配置ISE自註冊訪客門戶

目錄

簡介

本文檔介紹如何配置ISE自註冊訪客門戶功能並對其進行故障排除。

必要條件

需求

思科建議您瞭解ISE配置和以下主題的基本知識：

- ISE部署和訪客流量
- 無線區域網路控制器(WLC)的組態

採用元件

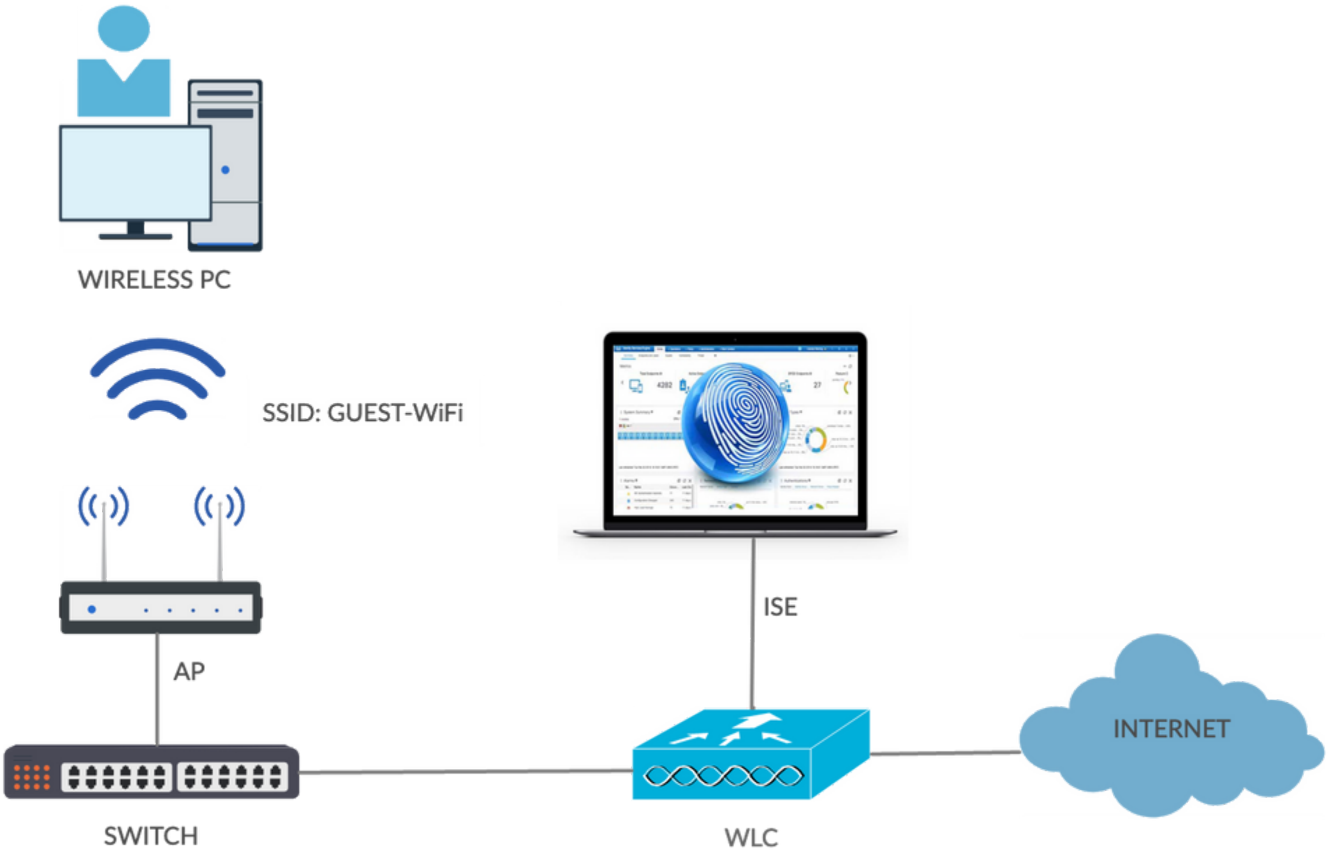
自助註冊訪客門戶，允許訪客使用者與員工一起自助註冊，以使用他們的AD憑證來獲得網路資源的訪問許可權。此門戶允許您配置和自定義多個功能。

本文中的資訊係根據以下軟體和硬體版本：

- Microsoft Windows 10 Pro
- Cisco WLC 5508（8.5.135.0版）
- ISE軟體版本3.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

拓撲和流



此案例為訪客使用者執行自助註冊時提供了多個可用選項。

以下是一般流程：

步驟 1.訪客使用者關聯到服務集識別符號(SSID)：訪客WiFi。這是一個開放式網路，使用ISE進行MAC過濾以進行身份驗證。此身份驗證匹配ISE上的第二個授權規則，並且授權配置檔案重定向到訪客自行註冊門戶。ISE返回包含兩個cisco-av-pair的RADIUS Access-Accept:

- url-redirect-acl(必須重新導向哪些流量，以及在WLC本機上定義的存取控制清單(ACL)的名稱)
- url-redirect（將流量重定向到ISE的位置）

步驟 2.訪客使用者重定向到ISE。使用者按一下Register for Guest Access，而不是提供憑證以便登入。 系統會將使用者重新導向至可建立該帳戶的頁面。可以啟用可選的秘密註冊碼，以將自註冊許可權限製為知道該秘密值的人員。建立帳戶後，將為使用者提供憑證（使用者名稱和密碼）並使用這些憑證登入。

步驟 3.ISE向WLC傳送RADIUS授權變更(CoA)重新驗證。當使用者傳送具有Authorize-Only屬性的RADIUS存取要求時，WLC會重新驗證使用者。ISE通過WLC本地定義的Access-Accept和Airespace ACL進行響應，僅提供對Internet的訪問（訪客使用者的最終訪問取決於授權策略）。

注意：可擴展身份驗證協定(EAP)會話，ISE必須傳送CoA Terminate以觸發重新身份驗證，因為EAP會話位於請求方和ISE之間。但是對於MAB（MAC過濾），CoA Reauthenticate就足夠了；不需要取消關聯/取消驗證無線客戶端。

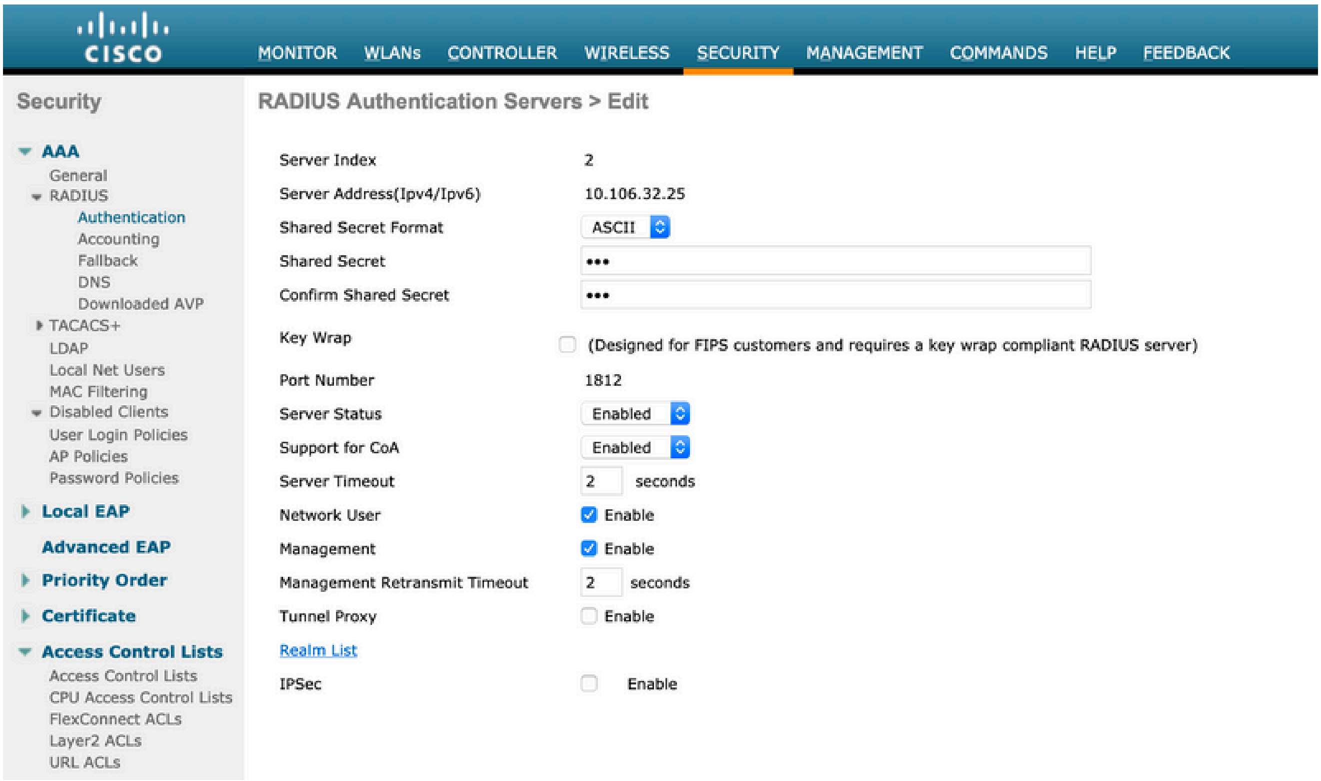
步驟 4.訪客使用者具有所需的網路訪問許可權。

可以啟用（稍後討論）多種其他功能，如狀態和自帶裝置(BYOD)。

設定

WLC

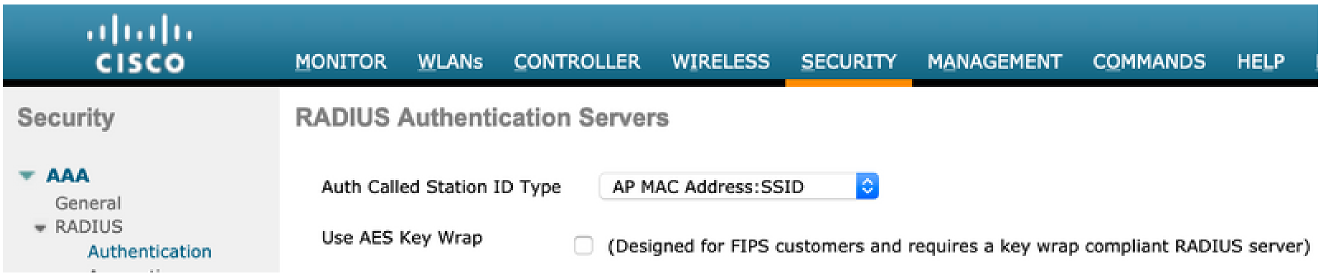
1. 新增用於身份驗證和記帳的新RADIUS伺服器。導覽至Security > AAA > Radius > Authentication以啟用RADIUS CoA(RFC 3576)。



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

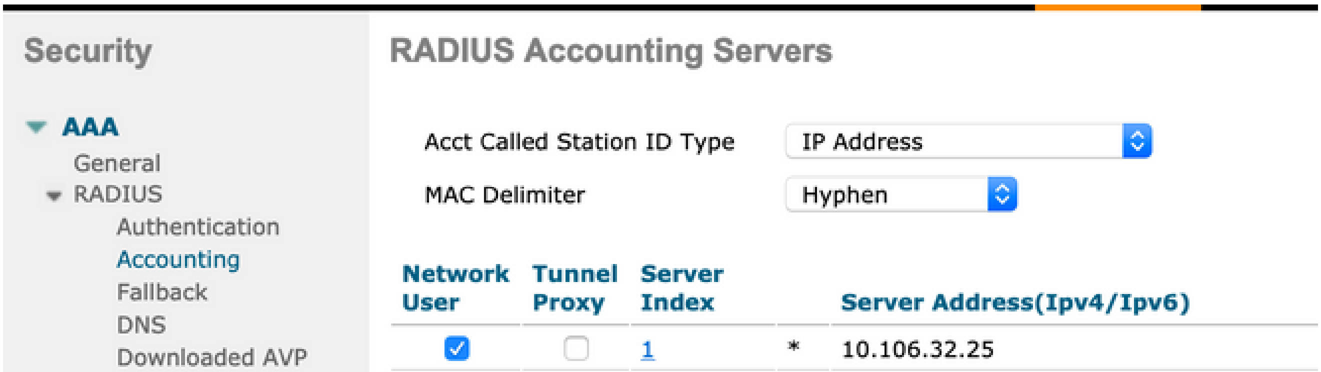
Accounting有類似的配置。建議在Called Station ID屬性中配置WLC以傳送SSID，這允許ISE根據SSID配置靈活的規則：



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

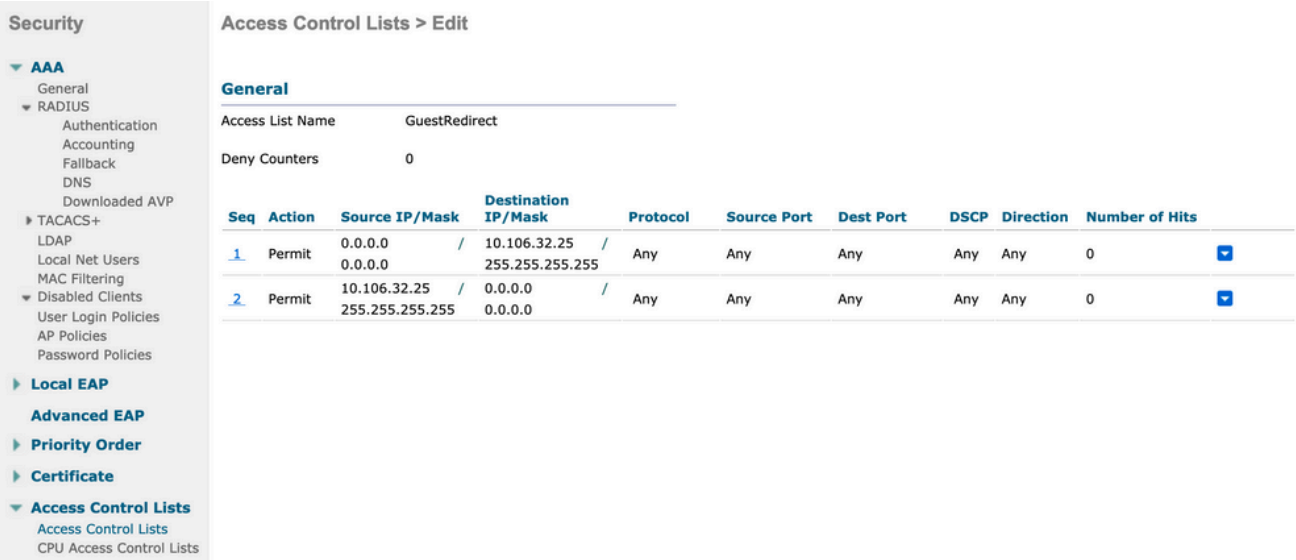
Network User	Tunnel Proxy	Server Index		Server Address(Ipv4/Ipv6)
☑	☐	1	*	10.106.32.25

2. 在WLANs頁籤下，建立無線LAN(WLAN)訪客WiFi並配置正確的介面。使用MAC過濾將Layer2 security設定為None。在安全/身份驗證、授權和記帳(AAA)伺服器中，選擇身份驗證和記帳的ISE IP地址。在Advanced頁籤上，啟用AAA Override，並將網路准入控制(NAC)狀態設定為ISE NAC（CoA支援）。

