Integrazione di ISE con Prime Infrastructure per la visibilità degli endpoint

Sommario

Introduzione

Questo documento descrive come integrare ISE con Prime Infrastructure per ottenere visibilità sugli endpoint autenticati.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco ISE
- Cisco Prime Infrastructure.
- Flusso AAA wireless o cablato per gli endpoint che eseguono l'autenticazione con ISE.
- Configurazione SNMP su dispositivi di accesso alla rete (NAD) come switch e WLC.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

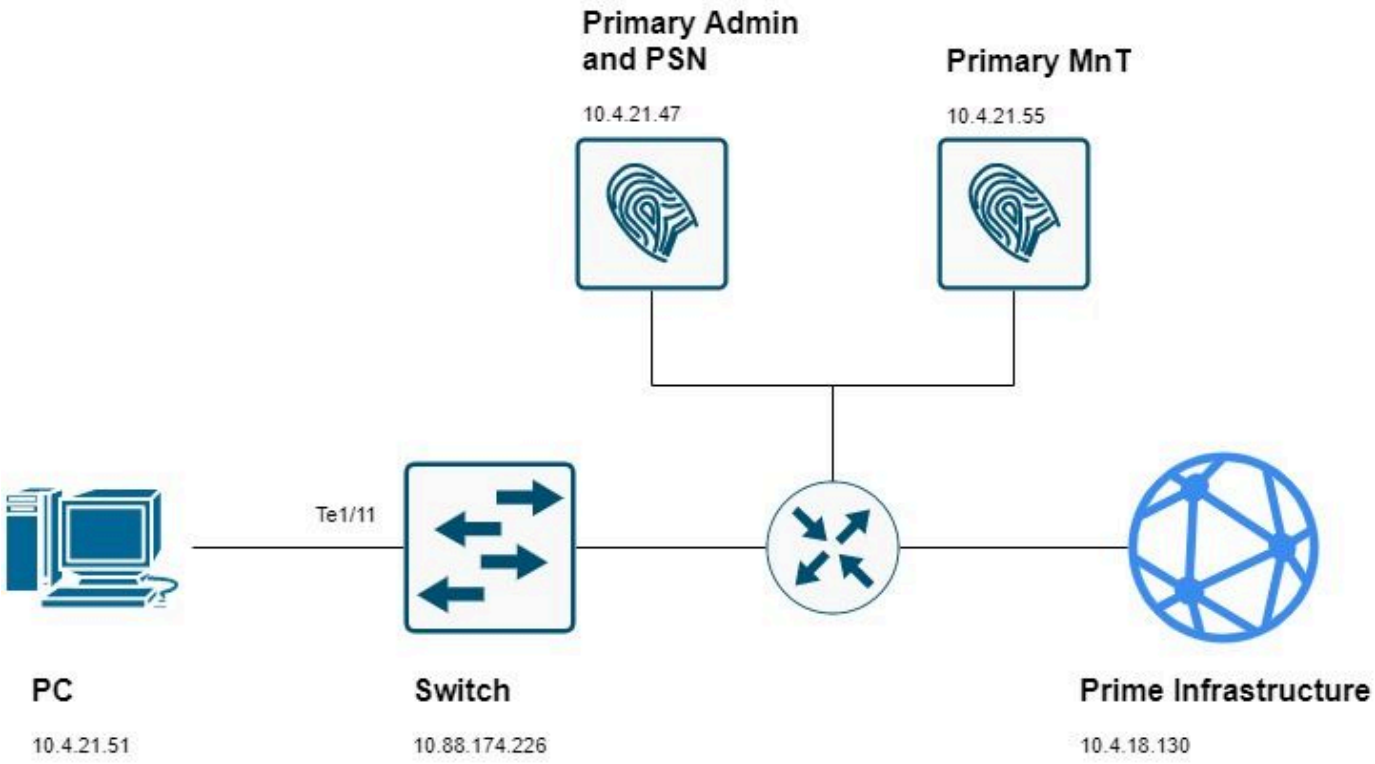
- Implementazione di ISE 3.1.

- Cisco Prime Infrastructure 3.8.1
- C6816-X-LE con Cisco IOS® 15.5.
- Computer Windows 10.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Configurazioni

Configurazione degli switch

1. Configurare il Network Access Device (NAD) per l'autenticazione AAA con ISE. In questa guida viene utilizzata la configurazione seguente:

```
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. Configurare Device Tracking nello switch:

```
device-tracking policy DT1
 tracking enable

device-tracking tracking auto-source
```

3. Configurare il portaswitch per l'autenticazione dot1x e allegarvi i criteri di rilevamento dei dispositivi:

```
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. Configurare la community SNMP RO e le trap SNMP per soddisfare i requisiti della rete (facoltativamente, è possibile configurare la community RW):

