Configurez les qualifications de périphérique sur la sonde de réseau de FindIT

Introduction

La Gestion de réseau de Cisco FindIT fournit les outils qui vous aident facilement surveillent, gèrent, et configurent votre Cisco 100 aux périphériques de réseau de gamme 500 tels que des Commutateurs, des Routeurs, et des Points d'accès Sans fil (WAPs) utilisant votre navigateur Web. Il vous informe également au sujet du périphérique et des notifications de support de Cisco telles que la Disponibilité du nouveau micrologiciel, de l'état des périphériques, des mises à jour de paramètres réseau, et de tous les périphériques Cisco connectés qui ne sont plus sous la garantie ou sont couverts par un contrat de support.

La Gestion de réseau de FindIT est une application distribuée qui est composée de deux composants ou interfaces distincts : un ou plusieurs sondes désignées sous le nom du réseau de FindIT sondent et un gestionnaire simple appelé le gestionnaire de réseau de FindIT.

Un exemple de la sonde de réseau de FindIT installée à chaque site dans le réseau exécute la détection de réseau, et communique directement avec chaque périphérique de Cisco. Dans un réseau de site unique, vous pouvez choisir d'exécuter un exemple autonome de sonde de réseau de FindIT. Cependant, si votre réseau se compose de plusieurs sites, vous pouvez installer le gestionnaire de réseau de FindIT à un emplacement commode et associer chaque sonde avec le gestionnaire. De l'interface de gestionnaire, vous pouvez obtenir une vue générale de l'état de tous les sites dans votre réseau, et vous connectez à la sonde installée à un site particulier quand vous souhaitez visualiser des informations détaillées pour ce site.

Pour que le réseau de FindIT entièrement découvre et pour gère le réseau, la sonde de réseau de FindIT doit avoir des qualifications à authentifier avec les périphériques de réseau. Quand un périphérique est d'abord découvert, la sonde tentera d'authentifier avec le périphérique utilisant le nom d'utilisateur et mot de passe et le protocole SNMP par défaut (la communauté SNMP. Si les qualifications de périphérique ont été changées du par défaut, alors il sera que vous fournissiez les qualifications correctes à FindIT. Si cette tentative échoue, un message de notification sera généré et des qualifications valides doivent être fournies par l'utilisateur.

Objectif

L'objectif de ce document est de t'afficher comment configurer les qualifications de périphérique sur la sonde de réseau de Cisco.

