The Why and How of Alarm Management in Adroit

The following document, aims to:

- introduce the need for and use of Alarm Management;
- explain the terminology and how it applies to Adroit and
- describe how to use the new AlarmManagement agent.

Why is alarm management needed?

In the past alarms were hardwired into the panels, which limited their number; now that alarms are software-driven, means that you can have an unlimited number of alarms.

In an effort to keep the operators sufficiently informed, SCADA installations typically use lots of alarms, each of which usually have very little awareness of the other alarms in the system. This means that each incident can generate a flood of alarms, which causes operators to become overloaded and confused and as a result they may even start ignoring alarms! Therefore LESS alarms are MORE effective.

Alarm management is concerned with improving the QUALITY of the information within the alarming configuration. This information should be used to reduce the QUANTITY of nuisance alarms (red herrings) so that only the most important and relevant alarms are displayed for your process.

In other words alarm management counteracts inefficient alarming by allowing you to create an alarming system that alerts the operator to the most relevant alarm for the current incident.

The following procedure describes the recommended method of using the AlarmManagement agent to configure and record your active incidents so that you can analyze this information to improve your alarming configuration.

What is an incident?

In Adroit, Alarm agents can monitor other agents for preset conditions or states. So that when a monitored condition occurs in an agent its Alarm agent uses predefined reporting methods to alert the necessary people and/or applications. That is why Alarming in Adroit primarily involves the configuration of the following two things:

- The preset conditions or states of each agent that you need to alarm, known as alarm types, which each constitute a separate alarm or event.
- The alarm routes that specify which alarm destinations (reporting mechanisms) you need to use to communicate the generated alarms and events to the necessary personnel and/or applications.

In Adroit an incident occurs when an agent enters a condition defined by an alarm type that is being monitored by an Alarm agent. However, an incident is ONLY an alarm, if it needs to be responded to; otherwise it is an event.

Quick Start to Configure and Record Incidents (Alarms/Events)

This explains the recommended method of implementing the AlarmManagement agent to configure and record your active incidents so that you can improve your alarming configuration.

Things you need to do before you can implement the AlarmManagement agent:

1. Ensure that your Adroit license has the necessary OEM code (4096), which enables your Alarm Management functionality to work.

   WITHOUT this OEM license your AlarmManagement agent stops populating the database with incidents after 1 hour.

2. Create the required OLE DB compatible database, we STRONGLY RECOMMEND that you use a MS SQL database for your alarm management.

   Note: You can NO LONGER connect to a MS ACCESS database for your AlarmManagement database, due to known performance issues.

   If you do not have SQL installed then install MS SQL EXPRESS.

3. If possible, create the required incidents, although these can be added to the AlarmManagement agent as needed.

4. We highly recommend that you configure any delays and/or conditions for your incidents in the Alarming configuration dialog when you alarm agents.

   IMPORTANT: DO NOT use or configure the delays and/or conditions provided by the AlarmManagement agent (or its database), since this functionality will be removed from future versions of Alarm Management.

To log and/or configure your incidents:

Add and/or locate the required AlarmManagement agent.

If necessary, add an agent of the required type, as follows:

In the Smart UI Designer:

Select the required Smart UI Server in the **Enterprise Manager**, as follows:

1. Open the **Enterprise Manager**.
2. If necessary, expand **Servers**.
3. If necessary, expand the name of the required Server connection.

   Tip: The connection name is prefaced by the Smart UI Server computer name.

4. If necessary, expand the **Datasources** category.
5. If necessary, expand the required Adroit datasource or its icon.
6. If necessary, expand the **AgentGroup** tree.
7. Right click the required agent type, which are listed alphabetically, and select **Create Tag**.
8. Specify the required **Tag Name** or agent name.

   The following rules apply when naming agents:

   a. Agent names have a maximum of 27 characters.

   b. Agent names cannot be the same as the names used for Agent Types or for Agent Groups.

   c. Agent names cannot use the following characters:

Space		Percent	**%**	Comma	**,**
Period	**.**	back slash	****	Dollar	**$**

9. If necessary, provide an optional **Description** that describes the purpose or describes the value of this tag (agent) for ease of reference.
10. Click the **Finish** button.

If necessary, locate the required agent, as follows:

In the Smart UI Designer:

Select the required Smart UI Server in the **Enterprise Manager**, as follows:

1. Open the **Enterprise Manager**.
2. If necessary, expand **Servers**.
3. If necessary, expand the name of the required Server connection .

   Tip: The connection name is prefaced by the Smart UI Server computer name.
4. If necessary, expand the **Datasources** category.
5. If necessary, expand the required Adroit datasource or its icon .
6. If necessary, expand the **AgentGroup** tree.
7. If necessary, expand the required agent type , which are listed alphabetically.
8. Locate the required agent , which is also listed alphabetically beneath their applicable agent type.

In the Enterprise Manager window: right click this agent and select **Configure**.

When the **Edit AlarmManagement agent** dialog is displayed:

1. Ensure that the **Start Alarm Management Agent** checkbox is checked.
2. Specify the location to the SQL database in the **Connection** field.

   Click the browse button ... to the right of this field and use the **Data Link Properties** dialog to create the required connection string to your SQL Server database, as follows:

   This **Data Link Properties** dialog specifies the location and the security credentials required to connect to this database.

   Note: If you need to configure or view this database and its data from other computers, like remote User Interfaces, then use a UNC path and not a local file system path to specify the location of this database.

   A. Double click the **Microsoft OLE DB Provider for SQL Server** item in the **Provider** tab of the **Data Link Properties** dialog.

   - Either type in the computer name of the SQL Server that you want to connect to, in the **Select or enter a server name** field.

     Tip: This is the fastest method, if you know the name of the SQL Server.
   - Or click the button to the left of the **Select or enter a server name** list box and select the name of the required SQL Server from the list.

   B. Specify the required security credentials to connect to this SQL Server, as follows:

   IMPORTANT1: If you need to connect to a remote SQL database and want to run the Agent Server service using the **Local System account**, then use **SQL Server Authentication**.

   IMPORTANT2: If you need to connect to a remote SQL database and want to **Use Windows NT Integrated security**, then ensure that the user profile that the Agent Server service uses to log onto the computer HAS the necessary rights to browse the network and connect to the remote database. This should **NOT** be the default **Local System account.**

   - **Use Windows NT Integrated security:** this option uses the username and password of the currently logged on Windows user.

Tip: We recommend that you configure your SQL Servers to use this option to avoid requiring additional database security.

- **SQL Server Authentication:** this option uses the **User name** and **Password** configured within the SQL Server you are attempting to connect to.

  Note: In this case it is recommended to check the **Allow saving password** checkbox.

C. Select the name of the required database from the **Select the database on the server** list box.

D. Click the **Test Connection** button to ensure that you are able to connect to this database using these details. Only proceed once 'Test connection succeeded' is displayed.

E. Click the **OK** button.

Your connection string will be created.

Note1: The **Advanced** tab of this dialog allows you to specify access permissions for this connection string. If you are unsure about these settings NEVER set these permissions to **Read** otherwise this connection string will fail.

Note2: These security credentials are database specific and should not be confused with application security.

Note3: You can edit this string directly, once it has been created, if necessary.

3. Click the **Update** button.

Categorizing your incidents

By default, all the incidents assigned to the alarm routes that use this AlarmManagement agent are added to the _**Uncategorised** category of its **Categories** tree.

Typically you will create and use categories for your incidents for one or both of the following reasons:

A. The more incidents in the **_Uncategorised** category, the harder it becomes to differentiate between these incidents.

For this reason, you can create other categories to distinguish between the following:

- different areas or sections of your process, such as crushing, flocculation etc.
- different equipment within each of these areas and if necessary down to the individual tag level.

Adding categories allows you to easily query (analyze) or report ONLY the incidents that you are interested in, instead of ALL the incidents, so that you can manage this data more effectively.

B. Categories also allow you to provide the name of the Operator that is responsible for the incidents allocated within it (and if necessary its sub-categories). This name is logged with these incidents, for auditing purposes.

Therefore, this setting only applies to categories that represent areas of your process that have different operators overseeing them.

The default **_Uncategorised** category is simply provided to make you aware of the incidents that you have not categorized. Therefore **this category does NOT allow you to assign an operator name** to these logged incidents.

Tip: To quickly categorize your incidents, click the **Learn alarms** (incidents requiring acknowledgement) and/or **Learn events** (incidents NOT requiring acknowledgement) buttons to add ALL the applicable unassigned incidents, that are routed to this alarmmanagement agent, to the **_Uncategorised** category.

We therefore recommend that you categorize your incidents as follows:

4. If necessary, in the **Categories** tree, rename the ROOT category to the HIGHEST category level that you require. For instance:if you are ONLY using this agent to manage the alarming of a single plant, call this category Plant XXX etc.

5. Add sub categories for every area of your process that is controlled by a different operator. In other words add one sub category for each operator (Clients).

For instance:if your plant has two remote Operators, one which controls the crushing section of your plant and another that controls the flocculation section, then add two sub categories to the root node, one called **Crushing** and the other called **Flocculation**.

6. Configure the **Operator Tag** properties of each of your categories to specify the tag that provides the name of the operator that is controlling the specified areas of your process.

   Click for more details:This ensures that the incidents that arise from the applicable area of your process will be logged using the name of the operator that was currently in control of that process area.

7. If necessary you can create further sub-categories for sections that do not have an associated operator, in order to make your queries of the data more accurate.

   For instance:you can create sub categories for each process area or for each item of equipment in each process area or even for each instrument tag!

8. Add this AlarmManagement agent to the routes of the required Alarm agents. We recommend that you add this agent to route 2 and 3 of the defaultAlarmAgent.

   Note: A default HTML document is created for each active incident on the specified alarm routes, which you can edit to provide assistance on how to deal with it.

   Click for more details:this document is created in the Data sub folder of the your designated project folder, which is typically C:\ProgramData\Adroit Technologies\Adroit\Configurations\Default\Data.

9. Categorize your incidents, by assigning the incidents that are routed along each selected alarm route to their required category (or sub category). For instance:

   > Assuming that you have a crushing section to your process, assign all the incidents (the alarmed alarm types) of the agents that relate to equipment within this section to the **Crushing** category.
   >
   > However, if you have two crushers and you created two sub-categories for them (within the **Crushing** category) called **Crusher1** and **Crusher2** then you would assign all the incidents of the relevant agents to the **Crusher1** and **Crusher2** categories instead.

   Note: If one or more of the incidents routed along the selected alarm routes become active before you have categorized them, they will be added to the **_Uncategorised** category, from which they can be dragged to their required categories.

   Tip: To quickly categorize your incidents, click the **Learn alarms** and/or **Learn events** buttons to add ALL the unassigned incidents, that are routed to this alarmmanagement agent, to the **_Uncategorised** category.

Configuring the added incidents

10. If necessary, configure your incidents, by specifying one or more of the following optional incident attributes:

    - Whether the operator is REQUIRED to specify the **Reason** (and sub-reason) for this incident.

      Note: Click the **Edit reasons...** button in the AlarmManagment agent to specify these available reasons and their sub-reasons.

    - Whether the operator is REQUIRED to specify **Notes** (textual comments) for this incident.
    - Whether **Associated Tag** values should be logged along with this incident.
    - The UNC path and filename of the **Document** that provides further information to clarify the incident and provide assistance on how to deal with it or react to it.

Incident icon colors and their meanings

The color of the incident icon indicates whether reasons and/or notes are required or not for this incident, as follows:

- The white icon ⚠ means that no reasons or notes are required.
- The yellow icon ⚠ means that ONLY reasons must be specified.

- The blue icon ⚠ means that ONLY notes must be specified.
- The red icon ⚠ means that BOTH reasons and notes must be specified.

For instance:If you were monitoring the Low-Low; Low; High and High-High alarm limits for a tank, you may only want your operators to specify the reason why the High and Low alarm limits are reached.
You may also want your operators to specify explanatory notes when the Low-Low and High-High alarm limits are reached, explaining why the High and Low alarm limits were exceeded.

Analyzing the logged incidents

11. The AlarmManagement agent provides the following preliminary methods of analyzing the logged alarming data:

    - Once your incidents are being logged to your database, you can launch the **View data** and **View graph** dialogs from mimics to perform queries to analyze this data.
    - A number of common KPIs are provided and you can create up to 6 user-defined KPI values (single value queries) from the database to measure the effectiveness of your operators and/or alarming system.

    If necessary, click the **Edit KPI's** button to change the KPI target values used by certain default queries and your own custom KPI queries, so that these queries better comply with your specific requirements. Click for more details:In the **Edit Alarm Management KPI values** dialog, double click the appropriate KPI (row) to edit its value.

    Although the AlarmManagement agent includes these preliminary methods of analyzing the logged data, we recommend that you use the Alarm Management and Analysis reporting utility, which provides you with the tools you need to improve your alarming system.

Related Links:

Configuring the AlarmManagement Agent: Describes all the configurable options provided by this agent.

How to create your own hierarchical (logical) structure of categories for your incidents:

Tip: This edit dialog can be maximized and resized to enlarge the screen area to design and view this **Categories** tree.

Adding Categories: Categories 🌐 can make your incidents easier to query and analyze.

For more details, see Reasons for categorizing your incidents.

Configuring Categories: Describes how to specify the ‘Operator tag’ setting for categories.

Adding Incidents: To add new and existing incidents to categories in the **Categories** tree.

Note1: You can only assign an incident to a SINGLE category.

Note2: The color of the incident icon indicates whether reasons and/or notes are required or not for this incident. For details, see Incident icon colors.

Removing Incidents: To reassign incidents to other categories or to permanently remove an incident from the alarm management database.

Configuring Incidents: You can configure one or more optional settings for each incident to improve the efficacy of your alarm management configuration.

Note: These configuration settings do not affect the manner in which the legacy Adroit alarming functions.

Tip: You can use the Export button to save and/or bulk configure categories and their incidents within a .CSV file instead. For details, see Exporting categories and their incidents.

About the AlarmManagement Database: Describes the database (the tables and their fields) that is created and maintained by the AlarmManagement agent, which a 3rd party application (such as VIZNET and/or OPUS) can access directly to report and analyze this data.

IMPORTANT: To clear the Alarm Management database - simply to delete all the tables and then restart the Agent Server, which recreates and populates the tables correctly. DO NOT use a script to empty this database, since many of the tables use an auto-incrementing index field, which is NOT reset in this case causing all manner of problems.

