將ISE與Prime基礎設施整合以實現終端可視性

目錄

[簡介](#)

[必要條件](#)

- [需求](#)
- [採用元件](#)

[設定](#)

- [網路圖表](#)
- [組態](#)
  - [交換器組態](#)
  - [Cisco Prime Infrastructure Configuration](#)
  - [終端配置](#)

[驗證](#)

- [驗證ISE](#)
- [檢驗NAD](#)
- [驗證Prime基礎設施](#)

[疑難排解](#)

簡介

本文檔介紹如何將ISE與Prime基礎設施整合以獲得經身份驗證的終端的可視性。

必要條件

需求

思科建議您瞭解以下主題：

- 思科ISE。
- Cisco Prime Infrastructure。
- 終端針對ISE進行身份驗證的無線或有線AAA流。
- NAD（網路存取裝置）（例如交換器和WLC）上的SNMP組態。

採用元件

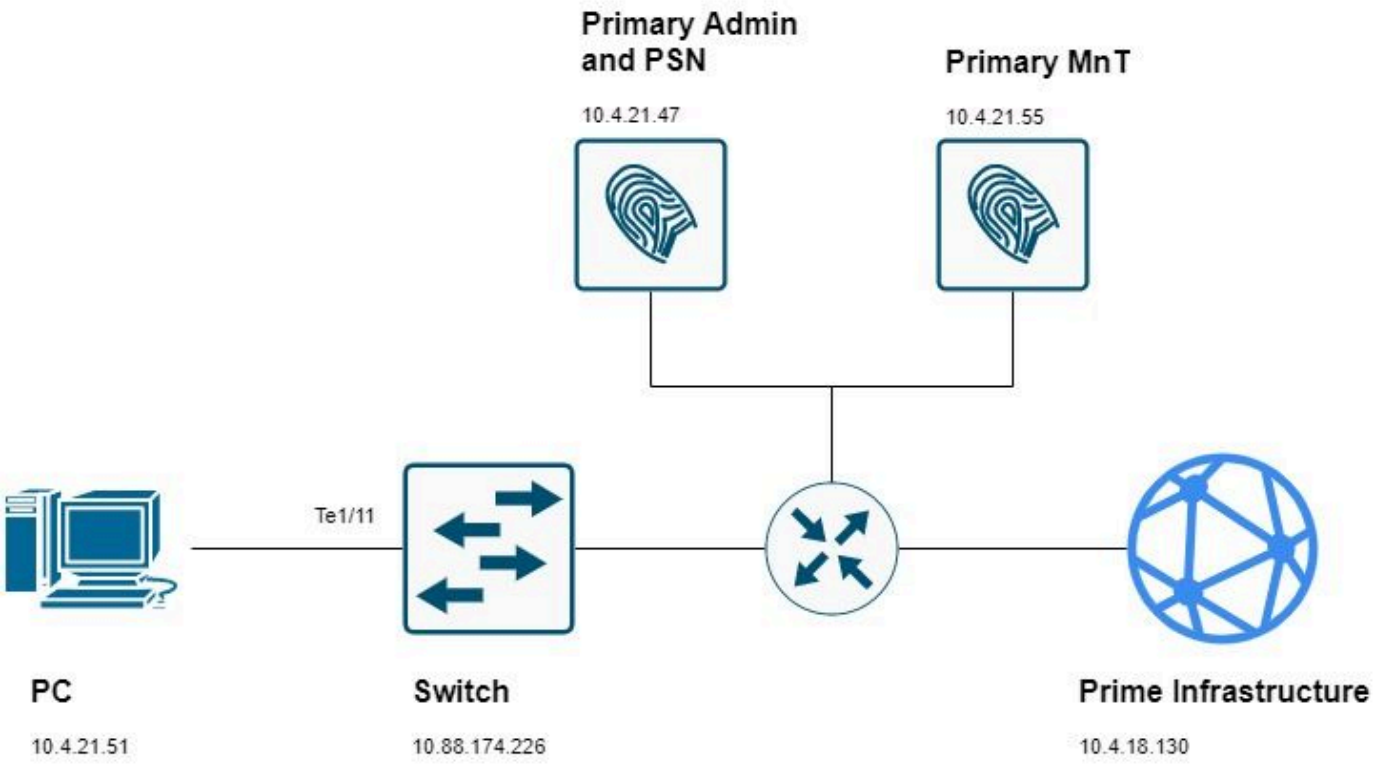
本文中的資訊係根據以下軟體和硬體版本：

- ISE 3.1部署。
- Cisco Prime基礎架構3.8.
- 執行Cisco IOS® 15.5的C6816-X-LE。
- Windows 10電腦。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

網路圖表



組態

交換器組態

1.配置網絡接入裝置(NAD)以對ISE進行AAA身份驗證。在本指南中，您將使用以下配置：

```
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.在switch:

```
device-tracking policy DT1
 tracking enable

device-tracking tracking auto-source
```

3.為switchport配置dot1x身份驗證，並將裝置跟蹤策略連線到該埠：

```
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.配置RO SNMP社群和SNMP陷阱以滿足網路要求（或者，您可以配置RW社群）：

