Configure as credenciais do dispositivo no FindIT Network Probe

Introduction

O Cisco FindIT Network Management fornece ferramentas que ajudam você a monitorar, gerenciar e configurar facilmente seus dispositivos de rede Cisco das séries 100 a 500, como switches, roteadores e pontos de acesso sem fio (WAPs) usando seu navegador da Web. Ele também notifica você sobre notificações de dispositivos e suporte da Cisco, como disponibilidade de novo firmware, status do dispositivo, atualizações de configurações de rede e quaisquer dispositivos conectados da Cisco que não estejam mais na garantia ou cobertos por um contrato de suporte.

FindIT Network Management é um aplicativo distribuído composto de dois componentes ou interfaces separados: um ou mais testes conhecidos como FindIT Network Probe e um único gerente chamado FindIT Network Manager.

Uma instância do FindIT Network Probe instalada em cada local na rede executa a descoberta de rede e se comunica diretamente com cada dispositivo da Cisco. Em uma única rede local, você pode optar por executar uma instância autônoma do FindIT Network Probe. No entanto, se a sua rede for composta de vários locais, você poderá instalar o FindIT Network Manager em um local conveniente e associar cada teste ao gerente. Na interface do gerente, você pode obter uma visão de alto nível do status de todos os sites da sua rede e se conectar à Sonda instalada em um site específico quando desejar exibir informações detalhadas desse site.

Para que a FindIT Network descubra e gerencie completamente a rede, o FindIT Network Probe deve ter credenciais para se autenticar com os dispositivos de rede. Quando um dispositivo é descoberto pela primeira vez, o Probe tentará se autenticar com o dispositivo usando o nome de usuário e a senha padrão e a comunidade SNMP (Simple Network Management Protocol). Se as credenciais do dispositivo tiverem sido alteradas do padrão, será necessário fornecer as credenciais corretas para FindIT. Se essa tentativa falhar, uma mensagem de notificação será gerada e credenciais válidas deverão ser fornecidas pelo usuário.

Objetivo

O objetivo deste documento é mostrar a você como configurar as credenciais do dispositivo no Cisco Network Probe.

