Problemen met algemene ISE-toegang voor gasten oplossen

Inhoud

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:

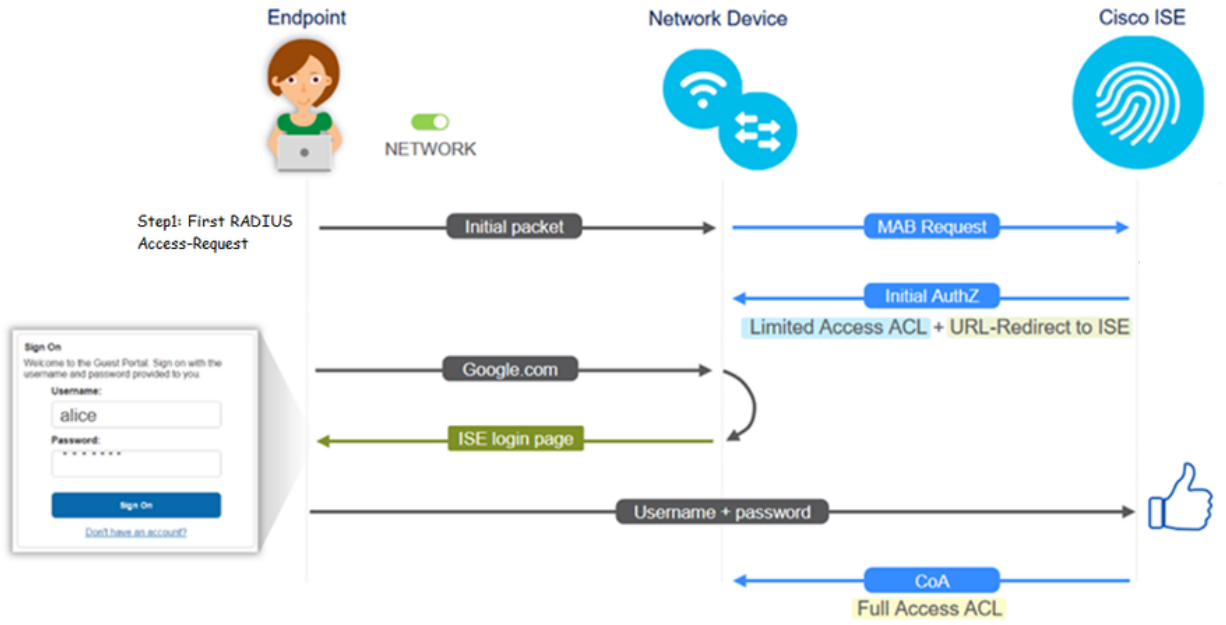
- WLC 5500
- Catalyst switch 3850 15.x versie
- Windows 10-werkstation

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

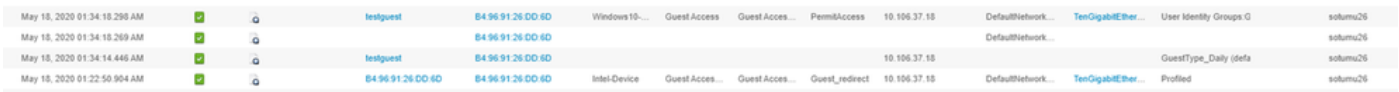
Het overzicht van de gaststroom is vergelijkbaar met bekabelde of draadloze instellingen. Deze afbeelding van het stroomschema kan worden gebruikt als referentie in het gehele document. Het helpt om de stap en de entiteit te visualiseren.



