Configurer les informations d'identification du périphérique sur la sonde FindIT Network

Introduction

Cisco FindIT Network Management fournit des outils qui vous aident à surveiller, gérer et configurer facilement vos périphériques réseau de la gamme Cisco 100 à 500, tels que les commutateurs, les routeurs et les points d'accès sans fil (WAP), à l'aide de votre navigateur Web. Il vous informe également des notifications relatives aux périphériques et à l'assistance Cisco, telles que la disponibilité du nouveau micrologiciel, l'état des périphériques, les mises à jour des paramètres réseau et tous les périphériques Cisco connectés qui ne sont plus couverts par la garantie ou par un contrat d'assistance.

FindIT Network Management est une application distribuée qui comprend deux composants ou interfaces distincts : un ou plusieurs sondes appelées FindIT Network Probe et un seul gestionnaire appelé FindIT Network Manager.

Une instance de FindIT Network Probe installée sur chaque site du réseau effectue la détection du réseau et communique directement avec chaque périphérique Cisco. Dans un réseau de site unique, vous pouvez choisir d'exécuter une instance autonome de FindIT Network Probe. Cependant, si votre réseau est composé de plusieurs sites, vous pouvez installer FindIT Network Manager à un emplacement pratique et associer chaque sonde au gestionnaire. À partir de l'interface Manager, vous pouvez obtenir une vue de haut niveau de l'état de tous les sites de votre réseau et vous connecter à la sonde installée sur un site particulier lorsque vous souhaitez afficher des informations détaillées pour ce site.

Pour que FindIT Network puisse découvrir et gérer pleinement le réseau, FindIT Network Probe doit disposer d'informations d'identification pour s'authentifier auprès des périphériques réseau. Lorsqu'un périphérique est découvert pour la première fois, la sonde tente de s'authentifier auprès du périphérique à l'aide du nom d'utilisateur et du mot de passe par défaut et de la communauté SNMP (Simple Network Management Protocol). Si les informations d'identification du périphérique ont été modifiées par défaut, vous devez fournir les informations d'identification correctes à FindIT. Si cette tentative échoue, un message de notification est généré et des informations d'identification valides doivent être fournies par l'utilisateur.

Objectif

L'objectif de ce document est de vous montrer comment configurer les informations d'identification des périphériques sur la sonde de réseau Cisco.

