- Alert Management -

FOR RISKMAN VERSION 2010

Last reviewed November 2020

CONTENTS

WHAT DO ALERTS DO?

Alerts are the backbone of your system – they orchestrate all the workflows that you require RiskMan to perform. This includes things like sending records to the right people at the right time; tracking due dates and sending reminders, and much more.

➜ How to access Alerts

You can access Alerts by navigating to *Administration > Alerts.* This will take you to your list of previously configured alerts. To create a new alert, select the target register (eg. Incidents, Risk) and click on the ➕ icon.

DETAILED OVERVIEW

Before we even get into the nitty-gritty, there is one point to make clear: **Alerts are not emails!**

On their most basic platform, the Alerts system is designed to grant users permission to certain records, based on the criteria you specify. Whether or not an email is sent when an alert is triggered is an *option* for an alert.

Having said that, we tend to talk about Alerts having 6 main purposes. Here we go.

Alert Type: To notify a user that a certain type of record has been entered

The most obvious use of Alerts is to make sure people who need to know are in the know. These alerts inform users that there is a record in the system that needs their attention. For example:

- Notify the CEO when a major or extreme incident is recorded
- Notify the relevant Department Manager when a complaint issue is raised regarding their department
- Notify a user when a control is assigned to them in a Risk

There is an extension to this type, in which, instead of notifying a user to each individual record, instead a Digest can be sent. More on that later.

Alert Type: Restrict what a user can see when they open a Register

Example: You have two users who are responsible for posting Incidents; the WHS Manager and the Director of Nursing. When each of these users opens the Inbox, they can see all of the Incidents from their facility. Each user requests that they not see the other's Incidents; they'd rather only see their own.

If you grant a user permission to see the Incident Inbox, they will see <u>all</u> the records which match their User Profile Site/Location restrictions *(this applies to all Registers as a general rule)*. Sometimes, this is not enough. This is where alerts can be used to control what a user can see.

The solution is to **create an Alert** for each of those users. The Alert for the DON will trigger for clinical incidents. The Alert for the WHS Manager will trigger for everything except clinical incidents, for the sake of the example.

The next step is to change each person's **Site/Location settings** in their respective **User Profile**:

Tick on **Show only "Alerted" Incident items in Inbox**. Now, each user will only see the incidents that concern them when they open the Inbox.

ⓘ **Note**

You can also use this method for restricting a user's reporting capabilities.

Alert Type: Remind a user that something is due soon, or is now overdue

Alerts can be used to track all kinds of time-based scenarios, and remind people when you want them reminded.

Some hypothetical examples include:

- Complaints in the Feedback register need to be closed within 30 days. If, 25 days after initial entry, a complaint has not been marked as 'Closed', send a reminder to the personal responsible to let them know the deadline is approaching.
- Company policy dictates that all incidents must have investigations at least started no more than 7 days after we were made aware of it. If, after that 7th day, there are still no investigations entered, send a reminder email to the responsible manager every 3 days until they actually do it.
- Remind the person responsible for the review of a Control in the Risk Register that they have not yet performed that review, and the due date for the review has now passed.

...and so on. Remember, reminder alerts are always based on a date field from the Register in question. You need to define three questions before you create a reminder alert:

- What specific situation are you reminding somebody about?
- When should you start reminding them, and
- Once you've started reminding them, how often do you want them to be reminded until they complete the action?

You can then go and create your alert.

Alert Type: Acknowledging that something has been completed

The system can generate acknowledgement emails automatically, based on the criteria you specify. Examples include:

- When a user submits an incident, send them an acknowledgement email, which thanks them for entering it. The email may also describe what will happen next, as well as some instructions on what the user can do to monitor the progress of the incident.
- When an incident is marked as closed / investigations completed, send an acknowledgement email back to the original reporter to thank them for taking the time to enter it, and what happened as a result of them doing so (closing the loop!!).

- When a complaint in the Feedback Register is marked as closed, send an acknowledgement email to all the users who contributed to the resolution, thanking them for their effort
- When a quality activity is marked as being completed, send an acknowledgement email to the users who contributed which includes the initial results of the activity

Alert Type: Counting the number of occurrences of a certain event

A 'Threshold' alert can be setup to count the number of occurrences of a certain type of event; for example, staff manual handling injuries.

When the number of staff manual handling incidents surpasses the tolerable level that you set, within the timeframe that you stipulate, the nominated user(s) will be notified.

For example, if you have more than 4 manual handling incidents within a 30 day period.

Threshold alerts are essentially the same to setup as notification alerts, with the added information of your tolerance within the given time frame.

Alert Type: Pipeline Processes

Pipeline Processes allow you to create a new record in a different Register, or a new record in the current Register, when the conditions that you define are triggered. The simplest examples include:

- A user is entering an incident. If they answer 'Yes' to the question 'Have you identified a potential new risk?', a new record is created in the Risk Register. This new risk might contain some of the information from the incident that was just entered.
- A user is performing the follow up of a complaint. They answer "Yes" to the question "Will this result in a quality improvement activity?". This creates a new quality activity, ready to be followed up on.
- Entering an incident where an inpatient had passed away could trigger a new record in the Mortality Audit Register

There are many possibilities for using Pipeline Processes; talk to us about any ideas you have!

Alert Types – In Summary

Alerts will do the following for you:

- **Notify** users when certain things happen
- Restrict what a user can see when they open a Register
- Remind a user that something is due soon, or is overdue
- Acknowledge to a user that something has been done or completed
- Count the number of occurrences of a certain event
- Pipe information from one Register to another

Of course, this is a fairly high-level summary, and there are plenty of nuances and different configurations that we use every day. This guide explains the meaning behind all of the settings when configuring alerts. Please use this guide in conjunction with the **Alerts Example Supplement** document, which provides several examples of different types of alerts.

CREATING ALERTS

The Alerts list page

The Alerts list page displays all of the alerts in your system, including useful information such as the status of each alert, who created it and when, who last modified it and when, and so on.

❶ Select the relevant register that you want to create an alert for (incidents, feedback etc.)

❷ Click on the ⊞ icon in the toolbar to create a new alert

❸ Click on the blue **ID Number** to view and edit an individual alert

❹ Click this icon to delete an alert – this cannot be undone!

ⓘ **Note**

The Alerts list page is just like other listings pages, where you have the ability to group by columns, filter, use your Selection Settings and set your column widths.

Modifying alert properties without opening the alert

❶ Double click on a row to modify the name, description, and current status of an alert

❷ Click the tick icon to save your changes, or the cross icon to cancel

Introduction to the Alert Edit page

This is what alert page looks like. We'll just have a look at how the page is structured first:
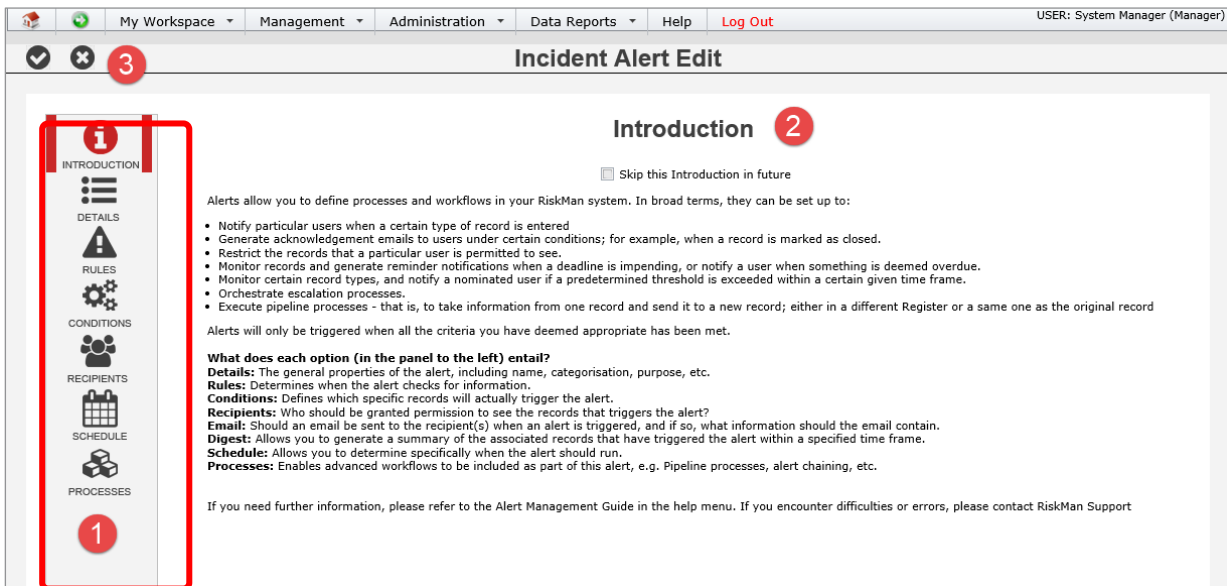
❶ Each of these **icons** represents a different group of settings for your alert. The icons displayed here will depend on the options that you choose during the setup of your alert.

❷ This is where the content and options for each group of settings appears. By default, you will land on the **Introduction** page when you create a new alert. There is some basic information on this page. If you no longer wish see the Introduction page when you create a new alert, check the box labelled **Skip this introduction in future** underneath the page heading.

❸ These are your **save** and **cancel** icons. Clicking either will result in you being taken back to the alerts list page.

Alert Details

❶ **Alert Name**: Give your alert a meaningful name. If you anticipate your system will have many alerts, it is advisable to come up with a standardised naming convention.

❷ **Purpose / Description**: Enter a meaningful description that clearly outlines the purpose of this alert. The more information you include, the better – as sometimes other users will be viewing alerts, and it should be easy for them to identify exactly what an alert does.

❸ **Alert Categorisation**: If you anticipate having a lot of alerts, the categorisation can help you sort your alerts more effectively. The folders that you see in this section are based on a list in list and codes maintenance (see below image)

❹ **Alert Status**: This is the on/off switch for the alert.

