

# Managing users and locations

ArchivesGateway user guide

# Table of contents

Introduction	2
Definitions and references	2
1 Initial login and set up	3
1.1 Set up multi-factor authentication	3
1.1.1 Send a code via SMS	3
1.1.2 Google authenticator app	5
1.2 Logging in after initial set up	8
2 Managing your account	9
2.1 Updating your profile	9
2.2 Password reset	10
2.3 Managing and changing MFA methods	11
2.4 Inactive users	12
3 Users, permissions, accounts and agency locations	13
3.1 User roles	13
3.1.1 Security Administrator	13
3.1.2 Senior Agency Administrator	14
3.1.3 Agency Administrators	14
3.1.4 Agency Contact	15
3.2 Permissions	16
3.2.1 General permissions	16
3.2.2 Access permissions	16
3.2.3 Authorised Delegate permissions	18
3.3 Creating users and accounts	19
3.3.1 Adding locations	19
3.3.2 Creating a new user	21
3.3.3 Adding existing users to locations	22
3.3.4 Setting permissions	23
3.3.5 Changing a user's type	25
3.3.6 Removing users from locations	25
3.3.7 Deleting locations	26
3.3.8 Authorised Delegate accounts	26
3.4 Editing users and setting positions	26
3.4.1 Change a user's details	27
3.4.2 Resetting a user's MFA	27
3.4.3 Making a user inactive	27
4 Navigating between agencies and locations	28
4.1 Switching between agencies and locations	28
4.1.1 Change agency	28
4.1.2 Change location	29
5 Machinery-of-government and administrative change	30
6 More information	31



## Introduction

The information in this guide applies to all government agency staff that use ArchivesGateway to transfer records to and manage their records at Queensland State Archives (QSA).

This user guide describes the key points and processes involved in logging in to ArchivesGateway, setting up users, editing permissions and managing various locations and agencies.

Other user guides are available for other functions within ArchivesGateway. See the [more information section](#) for details on how to find and access these other user guides.

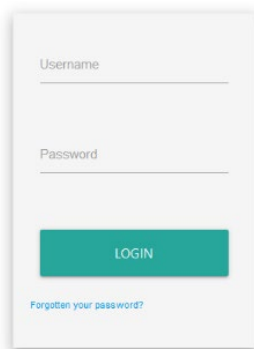
## Definitions and references

Relevant definitions of recordkeeping and archival terms used in this guide can be found in the glossary on the website.

See [recordkeeping and archival terms and their definitions](#).

# 1 Initial login and set up

Log into [ArchivesGateway](#) using the username and password provided.



© The State of Queensland  
Queensland Government

## 1.1 Set up multi-factor authentication

When logging into ArchivesGateway for the first logging, Multi-Factor Authentication (MFA) will need to be set.

MFA security codes can be generated using the Google Authenticator app on your mobile device or through a SMS system using your mobile number.

1. Log in to ArchivesGateway for the first time
2. Select your preferred MFA method:
  - Send a code via SMSOR
  - Use the Google Authenticator app

### 1.1.1 Send a code via SMS

If 'Send a code via SMS' is your preferred method:

1. Enter your mobile phone number were indicated on the screen

# Manage Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) uses your smartphone to add an extra layer of security to your QSA Agency Gateway account.

With MFA enabled, logging in is a two step process:

1. Enter your username and password as normal
2. Receive a code on your smartphone, and enter it to confirm your access

QSA Agency Gateway supports two different MFA methods: **code via SMS**, or **Google Authenticator**.

- Send a code via SMS
- Use Google Authenticator

## Code via SMS

Enter your phone number below and we will send you a secure code when you log in.

0412 377 495

Your mobile phone number (e.g. 0412 345 789)

0412 377 495 |

Confirm: Your mobile phone number (e.g. 0412 345 789)

SAVE

2. Click 'save' to proceed
3. The system will send a code via SMS to verify the mobile number provided

# Test your new MFA settings

We have just delivered a notification to the phone number you provided.

Please check that your new settings are working by entering the code you received:

|

Verification code

Didn't get a message?

SEND ANOTHER CODE

VERIFY

4. Enter the code generated and select 'verify'

# Test your new MFA settings

We have just delivered a notification to the phone number you provided.

Please check that your new settings are working by entering the code you received:

032163

Verification code

Didn't get a message?

SEND ANOTHER CODE

VERIFY


## 5. The home screen of ArchivesGateway will then appear



## Welcome

Your Multi-Factor Authentication settings have now been confirmed.

### Notifications

Record	Notification	Time of Event	
Role	Theo_Horsman permissions updated for Department of Natural Resources, Mines and Energy (l) - Agency Top Level Location	6/24/2020, 10:44:45 AM	<a href="#">VIEW</a>
Role	Albert_Bartlett permissions updated for Department of Natural Resources, Mines and Energy (l) - Agency Top Level Location	6/24/2020, 9:26:49 AM	<a href="#">VIEW</a>
 FIP34690	Has overdue items	5/15/2020	<a href="#">VIEW</a>

### 1.1.2 Google authenticator app

**Note:** to use Google Authenticator as MFA provider, the Google Authenticator app developed by Google LLC will need to be installed on your mobile device.

1. Select 'use google authenticator app' option
2. The screen will then display a QR code and a long alpha-numerical string as a key

# Manage Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) uses your smartphone to add an extra layer of security to your QSA Agency Gateway account.

With MFA enabled, logging in is a two step process:

1. Enter your username and password as normal
2. Receive a code on your smartphone, and enter it to confirm your access

QSA Agency Gateway supports two different MFA methods: **code via SMS**, or **Google Authenticator**.

