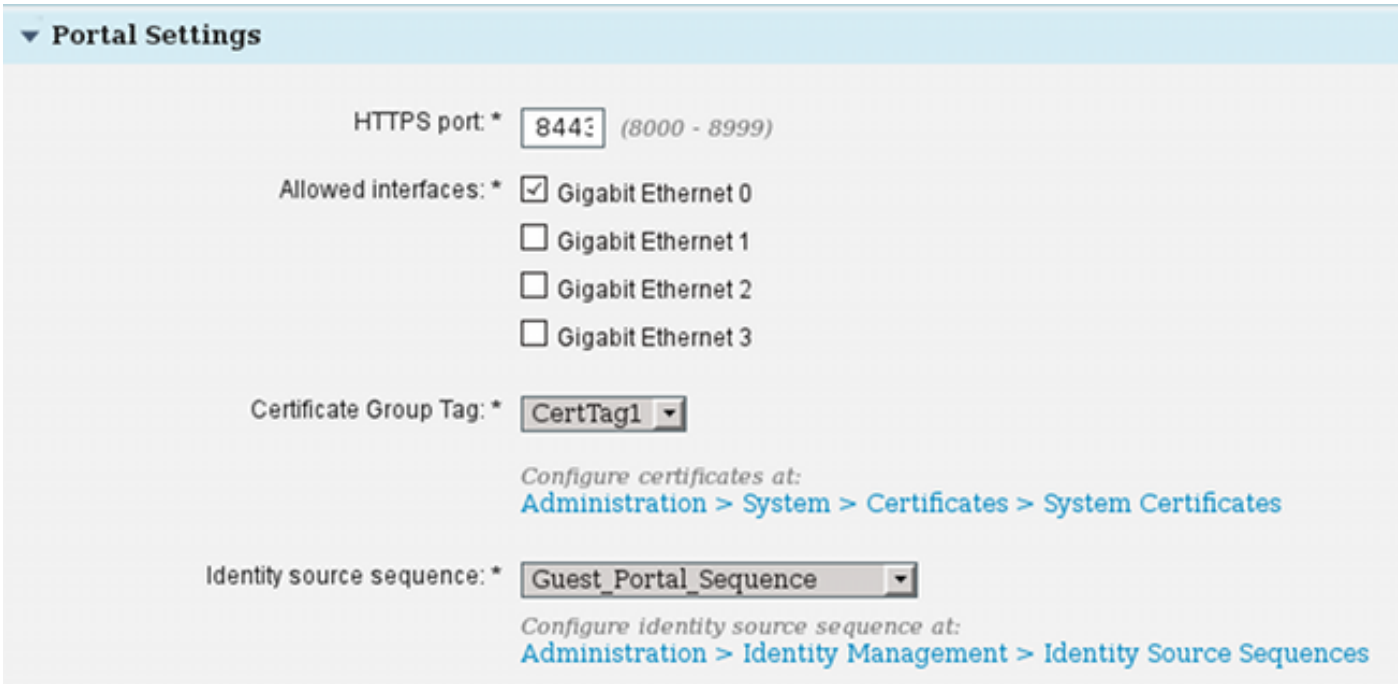
```
2014-08-01 21:35:08,435 ERROR  [http-bio-10.62.97.21-8443-exec-9][] guestaccess.
flowmanager.step.guest.ClientProvStepExecutor -:7AAF75982E0FCD594FE97DE2970D472F::-
CP Response is not successful, status=NO_POLICY
```

BYOD

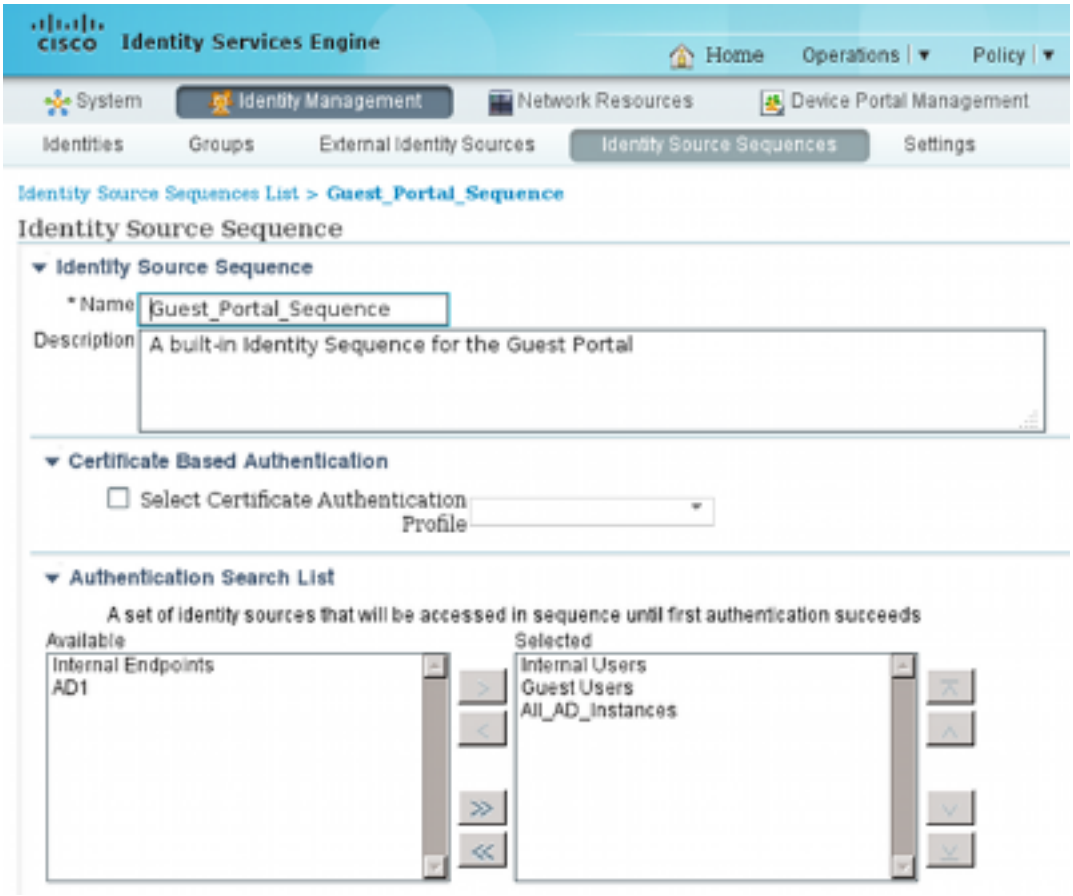
Network オプションの個人的なデバイスを使用する割り当て従業員が選択される場合、このポータルを使用する企業ユーザは BYOD をフローし、登録します個人的なデバイスを通過できます。ゲストユーザ向けに、その設定は何も変更しません。