Alert Categorisation

You can modify the folders that appear in the Alert Categorisation section if you have permission to List & Codes Maintenance:
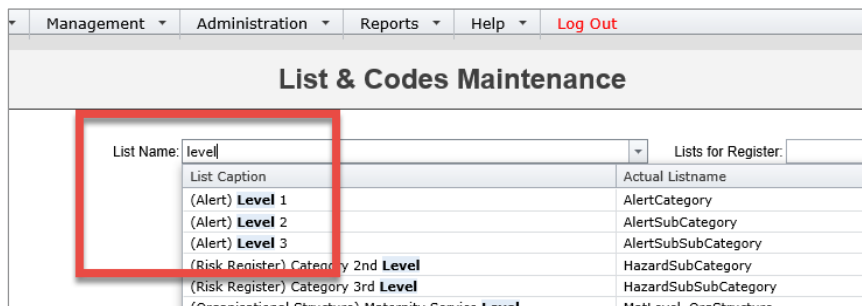
- Configuring these values will allow you categorise your alerts.
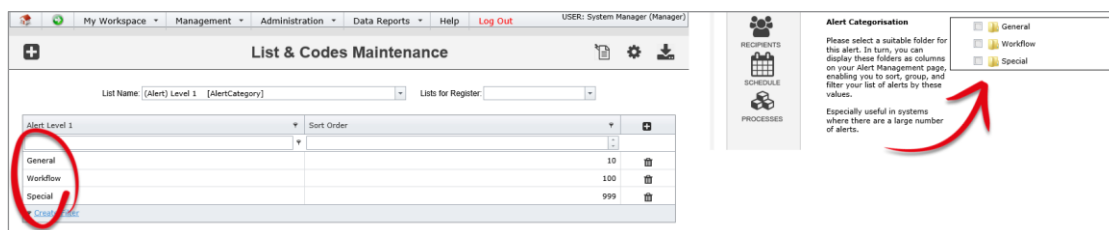
- You could then use your **Change Columns** function on the alerts list page to display these as columns in the list, meaning you can sort, group, and filter your alert by the values you have assigned:
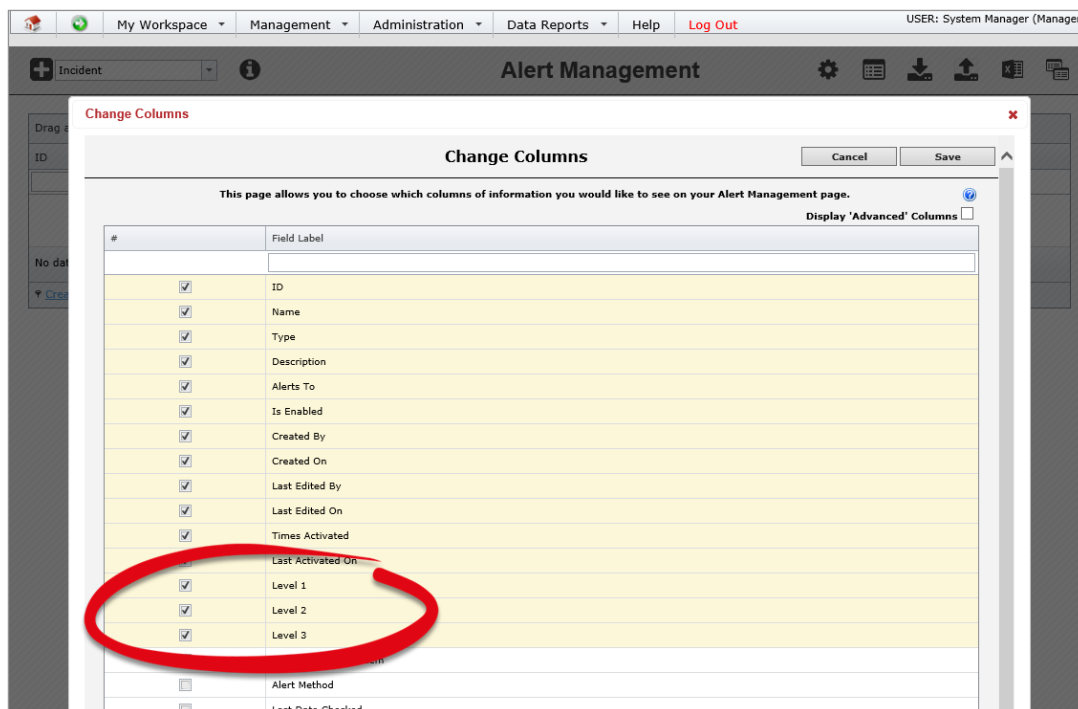
Alert Rules

The Rules page contains the 3 **Alert Methods❶**, and the various **Settings❷** that can be configured for each method:
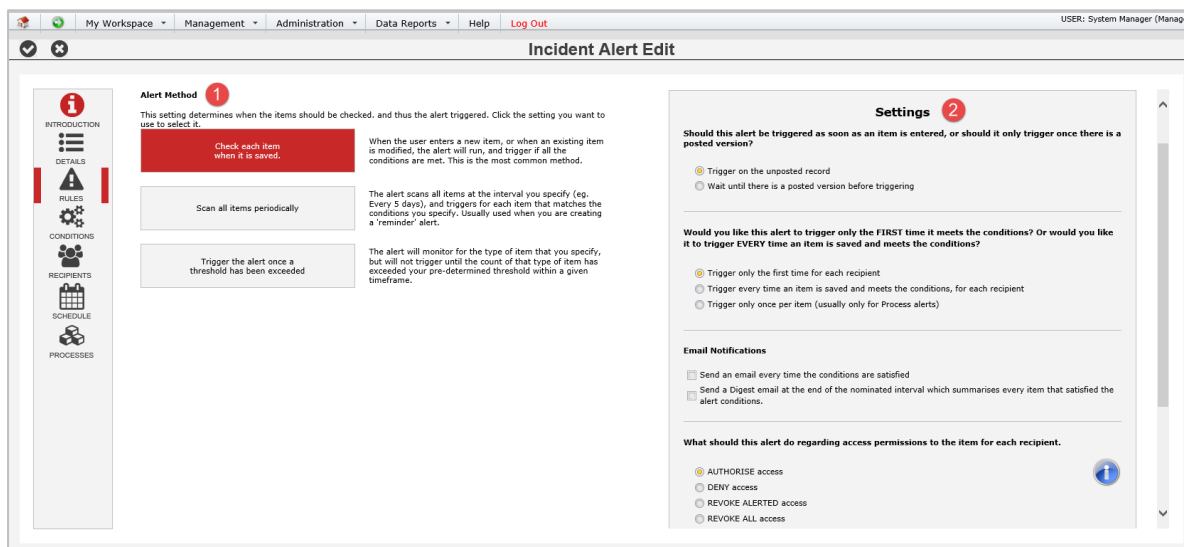
Alert Method	Explanation
Check each item when it is saved	When the user enters a new item, or when an existing item is modified, the alert will check each item, and trigger if all the conditions are met. This is the most common method.
Scan all items periodically	The alert scans all items at the interval you specify (e.g. Every 5 days), and triggers for each item that matches the conditions you specify. Usually used when you are creating a 'reminder' alert.
Trigger the alert once a threshold has been exceeded	The alert will monitor for the type of item that you specify, but will not trigger until the count of that type of item has exceeded your pre-determined threshold within a given timeframe.

Settings for each Alert Method

There is some overlap with the settings that are available for each alert method.

Settings displayed for **Check each item when it is saved**:

Only displayed if you are creating an alert for a register where Posting is used (i.e. Incidents, Feedback).

When using the alert method **Check each item when it is saved**, you would generally use the first option. If you used the second option, it means that every time the record is saved, if it still meets the conditions of your alert, another email will be sent to the recipient(s). This is usually an undesirable outcome.

Remember, not in every situation would you want an email to be sent when an alert is triggered. However, selecting either of these options will display its respective settings icon.

Alerts can authorise the recipient(s) access to see the record OR deny them access to see the record, depending on your desired outcome.
You can also elect to revoke alerted access or revoke ALL access to records.
Additionally, if you have denied access to someone in the past and want to over-ride this function, you can select 'remove deny access'.
If you do not want to assign any access permission to the recipient, select 'none'

If you wish to use an alert to retrospectively grant or deny the recipient(s) permission to see the matching records, you can enter the date to which you would like the system to go back to here.
There will be more information on this feature later in this guide.

Settings

Should this alert be triggered as soon as an item is entered, or should it only trigger once there is a posted version?

- ● Trigger on the unposted record
- ○ Wait until there is a posted version before triggering

Would you like this alert to trigger only the FIRST time it meets the conditions? Or would you like it to trigger EVERY time an item is saved and meets the conditions?

- ● Trigger only the first time for each recipient
- ○ Trigger every time an item is saved and meets the conditions, for each recipient
- ○ Trigger only once per item (usually only for Process alerts)

Email Notifications

- ☐ Send an email every time the conditions are satisfied
- ☐ Send a Digest email at the end of the nominated interval which summarises every item that satisfied the alert conditions.

What should this alert do regarding access permissions to the item for each recipient.

- ● AUTHORISE access
- ○ DENY access
- ○ REVOKE ALERTED access
- ○ REVOKE ALL access
- ○ Remove DENY access
- ○ NONE

Backdate

Use the Backdate function to apply your alert to past records. For further information please refer to the Alerts Guide.
Note: New alerts start from 'Now'. Backdate to pick up earlier records.
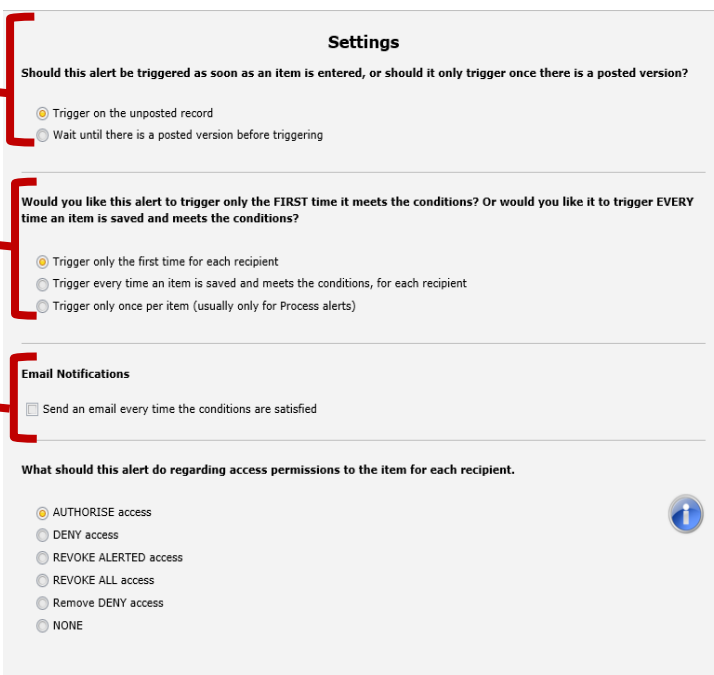Backdate to: [▼]

Alert Management

Settings displayed for **Scan all items periodically**:

Only displayed if you are creating an alert for a register where Posting is used (i.e. Incidents, Feedback).

