



Pacific Knowledge Systems

RippleDown User Guide: Administrator v8.1

This document focuses on the options and tasks available to RippleDown administrators and how to utilize these tools.

Copyright Notice

The information provided in this User's Guide is subject to change without notice and is not a commitment by Pacific Knowledge Systems Pty Ltd. The software described in this User's Guide is provided under a license or non-disclosure agreement. It is unlawful to copy this software except as allowed in the agreement.

No part of this User's Guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information retrieval systems, for any purpose other than for the purchaser's personal use, without the written consent of Pacific Knowledge Systems Pty Ltd.

Reproduction or disassembly of embodied programs or databases that make up the software is prohibited.

© Copyright Pacific Knowledge Systems Pty Ltd, 2019

All Rights Reserved.

Intended Use

The PKS Software, when used as a medical device, is intended to be used purely as a decision support system that provides complementary reports for patient data to qualified individuals based upon established rules set up by relevant trained customer domain experts (hereafter referred to as "domain experts").

The PKS Software generates and collates comments into a patient-centric report or workflow action based on rules created and maintained by domain experts. The PKS software presents all first-of-a-kind reports for review, modification (if applicable) and approval by the domain expert prior to release to clinicians or other individuals. Beyond this, the domain expert may automate the release of none, some or all identical reports. However, since a report may be generated and automatically approved for a case for which the domain expert has not previously considered, it is intended that the domain expert regularly review a representative sample of all output types.

It is intended that the clinicians receiving reports against patient results will consider the report in conjunction with all current and previous patient history and apply their own judgement when determining patient management. It is intended that the clinician does not rely on the existence of a report for the management of a patient.

The PKS software in itself does not provide automated diagnosis or treatment-making functions or have the capability to control, in any way, the performance of a device or to treat or diagnose any disease.



It is the responsibility of the licensee to use the product in accordance with its intended use. In support of this, it is recommended domain experts include a statement consistent with the following on all reports.

“This report has been generated using clinical decision support software. This report is intended to provide adjunctive information only and should not replace clinical judgement.

Disclaimer

Pacific Knowledge Systems Pty Ltd makes no warranties, either express or implied, regarding these computer software packages, or their fitness for any particular purpose other than warranty provisions embodied in any agreement or purchase contract.

Acknowledgments

Microsoft and Windows are registered trademarks of Microsoft Corporation.

Manufactured By

Pacific Knowledge Systems: <http://support.pks.com.au/product-register/>

RippleDown is distributed by Abbott Laboratories as AlinIQ CDS

RippleDown is distributed by Philips Healthcare as LABOSYS CDS

Contents

ADMINISTRATOR MODULE	5
Managing Users and User Groups.....	5
Managing Projects.....	8
Server security settings	9
Log files.....	12
Administrator Log Search	12
Licence Update Steps	14
Housekeeping.....	17
Ability to meet the GDPR requirements for “Right to Erasure”	17

Administrator Module

The Administrator is a component of RippleDown used to:

1. Manage users and user groups
2. Manage projects
3. Send and search the logs
4. Edit the server security settings

Managing Users and User Groups

The administrator client is used to manage users and user groups for the RippleDown applications.

A user is defined as the login name for the individual RippleDown user.

A user group is defined as a named set of user permissions pertaining to the various components of RippleDown. This set can allow permissions to all or some applications, projects and queues for all users of that group.

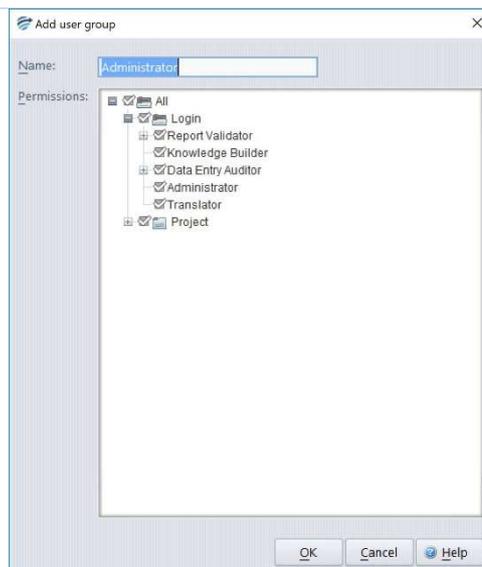
User groups and associated permissions should be set up prior to users being added to group/s.

