Investigations Case Management
- Admin Guide

VERSION 6.1.1

CONTENTS

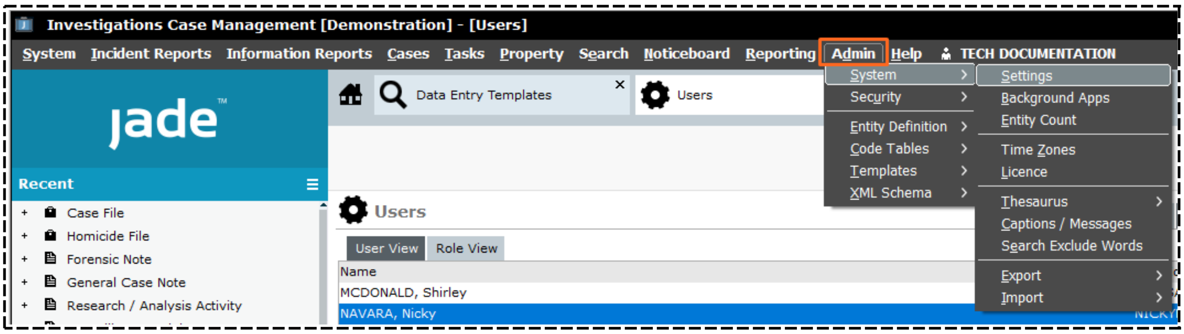
Overview

This Admin Guide explains how to set up Jade Investigations Case Management (ICM).

This person in your organisation who does this will need some training on how to use the software.

The admin user in your organisation should also be familiar with:

- Operational concepts of PCs that are compatible with ICM
- Microsoft Word



Security

Security in ICM is complex but flexible:

- You can view, record, and report on intelligence gathered from different sources and in a range of contexts.
- You can also protect and separate this data to meet legal and policy requirements.

ICM uses roles and permissions to control access to features. This means you can control what users can do – For example who can create cases.

All changes to data are audited. For example, you can see when data was changed, who changed it, and the old and new values.

When a user deletes information, they can't see it any more but it's still in the database. All deleted records are still in the database if you want to look at them.

Roles and permissions aren't used to assign access to individual cases, incident reports, information reports, and their associated entities. Instead, you can use the **Access** tab of individual entities and source entities to specify who can access them.

*See **Security Access** in the user guide.*

A team is a group of users who need the same level of access to information. For example, you might have an *Admin* team.

Consider Your Security Requirements

You can set up ICM to meet your needs and cater for your current and future business processes. Before you do this, you need to think carefully about your security requirements:

- What are the reporting structures in your organisation?
- What do you need to report?
- What are the current business processes for your organisation?
- Will the reporting and business processes in your organisation change?

Planning your security needs in ICM during the implementation process is important. Make sure you spend enough time on this so ICM works well for you.

Passwords

Administrators set up passwords for users. They specify:

- How long passwords and user IDs need to be.
- When passwords expire.
- Whether passwords must contain numbers.
- How many times a user can try to log on before they're locked out of ICM.

To set up password and logon rules for your organisation, select **Admin** > **System** > **Settings**.

Only administrators with the appropriate security can unlock a user who is locked out of ICM.

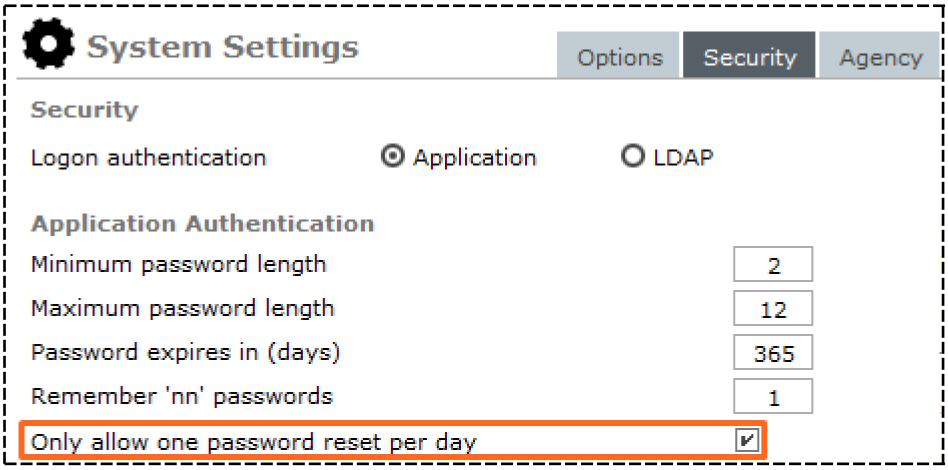
*Log on and log off attempts are audited. See **Logon History** in the user guide.*

If an administrator gives a user a new password, the user will need to change their password the next time they log in to ICM.

Restrict Password Reset to Once a Day

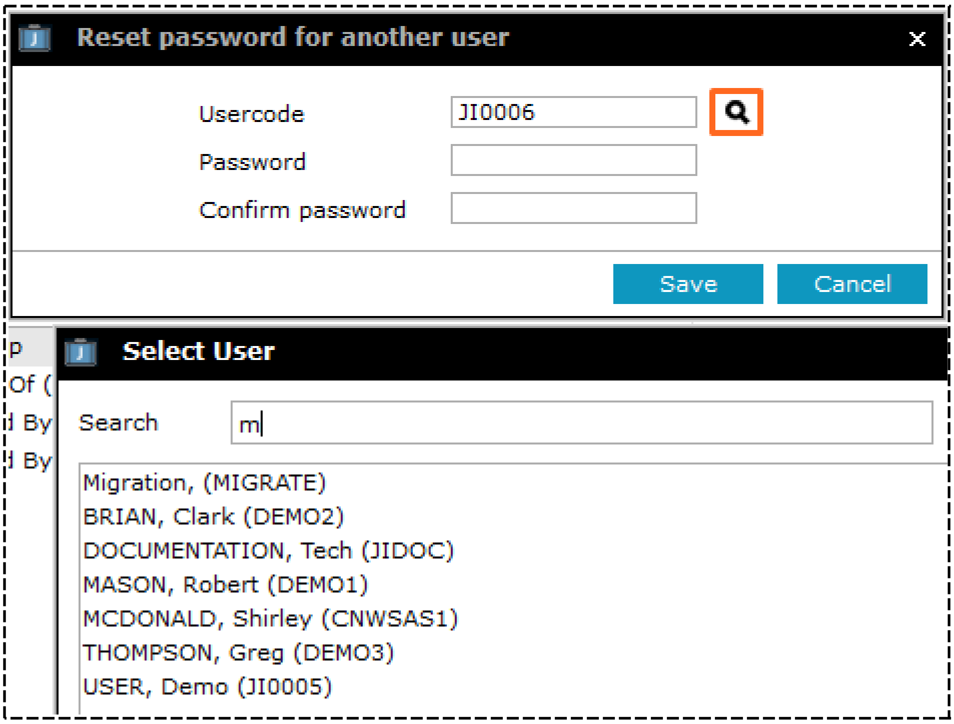
1. Select **Admin** > **System** > **Settings**.
2. Select the **Security** tab.
3. Select the **Only allow one password reset per day** checkbox.

   If an administrator changes a user's password after they change it on the same day, the user can change it again that day.



Change Another User's Password

1. Select **Admin** > **Security** > **Change Another User's Password**.
2. Enter your password in the field provided > Select **OK**.
3. Select the Search icon beside the **Usercode** field.
4. Enter the first few letters of the user's name in the **Search** field > Select the user > Select **OK**.



Security Alerts

Security alerts make it harder for users to act dishonestly.

A security alert is automatically generated when someone	**What happens next**
Resends a password	The *Password Reset* security alert prevents an administrator from resetting another user's password and using their account without their knowledge. When that user tries to log on, they incorrectly assume they've mistyped the password and ask for it to be reset.
Changes the Case officer for a case	The *Case Officer Change* security alert prevents an administrator from changing the case officer of a case to themselves, looking at the case, and then changing the case officer back to the original case officer. Although the audit log records this activity, it's not discovered until there's a reason to look at it.
Changes the security for a case	The *Case Security Change* security alert prevents an administrator changing the access list of a case to include themselves, looking at the case, and then changing the access list back to the original. Although the audit log records this activity, it isn't discovered until there's a reason to look at it.

These alerts show in the *Alerts* section of the Navigator.

Roles

You can use a role to group permissions based on the type of work a user does. For example, you can have a *case officer* role and a *team member* role.

Each role has a different set of permissions that grants or denies access to different areas of ICM.

The permission of a role determines what a user can see and do.

A role:

- is owned by an agency
- is managed by authorized users in that agency
- can contain zero, one, or many permissions

There's no limit to the number of roles you can create.

A user can have zero, one, or many roles.

To manage roles, you need the *Can Maintain Roles* permission.

Roles are managed and owned by the agency of the agency administrator that created the role. Other agency administrators can't see these.

Create a Role

1. Select **Admin** > **Security** > **Roles**.
2. Select **New**.
3. Enter a description for the role in the field provided.
4. To deactivate the role, select the **Deactivated** checkbox.

   You can't assign deactivated roles to users, but you can report on deactivated roles.
5. Select the role you want to base this role on in the **Super Role** drop-down.

   If you select a super role, the (subordinate) role you're defining can have only a subset of the permissions of the super role.

   You can create and save a role that has no permissions and add permissions to it
6. Specify permissions for the role:
   a. Select the **Permissions** tab.
   b. In the *Available* area, select the permission you want to assign to the role.

      Select the Expand + icon beside a header to show the permissions associated with that group.

      If you selected a role in the Super Role drop-down, the permissions the super role doesn't have are inactive and can't be selected.
   c. Use any of these methods to select permissions for the role:
      – Double-click a group header to expand the group > Use the Select icon to select permissions for that group, including child groups.
      – Double-click a permission.
      – Select a permission using the Select icon.
   d. To exclude a permission from the role:
      i. In the *Selected* area, select the permission you want to exclude.
      ii. Double-click the permission or click the Deselect icon.
7. Specify the designations that are associated with the role:
   a. Select the **Designations** tab at the bottom of the *Role Maintenance screen*.
   b. In the *Available* area, select the designation you want to assign to the role > Double-click the designation or click the Deselect icon.
8. Specify the teams associated with the role:
   a. Select the **Teams** tab at the bottom of the *Roles* screen.
   b. In the *Available* area, select the team you want to assign to the role.

      Double-click the team or click the Select icon.
   c. To exclude a team from the role:

   i. In the *Selected* area, select the team you want to exclude.

   ii. Double-click the team or select the .

9. Specify the users associated with the role:

   a. Select the **Users** tab at the bottom of the *Roles* screen.

   b. In the *Available* area, select the user you want to assign to the role.

   c. Double-click the user or click the Select icon.

   d. To exclude a user from the role:

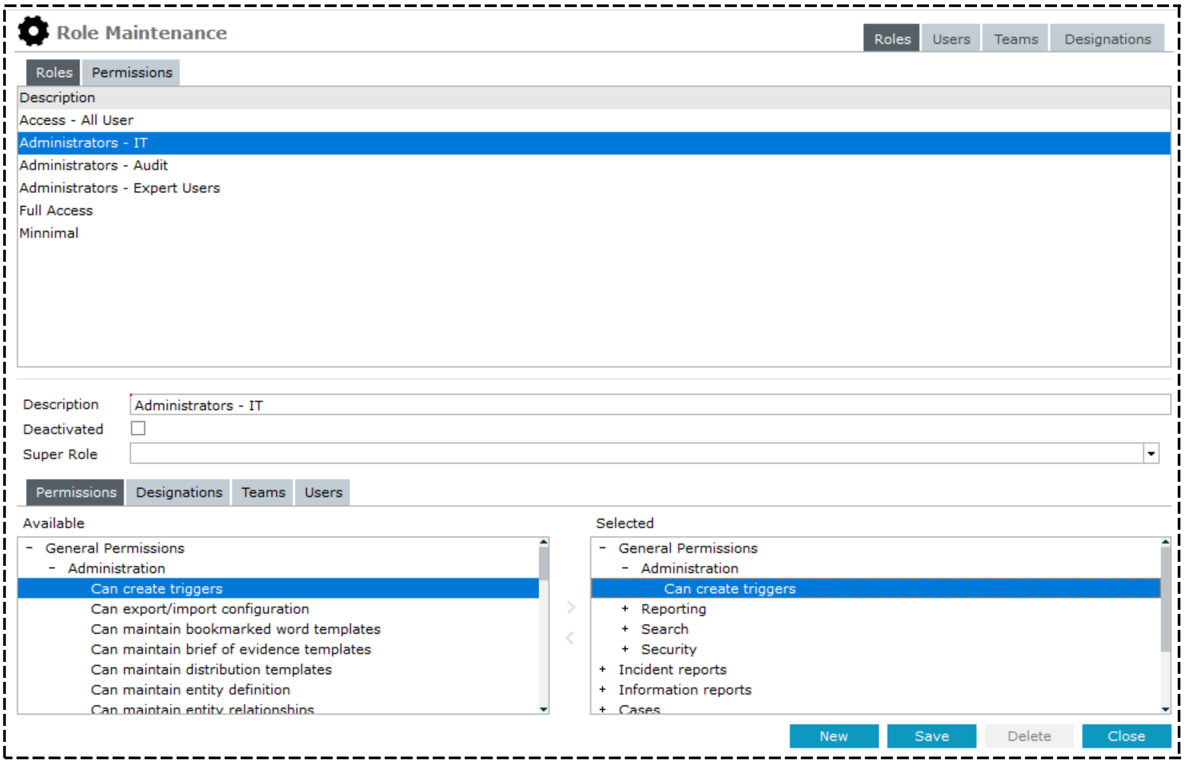
      i. In the *Selected* area, select the user you want to exclude.

      ii. Double-click the user.

10. Select **Save**.

Edit a Role

1. Select **Admin** > **Security** > **Roles**.
2. Select the role you want to edit.
3. Make your changes.
4. Select **Save**.



See the Permissions for a Role

The Permissions View of the Roles screen allows you to view the permissions that are associated with a role.

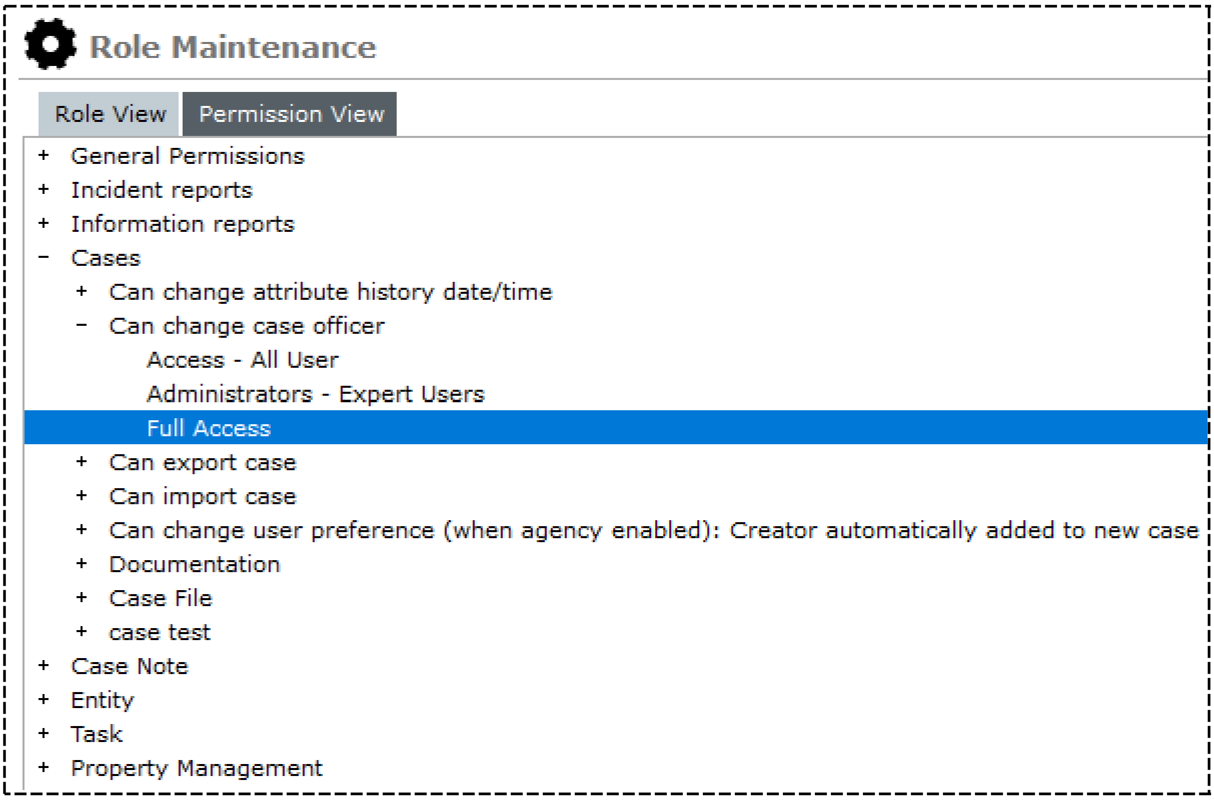
To view the users who are associated with a role, use the Role View of the Users screen on the Users screen.

See *Users Associated With a Role*.

To see the permissions associated with a role:

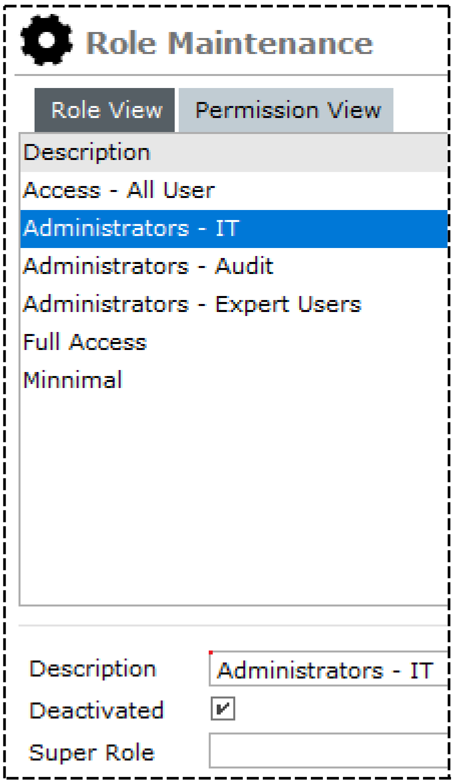
1. Select **Admin** > **Security** > **Roles**.
2. Make sure the **Roles** tab is selected.
3. To see permissions, select the **Permission View** tab.
4. To see the individual permissions of a category or subcategory, select the Expand + icon .
5. To see the roles of a permission, expand that permission.

The information in the Permission View is read-only. To *edit the permissions* of a role, use the **Role View** tab.



Deactivate a Role

1. Select **Admin** > **Security** > **Roles**.
2. Select the role you want to deactivate in the *Description* area.
3. Select the **Deactivated** checkbox.
4. Select **Save**.



Case Roles

Case roles are different to regular roles. They have these characteristics:

- You can use a case role to specify the access rights and permissions available to any user who has a particular role in a case.

  *For example, you might want to allow any user with a photographer role to have **read** access to general case notes, and **edit** access to scene examination case notes.*

- Case roles are like teams but they're specific to cases. Teams are system-wide and available to all cases in a business region or unit.

- Case roles only apply to case types. You can use them to specify access to any case notes and tasks that are part of the case.

  Case roles don't apply to Incident or Information Reports or any other source entity.

- Case roles are specific to individual cases.

  For example, if cases A and B have a photographer case role, an assigned user who has this role in case A doesn't automatically get access to anything in Case B.

- You can set up system-wide default case roles and the access rights associated with those roles. Use the Case Role system code table and the case entity types for this.

- Only an admin user can set up system-wide case roles.

  *Any user with the **Can add security access** permission can set up ad hoc case roles.*

- One or more users can be assigned to any case role in a specific case.

Teams

You can use a team to group users who need the same level of access to information.

You can use a team for a:

- Work group – For example, Investigation Team 1
- Group of users who need the same level of access to information – For example, senior officers

You can create as many teams as your agency needs.

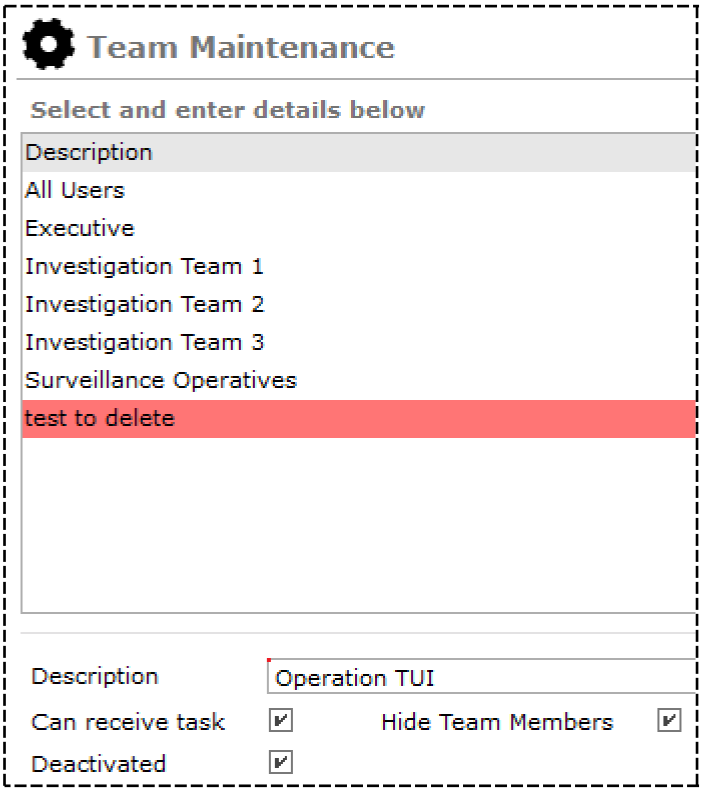
A user doesn't need to belong to a team. They can belong to more than one team.

*To manage teams, you need the **Can Maintain Teams** permission.*

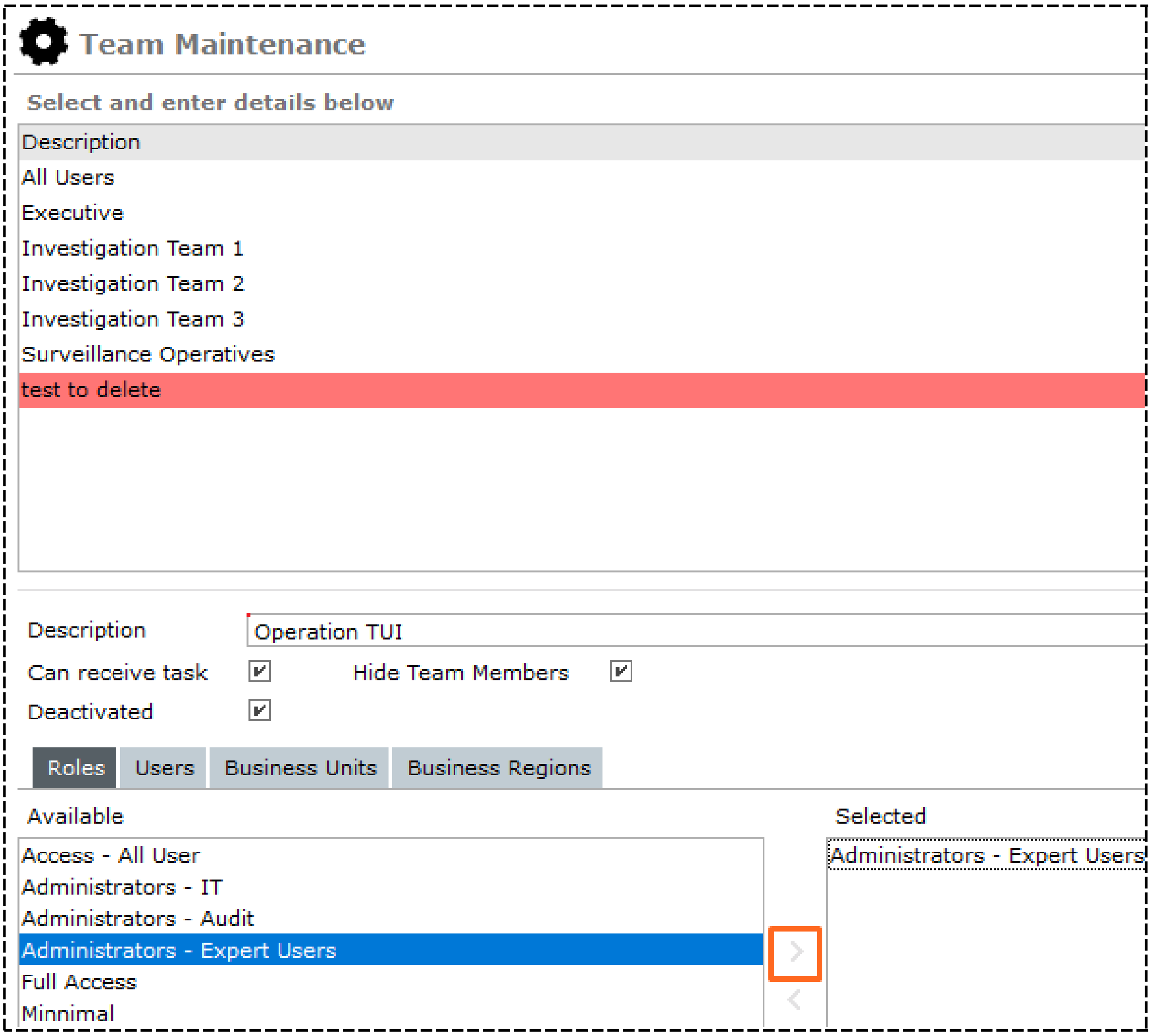
Create a Team

1. Select **Admin** > **Security** > **Teams**.
2. Select **New**.
3. Enter a description for the team in the field provided.
4. To let the team receive tasks, select the **Can Receive Task** checkbox.
5. To keep the members of a team anonymous, select the **Hide Team Members** checkbox.

   For example, you might have a covert operations team.
6. If the team isn't active yet, select the **Deactivated** checkbox.



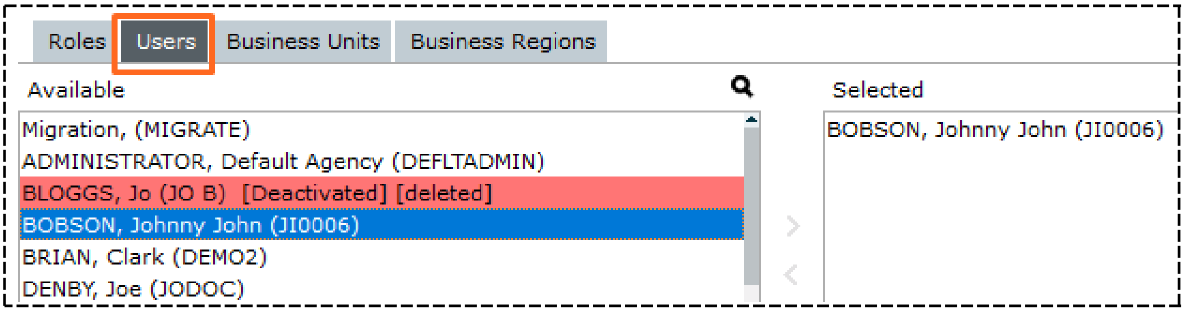
   You can't assign users to deactivated teams but you can report on deactivated teams.
7. To add roles to the team:
   a. Select the **Roles** tab.
   b. Double-click the role you want to assign to the team or use the Select icon.



8. To specify users who belong to the team:

   a. Select the **Users** tab.

   b. Double-click the user or use the Select icon to select the user.



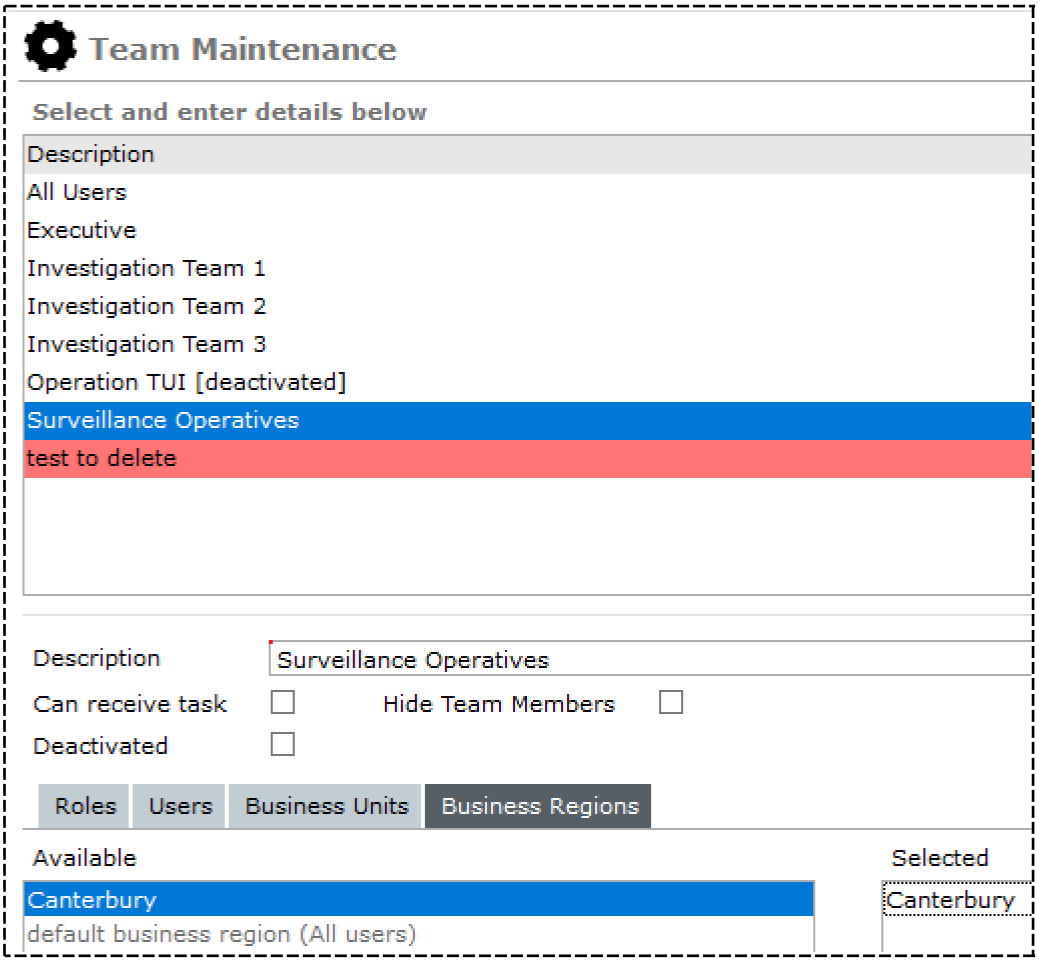
9. To specify the team's business unit, select the **Business Units** tab.

10. To specify the team's business region, select the **Business Regions** tab.

11. Select **Save**.

Edit a Team

1. Select **Admin** > **Security** > **Teams**.
2. Select the team you want to edit.
3. Make your changes.
4. Select **Save**.



Delete a Team

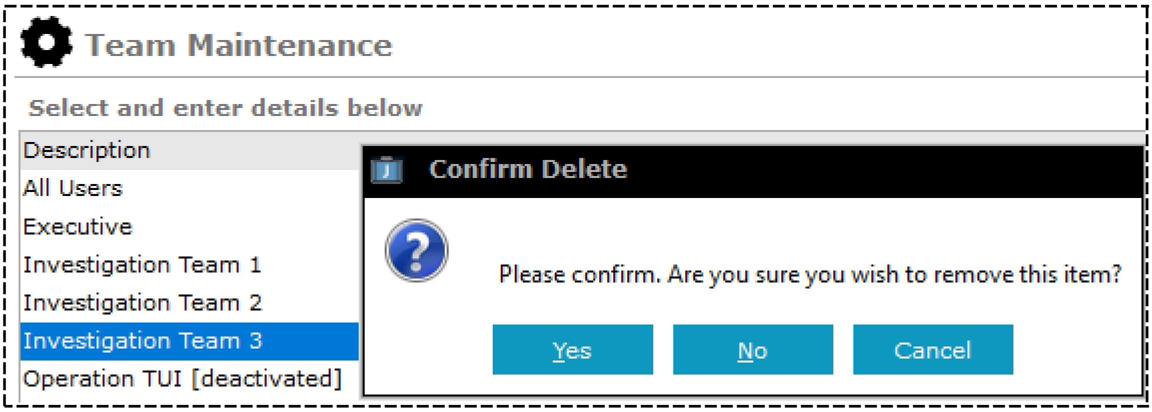
You can use either of these methods to remove a team:

- Deactivate the team – Select the **Deactivated** checkbox on the Team Maintenance screen.
- Delete the team.

To delete a team:

1. Select **Admin** > **Security** > **Teams**.
2. Select the team you want to delete.
3. Select **Delete**.
4. Select **Yes** to confirm you want to delete the selected team.

   Users in the team aren't deleted.



Designations

A designation allows you to logically group permissions based on a user's designation or title within an organisation. A designation can represent one user or a group of users.

You can create as many designations as your agency needs. A user can belong to zero, one, or many designations.

A designation:

- Is owned by an agency.
- Is managed by an agency administrator or authorized user. Designations are managed and owned by the agency of the agency administrator who created it. They can't be seen by other agency administrators.
- Can contain zero, one, or more users.

*To manage designations, you need the **Can Maintain Designations** permission.*

Create a Designation

You can specify that a user is designated to shadow another staff member or to be shadowed by another staff member. This will give the person with shadow designation the same privileges as the person being shadowed. This means the tasks assigned to a staff member can be taken over by another staff member if there's an emergency.

To specify a designation and then assign it to a user:

1. Select **Admin** > **Security** > **Designations**.
2. Select **New**.
3. In the *Description* field, enter a description for the designation.
4. To specify that the designation can receive a task, select the **Can Receive Task** checkbox.
5. *If you don't select this checkbox, the designation isn't available for selection when the recipients of a task are specified on the Task screen.*
6. To deactivate the designation, select the **Deactivated** checkbox.

   You can't assign deactivated designations but you can report on them.
7. To specify roles for the designation:
   a. Select the **Roles** tab at the bottom of the *Designation Maintenance* screen.
   b. In the *Available* area, select the role you want to associate with the designation.
   c. Double-click the role or click the Select icon.
   d. To exclude a role from the designation, select the role you want to exclude in the *Selected* area.
8. To specify users who belong to the designation:
   a. Select the **Users** tab at the bottom of the *Designation Maintenance* screen.
   b. In the *Available* area, select the user you want to assign to the designation.
   c. Double-click the user or click the Select icon.
   d. If you selected the **Can Receive Task** checkbox, you can exclude individual designations from the recipient list of a task on the *Task* screen.

      To enable a designation to receive a task, select the Expand + icon at the beside the designation.
   e. To exclude a user from the designation, select the user you want to exclude in the *Selected* area.
9. To update or set up shadow designation:
   a. Select the **Shadows** tab.

      *The **Is Shadowed by** field shows the designation of the user doing the shadowing.*
   b. The **Is Shadowing with** area shows the designations that the user will be shadowing.

c. To specify a new designation for shadowing:

   i. Select the Search icon beside the **Is Shadowed by** field.

   ii. Select a designation to be shadowed > Select **OK**.

   iii. To save your changes, select **Save** on the *Designation Maintenance* screen.

10. To associate business units with which the designation:

    a. Select the **Business Units** tab at the bottom of the *Designation Maintenance* screen.

    b. In the *Available* area, select the business unit you want to assign to the designation.

    c. Double-click the business unit or click the Select icon.

    d. To exclude a business unit from the designation, in the *Selected* area, select the business unit who you want to exclude.

11. To associate a business region with which the designation:

    a. Select the **Business Regions** tab at the bottom of the *Designation Maintenance* screen.

    b. In the *Available* area, select the business region you want to assign to the designation.

    c. Double-click the business region or click the Select icon.

    d. To exclude a business region from the designation, select the business region who you want to exclude in the *Selected* area.

12. Select **Save**.

Edit a Designation

1. Select **Admin** > **Security** > **Designations**.
2. Select the designation you want to edit.
3. Edit the required details in the tabs in the lower half of the screen.
4. Save your changes.

Delete a Designation

Use either of these methods to remove a designation:

- Deactivate the designation by selecting the **Deactivated** checkbox on the *Designation Maintenance* screen.
- Delete the designation.

To delete a designation:

1. Select **Admin** > **Security** > **Designations**.
2. Select the designation you want to delete.
3. Select **Delete**.

Business Units

You can set up security values based on the business unit a user belongs to.

Create a Business Unit

1. Select **Admin** > **Security** > **Business Units**.
2. Select **New**.
3. In the *Description* field, enter the name of the business unit you want to create.

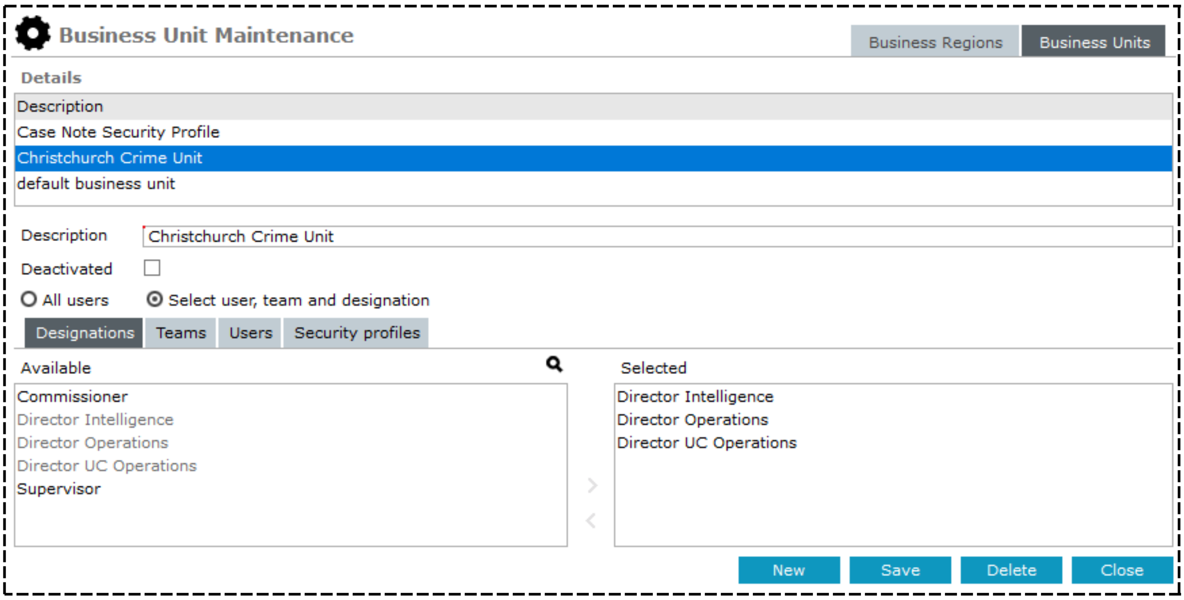
   For example, Legal Services.
4. To deactivate the business unit, select the **Deactivated** checkbox.

   Select this checkbox if the unit isn't active yet.

   You can't assign a user to a deactivated business unit.
5. To associate all users with the business unit, select **All users**.
6. To select the designations you want to associate with the business unit:
   a. Select the **Select user, team and designation** option button.
   b. Select the **Designations** tab at the bottom of the *Business Unit Maintenance* screen.
   c. In the *Available* area, select the designation you want to associate with the user – Double-click the designation or select the Select icon.
7. To select the teams you want to associate with the business unit:
   a. Double-click the team or click the Deselect icon.
   b. Check the **Select user, team and designation** option button.
   c. Select the **Teams** tab at the bottom of the *Business Unit Maintenance* screen.
   d. In the *Available* area, select the team you want to associate with the business unit.
8. To specify users who belong to the business unit:
   a. Select the **Select user, team and designation** option button.
   b. Select the **Users** tab at the bottom of the *Business Unit Maintenance* screen.
   c. In the *Available* area, select the user you want to assign to the business unit.
9. To see the security profiles associated with a business unit, select the **Security Profiles** tab at the bottom of the *Business Unit Maintenance* screen.
10. Select **Save**.

Edit a Business Unit

1. Select **Admin** > **Security** > **Business Units**.
2. Select the business unit you want to edit.
3. Make your changes.
4. Select **Save**.



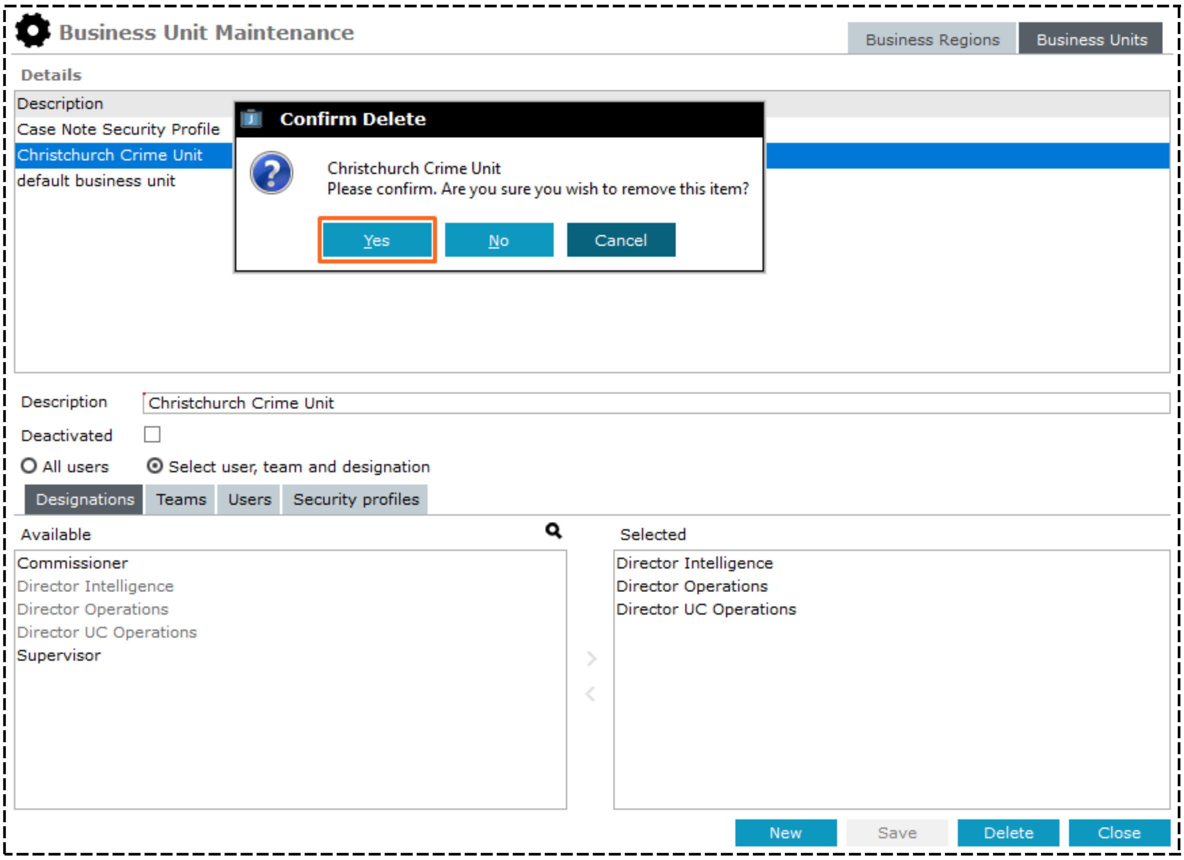
Delete a Business Unit

The following methods enable you to delete a business unit:

- Deactivate the business unit, by checking the Deactivated checkbox on the Business Unit Maintenance screen.
- Delete the business unit.

To delete a business unit:

1. Select **Admin** > **Security** > **Business Units**.
2. Select the business unit you want to delete.
3. Select **Delete**.
4. Select **Yes** to confirm you want to delete the business unit.



Business Regions

You can use business regions to set up security values based on the location or region a user is in.

Create a Business Region

1. Select **Admin** > **Security** > **Business Regions**.
2. Select **New**.
3. In the *Description* field, enter the name of the business region you want to create.

   *For example, **Otago**.*
4. To deactivate the business region, select the **Deactivated** checkbox.

   Select this checkbox if the region isn't yet active.

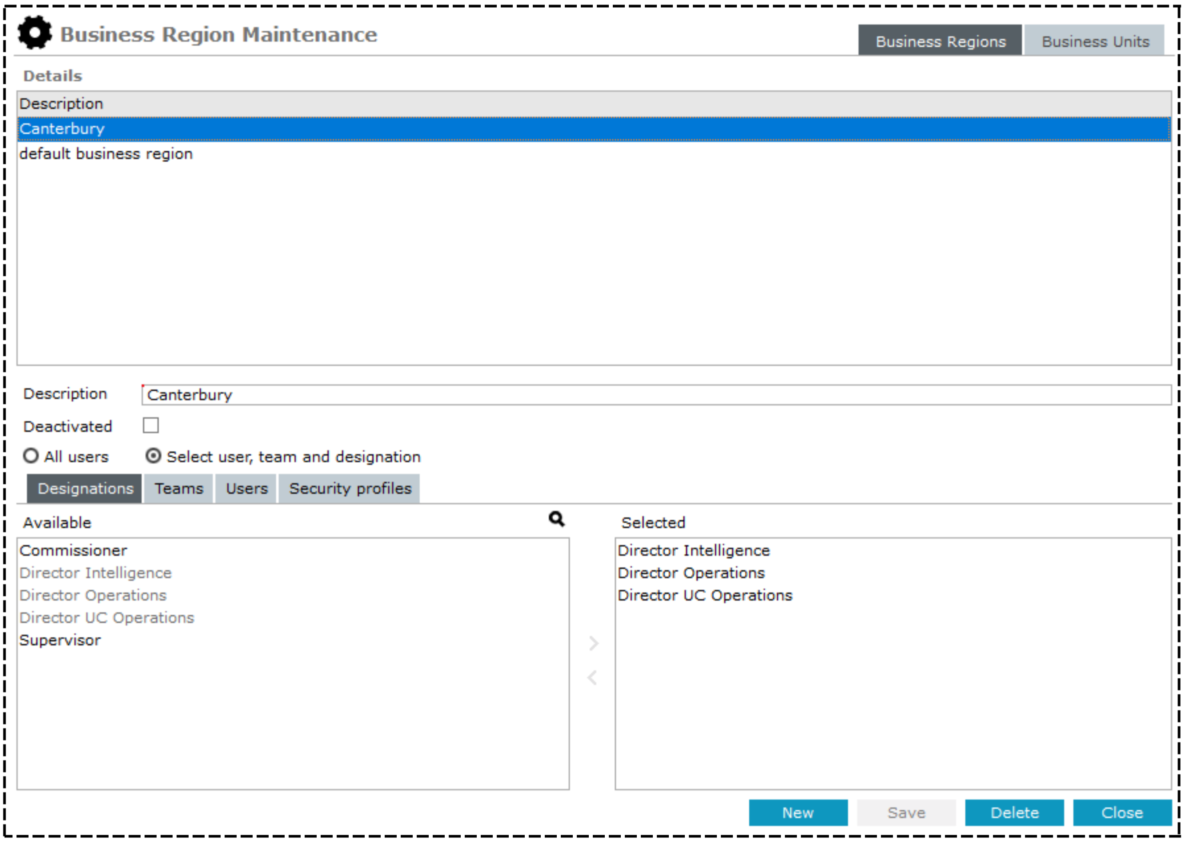
   You can't assign a user to a deactivated business region.
5. To associate all users with the business region, select **All users**.
6. To select the designations you want to associate with the business region:
   a. Select the **Select user, team and designation** option button.
   b. Select the **Designations** tab at the bottom of the *Business Region Maintenance* screen.
   c. In the *Available* area, select the designation you want to associate with the user.

      Double-click the designation or click the Select icon.
   d. To exclude a designation from the business region, select the designation you want to exclude in the **Selected** area > Double-click the designation or click the Select icon.
7. Select the teams you want to associate with the business region:
   a. Select the **Select user, team and designation option** button.
   b. Select the **Teams** tab at the bottom of the *Business Region Maintenance* screen.
   c. In the *Available* area, select the team you want to associate with the business region > Double-click the team or click the Select icon.

      The business region inherits the permissions associated with that team.
8. To specify users who belong to the business region:
   a. Select the **Select user, team and designation** option button.
   b. Select the **Users** tab at the bottom of the *Business Region Maintenance* screen.
   c. In the *Available* area, select the user you want to assign to the business region > Double-click the user or click the Select icon.
9. To see the security profiles associated with a business region, select the **Security Profiles** tab at the bottom of the *Business Region Maintenance* screen.
10. Select **Save**.

Edit a Business Region

1. Select **Admin** > **Security** > **Business Regions**.
2. Select the business region you want to edit.
3. Make your changes.
4. Save your changes.



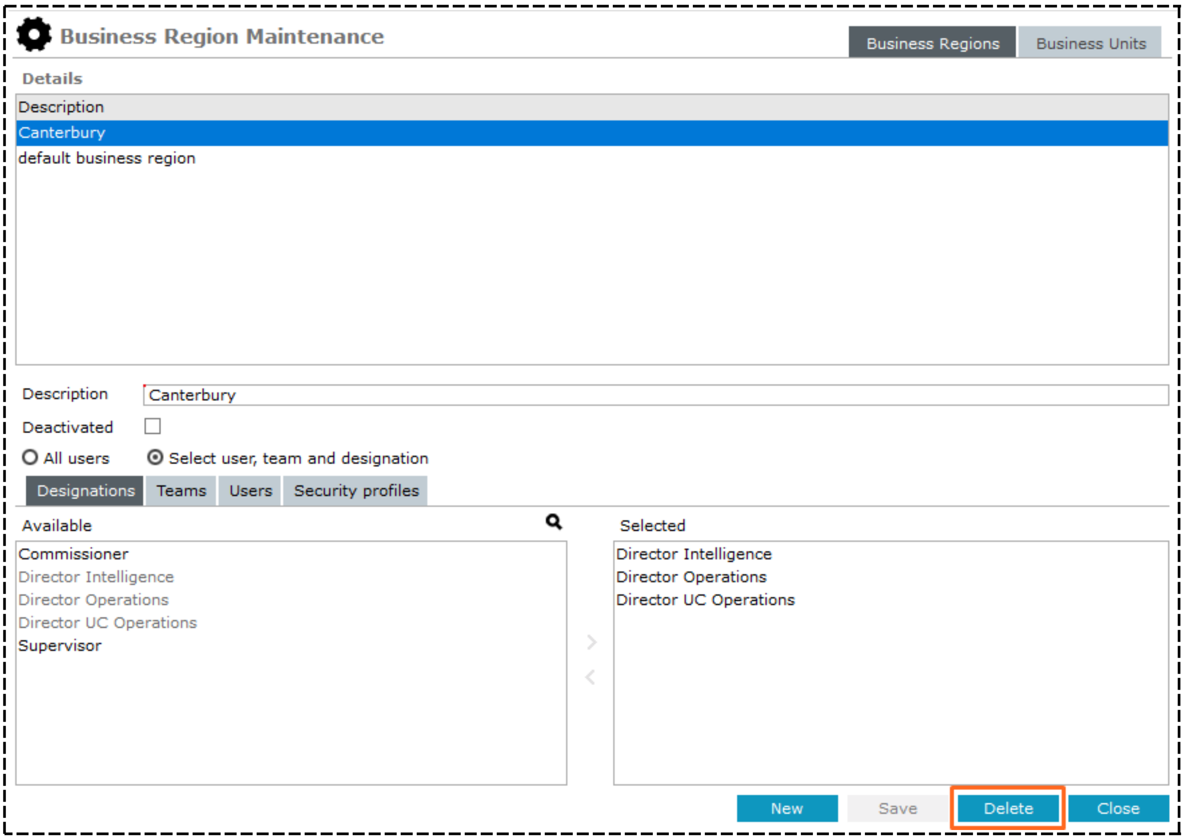
Delete a Business Region

Use either of these methods to delete a business region:

- Deactivate the business region – Select the **Deactivated** checkbox on the *Business Region Maintenance* screen.
- Delete the business region.

To delete a business region:

1. Select **Admin** > **Security** > **Business Regions**.
2. Select the business region you want to delete.
3. Select **Delete**.



Users

A user is a person who has a user identifier and a password.

The agency administrator in your business is responsible for creating a user identifier and an initial password for users.

Each user is owned by the agency that the administrator who created the user belongs to.

Users can't be seen or managed by other agency administrators.

To manage users, you need the ***Can Maintain Users*** *permission.*

Create a User

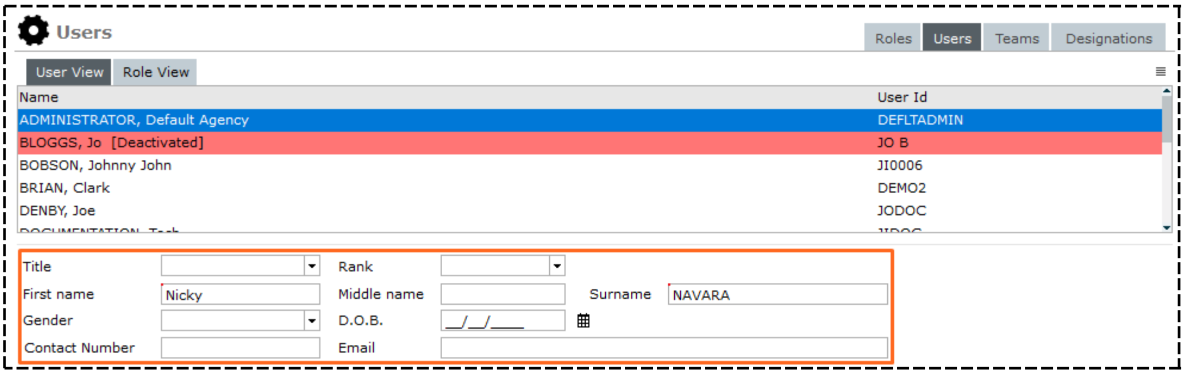
1. Specify a user's logon and personal data.
2. Specify a user's roles.
3. Specify a user's designations.
4. Specify a user's teams.
5. Specify a user's logon details and roles and teams.
6. Select access options for a user.
7. Select security access for a user.
8. Specify a user's business regions.
9. Add resource details for a user.

Specify a User's Logon and Personal Data

1. Select **Admin** > **Security** > **Users**.
2. Select **New**.
3. Enter the user's details first and last names in the fields provided.

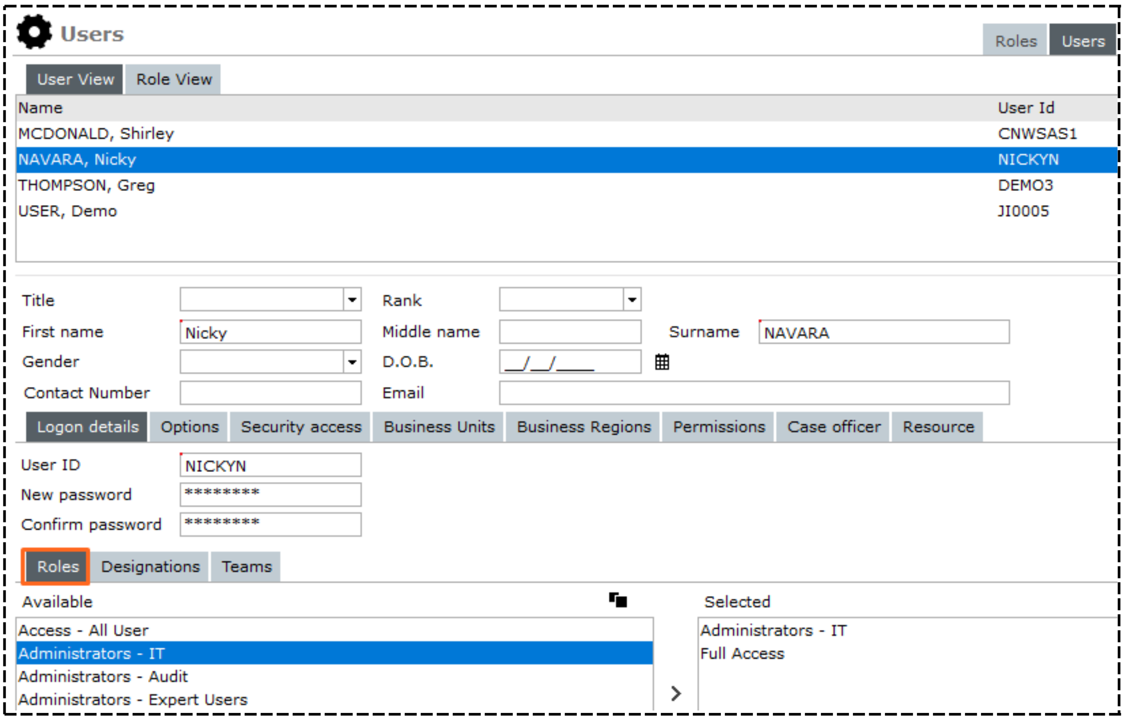
   You can't change a User's ID once someone has recorded a property item against their ID as the destination.

   *Select **Admin** > **System** > **Settings** to see the password and logon rules for your agency.*



Specify a User's Roles

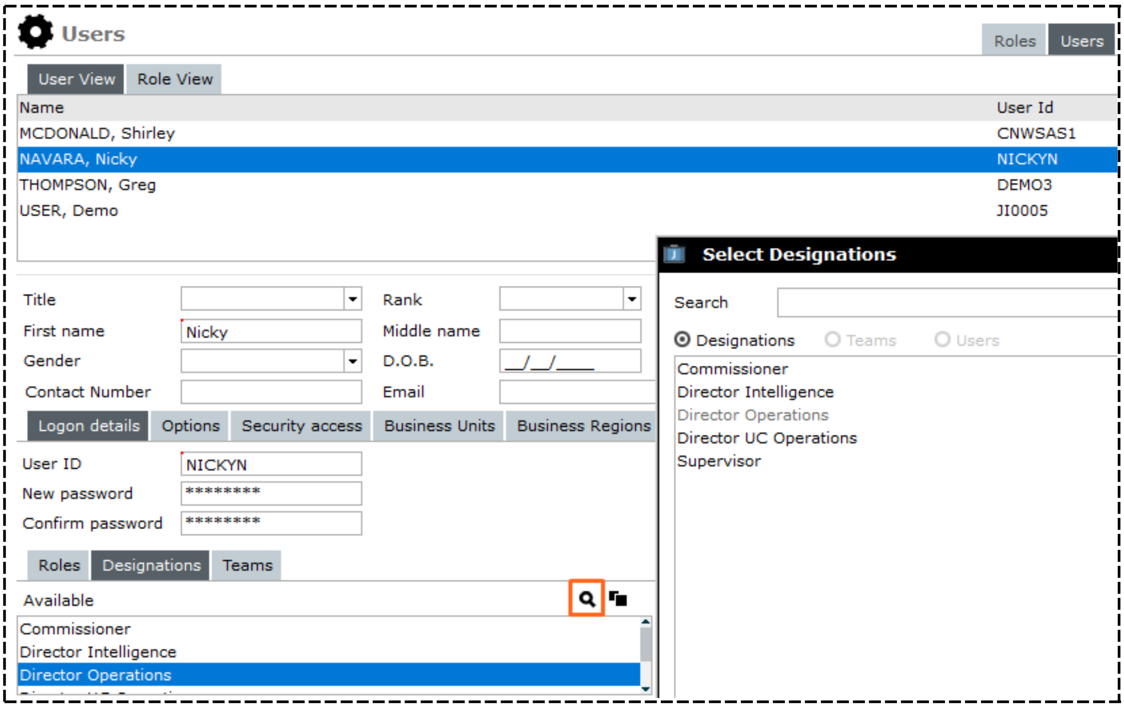
1. Select **Admin** > **Security** > **Users**.
2. Select the user.
3. Select roles for the user:
   a. Select the **Roles** tab.
   b. In the **Available** area, select the role you want to associate with the user.
   c. Double-click the role or click the Select icon.



Specify a User's Designations

1. Select **Admin** > **Security** > **Users**.
2. Select the user.
3. Select the user's designations:
   a. Select the **Designations** tab.
   b. In the **Available** area, select the designation you want to associate with the user.
   c. Double-click the designation or click the Select icon.

   If you have lots of designations, use the Search icon to find the ones you want.

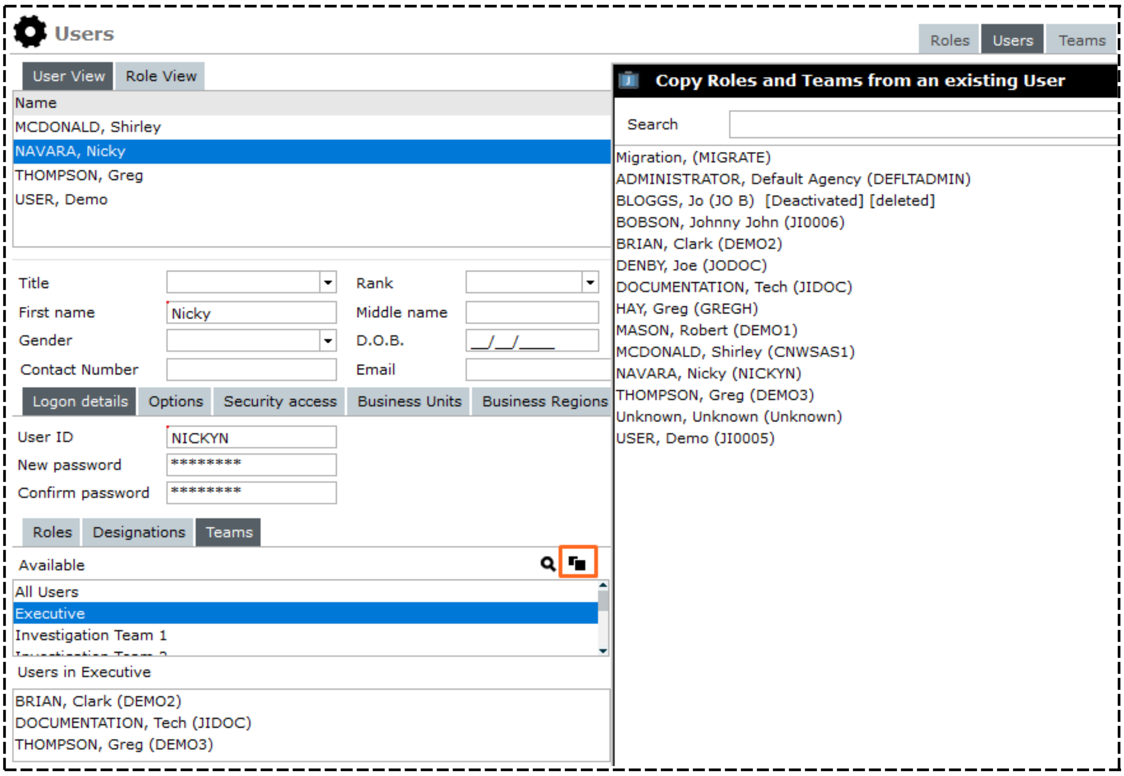


Specify a User's Teams

1. Select **Admin** > **Security** > **Users**.
2. Select the user.
3. Select the teams the user should be in:
    a. Select the **Teams** tab.
    b. In the **Available** area, select the team you want to associate with the user.
    c. Double-click the team or click the Select icon.

    If you have lots of teams, use the Search icon to find the ones you want.

    If you've set up roles and teams for another user, you can copy these for a user with the same roles and teams. To do this, select the copy icon.



Select System Options for a User

1. Select **Admin** > **Security** > **Users**.
2. Select the user.
3. To deactivate the user, select the **Deactivated** checkbox.

   A user will be deactivated automatically if they exceed the specified number of:

   - Failed logon attempts
   - Days without logging on

     If a deactivated user is currently logged into ICM, they won't be logged off as soon as you deactivate them. Once they log off, they won't be able to log on again.

4. To log a deactivated user out of ICM immediately, select the **Immediately logoff user** checkbox.

   *Once you select **Save**, the deactivated user will be logged out in five seconds. They will be notified of this.*

5. If the user has left your agency, select the **User left Organisation** checkbox.
6. To force the user to change their password the next time they next log on, select the **Force password entry at next logon** checkbox.
7. If you don't want the user to have to change their password, select the **Password never expires** checkbox.

   If you don't select this checkbox, the user will have to change their password after the specified period elapses.

8. To let a user to receive tasks, select the **Can receive task** ... checkbox.

   *This enables the **External task recipient** checkbox.*

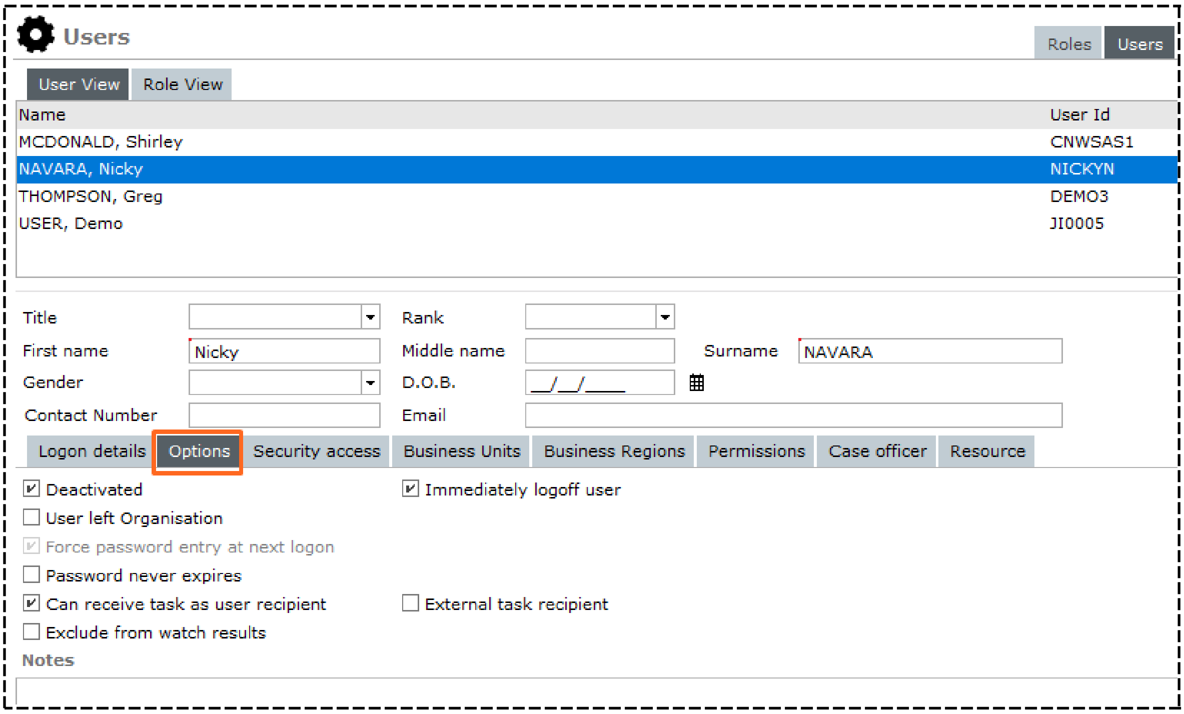
9. If the user has an email address outside your agency, select the **External task recipient** checkbox.
10. To let a user covertly access entities that are being watched, select the **Exclude from watch results** checkbox.

    If you select this checkbox, the user can access an entity that's being watched by another user. No alert containing this user’s details will be generated.

    You might want to use this checkbox for an internal investigation when a user operates undercover and you don't want staff to know about them.

11. Add a note in the **Notes** field.

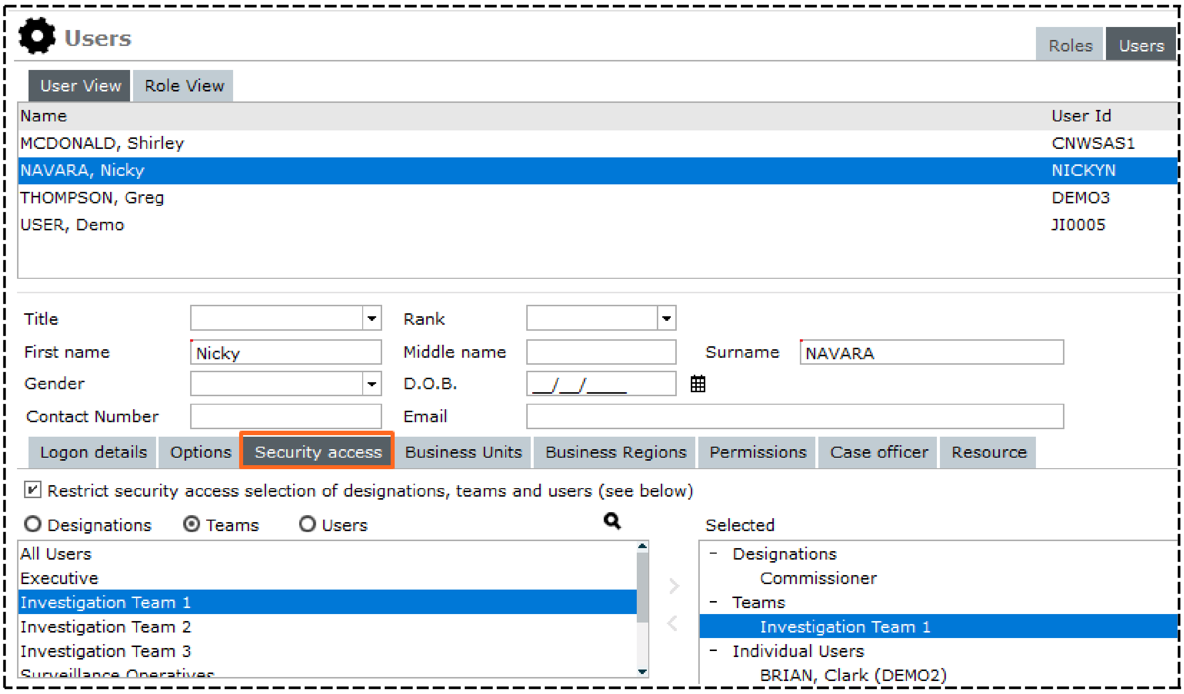
    For example, you could add instructional notes about deactivating a user.


