

CREATING USERS AND ALLOCATING PERMISSIONS



Original Software



JUSTIN MCDUGALL

AUGUST 2021

BERTIE 4

TABLE OF CONTENTS

Table of Contents	2
Synopsis	3
Creating Qualify Users and Allocating Permissions	4
Initial Install.....	4
Setting Password Rules for Qualify Resources.....	5
Creating LDAP Single Sign-on Resources	6
LDAP Single Sign-on Setup Set Up	6
Creating Qualify Native Resources	7
Creating Native Resources.....	7
Qualify Permissions	9
Security Roles	9
Allocating Permissions to Resources.....	12
Allocating Global Permission.....	12
Allocating Application Definition Permissions	12
Allocating Instance Level Permissions	13



SYNOPSIS

After initially installing Qualify you will only have the Administrator account on the system. This document shows how to set up users on the system and allocate permissions to assets and functionality.

This document discusses setting up both Native Resources and LDAP single sign-on Resources.

CREATING QUALIFY USERS AND ALLOCATING PERMISSIONS

INITIAL INSTALL

The initial install of Qualify will create one user, this is a Qualify resource with relevant permissions to set up the system including creating new resources.

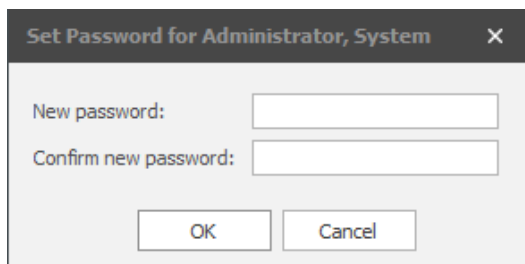
You will need to log into the Qualify Client to create and manage users, this cannot be performed via Qualify Web

To log in after the installation you will need to use the following credentials:

Login: Administrator

Password: Password

At this point you will be prompted to set the Administrator password, this needs to be at least 8 characters long, with mixed upper and lower case characters and at least one special character.



The screenshot shows a dialog box titled "Set Password for Administrator, System" with a close button (X) in the top right corner. Inside the dialog, there are two text input fields. The first is labeled "New password:" and the second is labeled "Confirm new password:". Below these fields are two buttons: "OK" and "Cancel".


SETTING PASSWORD RULES FOR QUALIFY RESOURCES

For Qualify Resources, you can set the frequency the password is required to be changed and how many incorrect attempts, before the account is locked.

To set the rules, perform the following:

1. Log on to the Qualify client with a user with administrative permissions
2. From the Management menu, open the Global settings

Administration

 New Application Definition

 Global

3. From the top menu bar, select the 'Settings', here you can set 'Change Frequency' and 'Invalid Attempts'

Password Settings:

Change Frequency:

Invalid Attempts:

- a. **Change Frequency:** This is the period the user is forced to change their password.
 - b. **Invalid Attempts:** This number sets the number of incorrect passwords that can be entered before locking the account.
4. Save the changes and restart Qualify to pick up the changes.

CREATING LDAP SINGLE SIGN-ON RESOURCES

For the Qualify Client, you can set up single-sign-on authentication. This will utilise the logged on Windows user to access Qualify.

Currently, this will not work on Quaify Web, if you intend a user to access both the Client and the Web versions of Qualify, then the LDAP setup will not be suitable. However, you can have a mixture of LDAP and Qualify Resources on the system if you desire.


With the LDAP set up, the management of the resource, password policy creation of the resource record is controlled by the Active Directory Server.

LDAP Single Sign-on Setup Set Up

To configure LDAP:

1. Log on to the Qualify client with a user with administrative permissions
2. From the Management menu, open the Global settings

Administration

 New Application Definition

 Global

3. From the top menu bar, select 'Settings', In the LDAP Server Settings area, the following need populating:
 - a. **Server Address:** IP address or DNS name of the LDAP server
 - b. **Root Container:** Domain Name for the LDAP server, you will need the LDAP Admin to tell you what this is e.g. CN=OriginalSoftware,CN=com for OriginalSoftware.com
 - c. **User Name:** AD account that has Query rights on the Active Directory or (DC=OriginalSoftware,DC=com for OriginalSoftware.com)
 - d. **Password:** Password for the AD account above
4. Once populated, select the 'Get LDAP Groups' button, this will populate the 'Group' drop-down box allowing you to select the desired group.
5. Save the changes and restart Qualify to pick up the changes.

