



# Alarm Management Gateway Setup Manual

# Contents

1. Introduction.....	3
2. Alarm Gateway Database Setup.....	4
2.1 Windows.....	4
2.2 Ubuntu.....	5
2.3 NetBSD.....	7
2.4 Fedora.....	8
2.5 Commands.....	10
2.6 Troubleshooting .....	10
3. Upgrade AMG Database from MySQL to PostgreSQL .....	11
3.1 Local NetBSD to Local NetBSD.....	11
3.2 Local NetBSD to Remote NetBSD/Fedora/Windows Unit.....	12
3.3 Commands.....	16
3.4 Troubleshooting .....	16
4. Setups on the Server .....	17
4.1 Communications Tab.....	17
4.2 Gateway Tab.....	18
4.3 Licensing .....	19
4.4 Enable Client to Connect to Gateway.....	20
4.5 Set up Operator Procedures.....	21
5. Gateway Menu Settings .....	24
5.1 Reports .....	24
5.2 Cases.....	26
5.3 Disabled Alarms.....	27
5.4 Users.....	27
5.5 Preset Comments .....	30
5.6 Heartbeat Monitoring.....	31
5.7 Settings .....	33
6. Conclusion .....	35

## 1. Introduction

This document deals with the setup of the Alarm Management Gateway. For information about the operation of an Alarm Management Gateway, please consult the Alarm Management Gateway Operation Manual.

For further support, contact [support@cat.co.za](mailto:support@cat.co.za).

### A NOTE ON CAMERA CHANNELS

The CathesisVision software packages have **limits on camera channels**. A multi-sensor camera is physically a single device (camera) but it **requires a camera channel for each one of the internal cameras**. The same applies to an encoder: a 16-channel encoder will account for 16 camera channels on the CathesisVision software, even though it is a single device.

### USEFUL LINKS

To view **tutorial videos** on CathesisVision setup, visit <https://cathesisvideo.com/resources/videos>

Find answers to Cathesis **Frequently Asked Questions**: <https://cathesis.crisp.help/en/?1557129162258>


## 2. Alarm Gateway Database Setup

This section takes the user through the setup process for an Alarm Gateway Postgres database. There are two steps that need to be taken to do this.

1. The unit needs to be licensed as an alarm gateway with the CAMG-1000 license.
2. The Postgres database needs to be prepared.

At present the setup process for the Postgres database for the Alarm Gateway is done via the command line/text terminal.

### Important notes:

- If a pre-existing Alarm Gateway Database was running on a software version up to, and including, 5043a, the user will have to run through the upgrade process. Please consult [Chapter 3 \(Upgrade AMG Database from MySQL to PostgreSQL\)](#) of this manual.
- To run the database utility, the user must be in the CathesisVision installation folder.
- The installation folders shown here are not always the same as the folder that CathesisVision will be installed in on the system. They are simply the default installation path offered when installing CathesisVision.
- Make sure to perform all actions as an **Administrator\root user**.
- If the unit is licensed for use as an Alarm Gateway, but a Postgres database has not been set up, there will be an icon in the bottom right-hand corner of the CathesisVision interface. 
- After licensing a unit with the gateway license, on any operating system, the user will need to reboot the unit for the licenses to take effect.
- Command line paths that contain spaces between the words will require quotes.



**It is vital that the user sets up the AMG database before proceeding to the next steps.**

**Note:** If a pre-existing Alarm Gateway Database was running on a software version up to, and including 5043a (the edition preceding CathesisVision 2014), the user will have to run through the upgrade process. Please follow the upgrade instructions in [Chapter 3](#).

### 2.1 Windows

#### 2.1.1 Create a New Database

Enter the Command Line Terminal.

1. Click on the Start Menu button. 
2. Type in "cmd" in the search box.
3. Right-click on **cmd** and select Run as Administrator. 

### 2.1.1.1 Navigate to the CathesisVision Installation Folder

**Note:** These commands must be run from the CathesisVision installation directory. The user will need to navigate to the CathesisVision installation directory. The paths provided will only be accurate if the user has installed to the default location.

The default Windows installation directory is “C:\Program Files\CathesisVision Server”. Thus, the user would type in **cd “C:\Program Files\CathesisVision Server”**.

### 2.1.1.2 Set up the Postgres Database

#### Check the Current Database Status

Type the following into the command line, and press **enter**.

```
bin\gateway_dbutil status
```

#### Configure a New Postgres Database

**Note:** DB\_PATH, below, represents the folder path, to wherever the user chooses to create the database. This does not have to be in the CathesisVision installation folder. For example, a valid installation path could be `c:\gatewaydb`. It is up to the user.

Type in the following, in the command line:

```
bin\gateway_dbutil create DB_PATH
```

The last line output will give the user the information regarding the success of the database creation. This will either be **"Create database - SUCCEEDED"** or **"Create database - FAILED"**

#### Re-start the Server, and Check the Status

1. Reboot the server
2. Navigate back to the CathesisVision installation folder
3. Run `bin\gateway_dbutil status` again

The output should now indicate that the database is both **configured** and **running**.

## 2.2 Ubuntu

### 2.2.1 Create a New Database on a Primary Disk

Enter the Command Line Terminal.



Click on the “Search your computer” Home button, and type “Terminal” in the search bar.

Click on the terminal icon which will show up in the results:



### 2.2.1.1 Navigate to CathesisVision Installation Folder

**Note:** These commands must be run from the CathesisVision installation directory. The user will need to navigate to the CathesisVision installation directory.

(The default Ubuntu installation directory is /usr/nvr. Thus, the user would type in `cd /usr/nvr` to get to the default installation directory.)

### 2.2.1.2 Set up the Postgres Database

#### Check the Current Database Status

Type the following into the command line, and press enter:

```
sudo ./launch.sh bin/gateway_dbutil status
```

#### Configure a new Postgres Database

Type the following on the command line.

```
sudo ./launch.sh bin/gateway_dbutil create DB_PATH
```

**Note:** the DB\_PATH is wherever the user chooses to create the database. This does not have to be in the CathesisVision installation folder.

The last line output will give the user the information regarding the success of the database creation. This will either be "**Create database - SUCCEEDED**" or "**Create database - FAILED**"


### 2.2.1.3 Re-start the Server, and Check the Status

1. Reboot the server
2. Navigate back to the CathesisVision installation folder
3. Run `sudo ./launch.sh bin/gateway_dbutil status` again.

The output should now indicate that the database is both **configured**, and **running**.

## 2.2.2 Creating a New Database on a Secondary Disk

When creating a Postgres database on a secondary disk, the user will need to do the following.

1. Start up CathesisVision.
2. Go to the Setup tab. (**Site** → **Open tab** — **Setup**)
3. Click on **Configure servers**  .
4. Select the server on which the gateway database is being set up.

5. Click on the **Databases**.
6. Click on **Manage Disks**.
7. Format and attach the secondary disk.
8. Using the Mount path for the secondary disk in the Manage disk.
9. Create database via command. For example:

```
sudo ./launch.sh bin/gateway_dbutil create /disk_mounts/fp2015031015192.../db
```

## 2.3 NetBSD

### 2.3.1 Create a New Database

Enter the Command Line Terminal.

