Integre o ISE com a infraestrutura Prime para visibilidade de endpoints

Contents

Introdução

Este documento descreve como integrar o ISE com a Prime Infrastructure para obter visibilidade para endpoints autenticados.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco ISE
- Infraestrutura Cisco Prime
- Fluxo AAA sem fio ou com fio para endpoints que se autenticam no ISE.
- Configuração de SNMP em NADs (dispositivos de acesso à rede) como Switches e WLCs.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

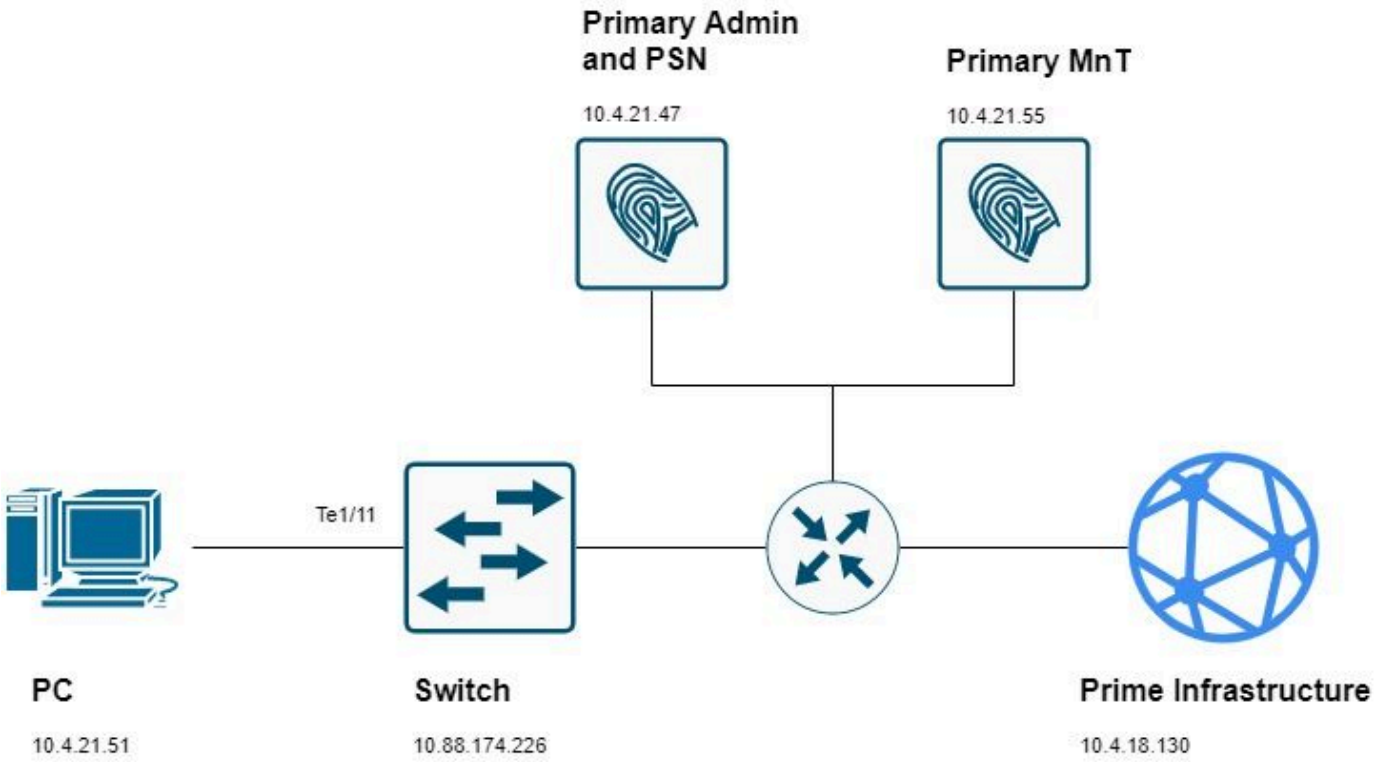
- Implantação do ISE 3.1.
- Infraestrutura 3.8 do Cisco Prime.

- C6816-X-LE executando o Cisco IOS® 15.5.
- Windows 10 Machine (Máquina Windows 10).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede



Configurações

Configuração do Switch

1. Configure o Network Access Device (NAD) para autenticação AAA em relação ao ISE. Neste guia, você está usando esta configuração:

```
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. Configure o Rastreamento de Dispositivo no switch:

```
device-tracking policy DT1
 tracking enable

device-tracking tracking auto-source
```

3. Configure a switchport para a autenticação dot1x e anexe a política de rastreamento de dispositivo a ela:

```
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. Configure a comunidade de SNMP de RO e interceptações SNMP para atender aos seus requisitos de rede (Opcionalmente, você pode configurar a comunidade RW):