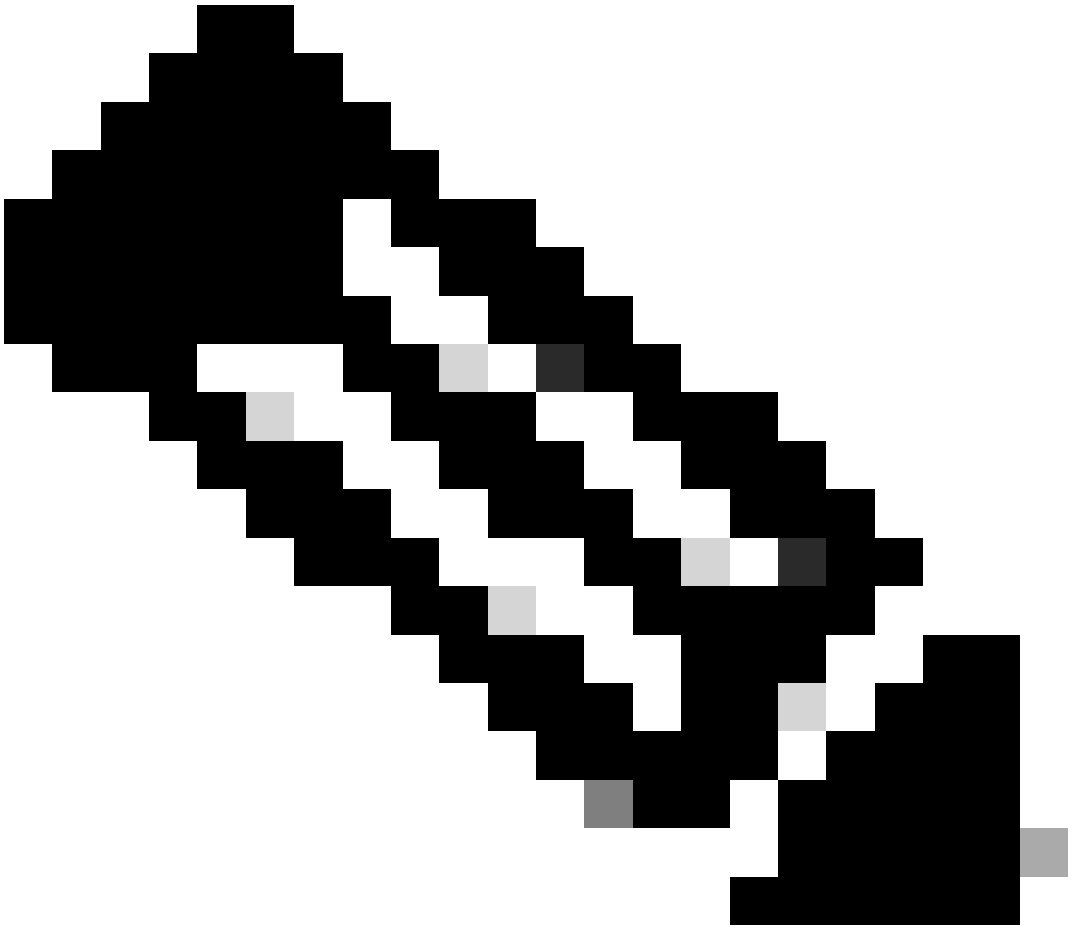
```
snmp-server community public RO
snmp-server community private RW
snmp-server trap-source TenGigabitEthernet1/16
snmp-server source-interface informs TenGigabitEthernet1/16
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps aaa_server
snmp-server 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. Configurare un accesso Telnet o SSH in modo che Prime possa gestire il dispositivo:

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

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

6. (Facoltativo) Per le connessioni SSH, è richiesta una chiave RSA. Se NAD non ne possiede una, eseguire la procedura seguente per generarla.