- Send a code via SMS  
 Use Google Authenticator

## Google Authenticator

You can enter your account details into Google Authenticator by scanning the following QR code:



Alternatively, manually enter the following key:

6B76TCQQABRBR3A02YQKHD432G7RPMST

Generate a new key if you have reason to think your key has been compromised (if you have lost your phone, for example).

3. Open the Google authenticator app on your device  
**Note:** the app may request permission to use the devices camera. Allow the app permission to access your devices camera to proceed.
4. Use the device camera to scan the QR code  
OR  
Manually enter the key provided below the QR code
5. Click 'save' to proceed
6. You will then be prompted to test the new MFA settings

# Test your new MFA settings

You have configured your account to use Google Authenticator for MFA. Please ensure you have imported the following secret into Google Authenticator:



Alternatively, manually enter the following key:

6B76TCQQABKBR3A0ZYQKHD432G7RPM8T

Please check that your new settings are working by entering the code from the Google Authenticator app below:

Verification code

VERIFY

7. Enter the code provided by the app in the 'test your new MFA settings' screen

# Test your new MFA settings

You have configured your account to use Google Authenticator for MFA. Please ensure you have imported the following secret into Google Authenticator:



Alternatively, manually enter the following key:

6B76TCQQABKBR3A0ZYQKHD432G7RPM8T

Please check that your new settings are working by entering the code from the Google Authenticator app below:

Verification code

VERIFY


8. The home screen of ArchivesGateway will appear



# Welcome

Your Multi-Factor Authentication settings have now been confirmed.

## Notifications

Record	Notification	Time of Event	
Role	Theo_Horsman permissions updated for Department of Natural Resources, Mines and Energy (II) - Agency Top Level Location	6/24/2020, 10:44:45 AM	<a href="#">VIEW</a>
Role	Albert_Bartlett permissions updated for Department of Natural Resources, Mines and Energy (II) - Agency Top Level Location	6/24/2020, 9:26:49 AM	<a href="#">VIEW</a>
 FIP34690	Has overdue items	5/15/2020	<a href="#">VIEW</a>

**Note:** a new key and QR Code can be generated in the above screen should your key be compromised, or your device lost or stolen.

## 1.2 Logging in after initial set up

When logging in to ArchivesGateway after initial set up, you must:

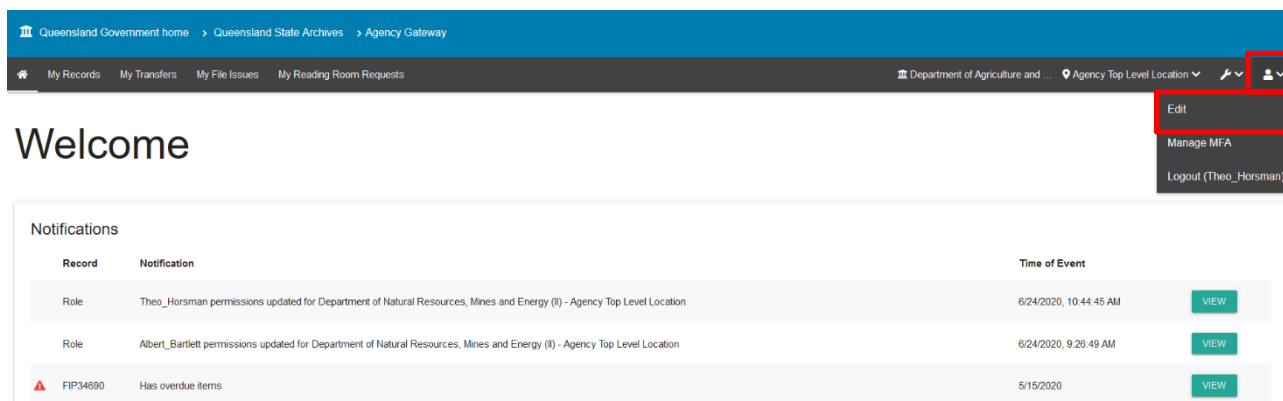
- enter your username and password
- enter in the MFA code provided via your chosen method.

## 2 Managing your account


### 2.1 Updating your profile

To update your profile:

1. Navigate to the User Menu by clicking on the 'person icon' on the top right and click 'edit'



The screenshot shows the top navigation bar of the ArchivesGateway system. The user menu is open, showing options: Edit, Manage MFA, and Logout (Theo\_Horsman). Below the menu is a 'Welcome' message and a 'Notifications' table.

Record	Notification	Time of Event	
Role	Theo_Horsman permissions updated for Department of Natural Resources, Mines and Energy (I) - Agency Top Level Location	6/24/2020, 10:44:45 AM	<a href="#">VIEW</a>
Role	Albert_Bartlett permissions updated for Department of Natural Resources, Mines and Energy (I) - Agency Top Level Location	6/24/2020, 9:26:49 AM	<a href="#">VIEW</a>
 FIP34690	Has overdue items	5/15/2020	<a href="#">VIEW</a>

2. In the profile form, fields that can be updated are:

- Name
- Position title
- Password
- Email address
- Contact number

There is also the option to reset your MFA.

3. Click 'save user' to implement any changes

Username  
Theo\_Horsman

\* Name  
Theo Horsman

\* Position  
Records Manager

Password  
\*\*\*\*\*  
Must be at least 12 characters in length; Include both upper and lower case letters; Include at least one non-letter (numeral, space or punctuation)

\* Email  
theo.horsman@archives.qld.gov.au  
Please contact your agency administrator if your email is incorrect

\* Contact Number  
07 1234 5678

Reset Multi-Factor Authentication?

