



# Investigations Case Management - Release Notes

VERSION 6.2.2

**jade**<sup>TM</sup>

## Overview

These 6.2.2 release notes explain the new features available in this release of Jade Investigations Case Management (ICM) .

There are changes for:

- [Regular users](#)
- [ICM System Administrators](#)

We've also [resolved a few minor issues](#) in this release.



## Changes for Regular Users

This section explains the changes in the 6.2.2 version of ICM that apply to regular users.

### Prevent a User from Accessing a Case

You can blacklist a user to prevent them from accessing a case.


If a user has been blacklisted, they won't be able to open the case or see the case in a search result.

If they try to access the case from the Favourites or Recent areas, they'll see a message that says:

*Your access to this entity has been removed.*

*You can't blacklist a Case Officer.*

To blacklist a user:

1. Open the case you want to prevent the user from accessing.
2. Select the **Access** tab.
3. Select the **Blacklist** subtab.
4. Select the user you want to blacklist.
5. Use the Select  icon to select them.

6. Save your changes.

**Case File [URN: 2]**

Details Contents Entities **Access** Comments (1)

**Access**

Security access Black list Bulk access

Available	Selected
Migration, (MIGRATE)	
ADMINISTRATOR, Default Agency (DEFLTADMIN)	
BOBSON, Johnny John (JI0006)	BOBSON, Johnny John (JI0006)
BRIAN, Clark (DEMO2)	
<b>DENBY, Joe (JODOC)</b>	
DOCUMENTATION, Tech (JIDOC)	
HAY, Greg (GREGH)	
MASON, Robert (DEMO1)	
MCDONALD, Shirley (CNWSAS1)	
NAVARA, Nicky (NICKYN)	
THOMPSON, Greg (DEMO3)	
USER, Demo (JI0005)	

>

<

## Edit a Phase or Line of Enquiry For a Completed Task or Task Result

For tasks and task results that have been completed, you can change a phase or line of enquiry.

## Map Comments when You Import Entities

When you import a file containing entities, you can map your comments.

When you select an attribute that has comments, you can map one of the columns in the file to the comments for that attribute.

## You'll Be Warned If You Export More Data to Excel than a Field Can Display

The row height in Excel has a hard limit. This means if you export a lot of data from ICM to Excel, Excel will visually truncate data that's too long to display in a field.

*The point at which truncation occurs is unpredictable because it also depends on the column width.*

We've added a warning message in ICM to remind you that some of your data might be hidden when you export it to Excel.

ICM will warn you if the amount of data in a **Description** field exceeds the predetermined length [set by your ICM system administrator](#). It won't limit or truncate the data.