1. Press CTRL+F4 (the CTRL key, and the F4 key, simultaneously)
2. Log in as a root user.1

#### *2.3.1.1 Navigate to CathesisVision Installation Folder*

**Note:** These commands must be run from the CathesisVision installation directory. The user will need to navigate to the CathesisVision installation directory.

(The default NetBSD installation directory is /usr/dvs. Thus, the user would type in `cd /usr/dvs` to get to the default installation directory.)

#### *2.3.1.2 Set up the Postgres Database*

##### **Check the Current Database Status**

Type the following into the command line, and press enter.

```
./bin/gateway_dbutil status
```

##### **Configure a new Postgres Database**

Type the following on the unit.

```
./bin/gateway_dbutil create DB_PATH
```

##### **Note:**

- The DB\_PATH is wherever the user chooses to create the database. This does not have to be in the CathesisVision installation folder.

- The database partition should probably be placed most often in /usr/data/wd0f because this will be the partition with the most space.
- The last line output will give the user the information regarding the success of the database creation. This will either be "**Create database - SUCCEEDED**" or "**Create database - FAILED**"

### Re-start the Server, and Check the Status

1. Reboot the server.
2. Navigate back to the CathexisVision installation folder.
3. Run `./bin/gateway_dbutil status` again.

The output should now indicate that the database is both **configured**, and **running**.

## 2.3.2 Special Warning on NetBSD

Do not set up a Gateway Database on a NetBSD unit that is also running, or going to run, an Integration Database. NetBSD can only support a single instance of PostgreSQL running at any one time. This means that running an Alarm Gateway and an Integration Database on the same system will cause a conflict.

## 2.4 Fedora

### 2.4.1 Create a new database

Enter the Command Line Terminal.

Right-click on the Desktop and select "Konsole".

#### 2.4.1.1 Navigate to CathexisVision Installation Folder

**Note:** These commands must be run from the CathexisVision installation directory. The user will need to navigate to the CathexisVision installation directory.

(The default Fedora installation directory is /usr/nvr. Thus, the user would type in `cd /usr/nvr` to get to the default installation directory).

#### 2.4.1.2 Set up the Postgres Database

##### Check the Current Database Status

Type the following into the command line, and press enter.

```
./bin/gateway_dbutil status
```



## Configure a New Postgres Database

Type the following on the command line.

```
./bin/gateway_dbutil create DB_PATH
```

**Note:** The DB\_PATH is wherever the user chooses to create the database. This does not have to be in the CathesisVision folder.

The last line output will give the user the information regarding the success of the database creation. This will either be "**Create database - SUCCEEDED**" or "**Create database - FAILED**"


## Re-start the Server, and Check the Status

1. Reboot the server.
2. Navigate back to the CathesisVision installation folder.
3. Run `./bin/gateway_dbutil status` again.

The output should now indicate that the database is both **configured** and **running**.

## 2.4.2 Creating a New Database on a Secondary Disk

When creating a Postgres database on a secondary disk, the user will need to do the following.

1. Start up CathesisVision.
2. Go to the Setup tab. (**Site / Open tab / Setup**)
3. Click on **Configure servers**  .
4. Select the server on which the gateway database is being set up.
5. Click on the **Databases**.
6. Click on **Manage Disks**.
7. Format and attach the secondary disk.
8. Using the Mount path for the secondary disk in the Manage disk create database via command. For example:

```
./bin/gateway_dbutil create /disk mounts/fp2015031015192.../db
```

## 2.5 Commands

The table below describes the commands that the user can use with the gateway\_dbutil.

Command	Description
gateway_dbutil status	Checks that database is configured
gateway_dbutil create   gateway_dbutil create_base	<ul style="list-style-type: none"> <li>Creates database cluster and initializes the Cathesis database</li> <li>Returns 0 on success</li> <li>If there is a pre-existing Cathesis PostgreSQL database, appending the line with “force” will override the existing .ini file, and create the new database.</li> <li><b>create_base</b> is used instead of <b>create</b> when upgrading from a MySQL to a PostgreSQL database. It creates the database at the base version (version1) which is necessary for the conversion process.</li> </ul> <p>This database will then be updated to the latest version later in the process.</p>
gateway_dbutil update	<p>Will update the database to the latest SQL schema version.</p> <p><b>Note:</b> This will always be done by the gateway server when it starts the database, and should not need to be used.</p>
gateway_dbutil start	Starts the SQL server
gateway_dbutil stop	Stops the SQL server

## 2.6 Troubleshooting

If the user has followed the above instructions, and the Alarm Gateway is not working, consider the following troubleshooting tips:

1. Is the gateway license applied and valid? (Check the time period for the license.)
2. Does “bin/gateway\_dbutil status” report the database as running?
3. Is it running?
  - a. Can the user see postgres in the task manager listing? (on Windows)  
The “see processes from other users” will have to be ticked.
  - b. On NetBSD/Fedora “ps -a | grep postgres” should show if it is running.

If the user has gone through the above steps, and the gateway is still not working, please contact [support@cat.co.za](mailto:support@cat.co.za), or the supplier for further assistance.

## 3. Upgrade AMG Database from MySQL to PostgreSQL

The user who has been running an Alarm Gateway on software versions up to, and including, 5043a will have to run this upgrade to PostgreSQL. This section details the steps required to upgrade an existing CathesisVision MySQL Alarm Gateway database to a PostgreSQL Alarm Gateway database.

This document provides instructions on how to convert from MySQL to PostgreSQL in 4 different circumstances:

1. Local NetBSD to local NetBSD.
2. Local NetBSD to remote NetBSD.
3. Local NetBSD to remote Linux.
4. Local NetBSD to remote Windows.

### Note:

- This chapter applies to units that **already have** a pre-existing Alarm Gateway Database running.
- **CathesisVision support for NetBSD 3 and earlier NetBSD versions was removed in CV2015. Support for NetBSD 4 was removed in CV2017.**
- **CathesisVision support for Fedora 16 was removed in CV2019.**
- To run the database utility, the user must be in the CathesisVision installation folder.
- The installation folders shown here are not always the folder that CathesisVision will be installed in on the system. They are simply the default installation path offered when installing CathesisVision.
- Make sure to perform all actions as an **Administrator\root user**.
- Command line paths that contain spaces between the words will require quotation marks.

Correct	Not Correct
<code>cd "c:\Program Files\gatewaysql"</code>	<code>cd c:\Program Files\gatewaysql</code>

### 3.1 Local NetBSD to Local NetBSD

This section details the procedures for converting a MySQL database to a PostgreSQL database on the same unit.

#### 3.1.1 Stop All Servers

The user will need to stop all **CathesisVision services**, and the **WatchDog**, before doing anything else.

1. Log in as root
2. Change directory to the CathesisVision installation folder: `cd /usr/dvs`
3. Run the following command, to disable the WatchDog: `./wdenable 0`
4. To disable the servers: `cd /usr/dvs/scripts`

## 3.1.2 Commands

These are the different command line entries that the user must make to complete the database creation, and conversion. For more information about what each command does, see [Commands](#) at the end of this chapter.