Dispositivos aplicáveis

- LocalizarSondaTI

Versão de software

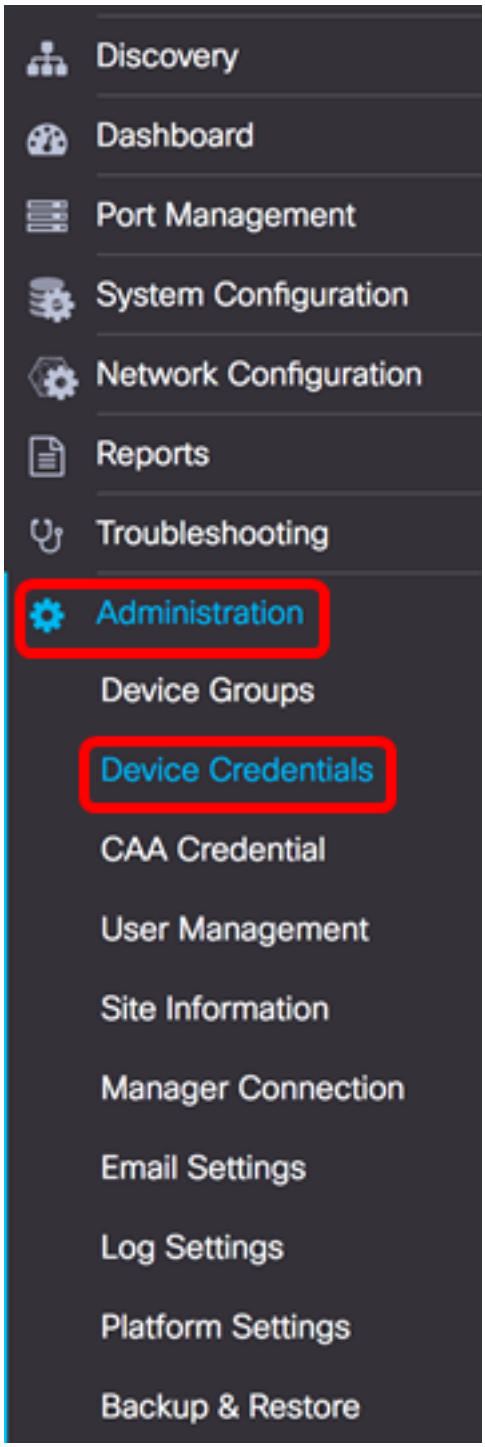
- 1.1

Configurar as credenciais do dispositivo

Adicionar novas credenciais

Insira um ou mais conjuntos de credenciais nos campos abaixo. Quando aplicada, cada credencial será testada em relação a qualquer dispositivo do tipo apropriado para o qual as credenciais de funcionamento não estão disponíveis. Um conjunto de credenciais pode ser uma combinação de nome de usuário/senha, uma comunidade SNMPv2 ou credenciais SNMPv3.

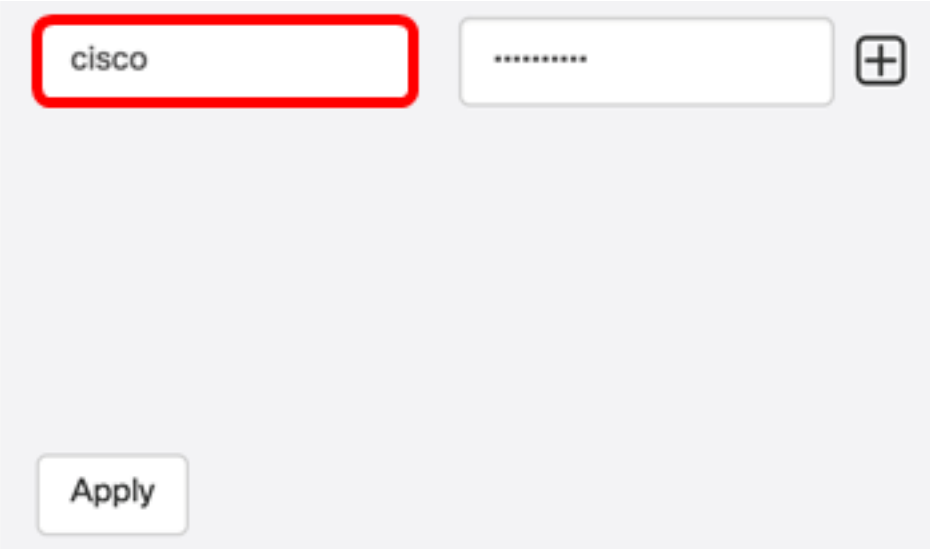
Etapa 1. Faça login na GUI do FindIT Network Probe Administrator e escolha **Administration > Device Credentials**.



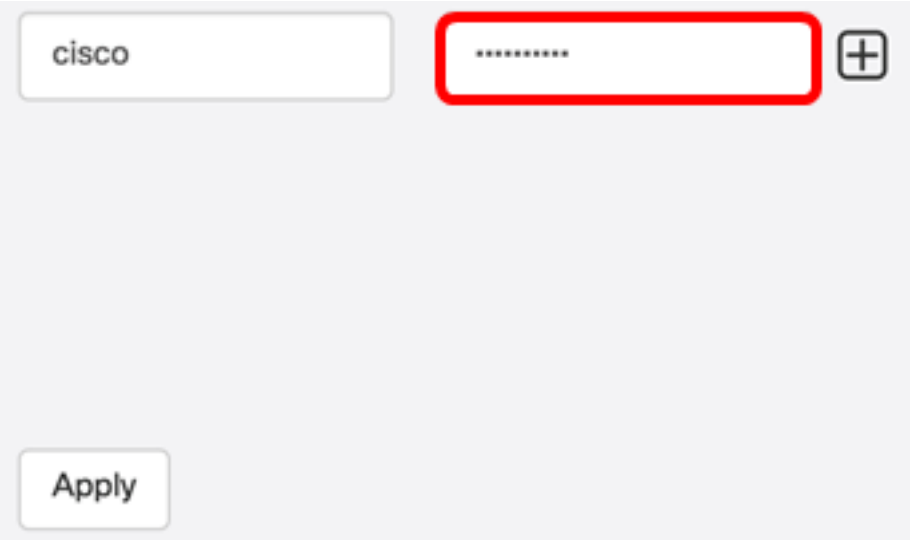
Etapa 2. Na área Adicionar novas credenciais, insira um nome de usuário a ser aplicado aos

dispositivos na rede no campo *Nome de usuário*. O nome do usuário e a senha padrão são cisco.