Périphériques applicables

- Sonde de FindIT

Version de logiciel

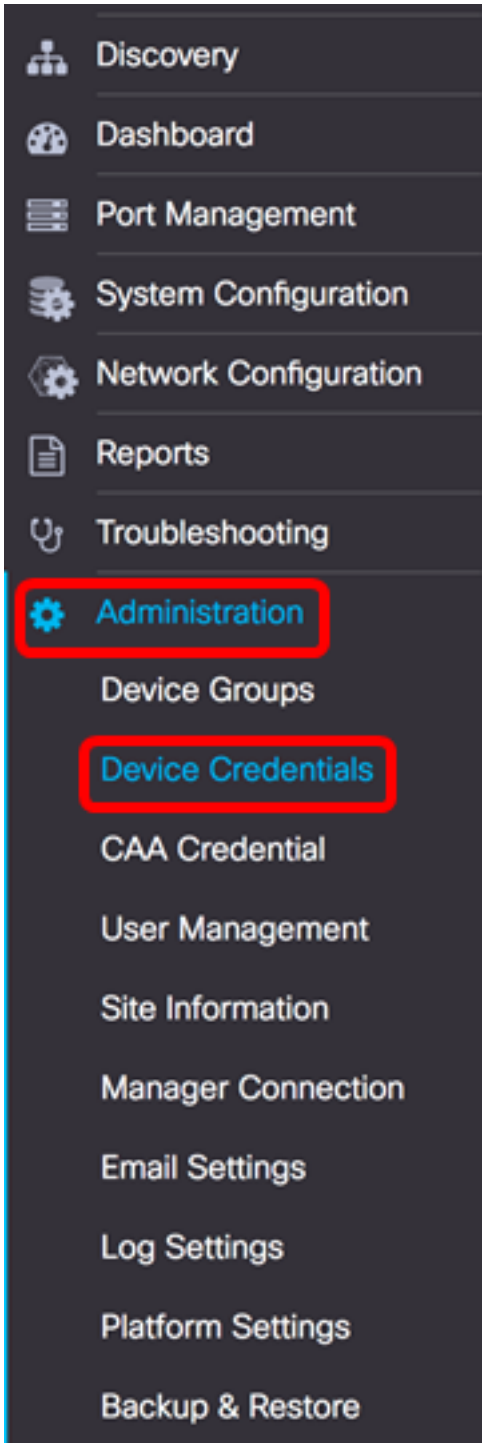
- 1.1

Configurez les qualifications de périphérique

Ajoutez les nouvelles qualifications

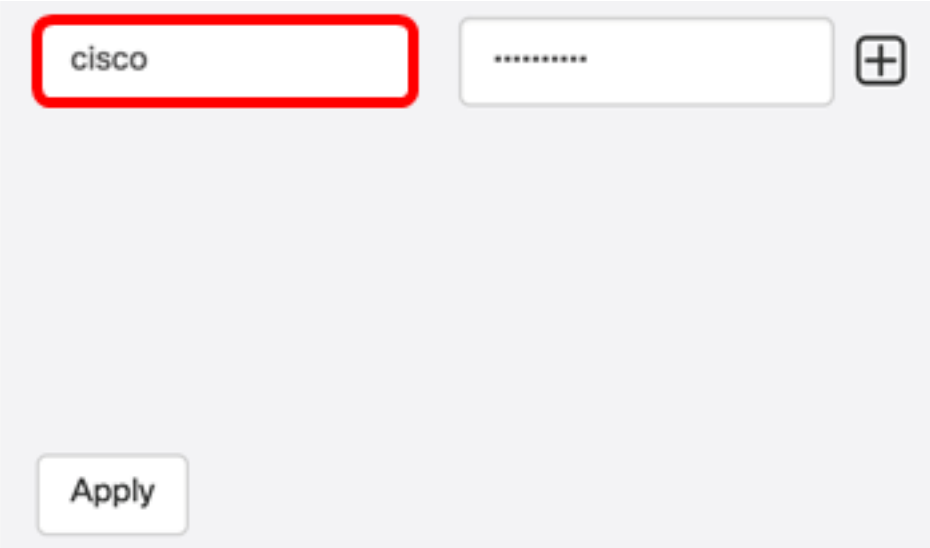
Entrez dans un ou plusieurs ensembles de qualifications dans les domaines ci-dessous. Quand appliqué, chaque laisser-passer sera testé contre tous les périphériques du type approprié pour lequel fonctionnant les qualifications ne sont pas disponibles. Un ensemble de qualifications peut être une combinaison de nom d'utilisateur/mot de passe, une communauté SNMPv2 ou les qualifications SNMPv3.

Étape 1. Ouvrez une session au GUI d'administrateur de sonde de réseau de FindIT et choisissez les **qualifications de gestion > de périphérique**.

