CheckMyCCTV™
Installation and User Guide

Issue 2.1

CheckMySystems

CONTENTS

INTRODUCTION

Thank you for installing CheckMyCCTV™, the automated Health, Status, and Operation monitoring application.

CheckMyCCTV™ diagnoses and reports issues from network connected CCTV systems.

CheckMyCCTV™ works by performing checks on the DVR and comparing the results against user defined thresholds. If the results fall outside of the threshold values, an alert is generated.

The status of all connected units can be viewed 'at-a-glance' and units with operation issues or fault conditions can be quickly identified. The 'core' checks include:

- Network Connection
- Camera failure status
- Time and Date Accuracy
- Recording Duration
- Disk Recording

CheckMyCCTV™ sends report emails to one or more email addresses when an alert condition is detected or cleared. These can be configured on an individual test basis.

SYSTEM REQUIREMENTS

The software is run in a Client/Server configuration, the Client being the front-end GUI (Graphic User Interface), and the Server being the service which runs the tests. These can be on the same or separate computers on the same network.

System requirements for the CheckMyCCTV™ Server or Client/Server running on the same computer:

- Microsoft Windows 7, 8, 10 or Server 2008 R2, 2012, 2016
- Dual Core Processor (Quad core recommended)
- 4GB of RAM (8GB Recommended)
- 100GB available Hard disk space (SSD Recommended)
- 1366x768 Screen resolution or higher (1920x1080 Recommended)

System requirements for Client Software *only*:

- Microsoft Windows 7, 8, 10 or Server 2008 R2, 2012, 2016
- Dual Core Processor (Quad core recommended)
- 4GB of RAM (8GB Recommended)
- 100GB available Hard disk space (SSD Recommended)
- 1366x768 Screen resolution or higher (1920x1080 Recommended)

RUNNING CHECKMYCCTV™

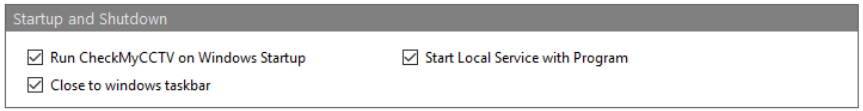
To run the software:

Locate the CheckMyCCTV™ folder in the Windows Start Menu. The default location is **All Programs > CheckMyCCTV** click on the CheckMyCCTV™ program.

Running the software will also start the CheckMyCCTV™ Service on your PC. The service runs in the background and continues running even if the main CheckMyCCTV™ application is subsequently closed.

The CheckMyCCTV™ service will take some computer resources and use bandwidth when it is running. The service can be stopped automatically when the software is closed

by clicking **File > Preferences** and then check the box labelled **Start Local Service with Program**:



Using the **Start Local Service with Program** option is not recommended if constant monitoring is required.

BEFORE USING CHECKMYCCTV™

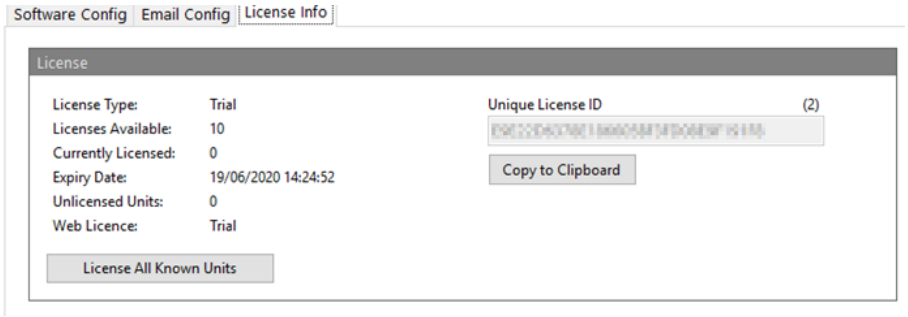
Before the software can be used, the correct license must be installed. The license is a file which is used to tell the software how many units can be monitored, and for what duration.

Installing the License Key

The first time the software is run, a license key is generated for the computer it is running on.

This license key needs to be activated for the software to operate. The CheckMySystems staff will assist with this:

1. Click on **Options > License Info** in the toolbar. The following page is displayed:



2. Copy the **Unique License ID** code and send it to **support@checkmysystems.com**

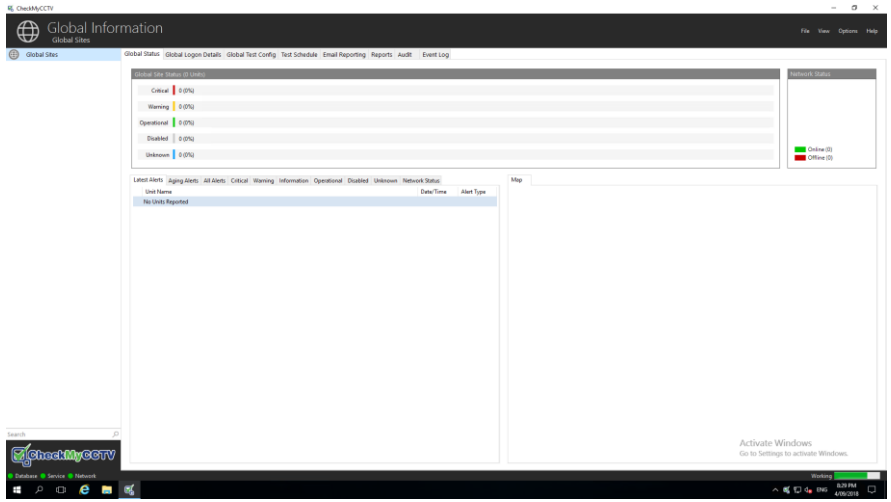
3. The License will be updated, and you will be sent a confirmation email

Once the License is updated, the software can be configured.

IMPORTANT: Not all tests described in this user guide are available for all devices. The Product Support Matrix document available on our website gives details of supported products and features.

CONFIGURING THE SITE TREE

Once the software has been installed, it will need to be configured for use. Double click on the CheckMyCCTV™ icon on the Desktop or from the Windows Start Menu. The initial screen is displayed as below:



There is an entry in the Site Tree for **Global Sites,** this is the root directory for the rest of the Customers, Sites, and Units.

Site Tree hierarchy

The site tree is used to easily organize Units into Customers and Sites, rather than having just a list of units. This allows units to be grouped together for easier configuration and improves performance.

The Site Tree hierarchy can be configured in the following ways:

Global Sites → Customer → Site → Unit
Global Sites → Customer → Unit
Global Sites → Site → Unit, or
Global Sites → Unit
A typical example of a site tree is as follows:

Customer folders can only be placed in the root of the site tree. Sites and Units can be added to a Customer, and Units can be added to a Site.

Adding Customers, Sites, and Units to the Site Tree

Customer folders, Site folders, and Units can be added manually using the **Add** function which can be found by using the right mouse button on the site tree. To add a Customer, Site, or Unit to the Site Tree:

1. Right click the required Customer, Site, or Unit selection. Go to “add” at the bottom of the menu and add the Customer, Site, or Unit.

2. Enter the corresponding IP/Address or Hostname if a Unit is being added, or the Site or Customer name and click **Add Unit** to add it to the site tree.

3. If a Unit is added, this will be placed into the root of the Site Tree. It will be displayed as a to indicate that the unit is not yet known. A Customer will be displayed as and a Site as .

TIP: It is possible to add Units directly into a Customer or Site folder rather than the Global folder by selecting the required folder before adding the Unit.

Once the Unit is added to the site tree the software will perform tests to identify what the unit is. Once these are complete the unit will display one of the following unit status icons in the site tree:

- The unit is in an unknown state, usually before it is detected.
- A valid unit has been detected but their HTTP (Video) password which is preventing the unit type from being detected.
- A valid unit has been discovered, but it has not yet been licensed for use.
- A unit has not been discovered or it is not a valid IP address, hostname, or port number.
- The unit has been discovered and is operational within the user defined settings.
- The unit has been discovered, but a ‘warning’ alert has been detected within the user defined settings.
- The unit has been discovered, but a ‘critical’ alert has been detected within the user defined settings.

Licensing Units for use

When a site tree is imported or a unit is added, CheckMyCCTV™ checks to see if the unit is valid or not. Once the check has taken place, the unit will display a key icon, which indicates a valid but unlicensed unit has been detected.

