About usernames, passwords and expiry dates

If you create accounts manually, you need to know about the makeup of usernames and passwords so you don't get slowed down by having them rejected by the system.

About usernames

Usernames must be unique and are not case sensitive when you or your account holders enter them. They are always displayed in lower case.

They must be at least 6 characters long and can be as long as 20 characters. All usernames will start with a prefix unique to your organisation. If you use any form of automated account creation, such as self-registration or bulk upload, usernames will be in a predictable format.

If you are allowing email addresses to be used as usernames, then the email addresses will also need to be unique.

About passwords

Password length must be between 8 and 20 characters and contain a mix of letters and characters that are not letters.

Passwords are case sensitive.

Passwords cannot:

- be the same as the username,
- contain series of ascending or descending characters
- contain strings known by hackers to be commonly used such as 'password' or 'letmein'

Passwords can:

- use characters from this list:
    - A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z 1 2 3 4 5 6 7 8 9 0 ! " £ $ % ^ & * ( ) - =_+[ ] { } ; ' # : @ ~ , . / < > ? \ |

For the best security, your own passwords should be difficult to guess but easy for you to remember and as lengthy as you can comfortably manage within the constraints.

The best policy is for users to always set their own passwords, but this is not always possible. In those cases you should avoid (so far as is practical):

- using the same password each time
- basing them on personal information such as
    - names,
    - emails,
    - birthdays, or
    - published or predictable patterns.

The safest way to reset user passwords is to trigger an activation email and let the account holder do it themselves.

About expiry dates

The account becomes expired ON the expiry date - i.e. it does not allow the user to log in on the expiry date. The same is true of any other types of expiry date that may be in use by your organisation's schema such as eligibility expiry or permission set expiry.

Expiry reminder emails, if enabled, are sent 30 and 15 days before expiry.

See also:

- About field sizes