ISE版本1.3 Self已注册访客门户配置示例

目录

简介

思科身份服务引擎(ISE)版本1.3有呼叫Self注册的访客门户的访客门户新类型，允许来宾用户赛弗寄存器，当他们获得访问到网络资源时。此门户允许您配置和定制多个功能。本文描述如何配置和排除故障此功能。

先决条件

要求

思科建议您有与ISE这些主题配置和基础知识的体验：

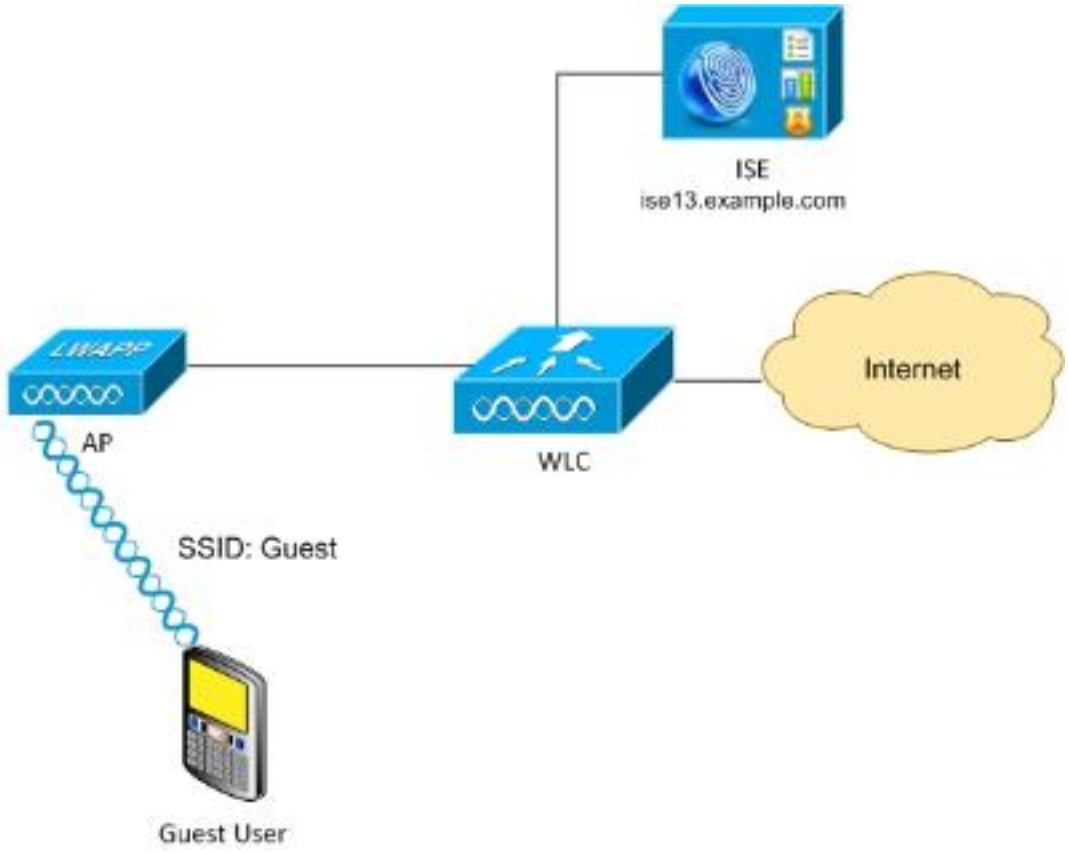
- ISE部署和访客流
- 无线局域网控制器(WLC)的配置

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Microsoft Windows 7
- Cisco WLC版本7.6和以上
- ISE软件，版本3.1和以上

拓扑和流



当他们进行赛弗注册时，此方案展示多个选项可用为来宾用户。

这是一般流：

步骤1.服务集标识(SSID)的来宾用户关联：访客。这是与过滤与验证的ISE的MAC的一个开放式网络。此验证匹配在ISE的第二个授权规则和授权配置文件重定向到访客赛弗注册的门户。ISE返回与两Cisco AV对的一RADIUS Access-Accept ：

- 流量应该重定向的url-redirect-acl (和在WLC定义的本地访问控制表(ACL)名称)
- url重新定向(在哪里重定向该数据流到ISE)

第二步：来宾用户重定向对ISE。而不是请提供凭证为了登陆，用户点击"Donot have a account"。用户重定向对该帐户可以创建的页。一个可选秘密注册代码也许启用为了限制赛弗注册权限人民谁认识该加密值。在帐户创建后，用户是提供的与那些凭证的凭证(用户名和密码)和登录。

步骤3. ISE发送RADIUS授权(CoA)再次验证崔凡吉莱对WLC。当发送与授权属性时的RADIUS

Access-Request WLC重新鉴别用户。ISE回应在WLC定义的本地Access-Accept和Airespace ACL，对仅互联网的提供访问(来宾用户的最终访问取决于授权策略)。

注意为可扩展的认证协议(EAP)会话， ISE必须发送CoA终止为了触发再验证，因为EAP会话是在请求方和ISE之间。但是对于MAB (过滤的MAC)， CoA再次验证是足够;没有需要DE associate/de验证无线客户端。

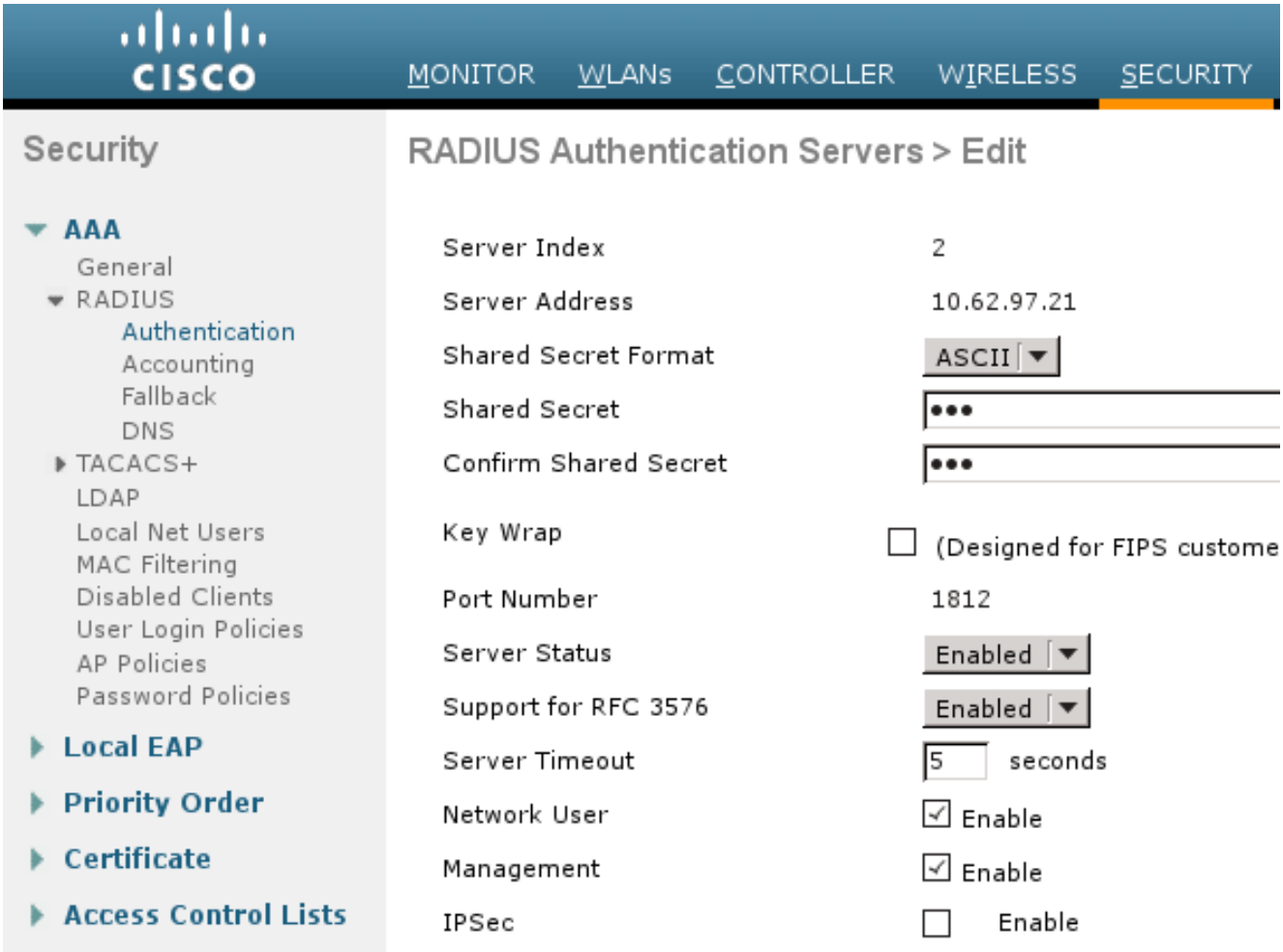
第四步：来宾用户希望对网络的访问。

多个其它功能类似状态和带来您自己的设备(BYOD)可以启用(讨论以后)。

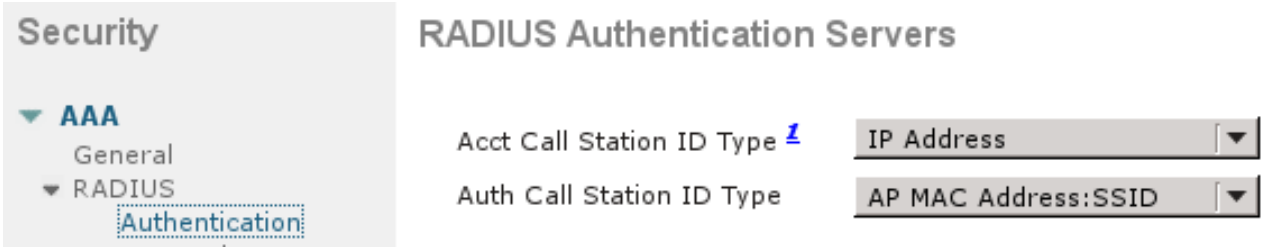
配置

WLC

1. 添加验证和核算的新的RADIUS服务器。导航对**安全>AAA > Radius>验证**为了启用RADIUS CoA (RFC 3576)。



有核算的一相似的配置。也建议配置WLC发送在被叫站ID属性的SSID，允许ISE配置根据SSID的灵活规则：

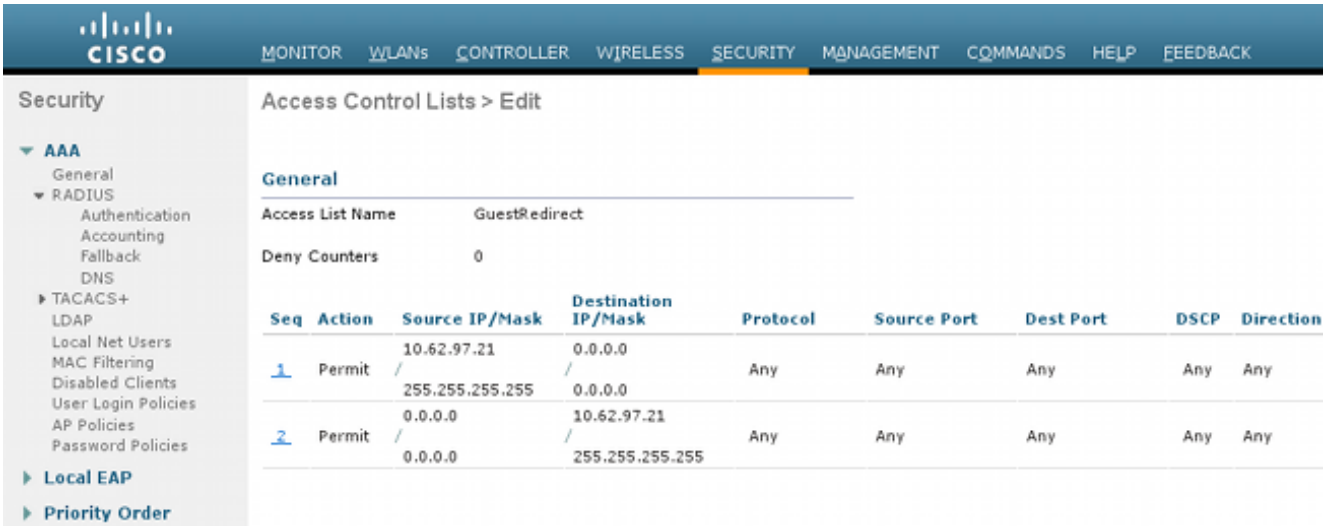


2. 在WLAN选项卡下，请创建无线局域网(WLAN)访客并且配置正确接口。设置Layer2安全对**无**与MAC过滤。在安全/验证、授权和统计(AAA)服务器中，请选择验证和核算的ISE IP地址。在高级选项卡。，请启用**AAA覆盖**并且设置网络准入控制(NAC)状态为RADIUS NAC (CoA支持)。

