Exemplo de configuração registrado auto do portal do convidado da versão 1.3 ISE

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Topologia e fluxo
Configurar
WLC
ISE
Verificar
Troubleshooting
Configuração opcional
Ajustes do Auto-registro
Ajustes do convidado do início de uma sessão
Ajustes do registro do dispositivo
Ajustes da conformidade do dispositivo do convidado
Ajustes BYOD
Contas Patrocinador-aprovadas
Entregue credenciais através de SMS
Registro do dispositivo
Postura
BYOD
Alteração de VLAN
Informações Relacionadas

Introdução

A versão 1.3 do Cisco Identity Services Engine (ISE) tem um novo tipo de portal do convidado chamado o portal registrado auto do convidado, que permite o auto-registro dos usuários convidado quando acede aos recursos de rede. Este portal permite que você configure e personalize características múltiplas. Este documento descreve como configurar e pesquisar defeitos esta funcionalidade.

Pré-requisitos

Requisitos

Cisco recomenda que você tem a experiência com configuração ISE e conhecimento básico destes assuntos:

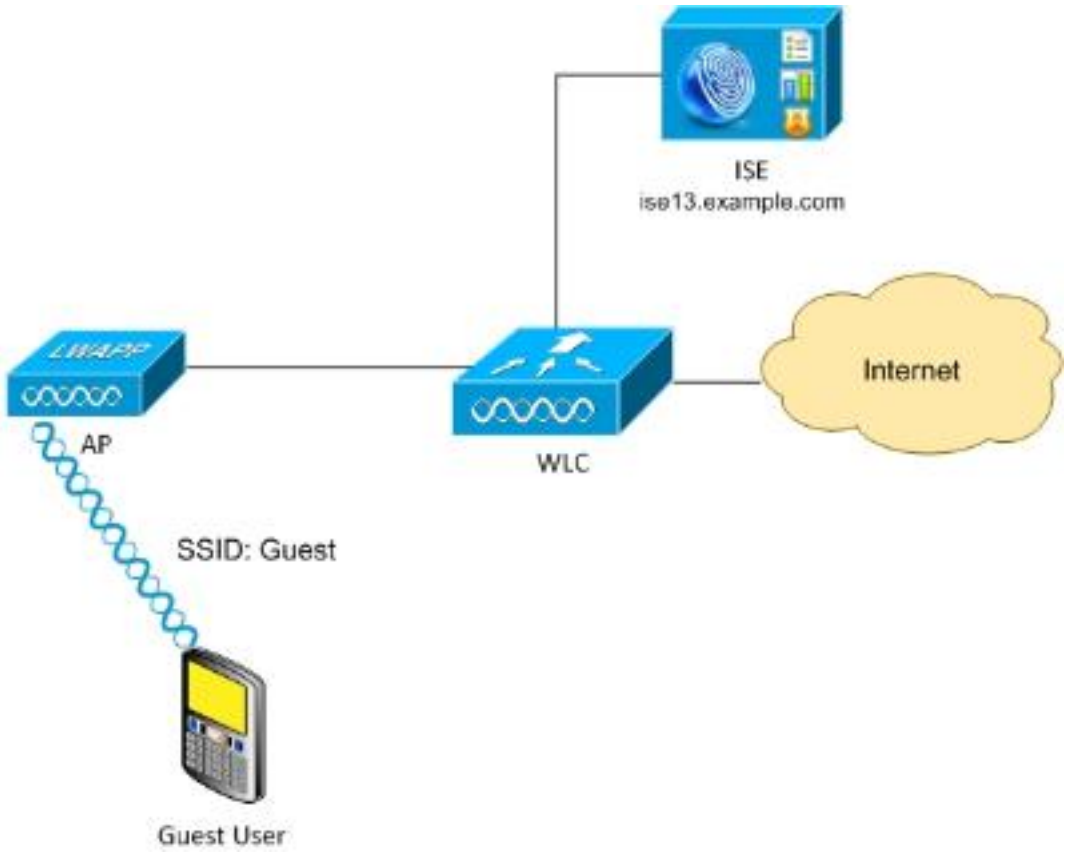
- Disposições ISE e fluxos do convidado
- Configuração dos controladores do Wireless LAN (WLC)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Microsoft Windows 7
- Versão 7.6 e mais recente de Cisco WLC
- Software ISE, versão 3.1 e mais recente

Topologia e fluxo



Esta encenação apresenta as opções múltiplas disponíveis para usuários convidado quando executam o auto-registro.

Está aqui o fluxo geral:

Etapa 1. Associados do usuário convidado ao Service Set Identifier (SSID): Convidado. Esta é uma rede aberta com o MAC que filtra com o ISE para a autenticação. Esta autenticação combina a segunda regra da autorização no ISE e o perfil da autorização reorienta ao portal registrado auto do convidado. O ISE retorna uma aceitação de acesso do RAIO com dois pares Cisco AV:

- URL-reorientar-ACL (que o tráfego deve ser reorientado, e o nome do Access Control List (ACL) definido localmente no WLC)
- URL-reoriente (onde reorientar esse tráfego ao ISE)

Etapa 2. O usuário convidado é reorientado ao ISE. Um pouco do que fornecem as credenciais a fim entrar, o usuário que os cliques “não têm uma conta”. O usuário é reorientado a uma página onde essa conta possa ser criada. Um código secreto opcional do registro pôde ser permitido a fim limitar o privilégio do auto-registro aos povos que conhecem esse valor secreto. Depois que a conta é criada, o usuário é credenciais fornecidas (nome de usuário e senha) e entra com aquelas credenciais.

Etapa 3. O ISE envia uma mudança do RAIO da autorização (CoA) Reauthenticate ao WLC. O WLC autenticar novamente o usuário quando envia a solicitação de acesso do RAIO com o atributo da autorização-Somente. O ISE responde com a aceitação de acesso e o Airespace ACL definidos localmente no WLC, que fornece o acesso ao Internet somente (o acesso final para o usuário convidado depende da política da autorização).

Note que para sessões do Extensible Authentication Protocol (EAP), o ISE deve enviar um CoA termina a fim provocar a reautenticação porque a sessão EAP está entre o suplicante e o ISE. Mas para MAB (MAC que filtra), o CoA Reauthenticate é bastante; não há nenhuma necessidade de-associate/de-authenticate o cliente Wireless.

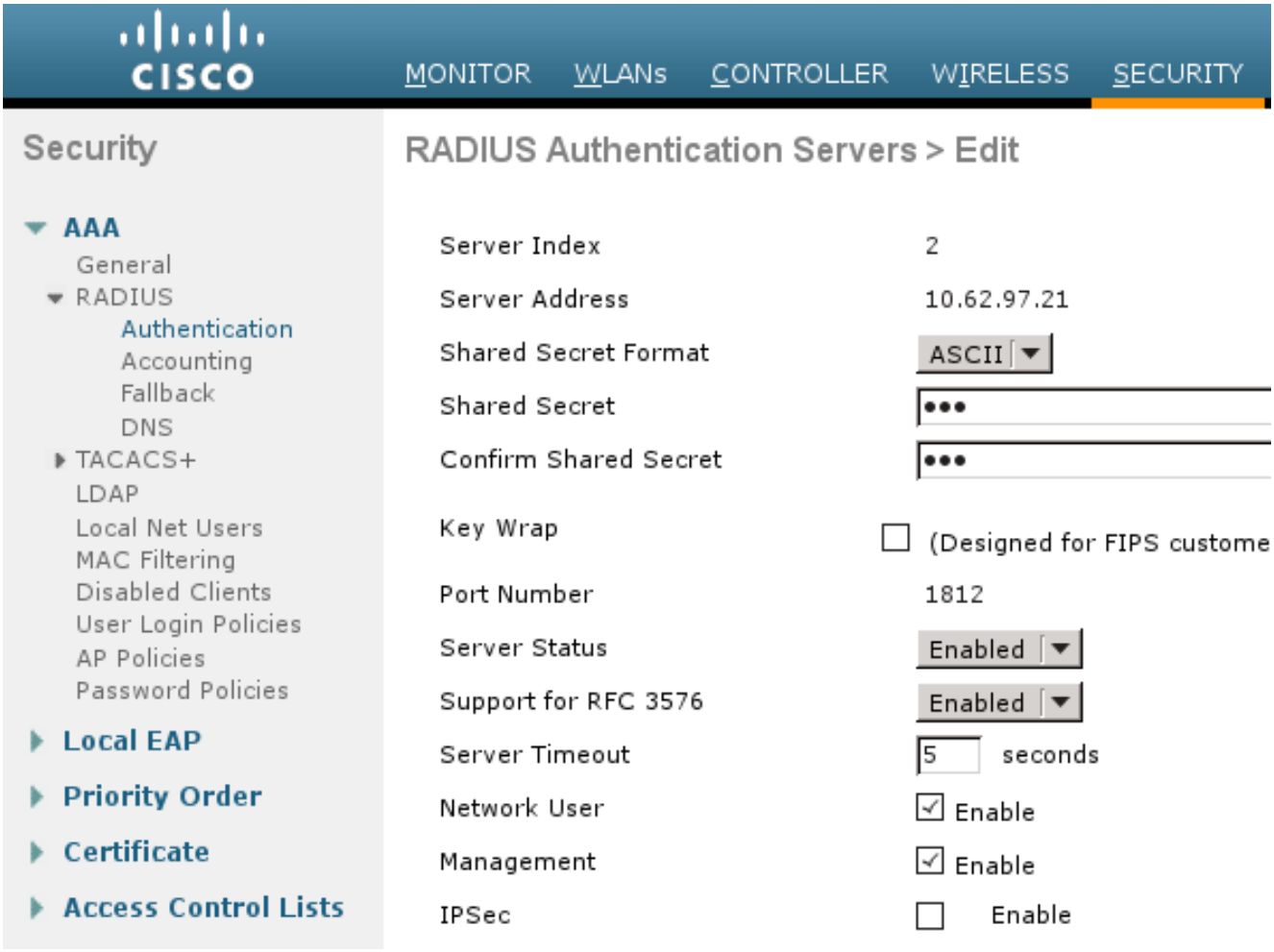
Etapa 4. O usuário convidado desejou o acesso à rede.

Os recursos adicionais múltiplos como a postura e o Bring Your Own Device (BYOD) podem ser permitidos (discutido mais tarde).

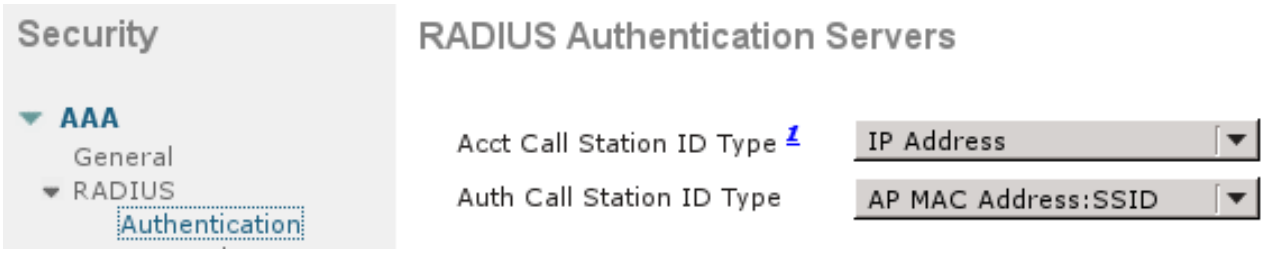
Configurar

WLC

1. Adicionar o servidor Radius novo para a autenticação e a contabilidade. Navegue à **Segurança > ao AAA > ao raio > à autenticação** a fim permitir CoA do RAIO (RFC 3576).



