

Intelligent Devices
Intelligent Incident
User Guide



4411 Suwanee Dam Road, Suite 510 Suwanee, GA 30024
T: (770) 831-3370 support@intelligentdevicesinc.com
Copyright 2011, Intelligent Devices, Inc. All Rights Reserved

TABLE OF CONTENTS

- INTRODUCING INTELLIGENT INCIDENT 3**
- INSTALLING INTELLIGENT INCIDENT 3**
- MAIN MENU BAR FUNCTIONS..... 5**
- FILE..... 5**
- AutoStart*..... 5
- Log On*..... 5
- Log Off*..... 6
- Change Password* 7
- Timeout*..... 8
- Extended Logging*..... 8
- Large Toolbar Icons*..... 9
- Exit*..... 9
- OPERATIONS 10**
- Incidents* 10
- GIS MAP View of Incidents* 17
- Incident Management*..... 19
- Incident Event Log*..... 23
- Refresh Incidents*..... 23
- Run* 23
- ADMINISTRATION..... 24**
- Configure* 24
- Operators*..... 36
- WINDOW 40**
- HELP 40**
- Search* 40
- About Intelligent Incident*..... 40
- HOW TO ADD A NEW INCIDENT MANAGEMENT SPREADSHEET 41**
- HOW TO ADD A STANDARD OPERATING PROCEDURE 48**
- UPDATING INTELLIGENT INCIDENT 51**
- INDEX 52**

INTRODUCING INTELLIGENT INCIDENT

Intelligent Incident, together with Intelligent Maintenance and Intelligent Parking, are companion products to Intelligent Control and make up the Intelligent Control suite of programs.

Intelligent Incident requires that Intelligent Control is installed and functional.

INSTALLING INTELLIGENT INCIDENT

Intelligent Control must be installed before Intelligent Incident.

1. Install the standard system

- i. Load the CD into the CD drive on the computer.
- ii. Select Start and then Run.
- iii. Either browse to setup.exe, or enter the drive letter and setup.exe in the command line (e.g. "D:\Intelligent Incident Setup v1.0.5.exe"– where D: is the CD Drive on your computer and v1.0.5 is the current version number).
- iv. Follow the prompts to install the system.

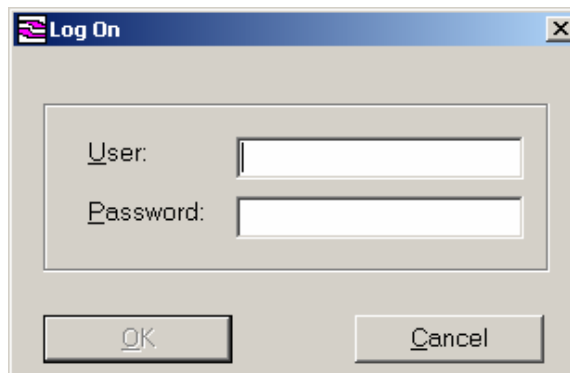
2. Start Intelligent Incident

Once Intelligent Incident is installed on the computer, open the software by clicking the shortcut from the desktop. If Intelligent Incident has not yet been installed, refer to the section headed Installing Intelligent Incident in this guide.

Click on this icon to open Intelligent Incident:

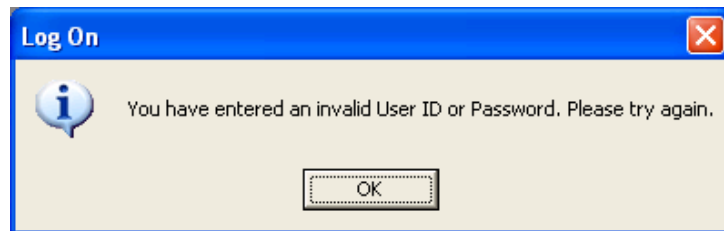


Once the system is loaded, the Log On screen will be displayed:



You will use the same User Name and password as the one you use for Intelligent Control.

If an incorrect User or Password is entered, the following message will be displayed:



Re-enter the User ID and/or Password.

Selections from the Main Menu (File, Operations, Administration, Window and Help) will not be accessible until you have successfully logged on.

MAIN MENU BAR FUNCTIONS

The Main Menu has the following options:

File, Operations, Administration, Window and Help.

FILE

The File menu consists of the following options:

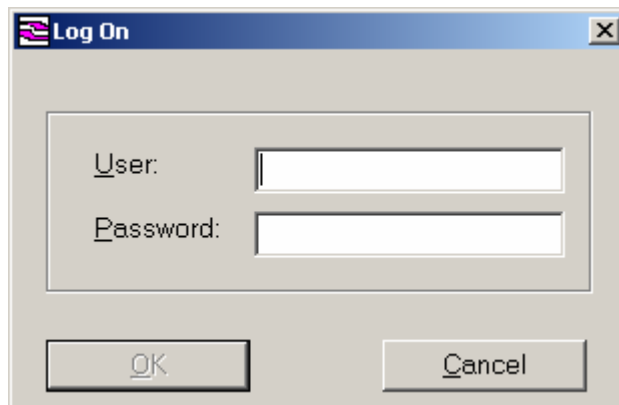
- AutoStart
- Log On
- Log Off
- Change Password
- Timeout
- Extended Logging
- Large Toolbar Icons
- Exit

AutoStart

If the instance of Intelligent Incident that is running on a client computer running a video wall in a Traffic Management Center, you can start that instance of Intelligent Incident automatically, without having a user log in. In this case, the AutoStart option will have a check next to it in the File Menu list and when Intelligent Incident is started, the current map will automatically be displayed.

Log On

Use the Log On screen to enter a User and Password to access the Intelligent Incident software.

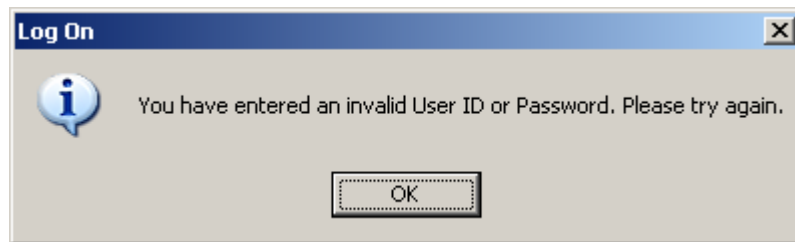


User is the name used to log on to the system. The name that is entered can be up to 10

characters in length and can consist of alpha and/or numeric characters. Note that the name is case sensitive.

The Password is unique to a User. It can be up to 10 characters in length and can consist of alpha and/or numeric characters. The password is case sensitive. Please make a note of the Password for each User.

Press enter or click on the OK button when the required information has been entered. If a valid User and Password is entered, the Log On window will close and the Main Menu will be enabled. If an invalid User or Password is entered, a message will be displayed advising you of the fact and allowing you to rectify and continue.

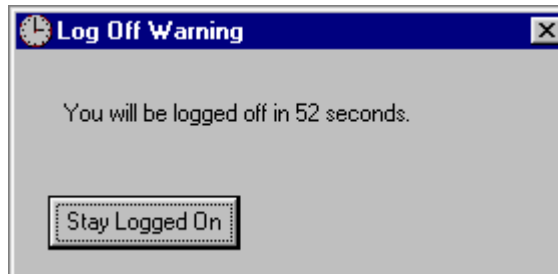


Only one User can be logged on at any one time. To log on as a different User, first log off as the current User and then log on again using another User name.

Log Off


Use the Log Off option to log off from the system. This function will not close the software. To close the software, select the Exit option.

If there is no activity for a specified period of time (as specified using the Timeout option on the File menu), a Log Off Warning window will appear, warning that the user will be logged off.



To remain logged on, click on the 'Stay Logged On' before the time indicated has elapsed.

Change Password



The 'Change Password' dialog box features a title bar with a close button. It contains three input fields: 'Old Password', 'New Password for Level1 Password', and 'New Password for Level1 Confirm'. At the bottom, there is a 'Change' button and a 'Close' button. A small icon is visible in the bottom-left corner of the dialog.

Use this utility to change passwords. The User is displayed for reference purposes. To change the Password, first enter the Old Password. If your entry for Old password is invalid, the following message will be displayed:

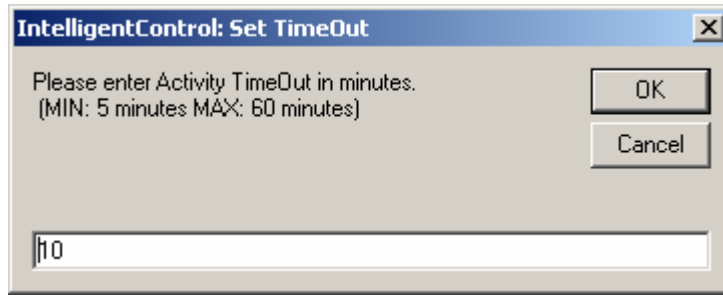


Correct the Old Password and then enter the new Password in both the Password field and the Confirm field. Click the Change button to update the User record with the new Password. If the same Password is entered in both fields (Password and Confirm), a message will be displayed advising that the password change was successful. The new Password will be effective immediately. Make a note of the new Password.

If the same Password is not entered in the Password and Confirm field, a message advising that the Passwords do not match will be displayed. The Change Password form will open again. Re-enter the same Password information into both fields and click the Change button to update the User record with the new Password.

Click on Close to close the form.

Timeout



Enter the number of minutes of inactivity that should pass before the timeout warning window is displayed. The value entered here can be between 5 and 60 minutes. Note that the default is 10 minutes and this value will automatically be entered when this option is selected from the File menu.

When the specified period of inactivity is reached, the following window will be displayed, allowing the User to choose to stay logged on:

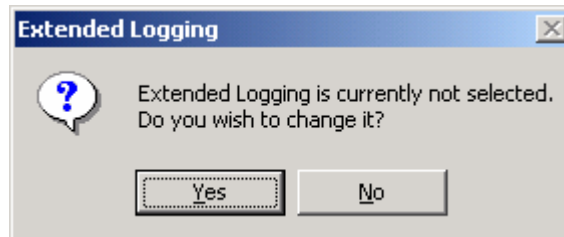


Click on the Stay Logged On button within the 10 seconds allowed, to remain Logged On under the current User. If you do not click the Stay Logged On button you will be logged off the system.

Extended Logging

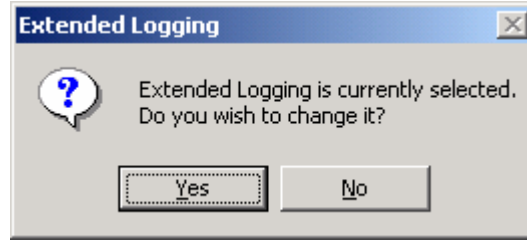
Extended Logging controls the amount and type of detail that is included in the log files. For standard operation, extended logging should not be turned on. It should only be turned on if additional detail is required in the log file for diagnostic purposes.

If Extended Logging is not selected, when the menu option is clicked, the following window will open:



Click the Yes button if extended logging should be activated or click No to leave extended logging inactive.

If Extended Logging is already selected, when the menu option is clicked, the following window will open:



Click the Yes button to turn extended Logging off or click No to leave Extended Logging active.

Large Toolbar Icons

All of the functions that can be accessed using the Menus in Intelligent Incident have associated Icons that are displayed on the left hand side of the screen. These Icons can be displayed in two sizes – normal and large. To have large icons displayed, select Large Toolbar Icons from the File menu. As soon as you do this, the Icons displayed will change to the larger size. To change from large toolbar icons to normal size, select Large Toolbar Icons from the File menu and the icons will immediately revert to the normal size.

A check mark next to Large Toolbar Icons in the File menu indicates that the large icons are selected.

Exit

Select this option to exit Intelligent Incident and close the software. To leave the system open for later Log In, select the Log Off option. If the system is connected to a Device at the time you Exit, that connection will automatically be closed.

OPERATIONS

The Operations menu consists of the following options:

- Incidents
- GIS Map View of Incidents
- Incident Management
- Incident Event Log
- Refresh Incidents
- Run...

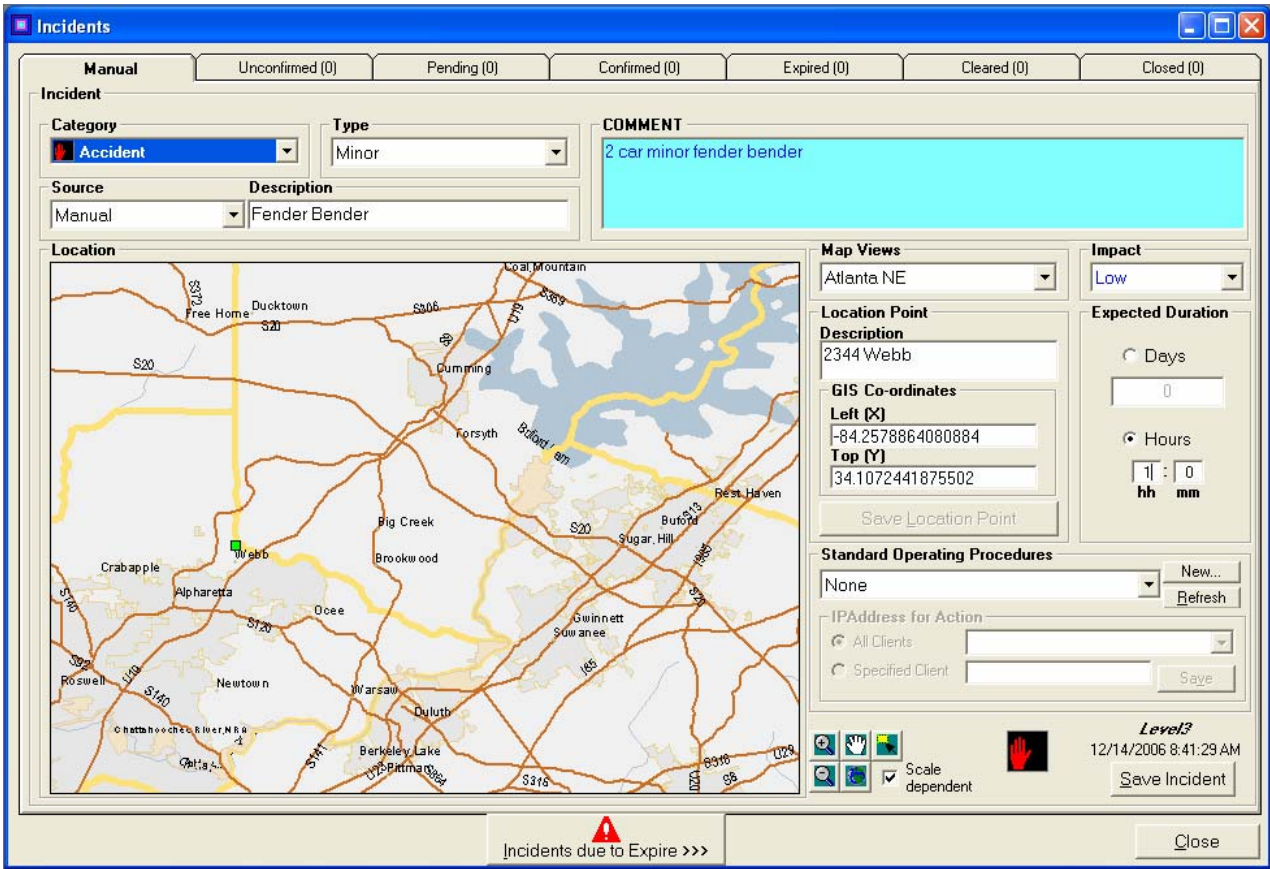
Incidents

This is where all the reported incidents can be view and are managed. When an incident is reported, the operator will enter the details of the incident here, by clicking the Manual tab and selecting and/or entering the correct options.

