

Gérez les utilisateurs de Gestion de réseau de FindIT

Objectif

La page de gestion des utilisateurs du gestionnaire de réseau de FindIT et de la sonde de réseau de FindIT te permet pour définir les utilisateurs qui peuvent accéder au réseau de FindIT, et te permet également pour implémenter des conditions requises de complexité de mot de passe et des configurations de session pour ces utilisateurs.

Supports réseau de FindIT deux types d'utilisateurs : admin et opérateur. Un admin a l'accès complet aux caractéristiques de réseau de FindIT, alors qu'un opérateur peut faire tout excepté gérer des utilisateurs. Quand le gestionnaire de réseau de FindIT est d'abord installé, un utilisateur par défaut d'admin est créé avec le nom d'utilisateur et mot de passe les deux positionnement à **Cisco**.

Cet article prévoit des instructions sur la façon dont ajouter, éditer, ou supprimer des utilisateurs, et change des configurations de session de complexité et d'utilisateur de mot de passe.

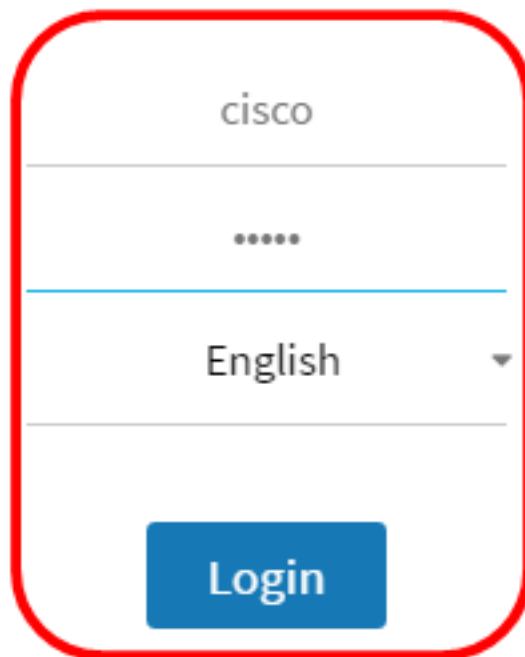
Gérez les utilisateurs de Gestion de réseau de FindIT

Ajoutez un nouvel utilisateur

Étape 1. Ouvrez une session au GUI de gestion de votre gestionnaire de réseau de FindIT ou sonde de réseau de FindIT.



FindIT Network Manager

A login form with a red rounded rectangular border. It contains a text input field with "cisco", a password field with six dots, a language dropdown menu set to "English", and a blue "Login" button.

cisco

.....

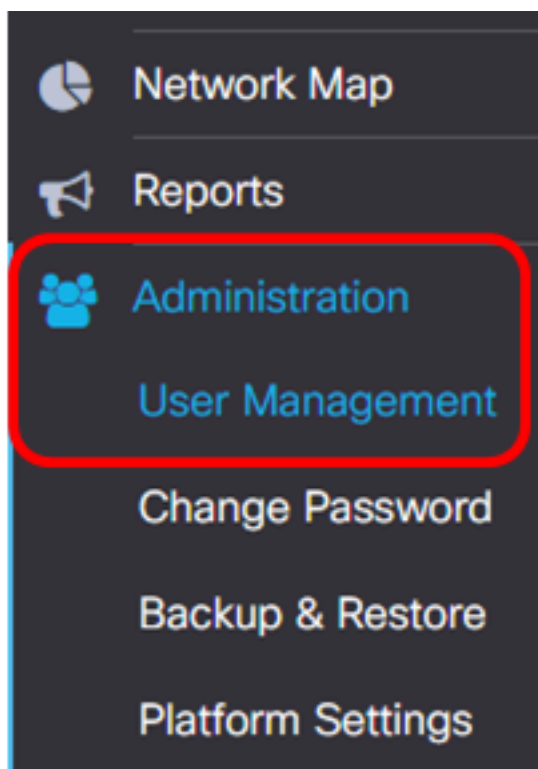
English ▼

Login

© 2015-2016 Cisco Systems, Inc. All Rights Reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.




