ECA

Engineered Computer Appliance Operating System

ecaOS 6.9

USER GUIDE

Revision 2.0
24 Jun 2025

Digital Copy

Document Title

Engineered Computer Appliance Operating System 6.9 User Guide

Document Revision

Revision	Date	Description	Author
00	20 Sep 2022	1st Edition	Jemiruddin
01	12 Oct 2022	2nd Edition	Jemiruddin
1.1	22 Nov 2022	2nd Edition with minor cosmetic change	Sengfu
1.2	19 March 2023	3rd Edition	Jemiruddin
1.3	19 April 2023	4th Edition (Bay orientation)	Jemiruddin
1.4	30 May 2023	Updated to ecaOS 6.1	Keong
1.5	23 Nov 2023	Updated to ecaOS 6.2	Keong
1.6	22 Jan 2024	ECA45 Redundant PSU	Keong
1.7	6 Mar 2024	Updated to ecaOS 6.3	Keong
1.8	15 Jul 2024	Updated to ecaOS 6.4	Keong
1.9	27 Sep 2024	Updated to ecaOS 6.8	Keong
2.0	24 Jun 2025	Updated to ecaOS 6.9	Keong

© GSF Corporation
Unit 21, Level 3A, Jalan Kenari 5, Bandar Puchong Jaya, 47170 Selangor D.E., Malaysia | +603-80908080 | info@gsfcorp.com

Table of Contents

1 ecaOS 6
1.1 ecaOS Login 7
1.2 ecaOS Locked Out 7
2 Dashboard and Notification 8
2.1 Accessing ecaOS Dashboard 9
2.2 How to use Security Key (USB) 9
2.3 How to use Virtual Security Key (ECA Access Code) 10
2.4 Get Virtual Security Key (ECA Access Code) 10
2.5 Accessing ecaOS Dashboard Remotely 14
2.6 Dashboards 16
8 Applications 18
8.1 System Monitor 18
8.2 App Monitor 21
8.2.1 Add Application 21
8.2.2 Delete Application 23
8.2.3 Add Services 24
8.2.4 Delete Services 26
8.3 System Activity 27
8.3.1 Processor Activity 27
8.3.2 Memory Activity 28
8.3.3 Disk Activity 30
8.3.4 Network Activity 31
8.4 Storage Monitor 32
8.4.1 Volumes 32
8.4.2 Disks 32
8.4.3 S.M.A.R.T. 34
8.4.4 Hard disk change during ECA Power Off 35
8.5 Session Shield 36
8.5.1 Activate Session Shield 36
8.5.2 Deactivate Session Shield 39
8.5.3 Exclusion List 40
8.5.4 Add Exclusion Files or Folder 41
8.5.5 Delete Exclusion Files or folder 42
8.5.6 Add Registry Keys 42
8.5.7 Delete Exclusion Registry Key 44
8.5.8 Status: Warning 44
8.5.9 Status: Critical 44
8.6 Device Monitor 46
8.6.1 Add New Monitor 46
8.6.2 Delete Monitor 48
8.7 Recording Monitor 49
8.7.1 Add New Monitor 50
8.7.2 Delete Monitors 51
9 Management 52
9.1 Machine 52
9.1.1 Authorize Restart 52
9.1.2 Authorize Shutdown 53
9.1.3 Saving & Deploy Layer 54
9.1.3.1 Save Layer 54
9.1.3.2 Soft Reset 56
9.1.3.3 Hard Reset 58
9.1.3.4 Last Saved Layer Information 60

© GSF Corporation
Unit 21, Level 3A, Jalan Kenari 5, Bandar Puchong Jaya, 47170 Selangor D.E., Malaysia | +603-80908080 | info@gsfcorp.com

9.1.4 Machine Name 60
9.1.5 Change Dashboard Port 60
9.1.6 ecaCentral Registration 60
9.2 Security Key 62
9.2.1 Register Security Key 62
9.2.2 Delete Security Key 63
9.2.3 Add Virtual Security Key 64
9.2.4 Delete Virtual Security Key 66
9.3 Network 67
9.3.1 Enable DDNS 67
9.3.2 Enable Network Teaming 67
9.3.3 Disable Network Teaming 68
9.4 RSS (Redundant Storage System) 69
9.4.1 Create Storage Pool 69
9.4.2 Delete Storage Pool 71
9.4.3 Extend Storage Pool 72
9.4.4 Repair Storage Pool 73
9.5 Settings 77
9.5.1 Email Recipient Settings 77
9.5.2 Mail Servers 77
9.5.3 Events 77
9.5.3.1 Events List 78
9.5.4 SNMP Settings 83
9.5.4.1 Enable SNMP 84
9.5.4.2 Download ECA MIB Files 84
10 Events 85
10.1 Notification 85
10.2 Logs 86
10.2.1 Filtering Log 86
10.2.2 Exporting Log 86
10.3 Report 90
11 Support 92
11.1 Microsoft Remote Desktop 92
11.2 Chrome Remote Desktop 93
11.2.1 Setup ECA into your Chrome Remote Desktop 93
11.2.2 Accessing ECA via Chrome Remote Desktop? 96
12 About 98
12.1 Machine Information 98
12.2 Heartbeat Information 99
13 APPENDIX 100
13.1 Processor Activity 100
13.1.1 CPU activity above limit 100
13.1.2 CPU activity back to normal 101
13.2 Memory Activity 102
13.2.1 Memory usage above limit 102
13.2.2 Memory activity back to normal 103
13.3 Disk Activity 104
13.3.1 Disk read activity above limit 104
13.3.2 Disk read activity back to normal 105
13.3.3 Disk write activity below limit 106
13.3.4 Disk write activity back to normal 107
13.4 Network Activity 108
13.4.1 Network send activity above limit 108

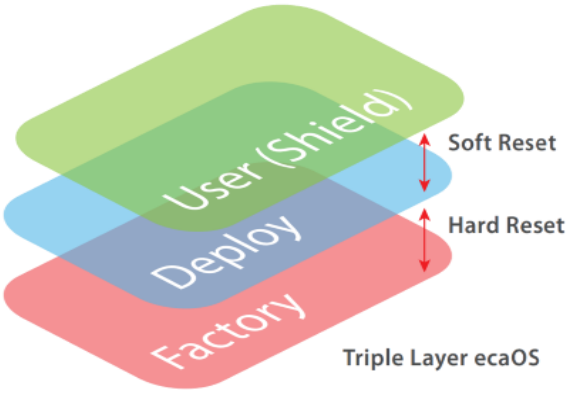
© GSF Corporation
Unit 21, Level 3A, Jalan Kenari 5, Bandar Puchong Jaya, 47170 Selangor D.E., Malaysia | +603-80908080 | info@gsfcorp.com

13.4.2 Network send activity back to normal 109
13.4.3 Network receive activity below limit 110
13.4.4 Network receive activity back to normal 111
13.5 Session Shield 112
13.5.1 Warning Status 112
13.5.2 Critical Status 113
13.5.3 Status back to normal 114
13.6 Disk Health 115
13.6.1 Warning Status Disk 115
13.6.2 Critical Status Disk 116
13.7 Disk Guard 117
13.7.1 New disk / Disk Inserted 117
13.7.2 Disk Removed 118
13.7.3 Disk Removed Acknowledge 119
13.7.4 Disk Replaced 120
13.7.5 Disk Replaced Acknowledge 121
13.8 Log 122
13.8.1 ECA reboot more than 3 times 122
13.8.2 AC Power loss 122
13.8.3 Unauthorize ECA Reboot 122
13.8.4 Unauthorize ECA Shutdown 123
13.8.5 Authorize ECA Shutdown 123
13.8.6 Authorize ECA Reboot 123
13.8.7 Power up ECA by pressing power button 123
13.8.8 Force shutdown by pressing power (heartbeat) button 124
13.8.9 Accessing Dashboard using Security Key 124
13.8.10 Accessing Dashboard using Virtual Security Key 124
13.8.11 Add new Security Key 124
13.8.12 Delete paired Security Key 125
13.8.13 Delete Virtual Security Key 125
13.8.14 Add Virtual Security Key 125
13.8.15 Open ECA cover chassis 125
13.8.16 Close ECA cover chassis 125
13.8.17 PSU Status 126
13.9 ecaOS SNMP Notification 127
13.9.1 CPU Activity 127
13.9.2 Memory Activity 128
13.9.3 Disk Activity 129
13.9.4 Network Activity 131
13.9.5 Disk Guard 134
13.9.6 Disk Health 137
13.9.7 Hardware Monitor 138
13.9.8 Session Shield [Only available in Windows Client] 139
13.9.9 Application Monitor 140
13.9.10 Redundant Storage System 141

1 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.



Layer	Description
User Layer *Current working layer*	This is a normal user operation layer with a protected OS environment, any system changes without using the Embedded Security Key will be discarded after system reboot (Fast Reset)
Deployment Layer *Backup Layer*	This is a good working state layer, usually saved by System Integrator with pre-configured NVR & camera settings
Factory Layer *Backup Layer*	This is a good working state layer, with original default settings shipped from factory

1.1 ecaOS Login

Some ECA may be shipped without automatic login, subject to configurations. In such case, the ecaOS prompt for OS login, as follow:

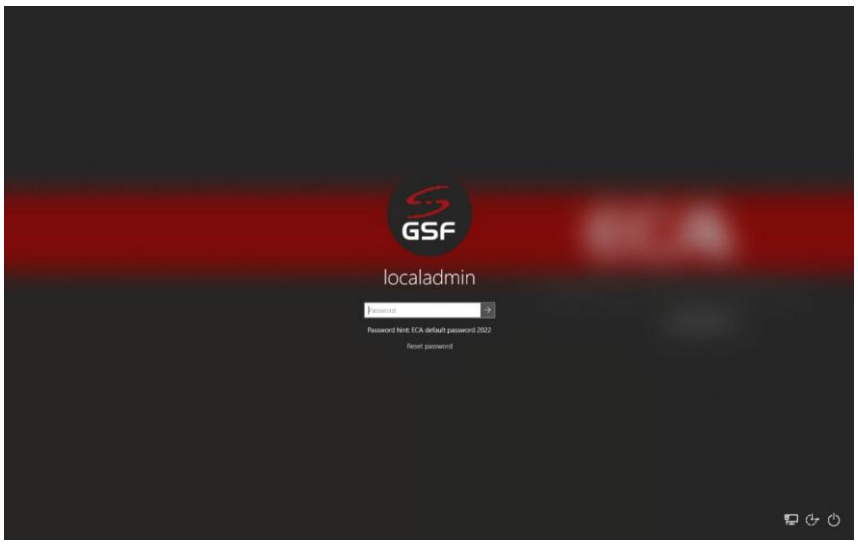


Figure 1: ecaOS Login Screen

Please contact **TrueBlue Support** to obtain the login credentials:

Email :	trueblue@gsfcorp.com
Contact number :	+60-3-80908277

Information to provide:

- Digital Certificate number of the ECA, usually can be found on the front panel of the ECA, and starts with **DC20XXXXXXXXX** (14-digits)
- End-user's name

1.2 ecaOS Locked Out

if the password is incorrect for 3 times consecutively, the login screen will lock for 15 minutes, before allowing retry.

Figure 2: Account Locked Out

2 Dashboard and Notification

Location of the Dashboard application and ecaOS Notification display area.

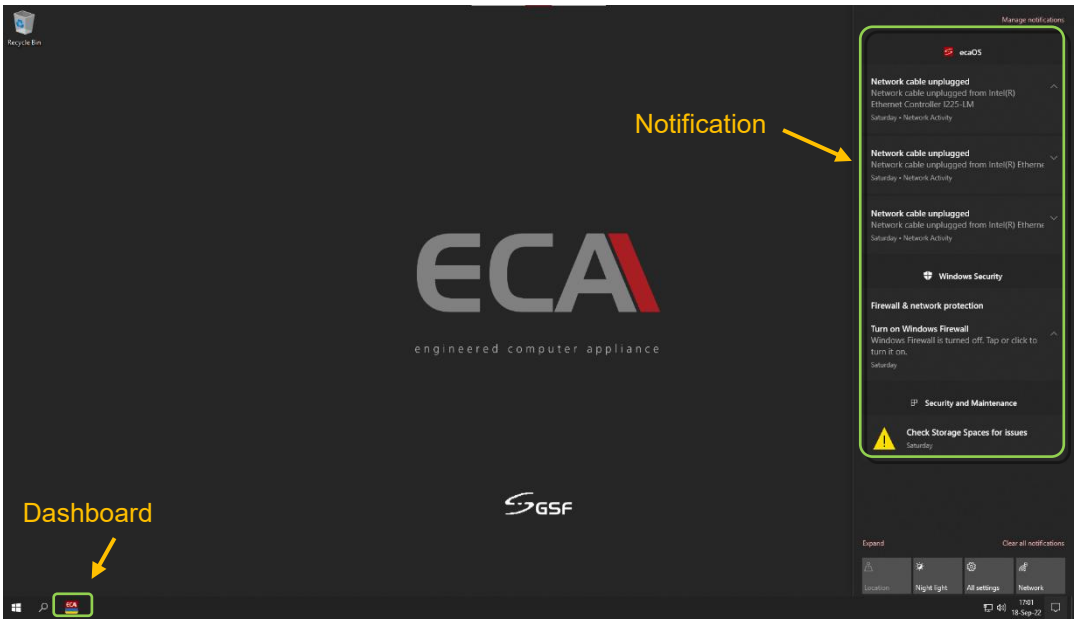


Figure 3: ecaOS Desktop

Notification	Where all the activities within the ECA will be prompted out
Dashboard	A web-based interface displaying overall information and system vitals of the ECA machine status

2.1 Accessing ecaOS Dashboard

There are two ways to access ecaOS Dashboard.