The Incidents Screen consists of several tabs. These tabs are used to group the incidents into categories so that they can be more logically viewed and managed.

Manual	This is where incidents are manually entered.
Unconfirmed	This is a list of the incidents that have been reported but not yet confirmed
Pending	This is a list of incidents that have been reported or scheduled but are in a pending status.
Confirmed	This is a lit of all the incidents that have been reported or scheduled and have been confirmed.
Expired	This is a list of incidents that have expired (their duration has passed) and they have not been cleared or closed.
Cleared	This is a list of incidents that have been cleared but cannot be closed yet as some further action is required.
Closed	This is a list of all the incidents that have been closed.

The Manual tab is different from all the others in that this is where the incident is reported. All the other tabs have identical content.



Category Indicates the broad category into which the incident falls. Examples would be accident, road works, maintenance etc. If the category that you wish to use does not display in the drop down list, you will have to add a new category as described in the Administration section of this User Guide.

Type Further defines the incident in terms of its category. For example, in the Accident category you could have type like fatal, minor, with injuries etc. If the type that you wish to use does not display in the drop down list, you will have to add a new type as described in the Administration section of this User Guide.

Source This indicates how the incident was reported:

Manual It was called in, emailed in, or was viewed on camera and reported.

Scheduled The incident is scheduled – a routine expected event. An example for this would be road closure for schedule maintenance.

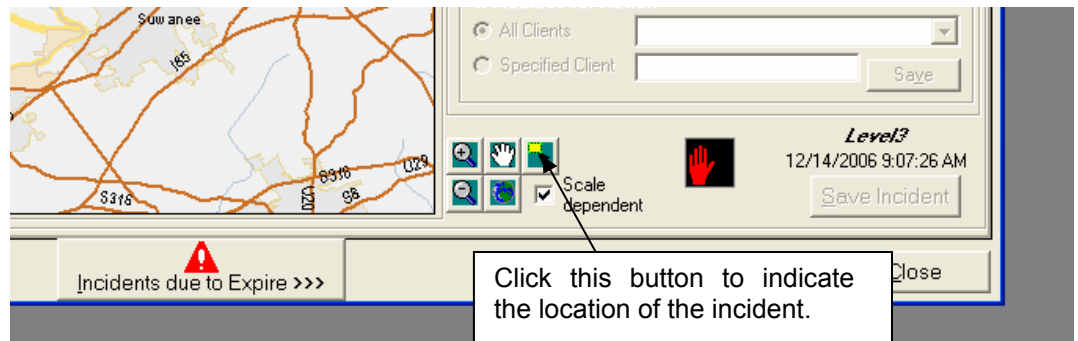
Auto Detection This incident was generated by the Central Schedule in Intelligent Control.

Description This is a brief description of the incident. It will display on the Incidents lists and in all reports so it should be as meaningful as possible

- Comment** This is a mandatory field and must be entered. It will be displayed in the log of the incident and should contain further details of the incident.
- Map View** Select the map on which the incident is to be displayed. Only the maps that have been created in Intelligent Control will be available for selection.
- Impact** Indicate the impact that the incident is having on traffic. The available options are Low, Medium, High and Emergency.
- Location Point** You must enter the description of the location. This is the information that will display on the incident lists and reports, so make it as accurate and as meaningful as possible.

The values of the GIS Co-ordinates will automatically be displayed when you select the location.

To add the location for the incident, click on the New Location button situated to the right of the map view.



When you click that button the cursor will change to a cross hair. Position the cursor at the incident location and click the mouse button. The GIS Location points for that position will automatically be entered.

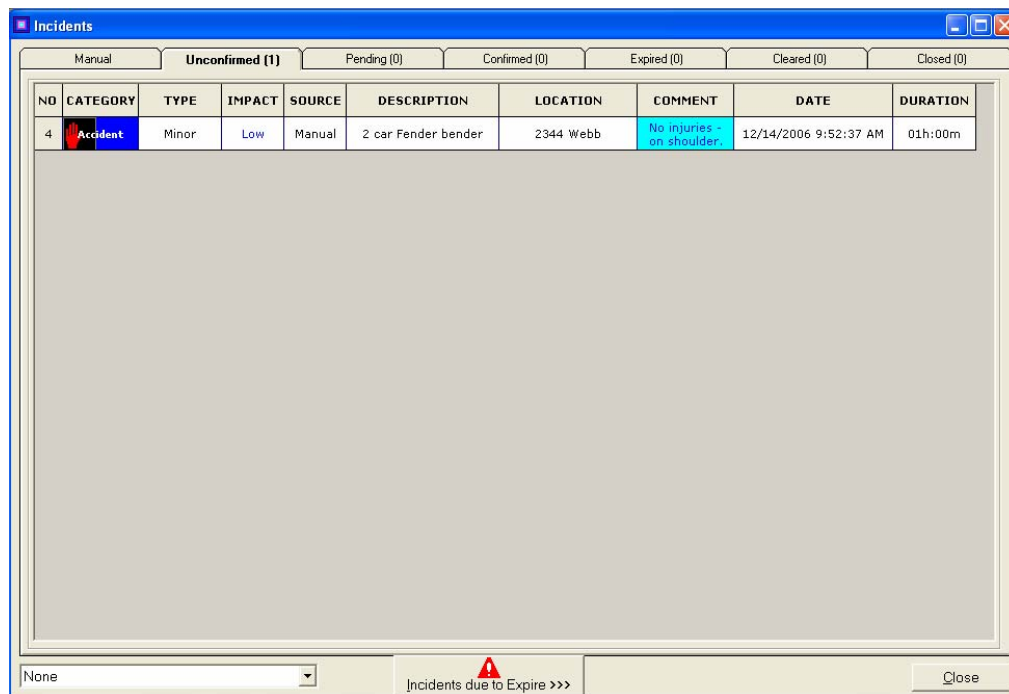
- Expected Duration** This indicates – either in days or hours, the length of time that it is anticipated that the incident will be active. This information is informational only.
- Standard Operating Procedure** If a standard operating procedure is to be attached to this incident, select the procedure from the drop down list box. If no standard operating exists, click on New to create one for this incident.

Once all this information has been entered, click on the Save Incident button. The incident

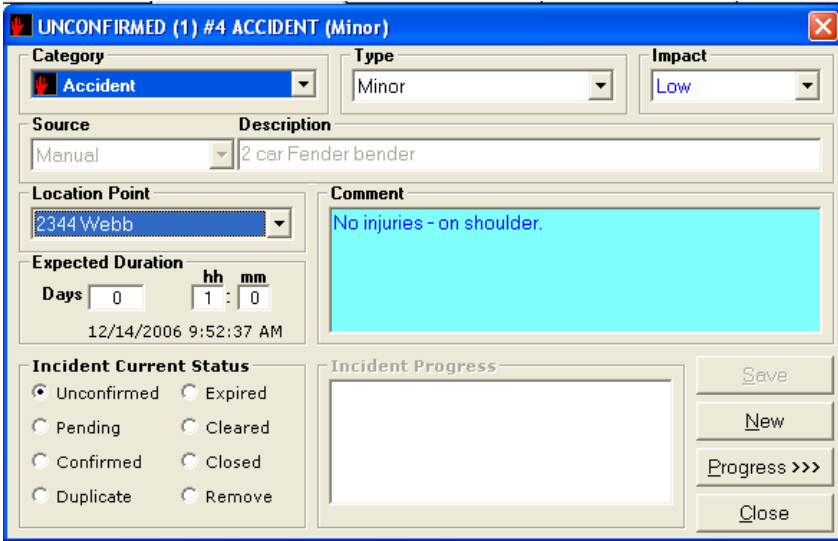
will be added to the database as an “unconfirmed” incident. And will appear in the Unconfirmed Tab list.

Once the Incident is in the Unconfirmed Tab list, it will be reviewed by a supervisor or manager, who would then update its status accordingly.

Click on the Unconfirmed tab to display the list.



As you will see, all the information that you captured when the incident was recorded, is displayed here. To access the incident and update its status, double click on any field within the record, and the following “Job card” window will open:



At this point, the supervisor can edit any of the displayed information and update the incidents' status.

Incident Current Status

This is where the current status of the incident can be changed.

- Unconfirmed** The incident is still not confirmed and must remain on the unconfirmed list.
- Pending** The incident is confirmed but certain details are still pending. It will be moved to the pending tab list.
- Confirmed** The incident is confirmed and will be moved to the Confirmed tab list. It will also be displayed on the GIS Map View of Incidents screen.
- Duplicate** The incident has already been reported and should be removed as a duplicate. This incident will be removed from the unconfirmed tab.
- Expired** The incident has expired – its duration has passed- but it has not yet been cleared or closed on the system. The incident will be transferred to the Expired tab.
- Cleared** The incident has been cleared and is no longer a problem, but some action is still required. The incident will be moved to the Cleared tab.
- Closed** The incident is closed – no further action remains. The incident will be moved to the Closed tab.
- Remove** The incident is invalid and must be removed from the database. This incident will not appear on any of the tabs.

Once you have selected the appropriate status, the Incident Progress will automatically be updated as shown below.

UNCONFIRMED (1) #5 ACCIDENT (Fatality)

Category: Accident | Type: Minor | Impact: Low

Source: Manual | Description: 2 car Fender bender

Location Point: 2344 Webb

Expected Duration: Days: 0 | hh: 1 | mm: 0
12/14/2006 10:09:03 AM

Incident Current Status:
 Unconfirmed Expired
 Pending Cleared
 Confirmed Closed
 Duplicate Remove

Incident Progress:
Status changed from UNCONFIRMED to CONFIRMED.

Buttons: Save, New, Progress >>>, Close

Click on Save to update the incident and it will automatically be moved to the correct tab.

If at any time you wish to view a log of the progress of the incident, double click on that incident to open the Job Card, and then click on the Show Pogress button to display the log as follows:

CONFIRMED (1) #5 ACCIDENT (Minor)

Category: Accident | Type: Minor | Impact: Low

Source: Manual | Description: 2 car Fender bender

Location Point: 2344 Webb

Expected Duration: Days: 0 | hh: 1 | mm: 0
12/14/2006 10:09:03 AM

Incident Current Status:
 Unconfirmed Expired
 Pending Cleared
 Confirmed Closed
 Duplicate Remove

Incident Progress:
Status changed from UNCONFIRMED to CONFIRMED.

Buttons: Save, New, Progress >>>, Close

Progress	User	Elapsed Time	Date
Status changed from UNCONFIRMED...	Level3	00h:02m	12/14/2006 10:11:15 AM

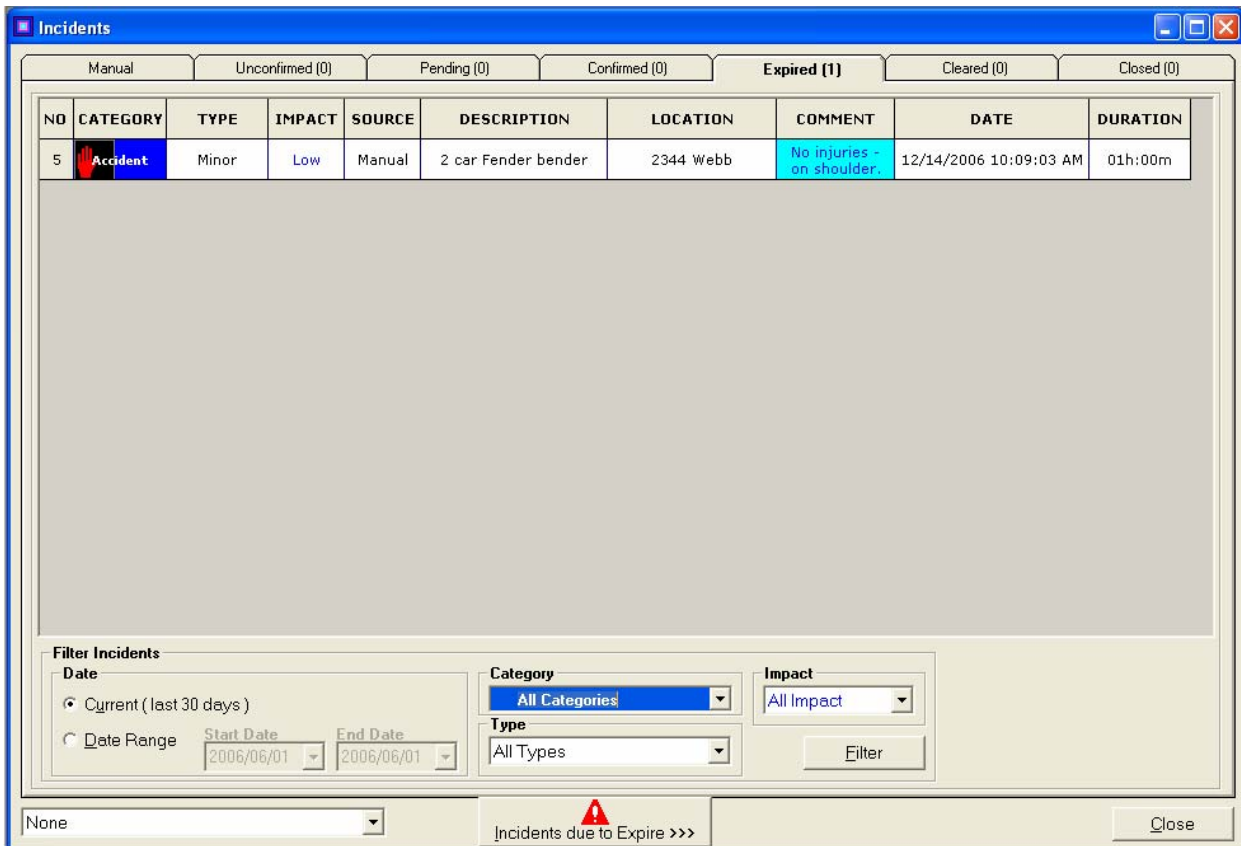
Click on Close to close the Job card without making any changes.

Incidents Due to Expire



The Incidents Due to Expire button will flash when any Incidents (on any tab) are due to expire. This is in order to draw the operator’s attention to the expiring incident so that the information can be checked and updated if necessary. If an incident is allowed to expire, it will be moved to the Expired tab.

Expired, Cleared and Closed Incident Tabs



In addition to the information that is included on the other tabs, these tabs have a section that allows you to further define which incidents you want to include in your list when you view it.

Filter Incidents

These are the parameters that can be chosen to narrow down the list that is displayed if necessary. You can chose to filter the incident list using any of the following:

Date You can select only those incidents that fall within the last 30 days, or you can enter a specific date range.