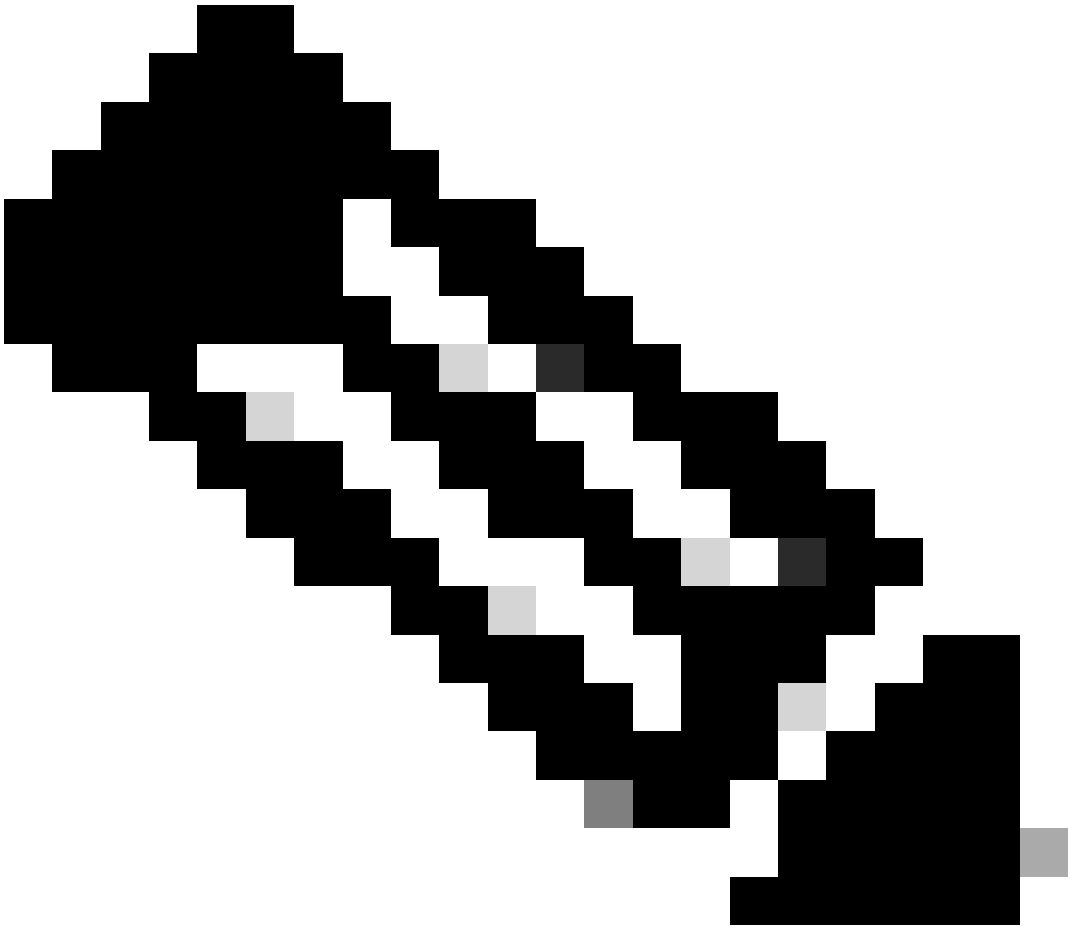
```
snmp-server community public RO
snmp-server community private RW
snmp-server trap-source TenGigabitEthernet1/16
snmp-server source-interface informs TenGigabitEthernet1/16
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps aaa_server
snmp-server 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. Configure um acesso Telnet ou SSH para que o Prime possa gerenciar o dispositivo:

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

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

6. (Opcional) Para conexões SSH, é necessária uma chave RSA. Se o NAD não tiver um, use estas etapas para gerá-lo.

