Configure las credenciales del dispositivo en la sonda de red FindIT

Introducción

Cisco FindIT Network Management proporciona herramientas que le ayudan a supervisar, administrar y configurar fácilmente los dispositivos de red de Cisco de las series 100 a 500, como switches, routers y puntos de acceso inalámbricos (WAP), mediante el explorador web. También le notifica sobre el dispositivo y las notificaciones de soporte de Cisco, como la disponibilidad de nuevo firmware, el estado del dispositivo, las actualizaciones de la configuración de red y cualquier dispositivo Cisco conectado que ya no esté en garantía o cubierto por un contrato de soporte.

FindIT Network Management es una aplicación distribuida que consta de dos componentes o interfaces independientes: una o varias sondas denominadas FindIT Network Probe y un solo administrador denominado FindIT Network Manager.

Una instancia de la sonda de red FindIT instalada en cada sitio de la red realiza el descubrimiento de la red y se comunica directamente con cada dispositivo de Cisco. En una red de sitio único, puede optar por ejecutar una instancia independiente de la sonda de red FindIT. Sin embargo, si la red está compuesta por varios sitios, puede instalar FindIT Network Manager en una ubicación conveniente y asociar cada sonda al administrador. Desde la interfaz del administrador, puede obtener una vista de alto nivel del estado de todos los sitios de la red y conectarse a la sonda instalada en un sitio determinado cuando desee ver información detallada para ese sitio.

Para que FindIT Network detecte y gestione completamente la red, la sonda de red FindIT debe tener credenciales para la autenticación con los dispositivos de red. Cuando se descubre un dispositivo por primera vez, la sonda intentará autenticarse con el dispositivo mediante el nombre de usuario y la contraseña predeterminados y el protocolo simple de administración de red (comunidad SNMP). Si las credenciales del dispositivo se han cambiado del valor predeterminado, será necesario que proporcione las credenciales correctas a FindIT. Si este intento falla, se generará un mensaje de notificación y el usuario deberá proporcionar credenciales válidas.

Objetivo

El objetivo de este documento es mostrarle cómo configurar las credenciales del dispositivo en la sonda de red de Cisco.