3. 导航到**安全>访问控制列出>访问控制列表**并且建立两访问列表：

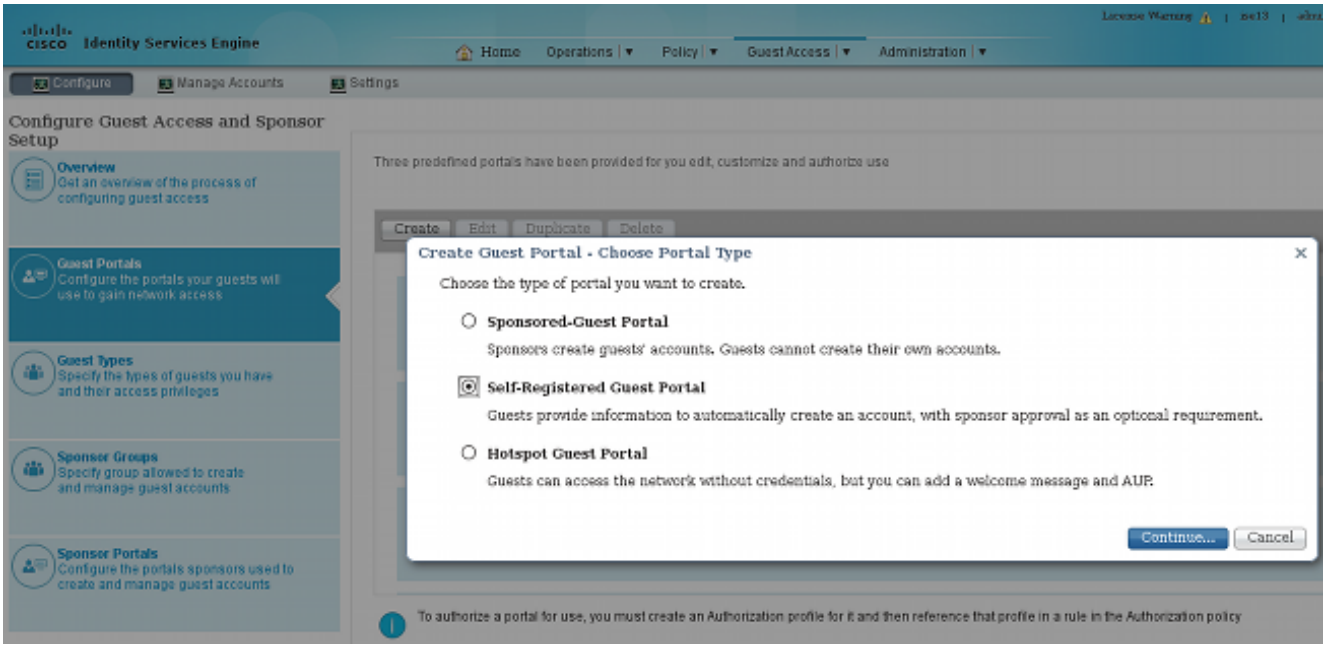
   GuestRedirect，允许流量不应该重定向并且重定向其他流量互联网，为公司网络拒绝并且为其他允许

   这是GuestRedirect ACL的(需要一示例从重定向排除到/从ISE的流量)：



ISE

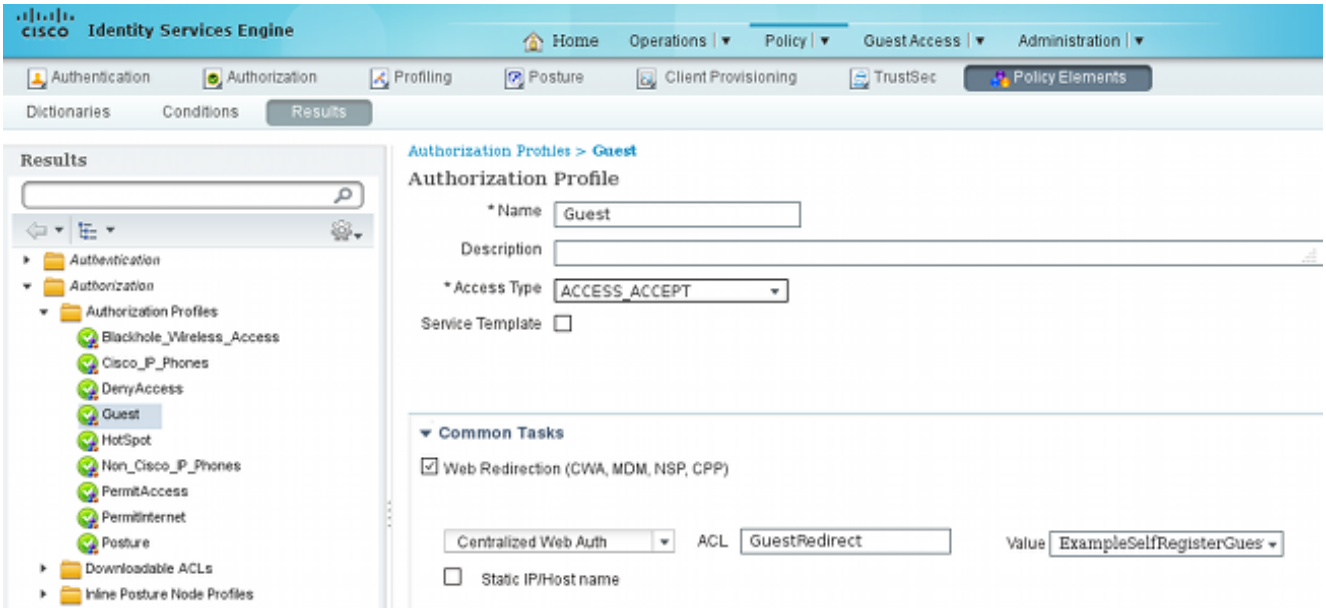
1. 导航对**访客访问>配置>访客门户**，并且创建一个新的门户类型，赛弗注册访客门户：



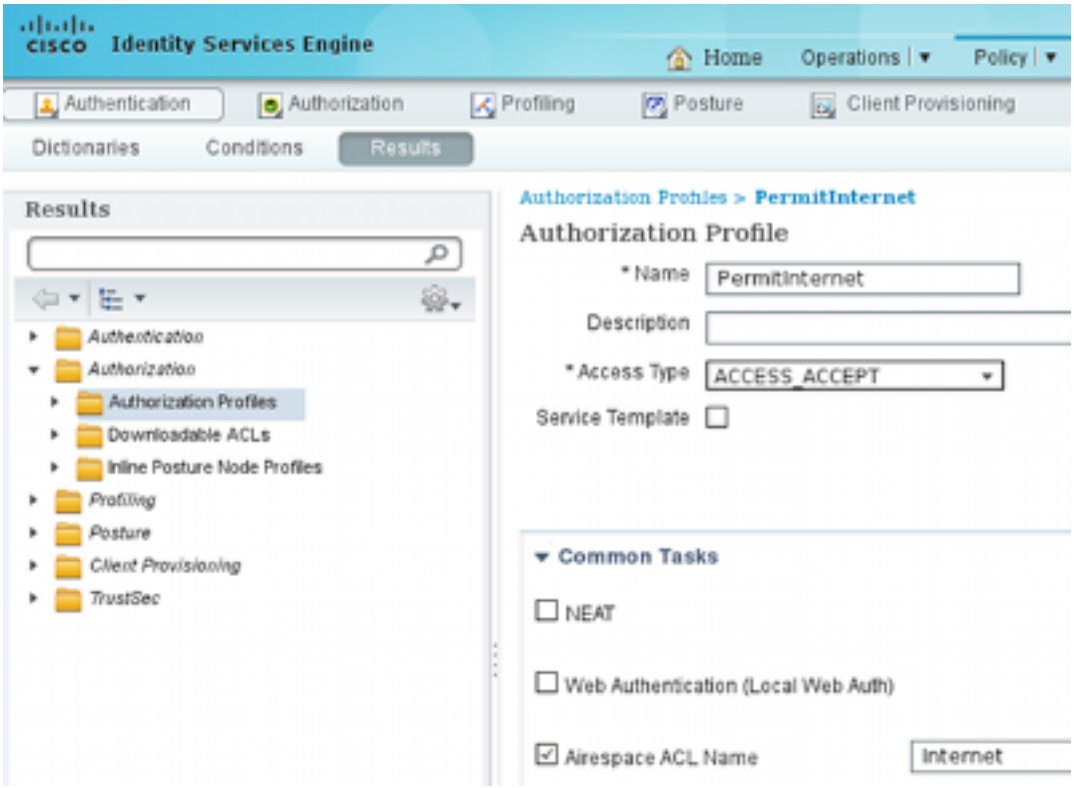
2. 选择将被参考授权配置文件的门户名称。设所有其他设置默认。在入口页面自定义下，被提交的所有页可以定制。

3. 配置授权配置文件：

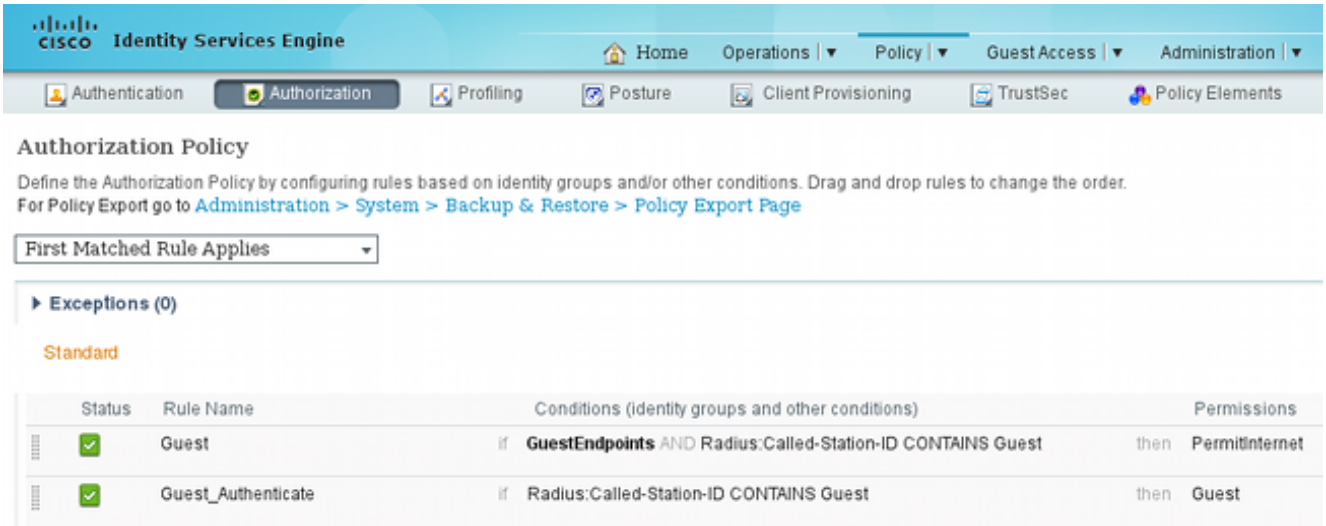
   访客(与对访客门户名称和ACL GuestRedirect)的重定向



   PermitInternet (用Airespace ACL等于互联网)