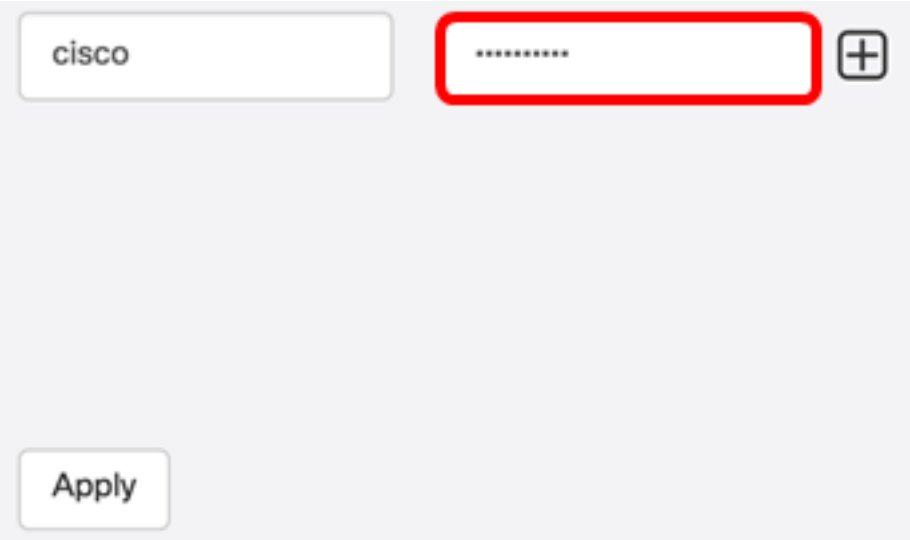


Étape 2. Dans la nouvelle région de qualifications d'ajouter, écrivez un nom d'utilisateur à appliquer aux périphériques dans le réseau dans le domaine de *nom d'utilisateur*. Le nom d'utilisateur et mot de passe par défaut est Cisco.

Remarque: Dans cet exemple, Cisco est utilisé.

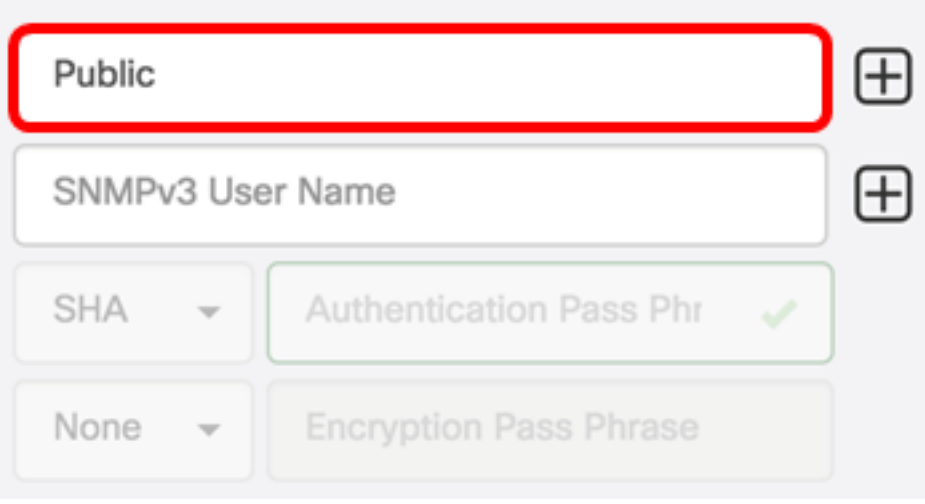


Étape 3. Dans le domaine de *mot de passe*, entrez un mot de passe.



Étape 4. Dans le domaine de la *Communauté SNMP*, écrivez le nom de la Communauté. C'est seulement la chaîne lue de la communauté pour authentifier la commande de snmp get. Le nom de la Communauté est utilisé pour récupérer les informations du périphérique SNMP. Le nom de la Communauté SNMP de par défaut est public.

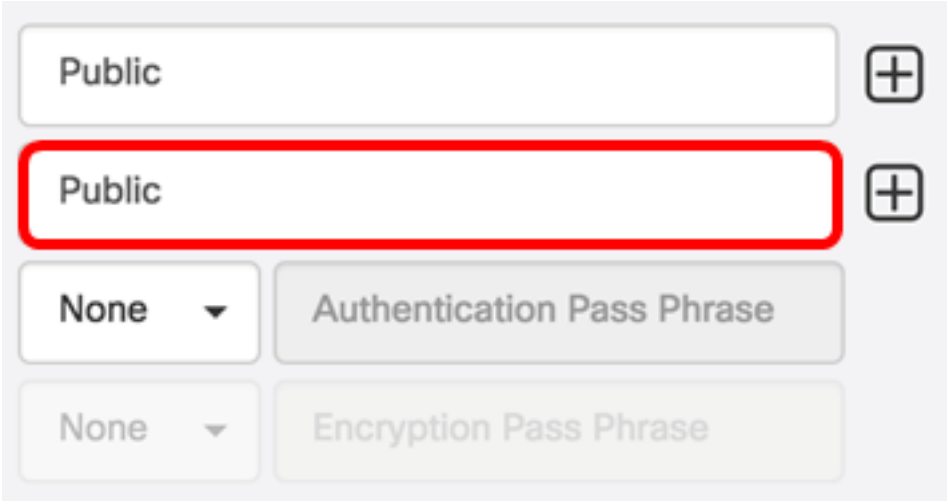
Remarque: Dans cet exemple, le public est utilisé.