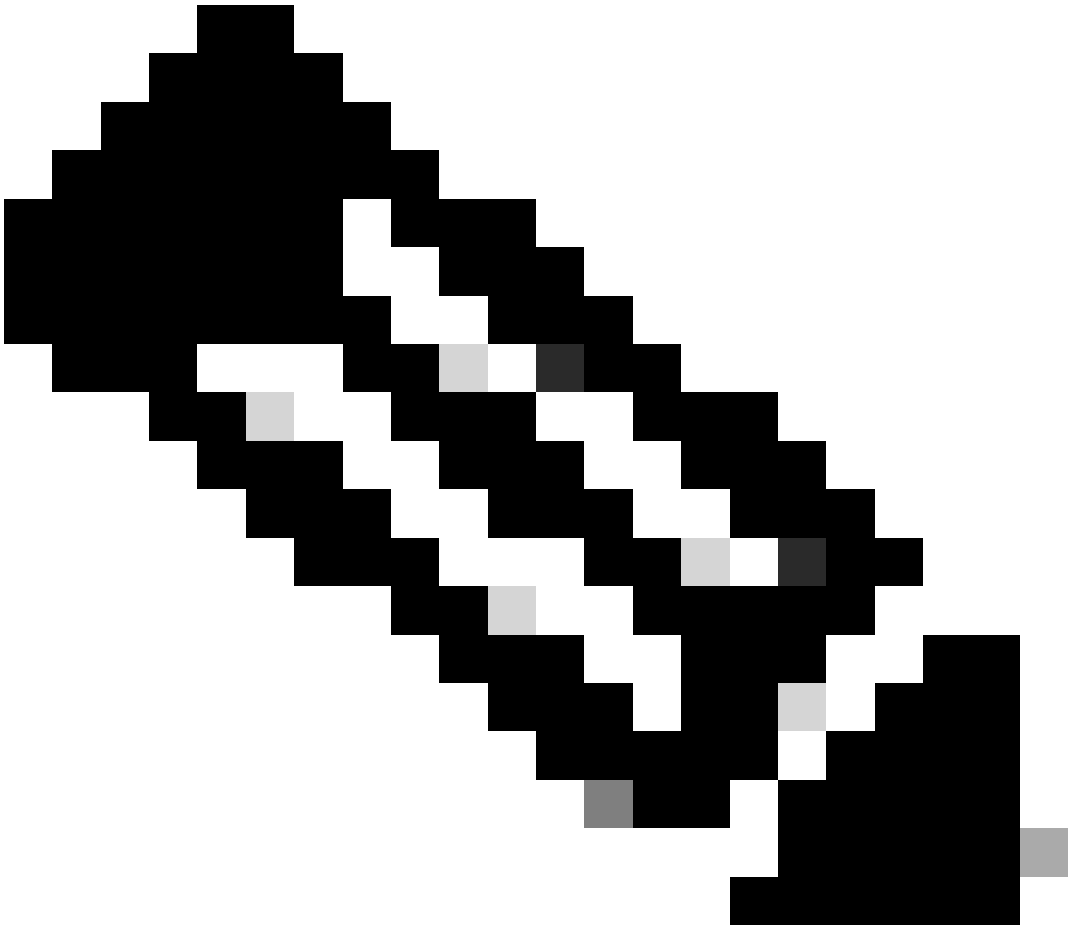
```
snmp-server community public RO
snmp-server community private RW
snmp-server trap-source TenGigabitEthernet1/16
snmp-server source-interface informs TenGigabitEthernet1/16
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps aaa_server
snmp-server 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.配置Telnet或SSH訪問，以便Prime可以管理裝置：

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

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

