# 配置ISE自注册访客门户

## 目录

## 简介

本文档介绍如何配置ISE自注册访客门户功能并对其进行故障排除。

## 先决条件

### 要求

思科建议您具有ISE配置经验并具备以下主题的基本知识：

- ISE部署和访客流量
- 无线局域网控制器(WLC)的配置

### 使用的组件

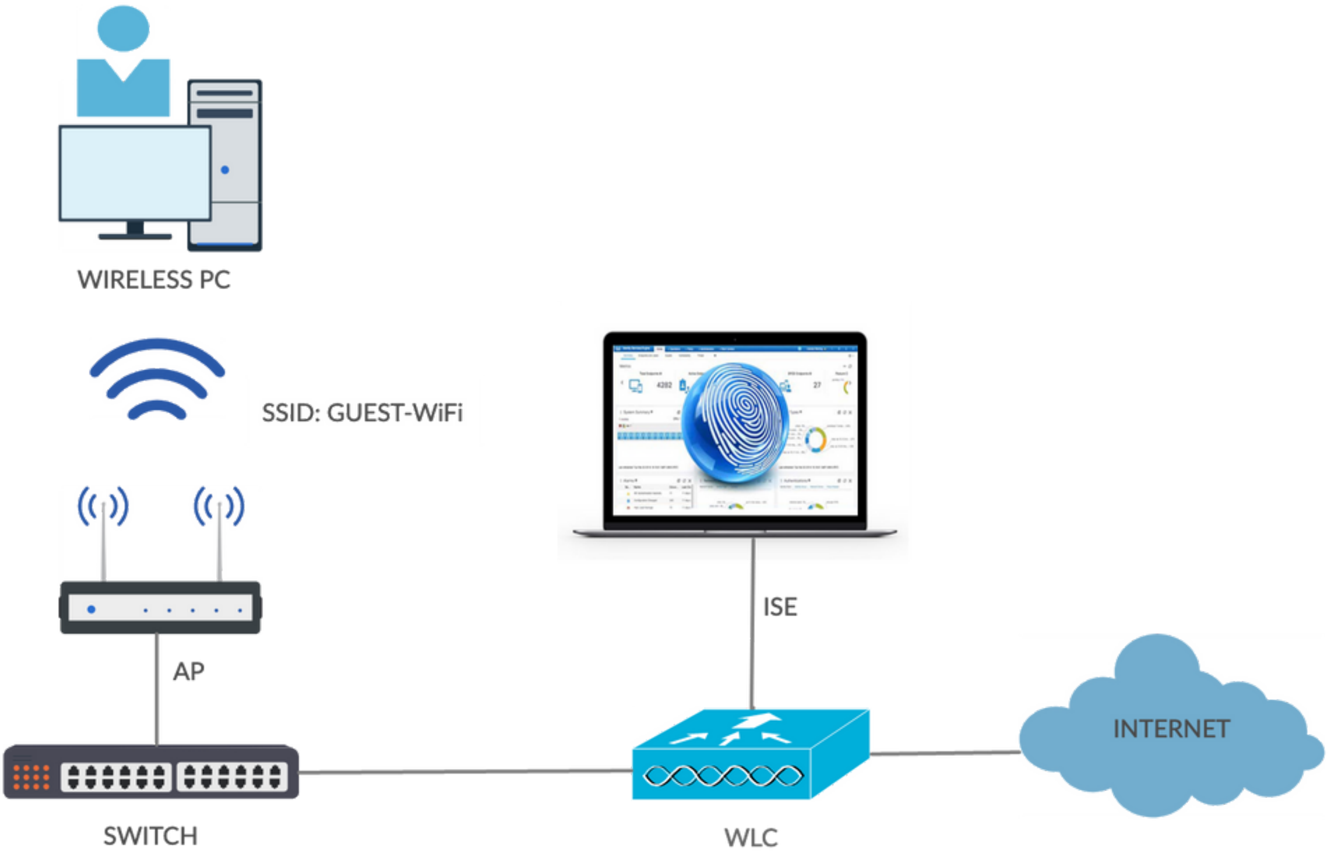
自助注册访客门户，允许访客用户与员工自助注册，以使用他们的AD凭证获得网络资源的访问权限。此门户允许您配置和自定义多个功能。

本文档中的信息基于以下软件和硬件版本：

- Microsoft Windows 10 Pro
- Cisco WLC 5508，版本8.5.135.0
- ISE软件，版本3.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 拓扑和流程



此场景为访客用户执行自助注册时提供了多个可用选项。

以下是一般流程：

步骤1:访客用户关联到服务集标识符(SSID)：访客WiFi。这是一个开放式网络，使用ISE进行MAC过滤以进行身份验证。此身份验证与ISE上的第二个授权规则匹配，并且授权配置文件重定向到访客自助注册门户。ISE返回包含两个cisco-av-pairs的RADIUS Access-Accept:

- url-redirect-acl(必须重定向哪些流量以及WLC上本地定义的访问控制列表(ACL)的名称)
- url-redirect（从何处重定向该流量 — 到ISE）

第二步：访客用户被重定向到ISE。用户点击Register for Guest Access，而不是提供凭证以便登录。 用户被重定向到可创建该帐户的页面。可以启用可选的加密注册码，以将自行注册权限限制为知道该加密值的人员。创建帐户后，系统将为用户提供凭证（用户名和密码），并使用这些凭证登录。

第三步：ISE向WLC发送RADIUS授权更改(CoA)重新身份验证。当WLC发送具有Authorize-Only属性的RADIUS Access-Request时，会重新验证用户。ISE使用在WLC上本地定义的Access-Accept和Airespace ACL进行响应，仅提供互联网访问（访客用户的最终访问取决于授权策略）。

注意：可扩展身份验证协议(EAP)会话，ISE必须发送CoA Terminate以触发重新身份验证，因为EAP会话位于请求方和ISE之间。但是对于MAB（MAC过滤），CoA重新身份验证就足够了；无需取消关联/取消验证无线客户端。

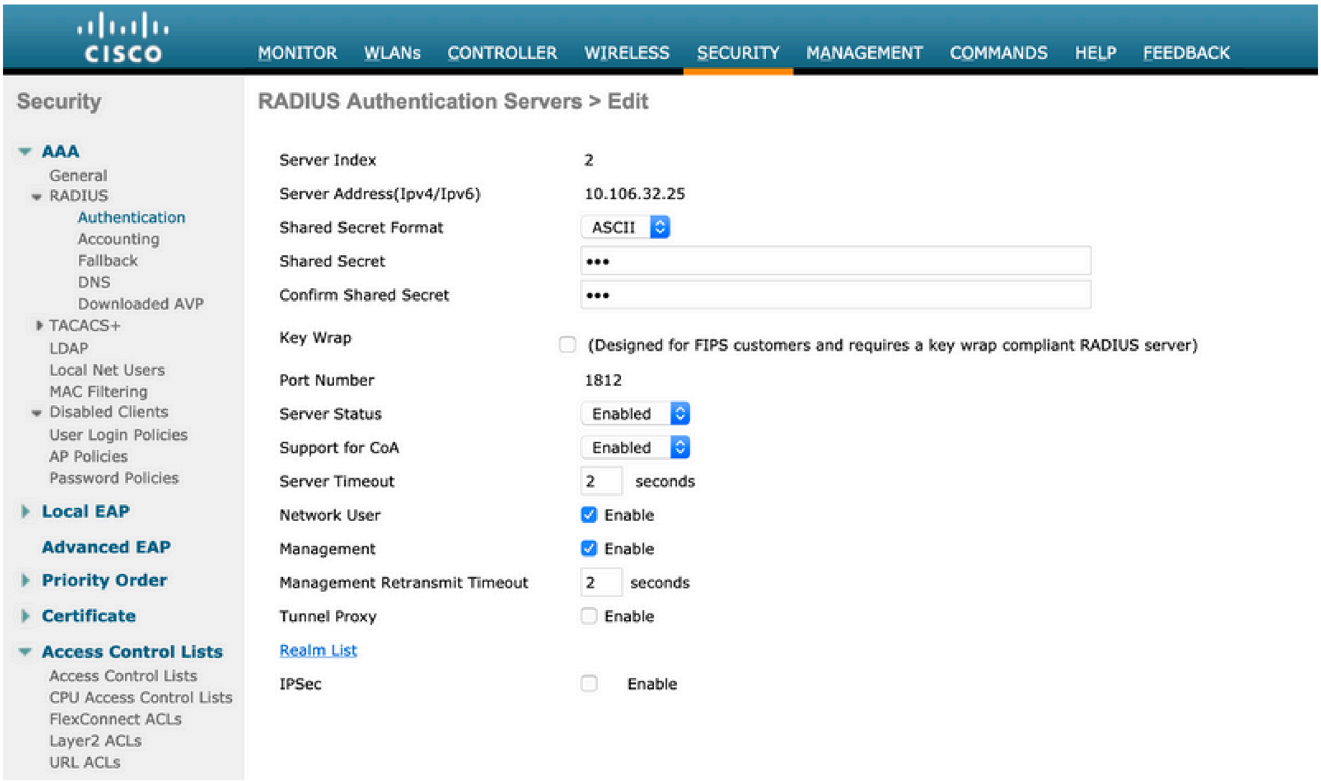
第四步：访客用户具有所需的网络访问权限。

可以启用多项其他功能，例如安全评估和自带设备(BYOD)（稍后讨论）。

# 配置

## WLC

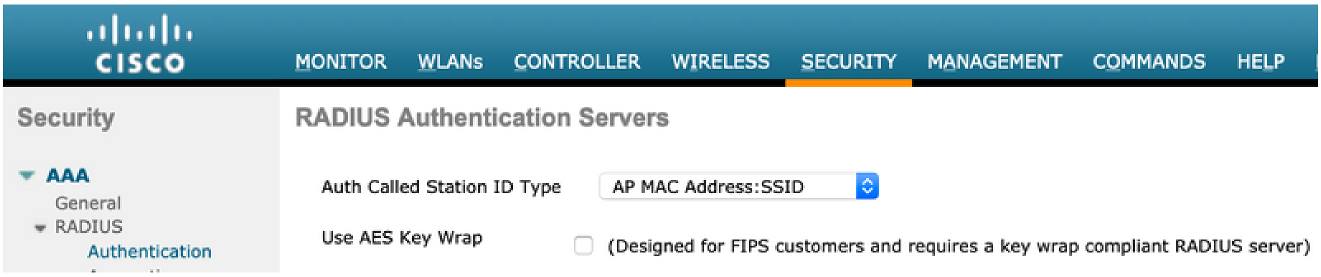
1. 为身份验证和记帐添加新的RADIUS服务器。导航到安全> AAA > Radius >身份验证以启用RADIUS CoA(RFC 3576)。



RADIUS Authentication Servers > Edit

| | |
|---|---|
| Server Index | 2 |
| Server Address(Ipv4/Ipv6) | 10.106.32.25 |
| Shared Secret Format | ASCII |
| Shared Secret | ••• |
| Confirm Shared Secret | ••• |
| Key Wrap | □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server) |
| Port Number | 1812 |
| Server Status | Enabled |
| Support for CoA | Enabled |
| Server Timeout | 2 seconds |
| Network User | ☑ Enable |
| Management | ☑ Enable |
| Management Retransmit Timeout | 2 seconds |
| Tunnel Proxy | □ Enable |
| Realm List | |
| IPSec | □ Enable |

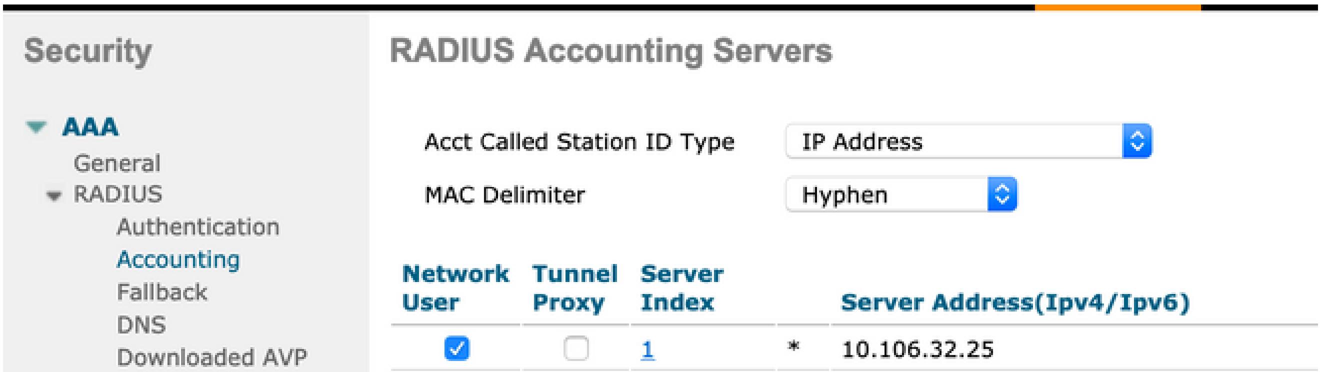
Accounting有类似的配置。建议将WLC配置为发送“被叫站ID”属性中的SSID，从而允许ISE根据SSID配置灵活的规则：



RADIUS Authentication Servers

Auth Called Station ID Type: AP MAC Address:SSID

Use AES Key Wrap □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)



RADIUS Accounting Servers

Acct Called Station ID Type: IP Address

MAC Delimiter: Hyphen

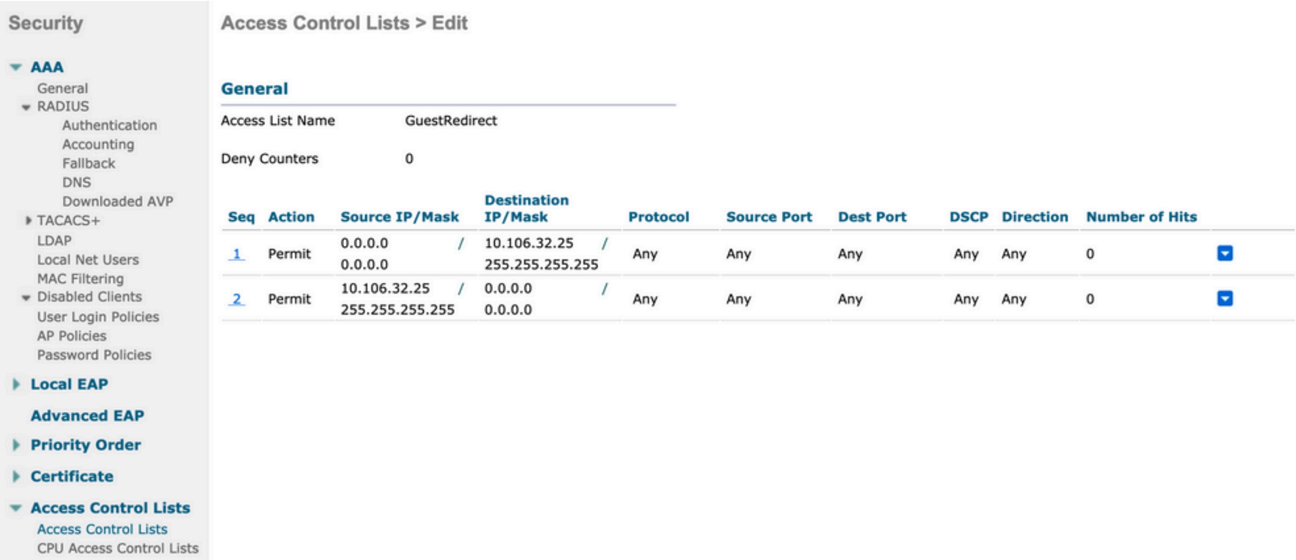
| Network User | Tunnel Proxy | Server Index | | Server Address(Ipv4/Ipv6) |
|---|---|---|---|---|
| ☑ | □ | 1 | * | 10.106.32.25 |

2. 在WLANs选项卡下，创建无线LAN(WLAN)访客WiFi并配置正确的接口。使用MAC过滤将第2层安全设置为None。在安全/身份验证、授权和记帐(AAA)服务器中，选择身份验证和记帐的ISE IP地址。在Advanced选项卡上，启用AAA Override，并将网络准入控制(NAC)状态设置为ISE NAC（CoA支持）。

3. 导航到安全>访问控制列表>访问控制列表，并创建两个访问列表：

   - GuestRedirect，允许不得重定向的流量并重定向所有其他流量
   - Internet，公司网络拒绝该协议，而所有其他网络均允许该协议

以下是GuestRedirect ACL的示例（需要从重定向排除ISE流量或来自ISE的流量）：



Access Control Lists > Edit

General

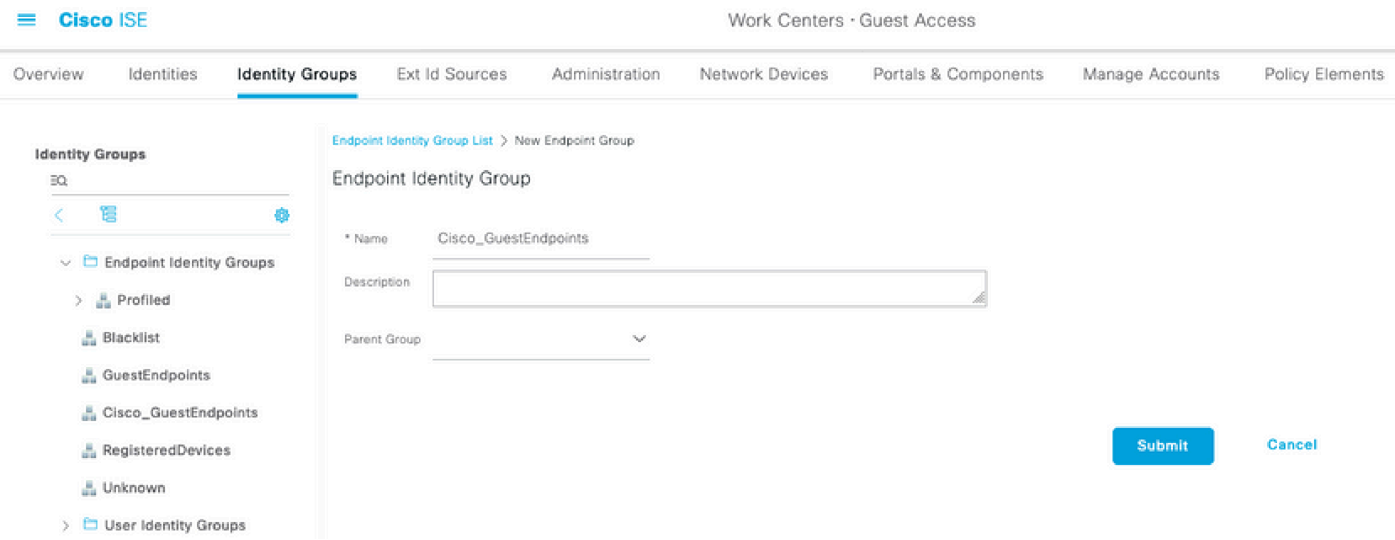
Access List Name: GuestRedirect

Deny Counters: 0

| 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 | 10.106.32.25 / 255.255.255.255 | Any | Any | Any | Any | Any | 0 |
| 2 | Permit | 10.106.32.25 / 255.255.255.255 | 0.0.0.0 / 0.0.0.0 | Any | Any | Any | Any | Any | 0 |

