

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

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[トポロジとフロー](#)

[設定](#)

「 [AeroScout RFID タグ](#)

[ISE](#)

[確認](#)

[トラブルシューティング](#)

[オプション設定](#)

[自己登録設定](#)

[ログオンゲスト設定](#)

[デバイス登録設定](#)

[ゲスト デバイス 準拠性設定](#)

[BYOD 設定](#)

[スポンサー公認アカウント](#)

[SMS によって信任状を渡して下さい](#)

[デバイス登録](#)

[ポストチャ](#)

[BYOD](#)

[VLANの変更](#)

[関連情報](#)

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。

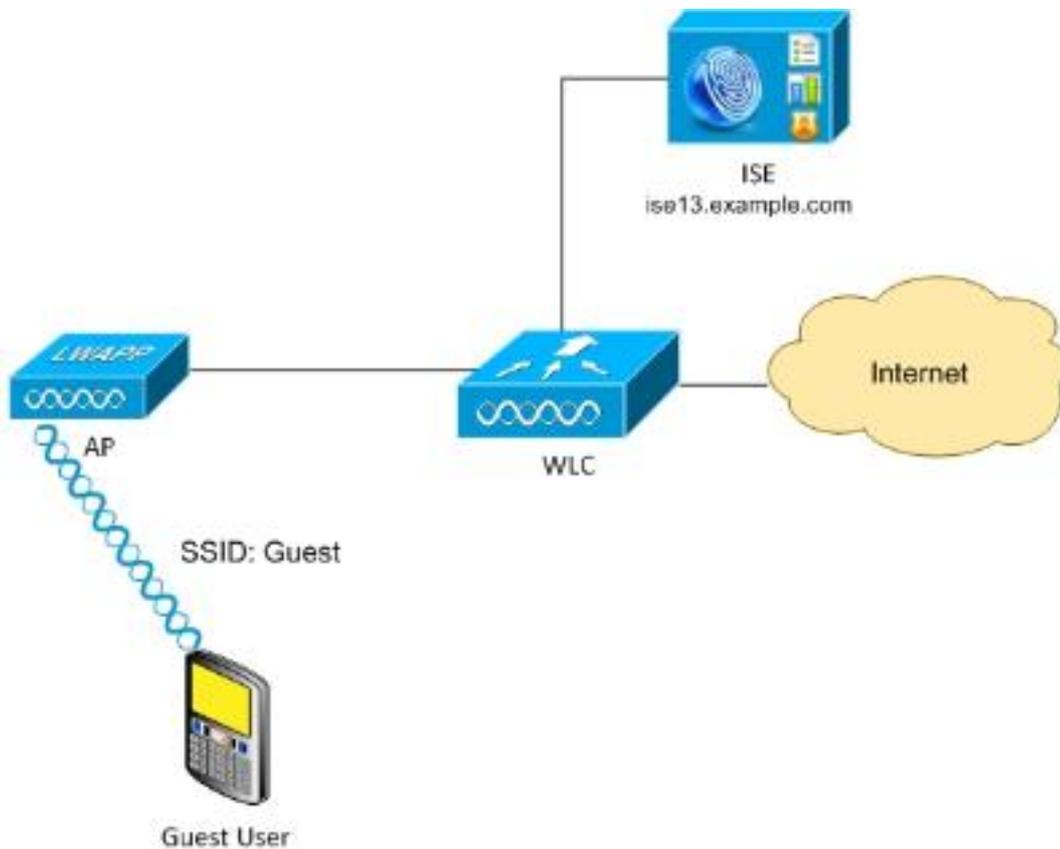
- ISE の導入およびゲスト フロー
- ワイヤレス LAN コントローラ (WLC) の設定

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. 認証とアカウントिंग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。

CISCO [MONITOR](#) [WLANS](#) [CONTROLLER](#) [WIRELESS](#) [SECURITY](#)

Security

- ▼ **AAA**
 - General
 - ▼ RADIUS
 - Authentication
 - Accounting
 - Fallback
 - DNS
 - ▶ TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
- ▶ **Local EAP**
- ▶ **Priority Order**
- ▶ **Certificate**
- ▶ **Access Control Lists**

RADIUS Authentication Servers > Edit

Server Index	2	
Server Address	10.62.97.21	
Shared Secret Format	ASCII ▼	
Shared Secret	●●●	
Confirm Shared Secret	●●●	
Key Wrap	<input type="checkbox"/>	(Designed for FIPS custome
Port Number	1812	
Server Status	Enabled ▼	
Support for RFC 3576	Enabled ▼	
Server Timeout	5 seconds	
Network User	<input checked="" type="checkbox"/>	Enable
Management	<input checked="" type="checkbox"/>	Enable
IPSec	<input type="checkbox"/>	Enable

