Configure the Device Credentials on the FindIT Network Probe

Introduction

The Cisco FindIT Network Management provides tools that help you easily monitor, manage, and configure your Cisco 100 to 500 Series network devices such as switches, routers, and wireless access points (WAPs) using your web browser. It also notifies you about device and Cisco Support notifications such as the availability of new firmware, device status, network settings updates, and any connected Cisco-devices that are no longer under warranty or covered by a support contract.

FindIT Network Management is a distributed application which is comprised of two separate components or interfaces: one or more Probes referred to as FindIT Network Probe and a single Manager called FindIT Network Manager.

An instance of FindIT Network Probe installed at each site in the network performs network discovery, and communicates directly with each Cisco device. In a single site network, you may choose to run a standalone instance of FindIT Network Probe. However, if your network is composed of multiple sites, you may install FindIT Network Manager at a convenient location and associate each Probe with the Manager. From the Manager interface, you can get a high-level view of the status of all the sites in your network, and connect to the Probe installed at a particular site when you wish to view a detailed information for that site.

For FindIT Network to fully discover and manage the network, the FindIT Network Probe must have credentials to authenticate with the network devices. When a device is first discovered, the Probe will attempt to authenticate with the device using the default username and password and Simple Network Management Protocol (SNMP community. If the device credentials have been changed from the default, then it will be necessary for you to supply correct credentials to FindIT. If this attempt fails, a notification message will be generated and valid credentials must be supplied by the user.

Objective

The objective of this document is to show you how to configure the Device Credentials on the Cisco Network Probe.