Périphériques pertinents

- RechercheIT

Version du logiciel

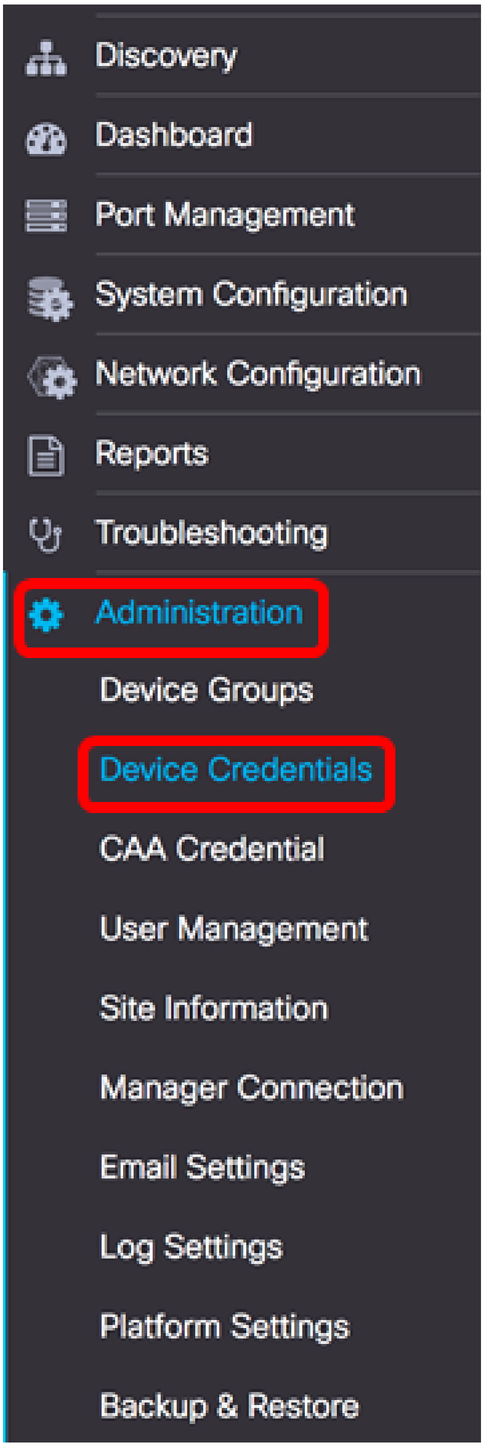
- 1.1

Configurer les informations d'identification du périphérique

Ajouter de nouvelles informations d'identification

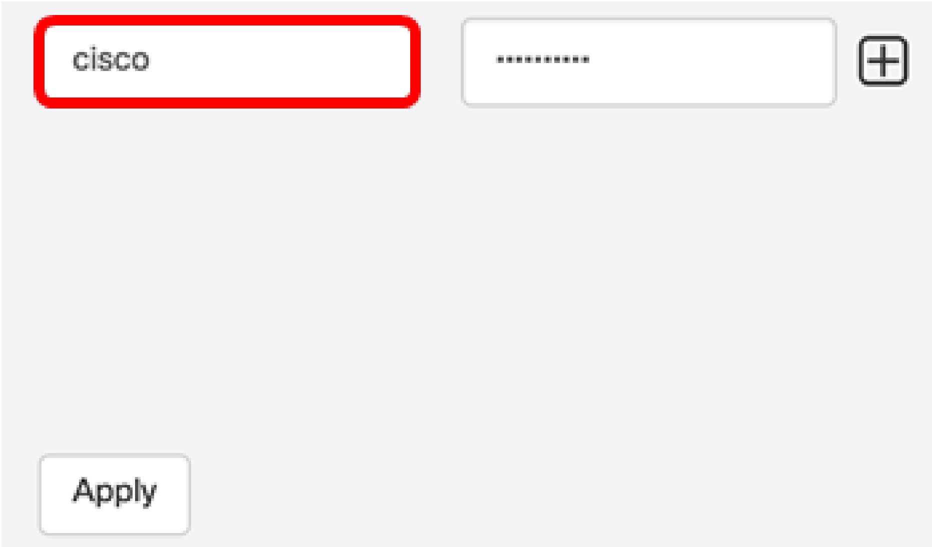
Entrez un ou plusieurs jeux d'informations d'identification dans les champs ci-dessous. Lorsqu'elles sont appliquées, chaque information d'identification est testée sur les périphériques du type approprié pour lesquels les informations d'identification de travail ne sont pas disponibles. Un jeu d'informations d'identification peut être une combinaison nom d'utilisateur/mot de passe, une communauté SNMPv2 ou des informations d'identification SNMPv3.

Étape 1. Connectez-vous à l'interface utilisateur de FindIT Network Probe Administrator et sélectionnez **Administration > Device Credential**.

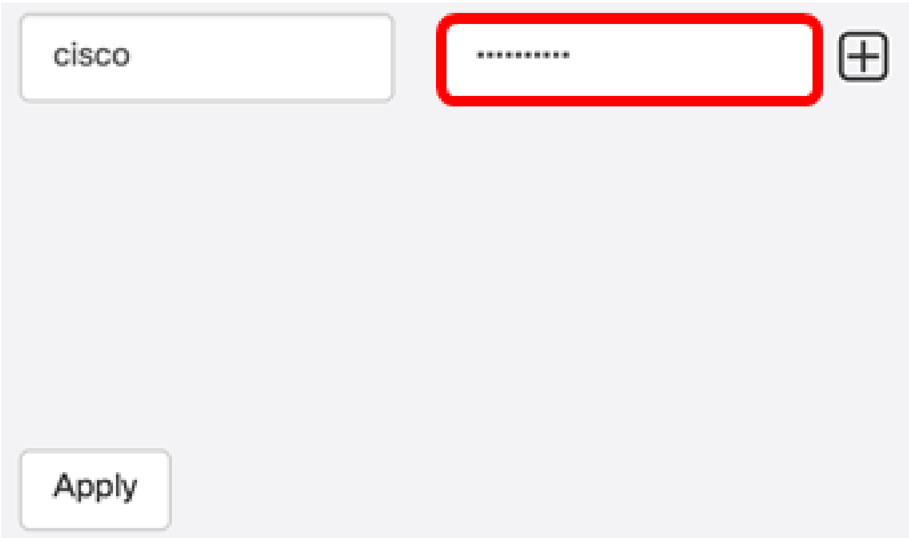


Étape 2. Dans la zone Ajouter de nouvelles informations d'identification, saisissez un nom d'utilisateur à appliquer aux périphériques du réseau dans le champ *Nom d'utilisateur*. Le nom d'utilisateur et le mot de passe par défaut sont cisco.

