



Engineered Computer Appliance

User Guide

Revision 3.5

Table of Content

- ECA Operating System (ECAOS).....1
- Security Key1
- 1. Notification Bar2
 - 1.1 Notification event list3
- 2. System Manager 4
 - 2.1 Change Windows Settings5
 - 2.2 Setting IP address6
 - 2.3 Disk Management6
- 3. Task Scheduler7
- 4. SmartLogic8
 - 4.1 DiskHealth8
 - 4.2 DiskActivity9
 - 4.3 NetworkActivity10
 - 4.4 Notification Setting10
- 5. TrueBlue Remote Support11
- 6. Layer Manager12
 - 6.1 User Mode12
 - 6.2 SI Mode13
 - 6.3 How to ‘Soft Reset’ 14
 - 6.4 How to ‘save Deployment’14
 - 6.5 How to ‘Hard Reset’14
 - 6.6 Forgot SI Password 15
- 7. HeartBeat16
 - 7.1 HeartBeat Behavior16
 - 7.2 ECA power LED indication.....16
 - 7.3 HeartBeat PIN out17

ECA Operating System (ECAOS)

ECAOS is a protected operating system environment, equipped with a unique and practical feature called **Triple Layers**, essential for both reliable and secure operation of the ECA.

Its ability to Soft Reset within few minutes significantly reduces system down time in the event of, though rare, system disaster, such as corrupted Video Management Software or misconfiguration.



User Layer

(prevention of any unauthorized system setting changes)

is a normal user operation layer with protected OS environment, any system changes without using the Embedded Security Key will be discarded after system reboot (Fast Reset)

Deploy Layer

(Soft Reset)

is a good working state layer, usually saved by System Integrator with pre-configured NVR & camera settings

Factory Layer

(Hard Reset, restoration to this layer only accessible by System Integrator)

is a good working state layer, with original default settings shipped from factory

Security Key (USB Type)

Security Key is a uniquely designed USB security key which is paired to the ECA. It only can be used with the paired ECA and is required to commit any changes into the system permanently.

If the key is lost, new key can be issued by GSF and the paired ECA will automatically reject the usage of the lost key, should they be recovered later..

The concept is as simple as changing the house lock & keys.



Generally, the Security Key has two management modes.

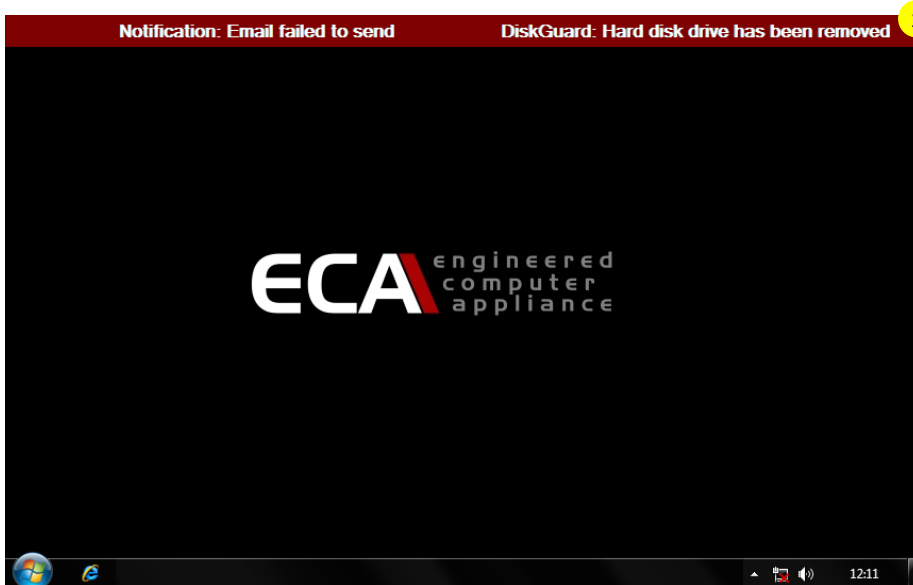
1) System Manager

2) Layer Manager

- User Mode
- System Integrator (SI) Mode

1. Notification Bar

Notification Bar is a overlay semi transparent on-screen event ECA notification. With Notification Bar, the user knows in a glance of event detected.

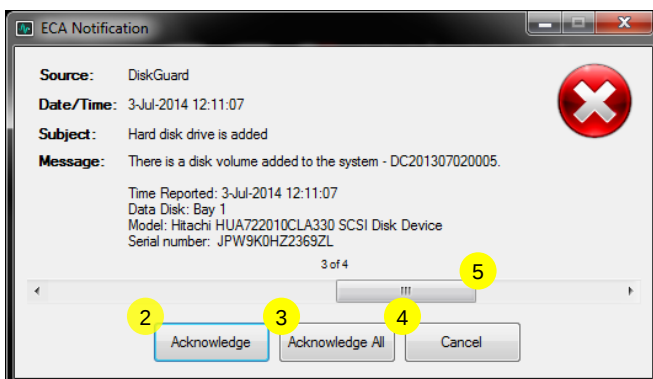


1. Left click on the Notification Bar to hide
2. Hidden Notification Bar will auto unhide after 5 minutes or new event detected
3. Move the cursor the top to unhide the Notification Bar