Note: Neste exemplo, a cisco é usada.

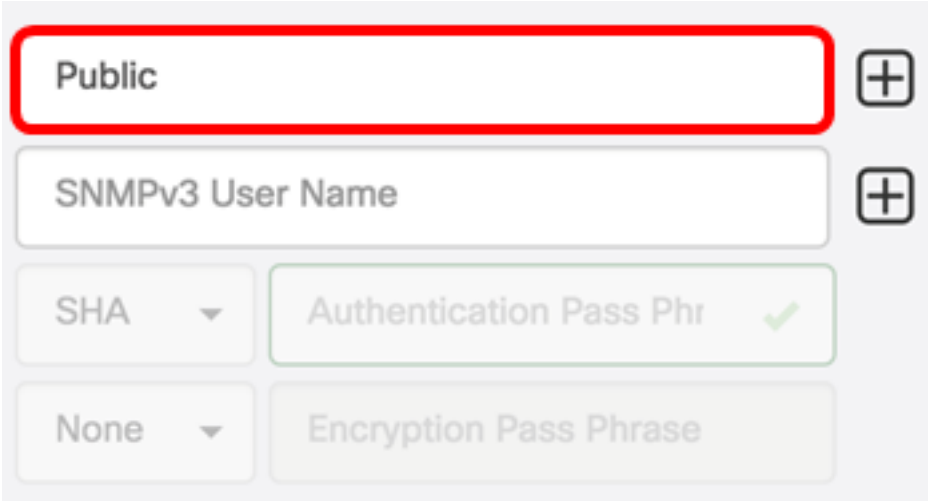


Etapa 3. No campo *password*, digite uma senha.



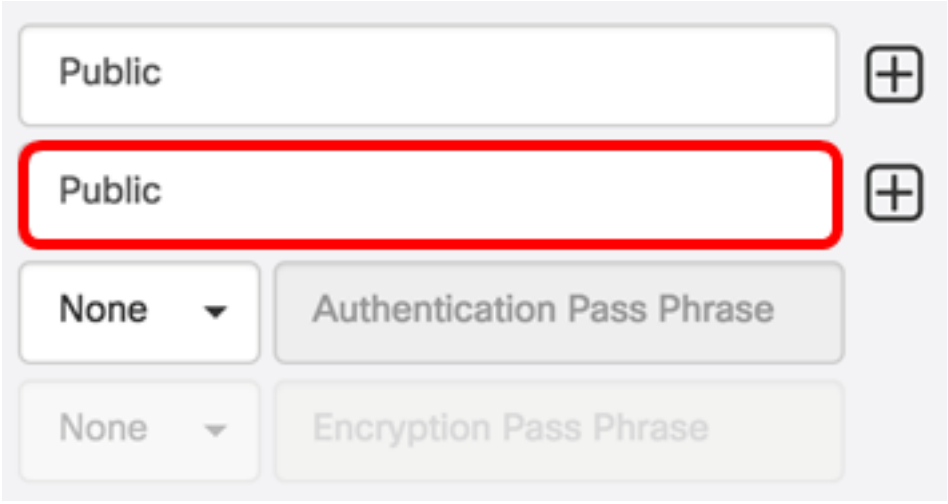
Etapa 4. No campo *SNMP Community*, insira o Community Name. É a string de comunidade somente leitura para autenticar o comando SNMP Get. O nome da comunidade é usado para recuperar as informações do dispositivo SNMP. O nome padrão da comunidade SNMP é Pública.

Note: Neste exemplo, Public é usado.



