엔드포인트 가시성을 위해 ISE를 Prime Infrastructure와 통합

목차

소개

이 문서에서는 ISE를 Prime Infrastructure와 통합하여 인증된 엔드포인트에 대한 가시성을 확보하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ISE.
- Cisco Prime Infrastructure입니다
- ISE에 대해 인증하는 엔드포인트에 대한 무선 또는 유선 AAA 흐름.
- 스위치 및 WLC와 같은 NAD(네트워크 액세스 디바이스)에 대한 SNMP 컨피그레이션

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

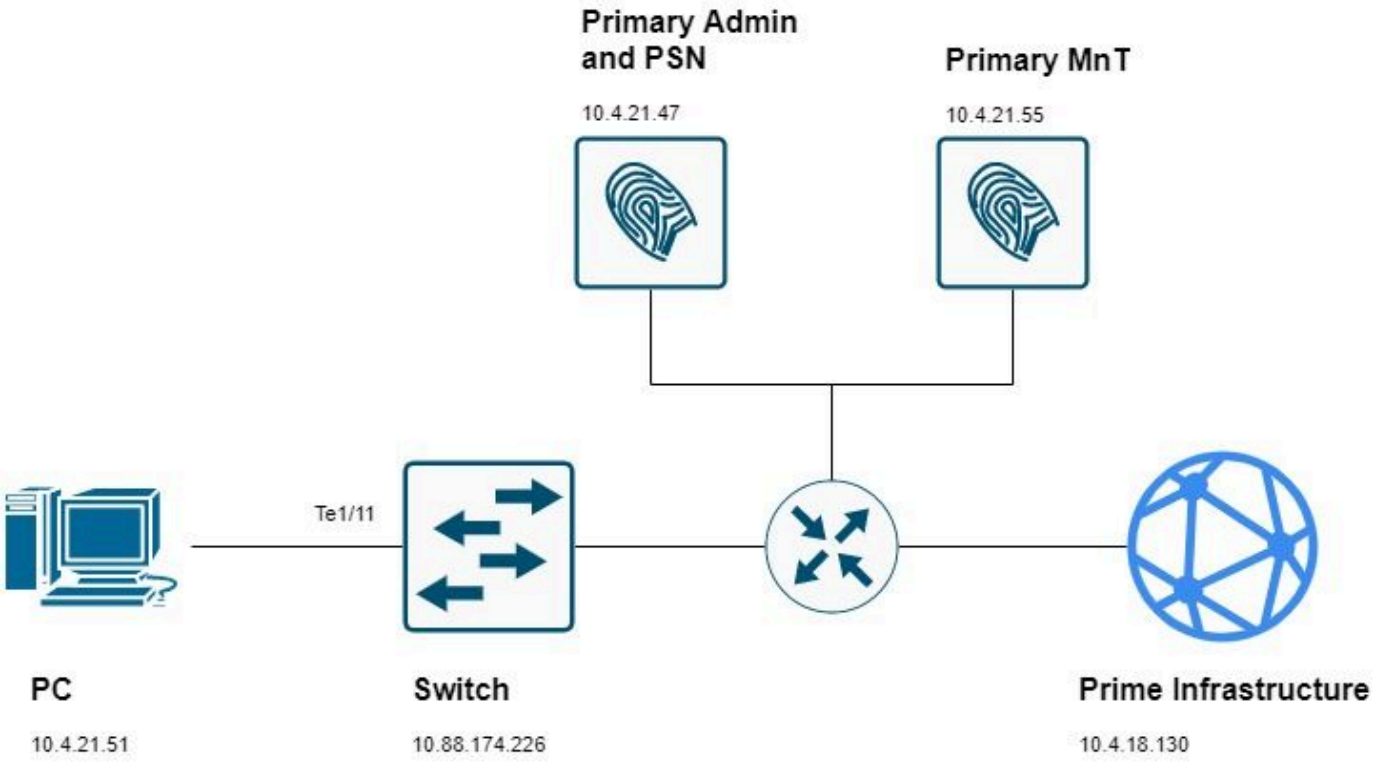
- ISE 3.1 구축.
- Cisco Prime Infrastructure 3.8.

- Cisco IOS® 15.5를 실행하는 C6816-X-LE
- Windows 10 시스템.

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.

구성

네트워크 다이어그램



설정

스위치 구성

1. ISE에 대한 AAA 인증을 위해 NAD(Network Access Device)를 구성합니다. 이 가이드에서는 다음 컨피그레이션을 사용합니다.

```
aaa new-model

radius server ise31
 address ipv4 10.4.21.47 auth-port 1812 acct-port 1813
 key Cisc0123

aaa server radius dynamic-author
 client 10.4.21.47 server-key Cisc0123

aaa group server radius ISE
```

```
 server name ise31

aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting dot1x default start-stop group ISE

dot1x system-auth-control
```

2. 스위치에서 디바이스 추적을 구성합니다.

```
device-tracking policy DT1
 tracking enable

device-tracking tracking auto-source
```

3. dot1x 인증을 위한 switchport를 구성하고 이에 디바이스 추적 정책을 연결합니다.

```
interface TenGigabitEthernet1/11
 device-tracking attach-policy DT1
 authentication host-mode multi-domain
 authentication order dot1x mab webauth
 authentication priority dot1x mab webauth
 authentication port-control auto
 mab
 dot1x pae authenticator
```