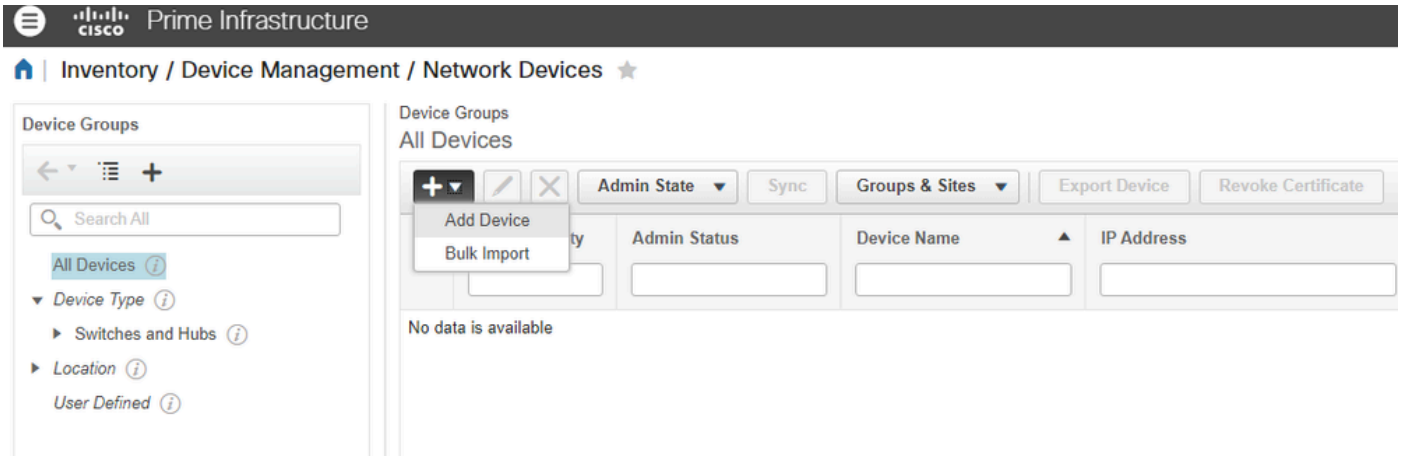


Nota: alcuni dispositivi richiedono un dominio configurato prima di generare RSA. Verificare che il dispositivo disponga di un dominio configurato in modo da non sovrascrivere quello esistente.

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

Configurazione di Cisco Prime Infrastructure

7. Aggiungere il dispositivo di rete in Inventario > Gestione dispositivi > Dispositivi di rete > Segno più (+) > Aggiungi dispositivo:



I campi obbligatori per completare l'inventario sono:

Per i dispositivi cablati:

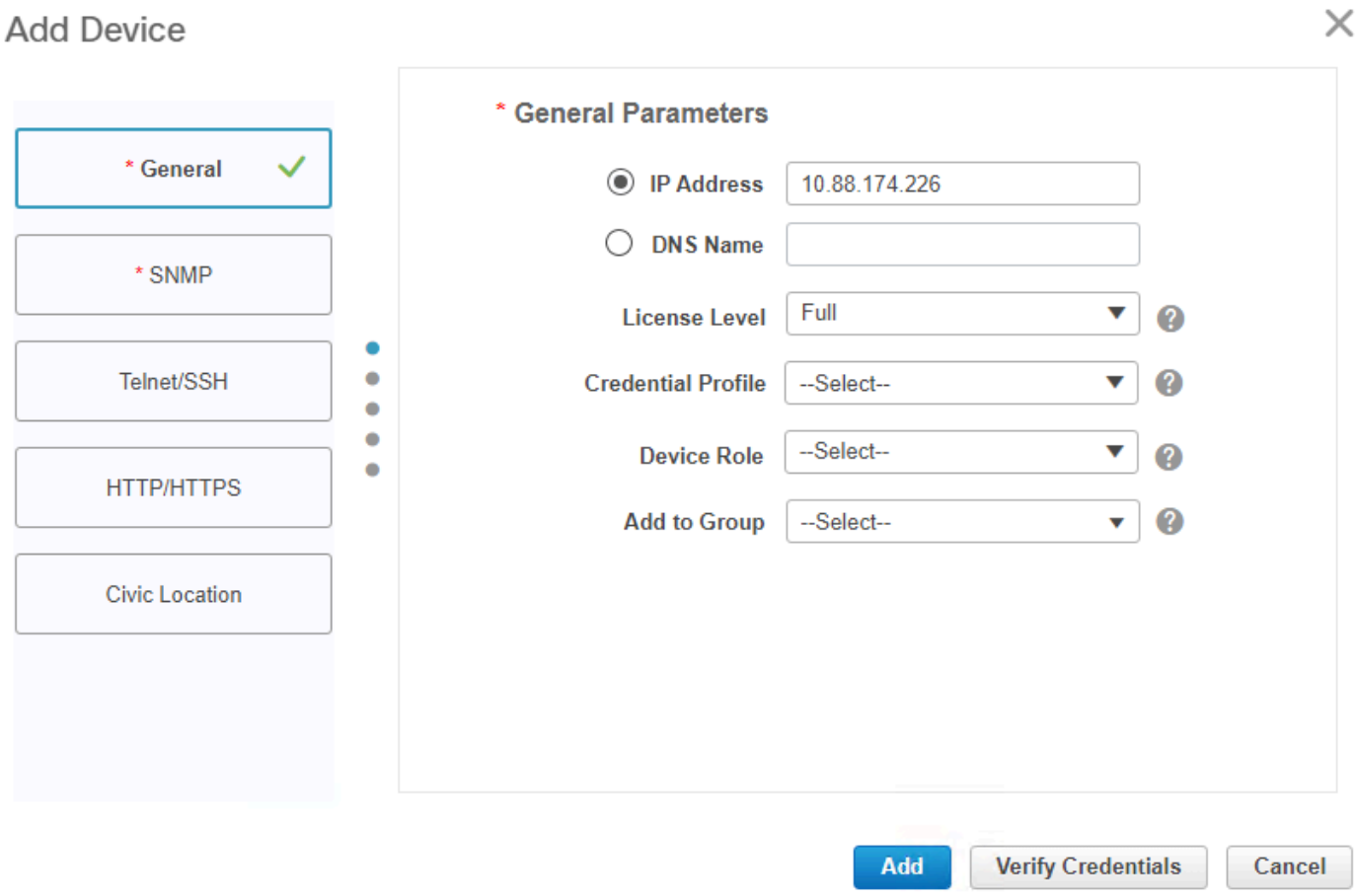
- Informazioni generali: IP o DNS.
- SNMP: È richiesta la community RO: accertarsi di configurarla anche nello switch/WLC.