3. 導覽至Security > Access Control Lists > Access Control Lists，然後建立兩個存取清單：

   - GuestRedirect，允許不得重定向的流量並重定向所有其他流量
   - Internet，公司網路被拒絕，所有其他網路都允許

以下是GuestRedirect ACL的範例（需要從重新導向中排除ISE來往流量）：



Access Control Lists > Edit

General

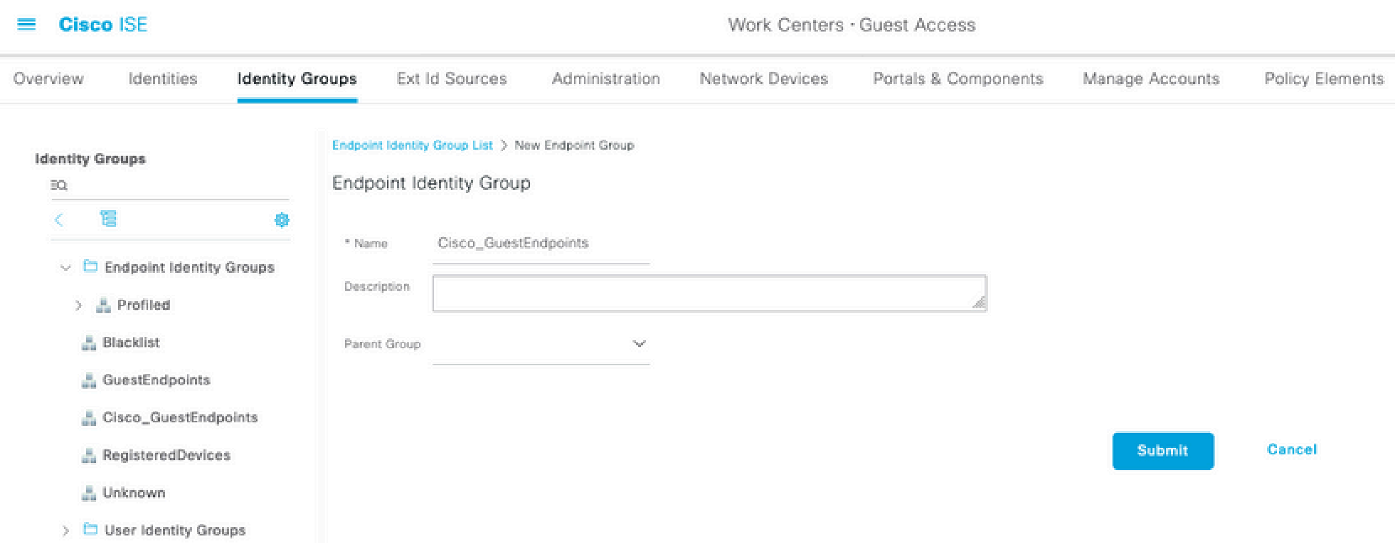
Access List Name: GuestRedirect

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. 從工作中心>訪客接入>網路裝置將WLC新增為網路接入裝置。
2. 建立端點身份組。導航至工作中心(Work Centers)>訪客訪問(Guest Access)>身份組(Identity Groups)>終端身份組(Endpoint Identity Groups)。



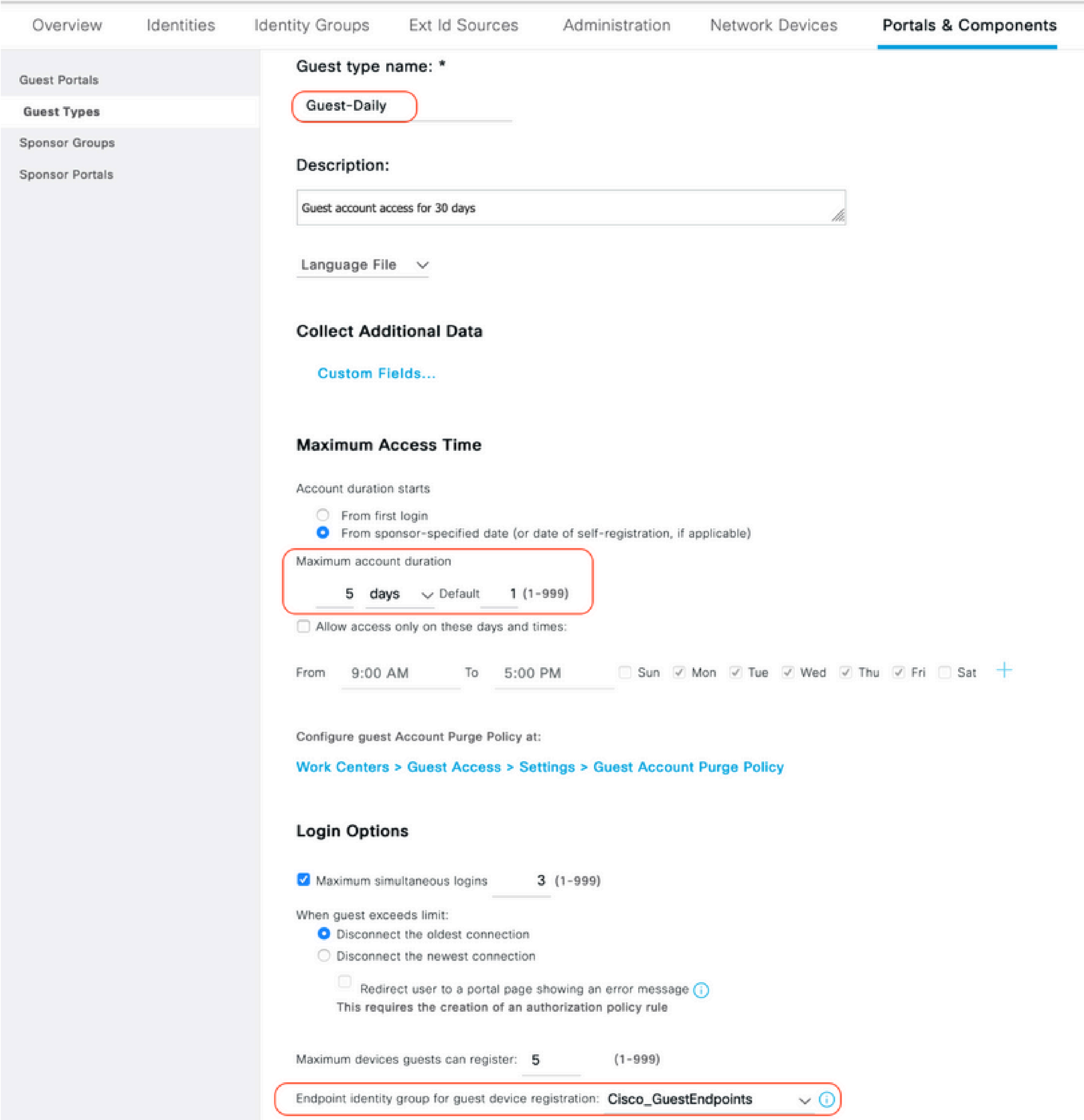
Endpoint Identity Group

* Name: Cisco_GuestEndpoints

Description:

Parent Group:

3.導航到工作中心>訪客接入>門戶和元件>訪客型別，建立訪客型別。請參閱在此新訪客型別下之前建立的終端身份組並儲存。



Guest type name: *

Guest-Daily

Description:

Guest account access for 30 days

Language File

Collect Additional Data

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

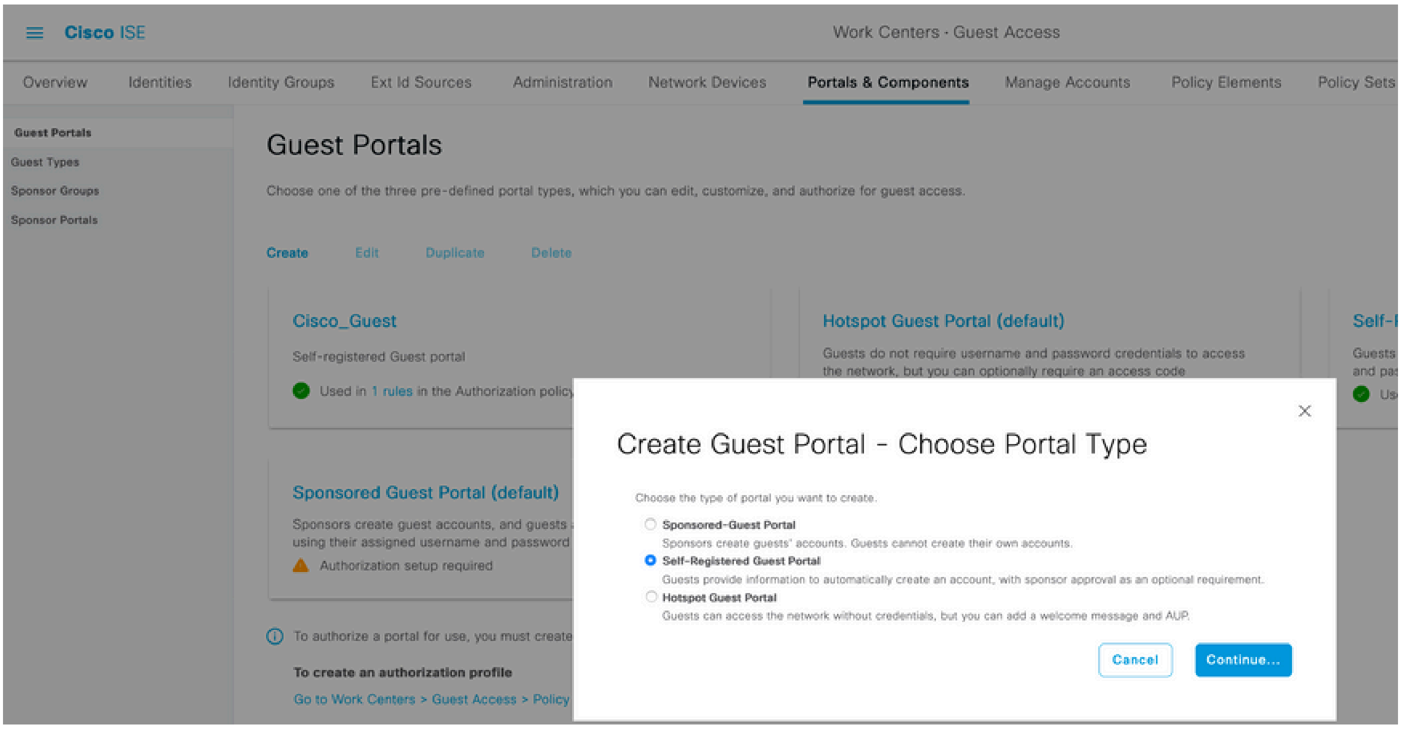
□ Redirect user to a portal page showing an error message

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.建立新的訪客門戶型別：自註冊訪客門戶。導航至工作中心(Work Centers)>訪客接入(Guest Access)>訪客門戶(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.

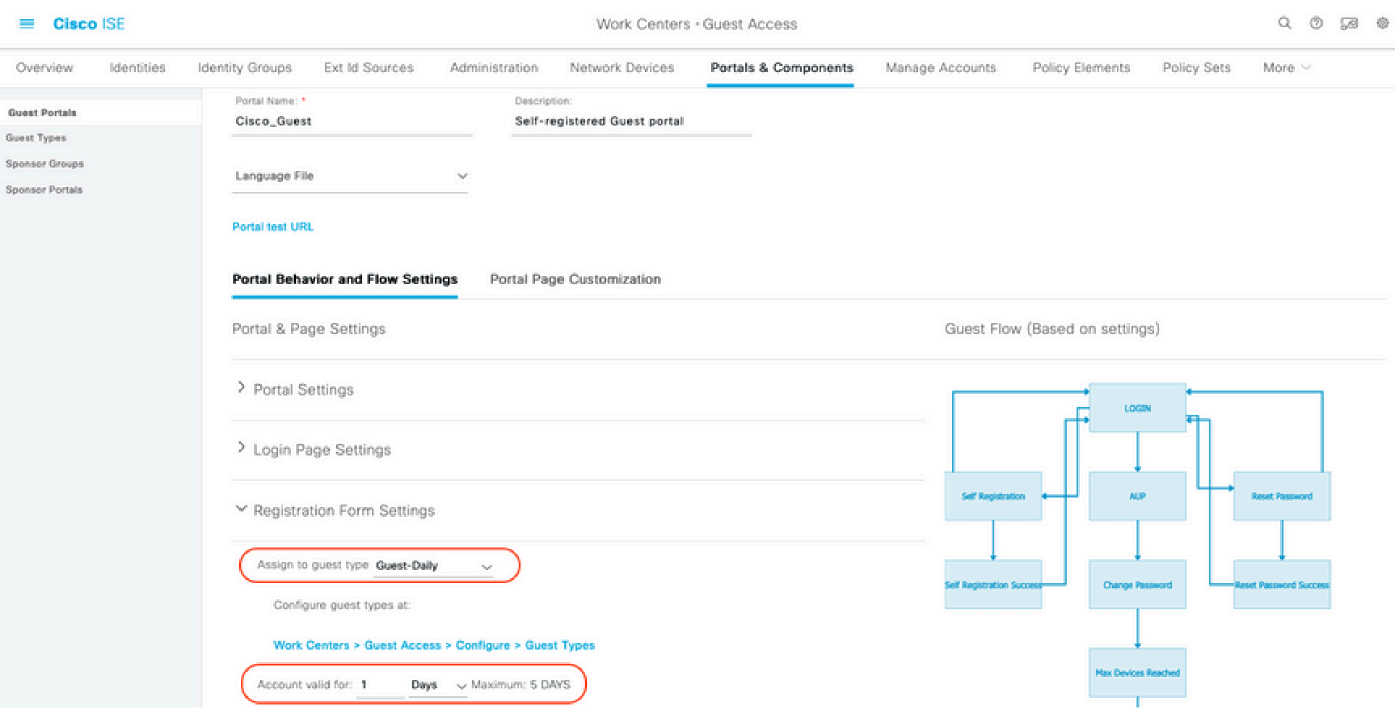
○ Hotspot Guest Portal
Guests can access the network without credentials, but you can add a welcome message and AUP.

5.選擇門戶名稱，參閱之前建立的訪客型別，然後在「登錄檔單」設定下傳送憑據通知設定，以通過電子郵件傳送憑據。

有關如何在ISE上配置SMTP伺服器的資訊，請參閱以下文檔：

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

將所有其他設定保留為預設值。在Portal Page Customization下，可以自定義顯示的所有頁面。預設情況下，訪客帳戶的有效期為1天，可以延長到在特定訪客型別下配置的天數。



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

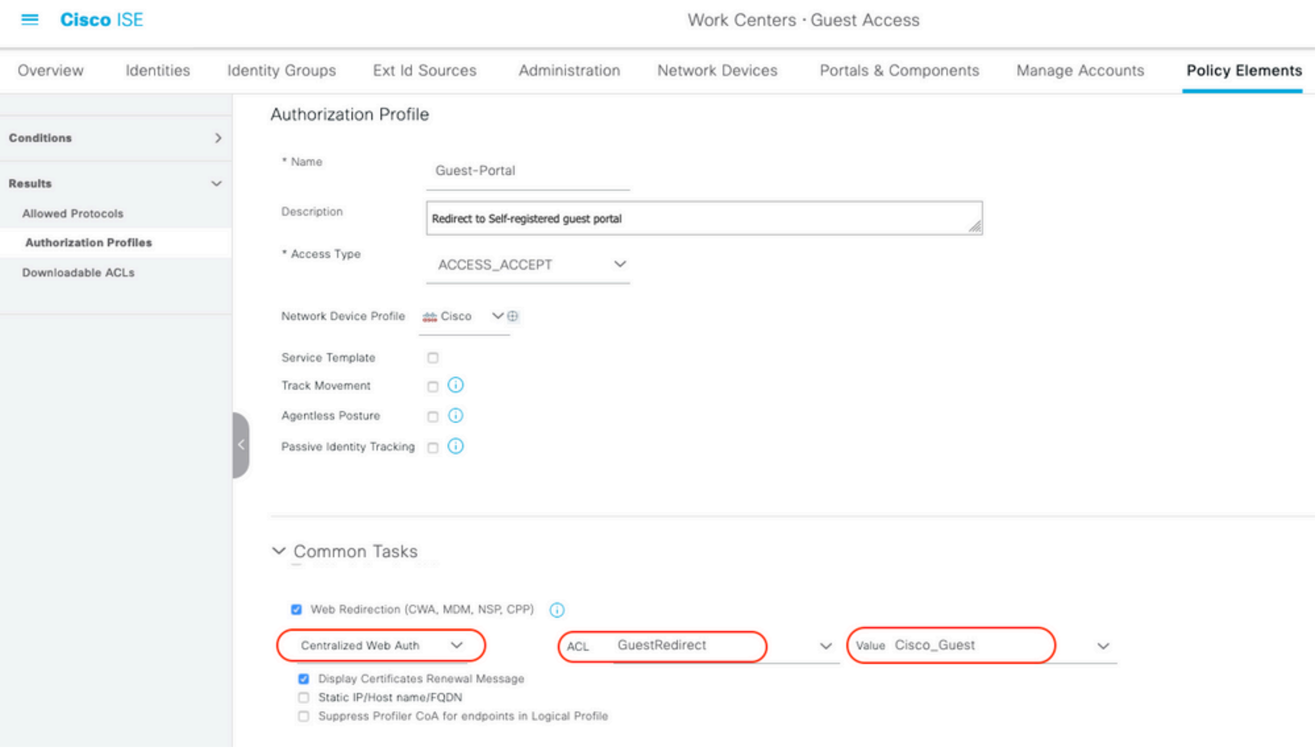
Configure guest types at:

Work Centers > Guest Access > Configure > Guest Types

Account valid for: 1 Days Maximum: 5 DAYS

6.通過導航到工作中心> Guest Access > Policy Elements > Results > Authorization Profiles來配置這兩個授權配置檔案。