Há uma configuração similar para explicar. Igualmente recomenda-se configurar o WLC para enviar o SSID no atributo da estação chamada ID, que permite que o ISE configure as regras flexíveis baseadas no SSID:



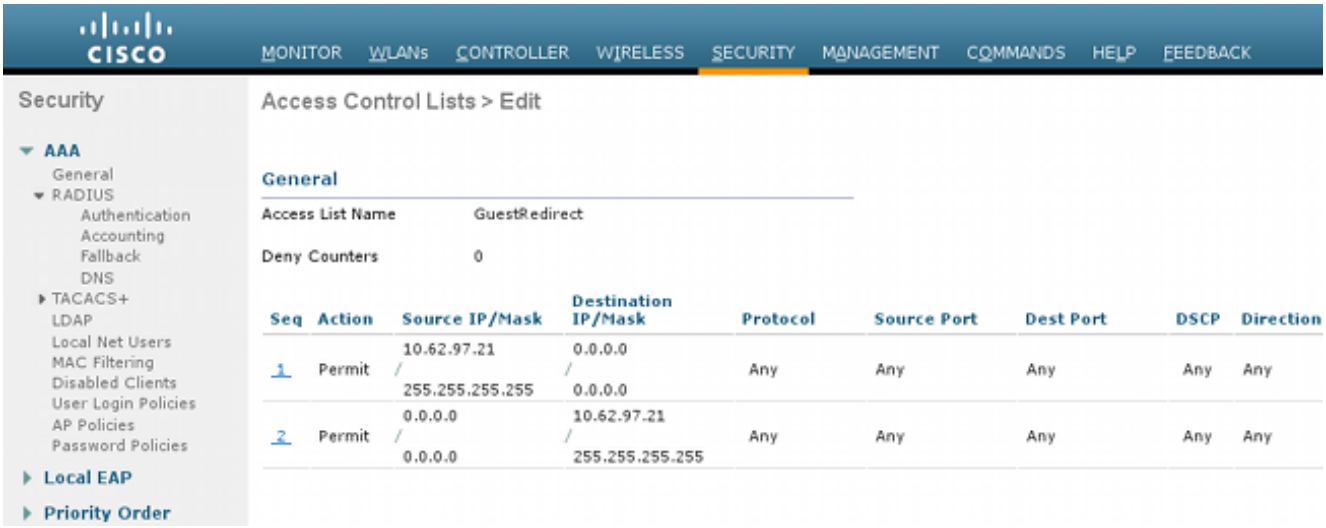
2. Sob os WLAN catalogue, crie o convidado do Wireless LAN (WLAN) e configurar a relação correta. Ajuste a Segurança Layer2 a **nenhuns** com filtração MAC. Em server da Segurança/Authentication, Authorization, and Accounting (AAA), selecione o endereço IP de Um ou Mais Servidores Cisco ICM NT ISE para a autenticação e a contabilidade. No guia avançada, permita a **ultrapassagem AAA** e ajuste o estado do Network Admission Control (NAC) ao RAIO NAC (apoio CoA).

3. Navegue à **Segurança > às listas de controle de acesso > às listas de controle de acesso** e crie duas Listas de acesso:

   GuestRedirect, que permite o tráfego que não deve ser reorientado e reorienta todo tráfego restanteInternet, que é negado para redes corporativas e permitido para todo o outro

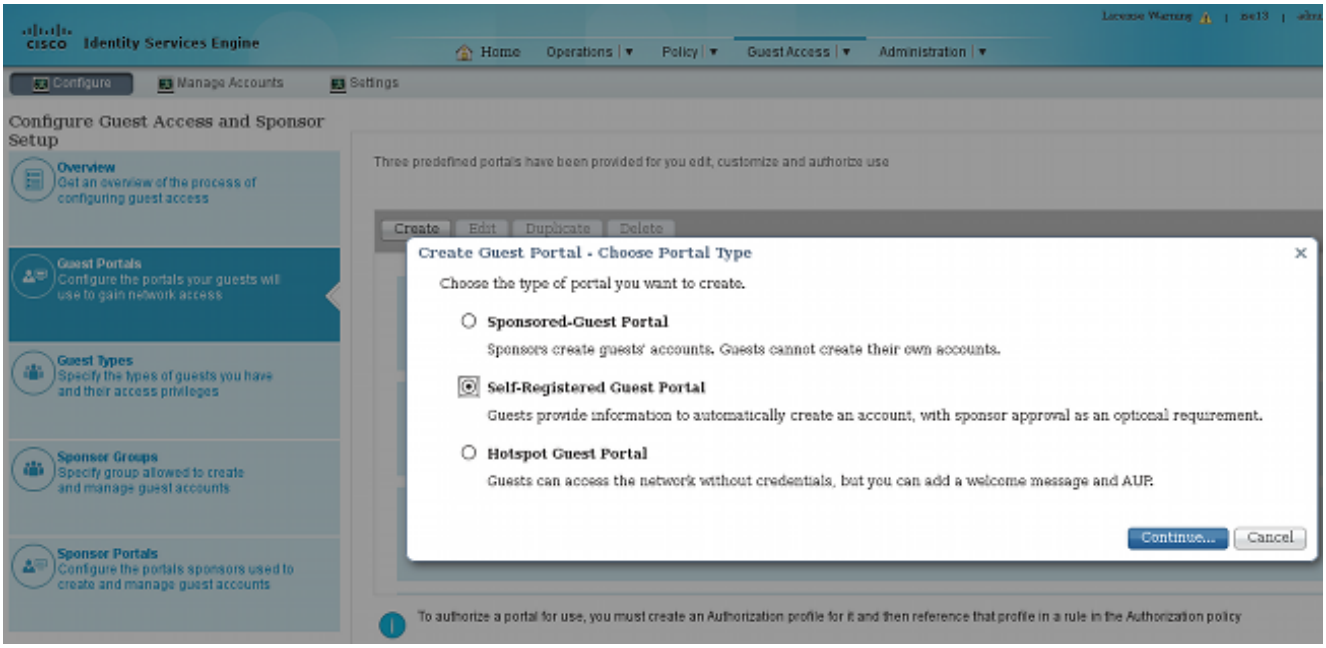
   Está aqui um exemplo para GuestRedirect ACL (necessidade de excluir o tráfego

para/desde o ISE da reorientação):



ISE

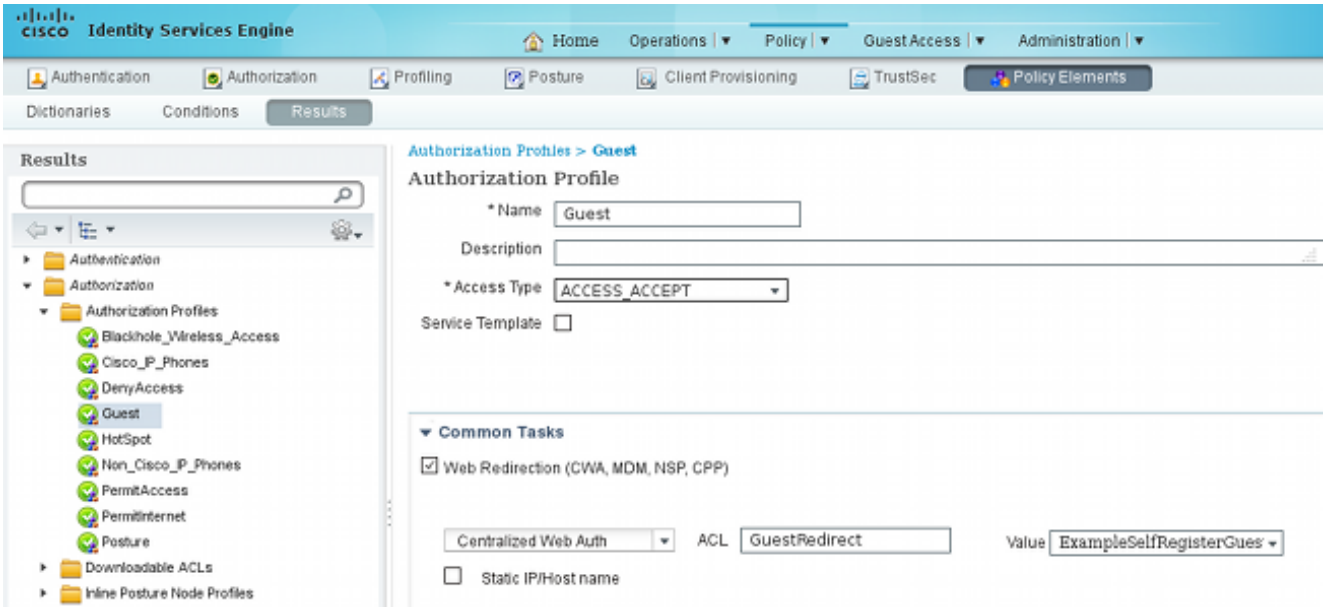
1. Navegue ao **acesso do convidado > configuram > portais do convidado**, e criam um tipo portal novo, portal registrado auto do convidado:



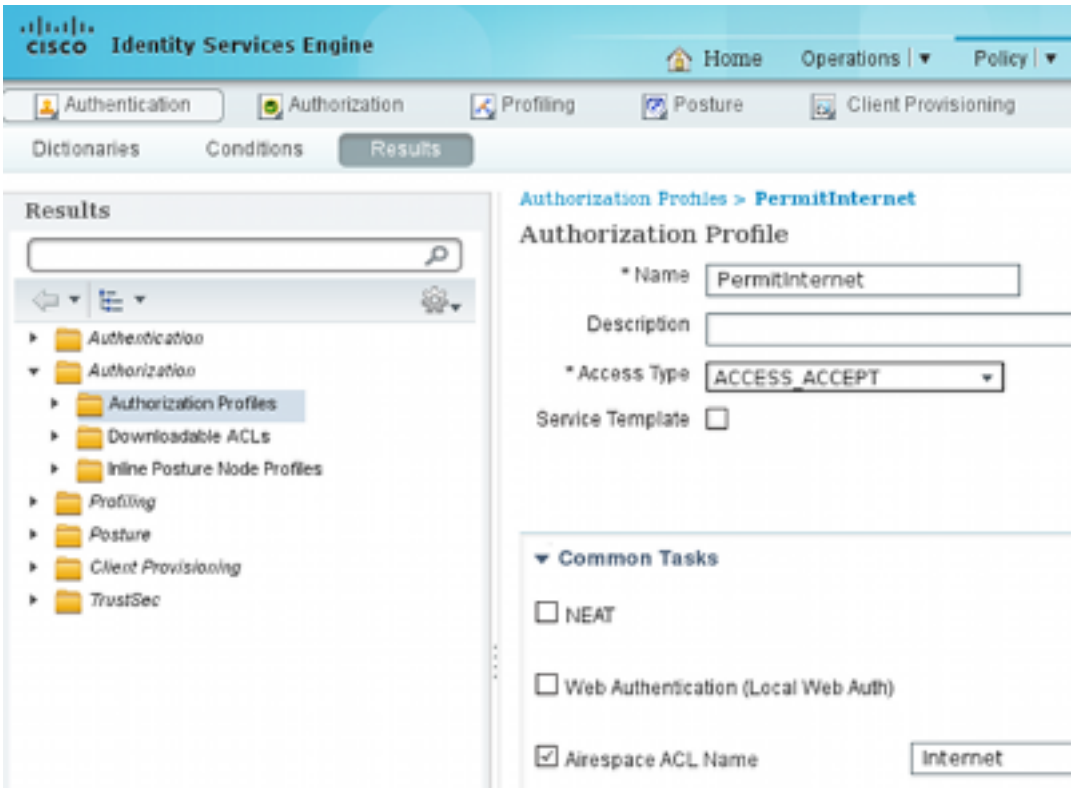
2. Escolha o nome portal que será provido no perfil da autorização. Ajuste todos os outros ajustes para optar. Sob a personalização portal da página, todas as páginas apresentadas podem ser personalizadas.