To license each unit individually:

Right Click on the unit icon and select **License Unit**. Once licensed, CheckMyCCTV™ will start its tests and remove a license from the License pool.

To license all units at once:

Click **Options > License Info** and click on **License All Known**.

All known units will be licensed immediately, and CheckMyCCTV™ will start to check each unit in turn.

IMPORTANT: Once a license has been assigned to a unit, it cannot be unassigned. Ensure that only the units that you want to license are in the site tree if you are using the **License All Known** option. If a unit is in the tree that you do not wish to license, **disable** it before using the **License All Known** option.

Note: The initial test of each unit may take several minutes as CheckMyCCTV™ is collecting unit information and creating a backup before conducting tests.

Setting the Unit map location

CheckMyCCTV™ has map integration built in, it is possible to view the geographic location of units on an interactive map, which will display the status of each unit indicated by a colour coded 'pin'.

To set the unit map location:

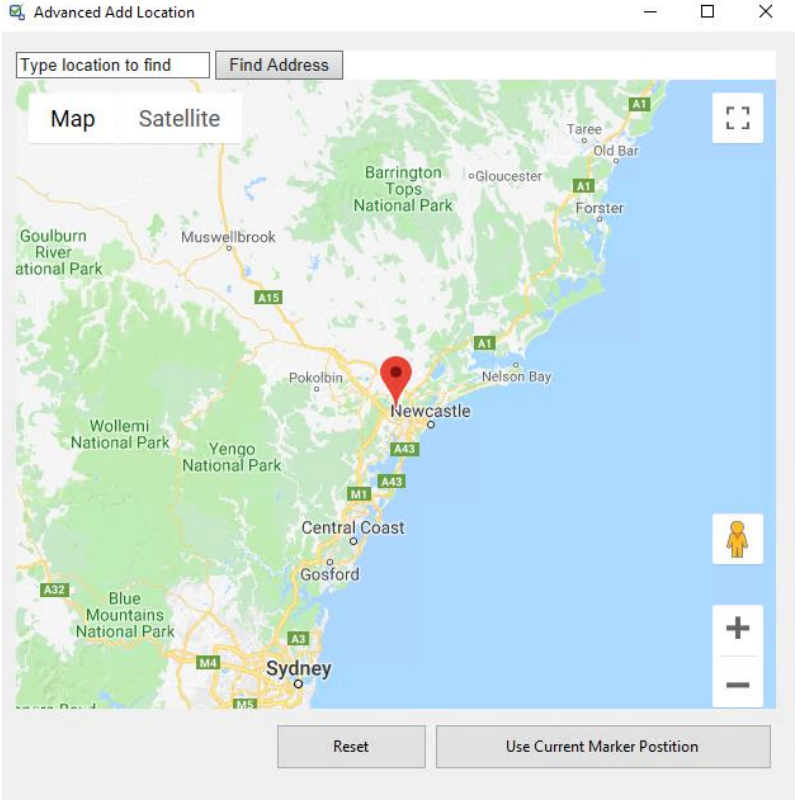
Click on the unit you wish to set in the Site Tree.

Select **Unit Summary** from the tabs at the top of the page.

Scroll down to the bottom of the page to Unit Map Location:

Click **Set Location** and a pop-up map will be displayed. To set a map position:

1) Enter a postcode or address in the 'Type location to find' box and click Find Address.
2) Click and hold the red marker and drag it to the desired location, it may be necessary to zoom into the map to achieve greater accuracy.



3) Once the desired location has been selected, Click **Use Current Marker Position.**
4) The map window will close, and the coordinates will be saved for that unit.

Managing Customers, Sites, and Units in the Site Tree.

Once Customers, Sites, and Units have been added to the site tree, it is possible to manage them:

MOVING A SITE OR UNIT

To move a Site or Unit to another location, **drag and drop** the item onto the Global Sites  , Customer  , or Site  where you wish to move the item. The software will ask for confirmation before it is moved.

RENAMING A CUSTOMER, SITE, OR UNIT

To rename a Customer, Site, or Unit, **right click** on the item and select Rename from the list. It will then be possible to change the name of the item. The software will ask for confirmation before it is renamed.

Note: Renaming a Unit will not change its IP address or hostname, only the displayed name.

DELETING A CUSTOMER, SITE, OR UNIT

To delete a Customer, Site, or Unit, **right click** on the item and select Delete from the list. It will then be possible to delete the item from the site tree. The software will ask for confirmation before it is deleted.

DISABLING AND ENABLING UNIT TESTING

It is possible to disable the testing on an individual unit from the site tree. **Right click** on the unit and select Disable Unit Testing. After a few seconds, the icon will be displayed next to the unit name. The unit will not be tested again until the Unit is re-enabled.

To re-enable testing, **right click** on the unit and select Enable Unit Testing. After a few seconds, the icon will change back to whatever was previously displayed and the tests will continue as per the test interval.

VIEWING THE UNIT SUMMARY

A quick way to display the Unit Summary page from the site tree is to **right click** on the unit and select View Unit Summary. The Unit Summary tab is then displayed in the right-hand window.

OPENING A UNIT IN A WEB BROWSER (OPTION)

A quick way to connect to the Unit using a web browser is to **right click** on the unit and select **Open Unit in Browser**. The default web browser will open and attempt to load the IP Address or Hostname of the Unit.

Note: Some units may not have access to an interface through a web browser.

EXPANDING AND COLLAPSING THE SITE TREE

The site tree can be expanded, showing every unit in each customer or site folder, or collapsed to display the sites and customers in the root. To expand or collapse the site tree, **right click** on the Global Sites icon  and select **Expand All** or **Collapse All**.

SHOWING/HIDING THE ALARM SET STATUS

The current alarm set status can be indicated by an icon next to each unit, site, or customer folder in the site tree, see **Alarm Set Status** on page 18 for more information. It is possible to display or hide these indicators; **right click** on the Global Sites icon  and select **Show Alarm Set Status** or **Hide Alarm Set Status**.

CONFIGURING THE SERVICE

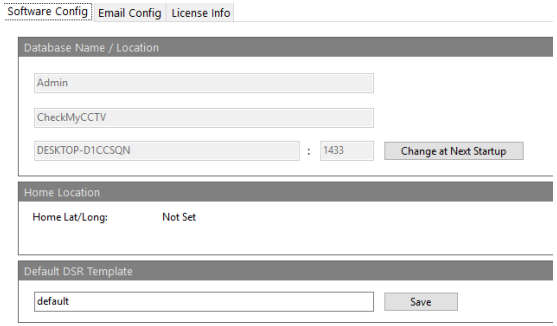
The service has default settings which allow it to operate as soon as it is installed. However, there are some additional options which can be configured to the users' requirements.

To configure the service:

1. Click the **Options** item in the toolbar.
2. Select **Software Config, Email Config**, or **Licence Config**.

The selected configuration screen is displayed as below:

Software Configuration Tab



DATABASE LOCATION

Select the location of the database on the network. By default, the database location is on the local PC, indicated as a '.' (full stop or period).

If the database is on another computer or server, then the network address will need to be entered here. For example, **//server** or the IP address of the database.

CAMERA TAMPER IMAGE PATH

If the Camera Tamper function is used, the service must be configured to store the snapshot images in a directory.

By default, the images are stored in the 'Images' directory of the installation path, usually **C:\Program Files\CheckMyCCTV\Images**. However, if the software is going to be used on multiple computers, the snapshot images may need to be stored on a network or shared device so other operators can view them.

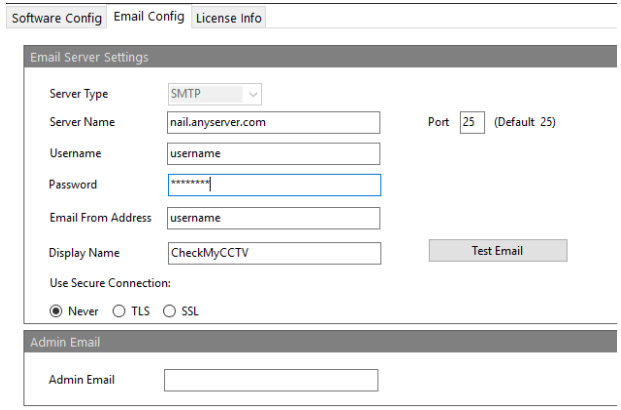
To do this, **browse** to a directory that the images are going to be saved to and click **Save**.