- 1 Notification Bar will appear if SmartLogic detected event on
 - **DiskHealth**
 - **DiskActivity**
 - **Network Activity.**

* Please refer to the SmartLogic section

How to see detail of the event? Double click on the notification bar



- 2 Acknowledge only current view notification
- 3 Acknowledge all notification
- 4 Will keep the notification bar active
- 5 Scroll the bar to see others notification

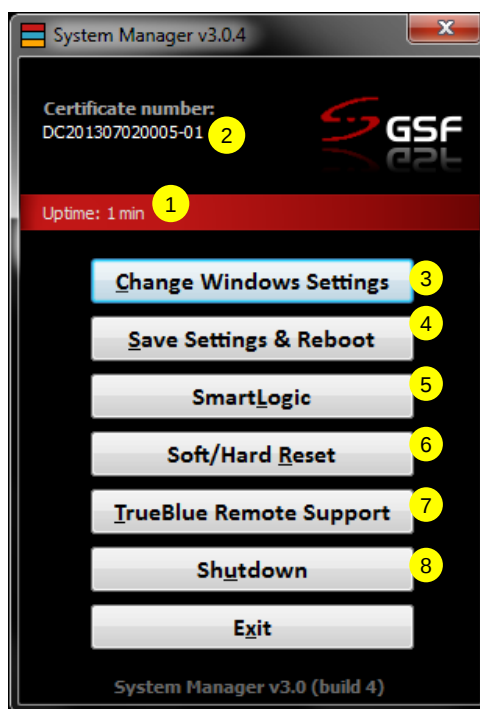
1.1 List of event will show on the notification bar;

Hard disk drive error is detected	The notification for this event is to notify user when the internal hard disk is below warning threshold value.
Hard disk drive is about to fail	The notification for this event is to notify user when the internal hard disk is below critical threshold value.
Hard disk drive has been removed	This event is triggered when system detected a volume storage changed (Disk Removed) and not match with inventory monitoring.
Hard disk drive is added	This event is triggered when system detected a volume storage changed (Disk Removed) but tally with disk inventory monitoring.
Potential CCTV is not recording	This event is triggered when the disk write activity is lesser than predefined threshold.
Potential CCTV being playback/copied	This event is triggered when the disk read activity is higher than predefined threshold
Potential video stream in error	This event is triggered when the network receiving bytes is lesser than predefined threshold
Potential video stream out	This event is triggered when the network sending bytes is higher than predefined threshold
Network connection is not available	This event is triggered when the network is NOT available
Network connection has resumed	This event is triggered when the network is available back.
Email failed to send	Email failed to send

2. System Manager

System Manager can be launched by inserting the Embedded Security Key into any USB port on the ECA while ECA is in Windows operating environment. System Manager allows user to modify system settings, such as IP Address, Date & Time and Disk Management.

The most important function of System Manager, however, is the ability to '**Save Settings & Reboot**', which permanently stores all modifications into the User Layer. Without doing so, all modifications of settings, software or Windows, are temporary only, and will be discarded once the ECA is powered off or reboot.



1 NVR Run Time

This is the time counter to indicate system Run time. Once the Run Time reaches '60 min', **Save Settings & Reboot** button will be **disabled**. You must reboot the ECA to enable the button.

2 Certificate Number

Shows the serial number of the ECA.

3 Change Windows Setting

Refer Section 2.1

4 Save Settings & Reboot

Save all modifications permanently to **User Layer**.

5 SmartLogic

Harddisk & Network monitoring

6 Soft/Hard Reset

Reboot the NVR into Layer Manager (for System Restoration or Backup purpose)

7 TrueBlue Remote Support

Remotely support ECA system via Internet

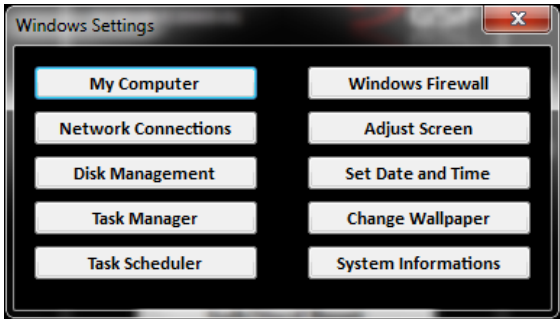
8

Shutdown

Shutdown the ECA

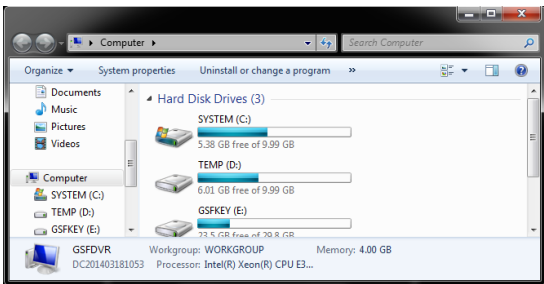
2.1 Change Windows Settings

Access to common Windows Setting, such as Network Connections and Disk Management.