従業員「ゲストとしてポータルを」は使用しているどういうことを意味しますか。

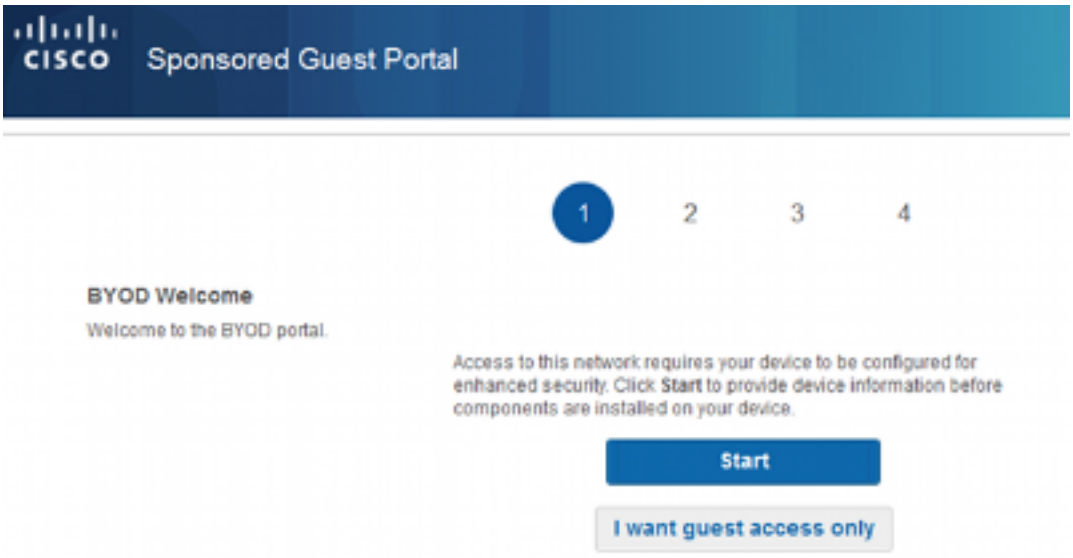
デフォルトで、ゲスト ポータルは **Guest_Portal_Sequence** 識別ストアで設定されます:



これは内部ユーザを最初に裁判にかける内部ストア シーケンスです (ゲストユーザの前に) :



この段階でゲスト ポータルで、ユーザは内部ユーザで保存する定義される BYOD リダイレクションは発生します信任状を提供し、とき:



この方法企業ユーザは個人的なデバイスのための BYOD を行うことができます。

内部ユーザ信任状の代りに、ゲストユーザ信任状は、標準フロー続きます提供されます時（BYOD 無し）。

VLANの変更

これはゲスト ポータルのために設定される ISE バージョン 1.2 の VLANの変更へ同じようなオプションです。 それは ActiveX かリリースし、更新するために DHCP を誘発する Javaアプレット

を実行することを可能にします。 これは CoA がエンド ポイントのための VLAN の変更を誘発するとき必要です。 MAB が使用されるとき、エンド ポイントは VLAN の変更に気づいていません。 可能な解決策は NAC エージェントとの VLAN を（DHCP リリースは/更新します）変更することです。 もう一つのオプションは Webページで戻るアプレットによって新しい IP アドレスを要求することです。 リリース/CoA 間の遅延は/設定することができます更新します。 このオプションはモバイルデバイスのためにサポートされません。

関連情報

- Cisco ISE コンフィギュレーション ガイドのポスチャ サービス
- Identity Services Engine を使用したワイヤレス BYOD
- BYOD 設定例のための ISE SCEP サポート
- Cisco ISE 1.3 アドミニストレータ ガイド
- WLC と ISE での中央 Web 認証の設定例
- ISE を搭載した WLC 上で FlexConnect AP を使用した中央 Web 認証の設定例
- テクニカル サポートとドキュメント – Cisco Systems