Password Complexity Configuration on the Cisco WAP121 and WAP321 Access Points

Objective

An increase in password complexity decreases the risk of a security breach. Hackers can usually crack a password that is less than 8 characters in length in a few hours. Hence it is vital that you use long passwords with a combination of upper and lower case letters, numbers, and symbols.

This article explains the password complexity configuration on the WAP121 and WAP321 access points.

Applicable Devices

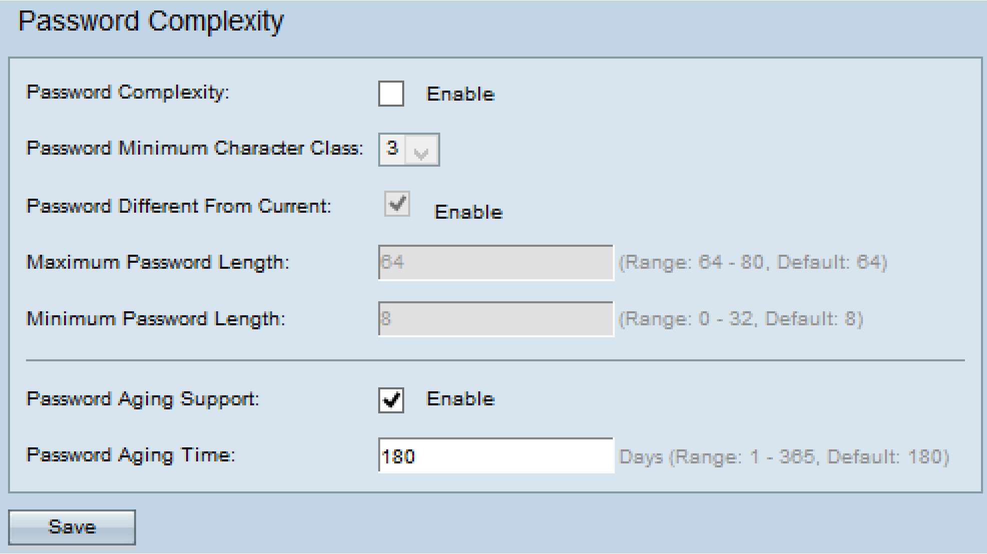
- WAP121
- WAP321

Software Version

- 1.0.3.4

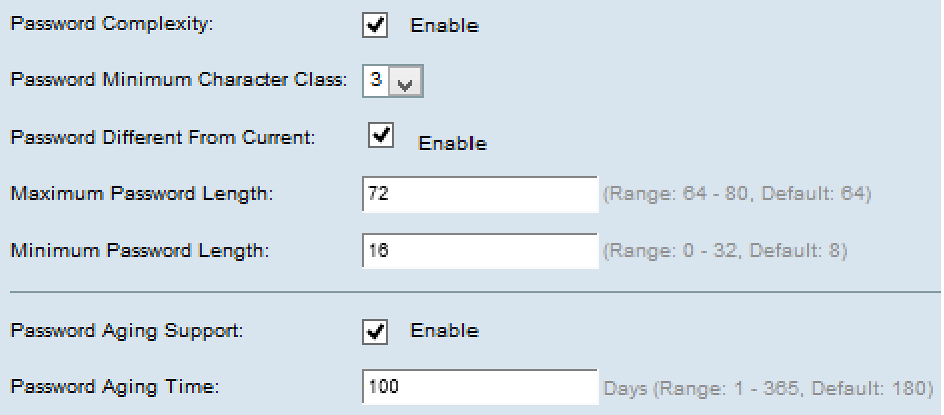
Password Complexity Configuration

Step 1. Log in to the web configuration utility and choose **System Security > Password Complexity**. The *Password Complexity* page opens:



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)



Password Complexity:	☑ Enable	
Password Minimum Character Class:	3	
Password Different From Current:	☑ Enable	
Maximum Password Length:	72	(Range: 64 - 80, Default: 64)
Minimum Password Length:	16	(Range: 0 - 32, Default: 8)
Password Aging Support:	☑ Enable	
Password Aging Time:	100	Days (Range: 1 - 365, Default: 180)

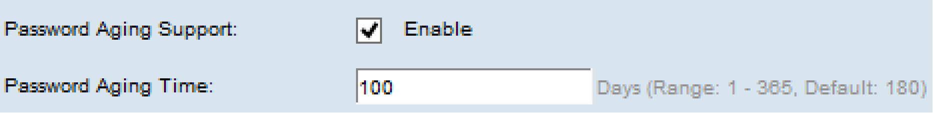
Step 2. Check **Enable** in the Password Complexity field to enable password complexity.

Step 3. Choose the appropriate minimum number of character classes from the Password Minimum Character Class drop-down list. Uppercase letters, lowercase letters, numbers, and the special characters available on a standard keyboard are the four possible character classes.

Step 4. (Optional) Check **Enable** in the Password Different From Current field to require you to enter a different password when the current password expires. If disabled, you can reenter the same password which you used earlier.

Step 5. Enter the maximum number of characters for a password in the Maximum Password Length field. The range is from 64 to 80.

Step 6. Enter the minimum number of characters that a password can have in the Minimum Password Length field. The range is from 0 to 32.



Password Aging Support:	☑ Enable	
Password Aging Time:	100	Days (Range: 1 - 365, Default: 180)

Step 7. (Optional) Check **Enable** in the Password Aging Support field in order for the password to expire after a certain time.

Step 8. If you enabled support for password aging in the previous step, enter the number of days until a password expires in the Password Aging Time field. The range is from 1 to 365 days.

Step 9. Click **Save** to save the settings.