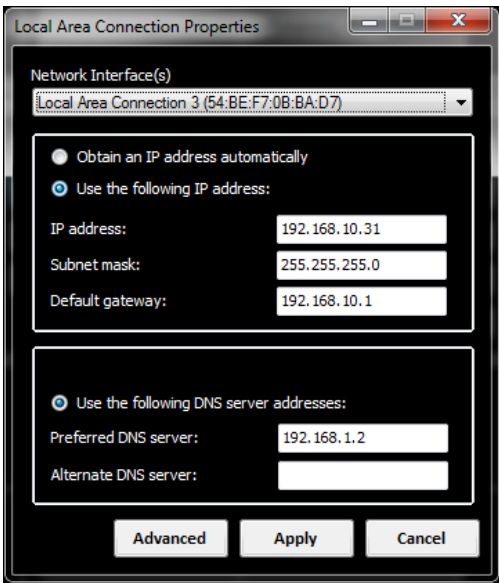
My Computer

Open Windows Explorer



Network Connections

Show / Change IP address, subnet, Gateway, DNS.



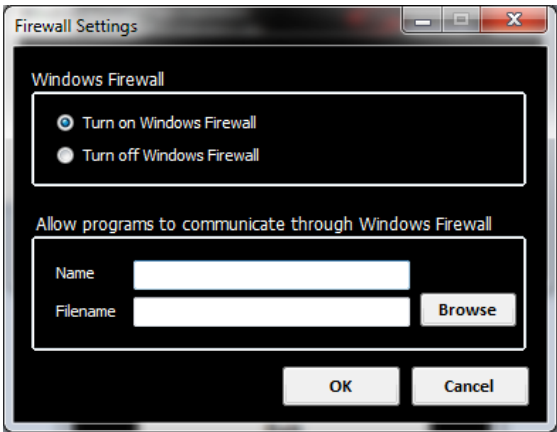
User may assign Secondary IP address to the network interface by pressing the 'Advanced' button.

Disk Management
Overview of all connected drives on the ECA. Allows management of the drives, such as Format drive.

Task Manager
Launch system monitor program, used to provide information about the processes and programs running on the ECA.

Task Scheduler
Change the SmartLogic scheduler
* Refer Task Scheduler on page 7

Firewall Settings
Controls the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through or not, based on applied rule set.



Adjust Screen
Change screen resolution, manage Primary and Secondary Monitor properties.

Set Date and Time
Change Windows Date and Time

Change Wallpaper
Change Windows Theme and Background

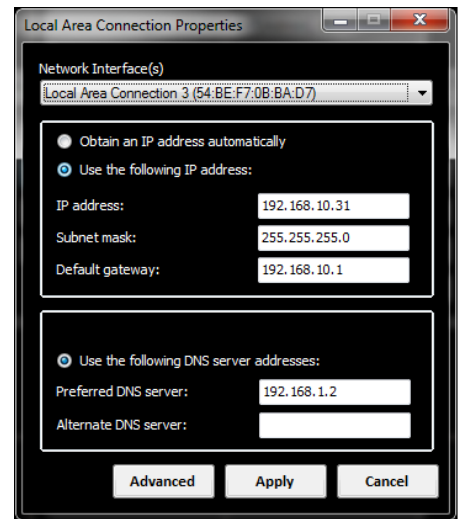
System Information
View System properties

2.2 Setting up IP address

All IP camera need to be in the same range with ECA.

1. Insert Security key into any USB port on the ECA
2. Click 'Change Windows Settings'
3. Click 'Network Connections'
4. Select Network Interface Card (NIC)
5. Enter the NIC IP address
6. Click 'Apply' to confirm
7. Click 'Save Settings & Reboot' to save setting under current layer

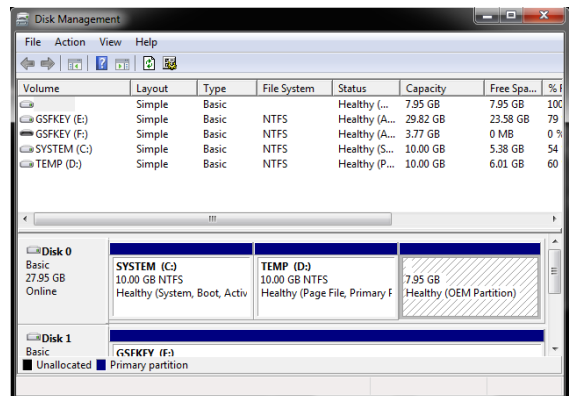
* For multiple IP address, please click the 'Advanced' button.



2.3 Disk Management

New hard drive must be format before can be use.

