Integre ISE con Prime Infrastructure para la visibilidad de terminales

Contenido

Introducción

Este documento describe cómo integrar ISE con Prime Infrastructure para obtener visibilidad de los terminales autenticados.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco ISE.
- Infraestructura Cisco Prime.
- Flujo AAA inalámbrico o con cables para terminales que se autentican con ISE.
- Configuración SNMP en NAD (dispositivos de acceso a la red) como switches y WLC.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

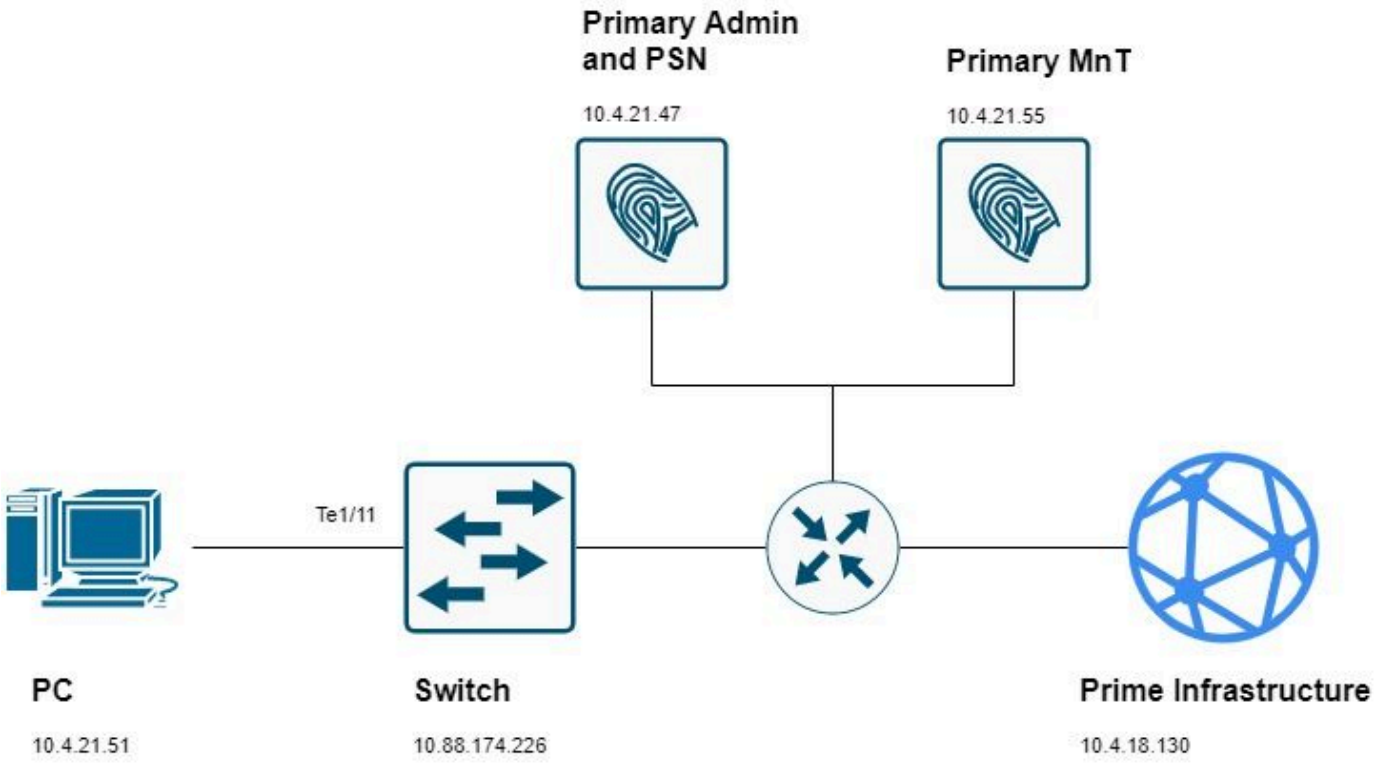
- Implementación de ISE 3.1.

- Cisco Prime Infrastructure 3.8.
- C6816-X-LE que ejecuta Cisco IOS® 15.5.
- Windows 10 Machine.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red



Configuraciones

Configuración del switch

1. Configure el dispositivo de acceso a la red (NAD) para la autenticación AAA con ISE. En esta guía está utilizando esta configuración:

```
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 el rastreo de dispositivos en el switch:

```
device-tracking policy DT1
 tracking enable

device-tracking tracking auto-source
```

3. Configure el switchport para la autenticación dot1x y adjunte la política de seguimiento de dispositivos a él:

```
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
```

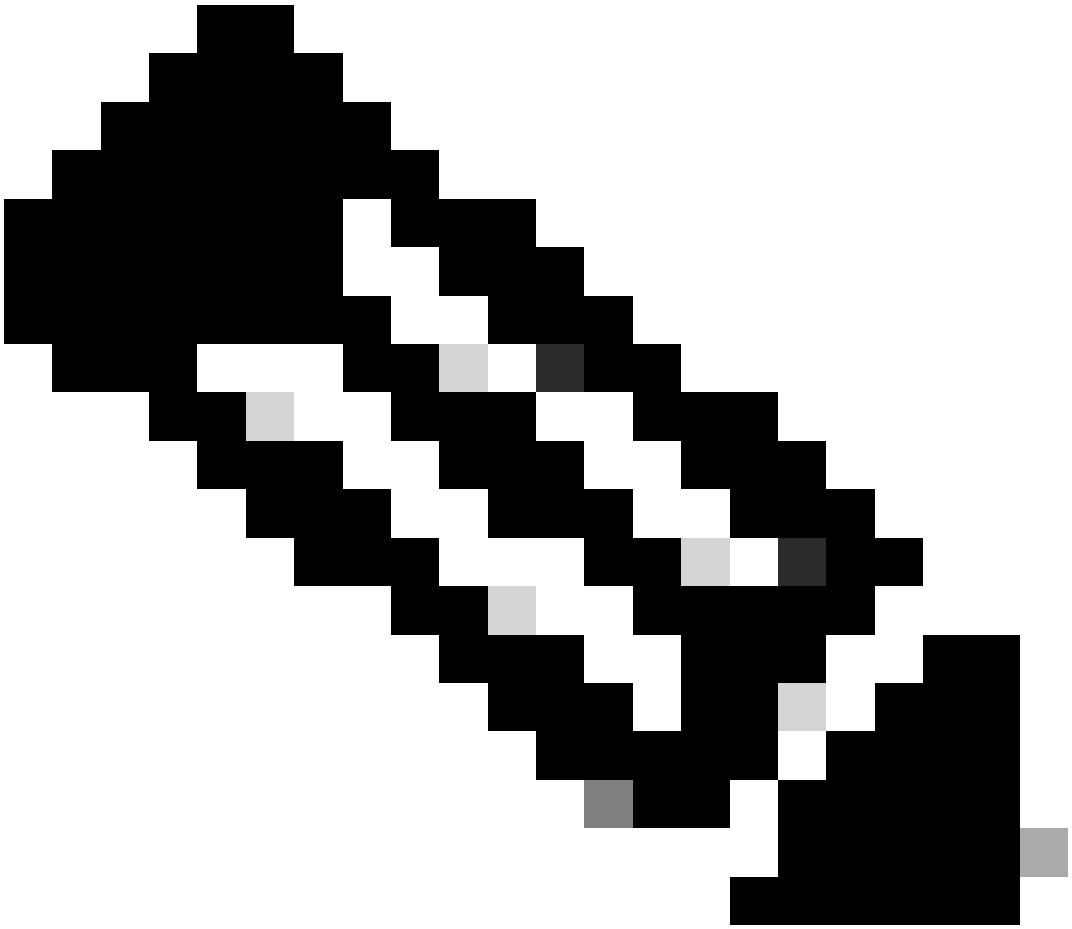
4. Configure RO SNMP community y SNMP traps para satisfacer los requisitos de su red (Opcionalmente, puede configurar la comunidad RW):

