Configurazione della complessità della password sui punti di accesso Cisco WAP121 e WAP321

Obiettivo

L'aumento della complessità delle password riduce il rischio di violazione della sicurezza. Gli hacker possono solitamente decifrare una password che ha meno di 8 caratteri in poche ore. È pertanto fondamentale utilizzare password lunghe con una combinazione di lettere maiuscole e minuscole, numeri e simboli.

In questo articolo viene illustrata la configurazione della complessità della password sui punti di accesso WAP121 e WAP321.

Dispositivi interessati

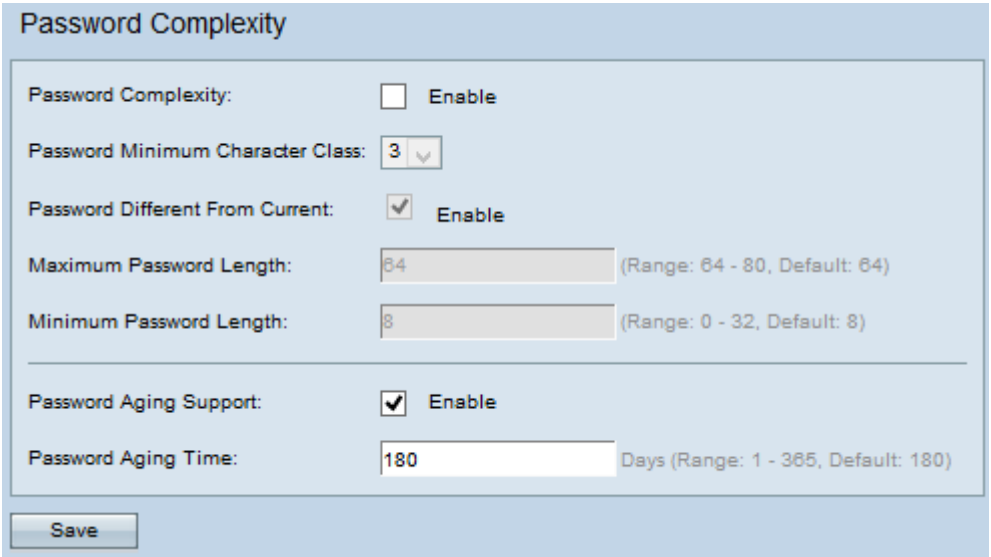
·WAP121
· WAP321

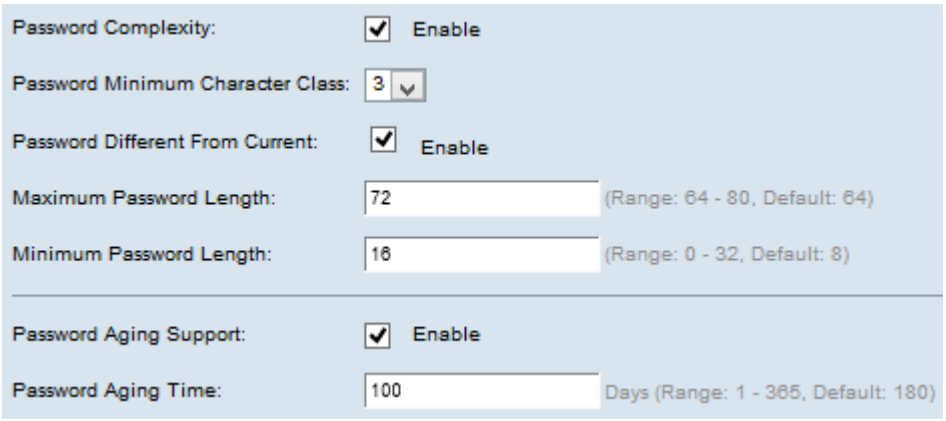
Versione del software

•1.0.3.4

Configurazione complessità password

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Sicurezza del sistema > Complessità della password**. Viene visualizzata la pagina *Complessità password*:





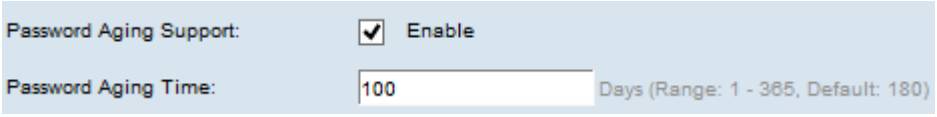
Passaggio 2. Selezionare **Abilita** nel campo Complessità password per abilitare la complessità della password.

Passaggio 3. Scegliere il numero minimo di classi di caratteri appropriato dall'elenco a discesa Classe di caratteri minima per la password. Le lettere maiuscole, le lettere minuscole, i numeri e i caratteri speciali disponibili su una tastiera standard sono le quattro classi di caratteri disponibili.

Passaggio 4. (Facoltativo) Selezionare **Abilita** nel campo Password diversa da quella corrente per richiedere l'immissione di una password diversa alla scadenza della password corrente. Se è disattivata, è possibile immettere nuovamente la stessa password utilizzata in precedenza.

Passaggio 5. Immettere il numero massimo di caratteri per una password nel campo Lunghezza massima password. L'intervallo è compreso tra 64 e 80.

Passaggio 6. Immettere il numero minimo di caratteri che una password può contenere nel campo Lunghezza minima password. L'intervallo è compreso tra 0 e 32.



Passaggio 7. (Facoltativo) Selezionare **Abilita** nel campo Supporto scadenzario password per fare in modo che la password scada dopo un determinato periodo di tempo.

Passaggio 8. Se nel passaggio precedente è stato abilitato il supporto per la misurazione durata password, immettere il numero di giorni fino alla scadenza della password nel campo Tempo di aging password. L'intervallo ammesso è compreso tra 1 e 365 giorni.

Passaggio 9. Fare clic su **Save** per salvare le impostazioni.