1. Insert 'New' hard drive
2. If no new hard drive detected, please reboot the NVR.
3. Insert Security key into any USB port on the ECA
4. Click on 'Change Windows Settings'
5. Click on 'Disk Management'
6. New hard drive notification will pop up OR **Right-click** on the disk and select **Initialize Disk**
7. Initialize the raw hard drive as a **GUID Partition Table (GPT)** partition style
8. Format as NTFS format. Make sure the drive letter correct.
9. Click 'Save Settings & Reboot' to save setting under current layer

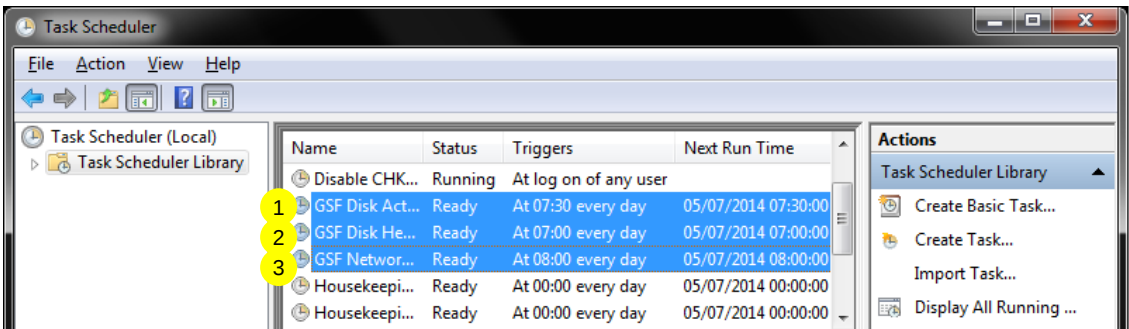


3. Task Scheduler

This Windows Task Scheduler services is used to trigger scanning time for

- DiskHealth
- DiskActivity
- NetworkingActivity

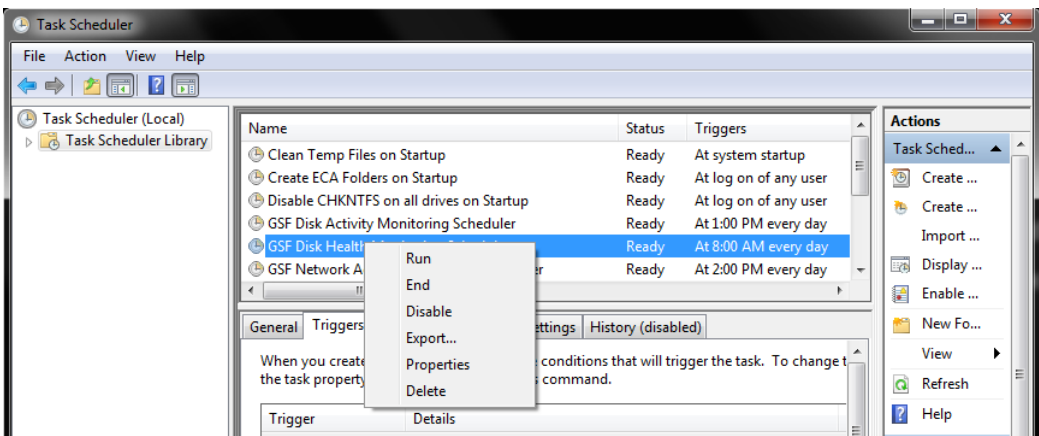
* Please refer SmartLogic page



- 1 **GSF Disk Activity Monitoring Scheduler**
 - Default time schedule: 7.30 every day
- 2 **GSF Disk Health Monitoring Scheduler**
 - Default time schedule: 7.00 every day
- 3 **GSF Network Activity Monitoring Scheduler**
 - Default time schedule: 8.00 every day

Re-schedule the time

Open the properties of the selected scheduler to change time accordingly



4. SmartLogic



1 DiskHealth

Monitor disk health & set the periodically email sent frequency whenever detected the health below certain threshold

2 DiskActivity

Monitor disk read write activity & set the periodically email sent frequency whenever detected the activity below certain threshold

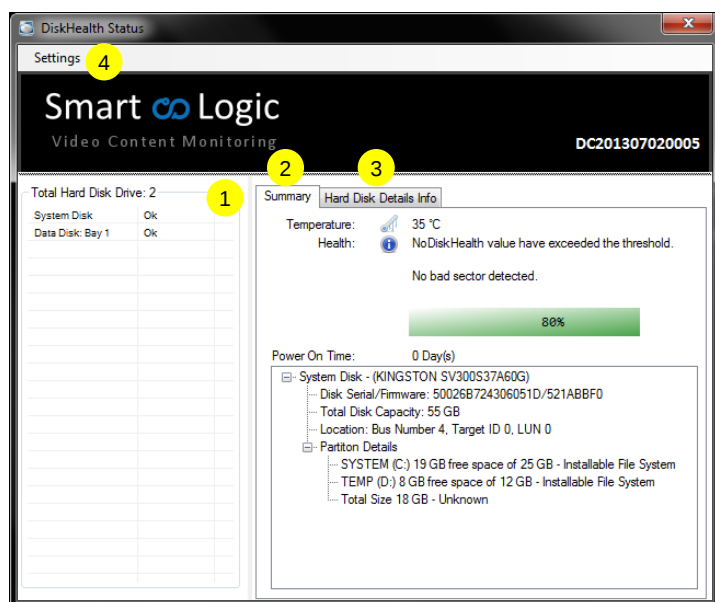
3 NetworkActivity

Monitor network incoming/outgoing bandwidth activity.

