

# Troubleshoot Common ISE Guest Access Issues

## Contents

---

### [Introduction](#)

### [Prerequisite](#)

[Requirements](#)

[Components Used](#)

### [Guest Flow](#)

### [Common Deployment Guides](#)

### [Frequently Encountered Issues](#)

[Redirection to the Guest Portal Does Not Work](#)

[Dynamic Authorization Fails](#)

[SMS/EMAIL Notifications Are Not Sent](#)

[Manage the Accounts Page is Not Reachable](#)

[Portal Certificate Best Practices](#)

### [Related Information](#)

---

## Introduction

This document describes how to troubleshoot common guest issues in deployment, how to isolate and check the issue, and simple workarounds to try.

## Prerequisite

### Requirements

Cisco recommends that you have knowledge of these topics:

- ISE guest configuration
- CoA configuration on Network Access Devices(NAD)
- Capture tools on workstations are required.

### Components Used

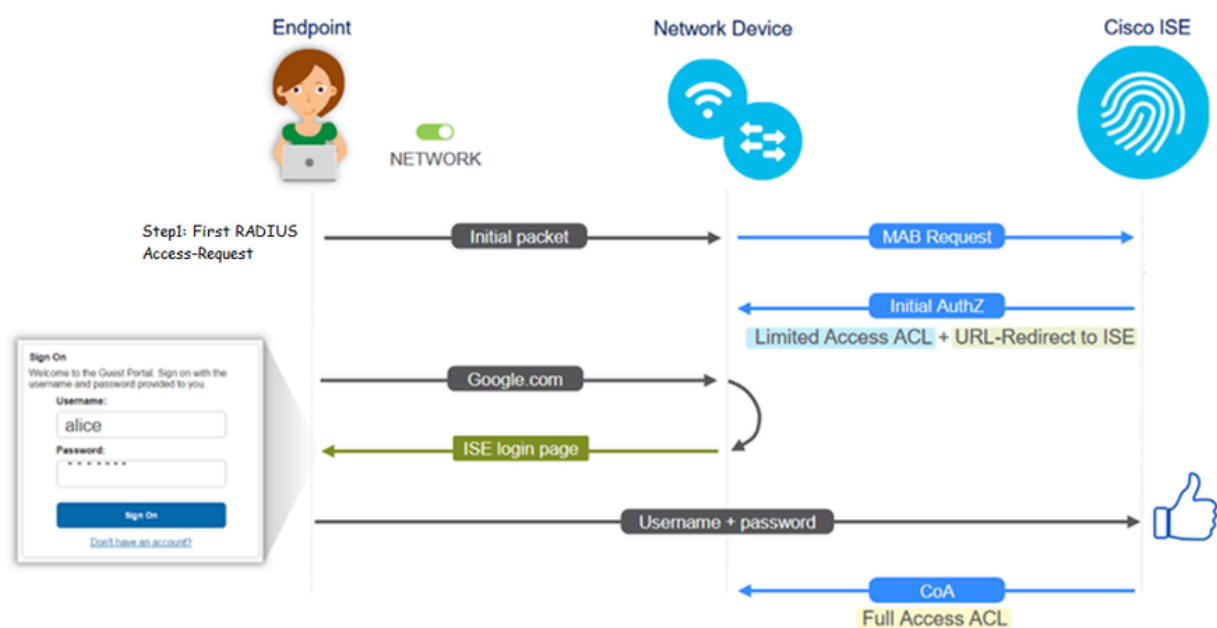
The information in this document is based on Cisco ISE, Release 2.6, and:

- WLC 5500
- Catalyst switch 3850 15.x version
- Windows 10 workstation

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Guest Flow

The guest flow overview is similar to wired or wireless setups. This image of the flow diagram can be used for reference throughout the document. It helps to visualize the step and the entity.