## ISE

1. 从Work Centers > Guest Access > Network Devices将WLC添加为网络接入设备。
2. 创建终端身份组。导航到工作中心(Work Centers)>访客接入(Guest Access)>身份组(Identity Groups)>终端身份组(Endpoint Identity Groups)。

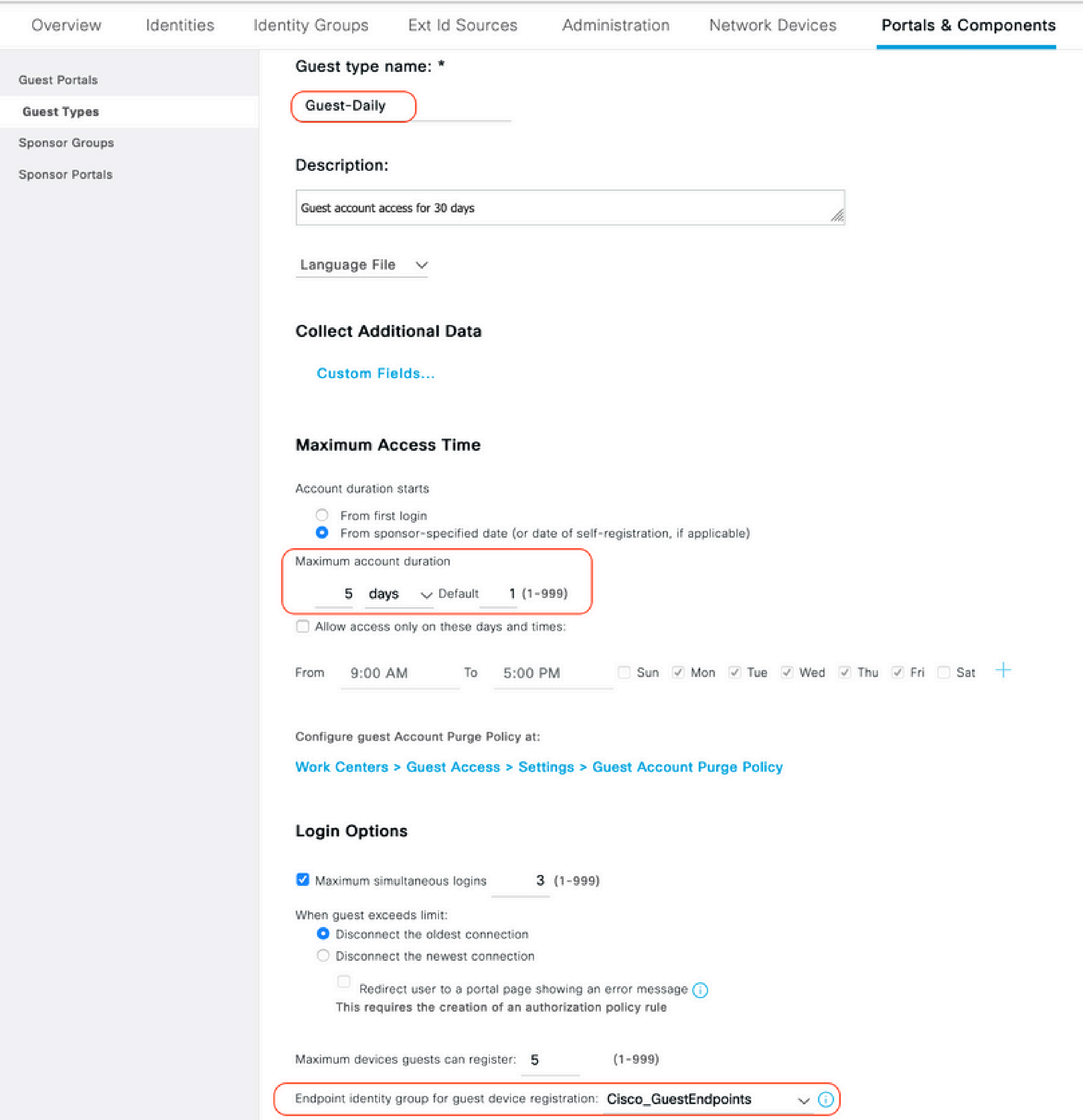


* Name Cisco_GuestEndpoints

Description

Parent Group

3.通过导航到工作中心>访客接入>门户和组件>访客类型，创建访客类型。请参阅之前在此新访客类型下创建的终端身份组并保存。



Guest type name: *

Guest-Daily

Description:

Guest account access for 30 days

Language File

Collect Additional Data

Custom Fields...

Maximum Access Time

Account duration starts

○ From first login
● From sponsor-specified date (or date of self-registration, if applicable)

Maximum account duration

5 days Default 1 (1-999)

□ Allow access only on these days and times:

From 9:00 AM To 5:00 PM □ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat

Configure guest Account Purge Policy at:

Work Centers > Guest Access > Settings > Guest Account Purge Policy

Login Options

☑ Maximum simultaneous logins 3 (1-999)

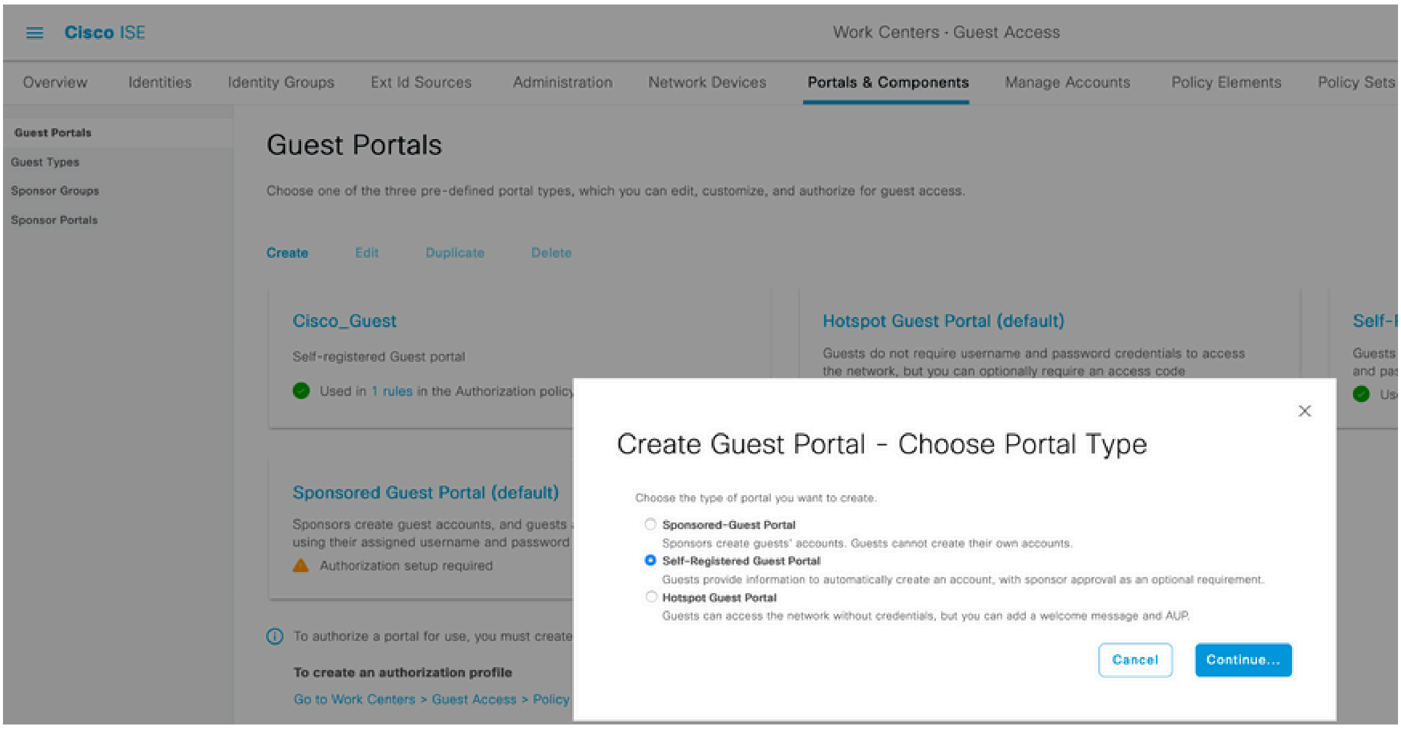
When guest exceeds limit:
● Disconnect the oldest connection
○ Disconnect the newest connection

□ Redirect user to a portal page showing an error message
This requires the creation of an authorization policy rule

Maximum devices guests can register: 5 (1-999)

Endpoint identity group for guest device registration: Cisco_GuestEndpoints

4.创建新的访客门户类型：自注册访客门户。导航至工作中心(Work Centers)>访客接入(Guest Access)>访客门户(Guest Portals)。



Guest Portals

Choose one of the three pre-defined portal types, which you can edit, customize, and authorize for guest access.

Cisco_Guest

Self-registered Guest portal

Used in 1 rules in the Authorization policy

Hotspot Guest Portal (default)

Guests do not require username and password credentials to access the network, but you can optionally require an access code

Sponsored Guest Portal (default)

Sponsors create guest accounts, and guests using their assigned username and password

Authorization setup required

To authorize a portal for use, you must create

To create an authorization profile

Go to Work Centers > Guest Access > Policy

Create Guest Portal - Choose Portal Type

Choose the type of portal you want to create.

○ Sponsored-Guest Portal
Sponsors create guests' accounts. Guests cannot create their own accounts.

● Self-Registered Guest Portal
Guests provide information to automatically create an account, with sponsor approval as an optional requirement.

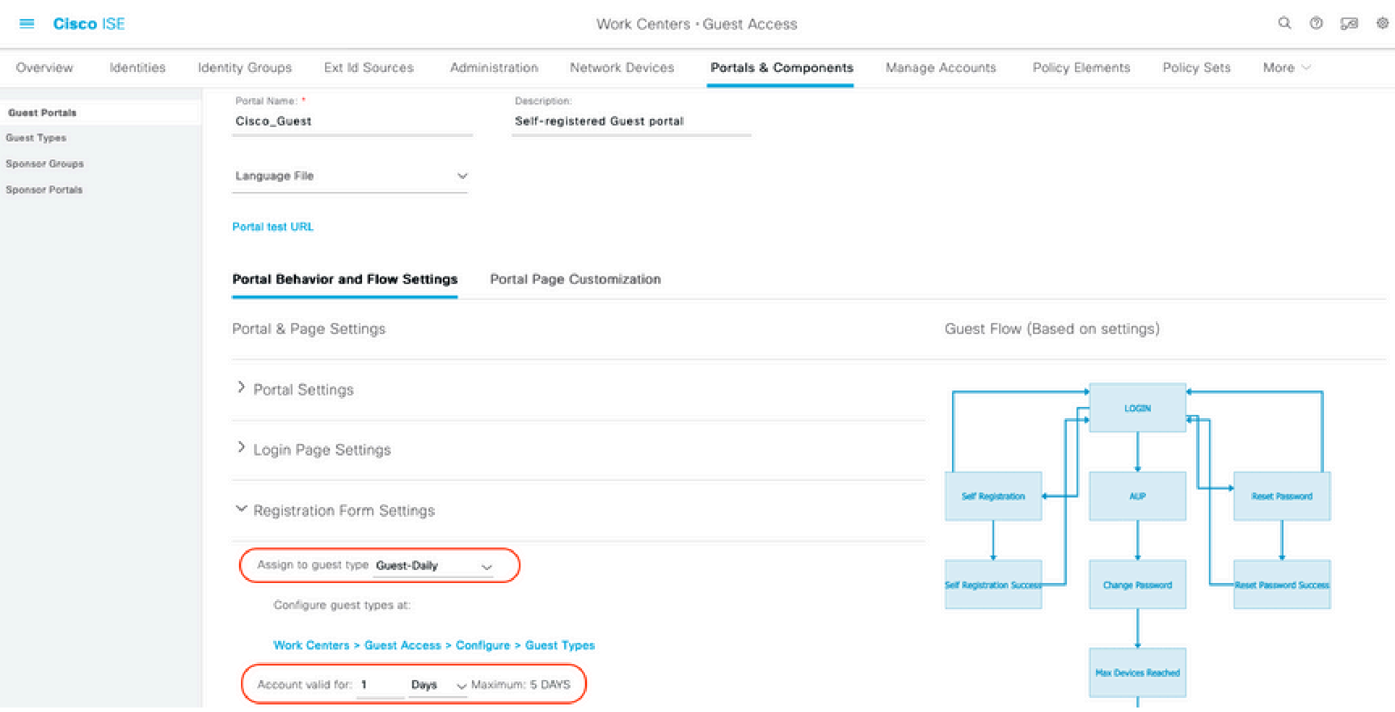
○ Hotspot Guest Portal
Guests can access the network without credentials, but you can add a welcome message and AUP.

5.选择门户名称，参阅之前创建的访客类型，然后在“注册表”设置下发送凭证通知设置，以通过邮件发送凭证。

有关如何在ISE上配置SMTP服务器，请参阅本文档：

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/216187-configure-secure-smtp-server-on-ise.html

将所有其他设置保留为默认值。在Portal Page Customization下，可以自定义显示的所有页面。默认情况下，访客帐户的有效期为1天，可以延长到特定访客类型下配置的天数。



Portal Name: * Cisco_Guest

Description: Self-registered Guest portal

Language File

Portal & Page Settings

› Portal Settings

› Login Page Settings

⌄ Registration Form Settings

Assign to guest type Guest-Daily

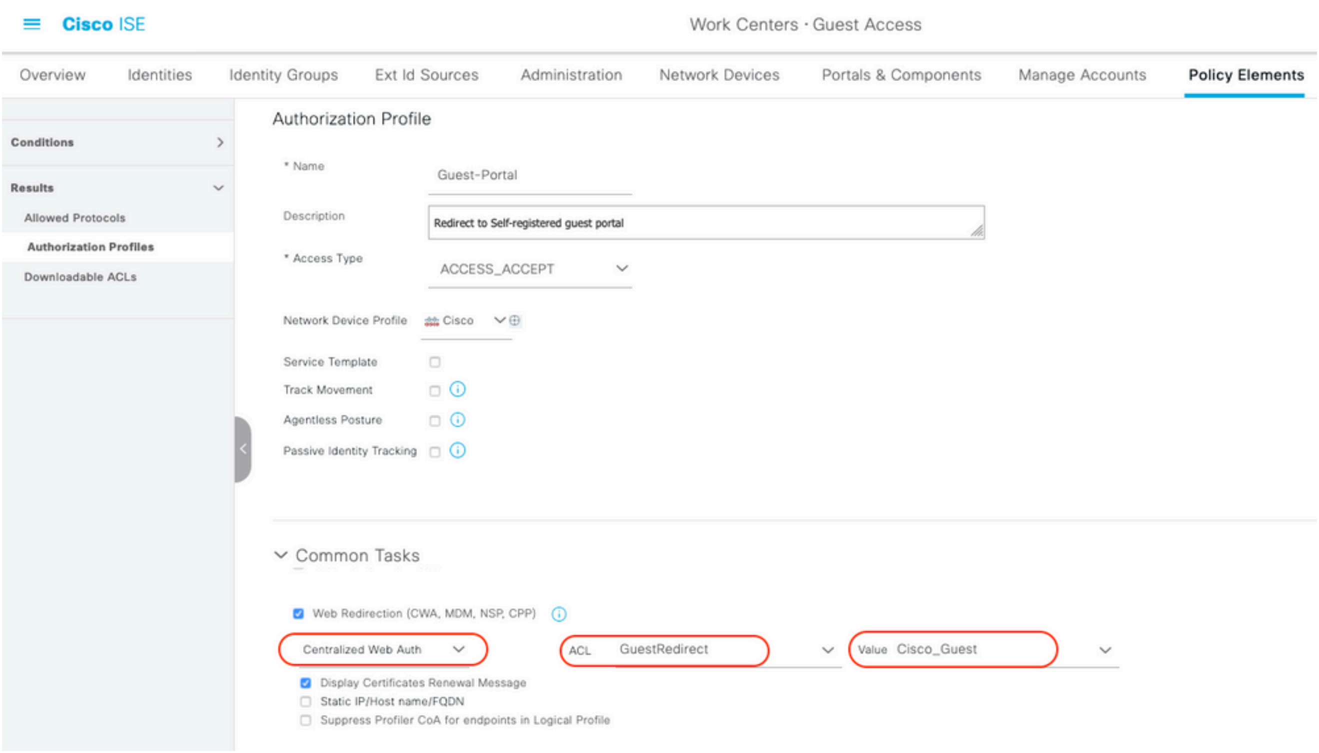
Configure guest types at:

Work Centers > Guest Access > Configure > Guest Types

Account valid for: 1 Days Maximum: 5 DAYS

6.通过导航到工作中心> Guest Access > Policy Elements > Results > Authorization Profiles 配置这两个授权配置文件。

- 访客门户(重定向到访客门户Cisco_Guest和名为GuestRedirect的重定向ACL)。此GuestRedirect ACL是之前在WLC上创建的。



Authorization Profile

* Name: Guest-Portal

Description: Redirect to Self-registered guest portal

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Agentless Posture □

Passive Identity Tracking □

Common Tasks

☑ Web Redirection (CWA, MDM, NSP, CPP)