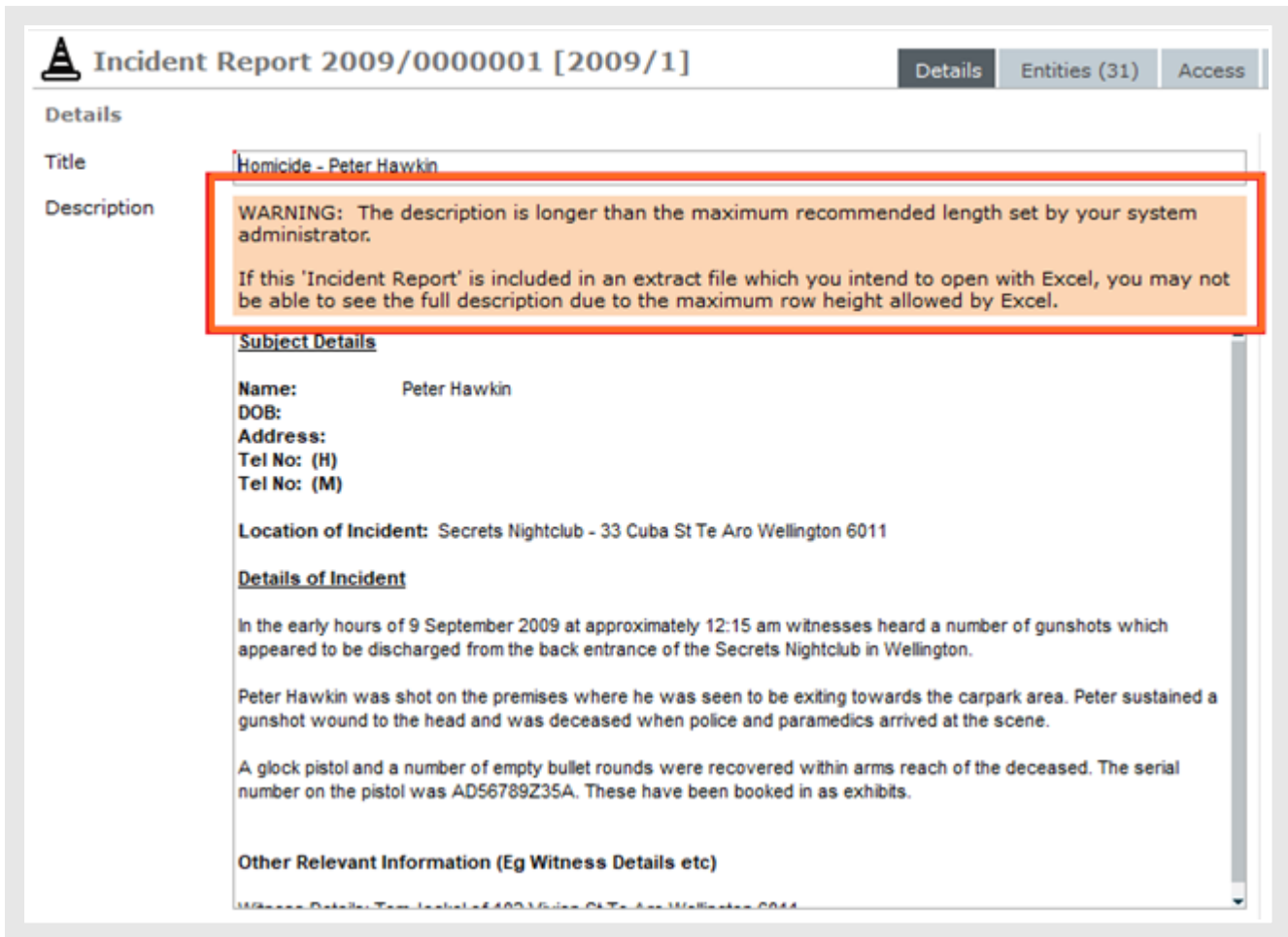
This warning is in place for exporting:

- [Source entities](#)
- Property Reports
- Property Items

The warning is re-evaluated when you tab out of the **Description** field. You'll only see it if there's hidden data.

You'll also be warned if you open an entity in which the Description exceeds the limit.

*You'll still be able to save longer descriptions.*



**Incident Report 2009/0000001 [2009/1]**

Details Entities (31) Access

**Details**

Title Homicide - Peter Hawkin

Description

WARNING: The description is longer than the maximum recommended length set by your system administrator.

If this 'Incident Report' is included in an extract file which you intend to open with Excel, you may not be able to see the full description due to the maximum row height allowed by Excel.

Subject Details

Name: Peter Hawkin

DOB:

Address:

Tel No: (H)

Tel No: (M)

Location of Incident: Secrets Nightclub - 33 Cuba St Te Aro Wellington 6011

Details of Incident

In the early hours of 9 September 2009 at approximately 12:15 am witnesses heard a number of gunshots which appeared to be discharged from the back entrance of the Secrets Nightclub in Wellington.

Peter Hawkin was shot on the premises where he was seen to be exiting towards the carpark area. Peter sustained a gunshot wound to the head and was deceased when police and paramedics arrived at the scene.

A glock pistol and a number of empty bullet rounds were recovered within arms reach of the deceased. The serial number on the pistol was AD56789Z35A. These have been booked in as exhibits.

Other Relevant Information (Eg Witness Details etc)

## It's Easier to Manage Exclusions for Disclosure

### Previously




For tasks and task results, only the case officer and the person who created the task could perform disclosure on tasks and task results in that case.