4. 为了验证授权规则，请导航对**策略>授权**。默认情况下在ISE版本1.3失败的MAC验证旁路(MAB)访问(没找到的MAC地址)验证的继续(没拒绝)。因为没有需要更改任何东西在默认验证规则，这为访客门户是非常有用的。



联合对访客SSID的新用户不作为任何标识组的部分。这就是为什么他们匹配第二个规则，使用访客授权配置文件重定向他们到正确访客门户。

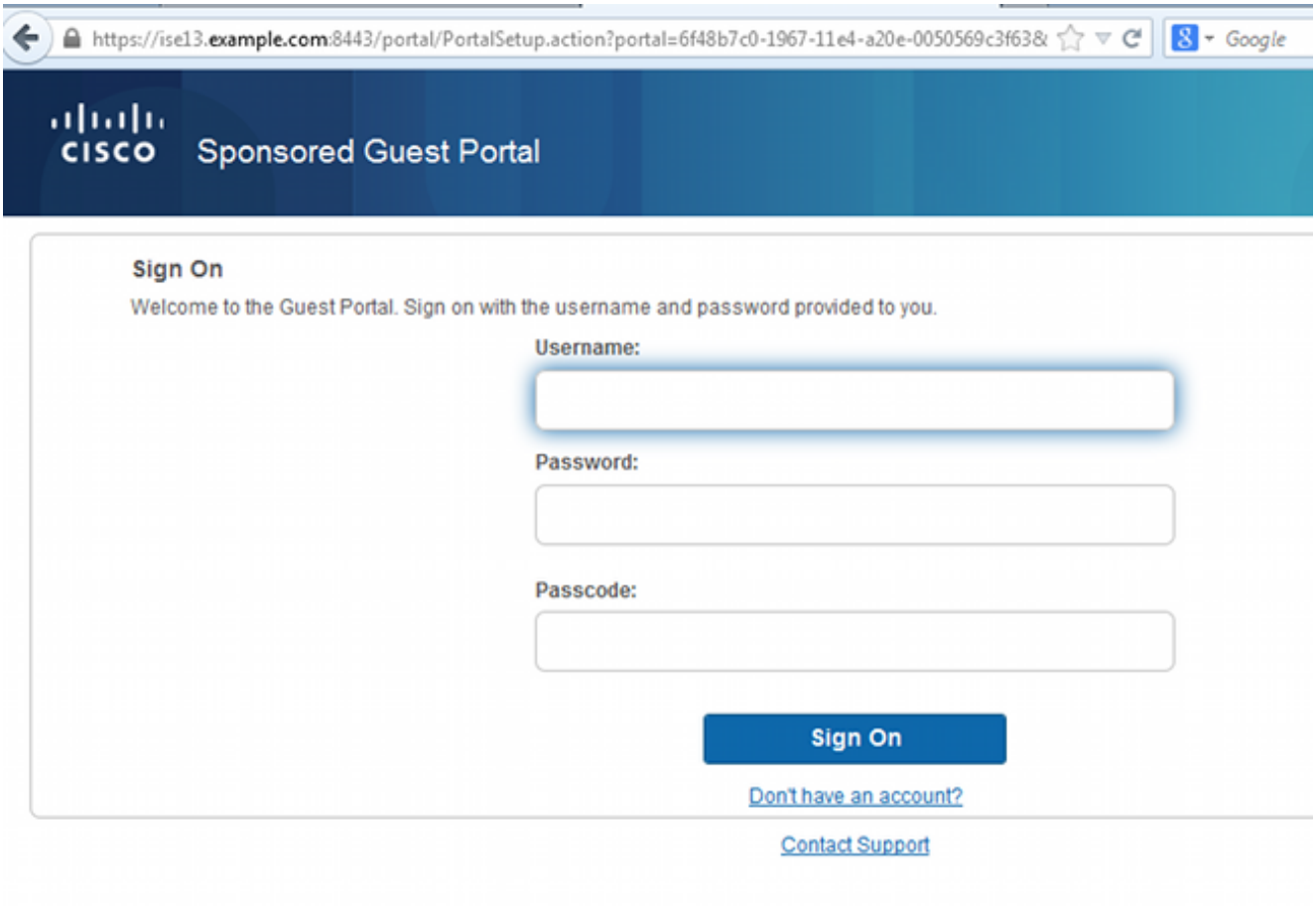
在用户创建帐户并且顺利后地登录， ISE发送RADIUS CoA，并且WLC执行再验证。这时，第一个规则与在WLC应用的授权配置文件PermitInternet一起匹配并且返回ACL名称。