Depending on the purpose of your alert, you would choose either of the first two options. Further explanation provided in the alert examples supplement.

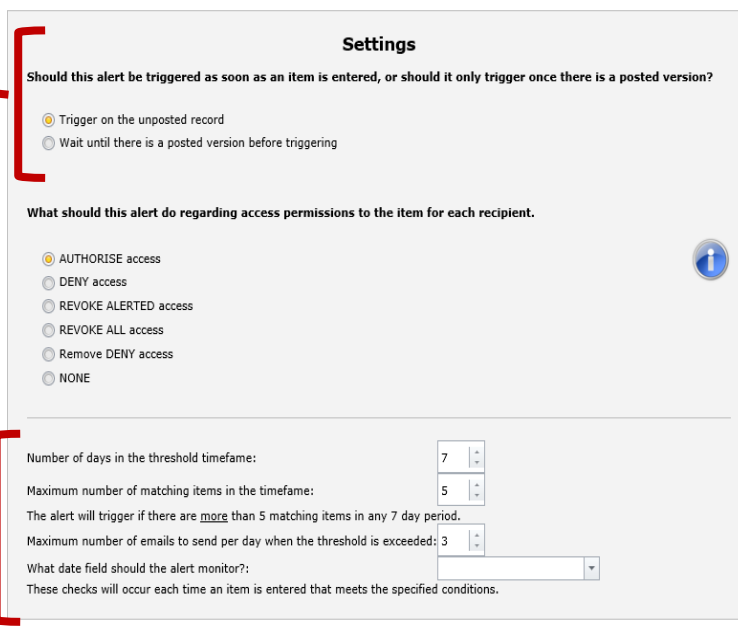Digest emails are not possible for this alert method.

Settings

Should this alert be triggered as soon as an item is entered, or should it only trigger once there is a posted version?

- Trigger on the unposted record
- Wait until there is a posted version before triggering

Would you like this alert to trigger only the FIRST time it meets the conditions? Or would you like it to trigger EVERY time an item is saved and meets the conditions?

- Trigger only the first time for each recipient
- Trigger every time an item is saved and meets the conditions, for each recipient
- Trigger only once per item (usually only for Process alerts)

Email Notifications

- Send an email every time the conditions are satisfied

What should this alert do regarding access permissions to the item for each recipient.

- AUTHORISE access
- DENY access
- REVOKE ALERTED access
- REVOKE ALL access
- Remove DENY access
- NONE

Settings displayed for **Trigger the alert once a threshold has been exceeded**:

Only displayed if you are creating an alert for a register where Posting is used (i.e. Incidents, Feedback).

Settings

Should this alert be triggered as soon as an item is entered, or should it only trigger once there is a posted version?

- Trigger on the unposted record
- Wait until there is a posted version before triggering

What should this alert do regarding access permissions to the item for each recipient.

- AUTHORISE access
- DENY access
- REVOKE ALERTED access
- REVOKE ALL access
- Remove DENY access
- NONE

This is where your threshold conditions can be stipulated.
See the alerts supplement for examples of different threshold alerts you might create.
Note that you always need to select which date from the form the alert needs to be based on.

Number of days in the threshold timefame:	7
Maximum number of matching items in the timefame:	5

The alert will trigger if there are _more_ than 5 matching items in any 7 day period.

Maximum number of emails to send per day when the threshold is exceeded:	3
What date field should the alert monitor?:	

These checks will occur each time an item is entered that meets the specified conditions.

Alert Conditions

This is where you will add the conditions required for your alert to trigger.

❶ **Conditions name**: Enter a name for the conditions you are building/have built, for example "All patient falls at Acacia Private". This information will be used elsewhere in the system in future.

❷ **Focus**: Choose whether the conditions you need come from the main form, or the main form and a sub form. More information on this in the alert examples supplement.

❸ **Fields**: These are all of the fields you can test, based on the choice you made in ❷. Start typing the name of a field to locate it.

❹ **Conditions**: Drag the field from ❸ to this grey 'drop zone', to configure the tests you want to perform.

❺ **Related filter**: Add additional filter criteria from another sub form. Usually only used in very complex alert conditions. See the alert example supplement for examples.

❻ **Test Conditions**: Click this button to test your conditions. The system will look at the register this alert is for, and tell you how many matching records already exist.

Creating alert conditions: The basics

For the purpose of explaining the basics of alert conditions, let's assume that the alert we are creating is to send all staff injuries to the WHS manager in the Incident register.

Alert Management

You must always carefully consider which information you need to have in place on the (incident) form that would make your alert trigger. We would recommend opening a blank incident entry form to assist identifying which fields will need to be tested. In the case of our example, we've decided we'll need to create conditions for two fields:

We want to test that the subject affected was a **Worker**, and that the level of harm sustained was **Injury/illness**.

We need to create a condition for each of those fields.

Adding conditions

Conditions work like this:
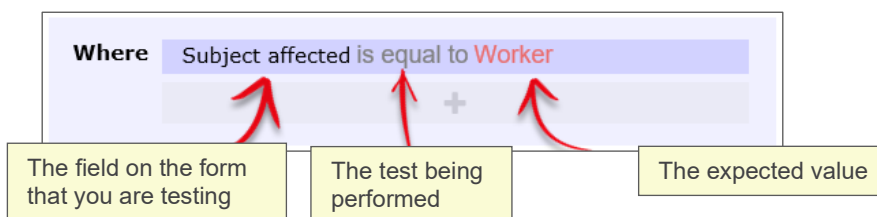
Once you have identified the name of the field you need to test, start typing that field name in the filter box. The list of fields will show the fields that match what you type.

Once you find the field you need, click and drag it to the **drop zone**:

Once you have the added the field in the drop zone, you need to select the type of test you need to perform:

Alert Management
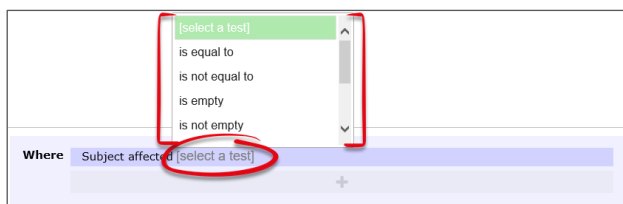
Then you need to select the value that you want for your test. Click **select an option**:
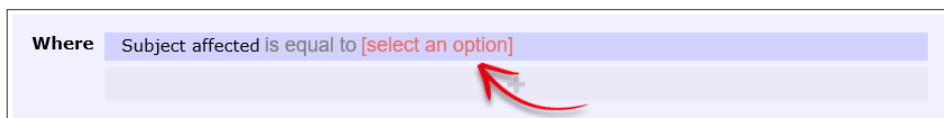
The values from the field you have select will appear. Choose the value you are testing for (**Worker** in our case):
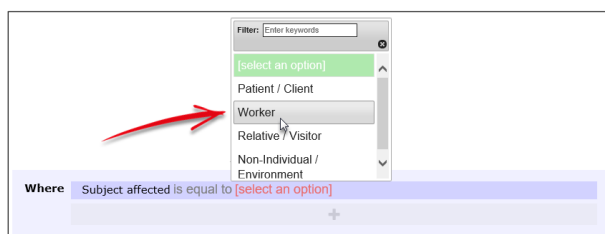
When trying to add a filter condition with a large list, you can start typing the value you want, and the system will display all the matching list values:
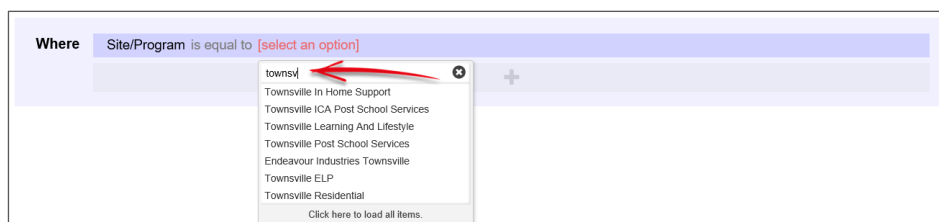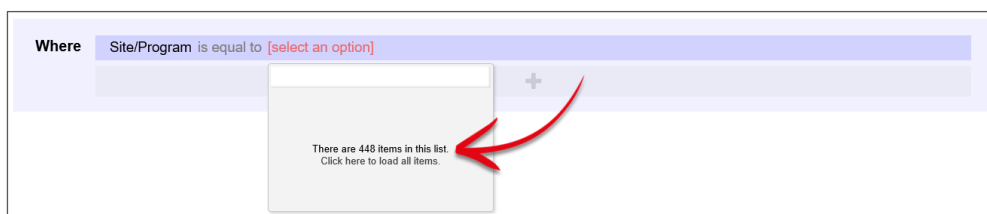
At any point, you can opt to click the **Click here to load all items** option. If you opt to retrieve all the values in a larger list, there might be a few seconds' delay. However, a "loading" icon will be displayed during that time, so that you know the request is being processed.

We then have to add our second condition. Follow the same process to find the field you need to test:

Note that for each subsequent field you add as a condition, there is a button at the start of each which contains **And** and **Or** (highlighted above). This allows you to stipulate whether both conditions need to be met for the alert to trigger, or if either of those conditions can make the alert trigger (click the button to change between And and Or).

So, for our example, the alert will only trigger if the subject affected was a **worker**, and the level of harm sustained was **Injury/Illness**.

What types of tests can be conducted?