アカウントिंग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。

Security

- ▼ **AAA**
 - General
 - ▼ RADIUS
 - Authentication

RADIUS Authentication Servers

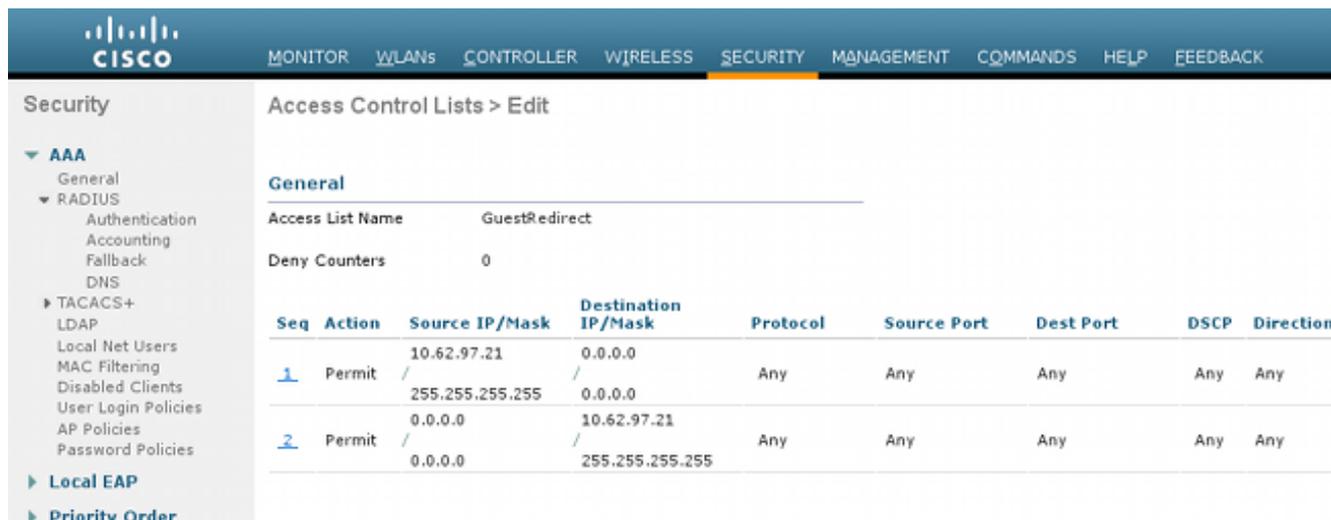
Acct Call Station ID Type ?	IP Address ▼
Auth Call Station ID Type	AP MAC Address:SSID ▼

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、アカウントング (AAA) サーバで、認証およびアカウントング両方に 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。

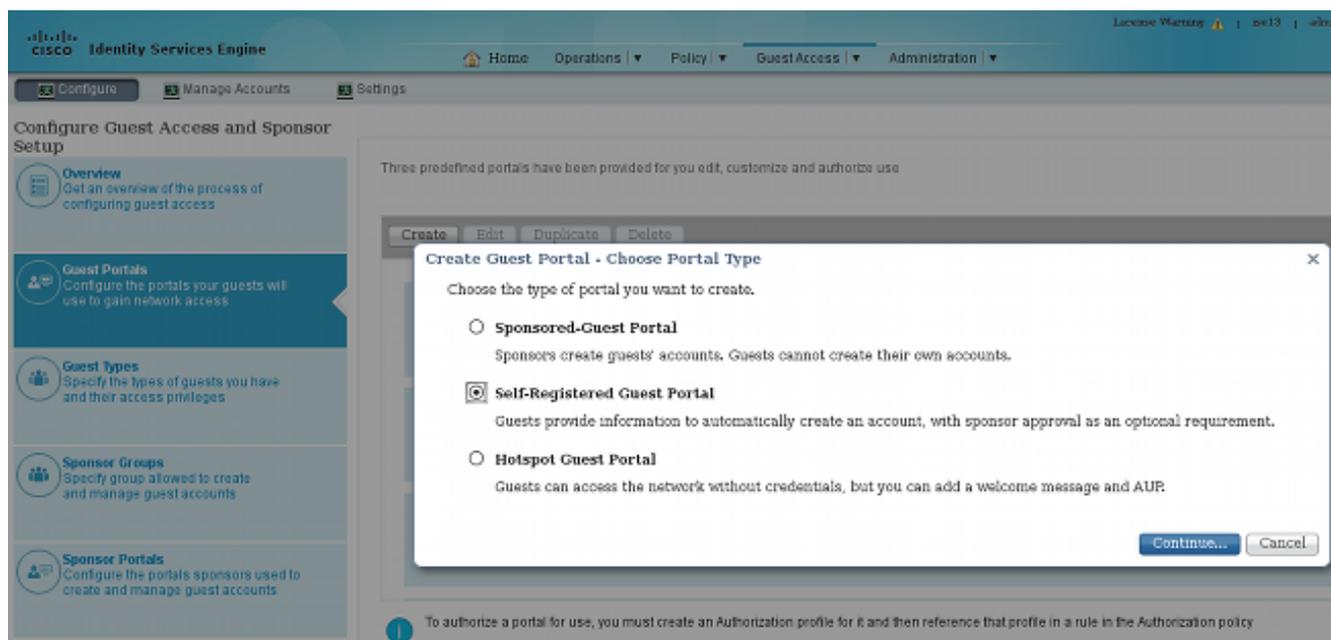
GuestRedirect ACL (リダイレクションから ISE に出入するトラフィックを除く必要) のための例はここにあります:



Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	10.62.97.21 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any
2	Permit	0.0.0.0 / 0.0.0.0	10.62.97.21 / 255.255.255.255	Any	Any	Any	Any	Any

