



Alarm Gateway Appnote

Contents

| | | |
|----|---|----|
| 1 | Introduction | 3 |
| 2 | Setups..... | 4 |
| a. | Setup on the Server (Setup Tab Settings)..... | 4 |
| | Gateway Tab..... | 4 |
| | Communications Tab..... | 5 |
| b. | Licensing | 5 |
| | CAMG-1000 Alarm Gateway Server License | 5 |
| | CBAS-7100 Alarm Gateway Base Station License..... | 5 |
| c. | Login Settings..... | 6 |
| | Command Line/ Shortcut | 6 |
| | Default Login | 6 |
| 3 | GUI menus..... | 7 |
| a. | Gateway Menu | 7 |
| | Reports..... | 7 |
| | Cases..... | 9 |
| | Disabled alarms | 9 |
| | Users..... | 10 |
| | Preset comments | 12 |
| | Heartbeat monitoring | 13 |
| | Settings..... | 14 |
| 4 | Operation | 16 |
| a. | Interface..... | 16 |
| | Gateway status information ② | 16 |
| | Incoming Alarm Table ③ | 17 |
| | Current Alarm Table ④ | 17 |
| | History/Preview Table ⑤ | 18 |
| b. | Incoming Alarm Table..... | 18 |
| | Alarm Previews..... | 19 |
| | Handle Alarm..... | 20 |
| | Clear Alarms | 23 |
| | Cases..... | 23 |
| | Filters..... | 25 |
| | Show Alarm Information | 26 |
| | Disable..... | 27 |
| | Connect To Site | 27 |

c. History Table: Alarms.....27
Right Click Menu.....27
Filter29

d. History Table: Sessions, Logins, and Cases30
Sessions30
Logins.....31
Cases.....32

DRAFT

1 Introduction

This Appnote will server to explain the specific steps involved in setting up, and using, a CathexisVision Alarm Management Gateway. It is not intended to replace the full CathexisVision manual, which should be on hand, in case the user has any further questions.

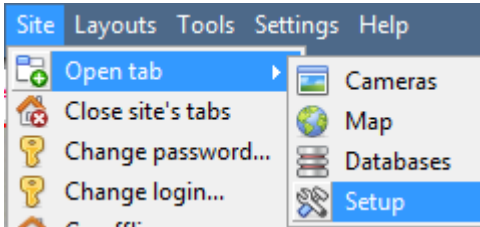
For further support contact support@cat.co.za.

DRAFT

2 Setups

a. Setup on the Server (Setup Tab Settings)

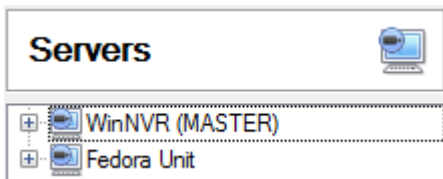
These settings take place in the Configure Servers Panel, in the Setup tab of the server unit/s which will be setup to send alarms to the Gateway unit. To open the Configure Servers setup, follow the instructions below.



After logging into your site, to open Configure Server simply click on **Site** → **Open Tab** → **Setup**. Once in the Setup Tab click on the

Configure Servers icon: 

Note: Right-Clicking on the tab of any open site will bring up the same menu as the one accessed via the method above.





You will see the servers list to the right, and the panel to the right of that will contain the options for the current selection. Left-click on the server you wish to use.

Gateway Tab

This section deals with the Alarm Gateway.

- **Send heartbeat monitoring alarms**

Send heartbeat monitoring alarms to  



If a heartbeat alarm is triggered, the gateway needs to take an action (send an alarm).



In general you would want this alarm to go to the gateway itself. So simply select the gateway from the drop down menu. If you want the heartbeat alarms to go to some other unit, then select/add that unit.

Note: If this is unchecked, these heartbeat alarms will not be sent anywhere.

- **If an alarm is not handled**

If an alarm in the gateway has not been handled in minutes then

if it is a technical alarm forward it to  

if it is an event alarm forward it to  

Move to History after forwarding

If they have not been handled for a while, you may want to send unhandled alarms to other gateways, or base stations,

Decide on the time frame, as well as where specific types of alarms are sent.

Note: If you send an alarm to another gateway, this alarm will appear in the incoming queue of both gateways. If one is handled, the other will remain in the incoming list. To avoid confusion you may want to check the Move to History after forwarding box, which will move the alarm to the history queue of the forwarding unit.

IMPORTANT: Both the **Heartbeat** and the **Heartbeat Monitor** (Dealt with below) must be enabled and configured for an alarm to be possible.

- ***Move to history***

Move gateway alarms to History if they have not been handled in minutes

The number of alarms can build up very fast, especially on large sites. If you are dealing with a site where alarms are only relevant for a short period of time you may have them automatically moved to the history queue.

Communications Tab

A Heartbeat is a signal sent from the capture unit (recording server) to an Alarm Management Gateway unit, which tells the Gateway that the server is still active. If the message fails to come through the Gateway will generate an alarm.

This will generate an alarm if the server goes down, or if the communications medium goes down.

Note: This needs to be setup on both the capture station and the Alarm Management Gateway.

- ***Enable Heartbeat***

To enable sending the heartbeat on your unit: check the Send gateway heartbeat tick box.

- ***Select a Base-Station***

The base station referred to here is the Alarm Management Gateway unit that you are going to be sending the heartbeat message to.

- ***Select an interval for your Heartbeat***

This will define how often your unit will send a Heartbeat to the Gateway.

b. Licensing

There are two relevant licenses here, one for the Alarm Gateway unit, and one for Viewing Stations that wish to view the Alarm Gateway tab, in CathexisVision.

CAMG-1000 Alarm Gateway Server License

The server license for a Gateway is the CAMG-1000.

CBAS-7100 Alarm Gateway Base Station License

This license is for Alarm Gateway viewing/basestations only.

c. Login Settings

Command Line/ Shortcut

To use the alarm gateway, you need to open a gateway tab, in your viewing client. To do this you will need to append the following text to the command line: `gw xxx.xxx.xxx.xxx`

Where `xxx.xxx.xxx.xxx` is the IP Address of the Alarm Gateway unit.

Note: This is in the client side. This may be appended to the Target line of a shortcut, if you are using Windows, or Linux.

Default Login

The default username and password for the gateway unit are:

Username: **admin**

Password: **admin**

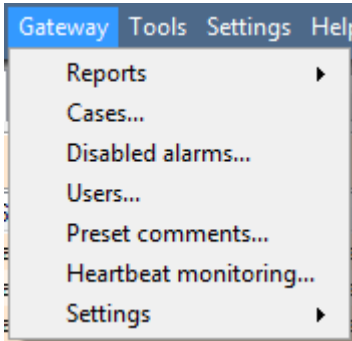
DRAFT

3 GUI menus

When you have a gateway running, you will see the Gateway Menu in the GUI. This section will take you through the different settings available in this menu.

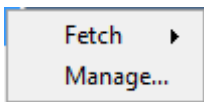
See the next section for information pertaining to the Gateway Tab, and its operation.

a. Gateway Menu



If you have configured your unit to connect to an Alarm Management Gateway, then you will see this menu in the CatVision interface

Reports

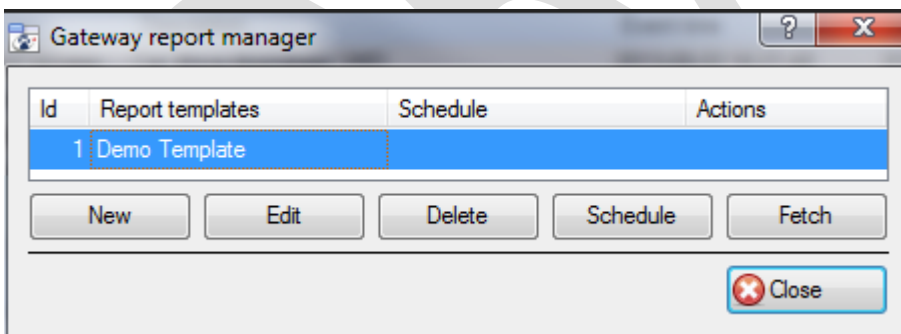


Under reports there are two options: **Fetch**, and **Manage**.

Fetch simply pulls up a pre-defined report; manage takes you to the report management window, which we will deal with in this section.

- **Manage (Gateway Report Management)**

Clicking on Manage will bring up the Gateway Report Manager window. It is here where you will create/maintain the reports.