- Telnet/SSH: Credenziali della modalità di esecuzione e della modalità di abilitazione.

Per WLC:

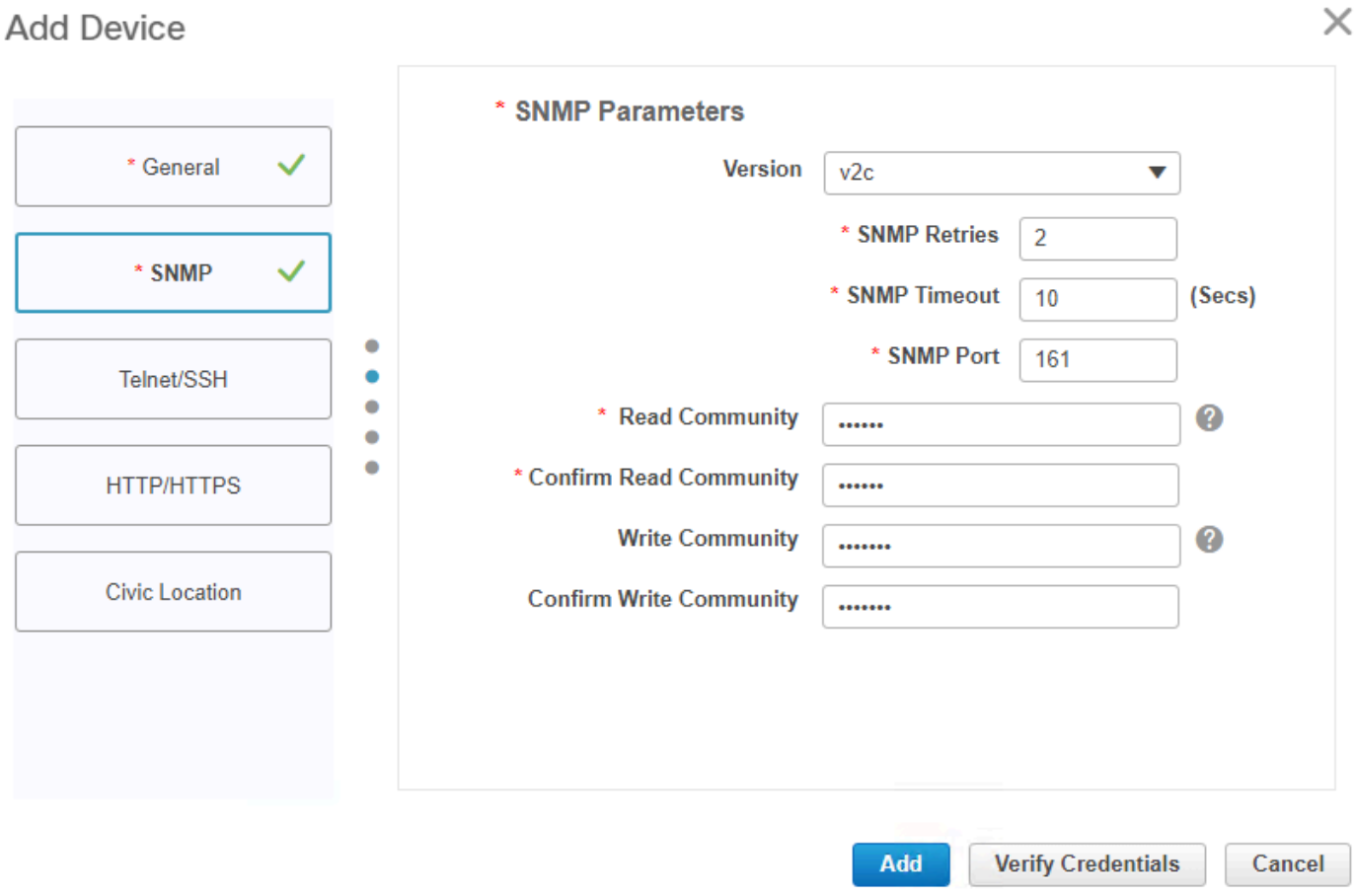
- Informazioni generali: IP o DNS.
- SNMP: È richiesta la community RO: accertarsi di configurarla anche nello switch/WLC.

In questa guida viene illustrato l'utilizzo di uno switch Cisco:

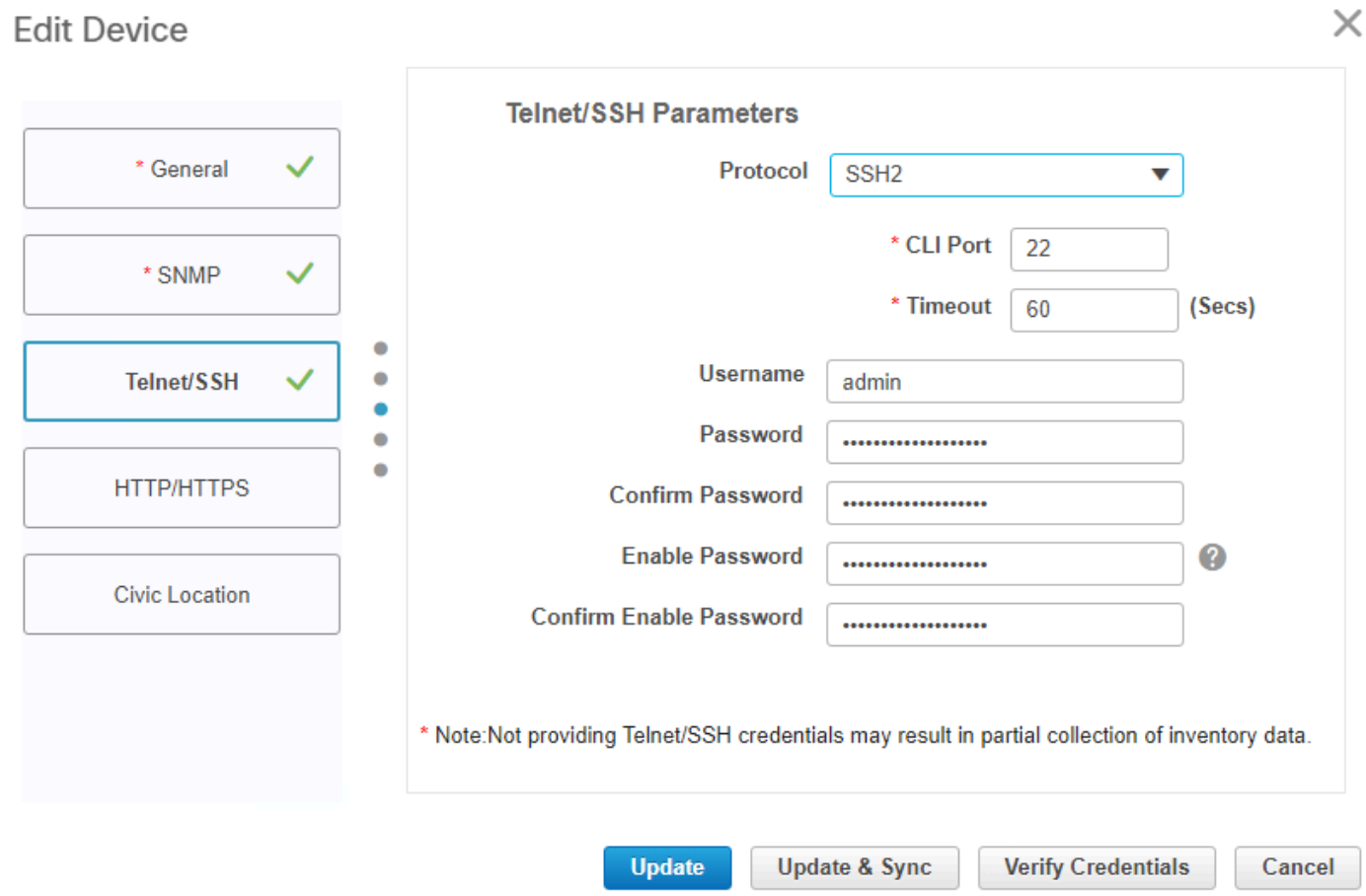
i. Sezione generale:



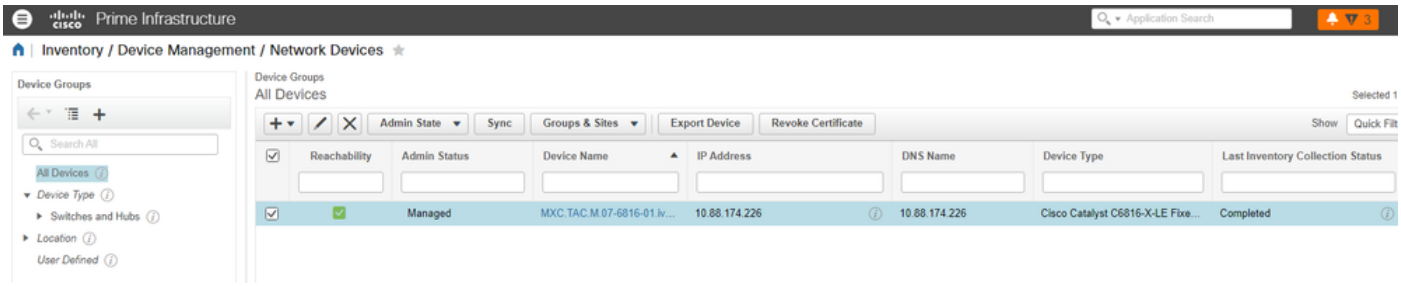
ii. Sezione SNMP:



iii. Sezione Telnet/SSH:



8. Una volta completati tutti i campi obbligatori, assicurarsi che Raggiungibilità e Stato raccolta siano rispettivamente verdi e completati:

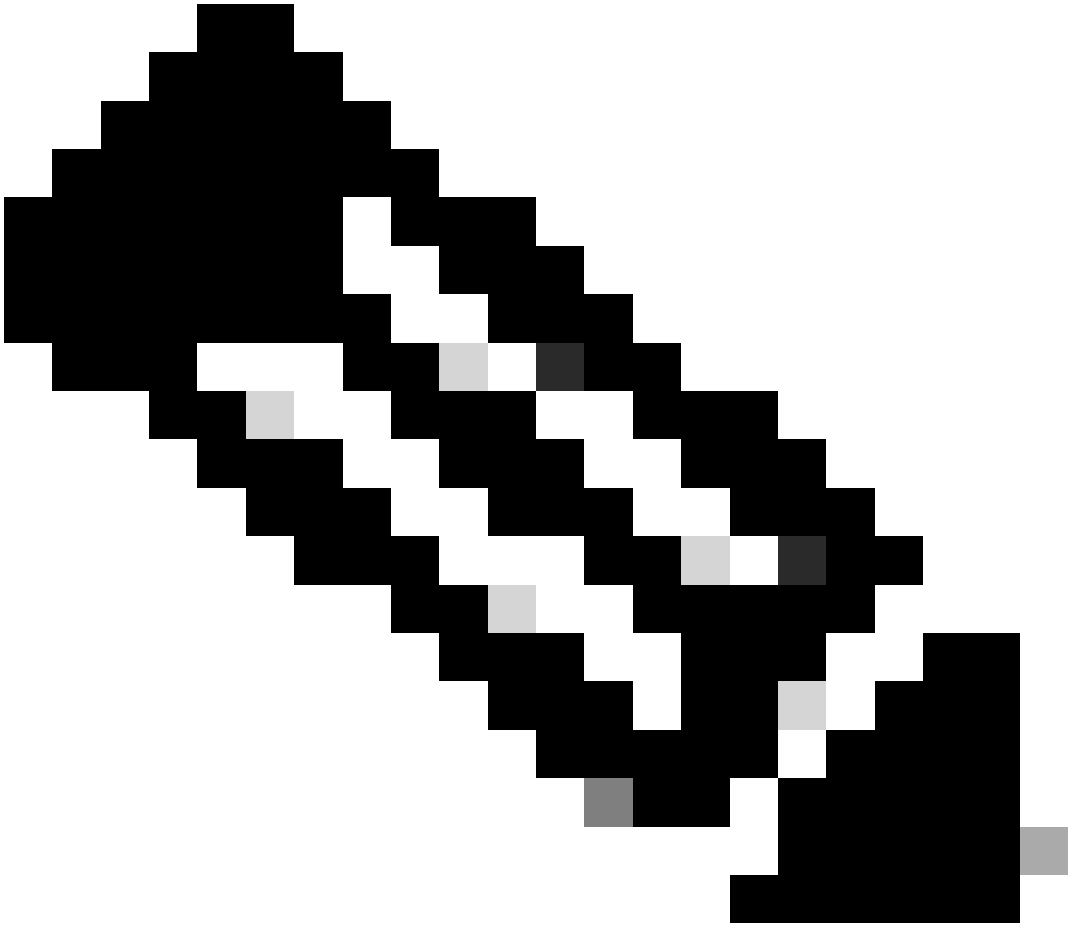


9. Integrare Prime con ISE.