Users
Roles
Users
User View
Role View
Name
User Id
MCDONALD, Shirley
CNWSAS1
NAVARA, Nicky
NICKYN
THOMPSON, Greg
DEMO3
USER, Demo
JI0005
Title
Rank
First name
Nicky
Middle name
Surname
NAVARA
Gender
D.O.B.
Contact Number
Email
Logon details
Options
Security access
Business Units
Business Regions
Permissions
Case officer
Resource
Deactivated
Immediately logoff user
User left Organisation
Force password entry at next logon
Password never expires
Can receive task as user recipient
External task recipient
Exclude from watch results
Notes

Select Security Access for a User

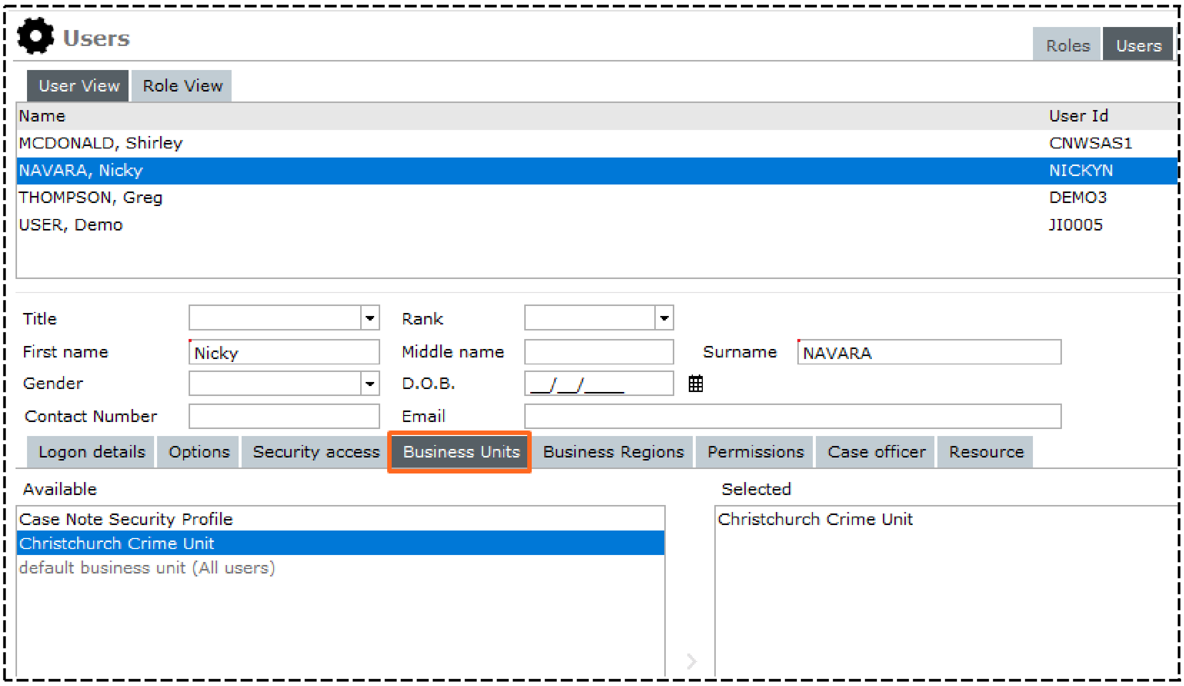
Security access controls how users can share cases and information reports inside and outside your own agency.

1. Select **Admin** > **Security** > **Users**.
2. Select the user.
3. Select the **Security Access** tab.
4. To prevent a user from sharing information outside your agency, select the **Restrict security access** ... checkbox.
5. Double-click the designations, teams, and users who should not be able to share information outside your agency.



Specify a User's Business Units

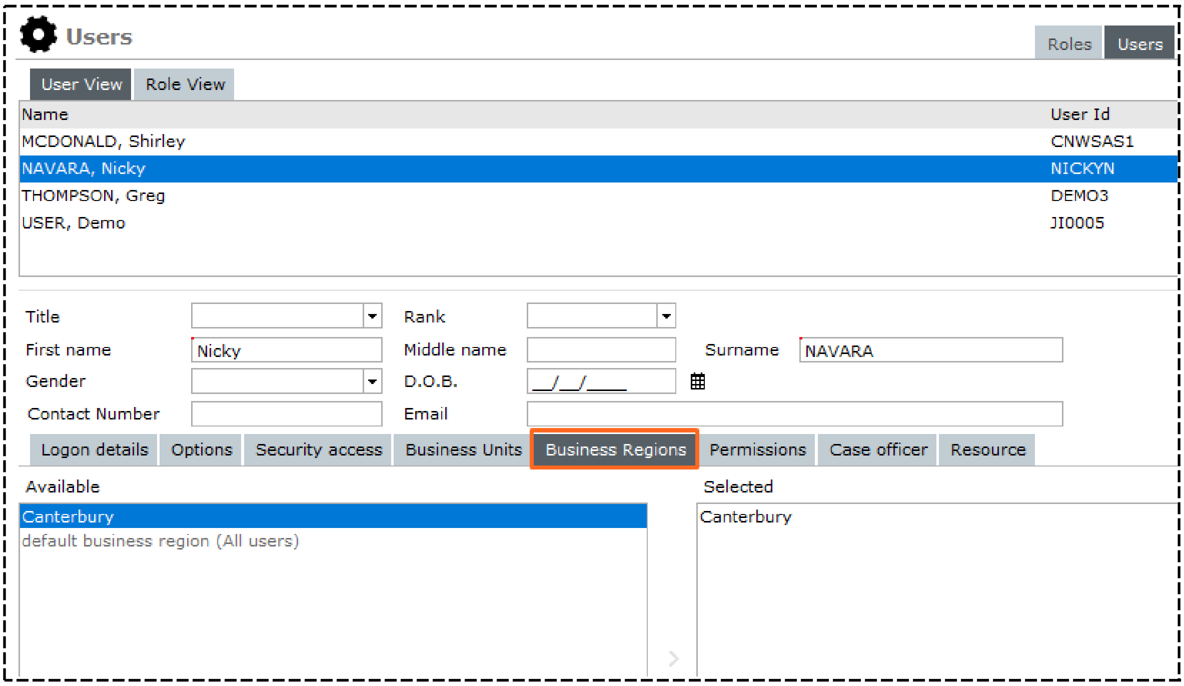
1. Select **Admin** > **Security** > **Users**.
2. Select the user.
3. Select the **Business Units** tab.
4. In the **Available** area, select the business unit you want to associate with the user.
5. Double-click the business unit or click the Select icon.



Specify a User's Business Regions

1. Select **Admin** > **Security** > **Users**.
2. Select the user you want to specify a business region for.
3. Select the **Business Regions** tab.
4. In the **Available** area, double-click the business region or use the Select icon select to associate it with the user.

   See <u>Business Regions</u>.



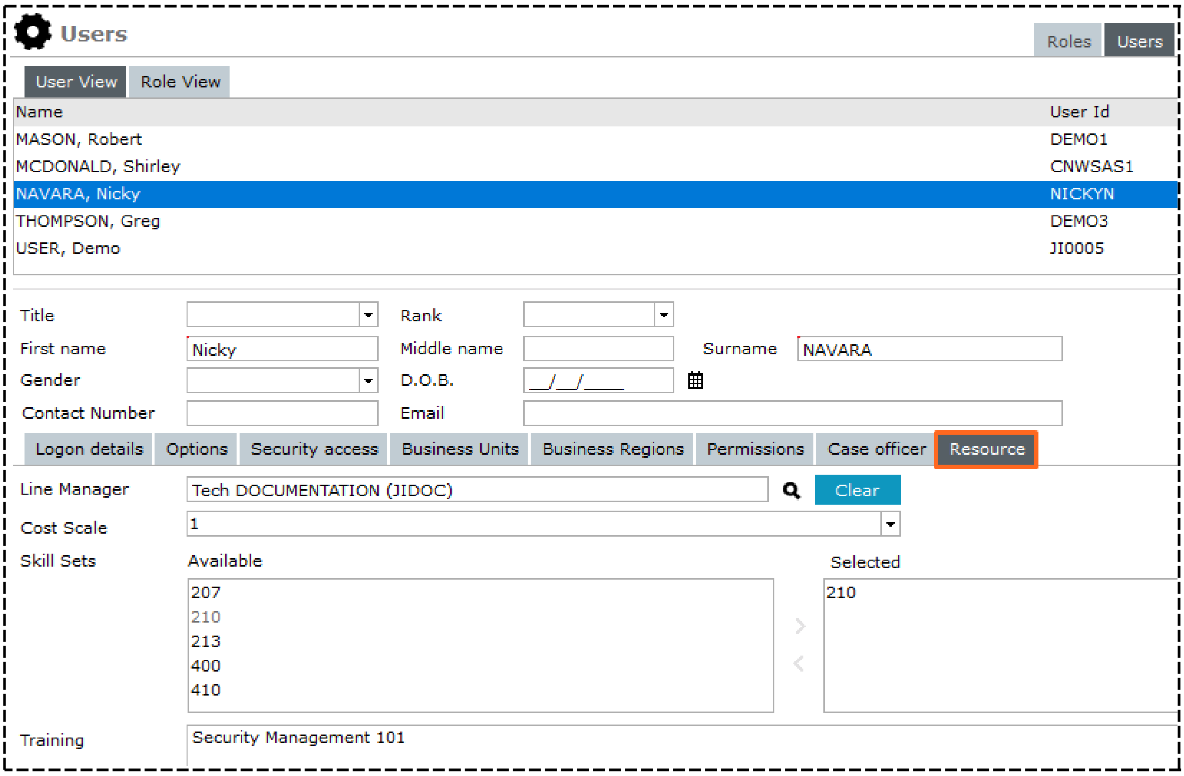
Specify Resource Details for a User

You can use this option to specify a user's resource details.

This applies if you've set up code tables to manage resources in your agency. You can set up your cost scale and skill set entries under **Admin** > **Code Tables** > **System**.

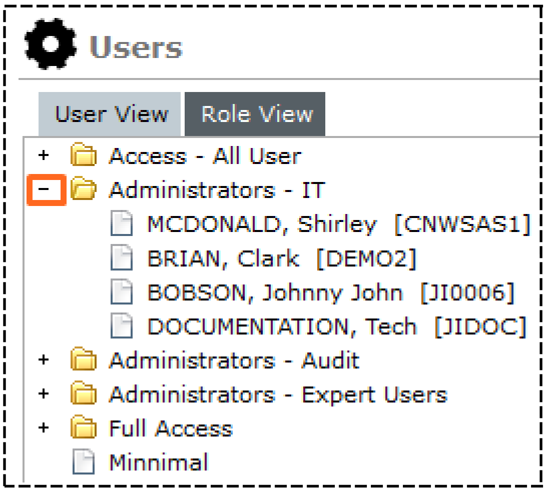
To access and manage resource information for the user:

1. Select **Admin** > **Security** > **Users**.
2. Select the new user.
3. Select the **Resource** tab.
4. Select the Search icon beside the **Line Manager** field > Select a user from the list.
5. Select the user's cost scale in the field provided.
6. Use select the user's skill sets from the Available list to the Selected list by double-clicking on entries.
7. Enter any notes you have about training the user has had in the Training field.
8. Save your changes.



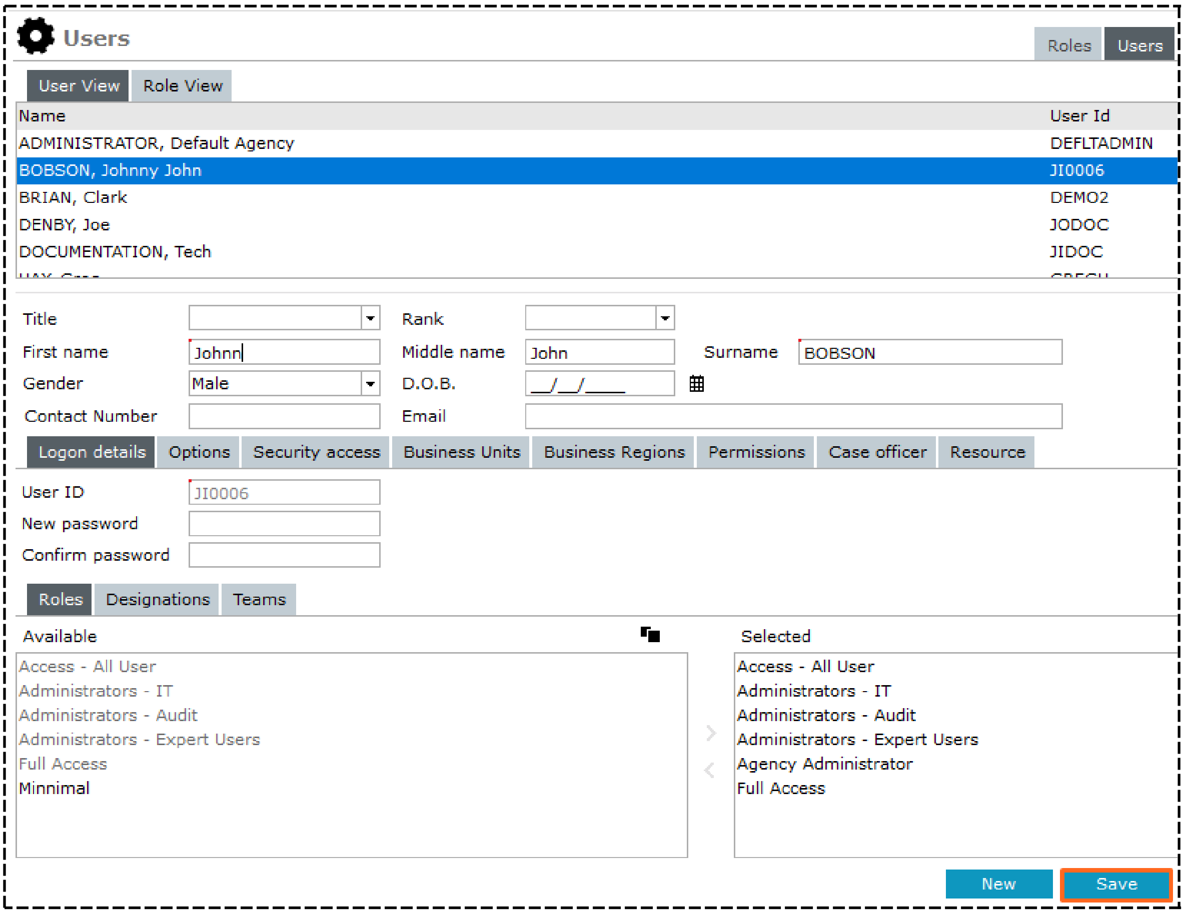
See Users Associated With a Role

1. Select **Admin** > **Security** > **Users**.
2. Select the **Role View** subtab.
3. To see the individual users of a role, select the Expand + icon.



Edit a User

1. Select **Admin** > **Security** > **Users**.
2. Select the user you want to edit.
3. Make your changes.
4. Select **Save**.



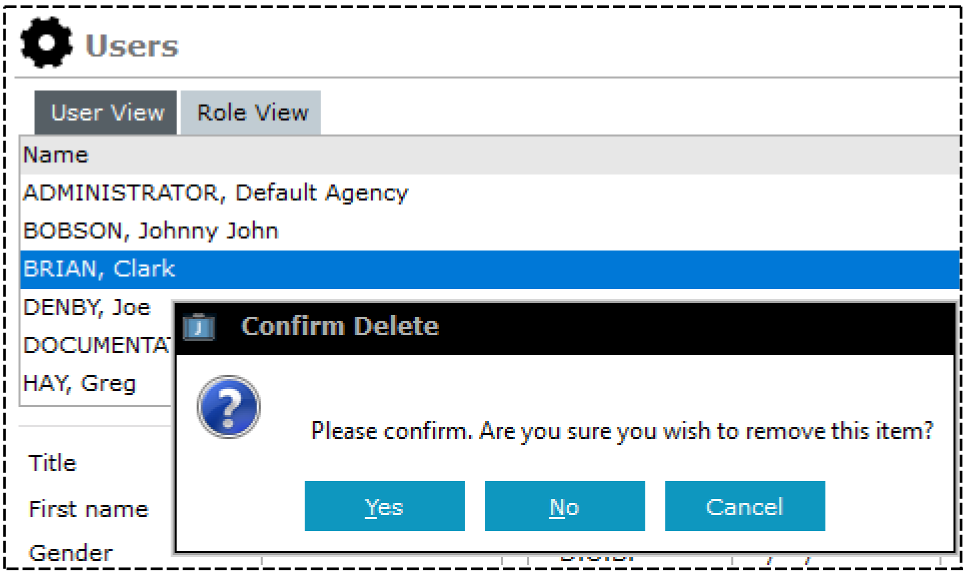
Delete a User

Use any of these methods to remove a user's access:

- Deactivate the user – Select the **Deactivated** checkbox on the *Options* screen.
- Identify the user as having left your agency – Select the **User left Organisation** checkbox on the *Options* screen.
- Delete the user.

To delete a user:

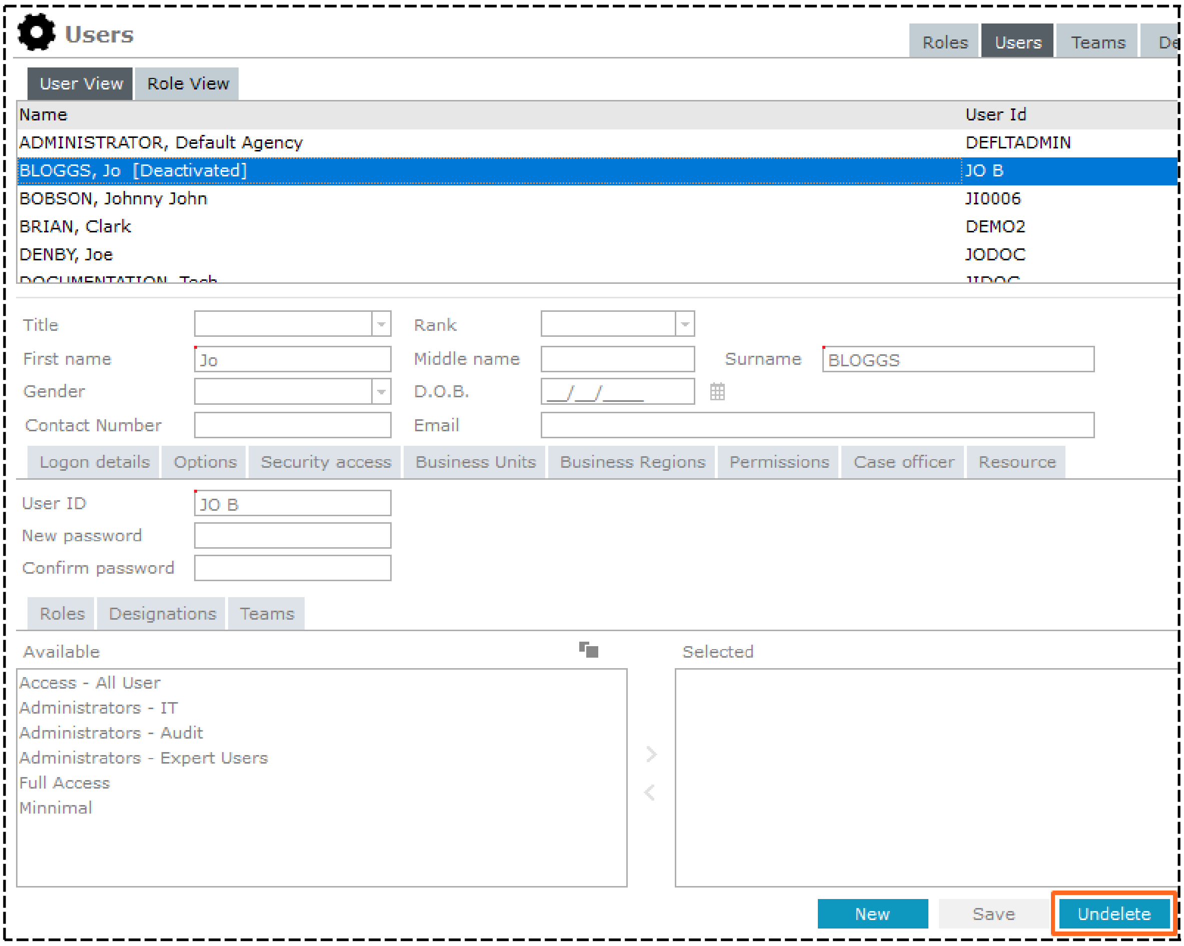
1. Select **Admin** > **Security** > **Users**.
2. Select the user you want to delete.
3. Select **Delete**.
4. Select **Yes** to confirm you want to delete the user.



You can reinstate a user you've accidentally deleted.

Reinstate a Deleted User

1. Select **Admin** > **Security** > **Users**.
2. Select the user you want to reinstate.
3. Select **Undelete**.



Bulk Capabilities

You can use the *Bulk Capabilities* screen to specify the case capabilities (functional access) for multiple users and teams.

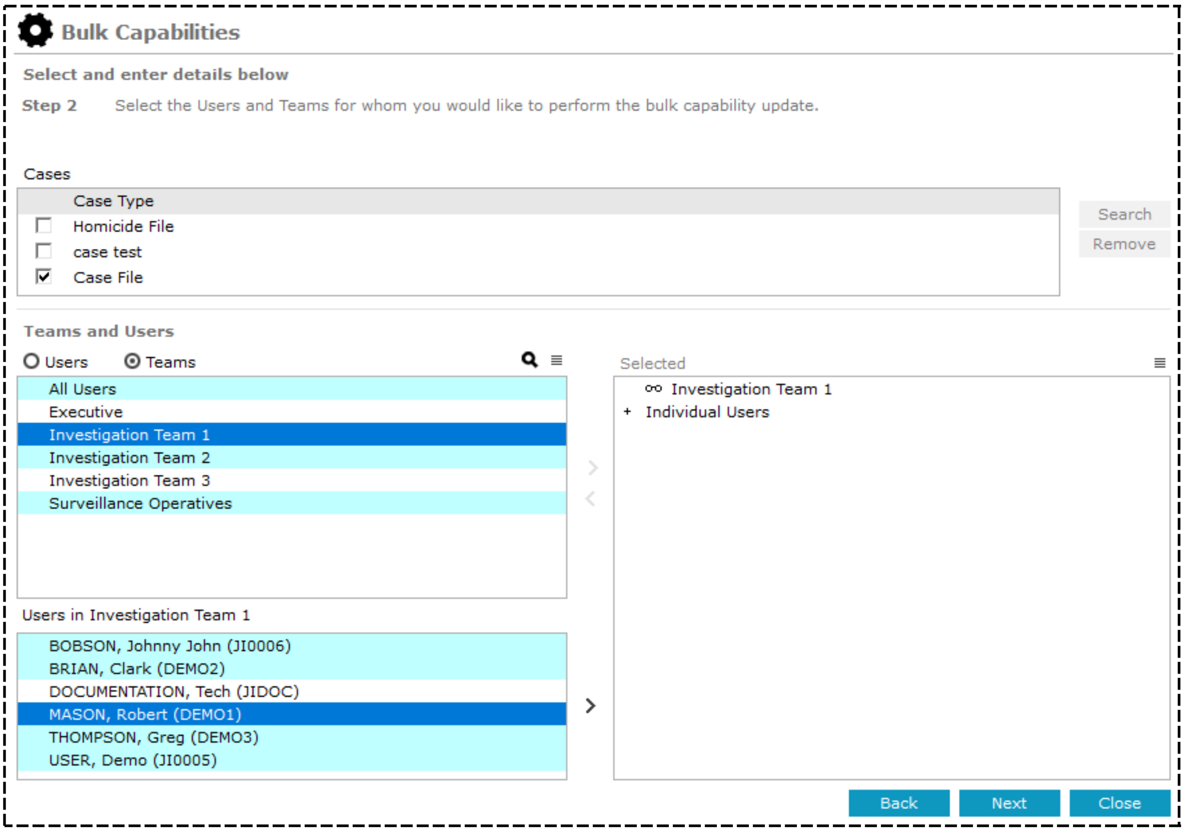
For example, you can specify which case types a team can manage, and then what that team can do with the case information.

Select Cases

Select **Admin** > **Security** > **Bulk Capabilities**.

You can use this screen to:

- Drag and drop specific cases from the *Favourites* or *Recent* sections to the *Cases* area
- Search for specific cases and add them to the cases area
- Select types of cases



Bulk Access

You can manage the security access list for types of cases, Incident Reports, and Information Reports.

You can also manage the security access list for one or more cases, Incident Reports, or Information Reports.

The screen name relates to each of type of source entity.

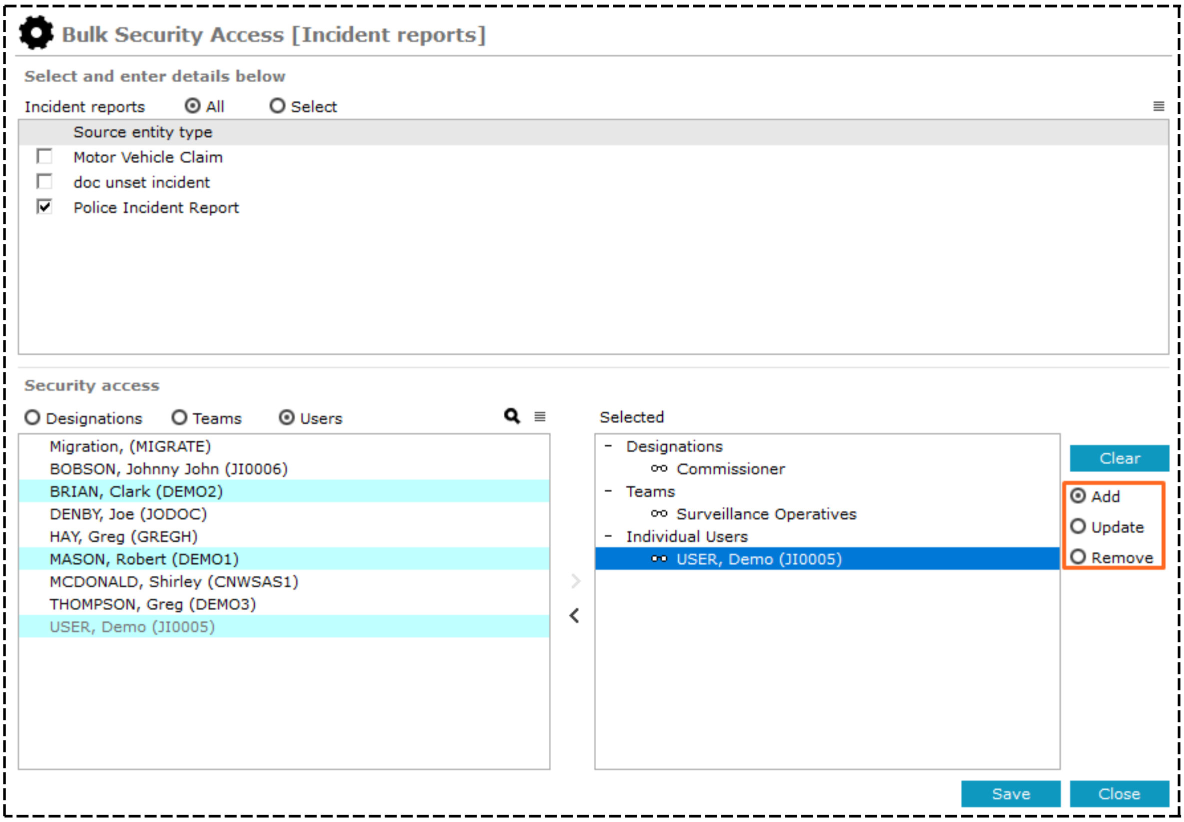
You can either:

- Select all source entities for the types you've selected – For example homicide investigations or case files.
- Search for types of source entities – For example Homicide Investigations with the keyword **Hagley**.

You can build a list of several source entities and give Designations, Teams, and Users access to these.

Grant Bulk Access to Source Documents

1. Select **Admin** > **Security** > **Bulk Access** > Select the required source entity.
2. Select the **All** option.
3. Select the types of source entities you want to apply security access changes to.
4. In the **Security Access** area, select the designations, teams, and users who should have access to the selected incident reports.
5. Specify the action that applies to each item in the **Selected** area:
   - Add
   - Update
   - Remove
6. Select **Save**.


Bulk Security Access [Incident reports]
Select and enter details below
Incident reports
All
Select
Source entity type
Motor Vehicle Claim
doc unset incident
Police Incident Report
Security access
Designations
Teams
Users
Migration, (MIGRATE)
BOBSON, Johnny John (JI0006)
BRIAN, Clark (DEMO2)
DENBY, Joe (JODOC)
HAY, Greg (GREGH)
MASON, Robert (DEMO1)
MCDONALD, Shirley (CNWSAS1)
THOMPSON, Greg (DEMO3)
USER, Demo (JI0005)
Selected
Designations
Commissioner
Teams
Surveillance Operatives
Individual Users
USER, Demo (JI0005)
Clear
Add
Update
Remove
Save
Close

PERMISSIONS

Permissions control access to creating a case, deleting relationships, downloading document files, and more. They determine what you can do in ICM.

Permissions are assigned to roles. They are not assigned to individual users.

Even where one user only is authorised to do something, you'll need to create a role for them to do that and assign it to them.

See Managing Roles.

ICM has these types of permissions:

- Static permissions are system-defined:

  You can't add, change, or delete them.

  Static permissions relate to the functions that are available to all agencies.

- Dynamic permissions are created automatically when your agency configures its own new high-level entity types

  For example, cases, incident reports, and information reports.

Permissions are grouped under several high-level headings and subheadings.

Defining Roles and Permissions

Roles and permissions control access to functionality in ICM. For example, they control who can create a case or delete an entity.

You can use roles to logically group permissions according to the type of work a user does.

For example, you can have a case officer role and a team member role. Each role has a different set of permissions that enables or disables access to different areas.

Permissions control access to particular functions. Essentially, they determine what users can do.

Here are some examples:

- Can Create a Case
- Can Delete a Relationship
- Can Download Document Files
- Can Maintain Roles

    You can't use roles and permissions to grant access to individual cases, incident reports, information reports, and their associated entities (data access).

    Entities and source entities have their own access area that you can use to specify who can access them.

General Permissions

General permissions control access to:

- General functions like seeing who's placed a watch on an entity
- Admin functions like managing templates

Relationship Permissions

These control who can delete a relationship. If you have the *Can delete a relationship* permission, you can remove and reinstate a relationship between two entities.

Report Permissions

If you have the *Can run reports* permission you'll see the *Reporting* menu, which you can use to run reports.

Search Permissions

Entity Search

An entity type that has search permissions selected displays for the user in the search menu.

An entity type with no search permission is hidden from the user in the search menu.

A *Can search* permission for each entity type in the *Entity* group—for example, Can Search Transaction—allows you to set the search permission for specific entity types.

System-defined types—for example, Event, Location, and Contact Number—and user-defined (miscellaneous) types display together under Entity. But because user-defined types require a category, they're always shown under their category header.

System-defined types display under their category, if one exists.

Each type of incident report, information report, case, case note, and task has a *Can search* permission.

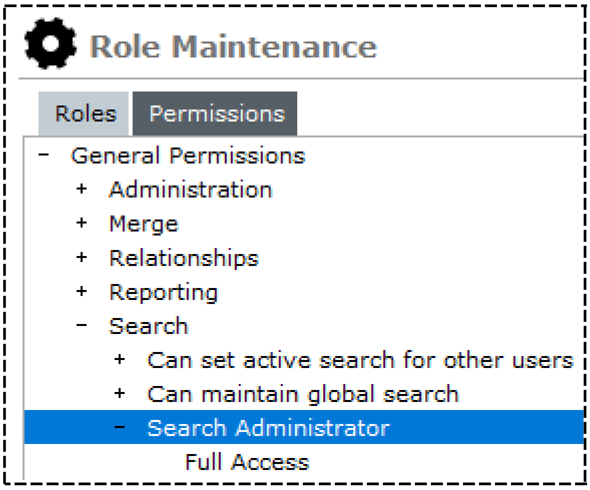
Permissions are based on category and individual search permissions.

For example, if you have the permission *Can search* (All Abc Category) but don't have the *Can search* (All Category for Cases) permission for all types in that category, you can search the Abc category but you'll only see results for the individual types you have permission to search.

Search Admin Permission

Users with this permission can:

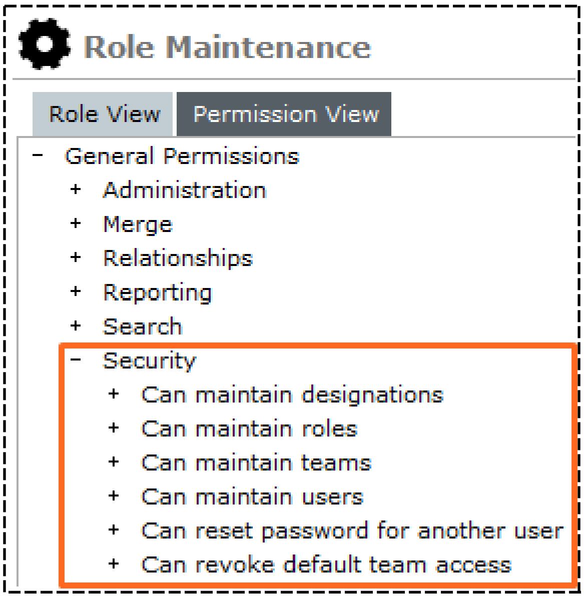
- Search for any entity type. This is effectively the same as granting search permission individually for each entity type.
- See all stored searches, regardless of entity type.



Security Permissions

Security permissions control access to security-related functions.

The following security permissions are available:



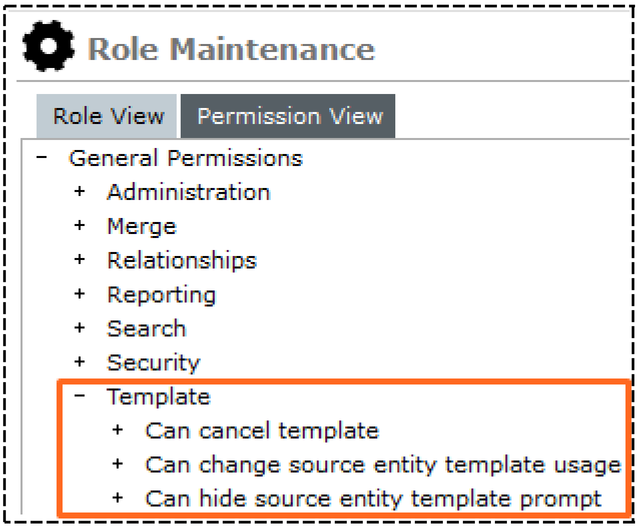
The table explains these.

Security Permission	What You Can Do If You Have This Permission
Can maintain designations	Use this permission to assign designations to users. *This permission gives access to data. We recommend you assign it sparingly.*
Can maintain roles	You can change an existing role by adding additional high-level permissions to that role, for example, *Can change security access of any system entity*. All users with this permission automatically get the newly updated high-level permissions. *This permission enables access to data. We recommend you assign it sparingly.*
Can maintain teams	Teams are one way to manage access to data. If you add an unauthorised user to a team, that user gains automatic access to all data the team has been assigned to. *This permission gives access to data. We recommend you assign it sparingly.*

Can maintain users	This permission lets you to assign roles to users. If you give an unauthorised user a high-level access role containing the permission—for example, Can change security access of any system entity and Can change case officer—that user can access data which could be restricted. *This permission enables access to data. We recommend you assign it sparingly.*
Can reset password for another user	Reset the password for another user. *This permission lets you permanently change another user's password. We recommend you assign it sparingly.*
Can revoke default team access	Remove the agency default teams that can access specified cases, incident reports, and information reports. This permission doesn't apply to the individual users of the default agency. *We recommend you restrict access to this permission.*

Template Permissions

The following template permissions are available:



The table explains these.

Template Permission	What You Can Do If You Have This Permission
Can cancel template	Enter data without using the template defined for that data entry purpose. *We recommend you restrict access to this permission.*
Can change description template usage	Decide which types of source entities a particular template is used for.
Can hide source entity template prompt	Hide or show the *Template Usage* screen. Select or deselect the **Hide Source Entity** checkbox on the *User Preferences* screen. The user can bypass being forced to use a template when they create a new source entity. This permission overrides using all templates, regardless of whether the user has the *Can cancel template* permission. *We recommend you restrict access to this permission.*

Thesaurus Permissions

Thesaurus permissions control whether a user can access the thesaurus management functions under **Admin** > **System** > **Thesaurus**.

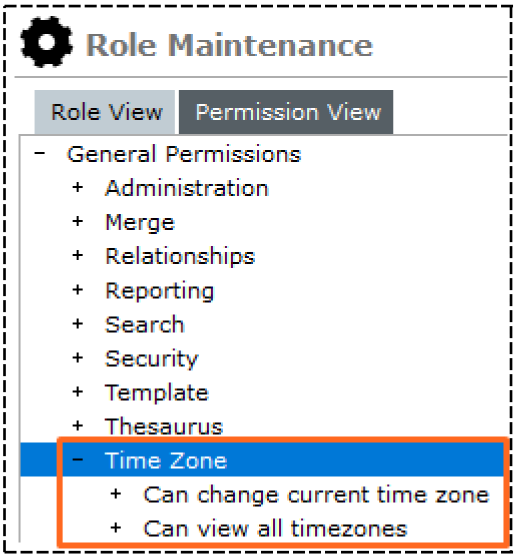
The following thesaurus permissions are available:

The table explains these.

Permission	Description
Can extract global thesaurus	Extract a thesaurus to an XML file. Makes the System > Thesaurus > Export menu visible.
Can load global thesaurus	Import a thesaurus from an XML file. Makes the System > Thesaurus > Import menu visible.
Can maintain global thesaurus	Maintain the thesaurus. Makes the System > Thesaurus > Maintenance menu visible.
Can maintain thesaurus search groups	Maintain thesaurus search groups. Makes the System > Thesaurus > Search Groups menu visible.

Time Zone Permissions

The following Time Zone permissions are available:



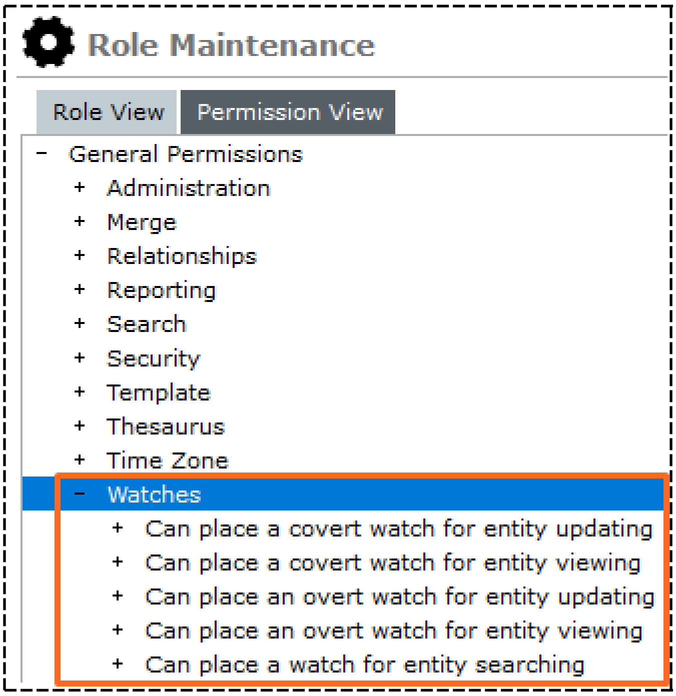
The table explains these.

Time Zone Permission	What You Can Do If You Have This Permission
Can change current time zone	Change the time zone of their workstation. Makes the Change Time Zone popup menu visible.
Can view all time zones	View the *Time Zones* screen. Makes the **Admin** > **System** > **Time Zones** screen visible.

Watch Permissions

Watch permissions control access to the types of watches that can be placed on entities.

The following watch permissions are available:



The table explains these.

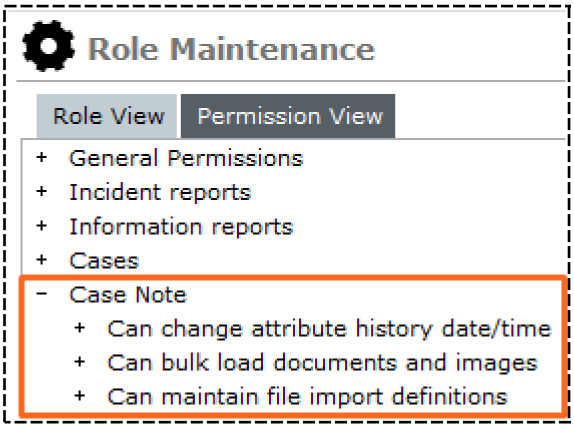
Watch Permission	What You Can Do If You Have This Permission
Can place a covert watch for entity updating	Types of covert update watches on an entity. Makes the *Watches* popup menu item visible. Makes the *Covert/Update* columns visible on the *Watches* screen.
Can place a covert watch for entity viewing	Types of covert view watches on an entity. Makes the *Watches* popup menu item visible. Makes the *Covert/View* columns visible on the *Watches* screen.
Can place an overt watch for entity updating	Types of overt update watches on an entity. Makes the *Watches* popup menu item visible. Makes the *Overt/Update* columns visible on the *Watches* screen.

Can place an overt watch for entity viewing	Types of overt view watches on an entity. Makes the Watches popup menu item visible. Makes the Overt/View columns visible on the Watches screen.
Can place a watch for entity searching	Types of search watches on an entity. Makes the Watches popup menu item visible. Makes the Search columns visible on the Watches screen. Covert watch.

Case Note Permissions

Case note permissions control access to case notes.

The following case note permissions are available:

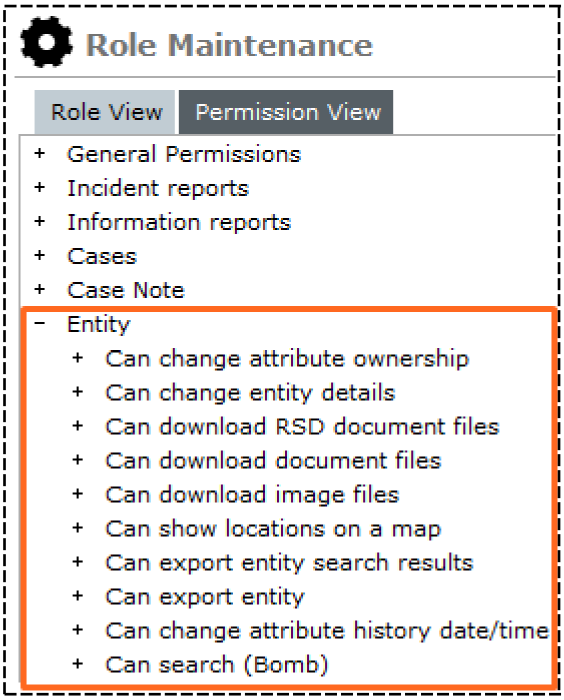


The table explains these.

Case Note Permission	What You Can Do If You Have This Permission
Can change attribute history date/time	Change the date and time that's recorded on case note attributes that have been specified as Behaviour-historical. *We recommend you restrict access to this permission because these changes could affect attributes used in case management queries and reporting.* *For example, status and workflow type attributes.*
Can bulk load documents and images	Upload multiple documents and images to a case note. Enables Bulk load menu item under the Overflow >> tab on case notes. Bulk load allows you to import documents and images in bulk from specified directory.
Can maintain file import definitions	Manage file import definitions for a case note. Enables the *File Import* menu item under the Overflow >> tab on case notes. File import allows you to create entities from file.

Entity Permissions

The following entity permissions are available:



The table explains these.

Entity Permission	What You Can Do If You Have This Permission
Can change attribute ownership	Move the source of attributes of an entity from one case note or information report to another. Allows the user to change the ownership of an attribute from the original source entity where the tangible entity was added. If restricted, the visibility of the attribute will be based on the security of the source entity it relates to.
Can change entity details	Edit an existing entity.

Can download RSD document files	Download the direct document for any report source document entities (RSD) they have access to. For example, an incident report or an information report. *To download the direct document, the **Direct Document** option for the incident or information report entity must be enabled.* *See **Specifying options for source entities other than a case**.*
Can download document files	Download documents about an entity to their workstation.
Can download image files	Download images about an entity to their workstation.
Can export entity search results	Export the list of search results of an entity to a file.
Can export entity	Extract all entities and their relationships to a file.
Can change attribute history date/time	Change the date and time that's recorded on entity attributes that have been defined as Behaviour-historical.
Can search	See the Search <type> menu.

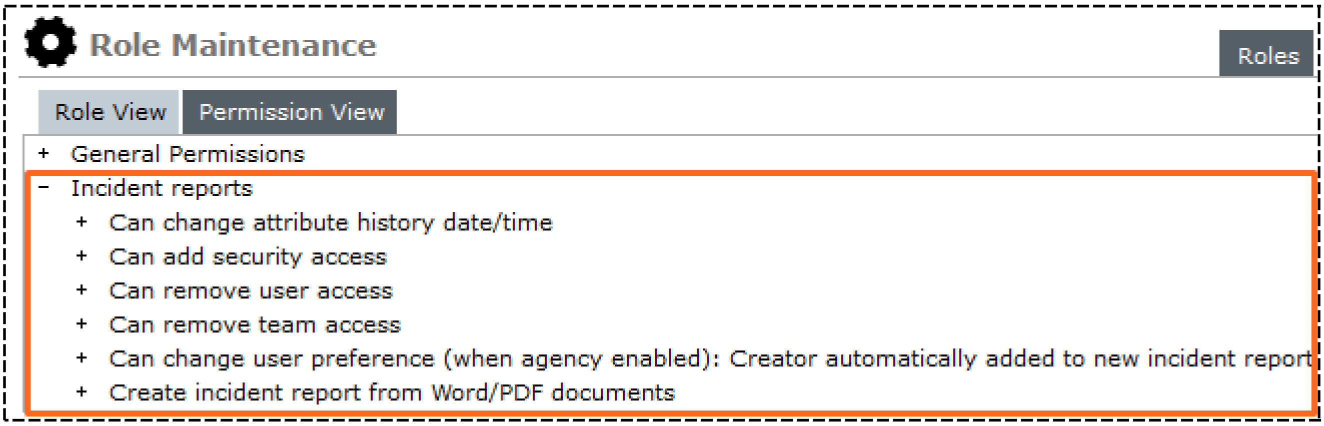
Incident Report Permissions

Incident report permissions control access to incident reports. When your agency sets up more types of incident report, these generate their own, specific, dynamic permissions.

You can assign dynamic permissions to roles using the Roles screen of the Entity Types maintenance screen for that entity.

*See **Associating Permissions with Roles for an Entity Type**.*

The following incident report permissions are available:



The table explains these.

Incident Report Permission	What You Can Do If You Have This Permission
Can change attribute history date/time	Change the date and time that's recorded on the incident Date/Time report, attributes that have been defined as Behaviour-historical. *We recommend you restrict access to this permission. These changes could affect attributes used in case management queries and reporting.* *For example, status and workflow type attributes.*
Can add security access	Add users and teams to the security access list of an incident report.
Can remove user access	Remove users from the security access list of an incident report.
Can remove team access	Remove teams from the security access list of an incident report.

Can change user preference (when agency enabled): Creator automatically added to new incident report	Select or deselect the Creator added to new Case checkbox on the User Preferences screen, and to change user preferences. *An option on the System Settings screen enables or disables the Creator added to new Case checkbox on the User Preferences screen for all users in the agency.* *See Managing Agency Parameters.*
Create incident report from Word/PDF documents	Does not include the update of attribute fields or populate the narrative description. It creates only a report with the title of the uploaded file and the path from which the file was created, in the description area. If the user doesn't check the Document direct checkbox, no narrative is uploaded. Assumes the When Reported and When Happened dates are that of the date of the upload.

Permissions for Incident Reports Defined by an Agency

Incident Report Permission	What You Can Do If You Have This Permission
Can create	Create a new incident report. *Without additional permissions (listed in this table), after the user saves the incident report, they can't edit it.*
Can change	Change the details and attributes of an existing incident report, if the user has direct edit access to the incident report. The user can't modify security or add entities but they can upload a document to the incident report.
Can delete	Delete an incident report. *This permission is overruled by the security access list of an incident report.* *If a user has this permission but not the **Can Change** permission, the Delete button is disabled.* *We recommend you restrict access to this permission.*
Can search	Search for the type of source entity.
Can change entity to entity relationship	Edit and update an existing relationship between entities in the incident report.
Can create source entity to entity relationship	Create a relationship between an entity and the incident report. *Users can do this, even if they don't have the permission to change an incident report.*
Can create case	Create a case directly from an incident report.
Can create entity to entity relationship	Link and create a relationship between the entities in an incident report.
Can create task	Create and thread a task to an incident report

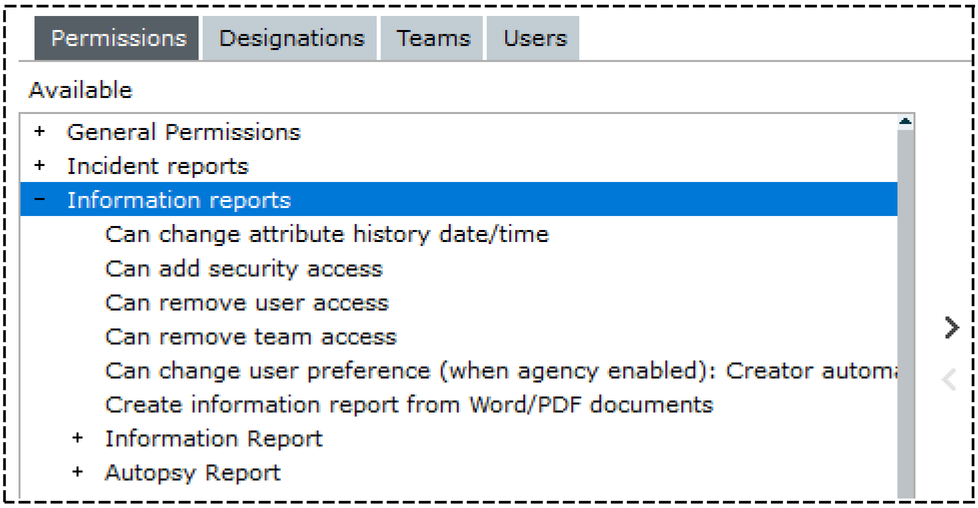
Can replace document	Replace the document that's been attached to an incident report, for example if that document was attached accidentally.

Information Report Permissions

Information report permissions control access to information reports. When your agency sets up more types of information reports, these generate their own specific, dynamic permissions.

Assign dynamic permissions to roles using the Roles screen of the Entity Types maintenance screen for that entity.

The following image shows the permissions that are listed under the Information reports item on the Role Maintenance screen.



The following Information report permissions are available:

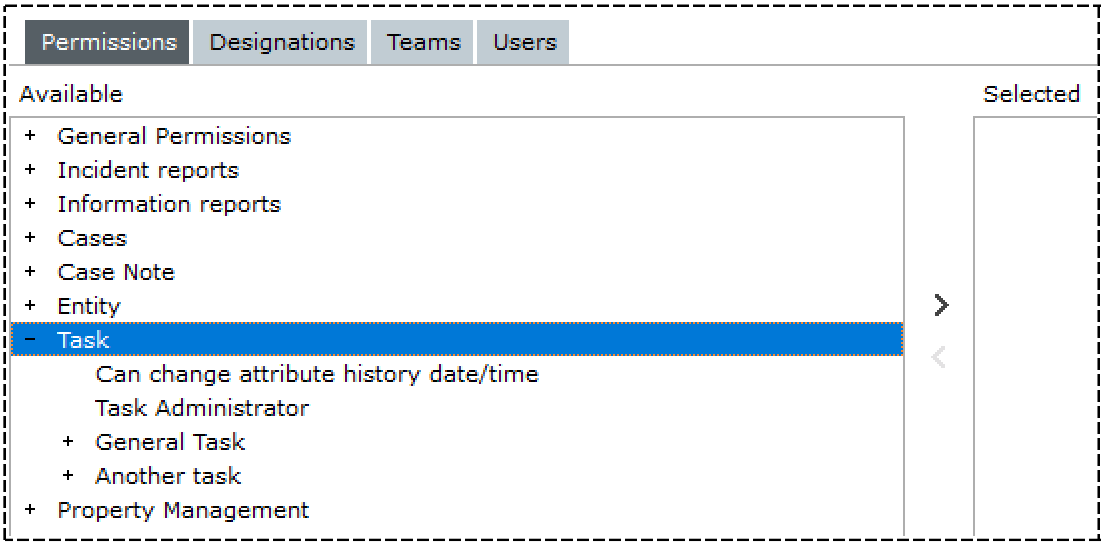
Information Report Permission	**What You Can Do If You Have This Permission**
Can change attribute history date/time	Change the date and time that's recorded on information report attributes that have been defined as Behaviour- historical. Determines whether the Maintain Attribute History menu item is available on the **Attributes** popup menu. *We recommend you restrict access to this permission. This is because these changes could affect attributes used in case management queries and reporting – For example, status and workflow type attributes.*
Can add security access	Add users and teams to the security access list of an information report.
Can remove user access	Remove users from the security access list of an information report.

Can remove team access	Remove teams from the security access list of an information report.
Can change user preferences (when agency enabled): Creator automatically added to new information report	Select or deselect the Creator added to new Case checkbox on the User Preferences screen, and to change user preferences. If set the user preference Creator automatically added to information report value will be used otherwise the agency default will be used. *An option on the System Settings screen enables or disables the Creator added to new Case checkbox on the User Preferences screen for all users in the agency.*
Create information report from Word/PDF documents	Create information reports from Word documents. Allocate this permission carefully. Creating information reports from Word documents: Does not include the update of attribute fields or populate the narrative description. It creates only a report with the title of the uploaded file and the path from which the file was created, in the description area. If the user doesn't check the Document direct checkbox, no narrative is uploaded. Assumes the When Reported and When Happened dates are that of the date of the upload.

Task Permissions

Task permissions control access to task-related functions.

The following image shows the permissions that are available.



The table explains these.

Task Permission	What You Can Do If You Have This Permission
Can change attribute history date/time	Change the date and time that's recorded on task attributes that have been defined as Behaviour-historical. *We recommend you restrict access to this permission. This is because these changes could affect attributes used in case management queries and reporting – For example status and workflow type attributes.*
Can search	Search for the type of source entity
Can view summary	See a summary of tasks by type, recipient, recipient status, priority, completion date, business unit, and business region
Can create case	Create a case directly from a task
Can change	Change the details and attributes of an existing task (if the user can edit the task)

The user can't change security or add any entities, but they can upload a document to the task.

Task Permission	What You Can Do If You Have This Permission
Can change source entity to entity relationship	Change the relationship between an entity and a task.
Can change entity to entity relationship	Edit and update a relationship between entities in the task.
Can create	Create a new task of the specified type. *Without additional permissions (listed in this table), after the user saves the task, they can't change it.*
Can create source entity to entity relationship	Create a relationship between an entity and task. *Users can do this even if they don't have the permission to change a task.*
Can create entity to entity relationship	Link and create a relationship between the entities in a task.
Can create task	Create and thread a task to an information report.
Can delete	*Delete a task.* *This permission is overruled by the security access list of a task.* *If a user has this permission but they don't have the **Can Change** permissions, they won't be able to delete a task.* *We recommend you restrict access to this permission.*

System Settings

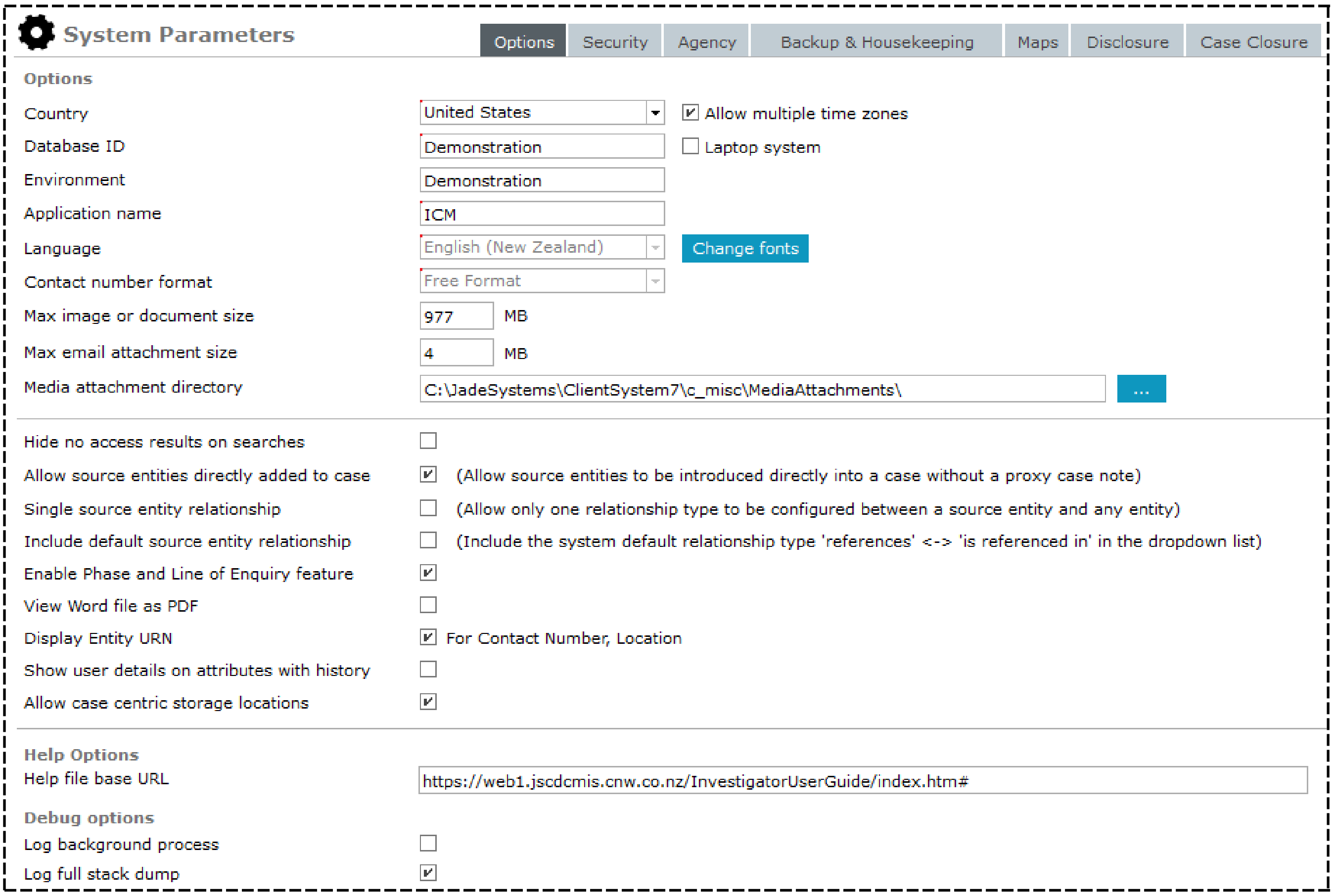
You can set up system-wide parameters like:

- The logo in ICM
- Security rules
- How long to keep database recovery journals

To access these options, select **Admin** > **System** > **Settings**.

The following tabs are available:

Tab	Function
Options	Specify general, Help, and debugging options.
Security	Specify logon rules and authentication parameters.
Agency	Specify logos, disclaimer messages, and preferences for your agency. This includes options for creating source entities.
Backup & Housekeeping	Specify options for journal, log, scheduling, backup times, and running a backup immediately.
Maps	Specify whether you want maps shown in ICM.
Disclosure	Enter the warning message associated with generating a marked up package. Specify the types of files that can be replaced by PDFs when a disclosure is processed.
Case closure	Enter the text you want displayed when a user is about to close a case.


System Parameters
Options
Security
Agency
Backup & Housekeeping
Maps
Disclosure
Case Closure
Options
Country
United States
Allow multiple time zones
Database ID
Demonstration
Laptop system
Environment
Demonstration
Application name
ICM
Language
English (New Zealand)
Change fonts
Contact number format
Free Format
Max image or document size
977
MB
Max email attachment size
4
MB
Media attachment directory
C:\JadeSystems\ClientSystem7\c_misc\MediaAttachments\
...
Hide no access results on searches
Allow source entities directly added to case
(Allow source entities to be introduced directly into a case without a proxy case note)
Single source entity relationship
(Allow only one relationship type to be configured between a source entity and any entity)
Include default source entity relationship
(Include the system default relationship type 'references' <-> 'is referenced in' in the dropdown list)
Enable Phase and Line of Enquiry feature
View Word file as PDF
Display Entity URN
For Contact Number, Location
Show user details on attributes with history
Allow case centric storage locations
Help Options
Help file base URL
https://web1.jscdcmis.cnw.co.nz/InvestigatorUserGuide/index.htm#
Debug options
Log background process
Log full stack dump

Manage Security Rules

1. Select **Admin** > **System** > **Settings**.
2. Select the **Security** tab.
3. Make sure **Application** is selected as the logon authentication option.
4. In the *Application Authentication* area, specify the rules that apply to passwords:
   a. In the **Minimum password length** field, enter the minimum number of characters required for passwords.
   b. In the **Maximum password length** field, enter the maximum number of characters required for passwords.
   c. In the **Password expires in (days)** field, enter the number of days after which users must change their password.
   d. In the **Remember 'nn' passwords** field, enter the number of previous passwords for ICM to remember.

      A user can't reuse a password that's stored in ICM.
   e. Select the **Allow direct logon from Windows** checkbox to let users run ICM without signing on.

      If you select this checkbox, when a user logs on to Windows, ICM will verify their ID.

      The logon screen won't display. The Home screen will open automatically.

      *When they select **System** > **Logoff**, they can use the sign-in screen to log on automatically with their current user ID, or log on as a different user.*
5. In the *User logons* area, specify the rules that apply to logon attempts:
   a. In the **Number of sessions allowed** field, enter the maximum number of sessions a user can be logged in to at a time.

      If a user exceeds the maximum permitted number of concurrent logons, they'll be notified of this.

      They won't be notified if the password validation happens when you're resetting another user's password.

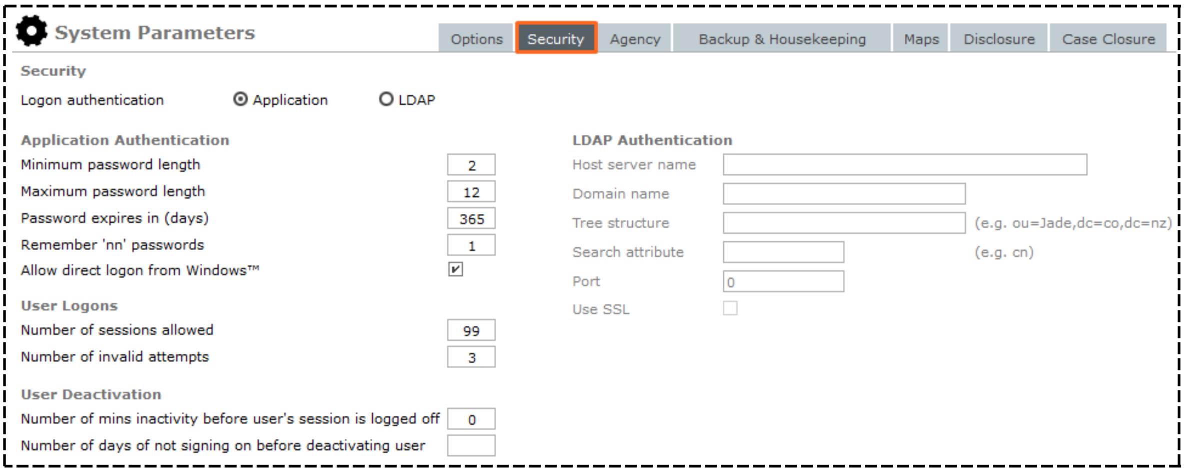
      The default value is zero. This means there's no limit to how many sessions a user can log in to.
   b. In the **Number of invalid attempts** field, enter the maximum number of invalid password attempts allowed at one time before the user needs to reset their password.

      A warning will display before the user makes their final permitted invalid password attempt.
6. In the **User deactivation** area, specify the rules that apply to deactivating users:
   a. In the **Number of mins inactivity** ... field, enter the number of minutes a user can be inactive for before they're logged off.
   b. In the **Number of days** ... field, enter the number of days after which an inactive user has access disabled.

An inactive user is someone who hasn't logged in for the amount of time specified.

After the specified amount of time, any user who hasn't logged on is prevented from doing so until you re-enable that user.

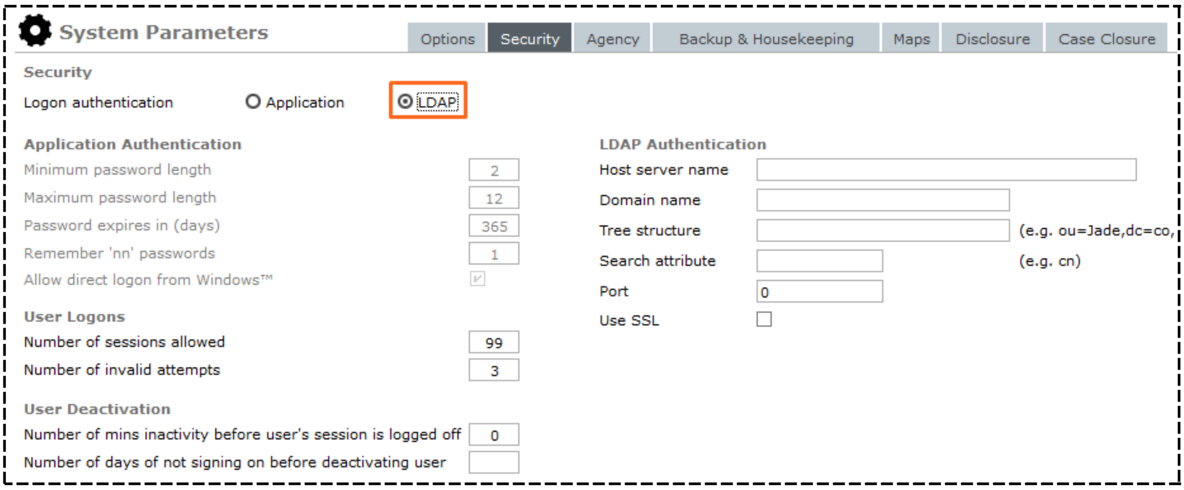
7. Select **Save**.



Manage Security Rules for the Lightweight Directory Access Protocol (LDAP)

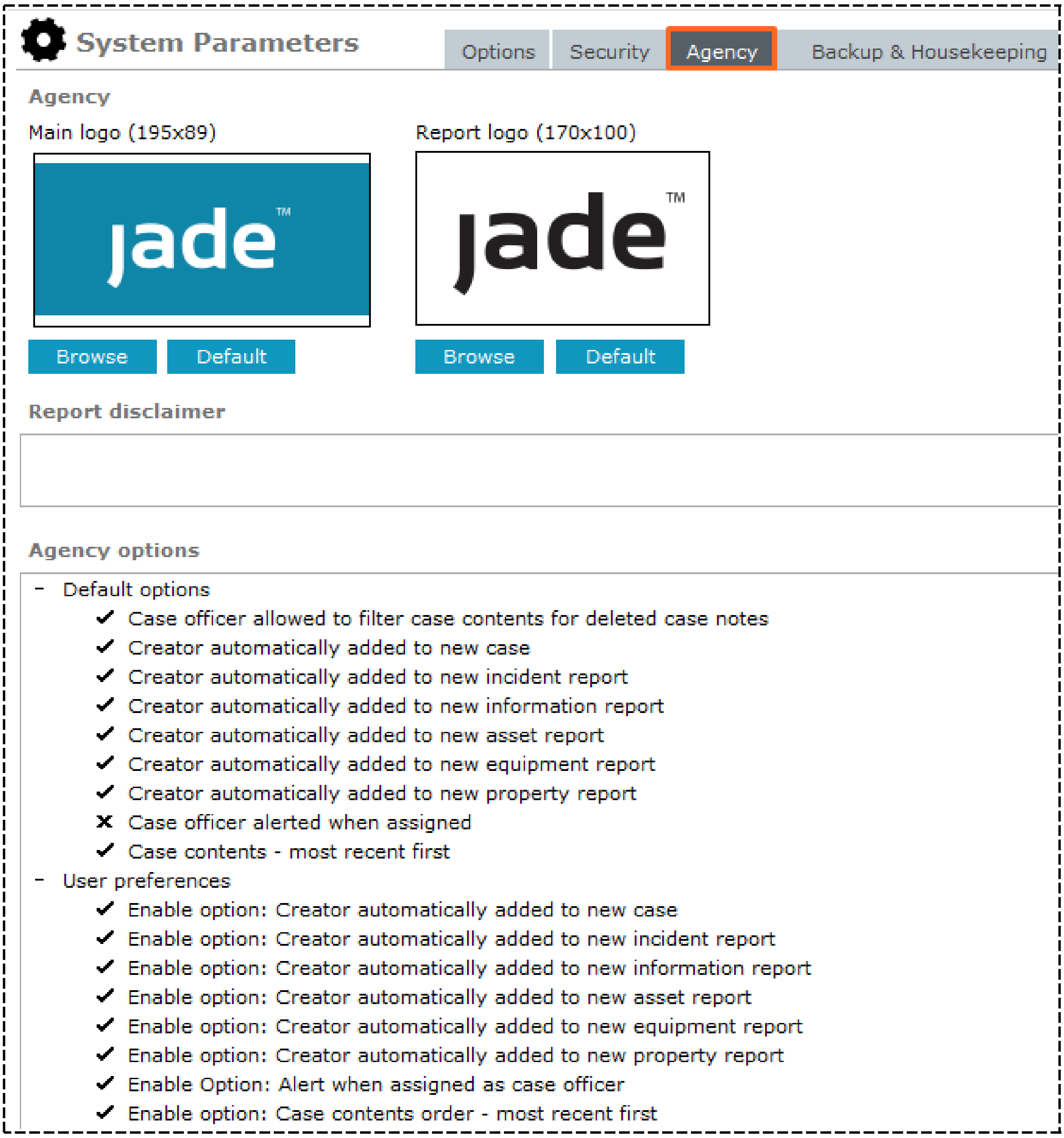
1. Select **Admin** > **System**> **Settings**.
2. Select the **Security** tab.
3. Select the **LDAP** option.

   You might need to ask your LDAP administrator for the information in these fields.
4. In the **Host server name** field, enter the LDAP host server name.
5. In the **Domain name** field, enter the LDAP domain name.
6. In the **Tree structure** field, specify the parameters that define the tree structure.
7. In the **Search attribute** field, specify the list of attributes you want returned in an LDAP search.
8. In the **Port** field, enter the port number your LDAP server listens on.
9. If your LDAP server uses Secure Sockets Layer(SSL), check the **Use SSL** checkbox.



Select Default System Options for Your Agency

1. Select **Admin** > **System** > **Settings**.
2. Select the **Agency** tab.
3. To include a disclaimer when you generate reports, enter a disclaimer in the **Report Disclaimer** field.
4. In the **Agency Options** area, toggle the Check mark ✓ icon s to specify the default settings and user preferences for your agency.
5. Select **Save**.



