일반적인 ISE 게스트 액세스 문제 해결

목차

소개

이 문서에서는 구축에서 일반적인 게스트 문제를 해결하는 방법, 문제를 격리하고 확인하는 방법, 간단한 해결 방법을 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ISE 게스트 컨피그레이션
- NAD(Network Access Devices)의 CoA 컨피그레이션
- 워크스테이션의 캡처 툴이 필요합니다.

사용되는 구성 요소

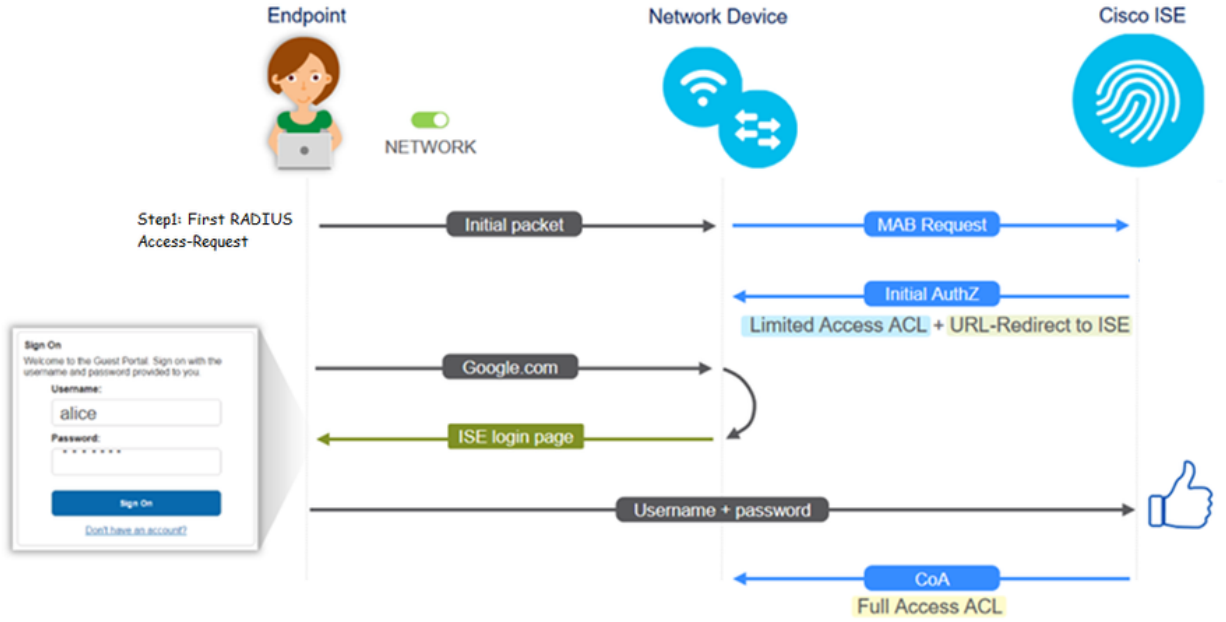
이 문서의 정보는 Cisco ISE, 릴리스 2.6 및:

- WLC 5500
- Catalyst switch 3850 15.x 버전
- Windows 10 워크스테이션

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

게스트 플로우

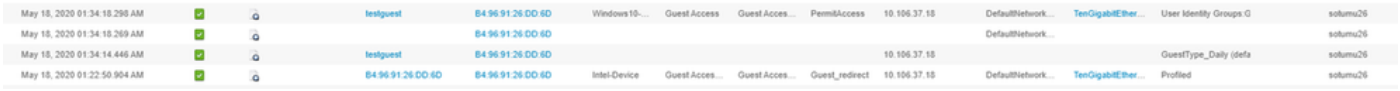
게스트 플로우 개요는 유선 또는 무선 설정과 유사합니다. 이 흐름도 이미지는 문서 전체에서 참조용으로 사용할 수 있습니다. 단계와 엔티티를 시각화하는 데 도움이 됩니다.



또한 이 흐름은 엔드포인트 ID를 필터링하여 ISE 라이브 로그 [**Operations(작업) > RADIUS Live Logs(RADIUS 라이브 로그)**]에서 따를 수 있습니다.

- MAB 인증 성공 - 사용자 이름 필드에 MAC 주소가 있음 - URL이 NAD로 푸시 - 사용자가 포털을 가져옵니다.
- Guest Authentication successful(게스트 인증 성공) - username(사용자 이름) 필드에 게스트 사용자 이름이 있으며 GuestType_Daily(또는 게스트 사용자에 대해 구성된 유형)로 식별되었습니다.
- CoA 시작 - 사용자 이름 필드가 비어 있으며, 자세한 보고서에 동적 권한 부여가 성공적으로 표시됨
- 게스트 액세스 제공

이미지의 이벤트 시퀀스(맨 아래에서 맨 위)



공통 구축 설명서

다음은 컨피그레이션 지원을 위한 링크입니다. 특정 활용 사례 트러블슈팅의 경우, 이상적이거나 예상되는 컨피그레이션을 인식하는 데 도움이 됩니다.

