# ISEとPrime Infrastructureの統合によるエンドポイントの可視化

## 内容


はじめに

前提条件

- 要件
- 使用するコンポーネント

設定

- ネットワーク図
- コンフィギュレーション
  - スイッチの設定
  - Cisco Prime Infrastructureの設定
  - エンドポイントの設定

確認

- ISEの確認
- NADの確認
- Prime Infrastructureの確認

トラブルシュート


## はじめに

このドキュメントでは、ISEとPrime Infrastructureを統合して、認証されたエンドポイントを可視化する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Cisco ISE.
- Cisco Prime Infrastructure.
- ISEに対して認証するエンドポイントのワイヤレスまたは有線AAAフロー。
- スイッチやWLCなどのNAD（ネットワークアクセスデバイス）でのSNMP設定

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

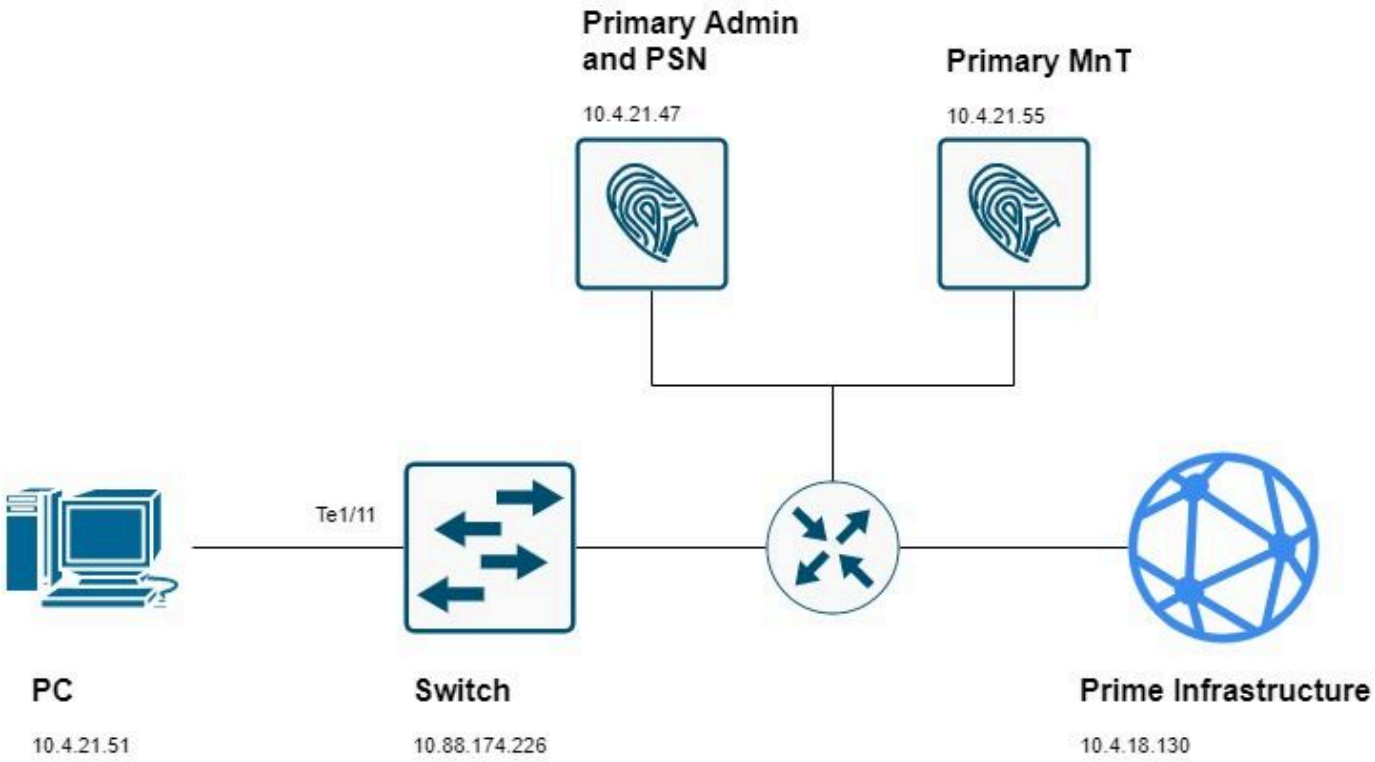
- ISE 3.1の導入
- Cisco Prime Infrastructure 3.8.

- Cisco IOS® 15.5が稼働するC6816-X-LE
- Windows 10 マシン.

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

# 設定

## ネットワーク図




## コンフィギュレーション

### スイッチの設定

1. ISEに対するAAA認証用にネットワークアクセスデバイス(NAD)を設定します。このガイドでは、次の設定を使用します。

```
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. スイッチでデバイストラッキングを設定します。

```
device-tracking policy DT1
 tracking enable

device-tracking tracking auto-source
```

3. dot1x認証用のswitchportを設定し、デバイストラッキングポリシーをアタッチします。

```
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. ネットワークの要件を満たすようにRO SNMPコミュニティとSNMPトラップを設定します（オプションで、RWコミュニティを設定できます）。

```
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
```