HOME LOCATION

The Home Location of the service or a company premises can be set here. This will allow your home location to be displayed in the map if that option is selected.

To set your Home Location, follow the 'Setting the Unit map location' instructions which can be found on page 8 of this manual.

Email Configuration Tab



EMAIL SERVER SETTINGS

Enter the details of the Email Server you wish to use to send emails. Contact your network administrator for details of the settings you must use.

Server Type: Currently set to SMTP only.

Server Name: Enter the address of the Server, such as *smtp.mailserver.com*

Username: Enter the Username used to connect to the email server.

Password: Enter the Password used to connect to the email server.

Use Secure Connection: Select the appropriate secure connection method for your email server.

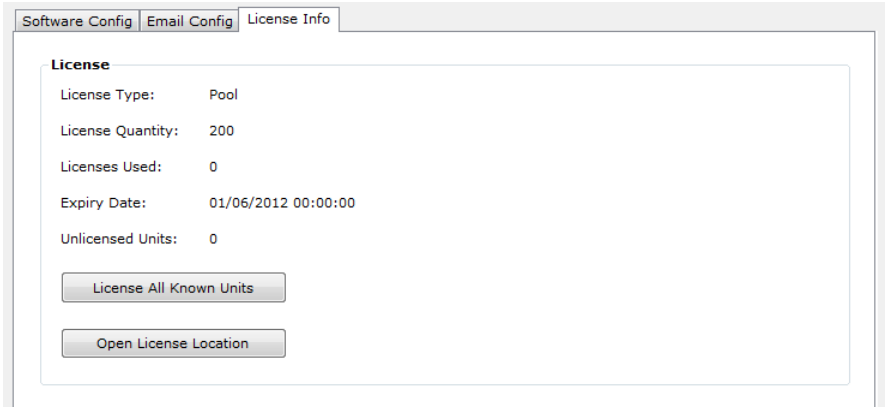
Port: Select the port number that your email server uses, the default is port 25, Google Mail (Gmail) uses port 465.

To test the email settings first click **Save Changes** and then the **Test Email** button, enter an email address where you want the test email to be sent to in the pop-up box.

If a local mail server is not available, it is possible to use a Google Mail (Gmail) account by first registering at www.gmail.com and using the following settings:

Server Type: **SMTP**
Server Name: **smtp.gmail.com**
Username: **[username]@gmail.com**
Password: **[password]**
Port: **465**
Use Secure Connection: **SSL**

License Info Tab



The **License Info** tab displays the current licensing information for CheckMyCCTV™. There are 3 different license types:

Trial – Trial license for software evaluation.
Individual – Licenses for individual units.
Pool – A pool of licenses which are used to license the units.

The page also shows how many licenses are available, how many have been used, their expiry date, and the number on unlicensed units in the software.

To license all the units on system in one go, click on the **License All Known Units** button.

IMPORTANT: Ensure that only required units are in the site tree, as it is not possible to unlicense units once they have been licensed.

When a site tree is imported or a unit is added, CheckMyCCTV™ checks to see if the unit is valid or not. Once the check has taken place, the unit will display an icon, which indicates a valid but unlicensed unit has been detected.

To license each unit individually:

Right Click on the unit icon and select **License Unit**. Once licensed, CheckMyCCTV™ will start its tests and remove a license from the License pool.

To license all units at once:

Click **Options > License Info** and click on **License All Known**.

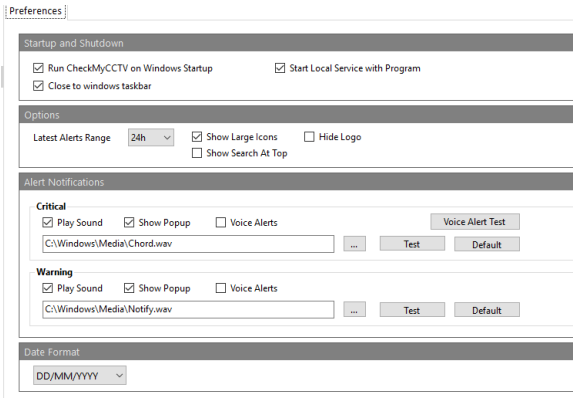
All known units will be licensed immediately, and CheckMyCCTV™ will start to check each unit in turn.

IMPORTANT: Once a license has been assigned to a unit, it cannot be unassigned. Ensure that only the units that you want to license are in the site tree if you are using the License All Known option. If a unit is in the tree that you do not wish to license, disable it before using the License All Known option.

Note: The initial test of each unit may take several minutes as CheckMyCCTV™ is collecting unit information and creating a backup before conducting tests.

CONFIGURING THE LOCAL SOFTWARE

To configure the software for the local user, click **File > Preferences** to display the following screen:



STARTUP AND SHUTDOWN

Select whether the software will run when Windows starts up, and whether the software will be sent to the task bar when it is closed, rather than shut down completely.

Run CheckMyCCTV™ on Windows Startup – Select this option to ensure that CheckMyCCTV™ runs when Windows is started.

Close to Windows taskbar – This minimises CheckMyCCTV™ to the taskbar, rather than closing the program completely. (Currently in development)

Start Local Service with Program – Select this option to only perform the CheckMyCCTV™ checking when the software is running.

This only applies to users who have the CheckMyCCTV™ Service running on the same PC as the CheckMyCCTV™ program. If the service is running on another PC, then it cannot be started or stopped from a remote PC.

ALERT NOTIFICATIONS

The software can generate a visual or audible alert depending on whether it is a Warning or Critical Alert. Use the check boxes to select whether a visual (pop-up) alert or audible alert is generated.

The Audible alerts can be user selected **WAV** audio files, click the  icon and browse to the file you wish to use.

The selected audio file can be tested by clicking the **Test** button. The audio files can be reset back to default by clicking the **Default** button.

CONFIGURING THE TESTS

The tests for each unit use the Global settings by default when they are first added into the software. It is useful to change the Global settings to a standard template to make it easier to configure Unit tests in the future.

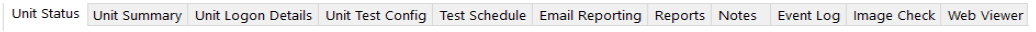
To change the **Global** Configuration settings:

1. Click on the Global Sites Icon  in the site tree.
2. The tabs on the right-hand side will change to **Global Status, Global Logon Details**, **Global Test Config** etc. All the tabs on this page will configure the Global settings of the software:

3. Select the required tab to display the configuration page.

To change the **Unit** Configuration settings:

1. Click on the Unit Icon in the site tree.
2. The tabs on the right-hand side will change to **Unit Status, Global Logon Details**, **Unit Test Config** etc. All the tabs on this page will configure the settings for that unit:

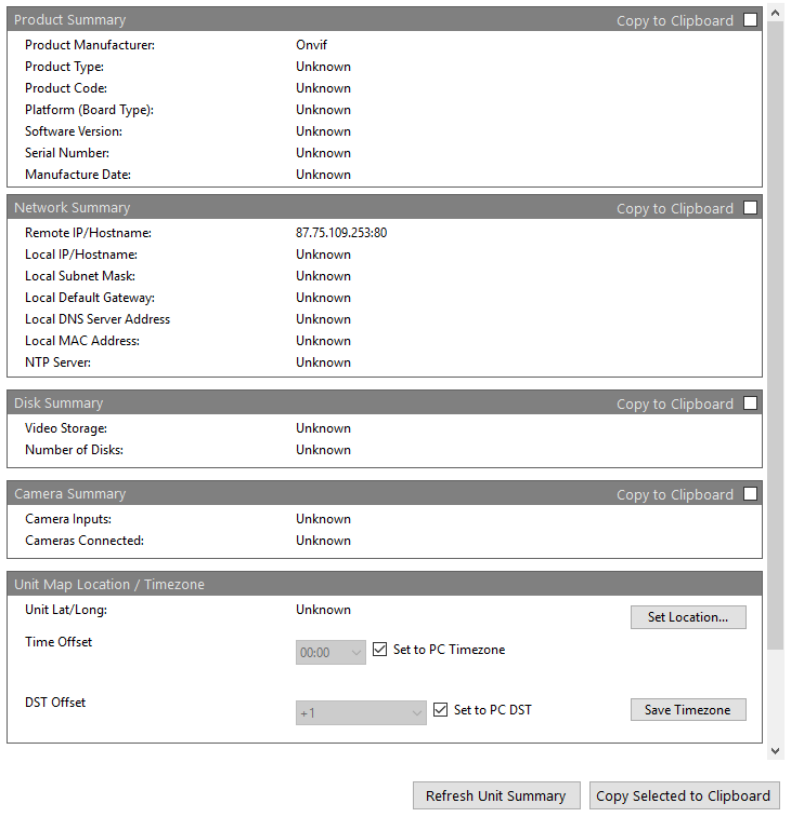


3. Select the required tab and change the configuration settings.

IMPORTANT: When the Global settings are adjusted, the settings may also adjust the individual Unit settings, if they are configured to use the Global configuration. See page 15 – Configuring the Tests for Individual or Global configuration for more details.