Remarque: Dans cet exemple, le gestionnaire de réseau de FindIT est utilisé.



Étape 2. Choisissez la **gestion > la gestion des utilisateurs**.



Étape 3. Cliquez sur + bouton pour ajouter ou créer un nouvel utilisateur.

Local Users

	User Name	User Type	Action
<input type="checkbox"/>	cisco	ADMIN	 

Étape 4. Écrivez votre nom d'utilisateur dans le *champ User Name*.

User Name: 

Remarque: Dans cet exemple, John est utilisé.

Étape 5. Entrez votre mot de passe dans le domaine de *mot de passe*.

Password: 

Étape 6. Ressaisissez votre mot de passe dans le domaine de *confirmation du mot de passe*.

Password: ✓

Confirm Password: ✓

Password Strength:  Strong

Le mètre de point fort de mot de passe affiche le point fort de Sécurité du mot de passe entré. Dans cet exemple, le point fort de mot de passe est fort.

Étape 7. Cliquez sur une case d'option de la région de type d'utilisateur.

User Type: Administrator Operator

Les options sont :

- Administrateur — Ce type d'utilisateur a l'accès complet aux caractéristiques de réseau de FindIT.
- Opérateur — Ce type d'utilisateur a l'accès complet aux caractéristiques de réseau de FindIT excepté gérer des utilisateurs.


Remarque: Dans cet exemple, l'opérateur est choisi.

Étape 8. Cliquez sur OK.

User Name: ✓

Password: ✓




Confirm Password: ✓





Password Strength:  Strong

User Type: Administrator Operator

Vous devriez maintenant avoir ajouté un nouvel utilisateur.

Local Users

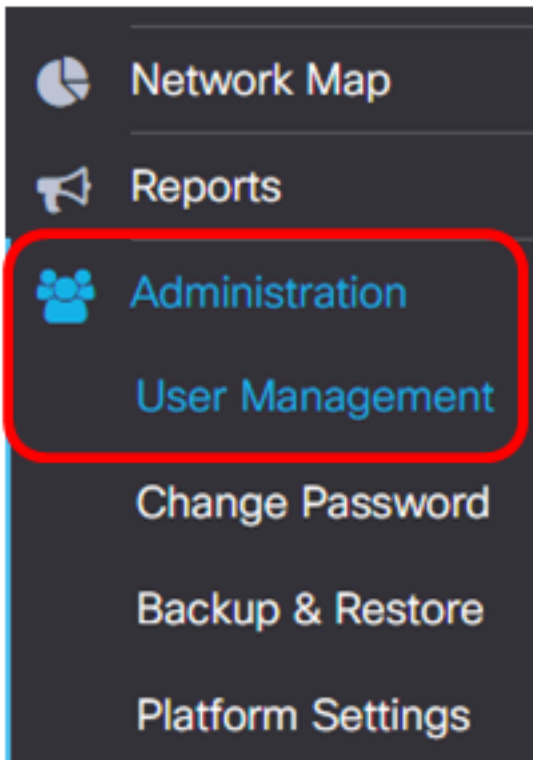
  

	User Name	User Type	Action
<input type="checkbox"/>	cisco	ADMIN	 
<input type="checkbox"/>	John	OPERATOR	 





Modifiez un utilisateur

Pour modifier un utilisateur existant, faites ce qui suit :

Étape 1. Choisissez la **gestion** > la **gestion des utilisateurs**.



Étape 2. Cochez la case à côté du nom d'utilisateur que vous voulez modifier alors cliquez sur l'icône d'**éditer**.

	User Name	User Type	Action
<input type="checkbox"/>	cisco	ADMIN	 
<input checked="" type="checkbox"/>	John	OPERATOR	 

Remarque: Dans cet exemple, la case à côté de John est cochée.