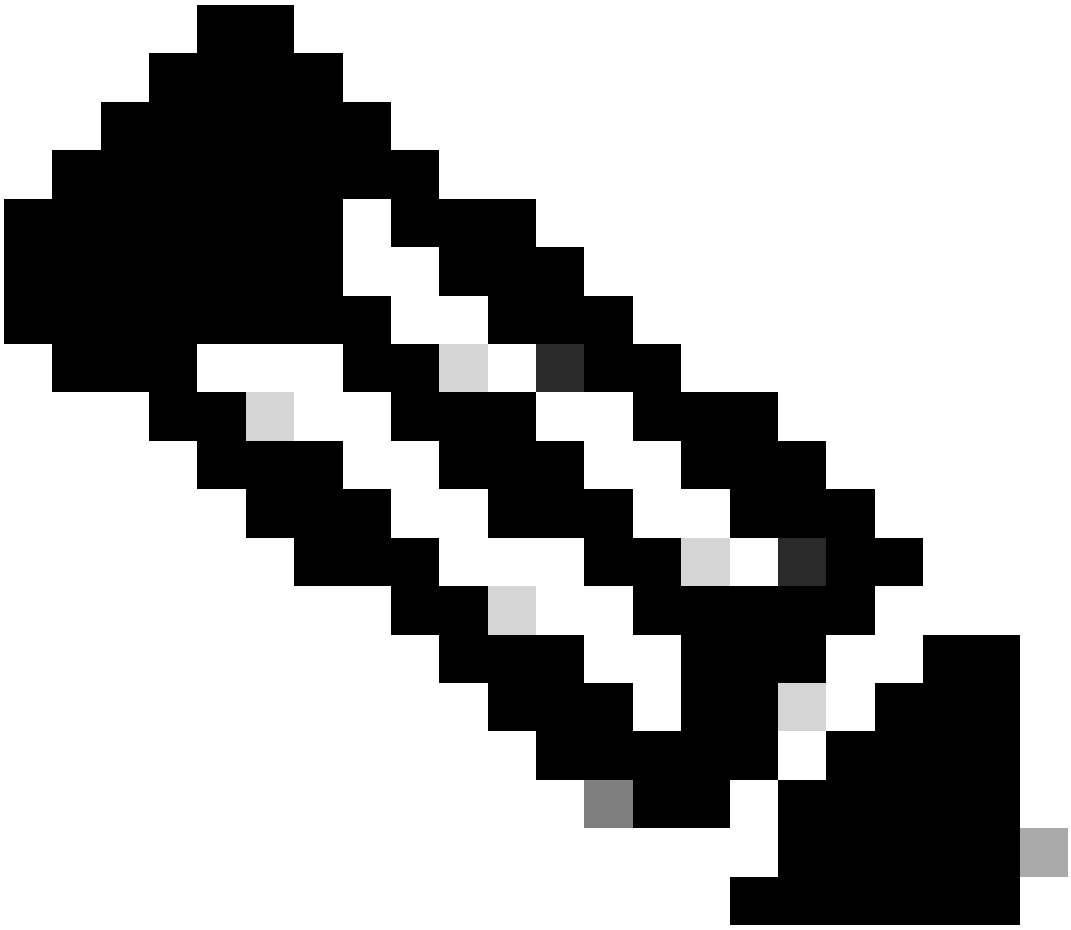
5. Primeでデバイスを管理できるように、TelnetまたはSSHアクセスを設定します。

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

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

6.（オプション）SSH接続では、RSAキーが必要です。NADにNADがない場合は、次の手順を使用してNADを生成します。

---



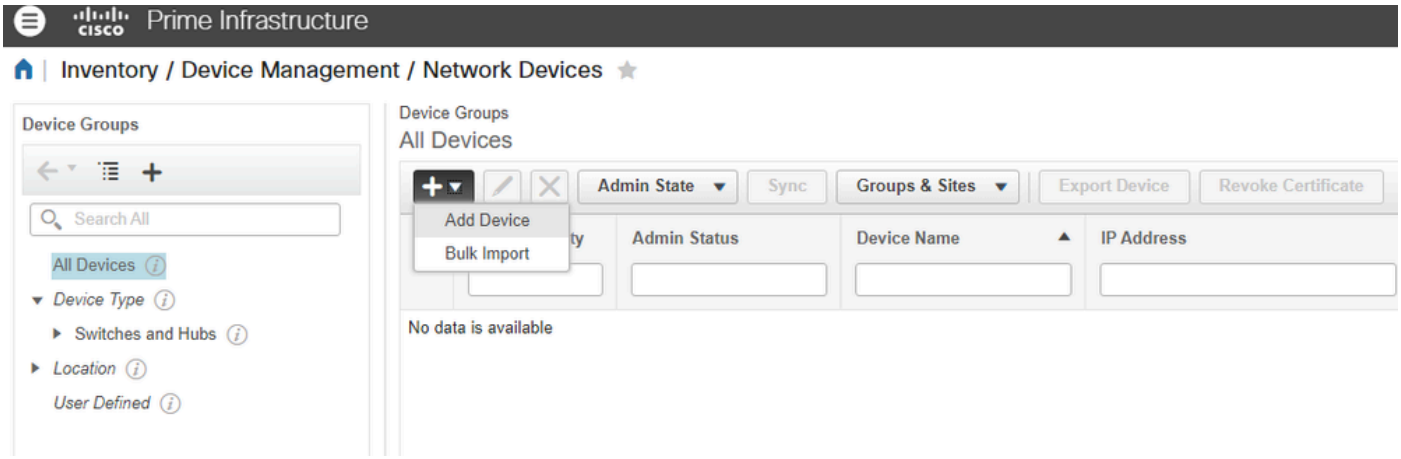
注：一部のデバイスでは、RSAを生成する前に設定済みのドメインが必要です。既存のドメインを上書きしないように、デバイスにドメインが設定されているかどうかを確認します。