Etapa 5. No campo *Nome de usuário SNMPv3*, insira um nome de usuário a ser usado no SNMPv3

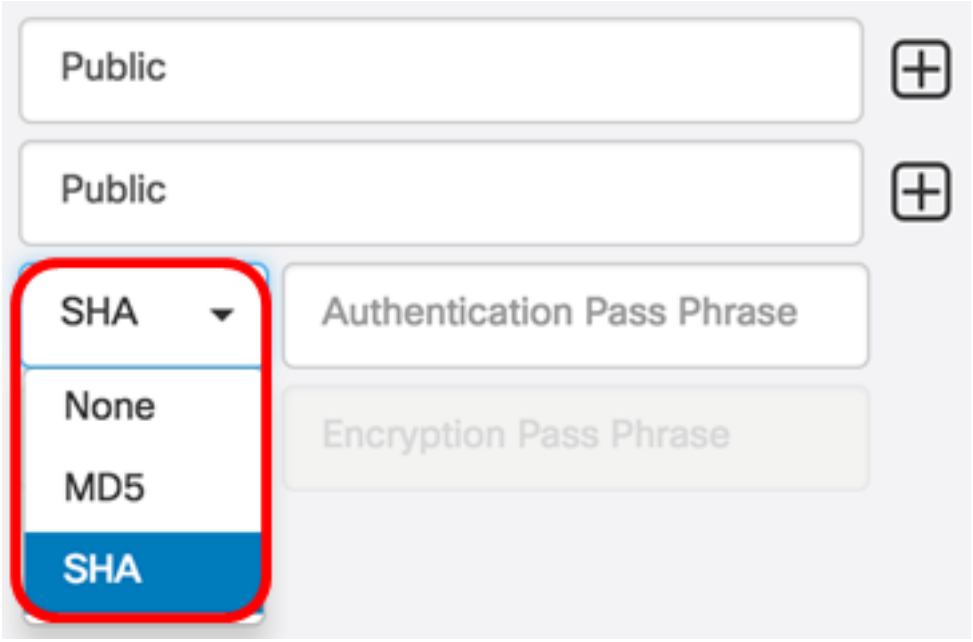
Note: Neste exemplo, Public é usado.



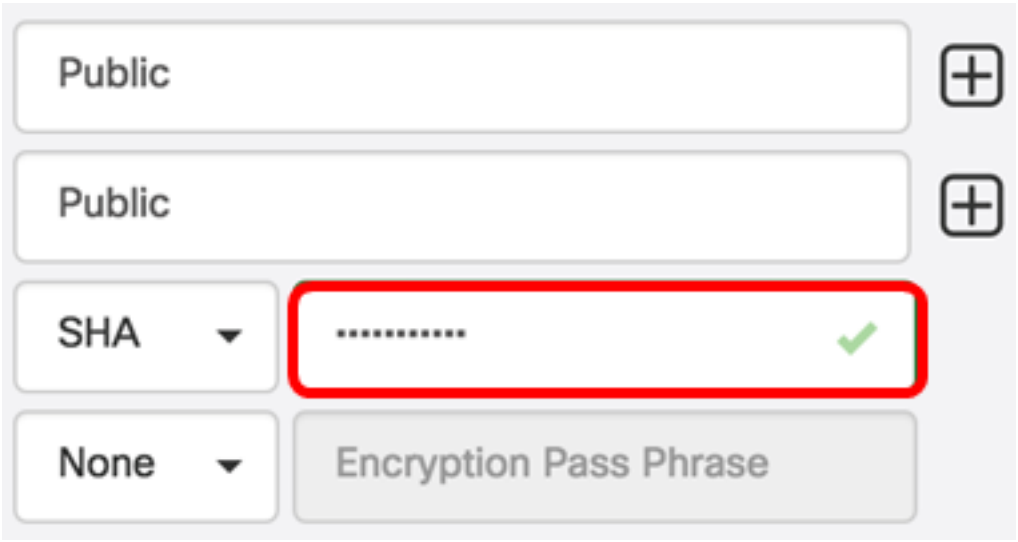
Etapa 6. No menu suspenso Authentication (Autenticação), escolha um tipo de autenticação que SNMPv3 usará. As opções são:

- Nenhum — Nenhuma autenticação de usuário é usada. Esse é o padrão. Se você escolher essa opção, vá para a Etapa 11.
- MD5 — Usa o método de criptografia de 128 bits. O algoritmo MD5 usa um sistema de criptografia público para criptografar dados. Se esta opção for selecionada, será necessário inserir uma frase de senha de autenticação.
- SHA — O Secure Hash Algorithm (SHA) é um algoritmo de hash unidirecional que produz um resumo de 160 bits. O SHA computa mais lentamente que o MD5, mas é mais seguro que o MD5. Se esta opção for selecionada, você precisará inserir uma frase de senha de autenticação e escolher um protocolo de criptografia.

