

Configurer les informations d'identification du périphérique sur le tableau de bord Cisco Business

Introduction

Le tableau de bord Cisco Business fournit des outils qui vous aident à surveiller, gérer et configurer facilement vos périphériques Cisco Business, 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.

Cisco Business Dashboard Network Management est une application distribuée qui comprend deux composants ou interfaces distincts : un ou plusieurs sondes appelées Sondage de tableau de bord Cisco Business et un tableau de bord unique appelé Tableau de bord Cisco Business.

Une instance de Cisco Business Dashboard 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 la sonde de tableau de bord Cisco Business. Cependant, si votre réseau est composé de plusieurs sites, vous pouvez installer Cisco Business Dashboard à un emplacement pratique et associer chaque sonde au tableau de bord. 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 Cisco Business Dashboard Network puisse découvrir et gérer pleinement le réseau, la sonde de tableau de bord Cisco Business 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 au tableau de bord Cisco Business. 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 du périphérique sur la sonde Cisco.

Périphériques pertinents | Version du logiciel

- Tableau de bord Cisco Business | 2.2

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 graphique de Cisco Business Dashboard et sélectionnez **Administration > Device Credential**.

Cisco Business Dashboard



Dashboard



Network



Inventory



Port Management



Network Configuration



Network Plug and Play



Event Log

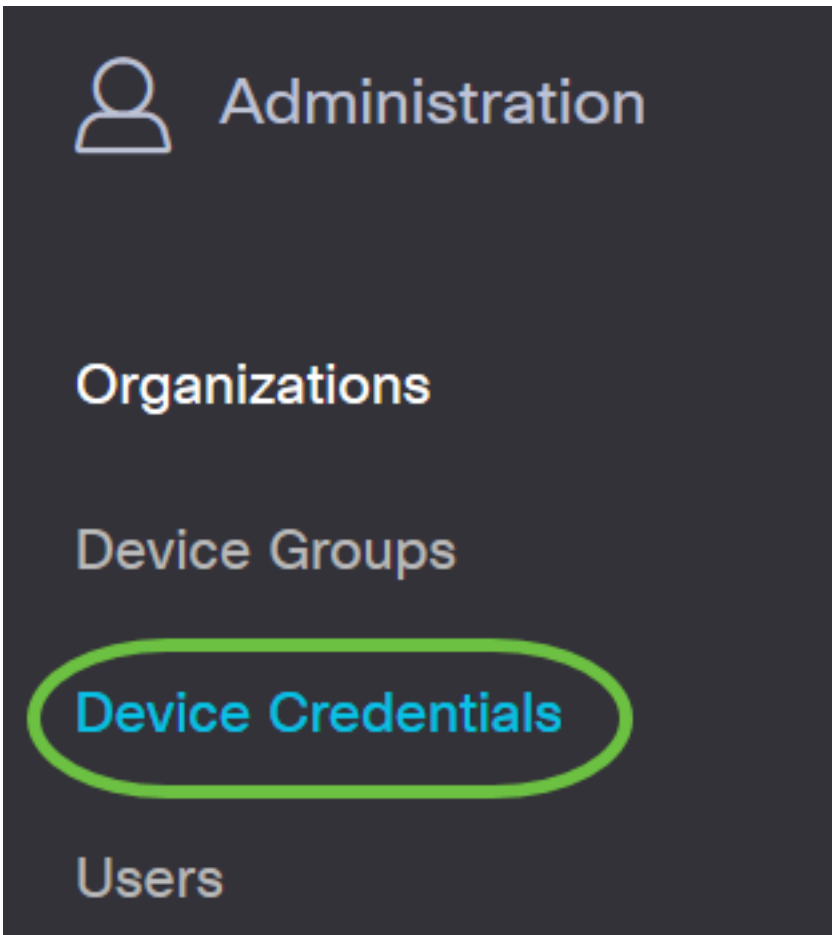


Reports



Administration





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.

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 of credentials may be either a username/password combination, an SNMPv2 community or SNMPv3 credentials.

cisco	••••••••	🗑️ +
cisco		🗑️

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

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 of credentials may be either a username/password combination, an SNMPv2 community or SNMPv3 credentials.

cisco	••••••••	🗑️ +
cisco		🗑️

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.