---

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

Cisco Prime Infrastructureの設定

7. Inventory > Device Management > Network Devices > Plus sign (+) > Add Deviceの順に選択し、ネットワークデバイスを追加します。




インベントリを完了するための必須フィールドは次のとおりです。

有線デバイス：

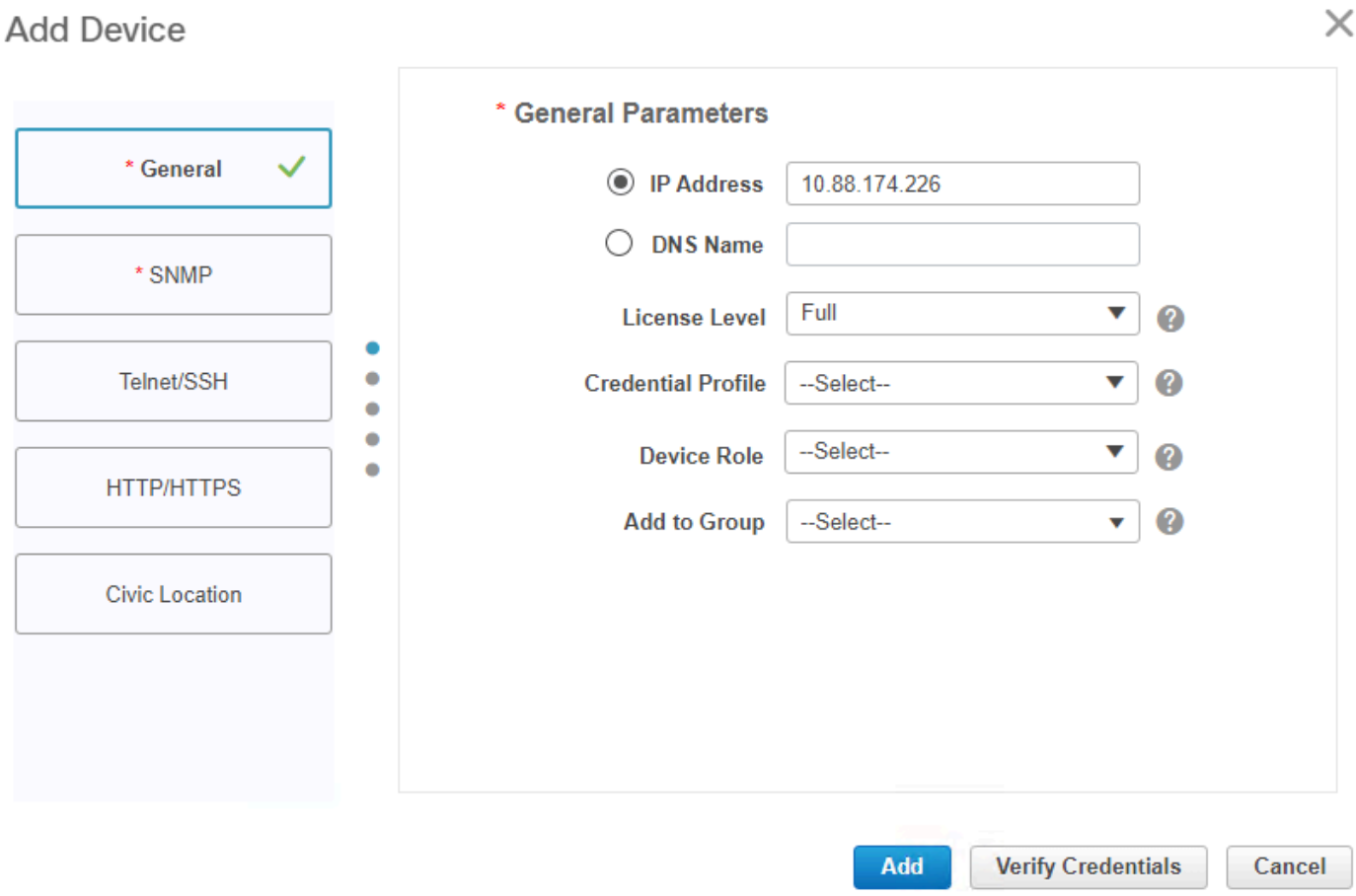
- 一般：IPまたはDNS。
- SNMP:ROコミュニティが必要です。スイッチ/WLCでも必ず設定してください。
- Telnet/SSH:Execモードおよびイネーブルモードのクレデンシャル。

WLCの場合：

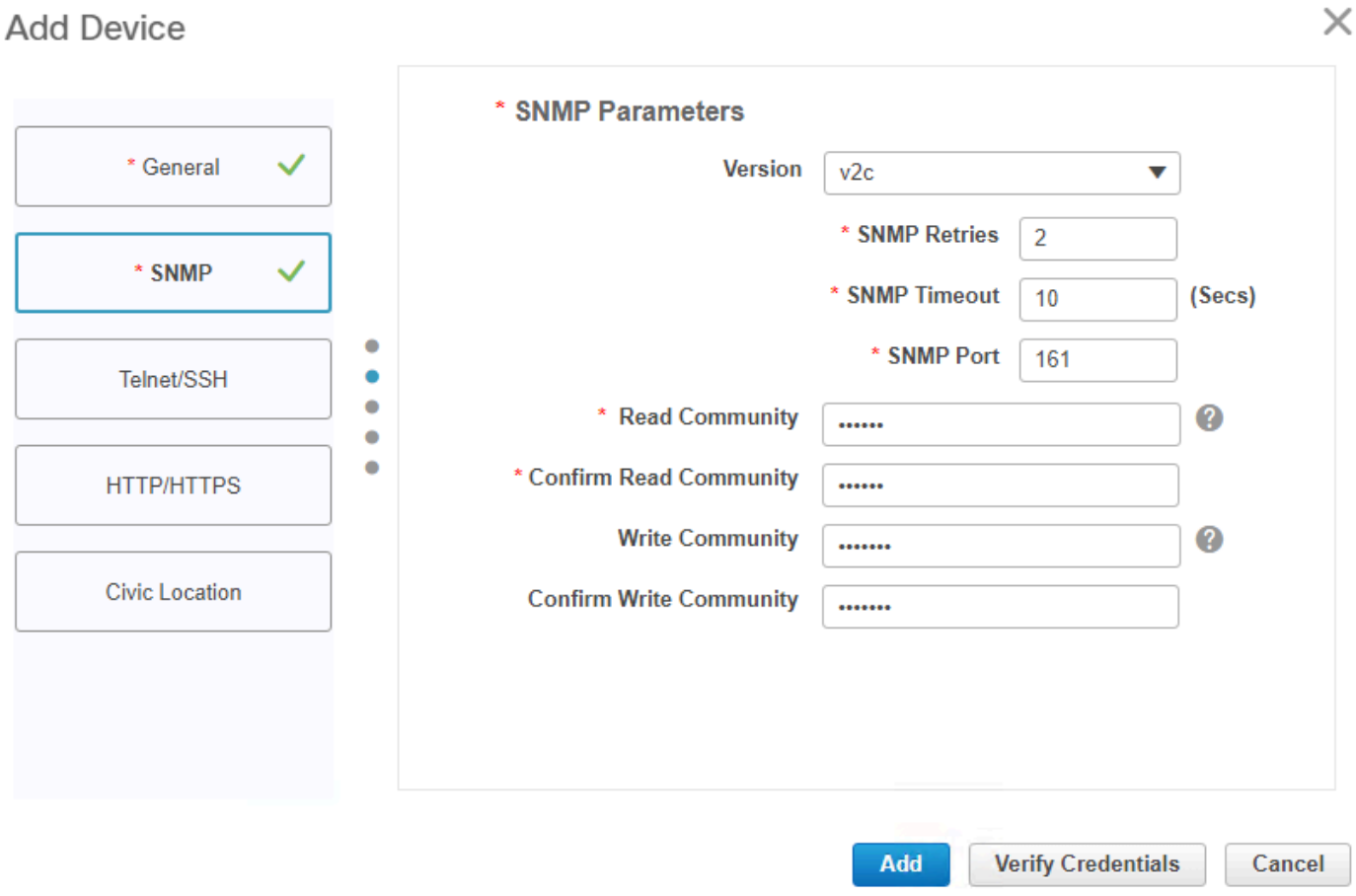
- 一般：IPまたはDNS。
- SNMP:ROコミュニティが必要です。スイッチ/WLCでも必ず設定してください。