3. Configurar perfis da autorização:

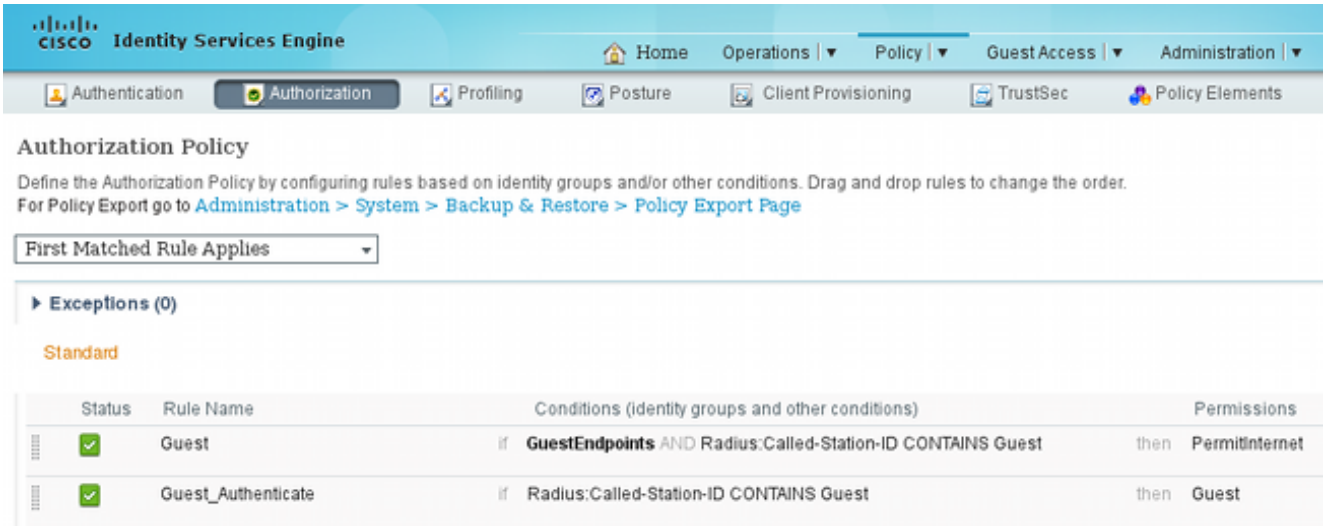
   Convidado (com reorientação ao nome portal do convidado e ao ACL GuestRedirect)



PermitInternet (com Internet do igual de Airespace ACL)



4. A fim verificar as regras da autorização, navegue à **política > à autorização**. Na versão 1.3 ISE para a autenticação falhada do acesso do desvio da autenticação de MAC (MAB) (MAC address não encontrado) é continuado à revelia (não rejeitado). Isto é muito útil para portais do convidado porque não há nenhuma necessidade de mudar qualquer coisa em regras da autenticação padrão.



Os novos usuários que associam ao convidado SSID não são ainda parte de qualquer grupo da identidade. Eis porque combinam a segunda regra, que usa o perfil da autorização do convidado para os reorientar ao portal correto do convidado.

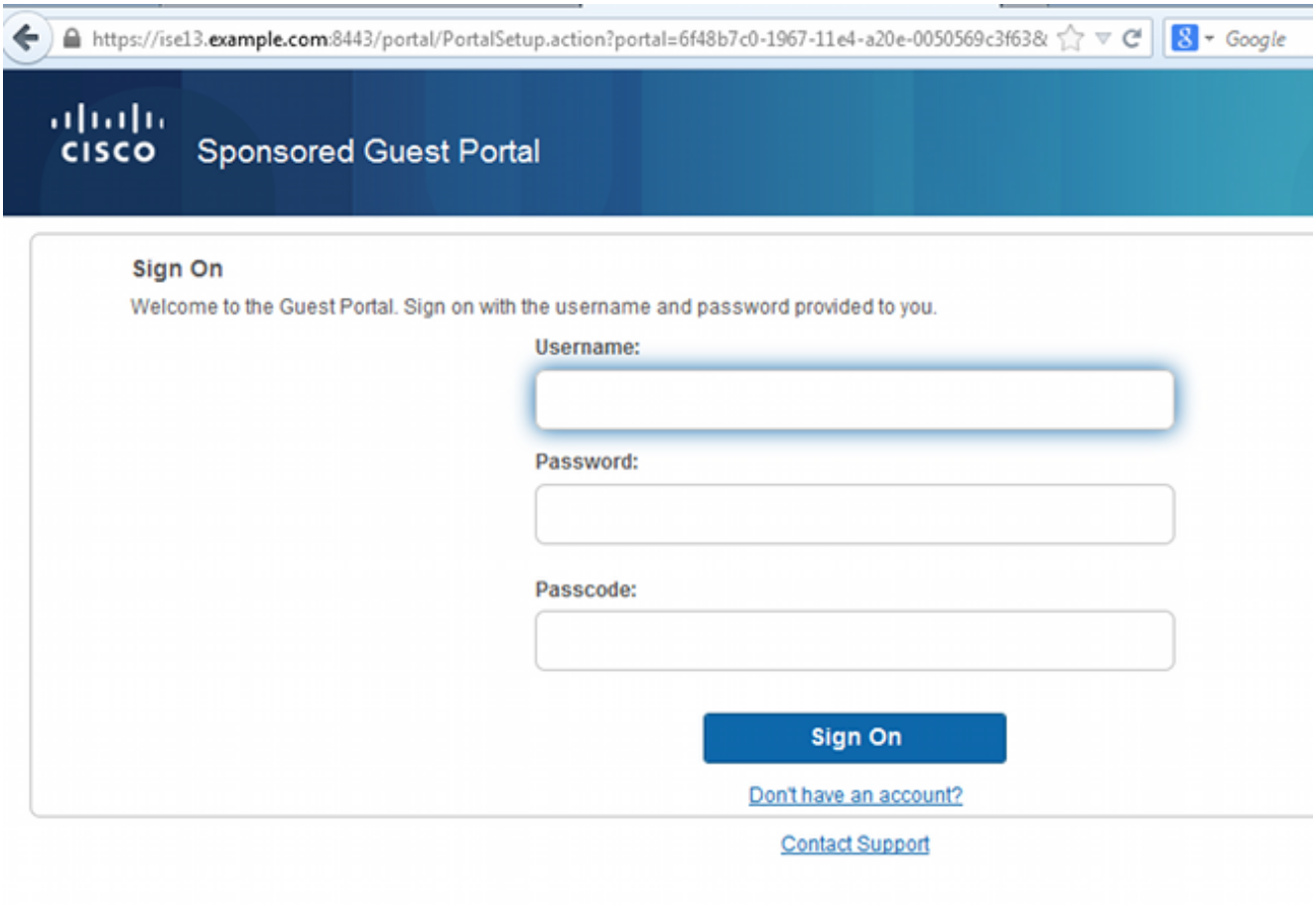
Depois que um usuário cria uma conta e entra com sucesso, o ISE envia um CoA do RAIO e o WLC executa a reautenticação. Esta vez, a primeira regra é combinada junto com o perfil PermitInternet da autorização e retorna o nome ACL que é aplicado no WLC.

5. Adicionar o WLC como um dispositivo do acesso de rede da **administração > dos recursos de rede > dos dispositivos de rede**.

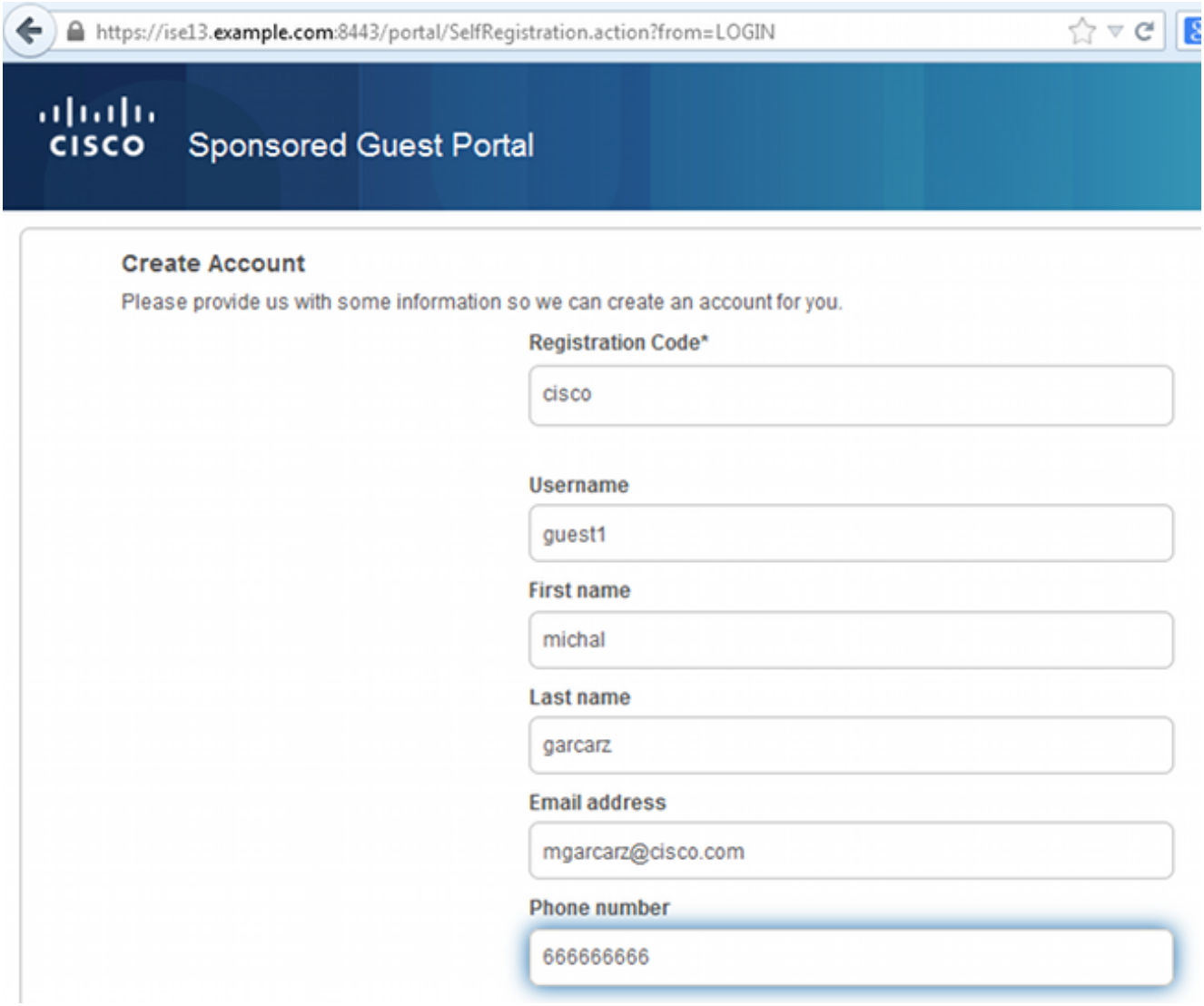
Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

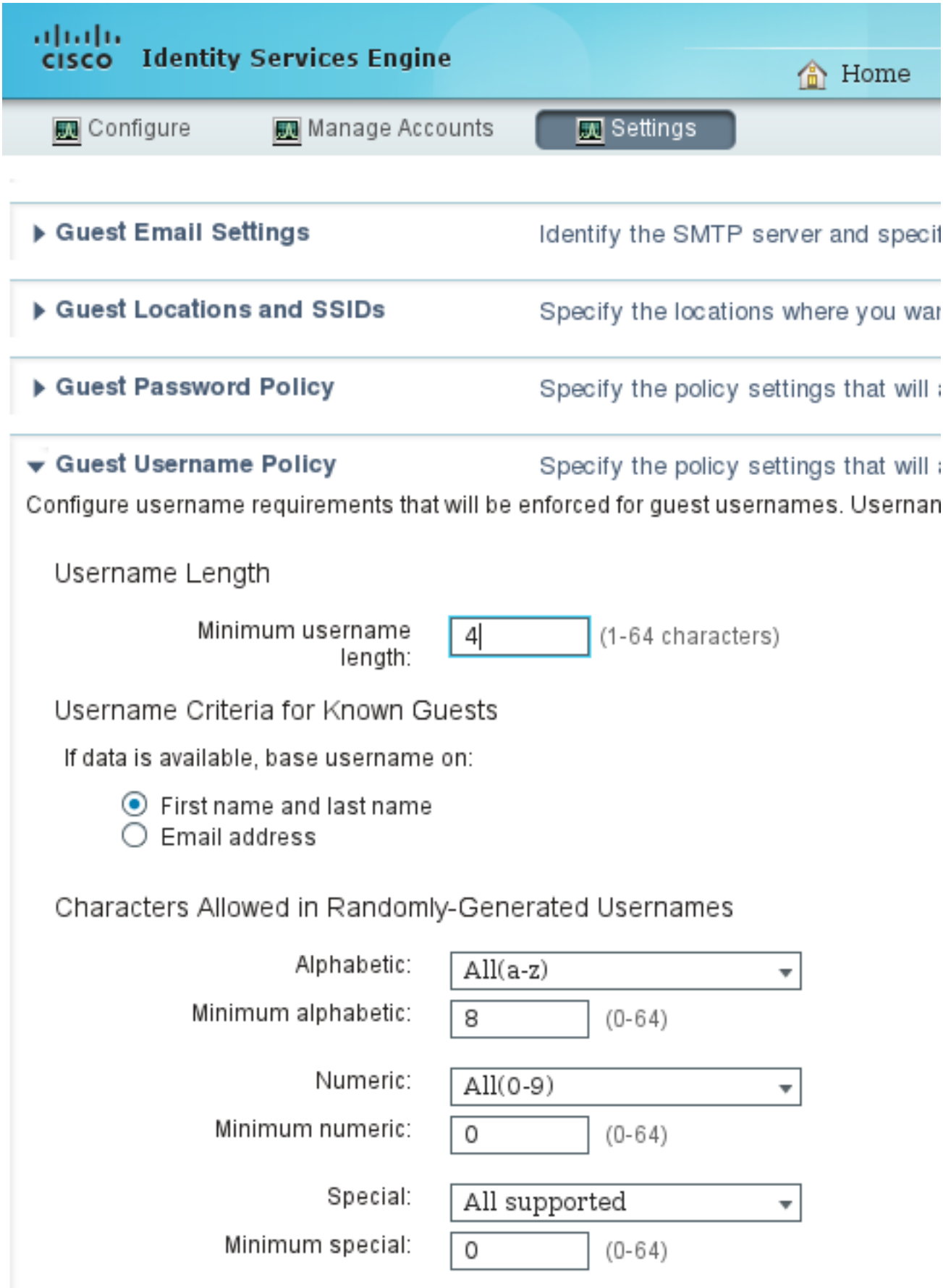
1. Depois que você associa com o convidado SSID e datilografa uma URL, a seguir você está reorientado à página de login:



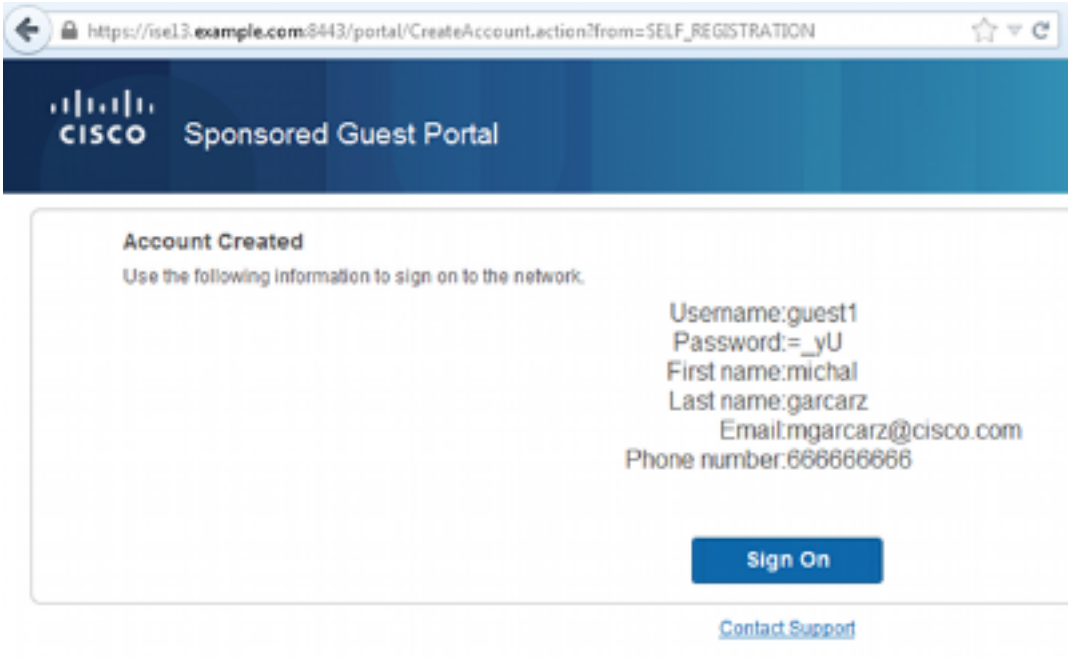
2. Desde que você não tem nenhumas credenciais ainda, você deve escolher **não tem uma conta?** opção. Uma página nova que permita indicadores da criação de conta. Se a opção do código do registro foi permitida sob a configuração portal do convidado, esse valor secreto é exigido (este se assegura de que somente o auto-registro esteja permitido aos povos com permissões correta).



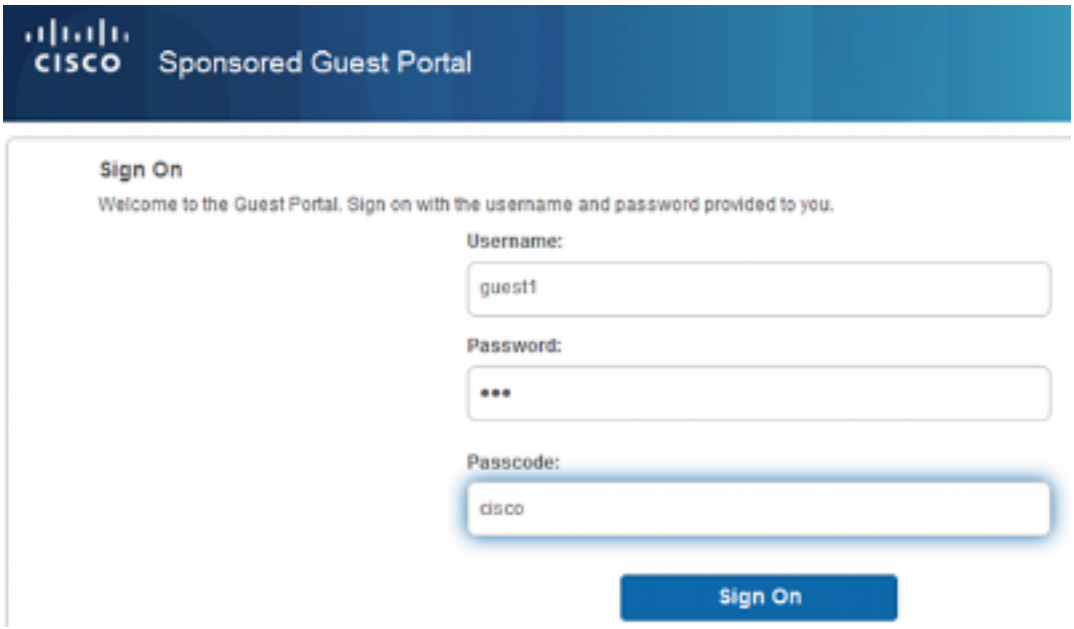
3. Se há algum problema com a senha ou a política de usuário, navegue ao **acesso do convidado > aos ajustes > à política de senha do convidado ou ao acesso do convidado > aos ajustes > à política username do convidado** a fim mudar ajustes. Aqui está um exemplo:



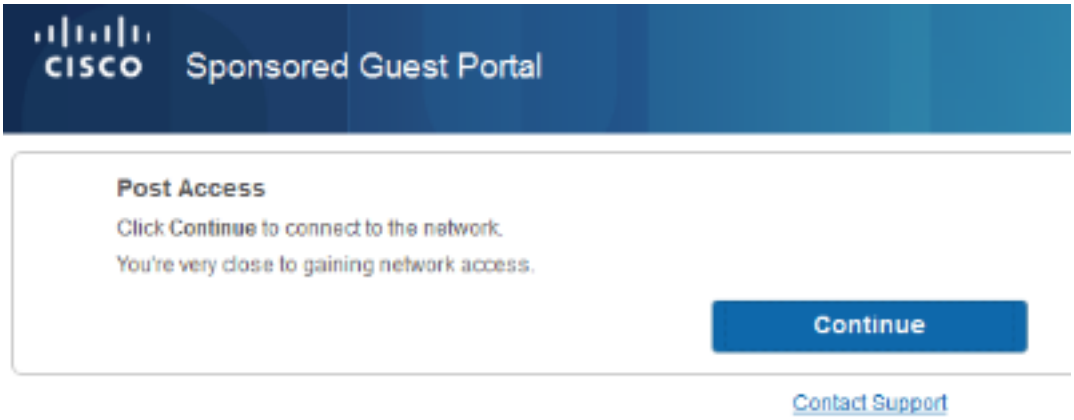
4. Após a criação de conta bem sucedida, você é presentado com credenciais (senha gerada conforme políticas de senha do convidado):



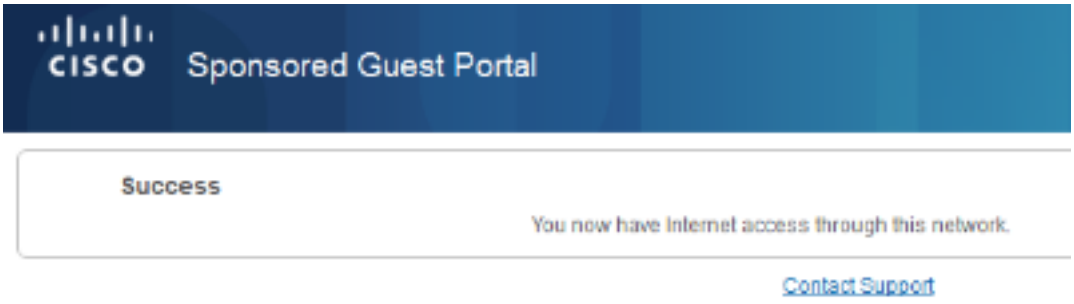
5. Clique o **sinal sobre** e forneça credenciais (a senha adicional do acesso pôde ser exigida se configurado sob o portal do convidado; este é um outro mecanismo de segurança que permita somente aqueles que conhecem a senha para entrar).



6. Quando bem sucedida, uma política de uso aceitável opcional (AUP) pôde ser apresentada (se configurado sob o portal do convidado). A página do acesso do cargo (também portal inferior configurável do convidado) pôde igualmente indicar.



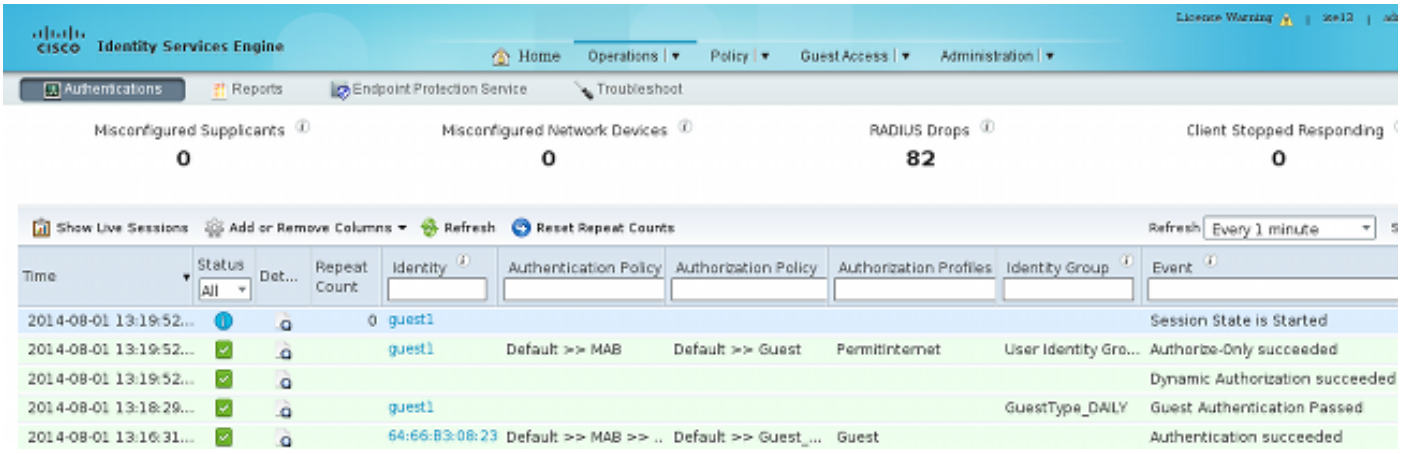
A última página confirma que o acesso esteve concedido:



Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

Nesta fase, o ISE apresenta estes logs:



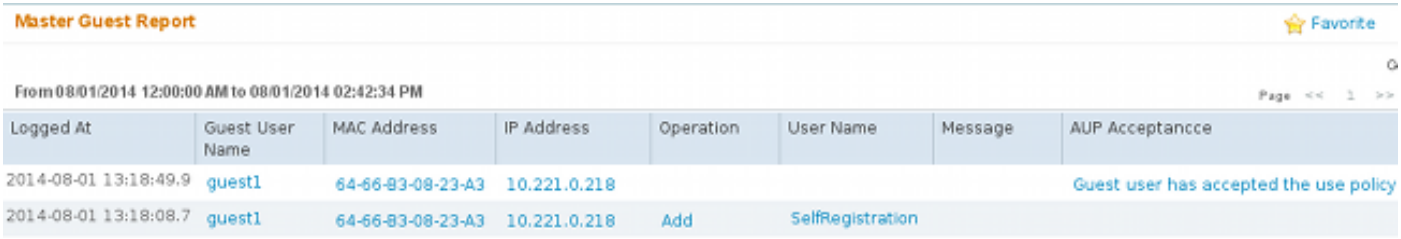
Está aqui o fluxo:

- O usuário convidado encontra a segunda regra da autorização (Guest_Authenticate) e é reorientado ao convidado (“Auhentication sucedeu”).