- 유선 게스트 컨피그레이션
- 무선 게스트 컨피그레이션
- FlexAuth AP를 사용하는 무선 게스트 CWA

자주 발생하는 문제

이 문서에서는 주로 다음과 같은 문제를 다룹니다.

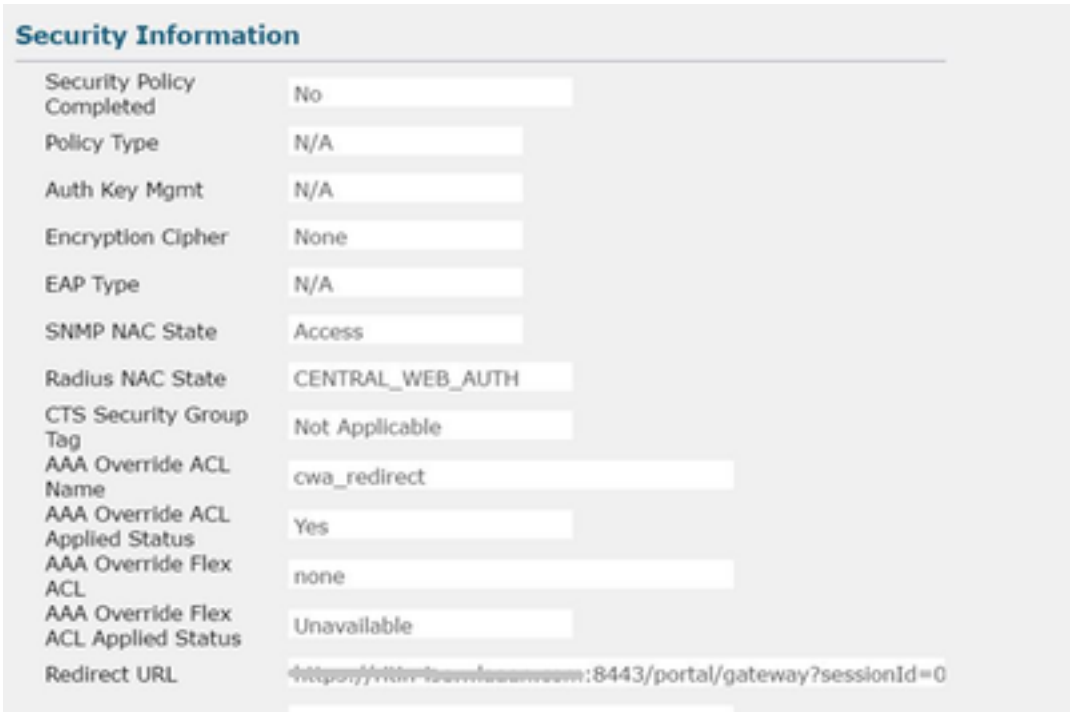
게스트 포털로 리디렉션할 수 없음

리디렉션 URL 및 ACL이 ISE에서 푸시되면 다음을 확인합니다.

