

解決常見ISE訪客訪問問題

目錄

[簡介](#)

[必備條件](#)

[需求](#)

[採用元件](#)

[訪客流量](#)

[通用部署指南](#)

[經常遇到的問題](#)

[重新導向至訪客輸入網站無法運作](#)

[動態授權失敗](#)

[未傳送SMS/電子郵件通知](#)

[無法訪問「管理帳戶」頁](#)

[門戶證書最佳實踐](#)

[相關資訊](#)

簡介

本文說明如何解決部署中的常見訪客問題、如何隔離和檢查問題以及要嘗試的簡單解決方法。

必備條件

需求

思科建議您瞭解以下主題：

- ISE訪客配置
- 網路接入裝置(NAD)上的CoA配置
- 需要在工作站上捕獲工具。

採用元件

本檔案中的資訊是根據 Cisco ISE版本2.6和：

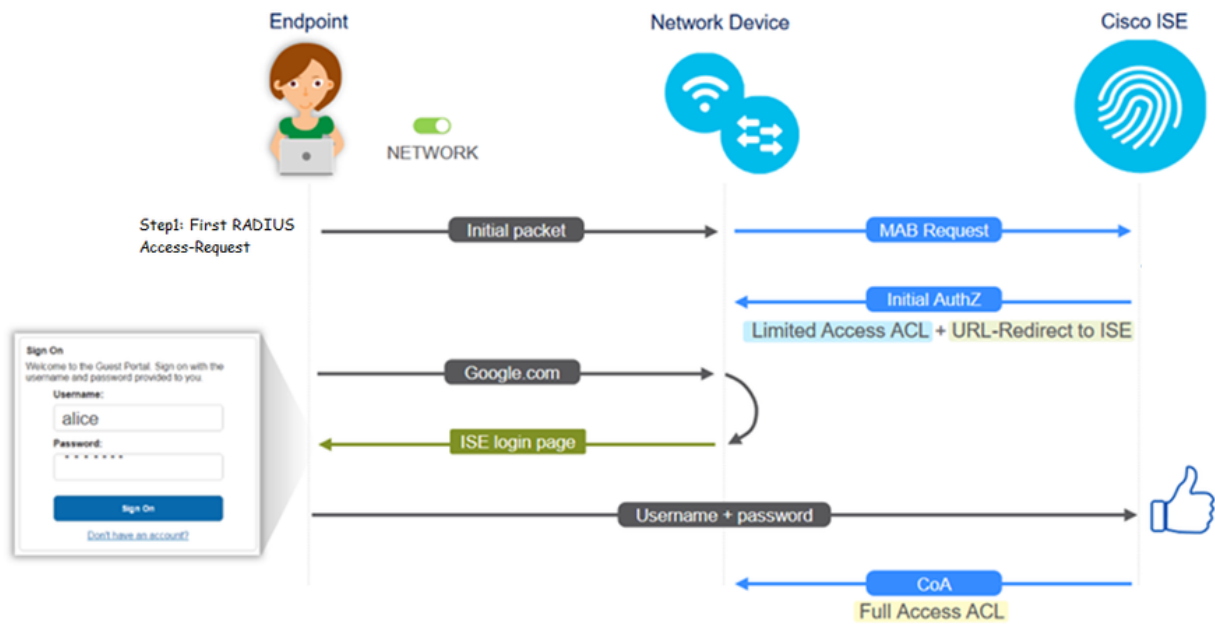
- WLC 5500
- Catalyst交換器3850 15.x版本
- Windows 10工作站

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。

訪客流量

訪客流概述類似於有線或無線設定。此流程圖影象可用於在文檔中參考。它有助於直觀地顯示步驟

和實體。



通過過濾終端ID，還可以在ISE即時日誌[Operations > RADIUS Live Logs]上跟蹤該流：

- MAB Authentication successful — 使用者名稱欄位具有MAC地址 — 將URL推送到NAD — 使用者獲取入口
- Guest Authentication successful - username欄位具有訪客使用者名稱，它被標識為 GuestType_Daily (或為訪客使用者配置的型別)
- CoA initiated — 使用者名稱欄位為空，詳細報告顯示動態授權成功
- 已提供訪客訪問許可權