SAVE USER

## 2.2 Password reset

1. A new password can be requested by following the 'forgotten your password?' link on the login page

Username

Password

LOGIN

Forgotten your password?

2. This will navigate to the password reset form

**Note:** your assigned **username**, not the email address attached to your account must be used when resetting passwords.

## Reset your password

Enter your username below. We will send a password reset email to the address we have on record.

Username

RESET MY PASSWORD

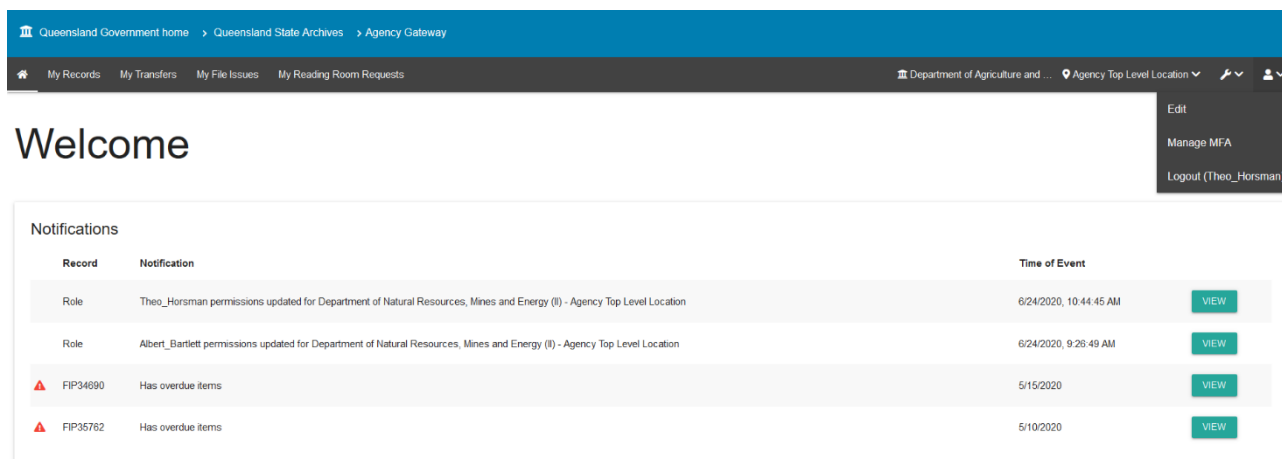
3. After clicking the 'Reset your password' link, an email with instructions for resetting your password will be sent to your nominated email address.
4. If an email is not received, check your 'junk' folder. The link provided may need to be copied into your browser.

If your password cannot be reset, contact the [File Issue team](#).

## 2.3 Managing and changing MFA methods

To change the MFA method used:

1. Log in to ArchivesGateway
2. Navigate to the User Menu by clicking on the 'person icon' on the top right and click 'Manage MFA'.



The screenshot shows the ArchivesGateway user interface. At the top, there is a navigation bar with the following items: Queensland Government home, Queensland State Archives, Agency Gateway, My Records, My Transfers, My File Issues, My Reading Room Requests, Department of Agriculture and ..., Agency Top Level Location, and a user profile icon. The user profile icon is expanded to show a menu with the following options: Edit, Manage MFA, and Logout (Theo\_Horsman). Below the navigation bar, the main content area displays a 'Welcome' message. Underneath the welcome message, there is a 'Notifications' section with a table of notifications. The table has three columns: Record, Notification, and Time of Event. Each row has a 'VIEW' button to the right of the 'Time of Event' column.

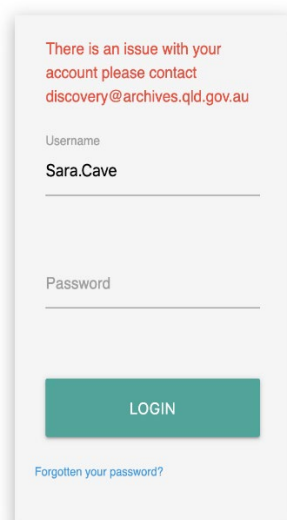
Record	Notification	Time of Event	
Role	Theo_Horsman permissions updated for Department of Natural Resources, Mines and Energy (I) - Agency Top Level Location	6/24/2020, 10:44:45 AM	<a href="#">VIEW</a>
Role	Albert_Bartlett permissions updated for Department of Natural Resources, Mines and Energy (I) - Agency Top Level Location	6/24/2020, 9:26:49 AM	<a href="#">VIEW</a>
▲ FIP34690	Has overdue items	5/15/2020	<a href="#">VIEW</a>
▲ FIP35762	Has overdue items	5/10/2020	<a href="#">VIEW</a>

3. Change the MFA method as required.

For more information, see the instructions on [Setting up multi-factor authentication](#).

## 2.4 Inactive users

If your account has been made inactive, when attempting to log in an alert message will be displayed.



The image shows a login form with a white background and a light gray border. At the top, there is a red error message: "There is an issue with your account please contact discovery@archives.qld.gov.au". Below this, there are two input fields: "Username" with the text "Sara.Cave" and "Password". A green "LOGIN" button is positioned below the password field. At the bottom left, there is a blue link that says "Forgotten your password?".

Accounts can be re-activated by the Senior Agency Administrator/s for your agency, or by QSA staff.

**Senior Agency Administrator/s:** See the instructions on how to [Make users inactive](#).

## 3 Users, permissions, accounts and agency locations

### 3.1 User roles

There are four user roles in ArchivesGateway:

- Security Administrator
- Senior Agency Administrator
- Agency Administrator
- Agency Contact

Subject to access permissions applied by public authorities, all users can search their records in ArchivesGateway, view digital and digitised records and submit Reading Room Requests.