5. 添加WLC作为网络接入设备从**Administration >网络资源>网络设备**。

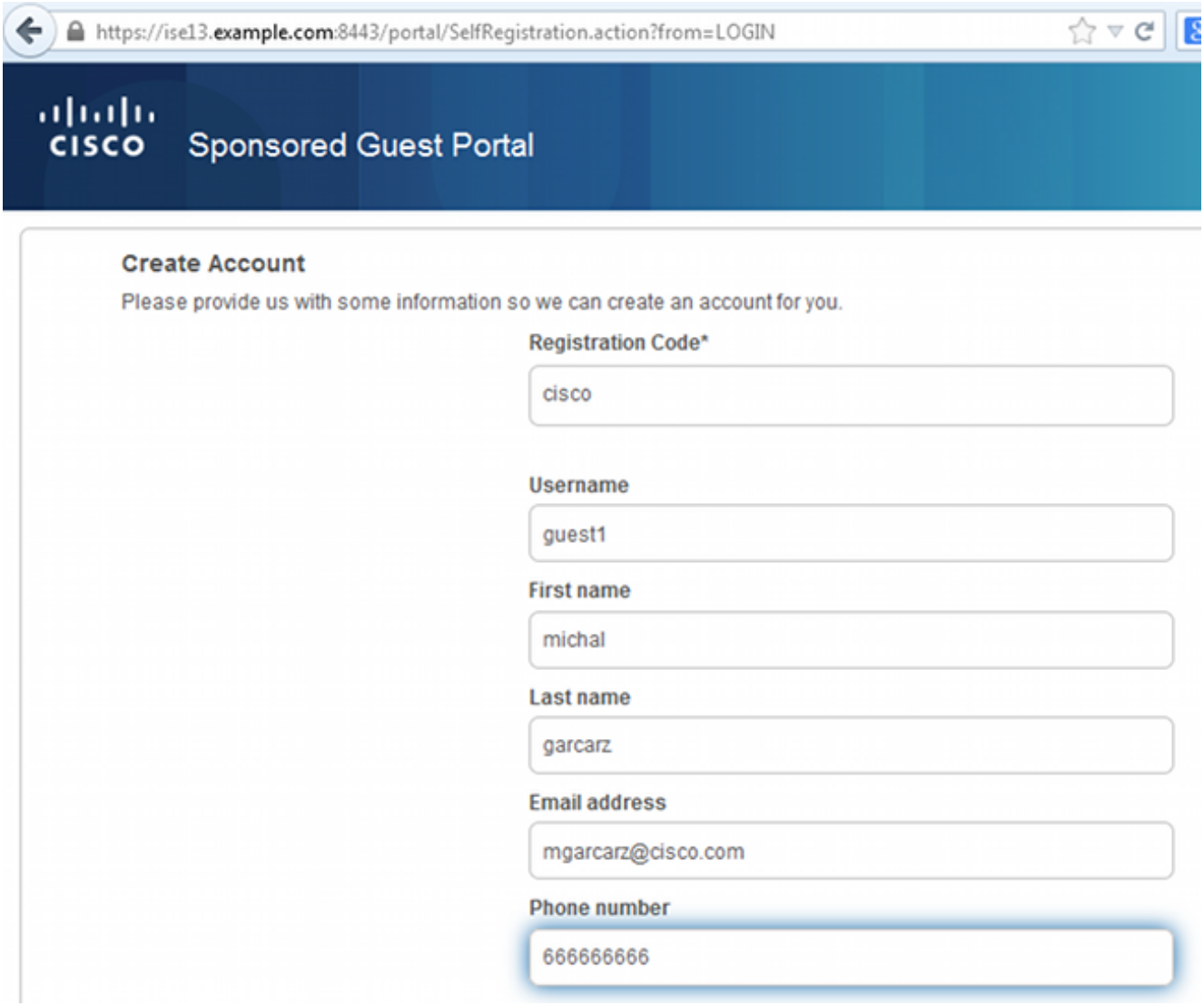
验证

使用本部分可确认配置能否正常运行。

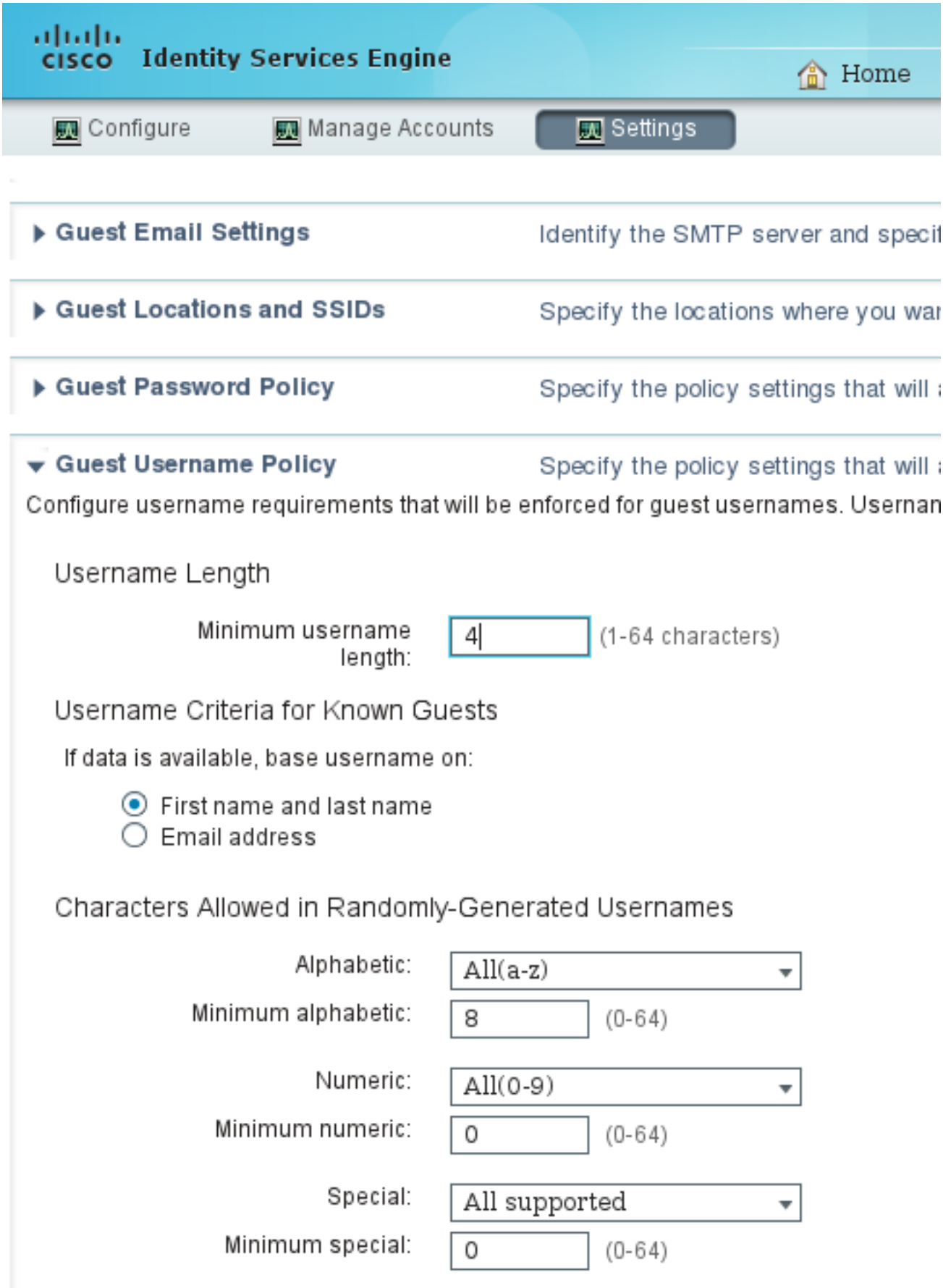
1. 在您与访客SSID产生关联并且键入URL后，然后您重定向对登录页：



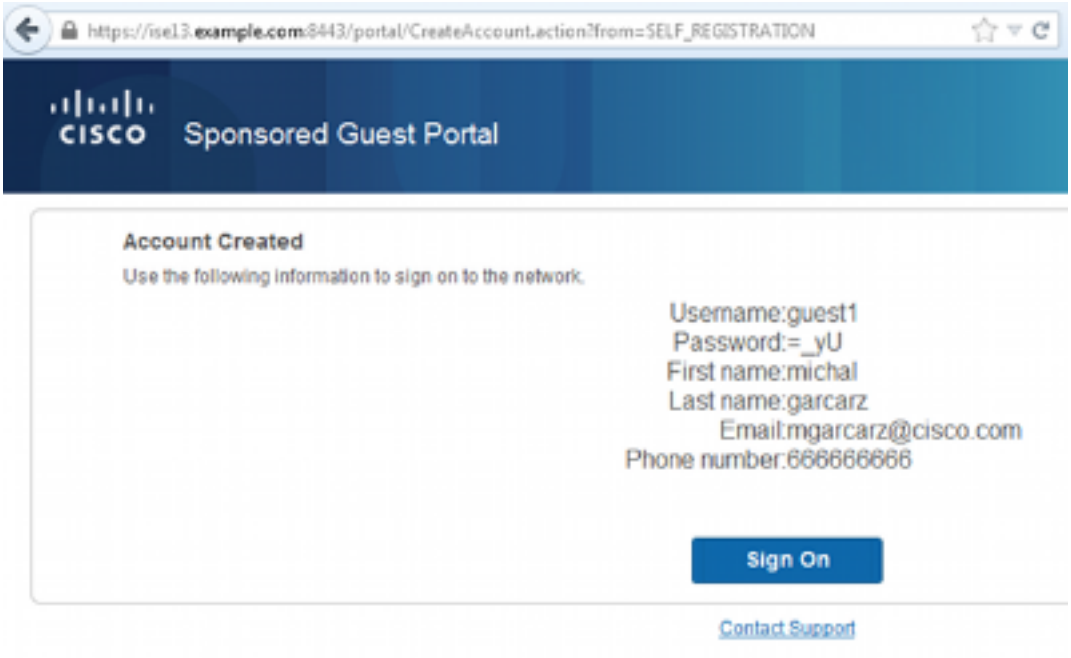
2. 因为您没有任何凭证，是否必须选择没**有帐户？**选项。允许帐户创建显示的新页面。如果注册代码选项启用在访客Portal配置下，该加密值要求(这保证有正确权限的只有人们允许赛弗寄存器)。



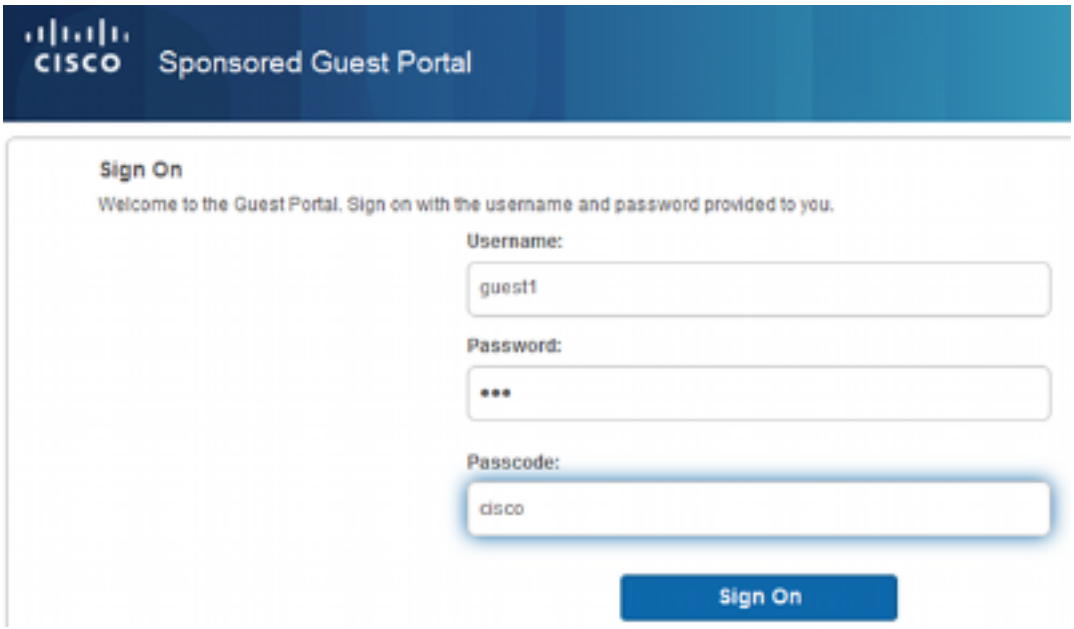
3. 如果有与密码或用户策略的任何问题，请导航对**访客访问>设置>访客密码策略或者访客访问>设置>访客用户名策略**为了更改设置。示例如下：



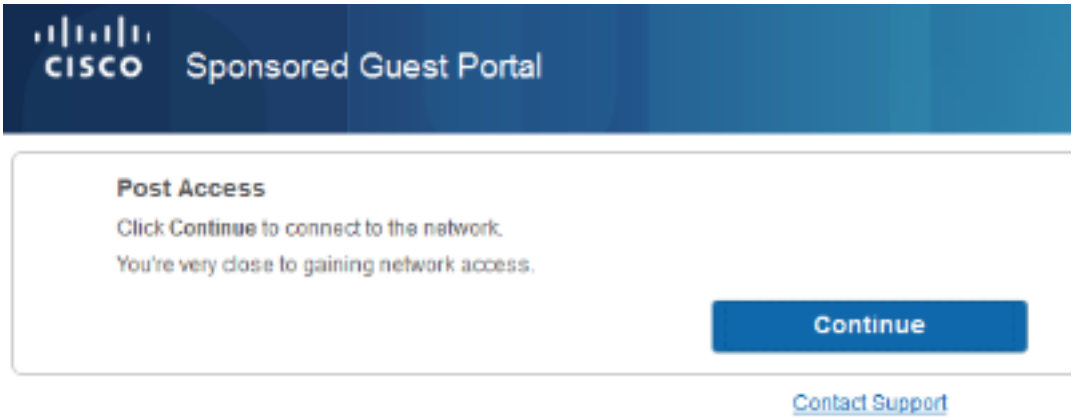
4. 在成功的帐户创建以后，您提交与凭证(根据访客密码策略生成的密码) ：



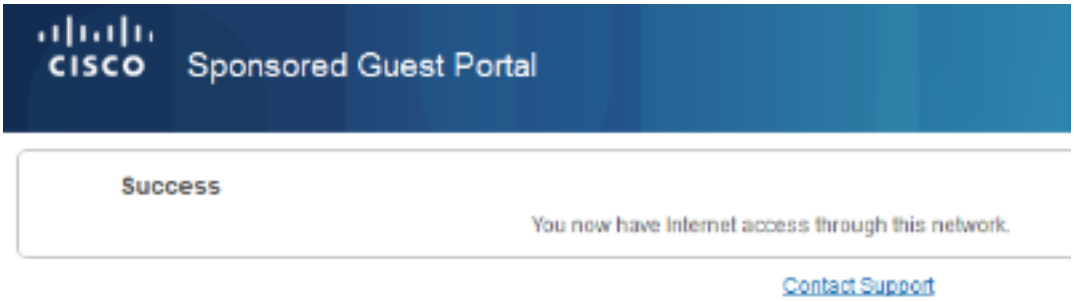
5. 点击**符号**并且提供凭证若被设定(另外的访问密码也许要求在访客门户下;这是允许只有那些人认识密码登陆)的另一安全机制。