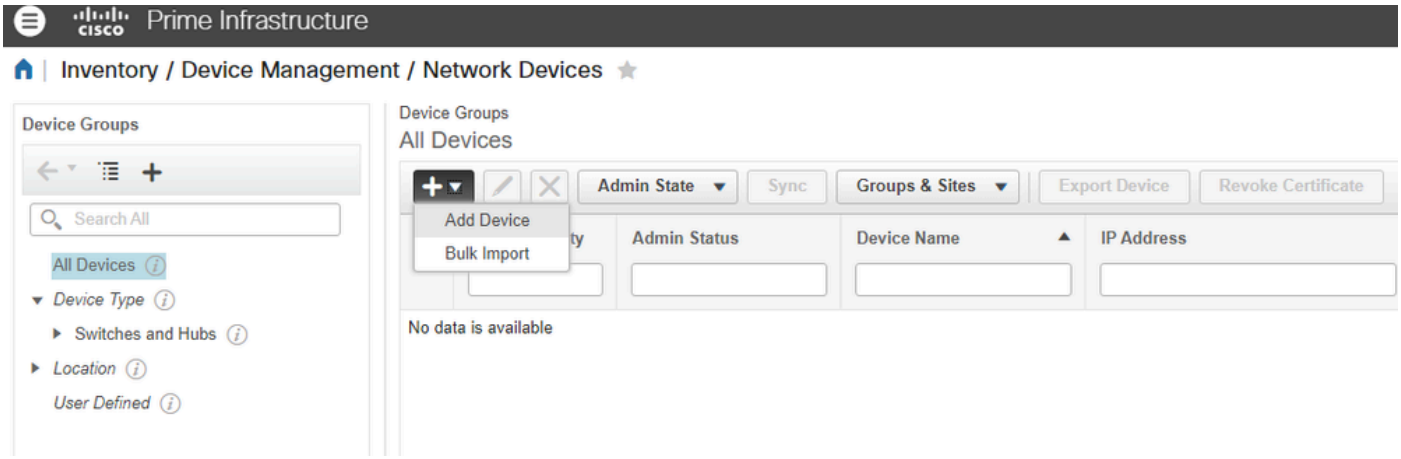


Note: Alguns dispositivos exigem um domínio configurado antes de gerar o RSA. Verifique se o seu dispositivo tem um domínio configurado para que você não substitua o existente.

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

Configuração da infraestrutura Cisco Prime

7. Adicione o Dispositivo de Rede em Inventário > Gerenciamento de Dispositivos > Dispositivos de Rede > Sinal de Adição (+) > Adicionar Dispositivo:



Os campos obrigatórios para concluir o estoque são:

Para dispositivos com fio:

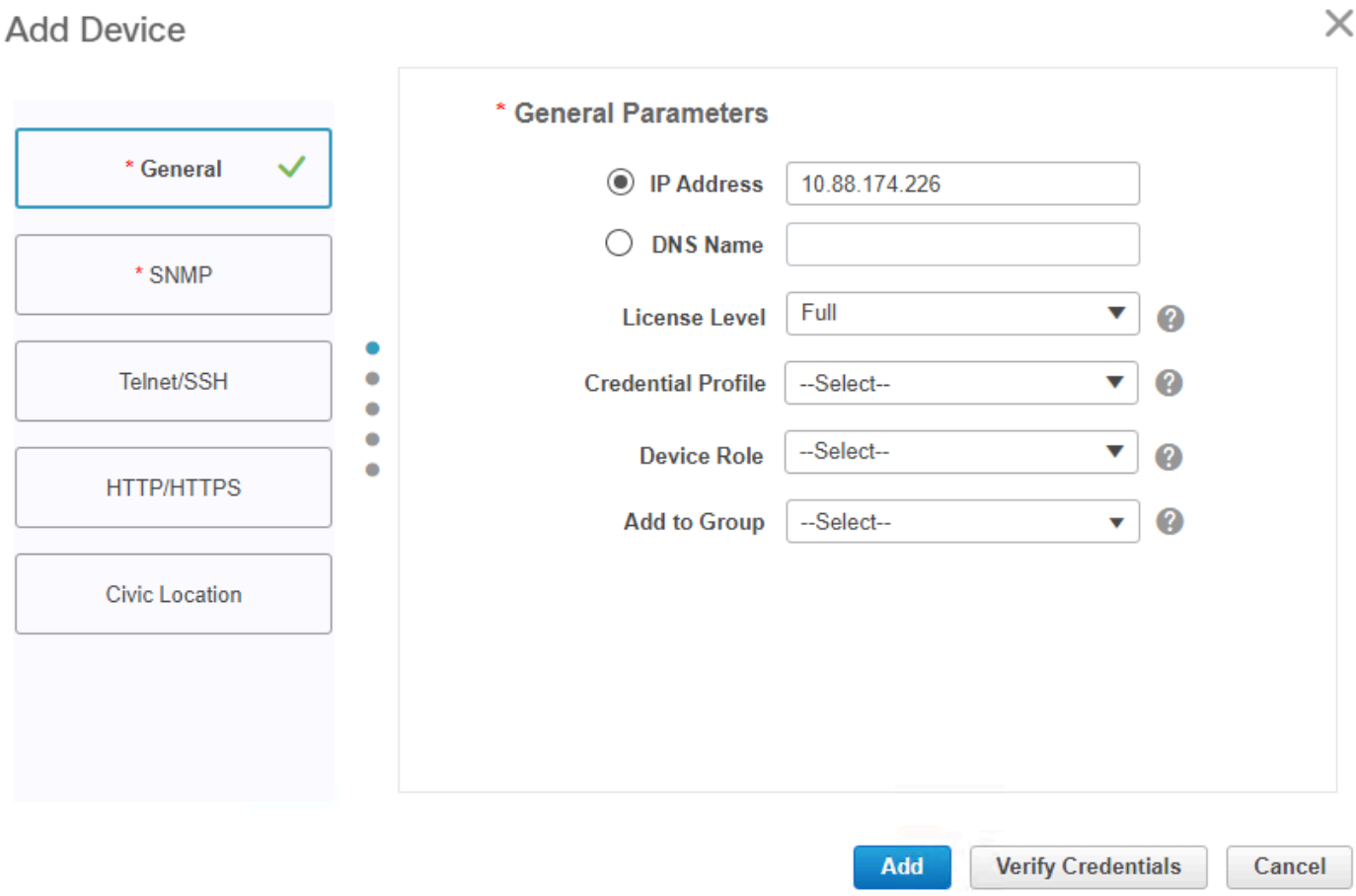
- General: IP ou DNS.
- SNMP: A comunidade RO é necessária - certifique-se de configurá-la também no Switch/WLC.
