Configuring Password Complexity for the WAP131, WAP150, WAP351, WAP361, WAP371, and WAP571

Objective

The Password Complexity page is used to modify the complexity requirements for passwords used to access the configuration utility. Complex passwords increase security.

The objective of this document is to explain how to configure Password Complexity on the WAP131, WAP150, WAP351, WAP361, WAP371, and WAP571 Access Points.

Applicable Devices

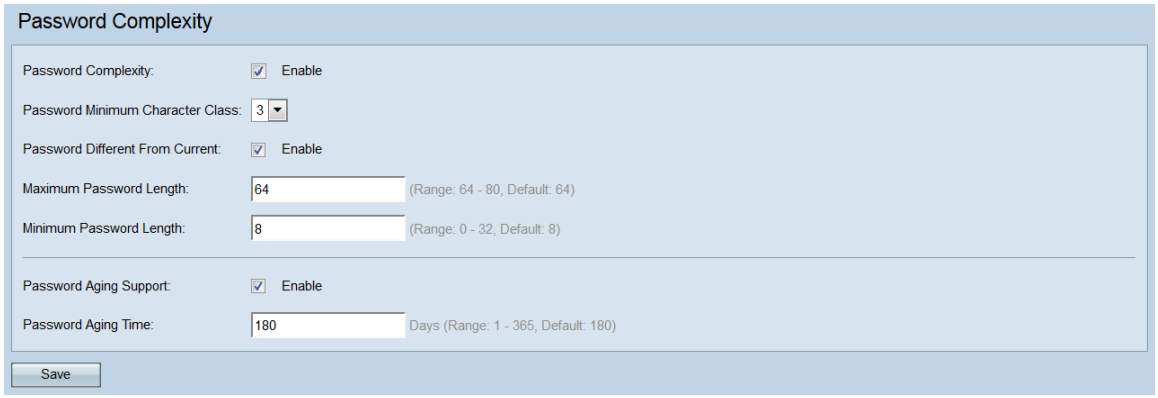
- WAP131
- WAP150
- WAP351
- WAP361
- WAP371
- WAP571

Software Version

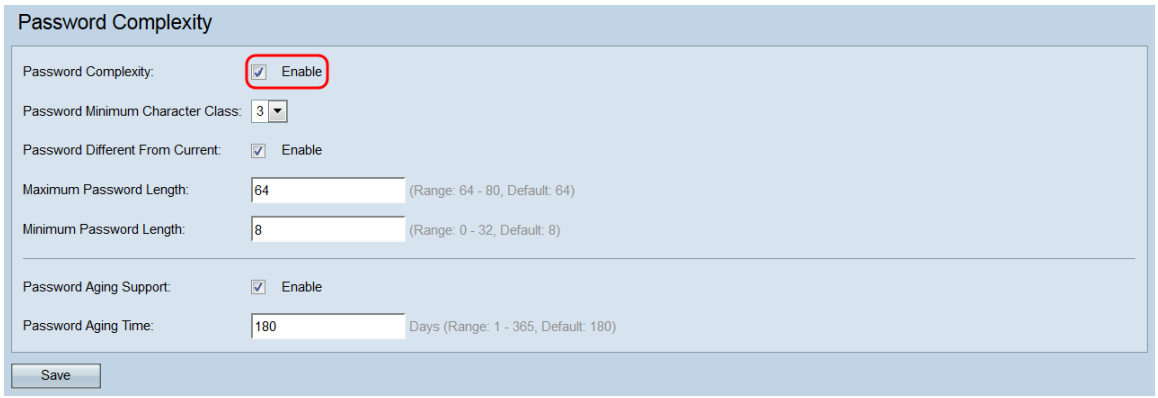
- 1.0.2.15 (WAP131, WAP351)
- 1.1.0.9 (WAP150, WAP 361)
- 1.3.0.6 (WAP371)
- 1.0.1.12 (WAP571)

Configuring Password Complexity

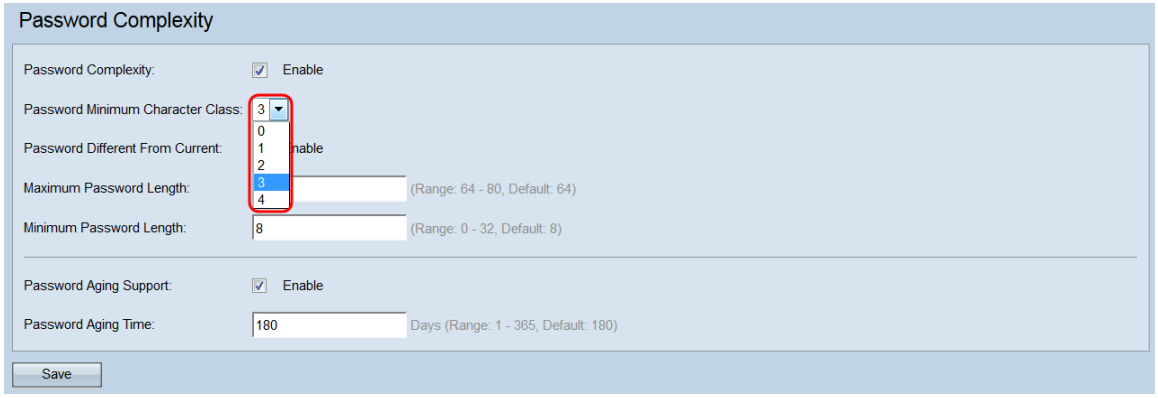
Step 1. Log in to the web configuration utility and choose **System Security > Password Complexity**. The *Password Complexity* page opens:



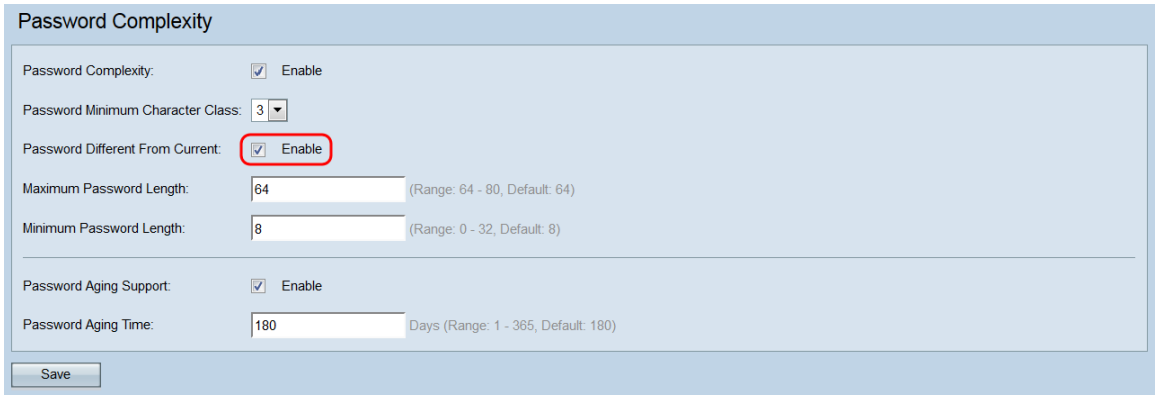
Step 2. Check the **Enable** checkbox in the *Password Complexity* field to enable password complexity. If you do not want to enable password complexity, uncheck the checkbox and skip to Step 7. It is checked by default.



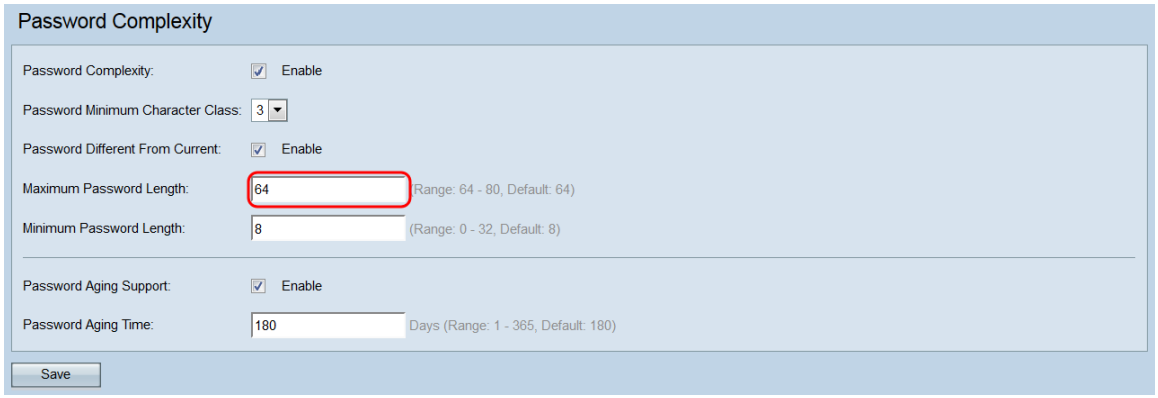
Step 3. In the *Password Minimum Character Class* drop-down list, select the minimum number of character classes that must be represented in the password string. These possible classes are uppercase letters, lowercase letters, numbers, and special characters. The default is 3.