WARNING! If you delete any of these tables, they will be recreated with their default configuration when the Agent Server is restarted, BUT you will LOSE any previous configuration or data that the tables may have contained.

Obtaining KPI Values: Describes how to obtain the common KPI values calculated by this agent and/or to configure queries to obtain up to 6 user-defined KPI values and how these values are stored by this agent.

Launching the View Data Dialog: Describes how to launch the **View data** dialogs from mimics to perform queries to analyze your data. For more details on using this dialog, see Querying Recorded Incidents.

Launching the View Graph Dialog: Describes how to launch the **View graph** dialogs from mimics to perform queries to analyze your data. For more details on using this dialog, see Viewing Incident Queries Graphically.

Related information

Configuring AlarmManagement Agents

Note: The **Cancel** button does not work for any edits made within the tree or the list views, such as the **Edit reason and sub-reason categories** dialog.

1. If necessary, add an AlarmManagement agent.

   Note1: Please ensure that this agent name is no more than 27 characters long.

   Note2: You can only add ONE AlarmManagement agent.

2. Edit all the Alarm agents that are required to send their alarms/events to this AlarmManagement agent, by adding the AlarmManagment agent to their required routes as an output agent, as follows:In the **Routes** dialog, of each of these Alarm agents, select the required route number and add this AlarmManagement agent to the **Output** agent list. Do this for each of the required routes.

3. Edit the AlarmManagement agent to display the **Edit AlarmManagement Agent** dialog.

4. Specify the location to the SQL database in the **Connection** field.

   Use an existing (or create) a SQL database for your alarm management.

   Note1: If you do not have SQL installed then install SQL Server 2008 R2 or its Express version.

   Note2: If multiple AlarmManagement agents (possibly from different Agent Servers) connect to the SAME database, then ensure that each agent is UNIQUELY named since incidents are logged using the name of its assigned AlarmManagement agent.

   Click the browse button ... to the right of this field and use the **Data Link Properties** dialog to create the required connection string to your SQL Server database, as follows:

   This **Data Link Properties** dialog specifies the location and the security credentials required to connect to this database.

   Note: If you need to configure or view this database and its data from other computers, like remote User Interfaces, then use a UNC path and not a local file system path to specify the location of this database.

   A. Double click the **Microsoft OLE DB Provider for SQL Server** item in the **Provider** tab of the **Data Link Properties** dialog.

   - Either type in the computer name of the SQL Server that you want to connect to, in the **Select or enter a server name** field.

     Tip: This is the fastest method, if you know the name of the SQL Server.

   - Or click the button to the left of the **Select or enter a server name** list box and select the name of the required SQL Server from the list.

   B. Specify the required security credentials to connect to this SQL Server, as follows:

   IMPORTANT1: If you need to connect to a remote SQL database and want to run the Agent Server service using the **Local System account**, then use **SQL Server Authentication**.

   IMPORTANT2: If you need to connect to a remote SQL database and want to **Use Windows NT Integrated security**, then ensure that the user profile that the Agent Server service uses to log onto the computer HAS the necessary rights to browse the network and connect to the remote database. This should **NOT** be the default **Local System account.**

   - **Use Windows NT Integrated security:** this option uses the username and password of the currently logged on Windows user.

     Tip: We recommend that you configure your SQL Servers to use this option to avoid requiring additional database security.

   - **SQL Server Authentication:** this option uses the **User name** and **Password** configured within the SQL Server you are attempting to connect to.

     Note: In this case it is recommended to check the **Allow saving password** checkbox.

C. Select the name of the required database from the **Select the database on the server** list box.

D. Click the **Test Connection** button to ensure that you are able to connect to this database using these details. Only proceed once 'Test connection succeeded' is displayed.

E. Click the **OK** button.

Your connection string will be created.

Note1: The **Advanced** tab of this dialog allows you to specify access permissions for this connection string. If you are unsure about these settings NEVER set these permissions to **Read** otherwise this connection string will fail.

Note2: These security credentials are database specific and should not be confused with application security.

Note3: You can edit this string directly, once it has been created, if necessary.

PLEASE NOTE:You CANNOT connect to an MS Access database because of its known performance issues - please a MS SQL database instead.

Note: Please use a UNC path when referring to this database instead of a local file system path, if you need to display or the **Show data** and **Show graph** dialogs from mimics on remote clients.

Once you add your incidents to this database, you can obtain statistical information about these incidents by querying this data and analyzing these queries.

Note: Currently this agent only provides correctly formatted queries for MS Access and SQL databases.

5. Use the **Housekeeping** section to specify how long, in days, that you want to store your logged alarms/events. This depends upon the storage capacity you have available for your database and how useful this data becomes to you the older it gets.

   By default, this is disabled, which means that you need to perform the required housekeeping.

   Note: You cannot specify an number of days less than 30, since you need some historical records to determine your alarming trends.

6. Use the **Shift times** section to specify the starting times of your shifts (the **shift1Time**, **shift2Time** and **shift3Time** slots), as each incident specifies the shift number in which it occurs. In other words:

   Any incident that occurs between **shift1Time** and **shift2Time**, is logged as a Shift 1 incident.

   Any incident that occurs between **shift2Time** and **shift3Time**, is logged as a Shift 2 incident.

   Any incident that occurs between **shift3Time** and **shift1Time**, is logged as a Shift 3 incident.

   Note: Instead of configuring this shift pattern information here, you can instead configure these shift patterns globally, by using a Shift agent. For details, see Configuring the Shift agent.

   Tip: If you only have two shifts then specify the same shift time for shift two and three.

7. Ensure that the **Start Alarm Management Agent** checkbox (the **enable** slot) is checked, to start adding incidents to the selected database.

   By default, all the incidents (the alarms and/or events that occur on the routes of the alarm agent/s you configured in step 2) are added to the **_Uncategorised** category of the **Categories** tree.

8. If you have clustered Agent Servers that both log incidents to the same database then check the **Disable recording on standby server** checkbox (the **disableStandby** slot) to prevent double entries from being added.

9. Typically you will create your own hierarchical (logical) structure of categories for your incidents, in the **Categories** tree, **as follows:**

   Tip: This edit dialog can be maximized and resized to enlarge the screen area to design and view this **Categories** tree.

   Adding Categories: Categories 🌐 can make your incidents easier to query and analyze. For more details, see Reasons for categorizing your incidents.

Configuring Categories: Where necessary, specify the 'Operator tag' setting for categories that represent sections of your process that are controlled by different operations. To ensure that the incidents you assign to this category (and if necessary its sub-categories) are logged using the name of the correct operator.

Adding Incidents: To add new and existing incidents to categories in the **Categories** tree.

Note1: You can only assign an incident to a SINGLE category.

Note2: The color of the incident icon indicates whether reasons and/or notes are required or not for this incident. For details, see Incident icon colors.

Removing Incidents: To reassign incidents to other categories or to permanently remove an incident from the alarm management database.

Configuring Incidents: You can configure one or more optional settings for each incident to improve the efficacy of your alarm management configuration.

Note: These configuration settings do not affect the manner in which the legacy Adroit alarming functions.

Tip: You can use the **Export** button to save and/or bulk configure categories and their incidents within a .CSV file instead. For details, see Exporting categories and their incidents.

Note: When you add an incident to a category, this is NOT an actual alarm/event, but instead represents and configures all the alarms/events that exist for this specific incident.

Tip: To quickly categorize your incidents, click the **Learn alarms** (incidents requiring acknowledgement) and/or **Learn events** (incidents NOT requiring acknowledgement) buttons to add ALL the applicable unassigned incidents, that are routed to this alarmmanagement agent, to the **_ Uncategorised** category.

10. The **Edit reasons...** button displays the **Edit reason and sub-reason categories dialog** for you to populate these entries for this AlarmManagement agent. For details, see Editing reasons and sub-reasons.

11. The **Edit KPI's...** button displays the **Edit Alarm Management KPI values** dialog for you to change the KPI target values used by certain default queries and your own custom KPI queries, so that these queries better comply with your specific requirements. For details, see Customizing KPI target values.

12. The **View data...** button displays a dialog to use queries to analyze the logged incidents and display the results in a grid or table. For details, see Querying recorded incidents.

    Tip: You can also launch this dialog directly from a Classic UI mimic. For details, see Launching the View Data dialog.

13. The **View graph...** button displays a dialog to use queries to analyze the logged incidents and display the results graphically, as a chart. For details, see Viewing Incident Queries Graphically.

    Tip: You can also launch this dialog directly from a Classic UI mimic. For details, see Launching the View Graph dialog.

14. The **View reasons...** button displays a dialog that ONLY lists the current incidents that still require reasons and/or notes to be specified. If necessary, these reasons and/notes can be specified for these incidents from this dialog. For details, see Viewing Incidents Requiring Reasons and/or Notes.

    Tip: You can also launch this dialog directly from a Classic UI mimic. For details, see Launching the View Reasons Dialog.

    WARNING! We do NOT RECOMMEND using the **View data** and **View graph** dialogs for an alarm management database that contains a huge number of historical incidents - this can cause your system to become unstable.

    Note: Although these dialogs can help you to analyze this data, we recommend that you use a 3rd party application (such as VIZNET and/or OPUS) to report and analyze this data more effectively. For details of the database (the tables and their fields) that is maintained by the AlarmManagement agent, see About the AlarmManagement Database.

PLEASE NOTE: If you need to display the **View data, View graph** and/or **View reasons** dialogs from mimics on remote clients, then please use a UNC path when specifying the OLE DB database of this AlarmManagement agent, otherwise you will NOT be able to DISPLAY these dialogs.

The AlarmManagement agent provides a number of common KPIs and allows you to create up to 6 user-defined KPI values (single value queries) from the database to measure the effectiveness of your operators and/or alarming system. For details, see Obtaining KPI Values.

15. The **Export alarm cfg** button, saves Adroit's complete alarming sub-system configuration to the Adr_AM_AlarmConfigurationDump table of the alarm management database. For details, see Exporting the Alarming Configuration of Adroit.

Working with Categories

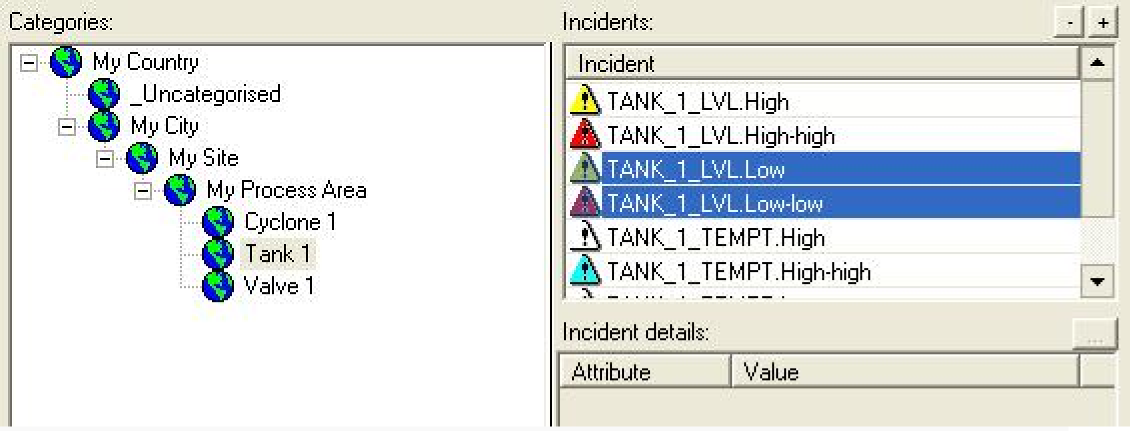
Categories in the **Categories** tree of the **Edit AlarmManagement Agent** dialog perform the following functions:

- To define the areas of your process that different operators control and/or
- To provide a logical framework to make your incidents easier to query.

Example:

Categories tree shows a hierarchical structure of the categories, while the top right-hand **Incidents** list displays all the incidents in the selected category and the bottom right-hand **category/incident details** list displays the selected category/ incident configuration.

Note: The incident details list is disabled when more than one incident is selected.



For a detailed description of why you should group incidents under categories, see Reasons for categorizing your incidents.

Arrange categories hierarchically: by adding, renaming or moving categories within categories:

Examples of possible levels of categories in a hierarchy of incidents:

- Country (e.g. South Africa)
- City (e.g. Johannesburg)
- Site (e.g. Kya Sands)
- Process area (e.g. Cement Plant)
- Unit name (e.g. Kiln001)
- PID number (e.g. PID0401)
- Instrument tag number (e.g. STP0445)

Note: All the categories and sub-categories that you add are automatically sorted alphanumerically.

To add a category:Right-click a category, such as the default **Root** category, and select **Add category...**.

To arrange categories hierarchically:
Add categories within categories.
For instance, you can include levels for:

- Country (e.g. South Africa)
- City (e.g. Johannesburg)
- Site (e.g. Kya Sands)
- Process area (e.g. Cement Plant)
- Unit name (e.g. Kiln001)
- PID number (e.g. PID0401)

Note: You can only add categories to the default **Root** category.

To rename a category:

1. Click the category to select it.
2. Click the category again and type in the required label.

To move a category:

1. Drag the category to the required position in the tree.

   Note: If you move or modify a category this affects all the sub-categories too.

To delete a category:

1. Right click the category and click the **Delete** menu item.

   Note1: You can only delete a category if it does not contain incidents or sub-categories.

   Note2: You cannot delete the default **Root** category, although you can rename it, if necessary.

Configuring Categories: Where necessary, specify the 'Operator tag' setting for categories that represent sections of your process that are controlled by different operations.

To ensure that the incidents you assign to this category (and if necessary its sub-categories) are logged using the name of the correct operator.

Tip1: You can use the **Export** button to save and/or bulk configure this **Categories** tree within a .CSV file instead. For details, see Exporting the categories and their incidents.

Tip2: To quickly categorize your incidents, click the **Learn alarms** (incidents requiring acknowledgement) and/or **Learn events** (incidents NOT requiring acknowledgement) buttons to add ALL the applicable unassigned incidents, that are routed to this alarmmanagement agent, to the **_Uncategorised** category.

Reasons for categorizing your incidents

By default, all the incidents assigned to the alarm routes that use this AlarmManagement agent are added to the _**Uncategorised** category of its **Categories** tree.

Typically you will create and use categories 🌍 for your incidents for one or both of the following reasons:

A. The more incidents in the **_Uncategorised** category, the harder it becomes to differentiate between these incidents.

   For this reason, you can create other categories to distinguish between the following:

   - different areas or sections of your process, such as crushing, flocculation etc.
   - different equipment within each of these areas and if necessary down to the individual tag level.