1. Security Key (USB type)
2. Virtual Security Key (card with QR code)

Figure 4: Security Key & Virtual Security Key Card

2.2 How to use Security Key (USB)

1. Insert Security Key to **SECURITY KEY** port on front panel of ECA.

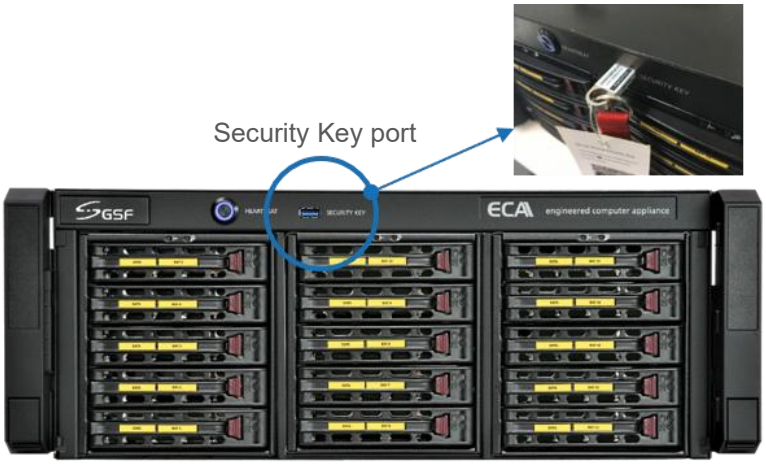


Figure 5: Security Key USB Port Location

2. Run 'ecaOS Dashboard' ' ' from Taskbar.

2.3 How to use Virtual Security Key (ECA Access Code)

1. Run ‘ecaOS Dashboard’ ‘ ’ from Taskbar.
2. Enter **Access Code** from authenticator apps.

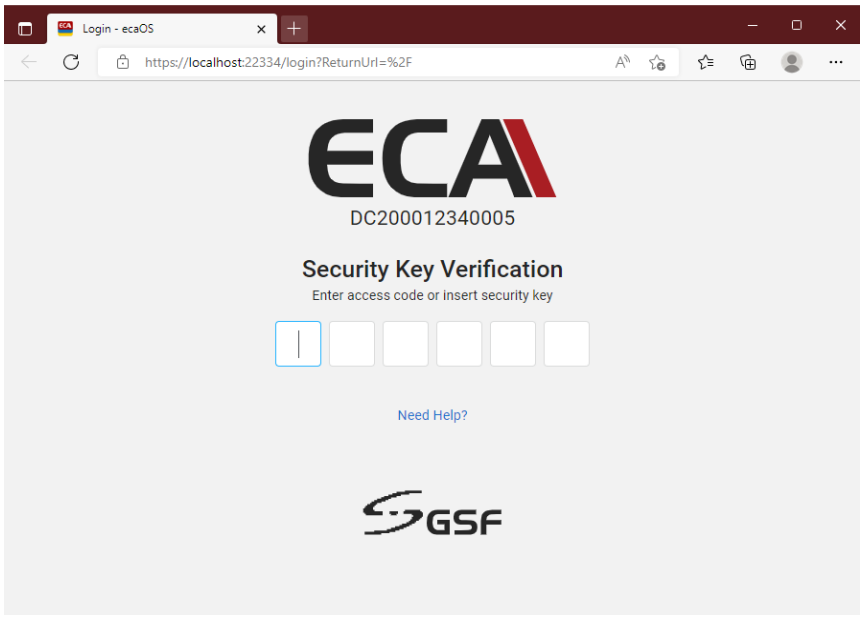


Figure 6: Dashboard Login Page

2.4 Get Virtual Security Key (ECA Access Code)

ECA Access code is mandatary for logging into the Dashboard. To obtain the ECA Access code, follow the procedures below:

1. Download an Authenticator app.
   - For **Android** user, go to **Google Play**.
   - For **iOS** user, go to **App Store**.

2. Search for ‘authenticator’. Then, **Google Authenticator** or **Microsoft Authenticator** should appear in the result. You can install either one as the authenticator to use with ecaOS for obtaining the Access code.

Figure 7: App search results

3. The following procedure is based on using Google Authenticator.

> ⚠ Before using an authenticator app, ensure that your device’s time is synchronized with ECA’s time. If it is not, the code may not work correctly

4. Run Google Authenticator on your device. Click **Begin** button.

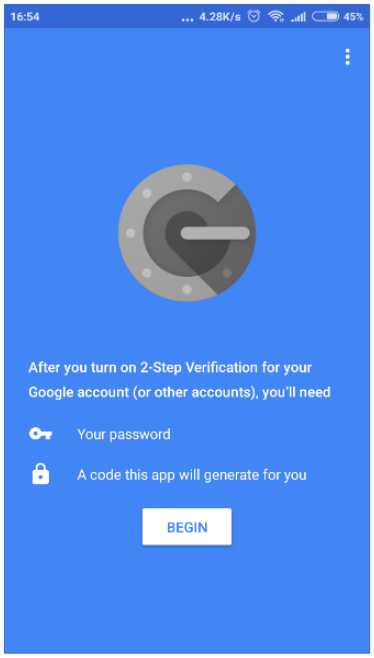


Figure 8: Authenticator Setup

5. Choose **Scan a barcode** to start scanning the QR code found on the Virtual Security Key card.

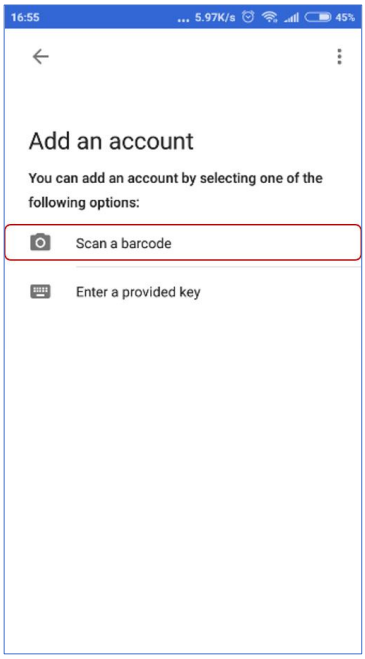


Figure 9: Authenticator Setup

6. Ensure the QR code is positioned correctly within the scanner frame.

Figure 10: Authenticator Setup

7. Once successful, the Access code will display in the app.

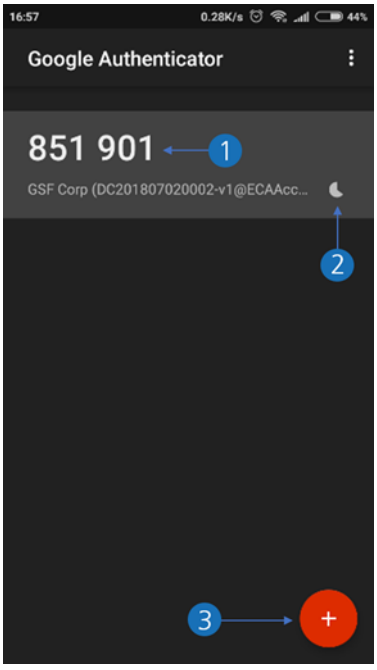


Figure 11: Authenticator Setup (4 of 4)

1. Access Code
2. Access Code will change for every 30 seconds
3. Click here to scan another QR Code for others ECA 'Virtual Security Key'.

8. Enter the 6-digits One-Time-Passcode (OTP) access code into the Security Key Verification page (ecaOS Dashboard login page).

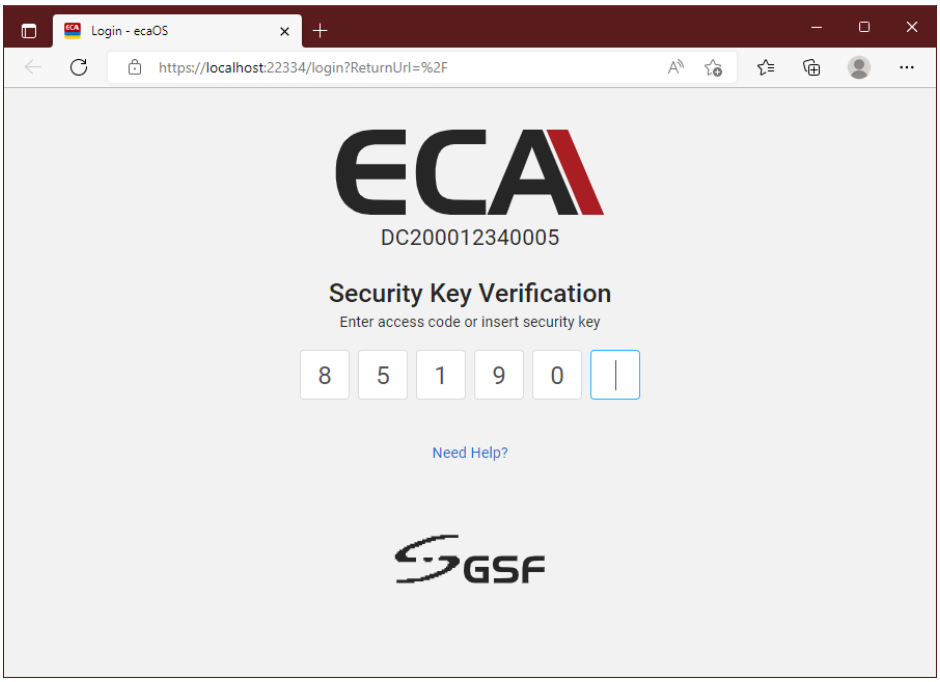


Figure 12: ecaOS Dashboard Login Page

2.5 Accessing ecaOS Dashboard Remotely

1. Open web browser on the remote computer.
2. In the web browser's address bar, enter the IP address of the ECA, in this format:

```
https://<ipaddress>
```

Example: `https://10.0.0.39`

Alternatively, you may also insert the ECA's Digital Certificate (DC number), also known as the serial number, in the following format:

```
https://<ECA serial number>
```

Example: `https://DC200012340005`

> ⚠ Default access port number for ecaOS Dashboard is **443**. This port number is customizable in the Dashboard configuration.

3. Click **Advanced**.

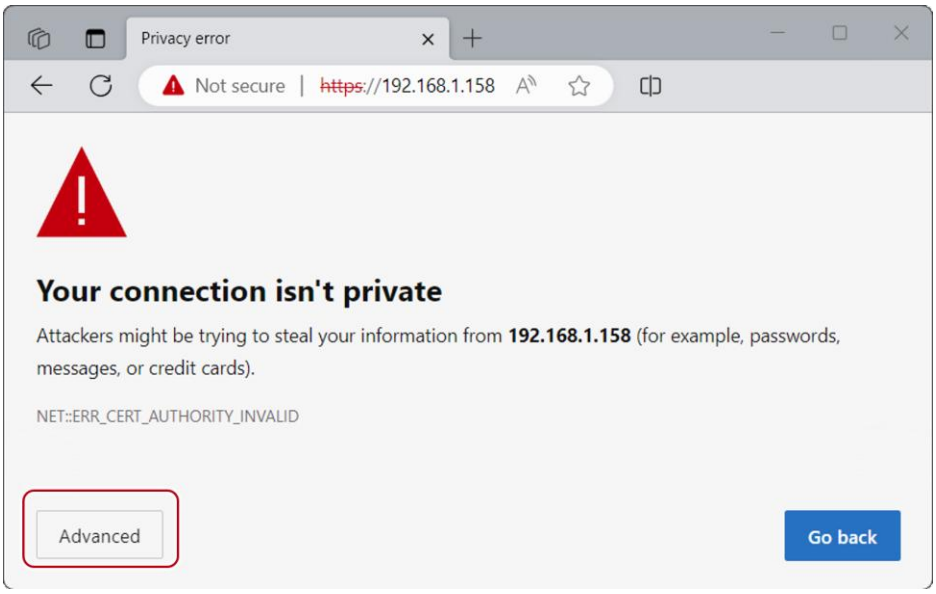


Figure 13: Dashboard Remote Access (1 of 2)

4. Click the link **Continue to dcxxxxxxxxxx (unsafe)**

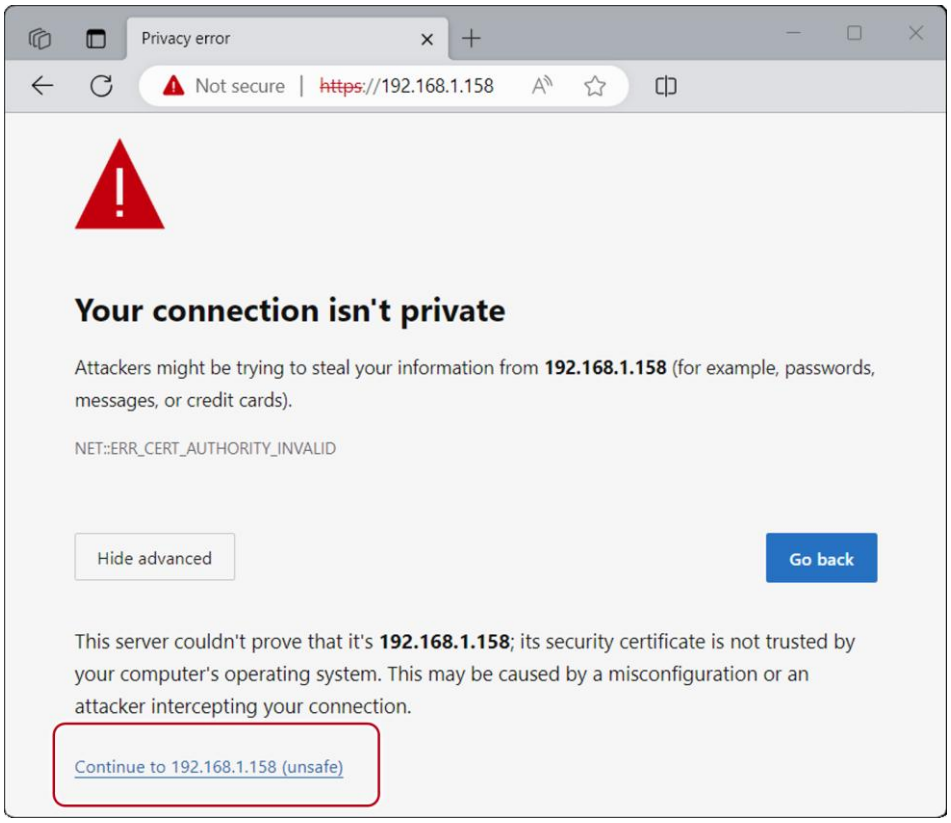


Figure 14: Dashboard Remote Access (2 of 2)

2.6 Dashboards

The Dashboards shows overall information about the ECA machine and some of its system vitals. The information is summarized in a card style display.