Applicable Devices

- FindIT Probe

Software Version

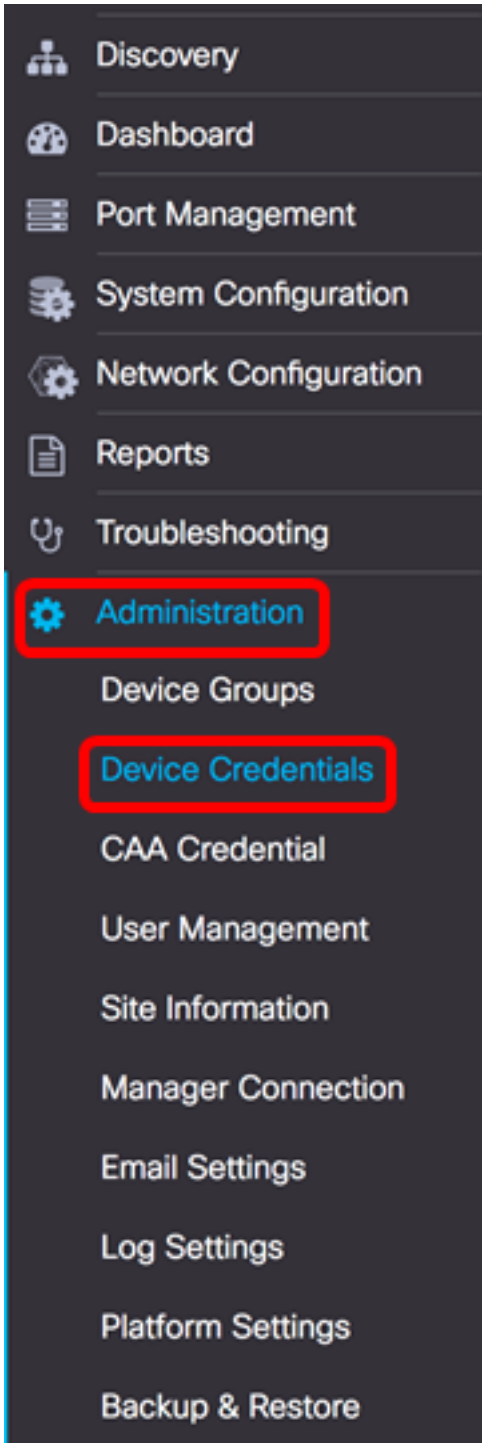
- 1.1

Configure the Device Credentials

Add New Credentials

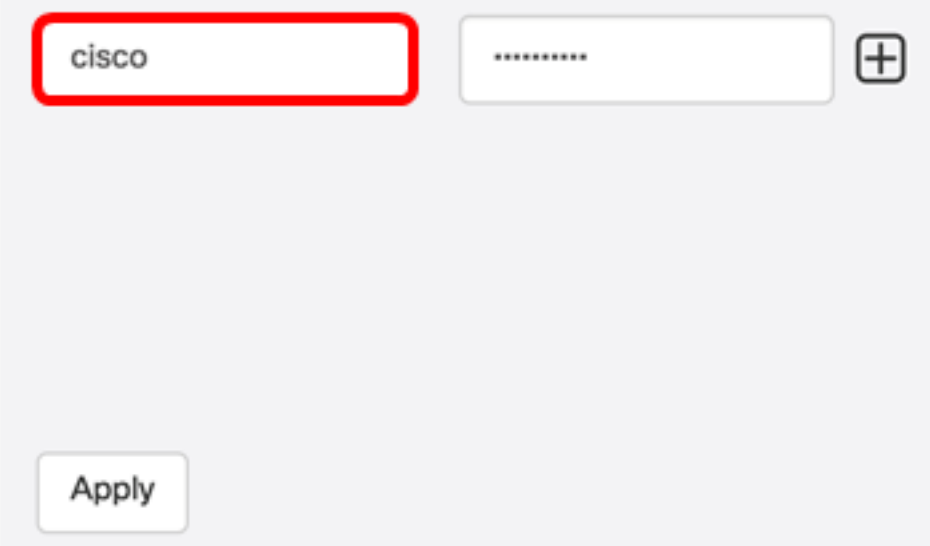
Enter one or more sets of credentials in the fields below. When applied, each credential will be tested against any devices of the appropriate type for which working credentials are not available. A set of credentials may be either a username/password combination, an SNMPv2 community or SNMPv3 credentials.

Step 1. Log in to the FindIT Network Probe Administrator GUI and choose **Administration > Device Credentials**.

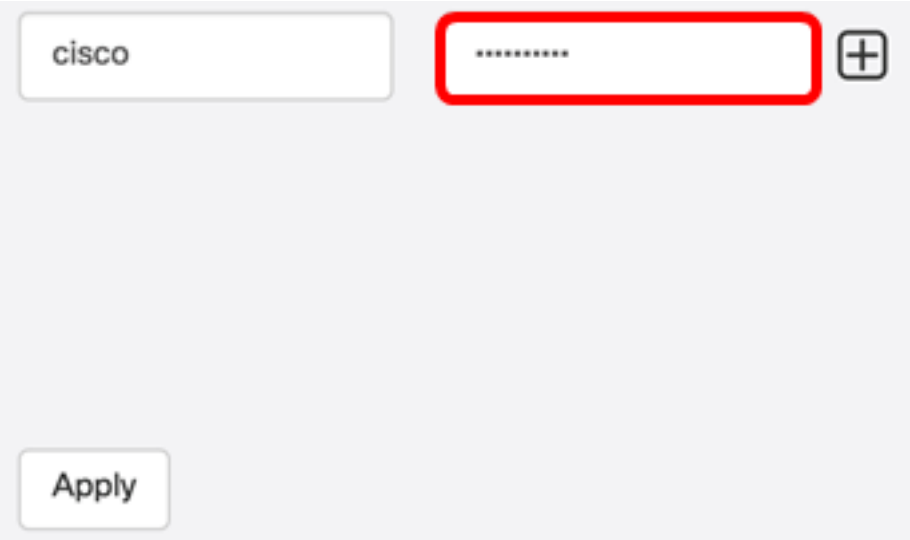


Step 2. In the Add New Credentials area, enter a user name to be applied to the devices in the network in the *Username* field. The default username and password is cisco.

Note: In this example, cisco is used.