   Adding categories allows you to easily query (analyze) or report ONLY the incidents that you are interested in, instead of ALL the incidents, so that you can manage this data more effectively.

B. Categories also allow you to provide the name of the Operator that is responsible for the incidents allocated within it (and if necessary its sub-categories). This name is logged with these incidents, for auditing purposes.

   Therefore, this setting only applies to categories that represent areas of your process that have different operators overseeing them.

   The default **_Uncategorised** category is simply provided to make you aware of the incidents that you have not categorized. Therefore **this category does NOT allow you to assign an operator name** to these logged incidents.

Tip: To quickly categorize your incidents, click the **Learn alarms** (incidents requiring acknowledgement) and/or **Learn events** (incidents NOT requiring acknowledgement) buttons to add ALL the applicable unassigned incidents, that are routed to this alarmmanagement agent, to the **_Uncategorised** category.

Configuring Categories

Categories identified by the 🌍 icon, allow you to provide a tag that specifies the name of the Operator that is responsible for the incidents allocated within it (and if necessary its sub-categories). This name is logged with these incidents, for auditing purposes.

Therefore, this setting only applies to categories that represent areas of your process that have different operators overseeing them.

When logging an incident to the database, the incident uses the 'Operator tag' specified for the category that is CLOSEST to this incident. **For instance:**

If the **Categories** tree is configured as follows:

- An operator named **Kobus** was responsible for the **Country** (level 0 or Root category)
- An operator named **Jaco** was responsible for the **Process Area** (level 3 in the category hierarchy).

If the **Operator tag** settings are configured for these categories and the TANK_1_LEVEL.High incident occurs within the Tank01 category (level 4 in the category hierarchy).

Then this incident is logged to the database with the operator name of **Jaco**, as this is the CLOSEST configured **Operator tag** for this incident.

To specify the operator name tag for a category:

1. Edit the required AlarmManagement agent.
2. Click the required category 🌍 in the **Categories** tree.
3. Double-click the **Value** cell next to the **Operator tag** in the **Attribute** column of the bottom right-hand **category details** list.

   This launches the tag browser dialog to specify this tag. For details, see Selecting a tag.
4. Specify the tag used for the **Operator tag name** setting of the applicable Classic User Interface.

   Tip: If you need to configure this setting for a large number of categories, then you may want to Export your categories and then perform this configuration in the exported .CSV file instead.

For details on locating the **Operator tag name** setting for an Classic User Interface, see Advanced UI Workspace settings.

Incident Icon Colors

The color of the incident icon indicates whether reasons and/or notes are required or not for this incident, as follows:

- The white icon ⚠ means that no reasons or notes are required.
- The yellow icon ⚠ means that ONLY reasons must be specified.
- The blue icon ⚠ means that ONLY notes must be specified.
- The red icon ⚠ means that BOTH reasons and notes must be specified.

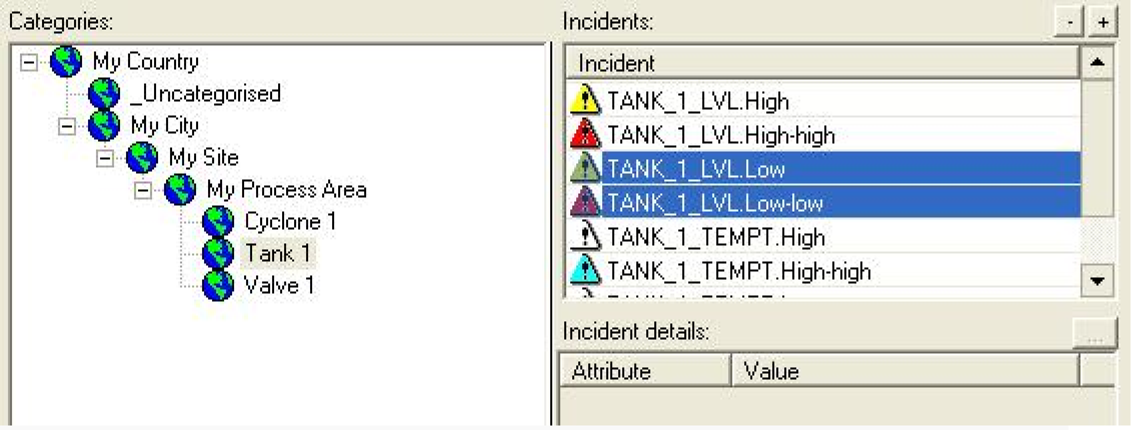
These colored icons indicate what the operator MUST specify for an incident before it is removed from the **Adr_AM_CurrentIncidents** table and is added to the **Adr_AM_HistoricalIncidents** table.

Note: Even though reasons and/or notes may not be required, they can still be specified.

Example:

Categories tree shows a hierarchical structure of the categories, while the top right-hand **Incidents** list displays all the incidents in the selected category and the bottom right-hand **category/incident details** list displays the selected category/ incident configuration.

Note: The incident details list is disabled when more than one incident is selected.



Categories:

- My Country
  - _Uncategorised
  - My City
    - My Site
      - My Process Area
        - Cyclone 1
        - Tank 1
        - Valve 1

Incidents:

Incident
TANK_1_LVL.High
TANK_1_LVL.High-high
TANK_1_LVL.Low
TANK_1_LVL.Low-low
TANK_1_TEMPT.High
TANK_1_TEMPT.High-high

Incident details:

Attribute	Value

Adding Incidents

Both new and existing incidents can be added to the categories you create in the **Categories** tree of the **Edit AlarmManagement Agent** dialog, as follows:

Note1: You can only assign an incident to a SINGLE category.

Note2: Incident names are automatically sorted alphanumerically.

ONLY the incidents assigned to the alarm routes that use this AlarmManagement agent will be logged to this database.

In other words, just because you have added an incident to this categorization tree does not automatically mean that it will be logged to this database.

To add one or more existing incidents: Typically used to categorize incidents currently in the default **_ Uncategorised** category.

1. Select the required category in the **Categories** tree
2. Select one or more of the incidents listed in the top right hand **Incidents** list.
3. Drag the selected incident/s to the required category in the **Categories** tree.

   Note: In this case this new Category ID is applied to any occurrences of the incident/s in the current and historical tables.

   Tip: If you cannot see the required category, when dragging then hold the selected incident/s over the collapsed category, to expand all of its sub-categories.

To add one or more new incidents: Typically used to add one or more incidents directly from the alarm routes.

1. Add or locate the required category in the **Categories** tree.
2. EITHER Right-click this category and select the **Add incident...** item OR click the **Add Incident** + button above the top right hand **Incidents** list.

   This displays the **Add incident** dialog.
3. Select the required Alarm agent from **Alarm agents** list (the left list).
4. Select the number of the required alarm route of this Alarm agent from the **Routes** list (the middle list).

   If the required alarm route is designated by "# - unrouted" then this AlarmManagement agent has NOT been added to this route.

   Click the **Add to route** button To add this AlarmManagement agent to this route.

   The incidents assigned to the selected route, that this AlarmManagement agent is added to, are displayed in the **Incidents** list.
5. Select the required incident/s that you would like to add to this category from the **Incidents** list (the right list).

Note: You cannot assign incidents to a category if they already exist in another category, such as the **_Uncategorised** category.

6. Click the **OK** button, to add the selected incident/s to the category.

   Tip: You can also add an incident by double clicking it, which also closes this dialog.

Tip: To quickly categorize your incidents, click the **Learn alarms** (incidents requiring acknowledgement) and/or **Learn events** (incidents NOT requiring acknowledgement) buttons to add ALL the applicable unassigned incidents, that are routed to this alarmmanagement agent, to the **_Uncategorised** category.

Removing Incidents

Since you can only assign an incident to a SINGLE category, you may want to remove an incident from one category and assign it to another. In this case either:

- drag the incident to the required category, this reassigns this incident immediately or
- select the required incident/s in the top right hand **Incidents** list and click the **Delete Incident** button. The deleted incident/s will be added to the **_Uncategorized** category when they re-occur.

To permanently remove an incident from an AlarmManagement agent:

- either remove this alarm type for this agent (add it to the **Available** list) OR
- reassign this incident to a route NOT assigned to a route on which this AlarmManagement agent is allocated

BEFORE deleting it from the database.

Optional Incident Configurable Settings

Each incident in the **Categories** tree of the **AlarmManagement Agent** edit dialog of an AlarmManagement agent provide a number of optional settings.

If you diligently configure these settings then you will improve the efficacy of your alarming configuration and ensure that each alarm complies with the industry-approved effective alarm characteristics.

Note: The color of the incident icon indicates whether reasons and/or notes are required or not for this incident. For details, see Incident icon colors.

Tip: You can also bulk configure these settings for all your incidents by exporting the **Categories** tree to a .CSV file. For details, see Exporting the categories and their incidents.

To manually configure a setting for a SINGLE incident:

1. Edit the required AlarmManagement agent.
2. Click the required category in the **Categories** tree.
3. Click the required incident in the top right hand **Incidents** list.
4. Double-click the **Value** cell next to the required entry in the **Attribute** column of the bottom right-hand **incident details** list.

Note: You are UNABLE to configure incident settings when you select MORE THAN ONE incident from the top right hand **Incidents** list.

The following OPTIONAL settings can be specified for each incident:

1. **Reason required:** When enabled (Yes), this enforces the entry of reasons for this incident. In other words when this incident is raised, the operator must specify a reason before this incident is removed from the **Adr_AM_CurrentIncidents** table and added to the **Adr_AM_HistoricalIncidents** table. Click for more details:

   A reason is simply the selection of the cause of the incident from a user-configurable list of reasons and, if necessary sub-reasons, which you need to specify.

   Note: Click the **Edit reasons...** button to edit the displayed reasons and their sub reasons for this AlarmManagement agent.

Tip: Operators can specify these reasons and/notes from the right-click menu of the Alarm List Viewer window.

2. **Notes required:** When enabled (Yes), this enforces the entry of notes for this incident. In other words when this incident is raised, the operator must specify a reason before this incident is removed from the **Adr_AM_CurrentIncidents** table and added to the **Adr_AM_HistoricalIncidents** table.

   A note is specific text that the operator must type in that is supplements a reason or replaces the need for a reason.

3. **AssociatedTags:** Specify one or more values to record with the incident.

   These values ensure that the alarm is relevant in that it provides the operator with information to respond to. If you are manually specifying this value, separate multiple tags with commas ",".

   To add a value:Double click the **AssociatedTags** row and use the in-built Tag browser to select the required tag. For details, see Selecting a Tag.

   To remove ALL the selected values:Select the **AssociatedTags** row and press the DELETE key.

4. **Document:** An optional document that can provide further information to clarify the incident and assistance on how to deal with it or react to it. This document can ensure that this incident (alarm) satisfies the last four of the Effective Alarm Characteristics.

   If left empty, a default HTML document is created by this agent for each active incident. Click for more details about the location and naming convention of this default document:

   - This document is created in the Data subfolder of your designated project folder, which is typically C:\ProgramData\Adroit Technologies\Adroit\Configurations\Default\Data.
   - This document adheres to the following naming format: AgentName.AlarmType.HTM e.g. ANA001.High-High.htm. Either edit this document using an HTML editor of your choice or create your own document.
   - This document supports the **Adroit Path** as specified in the **UI Preferences** tab of the **Adroit Configuration Setup** utility, so if it occurs within one of these folders, you ONLY need to provide the file name and can exclude the path.

   Note1: You are warned when you specify a local file pathinstead of a UNC path to this document. A UNC path is required if you need to view this alarm (and open this document) on remote clients.

   Note2: Please configure the appropriate access permissions to this document from the NTFS to ensure that ONLY the required users are able to edit this document. For details, see Securing Documents using NTFS.

Specify delays for incidents when you alarm agents in the Alarming configuration dialog. For details, see Delaying Incidents.

Specify conditional expressions for incidents when you alarm agents in the Alarming configuration dialog. For details, see Creating Conditional Expressions for Incidents.

Applying a condition ensures that incidents are unique and do not simply duplicate downstream alarms.

Effective Alarm Characteristics

The characteristic of an effective alarm is that it should be:

1. **Relevant:**requiring acknowledgment and corrective action i.e. NOT an event that can simply be ignored.
2. **Unique:** does not duplicate another alarm and is not a secondary consequence of a previous alarm.
3. **Timely:** is not triggered too long before any response is needed or too late to do anything. For instance, when monitoring for over temperature the High alarm is the most important event, not the High-High alarm because the damage is probably already done at this point!
4. **Prioritised:** indicates the importance with which the operator deals with the problem.
5. **Understandable:** has a message that is clear and easy to understand.
6. **Diagnostic:** identifies the problem that has occurred.

7. **Advisory:** indicates the action that is to be taken.
8. **Focusing:** draws attention to the most important issues.

While the AlarmManagement agent can ensure that the first four characteristics are met, the last 4 characteristics are supported within the Classic UI by assigning a document to each incident that is accessible from the alarm viewer.

For details about using the AlarmManagement agent, see Quick Start to Configure and Record Incidents (Alarms/Events).

For details about specifying a document for an incident, see Configuring Incidents.

Exporting categories and their incidents

The **Categories** tree of the **AlarmManagement Agent** edit dialog allows you to add and configure categories and incidents. You can use the **Export** button to save and/or edit these categories and incidents in a .CSV file editor instead.

Benefits:

- Ability to bulk add and/or configure categories and/or their incidents.

  Note: If necessary, you change the category of an incident to another existing category, in which case this new Category ID is applied to any occurrences in the current and historical tables.

- Ability to save your existing configuration to import this configuration into another AlarmManagement agent (in this case save this .CSV file to the name of the required agent first before importing it).

To export/import categories and their incidents: this described the process involved when bulk configuring the categories and/or incidents of the **Categories** tree for an **AlarmManagement agent.**

1. Click the **Export** button in the **AlarmManagement Agent** edit dialog.

   Note: A message box is displayed if there is nothing to export.

   This exports a .CSV file to the **Work** subfolder of your designated project folder, which is typically C:\ProgramData\Adroit Technologies\Adroit\Configurations\Default\Work. This file typically has the same name as this AlarmManagement agent.

   If you have MS Excel installed then this file opens in it, otherwise it opens in your default .CSV file editor.

2. Save this file, once you have performed the necessary changes to it and closed your .CSV editor.
3. Click the **Import** button in the **AlarmManagement Agent** edit dialog.
4. Specify the required .CSV to import, by default the file with the same name as this AlarmManagement agent is selected.