4 Notification

Setup email address

4.1 DiskHealth



1 Show the total hard disk & status

2 Detail for selected disk

3 Attribute detail for selected disk

4 Setting for DiskHealth Alert Threshold

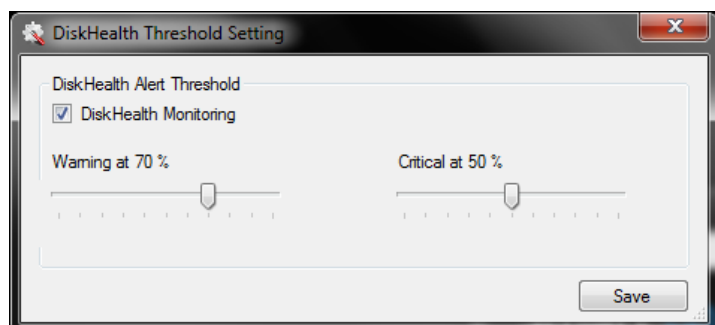
Type of Event:

Warning:

- Hard disk still safe to be used, recommend to change the hard disk

Critical:

- Please change the hard disk immediately



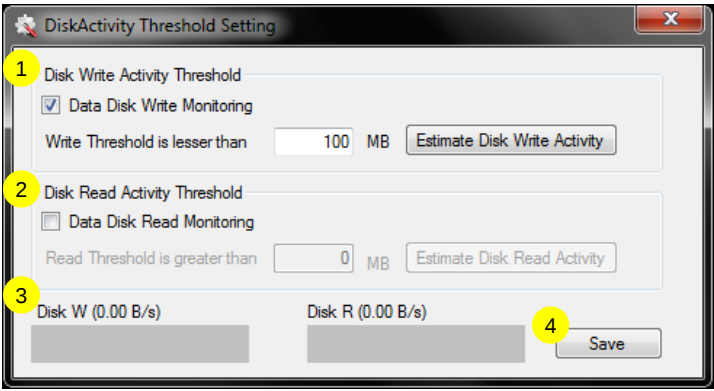
DiskHealth Alert Threshold

Threshold value for send email notification when the threshold value is hit.

Default value:

DiskHealth Monitoring: Enable
Warning 70%, Critical: 50%

4.2 DiskActivity



- 1 Monitor Disk Write activity
- 2 Monitor Disk Read activity
- 3 Real time disk activity
- 4 Save the setting

Disk Write Activity Threshold

Threshold value for send email notification when the threshold value is hit.

Default value:
DiskActivity Monitoring: Enable
Threshold: 100MB per day

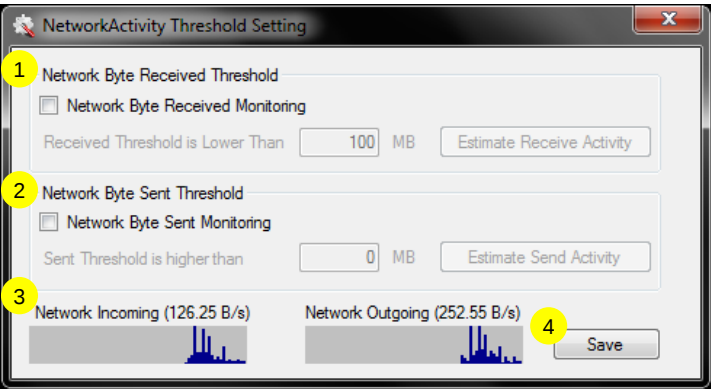
Disk Read Activity Threshold

Default value:
DiskActivity Monitoring: Disable
Threshold: 0MB per day

Not sure the value to be enter?

If user doesn't any idea on the value need to be enter, just press the 'Estimate Disk Write Activity' or 'Estimate Read Activity' button. The application will take 1 hour of data on the hard disk and display the value.

4.3 NetworkActivity



- 1 Monitor Incoming activity
- 2 Monitor Outgoing activity
- 3 Real time disk activity
- 4 Save the setting

Network Byte Received Threshold

Threshold value for send email notification when the threshold value is hit.

Default value:
DiskActivity Monitoring: Disable
Threshold: 100MB per day

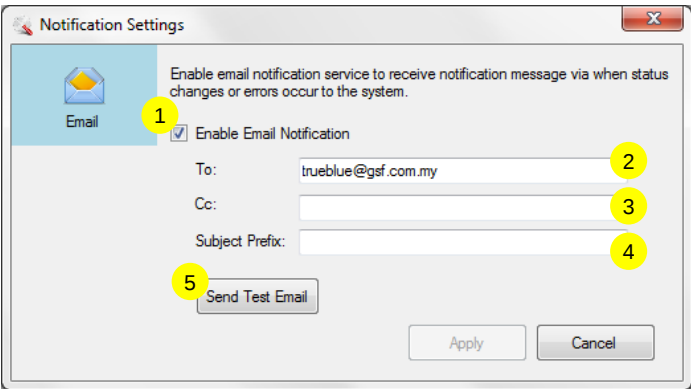
Network Byte Outgoing Threshold

Default value:
DiskActivity Monitoring: Disable
Threshold: 0MB per day

Not sure the value to be enter?