Dispositivos aplicables

- Buscar sonda de TI

Versión del software

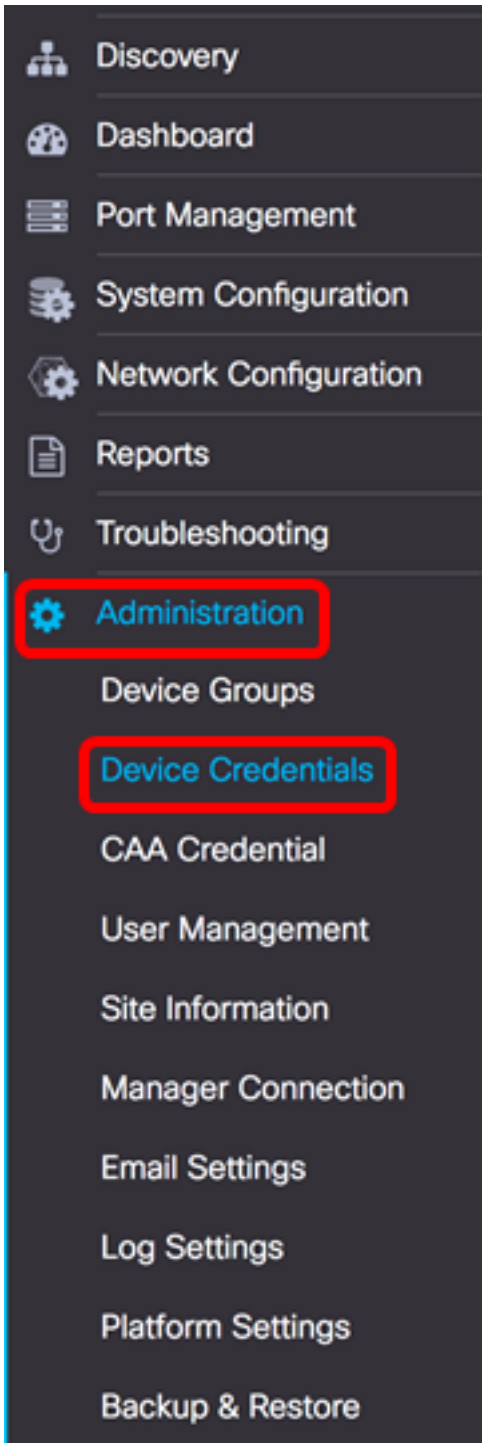
- 1.1

Configurar las credenciales del dispositivo

Agregar nuevas credenciales

Introduzca uno o varios conjuntos de credenciales en los campos siguientes. Cuando se aplica, cada credencial se probará con cualquier dispositivo del tipo adecuado para el que no estén disponibles las credenciales de trabajo. Un conjunto de credenciales puede ser una combinación de nombre de usuario/contraseña, una comunidad SNMPv2 o credenciales SNMPv3.

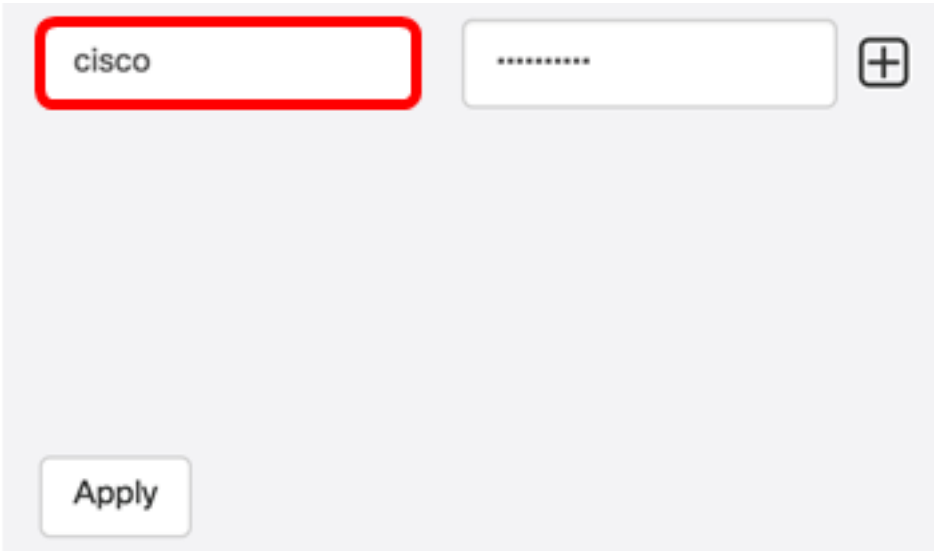
Paso 1. Inicie sesión en la GUI de FindIT Network Probe Administrator y elija **Administration > Device Credentials**.



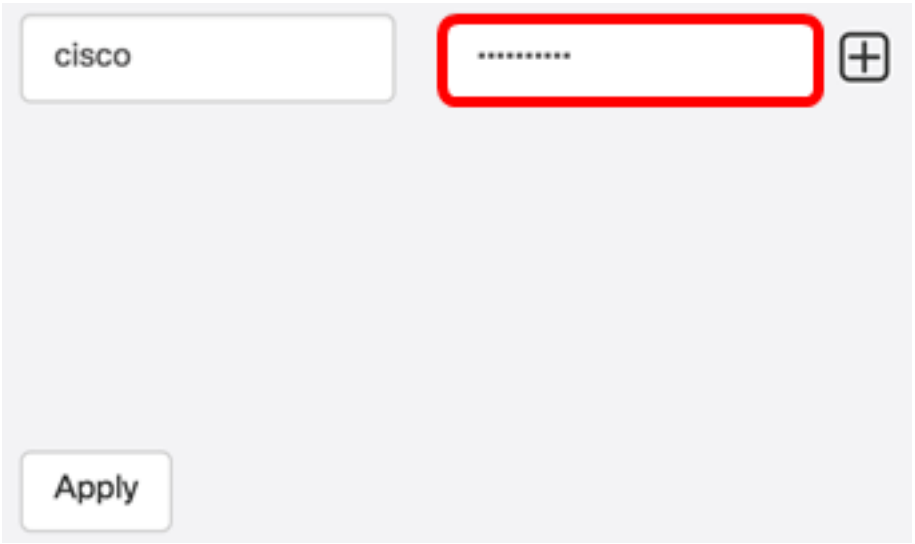
Paso 2. En el área Agregar nuevas credenciales, introduzca un nombre de usuario que se

aplicará a los dispositivos de la red en el campo *Nombre de usuario*. El nombre de usuario y la contraseña predeterminados son cisco.