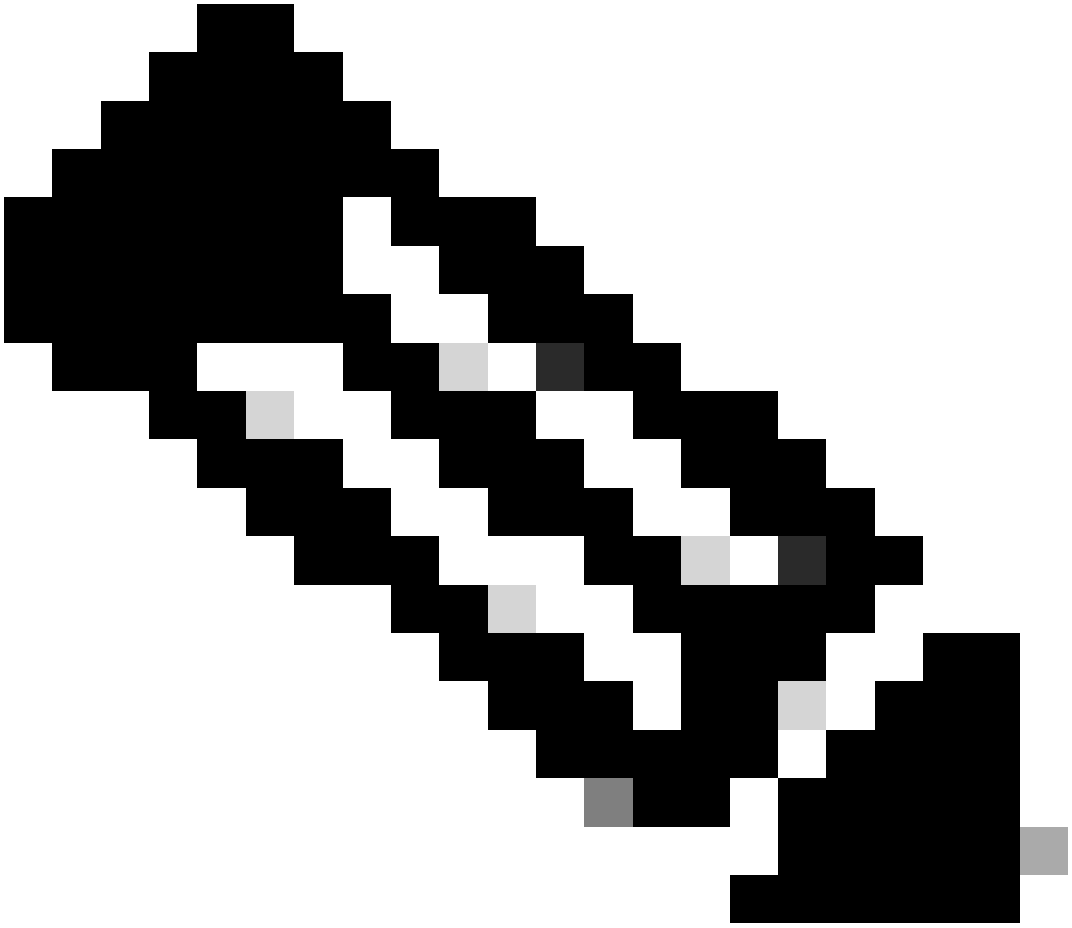
i. Selezionare Amministrazione > Server > ISE Server.

ii. Nel menu a discesa, selezionare Add ISE Server, quindi fare clic su Go:

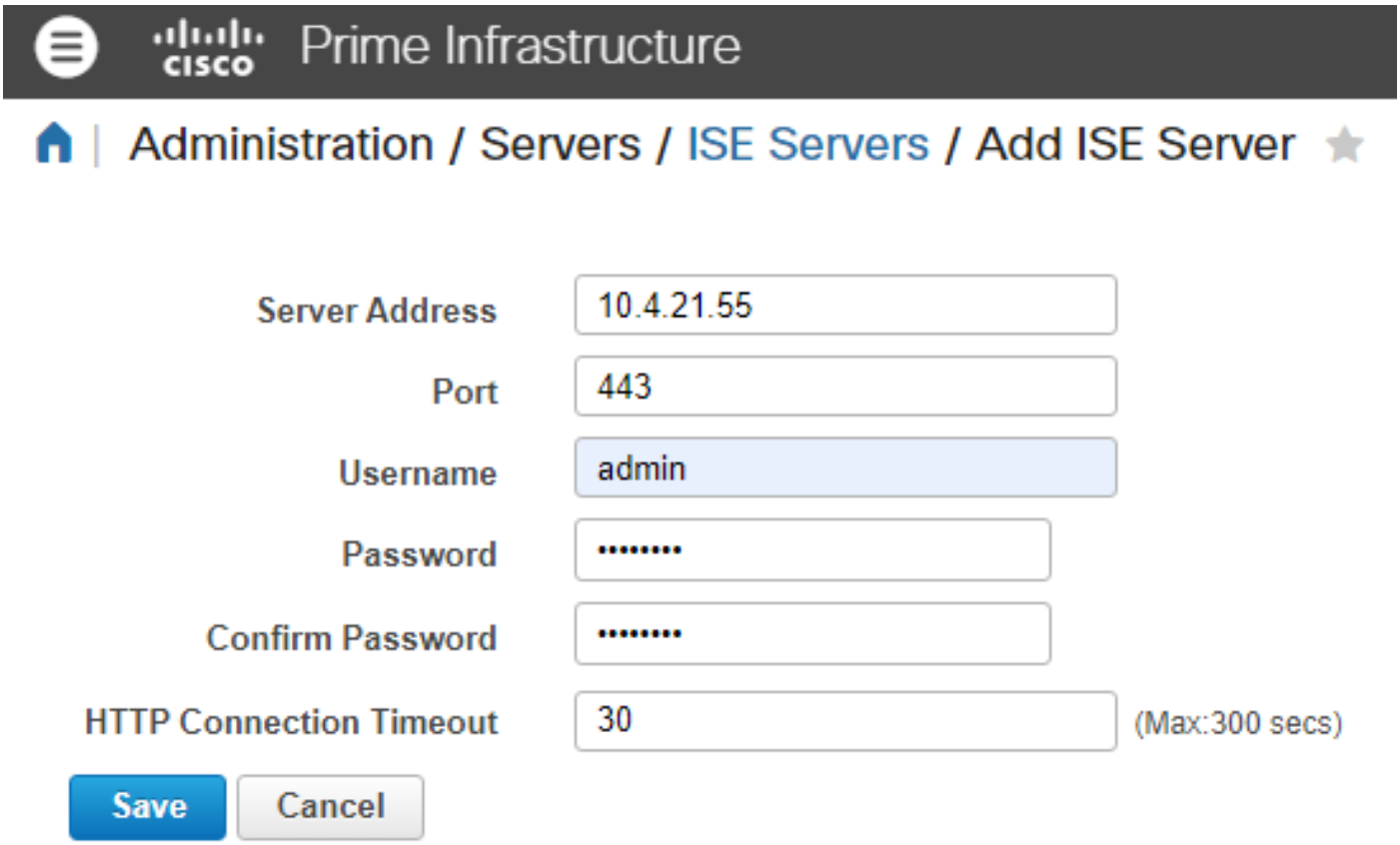
iii. Compilare tutti i campi e fare clic su Salva.



Nota: La connessione deve essere stabilita sui nodi primario e secondario (se applicabile) di monitoraggio ISE.



Nota: La porta predefinita è impostata su 443, ma è possibile utilizzare qualsiasi altra porta aperta in ISE per stabilire la connessione.



iv. Tornare alla pagina ISE Server. Lo stato del server è Raggiungibile e viene visualizzato il ruolo (Standalone, Primario [MnT] o Secondario [MnT]):

Configurazione degli endpoint