6.（可選）對於SSH連線，需要RSA金鑰。如果NAD沒有NAD，請使用以下步驟生成它。

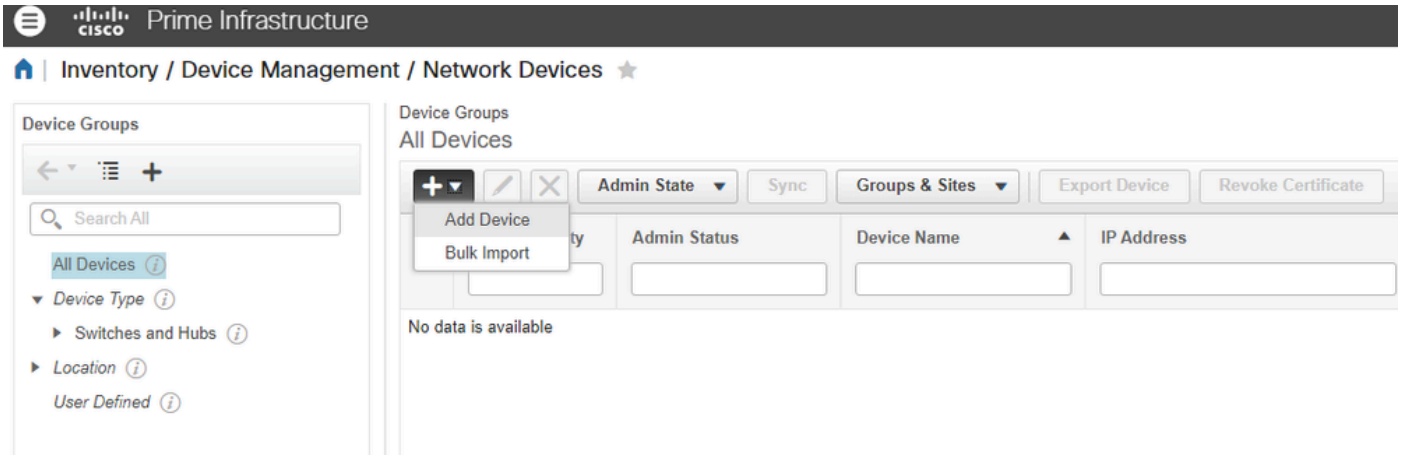


附註：某些裝置在生成RSA之前需要已配置的域。檢查裝置是否配置了域，以便不覆蓋現有域。

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

Cisco Prime Infrastructure Configuration

7.在清單>裝置管理>網路裝置>加號(+)>新增裝置中新增網路裝置:



要完成庫存，必須填寫以下欄位：

對於有線裝置：

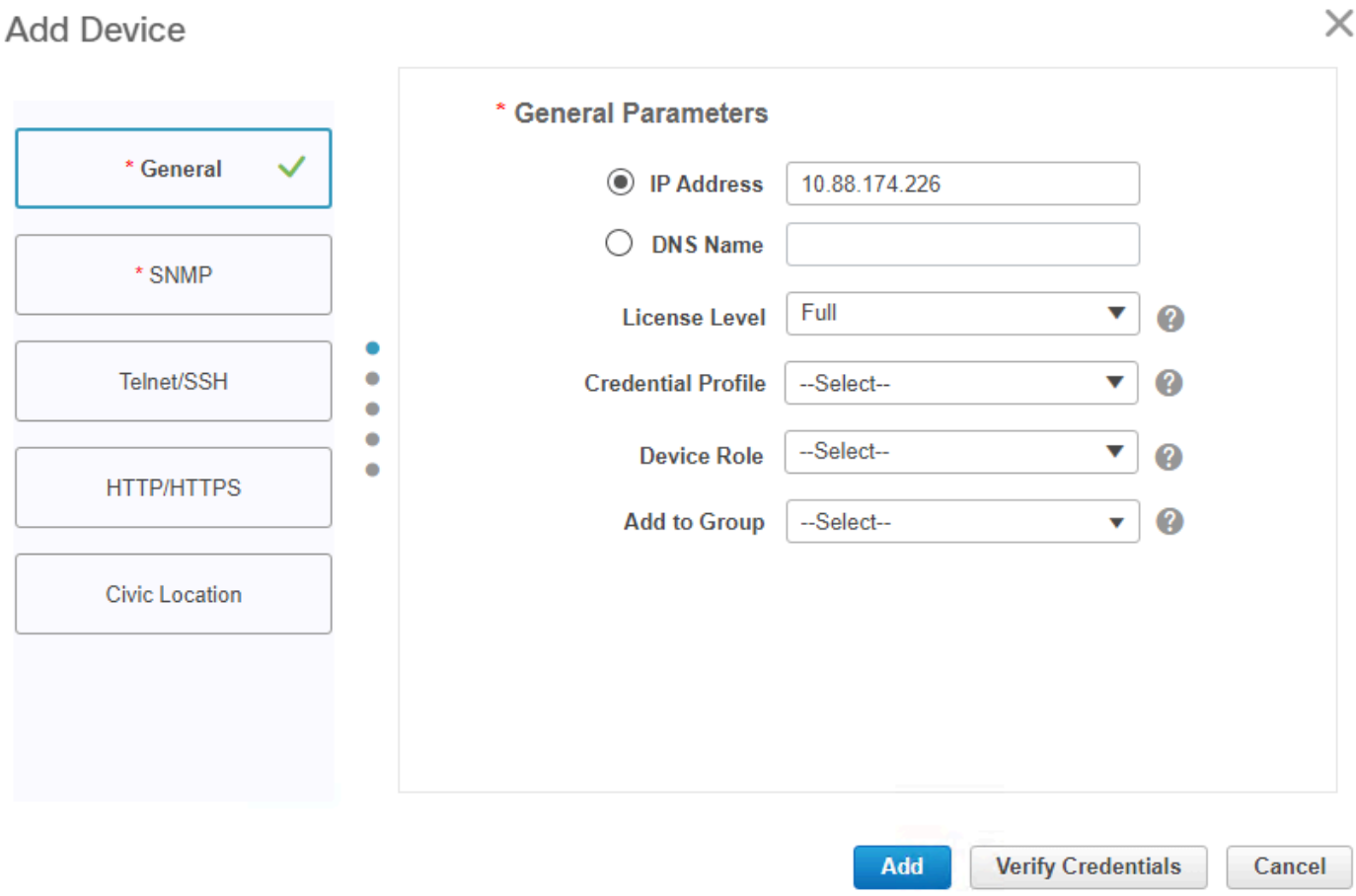
- 一般：IP或DNS。
- SNMP:需要RO社群 — 請務必也在交換器/WLC中設定該社群。
- Telnet/SSH:執行模式和啟用模式憑據。

對於WLC:

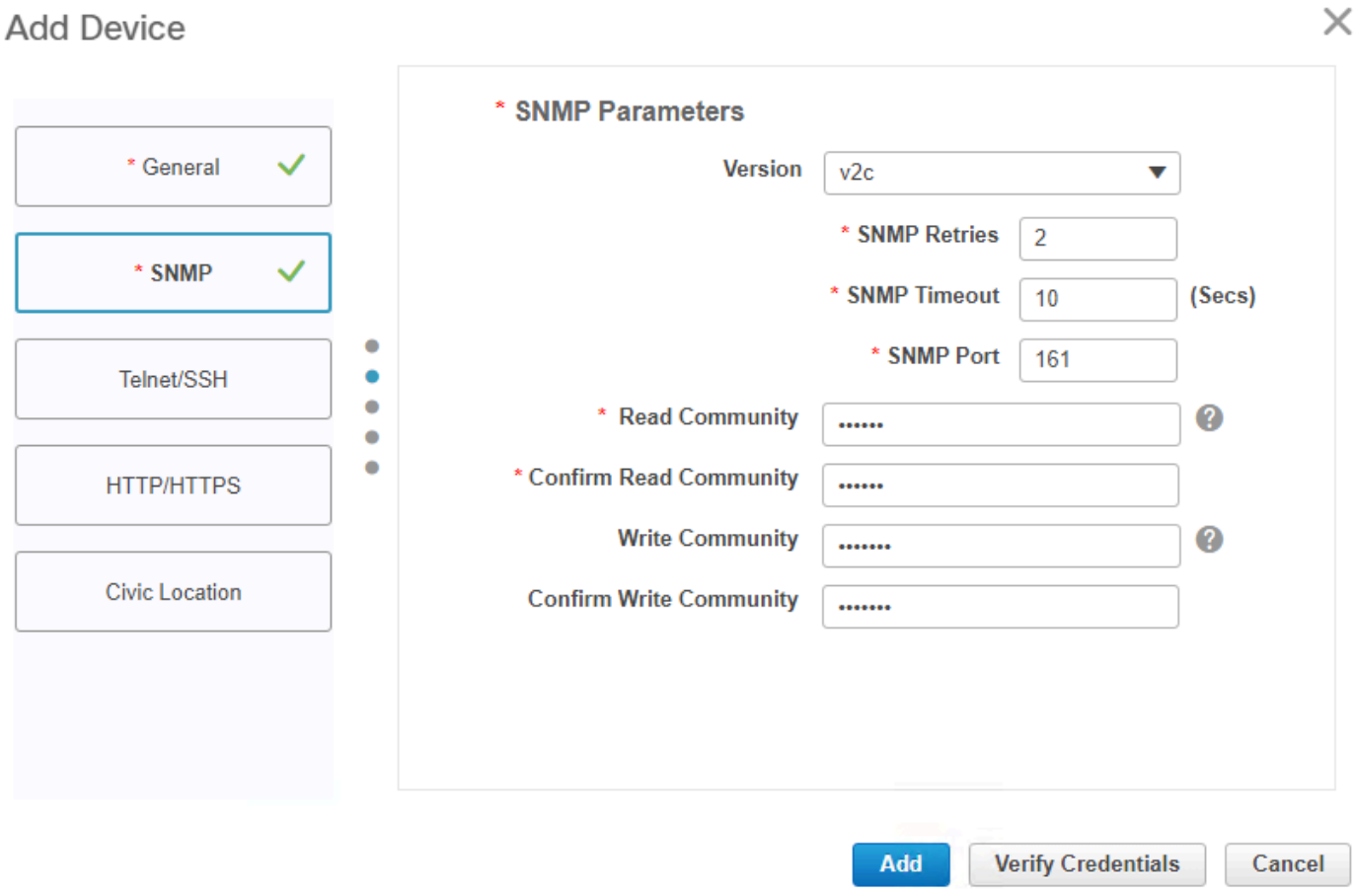
- 一般：IP或DNS。
- SNMP:需要RO社群 — 請務必也在交換器/WLC中設定該社群。