Étape 5. Dans le *champ User Name SNMPv3*, écrivez un nom d'utilisateur à utiliser dans le

SNMPv3

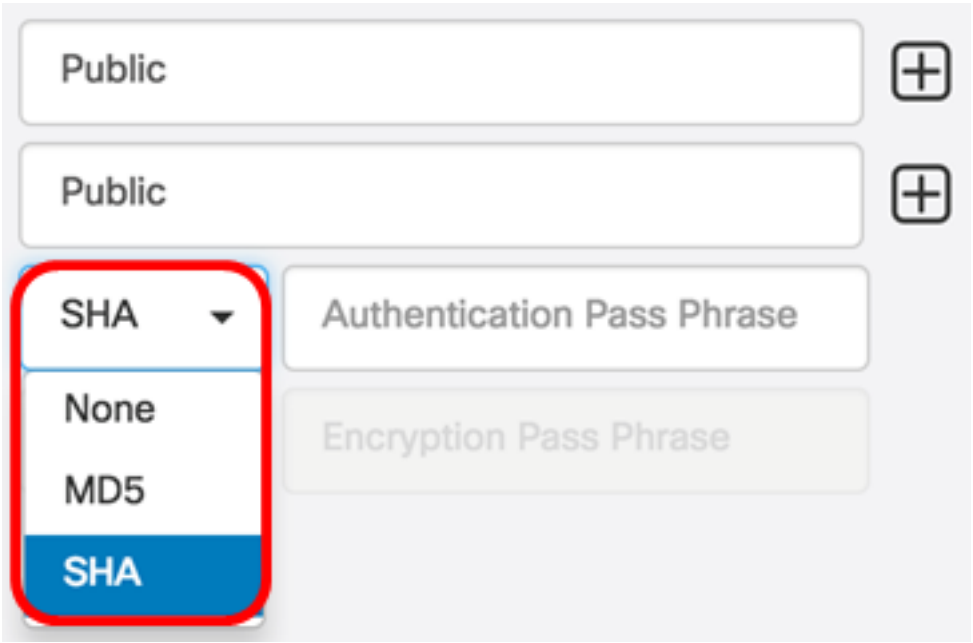
Remarque: Dans cet exemple, le public est utilisé.



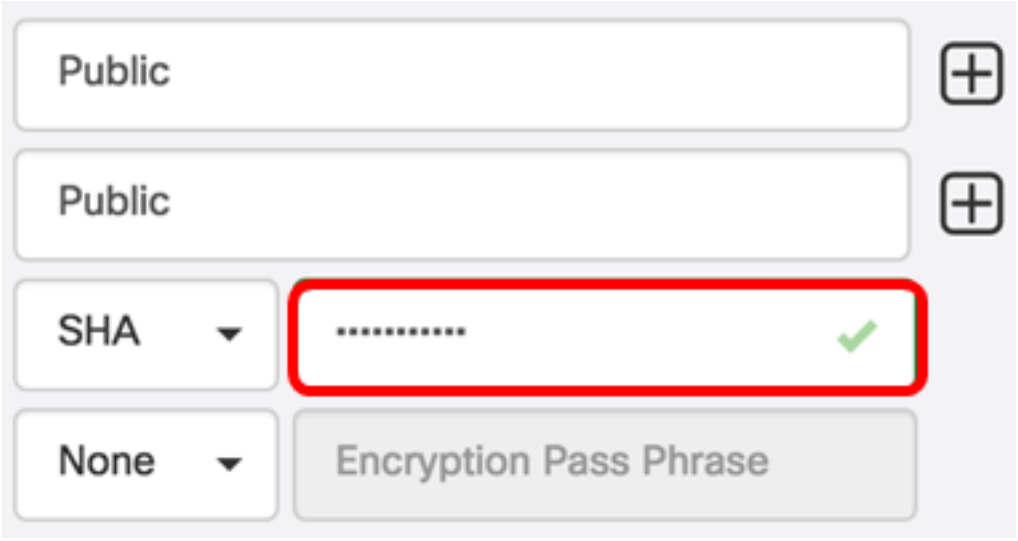
Étape 6. Du menu déroulant d'authentification, choisissez un type d'authentification que SNMPv3 utilisera. Les options sont :