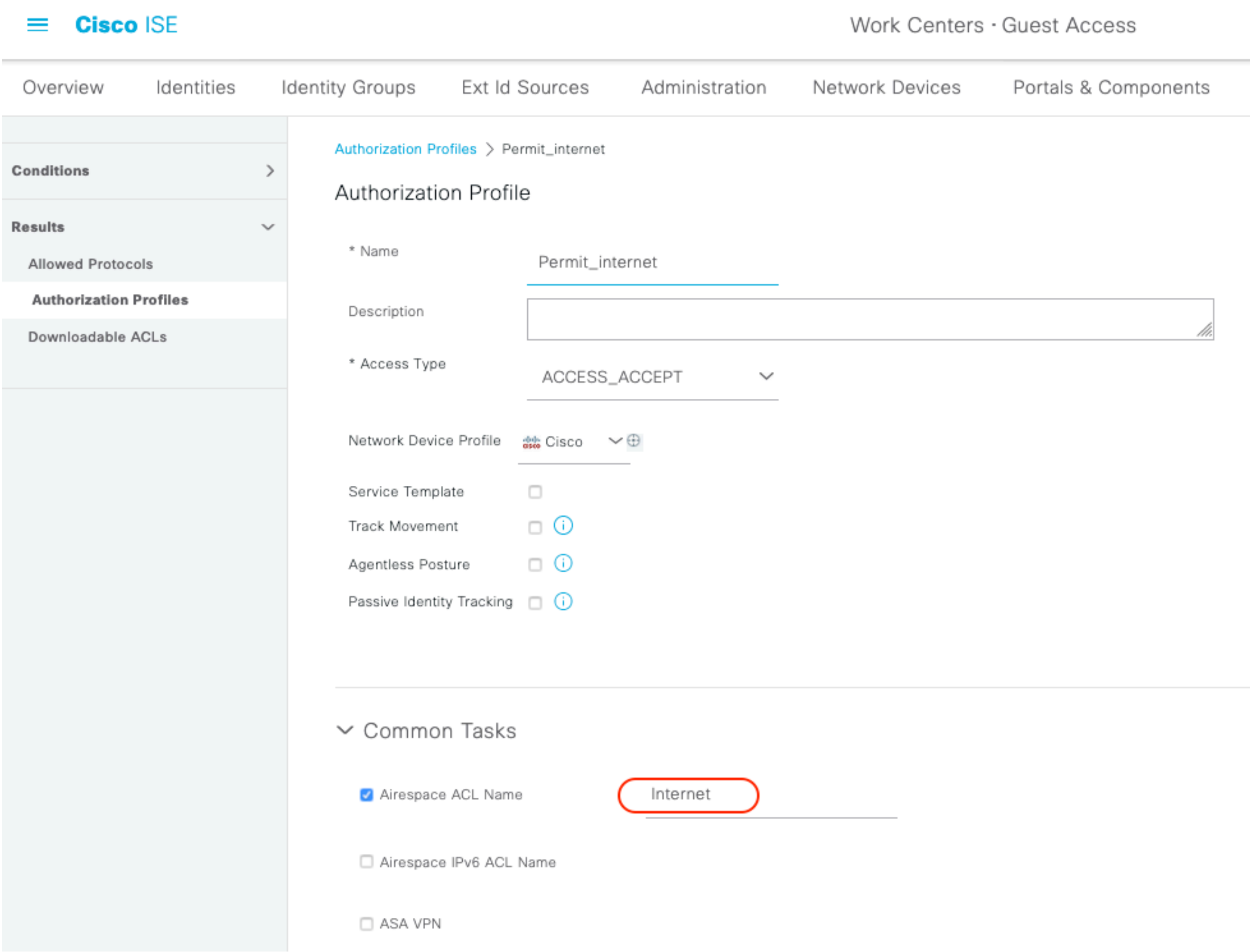
Centralized Web Auth | ACL GuestRedirect | Value Cisco_Guest

☑ Display Certificates Renewal Message

□ Static IP/Host name/FQDN

□ Suppress Profiler CoA for endpoints in Logical Profile

- Permit_Internet（Airespace ACL与Internet相同）



Authorization Profile

* Name: Permit_internet

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Agentless Posture □

Passive Identity Tracking □

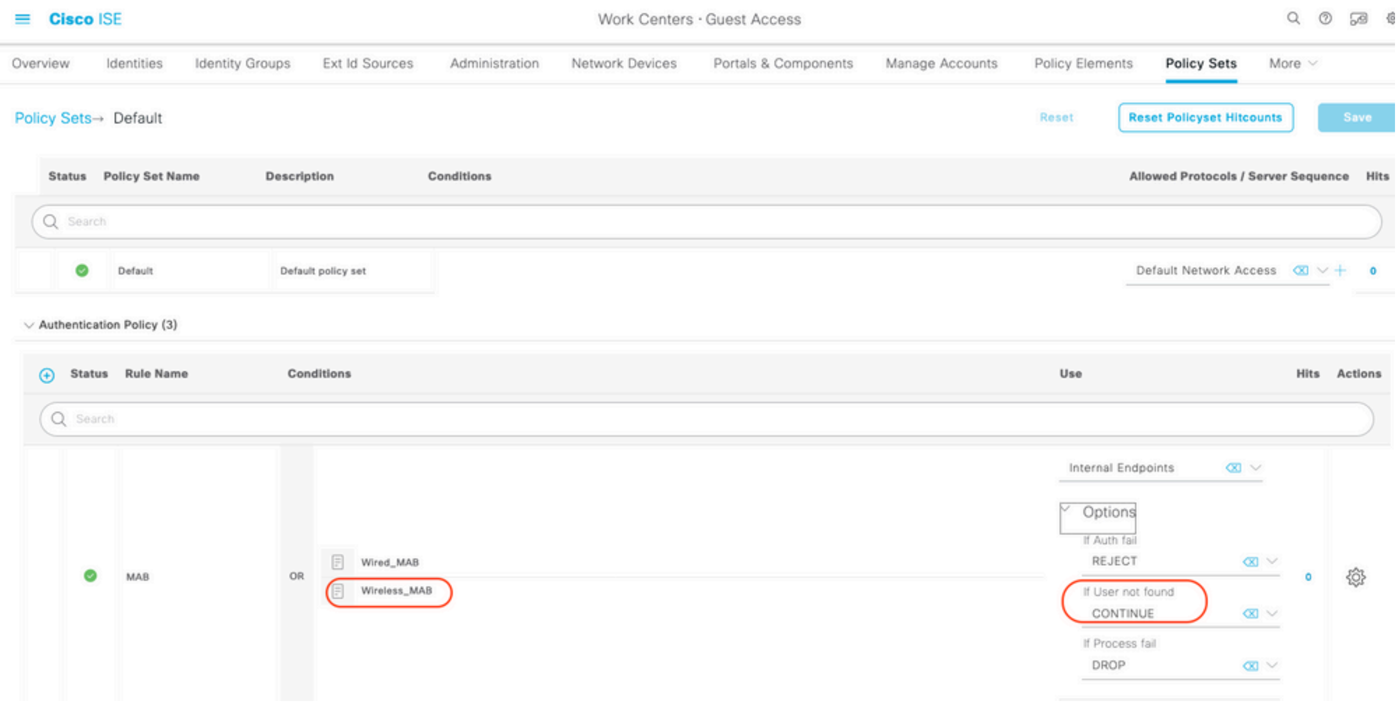
Common Tasks

☑ Airespace ACL Name: Internet

□ Airespace IPv6 ACL Name

□ ASA VPN

7.修改名为Default的策略集。已为访客门户访问预配置默认策略集。存在名为MAB的身份验证策略，该策略允许MAC身份验证绕行(MAB)身份验证针对未知Mac地址继续（而不是拒绝）。

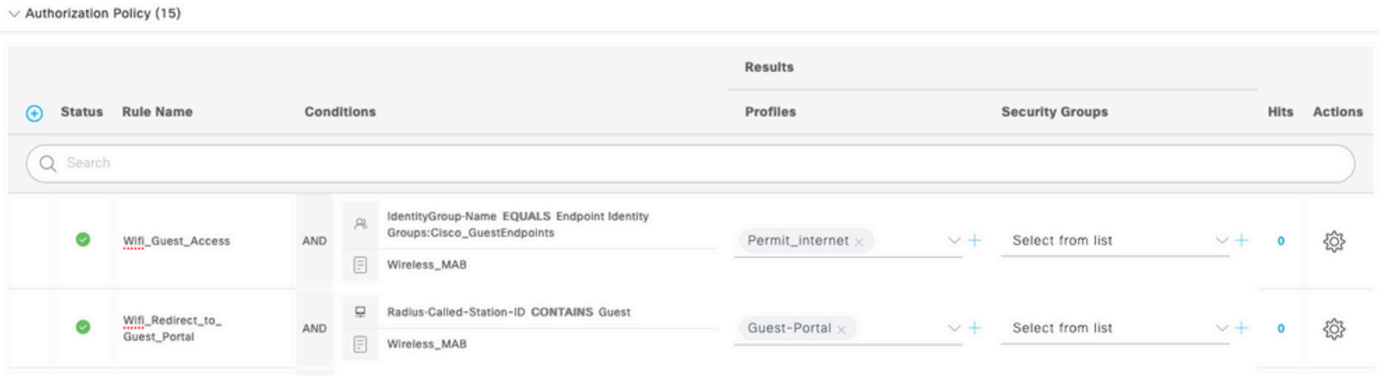


| Status | Policy Set Name | Description | Conditions | Allowed Protocols / Server Sequence | Hits |
|---|---|---|---|---|---|
| ● | Default | Default policy set | | Default Network Access | 0 |

Authentication Policy (3)

| Status | Rule Name | Conditions | Use | Hits | Actions |
|---|---|---|---|---|---|
| ● | MAB | OR Wired_MAB<br>Wireless_MAB | Internal Endpoints<br>Options<br>If Auth fail: REJECT<br>If User not found: CONTINUE<br>If Process fail: DROP | 0 | |

8.导航到同一页上的Authorization policy。创建此授权规则，如下图所示。



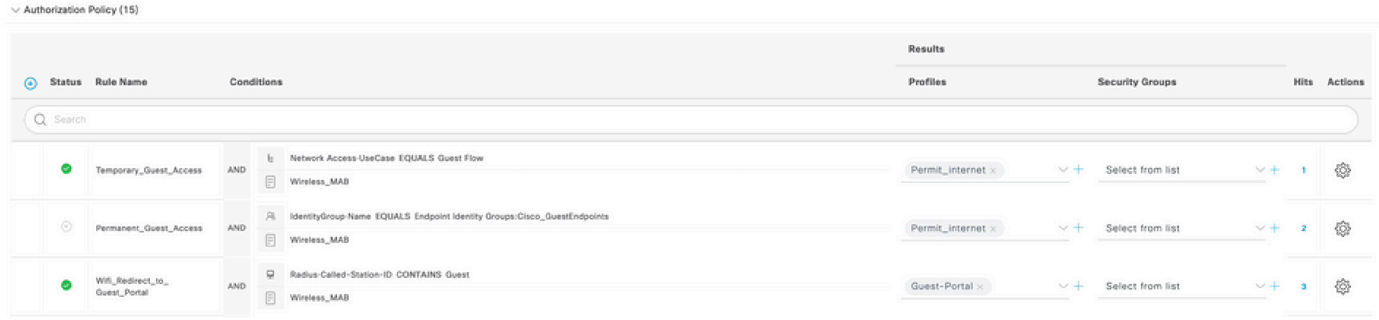
Authorization Policy (15)

| Status | Rule Name | | Conditions | Results: Profiles | Results: Security Groups | Hits | Actions |
|---|---|---|---|---|---|---|---|
| ● | Wifi_Guest_Access | AND | IdentityGroup·Name EQUALS Endpoint Identity Groups:Cisco_GuestEndpoints<br>Wireless_MAB | Permit_internet | Select from list | 0 | ⚙ |
| ● | Wifi_Redirect_to_Guest_Portal | AND | Radius·Called-Station-ID CONTAINS Guest<br>Wireless_MAB | Guest-Portal | Select from list | 0 | ⚙ |

与访客SSID关联的新用户尚未属于任何身份组，因此与第二条规则匹配并重定向到访客门户。

用户成功登录后，ISE会发送RADIUS CoA并且WLC会执行重新身份验证。此时，匹配第一个授权规则（当终端成为已定义的终端身份组的一部分时），并且用户获得Permit_internet授权配置文件。

9.我们还可以使用条件“访客”流程为访客提供临时访问权限。该情况正在检查ISE上的活动会话，并且它属于特定情况。如果该会话具有指示先前访客用户已经成功通过身份验证的属性，则匹配条件。在ISE收到来自网络接入设备(NAD)的Radius记帐停止消息后，会话被终止并随后被删除。在此阶段，不再满足Network Access:UseCase = Guest Flow的条件。因此，该终端的所有后续身份验证都会命中通用规则重定向以进行访客身份验证。



Authorization Policy (15)

| Status | Rule Name | | Conditions | Results: Profiles | Results: Security Groups | Hits | Actions |
|---|---|---|---|---|---|---|---|
| ● | Temporary_Guest_Access | AND | Network Access·UseCase EQUALS Guest Flow<br>Wireless_MAB | Permit_internet | Select from list | 1 | ⚙ |
| ○ | Permanent_Guest_Access | AND | IdentityGroup·Name EQUALS Endpoint Identity Groups:Cisco_GuestEndpoints<br>Wireless_MAB | Permit_internet | Select from list | 2 | ⚙ |
| ● | Wifi_Redirect_to_Guest_Portal | AND | Radius·Called-Station-ID CONTAINS Guest<br>Wireless_MAB | Guest-Portal | Select from list | 3 | ⚙ |

注：您一次可以使用临时访客接入和永久访客接入，但不能同时使用两者。

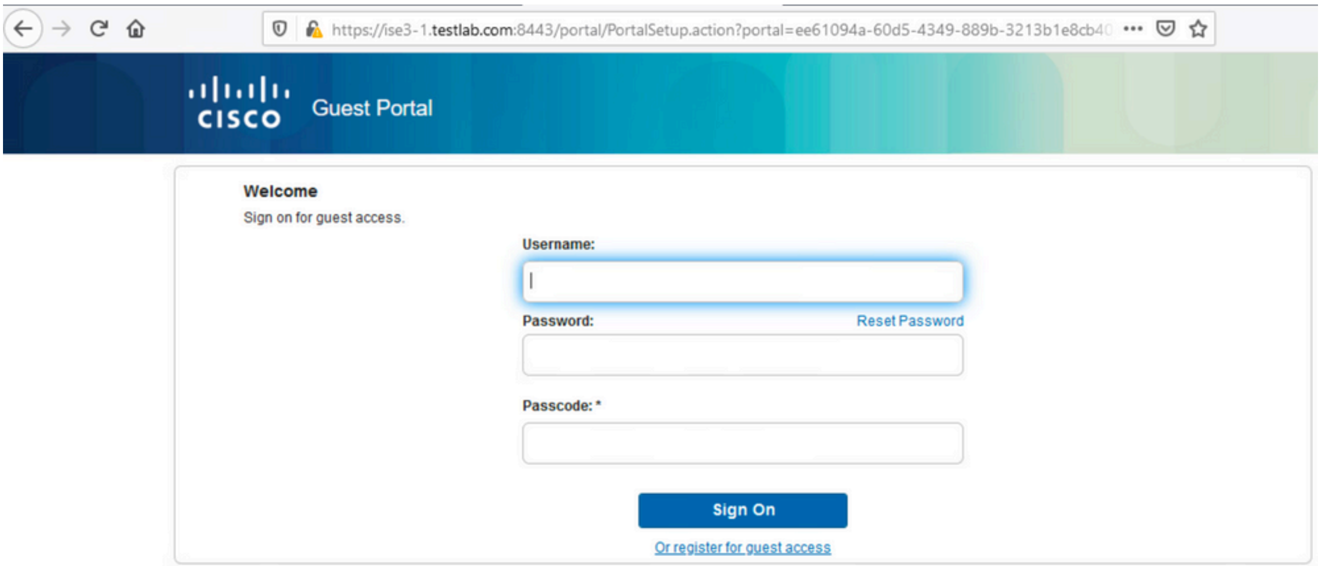
请参阅本文档详细了解ISE访客临时和永久访问配置。

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200273-Configure-ISE-Guest-Temporary-and-Perman.html

# 验证

使用本部分可确认配置能否正常运行。

1. 在关联访客SSID并键入URL后，系统将重定向到访客门户页面，如图所示。



https://ise3-1.testlab.com:8443/portal/PortalSetup.action?portal=ee61094a-60d5-4349-889b-3213b1e8cb40

Guest Portal

**Welcome**

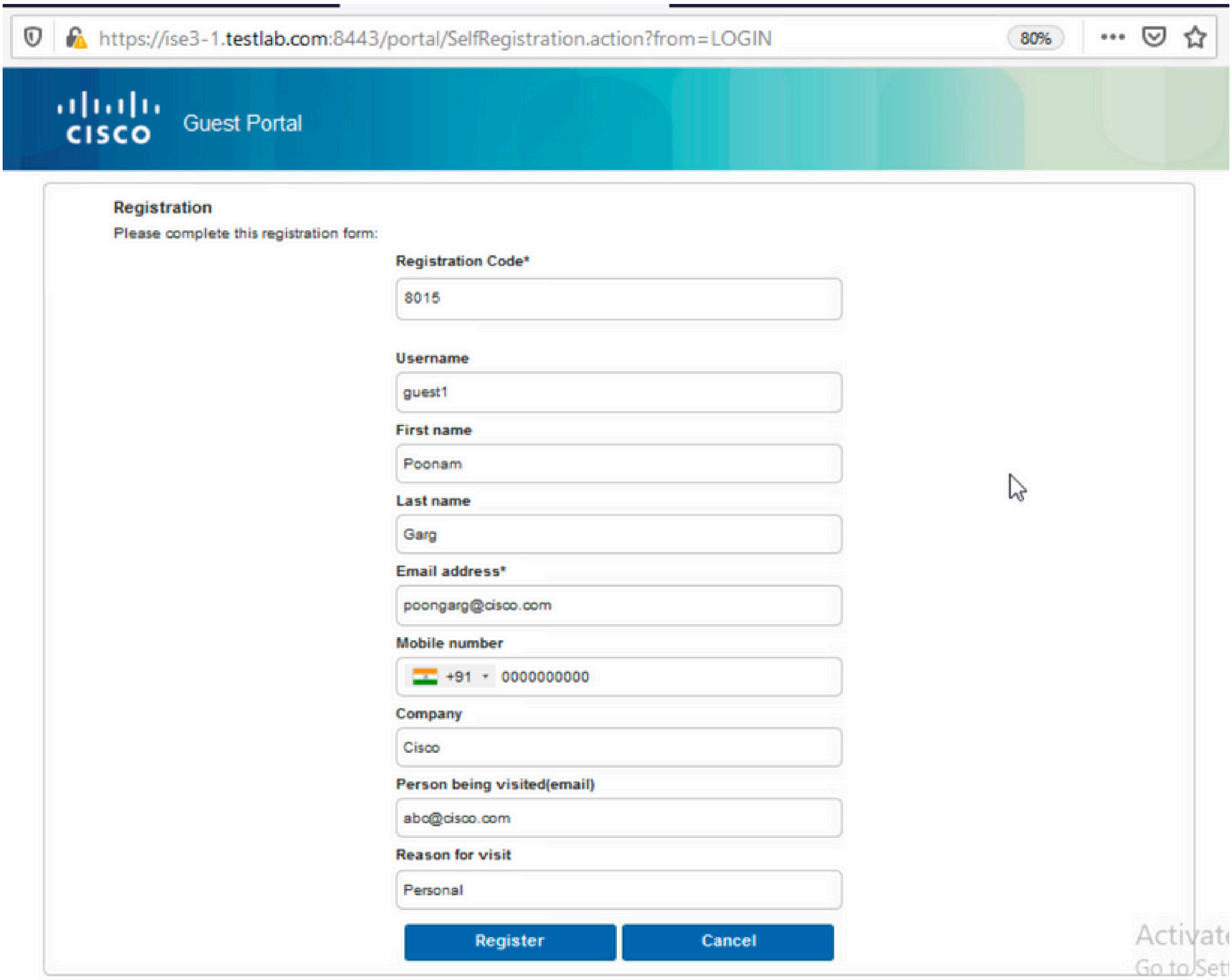
Sign on for guest access.