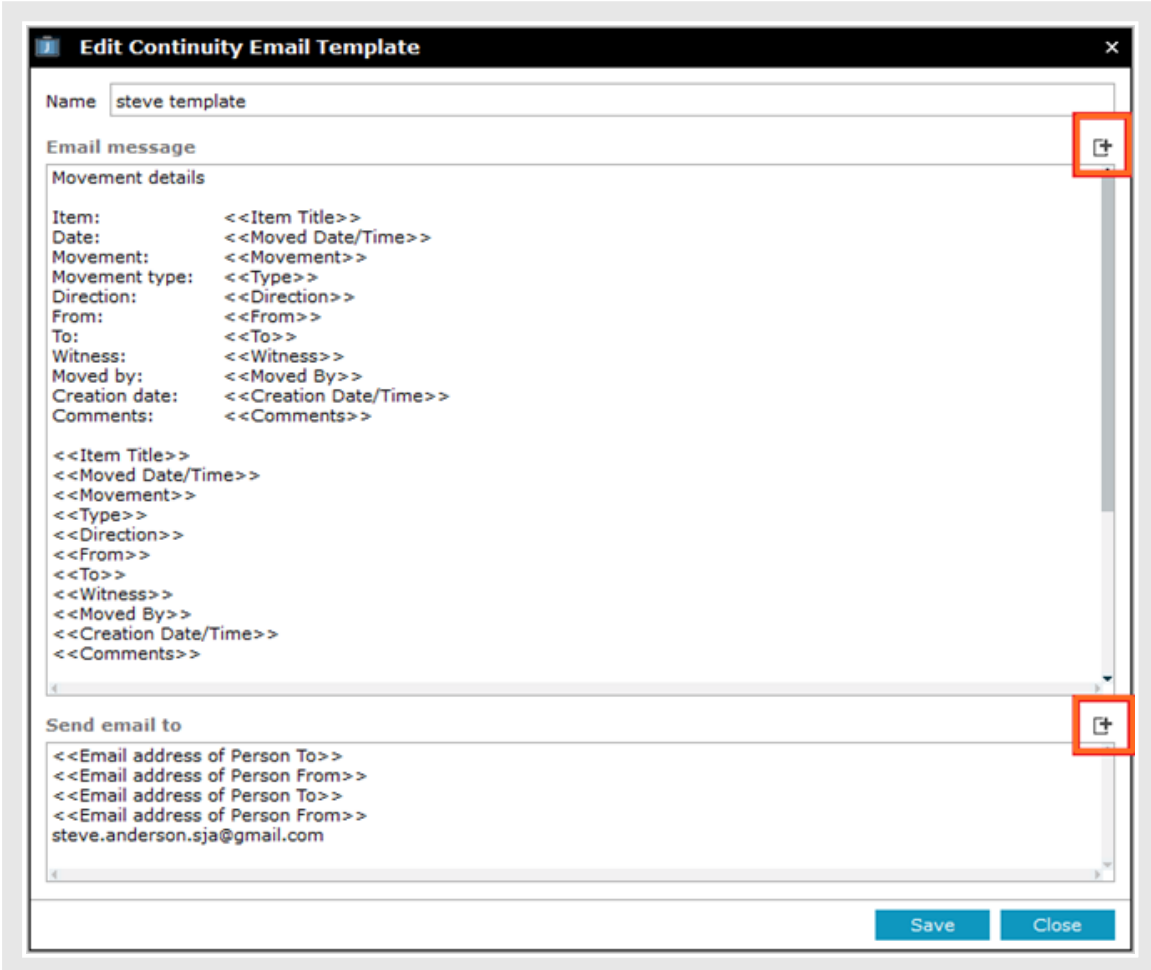
### Now

We've removed this restriction so any user with disclosure capabilities in a case can perform disclosure on tasks and task results in that case.

## It's Easier to Manage Property Continuity Emails

We've made the following changes to managing property continuity emails:

- If there's only one email continuity template available, it will be preselected for you.
- When you edit an email continuity template, you'll see two Add  icons instead of the old **Substitution** button:
  - You can use the first Add  icon to add to the email message.
  - The second Add  icon is for adding email addresses.



