# RLDatix™

# - Global Settings Descriptions -

FOR RiskMan Version 2501

Last reviewed February 2025

# CONTENTS

Global Settings Descriptions

# INTRODUCTION

This document aims to provide an explanation for each Global Setting in RiskMan.

The Global Settings for all Registers are available under the menu option: *Administration > Configuration > Global Settings.*

As the Global Settings can be modified by each organisation and additional global settings can be added for each Register used in RiskMan, this document presents the Global Settings in their default, unmodified state, and as such, there is a possibility that some screenshots used might not exactly match your system.

**Global Setting Helper Text**

All Global Settings have "helper text", which displays when you attempt to modify each individual setting.

To view helper text:
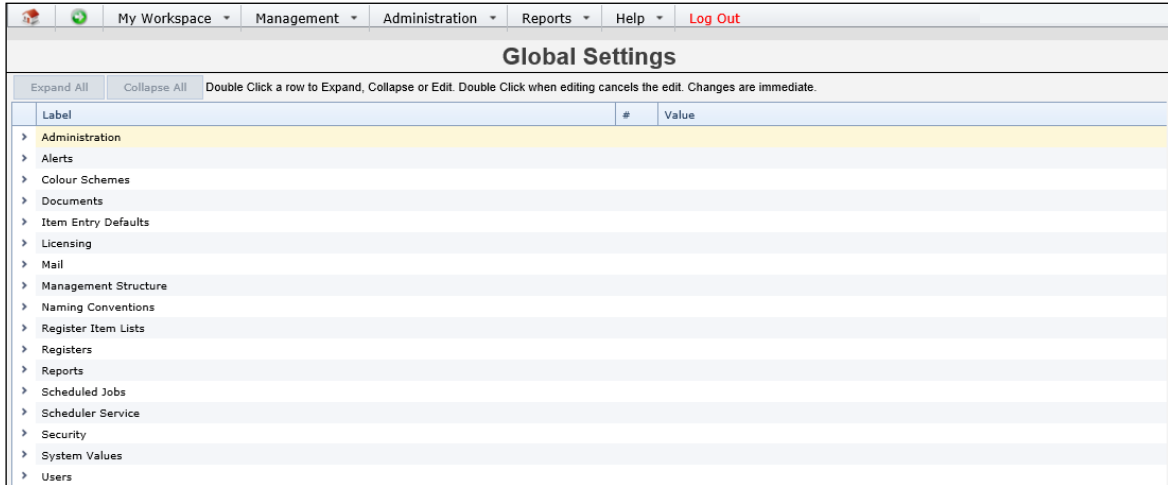
- Double click the name of the setting you wish to modify, or, click the **Edit** text
- The helper text appears, along with the type of setting you can modify (eg On/Off; Yes/No; arbitrary value, etc)
- If you make any changes to a setting, remember to click the Update button
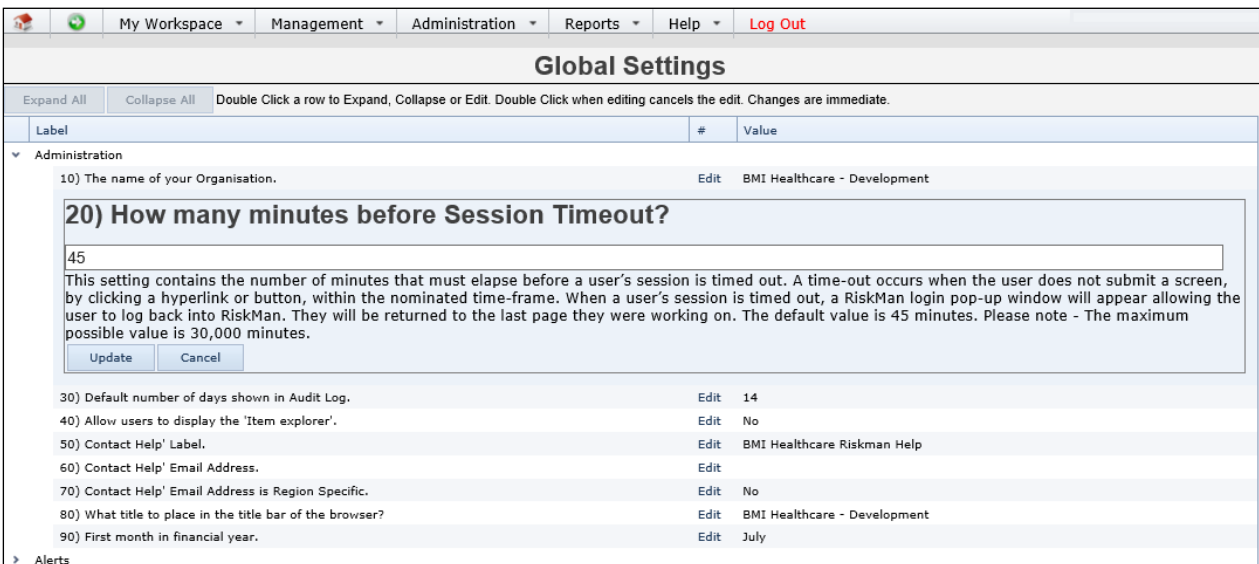


*Example of the helper text that appears when a user double-clicks the name of a Global Setting*

# THE GLOBAL SETTINGS TREE
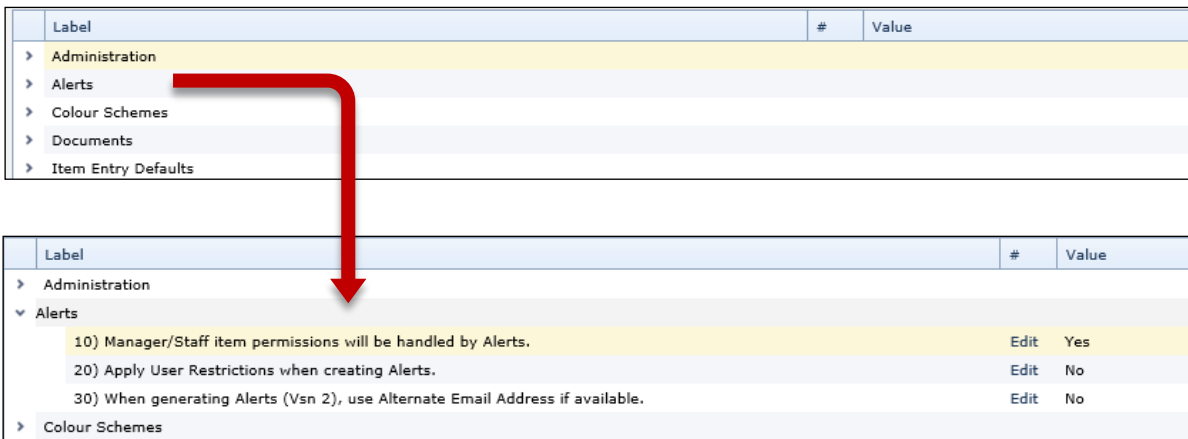
Global Settings are displayed in a "Tree" format, and are grouped by the type of function they modify:



*Example of the Global Settings tree*
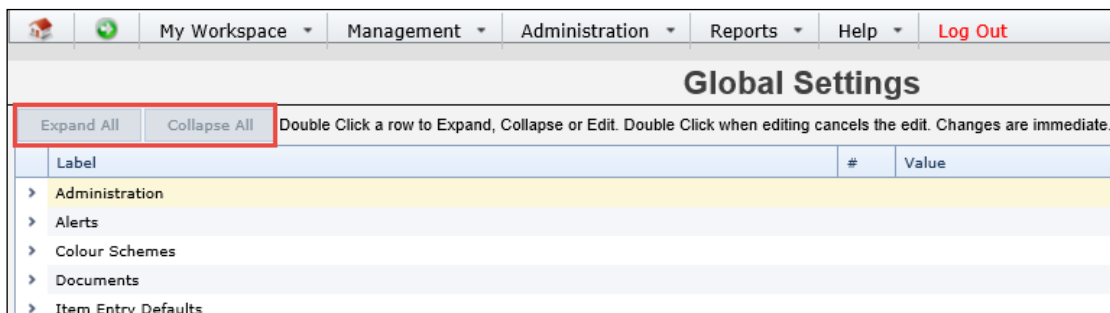
To display the available settings, double click on the name of the group, or on the **>** symbol:



Alternatively, you can use the **Expand All** and **Collapse All** buttons to display/hide all settings at once:

# CREATING REGISTER-SPECIFIC VERSIONS OF GLOBAL SETTINGS

As the name implies, **global** settings are enforced system-wide. However, in some circumstances, you might only want a setting to apply to one register and not another.

If this is required, most global settings have a button which will allow you to create a **Register Specific Version**.

For example, let's say that you want to enable the **Group Records** function in your Incident register, but NOT any of the other registers in your system.



In order to achieve this, you would set the standard Global Setting, as shown above, to **No**.

You can then open the global setting by double clicking it, or clicking the Edit link. The setting looks like this:

Global Settings Descriptions

We are going to add an exception to this global setting that will allow the Group Record function in only the incident register. Click the **Make Register Specific Version** button; you will be presented with the following dialog (over page):



❶ Select the register this setting should be applied to.

❷ This is the default **helper text** that you see when you go to modify a setting. You may wish to modify it to inform any other users that this is a register-specific setting.

❸ Click the tick icon ✔ when you are satisfied with your changes to **save** them.

❹ Click the cross icon ✖ to **cancel** the changes.

The setting you created will then appear under the **Registers** group, with the same structure as the original. You can then go and modify the setting specific to that register as required:

# ADMINISTRATION

**10) The name of your Organisation.**

This setting contains the name of your organisation (e.g. *Acme Health Care*), and is shown in the heading section of all system reports.

**20) SAML signout upon RiskMan session timeout.**

Adding the ability for SAML environments to obey the RiskMan timeout setting via the new global setting:

Users | Authentication | SAML Details | 20) SAML signout upon RiskMan session timeout.



When using SAML, a SAML session is created to record the current state. Normally, this session is created in memory on the web server. This is an issue if the site uses a web farm (multiple webservers), as the session is only recorded on one web server. If logging out happens to occur on the other server, the logout will fail.  To resolve this, set this setting to YES and the session will be recorded in the database. The SAML session is then shared across all servers and preserved correctly

**30) Default number of days shown in Audit Log.**

Audits of activity in RiskMan are logged and stored into RiskMan's database. The available functions that may be audited are found by selecting the cog on the right-hand side of the screen in the Audit Log function. Selection is made by choosing from the Action: and User: drop down lists.

This Global Setting allows you to determine, by number of days, how long audit logs are kept in the database if the functions as specified above are enabled.

**40) Allow users to display the 'Item Explorer'.**

*(Only relevant to users who use the RiskCat classification selector style for classifying records)*

If this option is checked it means any user with access to view Posted records will have access to the respective Explorer page (eg. Incident Explorer). Accessed from the *Management -> Enquiry -> [Item] Explorer* menu option. This page displays all posted records grouped by the RiskCat classifications that have been selected within the record.

*See following example of the Item Explorer*
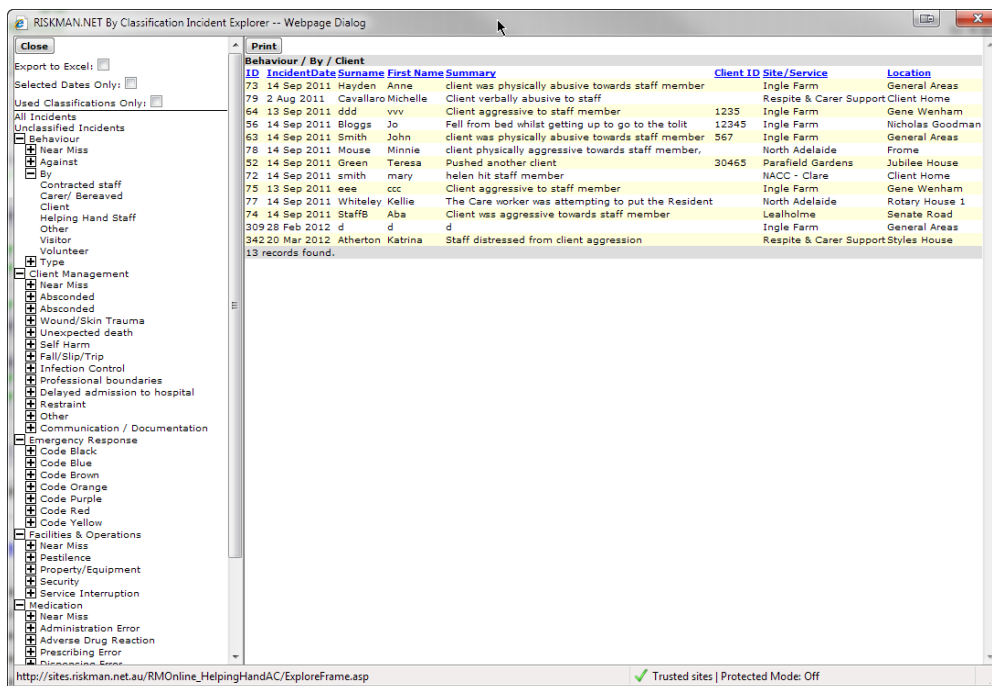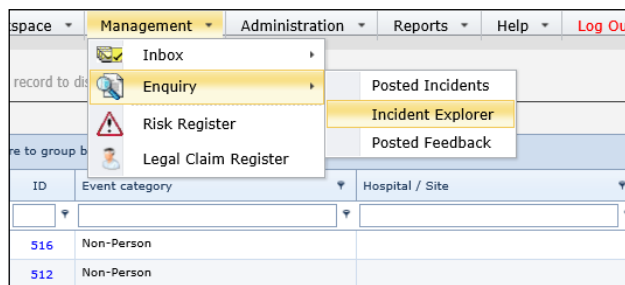
Global Settings Descriptions
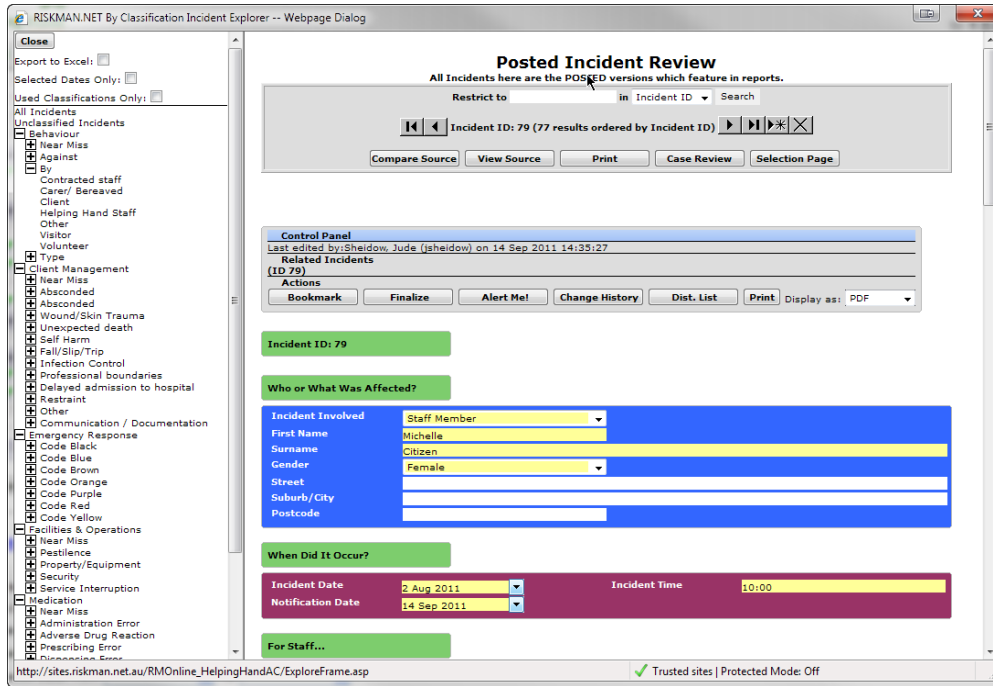