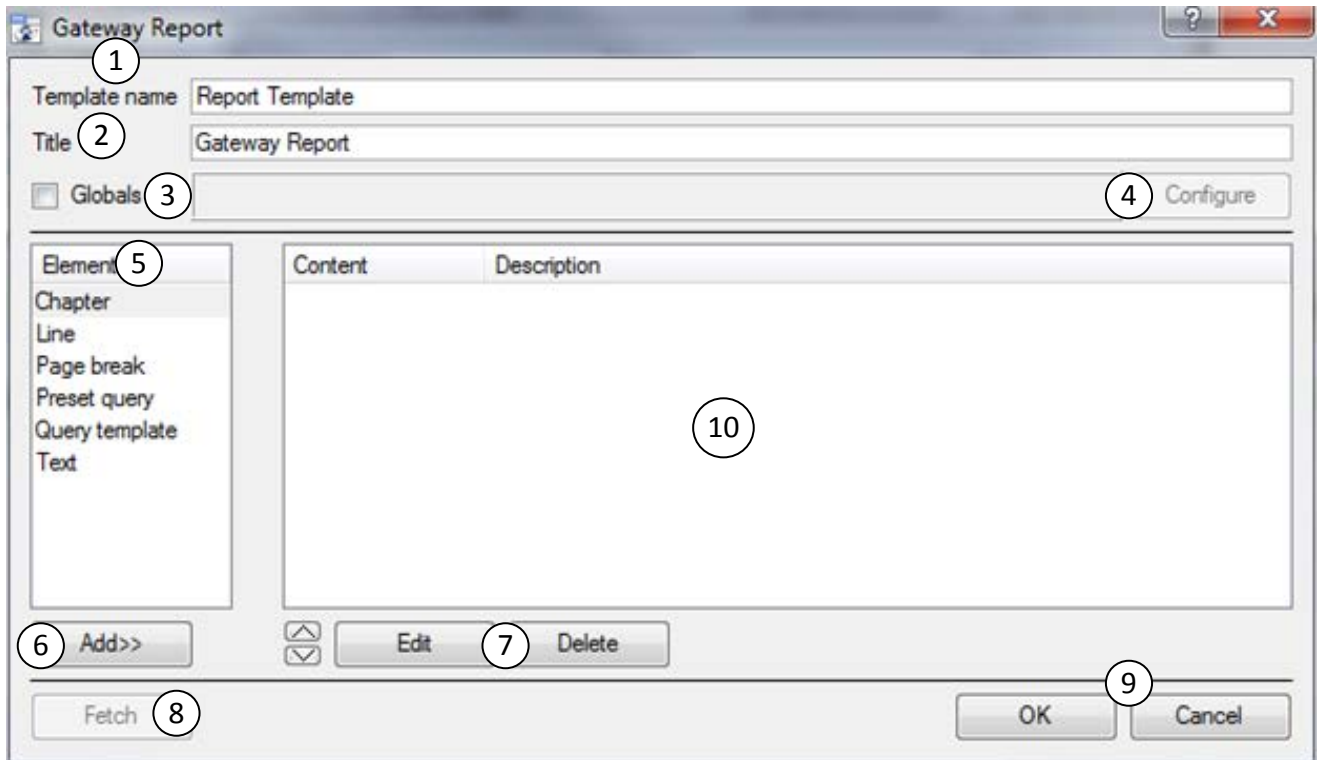
To create/edit a report click on **new/edit** respectively.

Schedule allows you to schedule reports that are fetched at time intervals, ranging from hours, to months.

Fetch will pull up the selected report.



Note: The email sending settings for the report are done in under **Site** → **Open Tab** → **Setup** → **Select the Server** → **Email Tab**.

- *Gateway Report Setup Window*

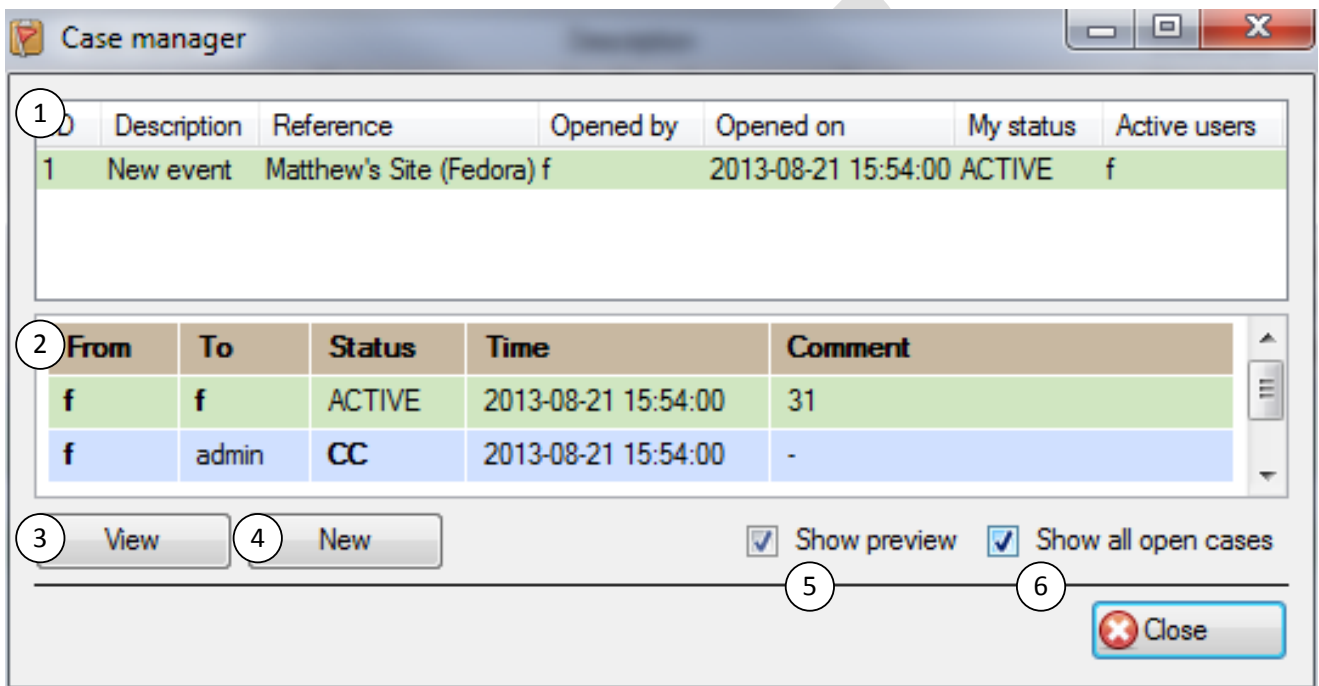


Gateway reports enable the analysis of control room operator responses, and general control room performance.

| | | |
|---|---------------|---|
| 1 | Template Name | This is the name that will appear in the <i>Fetch Reports List</i> ; not the name that will appear at the head of the fetched report. |
| 2 | Title | This is the title that will be displayed at the head of the <i>fetched report</i> . |
| 3 | Globals | There are three parameters that may be defined under Globals. These are the: <ul style="list-style-type: none"> • Time Range that you want your report to span. • The sites that you want to include in your report. • The specific units that you want to include in your report. |
| 4 | Configure | Clicking on configure will allow you to define the Globals' settings. |
| 5 | Element | The elements are the building blocks of your report. You add them in the order that you want them to appear in the report. To add an element, select it, and click on Add>> . Note: The Query Template option is there for users who want custom report setups. If you want to generate a report using information that you cannot find in the preset comments you will need to contact support@cat.co.za and request a report with the information that you require. Unless you have done this, there will be no Query Templates present. |
| 6 | Add | Selecting an element and clicking on Add will add it to the report contents window (10) |
| 7 | Edit/Delete | If you have an element selected in the report contents window you may edit/delete it by using one of these buttons. |
| 8 | Fetch | This will fetch the report that you have compiled. |

| | | |
|----|------------------------|--|
| 9 | Ok/Cancel | Ok will save the changes that you have made. Cancel will delete them. |
| 10 | Report Contents Window | This is the window in which all added elements reside. Note: the order that the elements are added here will be reflected verbatim in the output of the report. So if you want to add text as at the beginning of your report, then you should add Text First; or use the   buttons to move elements up and down the list. |

Cases



| | | |
|---|---------------------|---|
| 1 | Cases List | This will bring up a list of all cases currently open |
| 2 | Case Preview | This is a preview of the information contained in the case |
| 3 | View | Selecting a case, and clicking view will open the case |
| 4 | New | Clicking new will allow you to create a new case |
| 5 | Show Preview | Will enable/disable the case preview |
| 6 | Show all Open Cases | If you are at the admin access level, you will see an option to “ Show all open cases ”. Deselect this option to see only those cases to which you personally have been assigned. Users at all other levels will not see this option - they will see a list of only those cases to which they personally have been assigned. |

Disabled alarms

Disabled alarms

Manage disabled alarms

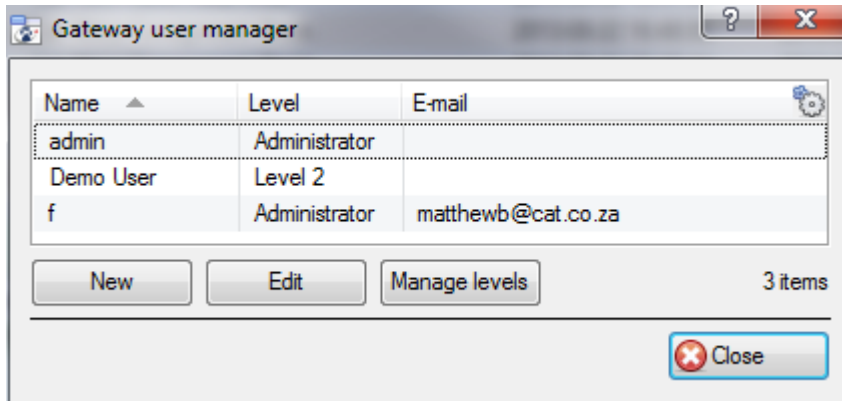
| Site name | Server name | Event | Expires | Disabled by | Time | Reason |
|-------------|---------------|----------|---------|-------------|-------|---------------------|
| catcentu... | Centurion ... | Cat T... | 1 hour | f | 20... | It is a false alarm |



This will bring up a windowed table, listing all the disabled alarms, along with relevant information.

Right click on the alarm to and click on **Clear** to **re-enable** it.

Users

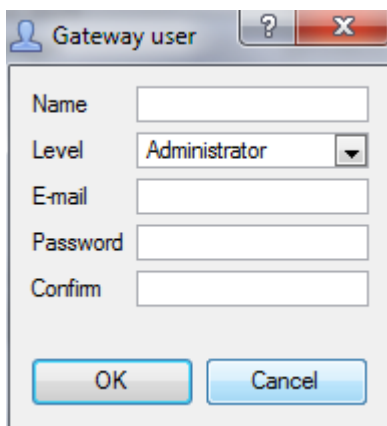


Having a gateway Login facilitates reporting relating to the gateway, escalation of alarms to defined individuals, and promotes accountability for alarm handling. It enables alarm handling to be controlled and audited against logged-in Gateway Users, rather than against server names.

The default username/password will be **admin/admin**.

Note: It is important to remember that the **gateway has its own user list, which is separate to the user list of the sites**. An operator will need login details for the Gateway, as well as login details for each site that he is handling the alarms for.

• *New/Edit User*



Enter a descriptive **name** for the user that you are creating.

Set the **level** of the user. (Gateway user levels will be dealt with below)

Set the **E-mail** address of the user.

Set, and confirm the **password** for this user.