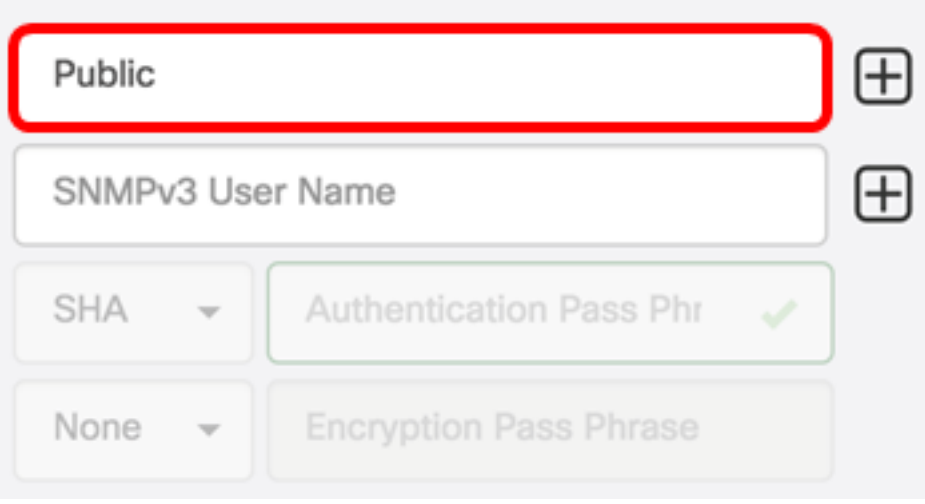


Step 3. In the *password* field, enter a password.



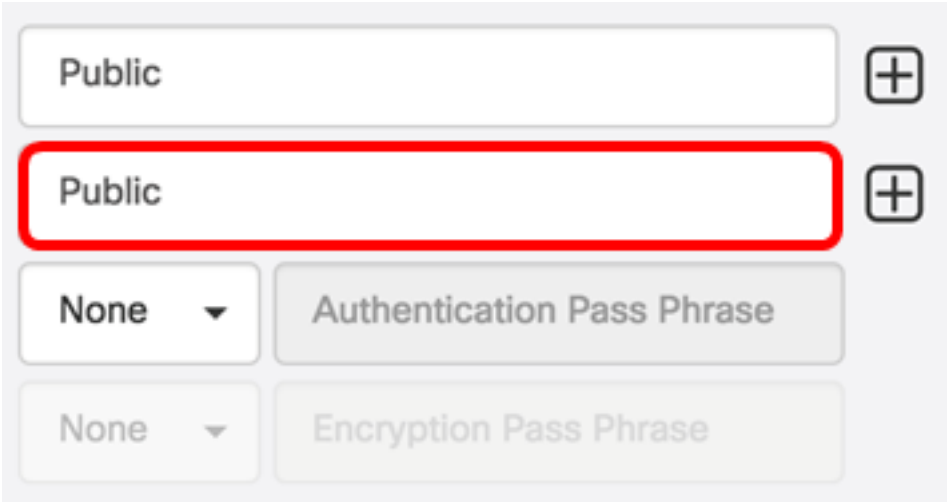
Step 4. In the *SNMP Community* field, enter the Community Name. It is the read only community string to authenticate the SNMP Get command. The Community Name is used to retrieve the information from the SNMP device. The default SNMP Community name is Public.

Note: In this example, Public is used.



Step 5. In the *SNMPv3 User Name* field, enter a user name to be used in the SNMPv3

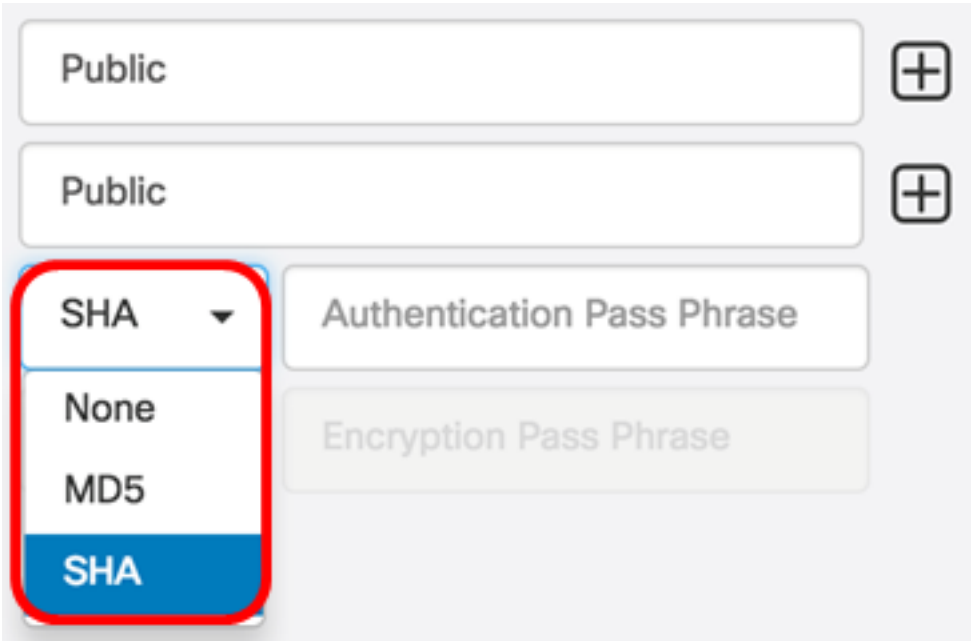
Note: In this example, Public is used.