Example of information and status display in the Dashboards are:

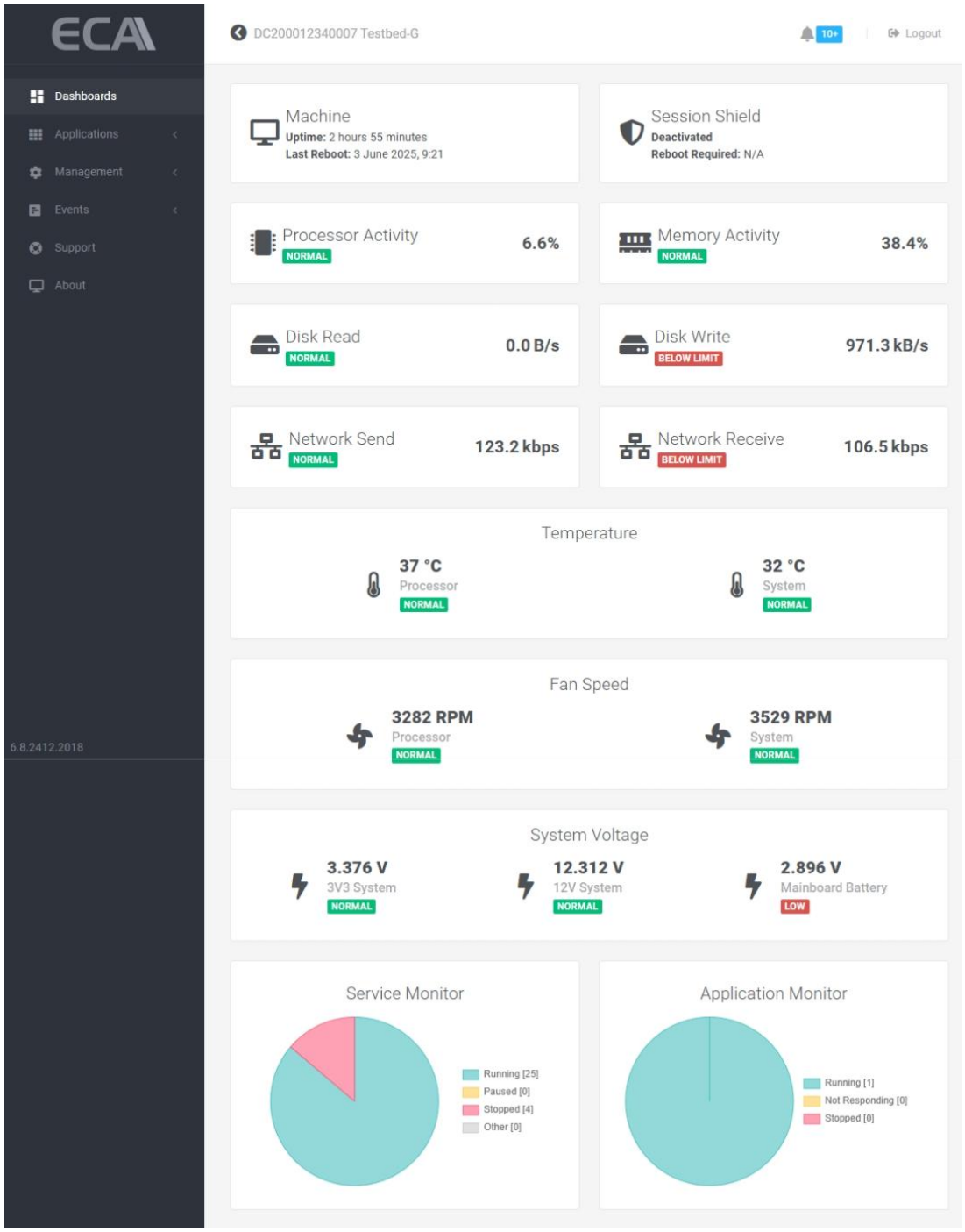


Figure 15: ecaOS Dashboards

Figure 16: ecaOS Dashboards – Disk Health

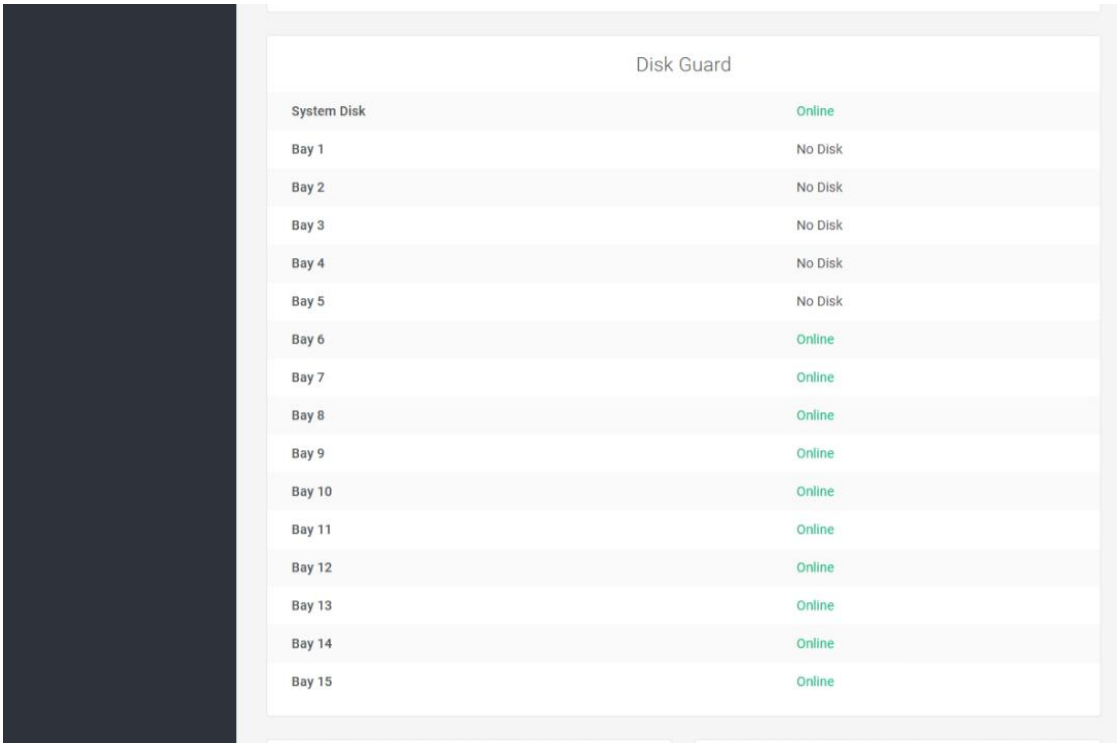


Figure 17: ecaOS Dashboards – Disk Guard

8 Applications

8.1 System Monitor

System Monitor provides users with real-time information on Processor Temperature, Mainboard Temperature, PSU Temperature*, Processor and System Fan Speeds, as well as 3.3V System Voltage, 12V System Voltage, and Mainboard Battery Voltage.

*Only applicable to ECA4.5 and above, with TBSP-ECAPSE-R600 power supply unit (PSU).