Add Your Logo

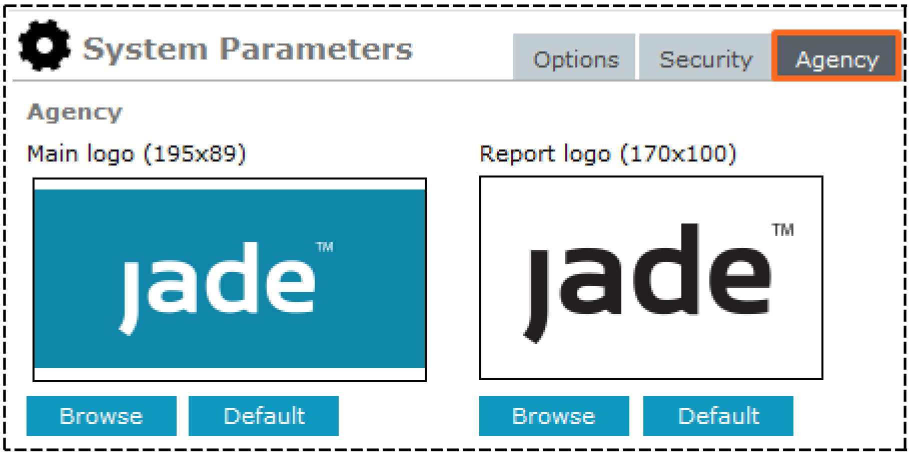
You can set parameters for your agency and include your agency's logo in ICM:

1. Select **Admin** > **System** > **Settings**.
2. Select the **Agency** tab.
3. In the *Agency* area, specify the logos you want to show in different parts of ICM:
   a. Select **Browse** below the *Main logo* to select a logo that will display above the Navigator > Locate and select the required logo.
   b. Select **Browse** below the *Report logo* to select the logo that will display on reports you generate > Locate and select the required logo.

      The recommended image size is shown in pixels at the right of each type of logo.

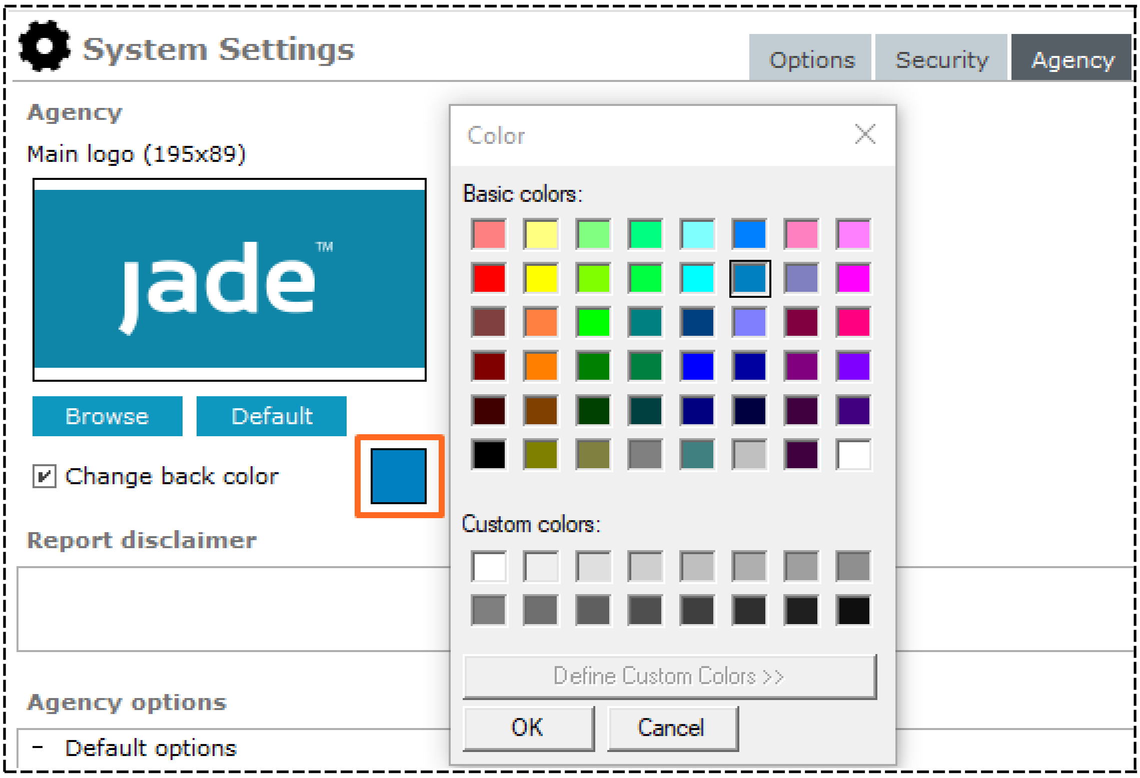
      If you use an image with different dimensions, it will be stretched to fit the space available.

      *Select **Default** to return to the default logo.*
4. To include a disclaimer when you generate reports, enter a disclaimer in the **Report Disclaimer** field.
5. In the *Agency Options* area, toggle the Check mark ✓ icon s to specify the default settings and user preferences for your agency.
6. Select **Save**.



Choose the Background Colour for Your Logo

1. Select **Admin** > **System** > **Settings**.
2. Select the **Agency** tab.
3. Select the **Change back colour** checkbox.
4. Select the colour you want as the background for your logo.
5. Select the colour you want > Select **OK**.
6. Select **Save**.



Backup and Housekeeping

You can set the parameters for these backup and housekeeping settings:

Setting	Description
General options	For example, storing an email address in the database so the system can notify a specified user whether the backup succeeded or failed
Backups of the database	Where the directory backups are saved to.
General housekeeping tasks	Housekeeping tasks are scheduled tasks that manage the database and make sure the required background apps are running. *For example, the number of days to keep log and journal files.*

Manage Backup and Housekeeping Parameters

1. Select **Admin** > **System** > **Settings**.
2. Select the **Backup & Housekeeping** tab:
   - The *Last backup* field shows when last a backup was done.
   - The *Last housekeeping* field shows the last time housekeeping was done.
3. In the **Start time** field, specify when you want to run the housekeeping and backup procedures each day.

   *If you want to run the housekeeping and backup processes immediately, select **Run Now**.*

   We recommend you schedule your database backups for when ICM isn't busy.
4. In the **Email addresses** field, specify where emails should be sent when the housekeeping and backup processes are running.
5. Specify your backup options:
   a. In the **Backup directory** field, specify where backup files are generated.
   b. To disable backups, select the **Disable backup** checkbox (not recommended).
   c. To do quiesced (quiet) backups, select the **Quiesced backup** checkbox.

      See the JADE Database Admin Guide to learn about these backups.
6. To exclude files in the MediaAttachments folder from the backup, select the **Don't backup media folder** checkbox.

   The MediaAttachments folder contains sensitive images, video, and audio files which you might want to keep separate from the main database backup.

   The files stored in the MediaAttachments folder include documents, images, and audio and visual files you've uploaded.

   *Files in the **MediaAttachments** folder aren't indexed.*

   If you store your documents in this folder, they won't come up in search results.

   *To make sure your documents are indexed (and therefore searchable), upload them as a **Document** entity.*
7. To exclude the MediaAttachments folder from the backup, select the **Yes** button.

   Your agency is then responsible for backing up the files in this folder.

   *Alternatively, select **No** to back up the MediaAttachments folder as part of the housekeeping process.*
8. To disable housekeeping, select the **Disable housekeeping** checkbox (not recommended).
9. In the **Delete logs older than** field, enter the number of days after which log files are deleted.

   To disable deleting log files during the housekeeping process, enter zero.

   Zero shows the log files are never deleted.
10. In the **Delete recovery journals older than** field, enter the number of days after which recovery journal files are deleted.

To disable deleting recovery journal files during the housekeeping process, enter zero.

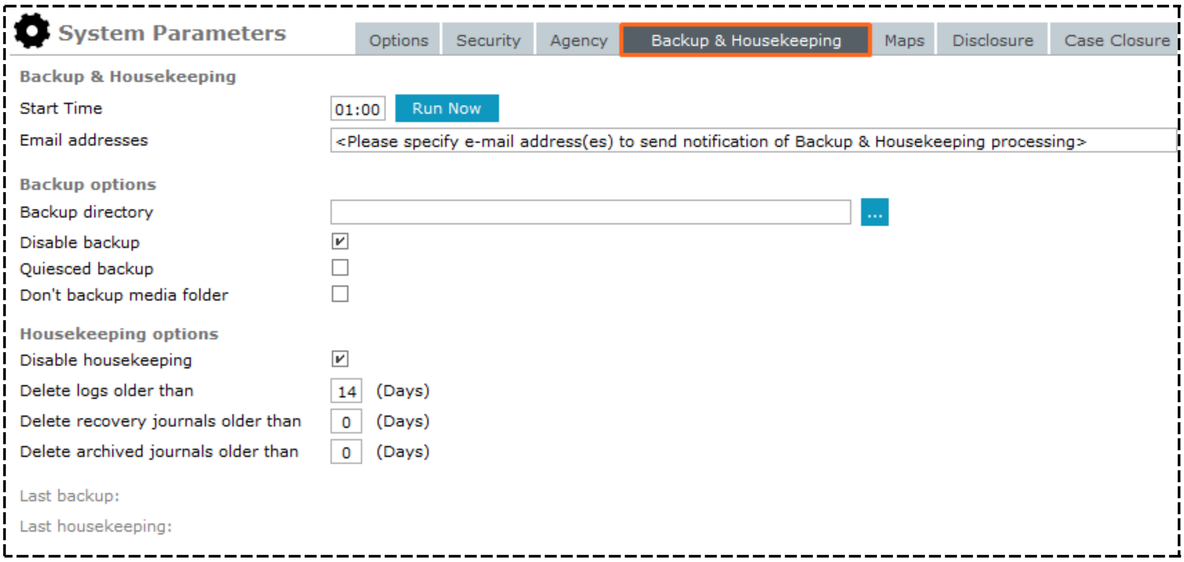
Zero shows the recovery journal files are never deleted.

11. In the **Delete archived journals older than** field, enter the number of days after which archived journal files are deleted.

    To disable deleting archived journal files during the housekeeping process, enter zero.

    Zero shows the archived journal files are never deleted.

12. Select **Save**.



Enable Maps

1. Select **Admin** > **System** > **Settings**.
2. Select the **Maps** tab.
3. Select the **Maps enabled** checkbox.

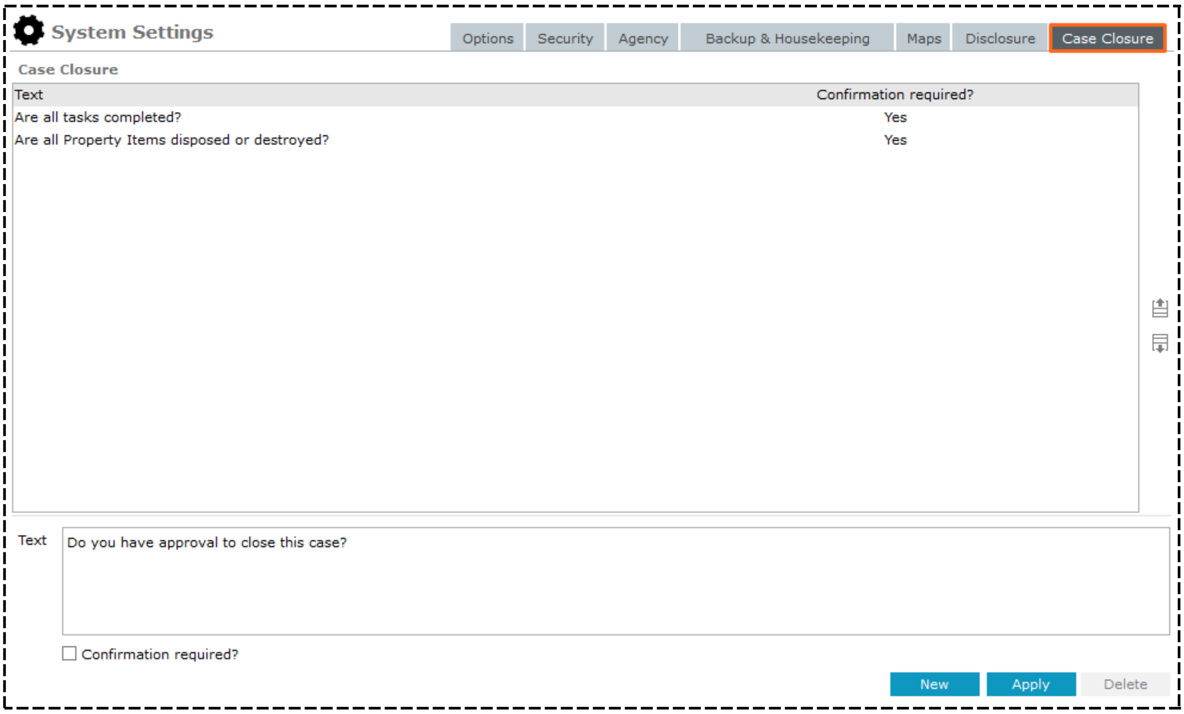
Manage Case Closure Parameters

You can specify the text shown when you're about to close a case.

This provides a way to remind users of the business rules your agency uses when closing cases.

To manage case closure parameters:

1. Select **Admin** > **System** > **Settings**.
2. Select the **Case Closure** tab.
3. To add text to the closure message:
    a. Select **New**.
    b. Enter your message.
    c. Select **Apply**.
4. To delete a message from the closure message:
    a. Select the text in the *Case Closure* area.
    b. Select **Delete**.
5. To edit a line in the closure message:
    a. Select the line in the *Case Closure* area.
    b. Make your changes in the **Text** field.
    c. Select **Apply**.
6. To prompt users to confirm they've complied with the message before closing the case, select the **Confirmation required** checkbox.
7. Save your changes.



Security Access Profiles

Case entities have a default security profile for when a case is open and a second security profile for when it's closed. The **Open Case** and **Closed Case** tabs on the Security access screen define these security profiles.

When a new case entity is created, the security profile defined in the **Open Case** tab is used to populate the **Security access** screen.

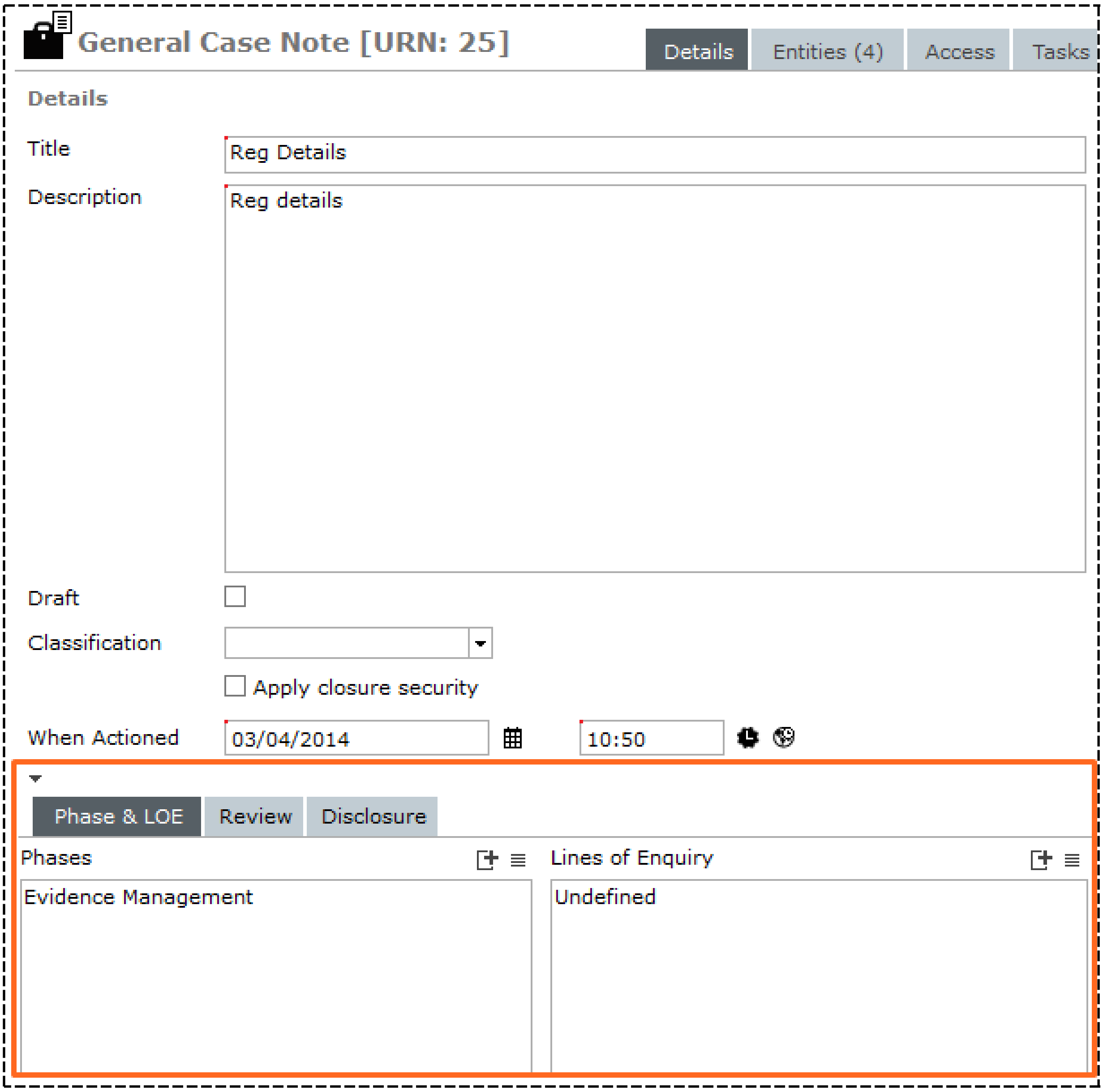
When someone closes a case, the security profile defined in the **Closed Case** tab is used to set the access to any case notes that have the **Apply closure security** checkbox on the **Details** tab even if the access for the case note is locked.

Hide Details About a Case Note You Don't Use

If you don't use the following tabs in case notes, you can hide them to declutter your screen:

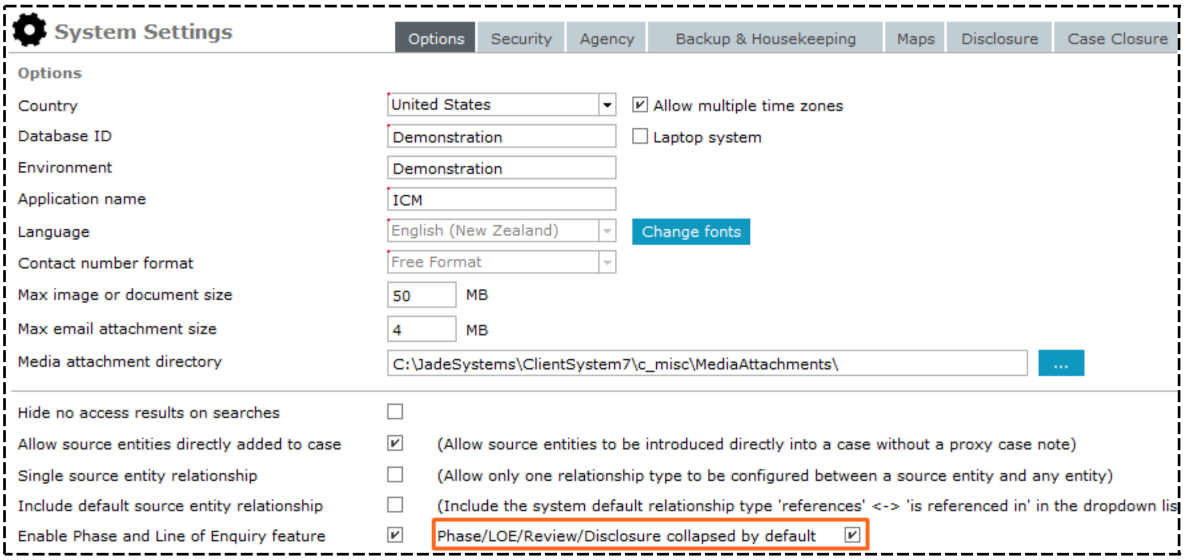
- Phase & LOE
- Review
- Disclosure

To do this, select the Hide additional details pane icon.



If most people in your organisation don't use these tabs, your ICM administrator can hide them by default:

1. Select **Admin** > **System** > **Settings**.
2. Select the **Phase/LOE/Review/Disclosure collapsed by default** checkbox.

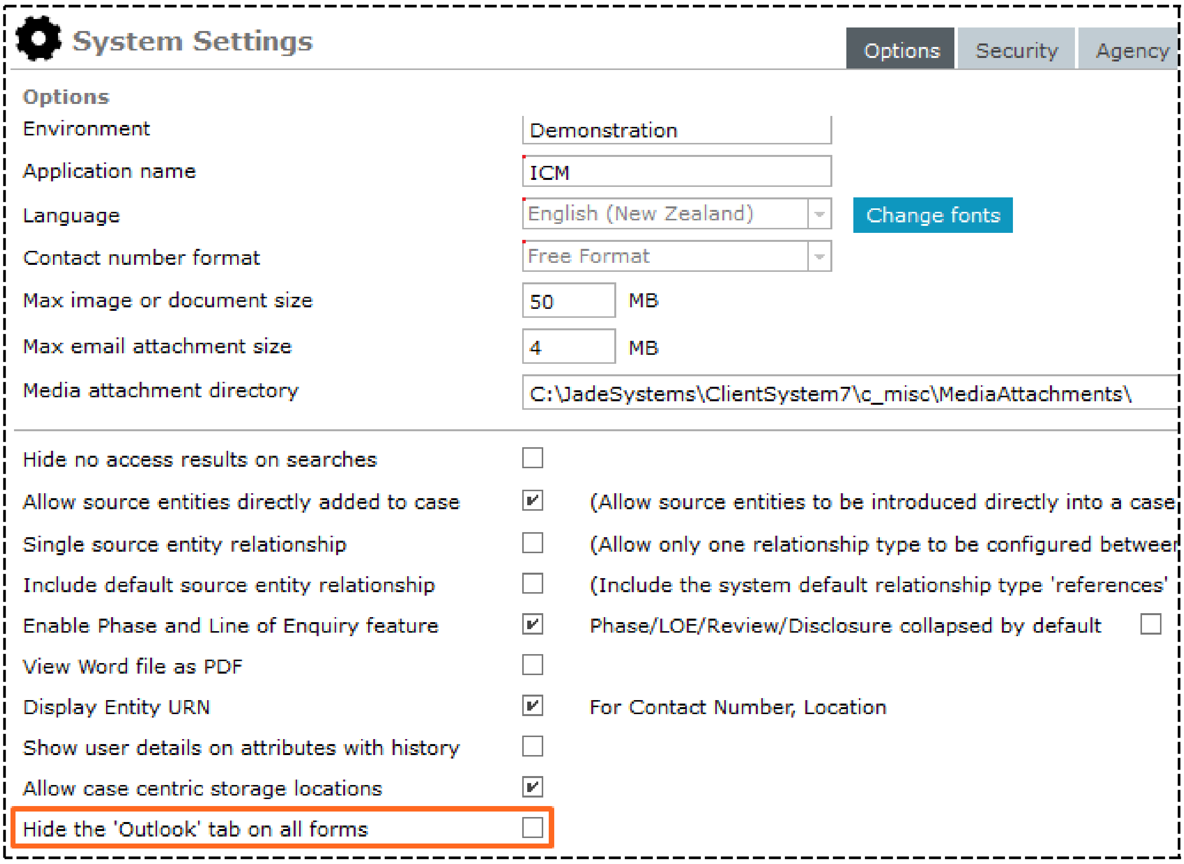


Hide the Outlook Feature

In Investigations Case Management (ICM) you can use Microsoft Outlook to schedule and manage meetings and tasks for a case.

If your organisation doesn't use this feature you can hide it from the menu:

1. Select **Admin** > **System** > **Settings**.
2. Select the **Hide the 'Outlook' tab on all forms** checkbox.

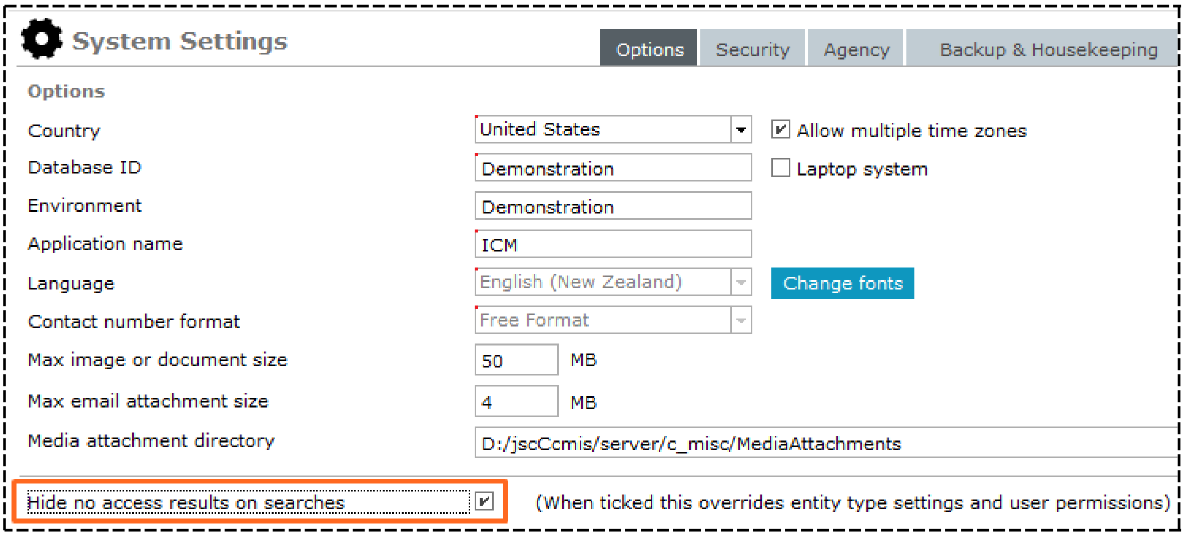


No Access Results

You can set the visibility of **No access results** at various levels:

- **User/team/designation level**
- **System level**

  When this is set, it overrides all other settings. **No access results** will never be shown.



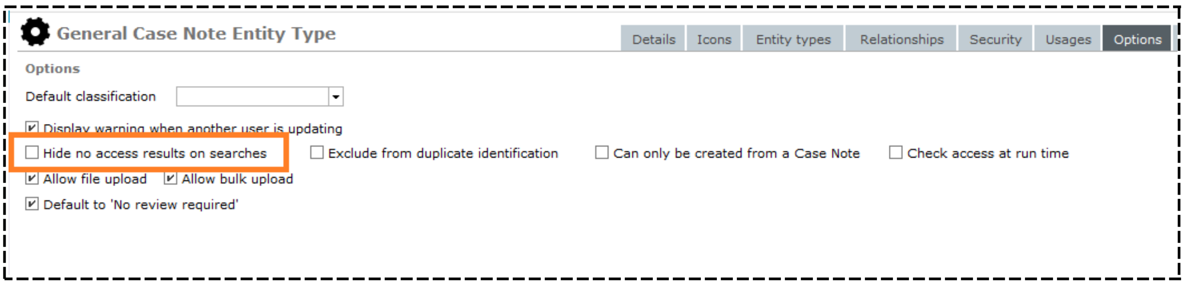
- **Entity type level**

  This is for types of:

  - Case notes
  - Incident reports
  - Information reports
  - Tasks
  - Task results

  When this is set, **No access results** won't be shown for the entity type selected.

  This overrides any setting that has been set up at the user/team/designation level.



- **User/team/designation level**

  There's a new permission called **Can see No Access Results on searches** that admin users can give to a role.

Any user/team/designation with this role will be able to see **No Access Results** on any search (unless overridden by higher-level settings).

*This is positive granting of permission to see **No access results**, not higher-level negative hiding of **No access results**.*

Select System Settings for Disclosure

1. Select **Admin** > **System** > **Settings**.
2. Select the **Disclosure** tab.
3. To make disclosure functions available on menus, select the **Disclosure Feature Enabled** checkbox.
4. To make it possible for a user to return a disclosure item from *Fully verified* to *Unverified*, select the **Unverify Enabled** checkbox.
5. To have a case note that's included for disclosure reviewed by another user before being finalised, select the **Case note review required** checkbox.
6. Enter a default warning message in the field provided.

   This message will display if a user tries to generate a marked up package that contains documents with visible redactions.

7. In the **Replacing PDFs** ... field, specify the file extensions of entities that were saved as PDF s that can be replaced with PDFs that were prepared manually.

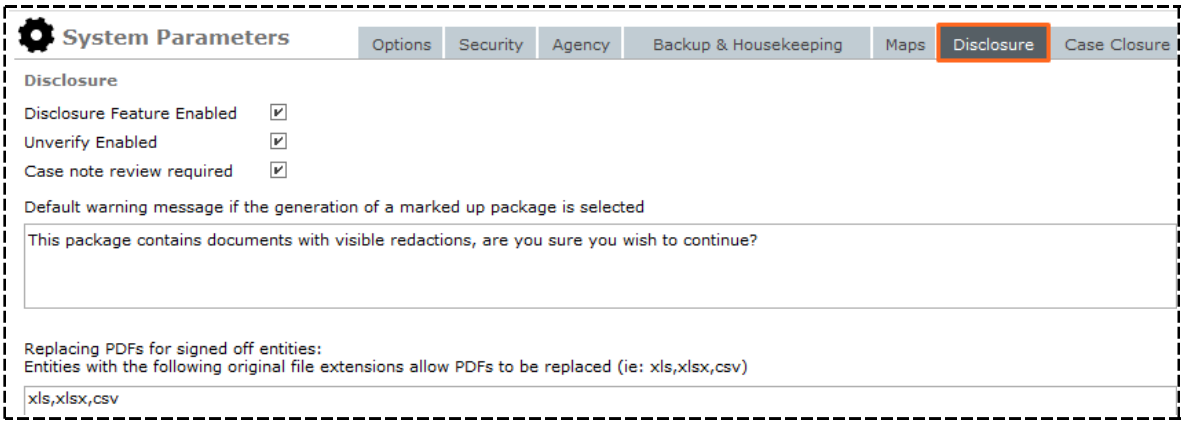
   Enter the file extensions without periods, separated by commas with no trailing comma.

   The Disclosure function converts all files that are attached to entities to PDF. This is because documents are delivered to the defence in this format.

   Some types of document files don't convert well to PDFs in the automatic process.

   To resolve this, you can replace PDFs generated from attached documents for some file types (like XLS) with PDFs you've prepared manually.

8. Select **Save**.



Entities and Attributes

For ICM to work properly, you need to set up entity types and source entities before you use them.

You can:

- Link entities to source entities.
- Choose which entities are included in source entities.
- Manage the following types of entities:
  - **System-defined** – Entities that already exist in ICM. You can only change the icon.
  - **User-defined** – Entities your agency sets up. These are based on entities that already exist in ICM.
- Create entities that:
  - Inherit details from existing entities. You can use some or all of the existing entity attributes and relationships. These entities can also have their own attributes and relationships.
  - Are independent, only have a title and description, and have their own entity attributes and relationships.

    To manage entities, you need the ***Can maintain code tables*** *permission.*

Types of Security

Entities have the following types of security:

Type of security	Details
Access	Entities and source entities have an *Access* tab. You can use this to specify who can see and edit an entity or source entity.
Attributes	**Attributes** – You can use an entity's *Attributes* tab to control who can add, edit, and delete attributes: ▪ All users ▪ Specific teams
Limited release security	**Limited release security** – In a case, the visibility of entities is controlled through the security of the case notes they're related to. This gives the following levels of security. If the user has: No access to the case note, no results are returned when they search for the case note or any related entities. Access to the case note, the case note, and any related entities are returned when the user searches for the case note or any related entities.
Limited release security	**Limited release security** – In a case, the visibility of entities is controlled through the security of the case notes they're related to. This gives the following levels of security: If the user has: ▪ No access to the case note, no results are returned when the user searches for the case note or any related entities. ▪ Access to the case note, the case note, and any related entities are returned when they search for the case note or any related entities.

Limited release provides an alternative intermediate level of security. If the user has no access to the case note, when they search for an entity, they can see only that it's related to a case and the name of the case officer. No other information is available.

When you add an entity as a case officer, you can make it visible to other users without divulging all the information about that entity. You can do this by making the entity a limited release entity – When you edit an entity type, select the **Limited Release** checkbox to have more information provided, at your discretion.

Setting up Entities

Before you can use ICM, you need to set up your:

- Information sources (for example, tables and templates)
- Background apps
- Security

You'll also need to specify the rules that apply to your agency.

Before you can set up ICM, we recommend you consider:

- How you're going to use it.
- Your security needs.
- What information you want to record.
- How you're going to record it in relation to your business processes.
- The structure of your agency, its relationship with any other agencies, and what information you're willing to share with external agencies.

To specify the entities your agency uses:

1. Identify system entities, for example cases and incident reports
2. Identify entities, for example people and addresses
3. Identify and specify how entities are related
4. Identify and specify the attributes of entities (how entities are described)
5. Define the roles and permissions associated with the entities

Entities in ICM

Entities in ICM are high-level source objects that intelligence is derived from.

You can use them to record all activity about an investigation.

Types of Entities in ICM

ICM has the following types of entities:

- Cases
- Case notes
- Disclosure index
- Dissemination index
- Incident reports
- Information reports
- Tasks
- Task results

You can set up entities to suit your agency:

- If you have a large agency, you might want to set up lots of entities for each type of entity.

  For example, you might need lots of different cases and incident reports.
- If you have a small agency, you might only need one entity for each type of entity.

Source Entities your Agency Can Use

You can set up the following source entities in ICM to suit your agency:

- Case
- Case Note
- Disclosure Index
- Dissemination Index
- Incident Report
- Information Report
- Tasks and Task Results

Make sure you identify the source entities your agency needs before you set them up in ICM.

Once you create a type of source entity, you can't change the type. For example, you can't change an intelligence project case to an investigation.

Identifying Entities

Entities represent the real-life objects that are relevant and interesting to an investigation. These objects are the primary constituents of your intelligence holdings and are immediately made available to all users (subject to security).

The following entities are already set up:

- Contact numbers
- Documents
- Events
- Images
- Locations
- Media
- Offence
- Organisations
- Persons
- Transactions
- Vehicles

Files (for example, documents, images, audio, and visual files) that are attached to the media entity are stored in the ***MediaAttachments*** *folder.*

Files in this folder aren't indexed. If you attach your documents to the Media entity, they're not included in any searches. To make sure a document is indexed (searchable), upload it as Document entity.

Identifying the Types of Document Entities You Need

You need to identify whether operational documents need to be uploaded under document subtypes or whether one type of document entity is enough.

*You'll need to select a high-level category for document subtypes, for example **Operational Documents**.*

You can create a new miscellaneous entity for each document subtype. The miscellaneous entity inherits the high-level design features of the document entity (title, description, browse, and upload capability).

This approach has the following benefits:

- Each document subtype has a separate **Document-Type** search screen.

  If you don't specify document subtypes, you must use the generic Document Search screen. The attribute parameter for document type must be specified as part of the search criteria.

- A separate tree structure is created for each document subtype. Individual documents of that subtype are listed under this. The tree structure is used in the Navigator and on each **Search to Add** entity screen.

  This is often useful because it's the same as having a separate, defined directory for each document subtype. This is instead of one document directory that lists all documents regardless of subtype.

- You can define different attributes for each document subtype.

  This means you don't have to use conditional attributes on the document entity to cater for different document subtypes.

- You can specify an icon to represent each document subtype.

  This makes the document subtype easier to see in a diagram and other screens in ICM.

We recommend you deactivate the predefined document entity. This will prevent you from accidentally selecting and creating a document entity instead of the specified document subtype.

Once you create a document based on a subtype, you can't change that subtype.

You'll need to delete the document and then recreate it as the correct subtype. For example, you can't change a correspondence document to a statement document.

The alternative to creating separate miscellaneous entities for each document subtype is to set up an attribute for the predefined document and select the document subtype from it.

For example, you can set up the Type attribute for the document entity. The code list for the Type attribute field could include the Correspondence, Statement, Legal Document, Plan, and General Miscellaneous document types.

This setup could be enough for your agency. But the benefits described in the previous list don't apply.

Identify Any Other Miscellaneous Entities You Need

You must nominate an entity type category for any new miscellaneous entities you define. Your agency can use the **Other Entities** general category that contains all new entities. Alternatively, you can define a specific category for each new miscellaneous entity.

When you create a new miscellaneous entity, consider whether that entity should inherit the intrinsic hard-coded design fields of any other entity. If you don't specify any inheritance, the design of the screen for the new entity includes two free-text data entry fields (title and description) only.

If you do specify inheritance, the design of the screen for the new entity is the same as that of the parent entity.

For example, if you create the marine vessel and aircraft miscellaneous entities from the predefined Vehicle entity (using inheritance), the screens for the new entities include the same fields as those of the parent vehicle entity (description, registration, country, and state).

The following table lists the hard-coded fields for the pre-defined entities and the miscellaneous entity.

Entity type (attributes)	**Default fields**
Contact number	Number
Document	Description Embedded Document
Event	Description Finish Date Finish Time Start Date Start Time
Image	Description Embedded Document

Location	Building Name City Country Latitude Longitude Number Postcode State Street Suburb Unit Number
Media	Description Media List screen
Miscellaneous	Title Description
Offence	Description Offence Count Offence Act Offence Code Started Date Started Time Finished Date Finished Time
Organisation	Name Country State

Person	Family name Given name 1 Given name 2 Given name 3 Title Gender Date of Birth Age (auto calculated) Date of Death
Transaction	Description Unknown Value Value When Date When Time
Vehicle	Country Description Registration State

The fields in the previous table are called hard attributes. You can't change these fields. Your agency can set up additional fields (attributes) for all entities.

Your agency is responsible for setting up the entities you'll use. You can set up new entities at any time.

The **Inheritance** column provides an indication of whether the miscellaneous entity type inherits the field design of a predefined entity type.

Creating Person Subtypes as Miscellaneous Entities

Your agency can create additional miscellaneous entities that represent subtypes of the person entity. This is useful if there are one or two distinct categories of person types associated with the primary business process.

For example, in a witness protection agency, there are two categories of Person entity. The primary person type is the witness. There are other people associated with the witness or the investigation in different ways.

In a victim support agency, there are several categories of Person entity. For example, victims, support workers assigned to those victims, and other people associated with the victim or the investigation.

By creating person subtypes as miscellaneous entities, the person subtype itself (for example, witness, victim, or support worker) essentially specifies the nature of the involvement (relationship) of the individual in an incident or investigation.

You need to carefully consider how you set up miscellaneous person subtype entities. Over time, your agency could create several different records for one person who has been identified through recidivist behaviour or by association with several investigations and incidents.

For example, the person could be a perpetrator, witness, and an alleged offender in one or more incidents and investigations.

If you don't link (associate) the relevant records, vital intelligence information could be disregarded.

After you create a person record of a specific subtype, you can't change the subtype. You must delete the person record and then recreate it as the correct subtype.

For example, you can't change a witness record to an offender record.

You can only merge person entities that are the same subtype.

*For details about merging records, see **Matching and merging duplicated entities**.*

To see all records about a specific individual, search for each person subtype.

Duplicate records of any type could exist in ICM as a consequence of enforcing security and access restrictions.

Identify and Define Attributes

ICM uses several standard, system-defined data entry fields. These are called hard attributes. You can use them to record information for entities and system entities.

These fields are available on the Details screen of all entities and source entities. You can't change or reconfigure these fields. They are generic enough to enable your agency to undertake an investigative or intelligence-based process. You can use them to record information.

The following table lists the mandatory system-defined attributes for **Case** and **Incident Report** entity types.

Entity type	Attribute name
Case	Case officer
	Title
	Description
Incident report	Title
	Description
	When reported date
	When reported time
	When happened date

You can set up additional data entry fields to capture information that's relevant to your business processes. These additional data entry fields are called attributes or soft attributes.

When ICM is first installed, no attributes are set up. You can set these up.

Your agency can set up attributes for entities and system entities:

- Attributes set up for system entities are usually needed to satisfy workflow query and your agency's reporting needs.
- Attributes set up for entities provide a way to give a more efficient way to identify entities of interest.

Defining Attributes

Identifying and setting up agency-specific attributes for entities isn't mandatory. The default ICM data entry fields might be enough for your agency.

If you need more attributes, we recommend your agency identifies these and sets them up before more people in your agency start using ICM.

Setting up an attribute involves:

1. Selecting the attribute category and title.
2. Specifying the type of value to record for that attribute.
3. Specifying the behaviour of the attribute – For example, whether users must specify a value for it.
4. Selecting additional settings – For example, whether comments can be recorded for the attribute (as well as a value).
5. Conditional specifications – For example, whether an attribute depends on the value of another attribute.

Selecting an Attribute Category

You can use these attribute categories:

- Header
- Attribute Name
- Group Parent

  *There's an additional attribute category called **Attribute Type**.*

  We don't recommend you use this category when setting up a new installation of ICM.

  This category exists only for backwards compatibility with previous versions of ICM.

Specify the Type of Attribute Value

When you set up **Attribute Name** type attributes, you must also specify the type of value for the attribute.

The following table lists the types of attribute values you can use.

Value type	Attribute value requirements
Free-text	Enter as free text unless the URL attribute for this field is specified. If that's the case, the field value will be treated as a URL. If the field has been defined as a URL, it will display as a link. You will be able to press **Ctrl**+click to open it.
Code table	A code that's selected from a list of values defined by your agency
Numeric	Numbers only, no text
Date	A date
Time	A time
Mask	In a specified format
User Id	Selected from a list of team codes defined by your agency
Calculated	Calculated using a specified equation

You don't need to specify a type of attribute value for attributes that are header or group parent categories. This is because they don't represent data entry fields.

You can't change types of attribute values after entities have been created that use that attribute. If an error has happened, you must delete that attribute and recreate it. This will affect any entity that uses that attribute.

Most types of attribute values are self-explanatory. But you'll need to think about how you want to use code tables, masks, and calculated attribute values.

Specifying Attribute Behaviour

For all the Attribute Name attribute types you set up, you'll also need to specify the behaviour for that attribute.

Here are some types of attribute behaviour:

- **History** – A history of changes are recorded for the attribute.

  Previous values and the current value are shown.
- **Mandatory** – You must specify a value for the attribute.
- **Multiple** – You can select multiple values for the attribute.

Managing Types of Entities

You can create and manage different types of entities.

*The **Property Report** and **Property Item** entity types only display if you have the Property Management licence.*

*The **Brief** entity type only displays if you have the **Brief** licence.*

To expand an entity type category, select the Expand + icon beside it.

You can still manage the attributes of entities that aren't selected.

To reorder entity types and categories, use the Move up icon or Move down icon.

You can set up entity types under the categories listed. You can also create additional miscellaneous entity types.

Before you set up entity types for your agency, we recommend you spend time planning which entity types you need and how they're related.

Consider the following entity types carefully:

- The **Offence** entity type needs someone in your agency to manage the **Offence Acts** code tables and the associated **Offence** codes. You'll also need to create the relationship between the **Person** and **Offence** entity types.

  Some agencies use a case note (with the type of **Offence**) to record offence details. This enables you to capture information in a less structured way. But it doesn't remove the need to manage **Offence** codes.

- Files (for example, documents, images, and audiovisual files) that are attached to the Media entity are stored in the **MediaAttachments** folder on the server.

No files in the MediaAttachments folder are indexed. If you attach your documents to the Media entity, they're not included in any searches. To make sure your documents are searchable, upload them as a **Document** entity.

Your agency is responsible for setting up entity types. You can do this any time. But once you've created a particular kind of entity, you can't change that entity type to another entity type.

For example, once you create an **Intelligence Project** case, you can't change it to an investigation.

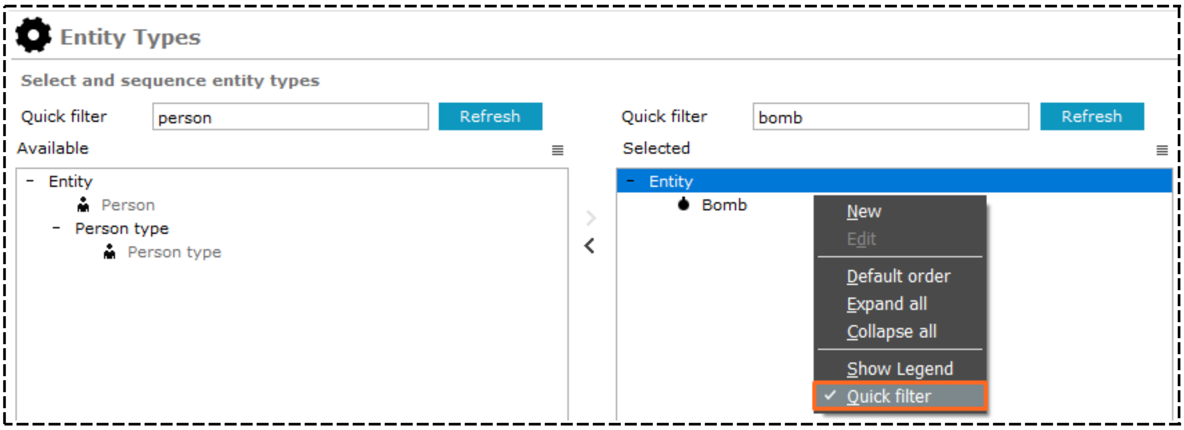
You can use entity type categories to group related entity types under one heading. For example, you can create an entity type category called **Animal**.

Quickly Find Entity Types

When you set up entity types you can use the quick filter to find the type of entity you're looking for.

Use either of these methods to access this feature:

- Press **Ctrl**+**F** or right-click in the *Available* or *Selected* area.
- Select **Quick Filter**.

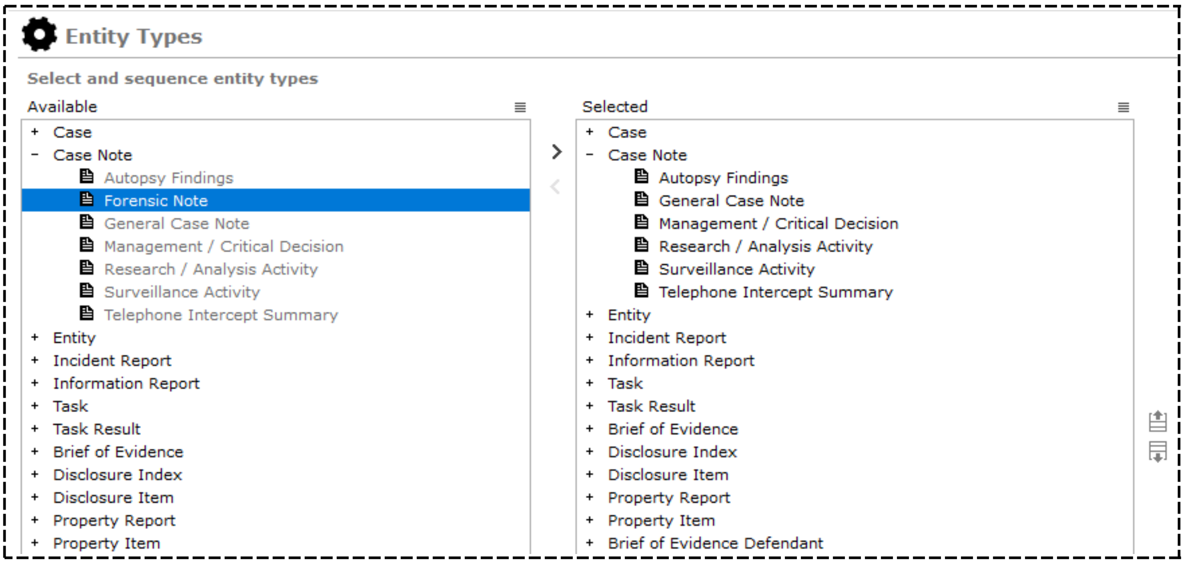


Specify Types of Entities for Your Agency

1. Select **Admin** > **Entity Definition** > **Types**.
2. To make an entity type available:
   a. In the **Available** area, select the entity type.
   b. Double-click it or use the Select icon.
3. To reorder entity types or categories:
   a. In the **Selected** area, select the entity type or category you want to move.
   b. Use the Move up icon or Move down icon to change the position.

      *To reset the order to the default, select the Options ≡ icon > Select **Default Order**.*
4. Select **Save**.

   The **Relationship** and **Usage** tabs are now available for types of source entities.

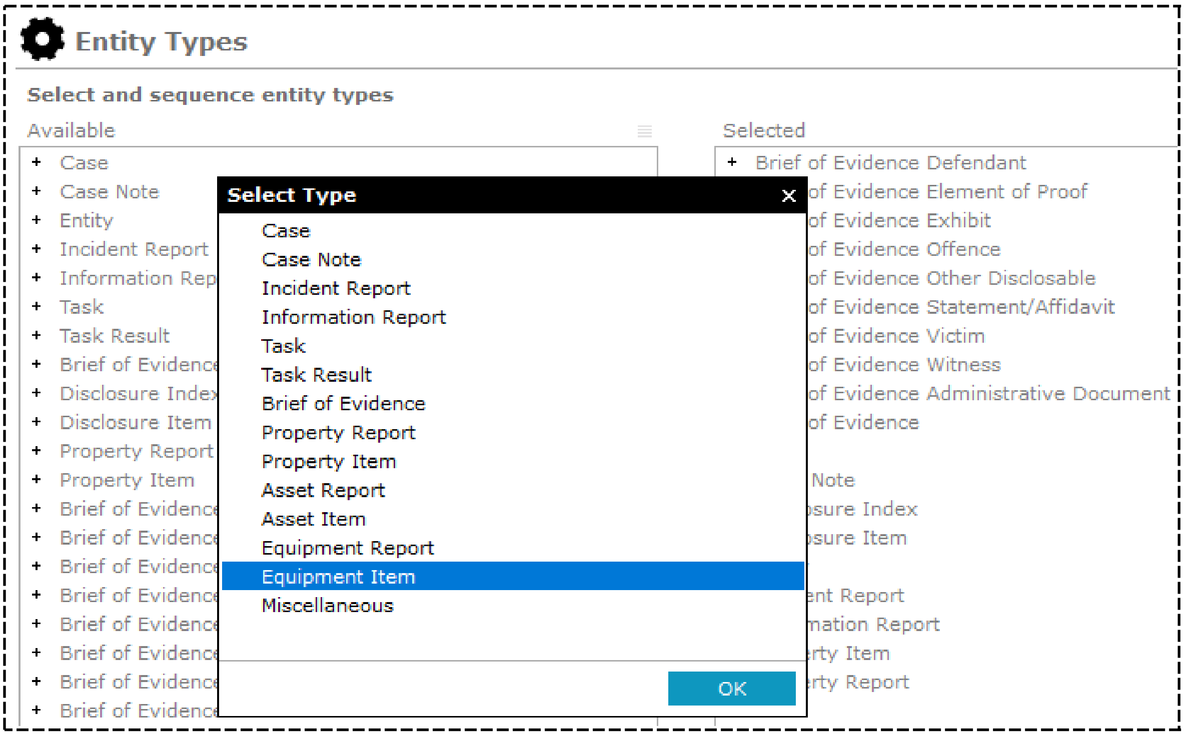


Create a New Type of Entity

When you create a new type of entity, you'll need to specify whether it's a source entity or a miscellaneous entity type:

1. Select **Admin** > **Entity Definition** > **Types**.
2. Select **New**.
3. Select the type of entity you want to create > Select **OK**.

   If you want to create a type of entity that isn't a source entity or a task, select ***Miscellaneous****.*
4. Set up the entity type as required.



Create a Compound Media Type of Entity

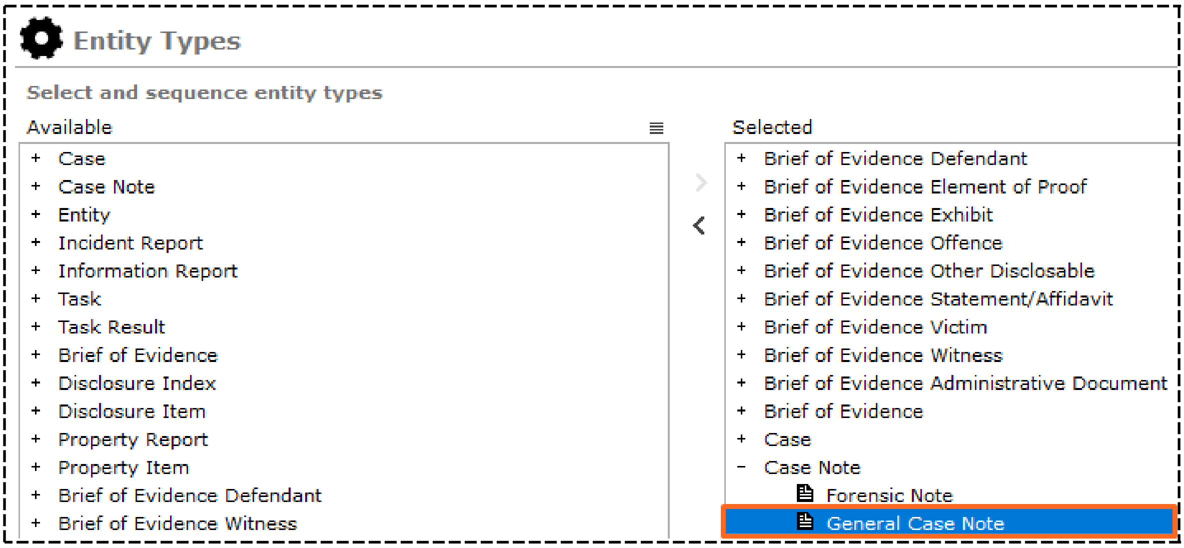
When you set up media entities that are part of the **Media Files** category, you can specify what types of media files are associated with the media entity type you're defining.

For example, you could have an **Interview audio files** entity type specified which inherits from the **Media** entity type and only allows audio file types to be attached to it.

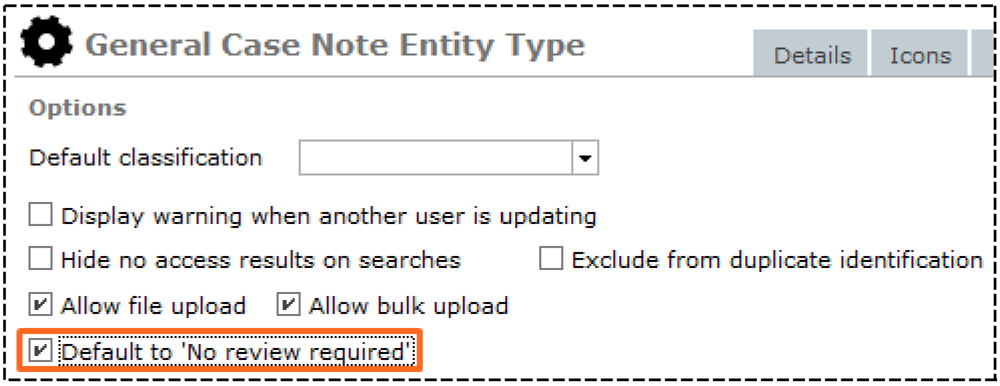
Default Setting for Case Note Reviews

You can have case notes default to *No review required*:

1. Select **Admin** > **Entity Definition** > **Types**.
2. Select the **General Case Note** entity type in the **Selected** field.



3. Select **Edit**.
4. Select the **Options** tab.
5. Select the **Default to 'No review required'** checkbox.



This setting will automatically be applied when a user creates a case note.

Change an Icon for an Entity

If you don't want to use the default icons for entities, you can upload your own ones:

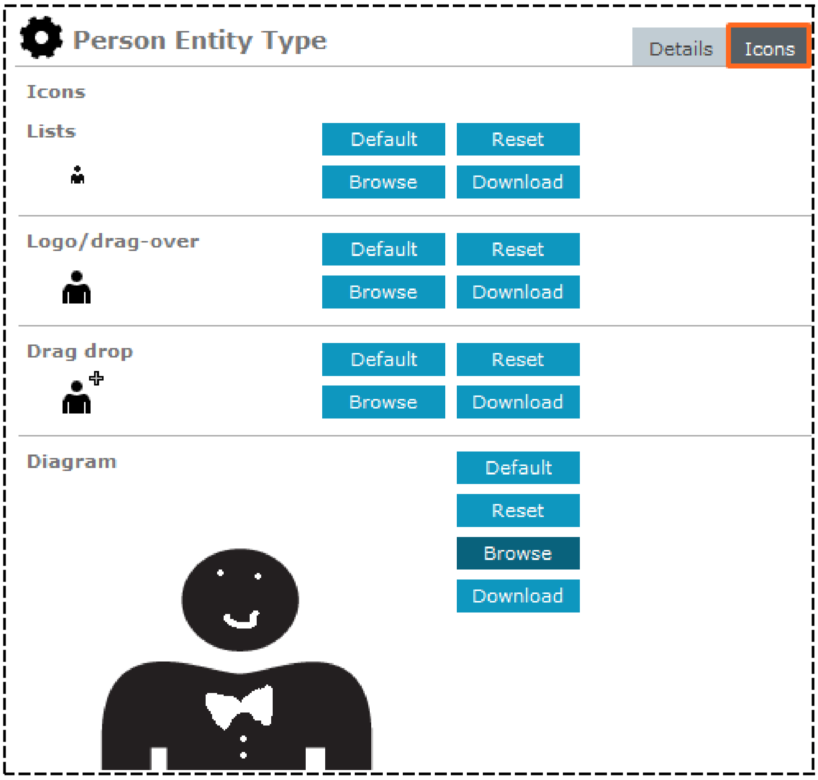
1. Select **Admin** > **Entity Definition** > **Types**.
2. Expand **Entity** in the *Selected* area.
3. Double-click **Person**.
4. Select the **Icons** tab.
5. In each area, use the following buttons to specify the icons you want:
   - **Browse** to find the icon you want.

     While this screen is open, if you've previously selected an icon for an entity, that folder is opened by default.

     When you select the required icon, select **Open**.

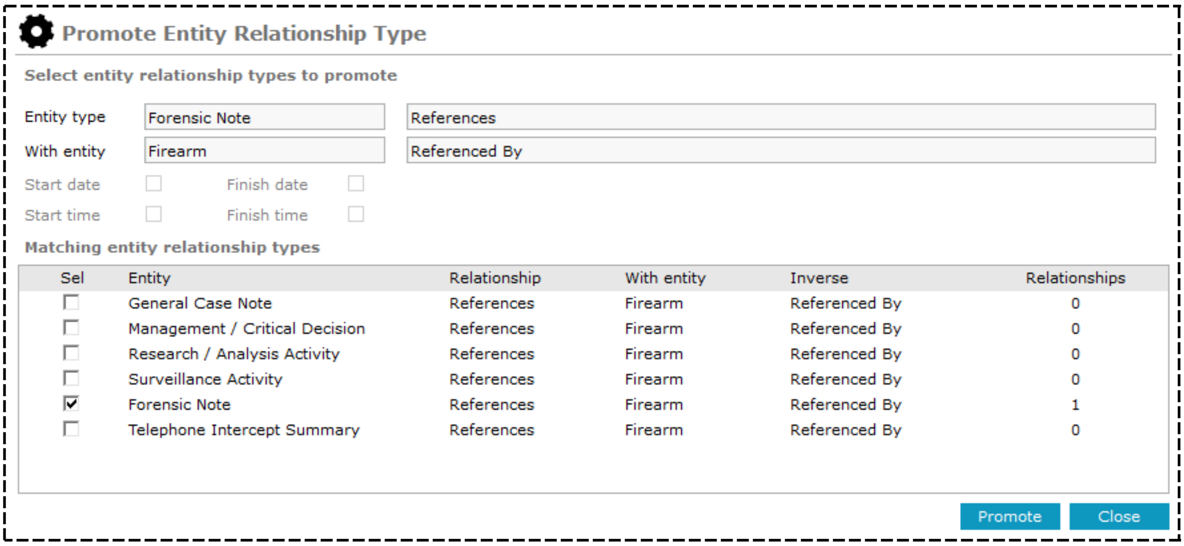
     The type of logo you're setting up determines the type of file you can select.
   - **Reset** to restore the icon to the last saved icon before you made any changes.
   - **Default** to restore the default icon for the entity.
   - **Download** to save the icon file to a specified location.

     You can edit the icon to suit your needs and select **Browse** to upload it.
6. Select **Save**.



Make a Relationship Global

1. Select the relationship you want to make global.
2. Select **Promote**.
3. Select the checkboxes beside the types of entity relationships you want to promote.
4. Select **Promote**.



Edit Entity Relationships

The Entity Relationship Type Maintenance screen (obtained via the **Admin** > **Entity Definition** > **Relationships**) allows you to edit the relationship between entities.

You need the **Can maintain entity relationships** permission to manage entity relationships.

See Security.

To manage entity relationships:

1. Select **Admin** > **Entity definition** > **Relationships**.
2. Use the Entity Relationship Type Maintenance screen to view, edit, set up, or delete a relationship.

   *For details about managing entity relationships, see **Defining Entity Relationships**.*

Import Entity Relationships

When you import entity relationships, make sure the:

- Entity type names exactly match those in the target system.
- File is tab-delimited.
- Entity Type Identifiers are in capital letters
- Relationships between content source documents and subentities must have their **StartDate**, **FinishDate**, **StartTime**, and **FinishTime** set to FALSE or empty.

  This is because these values aren't required.

  Duplicate relationship types won't be created.

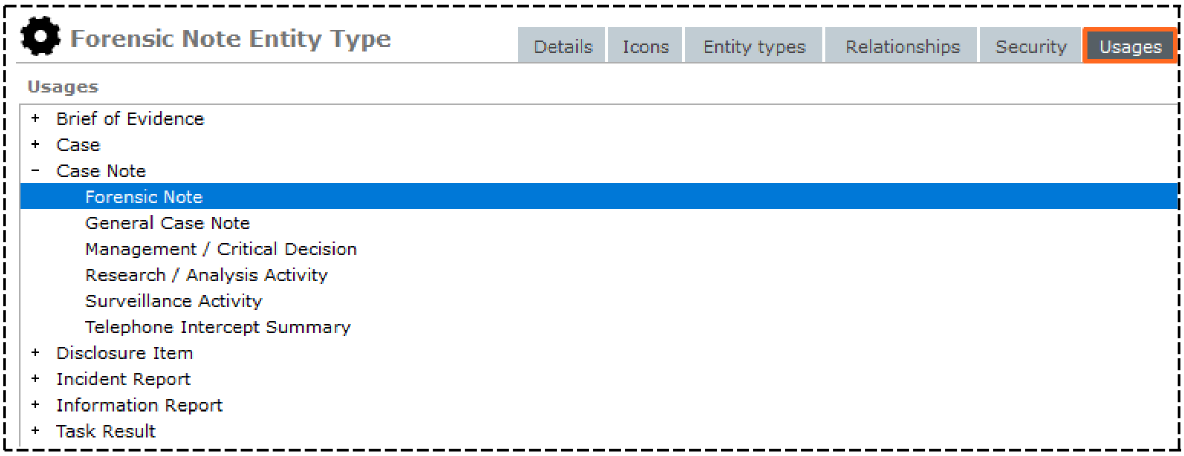
  *To import bulk relationship types, you need the **Can maintain entity relationships** permission.*

Import Bulk Relationship Types

1. Select **Admin** > **Entity Definition** > **Relationships**.
2. Select the Overflow >> tab > Select **File Import**.
3. Select the Browse ... button to find and select the file you want to import.

See Which Source Entities Use a Type of Entity

1. Select **Admin** > **Entity Definition** > **Types**.
2. Open a source entity.
3. Select the **Usages** tab.



Specifying Retention Criteria for an Entity

Source Entities and Entities can set up by your administrator to have Retention Criteria associated with them. The Retention criteria screen allows you to manage the review, retention, and permanent removal of data at specific elapsed times.

Many agencies have a strict data retention policy. Some data may require deletion due to data protection while other data must be kept to comply with local legislation.

When data is expunged from the system permanently. This includes any reference to that item, including the audit log entry from when the data was created or edited.

Specifying Unique Attributes for a Type of Entity

The Uniqueness screen allows you to define the attributes of an entity type that are used to check for potential duplicate entries when adding a new entity to a source entity.

For example, you can define that the Family name, Given name 1, and Citizenship Details attributes of a person entity type are unique.

When a user adds a new person to a source entity, using the Person Maintenance screen, ICM checks whether the family-name, given-name 1, and citizenship details entered match those of existing people in the system.

Define the Uniqueness of a Type of Entity

1. On your open source entity type maintenance screen, select the Overflow >> tab > Select the Uniqueness command from the list that displays.

   An example of the Uniqueness screen, for the Person Entity Type maintenance screen, is shown here.

   The Hard attributes area lists the hard attributes that are available for selection (you can't change hard-coded attributes).

   The Soft attributes area lists the attributes you have defined for the entity type, using the Entity Attributes screen (under **Admin** > **Entity Definition** > **Attributes**).

   The Uniqueness area lists the order in which the attributes are checked for potential duplicates.

2. To include an attribute in the Uniqueness area:

   a. In the Hard attributes area, or the Soft attributes area, select the required attribute.

   b. Select the > button or double-click the attribute.

      The selected attribute displays in the Uniqueness area.

      You can't define a soft attribute as unique if it has the MULTIPLE option enabled, on the Entity Attributes screen.

3. To exclude an attribute from the Uniqueness area:

   a. Select the attribute you want to exclude.

   b. Select the < button or double-click the attribute.

   c. The selected attribute displays in the Hard attributes area, or the Soft attributes area, as appropriate.

4. To change the order of the attributes in the Uniqueness area:

   a. Select the attribute you want to move.

   b. Select the Move up button, to move the selected attribute up one position, or select the Move down button, to move the selected attribute down one position.

5. To make all hard attributes mandatory, check the Make all hard attributes used for Uniqueness mandatory checkbox.

6. Select **Save**.

Select Options for Users Entering Information

The Options screen for Case Note, Incident Report, Information Report, and Task Result entity types allows you to specify the behaviour options that are available to users when entering information.

To specify options for source entities (other than a case):

1. Select the Overflow >> tab > Select **Options**.

   The options available depend on the entity type.

   A task entity type will have default review options as shown above while case note entity type will have file upload options.

2. Select a default classification in the Default classification drop-down, to apply a classification to all entities of that type.

3. To hide the entity from a user's search results if the user doesn't have access to the entity, check the Hide no access results on searches checkbox.

4. If you're managing a source entity type and want to exclude it from the duplicate identification process, check the Exclude from duplicate identification checkbox.

   - The **Exclude from duplicate identification** setting can only be placed on source entity types.

     It determines whether any tangible entities that will be contained within these source entities will be subject to the process of identifying duplicate tangible entities in the system.

     A "duplicate" is a tangible entity which has exactly the same attributes as another tangible entity and probably refers to the same real world item (for example, Person, Vehicle).

   - Adding a potential duplicate won't result in a warning if a user is adding a tangible entity with the same unique values as one already contained in the system.

     The system allows the user to add the duplicate instead of warning them of a potential duplicate.

   - Once the **Exclude from duplicate identification** is selected, you must restart the DbServer before it takes effect.

   - Once the option is selected, it can't be reversed.

5. If you're managing a Case Note entity type, check the Can only be created from a Case Note checkbox to specify that the entity type can be created only within the context of a case.

6. If you want a task type entity to always be authorised before being sent, then select the Requires Authorisation checkbox.

7. In some areas of the application entity types are displayed to the user you may not want to display because the user doesn't have access to any entities of that type.

   For instance, the Lines of Enquiry and Phases tabs display all entity types that are associated with the case but would not display any entity itself unless the user has access to that entity.

   But even showing that a particular entity type is used by the case might breach security.

For example, you might not want to display an entity type of "Covert Operation Note" unless the user has access to entities of this type already.

To prevent display of entity types, unless the user has access to some entities of this type then select the Check access at run time checkbox.

8. Check the Allow file upload checkbox, to allow text files to be uploaded to this source entity type.
9. Check the Allow bulk upload checkbox, to allow document and image entities to be uploaded to this source entity type.
10. Check the Allow direct document checkbox, to allow Word documents to be directly attached to Incident Report and Information Report document types.
11. Select **Save**.

Associating Permissions with Roles for Types of Entities

Use the Roles screen to associate the permissions that are dynamically-created for cases, information reports, and incident reports with specified roles.

For example, you can restrict the creation of a specified information report to users with the specified roles.

Permissions for new Information Reports and Incident Reports entity types are automatically created when they're saved.

No users have access to these new reports until the relevant permissions are assigned to roles.

Associate a Permission for an Information or Incident Report

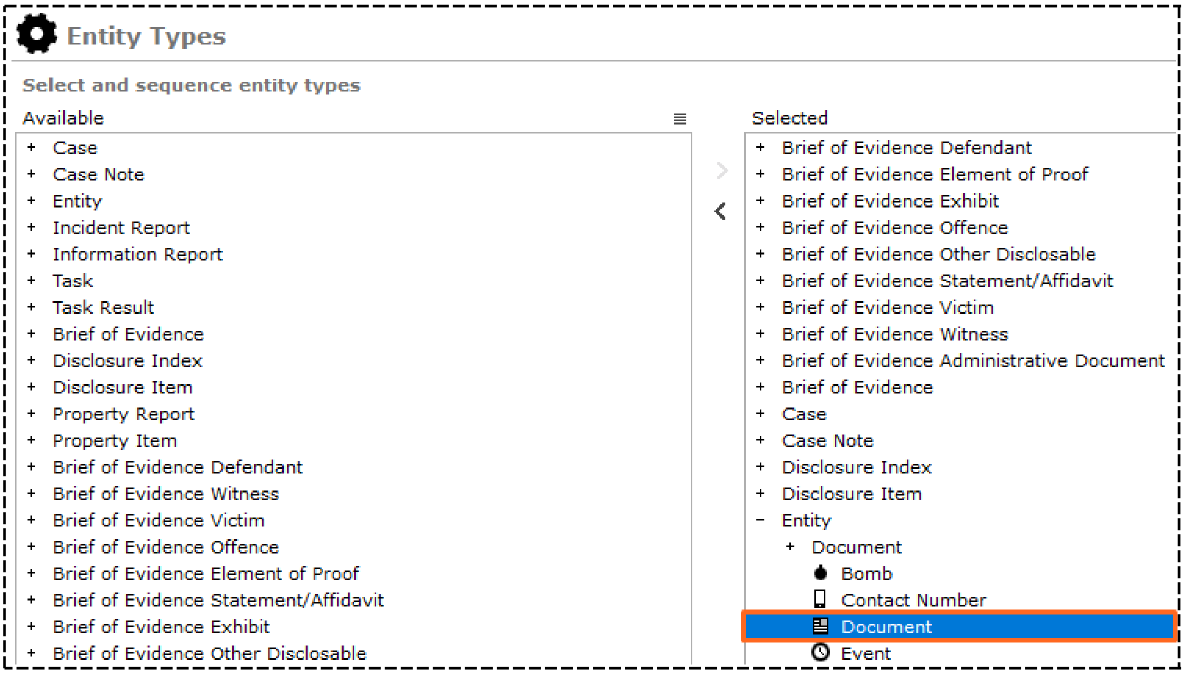
1. Select the Overflow >> tab > Select the **Roles** command.
2. In the Permission drop-down, select the permission you want to associate with a specific role.
3. To specify the roles that have the selected permissions:
    a. In the *Available* area, select the role you want to associate with the permission.
    b. Double-click the role or select the > button.