影象中的事件序列 (從下到上)

Timestamp	Status	Username	MAC Address	Device	Access Type	Permissions	IP Address	Network	Authentication Method	User Identity	Group	Source
May 15, 2020 01:34:18.290 AM	Success	testquest	84:96:91:26:DD:8D	Windows 10...	Guest Access	Guest Acces... PermiAccess	10.106.37.15	DefaultNetwork...	TenGigabitEther...	User Identity Groups G		sotumu26
May 15, 2020 01:34:18.269 AM	Success	testquest	84:96:91:26:DD:8D					DefaultNetwork...				sotumu26
May 15, 2020 01:34:14.446 AM	Success	testquest	84:96:91:26:DD:8D				10.106.37.15			GuestType_Daily (defa		sotumu26
May 15, 2020 01:22:50.904 AM	Success		84:96:91:26:DD:8D	Intel-Device	Guest Acces...	Guest Acces... Guest_redirect	10.106.37.15	DefaultNetwork...	TenGigabitEther...	Profiled		sotumu26

通用部署指南

以下是一些配置幫助的連結。對於任何特定使用案例故障排除，了解理想或預期配置會有所幫助。

- [有線訪客組態](#)
- [無線訪客配置](#)
- [含FlexAuth AP的無線訪客CWA](#)

經常遇到的問題

本檔案主要解決以下問題：

重新導向至訪客輸入網站無法運作

從ISE推送重定向URL和ACL後，請檢查以下內容：

1. 使用 `show authentication session int <interface> details` 指令設定交換器上的使用者端狀態 (如果

有線訪客存取) :

```
questlab#sh auth sess int Tl/0/48 de
      Interface: TenGigabitEthernet1/0/48
      IIF-ID: 0x1096380000001DC
      MAC Address: b496.9126.dd6d
      IPv6 Address: Unknown
      IPv4 Address: 10.106.37.18
      User-Name: B4-96-91-26-DD-6D
      Status: Authorized
      Domain: DATA
      Oper host mode: single-host
      Oper control dir: both
      Session timeout: N/A
      Restart timeout: N/A
      Common Session ID: 0A6A2511000012652C64B014
      Acct Session ID: 0x0000124F
      Handle: 0x5E00014D
      Current Policy: POLICY_Tel/0/48

Local Policies:
  Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
  Security Policy: Should Secure
  Security Status: Link Unsecure

Server Policies:
  URL Redirect: https://10.127.197.212:8443/portal/gateway?sessionId=0A6
A2511000012652C64B014&portal=26d19560-2e58-11e9-98fb-0050568775a3&action=cwa&tok
en=66bbf9ce930a43142fe26b9d9577971de
  URL Redirect ACL: REDIRECT_ACL

Method status list:
  Method      State
  mab         Authc Success
```

