

Gerenciar os usuários do FindIT Network Management

Objetivo

A página Gerenciamento de usuários do FindIT Network Manager e FindIT Network Probe permite definir usuários que podem acessar a rede FindIT, além de permitir que você implemente requisitos de complexidade de senha e configurações de sessão para esses usuários.

O FindIT Network suporta dois tipos de usuários: administrador e operador. Um administrador tem acesso total aos recursos da FindIT Network, enquanto um operador pode fazer tudo, exceto gerenciar usuários. Quando o FindIT Network Manager é instalado pela primeira vez, um usuário admin padrão é criado com o nome de usuário e a senha definidos como **cisco**.

Este artigo fornece instruções sobre como adicionar, editar ou excluir usuários e alterar a complexidade da senha e as configurações da sessão do usuário.

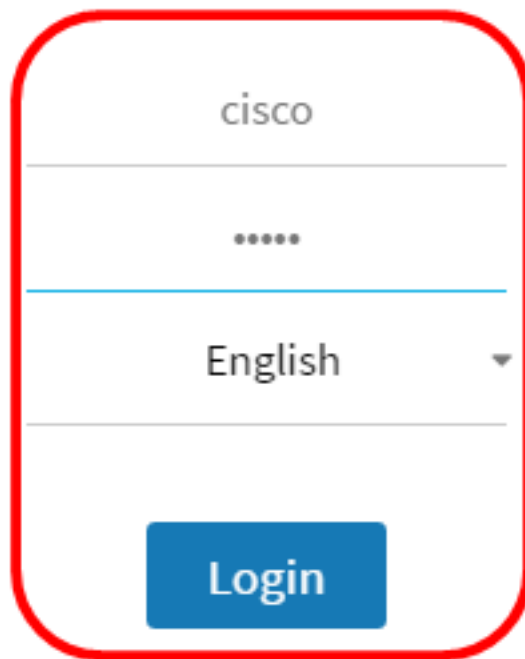
Gerenciar os usuários do FindIT Network Management

Adicionar um novo usuário

Etapa 1. Faça login na GUI de administração do FindIT Network Manager ou FindIT Network Probe.



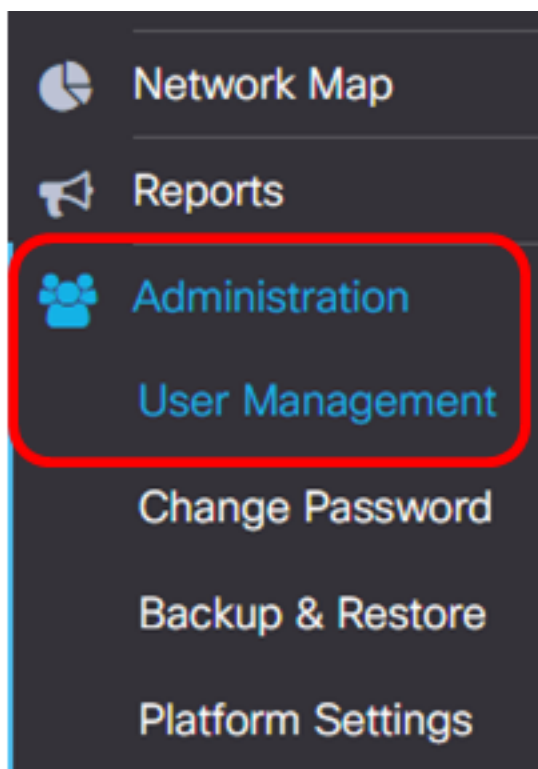
FindIT Network Manager

A login form for FindIT Network Manager, enclosed in a red rounded rectangle. It features a text input field with "cisco" entered, a password field with six dots, a language dropdown menu set to "English", and a blue "Login" button at the bottom.

© 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.

Note: Neste exemplo, o FindIT Network Manager é usado.

Etapa 2. Escolha **Administration**> **User Management**.



Etapa 3. Clique no + botão para adicionar ou criar um novo usuário.

Local Users

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

Etapa 4. Digite seu nome de usuário no campo *Nome de usuário*.

User Name:

Note: Neste exemplo, John é usado.

Etapa 5. Digite sua senha no campo Senha.

Password:

Etapa 6. Digite novamente sua senha no campo *Confirmar senha*.

