Configuration de la complexité des mots de passe sur les points d'accès Cisco WAP121 et WAP321

Objectif

L'augmentation de la complexité des mots de passe réduit le risque d'une faille de sécurité. Les pirates peuvent généralement craquer un mot de passe de moins de 8 caractères en quelques heures. Il est donc essentiel d'utiliser des mots de passe longs avec une combinaison de lettres majuscules et minuscules, de chiffres et de symboles.

Cet article explique la configuration de la complexité des mots de passe sur les points d'accès WAP121 et WAP321.

Périphériques pertinents

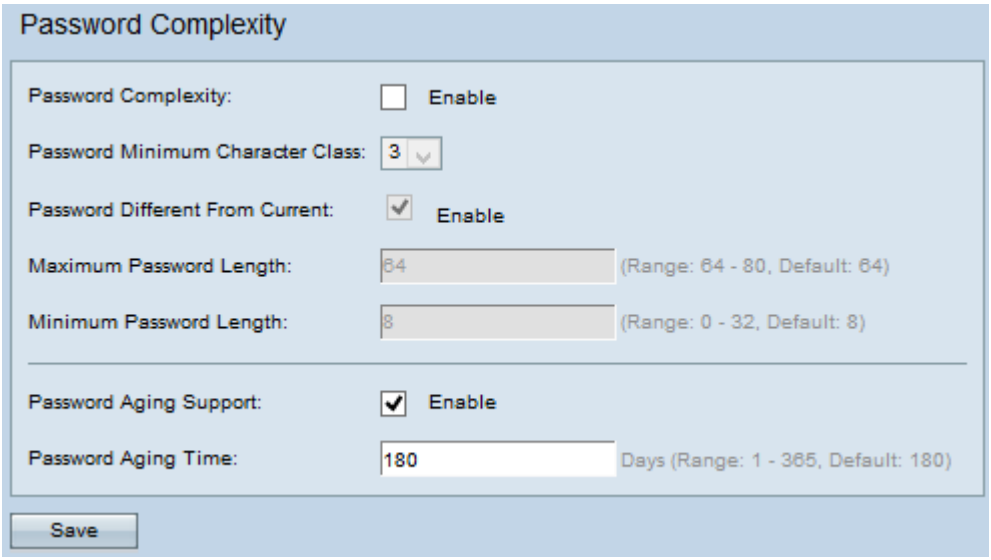
·WAP121
· WAP321

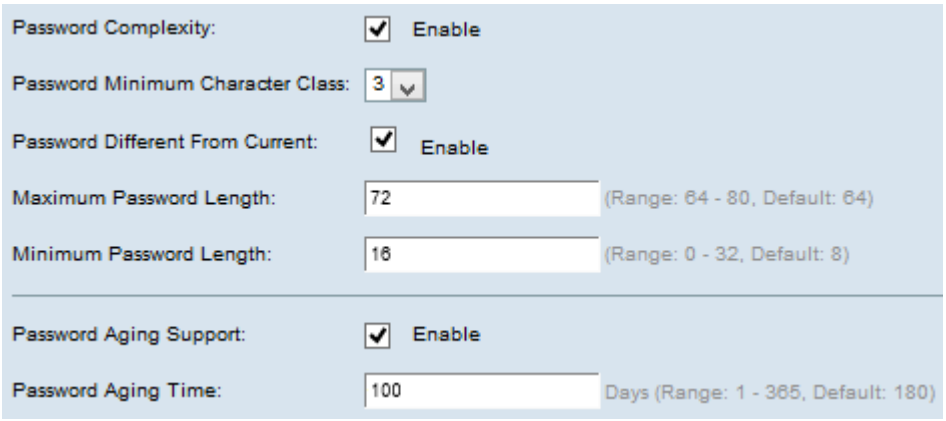
Version du logiciel

•1.0.3.4

Configuration de la complexité du mot de passe

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Sécurité du système > Complexité du mot de passe**. La page *Complexité du mot de passe* s'ouvre :





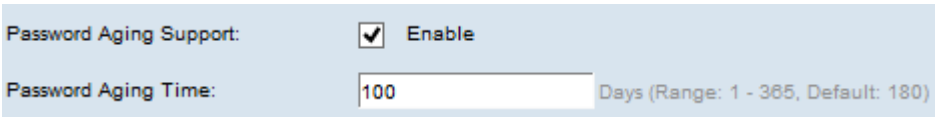
Étape 2. Cochez **Activer** dans le champ Complexité du mot de passe pour activer la complexité du mot de passe.

Étape 3. Choisissez le nombre minimum approprié de classes de caractères dans la liste déroulante Password Minimum Character Class. Les quatre classes de caractères possibles sont les majuscules, les minuscules, les chiffres et les caractères spéciaux disponibles sur un clavier standard.

Étape 4. (Facultatif) Cochez la case **Activer** dans le champ Mot de passe différent du champ Actuel pour exiger que vous saisissiez un autre mot de passe lorsque le mot de passe actuel expire. Si cette option est désactivée, vous pouvez saisir à nouveau le même mot de passe que celui que vous avez utilisé précédemment.

Étape 5. Saisissez le nombre maximal de caractères d'un mot de passe dans le champ Longueur maximale du mot de passe. Elle est située entre 64 et 80.

Étape 6. Saisissez le nombre minimal de caractères qu'un mot de passe peut contenir dans le champ Longueur minimale du mot de passe. Elle est située entre 0 et 32.



Étape 7. (Facultatif) Cochez **Enable** dans le champ Password Aging Support afin que le mot de passe expire après un certain temps.

Étape 8. Si vous avez activé la prise en charge de l'expiration du mot de passe à l'étape précédente, saisissez le nombre de jours jusqu'à ce qu'un mot de passe expire dans le champ Password Aging Time. La plage est comprise entre 1 et 365 jours.

Étape 9. Cliquez sur **Save pour enregistrer les paramètres.**