Username:

Password: Reset Password

Passcode: *

2. 由于您没有任何凭证，您必须选择Register for Guest access选项。系统将显示用于创建帐户的注册表。如果在Guest Portal配置下启用了Registration Code选项，则需要该密钥值（这可以确保仅允许具有正确权限的人员自行注册）。



https://ise3-1.testlab.com:8443/portal/SelfRegistration.action?from=LOGIN

Guest Portal

**Registration**

Please complete this registration form:

Registration Code*: 8015

Username: guest1

First name: Poonam

Last name: Garg

Email address*: poongarg@cisco.com

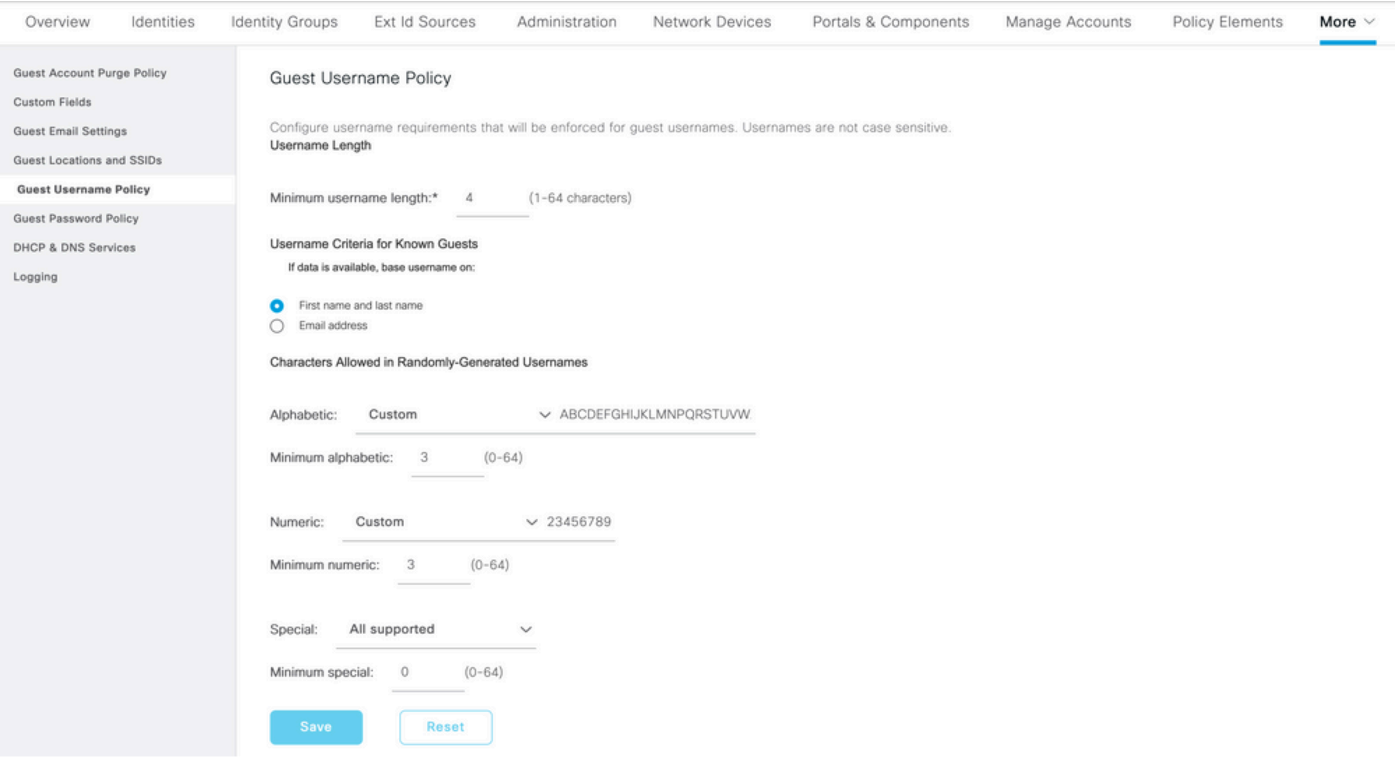
Mobile number: +91 0000000000

Company: Cisco

Person being visited(email): abc@cisco.com

Reason for visit: Personal

3.如果密码或用户策略存在任何问题，请导航至工作中心> 访客接入>设置>访客用户名策略以更改设置。例如：



Guest Username Policy

Configure username requirements that will be enforced for guest usernames. Usernames are not case sensitive.

Username Length

Minimum username length:* 4 (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: Custom ABCDEFGHIJKLMNPQRSTUVW

Minimum alphabetic: 3 (0-64)

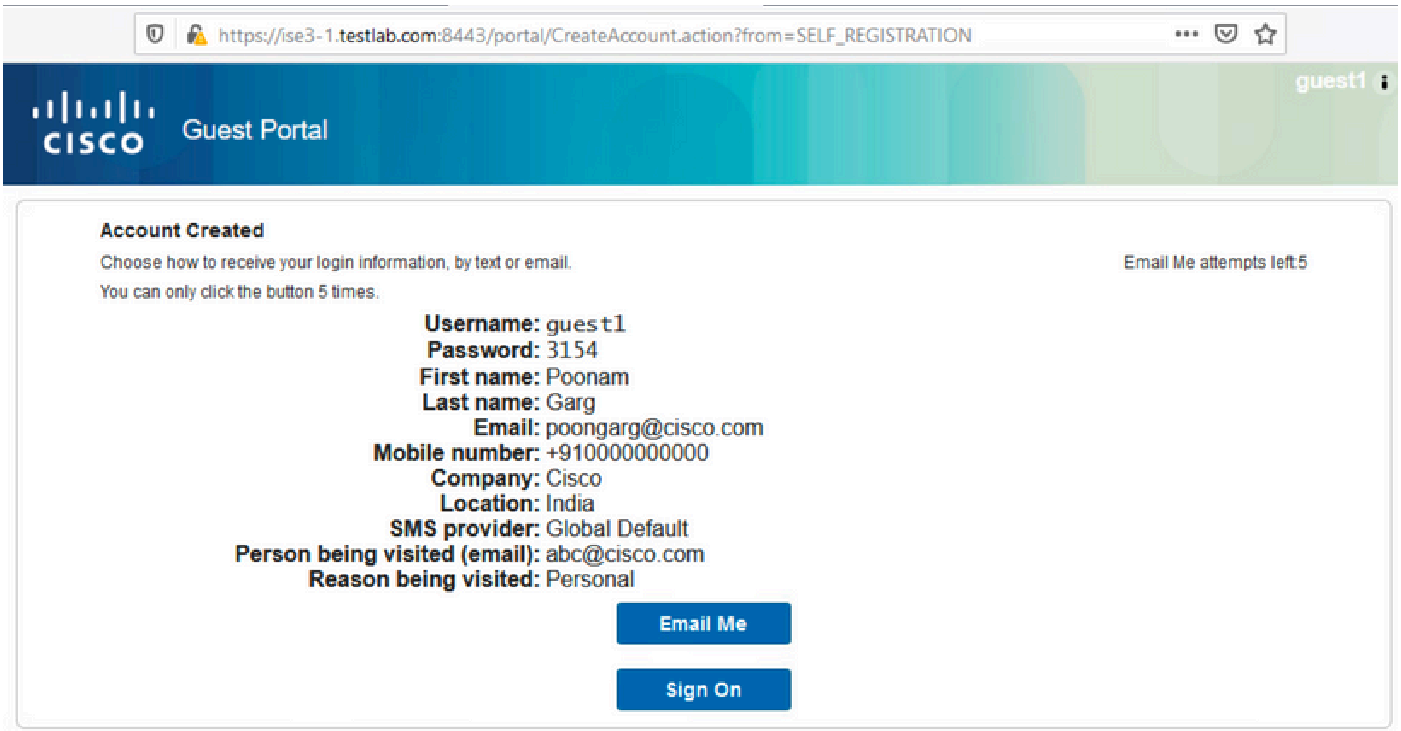
Numeric: Custom 23456789

Minimum numeric: 3 (0-64)

Special: All supported

Minimum special: 0 (0-64)

4.成功创建帐户后，系统将向您提供凭证（根据访客密码策略生成的密码），并且如果配置了凭证，访客用户还将收到电子邮件通知：


https://ise3-1.testlab.com:8443/portal/CreateAccount.action?from=SELF_REGISTRATION
guest1
cisco
Guest Portal

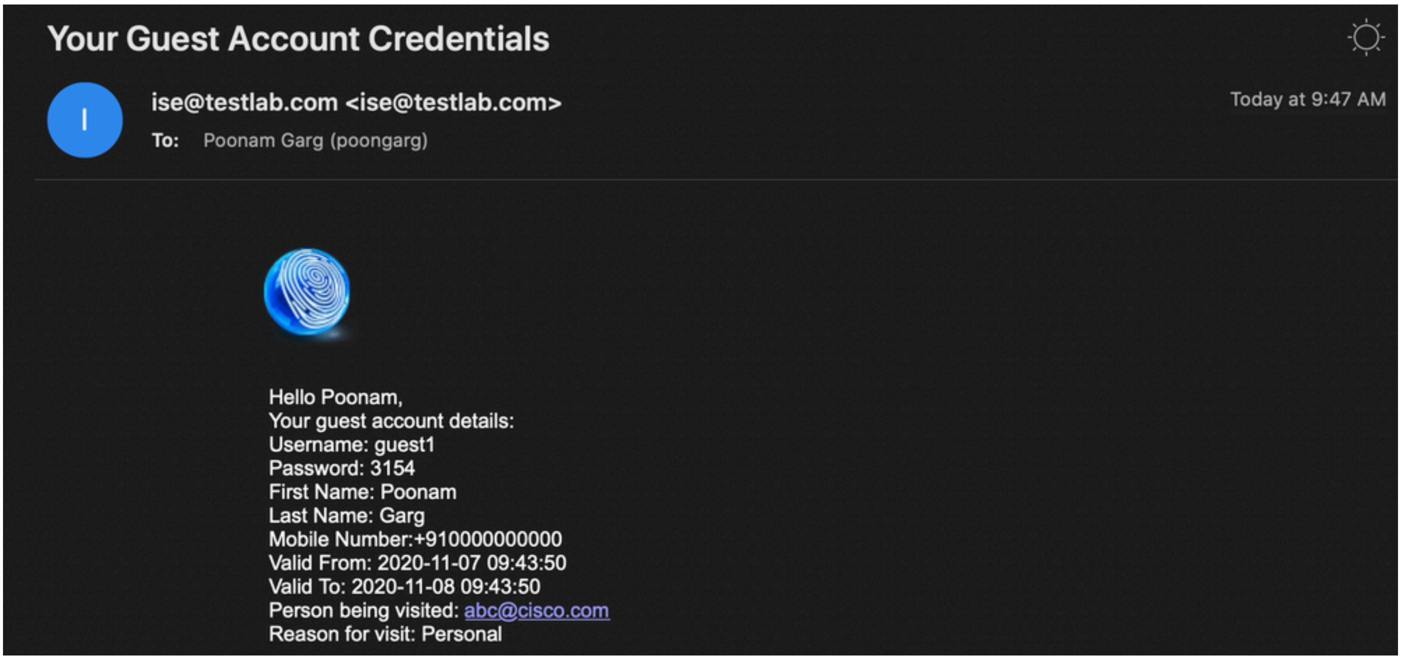
Account Created

Choose how to receive your login information, by text or email.

You can only click the button 5 times.

Email Me attempts left:5

**Username:** guest1
**Password:** 3154
**First name:** Poonam
**Last name:** Garg
**Email:** poongarg@cisco.com
**Mobile number:** +910000000000
**Company:** Cisco
**Location:** India
**SMS provider:** Global Default
**Person being visited (email):** abc@cisco.com
**Reason being visited:** Personal



Your Guest Account Credentials

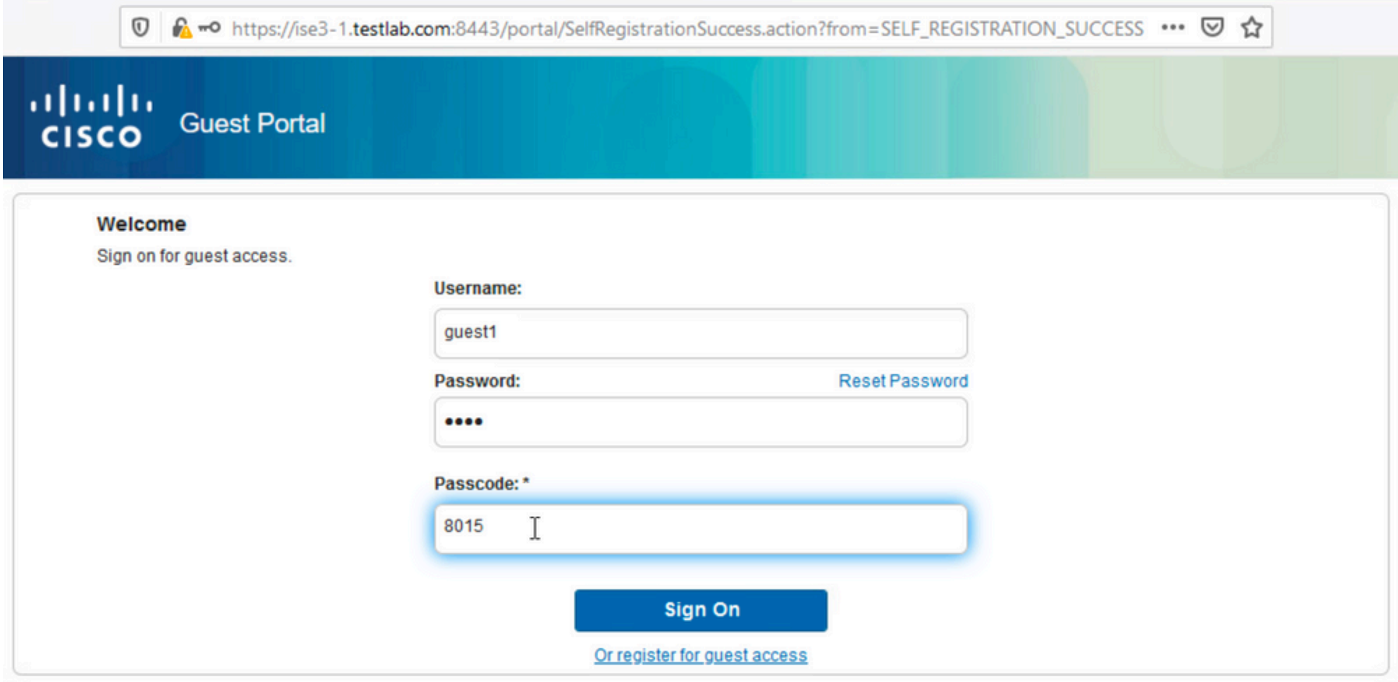
ise@testlab.com <ise@testlab.com>

To: Poonam Garg (poongarg)

Today at 9:47 AM

Hello Poonam,
Your guest account details:
Username: guest1
Password: 3154
First Name: Poonam
Last Name: Garg
Mobile Number:+910000000000
Valid From: 2020-11-07 09:43:50
Valid To: 2020-11-08 09:43:50
Person being visited: abc@cisco.com
Reason for visit: Personal

5.单击Sign On并提供凭据（如果在访客门户下配置，则可能需要其他访问密码；这是另一种只允许知道密码的用户登录的安全机制）。



https://ise3-1.testlab.com:8443/portal/SelfRegistrationSuccess.action?from=SELF_REGISTRATION_SUCCESS

Welcome

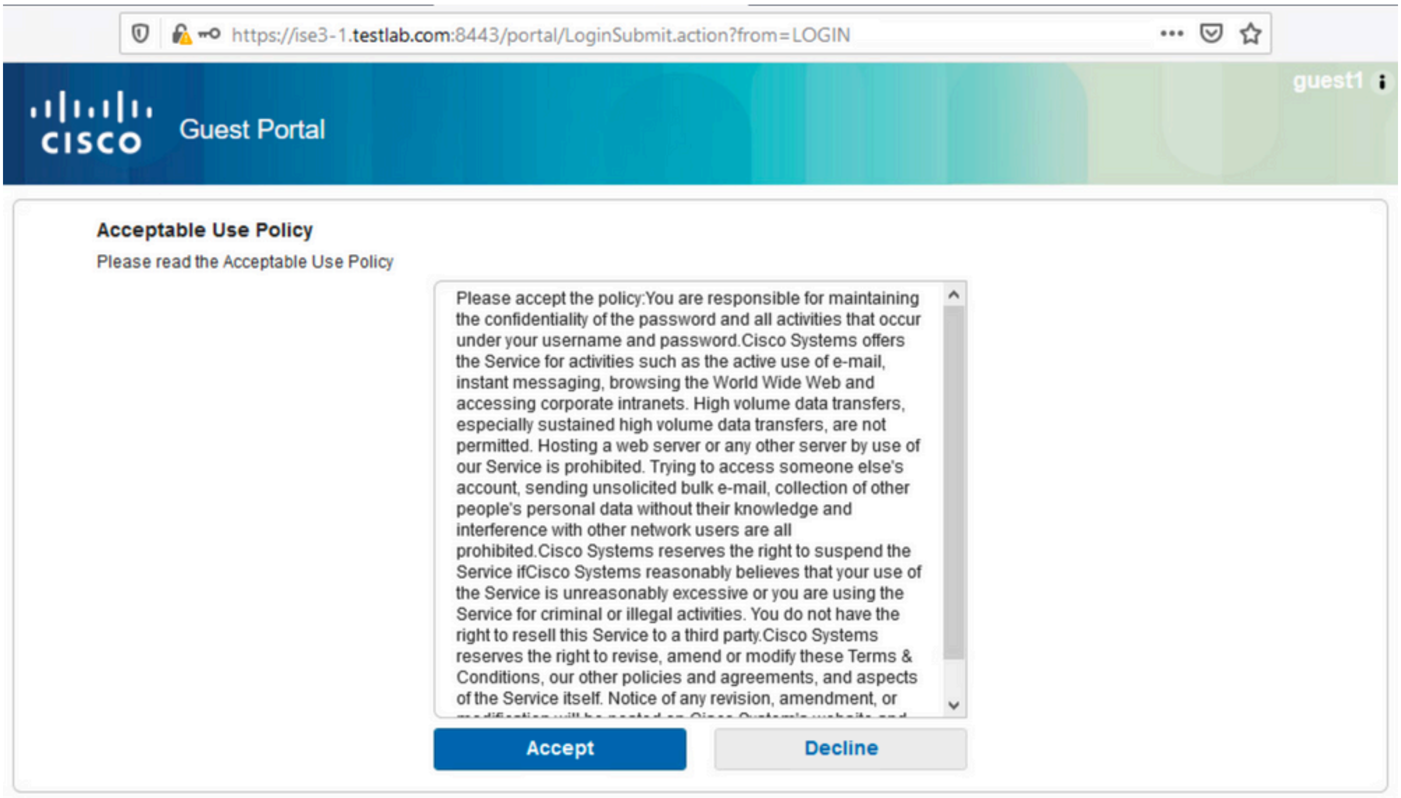
Sign on for guest access.