1. **show authentication session int <interface> 세부** 정보를 사용하는 스위치의 클라이언트 상태(유선 게스트 액세스**의 경우**)

```
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:  0A6A25110000012652C64B014
     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
A25110000012652C64B014&portal=26d19560-2e58-11e9-98fb-0050568775a3&action=cwa&tok
en=66bbfce930a43142fe26b9d9577971de
     URL Redirect ACL:  REDIRECT_ACL

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

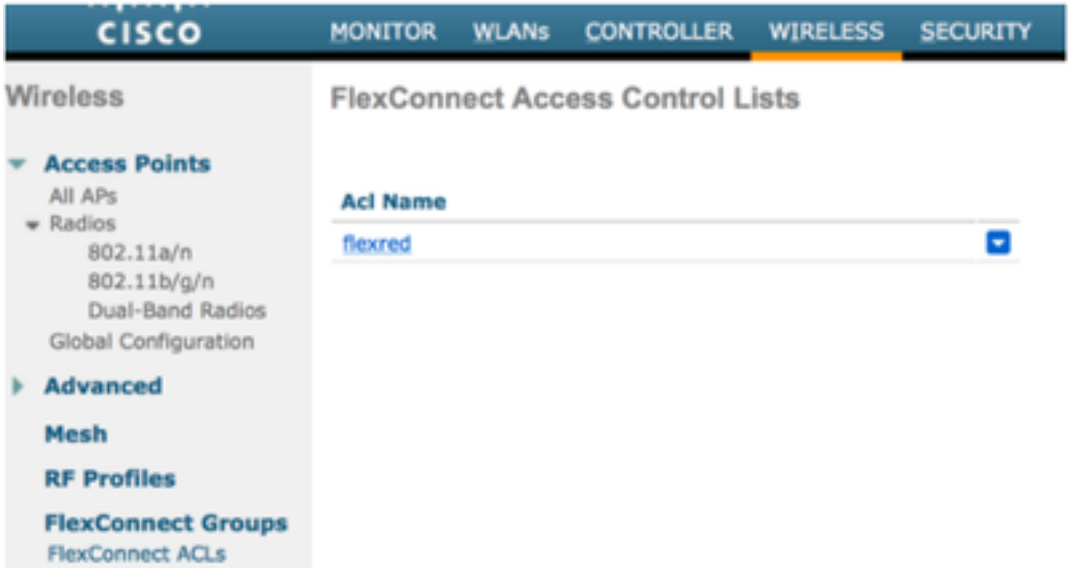
2. Wireless LAN Controller의 클라이언트 상태(무선 게스트 액세스인 경우): **Monitor(모니터) > Client(클라이언트) > MAC address(MAC 주소)**



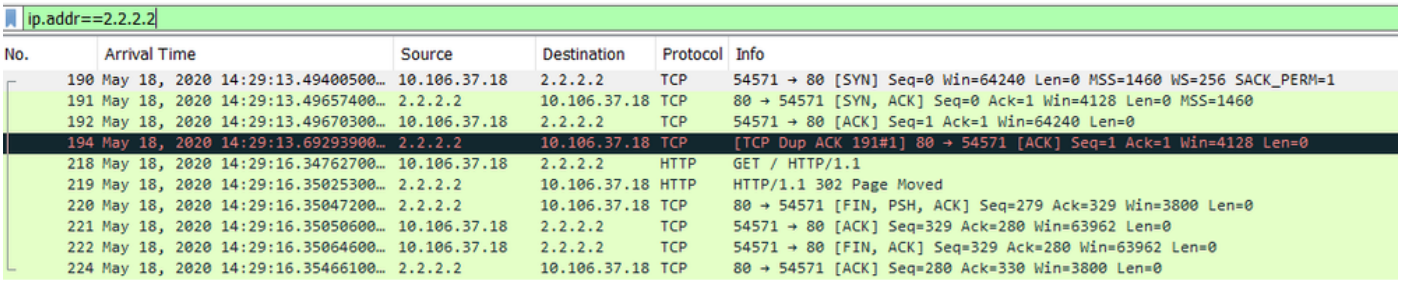