ISE

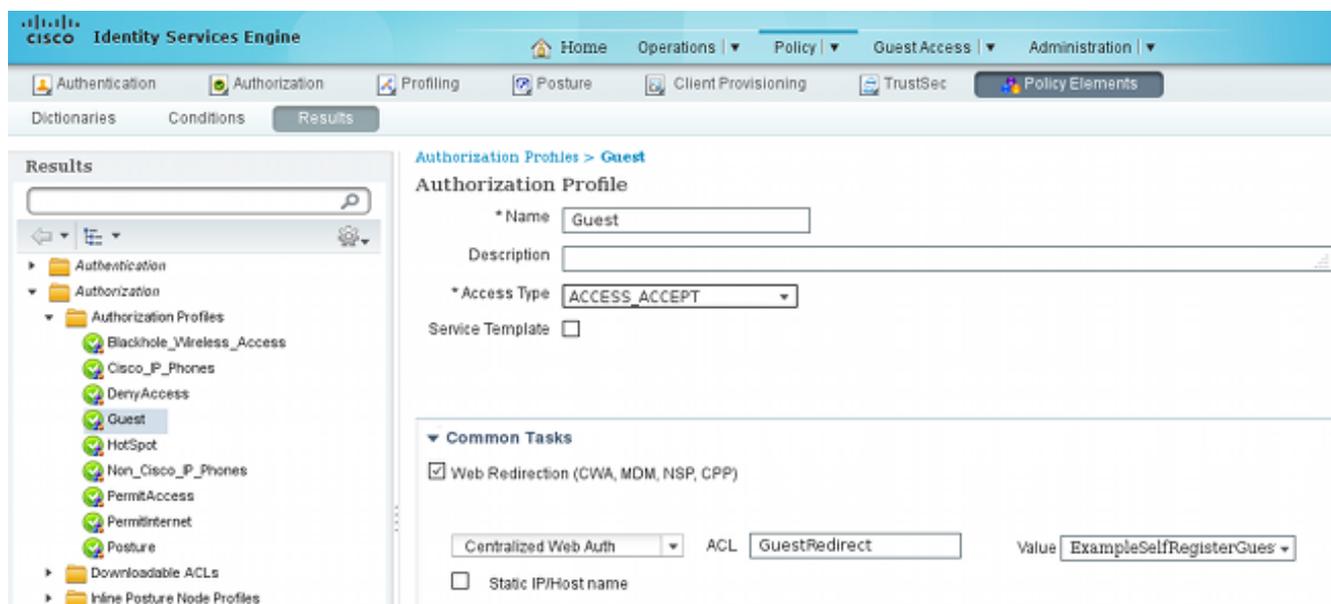
1. ゲスト アクセスへのナビゲートは >> ゲスト ポータル設定し、新しい門脈型を、自己によって登録されているゲスト ポータル作成します:



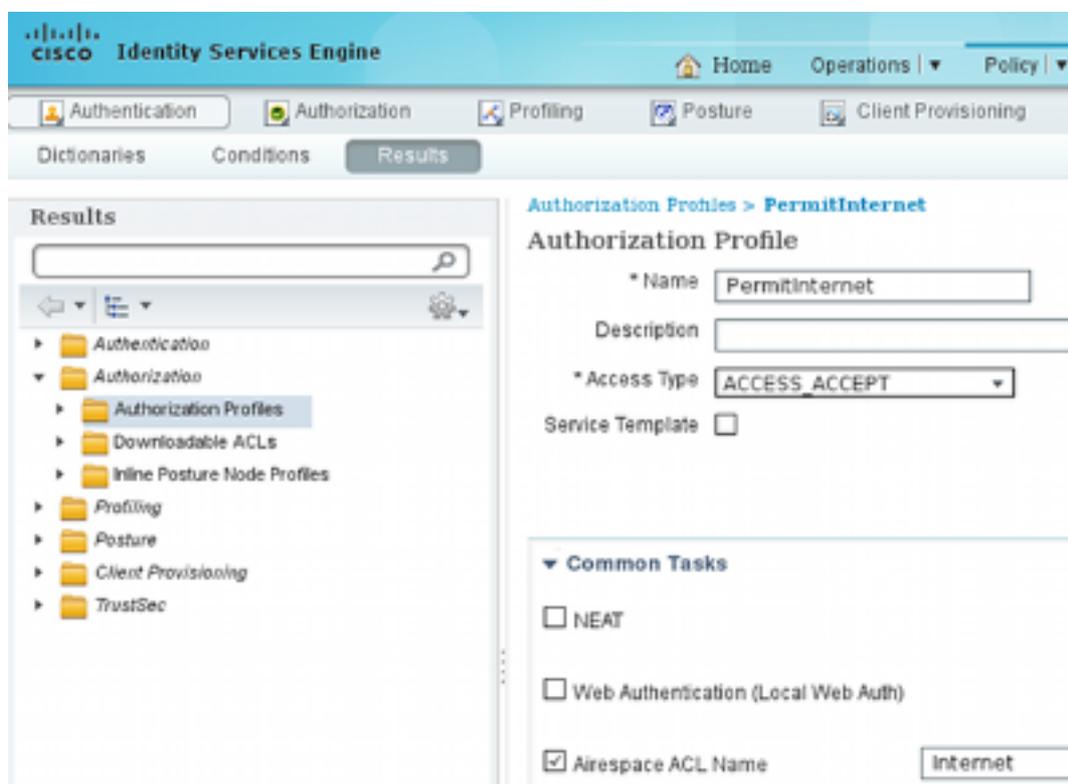
2. 認証プロファイルで参照されるポータル名を選択します。デフォルトするために他の設定すべてを行って下さい。門脈ページ カスタマイゼーションの下で、示されるすべてのページはカスタマイズすることができます。

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。

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

First Matched Rule Applies

▶ Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Guest	if GuestEndpoints AND Radius:Called-Station-ID CONTAINS Guest	then PermitInternet
✓	Guest_Authenticate	if Radius:Called-Station-ID CONTAINS Guest	then Guest

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:

← <https://ise13.example.com:8443/portal/PortalSetup.action?portal=6f48b7c0-1967-11e4-a20e-0050569c3f63&> ☆ ▾ ↻ 

 **Sponsored Guest Portal**

Sign On
Welcome to the Guest Portal. Sign on with the username and password provided to you.