Unit Summary

The Unit Summary page gives details of the manufacturer, type of unit, software version, hard disk capacity etc. A typical example could be:



It is possible to copy information from each section to a clipboard, check the **Copy to Clipboard** box and then click the **Copy Selected to Clipboard** button. It is then possible to paste the information to a text document using Ctrl+V on your keyboard or right click and select Paste.

Changing the Logon Details and Port numbers

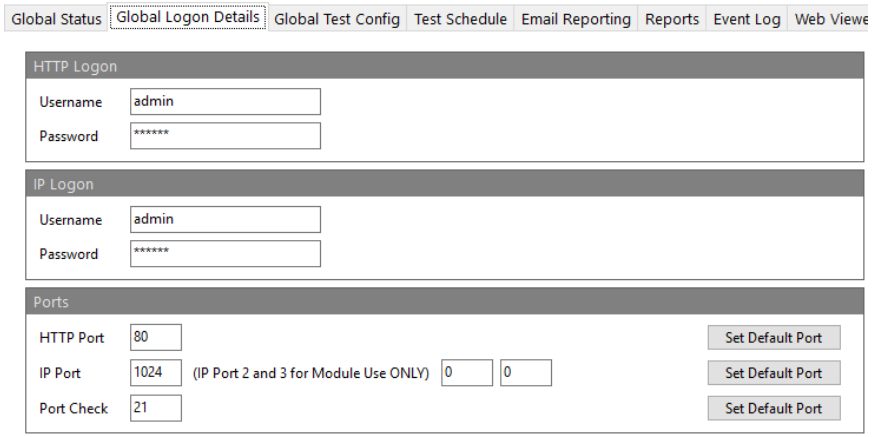
CheckMyCCTV™ needs to have a valid username and password for HTTP, Telnet, and FTP to be able to conduct all the tests on a unit. It is also necessary to allow access to the Unit by entering the correct port number if it is not using the default ports (80 for HTTP, 21 for FTP, and 23 for Telnet).

If the correct passwords have not been set, then a padlock icon is displayed as the Unit Icon. This indicates that a unit has been found but the password is not correct.

If the port number is not correct, then the icon is displayed as it will not be detected.

To change the logon details or port numbers:

1. Click on the Global Icon or Unit Icon in the site tree.
2. Click on the **Logon Details** tab on the right-hand side. The following screen is displayed:



3. Uncheck the **Use Global Config** box to allow details to be entered for the unit.

   Note: The Use Global Config box does not appear if it is the Global Logon Details that are being adjusted.

4. Enter the Username and Password details for HTTP, FTP, and Telnet.

5. Enter the relevant port number for HTTP, FTP, and Telnet. Click on **Set Default Port** to revert to the default setting.

6. Click on **Save Changes** to store the new details.

7. The software will to logon using the new details.

TIP: If the unit is not being detected, right click on the  icon for the unit and select **Open Unit in Browser,** if the web page of the Unit does not open, then it is possible that the wrong IP Address/Hostname or port number is being used.

IMPORTANT: For Dedicated Micros products, the HTTP Username and Password is for a **Video Account**, not for web page configuration.

Changing the Test Configurations.

The **Test Config** tab is where the core tests are configured, each of the tests are grouped into three Categories; Network Tests, Disk Tests, and Performance Tests. These use the Global Test Config settings by default unless the **Use Global Settings** box is unchecked.

Each test has all or some of following options which can be adjusted:

TEST INTERVAL – This is the duration between each test taking place. This can be a timed interval such as every 10 minutes, or a Manual test taking place when the operator instigates it, or a Daily test which starts the test at a user defined scheduled time.

ALERT THRESHOLD – This is the threshold that the test must cross before an alert is generated. These can be the number of times the test fails, such as 2x or 3x, a time duration, such as 5m, 1h, or 30d, or a threshold figure such as 50°C, or 128Kb/s.

Note: There is a 60 second wait between each retest attempts. So, if the HTTP test is configured with a 3x Alert Threshold, the HTTP test would have to fail three times over a 3-minute period before an alert is generated.

ALERT LEVEL – This is the severity of the alert. There are two states:

 Critical Alert.

 Warning Alert.

EMAIL – Check the Email box if an email is to be sent for this alert. See the Email Settings section on page 10 for more details on how to configure the software to send emails.

Configuring the Tests for Individual or Global configuration

The tests can be configured to use Global or Unit configurations, by default, the tests are using the Global Configuration. To change the type of configuration for each test, click the checkbox to select whether individual or global tests are performed:

 - Test disabled.

 - Use Global Configuration setting.

 - Use Unit Configuration setting.

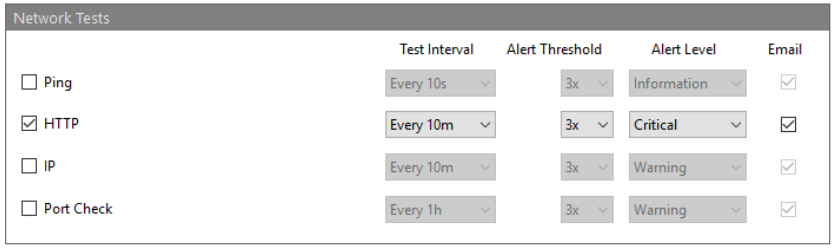
Note: When the Global Test Config page is being configured, only the Test Disabled checkbox  and Unit Configuration checkbox  are available.

Click on **Save Changes** save the options on the page.

The Test Config page is broken down into 4 sections; Network Tests, Disk Tests, Maintenance Tests, and Performance Tests:

Configuring the Network Tests.

The Network Tests section is used to conduct connection type tests to the unit. These tests will vary depending on the unit, but the HTTP (web) test is the most important to ensure the unit is working.



PING

The Ping test is a method used to test whether a device is reachable across an Internet Protocol (IP) network. It measures the 'round trip' time for packets to be sent from the computer to the destination device.

The advantage of using Ping is that is has a very low processor overhead and uses a tiny amount of bandwidth to check that a device is available, so it can have a lower Test Interval than other methods. However, ping packets are often blocked by routers over Internet connections, so it may only be possible to use Ping on devices connected to the local network.

HTTP

The HTTP test checks that a valid unit is present on the network connection. This uses the selected port number to test against. This uses a slightly higher network overhead than ping, so it is not recommended that it is performed as often.

SECONDARY IP

The HTTP test incorporates a Secondary IP check. This check is invoked once the primary HTTP check has failed. The purpose of the Secondary IP check is to see if there is still connection to the site, but not to the unit.

The Secondary IP address should be set as another IP device on the **same** network which has a Web Server, for example another DVR, a Router, or other network attached product.

CheckMyCCTV™ repeatedly checks network connectivity to the CCTV system and reports any issues. The available combinations of Primary and Secondary HTTP tests:

The Primary address passes – No alert indication.

The Primary address fails, and the Secondary address passes – Possible issue with the CCTV System.

The Primary address fails, and the Secondary address fails - Possible issue with the network connection to the site.

Typical issues if both the Primary and Secondary addresses fail could be:

1. Loss of broadband/network connection.
2. A change to the router/firewall configuration.
3. Loss of power on the site.
4. A problem with the network connection on the site.