Username: guest1

Password: ••••

Passcode: * 8015

6.成功后，可以提供一个可选的使用策略(AUP)（如果在访客门户下配置）。用户会看到更改密码选项，并且还可以显示登录后横幅（在访客门户下也可配置）。

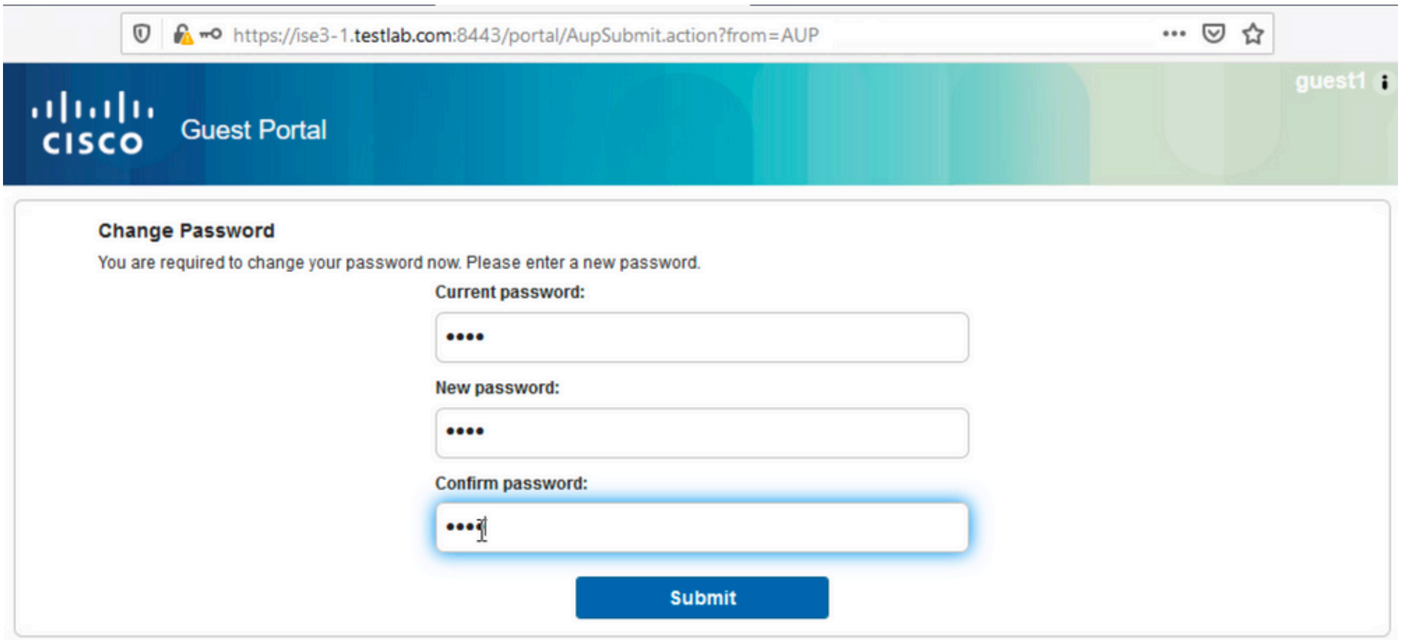


https://ise3-1.testlab.com:8443/portal/LoginSubmit.action?from=LOGIN

**Acceptable Use Policy**

Please read the Acceptable Use Policy

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited.Cisco Systems reserves the right to suspend the Service ifCisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party.Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or



https://ise3-1.testlab.com:8443/portal/AupSubmit.action?from=AUP

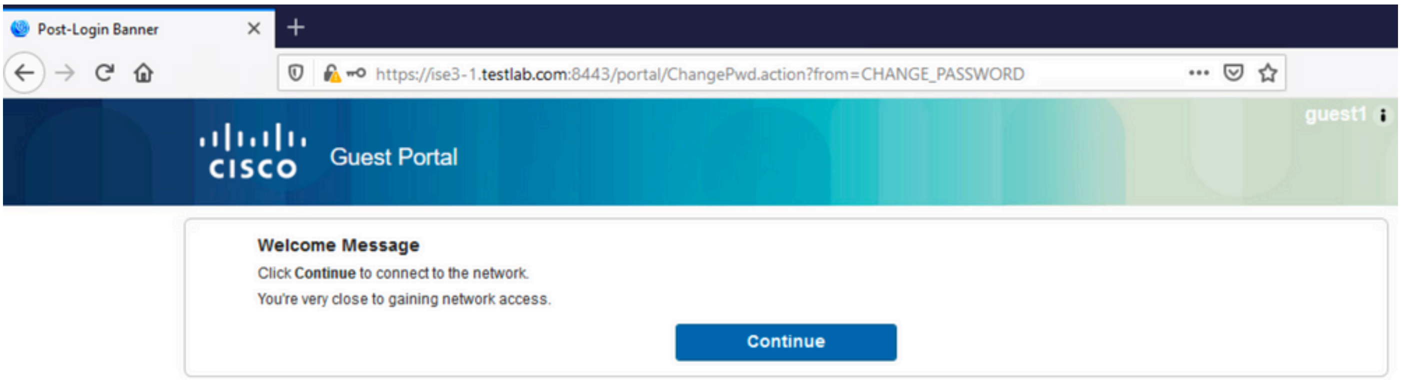
**Change Password**

You are required to change your password now. Please enter a new password.

Current password: ••••

New password: ••••

Confirm password: ••••



Post-Login Banner

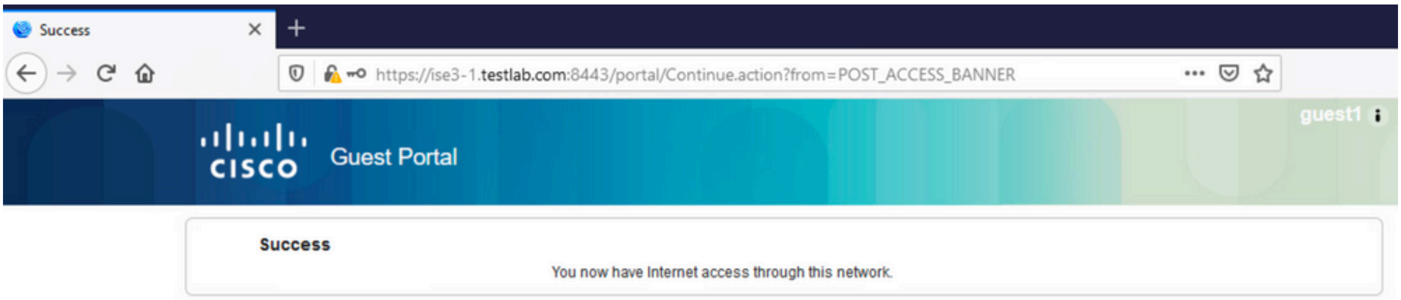
https://ise3-1.testlab.com:8443/portal/ChangePwd.action?from=CHANGE_PASSWORD

**Welcome Message**

Click **Continue** to connect to the network.

You're very close to gaining network access.

7.最后一页（登录后横幅）确认已授予访问权限：


Success
https://ise3-1.testlab.com:8443/portal/Continue.action?from=POST_ACCESS_BANNER
CISCO
Guest Portal
guest1

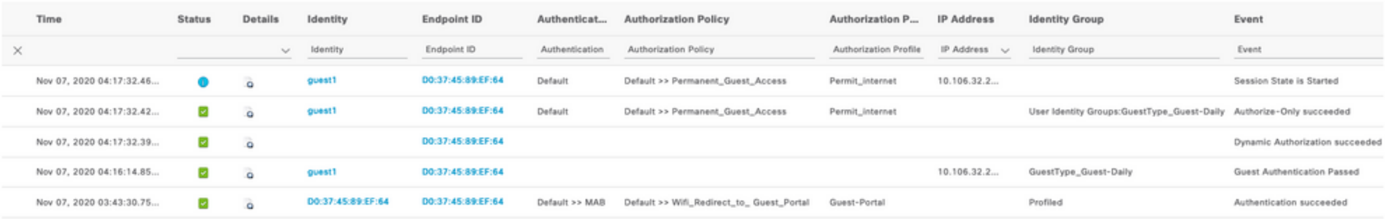
**Success**

You now have Internet access through this network.

# 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在Operations > RADIUS > Live Logs下显示这些日志，如图所示。

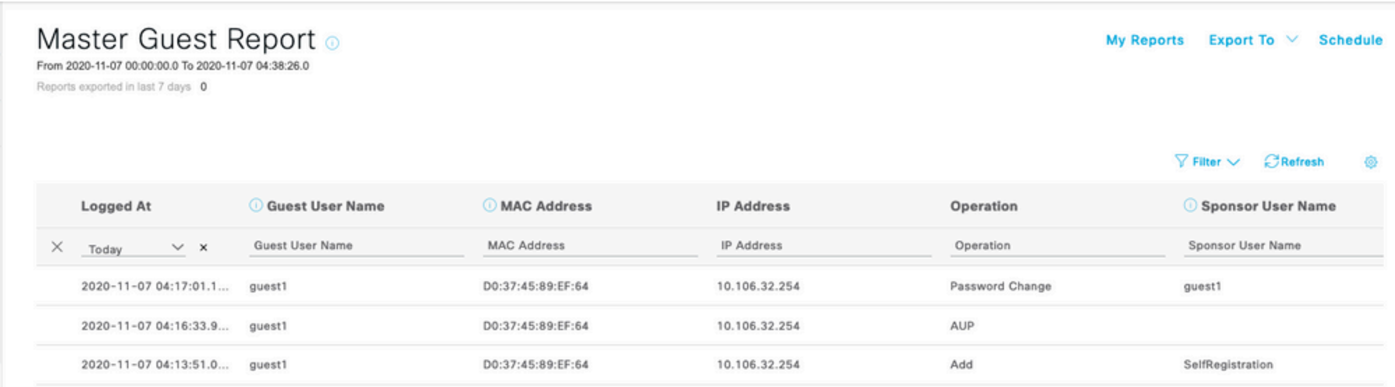


| Time | Status | Details | Identity | Endpoint ID | Authenticat... | Authorization Policy | Authorization P... | IP Address | Identity Group | Event |
|---|---|---|---|---|---|---|---|---|---|---|
| Nov 07, 2020 04:17:32.46... | ● | | guest1 | D0:37:45:89:EF:64 | Default | Default >> Permanent_Guest_Access | Permit_internet | 10.106.32.2... | | Session State is Started |
| Nov 07, 2020 04:17:32.42... | ✓ | | guest1 | D0:37:45:89:EF:64 | Default | Default >> Permanent_Guest_Access | Permit_internet | | User Identity Groups:GuestType_Guest-Daily | Authorize-Only succeeded |
| Nov 07, 2020 04:17:32.39... | ✓ | | | D0:37:45:89:EF:64 | | | | | | Dynamic Authorization succeeded |
| Nov 07, 2020 04:16:14.85... | ✓ | | guest1 | D0:37:45:89:EF:64 | | | | 10.106.32.2... | GuestType_Guest-Daily | Guest Authentication Passed |
| Nov 07, 2020 03:43:30.75... | ✓ | | D0:37:45:89:EF:64 | D0:37:45:89:EF:64 | Default >> MAB | Default >> Wifi_Redirect_to_ Guest_Portal | Guest-Portal | | Profiled | Authentication succeeded |

流程如下：

- 访客用户遇到第二个授权规则(Wifi_Redirect_to_Guest_Portal)并被重定向到访客门户(身份验证成功)。
- 访客被重定向以进行自助注册。成功登录（使用新创建的帐户）后，ISE发送CoA重新身份验证，由WLC确认(动态授权成功了)。
- WLC使用Authorize-Only属性执行重新身份验证，并返回ACL名称(Authorize-Only succeeded)。向访客提供正确的网络访问。

报告(Operations > Reports > Guest > Master Guest Report)还确认：



Master Guest Report

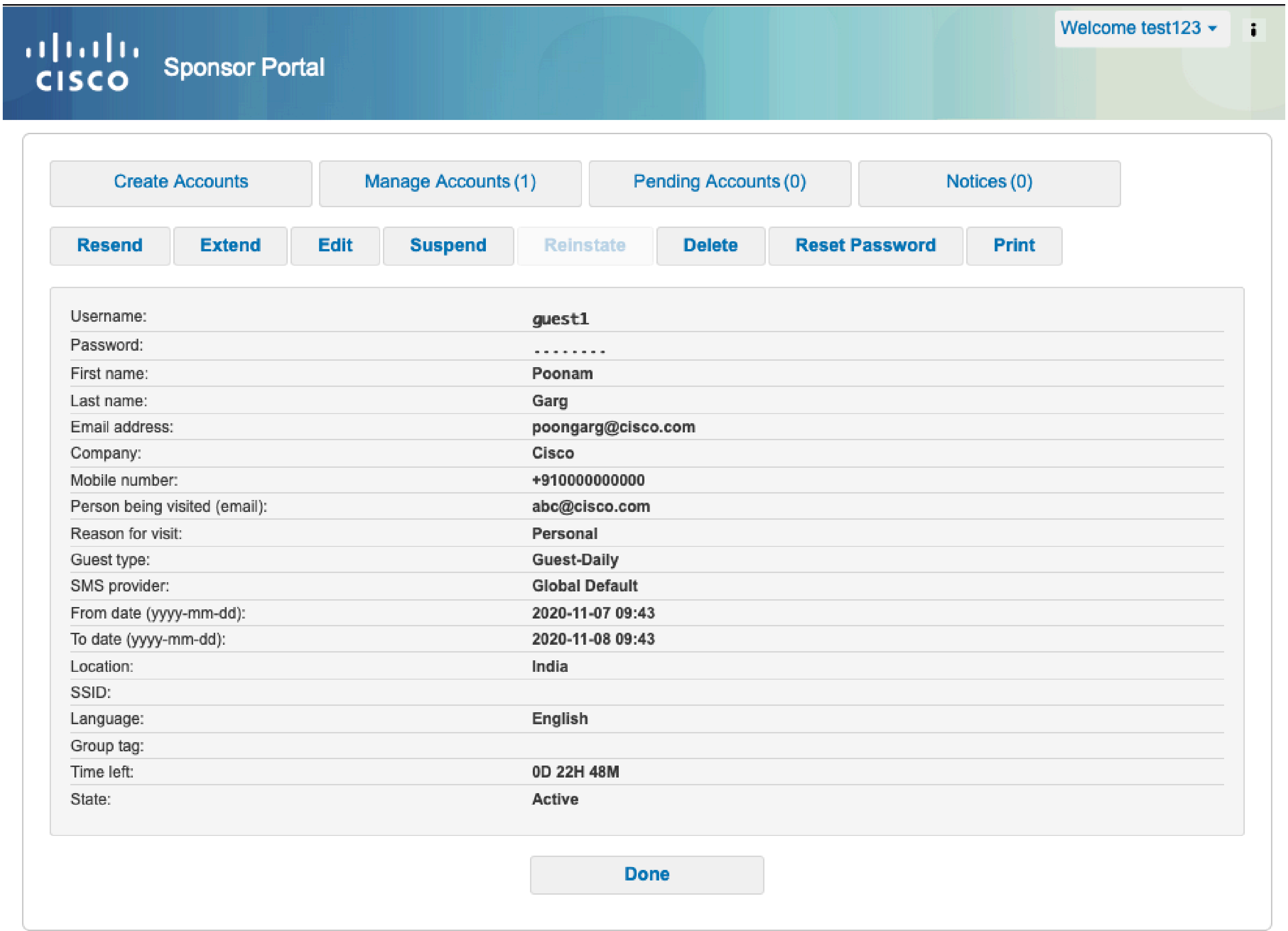
From 2020-11-07 00:00:00.0 To 2020-11-07 04:38:26.0