   Note: The imported changes are immediately made to the **Categories** tree, so you do not have to click the **Update** button.

The exported file contains the following columns: this describes the columns of this file and the possible reason for configuring each of them.

1. **Category:** This column specifies a separate entry (row) for each category in the hierarchical structure you create and a row for each of the incidents assigned to a category.

   The hierarchical structure of categories is represented in dot notation. For instance: Root.Category 1.Category 2. This makes it possible to:

   - rename and move categories as required and
   - move incidents and add other incidents as required.

2. **Operator tag:** This category-specific column specifies the tags that identify which operator names should be used when logging incidents within each category.

   Note: This column only applies to the categories that represent specific areas of your process that are managed by different operators.

3. **Incident:** This column specifies unique incidents (AgentName.AlarmType) for each of the categories.

   Note: If you specify the same incident for two categories ONLY the first incident is imported. If one of these incidents is already added to the incident tree, then the duplicate is discarded regardless of its position in the tree.

4. The other incident-specific columns, specify their optional configurable settings. For more details on their configuration, see Optional Incident Configurable Settings.

Editing Reasons and Sub-reasons

It may or may not be necessary to specify a reason for an incident before the incident can be removed from the Current Incident list for an AlarmManagement agent. Specifying a reason involves selecting of the cause of the incident from a user-configurable list of reasons and, if necessary sub-reasons.

To specify the reasons and sub-reasons:

1. Select the required AlarmManagement agent. For details, see Selecting agents.
2. Double click this agent to edit it.
3. Click the **Edit reasons...** button in the **Edit AlarmManagement agent** dialog.

   This displays the **Edit reason and sub-reason categories** dialog, which allows you to perform the following:

   To add a new reason:

   a. Click the **Add new reason...** button above the listed **Reasons**.
   b. Type in the name of a unique reason and click the **OK** button.

   The reason is added to the **Reason** list.

   To edit an existing reason:

   a. Select the required reason from the **Reason** list.
   b. Click the **Edit selected reason...** button above the listed **Reasons**.
   c. Edit this name and click the **OK** button.

   The updated name of this reason is added to the Reason list.

   To remove an existing reason and its sub-reasons:

   a. Select the required reason from the **Reason** list.
   b. Click the **Delete selected reason...** button above the listed **Reasons**.
   c. Click **Yes** to confirm that you want to delete this reason and ALL of its sub-reasons, if any.

   The selected reason and all of its sub-reasons are removed.

   To add a new sub-reason:

   a. Select the required reason from the **Reason** list.
   b. Click the **Add new sub-reason...** button above the listed **Sub-reasons**.
   c. Type in the name of a unique sub-reason and click the **OK** button.

   The sub-reason is added to the **Sub-reason** list.

   To edit an existing sub-reason:

   a. Select the required reason from the **Reason** list.
   b. Select the required sub-reason from the **Sub-reason** list.
   c. Click the **Edit selected sub-reason...** button above the listed **Sub-reasons**.
   d. Edit this name and click the **OK** button.

   The updated name of this sub-reason is added to the **Sub-reason** list.

   To remove an existing sub-reason:

   a. Select the required reason from the **Reason** list.
   b. Select the required sub-reason from the **Sub-reason** list.
   c. Click the **Delete selected sub-reason** button above the listed **Sub-reasons**.

The selected sub-reason is removed.

Querying Recorded Incidents

The AlarmManagement agent provides a dialog from which you can perform various statistical queries to analyze the logged incidents.

Many of these queries are derived from the EEMUA 191 guidelines. The incidents returned by these queries are displayed in a table, the columns of which are determined by the selected query.

Note: While this dialog allows you to analyze your logged incidents, we recommend that you use a 3rd party application (such as the Alarm Management and Analysis reporting utility) which is more suited to report and analyze this data.

Tip: This dialog can be resized and maximized and its last size and position is saved for the current UI session.

The currently selected **Query**, changes the following items of this dialog:

- The title of this dialog to the name of this query.
- The description of the selected query.
- The columns of the table used to display the incidents returned by the query.
- The available constraints.
- The available user interaction with the displayed incidents.

This dialog provides a number of default queries. For details, see Default Alarm Management Queries.

Note: If necessary, you can add your own queries to this list.

Certain queries support one or more of the following Constraints: These constraints are displayed by clicking the **Constraints...** button and can further refine the returned data. In other words they can eliminate unnecessary data.

1. **Top:** If enabled, specify the topmost number of incidents for this query to return.

   For instance, when the table records are ordered by time in ascending order, the specified number of the most recent records are returned.

   Likewise, when the table records are ordered by time in descending order, the specified number of the oldest records are returned.
2. **From:** If enabled, specify the date and time of the start of the interval of analysis.
3. **To:** If enabled, specify the date and time of the end of the interval of analysis.

   The **Now** button, if clicked, will return the incidents that have been added in the last day, by setting the **To** field to the current date and time and the **From** field to one day before the current date and time.
4. **Or use shift times:** If enabled, specify the required shift number to only view incidents that occur within this shift.
5. **Operator:** If enabled, select the name of the required operator from the list to only view the incidents that are logged to this operator.
6. **Category**If enabled, select the name of the required category (as specified in the **Incident categorization**(tree) containing the incidents that you are interested in.

PLEASE NOTE: These constraints are provided by adding special constraint parameters to these queries, so it is NOT possible to execute any queries that contain constraint parameters from 3rd party applications.

To change the frequency at which the data in the table is updated: This will determine how often this query is performed on the database to include the latest logged incidents in the current chart.

- Specify the required interval in the **Auto-refresh (secs)** spin control.

  Note: A value of 0 disables this automatic refreshing.

  Tip: Click the **Refresh** button to immediately perform the selected query on the database to include the latest logged incidents in the table.

This dialog provides the following grid configuration options, which allow you to configure both the table (grid) and the displayed incidents:

The following interaction options are always enabled:

To sort the table entries by a column:

- Click the required column heading.

  This column heading displays the » character when the rows of this table are sorted so that the contents of this column are displayed in ascending order.

  This column heading displays the « character when the rows of this table are sorted so that the contents of this column are displayed in descending order.

To change the widths of individual columns: This can be used to hide an unnecessary column from view.

- Drag the right hand side of the column left or right, as required.

  Note: The changes made to the column widths are saved for the currently selected query.

To resize the columns of the table to the width of their largest entry: this resets any changes that have been made to the column widths and displays any hidden columns.

- Right-click the table and select **Show all columns**.

  Note: The changes made to the column widths are saved for the currently selected query.

To export the table or grid to a CSV file: This allows you to view the data in a 3rd party application.

- Click the **Export...** button.

  This will open this file in the default .CSV file editor.

The following user interaction options are only enabled in the following instances:

To display the results of this query in a chart: This is only enabled if the selected query can also be displayed graphically.

- Right click and select **View graph...** or click the **Graph...** button.

  For details of using this dialog, see Viewing Incident Queries Graphically.

ONLY the **Current Incidents** and **Historical Incident** queries provide the following options:

To display the HTML document associated with the selected incident: This document provides further information to clarify the incident and assistance on how to deal with it or react to it.

- Right-click an incident and select **View document.**

  The HTML document associated with this incident is displayed.

To edit the HTML document associated with this incident: To ensure that this document does provide further information to clarify the incident and assistance on how to deal with it or react to it.

- Right-click an incident and select **Edit document**.

  Note: Please configure the appropriate access permissions to this document from the NTFS to ensure that ONLY the required users are able to edit this document. For details, see Securing Documents using NTFS.

  The associated HTML document is displayed in the default HTML editor.

ONLY the **Current Incidents** and **Outstanding reasons and notes** queries provide the following option:

To specify the reasons and/notes for each incident in this dialog:

- Right-click an incident and select **Reasons/notes...** or click the **Reasons...** button. This displays the **Incident reasons and notes** dialog.

  For details of using this dialog, see Specifying Reasons and/or Notes for Incidents.

Adding your own Queries: This describes how you can add you own queries so that they too can appear in this View Data dialog.

Launching the View Data dialog: This describes how you can also launch this dialog directly from a Classic UI mimic.

Default Alarm Management Queries

The following queries are displayed by the **View data** and unless otherwise noted the **View graph** dialogs:

> **Tip:** You can change the KPI values that are used by these default queries, so that they better comply with your specific requirements. Click for more details:Click the **Edit KPI's** button in the **Edit Alarm-Management agent** dialog; in the **Edit Alarm Management KPI values** dialog, double click the appropriate KPI (row) to change its value.

Current incidents: All incidents whose alarmed conditions are still active and/or which have NOT been fully responded to. In other words they still need to be acknowledged and/or have their required reasons specified and/or have their required notes specified.

On the basis of 6 alarms per hour this should never have more than 6 incidents under normal operating conditions or 60 under abnormal operating conditions.

> **Note:** This query is NOT displayed by the **View graph** dialog.

Historical incidents: All incidents whose alarmed conditions have returned to normal and which have been fully responded to, if necessary, for the specified period of time. In other words they have been acknowledged and/or had their required reasons specified and/or had their required notes specified.

This can be used to analyze your alarm configuration during set time periods.

> **Note:** This query is NOT displayed by the **View graph** dialog.

Historical incidents by operator: Incidents which have been logged against the specified operator. This can be used to analyze the effectiveness of your operators.

> **Note:** This query is NOT displayed by the **View graph** dialog.

Historical incidents by category: Incidents which have occurred for a specific category. This can be used to analyze your alarm configuration for specific process areas.

> **Note:** This query is NOT displayed by the **View graph** dialog.

Outstanding reasons and notes: All incidents that still need reasons and/or notes specified. Only those current incidents that have their **Reasons required** and/or **Notes required** settings enabled are added to this list.

> **Note:** This query is NOT displayed by the **View graph** dialog.

Incident count per hour: The total number of incidents that occur over each hour of the specified duration. In other words this query returns the number of logged incidents per hour for the specified duration.

Typically each number should be between 6 (normal conditions) to 60 (abnormal conditions). But different industries have different standards.

Burst rate: The number of incidents that occur in a 10 minute window. **Calculation:Burst rate = 6 * Maximum alarm count in a 10 minute period. (this is calculated as a per hour count, hence the 6 *)**

This is an important measure of the usability of an alarm system and the operator's capability to deal with alarms. Typically this should be between 1 (normal conditions) to 10 (abnormal conditions). But different industries have different standards.

Percent upset: The number of hours where there are more than 30 incidents per hour. If you want to specify a more appropriate maximum number of alarms, then change the **PUC** [Percent upset count] entry in the Adr_AM_UserKPIs table. **Calculation:Percent upset = 100 * [Number of hours where alarms exceeds 30/hour]/[Total number of hours].**

This is a measurement of alarm overload on operators, as follows:

- Overloaded > 50%
- Reactive 25%-50%
- Stable 5%-25%
- Robust 1%-5%
- Predictive < 1%.

Priority distribution: The priority distribution for incidents occurring over a period of time.

Typically this should be 5% high priority alarms (>Normal priority), 15% medium priority alarms (=Normal priority) and 80% low priority alarms (<Normal priority). But different industries have different standards.

Standing alarms: The number of current incidents at the end of an hour.

Typically this should be 9. But different industries have different standards.

Most frequent alarms (count by type): The most frequent alarms over time. The top 20 of these alarms can account for almost 50% of total alarm generation.

If properly reviewed, you will find that most of these incidents should not be classified as alarms at all, since they do not meet the proper criteria that defines an alarm, namely that they need to be responded to.

Intermittent incidents: The incidents that activate and deactivate within 10 seconds. If you want to specify a more appropriate time interval, then change the **IAP** [Intermittent alarm period (secs)] entry in the Adr_AM_UserKPIs table.

If properly reviewed, you will find that most of these incidents should not be classified as alarms at all, since they do not meet the proper criteria that defines an alarm.

Note: This query is NOT displayed by the **View graph** dialog.

Intermittent counts: The number of incidents that activate and deactivate within 10 seconds. If you want to specify a more appropriate time interval, then change the **IAP** [Intermittent alarm period (secs)] entry in the Adr_AM_UserKPIs table.

If properly reviewed, you will find that most of these incidents should not be classified as alarms at all in that they do not meet the proper criteria that defines an alarm.

Count by agent: The number of incidents specified per agent. This shows the agents that generate the greatest and least number of incidents.

Count by operator: The number of incidents by operator. This shows of incidents that each operator has had to contend with.

Total active time by incident: The total amount of time individual incidents have remained active. This shows how quickly or slowly incidents are being responded to.

Total unacknowledged time by incident: The total amount of time individual incidents have remained unacknowledged. This shows how quickly or slowly incidents are being responded to.

Hourly count grouped by hour of the day: Indicates what time of day incidents tend to occur more frequently.

Hourly count by incident: The total number of individual incidents that occur per hour. This shows which incidents cause more noise during different times of the day.

Note: This query is NOT displayed by the **View graph** dialog.

Daily count: The total number of incidents occurring per day. This shows which incidents cause more noise during different times of the week.

Average acknowledge time: The average time it takes for incidents to be acknowledged. This is a measure of how quickly your operators respond to incidents.

Note: This query is NOT displayed by the **View graph** dialog.

Average acknowledge time per incident: The average time it takes for individual incidents to be acknowledged. This shows which incidents take longer to acknowledge and therefore is an indication of the amount of work an operator has to do for an incident before acknowledging it.

Average alarm rate: The average number of incidents that occur per hour over the specified time period. This query produces a single averaged value for the specified duration. Calculation:Average rate = [number of logged incidents]/[number of hours]

Typically this should be between 6 (normal conditions) to 60 (abnormal conditions). But different industries have different standards.

Bulk acknowledgement counts: The number of alarms acknowledged within a specific time period, typically 1 second. If you want to specify a more appropriate time interval, then change the **BAP** [Bulk acknowledgement period (secs)] entry in the Adr_AM_UserKPIs table.

This monitors the acknowledgement behaviour of operators. This count should be equal to the number of alarms over the same period indicating that each alarm is receiving proper attention/action.

Incidents not configured for acknowledgement: Lists the incidents that are not configured for acknowledgement. This advises the user that, by definition, these incidents are not alarms, but rather events.

Customizing KPI target values: If necessary you can set KPI target values used by your own custom KPI queries and certain default queries to better comply with your specific requirements.

Adding your own Queries

PLEASE NOTE: This help topic assumes that you are familiar with working with databases and creating SQL queries.