- Aucun — Aucune authentification de l'utilisateur n'est utilisée. Il s'agit de la configuration par défaut. Si vous choisissez cette option, ignorez à l'étape 11.
- MD5 — Utilise la méthode de cryptage 128-bit. L'algorithme de MD5 emploie un système cryptographique public pour chiffrer des données. Si ceci est choisi, vous serez requis d'écrire un mot de passe d'authentification.
- SHA — L'Algorithme de hachage sûr (SHA) est un algorithme de hachage à sens unique qui produit un condensé 160-bit. Le SHA calcule plus lent que le MD5, mais est plus sécurisé que le MD5. Si ceci est choisi, vous serez requis d'écrire un mot de passe d'authentification et de choisir un protocole de cryptage.

Remarque: Dans cet exemple, le SHA est utilisé.



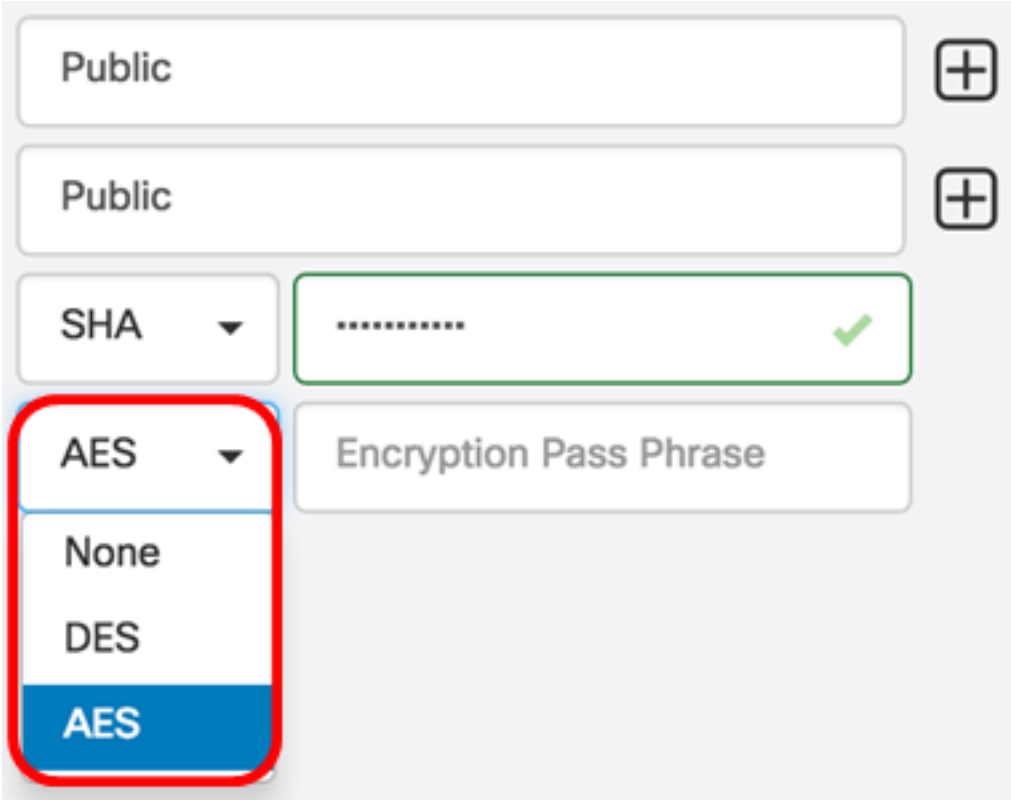
Étape 7. Dans le domaine de *mot de passe d'authentification*, entrez un mot de passe à utiliser par SNMPv3.