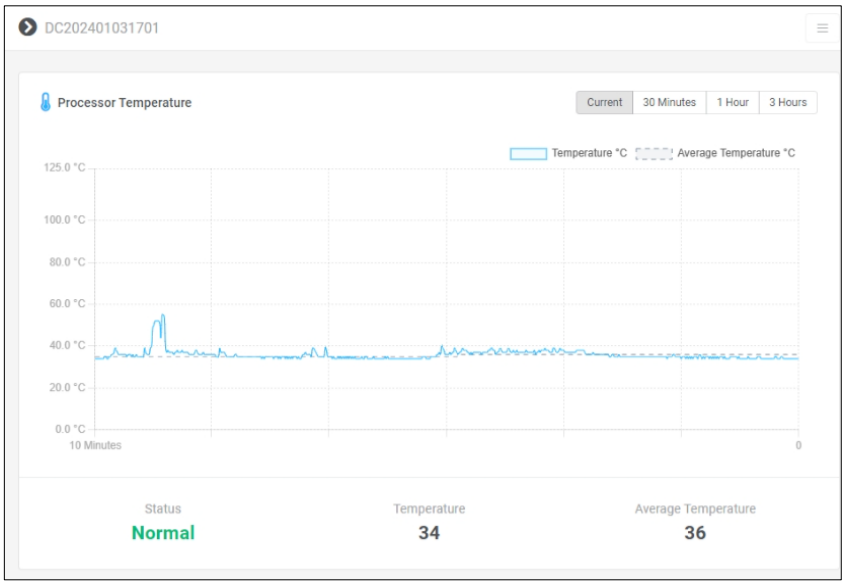


Figure 18: Processor Temperature monitor

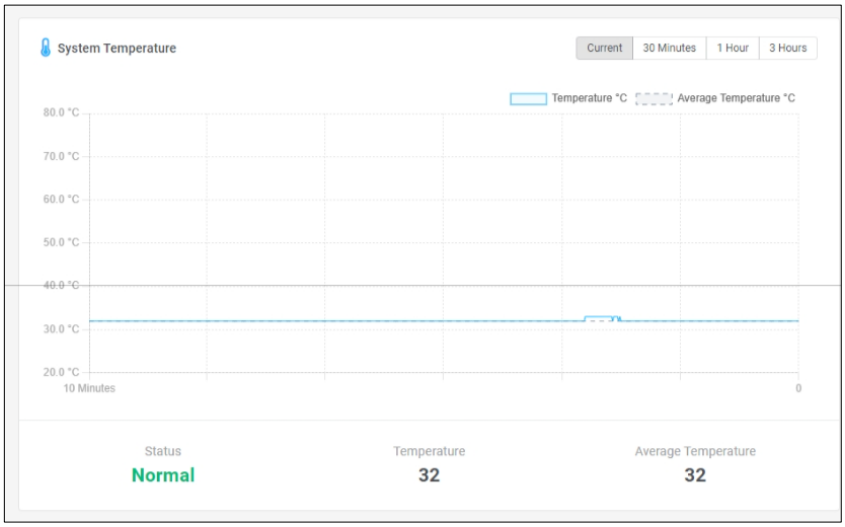


Figure 19: System Temperature monitor

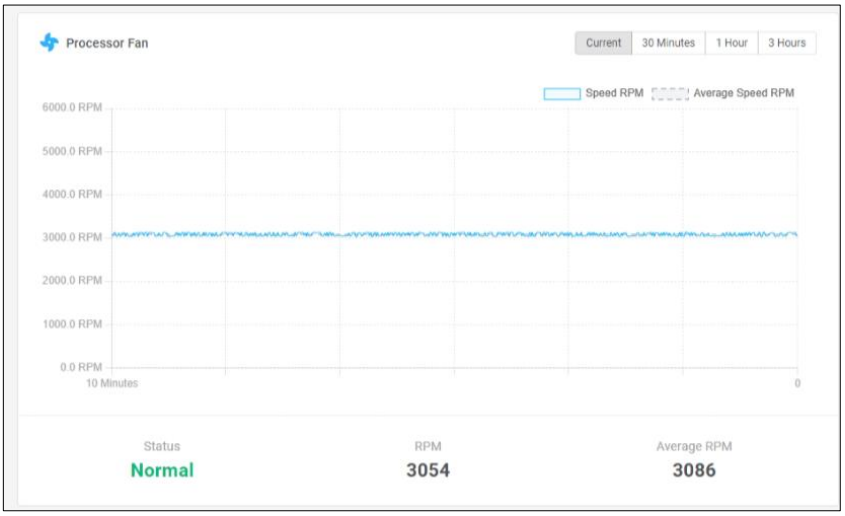


Figure 20: Processor Fan monitor

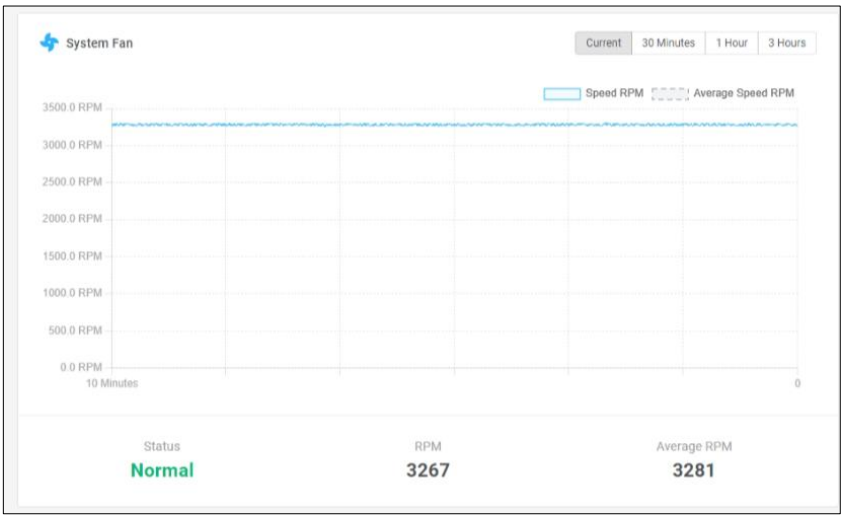


Figure 21: System Fan monitor

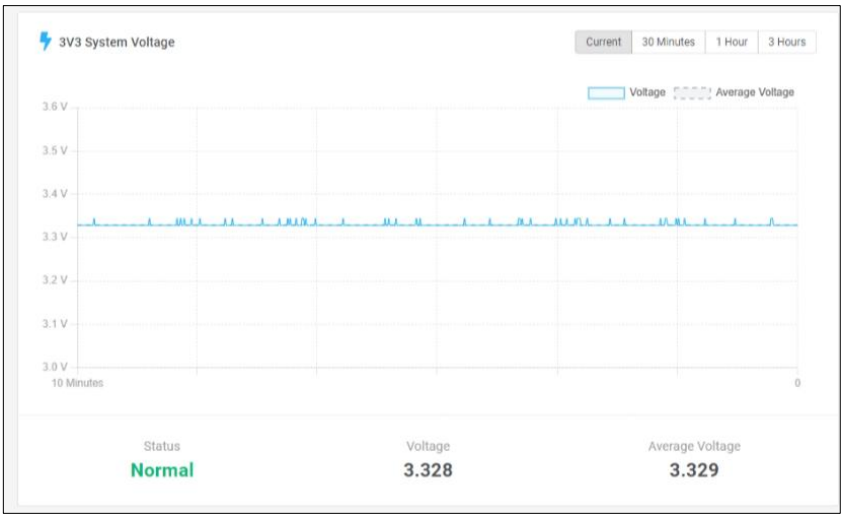


Figure 22: 3V3 System Voltage monitor

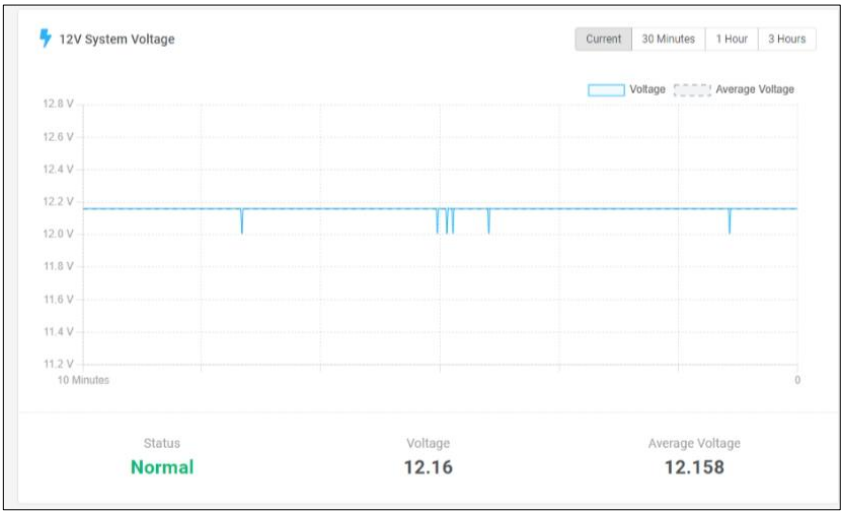


Figure 23: 12V System Voltage Monitor

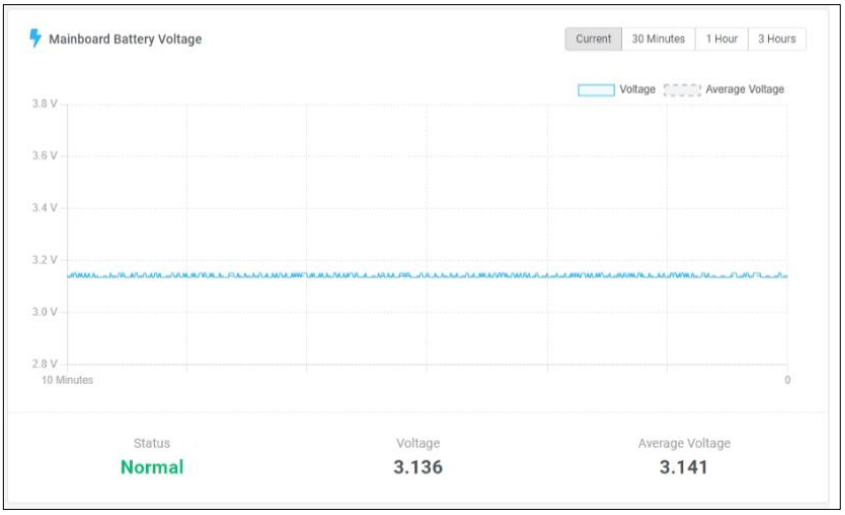


Figure 24: Mainboard Battery Voltage monitor

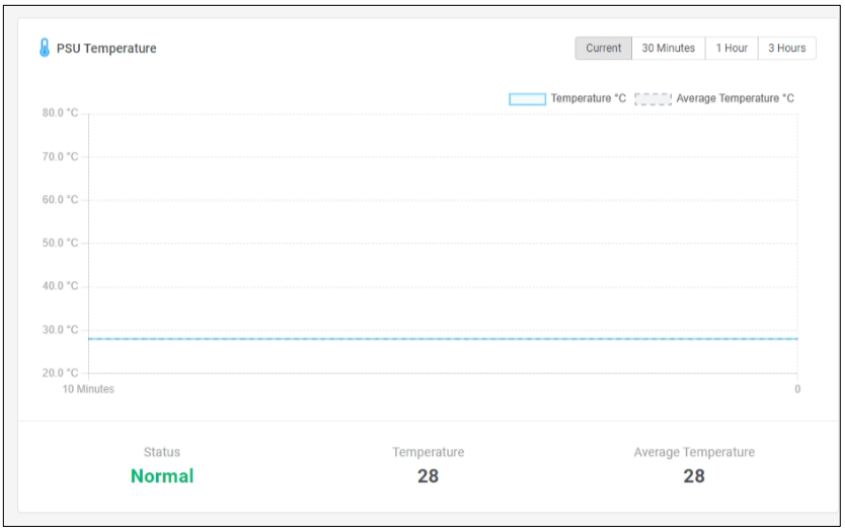


Figure 25: PSU Temperature monitor* (only applicable with TBSP-ECAPSE-R600 PSU.

8.2 App Monitor

The App Monitor displays the status of applications tracked by the Application Monitor, as well as services within ecaOS that have been included in the Service Monitor.

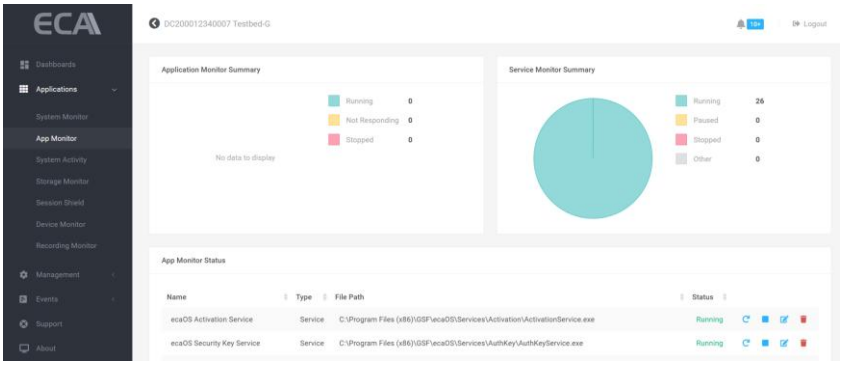


Figure 26: Service Monitor Summary

8.2.1 Add Application

1. To add application, click the Add Application button.

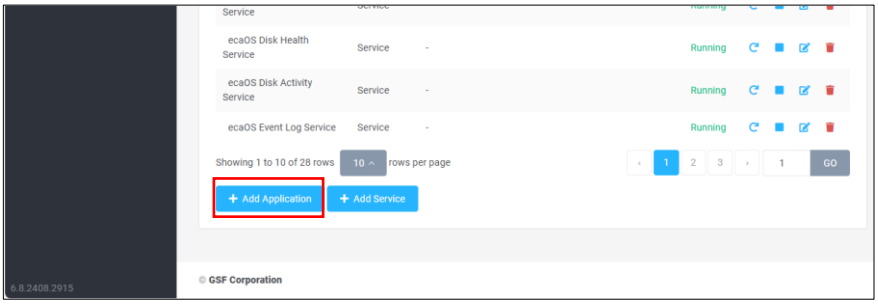


Figure 27: Add Applications

2. Enter the application name

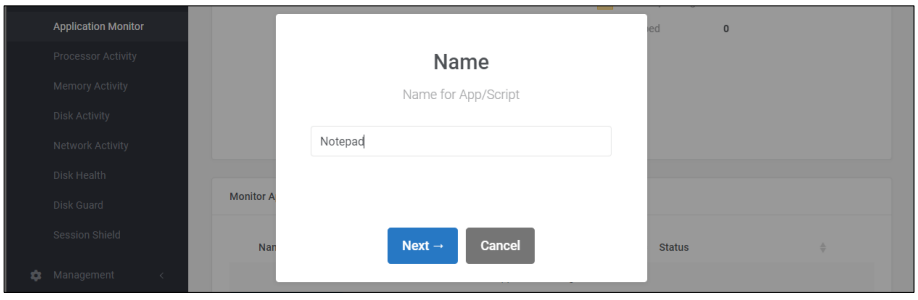


Figure 28: Application Monitor (1 of 4)

3. Insert the path to the application to be added. Then, press **Next**.

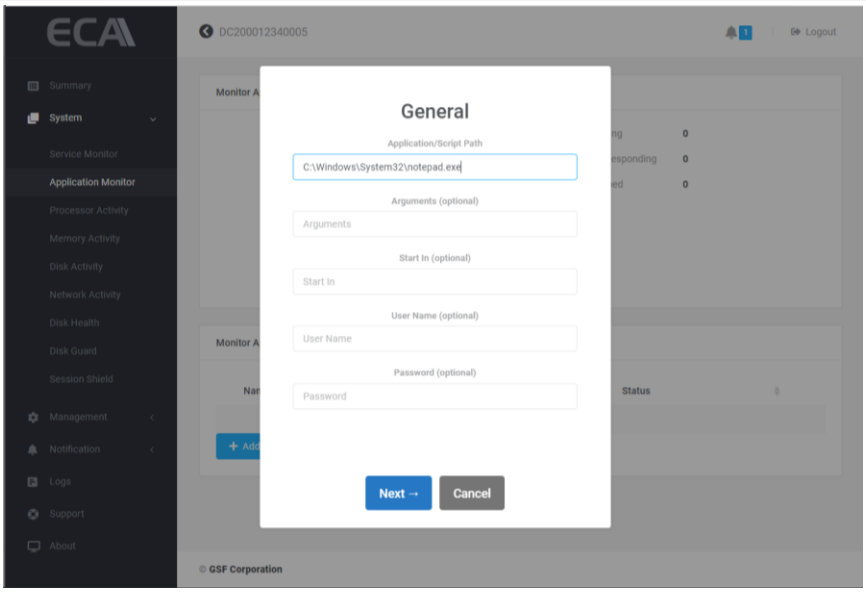


Figure 29: Application Monitor (2 of 4)

4. Apply setting

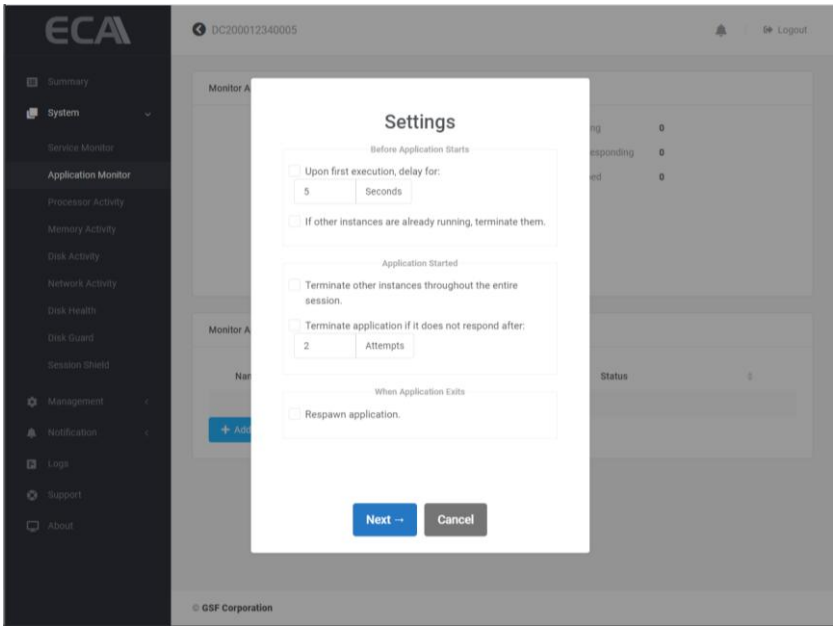


Figure 30: Application Monitor (3 of 4)

Settings	What it does
Upon first execution delay for	Set the delay before starting the application
If other instance(s) are already running, terminate them	If another instance of the same application is already started (not by Application Manager) terminate that instance.
Terminate other instance(s) throughout the entire session	If another instance attempts to start again after the Application Monitor has started the application, terminate it. This prevents duplicated instance.
Terminate application if it does not respond after __ attempts	If the application does not respond after the number of attempts specified, the Application Monitor will terminate it.
Respawn application	The Application Monitor will respawn the application if it is not running, or if it is closed. This ensures the application is always running.