The screenshot shows a configuration interface for SNMP. At the top, there is a text input field containing 'cisco' and a password field with 8 dots. Below these are two rows of community entries. Each row contains a community name, a checkmark, and a trash icon. The second row, with 'public' as the community name, is highlighted with a green circle. Below the community list are two dropdown menus: 'SHA' and 'AES', each followed by a password field with 16 dots.

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

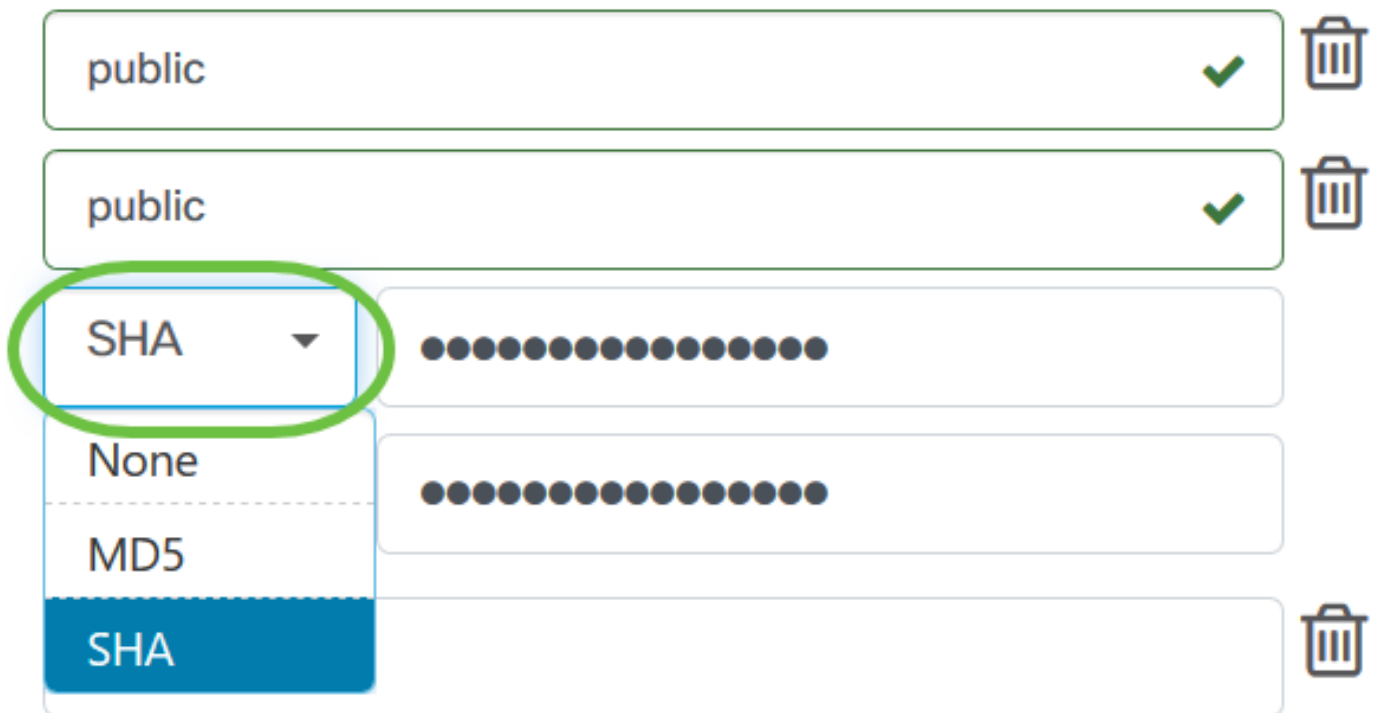
Note: Dans cet exemple, Public est utilisé.

The screenshot shows a configuration interface for SNMPv3. At the top, there is a text input field containing 'cisco' and a password field with 8 dots. Below these are two rows of user entries. Each row contains a user name, a checkmark, and a trash icon. The second row, with 'public' as the user name, is highlighted with a green circle. Below the user list are two dropdown menus: 'SHA' and 'AES', each followed by a password field with 16 dots.