Instead of only using the default queries to analyze your logged incidents, you can add your own queries to the **Adr_AM_UserQueries** table of the AlarmManagement database. Then these queries will also appear in the View Data and View Graph dialogs of this AlarmManagement agent.

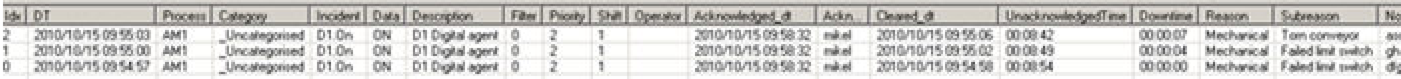
WARNING! It is recommended that you do NOT edit any table in this database, apart from **Adr_AM_UserKPIs** and **Adr_AM_UserQueries**; otherwise you WILL lose data.

Note: If you want to remove the queries you have created, simply delete the **Adr_AM_UserQueries** table and they will be re-created when the Agent Server starts up.

First you need to create the SELECT SQL statement for your query. In this example, we will add a custom downtime reporting query that:

- Displays the actual reason and sub reasons (not just their IDs)
- Displays the downtime in the hh:mm:ss time format
- Displays the category name instead of the category ID
- Displays the incident name instead of simply the incident ID
- Displays the unacknowledged time in the hh:mm:ss time format

Example entries returned by this custom query:



Idx	DT	Process	Category	Incident	Data	Description	Filter	Priority	Shift	Operator	Acknowledged_dt	Ackn...	Cleared_dt	UnacknowledgedTime	Downtime	Reason	Subreason	No
2	2010/10/15 09:55:03	AM1	_Uncategorised	D1.On	ON	D1 Digital agent	0	2	1		2010/10/15 09:58:32	mikel	2010/10/15 09:55:06	00:08:42	00:00:07	Mechanical	Torn conveyor	as
1	2010/10/15 09:55:00	AM1	_Uncategorised	D1.On	ON	D1 Digital agent	0	2	1		2010/10/15 09:58:32	mikel	2010/10/15 09:55:02	00:08:49	00:00:04	Mechanical	Failed limit switch	gh
0	2010/10/15 09:54:57	AM1	_Uncategorised	D1.On	ON	D1 Digital agent	0	2	1		2010/10/15 09:58:32	mikel	2010/10/15 09:54:58	00:08:54	00:00:00	Mechanical	Failed limit switch	dg

Note: the **Category** name (instead of CategoryId) column, the display format of the **UnacknowledgedTime** and **Downtime** columns and the textual descriptions provided in the **Reason** and **Subreason** columns.

The SQL syntax for this query is, as follows:

SELECT TOP %t Adr_AM_HistoricalIncidents.Idx,DT,Process,Adr_AM_Categories.Category AS Category,Incident,Data,Description,Filter,Priority,Shift,Operator,Acknowledged_dt,Acknowledged_by,Cleared_dt,convert(varchar,convert(datetime,1.0*UnacknowledgedTime / (60*24*24)),8) as UnacknowledgedTime,convert(varchar,convert(datetime,1.0*ActiveTime / (60*24*24)),8) as ActiveTime,Adr_AM_Reasons.Reason as Reason,Adr_AM_SubReasons.SubReason as Subreason,Notes FROM Adr_AM_HistoricalIncidents INNER JOIN Adr_AM_Categories ON Adr_AM_HistoricalIncidents.CategoryId = Adr_AM_Categories.CategoryId INNER JOIN Adr_AM_Reasons ON Adr_AM_HistoricalIncidents.ReasonId = Adr_AM_Reasons.Idx INNER JOIN Adr_AM_SubReasons ON Adr_AM_HistoricalIncidents.ReasonId = Adr_AM_SubReasons.ReasonIdx AND Adr_AM_HistoricalIncidents.SubReasonId = Adr_AM_SubReasons.Idx WHERE dt > '%b' AND dt < '%e' ORDER BY dt DESC

To add your own query:

1. Open SQL Server Management Studio and connect to the SQL Server that contains the database that the required AlarmManagement agent is connected to.
2. Display the **db.Adr_AM_UserQueries** table.
3. Right click this table and select **Edit top 200 rows**.

   This displays an editable grid of the queries.
4. Select the bottom new (NULL) record and type in the name of this custom query into the **Name** field e.g. “Custom downtime”.

   This is name that is displayed in the **Query** list box when selecting the query.

5. If necessary, provide the necessary **Description** to help your operators and other users to know what this query will return e.g. "Provides the actual reasons and the downtime in hh:mm:ss time format...".

6. Either type in the required SELECT SQL statement into the **Query** field or, in this case, paste it.

   Note: When pasting in a query, ensure that this SELECT SQL statement copies as a SINGLE line without any carriage returns!

7. Select the next NULL record to commit (save) this query (newly edited record).

8. Restart the Classic User Interface and open the **View Data** dialog of this AlarmManagement agent to use this new query.

   You will now find a new query called "Custom downtime" in the **Query** list.

Other things you can do:

- If necessary your query can support:

  One or more of the following constraints: these constrains are provided by the **View data** dialog so that your users can choose which incidents they need to analyze.

  - **Top**(%t): This allows your users to specify the number of topmost (most recent) incidents that are to be returned by the query.

    For instance, this %t constraint is used by the "Most frequent alarms (count by type)" query, as follows: SELECT TOP(%t) Incident, Count(Idx) AS [Count] FROM Adr_AM_HistoricalIncidents WHERE dt > ''%b'' AND dt < ''%e'' GROUP BY Incident ORDER BY Count DESC

  - **From**(%b) and/or **To**(%e): These constraints allow your users to specify the time period during which the required incidents occur.

    For instance: WHERE dt > #%b# AND dt < #%e#

    If necessary, you can provide ONLY one of these constraints, without the other. For instance: WHERE dt > #%b#

  - **Now** (%now). This allows users to specify the current date and time.

    For instance you can obtain the last 8 hours in SQL by using the following expression: WHERE dt > DATEADD(Hour, -8, '%now') AND dt < GetDate()

  - **Shift times:** This constraint is enabled when you specify the **From** (%b) and/or **To** (%e) constraints (see above), which allows your users to specify the shift during which the required incidents occur.

  - **Operator** (%o). This allows your users to display all the incidents that are logged against a specific operator.

    For instance: WHERE Operator='%o'

  - **Category** (%c). This allows your users to display all the incidents that are logged for a specific category.

    For instance: WHERE CategoryId='%c'

  One or more of the following KPI target values: these are the ideal values that you want to achieve.

  - **Average alarm rate** (%AAR). This per hourly count is 6 by default.

    For instance, this %AAR KPI target value is used by the "Most frequent alarms (count by type)" query, as follows: SELECT TOP(%t) Incident, Count(Idx) AS [Count] FROM Adr_AM_HistoricalIncidents WHERE dt > ''%b'' AND dt < ''%e'' GROUP BY Incident ORDER BY Count DESC

  - **Burst rate** (%BR). This per hourly count is 60 by default.

    For instance, this %AAR KPI target value is used by the "Most frequent alarms (count by type)" query, as follows: SELECT TOP(%t) Incident, Count(Idx) AS [Count] FROM Adr_AM_HistoricalIncidents WHERE dt > ''%b'' AND dt < ''%e'' GROUP BY Incident ORDER BY Count DESC

  - **Percent upset count** (%PUC). This number is 30 by default.

For instance, this %AAR KPI target value is used by the "Most frequent alarms (count by type)" query, as follows: SELECT TOP(%t) Incident, Count(Idx) AS [Count] FROM Adr_AM_HistoricalIncidents WHERE dt > ''%b'' AND dt < ''%e'' GROUP BY Incident ORDER BY Count DESC

- **Percent upset** (%PU). This percentage is 2 by default.

  For instance, this %AAR KPI target value is used by the "Most frequent alarms (count by type)" query, as follows: SELECT TOP(%t) Incident, Count(Idx) AS [Count] FROM Adr_AM_HistoricalIncidents WHERE dt > ''%b'' AND dt < ''%e'' GROUP BY Incident ORDER BY Count DESC

- **Intermittent alarm period** (%IAP). This time period in seconds is 10 by default.

  For instance, this %AAR KPI target value is used by the "Most frequent alarms (count by type)" query, as follows: SELECT TOP(%t) Incident, Count(Idx) AS [Count] FROM Adr_AM_HistoricalIncidents WHERE dt > ''%b'' AND dt < ''%e'' GROUP BY Incident ORDER BY Count DESC

- **Bulk acknowledgement period** (%BAP). This time period in seconds is 1 by default.

  For instance, this %AAR KPI target value is used by the "Most frequent alarms (count by type)" query, as follows: SELECT TOP(%t) Incident, Count(Idx) AS [Count] FROM Adr_AM_HistoricalIncidents WHERE dt > ''%b'' AND dt < ''%e'' GROUP BY Incident ORDER BY Count DESC

- **Average alarm duration** (%ALD). This time period in seconds is 60 by default.

  For instance, this %AAR KPI target value is used by the "Most frequent alarms (count by type)" query, as follows: SELECT TOP(%t) Incident, Count(Idx) AS [Count] FROM Adr_AM_HistoricalIncidents WHERE dt > ''%b'' AND dt < ''%e'' GROUP BY Incident ORDER BY Count DESC

- **Average acknowledgement duration** (%AKD). This time period in seconds is 10 by default.

  For instance, this %AAR KPI target value is used by the "Most frequent alarms (count by type)" query, as follows: SELECT TOP(%t) Incident, Count(Idx) AS [Count] FROM Adr_AM_HistoricalIncidents WHERE dt > ''%b'' AND dt < ''%e'' GROUP BY Incident ORDER BY Count DESC

If necessary, you can customize these default KPI target values and/or add your own and reference them in your queries by using the % prefix. For details, see Customizing KPI target values.

Add your own KPI target values : once added, your custom queries can ALSO use these KPI target values!

- If you want the data returned by this query to be viewed as a chart, then specify which chart you want to use by configuring the **ChartType** field, as follows:
  - 1 = Bar chart
  - 5 = Pie chart
  - 6 = Line chart

Note: By default the **ChartType** field is -1, which indicates that you do not want this query to appear in the **View Graph** dialog.

Launching the View Data Dialog

WARNING! We do NOT RECOMMEND using this dialog for an alarm management database that contains a huge number of historical incidents - this can cause your system to become unstable.

The AlarmManagement agent provides a dialog that allows you to use queries to analyze its logged incidents and displays these results in a grid or table.

Typically this dialog will not be viewed by operators but instead by management in order to appraise the process alarming system.

PLEASE NOTE: If you need to display this dialog from mimics on remote clients, then please use a UNC path when specifying the OLE DB database of this AlarmManagement agent, otherwise you will NOT be able to DISPLAY this dialog.

Viewing Incident Queries Graphically

The AlarmManagement agent provides a dialog from which you can perform various statistical queries to analyze the logged incidents.

Many of these queries are derived from the EEMUA 191 guidelines. The incidents returned by these queries are then displayed in a chart.

WARNING! We do NOT RECOMMEND using this dialog for an alarm management database that contains a huge number of historical incidents - this can cause your system to become unstable.

Note: While this dialog allows you to analyze your logged incidents, we recommend that you use a 3rd party application (such as VIZNET and/or OPUS) which is more suited to report and analyze this data.

Tip: This dialog can be resized and maximized and its last size and position is saved for the current UI session.

The currently selected **Query**, changes the following items of this dialog:

- The title to the name of this query and displays its description.
- The description of the selected query.
- The default chart used to display the data (incidents) returned by the query.
- The available constraints.
- The information displayed by the **Legend** and/or **Labels** for this chart.

This dialog provides a number of default queries. For details, see Default Alarm Management Queries.

Note: If necessary, you can create your own queries.

Certain queries support one or more of the following Constraints: These constraints are displayed by clicking the **Constraints...** button and can further refine the returned data. In other words they can eliminate unnecessary data.

1. **Top:** If enabled, specify the **topmost** number of incidents for this query to return.

   For instance, when the table records are ordered by time in ascending order, the specified number of the most recent records are returned.

   Likewise, when the table records are ordered by time in descending order, the specified number of the oldest records are returned.
2. **From:** If enabled, specify the date and time of the start of the interval of analysis.
3. **To:** If enabled, specify the date and time of the end of the interval of analysis.

   The **Now** button, if clicked, will return the incidents that have been added in the last day, by setting the **To** field to the current date and time and the **From** field to one day before the current date and time.
4. **Or use shift times:** If enabled, specify the required shift number to only view incidents that occur within this shift.
5. **Operator:** If enabled, select the name of the required operator from the list to only view the incidents that are logged to this operator.
6. **Incident categorization:** If enabled, select the name of the required category (as specified in the**Category** tree) that contains the incidents that you are interested in.

PLEASE NOTE: These constraints are provided by adding special constraint parameters to these queries, so it is NOT possible to execute any queries that contain constraint parameters from 3rd party applications.

To change the frequency at which the charted data is updated: This will determine how often this query is performed on the database to include the latest logged incidents in the current chart.

- Specify the required interval in the **Auto-refresh (secs)** spin control.

  Tip: Click the **Refresh** button to immediately perform the selected query on the database to include the latest logged incidents in the chart.

This dialog provides the following chart configuration options:

To create a .JPG image file of the displayed chart:

- Click the **Export...** button.

  This exports the displayed chart as a .JPG image to the following file:

  - This file is saved to the system temp folder, typically C:\Documents and

Settings[\UserName]\Local Settings\Temp.

- This file adheres to the following naming format: QueryName as at YYYY_MM_DD HH_MM_SS.JPG.

To print the displayed chart using the default printer:

- Click the **Print...** button.

To add a legend to the left of the chart: this displays the information for each data-point of the charted series.

- Click the **Legend** checkbox.

To rotate the labels of the X axis of the chart: when there are numerous data points on the X axis, some of their labels are not displayed for visibility reasons. In this case this option will display all these labels as their text is displayed vertically instead of horizontally.

- Click the **Rotate** checkbox.

Note: This ONLY applies to charts that have an X axis, therefore it has no effect for Pie charts.

To toggle the three dimensional display of the chart: by default, charts are displayed in three dimensions but you can display them in two dimensions if necessary.

- Click the **3D view** checkbox.

If this is cleared, the chart is displayed in 2 dimensions.

If this is ticked, the chart is displayed in 3 dimensions, the default selection.

To toggle between pie or bar charts: by default, charts are displayed using their default chart type but you change the type of chart to bar or pie charts.

- Click the **Swap pie/bar** checkbox.

If the current chart is a pie chart this becomes a bar chart and vice verse.