このガイドでは、次のシスコスイッチを使用しています。

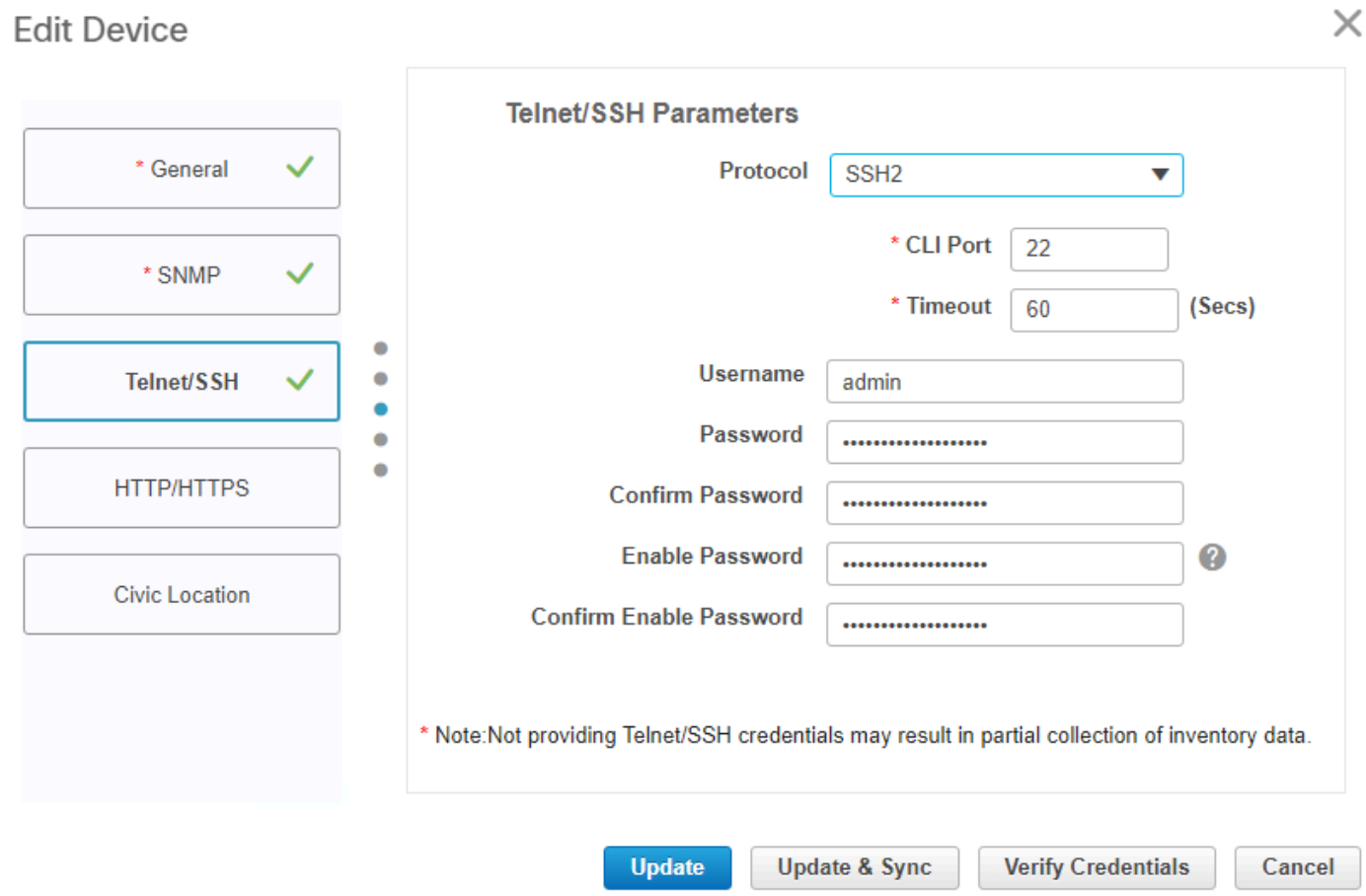
i.一般条項：



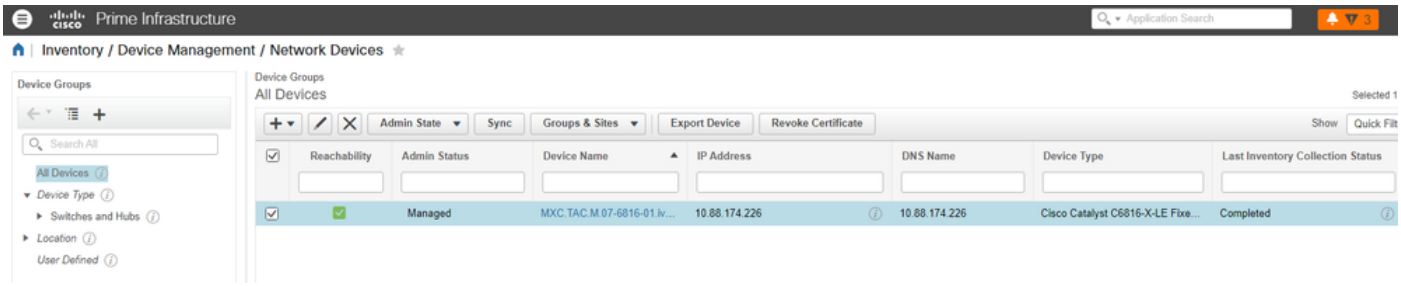

ii. SNMPセクション：



iii. Telnet/SSHセクション：




8. すべての必須フィールドに入力したら、ReachabilityおよびCollection Statusがそれぞれ GreenおよびCompletedであることを確認します。