Once Qualify has restarted, you will be able to see and select the new users from the 'Resource' menu

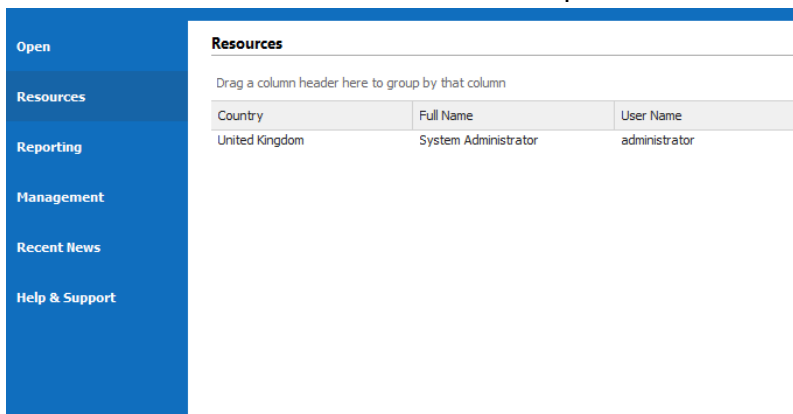
CREATING QUALIFY NATIVE RESOURCES

The native resource exists within the Qualify instance and is required to be managed within the Qualify Client. The Qualify Resource has no intrinsic permissions and these are required to be set before the login can be used.

Creating Native Resources.

To create a new Resource

1. Log in to the Qualify Client with the Administrator credentials
2. From the left menu select 'File' from the top menu followed by 'Resources'



3. Within the white space of the 'Resources' pane, 'right mouse click' and select 'Add' the following Screen is displayed.

Add Resource

Details | Roles | Holidays | Working Days | Working Hours

First Name:

Last Name:

Email Address:

Country:

Job Title:

Cell/Mobile:

User Interface:

User Name:

Password:

Confirm Password:

Resource must change password at next login

Resource account is locked

Notes:

OK Cancel

- a. **First Name:** This is a required field

- b. **Last Name:** This is a required field
- c. **Email Address:** This is not a required field, however, if you plan to utilise the email functionality this should be populated.
- d. **Country:** This is a required field, the Country is used for Resource Management and allows a default setting of working days and hours alongside holidays. If you are not planning on using Resource Management, then the choice would have no effect. If you would like to add a new country, this can be complete from the administration menu then select. Countries', a 'Right Mouse Click' will allow you to add a new country.
- e. **Job Title:** This is not a required field, however, is used when displaying user information with Qualify
- f. **Cell/Mobile:** This is not a required field, however, is used when displaying user information with Qualify
- g. **User Interface:** This is set to either:
 - i. **Standard:** This is the standard view of the application
 - ii. **Tile View:** This is the simplified Tile View
- h. **User Name:** This is the login information the resource will use to access Qualify.
- i. **Password:** The is the password required to log in, it will need to be 8 characters or longer with a mixture of upper and lower case and a special character.
- j. **Resource must change password at next login:** With this selected when the user first logs in, they will be forced to change their password. This means that the security is maintained, once the user has logged onto the system, only they will know the password.
- k. **Resource account is locked:** To keep a full audit of actions on the system, we prevent a user from being deleted. Checking this setting will lock the account.

QUALIFY PERMISSIONS

Once a resource record is created via LDAP or as a native resource, it will have no permissions to utilise any functionality within Qualify. This will need to be allocated before the user login in.

As security roles are specific to your Application Definition and system, they may differ from the examples shown in this document.