Password: ✓

Confirm Password: ✓

Password Strength:  Strong

O medidor de força da senha exibe a intensidade de segurança da senha inserida. Neste exemplo, a força da senha é Forte.

Passo 7. Clique em um botão de opção na área Tipo de usuário.

User Type: Administrator Operator

As opções são:

- Administrador — Este tipo de usuário tem acesso total aos recursos FindIT Network.
- Operador — Este tipo de usuário tem acesso total aos recursos da FindIT Network, exceto para gerenciar usuários.


Note: Neste exemplo, Operador é escolhido.

Etapa 8. Click OK.

User Name: ✓

Password: ✓




Confirm Password: ✓





Password Strength:  Strong

User Type: Administrator Operator

Agora você deve ter adicionado um novo usuário.

Local Users

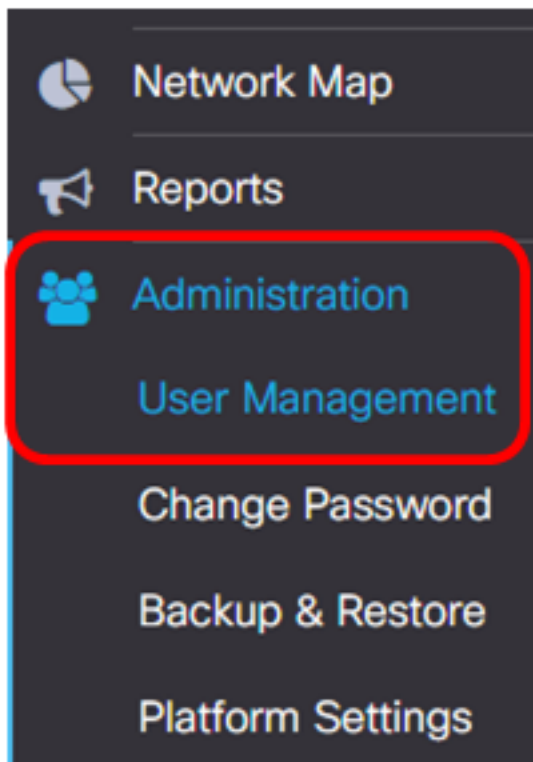
  

	User Name	User Type	Action
<input type="checkbox"/>	cisco	ADMIN	 
<input type="checkbox"/>	John	OPERATOR	 





Modificar um usuário

Para modificar um usuário existente, faça o seguinte:

Etapa 1. Escolha **Administração > Gerenciamento do usuário**.



Etapa 2. Marque a caixa de seleção ao lado do nome de usuário que deseja modificar e clique no ícone **Editar**.

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

Note: Neste exemplo, a caixa de seleção ao lado de John está marcada.

Etapa 3. (Opcional) Marque a caixa de seleção **Alterar senha** para alterar a senha atual.

Edit User

User Name: John

Change password

Note: Como alternativa, você pode desmarcar essa caixa de seleção para manter a senha atual. Se você escolher esta opção, vá para a [Etapa 5](#).

Etapa 4. (Opcional) Insira uma nova senha no campo *Senha*.

Change password

Password:

[Etapa 5](#). (Opcional) Insira novamente a senha no campo *Confirmar senha*.

Password:

Confirm Password:

Password Strength:



O medidor de força da senha exibe a intensidade de segurança da senha inserida. Neste exemplo, a força da senha é Forte.

Etapa 6. Clique em um botão de opção na área Tipo de usuário.

User Type:

Administrator Operator

As opções são:

- Administrador — Este tipo de usuário tem acesso total aos recursos FindIT Network.
- Operador — Este tipo de usuário tem acesso total aos recursos da FindIT Network, exceto para gerenciar usuários.

Note: Neste exemplo, Administrador é escolhido.

Passo 7. Click **OK**.