在本指南中，您使用的是Cisco Switch:

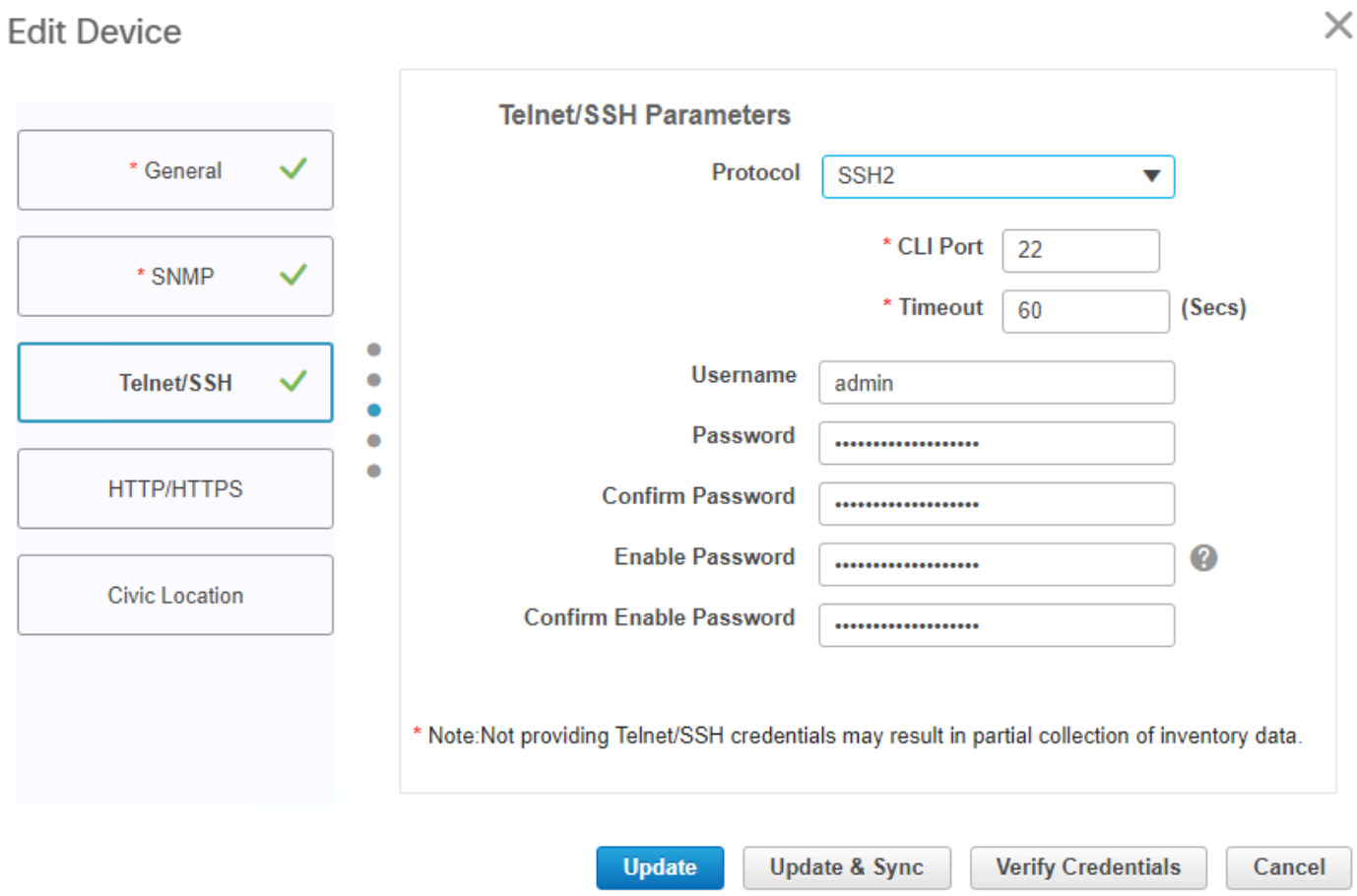
i.一般部分：


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

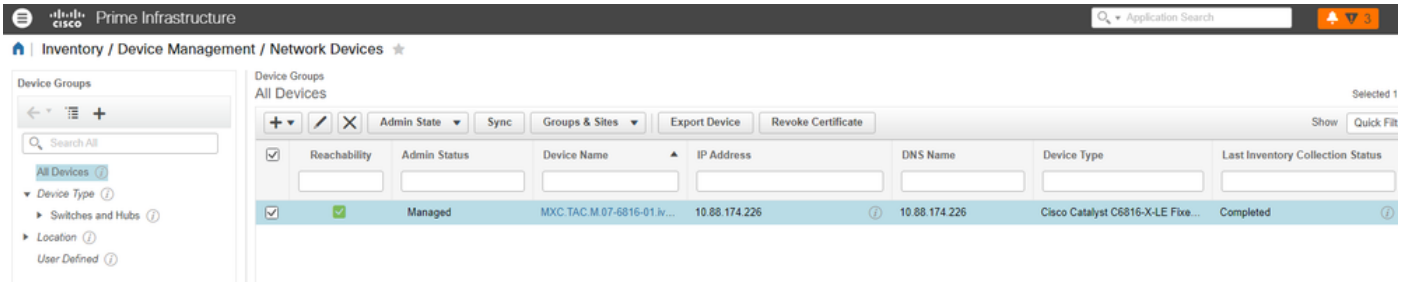
二。SNMP 區段:


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

三。Telnet/SSH部分：



8.完成所有必填欄位後，確保Reachability和Collection Status分別為Green和Completed:

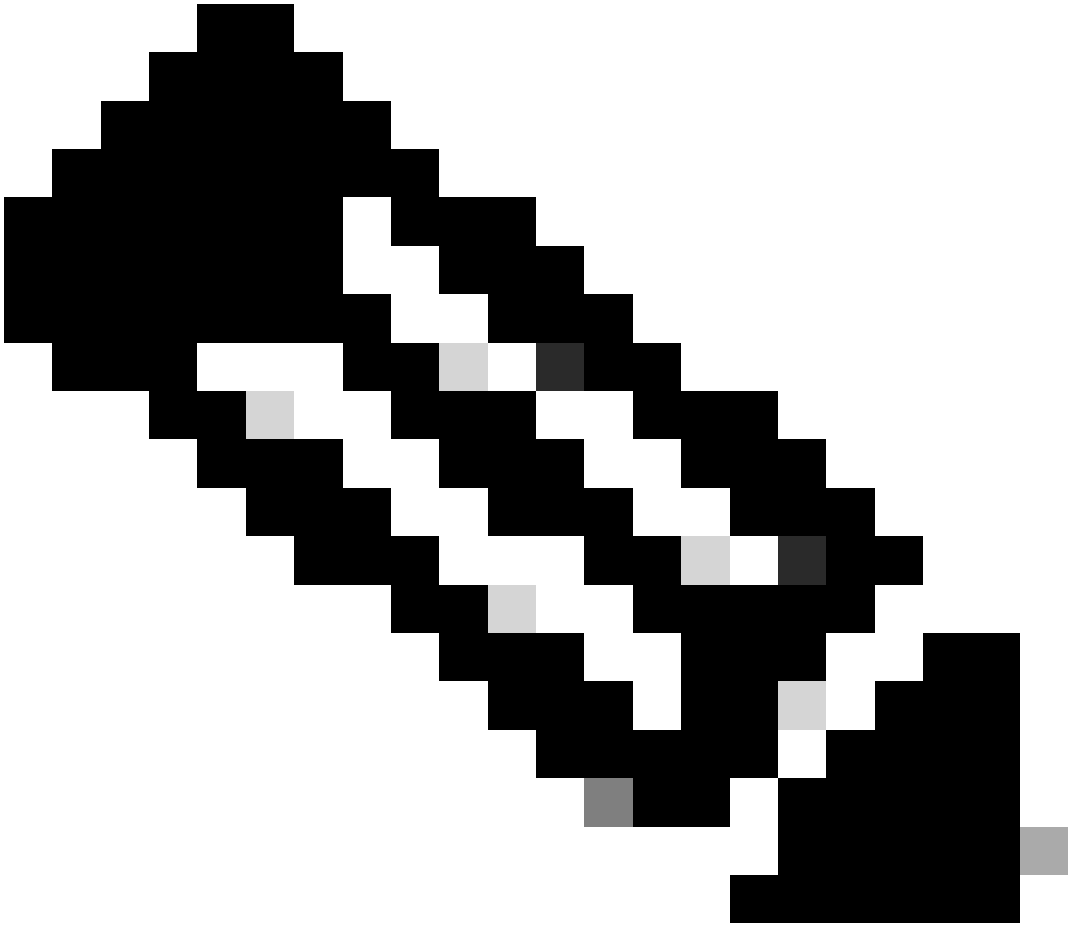


9.將Prime與ISE整合。

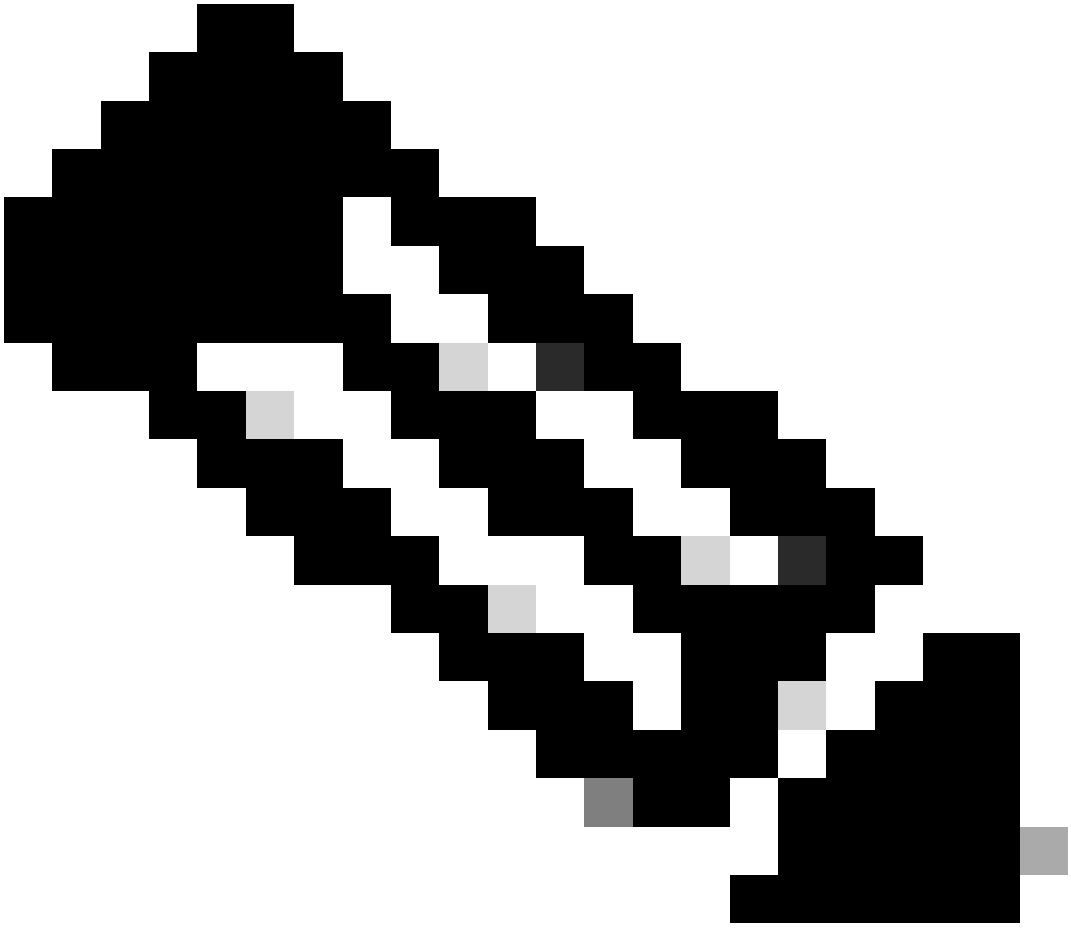
i.導航到Administration > Servers > ISE Servers。