4. RO SNMP 커뮤니티 및 SNMP 트랩을 구성하여 네트워크 요구 사항을 충족합니다(선택적으로, RW 커뮤니티를 구성할 수 있음).

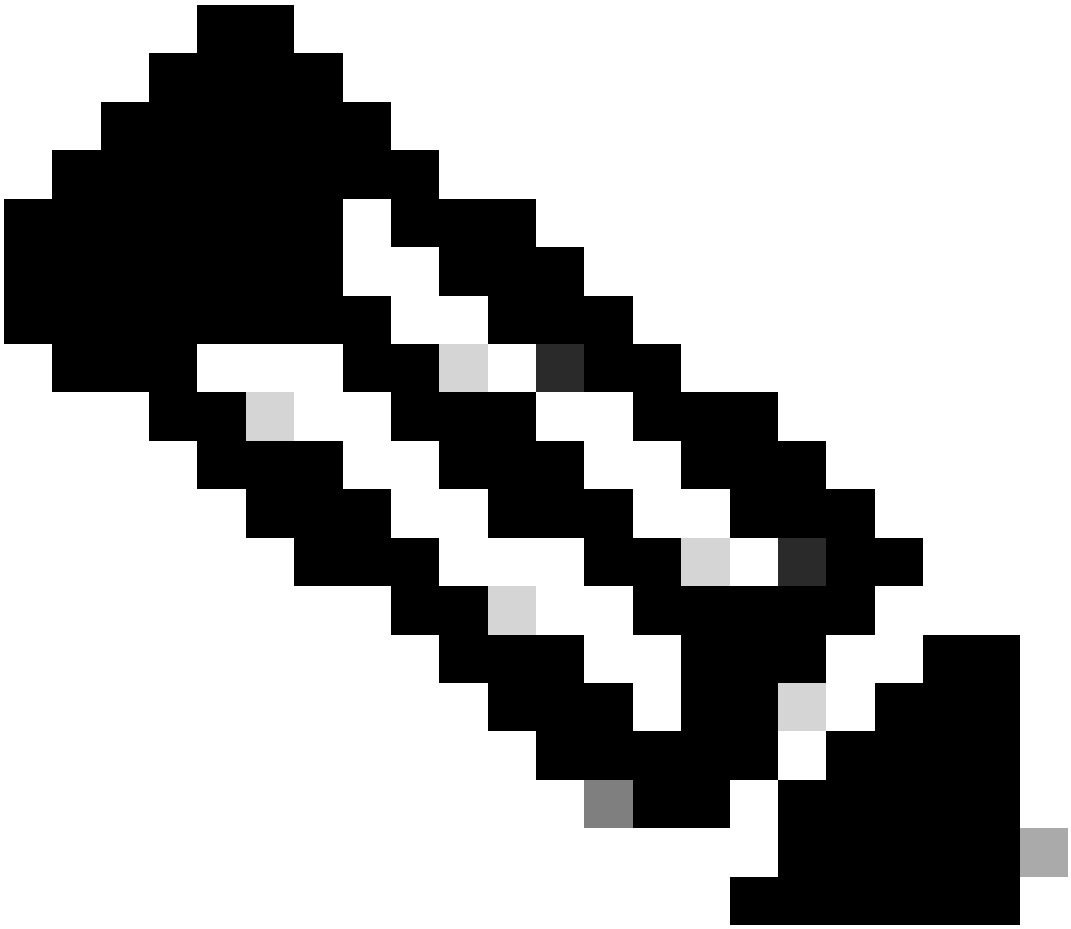
```
snmp-server community public RO
snmp-server community private RW
snmp-server trap-source TenGigabitEthernet1/16
snmp-server source-interface informs TenGigabitEthernet1/16
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps aaa_server
snmp-server enable traps trustsec authz-file-error
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps port-security
snmp-server enable traps event-manager
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server host 10.4.18.130 version 2c public udp-port 161
```

5. Prime이 디바이스를 관리할 수 있도록 텔넷 또는 SSH 액세스를 구성합니다.

```
username admin password 0 cisco!123
aaa authentication login default local

line vty 0 4
 transport input ssh
 login authentication default
```

6. (선택 사항) SSH 연결의 경우 RSA 키가 필요합니다. NAD에 하나 이 없는 경우 다음 단계를 사용하여 생성합니다.

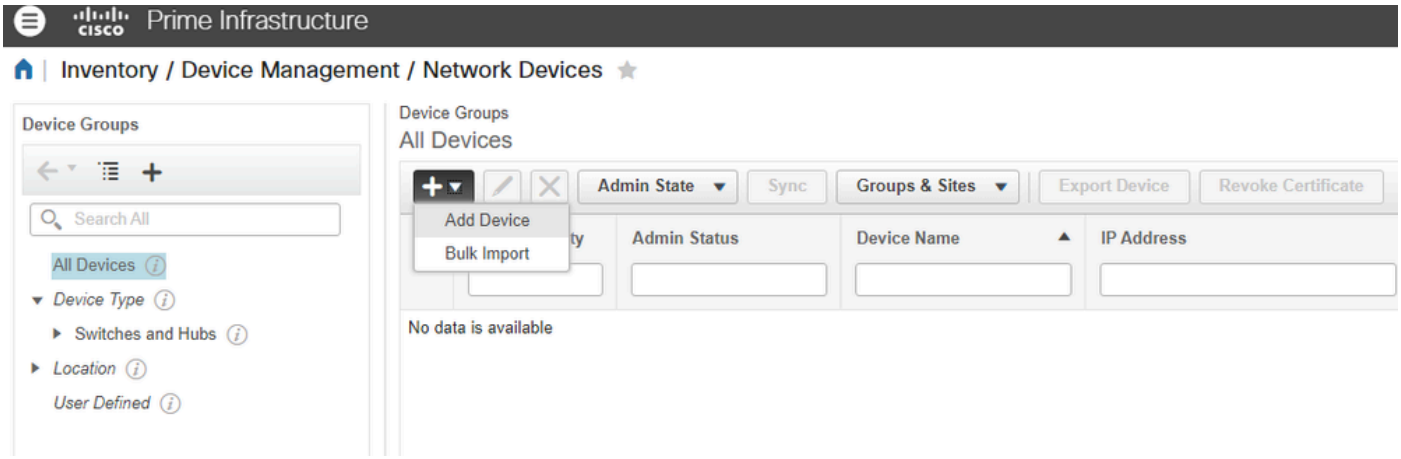


참고: 일부 디바이스에서는 RSA를 생성하기 전에 구성된 도메인이 필요합니다. 기존 도메인을 재정의하지 않도록 디바이스에 도메인이 구성되어 있는지 확인합니다.

```
ip domain-name cisco.com
crypto key generate rsa
```

Cisco Prime Infrastructure 컨피그레이션

7. Inventory(인벤토리) > Device Management(디바이스 관리) > Network Devices(네트워크 디바이스) > Plus sign(+) > Add Device(디바이스 추가)에서 네트워크 디바이스를 추가합니다.



인벤토리 완료를 위한 필수 필드는 다음과 같습니다.

유선 장치의 경우:

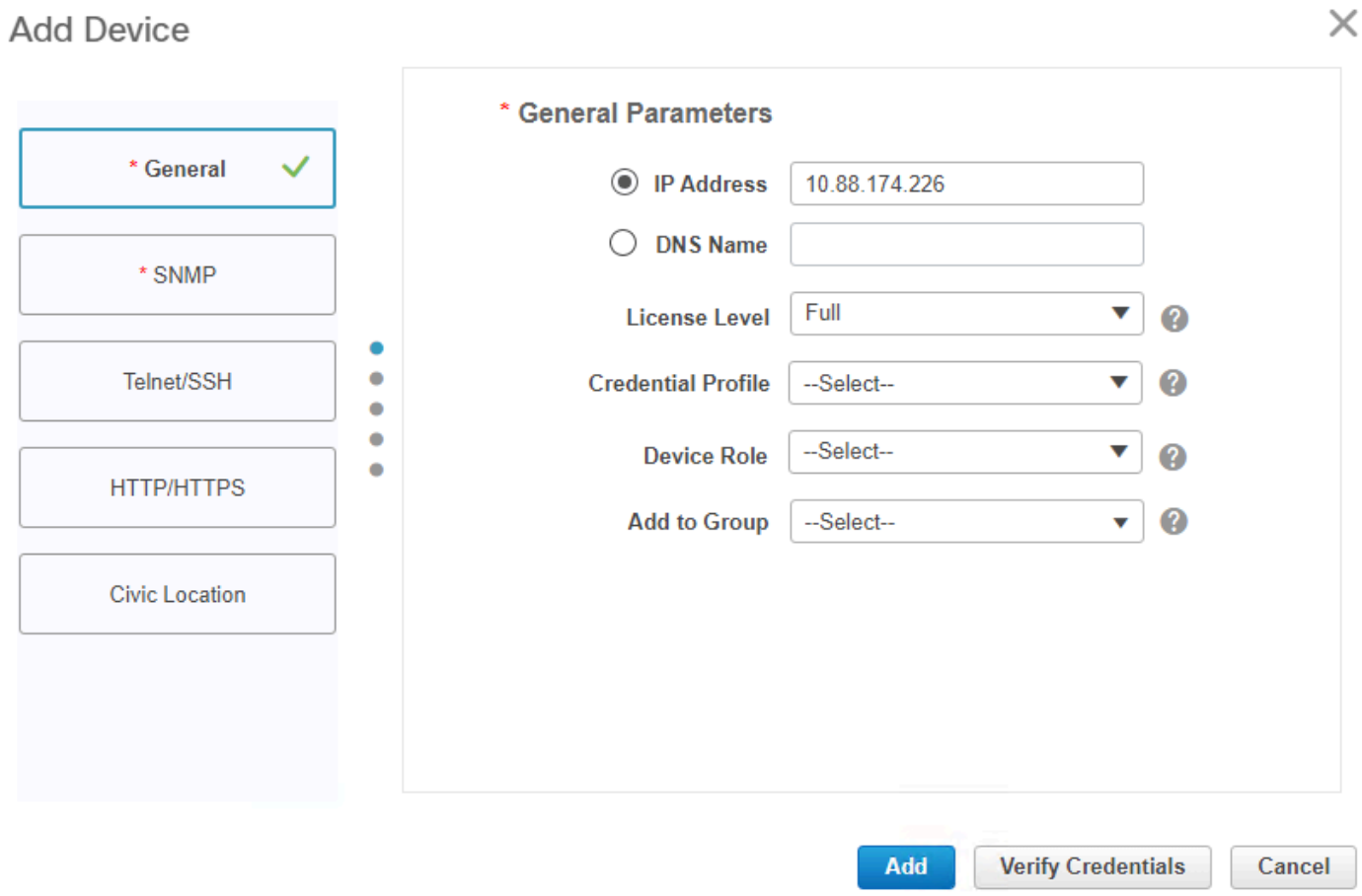
- 일반: IP 또는 DNS 중 하나를 선택합니다.
- SNMP: RO 커뮤니티가 필요합니다. 스위치/WLC에서도 구성해야 합니다.
- 텔넷/SSH: 실행 모드 및 활성화 모드 자격 증명

WLC:

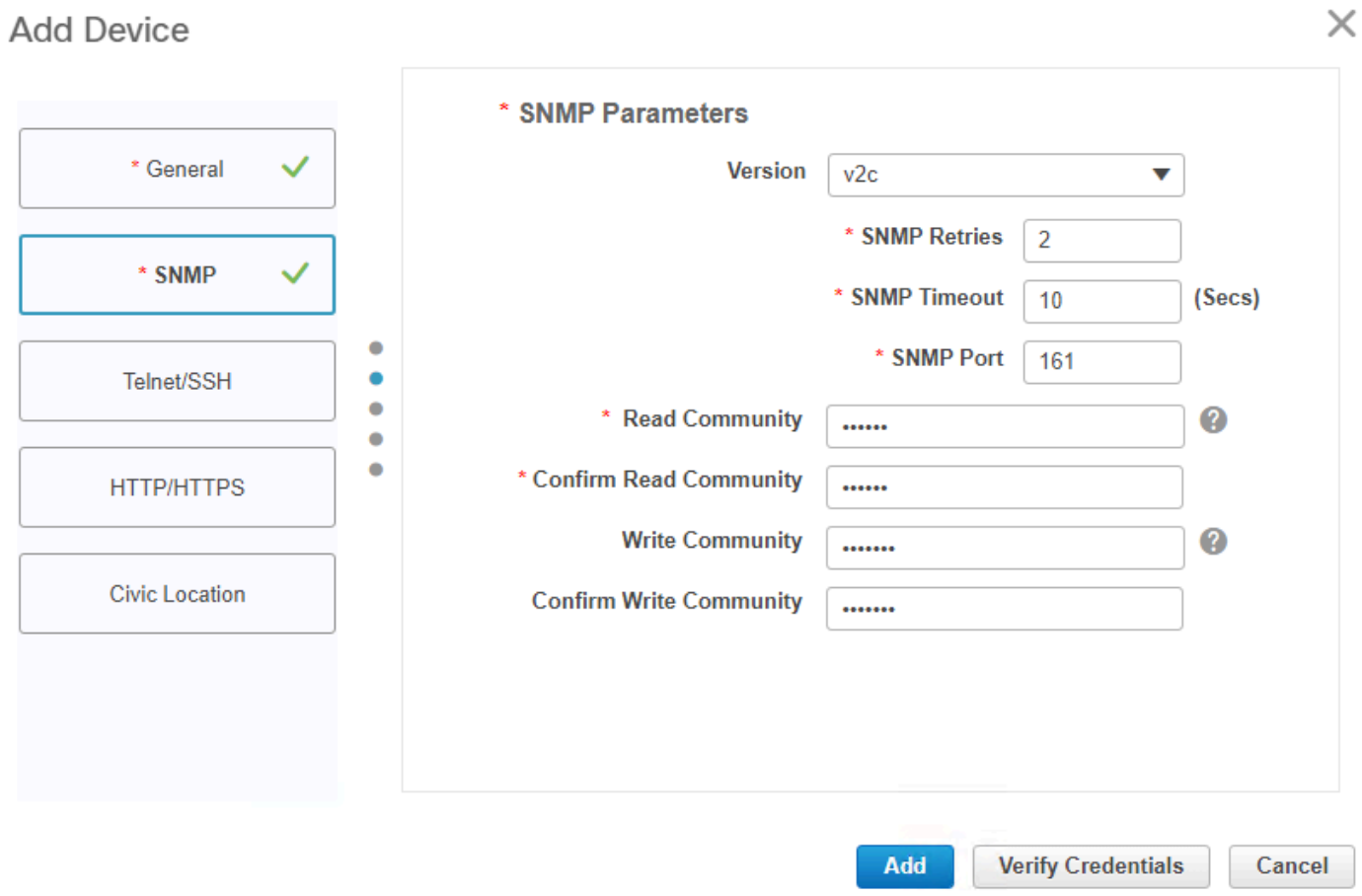
- 일반: IP 또는 DNS 중 하나를 선택합니다.
- SNMP: RO 커뮤니티가 필요합니다. 스위치/WLC에서도 구성해야 합니다.