Contrôle (facultatif) d'étape 3. la case de **mot de passe de modification** pour changer le mot de passe en cours.

Edit User

User Name: John

Change password

Remarque: Alternativement, vous pouvez décocher cette case pour retenir le mot de passe en cours. Si vous choisissez cette option, ignorez à l'[étape 5](#).

Étape 4. (facultative) entrent un nouveau mot de passe dans le domaine de *mot de passe*.

Change password

Password:

Confirmation (facultative) d'[étape 5](#). le mot de passe dans le domaine de *confirmation du mot de passe*.

Password:

Confirm Password:

Password Strength:



Le mètre de point fort de mot de passe affiche le point fort de Sécurité du mot de passe entré. Dans cet exemple, le point fort de mot de passe est fort.

Étape 6. Cliquez sur une case d'option de la région de type d'utilisateur.

User Type:

Administrator Operator

Les options sont :

- Administrateur — Ce type d'utilisateur a l'accès complet aux caractéristiques de réseau de FindIT.
- Opérateur — Ce type d'utilisateur a l'accès complet aux caractéristiques de réseau de FindIT excepté gérer des utilisateurs.

Remarque: Dans cet exemple, l'administrateur est choisi.

Étape 7. Cliquez sur OK.

User Name: John

Change password





Password: ✓

Confirm Password: ✓

Password Strength: Strong

User Type: Administrator Operator

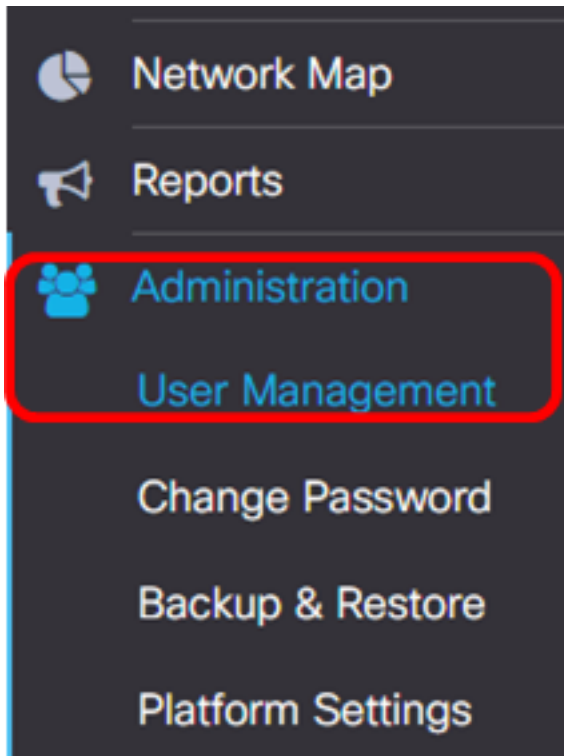
Vous devriez maintenant avoir modifié un utilisateur existant.

	User Name	User Type	Action
<input type="checkbox"/>	cisco	ADMIN	 
<input type="checkbox"/>	John	ADMIN	 





Supprimez un utilisateur

Pour supprimer un utilisateur existant, faites ce qui suit :

Étape 1. Choisissez la **gestion > la gestion des utilisateurs**.