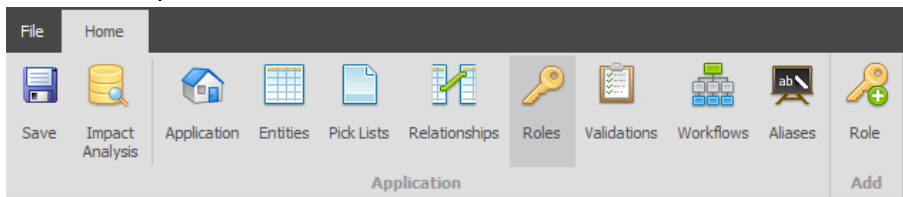
Security Roles

A security role is set at the Application Definition level or within the Global settings, the security role is allocated functional permissions, with resources being allocated that security role. Security Roles and inclusive, if a user is a member of multiple security roles they will have permissions for the set of security roles.

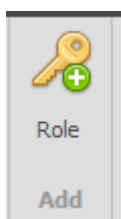
At the Application Definition level, the Security role is allocated to any Entities with relevant permission for that Entry set.

TO CREATE A SECURITY ROLE WITHIN THE APPLICATION DEFINITION

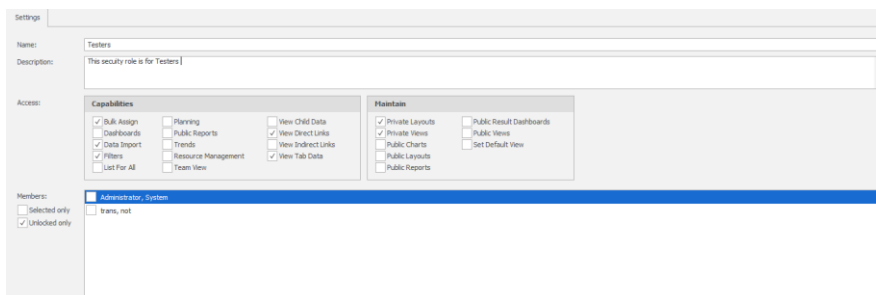
1. Log in to Qualify as the Administrator or a user with permissions to edit the Application Definition
2. From the top ribbon bar, select 'Roles'



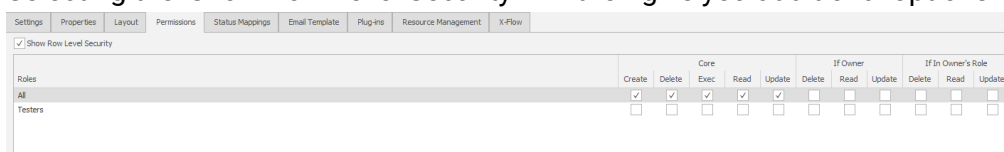
3. Here you can amend a current security role, or create a new security role. To add a new Security Role select the 'Add' menu item from the top menu bar.



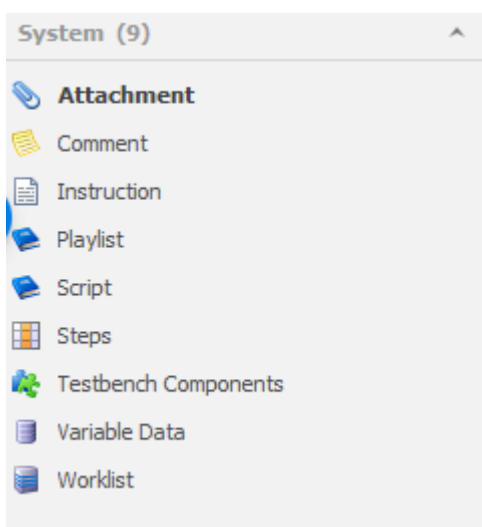
4. When creating the Security Role, you can allocate any Qualify functionality you would like members to have. You can allocate members to this role within this screen also.



5. For each Entity, you can then allocate permissions via the 'Permissions' tab. Selecting the 'Show Row Level Security' will then give you additional options.



- a. **Create:** This will allow a user to create a record
 - b. **Delete:** This will allow a user to delete a record, care should be taken allocating this permission, when deleting a record the audit history is also deleted.
 - c. **Exec:** If the Entity is executable (able to run a plugin from the right-click menu) this will allow the user to execute that record.
 - d. **Read:** This gives the ability to see the record.
 - e. **Update:** This permits to make changes to the record
 - f. **If Owner:** If the user is the owner of the record, you can give separate permissions. For example, if a user creates a record and therefore is the owner, you may want to allow them to delete, read or update that record. This can be useful to allow a user control over their work, without seeing or having access to other users work.
 - g. **If In Owners Role:** This works the same as f., however, the user will have control over other records where the user is on the same role.
6. From the left-hand Entities menu, you will see Entities under System, these will also require permissions setting as required.