Test name	Description
Is equal to	You want the stated value to be in this field
Is not equal to	You do not want the stated value to be in this field, but any other value is fine
Is empty	The field you are testing contains no data
Is not empty	The field you are testing does contain data
Contains the keyword	The field you are testing contains a keyword or particular string of text
Does not contain the keyword	The field you are testing does not contain a keyword or particular string of text
Is one of	More than one value being present in this field could satisfy this test
Is not one of	Any of these values not being present in this field could satisfy this test
Is less than	Can only be used on date, time, and numeric fields
Is greater than	Can only be used on date, time, and numeric fields
Is less than or equal to	Can only be used on date, time, and numeric fields
Is greater than or equal to	Can only be used on date, time, and numeric fields

Test examples

Is equal to	Incident Day Name is equal to Monday
Is not equal to	Specific location is not equal to Car park
Is empty	Closed on is empty

Is not empty	Date of birth is not empty
Contains the keyword	Action taken at time contains the keyword police
Does not contain the keyword	Occupation does not contain the keyword nurse
Is one of	Specific location is one of 4 selected Filter: Enter keywords ✓ Check all ✗ Uncheck all ☐ Meeting room ☑ Office ☑ Reception ☑ Shared/public toilet ☑ Staff lunch room ☐ Other
Is not one of	Incident Day Name is not one of 2 selected Filter: Enter keywords ✓ Check all ✗ Uncheck all ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☑ Saturday ☑ Sunday

Multi-test conditions

There will be times where you want to create conditions with more than one test. There are two main scenarios:

- Your condition tests one field for more than one possible value
- Your condition comprises of two or more different fields being tested

Testing **one field for more than one possible value** is straightforward. Select the field you wish to test, add it to the drop zone, and change the test type to **is one of**:
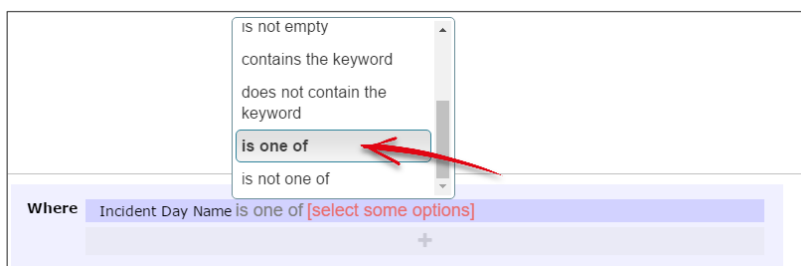
You can then go and select multiple values from the list:
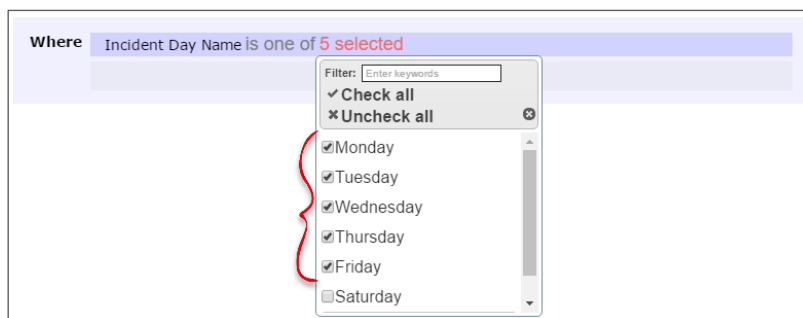
If you wanted to achieve the opposite, you could use the **is not one of** test (usually because it's more efficient):
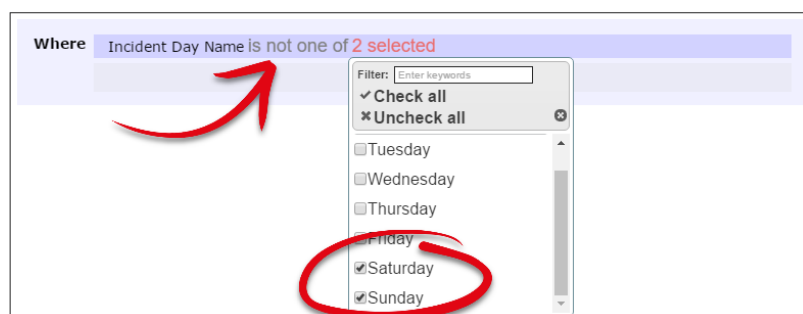
When your condition requires the **testing of two or more fields**, there are two distinct scenarios. The first is when that condition is the only one you require for your alert.

Use the **And/Or** button to determine whether <u>all</u> tests must be passed, or whether just one could satisfy the condition:
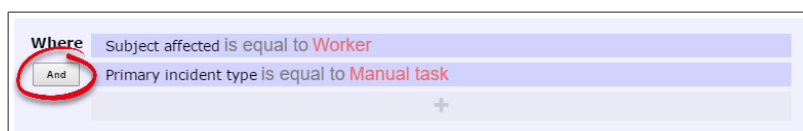
In the above example, we've chosen **And** to ensure that the alert will not trigger unless <u>both</u> of the tests we have added are passed.

In a lengthier example, we have said that the alert will only trigger if <u>all</u> of these tests are passed:
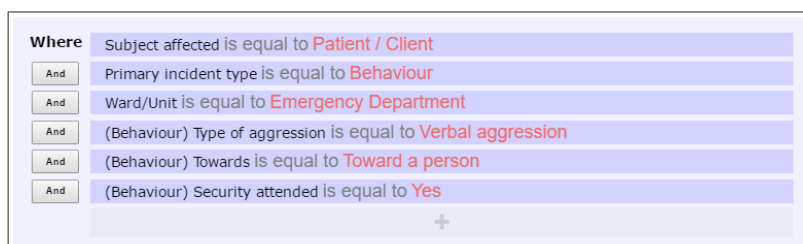
But what if we wanted the alert to trigger based on two unrelated conditions, and each of these conditions tested multiple fields?

Let's use the following example: We want this alert to trigger for **either**:

- Worker incidents that happened on Saturdays and Sundays, OR
- Relative/Visitor incidents that happened in the Emergency Department

We have two distinct sets of conditions there; each condition has its own sub-tests.

In this situation, you need to create two separate conditions in the drop zone. Click the [+   ] button in the drop zone to do this:
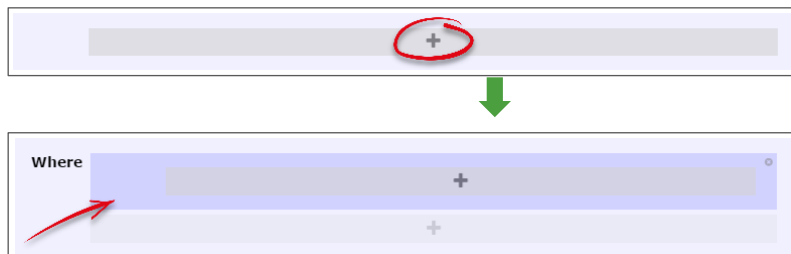
Note the new darker-blue box, with its own additional drop zone. This is where you can go and add the tests which make up the first condition listed above in our example:
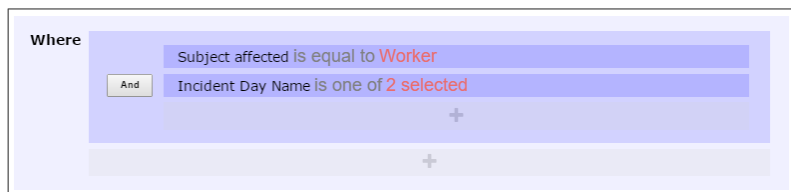
You can now click the outer-most drop zone to add a second distinct condition. Note the new **And/Or** button:
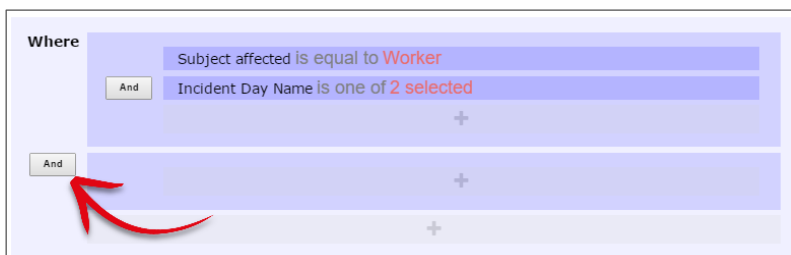
Once we add in the tests required for our second, unrelated condition, it looks like this:

The image above uses red boxes to denote that there are 2 completely separate conditions for this alert; each condition has several tests which must be met before the alert could trigger.

There is the ability to make even more complex conditions (which contain conditions within conditions), however we have provided examples of these in the alert examples supplement.

Deleting tests

Deleting tests is simple. When you hover your mouse over any test, you will note the ✕ icon at the end of the row:

Click the ✕ icon to delete the test. You will not be prompted to confirm this action.

Testing data stored in sub forms and related tables

By default, the list of fields that you can test from the register your alert is for will not include fields from any sub forms or related tables.

Examples of sub forms:

Example of related tables:

If the purpose of your alert included testing and triggering based on the information contained in these places, you can re-generate the list of fields available for testing by choosing the appropriate option in this drop down box:

In the above example, we have decided we want to test both fields from the main form, *and* the information contained within the **Actions** sub form. The fields from the Actions sub form will appear at the bottom of the list of all fields. The principles of creating filters are exactly the same as we have learned so far.

Adding time-based conditions for reminder alerts

When you are creating a reminder alert, one of the most crucial things to add is a condition which decides **when** the reminder should occur (or begin). This is always based on a date field:
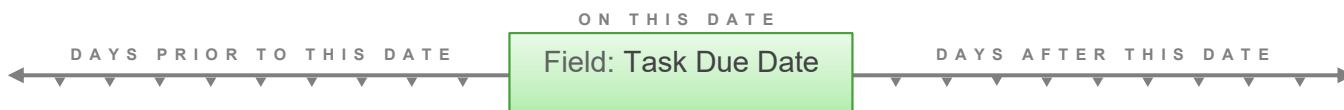
When you have selected the **alert method** of **Scan all items periodically**, every date field from the register your alert is for will have a duplicate in the list, with "(Periodic)" appended to the label text.

Alert Management

Add the (Periodic) duplicate field to the drop zone to create your desired test.
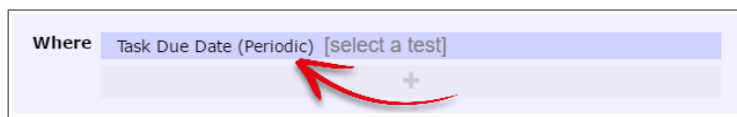
If you wanted to remind the recipient that the task was **due soon**, you would add a condition for the alert to trigger **prior** to the date listed in the Task Due Date field:

If you wanted to remind the recipient that **today was the due date** of the task, you would add a condition for the alert to trigger **on the date** in the Task Due Date field by using zero:
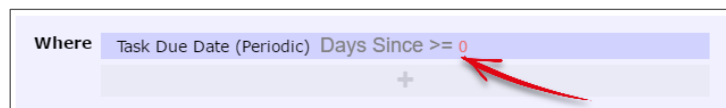
If you wanted to inform the recipient that the task was **overdue**, you would add a condition for the alert to trigger **after** the date listed in the Task Due Date field:

Note: How frequently the recipient is reminded via email is determined in the **Schedule** options.