6. 当成功，也许提交可选Acceptable Use Policy (AUP) (若被设定在访客门户下)。波斯特访问页(也可配置下面访客门户)也许也显示。



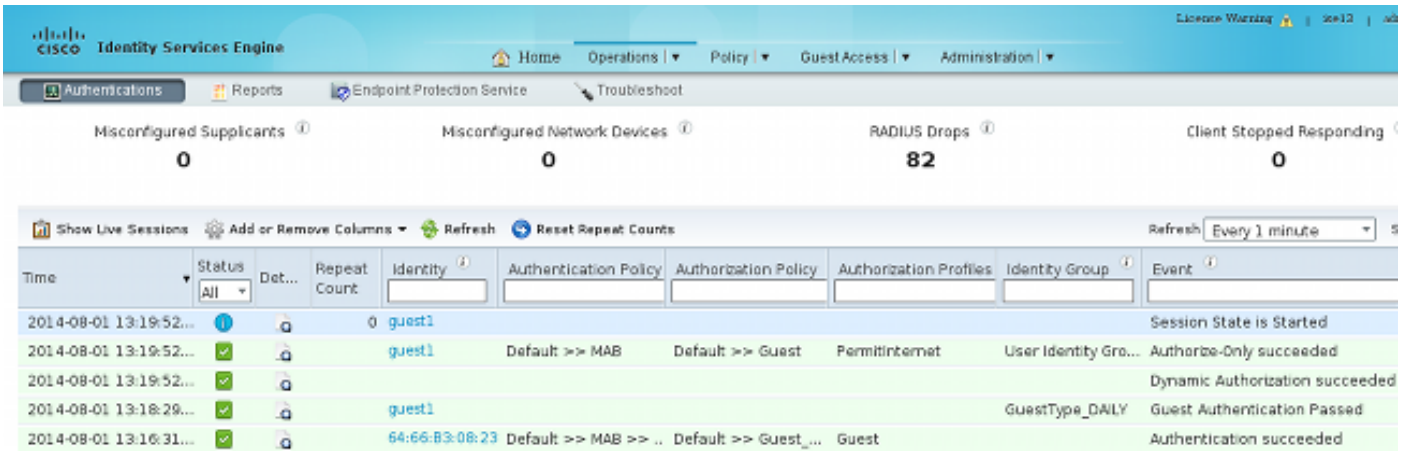
最后一页确认访问授权：



故障排除

本部分提供了可用于对配置进行故障排除的信息。

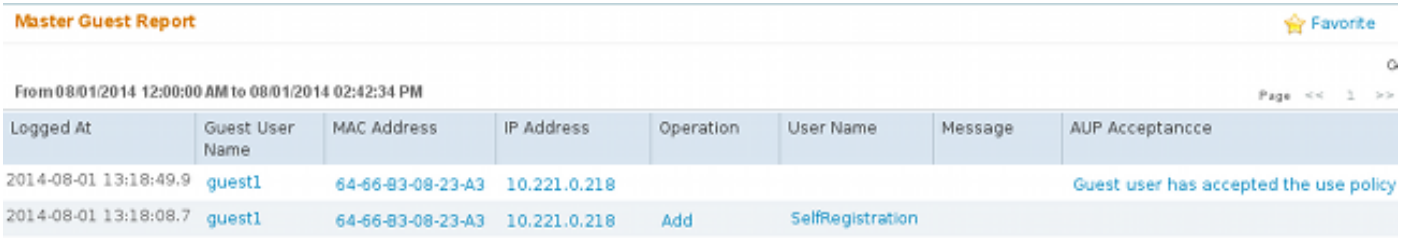
在此阶段， ISE提交这些日志：



这是流：

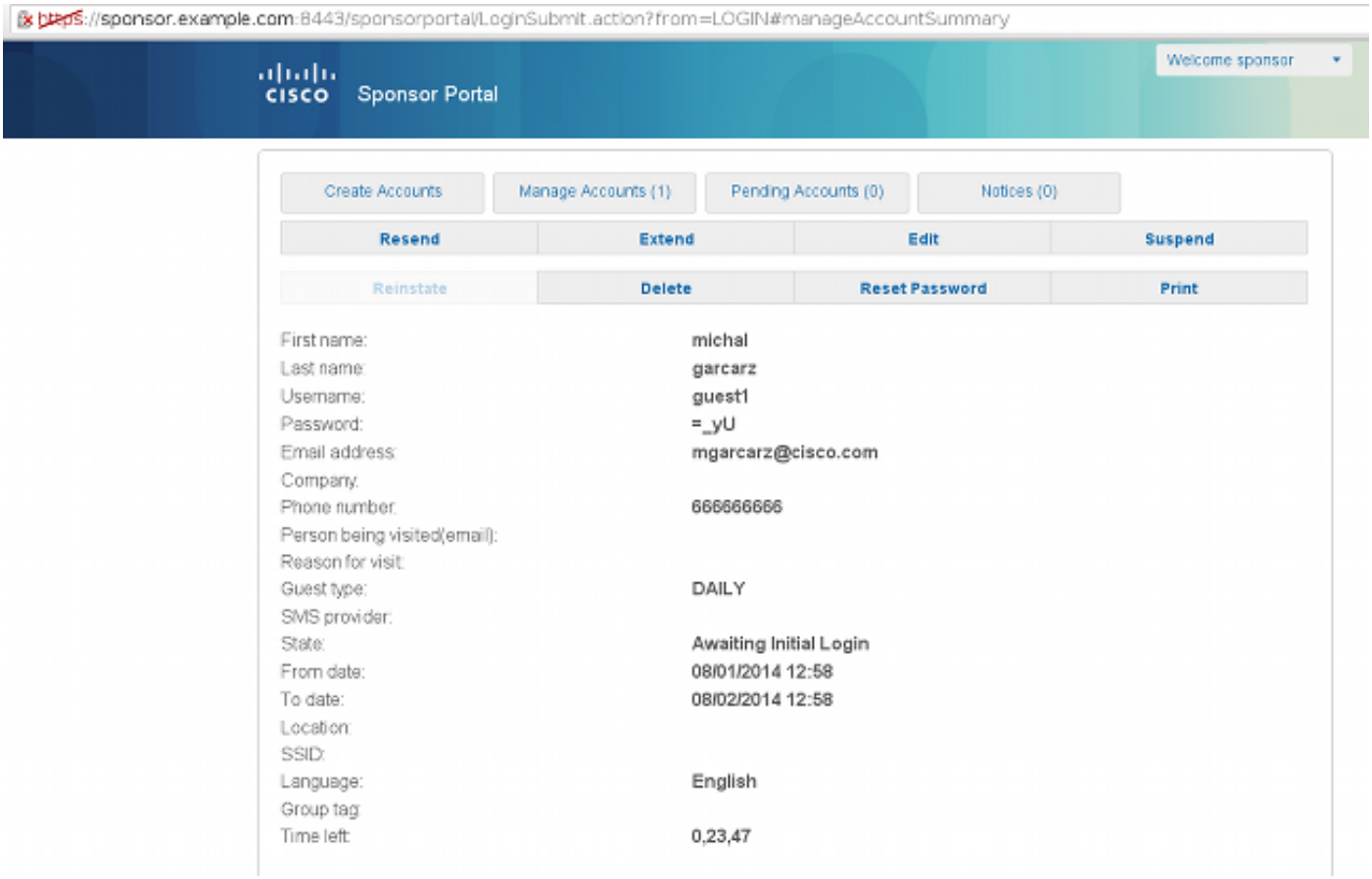
- 来宾用户遇到第二个授权规则(Guest_Authenticate)和重定向给访客(“Auhentication成功”)。
- 访客为赛弗注册重定向。在顺利登录(与新建立的帐户)后， ISE发送CoA再次验证，由WLC (“成功的动态授权确认”)。
- WLC执行再验证与授权属性，并且ACL名称返回(“成功的授权”)。提供访客正确网络访问。

报告(**操作>报告> ISE报告> guest报告访客访问报告>的主控**)也确认那：



赞助商用户(有正确权限)能验证来宾用户的当前状态。

此示例确认帐户创建，但是用户从未登陆(“等候首次登录”) ：



可选配置

对于此流每个阶段，不同的选项可以配置。所有此每个**访客访问的**访客门户配置**>配置>访客门户>** PortalName > Edit **>门户行为和流设置**。更加重要的设置包括：

赛弗注册设置

- 访客类型-多久描述帐户是活跃的，密码终止选项、登录小时和选项(这是时间配置文件和访客角色混合物从ISE版本1.2)
- 注册代码-如果启用，认识安全代码只有的用户允许赛弗寄存器(必须提供密码，当帐户创建)时
- AUP -在赛弗注册期间，接受使用策略
- 赞助商的需求能审批/激活访客帐户

洛金访客设置

- 接入代码-如果启用，认识安全代码只有的来宾用户允许登录
- AUP -在赛弗注册期间，接受使用策略
- 密码更改选项

设备已注册设置

- 默认情况下，设备自动地注册

访客设备法规遵从性设置

- 允许在流内的一状态

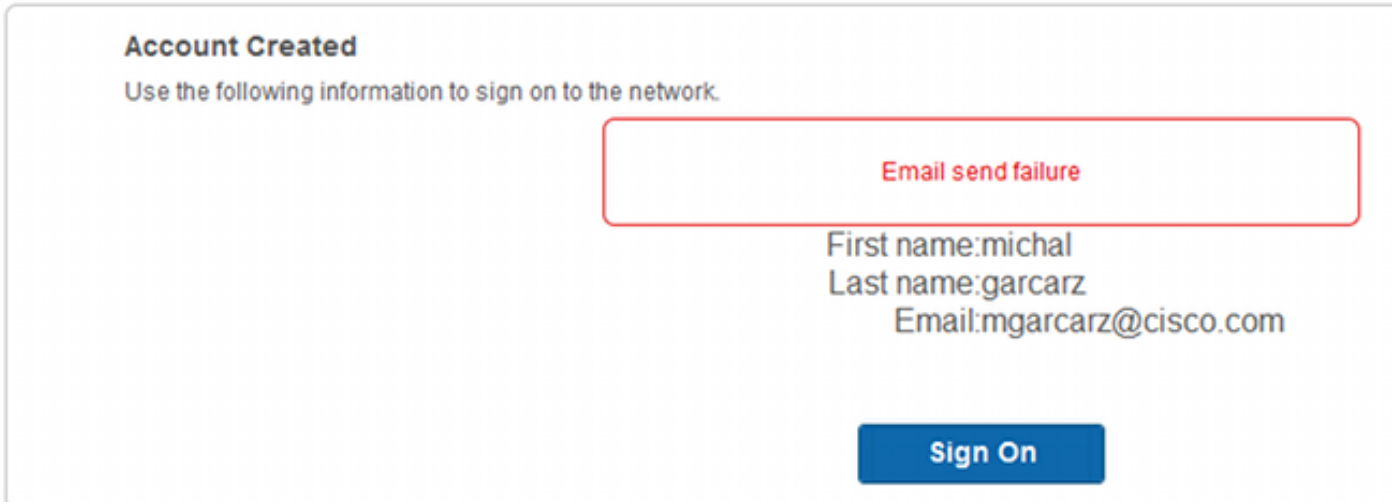
BYOD设置

- 允许使用门户作为访客注册他们的个人设备的集群用户

赞助商审批的帐户

如果**是Require赛弗注册的访客审批的**选项选择，则必须由赞助商审批访客创建的帐户。此功能也许使用电子邮件为了提供通知对赞助商(访客帐户批准) ：

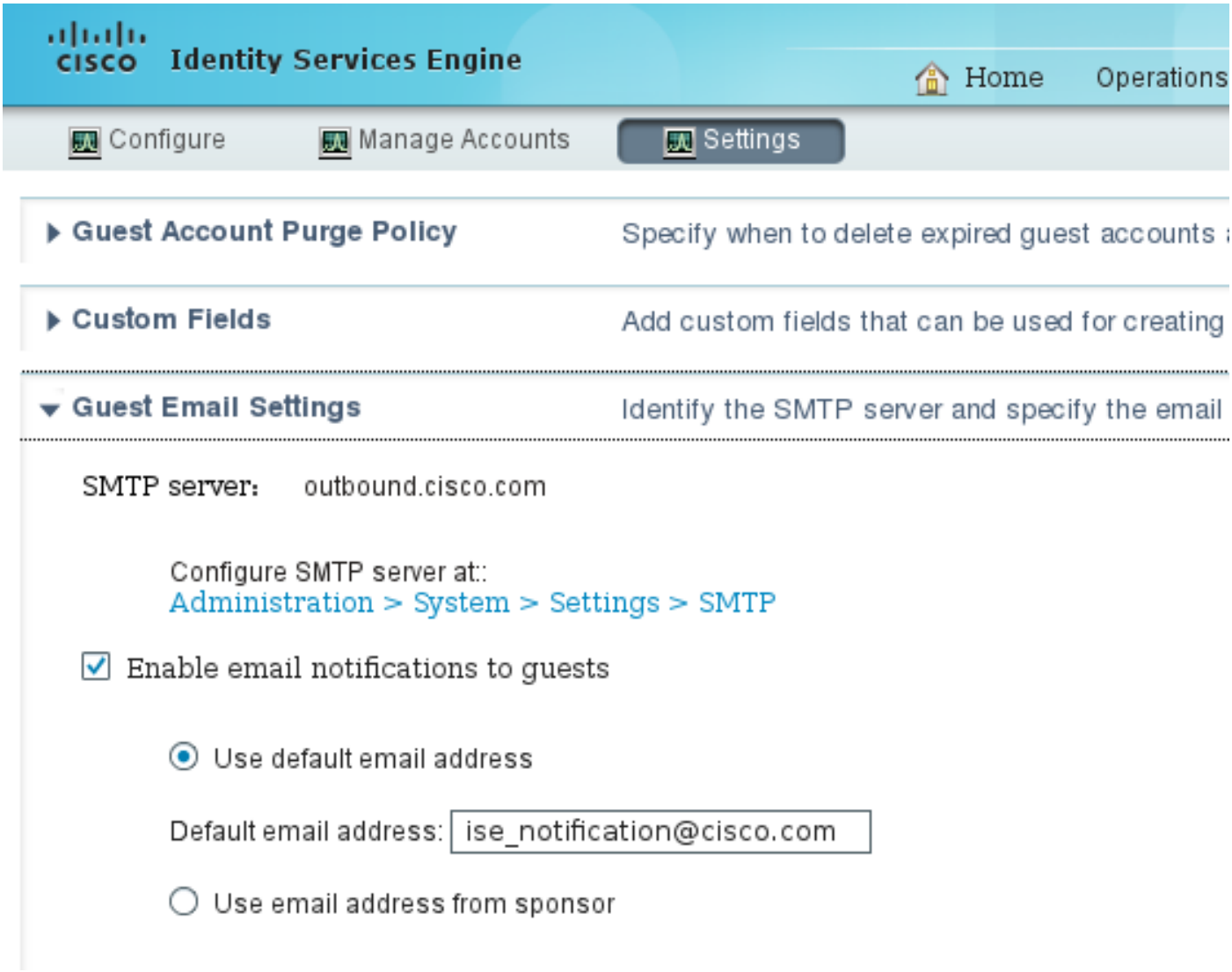
如果简单邮件传输协议(SMTP)服务器或默认从通知从电子邮件没有配置，则帐户不会创建：