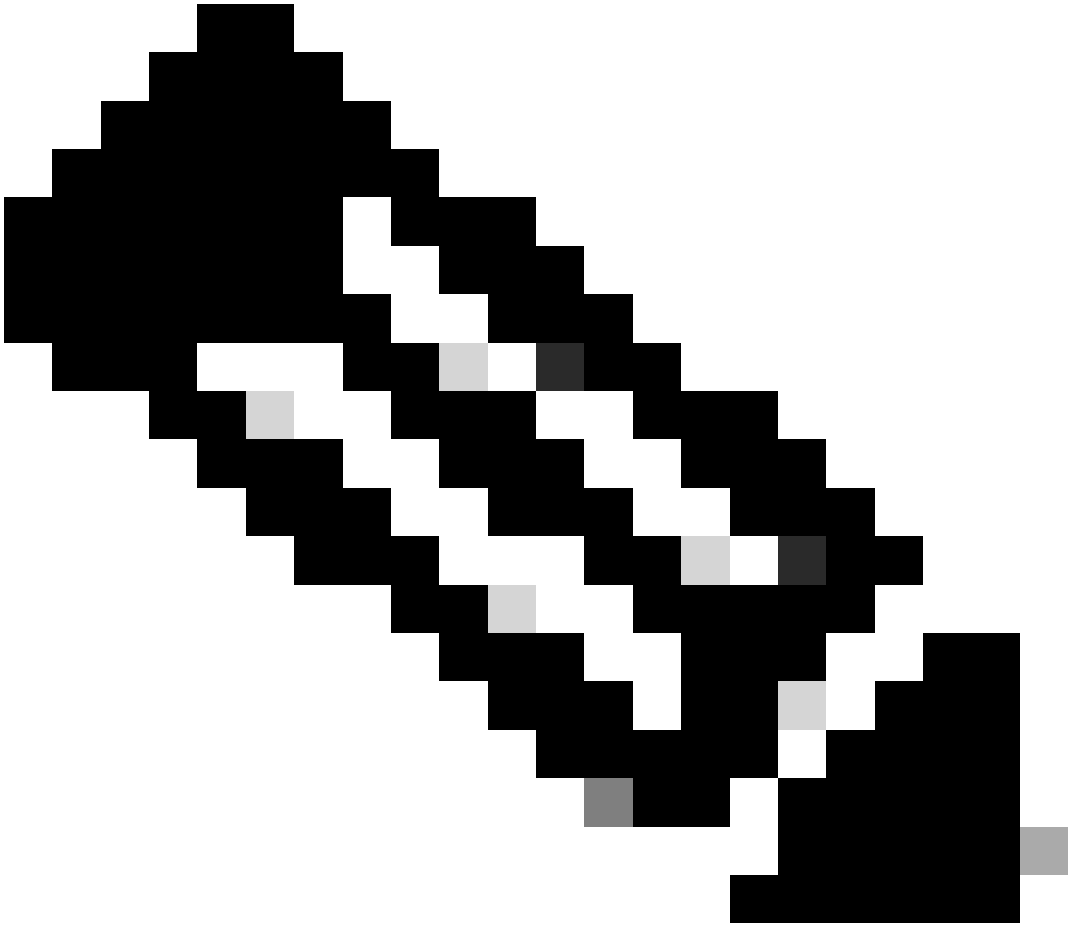



9. PrimeをISEと統合します。

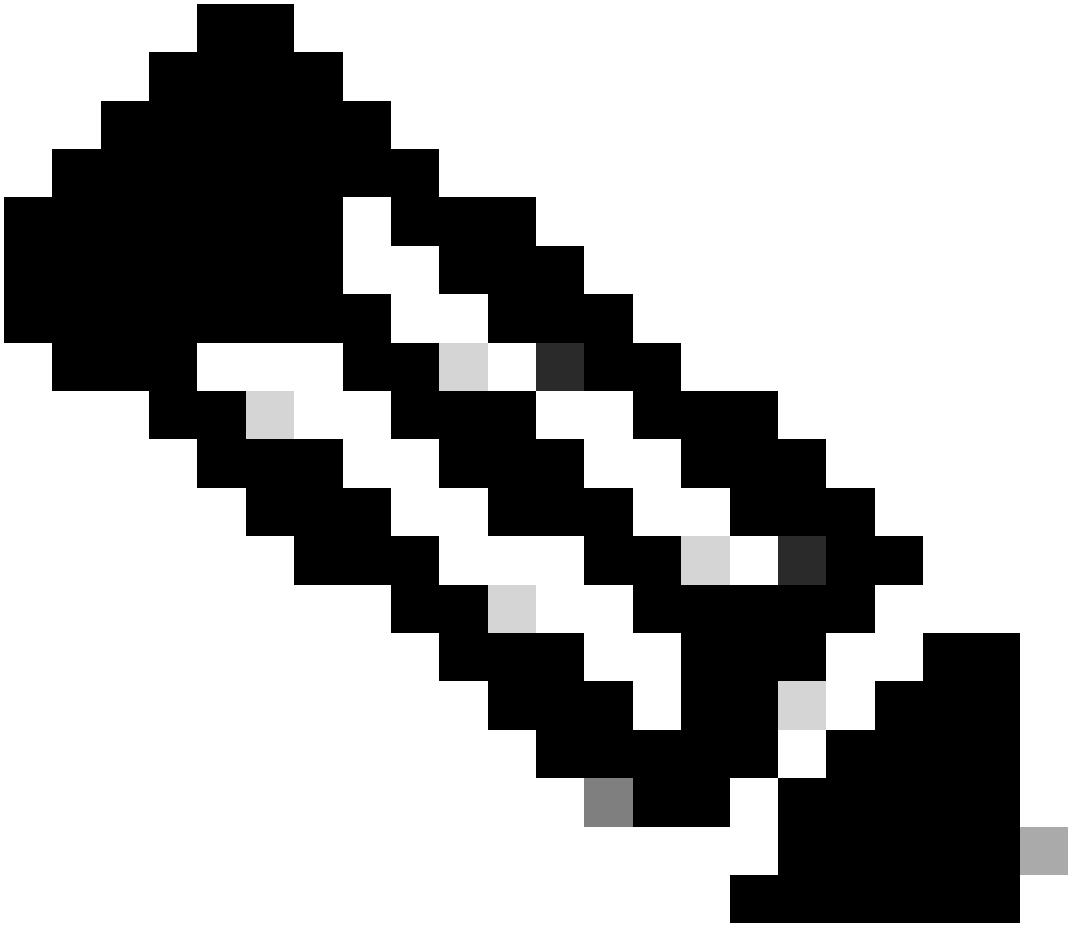
i. Administration > Servers > ISE Serversの順に移動します。