Testing your alert conditions

Once you have configured the conditions of your alert, you can test them to see if you are on the right track. Click the **Test Conditions** button:
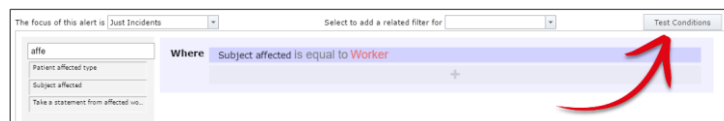
After a brief pause, the system will tell you how many records already exist in the system that match your alert setup. It will also list the ten most recent records by ID number that match your alert setup. This can be useful to check if the alert will trigger for the types of records you expect it to.
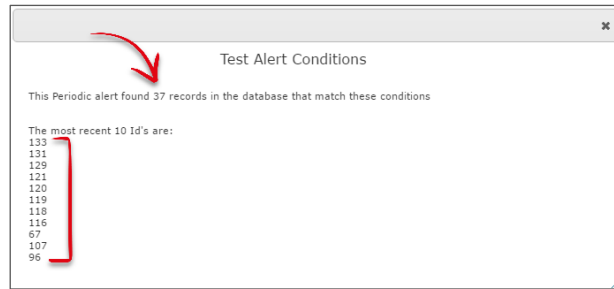
Alert Recipients

There are several ways that you can determine who the recipient(s) of your alert should be, but essentially it comes down to whether:

- The recipient is <u>always</u> going to be the <u>same person</u> (or people), or,
- The recipient is going to be different every time

So will the recipient for the alert be static, or dynamic?
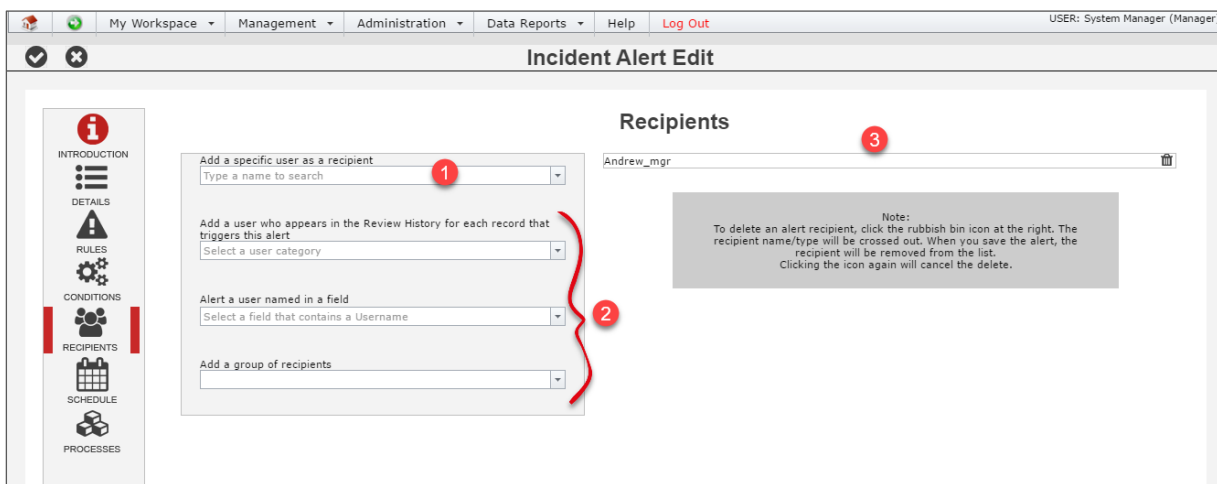
❶ **Static recipients:** When the recipient of your alert will be a specific user every time, search for that user here.

❷ **Dynamic recipients:** There are multiple ways that you can automatically determine who the recipient of the alert should be.

❸ **Recipients:** This is your actual list of alert recipients. Note that it is possible to have both static and dynamic recipients in an alert.

Adding static recipients

Alert Management

Adding static recipients is simple. Simply start typing the name of your intended recipient, and the system will narrow down the number of matches as you type:
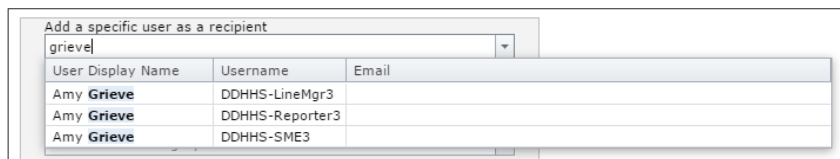
Click on the desired user and they will be added to the **Recipient List** on the right hand side of the page:

Repeat as required to add additional recipients.

Adding dynamic recipients: Users listed in the Review History of the record

Using this option automatically grabs the name of a certain type of user listed in the **Review History** of the record that has triggered your alert. Most choices in this list correspond to users recorded in the Review History, however some will start to look up the chain of management as well (if this feature is used in your system).
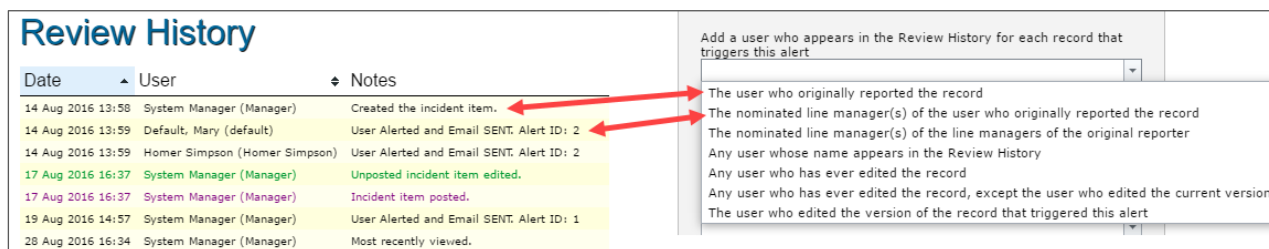
Selecting one of the values from this list will add it to the list of recipients on the right hand side of the screen:

Adding dynamic recipients: When the intended recipient is whichever user is listed in field in the record

Using this option automatically grabs the name of a user listed in a field from the record that triggered the alert.

Selecting one of the values from this list will add it to the list of recipients on the right hand side of the screen:

Adding dynamic recipients: When your recipient is the person in a particular group or role

This functionality might not be in use in your configuration of RiskMan.

Using this option performs a lookup into your organisation's list of roles or positions. Depending on how your system has been specifically configured, this list of roles or positions might be maintained via List & Codes Maintenance, or through a separate Organisation or Roles register. This functionality can also allow you to define a group of people via an SQL statement. Contact RiskMan Support for further information.

Parameters

Some of the options in this field configured in your system might require that you define a parameter before you can add the recipient group to the alert. This is clearly shown when you browse the list of groups:
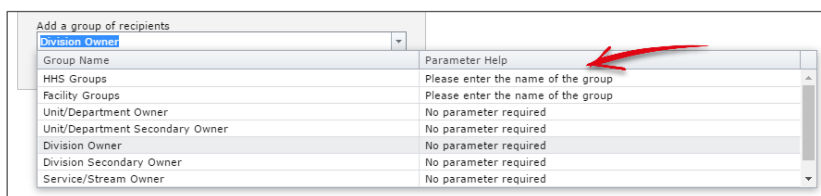
Groups with no parameters: Select the desired value and click the ✓ icon. The recipient will be added to the list of recipients on the right hand side of the page.

Groups where a parameter must be defined: When you select a group where a parameter must be defined, an extra text box will be shown. Add your parameter to this box, then click the ✓ icon. The recipient will be added to the list of recipients on the right hand side of the page.
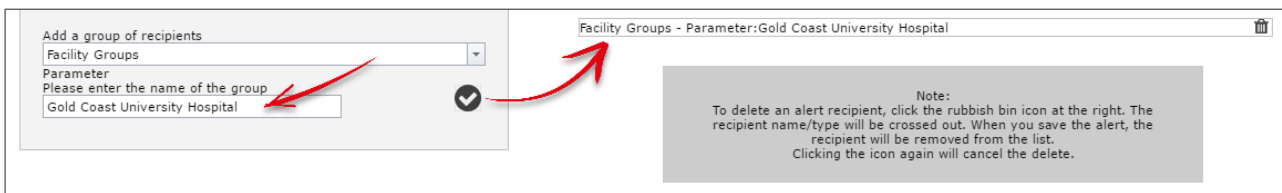
Deleting recipients

Deleting recipients is simple. To delete an alert recipient, click the 🗑 icon to the right of the respective recipient. The recipient name/type will be crossed out. When you save the alert, the recipient will be removed from the list.

Clicking the icon again will cancel the delete.
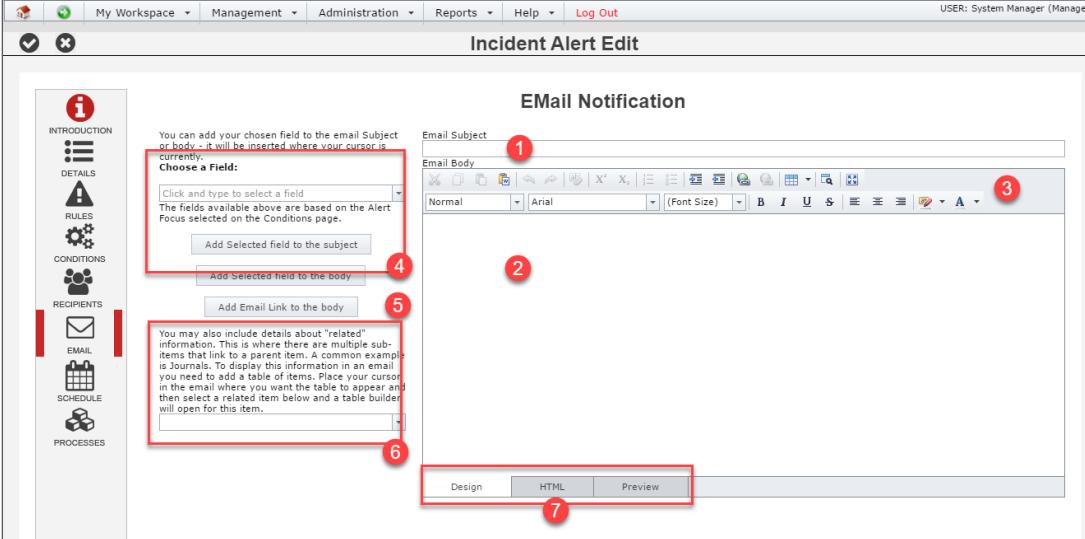
Alert Email

If, in the **Rules** options of your alert, you selected the option **Send an email every time the conditions are satisfied**, you will see the **Email options**:

❶ **Email Subject**: Enter the text that you want to have shown in the subject line of the email.