- Guest-Portal(具有重新導向至訪客入口Cisco_Guest和名為GuestRedirect的重新導向ACL)。此GuestRedirect ACL是先前在WLC上建立的。



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)

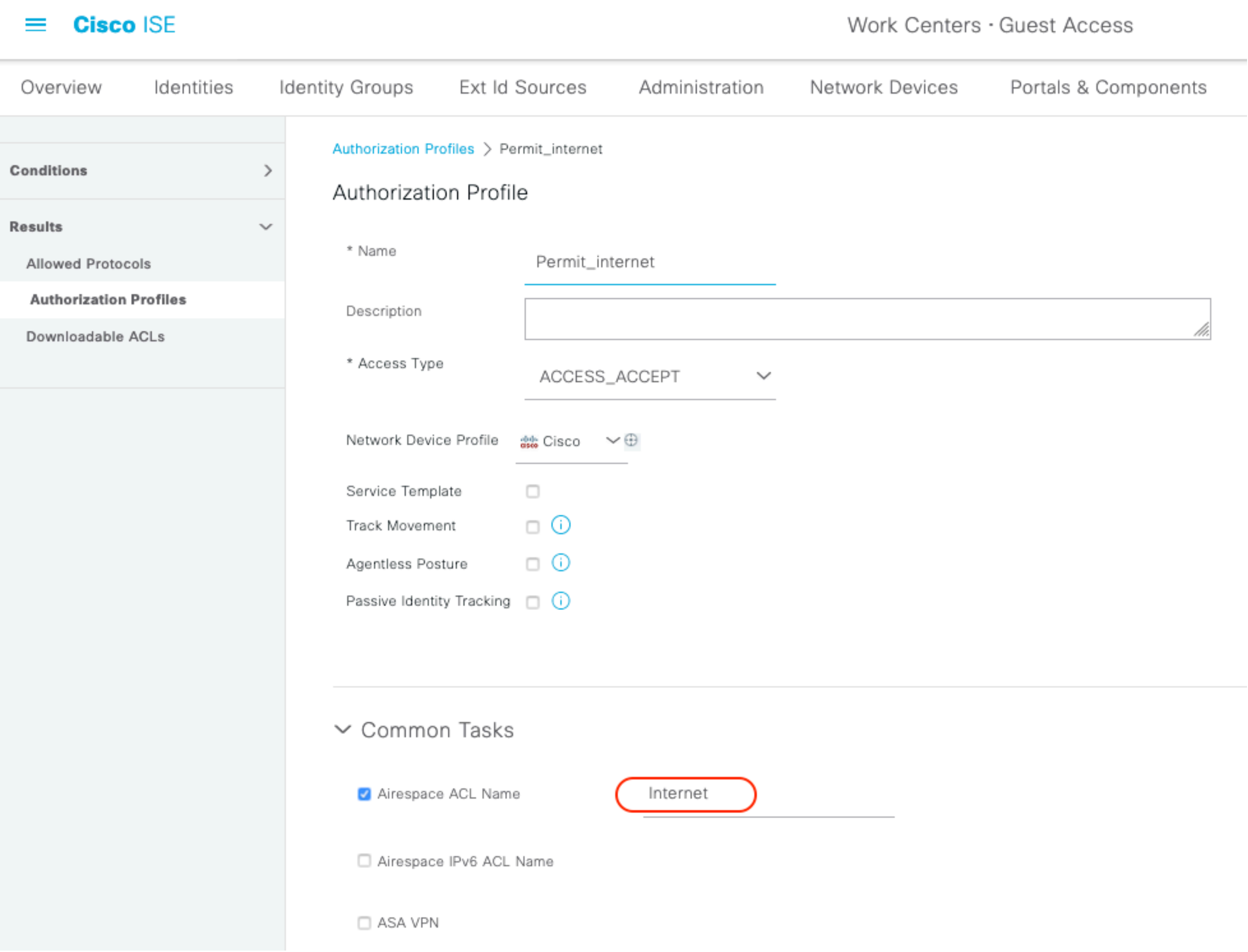
Centralized Web Auth — ACL: GuestRedirect — Value: Cisco_Guest

☑ Display Certificates Renewal Message

☐ Static IP/Host name/FQDN

☐ Suppress Profiler CoA for endpoints in Logical Profile

- Permit_Internet（Airespace ACL等於Internet）



Authorization Profile

* Name: Permit_internet

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Agentless Posture □

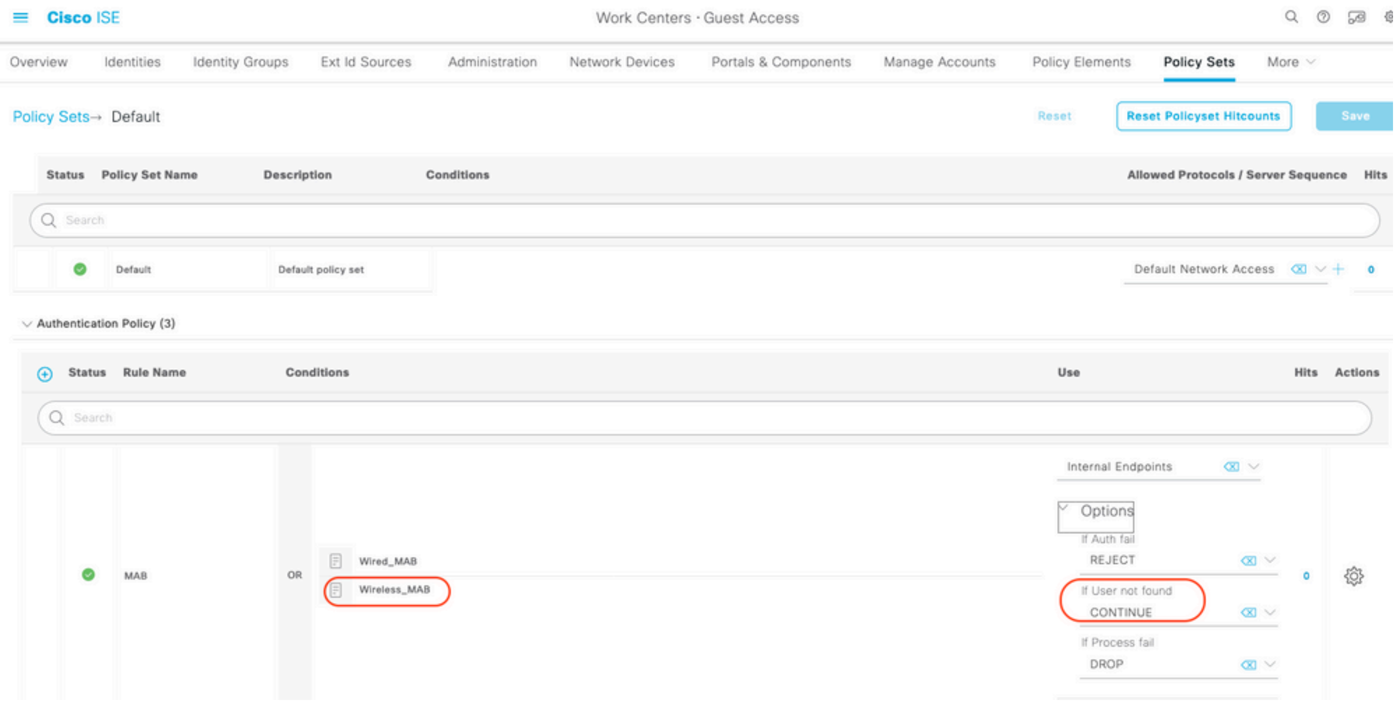
Passive Identity Tracking □

☑ Airespace ACL Name: Internet

□ Airespace IPv6 ACL Name

□ ASA VPN

7.修改名為Default的策略集。已為訪客門戶訪問預配置預設策略集。存在一個名為MAB的身份驗證策略，該策略允許MAC身份驗證繞過(MAB)身份驗證針對未知Mac地址繼續（而不是拒絕）。

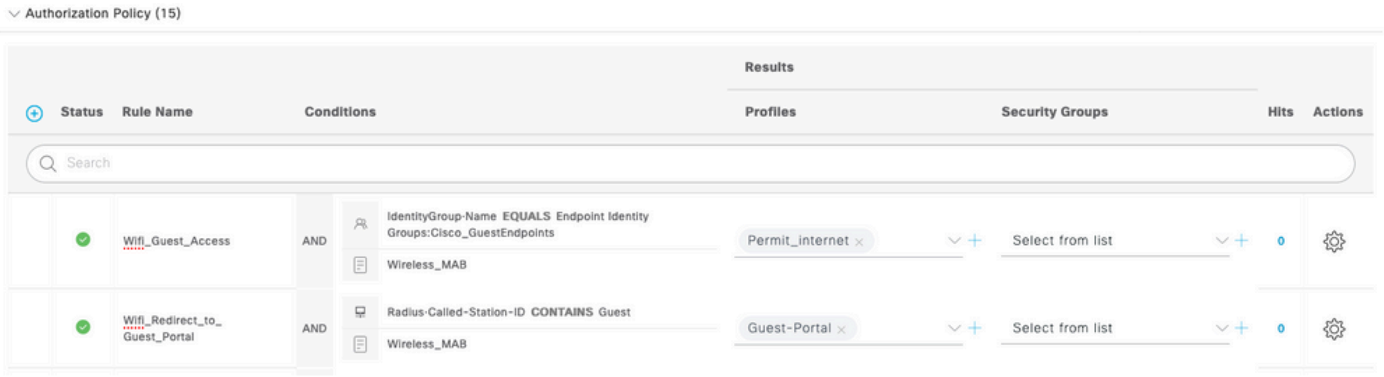


Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	Default	Default policy set		Default Network Access	0

Authentication Policy (3)

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

8.在同一頁上導航到Authorization策略。建立此授權規則，如下圖所示。



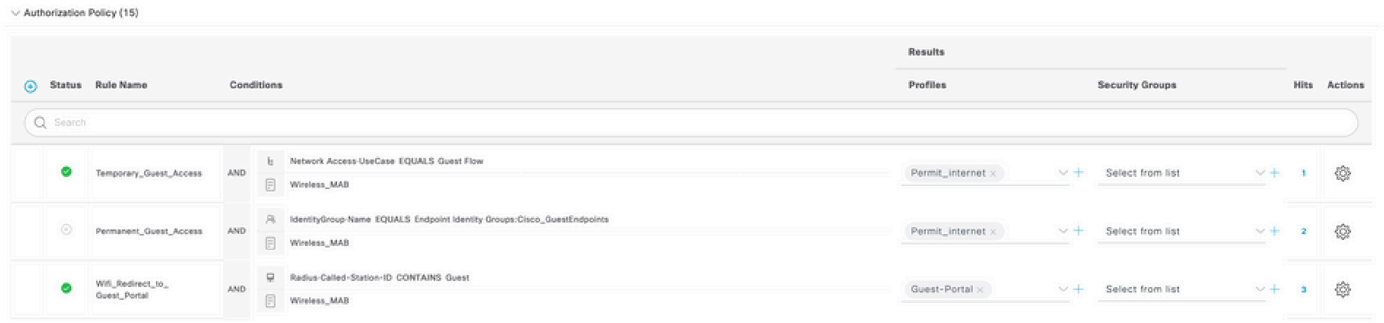
Authorization Policy (15)

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

與訪客SSID關聯的新使用者尚未屬於任何身份組，因此與第二個規則匹配並重定向到訪客門戶。

使用者成功登入後，ISE會傳送RADIUS CoA，而WLC會執行重新驗證。這一次，將匹配第一個授權規則（當端點成為定義的端點身份組的一部分時），並且使用者獲得Permit_internet授權配置檔案。

9.我們還可以使用Guest flow條件來臨時訪問訪客。該條件正在檢查ISE上的活動會話，且屬於屬性。如果該會話具有指示先前訪客使用者已成功通過身份驗證的屬性，則匹配條件。ISE收到來自網路接入裝置(NAD)的Radius記帳停止消息後，會話被終止並隨後刪除。在此階段，不再滿足Network Access:UseCase = Guest Flow的條件。因此，該終端的所有後續身份驗證都會遇到針對訪客身份驗證的通用規則重定向。



Authorization Policy (15)

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

注意：您每次可以使用臨時訪客訪問或永久訪客訪問，但不能同時使用兩者。

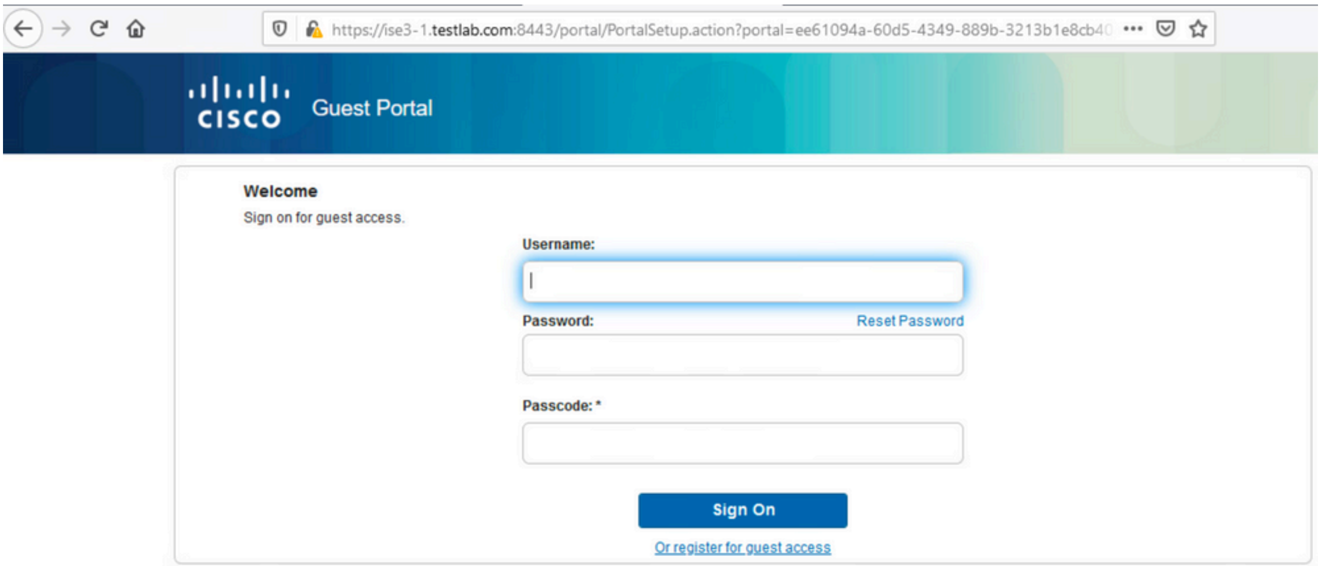
請參閱本文檔詳細瞭解ISE訪客臨時和永久訪問配置。

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

驗證

使用本節內容，確認您的組態是否正常運作。

1. 與訪客SSID關聯並輸入URL後，系統會將您重新導向至訪客門戶頁面，如下圖所示。



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

Guest Portal

Welcome

Sign on for guest access.