이 가이드에서는 Cisco 스위치를 사용하고 있습니다.

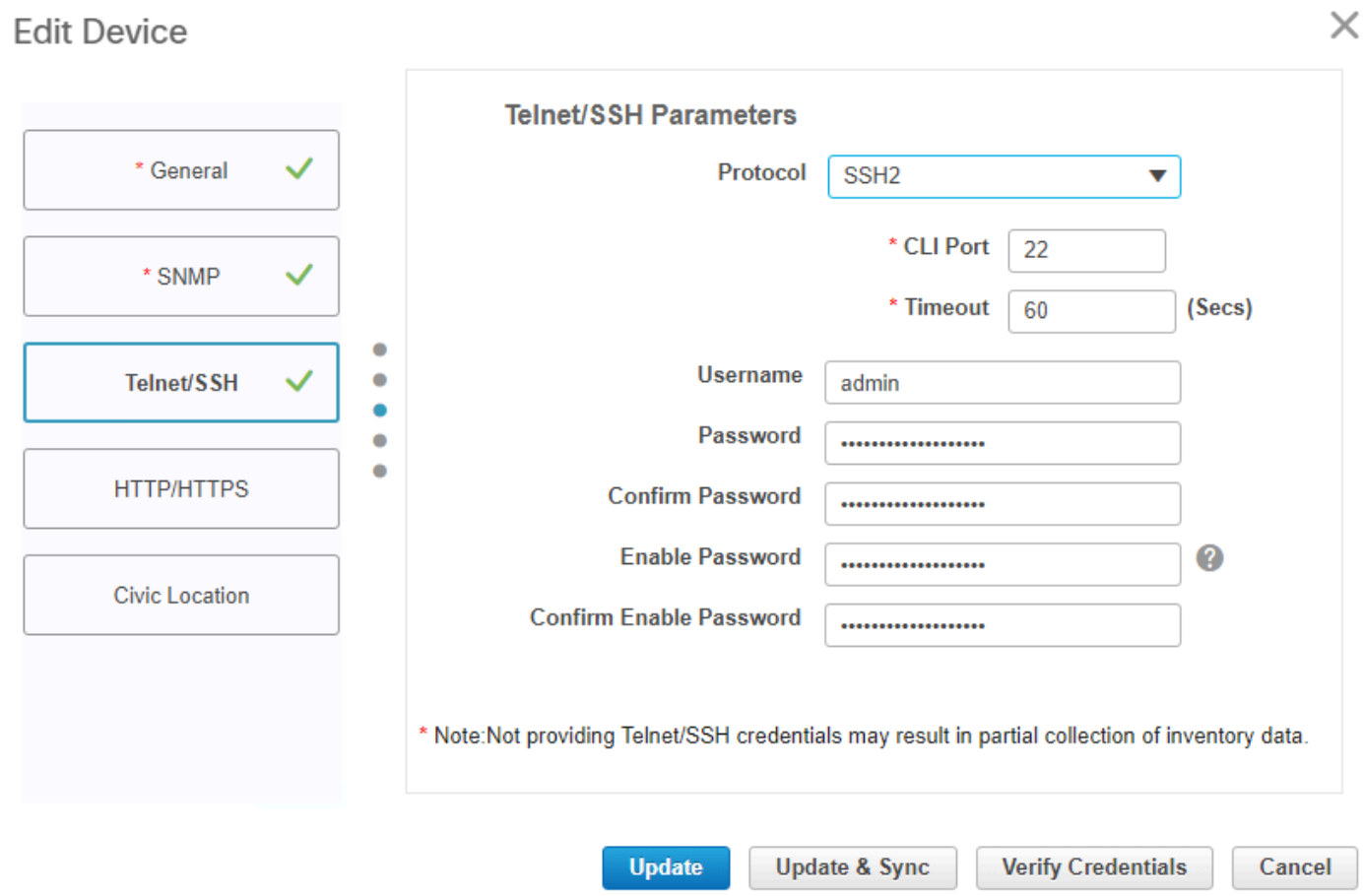
i. 일반 사항 섹션:


Add Device
* General
* SNMP
Telnet/SSH
HTTP/HTTPS
Civic Location
* General Parameters
IP Address
10.88.174.226
DNS Name
License Level
Full
Credential Profile
--Select--
Device Role
--Select--
Add to Group
--Select--
Add
Verify Credentials
Cancel

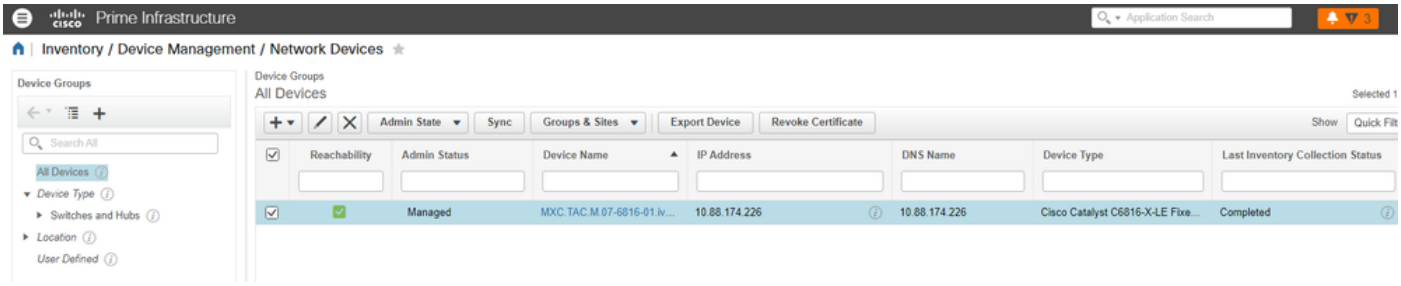
나. SNMP 섹션:


Add Device
* General
* SNMP
Telnet/SSH
HTTP/HTTPS
Civic Location
* SNMP Parameters
Version
v2c
* SNMP Retries
2
* SNMP Timeout
10
(Secs)
* SNMP Port
161
* Read Community
* Confirm Read Community
Write Community
Confirm Write Community
Add
Verify Credentials
Cancel

iii. Telnet/SSH 섹션:



8. 모든 필수 필드가 완료되면 도달 가능성 및 수집 상태가 각각 녹색 및 완료됨인지 확인합니다.