Create a new user group

1. Use the menu **Users | Manage user groups...**
2. Click the Add button. The Add user group dialog will appear.
3. Enter a descriptive name for the user group.
4. Click the appropriate permissions check box against the required options as follows:

Login Permissions allow a user to login to the corresponding RippleDown application. The following application permissions are possible:

- Report Validator
- Knowledge Builder
- Data Entry Auditor
- Administrator
- Translator



Project Permissions allows a user to access a specific project and its associated validation queues or translations. The following project permissions are possible:

- Knowledge Builder - this allows a user to open the specific project using the Knowledge Builder
- Original queues - this allows a user to validate the default queue for the project, or a queue defined by rules.
- Copy queues - this allows a user to review a copy queue for the project (All copy queues are defined by rules).
- Translations - this allows a user to open a specific translation for the project using the Translator.
- Report sections (only applicable to the Data Entry Auditor) - when a report is viewed in the Auditor, only those report sections for which a user has privileges will be shown.

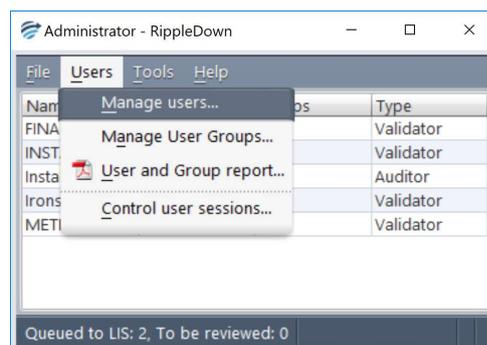
5. You can now add users to this group by modifying their user accounts.

To modify an existing user group

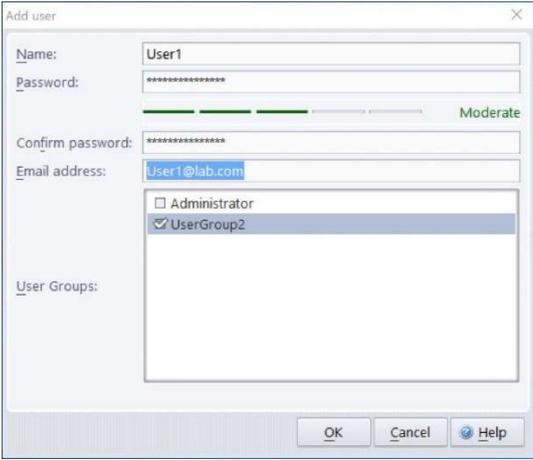
1. Use the menu **Users | Manage user groups...**
2. Select the group that requires modification
3. Click the Modify button.
4. Click the appropriate check box against the required options.

Managing Users

1. From the Users menu select Manage users...



2. The Users box opens and shows the list of users currently active in RippleDown
3. The following options available:

<p>Add</p>	<ol style="list-style-type: none"> 1. Click Add to show the following: <div data-bbox="507 259 1040 719" data-label="Image">  </div> 2. Enter the name and password- ensure required strength is met (this will be evident when the indicator bar turns green) 3. Confirm the password 4. Enter the optional email address. This can be use if cases are to be referred to this user from the Auditor or Validator 5. Select the user group that this user should belong to. If the list of user groups is empty it will be necessary to add user groups and then modify the user you have created 6. Click OK
<p>Modify</p>	<ol style="list-style-type: none"> 1. Click on the user 2. Click on Modify 3. Edit as required and click OK
<p>Remove</p>	<ol style="list-style-type: none"> 1. Click on the user name 2. Click on Remove and you will be asked to confirm the action 3. Click on Yes if this is correct

Generating a User and Group report

To generate a HTML report of the users and user groups that have been defined:

1. Use the Administrator menu **Users | User and Group report...**
2. A dialog will appear prompting the user for the name and location for the report. Enter the file name and folder name required.
3. Click the User and Group report button.
4. After a few seconds, a dialog will appear indicating that the report has been exported.
5. The file may be opened using any web browser and printed if required.

The report comprises of two sections:

Users: The first section of the report lists each user, the groups that user is a member of and the complete list of permissions these groups confer on that user.

Groups: The second section of the report lists each user group, the users in that group, and the permissions associated with that group.