ii.ドロップダウンメニューでAdd ISE Serverを選択し、Goをクリックします。

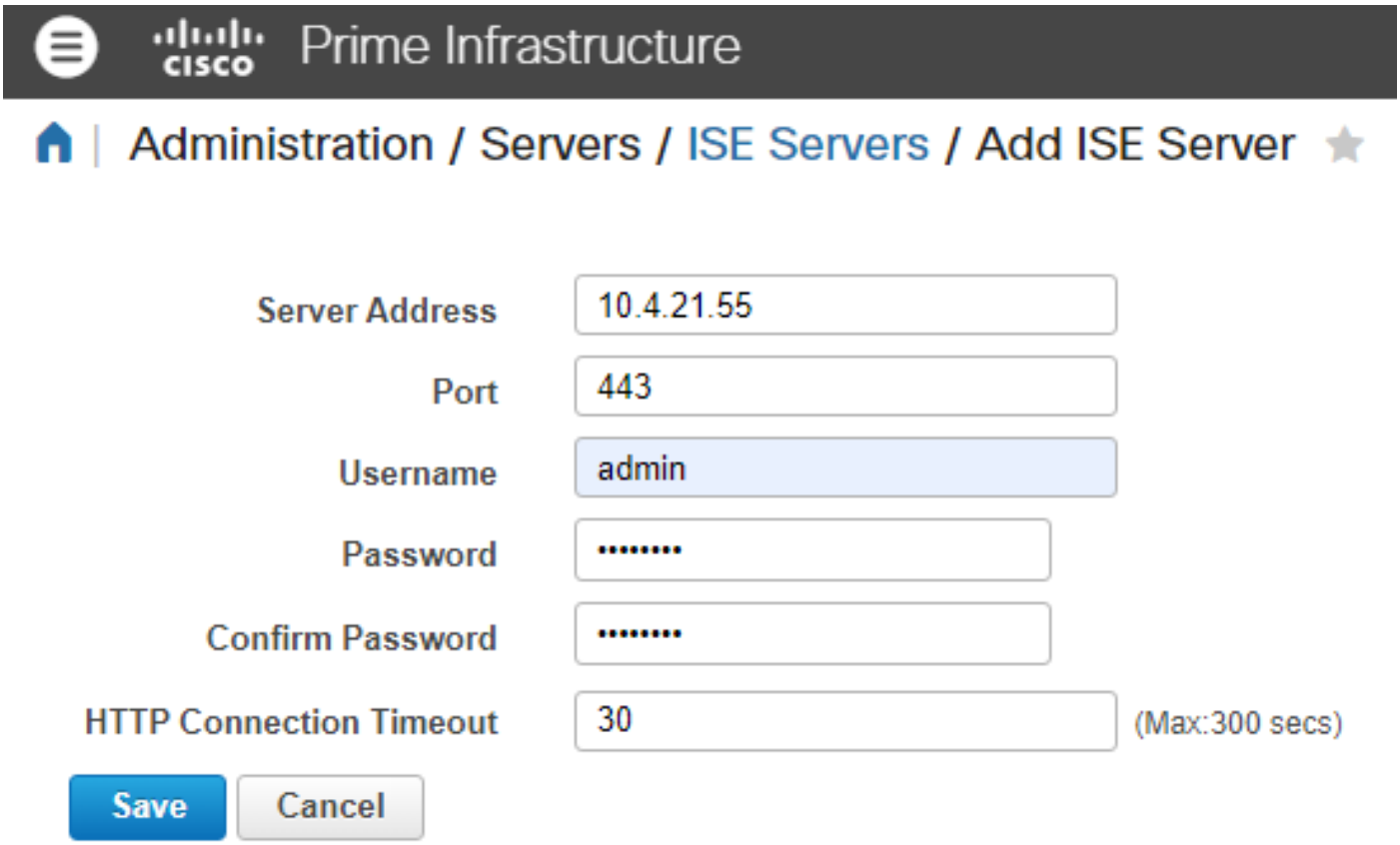

iii.すべてのフィールドに入力し、Saveをクリックします。



注：接続は、プライマリ（該当する場合）およびセカンダリ（該当する場合）モニタリングISEノードに対して確立する必要があります。



注：デフォルトポートは443に設定されていますが、ISEで開いている他のポートを使用して接続を確立できます。




iv. ISEサーバページに戻ります。サーバのステータスが到達可能と表示され、ロールが表示されます（スタンドアロン、プライマリ[MnT]、またはセカンダリ[MnT]）。


エンドポイントの設定

10. dot1x(RFC 3850)認証を実行するようにエンドポイントを設定する必要があります。これは、Cisco Network Access Manager(NAM)を設定するか、OSネイティブサプリカントを利用することで実現できます。この設定に関するガイドは多数あるため、これらの手順はこのガイドに含まれていません。