       The selected role displays in the Selected area.
4. To remove a role from a permission:
    a. In the Selected area, select the role you no longer want to associate with the permission.
    b. Double-click the role or select the < button.

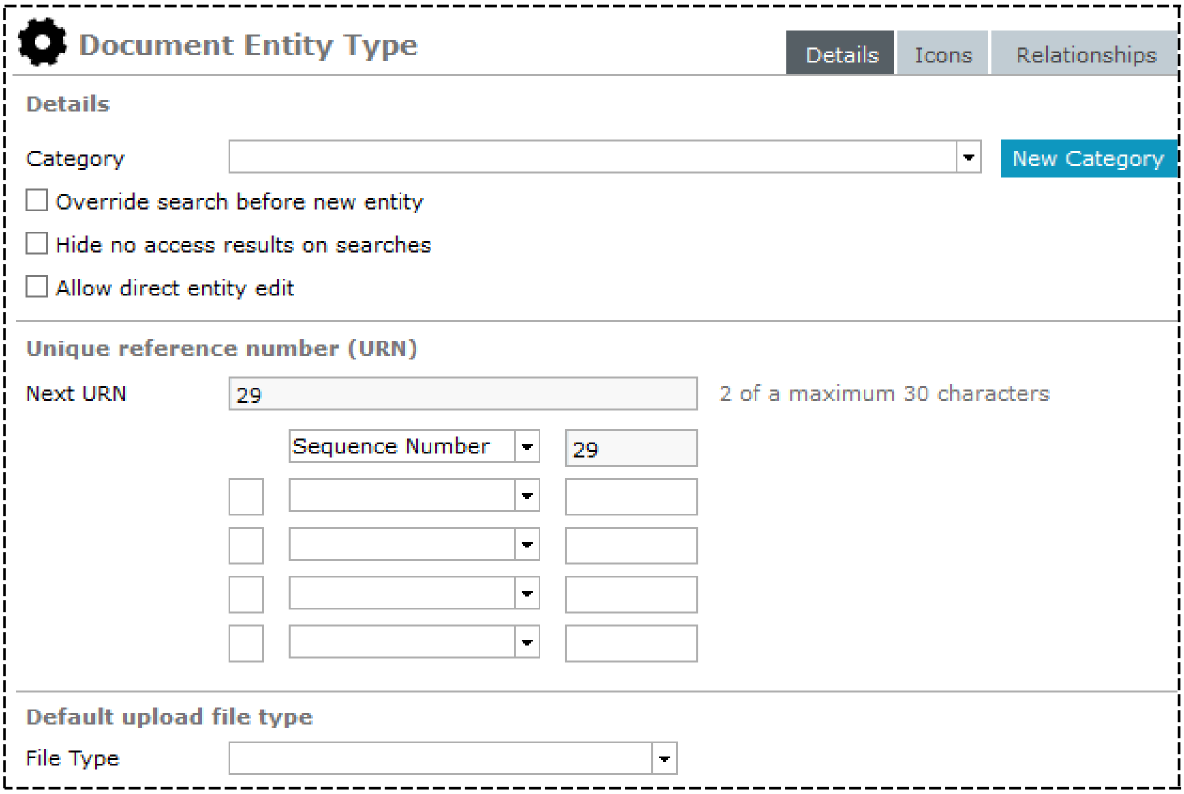
       The selected role displays in the Available area.
5. Select **Save**.

Edit a Type of Entity

1. Select **Admin** > **Entity Definition** > **Types**.
2. In the *Selected* area, select the entity type you want to edit.
3. Select **Edit** or double-click the selected entity type.



4. Edit the required details.
5. Save your changes.


Document Entity Type
Details
Icons
Relationships
Details
Category
New Category
Override search before new entity
Hide no access results on searches
Allow direct entity edit
Unique reference number (URN)
Next URN
29
2 of a maximum 30 characters
Sequence Number
29
Default upload file type
File Type

Set up a Unique Reference Number

If you're creating or editing a type of entity, you can specify the type of Unique Reference Number (URN) that's created.

For example, you can create a URN using text, year, and sequence number options, in any order you choose.

To set up a URN:

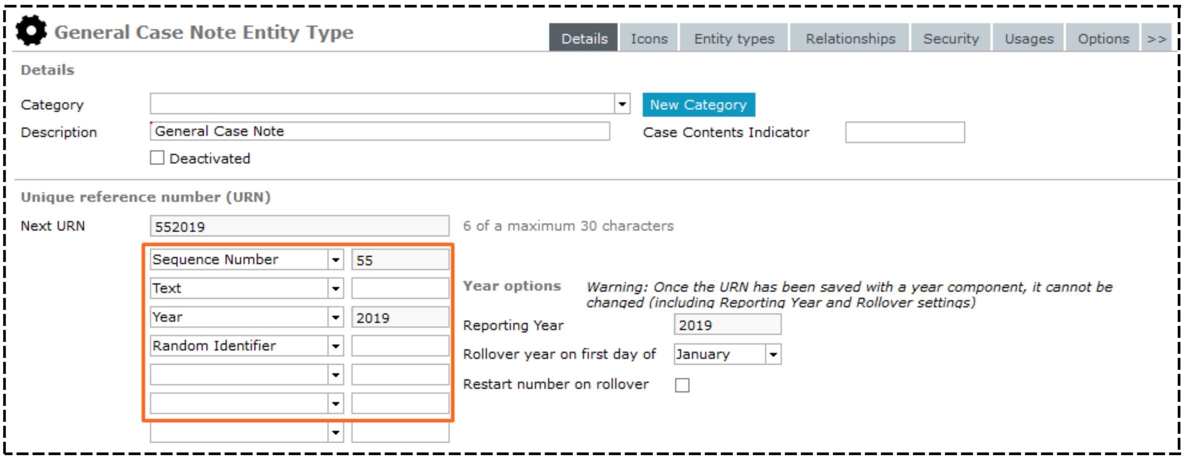
1. Open the type of entity you want to edit.

   *The **Next URN** field shows the default URN for this type of entity.*

2. Use the drop-downs under the **Next URN** field to select more parameters for the URN:

   - **Text**
   - **Sequence Number**
   - **Random Identifier**

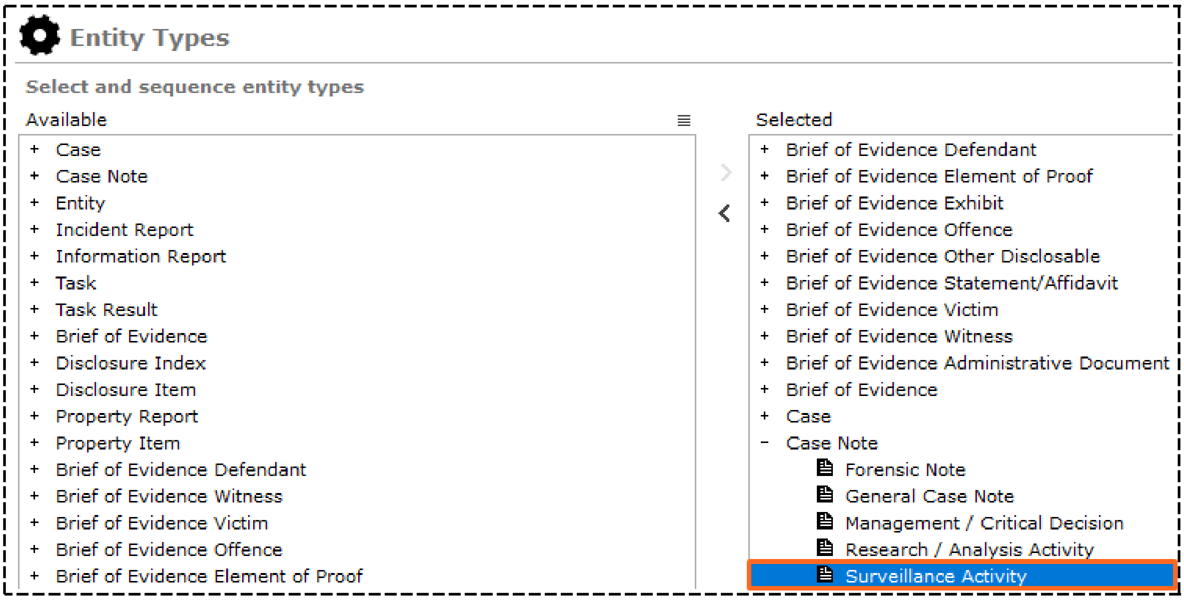
     Year



Deactivate a Type of Entity

You can't delete an entity type but you can deactivate it. This will let you keep the entity type for reporting purposes. Users won't be able to select the entity type but they will be able to report on it:

1. Select the **Admin** > **Entity Definition** > **Types**.
2. In the *Selected* area, select the entity type you want to deactivate.



3. Select **Edit** or double-click the entity type.
4. Make sure the **Details** tab is selected.
5. Select the **Deactivated** checkbox.

6. Save your changes.

Importing and Exporting Types of Entities

Importing and exporting entity types allows you to:

- Load entity types that have been exported from another ICM database into your ICM database.
- Export entity types from your ICM database to a file that you can import into another ICM database.

The files are exported and imported in XML format.

Data Access Whitelist

In ICM release 6.0.2 we introduced Permanent Access. This is high level data access you can give to users, teams, and designations for:

- Information reports
- Incident reports
- Case notes

You can also use the permanent access feature to block users, teams, and designations from these types of source entities.

In release 6.1 we address the need to block access to all users, teams, and designations except those on a whitelist.

You can make the Permanent Access list a whitelist.

For an agency, this means when you create new teams, users, or designations you don't have to block new teams and users from these source entities.

Grant Permanent Access for an Entity

1. Select **Admin** > **Entity Definition** > **Types**.
2. Open the type of information report, incident report, or case note you want to edit.
3. Select the **Security** tab.
4. Select the designations, teams, and users that should have permanent access to this type of entity.
5. Select **White List**.
6. Select **Save**.

Manage Categories for Types of Entities

You can use categories for your entity types to group similar entity types into one group.

For example, you can have an entity category (like Aircraft) and then define specific entity types within that category (for example, light plane or microlight). You can also specify relationships of entity categories with other entity categories and types.

The **Details** tab of the screen for all entity types shows the category. The category is optional for all types except user-defined (miscellaneous) types.

Manage Categories of Entity Types

1. Select the **Admin** > **Entity Definition** > **Types**.

   The Entity types screen shows the entity types that belong to the selected entity type category.

   To add an entity type to the entity type category, use the **Entity Types** maintenance screen.

   You can use the *Relationships* screen to view or edit relationships between the entity type category and other entity type categories and entity types.

2. To define a new entity type category:

   a. Select **New**.

   b. In the *Description* field, enter a description of the entity type category.

   c. In the *Category Type* drop-down, select the entity type you want to create.

      This drop-down allows you to group any types into user-defined categories.

      You can filter the display for a specific type of category or show all types of categories.

   d. To keep the entity type category for reporting purposes only, select the **Deactivated** checkbox.

      If you select this checkbox, the entity type category is deactivated but not deleted.

      Users can't select the entity type category but can report on that category.

   e. Select **Save**.

3. To add an entity type relationship:

   a. In the table at the top of the screen, select the entity type category you want to edit.

   b. Select the **Relationships** tab.

   c. Select **Add**.

4. To delete an entity type category:

   a. In the table at the top of the screen, select the entity type category you want to delete.

   b. Select **Delete**.

Edit Relationships Between Types of Entities and Their Categories

1. Select **Admin** > **Entity Definition** > **Categories**.
2. Select the entity type category whose relationships you want to view or edit.
3. Select the **Relationships** tab.
4. To define a new relationship:
   a. Select **Add**.

      The **Entity** drop-down shows the type of entity you're defining a new relationship for.

   b. In the **Relationship** field, enter the relationship.
   c. In the **With entity** drop-down, select the entity that the first entity is inversely related to.
   d. In the **Inverse** field, describe the inverse relationship.

      Relationship types must make sense when read in both directions.

      A way to check this is to say the relationship and its inverse out loud.

      For example, a person resides at a location and a location is a residence of a person.

      Don't add a relationship that doesn't make sense in both directions.

      Some relationships are the same in both directions, for example ***Also known as****.*

   e. If a start date is applicable, select the **Start date** checkbox.
   f. If a finish date is applicable, select the **Finish date** checkbox.
   g. If the relationship type is no longer active, select the **Deactivated** checkbox.
   h. Select **OK**.
5. To update a relationship:
   a. Select the relationship.
   b. Select **Update**.
   c. Make your changes.
   d. Save your entries.
6. Select **Save**.

Manage Entity Attributes

You can specify the values types and behaviour for attributes of selected entity types.

For example, for a Person entity type, you can define the following attributes about physical appearance:

- Hair colour
- Hair length
- Type of facial hair
- Height
- Eye colour

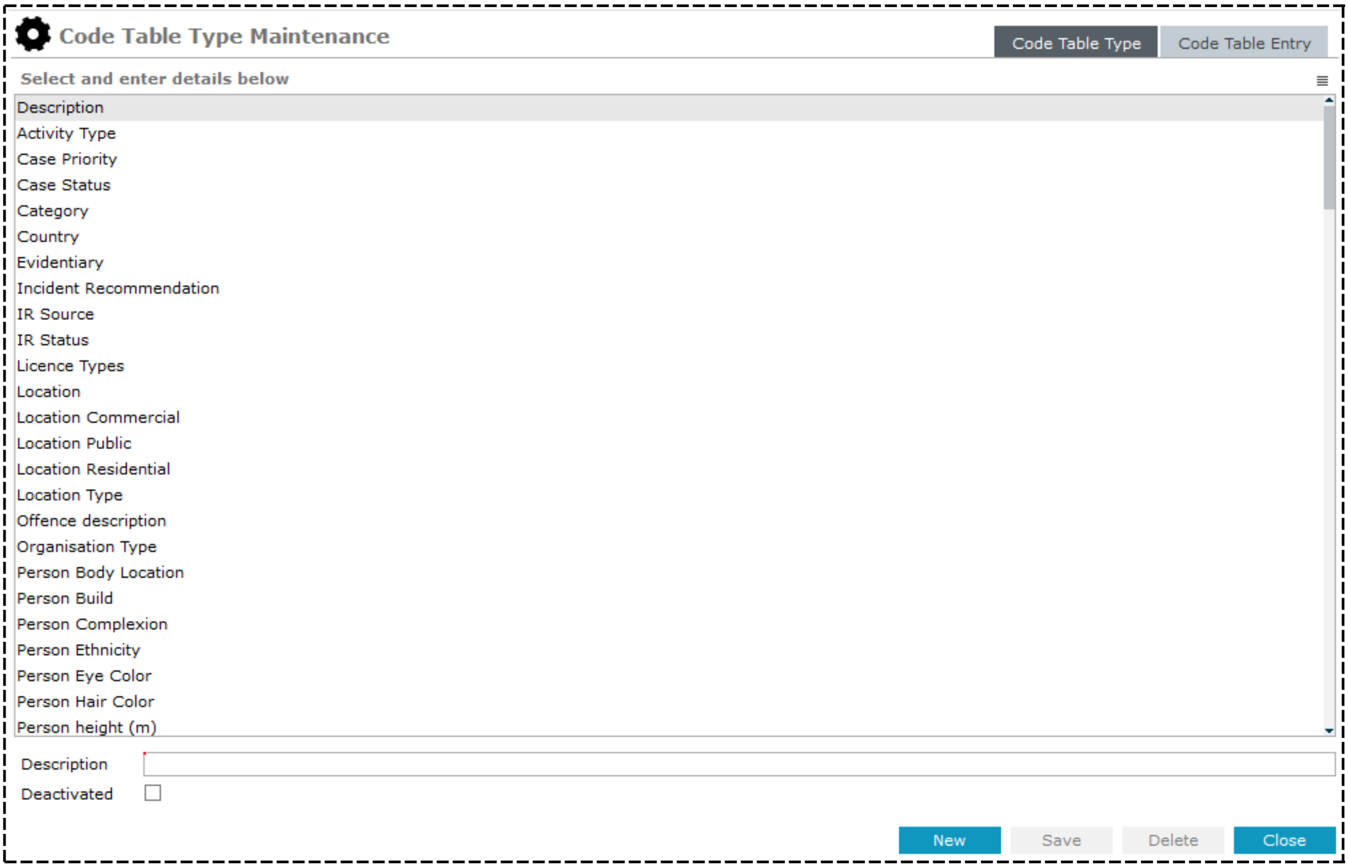
About Entity Attributes

Each attribute can have several values. You can set up the values for each attribute so users can select these. This makes sure values recorded for each attribute are consistent within your agency.

You can edit the attributes of entities that aren't selected. For example, if your agency extends the Document entity by using compound miscellaneous entities and then deselects the Document entity type so no one can add standard document entities, you can update the attributes of all the compound entity types by updating the attributes of the Document entity type.

*Entity types that aren't selected show as **[Deselected]** beside the **Select Type** drop-down.*

To manage the attribute codes you can apply to entity attributes, select **Admin** > **Code Tables** > **Attributes** > **Types**.



Types of Entity Attributes

- **Header**, under which similar attributes are listed.

  A Header attribute:

  - Can be the parent of a group parent or an attribute name.
  - Can be the child of an entity type or another header.
  - Cannot be selected when creating or updating an entity.

    Automatically selected when an attribute grouped under that header is selected.

- **Attribute Name**, which defines the behaviour and type of value for an attribute.

  For example, the Eye Colour attribute can include the Blue, Green, and Brown value options. Or the Credit Card attribute could be a 16-digit number of a specified (masked) format.

  An attribute name can be:

  - A child of entity type, header, or group parent.

    If the attribute name is the child of a group parent, the Default value option and the Mandatory and Multiple values under the Behaviour heading are disabled.

  - Selected when creating or updating an entity.

- **Group Parent**, which describes an attribute that's made up of a number other attributes.

  For example, the Battery attribute could be made up of the Brand, Voltage, and Cell size attributes.

  A group parent can be:

  - A parent of an attribute name or another group parent
  - A child of entity type or header
  - Selected when creating or updating an entity

Permissions You Need to Manage Entity Attributes and Values

To manage entity attributes, you need the *Can maintain entity definition* permission.

To manage the values available for selection for an attribute you need the *Can maintain code tables* permission – For more details, see "Security".

Specify Attribute Security

You can specify which teams can add, change, or delete an entity attribute.

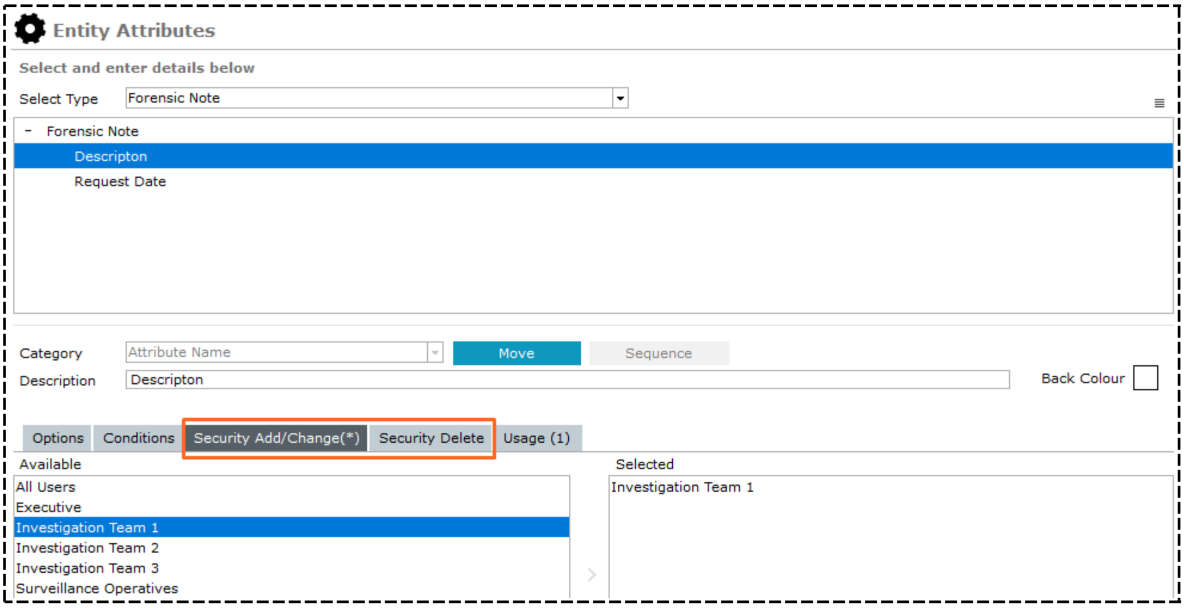
The permission to do each action is controlled on a separate screen. This means you can specify which teams can do what to an attribute.

By default, all teams can add, change, or delete an attribute.

To specify which teams can add, change, or delete the currently selected attribute:

1. Select **Admin** > **Entity Definition** > **Attributes**.
2. Select the attribute you want to control access to.
3. Select either of these tabs:
   - **Security Add/Change** tab to specify which teams can add or manage that attribute of the selected entity.
   - **Security Delete** tab to specify which teams can delete that attribute from the selected entity.

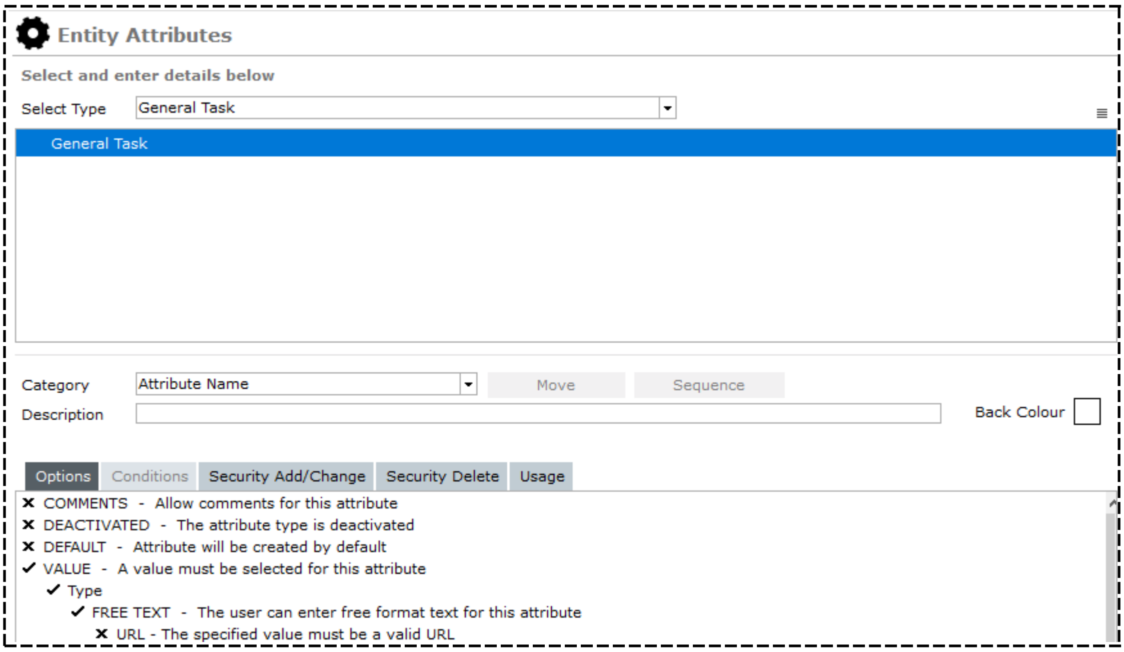
     By default, all teams can add, change, or delete an attribute.
4. Double-click a team or use the Select icon to select the required team.
5. Select **Save**.



Specify an Attribute for an Entity

1. Select **Admin** > **Entity Definition** > **Attributes**.
2. In the **Select type** drop-down, select the entity type.
3. Select **New**.
4. In the **Category** drop-down, select the category of the attribute:
   - Attribute name
   - Attribute type
   - Group parent
   - Header
5. Enter a description for the attribute in the field provided.
6. Select **Save**.

   You'll need to save your changes before you can specify the order of entity attributes or move an attribute to a different parent.
7. Use the following tabs to set up the attribute:
   - Options
   - Conditions
   - Security Add/Change
   - Security Delete
   - Usage

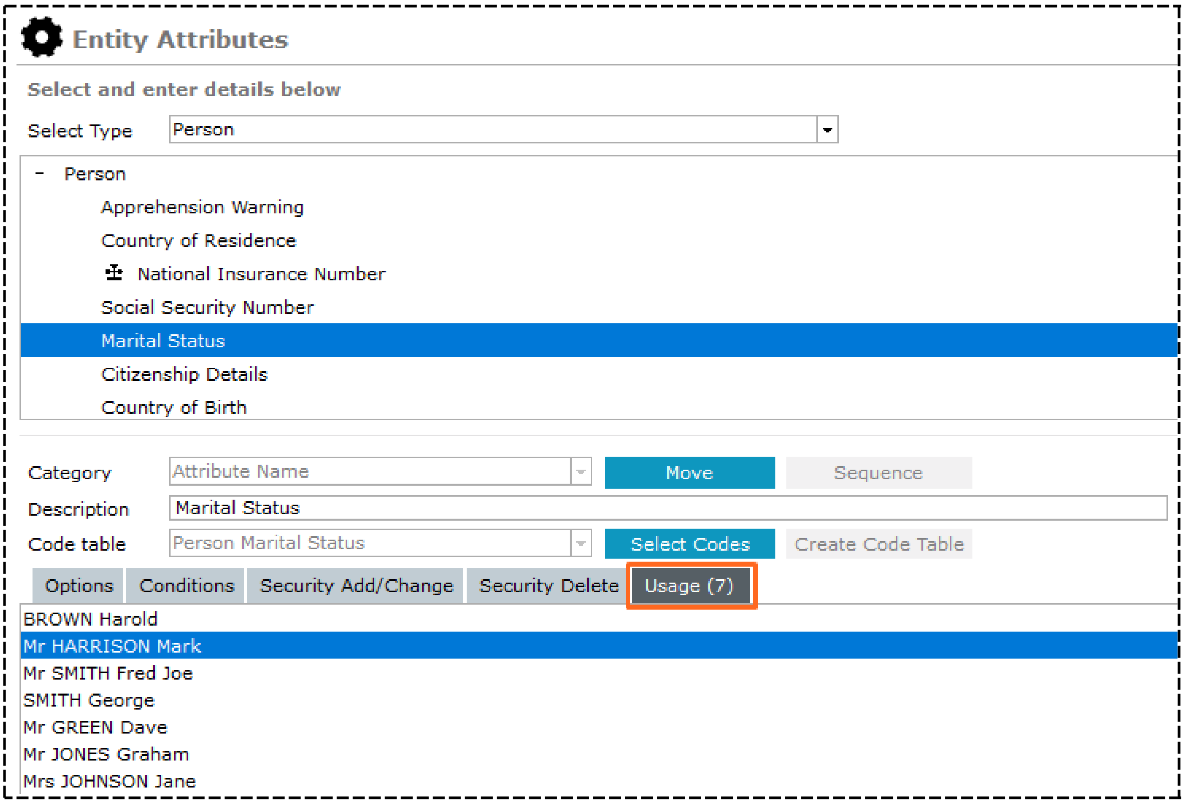


See How an Attribute is Used

Depending on your permission settings, you can see which entities are using an attribute. For example, you can see all the people who have an eye colour recorded.

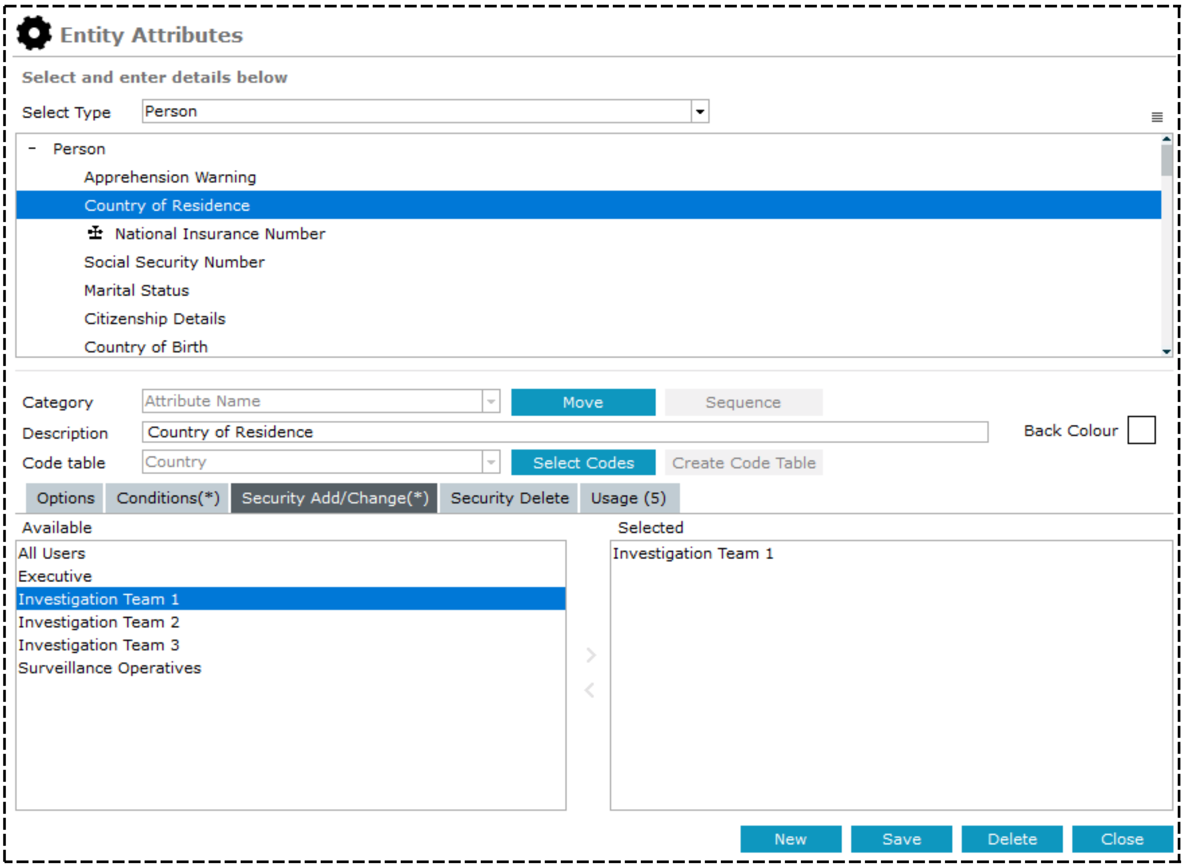
You can also see how many times the attribute is being used:

1. Select **Admin** > **Entity Definition** > **Attributes**.
2. Select an attribute.
3. Select the **Usage** tab.



Edit Attributes for a Type of Entity

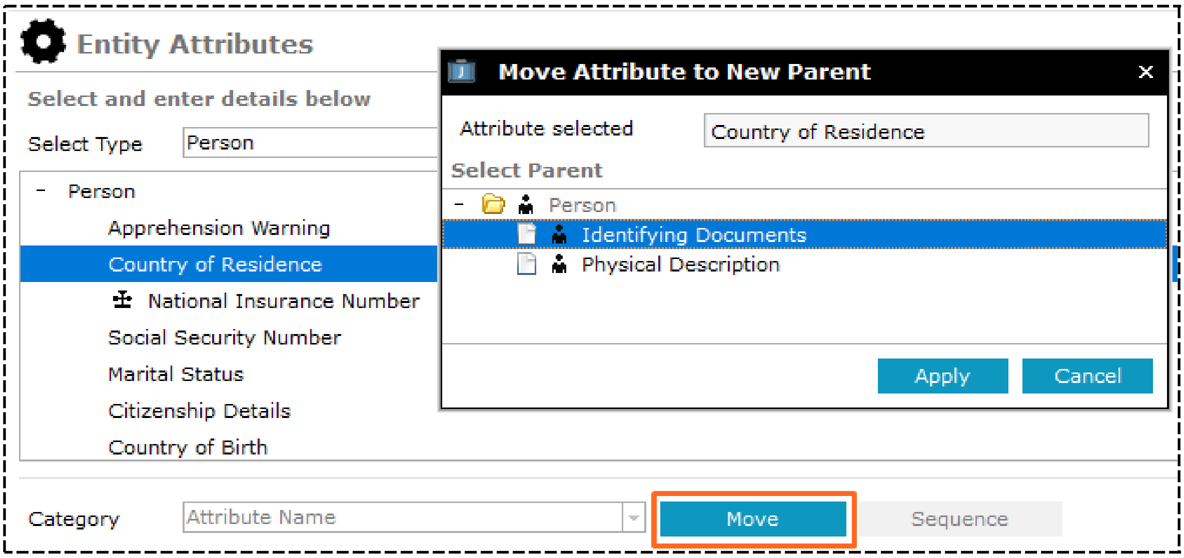
1. Select **Admin** > **Entity Definition** > **Attributes**.
2. In the **Select Type** drop-down, select the entity whose attributes you want to edit.
3. Double-click the attribute you want to edit.
4. Make your changes.
5. Select **Save**.



Change the Parent of an Attribute

You can move an attribute from one heading or group parent to another one (for that entity type):

1. Select **Admin** > **Entity Definition** > **Attributes**.
2. Use either of these methods to move the attribute:
   - Select the attribute you want to move > Select **Move**.
   - Right-click the attribute > Select **Move to New Parent**.
3. Select the heading or group parent you want to move the attribute to > Select **Apply**.
4. Select **Save**.



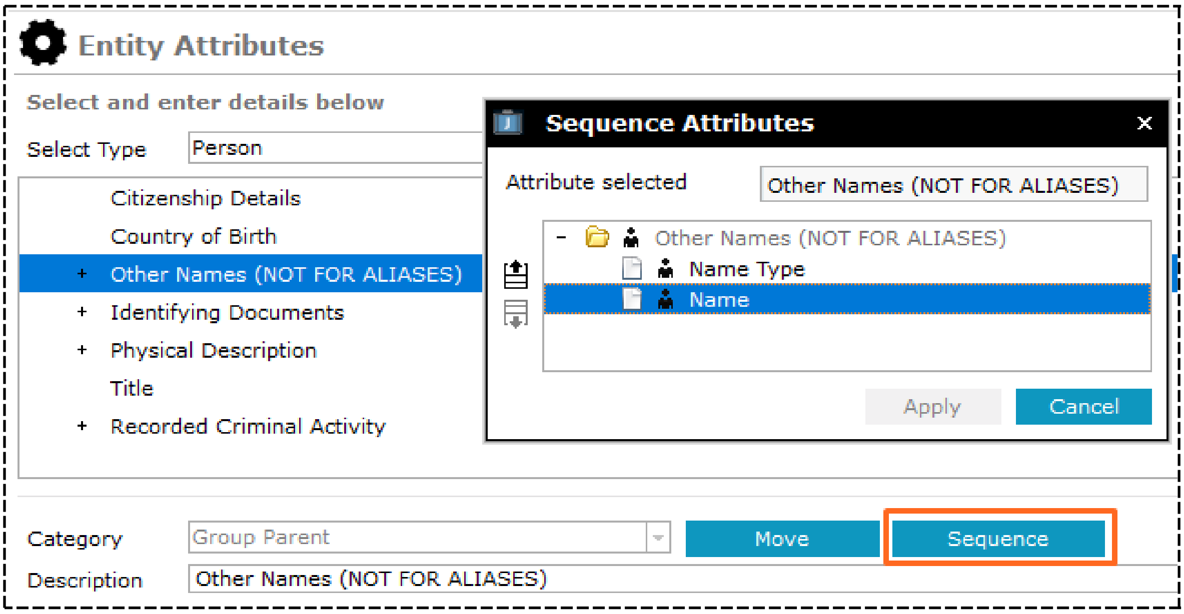
Resequence the Attributes of a Header or Group Parent

You can specify the order of the attributes under a heading or group parent that the sequencing option is enabled for.

*You can enable the Sequencing option under the **Options** tab for an attribute.*

To resequence the attributes of a header or group parent:

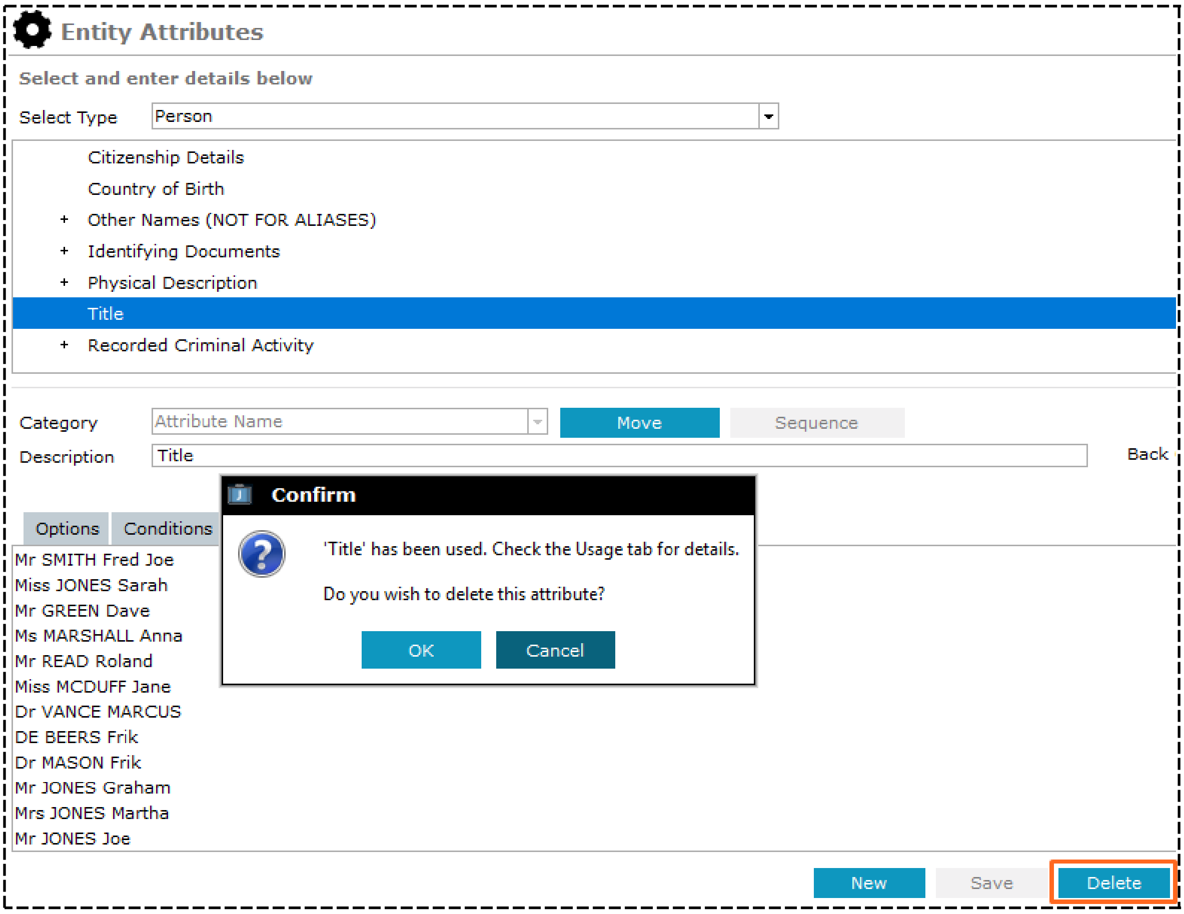
1. Select **Admin** > **Entity Definition** > **Attributes**.
2. Use either of these methods to resequence the attributes:
   - Select the header or group parent whose attributes you want to resequence > Select **Sequence**.
   - Right-click the header or group parent > Select **Sequence**.
3. To move the selected attribute up one position, select the Move up icon.
4. To move the selected attribute down one position, select the Move down icon.
5. Select **Save**.



Delete an Attribute from an Entity

1. Select **Admin** > **Entity Definition** > **Attributes**.
2. In the **Select Type** drop-down, select the entity.
3. Select the attribute you want to delete.

   You can't delete a Group Parent or Header attribute if it has child items.
4. Select **Delete**.
5. Select **OK** to confirm you do want to delete the selected attribute.



CODE TABLES

A code table is a list of values you can select when you enter information about an entity.

The list of values (or codes) is a predefined set.

Using a set of values that have been set up for an entity promotes consistency. It also improves data quality and makes it easier to collect and analyse data.

*To manage codes, you need the **Can Maintain Code Tables** permission.*

Setting Up a Country

You can set up countries, country codes, and calling codes.

The countries you add will be available in the *Country* drop-down on the *System Settings* screen.

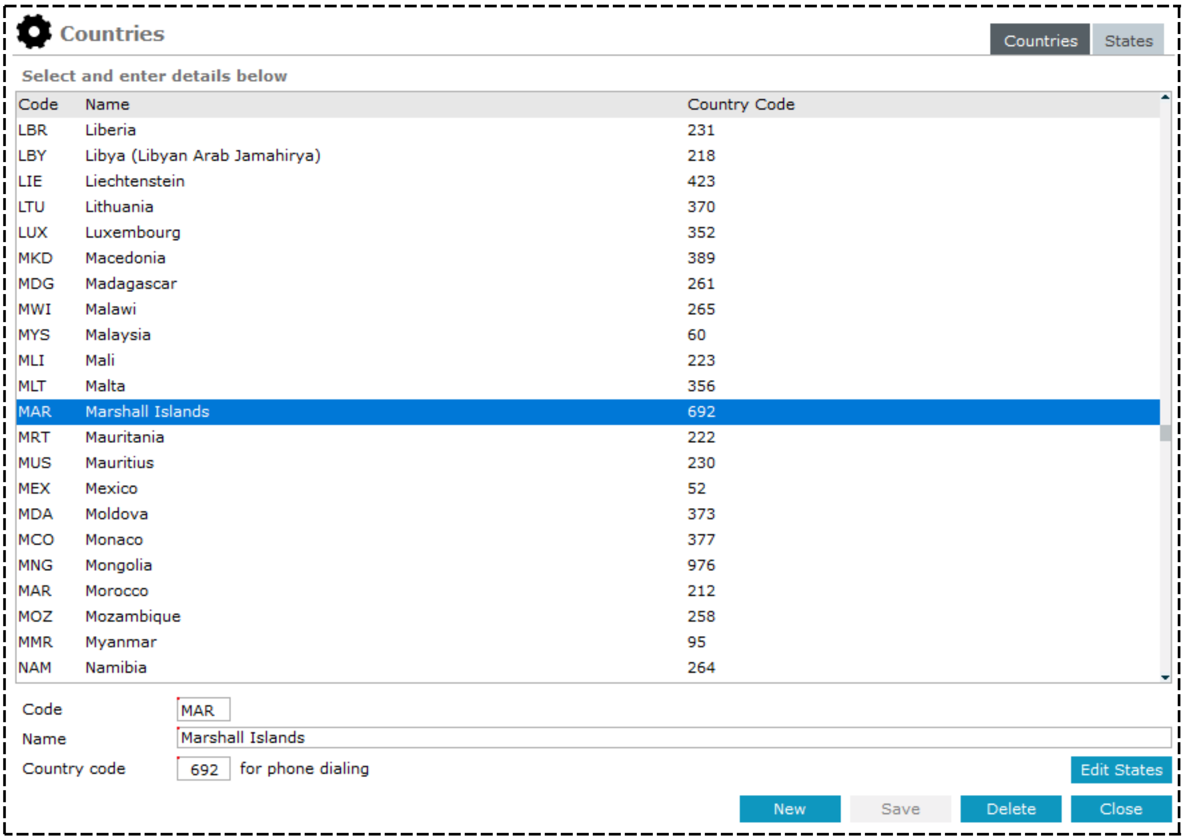
They're used for these types of entities:

- Location
- Contact number
- Organisation
- Vehicle

Set up Countries

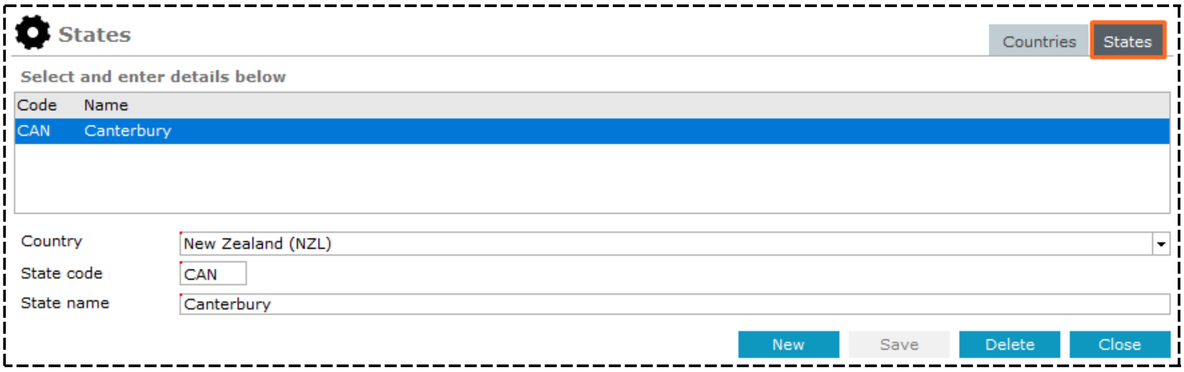
1. Select **Admin** > **Code Tables** > **Countries**.
2. To add a new country:
   a. Select **New**.
   b. Enter a code to identify the country in the **Code** field.
   c. Enter the country name in the field provided.
   d. Enter the country calling code in the **Country code** field.
   e. Select **Save**.
3. To edit a country:
   a. Double-click it.
   b. Make the required changes

      For example, you might want to add provinces or counties.
   c. Save your changes.
4. To delete a country:
   a. Double-click it.
   b. Select **Delete**.
   c. Select **Yes** to confirm your deletion.


Countries
Countries
States
Select and enter details below
Code Name Country Code
LBR Liberia 231
LBY Libya (Libyan Arab Jamahirya) 218
LIE Liechtenstein 423
LTU Lithuania 370
LUX Luxembourg 352
MKD Macedonia 389
MDG Madagascar 261
MWI Malawi 265
MYS Malaysia 60
MLI Mali 223
MLT Malta 356
MAR Marshall Islands 692
MRT Mauritania 222
MUS Mauritius 230
MEX Mexico 52
MDA Moldova 373
MCO Monaco 377
MNG Mongolia 976
MAR Morocco 212
MOZ Mozambique 258
MMR Myanmar 95
NAM Namibia 264
Code
MAR
Name
Marshall Islands
Country code
692
for phone dialing
Edit States
New
Save
Delete
Close

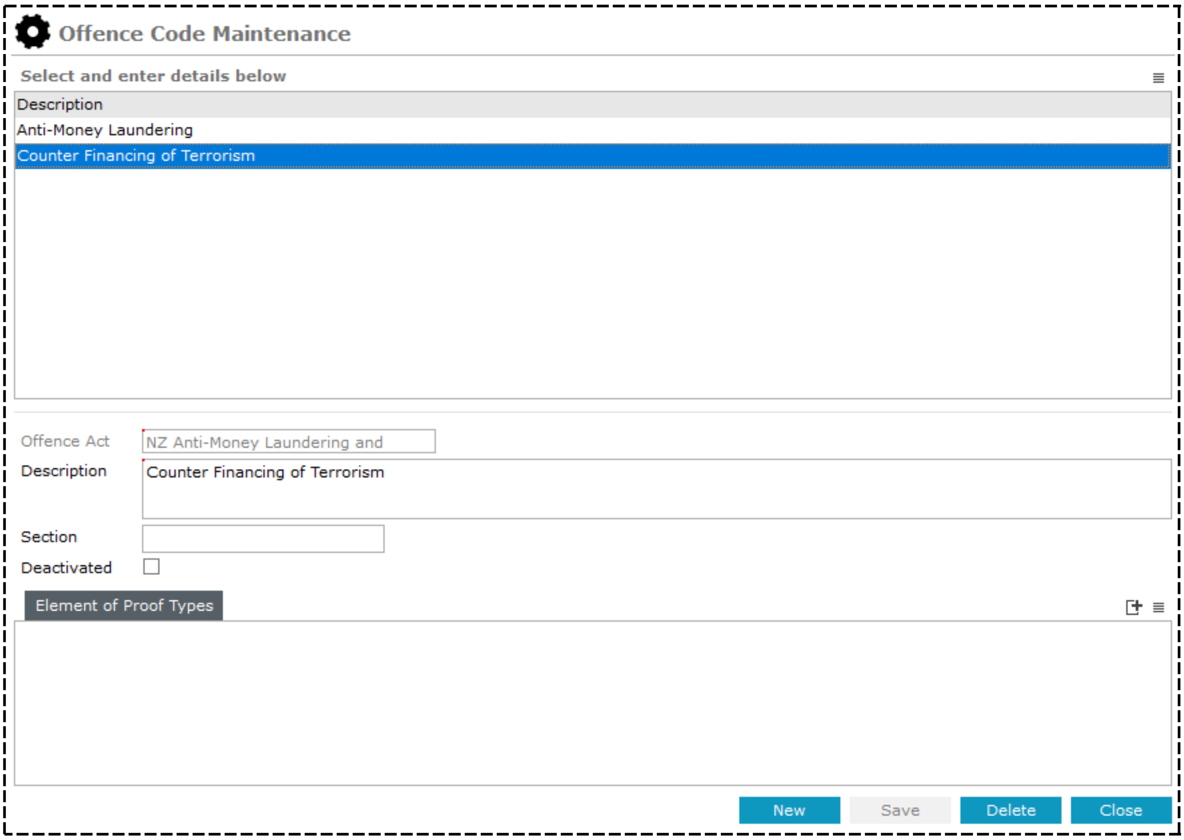
Manage States for a Country

1. Select **Admin** > **Code Tables** > **Countries**.
2. Select the country you want to manage.
3. Select the **States** tab.
4. To add a state:
   a. Enter the state code in the field provided.
   b. In the state name in the field provided.
   c. Select **Save**.
5. To edit a state:
   a. Select it.
   b. Make the required changes.
   c. Save your entries.
6. To delete a state:
   a. Select it.
   b. Select **Delete**.
   c. Select **Yes** button to confirm the deletion.



Set up Offence Acts and Codes for Cases and Incidents

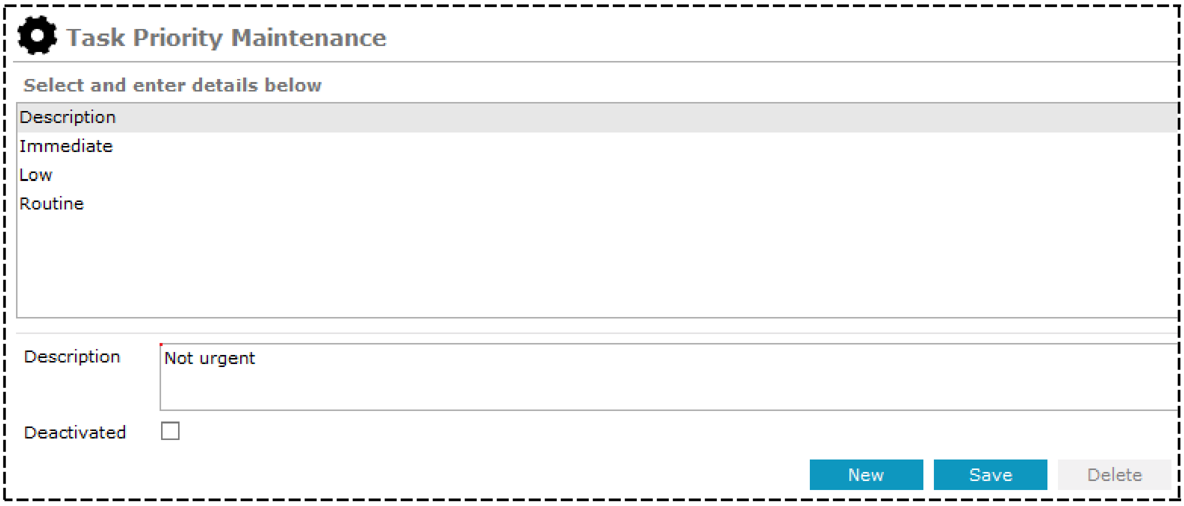
1. Select **Admin** > **Code Tables** > **Offence Acts**.
2. To add an offence act:
   a. Enter the name of the offence act in the **Description** field.
   b. Select **Save**. The offence act displays in the Description table.
      After you add an offence act, you can add sections to that offence act.
3. To set up an offence code for the act:
   a. Select the Add icon.
   b. Right-click in the **Offence Codes** area > Select **New**.
   c. Enter a description for the code in the field provided.
   d. Save your changes.
4. To edit an offence act:
   a. Select it.
   b. Make the required changes.
   c. Select **Save**.
5. To deactivate an offence act, select the **Deactivated** checkbox.
   If you deactivate an offence act, users won't be able to use it, but they will be able to report on it.


Offence Code Maintenance
Select and enter details below
Description
Anti-Money Laundering
Counter Financing of Terrorism
Offence Act
NZ Anti-Money Laundering and
Description
Counter Financing of Terrorism
Section
Deactivated
Element of Proof Types
New
Save
Delete
Close

Set up Task Priorities

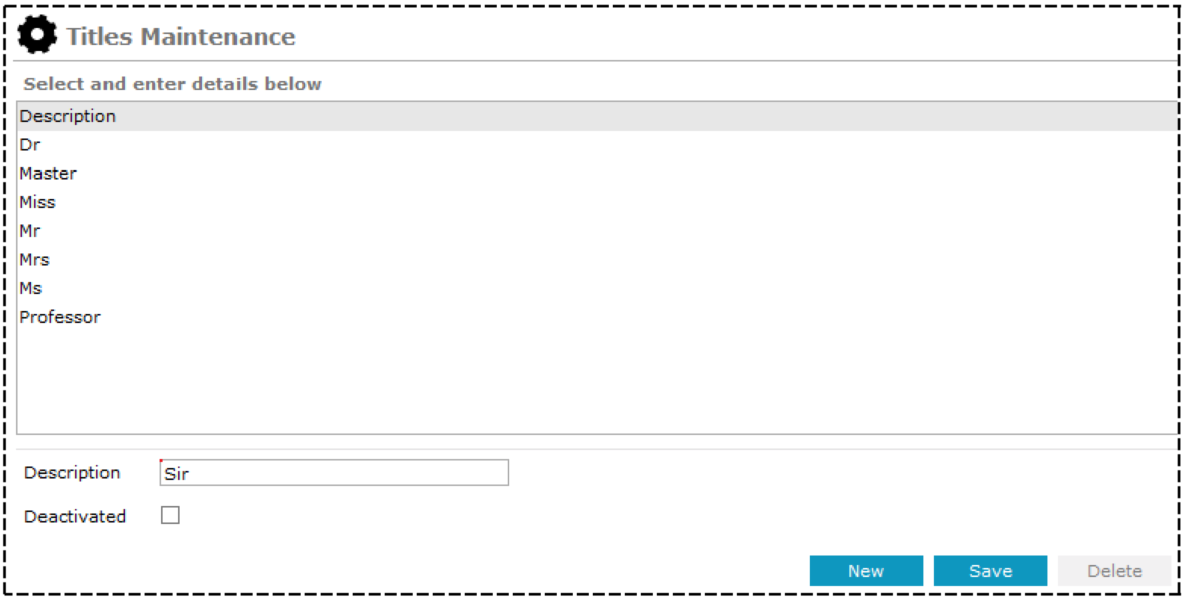
The priorities you set up show in the *Priority* drop-down on the *Task* and *Task Summary* screens.

1. Select **Admin** > **Code Tables** > **Task Priorities**.
2. To add a task priority:
   a. Select **New**.
   b. Enter a description for the task priority in the field provided.
   c. To deactivate the task priority, select the **Deactivated** checkbox.
      Users won't be able to select the task priority but they will be able to report on it.
   d. Select **Save**.
3. To edit a task priority:
   a. Double-click it.
   b. Make the required changes.
   c. Save your entries.
4. To delete a task priority code:
   a. Double-click it.
   b. Select **Delete**.
   c. Select **Yes** to confirm.



Manage the Titles Your Agency Uses to Address People

1. Select **Admin** > **Code Tables** > **Person Titles**.
2. To add a title:
3. Select **New**.
4. Enter a description of the title in the field provided.
5. Select **Save**.



Attribute Code Tables

You can use attribute code tables to specify the attributes that describe a type of entity.

For example, a Person entity type can have the Blue Eyes attribute value.

To specify an attribute code table, you'll need to specify these components:

- Code table name, for example, **eye colour**.
- Individual values that belong to that code table, for example blue.

Once you've set up the attribute code table, you can see how many times the attribute type codes have been used. These options are under **Admin** > **Code Tables** > **Attributes**.

You can use tabs to switch between Code Table Entry and Code Table Type.

Select **Admin** > **Code Tables** > **Attributes** > **Entities**.

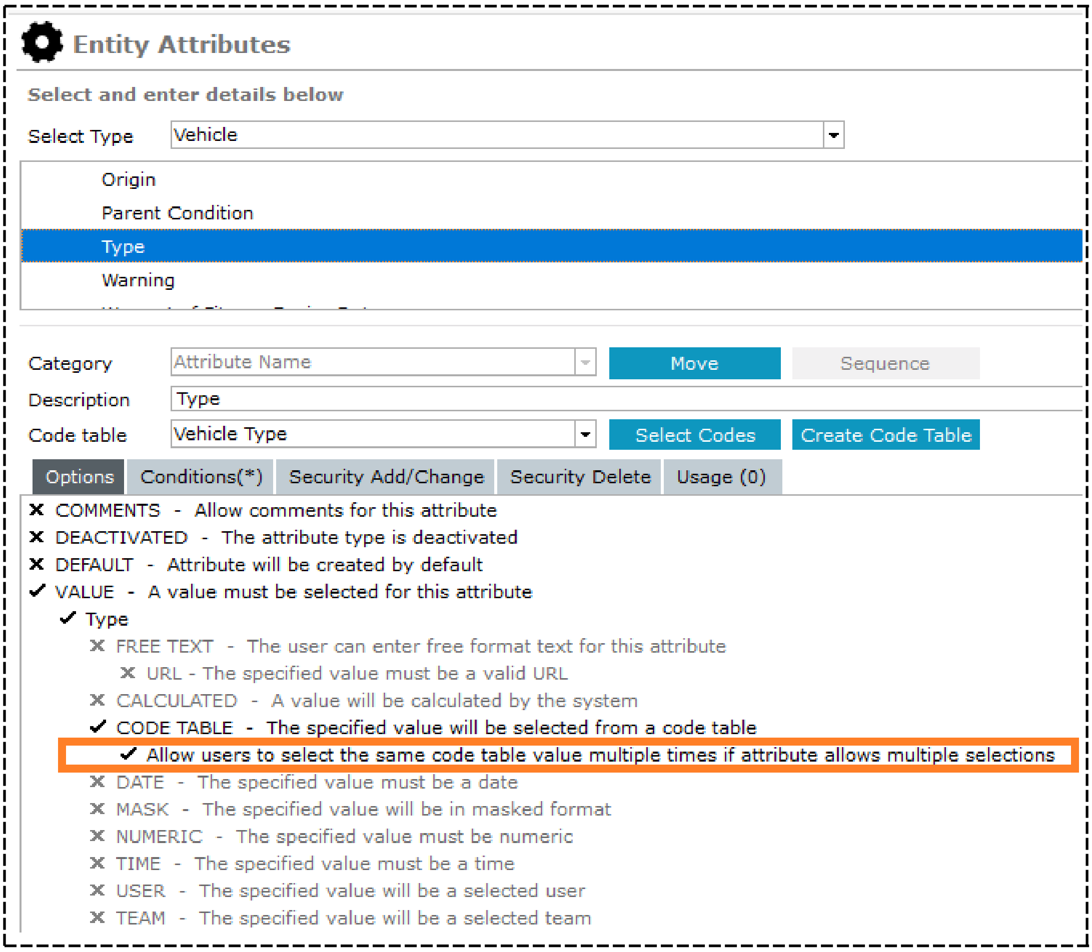
Set up Multiple Code Table Attributes

You can set the available list to remain unchanged when you add multiple attribute values that are code tables.

This is useful if you want to repeat an attribute but you want to reuse the same code value.

To set this up:

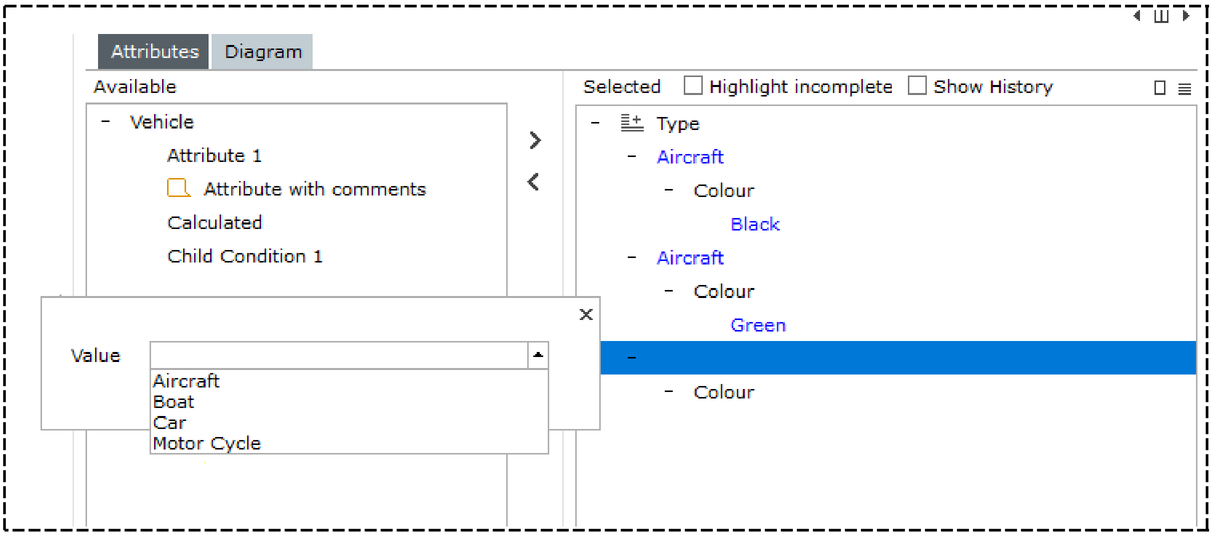
1. Select **Admin** > **Attributes** > **Types** > **Entity Type** > **Attribute Type**.
2. Select the **Security Add/Change** tab.



Example of Using Multiple Code Table Attributes

In the following image type is a multiple attribute with code value choices of Aircraft, Boat, Car, Motor Cycle.

You can select aircraft multiple times. It won't be removed from the available list once it has been used.



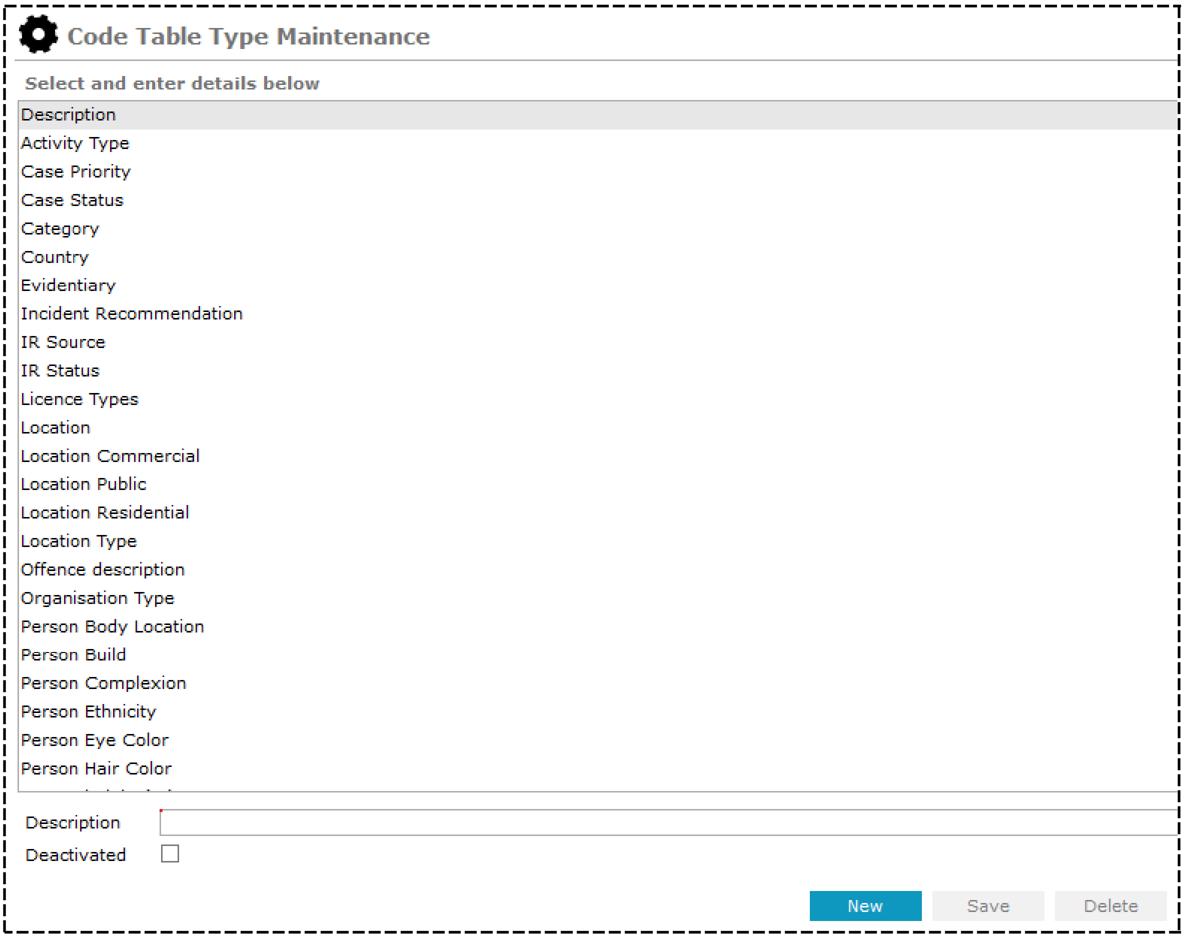
Manage Types of Attributes

Before you can specify attribute code values (or entries), you'll need to specify the attribute type the code values belong to:

1. Select **Admin** > **Code Tables** > **Attribute Code Tables** > **Types**.
2. To add a new type of attribute:
   a. Select **New**.
   b. Enter a description of the attribute type in the field provided.
   c. To deactivate the code, select the **Deactivated** checkbox.

      If you select this checkbox, users can't select the code but they can report on it.
   d. Select **Save**.
3. To edit an attribute type:
   a. In the table at the top of the screen, double-click the attribute type you want to edit.
   b. Edit the required details > Select **Save**.
4. To delete an attribute type:
   a. Select it.
   b. Select **Delete**.

c. Select **Yes** to confirm you want to proceed.



Manage Entity Attributes

You can edit the values for recording an attribute type.

For example, for the Eye Colour attribute, you can record Blue, Brown, Green, and so on.

You can also see the number of times the attribute type codes have been used.

To manage entity attributes:

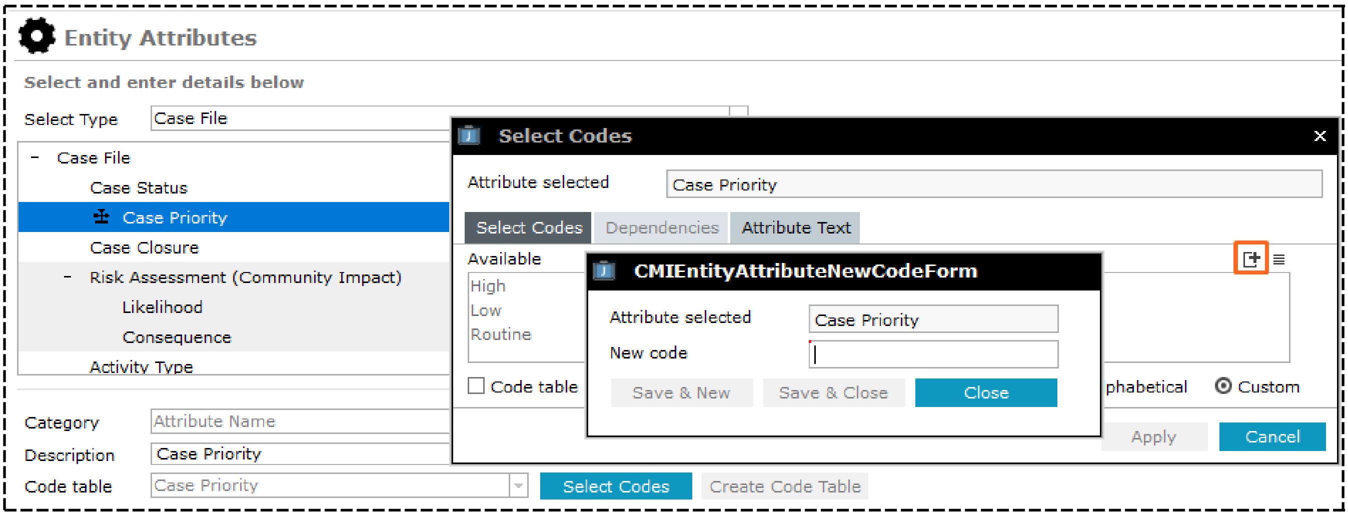
1. Select **Admin** > **Code Tables** > **Attributes** > **Entries**.
2. In the **Type** drop-down, select the attribute type code.

   *If the type you need isn't shown, select **New Type**.*
3. To imports several attribute values from a TXT file:
   a. Select **Bulk Load From File**.
   b. Select the file you want to import.
   c. Select **Open** to import the file.
4. To add a new attribute value:
   a. Select **New**.
   b. In the *Description* field, enter a description of the attribute value.
   c. To deactivate the attribute value, select the **Deactivated** checkbox.

      If you select this checkbox, users can't select the attribute value but they can report on it.
   d. Select **Save**.
5. To edit an attribute value:
   a. In the table at the top of the screen, double-click the attribute value you want to edit.
   b. Edit the required details > Select **Save**.
6. To delete an attribute value:
   a. Select it > Select **Delete**.
   b. Confirm you want to proceed.
   c. Select **Yes**.

Easily Add a New Value for a Code Table

If you need to add a new value for a code table, use the Add icon to do this.



See How Many Times an Attribute Code Value is Used

You can see how many times an attribute code value is used.

For example, you can see how many times the Blue Eyes attribute code has been used in a description of a Person entity.