- Telnet/SSH: Modo Exec e credenciais do modo enable.

Para WLC:

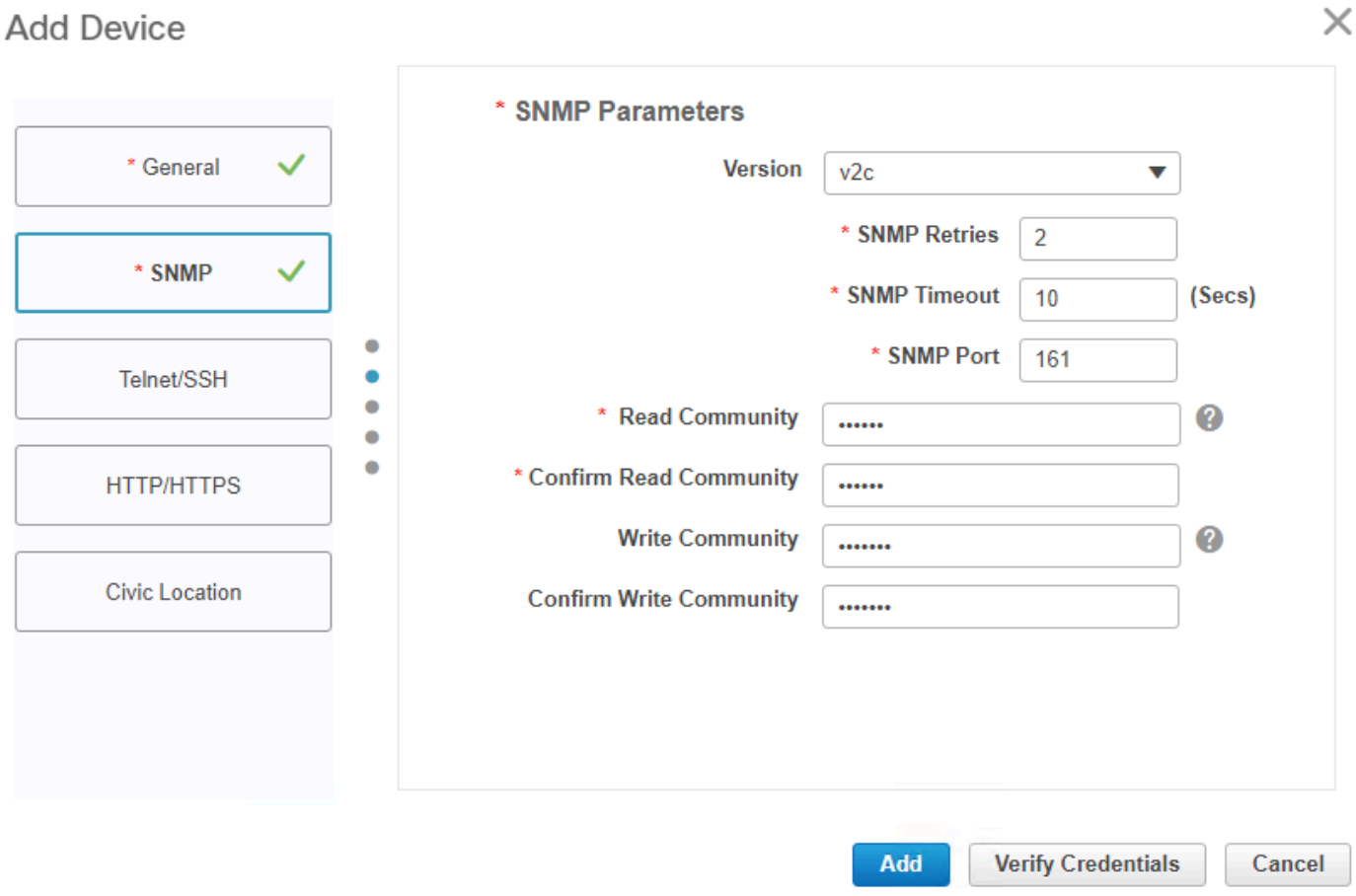
- General: IP ou DNS.
- SNMP: A comunidade RO é necessária - certifique-se de configurá-la também no Switch/WLC.

Neste guia, você está usando um switch da Cisco:

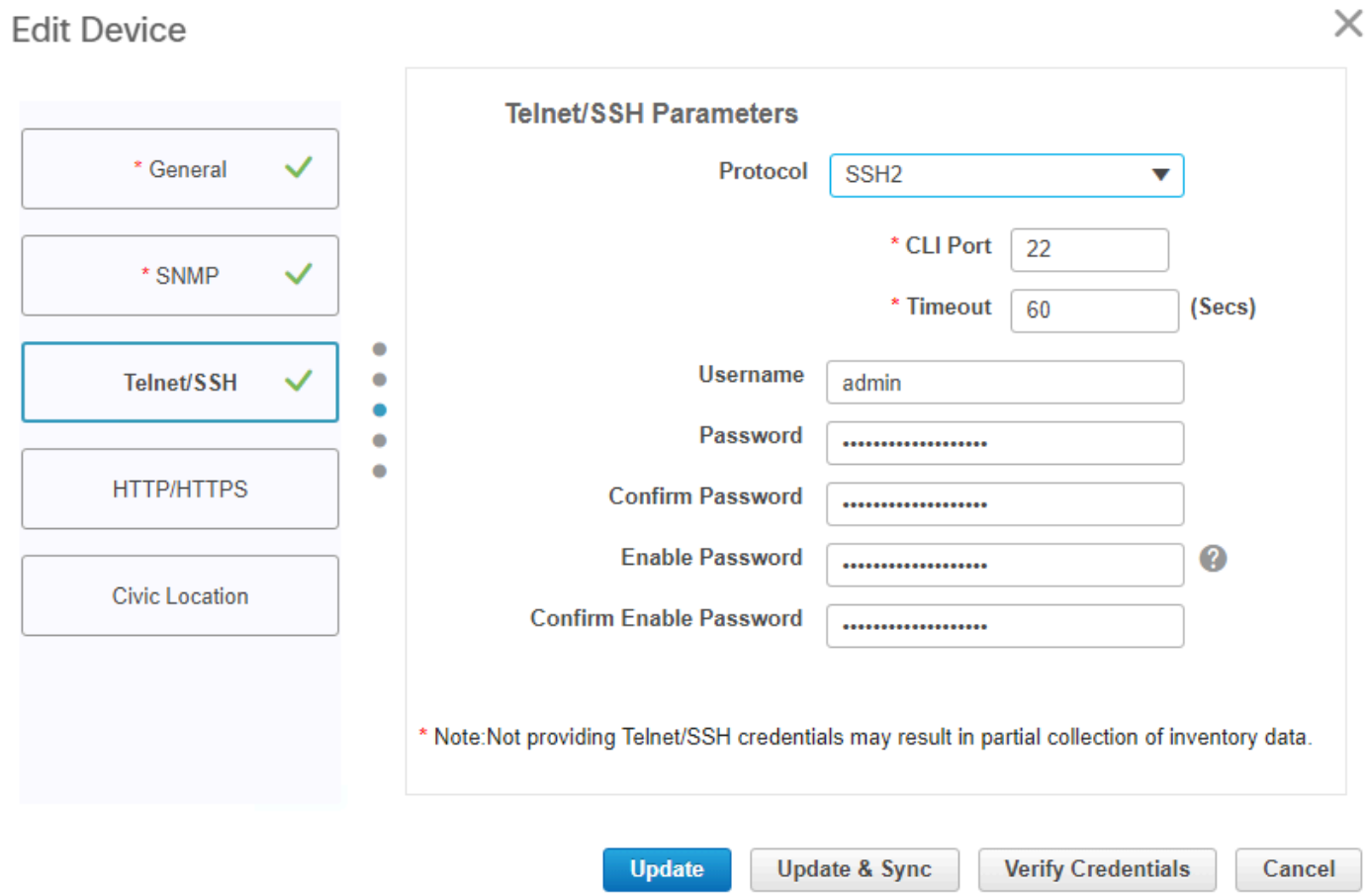
i. Seção geral:



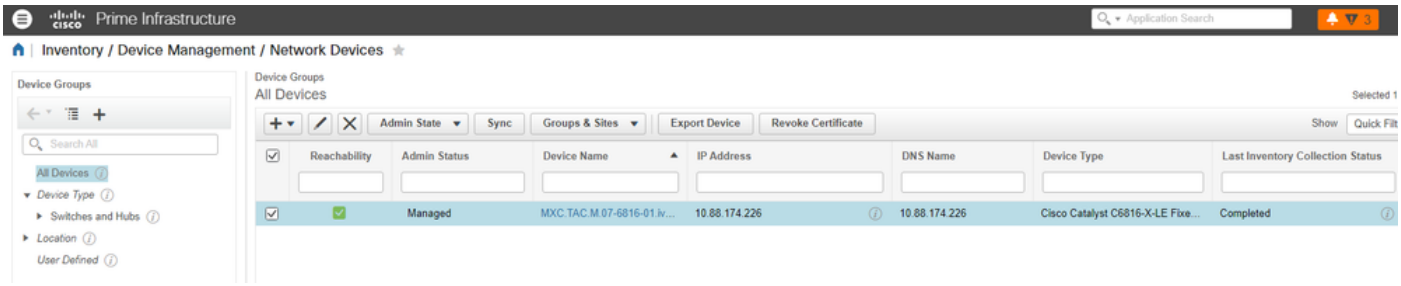
ii) Seção SNMP:



iii) Seção Telnet/SSH:



8. Quando todos os campos obrigatórios estiverem preenchidos, certifique-se de que Acessibilidade e Status da Coleta sejam Verde e Concluído, respectivamente:

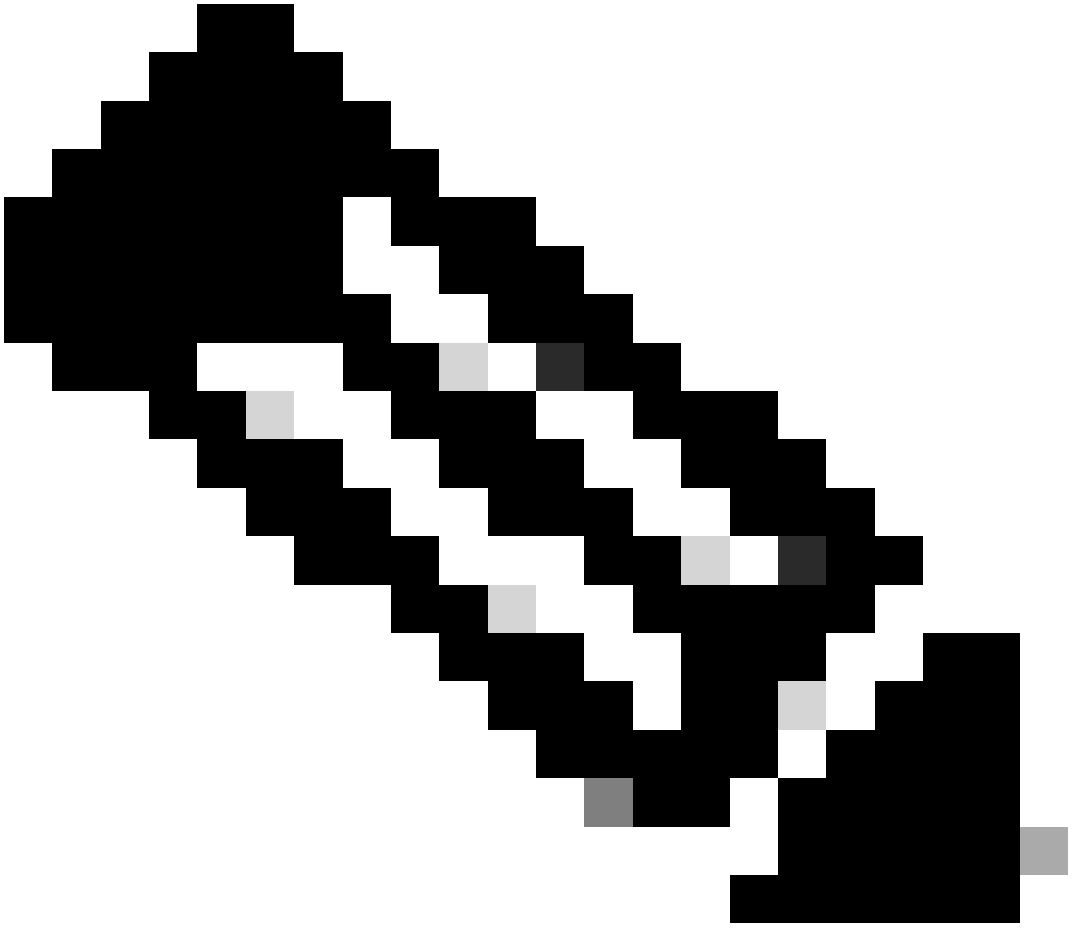


9. Integrar o Prime ao ISE.