Username:

Password:

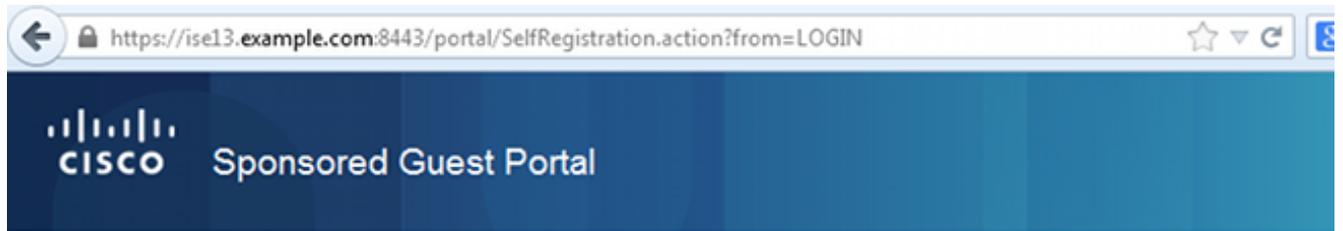
Passcode:

[Sign On](#)

[Don't have an account?](#)

[Contact Support](#)

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。



Create Account

Please provide us with some information so we can create an account for you.

Registration Code*

cisco

Username

guest1

First name

michal

Last name

garcarz

Email address

mgarcarz@cisco.com

Phone number

666666666

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。



▶ Guest Email Settings

Identify the SMTP server and specify

▶ Guest Locations and SSIDs

Specify the locations where you want

▶ Guest Password Policy

Specify the policy settings that will

▼ Guest Username Policy

Specify the policy settings that will

Configure username requirements that will be enforced for guest usernames. Usernames

Username Length

Minimum username length: (1-64 characters)

Username Criteria for Known Guests

If data is available, base username on:

- First name and last name
- Email address

Characters Allowed in Randomly-Generated Usernames

Alphabetic:

Minimum alphabetic: (0-64)

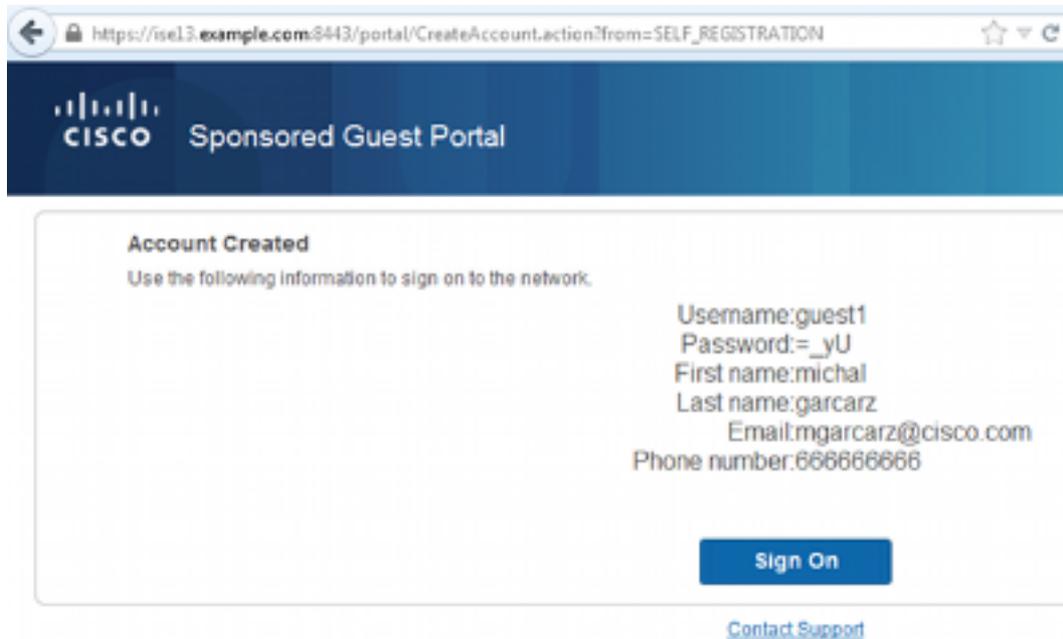
Numeric:

Minimum numeric: (0-64)