## 50) Contact Help Label

If text appears in this setting, then a new menu item (with the content of this setting) will appear under the **Help** menu. By selecting this menu option, an email window will open and if there is an email address in the *60) Contact Help Email Address* setting, this will be populated to the *Send To* field on the generated new email
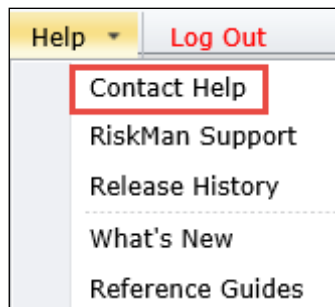


### Suggestion

*This is useful if you wish to enter an internal RiskMan Help desk email address for your users to contact if they are having issues/questions in relation to RiskMan*

## 60) Contact Help Email Address

Enter the email address where you wish RiskMan questions/issues to be sent to, if a user selects the Help menu option outlined in the previous setting.

**70) Contact Help Email Address is Site Specific**

When enabled, this setting allows you to specify a different support email address for each Site in your organisation. Useful for alliances or large organisations. To define the help email address for each Site, please modify the *Site Help Address* List in List & Codes Maintenance.
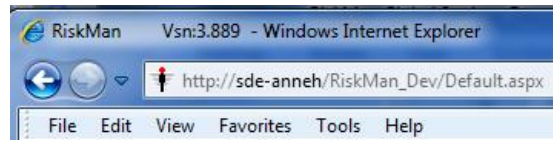
**Note**

*If you are unsure whether you need this functionality, please contact RiskMan* [https://hub.rldatix.com/SupportHUB/s/](https://hub.rldatix.com/SupportHUB/s/) *Please note you may need to request an account to access this service. If an account is needed, then please go to* [HUB: Sign In (rldatix.com)](HUB: Sign In (rldatix.com)) *and click on Request an account at the foot of the login box.*

**80) What title to place in the title bar of the browser?**

Specify the title that you want to display in your title bar of the browser. This might be "RiskMan Production System" or "<Organisation Name> RiskMan Training Site".

If left blank, the default title will default to the Version Number of RiskMan, as shown above.

**90) First month in financial year**

This setting defines which month is the first month in a financial year for your organisation. It may be used anywhere in the system where a financial year is required.

**100) Use custom user selector?**

You're now able to customise the user selection list to display different user details. Previously, the only detail displayed would be the user display name and username. The decision on what details are displayed is up to you. Details from the user profile can be displayed such as: Position, User Type, Email address, Phone number and / or Manager.

**110) How many hour(s) before Mobile Devices expire??**

This setting defines the number of hours that must elapse before a mobile device is expired. The default value is 24 hours. Please note - the maximum limit for expiry hours is 10000000.

**120) High Charts Export Server URL**

This setting relates to exporting charts generated by the InfoCentre or Home Page widgets. These are produced using a system known as 'High Charts'. The default value is 'HighchartsExport.axd' which will allow export of the charts. Setting the value to empty will disable exporting of the charts. The default uses an older export server but is available by default. A higher quality export is available but using this will require installation of additional software. There is also an ability to use a public server on the Internet, but this is not recommended for security reasons.

**160) Allow the GoTo page used by Alerts etc. to navigate to Posted Inquiry pages**

The GoTo page functionality was intended to take the user to the highest-level page they have permission to when used and is linked to from URLs in Alerts and some other places. From the page navigated to, the user can navigate down to other views, such as the Inbox review page, with one click if required. Due to the way this was implemented, the user was in effect never taken to a posted record inquiry page, even when available. Setting this option to 'Yes' will allow this to happen, 'No' will preserve the previous limitation.

**170) After submitting of a posted item, return to the Posted Enquiry page**

After submitting an edit of a posted item, do you want the system to return you to the Posted Enquiry page. When no, the entry form will be reloaded, which is the historical approach.

**180) Show custom banner logo**

When yes, the files from the Images\Banner folder on the web server will be displayed in the banner, and these can be customised/modified however the file name, size and type must NOT be changed

# ALERTS

**10) Manager/Staff item permissions will be handled by Alerts.**

There are many ways to send notifications to managers when a new record is in entered into RiskMan by staff that report to them, including but not limited to:

- Via the standard Line Manager Notifications (when *Global Setting > Mail > 20) Send EMail notification to the Line Managers when an Item is created* is checked), or
- By Using Alerts

If this Global setting is enabled, and the *Global Setting > Mail > 20) Send EMail notification to the Line Managers when an Item is created when an Item is created* is disabled, then Line Managers will only be notified of records entered by their subordinates via an Alert (which will need to be setup – usually called Reporter's Manager).

By notifying Line Managers of new records by an Alert only, the Line Manager will only have permission to see the records which triggered the Reporter's Manager alert, and will not be able to see *all* the records a staff member has ever entered in RiskMan when that staff member selects them as a Line Manager.

When setting up an Alert for Line Managers:

- You will need to set up an Alert for each Register, and in the **Recipients** section:
    - If using Alerts Version 1, The Alert To field should contain "Reporter's Managers" which is selected from the Alert To Category list
    - If using Alerts Version 2, choose *The nominated line manager(s) of the user who originally reported the record* from the *Add a user who appears in the Review History for each record that triggers this alert* drop down list
- Create a customised email message for the Line Manager eg. Who entered the record, where it occurred, summary, etc
- Ensure the conditions of the alert are such that the alert will trigger as soon as the record is entered into RiskMan eg. Summary is not null / is not empty

If this Global setting is **disabled**, and the *Global Setting → Mail → 20) Send EMail notification to the Line Managers when an Item is created* is **enabled**, then the Line Manager will be notified of any records that the staff member that reports to them enters into RiskMan. If that staff member changes their line manager, the new manager will have access to all records the staff member ever entered into RiskMan, regardless of whether they are relevant or not. The previous manager may

not get permission to view records that this staff member has entered if they had not viewed them before the staff member changed their line manager

## Recommendation

*Enable Alerts > 10) Manager/Staff item permissions will be handled by Alerts, and disable Mail > 20) Send EMail notification to the Line Managers when an Item is created and set up an alert for the Reporter's Manager.*

**20) Apply User Restrictions when creating Alerts.**

When enabled, a user's site/location restrictions will be included if that user creates an alert. This can be useful if you have users who are allowed to create alerts at different sites, by eliminating the chance of a user creating an alert that triggers for a record from a site that is not their own.

Refer to the *Alert Management Guide* for more information.

**30) When generating Alerts (V2), use Alternate Email Address if available.**

Alerts to RiskMan users normally get the email address for those users from the "Email Address" field in their User Profile. Enabling this setting (Yes) will cause the email address to be taken from the "Alternate Email Address" field, if available. The regular Email Address will be used if the "Alternate Email Address" field is empty in a user's profile.

**40) When finding recipients for Alerts Vsn2, don't include Deleted or Expired users.**

If this global setting is set to **yes** RiskMan will not sent alerts to deleted or expired users. When **No**, RiskMan will still alert users marked as deleted or expired. This can be appropriate in some situations. For example, if there are a large number of agency staff who are temporarily expired when not required.

**50) Maximum records when processing Periodic Alerts (Vsn 2)**

When processing Periodic Alerts, it is possible to configure an alert so that they return large numbers of records. This can be a problem, depending upon another alert configuration. For example, with no or broad filters, it is simple to return all records for a register. This could return tens or hundreds of thousands of records. Assigning or revoking permissions, for example, would take many hours and cause processing issues on normal pages. 'When Saved' alerts will handle this by processing in batchs of 500, then allowing alerts to continue, then processing a further 500 in the next run, etc. It will eventually complete after some time. Periodic alerts cannot use this technique. Having a periodic alert return more than this number of records will cause an error.

The alert will then be disabled until the conditions are corrected. 0 means no limit.

## 60) Maximum time to allow an individual Alert (Vsn 2) to process

If an alert processes for more than the specified number of minutes, an error will be generated, and the alert terminated (rolled back). The alert will be disabled until corrected. Alerts will 'notice' if this changes while the alert is processing, providing a way to terminate a long running alert. 0 means disabled.

## 70) Maximum time to allow Alerts (Vsn 2) to batch process before surrendering control

After Alert Vsn2 processing starts, it will process Alert after Alert until it either, encounters an alert it has already processed in this batch, or a time limit is reached. This setting indicates the number of minutes before reaching that time limit. After control is surrendered, emails can be sent and other processes completed, and then Alerts will begin processing again from where they left off.

## 80) How many 'Error' log records to keep per Alert V2

Alerts Vsn2 will log errors for an individual Alert to the Alert Log. The log is limited in how many records it keeps for each log type for each Alert, so that the total number of records is not unreasonable. Records more than the specified amount will be deleted, oldest first. Minimum value is 10.

## 90) How many 'Records Found' log records to keep per Alert V2

Alerts Vsn2 will log details to the Alert Log when it 'finds records' to process for an individual Alert. The log is limited in how many records it keeps for each log type for each Alert, so that the total number of records is not unreasonable. Records more than the specified amount will be deleted, oldest first. Minimum value is 10.

## 100) How many 'Process Complete' log records to keep per Alert V2

Alerts Vsn2 will log details to the Alert Log when it completes a processing run without finding matching records for an individual Alert. The log is limited in how many records it keeps for each log type for each Alert, so that the total number of records is not unreasonable. Records more than the specified amount will be deleted, oldest first. Minimum value is 10.

## 110) How many 'Digest Complete' log records to keep per Alert V2

Alerts Vsn2 will log details to the Alert Log when it completes processing a Digest part of an Alert. The log is limited in how many records it keeps for each log type for each Alert, so that the total number of records is not unreasonable. Records in excess of the specified amount will be deleted, oldest first. Minimum value is 10. Not all Alerts generate a Digest.

**120) The maximum number of retrieved rows allowed in a Periodic Digest Alert**

When running a Periodic Alert, it is possible to return a huge number of rows. When the Alert utilizes a Digest email, each row requires separate processing and cumulatively this could take a very long time. This could adversely affect normal RiskMan operations. To prevent this situation, this setting places a limit on the number of rows allowed for a Periodic Digest Alert. An error will be generated if the retrieved number of rows exceeds this value. Alert settings, e.g., number and type of recipients, will affect how long such an alert takes to process. Please keep this in mind, and run tests, before increasing this limit. Scheduling such alerts out of busy times would allow some leeway in processing times.

**130) Alert conditions required**

When enabled, it will prevent users from saving an alert without any conditions. When the global setting is set to "Yes", then alerts which do not have any conditions attached cannot be saved until a condition has been added. Upon clicking save on an alert with no conditions, users will receive the following warning: "You have entered no conditions, and it is mandatory for all alerts to contain conditions. Please add at least one condition to your alert so that it is valid and can be saved" When the global setting is set to "No" then alerts which do not have any conditions attached, then the behaviour is as per current functionality whereby the warning below is displayed, and upon clicking "OK" the alert is saved, clicking "Cancel" allows the user to continue editing the alert: "You have entered no conditions, which will have the effect of firing for every possible item.

# COLOUR SCHEMES

### 10) Which colour to use for system highlights?

This is the colour that will be used in the user login box on your login page, and the background colour for the titles of each section of an entry form in all Registers used in RiskMan (unless overridden). Click the Find Colour button to choose your desired colour or enter a Hexadecimal value. The default colour is CCCC99.
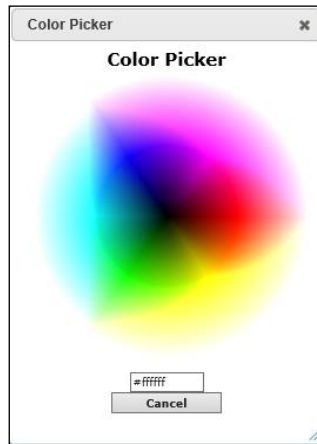


### 15) Which text colour to use for system highlights?

This is the text colour that will be used in the user login box on your login page, and text colour for the titles of each section of an entry form in all Registers used in RiskMan (unless overridden). Click the Find Colour button to choose your desired colour or enter a Hexadecimal value. The default colour is 000000 (Black).
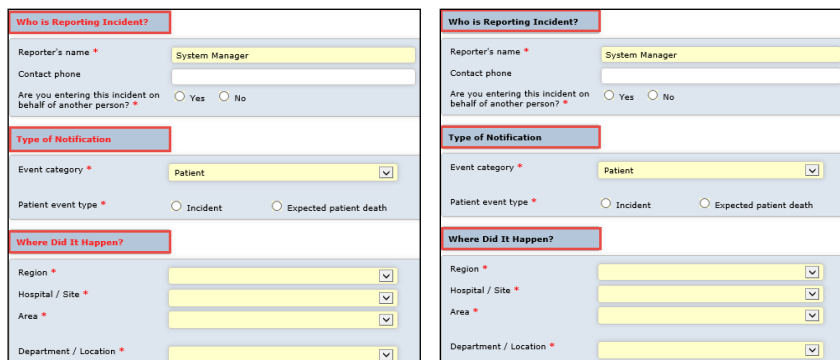
**20) Which colour to use for Mandatory fields?**

This is the colour that will be used to indicate mandatory fields on item entry forms. Click the Find Colour button to choose your desired colour or enter a Hexadecimal value. The default value is FFFF99, which is a yellow colour.