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)



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**:

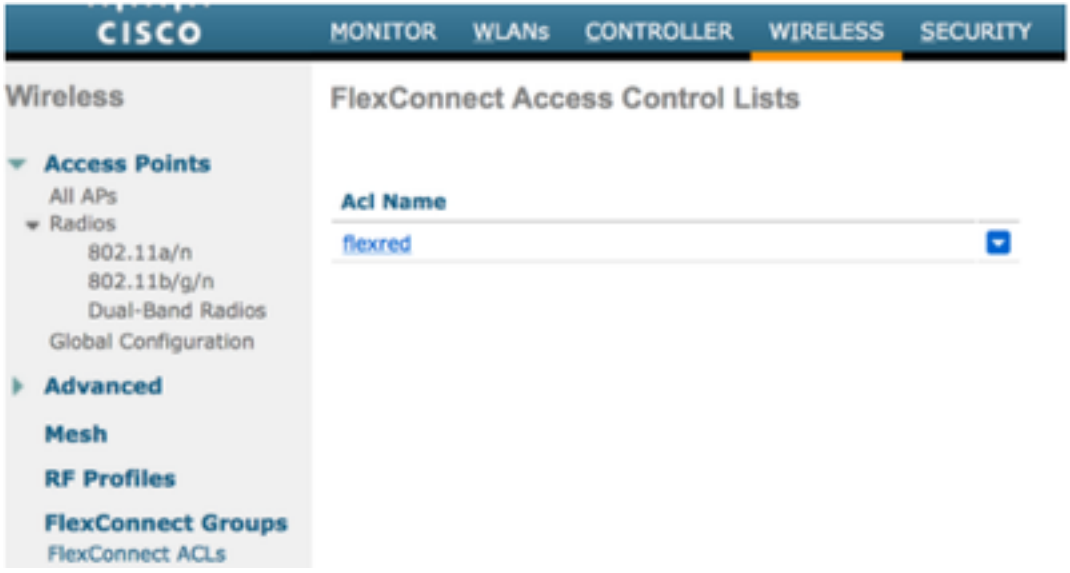
```
guestlab#sh auth sess int T1/0/48 de
            Interface:  TenGigabitEthernet1/0/48
              IIF-ID:  0x1096380000001DC
         MAC Address:  b496.9126.dd6d
        IPv6 Address:  Unknown
        IPv4 Address:  10.106.37.18
           User-Name:  B4-96-91-26-DD-6D
              Status:  Authorized
              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_Te1/0/48

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=66bbfce930a43142fe26b9d9577971de
     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**

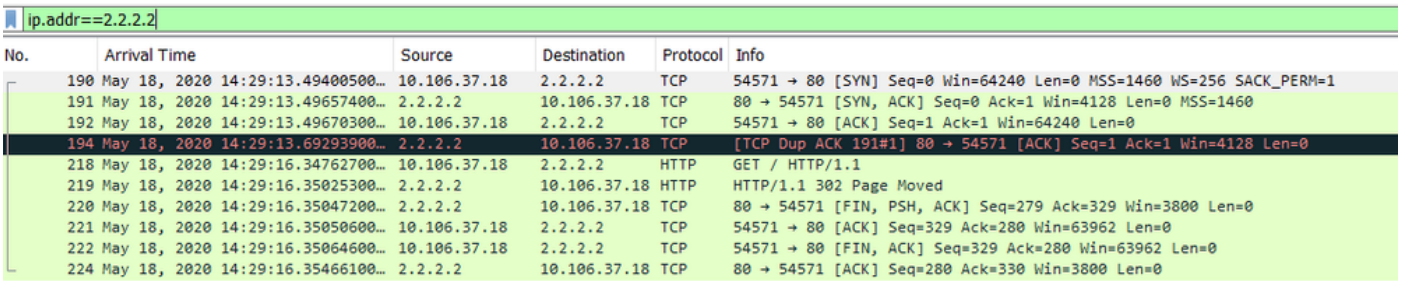
3. De bereikbaarheid van het eindpunt naar de ISE op TCP-poort 8443 met behulp van opdrachtprompt: **C:\Users\user>Telnet <ISE-IP> 843**

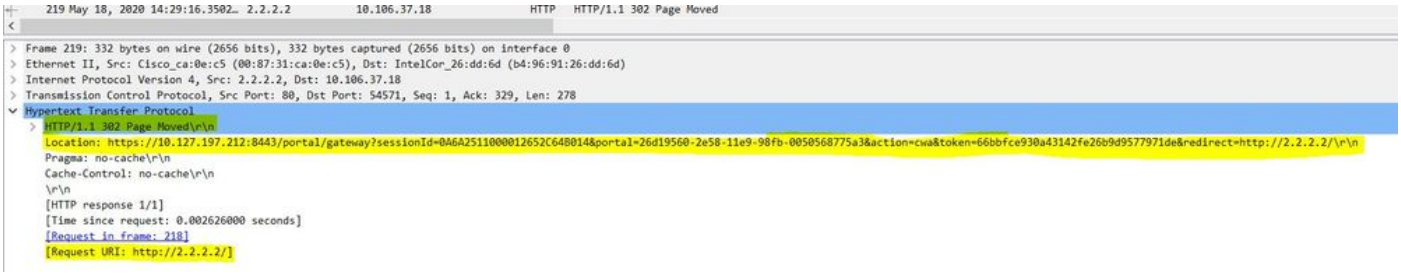
4. Als de portal URL een FQDN heeft, controleert u of de client kan oplossen via de opdrachtprompt: **C:\Users\user>nslookup guest.ise.com**

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.



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):





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
```