If your public authority is smaller and only has minimal records management staff, you may not need all four user roles. However, all public authorities with records at QSA must have at least one Security Administrator and one Senior Agency Administrator user in ArchivesGateway (these can be the same person if appropriate).

See below for a breakdown of the four user roles.

#### 3.1.1 Security Administrator

Security Administrators can:

- assign/manage access permissions to Agency Administrators and Agency Contacts
- authorise access classifications applied to records
- search and view the metadata of all records that have an access classification of non-sensitive, sensitive, and highly sensitive
- view digital records with an access classification of non-sensitive and sensitive
- request to view digital and physical records with an access classification of highly sensitive through the File Issue service

In addition to the above functions, Security Administrators will have Senior Agency Administrator permissions in ArchivesGateway by default and will therefore be able to perform Senior Agency Administrator functions as outlined in the Senior Agency Administrator role below.

Security Administrators must be nominated by your public authority's Chief Executive Officer (CEO), Deputy Director-General (DDG), or authorised delegate for records access under the *Public Records Act 2002* using the Security Administrator nomination form.

A maximum of two Security Administrators is recommended per public authority. Any new nomination form/s supplied to QSA will supersede and revoke any prior versions of the nomination form submitted to QSA.

Once QSA receives the nomination form, the Security Administrator for your public authority will be set up in ArchivesGateway by QSA.

The nominated Security Administrator will then receive a welcome to ArchivesGateway email providing them with their login details (if they are a new user), a link to ArchivesGateway and information to get them started.

For more information about Security Administrators, see the [Access Classification Labels and Permissions in ArchivesGateway – Digital Archive public authority Toolkit](#). For additional information on access permissions see the User permissions section below.

### 3.1.2 Senior Agency Administrator

Senior Agency Administrators can:

- assign general permissions to Agency Administrators and Agency Contacts
- add 'locations' to your public authority (i.e. business units or administration areas)
- search and view the metadata of all your public authority's records at QSA (subject to access permissions granted by the Security Administrator)
- view digital and digitised records maintained by QSA (subject to access permissions granted by the Security Administrator)
- request records through File Issue and the Reading Room (subject to access permissions granted by the Security Administrator)
- submit Search requests
- propose and manage Transfers to QSA

The Senior Agency Administrator must be nominated by your public authority's CEO, DDG, or authorised delegate for records access under the *Public Records Act 2002* using the Senior Agency Administrator nomination form.

A maximum of two Senior Agency Administrators is recommended per public authority. Any new nomination forms supplied to QSA will supersede and revoke any prior versions of the nomination form submitted to QSA.

Once QSA receives the nomination form, the Senior Agency Administrator account for your public authority will be set up in ArchivesGateway by QSA.

The nominated Senior Agency Administrator will then receive a welcome to ArchivesGateway email, providing them with their login details (if they are a new user), a link to ArchivesGateway and information to get them started.

Once set-up, the Senior Agency Administrator/s should create additional users for public authority staff who require access to ArchivesGateway and general permissions can be assigned. An annual review of users and permissions is recommended to ensure ongoing security.

For information on general permissions see the User permissions section below.

### 3.1.3 Agency Administrators

Agency Administrators are managed by your public authority's Senior Agency Administrator and can:

- assign general permissions to Agency Contacts
- search and view the metadata of all your public authority's records at QSA (subject to access permissions granted by the Security Administrator)
- view digital and digitised records maintained by QSA (subject to access permissions granted by the Security Administrator)

- request access to records in the Reading Room at QSA (subject to access permissions granted by the Security Administrator)

If Agency Administrators have been given permission by the Senior Agency Administrator, they can also:

- request records through File Issue (subject to access permissions granted by the Security Administrator)
- submit Search requests
- propose and manage Transfers to QSA

### 3.1.4 Agency Contact

Agency Contacts are managed by your public authority's Senior Agency Administrator and can:

- search and view the metadata of all your public authority's records at QSA (subject to access permissions granted by the Security Administrator)
- view digital and digitised records maintained by QSA (subject to access permissions granted by the Security Administrator)
- request access to records in the Reading Room at QSA (subject to access permissions granted by the Security Administrator)

If Agency Contacts have been given permission by the Senior Agency Administrator or the Agency Administrator they can:

- request records through File Issue (subject to access permissions granted by the Security Administrator)
- submit Search requests
- propose and manage Transfers to QSA

Agency Contacts cannot assign permissions to any other users.



## 3.2 Permissions

Users will need to be assigned specific permissions that govern what tasks a user can complete within ArchivesGateway. The permissions a user may have consist of:

- General permissions
- Access permissions
- Authorised Delegate permissions

Each user can be assigned different general permissions in ArchivesGateway based on their user role and 'location'. However users should be assigned the same access permissions across 'locations' and roles.

See [Access permissions](#) for information on what users can access and view in ArchivesGateway depending on the permissions assigned.

### 3.2.1 General permissions

Senior Agency Administrators and Agency Administrators can assign the general permissions of ***allow\_transfers*** and ***allow\_file\_issue*** to other users.

Transfer permissions allow a user to propose and manage transfers of digital and physical records to QSA on behalf of the agency. See [ArchivesGateway user guide: Transferring records](#) for more information pertaining to the transfer's process.

File Issue permissions allow a user to submit Search requests and File Issue requests on behalf of the agency. Depending on the access permissions granted, users may not be able to request records with Access Classifications above their set permissions. See [ArchivesGateway user guide: Searching and search requests](#) and [ArchivesGateway user guide: File Issue service](#) for more information.

