TORQUE
SOFTWARE

Lighthouse User Guide
System Administration and Global Settings

Version 6.2.2

CONTENTS

GLOBAL SYSTEM SETTINGS 6
Configuring Settings 6
Configuring the Dashboard 8
Tile Style 9
List Style 9
Default Dashboard Style 10
Dashboard Wording 10
Configuring Classifications 10
Configuring Countries 11
Configuring System Permissions and Email Workflow 11
System Email Setup 15
System Security 15
System Log 16
Survey logs 17
SMTP Settings 17
Lighthouse and Module License Maintenance 18
How to Update License 18
Managing Modules Licenses 19
GROUPS 20
Configuring Groups 20
System Administrators Group 20
Creating a new Group 20
User Sets 22
Include Criteria 23
Exclude Criteria 23
Criterium Types 23
Importing Users 24
MAINTAINING REPORTING PERMISSIONS 25
Adding, Editing and Deleting Reporting Permissions 25
Granted Users 26
Granted Records 26

Effective 27
Filtering Reporting Permissions 27
Exporting Reporting Permissions 28
MAINTAINING AUTHORITIES 28
Authoriser Questions – Master 28
Authorities 29
Authority Groups 30
MAINTAINING NOTIFICATIONS 31
Notification Templates Tab 33
Notifications 34
MAINTAINING FINANCE SETTINGS 36
Settings 37
Cost Centres 37
GL Codes 37
Cost Centres 37
General Ledger Codes 38
Expenditure Types 38
Payment Methods 39
MAINTAINING SYSTEM USERS 39
Updating System Users Information 40
Action Buttons 40
User Fields 40
Export Users to Excel 41
Merge Duplicate Users 41
Purge Unused Users 42
Editing and Adding Users 42
Reset Password 42
View a User's Permissions 42
Deleting Users 43
Printing and Saving the User Management Screen 44
MAINTAINING THE ORGANISATIONAL STRUCTURE 45
Viewing and Ad hoc Maintenance of the Organisational Structure 45

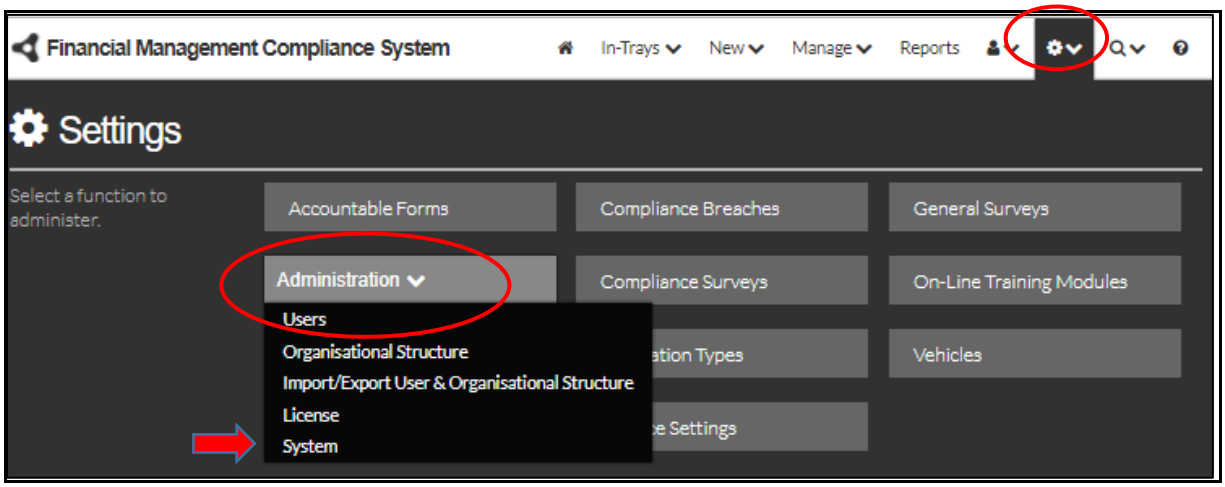
Editing an existing Organisational Unit 46
Moving an Organisational Unit 46
Create a new Organisational Unit 47
Deleting Organisational Units 47
Deactivating Organisational Units 47
IMPORTING USERS AND ORGANISATION STRUCTURE 47
Managing Data Sources 48
Creating a Data Source 48
Editing a Data Source 49
Importing on Demand 51
Import Scheduling 51
Exporting Data Source 52
Deleting Data Source 53
Exporting Users and Organisation Structure. 53
Import Logs 53
Settings 53
Import File Specification 54
File Format 54
Column Headings 54
System Fields 54
Recommended Import Practices 59
MAINTAINING MENU STRUCTURE 60
Adding Menu Items 61
Editing Menu Items 61
Menu Item Fields 62
Moving Menu Items 63
Deleting Menu Items 63
TEST MODE 64
IMPLEMENTATION GUIDE 65
Initial System Administrator Logon 65
Whitelisting 65
Authentication Method 65

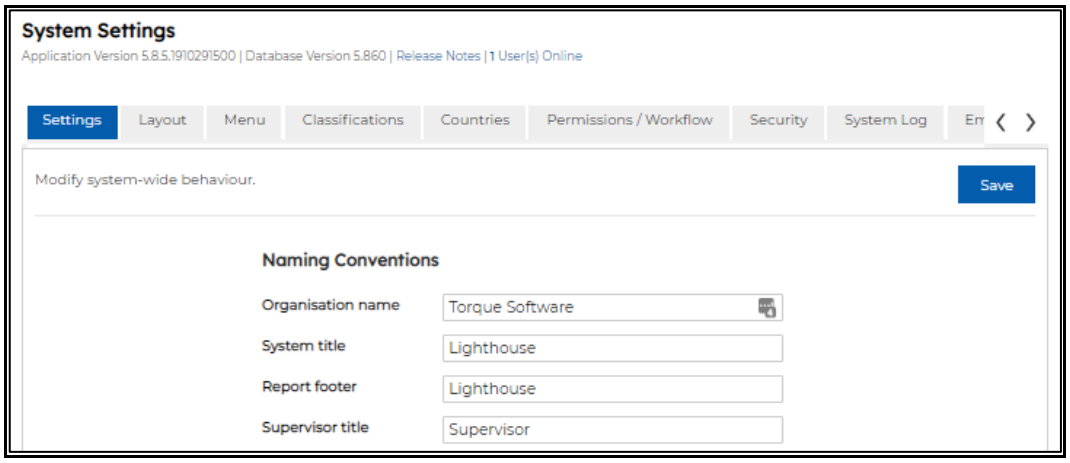
Option 1 – VANguard Federated Authentication Service 65
Option 2 – Torque Software's Propriety Single Sign On 66
Option 3 – Logon ID and Password 66
Populate Users & Organisation Structure 66
Classifications 67
Configure System Settings 67
From mask 67
BCC email address 67
Grant System Administrator Permissions 67

GLOBAL SYSTEM SETTINGS

The System Functions are only available to System Administrators. From this menu, System Administrators can manage global settings affecting the overall operation of Lighthouse. They are able to tailor Lighthouse to meet their organisation's requirements: change titles and labels, manage permissions and workflow options, and manage the security of the system.

Access these options through the **Administration** option from the **System Administration** menu, then click on System, as shown below.





Configuring Settings

From the Settings Tab, Administrators can change the name of the system and many of the labels to allow users to see titles consistent to those used in the organisation. They can also configure how users will see and use elements of the organisation structure.

Naming Conventions

Click into the field to be edited, type the changes and click on the Save button.

System title - this field sets the name of the system. Changes to the title are reflected throughout the system, including the masthead at the top of each screen.

Report footer - all reports show this footer.

Supervisor title - this is your agency's name for supervisor, e.g. 'Manager' or 'Supervisor', etc.

Branch title - put the name you call your organisation hierarchy here, e.g. 'Organisation Structure' or 'Zone/Branch/Division', etc.

Login title - put the name you call your login identifier here, e.g. 'Login' or 'Logon ID'.

User Display Format – these are merge fields to define how user details will be displayed throughout the system.

`{First}` - FirstName
`{Last}` - LastName
`{AGS}` - AGSNumber
`{LogonId}` – Logon ID
`{AGSorLogonId}` – if there's no AGS number this will display Logon ID, otherwise AGS Number will be displayed
`{EmailAddress}` – Email addy
`{EmailAddressAsLink}` – HTML formatted clickable hyperlink to email address
`{Branch}` – Org Structure node name (or "(not set)" if not set)
`{BranchPath}` – Full org Structure display path (x / y / z) (or "(not set)" if not set)
`{BranchPathAbbreviated}` – Full org Structure display path, but compressed down to max 70 chars like so "abc / def / ghi / … / jkl / mno / xyz " (or "(not set)" if not set)
`{ContactNumber}` – Phone number

User Display Format (Reporting) – these are merge fields to define how user details will be displayed in the Report Builder.

Salutation Format - configures the format of the {Salutation} merge field used in email templates. Any number of options may be included, separated by commas. The first non-null option will be used.

Organisation Structure

User-Organisation Unit Linkage - control how users are linked to organisation structures.

Mandatory - all users must be linked to an organisation structure; this allows effective reporting throughout all Lighthouse functions.

Optional - users do not have to have an organisation structure. Users without a nominated organisation must always nominate the relevant organisation structure within the function they are using.

Hidden - users will never have an organisation structure, so all references to a user's organisation structure are hidden to avoid confusion.

Organisation Unit Prompt - the text used to prompt the user to enter their org unit (both on the sign up screen and in the pop-up prompt).

Prompt for Organisation Unit - enable this function to prompt user to enter their org unit on login.

Update Organisation Unit - enable this function to prompt user to enter their org unit on login, every defined number of days.

Allow manual Organisation Unit update - enable this function to allow users to modify their org unit through the My Details page.

Group Types

This is the list of types groups can be allocated to within Group management.

Legal Entities

Lighthouse can facilitate allocation of individual branches to different legal entities. To enable this functionality turn **Use multiple legal entities** on and define each of the legal entities you wish to use.

Configuring the Dashboard

The dashboard can be displayed in a tile or grid style.

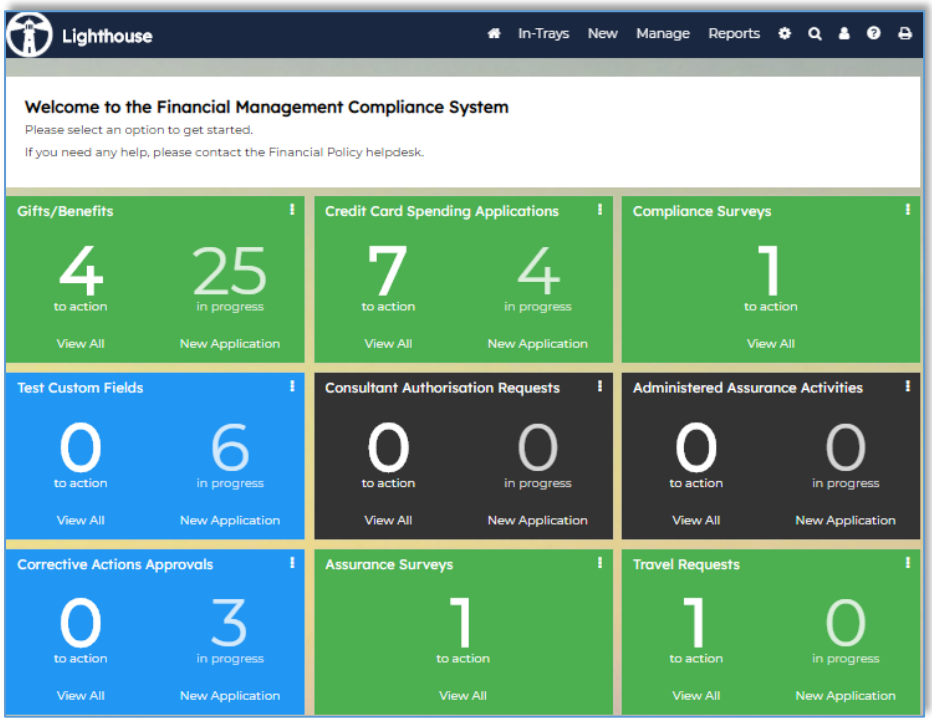
The System Administrator can configure the default display, ability to allow users to select their own default dashboard display and add agency specific text to the dashboard.

To configure the dashboard settings go to **System Administration > Administration > System > Dashboard**.

System administrators may override the default settings for any user by editing the user in the user list and setting the dashboard style and allow or disallow the user to change their dashboard style. Users can also be given permission to choose their own layout.

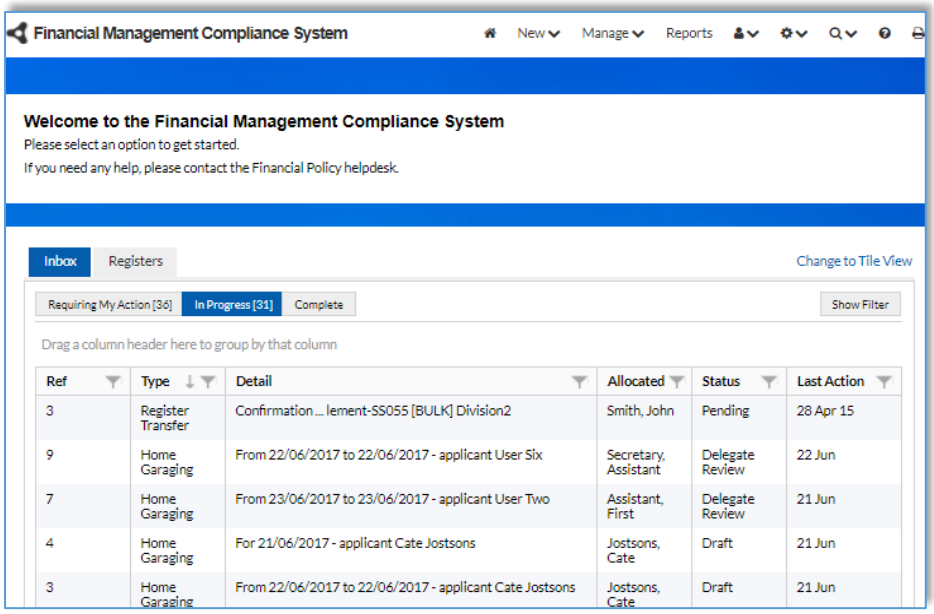
Tile Style

This style appears in a graphic view as shown below. It is particularly good for users who prefer a visual representation of their work.



List Style

The list style dashboard format combines all actions for the user into a single work list. This view is particularly useful for users that have transactions to action across several modules. The list can be grouped and filtered to suit individual preferences.



Default Dashboard Style

Select the default style from the dropdown box.

Allow users to change their dashboard style by selecting the Yes option, or make a style mandatory for the organisation by selecting the No option.

Dashboard Wording

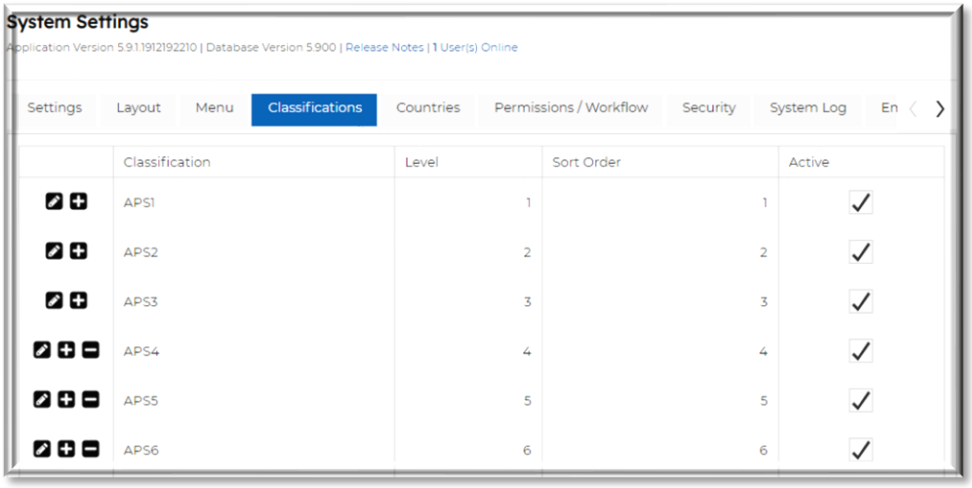
This information is displayed on the home page.

The information can be formatted in many different styles and may include hyperlinks to further information on the intra, or internet. The working can be viewed in Design, HTML or Preview modes. Click on the Save button to save any information entered.

Important: Don't forget to click on the Save button to save changes.

Configuring Classifications

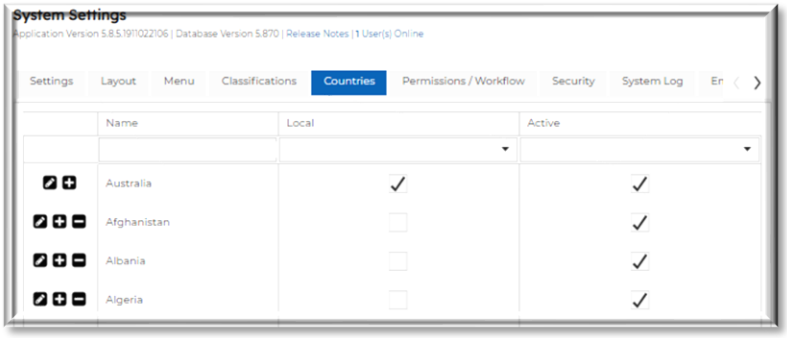
To configure classifications, click on the Classifications tab. This allows to you define the available position classifications. Note: These classifications are used when selecting a classification for a user, and other areas where a classification is required.



Note: Level is the relative level of the classification compared to other classifications.

Configuring Countries

To configure countries, click on the Countries tab. This allows to you define the available countries. The Local flag indicates the local country, I.e. Australia. Note: Countries are used in Gift/Benefit applications.



Configuring System Permissions and Email Workflow

To set up permissions and email workflow for the overall system click on the Permissions/Workflow tab.

Different permissions and email workflow can be set for each module by accessing the Module Settings for a particular module.