Category You can select only a specific category of incident for display.

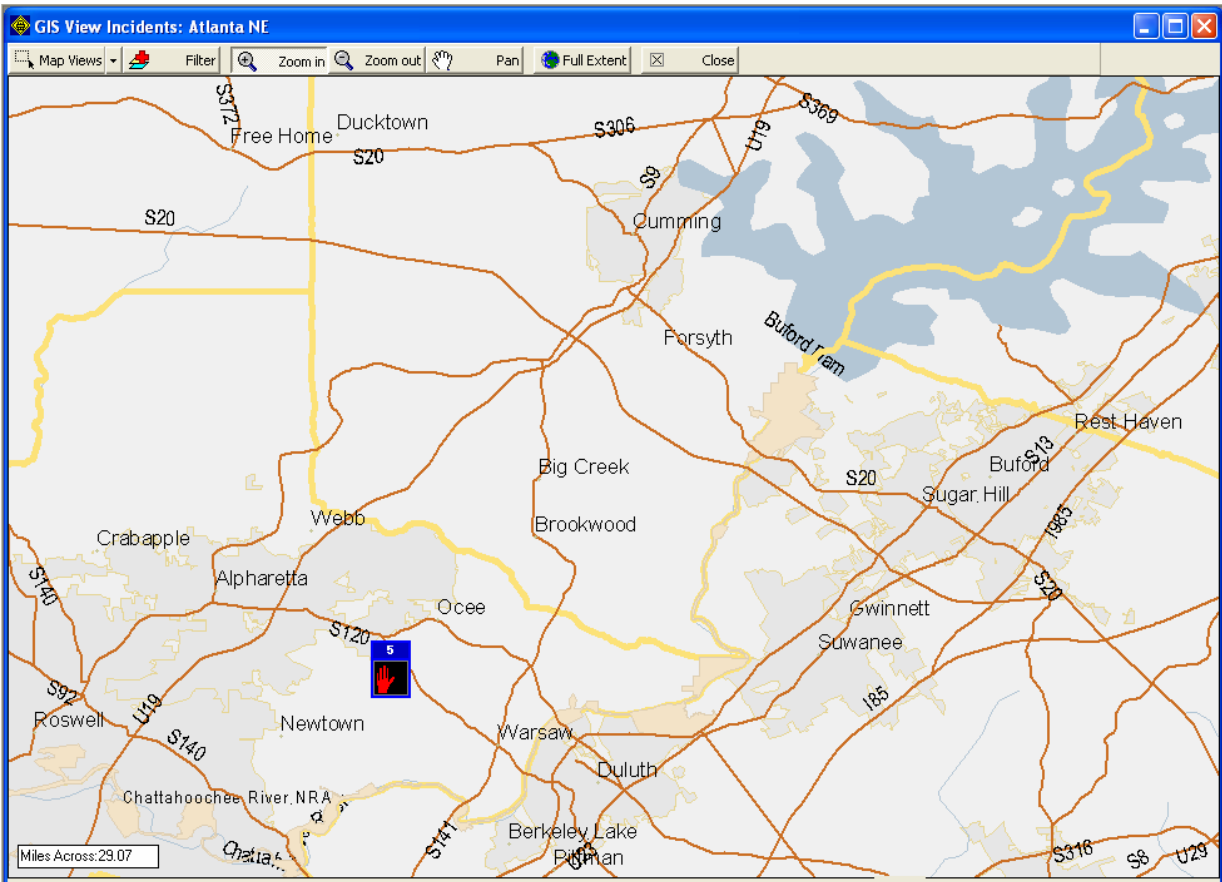
Type You can select only a specific type of incident within the category.

Impact You can select incidents based on their impact.

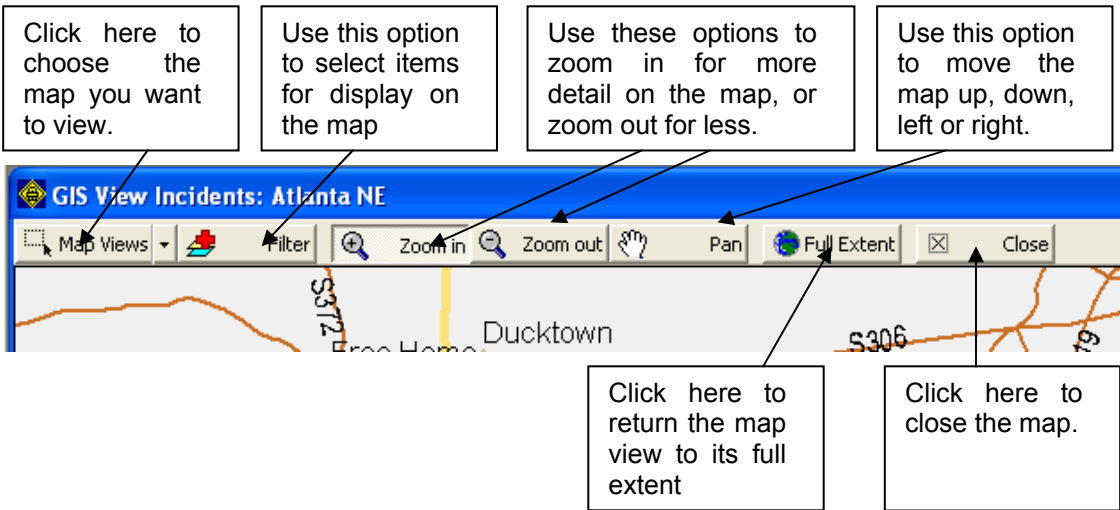
Once you have made your selections, click on the filter button and only those incidents that meet the parameters that you have entered will be included in the displayed list.

GIS MAP View of Incidents

This is a pictorial view of all confirmed incidents that have been reported. To view the Job Card for a particular incident, double click on the Icon that depicts the incident.



The map view can be manipulated using the buttons on the top task bar.



Map Views

You can select another map for viewing by clicking on the Map Views drop down list and highlighting the map that you wish to access.

Filter

Use the drop down list to display all the items available for display. Put a check in the box adjacent to this items that should display on the selected map. If an item is not checked, it will not display on the map.

Zoom in and Zoom out

When you Zoom In on a map, the detail level of the map itself will increase, as will the level of detail on the Icons for the Devices. To zoom in to an area, click the Zoom In button and then, holding the left hand mouse button down “draw” a box around the area that you want to look at, and release the mouse button. The Map and the Device icons will be repositioned and resized, still correctly reflecting the correct geographical position of the Devices.

To Zoom out to get a wider view of the map area, click on the Zoom Out button and then click the left hand mouse button anywhere on the map. The Map will Zoom Out one level (the actual details levels are set by the administrator) with each click on the mouse. The Device Icons will be repositioned and resized with each level.

Pan

To pan to another area of a map, click on the Pan Icon. The cursor will change to look like a hand. Position the cursor on the Map, and holding down the left hand mouse button, move

the map until east, west, north or south. The map will relocate, and the Devices will remain located in the actual geographical positions. Note that while you are actually moving the map, parts of the screen will appear blank, As soon as you release the mouse map, the entire screen will be redrawn with the new view area displayed.

Full Extent

To get back to the original map and display, click on the Full Extent button. This will revert the map to its original saved zoom level and icon display.

Close

Click here to close the map view.

Incident Management

Incident Management is a tool that allows you to automate processes that are predefined, depending on data that is received from external sources. At preset intervals, Intelligent Control will poll the Devices, retrieve specified data, use that data in calculations to determine the action (if any) that should be triggered. Incident Management uses Excel as the calculation engine. A standard Excel spreadsheet template is provided and this forms the basis for all the calculations that are performed by the Incident Management feature.

The spreadsheet consists of 3 sheets. The first sheet contains the input that is to be used to determine if any action needs to be taken. The data from this sheet is passed to the second sheet which manipulates the data and thus determines if any action needs to be taken. The results of the data manipulation are passed to the third sheet which then triggers the required output, depending on the outcome from the second sheet.

When you select Incident Management, the following overview window will open, allowing you to see the current status of any Incident Management procedures that have been created.

The Incidents that have been specified are listed here.

Further details of the selected Incident will be found here.

This button will either display Configure Spreadsheet or View Communications, depending on which view is currently selected. View Communications displays a log of the communications and results of the polling of the devices. Configure Spreadsheet displays details so that you can configure a spreadsheet for Incident management.

The Polling Rate indicates the interval at which Devices will be polled for each Spreadsheet, assuming the Polling is set to On for the Spreadsheet.

These are the available Device Types and Devices. Data from these Devices can be used for input for calculations or an action can be triggered for the Device based on the calculations made by Intelligent Control.

Each Device Type will have a list of values that can be used as data for calculations. Select the ones that you want to include as Input for the calculation.

This button will force the retrieval of Input Values so that the spreadsheet is calculated and any required output is triggered.

Database Management

Spreadsheet Name	Rate	Poll
<input checked="" type="checkbox"/> Accident	1	NO
<input checked="" type="checkbox"/> Travel Times	5	YES

Name
Travel Times

File Directory
C:\Program Files\Intelligent Control\Incident Management Spreadsheets\

Save As... **Delete...** **New...** **Retrieve latest database log values and re-calculate spreadsheet**

Actions Enabled

Polling Rate
5 Minutes

Polling
 ON OFF

Spreadsheet Column Selection

Device	OID Name
Overhead 1	dmsM
Sensor 27	percent
Sensor 27	percent
Sensor 27	endTime
Sensor 27	endTime
Sensor 27	sensor
Sensor 27	sensor
Sensor 27	speedDataBuffer_1_1
Sensor 27	speedDataBuffer_2_1
Sensor 27	volumeDataBuffer_1_1
Sensor 27	volumeDataBuffer_2_1
Sensor 28	percentOccupancyBuffer_1_1
Sensor 28	percentOccupancyBuffer_2_1
Sensor 28	endTimeBuffer_1_1
Sensor 28	endTimeBuffer_2_1
Sensor 28	sensorZoneOptions_1_1
Sensor 28	sensorZoneOptions_2_1
Sensor 28	edDataBuffer_1_1
Sensor 28	edDataBuffer_2_1

Configure

Device Types

- Weather Stn 1
- Overhead
- Camera
- Sensor
- Portable Sign
- VS
- ASC

Available Log table Columns

- essAirTemperature_1
- essAirTemperature_2
- essAvgWindDirection
- essAvgWindSpeed

Close

Spreadsheet Information

Name

The Name of the Spreadsheet will indicate exactly what sort of Incident is being managed.

File Directory

The Directory, including the full path and file name in which the selected incident's spreadsheet is located will be displayed here.

Polling Rate

The Devices that are included for Incident Management can be polled at selected intervals. The value here indicates how often the Devices will be polled to retrieve information and start the Incident Management process.

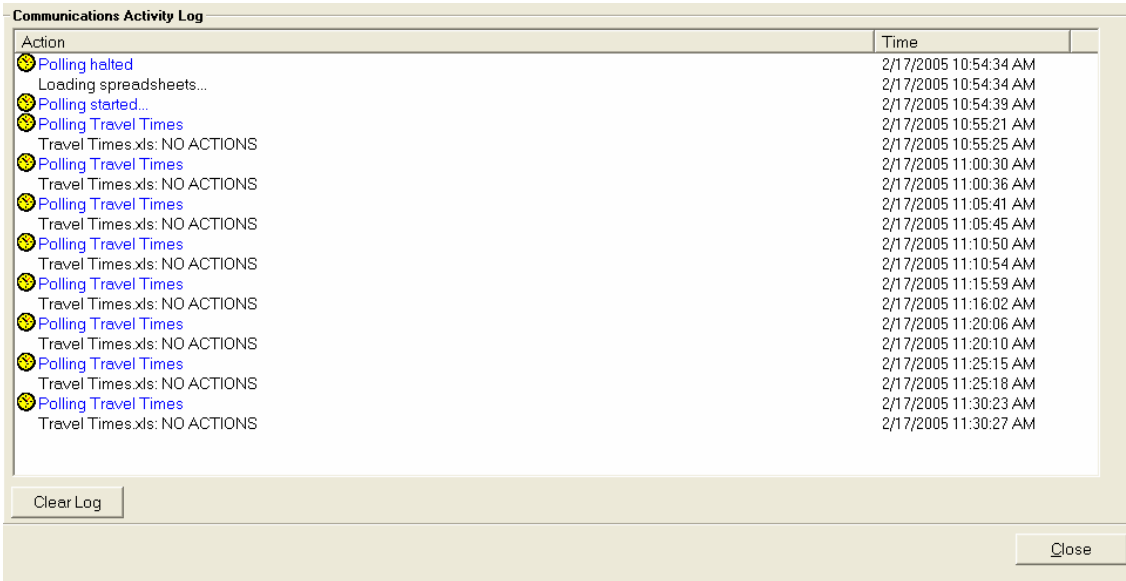
Polling

Indicate here whether or not Intelligent Control is to poll the Devices.

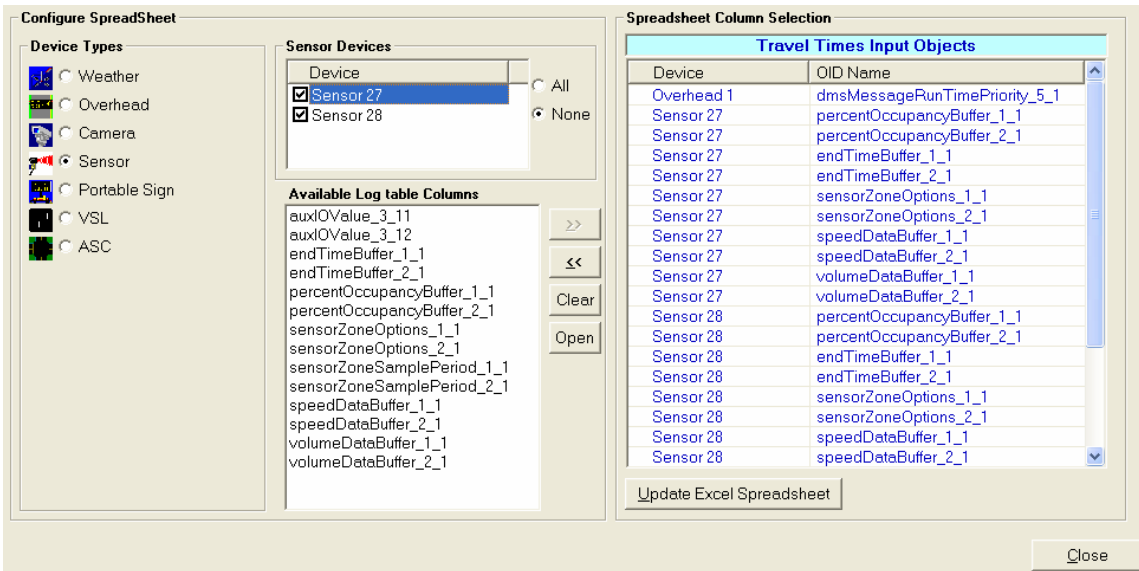
Actions Enabled

Configure Spreadsheet/View Communications

This button will display Configure Spreadsheet if you are currently in View Communications mode:



It will display View Communications if you are currently in Configure Spreadsheet mode:



Configure Spreadsheet is used to select the objects that are to be used as input for calculations by Excel for Incident management.