3. 명령 프롬프트를 통해 엔드포인트에서 TCP 포트 8443의 ISE로 연결할 수 있습니다
. **C:\Users\user>telnet <ISE-IP> 8443**

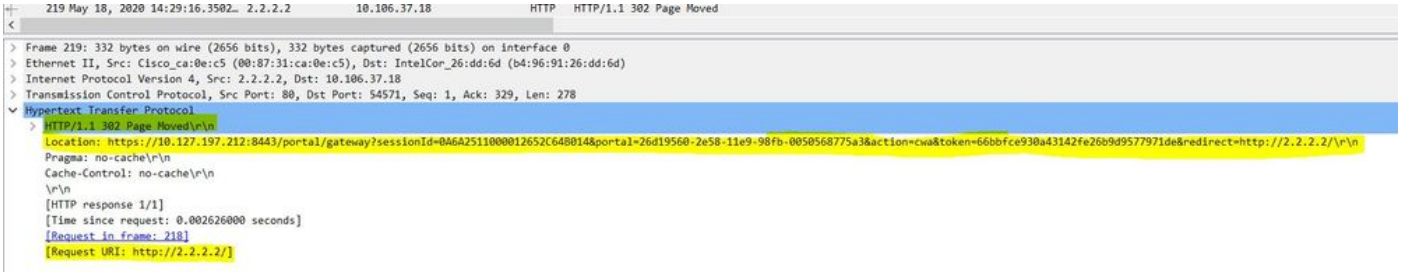
4. 포털 리디렉션 URL에 FQDN이 있는 경우 클라이언트가 명령 프롬프트에서 확인할 수 있는지 확인합니다. **C:\Users\user>nslookup guest.ise.com**

5. flex connect 설정에서 ACL 및 flex ACL에 동일한 ACL 이름이 구성되어 있는지 확인합니다. 또한 ACL이 AP에 매핑되어 있는지 확인합니다. 자세한 내용은 이전 섹션 7단계 b 및 c의 컨피그레이션 가이드를 참조하십시오.



6. 클라이언트에서 패킷 캡처를 가져온 다음 리디렉션을 확인합니다. 패킷 HTTP/1.1 302 Page Moved는 WLC/Switch가 액세스한 사이트를 ISE 게스트 포털(리디렉션된 URL)로 리디렉션했음을 나타냅니다.





7. HTTP(s) 엔진이 네트워크 액세스 디바이스에서 활성화되어 있습니다.

스위치에서:

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

