

Configuration de complexité de mot de passe sur les Points d'accès WAP551 et WAP561

Objectif

La sécurité du mot de passe augmente avec une augmentation de complexité de mot de passe. Il est essentiel que vous employiez de longs mots de passe avec une combinaison des lettres, des nombres, et des symboles de majuscule et minuscule pour mettre à jour la forte sécurité. La complexité de mot de passe est utilisée pour placer des conditions requises pour des mots de passe afin de diminuer le risque d'une brèche dans la sécurité.

Cet article explique la configuration de complexité de mot de passe sur les Points d'accès WAP551 et WAP561.

Périphériques applicables

- WAP551
- WAP561

Version de logiciel

- 1.0.4.2

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 :

Password Complexity

Password Complexity: Enable

Password Minimum Character Class: 3

Password Different From Current: Enable

Maximum Password Length: 64 (Range: 64 - 80, Default: 64)

Minimum Password Length: 8 (Range: 0 - 32, Default: 8)

Password Aging Support: Enable

Password Aging Time: 180 Days (Range: 1 - 365, Default: 180)

Save

Étape 2. Cochez la case d'**enable** 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 requises pour un mot de passe de la liste déroulante dans le domaine minimum de classe de caractères de mot de passe. Les classes incluent les lettres minuscules, les lettres majuscules, les nombres, et les caractères particuliers.

Password Complexity

Password Complexity: Enable

Password Minimum Character Class:

Password Different From Current: Enable

Maximum Password Length: (Range: 64 - 80, Default: 64)

Minimum Password Length: (Range: 0 - 32, Default: 8)

Password Aging Support: Enable

Password Aging Time: Days (Range: 1 - 365, Default: 180)

Étape 4. (facultative) pour exiger qu'un mot de passe différent est utilisé après que l'en cours expire, cochant la case d'**enable** dans le mot de passe différent du champ en cours. 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 8 à 32.

Étape 7. (facultative) pour le mot de passe à l'expire after un certain temps, cochant la case d'**enable** dans le domaine de support de vieillissement de mot de passe.

Étape 8. Si vous activez 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 terminer configurer la complexité de mot de passe.