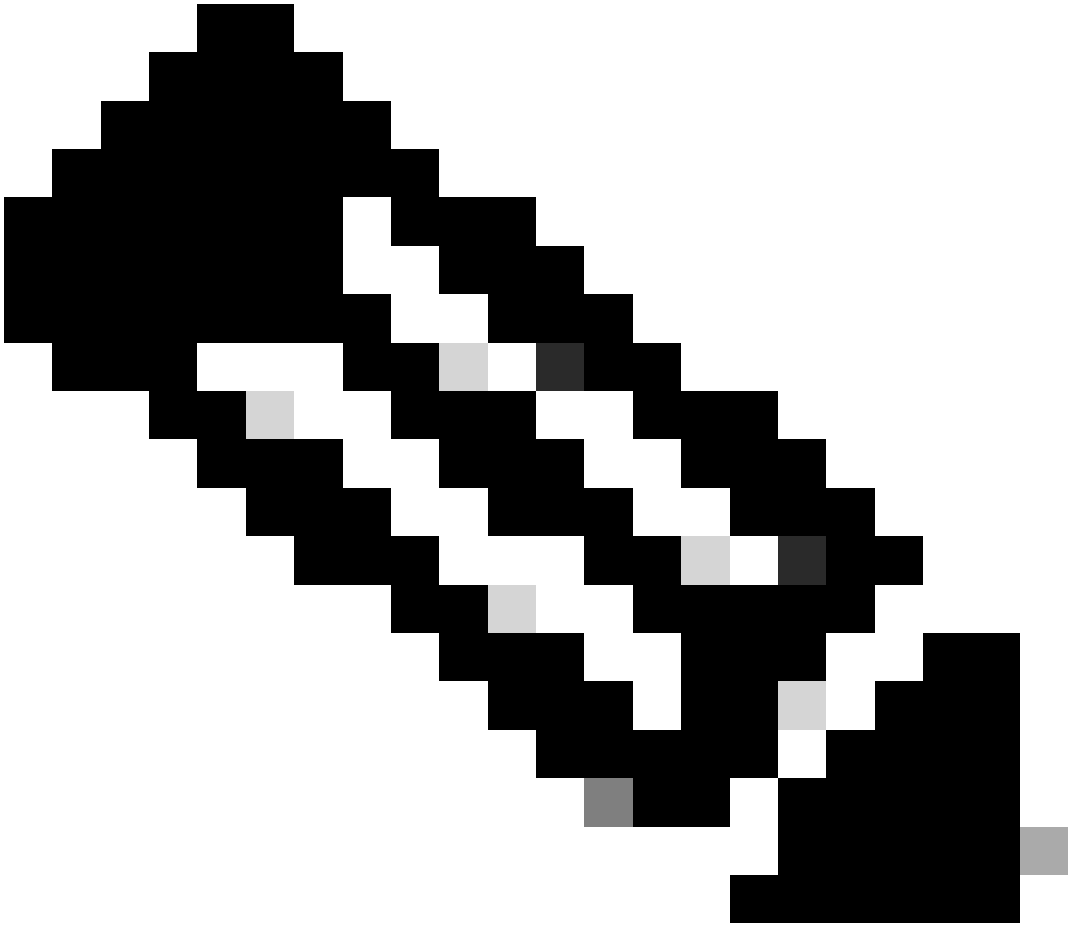
i. Navegue até Administração > Servidores > Servidores ISE.

ii) No menu suspenso, selecione Add ISE Server e clique em Go:

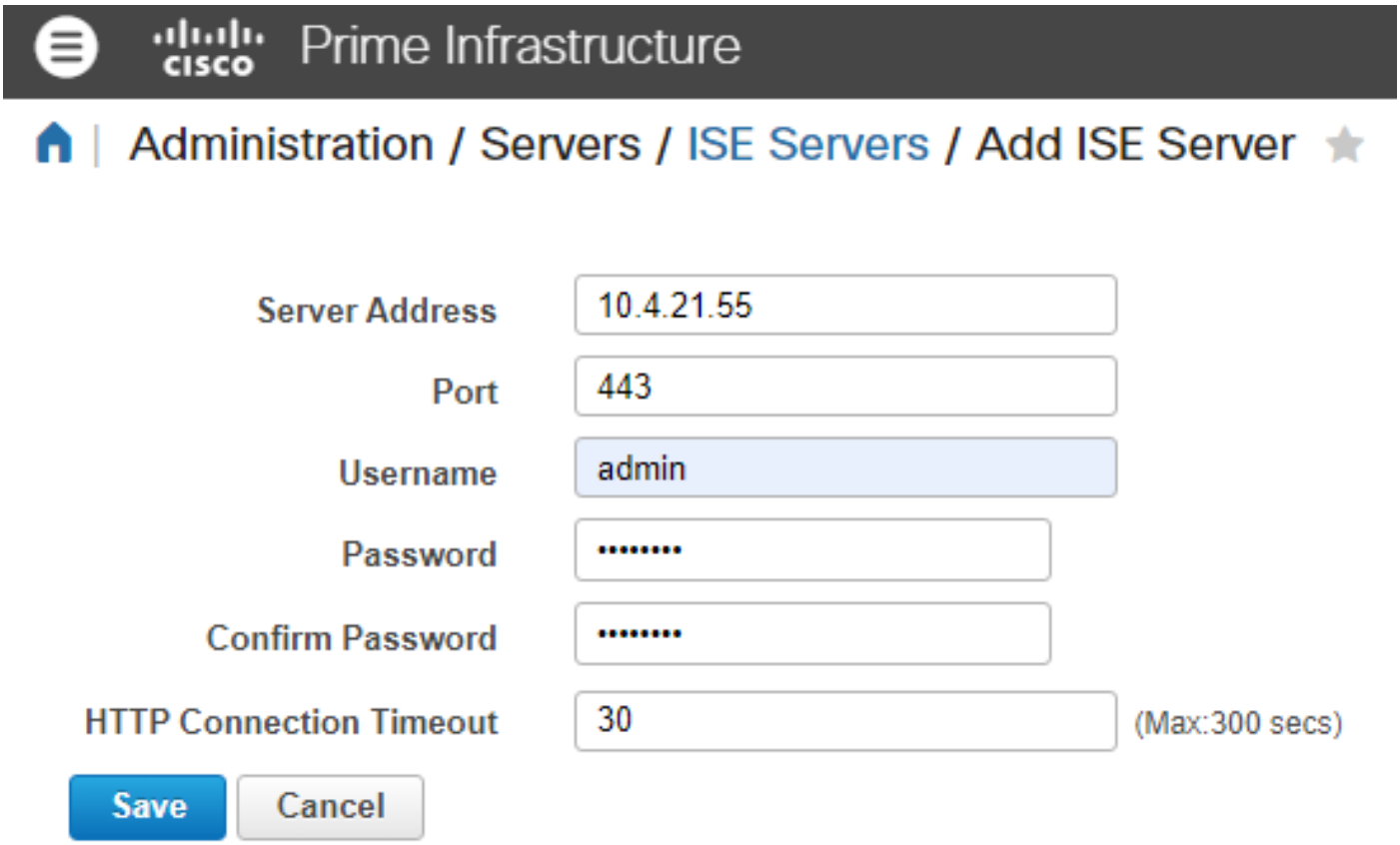
iii) Preencha todos os campos e clique em Salvar.



Note: A conexão deve ser estabelecida nos nós ISE de monitoramento primário e secundário (se aplicável).



Note: A porta padrão é definida como 443, mas você pode usar qualquer outra porta aberta no ISE para estabelecer a conexão.



iv) Navegue de volta para a página ISE Server. O status do servidor indica Acessibilidade e a Função é exibida (Independente, Principal [MnT] ou Secundário [MnT]):

Configuração do endpoint