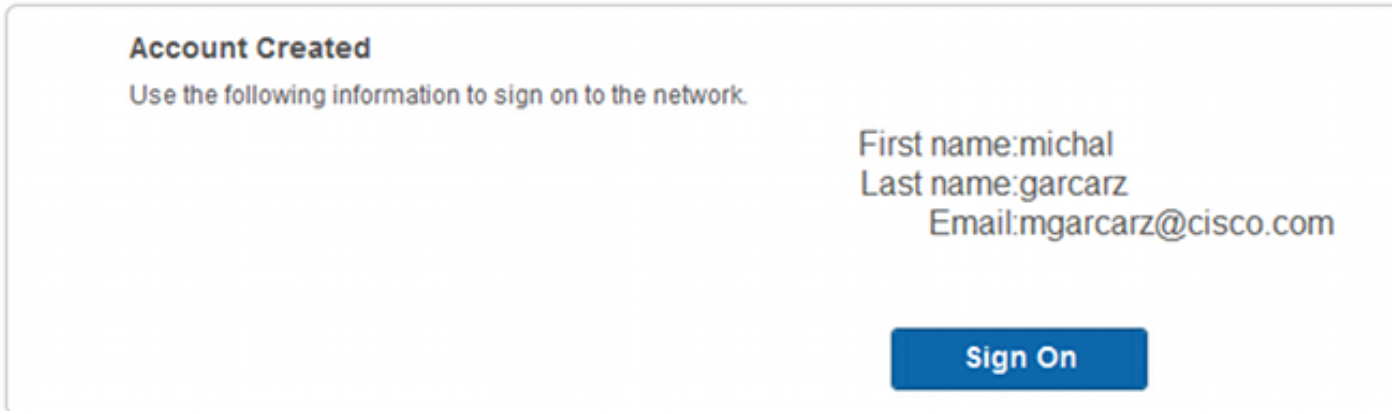


从guest.log的日志确认全局从用于通知的地址未命中：

```
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.
```

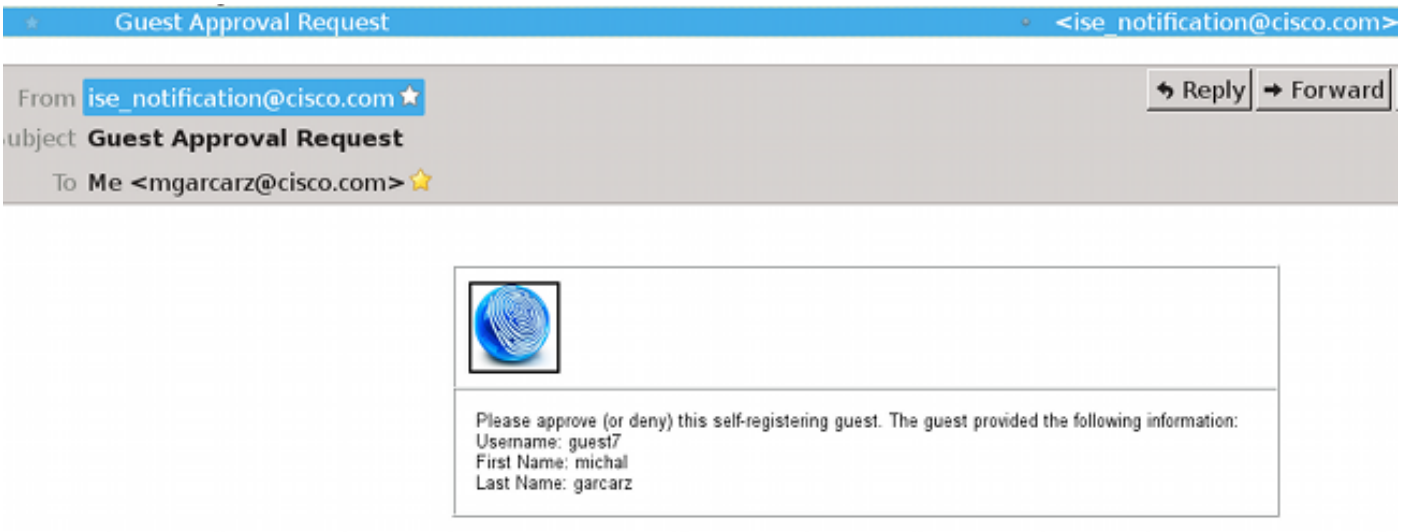
当您有适当的电子邮件配置时，帐户创建：



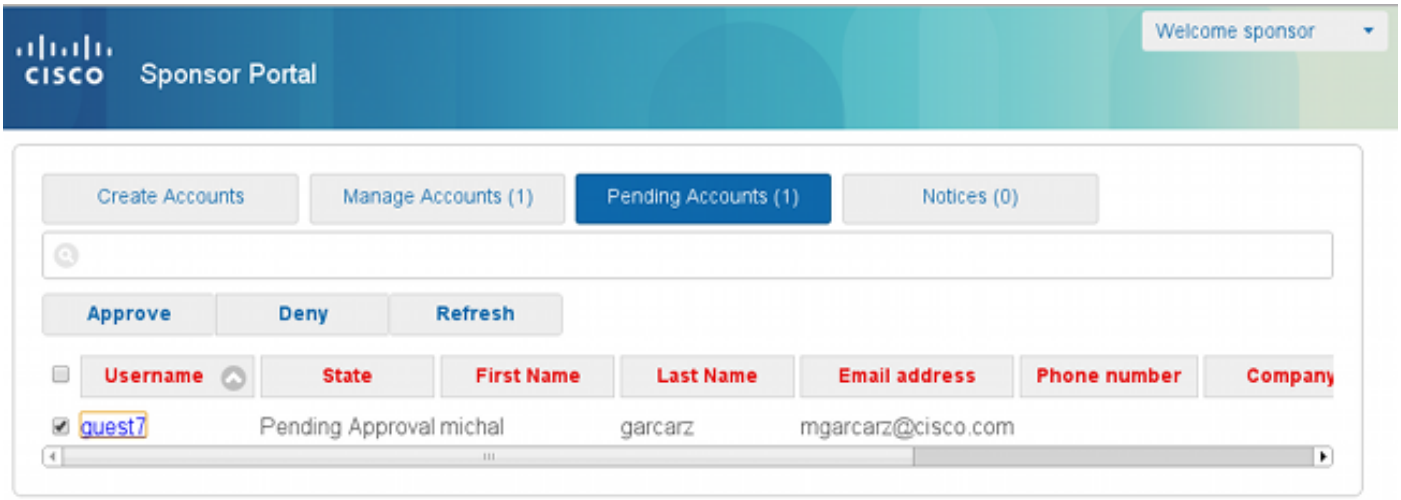


在您使**Require赛弗注册的访客是审批的**选项后，用户名和密码字段从**包括**自动地删除**关于赛弗注册成功页**部分的**此信息**。这就是为什么，当赞助商批准是需要的时，来宾用户的默认情况下凭证在引见信息显示的网页没有显示帐户创建。反而必须由短的信息服务(SMS)或电子邮件传送他们。**在批准的发送证件通知**必须启用**使用**部分(标记email/SMS)，此选项。

通知电子邮件传送给赞助商：



赞助商登录门户的赞助商并且审批帐户：



从这时起，来宾用户允许登录(当凭证接收由电子邮件或SMS)。

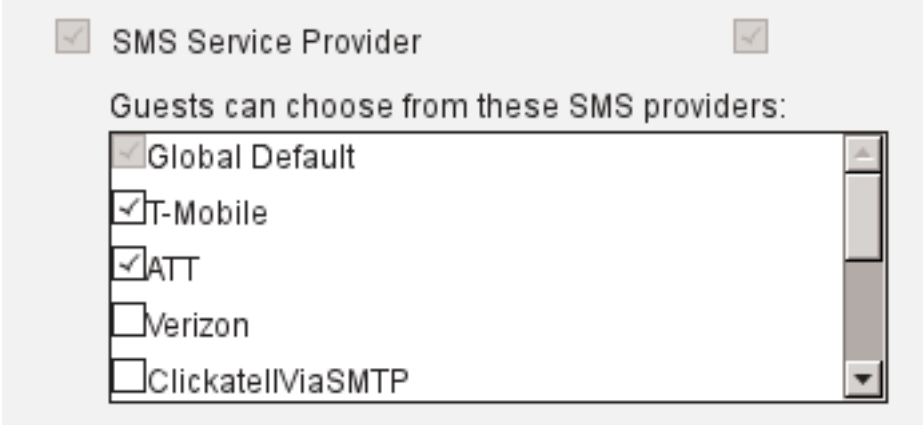
总之，有用于此流的三个电子邮件地址：

- 通知“从”地址。这静态定义或从赞助商帐户被采取并且使用作为从地址两个：通知赞助的(为获得批准)和证件详细信息对访客。这配置在**访客访问下>配置>设置>访客电子邮件设置。**
- “”寻址的通知。这用于为了通知赞助商接收一个帐户为获得批准。这在**访客访问下的**访客门户配置**>配置>访客门户>将审批的门户Name> Require赛弗注册的访客>电子邮件审批请求。**
- “”寻址的访客。这由来宾用户提供在注册时。如果**在批准的发送证件通知使用电子邮件**选择，与证件详细信息(用户名和密码)的电子邮件传送给访客。