❷ **Email Body**: Enter the text that you want to have shown in the body of the email.

❸ **Formatting Tools**: Use these "What you see is what you get" (WYSIWYG) tools to make your email look great.

❹ **Field Substitutions**: Similar to a mail merge function in MS Word, you can automatically grab information from the fields in the record triggering the alert and have that detail auto-populated into the email.

❺ **Email Link**: Place a link in the email so the user can click it to open the record that triggered the alert.

❻ **Add sub form table**: Use this tool if you want to add the information from a sub form to the body of the email.

❼ **Edit mode tabs**: Switch between different edit modes for more control, or to test the functionality of your email (to test hyperlinks, for example).

Email Formatting

The WYSIWYG tools are very similar to using word processor formatting tools. This image summarises the various formatting you can apply to your email:
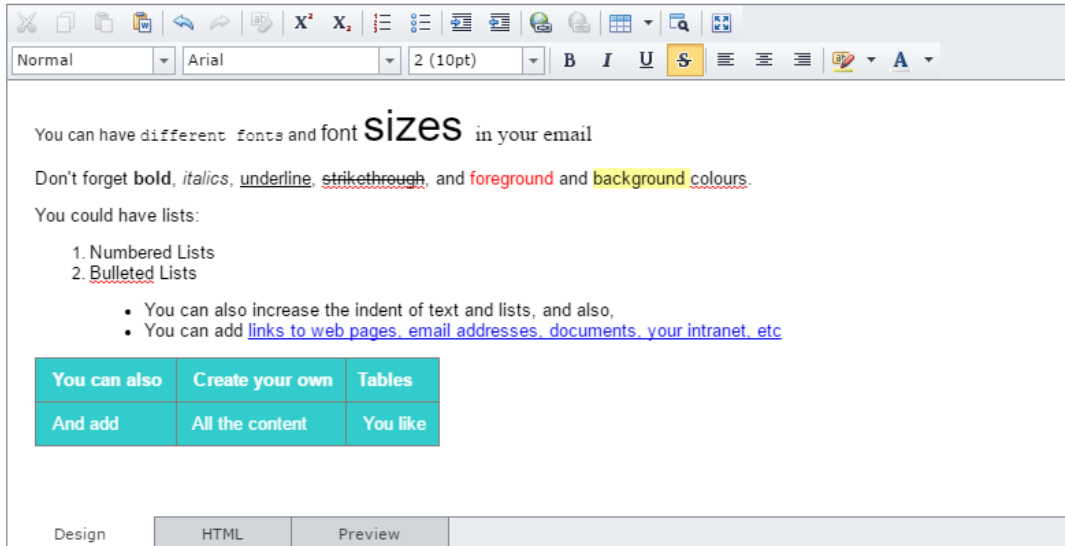
Dynamic email content

Alert emails don't just have to contain static content. You can draw information from the record that triggers the alert, and automatically add that information into the email at various points. For example, if we wanted to create an alert that sent an acknowledgement email to the person who reported a record, it might look like this if I we wrote it ourselves:

Dear Mary

Thank you for reporting incident 177 on 15 Sep 2016. It has now been sent on to the appropriate manager for follow up.

Some of that information could automatically be drawn from each incident when the alert is triggered:

Dear (Reporter's name)

Thank you for reporting incident (Incident ID number) on (Date the incident was entered). It has now been sent on to the appropriate manager for follow up.

To add these field substitutions to your email

Compose your email as you ordinarily would. When you arrive at content which can be populated by the information in the incident record, search for the related field in the **Field Substitution** box:
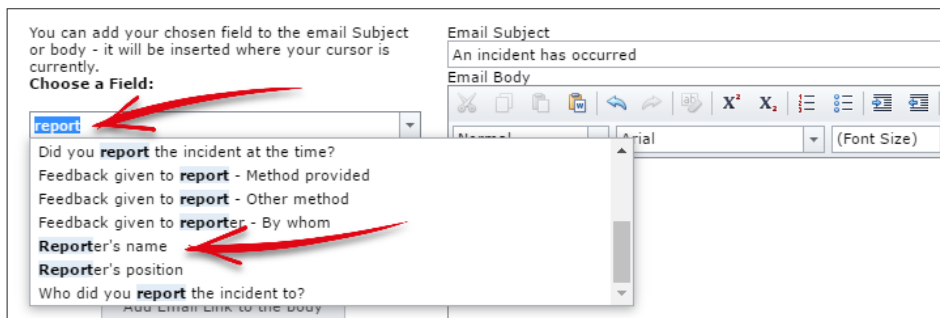
Select the field containing the content you want auto-populated where your cursor is in the email subject or body. Click the respective button to add the content where you want it to go:
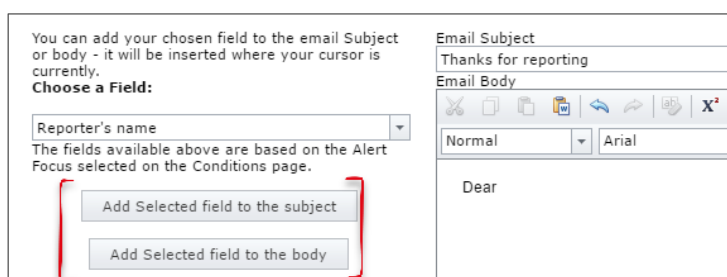
The field will be added to your form within [square brackets]:
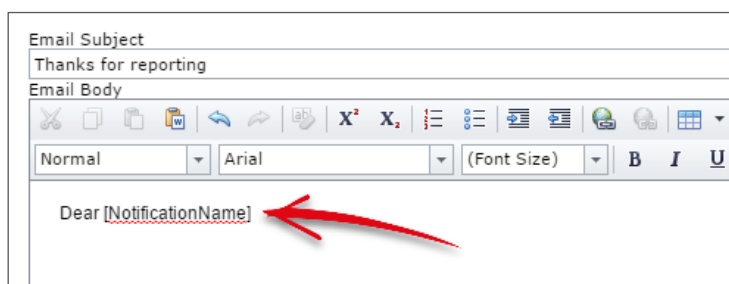
What is contained in the square brackets is the <u>database field name</u>, **not** the label you are used to seeing from the form – don't panic!

Alert Management

Using more field substitutions, we have configured our email to look like this:
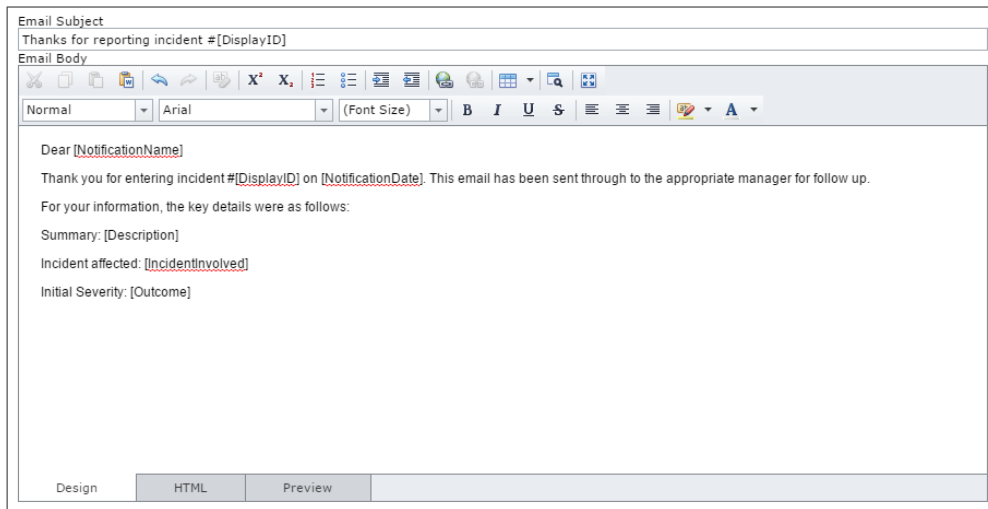
Now we want a link to be inserted that the user can click on to open the incident. To do that, we put our cursor where we want the link to go, and click the **Add email link to body** button:
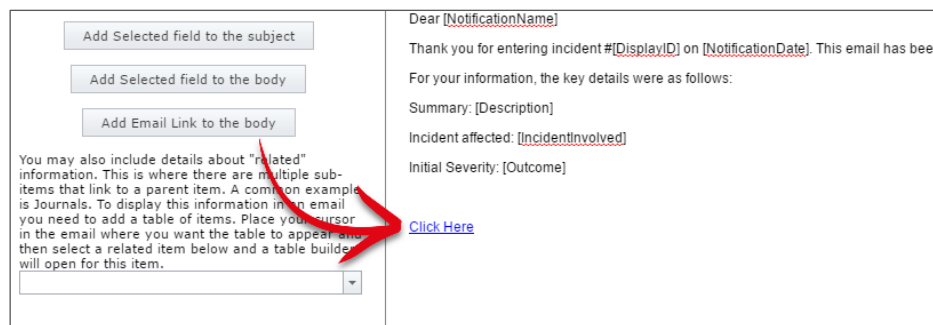
Once we modify how the link text appears, and apply some other formatting, our email looks like this:
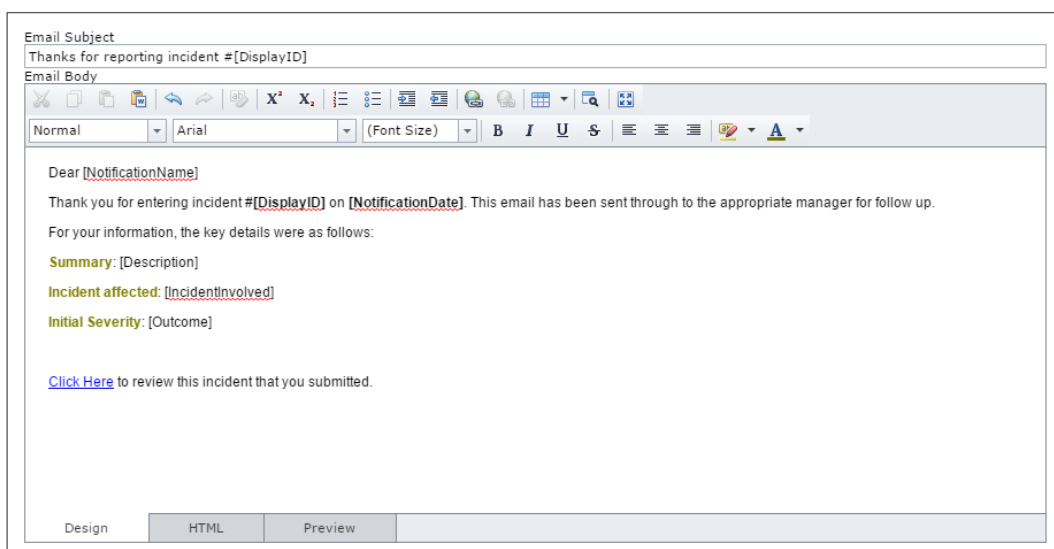
Adding the details from a sub form to the body of the email

Some of the information stored in the forms in your system are contained in **sub forms**:

	Action ID	Action commenced date	Action	Category of action	Strength of action	Due date	Status	Date Completed	Authorised	Responsible person name	Source of recommendation	
			Add Corrective Action									
	1	17 Aug 2016	Placement of signage in the cafeteria reminding staff of the banana peel disposal and safety policy	Policy/procedure/guideline	Moderate	23 Aug 2016	In progress		Yes	Billy Bloggs	WHS	✕

It is possible to add the content of these forms to the body of your email in a table format. To do so, select the appropriate sub form from the drop down box:


This will open the **Related Table Builder**.