Note: Neste exemplo, SHA é usado.



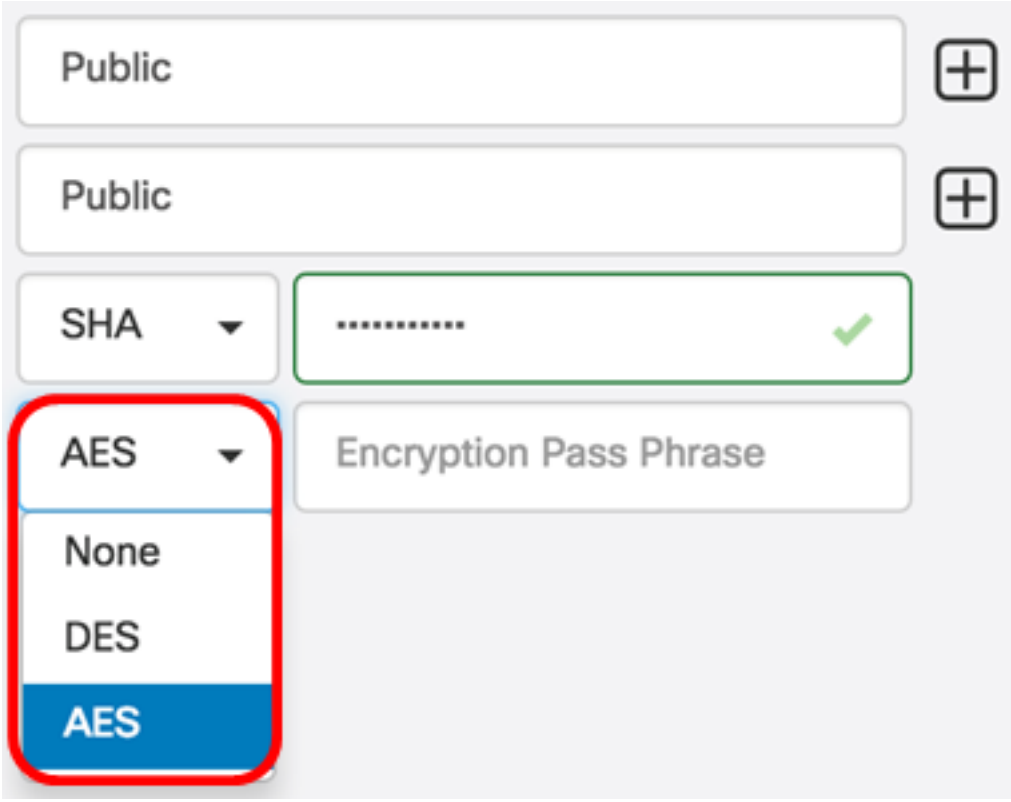
Passo 7. No campo *Authentication Pass Phrase*, insira uma senha a ser usada por SNMPv3.



Etapa 8. No menu suspenso Tipo de criptografia, escolha um método de criptografia para criptografar as solicitações SNMPv3. As opções são:

- Nenhum — Nenhum método de criptografia é necessário.
- DES — Data Encryption Standard (DES) é uma cifra de bloco simétrica que usa uma chave secreta compartilhada de 64 bits.
- AES128 — Advanced Encryption Standard que usa uma chave de 128 bits.