- O convidado é reorientado para o auto-registro. Depois que com sucesso o início de uma sessão (com a conta recém-criado), ISE envia o CoA Reauthenticate, que é confirmado pelo WLC (“autorização dinâmica sucedida”).

- O WLC executa a reautenticação com o atributo da autorização-Somente e o nome ACL é retornado (“Autorizar-Somente sucedeu”). O convidado é fornecido o acesso de rede correto.

Os relatórios (as **operações > relatam que > o ISE relata > relatórios do acesso do convidado > relatório do convidado do mestre**) igualmente confirmam aquele:


Master Guest Report

Favorite

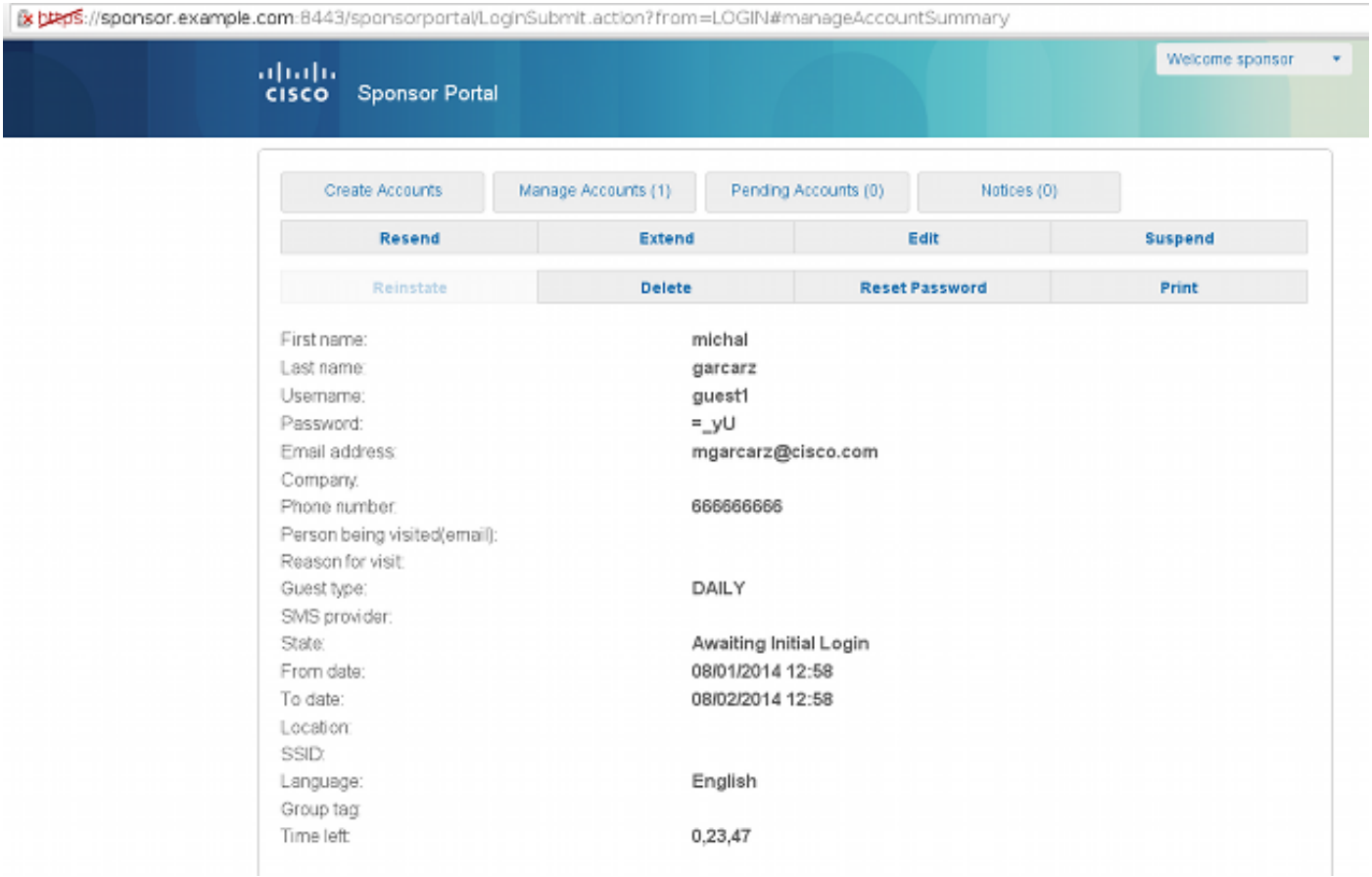
From 08/01/2014 12:00:00 AM to 08/01/2014 02:42:34 PM

Page << 1 >>

Logged At	Guest User Name	MAC Address	IP Address	Operation	User Name	Message	AUP Acceptancce
2014-08-01 13:18:49.9	guest1	64-66-B3-08-23-A3	10.221.0.218				Guest user has accepted the use policy
2014-08-01 13:18:08.7	guest1	64-66-B3-08-23-A3	10.221.0.218	Add	SelfRegistration		

Um usuário do patrocinador (com privilégios corretos) pode verificar o status atual de um usuário convidado.

Este exemplo confirma que a conta está criada, mas o usuário nunca entrou (“esperando o login inicial”):



Configuração opcional

Para cada fase deste fluxo, as opções diferentes podem ser configuradas. Toda a esta é configurada pelo portal do convidado no **acesso do convidado > configura > portais > PortalName do convidado > edita > ajustes portais do comportamento e do fluxo**. Uns ajustes mais importantes incluem:

Ajustes do Auto-registro

- Tipo do convidado - Descreve quanto tempo a conta é ativo, opções da expiração da senha, horas do fazer logon e opções (esta é a mistura do perfil e do papel de convidado do tempo da versão 1.2 ISE)
- Código do registro - Se permitidos, somente o auto-registro é permitido aos usuários que conhecem o código secreto (deve fornecer a senha quando a conta é criada)
- AUP - Aceite a política do uso durante o auto-registro
- A exigência para que o patrocinador aprove/ativa a conta do convidado

Ajustes do convidado do início de uma sessão

- Código de acesso - Se permitidos, somente são permitidos aos usuários convidado que conhecem o código secreto entrar
- AUP - Aceite a política do uso durante o auto-registro
- Opção da mudança da senha

Ajustes do registro do dispositivo

- Àrevelia, o dispositivo é registrado automaticamente

Ajustes da conformidade do dispositivo do convidado

- Permite uma postura dentro do fluxo

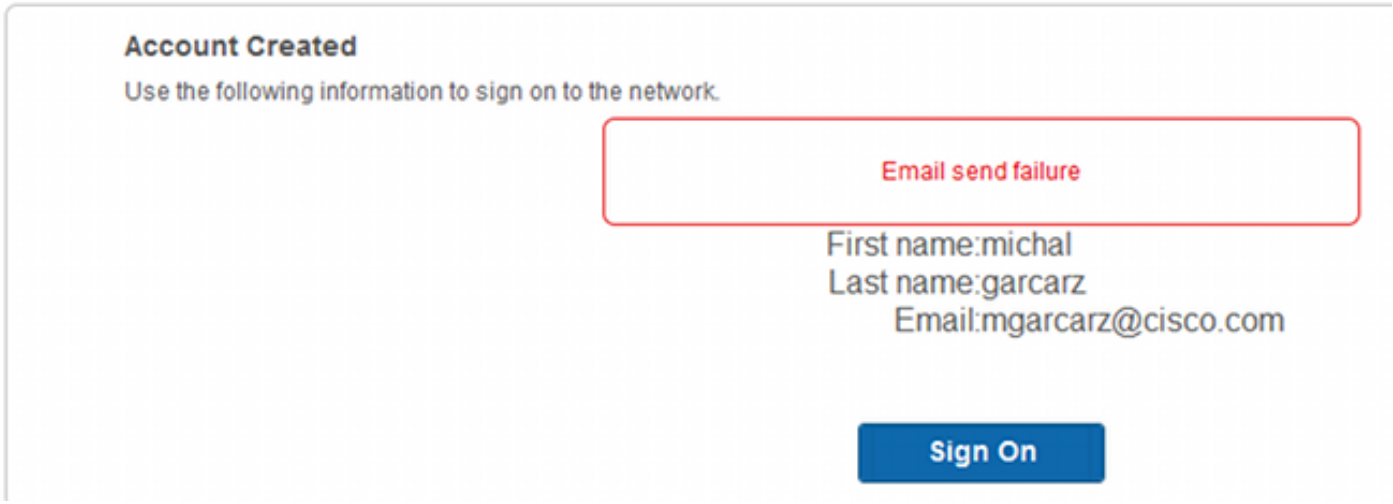
Ajustes BYOD

- Permite os usuários corporativos que usam o portal como convidados para registrar seus dispositivos pessoais

Contas Patrocinador-aprovadas

Se os **convidados auto-registrados Require a ser** opção **aprovada** são selecionados, a seguir a conta criada pelo convidado deve ser aprovada por um patrocinador. Esta característica pôde usar o email a fim entregar a notificação ao patrocinador (para a aprovação da conta do convidado):

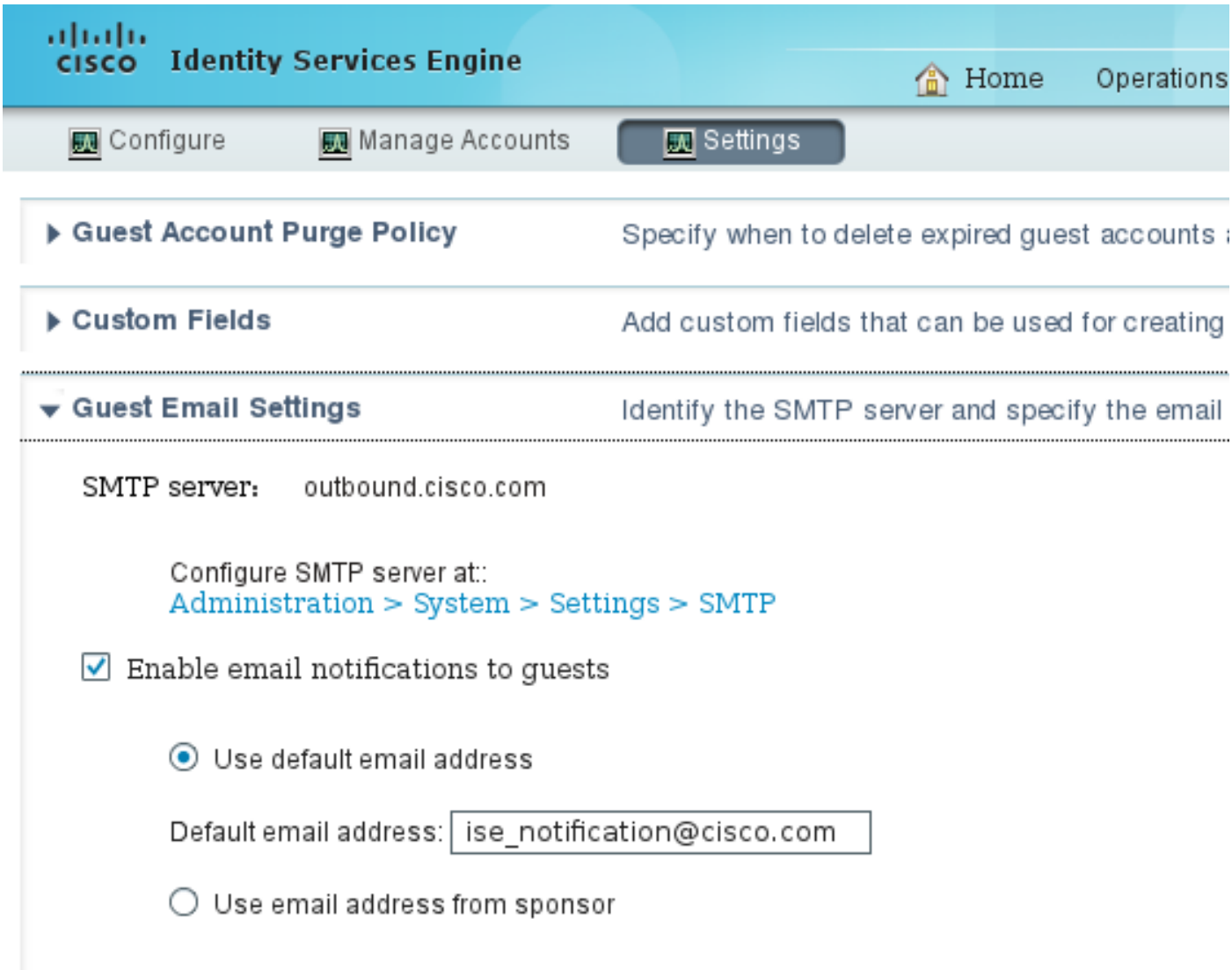
Se o server ou o padrão do Simple Mail Transfer Protocol (SMTP) da notificação do email não são configurados, a seguir a conta não estará criada:

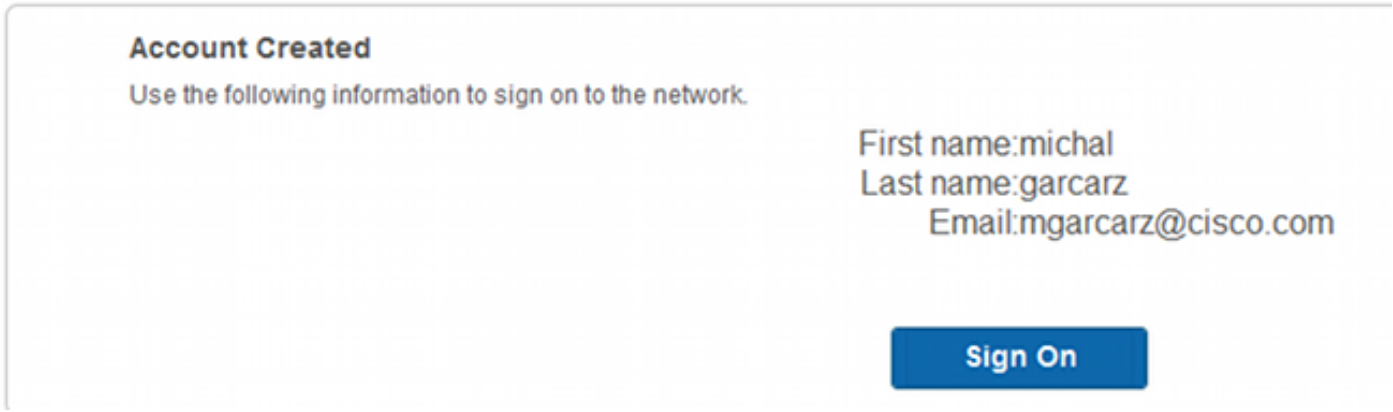


O log de guest.log confirma que o global do endereço usado para a notificação falta:

```
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.
```

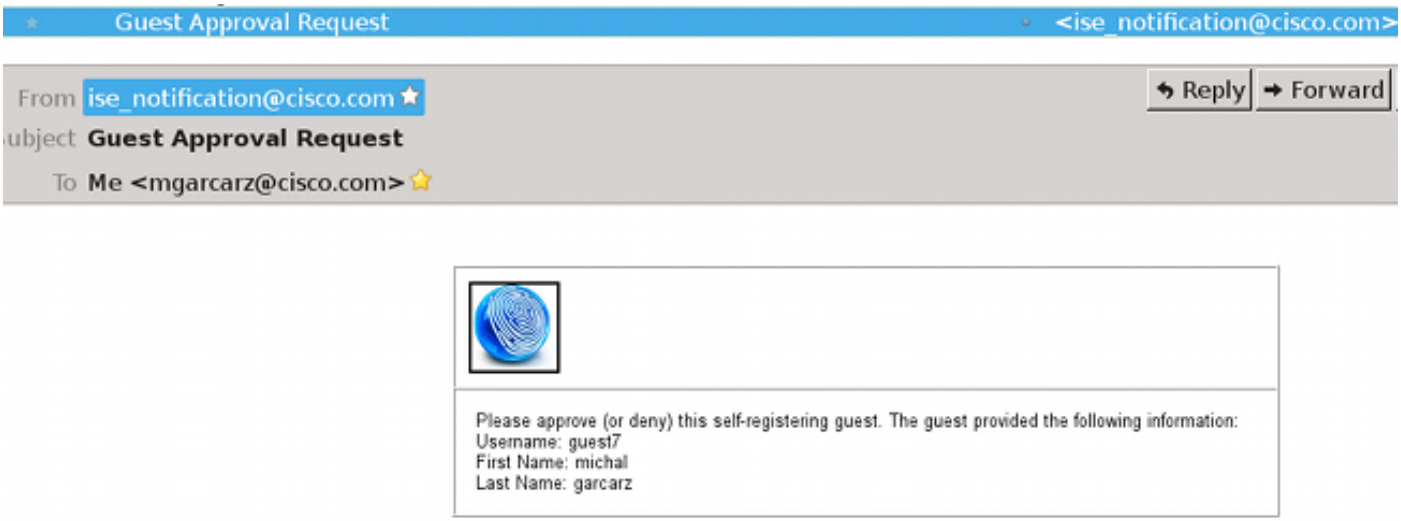
Quando você tem a configuração apropriada do email, a conta está criada:



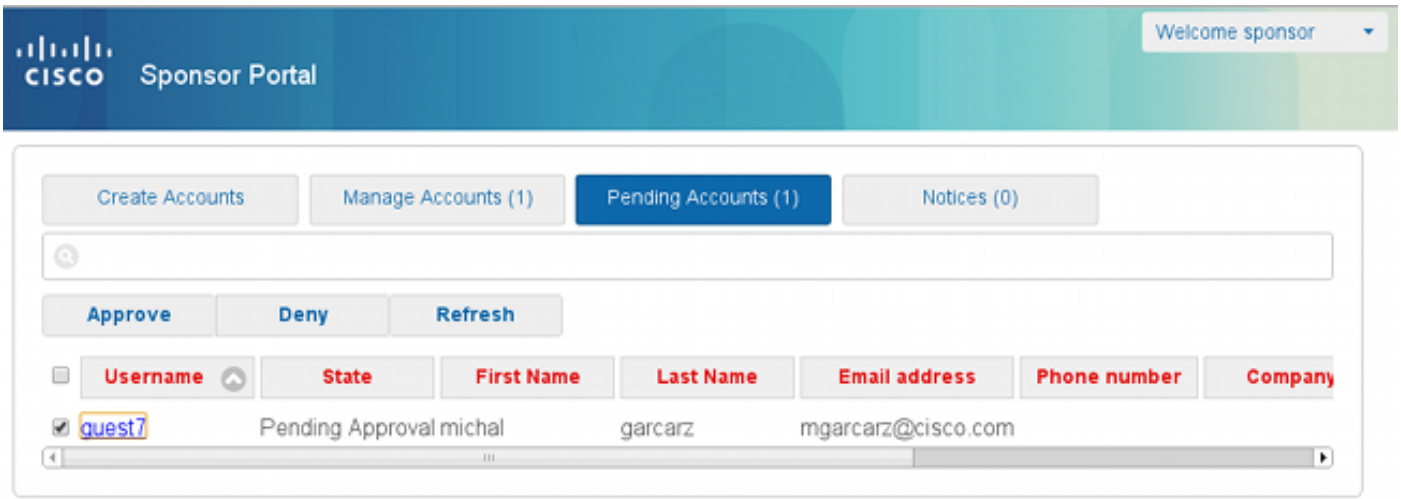


Depois que você permite os **convidados auto-registrados Require de ser** opção **aprovada**, os campos do nome de usuário e senha estão removidos automaticamente **incluir esta informação na** seção da **página do sucesso do Auto-registro**. Eis porque, quando a aprovação do patrocinador é precisada, as credenciais para usuários convidado não são indicadas à revelia no página da web que apresenta a informação para mostrar que a conta esteve criada. Em lugar de devem ser entregados por serviços de mensagem curtos (SMS) ou por email. Esta opção deve ser permitida na **notificação credencial da emissão em cima da aprovação usando a** seção (marca email/SMS).

Uma notificação de e-mail é entregada ao patrocinador:



Os logs do patrocinador no portal do patrocinador e aprovam a conta:



A partir daqui, é permitido ao usuário convidado entrar (com as credenciais recebidas pelo email ou pelo SMS).

Em resumo, há três endereços email usados neste fluxo:

- Notificação “” do endereço. Isto é definido estaticamente ou tomado da conta do patrocinador e usado como do endereço para ambos: notificação a patrocinar (para a aprovação) e detalhes credenciais ao convidado. Isto é configurado sob o **acesso do convidado > configura > ajustes > ajustes do email do convidado**.

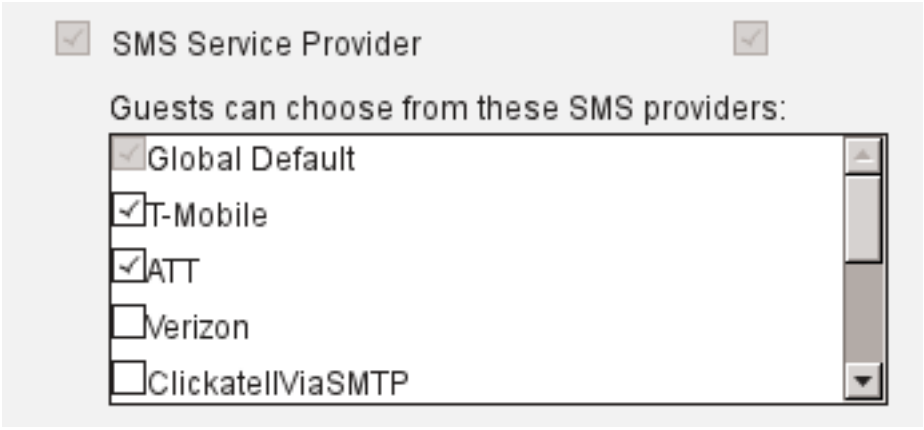
- Notificação “” a endereçar. Isto é usado a fim notificar o patrocinador que recebeu uma aprovação esclarecer. Isto é configurado no portal do convidado sob o **acesso do convidado > configura > portais do convidado > nome portal > os convidados auto-registrados Require a ser aprovados > requisição de aprovação do email a**.

- Convidado “” a endereçar. Isto é fornecido pelo usuário convidado durante o registro. Se **envie a notificação credencial em cima da aprovação que usa o email** está selecionada, o email com detalhes credenciais (nome de usuário e senha) está entregada ao convidado.