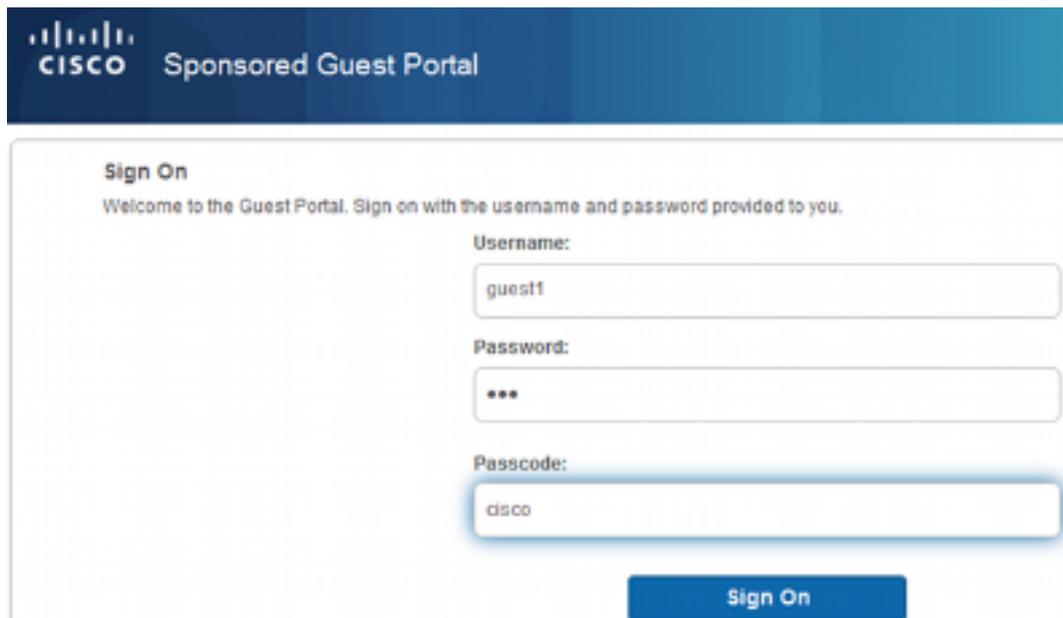
Special:

Minimum special: (0-64)

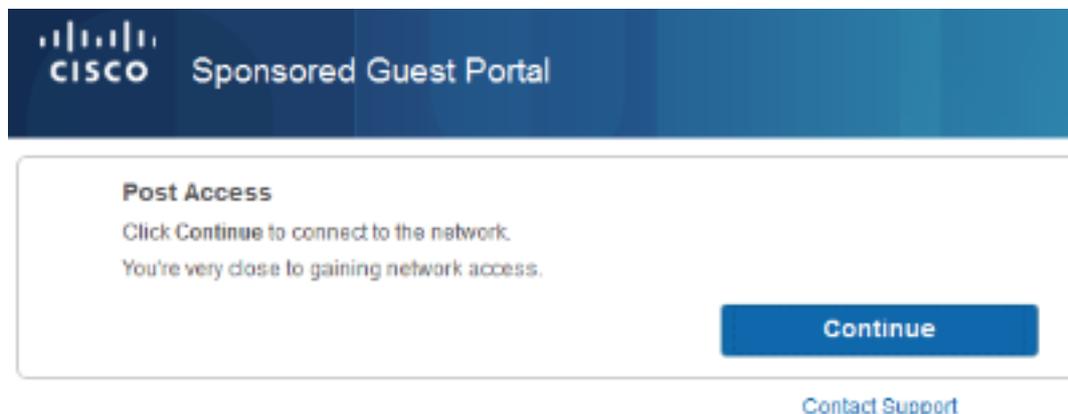
4. 正常なアカウントの作成の後で、信任状 (ゲスト パスワード ポリシーによって生成されるパスワード) が表示されます:



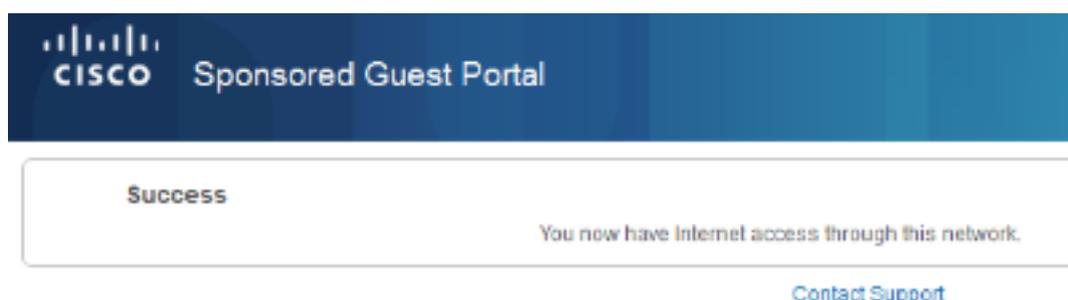
5. サインをクリックし、信任状を提供して下さい (ゲスト ポータルの下で追加アクセス パスコードがもし設定するなら必要となるかもしれません; これはログインにパスワードを知っている) 人だけ可能にするもう一つのセキュリティ機構です。



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:

Time	Status	Det...	Repeat Count	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Identity Group	Event
2014-08-01 13:19:52...	🔵	🔒	0	guest1					Session State is Started
2014-08-01 13:19:52...	🟢	🔒		guest1	Default >> MAB	Default >> Guest	PermitInternet	User Identity Gro...	Authorize-Only succeeded
2014-08-01 13:19:52...	🟢	🔒		guest1					Dynamic Authorization succeeded
2014-08-01 13:18:29...	🟢	🔒		guest1				GuestType_DAILY	Guest Authentication Passed
2014-08-01 13:16:31...	🟢	🔒		64:66:B3:08:23	Default >> MAB >> ..	Default >> Guest_...	Guest		Authentication succeeded

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 (「Authentication」 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:

Master Guest Report								★ Favorite
From 08/01/2014 12:00:00 AM to 08/01/2014 02:42:34 PM								Page << 1 >>
Logged At	Guest User Name	MAC Address	IP Address	Operation	User Name	Message	AUP Acceptance	
2014-08-01 13:18:49.9	guest1	64-66-83-08-23-A3	10.221.0.218				Guest user has accepted the use policy	
2014-08-01 13:18:08.7	guest1	64-66-83-08-23-A3	10.221.0.218	Add	SelfRegistration			