### 3.2.2 Access permissions

Access to digital records in ArchivesGateway will follow the principle of least privilege. This ensures users will only have access to what is necessary for them to perform their responsibilities. See the [Access Classification Labels and Access Permissions agency toolkit](#) for more information on the principle of least privilege and why is it important.

#### 3.2.2.1 Access Permissions in ArchivesGateway and Access Classification Labels

Permissions within ArchivesGateway are set up using a three-tier hierarchy based on the sensitivity of records. This ensures that access to records and metadata is only granted to users with the approved and allocated permissions, in accordance with the Access Classification Labels that have been applied. Refer to the table below for further information on the three permission types in ArchivesGateway and what levels of access they cover:

Permission Level	How it's displayed in ArchivesGateway	Coverage
<b>Access to non-sensitive and unclassified record</b>	<i>No Permissions set</i>	The most basic setting for general users does not include any permissions and only grants visibility to records and metadata that are either classified as non-sensitive or have no Access Classification assigned. ArchivesGateway users at this level can see the metadata of Sensitive records but not the records themselves. They can also see the metadata of Highly Sensitive records if it is published to the public catalogue, ArchivesSearch.
<b>Access to sensitive records</b>	<i>allow_access_sensitive</i>	This permission level allows users to see the metadata of all records that have an Access Classification of Sensitive, Non-sensitive, or have no Access Classification assigned. They will also be able to view digital records with these Access Classifications. If users have File Issue permissions, they will be able to request these records through the File Issue service. They can also see the metadata of Highly Sensitive records if it is published to ArchivesSearch.
<b>Access to highly sensitive records</b>	<i>allow_request_highly_sensitive</i>	This permission levels allows users to see all records. This includes records that have an Access Classification of Highly Sensitive, Sensitive, Non-sensitive, or have no Access Classification assigned. Users will be unable to view Highly Sensitive digital records in ArchivesGateway, but will be able to request them, as well as Highly Sensitive physical records through the File Issue service.

### 3.2.2.2 Summary of ArchivesGateway Access Permissions/ Access Classification Labels

		No Permissions set	allow_access_sensitive	allow_request_highly_sensitive
Non-Sensitive Records	Metadata	√	√	√
	Download Digital copy	√	√	√
Sensitive Records	Metadata	√	√	√
	Download Digital copy	x	√	√
Highly Sensitive Records	Metadata	o	o	√
	Download Digital copy	x	x	√ (Via File Issue Request only)

o - only if published to ArchivesSearch. Please note that in these instances, only the metadata is published to ArchivesSearch, however the link to the digital object is not.

### 3.2.3 Authorised Delegate permissions

If any of the user roles above have also been nominated by the agency's CEO as an Authorised Delegate for records access for your agency, they can:

- set and change restricted access periods
- grant access to restricted records

Authority to set or change restricted access periods (RAPs) for records which an agency is responsible and approve access to restricted records held at QSA conferred upon a responsible agency's Chief Executive Officer under the Public Records Act 2002 (the Act).

CEOs may delegate this authority under ss16-19 to set and change RAPs, and/or approve access to restricted records held at QSA by completing a delegation of authority form or similar instrument of delegation and forwarding it to QSA.

Delegations of authority may be made to either nominated positions (e.g. 'Records Officer') or named individuals (e.g. 'Susan Smith'). Once QSA has received a delegation of authority form, the permissions of **allow\_set\_and\_change\_raps** and **allow\_restricted\_acces** are assigned as stipulated on the form provided.

## 3.3 Creating users and accounts

### 3.3.1 Adding locations

An agency top-level location will automatically be created when your agency is set up in ArchivesGateway.

Other locations can be set up by the Senior Agency Administrator.

To create a location:

1. Click the spanner icon in the toolbar
2. Select 'manage agencies'



## Welcome

Notifications		
Record	Notification	Time of Event
Role	Theo_Horsman permissions updated for Department of Natural Resources, Mines and Energy (II) - Agency Top Level Location	6/24/2020, 10:44:45 AM
Role	Albert_Bartlett permissions updated for Department of Natural Resources, Mines and Energy (II) - Agency Top Level Location	6/24/2020, 9:26:49 AM
▲ FIP34590	Has overdue items	5/15/2020
▲ FIP35782	Has overdue items	5/10/2020

3. Click 'view' against the required agency



## Agencies

Search agency name

SEARCH AGENCIES RESET

Agency name	
Department of Agriculture and Fisheries	VIEW
Department of Natural Resources, Mines and Energy (II)	VIEW

**Note:** if you are associated with more than one agency, a list of these agencies will be visible.

4. Click 'add new location' on the top right

[Back to Agencies](#)

## Department of Agriculture and Fisheries

### Locations

[ADD NEW LOCATION](#)

Agency Top Level Location [ADD USER TO LOCATION](#) [EDIT LOCATION](#)

Username	Name	Position	Role	Permissions	
Graham_West	Graham_West	Records Officer	AGENCY_CONTACT	allow_transfers	<a href="#">SET PERMISSIONS</a>
Megan_test_user	Megan_test_user	Gaia Internal Testing	SENIOR_AGENCY_ADMIN	allow_transfers allow_file_issue	
Theo_Horsman	Theo_Horsman	Records Manager	SENIOR_AGENCY_ADMIN		

Locations

Users

### 5. Add the name and delivery address of the location

Name

Salisbury Office

---

Delivery Address

160 Lillian Terrace, Salisbury, 4107

---

[SAVE LOCATION](#)

