Password expiration

Password aging is in place with the LDAP password database for both Linux and Windows. For the sake of security, it is recommended to change important passwords on a regular basis. In our system, the password expiration time is set for 1 year. Ten days before your password expires, you will begin getting reminders when you log in, telling you to change your password within x days. This will give you some time to think about a new password which is not too hard to remember, and change it at a convenient moment during those 10 days.

Why?

User passwords are one of the weakest points in system security, especially if the same password is used elsewhere on other systems or websites that may get compromised. Changing the password from time to time does not eliminate this threat, but at least it limits the timeframe of vulnerability.

How?

To change your password, use the command 'passwd' on Linux. On windows, press ctrl-alt-delete and from the box that appears, select the 'Change Password' button. The new password should be sufficiently different from the previous one, and it should be a safe mixture of letters and other characters. Note also that passwords are case-sensitive.

Additional benefit

For those of you who have not yet changed their password since the transition to LDAP, changing the password has the additional benefit that your new password will then also work on Windows, e.g. for Terminal Services (winclient) and access on the scanner computer in room 511.

From:
<https://helpdesk.strw.leidenuniv.nl/wiki/> - **Computer Documentation Wiki**

Permanent link:
https://helpdesk.strw.leidenuniv.nl/wiki/doku.php?id=password_expiration

Last update: **2017/11/27 10:33**