Nota: En este ejemplo, se utiliza cisco.

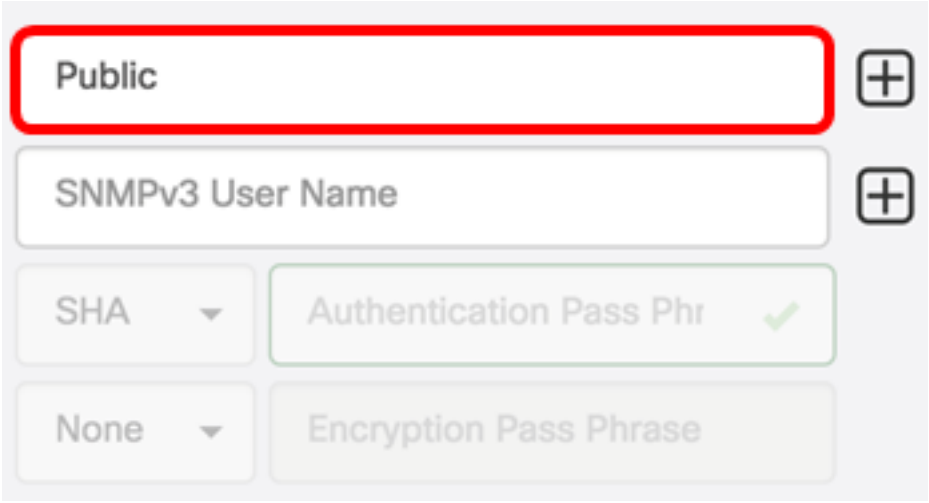


Paso 3. En el campo *password*, ingrese una contraseña.



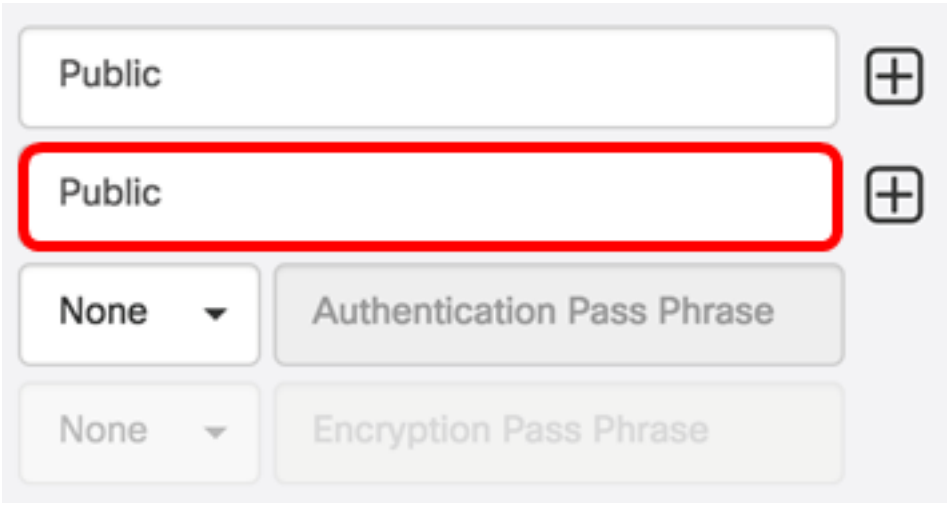
Paso 4. En el campo *Comunidad SNMP*, ingrese el nombre de la comunidad. Es la cadena de comunidad de sólo lectura para autenticar el comando SNMP Get. El nombre de comunidad se utiliza para recuperar la información del dispositivo SNMP. El nombre predeterminado de la comunidad SNMP es Public.

Nota: En este ejemplo, se utiliza Public.