If user doesn't any idea on the value need to be enter, just press the 'Estimate Reviece Activity' or 'Estimate send Activity' button. The application will take 1 hour of data on the hard disk and display the value.

4.4 Notification Setting



- 1 Notification toggle
- 2 Primary email to receive notification
- 3 Carbon copy email to receive notification
- 4 Set front prefix subject for easier to recognize from which ECA the notification recieve from
- 5 Send test email to recipient

How to add multiple email address? [email@email.com](#), [email2@email.com](#), [email3@email.com](#)
Example 'Subject Prefix': SVR1blockA, NVR@Factory B.

5 TrueBlue Remote Support

TrueBlue® Support

TrueBlue Remote Support is an online live support service backed by the professional TrueBlue Support team. This service allows our TrueBlue Engineer to remotely access the targeted ECA, and gain full control for troubleshooting, usually on software and OS related issues. Remote Support session works similar to Remote Desktop.

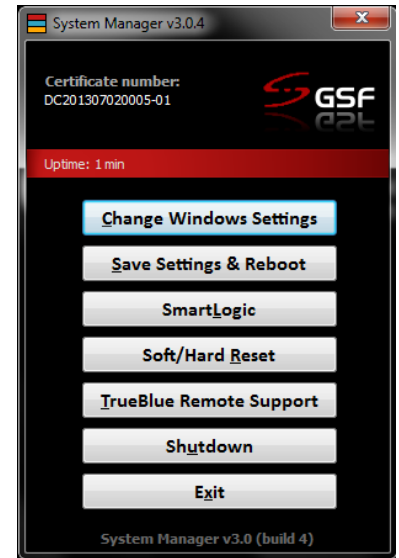
To establish TrueBlue Remote Support session, the targeted ECA

1. Must be connected to internet (check with your network administrator for appropriate settings);
2. Must be able to launch either in System Manager if the issue is Software or OS related; or
3. Must be able to launch in Layer Manager if the issue is OS related, example, cannot boot into Windows.

System Manager

To begin a TrueBlue Remote Support session in

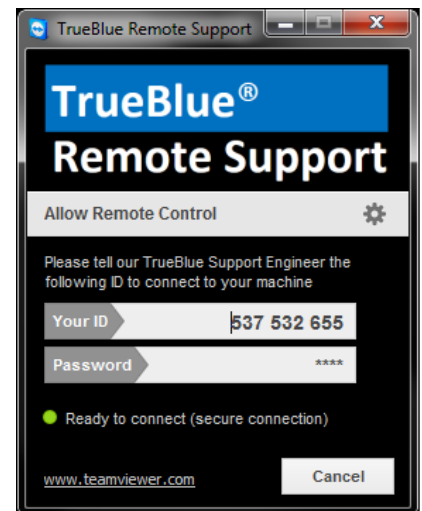
1. Call TrueBlue Support Line:
+60-3-8090 9090;
1. Insert Security key into any USB port on the ECA;
2. Press the “TrueBlue Quick Support” button;
3. Inform the ID number and password (if any) shown on the TrueBlue Quick Support window to the TrueBlue Engineer over the phone call.



Layer Manager,

To begin a TrueBlue Remote Support session in

1. Call TrueBlue Support Line:
+60-3-8090 9090;
1. Insert Security key into any USB port on the ECA.;
2. Power Up the ECA;
3. While in Layer Manager, log in to SI Mode (*Refer page 13*)
4. Press the “TrueBlue Quick Support” button;
5. Inform the information as belwo to TrueBlue Engineer over the phone
 1. ID number
 2. password (if any)



TrueBlue Engineer will keep you informed via phone call when they are done with the troubleshooting.

6. Layer Manager

Layer Manager is the second management mode on the Embedded Security Key that allows its user to perform administrative tasks to its paired ECA, such as Soft Reset, Hard Reset (Factory Default) and Save Deploy layer. Majority of these features are password protected.

How access to Layer Manager

Access Layer Manager mode on OFF-STATE

1. Insert the Security Key to any USB port on the ECA
2. Power On the ECA.
3. ECA will boot from Security key

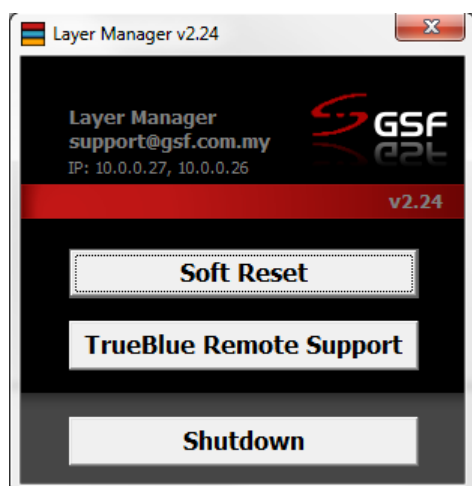
Access Layer Manager mode from Windows

1. Insert Security key to any USB port on the ECA
2. Click on '**Soft/Hard Reset**' on System Manager
3. ECA will reboot, keep the key in USB port & ECA will boot from Security key

6.1 Layer Manager – User Mode

In a short while, the Layer Manager will appear on the screen.