二。在下拉選單中，選擇Add ISE Server，然後按一下Go:

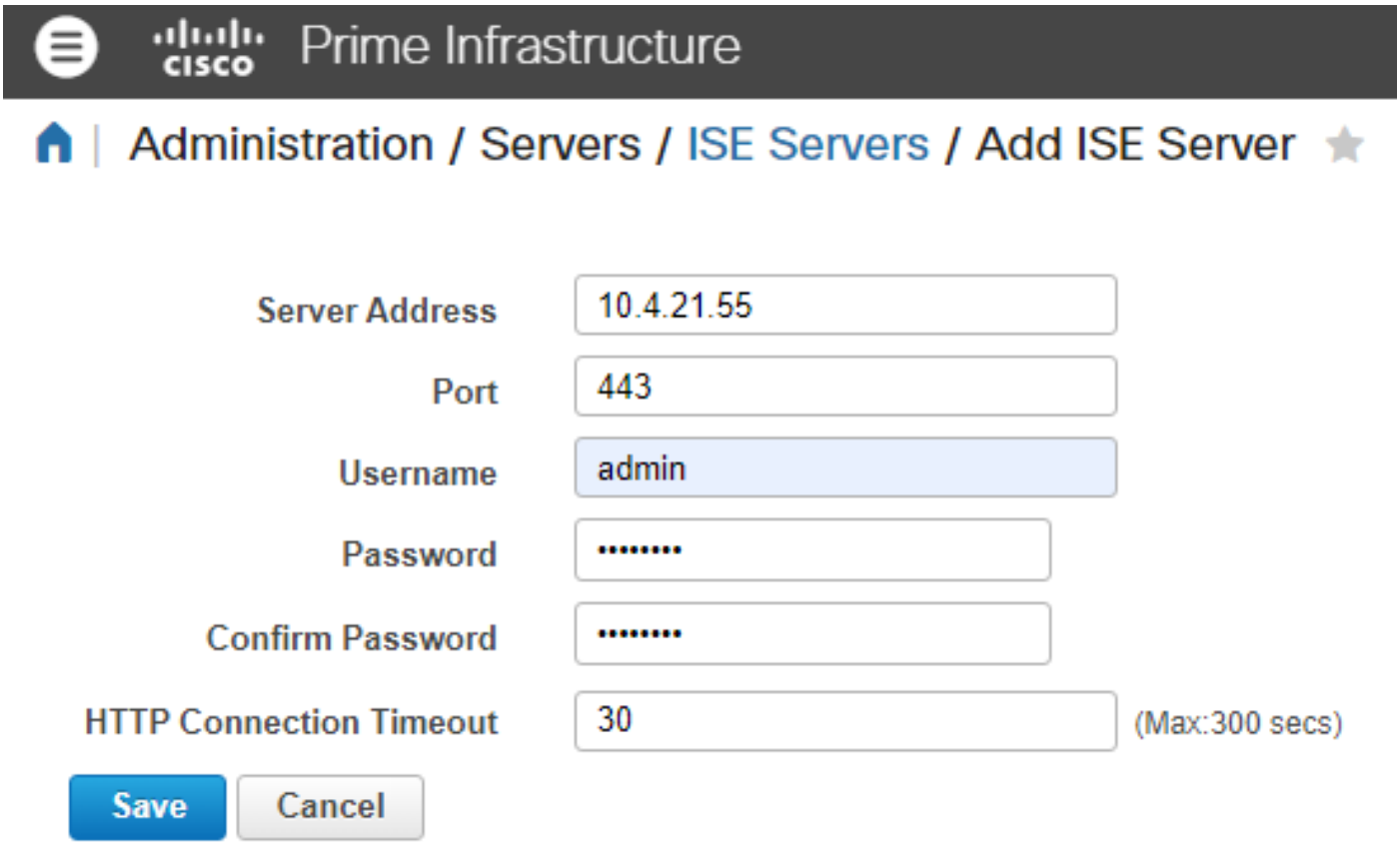
三。填寫所有欄位，然後按一下Save。



附註：必須針對主要和輔助（如果適用）監控ISE節點建立連線。



附註：預設埠設定為443，但您可以使用ISE中任何其他開啟的埠建立連線。



四。導航回到ISE Server頁面。伺服器狀態顯示「可訪問」(Reachable)並顯示「角色」(Role)（Standalone、Primary [MnT]或Secondary [MnT]）：

終端配置

10.必須將端點配置為執行dot1x(RFC 3850)身份驗證。這可以通過配置Cisco Network Access Manager(NAM)或利用OS Native Supplicant客戶端來實現。有許多關於此配置的指南，因此我們不包括本指南中的這些步驟。

驗證

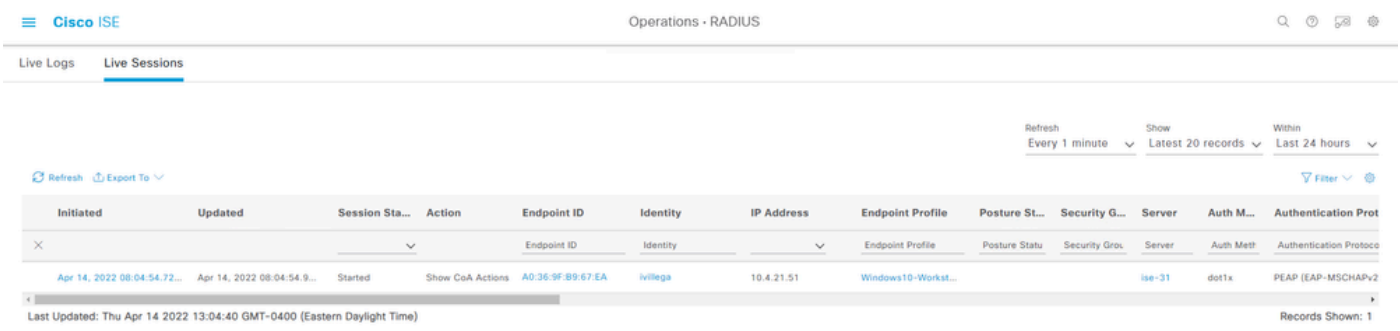
驗證ISE

ISE從NAD接收RADIUS請求並成功驗證使用者。

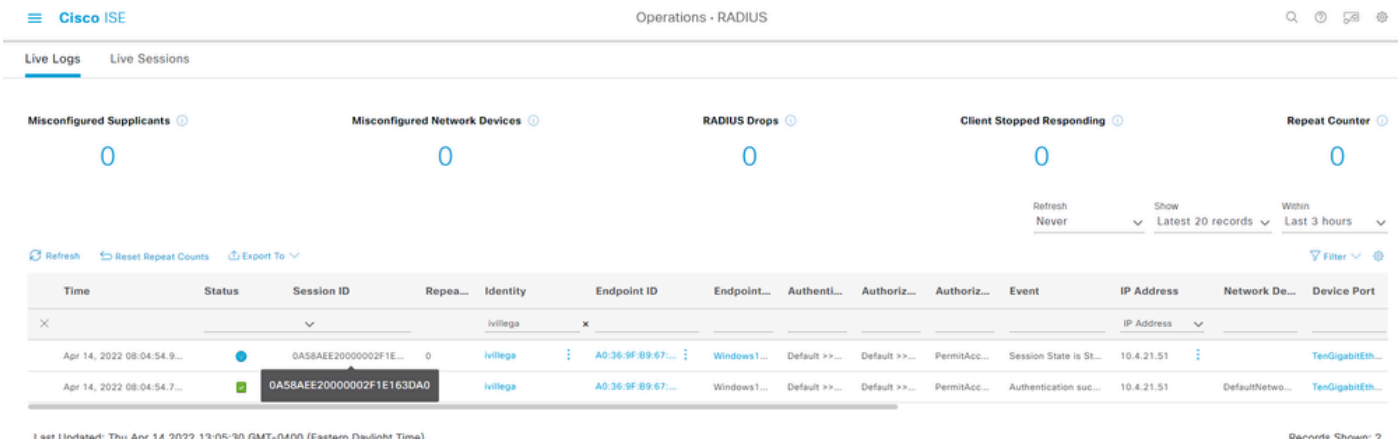
