

Problemen met algemene ISE-toegang voor gasten oplossen

Inhoud

[Inleiding](#)

[Voorwaarde](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Guest Flow](#)

[Gemeenschappelijke implementatiehandleidingen](#)

[Vaak voorkomende problemen](#)

[Omleiding naar de Gastenportal werkt niet](#)

[Dynamische autorisatie mislukt](#)

[Meldingen via sms/e-mail worden niet verzonden](#)

[De pagina Accounts beheren is niet bereikbaar](#)

[Portal Certificaat Beste praktijken](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u veel voorkomende gastproblemen in de implementatie kunt oplossen, hoe u het probleem kunt isoleren en controleren en hoe u eenvoudige tijdelijke oplossingen kunt proberen.

Voorwaarde

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ISE-gastconfiguratie
- CoA-configuratie op Network Access Devices (NAD)
- Er moeten opnametools op werkstations zijn.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco ISE, release 2.6 en:

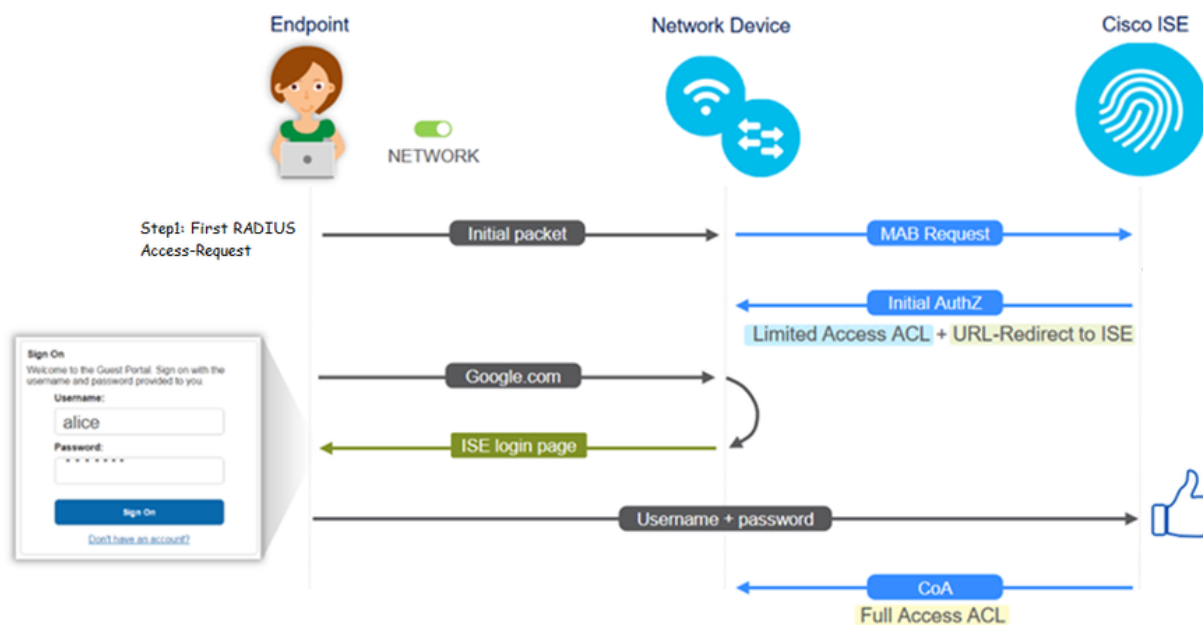
- WLC 5500
- Catalyst switch 3850 15.x versie
- Windows 10-werkstation

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële

impact van elke opdracht begrijpt.

Guest Flow

Het overzicht van de gaststroom is vergelijkbaar met bekabelde of draadloze instellingen. Deze afbeelding van het stroomschema kan worden gebruikt als referentie in het gehele document. Het helpt om de stap en de entiteit te visualiseren.