**Note:** these commands must be run from the CathesisVision installation directory. The user will need to navigate to the CathesisVision installation directory. (The default NetBSD installation directory is /usr/dvs. Thus, the user would type in `cd/usr/dvs` to get to the default installation directory.)

### 3.1.2.1 Run the Following Sequence of Commands

1. Run `./bin/gateway_dbutil create_base /usr/data/wd0f/gatewaysql`

**Note:** Select a partition with lots of free space, we recommend the wd0f partition which can be found under /usr/data/wd0f

2. Run `./bin/gateway_dbutil start`
3. Run `./bin/gateway_mysql2psql`

**Note:** This may take a while to convert. The time taken will relate to the size of the database that you are converting.

4. Reboot.
5. Navigate back to the installation folder and run `./bin/gateway_dbutil status` to verify that the database is configured and running.

## 3.2 Local NetBSD to Remote NetBSD/Fedora/Windows Unit

The user may move a MySQL database from one unit to another, and convert it to a PostgreSQL database in the process. This is useful when the user wants to install a new unit but still wants to keep the same Alarm Database.

**Note:**

- The source unit (the unit with the old database) must have the latest CathesisVision 5043a, or CathesisVision 2014, software on it.
- Remember that all commands must be run from the respective installation folders, on both units.

### 3.2.1 Stop All Servers (On Both Units)

The user will need to stop all CathesisVision services, and the WatchDog, on both units involved in this conversion/transferral.

### 3.2.1.1 Stopping Servers on a NetBSD Server

1. Log in as root.
2. Change directory to the CathesisVision installation folder: `cd /usr/dvs`
3. Run the following command, to disable the WatchDog: `./wdenable 0`
4. To disable the servers: `cd /usr/dvs/scripts`

### 3.2.1.2 Stopping Servers on Windows and Fedora Systems

On Fedora and Windows systems, the user may disable the servers and the watchdog, via the HTML interface. (**Note:** please ensure that port 33101 is open on the unit being upgraded.)

#### Enter the HTML interface

To do so, open a web browser and enter the connection details into the URL box. The connection details are:

- The IP address of the unit
- Followed by the colon (:)
- And the port: 33101

If the user is updating the database from the unit physically being worked on, the user may use the loopback IP address.	<b>127.0.0.1:33101</b>
If the user is updating the database from another unit, enter in the IP address of the unit whose database being updated.	<b>The_units_IP_address:33101</b> (e.g., 192.168.71.145:33101)

**Note:** the user will be required to enter a username and password. Enter a CathesisVision administrator's username and password.

<p><b>Cathesis NVR service</b></p> <p><a href="#">Control</a></p> <p><a href="#">Logs</a></p>	<p>The HTML interface will look like the image to the left.</p> <p>The settings the user needs are under <b>Control</b>. Click on this hyperlink.</p>
-----------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------

### 3.2.1.3 Control

[Restart servers](#)

[Stop all servers](#)

[Force stop all servers](#)

[Disable watchdog](#)

After clicking on Control, the user will be able to disable the watchdog, and servers, by clicking on their respective hyperlinks.

1. Stop all servers
2. Disable watchdog

The servers, and the watchdog, will re-start when the user reboots the unit.

## 3.2.2 Commands On the Target Unit

Run the following commands on the target unit. Follow the instructions in the section that relate to the Operating System of the target unit.

### 3.2.2.1 NetBSD Server

#### Run the Following Sequence of Commands

1. Run `./bin/gateway_dbutil create_base /usr/data/wd0f/gatewaysql`

**Note:** Select a partition with a lot of free space. We recommend the wd0f partition which can be found under `/usr/data/wd0f`

2. Run `./bin/gateway_dbutil start`

3. In this step, run the `mysql2psql` command with `"-sh SRC_IP"`. `-sh` stands for source host. It will connect to the MySQL on the source unit, and convert it into the local PostgreSQL database which was created using `gateway_dbutil`.

For example: If the remote unit, with the old database, has an IP address of 192.168.34.50, the entry would look like this:

`./bin/gateway_mysql2psql -sh 192.168.34.50`

**Note:** This may take a while to convert. The time taken will relate to the size of the database that is being converted.

4. Reboot
5. Navigate back to the installation folder and run `./bin/gateway_dbutil status` to verify that the database is configured and running.

### 3.2.2.2 Linux (Fedora) Server

**Note:** These commands must be run from the CathesisVision installation directory. The user will need to navigate to the CathesisVision installation directory. (The default Fedora installation directory is /usr/nvr. Thus the user would type in `cd /usr/nvr` to get to the default installation directory.)

#### Run the Following Sequence of Commands

1. Run `./bin/gateway_dbutil create_base /usr/gatewaysql`

**Note:** it is advisable to create a dedicated partition for this database, of around 50GB.

2. Run `./bin/gateway_dbutil start`

3. In this step you run the `mysql2psql` command with `"-sh SRC_IP"`. `-sh` stands for source host. It will connect to the MySQL on the source unit, and convert it into the local PostgreSQL database which was created using `gateway_dbutil`.

For example: if the remote unit, with the old database has an IP address of 192.168.34.50, then the entry would look like this:

```
./bin/gateway_mysql2psql -sh 192.168.34.50
```

**Note:** This may take a while to convert. The time taken will relate to the size of the database that you are converting.

4. Reboot
5. Navigate back to the installation folder and run `./bin/gateway_dbutil status` to verify that the database is configured and running.

### 3.2.2.3 Windows Server

**Note:** These commands must be run from the CathesisVision installation directory. The user will need to navigate to the CathesisVision installation directory. The paths provided will only be accurate if the user has installed to the default location.

The default Windows installation directory is `"C:\Program Files (x86)\Cathesis CathesisVision Suite NVR"`. Thus the user would type in `cd "C:\Program Files (x86)\Cathesis CathesisVision Suite NVR"`.

#### Run the Following Sequence of Commands

1. Run `bin\gateway_dbutil create_base C:\gatewaysql`

**Note:** it is advisable to create a dedicated partition for this database, of around 50 GB.

2. Run `bin\gateway_dbutil start`

3. In this step, the user runs the `mysql2psql` command with `"-sh SRC_IP"`. `-sh` stands for source host. It will connect to the MySQL on the source unit, and convert it into the local PostgreSQL database which was created using `gateway_dbutil`.

For example, if the remote unit, with the old database, has an IP address of 192.168.34.50, the entry would look like this:

```
.\bin\gateway_mysql2psql -sh 192.168.34.50
```

4. Reboot.
5. Navigate back to the installation folder and run `bin\gateway_dbutil status` to verify that the database is configured and running.

### 3.3 Commands

This is the full list of commands available, and the actions they perform. (To see this in the text terminal, run `gateway_dbutil` without any parameters.) Remember to run them from *within* the installation folder.