通过SMS传送凭证

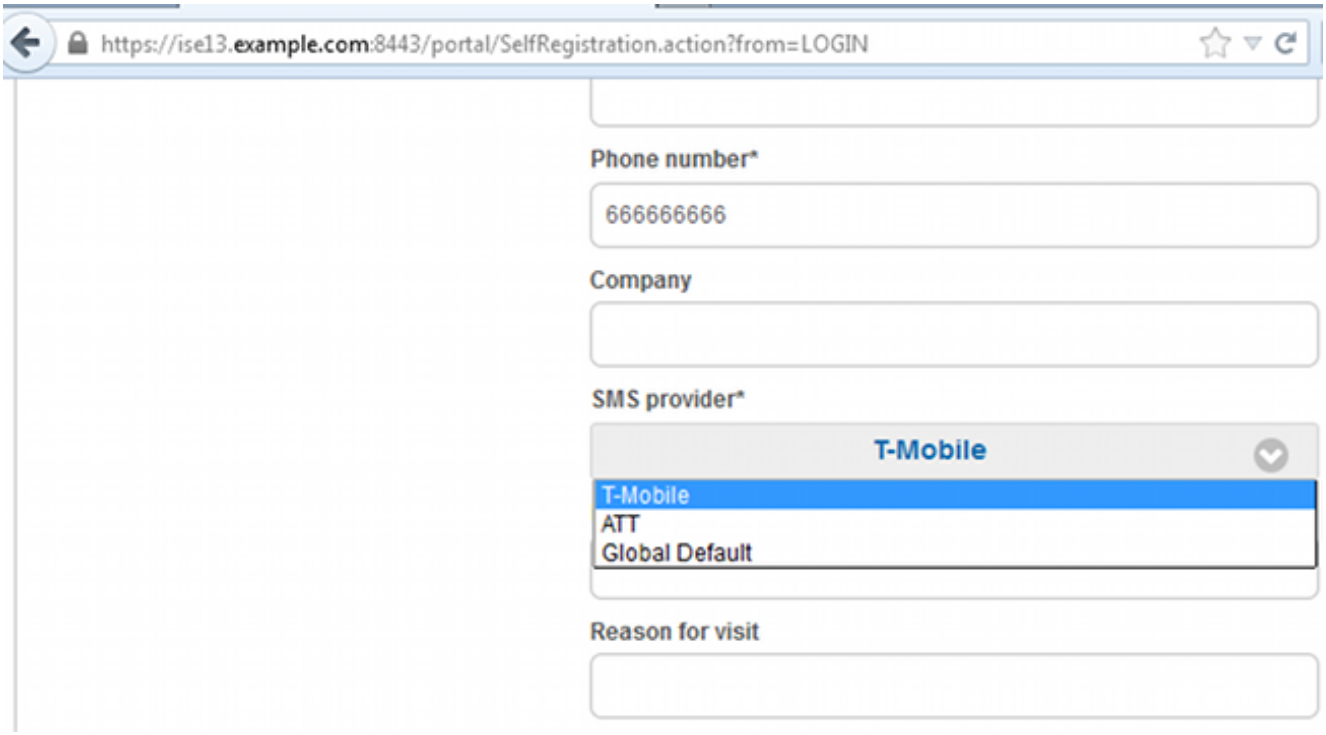
访客凭证可以由SMS也传送。应该配置这些选项：

1. 选择SMS服务提供商：

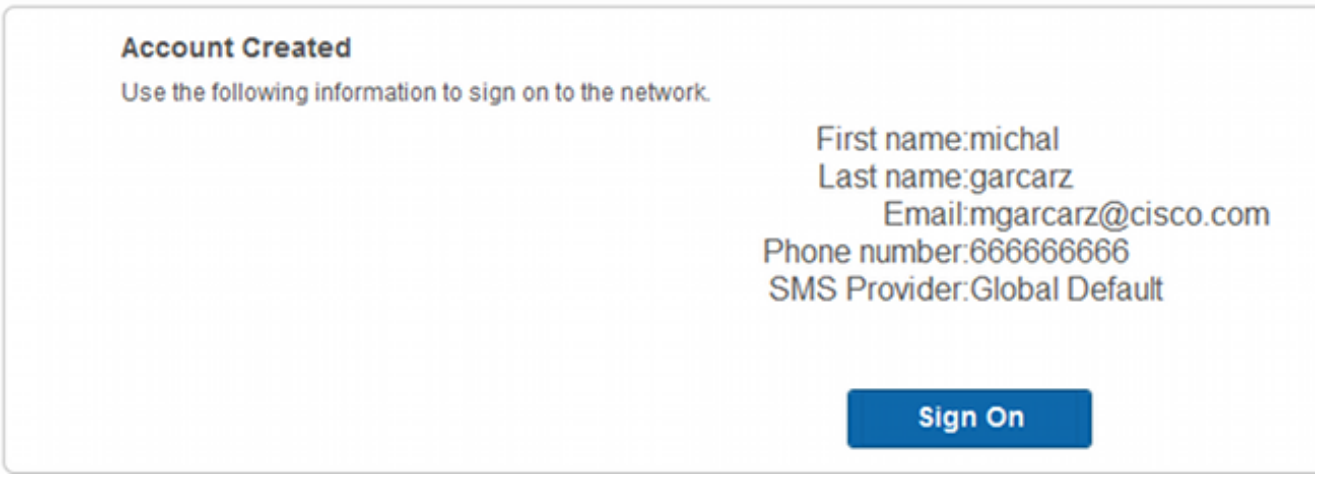


2. 检查**发送证件通知在批准使用：SMS**复选框。

3. 然后，当他创建帐户时，来宾用户询问选择可用的供应商：



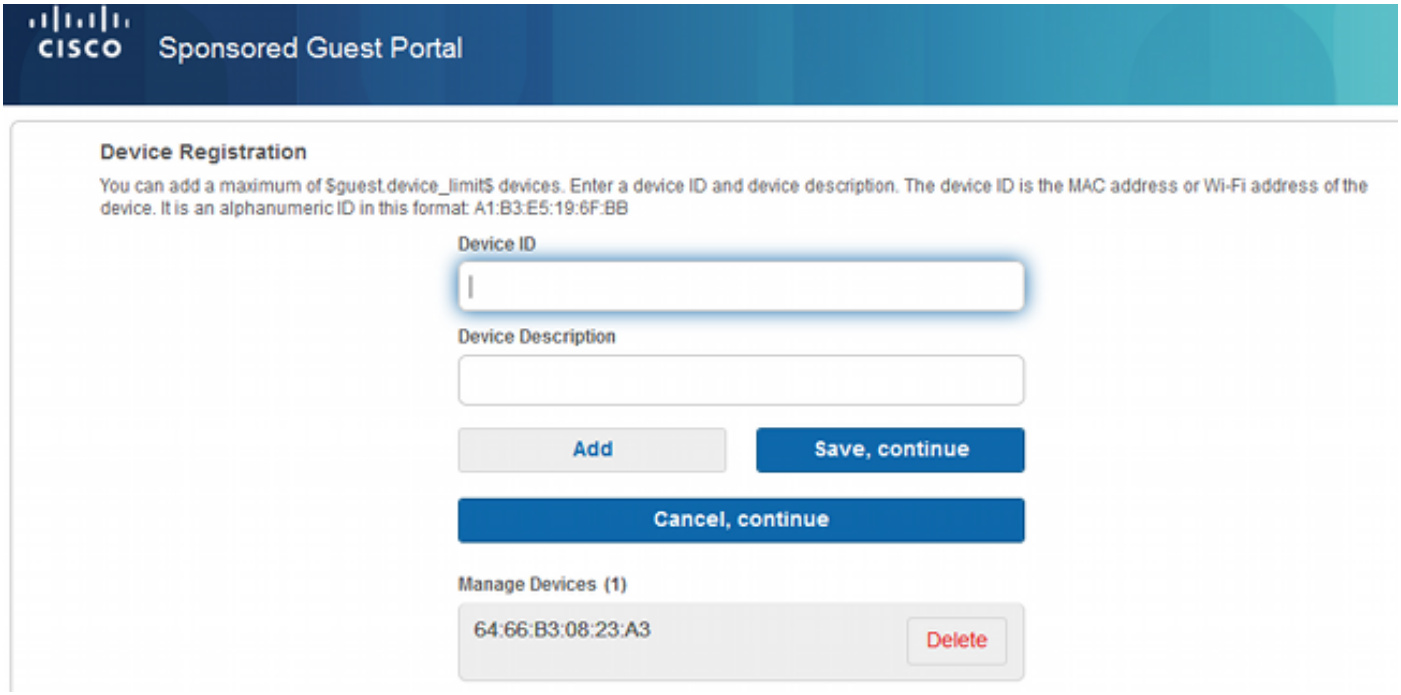
4. SMS用选定的供应商和电话号码传送：



5. 您能配置SMS供应商在**管理>System >设置> SMS网关**下。

设备已注册

如果**注册设备**选项的**允许访客**选择，在来宾用户登陆并且接受AUP后，您能注册设备：

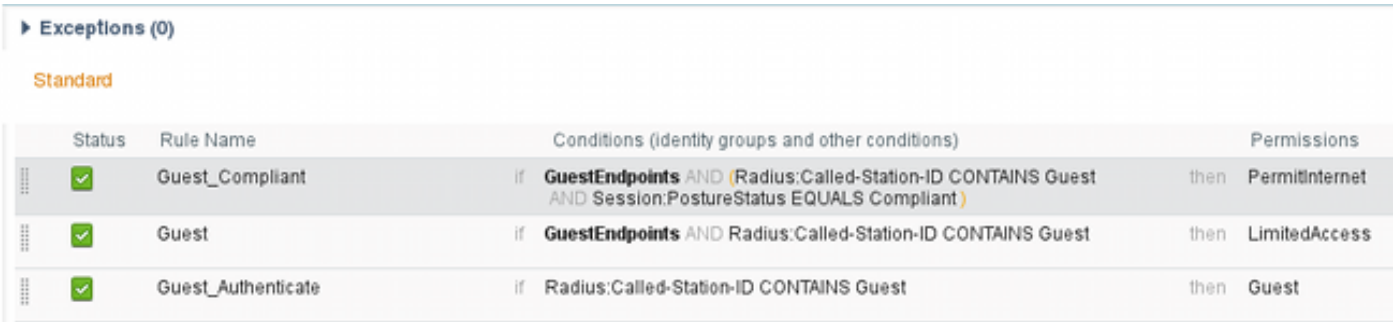


注意设备自动地已经被添加了(在Manage设备清单)。这是因为**寄存器访客设备自动地**选择。

状态

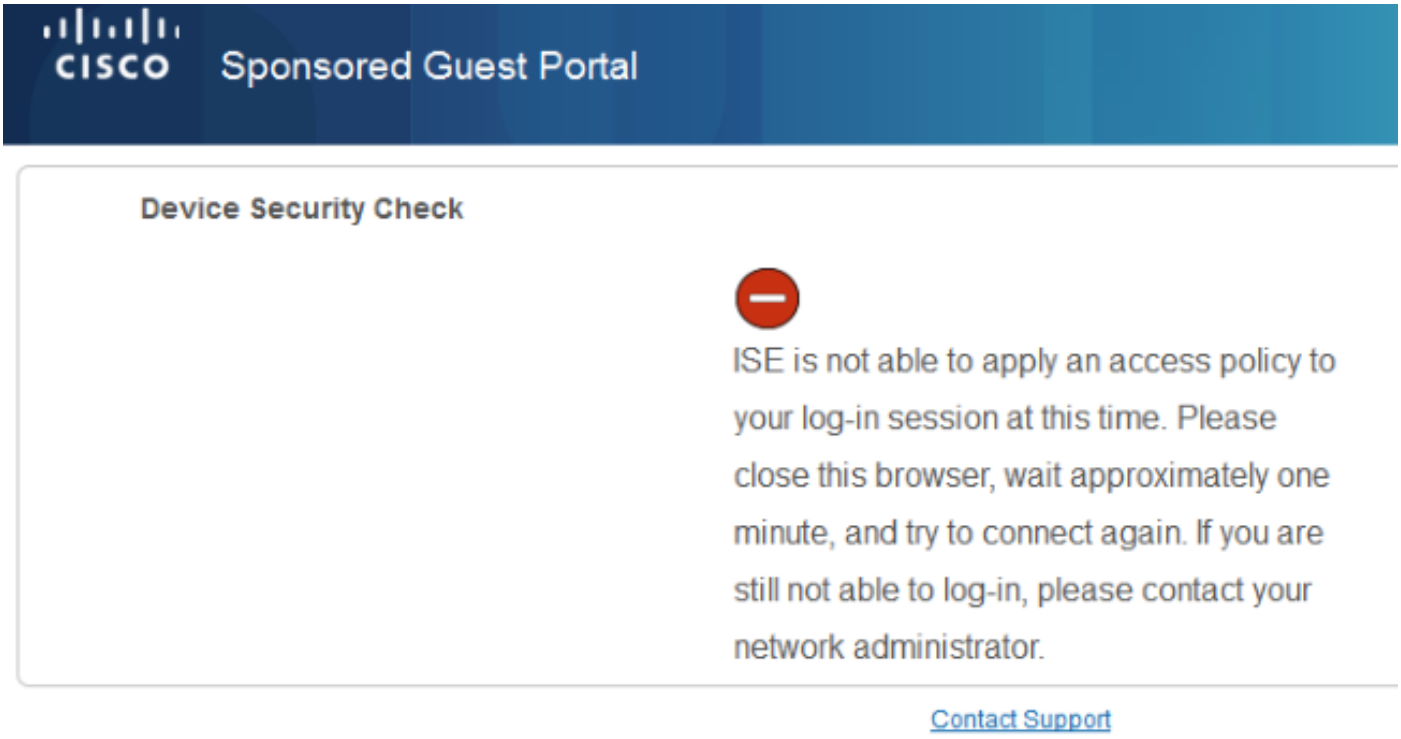
如果**要求访客设备标准**选项选择，则来宾用户配置有执行状态的代理程序(NAC/Web代理程序)，在他们登陆并且接受AUP后(和或者请执行设备已注册)。ISE处理客户端供应规则决定应该设置哪个代理程序。然后在站点运行的代理程序执行状态(根据状态规则)并且发送结果对ISE，若需要发送CoA重新鉴别更改授权状态。