在ISE > Administration > Network Resources > Network Devices中新增並配置NAD。

1.導覽至Operations > RADIUS > Live Sessions。

確保此頁中列出了使用者即時會話。會話資訊與Prime基礎設施共用。



2. 在Operations > RADIUS > Live Logs中檢查會話ID:



檢驗NAD

3.檢查NAD中的會話詳細資訊。會話ID與ISE中的會話ID匹配：

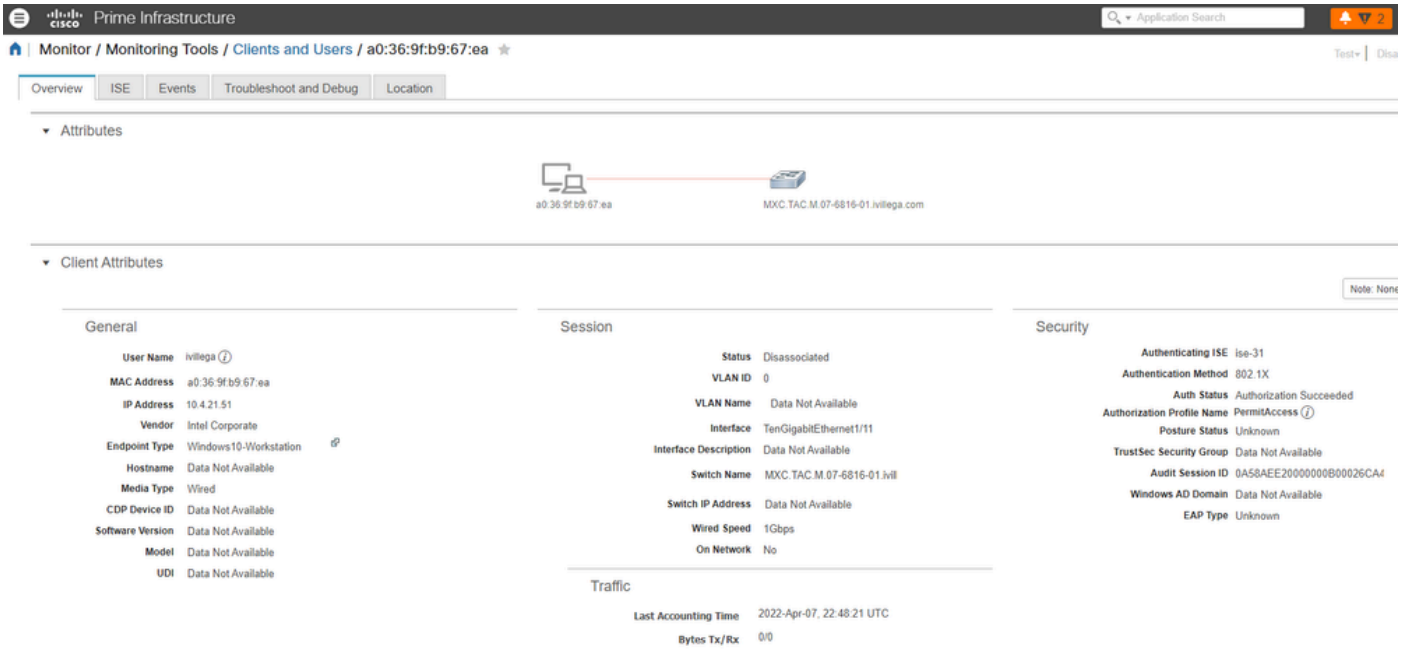
```
MXC.TAC.M.07-6816-01#show authentication session int Te1/11 detail
        Interface: TenGigabitEthernet1/11
      MAC Address: a036.9fb9.67ea
     IPv6 Address: Unknown
     IPv4 Address: 10.4.21.51