### 6. Click 'save location'

### 7. The location created in the agency profile will now be visible

# Department of Agriculture and Fisheries

Locations ADD NEW LOCATION

Agency Top Level Location ADD USER TO LOCATION EDIT LOCATION

Username	Name	Position	Role	Permissions
Graham_West	Graham_West	Records Officer	AGENCY_CONTACT	allow_transfers <span>SET PERMISSIONS</span>
Megan_test_user	Megan_test_user	Gaia Internal Testing	SENIOR_AGENCY_ADMIN	allow_transfers allow_file_issue
Theo_Horsman	Theo_Horsman	Records Manager	SENIOR_AGENCY_ADMIN	

Salisbury Office ADD USER TO LOCATION EDIT LOCATION DELETE LOCATION

No members for this location

Locations  
Users

**Note:** when a new location is created, no users will be attached. Users will need to be added to this new location.

### 3.3.2 Creating a new user

The type of users that can be created and the permissions they can be assigned differs based on whether the person creating the user/s is a Senior Agency Administrator or an Agency Administrator. See [User roles](#) for more information.

It is recommended that users are added to the agency top-level location and then added to sub-level locations as required. Users should only be created in sub-level locations when they only require access to specific locations.

To create a new user:

1. Navigate to the Agency profile page
2. Scroll down to the location required
3. Click 'add user to location'
4. Use the drop down to select the type of user (Agency Contact or Agency Administrator)
5. Enter the user's details in the fields provided
  - a. Usernames should be formatted as Firstname\_Lastname
  - b. Passwords must be at least 12 characters in length and include both upper- and lower-case letters and at least one non-letter such as a number, a space or symbol. Password generators can be used; however, the user of the account should update their password after they have logged in for the first time.

Adding a user to Salisbury Office

CREATE NEW USER    ADD EXISTING USER

Agency Contact

\* Position

\* Username

\* Name

\* Password

\* Email

CREATE USER

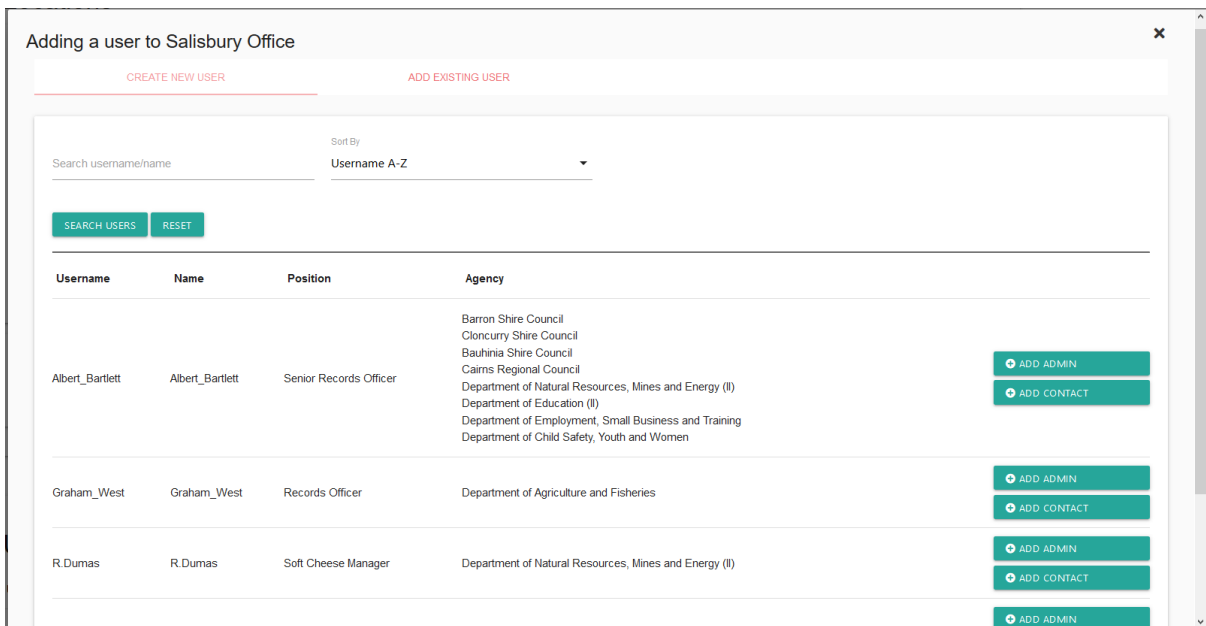
6. Click 'create user'
7. The new user will now be visible in the location they have been added to
8. This user can now be added to any other locations as required

**Note:** users can be added to multiple locations within your agency. If you are a Senior Agency Administrator for more than one agency, users can also be added to multiple agencies.

### 3.3.3 Adding existing users to locations

Existing users can be added to other locations within your agency.

1. On the agency profile page, navigate to the appropriate location
2. Click 'add user to location'
3. In the user profile form, select 'add existing user'



4. Use the search option to find the user by either username or name  
**Note:** users must be associated with your agency in ArchivesGateway.

5. Once located, click either:
- 'Add admin' – to set them as an Agency Admin level user for that location
  - 'Add contact' – to set them as an Agency Contact level user for that location

**Note:** the user role can be different in sub-level locations.

6. Permissions will then need to be set for that user for that location.

### 3.3.4 Setting permissions

Once a user is created their permissions will need to be set.

**Note:** Agency Admin users can only give Agency Contacts the same permissions that have been provided to you within ArchivesGateway.

For example, if you are an Agency Admin with File Issue permission, you will only be able to assign File Issue permissions to an Agency Contact. If you are an Agency Admin with no permissions, you will not be able to grant any permissions to an Agency Contact.