Username:

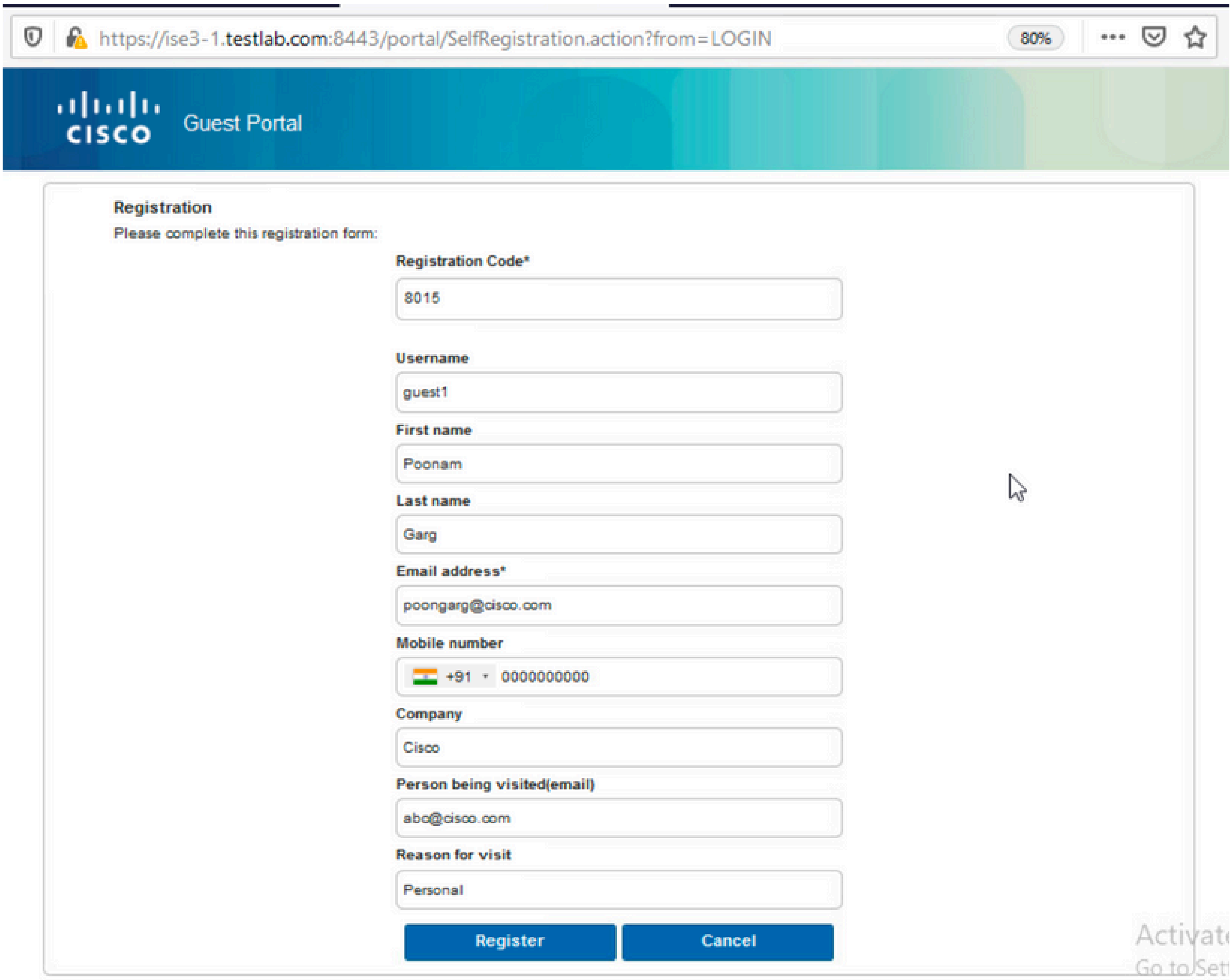
Password: Reset Password

Passcode: *

Sign On

Or register for guest access

2. 由於您沒有任何憑證，您必須選擇Register for Guest access選項。系統將顯示用於建立帳戶的登錄檔格。如果在「訪客門戶」配置下啟用了「註冊代碼」選項，則需要該金鑰值（這可以確保僅允許具有正確許可權的人員自行註冊）。



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

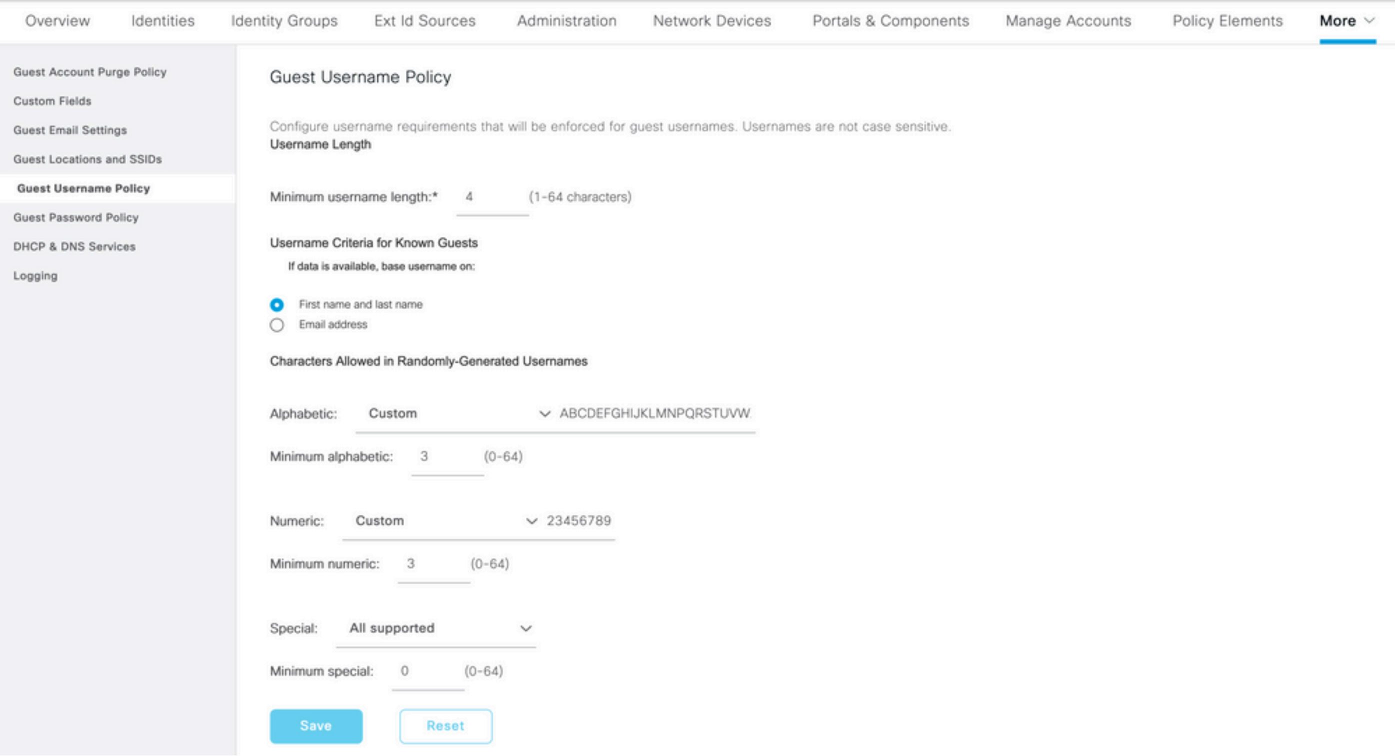
Company: Cisco

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

Reason for visit: Personal

Register Cancel

3.如果密碼或使用者策略存在任何問題，請導航至工作中心> Guest Access > Settings > Guest Username Policy以更改設定。以下是範例：



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)

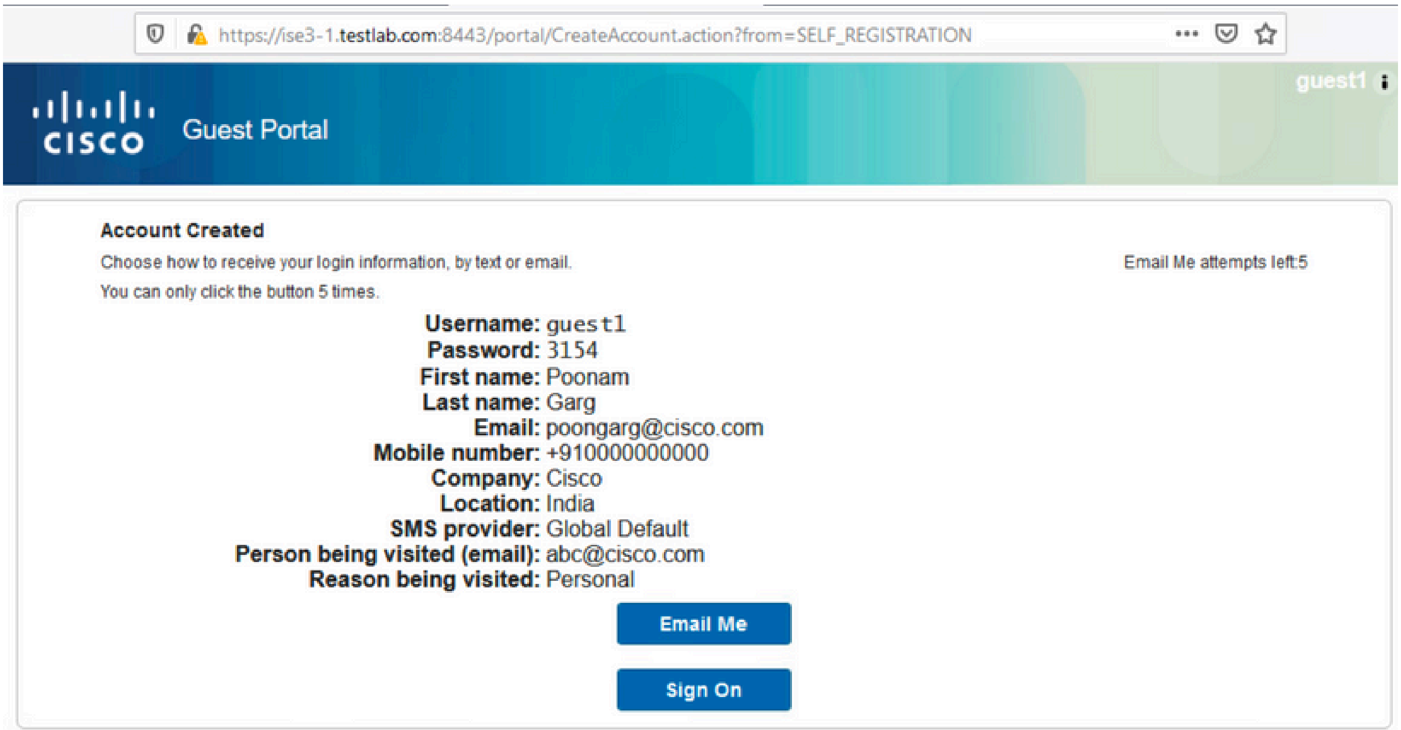
Numeric: Custom 23456789

Minimum numeric: 3 (0-64)

Special: All supported

Minimum special: 0 (0-64)

4.成功建立帳戶後，系統將向您提供憑證（根據訪客密碼策略生成的密碼），如果進行了配置，訪客使用者還將收到電子郵件通知：


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

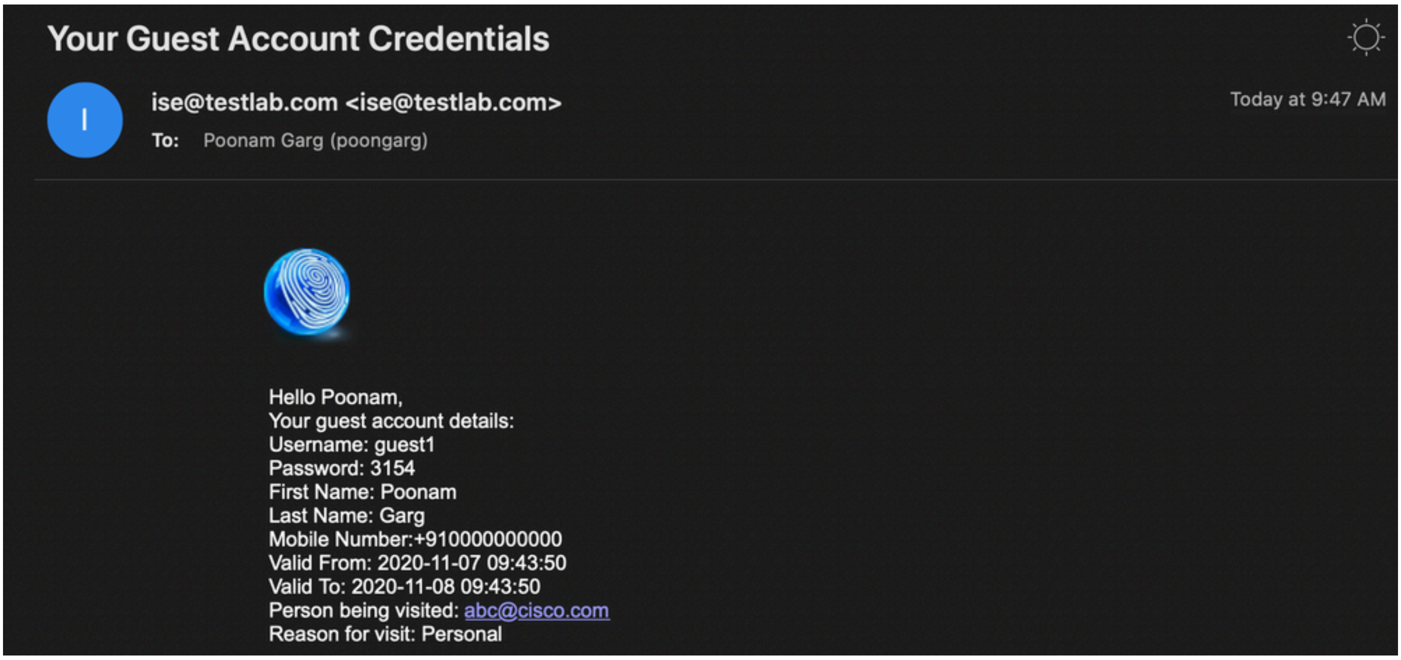
Account Created

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

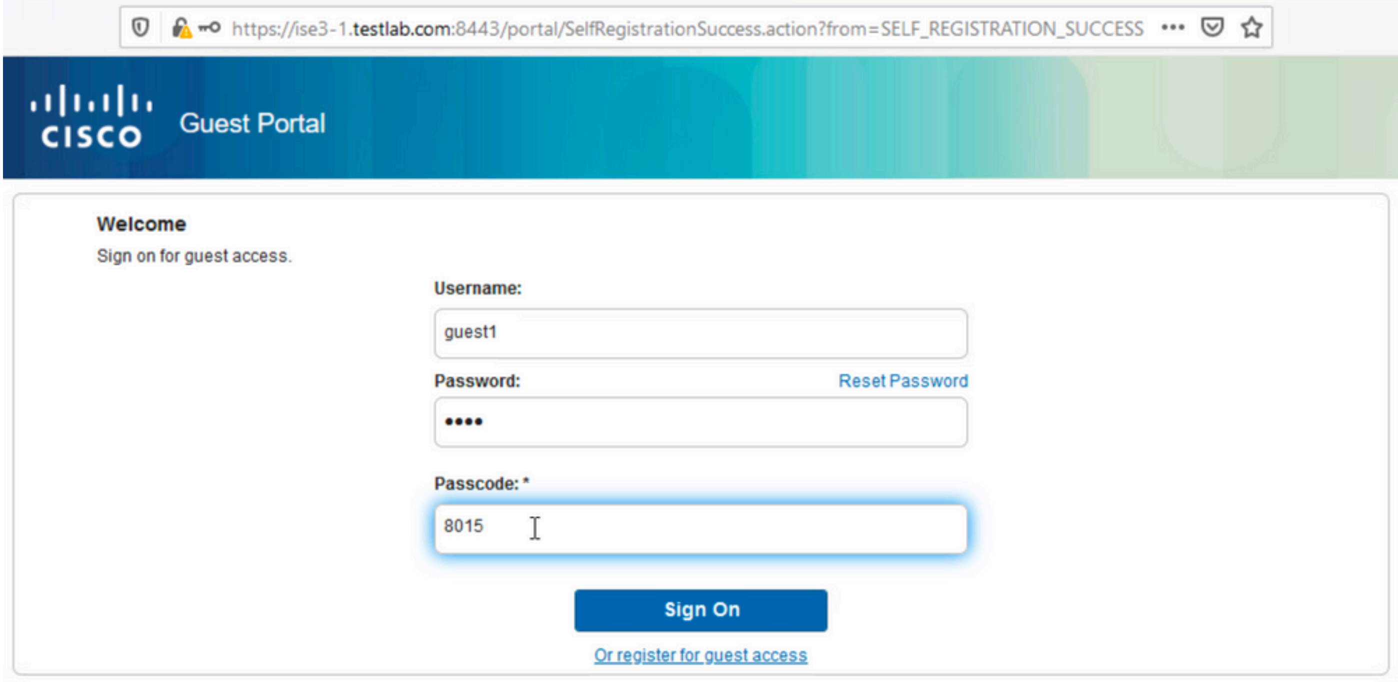
ise@testlab.com <ise@testlab.com>

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.按一下登入並提供憑據（如果在訪客門戶下配置，則可能需要其他訪問密碼；這是只允許知道密碼的使用者登入的另一種安全機制）。