❶ **Field Select**: Choose a field from the selected sub form to add to the table. It will be added to the table space in ❷.

❷ **Table columns**: Adjust the column order and widths of the fields you have chosen to put in your table.

❸ **Table format**: Choose a format for your table. You can make additional formatting changes once you have inserted it into the email body.

❹ **Add table to Email**: Click to close the related table builder and add the table to your email.

The table we configured above looks like this when inserted into our email:

Action ID	Action	Category of action	Due date	Status	Date Completed	Responsible person name
[PCAID]	[PCAAction]	[PCACategory]	[PCADueDate]	[PCAStatus]	[PCACompleteDate]	[PCARespPerson_name]

Design   HTML   Preview

From here, we could apply additional formatting to the content of the table if we wanted to.

When the email is generated, then the number of sub form entries in the record that has triggered the alert will be entered into this table. Please note there is no way to restrict which type of sub form entries go into this table (ie. Based on a filter).

Alert Digest

If, in the **Rules** options of your alert, you selected the option **Send a Digest email at the end of the nominated interval which summarises every item that satisfied the alert conditions**, you will see the **Digest options**:

The Digest is designed to provide the recipient with a summary of all the records which matched the conditions of the alert during a given timeframe.

❶ **Timeframe & Frequency**: Set the summary timeframe (eg. the previous calendar week) and how often the digest email should be sent (eg. every 7 days).

❷ **Email Subject**: Enter the text that you want to have shown in the subject line of the email.

❸ **Email Body**: Enter the text that you want to have shown in the body of the email.

❹ **Edit mode tabs**: Switch between different edit modes for more control, or to test the functionality of your email (to test hyperlinks, for example).

❺ **Summary table builder**: Use this tool to create a table which summarises all the records that matched the conditions of the alert

Setting the Digest timeframe and frequency

Alert Management

The timeframe is the duration of time you want to summarise. Any record which matched the conditions of this alert during the timeframe you stipulate will be included in the summary table you will build.

| Time Frame: | The previous | 1 | ⇕ | Months(s) | ▾ | up to | Prior Month End | ▾ |

The available options are:

The previous…	Timeframe	Up to
(arbitrary)	Day(s) Weeks(s) Month(s) Year(s)	Run date Prior day end Prior week end Prior month end Prior quarter end Prior year end Prior financial year end

The frequency is how often the Digest should be generated and emailed to the recipient.

| Run Frequency: Every | month | on the | 5th | at | 08 | : | 30 |

The available options are:
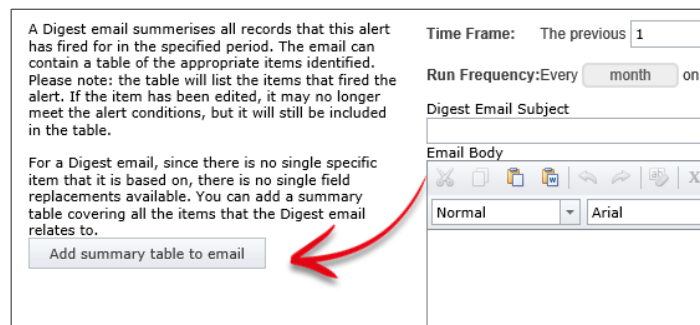
Every…	Timeframe options	Time
Day	-	The time of day the digest should be generated
Week	Days of the week	

Month	Dates of the month	
Year	Dates of the month and months of the year	

Building the digest table

You must ensure that you create the table which will summarise each record which matched the conditions of the alert. To do this, click the **Add summary table to email** button:

This will open the **Related Table Builder**:
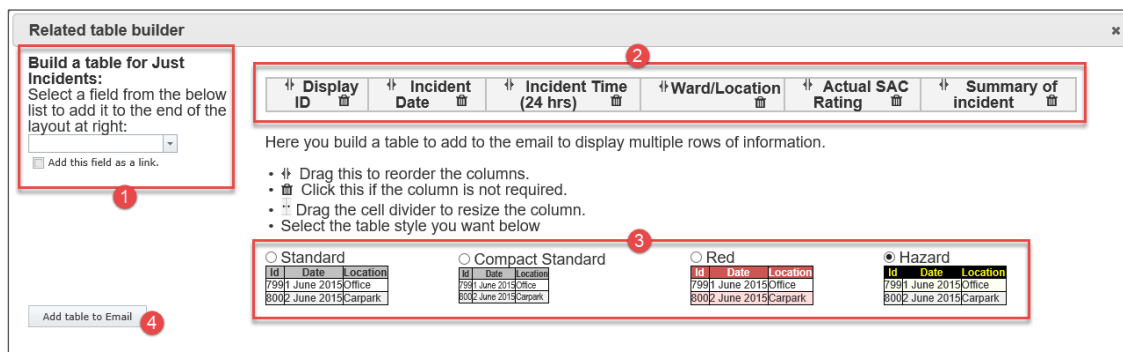
❶ **Field Select**: Choose a field from the selected sub form to add to the table. It will be added to the table space in ❷. If you want the value from the field to be a clickable link which opens the related record, check the box **Add this field as a link**, and *then* add the field. We would recommend making **Display ID** the clickable link.

❷ **Table columns**: Adjust the column order and widths of the fields you have chosen to put in your table.

❸ **Table format**: Choose a format for your table. You can make additional formatting changes once you have inserted it into the email body.

❹ **Add table to Email**: Click to close the related table builder and add the table to your email.

The table we configured above looks like this when inserted into our email:
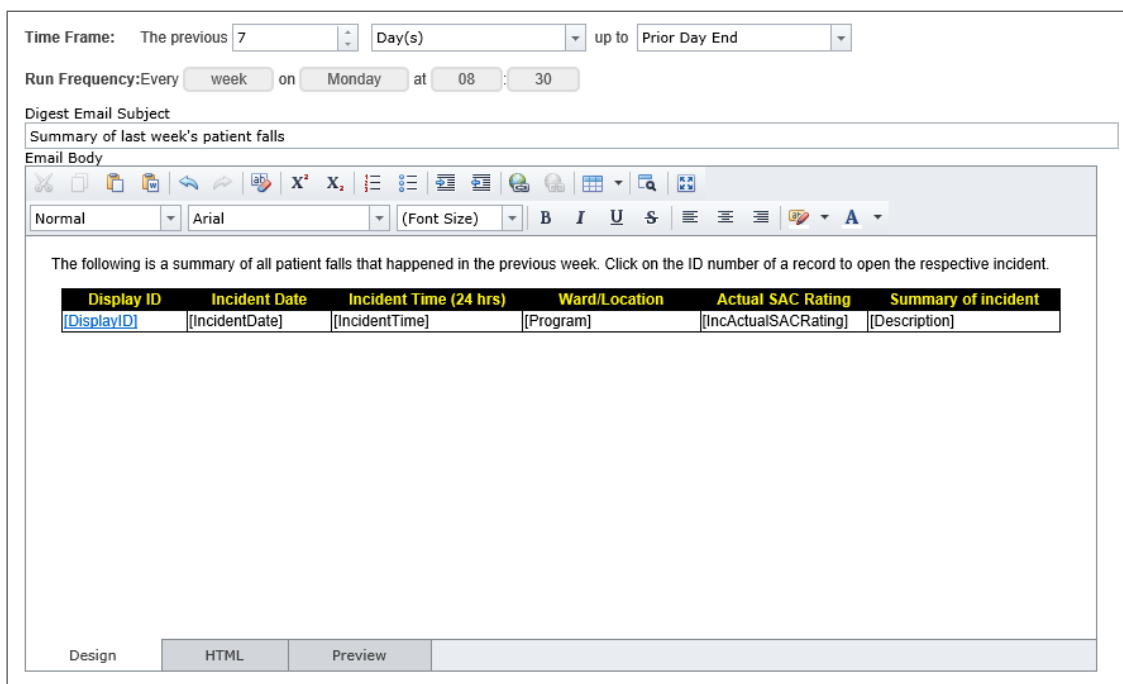
Alert Schedule

The schedule allows you to determine when your alert should be processed by the system
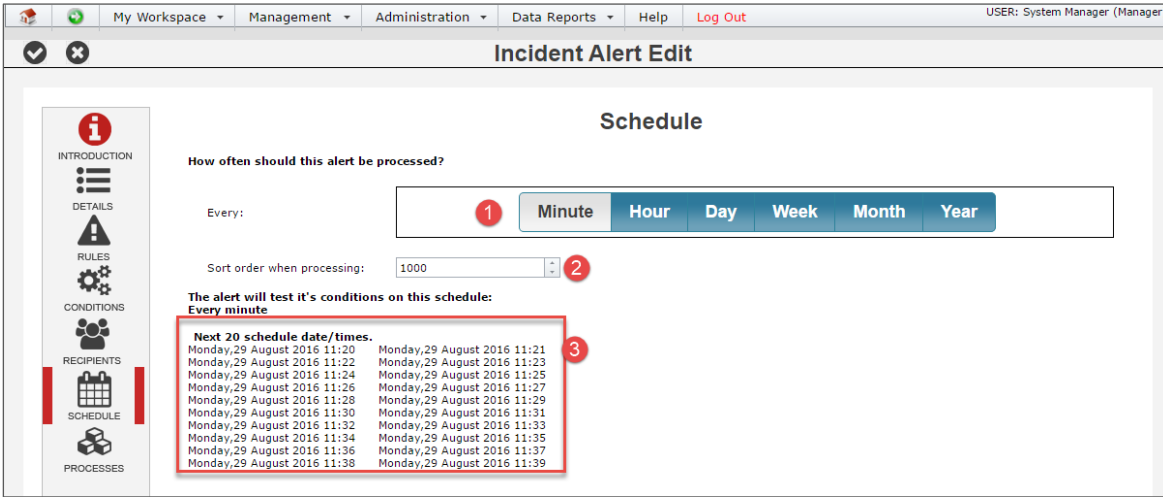
❶ **Frequency**: Use these options to set how often the alert will be processed.