To provide Y axis value labels for the charted series: this labels each charted data-point with its Y axis value.

- Click the **Value Labels** checkbox.

To provide full labels (both the X and Y values) for the charted series:

- Click the **Full Labels** checkbox.

To label each charted data-points with its X and Y axis value:

- Click the **Labels** checkbox.

Adding your own Queries: This describes how you can add you own queries so that they too can appear in this View Data dialog.

Launching the View Graph dialog: This describes how you can also launch this dialog directly from a Classic UI mimic.

Launching the View Graph Dialog

WARNING! We do NOT RECOMMEND using this dialog for an alarm management database that contains a huge number of historical incidents - this can cause your system to become unstable.

The AlarmManagement agent provides a dialog to use queries to analyze its logged incidents and displays these results graphically, as a chart.

Typically this dialog will not be viewed by operators but instead by management in order to appraise the process alarming system.

PLEASE NOTE: If you need to display this **View graph** dialog from mimics on remote clients, then please use a UNC path when specifying the OLE DB database of this AlarmManagement agent, otherwise you will NOT be able to DISPLAY this dialog.

Viewing Incidents Requiring Reasons and/or Notes

The AlarmManagement agent provides an **Outstanding reasons and notes** dialog which ONLY displays the current incidents that still require reasons and/or notes to be specified. In other words this dialog only displays the current incidents that have their **Reasons required** and/or **Notes required** settings enabled and as yet unspecified.

Note: An incident is removed from this dialog once its reason and/or note is specified.

Tip: This dialog can be resized and maximized and its last size and position is saved for the current UI session.

To change the frequency at which the charted data is updated: This will determine how often this query is performed on the database to include the latest logged incidents requiring reasons and/or notes.

- Specify the required interval in the **Auto-refresh (secs)** spin control.

  Tip: Click the **Refresh** button to immediately perform the selected query on the database to include the latest logged incidents in the chart.

This dialog provides the following grid configuration options: this allows you to configure both the table (grid) and specify the reasons and/notes for the displayed incidents.

To sort the table entries by a column:

- Click the required column heading.

  This column heading displays the » character when the rows of this table are sorted so that the contents of this column are displayed in ascending order.

  This column heading displays the « character when the rows of this table are sorted so that the contents of this column are displayed in descending order.

To change the widths of individual columns: This can be used to hide an unnecessary column from view.

- Drag the right hand side of the column left or right, as required.

  Note: The changes made to the column widths are saved for the currently selected query.

To resize the columns of the table to the width of their largest entry: this resets any changes that have been made to the column widths and displays any hidden columns.

- Right-click the table and select **Show all columns**.

  Note: The changes made to the column widths are saved for the currently selected query.

To export the table or grid to a CSV file: This allows you to report the data in a 3rd party application.

- Click the **Export...**.

  This will open this file in the default .CSV file editor.

To specify the reasons and/notes for each incident in this dialog: this will remove the incident from the dialog.

- Click the **Reasons...** button. This displays the **Incident reasons and notes** dialog.

  For details of using this dialog, see Specifying Reasons and/or Notes for Incidents.

  Tip: This dialog can also be displayed by double-clicking an incident listed in this **Outstanding reasons and notes** dialog.

Once the reason and/or note is specified this incident will be removed from this dialog.

Specifying Incident Reasons and/or Notes

The AlarmManagement agent provides an **Incident reasons and notes** dialog to specify reasons and/or notes for a selected incident in the database. In other words this dialog allows you to select the reason and its sub-reason that caused the incident to occur and/or to specify any other textual description or note concerning this incident.

Tip: The **ReasonsRequired** status bit of the AlarmManagement agent is enabled when there are incidents that require reasons and/or notes (this can take up to 30 seconds to reflect the current status).

Note: The dialog status is now sensitive to the Alarm Management agent name so that the correct set of outstanding reasons and notes are displayed in a proxy server environment, where multiple Alarm-Management agents may exist.

Depending upon the configuration of the incident either the reason and/or note may be mandatory displays the current incidents that have their **Reasons required** and/or **Notes required** settings enabled and as yet unspecified.

To specify a reason: this requires you to select a reason AND a sub-reason that best describes the cause of this incident.

1. Select the most applicable reason for this incident from the **Reasons** list of the **Incident reasons and notes** dialog.
2. Select the most applicable sub-reason (or cause) of this incident from the **Sub-reasons** list.
3. Click the **OK** button.

   This logs the specified reason to the database of this AlarmManagement agent.

To specify a note: this note should typically include some explanatory detail concerning the cause and action taken concerning this incident, especially if this is not adequately explained by the selected reason or sub-reason.

1. Type the required text into the **Notes** edit field of the **Incident reasons and notes** dialog.
2. Click the **OK** button.

   This logs the specified note to the database of this AlarmManagement agent.

If necessary, you can also launch the **Incident reasons and notes** dialog from a button or another picture element on a Classic UI mimic, see Customizing the launching of the View Reasons Dialog.

Launching the View Reasons Dialog

The AlarmManagement agent provides a dialog that ONLY lists its current logged incidents that still require reasons and/or notes to be specified.

Typically operators will need to view this dialog so that they can specify these outstanding reasons and/or notes.

PLEASE NOTE: If you need to display this **View reasons** dialog from mimics on remote clients, then please use a UNC path when specifying the OLE DB database of this AlarmManagement agent, otherwise you will NOT be able to DISPLAY this dialog.

Note: The dialog status is now sensitive to the Alarm Management agent name so that the correct set of outstanding reasons and notes are displayed in a proxy server environment, where multiple alarm-managment agents may exist.

Obtaining KPI Values

One of the possible uses of the database of incidents logged by your AlarmManagement agent/s is to determine how well your process or your operators are meeting the KPIs that you have set for them regarding alarming.

The AlarmManagement agent automatically calculates the following KPIs:

- The **kpi24Hrs** slot records the number of alarms per hour for the current 24 hour period.
- The **kpiMonth** slot records the number of alarms per hour for the current month.
- The **kpiPrev24Hrs** slot records the number of alarms per hour for the previous 24 hour period.
- The **kpiPrevMonth** slot records the number of alarms per hour for the previous month.
- The **kpiPrevShift** slot records the number of alarms per hour for the previous shift.
- The **kpiShift** slot records the number of alarms per hour for the current shift.
- The **kpiTotal** slot records the number of alarms per hour for the all incidents found in the database.

Furthermore, the AlarmManagement agent provides you with the ability to obtain the values of 6 user-defined KPIs.

IMPORTANT: Each KPI must be a SELECT query that is performed on the database of logged incidents that returns **a SINGLE numeric value called kpi**.

Example of a KPI query:

The following query returns a SINGLE value called kpi:

SELECT COUNT(Idx) / (MAX(CONVERT(float, dt) * 24) - MIN(CONVERT(float, dt) * 24)) AS kpi FROM HistoricalIncidents

These user-defined KPI Queries support the following optional parameters:

The following parameters **MUST ALL BE encased within a pair of SINGLE quotation characters:**

- %now - the current date and time

  Usage example (in SQL):

  The following example retrieves the average active time for the last 8 hours.

  SELECT AVG(ActiveTime) AS Kpi FROM Adr_AM_HistoricalIncidents WHERE dt > DATEADD(Hour,-8,'%now') AND dt < GetDate()

- %s1b - shift 1 start time
- %s1e - shift 1 end time
- %s2b - shift 2 start time
- %s2e - shift 2 end time
- %s3b - shift 3 start time
- %s3e - shift 3 end time

  Usage example (in SQL):

  SELECT AVG(ActiveTime) AS Kpi FROM Adr_AM_HistoricalIncidents WHERE (dt >= '%s1b') AND (dt < '%s1e')

The AlarmManagement agent therefore provides 6 sets of the following 3 slots, where [x] is a number from 1 to 6:

1. **kpi[x]Query:** A VARSTRING slot, that contains the KPI query, which is saved in the WGP file.
2. **kpi[x]Description:** A VARSTRING slot, that contains the description of this KPI, which is saved in the WGP file.
3. **kpi[x]:** A REAL slot, which retrieves the value of the KPI query.

   IMPORTANT: If the KPI query returns multiple columns and/or rows and not a SINGLE value, this kpi[x] slot will be set to 0.0.

   Note: These KPI queries are automatically executed by the AlarmManagement agent when a new record is added to the Historical Incidents table.

You can change the KPI values that are used by these default queries, so that they better comply with your specific requirements AND add your own custom KPIs that your user-defined KPI Queries can use.

Customizing KPI target values: If necessary you can set KPI target values that your own custom KPI queries and certain default queries use, so that these queries better comply with your specific requirements.

Adding your own KPI target values

PLEASE NOTE: This help topic assumes that you are familiar with working with databases.

You can add your own KPI target values that your custom KPI queries can use.

Simply edit the **Adr_AM_UserKPIs** table of the AlarmManagement database and add you own KPI targets to these.

To add your own KPI target value:

1. Open the OLE DB database that the required AlarmManagement agent is connected to.
2. Open the **Adr_AM_UserKPIs**table.
3. Type the abbreviation or acronym of this KPI target into the **Id** field of the last entry (row) of this table. This is name that you can prefix with a '%' to reference this value in a custom query.

   Note: You can ONLY specify an **Id** of 5 characters or less.
4. If necessary, provide the **Description** of this KPI target value to explain what the specified acronym stands for.
5. Specify the integer that represents the ideal target value for this KPI in the **Value** field.
6. Save the changes that you have made to this table.

Then configure the queries that use these custom KPI target values in the **Adr_AM_UserQueries** table. See Adding your own Queries.

WARNING! It is recommended that you do NOT edit any table in this database, apart from **Adr_AM_UserKPIs** and **Adr_AM_UserQueries**; otherwise you WILL lose data.

Note: If you want to remove the KPI target values you have edited or created, simply delete the **Adr_AM_UserKPIs** table and they will be re-create with the default KPI target values when the Agent Server starts up.

If necessary, you can change the KPI target values that certain default queries use and/or any KPI target values that you have added, which your own custom queries use. See Customizing KPI target values.

Default Alarm Management Queries : describes the default queries, some of which can be customized by changing the default KPI target values.

Customizing KPI target values

You can change the KPI target values that certain default queries use and/or any KPI target values that you have added, which your own custom queries use.

Typically, you should only change a KPI target value if it does NOT describe the performance levels that you need your alarming system to meet.

To change a KPI target value:

1. Edit your AlarmManagement agent. Click for more details:
   - Select the name of this AlarmManagement agent. For details, see To Select an Agent.
   - Right click and select the **Edit...** menu item.

     This will display the **Edit AlarmManagement Agent** dialog.
2. Click the **Edit KPI's** button in the **Edit AlarmManagement agent** dialog.

   This displays the **Edit Alarm Management KPI values** dialog.
3. Double click the appropriate KPI (row) to change its value.

Related topics:

Adding your own KPI target values : add your own KPI target values that your custom queries can use.

Default Alarm Management Queries : describe the default queries, some of which can be customized by changing the default KPI target values.

Obtaining KPI Values : Describes how to obtain the common KPI values calculated by this agent and/or to configure queries to obtain up to 6 user-defined KPI values and how these values are stored by this agent.

Exporting the Alarming Configuration

If necessary, you can save the entire configuration of the Adroit alarming sub-system in a single table of the alarm management database, for analysis

To export the Adroit alarming configuration to the AM database:

1. Edit your AlarmManagement agent. Click for more details:
   - Select the name of this AlarmManagement agent. For details, see Locating an agent.
   - Right click and select the **Edit...** menu item.

     This will display the **Edit AlarmManagement Agent** dialog.
2. Click the **Export alarm cfg** button in the **Edit AlarmManagement agent** dialog.
3. Click **Yes** when the confirmation dialog is displayed.

   The AlarmManagement agent creates the Adr_AM_AlarmConfigurationDump table in its associated OLE DB database and populates it with the alarming configuration.

The created **Adr_AM_AlarmConfigurationDump** table provides the following fields:

1. **Idx** (Integer), used to sort the table;
2. **Process** (a 30 character String) representing the applicable Agent Server;
3. **AlarmAgent** (a 30 character String);
4. **Incident** (a 80 character String);
5. **Description** (a 80 character String);
6. **Route** (Integer);
7. **AlarmLists** (a 80 character String);
8. **Devices** (a 80 character String);
9. **Outputs** (a 80 character String);
10. **Eventlogs** (a 80 character String);
11. **Priority** (Integer);
12. **AlarmDelay** (Integer);
13. **Acknowledge** (Integer);
14. **Condition** (a 80 character String);
15. **InhibitUntil** (a 20 character String).

About the AlarmManagement Database

The OLE DB compatible database specified by an **AlarmManagement** agent is the repository of all the logged incidents. This database allows you to obtain reports and KPIs focused around delivering a clear set of information on which the operators can act.

The AlarmManagement agent provides the View Data and View Graph dialogs to allow users to analyze the data contained in its database. However, we recommend that you use a 3rd party application (such as VIZ-NET and/or OPUS) to provide your own client front-ends to this data so you can more effectively report and analyze it and transform it into usable information.

For this reason, it is necessary to know the structure of the tables within the OLE DB database that the AlarmManagement agent populates. This database records all the incidents including the time of incident, time of acknowledgement and time the incident cleared.

IMPORTANT: To clear the Alarm Management database - simply to delete all the tables and then restart the Agent Server, which recreates and populates the tables correctly. DO NOT use a script to empty this database, since many of the tables use an auto-incrementing index field, which is NOT reset in this case causing all manner of problems.

WARNING! If you delete any of these tables, they will be recreated with their default configuration when the Agent Server is restarted, BUT you will LOSE any previous configuration or data that the tables may have contained.

Each incident is logged using the name of its assigned AlarmManagement agent, so that it is possible to unify your alarm management for your enterprise and have more than one AlarmManagement agent log incidents to the SAME database. In this case please ensure that your AlarmManagement agent are uniquely named.

The two primary tables in this database are the **Adr_AM_CurrentIncidents** and **Adr_AM_HistoricalIncidents** tables, which store all the logged incidents. An important field in these tables is the **IncidentID** field, which uniquely identifies each incident in this database. So by querying an entry in this field you can find out ALL the information pertaining to a specific alarm/event, such as every time this incident has been logged.

ALL incidents found in the **Adr_AM_CurrentIncidents** table as a result of the last Agent Server session are marked as acknowledged and their active times are set to zero.