IP

This is a connection to a unit which does not use HTTP for testing purposes.

FTP

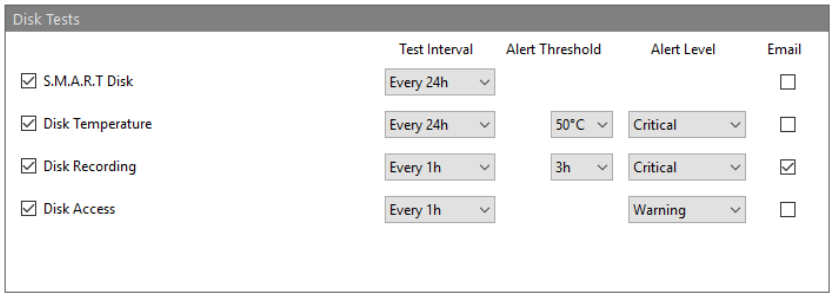
The FTP (File Transfer Protocol) test checks that a unit is able to make FTP connections, some models require this to be able to download footage or upload software.

TELNET

The Telnet test checks that a unit is able to make Telnet connections, some DVRs require Telnet to be available to send alarm responses to a central station.

Configuring the Disk Tests.

Disk tests are used to ensure that the disks attached internally or externally to the DVR are operating correctly and



S.M.A.R.T DISK

Some models allow information to be gathered directly from the hard disk to determine its health using S.M.A.R.T (Self-Monitoring, Analysis, and Reporting Technology). The disk performs its own tests and reports when a test threshold has been exceeded.

DISK TEMPERATURE

When used by CheckMyCCTV™, it can determine if a drive is running at a temperature which may indicate cooling or fan issues. A default value of greater than 50ºC is used to determine a critical issue.

DISK RECORDING

This test ensures that the hard disk is actually recording by checking that images are being recorded to the disk. The default threshold limit is 10 minutes, so if the unit has not been recording in the previous 5 minutes, then an alert will trigger. If the DVR is set up to record only activity or alarms, then this threshold limit will need to be increased in case there is no movement for greater than 10 minutes.

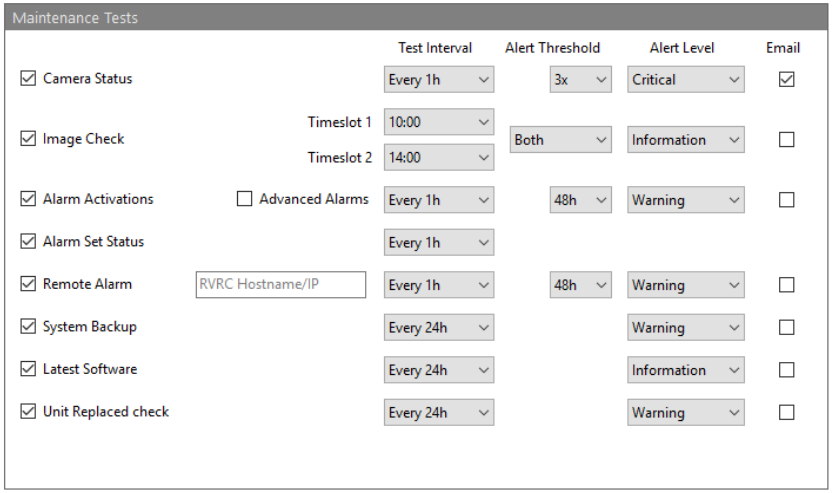
Note: This is a global test, so it is checking that images are being recorded on the system, not from a specific camera.

DISK ACCESS

This test ensures that all connected hard disks can be accessed by the software. This will alert if any drive is no longer accessible, which could indicate a faulty drive or connection problems on external drives.

Configuring the Maintenance Tests

The Maintenance Tests section contains tests that ensure the correct maintenance and operation of the unit.



CAMERA STATUS

The Camera Status test is a check to see firstly which cameras are connected, and secondly to check to see if any of those cameras have failed. This is an important test because if cameras have failed then the security system is severely compromised.

The results can be seen on the camera status bar indicating each camera status using a colour coded icon as below:

Grey – Camera 1 input is not used (disconnected in the DVR settings).

Green – Camera 1 is Operational.

Yellow – Camera 1 is in a Camera Tamper condition.

Red – Camera 1 is in a Failure condition.

Note: It is possible that camera inputs which have no cameras connected are reported as failed cameras. Ensure that these cameras are set to 'Disconnected' in the DVR menus to prevent this from happening.

CAMERA TAMPER

The camera tamper test takes a snapshot image from each camera once or twice every day. The image contents are analysed and compared against the previous days' images and a Camera Tamper alert condition is raised if the images differ by greater than the user defined threshold.

There are two timeslots for image snapshots to be taken. It is recommended that one timeslot is during the day and one is during the night to ensure that there is a contrast between the images to improve tamper detection reliability.

The Alert Threshold can be set to trigger an alert condition for Timeslot 1, Timeslot 2, Either, or Both:

Timeslot 1 – Camera Tamper alerts are only generated for Timeslot 1 images, Timeslot 2 images do not generate alerts, regardless of the changes in the image.

Timeslot 2 – Camera Tamper alerts are only generated for Timeslot 2 images, Timeslot 1 images do not generate alerts, regardless of the changes in the image.

Either – Camera Tamper alerts are only generated for Timeslot 1 *or* Timeslot 2 image.

Both - Camera Tamper alerts are only generated when both Timeslot 1 *and* Timeslot 2 images differ by greater than the user defined threshold. This is the default setting as it provides an effective 'double knock' solution.

More information of how to set-up and configure the Camera Tamper function can be found on page 23 - Configuring Camera Tamper settings.

ALARM ACTIVATIONS

The Alarm Activations test is used to make sure that alarms are being activated on the unit over a user defined period, such as the last 24 hours. This is used to ensure that alarm connections have not been disconnected or the settings tampered with. If it is expected that alarms would be generated over a certain period, then this function ensures that they are.

ALARM SET STATUS

Alarm Set Status is used to check whether the alarm system is in a SET (Armed) or Unset (Disarmed) state. This can be used to see if the system is being Set and Unset correctly.

Being in the wrong Alarm Set state will compromise the security system as it is often when the system is Set when alarms and remote connections are activated.

The Alarm Set Status is displayed next to the unit status icon in the Site Tree, for example:

In the example above, the unit called Test Unit is currently Unset, as indicated by the green dot next to the unit name. To show or hide the Alarm Set Status icon in the Site Tree, right click on **Global Sites** and select **Show/Hide Alarm Set Status**.

The available Set Status icons are:

- System Set Status is Unknown (cannot be detected or not available)
- System is Unset/Disarmed
- System is Set/Armed

TIP: The green and red icons are displayed against a Site or Customer folder if all the containing units are either set or unset. If a Site or Customer folder displays a grey dot, then there is a mix of set and unset units in that folder.

Note: This test is currently for indication only, no alert conditions can be configured.

REMOTE ALARM CONNECTION

The Remote Alarm Connection test checks that the unit has connected to a remote central station whilst in an alarm condition over a user defined period, such as the last 48 hours.

The Remote Alarm Connection test comprises of three tests:

Unit RVRC Reporting check – Checks that remote reporting is enabled on the unit.

Unit RVRC Host check – Checks that the hostname/IP address of the RVRC is the same as that configured in the unit.

RVRC Alarm connection – Checks that an alarm connection has been made to the RVRC in a user defined time period.

If any of these three checks fail, then the Remote Alarm Connection test will fail.

Note: The RVRC Host check can be disabled by leaving the **RVRC Hostname/IP** box blank.

SYSTEM BACKUP

CheckMyCCTV™ will take a backup at a user defined time period. If a backup cannot be found during that period, then an alert is triggered. The backup files can be found in the Backups folder of the CheckMyCCTV™ installation folder, C:\Program Files\CheckMyCCTV\Backups\[IP Address]

There is a Reference backup file, which is the backup taken when the unit is first imported, and the last 90 days of backups.

LATEST SOFTWARE

CheckMyCCTV™ will check that the currently installed software on the DVR is the latest up to date version. An alert condition is triggered if the currently installed software is not up to date.