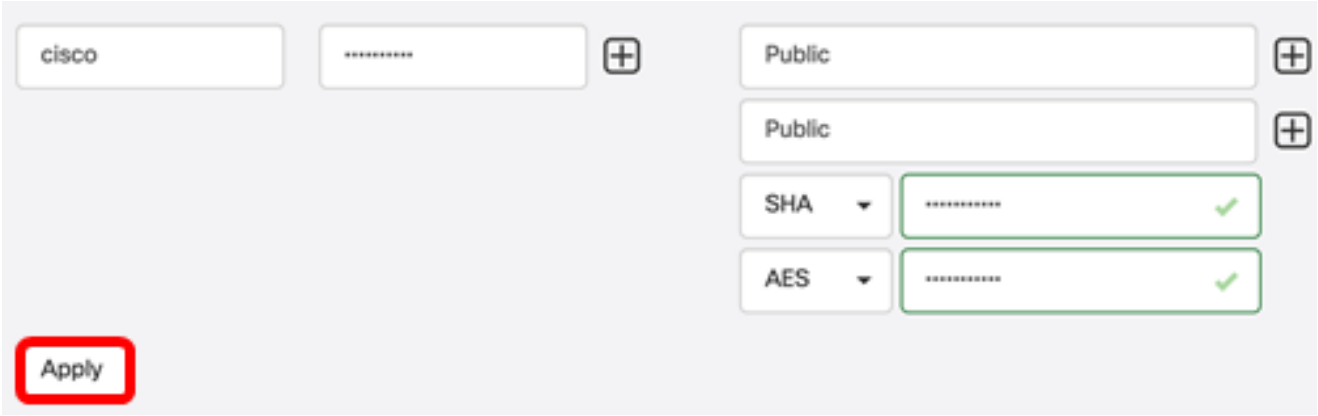
Note: Neste exemplo, AES é escolhido.



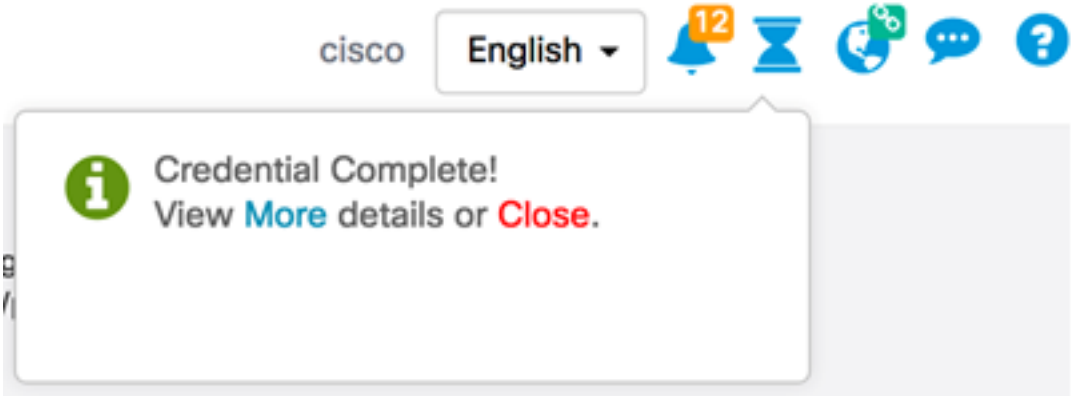
Etapa 9. No campo *Encryption Pass Phrase*, insira uma chave de 128 bits a ser usada pelo SNMP para criptografia.

Etapa 10. (Opcional) Clique no botão para criar uma nova entrada para o nome de usuário e título. Você pode adicionar até uma ou duas entradas adicionais, dependendo do tipo de credenciais.

Etapa 11. Clique em Apply.



Uma janela será exibida abaixo do ícone de vidro de hora para informá-lo de que as configurações necessárias foram aplicadas.



Agora você deve ter configurado com êxito as credenciais do dispositivo no FindIT Network Probe.

Exibir dispositivos na rede

A Tabela abaixo exibe os dispositivos descobertos pelo Cisco FindIT Network Probe.

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 - O nome do dispositivo descoberto na rede. O nome de um dispositivo pode aparecer várias vezes, dependendo do tipo de credenciais operacionais.
- Tipo de credencial — Pode ser ID de usuário/senha do administrador ou SNMP. Isso é usado para extrair informações do dispositivo.
- Credencial Ok? — Uma verificação ou um X vermelho pode aparecer para determinar

se as credenciais inseridas nos campos acima foram aplicadas ao dispositivo apropriado. Clicar no X vermelho na lista de dispositivos ativará a configuração das credenciais do dispositivo.
- Razão da falha — Um motivo da falha aparece na coluna se um dispositivo não conseguir se comunicar com a sonda. As mensagens possíveis incluem "Credencial inválida" ou "SNMP desabilitado".

Note: Recomenda-se habilitar o SNMP no dispositivo para ter uma topologia de rede mais precisa.

Agora você deve ter visualizado com êxito a identidade dos dispositivos na rede e o tipo de credencial correspondente.