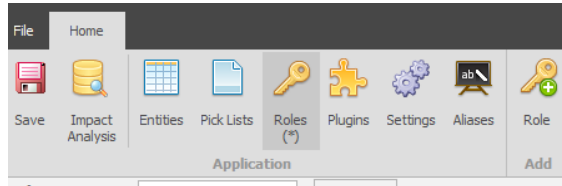


CREATING GLOBAL SECURITY ROLES

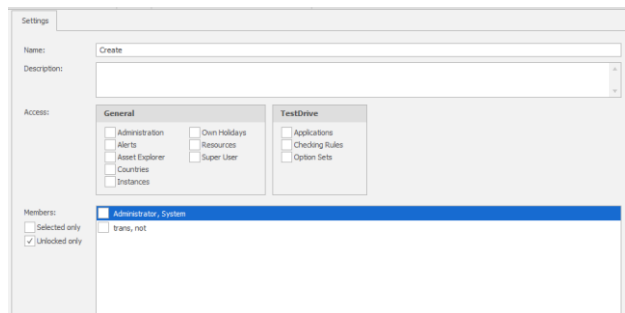
As opposed to the Application Definition that allows you to allocate permission within that single Application Definition, the Global Security allocated global permissions within Qualify.

As an example, you may wish to allow a user to create a new instance, whilst restricting other administration functions.

1. Log in to Qualify as the Administrator or a user with administrator permissions, edit the Global settings.
2. From the top menu bar, select Roles.



3. Here you can create a new Global security role and allocate permissions as required.



ALLOCATING PERMISSIONS TO RESOURCES

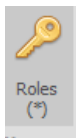
Once Security Roles have been configured they will need allocating to users, this can be done individually, at the group level and for both the Application Definition by default or at individual instances.

Allocating Global Permission

Global Permissions can be set by editing Global settings alongside editing the Resource record.

EDITING THE GLOBAL SETTINGS

1. Open qualify and the Global settings as an Administrator
2. Select the Roles tab, from the Top ribbon bar



3. Select the Global Security role, this will list all of the Resources on the system, select the check box to allocate that user the role.

Settings

Name: Create

Description:

Access:

General

Administration Own Holidays

Alerts Resources

Asset Explorer! Super User

Countries

Instances

TestDrive

Applications

Checking Rules

Option Sets

Members:

Administrator, System

trans, not

Selected only

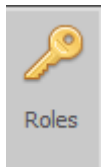
Unlocked only

Allocating Application Definition Permissions

Global Permissions can be set by editing Global settings alongside editing the Resource record.

EDITING THE APPLICATION DEFINITION

1. Open Qualify and edit the Application Definition as the administrator or as a user with administrator permissions.
2. Select 'Roles' From the top ribbon menu



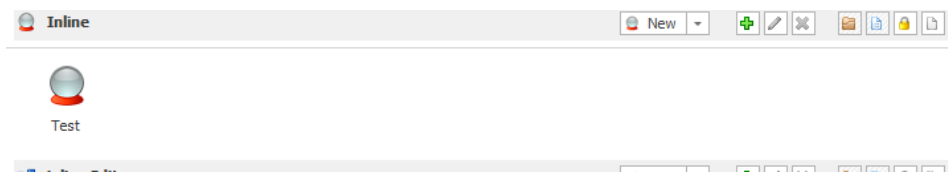
3. Select the Security Role you wish to add resources to, simply checking the tickbox will assign the permission.
4. Saving and restarting qualify will allow the new permission to be picked up.

Allocating Instance Level Permissions

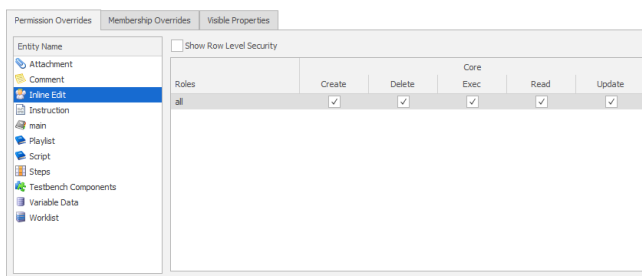
Allocating permissions at the instance level is used when automatic access to all instances is desired by default. We can allocate permissions at the individual instance level alongside allocate differing permissions.