Note: Editing a user is identical, except Password/Confirm are replaced with

Change password

• *Manage Users*

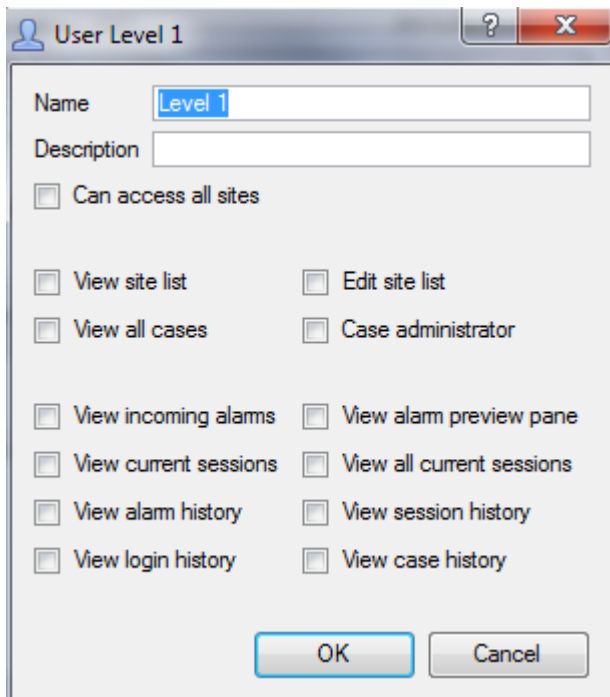
When a site sends an alarm to a Gateway, a gateway user (alarm-respondent/control-room operator) normally responds by connecting to the site and investigating the cause of the alarm.

In many CatAlarm solutions, there is advantage to allocating *particular* alarms to *particular* operators. For example:

- Junior operators should not see or be able to respond to difficult or sensitive site alarms, but senior operators should have access to all alarms.
- In large installations, the Gateway alarm queue can become exceptionally long, so an allocation of sites streamlines handling and response time. Gateway managers asked questions such as "Our alarm queue is too long for effective response; can we not have a means of splitting the alarms between our control room operators?"
- Individual operators may have privileged information on particular sites, or in some cases have a history of employment at those sites, so they are best suited to handling those sites.
- By repeatedly responding to particular sites, operators develop successful tactics and relationships with those sites, so it makes sense to allocate them. For example, managers may ask questions such as "Can we not have Bob respond to our alarms? He has been brilliant in the past, and he knows our site."

- Some sites may be sensitive in terms of security (e.g. casinos and diamond mines), requiring only particular responding operators with appropriate authorisation or security classification. The management from these sites ask questions such as “Who is this respondent?”, “How trustworthy is he/she?”

- **Manage User Levels**



In the Setup, it is possible to define “User Levels” of access to the CatAlarm interface/gateway alarm queue, from Level 1 to Level 10.

Each Level can be customised in terms of what that level of operator can see and do within the CatAlarm interface. E.g. perhaps a Level 1 user can view incoming alarms, but a Level 6 user cannot.

Note: To define the relevant access levels for each site follow this path:

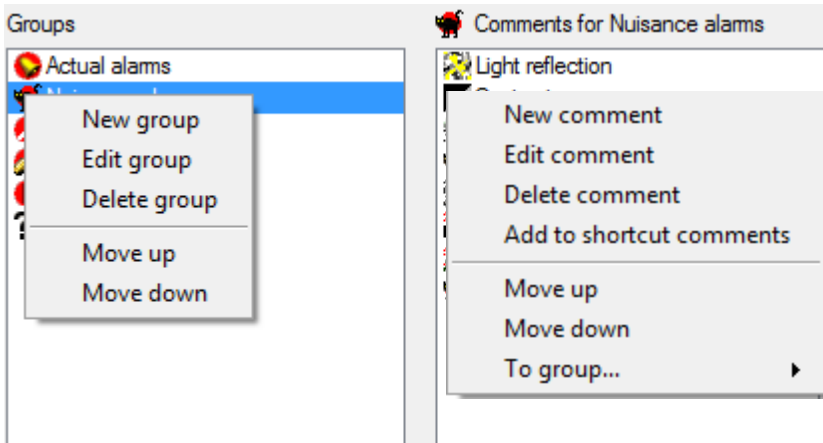
File Menu → Enterprise Manager → Right Click on the Site → Properties → Access Tab → Set the Level.

| | |
|----------------------------------|--|
| Name | This does not have to be a “Level”, and it does not need to reflect a hierarchical position. You could use Levels more as “Groups”. For example, you may opt to define certain levels geographically, with names like “Eastern region”, “Northern Europe”, or by client type, with names like “Warehousing”, “Retail”, etc. |
| Description | Optional brief description of this Level. For example: “Authorised casino operation, following successful completion of Casino Surveillance Course.” |
| Can access all sites | No restriction on sites. |
| View site list | Access to the Enterprise Manager for viewing only. |
| Edit site list | Access to the Enterprise Manager for viewing and editing. Members of this group must be competent, careful and trustworthy. |
| View all cases | Will allow users to view all cases |
| Case administrator | Case administrators are likely to be a group for management-level people with experience in this industry. |
| View incoming alarms | Can view the INCOMING table in the CatAlarm interface |
| View current sessions | Can view the CURRENT sessions table in the CatAlarm interface for his/her Login, but not all operator current sessions |
| View all current sessions | Can view the CURRENT sessions table in the CatAlarm interface for all Logins |
| View alarm history | Can view the History-Alarms table in the CatAlarm interface |

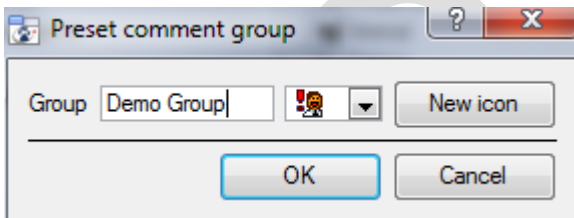
| | |
|-----------------------------|---|
| View session history | Can view the History-Sessions table in the CatAlarm interface |
| View login history | Will allow the user to view all user logins. |
| View case history | Will allow the user to view all historic cases. |

Preset comments

When handling an alarm a user is required to add a comment before it can be closed. There is a predefined list of comments available, but an administrator may define others. Comments may be grouped, selecting a group on the left will expose that groups comments on the right.



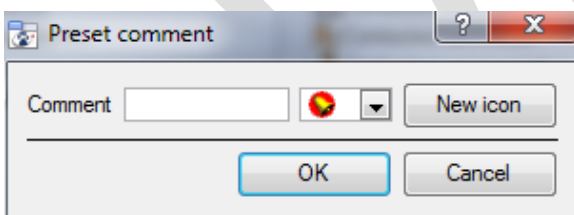
- **Add/Edit a Comment Group**



To Add/Edit a group right click anywhere on in the Group panel, and click on the relevant text.

Give the group a descriptive **name**, and either choose and icon, or add a new one.

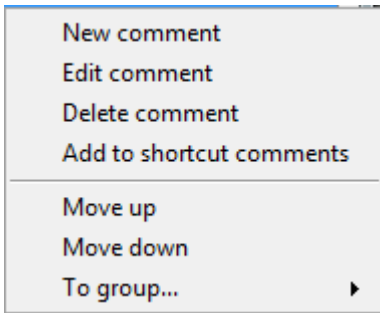
- **Add/Edit Comments**



To add/edit a comment right click anywhere in the comments panel, and click on the relevant text.

Give the comment a descriptive **name**, and either choose and icon, or add a new one.

- **Add Comments to Shortcut, and group**



Right clicking on an existing comment you will see the option to add a comment to the **Shortcut Comments**. (Shortcut comments are used when you right click on an alarm in the Incoming table, and select “Handle alarms with comment...”

You will also be able to add the comment to a comment group, simply click on **To group...** and select the group from the list that appears.

Heartbeat monitoring

Heartbeat monitoring is the way that the gateway monitors communication between the gateway and the servers that it receives alarms from. This is achieved by having the server send a digital ‘heartbeat’ to the gateway, and having the gateway monitoring the arrival of these heartbeats.

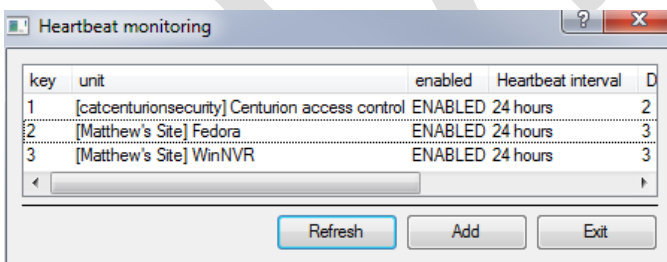
A missing heartbeat will trigger an alarm, which may be sent to the gateway, or forwarded to another gateway.

Note: There are three separate aspects to setting up heartbeat monitoring:

| Steps | Path to the Setup |
|--|---|
| 1. Setting up the recording <u>server</u> to send heartbeats. | Site Menu → Open Tab → Setup → → Left Click on the Gateway unit’s name → Communications tab |
| 2. Setting up the <u>gateway</u> to receive heartbeats. | Gateway Menu → Heartbeat monitoring ... |
| 3. Setting up the <u>gateways</u> reaction to a received heartbeat alarm. | Site Menu → Open Tab → Setup → Left Click on the Gateway unit’s name → Gateway Tab |

- **Setting up the gateway to monitor heartbeats**

To instruct the gateway to monitor heartbeats from a specific recording server, follow the **Gateway Menu → Heartbeat monitoring ...** path and follow the instructions below:



Click on Add, this will bring up a new window.

Select the relevant server/s from the drop-down menu, and click OK.

The server will now be added to the list, but there are still more settings to make.