**25) Which icon rollover colour to use (e.g. Inbox)?**

This is the colour that will be used for the mouse rollover of Icons in places like Inbox. Generally, this will match the text highlight colour, but may be changed separately if required, e.g. for a very light highlight colour.

**30) Which colour scheme to use for the navigation buttons in the Control Panel of saved records?**

This setting chooses the colours for the navigation buttons that appear in the Control Panel at the top of Item Review screens.

**40) Which colour theme to apply to the page containing the Main Menu**

This setting determines the colours applied to the main display of RiskMan. One of the applied changes will reflect in the top section of the RiskMan screen and the menu bar.

**50) Which colour theme to apply generally**

Specifies the colour scheme (Theme) to apply to web page controls in RiskMan.

**60) Repeated background Image URL to use in the greyed out section when timed out?**

When RiskMan times out, a login dialog is displayed. The rest of the screen is obscured for security reasons. This image specified here is repeated in the greyed background area. The default is 'images/RMdevice.png', the RiskMan logo. Another image may be substituted, or the field may be left blank for no image.

Global Settings Descriptions
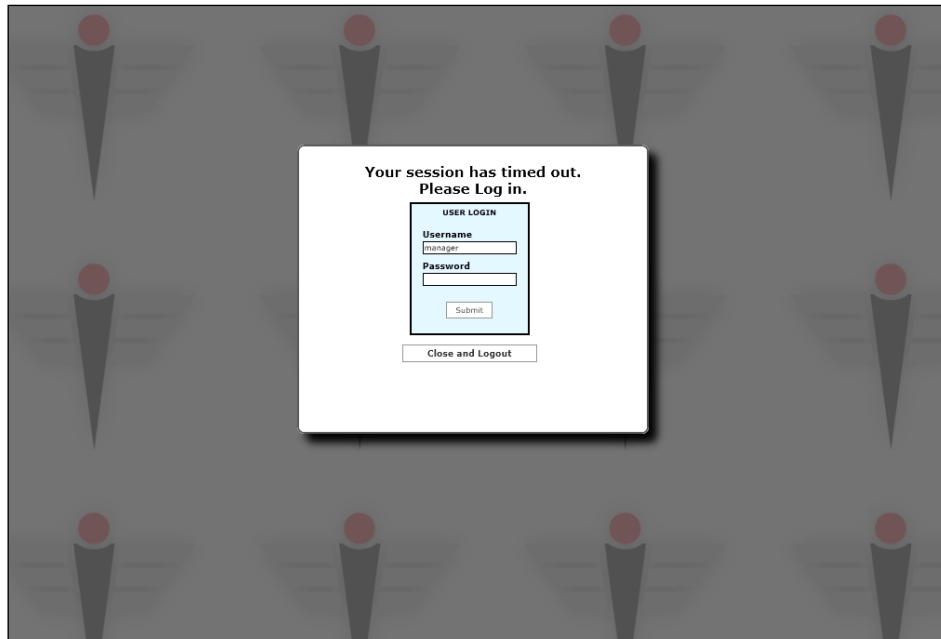


## 70) Which Style set to apply to the Entry form

Determine which CSS set to apply to the Entry form.

## 80) Apply colour coding to Review History

Enabling this setting will cause different rows in Review History to be colour coded depending upon the reason for the History entry, for example deletes will display in red.



**Review History**

| Date | User | Notes |
|---|---|---|
| 10 Oct 2024 15:07 | corinne (Corinne Kelly) | Created the incident item. |
| 10 Oct 2024 15:08 | Lauren Haupt (Lauren Haupt) | Initial Journal Alert Email SENT: Created by corinne (Corinne Kelly). Journal ID: 10194 |
| 10 Oct 2024 15:08 | corinne (Corinne Kelly) | Most recently viewed. |
| 10 Oct 2024 15:08 | corinne (Corinne Kelly) | Unposted incident item edited. |
| 10 Oct 2024 15:08 | corinne (Corinne Kelly) | Incident item posted. |
| 10 Oct 2024 15:10 | Lauren Haupt (Lauren Haupt) | Incident item first viewed. |
| 10 Oct 2024 15:11 | Lauren Haupt (Lauren Haupt) | Journal marked as ACTIONED. Journal ID: 10194 |
| 10 Oct 2024 15:11 | jjones (Jack Jones) | On distribution list created by Lauren Haupt (Lauren Haupt): Incident item NOT yet viewed. |
| 10 Oct 2024 15:12 | Lauren Haupt (Lauren Haupt) | Most recently viewed. |
| 10 Oct 2024 15:12 | Lauren Haupt (Lauren Haupt) | Unposted incident item edited. |

# DOCUMENTS

**10) Restrict the type of files which can be attached to a record?**

This setting allows you to define which file types are allowed to be attached to a record in a Register, using the Attach Documents function. By default, this is set to "No", which means that any type of file may be attached to a record (as long as the file size does not exceed the limit you have set in Attach Document Settings under the Administration menu). If you would like to prevent users from attaching certain types of files (for example .EXE files), select "Yes" here. You will then be able to nominate which file types are permitted by using the [(Documents) File Extensions] list in List & Codes Maintenance.

# ITEM ENTRY DEFAULTS

## Distribution Lists

**10) Enable Distribution Lists**

Enabling this option allows the Distribution List feature to be used. Distribution Lists are a method of allowing selected users to grant others permission to see a saved register item.

To use Distribution Lists, this setting **must** be enabled, and the permission "Can apply Distribution Lists" must be enabled on the required User Template(s) and/or Profile(s).

**20) Make Distribution lists sequential.**

If Distribution Lists are enabled, enabling this option causes the Distribution List Notification E-mail to be sent to each Reviewer one-by-one. Once a reviewer has reviewed and released the item, the next person on the Distribution list will be notified of the item and be granted permission to view the item (ie. as the prior Reviewer on the distribution list completes their review/amendments).

If this option is disabled, the Distribution List will be "concurrent". That is, the Distribution List Notification E-mail will be sent to all Reviewers at the same time giving them permission to view the item at the same time.

**Note**

*We recommend that distribution lists are set as concurrent to ensure users are notified as quickly as possible in regard to the item and to eliminate any delays in notifying nominated users*

**30) Send Email notification to users on a distribution list.**

When enabled, this setting sends an email notification to any users who have been added to a Distribution List.

**Note**

*If sequential distribution lists are enabled, users will be notified when they become ACTIVE.*

**40) Send only one email notification to each user on a distribution list.**

When enabled, a notification will only be sent once to a person on a Distribution list. If additional personnel are added to the Distribution List after the initial email has been forwarded, those users who previously received an email will not be sent another (prevents double-ups).

**Note**

*If there are existing users on the Distribution list, it means those users have not viewed the record. If you add more users to the list and you enter additional comments to be included in the Distribution List email, then ALL users (even those already sent an email) will be sent an email notification unless Option 50) is enabled.*

**50) Do not send Distribution List emails again, even if email comments are entered**

Normally RiskMan will send an email to everyone on a distribution list, even if they have been notified before and additional comments are added to the email notifications. If this option is disabled, and additional users are added to a distribution list where there are already users on the list (who have not yet viewed the item), and additional comments are added to the email notification, ONLY the newly added users will receive the email notification

**Note**

*Any comments added to the Distribution List email notification can be viewed from the Review History by clicking on the <Email> link (dependent on the setting 60) Email notes for Distribution List emails display in Review History using this policy).*

**60) Email notes for Distribution List emails display in Review History using this policy.**

The additional notes included when a distribution list is created can be viewed from the Review History of a notification/item/activity. There are 3 choices as to how these additional notes are viewed:
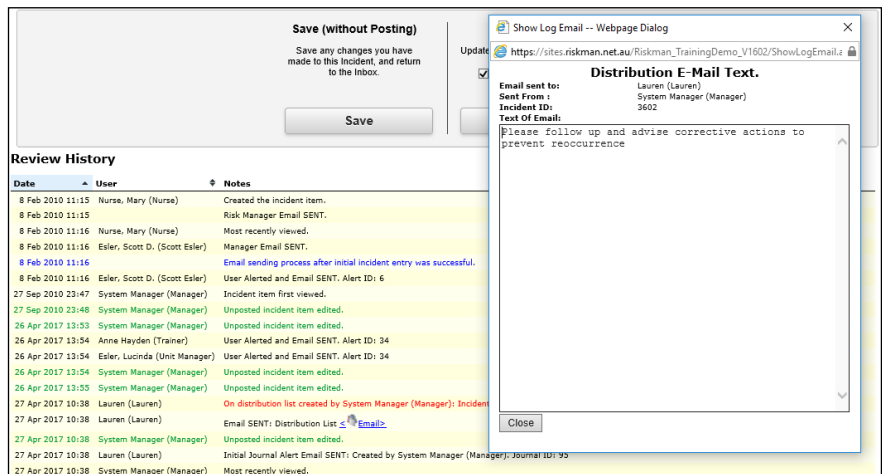


- **Do not display**: The  <Email>  link will never be displayed in the Review History
- **Only for Sender, Receiver**: The <Email> link will only appear in the Review History of the record if the user viewing it is the creator of the Distribution list or is one of the recipients of that distribution list
- **Always Display**: This is the default. The <Email> link will always display in the Review History of a record where a distribution list is created and an additional comment is added, so that all users with access to that record can view the comment

**Note**

*There is a User Permission under each the Register User Profiles/Templates (except Feedback): "Can always see Review Log Distribution List email Links", which will override the above options and allow the user to view all distribution list comments on items they have authority to view.*
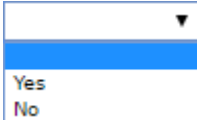
## Form Options

**10) Select the display option for Yes/No questions on item entry forms.**

Some data items in Item Entry forms have "Yes/No" responses. Select the style of your Yes/No fields from the drop down list.

Radio Buttons      ◯ Yes    ◯ No

Drop Down list

Yes
No

Checkbox      Next Of Kin Notified ☐

**20) Mandatory setting for Date of Birth field applies to Items involving a Client only.**

Enabling this setting means that if the **Date of Birth** is set as a mandatory-entry field in the User Template, then it will be set to mandatory on the Incident Entry form **only** if the Incident Involved belongs to the Patient Class eg. Resident, Client, Patient

**30) Date entry fields display option.**
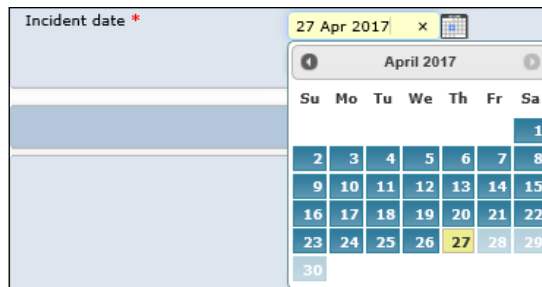
This setting changes the way users will enter any dates on item entry forms.

**Use dropdown list** provides a separate drop down box for the day, month and year values:



**Free form entry field** will display a single text box, where the user can either enter a date/time in a variety of formats (e.g. 1/6/04, 1 June 2004, 0400, 13:00) and RiskMan will attempt to interpret the entered date/time into a standard form. This option will also provide a drop-down date picker on date fields:



**40) Username display style.**

Defines how a name should be displayed when searching for another RiskMan user, and also the logged-in user's name in the top right of the screen eg. John Smith, John Smith (smithj), smithj, smithj (John Smith)

**50) How many items to show in a multi-select list?**

Defines the maximum number of values shown in a multi-select list before a scroll bar is used. Default value is 5.

# Item Version Management

**10) Create an unposted copy of the record when it is posted or reposted.**

When turned on, the edit of a Posted record will also create a new Unposted Edit version automatically. This has advantages in that the next edit will contain all updated information by default, simplifying the review process; also, users without access to the posted record will see the latest information.

**Note**

*It is recommended that this option is set to Yes*

**20) Description to appear above the "Post" and "Update the Posted Record" buttons on the form for the above function.**

This option refers to Option 10). It allows you to specify the wording that will appear above the "Post" and "Update the Posted Record" buttons.

The default value is "Make these changes available to all Authorised Users?"

**30) Make the above action the default**

By enabling this setting, the check box for the setting *10) Create an unposted copy of the record when it is posted or reposted.* will be checked by default.

**35) Automatically set the above action to "Yes" and hide this option**

When editing a posted record, there is normally an option displayed saying "Make these changes available to all authorised users" or similar wording (as specified in Item Entry Defaults | Item Version Management | 20) Description to appear above the "Post" and "Update the Posted Record" buttons on the form for the above action). This means that a new unposted version mirroring the posted version is created when this the posted version is updated. This is good because any changes or updates made to the record (posted or unposted) are available to be included in the next version.

Historically, the option existed because of the rare case where the posted version may have confidential information not appropriate to be read by the original submitter or other involved parties. In practice this proved too difficult to manage and caused potential overwrite issues if not managed correctly. Problematic entries now tend to be handled by restricting access to the whole record via the alerts. Setting this option to "Yes" (recommended) hides the option, preventing incorrect use.

**40) "Can review own/subordinates entries" edit mode when "Allow item entry" is OFF**

This setting allows a user to determine whether a user should be able to modify a record when they do not have the user permission "Can do item entry", but do have the permission "Can review own/subordinate's entries".

What this means in a practical sense is that you can setup a user who cannot enter new records, but can see existing records as they are granted permission to do so, and then determine whether the user should be able to modify those records or not.

# Journals

**10) Enable Journal Entry**

Checking this option enables Journal Entry features in RiskMan. Journals are date/time-stamped categorised entries which can be used to allocate tasks, include progress/file notes, reviews, document meetings/telephone conversations

**Note**

*It is recommended that this feature be turned on. Permissions to use the journals is set in the User Profiles & Templates*

**20) Make the "Journal Type" field on journals mandatory.**

When enabled, the **Journal Type** field will be mandatory when adding a new Journal entry.

**30) CC Journal Creator when Journal Alert Reminder is sent.**

If this setting is enabled, Journal Alert reminder emails will be sent to both the person allocated the follow-up of the Journal, *and* the creator of the Journal.