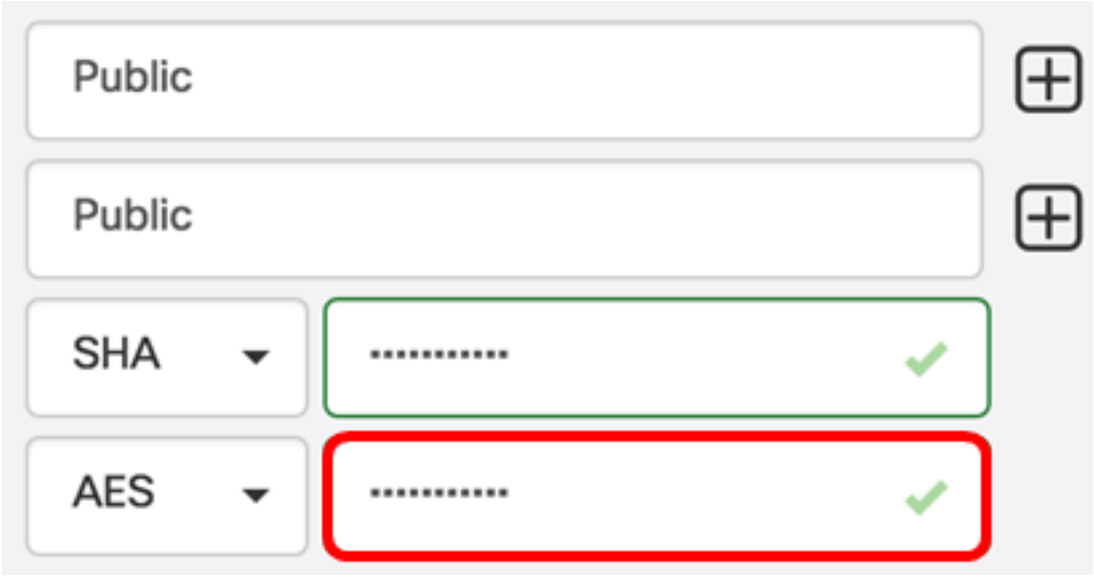
Étape 8. Du menu déroulant de type de cryptage, choisissez une méthode de cryptage pour chiffrer les demandes SNMPv3. Les options sont :

- Aucun — Aucune méthode de cryptage n'est exigée.
- DES — Le Norme de chiffrement de données (DES) est un chiffre par bloc symétrique qui utilise une clé secrète partagée 64-bit.
- AES128 — Advanced Encryption Standard qui utilise une clé 128-bit.

Remarque: Dans cet exemple, AES est choisi.