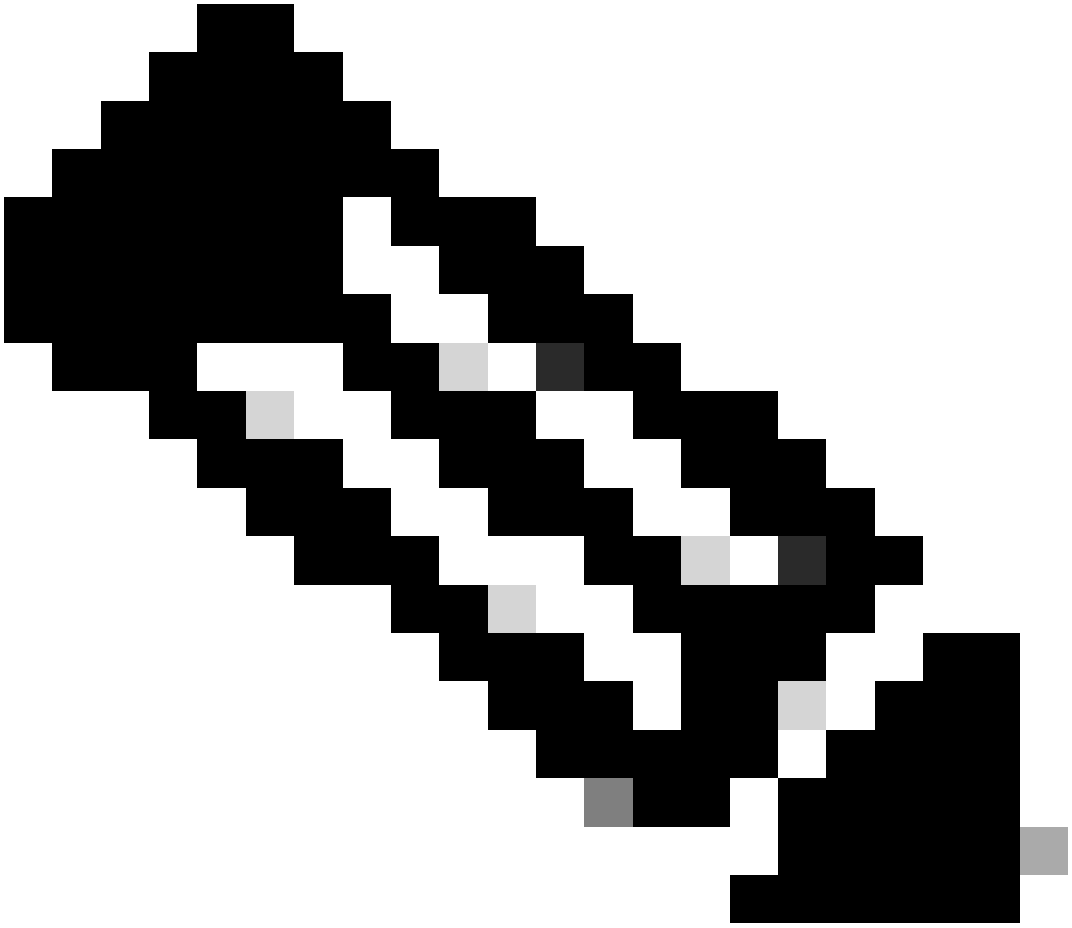


9. Prime과 ISE의 통합

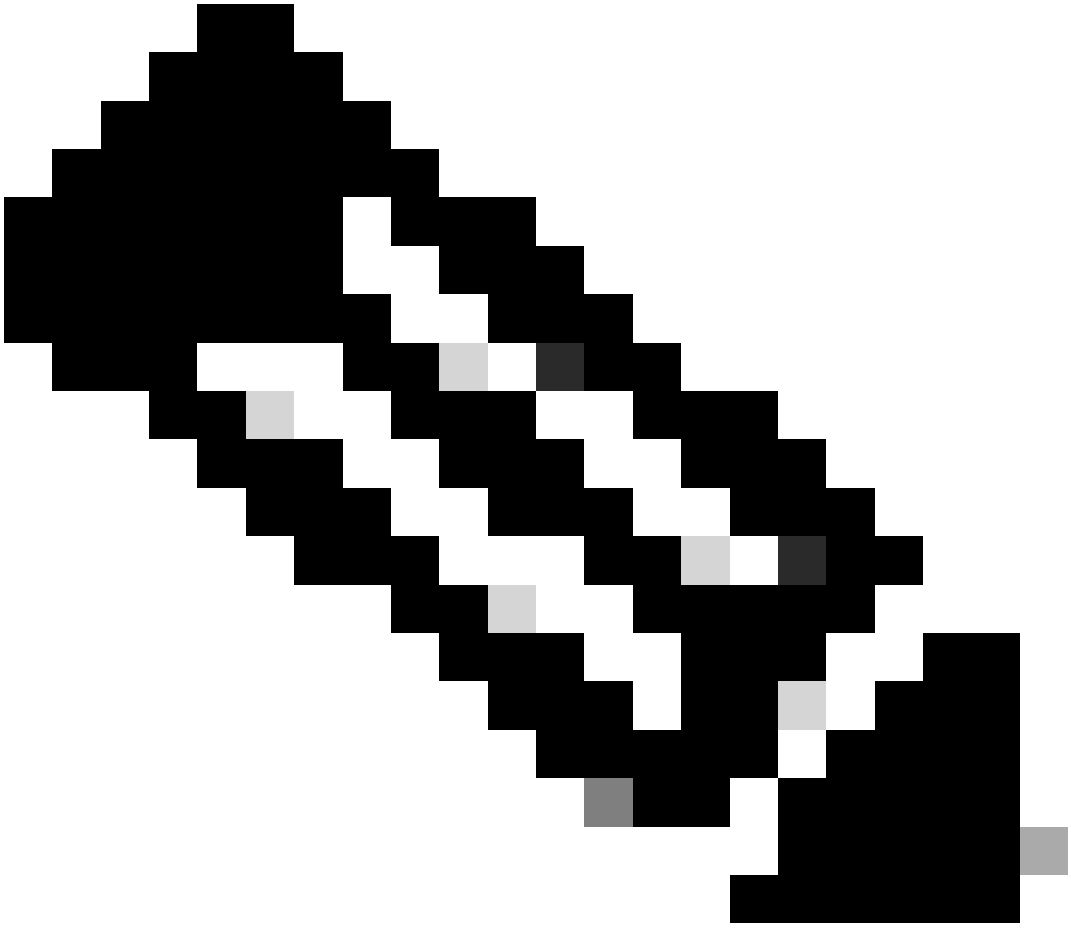
i. Administration(관리) > Servers(서버) > ISE Servers(ISE 서버)로 이동합니다.

나. 드롭다운 메뉴에서 Add ISE Server(ISE 서버 추가)를 선택한 다음 Go(이동)를 클릭합니다.