**40) When a Journal is actioned, it is mandatory to enter the "Task Outcome" and "Task Completed Date" fields.**
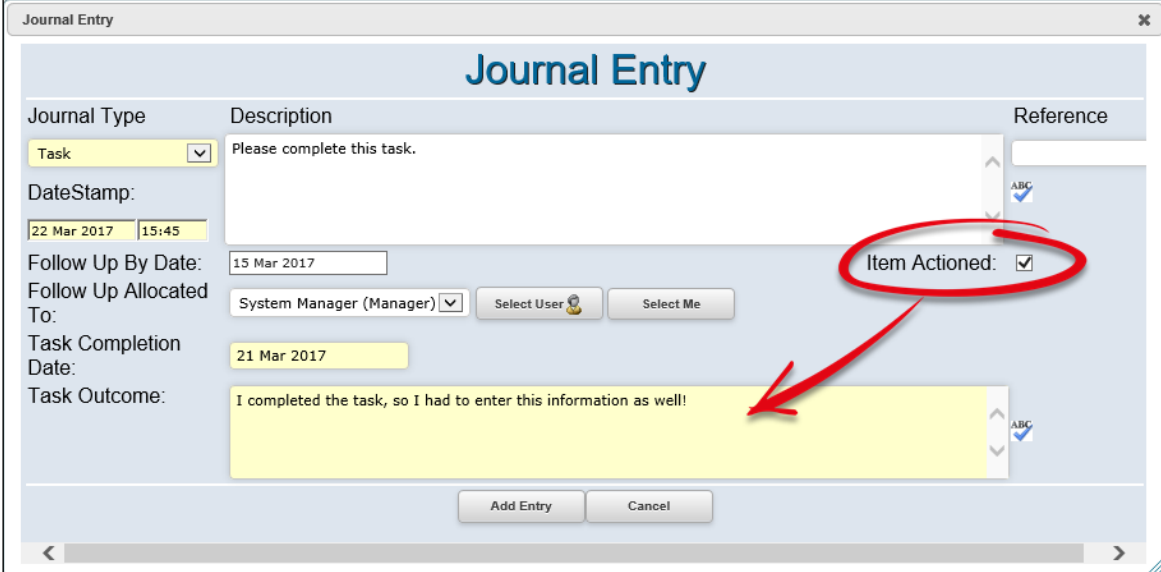
When enabled, a user Actioning a journal will be required to enter information in the **Journal Task Outcome** field, and also a **Journal Task Completion Date** field.

If these fields are not shown under the current rules for the Journal Type, they will be shown automatically.

This rule will apply for a new (unsaved) journal entry if the **Item Actioned** field is shown and the user checks it.

When a journal is displayed, e.g. in a report, the outcome and task completion date will be shown if the item is actioned and there is a value in the task completion date field.



**Note**

*These fields will be shown even if they are set to not be displayed under the current rules for the Journal Type (via List & Codes Maintenance).*

**50) Allow users to change Date and Time Stamp on Journals**

Setting it to "No" will disable the Date and Time (DateStamp) fields on Journal Entry page. Setting it to Yes will allow the user to change the Date and Time fields.

# Record Locking

**10) Enables Record Locking to prevent two users editing the same record.**

When enabled, record locking is implemented. When an existing entry record is opened, the server is informed to a place a lock on that record. This will prevent another user from editing this record while the user is actively using it.

To do this, the browser will communicate with the server frequently to maintain the lock, and the lock will automatically expire after a period (configured by other global settings) if no communication is received by the server.

*Note: While normally very reliable, this process does have limitations. Notably, if a user switches to another tab in the browser or minimises the browser then the communication with the server may not occur frequently enough to maintain the lock. This is outside the coding options available and cannot be resolved. If a user opens a record and doesn't navigate away, then the record will be locked indefinitely.*

Despite these minor limitations this functionality can be quite helpful.

**20) Lock Lifespan, how long to hold a record lock (in seconds)**

This setting indicates to the web server how long to hold a lock before releasing it. When a record is locked, the browser communicates with the server regularly to inform the server that the user is still using the record. If the server does not receive a lock confirmation within the period specified here, then the lock will be available for another user to take. For this reason, the cycle time setting should be shorter than this by a reasonable margin.

Default value is 30 seconds. A shorter period means that the lock is released quicker but makes the possibility of a lock being released incorrectly higher. A value of 20 should be fine but be wary of making this value much shorter than that. Suitable values will depend largely upon your infrastructure.

**30) How frequently to confirm a record lock is still required (in seconds)**

This setting indicates how frequently the browser will communicate with the web server to confirm a lock is still required. This value should be significantly smaller than that specified in the Lifespan global setting, since communication takes time and can vary.

Default value is 14 seconds. A shorter period means better responsiveness and reliability, but more traffic with the web server. Suitable values will depend upon your infrastructure.

# Item Entry Defaults

**10) Allow users to modify forms, maintaining all versions**

Checking this option allows users to directly modify information previously entered in a saved record. A record modified in this fashion will be re-submitted to the Administrator's Inbox for review, with a status of "New Edit". Disabling this setting will prevent users from directly modifying information previously reported. Each time a modification is made to a saved record, a new version is created, thus ensuring that the original notification that was entered remains intact

**Note**

*If your organisation still wishes to receive further information from reporters, but does not want to allow reports to be altered directly, enable the setting 20) Allow users to add notes to existing forms). However, we do recommend that users have the ability to edit notifications*

**Warning**

*If the system has been in operation for some time, and users have been able to submit direct changes to previously entered reports, the system will have been accumulating multiple versions of existing records. Disabling this function at this point may disable access to these record versions. If it is required that this option be disabled after a period of operation with it enabled, please contact support at RiskMan Support to ensure no data loss occurs –* https://hub.rldatix.com/SupportHUB/s/

**20) Allow users to add notes to existing forms**

By enabling this setting, a user can open a record they have submitted and add additional notes via the "Comments" field at the top of the form. The attached notes are then re-submitted for their Manager to review.

**Note**

*The notes entered into the "Comments" field will not be saved with the Posted version (if the Register uses the posting paradigm). We suggest that if you wish to capture these notes in the posted records, copy them into a Journal Entry.*

*It is recommended this feature should not be turned on, and where possible, encourage your staff to enter additional notes via the Journals*

## 30) Enable Group (Multi-Person) Entries

A grouped entry is where more than one record is linked to another record.

**Example in Incidents**: A grouped incident is usually a multi-person event where there was more than one person involved e.g. Aggressive behaviour from a client to a staff member; in this case, 2 separate incidents may be entered but because they both relate to one another, they can be linked.

### Note

*This setting does not need to be enabled simply "because you can". You should ensure that your organisation has a clearly defined purpose for using this setting before enabling it.*

## 40) Enable DENY ACCESS function in Distribution Lists

If set to YES, any users with permission to create Distribution Lists will have the option to remove other users' permission to an item which they have previously been granted permission to see.

This is an Administrator-level function and should <u>ONLY</u> be used to remove a user's permission to see a record if that permission was granted in error. If required, this option should be enabled, the required action taken, and then immediately disabled once completed.

**50) Post entries automatically, bypass 'Inbox' (where applicable)**

For Registers that use the posting paradigm eg. Incidents, by enabling this setting, new items will be "posted" immediately, bypassing the need to be first reviewed via the Inbox. *This may be an appropriate option if a large number of paper-based reports were being "bulk-keyed" into the system.*

Disabling this setting will cause all new items to be initially sent to the Inbox for review.

**Note**

*Auto-posting can be turned on based on specific criteria e.g. for a particular facility or Incident Involved Type. If you would like auto-posting turned on for specific situations, please contact RiskMan support –* https://hub.rldatix.com/SupportHUB/s/

**60) Mouse Scroll handling on entry forms**

The mouse scroll wheel can change the selected option of a dropdown list accidentally, when the intent is to scroll the page. This setting only has an effect when entering or viewing records, and nowhere else.

Available options are:

- **Default behaviour**: The user's browser and browser version will determine the behaviour when they use their scroll wheel
- **Disable all scroll for page**: Using the scroll wheel on a record entry form will have no effect at all
- **Disable scroll for dropdown lists only**: Scrolling is enabled on the record entry form, but has no effect if a dropdown list is currently selected (recommended).

**70) Limit the Summary field on entry form (where present) to this many characters:**

Specify the maximum number of characters that a user is allowed to enter into the "Summary" field (where present) of a record. The maximum number of characters allowed in this field is 8000

**Recommended**
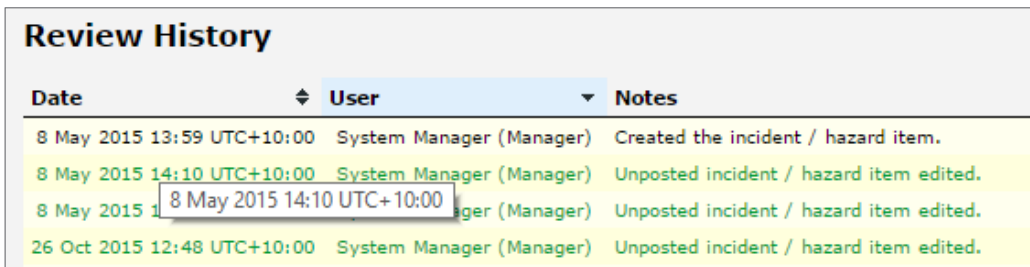
*Limit the size of this field from 50 to 200 characters*

**80) Display the 'Most Recently Viewed' status in the Review History.**

RiskMan notes when a user first views an existing record, and saves this information in that record's Review History. Enabling this setting will mean that RiskMan will also record when a user has most recently viewed a record as well.

**85) Display UTC date values in Review History**

Display Server UTC date/time in the Review History of a record. Mouseover the date to display the local date/time for an entry.



**90) Show all risks on Associated Risk Page.**

If this option is __NOT__ enabled, then when a user clicks the **Add Associated Risk** button on the Item Entry form, they will see the following:

- All risks with the status of Open or Reopen, which do not have a selected responsible Site and/or Site/Location (Organisation Wide Risks), and,
- All risks with a responsible Site and/or Site/Location matching the selected one on the current Item form (this is the current default behaviour)

If this option __IS__ enabled, then when a user clicks the **Add Associated Risk** button on the Item Entry form, they will see the following:

- All risks with a status of Open or Reopen, regardless of the Responsible Site and/or Site/Location selected on the Entry form

**100) Make Classifications 'Single Select'.**

*(Only relevant to users who use the RiskCat classification selector style for classifying records)*

If this setting is enabled, a user will only be able to select ONE classification from the relevant RiskCat.

**Note**

*We advise you take care with this setting, as it may not meet the requirements of your reporting and may reduce the information you are capturing in your system*

**110) Eliminate the first 'Confirm' page on initial item entry.**

If enabled, the "Acknowledgement" page (displayed after you save a new record) will be bypassed when a user submits a new record. Instead, the user will be directed to the Confirmation page.

**Note**

*Any user defined text that normally appears on the Acknowledgement page will not be displayed on the Confirmation page*

**Recommend**

*This setting is deprecated and thus should be enabled.*

**120) Allow users to display the 'Change History' (from the Control Panel).**

If enabled, a "Change History" button will display in the Control Panel of an existing record when reviewed. By clicking this button, a user will be able to view all the changes that have been made to that record - they will only see the changes made to fields that they have permission to see.

**130) Enable the AutoSave function for new forms.**

When enabled, RiskMan automatically saves a 'draft' version of a new item in case a user's session ends unintentionally. When that user next attempts to enter a new notification of the same type, RiskMan will prompt them to either open the AutoSaved record, and complete it; or discard the AutoSaved record, and start with a blank form.

**Note**

*This function is generally not recommended if your organisation uses any anonymous or generic system logins.*

**140) User to apply when generating records anonymously**

When a user opts to create a form anonymously, this username will be used in place of the users own identity. To disable the Anonymous functionality, leave this field blank. To use the anonymous functionality, it must be coded into the configuration of relevant registers.

**150) Mandatory field Prefix/Suffix setting**

Controls whether mandatory fields should have a prefix, a suffix, both, or none at all. You can make register-specific versions of this setting.

**160) Prefix string for the title of mandatory fields.**

This setting contains the text you want as a prefix on the labels of mandatory fields. You can use HTML tags to control the format of the text. You can make register-specific versions of this setting.

**170) Suffix string for the title of mandatory fields.**

This setting contains the text you want as a suffix on the labels of mandatory fields. You can use HTML tags to control the format of the text. You can make register-specific versions of this setting.



**180) Date pickers should start the week on what day?**

Allow you to change which day of the week should be in the first column on date pickers. The default day is Sunday.
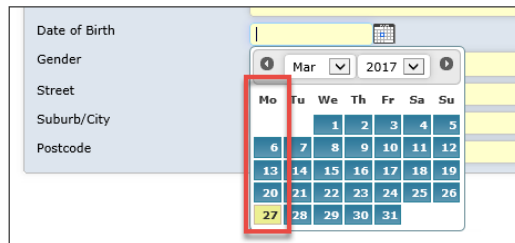


**190) By-Pass the Submit or Submit and Clone pop-up page.**

This Global Setting will allow you to determine if the Submit and Clone pop-up page presents to the user or not. You need to consider the user's ability to create Drafts. Submit and Clone pop-up page bypass cannot be set to "yes" if the user has the ability to create Draft records turned on in the Template for the User profile.

This global setting can be made Register specific, but if there is no Register specific setting then it will apply to all Registers

This Global Setting applies to Post, Update and Save buttons at the bottom of a record.

# Shortcuts

**10) Draft shortcut expiry time (days)**

Allows you to set whether personal drafts created from items expire after a particular timeframe. If this field is set to 0, drafts created will never expire. If you put a numerical figure in here, this is the number of days that any draft will remain in the system before expiring (e.g. 5 would mean each draft created expires after 5 days).

**20) Maximum age (days) of expired drafts**

The maximum number of days of expired draft entries. Please keep in mind that when a draft is deleted, the user will no longer be able to access it. If drafts should never be auto deleted, enter 0 (zero) in this setting.

# LICENSING

**10) Send licensing emails to administrators**

RiskMan will inform administrative users via email if licensing issues occur. When enabled, this function sends these emails to any users with permissions to User Profiles pages.

**20) Send licensing emails to a nominated user**

RiskMan will inform a nominated user via email if licensing issues occur. When enabled, this function sends these emails to the user nominated in the following setting (30).

