Configuration de complexité de mot de passe sur les Points d'accès WAP121 et WAP321 de Cisco

Objectif

Une augmentation de complexité de mot de passe diminue le risque d'une brèche dans la sécurité. Les pirates informatiques peuvent habituellement fendre un mot de passe qui est moins de 8 caractères de longueur en quelques heures. Par conséquent il est essentiel que vous utilisiez de longs mots de passe avec une combinaison des lettres, des nombres, et des symboles de majuscule et minuscule.

Cet article explique la configuration de complexité de mot de passe sur les Points d'accès WAP121 et WAP321.

Périphériques applicables

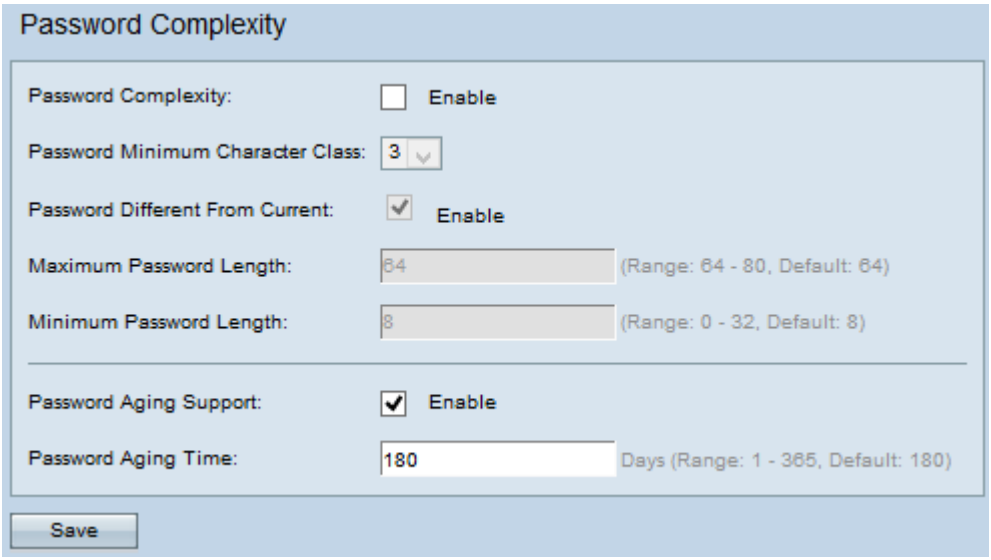
- WAP121
- WAP321

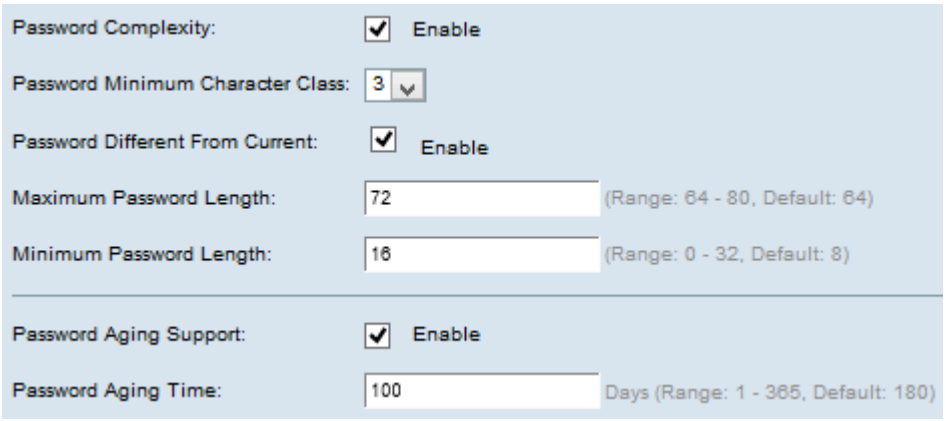
Version de logiciel

- 1.0.3.4

Configuration de complexité de mot de passe

Étape 1. Ouvrez une session à l'utilitaire de configuration Web et choisissez la **complexité de sécurité des systèmes > de mot de passe**. La page de *complexité de mot de passe* s'ouvre :





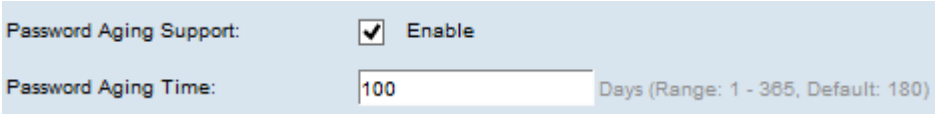
Étape 2. Enable de contrôle dans le domaine de complexité de mot de passe pour activer la complexité de mot de passe.

Étape 3. Choisissez le nombre minimal approprié de classes de caractères de la liste déroulante minimum de classe de caractères de mot de passe. Les lettres majuscules, les lettres minuscules, les nombres, et les caractères particuliers disponibles sur un clavier standard sont les quatre classes de caractères possibles.

Enable (facultatif) de contrôle d'étape 4. dans le mot de passe différent du champ en cours pour exiger de vous d'entrer un mot de passe différent quand le mot de passe en cours expire. Si désactivé, vous pouvez ressaisir le même mot de passe que vous avez utilisé plus tôt.

Étape 5. Écrivez le nombre maximal de caractères pour un mot de passe dans le domaine maximum de longueur du mot de passe. La plage est de 64 à 80.

Étape 6. Écrivez le nombre minimal de caractères qu'un mot de passe peut avoir dans le domaine minimum de longueur du mot de passe. La plage est de 0 à 32.



Enable (facultatif) de contrôle d'étape 7. dans le domaine de support de vieillissement de mot de passe afin du mot de passe à l'expire after un certain temps.

Étape 8. Si vous activiez le soutien du vieillissement de mot de passe dans l'étape précédente, écrivez le nombre de jours jusqu'à ce qu'un mot de passe expire dans le domaine de durée de vieillissement de mot de passe. La plage est de 1 à 365 jours.

Étape 9. **Sauvegarde de** clic pour sauvegarder les configurations.