```
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 un acceso Telnet o SSH para que Prime pueda administrar el 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 las conexiones SSH, se requiere una clave RSA. Si el NAD no tiene uno, utilice estos pasos para generarlo.

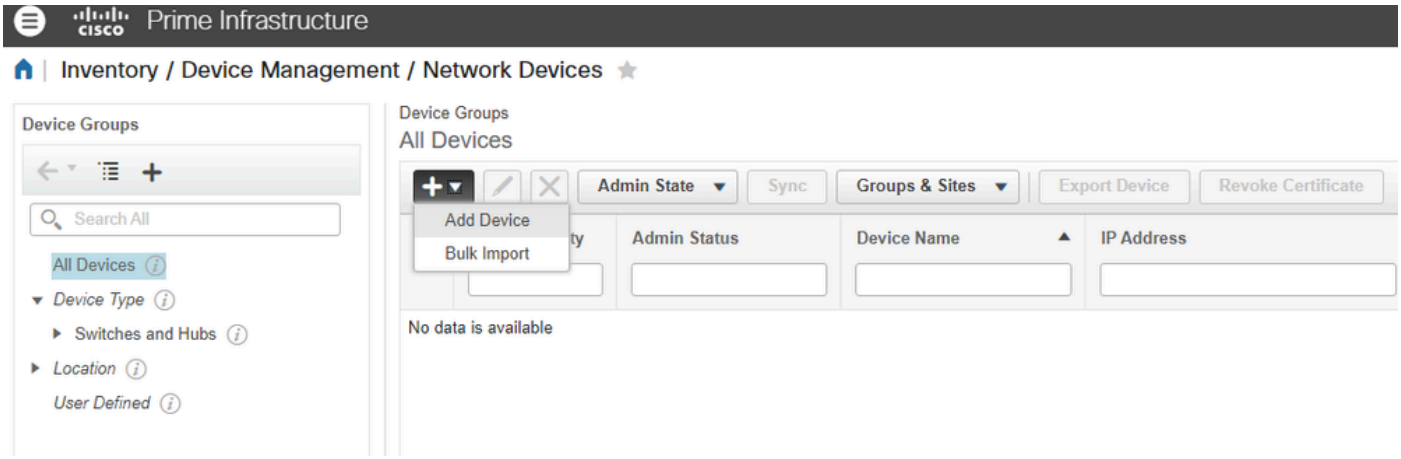


Nota: Algunos dispositivos requieren un dominio configurado antes de generar el RSA. Compruebe si el dispositivo tiene un dominio configurado de modo que no anule el dominio existente.

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

Configuración de Cisco Prime Infrastructure

7. Agregue el Dispositivo de red en Inventario > Administración de dispositivos > Dispositivos de red > Signo más (+) > Agregar dispositivo:



Los campos obligatorios para completar el inventario son:

Para dispositivos con cables:

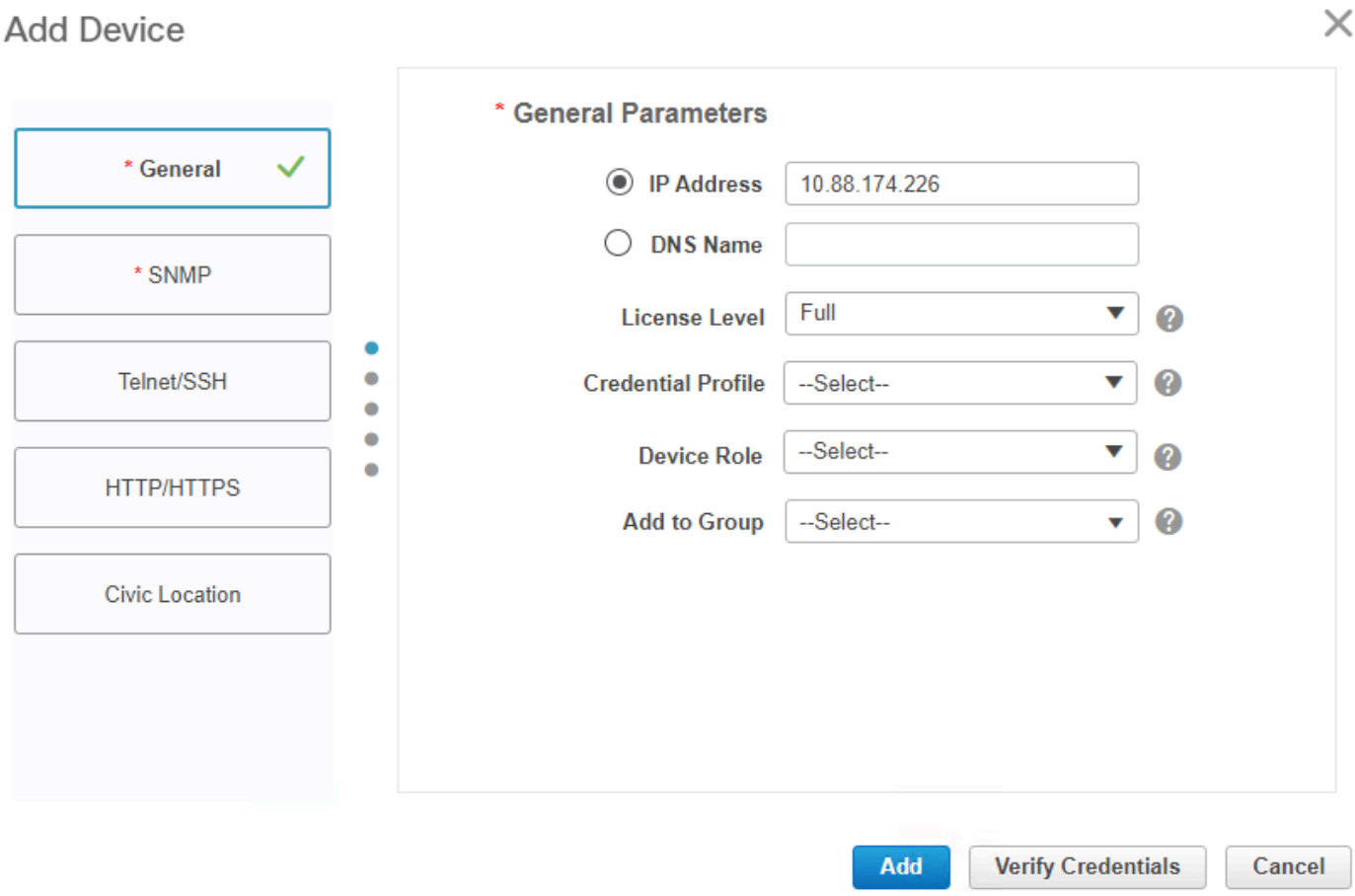
- General: IP o DNS.
- SNMP (Protocolo de administración de red simple): La comunidad RO es necesaria - asegúrese de configurarla también en el Switch/WLC.
- Telnet/SSH: Credenciales de modo Exec y modo enable.

Para WLC:

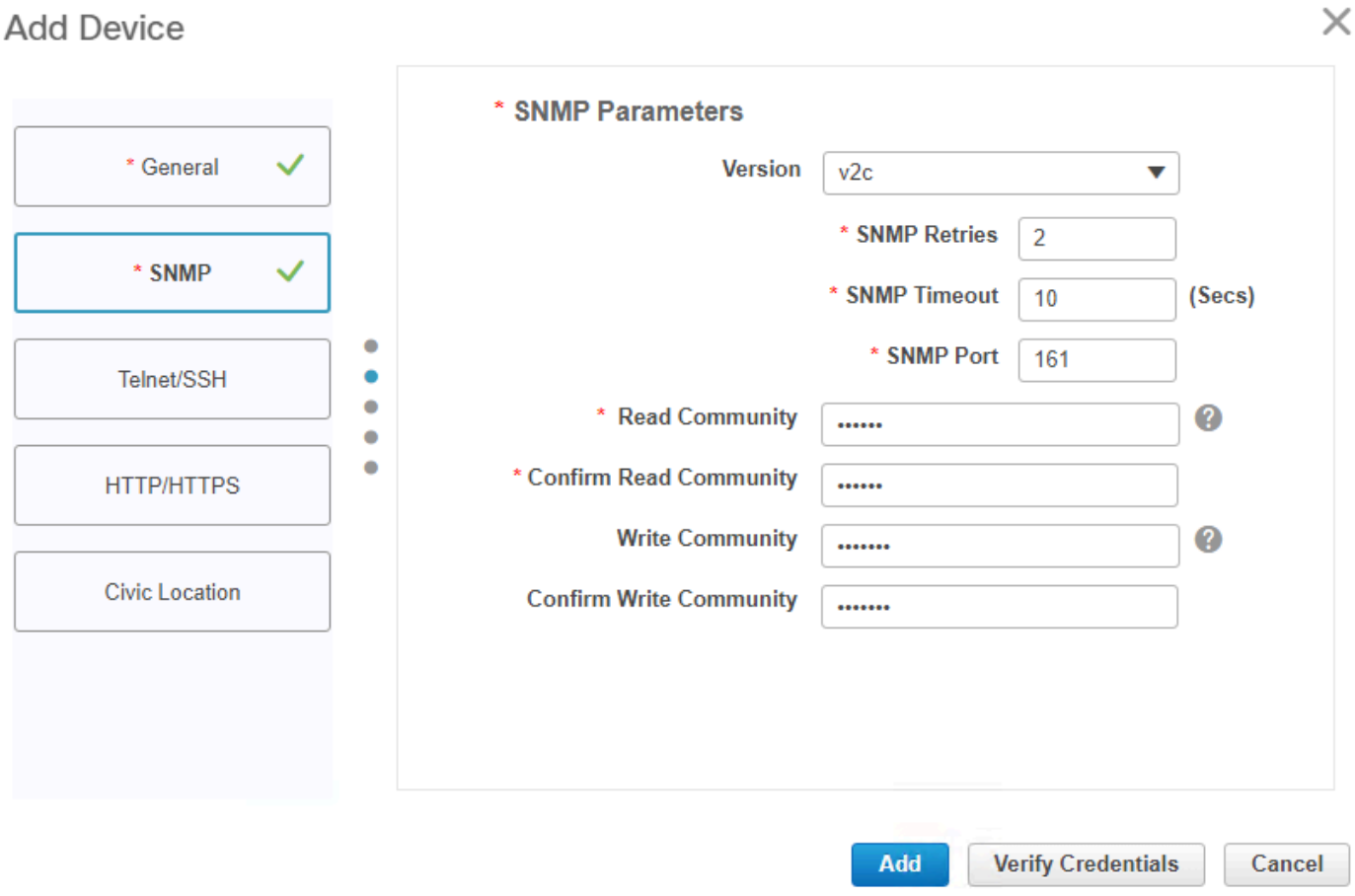
- General: IP o DNS.
- SNMP (Protocolo de administración de red simple): La comunidad RO es necesaria - asegúrese de configurarla también en el Switch/WLC.