Entregue credenciais através de SMS

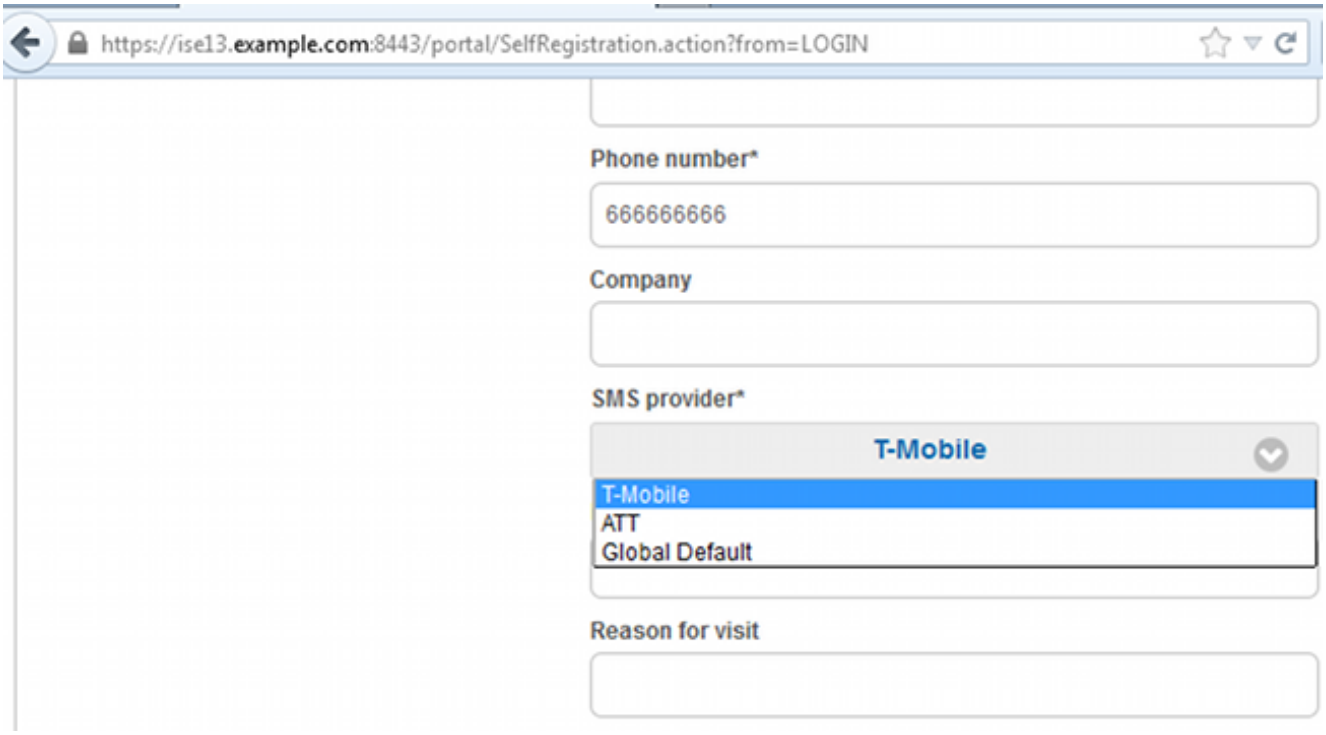
As credenciais do convidado podem igualmente ser entregadas por SMS. Estas opções devem ser configuradas:

1. Escolha o provedor de serviços de SMS:

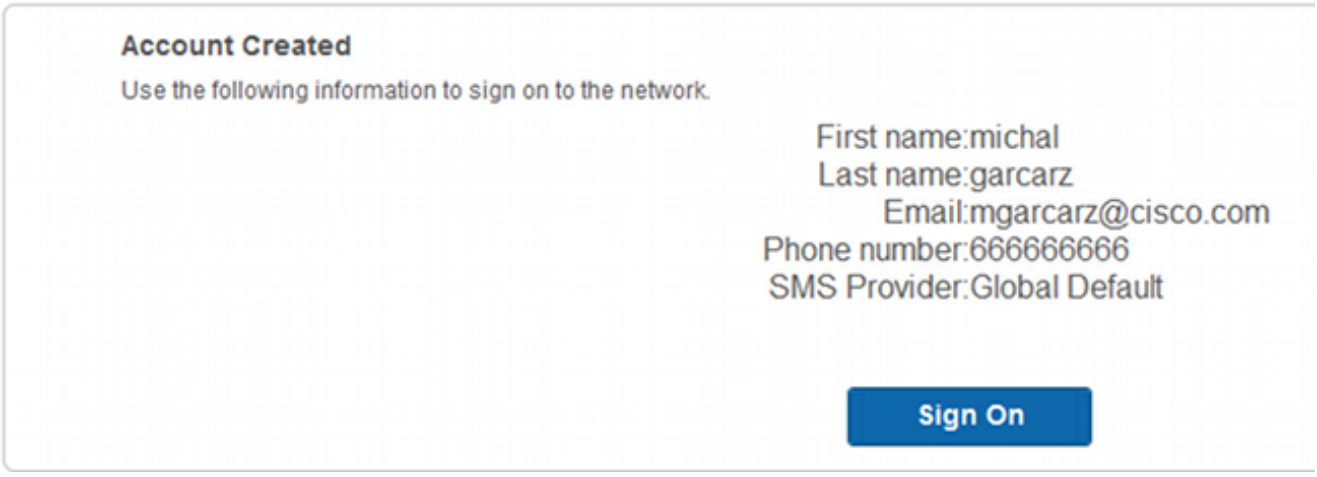


2. Verifique a **notificação credencial da emissão em cima da utilização da aprovação:** Caixa de verificação de **SMS**.

3. Então, o usuário convidado está pedido para escolher o fornecedor disponível quando cria uma conta:



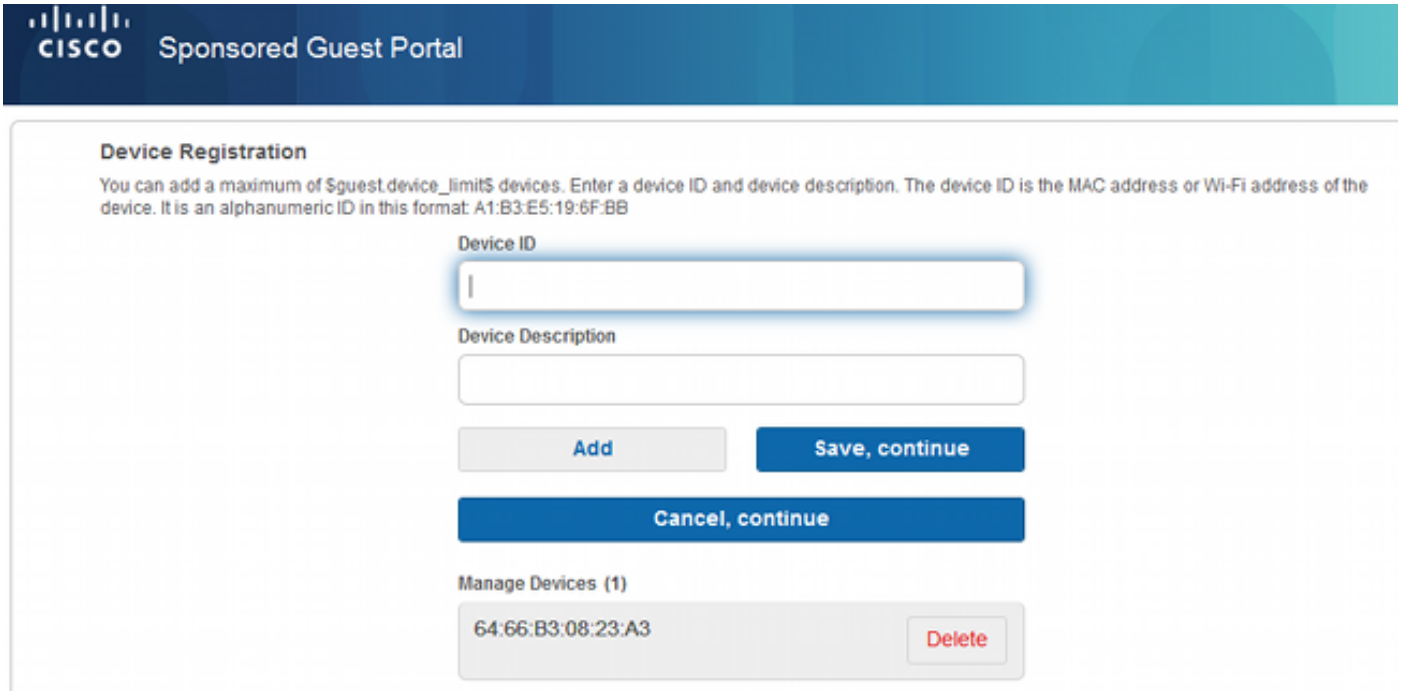
4. SMS é entregado com o fornecedor e o número de telefone escolhidos:



5. Você pode configurar fornecedores de SMS sob a **administração > o sistema > os ajustes > o gateway de SMS**.

Registro do dispositivo

Se os **convidados reservar para registrar a opção de dispositivos** são selecionados depois que um usuário convidado entra e aceita o AUP, você pode registrar dispositivos:

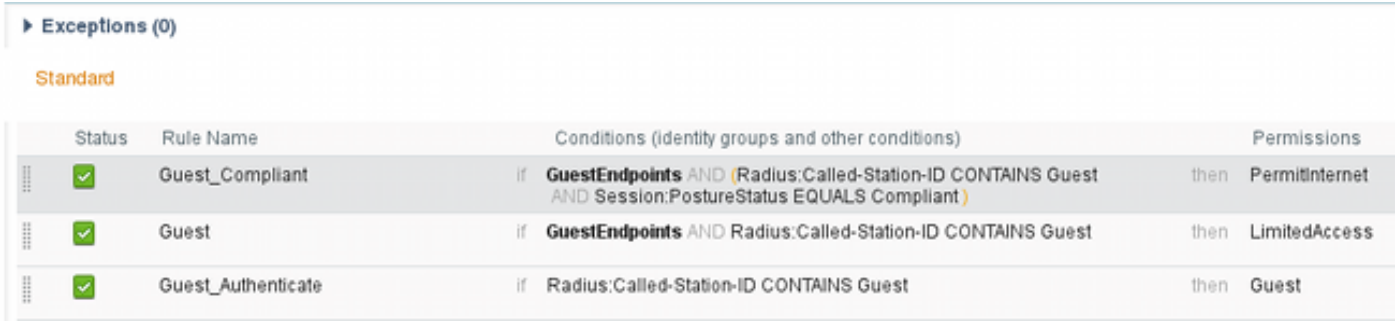


Observe que o dispositivo esteve adicionado já automaticamente (está na lista de dispositivos Manage). Isto é porque os **dispositivos do convidado do registro** foram selecionados **automaticamente**.

Postura

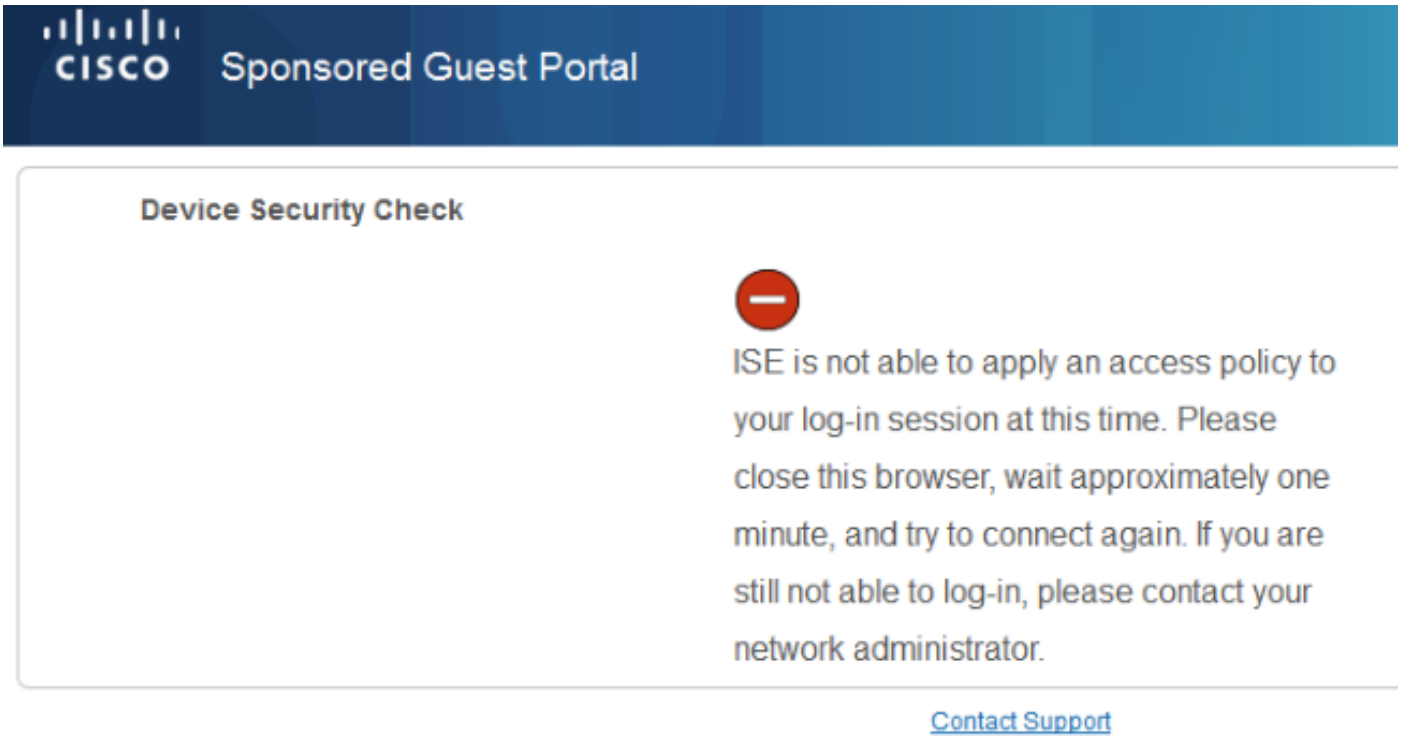
Se a opção da **conformidade do dispositivo do convidado da exigência** é selecionada, a seguir os usuários convidado são fornecida com um agente que execute a postura (agente NAC/Web) depois que entram e aceitam o AUP (e execute opcionalmente o registro do dispositivo). O ISE processa regras do abastecimento do cliente para decidir que agente deve ser fornecida. Então o agente que é executado na estação executa a postura (conforme regras da postura) e envia resultados ao ISE, que envia o CoA reauthenticate para mudar o estado de autorização se necessário.