System Settings
Settings
Layout
Menu
Classifications
Countries
Permissions / Workflow
Security
System Log
Modify the workflow behaviour for the system.
Save
Permissions
Item Type managers
Item Type Managers
This group contains the members who manage all item types and create new types.
Risk module administrators
Risk Module Administrators
This group contains the members who can administer the risk module.
Authority Administrators
System Administrators
This group contains the members who can manage authorities and limits.
Financial Administrators Group
System Administrators
This group contains the members who can administer these system-wide financial settings.
Group Creators
System Administrators
This group contains the members who have implicit edit, create and manage control over all groups.
Report Administrators
Report Administrators
This group contains the members who have implicit edit, schedule and sharing control over all reports.
Lookup List Administrators
System Administrators
This group contains the members who have implicit edit, update and delete control over generic lookup lists.
Custom Form Template Creators
System Administrators
This group contains the members who have permission to create new custom form templates.
Notification Managers
System Administrators
This group contains the members who have permission to manage and send notifications.
Unlimited Email Senders
System Administrators
This group contains the members who have permission to send more than 100 notifications in a single tranche.
User and Organisational Structure management team
System Administrators
Data connection administrators
System Administrators
This group contains the users who can create data connections.
System Email Setup
Administrator email
admin@torquesoftware.com.au
The default reply-to for emails sent from the system; users are also notified to contact this address if they are unable to login; and queued import error notifications are sent to this address.
Email footer
If you have any questions, please contact us immediately.
Kind regards,
Financial Policy
Appears at the bottom of all email correspondence
From mask
When blank, will use system title
BCC email address
FMCSEmailLog@torquesoftware.com.au
All emails generated by the system will BCC this address.

Item Type managers Group

Members of the selected group have permission to configure all items types.

Select the group from the drop down list.

To view the group, click on the view icon to the side of the field.

To create a new Group – see Managing Groups.

Risk Module Administrators Group

Members of the selected group have permission to configure the risk module.

Select the group from the drop down list.

To view the group, click on the view icon to the side of the field.

To create a new Group – see Managing Groups.

Authority Administrators Group

Members of the selected group have permission to maintain Authorities.

Select the group from the drop down list.

To view the group, click on the view icon to the side of the field.

To create a new Group – see Managing Groups.

Financial Administrators Group

Members of the selected group have permission to maintain finance settings.

Select the group from the drop down list.

To view the group, click on the view icon to the side of the field.

To create a new Group – see Managing Groups.

Group Creators Group

Members of the selected group have permission to create new groups.

Select the group from the drop down list.

To view the group, click on the view icon to the side of the field.

To create a new Group – see Managing Groups.

Report Administrators Group

Members of the selected group have global permission to maintain all report builder templates.

Select the group from the drop down list.

To view the group, click on the view icon to the side of the field.

To create a new Group – see Managing Groups.

Lookup List Administrators Group

Members of the selected group have global permission to maintain all lookups used in custom form templates.

Select the group from the drop down list.

To view the group, click on the view icon to the side of the field.

To create a new Group – see Managing Groups.

Custom Form Template Creators Group

Members of the selected group have permission to create new custom form templates.

Select the group from the drop down list.

To view the group, click on the view icon to the side of the field.

To create a new Group – see Managing Groups.

Unlimited Email Senders Group

Members of the selected group have permission to configure email notifications to any number of recipients. Users not in this group may only send to a maximum of 100 users.

Select the group from the drop down list.

To view the group, click on the view icon to the side of the field.

To create a new Group – see Managing Groups.

User and Organisational Structure Management Team

Members of the selected group have permission to maintain users and the organisation structure.

Select the group from the drop down list.

To view the group, click on the view icon to the side of the field.

To create a new Group – see Managing Groups.

Data Connection Administrators

Members of the selected group have permission to create and maintain data connections used to import users and organisation units.

Select the group from the drop down list.

To view the group, click on the view icon to the side of the field.

To create a new Group – see Managing Groups.

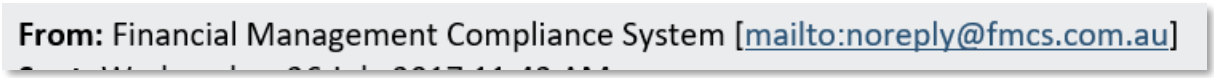
System Email Setup

Administrator email - The administrator email is now only used for system related purposes such as the following;

- Default Reply To address for emails sent by the system
- Contact address for users unable to log in
- Queued import errors.

Email Footer - this text appears at the bottom of all emails sent by the system.

From Mask – a user friendly name that system emails will be displayed as. The default from mask is the System Title. However, this option allows the From Mask to be changed to a different value.



Bounce Address – set an address here for system emails that have bounced from recipients. Note: This option is only available when Lighthouse is hosted on client premises and is not available when cloud hosted.

BCC email address – enter an address here to have a copy of all system emails stored to create an email systems log.

Important: Don't forget to click on the Save button to save changes.

System Security

This section allows System Administrators to modify the security settings for access to the system.

Disable manual registration – ticking this option stops users from registering themselves in the system. This means that only System Administrators can add new users to the system either manually or by importing them.

Verify on Import – this function, if ticked, allows the system to automatically verify a user in the system if they have been added by the import function. See Section on importing users.

Allow any domain – when selected this option allows users from any domain to use the system and the email domains option listed below becomes inactive.

Email Domains – the system will only allow users we defined email domains to be permitted access to the system. Use the Add, Edit and Delete icons to maintain allowed domains.

Password-based login group – Only members of this group may login via logon and password.

Password Complexity – sets the number of password complexity rules that must be met when a user creates a password. Up to five rules may be selected. Note: if an existing user's password no longer meets the password complexity rules, they will be asked to change their password when they next logon.

Account Lockout – these options allow the system to lock a user out for multiple failed logins. These settings are not relevant to organisations that have single sign on. They are used for staff who log in remotely or are required to log into Lighthouse each time they use the system.

Security Emails

These emails are not relevant to organisations that have single sign on. They are used for staff who log in remotely or are required to log into Lighthouse each time they use the system.

Notification emails can be turned off. To do this, uncheck the relevant box and click **Save**.

To edit an email template, click the (**edit**) link next to its description.

Update the subject and body (remembering that the generic **Email signature**, specified above, will be appended to the bottom of all emails); put the cursor in the email body box and select a merge field from the drop-down list to insert it at that location. When you're done, click **Save**. To cancel, click the X in the top right hand corner.

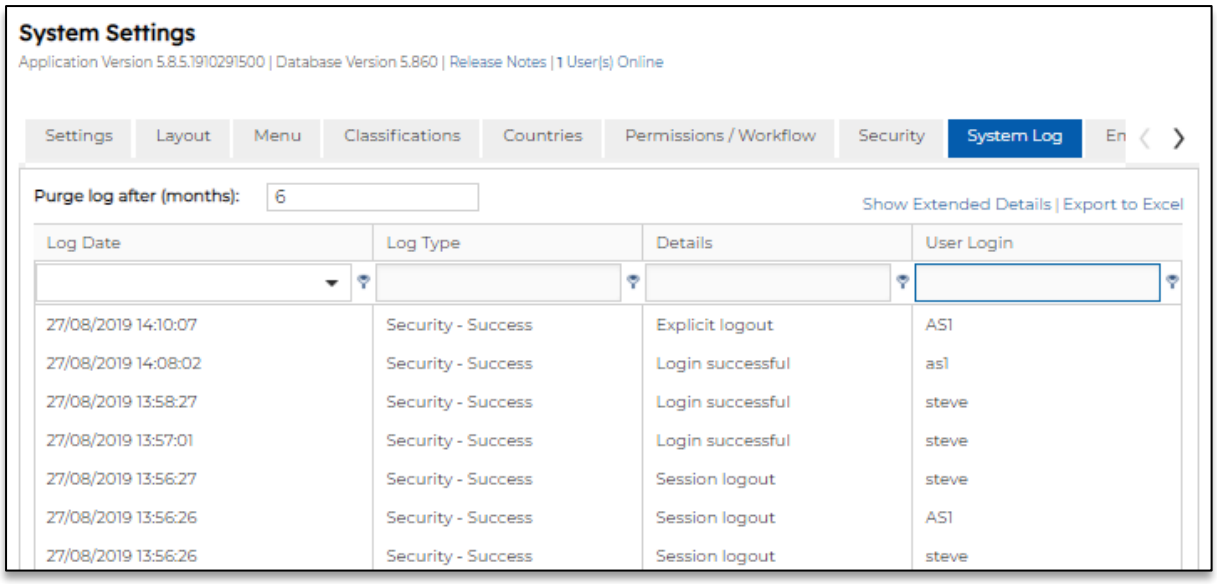
Forgot password - the email sent to users requesting their password be sent to them (via the login screen).

Reset password - the email sent to users when administrators reset their password for them (via User Management).

Require verification - checking this box indicates that users will be sent the associated email, complete with a verification link to validate their email address prior to allowing them access to the system.

System Log

Allows System Administrators to monitor logged events in the system.



Click on the "Show Extended Details" text to show more or less information.

To filter the system log, click on the filter boxes to define the filter.

The system log can be exported to Excel by clicking on Export to Excel. If a filter has been applied only records matching the filter will be exported. Only the most recent 100,000 records will be exported.

Log records will be deleted after the number of months nominated in the Purge Log field.

Survey logs

All actions performed on a survey are logged and can be viewed in the 'log' tab under 'Survey Administration'. Manage > Survey type > Action > Design > Log

Note: You must be logged in as an Administrator (System, Survey or module).

SMTP Settings

SMTP are transfer protocols that should only be edited by qualified technical staff. If the settings are to be modified a warning message will appear confirming that you wish to proceed.

Navigate: System Administration > Administration > System > SMTP settings

From email address - the reply email address used when sending notifications out of the system, e.g. "noreply@fmcs.com.au"

Server- the URL to the SMTP server used to send notifications, e.g. "fmcs.com.au"

Server Port - the port used when connecting to the SMTP server, e.g. "25"

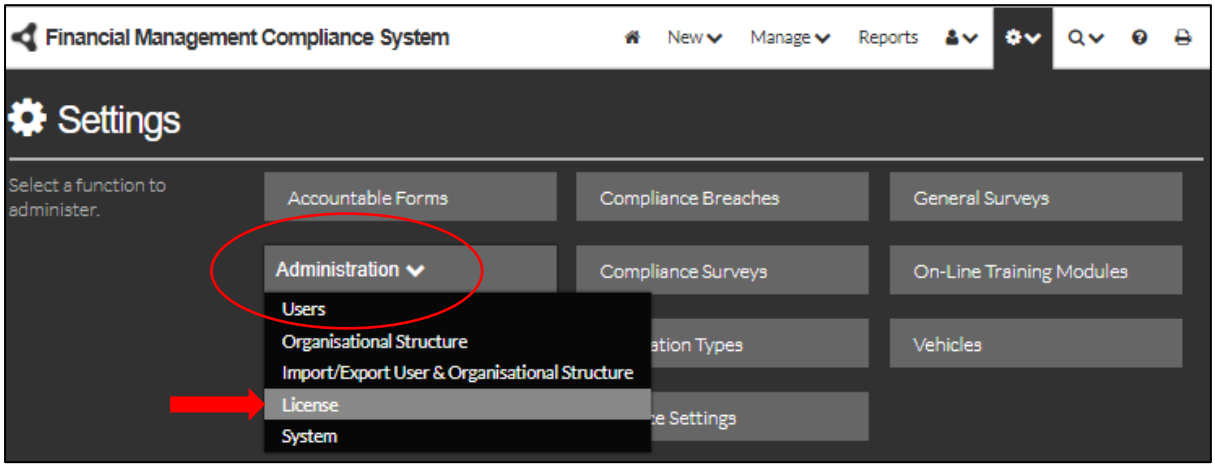
Use default credentials - a flag indicating whether to use anonymous credentials when connecting to the server.

Use SSL - indicates whether the SMTP server requires SSL.

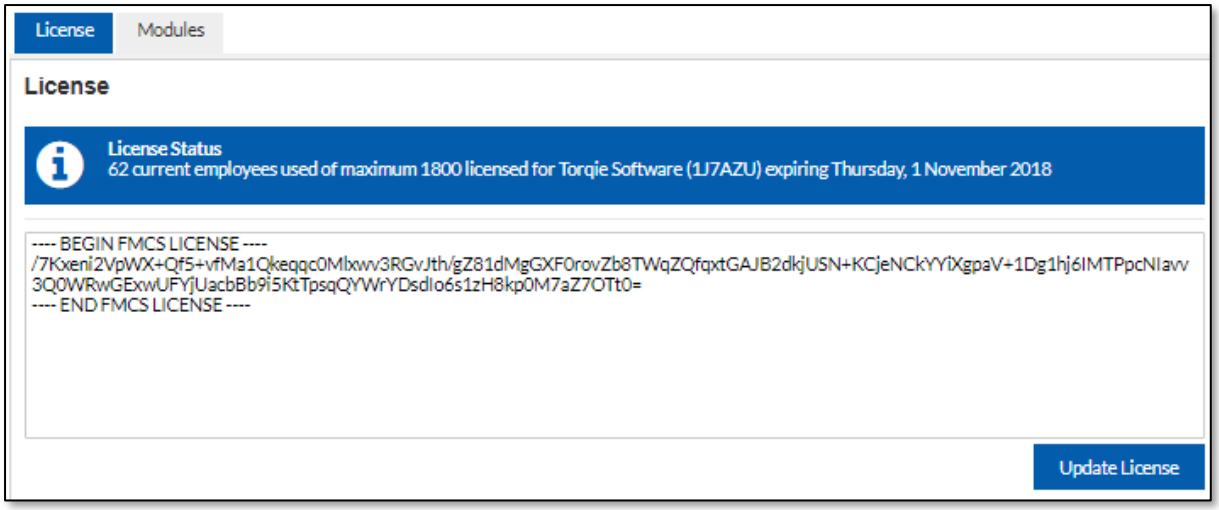
Test SMTP Settings – click her to test new settings.

Lighthouse and Module License Maintenance

System Administrators can view and manage Lighthouse License status by access information under the License option from the System Administration Menu, Administration, then License.



How to Update License



The license status is displayed in the blue header. It includes the ASL the license is registered for and the date of expiration.

When it is time to update the license the System Administrator will receive an email from Torque Software with the new License key. Once this has happened, click on the Update License button and copy the new license key into the field.

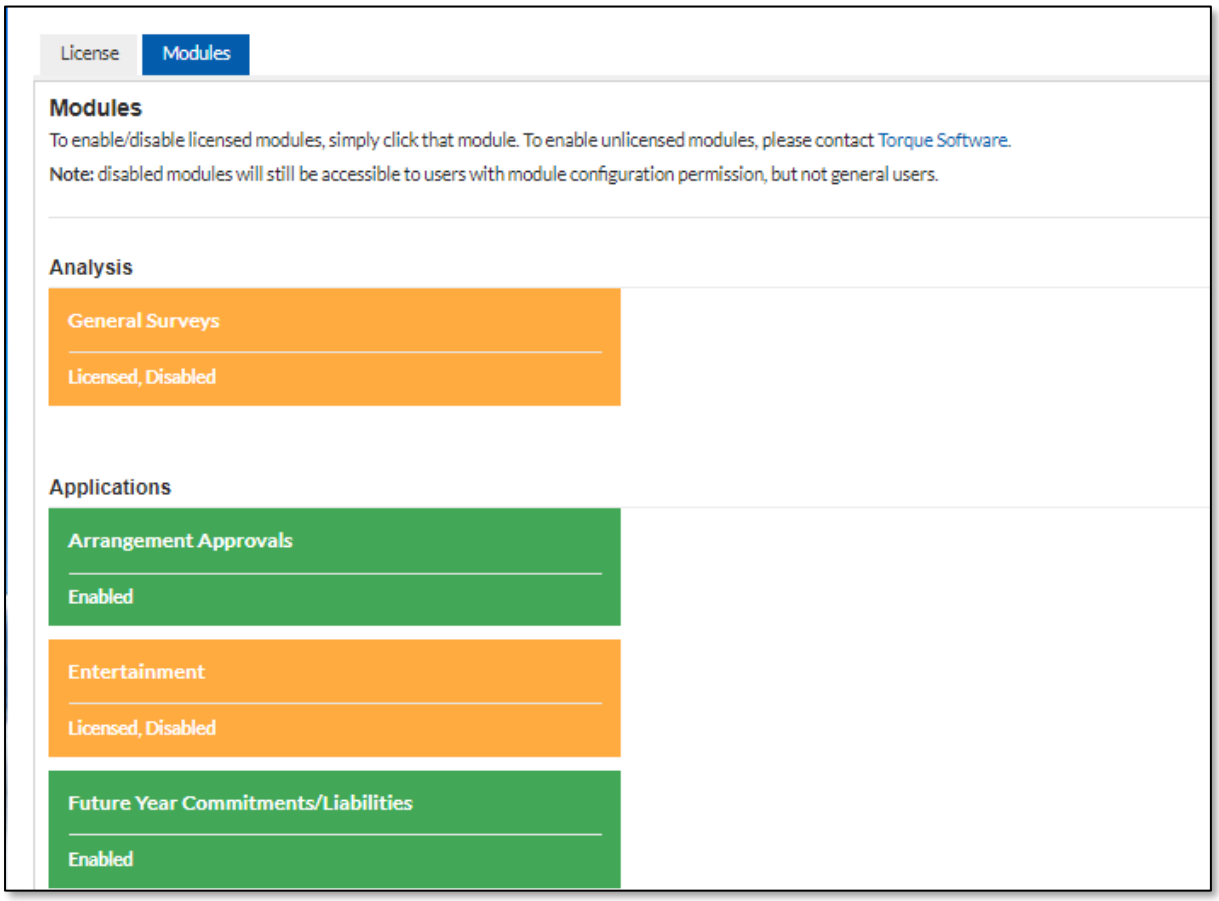
License changes are recorded in the System Log.

Managing Modules Licenses

Click on the Modules tab to access manage individual modules in Lighthouse.

System Administrators are able enable and disable any Module the organisation is licensed to use.

It is advised to disable a module when administrators are configuring, or editing the configuration, of a module. This will prevent users access the module while administrators are working within the settings.



Click on the module to disable. Click on the module again to enable it when ready.

Enabled modules will appear green, and disabled modules appear yellow.

Enable/disable actions are recorded in the System Log.

GROUPS

A group is a list of users who are selected based on a set of criteria. Only current users are selected. Groups are used in many ways, including granting permissions such as system administration and module configuration. Workflow and other actions may also be directed to a group instead of an individual user. A user group may contain any number of users. A user group may also contain other user groups.

A group can be assigned to several permissions. This means a person can be assigned multiple permissions simply by including them in the group without having to give separate permissions.

New user groups can be created by users with system administration or module configuration permissions.

The users and groups in a user group may be members of the group, administrators of the group or both. Users may access the groups they have permission to administer by going to **Manage > Groups**.

When a group is granted a permission all the members of the group are granted the same permission.

Groups can contain other groups whose members then become part of the group.

Changes to the members of a group are recorded in the System Log.