En esta guía se utiliza un switch de Cisco:

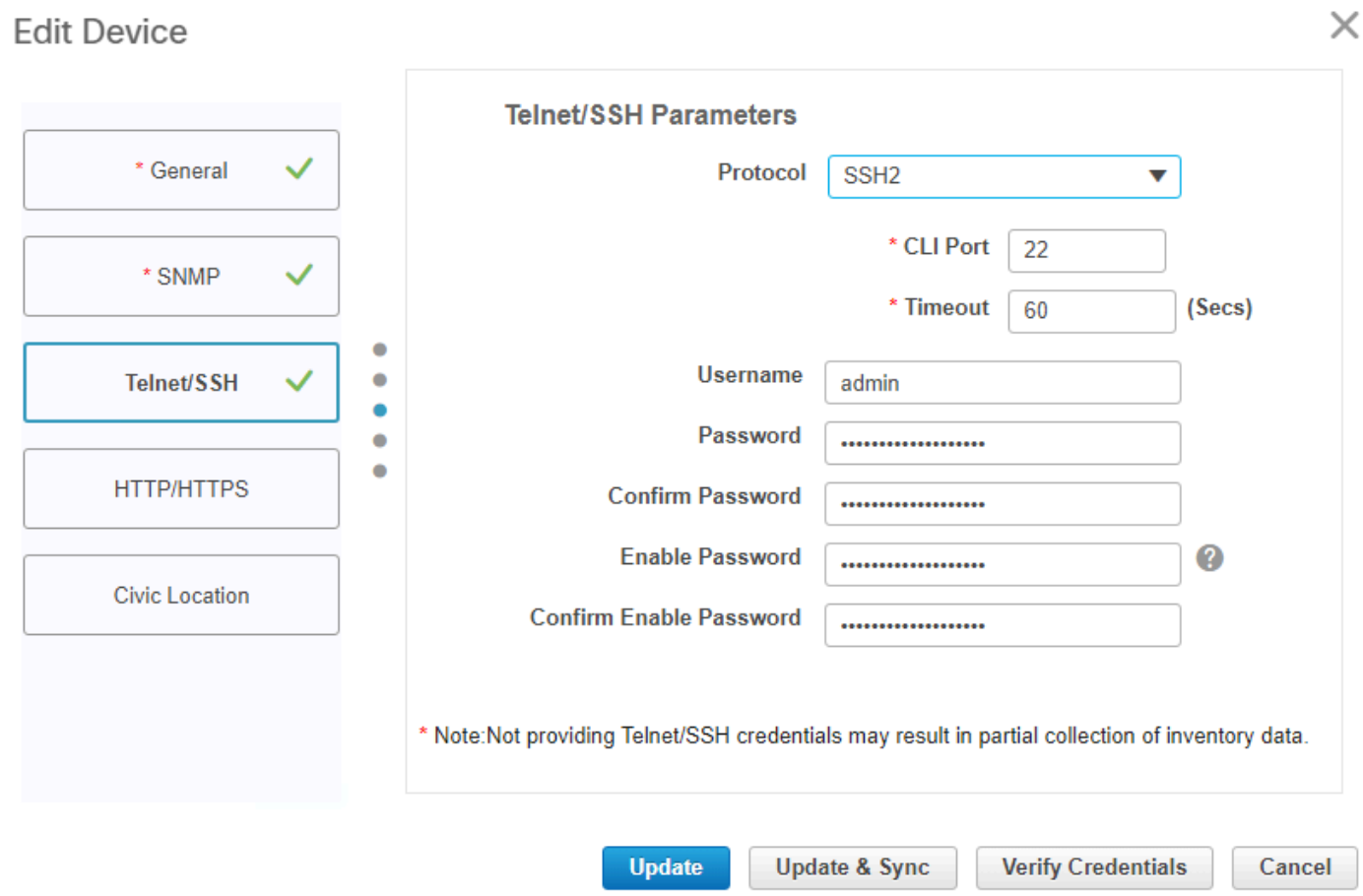
i. Sección General:



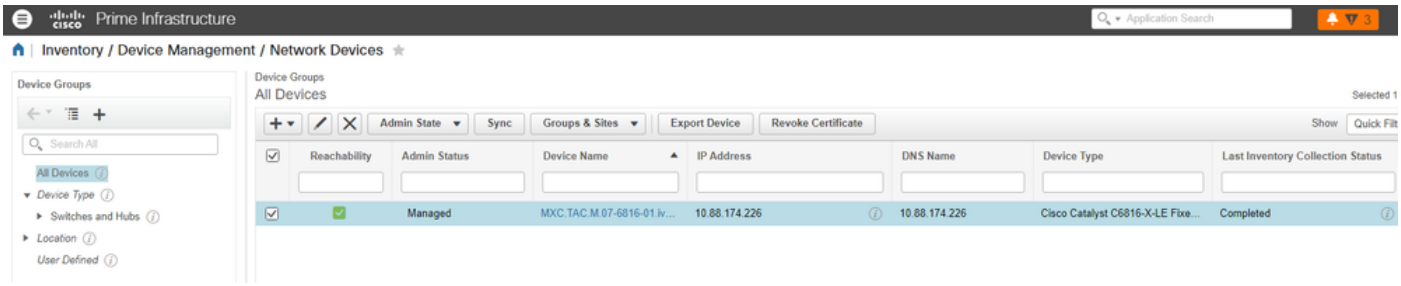
ii. La sección SNMP:



iii. Sección Telnet/SSH:



8. Una vez cumplimentados todos los campos obligatorios, asegúrese de que Reachability y Collection Status son Green y Completed, respectivamente:

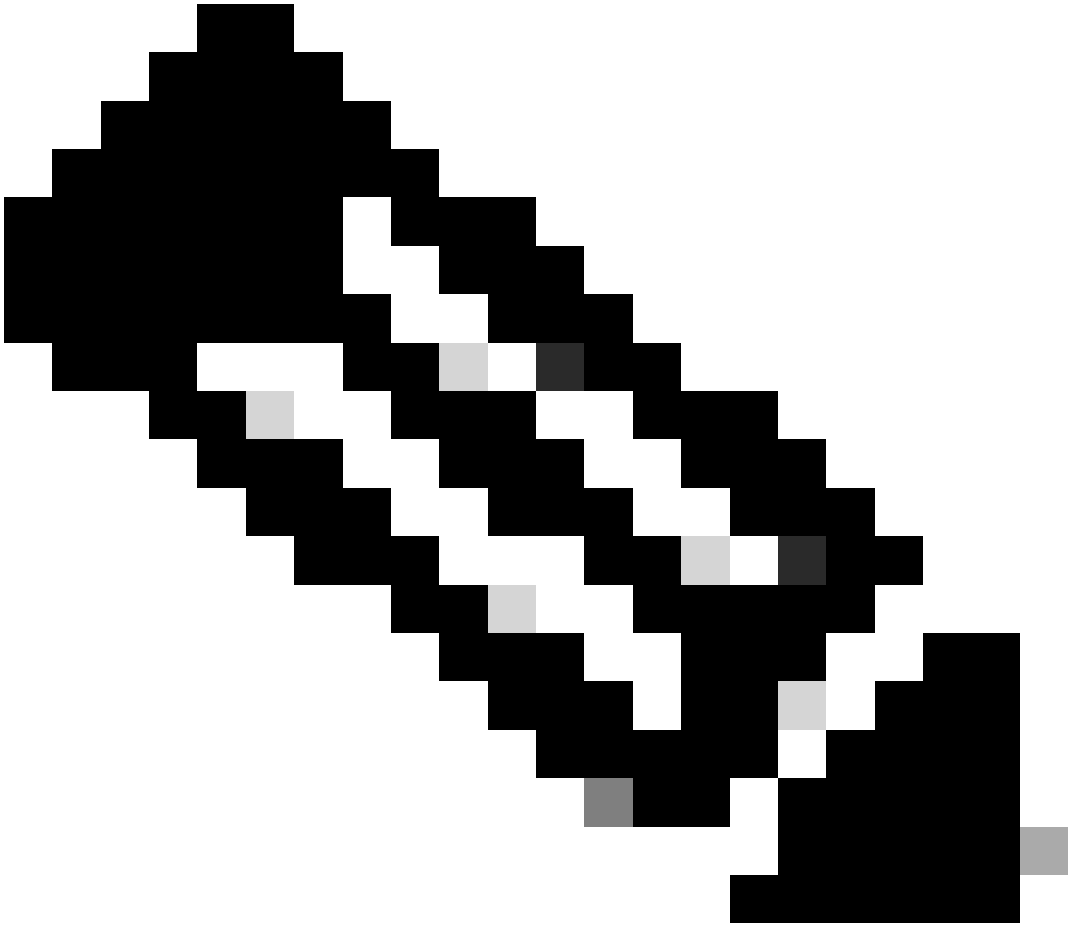


9. Integre Prime con ISE.

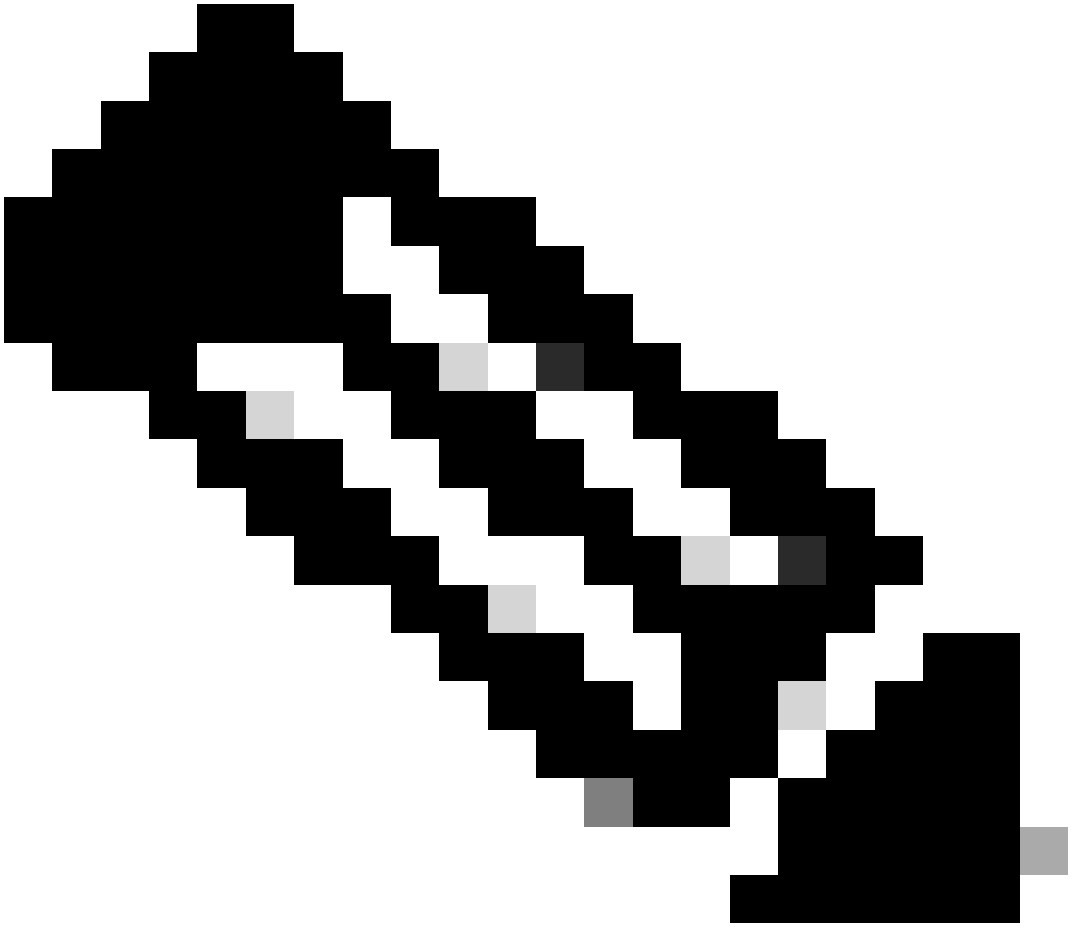
i. Vaya a Administration > Servers > ISE Servers.

ii. En el menú desplegable, seleccione Add ISE Server y haga clic en Go:

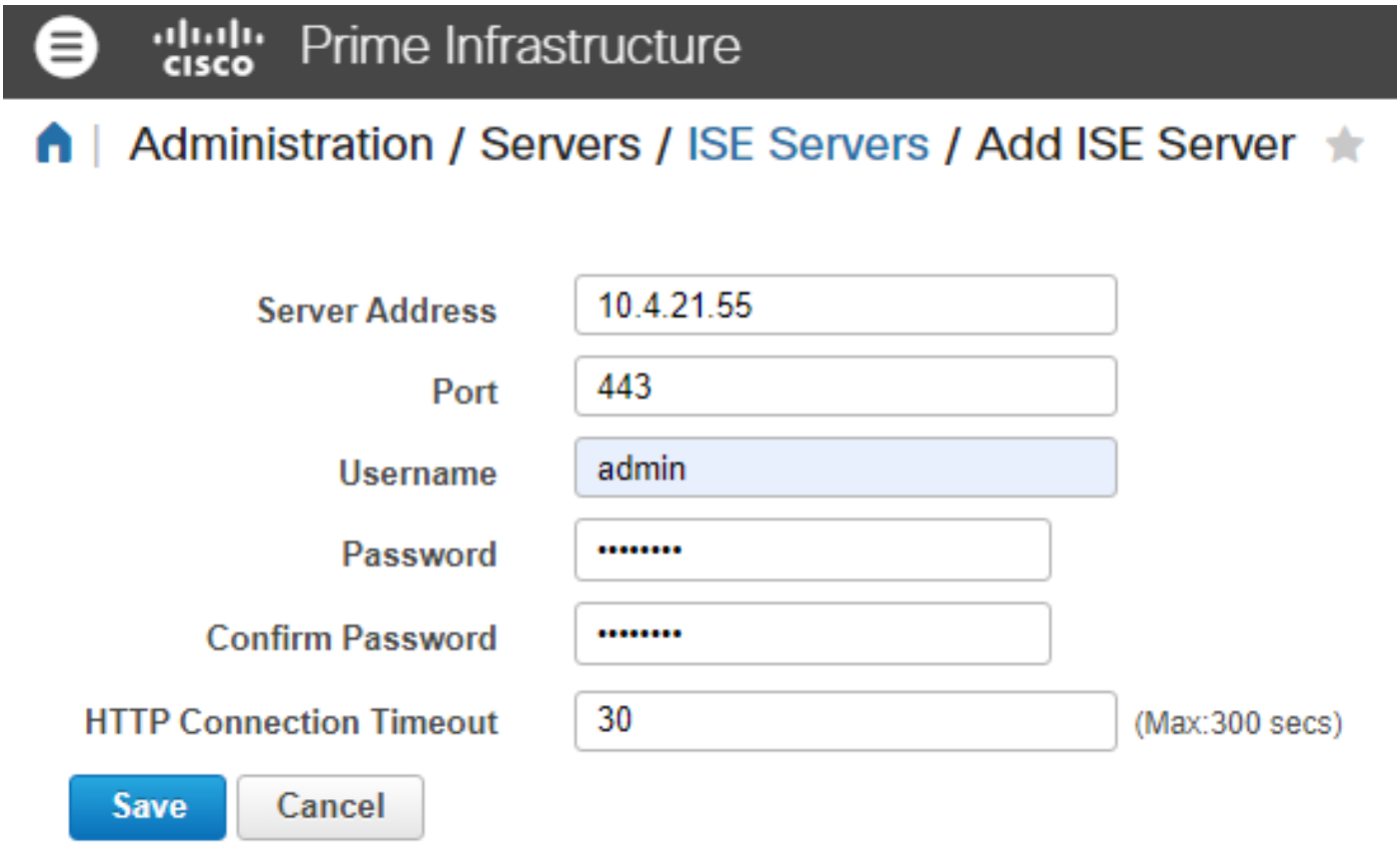
iii. Rellene todos los campos y haga clic en Guardar.



Nota: La conexión se debe establecer con respecto a los nodos ISE de supervisión primarios y secundarios (si procede).



Nota: El puerto predeterminado está establecido en 443, pero puede utilizar cualquier otro puerto abierto en ISE para establecer la conexión.



iv. Vuelva a la página Servidor ISE. El estado del servidor indica alcanzable y se muestra el rol (independiente, principal [MnT] o secundario [MnT]):

Configuración de terminales

10. El terminal debe configurarse para realizar la autenticación dot1x (RFC 3850). Esto se puede conseguir configurando Cisco Network Access Manager (NAM) o aprovechando el suplicante nativo del sistema operativo. Hay muchas guías con respecto a esta configuración, por lo que no incluimos esos pasos en esta guía.

Verificación

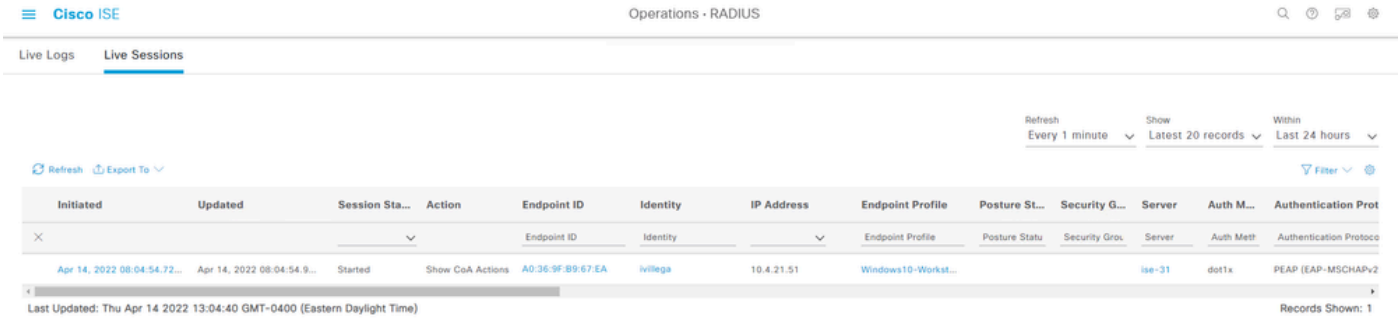
Verificar ISE

ISE recibe la solicitud RADIUS del NAD y autentica correctamente al usuario.