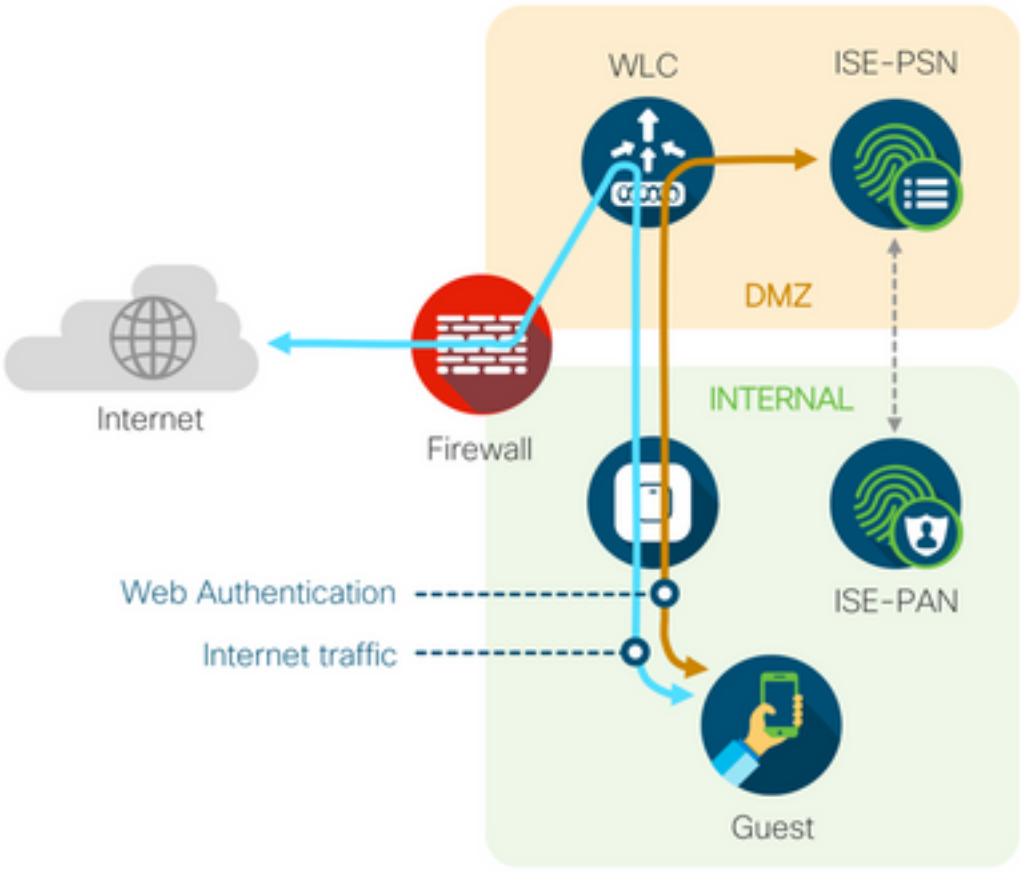
WLC에서:

8. WLC가 외부 앵커 설정에 있는 경우 다음 사항을 확인합니다.

1단계. 클라이언트 상태는 두 WLC에서 동일해야 합니다.

2단계. 리디렉션 URL은 두 WLC에서 모두 표시되어야 합니다.

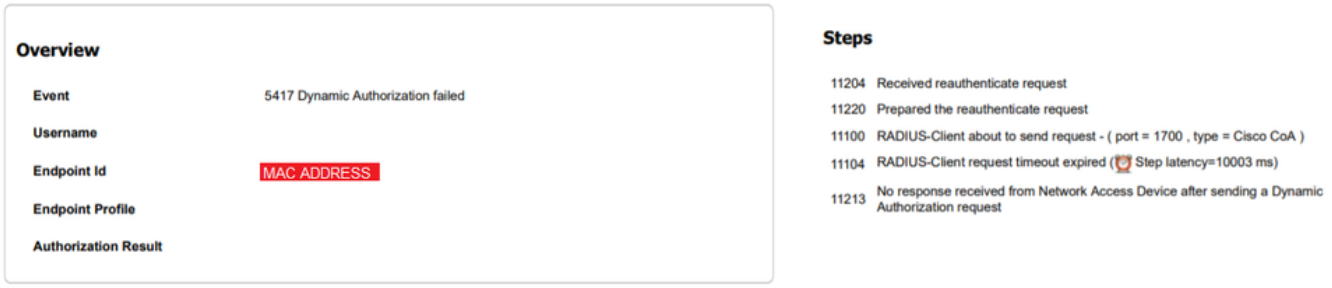
3단계. 앵커 WLC에서 RADIUS 계정 관리를 비활성화해야 합니다.



동적 권한 부여 실패

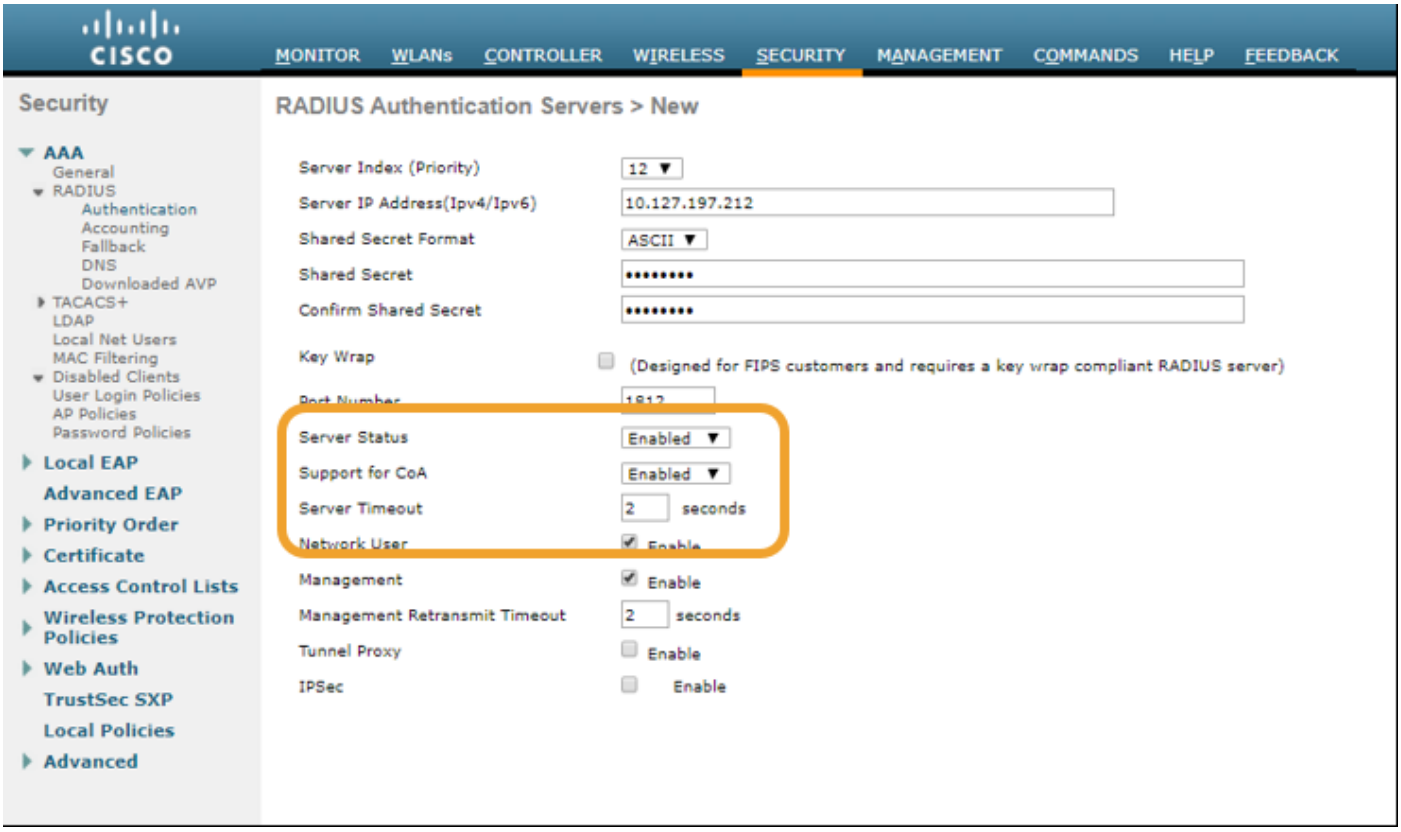
최종 사용자가 게스트 포털에 액세스 할 수 있고 성공 적으로 로그인 할 수 있는 경우, 다음 단계는

사용자에게 전체 게스트 액세스를 제공 하기 위해 권한 부여를 변경 할 수 있습니다. 이 방법이 작동하지 않으면 ISE Radius Live Logs(ISE Radius 라이브 로그)에서 Dynamic Authorization(동적 권한 부여) 오류가 표시됩니다. 문제를 해결하려면 다음을 확인하십시오.



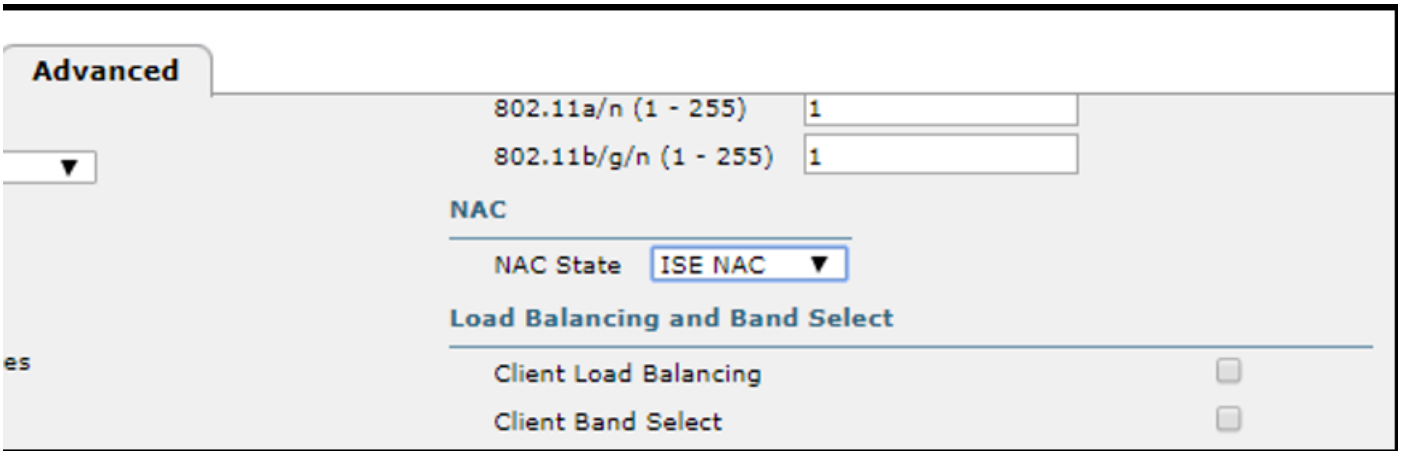
1. NAD에서 CoA(Change of Authorization)를 활성화/구성해야 합니다.