De stroom kan ook worden gevolgd op live ISE-logs [Operations > RADIUS Live Logs] door het filteren van de eindpunt-ID:

- MAB-verificatie succesvol - het veld gebruikersnaam heeft het MAC-adres - URL wordt naar de NAD gedrukt - Gebruiker krijgt het portal
- Gastverificatie succesvol - het gebruikersnaamveld heeft de gastgebruikersnaam, het is geïdentificeerd als GuestType_Daily (of het ingestelde type voor de gastgebruiker)
- CoA geïnitieerd - het gebruikersbenamingsveld is leeg, gedetailleerd rapport toont succesvolle Dynamische Vergunning
- Gasttoegang beschikbaar

De volgorde van de gebeurtenissen in het beeld (van onder naar boven)

Timestamp	Status	Endpoint ID	Username	MAC Address	Device	Access Type	Access Name	Permissions	IP Address	Network	Authentication Method	Group	Source
May 15, 2020 01:34:18.290 AM	✓	testguest		84 96 91 26 DD 8D	Windows15...	Guest Access	Guest Acces...	PermiAccess	10.106.37.15	DefaultNetwork...	TenGigabitEthe...	User Identity Groups G	sotumu26
May 15, 2020 01:34:18.269 AM	✓	testguest		84 96 91 26 DD 8D					10.106.37.15	DefaultNetwork...			sotumu26
May 15, 2020 01:34:14.446 AM	✓	testguest		84 96 91 26 DD 8D					10.106.37.15			GuestType_Daily (defa	sotumu26
May 15, 2020 01:22:50.904 AM	✓	84 96 91 26 DD 8D		84 96 91 26 DD 8D	Intel-Device	Guest Acces...	Guest Acces...	Guest_redirect	10.106.37.15	DefaultNetwork...	TenGigabitEthe...	Profiled	sotumu26

Gemeenschappelijke implementatiehandleidingen

Hier zijn een aantal links voor hulp bij configuratie. Voor elk specifiek geval van probleemoplossing helpt het om zich bewust te zijn van de ideale of verwachte configuratie.

- [Gastconfiguratie via kabel](#)
- [Draadloze gastconfiguratie](#)
- [Draadloze gastgateway met FlexAuth AP's](#)

Vaak voorkomende problemen

In dit document komen deze kwesties vooral aan de orde:

Omleiding naar de Gastenportal werkt niet

Zodra de omleiding URL en ACL van ISE worden gedrukt, controleer deze:

1. De clientstatus op de switch (indien bekabelde gasttoegang) met de opdracht **toont verificatiesessie in <interface>-gegevens:**

```
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-00505668775a3&action=cwa&tok
en=66bbf9ce930a43142fe26b9d9577971de
  URL Redirect ACL: REDIRECT_ACL

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

2. De clientstatus op de draadloze LAN-controller (indien draadloze gasttoegang): **Monitor > Client > MAC-adres**

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	<http://10.10.10.10:8443/portal/gateway?sessionId=0

3. De bereikbaarheid van het eindpunt naar de ISE op TCP-poort 8443 met behulp van opdrachtprompt: **C:\Users\user>Telnet <ISE-IP> 843**

4. Als de portal URL een FQDN heeft, controleert u of de client kan oplossen via de opdrachtprompt: **C:\Users\user>nslookup guest.ise.com**

5. Zorg er in flex connect-instelling voor dat dezelfde ACL-naam is geconfigureerd onder ACL en flex ACL's. Controleer ook of de ACL op de AP is toegewezen. Raadpleeg de configuratiehandleiding van de vorige sectiestappen 7 b en c voor meer informatie.

The screenshot shows the Cisco FlexConnect configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', and 'SECURITY'. The 'WIRELESS' tab is active. On the left, the 'Wireless' menu is expanded to show 'Access Points' (with sub-items: All APs, Radios, 802.11a/n, 802.11b/g/n, Dual-Band Radios, Global Configuration) and 'Advanced' (with sub-items: Mesh, RF Profiles, FlexConnect Groups, FlexConnect ACLs). The main content area is titled 'FlexConnect Access Control Lists' and features a dropdown menu for 'Acl Name' with 'flexred' selected.

6. Neem een pakketopname van de client en controleer op de omleiding. Het pakket HTTP/1.1 302 Page Moved is om aan te geven dat de WLC/Switch de benaderde site naar het ISE guest portal heeft omgeleid (omgeleid URL):

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=0A6A2511000012652C648014&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. De HTTP(s)-engine is ingeschakeld op de netwerktoegangsapparaten:

Aan de switch:

```

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

Op de WLC:



The screenshot shows the Cisco WLC Management interface. The 'Management' tab is selected, and the 'HTTP-HTTPS Configuration' page is displayed. The configuration is as follows:

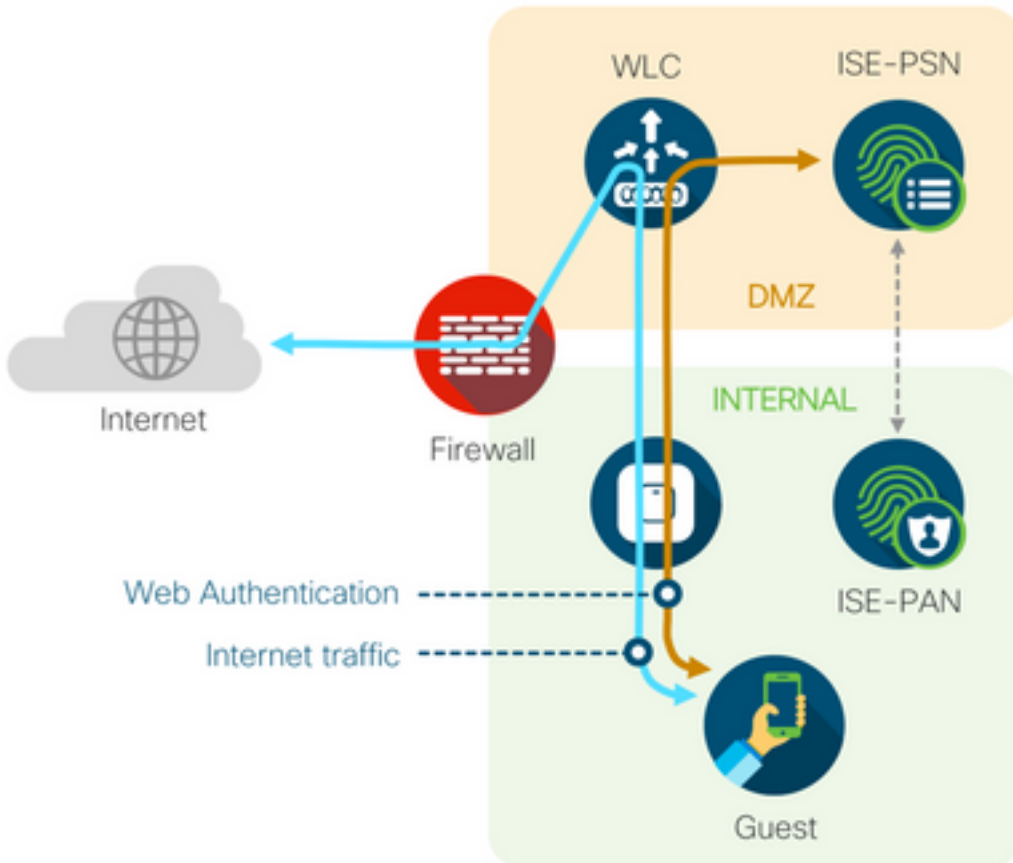
- HTTP Access: Enabled
- HTTPS Access: Enabled
- WebAuth SecureWeb: Enabled
- HTTPS Redirection: Disabled
- Web Session Timeout: 30 Minutes

8. Als de WLC in een instelling voor een buitenlands anker staat, controleert u deze:

Stap 1. De cliëntstatus moet het zelfde op beide WLCs zijn.