**30) User nominated to receive licensing emails**

Select the user to receive RiskMan licensing emails. Works in conjunction with the previous setting (20).

**40) Send licensing emails to a nominated email address**

RiskMan will email a specific address if licensing issues occur. When enabled, this function sends licensing emails to the email address specified in the following setting (50). A benefit of this option is that the person informed of licensing issues does not need to be a registered RiskMan user.

**50) Nominated email address**

This is the email address to send licensing emails to. Works in conjunction with the previous setting (40). This must be an organisational email address, i.e. user@yourorganisation.com, and cannot be an external address, i.e. Gmail, Bigpond, etc.

**60) Send licensing emails to all users who belong to a nominated Template**

RiskMan will inform all the users of a nominated User Template if licensing issues occur. When enabled, this function sends licensing emails to any users who belongs to the User Template nominated in the following setting (70).

**70) Nominated User Template**

Select the Template containing the users who will receive licensing emails. Note that ALL the users on this template will be emailed. Works in conjunction with the previous setting (60).

**80) Show Message when percentage of the total number of user licenses used?**

The default value is 95.

Please note: The minimum possible value is 1

Please note: The maximum possible value is 100

Please note: Otherwise, the value will be 95

# MAIL

**10) Email Sending.**

Choose the method of sending emails from RiskMan. This setting should only be modified in consultation with RiskMan Support – https://hub.rldatix.com/SupportHUB/s/

Version 2209 has added alternative options to Mail Sending. As Microsoft is looking to deprecate Basic Authentication which may impact the current "Standard Method"

There are four email sending options:

1. **MailKit**: This should be considered the default option. Added in 2022, and the component is widely recommended, including by Microsoft. It is the most modern, complete, and capable option.

2. **Microsoft SMTPClient**: Previously labelled "Standard Method", this was the previously recommended method. Microsoft themselves now consider this obsolete and suggest using some other method, specifically suggesting MailKit.

3. **Alternate Method (JMail)**: This was the best available product at the time but is quite old. While it still works in some situations, it has some important limitations such as international characters not being supported. Not usually recommended.

4. **Disabled**: Emails will not be sent.

**20) Send Email notification to the Line Managers when an Item is created**

When RiskMan users create new records, they are available for review by any RiskMan user who is defined as the Reporter's Manager *(RiskMan uses the term Line Managers, but this refers to any manager in a user's line of standard reporting)*. In addition to new items being placed in the Manager's Review List, RiskMan can also send e-mail notifications of new items to the relevant Manager(s).

**Note**

*Alerts can be used instead of standard Line Manager Notifications. Refer to the description of setting (10) under the Alerts group for more information*

**30) Send EMail notification to the Risk Manager when an Item is created.**

In addition to new item notifications appearing in the Inbox, this setting can also send e-mail notifications of new items to the Administrator (the email address that appears in the setting *Mail >*

*Mail Configuration > 10) Risk Manager's Email Address)*, thereby keeping the Administrator informed of new notifications without the need to be constantly logged on and refreshing the Inbox.

Alternatively an alert can be set up to notify the Risk Manager/s of specific items eg. Serious Incidents, Risks with an Extreme or High rating, rather than every item that is entered into RiskMan – *refer to the Alert Management Guide for more details*

**40) Send EMail notification to the Risk Manager when a user creates their own login.**

If user self-registration is enabled *(refer to the Users settings group)*, enabling this setting causes the system to send the Administrator (eg. *Risk Manager*) an email each time a user creates their own login *(to the email address recorded in Mail > Mail Configuration > 10) Risk Manager's Email Address).*

**50) Maximum number of emails to send per cycle**

This setting allows users to specify how many emails are to send out per mail cycle.

If the global setting is set to 0, then there are no maximum emails to send per cycle, therefore the cycle will finish once all unsent emails have been sent out

**60) Maximum number of tries to try resending unsent emails**

This setting will limit the number of retries for resending an unsent email before it no longer attempts to resend.

The default value has been set to 150 tries which will be reached after 100 resent attempts every 1 minute + 50 resend attempts every 2 hours = approximately 4.3 days.

If the global setting is set to 0, then there will be no limit on the number of retries an email will continue trying to send for, which is how the email resending has previously worked, which can result in an email which is months or years old suddenly resending if the reason it was unsent is resolved.

Note: The retry rate remains unchanged from the current functionality which is:

- Retry every 1 minute for the first 100 tries
- Retry every 2 hours between 100 and 200 tries
- Retry once per day after 200 tries

# Mail Configuration

**10) Risk Manager's Email Address**

If Risk/Quality Manager email notifications are enabled, specify the email address of the Risk/Quality Manager in this field. To send to more than one email address, separate addresses with a semi-colon (;).

**15) What title to use for the Risk Manager**

There are various places in the system where the top level administrator of RiskMan is referred to. For example, when logging an email sent about creation of a new item. This setting details the terminology to use for that person/role.

The title of the risk manager will now be placed in the "User" column of the review history instead of the hard-coded value "Clinical Risk Manager" and the Notes column will advise an email was sent to the risk manager.

**20) The address of your Mail Server**

This setting nominates the network address of your e-mail server. This may either be a TCP/IP formed address (e.g. 172.16.1.27), the network name of a server (e.g. MailServer1) or an Internet address (e.g. mail.mailcentral.com). The mail server must be SMTP mail-capable. This setting may not apply for all mail server types.

Please contact RiskMan support - https://hub.rldatix.com/SupportHUB/s/ or your IT Administrator for details on the correct setting to use in your organisation.

**25) Does the server require SSL enabled?**

This setting is related to RiskMan's ability to support Office 365 using SSL authentication.  By default, Office 365 using SSL authentication will use port number 587 unless specified. When set to "Not required" no action will be taken and default to port 25. This is a default port number for SMTP mail service. When set to "SSL required", SSL functionality will be enabled in the mail client.

**27) What port is required?**

If left empty the default port is used. Only put a value here if needed. When the option "SSL required" is set then the default is 587, supporting "Office 365" otherwise the port will be 25.

## 30) What name do you want used as the 'Senders Name'?

This is the text that will appear in the "From" field when RiskMan generates emails. Usually this is set as "RiskMan Notification" or similar.

**Note**

*Not all email systems support this setting.*

## 40) What email address do you want used as the 'Reply To' address?

If users are accidently replying to emails that have been sent from RiskMan, this setting nominates the actual email address used as a return email address if an automated Notification e-mail is replied to. This is often the same email address as 10) Risk Manager's Email Address

**Note**

*Not all e-mail systems support this setting.*

## 50) Use user's email address as 'Reply To' address

An alternative to setting (40). If this setting is enabled, and a user does reply to a RiskMan notification, then the email will be sent to the originator of the email eg. the email address of the person who created the distribution list, journal alert, etc.

## 60) Mail SMTP Authentication Type.

This setting should not be changed. It will be configured if required but consultation with support at *RLDatix* https://hub.rldatix.com/SupportHUB/s/ is required.

## 70) SMTP Username.

This setting should not be changed. It will be configured if required but consultation with support at RLDatix https://hub.rldatix.com/SupportHUB/s/ is required.

## 80) SMTP Password.

This setting should not be changed. It will be configured if required but consultation with support at RLDatix https://hub.rldatix.com/SupportHUB/s/ is required.

**90) Send Email notification to the Risk Manager when a user retrieves their password**

If standard logons are used in RiskMan, there is an option for users to retrieve their password (via email) if they cannot remember it *(see details the setting User Control > 100) Allow users to recover their own password by email.)*

If this global setting is enabled, the email addresses that appears in the setting *Mail > Mail Configuration > 10) Risk Manager's Email Address* will be notified whenever a user retrieves their password (the password will not be displayed in the email)

**Note**

*This option would <u>not</u> be turned on if Network Logins and Passwords have been setup in your system ie. LDAP is turned on under Users > Authentication > 10) RiskMan User Authentication Method = LDAP*

**100) Allow automatic update the RiskMan site URL (i.e. Use the below value always). Select no to allow the update.**

This setting should not be changed. It will be configured if required but consultation with support at RLDatix https://hub.rldatix.com/SupportHUB/s/ is required.

**110) The RiskMan Site address as used in Emails.**

This setting should not be changed. It will be configured if required but consultation with support at RLDatix https://hub.rldatix.com/SupportHUB/s/ is required.

**120) Maximum number of error emails to send a user (email address) in 1 day**

Under some circumstances, RiskMan may generate a large number of 'RiskMan Error' emails addressed to an individual in a short period of time. This setting will limit the number actually sent in any rolling 24 hour period. If the count of emails to be sent exceeds the limit, then a single notification will be sent each hour that there are multiple emails waiting to be viewed.

The user will have access to their **Email Log** page in RiskMan - accessed from their *My Workspace > My Email Log* menu option *(provided the General permission: **Can access the personal email log from the menu** is checked)* to review these emails awaiting delivery, and optionally never actually send the emails if they are not required.

Set the value to **0** to disable this functionality ie. If disabled, <u>**all**</u> RiskMan Error emails will be sent to the RiskMan Administrator as they occur.

**130) Email address validation Regular Expression**

Defines a Regular Expression which is used to test that an email address is valid. Not all mail servers accept the same acceptable characters, and validating to be strictly correct is very difficult.

**140) Email address to which ALL emails will be sent instead of the original recipient.**

When this setting has a value, ALL emails will be sent only to this address. It is intended for testing purposes only.

# MANAGEMENT STRUCTURE

**10) 'Input/Entry' (Responsible Site and Location only) restrictions in 'Entered Items' are overridden by Manager/Staff relationships.**

A Line Manager may be restricted to view only the items reported at specific Sites or Locations, which may not necessarily be the same Sites or Locations as the staff that report to them.

By enabling this setting, items that have been entered by a staff member who is reporting against a Site/Location to which their Line Manager does not have access, will allow the Line Manager to view those items from their respective "Entered Items" page.

If this option is unchecked, the Line Manager will not have permission to view the items entered by their staff for a Site/Location to which they do not have access.

# NAMING CONVENTIONS

The list of fields/sections under this group enables you to redefine the labels used for specific fields and sections of the Item Entry forms (Figure 9)

The Naming Conventions that relate to "Sections" in this list refer to the sections on the Incident Register only

The Naming Conventions that relate to fields are the fields that are used across all Registers and in Alerts and Reports

**Note**

*As Administrators have the option to change field and section labels for each Register via User Templates and Profiles, any values you specify in this group of settings may be overridden by these customisations.*

# REGISTER ITEM LISTS

**10) How many rows to show by default in Inbox and other places?**

Select a number from the drop down list. This number is the default number of rows that will be displayed when you access any item listing pages eg. Inbox, Entered Risks, Posted Feedback, Deleted Incidents, Quality Activities.

The number of rows displayed can also be altered at the time you display a list, by changing the Settings at the bottom of the relevant list page. This setting is remembered on a per-user basis, so although you can specify the default number of rows, each individual user may choose how many records they show on a page.

The default value is 10.

**20) Default the Entered Item pages to display only the most recent "X" months.**

Select how many months, by default, of data a user can view in their displayed Entered Items pages. Individual users can override this setting by entering their own date ranges under the **Selection Settings** section of the Entered Items page. If a user overrides this setting, it will be remembered and used whenever they return to that page.

**30) Reason for linking register records together.**

When set to **yes**, the "Reason for linking / de-linking" text box will be shown in the Link Records dialog. The reason entered while linking records will then show up under review log for the master record.



**40) Minimum length of Reason for Linking text when enabled**

When the Reason for linking feature is enabled, this setting will define the minimum number of characters the user will need to enter in the Reason For Linking text box. Any value greater than "0" will make the field mandatory. Set it to "0" to make the field optional.

**50) Maximum length of Reason For Linking text when enabled**

When the Reason for linking feature is enabled, this setting will define the maximum number of characters a user can enter as Reason For Linking text.

**60) Maximum number of rows allowed in Inbox and other listing pages**

Allowing very large numbers of rows in Inbox and similar pages can cause seeming performance issues. The time taken to retrieve the rows can vary dramatically depending upon the selected columns shown and the general configuration of your system, so a practical number suitable for your system should be chosen. If the number is too large and under specific conditions, after a certain amount of time the system may error with a "time out", which is a bad experience for the end user. Choose a lower value.

**60) Maximum number of rows allowed in Inbox and other listing pages**

# REGISTERS

## Note

*The settings described here are the defaults only. However, whenever you create a "Register-Specific Version" of a Global Setting, it will appear in this section. In addition to this, if you have any custom Registers in your system (ie. other than Incidents, Feedback and Risk), they will have settings stored in this section also eg. Quality Activities*

*Consequently, you may potentially see several more items appearing in this section, dependant on your system configuration.*

## Feedback

### Note

*These are specific Feedback settings that are not available in the Feedback Global Settings*

**220) URL for the 'Consequences' descriptions page in SAC Matrix (leave empty for none)**

If you wish to provide the descriptions of the **Consequences** used in your Feedback SAC Matrix, these can be documented in a suitable format eg. HTML, PDF file. The file can either be placed in the RiskMan web server folder in your organisation or in another location that is accessible by the users. If the file is located in the RiskMan folder then only the file name (including the extension) is required in this field, otherwise the URL of the file location together with the filename (including the extension) will also need to be included in this field eg. **http://organisation/policies/sample_consequences.htm**. This will result in the "Consequences" button appearing on the Matrix which is used to open this file.

**230) URL for the 'Likelihood' descriptions page in SAC Matrix (leave empty for none)**

If you wish to provide the descriptions of the **Likelihood** used in your Feedback SAC Matrix, these can be documented in a suitable format eg. HTML, PDF file. The file can either be placed in the RiskMan folder on the server in your organisation or in another location that is accessible by the users. If the file is located in the RiskMan folder then only the file name (including the extension) is required in this field, otherwise the URL of the file location together with the filename (including the extension) will also need to be included in this field eg. **http://organisation/policies/sample_likelihood.htm**. This will result in the "Likelihood" button appearing on the Matrix which is used to open this file.