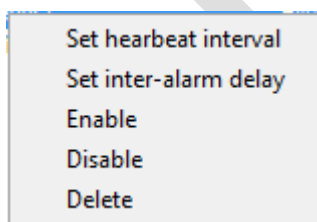
Note:

1. you will need to have already set up the server to send heartbeats to the gateway before you follow this step, as the list of available servers will not have been populated.
2. Sites will only display in the available sites from the “Add” Site option below, once they have generated at least one alarm to the alarm gateway unit. So it is advisable to start configuring the client side first, so heartbeat alarms can create an entry for the site to be selected from the heartbeat monitoring Server setup side.

Heartbeat Monitoring Column Definitions

| | |
|---------------------------|---|
| Unit | This is a list of all units that have been added to Phantom Alarm Monitoring (by means of the “Add” button) |
| Enabled | Status – ENABLED or DISABLED heartbeat monitoring (right click to specify) DISABLED will stop heartbeat monitoring, even if the unit is still sending heartbeats. |
| Heartbeat Interval | The maximum acceptable period without a heartbeat. If there is no heartbeat for this period, the Gateway will simulate a technical alarm from the dead unit. Default is 24 hours. Minimum is 10 minutes. Commonly used period is 2 hours. This period must not be less than the heartbeat period set on the capture station, or there will be false alarms. Right-click to configure this period. |
| Diff (Minutes) | The difference in expectations. “0” is good – heartbeats are normal. “-1” indicates that the Gateway has received NO heartbeat from the unit, so it cannot calculate a “difference”. A positive figure is not good. For example, “3” indicates no heartbeat for 3 hours , and generates an alarm: |
| Num Updates | This would be the number of updates it received from the remote Site. The remote site needs to send enough alarms or more than the receiving side. So the remote site could be configured to send a heartbeat alarm every 15 minutes, and the monitoring side’s interval would be configured at 30 minutes. So it gets at least 1 alarm in that period. |
| Inter-Alarm Delay | This the time between alarming to the alarm gateway that a unit has not communicated back. So if a unit fails to send alarm monitoring updates, it will generate an alarm for that unit, and it will wait the “Inter-Alarm Delay” specified to send another alarm. |

- **Right Click on a Server in the Heartbeat Monitoring list**

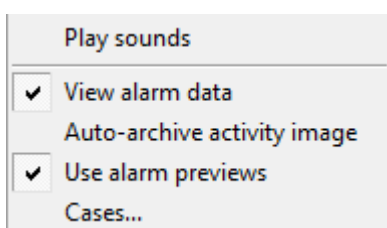


The **heartbeat interval** is the time period between which the gateway looks for new heartbeats. (Make this half the time of the periods between heartbeat transmissions from the recording server, to ensure reception.)

Inter-alarm delay is the frequency of alarms the gateway will generate if it fails to receive a heartbeat from a server.

Note: make sure to enable the server in the list after you have added it, as it is not automatically enabled.

Settings



- ***Play sounds***

There are three alarm level priorities (the priority of the event is defined in the General tab, of the Event Setup). Each event has a distinctive alarm sound, which will play a distinctive sound as the alarm comes in.

To enable these audio notifications, click on **Play sounds**.

- ***View alarm data***

This will show you the video data that is attached to the alarm when you handle it.

If you do not wish to see this video, un-tick the View alarm data option.

- ***Auto-archive activity image***

Some alarms will have an image capture sent with them that indicates where in the video image the initial trigger occurred. If you check *Auto-archive activity image* this image will be automatically archived with the alarm, after it has been handled

- ***Use alarm previews***

In the Event setup you may specify what, if any, previews are attached to the event alarm. In this menu setting you may choose whether or not to view these previews.

- ***Cases***

Here you define the maximum size of the individual files that may be attached to a case.

4 Operation

After introducing the interface of the Gateway Tab, this section will take you through its operation.

a. Interface

This section will provide a quick introduction to the interface of the Alarms tab.

The screenshot shows the Alarm Management interface with the following sections:

- 1**: Alarm Management Tab
- 2**: Gateway status information (cases, counters, connection health)
- 3**: INCOMING section with a table of incoming alarms.
- 4**: CURRENT section with a table of current alarms.
- 5**: HISTORY - Alarms section with a table of historical alarms.

| Site name | Description | Event time | Arrival time | Cases | ID |
|--|---------------------------|---------------------|---------------------|-------|--------|
| catcenturionsecurity (Centurion access ... | Cat Tech Admin Area VMD | 2013-09-06 12:23:14 | 2013-09-06 11:56:56 | | A56913 |
| catcenturionsecurity (Centurion access ... | Cat Tech assembly 2 VMD | 2013-09-06 12:23:15 | 2013-09-06 11:56:58 | | A56914 |
| catcenturionsecurity (Centurion access ... | Cat Africa downstairs VMD | 2013-09-06 12:23:37 | 2013-09-06 11:57:20 | | A56915 |
| catcenturionsecurity (Centurion access ... | Cat Tech Admin Area VMD | 2013-09-06 12:23:40 | 2013-09-06 11:57:23 | | A56916 |
| catcenturionsecurity (Centurion access ... | Cat Tech Admin Area VMD | 2013-09-06 12:24:13 | 2013-09-06 11:57:56 | | A56917 |
| catcenturionsecurity (Centurion access ... | Cat Tech assembly 2 VMD | 2013-09-06 12:24:20 | 2013-09-06 11:58:03 | | A56918 |
| catcenturionsecurity (Centurion access ... | Cat Africa downstairs VMD | 2013-09-06 12:25:23 | 2013-09-06 11:59:06 | | A56919 |
| catcenturionsecurity (Centurion access ... | Cat Tech Admin Area VMD | 2013-09-06 12:25:29 | 2013-09-06 11:59:13 | | A56920 |
| catcenturionsecurity (Centurion access ... | Cat Tech assembly 2 VMD | 2013-09-06 12:25:43 | 2013-09-06 11:59:27 | | A56921 |

| Site name | Operator | Description | Event time | Arrival time | Recordings | Comments | ID |
|----------------------|----------------|-------------------------|---------------------|----------------------------|------------|----------|--------|
| catcenturionsecurity | f (MATTHEW-PC) | Cat Africa upstairs VMD | 2013-09-06 12:22:23 | 2013-09-06 11:56:06.911554 | | | S10005 |
| Matthew's Site | f (MATTHEW-PC) | Cat Africa upstairs VMD | 2013-09-06 12:22:23 | 2013-09-06 11:56:06.911554 | | | S10004 |

| Site name | Description | Handled by | Arrival time | Comments | Recordings | Cases | ID |
|--|-------------------------|------------|----------------------------|----------|------------|-------|--------|
| catcenturionsecurity (Centurion access ... | Cat Tech Admin Area VMD | -- AUTO -- | 2013-09-06 11:42:09.267361 | | | | A56879 |
| catcenturionsecurity (Centurion access ... | Cat Tech Admin Area VMD | -- AUTO -- | 2013-09-06 11:41:42.153504 | | | | A56878 |
| catcenturionsecurity (Centurion access ... | Cat Tech Admin Area VMD | -- AUTO -- | 2013-09-06 11:41:02.938363 | | | | A56877 |
| catcenturionsecurity (Centurion access ... | Cat Tech Admin Area VMD | -- AUTO -- | 2013-09-06 11:40:29.657492 | | | | A56876 |
| catcenturionsecurity (Centurion access ... | Cat Tech assembly 2 VMD | -- AUTO -- | 2013-09-06 11:39:00.115294 | | | | A56875 |
| catcenturionsecurity (Centurion access ... | Cat Tech Admin Area VMD | -- AUTO -- | 2013-09-06 11:38:48.927379 | | | | A56874 |

Alarms are managed via the Alarm Management Tab (1) which consists of three sections. These sections are Incoming (3), Current (4), and History sections (5).

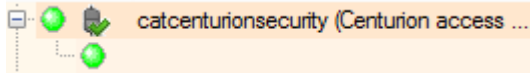
Gateway status information (2)

This displays information relevant to the gateway, and to the currently logged in user.

| | |
|--|---|
| | Indicates that there are cases open in the user's name. |
| | These counters indicate how many unhandled alarms there are. Green, Yellow, and Red counters represent Low Medium, and High priority alarms respectively. |
| | This sign indicates the health of the connection to the gateway. If the connection is lost, this will turn red. |
| | This indicates that there are currently disabled alarms. To view a list of disabled alarms follow Gateway Menu → Disabled Alarms . |

Incoming Alarm Table ³

The incoming section is where the new, unhandled, alarms that arrive from the monitored sites go. They will remain in the incoming table until they are handled by an operator (unless the gateway has been setup to automatically move alarms to the history table after a period)¹.



When a new alarm arrives from a site it creates an event folder, called a session, (🟢). The connection to the alarming site remains open for 5 minutes after an alarm arrives. The 🟢 icon indicates that the connection is still open.

Note: Multiple new alarms may arrive from the site while this connection remains open. If these new arrivals are the same as the alarm that opened the session, they will be grouped under this session. Otherwise they will start new folders.

The alarms are given a **priority** based on the priority given to the event, in the event setup. The priority of a session folder will be determined by the highest priority alarm in that folder.

- Low priority
- Medium priority
- High priority

• *Columns in the Incoming Table*

| Column Title | Description |
|--------------|---|
| Site Name | Name of the connecting site. Each site name in this list represents a session (an uninterrupted connection). |
| Description | Name of the alarm, as created in the remote capture station's Event setup. |
| Event Time | Remote time that the alarm occurred at the site. |
| Arrival Time | Local time that the alarm arrived here at the base station. |
| Cases | Cases associated with the alarm. |
| ID | An ID number assigned to cases. You can also see this number if you mouse-over the case icons in the history panel. |

Current Alarm Table ⁴

This lists sessions currently being handled by operators.





Opening a new connection will create a new node (🟢). But, if an operator has a connection to a site already open, and a new alarm is handled from the same site, it will be added to the queue of the currently open node.

Manually logged in sessions will be reflected in the audit trail.

Note: The operator has a means of filtering the current list by selecting either **My base station** or **All base stations**. **My base station** will display only the operator's own accepted alarms; **All base stations** displays accepted alarms from all base station operators.