The flow can also be followed on ISE live logs [**Operations > RADIUS Live Logs**] by filtering the endpoint ID:

- MAB Authentication successful– username field has the MAC address- URL is pushed to the NAD - User gets the portal
- Guest Authentication successful- username field has the guest username, it has been identified as GuestType\_Daily (or the configured type for the guest user)
- CoA initiated- username field is blank, detailed report shows Dynamic Authorization successful
- Guest Access provided

The sequence of events in the image (bottom to top):

May 18, 2020 01:34:18.290 AM	✔	🔍	testguest	84:96:91:26:DD:8D	Windows10...	Guest Access	Guest Acces...	PermAccess	10.106.37.18	DefaultNetwork...	TenGigabitEther...	User Identity Groups G	sotumu26
May 18, 2020 01:34:18.269 AM	✔	🔍		84:96:91:26:DD:8D						DefaultNetwork...			sotumu26
May 18, 2020 01:34:14.446 AM	✔	🔍	testguest	84:96:91:26:DD:8D					10.106.37.18			GuestType_Daily (defa	sotumu26
May 18, 2020 01:22:50.904 AM	✔	🔍		84:96:91:26:DD:8D	Intel-Device	Guest Acces...	Guest Acces...	Guest_redirect	10.106.37.18	DefaultNetwork...	TenGigabitEther...	Profiled	sotumu26

## Common Deployment Guides

Here are some links for configuration assistance. For any specific use case troubleshooting, it helps to be aware of the ideal or expected configuration.

- [Wired Guest Configuration](#)
- [Wireless Guest Configuration](#)
- [Wireless Guest CWA with FlexAuth APs](#)

## Frequently Encountered Issues

This document primarily addresses these issues:

### Redirection to the Guest Portal Does Not Work

Once the redirect URL and ACL are pushed from ISE, check these:

1. The client status on the switch (if wired guest access) with the command **show authentication session int <interface> details**:

```
questlab#sh auth sess int T1/0/48 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=66bbf3ce930a43142fe26b9d9577971de
  URL Redirect ACL: REDIRECT_ACL

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

2. The client status on the Wireless LAN Controller (if wireless guest access): **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	<a href="http://10.10.10.10:8443/portal/gateway?sessionId=0">http://10.10.10.10:8443/portal/gateway?sessionId=0</a>

3. The reachability from the endpoint to the ISE on TCP port 8443 with the help of command prompt: **C:\Users\user>telnet <ISE-IP> 8443.**

4. If the portal redirect URL has an FQDN, check if the client is able to resolve from the command prompt: **C:\Users\user>nslookup guest.ise.com.**

5. In flex connect setup, ensure the same ACL name is configured under ACL and flex ACLs. Also, verify if the ACL is mapped to the APs. Refer to the config guide from the previous section-Steps 7 b and c for more information.

**CISCO**    **MONITOR**    **WLANs**    **CONTROLLER**    **WIRELESS**    **SECURITY**

**Wireless**

- Access Points
  - All APs
  - Radios
    - 802.11a/n
    - 802.11b/g/n
    - Dual-Band Radios
    - Global Configuration
- Advanced
  - Mesh
  - RF Profiles
  - FlexConnect Groups
  - FlexConnect ACLs

**FlexConnect Access Control Lists**

**Acl Name**

**flexred**

6. Take a packet capture from the client, and check for the redirection. The packet HTTP/1.1 302 Page Moved is to indicate the WLC/Switch redirected the accessed site to the ISE guest portal (redirected 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:0e:c5 (00:07:31:ca:0e: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\r\n
    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/\r\n
    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. HTTP(s) engine is enabled on the Network Access Devices:

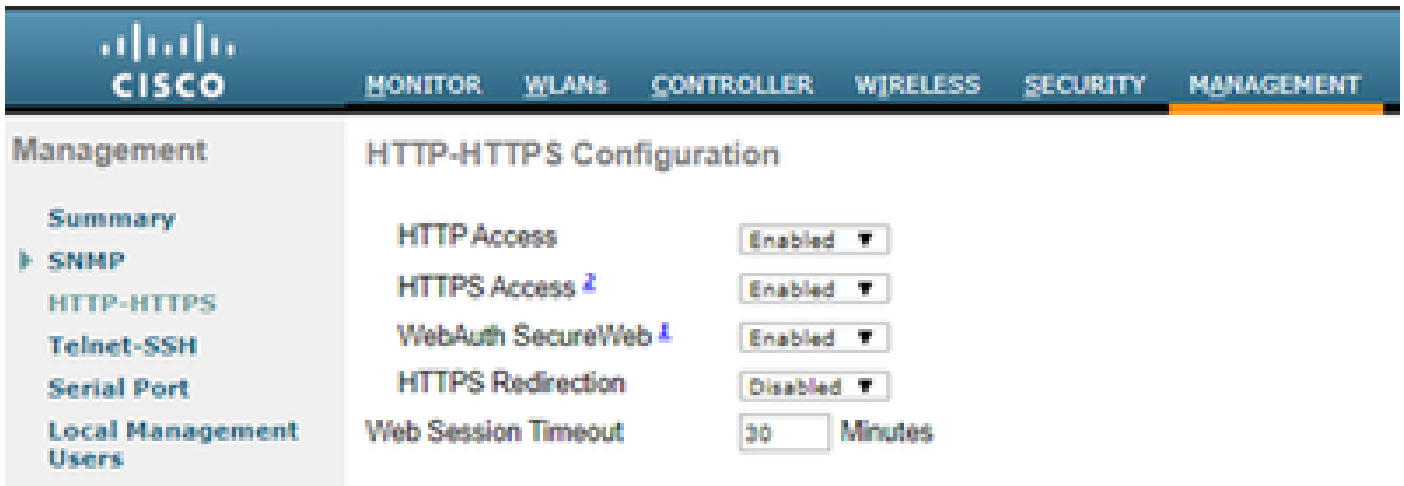
- On the switch:

```

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

```

- On the WLC:

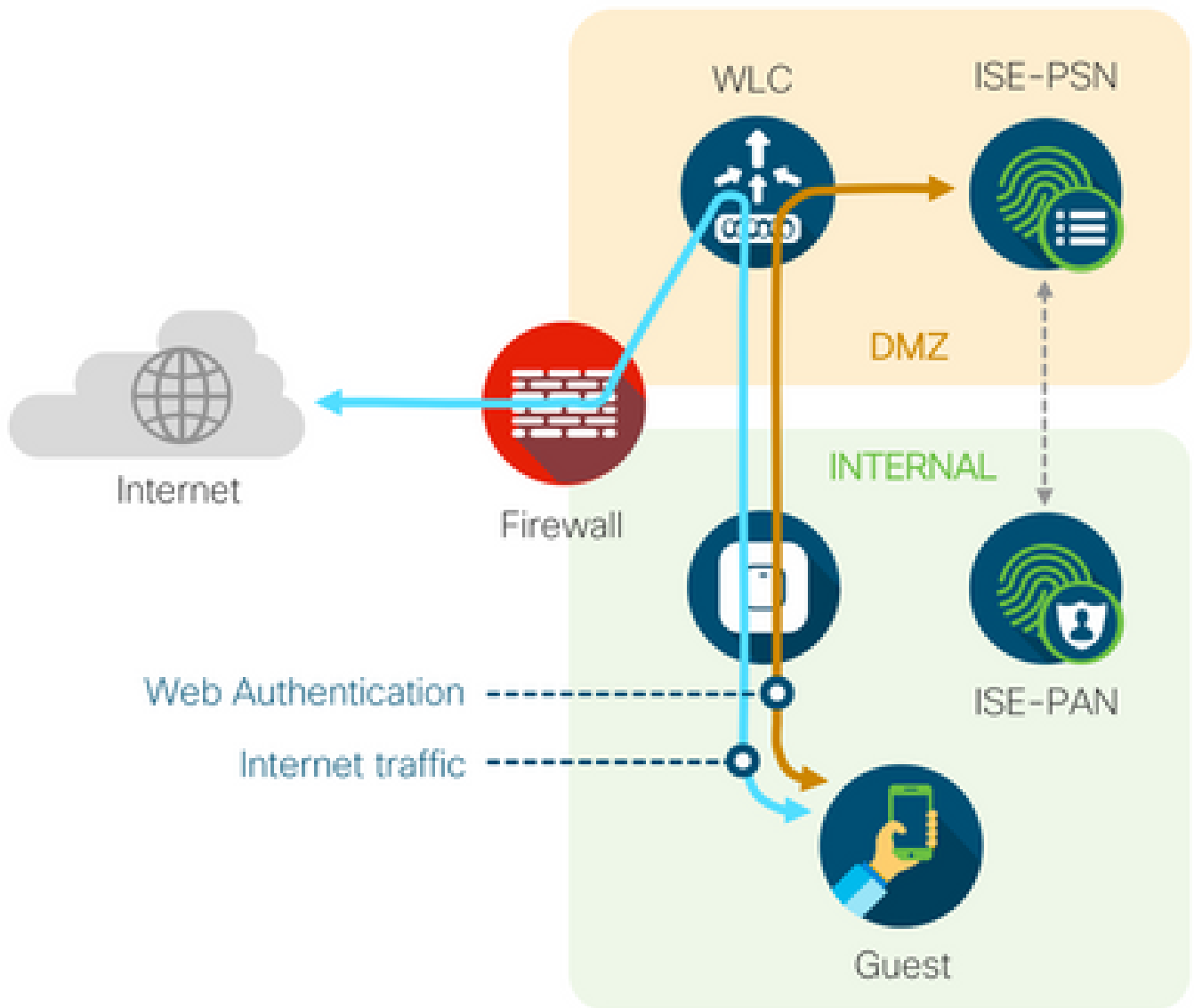


8. If the WLC is in a foreign-anchor setup, check these:

Step 1. The client status must be the same on both the WLCs.

Step 2. Redirect URL must be seen on both the WLCs.

Step 3. RADIUS Accounting must be disabled on the anchor WLC.



## Dynamic Authorization Fails

If the end-user is able to access the guest portal and log in successfully, the next step would be a change of authorization to give full guest access to the user. If this does not work, you see a Dynamic Authorization failure on ISE Radius Live Logs. To remedy the issue, check these:

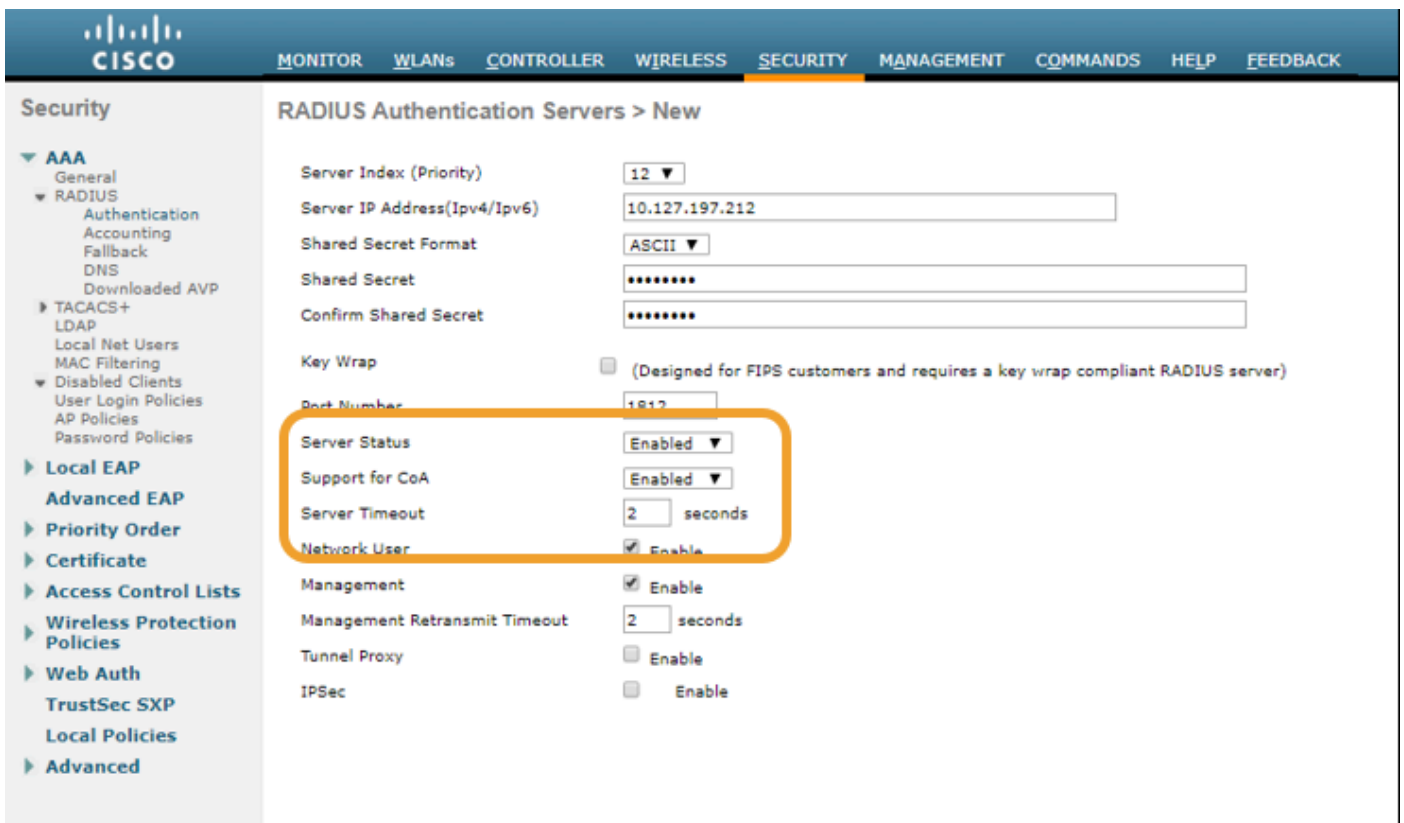
Overview	
Event	5417 Dynamic Authorization failed
Username	
Endpoint Id	MAC ADDRESS
Endpoint Profile	
Authorization Result	

### 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

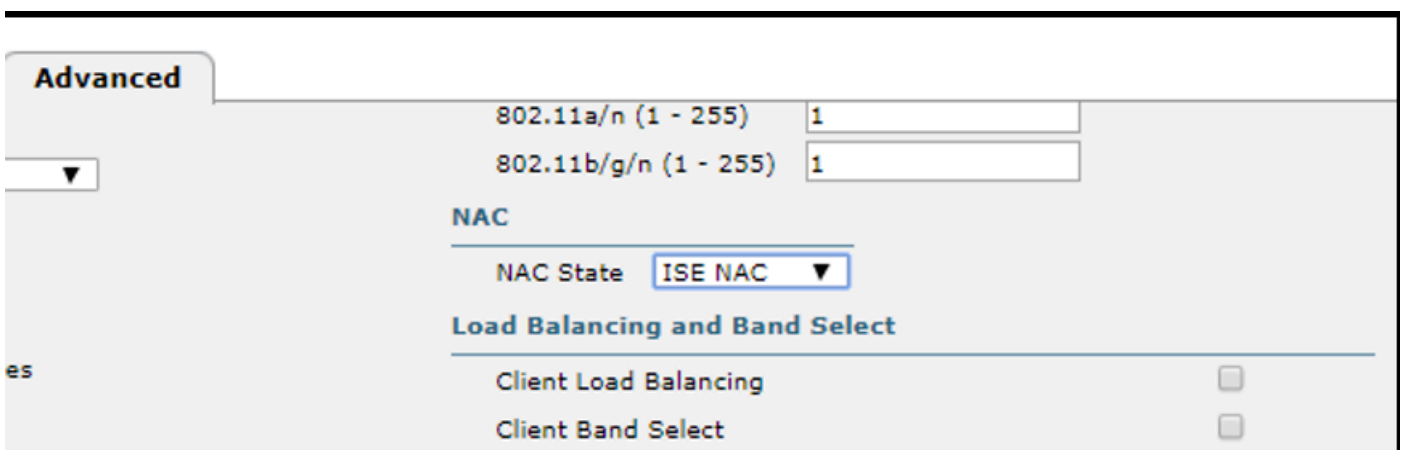
1. Change of Authorization (CoA) must be enabled/configured on the NAD:

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



2. UDP Port 1700 must be allowed on the firewall.