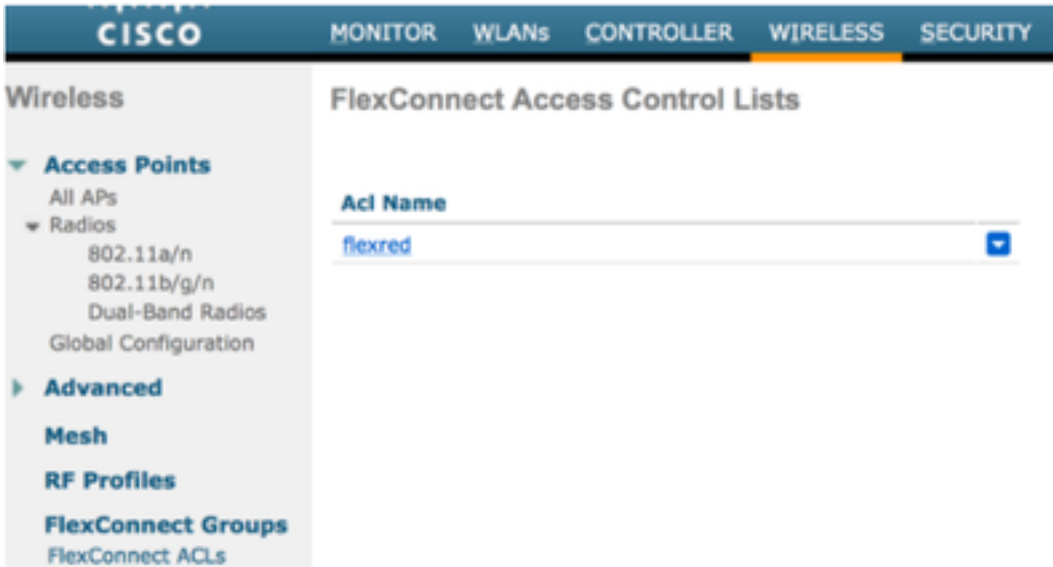
2.無線LAN控制器上的使用者端狀態 (如果無線訪客存取) : Monitor > Client > MAC address

Security Information	
Security Policy Completed	No
Policy Type	N/A
Auth Key Mgmt	N/A
Encryption Cipher	None
EAP Type	N/A
SNMP NAC State	Access
Radius NAC State	CENTRAL_WEB_AUTH
CTS Security Group Tag	Not Applicable
AAA Override ACL Name	cwa_redirect
AAA Override ACL Applied Status	Yes
AAA Override Flex ACL	none
AAA Override Flex ACL Applied Status	Unavailable
Redirect URL	https://10.127.197.212:8443/portal/gateway?sessionId=0

3.藉助命令提示符，從終端到TCP埠8443上ISE的可達性 : C:\Users\user>telnet <ISE-IP> 8443

4.如果門戶重定向URL具有FQDN，請檢查客戶端是否可以從命令提示符進行解析 : C:\Users\user>nslookup guest.ise.com

5.在flex connect設定中，確保在ACL和flex ACL下配置相同的ACL名稱。此外，驗證ACL是否已對映到AP。有關詳細資訊，請參閱上一節中的配置指南 — 步驟7b和c。



6.從使用者端擷取封包，並檢查重新導向。移動的資料包HTTP/1.1 302頁面表示WLC/交換機將訪問站點重定向到ISE訪客門戶（重定向的URL）：

ip.addr==2.2.2.2

No.	Arrival Time	Source	Destination	Protocol	Info
190	May 18, 2020 14:29:13.49400500...	10.106.37.18	2.2.2.2	TCP	54571 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
191	May 18, 2020 14:29:13.49657400...	2.2.2.2	10.106.37.18	TCP	80 → 54571 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=1460
192	May 18, 2020 14:29:13.49670300...	10.106.37.18	2.2.2.2	TCP	54571 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
194	May 18, 2020 14:29:13.69293900...	2.2.2.2	10.106.37.18	TCP	[TCP Dup ACK 191#1] 80 → 54571 [ACK] Seq=1 Ack=1 Win=4128 Len=0
218	May 18, 2020 14:29:16.34762700...	10.106.37.18	2.2.2.2	HTTP	GET / HTTP/1.1
219	May 18, 2020 14:29:16.35025300...	2.2.2.2	10.106.37.18	HTTP	HTTP/1.1 302 Page Moved
220	May 18, 2020 14:29:16.35047200...	2.2.2.2	10.106.37.18	TCP	80 → 54571 [FIN, PSH, ACK] Seq=279 Ack=329 Win=3800 Len=0
221	May 18, 2020 14:29:16.35050600...	10.106.37.18	2.2.2.2	TCP	54571 → 80 [ACK] Seq=329 Ack=280 Win=63962 Len=0
222	May 18, 2020 14:29:16.35064600...	10.106.37.18	2.2.2.2	TCP	54571 → 80 [FIN, ACK] Seq=329 Ack=280 Win=63962 Len=0
224	May 18, 2020 14:29:16.35466100...	2.2.2.2	10.106.37.18	TCP	80 → 54571 [ACK] Seq=280 Ack=330 Win=3800 Len=0