¹ This is done via **Site Menu** → **Open Tab** → **Setup** → **Left Click on the Gateway unit's name** → **Gateway**

- *Columns in the Current Table*

| Column Title | Description |
|---------------------|--|
| Site Name | Name of the connecting site. |
| Operator | The login name of the operator who has accepted this alarm. |
| Description | Name of the alarm, as created in the remote capture station's Event setup. |
| Event Time | Remote time that the alarm occurred at the site. |
| Arrival Time | Local time that the alarm arrived here at the base station. |
| Recordings | <p>If there are recordings associated with CURRENT alarms, their icons display in this column. Double-click a recording to replay it. Types of recordings:</p> <ul style="list-style-type: none">  Activity detection image  Camera recording  Audio <p>Double-click the  icon to display a pop-up with the Alarm Preview images.</p> |
| Comments | These are comments that have been added while the operator deals with the alarm. More comments may be added before closing this alarm. Double-click to display comment descriptions. |
| ID | An ID number assigned to cases. You can also see this number if you mouse-over the case icons in the HISTORY panel. |

History/Preview Table ⁵

The history/preview table may be toggled as a history of handled alarms; or a preview of the currently selected alarm. (Alarm previews have to be defined in the event setup.)

You may filter  the contents of the history table, to increase the relevance of the listed results.

The history table may be configured to display a history of:  Alarms,  Sessions,  Logins,  Cases.

Full details on the operation of the History Table will be found under [History Table: Alarms](#), below

Note: The operators, as primary responders are concerned mainly with the Incoming and Current Tables, supervisors and managers are likely to be concerned with the History Table, and its various options.

b. Incoming Alarm Table

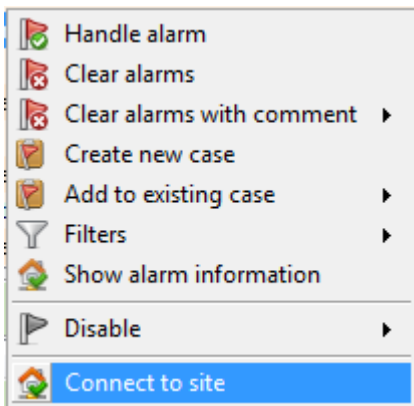
To handle an alarm the operator must double click on it. He/she may either open an entire folder of alarms (a session), or an individual alarm, by expanding the session and selecting it. This drops the alarm down into the Current Table.

Note: if the operator already has a session open, and newly handled alarms, from that site, will be added to the currently opened session in the Current Table.

This section will deal with the eventualities and procedures required of an operator when handling an alarm.

- **Incoming Alarm Options**

You may see a full list of available responses to incoming alarms by right clicking on a particular alarm. Below is a short table introducing the available responses, which will be dealt with in detail below:



Handle Alarm will open the site from which the alarm came, allowing the user to interact with that site, and review footage related to the alarm.

Clear Alarms this allows the operator to clear alarms that he has decided are redundant for whatever reason. He will have to add a comment to justify this. Clear Alarms with comment will provide a quick list of commonly used comments.

Cases are used when an alarm needs either further investigation, or needs to be elevated to a superior, or expert.

Filters allow you to filter alarms based on either the originating server, or site.

Show Alarm Information gives you a full breakdown of all information related to this alarm.

Disable allows the operator to temporarily disable nuisance alarms, based on alarm, server, or site.

Connect to Site will connect to, and open, the originating site.

Alarm Previews

The alarm preview will display a sequence of looping images from cameras related to the alarm in the event setup.

Alarm previews allow the operator to cycle quickly through alarms, and decide based on a few preview images whether it is worth opening up the alarm, or if he/she should simply clear it.

Note: While this section is physically in the History table, it is most often related to the handling of incoming alarms. Therefore this is the logical placing for this section.

- **Alarm previews, and the Incoming Table**

The primary purpose of Alarm Previews is to provide a means for base station operators to preview a sequence of images of a selected *Incoming* alarm.

When previewed from the Incoming table, the Preview is displayed within the History/Previews table of the interface.

By previewing the alarm, operators have some idea on *whether* to handle, and *how* to handle the alarm.

For example, it may be immediately evident from the preview that this is a false alarm, prompting an operator to disregard the alarm.



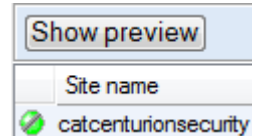
Each Alarm Preview is a short clip of Pre + Post event images.

By default, the images will loop repeatedly, but the display has a basic set of replay buttons →



- **To preview an incoming alarm**



Alarm previews are displayed in place of the history table. The Show History/Preview button is found at the top left hand corner of the History Table.



Click this button to toggle Alarm Previews on/off.

Once previews are enabled, you may left click on any of the alarms in the Incoming Table. If the alarm has a preview attached to it the sequence of images will begin cycling.

- **Preview alarms from History, and Current, tables**

You may preview an alarm from the Current, or History tables, if see the preview icon  in the Recordings column. Simply double-click on the , and the preview will appear in a floating window.

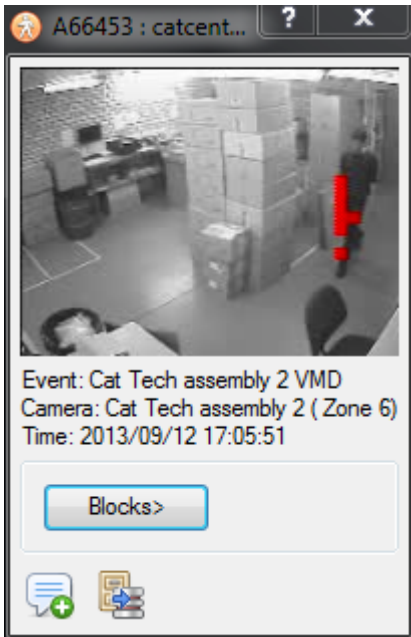
Handle Alarm

When you click on **Handle Alarm** it will immediately switch you to the Cameras Tab of the originating site. If you are not already connected to the site you will have to log in.

The following features will be visible in the interface. They are there to aid you in your response, and will be dealt with in detail, below the table:

| | |
|---|--|
| Activity Detection Event Item Window | This is a floating replay window. It will show a snapshot of the image, highlighting the areas in the image which initially triggered the alarm. |
| Image Sequence Event Action Window | This is a floating replay window that will allow you to replay the event. You may view it in sequential frames, or as a single image window. |
| Alarm Procedures | This panel displays for the Cameras / resources desktop. |
| Live cameras | The camera related to the alarm will be displayed in the Cameras Tab. |

- **Activity Detection Window**



In this window you will see a snapshot of what the motion detection algorithm saw. Highlighted in red will be the cells that triggered the event.

Below the image you will see information about the **event name**, **camera name**, and the **time** that the even occurred.

You may add comments to the alarm here.

You may also archive the recordings to your workstation from here.

will hide/display the red VMD blocks that initially triggered the alarm.

- **Image Sequence Event Action Window**



This window is designed to allow you to quickly playback the event that triggered the alarm which you are responding to. You may display the window as a series of sequential frames , or as a single video window .

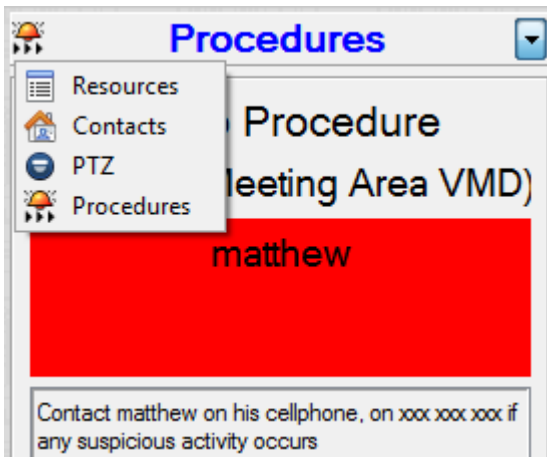
Note: After setting a window option, the next time you handle an alarm it will remain on the setting you chose.

You may add comments to the alarm here.

You may also archive the recordings to your workstation from here.

- **Alarm Procedures Panel**

The alarm procedures are meant to give the operator a quick reference as to how to respond to a specific event. Procedures are created, and associated with alarms under **Site** → **Setup** → **Procedures**.



If there are any procedures associated with this alarm they will show up in the **Procedures Panel** to the right of the live cameras.

This panel can also be used to view the Site's **Contacts** if you need to contact someone who is not listed in the Procedure.

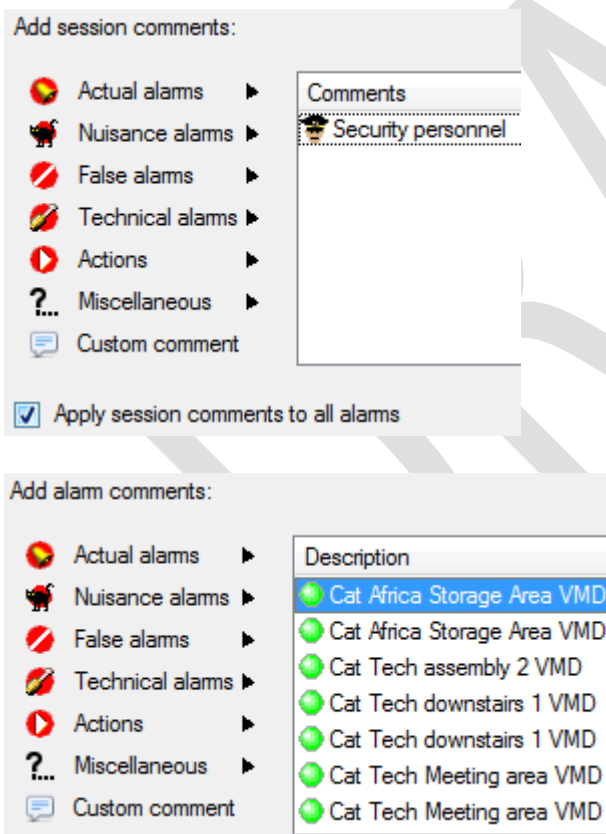
You may view the sites **resources** if there are other cameras, or resources that you need to view to handle this alarm.