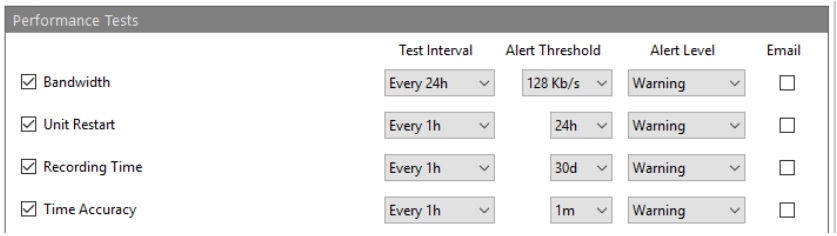
Note: By default, an 'Information' alert condition is generated if the software is out of date, this would need to be changed to a Warning or Critical condition if a visual indication is required.

DVR REPLACED

The DVR Replaced Check is to ensure warn the user that the current DVR is not the same as first detected by the software. This alert can be used by the operator to warn that the installed unit may not be configured in the same way as the previous one.

It is important that if a unit is replaced, the alarm and central station settings are updated. If the unit has been replaced with the exact same model, then use the backup file to restore the settings to the unit.

Configuring the Performance Tests.



BANDWIDTH

This test downloads data from the DVR and calculates the real-world download bandwidth available from the DVR to the test computer. There is a default threshold limit of 128Kb/s, if the bandwidth drops below this limit then an alert is triggered.

UNIT RESTART

This test determines the last time a unit has been restarted, and on some models the reason why the unit was restarted is given. The default alert threshold is one day, meaning that if the unit has restarted in the last day, then an alert is triggered.

RECORDING TIME

This test determines the length of time the DVR is recording for. This is the actual record time rather than what was configured on the DVR, so it takes into account any alarm activations and any movement recording in conditional refresh recordings such as MPEG4 and H.264. The default alert threshold setting is 30 days. If the unit does not achieve 30 days, then an alert is generated.

Note: If the DVR has been running for less time than the alert threshold has been set for, no alert will be generated.

TIME ACCURACY

This test checks the DVR time against the clock setting on the PC running the CheckMyCCTV™ service. If the difference in time is greater than the alert threshold, then an alert is generated.

TIP: The time difference is displayed in seconds so if the result is around 3600 seconds fast or slow then check that it is configured for the correct time zone and that the unit's daylight-saving time (DST) settings are correct.

TEXT RECORDING

This test ensures that if an ASCII text feed is connected to the DVR, it is recording as expected. The default threshold limit is 24 hours, so if the unit has not been recording text in the previous 24 hours, then an alert will trigger.

Note: This is a global test, so it is checking that there is text recording on the system, not a specific camera.

CONFIGURING A TEST SCHEDULE

CheckMyCCTV™ is designed to run continuously, 24-hours a day. However, it can be configured to run only during specific times. A typical example would be for a central monitoring station to run the tests during non-peak times (i.e. during the day).

The above example shows that the tests are not performed between 18:00 hours and 08:00 hours and between 12:00 hours and 13:00 hours.

The Test Schedule can be configured on an individual Unit basis, or by using the Global Configuration.

Check the **Ping overrides the test schedule** box to ensure the Ping test runs continuously.

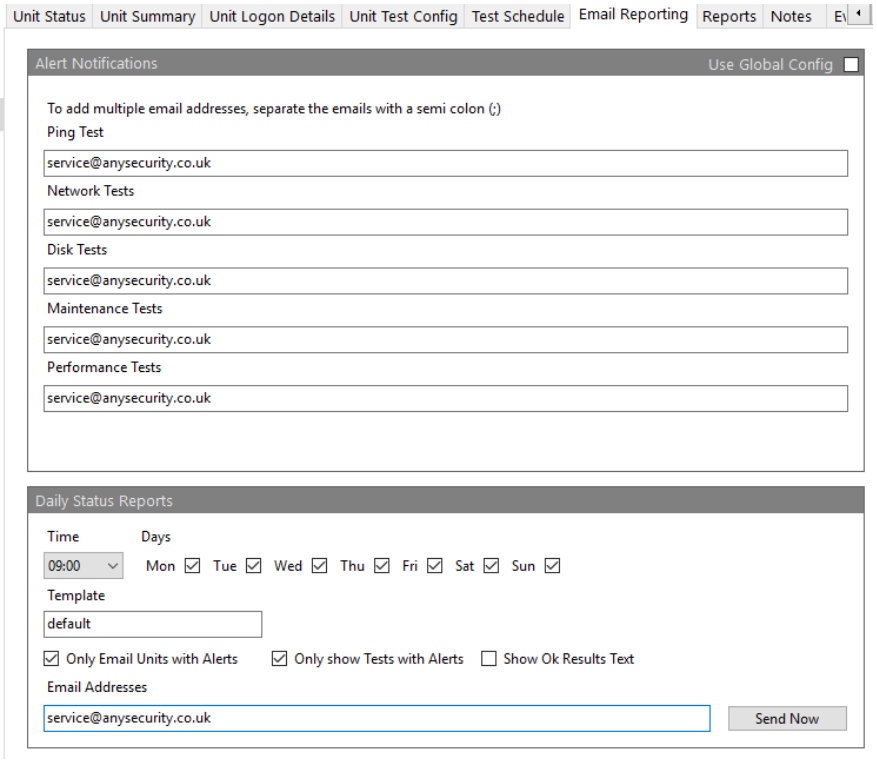
IMPORTANT: The schedule determines when the tests are NOT going to be performed.

CONFIGURING EMAIL REPORTING

CheckMyCCTV™ can send Alert Notifications and Daily Status Reports to user-defined addresses:

Alert Notifications – These are email notifications that an alert has been generated or cleared. Alert Notifications are sent immediately when an alert is generated.

Daily Status Reports – These are emails reporting the current status of a Customer, Site, or Unit. Daily Status Reports are 'snapshots' of the unit status the moment the report is generated.



ALERT NOTIFICATIONS

Alert Notification emails are grouped into four categories; Network Tests, Disk Tests, Maintenance Tests, and Performance Tests. Enter the email address any of the boxes, and separate using a semi-colon (;)

Email addresses can be configured on an individual Unit basis, or by using the Global Configuration.

DAILY STATUS REPORTS

Select the time that the report will be generated and sent, if multiple reports are generated at the same time, it may take some time to generate and send the report.

The **Only Email Exceptions** option determines if an email report is sent when there are exceptions (alerts) on the unit, or whether emails are sent regardless of whether there is an exception or not.

Sending only email exceptions will send a report for the Global Sites, Customer, Site, or Unit when an alert is recorded on that unit. If **Only Email Exceptions** box is unchecked, then the report will be generated for every regardless to whether there is an alert condition. Enter the email address any of the boxes, and separate using a semi-colon (;)

The Daily Status Report can be generated for Global Sites, Customers, Sites, and Units. This allows a single email report with the status of all units rather than multiple emails at the same time. To do this:

1. Click on the Customer or Site in the Site Tree.
2. Select **Email Reporting** from the tabs.
3. Configure the time and email addresses where the report will be sent.
4. Click Save.

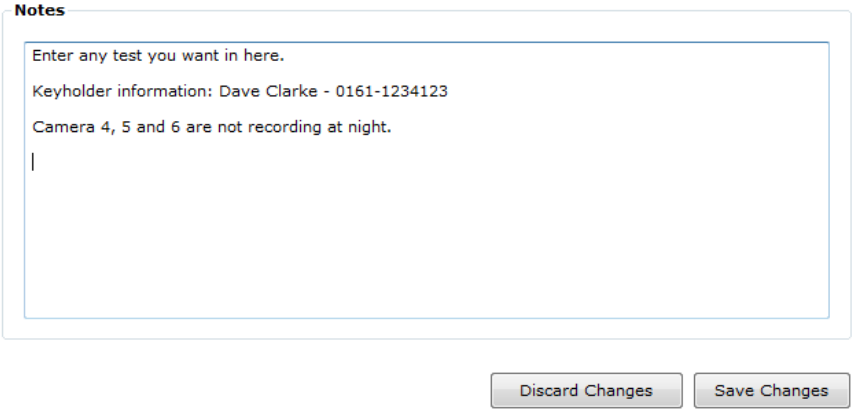
So, for example, selecting **Global Sites** from the site tree and following the above instructions will generate a single report for all the Customers, Sites, and Units in the Site Tree.