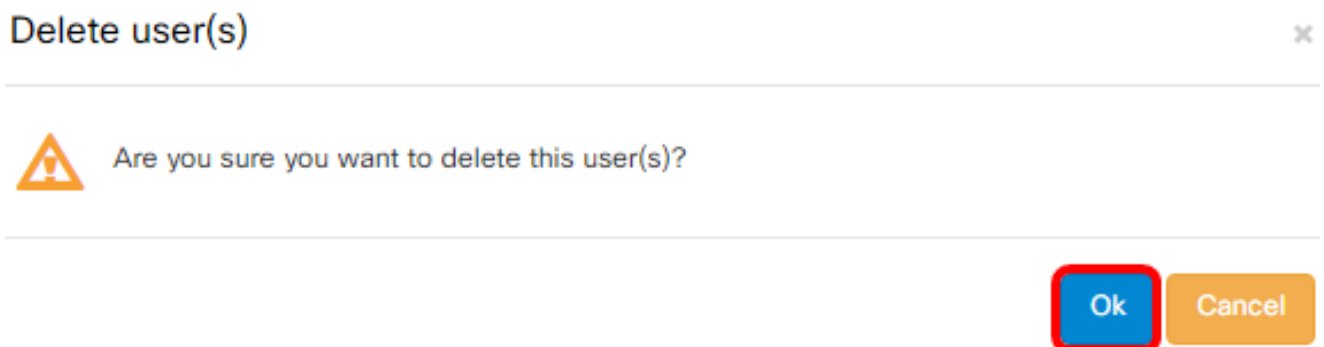


Étape 2. Cochez la case à côté du nom d'utilisateur que vous voulez modifier alors cliquez sur le bouton d'effacement.

	User Name	User Type	Action
<input type="checkbox"/>	cisco	ADMIN	 
<input checked="" type="checkbox"/>	John	ADMIN	 

Remarque: Dans cet exemple, John est choisi.

Étape 3. Ok de clic à poursuivre.



Vous devriez maintenant avoir supprimé un utilisateur.

Deleted user(s) successfully 2 sec

Local Users

Filter icons: funnel, plus, trash

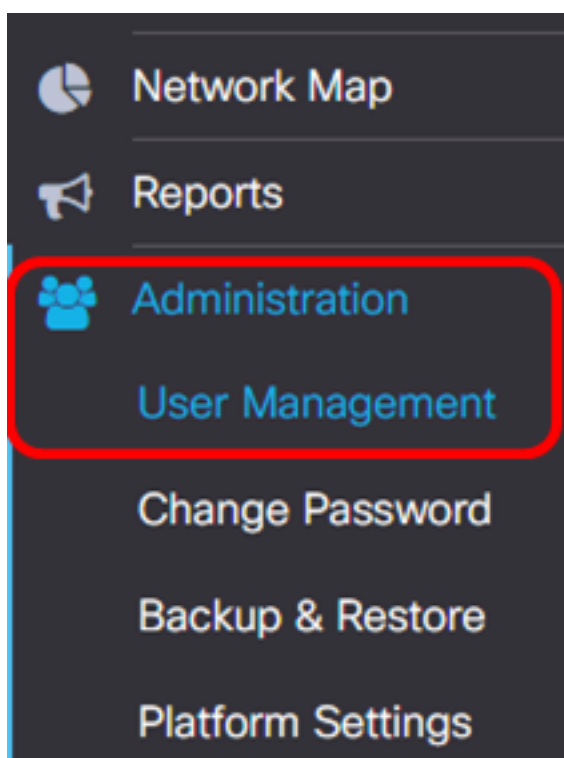
	User Name	User Type	Action
<input type="checkbox"/>	cisco	ADMIN	

Navigation: 1 | 10 per page | 1 - 1

Configurez la complexité de mot de passe

Pour activer ou changer des conditions requises de complexité de mot de passe, faites ce qui suit :

Étape 1. Choisissez la **gestion > la gestion des utilisateurs**.



Contrôle (facultatif) d'étape 2. la case de **configurations de complexité de mot de passe** pour activer des règles de complexité pour des mots de passe. Si cette caractéristique est activée, les nouveaux mots de passe doivent se conformer aux valeurs par défaut suivantes :

- Devrait avoir une longueur minimale de huit caractères.
- Devrait contenir des caractères au moins des classes à trois caractères (lettres majuscules, lettres minuscules, nombres, et caractères particuliers disponibles sur un clavier standard).
- Devrait être différent du mot de passe en cours.