219 May 18, 2020 14:29:16.3502... 2.2.2.2 10.106.37.18 HTTP HTTP/1.1 302 Page Moved

```

> Frame 219: 332 bytes on wire (2656 bits), 332 bytes captured (2656 bits) on interface 0
> Ethernet II, Src: Cisco_ca:08:c5 (08:87:31:ca:08:c5), Dst: IntelCor_26:dd:6d (b4:96:91:26:dd:6d)
> Internet Protocol Version 4, Src: 2.2.2.2, Dst: 10.106.37.18
> Transmission Control Protocol, Src Port: 80, Dst Port: 54571, Seq: 1, Ack: 329, Len: 278
> Hypertext Transfer Protocol
  > HTTP/1.1 302 Page Moved
    Location: https://10.127.197.212:8443/portal/gateway?sessionId=046A2511000012652C648014&portal=26d19560-2e58-11e9-98fb-0050568775a3&action=cwa&token=66bbfce930a43142fe26b9d9577971de&redirect=http://2.2.2.2/
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.002626000 seconds]
    [Request in frame: 218]
    [Request URI: http://2.2.2.2/]
  
```

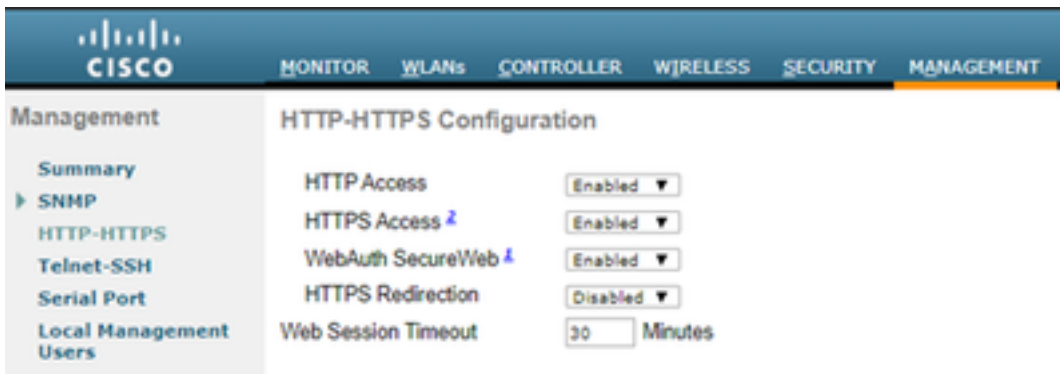
7.在網路訪問裝置上啟用HTTP(s)引擎：

在switch:

```

guestlab#sh run | in ip http
ip http server
ip http secure-server
  
```

在WLC上：

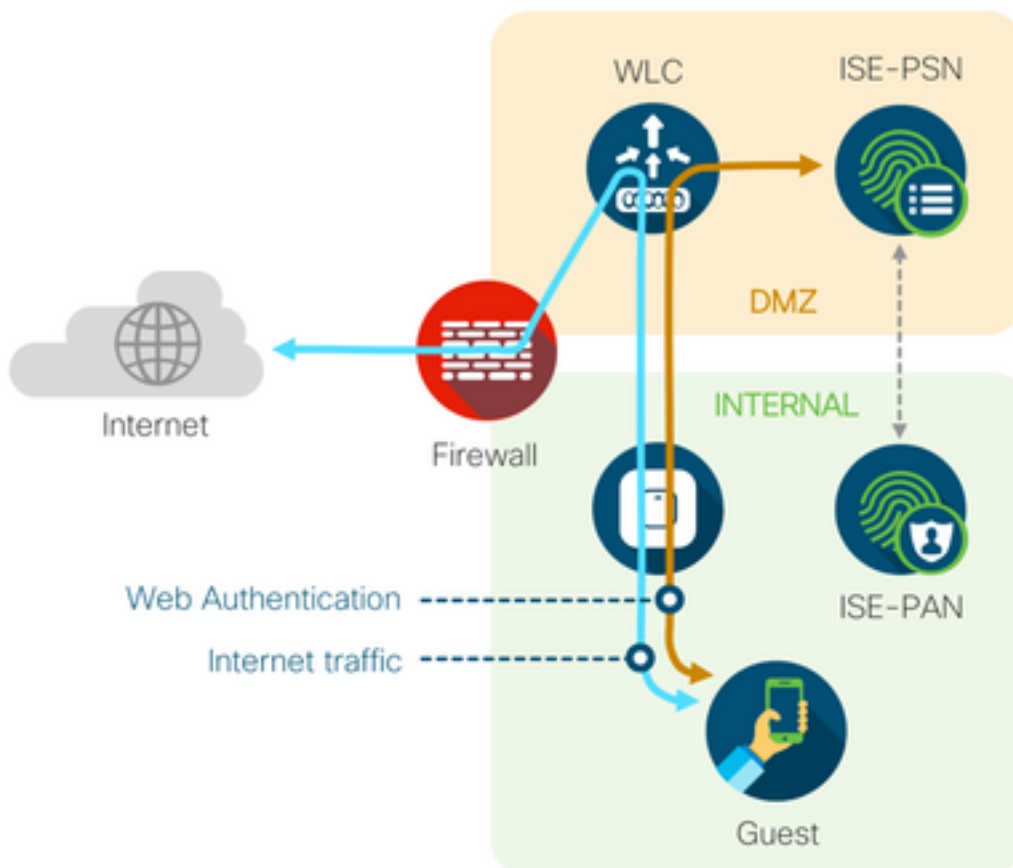


8. 如果WLC處於外部錨點設定中，請檢查以下專案：

步驟1. 兩個WLC上的使用者端狀態必須相同。

步驟2. 必須在兩個WLC上看到重新導向URL。

步驟3. 必須在錨點WLC上禁用RADIUS記帳。



動態授權失敗

如果終端使用者能夠訪問訪客門戶並成功登入，則下一步將是更改授權，向使用者授予完全訪客訪問許可權。如果這不起作用，您會看到ISE Radius Live Logs上的動態授權失敗。若要修正問題，請檢查以下專案：