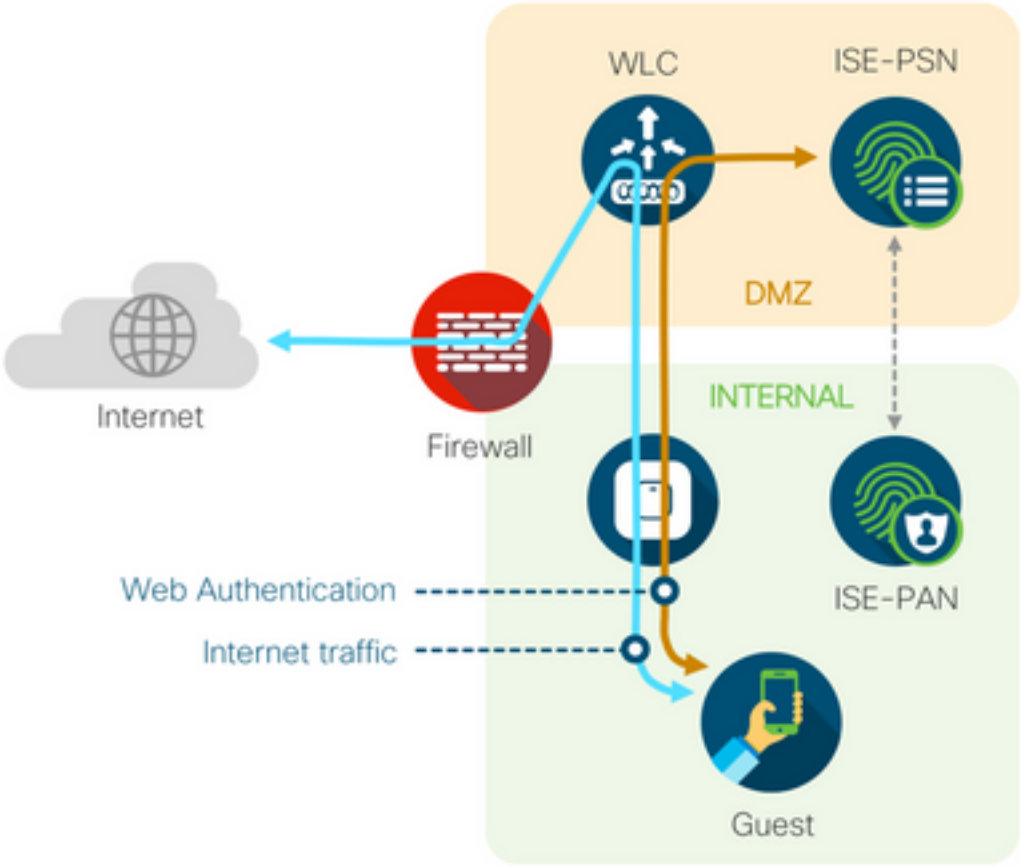
Op de WLC:

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.