Device Types

All the Device Types that have been configured in Intelligent Control will be listed here for selection. Select the required Device Type by clicking on the Radio button next to its name.

Devices

All the Devices of the selected device Type will be listed here so that you specify exactly which Device(s) will provide the input for the calculations. Select the Device(s) by checking the check box next to the name of each device in the Devices window.

Available Log Table Columns

All the objects that are available as input for the calculations will be displayed here. Note that only the objects that have been included on the Log that is configured on the Map for each Device will be available for selection. If an object does not appear here, then you should add it to the Log for that Device by editing the Log on the Map.

Spreadsheet Column Selection

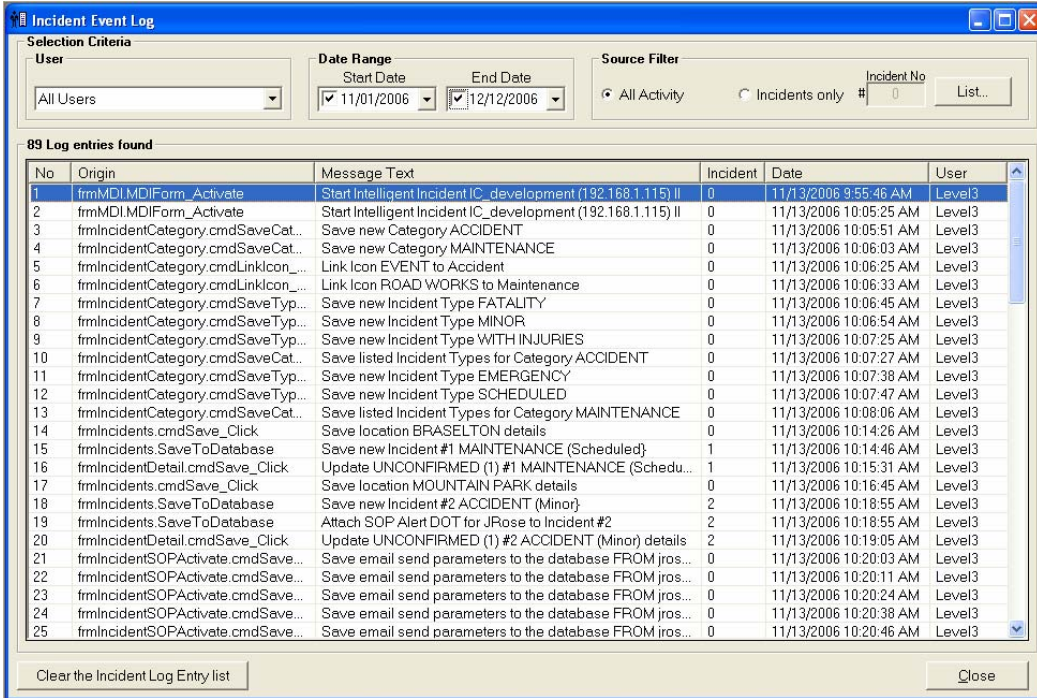
This displays all the Objects that you have selected to be used as input on the Excel spreadsheet.

Update Excel Spreadsheet

Clicking this button will update the spreadsheet for the highlighted Incident Management function and will open Excel so that the spreadsheet can be further manipulated if required.

Incident Event Log

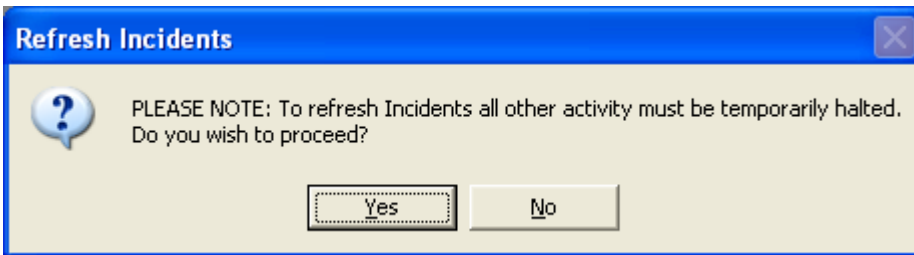
This is a log file that displays all the activity in Intelligent Incident.



Refresh Incidents

This utility is used to refresh the database and the map view. Use it only if incidents are not appearing correctly in the Incident Management section or on the GIS Map View.

When you chose this option, the following warning will be displayed.



Click yes to proceed and the database will be updated.

Run

This utility allows you to run other executable programs from within Intelligent Incident.

ADMINISTRATION

The Administration Menu consists of the following options:

- Configure
 - Alarm Thresholds
 - Alarm Responses
 - Incident Category Management
 - Incident Location Management
- Operators
 - Access Levels
 - Profiles

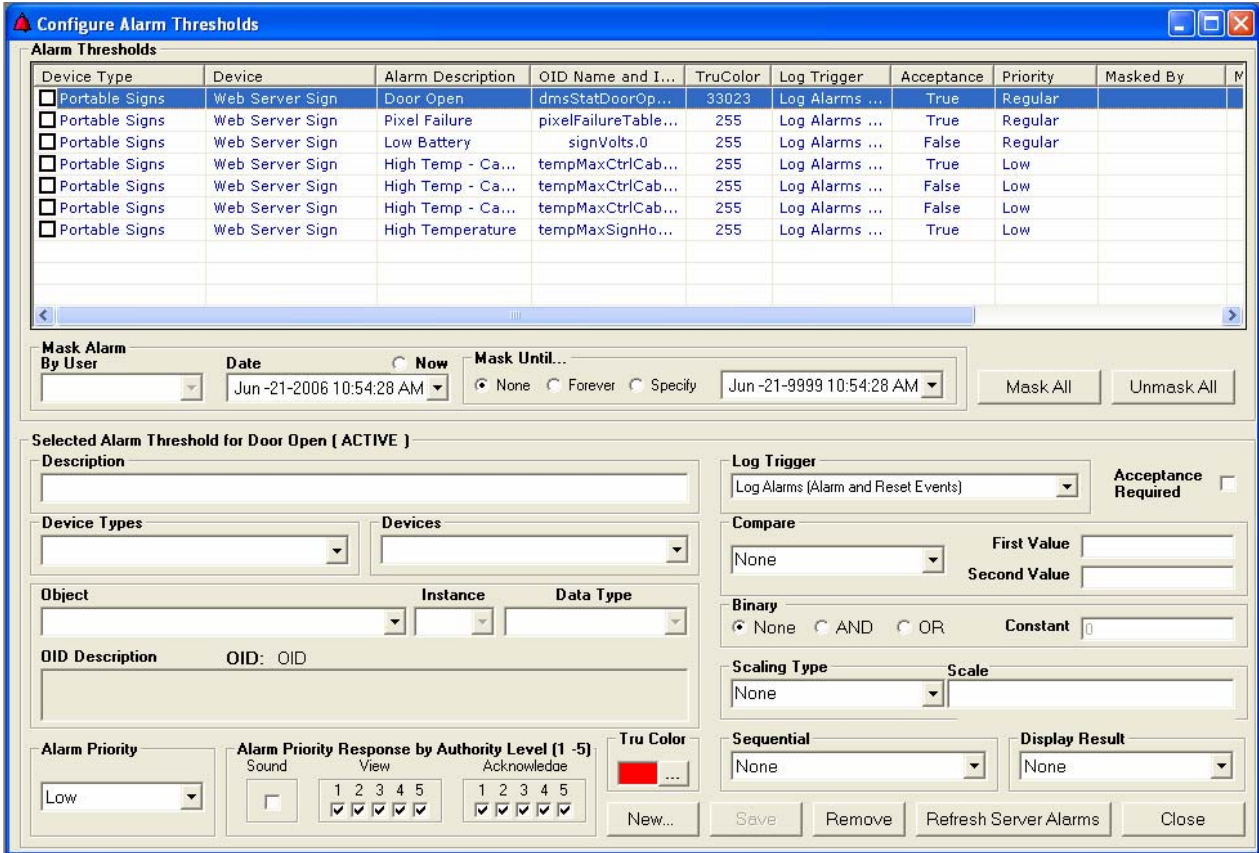
Configure

The Configure section is where you configure some of the features in Intelligent Incident to accommodate your unique requirements.

- Alarm Thresholds
- Alarm Responses
- Incident Category Management
- Incident Location Management

Alarm Thresholds

You can identify and specify the conditions under which Devices should report alarm situations. The Alarm Thresholds function (Administration, Configure, Alarm Thresholds) is where you set the parameters for each Device and the conditions under which that Device should report an alarm.



Mask Alarm

Alarms will typically trigger each time a Device is polled. In some instances, this will become an annoyance and you might want to suppress the alarm for a period of time. If an alarm is masked, it will alarm the first time it is triggered and then not until it is unmasked or the mask expires.

By User

The User that last masked or unmasked the highlighted alarm will be displayed here.

Date and Now

The date from which the alarm should be masked is selected here. To set the date to the current computer date, click on Now. Otherwise enter the required date.

Mask Until

You can select to mask an alarm for specific periods of time. The alarm state for the Device will not be reported while the alarm is in mask status. You can select one of three options for the duration of a mask.

- None The Alarm will be triggered each time the Device is polled
- Forever The Alarm will be triggered the first time but not again until the mask is

removed.

Specify The Alarm will trigger the first time the alarm condition is met, and then not again until after the specified date and time. The date and time is selected from the drop down list box.

Mask All

Click this button if you want all the Alarms to be masked. This would typically be used on a holiday when it is known that there will be no one available to respond to the alarm.

Unmask All

Click this button to remove any and all masks from the listed alarms.

Alarm Threshold Information

This is where you enter/edit the information for each alarm threshold for the Devices.

Description

Enter the name of the alarm. Make the name as descriptive as possible so that it is obvious what the alarm is for when it is displayed. This is a free format field.

Device Types

Select the Device Type from the drop down list box. All the Device Types that are installed on Intelligent Control will be shown so that you can make your selection.

Devices

Select the Device for which you are setting up an alarm. Only the Devices of the selected Device Type will be available for selection.

Object

All the available Objects for the selected Device will be displayed. Select the one that is to be used for the alarm.

Instance

If there is more than one instance of the Object, select the required Instance here.

Data Type

This will display the type of data that the object contains.

OID Description and OID

The Description and number of the OID will be displayed here for verification purposes.

Alarm Priority

This is where you select/edit the priority level for each alarm. Select the required Alarm Priority level from the drop down list box.

Alarm Priority Response by Authority Level (1-5)

The parameters that have been set for each level will display in the Alarm Priority Response by Authority fields. Note that the information in this section is pre-defined and is displayed here for information only. To change any of the Alarm priority values, select Administration, Configure, Alarm Priority Responses.

Tru Color

This indicates the color that will be displayed when the Device is in an alarm state.

Log Trigger

This is where you select which Events and Types of Alarms should be logged. Select from the following available options:

Log Alarms (Alarm and Reset Events)	Log alarms only for both Alarm and reset events.
Log Alarms (Alarm Events Only)	Log alarms only for alarm events.
Log Alarms and Reset (Alarm and Reset Events)	Log alarms and resets for both alarm and reset events.
Log Alarms and Reset (Alarm Events Only)	Log alarms and resets only for alarm events.
No Logs (Alarm and Reset Events)	Do not Log any information
No Logs (Alarm Events Only)	Do not log any information for alarm events.

Acceptance Required

If this box is checked, the Device will display in an alarm state until a user with the correct level of authority accepts (acknowledges) that alarm.

Compare

If you are generating an alarm for an OID that can be compared to a set value or range of values, you can specify the type of comparison and the values for that comparison here. The types of comparison that can be performed are:

None	No comparison will be made.
> than	The OID value should be greater than the value entered in First Value.
< than	The OID value should be less than the value entered in First Value.
= to	The OID value should be equal to the value entered in First Value.
Between range	The OID value should be between the value entered in First value and The value entered in Second value

Outside Range The OID value should fall outside the values entered in First Value and Second value.

First Value

This is the first and only value that will be used if the OID value is being compared to a single value.

Second Value

This is the second value that will be used if the OID is being compared to a range of values.

Binary

These fields can be used instead of the Compare section described above. By referring to the manufacturers' specifications for a Device's NTCIP objects, it is possible to use the binary value to define the threshold.

Select AND or OR depending on how you want the constant added to the original binary value for the object in question.

Constant

A decimal value that will be converted to a binary number to be used with And or Or to determine the threshold.

Scaling Type and Scale

NTCIP values are often reported in measurements that are not easily understood. For example, battery voltage is reported in hundredths of a volt. The more meaningful value for a user would be whole volts. You can specify here the scale that is to be used to adjust the NTCIP value to a more understandable value for the User. In this case, the scale type would be multiply and the scale would be .01 to bring the returned OID value into whole volts for displaying on the grid. The valid options for scaling are:

ENUM
NTCIPDATE
FORMULA
MULTPLY
DIVIDE

Sequential

This field is not in use at this time.

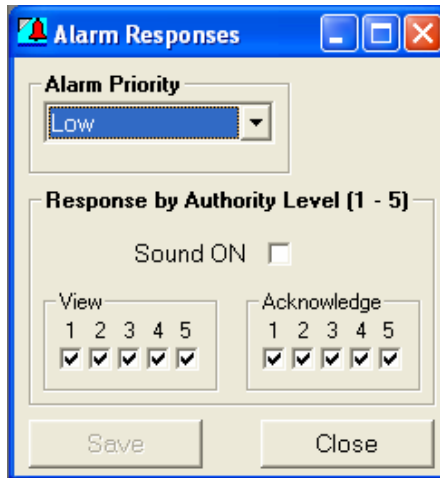
Display Result

This drop down list allows for three choices:

- None Select this value (the default) if the results should be displayed in their native NTCIP format.
- Decimal (2 positions) Select this option to convert an NTCIP numeric value to a 2 digit decimal value.
- English Format Select this option to display words / messages without the tags. For example, a message from a sign in NTCIP format would be: TEST[nl]SIGN 1[nl]. In English Format, the same sign would be displayed: TEST SIGN 1

Alarm Responses

There are 4 levels of alarm priority that can be allocated to each alarm condition created. Alarm Thresholds are created using the Administration. Configure, Alarm Threshold. You can specify up to 5 Authority level responses for each alarm priority. For each of these levels, you can specify if the sound should be on and which of the 5 authority levels should have access to View and Acknowledge the alarm.



Alarm Priority

Select one of the following 4 alarm priorities:

- Low
- Regular
- High
- Emergency

Response By Authority Level (1-5)

Sound On

Check this box if you want the alarm to include sound. If you do not want the alarm to make sound, leave the box unchecked.

View

Check the authority level(s) that should have access to view the alarm for the selected priority level.