1. Select the **Admin** > **Code Tables** > **Attributes** > **Entries**.
2. In the **Type** drop-down, select the attribute type code for the values you want to see.
3. Select the **Usage** tab.
4. Select the Expand + icon beside a code value or entity to see how it's being used.

Manage System Code Tables

You can set up the following system codes:

System Code	Description	Examples
Case Role	The roles a user can be assigned within a case.	Suspect, witness, case manager
Disclosure Status	The status of entities. This shows whether entities should be part of the disclosure process and how they should be treated.	
Dissemination Status	The status of entities indicating whether they should be part of the dissemination process and how they should be treated.	
Information Grade	The reliability of the information your agency has received for an investigation.	*confirmed* or *improbable*
Information Source Grade	How reliable the information source is. This is a person.	Usually reliable
Involvement	The types of involvement a person can have in a case. A person can have one current involvement and a history of different types of involvements.	They might have been a witness but now they're a suspect.
Phase	An area of responsibility for a user in a case.	Crime scene, witness, evidence
Rank	The types of rank held by users in an agency.	Sergeant, senior sergeant, detective
Relationship Category	Your agency specifies these for an entity.	Family or social organisation
Relationship Status	Status of a relationship recorded in a source entity.	Confirmed, suspected, or disproven
Source Agency	Agencies you share information with.	Customs or other enforcement agencies.

Manage System Codes

1. Select **Admin** > **Code Tables** > **System**.
2. In the **Type** drop-down, select the type of system code you want to manage.
3. To add a new system code:
    a. Select **New**.
    b. Enter a description for the system code in the field provided.
    c. Select the **Deactivated** checkbox to deactivate the code.

       If you select this checkbox, users can't select the code but they can report on it.
    d. Select **Save**.
4. To edit a system code:
    a. Double-click the code you want to edit.
    b. Make your changes.
    c. Select **Save**.
5. To delete a system code:
    a. Double-click the code you want to delete.
    b. Select **Delete**.
    c. Select **Yes** to confirm.

Adding a System-wide Default Case Role

You might want to make a case role available for users to select when they assign a user to a case role in a type of case.

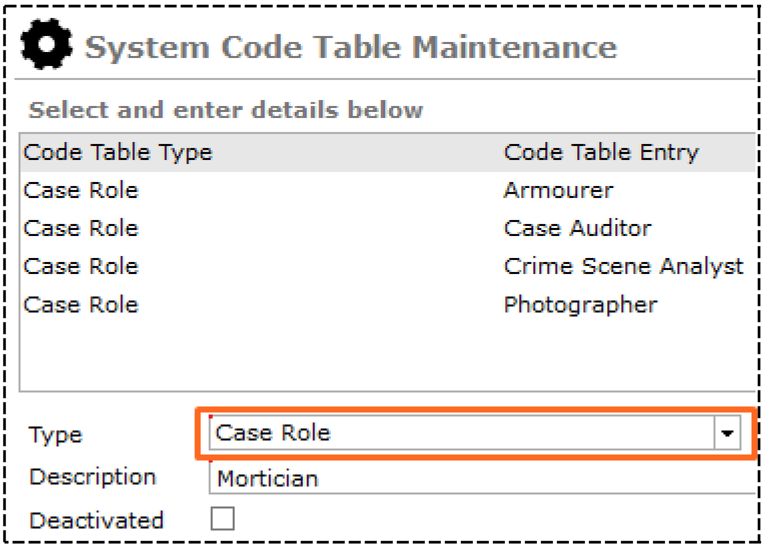
This will make sure the role is consistently named across all cases.

To do this, you'll need to add the case role and the type of case entity to the case role system code table.

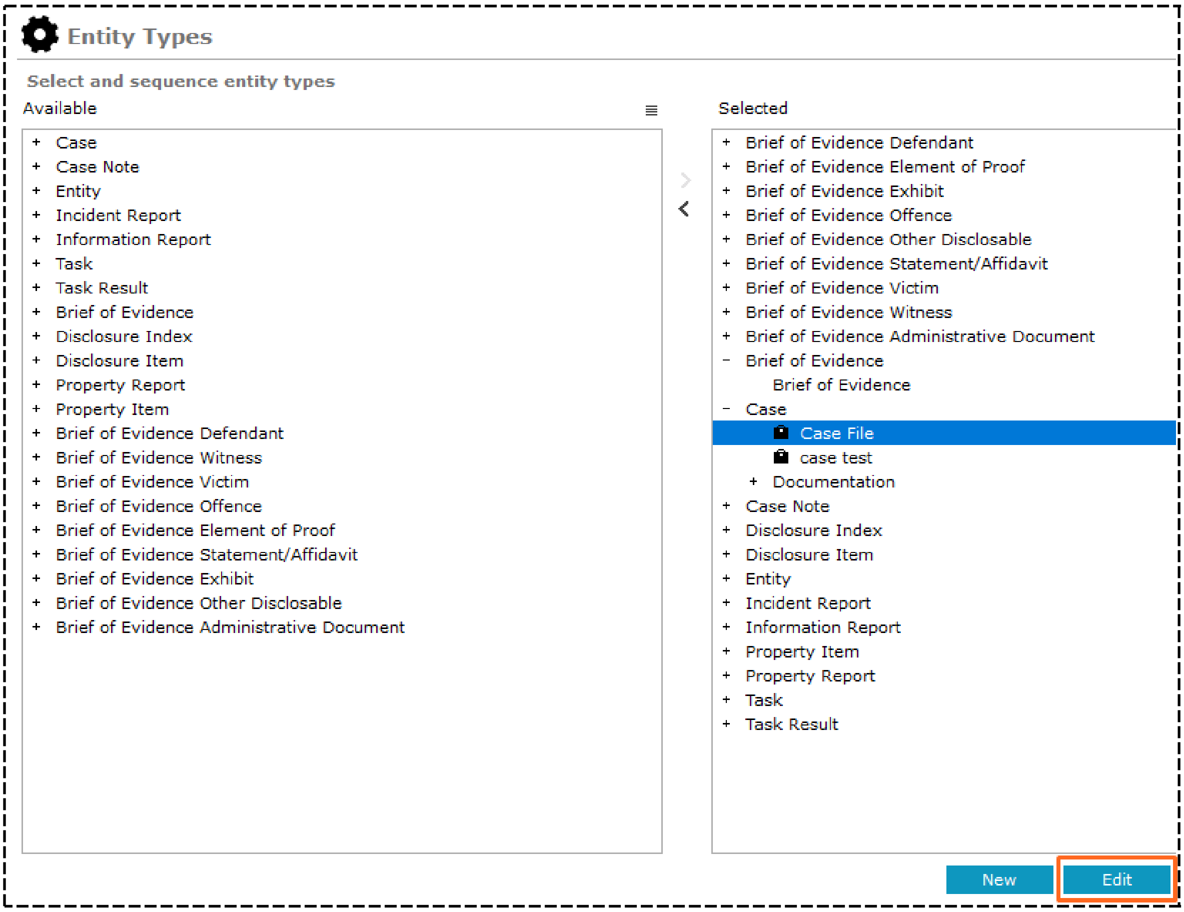
*If a user wants to add a case role to their case and the case role hasn't been set up as a system-wide case role, they can add an ad hoc case role to their case. See **Adding an Ad hoc Case Role to a Case** in the user guide.*

Set up a System-wide Case Role

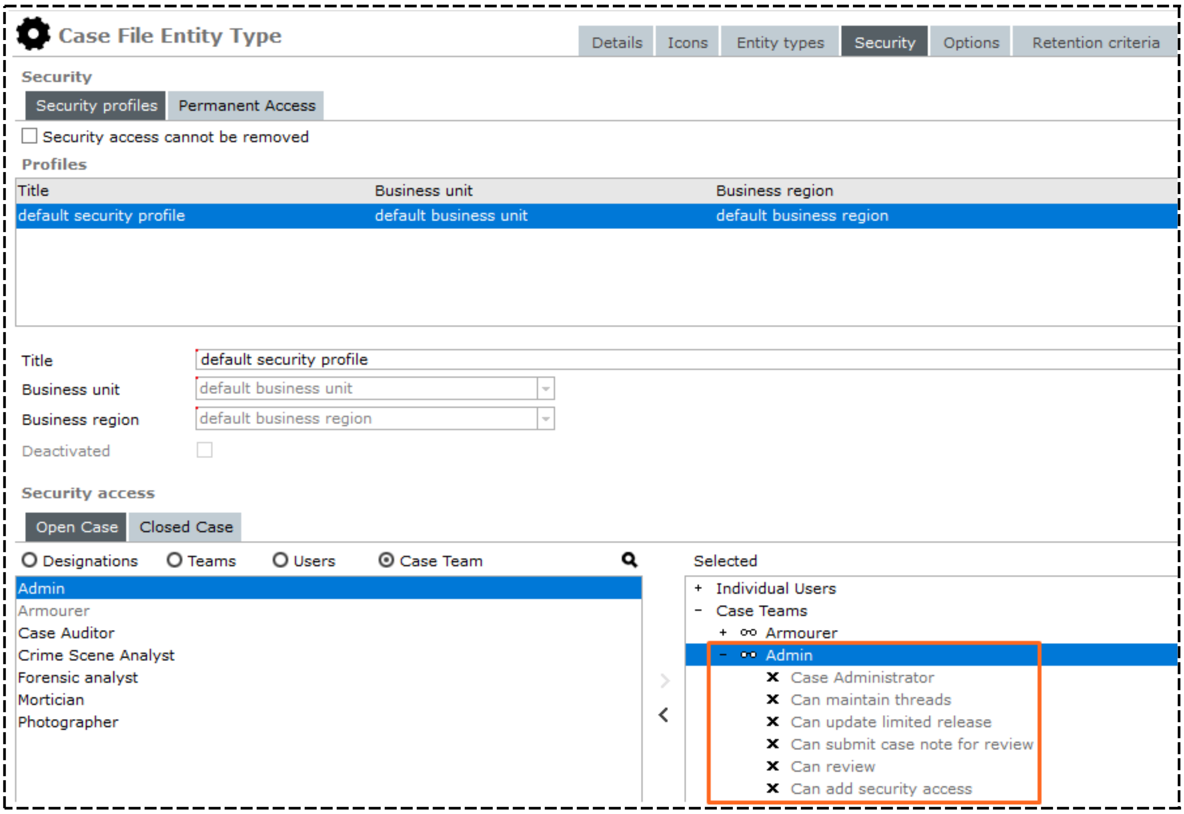
1. Select **Admin** > **Code Tables** > **System**.
2. Expand the **Type** drop-down > Select **Case Role**.
3. Enter a description for the role in the field provided.
4. Select **Save**.



5. Select **Admin** > **Entity Definition** > **Types**.
6. Find and select the type of case entity you want to add a system-wide case role definition to.
7. Select **Edit**.



8. Select the **Security** tab.
9. Select the **default security profile**.
10. In the **Security access** area, select the **Case Team** option.
11. Double-click the case team you created or use the Select icon to associate it with this type of case file entity.
12. To change the access rights from view to edit, toggle the icons beside the case roles.



Importing and Exporting Code Tables

Importing and exporting code tables allows you to:

- Import code tables that have been exported from another ICM database into your ICM database.
- Export code tables from your ICM database to a file that you can then import into another ICM database.

You can import and export files in XML format.

*To export or import code tables, you need the **Can Maintain Code Tables** permission.*

Value Masks

You can use a value mask for fields where users need to enter data in a specific format. This enhances consistency and reduces the possibility of input error.

A value mask is a linked series of symbols you can use to define:

- The type of data users can enter
- The text that will show in the current field
- The type of data user need to enter – Upper case or numbers, for example
- The numeric range allowed for the numeric portion of a field or label

Mask Characters

Here are the characters you can use to define a value mask for a field:

A	Mandatory text character
a	Optional text character
9	Mandatory numeral
#	Optional numeral
C	Mandatory any character – Text or number
c	Optional any character – Text or number
>	Forces the right adjoining text character to upper case
>>	Forces all following text characters to upper case

<	Forces left adjoining text character to lower case
<<	Forces all previous text characters to lower case
$	Currency symbol – Locale-dependent
.	Actual character expected – Locale-dependent
-	Actual character expected – Locale-dependent
,	Separator is automatically inserted into the numeric value as the number is entered – Locale-dependent
****	Treat the next character as a literal

If one of these characters isn't specified in the mask, the mask won't be saved.

Disallowed Characters

Any other symbol entered in the mask is treated as a literal, except for the symbols listed in this table.

Use the backward slash \ to treat symbols as literals.

"	Double quote H Uppercase H L Uppercase L T Uppercase T W Uppercase W R Uppercase R
|	Pipe
[	Left square bracket
]	Right square bracket
@	At symbol

You can't create a value mask using any of the characters listed in the previous table.

Mask Examples

This table shows examples of using value masks to format the data entered in a text field.

AAA999	ABC123 or abc123
aaa999	ABC123, AB123, abc123, or ab123
aaa###	ABC123, AB12, or ABC1 >
AAA999	ABC123 or Abc123 >>AAA999 ABC123
999\-999\-999	123-456-789
999 999 999	123 456 789
### ### ###	123 456 789, 12 34 567, 1 234 567
$###.##	$900, $1,000, $20.00, or $300.00
\DEF###	DEF1, DEF12, or DEF123
CAA999	1BC123, ABC123, 1bc123, or abc123
cAA999	1BC123, ABC123, 1bc123, or abc123

BACKGROUND PROCESSES

Resource-intensive and long-running background processes run on the application server.

They start automatically when the application server starts.

To access the Background Processes screen, select **Admin** > **System** > **Background Apps**.

You can manage these background apps:

Keywords	Builds keyword data in the background so foreground updates don't have to wait while keywords are built.
Email	Emails generated by ICM.
Named Entity Extraction	Processes text to identify text fragments that might represent entities that can be extracted and created as ICM entities. The process passes back candidate entities reviewed by a user. The user accepts them, creates an entity, or discards them.
ERP Search	Processes entity relationship path searches that don't have immediate priority.
Active Search	Processes active searches.
Alerts	Processes alerts.
Audit	Processes audit information so foreground updates don't have to wait while audit details are built.
File Load	Processes file import requests.

ODBC Server	Processes relational database requests from other applications that need to use the database.
Backup and Housekeeping	Processes backups and housekeeping of old log files.
Duplicate Entities Identification	Processes identifying duplicate entities.
Triggers	Processes triggers.
Lazy Updater	This process offloads processing some types of updates to improve processing speed and efficiency. This is important when single point collections are being updated. The Lazy Updater is usually only used on implementations where lots of users are entering case notes, tasks, and task results at a rate where these start conflicting with each other. You don't need to enable this option for smaller implementations.

See Which Background Apps Are Running on the Application Server

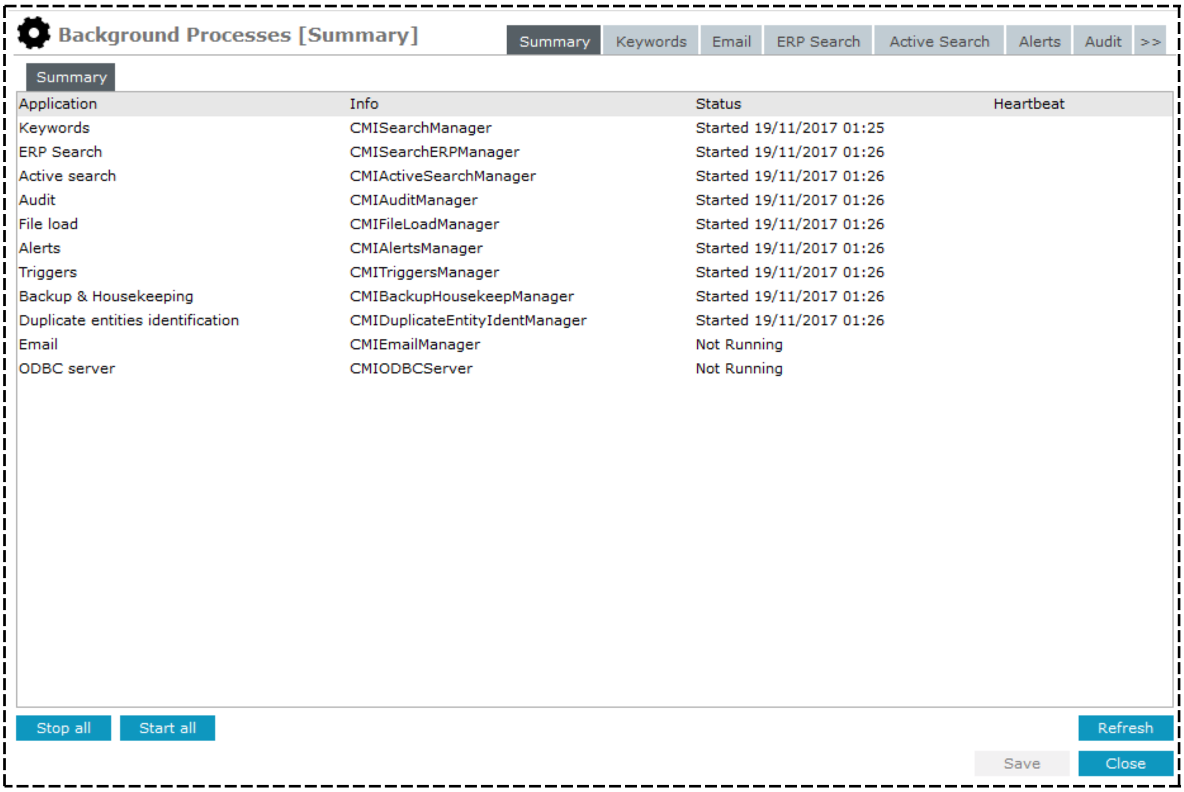
1. Select **Admin** > **System** > **Background Apps**.

   You'll see which applications are running as background apps.

   *The **Heartbeat** column shows the last time the process communicated.*
2. To see any background apps that have started since you opened this screen, select **Refresh**.
3. To start all background apps, select **Start all**.

   Starting all background apps might have a temporary performance impact on users.
4. To stop all background apps, select the **Stop all** button.

   Stopping all background apps affects the people in your organisation who are busy using ICM.



Keywords

The keywords background process indexes text when immediate indexing isn't set.

You can monitor, view the status of, and set up parameters for this process.

ICM creates keyword indexes for all the information you enter. You can use indexing to find information in the database.

If you add a new entity but can't find it when you search, this is probably because it hasn't yet been indexed yet.

Files in the MediaAttachments folder aren't indexed. If you store your documents in this folder, they're not included in any searches. To make sure your documents are indexed (and searchable), upload them as Document entities.

The keywords background process makes sure the keywords used in searches are up to date. If you find an item that hasn't been indexed yet, it might not be returned in the search results. The background search manager starts automatically when you start the database on the server.

Monitor the Keywords Background Process

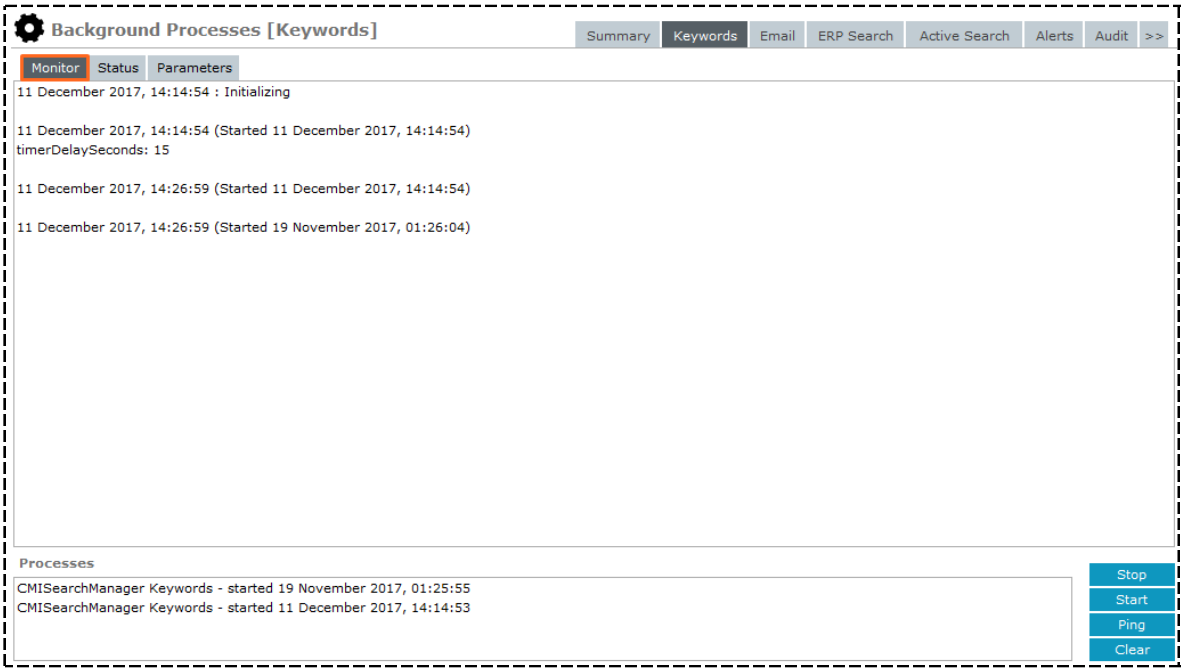
1. Select **Admin** > **System** > **Background Apps**.
2. Select the **Keywords** tab.

   You'll see when the keywords background process started or stopped and the search managers that are active.
3. To start the keywords background process, select **Start**.

   If a keywords background process is already running, you're prompted to confirm you want to start an additional process.

   Multiple active processes for the same background process can cause locking contentions.
4. To check the status of the keywords background process, select **Ping**.
5. To stop the keywords background process, select **Stop**.

   Stopping the keywords background process impacts users severely. This is because entities that haven't been indexed aren't returned in a search.
6. To clear the upper area, select **Clear**.



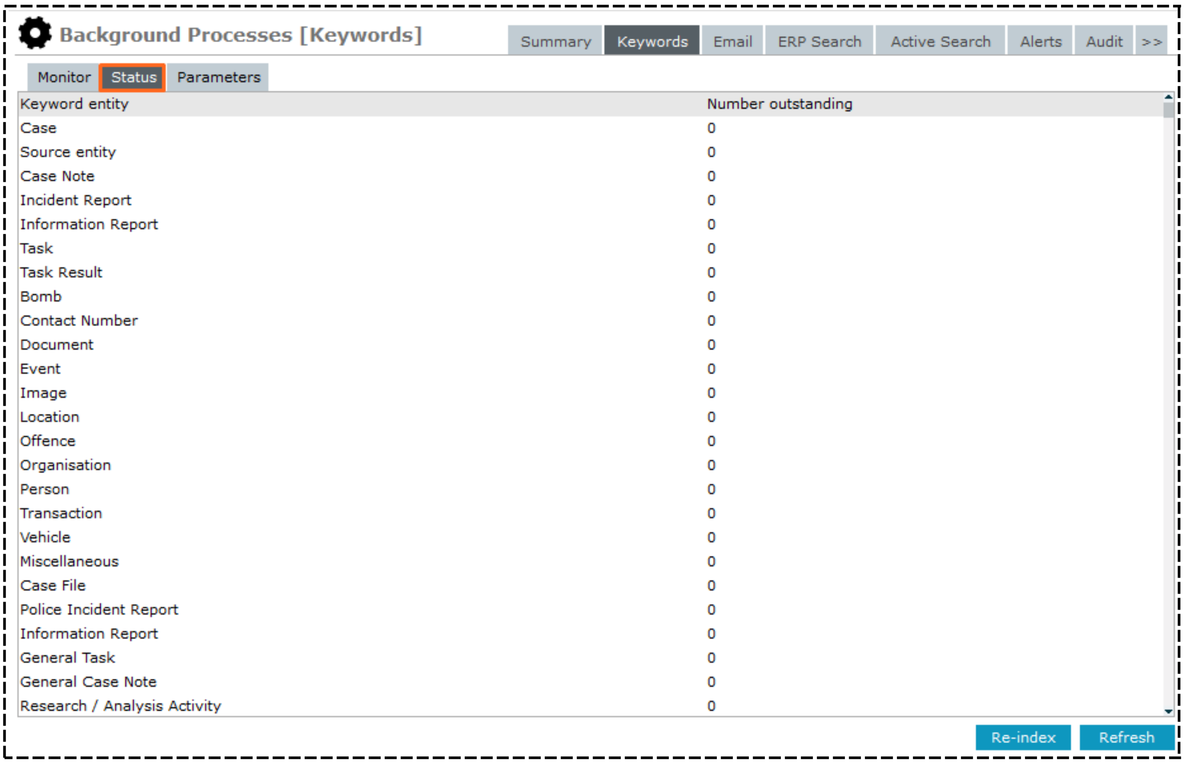
Check Status of Keywords Background Process

1. Select **Admin** > **System** > **Background Apps**.
2. Select the **Keywords** tab.
3. Select the **Status** subtab.

   If there are lots of outstanding updates, your keywords will probably be out of date.

   Make sure the Keywords background process is active.

4. To refresh the status list, select **Refresh**.



Set up Parameters for the Keywords Background Process

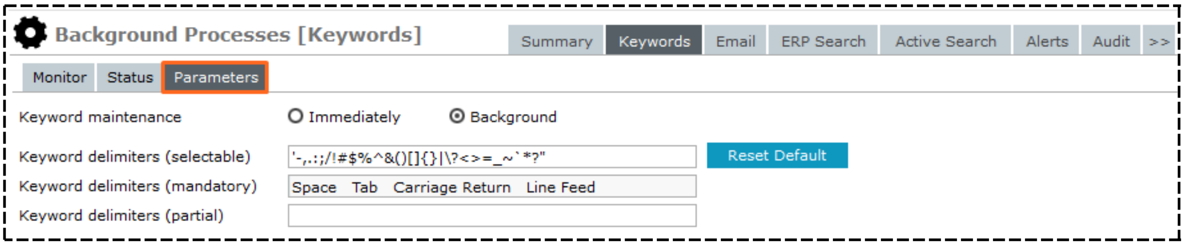
You can set up parameters of the Keywords background process.

For example, you can enter keyword delimiters (characters that show the start and end of a keyword).

To access these options:

1. Select **Admin** > **System** > **Background Apps**.
2. Select the **Keywords** tab.
3. Select the **Parameters** subtab.
4. To specify how keywords should be managed, select either of these options:
   - **Immediately** to update entity keywords as soon as they're entered and the entity is saved.
   - **Background** to update keywords the next time the Keywords background process runs.
5. To specify keyword delimiters:
   a. In the **Keyword delimiters (selectable)** field, delete any default keyword delimiters you don't want to keep.
   b. Enter any required keyword delimiters.
6. To reset the *Keyword delimiters (selectable)* field to its original state, select **Reset Default**.
7. Select **Save**.

   *If you changed the keyword maintenance from Immediate to Background, the background process starts automatically when you select **Save**.*



Email Background Process

The email background process sends emails from ICM. You can set up parameters for this process.

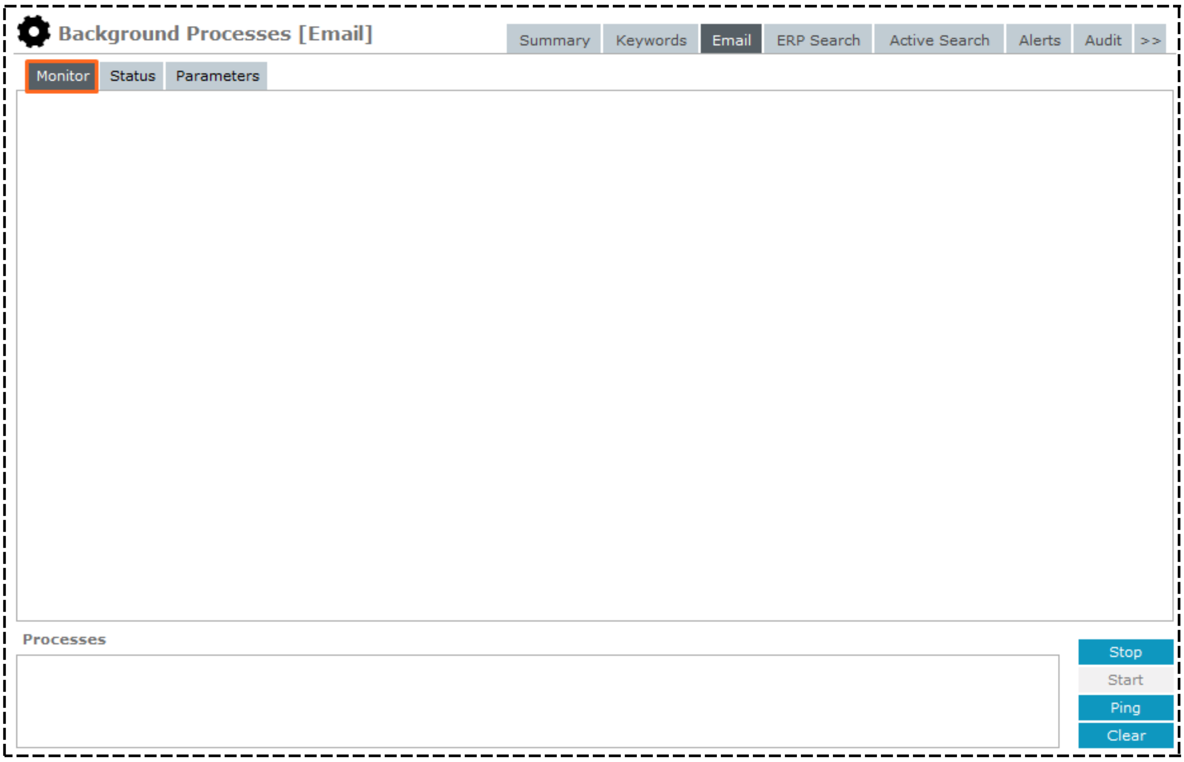
Monitor the Email Background Process

1. Select **Admin** > **System** > **Background Apps**.
2. Select the **Email** tab.

   You'll see details about when the email background process started or stopped and the processes that are active.

   The *Processes* area shows any processes that are running.

   You'll need to set up the email background process to send email messages.

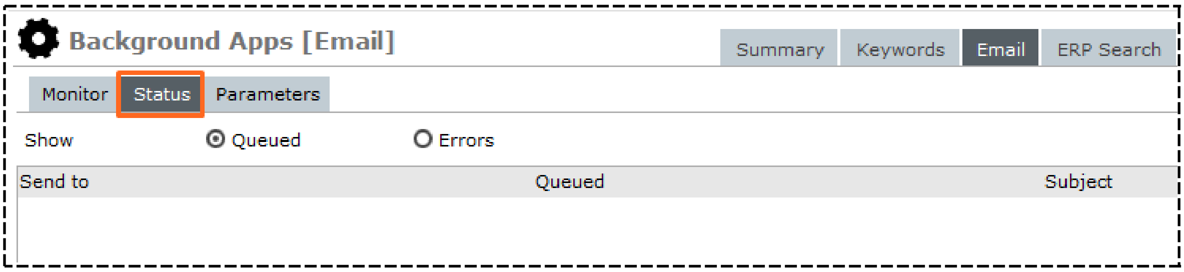


Check the Status of the Email Background Process

1. Select **Admin** > **System** > **Background Apps**.
2. Select the **Email** tab.
3. Select the **Status** subtab.

   You'll see a list of any emails that are waiting to be sent or couldn't be sent.

4. To specify the email messages you want to see, select one of these options:
   - **Queued** to see unsent emails.
   - **Errors** to see emails that couldn't be sent because of an error.



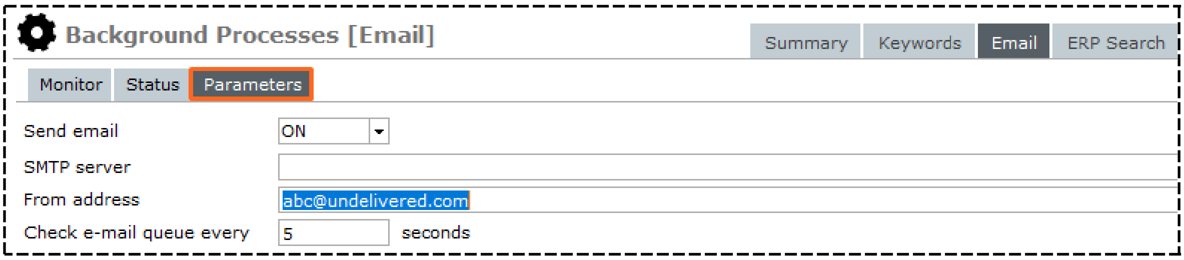
Set up Parameters for the Background Process

1. Select **Admin** > **System** > **Background Apps**.
2. Select the **Email** tab.
3. Select the **Parameters** subtab.
4. To allow emails to be sent, select **ON** in the *Send email* drop-down.

   *If you select **Off**, you won't be able to start the email background process under the Monitor subtab.*
5. In the **SMTP server** field, enter the address of the Simple Mail Transfer Protocol (SMTP) server that will send emails.

   Enter an Internet Protocol (IP) address or a domain name.
6. In the **From address** field, enter the email address that emails will be sent from.

   This is the email address undeliverable messages will be returned to.
7. In the **Check email queue every** field, enter the number of seconds between checks for items on the email queue.
8. Select **Save**.



Entity Relationship Path Search

The ERP Search background process does Entity Relationship Path (ERP) searches.

You can set up the parameters for this process.

See the user guide for details about doing an ERP search.

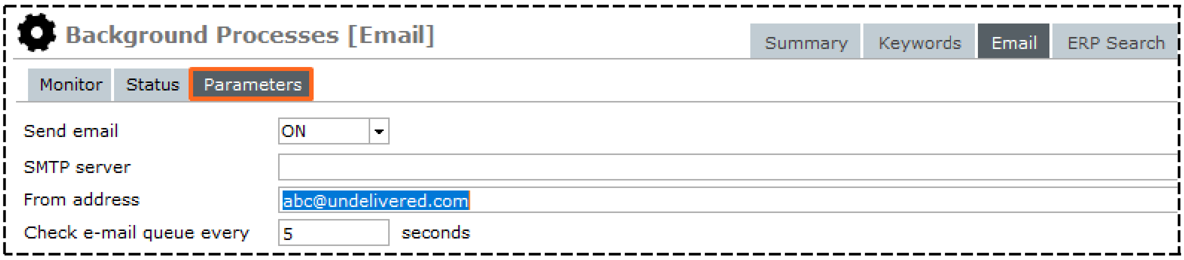
Monitor ERP Search Background Process

1. Select **Admin** > **System** > **Background Apps**.
2. Select the **ERP Search** tab.

   You'll see when the ERP Search background process started or stopped and any active search managers.

   The **Processes** area shows any processes that are running.

   Stopping the ERP Search background process will prevent users from running ERP searches.

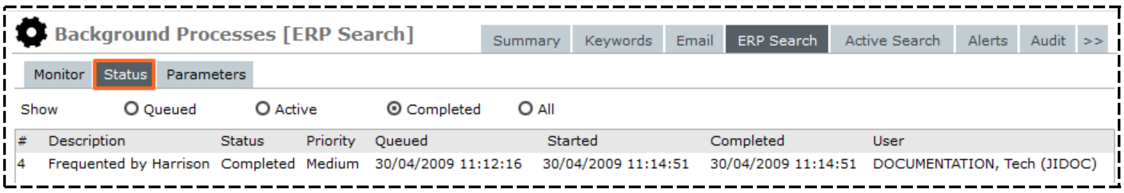


See the Status of the ERP Search Background Process

1. Select **Admin** > **System** > **Background Apps**.
2. Select the **ERP Search** tab.
3. Select the **Status** subtab.

   You'll see ERP searches that are complete or waiting to be processed.

4. To specify the ERP searches you want to see, select one of these options:
   - **Queued** – Only see queued ERP search requests.
   - **Active** – Only see active ERP search requests.
   - **Completed** – Only see completed ERP search requests.
   - **All** – See all ERP search requests.
5. Select **Refresh** to refresh the status list.
6. To see details about the ERP search:
   a. Select the search.
   b. Click **Select**.



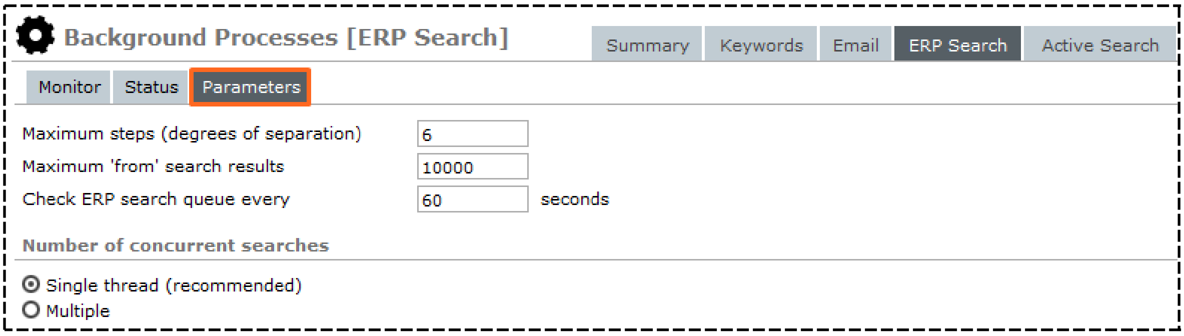
Set up Parameters for ERP Search Background Process

1. Select **Admin** > **System** > **Background Apps**.
2. Select the **ERP Search** tab.
3. Select the **Parameters** subtab.
4. In the **Maximum steps (degrees of separation)** field, enter the maximum number of degrees of separation to display in the ERP search results.
5. In the **Maximum 'from' search results** field, enter the maximum number of ERP search results that are returned.

   If the number of search results exceeds the specified value, the search is abandoned.
6. In the **Check ERP search queue every** field, enter the number of seconds between which the ERP search background process checks for queued ERP search requests.
7. In the **Number of concurrent searches** area, select either of these options to specify how the ERP Search BGP should process concurrent ERP search requests:
   - **Single thread** to do concurrent searches as a single thread process.

     We recommend you use this option.
   - **Multiple** to do concurrent searches as a multiple thread process.

     Enter the number of worker controllers that should process ERP search requests.
8. Select **Save**.



Active Search

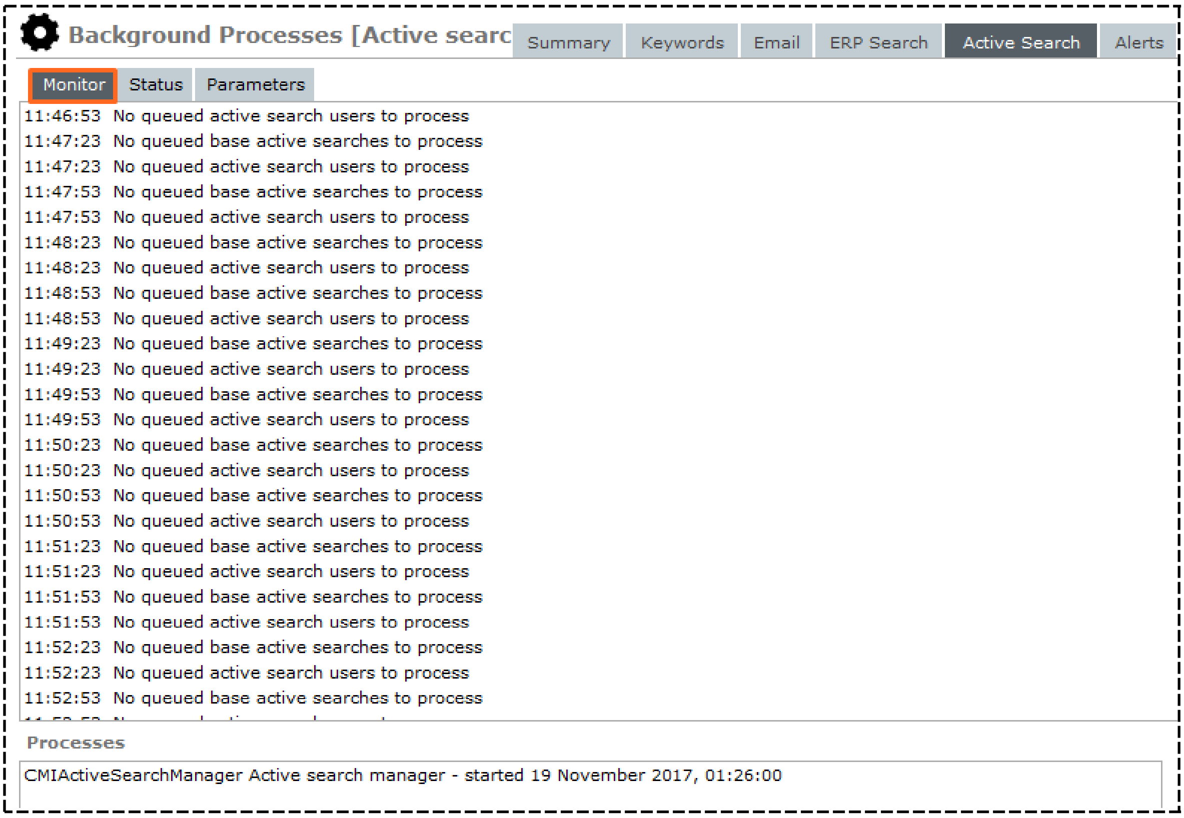
The Active Search background process does active searches.

Monitor the Active Search Background Process

1. Select **Admin** > **System** > **Background Apps**.
2. Select the **Active Search** tab.

   You'll see details about when the Active Search background process was started or stopped and which search managers are active.

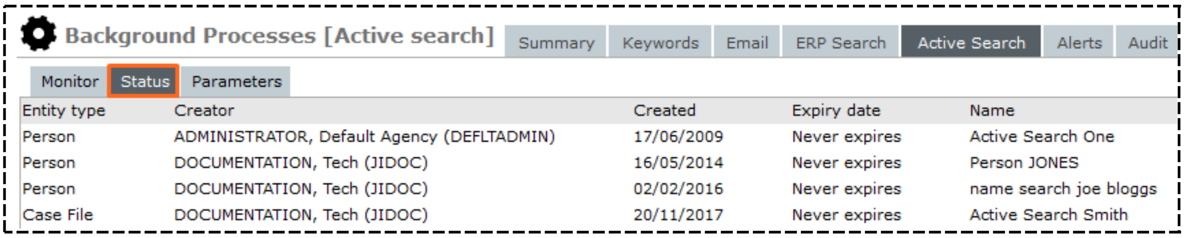
   *The **Processes** area shows the processes that are running.*



Check the Status of the Active Search Background Process

1. Select **Admin** > **System** > **Background Apps**.
2. Select the **Status** tab.

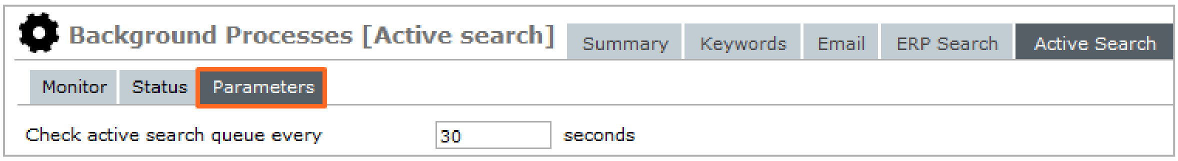
   You'll see active searches that are complete or waiting to be processed.
3. To refresh the status list, select **Refresh**.



Set Parameters for the Active Search Background Process

1. Select **Admin** > **System** > **Background Apps**.
2. Select the **Parameters** tab.
3. In the **Check active search queue every** field, enter how many seconds there should be between the Active Search background process checking for queued active search requests.

   *More seconds means a longer the delay between active searches. If you need active searches to return results sooner, enter a smaller number like **10**, for example.*
4. Select **Save**.



Alerts

You can check how alerts are being processed and any backlog.

Monitor the Alerts Background Process

1. Select **Admin** > **System** > **Background Apps**.
2. Select the **Alerts** tab.

   You'll see when the alerts background process started or stopped and which processes are active.

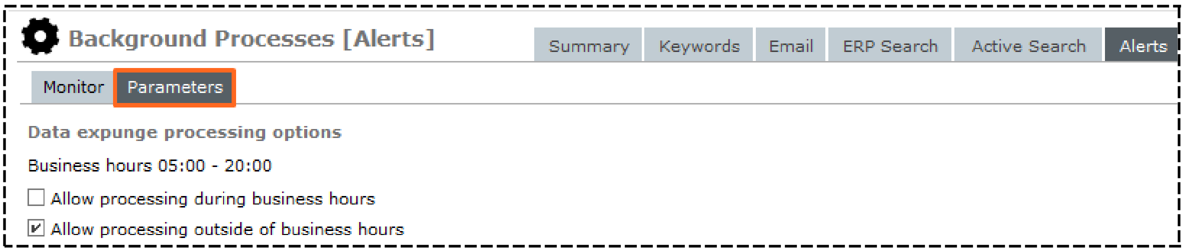
   If you stop the alerts background process, system-generated alerts won't be sent to users.

Set up Parameters for the Alerts Background Process

1. Select **Admin** > **System** > **Background Apps**.
2. Select the **Alerts** tab.
3. Select the **Parameters** subtab.
4. To allow processing to happen during business hours, select the **Allow processing during business hours** checkbox.

   If the background process runs during business hours, there will be a five second pause when each entity is expunged.

   If neither checkbox is selected, the expunge background process won't run.
5. Select **Save**.



About the Data Expunge Background Process

- The process runs daily
- Expunges all entities that have been marked for expunging.
- Finds all entities that have retention periods that have lapsed for the current day.

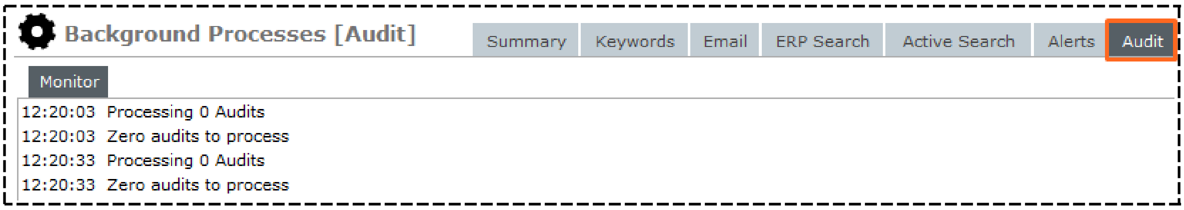
  *If the business process has the **Automatic Deletion** option selected in the Retention Criteria for the current entity type, all entities found are expunged by a background process without any notification to the relevant user.*

  *If the business process has the **Review** option selected, a background process includes all found entities in the review list and generates alerts for the reviewer or reviewers.*
- Recalculates the retention period for all entities if the period has been changed for the related retention criteria setup.

Check Processing of Auditing Data and Any Backlog

1. Select **Admin** > **System** > **Background Apps**.
2. To see what data has changed, select the **Audit** tab.

   The Processes pane area shows any processes that are running.



Monitor the File Load Background Process

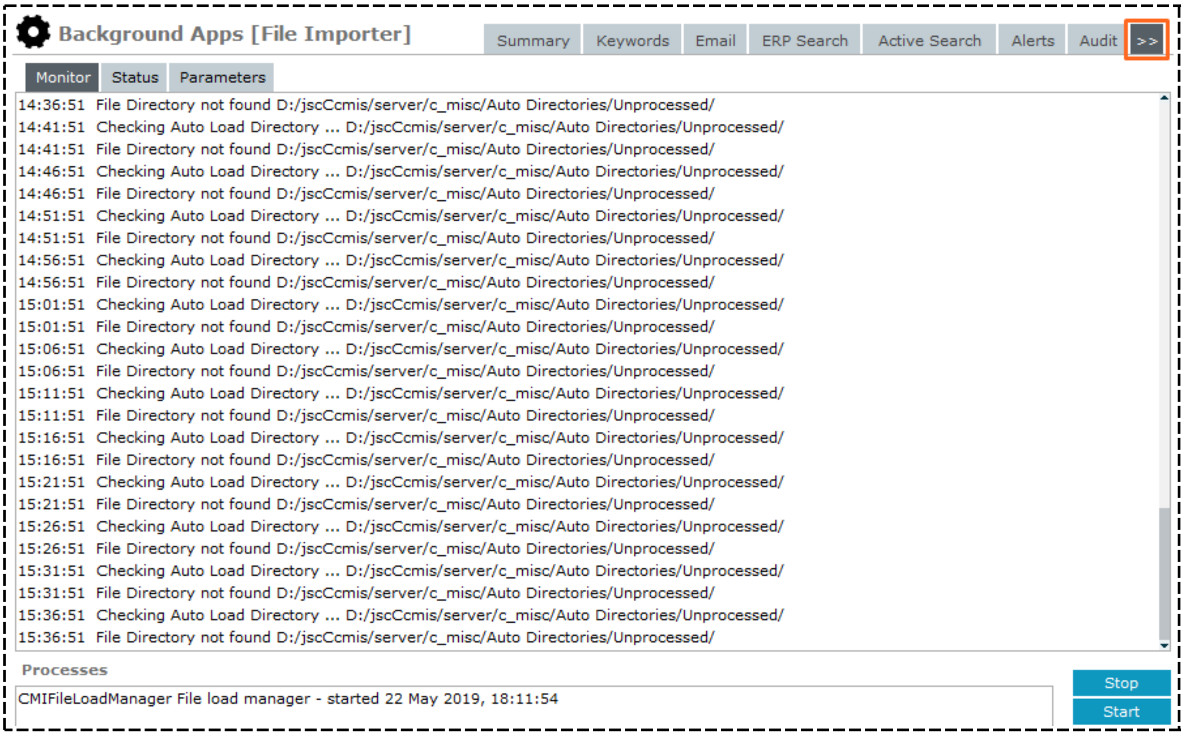
The File Load background process imports files into source entities.

To monitor this process:

1. Select **Admin** > **System** > **Background Apps**.
2. Select the Overflow >> tab > Select **File Importer**.

   You'll see when the process started or stopped and messages from the processes that are running.

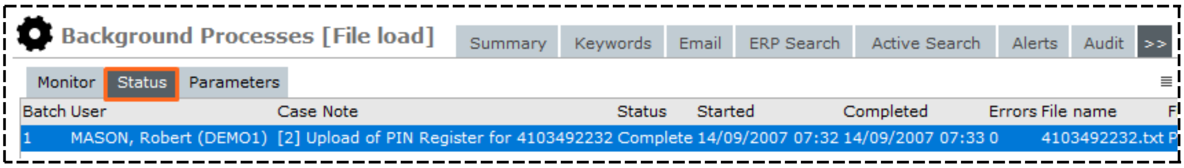
   If you stop the File Load background process, users won't be able to import files.



Check Status of File Load Background Process

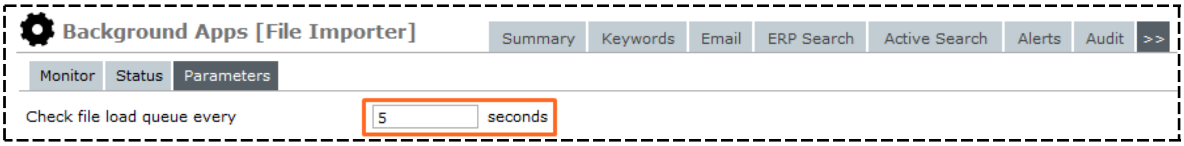
1. Select **Admin** > **System** > **Background Apps**.
2. Select the Overflow >> tab > Select **File Importer**.
3. To see the files are waiting to be imported into the database and the files that have already been imported, select the **Status** subtab.

   *To refresh this list, select **Refresh**.*



Specify Parameters for the File Load Background Process

1. Select **Admin** > **System** > **Background Apps**.
2. Select the Overflow >> tab > Select **File Importer**
3. Select the **Parameters** subtab.
4. In the **Check file load queue every** field, enter the number of seconds between which the File Load background process checks for queued file load requests.
5. Select **Save**.

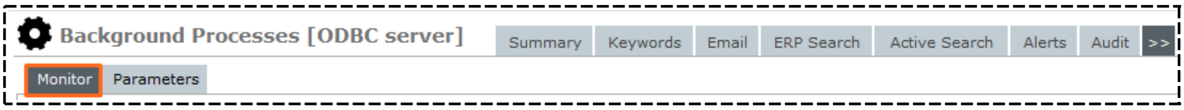


ODBC server

The ODBC server enables processes to access an external relational database.

To see how database requests are processed to an external database:

1. Select **Admin** > **System** > **Background Apps**.
2. Select the Overflow >> tab > Select **ODBC Server**.



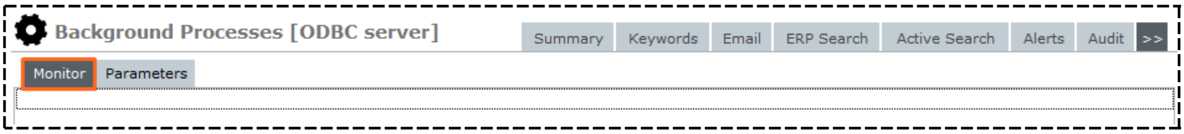
Monitor the ODBC Server Background Process

To see when the ODBC server background process started or stopped:

1. Select **Admin** > **System** > **Background Apps**.
2. Select the Overflow >> tab > Select **ODBC Server**.

   You'll see any messages from active processes.

   If you stop the ODBC server background apps, scheduled housekeeping and tasks that rely on a connection to an external database can't be done.



Set Up Parameters for the ODBC Server Background Process

1. Select **Admin** > **System** > **Background Apps**.
2. Select the Overflow >> tab > Select **ODBC Server**.
3. Select the **Parameters** tab.
4. To enable the ODBC server, select the **ODBC enabled** checkbox.
5. In the **Listen host name** field, enter the Internet Protocol (IP) address on which the ODBC server listens for queries from external tools > Enter either of these options:
   - An IP address – For example, **143.96.124.74**
   - A host name – For example, **lajd0005**

   If you don't enter a value, the IP address will be set to 0.0.0.0. This means the ODBC server will listen on all interfaces.
6. In the **Listen Port** field, enter the port number the ODBC server listens to for queries from external tools.

   Enter a value between 49152 and 65534 in this field – See www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml.

   Make sure the specified port doesn't conflict with any other Transmission Control Protocol (TCP) service running on the host machine.

   The port you specify must be open on the host machine and included in the relevant firewall rules.
7. In the **Read timeout (seconds)** field, enter the number of seconds after which an unserviced network read request (query) ends.

   The default value of zero means no timeout is imposed.
8. In the **Minimum workers** field, enter the minimum number of ODBC worker processes that can run to process external queries.

   The default value is two. This is the minimum value.
9. In the **Maximum workers** field, enter the maximum number of ODBC worker processes that can run to process external queries.

   We don't recommend you use a value higher than 5.
10. In the **Queue depth limit** field, enter the number of queued ODBC processes allowed.

    The default value is zero. This means no additional ODBC worker controllers are started.
11. In the **Queue depth limit timeout (seconds)** field, enter the maximum number of seconds a queued ODBC process waits before a new ODBC worker process is started.

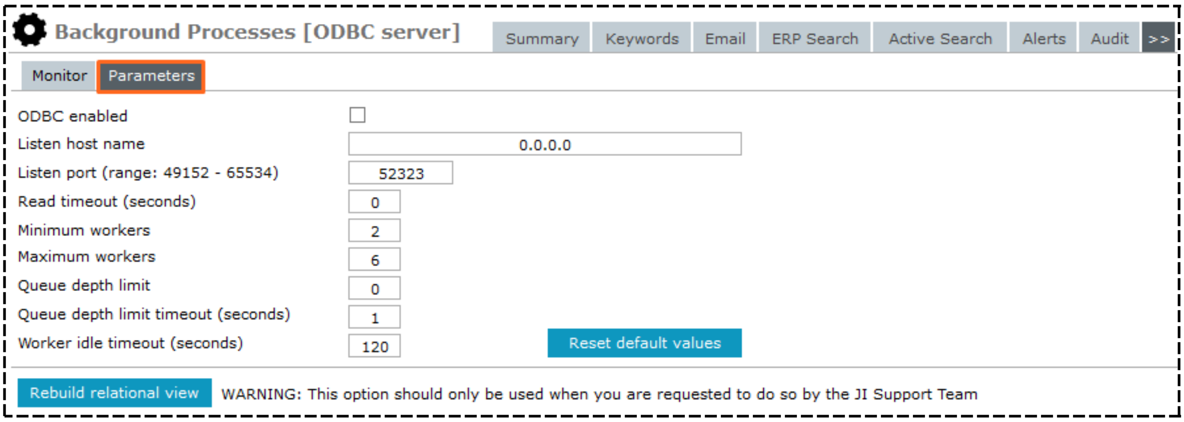
    The default value is one second.
12. In the Worker Idle Timeout (seconds) field, enter the number of seconds of inactivity after which an ODBC worker process ends.

    The default value is 120 seconds.

An idle ODBC worker process only ends if the total number of ODBC worker processes exceeds the specified minimum number of workers.

13. Select **Save**.

14. To monitor the ODBC server BGP, select the **Monitor** tab.



Monitor the Backup and Housekeeping Process

1. Select **Admin** > **System** > **Background Apps**.

2. Select the Overflow >> tab > Select **Backup & Housekeeping**.

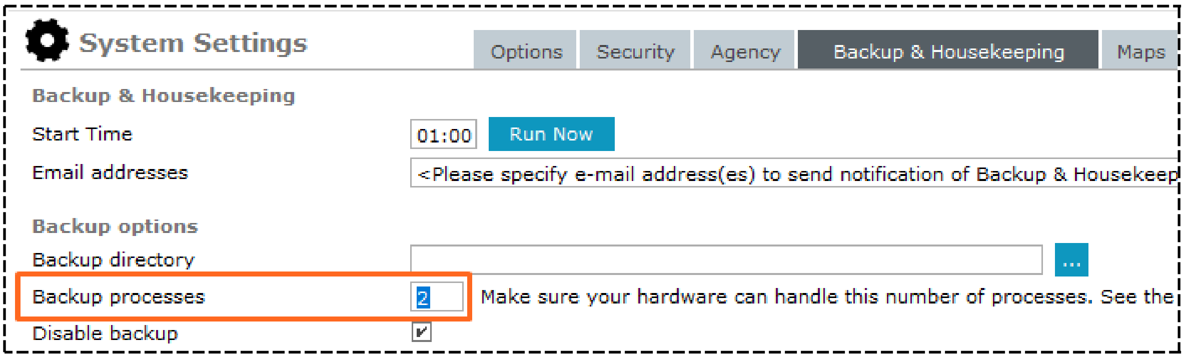
   You'll see when the Backup & Housekeeping background process started or stopped and the processes that are active.

   If you stop the Backup and Housekeeping background process, scheduled housekeeping and backup tasks can't be done.

Speed up Your Backups

1. Select **Admin** > **System** > **Settings**.
2. Select the **Backup & Housekeeping** tab.
3. Enter the number of backup processes you need in the field provided.

   Make sure your selection matches the data transfer speed your hardware supports. The number of workers should not exceed your number of server CPU cores. Use Windows Task Manager to check disc activity during a backup. If it reaches 100%, reduce the number of backup workers.



Duplicate Entities Identification

The Duplicate Entities Identification background apps identifies potential duplicate entities.

You can monitor the parameters for this background process.

Monitor the Duplicate Entities Identification Background Process

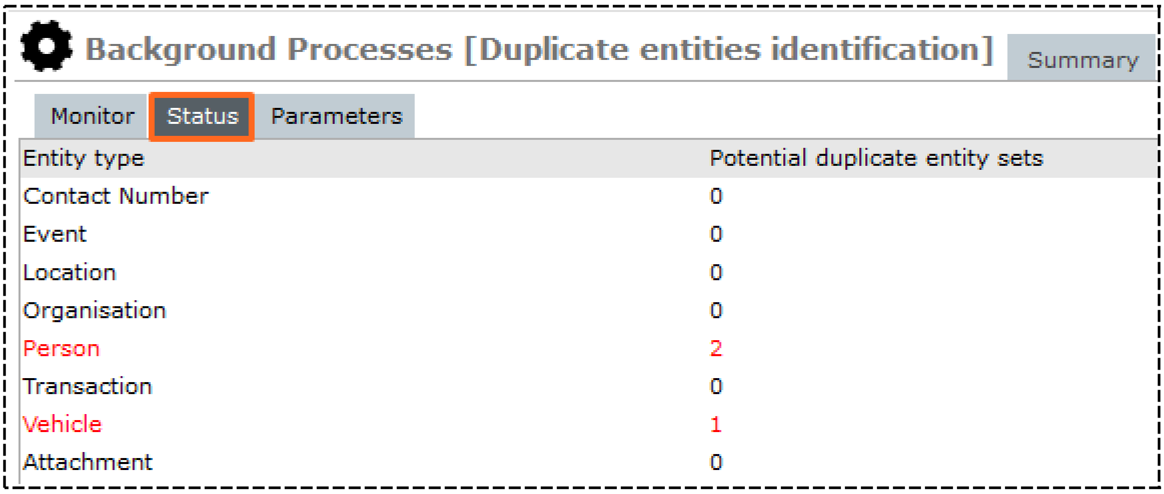
1. Select **Admin** > **System** > **Background Apps**.
2. Select the Overflow >> tab > Select **Duplicate Entities Identification**.

   You'll see when the Duplicate Entities Identification background process started or stopped, and any messages from the processes that are active.

Check Status of Duplicate Entities Identification Background Process

1. Select **Admin** > **System** > **Background Apps**.
2. Select the Overflow >> tab > Select **Duplicate Entities Identification**.
3. Select the **Status** subtab.

   You'll see all the types of entities in the database. Those with potential duplicate entity sets have red text.
4. To refresh the status list, select **Refresh**.
5. To merge duplicate entities, use either of these methods:
   - Select the entity type > Click **Select**.
   - Double-click the entity type.
6. Merge any duplicate entities.



Entity type	Potential duplicate entity sets
Contact Number	0
Event	0
Location	0
Organisation	0
Person	2
Transaction	0
Vehicle	1
Attachment	0

Setting up Parameters for the Duplicate Entities Identification Background Process

You can set up parameters for the Duplicate Entities Identification background process.

For each entity type, you can run either of these scans when searching for potential duplicate entities:

- **Normal scan** – Only checks recently created or updated entities for potential duplicates.
- **Deep scan** – Checks all entities for potential duplicates. Deep scan is automatically used:
  - The first time you run the Duplicate Entities Identification background process
  - When you've changed the unique attributes for an entity type.

Two entities are considered potential duplicates if the unique attributes specified for the entity type are an exact match.

We recommend you use the normal scan when you run the Duplicate Entities Identification background process. If you use the deep scan, it's likely the background process won't finish scanning the entities of the selected entity types within the specified time. The background process will stop and then resume scanning at the last scanned entity when the next Start Time is reached.

Set up Parameters of Duplicate Entities Identification Background Process

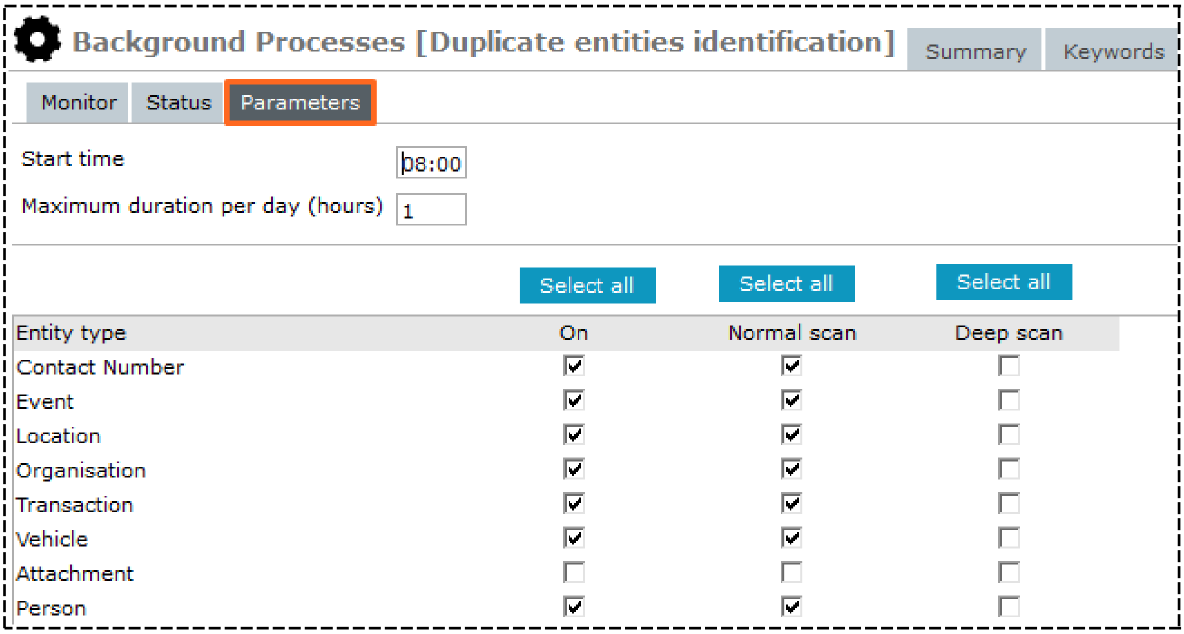
1. Select **Admin** > **System** > **Background Apps**.
2. Select the Overflow >> tab > Select **Duplicate Entities Identification**.
3. Select the **Parameters** subtab.
4. In the **Start time** field, enter the time you want to run the duplicate entities identification process each day.

   We recommend you schedule the Duplicate Entities Identification background process to run when ICM isn't busy.
5. In the Maximum duration per day (hours) field, enter the maximum number of hours you want the duplicate entities identification process to run for.

   The maximum value you can enter is **23**.
6. Select the entity types you want to include in the duplicate entities identification process:
   - To include all entity types, click **Select all** above the *On* column.
   - To deselect all entity types, click **Unselect all** above the *On* column.
   - To select individual entity types, select the corresponding checkbox of each entity type in the *On* column.
   - To deselect an entity type, deselect the corresponding checkbox in the *On* column.

     When you select an entity type in the On column, the corresponding checkbox for that entity type in the Normal Scan column is also selected.
7. Select the type of scan you want to use in the duplicate entities identification process.

   To select the:
   - Normal scan for all entity types, click **Select all** above the *Normal* scan column.
     - *To deselect the normal scan for all entity types, click **Unselect all** above the Normal scan column.*
   - Deep scan for all entity types, click **Select all** above the *Deep scan* column.
     - *To deselect the deep scan for all entity types, click **Unselect all** above the Deep scan column.*
8. Select **Save**.

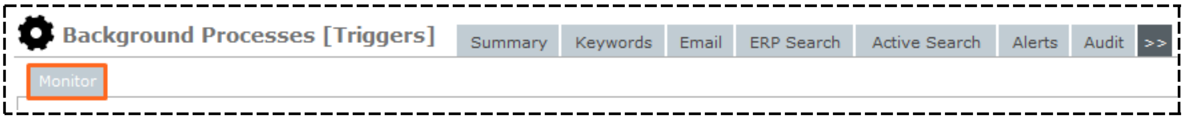


Monitor the Trigger Background App

To see when the Triggers background process started or stopped, and any messages from the processes that are active:

1. Select **Admin** > **System** > **Background Apps**.
2. Select the Overflow >> tab > Select **Triggers**.

   If you stop the Triggers background process, ICM won't be able to send out alerts when the trigger conditions are met.



Lazy Update Background Process

The Lazy Update background process offloads processing some types of updates. It does this to improve processing speed and efficiency. This is particularly important when single point collections are being updated.

This feature is usually only used on implementations where several users are entering case notes, tasks, and task results at a rate where they conflict with each other. It's not necessary to enable this feature for smaller implementations.

Process Entity Relationships

The entities processed by the Lazy Update background process include relationships that link these entities with a case:

- Case note
- Information report
- Incident report
- Task
- Task result

Lazy Update Warning

To reduce contention and improve performance, the Lazy Updater updates:

- After five minutes since the last batch was processed.
- When the next batch has more than 200 entries.

The Lazy Updater queues requests for a few minutes before processing them. Because of this small delay, some types of search (like relationship-centric searches) won't return expected results until the appropriate relationship links have been created.

INI File Setting

There's an INI file setting that directs the processing that links entities in a relationship. This is done by the Lazy Update process.

The INI file setting is **[CMIS]**.

LazyUpdateEntityRels=true.

Start or Stop the Lazy Update Process

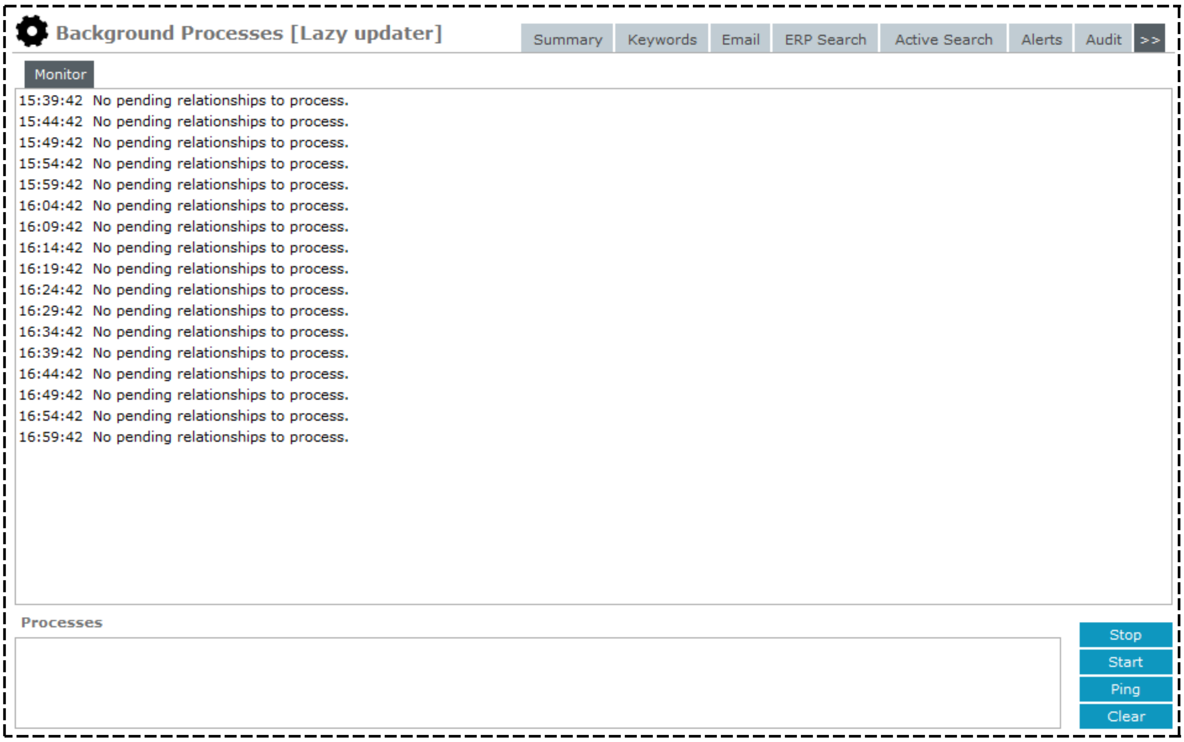
1. Select **Admin** > **System** > **Background Apps**.
2. Select the Overflow >> tab > Select **Lazy Updater**.
3. Start or stop processes as required.