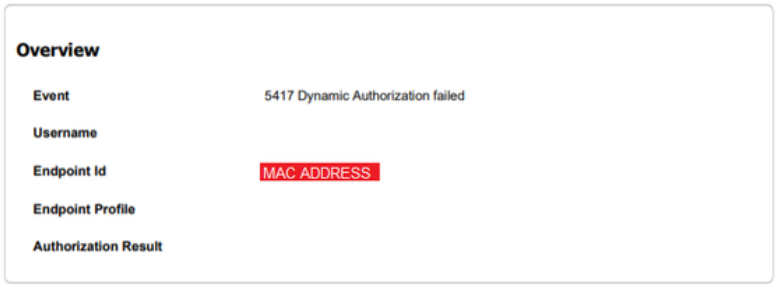
Stap 2. Redirect URL moet op beide WLCs worden gezien.

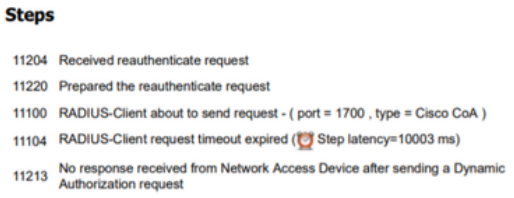
Stap 3. RADIUS-accounting moet op het anker WLC worden uitgeschakeld.



Dynamische autorisatie mislukt

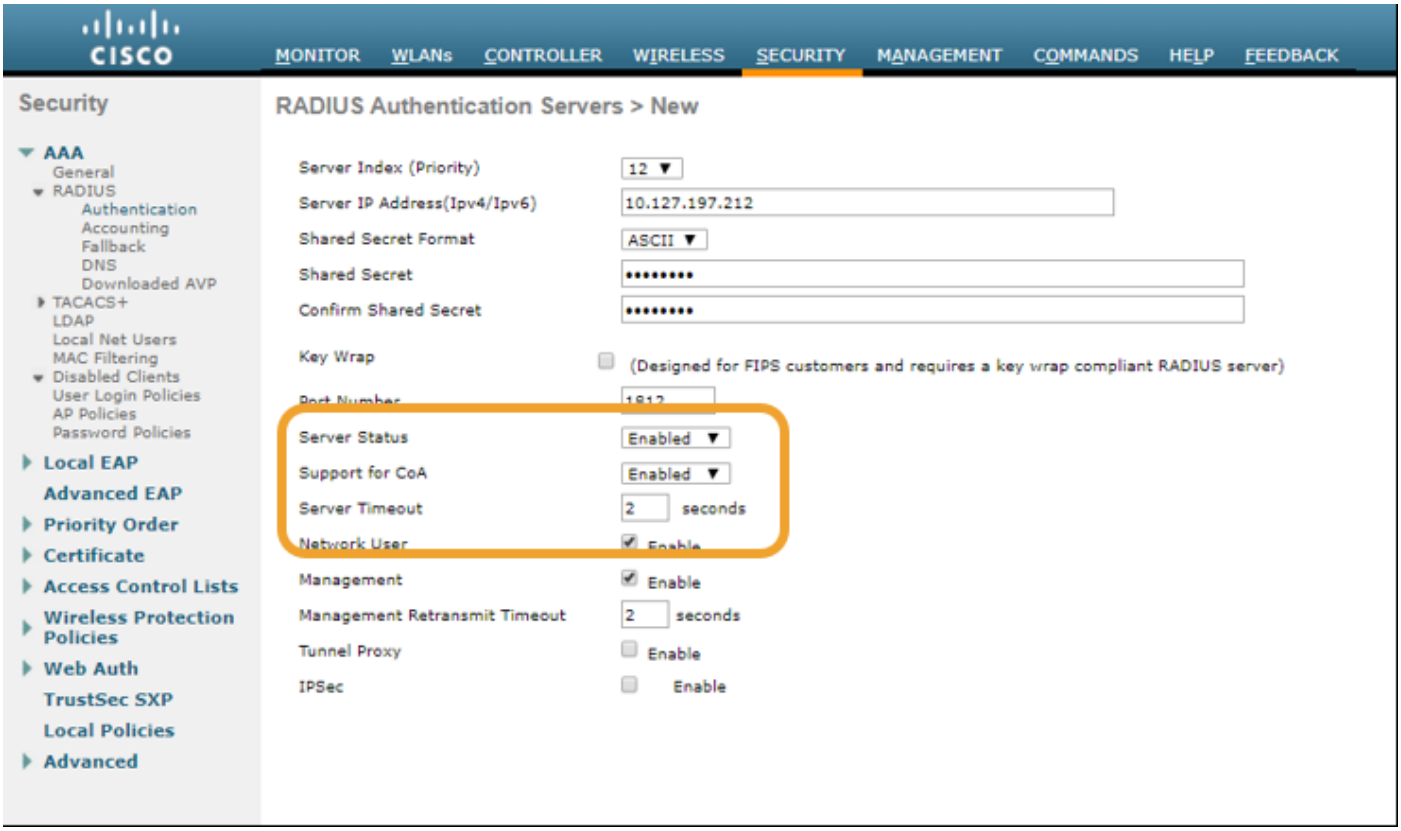
Als de eindgebruiker toegang kan krijgen tot het gastportaal en met succes kan inloggen, is de volgende stap een wijziging van de autorisatie, om volledige gasttoegang te verlenen aan de gebruiker. Als dit niet werkt, zou u een Dynamische mislukking van de Vergunning op de Levende Logboeken van de Straal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