This is the **User Mode** of the Layer Manager.



Soft Reset

Reset the ECA to Deployment Layer (Layer previously saved)

TrueBlue Remote Support

Reset the ECA to Deployment Layer (Layer previously saved)

Shutdown

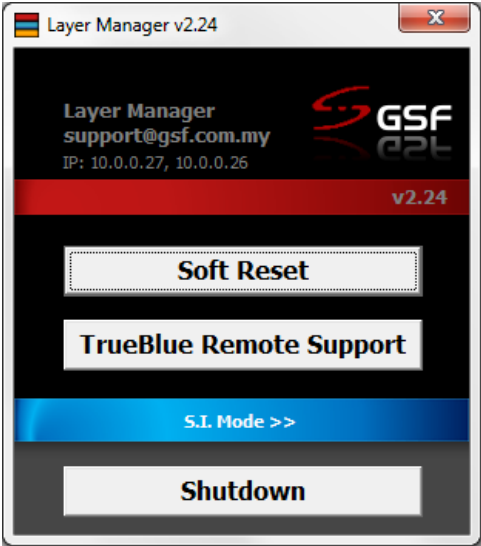
Do nothing and Shutdown the NVR system

6.2 Layer Manager – SI Mode

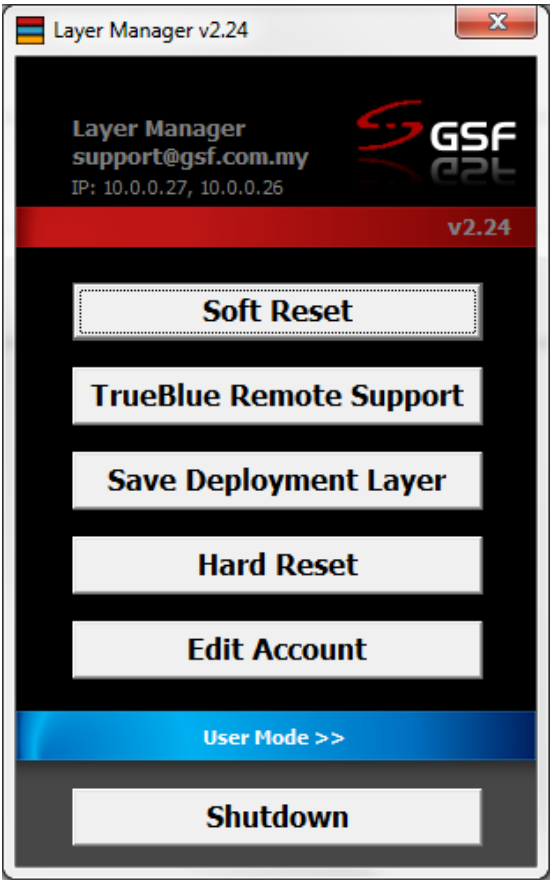
SI mode of Layer Manager is a password protected advanced mode, which allows the user to perform crucial administrative task.

How access to SI Mode

1. Press and hold keyboard “**Shift**” button while in Layer manager.
2. A blue color band will unhide, disclosing the “**S.I. Mode >>**” wordings.
3. Now, while still holding the “Shift” button on the keyboard, “**left mouse click**” on the “**S.I. Mode >>**” words.
4. You’ll be prompted for password in order to access S.I. Mode., the default password is **PassWord123**.



This is the **SI mode** of the Layer Manager.



Soft Reset

Reset the ECA to Deployment Layer

TrueBlue Quick Support

Online live support service backed by the professional TrueBlue Support team
(Refer page 6)

Save Deployment Layer

Save current User Layer as Deployment Layer. Take note that doing so will **OVERWRITE** previous deployment layer.
(Refer page 6)

Hard Reset

Reset the ECA to Factory Layer (Factory Default)

Change Password

Provides option to change the password for access to S.I. Mode of Layer Manager

Shutdown

Do nothing and Shutdown the NVR system

6.3 How to ‘Soft reset’?

1. Access to Layer Manager (*refer page 12*)
2. Click on **Soft Reset** to start the recovery procedure.
3. Key-in ‘**1234**’ to confirm
4. The NVR will be shutdown once is done.
5. Remove the USB Security Key, and reboot the NVR.

6.4 How to ‘Save Deployment’?

1. Access to Layer Manager (*refer page 12*)
2. Access to SI mode (*refer page 13*)
3. Click on ‘**Save Deployment Layer**’ to start saving current user layer
4. Key-in ‘**1234**’ to confirm
5. The NVR will be shutdown once is done.
6. Remove the USB Security Key, and reboot the NVR.