Note: Dans cet exemple, cisco est utilisé.

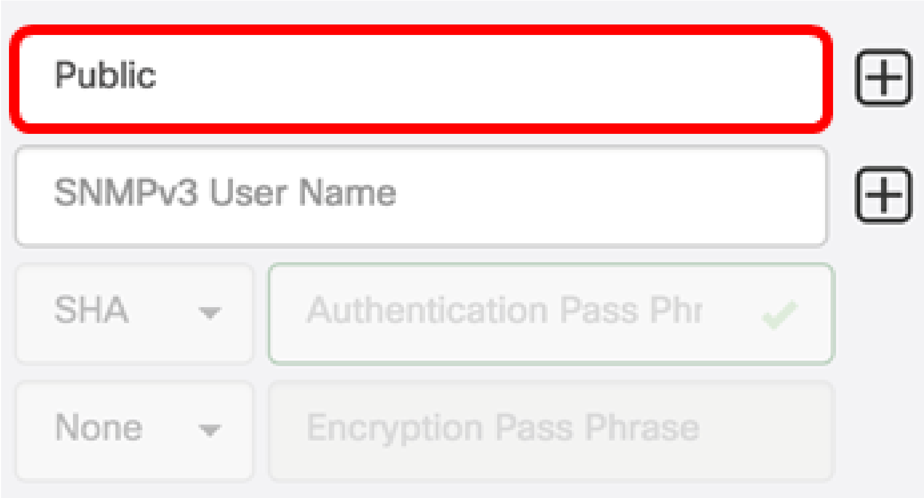


Étape 3. Dans le champ *mot de passe*, saisissez un mot de passe.



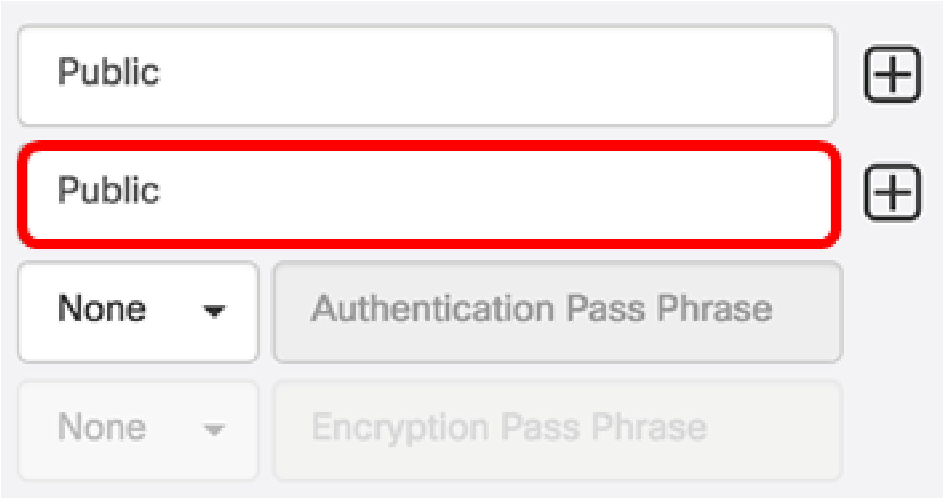
Étape 4. Dans le champ *Communauté SNMP*, saisissez le nom de la communauté. Il s'agit de la chaîne de communauté en lecture seule pour authentifier la commande SNMP Get. Le nom de communauté est utilisé pour récupérer les informations à partir du périphérique SNMP. Le nom de communauté SNMP par défaut est Public.

Note: Dans cet exemple, Public est utilisé.