**240) Show short description on the Feedback SAC matrix Consequence and Likelihood fields**

The Feedback SAC Matrix has been updated to enable the display of short descriptors (maximum of 250 characters) underneath the Consequence and Likelihood fields when the global setting is enabled, and values have been set up in the following lists:

- **Feedback:** SAC Matrix Consequence Descriptors
- **Feedback:** SAC Matrix Likelihood Descriptors

# Incidents

**260) Incident Risk Matrix display style**

**Note**

*It is very rare that individual incidents receive a Risk Stratification rating, and as such, this setting will likely not apply to your configuration of RiskMan.*

When a user opens the Risk Matrix from the Risk Stratification or Potential Risk Stratification fields in an Incident the Risk Levels can be viewed as follows:

- **Show Scores:** Only the scores behind each cell will be displayed on the Risk Matrix
- **Show Rating:** Only the risk ratings (the default) will be displayed on the Risk Matrix
- **Show Rating and Scores:** Both the risk rating and the scores will be displayed on the Risk Matrix (See next page for an example)

| Likelihood | Consequences | | | | |
|---|---|---|---|---|---|
| | Insignificant | Minor | Moderate | Major | Catastrophic |
| Almost Certain | Medium(6) | High(7) | High(8) | Extreme(9) | Extreme(10) |
| Likely | Medium(5) | Medium(6) | High(7) | High(8) | Extreme(9) |
| Possible | Low(4) | Medium(5) | Medium(6) | High(7) | High(8) |
| Unlikely | Low(3) | Low(4) | Medium(5) | Medium(6) | High(7) |
| Rare | Low(2) | Low(3) | Low(4) | Medium(5) | Medium(6) |

| Legend | |
|---|---|
| Extreme | Extreme Risk; Immediate Attention Required |
| High | High Risk; Senior Management Attention Needed |
| Medium | Medium Risk; Management responsibilty must be specified |
| Low | Low Risk; Manage by routine procedures |
| Undefined | <---- Click this button if stratification undefined. |

☐ Show Scores.

Adapted from Standards Australia, Risk Management Standard AS/NZS ISO 31000:2009

*Example of the Risk Matrix showing only the Risk Scores in each of the cells*

**280) Show Incidents Notifications in top right hand corner of the home page?**

By selecting "Yes", the notifications for incidents inbox appear at the top right hand corner of the home page.
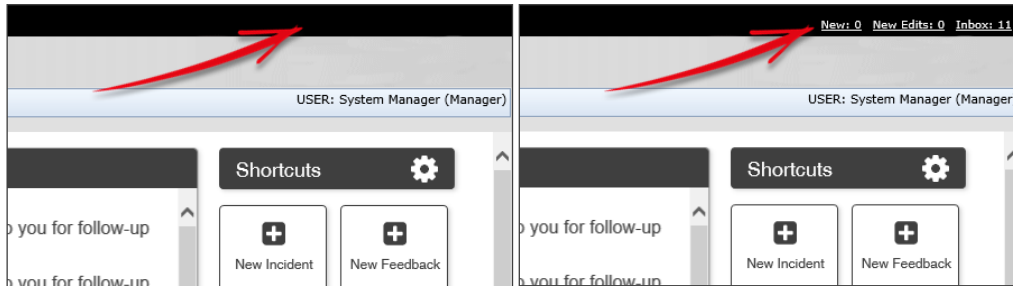
**Recommended**

*Disable this setting.*

# Risk

**200) URL for the 'Consequences' descriptions page in Risk Stratification (leave empty for none)**

If you wish to provide the descriptions of the **Consequences** used in your Risk Matrix, these can be documented in a suitable format eg. HTML, PDF file. The file can either be placed in the RiskMan web server folder in your organisation or in another location that is accessible by the users. If the file is located in the RiskMan folder then only the file name (including the extension) is required in this field, otherwise the URL of the file location together with the filename (including the extension) will also need to be included in this field eg. **http://organisation/sample_consequences.htm**. This will result in the "Consequences" button appearing on the Risk Matrix *(available in both Incident Notifications and the Risk Register)* which is used to open this file.

**210) URL for the 'Likelihood' descriptions page in Risk Stratification (leave empty for none)**

If you wish to provide the descriptions of the **Likelihood** used in your Risk Matrix, these can be documented in a suitable format eg. HTML, PDF file. The file can either be placed in the RiskMan folder on the server in your organisation or in another location that is accessible by the users. If the file is located in the RiskMan folder then only the file name (including the extension) is required in this field, otherwise the URL of the file location together with the filename (including the extension) will also need to be included in this field eg. **http://organisation/sample_likelihood.htm**. This will

result in the "Likelihood" button appearing on the Risk Matrix *(available in Incident Notifications and the Risk Register)* which is used to open this file.

**270) Risk Register Risk Matrix display style**

When a user opens the Risk Matrix from the Residual, Inherent or Potential Risk fields in the Risk Register, the Risk Levels can be viewed as follows

- **Show Scores:** Only the scores behind each cell will be displayed on the Risk Matrix
- **Show Rating:** Only the risk ratings (the default) will be displayed on the Risk Matrix
- **Show Rating and Scores:** Both the risk rating and the scores will be displayed on the Risk Matrix



*Example of the Risk Matrix in the Risk Register showing only the Risk Scores in each of the cells*

**300) When generating Heat Map image, use Web Browser image**

For Risk Heat Map printing, in order to enable the image to be captured within the Web Browser instead of being stored to disk and to ensure the image prints correctly. To enable this option, the below global setting will need to be enabled:

Registers > Risk > 300) When generating Heat Map image, use WebBrowser image

Edit and set to **Yes**.

# REPORTS

**20) Default report file format for generating reports**

This setting determines the default file format when reports are created. Users can easily choose other file formats as reports are previewed.

**30) Default report file format for generating Feedback reports**

This setting determines the default file format when Feedback reports are created. Users can easily choose other file formats as reports are previewed.

**40) File format for the 'Print Preview' reports**

This setting determines the default file format used when the "Print Preview" button is clicked from the **Control Panel** of an existing record.

**50) Report to display for the Report Button on the Posted Item Review page**

Select the report that will be generated from the Posted Item page as per the following descriptions *(Figure 12)*

- **Batched Insurer Report:** This is an Insurer report style that will display specific fields from the record.
- **Comprehensive Adverse Incident Report**: The static comprehensive report which only includes all the standard fields and does not reflect the user's permissions to fields on the Item Entry page
- **Comprehensive Custom Report:** Comprehensive report that includes standard and customer specific fields as well as adhering to the user profile of the user running the report ie. fields and sections the user has access to view in the Notification

**Note**

*The label that appears on the button to display the above reports is defined in the Global Setting: Reports > 110) What label to use for the Report Button on the Posted Item Review page?*
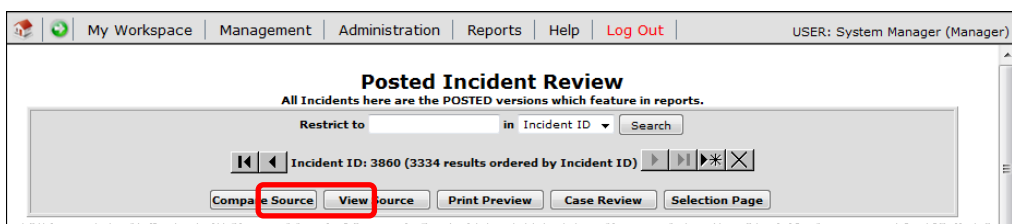
*In this example the report button is called "Print Preview" and will generate the Comprehensive Custom report as a PDF on the Posted incidents page*

## 60) Show Additional Comments section on the Comprehensive report from the Unposted Review Item page

When this setting is enabled, the comments that appear at the top of a record for review will also appear in the printed version of the record report. This option would only be turned on if option (20) under Item Entry Defaults is turned on.

### Note

*The notes entered in the "Comments" field will not be saved with the Posted Item. We suggest that if you wish to keep a copy of the notes, copy them into a Journal Entry.*

## 80) Include the Review History in the Comprehensive Custom Report

If this is setting is enabled, the Review History of the current record will appear at the bottom of the Comprehensive Custom Report (when a user presses the **Print Preview** button from an opened record).

### Note

*A "Print Comprehensive Custom Report Review History" option will display on the respective Reports pages when the Comprehensive Custom Report layout is selected. Users will have the option to show/hide the Review History when using the Comprehensive Custom Report layout.*

## 90) Order Journals by Date Created in the Comprehensive Custom Report.

If this setting is enabled, and there are Journals included in the current record, they will be ordered in Journal Entry Date order from oldest to newest when a user prints the Comprehensive Custom Report.

### Note

*A "Journal Order: Date ⊙ Journal Type⊙" option will display on the respective Reports pages when the Comprehensive Custom Report layout is selected. Users will have the option to display the Journals in Journal Type or Journal Entered Date order by selecting the respective option.*

## 100) By default, the Management Summary excludes any rows that contain 0 results.

This setting is deprecated and is scheduled to be removed.

## 110) What label to use for the Report Button on the Posted Item Review page?

Specify the label that is to appear on the "Report" button on the Posted Record review page (this relates to the *Report settings (40) and (50) above) – Figure 15*

The button label will not display more than 14 characters, so it is better to keep this button label short eg. **Print** or **Print Preview**



## 120) What label to use for the Report Button on the Unposted Item Review page?

Specify the label that is to appear on the "Report" button on individual Item Review pages. You will be able to select the output format at the time you generate the report ie. Adobe™ PDF, Word™, Excel™, RTF, Standard Format:
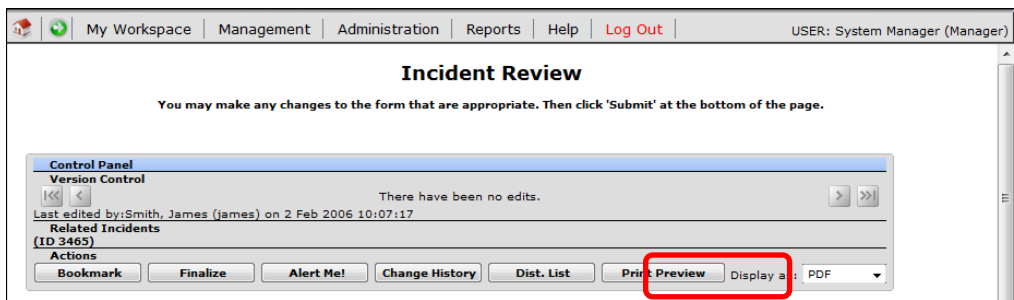


## 130) Default report Font name

This setting determines the Font used when generating reports. The default font is Verdana.

### Note

*The font size can also be adjusted and this setting will affect all fonts except the Chart Legend.*

## 140) Show/Hide a logo in the heading of the Comprehensive Custom Report

By checking this option, a logo is placed at the top of the Comprehensive Custom Report instead of the organisation name. The logo should be in a file called "logo.jpg" in the Images folder on the web server. The logo size should be no larger than 68(W) * 72(H) pixels.  This setting can be made register specific.

**150) Show/Hide the Printed By name in the footer of the Comprehensive Custom Report**

By checking this option, the name of the user who generated the report is placed in the footer of the Comprehensive Custom Report. This setting can be made register specific.

**160) What is the maximum number of Widget panels allowed in Infocentre?**

Restrictions can be applied to the number of groups that a user can add to their view of the InfoCentre.

**Note**

*If a user has access to global settings, this global setting will not be enforced as they are viewed as a "Super User"*

**170) What is the maximum number of Widgets allowed per panel in InfoCentre?**

Restrictions can be applied to the number of widgets that a user can add to any group in the InfoCentre.

**Note**

*If a user has access to global settings, this global setting will not be enforced as they are viewed as a "Super User"*

**180) When producing reports, mask fields that the user doesn't have permission to.**

When No is selected, RiskMan will display all fields on a report. When Yes, fields the user does not have permission to will be masked out. See the mask setting below.

| Incidents by Facility | | | | |
|---|---|---|---|---|
| ID | Incident Date<br>Incident Time<br>15:00 | Summary | Location<br>Service<br>General Medicine | Severity |
| 56 | 3 Nov 2012<br>11:30 | Pt fasting too long prior to surgery and pt became hypoglygaemic | Ward A3<br>Obstetric and Gynaecology | ********** |
| 57 | 1 Nov 2012<br>(None Entered) | Pt did not wait for first antenatal appointment | Ward A3<br>Obstetric and Gynaecology | ********** |
| 58 | 4 Nov 2012<br>15:00 | Ventilator malfunctioning | Emergency Department<br>Emergency Medicine | ********** |
| 59 | 5 Nov 2012<br>20:00 | Skin tear to leg ? Origin of same | Emergency Department<br>Emergency Medicine | ********** |
| 60 | 6 Nov 2012<br>01:30 | Pt received wrong dose of medicaltion | Ward A2<br>General Medicine | ********** |
| 61 | 4 Nov 2012<br>(None Entered) | Ultrasound result not satisfactory.  Pt had to have another ultrasound | Ward A3<br>Obstetric and Gynaecology | ********** |
| 63 | 4 Nov 2012<br>14:00 | Car damage whilst attending appointment in carpark | carpark<br>Obstetric and Gynaecology | ********** |
| 64 | 9 Nov 2012<br>18:45 | Pt received dose of Pencillin ?pt is allergic to same | Emergency Department<br>General Medicine | ********** |

**190) What mask to use when obscuring "Don't Display" fields.**

When "Don't Display" field masking is on, what is the value to be used in place of the actual value? The above example displays as **********

## 200) Maximum records to display when producing a report based on the Comprehensive Custom Report

Running a report with an excessively large number of records can adversely affect system performance for other users in extreme cases. This setting limits the maximum number of records that can be requested at a time to prevent this situation, by selecting only the first specified number of records. A suggested starting limit could be 100, but this could be adjusted based on actual test results. A value of 0 disables limits.

## 210) Use custom filters for reports

This global setting has a number of benefits that may be of use to you that are related to the standard and advanced filtering options available in standard reports:

- Ensures values to be selected are consistent between standard and advanced filters if they're not already.
- Will not allow values to be displayed in code, it will display text only.

## 220) What is the maximum number of folder levels allowed in the My Reports / Report Library structure?

This setting controls how many levels of sub folders may be created in the Report Library and My Reports. Setting this to 1 means that users are able to create folders, but those folders cannot have sub folders created within them.

**Please Note:** Changing this setting to a value lower than the current value can result in inconsistent behaviour in the system as well as potential loss of data. Please contact RiskMan support if you want to change this value to one lower than what is currently set.

## 230) Maximum size of data to apply to a report between specified times, in K.

Running an extremely large report can impact server performance for other users. To mitigate this, this setting can be configured to limit the size of the data loaded into a report. The data volume, rather than record count, is considered the best measurable value to use since a simple report with a large number of records may produce with no issues.