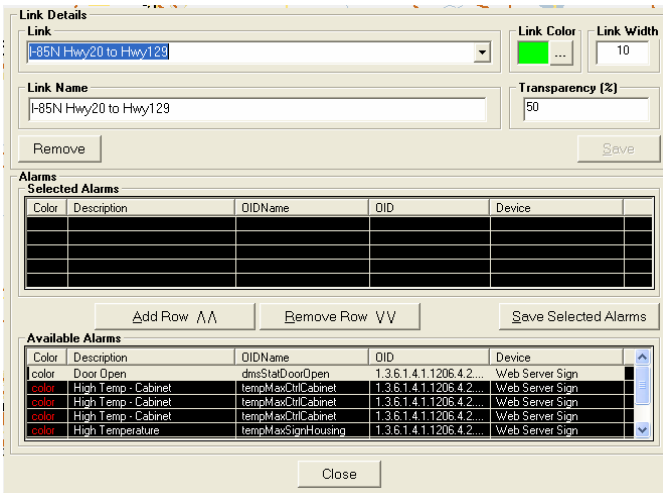
Acknowledge

Check the authority level(s) that should have access to acknowledge the alarm for the selected priority level.

Once you have set the parameters for each priority level, click on Save to update the database.

Link Alarms

To link alarms, first set up the alarms using Administration, Configure, Alarm Thresholds. Once the alarm thresholds are configured, click on Link Details and select the link to which an alarm should be applied. The Link Detail will be as displayed below, showing all available alarms:



Select an alarm under Available Alarms and click Add Row. This will copy the alarm into the Alarms section under Selected Alarms. Click Save Selected Alarms to save the alarms.

To remove an alarm from the selected link, click on the alarm that needs to be deleted in the Selected Alarms section and click Remove Row. Click Save Selected Alarms to save the changes.

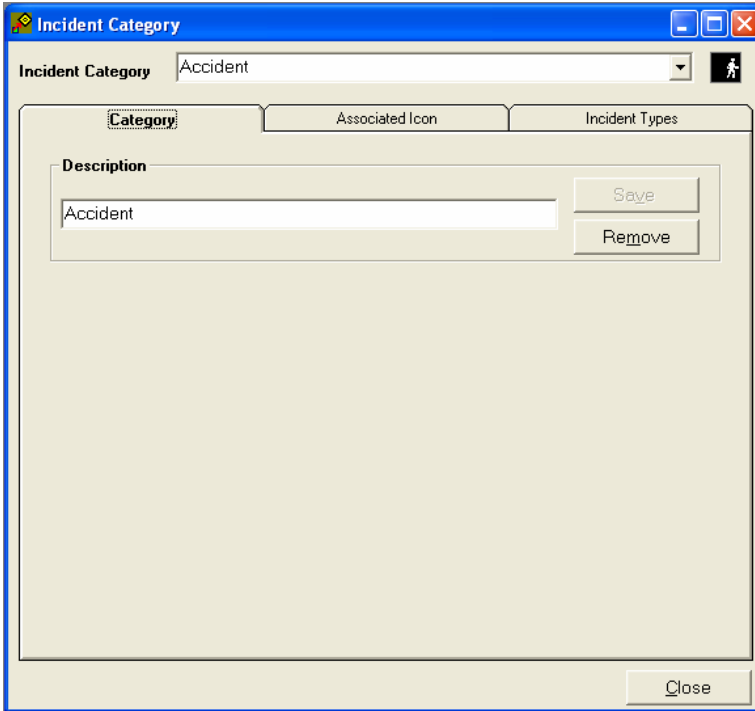
When you are finished adding or removing alarms from the list of selected alarms, click Close to exit this window.

Once alarms are set for a link, the thresholds will be checked as defined under Administration, Configure, Log Device Polling or Administration, Configure, Realtime Polling, Polling.

Incident Category Management

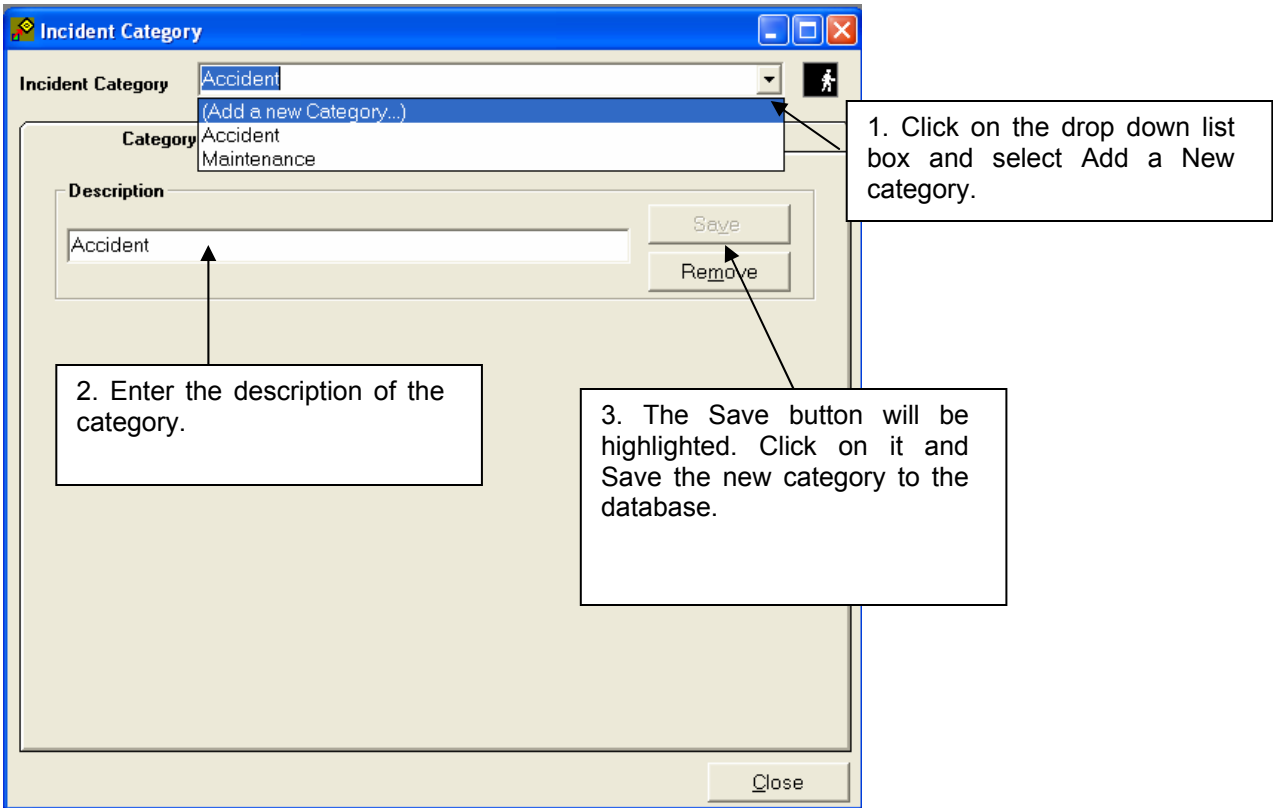
If you should find that a particular incident that you are adding to the Incident screen does not exist, this is where you would add the Category to cover that incident.

When you select the Incident Category option, the following window opens, allowing you to add a new Incident Category, change some details of an existing category or delete a particular category.



Adding a New Incident category

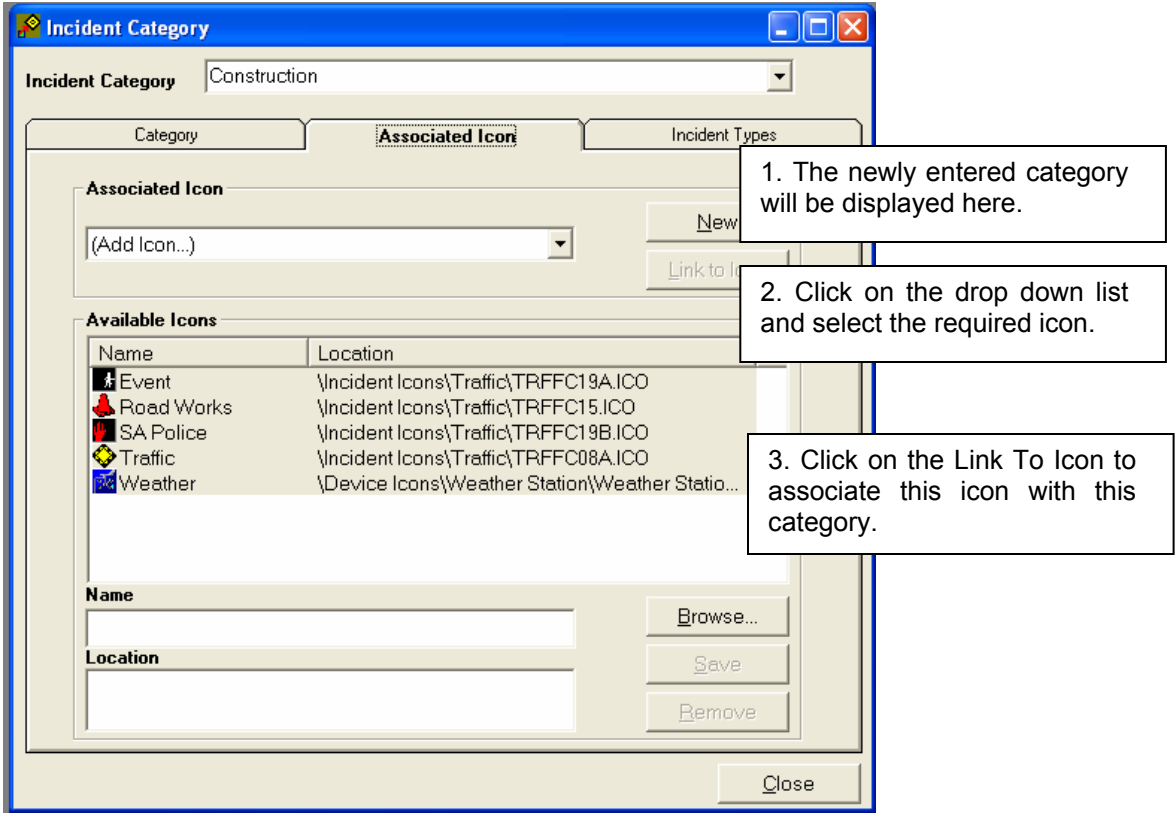
To add a new incident category, click on the drop down list box and select "Add a New category". The description field will be blank, allowing you to enter the description for the new category.



Incident Category is a drop down list that will display all the available incident categories. Additionally, it will display “Add a New category” which is the selection you should make to add a new type of incident..

Description is a free format text field that describes the Incident category. Make this name of the Incident as meaningful as possible so that any operator will understand the nature of the incident when it is displayed in Intelligent Incident.

Once you have entered the new incident category description, Click on the Save button to add the category to the database. Then click on the Associated Icon tab to select the icon that should be used when this incident is reported elsewhere in Intelligent Incident.



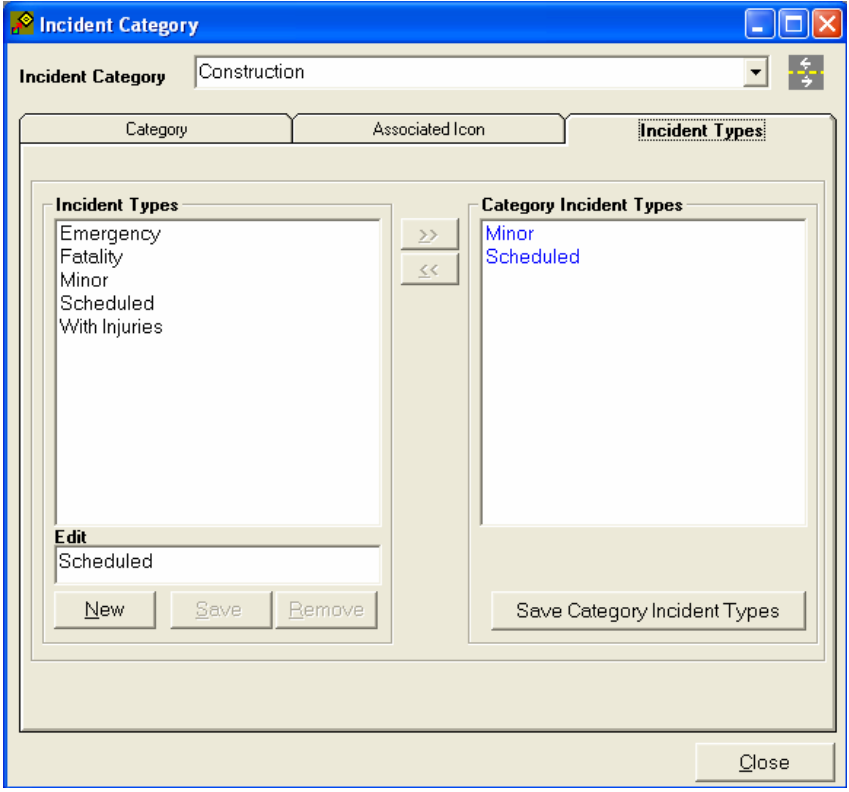
Either select an icon from the drop down list,. Or select Add Icon to add a new icon.

If you select Add a new Icon, Enter the Name for the new Icon and then browse to that icon by clicking on the Browse button. When you have selected the correct icon, click on Save. That Icon will now be included in the drop down list above.

Now you can select the required icon. Highlight that Icon in the drop down list box and click on Link To Icon. That icon will now be used to depict that category when it is displayed in Intelligent Incident.

Now that you have associated an Icon for the category, you will be able to define the “types” of occurrence for that category. For example, the accident category can have several types - minor, fatality, injuries etc.

Click on the Incident Types tab, and the following window will open:



All the Incident Types that have been entered already will be displayed in the Incident Types window. You will be able to select the ones from this list that are applicable for the new category that you have created. Double click on the Incident Type and it will be displayed in the Category Incident Types window. If a type does not exist, you can add a new type by clicking on the “New” button, and entering the new type in the Edit field. Then click on Save to add that new type to the list.

Click Close to exit the Incident category configuration utility.

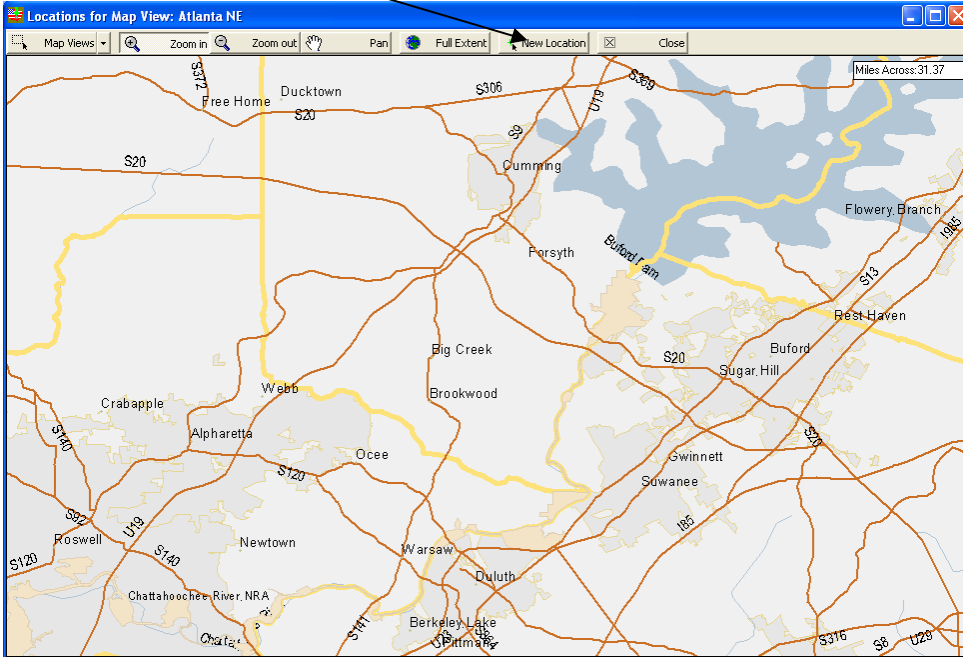
Now that you have created a category, you will need to add a default location for that category. This is used merely to create a record in the database. The actual location for each incident that is reported will be entered when the incident is captured using the Incidents screen.