Stap 2. Redirect URL moet op beide WLCs worden gezien.

Stap 3. RADIUS-accounting moet op het anker WLC worden uitgeschakeld.



Dynamische autorisatie mislukt

Als de eindgebruiker toegang kan krijgen tot het gastportaal en met succes kan inloggen, is de volgende stap een wijziging van de autorisatie, om volledige gasttoegang te verlenen aan de gebruiker. Als dit niet werkt, zou u een Dynamische mislukking van de Vergunning op de Levende Logboeken van de Straal van ISE zien. Controleer het probleem op de volgende manieren:

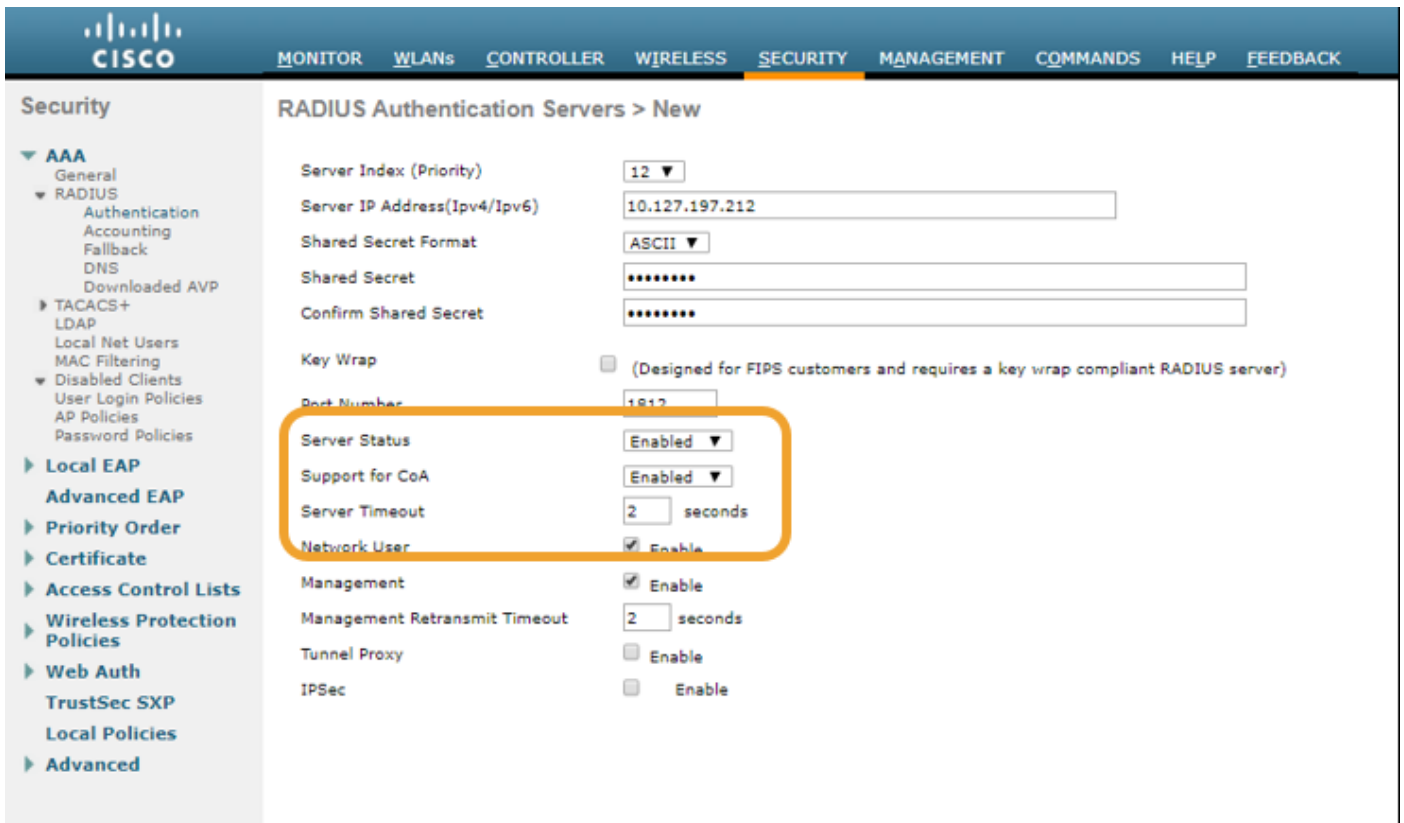
Overview	
Event	5417 Dynamic Authorization failed
Username	
Endpoint Id	MAC ADDRESS
Endpoint Profile	
Authorization Result	