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



2. 방화벽에서 UDP 포트 1700을 허용해야 합니다.

3. WLC의 NAC 상태가 잘못되었습니다. Advanced settings on WLC **GUI(WLC GUI > WLAN)**에서 NAC 상태를 ISE NAC로 변경합니다.

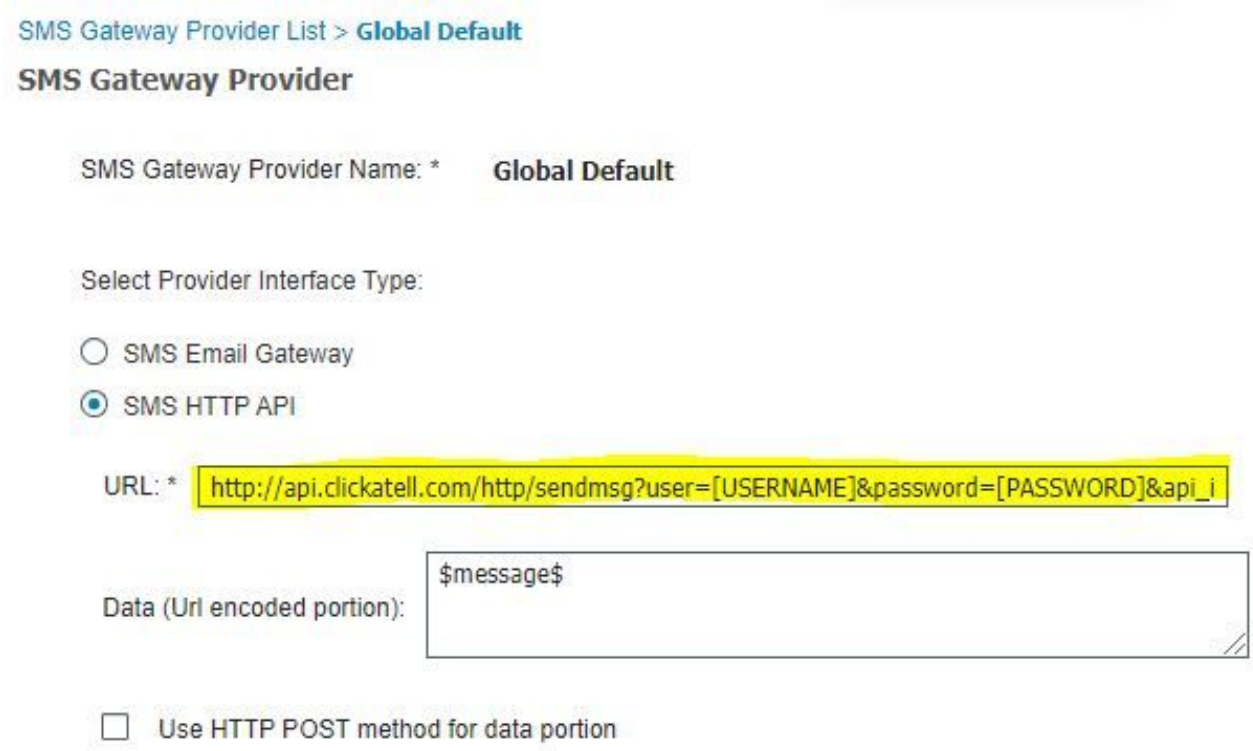


SMS/이메일 알림이 전송되지 않음

1. Administration(관리) > **System(시스템) > Settings(설정) > SMTP 아래에서 SMTP 컨피그레이션을 확인합니다**.

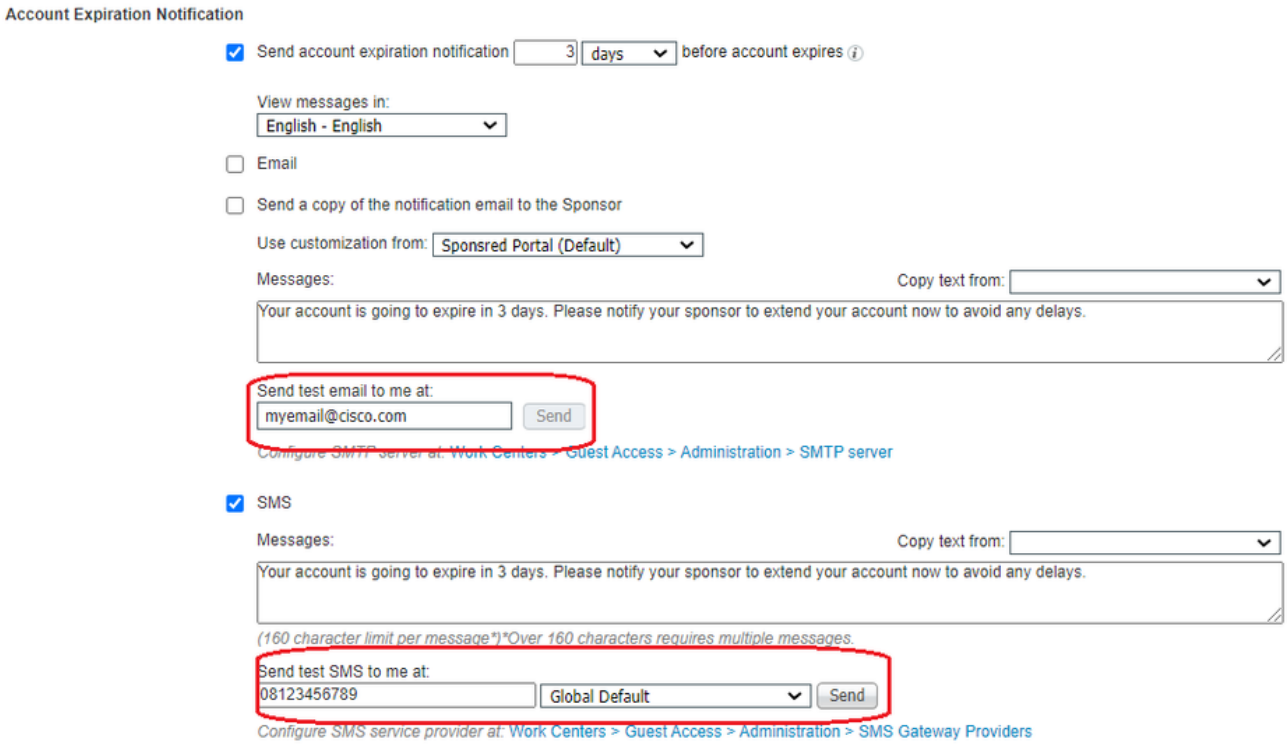
2. ISE 외부의 SMS/이메일 게이트웨이에 대한 API를 확인합니다.

API 클라이언트 또는 브라우저에서 공급업체가 제공한 URL을 테스트하고, 사용자 이름, 비밀번호, 휴대폰 번호 등의 변수를 교체하고, 연결성을 테스트합니다. [**관리 > 시스템 > 설정 > SMS 게이트웨이**]



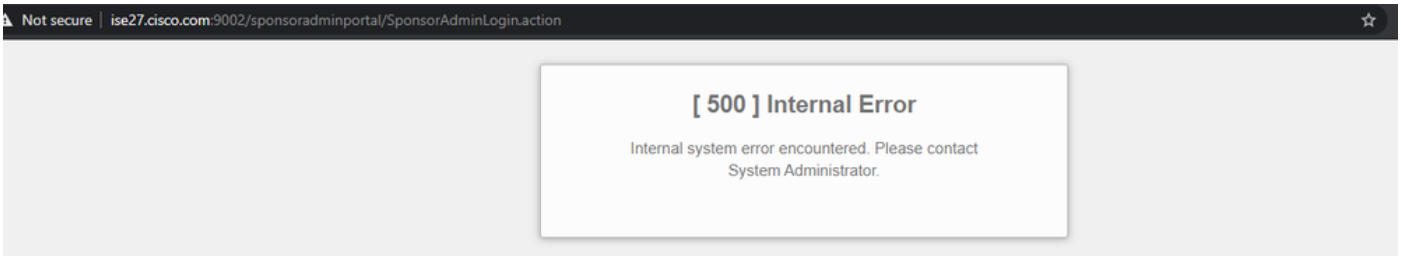
