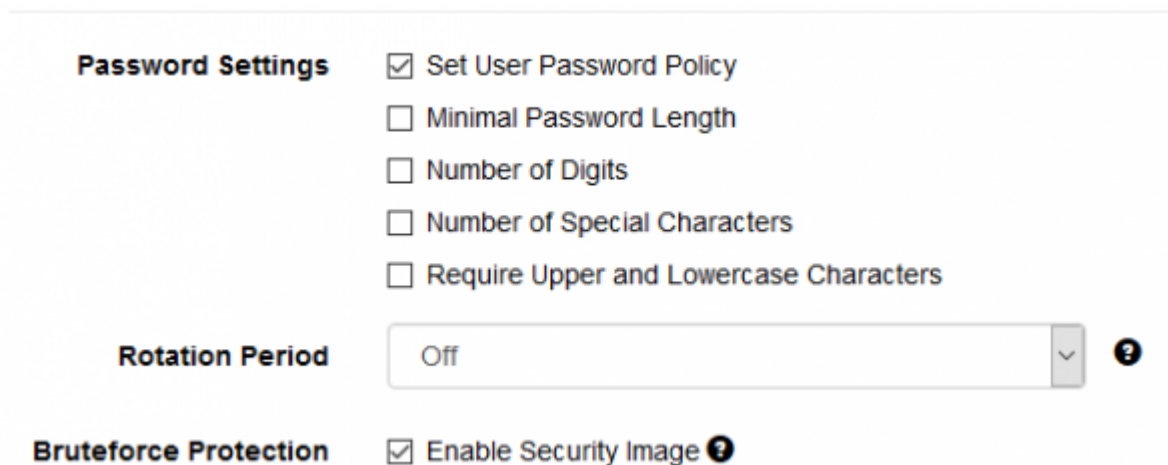




Password Policy

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:



The screenshot shows a configuration panel for Password Policy. It has three sections: 'Password Settings', 'Rotation Period', and 'Bruteforce Protection'. Under 'Password Settings', there are five checkboxes: 'Set User Password Policy' (checked), 'Minimal Password Length' (unchecked), 'Number of Digits' (unchecked), 'Number of Special Characters' (unchecked), and 'Require Upper and Lowercase Characters' (unchecked). The 'Rotation Period' section has a dropdown menu set to 'Off' and a help icon. The 'Bruteforce Protection' section has one checkbox 'Enable Security Image' which is checked and has a help icon.

Password Settings	<input checked="" type="checkbox"/> Set User Password Policy
	<input type="checkbox"/> Minimal Password Length
	<input type="checkbox"/> Number of Digits
	<input type="checkbox"/> Number of Special Characters
	<input type="checkbox"/> Require Upper and Lowercase Characters
Rotation Period	Off 
Bruteforce Protection	<input checked="" type="checkbox"/> Enable Security Image 

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).



Login

Email

Password

[Forgot?](#)

Language

English ▼

pxrjon

Security Code

Login

Copyright © 2019 Lucy Security AG
All Rights Reserved

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.

supervisor

E-mail

supervisor@supervisor.com

Phone

Name

supervisor

Role

Supervisor

▼

[Change Password](#)

Current Certificate

N/A 

☐ Certificate Required

- Permissions
- ☐ Access All Campaigns

☐ Scenario Templates

☐ Awareness Templates

☐ Clients

Do you want to open or save **supervisor@supervisor.com.pfx** (2.66 KB) from **192.168.178.40**?

From:
<https://wiki.lucysecurity.com/> - LUCY

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

Last update: 2019/07/25 12:49