10. L'endpoint deve essere configurato per eseguire l'autenticazione dot1x (RFC 3850). A tale scopo, è possibile configurare Cisco Network Access Manager (NAM) o utilizzare il sistema operativo Native Supplicant. Sono disponibili numerose guide relative a questa configurazione, pertanto i passaggi descritti non verranno inclusi in questa guida.

Verifica

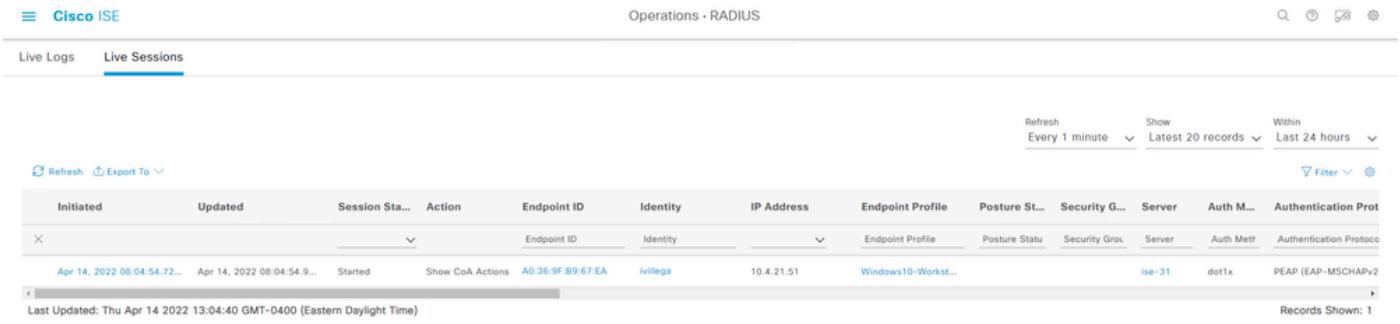
Verifica ISE

ISE riceve la richiesta RADIUS da NAD e autentica correttamente l'utente.

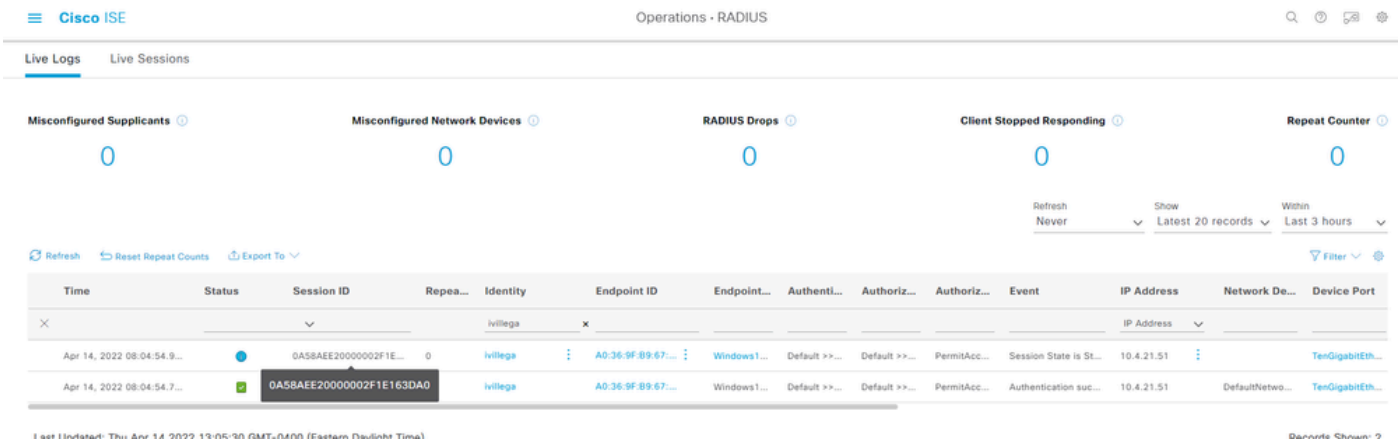
Il NAD viene aggiunto e configurato per RADIUS in ISE > Amministrazione > Risorse di rete > Dispositivi di rete.

1. Passare a Operazioni > RAGGIO > Sessioni attive.