Configuring Groups

System Administrators Group

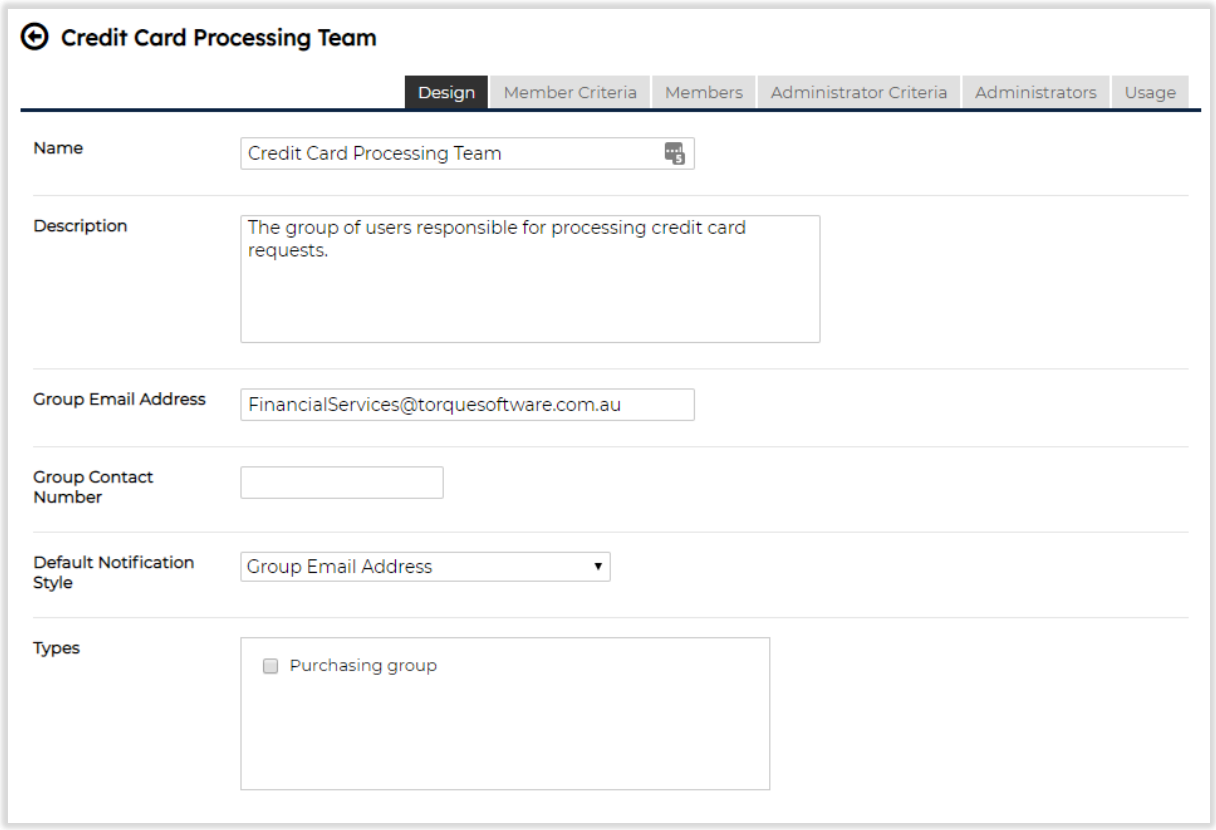
The System Administrators group is a special group containing only those users with permission to perform the system administrator role. Rules apply to the system administrators group that do not apply to any other group;

- System administrators group cannot be deleted
- Name and Description cannot be changed

System administration permission is granted by making the user a member of the System Administration Group.

Creating a new Group

Only System Administrators and Module Administrators may create Groups. Go to Manage > **Groups > Create New Group.** Each group contains the following tabs that allow the group to be managed.



Design Tab

The design tab allows creation of basic set up information relating to the group. This tab has the following fields;

- Name – a unique name for the group
- Description
- Group Email Address – the address used to send emails to the group - optional
- Group Contact Number – phone number for the group – optional
- Default Notification Style – specifies if emails are addressed to the Group Email Address, all members or both
- Select the 'Save' button to move to the users tab. After saving, all other tabs will be available.

Member Criteria Tab

The Member Criteria tab specifies the criteria used to determine the users who are members of the group.

Members Tab

The Members tab lists all users who meet the member criteria and are therefore members of the group.

Administrator Criteria Tab

The Administrator Criteria tab specifies the criteria used to determine the users who are granted group administration permission. This permission allows users to make changes to the group settings. The permission may also be granted to all group members by turning on the Members Can Administer setting in the Actions menu.

Members of the System Administrators group may administer any group, irrespective of the Administrator criteria.

Administrator Tab

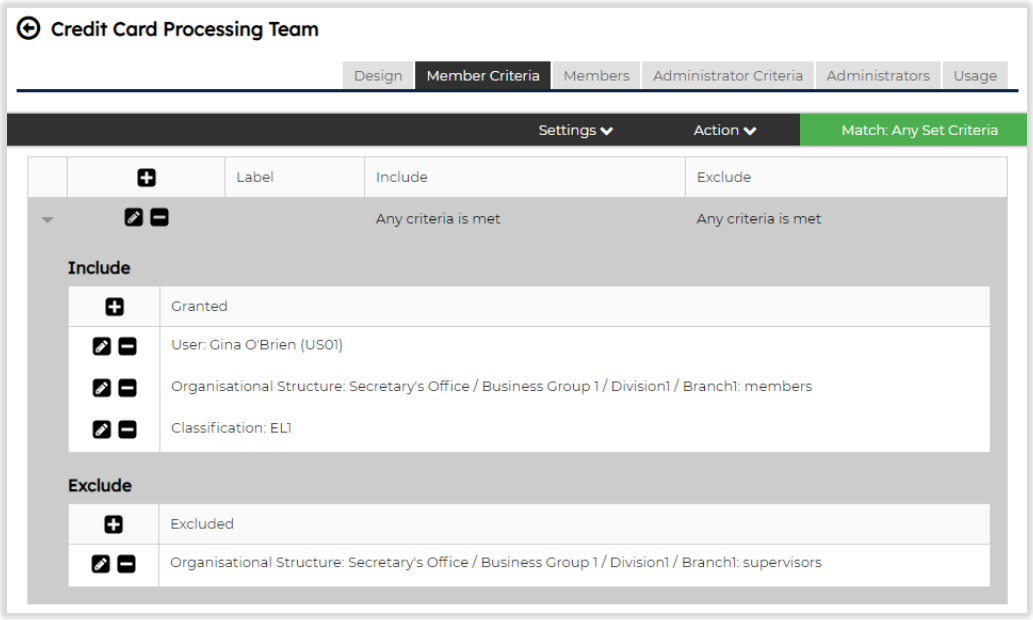
The Administrator tab lists all users who meet the administrator criteria and are therefore administrators of the group.

Usage Tab

Lists all the locations where the group is used within the system..

User Sets

Member criteria and administrator criteria contain one or more user sets. A user set contains users meeting specified criteria.



Options are available to specify if users must be contained in all sets, or any set, to meet the member criteria requirements. See the options **Any Set Must Meet Criteria** and **All Sets Must Meet Criteria** in the Settings menu within the member and administrator tabs.

Select ✚ at the top of the tab to add a new set. Creating a new set provides the following options;

Label – Optional label to identify the set.

Include where – Specifies if the user must meet all the include criteria or any of the include criteria to be included in the set.

Exclude where – Specifies if the user must meet all the exclude criteria, or any of the exclude criteria, to be excluded from the set.

Include and exclude criteria are made available by selecting the grey arrow next to a saved set.

Include Criteria

Include criteria specifies those users who are included in the set. One or more include criterium may be specified.

Exclude Criteria

Exclude criteria specifies those users who are excluded from the set. Any number of exclude criterium may be specified. Excluded users are always excluded from the set, irrespective of any include criteria.

Criterium Types

Include and exclude criterium may be any of the following types;

All Users – Selects all active users.

User – Selects an individual user.

Group – Selects a group of users.

Organisation Unit – Selects a specified organisation unit and optionally all lower levels of the organisation unit.
Options are available to select only members of the organisation unit (and lower levels if selected), supervisors of the organisation unit (and lower levels if selected), or both.

Classification – Selects all users of a specified classification.

Classification Level – Selects all users where the level of their classification is within one of more ranges. E.g. 10-30, 50, 80-100.

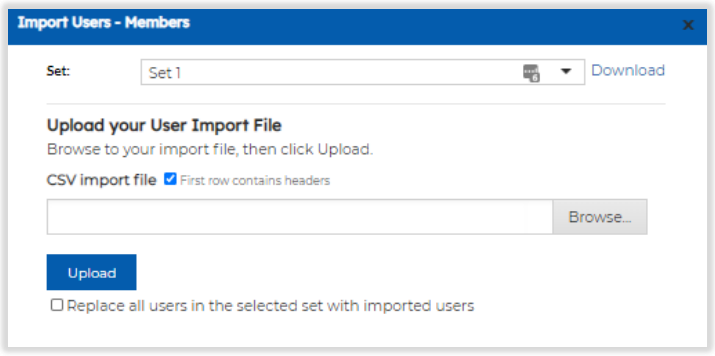
Email Address – Selects all users where their email address partially matches a specified string. E.g. ".gov.au"

Position – Selects all users holding a specified position.

Note: Only current users may be included in groups. Non-current users are always excluded from groups.

Importing Users

Users may be imported into a set by using the Import User action. Note: The import user action does not allow import of group, organisation unit, classification, or email address criteria.

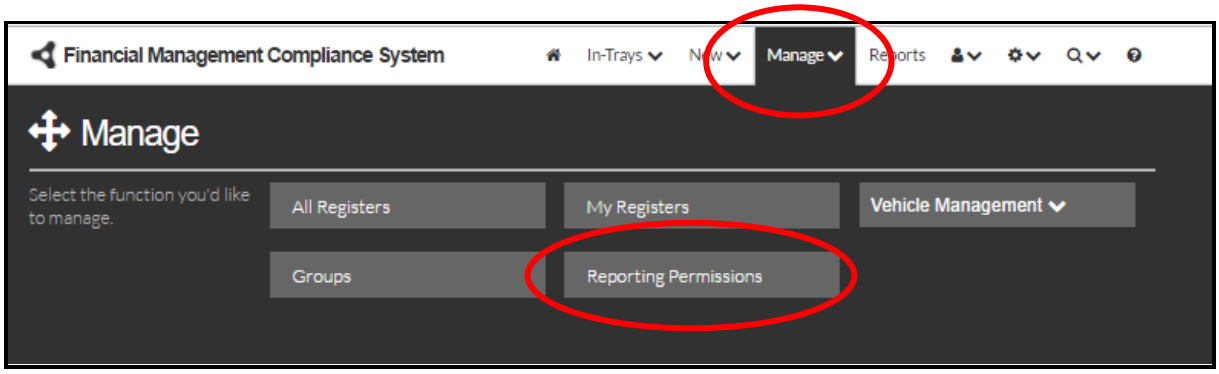


The option "Replace all users in the selected set with imported users" will also remove any users from the group who are not in the import file.

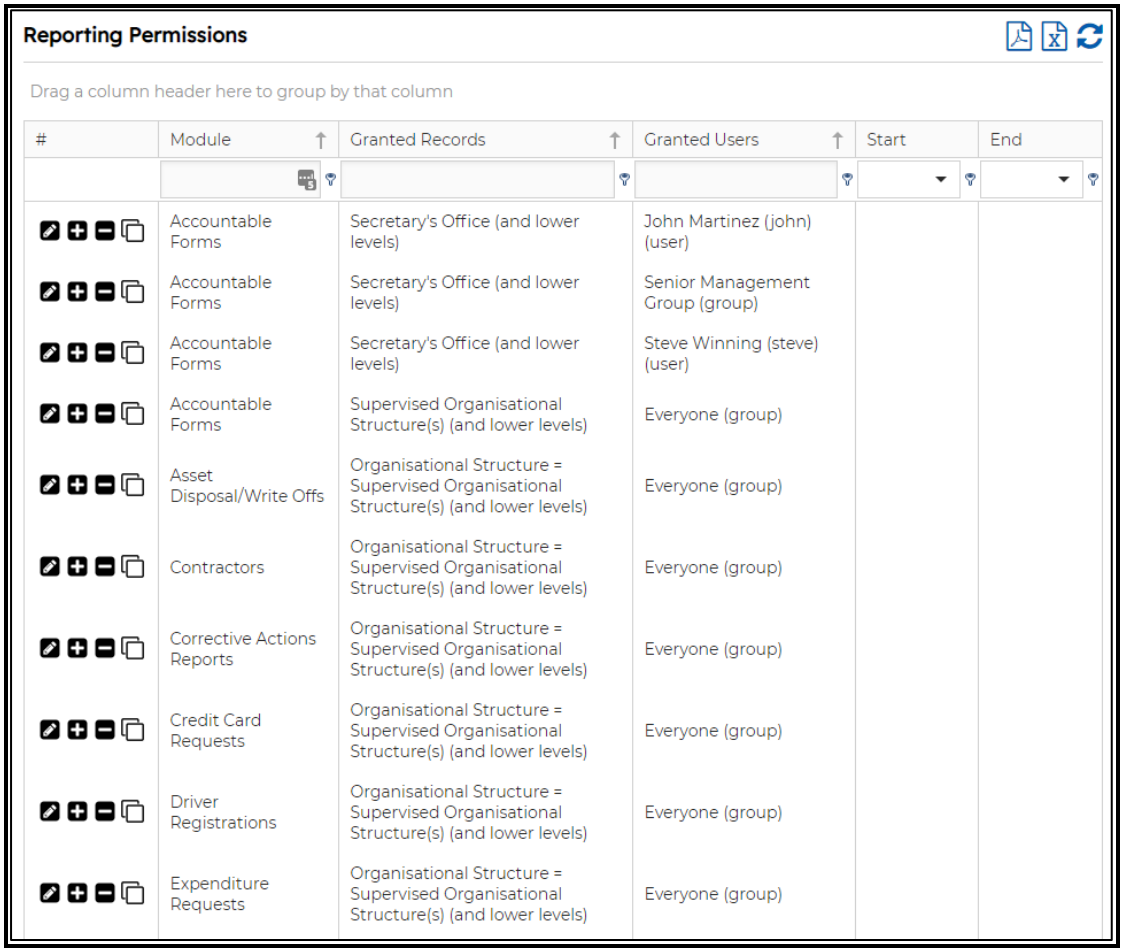
MAINTAINING REPORTING PERMISSIONS

Reporting permissions allow users to obtain reports for a permitted module and organisation unit. Only system administrators and module administrators can grant Reporting Permissions. System administrators can assign reporting permissions for any module. Module administrators may only assign reporting permission for the modules they administer.

To Access the Reporting Permissions, go the Manage Menu and Select Reporting Permissions.



Adding, Editing and Deleting Reporting Permissions

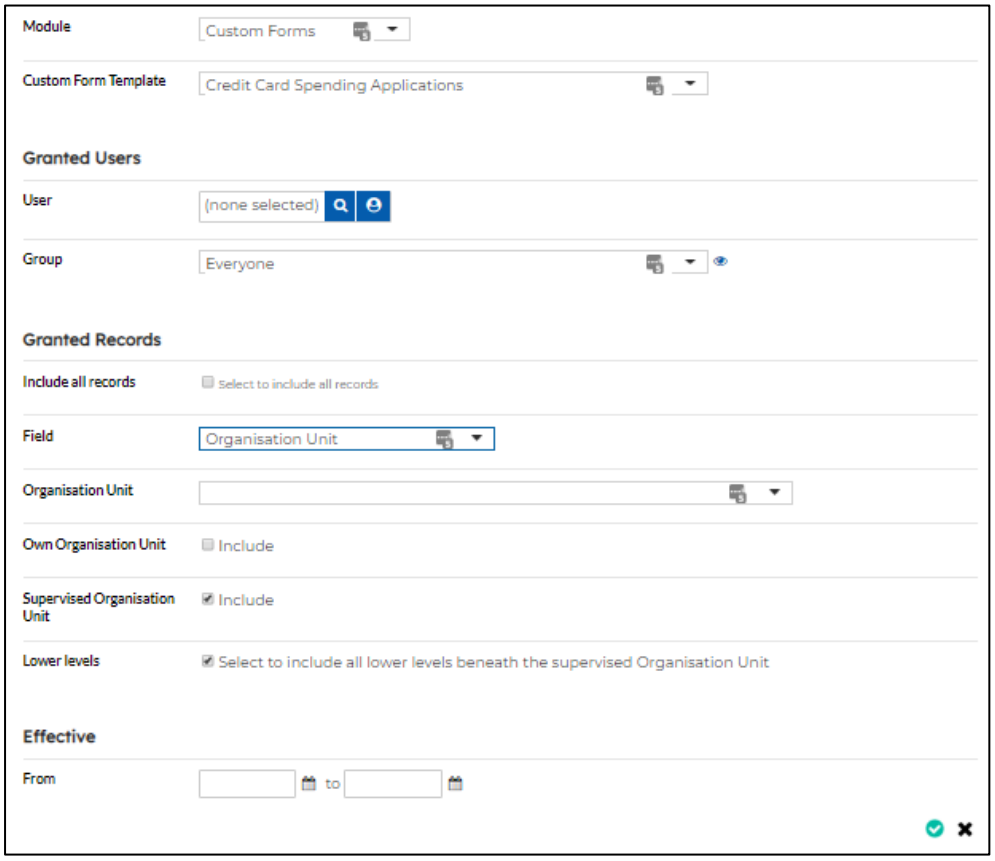


Reporting Permissions

Drag a column header here to group by that column

#	Module	Granted Records	Granted Users	Start	End
	Accountable Forms	Secretary's Office (and lower levels)	John Martinez (john) (user)		
	Accountable Forms	Secretary's Office (and lower levels)	Senior Management Group (group)		
	Accountable Forms	Secretary's Office (and lower levels)	Steve Winning (steve) (user)		
	Accountable Forms	Supervised Organisational Structure(s) (and lower levels)	Everyone (group)		
	Asset Disposal/Write Offs	Organisational Structure = Supervised Organisational Structure(s) (and lower levels)	Everyone (group)		
	Contractors	Organisational Structure = Supervised Organisational Structure(s) (and lower levels)	Everyone (group)		
	Corrective Actions Reports	Organisational Structure = Supervised Organisational Structure(s) (and lower levels)	Everyone (group)		
	Credit Card Requests	Organisational Structure = Supervised Organisational Structure(s) (and lower levels)	Everyone (group)		
	Driver Registrations	Organisational Structure = Supervised Organisational Structure(s) (and lower levels)	Everyone (group)		
	Expenditure Requests	Organisational Structure = Supervised Organisational Structure(s) (and lower levels)	Everyone (group)		

Select the add or edit icon.



The following configurations are available.

Module – Selects the module reporting permissions are to apply to.

Custom Form Template – Selects the custom form the reporting permissions are to apply to. Only applies if Custom Forms selected as the module

Granted Users

This section determines the users who will be granted permissions. An individual user and/or a group may be selected.

Granted Records

This section determines the records to be available for reporting based on various criteria. The following criteria options are available.

Include all records – Grants permission to report on all records with no restrictions.

Field – Grants permission to records based on the values of the selected custom field within a custom form. Only custom fields with answer type Organisation Unit or Lookup List may be selected. Only applies if Custom Forms selected as the module.