You may also use this panel to control a **PTZ** camera, if you require

- *Live cameras*

The interface will also switch to the live view of the camera associated with the event alarm.

- *Close the Connection to the Site, and add comments*



Once the operator has finished dealing with the alarm they should close the connection to the site. This is because they will be required to add a comment to the alarm, once the connection is closed.

With **Apply session comments to all alarms** checked this comment will apply to all alarms handled in that session.

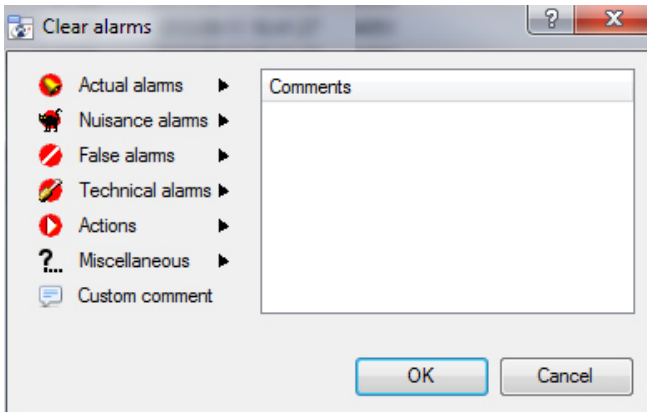
Note: if **Apply session comments to all alarms** is checked, the comment added here will be added to all alarms contained in the session.

If it is unchecked the user will have to select alarms, and add comments to them individually.

This is an important reason to close your connection to a site, when you are finished responding to an alarm.

Once you have added this comment the alarm session will be considered 'handled', and will be transferred from the Current Table, to the History Table.

Clear Alarms



In order to clear an alarm, the operator will need to provide comment about the alarm.

There are a number of preset alarms available, and there is the option to provide a custom text comment with the alarm too.

The process of defining your own comments is dealt with [above](#), under 2. Preset Comments.

Note: you may select multiple alarms at a time.

Cases


Cases offer a means of escalating an alarm to the relevant people. There are a number of other benefits of using cases:

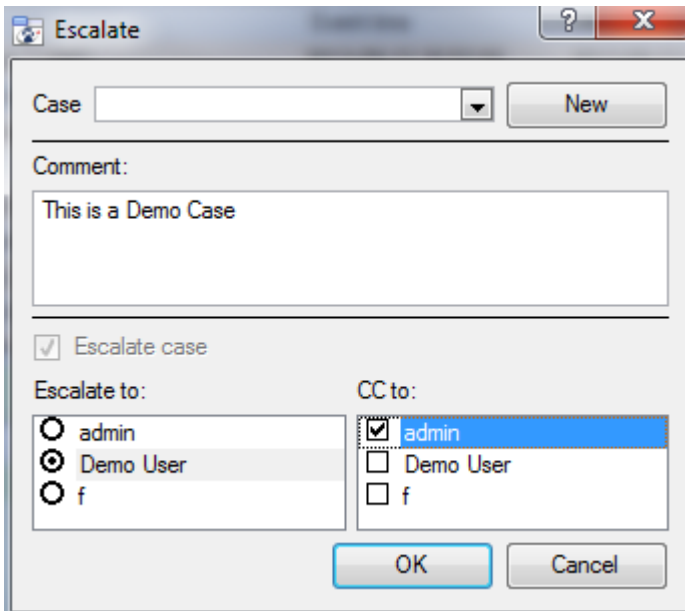
1. They safeguard against important alarms being left unhandled, or overlooked.
2. They provide the ability to audit the handling of the alarm.
3. Provide a collation point for all relevant information relating to the alarm.
4. Add the ability to add extra files, and people to the handling of an alarm.

This is especially useful in large scale operations, such as mining, airports, and casinos. In these situations you are likely to have multiple tiers of security clearance, and many alarms to deal with. An example setup would be on where certain operators are only responsible for flagging suspicious alarms. The operator level above them will be responsible for assessing the validity of the problem, and taking action on that.

• *Creating/Editing a Case*

To add an alarm to a case you right click on the alarm, or session, and select Create new case, or Add to existing case if it is related to an already existing case.

Note: If the currently logged in user has any cases in his/her name a  will appear in the notification bar, to the left of the alarm counters. The icon will flash when a new case arrives.



The 'Escalate' dialog box contains the following elements:


- Case:** A dropdown menu and a 'New' button.
- Comment:** A text area containing 'This is a Demo Case'.
- Escalate case:** A checked checkbox.
- Escalate to:** Radio buttons for 'admin', 'Demo User', and 'f'. 'Demo User' is selected.
- CC to:** Checkboxes for 'admin', 'Demo User', and 'f'. 'admin' is checked.
- Buttons:** 'OK' and 'Cancel'.

You will need to specify which **case** you want to add this alarm to. If it is a new case, click on New, and fill in the relevant details.

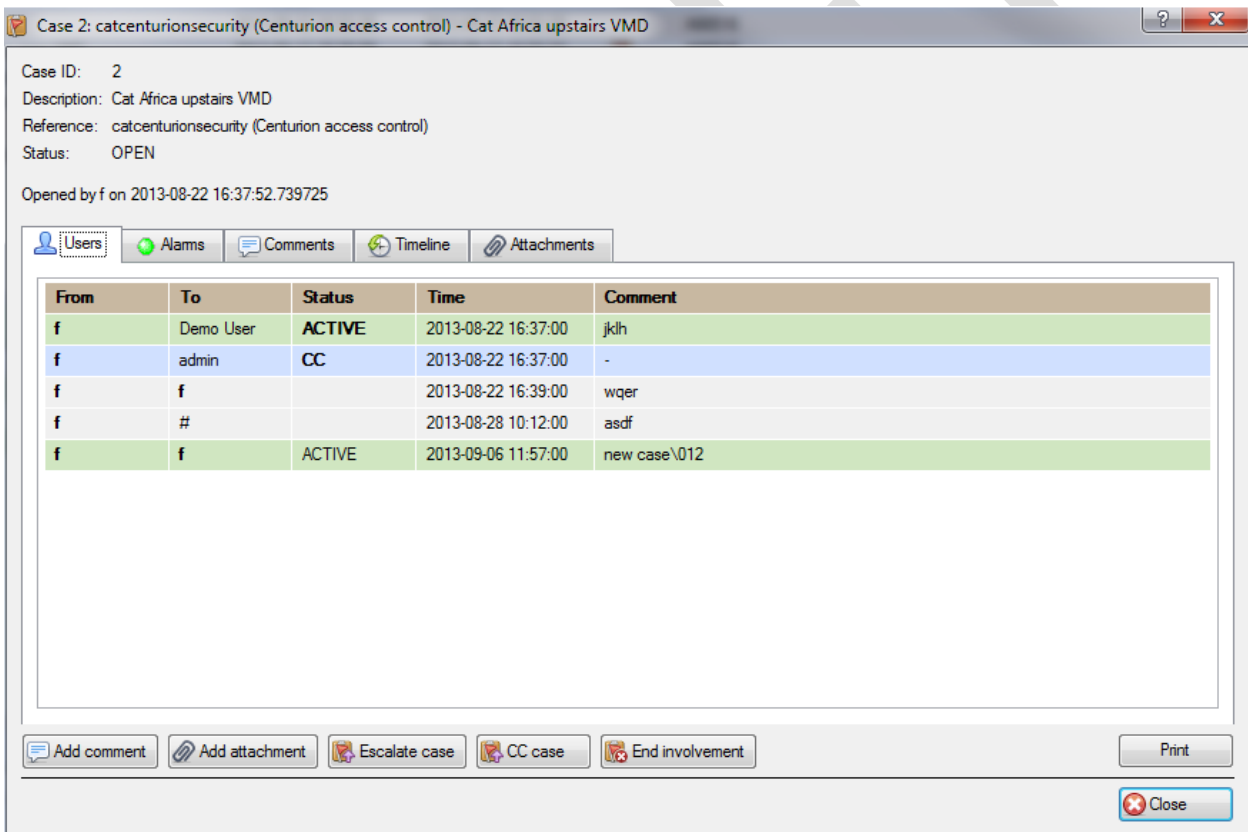
Add a **comment** to the case, as a quick reference as to why you feel this alarm/session needs to be added to a case.

If you are creating a new case you will have to Escalate it, so **Escalate case** will be greyed out.

Select the Users who you want to escalate this case to, and **CC** in whoever you also want to be informed about this case.

Click OK, an  icon will appear in the Cases column.

• *Case Interface*



Case ID: 2
 Description: Cat Africa upstairs VMD
 Reference: catcenturionsecurity (Centurion access control)
 Status: OPEN
 Opened by f on 2013-08-22 16:37:52.739725

Users | Alarms | Comments | Timeline | Attachments

| From | To | Status | Time | Comment |
|------|-----------|--------|---------------------|--------------|
| f | Demo User | ACTIVE | 2013-08-22 16:37:00 | jkjh |
| f | admin | CC | 2013-08-22 16:37:00 | - |
| f | f | | 2013-08-22 16:39:00 | wqer |
| f | # | | 2013-08-28 10:12:00 | asdf |
| f | f | ACTIVE | 2013-09-06 11:57:00 | new case\012 |

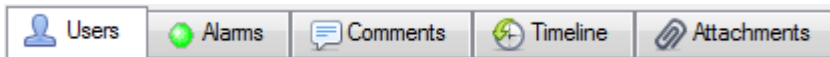
Add comment | Add attachment | Escalate case | CC case | End involvement | Print | Close

Case ID: 2
 Description: Cat Africa upstairs VMD
 Reference: catcenturionsecurity (Centurion access control)
 Status: OPEN
 Opened by f on 2013-08-22 16:37:52.739725

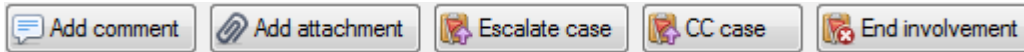
Each new case is given its own **Case ID** number. The **description** and **reference** fields are filled in by the Operator who created the case.