Accertarsi che la sessione utente live sia elencata in questa pagina. Le informazioni sulla sessione vengono condivise con Prime Infrastructure.



2. Controllare l'ID sessione in Operazioni > RADIUS > Live Log:



Verificare il NAD

3. Controllare i dettagli della sessione nel NAD. L'ID sessione corrisponde all'ID sessione in ISE:

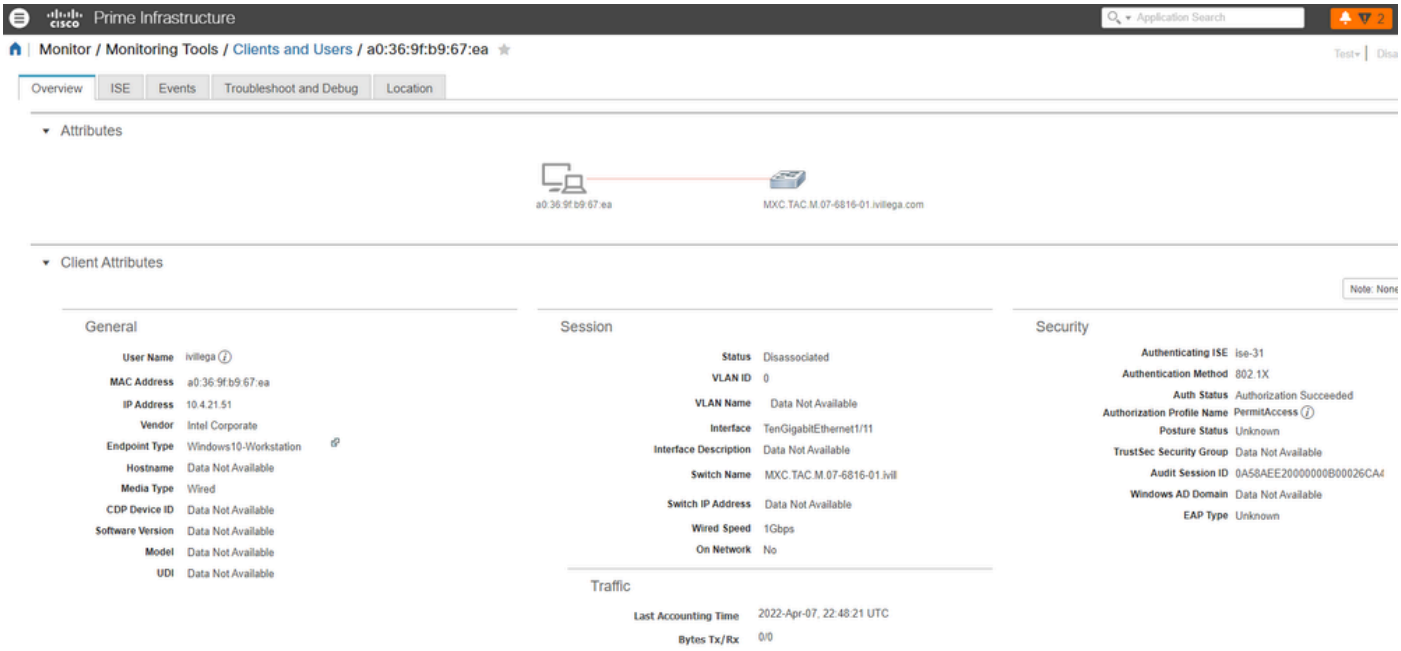
```
MXC.TAC.M.07-6816-01#show authentication session int Te1/11 detail
        Interface: TenGigabitEthernet1/11
      MAC Address: a036.9fb9.67ea
     IPv6 Address: Unknown
     IPv4 Address: 10.4.21.51
        User-Name: ivillega
           Status: Authorized
           Domain: DATA
   Oper host mode: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