5. Once the application has been successfully added, its status will appear on the 'Application Monitor'

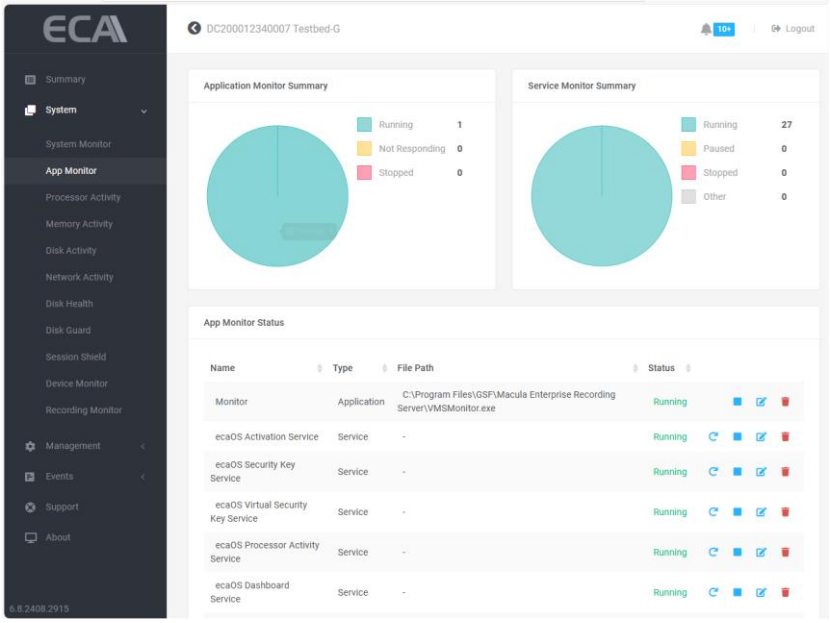


Figure 31: Application Monitor (4 of 4)

8.2.2 Delete Application

1. To delete application to be monitor, click the button of the application to be delete

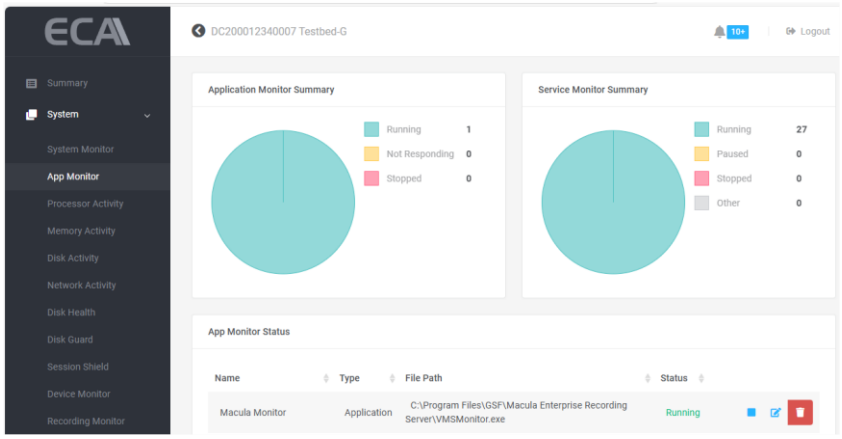


Figure 32: Delete monitored application (1 of 2)

2. Click on to proceed with the deletion

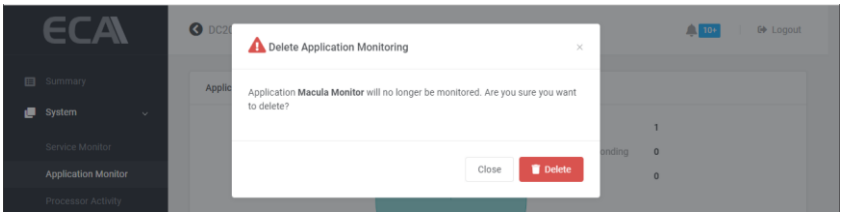


Figure 33: Delete monitored application (2 of 2)

8.2.3 Add Services

1. To add services, click the Add Service button.

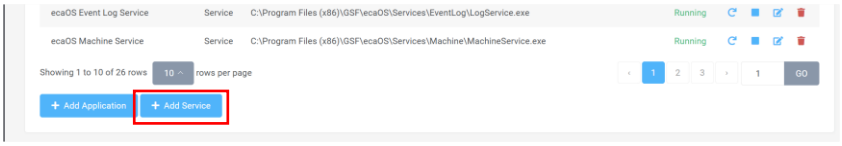


Figure 34: Add Services

2. Click the drop-down button.

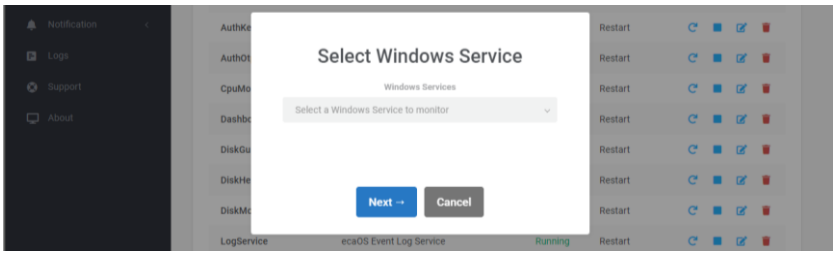


Figure 35: Select Windows Services (1 of 4)

3. Select the services to be added into Service Monitor.

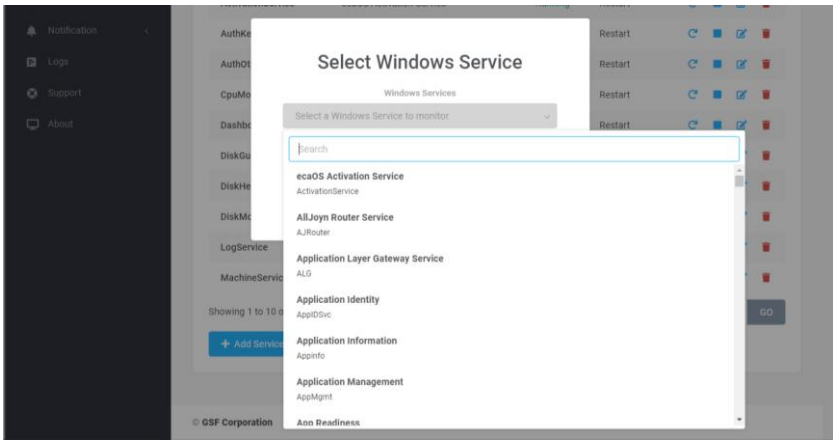
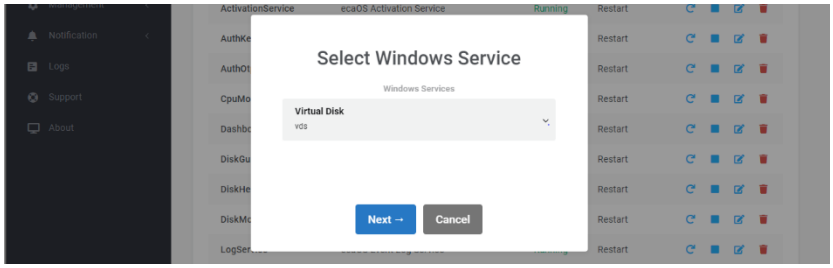


Figure 36: Select Windows Services (2 of 4)

4. Click Next → button



5. Select the actions that Service Monitor should perform when the services stop working. Click Save to save the setting.

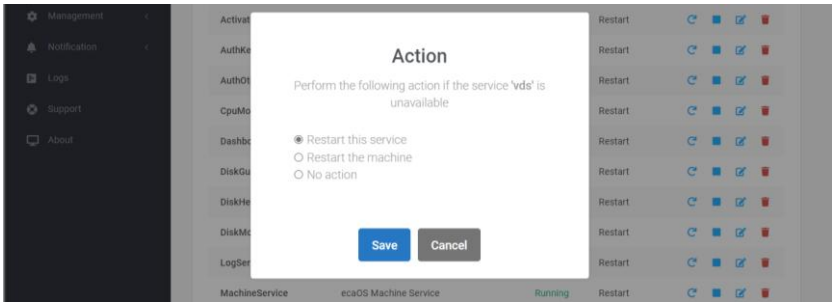


Figure 37: Select Windows Services (4 of 4)

8.2.4 Delete Services

1. To delete services, click the button of the service to be deleted.

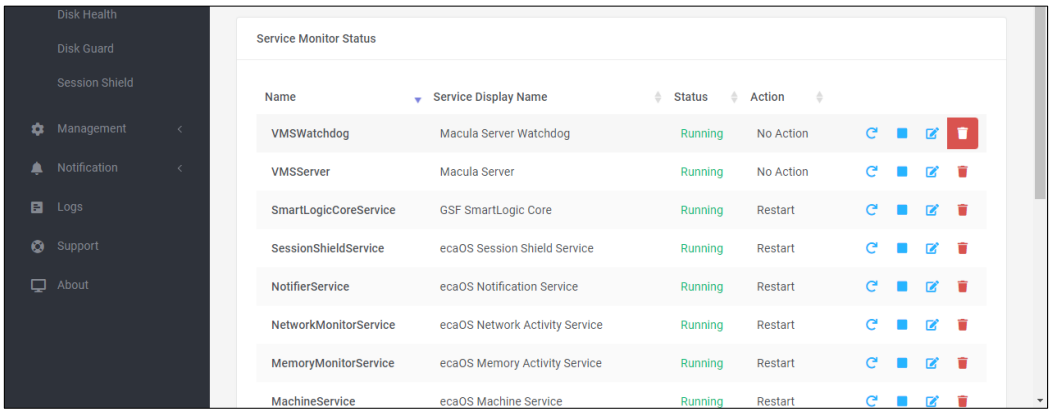


Figure 38: Delete Services (1 of 2)

2. Click on Delete to proceed with the deletion.

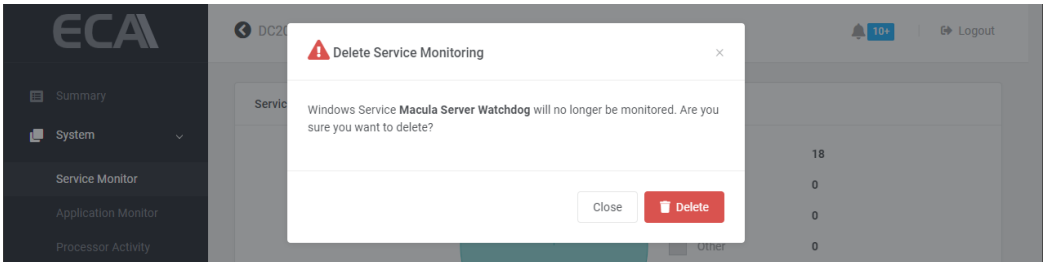


Figure 39: Delete Services (2 of 2)

8.3 System Activity

8.3.1 Processor Activity

Processor Activity monitors CPU usage and notify via email when the usage above the threshold value.

ecaOS can generate notification to alert users, when ECA CPU Alert utilization goes above the configured threshold for a pre-defined period.

Average Utilization ❶: The status will be based on Average CPU Utilization. The status will change to **High** if average CPU Utilization exceeds the threshold set under **Processor Activity Monitor ❷**.

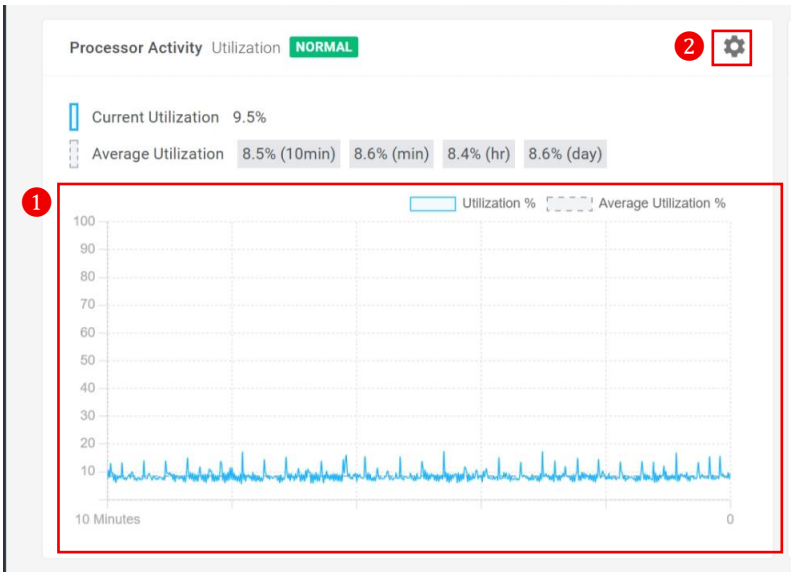


Figure 40: Processor Activity (1 of 2)

The example below demonstrates the Processor Activity Monitor configured with a threshold of 50% over 10 minutes. If the average Processor utilization exceeds 50% for more than 10 minutes, the CPU activity status will change to "High." This event will trigger an email notification and an alert in the notifications panel.

Figure 41: Processor Activity (2 of 2)

NOTE:

- Click on **Use Suggested** for recommended value calculated by the system based on real-time usage.

- For email and notification setting, go to Settings
- Sample email of the Processor activity event can be found in the Appendix Processor Activity

8.3.2 Memory Activity

Monitor the memory usage and notify/email if the usage above the threshold value. ecaOS can generate notification to alert users when ECA Memory utilization goes above the configured threshold for a pre-defined period.

Memory Activity: The status will be based on Average Memory Usage. The status will change to High if the Average Memory Usage is higher than threshold set under Memory Activity Monitor.