❷ **Sort order when processing**: This generally only needs to be used on the advice of RiskMan Support. If you have more than one alert that needs to be processed at the same time, the value in this field allows you to determine the order in which each competing alert should be processed.

❸ **Next scheduled run time**: Tells you exactly when the alert will next be processed.

When should the Schedule function be used?

Alert method	Usage	Comments
Check each item when it is saved	Scheduling is optional	Generally you wouldn't need to schedule alert processing as these alerts are for notifying recipients as soon as something has happened. However, you may wish to schedule the alert to be processed in restricted times only, for example if the recipient only wants to receive emails during office hours.

		By default, if you don't make modifications in the Schedule options, the alert can process "all the time".
Scan all items periodically (i.e. reminder alerts)	You must make a schedule	You must tell the system how often the recipient should be reminded
Trigger the alert once a threshold has been exceeded	Not recommended	If you really need to, you can restrict when threshold checking is performed, however because many threshold alerts are monitoring vital information, it is generally not recommended to further restrict when the alert is processed.

Please note that **Digest Emails** are not subject to any scheduling that you set here, as they have their own prescribed frequency.

Examples of Schedules

The following schedule could be used prevent an alert from running outside of regular business hours:

Note that for any records that match the conditions of the alert, but are entered <u>outside</u> the scheduled processing times, those records will be included when the alert next processes.

Alert Management

For example, based on the above schedule, if an incident occurred at 11:30pm on Tuesday night, the alert would generate an email and send it to the recipient at 8:00am on Wednesday morning.

This schedule might be used for a reminder alert. It will alert the recipient every Tuesday and Thursday at 2:30pm:

Every:	Minute	Hour	Day	**Week**	Month	Year

Days of week:	Saturday	Sunday	Monday	**Tuesday**	Wednesday	**Thursday**	Friday

Hours of the day:

00	01	02	03	04	05	06	07	08	09	10	11
12	13	**14**	15	16	17	18	19	20	21	22	23

Minutes of the hours:

00	01	02	03	04	05	06	07	08	09
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59

This schedule might be used as a reminder that something is overdue. It reminds the recipient every four days, at 8:00am, until they complete what is outstanding.

Every:	Minute	Hour	Day	Week	**Month**	Year

Days of month:

1st	2nd	**3rd**	4th	5th	6th	**7th**	8th	9th	10th
11th	12th	13th	14th	**15th**	16th	17th	18th	**19th**	20th
21st	22nd	**23rd**	24th	25th	26th	**27th**	28th	29th	30th
				31st					

Hours of the day:

00	01	02	03	04	05	06	07	**08**	09	10	11
12	13	14	15	16	17	18	19	20	21	22	23

Minutes of the hours:

00	01	02	03	04	05	06	07	08	09
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59

Alert Processes

Processes has two functions:

❶ **Processes**: If the alert you are setting up is to execute a **pipeline process**, select the respective process here.

❷ **Alert Chaining**: Allows you to designate that an individual record either:

- Cannot trigger this alert unless that record has already triggered the selected alerts on the left; and/or,
- Can trigger this alert only if the selected alerts on the right hand side have not been triggered by that record.

This allows for some reasonably complex workflows to be orchestrated. However, these processes would generally be setup in conjunction with RiskMan, in particular pipeline processes.

Save your alert

Once you have setup your alert, save it by clicking the ✔ icon in the toolbar:
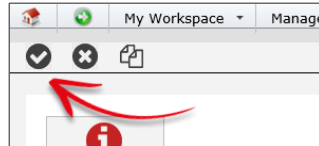
Clicking the ✖ icon will take you back to the Alerts list page without saving your changes.

Clone an alert

If you have several alerts to create, but perhaps with slightly different conditions or different recipients, you can open an existing alert, click the 🗐 icon in the toolbar, make your desired changes, and save this as a new alert.

Alert Logging

Once you have saved your alert, the activity associated with it can be seen in the **Logging** section.

ADMINISTRATION OF ALERTS

There is one permission for each register:

Register tab (e.g. Incidents) > **Administrative Permissions**

- Can manage Alerts

There is also a Global Setting that affects the behaviour of Alerts:

Global Settings > **Alerts** > 20) Apply user restrictions when creating alerts

Enabling this setting will automatically include a user's site restrictions (if any) as conditions when the alert is created.

Alert Import / Export

It is possible to export alerts from one system to another. This could be practical if you have, for example, setup alerts on your training or model system, and want to import them into your live system once you are happy that they are setup correctly.
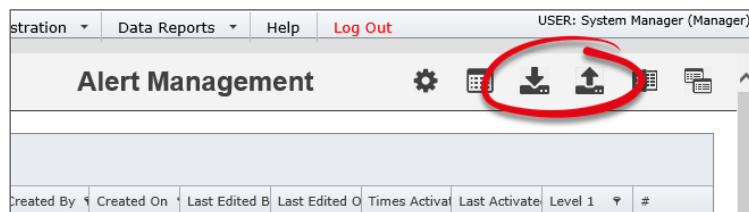
To export alerts: First, filter the list of alerts that you wish to export. Then, click on the export icon. Your web browser will prompt you to either save or open the resulting text file:

Alert Management
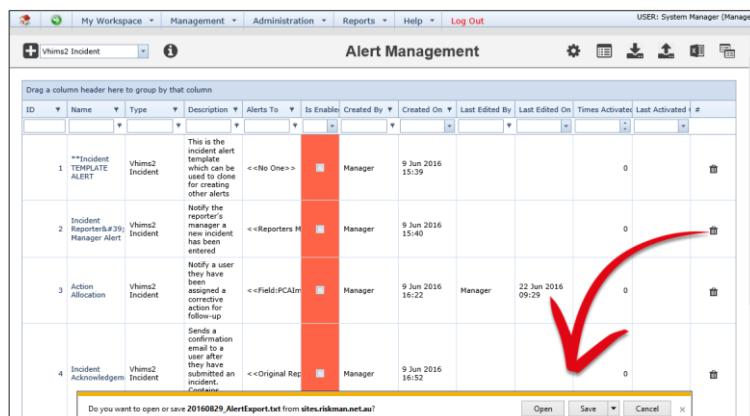
To import alerts: Click on the import icon ⬆. The **Alert Import** dialog will appear:
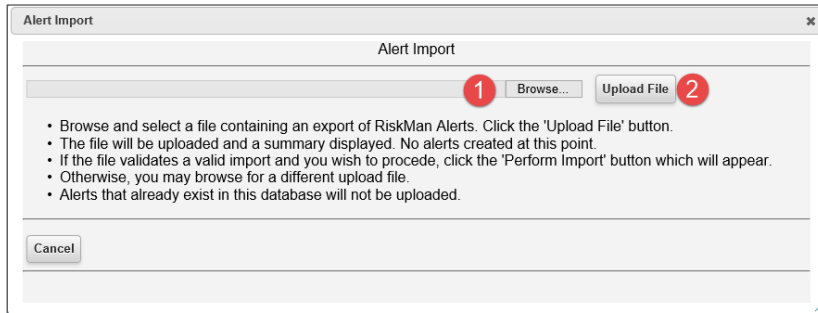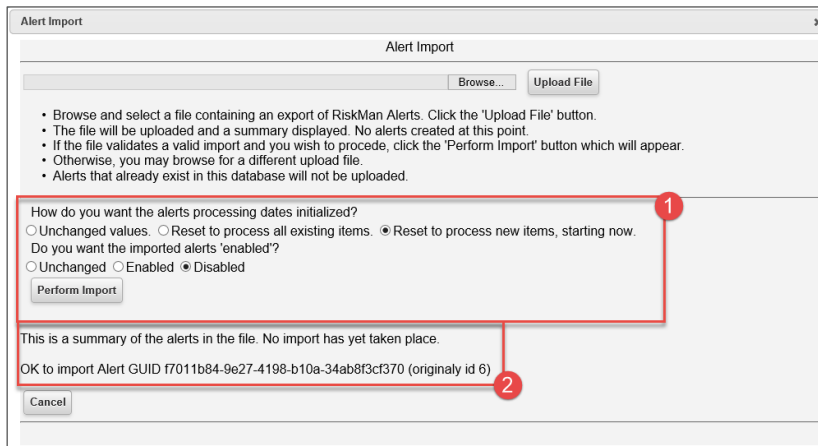

❶ **Browse**: Search for the target file on your computer that contains the alerts you wish to import.

❷ **Upload File:** Uploads the file for analysis.

After uploading your import file:

❶ **Import Options**: Allows you to designate which records should be processed by the imported alert(s):

- **Reset to process all existing items** means that when your alert is imported and enabled, it will look through your **entire** database, and based on the rules of that alert, will trigger for any matching record.
- **Reset to process new items, starting now** means that the alert will ignore all the existing records in your database, and only process for new records that are submitted <u>after</u> alert is imported and enabled.
- **Unchanged values** will retain whatever values were in the original alert in the source system,

As well as the alert status (enabled/disabled):

- **Unchanged**: Keeps the status each alert had in the source system
- **Enabled**: Enables all alerts in the import
- **Disabled**: Disables all alerts in the import

Click the **Perform Import** button to complete the import.

❷ **Import Summary:** This summary tells you whether the alert exists in the destination system. Any alert that already exists will be skipped.

ADDITIONAL INFORMATION & TIPS

Please note that if a user has permission to see the Alerts Management page, they can see all alerts in the system – not just the ones they have created. For that reason, please exercise caution as to who is able to maintain alerts. Changes made to alerts cannot be reversed.

Please refer to the **Alert Examples Supplement** for detailed examples of different alert types, and the appropriate configuration of all the applicable settings.

RELATED TOPICS

Global Settings