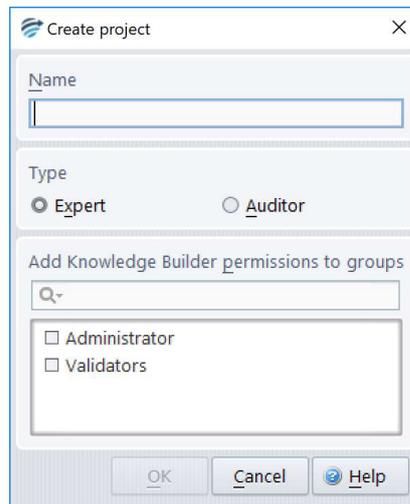
Managing Projects

The administrator client us is used to create and manage projects.

Setting Up a New Project

To setup a new project:

1. Use the menu **File | Create project**

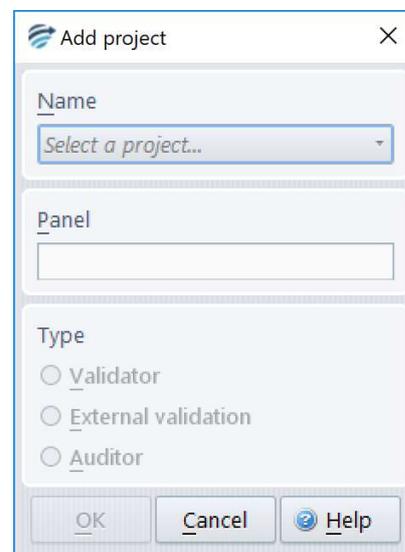


2. Enter the name and type of project.
3. Tick the user group/s required to have permission to the new project.
4. Select OK.

Adding a project Online

To place a project Online (ready to receive cases):

1. Use the menu **File | Add project**



2. Select the name of the project from the drop-down menu. The type of project should be automatically selected.
3. Enter the Panel code - This should be in upper case. The panel code is the code(s) the clinical data source uses to refer to a project. There may be multiple panel codes per project, however a panel code can belong to only 1 project
4. Select OK.

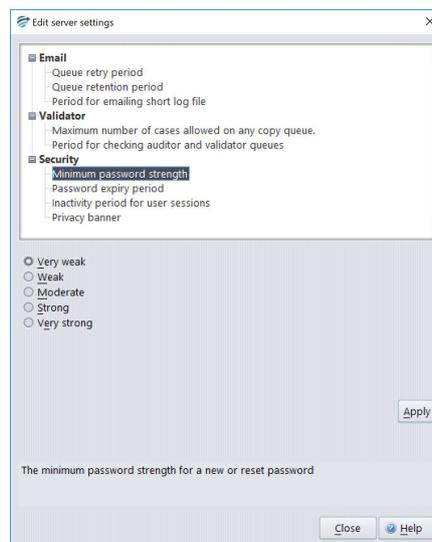
Server security settings

The administrator client is used to set the Inactivity period for users and the Privacy banner to be displayed at log in.

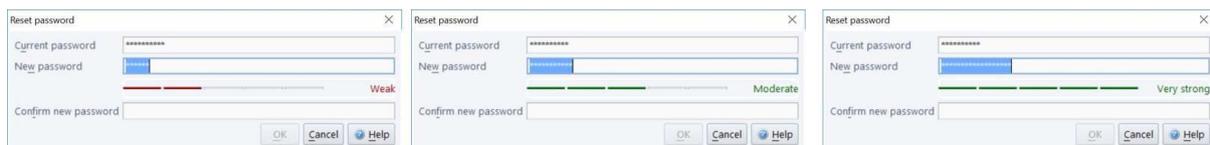
Minimum password strength.

The minimum password strength will be set to moderate by default. The administrator will have the role of adjusting this to one of five levels as necessary to align with the organisational security protocols. Users are able create strong passwords by including letters in both upper and lower case, numbers and/or symbols.

To change this setting, use the menu **Tools | Edit server settings | Security | Minimum password strength**.



During password setting or resetting, a strength indicator will alert the user of the strength of their password (see fig 3).



Upon confirmation of the new password the OK button becomes enabled only if the strength and match criteria are met.

Please note: Passwords cannot be reused within the installation.

Password expiry period.