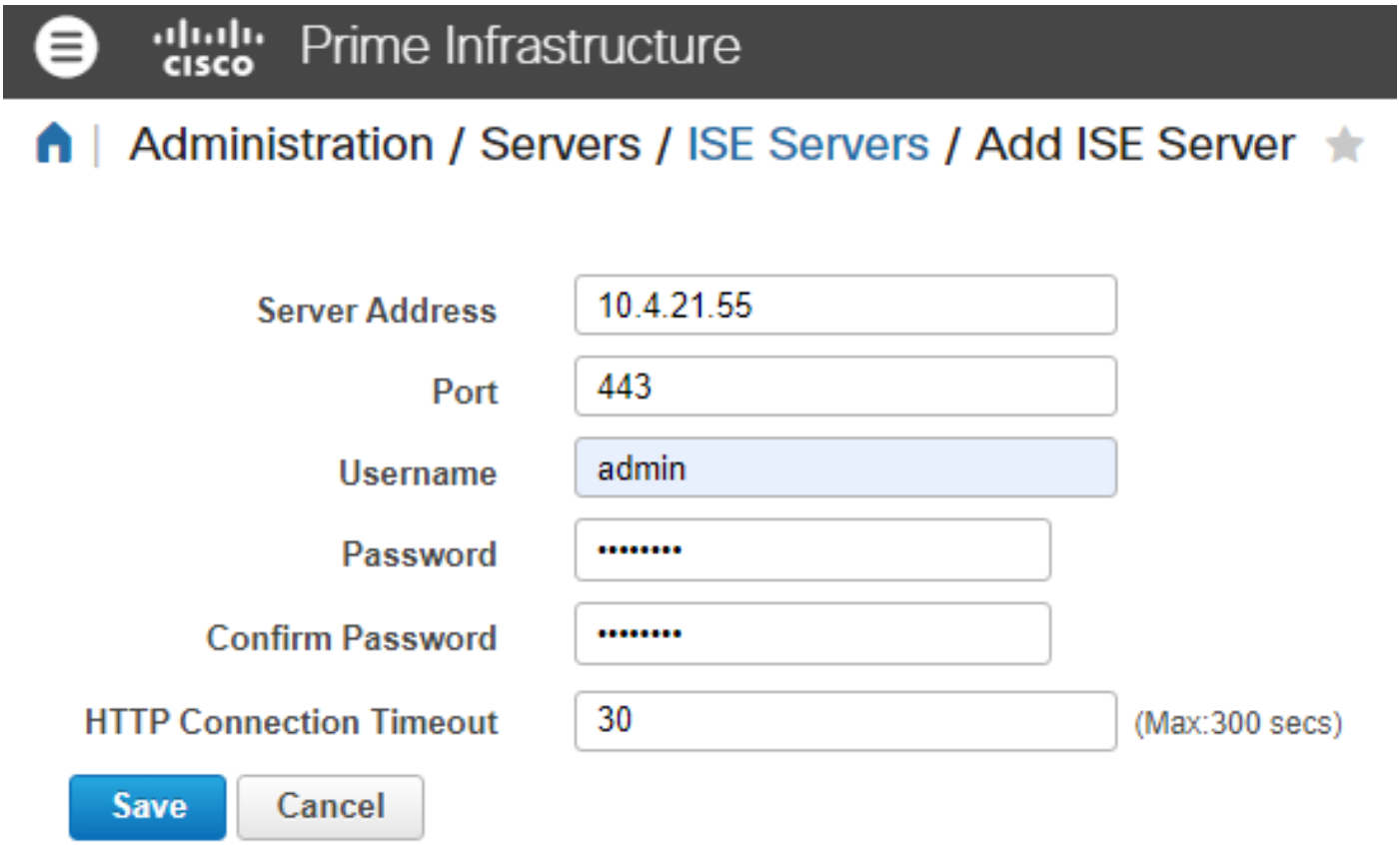
iii. 모든 필드를 채우고 저장을 클릭합니다.



참고: 기본 및 보조(해당되는 경우) 모니터링 ISE 노드에 대해 연결을 설정해야 합니다.



참고: 기본 포트는 443으로 설정되지만 ISE에서 열려 있는 다른 포트를 사용하여 연결을 설정할 수 있습니다.



iv. ISE Server 페이지로 다시 이동합니다. 서버 상태가 Reachable(연결 가능)로 표시되고 Role(역할)이 표시됩니다(Standalone(독립형), Primary(주) [MnT] 또는 Secondary(보조) [MnT]).

엔드포인트 컨피그레이션

10. dot1x(RFC 3850) 인증을 수행하도록 끝점을 구성해야 합니다. 이는 Cisco NAM(Network Access Manager)을 구성하거나 OS Native Supplicant를 활용하여 구현할 수 있습니다. 이 컨피그레이션과 관련된 설명서는 많으므로 이 설명서에 이러한 단계는 포함하지 않습니다.

다음을 확인합니다.

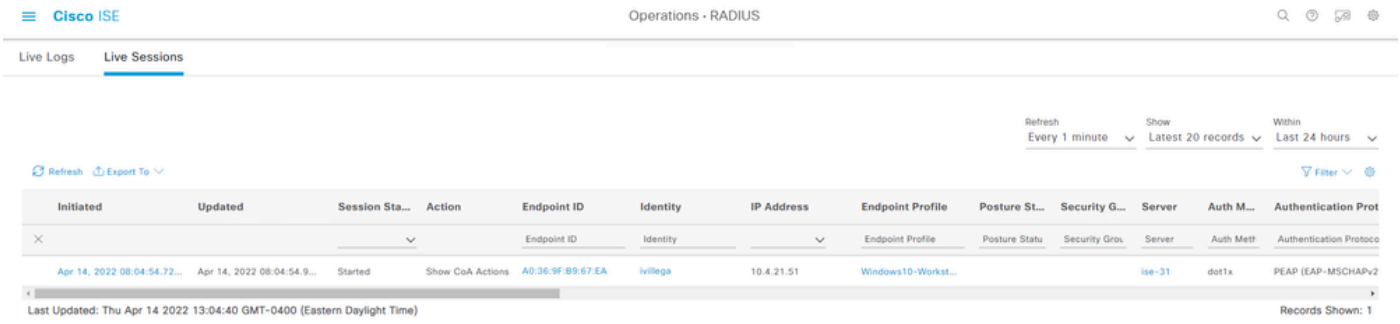
ISE 확인

ISE는 NAD로부터 RADIUS 요청을 받고 성공적으로 사용자를 인증합니다.