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

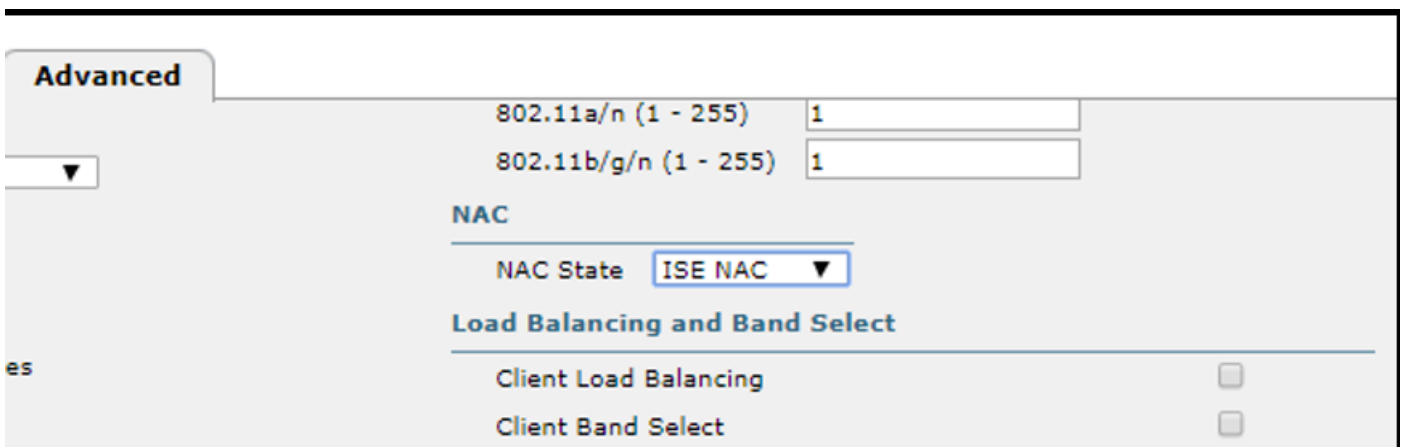
1. Wijziging van autorisatie (CoA) moet worden ingeschakeld/geconfigureerd op het NAD:

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



2. UDP-poort 1700 moet zijn toegestaan op de firewall.

3. De NAC-status op WLC is onjuist. Onder Geavanceerde instellingen voor WLC GUI > WLAN wijzigt u de NAC-status in ISE NAC.



Meldingen via sms/e-mail worden niet verzonden

1. Controleer de SMTP-configuratie onder **Beheer > Systeem > Instellingen > SMTP**.

2. Controleer de API op SMS-/e-mailgateways buiten ISE:

Test de URL(s) die door de verkoper op een API-client of een browser wordt geleverd, vervang de variabelen zoals gebruikersnaam, wachtwoorden, mobiel nummer en test de bereikbaarheid.

