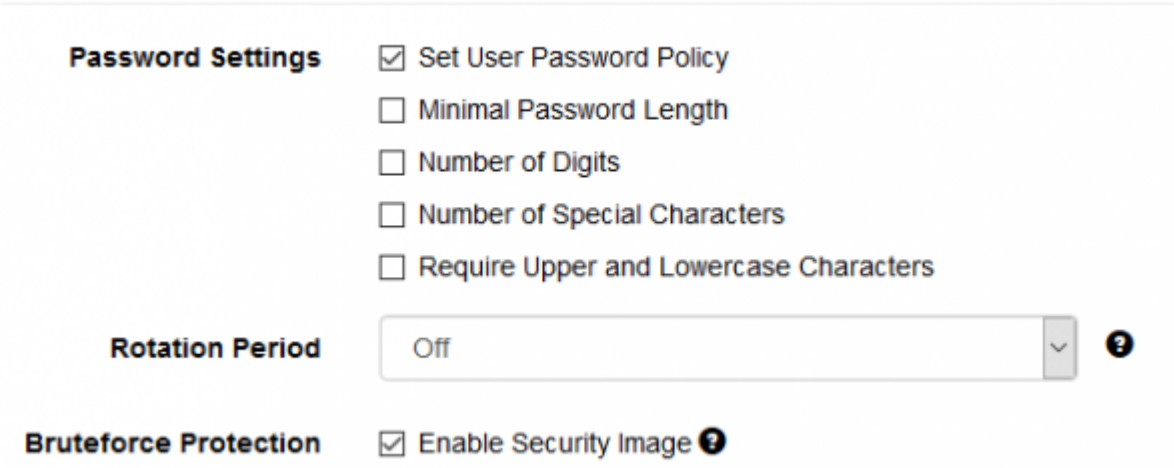
Password Policy

A password policy is a set of rules designed to force users to employ strong passwords and use them properly. In LUCY you can configure the password policy under the advanced settings:

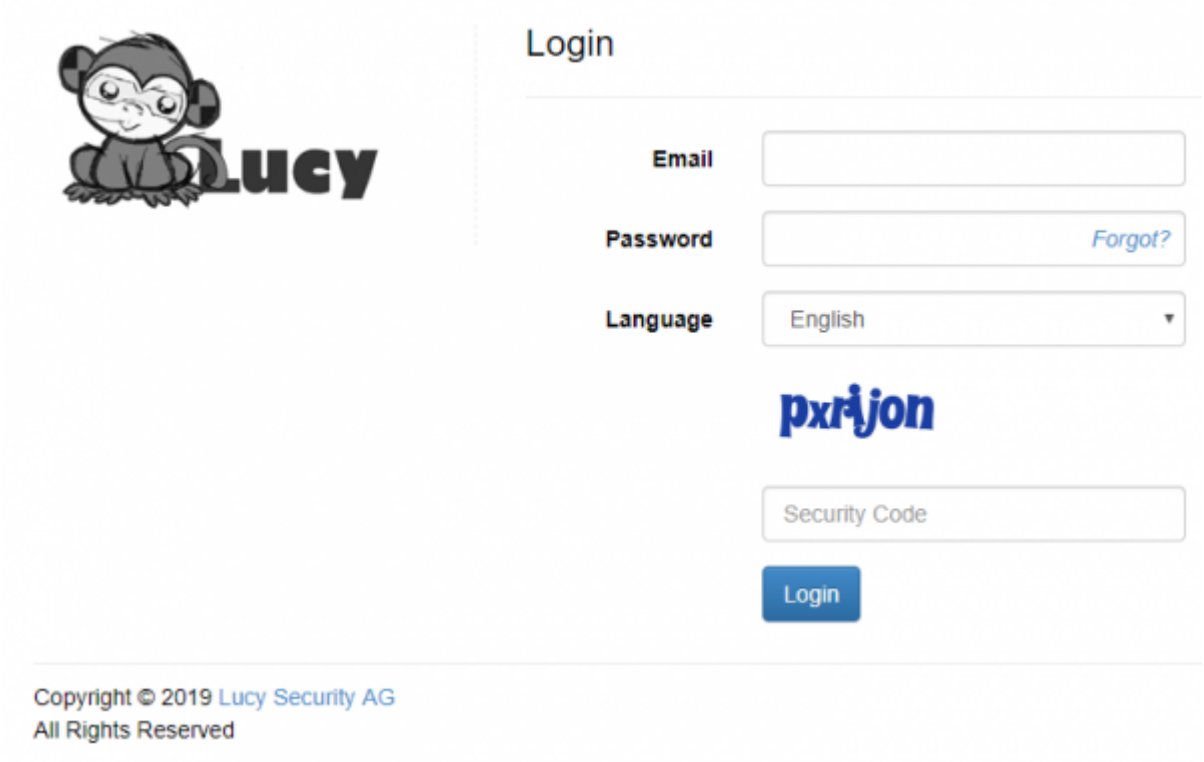


You can define the following settings:

- Enable password policy for all LUCY users
- Set a minimal password length
- Require Digits within the password and set the number of required digits
- Require Special Characters within the password and set the number of required Special Characters
- Require Upper and Lower Case Characters within the password
- Rotation period: force the user to change the password after a custom time frame

Brute Force Protection

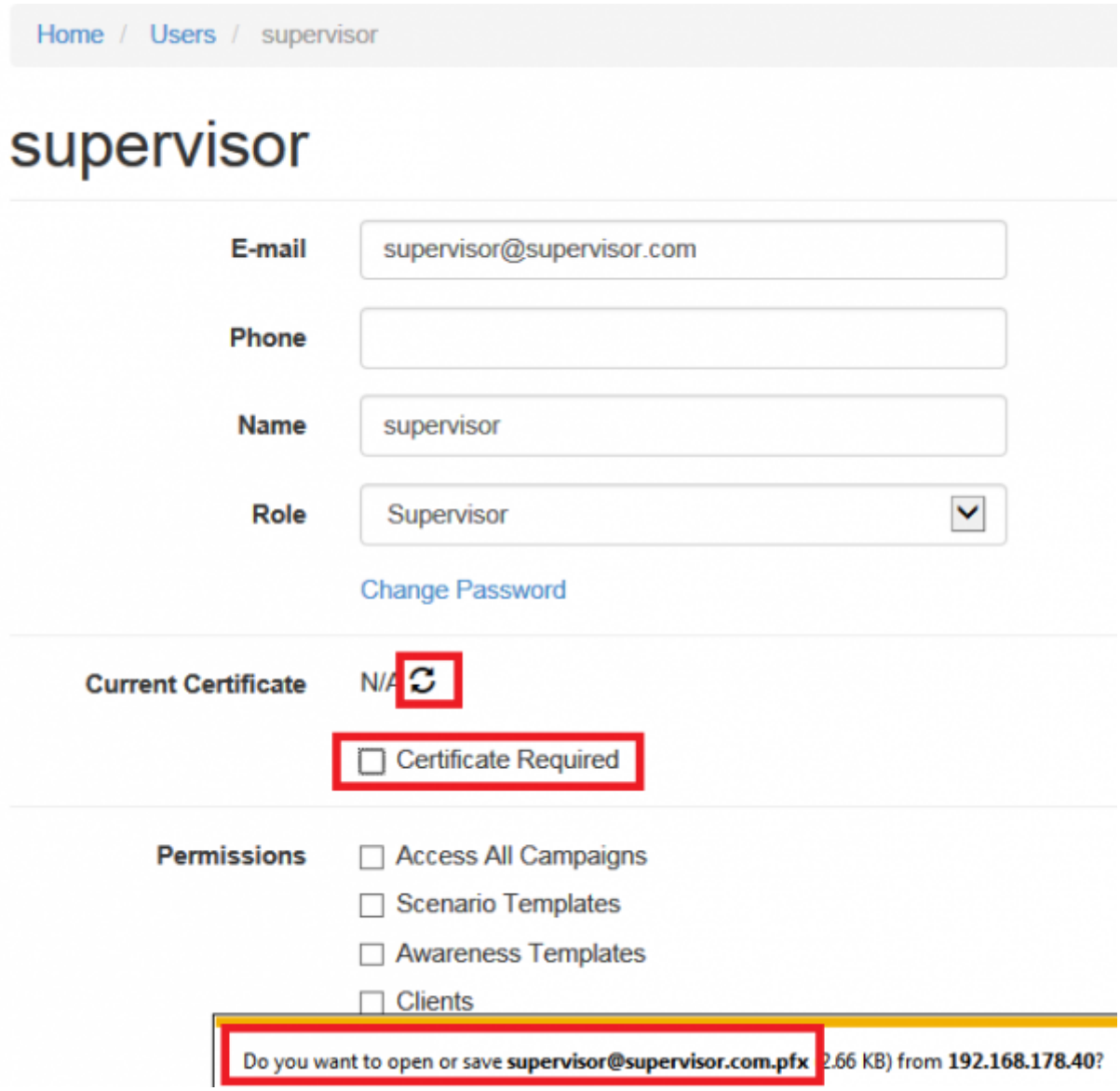
If you enable the security image within the login page the user will have to enter a captcha text together with his login which will protect the login from automated login attempts (see https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks).



Strong Authentication (Certificate Based)

Certificate-based authentication is the use of a Digital Certificate to identify a user, machine, or device before granting access to a resource, network, application, etc. In the case of user authentication, it is often deployed in coordination with traditional methods such as username and password.

In order to enable certificate-based authentication for a LUCY user, you need to go into the user management (in settings) and within the specific user you have to enable the checkbox "certificate required". Before creating the certificate you need to save the changes. Once you enabled this setting you have to click on the certificate generation icon. After a few seconds, you will be able to download the certificate.



From:
https://wiki.lucysecurity.com/ - **LUCY**

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=password_policies_login_protection_strong_authentication&rev=1562145994

Last update: **2019/07/25 12:50**