Organisation Unit – Grants permission to records where the selected organisation unit matches the organisation unit of the record. Permission may also be granted to all levels below the organisation by checking the Lower levels option. Only applies where the the selected module is Custom Forms and the Field selected has an answer type of Organisatioin Unit, or any other module is selected.

Own Organisation Unit – Grants permission to records where the granted user's current organisation unit matches the organisation unit of the record. Permission may also be granted to all levels below the organisation by checking the Lower levels option. Only applies where the the selected module is Custom Forms and the Field selected has an answer type of Organisatioin Unit, or any other module is selected.

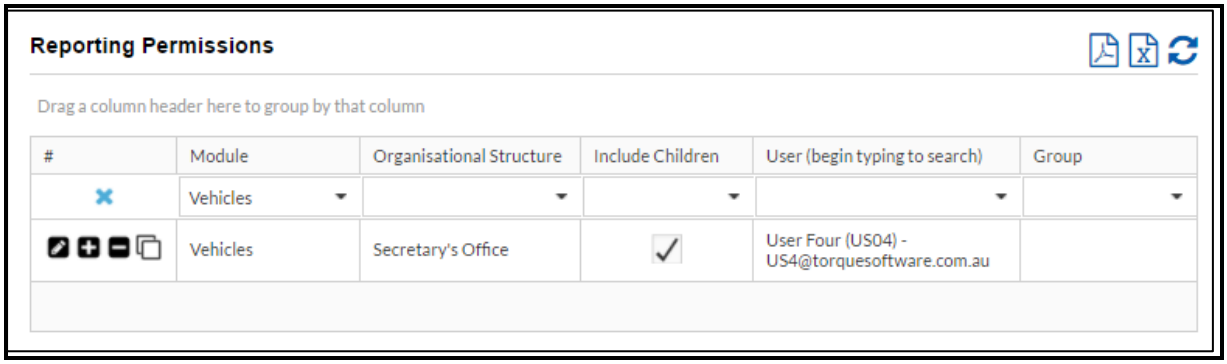
Supervised Organisation Unit – Grants permission to records where the granted user is the nominated supervisor of the organisation unit of the record. Permission may also be granted to all levels below the organisation by checking the Lower levels option. Only applies where the the selected module is Custom Forms and the Field selected has an answer type of Organisatioin Unit, or any other module is selected.

Lookup value – Grants permission to records where the selected lookup value matches the lookup value field in a custom form. Permission may also be granted to all levels below the lookup value by checking the Lower levels option. Only applies where the the selected module is Custom Forms and the Field selected has an answer type of Lookup Value.

Effective

This section determines the time period the reporting permission is effective. Either a from date and/or end date may be selected. Leave blank if no restriction is to apply.

Filtering Reporting Permissions



The first line in the table are the filter options. Click on the down arrows and select an option to limit to the view to only those items required. Click on the blue cross to remove the filter or select the Refresh button at the top right of screen.

Exporting Reporting Permissions

Part or all the information contained in Reporting Permissions can be exported to PDF or Excel.

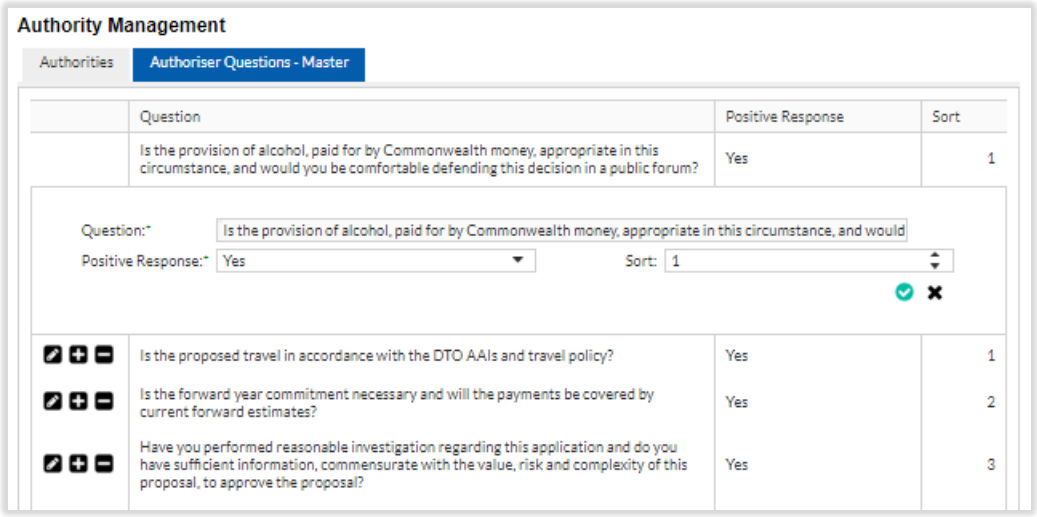
1. Apply any filters required to limit the information exported.
2. Click on the PDF or Excel icons at top right of screen.
3. A link will appear at the bottom left of screen once the file is ready.
4. Click on the link to open the file.

MAINTAINING AUTHORITIES

Authorities define the authorities users may exercise to action a workflow stage in Custom Forms. An authority may be a statutory authority or another type of authority which allows a user to perform a workflow action. When an authority is exercised by the authoriser, an outcome is recorded which either authorises or does not authorise the workflow step. Authorities also define the group of users who may be selected to exercise the authority. Authorities are used in Expense Types and Custom Forms. Authority settings are maintainable by users who are members of the group with Authority Administrator permission. Authority maintenance is available from the menu system (usually System Administration > Authorities) or by selecting alt+M and searching for "Administration - Authorities".

Authoriser Questions – Master

Master list of questions an authoriser must answer when exercising an authority.



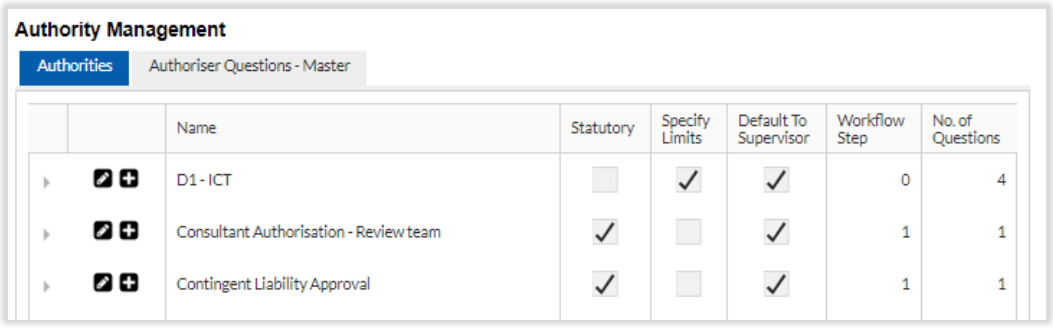
Authority questions have the following fields.

Question – Question text.

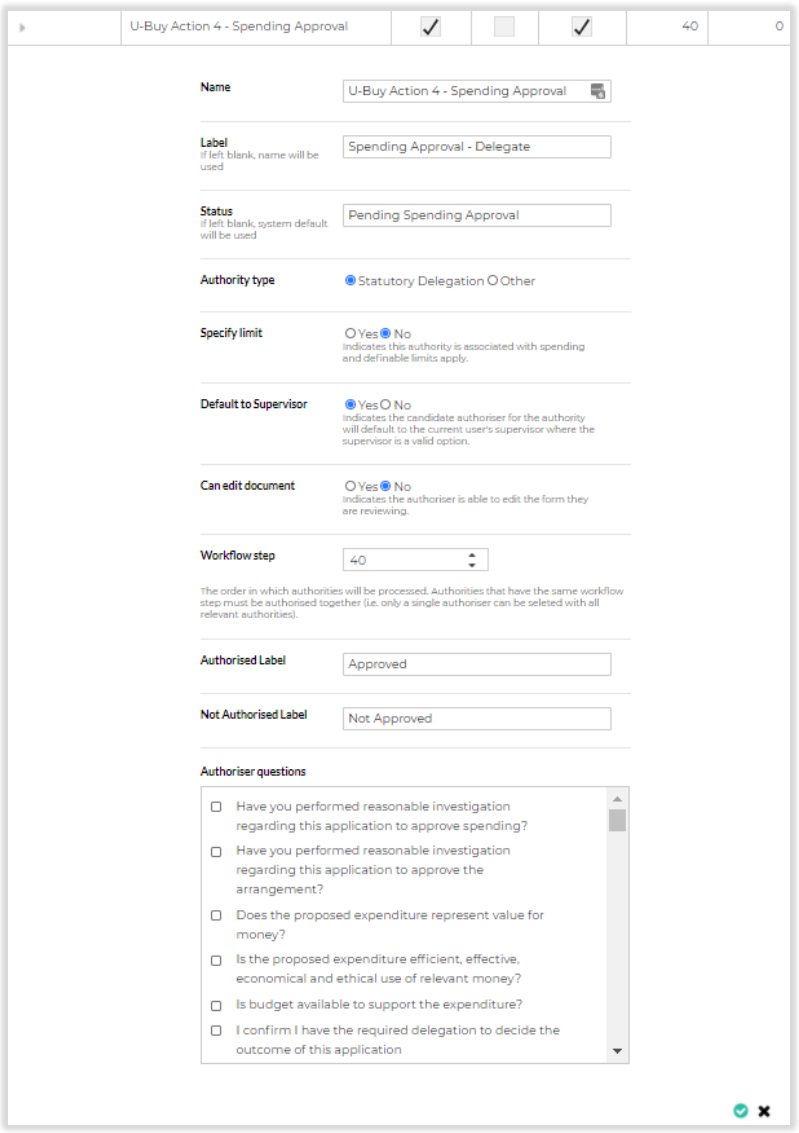
Positive Response – The response expected when exercising an authority to accept.

Sort Order – The order the question is displayed in when multiple questions apply for an authority.

Authorities



Authorities have the following fields.



Name – Name of the authority.

Label – Label to be used for the authority in the workflow section of a custom form. If left blank the Name will be used.

Status – Status to be displayed in the orient strip when the authority is the current workflow step. If left blank then "Pending Review" will be used.

Authority type – An authority may be a statutory authority or another type of authority which allows a user to perform a workflow action

Specify limit – Indicates the authority is restricted by spending limits and the spending limits will be specified. Note: while an authority may be restricted by spending limits, this field should only be set to Yes if the spending limits are to be specified for the Authority.

Default to supervisor – The proposed authoriser will default to the current user's supervisor if this is a valid option.

Can edit document – Sets if the authoriser has permission to edit the document prior to exercising their authority.

Workflow step – When more than one authority is required, indicates the order the authorities will be workflowed.

Authoriser Questions – The questions the authoriser must answer when exercising their authority. Selected from the authority question master list.

Authorised Label – The label used for the outcome option where the workflow step is authorised. E.g. "Approved", "Accepted" etc.

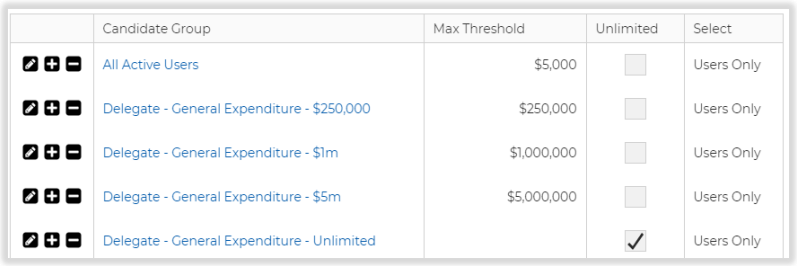
Not Authorised Label – The label used for the outcome option where the workflow step is not authorised. E.g. "Not Approved", "Rejected" etc.

Authority Groups

Identifies the users who may be selected to exercise an authority.

Note: the users in these groups will not necessarily have the required authority. Being a member of the group only allows the user to be selected. The user making the selection and the selected user must ensure the selected user has the required authority.

Select the small grey arrow next to the Authority to view the authority groups.



	Candidate Group	Max Threshold	Unlimited	Select
	All Active Users	$5,000	☐	Users Only
	Delegate - General Expenditure - $250,000	$250,000	☐	Users Only
	Delegate - General Expenditure - $1m	$1,000,000	☐	Users Only
	Delegate - General Expenditure - $5m	$5,000,000	☐	Users Only
	Delegate - General Expenditure - Unlimited		☑	Users Only

Candidate Group – The group containing the users and/or groups who are candidates for selection to exercise the authority. Select a group by typing part of the group name into the Group. Select from the list of matching groups.

Max Threshold – The maximum amount than can be approved when limits are specified. Note: this field is only available when limits are specified.

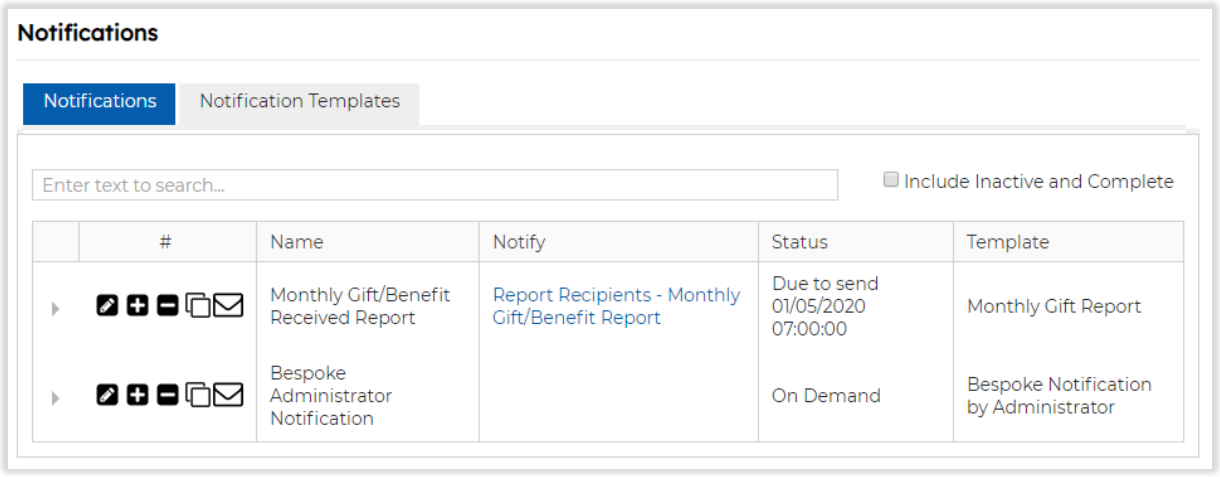
Unlimited – Indicates the maximum amount than can be approved is unlimited. Note: this field is only available when limits are specified.

Select – Indicates whether a group and/or a user may be selected to exercise the authority. Options are;

- **Users Only** – Only a user from the candidate group may be selected.
- **Groups Only** – Only a group contained in the candidate group may be selected. In this case, all members of the group will be able to access the custom forms from their in-tray.
- **Users and Groups** – A user of a group contained in the candidate group may be selected. If a group is selected to exercise the authority, all members of the group will be able to access the custom form from their in-tray.

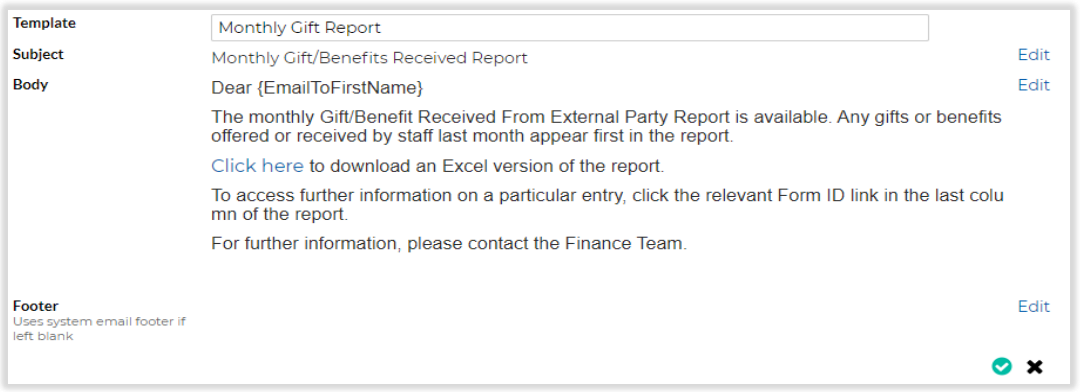
MAINTAINING NOTIFICATIONS

Allows notifications to be sent by email to users. Emails may sent at a specified time, on demand, or at recurring times for a defined interval. Only system administrators may maintain notifications.


Notifications
Notifications
Notification Templates
Enter text to search...
Include Inactive and Complete
#
Name
Notify
Status
Template
Monthly Gift/Benefit Received Report
Report Recipients - Monthly Gift/Benefit Report
Due to send 01/05/2020 07:00:00
Monthly Gift Report
Bespoke Administrator Notification
On Demand
Bespoke Notification by Administrator

Notification Templates Tab

Allows the templates used for notification emails to be configured.



The following settings are available.

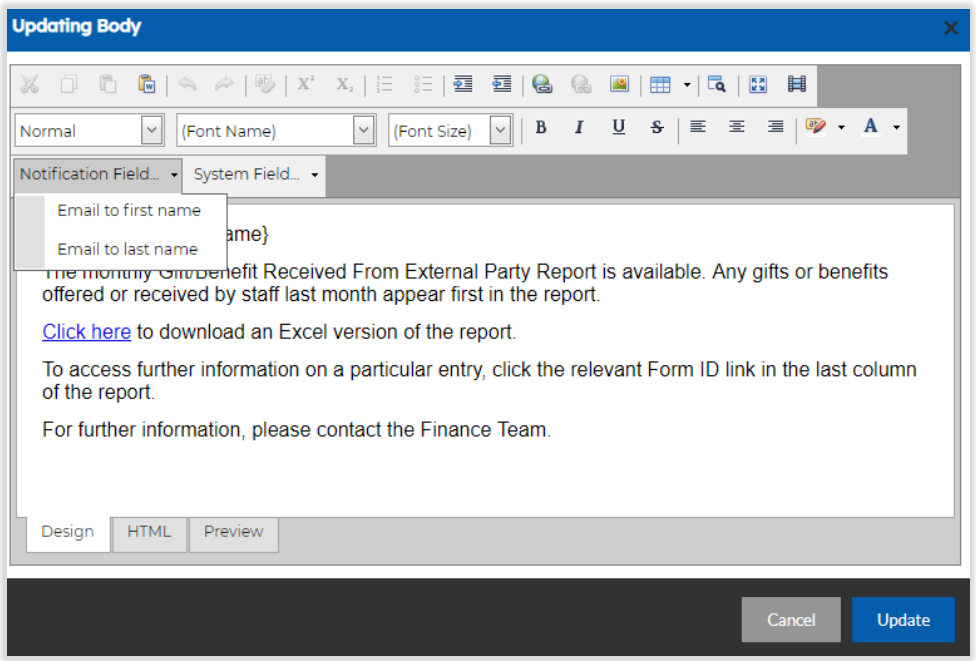
Template – Unique name for the template.