The default password expiry period for users is set to 90 days. When the user attempts to log in after not having reset their password within this period, they will be prompted to change their password. There is the option, if required to disable this feature by selecting the Passwords do not expire button.

To change this setting, use the menu **Tools | Edit server settings | Security | Password expiry period.**

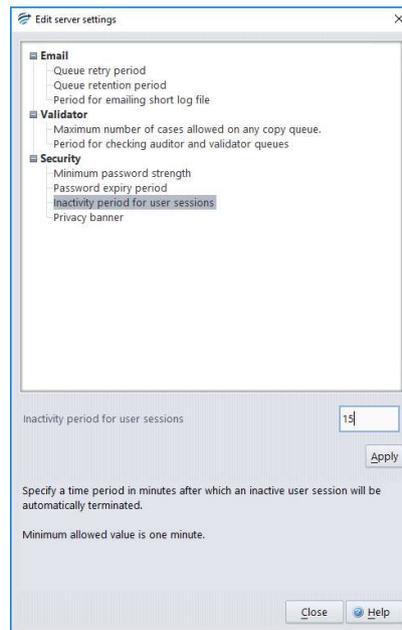
It is useful to also note, that users are able to reset their password at any time via the menu **Help | Reset password** available in all RippleDown modules



Inactivity period.

The default inactivity period for users is set to 15 minutes. The application will log the user out of the current module and display the module selector. The user will need to reapply their username and password to regain access to the application.

To change this setting, use the menu **Tools | Edit server settings | Security | Inactivity period for user sessions.**



Enter the required number of minutes in the text field and click apply- the maximum value is 1500 minutes.

Privacy banner.

The application has a default privacy banner which is displayed to the user and must be agreed to before a user can log into a RippleDown module.

To change this setting, use the menu **Tools | Edit server settings | Security | Privacy banner.**



To change the privacy statement, enter the required text into the Privacy banner field and click apply.

The privacy statement can be deactivated by removing all text from the privacy banner field and clicking apply.

Log files

The administrator client is used to search and email the log files for diagnostic purposes.

Emailing the log files.

Use the menu **Tools | Email log file**. The log will be emailed to the email address as defined in the Rippledwn/properties/AESender.properties file.

Administrator Log Search

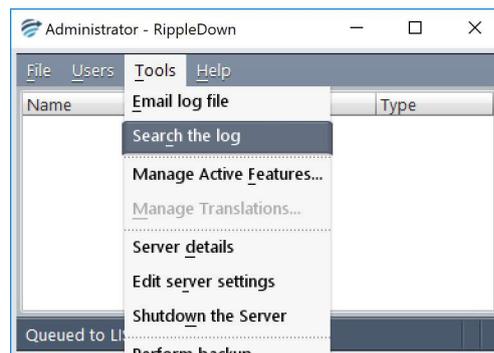
If a user reports an issue, there are a few ways you can investigate the issue to gather the required information:

1. Search the Administrator log to find the history of the case within RippleDown.
2. Search for the case in RippleDown
3. Search for the message sent to RippleDown
4. Search for the message sent back from RippleDown

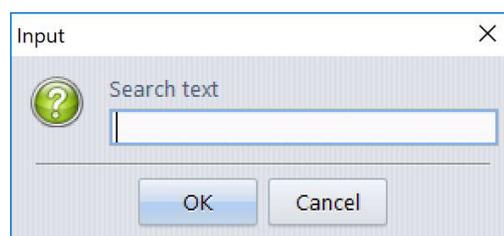
Searching the Administrator Log

To find the history of a case in RippleDown, as an administrator, you can search the Administrator logs. This will show all log entries containing the search text. To perform this search:

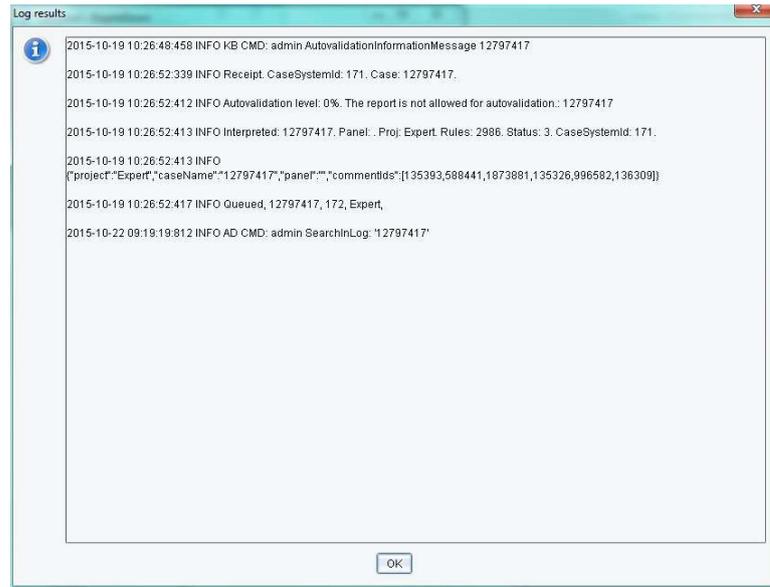
1. Log in to the Administrator module using your username and password.
2. From the Tools menu, select "Search the log"



3. Enter the string/text you want to search for



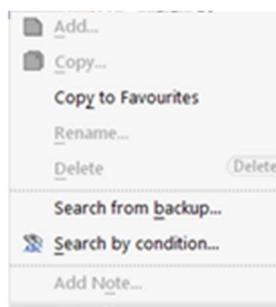
4. After the search is complete, the log entries for the case will be displayed.



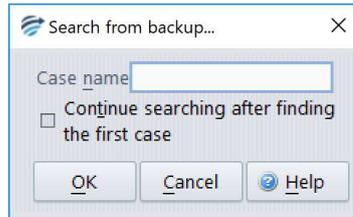
Search for a case in RippleDown

To find the case within RippleDown, you can search within the Knowledge Builder in two ways depending on how recent the case is.

1. Log into the Knowledge Builder using your username and password.
2. From the File menu, open the relevant project.
 - a) If the case is within the archive retention period then simply click on the archive case list and type the case number in which will bring the case in to view.
 - b) If the case is outside the archive retention period then right click anywhere within the Archive case list window and select "Search from backup..."



3. Enter the case name you want to search for. As there may be more than one version of the case that has been sent to RippleDown, tick the box if you would like all versions.



4. The application will then search all archived files. A progress bar will be shown in the bottom left hand side of the screen.
5. Once the case has been found, the case will appear at the bottom of the Search case list.

Search for the messages sent to and from RippleDown

To find the messages sent to and from RippleDown:

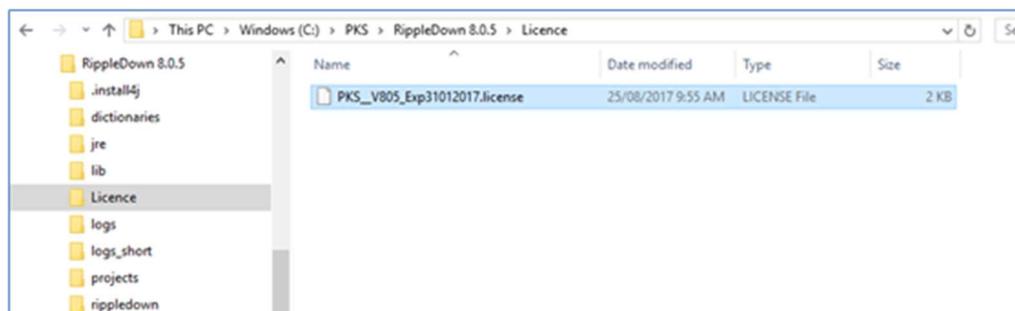
- Go to the Installation folder/projects/backup/archive
- The in messages will end in panel name.in
- The out messages will end in panel name.out

The current days messages will be within this location. Any previous messages will be held in the “zips” folder in this location.