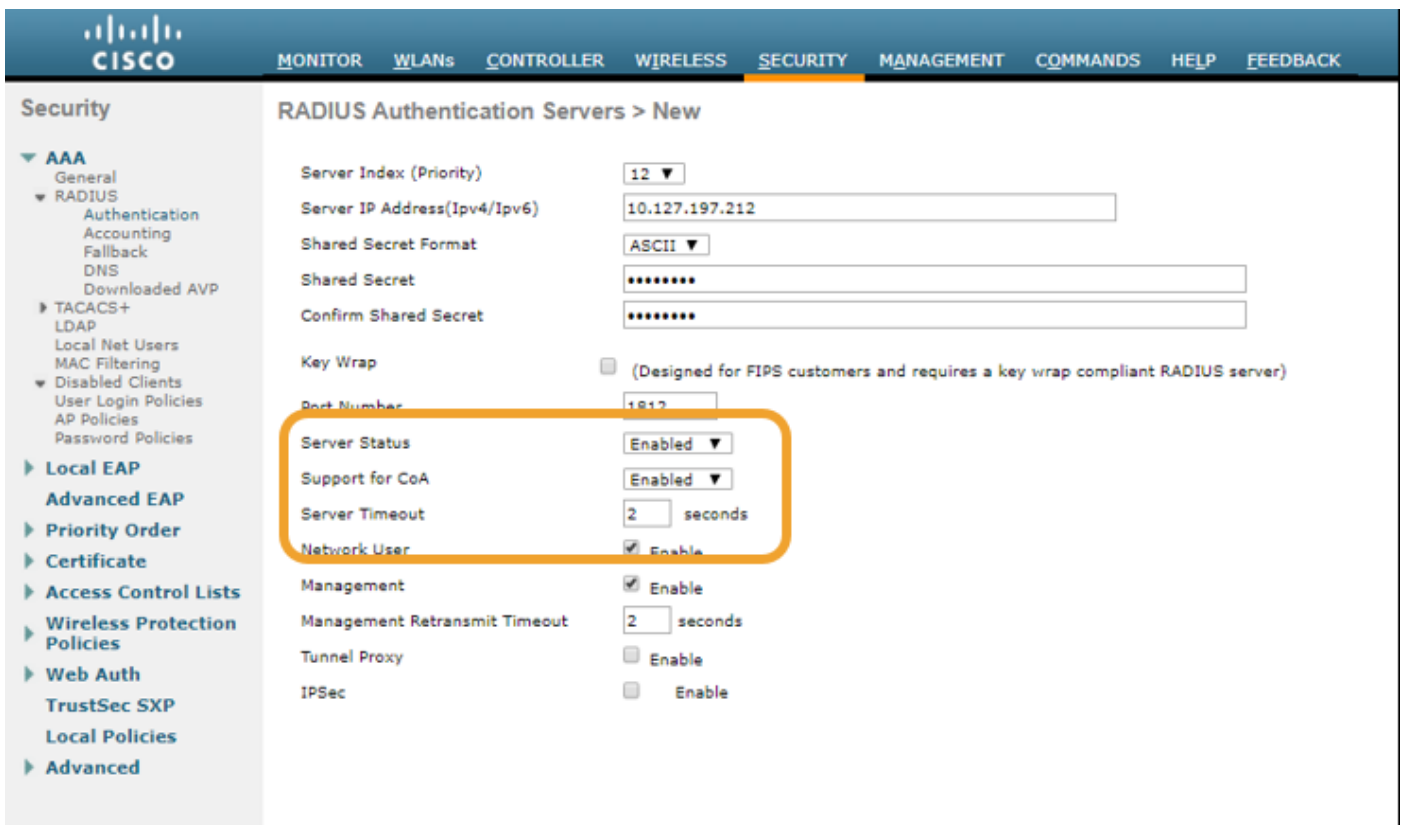
Overview	
Event	5417 Dynamic Authorization failed
Username	
Endpoint Id	MAC ADDRESS
Endpoint Profile	
Authorization Result	

Steps

- 11204 Received reauthenticate request
- 11220 Prepared the reauthenticate request
- 11100 RADIUS-Client about to send request - (port = 1700 , type = Cisco CoA)
- 11104 RADIUS-Client request timeout expired (🕒 Step latency=10003 ms)
- 11213 No response received from Network Access Device after sending a Dynamic Authorization request

1. 必須在NAD上啟用/配置授權變更(CoA):

```
!
aaa server radius dynamic-author
  client 10.127.197.209 server-key cisco123
  client 10.127.197.212 server-key cisco123
!
```



2. 防火牆上必須允許UDP埠1700。

3. WLC上的NAC狀態不正確。在WLC GUI > WLAN上的Advanced settings下，將NAC狀態更改為ISE NAC。

Advanced

802.11a/n (1 - 255)

802.11b/g/n (1 - 255)

NAC

NAC State

Load Balancing and Band Select

Client Load Balancing

Client Band Select

未傳送SMS/電子郵件通知

1. 檢查管理>系統>設定> SMTP下的SMTP配置。

2. 檢查ISE以外的SMS/電子郵件網關的API:

測試供應商在API客戶端或瀏覽器上提供的URL，替換使用者名稱、密碼、手機號碼等變數，並測試可訪問性。[Administration > System > Settings > SMS Gateways]

SMS Gateway Provider List > Global Default

SMS Gateway Provider

SMS Gateway Provider Name: *

Select Provider Interface Type:

SMS Email Gateway

SMS HTTP API

URL: *

Data (Url encoded portion):

Use HTTP POST method for data portion

或者，如果您從ISE發起人組[Workcenters > Guest Access > Portals and Components > Guest Types]進行測試，則在ISE和SMS/SMTP網關上捕獲資料包以檢查是否

1. 請求資料包未經篡改即可到達伺服器。
2. ISE伺服器具有供應商推薦的網關處理此請求的許可權/許可權。

Account Expiration Notification

Send account expiration notification days before account expires ⓘ

View messages in:

Email

Send a copy of the notification email to the Sponsor

Use customization from:

Messages: Copy text from:

Send test email to me at:

Configure SMTP server at: [Work Centers > Guest Access > Administration > SMTP server](#)

SMS

Messages: Copy text from:

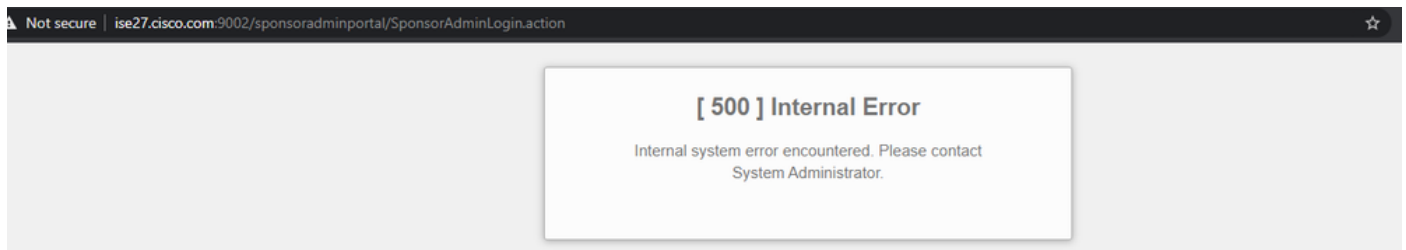
(160 character limit per message)*Over 160 characters requires multiple messages.

Send test SMS to me at:

Configure SMS service provider at: [Work Centers > Guest Access > Administration > SMS Gateway Providers](#)

無法訪問「管理帳戶」頁

1.在Workcenters > Guest Access > Manage accounts按鈕下，重定向到埠9002上的ISE FQDN，ISE管理員可以訪問發起人門戶：



2.使用nslookup <FQDN of ISE PAN>命令檢查訪問發起人門戶的工作站是否解析了FQDN。

3.使用show ports命令檢查ISE TCP埠9002是否從ISE的CLI開啟 |包括9002。

門戶證書最佳實踐

- 為了獲得無縫的使用者體驗，用於門戶和管理員角色的證書必須由著名的公共證書頒發機構（例如：GoDaddy、DigiCert、VeriSign等）進行簽名，瀏覽器通常信任該機構（例如：Google Chrome、Firefox等）。
- 建議不要將靜態IP用於訪客重定向，因為這會使ISE的私有IP對所有使用者可見。大多數供應商不提供第三方簽名的私有IP證書。
- 當您從ISE 2.4 p6移至p8或p9時，有一個已知的錯誤：思科錯誤ID [CSCvp75207](#)，其中Trust for authentication within ISE和Trust for client authentication框在修補程式升級後必須手動選中。這可確保ISE在訪問訪客門戶時發出TLS流的完整證書鏈。

如果這些操作不能解決訪客訪問問題，請聯絡TAC，使用從文檔[Debugs to enable on ISE](#)收集的支

[援捆綁包。](#)

相關資訊

- [思科技術支援與下載](#)

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）。