Monitor the Lazy Update Process

1. Select **Admin** > **System** > **Background Apps**.
2. Select the Overflow >> tab > Select **Lazy Updater**.

   You'll see a log of any Lazy Updater activity.

3. Start or stop the process, or select **Ping** to get a status update from the process.



DATA AND TEMPLATES

Permissions control how data is entered, shown, and managed in ICM.

For example, you can:

- Set up source entity templates to standardize how users enter data.
- Ask about changes to data.

  All data edited by users is audited.
- Have screen labels automatically translated to another language.

Templates

You can use data entry templates to standardise how users enter data.

The table explains the templates are available.

Template	What you can do with it
Source entity templates	Specify how source entity data should be entered.
Bookmarked Word templates	Set up the Bookmarked Word reports your agency uses.
Entity-Based Word templates	Set up templates for running reports on case entities with the ability to generate data that's in a hierarchy with repeating group attributes or repeating entity groups.
Disclosure templates	Specify how disclosure schedule data gets mapped to merge fields in a Word template. This allows you to create disclosure schedules that list the evidential documents delivered to the defence from the prosecution.
Dissemination templates	Specify how dissemination schedule data gets mapped to merge fields in a Word template. This allows you to create dissemination schedules that list the evidential documents that are delivered to the defence from the prosecution.
Brief of Evidence templates	Specify the formats of the various documents produced. *The Brief of Evidence feature is optional.*
Word import templates	Set up the Word documents that are templates from which attribute values are imported into report source entities.

To manage the templates for your agency, select **Admin** > **Templates** > **Data Entry**.

Data Entry

You can use source entity templates to define templates for data entry for each of your source entities. Using a template makes sure data is recorded in a uniform way, which makes comparisons and reporting easier.

The **Hide description** template allows you to override the use of source entity templates, if they've been defined.

*See **Preferences** in the user guide.*

*To manage source entity templates, you need the **Can Maintain Description Templates** permission* – For more details, see "Security".

Before you create a new source entity template, you should search to make sure it doesn't already exist.

When you define a source entity template, you can specify the:

- Attributes that are available for inclusion
- Information that displays
- Information users must enter when using that source entity template

Edit Source Entity Template

1. Before you add or edit a source entity template, search for that template.
2. If the template doesn't show in your search results, select the Expand + icon on the *Data Entry* screen.

   The template identifier is automatically assigned after you save the template.
3. To manage template details:
   a. Select the **Details**.
   b. In the **Name** field, enter the name of the template.
   c. To deactivate the template, select the **Deactivated** checkbox.

      Users won't be able to use the template but it can be used for reporting purposes.
   d. In the **Description** field, enter a description of the template.

      The description should give users enough information to decide whether that template is correct for the intended use.
   e. In the **Applies to** pane, select one or more source entities that this template can be applied to.

      If you select the top-level source entity type—for example, Incident Report or Case Note— all the lower-level source entities are disabled.

      Any changes you make to the template are applied to all the lower-level source entities.
   f. To design the layout of the screen data will be added to, enter the required details on the **Content** screen.
4. When you've made the required changes, select **Save**.
5. To save the template with a different name:
   a. In the *Name* field, enter the name of the template.
   b. Select **Copy as new**.
6. If you changed an existing template, you must activate the changes you made.

   You'll see a warning at the bottom of the *Details* screen if you save a template whose changes haven't been activated.
   a. Select the **Content** tab.

      Select the **Activate Changes** checkbox.
   b. Select **Save**.

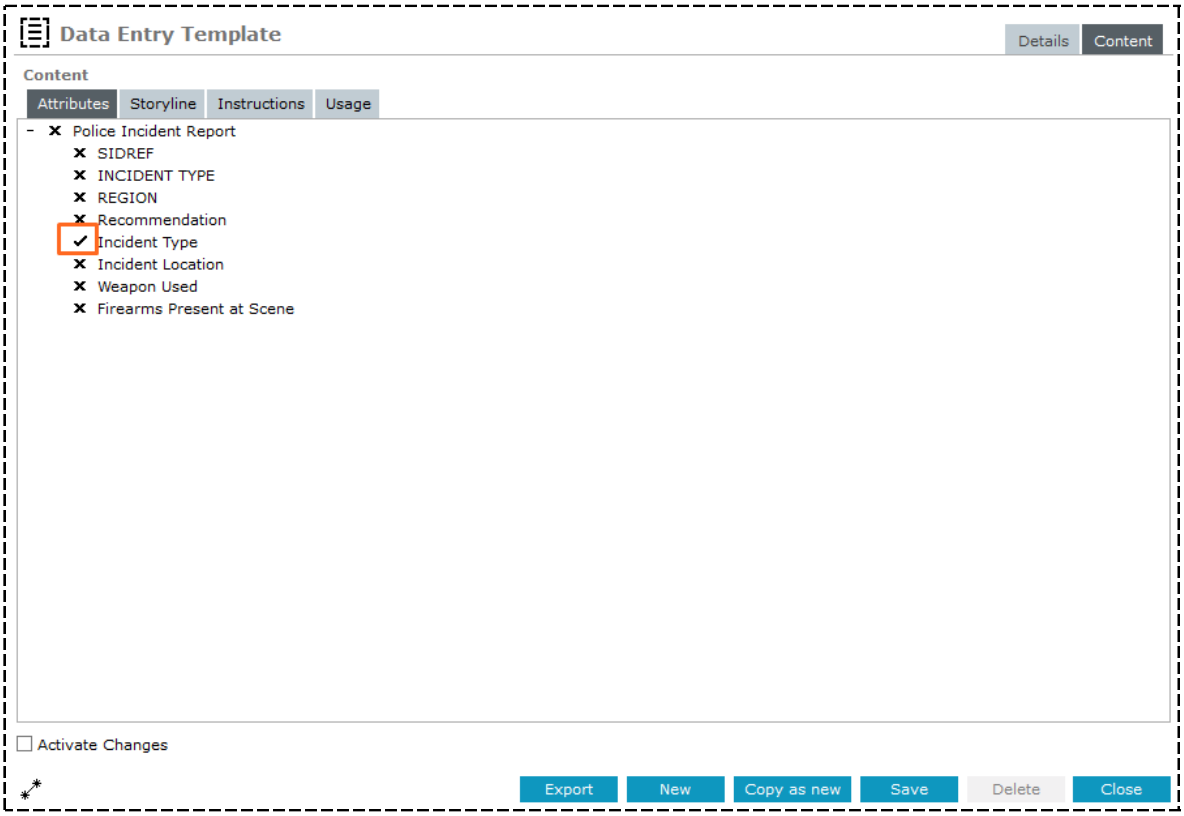
Edit Template Attributes

You can manage the attributes of a source entity template. The attributes you select will be available to users when they use the template.

To manage template attributes:

1. Select **Admin** > **Templates** > **Data Entry**.
2. Search for the template.

   *For details about selecting a source entity template, see **Searching for a source entity template**.*
3. Select the **Content** tab.
4. To see the default attributes associated with the source entity, select the **Attributes** subtab.
5. To include an attribute in the template, select the Expand + icon so it becomes a Check mark ✓ icon.
6. Select **Save**.



Edit Storyline Content

You can specify the:

- Content – The information users should enter.
- Formatting information – How this displays in the *Description* field of the source entity after users enter it.

To manage template storyline details:

1. Select **Admin** > **Templates** > **Data Entry**.
2. Open the source entity template.

   See Searching for a Source Entity Template.
3. Select the **Content** tab.
4. Select the **Storyline** subtab.
5. Specify and format the template data fields (or input placeholders).

   An input placeholder identifies where information will show on the template.
6. Select the **Instructions** subtab to specify the type of information (for example, numbers only) and enter any special instructions for users.
7. Enter headings and titles to show source entity information.
8. To add an input placeholder:
   a. Position your cursor where you want to add a placeholder.

      *For example, beside **Name**.*

   b. Select **Add Input**.

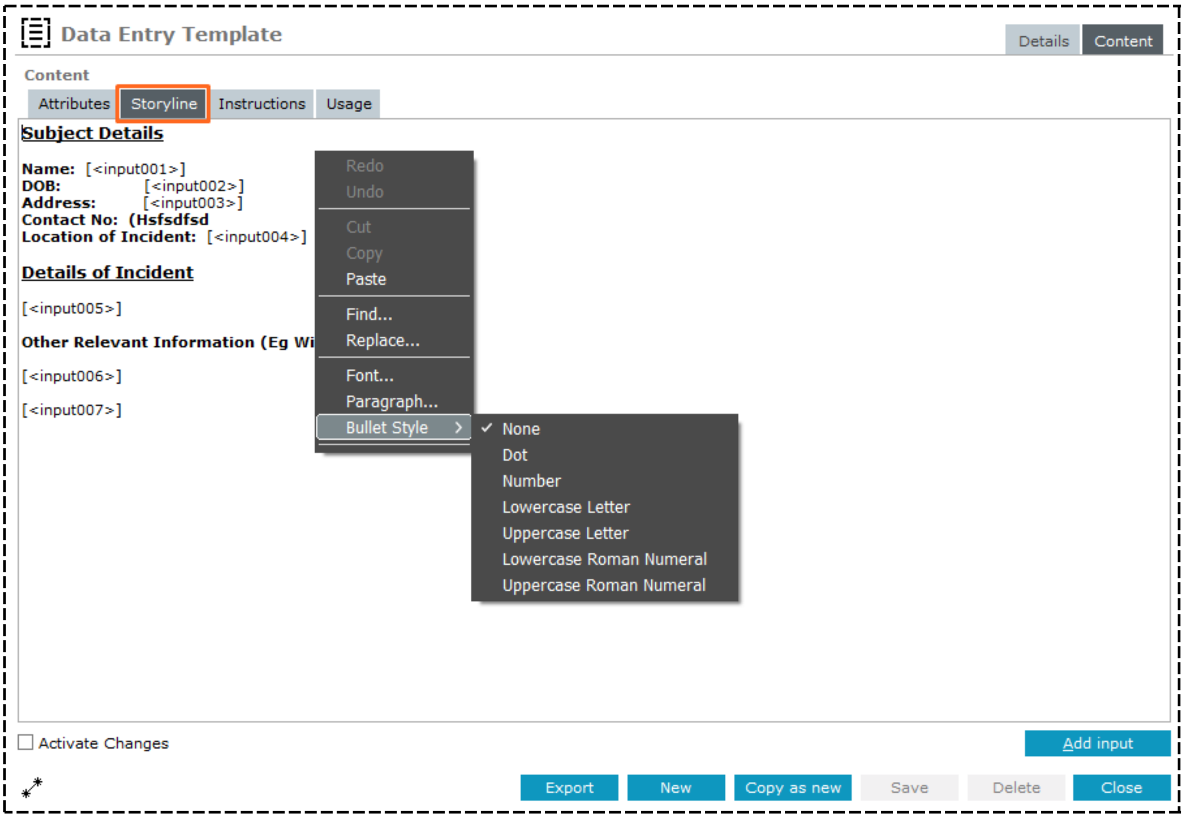
      The placeholder has the following format: [<input>] Use the Instructions screen to specify details about that placeholder.

      For example, whether it needs text or a date format input.
9. Format the text according to how you want it to be displayed.
   a. Select the word or line you want to format.

   b. Right-click > Select the required command from the popup menu that displays.

      The formatting is then applied to the selected text (including input placeholders).

      If you want to change the size of the input placeholder text, you must select the entire placeholder, including the square brackets ([ ]), before changing the font size.
10. When you've made the required changes, select **Save**.


Data Entry Template
Details
Content
Content
Attributes
Storyline
Instructions
Usage
Subject Details
Name: [<input001>]
DOB: [<input002>]
Address: [<input003>]
Contact No: (Hsfsdfsd
Location of Incident: [<input004>]
Details of Incident
[<input005>]
Other Relevant Information (Eg Wi
[<input006>]
[<input007>]
Redo
Undo
Cut
Copy
Paste
Find...
Replace...
Font...
Paragraph...
Bullet Style
None
Dot
Number
Lowercase Letter
Uppercase Letter
Lowercase Roman Numeral
Uppercase Roman Numeral
Activate Changes
Add input
Export
New
Copy as new
Save
Delete
Close

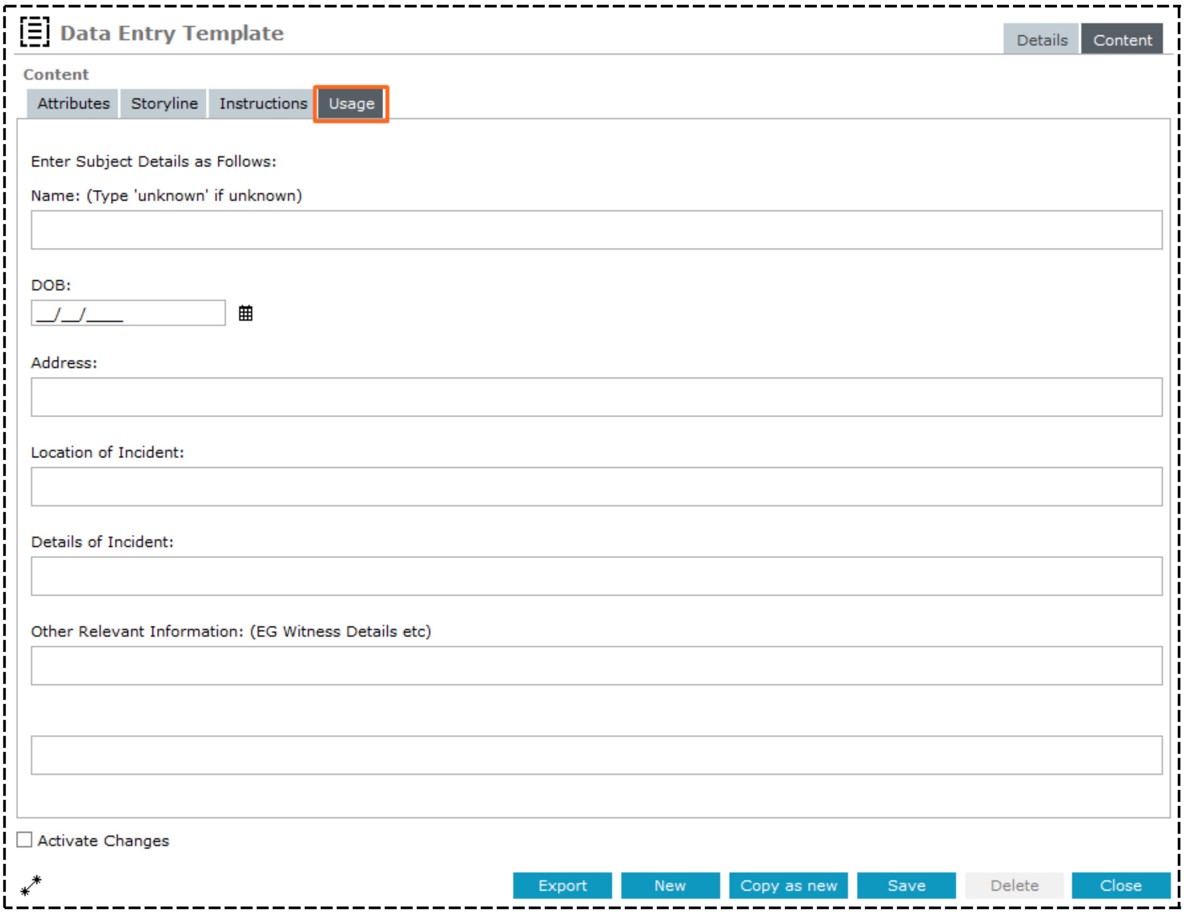
Preview a Template

You can preview a source entity template.

*Input fields won't show until you've completed the required actions under the **Storyline** and **Instructions** tabs.*

To preview a template:

1. Open the template.
2. Select the **Content** tab.
3. Select the **Usage** subtab.



Bookmarked Word Reports

You can use bookmarked Word templates to design your own reports that generate information about specified entities. The file format for this is a Microsoft Word document – DOCX.

1. To create a bookmarked Word template, import a Word template.
2. Map entity attributes to the bookmarked fields in that template.

   Your Word template can map attributes from more than one entity to different bookmarks in the underlying document.

*See **Running Bookmarked Word Reports** in the user guide.*

*To manage Bookmarked Word templates, you need the **Can Maintain Bookmarked Word Reports** permission.*

Grouping Bookmarks

You can use bookmark groups to group data that's to be included in a report.

For example, you could create a group of all the information about a person – First name, surname, date of birth.

Grouping bookmarks helps users visualise what information needs to be in a report before they run it.

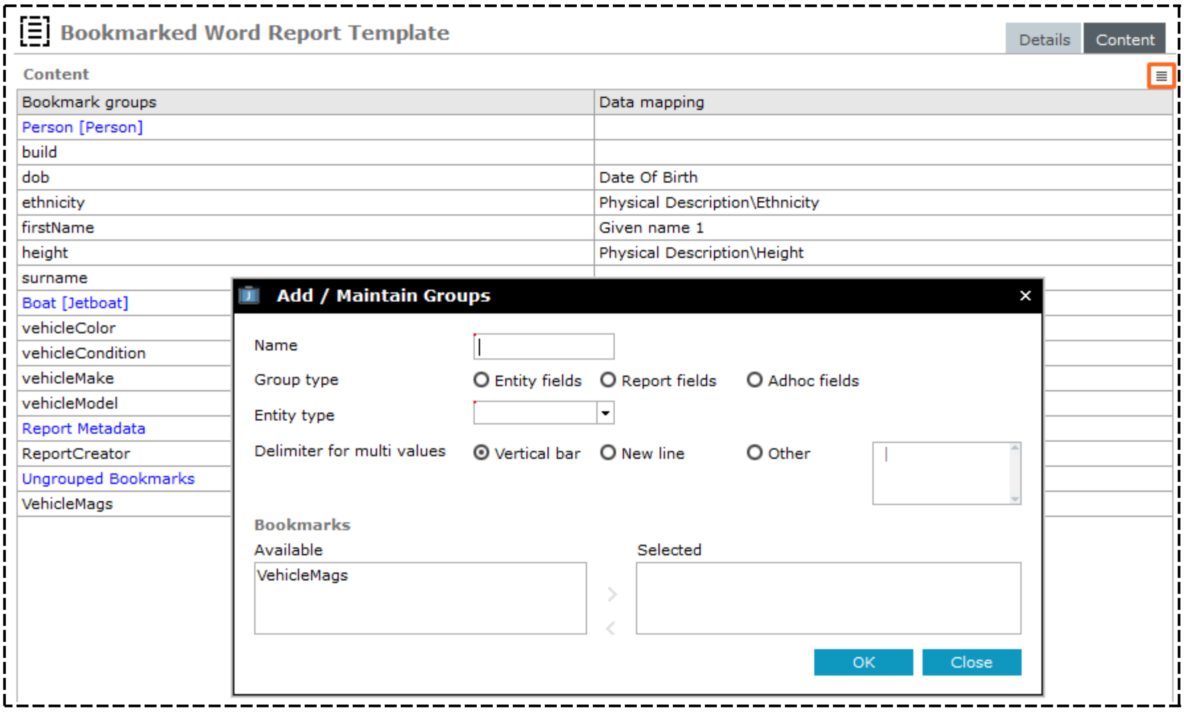
Create a Group of Bookmarks

1. Select **Admin** > **Templates** > **Bookmarked Word Reports**.
2. Open the template you want to edit.
3. Select the **Content** tab.
4. Add a group using either of these options:
   - Select the Options ≡ icon > Select **Add Group** .
   - Right-click the Content table > Select **Add Group**.
5. In the **Name** field, enter the name of the group of bookmarks.
6. In the **Entity** type drop-down, select the type of entity the bookmarks relate to.
7. Use the **Bookmarks** area to select the bookmarks in the Word document you want to include in the group.
8. To include a bookmark:
   a. Select it in the **Available** area.
   b. Select the Select icon button or double-click the selected bookmark.
9. Select **OK**.
10. Select **Save**.

    The group name shows in blue text.

    The entity type shows in square brackets (for example, [Vehicle]) beside the group name.

    Bookmarks that are part of that group are listed under the group name.
11. Once you've added a bookmark to a group, link it to the entity data that will be generated in the report (map entity data to the bookmarks).



About Ad Hoc Fields

- Ad hoc fields allow for data entry at run-time, whereas Report fields are mapped to database items.
- For example, if you need to show who ran a report, you could map a bookmark in the template to the Report field:

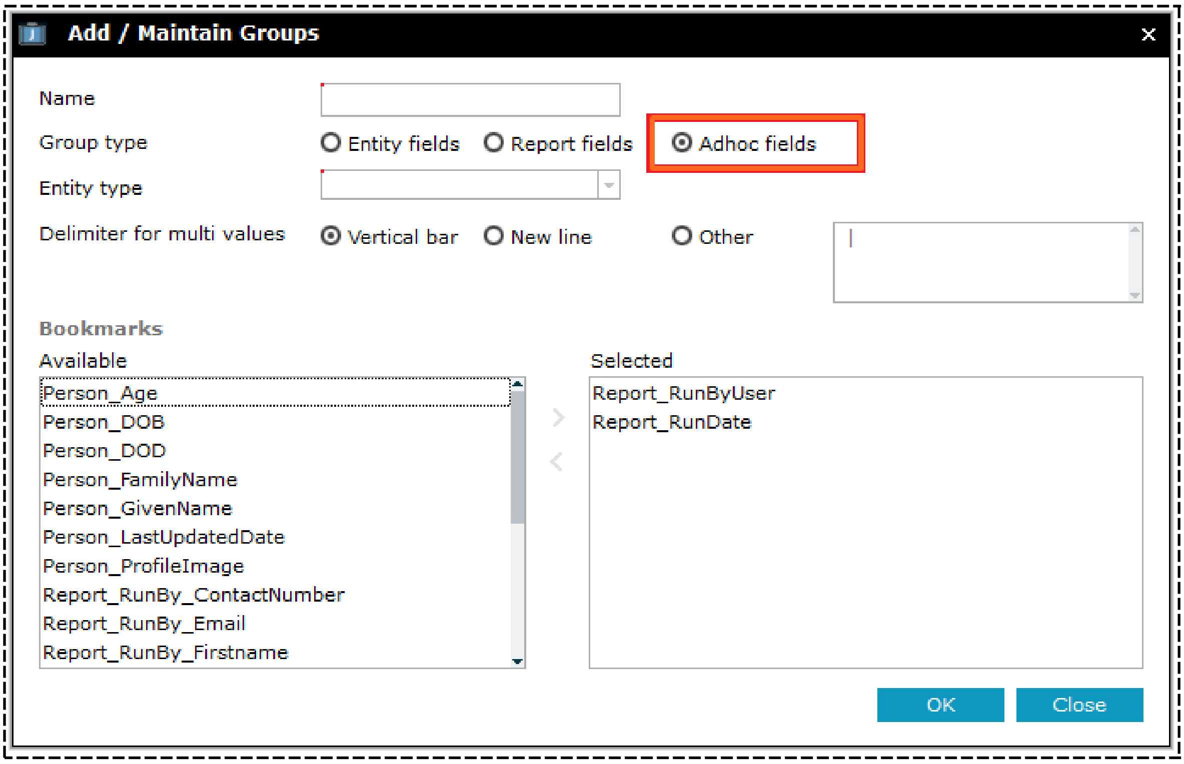
  Run by: <First name> < Surname>

  At run-time the report would automatically populate the report.
- You can achieve the same thing with an ad hoc field. But you need to enter the name of the user when you run the report.

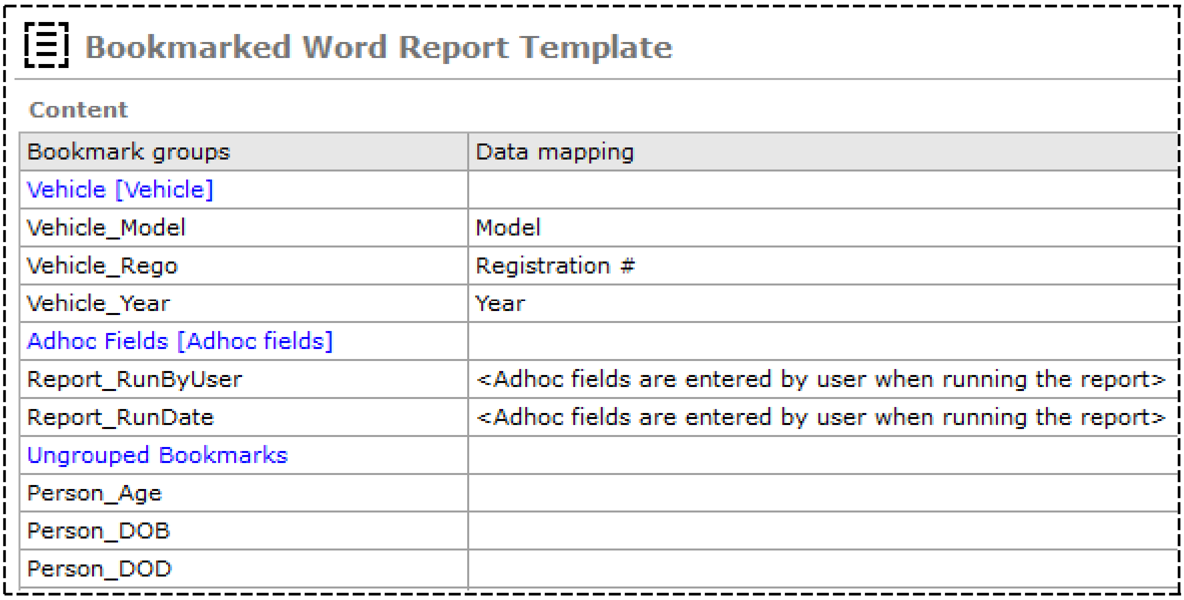
Add Ad Hoc Fields to a Report Template

If you want to include details that are entered by a user at run-time, you can add ad hoc fields to your template:

1. Open the Bookmarked Word Report, or Entity-based Word Report template.
2. Add the mapping:
   a. Right-click in the *Content* area > Select **Add Group**.
   b. Enter a name for the group.
   c. Select **Ad hoc fields** as the group type.



   d. Select the required bookmarks.
   e. Select **OK**.



Bookmarked Word Report Template

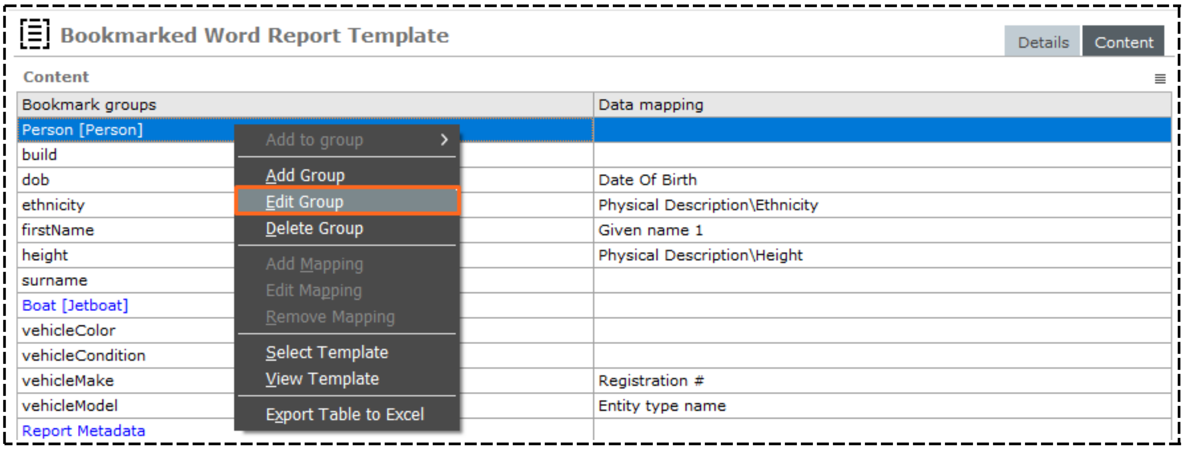
Content

Bookmark groups	Data mapping
Vehicle [Vehicle]	
Vehicle_Model	Model
Vehicle_Rego	Registration #
Vehicle_Year	Year
Adhoc Fields [Adhoc fields]	
Report_RunByUser	<Adhoc fields are entered by user when running the report>
Report_RunDate	<Adhoc fields are entered by user when running the report>
Ungrouped Bookmarks	
Person_Age	
Person_DOB	
Person_DOD	

Edit a Group of Bookmarks

1. Open the template you want to edit.
2. Select the **Content** tab.

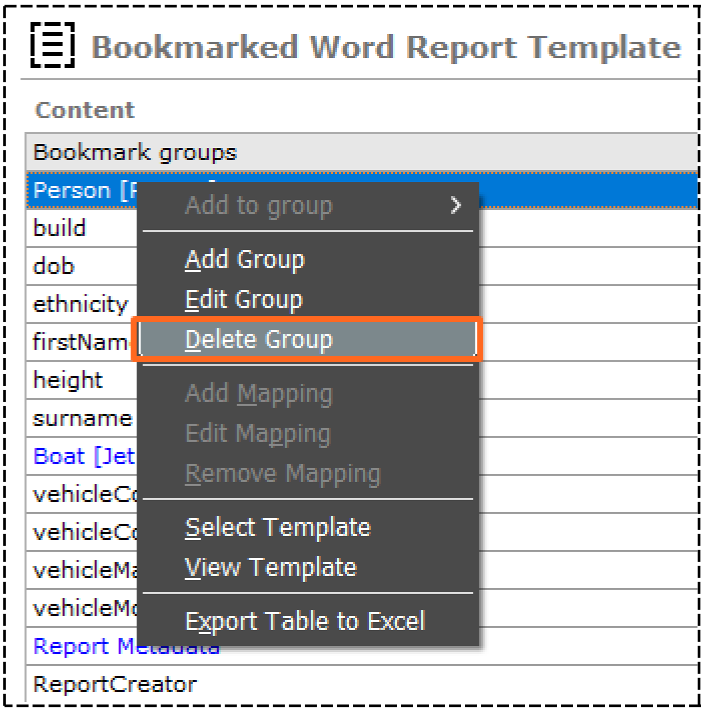
   Select the heading of the bookmark group you want to edit.
3. Use any of these options to edit it:
   - Select the Options icon > Select **Edit Group**.
   - Right-click the Content table > Select the *Edit Group* command from the list that displays.
   - Double-click the selected heading.
4. Edit the required details.
5. Select **Save**.



Delete a Group of Bookmarks

1. Open the bookmarked Word template you want to edit.
2. Select the **Content** subtab.
3. Select the heading of the bookmark group you want to delete.
4. Use either of these methods to delete a group:
   - Select the Options ≡ icon > Select **Delete Group**.
   - Right-click the Content table > Select **Delete Group**.
5. Confirm you want to delete the selected bookmark.

   *Deleting a group doesn't delete its bookmark. Instead they're listed under **Ungrouped Bookmarks**.*
6. Select **Save**.



Map Entity Data to a Bookmark

After you've grouped the bookmarks in a report, you'll need to map entity data to each bookmark.

By mapping entity data to a bookmark, you can specify what entity information should be included in the report.

For Word import templates you can map bookmarks to entity attributes, whose values are imported.

To map entity data to a bookmark:

1. Open the template you want to edit.
2. Select the **Content** subtab.
3. Select the bookmark you want to map entity data to.

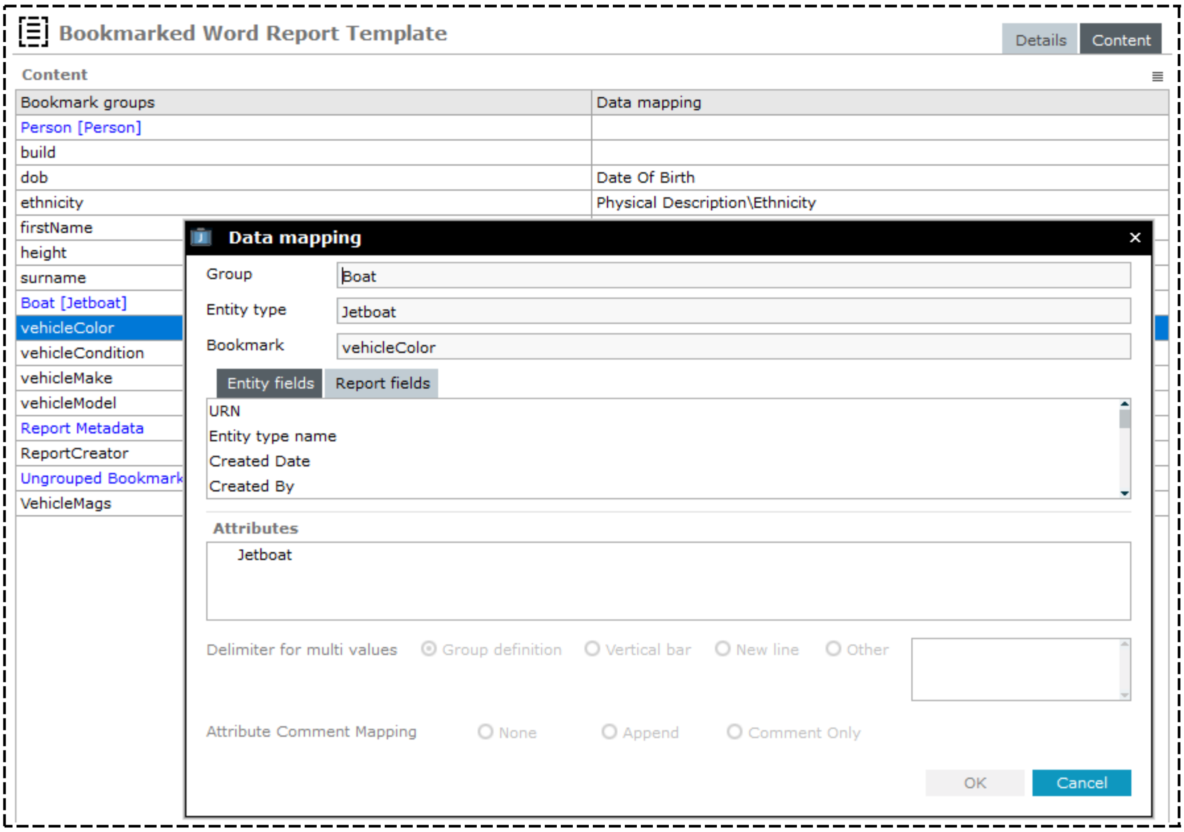
   You can only map one value to one bookmark.
4. Do one of these things:
   - Double-click the bookmark.
   - Select the Options ≡ icon > Select **Add Mapping**.
   - Right-click the **Content** table > Select **Add Mapping**.
5. a. Select the **Content** subtab. The:
      - **Group** field shows the name of the bookmark group.
      - **Entity type** field shows the type of entity you're creating a mapping for.

        The type of entity determines the data you can include in the report.
      - **Bookmark** field shows the name of the bookmark you're mapping entity data to.

   b. Select the bookmark you want to map entity data to.

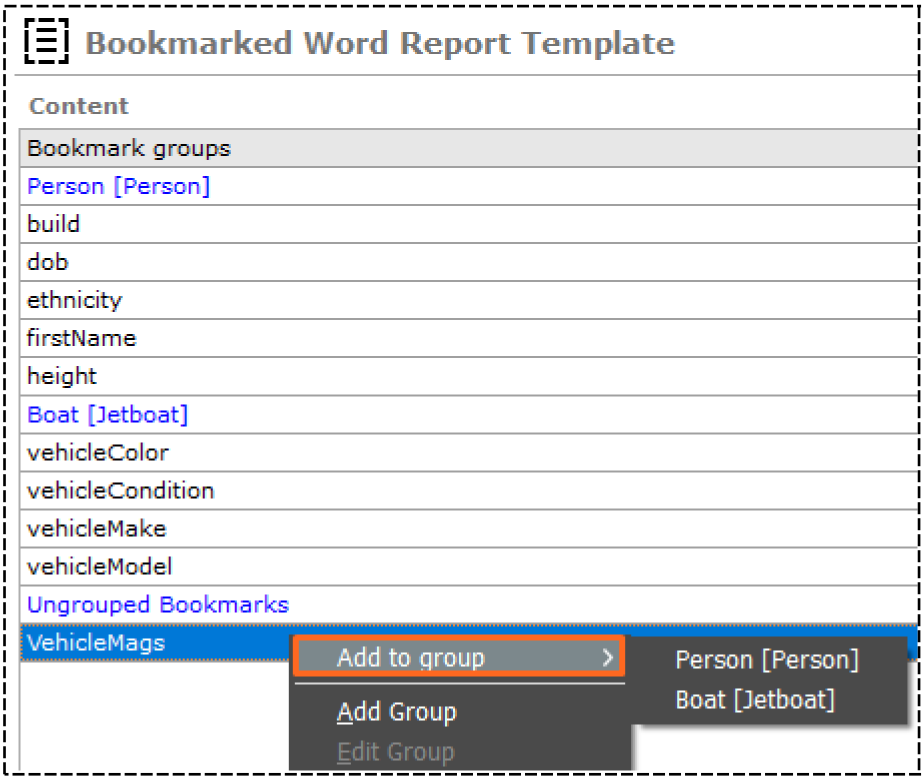
   c. Select **OK**.

   *The selected attribute or field shows in the **Data Mapping** column for that bookmark.*
6. Select **Save**.


Bookmarked Word Report Template
Details
Content
Content
Bookmark groups
Data mapping
Person [Person]
build
dob
Date Of Birth
ethnicity
Physical Description\Ethnicity
firstName
height
surname
Boat [Jetboat]
vehicleColor
vehicleCondition
vehicleMake
vehicleModel
Report Metadata
ReportCreator
Ungrouped Bookmark
VehicleMags
Data mapping
Group
Boat
Entity type
Jetboat
Bookmark
vehicleColor
Entity fields
Report fields
URN
Entity type name
Created Date
Created By
Attributes
Jetboat
Delimiter for multi values
Group definition
Vertical bar
New line
Other
Attribute Comment Mapping
None
Append
Comment Only
OK
Cancel

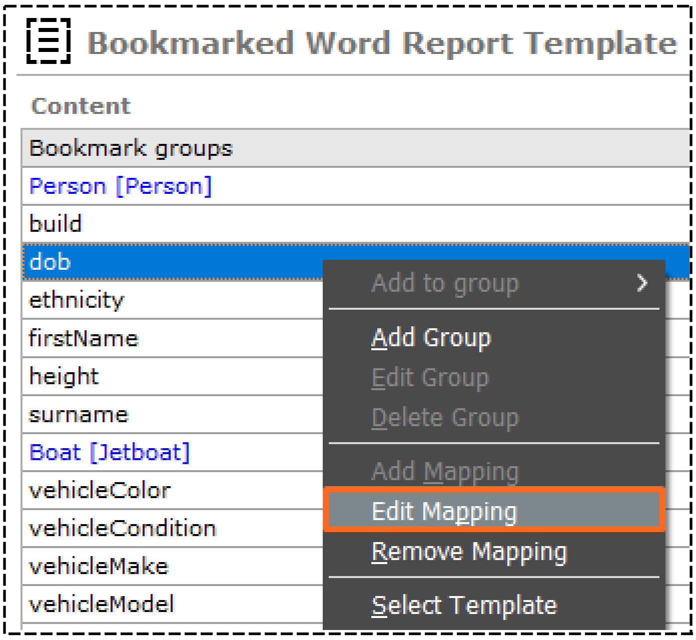
Add an Ungrouped Bookmark to a Group

1. Select **Admin** > **Templates**.
2. Select either of these options:
   - **Bookmarked Word Reports**
   - **Entity-based Word Reports**
3. Right-click an ungrouped bookmark > Select **Add to Group** > Select the existing group you want to add the bookmark to.



Edit Mapped Entity Data

1. Open the template you want to edit.
2. Select the **Content** tab.
3. Select the attribute or field you want to edit.
4. Do one of these things:
   - Double-click the selected attribute or field.
   - Right-click the *Content* table > Select **Edit Mapping**.
   - Select the Options ≡ icon > Select **Edit Mapping**.
5. Make your changes.
6. Select **Save**.

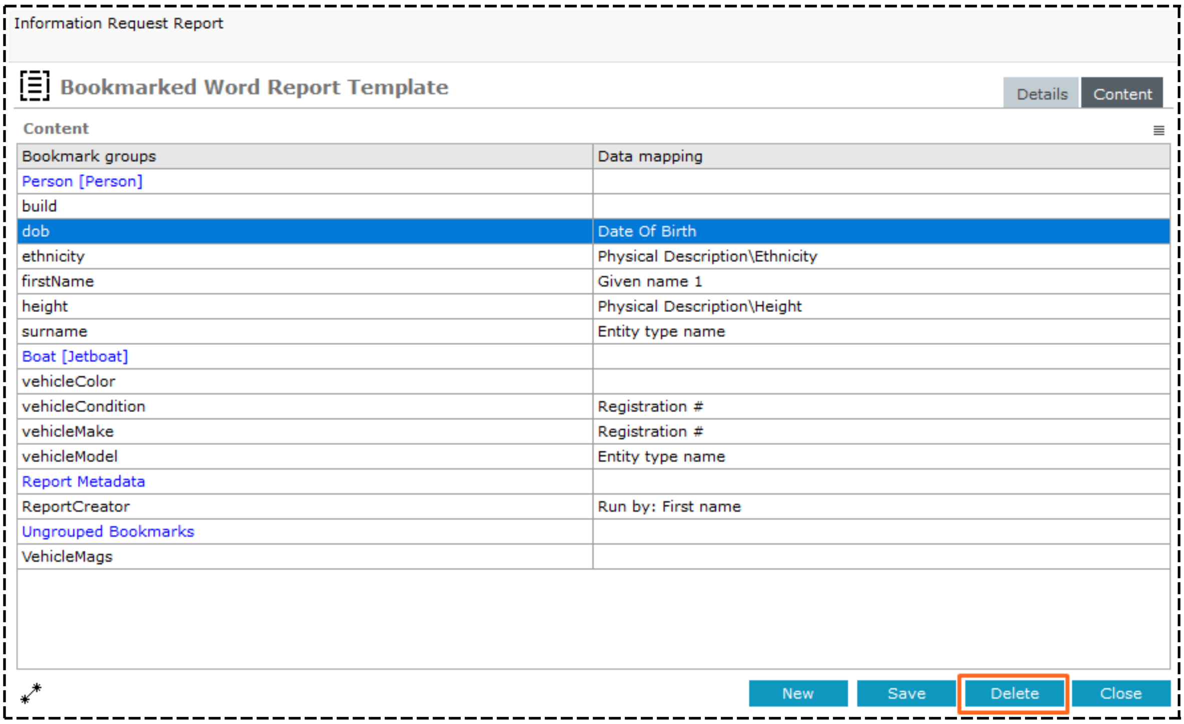


Edit a Bookmarked Word Template

1. Select **Admin** > **Templates** > **Bookmarked Word Reports**.
2. Open the template you want to edit.
3. Make your changes.
4. Select **Save**.

Delete a Bookmarked Word Template

1. Open the template you want to delete.
2. Select **Delete**.
3. Confirm you want to delete the template.



Entity-Based Word Templates

Entity-based Word templates provide flexible reporting of entities and their attributes within a type of case. The report can include multiple child entities of the parent case and multi-valued attributes in a hierarchical structure within each entity.

These are the stages for setting up an entity-based report:

1. Create a Word template file with a bookmark for each hard or soft attribute from the entities you want to report on.

   You'll also specify group bookmarks that define a group of bookmarks that make up an entity.
2. Create an entity-based report definition and select the template you've created.

   This is so the bookmark names can be imported into the definition.
3. Add data mapping definitions to the report definition so each bookmark will have a data source from the entity's hard or soft attributes.
4. Run the report to see if it looks the way you thought it would.

Create an Entity-based Word Template

The procedure to create the template uses the bookmarking feature in Word to lay out the reporting format and provide the links the report needs to merge data with the bookmark fields.

To create an entity-based Word template:

1. Create the layout of the document with the formatting you need, including headers and footers and your agency logo, if required.
2. Add bookmarks for the data that will be inserted in the document when the report runs.
3. Create bookmarks for groups of data items.

   For example, you can have a person group that defines a group of attributes that belong to a person entity. Within that group you can have a tattoos group with multiple values.
4. Save the template file. You'll select it from this location when you create the report definition.

Create an Entity-based Report Definition

1. Select the **Admin** > **Templates** > **Entity-Based Word Reports**.
2. To create a new template report, select the Expand + icon above the *Search* button.
3. Enter a name for the report template in the field provided.
4. Enter a description of the template in the field provided.
5. Select the base type or category in the drop-down provided.

   If you choose the case system entity type or a category, you won't be able to use any of the soft attributes available because system entity types only have hard attributes.
6. Select the **Content** tab > Right-click in the **Content** screen > Click **Select Template**.
7. Locate and select your saved template file > Select **Open**.

   The bookmarks and their hierarchy will show on the ***Content*** *screen.*
8. Select **Save**.

Create Data Mapping Definitions

For each group of bookmarks and bookmark, you'll need to select a data source. This will show in the *Data Mapping* column.

1. Select **Admin** > **Templates** > **Entity-Based Word Reports**.
2. Double-click a bookmark group.
3. Enter data in these fields:
    - **Related entity drop-down**

      Choose a child entity that's related to the parent entity.

      For example, if you select the Person entity, the bookmark group for the related entity chosen will be repeated for each related entity in the report generated. Details of every person entity will be included in the report generated.
    - **Group attribute option**

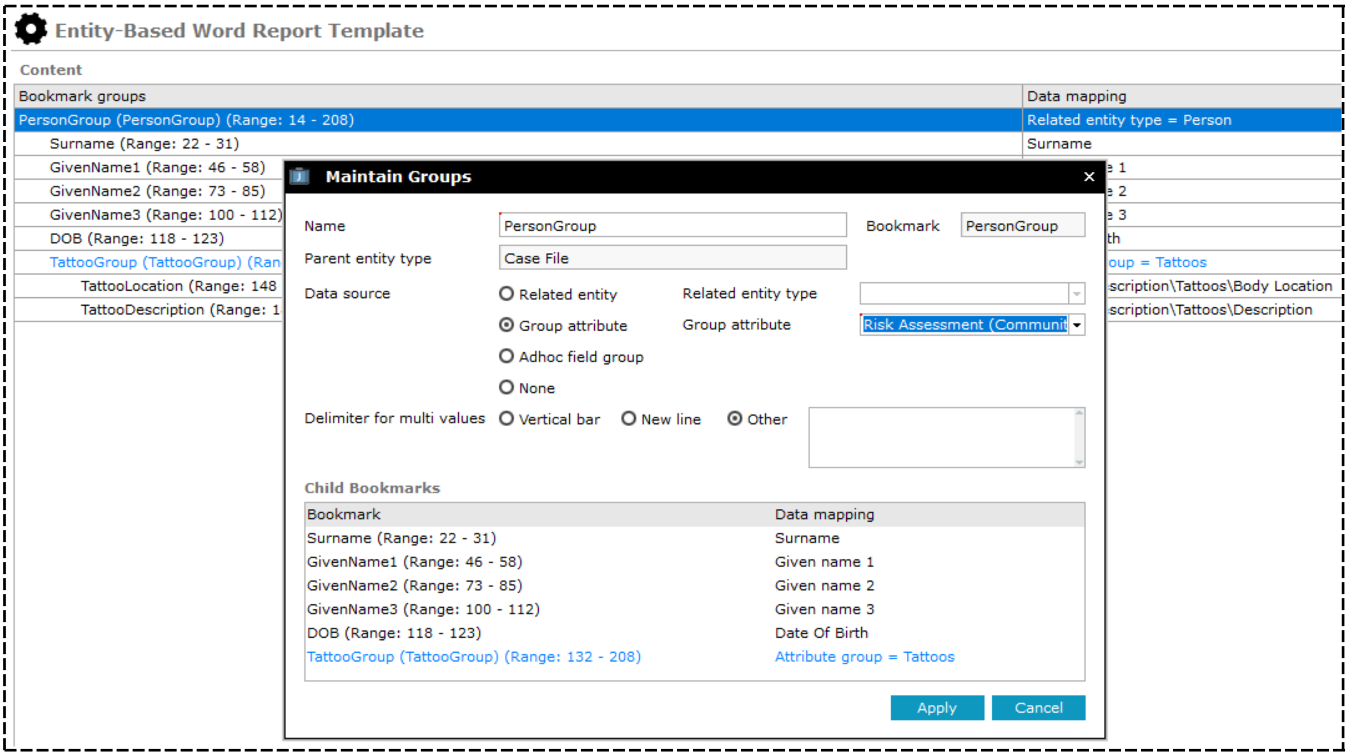
      Choose this option when you want to select an attribute of the child entity of the base entity type.
    - **Group attribute drop-down**

      This is enabled by the Group attribute option being selected. It contains group attribute types in the context of:

      – *The parent group entity type, if the parent data source is an actual entity type.*

      – *The template entity type if there's no parent group and the template entity type is an actual entity type.*
    - **Child Bookmarks**
    - Select **Apply**

      *The data mapping screen shows the mapping of the **PersonGroup** to the **Person Entity**.*


Entity-Based Word Report Template
Content
Bookmark groups
Data mapping
PersonGroup (PersonGroup) (Range: 14 - 208)
Related entity type = Person
Surname (Range: 22 - 31)
Surname
GivenName1 (Range: 46 - 58)
GivenName2 (Range: 73 - 85)
GivenName3 (Range: 100 - 112)
DOB (Range: 118 - 123)
Maintain Groups
Name
PersonGroup
Bookmark
PersonGroup
Parent entity type
Case File
Data source
Related entity
Related entity type
Group attribute
Group attribute
Risk Assessment (Communit
Adhoc field group
None
Delimiter for multi values
Vertical bar
New line
Other
Child Bookmarks
Bookmark
Data mapping
Surname (Range: 22 - 31)
Surname
GivenName1 (Range: 46 - 58)
Given name 1
GivenName2 (Range: 73 - 85)
Given name 2
GivenName3 (Range: 100 - 112)
Given name 3
DOB (Range: 118 - 123)
Date Of Birth
TattooGroup (TattooGroup) (Range: 132 - 208)
Attribute group = Tattoos
Apply
Cancel

Map Normal Bookmarks

1. Select **Admin** > **Templates** > **Entity-Based Word Reports**.
2. Open a template.
3. Select the **Content** tab.
4. Double-click a normal bookmark row in a group.

   *The **Data mapping** screen shows a list of attributes you can select as a data source for the bookmark.*

   *The **Entity Fields** tab shows the entity's hard attributes.*

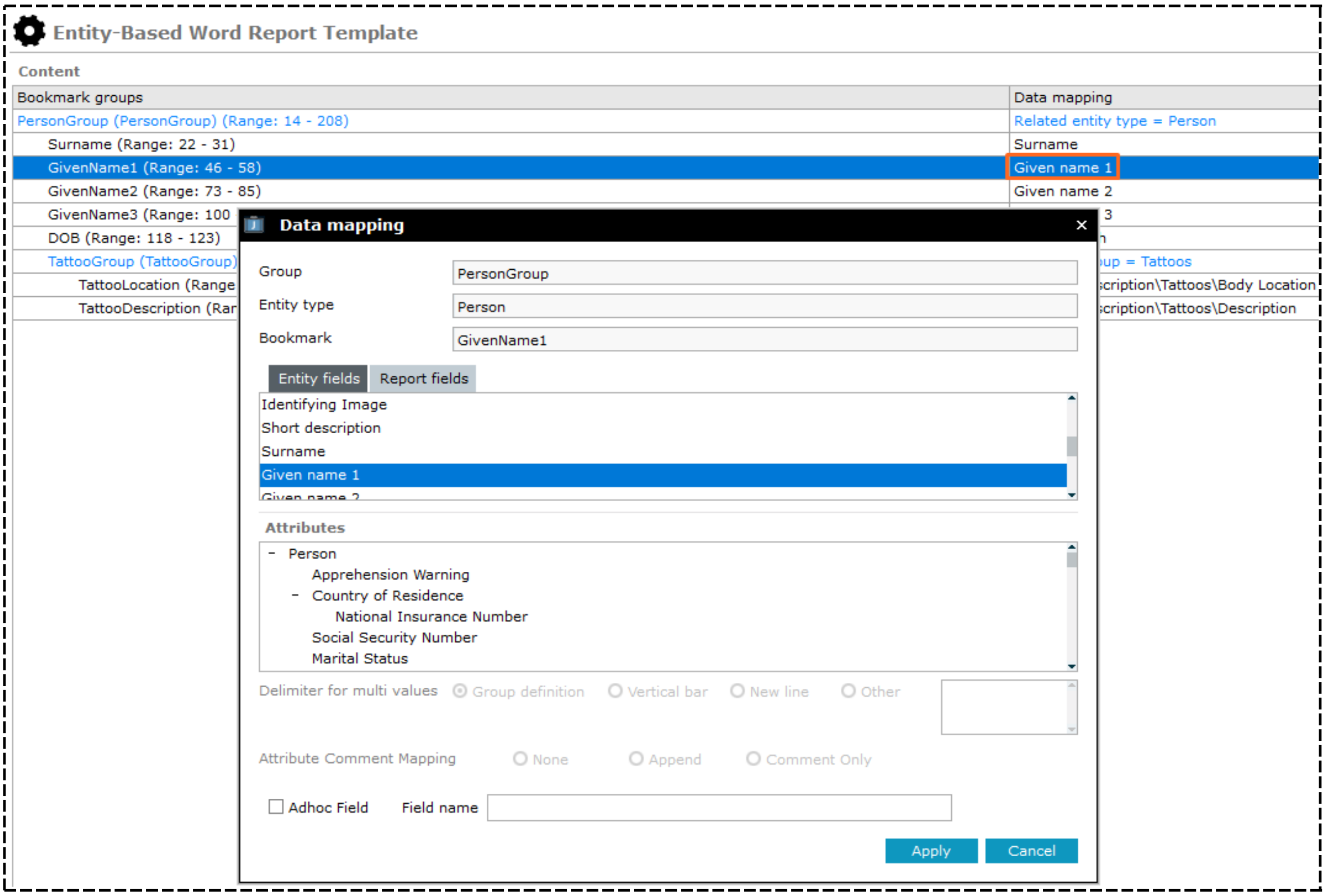
   *The **Attributes** area shows the entity's soft attributes.*
5. Use either of these methods to map the bookmark to the attribute type:
   - Select the attribute > Select **Apply**.
   - Double-click the attribute.

     You can use the delimiter for the multi-values field on the data mapping screen to specify what character will be used to separate the values of an attribute that has multiple values.

     *For example, a **Person** entity has an **Apprehension Warning** attribute that can have multiple values.*

     If an entity has a multi-valued attribute, each will be generated, separated by the character specified.

     You can't use a tab character as a delimiter.
6. Select **Save**.



Disclosure Templates

You can use a disclosure template to map field attributes in the Disclosure Index to appropriate positions in a Word document that's used to create the schedule cover screen.

The disclosure template works with a Microsoft Word template with one merge field for each attribute specified in the Disclosure Index entity.

The Disclosure Template specifies the layout and content of the schedule cover sheet to create this as a PDF.

Word Import Templates

You can use Word import templates to import attribute values for an entity from a Word document into a new incident report or information report you're currently editing.

To import attribute values into an entity, you must set up a template that maps the bookmarks in the Word document to the attributes of that entity type.

Before you can associate a Word import template with an incident report or information report, you must design the Word document containing the bookmarks from which the attribute values will be imported.

Checking Your Word Template Has the Required Bookmarks

When you import a Microsoft Word template, ICM checks whether the template contains the bookmarks you need for the report.

If any bookmarks are missing, ICM will tell you which ones you need to add.

It won't save a template that doesn't have the bookmarks you need.

Import an Updated Word Template

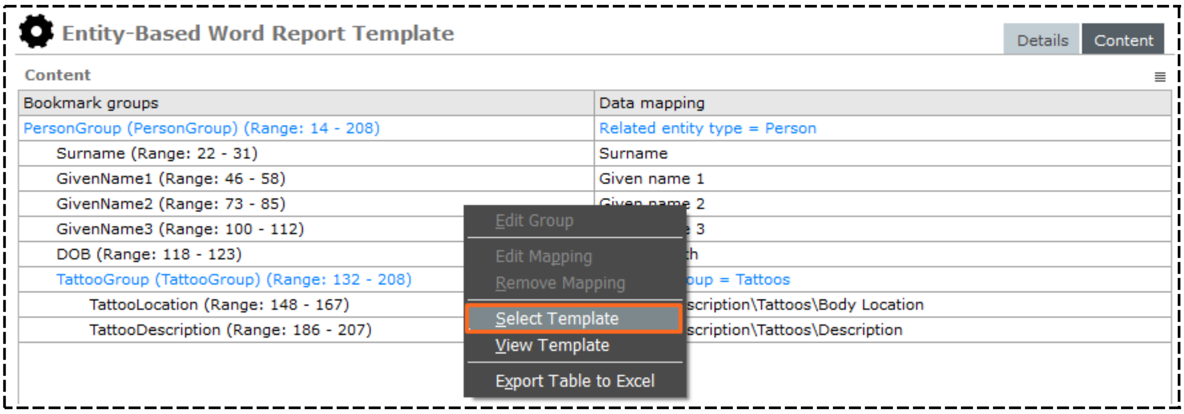
Previously you couldn't update a template once you'd added it to ICM. This made it difficult to map data items in large reports.

You can now add new bookmarks to groups and map these as required.

If there are missing bookmarks, you'll be warned about these.

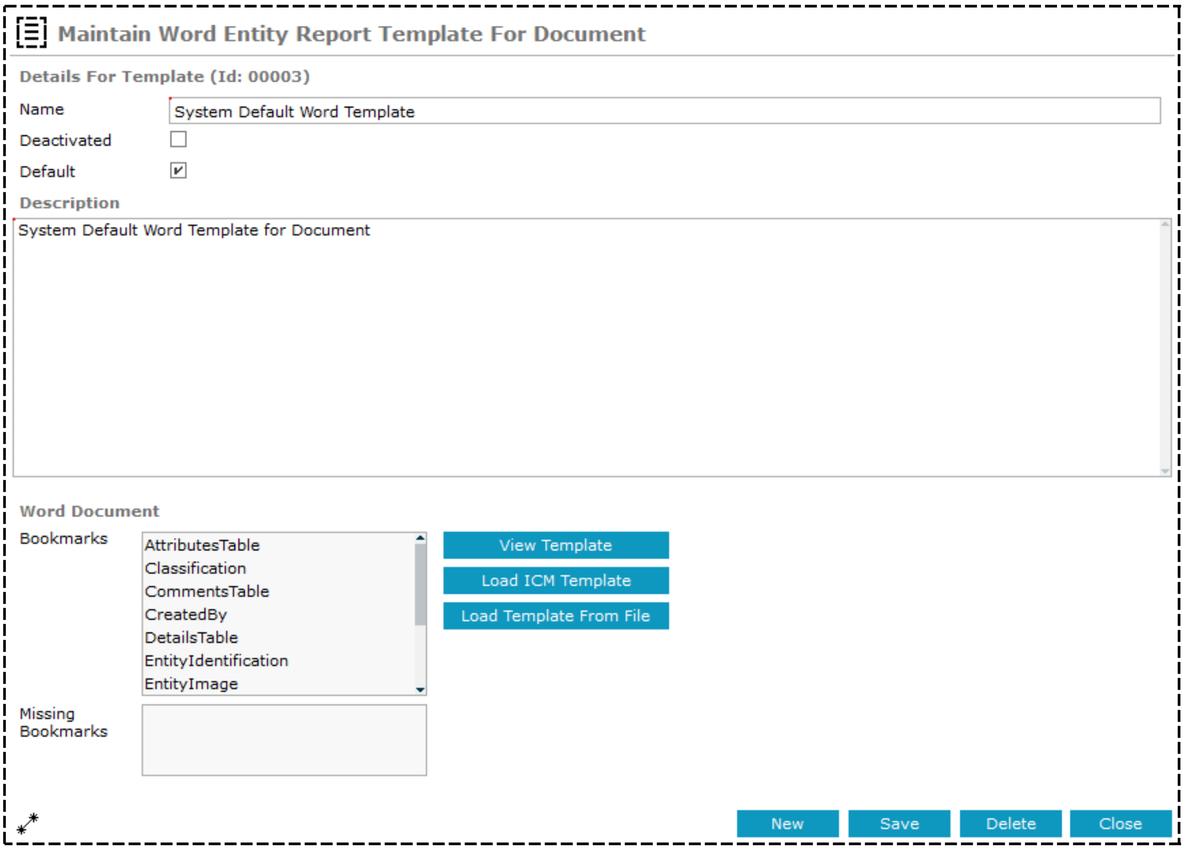
Once you have edited your Word template you can reimport it into ICM and see your changes reflected:

1. Select **Admin** > **Templates**.
2. Select either of these options:
   - **Bookmarked Word Reports**
   - **Entity-based Word Reports**
3. Open the report you want to replace.
4. Select the **Content** tab.
5. Right-click in the *Content* area > Choose **Select Template**.
6. Locate and select your updated Word template.
7. Select **Open**.



Edit a Word Import Template

1. Select **Admin** > **Entity Definition** > **Types**.
2. Open the type of entity you want to see.
3. Select the Overflow tab > Select **Templates**.
4. Select the Word import template you want to edit.
5. Use any of these methods to edit the template:
    - Double-click it.
    - Select the Options icon > Select **Edit**.
    - Right-click in the *Word Report Templates* area > Select **Edit**.
6. Make your changes.
7. Select **Save**.



Data Retention Criteria

Source entities and entities can set up to have Retention Criteria associated with them.

You can manage the review, retention, and permanent removal of data at specific elapsed times.

Several agencies have a strict data retention policy. Data might need to be deleted to comply with local legislation or for protection.

Set up Retention Criteria

1. Open the entity.
2. Select the **Retention criteria** tab.
3. To activate the retention criteria for all these types of entities, select the **Activate retention period** checkbox.

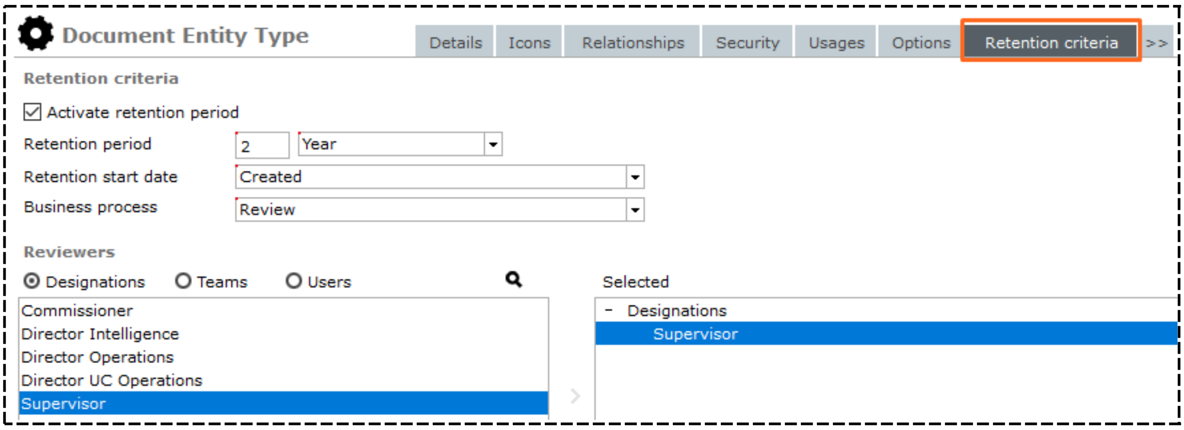
   If this checkbox is deselected, data won't be exposed for review or expunged.
4. In the **Retention period** fields, specify how long your agency wants to keep entity data for.
5. In the **Retention start date** drop-down, select when you want to start the retention calculation:
   - **Created** to start the retention calculation from the date the entity was created.
   - **Last Modified** to start the retention calculation from the last time the entity was last changed.

     Users will be warned that their changes need to be recalculated.
6. In the **Business process** drop-down, select one of these options:
   - **Review** to include the entity in the review list at the calculated time.

     You can review the entity and keep it or expunge it from the database.
   - **Automatic deletion** to automatically expunge the data at the calculated time, without sending any notification.

     Expunged entities can't be recovered.

     *Before you select **Automatic deletion**, make sure you won't need the entity later.*
7. To assign the review task to specified recipients, select a Designations, Teams, or Users.
8. Select **Save**.



PROPERTY

In ICM you can manage:

- Property – Like exhibits in criminal prosecutions.
- Assets – Like seized assets, under criminal proceeds recovery legislation.
- Equipment used by an investigations agency.

The Property Management features has these key features:

- One or more jurisdictions define operational areas of the agency.

  These may be geographically-based.
- Each jurisdiction has one or more storage locations that can be used to store property items, asset items, and equipment items.
- Storage locations are defined as a hierarchy

  For example, Location > Room > Filing Cabinet > Shelf.
- User-defined action types, movement types, and movement directions for items stored.
- A full audit trail provides for end-to-end continuity of actions and movements performed for items in storage.

Actions and Movements

You can set up actions and movements to monitor property items as they are shifted between storage locations.

Types of Actions

You can create one or more types of actions for your agency. These describe what can be done to a property item.

For example, **Destroyed** or **Returned to Owner**.

You must specify at least one type of action for your agency.

You can set a type of action with the attribute **Is a final action**. This means nothing else can be done to the property item.

For example, no further actions are possible on items that are returned to the owner or destroyed.

Types of Movement

Movement types describe how property items can be moved. You can create one or more movement types for your agency.

For example, you could have movement types for **Acquisition** and **Transfer**.

You must define at least one type of movement.

Movement Direction

You can create one or more movement directions for your agency.

For example you could define a movement direction of **In**, **Out**, or **Internal**.

You must define at least one movement direction.

Setup

Setup Process

Use this process to set up Property Report types, Property Item types, Jurisdiction types, Storage location types, and the security permissions to use the property management functions.

We recommend you do this in the following order:

1. **Actions and Movements** – Set up Action types, Movement Types, and Movement Directions.
2. **Set up Jurisdictions** – A Jurisdiction is an organisational area, usually geographically based, that contains several locations with storage facilities for property, assets, and equipment.

   This part of the process is usually only done once for the whole system unless a new jurisdiction arises or is merged with another.
3. **Set up Storage Locations for each Jurisdiction** – Jurisdictions have one or more storage locations. A storage location is a secure physical facility that can be used to store physical items.

   Storage locations can be represented as a hierarchy of containers like rooms in a building, a filing facility in a room, a shelf in a filing facility, a bin on a shelf, a container in a bin.

   Storage locations will be set up initially for the whole system.

   Storage locations can change according to demand for space to store property items.

   Storage locations can only be deleted if they or its sub-locations haven't been used to store items.
4. **Case-based Locations** – Users with appropriate rights can also set up locations that are only used by a case.
5. **Define Property Entity Types** – Set up Property Entity Types as sub-types of Property Reports.

   For example, **Homicide Evidence Report**.

   Do the same for Property Items.

   *For example, **Homicide Exhibit**.*

   Set up relationships between these entities and other types of entities.
6. **Security Permissions** – Set up appropriate security permissions for:
   - Property management functions to manage Action types, Movement types and Directions, Jurisdictions and Storage locations.
   - Create, Change, Delete, Reporting, Wizard Access and Search functions for the Property Report and Property Item types and subtypes defined in the previous stage.

     These changes will allow the Users, Roles, Teams and Designations you have authorised to use the Property menu options (Create, Search and Activities options) on the main menu.
7. **Use Property Management** – Start using the property management functions you've set up.

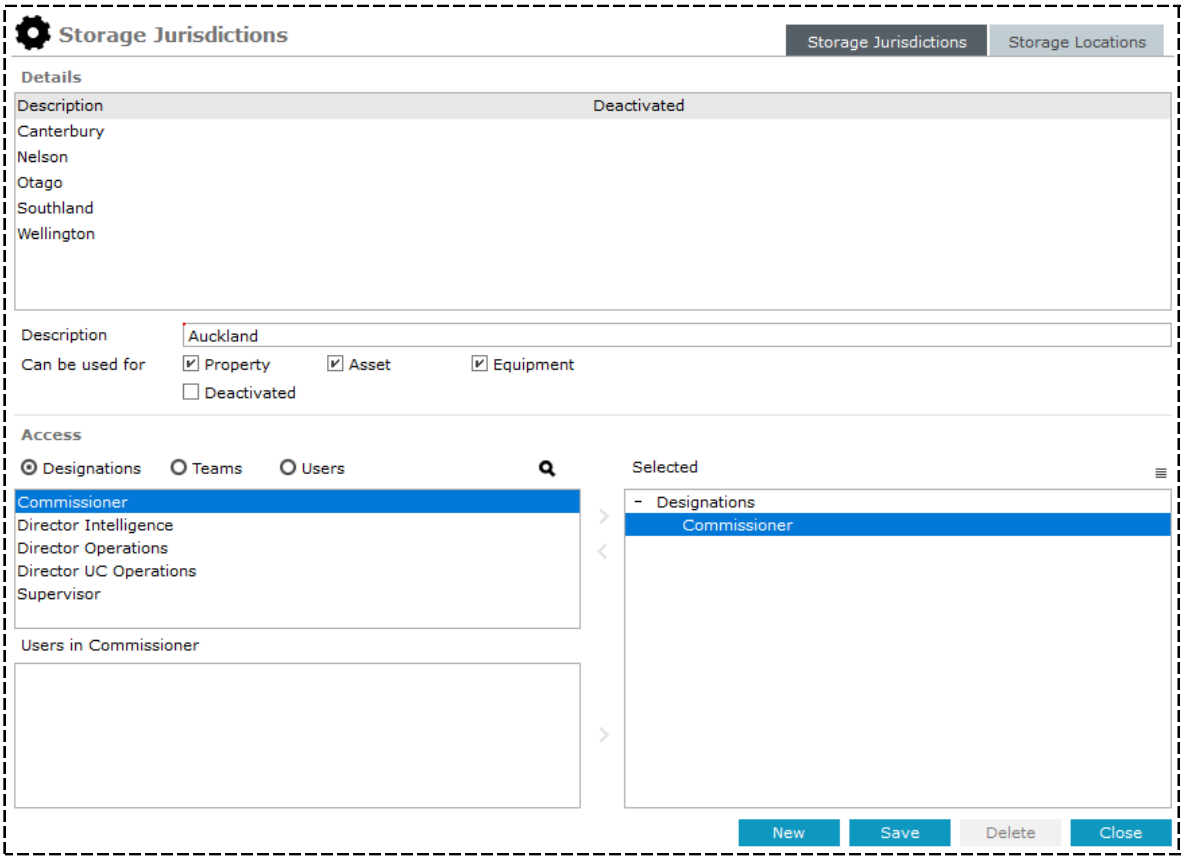
Managing Jurisdictions

Jurisdictions define operational areas of the organisation. They may be geographically-based.