## 確認

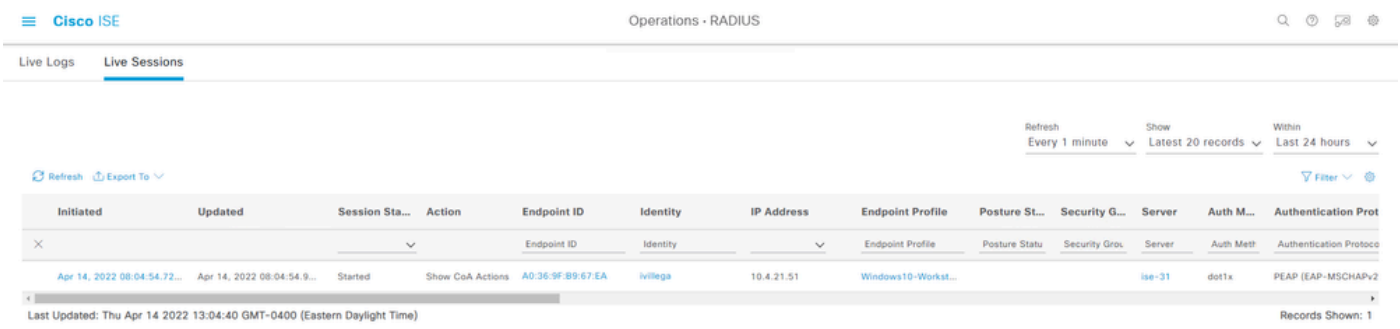
### ISEの確認

ISEはNADからRADIUS要求を受信し、ユーザを正常に認証します。

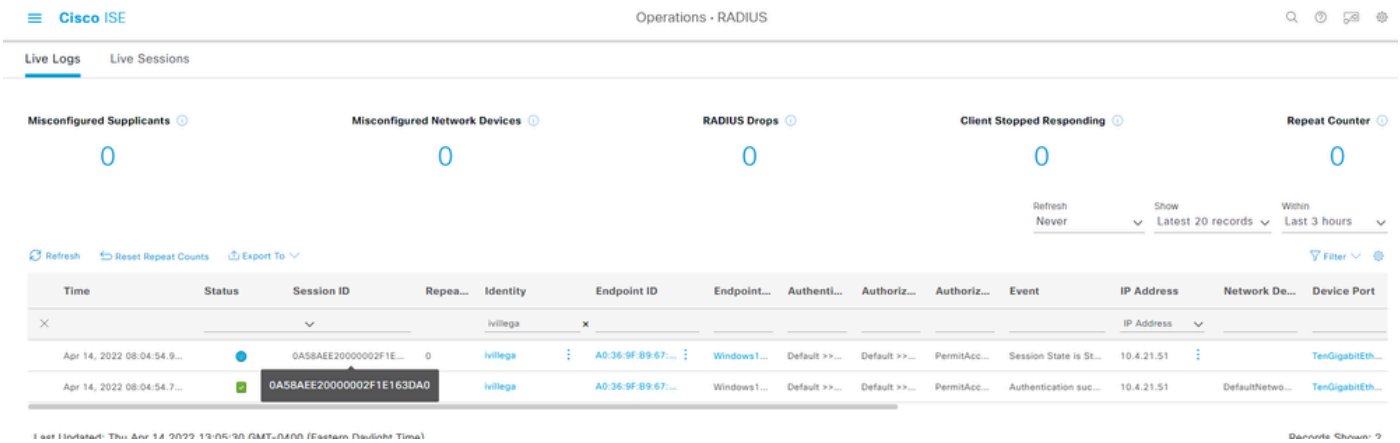
NADは、ISE > Administration > Network Resources > Network DevicesでRADIUS用に追加され、設定されます。