Paso 5. En el campo *SNMPv3 User Name*, ingrese un nombre de usuario que se utilizará en el SNMPv3

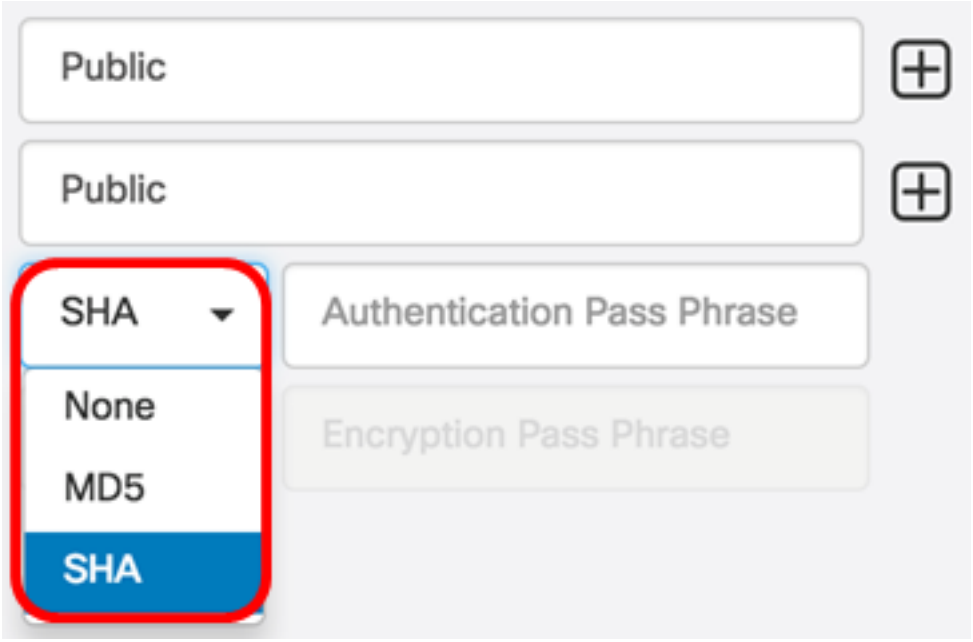
Nota: En este ejemplo, se utiliza Public.



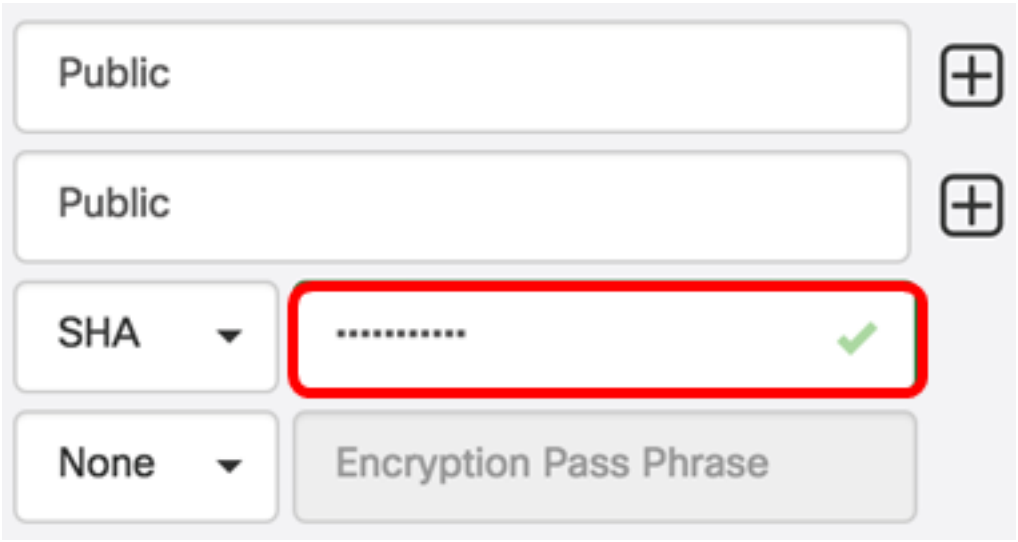
Paso 6. En el menú desplegable Authentication , elija un tipo de autenticación que SNMPv3 utilizará. Las opciones son:

- Ninguno: no se utiliza autenticación de usuario. Este es el valor predeterminado. Si elige esta opción, vaya directamente al Paso 11.
- MD5: utiliza el método de encriptación de 128 bits. El algoritmo MD5 utiliza un criptosistema público para cifrar datos. Si selecciona esta opción, se le solicitará que introduzca una frase de paso de autenticación.
- SHA: el algoritmo hash seguro (SHA) es un algoritmo de hash unidireccional que produce un resumen de 160 bits. SHA calcula más lentamente que MD5, pero es más seguro que MD5. Si selecciona esta opción, se le solicitará que introduzca una frase de paso de autenticación y elija un protocolo de cifrado.

Nota: En este ejemplo, se utiliza SHA.