- If these entries do not require reasons and/or notes then they are automatically added to the **Adr_AM_HistoricalIncidents** table.
- If the entries require reasons and/or notes, then they will remain in the **Adr_AM_CurrentIncidents** table until these entries have been completed by the operator.

For a description of each of the tables and their fields, see AlarmManagement Database Tables.

AlarmManagement Database Tables

The AlarmManagement agent creates and maintains the following tables in its associated OLE DB database:

IMPORTANT: To clear the Alarm Management database - simply to delete all the tables and then restart the Agent Server, which recreates and populates the tables correctly. DO NOT use a script to empty this database, since many of the tables use an auto-incrementing index field, which is NOT reset in this case causing all manner of problems.

WARNING! If you delete any of these tables, they will be recreated with their default configuration when the Agent Server is restarted, BUT you will LOSE any previous configuration or data that the tables may have contained.

- **Adr_AM_AssociatedValues:** This table stores the values of the tags that are associated with each incident. Each tag associated with an incident is stored as a separate record in this table. This table has the following fields (columns):
  1. **Idx:** The Key field, which is a unique, automatically incrementing number.
  2. **IncidentIdx:** The unique incident index value of the associated incident record, which is an **Idx** value in either the **Adr_AM_HistoricalIncidents** or **Adr_AM_CurrentIncidents** table.
  3. **Tag:** The name of the tag associated with the incident specified by **IncidentIdx**.
  4. **TagValue:** The value of the associated **Tag**.
- **Adr_AM_Categories:** This table defines the hierarchical structure used to categorize the incidents. Each category is stored as a separate record in this table. This table has the following fields (columns):
  1. **CategoryId:** The Key field, which is a unique, automatically incrementing number.
  2. **ParentId:** The unique category ID of this category’s immediate parent i.e. the category that is above this category in the hierarchy.
  3. **Category:** The name of the category specified by **CategoryId**.
  4. **OperatorTag:** An optional field for a tag that contains the name of the Operator that will be logged for all the incidents in this category and, if necessary, its sub-categories too.
- **Adr_AM_CurrentIncidents:** This table is the initial destination for every incident generated by the alarm agents and logged by the AlarmManagement agent/s. Incidents are ONLY moved to the **Adr_AM_HistoricalIncidents** table if they are valid and they have been cleared and/or acknowledged and when any mandatory reasons and/or notes have been specified.

  Note: All entries in this table are DELETED when an Agent Server starts.

  This table has the following fields (columns):

1. **Idx:** The Key field, which is a unique, automatically incrementing number for each incident that is logged to it.
2. **dt:** The date and time of the occurrence of this incident.
3. **Process:** The name of the AlarmManagement agent that logged this incident. This is required to uniquely identify incidents across the enterprise (if multiple agents log to the SAME database.

   Note: These names have a maximum of 30 characters.
4. **CategoryId:** The unique identification of the category in which this incident is located.
5. **IncidentID:** This is an **important** field as it uniquely identifies each incident in this database. This is simply the index (**Idx** field) that is used for an incident the FIRST time that the incident is logged to the database.
6. **Incident:** The name of the incident, which is the agent name and alarm type combination e.g. KILNTEMP.HI
7. **Data:** The Reported data values for this incident as received from Adroit.
8. **Description:** The description of the agent causing the incident.
9. **Filter:** The Agent filter group as received from Adroit for the agent referenced by the incident.
10. **Priority:** The Agent priority as received from Adroit for the agent referenced by the incident.
11. **Shift:** The Shift number in which incident occurred, in other words the **dt** is greater than the starting time of this shift and less than the starting time of the next shift.
12. **Operator:** This is the value of the tag configured for the **Operator tag** setting of the category in which this incident is located (or of the CLOSEST higher-level categories, if any).
13. **Acknowledged_dt:** The date and time that the incident was acknowledged.

    Note: This time is equal to the **dt** field, if the incident does not require acknowledgement.
14. **Acknowledged_by:** The name of operator who acknowledged the alarm. In other words the name of the currently logged on user of the Adroit client (or Windows).
15. **Cleared_dt:** The date and time that this incident was cleared.
16. **Delay:** The **Delay** field from the **Incident** table. In other words the number of seconds the incident needs to be active (**Cleared_dt** field – **dt** field) in order to be considered valid. If the alarm is cleared before this **Delay** then the incident is removed from the Adr_AM_CurrentIncidents table.
17. **ReasonId:** The **Idx** field from the **Reasons** table that is associated with the currently specified reason. If this is 0 then it is assumed that no reason has been specified.
18. **SubReasonId:** The **Idx** field from the **SubReasons** table that is associated with the currently specified sub-reason. If this is 0 then it is assumed that no sub-reason has been specified.
19. **Notes:** The text specifying any notes that have been specified for this incident.
20. **Record_dt:** The date and time that this incident was received by the SQL database, which can be used to improve the quality of the AM reports.

- **Adr_AM_HistoricalIncidents:** This table stores every completed incident in other words the incidents from the **Adr_AM_CurrentIncidents** table that have been cleared and/or acknowledged and whose mandatory reasons and/or notes have been specified. This table has the following fields (columns):

  1. **Idx:** The Key field, which is the unique **Idx** field that this incident had in the Adr_AM_CurrentIncidents table, before it was moved to this table.
  2. **dt:** The date and time of the occurrence of this incident.
  3. **Process:** The name of the AlarmManagement agent that logged this incident.

4. **CategoryId:** The unique identification of the category in which this incident is located.
5. **IncidentID:** This is an **important** field as it uniquely identifies each incident in this database.

   Tip: Querying this field will obtain all the information concerning a specific event/alarm in the database.
6. **Incident:** The name of the incident, which is the agent name and alarm type combination e.g. KILNTEMP.HI
7. **Data:** The Reported data values for this incident as received from Adroit.
8. **Description:** The description of the agent causing the incident.
9. **Filter:** The Agent filter group as received from Adroit for the agent referenced by the incident.
10. **Priority:** The Agent priority as received from Adroit for the agent referenced by the incident.
11. **Shift:** The Shift number in which incident occurred.
12. **Operator:** This is the value of the tag configured for the **Operator tag** setting of the category in which this incident is located (or of the CLOSEST higher-level categories, if any).
13. **Acknowledged_dt:** The date and time that the incident was acknowledged.

    Note: This time is equal to the **dt** field, if the incident does not require acknowledgement.
14. **Acknowledged_by:** The name of operator who acknowledged the alarm. In other words the name of the currently logged on user to Adroit client (or Windows).
15. **Cleared_dt:** The date and time that this incident was cleared.
16. **UnacknowledgedTime:** The number of seconds (**Acknowledged_dt** field – **dt** field) it took to acknowledge the incident.
17. **ActiveTime:** The number of seconds (**Cleared_dt** field – **dt** field) it took for the alarm to be cleared.
18. **ReasonId:** The **Idx** field from the **Reasons** table that is associated with the currently specified reason. If this is 0 then it is assumed that no reason has been specified.
19. **SubReasonId:** The **Idx** field from the **SubReasons** table that is associated with the currently specified sub-reason. If this is 0 then it is assumed that no sub-reason has been specified.
20. **Notes:** The text specifying any notes that have been specified for this incident.
21. **Record_dt:** The date and time that this incident was received by the SQL database, which can be used to improve the quality of the AM reports.

- **Adr_AM_Incidents:** This table defines the incidents and their optional settings. This table has the following fields (columns):
  1. **Idx:** The Key field, which is a unique, automatically incrementing number.
  2. **CategoryID:** The unique identification of the category in which this incident is located.
  3. **Name:** The name of the incident, which is the agent name and alarm type combination e.g. KILNTEMP.HI
  4. **AliasAlarmType:** An optional field that can override the default incident name e.g. TANKLEVEL.High can be changed to TANKLEVEL.Overflow.
  5. **Agent:** The name of the agent for the agent causing the incident.
  6. **AgentType:** The agent type of the agent causing the incident.
  7. **AlarmType:** The alarm type specified for the incident.
  8. **Document:** : An optional UNC path to a HTML document that further clarifies the incident and provides assistance on how to deal with it or react to it.

9. **Delay:** An optional delay time, in seconds, that must elapse before the incident is considered to be valid.
10. **Condition:** An optional BOOLEAN tag whose value must be TRUE for the incident to be valid.
11. **ReasonRequired:** An option to enforce the entry of reasons on each occurrence of the incident – default value FALSE.
12. **NotesRequired:** An option to enforce the entry of notes on each occurrence of the incident – default value FALSE.
13. **AssociatedTags:** Optional, comma delimited tags whose values must be recorded when the incident occurs.

- **Adr_AM_Licence:** This table is for internal use only and should not be used by customers.
- **Adr_AM_Operators:** This table stores each new operator name and is provided to make it easier to query these operators. This table has the following field (column):

  1. **Name:** The name of the operator.

- **Adr_AM_Reasons:** This table contains an indexed list of reasons that can are used to determine the cause of incidents. This table has the following fields (columns):

  1. **Idx:** The Key field, which is a unique, automatically incrementing number.
  2. **Reason:** The Reason that is displayed in the reasoning dialog.
  3. **Description:** An optional description of this reason, this is NOT referenced by Adroit.

- **Adr_AM_SubReasons:** This table contains an indexed list of sub-reasons for the reasons specified in the **Reasons** table that can are used to determine the cause of incidents. This table has the following fields (columns):

  1. **Idx:** The Key field, which is a unique, automatically incrementing number. Ensure that this is the SAME as the **Idx** field in the **Reasons** table, in order to specify sub-reasons for a particular reason.
  2. **SubReason:** The Sub-reason that is displayed in the reasoning dialog.
  3. **Description:** An optional description of this sub-reason, this is NOT referenced by Adroit.

- **Adr_AM_UserKPIs:** This table allows users to configure the values of the KPI targets used by the queries of the AlarmManagement agent.

  This table has the following fields (columns):

  1. **Idx:** The Key field, which is a unique, automatically incrementing number for each KPI added to this table
  2. **Id:** A unique short name (acronym) identifier for the KPI, which is a maximum of 5 characters.

     Note: This field can be used with a % prefix to parameterize user queries where it makes sense to do so.

  1. **Description:** An English description of the KPI target.
  2. **Value:** The user configurable Integer value for this KPI target.

- **Adr_AM_UserQueries:** This table contains all the queries that made available to the **View Data** and, if necessary to the **View Graph** dialogs, so that users can analyze the database from the Classic User Interface.

  Note1: If necessary, you can create your own queries and add them to this table so that they too will appear in these dialogs. For details, see Adding your own Queries.

  Note2: It is NOT recommended that you edit the existing queries especially the first 6 queries otherwise the functionality provided by the AlarmManagment agent will be compromised.

  Note3: These queries CANNOT be all be used by 3rd party applications as certain queries contain criteria parameters, which support the criteria of the **View Data** dialog.

  This table has the following fields (columns):

   1. **QueryId:** The Key field, which is a unique, automatically incrementing number for each query that is added to this table.
   2. **Name:** The name that is displayed in the Query list box when selecting the query.
   3. **Description:** It is recommended to specify a description to help your users to know what this query will return.
   4. **Query:** The query itself in SQL query syntax, if necessary specify optional proprietary characters to enable the use of one or more of the constraints in the **View Data** dialog.
   5. **ChartType:** If you want this query to be displayed in the **View Graph** dialog, then use this field to specify which chart should be used to display the results of this query. The default value of -1 indicates that you do NOT want this query to appear in the **View Graph** dialog.

- **Adr_AM_Version**: This table is typically used by third party applications to display the current version of the Alarm Management database to determine which version of the database is currently installed.

  This table has the following fields (columns):

   1. **Idx:** The Key field, which is a unique, automatically incrementing number for each KPI added to this table
   2. **Description:** Database version.
   3. **Value:** This is the file revision of the AlarmManagement agent DLL.

- **Adr_AM_AlarmConfigurationDump**: This is an optional table that is created when the user clicks the **Export alarm cfg** button in the **Edit AlarmManagement agent** dialog and populates it with the alarming configuration. For details about its fields, see Exporting the Alarming Configuration.

Specific Status Bits of the AlarmManagement Agent

The following status bits of this agent can be used for diagnosing the status of its connection to the database that it logs incidents to and the status of any queries that it performs, as follows:

• status bit 16 ConnectionError	Set to TRUE (1) when the connection with OLE DB source cannot be established.
• status bit 17 QueryError	Set to TRUE (1) when a query error has occurred.
• status bit 18 ReasonsRequired	Set to TRUE (1) when there are incidents that require reasons and/or notes. **Note:** Indication can take up to 30 seconds to reflect the current status.
• status bit 19 Unlicensed	Set to TRUE (1) when the required OEM code is missing from the Agent Server license.

Securing Documents using NTFS

NTFS, the secure file system for Windows NT operating systems, (available from Windows NT onwards), allows you to set permissions for groups or individual users to access files, as follows:

Note: Ensure that you have formatted the required local partition using NTFS.

1. Launch Windows Explorer.
2. Browse to the required document on your local hard drive.
3. Right click this document and select **Properties**.
4. Click on the **Security** tab in the Properties dialog.
5. Add the required groups and/or individual users to the **Group or user names** list.
6. Click each group and user and configure their required access permissions by checking and clearing the permission checkboxes.
7. Click the **OK** button when finished.

Delaying Incidents

Sometimes you do not want an incident to enter your alarming system as soon as it becomes active, this is typically for one of the following reasons:

- To prevent intermittent alarms from flooding your alarm system and distracting your operators from the other more important incidents.
- To ensure that this alarm is raised when the operator needs to respond to it, not too early and not too late.

In these cases, you can configure a delay appropriate for each incident.

This delay is simply the number of seconds that the alarm system should wait, once an incident becomes active, before this incident is recognized as being ‘officially’ active and is made known to your operators via the configured Alarm routes.

Note1: If the incident is cleared before the delay has expired then the incident NEVER enters your alarming system, so your operators will NOT know about it.

Note2: This delay must NOT be LESS THAN the scan period of the tag that creates the alarm otherwise the incident will ALWAYS enter your alarming system, and the time delay is ineffective.

Note3: If BOTH a delay and a conditional expression is specified for an incident, then the conditional expression is evaluated BEFORE and AFTER the specified delay expires.

To configure a delay for an incident:

1. Select the required agent, in other words the agent containing the required alarmed alarm type/s. For details, see Locating an agent.
2. Right click this agent and select the **Alarm...** menu item.
3. Click on the required alarm type in the **Current** list of the **Alarming** dialog.
4. Specify the required delay for this alarm type, in seconds, in the **Delay (secs)** field at the bottom of this dialog.