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

Welcome

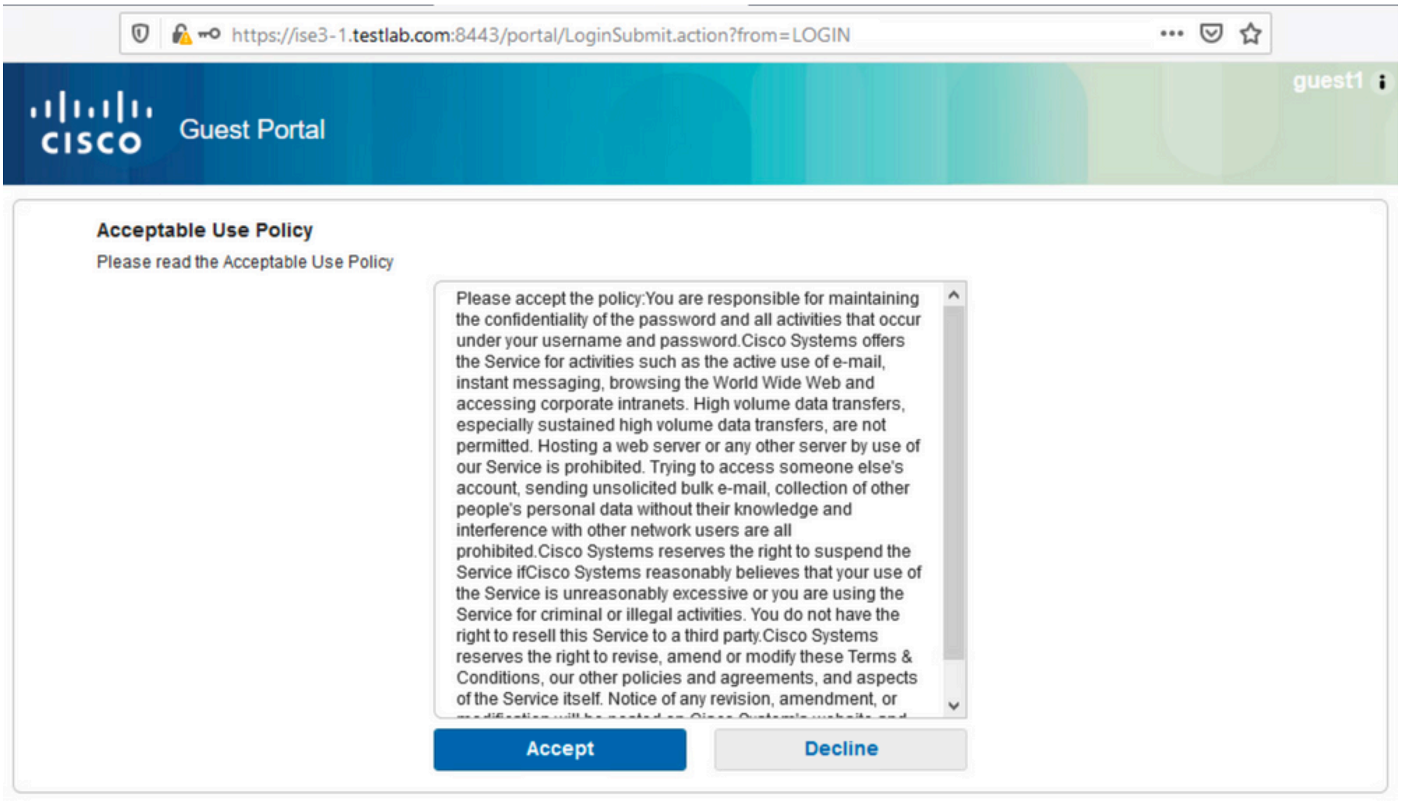
Sign on for guest access.

Username: guest1

Password: ••••

Passcode: * 8015

6.成功後，可提供一個可選的使用策略(AUP)（如果在訪客門戶下配置）。系統向使用者顯示更改密碼選項，還可以顯示登入後橫幅（也可在Guest Portal下配置）。



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

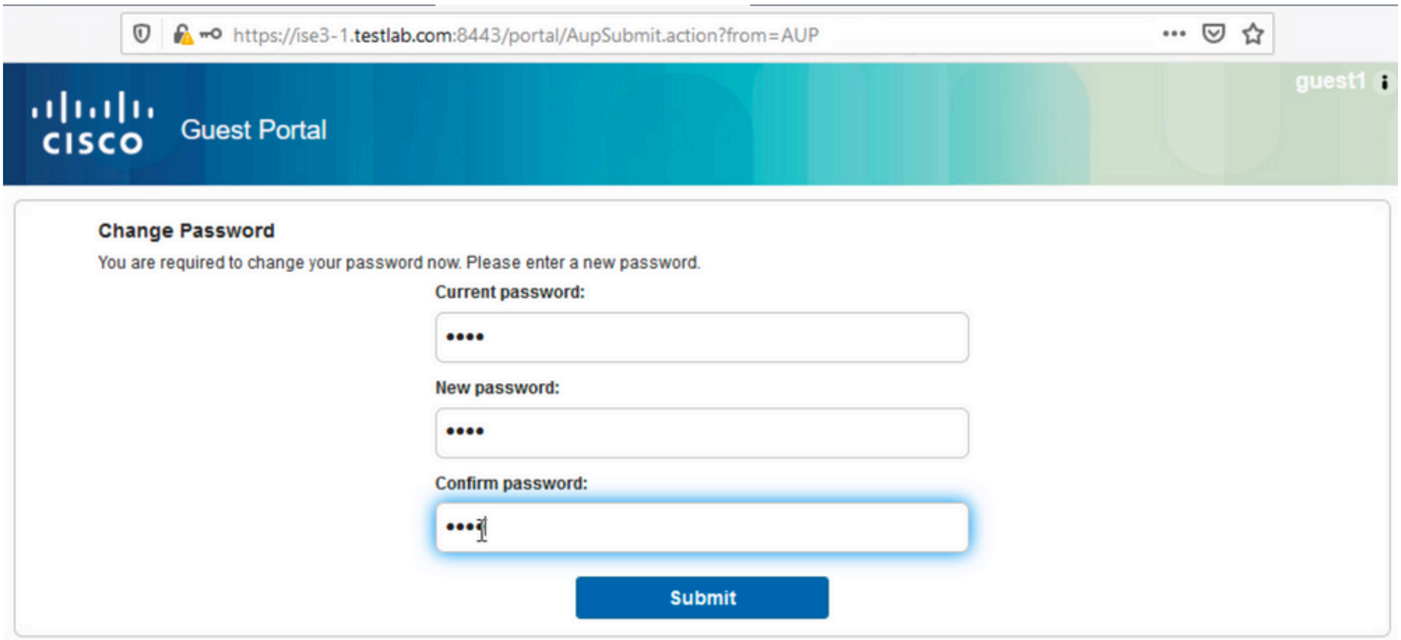
Guest Portal

guest1

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

Guest Portal

guest1

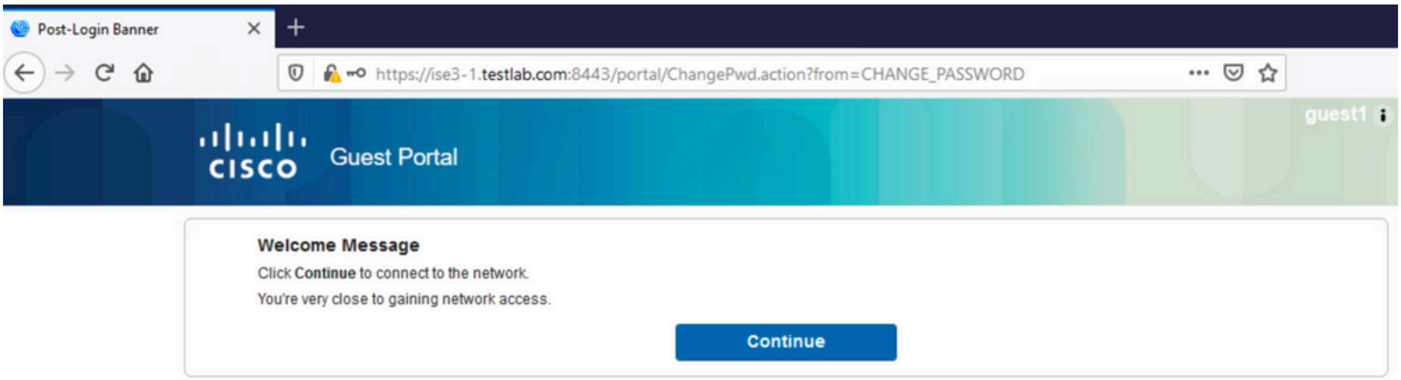
Change Password

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

Guest Portal

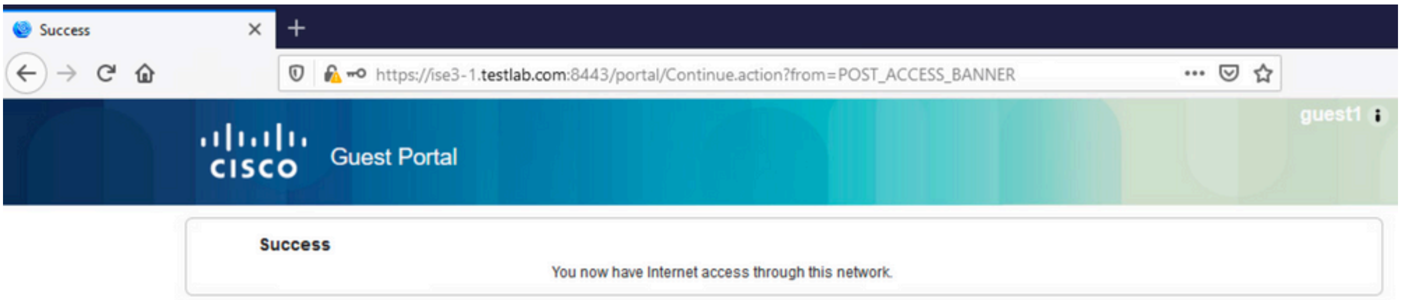
guest1

Welcome Message

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

You're very close to gaining network access.

7.最後一頁（登入後橫幅）確認已授予訪問許可權：


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

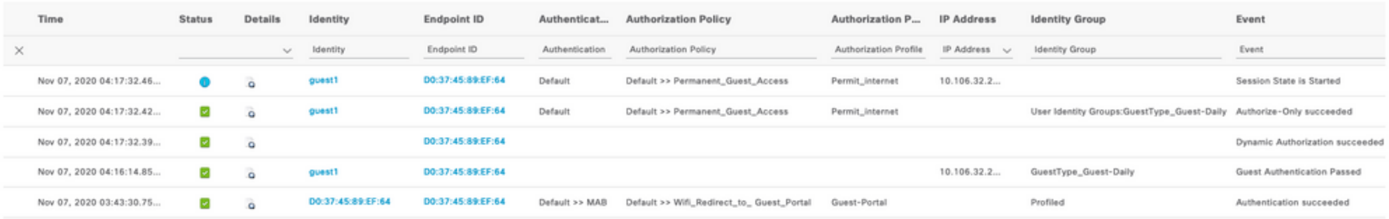
Success

You now have Internet access through this network.

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

在此階段，ISE在Operations > RADIUS > Live Logs下顯示這些日誌，如圖所示。

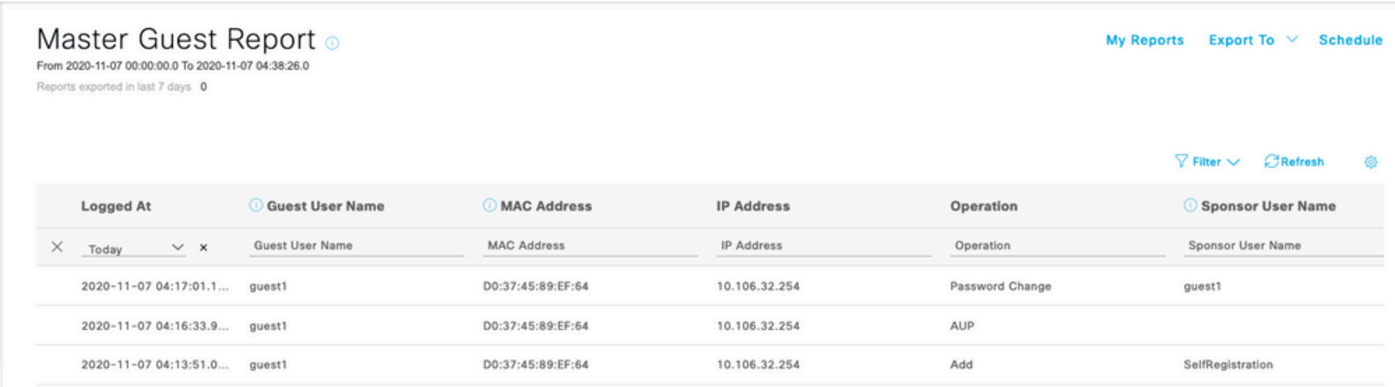


Time	Status	Details	Identity	Endpoint ID	Authenticat...	Authorization Policy	Authorization P...	IP Address	Identity Group	Event
			Identity	Endpoint ID	Authentication	Authorization Policy	Authorization Profile	IP Address	Identity Group	Event
Nov 07, 2020 04:17:32.46...	●		guest1	D0:37:45:89:EF:64	Default	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

以下是流程：

- 訪客使用者遇到第二個授權規則(Wifi_Redirect_to_Guest_Portal)，並被重定向到Guest-Portal(驗證成功)。
- 訪客被重新導向以進行自我註冊。成功登入（使用新建立的帳戶）後，ISE會傳送CoA重新驗證，並由WLC確認(動態授權成功)。
- WLC使用Authorize-Only屬性執行重新身份驗證，並返回ACL名稱(Authorize-Only succeeded)。為訪客提供了正確的網路訪問。

報告(Operations > Reports > Guest > Master Guest Report)還確認：



Master Guest Report

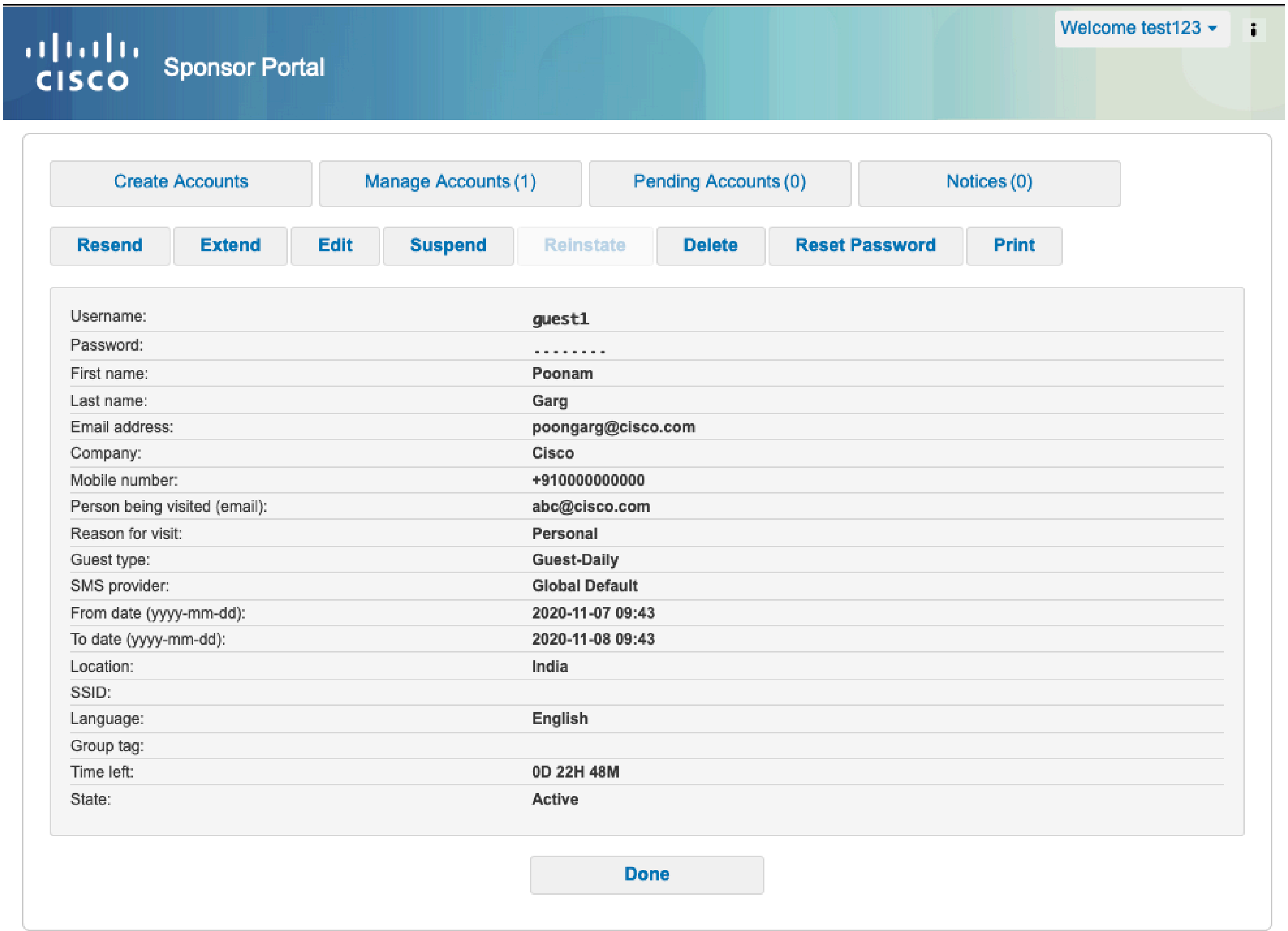
From 2020-11-07 00:00:00.0 To 2020-11-07 04:38:26.0