Subject – text to display in the subject line of the email.

Body – text to display in the body of the email.

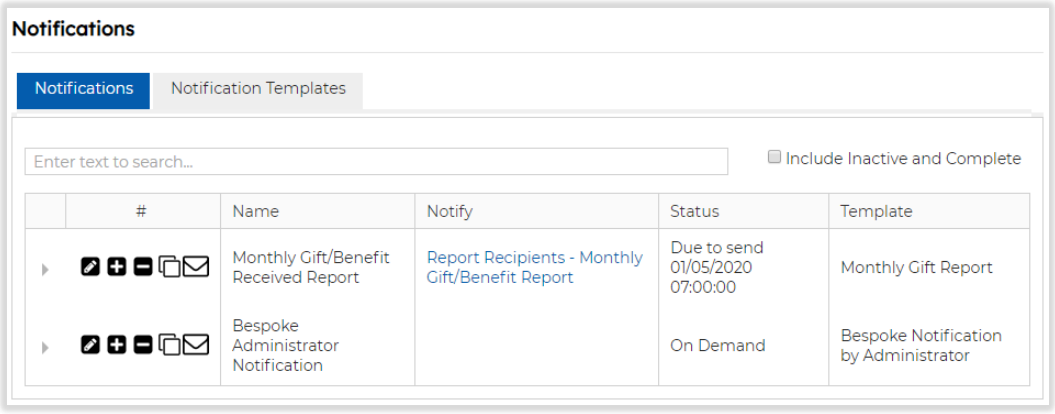
Footer – text to display in the footer of the email. The footer is always at the bottom of the email in a grey bar. If no value is entered the system email footer will be displayed.

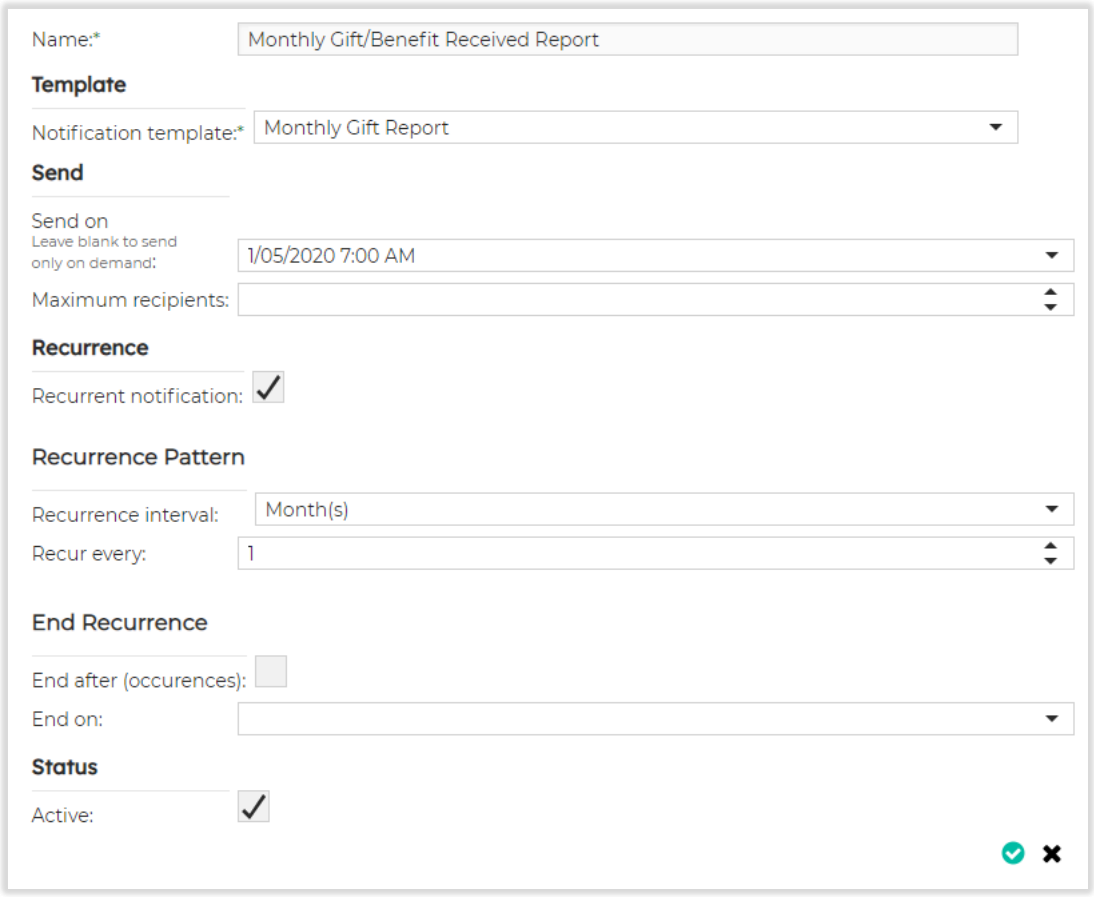
The text to display in a section can be modified by selecting the Edit button. Merge fields can be added by selecting from Notification Fields or System Fields lists.



Notifications

Configures the schedule for sending notification emails.





The following settings are available.

Name – Unique name for the notification.

Notification template – The notification template to use for the notification.

Send on – The date and time the notification is to be sent. Leave blank to only send on demand by selecting the ✉ button.

Maximum recipients – If the total number of recipients exceeds this value, the email will not be sent and instead an advisory email will be sent to the system administrators. Use this to prevent sending emails accidentally to large numbers of users.

Recurrent notification – Check if the notification is to recur after the initial Send on date and time. Recurring emails will always be sent on the time defined in the Send on date and time.

Recurrence interval – The time period (month or day) between each notification, starting from the date in the Send on date and time.

Recur every – The number of recurrence intervals between each recurring notification.

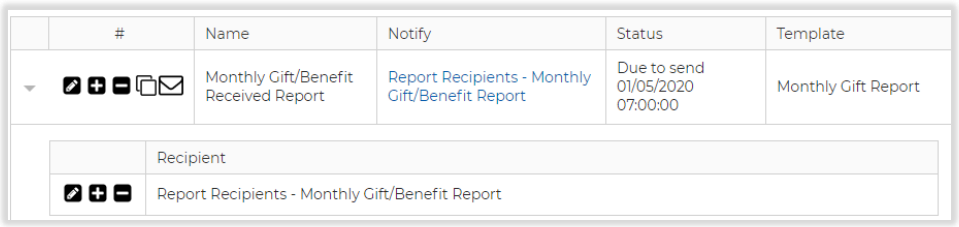
End after – Ceases the recurrent notification after a set number of recurrences.

End on – Ceases the recurrent notification on a specified date.

Active – Uncheck to temporarily or permanently cease the notification.

Notification Recipients

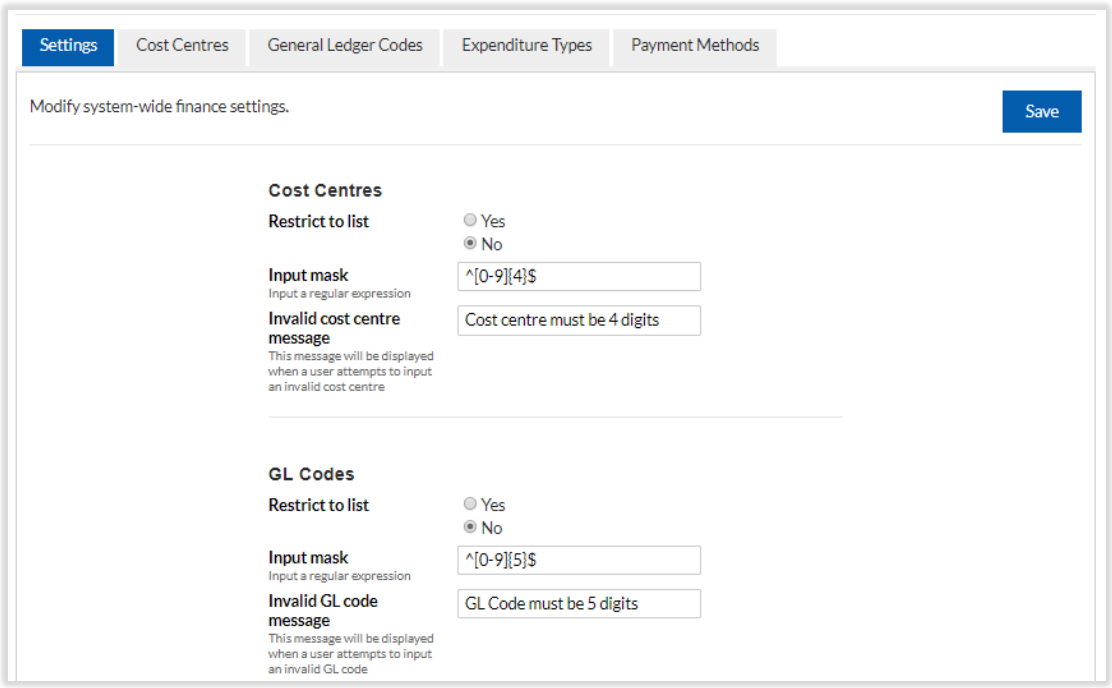
Select the small grey arrow next to the notification to configure the recipients of the notification. Any number of recipient groups may be configured.



> Warning: Do not select groups with large numbers of members as this may result in numerous emails being sent.

MAINTAINING FINANCE SETTINGS

Finance settings are maintainable by users who are members of the group with Finance Administrator permission, set in system settings. Finance settings are available by selecting System Administration > Finance Settings.



Settings

Cost Centres

Restrict to list – If Yes, cost centre must be selected from the valid list of cost centres maintained in Finance Settings.

Input mask – If entered, cost centres must match the regular expression. Any regular expression can be used. The example above requires the cost centre to be four numeric characters.

Invalid cost centre message – message displayed if cost centre does not match input mask.

GL Codes

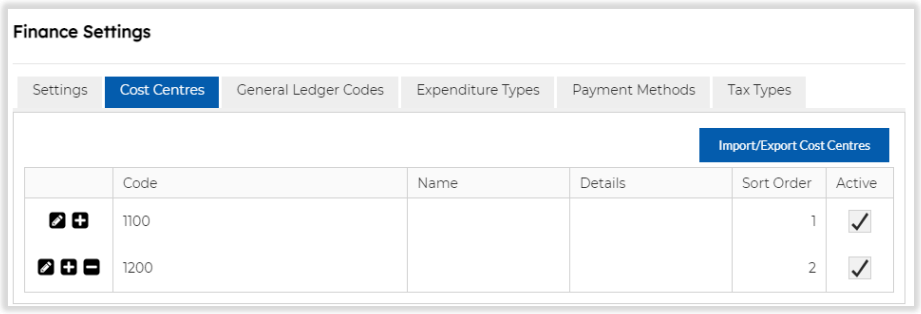
Restrict to list – If Yes, general ledger codes must be selected from the valid list of general ledger codes maintained in Finance Settings.

Input mask – If entered, general ledger codes must match the regular expression. Any regular expression can be used. The example above requires the general ledger codes to be five numeric characters.

Invalid cost centre message – message displayed if the general ledger code does not match input mask.

Cost Centres

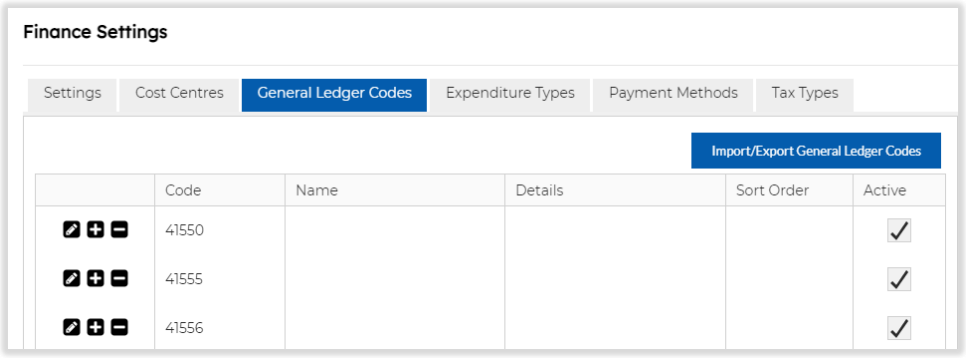
List of valid cost centres. Used when a lookup list of cost centres is displayed.



Cost centres may be imported and exported via csv file.

General Ledger Codes

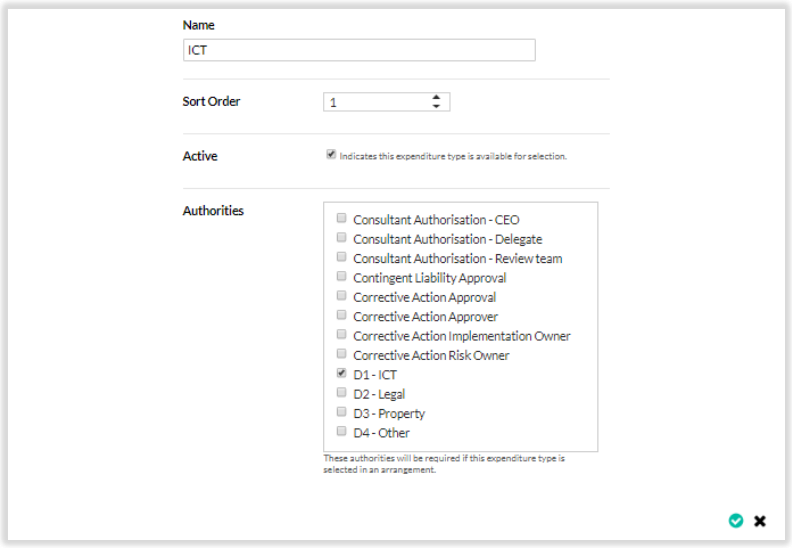
List of valid general ledger codes. Used when a lookup list of general ledger codes is displayed.



General ledger codes may be imported and exported via csv file.

Expenditure Types

List of valid expenditure types used in custom forms where expenditure approval is required. Expenditure types are linked to the Authorities required to approve the type of expenditure.



Payment Methods

Configures the payment methods available in payments processing and contingent liabilities.

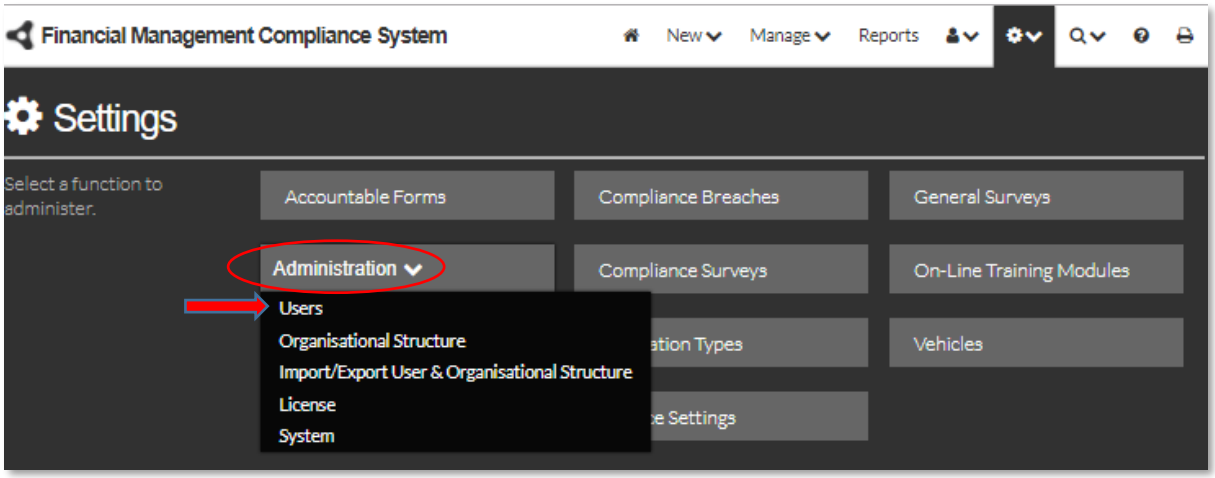
	Method	Sort Order	Active
	Bitcoin		✓
	Cash		✓
	Cheque		✓
	Credit Card		✓
	Direct Debit		✓
	EFT		✓
	EFTPOS		✓
	Gift Card / Voucher		✓
	Money Order		✓
	Paypal		✓

MAINTAINING SYSTEM USERS

Only System Administrators will have permission to maintain users on a system wide basis.

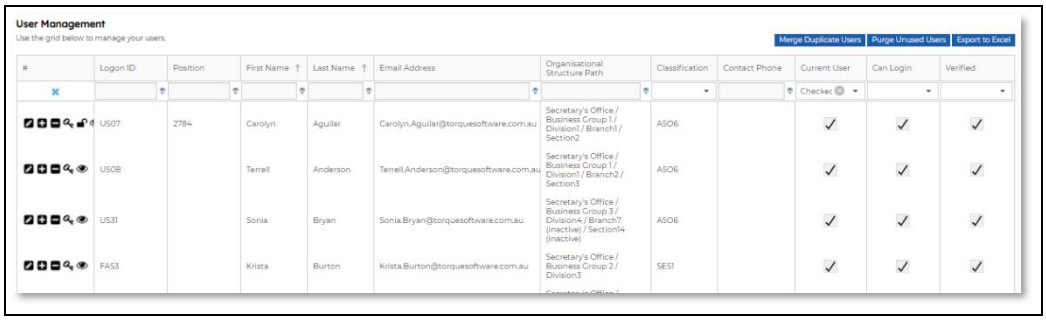
In this section of the system, Administrators can view, edit and maintain the users in Lighthouse affecting all modules.

To access these functions, go the System Administration icon, and select the Users option from the Administration Menu.



Updating System Users Information

This screen contains a large amount of information for each user, and the scroll bars at top and side of screen may be used to shift the view to see further information. Note: Users are filtered by default to only show Current Users.



Quick Tip: For more info on standard grid functions, please see General Concepts - Grid Functions.

Filters can be applied to columns using at the top of each column. Click the to remove filters.

Display order in which the users are shown in the table can be set by clicking in the column heading. This will group all users according to the heading criteria selected. Ascending or descending order can be chosen by clicking on the direction arrow displayed in the header. For example, to order users by last name, click in last name heading, to show "A" at top of list select the arrow up, to show "Z" show first select arrow pointing down.

Action Buttons

The following actions may be performed by selecting the following buttons from the User management list screen.

- Edit the user record.
- Add a new user.
- Delete user. Only available if the user is not linked to any records.
- Reset user's password. Only available when authentication is by logon and password.
- View user's permissions, and links to records.
- Unlock the user. Only available where user has failed the Account lockout rules and is currently locked out.