   Note: If this value is zero, the default setting, then no delay checking is performed and as soon as the incident becomes active it is routed to your operators.

Creating Conditional Expressions for Incidents

Often incidents are set off in a chain reaction that distracts your operators as they only highlight a problem that has already been identified. First-out or SOE (Sequence Of Events) alarming strives to ensure that each incident is unique and is NOT caused by a condition that your operators have already been alerted to.

You can implement first-out alarming by creating conditional expressions for your related incidents, so that if an incident becomes active, it ONLY enters your alarming system WHEN its conditional expression is SUCCESSFUL. In this way you can disregard the incidents that echo existing problems, so that your operators can focus on the real issues at hand.

Note1: If the RESULT of the conditional expression for an incident is a NULL or zero value then the incident NEVER enters your alarming system, so your operators will NOT know about it.

Note2: If BOTH a delay and a conditional expression is specified for an incident, then the conditional expression is evaluated BEFORE and AFTER the specified delay expires.

To configure a conditional expression for an incident:

1. Select the required agent, in other words the agent containing the required alarmed alarm type/s. For details, see Locating an agent.
2. Right click this agent and select the **Alarm...** menu item.
3. Click on the required alarm type in the **Current** list of the **Alarming** dialog.
4. Specify the required expression for this alarm type in the **Conditional expression** field at the bottom of this dialog.

   Typically you will create a logical expression, whereby the required tag is followed by a value condition, such as:

Logical expression	Condition for success
`Tag(TANKLEVEL.value) = 80`	SUCCESSFUL if the tag is equal to the value
`Tag(TANKLEVEL.value) <> 80`	SUCCESSFUL if the tag is not equal to the value
`Tag(TANKLEVEL.value) > 80`	SUCCESSFUL if the tag is greater than the value
`Tag(TANKLEVEL.value) >= 80`	SUCCESSFUL if the tag is greater than or equal to the value
`Tag(TANKLEVEL.value) < 80`	SUCCESSFUL if the tag is less than the value
`Tag(TANKLEVEL.value) <= 80`	SUCCESSFUL if the tag is less than or equal to the value

Note: You need to enclose each tag within the Tag() specifier e.g. Tag(systeminfo.second)

IMPORTANT: If a tag is NOT enclosed within a Tag() specifier then this incident will NEVER become active.

Tip: When adding a tag to the expression, click the browse ... button and use the **Adroit Agent Browser** to locate and copy the required tag for you (then use the CTRL+V shortcut to paste it into the expression). This saves you from having to type in the tag yourself and ensure that there are NO spelling errors.

Your expressions can make use of one or more of the following elements:

Note1: Multiple items are separated by commas ','.

Note2: Where necessary the description of an operator is displayed in brackets () after the operator.

Element Type	Operators / Example
Other logical operators	! (not), & (and), | (or)
Arithmetic operators	+, -, *, /, % (modulus),^ (power)
Parentheses	(), {}, []
Scientific notation	3E+10
Constants	2, 3, 50
Functions	MIN(4,5), SQR(34)

By making use of these elements, you can create expressions that contain more than one tag, such as:

```
(Tag(TANKLEVEL.value) < 20) | (Tag(TANKLEVEL.value) > 80)
```

This will be SUCCESSFUL if the tag (Tanklevel.value) is less than 20 or greater than 80.

Click here for a list of Functions that you can use in your expressions:

Note1: These functions can take either constants or tags as their parameters.

Note2: For simplicity sake, the tag specifiers have been omitted so Tag1 = Tag(agent1.slot1)

Function	Usage
MIN : returns the minimum value	MIN(2, 3, 4, 5) is 2.
MAX : returns the maximum value	MAX(2, 3, 1, 0) is 3.
IF(condition, valueIfTrue, valueIfFalse)	IF(1, 2, 3) is 2
SUM : adds the values together	SUM(1, 2, 3, 4) is 10
AVG :averages the values	AVG(1, 2, 3, 4, 5) is 3
SQR: returns the square of the value	SQR(Tag1)
SQRT: returns the square root of the value	SQRT(Tag1)
EXP : Returns E raised to the power of the value	EXP(Tag1)
INTPOW(Base, power): raises the Base to an integral power.	INTPOW(2, 3) = 8

Function	Usage
POW(Base, power): raises the Base to any power. **Note:** For fractional exponents or exponents greater than MaxInt, the Base must be greater than 0.	POW(2,3) = 8
LN: returns the natural logarithm of the value	LN(Tag1)
LOG: returns the base-10 logarithm of the value	LOG(Tag1)
LOGN(Base, value): returns the log Base of the value	LOGN(10, 100) = 2
ABS: returns the absolute value	ABS(Tag1)
SIGN: returns the sign of the value	SIGN(Tag1) returns -1 if Tag1<0; +1 if Tag1>0, 0 if Tag1=0
TRUNC: discards the fractional part of the value	TRUNC(-3.2) is -3, TRUNC(3.2) is 3
CEIL: returns the value rounded up, away from zero	CEIL(-3.2) = -3, CEIL(3.2) = 4
FLOOR: returns the value rounded down, toward zero	FLOOR(-3.2) = -4, FLOOR(3.2) = 3
SIN: returns the sine of the value (an angle in radians).	SIN(Tag1)
COS: returns the cosine the value (an angle in radians).	COS(Tag1)
TAN: returns the tangent of the value (an angle in radians).	TAN(Tag1)
ATAN: returns arctangent, or inverse tangent, of the value. The returned angle is specified in radians.	ATAN(Tag1)
SINH: returns the hyperbolic sine of the value.	SINH(Tag1)
COSH: returns the hyperbolic cosine of the value.	COSH(Tag1)
COTAN: returns the cotangent of the value.	COTAN(Tag1)

Configuring the Shift Agent

Edit an agent of type: **Scheduler**.

Please use the following sequence when adding shift patterns:

1. Entries that contain a **Special date** or **Day of month** value must always be specified first.

2. **Special date** entries must use the format "yyyy/mm/dd" e.g. 2010/04/04. An example of a "special date" is a public holiday which falls on a different day every year e.g. Easter Monday.

3. **Day of month** entries must use the format "mm/dd". An example of a "day of month" is a public holiday which falls on the same day every year e.g. New Years day.

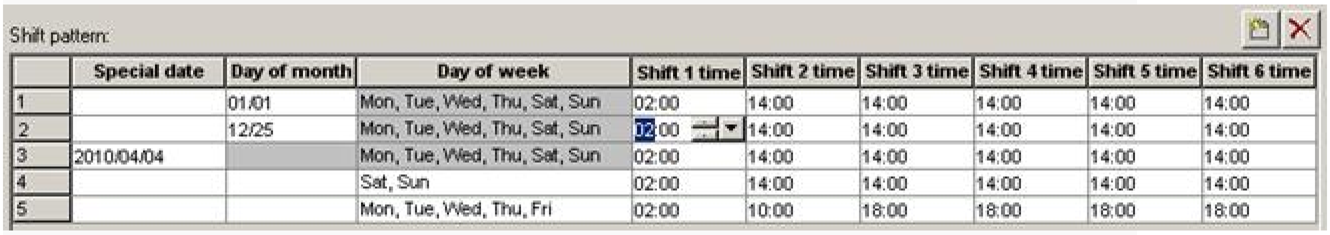
   Note1: Entries containing a **Special date** cannot contain a **Day of month** value too.

   Note2: Entries containing a **Special date** or **Day of month** value force (disable) their **Day of week** value.

   Tip: Use the DEL key to delete unneeded **Special date** or **Day of month** field entries

4. The last entries should be the default shift patterns that ONLY contains a **Day of week** value and NO **Special date** or **Day of month** values.

Shift pattern examples:



Shift pattern:

	Special date	Day of month	Day of week	Shift 1 time	Shift 2 time	Shift 3 time	Shift 4 time	Shift 5 time	Shift 6 time
1		01/01	Mon, Tue, Wed, Thu, Sat, Sun	02:00	14:00	14:00	14:00	14:00	14:00
2		12/25	Mon, Tue, Wed, Thu, Sat, Sun	02:00	14:00	14:00	14:00	14:00	14:00
3	2010/04/04		Mon, Tue, Wed, Thu, Sat, Sun	02:00	14:00	14:00	14:00	14:00	14:00
4			Sat, Sun	02:00	14:00	14:00	14:00	14:00	14:00
5			Mon, Tue, Wed, Thu, Fri	02:00	10:00	18:00	18:00	18:00	18:00

This screenshot exemplifies the required order of entries and provides the following shift patterns:

1. For the 1st of January of any year.

2. For the 25th of December for any year.

3. ONLY on the 4th of April 2010

4. For ALL Saturdays and Sundays

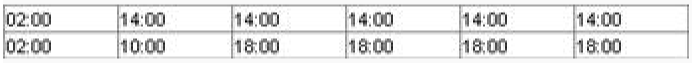
5. For ALL normal weekdays

Notice how the shift patterns that do NOT contain a **Special date** or **Day of month** column are at the END of this list.

The Shift agent caters for a maximum of 6 shifts per day. If you need less than 6 shifts, then specify the starting time of the last applicable shift for the unneeded shifts.

For instance, if only 3 shifts are used, then specify the starting time of shift 3 as the starting times of shifts 4, 5 and 6.

Shift number examples:



02:00	14:00	14:00	14:00	14:00	14:00
02:00	10:00	18:00	18:00	18:00	18:00

This screenshot shows the following shift time configurations:

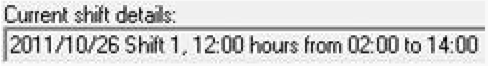
- The first has TWO shifts one starting at 2 AM and the other at 2 PM.
- The second has THREE shifts, which start at 2 AM, 10 AM and 6 PM

Notice how the unneeded shifts ALWAYS specify the starting times of the last applicable shift.

SQL connection string: If specified, the shifts are added to the Adr_Grouping_Details table as the shifts occur in real time, which is used by Adroit SCADA Intelligence.

> **Note:** If you specify **global**, this will use the connection string specified in the **Adroit Configuration Setup**, as follows: type PSEXE into the **Start** menu **Search** dialog and ENTER. Click the **Advanced...** button on the default **Agent Server** tab and in the **Server auditing** section at the bottom of this dialog, the **Custom OLE DB connection** field specifies this connection string.

The **Current shift details** field displays the current day, the current shift number, the current shift duration and then the starting and ending times of the current shift. Example:



Current shift details:

2011/10/26 Shift 1, 12:00 hours from 02:00 to 14:00

> **Tip:** If this does not reflect recent configuration changes then click the **Update** and then the **Refresh** buttons and it should display correctly.

Selecting a Tag Using the Agent Explorer

Select a tag using the **Select Agent** dialog, as follows:

A. Select (click on) the required list of agent types in the left pane, from the following options:

- **AgentGroup:** This lists EVERY agent type in the Agent Server - only use this if you cannot find the required agent type in the other categories.
- **Advanced:** A list of the more advanced agent types that typically advanced users will use.
- **Basic:** A list of the more common agent types that most users will use.
- **System:** A list of agent types that are created by Adroit.

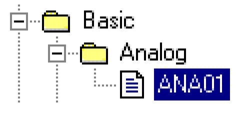
B. Select the required type of agent that you require from this list.

> **Note:** To also display remote agents on other Agent Servers associated with your project, then open the **View** menu and ensure that the **Remote Agents** option is ticked.

- If the required agent exists, in this agent type, then select it.

  Example:

  This shows how to locate an Analog agent.



- If the required agent does not exist, in this agent type then click the **Add...** button to create it, as follows:
    a. Type in the required **Agent Name** in the **Add Agent** dialog.
    b. If required, specify an **Agent Description** which provides additional information about this agent.
    c. Click **OK** when finished.

  To save any newly-created agents, open the **Options** menu and click the **Save Agents Now** menu item.

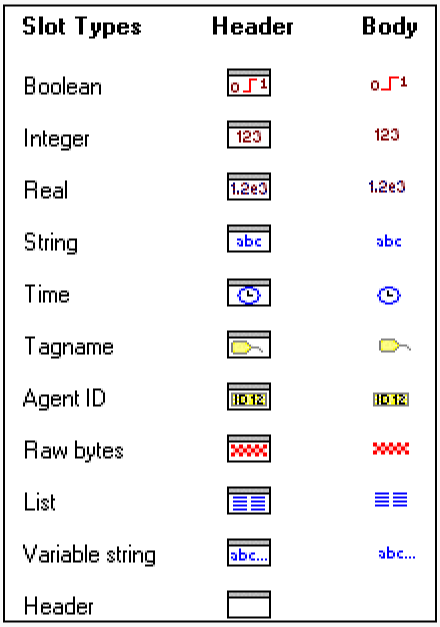
C. If necessary, select the required slot for this agent in the right pane.

By default, this browser:

- Selects the most commonly used slot for each agent type.
- Does not display the slots from the header of an agent. To display these open the **View** menu and ensure that the **Header slots** option is ticked.
- ONLY displays the slots types than can be used in the specified field. To display ALL the available slots, open the **View** menu and ensure that the **Filtered Slot Types** option is not ticked.

The available slot types are indicated by the following icons:

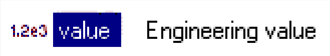
In addition to displaying the relevant slot type, these icons ALSO indicate whether the slot belongs to the header or the body of the agent, as follows:



Slot Types	Header	Body
Boolean	o⌐1	o⌐1
Integer	123	123
Real	1.2e3	1.2e3
String	abc	abc
Time	🕒	🕒
Tagname	🏷	🏷
Agent ID	ID12	ID12
Raw bytes	▨	▨
List	≡≡	≡≡
Variable string	abc...	abc...
Header	□	

Example:

This shows how a slot will appear in the right pane, display its slot type icon, its name and a textual description:



1.2e3 value Engineering value

D. Click the **OK** button to insert the selected agent and slot into the required field.

Selecting a known agent

If necessary, locate the required agent, as follows:

In the Smart UI Designer:

Select the required Smart UI Server in the **Enterprise Manager**, as follows:

1. Open the **Enterprise Manager**.
2. If necessary, expand **Servers**.
3. If necessary, expand the name of the required Server connection.

   Tip: The connection name is prefaced by the Smart UI Server computer name.
4. If necessary, expand the **Datasources** category.
5. If necessary, expand the required Adroit datasource or its icon.
6. If necessary, expand the **AgentGroup** tree.
7. If necessary, expand the required agent type, which are listed alphabetically.
8. Locate the required agent, which is also listed alphabetically beneath their applicable agent type.