Reports exported in last 7 days 0

Logged At	Guest User Name	MAC Address	IP Address	Operation	Sponsor User Name
Today	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

保證人使用者（具有正確許可權）可以驗證訪客使用者的當前狀態。

此示例確認已建立帳戶，且使用者已登入到門戶：



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

可選配置

對於此流程中的每個階段，可以配置不同的選項。所有這一切都是根據Guest Portal配置的，其地址為：Work Centers > Guest Access > Portals & Components > Guest Portals > Portal Name > Edit > Portal Behavior and Flow Settings。更重要的設定包括：

自助註冊設定

- 訪客型別 — 描述帳戶處於活動狀態的時間、密碼到期選項、登入時間和選項（這是時間配置檔案和訪客角色的混合）
- 註冊碼 — 如果啟用，則僅允許知道密碼的使用者進行自我註冊（必須在建立帳戶時提供密碼）
- AUP — 在自行註冊期間接受使用策略
- 發起人批准/啟用訪客帳戶的要求。

登入訪客設定

- 訪問代碼 — 如果啟用，則只允許知道密碼的訪客使用者登入。
- AUP — 在自行註冊期間接受使用策略。

- 密碼更改選項。

裝置註冊設定

- 預設情況下，裝置會自動註冊。

訪客裝置合規性設定

- 允許在流內設定狀態。

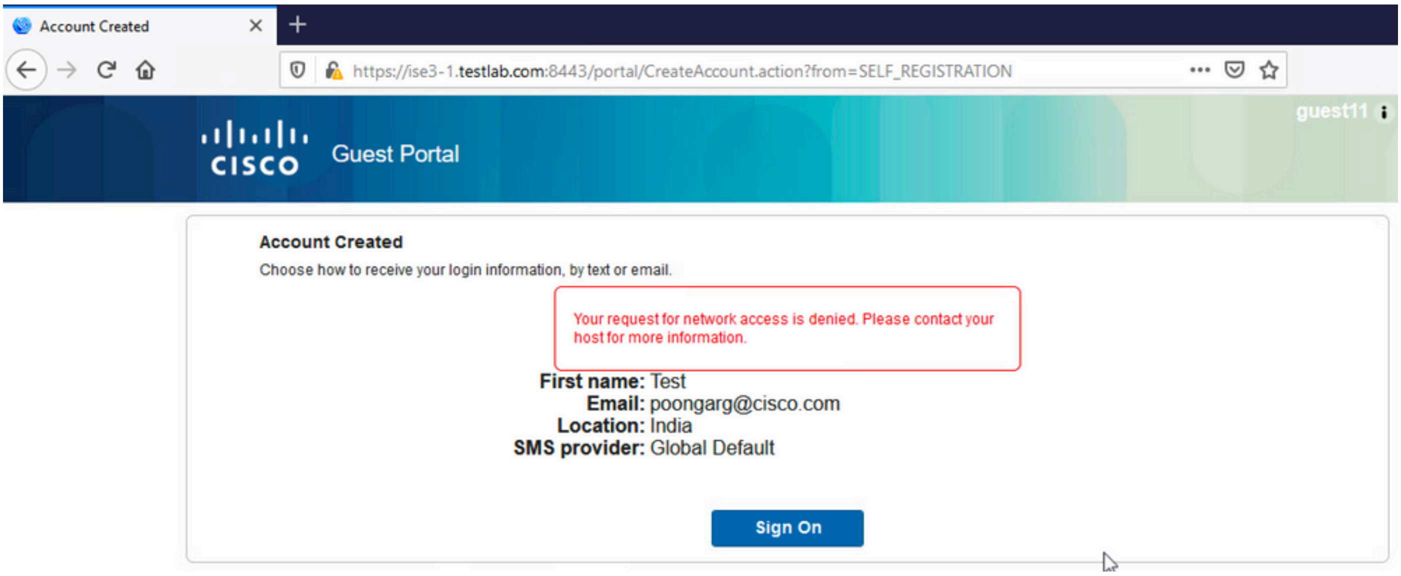
BYOD設定

- 允許將門戶用作訪客的企業使用者註冊其個人裝置。

發起人批准的帳戶

如果在登錄檔單設定下選擇了要求訪客獲得批准選項，則訪客建立的帳戶必須由發起人批准。此功能可以使用電子郵件向發起人傳遞通知（用於訪客帳戶批准）：

如果簡單郵件傳輸協定(SMTP)伺服器配置錯誤，則不會建立帳戶：


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

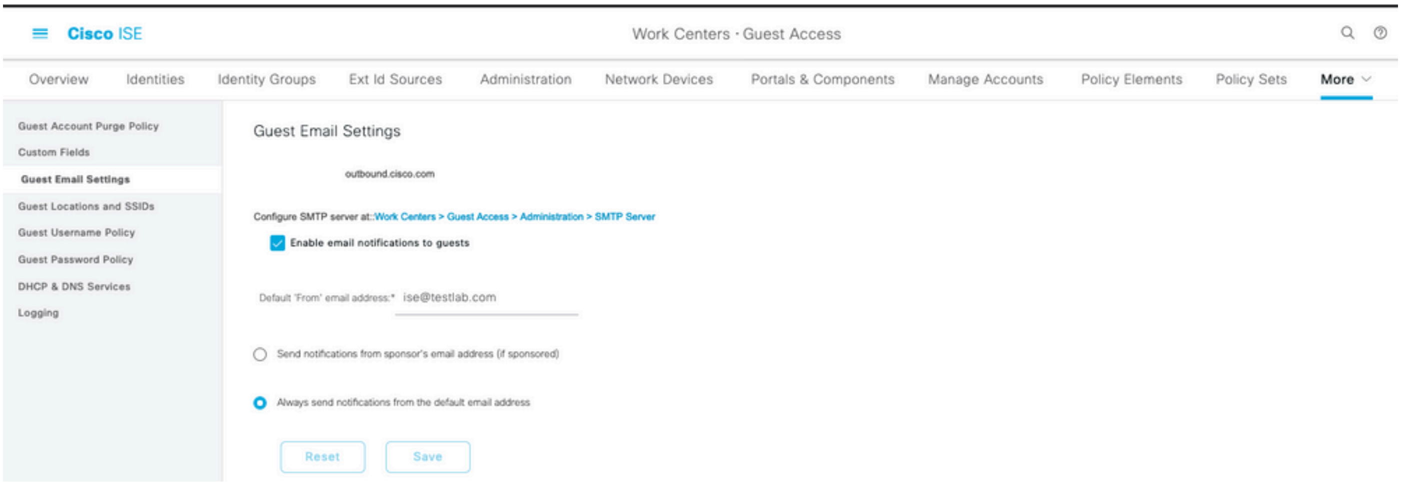
來自guest.log的日誌確認，由於SMTP伺服器配置錯誤，向發起人電子郵件傳送批准通知時出現問題：