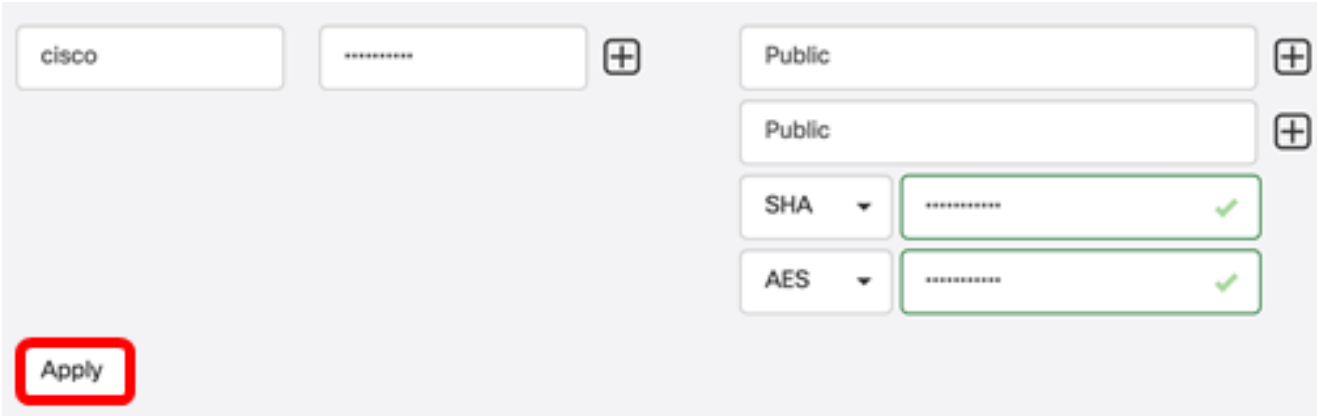


Étape 9. Dans le domaine de *mot de passe de cryptage*, introduisez une clé 128-bit à utiliser par SNMP pour le cryptage.

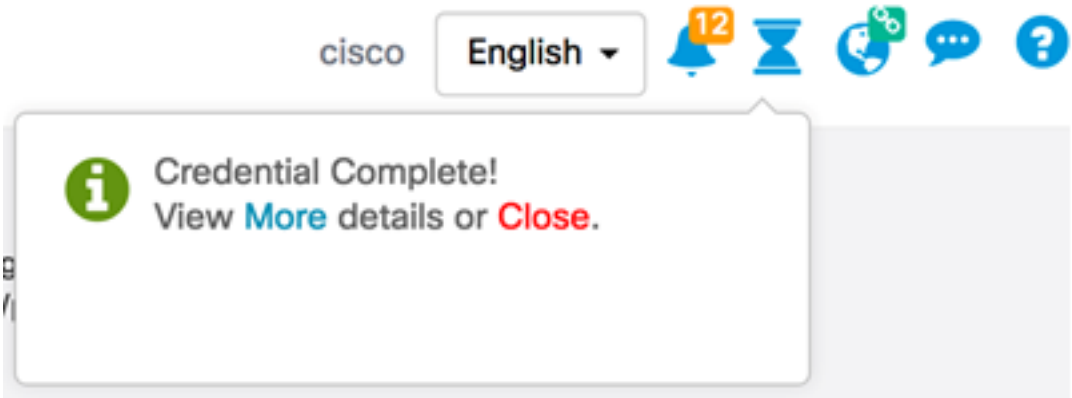


Clic (facultatif) d'étape 10. le bouton pour créer une nouvelle entrée pour le nom d'utilisateur et le titre. Vous pouvez ajouter à un ou deux entrées supplémentaires, selon le type de qualifications.

Étape 11. Cliquez sur Apply.



Une fenêtre semblera sous l'icône de sablier vous informer que les configurations nécessaires ont été appliquées.



Vous devriez avoir maintenant avec succès configuré les qualifications de périphérique sur la sonde de réseau de FindIT.

Périphériques de vue sur le réseau

Le Tableau ci-dessous affiche les périphériques découverts par la sonde de réseau de Cisco FindIT.

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

- Périphérique — Le nom du périphérique découvert sur le réseau. Un nom du périphérique peut apparaître de plusieurs périodes selon le type de qualifications utiles.
- Type de créance — Ceci peut être ID utilisateur/mot de passe ou SNMP d'admin. Ceci est utilisé pour tirer les informations du périphérique.
- Ok de laisser-passer ? — Un contrôle ou un X rouge peut sembler déterminer si les qualifications sont entrées dans l'appliqué ci-dessus de champs au périphérique approprié. Cliquer sur sur le X rouge sur la liste de périphériques évoquera la configuration pour les qualifications de périphérique.
- Raison de panne — Une raison de panne apparaît dans la colonne si un périphérique ne communique pas avec la sonde. Les messages possibles incluent « le laisser-passer non valide » ou le « SNMP désactivé ».

Remarque: Il est recommandé pour permettre au SNMP sur le périphérique d'avoir une topologie du réseau plus précise.

Vous devriez avoir maintenant avec succès visualisé l'identité des périphériques sur le réseau et son type de créance correspondant.