**Edit Continuity Email Template**

Name: steve template

Email message

Movement details

Item: <<Item Title>>  
Date: <<Moved Date/Time>>  
Movement: <<Movement>>  
Movement type: <<Type>>  
Direction: <<Direction>>  
From: <<From>>  
To: <<To>>  
Witness: <<Witness>>  
Moved by: <<Moved By>>  
Creation date: <<Creation Date/Time>>  
Comments: <<Comments>>

<<Item Title>>  
<<Moved Date/Time>>  
<<Movement>>  
<<Type>>  
<<Direction>>  
<<From>>  
<<To>>  
<<Witness>>  
<<Moved By>>  
<<Creation Date/Time>>  
<<Comments>>

Send email to

<<Email address of Person To>>  
<<Email address of Person From>>  
<<Email address of Person To>>  
<<Email address of Person From>>  
steve.anderson.sja@gmail.com

Save Close

- If required you can send a continuity email to the address of the **Person From**.

**Maintain Continuity**

**Details**

Movement

Person to person

Movement Type

Temporary

Movement Direction

Transfer

From

DUFFY, Peter (DEMO6)

To

ANDERSON, Steve (SJA) +64 3 367 8412 sanderson@jadeworld.com

Send email

☒ Content To <<Email address of Person To>> <<Email address of Person From>>

Witness

☐ Internal ☒ External

Joe Smith

Moved By

GARDINER, Hamish (HG)

Moved Date/Time

15/12/2020 09:44

**Comments**



## Changes for ICM System Administrators

This section explains the changes in the 6.2.2 version of ICM that apply to the ICM System Administrator in your organisation.

### Specify a Character Limit for Warning Users About an Entity Description

If you're a system administrator for ICM, you can specify the maximum length of an entity description.

If a user enters a description that's longer than what you've specified, they'll be warned that their description might be truncated when they export the data to Excel.

To specify a character limit:

1. Select **Admin > System > Settings**.
2. Make sure the **Options** tab is selected.
3. In the **Warn user when entity description ...** field, enter the maximum number of characters for an entity description.
4. Save your changes.

The screenshot shows the 'System Settings' window with the 'Options' tab selected. The 'Warn user when entity description longer than' field is highlighted with a red box and contains the value '500'. The field is labeled '(Number of characters. 0 = warning never displayed)'. Other settings visible include Country (United States), Database ID (Demonstration), Environment (Demonstration), Application name (ICM), Language (English (New Zealand)), Contact number format (Free Format), Max image or document size (50 MB), Max email attachment size (4 MB), Media attachment directory (D:/jscCcmis/server/c\_misc/MediaAttachments), and various checkboxes for search and display options.

## Increase the Complexity Requirement for Passwords

If you are the ICM system administrator, you can set an option to enforce complex passwords.

These reduce the chance of your system being compromised in a security event.

If you enable the complex password setting, a user's password will need to contain characters from at least three of the following character sets:

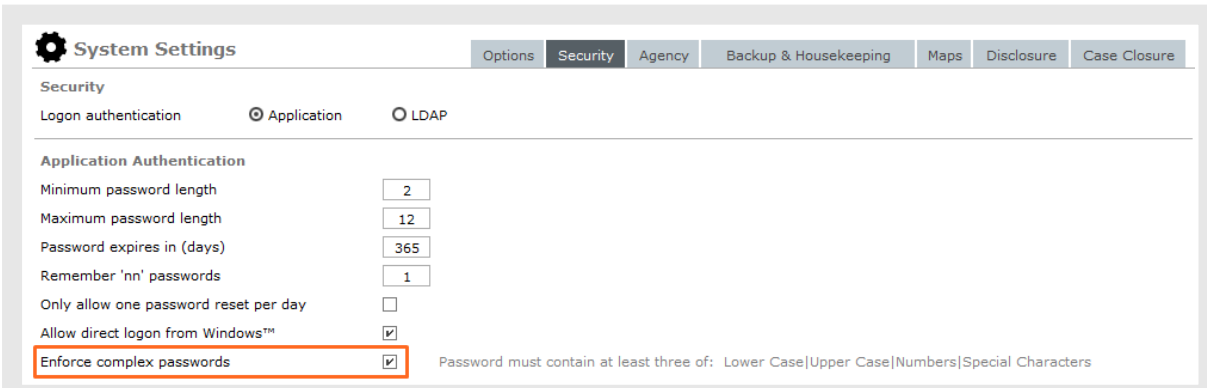
- Lower case characters
- Upper case characters
- Numbers
- Special characters

Once you've enabled the setting for more complex passwords, the next time a user logs in to ICM with an existing password that fails to meet the criteria, they'll be notified of this.