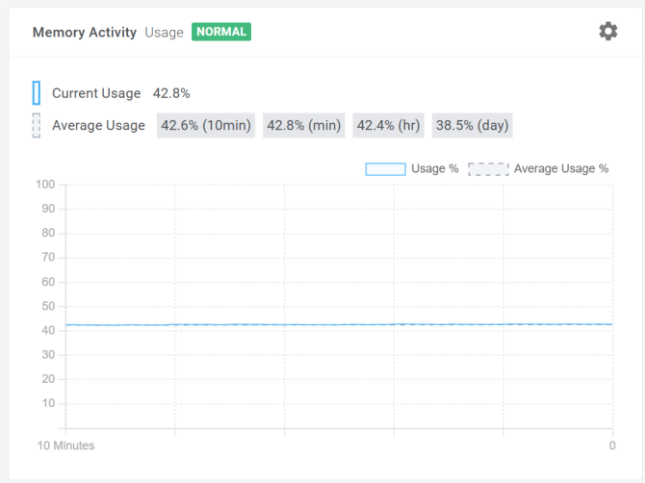


Figure 42: Memory Activity (1 of 2)

The example below to demonstrate that the Memory Activity Monitor set to enable, the threshold set to 50% for 5 minutes. The Memory Activity status will change to High if the Average Memory Utilization is higher than 50% for more than 5 minutes. This event will be notified by email and at the notification.

Figure 43: Memory Activity (2 of 2)

NOTE:

- Click on ‘Use Suggested’ for reference value calculated by the system.

- For email and notification setting, go to Settings
- Example email of the Memory activity event in the Appendix Memory Activity

© GSF Corporation
Unit 21, Level 3A, Jalan Kenari 5, Bandar Puchong Jaya, 47170 Selangor D.E., Malaysia | +603-80908080 | info@gsfcorp.com

8.3.3 Disk Activity

Disk Activity provides real-time monitoring of disk usage, tracking average activity per minute, hour, and day. It includes automatic alerts if disk read or write activity deviates above or below predefined threshold limits for a specified duration. This feature is particularly useful for detecting issues such as accidental deactivation of the recording function in VMS software. When recording is turned off, disk writing ceases, prompting the system to alert users of potential CCTV recording interruptions.

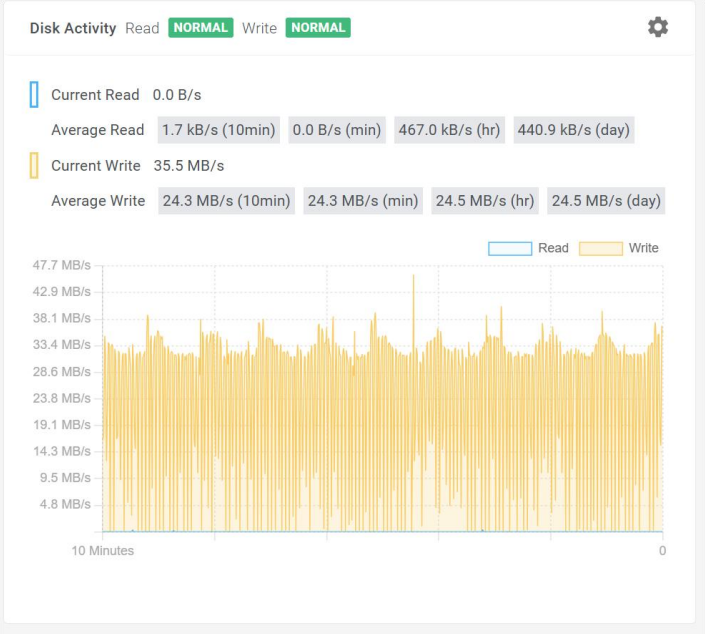


Figure 44: Disk Activity (1 of 2)

The following example demonstrates the configuration of the Disk Activity Monitor for both read and write operations.

The average disk read threshold is set to exceed 1 MB/s for 5 minutes, while the average disk write threshold is configured to drop below 22 MB/s for the same duration. If these thresholds are exceeded, the system will send a notification via email and display an alert in the notification panel.

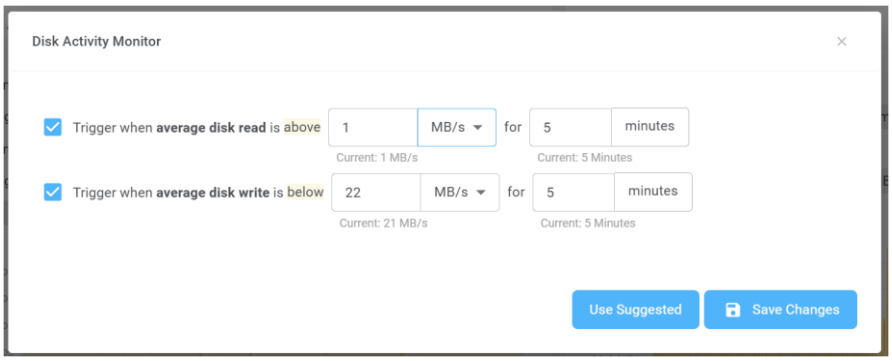


Figure 45: Disk Activity (2 of 2)

NOTE:

- Click on ‘Use Suggested’ for reference value calculated by the system.
- For email and notification setting, go to Settings
- Example email of the Disk activity event in the Appendix Disk Activity

8.3.4 Network Activity

Network Activity displays real time network usage activity. It can automatically calculate average network utilization per minute, per hour or per day. This average value is important for the estimation and observation of network utilization, as incoming throughput from the network cameras or video sources varies throughout the day, where daytime throughput is usually higher than nighttime.

Automatic alert if network received or sending is fall or raise above threshold limit for a period of time. This is very useful if some of the cameras was accidentally offline due to faulty PoE switch.

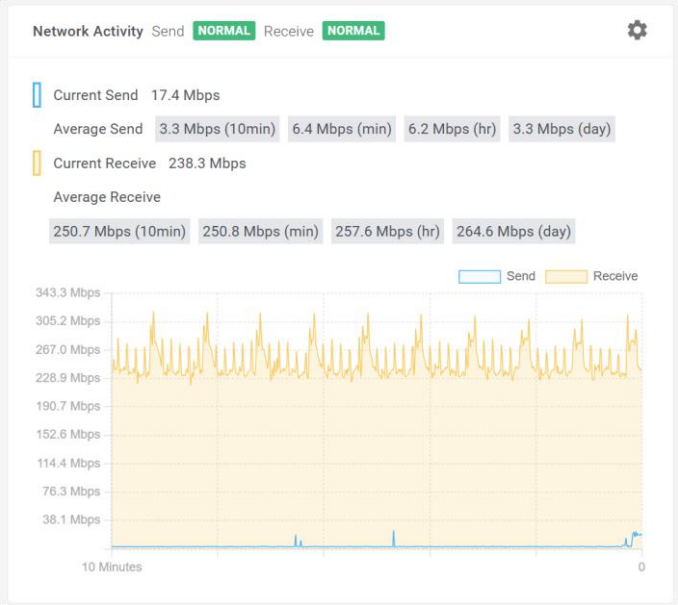


Figure 46: Network Activity (1 of 2)

By the example below to demonstrate that the Network Activity set to trigger email & desktop notifications.

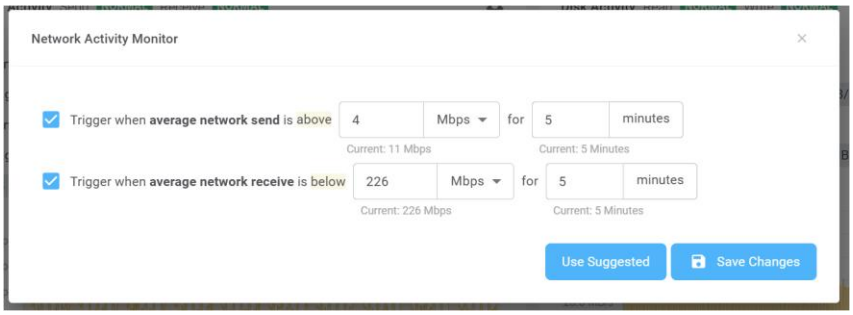


Figure 47: Network Activity (2 of 2)

It will trigger when the data send over network above 4 Mbps for 5 minutes

It will trigger when the data receive below set threshold 226 Mbps for 5 minutes

NOTE:

- Click on ‘Use Suggested’ for reference value calculate by the system.
- For email and notification setting, go to Settings
- Example email of the Network activity event in the Appendix Network Activity

8.4 Storage Monitor

The "Storage Monitor" can provide details about every disk that is connected to the ECA.

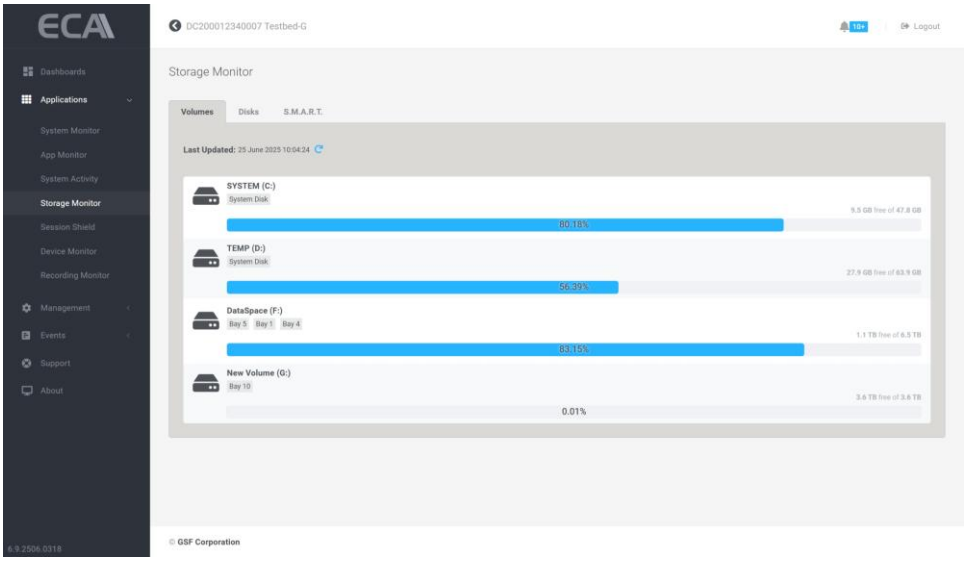


Figure 48: Storage Monitor

8.4.1 Volumes

All of the available volumes will be placed here under the Volumes tab.

In figure 60, showing four volumes together with their respective usage bars. DataSpace (F:) is an RSS storage, it spans across Bays 1, 4, and 5, and already consumed 83.15% of its available space. New Volume (G:) is located in Bay 10 and currently unused.

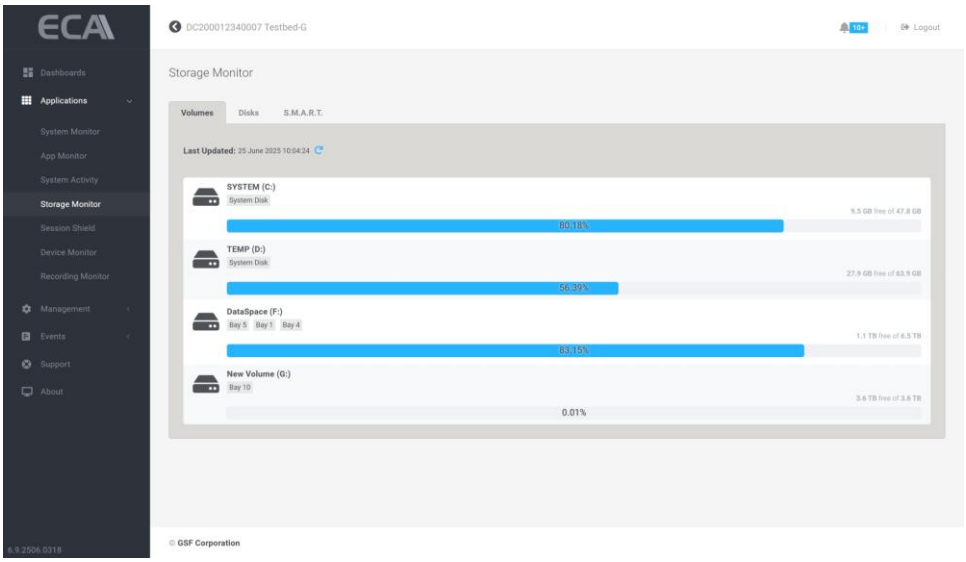


Figure 49: Storage Monitor – Volumes

8.4.2 Disks

Display status all connected hard disk to the ECA.

HDD stores important video evidence data. It is important to ensure the data remains intact in the ECA. HDD insertion and removal events on the ECA are tracked by Storage Monitor. Additionally, it keeps track of disk health and alerts users when it falls below a predetermined threshold.

Details about the disk in the Disks tab:

- HDD Model, Serial number, Firmware
- HDD Status, Temperature, Power up time
- HDD volume information
- Disk Guard status
    - **Online:** Hard disk installed. Using by OS
    - **Offline:** Hard disk installed. Not using by OS
    - **No Disk:** No hard disk installed.
    - **Removed:** Previous hard disk has been removed.
    - **Replaced:** Hard disk has been replaced with different serial number.