User Fields

Logon ID – is the users Logon ID displayed throughout the application.

Alternate Logon ID – is an alternative logon the user may also use to logon.

AGS Number – a non mandatory field to record the users AGS or corporate HR Number.

Position – User's position within the organisation. Can be any text value.

First Name – User's first name.

Last Name – User's last name.

Email Address – Email address used to send emails to the user.

Organisation Structure – the lowest level of the organisation unit the user belongs to.

Organisation Structure Path– the organisation unit the user belongs to.

Manager – The user's immediate manager. If this field is not completed, the supervisor of the user's organisation unit will be used to determine the user's manager.

Classification – The user's job classification level.

Preferred Salutation – Can be used to record a specific salutation.

Contact Phone. – contact phone number for the user.

Dashboard style – the style of dashboard the user will see. It can be set to the default set up by the System Administrator in System Settings, changed to Tile or List.

Change dash style – ticking this box allows the user to change their dashboard style to their requirements whenever they choose.

Never Email - nominated user will never receive a workflow email (admins can still send Survey reminders and forgotten password emails).

Current User - this indicates the user is current in the system and will appear in appropriate user lookups. Unchecking this field will also stop the user from being able to login.

Can Login - only users with this permission can access the system. Disable this for users who are current but should not have system access.

Verified - if you require email address verification prior to allowing users to login, this flag will indicate whether they have clicked the link in their verification email.

Export Users to Excel

Allows the administrator to export the user data to an excel spreadsheet.

Merge Duplicate Users

Allows two user records to be merged. Should only be used where duplicate user records exist for the same person. Merges all records related to both users into a single user. Select the Merge Duplicate User button from the User Management screen.

Set Primary Alternate Login to Duplicate Login – If checked, will set the Alternate Logon ID of the primary user to the Logon ID of duplicate user.

Purge Unused Users

Deletes all users where the following criteria applies;

- The user is not a Current User and;
- The user is not linked to any transactions or any other record.

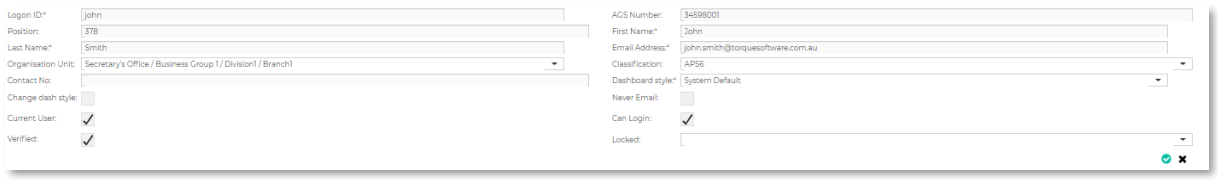
Provides a way to bulk remove users who no longer have any requirement to be recorded as a user.

Editing and Adding Users

To add a new user, click on any of the Add icons

To editing an existing user, click on the edit icon on their line

An editing dialog box will be displayed.



Complete the fields as described above. And Click on the save button .To cancel click on the cancel button

Reset Password

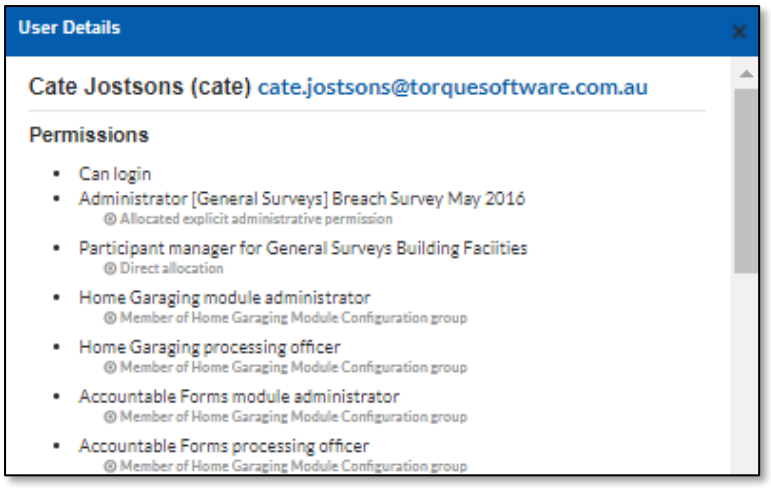
This function is not used for organisations that use single sign on – where users log onto their computer and access Lighthouse through the intranet.

The reset password function applies for users who log into Lighthouse independently of their organisation's intranet. If they have forgotten their password or have unsuccessfully attempted to login more that the System Administrator has set the system to accept (See System Settings).

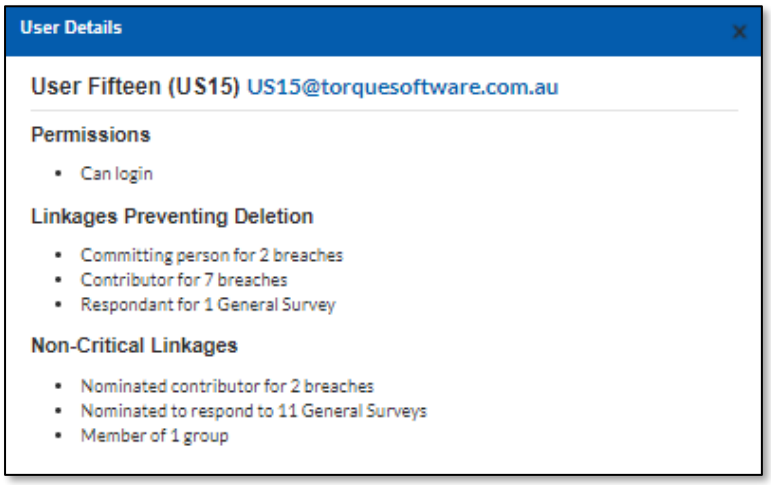
By clicking the Reset Password button , Lighthouse will send an automated email to the user's registered email address with a new temporary password.

View a User's Permissions

To view a User's permissions and links within the system, click on the View icon .



Permissions are all the administrative permissions the user has been granted across all modules in Lighthouse.



Linkages are tasks and functions the user is connected to throughout Lighthouse. Some links will be non-critical, while others are so critical that by deleting this user, data within Lighthouse will be compromised, in which case, the system will not allow this user to be deleted.

Deleting Users

Important: Before deleting a User, it is strongly recommended that User Details be viewed as described above, for linkages.

If there are no linkages preventing deletion, click the Delete icon ⛔.

A warning will be displayed if there are any outstanding items against the user or any linkages that will prevent deletion. Click OK to continue or Cancel to abort the deletion.

Some links are so critical to the integrity of linked data that by deleting this user, data within Lighthouse will be compromised. In this case the system will not allow this user to be deleted.

To prevent the user being displayed in standard drop lists to be selected for any new actions and functions in the system, untick the Current Employee field for the user. This will effectively archive the user, while maintaining the integrity of all other information they have been linked to in the past.

Printing and Saving the User Management Screen

Once any filters, or sort orders, have been applied to the User Management screen, the results can be exported to a CSV file.

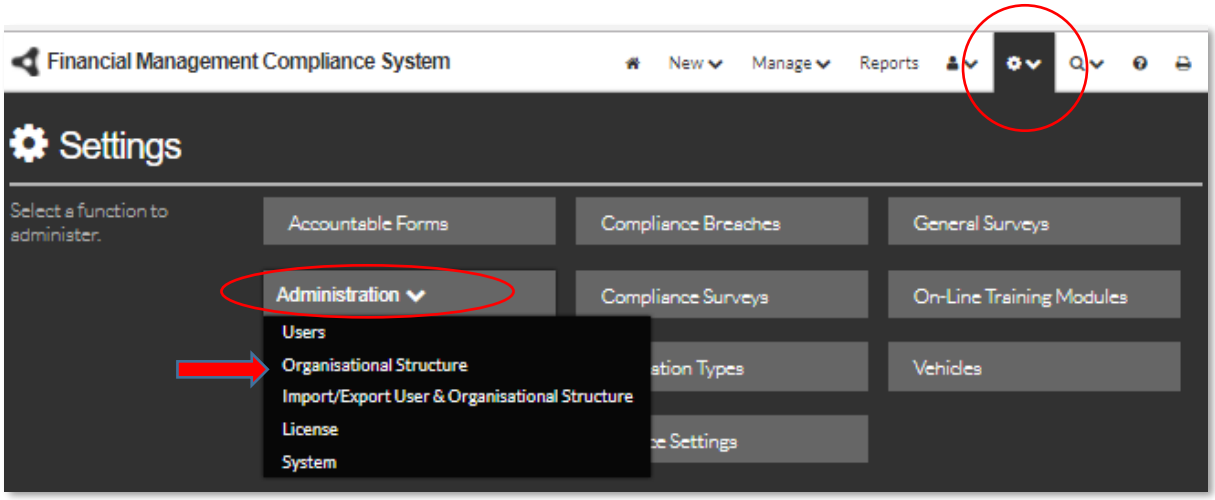
Simply apply the filters and sort order, then click on *Export current view to Excel* text at the top right of screen. The download link will appear on the screen. Click to open.

MAINTAINING THE ORGANISATIONAL STRUCTURE

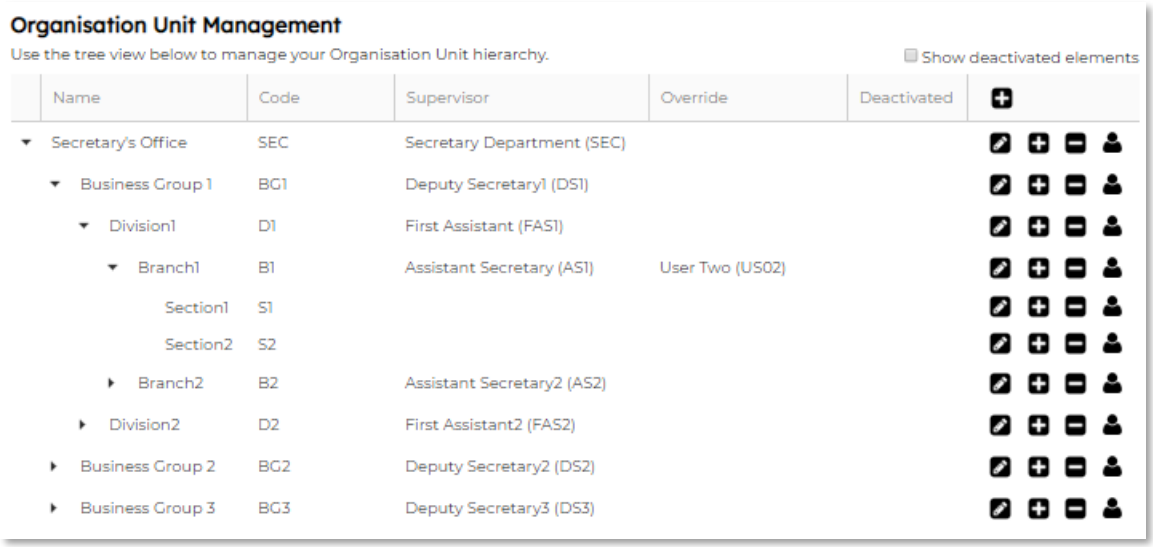
To maintain optimal usability of Lighthouse, it is strongly advised that your organisational structure is kept up as up to date as possible. It is also important that the organisational structure is in place and accurate when you import users so that they align in the correction units.

Viewing and Ad hoc Maintenance of the Organisational Structure

To view the current organisational structure, go to System Administration, then Administration and Organisational Structure.



The organisational structure is displayed in hierarchical format that can be expanded or contract by clicking on the expand/contract arrows. See the example below.



Quick Tips:

- You can move nodes by dragging and dropping them; dropping a node on the Name column heading will place it at the top of the hierarchy.
- When copying nodes, hold shift to copy rather than move them.

Name field - is the text presented to the user when they are selecting an Organisational Structure.

Code field - is used to uniquely identify this code and is vital for integrated branch updates (where applicable).

Supervisor field- is used to identify the person who manages the organisation unit.

Override – Shows the user who is performing the duties of the Supervisor as at the current date. This overrides the selection of the supervisor by the system in all locations. E.g. where the supervisor is defaulted as an approver. Select the button to enter an override.

Legal Entity – This is the legal entity the organisation unit belongs to. This is only available if your organisation is using legal entities.

Deactivated field – shows the date the organisation was deactivated.

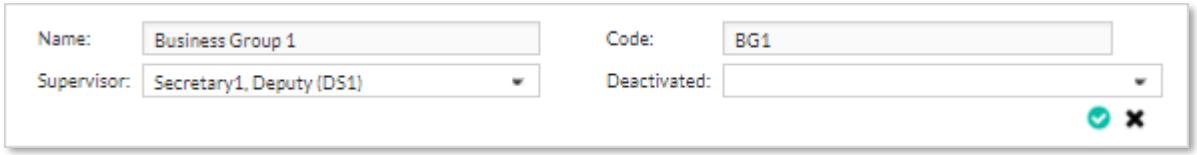
Clicking the **Show deactivated elements** link will show all active branches as well as any that have ever been deactivated all in the one view.

Note on Supervisors: When you allocate a user as a Supervisor, they will begin to appear in the Supervisor look-ups throughout the system. They will also have visibility of all data within their allocated branch and those hierarchically below it.

When the system is looking up the nominated Supervisor for a selected branch, if the branch has no Supervisor, the system will continue looking up the hierarchy until it finds a Supervisor or it hits the top of the tree.

Editing an existing Organisational Unit

To edit an existing organisational unit, click on the edit icon for that unit.



Make the required changes and click on the Save icon.

Moving an Organisational Unit

Organisational units can be moved in the hierarchy by clicking dragging the unit to drop it in its new location.

Create a new Organisational Unit

To create a new organisational unit, click on the new icon of the parent unit it will sit under. Enter the details required and click on the Save icon.

Deleting Organisational Units

Organisational units can only be deleted if there is no data linked to that unit. If data is linked to the unit, it can be deactivated. This means that all data related to that unit will remain intact and preserve the integrity of the data, but the organisational unit will not be visible by default.

To delete an organisational unit, click on the Delete icon for that unit. If the function is possible, a confirmation box will be displayed. Select OK to delete or Cancel to abort the deletion.

If there is data linked to the unit dialogue box will display the reasons why it cannot be deleted. Select OK and proceed to Deactivate the unit.

Deactivating Organisational Units

To deactivate an Organisational click on the Edit icon of the unit. Click into the Deactivated field and select the date the deactivation date to be effective.

To reactivate a unit, simply clear the deactivated field.

Deactivated units can be viewed by checking the *Show deactivated elements* option at the top of the screen.

IMPORTING USERS AND ORGANISATION STRUCTURE

The best approach to maintain users and the organisation structure is to regularly import the organisation structure and users via csv or Excel file. This information is usually extracted from the Human Resources system or some other appropriate source.

Importing users and organisation structure is performed by creating a data source which allows the following to be configured;

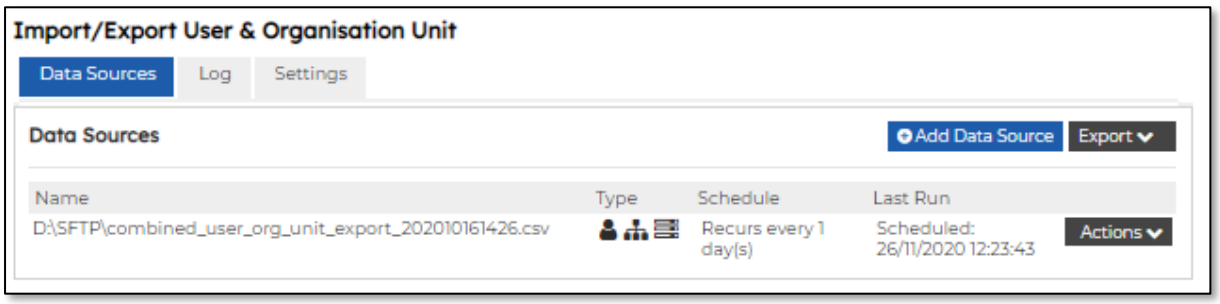
- Source of the import file
- Mapping the contents of the import file to Lighthouse user and organisation unit fields
- Scheduling the timing of the import
- Behaviour of the import process.

Managing Data Sources

Data sources are managed from the Data Source tab on Import/Export & Organisation Unit screen.

This screen is available by selecting Alt M and then "Administration - Import Users and Organisation Structure" or by selecting the appropriate menu item.

Users must be a member of the group nominated as Data connection administrators in System Settings or have been given configuration permission to a Data Source to be able to manage data sources.



Existing data sources are listed. Actions may be performed against existing data sources by selecting the Actions button.

Creating a Data Source

Users must be a member of the group nominated as Data connection administrators in System Settings to be able to create a data source.

A data source is created by selecting Add Data Source from the Import/Export & Organisation Unit screen.

Data Source Location

On creation of the new data source, the location of the import file is first identified. Two options are available;

API Integration – Import file will be provided via an Application Program Interface.

Browse for File – User will be requested to browse to the import file each time an import is performed.

After selecting the import file location, select Next: Configure Data Map to edit the data source.

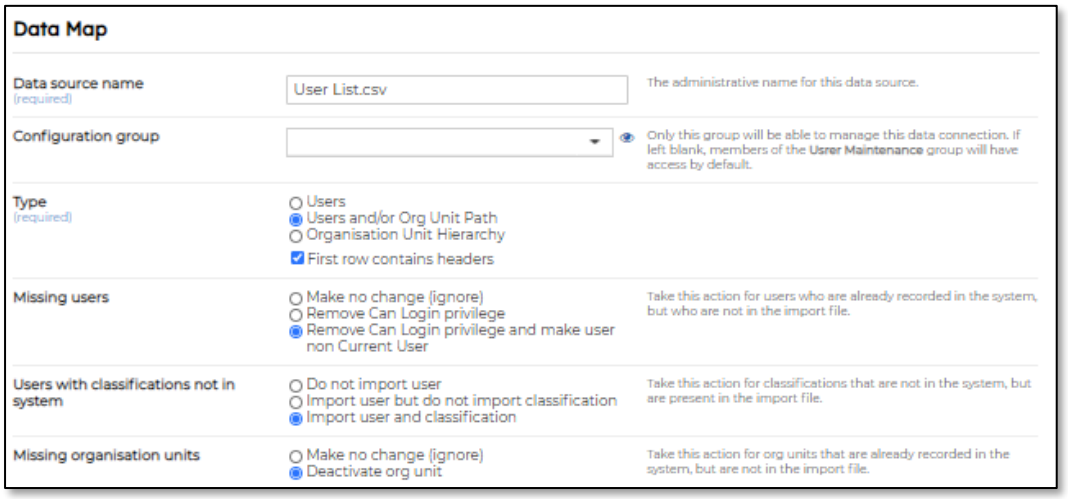
Editing a Data Source

A data source can be edited by either of the following;

- Selecting the Configure Data Map button from the Data Source Location screen
- Selecting Action > Edit from the Import/Export & Organisation Unit screen

Data Map

The data map configures the behaviour of the import and maps the import file columns to Lighthouse user and organisation unit fields.