Étape 5. Dans le champ *Nom d'utilisateur SNMPv3*, saisissez un nom d'utilisateur à utiliser dans SNMPv3

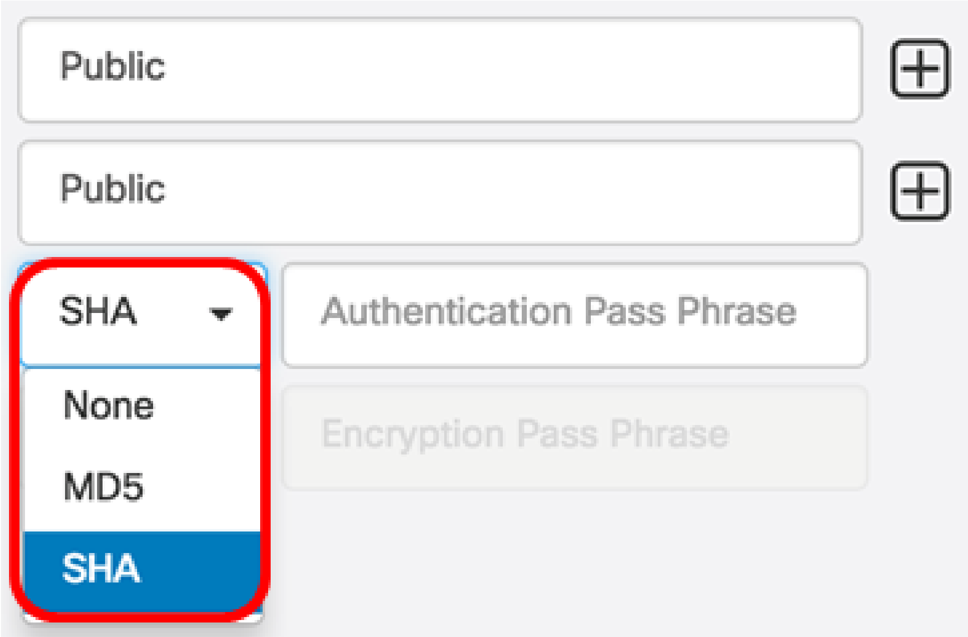
Note: Dans cet exemple, Public est utilisé.



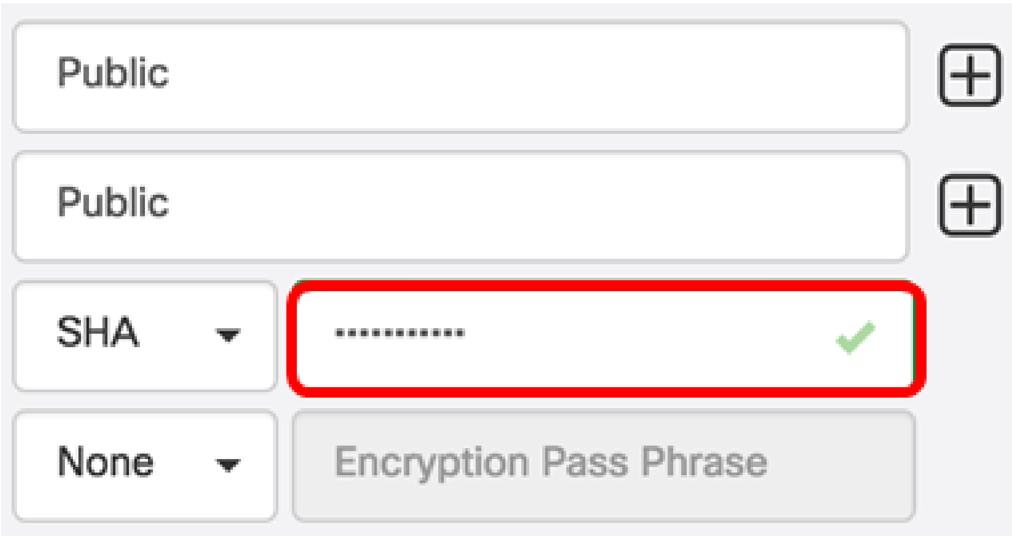
Étape 6. Dans le menu déroulant Authentication, sélectionnez un type d'authentification que SNMPv3 utilisera. Les options sont les suivantes :

- Aucun : aucune authentification utilisateur n'est utilisée. Il s'agit de la configuration par défaut. Si vous choisissez cette option, passez à l'étape 11.
- MD5 : utilise une méthode de cryptage 128 bits. L'algorithme MD5 utilise un système de chiffrement public pour chiffrer les données. Si cette option est sélectionnée, vous devrez saisir une phrase d'authentification.
- SHA : SHA (Secure Hash Algorithm) est un algorithme de hachage unidirectionnel qui produit un résumé de 160 bits. SHA calcule plus lentement que MD5, mais est plus sécurisé que MD5. Si cette option est sélectionnée, vous devrez entrer une phrase d'authentification et choisir un protocole de chiffrement.