Local User Password Complexity

Password Complexity Setting



Remarque: Alternativement, vous pouvez décocher cette case pour désactiver les configurations de complexité de mot de passe de l'utilisateur local. Si vous choisissez cette option, ignorez à l'[étape 6](#).

Étape 3. Écrivez une valeur dans le domaine *minimum de longueur du mot de passe*. La valeur par défaut est 8, et la plage est 6 à 64 caractères.

Password Complexity Setting




Minimum Password Length 

Remarque: Dans cet exemple, 12 est utilisés.

Étape 4. Écrivez une valeur dans le *nombre minimal de champ de classes de caractères*. La valeur par défaut est 3, et la plage est 0 à 4 caractères.

Minimum number of character classes 

The four classes are: Upper case(ABCD...), lower case(abcd...), numerical(1234...) and special characters(!@#\$...).

Remarque: Dans cet exemple, 4 est utilisés.

Le contrôle (facultatif) d'étape 5. la case d'**enable** dans le le nouveau mot de passe doit être différent que l'en cours pour exiger un seul mot de passe sur la modification de mot de passe.

The new password must be different than the current one



[Étape 6](#). Sauvegarde de clic.

Local User Password Complexity

Password Complexity Setting

Enable

Minimum Password Length ?

12

Minimum number of character classes ?

4

The four classes are: Upper case(ABCD...), lower case(abcd...), numerical(1234...) and special characters(!@#\$...).

The new password must be different than the current one

Enable

Save

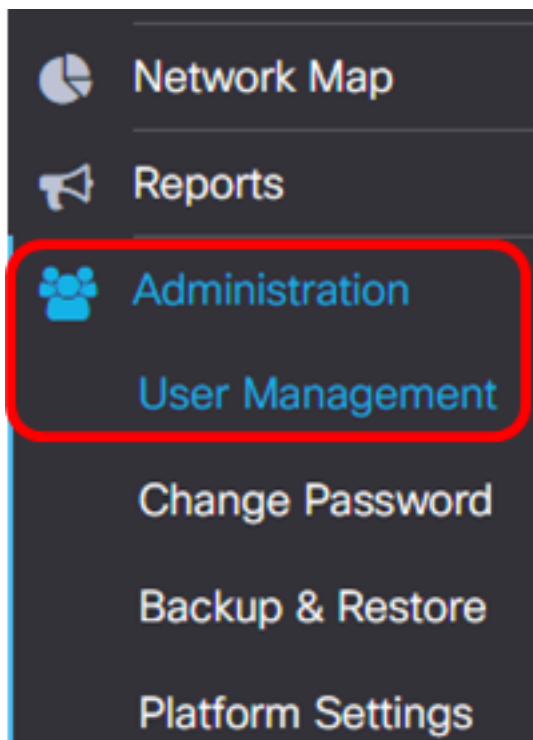
Cancel

Vous devriez maintenant avoir changé les configurations de complexité de mot de passe pour des utilisateurs locaux.

Configurez la configuration de session d'utilisateur

Pour activer ou changer des conditions requises de complexité de mot de passe, faites ce qui suit :

Étape 1. Choisissez la **gestion** > la **gestion des utilisateurs**.



Étape 2. Écrivez une valeur dans le domaine *de veille de délai d'attente (minute)*. La valeur

par défaut est 60, et la plage est de 10 à 60 minutes.

User Session Setting

Idle Timeout (min): ?

 ✓

Remarque: Dans cet exemple, 30 minutes est utilisées.

Étape 3. Écrivez une valeur dans le domaine de *temporisation absolue (heure)*. C'est la durée maximale qu'une session peut être en activité. La valeur par défaut est 24, et la plage est de 1 à 24 heures.

User Session Setting

Idle Timeout (min): ?

Absolute Timeout (hour): ?

Remarque: Dans cet exemple, 12 heures est utilisées.

Étape 4. **Sauvegarde de clic.**

Absolute Timeout (hour): ?

 ✓

Vous devriez maintenant avoir configuré les configurations de session d'utilisateur.