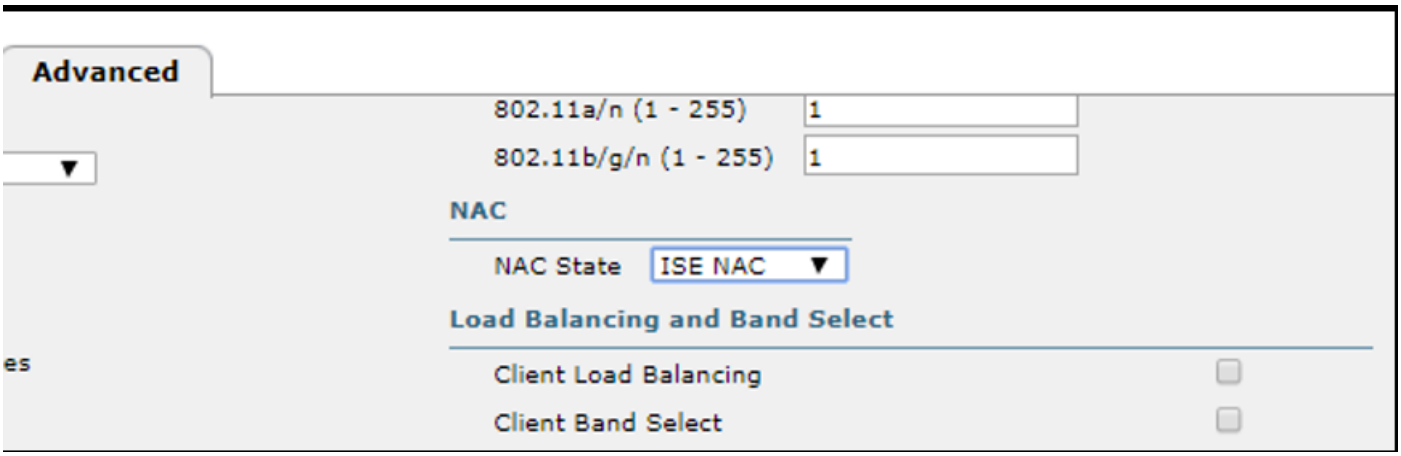
1. Wijziging van autorisatie (CoA) moet worden ingeschakeld/geconfigureerd op het NAD:

```
!
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.

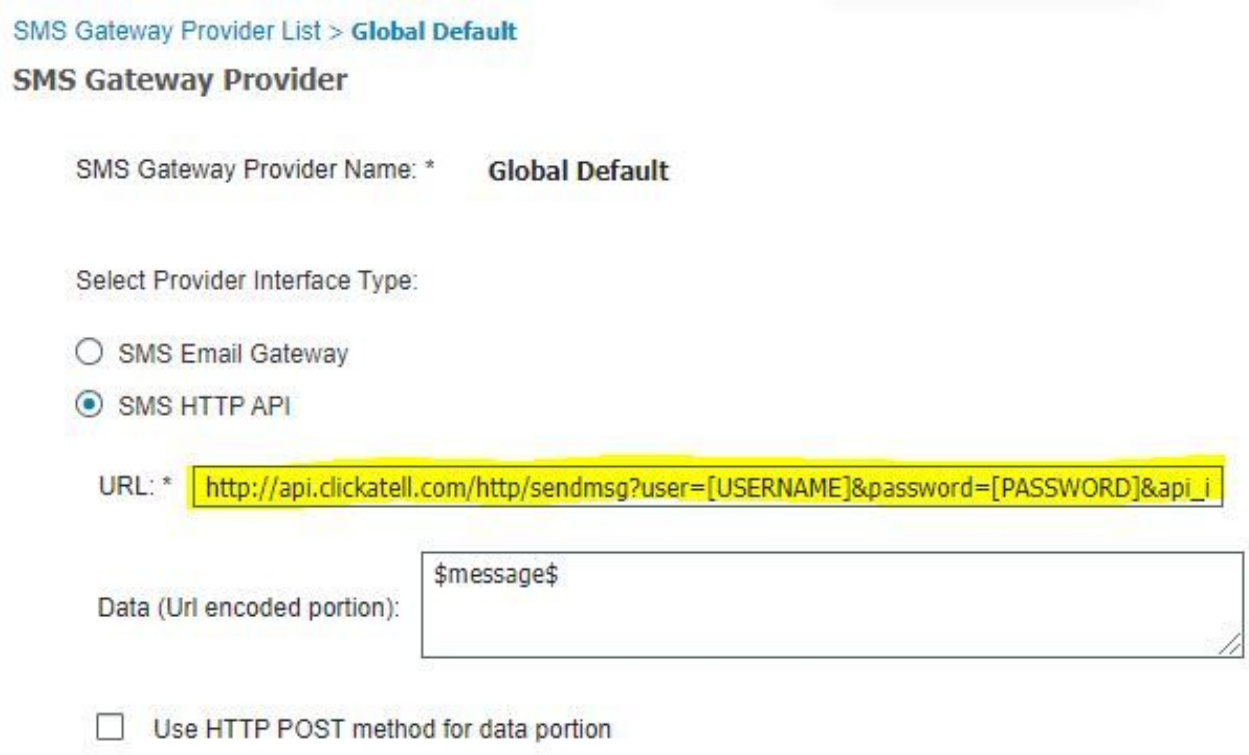


Meldingen via sms/e-mail worden niet verzonden