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):

https://sponsor.example.com:8443/sponsorportal/LoginSubmit.action?from=LOGIN#manageAccountSummary

Welcome sponsor

Create Accounts Manage Accounts (1) Pending Accounts (0) Notices (0)

Resend Extend Edit Suspend
 Reinstate Delete Reset Password Print

First name: michal
 Last name: garcarz
 Username: guest1
 Password: =_yU
 Email address: mgarcarz@cisco.com
 Company:
 Phone number: 666666666
 Person being visited(email):
 Reason for visit:
 Guest type: DAILY
 SMS provider:
 State: Awaiting Initial Login
 From date: 08/01/2014 12:58
 To date: 08/02/2014 12:58
 Location:
 SSID:
 Language: English
 Group tag:
 Time left: 0,23,47

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ィールおよびゲスト ロールの 1.2) が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) サーバが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:

The screenshot shows a web interface for account creation. At the top, it says "Account Created" in blue. Below that, it says "Use the following information to sign on to the network." in blue. In the center, there is a red-bordered box containing the text "Email send failure" in red. Below this box, the user's details are listed: "First name:michal", "Last name:garcarz", and "Email:mgarcarz@cisco.com". At the bottom right, there is a blue button with the text "Sign On" in white.

quest.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:

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes the Cisco logo, the text "Identity Services Engine", and links for "Home" and "Operations". Below the navigation bar are three main menu items: "Configure", "Manage Accounts", and "Settings" (which is highlighted). The main content area is divided into three sections: "Guest Account Purge Policy", "Custom Fields", and "Guest Email Settings". The "Guest Email Settings" section is expanded, showing the SMTP server configuration. The SMTP server is set to "outbound.cisco.com". Below this, there is a link for "Administration > System > Settings > SMTP". There are three radio button options: "Enable email notifications to guests" (checked), "Use default email address", and "Use email address from sponsor". The "Use default email address" option is selected, and the default email address is shown as "ise_notification@cisco.com". At the bottom of the page, there is a "Sign On" button.

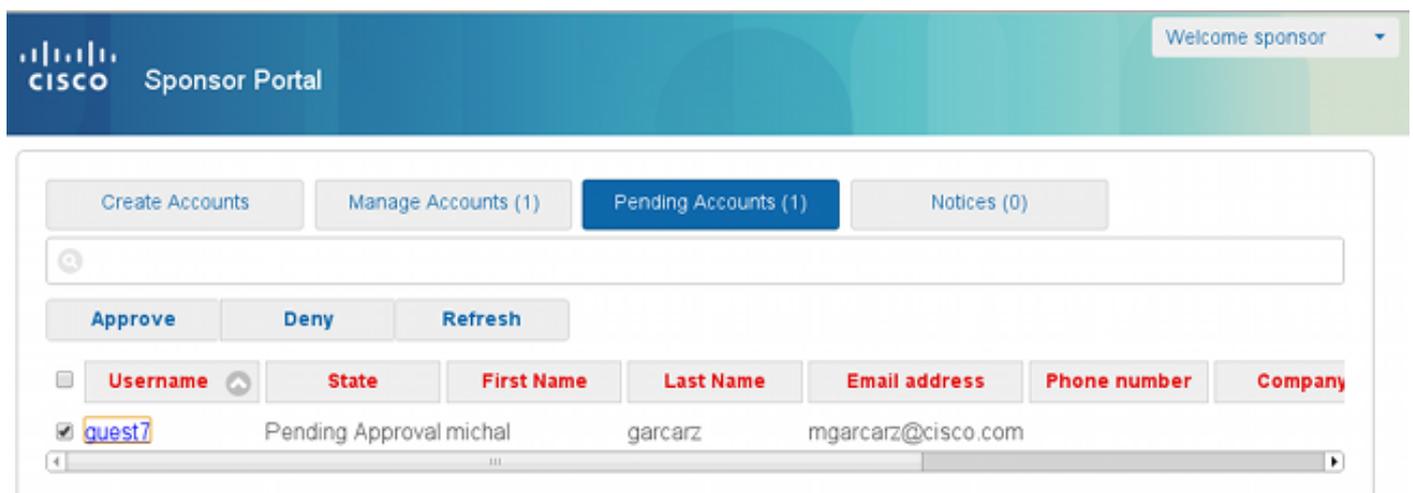
require によって自己登録されるゲストが承認されたオプションであることを可能にした後ユーザ名およびパスワードフィールドは含から自動的に自己登録成功ページセクションのこの情報削除されます。 こういうわけで、スポンサー承認が必要なときアカウントが作成されたことを示す

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:

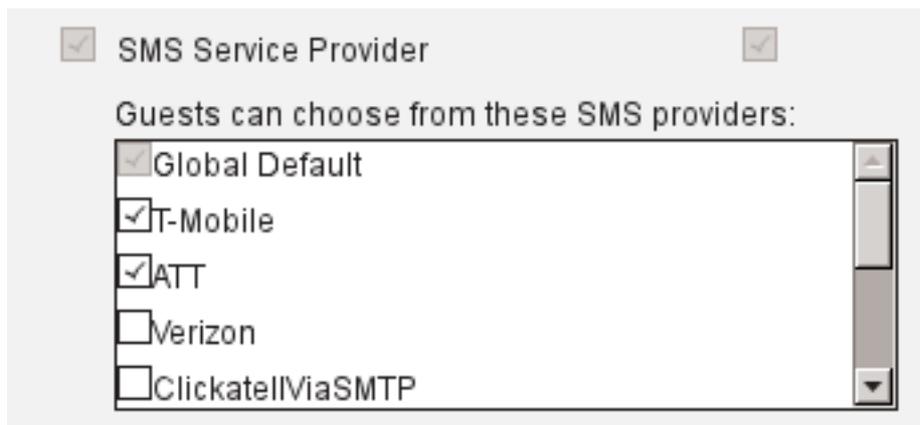
- 」アドレスからの通知「。これは統計的に定義されか、またはスポンサー アカウントから奪取され、アドレスからのとして両方のために使用されます: ゲストに (承認のために) およびクレデンシャル詳細後援すべき通知。これはゲスト アクセスの下で > 設定します > 設定 > ゲスト メール設定設定されます。
- アドレス指定すべき通知「」。これは承認のためのアカウントを受け取ったことスポンサーを知らせるために使用されます。これはゲスト アクセスの下でゲスト ポータルで > 設定します > ゲスト ポータル > 門脈名前 > > メール 承認要求に承認されるべき Require によって自己登録され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

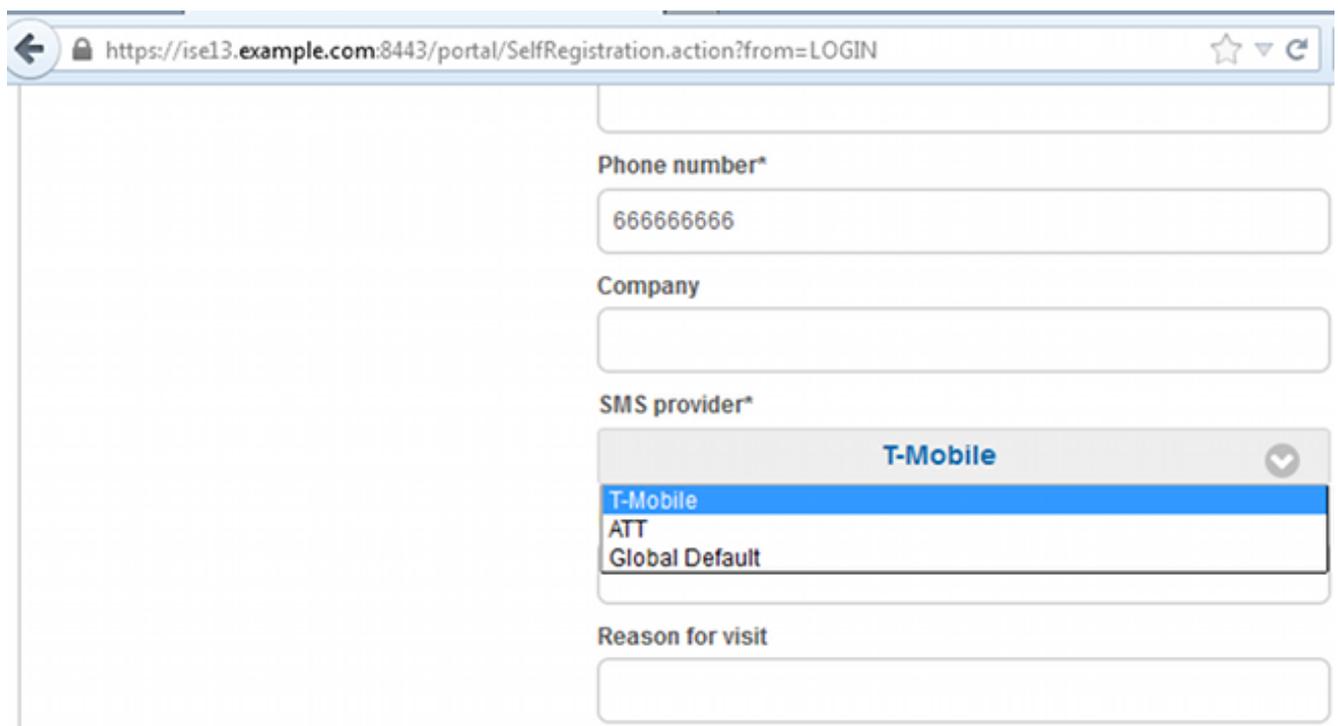
ゲスト信任状はまた SMS によって渡すことができます。これらのオプションは設定する必要があります:

1. SMS サービス プロバイダーを選択して下さい:



The screenshot shows a configuration window for SMS Service Providers. At the top, there is a checkbox labeled "SMS Service Provider" which is checked. Below this, the text "Guests can choose from these SMS providers:" is displayed. Underneath, there is a list of providers with checkboxes: "Global Default" (checked), "T-Mobile" (checked), "ATT" (checked), "Verizon" (unchecked), and "ClickatellViaSMTP" (unchecked).

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:



The screenshot shows a web browser window with the URL <https://ise13.example.com:8443/portal/SelfRegistration.action?from=LOGIN>. The form contains the following fields: "Phone number*" with the value "666666666", "Company", "SMS provider*" with a dropdown menu showing "T-Mobile" selected and options "T-Mobile", "ATT", and "Global Default" visible, and "Reason for visit".

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:

Account Created

Use the following information to sign on to the network.