When they select OK on the message that notifies them, they'll have to change their password before they can use ICM.

## ACTIVATE THE COMPLEX PASSWORD REQUIREMENT

1. Select **Admin > System > Settings**.
2. Select the **Security** tab.
3. Select **Enforce complex passwords**.



The screenshot shows the 'System Settings' window with the 'Security' tab selected. Under 'Application Authentication', the 'Enforce complex passwords' checkbox is checked and highlighted with a red box. To the right of this checkbox, a text label reads: 'Password must contain at least three of: Lower Case|Upper Case|Numbers|Special Characters'. Other settings visible include 'Minimum password length' (2), 'Maximum password length' (12), 'Password expires in (days)' (365), 'Remember 'nn' passwords' (1), 'Only allow one password reset per day' (unchecked), and 'Allow direct logon from Windows™' (checked).

## Make an Attribute Only Required for New Entities

Some attribute types are required. If you are the ICM system administrator, you can set these attribute types to only be required when a user creates a new entity.

This enables users to edit existing entities without having to enter data for that attribute.

**Entity Attributes**

Select and enter details below

Select Type: Investigation File

- Investigation File
  - Assigned Team
  - (B) Mandatory Group
    - Attr 1
    - Attr 2
    - File Number**
    - First Response Officer

Category: Attribute Name Move Sequence

Description: File Number

**Options** Conditions Security Add/Change Security Delete Usage (10)

- ☒ COMMENTS - Allow comments for this attribute
- ☒ DEACTIVATED - The attribute type is deactivated
- ☒ DEFAULT - Attribute will be created by default
- ☒ VALUE - A value must be selected for this attribute
- ☒ Type
  - ☒ FREE TEXT - The user can enter free format text for this attribute
  - ☒ URL - The specified value must be a valid URL
  - ☒ CALCULATED - A value will be calculated by the system
  - ☒ CODE TABLE - The specified value will be selected from a code table
  - ☒ DATE - The specified value must be a date
  - ☒ MASK - The specified value will be in masked format
  - ☒ NUMERIC - The specified value must be numeric
  - ☒ TIME - The specified value must be a time
  - ☒ USER - The specified value will be a selected user
  - ☒ TEAM - The specified value will be a selected team
- ☒ Behaviour
  - ☒ HISTORY - Preserve history of changes for this attribute
    - ☒ The history is a point in time only, not a contiguous date/time range
    - ☒ Can change effective date/time of history
    - ☒ Clear comments for new value when existing value is changed
  - ☒ MANDATORY - Selection of this attribute is mandatory
    - ☒ ONLY WHEN NEW - Selection of this attribute is mandatory only when creating new entities

**How do I know whether an attribute is always required, or only required when a new entity is created?**

Look for the number of asterisks \* in the attribute lists:

- One asterisk \* means the attribute is always required
- Two asterisks \*\* mean the attribute is only required when new entities are created

## Issues Resolved in 6.2.2

We've resolved the following issues in this release:

- You can complete the following actions without getting an unhandled exception error:
  - Open a Task List from a system notification
  - Open the disclosure for an entity which has at least one case where it has been fully verified, and then:
    - Select **All** in the case drop-down
    - Select a fully verified entry
    - Use the **Unverified** button

- You can exclude **Completed** tasks from a disclosure.
- The **Case Contents** automatically refreshes when a case note is deleted from the case.  
This is most noticeable when you open the case note from the **Case Contents** to delete it.
- The backup dialog under **System Settings > Backup & Housekeeping** shows when the backup is complete.
- The backup no longer creates excessive logs when a file exception occurs.

This happened sometimes when the system cleaned up old folders or renamed existing ones.

We've also suppressed the backup being retried multiple times when an error occurs.

- If an error occurs during bulk security updates, this won't cause an entire failure. Instead, ICM will collate the errors and let you know it's done this.
- You won't be able to see the **Admin > Security > Business Unit/Region** option unless you're an ICM system administrator.