Incident Location Management

Select Incident Location Management from the Administration menu. The following screen will be displayed:

Select the required map view from the Map Views drop down list.

Click here to add a new location.



Click on the New Location button and the cursor will change to a “Bullseye”. Drag the cursor to the required location on the map and right click the mouse. The icon will be displayed as a green square.

Click Close to close the Incident Location utility.

Operators

Access Levels

The screenshot shows a window titled "Access Levels" with a "Select Form:" dropdown menu. Below it is a table titled "Form Controls and Group Access" with columns for "Control Name", "Description", "Operations", "Maintenance", and "Administrator". At the bottom, there is a "Change Group Access Level" section with three dropdown menus for "Operations:", "Maintenance:", and "Administration:", along with "Apply" and "Close" buttons.

Various access levels for each of the users that have access to the system can be set. The functions that a particular user can access are set based upon the Access Level that is allocated for each user.

Each user is allocated an access level when their details are added to the system. Up to 3 levels are provided for – Operations, Maintenance and Administration.

Every form in the system has controls on it. You can specify which controls should be accessible by which level of user.

To do this, click on the Forms drop down list box and highlight the form for which access levels are to be set.

Each control that is available on the form will be listed in the Control Name list.

Select Form:

Form Controls and Group Access

Control Name	Description	Operations	Maintenance	Administrator
Devices		read-write	read-write	read-write
IllumControl		read-write	read-write	read-write
Status		read-write	read-write	read-write
AddLine	Add Line	read-write	read-write	read-write
ApplyEdit	Apply Edit	read-write	read-write	read-write
DeleteLine	Delete Line	read-write	read-write	read-write
RefreshFromSign	Refresh Values From Si...	read-write	read-write	read-write
SaveToDatabase	Save Values To Databa...	read-write	read-write	read-write

Change Group Access Level

Operations:

Maintenance:

Administration:

The Description field provides a brief description of the function of the control.

Each level can have one of three types of access allocated – read write, read only or not accessible. Read write allows the operator full access to the field or control function, read only allows limited access (can only view the field or control function) and not accessible renders that field or control completely inaccessible to that level of operator.

To edit the access levels for a particular control or field, highlight that control or field in the list and its details will be displayed in the edit fields below the data window. Select the applicable access requirement for each Level and click on the Apply button.

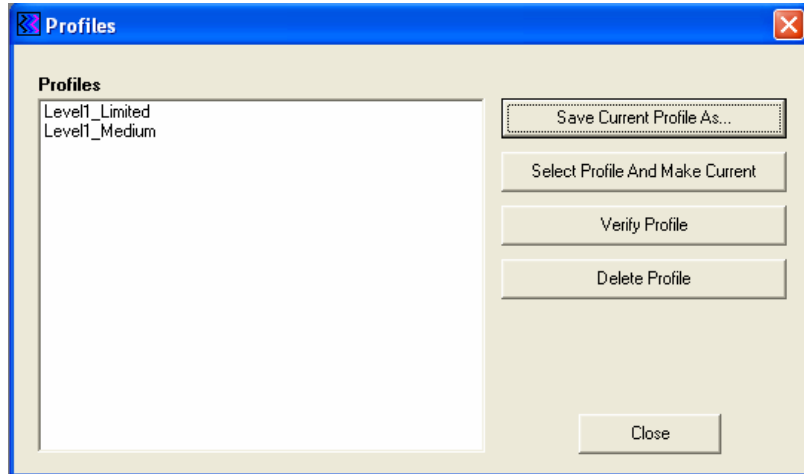
Note about Menu Items: You can set the access levels for menu items in a similar manner to setting access levels on forms. The setting of access to menu items is done by selecting MDI from the “Forms” drop down list box. The menu items will be displayed and you can set the access levels for each level of user. Note that read-write will provide full access to the menu, read only will grey the menu item so that it can be viewed but is not actionable, while not accessible will cause the menu item to ‘disappear’ completely and the operator will not even know of its existence.

Profiles

The Profile function serves two main purposes. The first is to ensure that each and every form and control in Intelligent Control is included in the database so that Access Levels can be correctly set for them. The second is to allow you to create and save different profiles. This feature would be used if you wanted to experiment with empowering users by giving them more authority. If you save the current profile before making those changes, you can easily revert to it if and when you decide that the experiment was unsuccessful. Alternatively, if you request Intelligent Devices, Inc to create a specific set of Access Levels,

that set of Access Levels can be sent to you as a Saved profile and can be applied to your database by selecting it and making it the current profile.

Save Current profile As.....



Each level of user in Intelligent Control can be assigned differing levels of access to each and every aspect of Intelligent Control, as described in the Access Level section above. This allows the look and feel and authority for each level to be customized for your installation. Once you have set the Access Levels, you can save that group of settings into a Profile for future use. To do this, click on the Save Current Profile As... button. The following window will open requesting you to enter a name for the profile:

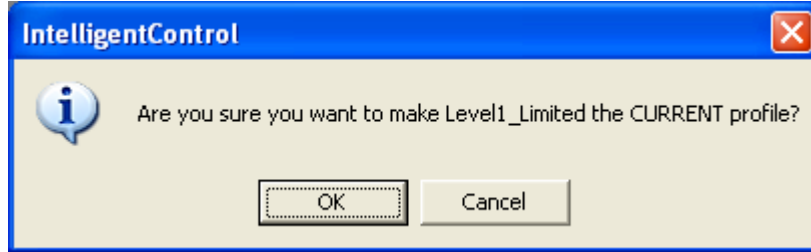


Name the profile in such a way that you can easily recognize the authority levels that it represents. Click on OK to save the Profile.

Select Profile and make Current

This function is used to change the current profile. If you have set Access Levels that are not working to your satisfaction, you can revert to a previously saved profile. This allows you to easily recover from experiments that go wrong. Also, you would use this option to install a profile that is acquired from another source, for example if you had Intelligent Devices, Inc create a customized profile for you.

To select a particular profile, highlight the name of the profile in the profiles list and click on the Select profile and Make Current button. A window will open asking you to verify that you are sure that this is the action you wish to take:



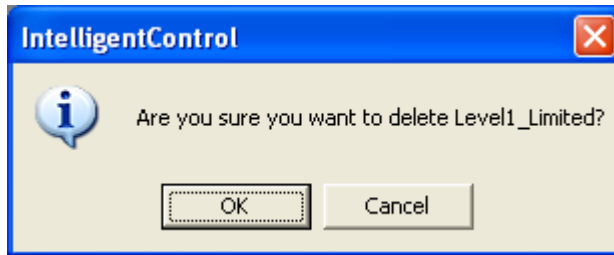
Click OK to use the selected profile.

Verify Profile

This option will scan through Intelligent Control and make sure that the Access Level form contains all the forms and controls in Intelligent Control so that the Access Level settings are correct.

Delete Profile

This option allows you to delete an unused Profile. Highlight the Profile that is no longer required and click the Delete Profile button. The following window will open asking you to verify your action:



Click OK to delete the selected Profile or Cancel to retain the Profile.

New Devices can be added, existing Device information can be edited and Devices that are no longer required can be deleted.

WINDOW

This menu option lists all the windows that are currently open. The active window is the one that has a check mark next to it.

HELP

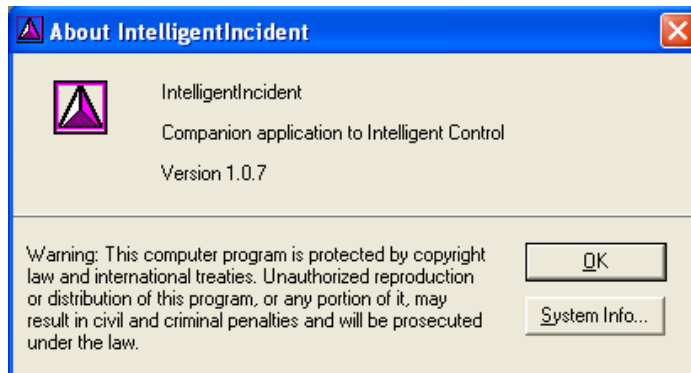
The Help menu accesses the help file and provides details about the version of Intelligent Incident that is running.

Search

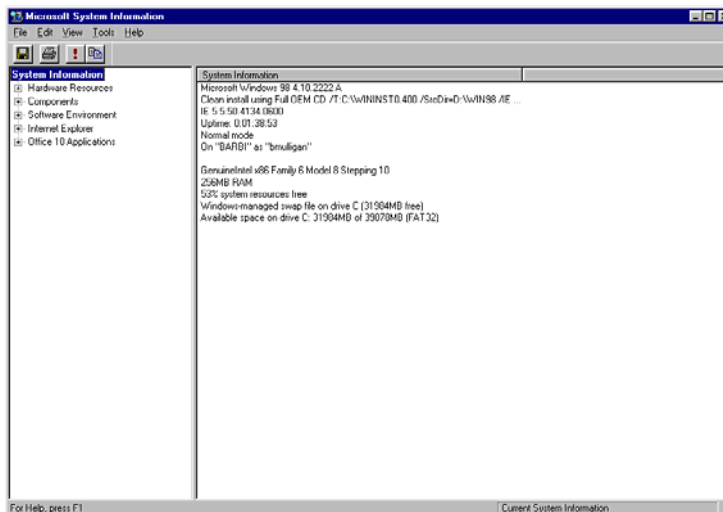
This will open the help file, enabling the utility to search for help on a specific topic.

About Intelligent Incident

Clicking on About Intelligent Incident will open the following window that will detail the current version that is installed.



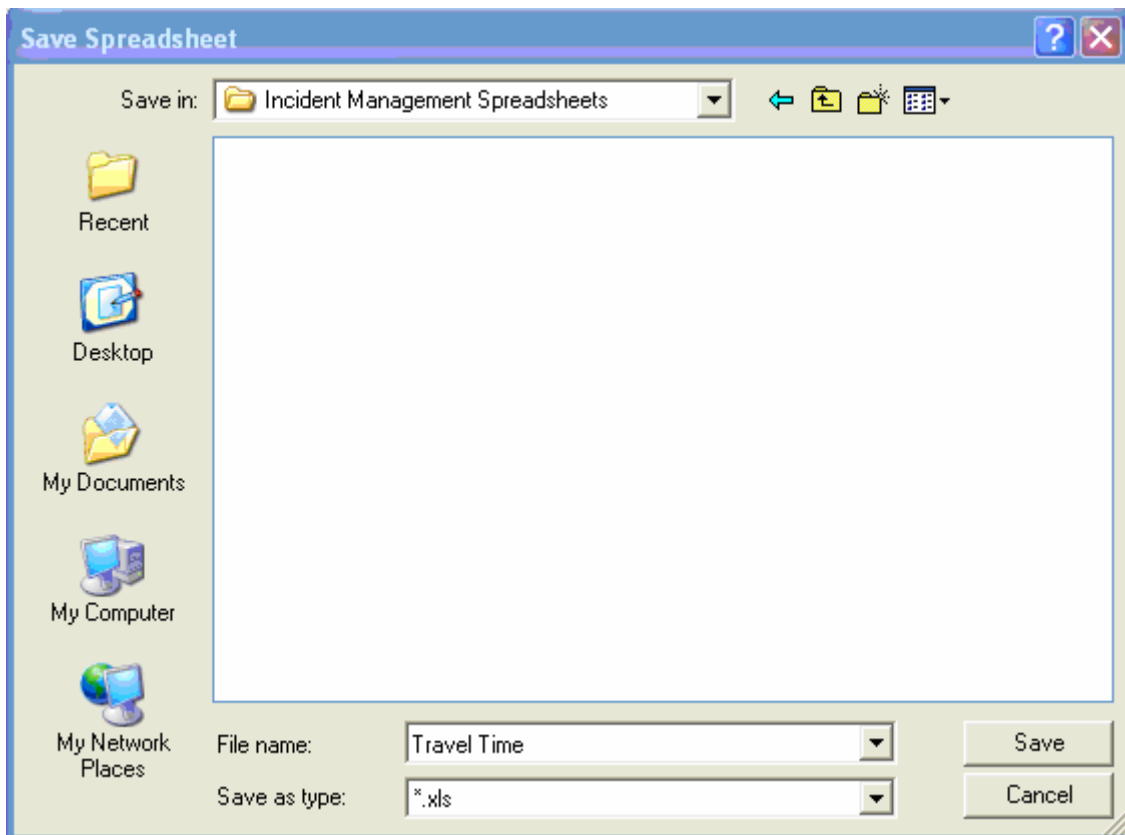
The System Info button will display the following window, providing a summary of system details. This may be required for diagnostic purposes.