ALLOCATING PERMISSIONS AT INSTANCE CREATION

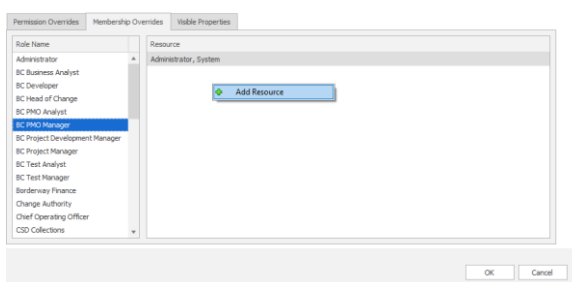
1. Log on to Qualify as the Administrator or a user with relevant permissions.
2. From the Open menu item on the left-hand menu, select 'New'



3. At the Permissions Override tab, you can change the Security Role Permissions per Entity if required.



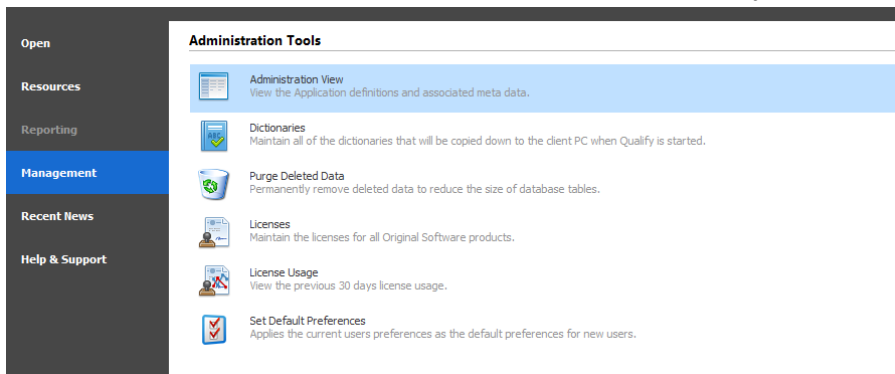
4. At the 'Membership Overrides' tab, you can select the Security Role and 'right mouse click' to add additional Resources'.



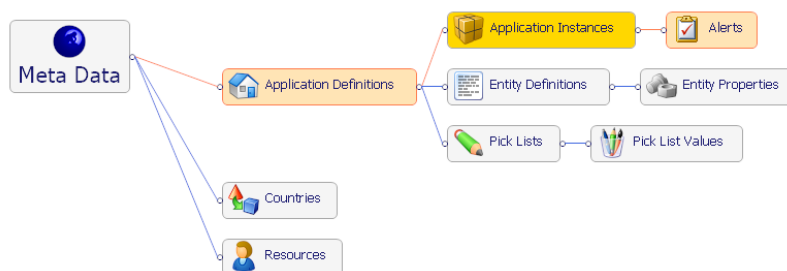
EDITING INSTANCE PERMISSIONS

You can edit the permissions for an instance that has already been created.

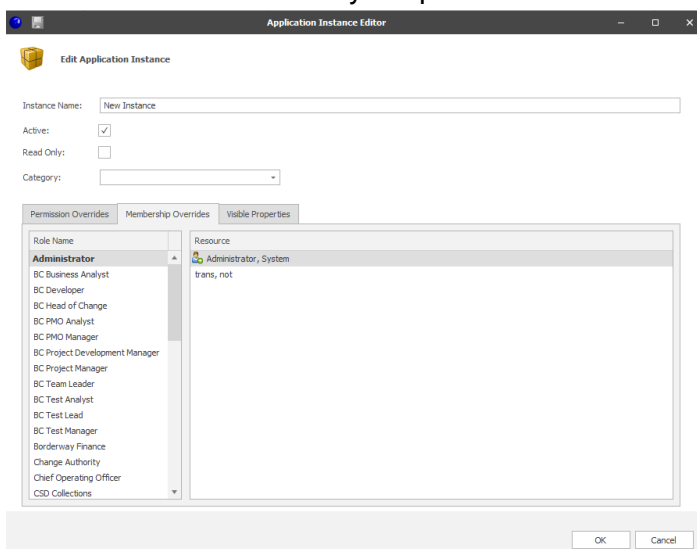
1. Log on to Qualify as the Administrator or a user with relevant permissions
2. From the left-hand menu, select 'Management' followed by 'Administration View'