As regras possíveis da autorização puderam olhar similares a esta:



Os primeiros novos usuários que encontram a regra de Guest_Authenticate para reorientar ao portal do convidado do registro do auto. Depois que os auto-registros do usuário e entram, o CoA muda o estado de autorização e o usuário é fornecido com o acesso limitado para executar a postura e a remediação. Somente depois que o agente NAC é fornecida e a estação é complacente faz o estado de autorização da mudança CoA mais uma vez a fim fornecer o acesso ao Internet.

Os problemas típicos com postura incluem a falta de regras corretas do abastecimento do cliente:



Isto pode igualmente ser confirmado se você examina o arquivo de guest.log (novo na versão 1.3 ISE):

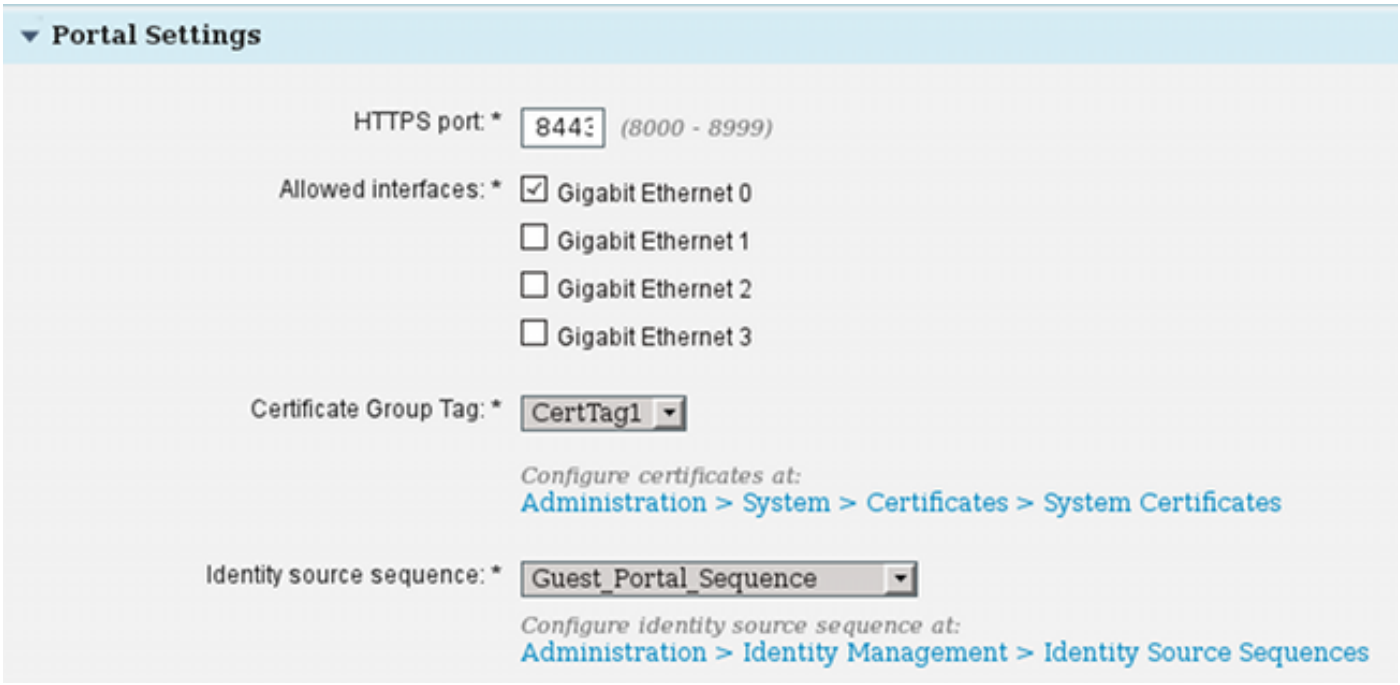
```
2014-08-01 21:35:08,435 ERROR  [http-bio-10.62.97.21-8443-exec-9][] guestaccess.
flowmanager.step.guest.ClientProvStepExecutor -:7AAF75982E0FCD594FE97DE2970D472F::-
CP Response is not successful, status=NO_POLICY
```

BYOD

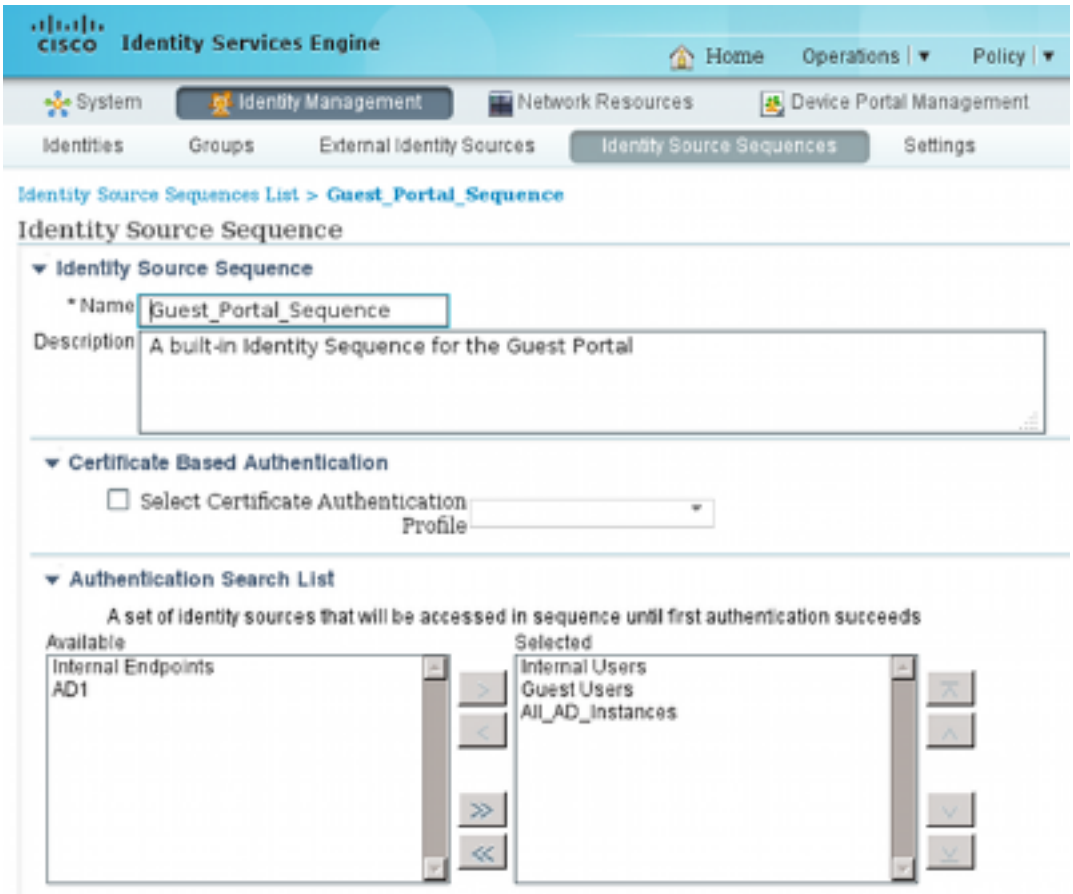
Se os **empregados reservar para usar dispositivos pessoais na opção de rede** são selecionados, a seguir os usuários corporativos que usam este portal podem atravessar BYOD fluem e registram dispositivos pessoais. Para usuários convidado, esse ajuste não muda qualquer coisa.

Que os “empregados que usam o portal como o convidado” significam?

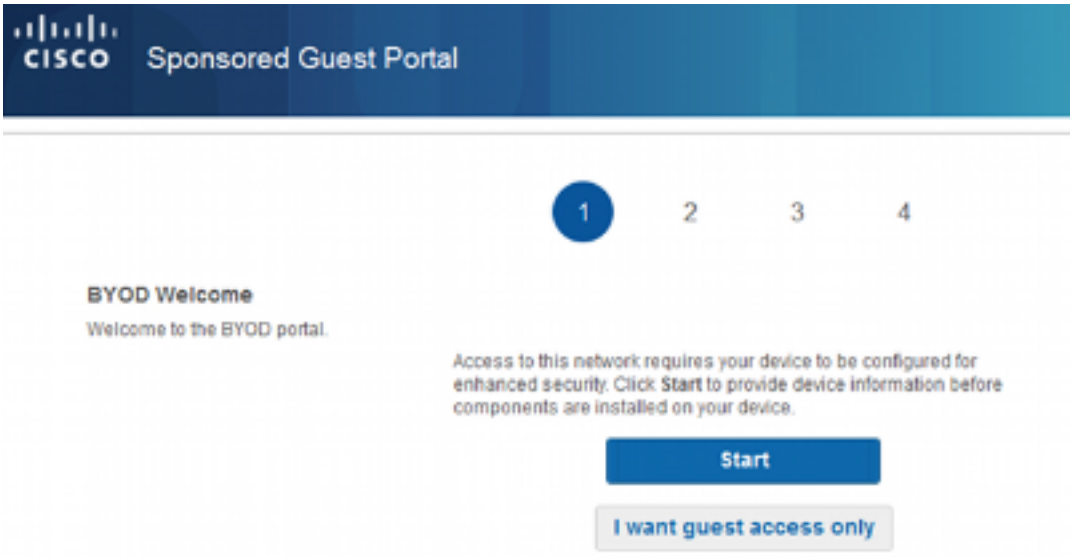
Àrevelia, os portais do convidado são configurados com a loja da identidade de **Guest_Portal_Sequence**:



Esta é a sequência interna da loja que tenta os usuários internos primeiramente (antes dos usuários convidado):



Quando nesta fase no portal do convidado, o usuário fornece as credenciais que são definidas nos usuários internos armazenam e a reorientação BYOD ocorre:



Os usuários corporativos desta maneira podem executar BYOD para dispositivos pessoais.

Quando em vez das credenciais dos usuários internos, as credenciais dos usuários convidado forem fornecidas, fluxo normal são continuadas (nenhum BYOD).

Alteração de VLAN

Esta é uma opção similar à alteração de VLAN configurada para o portal do convidado na versão 1.2 ISE. Permite que você execute activeX ou um Java applet, que provoque o DHCP para se liberar e renovar. Isto é precisado quando o CoA provoca a mudança do VLAN para o valor-limite. Quando o MAB é usado, o valor-limite não está ciente de uma mudança do VLAN. Uma solução possível é mudar o VLAN (a liberação DHCP/renova) com o agente NAC. Uma outra opção é pedir um endereço IP de Um ou Mais Servidores Cisco ICM NT novo através do applet retornado no página da web. Um atraso entre a liberação/CoA/renova pode ser configurado. Esta opção não é apoiada para dispositivos móveis.

Informações Relacionadas

- Serviços da postura no manual de configuração de Cisco ISE
- Sem fio BYOD com Identity Services Engine
- Apoio ISE SCEP para o exemplo de configuração BYOD
- Guia de administradores de Cisco ISE 1.3
- Autenticação da Web central no exemplo de configuração WLC e ISE
- Autenticação da Web central com FlexConnect AP em um WLC com exemplo de configuração ISE
- Suporte Técnico e Documentação - Cisco Systems