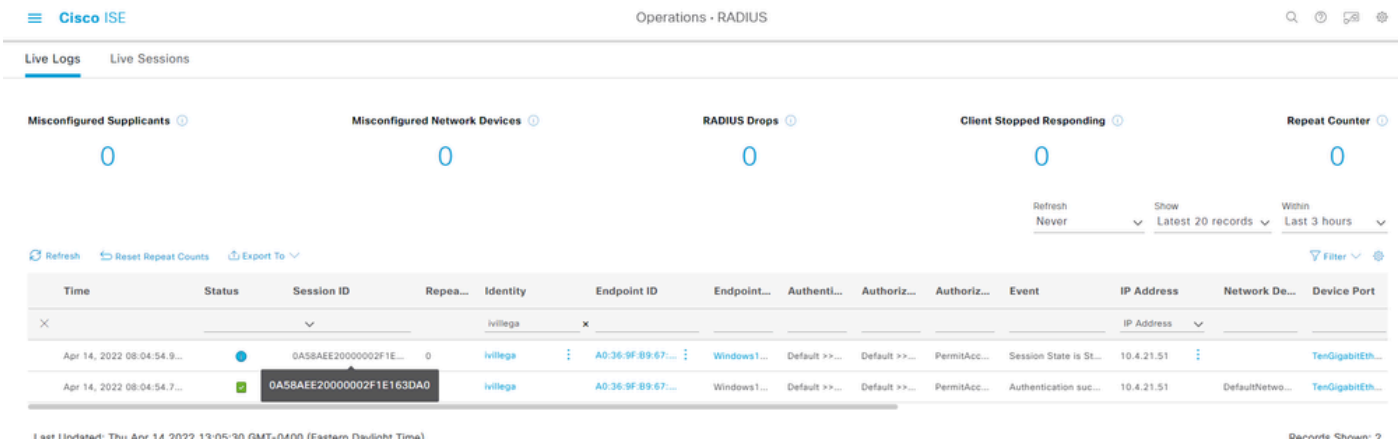
El NAD se agrega y configura para RADIUS en ISE > Administration > Network Resources > Network Devices .

1. Vaya a Operaciones > RADIUS > Sesiones en Vivo.

Asegúrese de que la sesión en directo del usuario aparece en esta página. La información de la sesión se comparte con Prime Infrastructure.