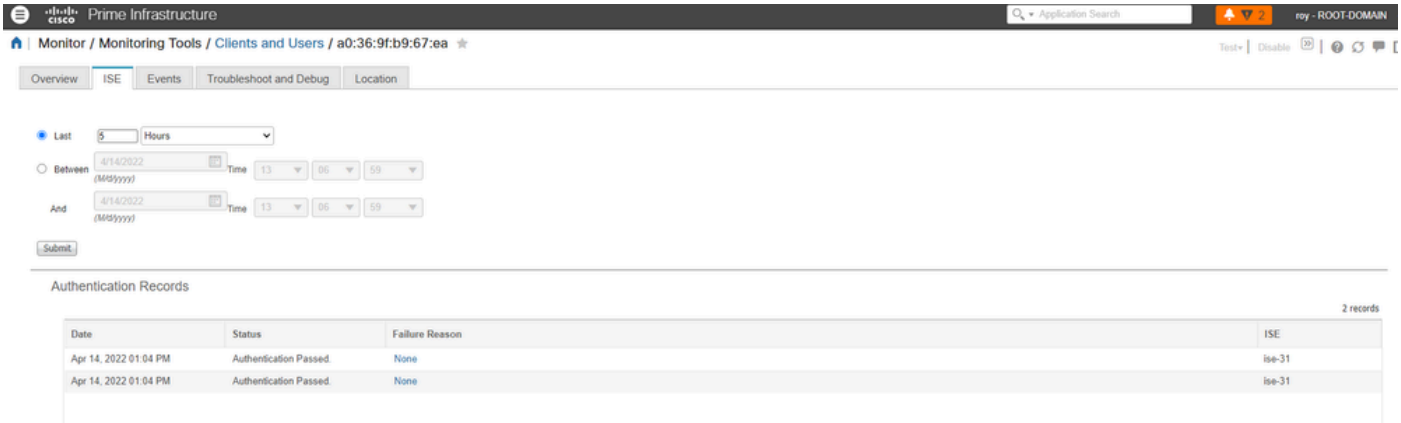
Verifica di Prime Infrastructure

4. Passare a Controlla > Strumenti di controllo > Acquirenti e utenti. Viene visualizzato l'indirizzo MAC dell'endpoint:

5. Facendo clic su di esso, vengono visualizzati i dettagli della sessione utente e le informazioni sul server ISE:



6. È disponibile anche una scheda etichettata come ISE per recuperare gli eventi della sessione per questo particolare endpoint. È possibile selezionare un intervallo di tempo che Prime Infrastructure utilizza per recuperare gli eventi da ISE:



Risoluzione dei problemi

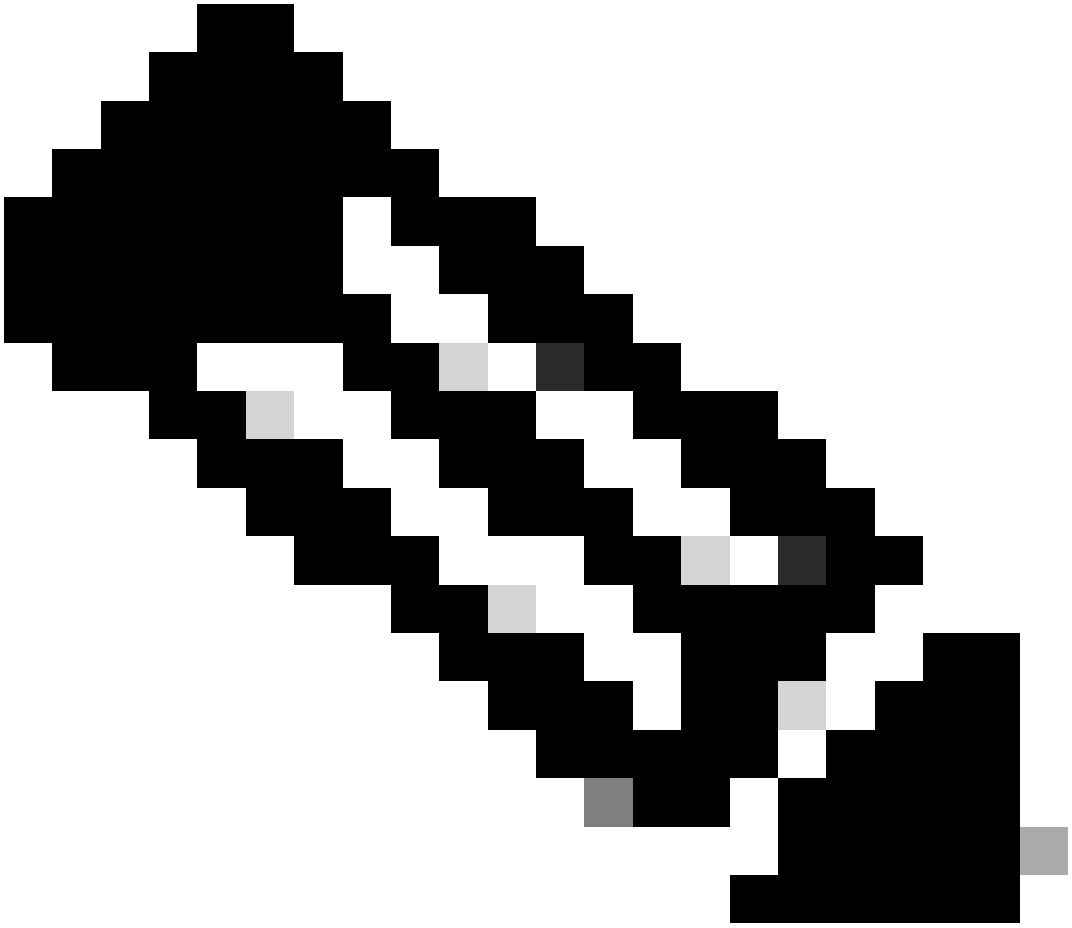
1. Test della connettività tra ISE e Prime Infrastructure con ping. In assenza di connettività, è possibile utilizzare le route di traccia da ISE o IP per individuare il problema.

2. Verificare che la porta configurata nel passaggio 9 sia aperta nel nodo ISE NT (la porta predefinita è 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
```

Se la porta è elencata nell'output, significa che la porta è aperta in ISE MnT.

Se non c'è output o la porta non è presente nell'elenco, significa che per ISE NT la porta è chiusa. In questo caso, è possibile provare con un'altra porta o aprire una richiesta TAC con il team ISE per verificare il motivo per cui la porta non è aperta.



Nota: Il nodo ISE MnT utilizza solo alcune porte; non è possibile aprire le porte nel nodo ISE MnT non elencate nella guida all'installazione di ISE, sezione Port reference.

---

3. Verificare la porta configurata nella fase 9 con Telnet da Prime Infrastructure:

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

Se l'output del test telnet è Connesso a <ISE MnT IP/FQDN>, significa che il test è stato eseguito correttamente.

Se l'output del test telnet è bloccato su Trying <ISE MnT IP/FQDN>, significa che il test non è riuscito. Ciò può essere correlato agli ACL nei dispositivi di rete intermedi o alle regole del firewall.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).