**Note:** only users who have been assigned the Security Administrator role will be able to tick 'allow access sensitive' and 'allow request highly sensitive' for other users within the agency.

**Only tick the 'allow, set and change RAPs' and 'allow restricted access' permissions if the user is an authorised delegate for your agency.**



To set users permissions:

1. In the agency profile page, navigate to the user under the relevant location
2. Click 'set permissions' on the right

## Department of Agriculture and Fisheries

The screenshot shows a web interface for managing users and locations. On the right side, there is a vertical navigation menu with 'Locations' and 'Users' options. The main content area is titled 'Locations' and contains two sections:

- Agency Top Level Location:** This section has buttons for 'ADD NEW LOCATION', 'ADD USER TO LOCATION', and 'EDIT LOCATION'. It contains a table with the following data:

Username	Name	Position	Role	Permissions	
Graham_West	Graham_West	Records Officer	AGENCY_CONTACT	allow_transfers	SET PERMISSIONS
Megan_test_user	Megan_test_user	Gaia Internal Testing	SENIOR_AGENCY_ADMIN	allow_transfers allow_file_issue	
Theo_Horsman	Theo_Horsman	Records Manager	SENIOR_AGENCY_ADMIN		
- Salisbury Office:** This section has buttons for 'ADD USER TO LOCATION', 'EDIT LOCATION', and 'DELETE LOCATION'. Below the buttons, it states 'No members for this location'.

3. Tick the appropriate permissions check boxes in the form

The screenshot shows a modal window titled 'Permissions for Theo\_Horsman'. It includes a close button (X) and a 'REMOVE FROM LOCATION' button. The form contains the following elements:

- Role:** A dropdown menu currently showing 'Agency Contact'.
- Permissions:** A list of permissions with checkboxes:
  - allow\_transfers
  - allow\_file\_issue
  - allow\_access\_sensitive
  - allow\_request\_highly\_sensitive
- Public Service Act 2008 Delegations:** A list of delegations with checkboxes:
  - allow\_set\_and\_change\_raps
  - allow\_restricted\_access
- SAVE PERMISSIONS:** A teal button at the bottom left.

4. Click 'save permissions'

### 3.3.5 Changing a user's type

**Senior Agency Administrator/s:** if required, Agency admin or Agency Contact user roles can be changed in the permissions settings window.

### 3.3.6 Removing users from locations

When removing users from a location, they must remain associated with at least one location for your agency – they cannot be removed altogether. The 'remove from location' button will be greyed out if they are only attached to one location. If a user must be removed completely, see how to [make a user inactive](#).

To remove users from locations:

1. In the agency profile screen, navigate to the location a user is to be removed from
2. Click 'set permissions' on the right

## Department of Agriculture and Fisheries

**Locations**

ADD NEW LOCATION

Agency Top Level Location

ADD USER TO LOCATION EDIT LOCATION

Username	Name	Position	Role	Permissions
Graham_West	Graham_West	Records Officer	AGENCY_CONTACT	allow_transfers
Megan_test_user	Megan_test_user	Gaia Internal Testing	SENIOR_AGENCY_ADMIN	allow_transfers allow_file_issue
Theo_Horsman	Theo_Horsman	Records Manager	SENIOR_AGENCY_ADMIN	

SET PERMISSIONS

Salisbury Office

ADD USER TO LOCATION EDIT LOCATION DELETE LOCATION

Username	Name	Position	Role	Permissions
Graham_West	Graham_West	Records Officer	AGENCY_ADMIN	allow_transfers allow_file_issue

SET PERMISSIONS

3. In the permissions window, click 'remove from location' button on the top right

Permissions for Graham\_West

REMOVE FROM LOCATION

Role: Agency Admin

Permissions:

- ✓ allow\_transfers
- ✓ allow\_file\_issue

Public Service Act 2008 Delegations:

- allow\_set\_and\_change\_raps
- allow\_restricted\_access

SAVE PERMISSIONS

### 3.3.7 Deleting locations

Only Senior agency administrators and QSA can delete locations.

Deleting locations is not recommended as all audit history of transactions completed by users within that location will be lost.

If a location needs to be 'deactivated' it is recommended it is renamed to include the words DO NOT USE or similar at the beginning.

### 3.3.8 Authorised Delegate accounts

An account for the Authorised Delegate for your agency may need to be created in ArchivesGateway.

You **do not need to log in** to this general delegate account.

General delegate accounts are used as the contact point for any automated requests from the public to access restricted records of your agency.

Accounts for Authorised Delegates within ArchivesGateway are created by QSA once a current delegation of authority form signed by the Chief Executive Officer (CEO) is provided.

Find out more about [authorised delegates](#) and [requests from the public to access restricted records](#).

**Note:** authorised delegates are preferably assigned to a position not a person. It is recommended that a generic account is created for the delegate position within your agency, not the person currently in the position, and a generic email address used.

## 3.4 Editing users and setting positions

Senior Agency Administrator and Agency Administrator users can edit user details for users assigned the level/s below them e.g. Agency Administrators can edit the user details of an Agency Contact. This includes making users inactive, updating their details, and resetting their MFA. The details that can be updated for a user include:

- Name
- Position title
- Password
- Email address
- Contact number

See [permissions](#) for more details on user levels.

**Note:** the username cannot be changed.

**Note:** if the user to be edited also has permissions for another Agency which you do not have permissions for, their details will not be able to be changed. In this case [contact QSA](#) for assistance.