Name, Configuration Permission, and Import Behaviour

Data source name – unique name used to identify the data source.

Configuration group – the group of users who have permission to maintain the data source. If left blank, only users who are members of the group nominated as Data Connection Administrators in System Settings are able to maintain the data source. Note: Members of the group nominated as Data Connection Administrators in System Settings are always able to maintain all data sources.

Type – defines the type of information included in the import file.

> **Users** – user information with the user's organisation unit defined by a single organisation unit code. Note: any new organisation units in this file must first be imported via an import file of type Organisation Unit Hierarchy.
>
> **Users and/or Org Unit Path** – user information with the user's organisation unit defined by a full organisation unit path with each organisation unit level in separate columns. The organisation unit path is also used to create the organisation structure.
>
> **Organisation Unit Hierarchy** – organisation structure information in a hierarchical format.

Missing users - select the action to take when users are omitted from the import file.

Make no change (ignore) – no action will be taken for users not in the import file.

Remove Can Login privilege – Can Login will be turned off for users not included in the import file.

Remove Can Login privilege and make user non current user - Can Login and Current User will be turned off for users not included in the import file.

Users with classifications not in the system - select the action to take for users where the user's classification in the import file is not recorded as a valid classification in Lighthouse.

Do not import user – User will not be imported.

Import user but do not import classification – User will be imported, but the user's classification will be left blank.

Import user and classification – User will be imported and the classification added to the recorded classifications in Lighthouse.

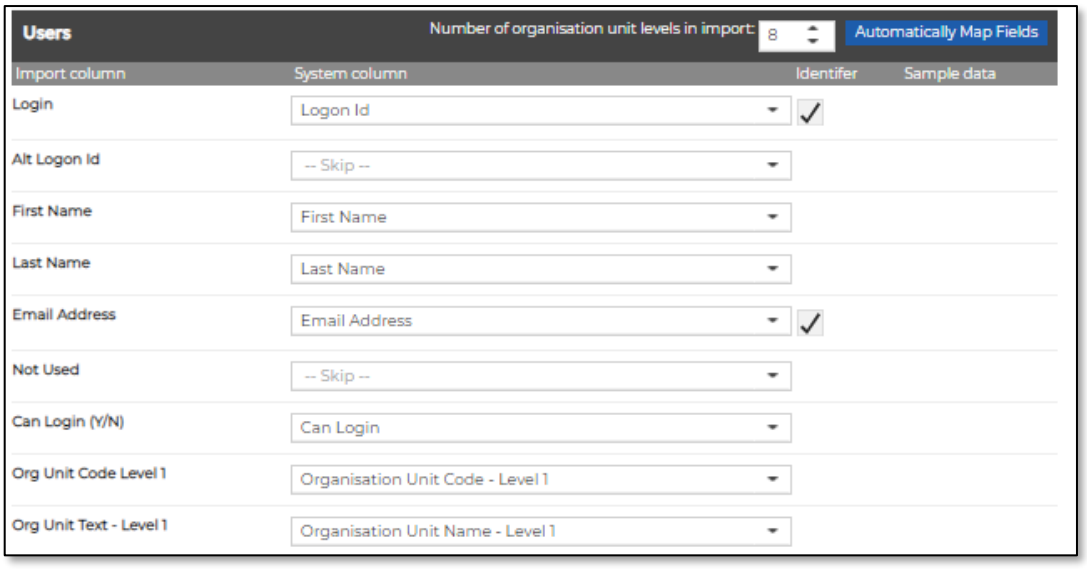
Missing organisation units - select the action to take when organisation units are omitted from the import file.

Make no change (ignore) - no action will be taken for organisation units not in the import file.

Deactivate org unit - sets the organisation unit's deactivation date to the date of the import for organisation units not in the import file.

Data Definition.

The data definition allows columns in the import file to be mapped to Lighthouse system user and organisation structure fields.



Number of organisation unit levels in import – only applies to data sources of type **Users and/or Org Unit Path**. Nominates the number of organisation unit levels in the import file. A maximum of eight is allowed.

Automatically Map Fields – attempts to match import file columns to Lighthouse system fields by using the import file column name. This action is automatically performed for new data sources.

Import column – The name of import file field, obtained from the first row of the import file.

System column – The name of the Lighthouse system field to be mapped to the import file field in the Import Column. See Import File Specification section for the available Lighthouse system fields and related operation rules.

Identifier – Indicates the unique identifiers to use to match users in the import file with users in the Lighthouse system. Up to three identifiers can be selected. If a user in Lighthouse is found matching any of the identifiers of the user in the import file, the users will be considered to match.

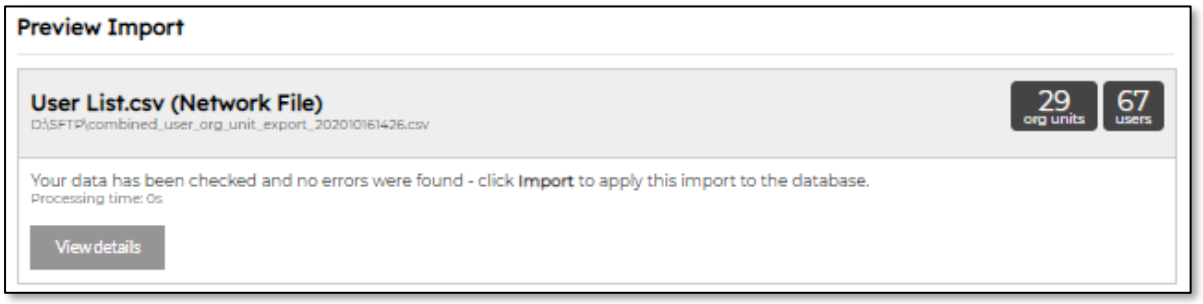
Sample data – displays the first few rows of data in the import file as a sample.

Importing on Demand

A data source can be imported on demand by either of the following;

- Selecting the Preview Import button from the Data Map screen
- Selecting Action > Import from the Import/Export & Organisation Unit screen

The Preview Import screen will first display which shows information about the import. Further information, errors and the complete import file can be obtained by selecting the View details button.



Import the import file by selecting the Import button at the bottom of the screen.

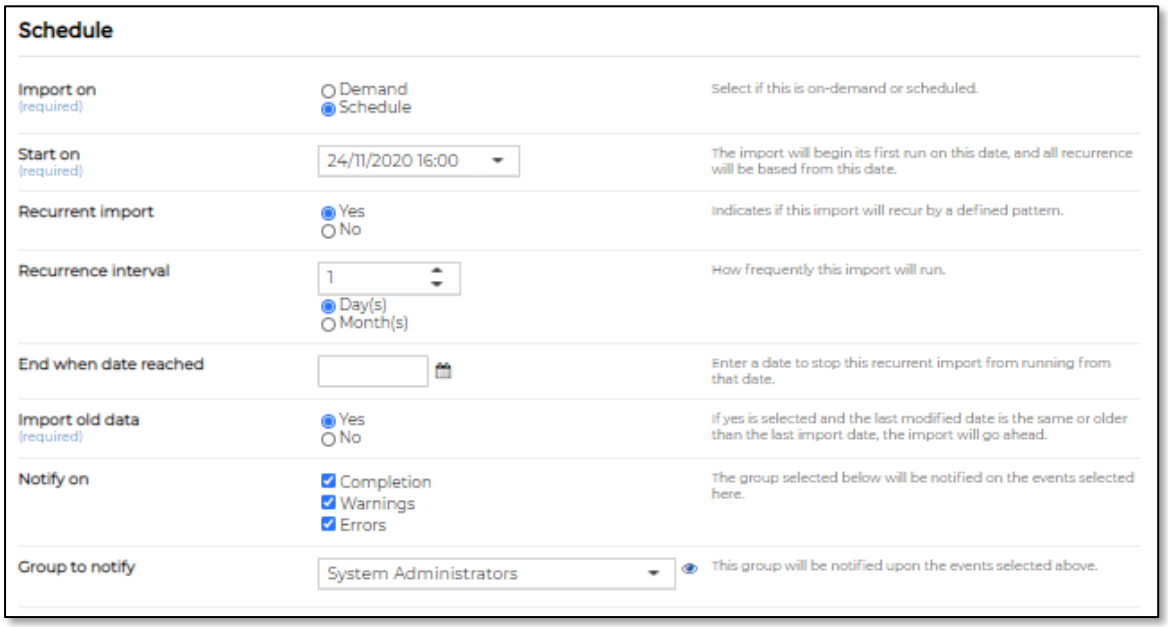
Import Scheduling

Scheduling allows the import to be performed at a nominated time and also on a recurring basis. Only data sources with an API file location can be scheduled.

An import can be scheduled by either of the following;

- Selecting the Configure Schedule button from the Preview Import screen
- Selecting Action > Schedule from the Import/Export & Organisation Unit screen

The Preview Import screen will first display which shows information about the import. Further information, errors and the complete import file can be obtained by selecting the View details button.



Import On – Identifies if the import will occur only on demand or be scheduled.

Start On – Start date and time for the first scheduled import.

Recurrent Import – Indicates if the import will recur after the first scheduled import.

Recurrence Interval – The number of days or months between recurring imports.

End when date reached – The last recurring import will occur on the selected date.

Import old data – If no is selected and the last modified date of the import file is the same or older than the last import date, the import will not be performed.

Notify on – Indicates the events that will be included in the import notification sent to the notify group after the import is completed.

Group to Notify – Group of users who will receive the import notification.

Exporting Data Source

An export can be obtained of the current Lighthouse users and/or organisation structure in the format configured in the data source by selecting Action > Import from the Import/Export & Organisation Unit screen.

Deleting Data Source

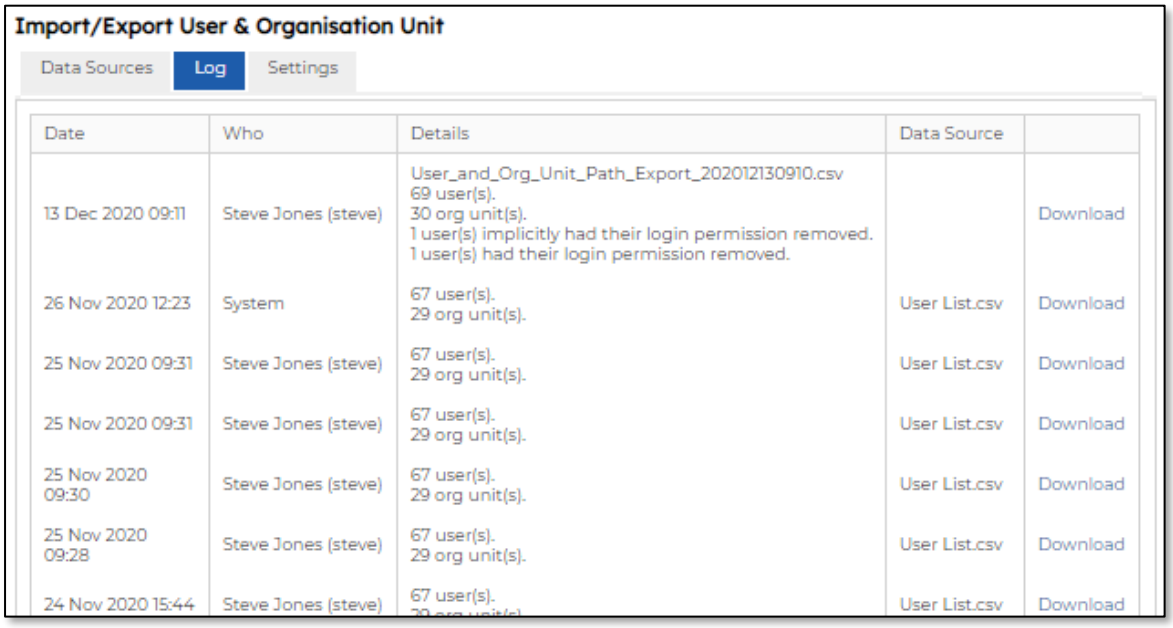
A data source can be deleted by selecting Action > Delete from the Import/Export & Organisation Unit screen.

Exporting Users and Organisation Structure.

Current users and organisation structure can be exported by selecting Export from the Import/Export & Organisation Unit screen. Note: exports may be used as templates for the import file used in a data source.

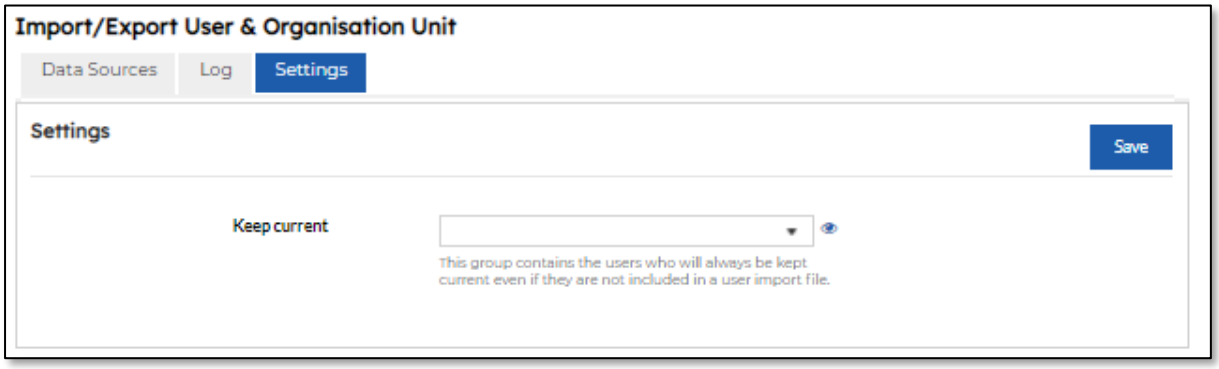
Import Logs

A log of all imports is available from the Log tab on Import/Export & Organisation Unit screen.



Select Download to download the details of any notifications and a copy of the import file.

Settings



Keep current - Allows a group of users to be defined who will always be kept current even if they are not included in an import file and the option "Remove Can Login privilege and make user non Current" is selected.

This option is useful to ensure staff (e.g. contractors), who may cannot be included in the import file, are kept current at each import.

Import File Specification

Users and organisation structure may be imported via a file with the following specification.

File Format

Import files must be in csv or Microsoft Excel format.

Column Headings

The first row may contain column headings.

System Fields

The columns in the import file must map to specified Lighthouse system fields.

Import files of type Users and Users and/or Org Unit Path containing new users must map to the following system fields at a minimum;

- At least one unique identifier being Logon Id, Email Address and/or AGS.
- First Name
- Last Name
- Email Address
- Organisation Unit if organisation unit is configured as a mandatory field in Lighthouse

Import file types Users and Users and/or Org Unit Path not containing new users must map to the following system fields at a minimum;

- At least one unique identifier being Logon Id, Email Address and/or AGS.
- One other field

Any system fields not mapped in an import file will be ignored and no change will be made to the system field value in Lighthouse.

The system fields available depend on the import file type.

Import File Types – Users, User and/or Org Unit Path

The following system fields are available for mapping for both Users and Users and/or Org Unit Path import file types.

System Column	Description	Behaviour
Login Id	Login Id of the user. Usually the network login or email address. May be used as the unique key to identify existing users in Lighthouse on import.	Mandatory Must be unique within both Login Id and Alternate Login Id
Alternate Login Id	An alternate Login Id of the user. Usually the network login or email address.	Mandatory Must be unique within both Login Id and Alternate Login Id
AGS Number	Australian Government Service Number	Optional
Position	User's position within the organisation's establishment	Optional
First Name	First name of user. May also contain middle names if required.	Mandatory
Last Name	Last name of user.	Mandatory
Email Address	Email address of user.	Mandatory Must be unique
Manager	Logon Id or Email Address of the user's direct manager	Optional
Classification	Classification of the user	Valid values are; • Empty (no value) – Current value will not be changed. • "Null" – The user's classification will be set to null. • Classification (e.g. EL2).
Preferred Salutation	Preferred salutation including name and any honorifics	Valid values are; • Empty (no value) – Current value will not be changed. • "Null" – The user's preferred salutation will be set to null. • Any other text value.
Contact Phone	User's contact phone number	Valid values are;

		• Empty (no value) – Current value will not be changed. • "Null" – The user's contact phone will be set to null. • Any other text value.
Dashboard Style	The presentation style of the home dashboard	Valid values are; • Empty (no value) – Existing Users - Current value will not be changed. New User – Set to "System Default" • "System Default" • "Tiles" • "List"
Change Dash Style	Defines if user can change their dashboard style.	"Y" – Yes "N" – No Null – Value unchanged for existing users. Defaults to "N" for new users.
Never Email	Defines if user is not to receive any emails.	"Y" – Yes "N" – No Null – Value unchanged for existing users. Defaults to "N" for new users.
Current User	Identifies the user as being current.	"Y" – User is current "N" – User is no longer current Null – Value unchanged for existing users. Defaults to "Y" for new users.
Can Login	Grants permission for the user to log into Lighthouse.	"Y" – User can log in "N" – User cannot log in Null – Value unchanged for existing users. Defaults to "Y" for new users.
Supervisor for Organisation Unit (Code)	User will be assigned as the supervisor of the nominated organisation unit code.	Optional Must be a valid organisation unit code if not null. Multiple columns may be mapped to this system field.

Import File Types – Users Only

The following system field is available for mapping for the Users import file type only.

System Column	Description	Behaviour
Organisation Unit (Code)	User will be assigned as belonging to the organisation unit with this code	Mandatory or Optional depending on settings in Lighthouse. Must be a valid organisation unit code if not null.

Import File Types – Users and/or Org Unit Path Only

The following system fields are available for mapping for the Users and/or Org Path import file type only.

Note: The org unit levels in the upload do not imply any particular type of org unit. They only reflect the relative levels of the organisation.