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

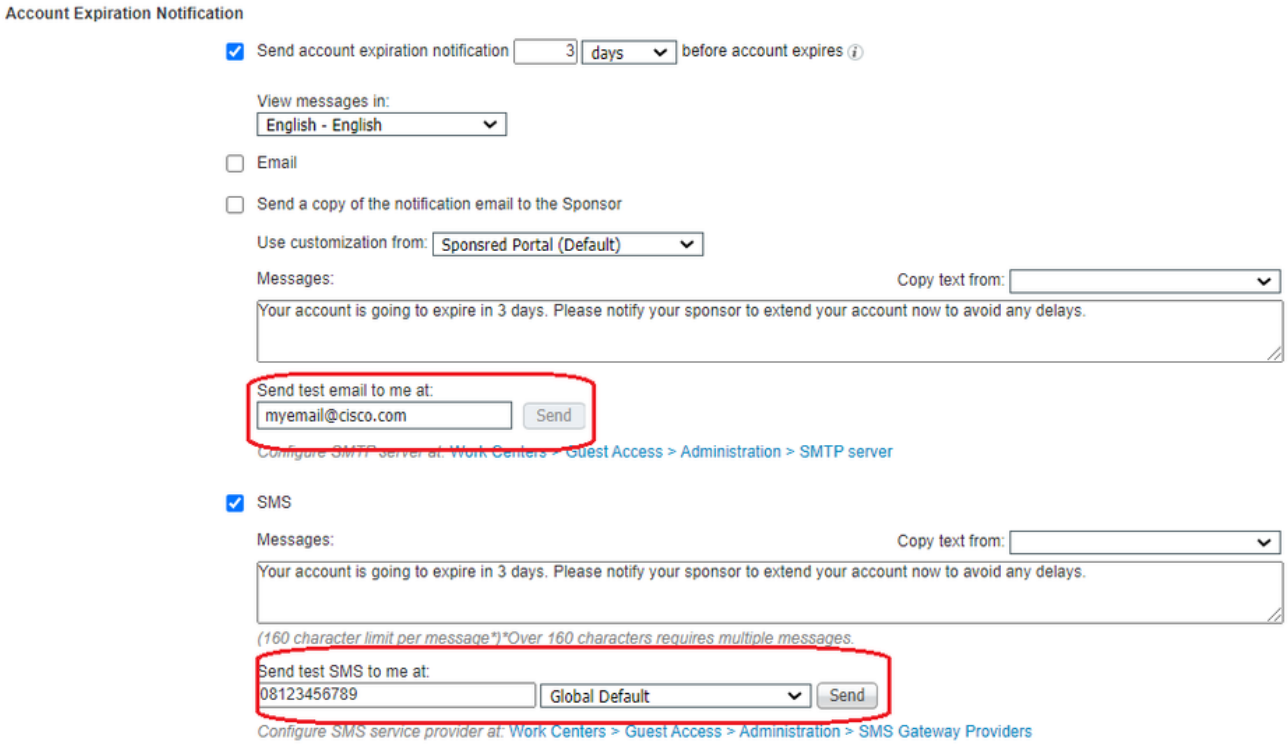
2. Controleer de API op SMS-/e-mailgateways buiten ISE:

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**]



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