This restriction will apply to both normally produced and scheduled reports, as they both contribute to the issue. If the report includes related tables with multiple data sources, all will be considered. The period of time to limit the size of the report is specified in other Global Settings. A value of 0 (zero) will disable this functionality. Size is in k Bytes, i.e. 1000 characters.

**240) Start time for limiting maximum size of Data to apply to a Report.**

Start time for limiting maximum size of Data to apply to a Report. Please specify as HH:mm recorded in 24-hour format, for example, 9:00 for 9AM, 16:00 for 4pm. Running an extremely large report can impact server performance for other users. To mitigate this, there is a setting that can be configured to limit the size of the data loaded into a report. An invalid value will imply a value of "9:00"

**250) End time for limiting maximum size of Data to apply to a Report.**

End time for limiting maximum size of Data to apply to a Report. Please specify as HH:mm recorded in 24-hour format, for example, 9:00 for 9AM, 16:00 for 4pm. Running an extremely large report can impact server performance for other users. To mitigate this, there is a setting that can be configured to limit the size of the data loaded into a report. An invalid value will imply a value of "18:00"

**260) Allow deleting of a report layout**

If Yes, then users will be able to delete report layouts

**260) Show preview page for Workbook Reports?**

Note: The preview page can only work when RiskMan is set up in a non-Load Balancing environment

**270) Include disabled classifications on the aggregate reports classifications filter**

Include disabled classifications on the aggregate reports classifications filter.

# SCHEDULED JOBS

The settings in the **Scheduled Jobs** group allow you to nominate the tasks (that you wish to have enabled and at what frequency ie. Emails, Process Alerts (created from the Alert Management page), Journal Alerts if those jobs are enabled, and the Likelihood Threshold checking for risks in your Risk Register

**10) Enable Email Delivery**

Enabling this setting allows RiskMan to send emails to users.

If the settings **20) Enable Alert Processing** and **30) Enable Journal Alert Sending** are also checked, email notifications will be sent for these types of alerts.

The dispatch frequency for emails can be specified in the setting **50) Email Delivery process start frequency (minutes)**.

**20) Enable Alert processing**

By enabling this setting, processing of User Defined Alerts (UDAs) will become operational. For email notifications to be sent for Alerts, the setting **10) Enable Email Delivery** must also be enabled.

The processing frequency for Alerts can be specified in the setting **60) Alert Processing process start frequency (minutes)**.

**25) Enable Alert Version 2 processing**

When enabled, processing of User Defined Alerts (UDA's) in the Version 2 functionality will be operational. For email notifications to be sent for Alerts, the setting "Enable Email Delivery" must also be enabled. The frequency for processing alerts is based on the schedule for each alert.

**30) Enable Journal Alert sending**

In most Registers, a user can allocate a Journal to another RiskMan user to action. By enabling this setting, processing of Journal Alerts will be operational.

For email notifications to be sent for Journal Alerts, the setting **10) Enable Email Delivery** must also be enabled.

Global Settings Descriptions

The processing frequency for Journal Alerts can be specified in the setting **70) Journal Alert Processing process start frequency (minutes)**.

This setting can be turned off in favour of manually configuring your own Journal alerts for each register in your system.

**50) Email Delivery process start frequency (minutes)**

Specifies how often RiskMan should check to see if there are any new emails waiting to be sent to users. Relates to the setting *10) Enable Email Delivery*.

**60) Alert Processing process start frequency (minutes)**

Specifies how often RiskMan should process, or 'run' your User Defined Alerts. Relates to the setting *20) Enable Alert processing*.

**70) Journal Alert Processing process start frequency (minutes)**

Specifies how often RiskMan should process, or 'run' your User Defined Journal Alerts. Relates to the setting *30) Enable Journal Alert sending.*

**80) Enable File Path Monitoring**

This setting is used to activate the data import process within RiskMan. It is used in conjunction with the administration list **File Path Monitoring Jobs**. Contact RiskMan Support if you need to use this process.

**90) Address to notify for scheduled report failures**

This allows you send an e-mail to a certain person in case a scheduled report job fails. The purpose of this is to allow an administrator to know of potential issues with the scheduler utility. The system will generate an e-mail and send it to the address entered in this setting.

**100) Email delivery check frequency (seconds).**

When a value other than 0 is specified, whilst the email sending process is running, after the specified number of seconds, the global setting for "Enable Email Delivery" will be checked to see if it is still enabled or not. Therefore, if email sending is disabled in the middle of the email sending process, it will stop sending out all the emails, where previously disabling the email delivery would only take affect from the next time the email sending process was due to start.

**110) Maximum age (days) of Error Log entries**

When RiskMan encounters an unexpected error, information regarding the error is logged for use in resolving the issue. Some errors have no practical effect on the operation of RiskMan, but come can be critical to its operation.

The Logs are the best resource available for resolving issues in RiskMan but are increasingly less useful as they age. After an upgrade existing error logs would contain very little value as the situation has changed. Some causes of error logs being produced can generate many errors because they are regularly repeated, for example Alerts.

Because of this, this setting is available to limit the age of Error Logs stored by RiskMan to save space in the database.

Configure this setting to the number of days you wish to preserve the Error Logs. If you set a value of 0, Error Logs will never be deleted. If setting a non-zero value, RiskMan would not recommend a value less than, say, 30. Should you have cause to contact RiskMan support, recent logs may be needed to help resolve the issue.

When your staff utilise the **Send error to RiskMan** from the pink error screen (head banger), much of the information contained in that error log is sent to RiskMan and we preserve that data.

*Note: after the elapsed period, the Error Logs are deleted and are not recoverable.*

**120) Maximum age (days) of Audit Log entries**

Audit Logs are stored in the database and preserve information regarding certain events. Generally, the events that will be logged are based on the settings configured in the list "Audit Log Settings". Some events, like a change to a Global Setting such as this one, are always logged.

However, Audit Logs do take space in the database. If it is decided that Audit Logs are not required after a period, you may set a preservation period for Audit Logs, in days.

Configure this setting to the number of days you wish to preserve the Audit Logs, with as value of 0 meaning they will never be deleted. All types of Audit Log will be deleted. It is recommended the preservation period be quite long, or 0.

*Note: after the elapsed period, the Audit Logs are deleted and are not recoverable.*

# SCHEDULER SERVICE

## Scheduler Service Server Settings

**10) Name of the scheduler instance.**

Name of this scheduler. Any change will require a Scheduler Service restart.

**20) Port that the scheduler will use to receive requests.**

Port that the scheduler will user to receive requests. Any change will require a Scheduler Service restart and a change to the port in the client configuration.

**30) Number of worker threads in the service pool.**

Number of threads allocated to service jobs. Any change will require a Scheduler Service restart.

**40) Is this Scheduler Service part of a scheduler cluster?**

Is this Scheduler Service part of a scheduler cluster? This should only be changed in consultation with RiskMan support. Any change will require a Scheduler Service restart for all the schedulers in the cluster. Never run clustering on separate machines, unless their clocks are synchronized using some form of time-sync service (daemon) that runs very regularly (the clocks must be within a second of each other).

**50) Misfire threshold**

The number of milliseconds the scheduler will tolerate a trigger to pass its next-fire-time by, before being considered misfired. Any change will require a Scheduler Service restart.

**60) Enable Scheduler Service for ALL jobs?**

This is effectively the on/off switch for the scheduler tool.

**60) Host or IP of the scheduler server.**

This value should be the host name or IP address of the server running the scheduler service. If this value is changed, the RiskMan application pool should be restarted.

# Scheduled Report Settings

**10) Notify register administrator if there is a failure in the running of a scheduled report?**

If a particular scheduled job fails, send a notification email to the user(s) designated as administrators for the register in question.

**20) Enable Scheduler Service for Scheduled Report Jobs?**

This is effectively the on/off switch for the scheduled report tool.

# SECURITY

**10) CSRF Security Token type**

This setting describes how to implement a security stategy intended to protect against a hacking method known as CSRF. This mean Cross Site Request Forgery, (sometimes called CSurf) and involves submitting a form from a remote computer maliciously. The options for this setting are:

- **None**: Functionality is disabled.
- **Session**: This implements a session based token method that should give minimal or no disruption in general use.
- **Page**: Implements a per page token mechanism which is the most secure, but may under some situations cause some disruption, e.g. with pages reloaded using the back button on the browser.

The token is implemented on critical state changing pages only.

**20) Page to redirect to after Log Out**

When using single sign on functionality, the "Log Out" function is required to both terminate the RiskMan session and log the user out of the single sign on. Pointing the "Log Out" menu item at "TerminateSession.aspx" will explicitly end the RiskMan session, and then, if this field is non-blank, redirect to specified page. The specified page is expected to be the single sign on logout page, but could just be, for example, the corporate home page.

# SYSTEM VALUES

**10) RiskMan Major Version**

Your system's version number. This number is broken down into year, month, and patch version. Therefore, the Major Version number of 120604 can be interpreted as 20<u>12</u> (year), June (month – 06), and Patch <u>04</u>.

**20) RiskMan Minor Version**

Your system's version number, using the original numbering standard.

**30) Site ID**

A unique identification number assigned to every individual RiskMan system.

**40) Web Server Temporary File Folder**

Specifies the folder on the Web Server used when a temporary file is required, usually for reports. It must be a local folder on the web server, not UNC, and must terminate in a backslash (\). Default is "C:\Temp\"

**50) Internal Application Version**

**60) RiskMan Scheduler Version**

**70) Internet Explorer Document Mode**

The ability to alter the Internet Explorer "Document Mode" setting within RiskMan has been deprecated. The system will now automatically be configured to run under "Standards" based code, in Internet Explorer this is known as "Edge". This should give the most reliable and consistent code platform, and all pages have been recoded to expect this mode. Custom pages specific to your site may have been built expecting older browsers, and may need to be updated. Please contact RiskMan support.

**80) Inbox Page Name**

This setting which system page should be used for the "Inbox", and should only be changed in consultation with RiskMan.

# USERS

## Authentication

**10) RiskMan User Authentication Method**

This setting is used to configure RiskMan to use organisational Network Login accounts. It is defaulted to "Standard".

We strongly recommend that this item only be changed in consultation with RiskMan support. Methods other than 'Standard' req uire additional configuration.

- **Standard**: RiskMan maintains its own authentication database of usernames and passwords
- **LDAP**: RiskMan authenticates against an LDAP source. RiskMan maintains no passwords. Users log in using the standard username/password boxes on the RiskMan form, but the username and password is checked against LDAP. To use this method please contact RiskMan Support.
- **SAML2**: A standard that most importantly addresses web browser single sign-on (SSO). To use this authentication method, please contact RiskMan Support.
- **ADFS**: ADFS is an acronym used to describe the Actie Directory Federation Services (ADFS).  ADFS is an identity access solution that provides client computers (internal or external to your network) with seamless Single-Sign-On implementation (SSO) access. To use this authentication method, please contact RiskMan Support.

**LDAP AND SAML2 DETAILS**

**Caution**

*These settings must only be modified with the assistance of RiskMan Support. Incorrectly modifying settings in this group may prevent users from logging in to the system at all.*

1. *For assistance with these settings please contact RiskMan support via the following:*

    - *By phone: Call the helpdesk directly on **+61 3 9686 0009***

    - *By email: Send your queries, along with other helpful materials to https://hub.rldatix.com/SupportHUB/s/  Please note you may need to request an*

*account to access this service. If an account is needed, then please go to **[HUB: Sign In (rldatix.com)](#)** and click on Request an account at the foot of the login box.*

# LDAP Details

**20) Self-creation Username validation Regular Expression**

This item may be left blank, in which case the Usernames are completely free form. Under LDAP, the username is drawn from the LDAP login and this does not apply.

**40) Directory Path**

This describes to RiskMan how to access the LDAP server. The value will be dependent on your organizations LDAP server configuration. Typically, it will contain the server name, either by itself or fully qualified, but may take a number of different formats:

- Ldapserver, or
- ldapserver.yourdomain.org.au, or
- An IP address, e.g.: 10.10.1.1, or
- In some environments, if it is a domain controller: LDAP://ldapserver.mydomain.org.au/dc=mydomain,dc=org,dc=au,or
- If 'ldapserver' is not a domain controller, more simply as: LDAP://dc=mydomain,dc=org,dc=au

*Note: The 'LDAP://' prefix may not be required.*

**50) Directory Port.(Default=389)**

The port used to access the LDAP server. The default port is 389.

**60) Connect using Secure Sockets Layer**

**70) When using LDAP over SSL, does the certificate need to be imported to the local MONO certificate store?**

When No, RiskMan will accept any SSL certificate. When Yes, RiskMan will only accept certificates that are in the local MONO Certificate store. This requires installation of the MONO RunTime and manual importation of the LDAP SSL certificate (using the RiskMan tool).

## 80) Administrative user capable of retrieving user lists

This specifies an LDAP account that has permission to retrieve the details of other LDAP accounts from the LDAP server. For many systems this can be left blank as it is common to allow an anonymous user to retrieve sufficient detail. If an account is needed, it is recommended that an appropriate LDAP user be created especially with minimal permissions and a non-expiring password. The account can be read-only as updates are NOT made back to the LDAP server. For security reasons, we strongly recommend NOT using an account like 'Administrator', though it will work.

## 90) Password for the above account

Password for the account specified in '80) Administrative user capable of retrieving user lists.', if required.

## 100) User list search pattern

An LDAP query to specify the list of users that can potentially login. The "" part will be replaced by the username that the user has typed in, and this query should only return potential accounts that match exactly. Each account found (potentially multiple accounts) will then be tested against the password typed in to authenticate the login. The syntax depends on the specific LDAP implementation. Ideally, the query should efficiently limit the search for possible logins to only users appropriate for RiskMan.  A recommended starting query for Active Directory that will leave out system accounts and deleted users, though this can be modified if appropriate: (&(objectClass=person)(sAMAccountName=)(&(userAccountControl:1.2.840.113556.1.4.803:=512)(!(userAccountControl:1.2.840.113556.1.4.803:=2))))

## 110) User list search pattern, for Admin searches

This is an LDAP query used for RiskMan administrators to search for users. This can be more relaxed than the login query to make it easy to find an appropriate user. For example, it is common to do an automatic wildcard match on name as well as login. If we are looking for a user, 'Andrew Martin' who has a username of 'andrewm', for the the login query ("100) User list search pattern."), the account could only be found when 'andrewm' is used in the search.  To make searching easier on administrative pages, this query could return that account (and possibly others) when searching for 'Andrew', 'Martin', 'andrewm', or even 'And'. A List of found users would be presented to allow selection of the correct one. A recommended query for Active Directory that will leave out system accounts and deleted users and automatically search name as well using wildcards (*), though it may be appropriate to modify this:

(&(objectClass=person)(|(sAMAccountName=)(displayName=\*\*))(&(userAccountControl:1.2.840.11 3556.1.4.803:=512)(!(userAccountControl:1.2.840.113556.1.4.803:=2))))

If this field is left blank, then the "100) User list search pattern." query will be used for searching. That would mean you would only be able to search for the login field, though the star (\*) can be used as a wild card. You could find the above example account by typeing "And\*". When logging in, wildcards are filtered out.