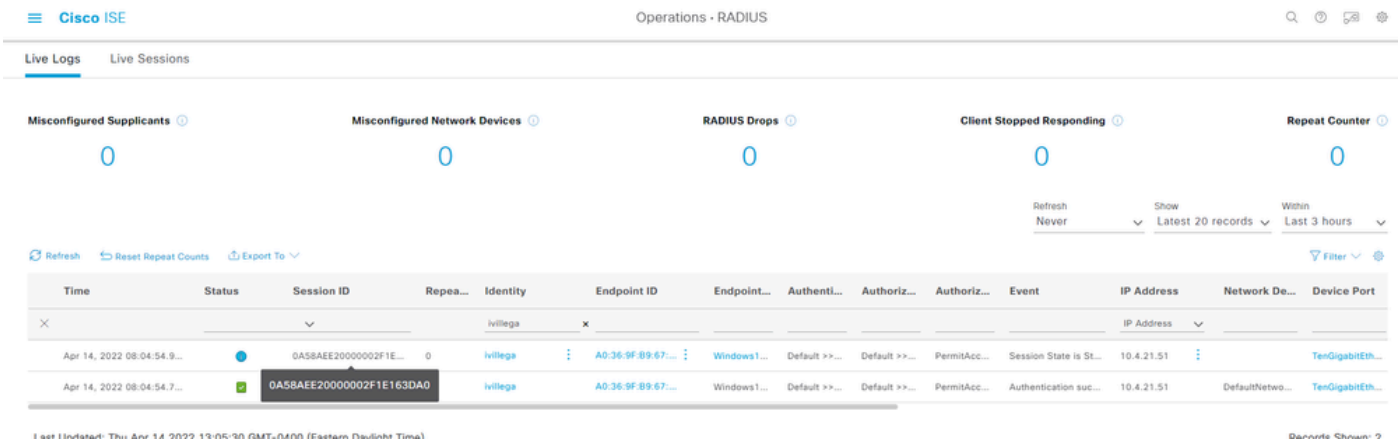
NAD는 ISE > Administration > Network Resources > Network Devices에서 RADIUS에 대해 추가 및 구성됩니다.

1. Operations(운영) > RADIUS > Live Sessions(라이브 세션)로 이동합니다.

사용자 라이브 세션이 이 페이지에 나열되어 있는지 확인합니다. 세션 정보는 Prime Infrastructure와 공유됩니다.



2 . Operations(운영) > RADIUS > Live Logs(라이브 로그)에서 세션 ID를 확인합니다.



NAD 확인

3. NAD에서 세션 세부사항을 확인 합니다. 세션 ID는 ISE의 세션 ID와 일치합니다.

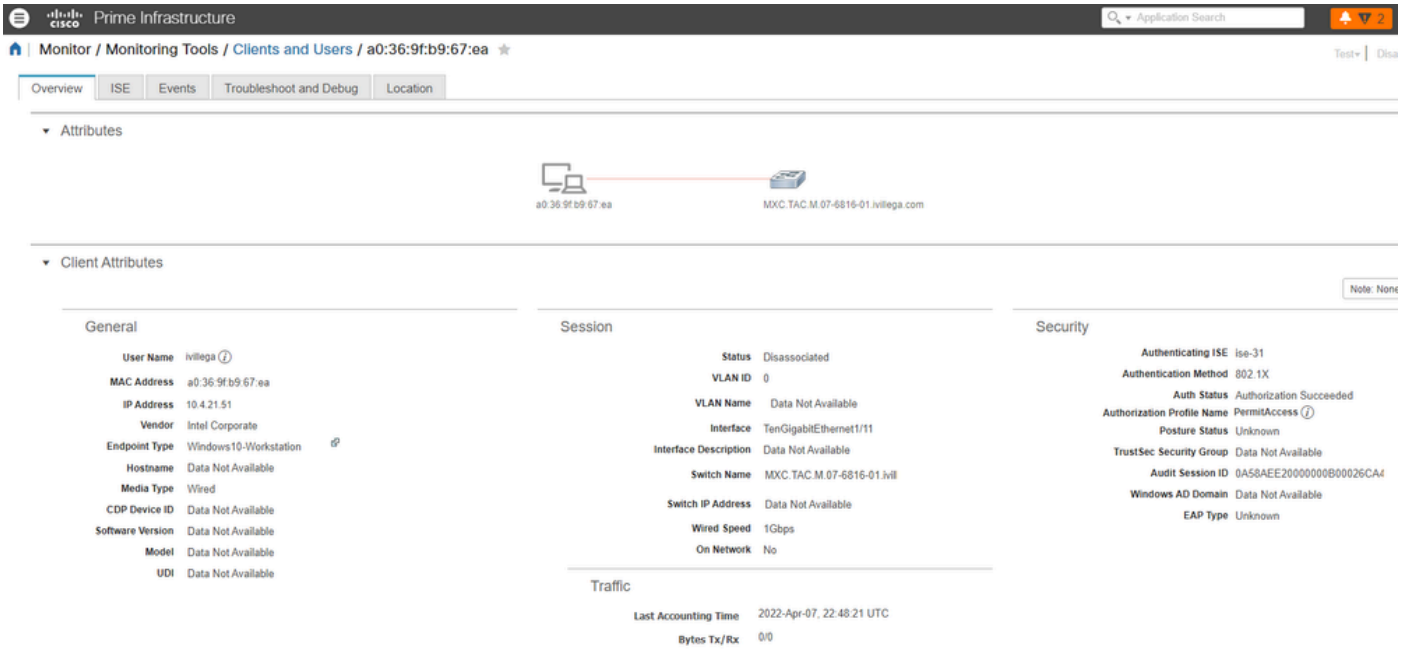
```
MXC.TAC.M.07-6816-01#show authentication session int Te1/11 detail
        Interface: TenGigabitEthernet1/11
      MAC Address: a036.9fb9.67ea
     IPv6 Address: Unknown
     IPv4 Address: 10.4.21.51
        User-Name: ivillega
           Status: Authorized
           Domain: DATA
   Oper host mode: multi-domain
 Oper control dir: both
  Session timeout: N/A
Common Session ID: 0A58AEE20000002F1E163DA0
  Acct Session ID: 0x00000023
           Handle: 0xD9000001
   Current Policy: POLICY_Te1/11

Method status list:
        Method      State
        dot1x       Authc Success
```