6.5 How to ‘Hard Reset’?

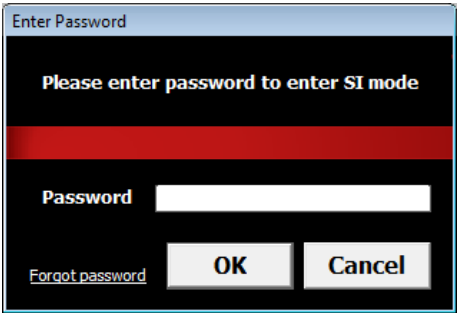
1. Access to Layer Manager (*refer page 12*)
2. Access to SI mode (*refer page 13*)
3. Click on **Hard Reset** to start the recovery procedure.
4. Key-in ‘**1234**’ to confirm
5. The NVR will be shutdown once is done.
6. Remove the USB Security Key, and reboot the NVR.

*** DO NOT reboot OR power Off ECA during recovery process**

6.6 Forgot Password

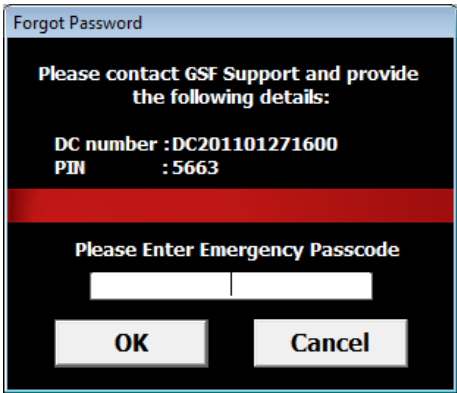
The System Integrator (S.I) won't be able to access S.I. mode without password . This section will explain how to recover the password for S.I. mode.

- 1. Access SI mode (*Layer Manager – SI Mode*)
- 2. Left click on the **Forgot password**



- 3. Write down the 'DC number' & 'PIN'
- 4. Contact GSF TrueBlue™ Support GSF TrueBlue™ Support will ask for DC number & PIN
- 5. Enter the Emergency Pass code given by GSF TrueBlue™ support personnel.
- 6. Click 'OK'
- 7. Enter new password

* PIN only valid in the same day.



7 Heartbeat

Heartbeat is a round the clock hardware safeguard. Its micro controller overlooks the whole hardware platform to ensure continuous operation even in the event of critical breakdown.

In the event the server failed, it will send help signal via digital I/O or can be connect to CMS Alarm.

In what event the HeartBeat will react?

- Unauthorized Shutdown:** The HeartBeat will reboot the ECA
- Unauthorized Power Unplug:** HeartBeat will produce beep tone (Tone Pattern 5)
- ECA hang:** HeartBeat will force restart the ECA after 5 minutes no respond
- Blue screen:** HeartBeat will force restart the ECA after 5 minutes no respond

7.1 HeartBeat Behavior

Beep Tone Pattern		Repeating Interval	ECA scenario	Description
1		No repeat	•ECA OFF •In OS/BIOS	•Shutdown/Power Cut detected •HeartBeat initiate reboot
2		20s	•ECA OFF •ECA ON	•Low HeartBeat battery ¹ •HeartBeat failed to reboot
3		No repeat	ECA Rebooting	HeartBeat initializing after first reset .
4		No repeat	ECA Rebooting	HeartBeat establish USB link.
5		10s	•ECA OFF •ECA ON	•Unauthorized power unplug ² •Unauthorized ECA reboot more than 3 times ³

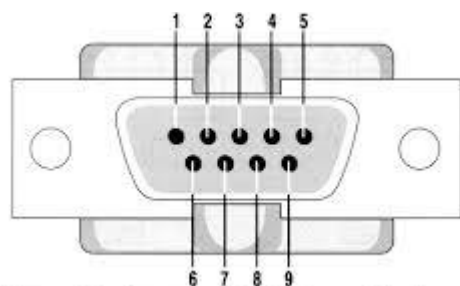
¹ , ² Power ON the ECA will mute the beep tone

³ Shutdown the ECA will mute the beep tone (This doesn't apply to AC power cut)

7.2 ECA power LED indication

LED Status	ECA scenario	Description
Slow glow and dim	ECA ON/ in OS	•HeartBeat operating normally
Blinking	•ECA OFF •ECA rebooting	•Low HeartBeat battery •ECA in rebooting status

7.3 HeartBeat digital I/O PIN out



Relay Contact Maximum Rating

Max. operating voltage: 125 VAC, 60 VDC

Max. operating current: 1 A

Pinout

Pin 7 : Normal Open

Pin 8 : COM

Pin 9 : Normal Close



GSF Solutions Sdn Bhd (733346-x)

Unit 21, Level 3A, IOI Boulevard, Jalan Kenari 5, Bandar Puchong Jaya, 47170 Puchong, Selangor D.E., Malaysia.

Tel: +603 80803989 Fax: +603 80803990

Email: info@gsf.com.my Web: <http://www.gsf.com.my>