2. Verifique el ID de sesión en Operaciones > RADIUS > Registros en vivo:



Verifique el NAD

3. Compruebe los detalles de la sesión en el NAD. El ID de sesión coincide con el ID de sesión en ISE:

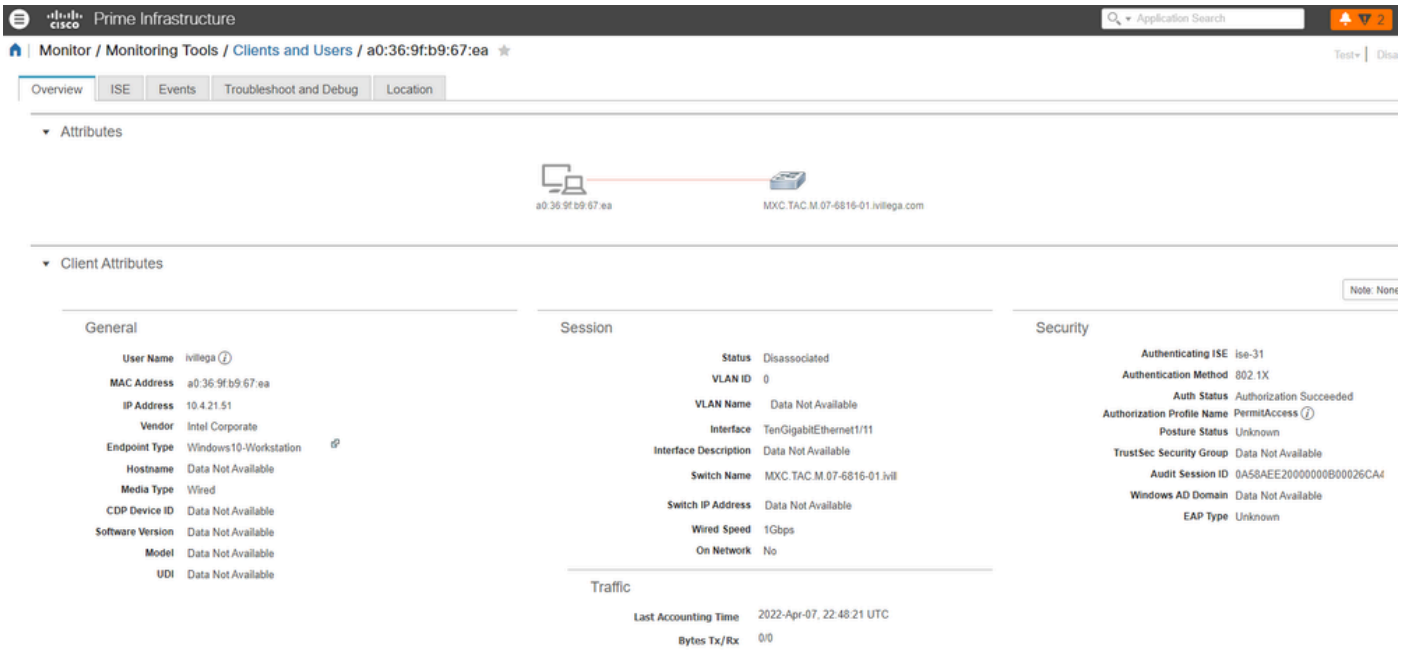
```
MXC.TAC.M.07-6816-01#show authentication session int Te1/11 detail
        Interface: TenGigabitEthernet1/11
      MAC Address: a036.9fb9.67ea
     IPv6 Address: Unknown
     IPv4 Address: 10.4.21.51
        User-Name: ivillega
           Status: Authorized
           Domain: DATA
   Oper host mode: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

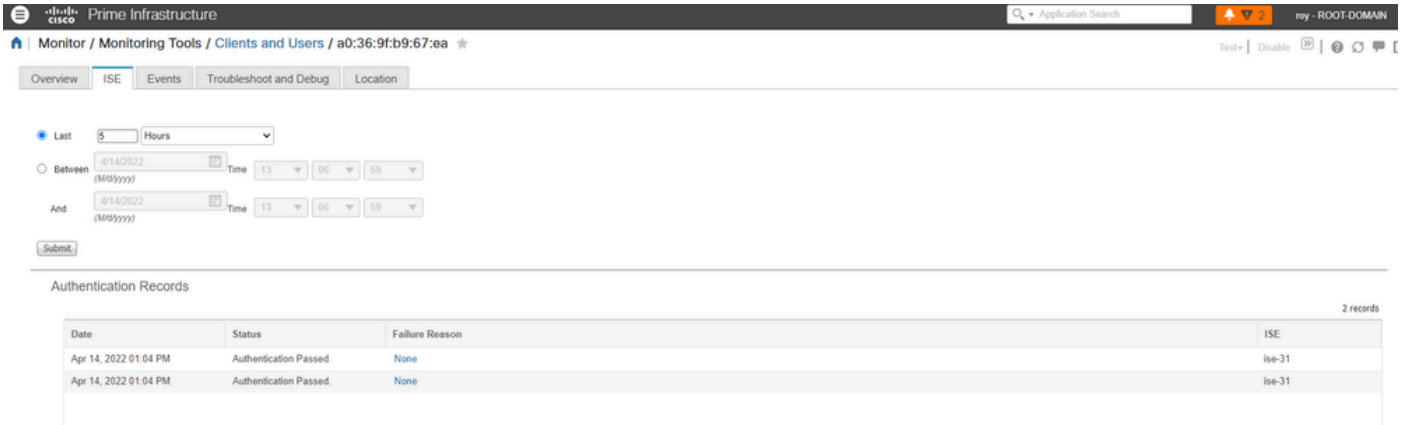
Verificar la infraestructura Prime

4. Vaya a Monitor > Herramientas de Monitoreo > Clientes y Usuarios. Se muestra la dirección MAC del terminal:

5. Si hace clic en él, verá los detalles de la sesión del usuario y la información del servidor ISE:



6. También hay una pestaña etiquetada como ISE para recuperar los eventos de sesión para este terminal en particular. Puede seleccionar un período de tiempo que Prime Infrastructure utilizará para recuperar los eventos de ISE:



Troubleshoot

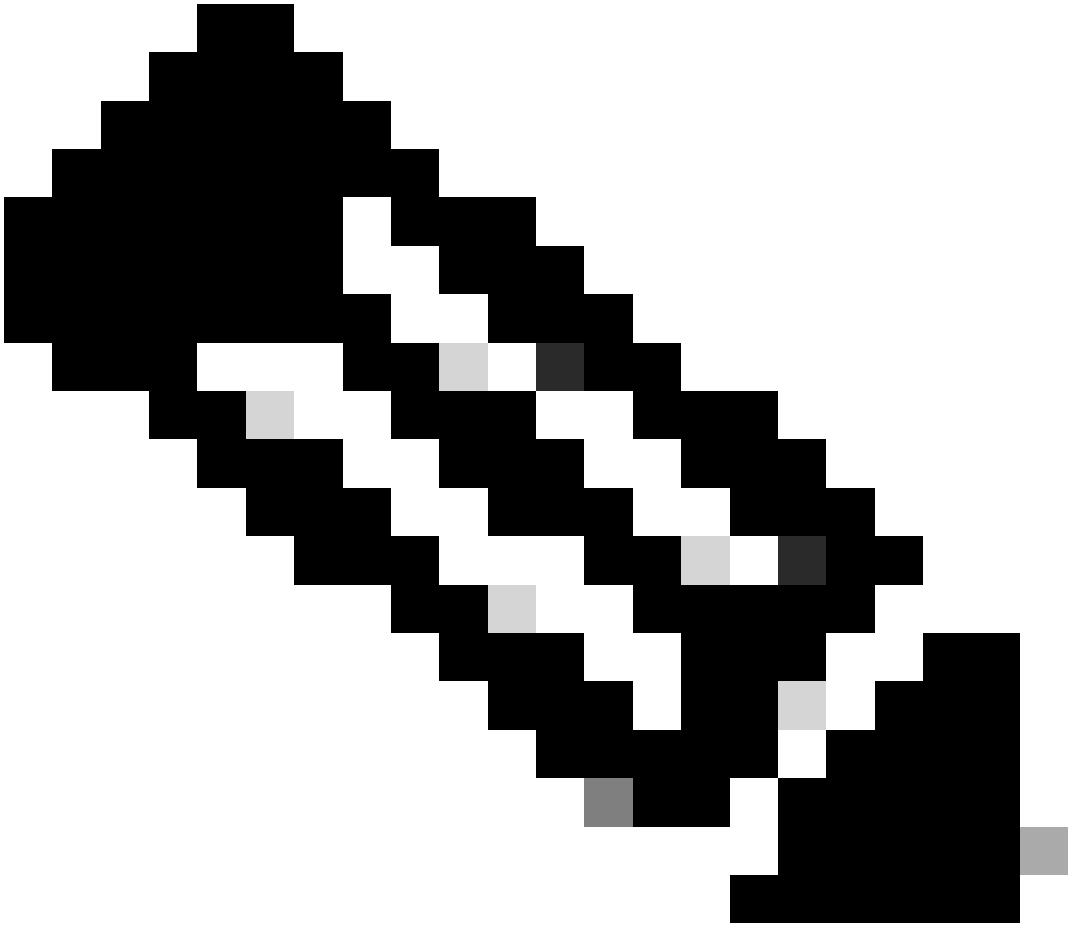
1. Pruebe la conectividad entre ISE y Prime Infrastructure con pings. Si no hay conectividad, puede utilizar rutas de seguimiento de ISE o PI para localizar el problema.

2. Compruebe que el puerto configurado en el paso 9 está abierto en el nodo ISE MnT (el puerto predeterminado es el 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
```

Si el puerto aparece en la salida, significa que ISE MnT tiene el puerto abierto.

Si no hay salida o el puerto no aparece en la lista, significa que ISE MnT tiene ese puerto cerrado. En tal caso, puede probar con otro puerto o abrir un caso TAC con el equipo ISE para verificar por qué el puerto no está abierto.



Nota: El nodo MnT de ISE solo utiliza algunos puertos. No hay forma de abrir puertos en el nodo MnT de ISE que no aparezcan en la guía de instalación de ISE, sección Referencia de puerto.

3. Pruebe el puerto configurado en el paso 9 con Telnet desde la infraestructura Prime:

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

Si la salida de la prueba telnet está conectada a <ISE MnT IP/FQDN>, significa que la prueba se realizó correctamente.

Si el resultado de la prueba telnet se bloquea en Intentando <ISE MnT IP/FQDN>, significa que la prueba ha fallado. Esto puede estar relacionado con las ACL en los dispositivos de red

intermediarios o con las reglas de firewall.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).