Pacific Knowledge Systems

RippleDown 8.1 New Features Guide

This document outlines new features of RippleDown version 8.1

Copyright Notice

The information provided in this User Guide is subject to change without notice and is not a commitment by Pacific Knowledge Systems Pty Ltd. The software described in this User 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 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

Password requirement improvements

The following improvements have been implemented regarding password administration.

Expiry Period

Administrators may now set a password expiry period through the Administrator module under Security (see fig 1). This option can be set from 1 to 999 days or disabled so that passwords do not expire, dependent on the client organizational preferences. The default setting is 90 days.

To change this setting, use the menu **Tools | Edit server settings | Security | Password expiry period.**
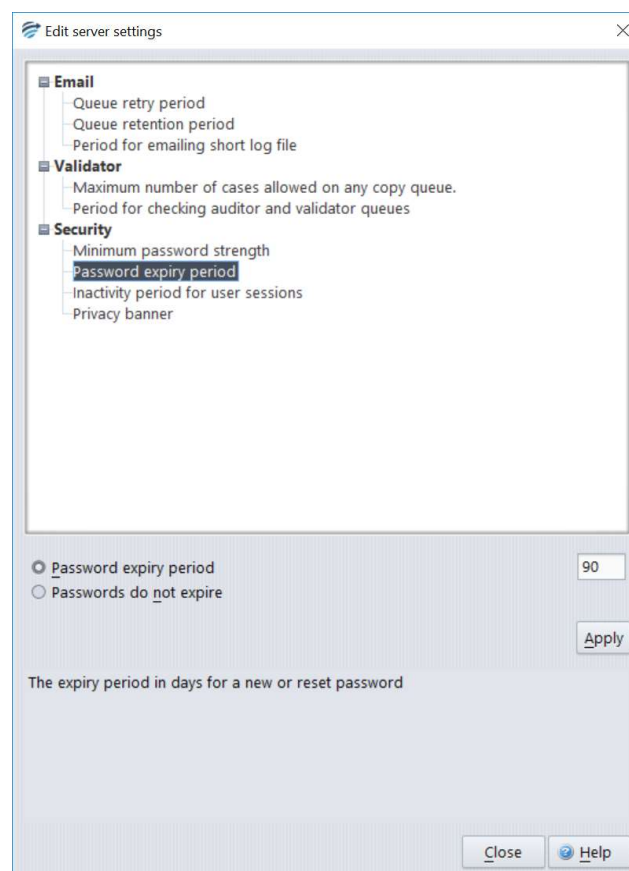
Figure 1: Password expiry period

Once set, the password expiry period will apply to all RippleDown modules (Validator, Knowledge Builder, Data Entry Auditor, Administrator, Translator) and users.

Once the period is set, a user will be alerted of the expiration of their password upon first log in post expiration. This expiration event is logged by the server.

Password Strength

Administrators may now set a variable password strength level for users. The default of the installation is set to 'moderate' and this option can be adjusted as necessary in order to align with client's organisational security protocols.

Presented under security settings (see fig 2) by accessing **Tools | Edit server settings | Security | Minimum password strength,** the option may be selected for one of 5 levels.
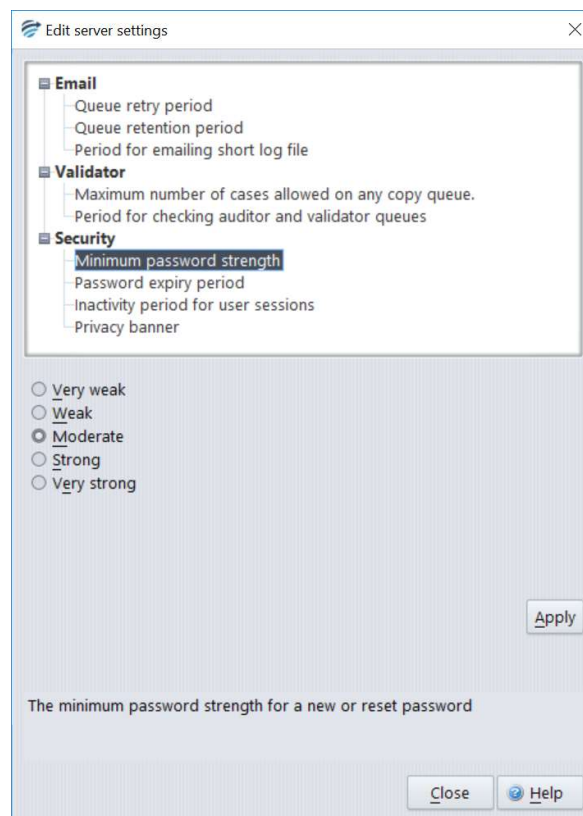

Figure 2: Minimum password strength for the installation.

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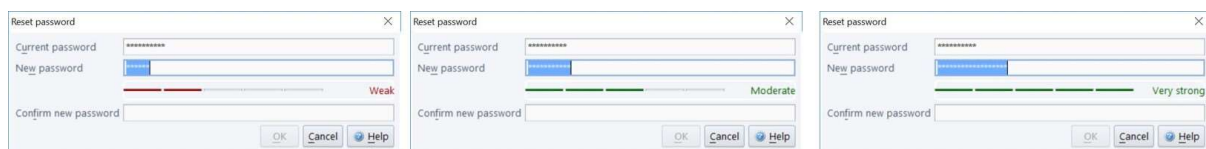

Figure 3: Password strength indicator

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.

Default setting for the retention of archive cases

The default setting for days to keep cases in the archive case list has been changed from -1 (indefinite) to 90 days. This has been changed to avoid unnecessary accumulation of old cases. The major use of the cases in the archive case list is to ensure example cases can be found for rule building sessions. It is recommended that this setting is changed to a value that would represent a case throughput of approximately 100,000 cases within each knowledge base. For example, if 5,000 cases are expected to be processed through knowledge base X each day, this setting should be changed to 20.

To change this setting, open the relevant knowledge base in the Knowledge Builder module. Use the menu **Options | Settings… | Days to keep archived cases** (see fig 4).

Figure 4: Days to keep archived cases.

Increase in log files retained

Previously, 20 of the most recent log files were kept for an installation. This has now been increased to include the most recent 100 log files. Each log file will roll at 10MB or at housekeeping. The log files can be used for traceability and troubleshooting purposes.

To search the logs, please access from **Tools | Search the log** menu in the Administrator module.

Audit Trail Optimisation

Previously, there was a secondary database used to store the Audit Trail for each knowledge base. This data has now been consolidated into the knowledge base database. System administrators will notice mv.db files are no longer retained.