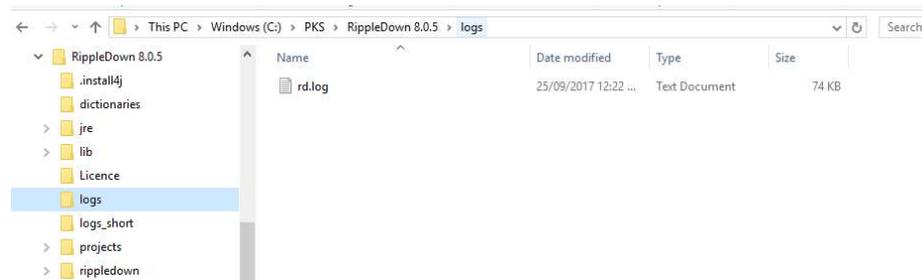
Name	Type	Date modified	Size
000000023.INSTALLTEST.in	IN File	19/09/2017 2:44 PM	4 KB
000000023.INSTALLTEST.out	OUT File	19/09/2017 2:44 PM	1 KB
000000024.INSTALLTEST.in	IN File	19/09/2017 2:46 PM	5 KB
000000024.INSTALLTEST.out	OUT File	19/09/2017 2:46 PM	1 KB
000000025.INSTALLTEST.in	IN File	19/09/2017 2:49 PM	5 KB
000000025.INSTALLTEST.out	OUT File	19/09/2017 2:49 PM	1 KB
000000026.INSTALLTEST.in	IN File	19/09/2017 3:01 PM	6 KB
000000026.INSTALLTEST.out	OUT File	19/09/2017 3:01 PM	1 KB
000000027.INSTALLTEST.in	IN File	19/09/2017 3:12 PM	1 KB
000000027.INSTALLTEST.out	OUT File	19/09/2017 3:12 PM	1 KB
000000028.INSTALLTEST.in	IN File	19/09/2017 3:16 PM	2 KB
000000028.INSTALLTEST.out	OUT File	19/09/2017 3:16 PM	1 KB

Licence Update Steps

1. Identify the licence folder. The name of this folder is 'licence', and it is located under the RippleDown installation root folder:



2. Open the folder
3. Stop the RippleDown service
4. Move the existing license into a temporary folder, in case the new license is not configured correctly (e.g. wrong MAC address)
5. Make sure the <RippleDown installation root folder >\licence directory is empty
6. Copy the new license file to this folder
7. Restart the RippleDown Service
8. Open the RippleDown log file named log.txt.0 (under <RippleDown installation root folder >\logs directory)



9. Check that the license check passed, by looking for a current datetime entry similar to the below:

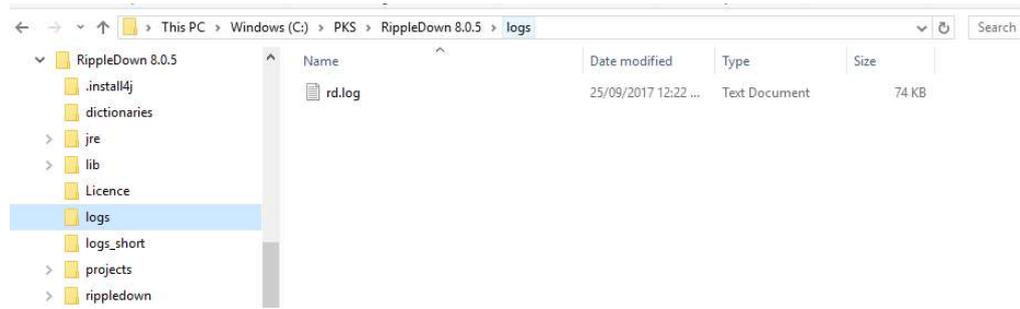
```
2018-11-07 08:43:57:217 INFO About to check the licence.
```

```
2018-11-07 08:43:57:271 INFO Licence status: Licence OK. Expiry Date:
31 Jan 2020 Grace Period End Date: 28 Feb 2020
```

Rollback of licence

If the licence does not register successfully as per step 9 above, the following steps should be taken:

1. Stop the RippleDown service
2. Delete the new licence from the \ <RippleDown installation root folder >\licence directory so that this directory is again empty
3. Restore the original licence from 4 above back to \ <RippleDown installation root folder >\licence directory.
4. Restart the RippleDown Service
5. Open the RippleDown log file named log.txt.0 (under \ <RippleDown installation root folder >\logs directory)



6. Check that the original license check passed, by looking for a current datetime entry similar to the below:

```
2018-11-07 08:43:57:217 INFO About to check the licence.
```

```
2018-11-07 08:43:57:271 INFO Licence status: Licence OK. Expiry Date:
31 Jan 2020 Grace Period End Date: 28 Feb 2020
```

7. Contact PKS support on support@pks.com.au for re-issue of replacement licence if required.

Housekeeping

Housekeeping of the system is performed automatically once per day and typically takes roughly 15 minutes to complete. The default time for housekeeping to begin is 2am local time, however this can be modified if needed. When housekeeping begins, all users will be logged off automatically and will not be able to log back on until housekeeping is complete.