10. O ponto final deve ser configurado para executar a autenticação dot1x (RFC 3850). Isso pode ser obtido configurando o Cisco Network Access Manager (NAM) ou aproveitando o suplicante nativo do SO. Há muitos guias relacionados a essa configuração, portanto, não incluímos essas etapas neste guia.

Verificar

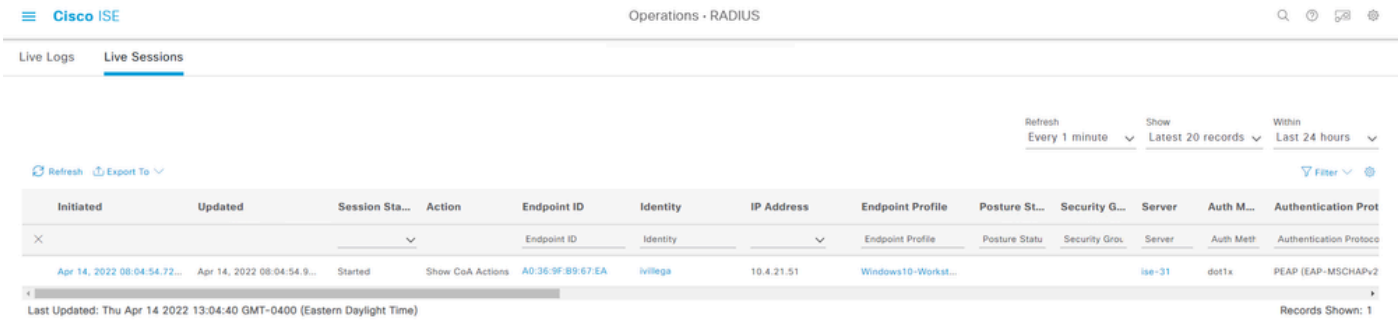
Verificar o ISE

O ISE recebe a solicitação RADIUS do NAD e autentica com êxito o usuário.

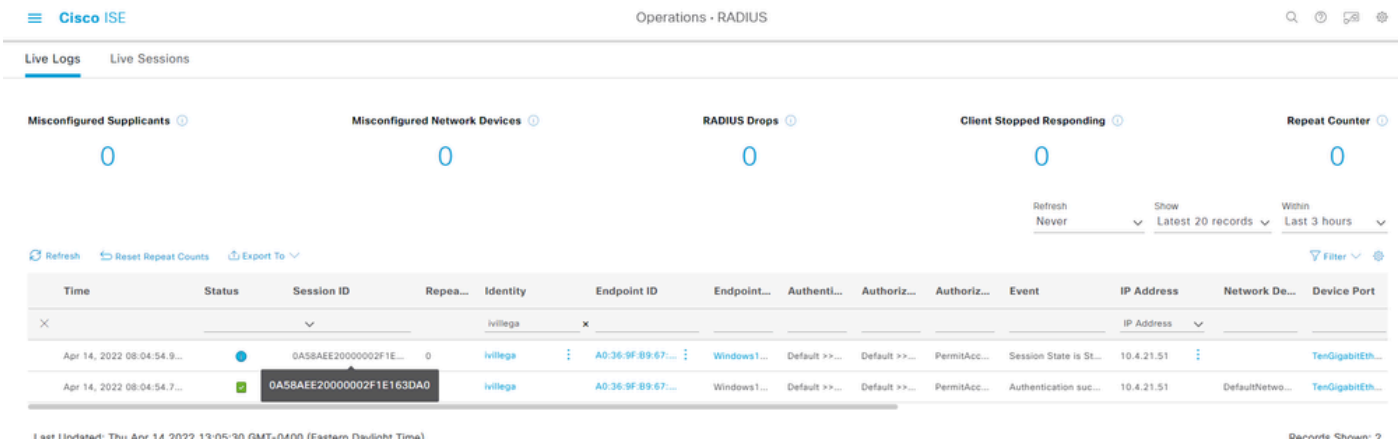
O NAD é adicionado e configurado para RADIUS no ISE > Administração > Recursos de rede > Dispositivos de rede.

1. Navegue até Operations > RADIUS > Live Sessions.