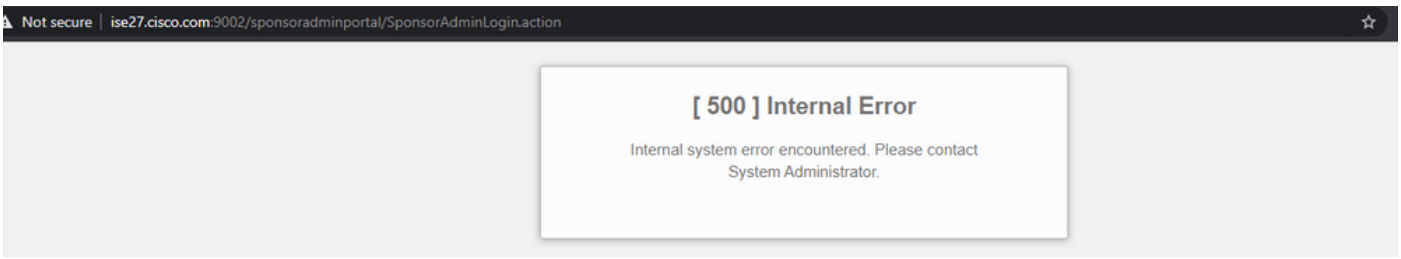
1. Het verzoekpakket bereikt de server onaangetast.
2. ISE-server heeft de door de verkoper aanbevolen rechten/rechten voor de gateway om deze aanvraag te verwerken.



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.