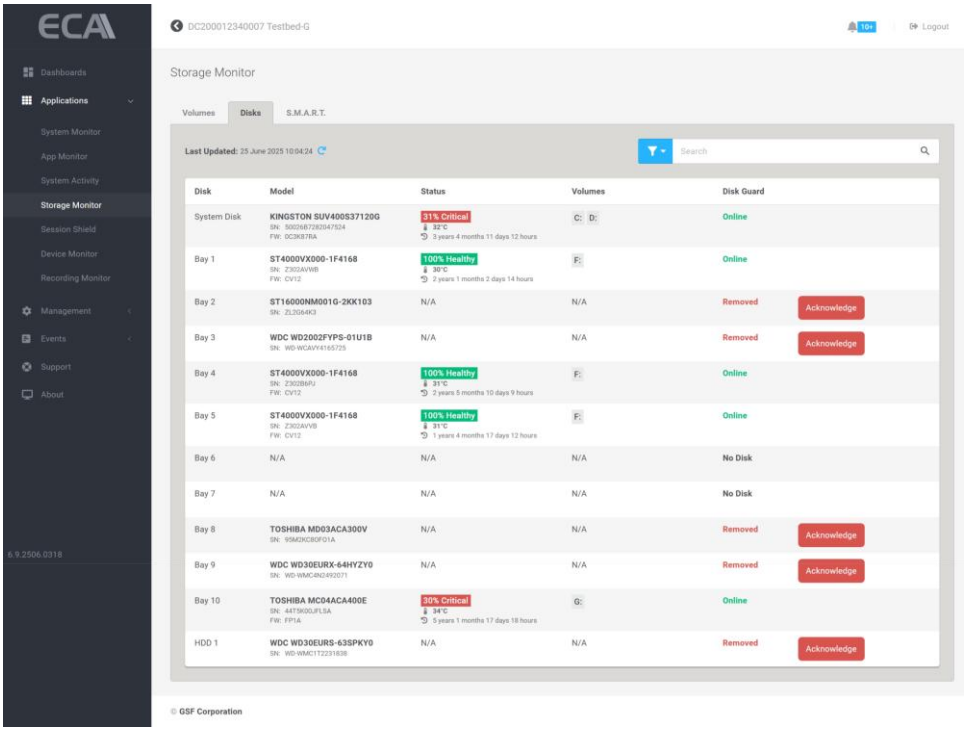


Figure 50: Storage Monitor – Disks

Disk list shown depending on the ECA model:

- ECA-FX46: System Disk, Bay 1 – Bay 15
- ECA-EX46: System Disk, Bay 1 – Bay 10 & HD1
- ECA-DX46: System Disk, Bay 1 – Bay 5, HDD1, HDD 2
- ECA-MX46: System Disk, HDD1, HDD 2
- ECA-VW44: System Disk, HDD1, HDD 2

NOTE:

- System Disk is the drive containing operating system.

- Hard disks insert in the hotswap bay will label shows as a ‘Bay’.
- Internal hard disk will label HDD1 & HDD2 is for the internal hard disk.
- When hard disk removed, the hard disk information still shown with ‘Removed’ status. Acknowledge the removed hard disk will change to latest status.

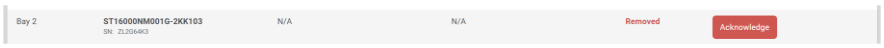


Figure 51: Disk removed

8.4.3 S.M.A.R.T.

Under S.M.A.R.T (Self-Monitoring, Analysis and Reporting Technology), will display S.M.A.R.T value. Its primary function is to detect and report various indicators of drive reliability with the intent of anticipating imminent hardware failures.

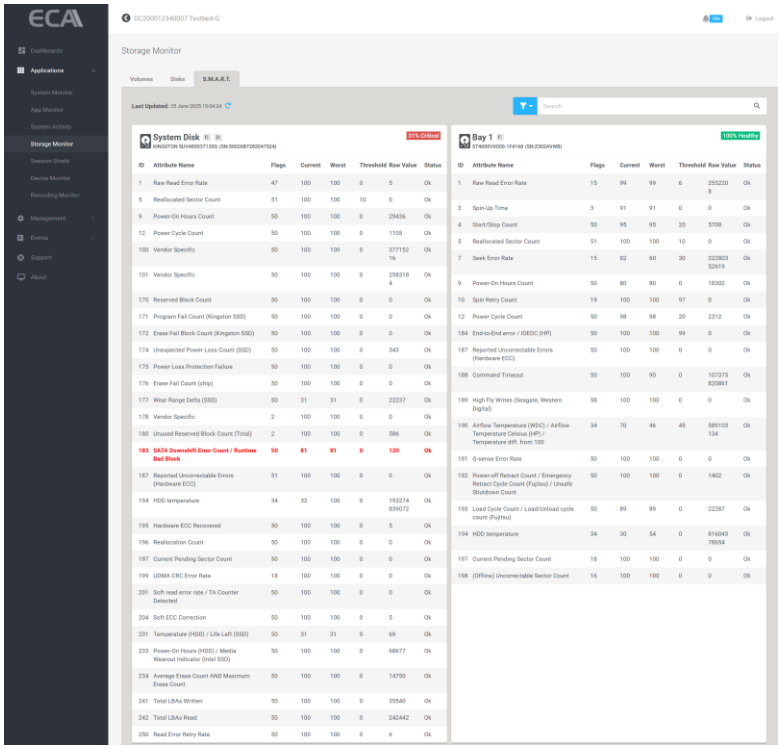


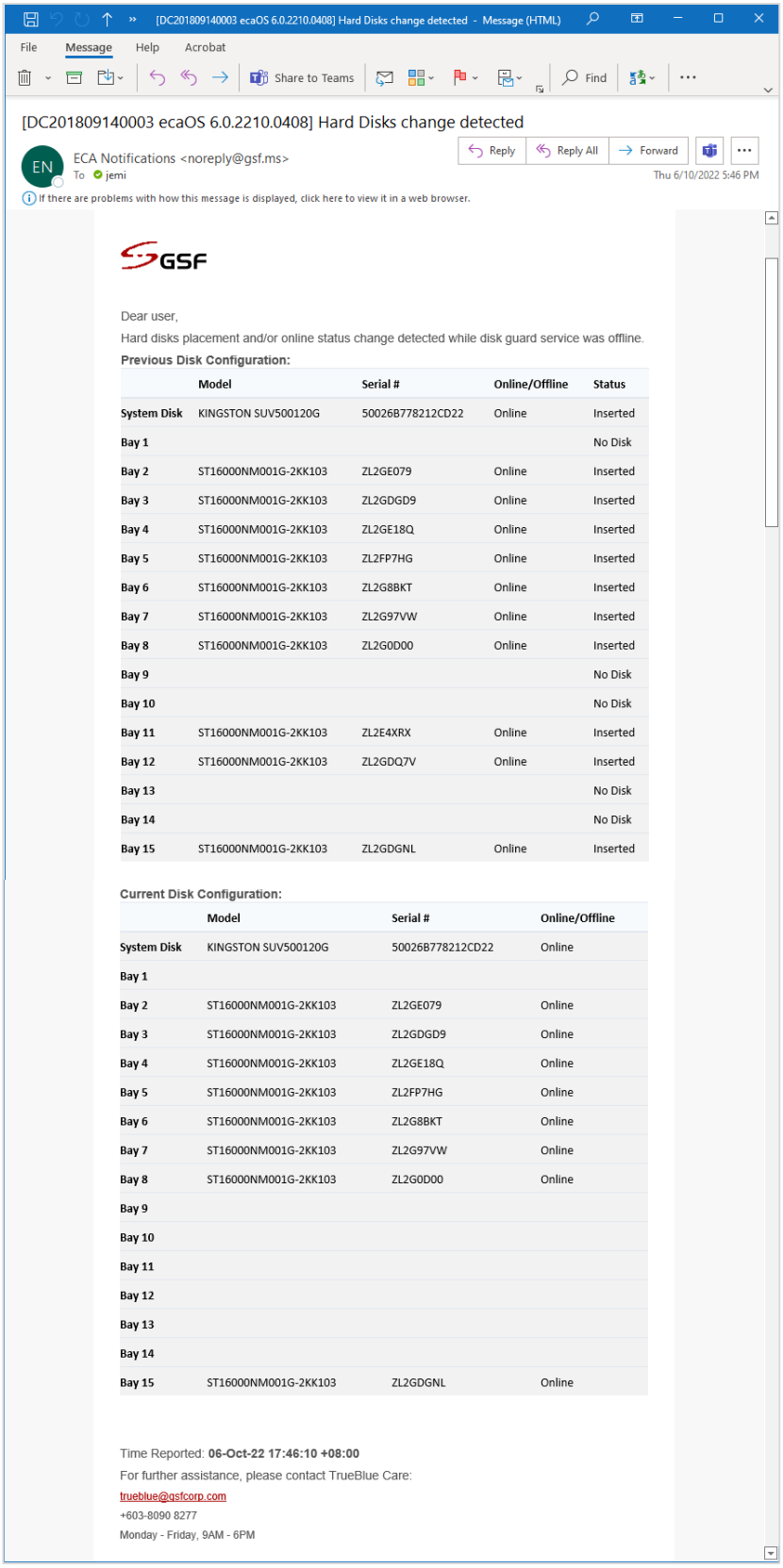
Figure 52: Storage Monitor – S.M.A.R.T.

NOTE:

- For email and notification setting, go to Settings
- Example email of the Disk Health event in the Appendix Disk Health
- Example email of the Disk Guard event in the Appendix Disk Guard

8.4.4 Hard disk change during ECA Power Off

Dashboard will be sending notification via email to inform there is hard disk changing during ECA off stage (power off). This feature is part of Disk Guard, to protect the Data/Evidence, ensure the same serial number was in the ECA machine before and after power on.



[DC201809140003 ecaOS 6.0.2210.0408] Hard Disks change detected - Message (HTML)

File Message Help Acrobat

Share to Teams Find

[DC201809140003 ecaOS 6.0.2210.0408] Hard Disks change detected

EN ECA Notifications <noreply@gsf.ms>
To jemi

Reply Reply All Forward

Thu 6/10/2022 5:46 PM

If there are problems with how this message is displayed, click here to view it in a web browser.

GSF

Dear user,

Hard disks placement and/or online status change detected while disk guard service was offline.

Previous Disk Configuration:

	Model	Serial #	Online/Offline	Status
System Disk	KINGSTON SUV500120G	50026B778212CD22	Online	Inserted
Bay 1				No Disk
Bay 2	ST16000NM001G-2KK103	ZL2GE079	Online	Inserted
Bay 3	ST16000NM001G-2KK103	ZL2GDGD9	Online	Inserted
Bay 4	ST16000NM001G-2KK103	ZL2GE18Q	Online	Inserted
Bay 5	ST16000NM001G-2KK103	ZL2FP7HG	Online	Inserted
Bay 6	ST16000NM001G-2KK103	ZL2G8BKT	Online	Inserted
Bay 7	ST16000NM001G-2KK103	ZL2G97VW	Online	Inserted
Bay 8	ST16000NM001G-2KK103	ZL2G0D00	Online	Inserted
Bay 9				No Disk
Bay 10				No Disk
Bay 11	ST16000NM001G-2KK103	ZL2E4XRX	Online	Inserted
Bay 12	ST16000NM001G-2KK103	ZL2GDQ7V	Online	Inserted
Bay 13				No Disk
Bay 14				No Disk
Bay 15	ST16000NM001G-2KK103	ZL2GDGNL	Online	Inserted

Current Disk Configuration:

	Model	Serial #	Online/Offline
System Disk	KINGSTON SUV500120G	50026B778212CD22	Online
Bay 1			
Bay 2	ST16000NM001G-2KK103	ZL2GE079	Online
Bay 3	ST16000NM001G-2KK103	ZL2GDGD9	Online
Bay 4	ST16000NM001G-2KK103	ZL2GE18Q	Online
Bay 5	ST16000NM001G-2KK103	ZL2FP7HG	Online
Bay 6	ST16000NM001G-2KK103	ZL2G8BKT	Online
Bay 7	ST16000NM001G-2KK103	ZL2G97VW	Online
Bay 8	ST16000NM001G-2KK103	ZL2G0D00	Online
Bay 9			
Bay 10			
Bay 11			
Bay 12			
Bay 13			
Bay 14			
Bay 15	ST16000NM001G-2KK103	ZL2GDGNL	Online

Time Reported: **06-Oct-22 17:46:10 +08:00**

For further assistance, please contact TrueBlue Care:

trueblue@gsfcorp.com

+603-8090 8277

Monday - Friday, 9AM - 6PM

Figure 53: Hard Disks change detected (1 of 1)

8.5 Session Shield

Session shield 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.

Total size availability will be half of the amount of the RAM.

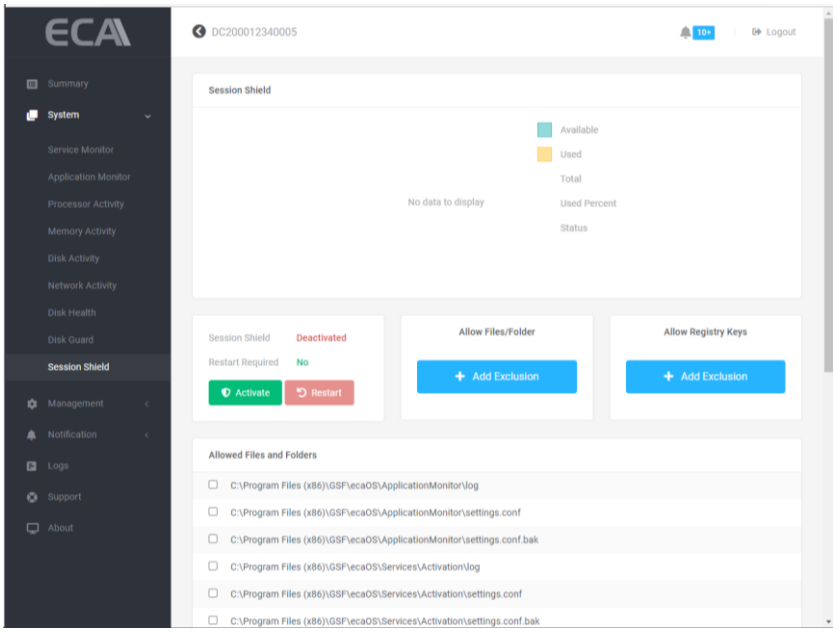


Figure 54: Session Shield

8.5.1 Activate Session Shield

All setting/files in the ‘C:\’ will be protected. All setting/files will be return to its original state after reboot the ECA.