User Name: John

Change password

Password:

 ✓

Confirm Password:

 ✓





Password Strength:

Strong

User Type:

Administrator Operator

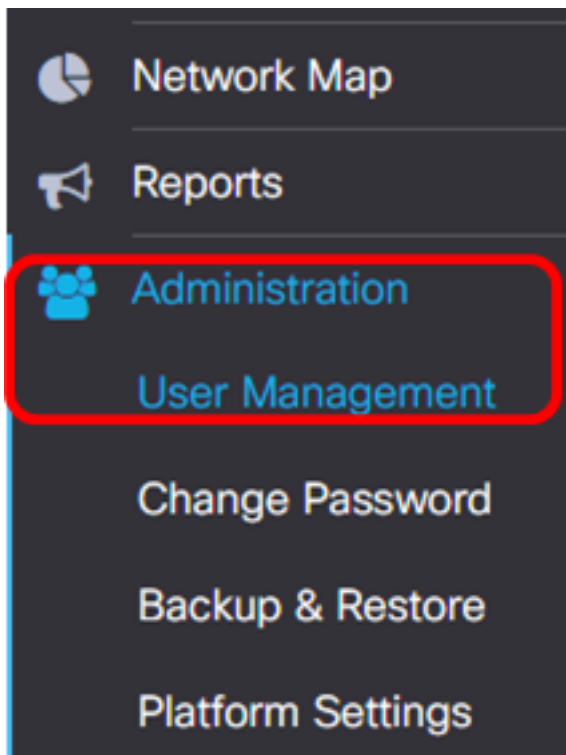
Agora você deve ter modificado um usuário existente.

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





Excluir um usuário

Para excluir um usuário existente, faça o seguinte:

Etapa 1. Escolha **Administração > Gerenciamento do usuário**.

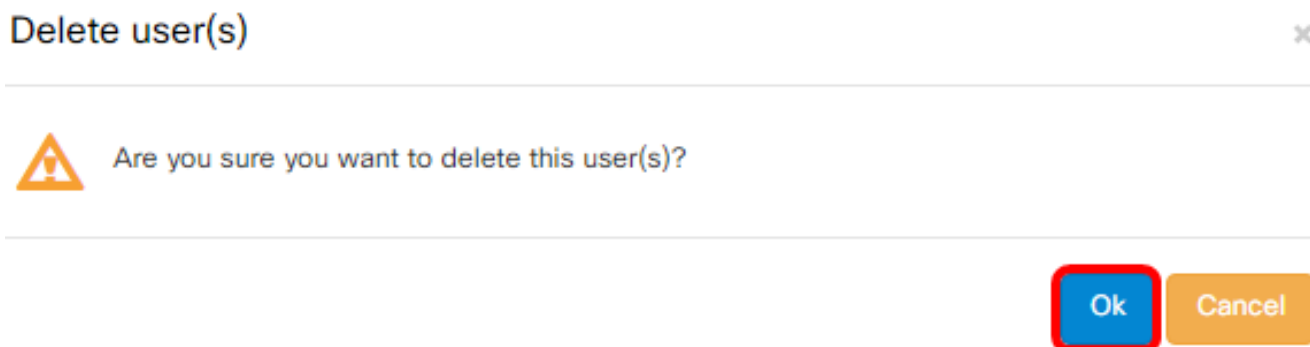


Etapa 2. Marque a caixa de seleção ao lado do nome de usuário que deseja modificar e clique no botão **Excluir**.

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

Note: Neste exemplo, John é escolhido.

Etapa 3. Clique em **Ok** para continuar.



Agora você deve ter excluído um usuário.

Deleted user(s) successfully 2 sec

Local Users

Filter + Delete

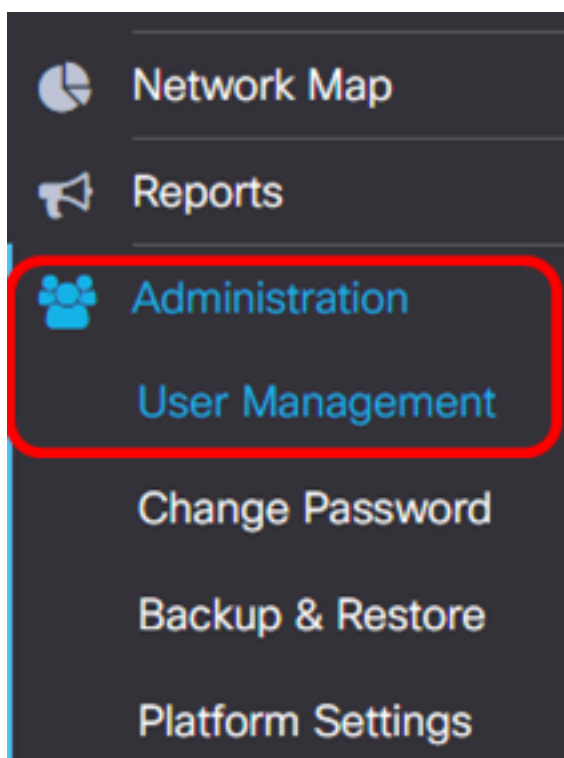
	User Name	User Type	Action
<input type="checkbox"/>	cisco	ADMIN	

1 10 per page 1 - 1

Configurar a complexidade da senha

Para ativar ou alterar os requisitos de complexidade de senha, faça o seguinte:

Etapa 1. Escolha **Administração > Gerenciamento do usuário**.