Status will indicate whether the case is still open, or not.

The last line gives the info about the case's opening.

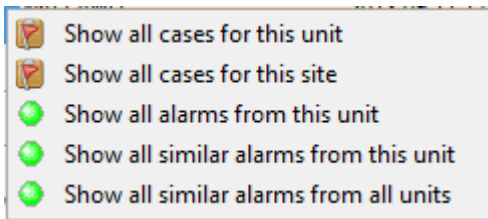


| Tab | description |
|--------------------|--|
| Users | Indicates the users that are are/have been involved in the case. |
| Alarms | Will list the individual alarms that are attached to this case. |
| Comments | Will list the comments that users have added. |
| Timeline | This is a complete list of all the actions taken on this case, from the time it was opened, until present. |
| Attachments | This will list all files that have been attached to this case. |



| Button | Description |
|------------------------|---|
| Add Comment | The operator may add further comments to the case. |
| Add Attachment | You may attach files of any size, or type to a case. |
| Escalate Case | The operator may escalate the case to another user. |
| CC Case | The operator may CC in another user on this case. |
| End Involvement | The operator may end his/her involvement with the case from here. They will, however, be required to enter a comment to justify this. |

Filters



You may filter incoming alarms based on:

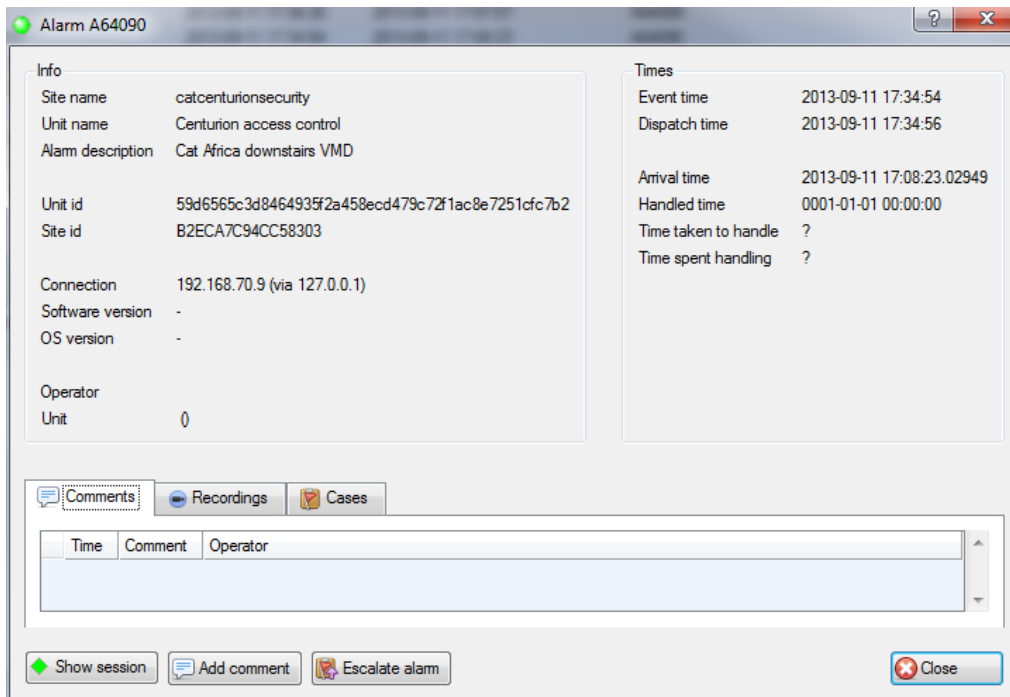
The **cases** for the site, or unit/server.

The **alarms** from

1. The unit/server that the alarm originated from.
2. The site the alarm originated from
3. Similar alarms from across all sites on this gateway

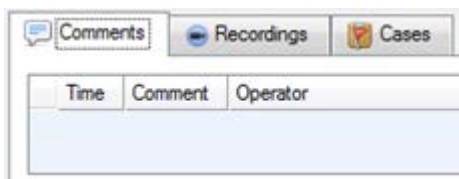
Note: the filtered alarms will be presented in the History Table, below, and not the Incoming alarms table.

Show Alarm Information



To show the alarm information, right click on an alarm in the incoming queue.

- **Tabs**



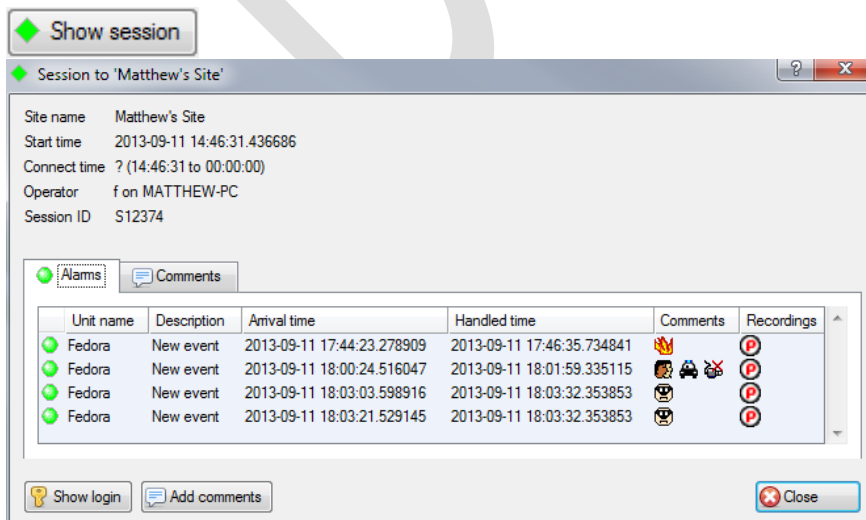
Comments are the comments added by a user handling, or clearing the alarm.

Recordings. If the operator downloads the video from the server to the gateway, then it shows up in the "Recordings"

Cases will be a list of cases that this alarm is associated with.

- **Buttons**

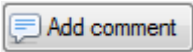
There are three buttons at the bottom of the Show Alarm Information window. **Show Session**, **Add Comment**, and **Escalate Alarm**



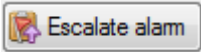
Show session will bring up all the details from this session. Sessions are described in detail, [above](#), under the [3.a. Incoming Alarm Table](#)

Show Login will show you the login details for the user that handled this alarm, and a list of sessions that they handled while they were logged in.

You may also add **comments** from this dialogue.

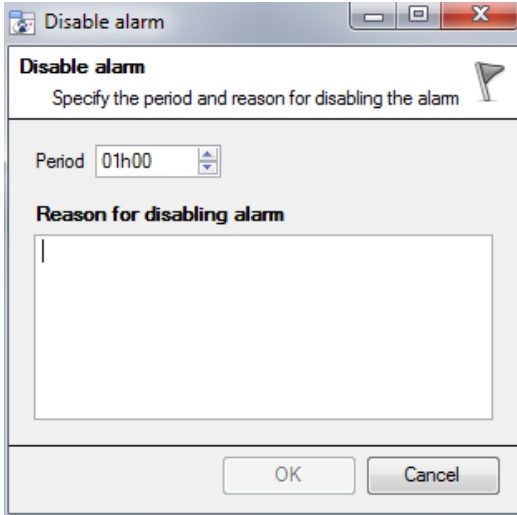


Will allow you to add further comments to this alarm.



Will allow you to escalate this alarm to a case.

Disable



The operator may disable an alarm.

This is useful for nuisance alarms, that are perhaps retriggering due to some environmental influence, such as a flashing light.

The operator will set the **period** that the alarm will be disabled for.

And will also be required to input a **Reason for disabling alarm** in the text box.

Connect To Site

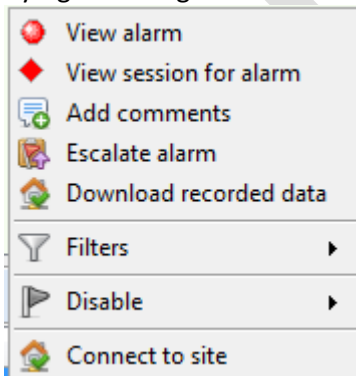
This will open the site that the alarm originated from.

c. History Table: Alarms

The history table is the bottom table in the Alarm Gateway interface. It is the table where alarms are sent after they are handled. It may be configured to display the Alarm History, Session History, Login History, and the Cases.

Right Click Menu

By right clicking on an alarm in the history table you will see the available actions.



View Alarm is identical to [Show Alarm Information](#), above.

View Session for alarm will show you a list of all alarms that were in the same session.

Add comments allows you to add further comments to this alarm.

Escalate alarm will allow you to edit, or create a case, for this alarm.

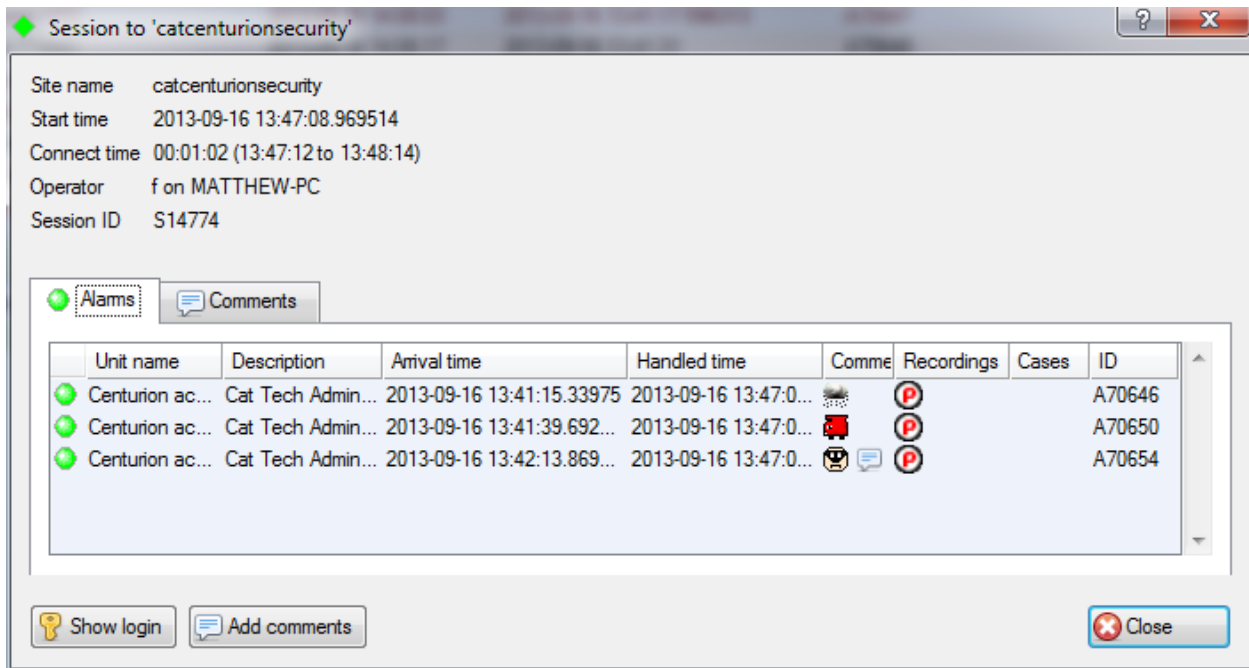
Download Recorded Data will download video, and associated data, from the server, to the local client computer.

