TECHNICAL SERIES

QUALIFY PASSWORD SETTINGS

Original Software

JUSTIN MCDOUGALL

OCTOBER 2021

BERTIE RELEASE

TABLE OF CONTENTS

SYNOPSIS

Native Qualify resources are required to have a password, this password is encrypted and stored in the database.

This document explains the password requirements and demonstrates the functionality to force password resets at specific intervals and set the number of incorrect login attempts before locking the account.

QUALIFY PASSWORDS

Qualify only holds passwords for native Qualify resources, if you are utilising LDAP single sign-on the Active Directory password policy will dictate password use.

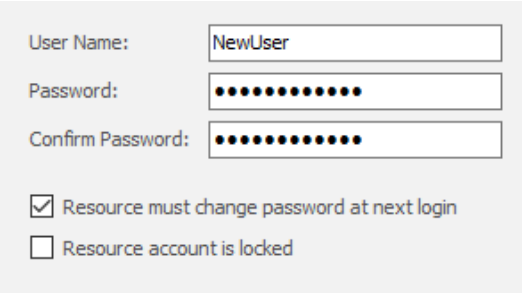
Password Requirements

Qualify passwords must be a minimum of 8 characters in length, contain a minimum of 1 uppercase, lowercase, number and special character.

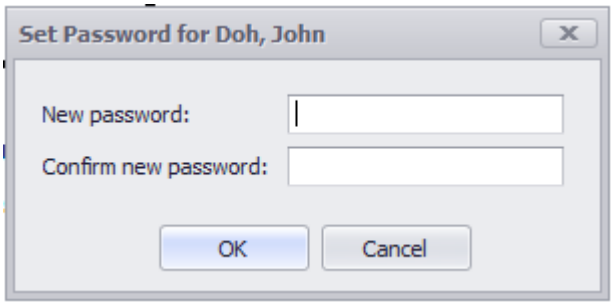
Setting Initial Passwords

When setting up a user you would normally want to keep the user's password secure. This can be achieved by forcing the user to set their password at first login.

When creating the resource, set the password and select the 'Resource must change password at next login'



They will then be forced to set a password before first connecting to Qualify.



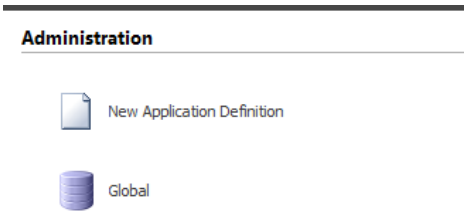
CONFIGURING PASSWORD POLICY

By default, the password complexity is hardcoded and cannot be changed. The ability to configure and force a user to change their password is configurable alongside invalid login attempts.

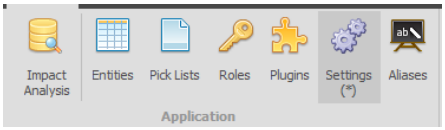
Password Global Settings

You can configure the frequency a user is forced to change their passwords. By default, a user is never forced to change their password once set. You can also specify the invalid login attempts before the resource is locked out, by default this is also not set.

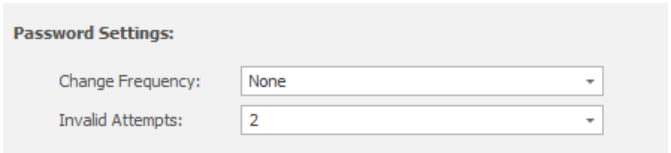
1. Log in to Qualify as a user with administrative permissions
2. From the front screen select 'Management', under Administration select the 'Global' Icon.



3. From the top menu bar, select 'Settings'

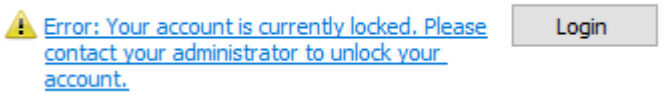


Scroll down and find 'Password Settings', change as desired.



RESETTING A LOCKED ACCOUNT.

If a user exceeds the 'Invalid Attempts', they will be presented with the following message.



A user with administrative permissions will be required to unlock the user.

Selecting the Resource record for the user that is locked out, the Resource locked flag will need to be reset.