Etapa 2. (Opcional) Marque a caixa de seleção **Password Complexity Settings** para ativar regras de complexidade para senhas. Se esse recurso foi ativado, as novas senhas devem estar de acordo com as seguintes configurações padrão:

- Deve ter um comprimento mínimo de oito caracteres.
- Deve conter caracteres de pelo menos três classes de caracteres (letras maiúsculas, letras minúsculas, números e caracteres especiais disponíveis em um teclado padrão).
- Deve ser diferente da senha atual.

Local User Password Complexity

Password Complexity Setting



Note: Como alternativa, você pode desmarcar essa caixa de seleção para desativar as configurações de complexidade de senha do usuário local. Se você escolher esta opção, vá para a [Etapa 6](#).

Etapa 3. Insira um valor no campo *Tamanho mínimo da senha*. O valor padrão é 8 e o intervalo é de 6 a 64 caracteres.

Password Complexity Setting



Minimum Password Length 

Note: Neste exemplo, 12 é usado.

Etapa 4. Insira um valor no campo *Número mínimo de classes de caracteres*. O valor padrão é 3 e o intervalo é de 0 a 4 caracteres.

Minimum number of character classes 

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

Note: Neste exemplo, 4 é usado.

Etapa 5. (Opcional) Marque a caixa de seleção **Habilitar** na caixa A nova senha deve ser diferente da atual para exigir uma senha exclusiva após a alteração da senha.

The new password must be different than the current one



[Etapa 6](#). Click **Save**.

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

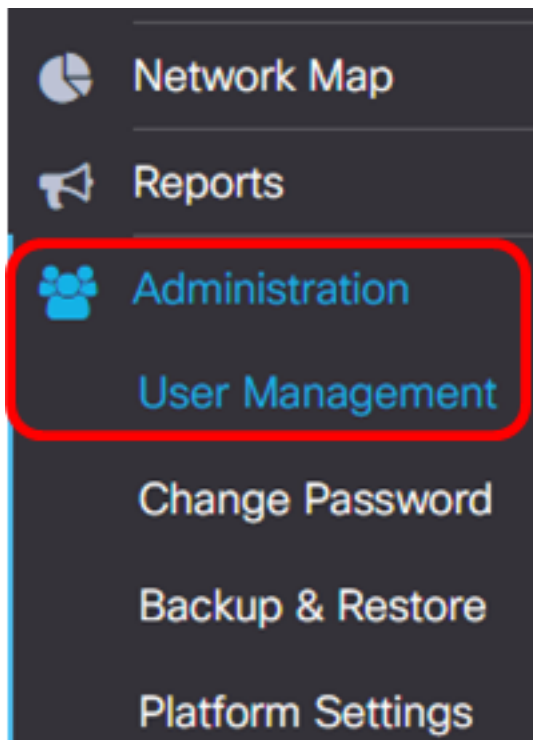
Cancel

Agora você deve ter alterado as configurações de complexidade de senha para usuários locais.

Configurar a sessão do usuário

Para ativar ou alterar os requisitos de complexidade de senha, faça o seguinte:

Etapa 1. Escolha **Administração > Gerenciamento do usuário**.



Etapa 2. Insira um valor no campo *Idle Timeout (min)*. O valor padrão é 60, e o intervalo é de 10 a 60 minutos.

User Session Setting

Idle Timeout (min): ?

 ✓

Note: Neste exemplo, são usados 30 minutos.

Etapa 3. Insira um valor no campo *Tempo limite absoluto (hora)*. Este é o tempo máximo que uma sessão pode estar ativa. O valor padrão é 24 e o intervalo é de 1 a 24 horas.

User Session Setting

Idle Timeout (min): ?

Absolute Timeout (hour): ?

Note: Neste exemplo, 12 horas são usadas.

Etapa 4. Click **Save**.

Absolute Timeout (hour): ?

 ✓

Agora você deve ter configurado as configurações da sessão do usuário.