HOW TO ADD A NEW INCIDENT MANAGEMENT SPREADSHEET

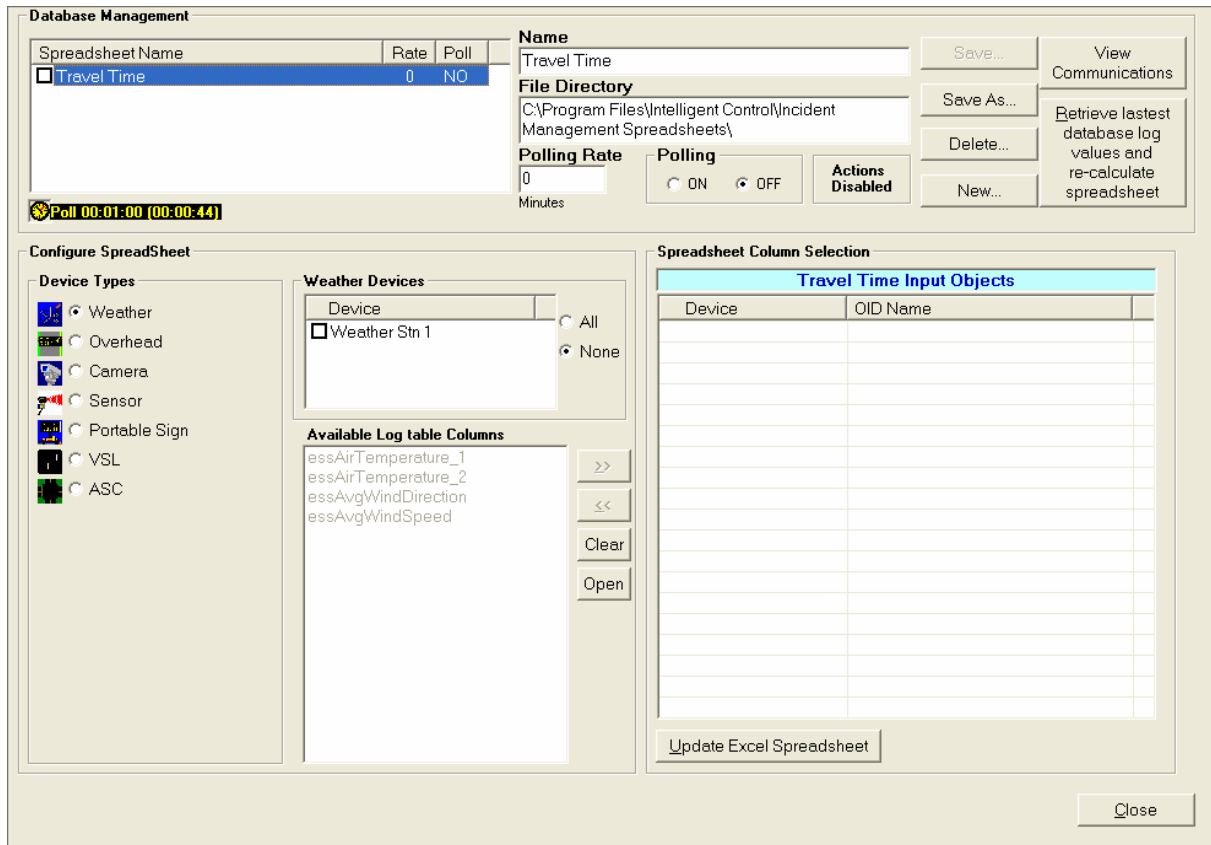
The following steps will illustrate the procedure that needs to be followed to create a new Incident Management routine. For the purposes of this example, we will step through the creation of an Incident management routine that displays travel times on signs based on the information retrieved from sensors.

1. Click on the New button. A window will open asking you to Save the spreadsheet for the Incident Management routine:

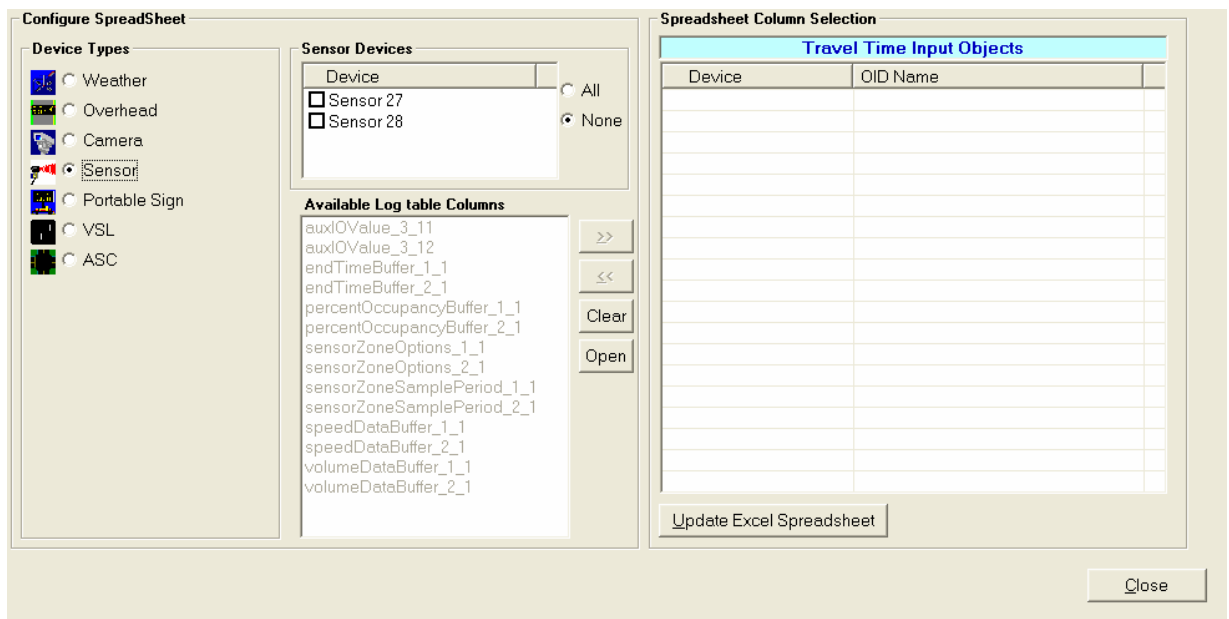


Navigate to the directory in which the spreadsheet is to be stored (in this example Incident Management Spreadsheets), enter the File name (in this case Travel Time) and then click Save.

2. The following window will open so that you can configure the spreadsheet:



Select the Device Type from the list – in this example, click on Sensor. All the Sensors that are configured in Intelligent Control will be listed:

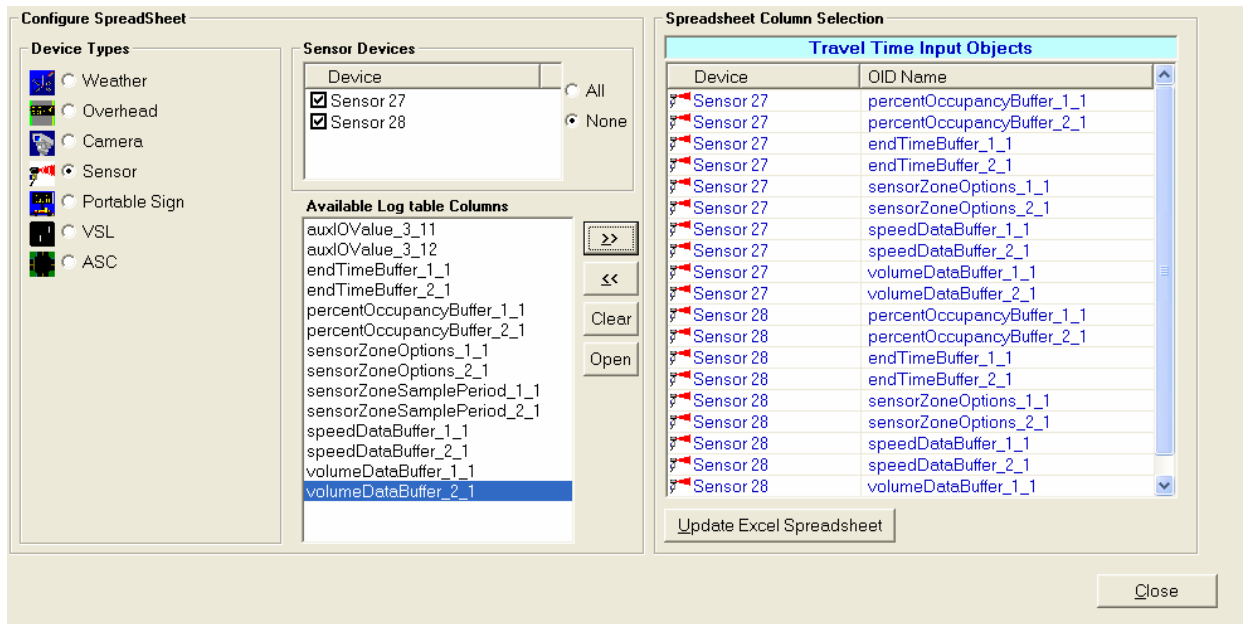


In addition, the available Log Table objects will be displayed. Note that the objects that are displayed for selection here are the only objects that can be used as data for the calculations in Incident Management.

The available Log Table Objects are those objects that are included in the Log Configuration for each Device. The Log is configured in Maps, and the maps Log determines which objects will be retrieved from a Device when it is polled.

Note that if the Device(s) that you are intending to use as the source of data for your Incident Management calculations is not one of the Devices on your Map and does not have a Log Configured, no objects will be available to you for selection when you configure the spreadsheet in Incident Management.

Click the checkboxes next to the Devices that are to be used in the Spreadsheet (in this example, Sensor 27 and Sensor 28 should be checked). Once the Devices have been checked, the list of Available Log Table Columns will be un-grayed and you will be able to select them for your spreadsheet.

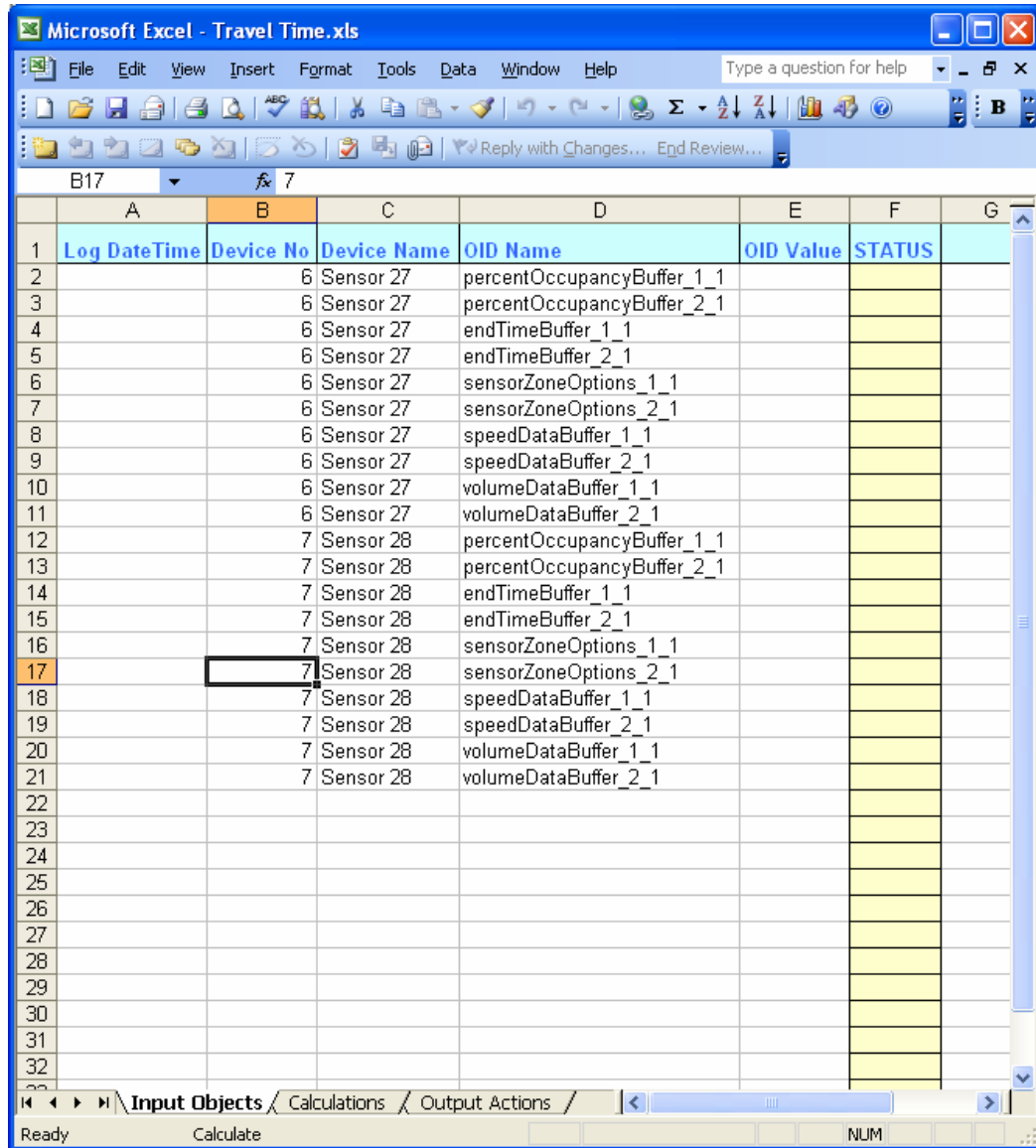


Highlight the required object and then click on the double right arrow to move the selected object for each of the selected Devices to the Spreadsheet Column Selection window. In our example, we are using all the available objects for both sensors for lane 1 and lane 2.

3. Update the spreadsheet with the Input Objects

Once you have made all the required selections, click on the Update Excel

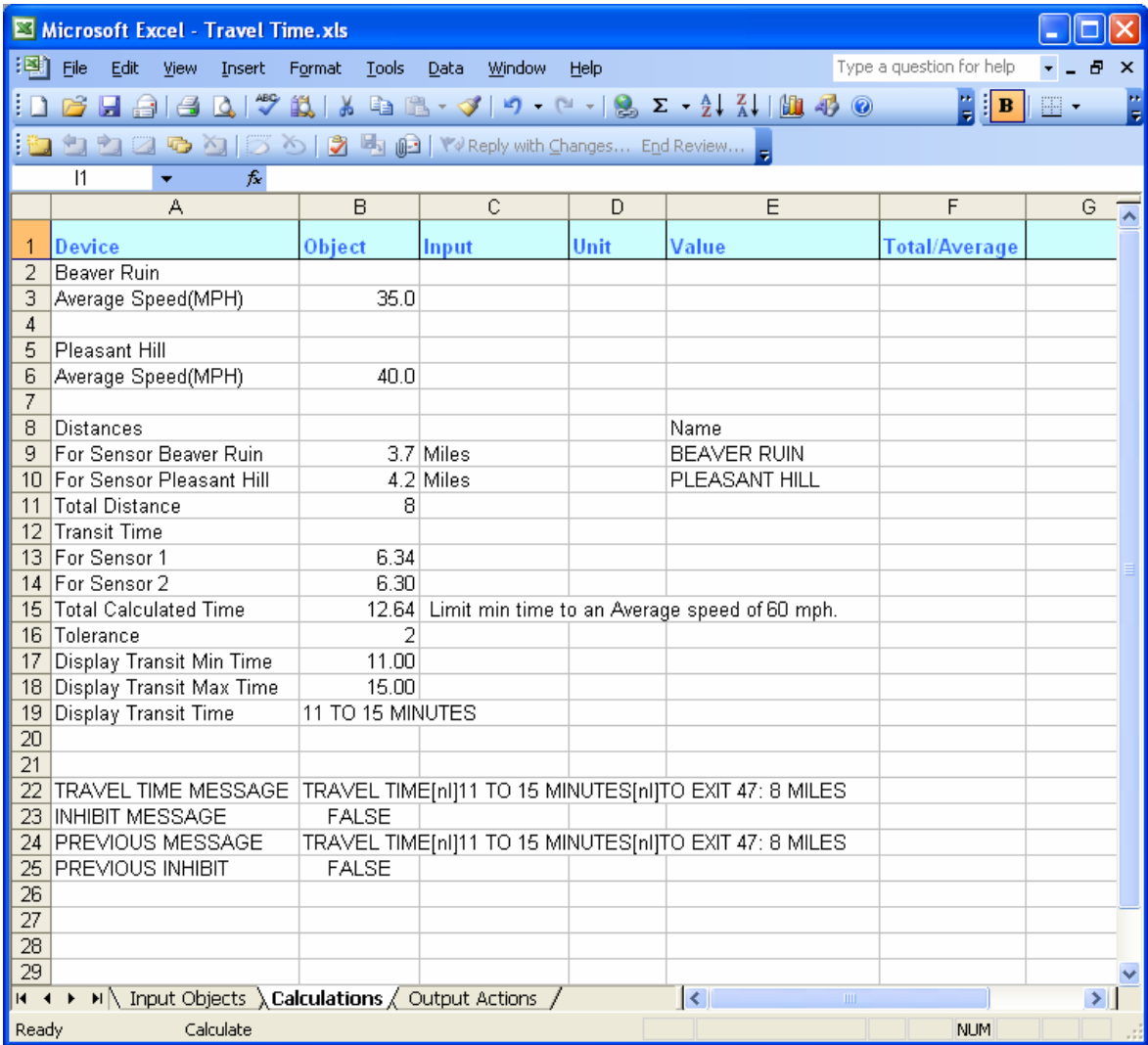
Spreadsheet button. The Input Sheet (Sheet 1) of the spreadsheet will look like this:



Note that until you retrieve the values for the spreadsheet, the Log Date Time, OID Value and Status fields will remain empty.