IMPORTANT: Daily Status Reports are 'snapshots' of the current unit status **at the time the report is generated**. Historical alerts are not sent in Daily Status Reports.

ADDING NOTES TO A CUSTOMER, SITE, OR UNIT

It is possible to add ASCII text notes to a Customer, Site, or Unit. Click on the Notes tab and type text into the text area. Click **Save Changes** or **Discard Changes** once completed.

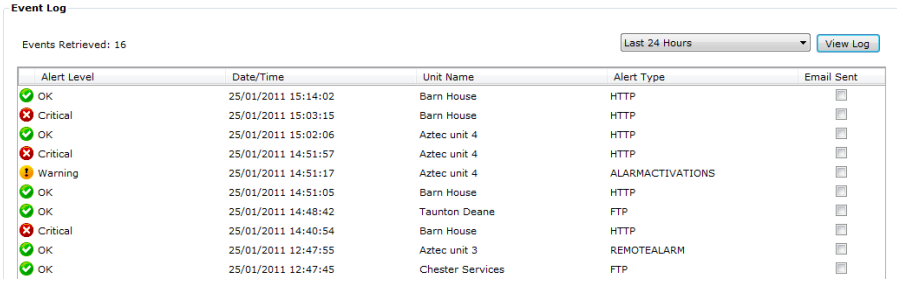
The notes page can be edited at any time; text can be added or deleted. A typical example of a notes page for a unit is:



VIEWING THE EVENT LOG

Every alert that is generated by CheckMyCCTV™ is recorded in the Event Log. There is an Event Log for Global, Customers, Sites, or Units.

Viewing the Global Event Log will display the alerts for all units in the site tree, likewise, the Customer Event Log will display the alerts for that customer and so on.



Alert Level	Date/Time	Unit Name	Alert Type	Email Sent
OK	25/01/2011 15:14:02	Barn House	HTTP	
Critical	25/01/2011 15:03:15	Barn House	HTTP	
OK	25/01/2011 15:02:06	Aztec unit 4	HTTP	
Critical	25/01/2011 14:51:57	Aztec unit 4	HTTP	
Warning	25/01/2011 14:51:17	Aztec unit 4	ALARMACTIVATIONS	
OK	25/01/2011 14:51:05	Barn House	HTTP	
OK	25/01/2011 14:48:42	Taunton Deane	FTP	
Critical	25/01/2011 14:40:54	Barn House	HTTP	
OK	25/01/2011 12:47:55	Aztec unit 3	REMOTEALARM	
OK	25/01/2011 12:47:45	Chester Services	FTP	

The Event Log contains the following information:

Alert Level – Critical, Warning, Information, or OK (Cleared).

Date/Time - Time and Date of when the alert was generated.

Unit Name - Name of the Unit in the Site Tree.

Alert Type – Which test has triggered the Alert.

Email Sent – Indicates if an email was sent as part of the Alert.

It is possible to filter the Alerts to the Last 24 Hours (default), Last 48 Hours, Last Week, Last Month, and Show All.

CONFIGURING CAMERA TAMPER SETTINGS

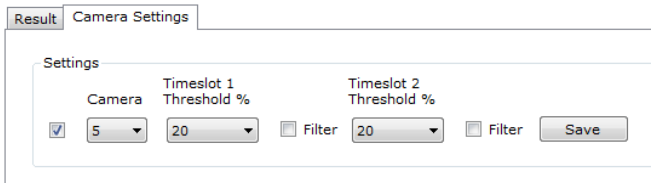
The Camera Tamper Detection function is a semi-automatic test. CheckMyCCTV™ checks the current image view against the previous days' images automatically, and when a Camera Tamper is detected, the operator can confirm whether the camera has been tampered with or not.

For Camera Tamper to work, it must first be enabled and configured in the Test Config Tab, see page 18- Configuring the Maintenance Tests.

The Camera Tamper configuration will determine when the snapshot images are taken, and the alert type that is generated. The Camera Tamper function needs to be enabled on each Camera before images are captured:

To enable Camera Tamper for a unit:

1. Click on the Unit to configure in the site tree and select the Camera Tamper tab, then Camera Settings:



2. Choose the camera to enable and check the enable checkbox. To enable every camera on the unit, choose ALL from the Camera dropdown and check the box.
3. Click **Save**.

Optimising Image Check Settings

Not all camera scenes are suitable for Camera Tamper Detection, such as:

PTZ or Dome cameras – These will give false tamper detection readings.

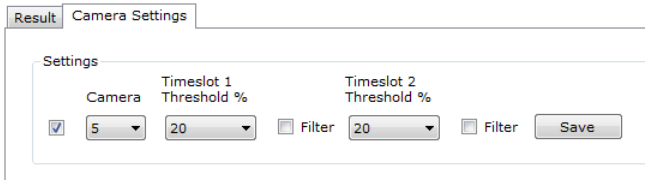
Cameras with scenes of very little detail – Such as, cameras pointing towards a plain wall or floor.

Cameras with a very wide field of view – Such as a car park or field.

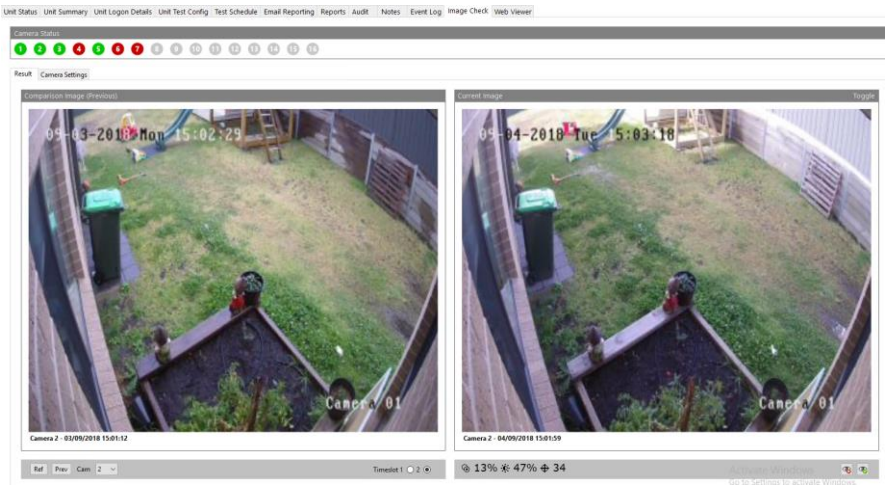
Cameras where the scene changes regularly – Such as a camera in a room which may turn pitch black when the lights are switched off.

Cameras where the scene is different day by day – such as car parks, or busy high streets.

To alleviate false Tamper alerts, configure the Threshold and Filter values to reflect the changes between the current and previous snapshot.



A difference threshold of 20% is the default value, this can be changed between 1-100% difference threshold.



Filtering noise out of camera tamper images

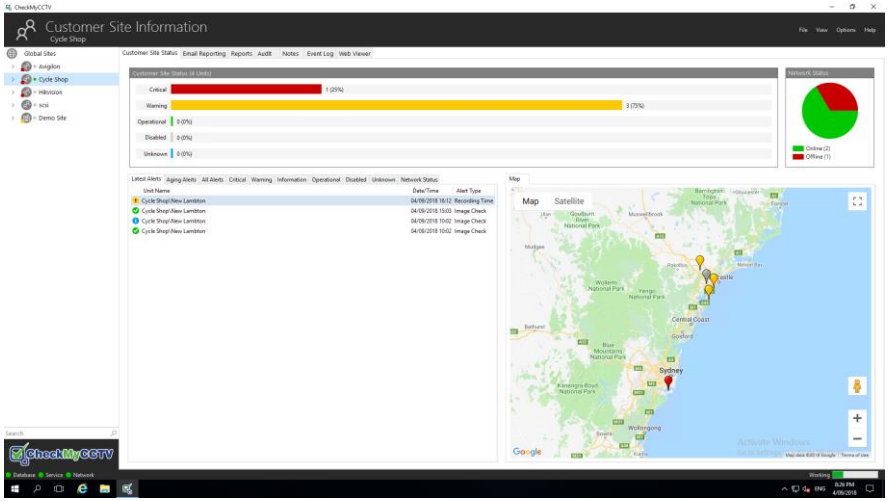
If an image has a lot of noise content, pixelization, or fine detail from foliage or trees, then enabling the **Filter** for that timeslot will reduce the number of false triggers from that image.