To edit a user's details:

1. In the agency profile page, navigate to the user's section

Users				
Username	Name	Position	Email	Role(s)
Graham_West	Graham_West	Records Officer	wayne.mcmullin@daf.com	Agency Top Level Location — AGENCY_CONTACT Salisbury Office — AGENCY_ADMIN
Megan_test_user	Megan_test_user	Gaia Internal Testing	megan@gaiaresources.com.au	Agency Top Level Location — SENIOR_AGENCY_ADMIN
Theo_Horsman	Theo_Horsman	Records Manager	emma.horsman@archives.qld.gov.au	Agency Top Level Location — SENIOR_AGENCY_ADMIN

2. Click on 'edit user' button for the relevant person
3. The edit user screen will open

### 3.4.1 Change a user's details

To change a user's details:

1. Update details as required
2. Click save.

### 3.4.2 Resetting a user's MFA

To reset a user's MFA:

1. Resetting MFA means a complete reset. When they next log in they need to set up their MFA again
2. To reset, tick the 'reset Multi Factor Authenticator' checkbox
3. Click 'save'

### 3.4.3 Making a user inactive

To make a user inactive:

1. To make a user inactive tick the inactive button at the bottom of the profile page
2. Click save

## 4 Navigating between agencies and locations

If you are associated with multiple agencies and/or locations in ArchivesGateway, it is possible to switch between them to see the records associated with that agency or location.

There is no need to log out and log back in to ArchivesGateway, nor is a separate log in required.

### 4.1 Switching between agencies and locations

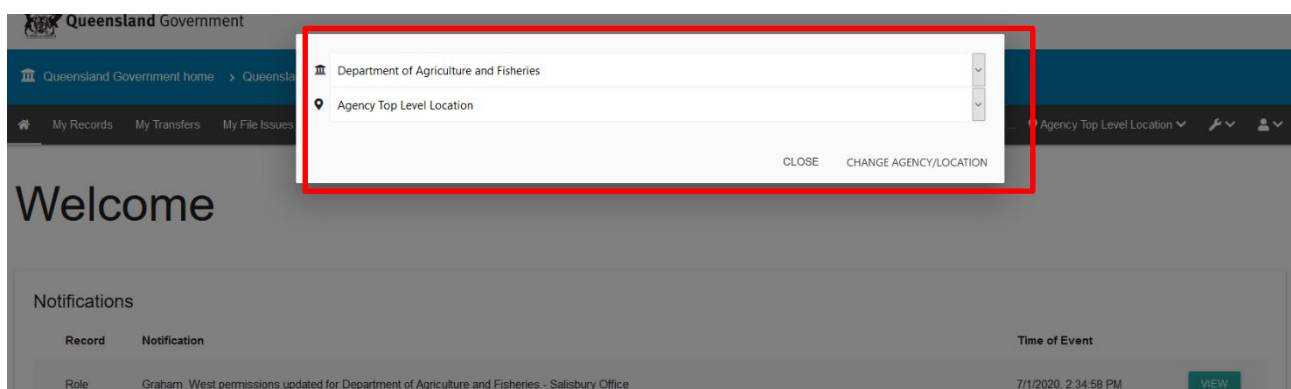
To switch between locations or agencies:

1. Click the drop-down arrow next to the agency name and location in the toolbar to display the pop-up window



## Welcome

Notifications			
Record	Notification	Time of Event	
Role	Graham_West permissions updated for Department of Agriculture and Fisheries - Salisbury Office	7/1/2020, 2:34:58 PM	<a href="#">VIEW</a>
Location	Department of Agriculture and Fisheries - Salisbury Office created by Theo_Horsman	7/1/2020, 11:16:56 AM	<a href="#">VIEW</a>
Role	Theo_Horsman permissions updated for Department of Natural Resources, Mines and Energy (II) - Agency Top Level Location	6/24/2020, 10:44:45 AM	<a href="#">VIEW</a>
Role	Albert_Bartlett permissions updated for Department of Natural Resources, Mines and Energy (II) - Agency Top Level Location	6/24/2020, 9:26:49 AM	<a href="#">VIEW</a>
FIP34690	Has overdue items	5/15/2020	<a href="#">VIEW</a>



#### 4.1.1 Change agency

1. In the pop-up window click on the agency drop down (top option)
2. Select the agency required
3. Click 'change agency/location' button on the bottom right
4. This will change the agency and bring up the records for that agency

**Note:** this must be done before the specific location for that agency can be selected.

#### 4.1.2 Change location

1. Click on the location drop down (second option)
2. Select the location required
3. Click 'change agency/location' button on the bottom right
4. This will change the location within the agency selected and bring up the requests done within that location

## 5 Machinery-of-government and administrative change

When there is a machinery-of-government (MOG) or administrative change and the ownership of records transfers to another agency, there is a grace period of three months where both the preceding and succeeding agency can view and access records, and conduct business such as transferring records.

Both agencies can continue to access the records where responsibility has been assigned.

Succeeding agencies are expected to assign revised or new agency delegates and establish revised user profiles and permissions.

Find out more about [Custody, ownership and responsibility for records during a MOG or administrative change](#).

See also the [user guide for Searching records](#) for more information on how records affected by a MOG change will display in ArchivesGateway.

## 6 More information

Further information is available on the Recordkeeping section of the For Gov website:

- [Use ArchivesGateway](#)
- [Transfer records to QSA](#)
- [Restrict access to records at QSA \(Restricted Access Periods\)](#)
- [Retrieve or access your agency's records at QSA \(File Issue service\)](#)
- [Provide access to closed records](#)

Other user guides are also available for specific functions within ArchivesGateway and are available on the relevant pages listed above.

If further assistance is required with ArchivesGateway, contact the File Issue team via email: [fileissue.qsa@archives.qld.gov.au](mailto:fileissue.qsa@archives.qld.gov.au).