Command	Description
<code>gateway_dbutil status</code>	Checks that the database is configured
<code>gateway_dbutil create</code>   <code>gateway_dbutil create_base</code>	<ul style="list-style-type: none"> <li>• Creates the database cluster and initializes the Cathexis database.</li> <li>• Returns 0 on success.</li> <li>• If there is a pre-existing Cathexis PostgreSQL database, appending the line with “<b>force</b>” will override the existing .ini file, and create the new database.</li> <li>• <b>create_base</b> is used instead of <code>create</code> when upgrading from a MySQL to a PostgreSQL database. It creates the database at the base version (version 1) which is necessary for the conversion process. This database will then be updated to the latest version later on in the process.</li> </ul>
<code>gateway_dbutil update</code>	Will update the database to the latest SQL schema version.  <b>Note:</b> This will always be done by the gateway server when it starts the database, and should not need to be used.
<code>gateway_dbutil start</code>	Starts the SQL server.
<code>gateway_dbutil stop</code>	Stops the SQL server.

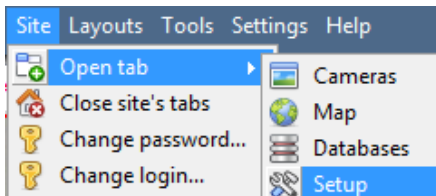
### 3.4 Troubleshooting

If the above steps have been followed, and the gateway is still not working, please contact [support@cat.co.za](mailto:support@cat.co.za), or the supplier, for further assistance.



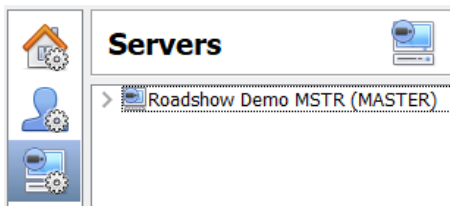
## 4. Setups on the Server

Here, the user will set up the desired server unit/s to send alarms to the Gateway unit. These settings take place in the Configure Servers Panel in the Setup Tab.

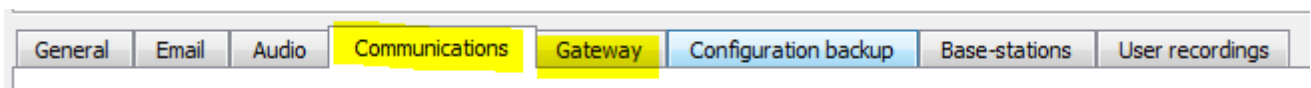


### 1. Site / Open Tab / Setup

2. The Setup Tab is now open. Click on the Configure Servers icon:



3. Once in the Configure Servers panel, click on the name of the desired server. Do not expand it. The tab options below will be displayed:



The following section will deal with the **Communications** and **Gateway** tabs.

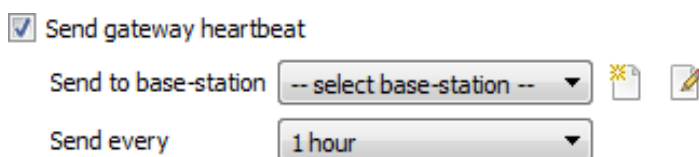
**Important:** both the **Heartbeat** ([Communications tab](#)) and the **Heartbeat monitor** ([Gateway tab](#)) must be enabled and configured for an alarm to be possible.

### 4.1 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.

An alarm is generated if the server goes down, or if the communications medium goes down.

#### 4.1.1 Send Gateway Heartbeat



1. Check **Send gateway heartbeat** to enable the heartbeat.

2. Select the base-station (gateway) that the heartbeat will be sent to.

3. Define how often the unit will send a heartbeat to the Gateway.

**Note:** this needs to be set up on both the capture station and the Alarm Management Gateway.

### 4.1.1.1 Create/Edit Base-Station



Click to create a base-station.



Click to edit a base-station.

This will bring up the window below.

**Name** the base-station.

Select the base-station **Type**.

Enter the **IP address** of the Gateway unit (i.e. the unit that will be receiving all gateway alarms).

The next section will deal with the settings in the **Gateway** tab.

## 4.2 Gateway Tab

This section deals with the Alarm Gateway.

### 4.2.1 Enable Heartbeat Monitoring Alarms





Send heartbeat monitoring alarms to -- select base-station --

Tick the box to send heartbeat monitoring alarms. Select the base-station to which these alarms will be sent.

**Note:** if the box is unchecked, the alarms will not be sent anywhere.

#### 4.2.1.1 If An Alarm is Not Handled

If alarms have not been handled for a while, the user might wish to send unhandled alarms to other gateways, or base-stations.

If an alarm in the gateway has not been handled in <input type="text" value="5"/> minutes then <ul style="list-style-type: none"> <li>▪ if it is a technical alarm forward it to <input type="text" value="test base-station"/>  </li> <li>▪ if it is an event alarm forward it to <input type="text" value="test base-station"/>  </li> </ul> <input checked="" type="checkbox"/> Move to History after forwarding	1. Decide the amount of time before which unhandled alarms are sent to other base-stations or gateways. 2. Decide which base-stations/gateways specific types of alarms will be sent to.
Move gateway alarms to History if they have not been handled in <input type="text" value="-"/> minutes	
3. Select <b>Move to History after forwarding</b> to move unhandled alarms to the history after they have been forwarded to the gateway. 4. Decide the amount of time before unhandled alarms are moved to History.	
<p><b>Tip:</b> if an alarm is sent 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, the user may wish to check the <b>Move to history after forwarding</b> box, which will move the alarm to the history queue of the forwarding unit.</p>	

#### 4.2.1.2 Create/Edit Base-Station



Click to create a base-station.



Click to edit a base-station.

## 4.3 Licensing

The Cathexis Alarm Gateway provides an extremely comprehensive multi-user alarm management capability for on-site, or multi-site, management of events or alarms.

### 4.3.1 Alarm Management Gateway Server License (CAMG-1000)

This **CAMG-1000** license enables the Alarm Management Gateway on the CathexisVision software and database for a site or a control room environment.

Typically, only one of these licenses is needed for a control room to manage alarms for an unlimited number of servers, cameras, or remote sites. The CAMG-1000 license comes **bundled** with a CathexisVision **Professional** Site license.

This software will create a unique database for the management and reporting of alarms, and user actions, and should be applied to any server on which the alarm database is to reside.

**Note:** The Professional site license that is bundled with the CAMG-1000 license has no value on its own and is inseparable from the CAMG-1000 license. The Professional site license is added solely to enable a separate setup of an AMG server without the added site license cost.

### 4.3.2 Alarm Client License (CBAS-7100)

This is the license required for each client or operator who is connecting to the Alarm Gateway.

**Note:** Clients who are viewing the site but not connecting to the gateway do not require this license. This license should be applied to the client machine. A client map license (CMAP-3000) is included with the purchase of a CBAS-7100 license.

## 4.4 Enable Client to Connect to Gateway

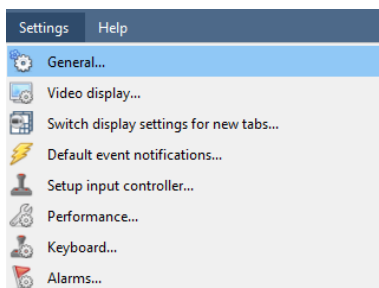
To connect to the Alarm Management Gateway, the Client unit will need to be enabled to connect. This can be done in two ways: either within the Client interface (**only applicable to CathesisVision 2018.1 and later**), or by appending the CathesisVision shortcut Target line.