Filters will allow you to filter the alarms in the history table.

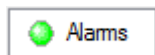
Disable will allow you to temporarily disable an alarm.

Connect to site will connect you to the alarm's originating site.

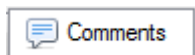
- *View session for alarm*



Tabs



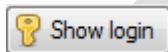
Will show a list of the alarms that were grouped into this session.



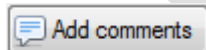
These are comments that are attached to the session.

Note: that, comments attached to individual alarms will only appear in the comments column under the Alarms tab. Comments that are added to the whole session will appear under the Comments tab.

Buttons



Will show you the login details for the user who handled this session. As well as the other sessions that that user handled while logged in.



Will allow you to add comments to the session.

Note: that this is for the session, and not the individual alarms within that session.

- *Add Comments*

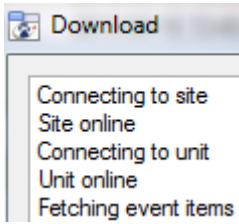
This will add comments to the selected alarm.

- *Escalate Alarm*

This will either escalate the alarm further, or create a case for the alarm, depending on what action the operator deems necessary.

For more information on cases see [d.Cases](#), below.

- **Download Recorded Data**



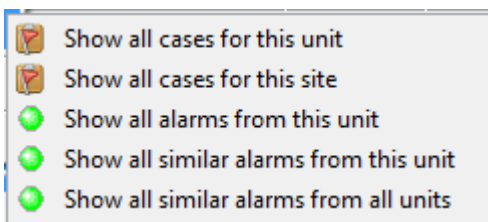
This will download video, and associated data, from the server, to the local client computer.

Once the data is fetched the same floating windows will appear in the as when you handle an alarm: **The Image Sequence Activation Window**, and the **Activity Detection Window**. You may review the data as you would, if you had handled the incoming alarm.

Note:

1. You will have to log into the site, to fetch the data.
2. You will also have to leave a comment as to why you logged in

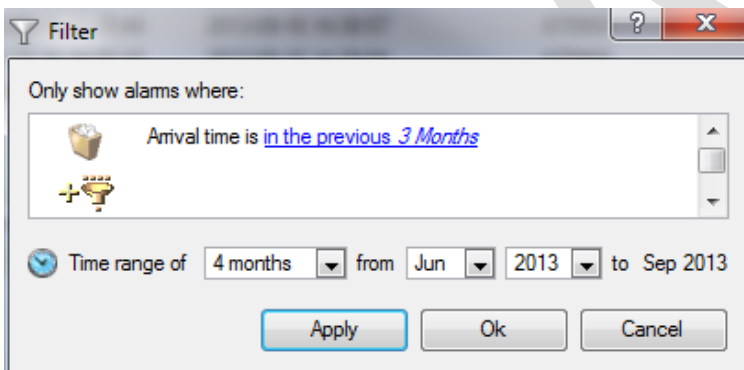
- **Filters**



Right clicking on an alarm and selecting Filters will allow you to filter the history table, with the alarm you clicked on as the focus.

So you may filter cases, and alarms that relate to the selected alarm.

Filter



A far more versatile filter is available in the top right hand corner of the History Table. Clicking on → **Edit Filter** will bring up the Filter dialogue. means there are active filters.

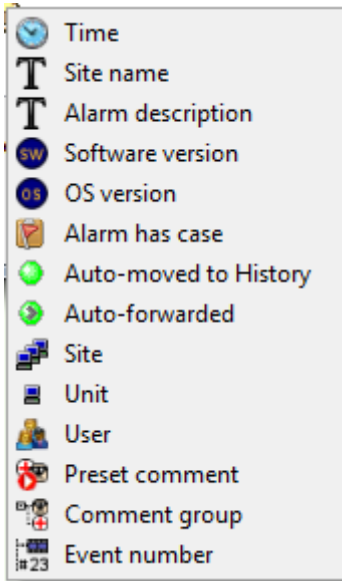
The **time range** will default to the last time range set.

Click on to add a filter, and click on to remove an added filter.

Note:

1. After adding a filter you will have to click on the blue hyperlink, and define the parameters of that filter. (Except for the Alarm Has Case, Auto-Moved, and Auto-Forwarded options.)
2. If you leave an added filter with its parameters un-set, there is a good chance that your filter will return zero results.

- **Available filters**



Time allows you to further define the time period.

Site name requires that you enter a string.

Alarm description also requires a manually entered string.

Software version is the CatVision version that sent the alarm.

OS version is the operating system the originating CatVision is running on.

Alarm has case will only return alarms that have already been escalated.

Auto-moved to History will feature alarms that timed out of the incoming queue, and were sent to the history table without being handled.

Auto-forwarded will list all alarms that were automatically sent to the gateway.

Site will give filter based on all Sites that send alarms to this gateway.

Unit will filter based single units, within sites, that send alarms to this gateway.

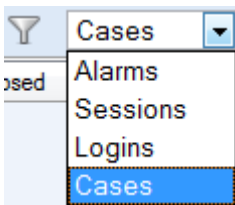
User will filter based on Gateway users (not site users).

Preset comment filters alarms based on the comments that have been added to them.

Comment group filters based on comment groups (e.g. Actual Alarms).

Event number This is the unique ID number given to the event.

d. History Table: Sessions, Logins, and Cases




The History Table lists three other sets of historic data: the **Sessions**, **Logins**, and **Cases** that this Gateway has handled.

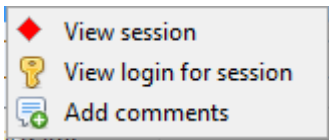
Sessions

Sessions are formed when the same alarm arrives from a site, while the connection to the gateway is still open.

- **Session Columns**


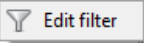
| Sessions  | Description |
|--|--|
| Site name | The name of the originating site |
| Description | The description of the alarm |
| Handled by | Which operator handled the alarm. |
| Arrival time | When the alarm arrived at the gateway |
| Comments | User added comments |
| Recordings | If the operator downloads the video from the server to the gateway, then it shows up in the "Recordings" |
| Cases | Cases that this session has been escalated to, if any |
| ID | The unique session ID |

- **Right Click Menu**



View Session will show you the session, as per Show Alarm Information, above.
View Login for session will detail the activities of the user, while they were logged in, and dealt with this session.
Add comments will allow you to add comments to the session.

- **Session Filters**


To filter the session click on the  icon in the top right of the History table, and click on . This will bring up the Filter dialogue.



Time allows you to filter sessions within a specified period.
Alarms were handled will only show sessions where alarms were handled.
No alarms were handled will only show sessions where alarms were handled.
Site will only show sessions from selected sites.
User will only show sessions dealt with by specific users.
Base Station will only show sessions originating from specific base stations.

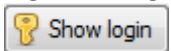
Logins

- **Login columns**

| Logins  | Description |
|--|---|
| User | Is the user that was logged in. |
| Base station | Is the base station on which this user was logged in. |
| Login | This is the date, and time, that this user logged into this base station. |
| Logout | The date, and time, that this user logged out of this base station. |
| Duration | This is the time period the user was logged in for. |
| Sessions | How many sessions the user handled during this login period. |
| ID | This is the unique number given to this login session. |

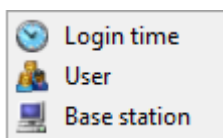
- **Right click menu**

Right clicking on a specific login will give you the following menu options:



Will show same details that you see in this table. As well as a table of the sessions that the user handled while logged in.



- **Logins filters**



Login time will only show logins within the time period you set.
User will only show logins by the user that you set.
Base station will filter logins by the base station on which the user logged in.

Cases










- **Case Columns**

| Cases   | Description |
|---|---|
| Case id | This is the unique ID number given to the case. |
| Reference | This is the reference given to the case by the person who escalated it. |
| Description | The description of the alarm that was first escalated. |
| Opened | The time and date the case was created. |
| Opened by | Which user opened the case. |
| Closed | The time and date the case was closed. |
| Closed by | Which user closed the case. |

- **Right Click menu**

 **View case** will expand the case, so the operator/administrator may view the full case.

- **Case Filters**

| | |
|---|----------------|
|  | Open time |
|  | Close time |
|  | Description |
|  | Reference |
|  | Comment |
|  | Case is open |
|  | Case is closed |
|  | Open user |
|  | Close user |

Open time: filter based on when the case was opened.

Close time: filter based on when the case was closed.

Description: filter on descriptions based on the presence/absence of a user input string

Reference: filter on references based on the presence/absence of a user input string.

Comment: filter on comments based on the presence/absence of a user input string.

Case is open: only show open cases.

Case is closed: only show closed cases.

Open user: only show cases opened by a specific user.

Close user: only show cases closed by a specific user