[**Beheer > Systeem > Instellingen > SMS-gateways**]

SMS Gateway Provider

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

Select Provider Interface Type:

SMS Email Gateway

SMS HTTP API

URL: *

Data (Url encoded portion):

Use HTTP POST method for data portion

Als u een test uitvoert vanuit de ISE-sponsorgroepen [**Workcentres > Guest Access > Portals and Components > Guest Types**], neem dan een pakketopname op ISE en de SMS/SMTP-gateway om te controleren of

1. Het verzoekpakket bereikt de server onaangetast.
2. ISE-server heeft de door de verkoper aanbevolen rechten/rechten voor de gateway om deze aanvraag te verwerken.

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.

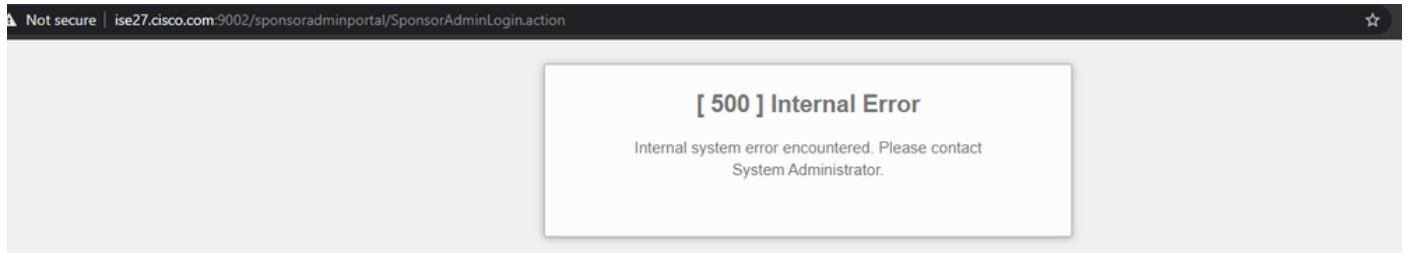
Send test SMS to me at:

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

De pagina Accounts beheren is niet bereikbaar

1. Onder de knop **Workcentres > Guest Access > Account beheren** wordt op poort 9002 omgeleid

naar de ISE FQDN, zodat de ISE-beheerder toegang heeft tot het sponsor-portal:



2. Controleer of de FQDN is opgelost door het werkstation vanwaar Sponsor Portal wordt benaderd met de opdracht **snackup <FQDN of ISE PAN>**.

3. Controleer of ISE TCP-poort 9002 open is vanaf de CLI van de ISE met de **opstartpoorten** van de opdracht | met inbegrip van **9002**.

Portal Certificaat Beste praktijken

- Voor een naadloze gebruikerservaring moet het certificaat dat wordt gebruikt voor portalen en beheerdersrollen worden ondertekend door een bekende openbare certificaatautoriteit (bijvoorbeeld: GoDaddy, DigiCert, VeriSign, enz.), die vaak wordt vertrouwd door browsers (bijvoorbeeld: Google Chrome, Firefox, enz.).
- Het is niet aan te raden om statische IP te gebruiken voor gastenomleiding, omdat dat de private IP van ISE zichtbaar maakt voor alle gebruikers. De meeste leveranciers bieden geen door derden ondertekende certificaten voor particuliere IP.
- Wanneer u van ISE 2.4 p6 naar p8 of p9 verhuist, is er een bekende bug: Cisco bug ID [CSCvp75207](#) waar het **vertrouwen voor verificatie binnen ISE** en **Trust voor client authenticatie en Syslog** vakjes handmatig moeten worden gecontroleerd na de patch upgrade. Dit zorgt ervoor dat ISE de volledige cert-keten voor TLS-stroom uitstuurt wanneer het gastportaal wordt benaderd.

Als deze acties geen problemen met de toegang van gasten oplossen, neem dan contact op met TAC met een ondersteuningsbundel die is verzameld met instructies uit het document: [Debugs om op ISE in te schakelen](#).

Gerelateerde informatie

- [Cisco technische ondersteuning en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.