**Note:** Appending the shortcut target line will override any settings configured in the CathesisVision interface.

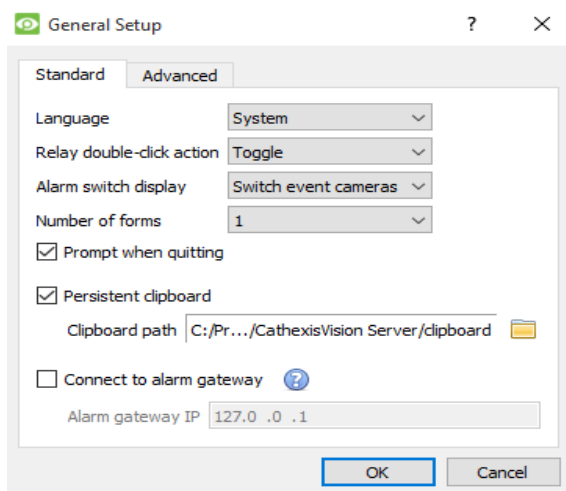
### 4.4.1 Enable in CathesisVision Interface

**Note:**

1. This method is only available in CathesisVision 2018.1 and later. However, the Target line method (below) may also be used.
2. Gateway settings configured via the Target line will override the settings configured in the interface.



In CathesisVision, select **Settings Menu / General...**



### Connect to Alarm Gateway

Check to enable connection to the alarm gateway. Enter the gateway unit's IP address.

Click the **question mark icon** to display license information. These settings can also be configured by editing the command line. See the command line options [below](#).

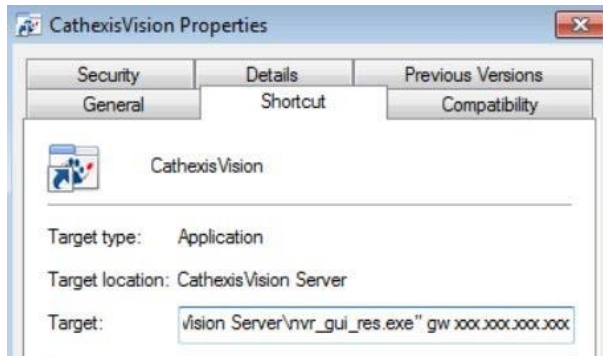
**Note:** editing the command line will override these settings.

Re-start CathesisVision for the settings to take effect.

## 4.4.2 Append Shortcut Target Line

**Note:**

1. This method must be used for all pre-2018.1 CathesisVision systems.
2. While this method may also be used in CathesisVision 2018.1 and later, it should be noted that the settings configured here will override any settings configured in the CathesisVision interface.



The following needs to be appended to the target line of the Client shortcut:

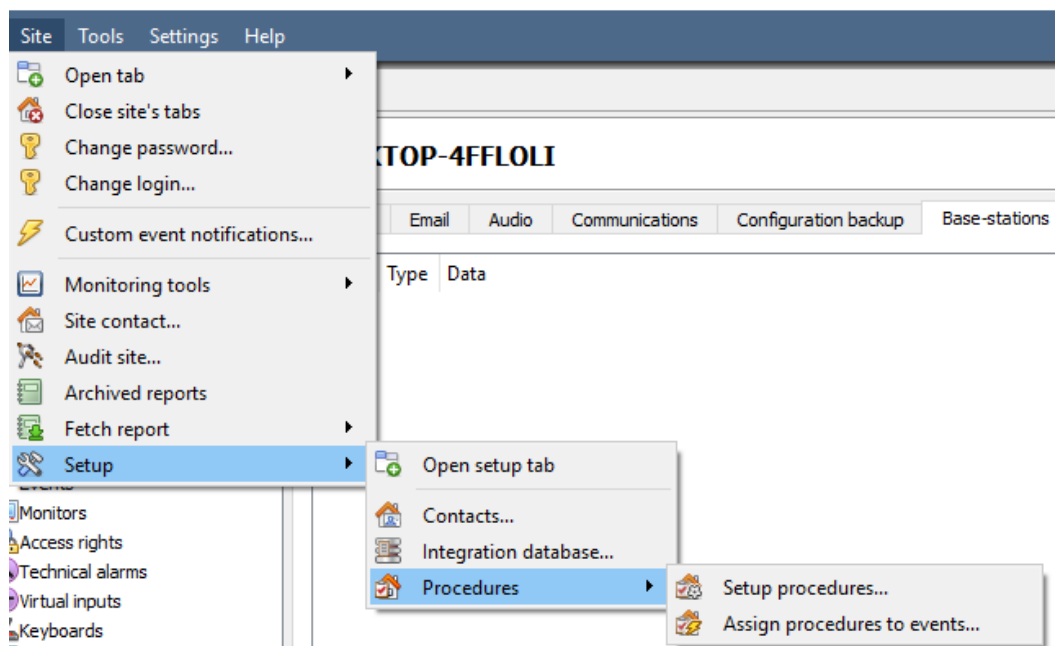
gw xxx.xxx.xxx.xxx

(Where xxx.xxx.xxx.xxx is the IP address of the Alarm Gateway unit that the Client is connecting to.)

## 4.5 Set up Operator Procedures

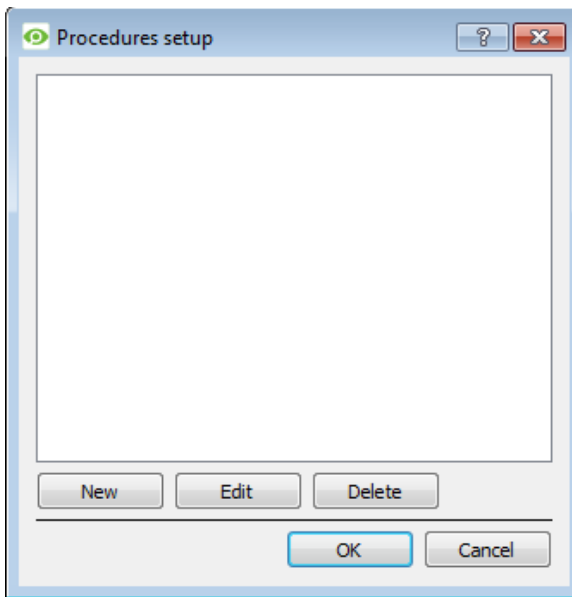
Setting up procedures is useful to guide operators in the preferred procedures for responding to a particular event. This may include up to 6 contact people, and written instructions.

### Site Menu / Setup / Procedures



<b>Setup procedures...</b>	Click to configure procedures.
<b>Assign procedures to events...</b>	Click to assign configured procedures to existing events.

## 4.5.1 Setup Procedures



New

**Create new procedure.**

Edit

**Edit existing procedure.**

Delete

**Delete procedure.**

See below for creating a new procedure.

### 4.5.1.1 New Procedure



Give the procedure a **Name**.

Select up to six **Contacts** which the operator should/can contact.

**Note:** Contacts must already be configured for them to appear in the drop-down menus. Contacts are configured in **Site / Setup / Contacts**.

Type specific instructions for the operator to follow when the alarm is received.