<#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.nc
com.cisco.cpm.guestaccess.exception.GuestAccessSystemException: com.cisco.cpm.guestaccess.exception.Gues
```

當您具有正確的電子郵件和SMTP伺服器配置時，帳戶將建立：



Guest Email Settings

outbound.cisco.com

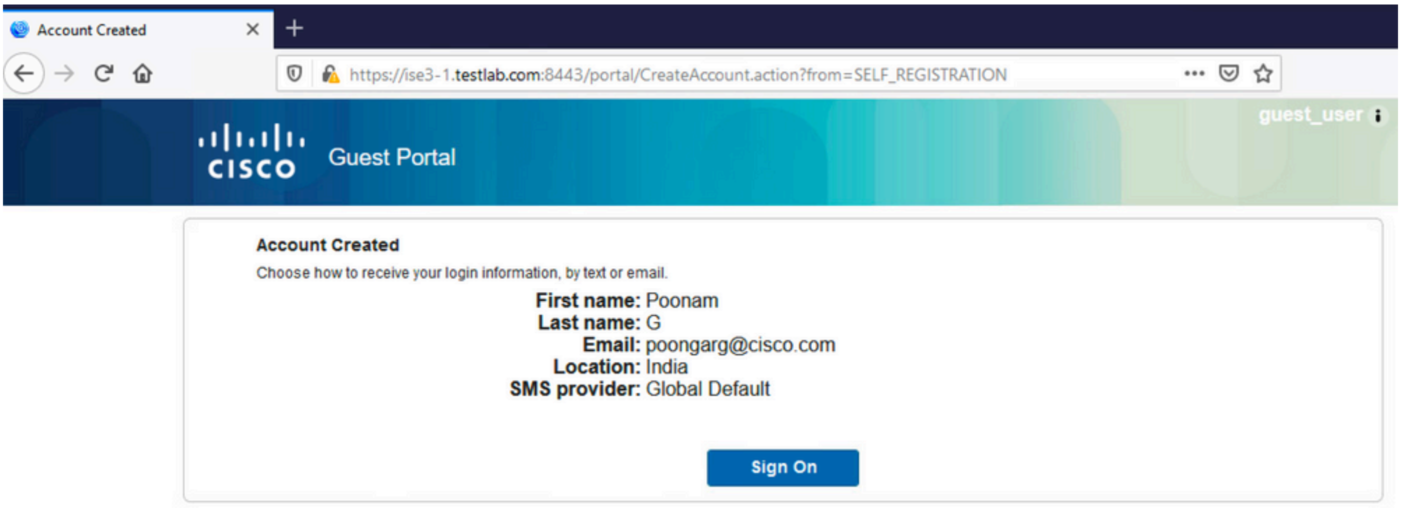
Configure SMTP server at::Work Centers > Guest Access > Administration > SMTP Server

☑ 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


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

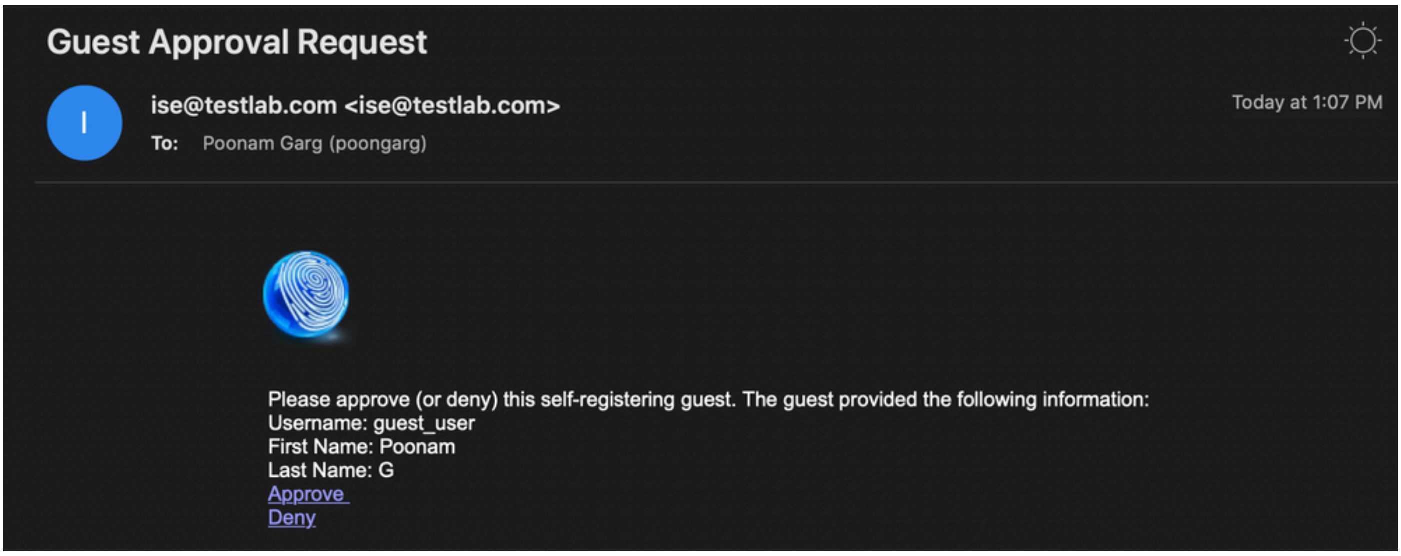
Account Created

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

啟用要求訪客獲得批准選項後，使用者名稱和密碼欄位將自動從Include this information on the Self-Registration Success page部分刪除。這就是在需要發起人批准時，訪客使用者的憑據預設情況下不會顯示在顯示帳戶已建立資訊的網頁上的原因。相反，它們必須通過簡訊服務(SMS)或電子郵件傳送。此選項必須在Send credential notification upon approval using部分(標籤電子郵件/SMS)中啟用。

向發起人傳送通知電子郵件：



Guest Approval Request

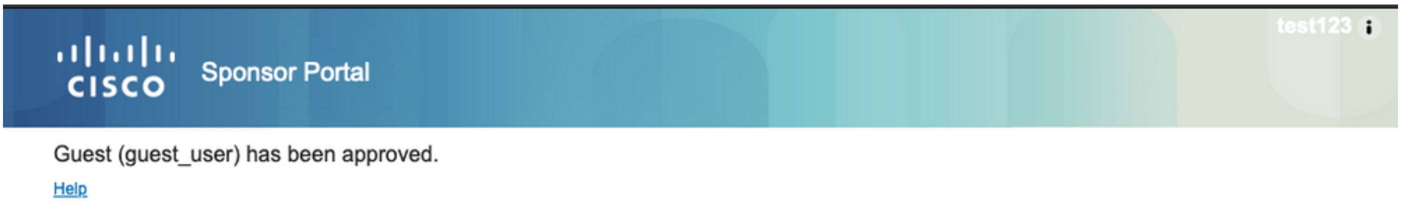
ise@testlab.com <ise@testlab.com>

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

發起人點選Approval連結並登入到Sponsor門戶，該帳戶已獲批准：



Guest (guest_user) has been approved.

Help

從此時起，允許訪客使用者登入（使用通過電子郵件或SMS接收的憑證）。

總而言之，此流程中使用了三個電子郵件地址：

- 通知「發件人」地址。這是靜態定義的，或者從發起人帳戶中定義，並用作發起人通知（用於審批）和訪客憑證詳細資訊的「發件人」地址。在工作中心(Work Centers)>訪客接入(Guest Access)>設定(Settings)>訪客郵件設定(Guest Email Settings)下配置此設定。

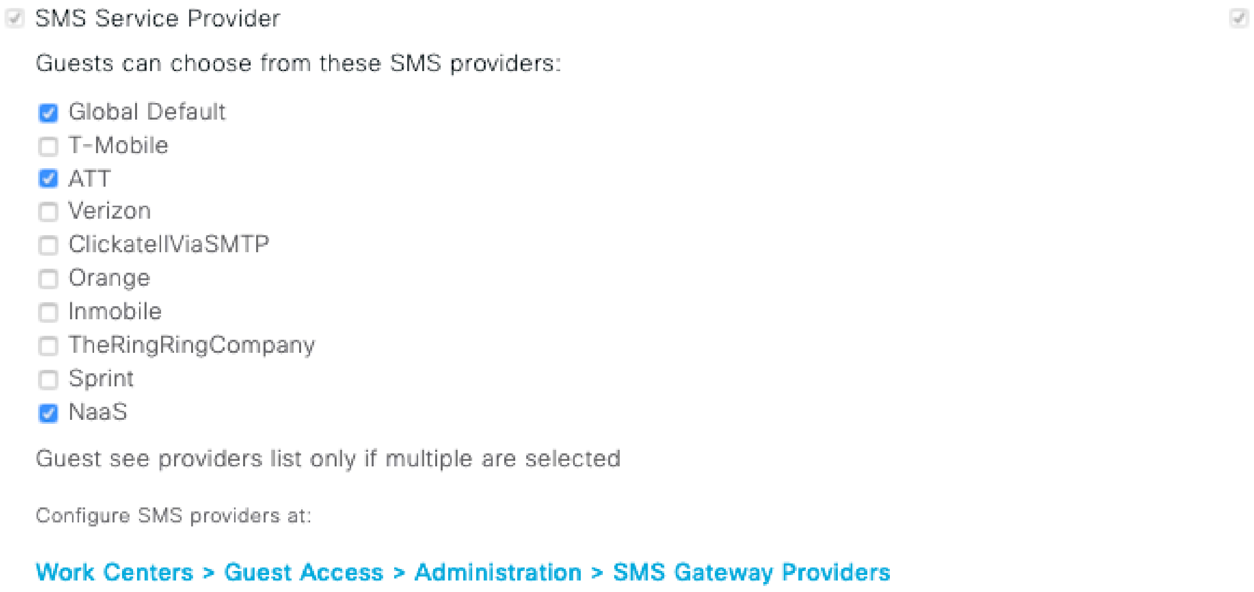
- 通知「收件人」地址。用於通知發起人已收到要審批的帳戶。在Guest Portal中的Work Centers > Guest Access > Guest Portals > Portals and Components > Portal Name > Registeration Form Settings > Require guests to be approved > Email approval request to下配置此項。

- 訪客「收件人」地址。這是由訪客使用者在註冊期間提供的。如果選中Send credential notification upon approval using Email，則會將包含憑據詳細資訊（使用者名稱和密碼）的電子郵件傳送給訪客。

通過簡訊傳遞憑證

訪客憑證也可以通過SMS傳送。必須配置以下選項：

1. 在Registration Form Settings（登錄檔單設定）下選擇SMS服務提供商：



☑ SMS Service Provider ☑

Guests can choose from these SMS providers:

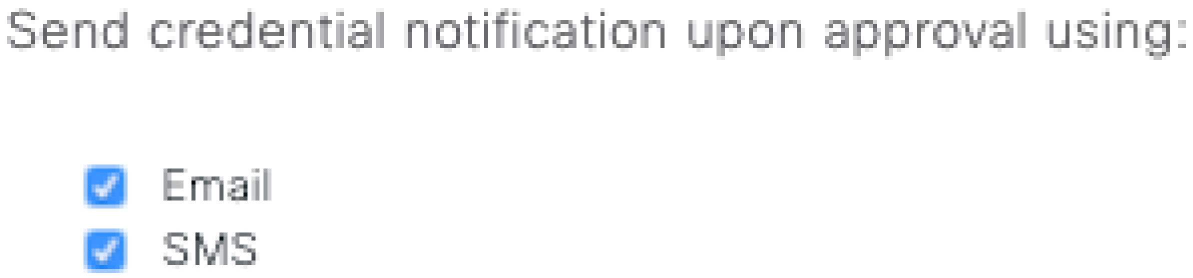
☑ Global Default
□ T-Mobile
☑ ATT
□ Verizon
□ ClickatellViaSMTP
□ Orange
□ Inmobile
□ TheRingRingCompany
□ Sprint
☑ NaaS

Guest see providers list only if multiple are selected

Configure SMS providers at:

Work Centers > Guest Access > Administration > SMS Gateway Providers

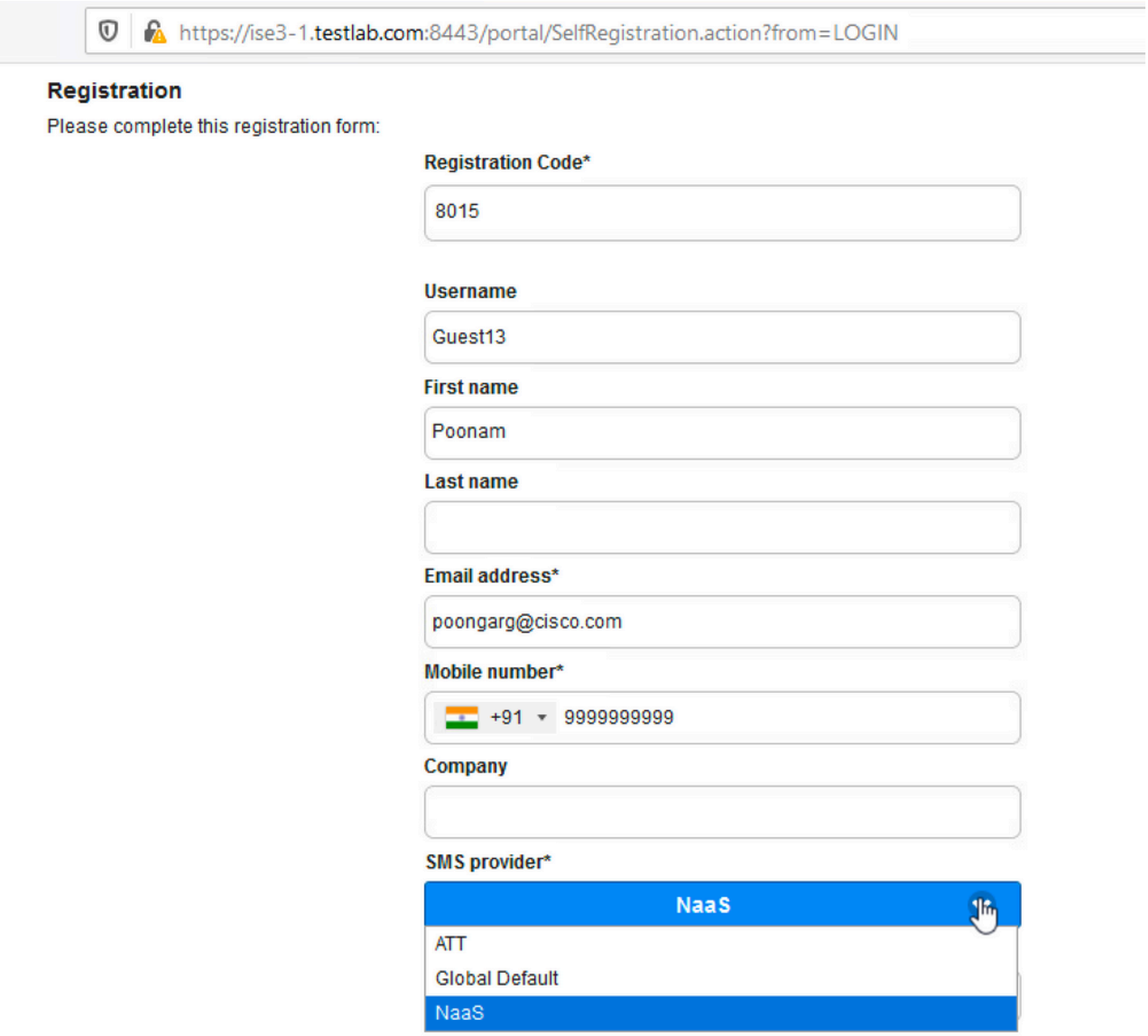
2. 選中Send credential notification upon approval using: SMS覈取方塊。



Send credential notification upon approval using:

☑ Email
☑ SMS

3. 然後，訪客使用者在建立帳戶時需要選擇可用的提供商：



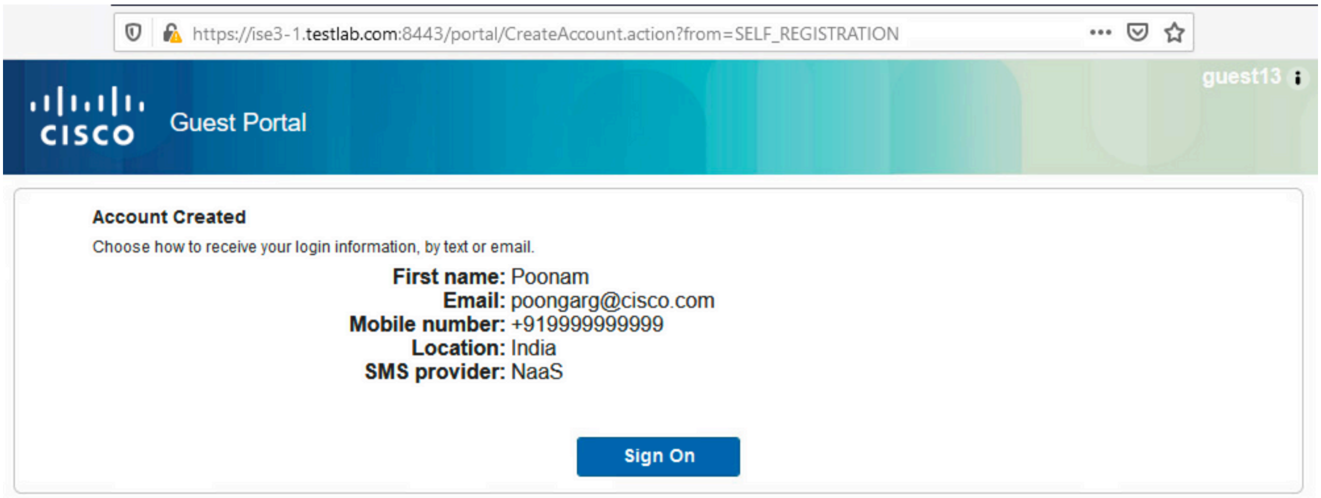
https://ise3-1.testlab.com:8443/portal/SelfRegistration.action?from=LOGIN

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. 隨所選提供商和電話號碼傳送SMS:



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

Account Created

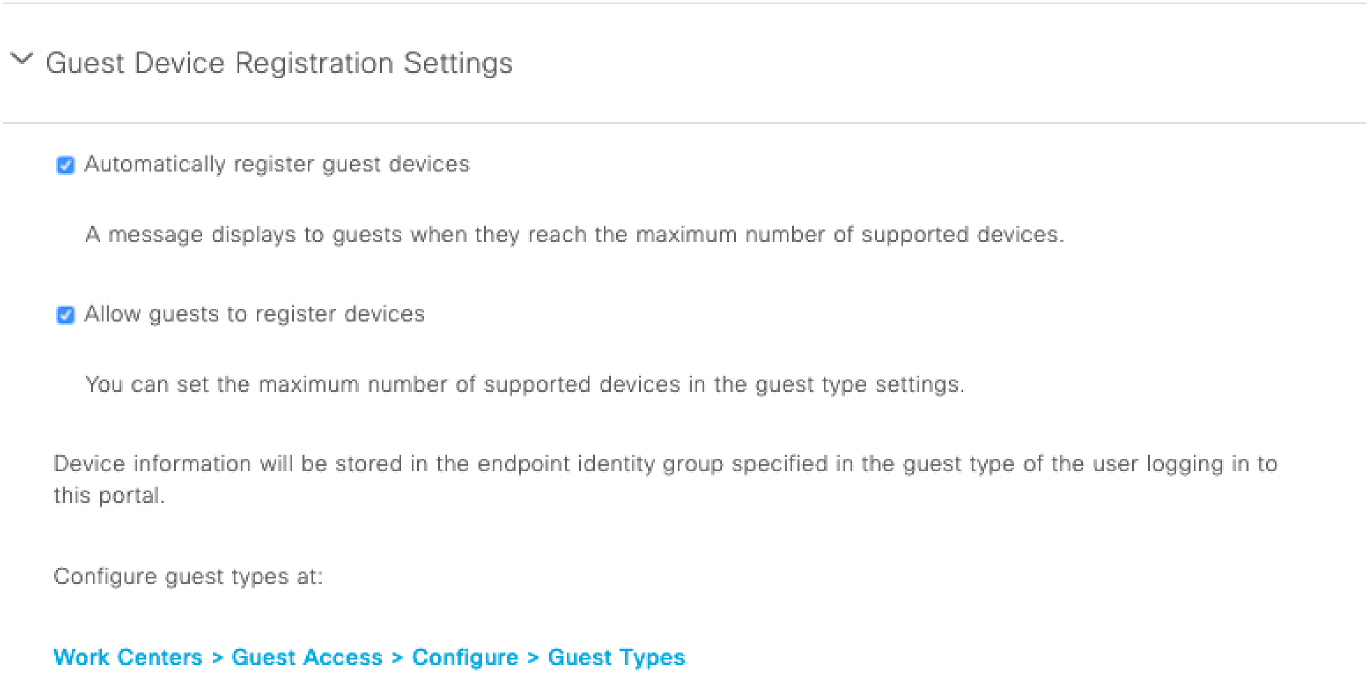
Choose how to receive your login information, by text or email.

First name: Poonam
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提供程式。

裝置註冊

如果在訪客使用者登入並接受AUP後選擇了Allow guests to register devices選項，則可以註冊裝置：



Guest Device Registration Settings

☑ Automatically register guest devices