Verifique se a sessão ao vivo do usuário está listada nesta página. As informações da sessão são compartilhadas com o Prime Infrastructure.



2. Verifique o ID da sessão em Operations > RADIUS > Live Logs:



Verificar o NAD

3. Verifique os detalhes da sessão no NAD. A ID da sessão corresponde à ID da sessão no ISE:

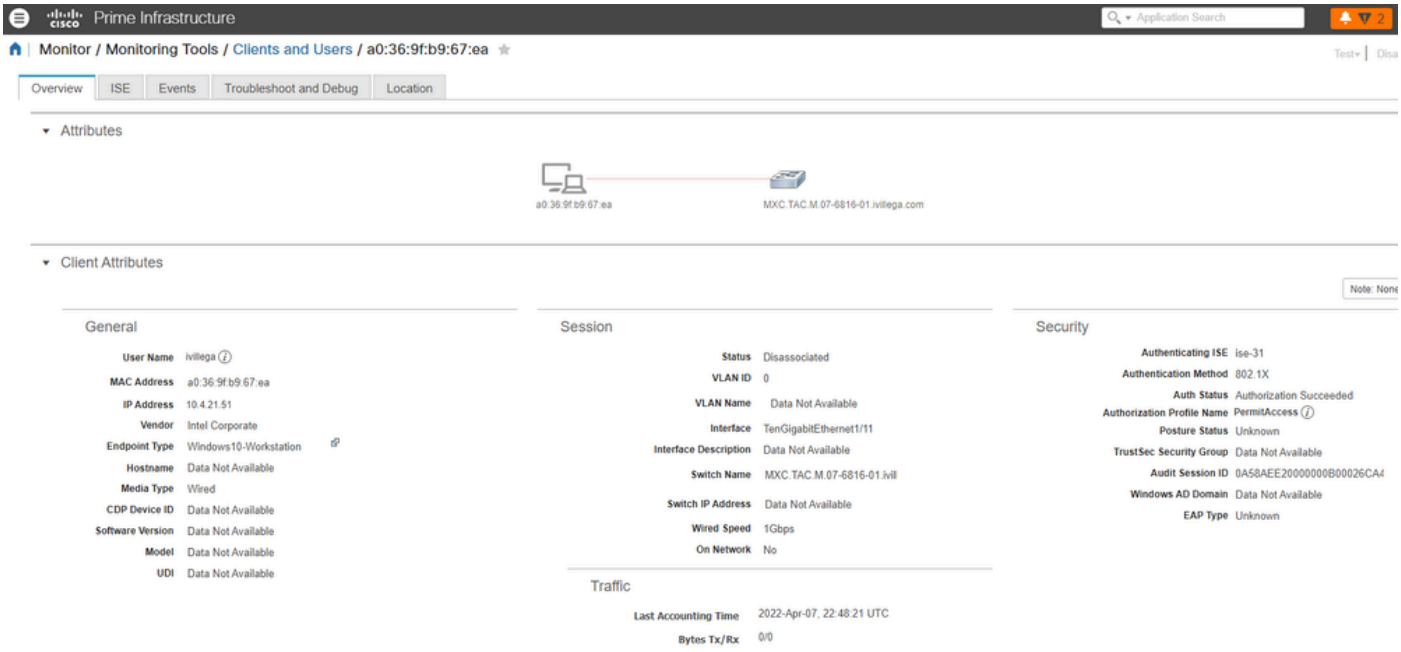
```
MXC.TAC.M.07-6816-01#show authentication session int Te1/11 detail
        Interface: TenGigabitEthernet1/11
      MAC Address: a036.9fb9.67ea
     IPv6 Address: Unknown
     IPv4 Address: 10.4.21.51
        User-Name: ivillega
           Status: Authorized
           Domain: DATA
   Oper host mode: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