Note: Dans cet exemple, SHA est utilisé.



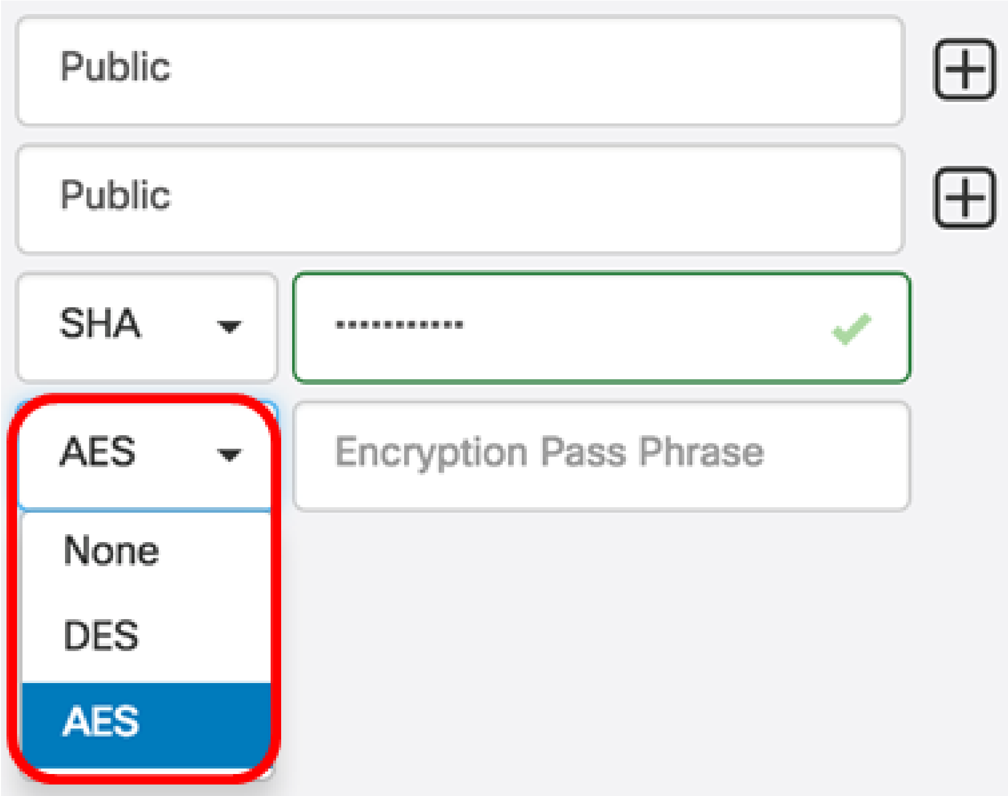
Étape 7. Dans le champ *Authentication Pass Phrase*, saisissez un mot de passe à utiliser par SNMPv3.



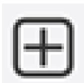
Étape 8. Dans le menu déroulant Encryption Type, sélectionnez une méthode de cryptage pour chiffrer les requêtes SNMPv3. Les options sont les suivantes :

- Aucun : aucune méthode de chiffrement n'est requise.
- DES : Data Encryption Standard (DES) est un chiffrement de bloc symétrique qui utilise une clé secrète partagée de 64 bits.
- AES128 - Advanced Encryption Standard qui utilise une clé de 128 bits.