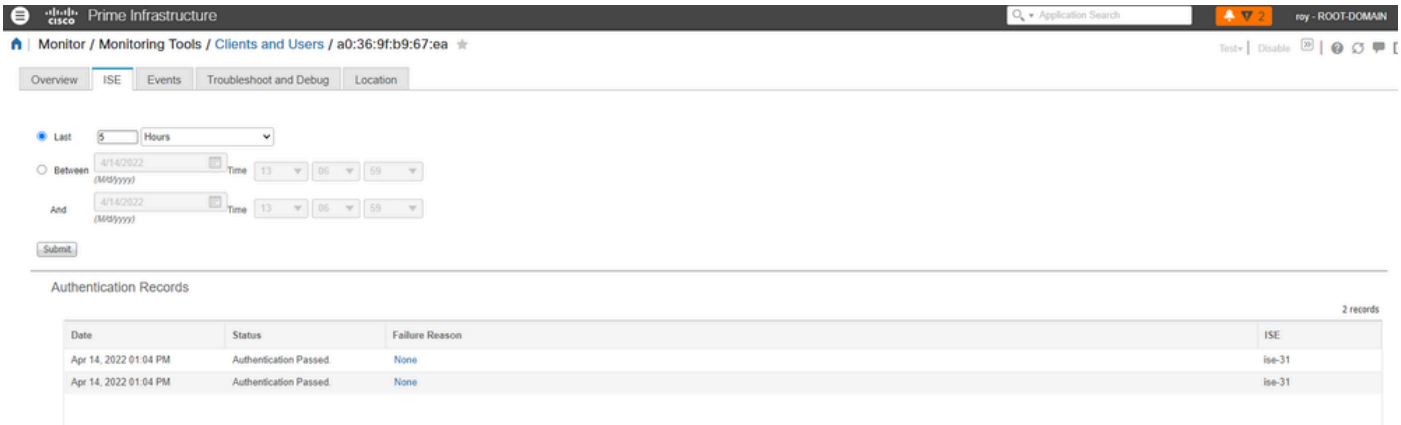
Prime Infrastructure 확인

4. 모니터링 > 모니터링 도구 > 클라이언트 및 사용자로 이동합니다. 엔드포인트의 MAC 주소가 표시됩니다.

5. 클릭하면 사용자 세션 세부사항 및 ISE 서버 정보가 표시됩니다.



6. 이 특정 엔드포인트에 대한 세션 이벤트를 검색할 수 있는 ISE라는 탭이 있습니다. Prime Infrastructure가 ISE에서 이벤트를 가져오는 데 사용하는 시간 프레임을 선택할 수 있습니다.



문제 해결

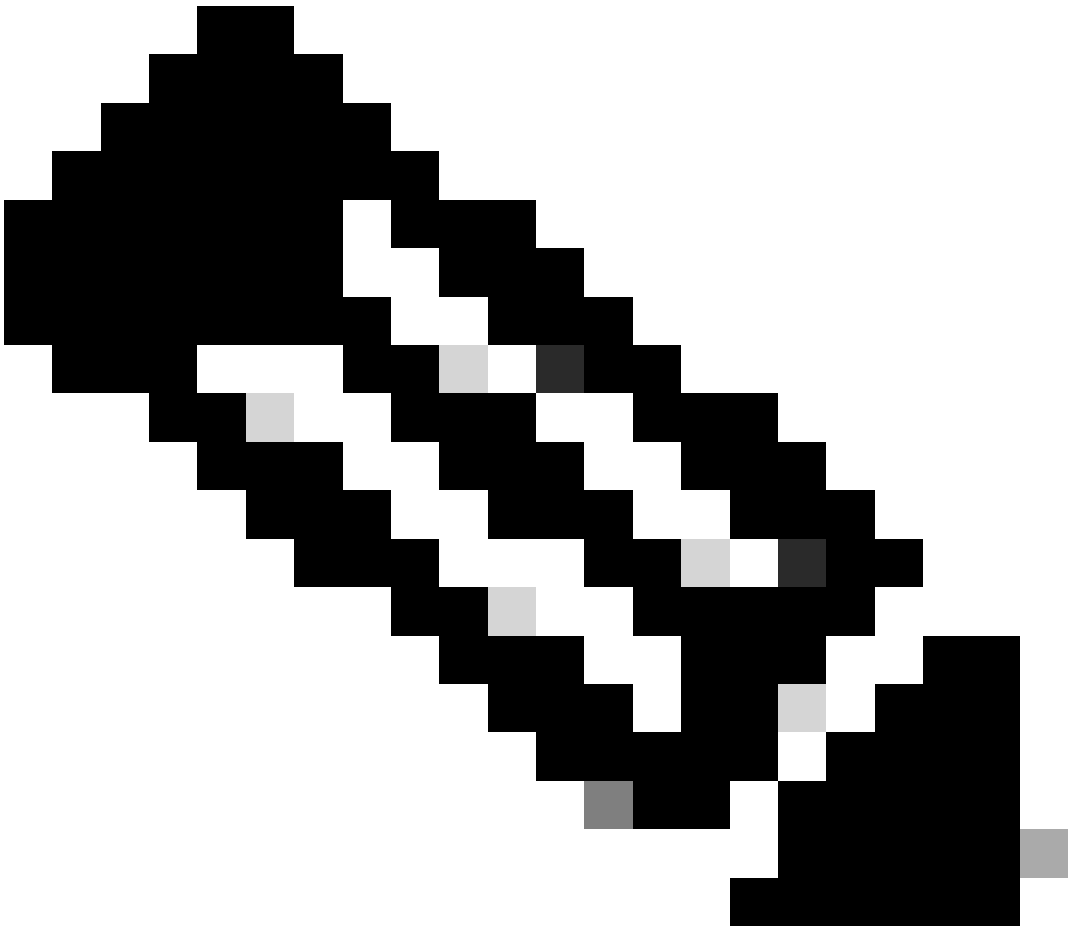
1. ping을 사용하여 ISE와 Prime Infrastructure 간의 연결을 테스트합니다. 연결이 없는 경우 ISE 또는 PI에서 추적 경로를 사용하여 문제를 찾을 수 있습니다.

2. 9단계에서 구성된 포트가 ISE MnT 노드에서 열려 있는지 확인합니다(기본 포트는 443).

```
ise-31-1/admin# show ports | include :443
     tcp: 0.0.0.0:80, 0.0.0.0:19444, 0.0.0.0:19001, 0.0.0.0:443
```

포트가 출력에 나열되어 있으면 ISE MnT에서 해당 포트를 연 것입니다.

출력이 없거나 포트가 나열되지 않으면 ISE MnT에서 해당 포트를 닫았음을 의미합니다. 이 경우 다른 포트로 시도하거나 ISE 팀과 TAC 케이스를 열어 포트가 열려 있지 않은 이유를 확인할 수 있습니다.



참고: ISE MnT 노드는 일부 포트만 사용하며, ISE 설치 가이드, 포트 참조 섹션에 나열되지 않은 ISE MnT 노드의 포트를 열 수 있는 방법이 없습니다.

---

3. Prime Infrastructure에서 텔넷을 사용하여 9단계에서 구성한 포트를 테스트합니다.

```
prime-testcom/admin# telnet 10.4.21.55 port 443
Trying 10.4.21.55...
Connected to 10.4.21.55.
```

텔넷 테스트의 출력이 <ISE MnT IP/FQDN>에 연결되어 있으면 테스트가 성공했음을 의미합니다.

텔넷 테스트의 출력이 Trying <ISE MnT IP/FQDN>에서 멈춘 경우 테스트 실패를 의미합니다. 이는 중간 네트워크 디바이스의 ACL 또는 방화벽 규칙과 관련될 수 있습니다.

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.