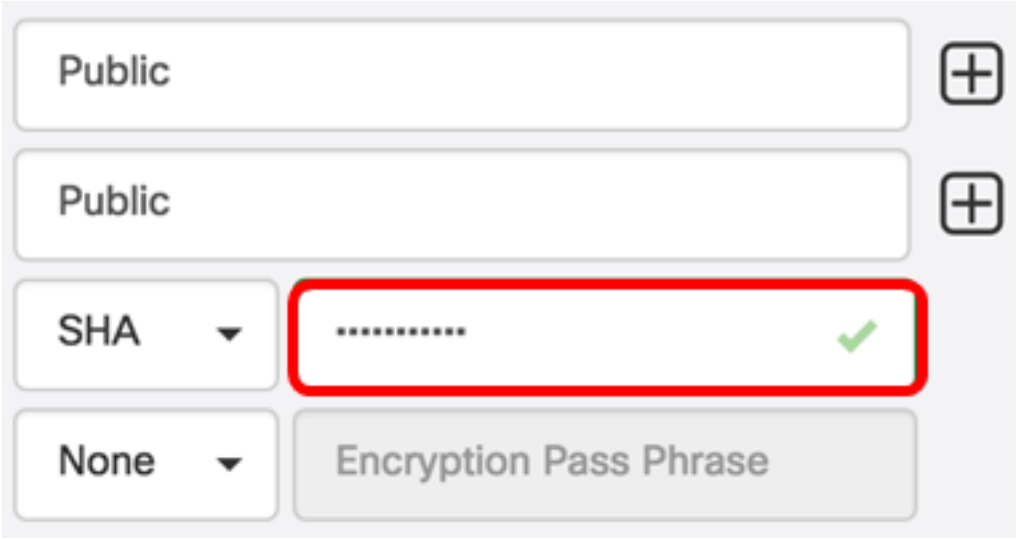
Step 6. From the Authentication drop-down menu, choose an authentication type that SNMPv3 will use. The options are:

- None — No user authentication is used. This is the default. If you choose this option, skip to Step 11.
- MD5 — Uses 128-bit encryption method. The MD5 algorithm uses a public cryptosystem to encrypt data. If this is chosen, you will be required to enter an Authentication Pass Phrase.
- SHA — Secure Hash Algorithm (SHA) is a one-way hashing algorithm that produces a 160-bit digest. SHA computes slower than MD5, but is more secure than MD5. If this is chosen, you will be required to enter an Authentication Pass Phrase and choose an encryption protocol.

Note: In this example, SHA is used.



