Password Security and Configuration options

Last Modified on 19/04/2022 4:30 pm ACST

CareRight supports a number of security features with user authentication. Note, many of these can be configured to your organisational policies - discuss with us your specific requirements.

Feature	Description
SAML	The ability for a SAML identity provider to be configured, for user authentication. System Administration > Users and Groups > SAML
LDAP	The ability for an LDAP server to be configured, for user authentication. System Administration > Users and Groups > LDAP
Password Complexity	A password policy to ensure the use of special characters, varied case and alphanumeric characters. Recommend: **1 lower 1 numberic 1 special 1 upper.** System Administration > Users and Groups > LDAP
Password Expiry	Time in days/months for password expiry. Recommended **2 months**. System Administration > Global Settings > Read Only Settings
Password Minimum Length	A minimum length of password the users are required. Recommended: **8** System Administration > Global Settings > Read Only Settings
Password Maximum Attempts	The maximum number of failed login attempts before an account is temporarily locked. Defaults to **20**.
Account locking	See Unlock a User Account
Password History	Allows or disallows reuse of old passwords. Recommended setting is **Disallow** and remembering the **last 2 passwords**. System Administration > Global Settings > Read Only Settings