Reports exported in last 7 days 0

| Logged At | Guest User Name | MAC Address | IP Address | Operation | Sponsor User Name |
|---|---|---|---|---|---|
| 2020-11-07 04:17:01.1... | guest1 | D0:37:45:89:EF:64 | 10.106.32.254 | Password Change | guest1 |
| 2020-11-07 04:16:33.9... | guest1 | D0:37:45:89:EF:64 | 10.106.32.254 | AUP | |
| 2020-11-07 04:13:51.0... | guest1 | D0:37:45:89:EF:64 | 10.106.32.254 | Add | SelfRegistration |

保证人用户（具有正确权限）可以验证访客用户的当前状态。

此示例确认已创建帐户，且用户已登录到门户：



| | |
|---|---|
| Username: | guest1 |
| Password: | ........ |
| First name: | Poonam |
| Last name: | Garg |
| Email address: | poongarg@cisco.com |
| Company: | Cisco |
| Mobile number: | +910000000000 |
| Person being visited (email): | abc@cisco.com |
| Reason for visit: | Personal |
| Guest type: | Guest-Daily |
| SMS provider: | Global Default |
| From date (yyyy-mm-dd): | 2020-11-07 09:43 |
| To date (yyyy-mm-dd): | 2020-11-08 09:43 |
| Location: | India |
| SSID: | |
| Language: | English |
| Group tag: | |
| Time left: | 0D 22H 48M |
| State: | Active |

# 可选配置

对于此流程的每个阶段，可以配置不同的选项。所有这一切都是根据访客门户在Work Centers > Guest Access > Portals & Components > Guest Portals > Portal Name > Edit > Portal Behavior and Flow Settings上配置的。更重要的设置包括：

## 自助注册设置

- 访客类型 — 描述帐户处于活动状态的时间、密码到期选项、登录时间和选项（这是时间配置文件和访客角色的混合）
- 注册码 — 如果启用，则只允许知道密码的用户自行注册（必须在创建帐户时提供密码）
- AUP — 在自行注册期间接受使用策略
- 发起人批准/激活访客帐户的要求。

## 登录访客设置

- 访问代码 — 如果启用，则只允许知道密码的访客用户登录。
- AUP — 在自行注册期间接受使用策略。
- 密码更改选项。

### 设备注册设置

- 默认情况下，设备会自动注册。

### 访客设备合规性设置

- 允许在流内进行安全评估。

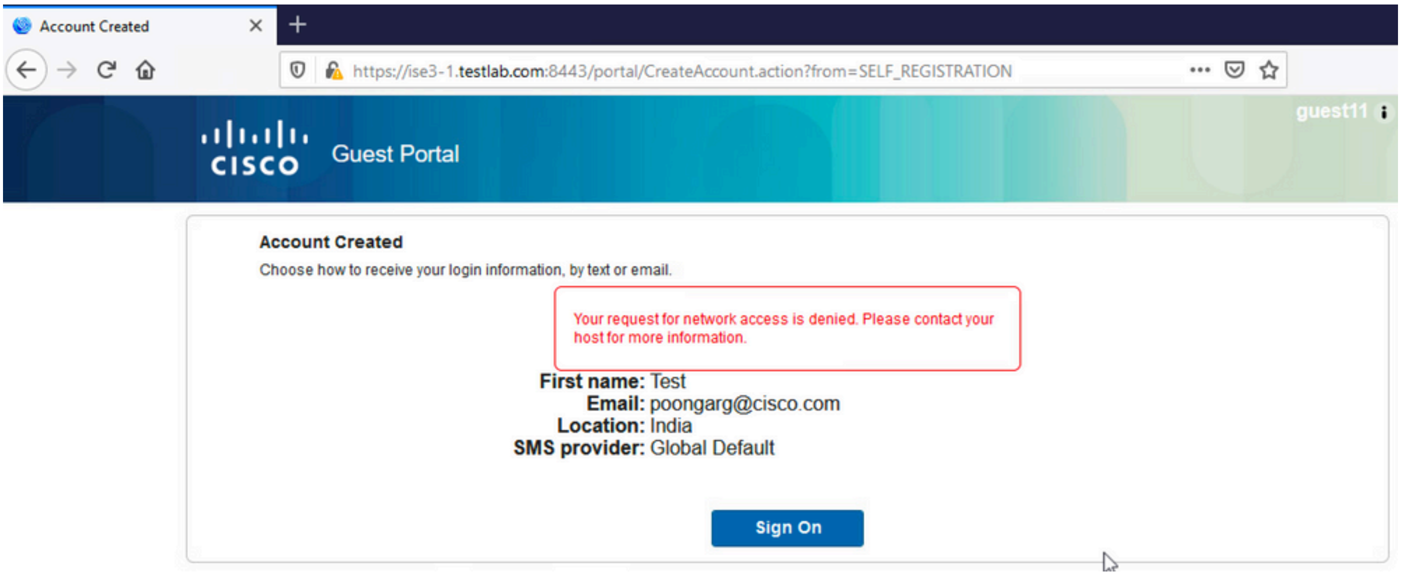
### BYOD设置

- 允许将门户用作访客的企业用户注册其个人设备。

## 发起人批准的帐户

如果在Registration Form Settings下选择了Require guests to be approved选项，则访客创建的帐户必须由发起人批准。此功能可以使用电子邮件向发起人发送通知（用于访客帐户审批）：

如果简单邮件传输协议(SMTP)服务器配置错误，则不会创建帐户：


Account Created
https://ise3-1.testlab.com:8443/portal/CreateAccount.action?from=SELF_REGISTRATION
guest11
cisco
Guest Portal

Account Created

Choose how to receive your login information, by text or email.

Your request for network access is denied. Please contact your host for more information.

**First name:** Test
**Email:** poongarg@cisco.com
**Location:** India
**SMS provider:** Global Default

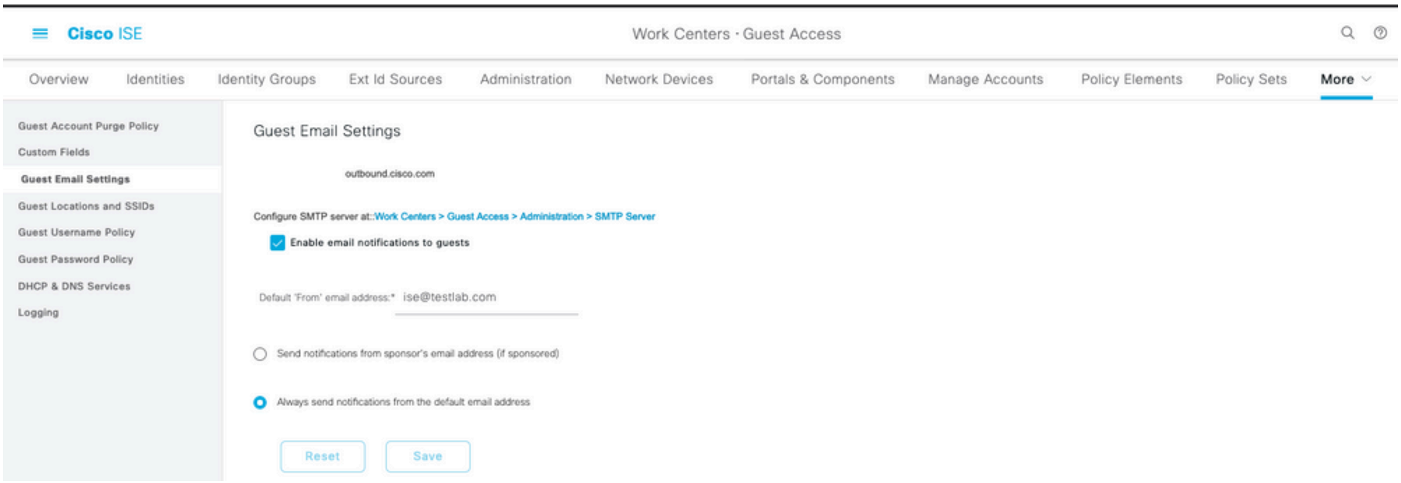
来自guest.log的日志确认，由于SMTP服务器配置错误，向发起人邮件发送批准通知存在问题：

<#root>

```
2020-11-07 07:16:38,547 ERROR [GUEST_ACCESS_SMTP_RETRY_THREAD][] cpm.guestaccess.apiservices.util.SmtpMs
javax.mail.MessagingException: Could not connect to SMTP host: outbound.cicso.com, port: 25, response: 4

2020-11-07 07:16:38,547 ERROR [https-jsse-nio-10.106.32.25-8443-exec-1][] cpm.guestaccess.apiservices.no
com.cisco.cpm.guestaccess.exception.GuestAccessSystemException: com.cisco.cpm.guestaccess.exception.Gues
```

当您拥有正确的电子邮件和SMTP服务器配置时，帐户创建如下：



Guest Email Settings

outbound.cisco.com

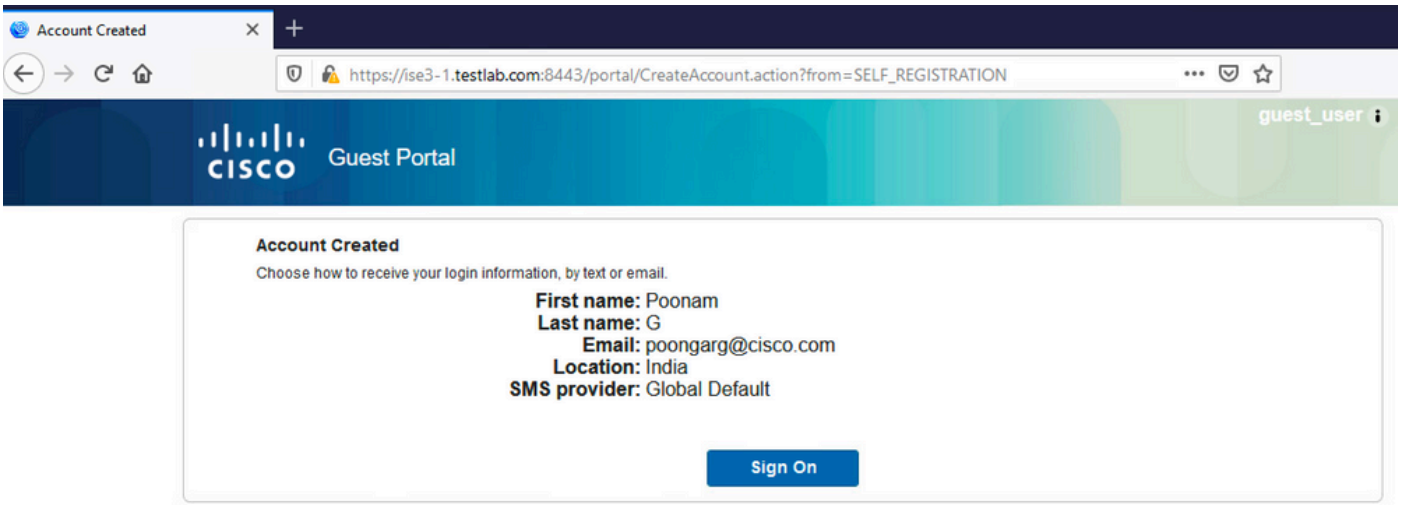
Configure SMTP server at::Work Centers > Guest Access > Administration > SMTP Server

☑ Enable email notifications to guests

Default 'From' email address:* ise@testlab.com

○ Send notifications from sponsor's email address (if sponsored)

● Always send notifications from the default email address



https://ise3-1.testlab.com:8443/portal/CreateAccount.action?from=SELF_REGISTRATION

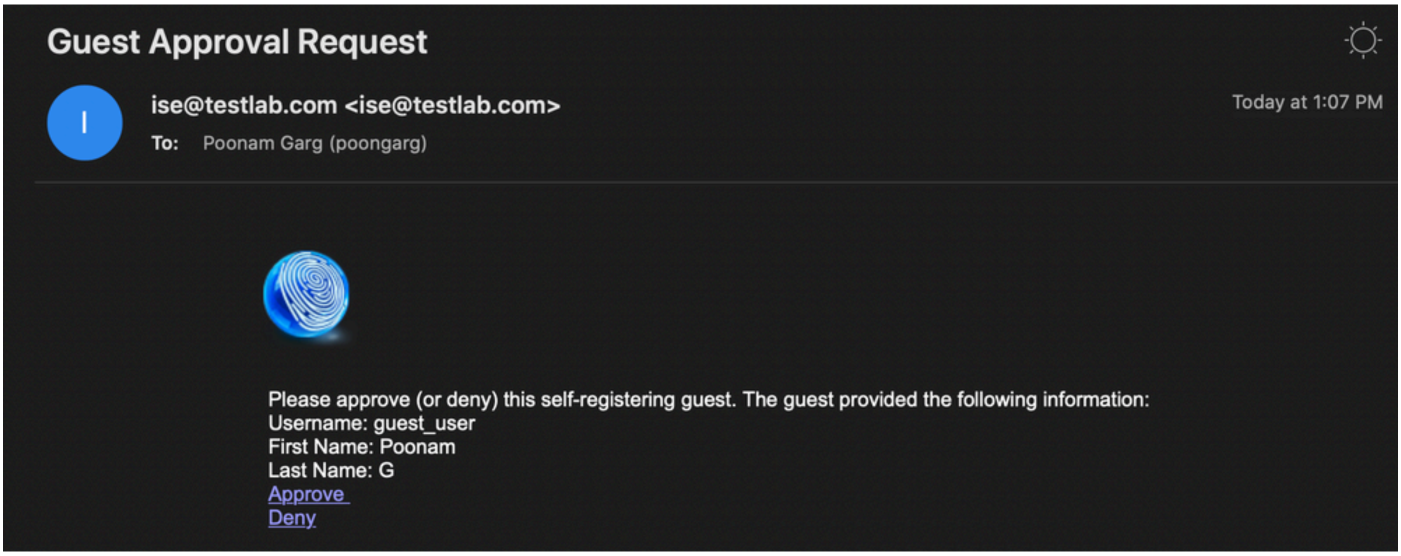
**Account Created**

Choose how to receive your login information, by text or email.

**First name:** Poonam
**Last name:** G
**Email:** poongarg@cisco.com
**Location:** India
**SMS provider:** Global Default

启用要求访客获得批准选项后，用户名和密码字段将自动从Include this information on the Self-Registration Success page部分中删除。这就是为什么在需要发起人批准时，访客用户的凭证默认不会显示在显示帐户已创建信息的网页上。相反，它们必须通过短信服务(SMS)或电子邮件传送。此选项必须在Send credential notification upon approval using部分中启用（标记电子邮件/SMS）。

通知电邮将发送给发起人：

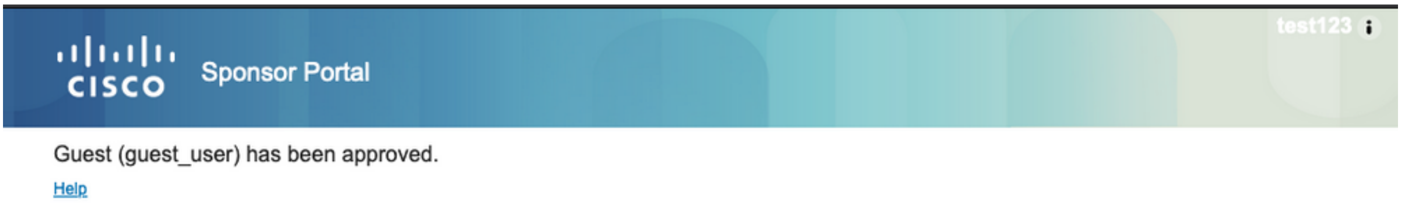


Guest Approval Request

ise@testlab.com <ise@testlab.com>
To: Poonam Garg (poongarg)
Today at 1:07 PM

Please approve (or deny) this self-registering guest. The guest provided the following information:
Username: guest_user
First Name: Poonam
Last Name: G
Approve
Deny

发起人点击Approval（审批）链接并登录发起人门户，该帐户已获批准：



Guest (guest_user) has been approved.