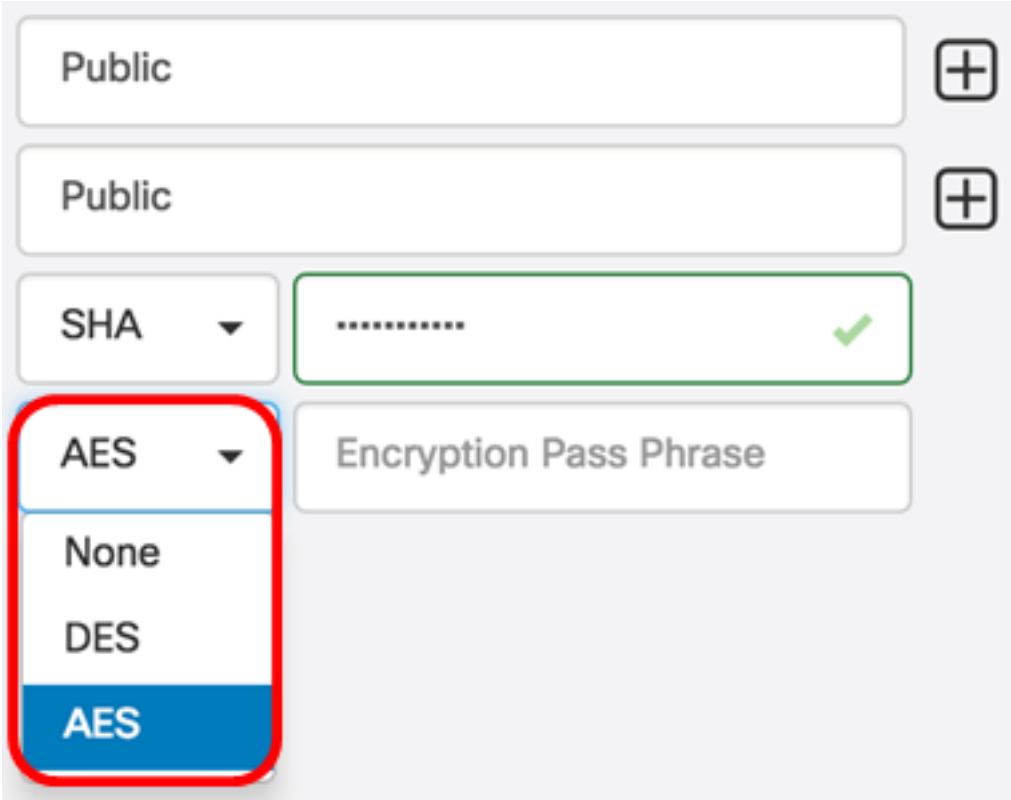
Step 7. In the *Authentication Pass Phrase* field, enter a password to be used by SNMPv3.



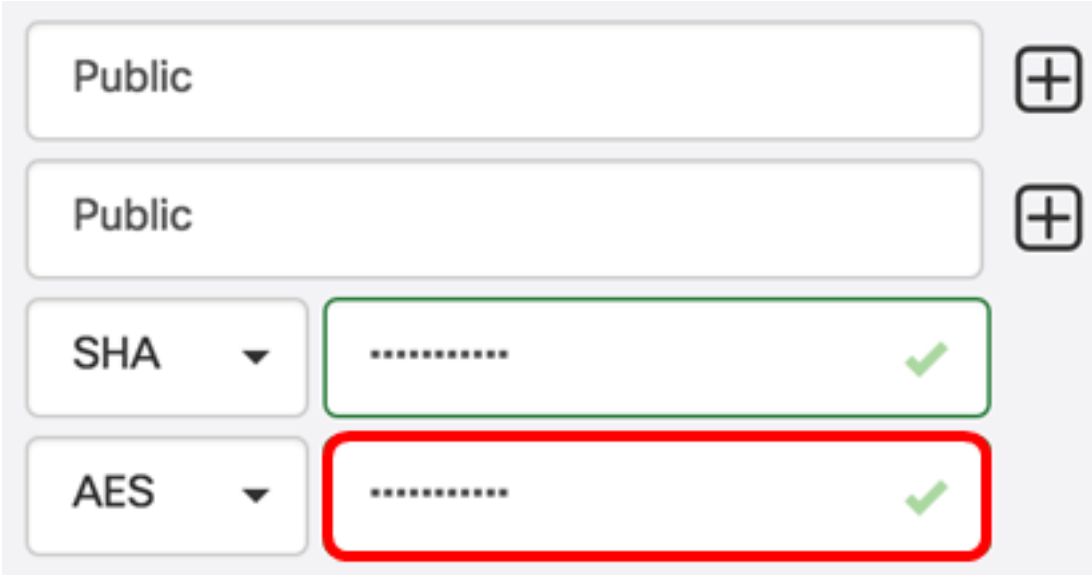
Step 8. From the Encryption Type drop-down menu, choose an encryption method to encrypt the SNMPv3 requests. The options are:

- None — No encryption method is required.
- DES — Data Encryption Standard (DES) is a symmetric block cipher that uses a 64-bit shared secret key.
- AES128 — Advanced Encryption Standard that uses a 128-bit key.

Note: In this example, AES is chosen.