System Column	Description	Behaviour
Organisation Unit Code - Level 1	Code representation of the user's highest level organisation unit.	Mandatory Note: Up to 8 organisation unit levels may be entered.
Organisation Unit Name – Level 1	Description of the user's highest level organisation unit.	Mandatory
Organisation Unit Code - Level 2	Code representation of the user's second level organisation unit.	Mandatory if organisation unit at level 2 exists, null otherwise
Organisation Unit Name – Level 2	Description of the user's second level organisation unit.	Mandatory if organisation unit at level 2 exists, null otherwise
Organisation Unit Code - Level 3	Code representation of the user's third level organisation unit.	Mandatory if organisation unit at level 3 exists, null otherwise
Organisation Unit Name – Level 3	Description of the user's third level organisation unit.	Mandatory if organisation unit at level 3 exists, null otherwise
Organisation Unit Code - Level 4	Code representation of the user's fourth level organisation unit.	Mandatory if organisation unit at level 4 exists, null otherwise
Organisation Unit Name – Level 4	Description of the user's fourth level organisation unit.	Mandatory if organisation unit at level 4 exists, null otherwise
Organisation Unit Code - Level 5	Code representation of the user's fifth level organisation unit.	Mandatory if organisation unit at level 5 exists, null otherwise
Organisation Unit Name – Level 5	Description of the user's fifth level organisation unit.	Mandatory if organisation unit at level 5 exists, null otherwise

Organisation Unit Code - Level 6	Code representation of the user's sixth level organisation unit.	Mandatory if organisation unit at level 6 exists, null otherwise
Organisation Unit Name – Level 6	Description of the user's sixth level organisation unit.	Mandatory if organisation unit at level 6 exists, null otherwise
Organisation Unit Code - Level 7	Code representation of the user's seventh level organisation unit.	Mandatory if organisation unit at level 7 exists, null otherwise
Organisation Unit Name – Level 7	Description of the user's seventh level organisation unit.	Mandatory if organisation unit at level 7 exists, null otherwise
Organisation Unit Code - Level 8	Code representation of the user's eighth level organisation unit.	Mandatory if organisation unit at level 8 exists, null otherwise
Organisation Unit Name – Level 8	Description of the user's eighth level organisation unit.	Mandatory if organisation unit at level 8 exists, null otherwise

Import File Types – Organisation Unit Hierarchy Only

The following system fields are available for mapping for the Organisation Unit Hierarchy import file type only.

Column Label	Description	Behaviour
Code	Organisation unit code. Used as the unique key to identify existing organisation units in Lighthouse on import.	Mandatory
Parent Code	Organisation unit code of the organisation unit directly above the organisation unit code in column 2. Allows a hierarchy of organisation units to be created.	Null allowed only for the highest organisation unit.
Name	Description of the organisation unit.	Mandatory
Legal Entity Code	Legal entity the organisation unit belongs to.	Optional Must be a valid legal entity code if not null.
Supervisor	Logon Id or Email Address of the organisation unit's supervisor.	Optional
Deactivated Date	Date the organisation was deactivated.	Optional Must be a valid date if not null.

Recommended Import Practices

The following recommendations are designed to keep the Lighthouse organisation structure and users as up to date as possible. The recommendations also assist with keeping the number of active users within an organisation's licensed users.

- Obtain regular extracts of the current active organisation structure and the current active users (staff members) from the Human resource system or other appropriate source.
- Ensure the organisation unit extract contains only the current organisation structure.
- Ensure the user extract contains all the current active staff members and does not contain staff who have left the organisation.
- Review the extracts to ensure they appear accurate.
- Resolve any errors reported when the extracts are selected for import. Do not continue with the import until all errors have been resolved.

- When importing, choose the following options

  Missing Organisation Units – Deactivate org unit
  Missing Users - Remove Can Login privilege and make user non Current Employee

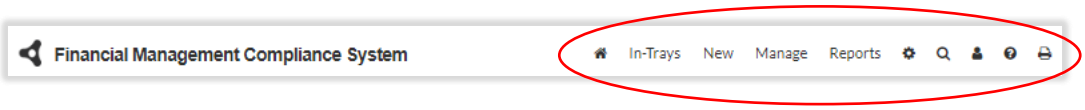
- If a test environment is available, perform the upload in the test and environment and ensure the results are as expected prior to performing the upload in the production environment.

MAINTAINING MENU STRUCTURE

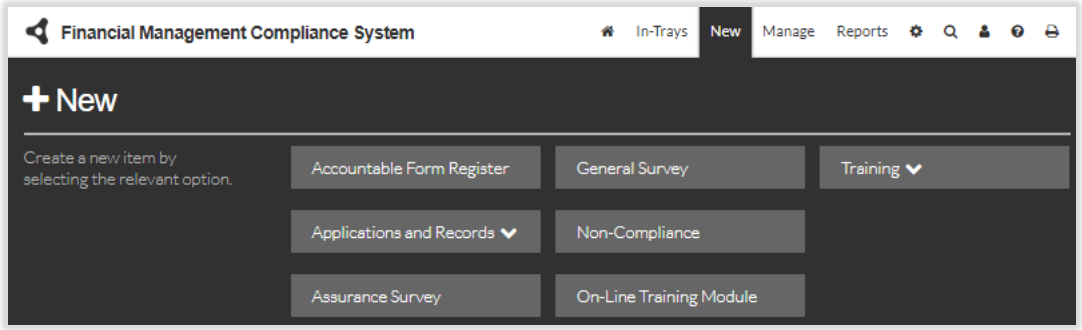
The menu structure for accessing all functions is configurable by the system administrator. This allows functions to be grouped within the menu system according to an organisation's specific requirements.

Up to four levels of menu items are available.

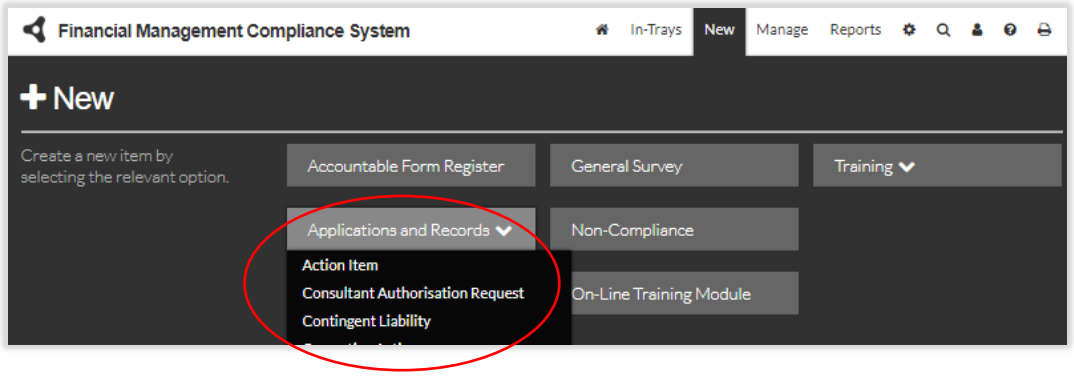
Level one appears on the mast head. E.g.



Level two appears as a sub menu under the selected level one menu. E.g.

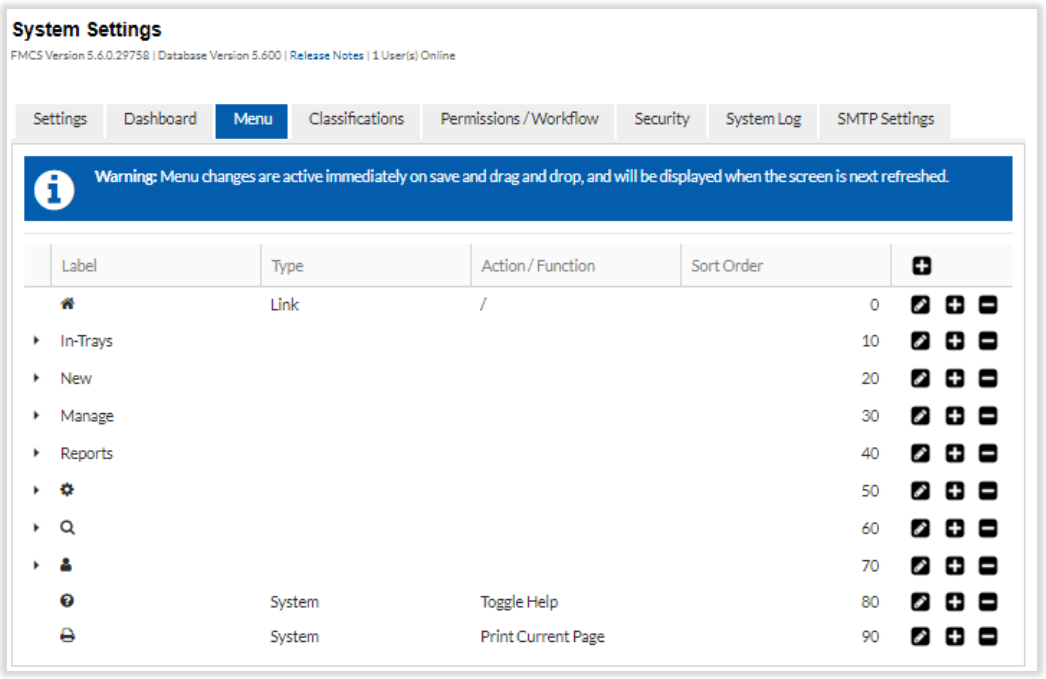


Levels three and four appear as a drop-down list under the selected level two menu. E.g.

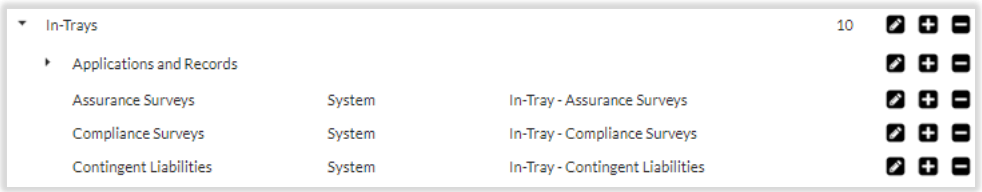


Maintain the menu structure by finding the System Settings menu item in the menu structure or type alt+M and find the function named "Search – Functions". Then select the Menu tab.

> Warning: Menu changes are active immediately on save, drag and drop and delete. Menu changes will be displayed when the screen is next refreshed. Menu changes cannot be undone.



Click on the arrow on the left to view the items below the selected menu item.



Adding Menu Items

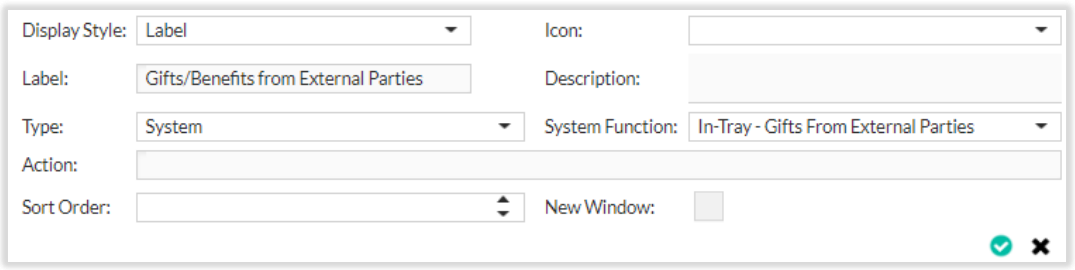
Click on any ⊕ button to add a new menu item. Menu items are always added below the item next to where the ⊕ was selected. To add a new level one menu item, select the ⊕ button in the list header section. Select the ✓ tick to accept the changes or the ✖ cross to cancel.

Editing Menu Items

Click on the ✎ button next to the menu item to be edited. Select the ✓ tick to accept the changes or the ✖ cross to cancel.

Menu Item Fields

When adding or editing menu items the following fields are available for configuration.



Display Style – Menu item can be displayed as a text label, an icon or both. If both is selected, the icon is displayed to the left of the label.

Icon – Used when the display style is Icon or Both. Select the required icon from the lookup list.

Label – Name of the menu item. Label is displayed in the menu structure if display style is Label or Both.

Description – Description of the function. Also used as a tool tip when mouse is hovered over the menu item.

Type – The type of function to be performed when the menu item is selected. Options are;

Link	Opens any link. Enter the link in the Action field.
Javascript	Allows javascript to be executed. Enter the javascript in the Action field.
System	Opens a predefined system function. Select the system function from the system function field.
None	No action is performed. This option is usually selected for higher level menu items that are used to group lower level menu items and do not perform any functions.

System Function – System function to be performed. Required when the System type is selected.

System function names have a prefix indicating the type of function as follows;

Account	Functions related to a user's account.
Administration	System administration functions
In-Tray	In-Tray functions.
Manage	Management functions. E.g. Groups, Reporting Permissions.
New	Functions to create new items.
Reporting	Functions for executing reports.

Search	Functions allowing searching for items.

The system function name follows the prefix. The system function name of on demand surveys/training and application types is the name of the survey/training or application type.

The following special function names are also used.

Print Current Page	Performs the page print function.
Toggle Help	Opens and closes context sensitive help.

Action – Action to be performed when the following types are selected;

Javascript	Must be a valid javascript statement.
Link	Any web link may be inserted. Links can be absolute or relative. Absolute links require the full url. Relative links act as if the link is prefixed by the url where Lighthouse is located.

Sort Order – Explicit order used when listing the menu item. Only applies to menu items within the same level. Menu items without a sort order are listed in alphabetic order.

New Window – Opens the function in a new window.

Moving Menu Items

Menu items can be moved between levels by using drag and drop. A dropped menu item will be placed under the menu item location where it was dropped. To move a menu item to the top level, drop the menu item on the list header. Note: drag and drop cannot be used to move a menu item within the same menu level.

Deleting Menu Items

Click on the ⛔ button next to the menu item to be deleted and then confirm the delete.

TEST MODE

Using Test Mode is recommended when testing in a test environment. When in test mode, Lighthouse behaves as follows;

- "***Test Mode***" is clearly displayed on the bottom of all screens.
- Password reset request emails will always be sent.
- All other emails generated by Lighthouse are only sent if the email recipient is a member of a specific group (usually named "Test Members"). Emails (except password reset requests) to any other user will not be sent. This prevents emails being inadvertently being sent to users not involved in performing testing.

Contact Torque Software to configure Test Mode.

IMPLEMENTATION GUIDE

This is guide provides the tasks required to implement Lighthouse when hosted on Torque Software's cloud hosting services.

All implementation tasks except Grant System Administrator Permissions can be performed concurrently. Tasks should be started as soon as possible. The implementation tasks assume Lighthouse has been installed on the cloud hosting environment by Torque Software.

Initial System Administrator Logon

Torque Software will supply the initial client a system administrator Lighthouse Logon ID. Use the forgotten password process to set the initial password.

Note: Lighthouse will initially be configured for authentication by logon id and password until a single sign on authentication method (option 1 or 2 in the Authentication Method section) is implemented.

Whitelisting

Request IT support to perform the following;

- Whitelist the Lighthouse cloud URL. The URL will be provided by Torque Software
- Ensure web fonts are allowed for the Lighthouse cloud URL for all users
- Whitelist the Lighthouse email send address; notify@lighthouse.torque.software

Authentication Method

Select the authentication method used to access Lighthouse. There are three options available. Option 1 - Vanguard Federated Authentication is preferred.

If options 1 or 2 are selected, Torque Software will liaise with the client's IT team to implement the selected authentication method.

It is also possible to configure Lighthouse to allow either Option 1 or 2 and Option 3. This is not recommended but is sometimes useful when not all Lighthouse users have access to the client's network or during the initial stages of implementation.

Option 1 – VANguard Federated Authentication Service

VANguard is provided by the Department of Industry, Innovation and Science and is recommended for Federal Government agencies wishing to obtain authentication services for internet applications.

The VANguard Federated Authentication Service provides single sign on by allowing users logged on to their own Government agency's network to authenticate and then use web

applications such as Lighthouse. Authentication occurs seamlessly without additional credentials or software being required on the user's computer.

Note: Most large Australian Federal Government entities already use VANguard and so configuration to include Lighthouse is usually minimal. However, if the client organisation is not already a VANguard user, then arrangements with the Department of Industry, Innovation and Science must be made to use VANguard in the client environment.

Option 2 – Torque Software's Propriety Single Sign On

Torque Software provides a small .NET authenticator application (or source code if building in SharePoint or similar is preferred) which runs on the client's internal IIS server or SharePoint server. Note: the server must be on the client's Active Directory domain so the application can transparently identify the user.

Option 3 – Logon ID and Password

User's login via a Logon ID (usually their client network Logon ID) and a password. It should be noted the password will not necessarily be the same as the client network password.

The default password complexity requirements are as follows;

- Minimum 12 characters in length
- Includes at least one numeral
- Includes at least one upper and one lower case character
- Includes at least one extended character: !@#$%^&*?_~-()

The default password complexity requirements may be changed in Lighthouse's System Settings - Security.

Populate Users & Organisation Structure

It is important the users and organisation structure in Lighthouse are accurate and kept up to date. Clients with only a small number of users may choose to manually maintain users and organisation structure. However, most clients should arrange to automate this process by following the steps below. Assistance from the client HR and/or IT teams will most likely be required.

- Arrange an automatic, regular HR download (preferably nightly) of all current staff from the client HR system. The download should also include contractors if possible. See the Import File Specification section for the available formats. Note: Combined format is recommended.

- The following information is optional in the import file;

  Organisation Unit Supervisors
  User Classification
  User AGS

  It is recommended all optional information be included if possible.

- Arrange for the HR download file to be automatically sent by SFTP to the cloud hosting environment. Torque Software will provide your IT team the required details.

Note: The HR download from the HR system and/or the upload into Lighthouse may be performed manually until the process is automated.

Classifications

If the HR download file will also include user's classifications, then the classifications must be populated in Lighthouse as they are used to validate the classification in the HR download file when importing. See the Configuring Classifications section.

Configure System Settings

Torque Software will provide a default configuration for system settings which will likely meet most client requirements. However, system settings should be reviewed and modified if required. See section Global System Settings.

The following settings are optional; however, it is recommended they be implemented.

From mask

This value displays as the from value in emails sent by Lighthouse. It is recommended this be set as the System Administrator's group email address.

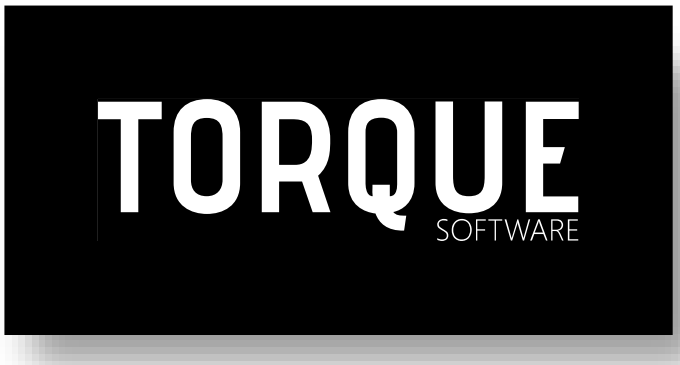
BCC email address

A copy of all email notifications generated by Lighthouse will be sent to the BCC email address. This is useful for analysing notifications sent by Lighthouse.

Grant System Administrator Permissions

Ensure all users who will be acting as system administrators are granted permission by making them members of the System Administrators group. See section User Groups.

Note: System administrators must be valid users in Lighthouse prior to granting permission.



Phone: 1300 795 581
www.torquesoftware.com.au.

© Torque Software, All Rights Reserved.