3. From the Application Map select 'Instances'



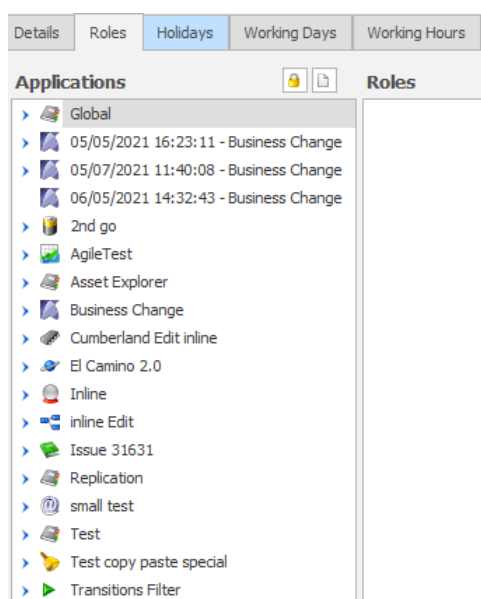
4. From the list of instances, double mouse click to edit, or right mouse click and select 'Edit'.
5. You are then able to modify the permissions for the Instance.



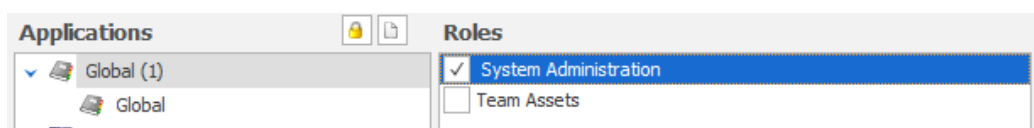
EDITING THE RESOURCE RECORD

You can allocate permissions at the Resource level, this would be useful where the number of users was low, or when adding a new single user.

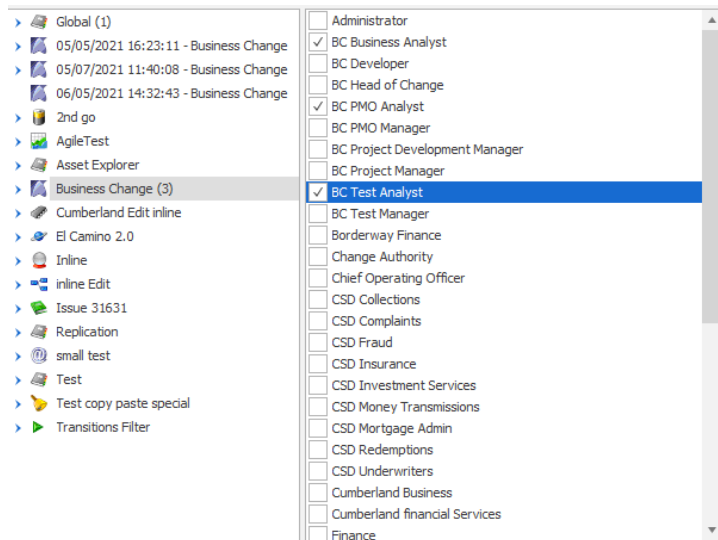
1. Log on as the Administrator, or a user with the relevant permissions
2. From the left-hand menu, select 'Resources'
3. Double click, or right mouse click and select 'Edit' on the Resource you wish to allocate permissions to.
4. Select the Roles tab, this will show the Global configuration alongside every Application definition and Instance.



5. Applying Global permissions.
 - a. From the top level, select the Security Role desired



6. Applying Application Definition Permissions
 - a. From the top level, select the Security Roles(s) required



7. Applying individual instance Permissions

- a. From the application Definition at the top level, expanding will show all of the current instances created. Checking individual instances will allow you to allocate to particular instances.