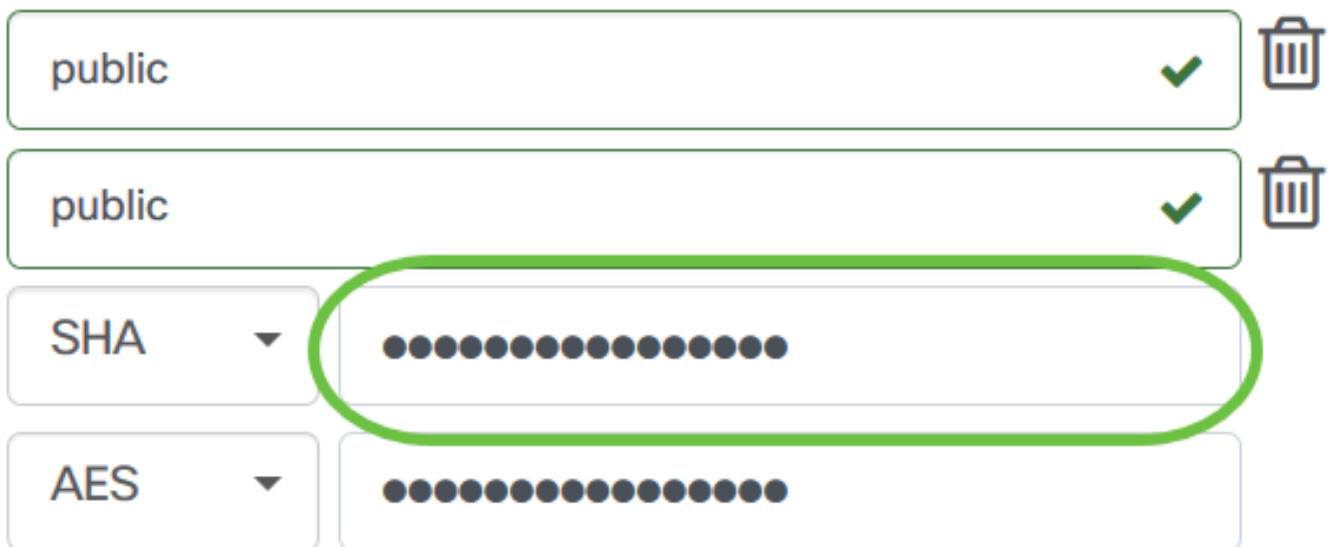
Étape 6. Dans le menu déroulant *Authentication*, sélectionnez un type d'authentification que SNMPv3 utilisera. Les options sont les suivantes :

- 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.

The image shows a configuration interface with several rows. The first two rows are labeled 'public' and have a green checkmark and a trash icon. The third row is labeled 'SHA' and has a series of black dots. The fourth row is labeled 'AES' and has a series of black dots; this row is highlighted with a green circle. Below this, a dropdown menu is open, showing options: 'None', 'DES', and 'AES' (which is highlighted in blue). To the right of the 'None' and 'DES' rows is a trash icon. Below the 'AES' row is a series of colored squares representing data. At the bottom, there are more rows with colored squares.

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

This image is similar to the one above, showing the same configuration interface. The 'AES' row is now highlighted with a green circle, indicating that the 'Encryption Pass Phrase' field is the focus of the next step. The dropdown menu is no longer open.

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.

🗑️ ⊕

✓ 🗑️

✓ 🗑️

SHA

AES

Étape 11. Cliquez sur Apply.

🗑️ ⊕

✓ 🗑️

✓ 🗑️

SHA

AES

Apply Reset

Vous devez maintenant avoir correctement configuré les informations d'identification du périphérique sur l'analyse du tableau de bord Cisco Business.

Affichage des périphériques sur le réseau

Le tableau ci-dessous présente les périphériques détectés par Cisco Business Dashboard Probe.

Device	Type	Organization	Network	Credential	Status	Last Used	Last Used Successfully	Action
SG300-10PP	Switch	Branch Offices	Branch 1	SNMPv2/*****	N/A	Aug 5 2020 10:47:33	Aug 5 2020 10:47:33	🗑️ 🗑️ 🗑️
SG300-10PP	Switch	Branch Offices	Branch 1	cisco/*****	N/A	Aug 4 2020 13:42:48	Aug 4 2020 13:42:48	🗑️ 🗑️ 🗑️
switch0294f9	Switch	Branch Offices	Branch 1	SNMPv2/*****	N/A	Aug 5 2020 10:47:30	Aug 4 2020 13:12:12	🗑️ 🗑️ 🗑️

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.