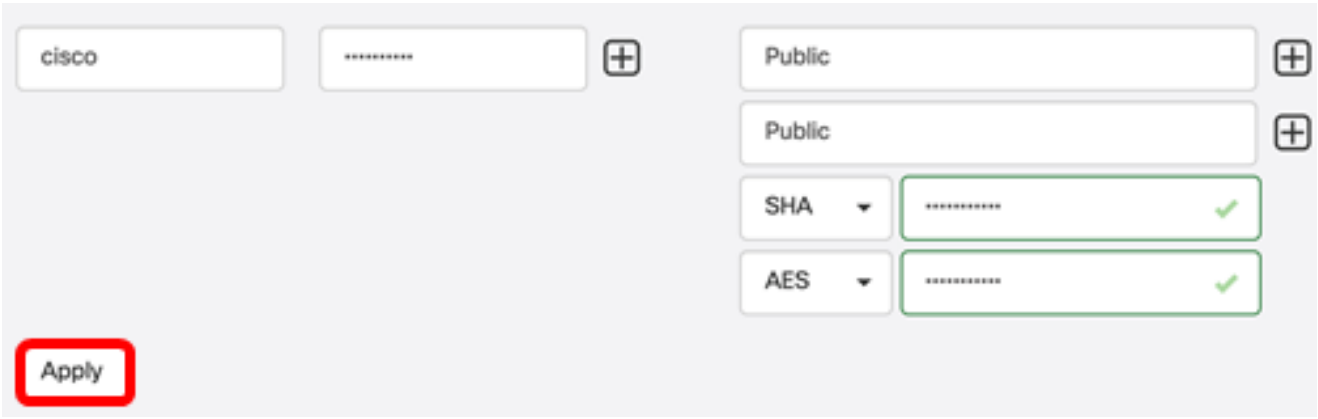


Step 9. In the *Encryption Pass Phrase* field, enter a 128-bit key to be used by SNMP for encryption.

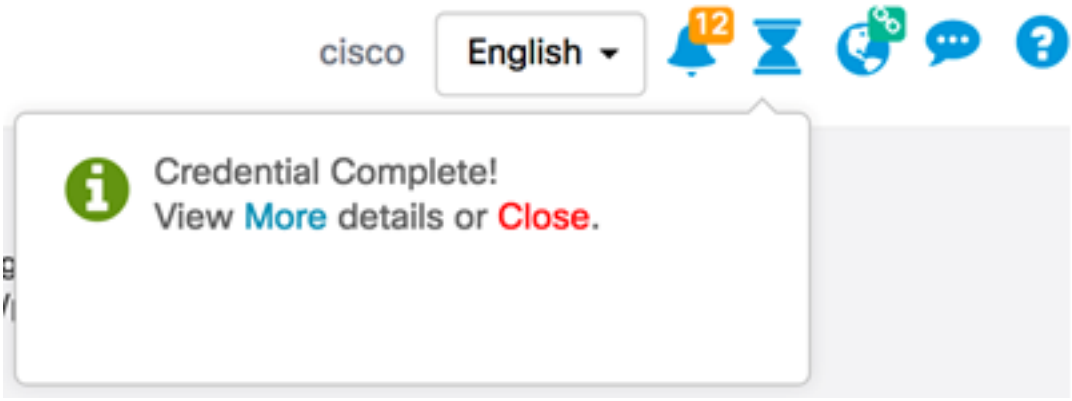


Step 10. (Optional) Click the button to create a new entry for the username and title. You can add up to one or two additional entries, depending on the type of credentials.

Step 11. Click **Apply**.



A window will appear beneath the hour glass icon to inform you that the necessary configurations have been applied.



You should now have successfully configured the Device Credentials on the FindIT Network Probe.

View Devices on the Network

The Table below displays the devices discovered by 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

- Device — The name of the device discovered on the network. A device name may appear multiple times depending on the type of credentials serviceable.
- Credential Type — This may either be Admin Userid/Password or SNMP. This is used to pull information from the device.
- Credential Ok? — A check or a red X may appear to determine whether or not the credentials entered in the fields above applied to the proper device. Clicking on the red X on the device list will bring up the configuration for the device credentials.
- Failure Reason — A reason of failure appears in the column if a device fails to communicate with the Probe. Possible messages include “Invalid credential” or “SNMP disabled”.

Note: It is recommended to enable SNMP on the device to have a more accurate network topology.

You should now have successfully viewed the identity of the devices on the network and its corresponding credential type.