1. [操作] > [RADIUS] > [ライブセッション] に移動します。

このページにユーザのライブセッションが表示されていることを確認します。セッション情報はPrime Infrastructureと共有されます。




2. Operations > RADIUS > Live Logsでセッションを確認します。




## NADの確認

3. NADでセッションの詳細を確認します。セッションIDは、ISEのセッションIDと一致します。

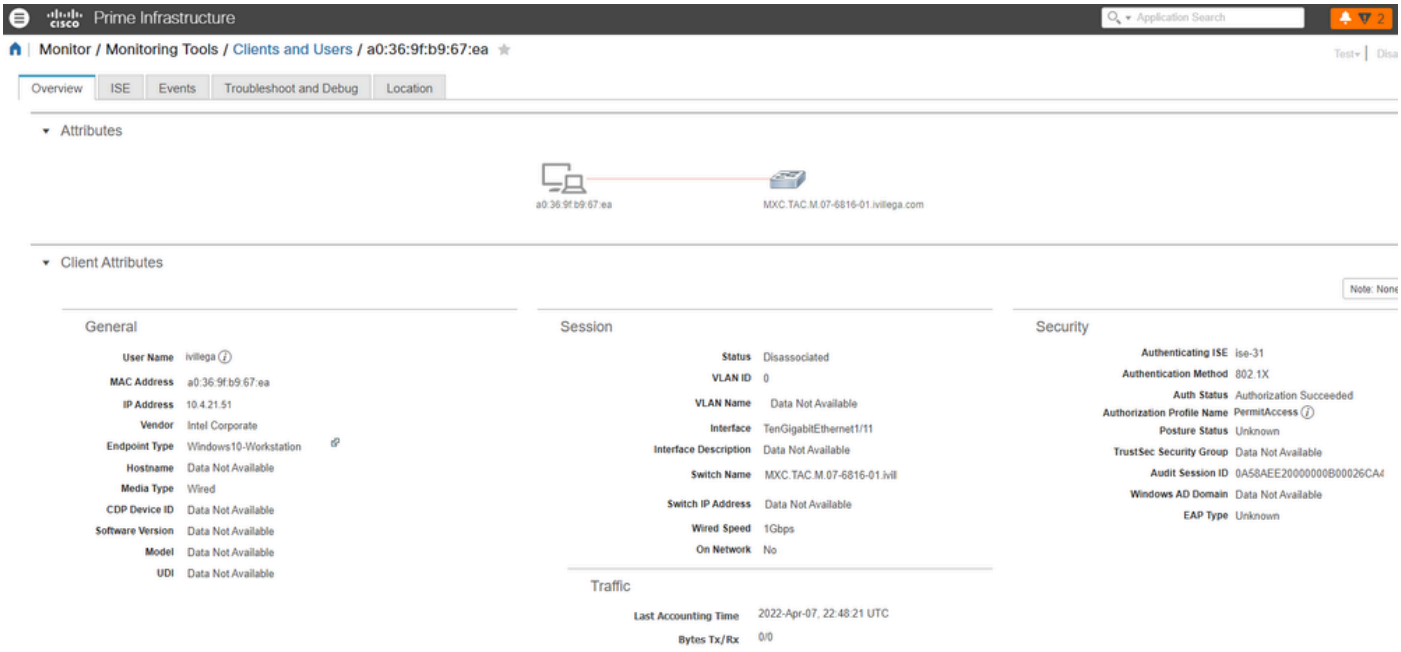
```
MXC.TAC.M.07-6816-01#show authentication session int Te1/11 detail
        Interface: TenGigabitEthernet1/11
      MAC Address: a036.9fb9.67ea
     IPv6 Address: Unknown
     IPv4 Address: 10.4.21.51
        User-Name: ivillega
           Status: Authorized
           Domain: DATA
   Oper host mode: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

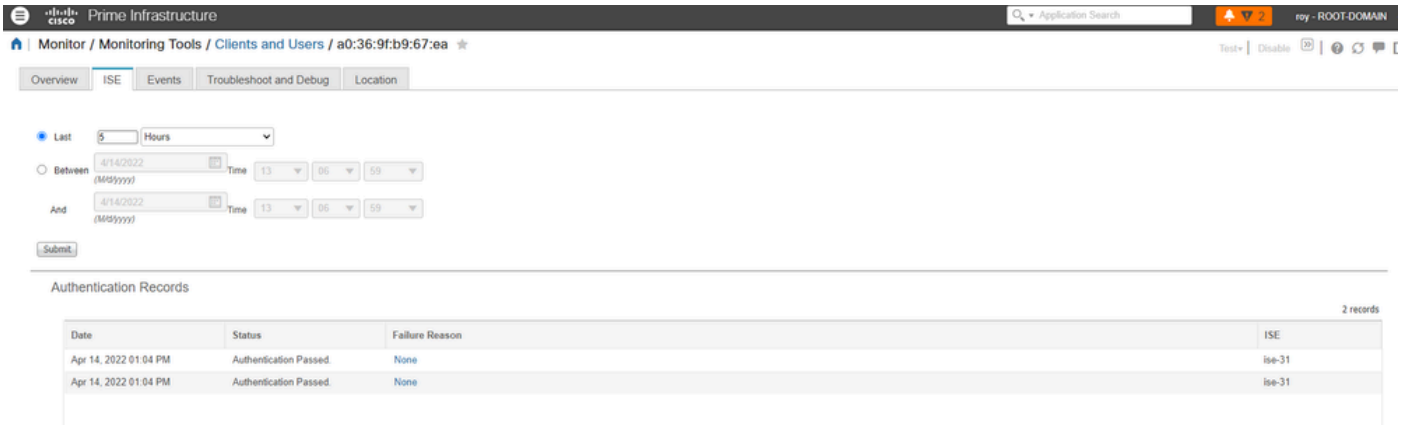
## Prime Infrastructureの確認

4. Monitor > Monitoring Tools > Clients and Usersの順に移動します。エンドポイントのMACアドレスが表示されます。


5. これをクリックすると、ユーザセッションの詳細とISEサーバの情報が表示されます。




6. この特定のエンドポイントのセッションイベントを取得するために、「ISE」というラベルの付いたタブもあります。Prime InfrastructureがISEからイベントを取得するために使用するタイムフレームを選択できます。



# トラブルシュート

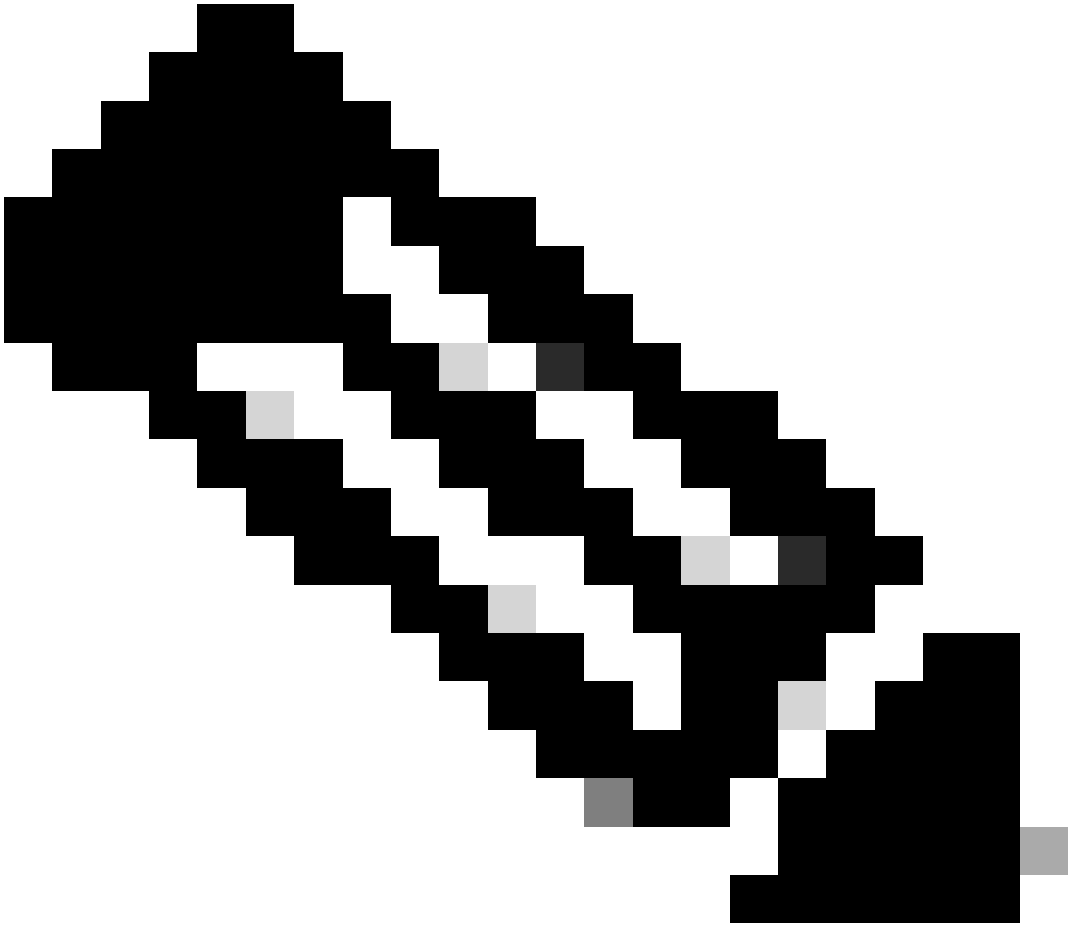
1. ISEとPrime Infrastructureの間の接続をpingを使用してテストします。接続がない場合は、ISEまたはPIからのトレースルートを使用して問題を特定できます。

2. ステップ9で設定したポートがISE MnTノード（デフォルトポートは443）で開いていることを確認します。

```
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
```

ポートが出力にリストされている場合、ISE MnTでポートが開いていることを意味します。

出力がない場合、またはポートがリストされていない場合は、ISE MnTでそのポートが閉じられていることを意味します。このような場合は、別のポートで試すか、ISEチームでTACケースをオープンして、ポートがオープンされない理由を確認できます。



注:ISE MnTノードは一部のポートのみを使用します。ISEインストールガイドの「ポート参照」セクションに記載されていないポートをISE MnTノードで開く方法はありません。

3. ステップ9で設定したポートを、Prime infrastructureからのTelnetでテストします。

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

telnetテストの出力が「Connected to <ISE MnT IP/FQDN>」の場合、テストが成功したことを意味します。

telnetテストの出力が「Trying <ISE MnT IP/FQDN>」でスタックしている場合は、テストが失敗したことを意味します。これは、中間ネットワークデバイス内のACLまたはファイアウォールルールに関連している可能性があります。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。