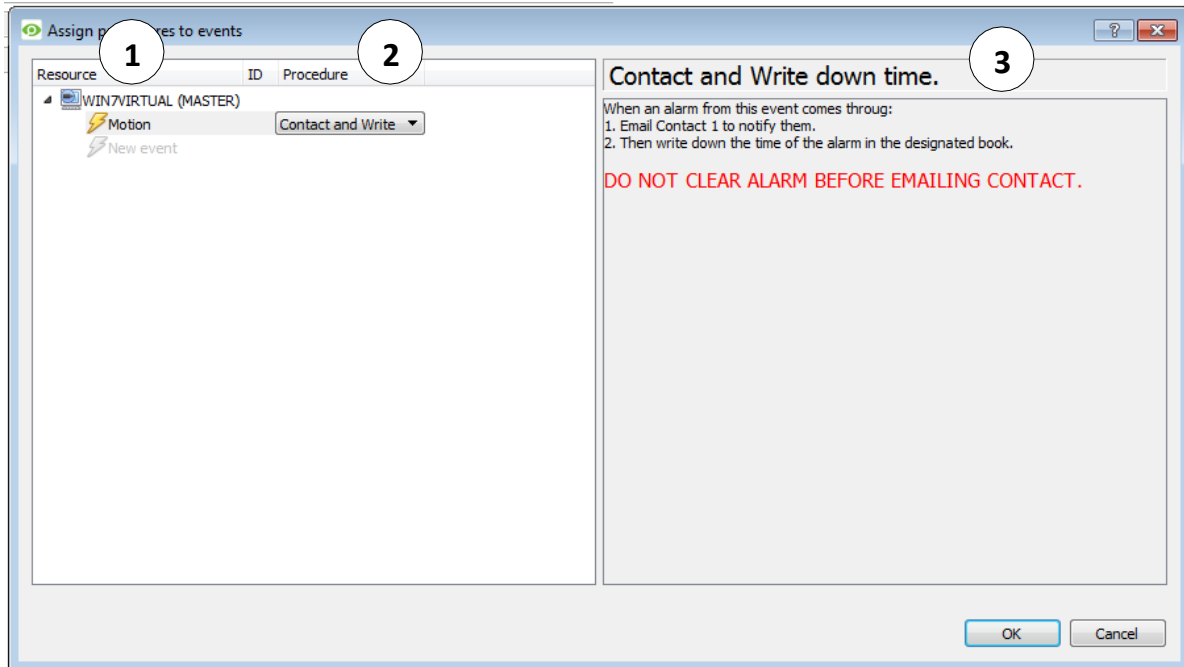
Use the test-editing tools to emphasise instructions.

Click **OK** when done.

### 4.5.2 Assign Procedures to Events

To ensure that procedures are displayed when an event alarm comes through, the procedure must be assigned to the correct event.

**Note:** events must already be configured.

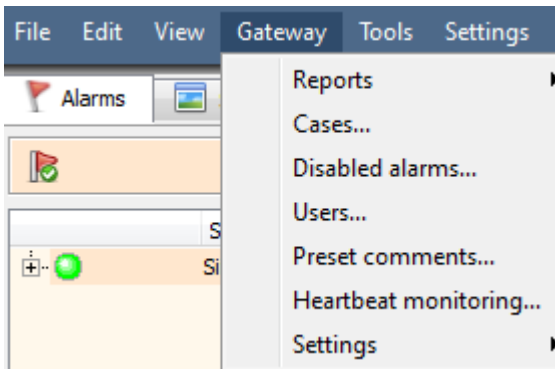


<b>1</b>	Resource List	Under the relevant server name, select the required event. <b>Note:</b> Events must already be configured or this list will be empty.
<b>2</b>	Procedures List	Select the required procedure for the event from the drop-down menu. <b>Note:</b> Procedures must already be configured or this menu will be empty.
<b>3</b>	Procedure Description	This is the title and description of the selected procedure. This is what the operator will see when the event alarm comes through.

Click **OK** when done.

## 5. Gateway Menu Settings

When a Gateway is running, the Gateway Menu will appear in the menu bar:



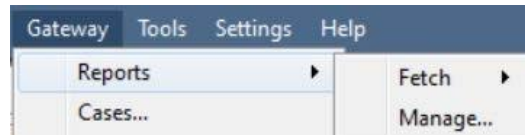
This section goes through the different settings available in this menu. See the next section for information pertaining to the Gateway Tab and its operation.

### 5.1 Reports

Under **Reports** there are two options: **Fetch** and **Manage**.

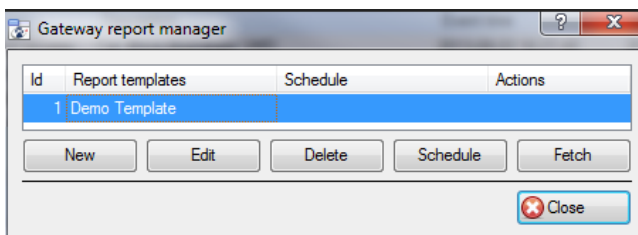
**Fetch** pulls up a pre-defined report.

**Manage** takes the user to the report management window, which is dealt with below.



#### 5.1.1 Manage (Gateway Report Management)

Clicking on **Manage** (above) will bring up the Gateway Report Manager window. It is here that the user will create/maintain the reports.



To create/edit a report click on **New/Edit** respectively.

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

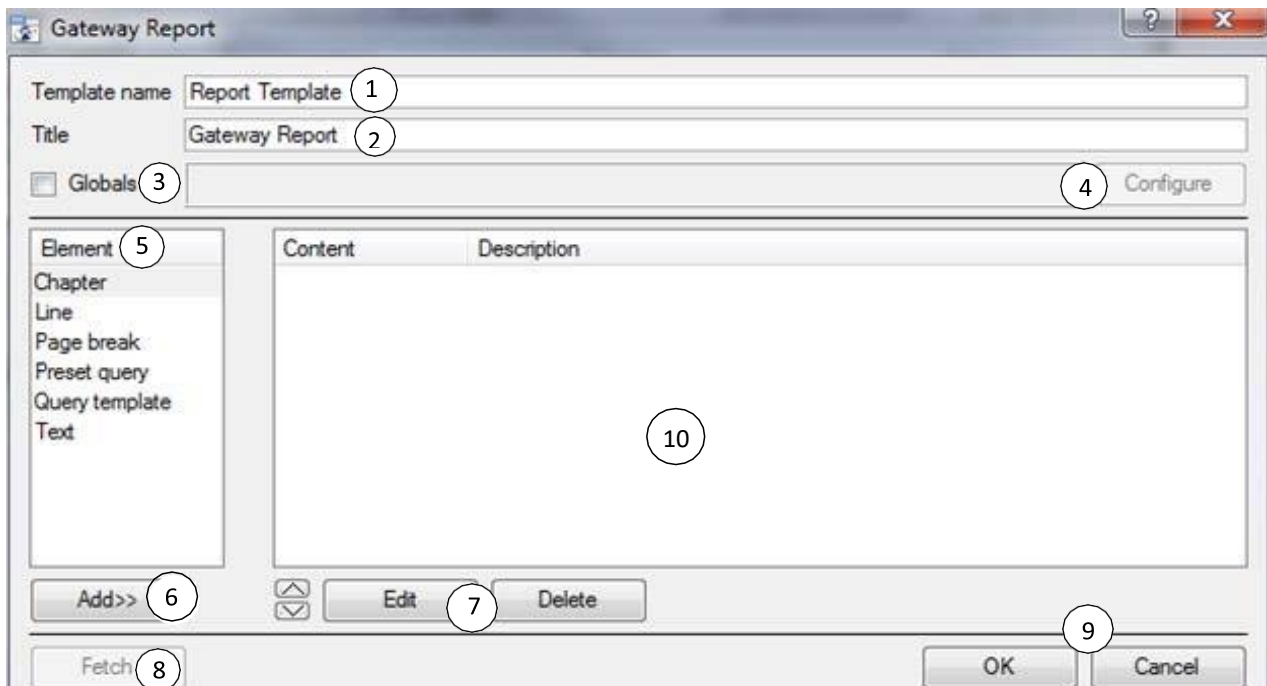
**Fetch** will pull up the selected report.