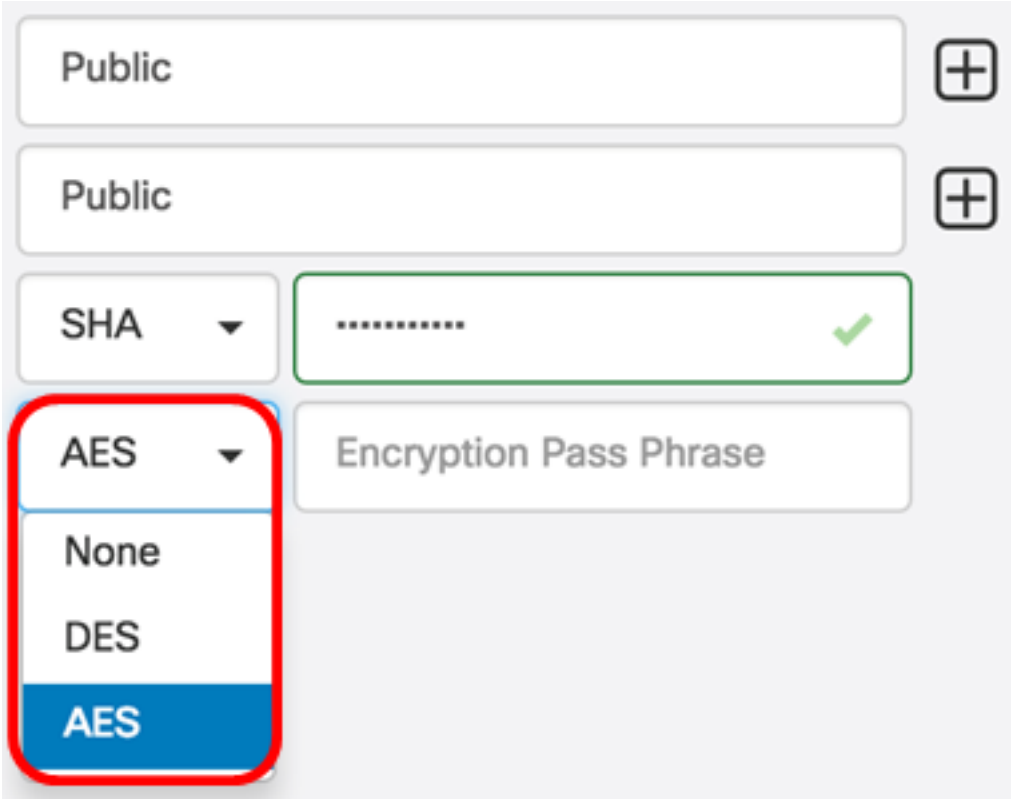
Paso 7. En el campo *Frase de Paso de Autenticación*, ingrese una contraseña para ser utilizada por SNMPv3.



Paso 8. En el menú desplegable Tipo de cifrado, elija un método de cifrado para cifrar las solicitudes SNMPv3. Las opciones son:

- Ninguno: no se requiere ningún método de encriptación.
- DES: el estándar de cifrado de datos (DES) es un cifrado de bloque simétrico que utiliza una clave secreta compartida de 64 bits.
- AES128: Estándar de cifrado avanzado que utiliza una clave de 128 bits.

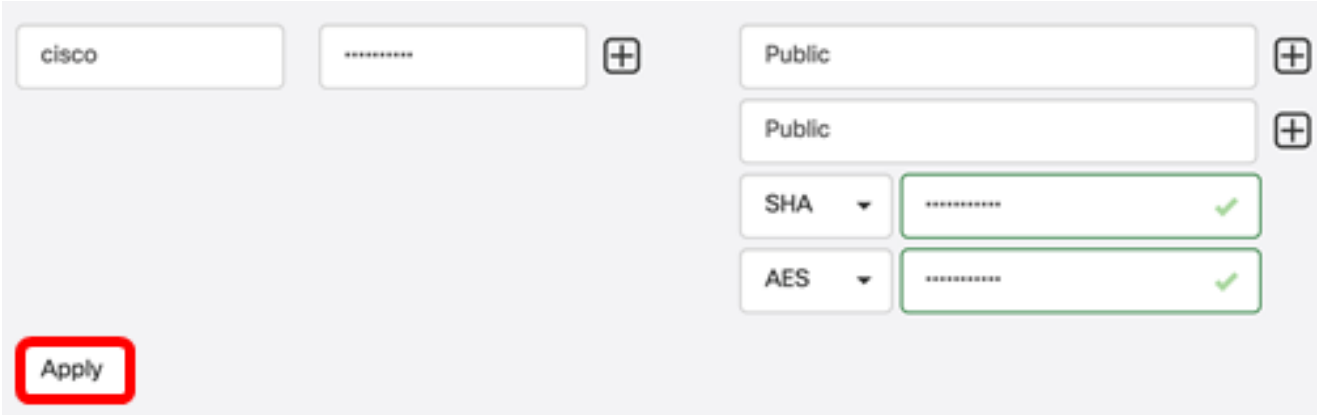
Nota: En este ejemplo, se elige AES.