- 4. Now that the Input values have been determined, you will want to specify the calculations that need to take place to determine what action should be taken, if any.

To do this, click on the Calculations Sheet in the Excel Spreadsheet:



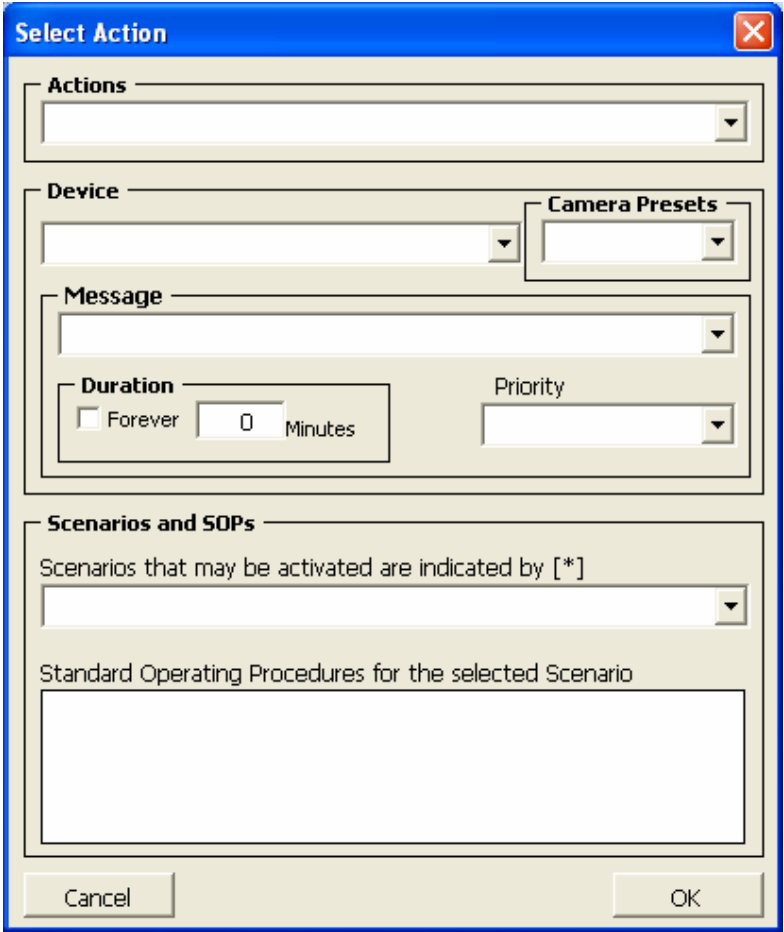
The Calculation spreadsheet will use the data that it retrieved into Sheet 1 (Input Objects) and will then perform calculations to determine what action should be taken.

In this example, the spreadsheet calculates travel time based on the speed retrieved from the sensor and the distance to be traveled. The calculations are performed using standard Excel formulas and macros. Calculations will be triggered by a change in the Input values in sheet 1 (Input Objects) when the Devices are polled. If there is no change to the input data, no calculations are performed and no output actions are triggered. If there are changes in the data retrieved, the calculation is triggered and output Actions are triggered.

When it has completed its calculations, specific cells will be marked and the program will use these cells to determine if any action is to be taken. If some action is to be taken, that action will be performed by Sheet 3 (Output Actions).

5. Specify the Action that should be taken based on the results of the calculations:

There is a range of actions that can be triggered by Incident management. To define Actions, select the 3rd Sheet (Output Actions) and double click on an empty line – preferably the first empty line, in the Action Column. The following window will open:



Select from one of the following Actions:

Activate Message

This will activate the message specified in message on the Device specified, using the Duration and Priority settings indicated here.

Download and Activate message

This will download the message generated by Sheet 2 (Calculations), on the Device specified by the Output Actions using the Duration and Priority settings specified on the Output Actions sheet.

Trigger Scenario

This will trigger the scenario selected in the Scenario and SOPs field. If there is a Standard Operating Procedure (SOP) attached to the Scenario, that SOP will also be included in the activation.

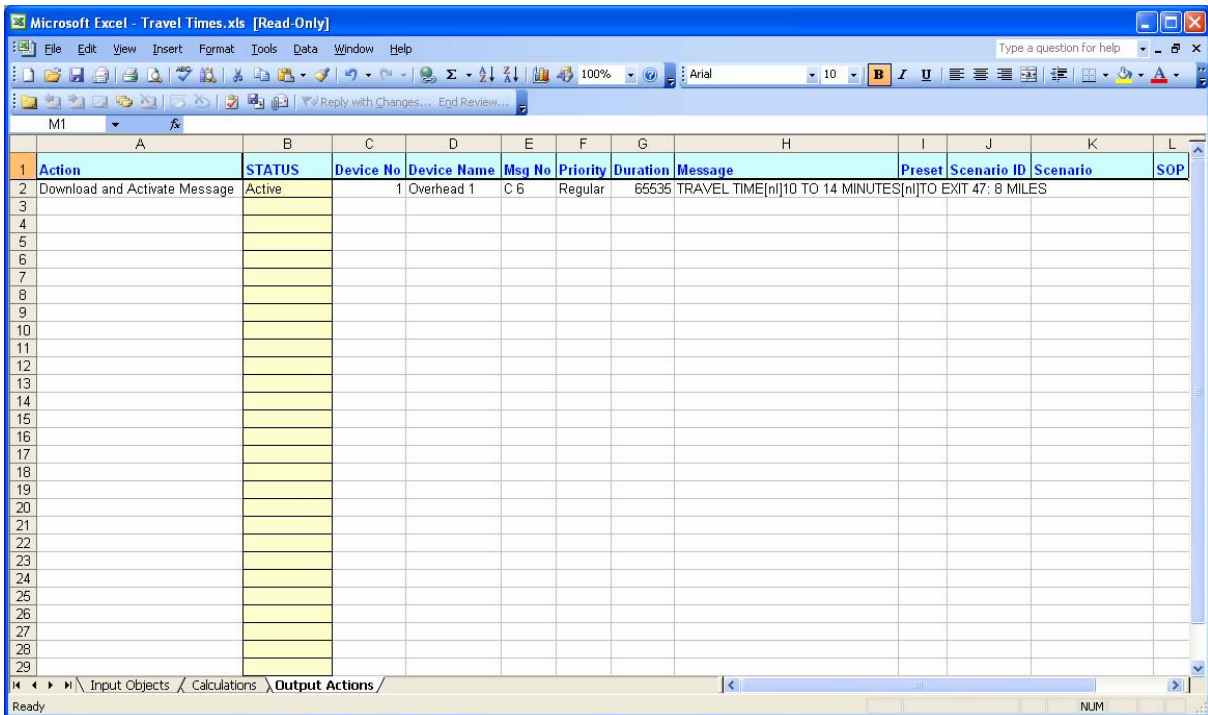
Trigger Scenario SOP

Only the selected Standard Operating procedure will be triggered and not the Scenario to which it is attached.

Trigger Camera Preset

This will trigger the camera presets indicated in the Camera Preset field.

Each row of the Output Action sheet will contain one action that is to be triggered. If you want to trigger a message that should be displayed on multiple Devices, you would create a scenario that would cater to that and then trigger that Scenario in Incident Management.



The Status cell for each action is the indicator that Incident Management uses to trigger each Action. If the status is Active, the Output Action specified in that row will be activated.

6. Save the Spreadsheet

Close Excel and Save the spreadsheet. You will be returned to the Incident Management form.

HOW TO ADD A STANDARD OPERATING PROCEDURE

Intelligent Incident can be configured so that in the event of an incident, a Standard Operating Procedure can be activated to provide instructions to the operator regarding the necessary action required for that specific incident. Smart tags can be attached to the instructions so that critical contact information need only be maintained in one location, therefore ensuring that the most up to date information is displayed.

To add a Standard Operating Procedure click new from the Manual tab in Incidents. A menu will be opened. Select New and from the menu that is then displayed, select Standard Operating Procedure. The following window will be opened:

No	Notify	Contact Name	Phone
1			
2			
3			
4			
5			
6			

Name

Enter the Name of the procedure that is to be implemented for the selected Scenario.

Description

Enter a description of the Standard Operating Procedure.

Procedure Properties

These fields indicate the details for the procedure that is selected.

Path in Scenarios

This indicates the location of the standard operating procedure.

Notify

This lists details of all the agencies and personnel that have to be notified.

Priority

Each Standard Operating Procedure that is added to the system can have priority attached to it, indicating the importance of the action that is to be taken. Check the button next to the required priority level.

Mode

Each Standard Operating Procedure is allocated a Mode that indicates the whether the Standard Operating Procedure is Advisory, Mandatory or Informative.

Notifications

This list contains details of all the people or agencies that have to be notified as part of the Standard Operating Procedure.

Access those contacts that have already been added to the system by clicking on the drop down list box on the "New Contact" field. To add a new contact, enter the Contact Title, Contact Name and Phone Number in the appropriate fields and then click on the Save Notification button. Details for that contact will be added.

To add a contact to the Notify List, highlight the Contact in the Notifications drop down list box and then click the mouse anywhere on the Notify form. The details for that contact will be displayed in the notify list. If you select and add a contact to the list in error, highlight the incorrect contact in the Notify list and press the Delete key to remove the details from the notify list.

Add as many Notifications as are required and then click on the Close button.

The Standard Operating Procedure will be displayed with the Scenario for which it was created:

The screenshot displays the Intelligent Incident software interface. On the left is a tree view under 'SCENARIOS AND AMBER ALERTS'. The 'SCENARIOS' folder is expanded to show 'Amber Alert - Radio Msgs', which includes 'Overhead 1', 'Trailer', and 'Bridge Ice Warning'. 'Bridge Ice Warning' is selected and highlighted. Below it are 'Construction Delay I-39 Northbound' and 'Nor...'. A callout box with an arrow pointing to 'Bridge Ice Warning' contains the text: 'Standard Operating Procedure included as part of Scenario'.

On the right, a table lists messages:

No	Device	Message	Status
1	Overhead 1	FREEZE WARNING ON[n]BRIDG...	Active
4	Trailer	ICE ON[n]BRIDGE[n]AHEAD[mp]...	Active
	Ice On Bridge	Standard Operating Procedure	SOP

Below the table is a 'Communications Activity Log for Bridge Ice Warning' window with columns for 'Time' and 'Action'. At the bottom of the interface are buttons for 'Verify', 'Activate', 'Clear Log', and 'Close'.

UPDATING INTELLIGENT INCIDENT

When a new version of Intelligent Incident has to be installed, there are several steps that should be taken to ensure a trouble free upgrade. In most instances, it will not be necessary for you to change your database. Special instructions will be provided should it be necessary for changes to be made to your existing database.

To install a later version of Intelligent Incident, you should do the following:

1. Exit Intelligent Incident.
2. Open Task Manager (press Alt-Ctrl and Del).

Check the Processes tab to ensure that no Intelligent Incident Processes are still running. If any of the following processes are still running (which may be the case if the computer is the Server for an Intelligent Incident system or if Intelligent Incident was not terminated correctly), you should end them by clicking on them and selecting End Task.

IntelligentIncident.exe
NTCIPDatamanager.exe
NTCIPServer.exe

3. Uninstall Intelligent Incident (using the Add/Remove Programs options from the Control panel).
4. Navigate to the directory in which Intelligent Incident is installed (typically C:\Program Files\Intelligent Incident). The only files that should remain in this directory are the Directories and any .mdb files. Delete any other files (including any .exe, .dll, .ocx, .tlb and .oca files) that are in the directory.
5. Install the new version and follow the on-screen prompts.

INDEX

About Intelligent Incident.....	40	Spreadsheet.....	41
Acceptance Required.....	27	How to Add a Standard Operating Procedure	48
Access Levels.....	36	Impact.....	12
Acknowledge.....	30	Incident Category Management	31
Administration	24	Incident Current Status.....	14
Alarm Priority.....	26, 29	Incident Event Log.....	23
Alarm Priority Response	27	Incident Location Management.....	34
Alarm Responses.....	29	Incident Management.....	19
Alarm Threshold Information.....	26	Incidents	10
Alarm Thresholds	24	Incidents Due to Expire	16
Auto Detection.....	11	Input Objects	43
AutoStart	5	Installing Intelligent INCIDENT.....	3
Available Log Table Columns	22	Large Toolbar Icons	9
Binary	28	Link Alarms.....	30
Calculations.....	44	Location Point.....	12
Category.....	11	Log Off.....	6
Change Password.....	7	Log On.....	5
Cleared.....	10	Log Trigger	27
Closed	10	Manua.....	10
Comment.....	12	Manual.....	11
Compare.....	27	Map View.....	12
Configure.....	24	Map Views	18
Configure Spreadsheet/View Communications	21	Mask Alarm	25
Confirmed.....	10	Mask All.....	26
Constant.....	28	Mask Until.....	25
Delete Profile.....	39	Mode.....	49
Description	11, 48	Name	20, 48
Device Types	22	Notifications	49
Devices.....	22	Notify	49
Directory	20	Operators	36
Display Result	29	Output Actions.....	46
Exit	9	Pan	18
Expected Duration.....	12	Path in Scenarios	49
Expired	10	Pending	10
Extended Logging	8	Polling.....	21
Filter	18	Polling Rate	20
Filter Incidents.....	16	Priority	49
First Value	28	Procedure Properties	48
Full Extent	19	Profiles.....	37
GIS MAP View of Incidents.....	17	Refresh Incidents	23
Help.....	40	Remove	14
How to Add A New Incident Management		Response By Authority Level (1-5)	29

Run.....	23	Starting Intelligent Incident.....	3
Scaling Type and Scale	28	Timeout.....	8
Scheduled	11	Tru Color	27
Search	40	Type.....	11
Second Value	28	Unconfirmed	10
Select Profile and make Current	38	Unmask All	26
Sequential	28	Update Excel Spreadsheet.....	22
Show Pogress	15	Updating Intelligent Incident.....	51
Source	11	Verify Profile	39
Spreadsheet Column Selection	22	Window.....	40
Spreadsheet Information.....	20	Zoom in.....	18
Standard Operating Procedure	12	Zoom out	18