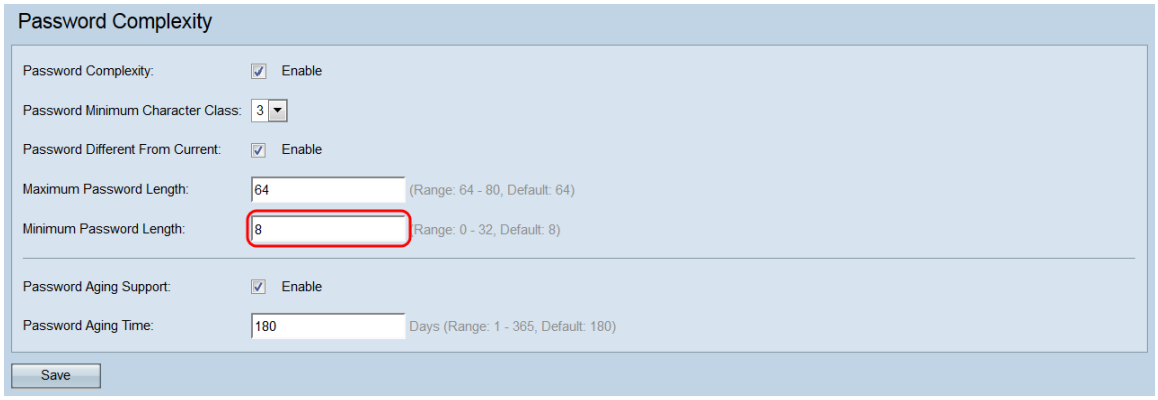
Step 4. In the *Password Different From Current* field, check the **Enable** checkbox if you want users to enter a different password than their current password when it expires. Unchecking this allows users to reuse the same password when it expires. It is checked by default.



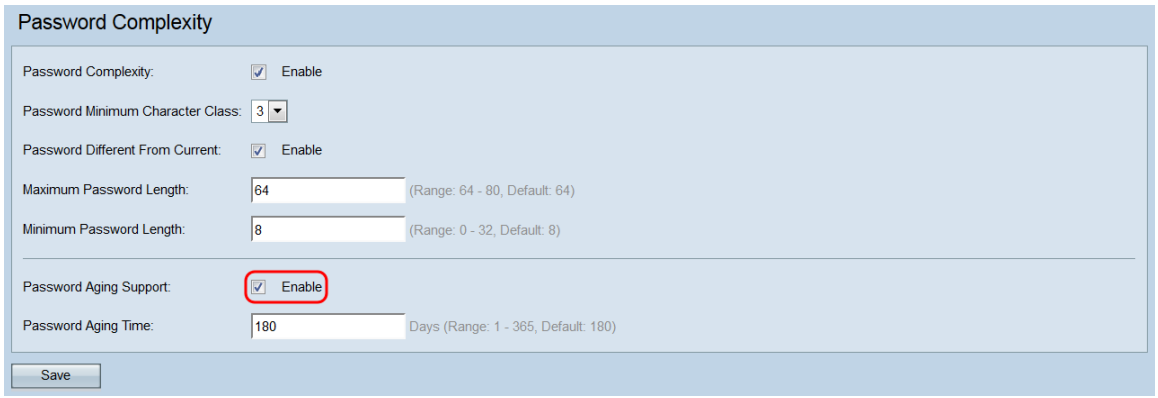
Step 5. In the *Maximum Password Length* field, enter in the maximum number of characters a password can be. The range is 64 – 80, and the default is 64.



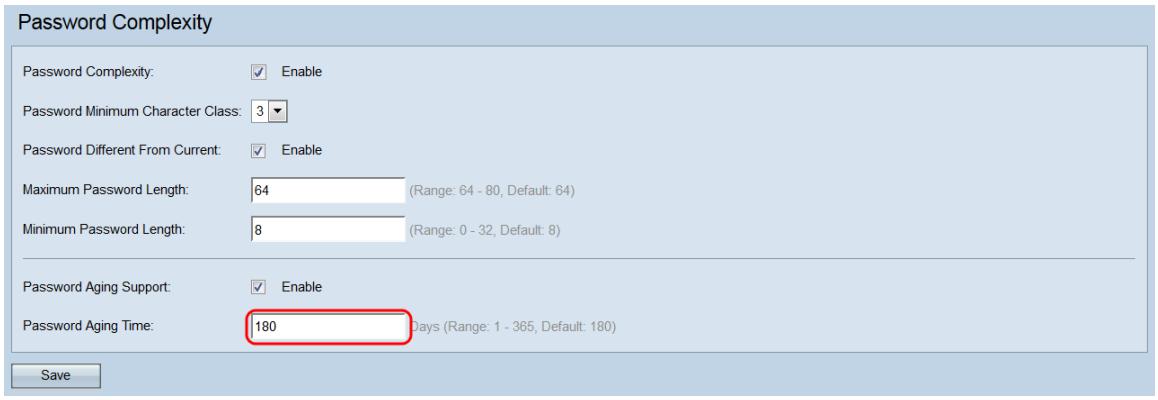
Step 6. In the *Minimum Password Length* field, enter in the minimum number of characters a password can be. The range is 0 – 32, and the default is 8.



Step 7. In the *Password Aging Support* field, check the **Enable** checkbox to have passwords expire after a set time period. If you do not want passwords to expire, uncheck this checkbox and skip to Step 9. It is checked by default.



Step 8. In the *Password Aging Time* field, enter in the number of days before a new password expires. The range is 1 – 365, and the default is 180.



Step 9. Click **Save** to save your changes. You will be logged out of the web configuration utility, and must re-enter the new login information to regain access.