TIP: To get the best out of the Camera Tamper Detection function, it is advisable to run it for at least a week in a 'non-live' state, so it is possible to filter out false alerts and disable unsuitable cameras.

USING CHECKMYCCTV

Once CheckMyCCTV™ has been installed and configured, it will run automatically and autonomously in the background without any operator intervention.

GLOBAL/CUSTOMER/SITE INFORMATION VIEW



The Global/Customer/Site information view is used to see an overview of all the units that CheckMyCCTV™ is connected to, or the status of units within a Customer or Site folder.

Switching views

There are several views which can be selected in CheckMyCCTV™, click on the corresponding icon in the Site Tree to select the desired view:

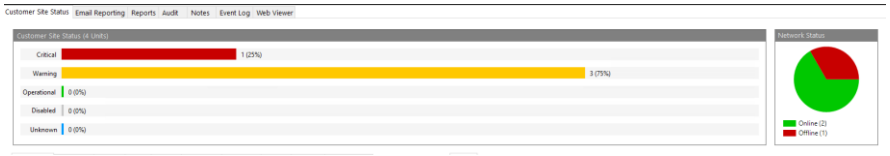
Global View – Displays unit status in the Global tree.

Customer View - Displays unit status in the Customer tree.

Site View – Displays unit status in the Site tree.

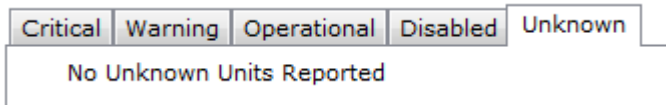
Unit View – Displays detailed status information for the selected unit.

Global, Customer, and Site views will display a graphical bar to represent the status of the units within the folder. A typical example could be:



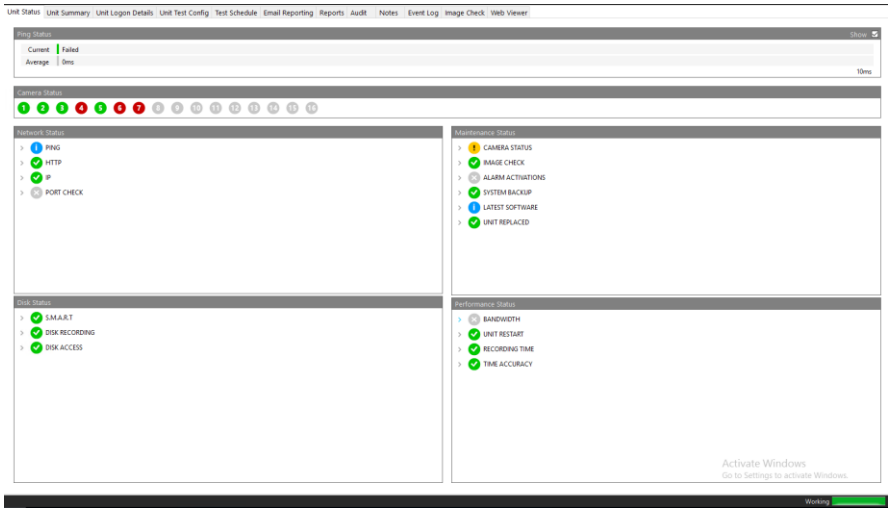
This is showing that the Global View has been selected and that there are 35 units within the Global folder. 4 units have a critical issue, 10 units are displaying a warning, 20 units are operational, with 1 unit is disabled (not connected or not licensed).

Underneath the graphic bars are category tabs; Critical, Warning, Operational, Disabled, and Unknown. By clicking on a tab, the units which fall in the selected category are displayed.

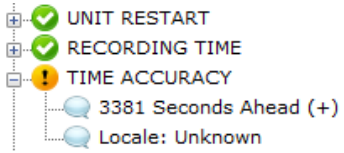


Double click on an icon to display the Unit View page, this is an in depth summary of all the tests and their corresponding results.

Clicking on the Unit View displays a detailed display of the Unit Status. This screen allows the operator to see exactly what issue is causing an alert:



It is possible to display the result of a test by clicking on the + symbol next to the test. For example, to display the Time Accuracy result, click on the + symbol next to TIME ACCURACY and the result is shown:



Viewing the map

To view the map, click on **View > Maps > Show Map Window**

Once the map is displayed, it is possible for the software to control what is displayed.

Click on a Global, Customer, Site, to see the locations of each Unit within that group or click on an individual unit to see its location.

The software displays a different coloured ‘pins’ depending on the status of the unit. Clicking an Icon on the graph will display the Status details of that unit within the software.

Grey – ‘Home’ location.

Green – Unit is Operational.

Yellow – Unit has a Warning condition.

Red – Unit has a Critical condition.

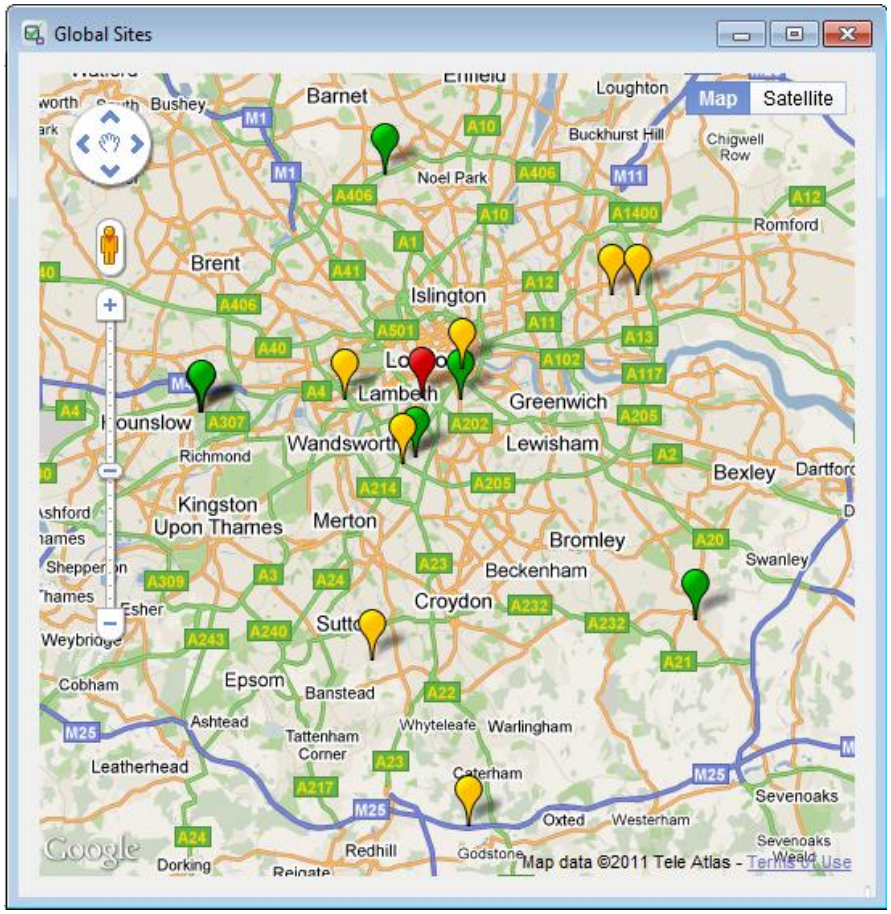
Note: The pins are displayed with the highest issue level on top to ensure that units with issues are not hidden.

DISPLAYING THE HOME LOCATION

To view the ‘Home’ position on the map, click on **View > Maps > Show Home Location**. This will always show the grey home location pin on the map. Details on how to set the home location can be found on page 10 - Configuring the Service.

DISPLAYING ALL UNITS

It may be necessary for the map to display all units, regardless of what is selected in the site tree. To force the map to display all the units continually, click on **View > Maps > Show All Units**.



LEGAL INFORMATION

COPYRIGHT

DISCLAIMER

CheckMySystems does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. CheckMySystems further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

TRADEMARKS

CheckMySystems and CheckMyCCTV™ are registered trademarks of CheckMySystems Ltd. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Tel: +44 (161) 8706137
info@checkmysystems.com