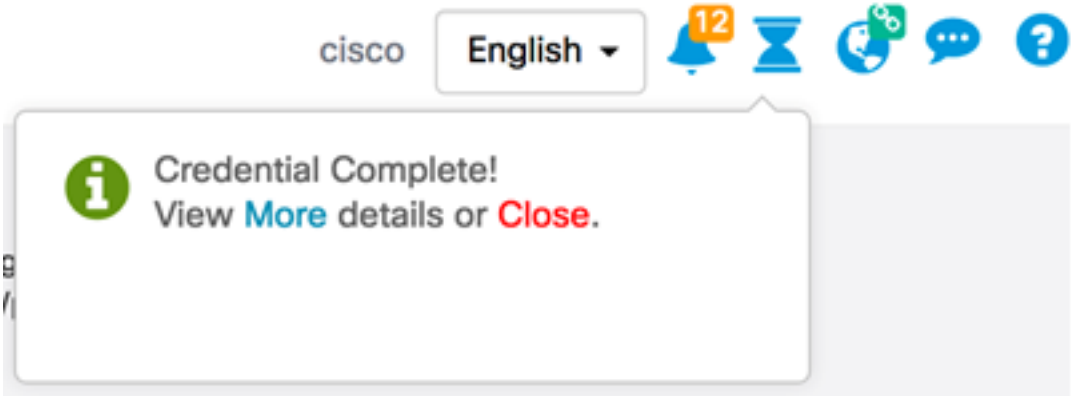
Paso 9. En el campo *Encryption Pass Phrase (Frase de paso de cifrado*), ingrese una clave de 128 bits que SNMP utilizará para el cifrado.

Paso 10. (Opcional) Haga clic en el botón para crear una nueva entrada para el nombre de usuario y el título. Puede agregar hasta una o dos entradas adicionales, dependiendo del tipo de credenciales.

Paso 11. Haga clic en Apply (Aplicar).



Aparecerá una ventana debajo del icono de cristal de hora para informarle de que se han aplicado las configuraciones necesarias.



Ahora debería haber configurado correctamente las credenciales del dispositivo en la sonda de red FindIT.

Ver dispositivos en la red

La tabla siguiente muestra los dispositivos detectados por la sonda de red FindIT de Cisco.

Device	Credential Type	Credential Ok?	Failure Reason
WAP			
wap5e0940	Admin Userid/Password	✓	
wap5e0940	SNMP	✗	SNMP disabled
wampipti	Admin Userid/Password	✓	
wampipti	SNMP	✗	Invalid credential
WAP150	SNMP	✗	Invalid credential
WAP361	Admin Userid/Password	✗	Invalid credential

- Dispositivo: el nombre del dispositivo detectado en la red. Un nombre de dispositivo puede aparecer varias veces dependiendo del tipo de credenciales que se pueden reparar.
- Tipo de credencial: puede ser Admin Userid/Password o SNMP. Esto se utiliza para extraer información del dispositivo.

- ¿Credencial Ok? — Puede aparecer una verificación o una X roja para determinar si las credenciales introducidas en los campos anteriores se aplican o no al dispositivo adecuado. Al hacer clic en la X roja de la lista de dispositivos, aparecerá la configuración para las credenciales del dispositivo.
- Motivo del error: aparece un motivo de error en la columna si un dispositivo no se comunica con la sonda. Los mensajes posibles incluyen "credencial no válida" o "SNMP inhabilitado".

Nota: Se recomienda habilitar SNMP en el dispositivo para que tenga una topología de red más precisa.

Ahora debería haber visto correctamente la identidad de los dispositivos de la red y su tipo de credencial correspondiente.