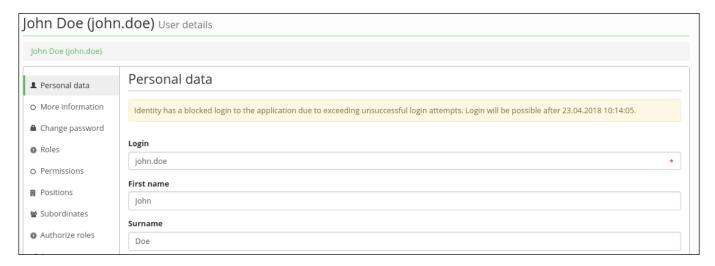# A temporary login block after X unsuccessful login attempts

In order to prevent CzechIdM from brute force attacks, you can use a feature for blocking login after X unsuccessful login attempts. The feature can be set only for a **default validation password policy**.

When a user has exceeded the **Maximum number of unsuccessful login attempts**, the user is blocked for a specified number of seconds (**Login blocking time (seconds)**). When a block has occurred, a notification is sent to the user regarding the block instance (topic: **loginBlocked**). If a user still tries to log in after the block has been activated, the block time isn't increased. The interval remains the same. Once the blocking time has elapsed, the user can then log in.
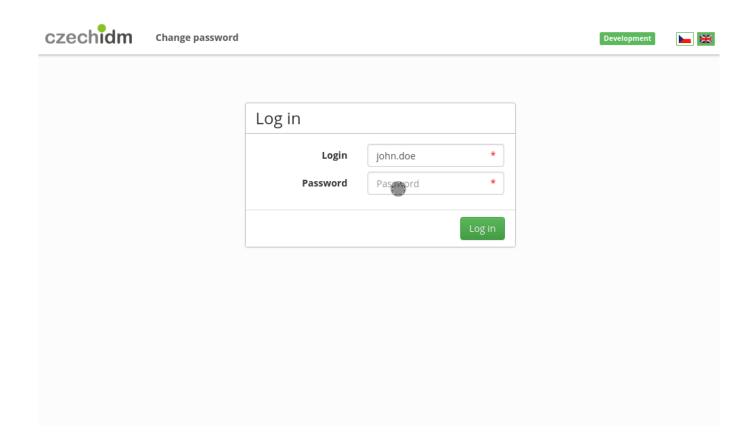
Information about the block is shown in the user's detail.

A user was populated from a connected system and doesn't have a password in IdM, authentication is done through this system, will this feature still work for such a user?

Yes. When a user tries for the first time to log in to IdM, an empty password object is created for the user. It is this object that will collect information about any respective unsuccessful login attempts.

Block example

czechidm **Change password**   Development 🇨🇿 🇬🇧

Log in

Login	john.doe	*
Password	Password	*

Log in

From:
https://wiki.czechidm.com/ - **CzechIdM Identity Manager**

Permanent link:
https://wiki.czechidm.com/tutorial/adm/block_user_unsuccessful_login_attemps?rev=1548143810

Last update: **2019/01/22 07:56**