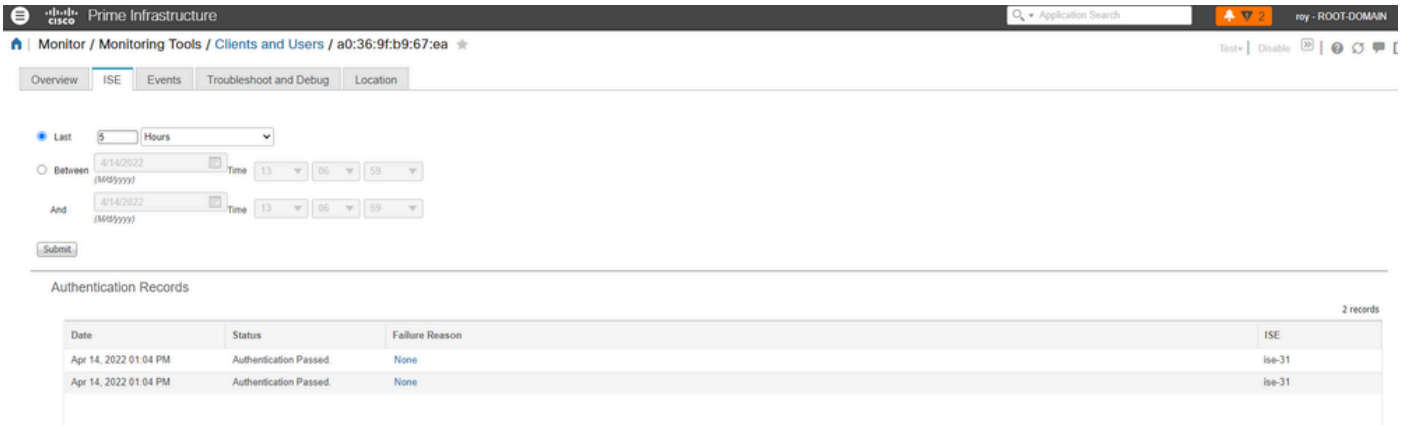
Verifique a infraestrutura Prime

4. Navegue até Monitor > Ferramentas de Monitoramento > Clientes e Usuários. O endereço MAC do ponto final é exibido:

5. Se você clicar nele, verá os detalhes da sessão do usuário e as informações do servidor ISE:



6. Há também uma guia rotulada como ISE para recuperar os eventos de sessão para este endpoint específico. Você pode selecionar um período de tempo que a Prime Infrastructure usa para buscar eventos do ISE:



Troubleshooting

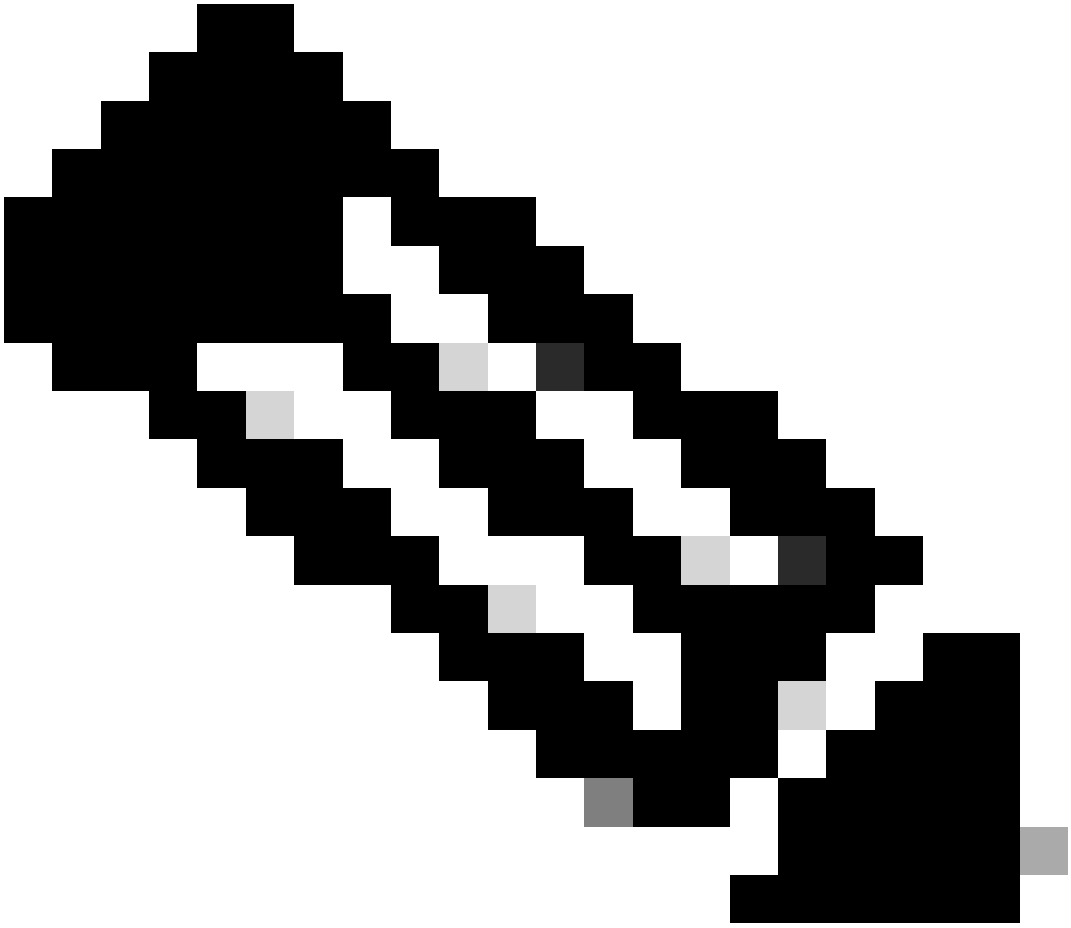
1. Teste a conectividade entre ISE e Prime Infrastructure com pings. Se não houver conectividade, você poderá usar rotas de rastreamento do ISE ou do PI para localizar o problema.

2. Verifique se a porta configurada na Etapa 9 está aberta no nó ISE MnT (a porta padrão é 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 a porta estiver listada na saída, isso significa que o ISE MnT tem a porta aberta.

Se não houver saída ou se a porta não estiver listada, significa que o ISE MnT tem essa porta fechada. Nesse caso, você pode tentar com outra porta ou abrir um caso de TAC com a equipe do ISE para verificar por que a porta não está aberta.



Note: O nó MnT do ISE usa apenas algumas portas; não há como abrir portas no nó MnT do ISE que não estejam listadas no guia de instalação do ISE, seção Referência de porta.

3. Teste a porta configurada na Etapa 9 com Telnet da infraestrutura Prime:

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

Se o resultado do teste telnet for Conectado a <ISE MnT IP/FQDN>, isso significa que o teste foi bem-sucedido.

Se o resultado do teste telnet estiver travado em Trying <ISE MnT IP/FQDN> (Tentando <IP/FQDN ISE MnT>), isso significa que o teste falhou. Isso pode estar relacionado às ACLs em seus dispositivos de rede intermediários ou às regras de firewall.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.