从此时起，允许访客用户登录（使用通过电邮或SMS接收的凭证）。

总之，此流程中使用三个邮件地址：

- 通知“发件人”地址。这是静态定义的，也可以从保证人帐户中定义，并用作保证人通知（用于审批）和访客凭证详细信息的“发件人”地址。这在工作中心(Work Centers)>访客接入(Guest Access)>设置(Settings)>访客邮件设置(Guest Email Settings)下配置。

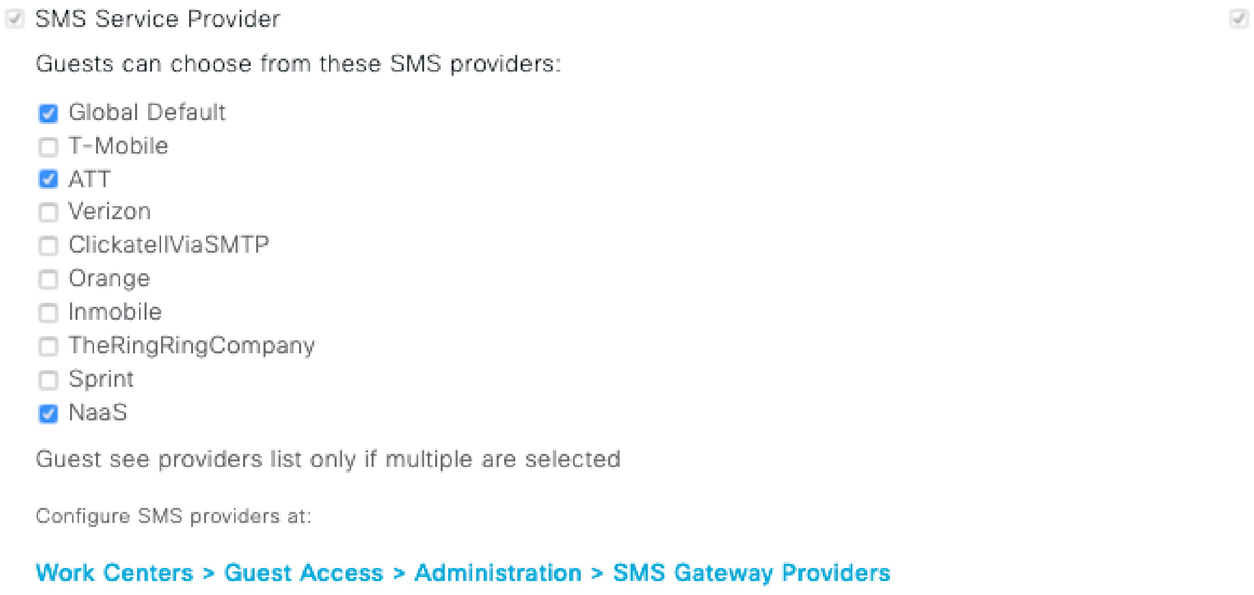
- 通知“收件人”地址。用于通知发起人它已收到要审批的帐户。这在Guest Portal中的Work Centers > Guest Access > Guest Portals > Portals and Components > Portal Name > Registeration Form Settings > Require guests to be approved > Email approval request to下配置。

- 访客“收件人”地址。此功能由访客用户在注册期间提供。如果选中Send credential notification upon approval using Email，则会向访客发送包含凭证详细信息（用户名和密码）的邮件。

# 通过短信传送凭证

访客凭证也可以通过SMS传送。必须配置以下选项：

1. 在Registration Form Settings（注册表单设置）下选择SMS服务提供商：



☑ SMS Service Provider

Guests can choose from these SMS providers:

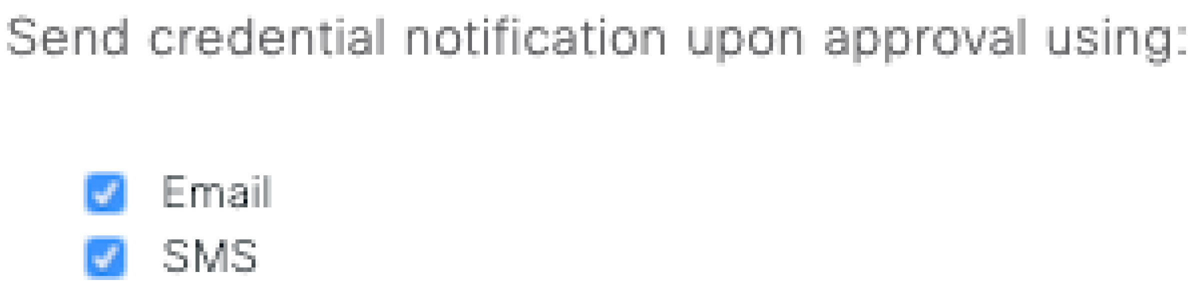
☑ Global Default
□ T-Mobile
☑ ATT
□ Verizon
□ ClickatellViaSMTP
□ Orange
□ Inmobile
□ TheRingRingCompany
□ Sprint
☑ NaaS

Guest see providers list only if multiple are selected

Configure SMS providers at:

Work Centers > Guest Access > Administration > SMS Gateway Providers

2. 选中Send credential notification upon approval using: SMS复选框。

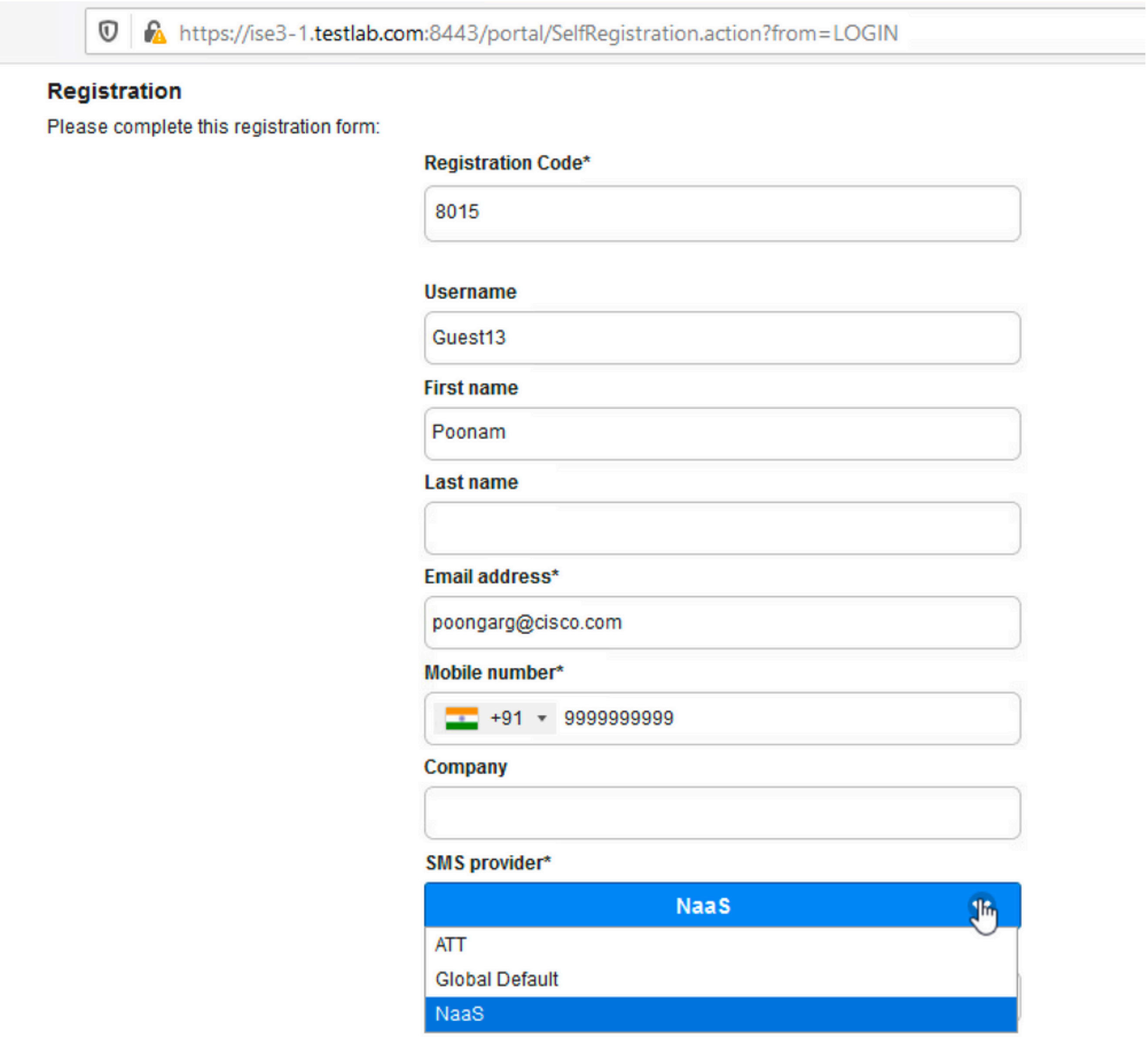


Send credential notification upon approval using:

☑ Email

☑ SMS

3. 然后，访客用户在创建帐户时需要选择可用的提供商：



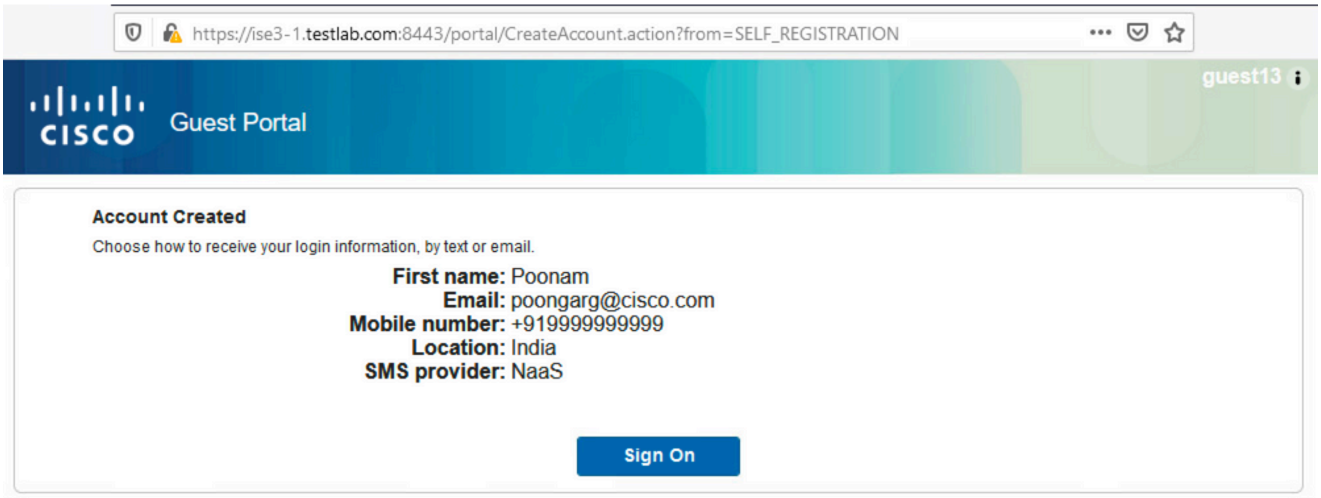
https://ise3-1.testlab.com:8443/portal/SelfRegistration.action?from=LOGIN

**Registration**

Please complete this registration form:

| | |
|---|---|
| Registration Code* | 8015 |
| Username | Guest13 |
| First name | Poonam |
| Last name | |
| Email address* | poongarg@cisco.com |
| Mobile number* | +91 9999999999 |
| Company | |
| SMS provider* | NaaS |

4. SMS与所选提供商和电话号码一起发送：


https://ise3-1.testlab.com:8443/portal/CreateAccount.action?from=SELF_REGISTRATION
cisco
Guest Portal
guest13

**Account Created**

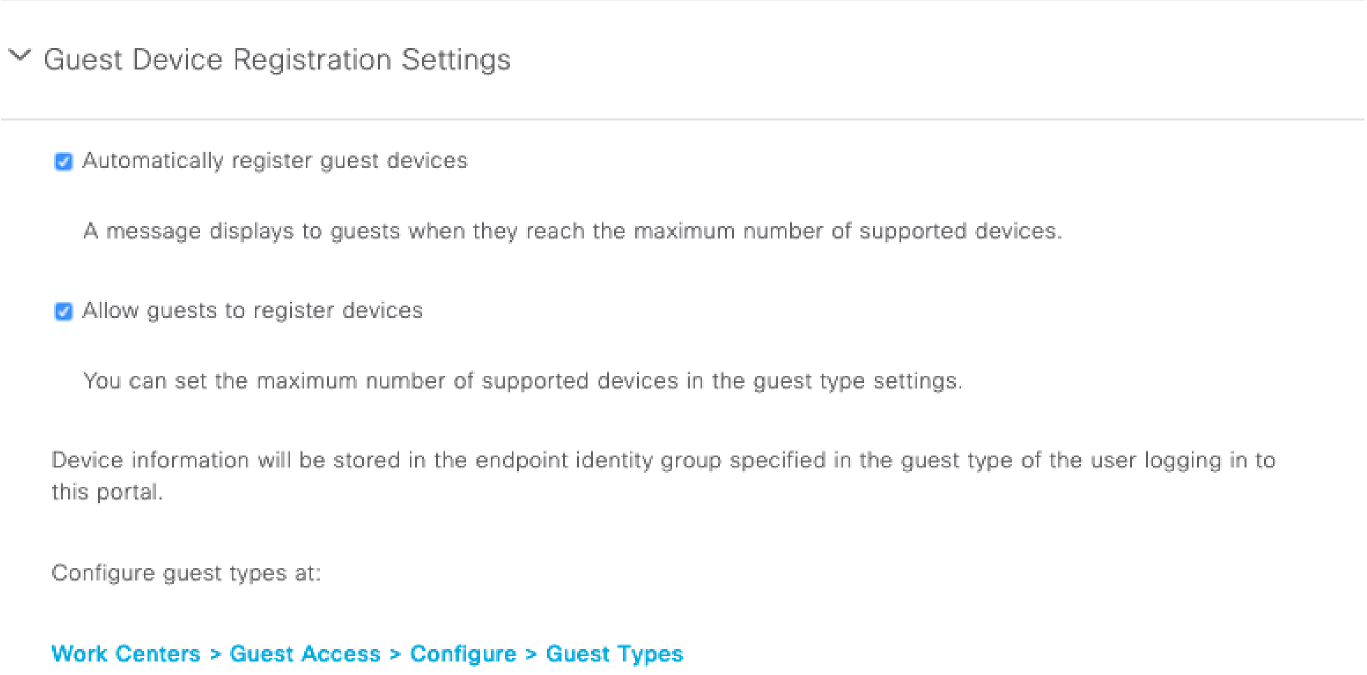
Choose how to receive your login information, by text or email.

**First name:** Poonam
**Email:** poongarg@cisco.com
**Mobile number:** +919999999999
**Location:** India
**SMS provider:** NaaS

5. 您可以在Administration > System > Settings > SMS Gateway下配置SMS提供程序。

# 设备注册

如果在访客用户登录并接受AUP后选择了Allow guests to register devices选项，则可以注册设备：



Guest Device Registration Settings

☑ Automatically register guest devices

A message displays to guests when they reach the maximum number of supported devices.

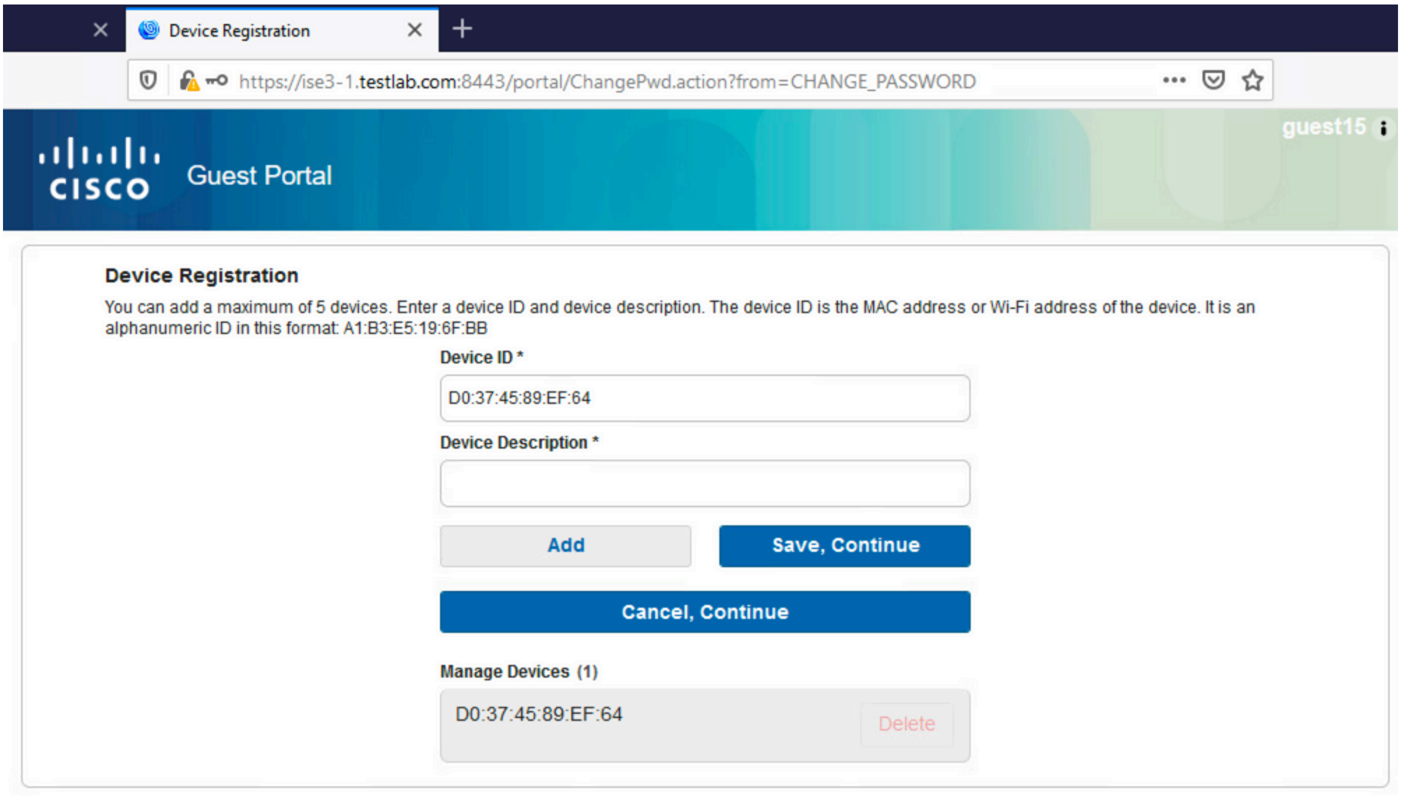
☑ Allow guests to register devices

You can set the maximum number of supported devices in the guest type settings.

Device information will be stored in the endpoint identity group specified in the guest type of the user logging in to this portal.