可能的授权规则也许看起来类似于此：



遇到Guest_Authenticate规则重定向到赛弗寄存器访客门户的第一个新用户。在用户赛弗寄存器和登录， CoA更改后授权状态和用户带有有限访问执行状态和修正。在美洲台代理程序设置，并且之后站点是兼容的再次执行CoA更改授权状态为了提供存取对于互联网。

与状态的典型的问题包括缺乏正确客户端供应规则：



这可能也被确认是否检查guest.log文件(新建在ISE版本1.3) ：

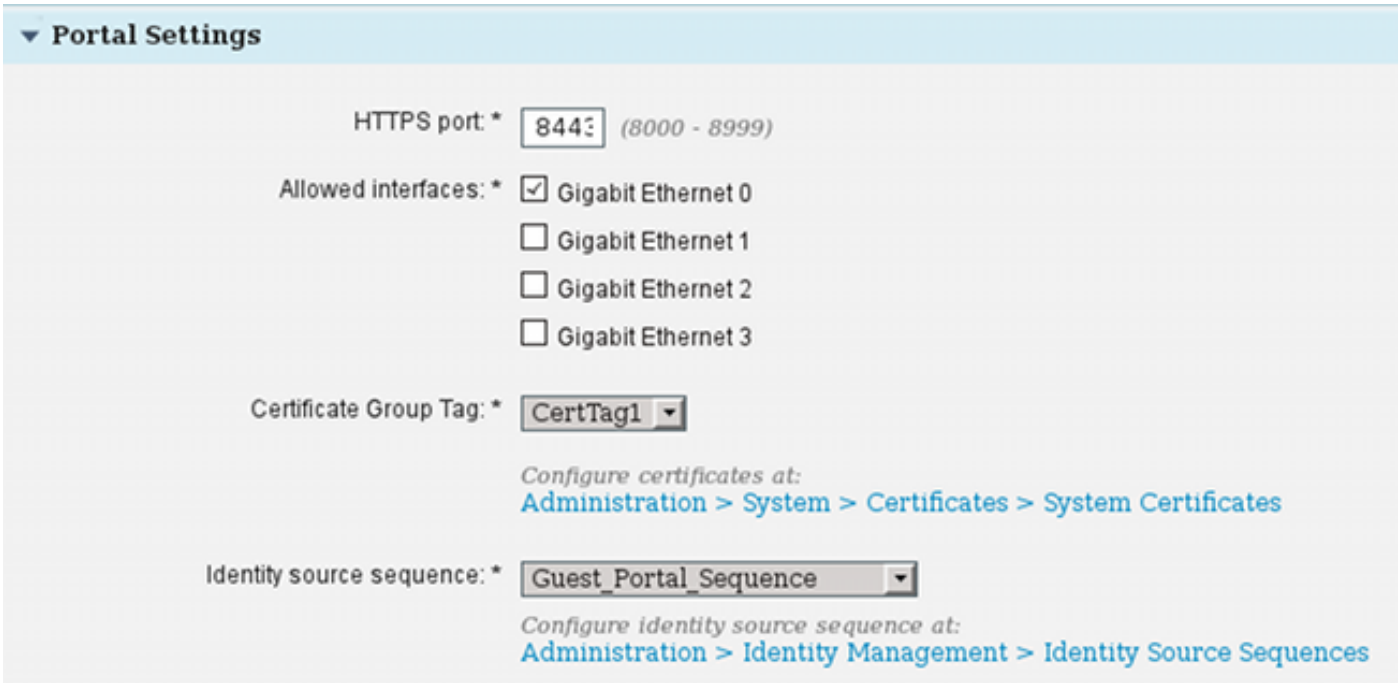
```
2014-08-01 21:35:08,435 ERROR  [http-bio-10.62.97.21-8443-exec-9][] guestaccess.
flowmanager.step.guest.ClientProvStepExecutor -:7AAF75982E0FCD594FE97DE2970D472F::-
CP Response is not successful, status=NO_POLICY
```

BYOD

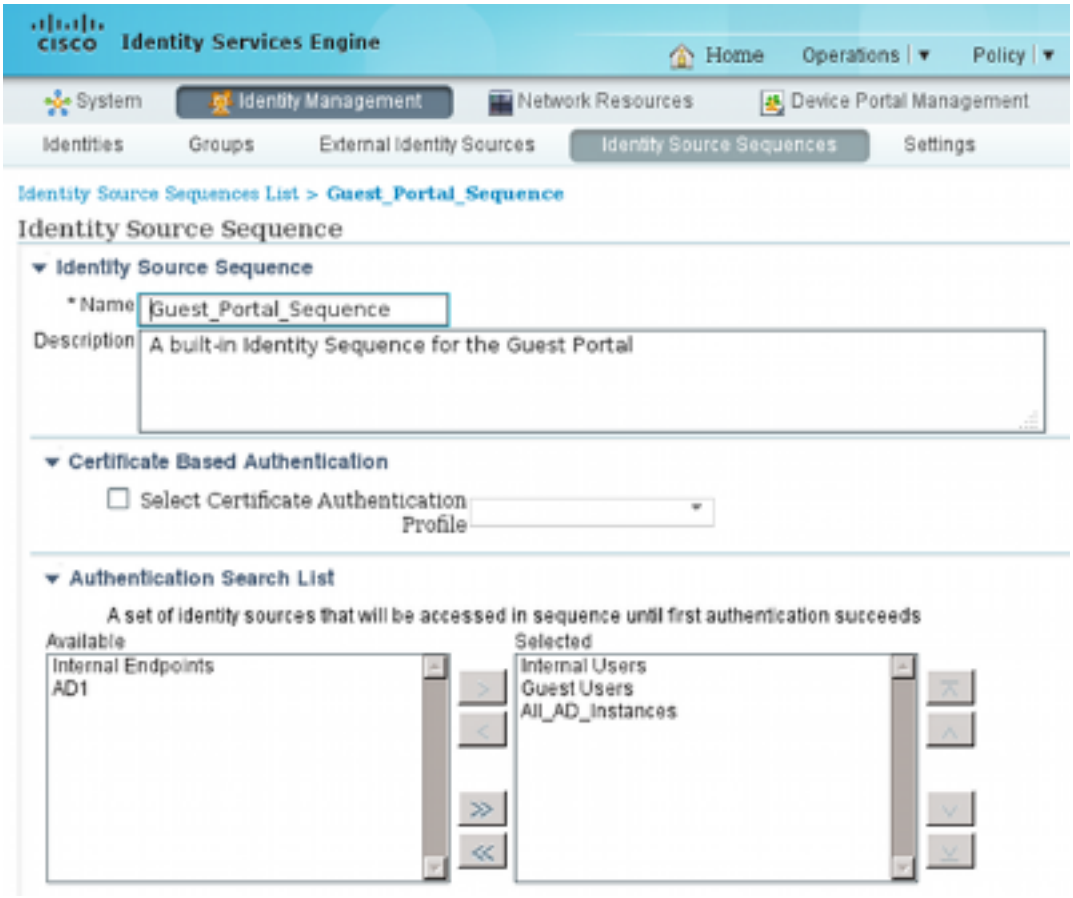
如果**使用在Network选项的个人设备的允许员工**选择，则使用此门户的集群用户可以通过BYOD流并且注册个人设备。对于来宾用户，该设置不更改什么。

“使用门户的员工作为访客”是什么意思？

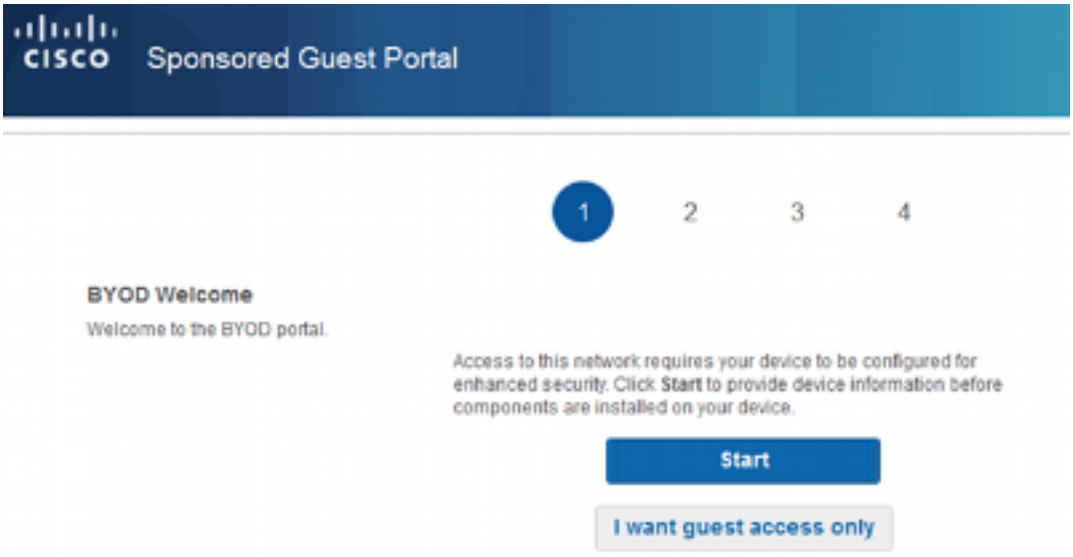
默认情况下，访客门户配置与Guest_Portal_Sequence标识存储：



这是首先审判内部用户的内部存储顺序(在来宾用户前) ：



当在此阶段在访客门户，用户提供在内部用户存储定义，并且BYOD重定向发生的凭证：



此方式集群用户可执行个人设备的BYOD。

当而不是内部用户凭证，提供来宾用户凭证，正常流继续(没有BYOD)。

VLAN更改

这是一个相似的选项对为访客门户配置的VLAN更改在ISE版本1.2。它允许您运行ActiveX或Java程序，触发DHCP发布和更新。当CoA触发VLAN更改终端的时，这是需要的。当使用时MAB，终端不知道VLAN更改。可能的解决方案将更改VLAN (DHCP版本/更新)用美洲台代理程序。另一个选项是请求一个新的IP地址通过在网页返回的applet。版本/CoA之间的延迟/更新可以配置。此选项不为移动设备支持。

相关信息

- 在思科ISE配置指南的状态服务
- 无线BYOD用身份服务引擎
- ISE BYOD配置示例的SCEP支持
- 思科ISE 1.3管理员指南
- 在WLC和ISE配置示例的中央Web验证
- 与FlexConnect AP的中央Web验证在与ISE配置示例的一WLC
- 技术支持和文档 - Cisco Systems