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

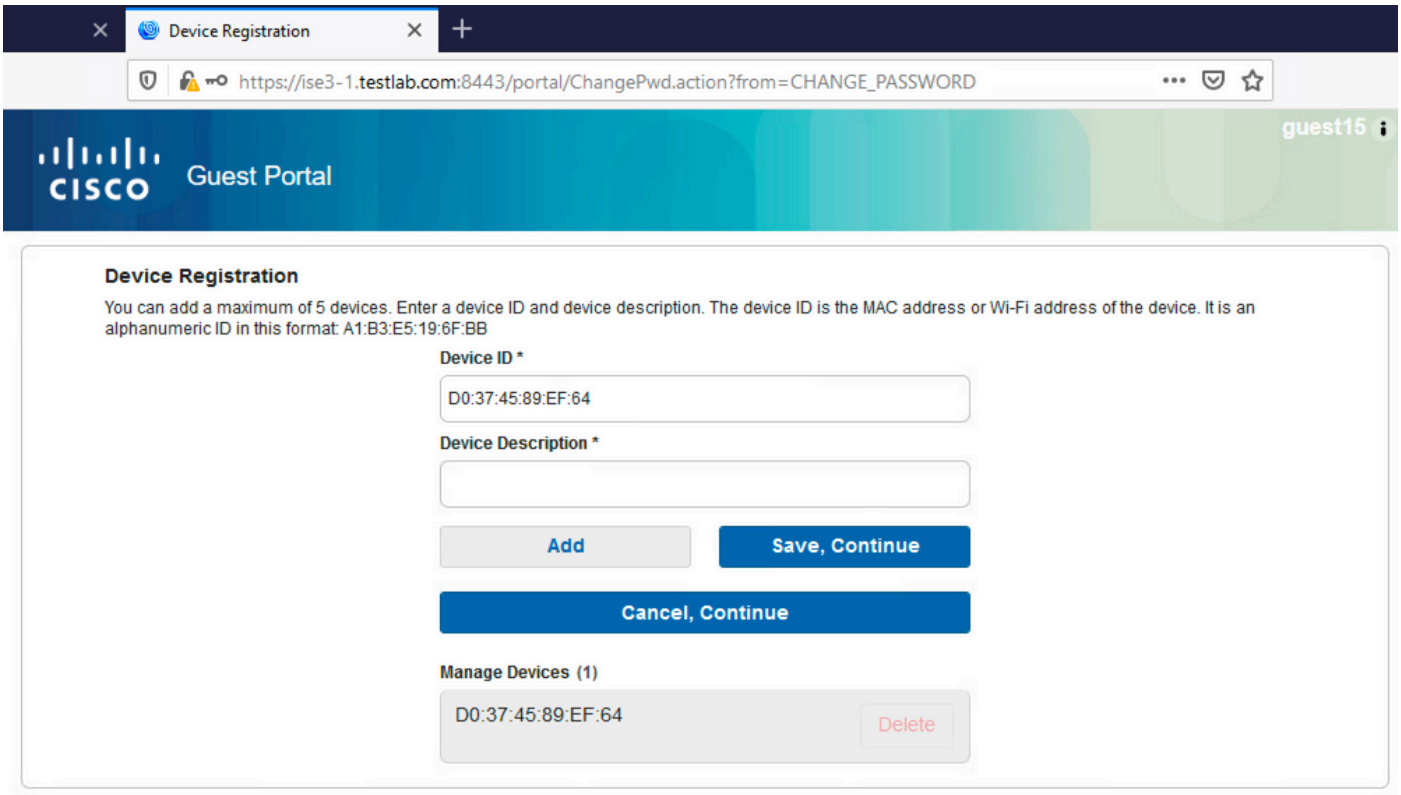
☑ Allow guests to register devices

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
cisco
Guest Portal
guest15

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)

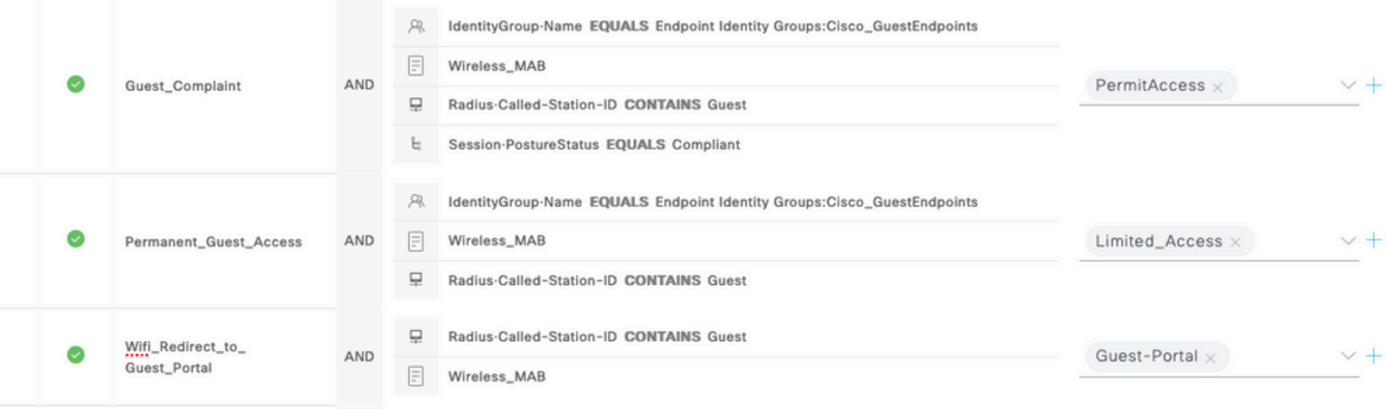
D0:37:45:89:EF:64

請注意，裝置已自動新增(它位於「管理裝置」(Manage Devices)清單中)。這是因為選擇了Automatically register guest devices。

狀態

如果選擇了Require guest device compliance選項，則訪客使用者登入並接受AUP（以及可選地執行裝置註冊）後，會使用執行狀態（NAC/Web代理）的代理進行調配。ISE處理客戶端調配規則以確定必須調配哪個代理。然後，在站點上運行的代理執行安全評估（根據安全評估規則）並將結果傳送到ISE，ISE會根據需要傳送CoA重新身份驗證以更改授權狀態。

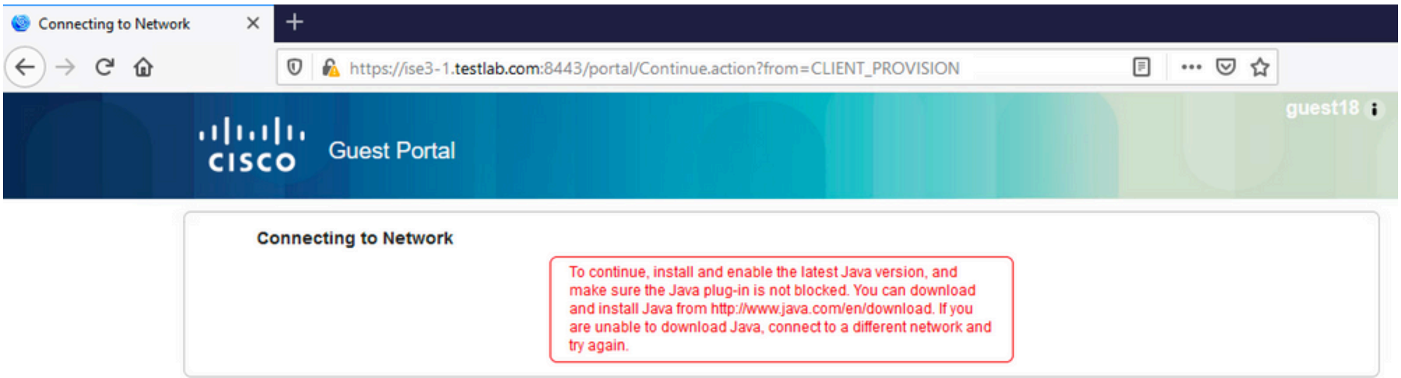
可能的授權規則可能如下所示：



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

第一個遇到Guest_Authenticate規則的新使用者重定向到自助註冊訪客門戶。使用者自行註冊並登入後，CoA會更改授權狀態，使用者將獲得執行狀態和補救的有限訪問許可權。只有在設定了NAC代理且工作站符合要求後，CoA才會再次更改授權狀態，以便提供對Internet的訪問。

安全狀態的典型問題包括缺少正確的客戶端調配規則：



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.

如果您檢查guest.log檔案：

<#root>

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

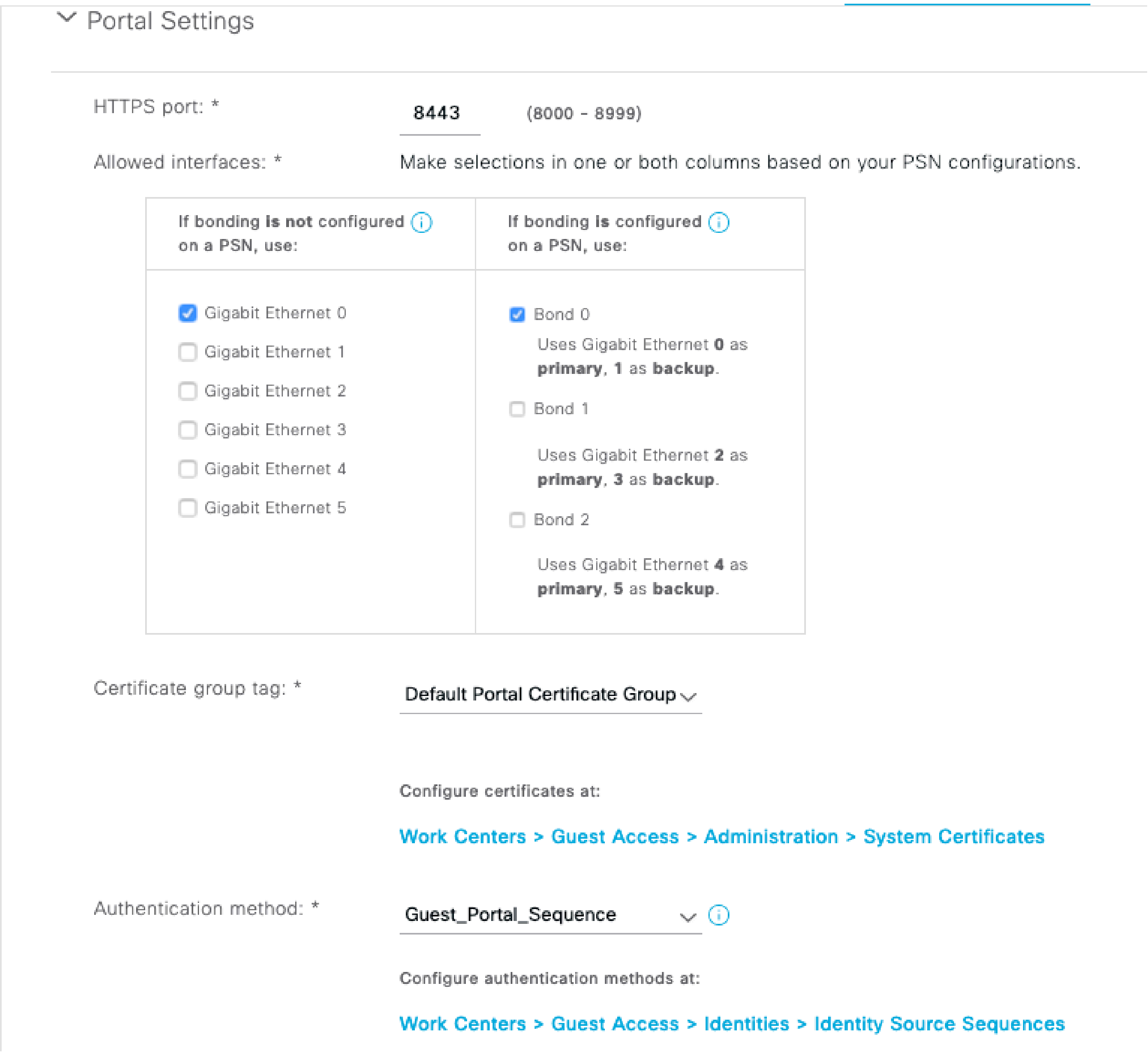
自帶裝置

如果選中Allow employees to use personal devices on the network選項，則使用此門戶的公司使用

者可以通過BYOD流程並註冊個人裝置。對於訪客使用者，該設定不會更改任何內容。

「員工使用門戶作為訪客」是什麼意思？

預設情況下，使用Guest_Portal_Sequence identity store配置訪客門戶：



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 □ Gigabit Ethernet 1 □ Gigabit Ethernet 2 □ Gigabit Ethernet 3 □ Gigabit Ethernet 4 □ Gigabit Ethernet 5	☑ Bond 0 Uses Gigabit Ethernet **0** as **primary**, **1** as **backup**. □ Bond 1 Uses Gigabit Ethernet **2** as **primary**, **3** as **backup**. □ Bond 2 Uses Gigabit Ethernet **4** as **primary**, **5** as **backup**.

Certificate group tag: * Default Portal Certificate Group

Configure certificates at:

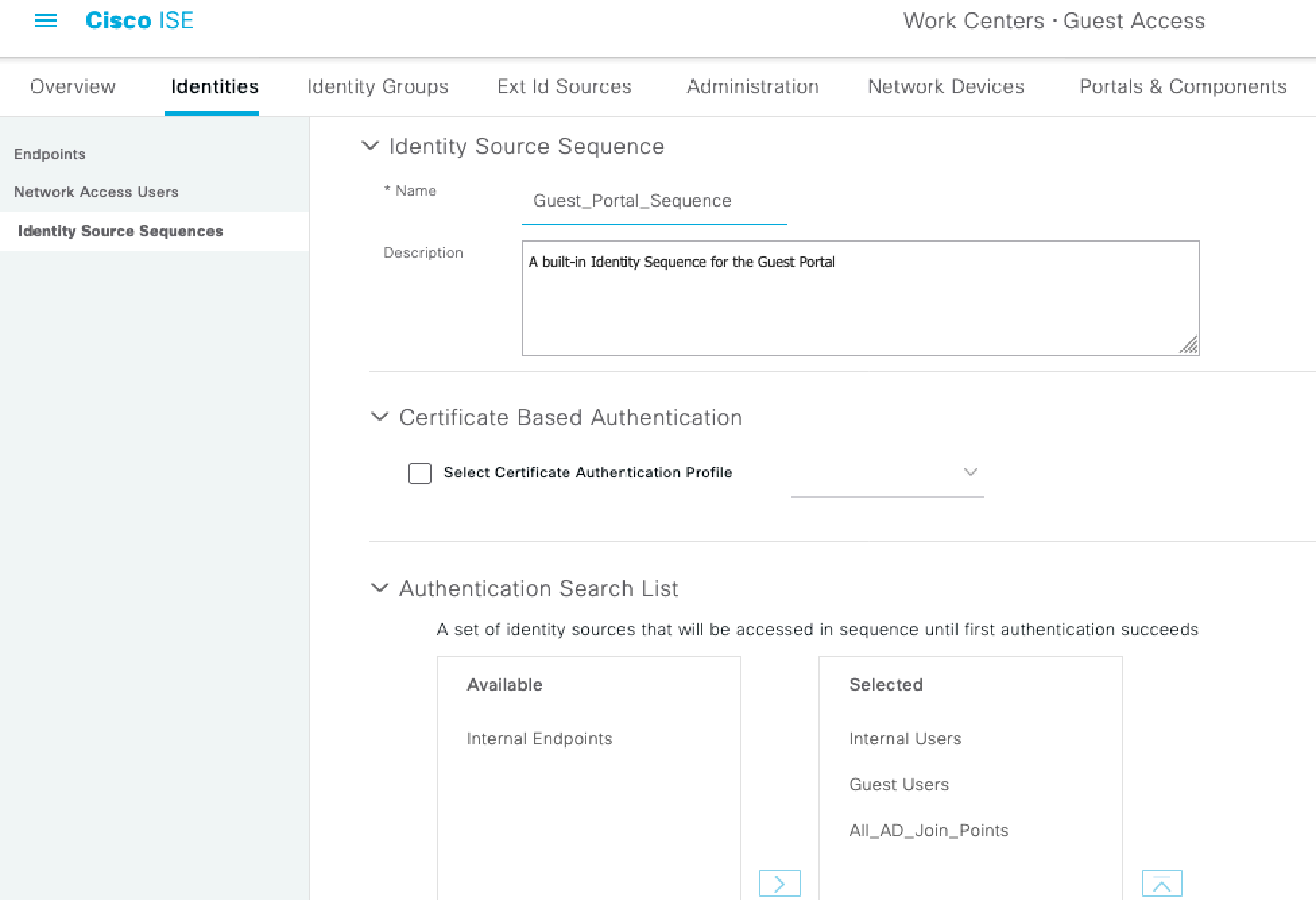
Work Centers > Guest Access > Administration > System Certificates

Authentication method: * Guest_Portal_Sequence

Configure authentication methods at:

Work Centers > Guest Access > Identities > Identity Source Sequences

這是先嘗試內部使用者（在訪客使用者之前）然後嘗試新增AD憑據的內部儲存序列。由於高級設定將在無法訪問所選身份庫進行身份驗證時繼續進入序列中的下一個儲存，因此具有內部憑據或AD憑據的員工可以登入門戶。



Identity Source Sequence

* Name: Guest_Portal_Sequence

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

Certificate Based Authentication

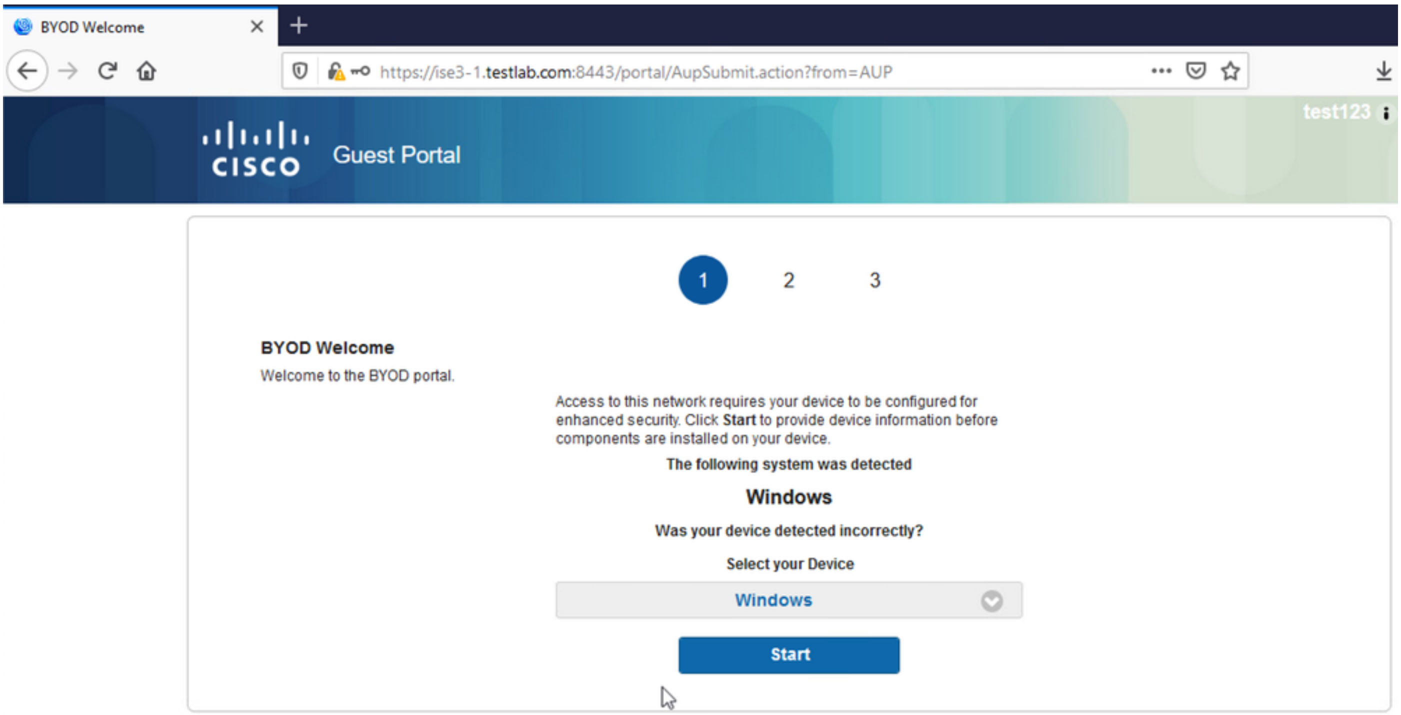
□ Select Certificate Authentication Profile

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

在訪客門戶的此階段，使用者提供在內部使用者儲存或Active Directory中定義的憑證，並進行BYOD重定向：


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

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

這樣，企業使用者可以針對個人裝置執行BYOD。

當提供訪客使用者憑證而不是內部使用者/AD憑證時，繼續正常流程（無BYOD）。

VLAN更改

它允許您運行activeX或Java小程式，從而觸發DHCP的釋放和續訂。當CoA觸發終端的VLAN更改時，需要執行此操作。使用MAB時，終端並不知道VLAN的變化。一種可能的解決方案是使用NAC代理更改VLAN（DHCP發佈/更新）。另一種方法是通過網頁上返回的小程式請求新的IP地址。可以配置發佈/CoA/續訂之間的延遲。流動裝置不支援此選項。

相關資訊

- 思科ISE上的終端安全評估服務配置指南
- 帶身份服務引擎的無線BYOD
- 適用於BYOD的ISE SCEP支援配置示例
- WLC 和 ISE 的中央 Web 驗證的組態範例
- 使用ISE的WLC上使用FlexConnect AP進行中央Web身份驗證的配置示例
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。