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




## 5.1.2 Gateway Report Setup Window

Click **New** or **Edit** to create a new Gateway Report. This will bring up the Gateway Report setup window:



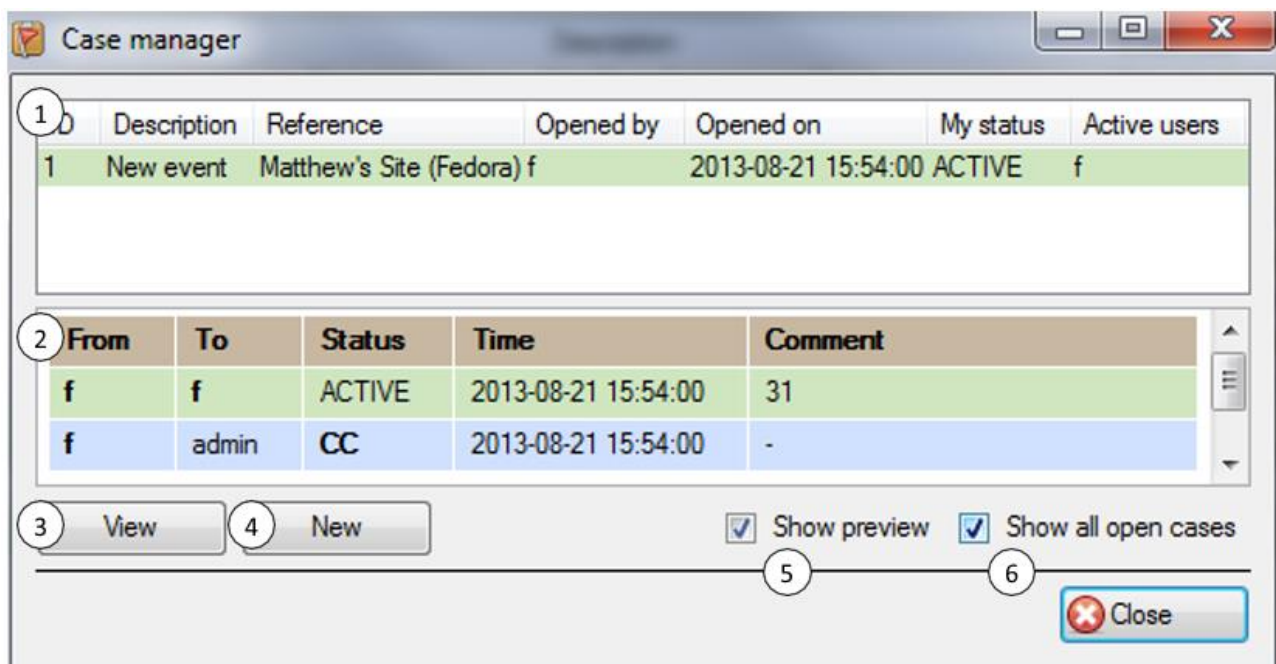
Gateway reports enable the analysis of control room operator responses, and general control room performance.

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>Fetch Report</i> .
3	Globals	There are three parameters that may be defined under Globals. These are the: <ul style="list-style-type: none"> <li>• Time Range that for the report to span.</li> <li>• The Sites to include in the report.</li> <li>• The specific units to be included in the report.</li> </ul>
4	Configure	Clicking on configure will allow the user to define the Globals' settings
5	Element	<p>The elements are the building blocks of the report. The user adds them in the order that they will appear in the report.</p> <p>To add an element, select it and click on <b>Add</b>.</p> <p><b>Note:</b> the Query Template option is there for users who want custom report setups. If a user wishes to generate a report using information that cannot be found in the present comments, the user will need to contact <a href="mailto:support@cat.co.za">support@cat.co.za</a> and request a report with the information that is required. Unless the user has done this, there will be no Query Templates present.</p>

6	Add	Selecting an element and clicking on Add will add it to the report contents window (10).
7	Edit/Delete	If the user has selected an element in the report contents window, it may be edited/deleted by using one of these buttons.
8	Fetch	This will fetch the report that has been compiled.
9	OK/Cancel	OK will save the changes that have been made. Cancel will delete them.
10	Report Contents Window	This is the window in which all added elements reside. <b>Note:</b> the order that the elements are added here will be reflected verbatim in the output of the report. If the user wants to add text at the beginning of the report, then the user should add Text First, or use the buttons to move elements up and down the list. 

## 5.2 Cases

In the Gateway Menu of the menu bar, click on **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 the user to create a new case.
5	Show Preview	Will enable/disable the case preview.
6	Show all Open Cases	If the user is at the Admin access level, an option will display: <b>Show all open cases.</b> De-select this option to see only those cases to which the user has personally been assigned. Users at all other levels will not see this option – they will see a list of only those cases to which the personally have been assigned.

### 5.3 Disabled Alarms

In the Gateway Menu of the menu bar, click on **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 and click **Clear**, to re-enable it.

### 5.4 Users

In the Gateway Menu of the menu bar, click on **Users...**

Name	Level	E-mail
admin	Administrator	
Demo User	Level 2	
f	Administrator	matthewb@cat.co.za

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**.

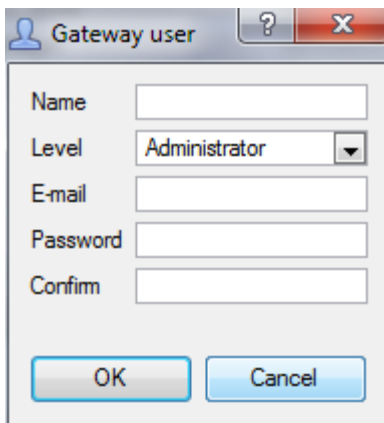
**Note:** It is important to remember that the **Gateway has its own user list, which is separate to the user list of the sites.** An operator will need login details for the Gateway, as well as login details for each site for which alarms are being handled.

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 gateway solutions, there is advantage to allocating *particular* alarms to *particular* operators. For instance:

- 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. Allocating 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 this operator response 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 this respondent?”