*You'll need the **Can maintain storage jurisdictions** permission to manage Jurisdictions.*

Add a Jurisdiction

1. Select **Admin** > **Code Tables** > **Property** > **Storage Jurisdictions**.
   a. Select **New**.
   b. Enter the name of the new jurisdiction in the **Description** field.
   c. Select the appropriate Property, Asset and Equipment checkboxes to define which types of property item type this jurisdiction can be used with.
   d. Select **Save**.
2. Use the Select icon to set the Designations, Teams and User access to the jurisdiction.
3. Select **Save**.

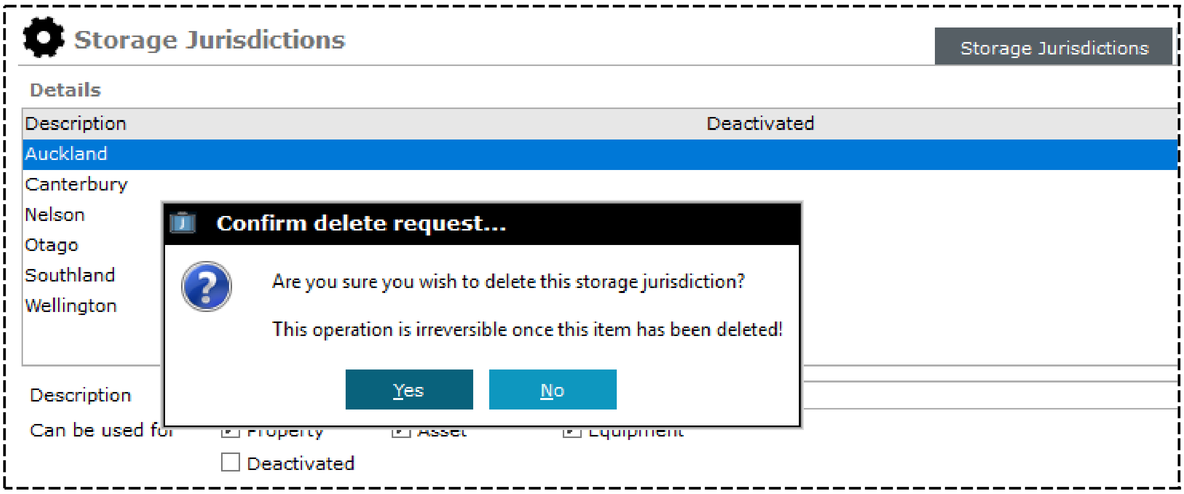


Delete a Jurisdiction

You can't delete a jurisdiction that has storage locations set up for it but you can deactivate it by selecting the **Deactivated** checkbox.

To delete a jurisdiction:

1. Select the **Admin** > **Code Tables** > **Property** > **Storage Jurisdictions**.
2. Select the jurisdiction you want to delete in the *Details* area.
3. Select **Delete**.
4. Select **Yes** to confirm.

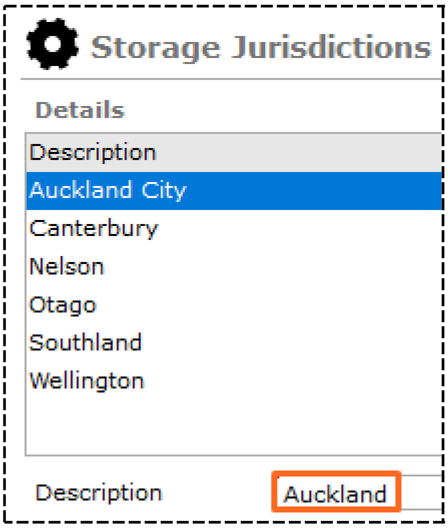


Rename a Jurisdiction

You can't rename a jurisdiction once an item has been stored in one of its storage locations or one of its storage locations sub-locations.

To rename a jurisdiction:

1. Select the **Admin** > **Code Tables** > **Property** > **Storage Jurisdictions**.
2. Select the jurisdiction you want to rename in the **Details** area.
3. Enter the new name in the **Description** field.
4. Select **Save**.



Storage Locations

Storage locations represent real world locations where evidential exhibits and seized properties are stored. They belong to a jurisdiction and are organised in a hierarchical structure.

*For example, **Location** > **Building** > **Room** > **Shelf**.*

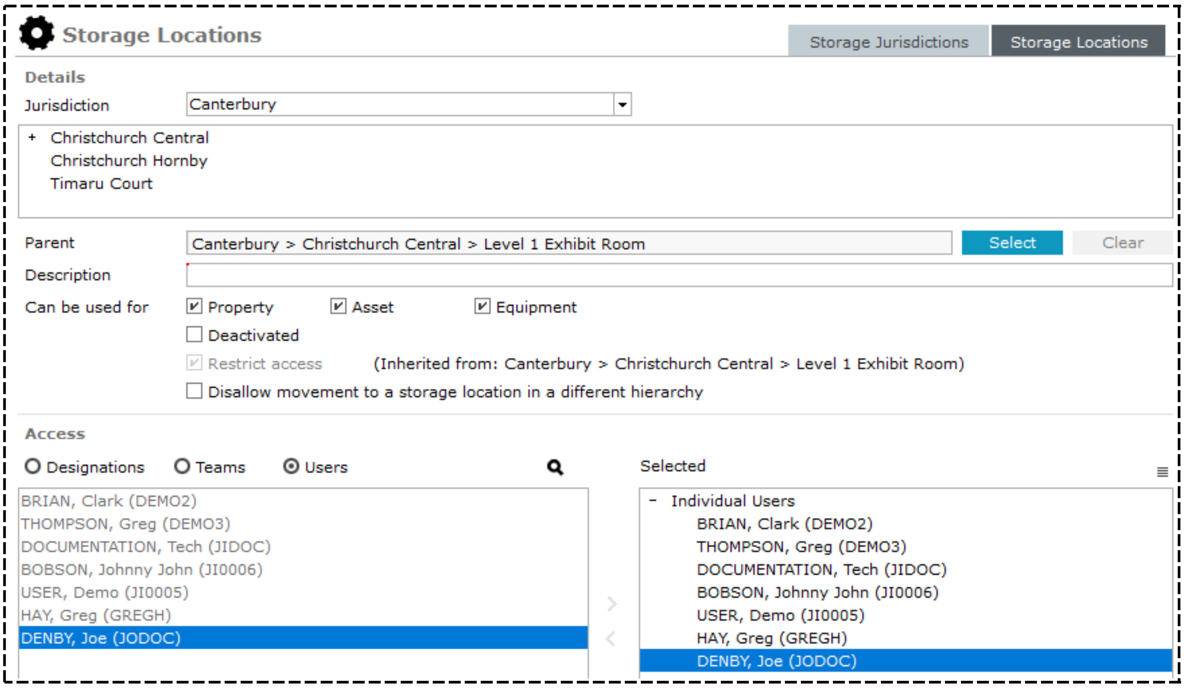
*To manage storage locations, you need the **Can maintain type storage locations** permission.*

Add a Storage Location

1. Select **Admin** > **Code Tables** > **Property** > **Storage Locations**.
2. Select the jurisdiction you want to add a storage location to.
3. Select **New**.
4. Enter the name of the new storage location in the **Description** field.

   It's easier to find items in storage locations if you include the physical location of a storage location in its name.
5. To specify the position in the hierarchy where you want to add this location, click **Select** > Choose the appropriate option.
6. Select **Save**.
7. To restrict access to the storage location, select the **Restrict Access** checkbox > Add the Designations, Teams, and Users you want to give access to.

   If you restrict access to a storage location, only users included in the storage location's access list will be able to access the storage location and all its sub-locations. Sub-location access lists won't override this constraint.
8. Use the checkboxes to specify how the storage location can be used:
   - **Can be used for** – Allow the storage location to be used with property, asset, or equipment reports.
   - **Deactivated –** Deactivate the storage location and its sublocations so it can't be used to store any more property items.
   - **Restrict Access** – Specify which users, teams, and designations can manage the storage location and its sublocations. For example, who can move items into the storage location.
   - **Disallow movement** – Prevent items in a storage location being moved without information about the move.
9. To keep adding entries at this level, enter a new storage location name in the **Description** field > Select **Save**.
10. To add a new storage location at a different level, enter the new storage location name in the **Description** field, click **Select** to select the location for the new storage location > Select **OK**.
11. Select **Save**.



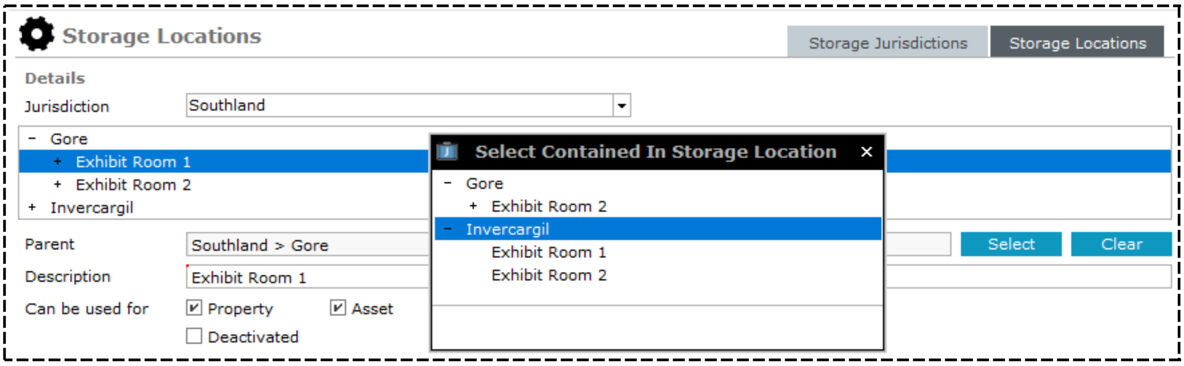
Move a Storage Location

You might want to move a storage location if it's moved to another location.

For example, if a filing system might be moved to a different floor or a building.

To move a storage location:

1. Select a storage location in the tree hierarchy in the Details list.
2. Click **Select** and choose a location to move the storage location to.
3. Select **OK**.
4. Save your changes.



Delete a Storage Location

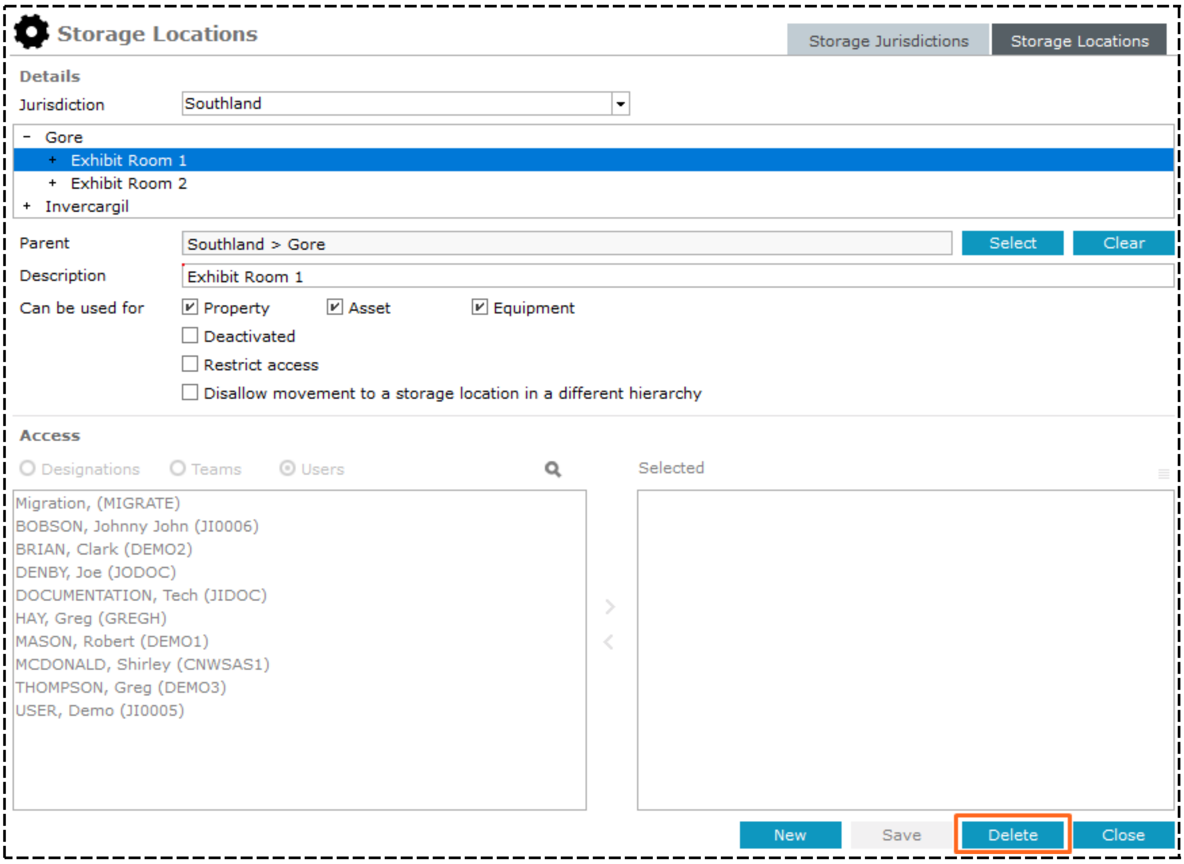
You can't delete a storage location if it has:

- child locations attached to it
- had items stored in it
- one or more continuities recorded in it

  You can't rename a storage location once an item has been stored in it or one of its sub-locations.

To delete a storage location:

1. Select a storage location in the tree hierarchy in the **Details** area.
2. Select **Delete**.



Admin Tools

Match and Merge Duplicate Entities

You can find potential duplicate entities and merge them, if appropriate.

Two entities are duplicates if they meet the criteria specified in the system-defined identification procedures.

Merging takes all the relationships and entity attributes from the suspected duplicate entity (referred to as the slave), and adds them to the master entity you intend to keep. The slave entity is deleted.

You can only merge duplicate entities of the entity types specified on the **Parameters** screen, of the Duplicate Entities Identification screen.

Merging entities is irreversible. Only proceed if you're sure the two entities represent the same real-world entity. Research your data thoroughly to confirm this. For example, don't accept that two person entities are duplicates because they have the same name and date of birth. They could be two separate people with the same name and date of birth.

The following permissions are available for merging and matching entities:

Permission	What it lets you do
Can Match and Merge Entities Auto	Do an automated match and merge
Can Match and Merge Manually	Manually match and merge records
Can force merge of entities even when dissimilar	Match and merge entities that don't meet the matching rules

Merge Duplicate Entities Using Automated Match and Merge

1. Select **System** > **Tools** > **Match and Merge (Auto)**.
2. In the **Entity Type** drop-down, select the type of duplicate entity you want to find.

   *For example, to find duplicate vehicle records, select **Vehicle**.*
3. To scroll through the **Results** area of potential duplicate sets, select the **First**, **Previous**, **Next**, or **Last** buttons:
4. To see more details about an entity, select it entity in the **Results** area.
5. To edit an entity's attributes, double-click it in the **Results** area.
6. To specify the merge action for each entity in a set of possible duplicates, select one of these checkboxes:
   - **Unique** to keep the entity.

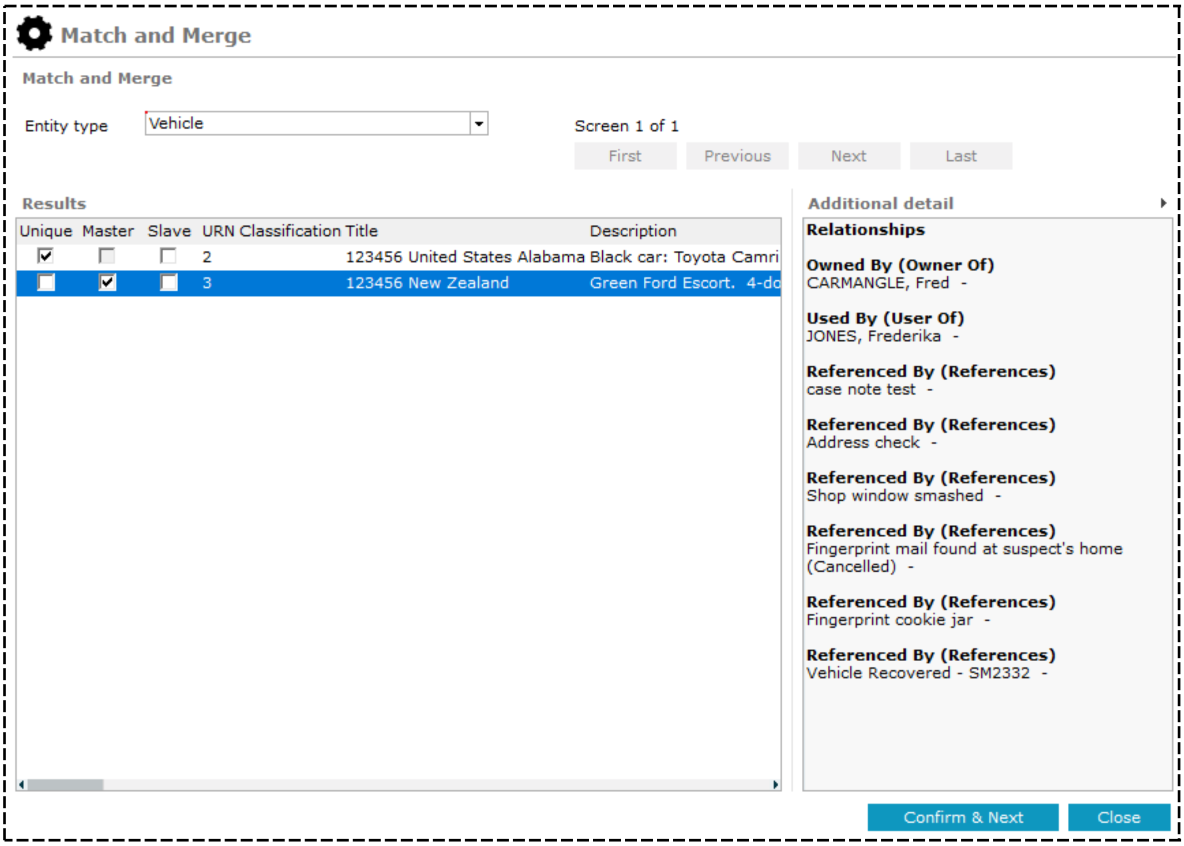
     A unique entity has no duplicates.

     You can specify all the entities in the set as unique.
   - **Master** to keep this entity as the master of the set.

     You can specify only one master entity of the set – All other entities must be unique, or slaves.
   - **Slave** if you don't want to keep this entity.

     You must specify at least one entity in the as the slave, if you've specified a master entity for that set.
7. Select **Confirm & Next** to merge the specified records for the current results.
8. To merge the relationships and attributes of the slave entities with the master entity, select **Merge**.

   The slave entities are deleted.
9. Select **OK**.


Match and Merge
Match and Merge
Entity type
Vehicle
Screen 1 of 1
First
Previous
Next
Last
Results
Unique Master Slave URN Classification Title Description
2 123456 United States Alabama Black car: Toyota Camri
3 123456 New Zealand Green Ford Escort. 4-do
Additional detail
Relationships
Owned By (Owner Of)
CARMANGLE, Fred -
Used By (User Of)
JONES, Frederika -
Referenced By (References)
case note test -
Referenced By (References)
Address check -
Referenced By (References)
Shop window smashed -
Referenced By (References)
Fingerprint mail found at suspect's home (Cancelled) -
Referenced By (References)
Fingerprint cookie jar -
Referenced By (References)
Vehicle Recovered - SM2332 -
Confirm & Next
Close

Duplicate Identification Procedures

This subsection covers the system-defined identification procedures used to determine whether two entities, of the same entity type, might be duplicates.

The following types of entities aren't used in the duplicate identification procedure:

- Document
- Image
- Media
- Offence
- All the miscellaneous types of entities that are inherited from the previous list

This table lists the duplicate identification procedures for the entity types.

Entity type	Two entities are duplicates if...
Contact number (free format)	The **Number** field isn't blank One of the words or numbers, of more than four characters in length, are an exact match
Contact number (default)	The **Number** field isn't blank, and the **Number** fields are an exact match The **Country** field isn't blank, and the **Code** fields are an exact match
Event	The **Begin Date** fields are the same At least one word in both **Description** fields is the same (case- sensitive)
Location	The **Building Name** fields aren't blank and close-matched. One location has a blank **Street Number**, or both **Street Number** fields are close-matched, and: The **Street Name** fields are close-matched One location has a blank **Country** field, or both **Country** fields are the same One location has a blank **State** field, or both **State** fields are the same One location has a blank **City** field, or both **City** fields are close- matched One location has a blank **Suburb** field, or both **Suburb** fields are close-matched

Miscellaneous	The entity type for both entities is the same At least one word, in the first three words, of both **Title** fields is the same (case-sensitive) *If the entity type is inherited from a system-defined entity type, the entities are handled the same way as the entity types they're inherited from.*
Organisation	One organisation has a blank **Country** field, or both **Country** fields are the same One organisation has a blank **State** field, or both **State** fields are the same The **Name** fields are close-matched.

Person	The first set or second set of conditions apply:
	
	First set of conditions:
	
	One person has a blank or unknown Gender field, or both Gender fields are close-matched.
	
	Both Surname fields are blank, and one of the following applies:
	
	▪ The Given name 1 fields are close-matched
	
	▪ The Given name 2 fields are close-matched
	
	    ▫ The Given name 1 field of one person is close-matched with the Given name 2 field of the other person
	
	    ▫ The Given name 2 field of one person is close-matched with the Given name 1 field of the other person
	
	▪ One person has a blank D.O.B. field, or both D.O.B. fields are close-matched (within a range of one year), and one of the following:
	
	    ▫ The Given Name 1 fields are reasonable-matched (for the first two characters), or both names are missing
	
	    ▫ The Given Name 2 fields are reasonable-matched (for the first two characters)
	
	    ▫ The Given Name 1 field of one person is close- matched with the Given name 2 field of the other person
	
	    ▫ The Given Name 2 field of one person is close- matched with the Given name 1 field of the other person Second set of conditions (which must all apply):
	
	One person has a blank or unknown Gender field, or both Gender fields are close-matched.
	
	The Surname fields are close-matched.
	
	The D.O.B. fields are close-matched (within a range of six months).

Transaction	The Date fields are the same. One transaction has a blank Value field, or both Value fields are close-matched (within a ten percent range). At least one word, in the first three words, of both Description fields is the same (case-sensitive).
Vehicle	The Registration Number fields are close-matched (ignoring embedded non-alphanumeric characters and spaces).

Translate the Interface

You can translate the interface into any language and character set without any programming or technical knowledge.

You can also use translation strings to include changing individual terms to match local common usage.

Translation only affects the user interface. Any information entered always remains in the language in was entered in.

To edit translations, you need the **Can Translate** permission.

For more details, see "Security".

Find and Open a Translatable String

1. Select **Admin** > **System**> **Captions / Messages**.
2. In the Locale drop-down, select the Microsoft Windows locale used in your country.
3. Use these fields to specify your search criteria:
   a. **Name filter** – Enter all or some of the internal name of the string.

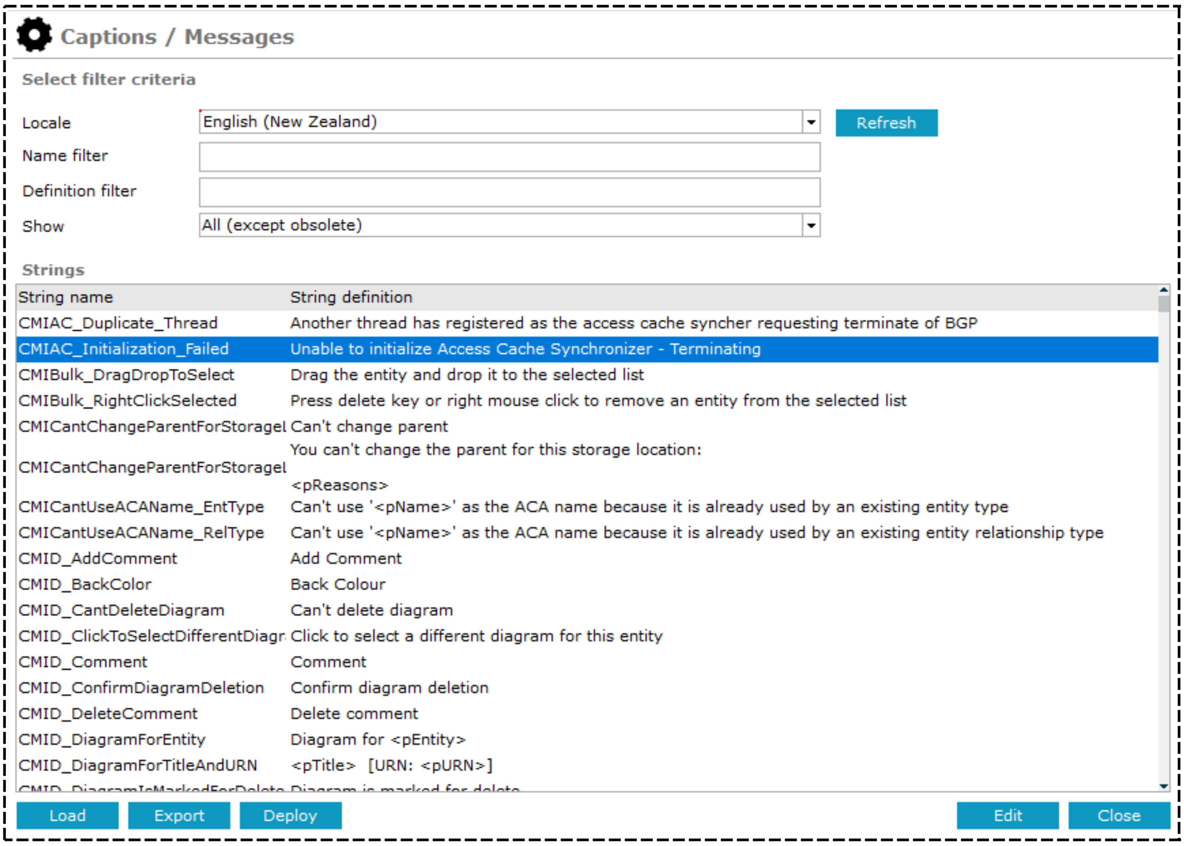
      If you enter part of the string name, the search results will include any string that includes the specified text in its name.

   b. **Definition filter** – Enter all or some of the internal definition of the string.

      If you enter part of the string definition, the search results include any string that includes the specified text in its definition.

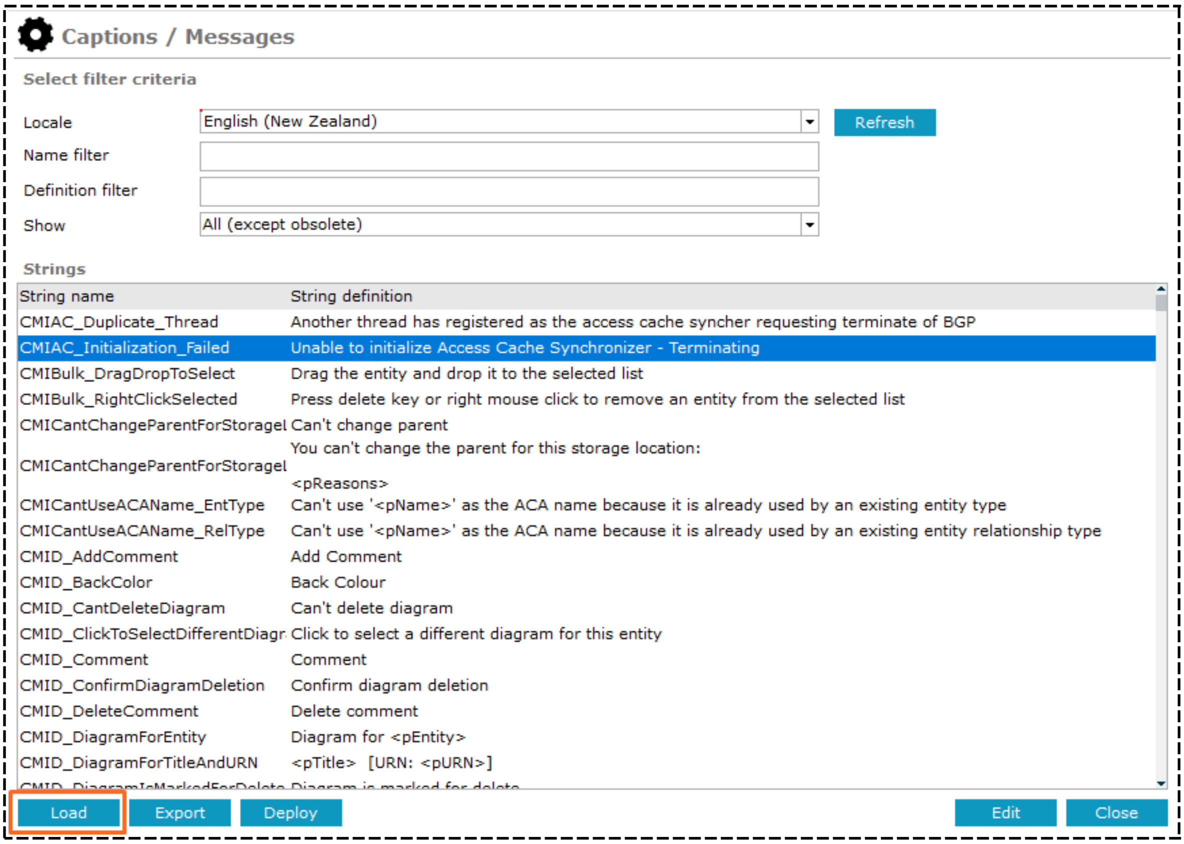
   c. **Show** – Select the translation status of the strings you want to see in the search results.
4. Select **Refresh**.
5. To see details about a string, select its row in the **Strings** table > Double-click it.

   For more details, see "Translate a String".



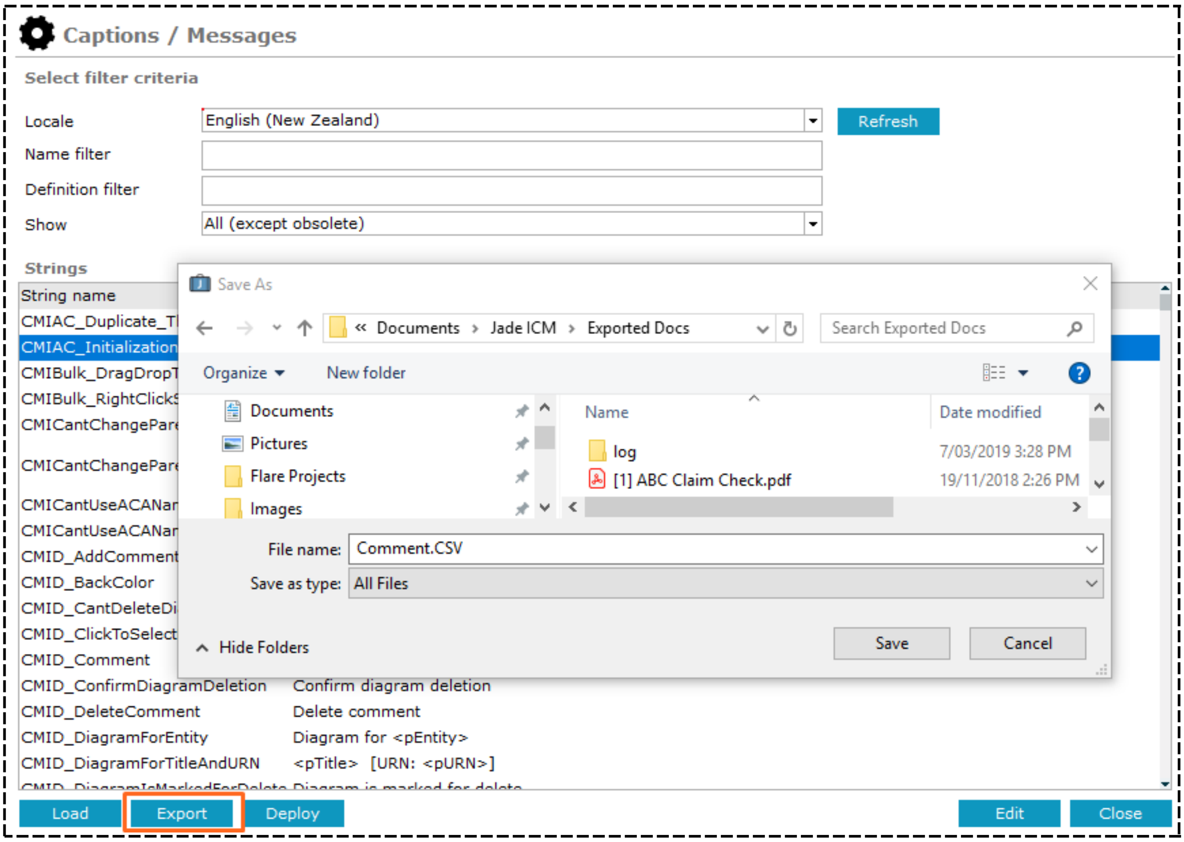
Import a File Containing Translated Strings

1. Select **Admin** > **System** > **Captions / Messages**.
2. Select **Load**.
3. Select the file you want to import.
4. Select **Open**.



Export a Translated Strings File

1. Select **Admin** > **System** > **Captions / Messages**.
2. Select **Export**.
3. Enter a name and file extension (CSV or TXT) for the file you want to export.
4. Select **Save**.



Translate a String

1. Select **Admin** > **System**> **Captions / Messages**.
2. Double-click the string you want to translate.

   *The **Original English Version** field shows the original English string as a reference.*

   *The **Translated Version** field shows the current translated version of the English version for the selected locale.*

   *The **Edit Definition** field shows the elements of the string you want to translate. All strings contain at least one string literal element and can contain one or more parameters. The string literal is what is translated and the parameter is a placeholder for a value generated while the application is running.*

   You can also specify that a string doesn't need to be translated, or can't be, and is a way to exclude this string in future.

   *The **Comments on usage** ... field shows any additional comments about the string or translation.*

2. Enter the translated text you want to replace the string literal with.

   The number and order of the translated string literals and parameters might not match the English structure.

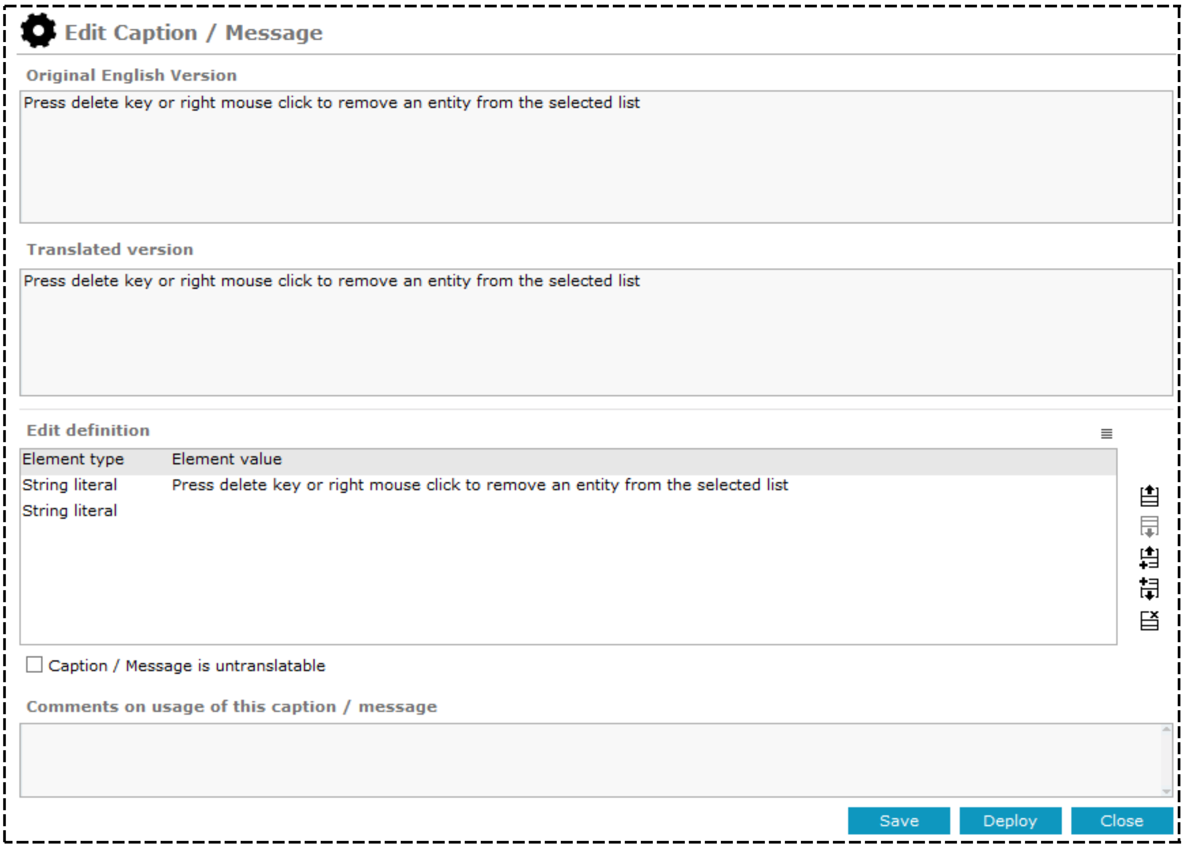
3. In the **Edit string** definition table, select the row of the text whose position you want to change in the translation generated.

   Use the buttons beside the **Edit Definition** field to adjust the position of the text:

   - To move the selected row up one position, select the Move up icon.
   - To move the selected row down one position, select the Move down icon .
   - Add a row above the selected row, select the insert row above icon .
   - Add a row below the selected row, select the Insert row below icon.
   - To delete the selected row, select the Delete row icon.

4. If you can't translate the string, select the **String is untranslatable** checkbox.

5. Select **Deploy** to apply your changes to the selected locale.



Auditing Data

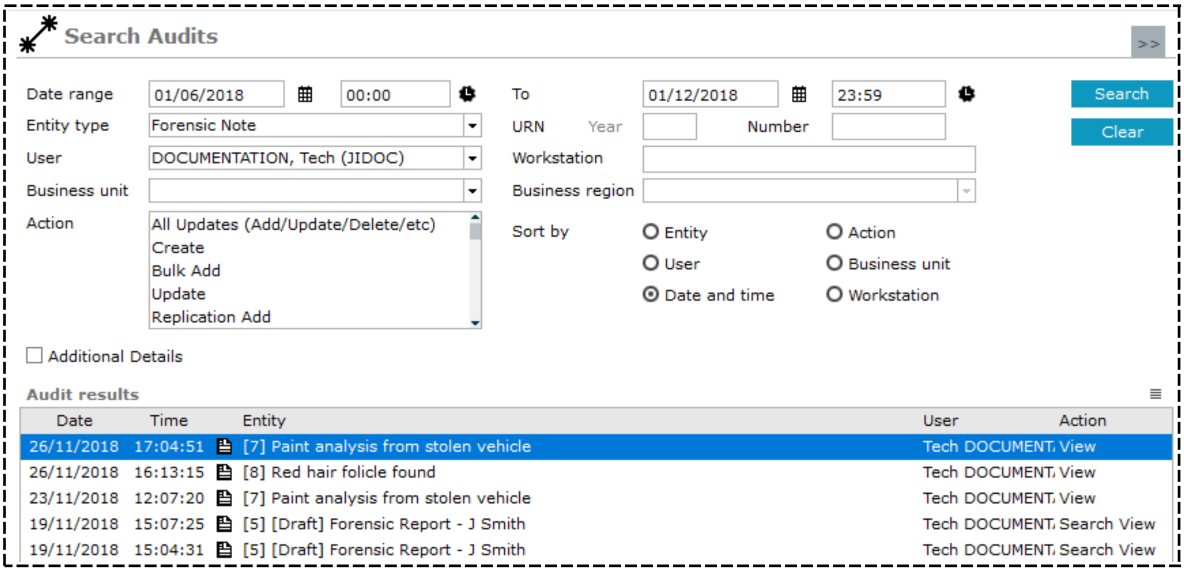
Audit records are written for all user activity and all data changes. The audit log is a permanent record of:

What was done, for example when a user	- Logs on, logs off, and the number of unsuccessful log on attempts - Adds data - Updates data (the record includes the original value and the new value) - Deletes data - Views data - Performs a search (the record includes the search parameters) - Prints data - Merges data - Views an image or document file - Downloads an image or document file
The date and time it happened	
The workstation used	
The User ID of the user who did it.	This level of auditing allows data to be reconstructed and associated with all user actions in any session. You can audit: - Everything - One entity Auditing capability isn't made available to all users. It's allocated by permissions against a specified role. Those users who undertake auditing are likely to have additional access rights and menu options activated. To audit data, you need one the *Can View Audit Log* permission.

Access Audits

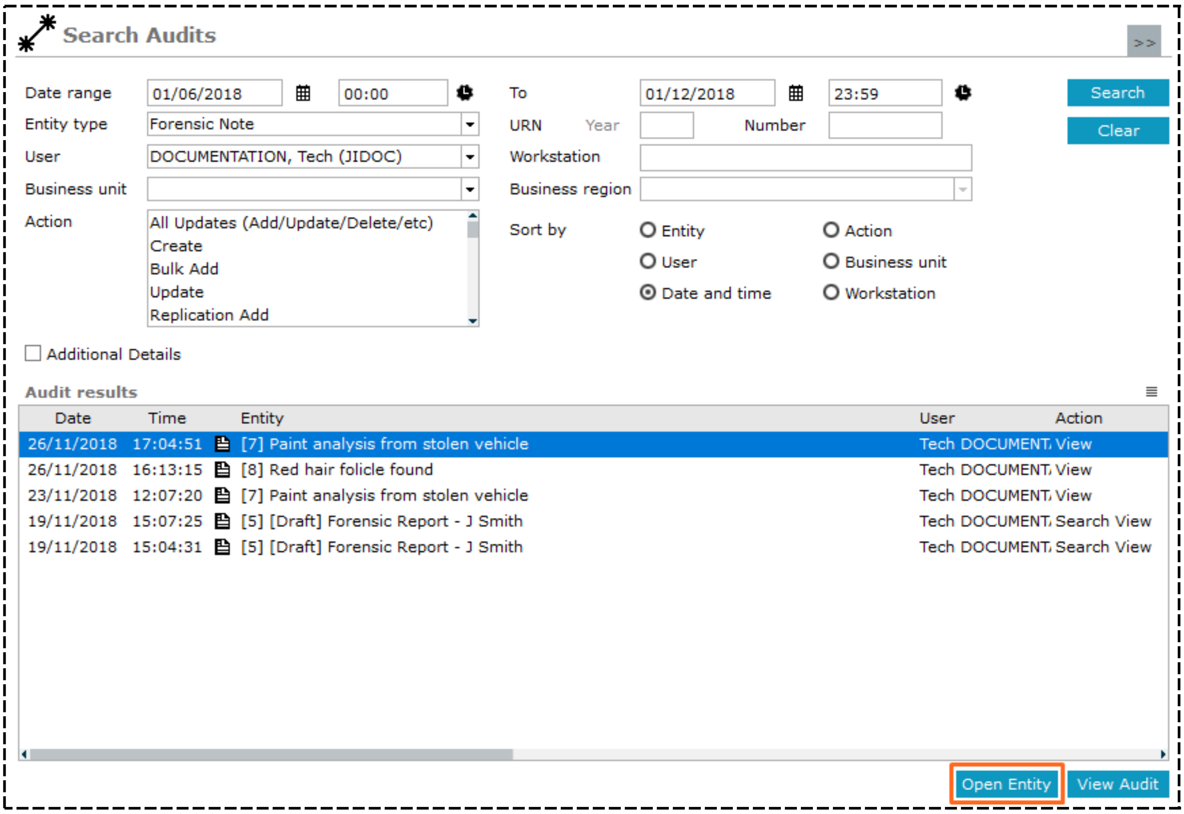
1. Use either of these methods to access audits:
   - Select **System** > **Search Audits**.
   - Open an entity > Select **Show audit log**.
2. Enter the date and time range in the fields provided.
3. In the **Entity type** drop-down, select the type of entity you want to audit.

   If you want to audit a user's actions, don't select a value in this drop-down.
4. Enter the year and number of the URN you want to find in the fields provided.
5. Select the user you want to audit in the field provided.
6. Enter the workstation used.
7. Enter the business unit you want to find.
8. Enter the business region in which you want to search.
9. In the Action drop-down, select the type of action (for example, add, update, or download) you want to find.
10. To specify the order in which the search results are shown, select an option button at the right of the **Sort by** field.
11. Select **Search**.



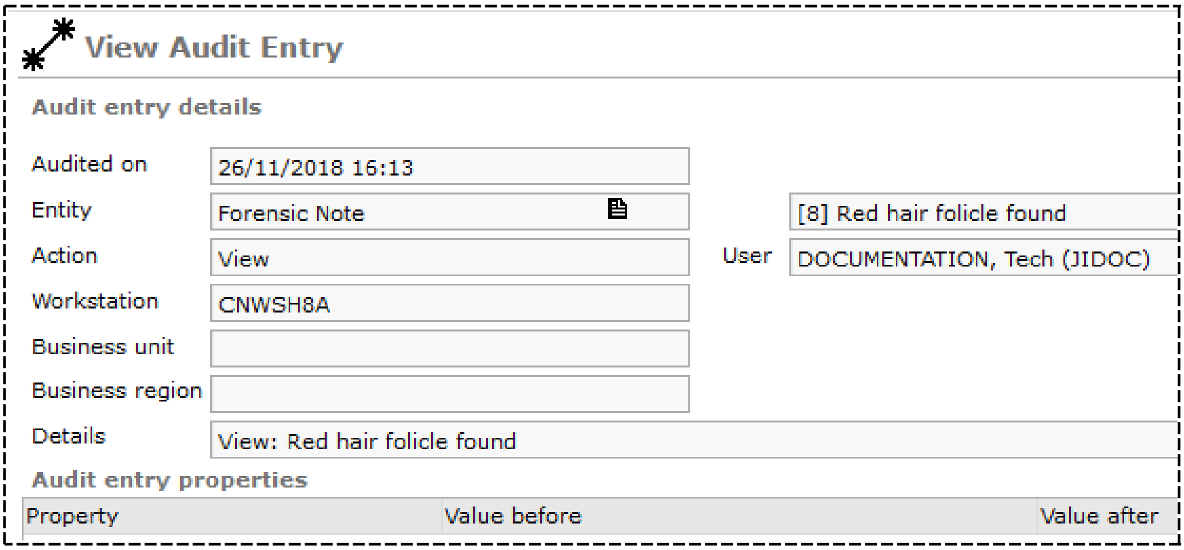
Access Details about an Entity in the Search Details

1. Select **System** > **Search Audits**.
2. Select the entity you want to see.
3. Double-click it or select **Open Entity**.



Access Audit Record Details

1. Select **System** > **Search Audits**.
2. Select that item you want to view.
3. Select **View Audit**.



See How Source Entities Have Been Used

You can generate a CSV file that contains the usage statistics for source entities that have been created over a period time:

1. Select **System** > **Search Audits**.
2. Select the date range for the usage statistics you want to see.
3. Select the Overflow >> tab > Select **Statistics**.
4. Enter a name for the file.
5. Select **Save**.

   You can import the data into a spreadsheet. Information in the file generated is sorted by who performed the action. It includes the workstation used.

THESAURUS

The thesaurus is a hierarchical list of one or more words that are linked with their:

- **Broader terms (BT)** like road and transport
- **Narrower terms (NT)** like sedan and station wagon
- **Related terms (RT)** like petrol, road, or highway
- **Synonyms** like vehicle, motor vehicle, or automobile

The terms you define are used when you do a thesaurus search.

You can use the search to:

- Expand a search with one word or phrase as criteria into many other relevant words or terms.
- Search for a concept, rather than a specific word.
- Expand a search to include common abbreviations or misspellings.

Rules for Thesaurus Terms

- The terms can be one or more words
- They can have a qualifier which clarifies the meaning of the term

  For example, crane (bird) and crane (machine)
- They are either preferred or not preferred
  - Preferred terms can't be the right side of a USE relationship.

    For example, if Truck is the preferred term, the following thesaurus relationship is invalid: ***Lorry USE Truck***
  - Non-preferred terms can't have a BT, NT, or RT relationship and can't be the left side of a UF relationship
- Thesaurus BT relationships can't be linked to a term that already has an NT relationship
- Thesaurus NT relationships can't be linked to a term that already has a BT relationship
- Thesaurus BT, BTI, BTP, BTG, NT, NTI, NTP, and NTG relationships defined in the thesaurus should be independent of context (always true).

Manage Thesaurus Terms

You can use thesaurus terms in a thesaurus search or a search group.

*To manage thesaurus terms, you need the **Can Maintain Global Thesaurus** permission.*

Create a Term

Use the New term screen to add a new term to the thesaurus.

To save time, you can import thesaurus terms from a file if you've previously exported one.

To link a new term to an existing thesaurus term, use the Link to new command that displays when you right-click in the Tree pane of the Thesaurus Maintenance screen.

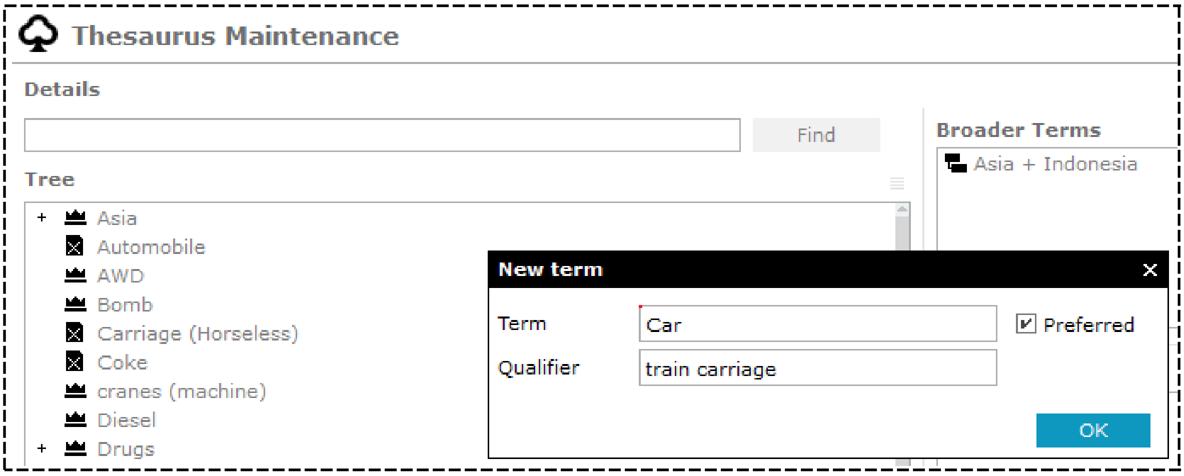
To add a new term to the thesaurus:

1. Select **Admin** > **System** > **Thesaurus** > **Maintain**.
2. Right-click in the Tree pane > Select **New term**.
3. In the **Term** field, enter the term you want to add to the thesaurus.

   The term can be more than one word.
4. Select the **Preferred** checkbox if this is the preferred term.
5. In the **Qualifier** field, enter a qualifier.

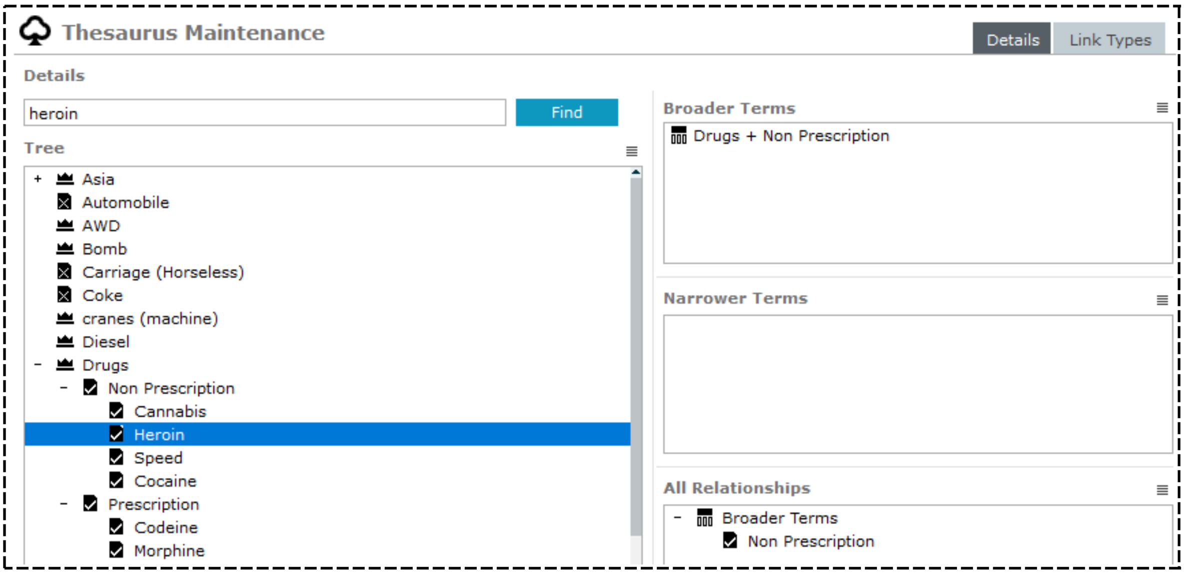
   If the term has more than one meaning, depending on context, enter a qualifier what it means.
6. Select **OK**.

   If the term is related to other words in the thesaurus, specify those links.



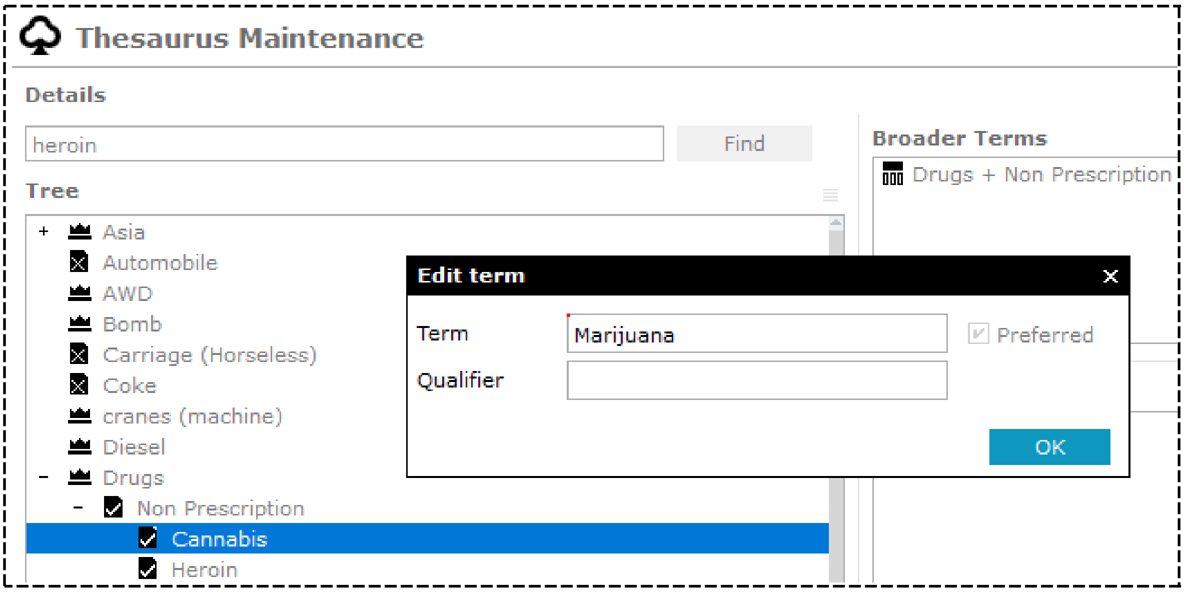
Find a Thesaurus Term

1. Select **Admin** > **System** > **Thesaurus** > **Maintain**.
2. Enter the term in the **Details** field.
3. Select **Find**.



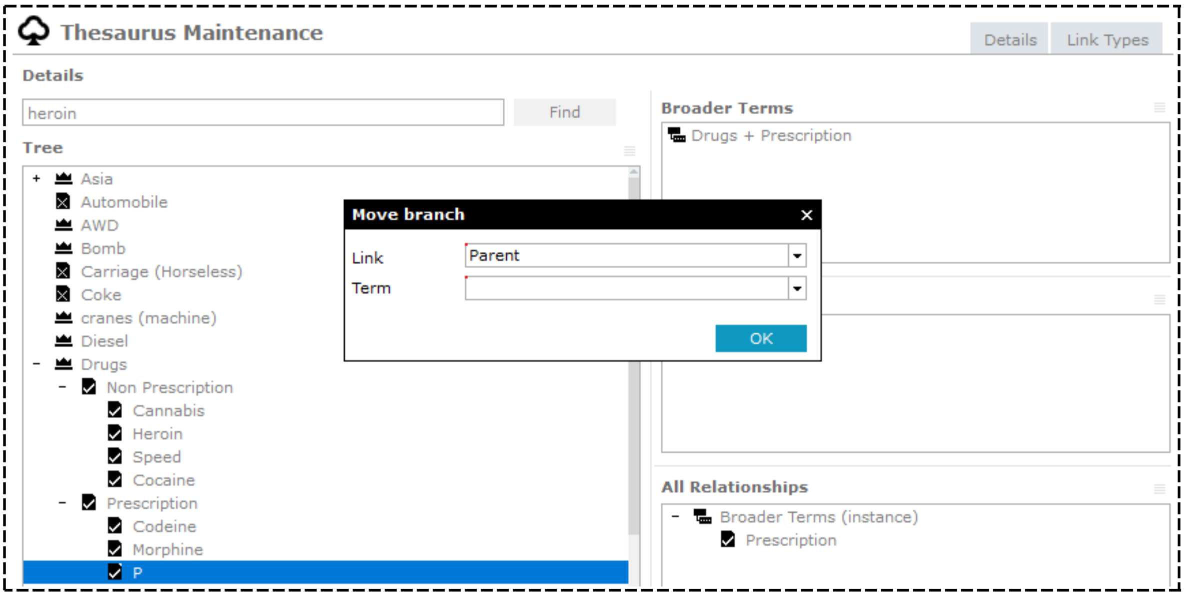
Edit a Term in the Thesaurus

1. Select **Admin** > **System** > **Thesaurus** > **Maintain**.
2. Right-click the term you want to edit > Select **Edit term**.
3. Edit the required details.
4. Save your changes.



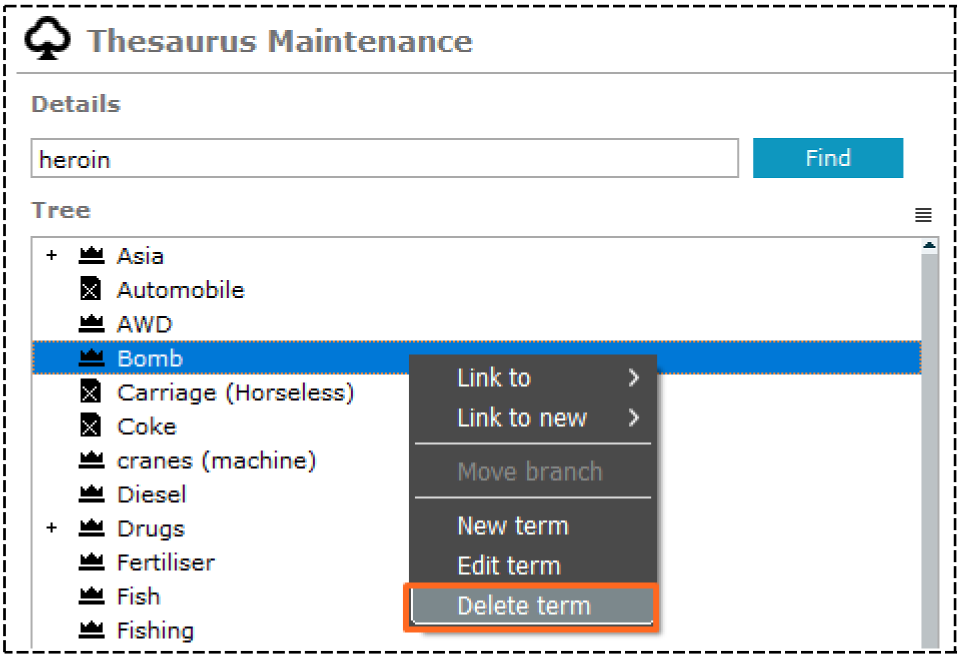
Move a Thesaurus Term to a Different Branch

1. Select **Admin** > **System** > **Thesaurus** > **Maintain**.
2. Right-click the term you want to move Select Move Branch
3. Right-click the term > Select **Move branch**.
4. In the **Link** drop-down, select the type of link you want the term you're moving to have with its new branch.
5. In the **Term** drop-down, select the term you want to move the selected term to.
6. Select **OK**.



Delete a Term from the Thesaurus

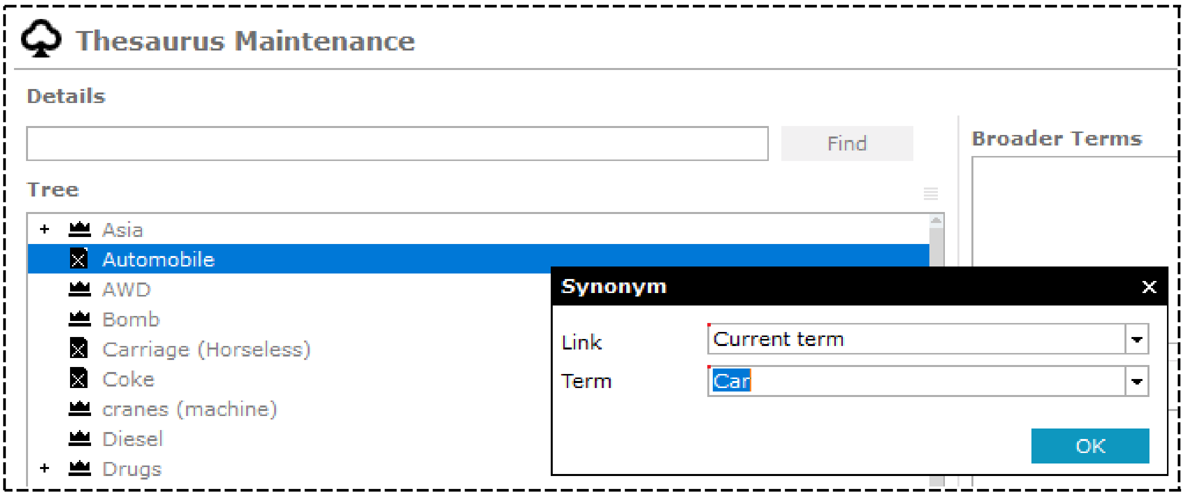
1. Select **Admin** > **System** > **Thesaurus** > **Maintain**.
2. Right-click the term you want to delete > Select **Delete**.
3. Select **Yes**.



Linking Thesaurus Terms

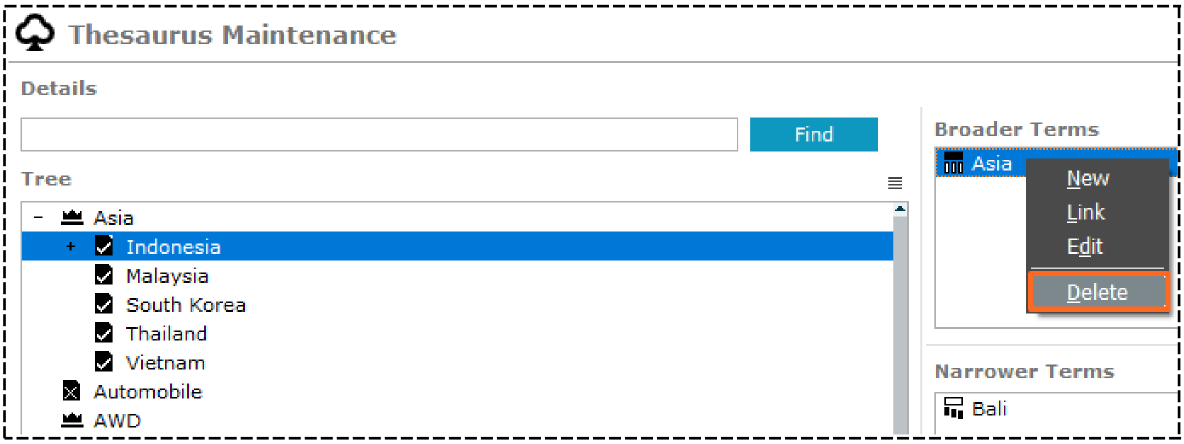
Link Thesaurus Terms

1. Select **Admin** > **System** > **Thesaurus** > **Maintain**.
2. Select the term you want to link to an existing term.
3. Use either of these methods to link the term:
   - Right-click the term > Select **Link to**.
   - Select the Options ≡ icon > Select **Link to**.
4. In the **Link** drop-down, select the type of link you want to create.
5. In the **Term** drop-down, select the term to which you want to link the term you selected earlier.
6. Select **OK**.



Delete a Thesaurus Link

1. Select **Admin** > **System** > **Thesaurus** > **Maintain**.
2. In the **Tree** pane, select the term you want to delete a link from.
3. Select the term you want to delete a link from in one of these panes:
   - Broader Terms
   - Narrower Terms
   - All Relationships pane
4. Right-click the term > Select **Delete link**.
5. Confirm you do want to delete the selected link.



Managing Types of Links

The Link Types screen of the Thesaurus Maintenance screen lists the ways in which thesaurus terms are related – Link types.

The link types listed in the following table are defined, by default.

Relationship	Description	Example
BT/NT	broader term/narrower term	Granny Smith BT apple Apple NT Granny Smith
BTG/NTG	broader term generic/narrower term generic	Mouse BTG rodent Rodent NTG mouse
BTI/NTI	broader term instance/narrower term instance	Sydney BTI cities Cities NTI Sydney
BTP/NTP	broader term partitive/narrower term partitive	Sydney BTP Australia Australia NTP Sydney
RT	related terms	Barley RT wheat
UF/USE	used for/use instead of	Dress USE frock Frock UF dress (where frock is the preferred term)

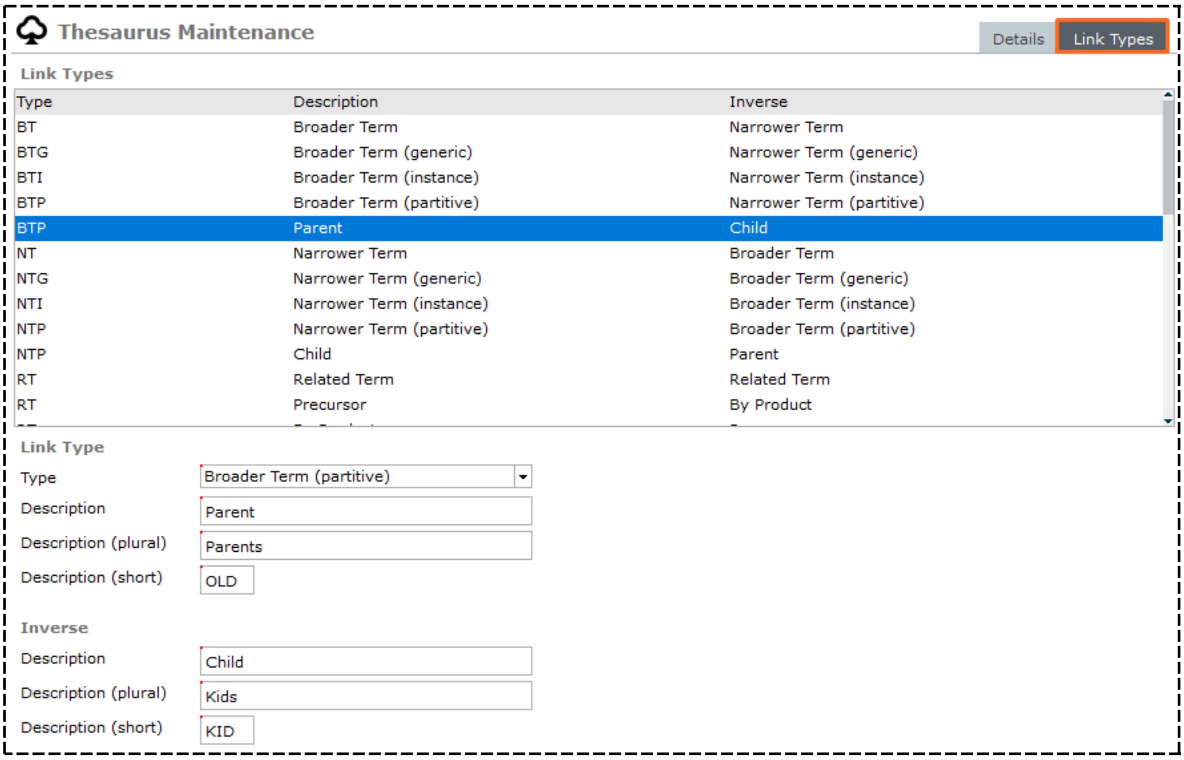
Use the Link Types screen to define additional types of links to describe how terms are related.

For example, you can define a historic term (for example, Siam) and current term (for example, Thailand) as a UF/USE link type.

Add a New Type of Link to the Thesaurus

1. Select **Admin** > **System** > **Thesaurus** > **Maintain**.
2. Select the **Link Types** tab.

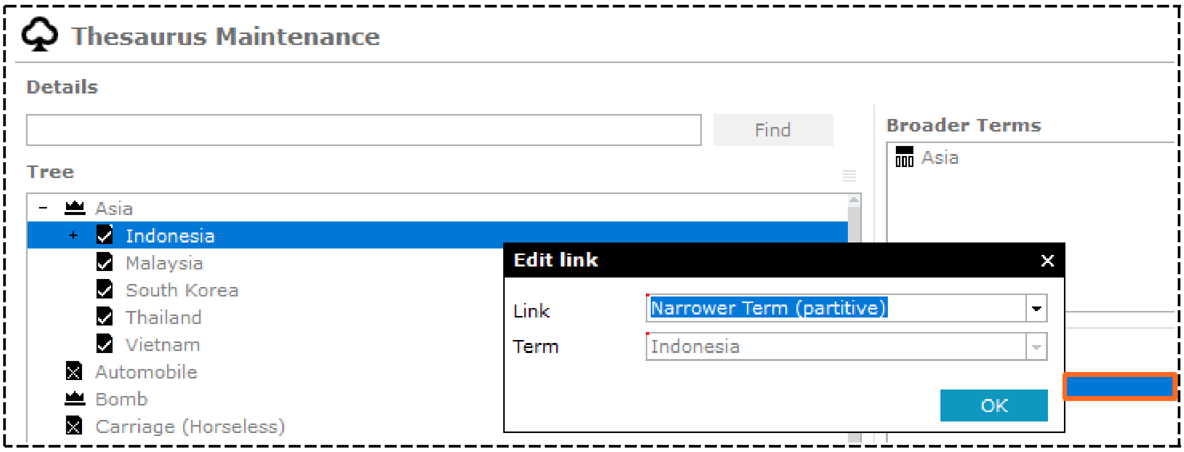
   The Link Types table lists all the types of links that are possible between thesaurus terms.
3. To see details about a type of link, select it.
4. To add a new link, select **New**.
5. In the **Link Type** area, specify details about the link.
6. Select **Save**.