First name:michal
Last name:garcarz
Email:mgarcarz@cisco.com
Phone number:666666666
SMS Provider:Global Default

Sign On

- 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:

The screenshot shows the 'Device Registration' page in the Cisco Sponsored Guest Portal. At the top, there is a Cisco logo and the text 'Sponsored Guest Portal'. Below this, the page title is 'Device Registration'. A note states: 'You can add a maximum of \$guest.device_limit\$ devices. Enter a device ID and device description. The device ID is the MAC address or Wi-Fi address of the device. It is an alphanumeric ID in this format: A1:B3:E5:19:6F:BB'. There are two input fields: 'Device ID' and 'Device Description'. Below these fields are three buttons: 'Add', 'Save, continue', and 'Cancel, continue'. At the bottom, there is a section titled 'Manage Devices (1)' which contains a table with one row: '64:66:B3:08:23:A3' and a 'Delete' button.

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:

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Guest_Compliant	if GuestEndpoints AND (Radius:Called-Station-ID CONTAINS Guest AND Session:PostureStatus EQUALS Compliant)	then PermitInternet
✓	Guest	if GuestEndpoints AND Radius:Called-Station-ID CONTAINS Guest	then LimitedAccess
✓	Guest_Authenticate	if Radius:Called-Station-ID CONTAINS Guest	then Guest

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:

Device Security Check

ISE is not able to apply an access policy to your log-in session at this time. Please close this browser, wait approximately one minute, and try to connect again. If you are still not able to log-in, please contact your network administrator.

[Contact Support](#)

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:

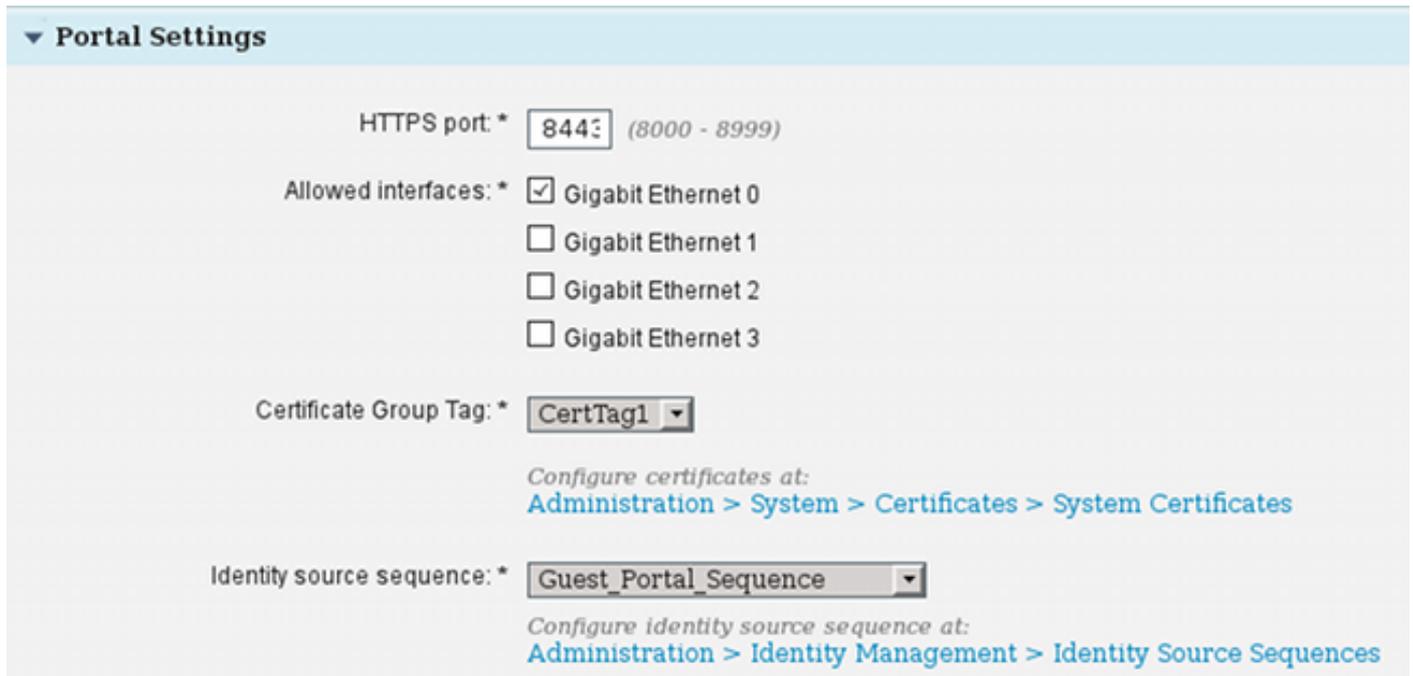
```
2014-08-01 21:35:08,435 ERROR [http-bio-10.62.97.21-8443-exec-9][ ] guestaccess.  
flowmanager.step.guest.ClientProvStepExecutor --7AAF75982E0FCD594FE97DE2970D472F::--  
CP Response is not successful, status=NO_POLICY
```

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:



The screenshot shows the 'Portal Settings' configuration page. It includes the following fields and options:

- HTTPS port:** * 8443 (8000 - 8999)
- Allowed interfaces:** *
 - Gigabit Ethernet 0
 - Gigabit Ethernet 1
 - Gigabit Ethernet 2
 - Gigabit Ethernet 3
- Certificate Group Tag:** * CertTag1
- Configure certificates at:*
[Administration > System > Certificates > System Certificates](#)
- Identity source sequence:** * Guest_Portal_Sequence
- Configure identity source sequence at:*
[Administration > Identity Management > Identity Source Sequences](#)

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 がリリースし、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](#)