### 5.4.1 Create/Edit a User

#### Gateway Menu / Users... / New/edit



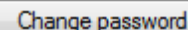
Enter a descriptive **name** for the user being created.

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

Set the **email 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**.



## 5.4.2 Manage User Levels

Gateway Menu / Users... / Manage levels / Select user level and click **Edit**.

In the Setup, it is possible to define “User levels” of access to the gateway 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 Gateway interface. For example, 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:

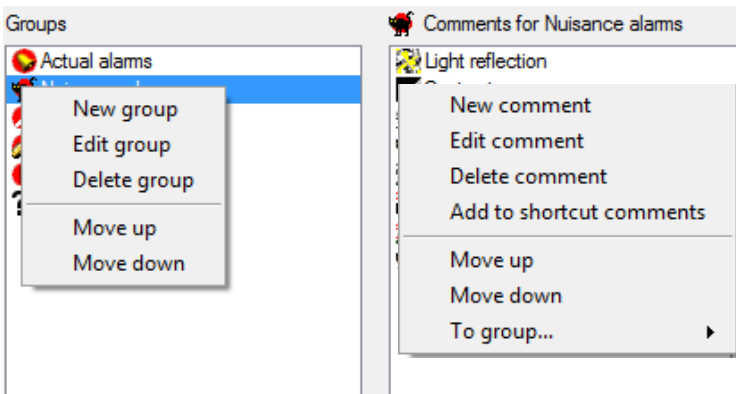
**File Menu / Enterprise Manager / Right-click on the Site / Properties / Access Tab / Set the Level.**

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

<b>View all current sessions</b>	Can view the CURRENT sessions table in the alarm gateway interface for all Logins.
<b>View alarm history</b>	Can view the History-Alarms table in the alarm gateway interface.
<b>View session history</b>	Can view the History-Sessions table in the alarm gateway interface.
<b>View login history</b>	Will allow the user to view all user logins.
<b>View case history</b>	Will allow the user to view all historic cases.
<b>Disable specific alarms</b>	Will allow the user to disable only individual alarm events.
<b>Disable alarms for a server</b>	Will allow the user to disable all alarm events for a server.
<b>Disable alarms for a site</b>	Will allow the user to view all alarm events for all servers on a site.

## 5.5 Preset Comments

In the Gateway Menu of the menu bar, click **Preset comments...**

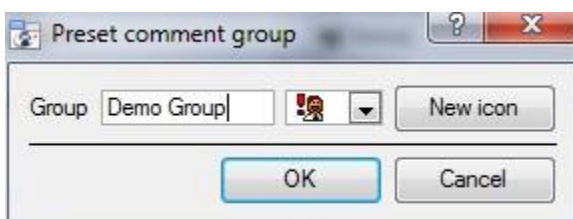


When handling an alarm, a user is required to add a comment before it can be closed.

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 group's comments on the right.

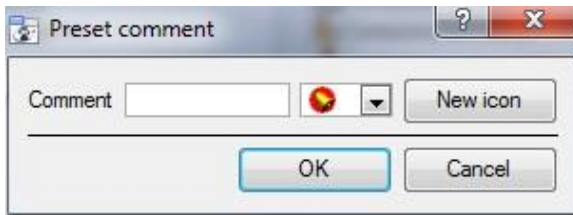
### 5.5.1 Add/Edit a Comment Group



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

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

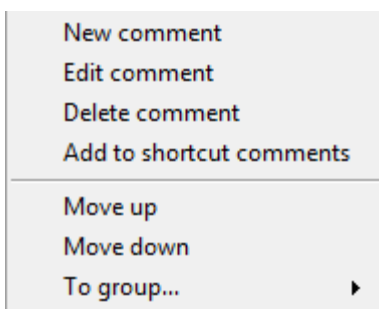
## 5.5.2 Add/Edit Comments



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 an icon, or add a new one.

## 5.5.3 Add Comments to Shortcut, and Group



Right-clicking on an existing comment will bring up the option to add a comment to the **Shortcut Comments**.

(Shortcut comments are used when the user right-clicks on an alarm in the Incoming table, and selects “Handle alarms with comment...”)

The user 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.

## 5.6 Heartbeat Monitoring

In the Gateway Menu of the menu bar, click **Heartbeat monitoring...**

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

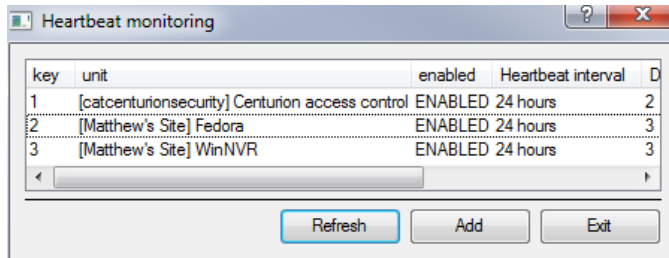
A missing heartbeat will trigger an alarm, which may be sent to the Gateway or forwarded to another Gateway.

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

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

## 5.6.1 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:



1. Click on Add. This will bring up a new window.

2. Select the relevant server/s from the drop-down menu. Click OK.

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

### Note:

1. The user will need to have already set up the server to send heartbeats to the gateway before following this step, because 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. It is advisable to start configuring the client side first, so that heartbeat alarms can create an entry for the site to be selected from the heartbeat monitoring Server setup side.

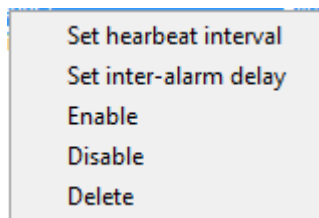
### 5.6.1.1 Heartbeat Monitoring Column Definitions

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 <b>no heartbeat for 3 hours</b> , 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. 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. It would get 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.  Thus, 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.

### 5.6.1.2 Right-click on a Server in the Heartbeat Monitoring List



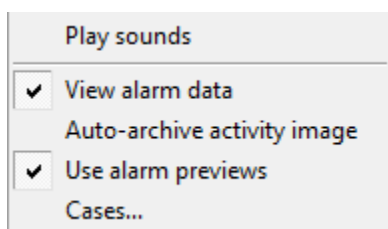
The **heartbeat interval** is the time period between which the gateway looks for new heartbeats. (Make this half the time of the periods between heartbeat transmissions from the recording server, to ensure reception.)

**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 it has been added, as it is not automatically enabled.

## 5.7 Settings

In the Gateway Menu of the menu bar, click on **Settings...**



### 5.7.1 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**.

---

## 5.7.2 View Alarm Data

This will show the user the video data that is attached to the alarm when the user handles it. If the user does not wish to see this video, un-tick the View alarm data option.

## 5.7.3 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 the user checks *Auto-archive activity image* this image will be automatically archived with the alarm, after it has been handled.

## 5.7.4 Use Alarm Previews

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

## 5.7.5 Cases

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

## 6. Conclusion

This app-note was designed to deal specifically with the setup of the Alarm Management Gateway. For further information about the CathesisVision software, please consult the main manual (<http://cathesisvideo.com>).

For support, please contact [support@cat.co.za](mailto:support@cat.co.za)