Housekeeping tasks:

- The archive case lists will be purged of the oldest cases and the number of days selected per project to keep archived cases will be retained.
- New reports that have been approved will be removed from the New reports case list.
- Rejected case list will be purged of the oldest cases and the number of days selected per project to keep rejected cases will be retained.
- Backups of all projects including the RippleDownServer and InterpStore projects will be created and replace the oldest backups.
- The log file will be sent for evaluation to a specified monitoring address.
- The licence file will be validated
- All statistics will be updated

Note: If a user attempts to log into the application while housekeeping is being performed, when the OK button is selected, the application will not open and the application selector will remain on the screen.

Ability to meet the GDPR requirements for “Right to Erasure”.

See Article 17, General Data Protection Regulation (GDPR) Right to erasure (‘right to be forgotten’)

When the right to erasure is successfully invoked, to remove a record from within the software the user should complete Parts 1- 4 below.

Part 1: The Knowledge Builder

Note: the following must be performed for each knowledge base by a user with appropriate privileges.

1. Log into the Knowledge Builder and search each case list for the individual.
2. Record any case name/s, associated queues and date received, as this/these will be required in Part 2 and 4 below.
3. Delete the case from the following lists, by right clicking on the case and selecting Delete from the menu:
 - Rejected
 - New Reports
 - Favourites
 - Search
4. The Archive case list is regularly purged by the system using a “Days to Keep” configuration option.

If the case is in the Archive case list and requires deletion more urgently than that defined in the “Days to Keep”, adjust to have the case removed at the next housekeeping (housekeeping can be invoked via the Administrator module if desired).

This menu option can be found here:

- Options -> Settings -> Days to keep archived cases

Note – this setting will need to be readjusted after housekeeping to resume the normal case storage length retained by the Archive case list.

5. The interface case list is rarely used and is most likely not set up in your configuration. If used and the case is in the Interface case list, review the seconds to keep interface cases and adjust if appropriate to have the case removed at the next housekeeping (housekeeping can be invoked via the Administrator module if desired). This menu option can be found here:

- Options -> Settings -> Seconds to keep interface cases

Note - This setting will need to be readjusted after housekeeping to resume the normal case storage length retained by the Interface case list.

6. If the case is in the Cornerstones case list, contact support@pks.com.au for assistance.

Part 2: The Validator and Auditor modules

1. Log in to the Validator and/or Auditor and open any Queues identified in Part 1 above and find the case. This menu option can be found here:

- File -> Find Case

2. In Auditor, process this case as usual. This removes the case from the Auditor queue.

3. In Validator, process the report as usual. If changes are made to the interpretation, ensure to deselect the check box “Also send to the Knowledge Builder”. This removes the case from the Validator queue and prevents the case going to the Rejected case list.

Part 3: Administrator module

1. Log in to the Administrator module, and using the case name identified in Part 1, search the Logs for all remaining entries referring to the case. Record the date and timestamp associated with this log entry. This menu option can be found here:

- Administrator -> Tools -> Search the log

2. Where a log entry is identified, the administrator will open the associated log, identified based on the date and timestamp, and will manually delete this entry

The log files are found in the <installation directory>\logs\

Part 4: Clean-up of .IN and .OUT files

RippleDown maintains a copy of the message file received (the .IN file) and sent (the .OUT file) in the case archive directory. These are zipped daily during housekeeping, and by default only the last 30 days are maintained.

There is an optional setting in server.properties with key CLEANUP_CASE_ARCHIVE. If this is not in the file, 30 days are maintained. If the case is in the Archive directory and requires deletion more urgently than that defined in that defined in CLEANUP_CASE_ARCHIVE then the following should be done.

1. Log on to the RippleDown server and locate any Archive/s identified by the processing date/s recorded in Part 1 above. The archive will be found here:

- <RippleDown Installation directory>\Projects\backup\archive\

2. The administrator will open the archive/s and search for the case based on the case name. Any instances, i.e. .IN and .OUT should be manually deleted, and the archive closed.