Edit a Thesaurus Link

1. Select **Admin** > **System** > **Thesaurus** > **Maintain**.
2. Select the term you want to edit links for.
3. In the pane, select the term you want to edit in one of these areas:
   - Broader Terms
   - Narrower Terms
   - All Relationships
4. Right-click the selected term > Select **Edit**.

   The Term field shows the term with which the selected term is linked.
5. In the **Link** drop-down, select the type of link you want for this term.
6. Select **OK**.



Import Terms

You can import an XML file that contains thesaurus terms used by your agency.

This saves you time because you to don't have to create new terms or links.

The imported terms overwrite any existing terms in the thesaurus. make sure that the file you're importing contains any thesaurus terms you want to keep.

You should import only files exported from another ICM database.

To import thesaurus terms from a file, you need the *Can Load Global Thesaurus* permission.

To import thesaurus terms from an XML file:

1. Select the **Admin** > **System** > **Thesaurus** > **Import**.
2. On the screen that displays, select the file that contains the thesaurus terms you want to import.

   A warning displays, prompting you that all existing thesaurus terms are to be overwritten by those in the imported file.
3. Select **Yes**.

Export Thesaurus Terms

Use the Extract Thesaurus command to export a thesaurus to an XML file.

You can then import the exported file into another ICM database.

To export a thesaurus terms to a file, you need the *Can Extract Global Thesaurus* permission.

To export thesaurus terms to an XML file:

1. Select the **Admin** > **System** > **Thesaurus** > **Export**.
2. On the generic Save As screen that displays, specify the name and the location for the file generated.

   Save the file.

   The thesaurus terms are generated to an .xml file in the location you specified on the Save As screen.

Thesaurus Search Groups

Thesaurus search groups enable you to define and save thesaurus searches that contain multiple search terms.

For example, you might want to find instances of drugs smuggled in shoes from Vietnam. The search terms for these keywords can be entered into one search group and then used by the Thesaurus search to find entities that match that set of terms.

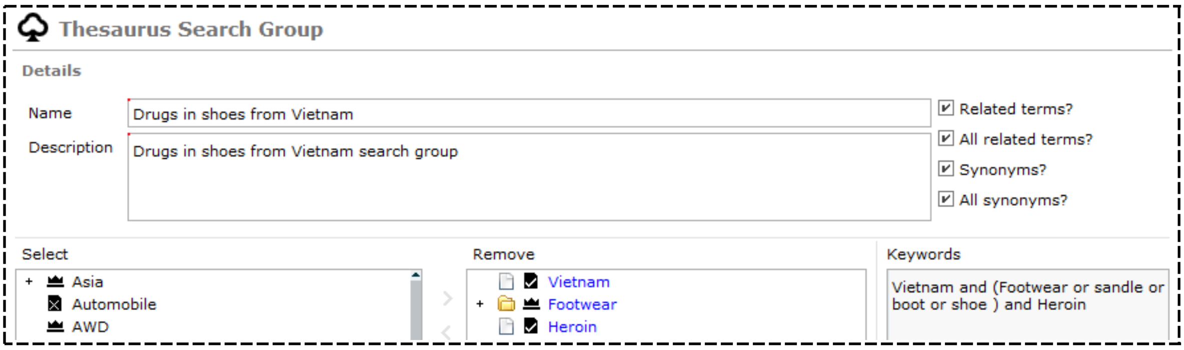
To manage thesaurus search groups, you need the *Can Maintain Thesaurus Search Groups* permission.

For more details, see "Security".

Create a Search Group

1. Select **Admin** > **System** > **Thesaurus** > **Search Group**.
2. Select the Add icon.
3. Enter a name for the search group in the field provided.
4. Enter a description of the search group in the field provided.
5. To select the terms you want to include in the search group:
    a. In the **Select** pane, select the term you want to include in the search group.
    b. Click the Select icon or double-click the term.

    If the term has related terms, these are also included.
6. To select the terms you want to remove from the search group:
    a. In the **Remove** pane, select the term you want to remove from the search group.
    b. Select the Deselect icon.
7. To specify the breadth of the search, select the required checkboxes:
    - **Related terms**
    - **All related terms**
    - **Synonyms**
    - **All synonyms**
8. Select **Save**.



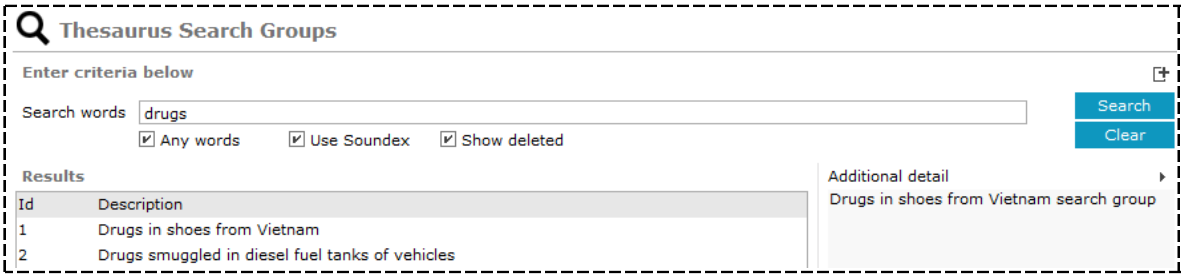
Find a Thesaurus Search Group

1. Select **Admin** > **System** > **Thesaurus** > **Search Groups**.
2. In the **Search words** field, enter any word or words associated with the search group that you want to find.
3. To return any search group that uses any of the specified words, check the **Any words** checkbox.

   If you don't select this checkbox, the search only returns search groups that contain an exact match of the specified words.
4. To return any search groups that use words that sound like the specified words (as well as exact matches), select the **Use Soundex** checkbox.

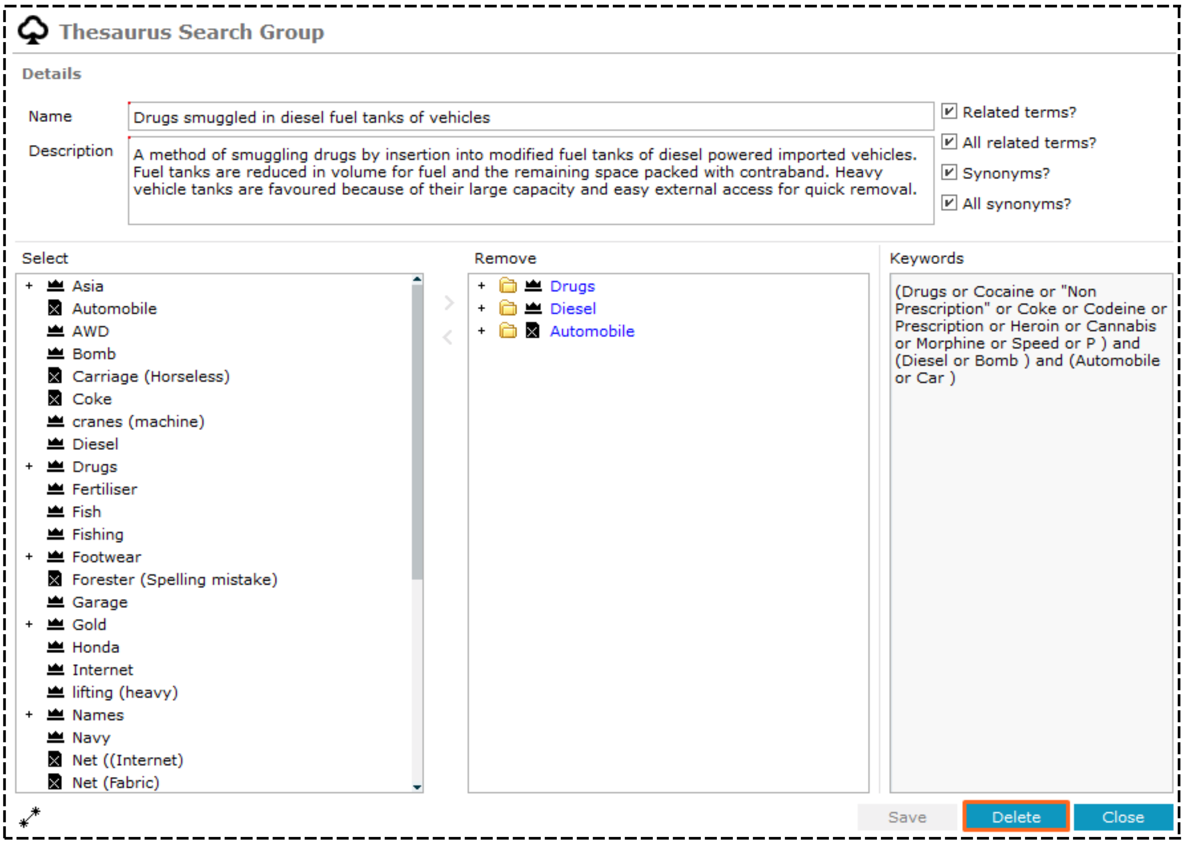
   You can use Soundex to do a phonetic search so any words that sound like the specified criteria are returned.

   *For example, if you enter **Robert**, the search results might include **Robert** and **Rupert**.*
5. To include deleted search groups in the results, select the **Show deleted** checkbox.
6. Select **Search**.



Edit or Delete a Thesaurus Search Group

1. Select **Admin** > **System** > **Thesaurus** > **Search Groups**.
2. Select the thesaurus search group you want to edit or delete.
3. Click **Select** or double-click the selected search group.
4. Make your changes and select **Save** or select **Delete**.



Time Zones

Because the information you collect can be from many different locations and time zones, all information is recorded with a time zone and local time.

This make it possible to show events in different time zones in the correct chronological order.

This is how time zones work:

- The date and time are set on the application server to provide the base line for dates and times in the database.
- Clients can have a different time zone set to that on the server, if they're located in a different time zone from the server.

  See Change the Default Time Zone in the user guide.
- Clients can record dates and times for different time zones by setting the correct time zone for that time when they enter data.

Setting the Time Zone on the Server

The server date and time, server time zone, and client time zone determine the date and time values applied automatically when you enter data.

Set the server time zone by using the Time Zone screen on the Windows Control Panel Date and Time Properties.

For ICM to work properly, the server time zone must be set correctly.

Set Time Zone on Application Server

1. Open the Windows Control Panel on the application server.
2. Double-click the Date and Time icon.
3. Select the **Time Zone** tab.
4. Use the drop-down to select the time zone in which the server is located.
5. If the time zone you selected uses daylight saving, select the **Automatically adjust clock for daylight saving changes** checkbox.

   If you select this checkbox, the time is automatically adjusted for the standard start and finish dates of daylight saving in that time zone.

   *If the start or finish of daylight saving varies, you can record this on the **Time Zones** screen.*
6. Select **OK**.

   Use the Date and Time screen on the Date and Time Properties screen to set the date and time on the server.

Set Date and Time on Database Server

1. Open the Windows Control Panel on the database server.
2. Double-click the Date and Time icon.
3. Select the **Date and Time** tab.
4. In the **Date** area, specify the current date of the time zone in which the server is located.
5. In the **Time** area, specify the current time of the time zone in which the server is located.
6. Select **OK**.

   If you operate in multiple time zones, set the time zone on the local workstation.

Manage Time Zone Variations

You can record the:

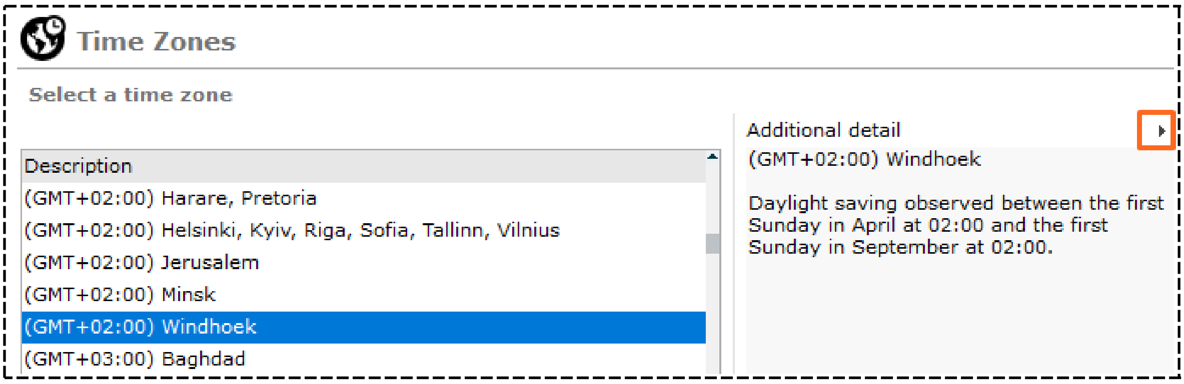
- Introduction of daylight saving in a time zone that doesn't use daylight saving.
- Permanent end of daylight saving in a time zone that currently uses daylight saving.
- Variation of the start or finish date and time in a time zone that currently uses daylight saving.

Don't use the *Time Zones* screen for the usual variation between standard and daylight saving time on the normal start or finish date. Windows handles this variation automatically.

The Global Administrator is the only user who can manage time zones. Users who have an Administrator or Agency Administrator permission can view the screen, but they can't change it.

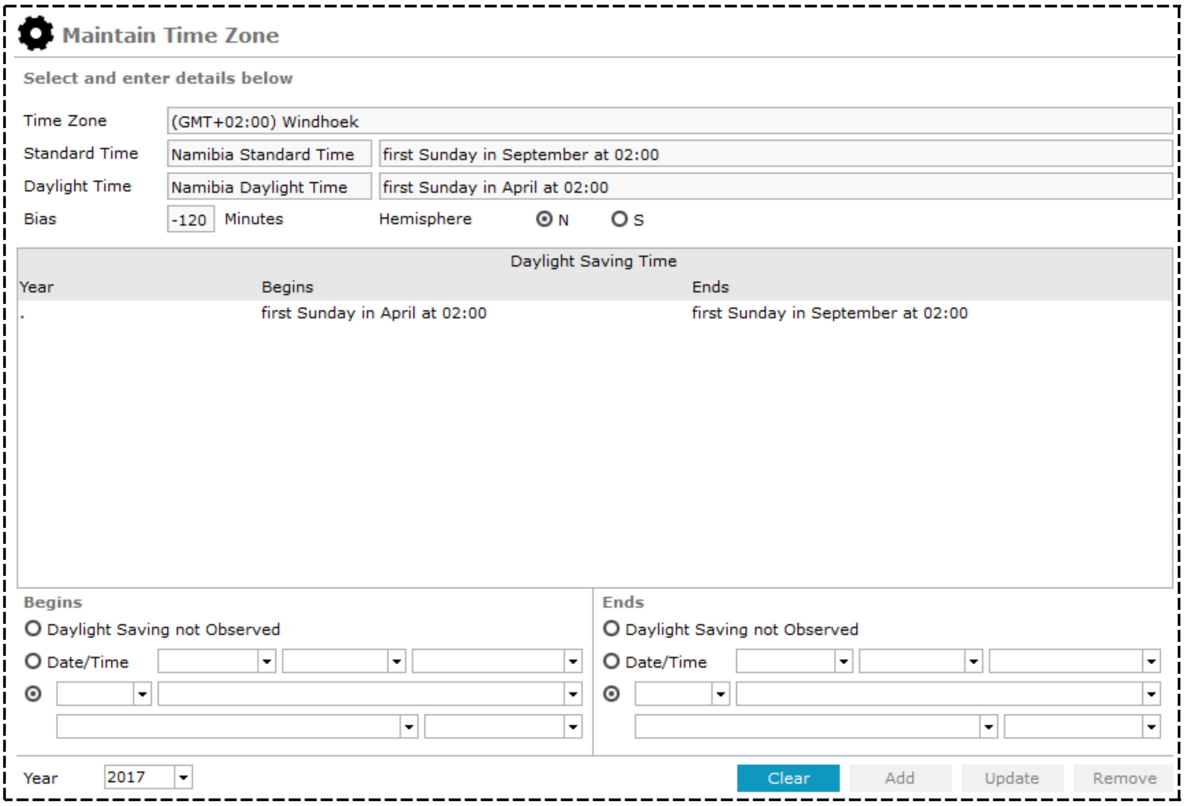
Manage Time Zone Variations

1. Select **Admin** > **System** > **Time Zones**.
2. To see more details about a time zone, simply select it.
3. To hide or show the **Additional Detail** pane, select the hide ▸ or show ◂ arrow.



Edit a Time Zone

1. Select **Admin** > **System** > **Time Zones**.
2. Double-click the time zone you want to change or select it > Click **Select**.
3. Select the last row in the table.
4. Change when daylight savings starts and ends.
5. Select **Update**.



Manage Search Words

You manage a list of words you want excluded from particular searches.

For example, words like **as**, **the**, **but**, **to**, and **for** don't enhance your search.

You can also see how many times certain words have been used.

Exclude Words from Standard or Extended Searches

Use the Standard screen or Extended screen to manage a list of words that will be excluded from a standard or extended search.

To manage the list of words that are excluded from a search:

1. Select **Admin** > **System** > **Search Exclude Words**.
2. Perform one of the following actions.

   To exclude words from the:

   - Standard search, select the Standard tab to display the Standard screen.
   - Extended search, select the Extended tab to display the Extended screen.
     - Both screens operate in the same way.

       An example of the Standard screen is shown here.
     - Words that are excluded from searches are displayed.
3. To add a word to the list of excluded words:
   a. In the Exclude Word field, enter the word you want to exclude from the search.
   b. Select **Save** or press **Enter**.

      The word displays in the list on the screen.
4. To remove a word from the list of excluded words:
   a. Double-click the word you want to remove from the list of excluded words.

      The selected word displays in the Exclude Word field.
   b. Select **Delete**.
   c. Confirm you don't want to remove the selected word.

5. Select **Yes**.


Search Exclude Words
Standard
Extended
Usage
Select and enter details below
Words
and
because
car
for
that
to
Exclude Word

Import and Export Setup Data

If you need to change how ICM is set up, you can:

1. Export setup data from one ICM system.
2. Import this data into an empty or older ICM system.

   The ICM system you're importing setup data into must not contain setup data.

   *You need the **Can export/import configuration** permission to import and export setup data.*

Limitations to Importing and Exporting Data

- For some setup changes you need to import setup data several times.

  For example, you might first need to import an object if other objects depend on it.
- If you cancel an import, the changes that have already been made won't be rolled back.

  This is because each object imported is committed individually.

  If you need to roll back to an earlier setup, restore the configuration from a backup copy of the database.
- You can't change an attribute property.

  For example, you can't change the URN format for an entity.

Business Rules

Types of Entities

- System entity types (like person or location) are imported if they don't exist in the target system.

  These should have already been created when you first set up your system.

- Attributes aren't updated for entity types that already exist in the target system. This includes system entity types.
- If an entity type already exists in the target system:
  - But it has no entity category, it will be updated to match the source system.
  - And is already in a category, it won't be changed in the target system.
  - But isn't selected for the current agency, it will be updated to match the source system.
  - Its display sequence will be updated to match the source system where possible.

    This depends on the category and what other entity types are in the category.

- New entity types in the target system will have the same display sequence as the source system.
- New compound entity types will have their **Inherited from entity type** set.
- If an entity type already exists with no **Inherited from entity type** set, this won't be updated.
- Security profiles are included in the entity type import.

  Users, teams, and designations are excluded.

What Happens to Types of Entity Attributes when You Import Setup Data

- ICM will try to set references to code tables, conditions, and calculations.

  If these already exist, they will be set for any existing entity attribute types included in the import to the target system.

- If an entity attribute type already exists in the target system, any references to code tables, conditions, and calculations will be added.
- References to code tables, conditions, and calculations that already exist in the target system won't be changed.
- Attribute types will be added to compound entity types if this reference exists in the source system, but not the target system.
- Existing attribute types on existing compound entity types in the target system won't change.
- Entity attribute type conditions will be imported even if one of their conditional entity attribute types doesn’t exist in the target system.
- ICM will try to set the code table or conditional attribute type for an attribute type condition.

  It will log an error if it can't find the code table or conditional attribute type.

- If there's an existing attribute type condition in the target system, any references to code tables or conditional attribute types will be added.
- The following automatic attribute types (which are created when the entity type is created) aren't removed from the target system.

  This is true even if they have been removed in the source system:

  <all Case Entity Types>::status

  Media::MetaData

  Document::MetaData

  Image::MetaData

- Attribute types that are automatically added with entity types won't be updated.

  The same is true for existing attribute types.

- Attribute types are matched by name.

  If the name of an automatically created attribute type is changed in the source system it will be imported alongside the automatically created attribute type with the old name in the target system.

- Automatic attribute types are matched by an internal name.

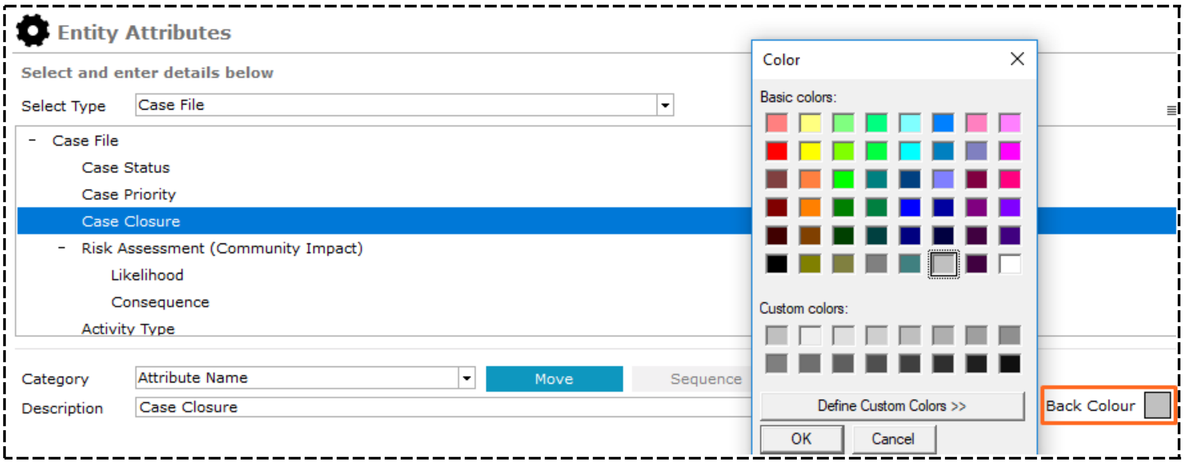
  So if the attribute type name has changed in the source system, it will still match the attribute type with the old name in the source system.

  The name, comments, and behaviour of the automatic attribute type in the target system will be updated to match the source system.

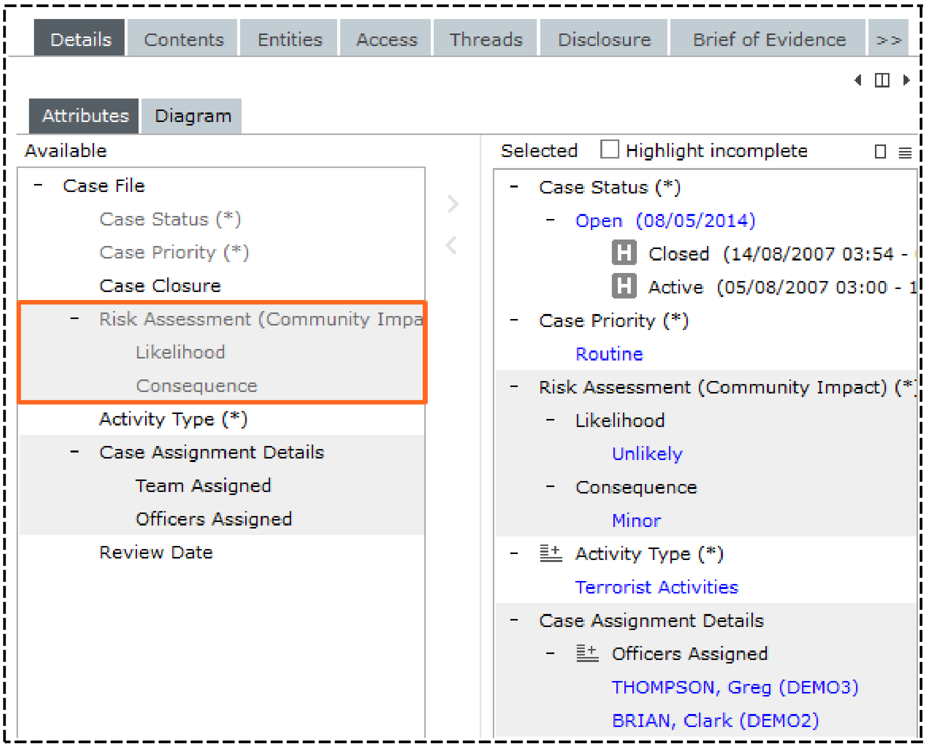
Make it Easier to Look at Entity Attributes

You can make the data on the **Attributes** screen easier to read by adding a background colour to an attribute row:

1. Select **Admin** > **Entity Definition** > **Attributes**.
2. Select the type attribute you want to shade.
3. Select the **Back Colour** checkbox > Select a background colour > Select **OK**.



4. Save your changes.
5. Open the type of entity you changed to see the shaded rows.



Export Data from ICM

1. Select **Admin** > **System** > **Export**.
2. Select the type of data you want to export.
   - **General Config – Entity / Attribute / Relationship Types**
   - **Users / teams / designations / Roles**
   - **Access / Security Profiles**
3. Select **Browse** to specify where you want to send the exported data file.
4. Select **Export**.

Import Different Kinds of Data into ICM

1. Select **Admin** > **System** > **Import**.
2. Select the type of data you want to import.
   - **General Config – Entity / Attribute / Relationship Types**
   - **Users / teams / designations / Roles**
   - **Access / Security Profiles**
   - **Brief of Evidence Config**

     For more details, see "Import Brief of Evidence Codes".
3. Select **Browse** to find and select the files you want to import.
4. Select **Load**.

Copy a Case

You can send the details of a case to your laptop. This is useful if you're a case officer working in the field and you need to carry the details of a case with you on a laptop.

Case information is synchronised with the server so you'll have access to the latest information.

Auditing

All updates to entities are audited in a similar way to entity updates via screens.

An audit record is generated each time you try to import or export a case.

Synchronisation

Having data synchronised between the server and the laptop allows the laptop to show server case data and collect new data for a case.

The case data on the server is the master copy. It won't be changed by any imports except when new data that doesn't exist on the server yet is imported from the laptop.

This includes data from adding:

- A new entity
- A new attribute to an entity
- Another value to a multi-valued attribute.

For example, if a case has two officers assigned to it (stored as two attribute values), adding another officer to the case on the laptop is regarded as new data when the case is imported back onto the server.

If you changed one of the officers assigned, this change would be ignored when the data was imported by the server.

When you're dealing with case data on a laptop it's important to remember that:

Importing a case to a laptop brings all the current case data and any related subentities onto the laptop. The exception is Tasks, Task Results, Property management data and Disclosure data.

- Any new data you add to a case on the laptop will be added to the server when you import the case to the server.
- You are warned about any data that's overwritten on the laptop when you import case data to the laptop.
- You are warned about any case data you changed on the laptop that wasn't uploaded to the server when you imported the laptop case data to the server.

Entity Identification

This section explains how entities are identified and synchronised between a server and laptop.

Server

On a server all entities are identified by their Unique Reference Number (URN).

The URN is made up of an optional prefix and a unique ID to show the entity type.

For example, General Case Notes has the URN GCN\9999999.

9999999 is a sequence number starting at 1.

Laptop

- Entities from the server imported to the laptop keep the same URN.
- Entities created on the laptop are allocated a temporary URN by creating a normal URN but replacing the first **0** of the sequence number by **T**.

  For example, GCN/000023 becomes GCN\T00023.

  This means a URN created on the laptop can't clash with a URN on the server when its imported to the server.
- When an entity created on a laptop is imported to the server it's allocated a permanent server URN.

  When it's next exported to a laptop, the temporary URN of the entity on the laptop is replaced by the permanent URN from the server entity.

System Identification

Two parameters are used to identify the type of database system. This information allows the replication function to check the replication is being run against the correct systems.

The Database ID should be unique for every laptop system. The Database ID of the server system isn't used for any purpose in the import or export process.

Laptop systems should have the **Laptop System** checkbox selected. The system marked as a laptop system can reside on any system like a desktop, server, or other compatible computing device.

Configuration Compatibility

The configuration of the copy of ICM installed on the laptop and the server must be the same for replication to work.

Use the Export / Import feature to achieve this by exporting from the (master) server copy and importing that configuration into the laptop copy.

User Information Transfer

A case and all its associated data might contain several references to users, teams, designations, and roles. This information can differ between a laptop and a server.

To make sure all references to roles, designations, teams, and users are resolved, these are exported from the server and imported to the laptop.

The server contains the master list of users. This means data can only move from the server to a laptop, not in the other direction.

Importing and Exporting Cases

We recommend you create two folders to receive the exported data and label them clearly so you don't get mixed up.

For example:

- **\ExportedFromServer**
- **\ExportedFromLaptop**

Importing Case Data to Server

Case Data Included

Cases can only be imported to a server one case at a time.

Case data is located in the folder that it was exported to from the laptop system.

Source entities and any tangible subentities (for example, Persons, documents, locations) are included in the import. Task data isn't imported as it isn't exported from the laptop system.

Matching Process

A matching process determines whether a new entity is to be created on the server or an existing entity on the server is to be updated.

Server Data Update Rules and Conflict Logging

The rules governing when server data is updated and how conflicts are logged are:

Server Entity Field or Attribute Being Updated	Laptop Import File Entity File Entity Field or Attribute	Action
Present	Present and same	None
	Present and different	No update Message to log
	Absent	Retain server data
Absent	Present	Update server with laptop imported data
	Absent	None

You can see from the above that if you change an attribute on an entity it won't change the server data. But if you add an attribute then the server data will have the additional attribute data added to it.

Multiple Values

- If a field has multiple values, any new values in the import file from the laptop are added to the server data and no existing server data values are removed.
- If a “child” object has multiple values (for example, the case roles for a case), then if the object being imported doesn't exist on the server, it is added.

  If the object exists on the server, it's updated field by field according to the rules in the table above.

  To decide whether an object is new to the server or already exists on it, a key field which depends on the type of object, is used.

Importing Case Data to a Laptop

Case Data Included

You can only import a case to a laptop one case at a time.

Case data is in the folder it was exported to from the server system.

Source entities and any tangible subentities (for example, persons, organisations, documents, images, contact numbers, events, media, and locations) are included in the import.

Matching Process

A matching process determines whether a new entity is to be created on the laptop or an existing entity on the laptop is to be updated.

Laptop Data Update Rules and Conflict Logging

The table outlines rules that govern when laptop data is updated and how conflicts are logged.

Laptop Entity Field or Attribute Being Updated	**Server Download File Entity Field or Attribute**	**Action**
Present	Present and same	None
	Present and different	Update laptop data. Write log message.
	Absent	Remove laptop data. Write log message. References to other entities are removed but not the other entity itself.
Absent	Present	Update laptop data with server data.
	Absent	None

Exception for Relationships

There's an exception to these rules:

Entity relationships that are present in the laptop system but not in the import files, aren't removed.

Multiple Values

If a field has multiple values:

- Any new values in the import file from the server are added to the laptop data.
- Any existing values in the laptop data that are not in the import file are removed.

If a child object has multiple values and the object being imported doesn't exist on the laptop system, it will be added. This could happen with case roles for a case.

If the object exists on the laptop, it's updated field by field according to the rules in the table above.

Any objects that don't match an object being imported, are removed.

ICM uses a key field to decide whether an object is new to the laptop or already exists on it.

Laptop Entities with Temporary URNs

An entity will have its permanent URN set from the imported server entity if:

- It's created on the laptop.
- It's on the laptop and its temporary URN is updated.

Laptop Data at Completion of Import Process

When the server data has been imported onto the laptop, all imported entities will be exact replicas of the server entities at the time of the export.

Laptop entities might end up with more relationships to other entities than the same entity that exists on the server. This is because those extra relationships on the laptop aren't deleted.

Data Loss

Data on the laptop might be lost during the import. Use the conflict log if you need to restore data.

Export Case Data

You can export data if you have the *Case Administrator* permission.

This example shows how to export from a server:

1. Use ICM on the server or laptop to find and open the case you want to export.
2. Select the Overflow >> tab > Select **Export (for server)**.
3. Select **Browse** to specify where you want to save the case file.

   This file location should be on a USB drive or a network drive that can be accessed from the laptop.
4. Select **Encryption not required** if you don't need the files to be encrypted.

   Only use this for diagnostic purposes.
5. Select **Export** > **Select OK.**.

   The data is sent to the location you specified.

   Progress is shown in the *Log* area.

   The entries are also written to a file called **case export<n>.log**. **n** starts at a value of 1 and increments by 1 for each successive log written.

   The first case export log will be named **case export1.log**.

   When it reaches a certain size, it's closed. Logging will continue with a log called **case export2.log**.

   Logs are written to the **\logs** folder in the server environment folder.

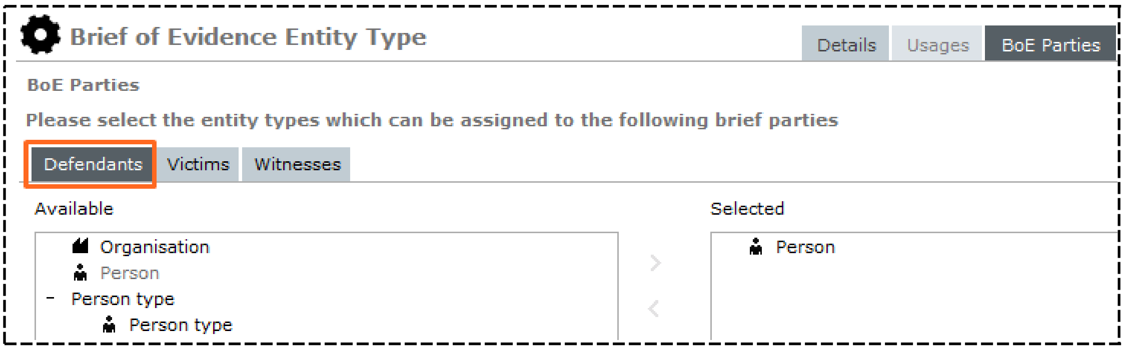
BRIEF OF EVIDENCE

Create a Type of Entity for a Brief of Evidence

1. Select **Admin** > **Entity Definition** > **Types**.
2. Select **New** > Select **Brief of Evidence** > Select **OK**.
3. Enter a description of the type of brief you're creating in the field provided.

4. Select the types of entities users can assign to brief of evidence parties:
   a. Select the **BoE Parties** tab.
   b. Select the **Defendants** subtab.
   c. Double-click or use the Select icon to select the types of entities that will be available to use for defendants.

   These will usually be types of person entities you've set up in ICM.



5. Select the types of entities that can be used for victims:
   a. Select the **Victims** tab.
   b. Double-click or use the Select icon to select the Person entities.

These will generally be types of Person entities you've set up in ICM.

6. Select the types of entities that can be used for witnesses:

   a. Select the **Witnesses** tab.

   b. Double-click or use the Select icon to select Person entities.

   These will generally be types of Person entity you've specified in your system.

7. Select the **BoE Components** tab.

   Administrative Documents are either documents that can be imported from an external file—like a Disclosure Certificate—or documents that will be generated from a Word template and data you've entered into a brief of evidence*.*

   You can change the default Word templates to meet your needs.

   You can't add new template types.

   a. Select the **Administrative Documents** subtab.

   Select the Add icon.

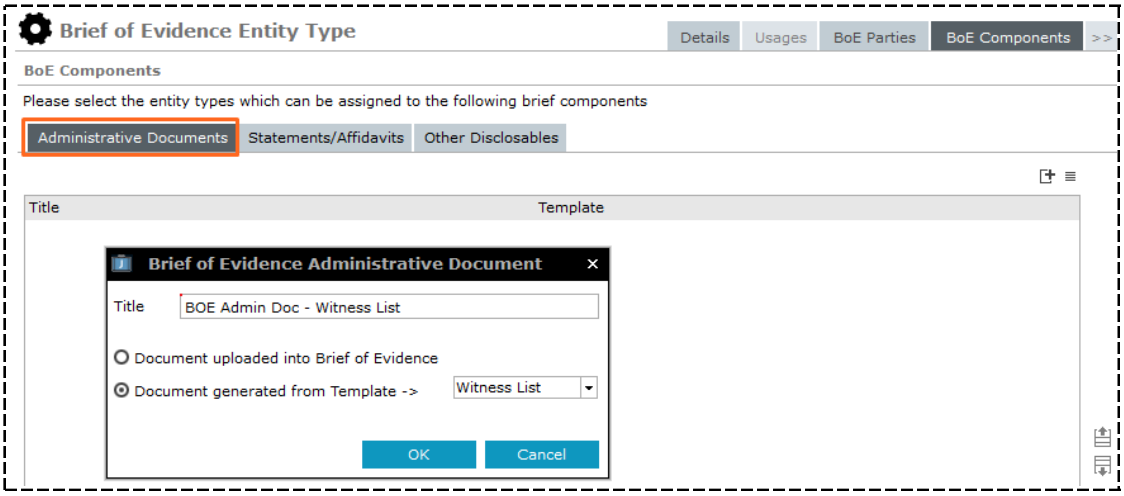
   Enter a title for the admin document.

   Select either of these options to set up the document:

   – **Document uploaded into** brief of evidence to let users upload an external file.

   – **Document generated from template** > Select a template from the drop-down.

Select **OK**.

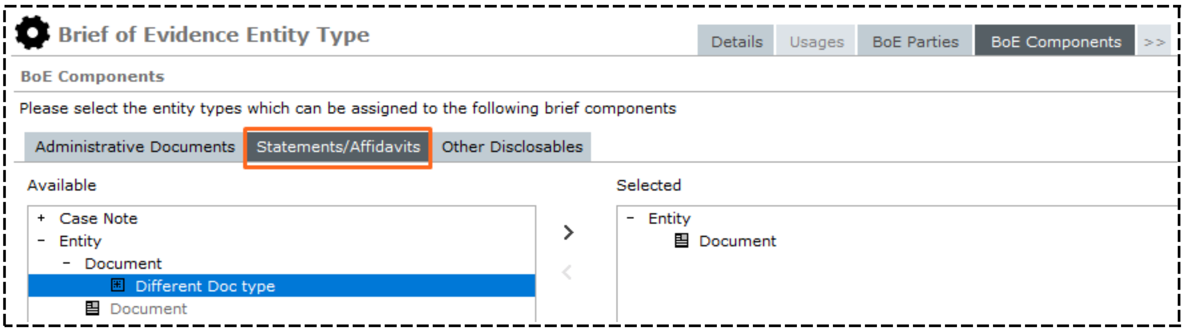


8. Select which types of entities can be assigned to these brief components:

   a. Select the **Statements/Affadavits** tab.

   b. Double-click or use the Select icon to select the entity types that will be available to use as Statements.

      These will generally be types of document entities you've specified in your system.



9. Select the types of entities that can be assigned to the brief components:

   a. Select the **Other Disclosables** tab.

   b. Double-click or use the Select icon to select the entity types that will be available to use as other disclosable documents.

      These will generally be types of Document, Image, or Media entity you have specified in your system.

Manage Brief of Evidence Templates

Templates are normal Word templates containing text and merge fields which are mapped to entity attributes.

You can change the text in these templates to suit your needs.

But you can't change merge field mapping.

1. Select the **Admin** > **Templates** > **Brief of Evidence Templates** option from the main menu.
2. Select a template entry > Click **Select** or double-click the template entry.
3. You can:
   - Extract the template – Select **Extract Template** and specify a destination and filename
   - Upload a template – Select **Upload Template** and specify a source folder and file name
4. Select **Close**.

Brief of Evidence Entity Attributes

Defendant Soft Attributes

A brief of evidence defendant has the System Soft Attributes listed in the following table. None of the attributes are mandatory.

When a brief of evidence defendant is being created, attributes marked "*Default" in the table below are set in this way:

- Existing brief of evidence defendants are searched to find any that have the same name and that are related to Persons of that name.

  These Defendants can be in a different Brief in the same case, or in a different case.
- If any are found, the Defendant which was created most recently, is used as the source from which to copy those attributes marked "*Default", to the Defendant being created.

Attribute Name	Attribute Type etc.	Notes
Address	Free text.	*Default
Aboriginal or Torres Strait	Code table (Yes/No/Unknown)	*Default
Interpreter Needed	Code table (Yes/No)	*Default
Language	Free text	*Default
Criminal record	Code table (Yes/No/Unknown)	*Default
Criminal record details	Free text, conditional on Criminal record = Yes	*Default
Expiry Date for Prosecution	Date	
Defendant arrested	Code table (Yes/No)	
Date of arrest	Date. Conditional on Defendant arrested = Yes	
Defendant on bail	Code table (Yes/No). Conditional on Defendant	

Bail conditions	Free text. Conditional on Defendant on bail = Yes	
Court Date/Time	Date and Time	
Court Name	Free text	
Role in offence	Free text	

Victim Soft Attributes

A brief of evidence victim has the System Soft Attributes listed in the following table. None of the attributes are mandatory.

When a brief of evidence Victim is being created, attributes marked "*Default" in the table below are set in this way:

- Existing brief of evidence victims are searched to find any that have the same name and that are related to Persons of that name.

  These Victims can be in a different brief in the same case, or in a different case.

- If any are found, the Victim which was created most recently, is used as the source from which to copy attributes marked "*Default", to the Victim being created.

Attribute Name	Attribute Type etc.	Notes
Vulnerabilities	Free text, multiple.	*Default

Witness Soft Attributes

A brief of evidence witness has the System Soft Attributes listed in the following table. None of the attributes are mandatory.

When a brief of evidence witness is being created, attributes marked "*Default" in the table below are set in this way:

- Existing brief of evidence witnesses are searched to find any that have the same name and that are related to Persons or Users of that name.

  These Witnesses can be in a different brief in the same case, or in a different case.

- If any are found, the Witness which was created most recently, is used as the source from which to copy attributes marked "*Default", to the Witness being created.

Attribute Name	Attribute Type etc.	Notes
Home address	Free text	*Default
Work address	Free text	*Default
Home email address	Free text	*Default
Work email address	Free text	*Default
Home phone number	Free text	*Default
Work phone number	Free text	*Default
Mobile phone number	Free text	*Default

Import Brief of Evidence Codes

You can the import CSV files that contain the following information:

- Offence acts
- Offence codes – These specify the offences that are possible in a brief of evidence
- Elements of proof that are related to the offences

File Formats

These examples show the file format of each file.

```
Offence Act Description
Biosecurity Act 1993
Civil Aviation Act 1990
```

Offence Codes:

```
Offence Act Description,Offence Code Description,Offence Code Section
Biosecurity Act 1993,Uncleared Imports,30
Biosecurity Act 1993,Boarding of Craft,31
Civil Aviation Act 1990,Requirement to register aircraft,6
Civil Aviation Act 1990,Duties of pilot-in-command,13
```

Elements of Proof:

```
Offence Code Description,Element Of Proof Description
Uncleared Imports,Failure to complete form UI 12
Boarding of Craft,Ignoring boarding request
Boarding of Craft,Physically restraining authorised officer
Requirement to register aircraft,False details declared
Requirement to register aircraft,Failure to notify changed owner
Duties of pilot-in-command,Pilot under influence of alcohol
Duties of pilot-in-command,Pilot under influence of drugs
Duties of pilot-in-command,Failure to obey ATC
Duties of pilot-in-command,Failure to comply with NOTAMs
```

Import Brief of Evidence Data

1. Select **Admin** > **System** > **Import** > **Brief of Evidence Config**.
2. Select **Browse** to find and select each file you want to import.
3. Select **Load** to import the files.

   Details are provided about any errors encountered.

Managing Brief of Evidence Codes

Brief of evidence codes are managed in the same way as all other system codes.

Select **Admin** > **Code Tables** > **Offence Acts** to manage brief of evidence codes.

Brief of evidence codes have a hierarchy: | | The brief of evidence codes are related by these rules:

- Each Offence Act can have one or more Offences Codes associated with it.
- Each Offence Code can have one or more Elements of Proof associated with it.

The following rules apply if you want to delete brief of evidence codes:

- You can only delete codes that aren't being used by any briefs of evidence.
- Elements of Proof must be deleted before the Offence Code that they belong to can be deleted.
- Offence Codes must be deleted before the Offence Act that they belong to can be deleted.

Upgrading Your Version of ICM

This content explains how to upgrade your version of Jade Investigations Case Management (ICM).

It applies to ICM version 6 or higher.

If you're running behind with your upgrades, you'll need to upgrade from one major version to another, step by step. For example, you'll need to go from 6.0 to 6.1, and then to 6.2. You can't jump from 6.0 to 6.2.

If you're using ICM version 5 or lower, contact us to learn how to upgrade.

This content uses an installation on the D drive as an example to illustrate the upgrade process:

- D:\Investigator\c_bin
- D:\Investigator\c_system
- D:\Investigator\c_bin\jade.ini

You might have a different folder structure for your installation of ICM.

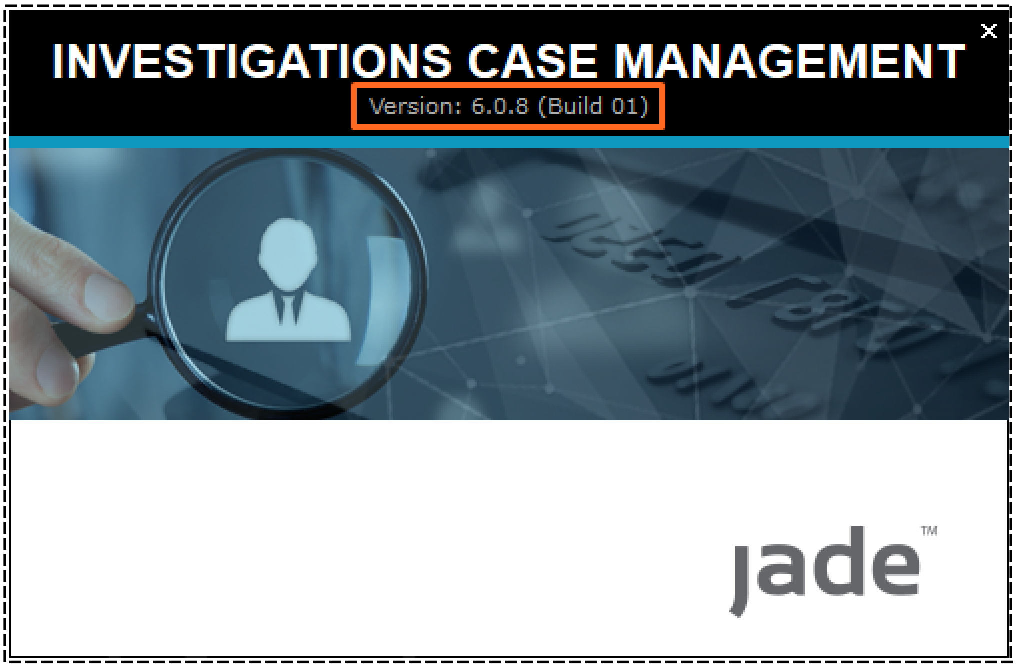
For example, you might:

- Not have the **c_** prefix for the **bin/system** folders.
- Have a different location for the **jade.ini** file.

If this is the case, you'll need to adjust the instructions to match your installation.

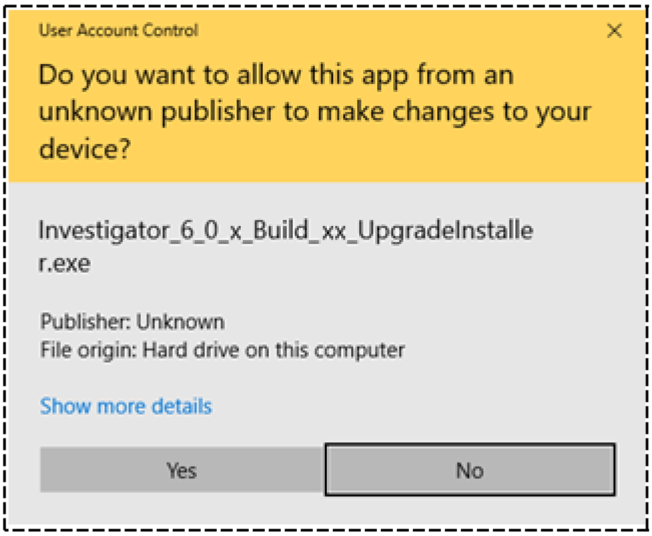
What Version of ICM Am I Using?

Select **Help** > **About**.

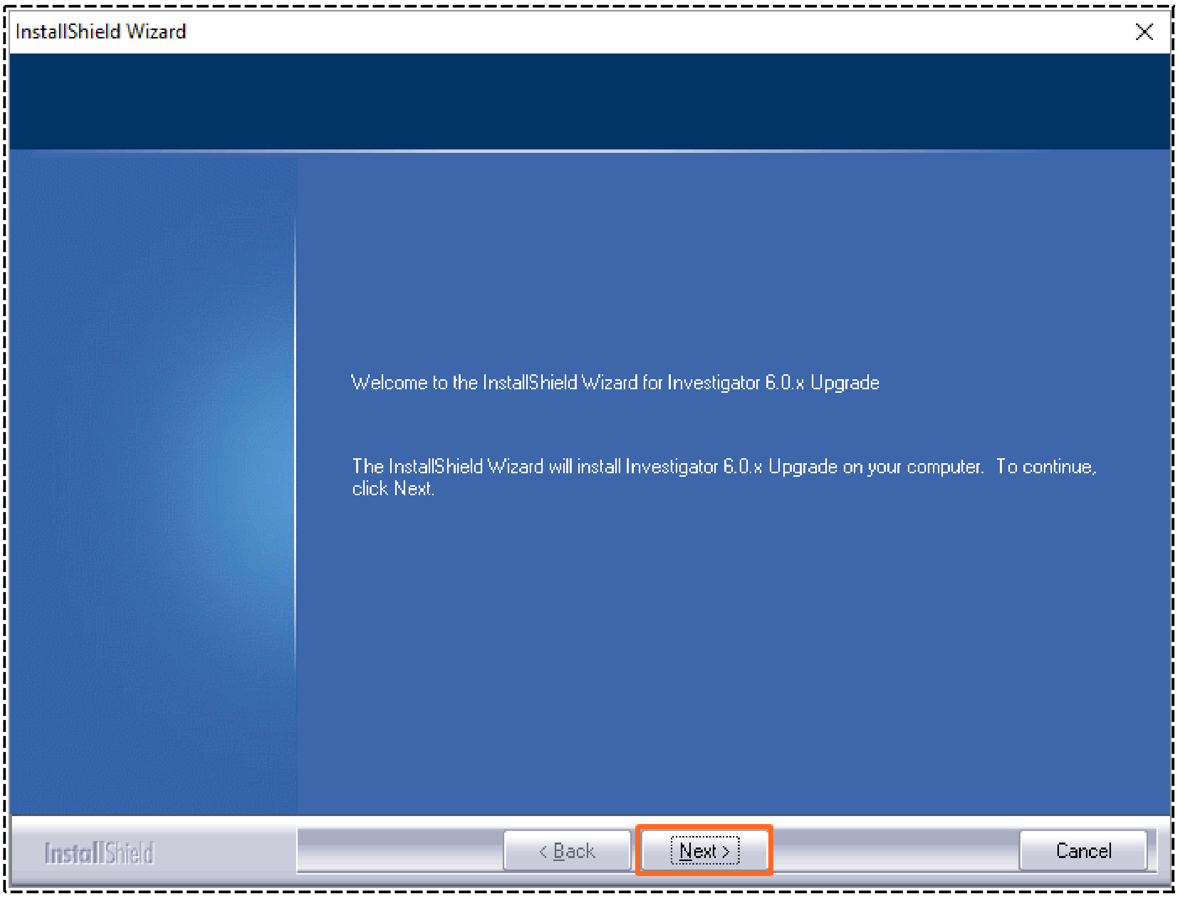


Upgrade Your Version of ICM

1. Make sure everyone in your organisation stops using ICM.
2. Open the ICM installation file –**Investigator_6_x_x_Build_xx_UpgradeInstaller.exe**.
3. Select **Yes** if you see the **Use Account Control** window.



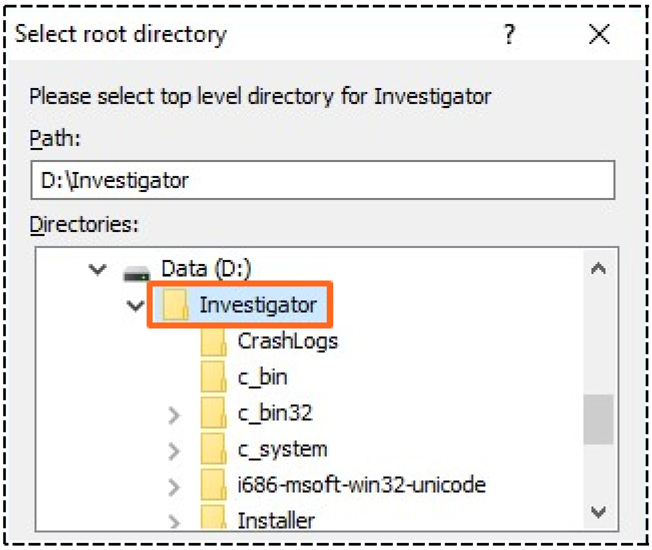
4. Select **Next** on the InstallShield Wizard to start the installation.



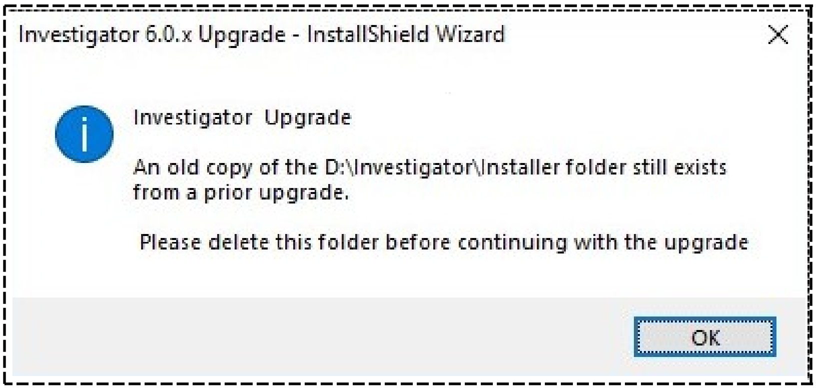
5. Select the browse

 button beside the **Install Directory** field > Choose the existing installation you want to upgrade.

6. Select the folder that contains the **bin/system** folder > Select **OK**.

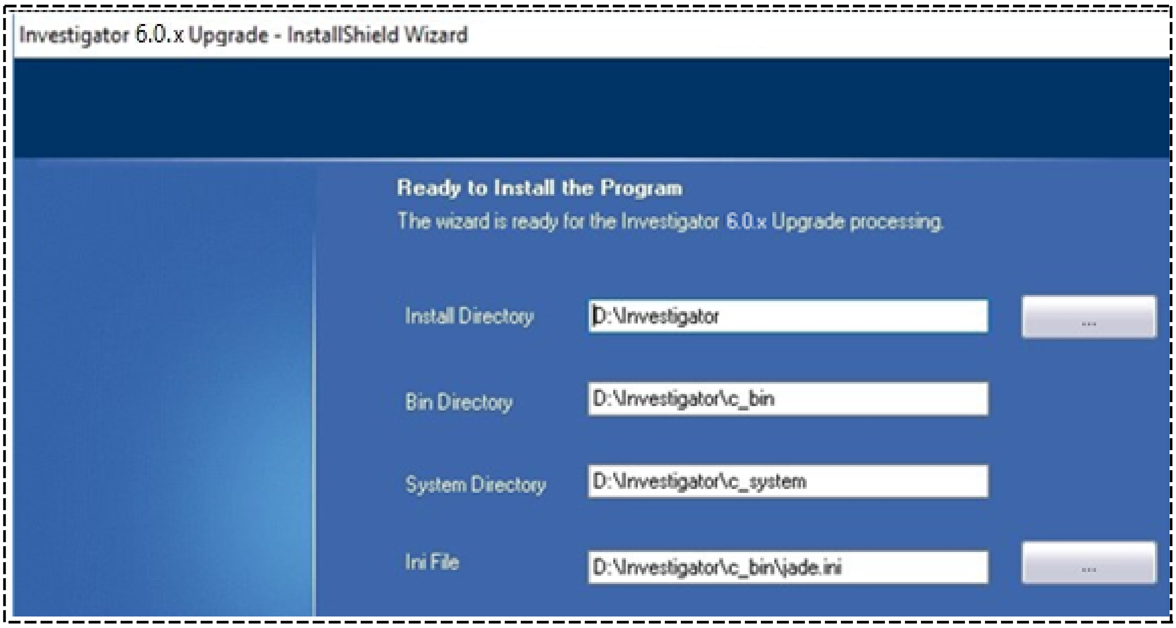


If you've previously aborted an upgrade, you might see this message:



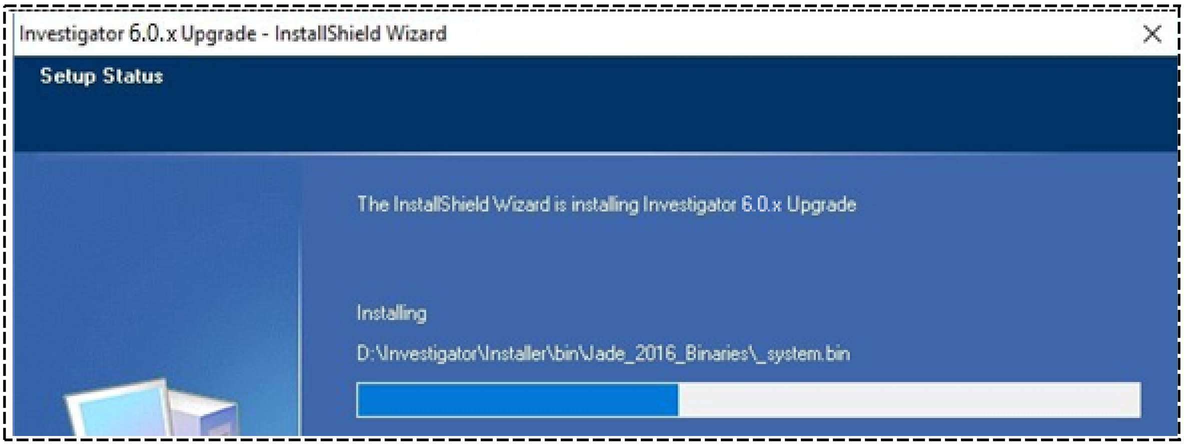
To resolve this, delete the existing **Installer** folder under **D:\Investigator** – The InstallShield Wizard should now automatically populate the directory fields and the location of the INI file.

7. Make sure the folder locations are correct for your system > Select **Next**.

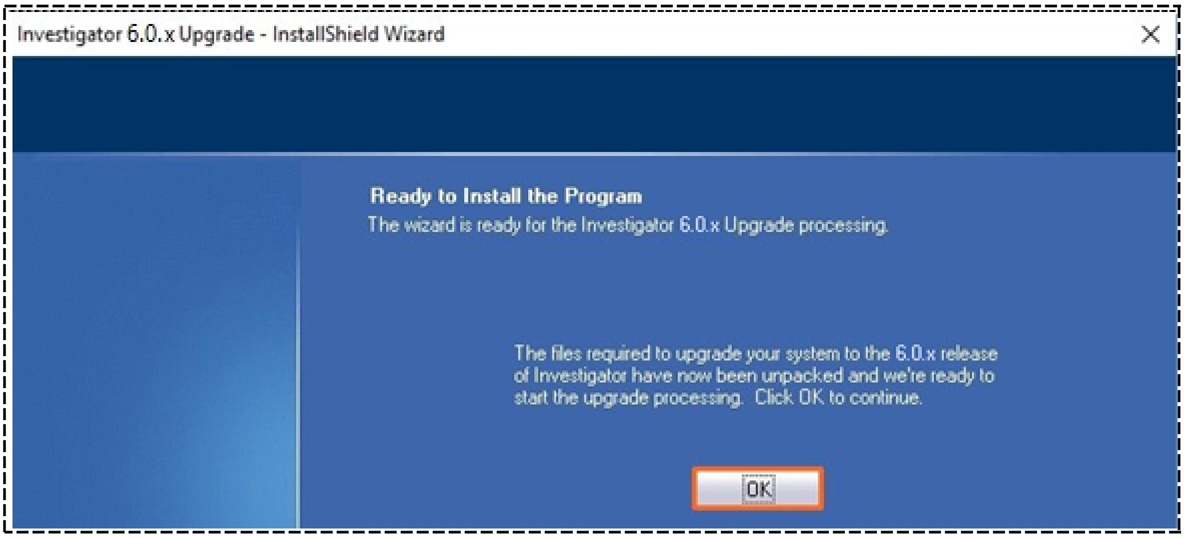


8. Select **Install** to proceed with the installation using the folder locations and INI file specified.

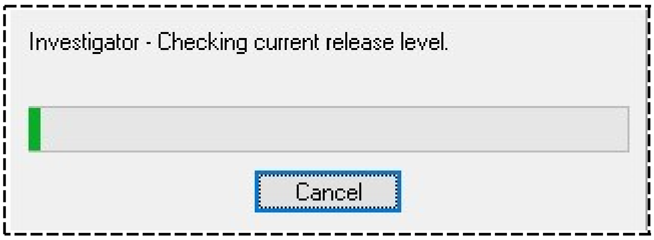
9. Wait while the files are unpacked.



10. Select **OK** to start the upgrade.

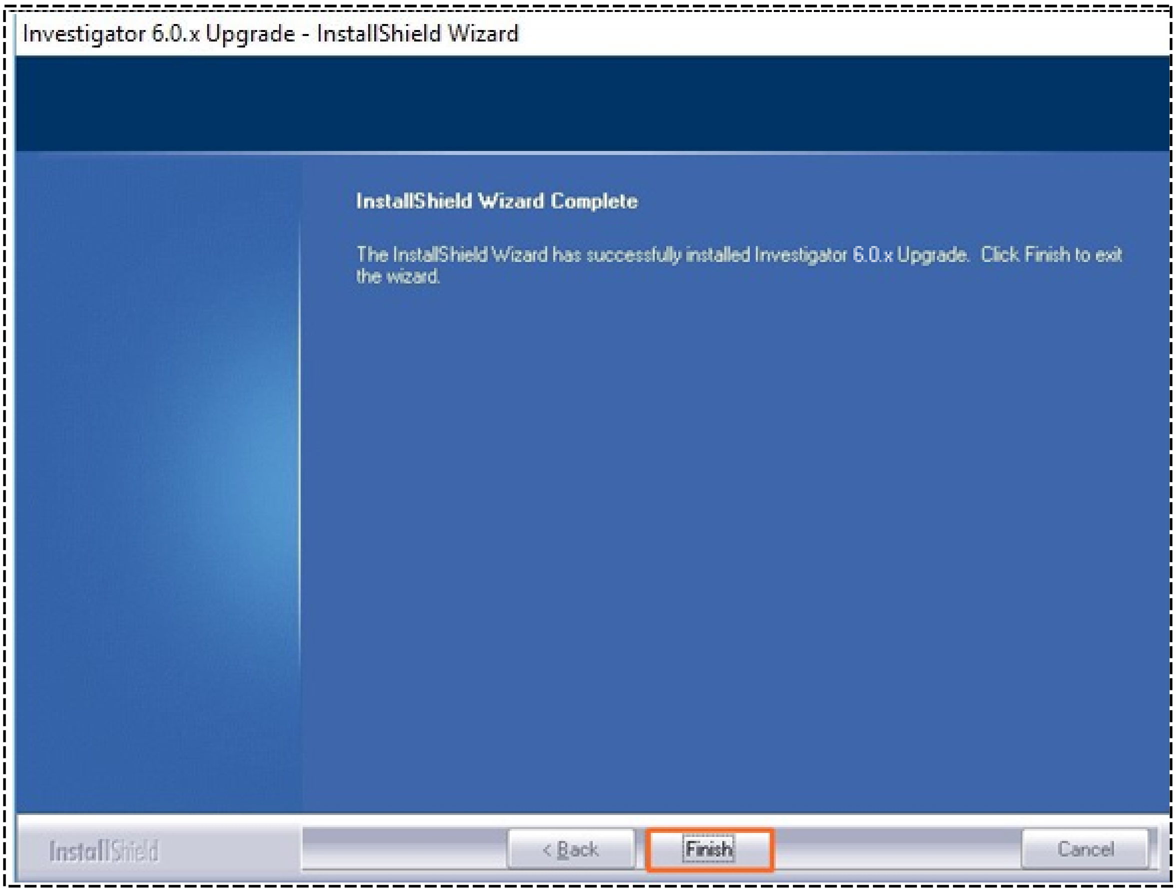


You'll see a progress window with status messages about each phase of the upgrade.



When the upgrade is complete, you'll see message that says **Installation Complete**.

11. Select **Finish** to close the InstallShield Wizard.



12. Do a backup before you allow people in our organisation to use ICM again.

Problems Upgrading?

In the unlikely event of an error during the upgrade, you'll see a message about the problem and the phase in which it happened.

If possible, please include a screenshot of the message when you contact ICM Support.

Please make sure you include any logs and **cn_dump** files that were created or updated around the time of the failure. This will help us diagnose what happened.

New Licence Requirements

You'll need a new licence to use ICM 6.1 and higher.

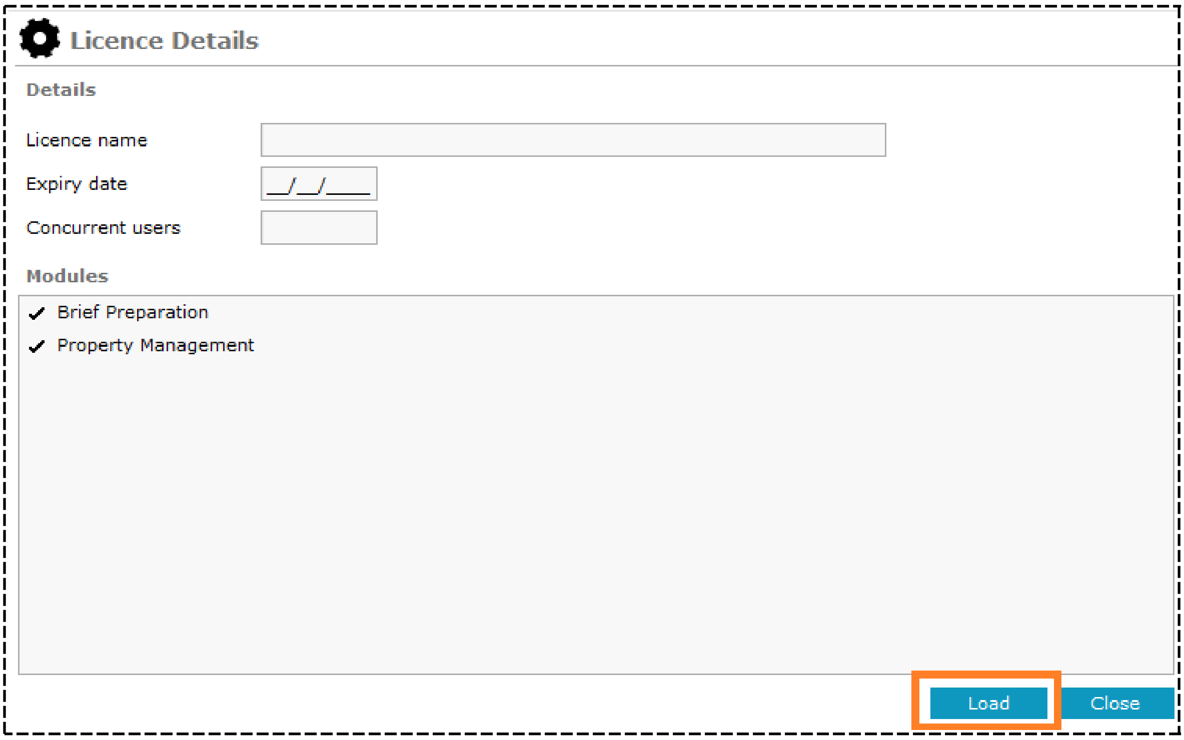
If you haven't got your new licence yet, please email icmsupport@jadeworld.com and let us know if you want the following modules:

- Brief of Evidence Preparation
- Property (Evidence) Management

  There's no charge for these extra features.

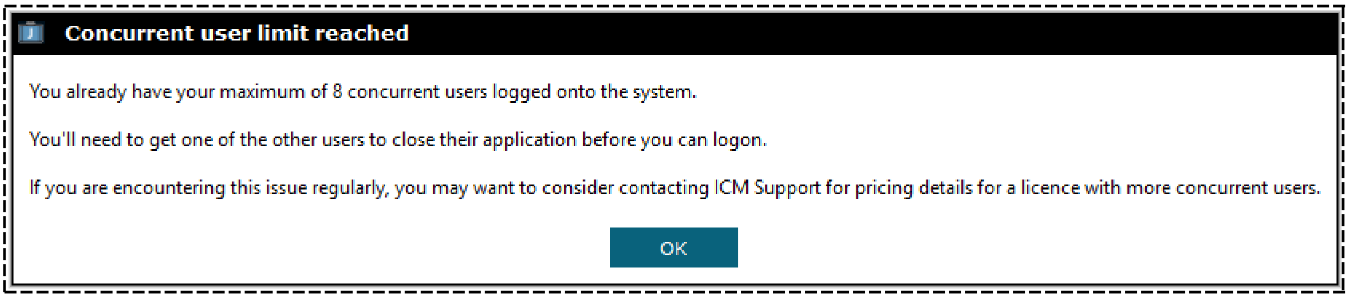
To load your new licence:

1. Select **Admin** > **System** > **Licence**.
2. Select **Load**.



3. Locate and select your licence file.
4. Select **Open**.
5. Select **Apply** to load your licence.

The new licence includes the number of concurrent users allowed. Logon attempts beyond this limit will be blocked.



There's a 10-week grace period to load your licence once you've upgraded to 6.1. After that you'll need to contact ICM Support to log in to ICM.