        User-Name: ivillega
           Status: Authorized
           Domain: DATA
   Oper host mode: 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
```

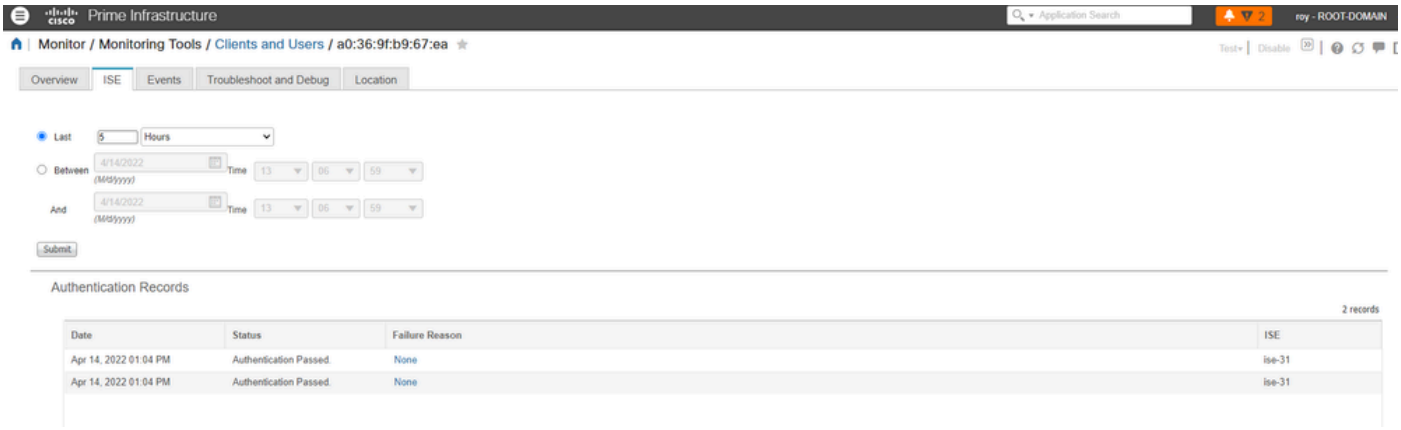
驗證Prime基礎設施

4.定位至監控>監控工具>客戶機和使用者。終端的MAC地址顯示：

5.如果按一下它，您將看到使用者會話詳細資訊和ISE伺服器資訊：



6.還有一個標籤為ISE的頁籤用於檢索此特定端點的會話事件。您可以選擇Prime Infrastructure用於從ISE提取事件的時間範圍：



疑難排解

1.使用ping測試ISE和Prime基礎設施之間的連通性。如果沒有連線，您可以使用來自ISE或PI的跟蹤

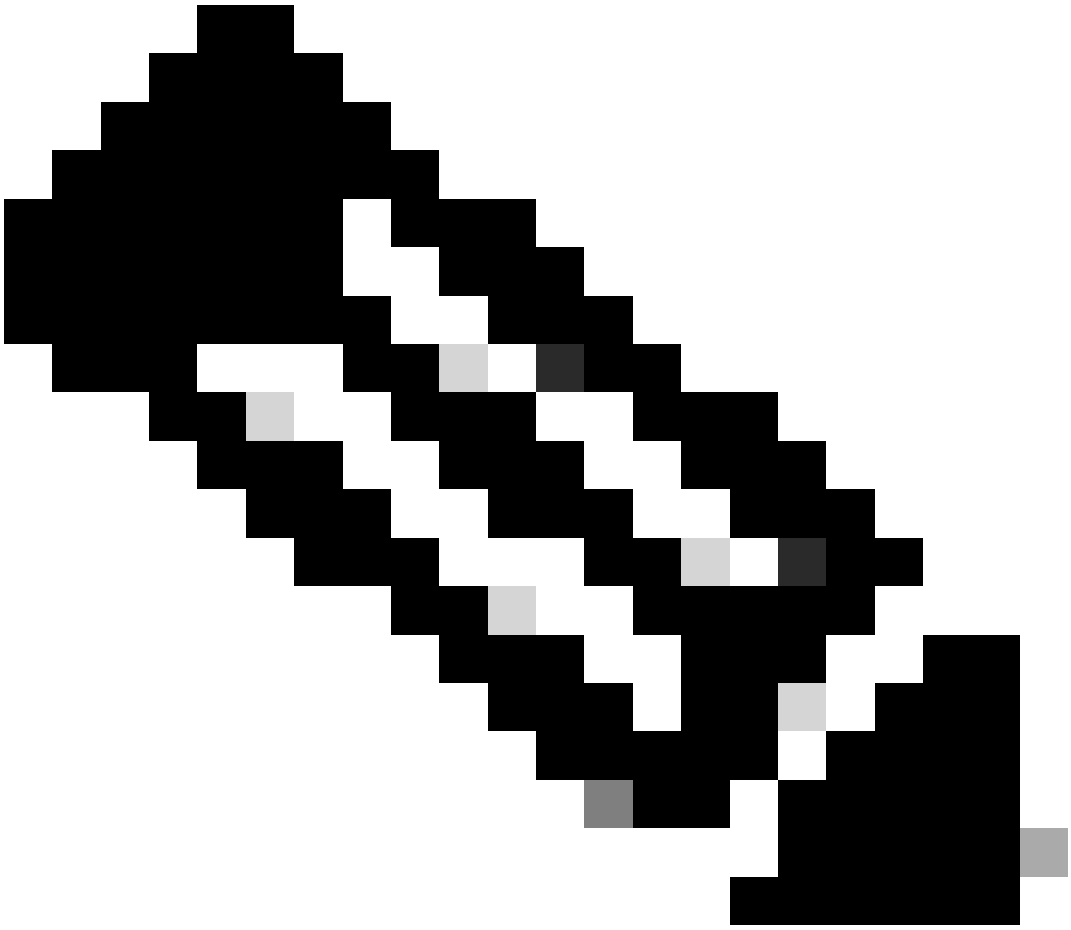
路由查詢問題。

2.檢查步驟9中配置的埠是否在ISE MnT節點中開啟（預設埠為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
```

如果輸出中列出埠，則表示ISE MnT已開啟埠。

如果沒有輸出或未列出埠，則表示ISE MnT已關閉該埠。在這種情況下，您可以嘗試使用另一個埠，或通過ISE團隊開啟TAC案例，檢查埠未開啟的原因。



附註：ISE MnT節點僅使用某些埠，無法開啟ISE MnT節點中未在ISE安裝指南「埠參考」部分列出的埠。

3.使用從Prime基礎設施的Telnet測試步驟9中配置的埠：

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

如果telnet測試的輸出為Connected to <ISE MnT IP/FQDN>，則表示測試成功。

如果telnet測試的輸出停滯在<ISE MnT IP/FQDN>，則表示測試失敗。可能與中間網路裝置中的ACL相關，或與防火牆規則相關。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。