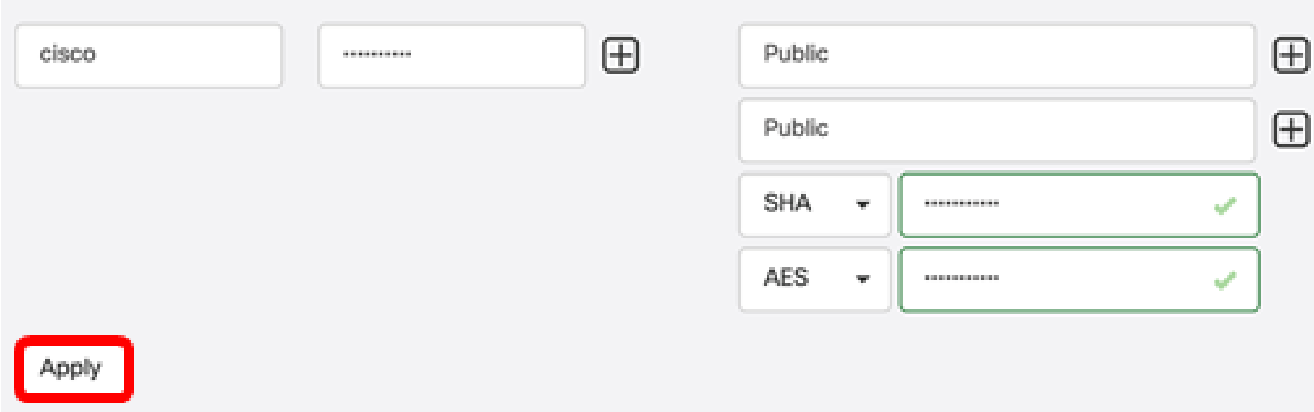
Note: Dans cet exemple, AES est sélectionné.



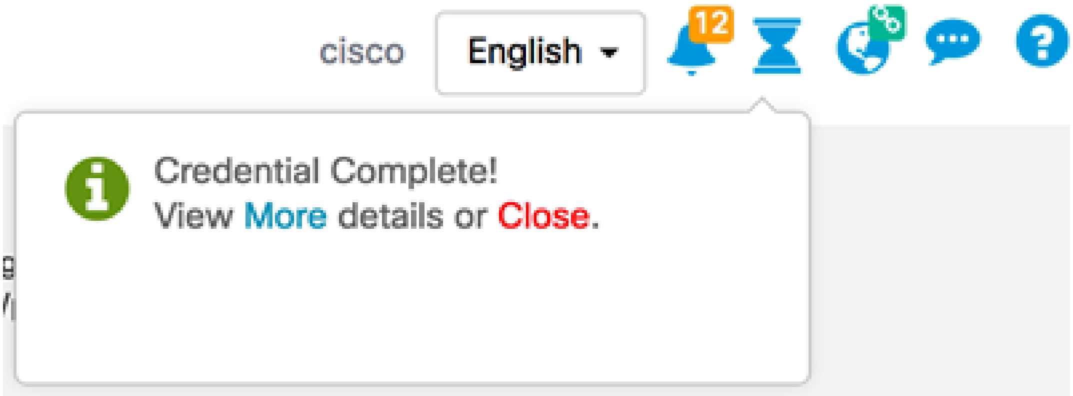
Étape 9. Dans le champ *Encryption Pass Phrase*, saisissez une clé de 128 bits à utiliser par SNMP pour le chiffrement.

Étape 10. (Facultatif) Cliquez sur le  bouton pour créer une nouvelle entrée pour le nom d'utilisateur et le titre. Vous pouvez ajouter jusqu'à une ou deux entrées supplémentaires, selon le type d'informations d'identification.

Étape 11. Cliquez sur Apply.



Une fenêtre s'affiche sous l'icône de la vitre de l'heure pour vous informer que les configurations nécessaires ont été appliquées.



Vous devez maintenant avoir correctement configuré les informations d'identification de périphérique sur la sonde FindIT Network.

Affichage des périphériques sur le réseau

Le tableau ci-dessous présente les périphériques détectés par 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 : nom du périphérique détecté sur le réseau. Un nom de périphérique peut apparaître plusieurs fois en fonction du type d'informations d'identification pouvant être réparées.
- Credential Type : il peut s'agir de Admin Userid/Password ou SNMP. Cette option permet d'extraire des informations du périphérique.

- Informations d'identification OK ? — Une coche ou un X rouge peut apparaître pour déterminer si les informations d'identification entrées dans les champs ci-dessus s'appliquent au périphérique approprié. Cliquez sur le X rouge dans la liste des périphériques pour afficher la configuration des informations d'identification du périphérique.
- Raison de l'échec : une raison de l'échec apparaît dans la colonne si un périphérique ne communique pas avec la sonde. Les messages possibles incluent “ ” d'informations d'identification non valides ou “ SNMP désactivé ”.

Note: Il est recommandé d'activer SNMP sur le périphérique pour avoir une topologie réseau plus précise.

Vous devez maintenant avoir correctement affiché l'identité des périphériques sur le réseau et son type d'informations d'identification correspondant.