

siterra | Knowledge Base Article

Users & Security - How to Enable the Enhanced Password Policy

Siterrra's standard password policy requires that a user's password be at least six characters long, and that the password must be different from the user name.

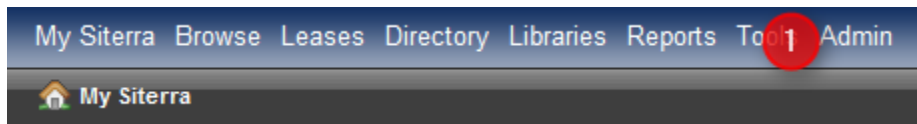
If additional password security is required, the enhanced password policy can be enabled. This requires strong passwords by enforcing the following rules.

- Password must be at least eight (8) alphanumeric characters long
- Password must contain both upper (e.g., A,B,C,Z) and lower case (e.g., a,b,c,z) Letters
- Password must also contain digits (e.g., 0,1,2,9)
- Password must also contain punctuation characters (e.g., !@#\$%^&*()_+~-'{}[]:<>?,./)
- Password must be different from the user name

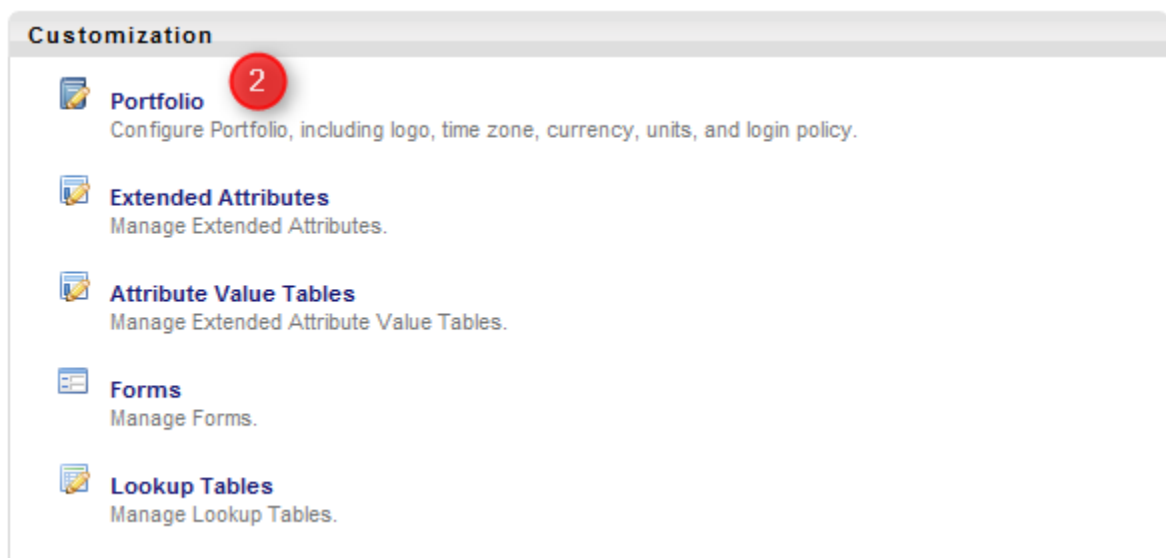
Changing the Password Policy:

You must be logged in as an administrator in order to perform this procedure.

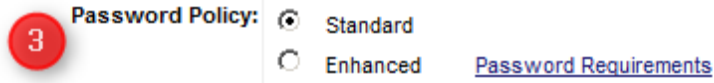
1. From the Siterrra home page, select Admin (1).



2. In the Customization section, select Portfolio (2).



3. Change the Password Policy from Standard to Enhanced (3).



4. Scroll to the bottom of the page, and select OK (4) to save the change. When users next change their passwords, they will be required to use strong passwords.