**120) User list search base**

Specifies the directory search base; the place in the LDAP structure to begin the search. For efficiency of searching the LDAP directory, it is good practice to target the highest-level container that holds all the user records, but if required this can encompass the entire directory. The location is likely to be different for each installation, but a typical example would be: CN=Users,DC=yourdomain,DC=com,DC=au

**130) The property to get the Email address from**

**140) The property to get the Alternate Email address from**

**150) The property to get the Display Name from**

If the DisplayName is left empty, but Firstname and Lastname have values, then the name parts will be retrieved separately and combined as per the Global Setting.

**160) The property to get the First Name from**

**170) The property to get the Last Name from**

**180) The property to get the Phone Number from**

**190) The property to get the Mobile number from**

**195) The property to get the User Position from**

If this global setting has a property, when a new user is created then their User Position will be sourced from this property in LDAP or if utilised SAML

If the property to get the User Position from" has a parameter defined, if the Create Login Page is displayed to users (ie it is not bypassed), then the "User Position" field will no longer be visible as this information is retrieved from LDAP or SAML

If the Global Settings are also set to enabled for "Users | User Control | 150) Update user details whenever a user logs in", in the User Profiles this field will now be set to Read Only so that it can only be updated via the information provided from LDAP

**200) The RiskMan Template to use when self-creating new users**

**210) The LDAP property containing the RiskMan Template to use for an individual when creating new users**

**220) The property to use as the RiskMan account username when creating new users**

What property to use as an identifying value for a specific user. Commonly in Active Directory systems this would be 'sAMAccountName'. Other options could include 'CN' which is usually the users name, or 'mail' where the user logs in using their email address. This setting needs to correspond to the queries in 'LDAP Details/100) User list search pattern.' and 'LDAP Details/110) User list search pattern, for Admin searches.'.
*WARNING:* Changing this property once user accounts are configured may require relinking all existing accounts.

**230) Enable use of Multiple LDAP services**

In a Multi LDAP environment, the service listed on this page will be the default (top listed) selection. Configuration of the other sets is via List Management.

**235) Search Multiple LDAP services to login**

When RiskMan is configured as a Multi LDAP environment, search the defined LDAP services one after another when attempting login. The user does not need to specify which service they are a member of.
*WARNING:* Unless your organization is confident that LDAP usernames are unique across all services, this setting is not recommended.

**240) The name of this LDAP service in a Multi LDAP environment**

**250) Allow standard users as well as LDAP users**
When enable, users with appropriate permissions will be able to create User Profiles using either LDAP or RiskMan 'Standard' accounts.

**260) When 'Allow users to create their own Login' (a user permission) is enabled, permit creation of standard RiskMan accounts as well as LDAP**

**270) Allow Login based on just the defined LDAP account (see item 220) rather than using the full DN**

**280) Automatically Login a user, detecting their account**

# SAML Details

**10) When using SAML, store SAML session in the Database**
When using SAML, a SAML session is created to record the current state. Normally, this session is created in memory on the web server. This is an issue if the site uses a web farm (multiple webservers) since the session is only recorded on one web server. If logging out happens to occur on the other server, the logout will fail.

To resolve this, set this setting to YES and the session will be recorded in the database. The SAML session is then shared across all servers and preserved correctly.

**20) SAML signout upon RiskMan session timeout**

When using SAML, a SAML session is created to record the current state. Normally, this session is created in memory on the web server. This is an issue if the site uses a web farm (multiple webservers), as the session is only recorded on one web server. If logging out happens to occur on the other server, the logout will fail. To resolve this, set this setting to **YES** and the session will be recorded in the database. The SAML session is then shared across all servers and preserved correctly.

**30) Allow editing of SAML link values on the User Profile page**

RiskMan administrators to have the ability to modify the SAML Username and SAML Unique Identifier. Once the global setting has been enabled, users will now have an "Enable SAML Link Edit" button to the right of the SAML account fields, and upon clicking this button the fields will become editable.
The additional step of needing to click the button as well as having the global setting enabled is to ensure that users consciously decide to modify these details to ensure that there are no accidental changes made to these which can be difficult to reverse
*NOTE:  SAML account links may be technical and are usually not known by RiskMan administrators, therefore this option will be left as the default value of No in most client environments*

# Password Management

**10) Password change/create validation Regular Expression.**

This item may be left blank, in which case the Password is completely free form. This is separate from the Password Strength rules (items 30 - 80 below). RiskMan recommends using the Password Strength rules below instead, as it is much easier to manage. When using LDAP, the passwords are controlled by the LDAP server and this item does not apply.

**20) How often must users change their password in days?**

When enabled (greater than zero), users that are not linked to an LDAP account will be required to change their password after the specified period. Please Note that all users Passwords are considered to have been changed on the day the update that implemented this feature was installed, which was 08 Apr 2014

**25) Only allow one password change per day**

When enabled, users will only be able to change their passwords once per day. This prevents users, when forced to change their password, from immediately changing it back.

**30) Require that user-created passwords meet the below strength tests?**

When a user creates a password for their account, they will be notified of the approximate password strength of the text they are entering. If this setting is on, they will not be allowed to save unless the password meets ALL of the requirements specified below. If this setting is OFF then the password strength will still show, but compliance is not mandatory.

**Note**

*Users that are linked to an LDAP account cannot change passwords in RiskMan.*

**40) What is the minimum length of the password?**

Minimum length of a password for a standard RiskMan account.

**50) What is the maximum length of the password?**

Maximum length of a password for a standard RiskMan account.

**60) What is the minimum number of numeral characters?**

The minimum number of Numeral characters required in a password for a standard RiskMan account.

**70) What is the minimum number of Upper Case characters?**

The minimum number of upper case characters required in a password for a standard RiskMan account.

**80) What is the minimum number of special characters?**

The minimum number of special characters required in a password for a standard RiskMan account.

**90) What special characters are acceptable in passwords?**

The special characters are acceptable in a password for a standard RiskMan account.

**95) Enforce new users to change password on first login**

When enabled, this will tick the 'Force Change Password' checkbox on the User Profiles page when a new user is created. On a per-user basis, a system administrator can untick this option in a user's profile if they do not wish to enforce the change password rule.

# User Control

**5) Auto Create User from login prompt.**

When LDAP is enabled and a user enters valid LDAP (NetWork) credentials at the logon prompt, automatically create a Default user if none exists. NOTE: The account will only contain details retrieved from LDAP, user will not be given an opportunity to enter additional information at this point.

**10) Allow users to create their own Login.**

This setting permits unregistered users to create their own system login without administrator intervention. When a user creates their own user login, they are allocated the permissions to RiskMan defined by the "Default" user template eg. Access to Incident and/or Feedback Entry

**20) Prevent the Username being modified on user creation**

When enabled, this global setting will prevent any modification of a username provided by LDAP/SAML so that it is not automatically created with a number incremented if the username already exists in RiskMan.  For example, if RiskMan already contains a user with a username of jsmith, if a new LDAP/SAML user tries logging in (with different credentials) where they have a username of jsmith they will be unable to login, whereas previously they would be created in RiskMan with a username of jsmith1

This prevents creation of a new account when there is a possible mismatch in the login credentials, and a RiskMan administrator would need to then check the existing user account to confirm if it is the same user and then relink to the new LDAP/SAML account, or if it is a different user to create a new RiskMan account setting the RiskMan username manually to have a number on the end

**30) When users create their own Login, save the User Display Name as:**

Select whether the user's display name is displayed as First Name, Last Name or Last Name, First Name. This is visible in all areas where the user's name and login are visible eg. User Profiles, Review History, Distribution Lists

**40) When users create their own Login, allow them to specify Site Restrictions.**

Enable this setting if users are allowed to select the Site(s) where they are working when they first create their login.

By selecting a Site or Sites, the user is restricted to only view the selected Sites in all aspects of RiskMan eg. Incident and Feedback Entry forms, Risk Register, Incident and Feedback reports

**50) When users create their own Login, allow them to specify Location Restrictions.**

Enable this setting if users are allowed to select the Locations where they are working when they first create their login

By selecting a Location or Locations, the user is restricted to only view the selected Locations in all aspects of RiskMan eg. Incident and Feedback Entry forms, Risk Register, Incident and Feedback reports

**60) When users create their own Login, make it mandatory to specify Site Restrictions.**

If users are able to specify the Sites(s) where they are working, on creation of their login, enable this setting if the Site selection is to be mandatory

**70) When users create their own Login, make it mandatory to specify Location Restrictions.**

If users are able to specify the Location(s) where they are working, on creation of their login, check this setting if the Location selection is to be mandatory

**80) Allow users to change their password. (RiskMan 'Standard' accounts only.)**

This setting permits registered users to alter their own system password without administrator intervention. This is achieved using the menu option *My Workspace > My Details*.

**Note**

*This setting should not be turned on if Network Logins are used in your system as the password will be controlled by your Network*

**90) Prevent users from changing their Manager on a new Item Entry form (if changing Managers is permitted).**

If this setting is enabled (and a user has the user permission: "Can edit own line managers"), when a user enters a new item, they are unable to change the manager they report to. If disabled, a button is displayed at the bottom of an item entry form labelled "Change the people you report to". This allows the user to change their line manager whenever they save a new record.

Users will still have permission to edit the manager they report to through the *My Workspace > Edit My Managers* menu option

Disabling this setting can be useful when you have staff that work different shifts or across different sites.

**100) Allow Users to recover their own password by email. (RiskMan 'Standard' accounts only)**

When this setting is enabled a **Forgotten Password** button will appear under the Login section on
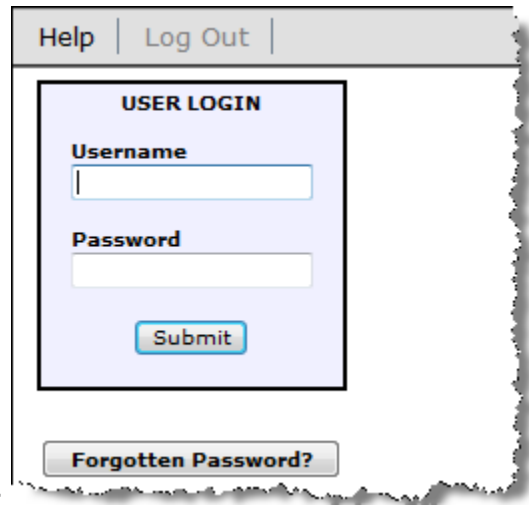


the Login page, prior to users logging onto RiskMan:

By turning this option on, a user will have the ability to enter either their user name or email address (as recorded in their user profile) into the Password Recovery page. Provided that the user has a unique user name and email address, they will be forwarded an email providing them with their password.

An email can also be sent to the Risk Manager *(email that is entered under the Global Settings group Mail > Mail Configuration > 10) Risk Manager's Email Address)* informing them that a user (their name is provided) has requested their password. The Risk Manager will not be provided with the password details. This will be dependent on the setting *Mail > Mail Configuration > 80) Send Email notification to the Risk Manager when a user retrieves their password.*

If a user does not have an email address or a unique username or email address, then they will be informed that they will need to contact the Risk Manager. In this case, the Risk Manager or Administrator will have to re-assign the user a password in their user profile. The user can then change their password once they have logged on using the menu option *My Workspace > My Details*

**Note**

*If Network logins are used, either this option should be turned off as the passwords will not be recoverable for users with network accounts, or leave this option turned on but inform users that if*

*they are using a Network logon they will not be able to use this feature (but those with non-network accounts will)*

**110) Allow users to edit their own Site. (Not Recommended)**

If this setting is enabled, and the setting *Users > User Control > 120) Allow users to edit their own personal details* is also checked, then the user permission "Can change own site" *(to allow users to change their Entry/Update Site restrictions)* will be visible under the **My Details** user permissions in the General User Profiles and Templates

**Recommended**

*This setting should only be used in isolated circumstances. Contact RiskMan Support for assistance if you believe you might want to use this setting.*

**120) Allow users to edit their own personal details.**

If this setting is enabled, then the **My Details** user permissions in the General User Profiles and Templates will become visible, allowing the RiskMan Administrator to set permissions as to which parts of a user's personal details (eg. display name, contact number, email address, position, site) can be modified by the user – *refer to the User Management Guide for more information*

**130) Enable viewing of users across all departments.**

Allow users to see users from all Sites on the **Assign Your Managers** page.

**140) Maximum number of successive failed login attempts allowed.**

This setting can be used to define the maximum number of successive failed login attempts allowed before the user gets locked out. Set this to 'Disable' to prevent user lock out altogether. Once a user completes the number of attempts defined in the setting, they will be locked out for a period of 30 minutes. After 30 minutes, the user will once again have the defined number of login attempts. If this Global Setting is set to 'Disable', the user lock out feature will be switched off, and users will have unlimited failed login attempts.

**150) Update user details whenever a user logs in**

When **yes** is selected, a user will login to RiskMan, their details will be retrieved from the LDAP server and their RiskMan user profile will be updated. Provided the fields are configured in LDAP, updates will be made to User Display Name, Email Address, Phone number, Mobile Number and position. When this setting is yes, these fields will be read only in the User Profile page (for LDAP accounts) since changes made manually would be ineffective as they would be overwritten.

To have an LDAP environment return the User Position to populate the field in the User Profile, the following global setting will need to be updated with the appropriate LDAP property: Users | Authentication | LDAP Details | 195) The property to get the User Position from.

**160) Allow the "New User' buttons to be seen in administrative pages (User Profile)**

This global setting will hide the New User button on the User Profiles page to prevent users from manually adding User Profiles. It may be appropriate when alternative methods for User Profile creation are being used.

When this is set to No, the New User button will be removed from the User Profile page.



When this is set to Yes, the New User button will be visible in the User Profile page