Configure guest types at:

Work Centers > Guest Access > Configure > Guest Types



Device Registration
https://ise3-1.testlab.com:8443/portal/ChangePwd.action?from=CHANGE_PASSWORD
guest15
CISCO
Guest Portal

**Device Registration**

You can add a maximum of 5 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

Device ID *: D0:37:45:89:EF:64

Device Description *:

Manage Devices (1)

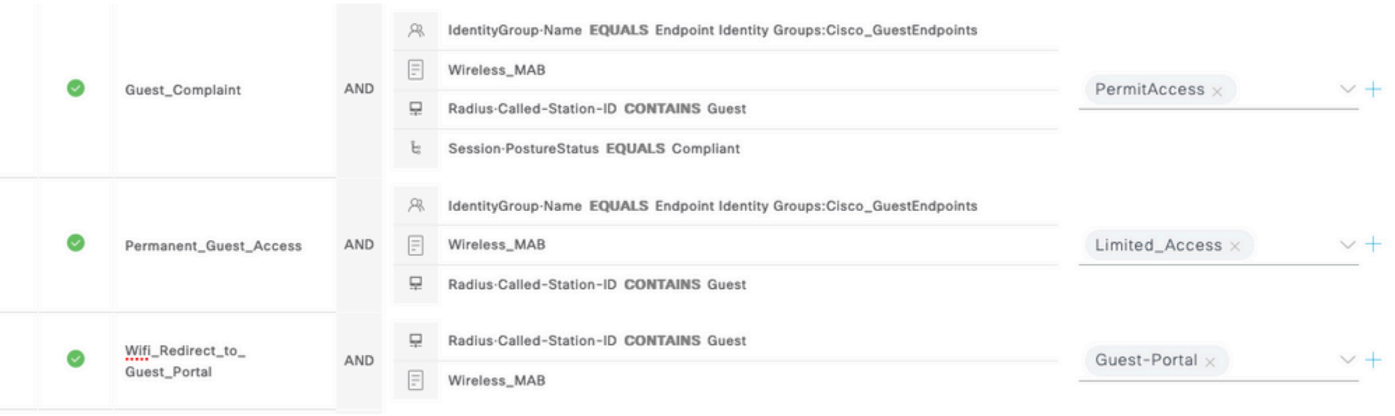
D0:37:45:89:EF:64

请注意，设备已自动添加（它位于Manage Devices列表中）。这是因为已选择Automatically register guest devices。

# 状态

如果选择了Require guest device compliance选项，则访客用户会在登录并接受AUP（以及可选地执行设备注册）后获得执行安全评估（NAC/Web代理）的代理。ISE处理客户端调配规则以确定必须调配哪个代理。然后，在站点上运行的代理执行安全评估（根据安全评估规则）并将结果发送到ISE，ISE会根据需要发送CoA重新身份验证以更改授权状态。

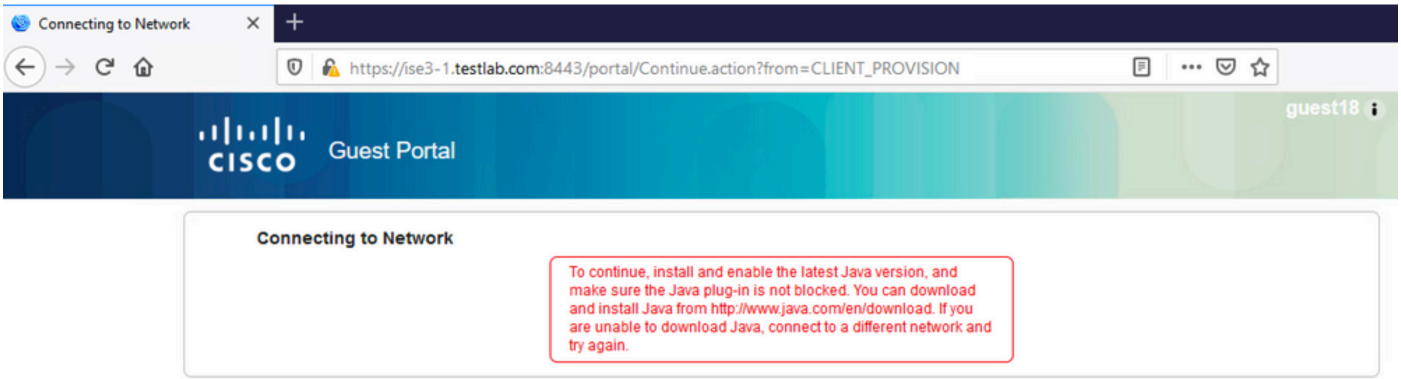
可能的授权规则可能如下所示：



| | | | | |
|---|---|---|---|---|
| ✓ | Guest_Complaint | AND | IdentityGroup·Name EQUALS Endpoint Identity Groups:Cisco_GuestEndpoints<br>Wireless_MAB<br>Radius·Called-Station-ID CONTAINS Guest<br>Session·PostureStatus EQUALS Compliant | PermitAccess |
| ✓ | Permanent_Guest_Access | AND | IdentityGroup·Name EQUALS Endpoint Identity Groups:Cisco_GuestEndpoints<br>Wireless_MAB<br>Radius·Called-Station-ID CONTAINS Guest | Limited_Access |
| ✓ | Wifi_Redirect_to_Guest_Portal | AND | Radius·Called-Station-ID CONTAINS Guest<br>Wireless_MAB | Guest-Portal |

第一个遇到Guest_Authenticate规则的新用户重定向到自助注册访客门户。用户自行注册并登录后，CoA会更改授权状态，用户将获得执行状况和补救的有限访问权限。只有在调配NAC代理且工作站符合要求后，CoA才会再次更改授权状态，以提供对Internet的访问。

安全状态的典型问题包括缺少正确的客户端调配规则：


Connecting to Network
https://ise3-1.testlab.com:8443/portal/Continue.action?from=CLIENT_PROVISION
CISCO
Guest Portal
guest18

Connecting to Network

To continue, install and enable the latest Java version, and make sure the Java plug-in is not blocked. You can download and install Java from http://www.java.com/en/download. If you are unable to download Java, connect to a different network and try again.

如果检查guest.log文件，也可以确认这一点：

<#root>

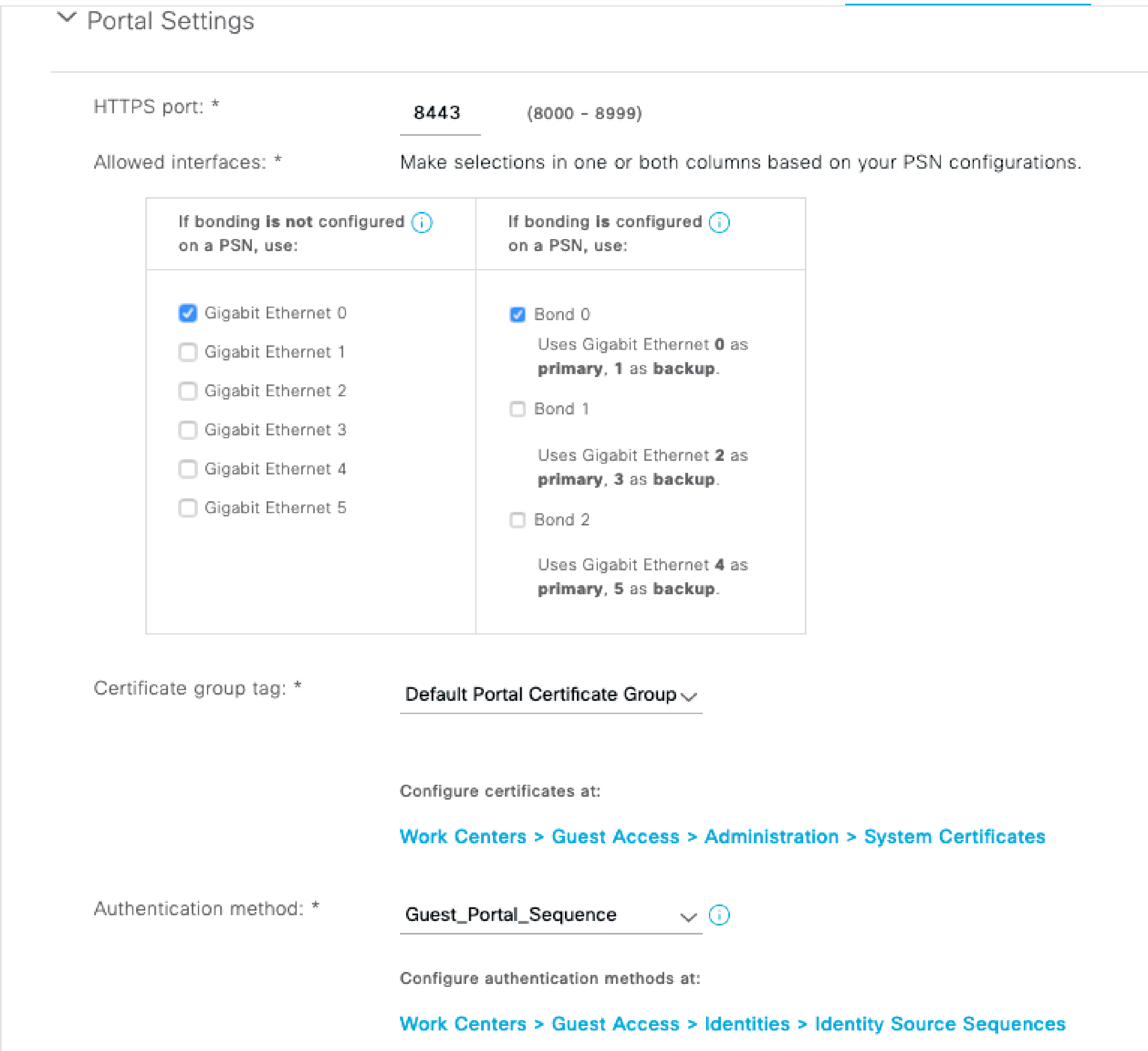
```
2020-11-09 09:23:32,157 ERROR [https-jsse-nio-10.106.32.25-8443-exec-7][] guestaccess.flowmanager.step.g
```

# 自带设备

如果选中Allow employees to use personal devices on the network选项，则使用此门户的企业用户可以通过BYOD流程并注册个人设备。对于访客用户，该设置不会改变任何内容。

“员工使用门户作为访客”是什么意思？

默认情况下，访客门户使用Guest_Portal_Sequence身份库进行配置：



Portal Settings

HTTPS port: * 8443 (8000 - 8999)

Allowed interfaces: * Make selections in one or both columns based on your PSN configurations.

| If bonding **is not** configured on a PSN, use: | If bonding **is** configured on a PSN, use: |
|---|---|
| ☑ Gigabit Ethernet 0<br>□ Gigabit Ethernet 1<br>□ Gigabit Ethernet 2<br>□ Gigabit Ethernet 3<br>□ Gigabit Ethernet 4<br>□ Gigabit Ethernet 5 | ☑ Bond 0<br>Uses Gigabit Ethernet **0** as **primary**, **1** as **backup**.<br>□ Bond 1<br>Uses Gigabit Ethernet **2** as **primary**, **3** as **backup**.<br>□ Bond 2<br>Uses Gigabit Ethernet **4** as **primary**, **5** as **backup**. |

Certificate group tag: * Default Portal Certificate Group

Configure certificates at:

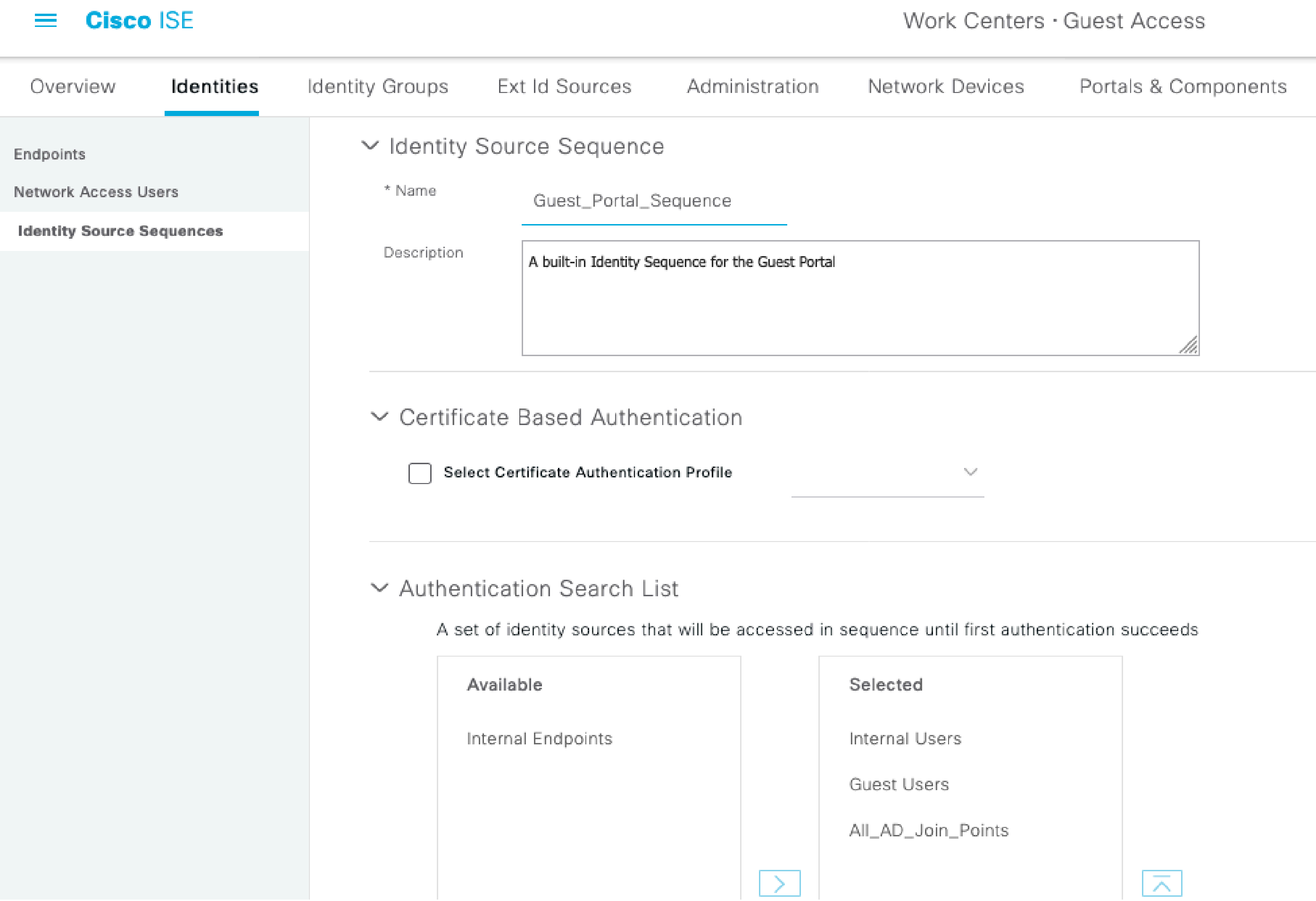
Work Centers > Guest Access > Administration > System Certificates

Authentication method: * Guest_Portal_Sequence

Configure authentication methods at:

Work Centers > Guest Access > Identities > Identity Source Sequences

这是内部存储序列，先尝试内部用户（在访客用户之前），然后尝试AD凭证。由于高级设置是在选定的身份库无法访问进行身份验证时继续进入序列中的下一个存储，因此具有内部凭证或AD凭证的员工可以登录门户。



Identity Source Sequence

* Name: Guest_Portal_Sequence

Description: A built-in Identity Sequence for the Guest Portal

Certificate Based Authentication

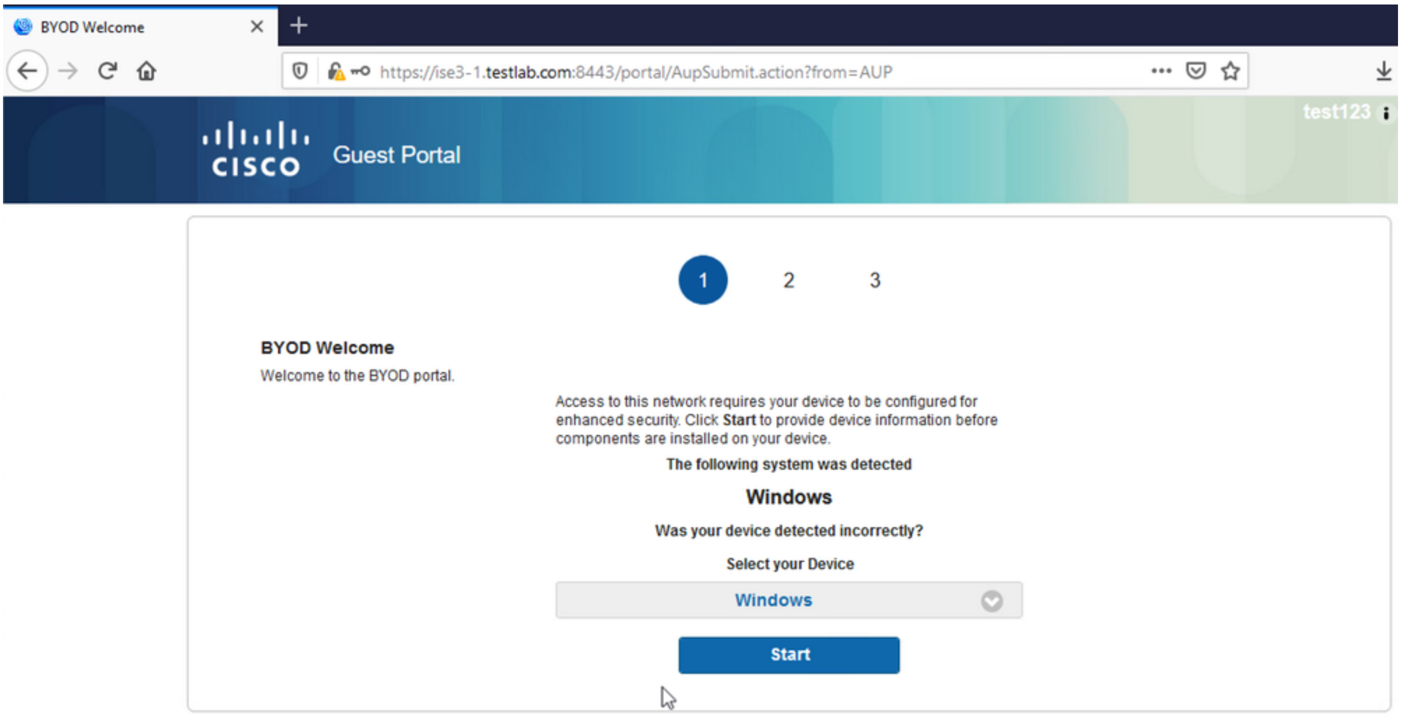
□ Select Certificate Authentication Profile

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

| Available | Selected |
|---|---|
| Internal Endpoints | Internal Users |
| | Guest Users |
| | All_AD_Join_Points |

在此阶段，在访客门户上，用户提供在内部用户存储或Active Directory中定义的凭证，并进行BYOD重定向：



BYOD Welcome
https://ise3-1.testlab.com:8443/portal/AupSubmit.action?from=AUP
cisco
Guest Portal
test123
1
2
3

BYOD Welcome

Welcome to the BYOD portal.

Access to this network requires your device to be configured for enhanced security. Click **Start** to provide device information before components are installed on your device.

The following system was detected

Windows

Was your device detected incorrectly?

Select your Device

Windows

这样，企业用户可以针对个人设备执行BYOD。

当提供访客用户凭证而不是内部用户/AD凭证时，继续正常流程（无BYOD）。

## VLAN更改

它允许您运行activeX或Java小程序，从而触发DHCP释放和更新。当CoA触发终端的VLAN更改时，需要执行此操作。使用MAB时，终端不知道VLAN发生更改。一种可能的解决方案是使用NAC代理更改VLAN（DHCP发布/更新）。另一种方法是通过网页上返回的小程序请求新的IP地址。可以配置版本/CoA/续订之间的延迟。移动设备不支持此选项。

## 相关信息

- 思科ISE上的状态服务配置指南
- 带身份服务引擎的无线BYOD
- BYOD的ISE SCEP支持配置示例
- WLC 和 ISE 上的集中式 Web 身份验证配置示例
- 在带有ISE的WLC上使用FlexConnect AP进行集中式Web身份验证的配置示例
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。