Configuration du nom d'utilisateur et du mot de passe sur les routeurs VPN RV016, RV042, RV042G et RV082

Objectif

Pour un réseau sécurisé, il est important d'avoir un mot de passe difficile à deviner. Il est recommandé de modifier le nom d'utilisateur (admin) et le mot de passe (admin) de l'administrateur par défaut. En outre, certaines configurations nécessitent la modification du mot de passe administrateur par défaut. Ce document explique la procédure à suivre pour modifier le nom d'utilisateur et le mot de passe sur les routeurs VPN RV016, RV042, RV042G et RV082.

Périphériques pertinents

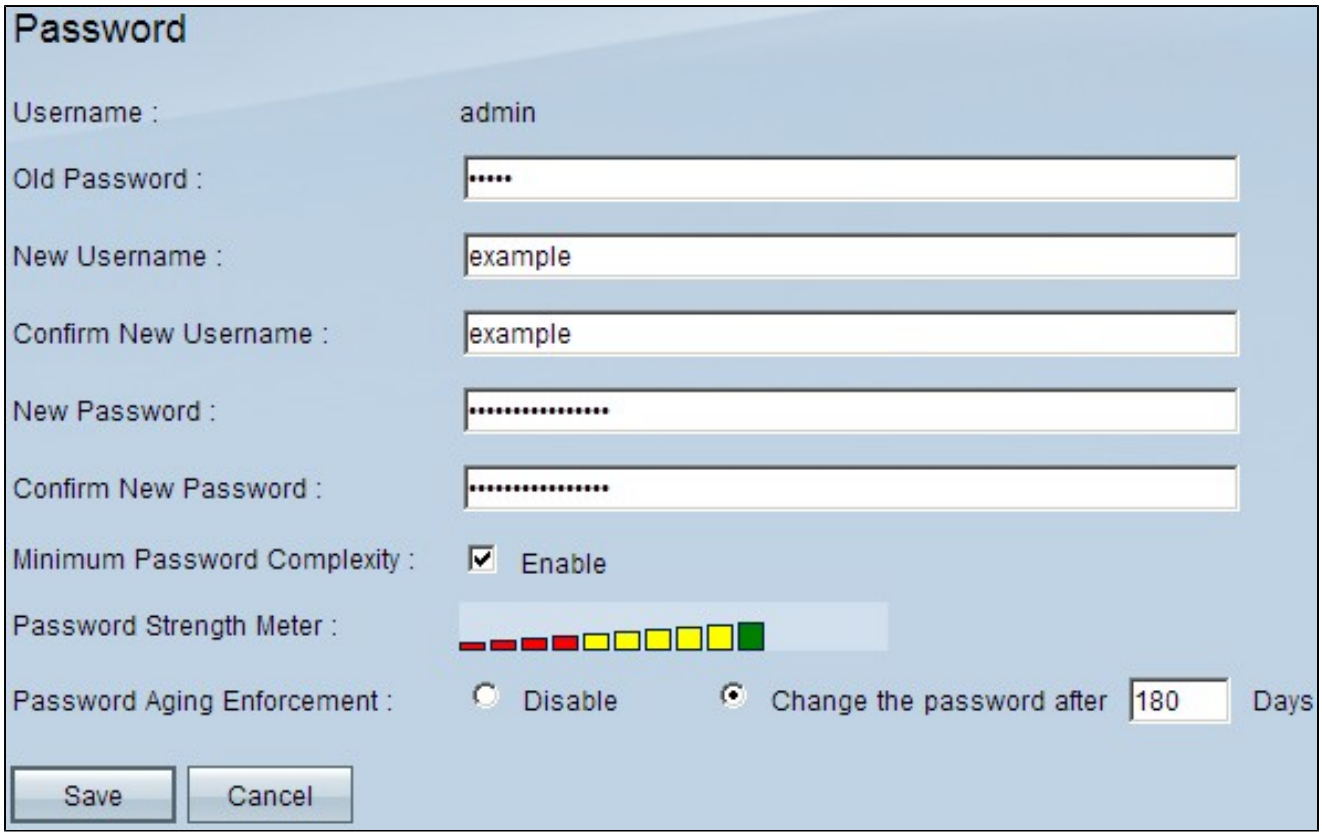
- RV016
- RV042
- RV042G
- RV082

Version du logiciel

- v 4.2.1.02

Modifier le nom et le mot de passe

Étape 1. Connectez-vous à l'interface graphique utilisateur du routeur. Pour accéder à la page, suivez les étapes de l'article Comment se connecter à l'interface utilisateur graphique d'un routeur Cisco Business. Choisissez Setup > Password et la page Password s'ouvre :



Le champ Nom d'utilisateur affiche le nom d'utilisateur par défaut, admin.

Étape 2. Entrez l'ancien mot de passe dans le champ Ancien mot de passe.

Étape 3. Entrez le nom d'utilisateur souhaité dans le champ Nouveau nom d'utilisateur. Si vous souhaitez conserver le nom d'utilisateur actuel, laissez ce champ vide.

Étape 4. Saisissez à nouveau le nom d'utilisateur souhaité dans le champ Confirmer le nouveau nom d'utilisateur. Si vous souhaitez conserver le nom d'utilisateur actuel, laissez ce champ vide.

Étape 5. Entrez le mot de passe souhaité dans le champ Nouveau mot de passe. Pour le mot de passe, vous pouvez utiliser des chiffres alphanumériques ou des caractères spéciaux, mais l'utilisation d'espace n'est pas autorisée.

Étape 6. Saisissez à nouveau le nouveau mot de passe souhaité dans le champ Confirmer le nouveau mot de passe.

Étape 7. (Facultatif) Pour appliquer un niveau de sécurité minimum au mot de passe, cochez la case Enable dans le champ Minimum Password Complexity.

Remarque : La complexité minimale du mot de passe nécessite qu'il comporte au moins 8

caractères et qu'il ne soit pas identique au nom d'utilisateur ou au mot de passe actuel. Il devrait également contenir 3 des 4 catégories suivantes : lettres majuscules, lettres minuscules, chiffres et caractères spéciaux.

La force du mot de passe est indiquée par le testeur de force du mot de passe qui est basé sur les règles de complexité. Les barres de couleur apparaissent lorsque vous saisissez votre mot de passe. Les couleurs sont le rouge, ce qui signifie que le mot de passe est faible et inacceptable, le jaune, ce qui indique que le mot de passe est moyen et acceptable, et le vert, ce qui signifie que le mot de passe est fort.

Étape 8. (Facultatif) Pour activer le vieillissement du mot de passe, cliquez sur la case d'option Modifier le mot de passe après ___ jours dans le champ Application du vieillissement du mot de passe. Si vous choisissez cette option, vous devrez modifier votre mot de passe après l'expiration du délai.

Gain de temps : Si vous choisissez Disable à l'étape 8, ce qui signifie que vous ne voulez pas que le mot de passe expire, passez à l'étape 10.

Étape 9. Entrez le nombre de jours avant l'expiration du mot de passe dans le champ Changer le mot de passe après ___ jours. La valeur par défaut est 180 jours.

Étape 10. Cliquez sur Save pour enregistrer les modifications.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.