또는 ISE 스폰서 그룹 [**Workcentres > Guest Access > Portals and Components > Guest Types**]에서 테스트하는 경우, ISE 및 SMS/SMTP 게이트웨이에서 패킷 캡처를 수행하여 다음을 확인합니다

1. 요청 패킷이 변조되지 않은 상태로 서버에 도착합니다.
2. ISE 서버에는 게이트웨이가 이 요청을 처리할 수 있는 공급업체의 권장 권한/권한이 있습니다.



Manage the Accounts Page not Reachable(어카운트 관리 페이지에 연결할 수 없음)

1. Workcenters(작업 센터) **> Guest Access(게스트 액세스) > Manage accounts(계정 관리)** 버튼 아래에서 ISE 관리자가 스폰서 포털에 액세스할 수 있도록 포트 9002의 ISE FQDN으로 리디렉션됩니다.



2. FQDN이 nslookup <FQDN **of ISE PAN>** 명령을 사용하여 스폰서 포털에 액세스하는 **워크스테이션에서 확인되는지 확인합니다**.

3. 명령 **show ports**를 사용하여 ISE의 CLI에서 ISE TCP 포트 9002가 열려 있는지 확인합니다 **| 9002 포함**.

포털 인증서 모범 사례

- 원활한 사용자 환경을 위해 포털 및 관리자 역할에 사용되는 인증서는 잘 알려진 공용 인증 기관(예: GoDaddy, DigiCert, VeriSign 등)에서 서명해야 하며 일반적으로 브라우저(예: Google Chrome, Firefox 등)에서 신뢰합니다.

- 게스트 리디렉션에 고정 IP를 사용하지 않는 것이 좋습니다. 이렇게 하면 모든 사용자에게 ISE의 개인 IP가 표시됩니다. 대부분의 공급업체는 프라이빗 IP에 대해 서드파티 서명 인증서를 제공하지 않습니다.

- ISE 2.4 p6에서 p8 또는 p9로 이동할 때 알려진 버그(Cisco 버그 ID CSCvp75207)가 있습니다.

여기서 ISE 내의 인증을 **위한 신뢰**와 **클라이언트 인증 및 Syslog 상자를 위한 신뢰는** 패치 업그레이드 후 수동으로 확인해야 합니다. 이렇게 하면 게스트 포털에 액세스할 때 ISE에서 TLS 플로우에 대한 전체 인증서 체인을 전송합니다.

이러한 작업으로 게스트 액세스 문제가 해결되지 않을 경우, 문서의 지침과 함께 수집된 지원 번들을 사용하여 TAC에 문의하십시오. ISE에서 활성화할 디버그.

관련 정보

- **Cisco 기술 지원 및 다운로드**

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.