3. NAC state on WLC is incorrect. Under Advanced settings on **WLC GUI > WLAN**, change the NAC state to ISE NAC.





## SMS/EMAIL Notifications Are Not Sent

1. Check the SMTP configuration under **Administration > System > Settings > SMTP**.
2. Check the API for SMS/Email gateways outside ISE:

Test the URL(s) provided by the vendor on an API client or a browser, replace the variables like usernames, passwords, mobile number, and test the reachability [**Administration > System > Settings > SMS Gateways**].

SMS Gateway Provider List > Global Default

### SMS Gateway Provider

SMS Gateway Provider Name: \* **Global Default**

Select Provider Interface Type:

- SMS Email Gateway
- SMS HTTP API

URL: \* `http://api.clickatell.com/http/sendmsg?user=[USERNAME]&password=[PASSWORD]&api_i`

Data (Url encoded portion):

Use HTTP POST method for data portion

Alternatively, if you test from the ISE sponsor groups [**Workcentres > Guest Access > Portals and Components > Guest Types**], take a packet capture on ISE and the SMS/SMTP gateway to check if:

1. The request packet reaches the server untampered.
2. ISE server has the vendor recommended permissions/privilege for the gateway to process this request.

## Account Expiration Notification

Send account expiration notification  days before account expires [i](#)

View messages in:

Email

Send a copy of the notification email to the Sponsor

Use customization from:

Messages:

Copy text from:

Your account is going to expire in 3 days. Please notify your sponsor to extend your account now to avoid any delays.

Send test email to me at:

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

SMS

Messages:

Copy text from:

Your account is going to expire in 3 days. Please notify your sponsor to extend your account now to avoid any delays.

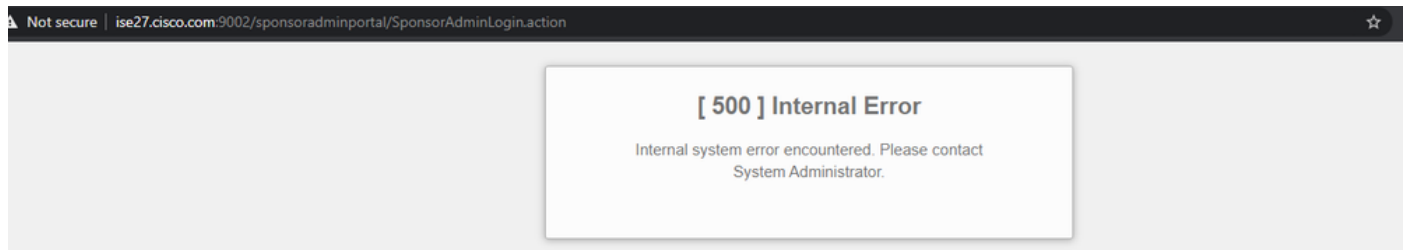
(160 character limit per message)\*Over 160 characters requires multiple messages.

Send test SMS to me at:

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

## Manage the Accounts Page is Not Reachable

1. The **Workcentres > Guest Access > Manage accounts** button redirects to the ISE FQDN on port 9002 for the ISE admin to access the sponsor portal:



2. Check if the FQDN is resolved by the workstation from which Sponsor Portal is accessed with the command **nslookup <FQDN of ISE PAN>**.

3. Check if ISE TCP port 9002 is open from the CLI of the ISE with the command **show ports | include 9002**.

## Portal Certificate Best Practices

- For a seamless user experience, the certificate used for portals and admin roles must be signed by a well-known public Certificate Authority (example: GoDaddy, DigiCert, VeriSign, etc), commonly trusted by browsers (example: Google Chrome, Firefox, and so on).
- It is not recommended to use a static IP for guest redirection, since that makes the private IP of ISE visible to all users. Most of the vendors do not provide third party-signed certificates for private IPs.
- When you move from ISE 2.4 p6 to p8 or p9, there is a known bug: Cisco bug ID [CSCyp75207](#), where the **Trust for authentication within ISE** and **Trust for client authentication and Syslog** boxes must be manually checked after the patch upgrade. This ensures

that ISE sends out the full cert chain for the TLS flow when the guest portal is accessed.

If these actions do not resolve guest access problems, please reach out to TAC with a support bundle collected with instructions from the document: [Debugs to enable on ISE](#).

## **Related Information**

- [Cisco Technical Support & Downloads](#)