1. Click on ‘Activate’

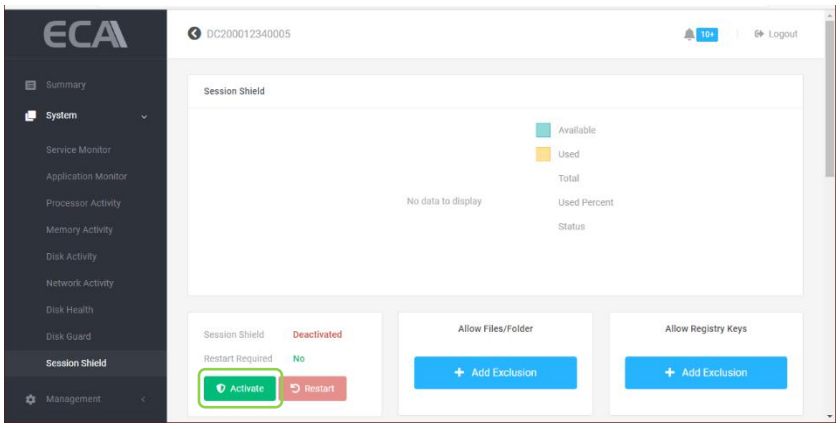


Figure 55: Activate Session Shield (1 of 5)

2. Click ‘Change Settings’ to save the setting

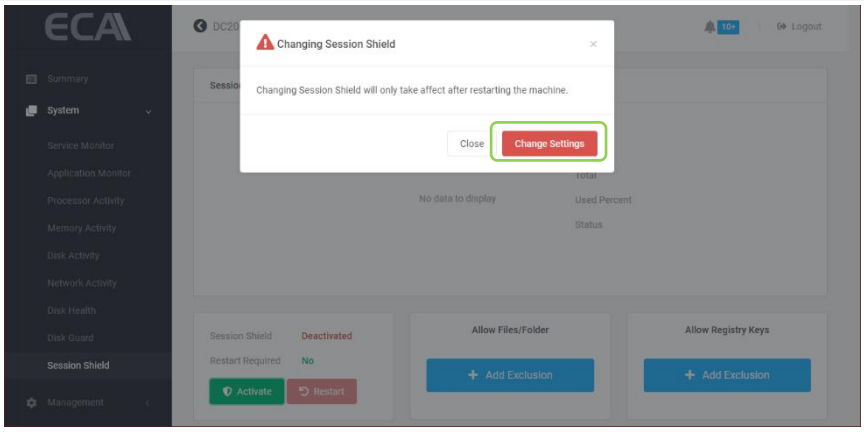


Figure 56: Activate Session Shield (2 of 5)

3. Click ‘Restart’ to reboot ECA and apply the setting.

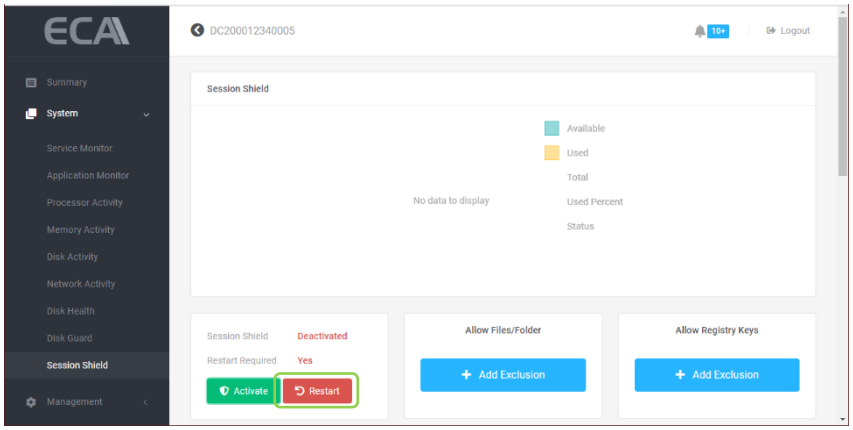


Figure 57: Activate Session Shield (4 of 6)

4. Type Restart then click ‘Restart’ button

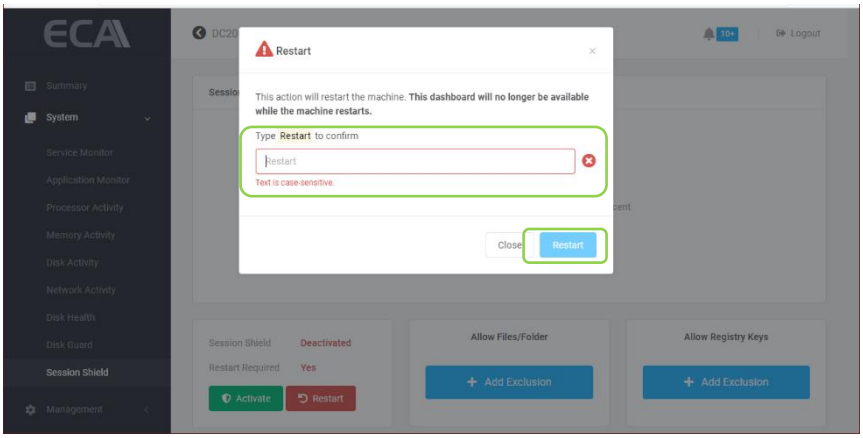


Figure 58: Activate Session Shield (5 of 6)

5. Once the Session Shield successfully activated. The Session Shield information shown as below

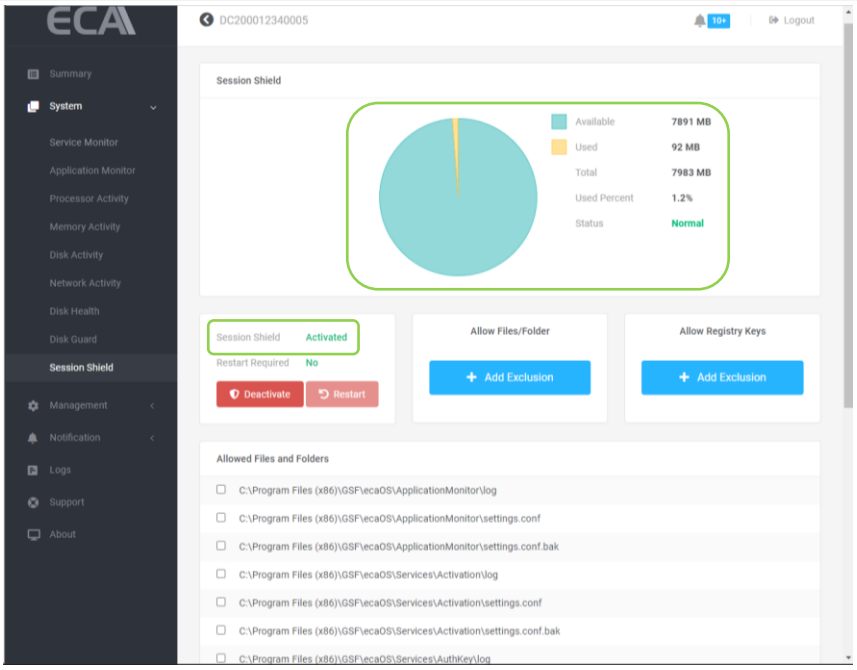


Figure 59: Activate Session Shield (6 of 6)

8.5.2 Deactivate Session Shield

All setting/files in the 'C:\' will not be protected. All files setting will be permanently written.

1. Click on 'Deactivate'

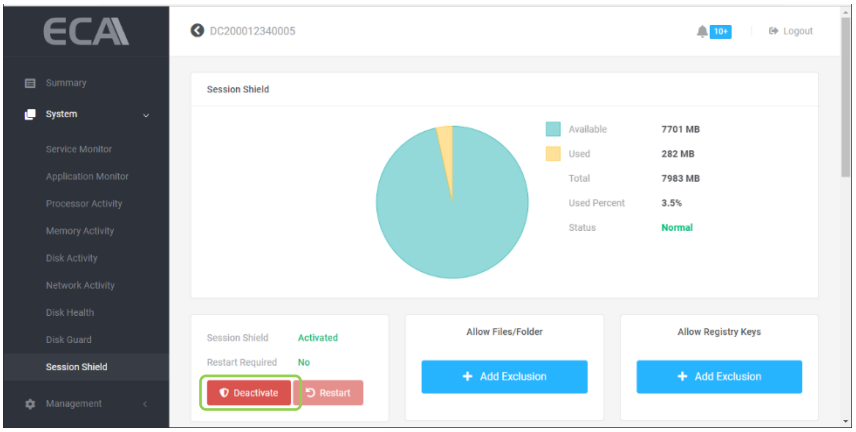


Figure 60: Deactivate Session Shield (1 of 3)

2. Click 'Change Settings' to save the setting

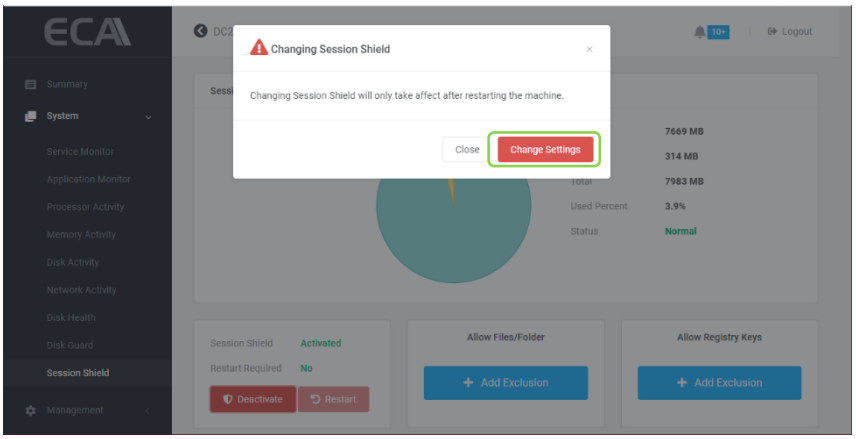


Figure 61: Deactivate Session Shield (2 of 3)

3. Click 'Restart' to reboot ECA and apply the setting

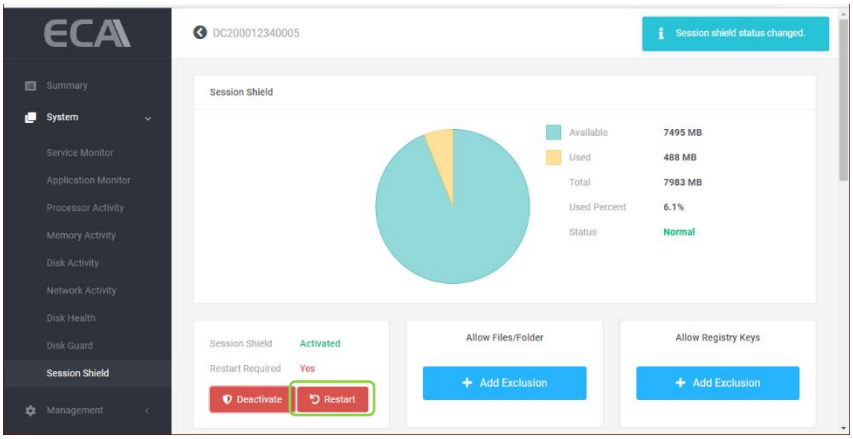


Figure 62: Deactivate Session Shield (2 of)

4. Type Restart then click 'Restart' button

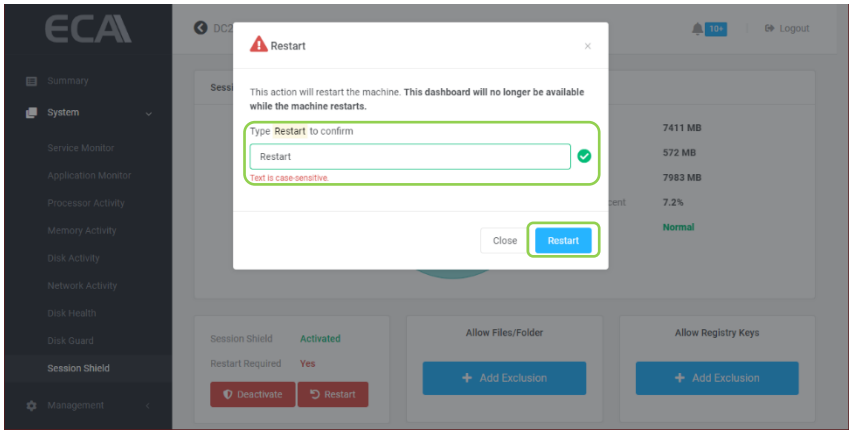


Figure 63: Deactivate Session Shield (3 of 3)

8.5.3 Exclusion List

All paths below will not be affected when Session Shield is activated. The data destined to these paths will be able to pass-through and written permanently:

```
C:\Program Files (x86)\GSF\ecaOS\ProcessMonitor\log
C:\Program Files (x86)\GSF\ecaOS\ProcessMonitor\settings.conf
C:\Program Files (x86)\GSF\ecaOS\ProcessMonitor\settings.conf.bak
C:\Program Files (x86)\GSF\ecaOS\Services\Activation\log
C:\Program Files (x86)\GSF\ecaOS\Services\Activation\settings.conf
C:\Program Files (x86)\GSF\ecaOS\Services\Activation\settings.conf.bak
C:\Program Files (x86)\GSF\ecaOS\Services\AuthKey\log
C:\Program Files (x86)\GSF\ecaOS\Services\AuthKey\settings.conf
C:\Program Files (x86)\GSF\ecaOS\Services\AuthKey\settings.conf.bak
C:\Program Files (x86)\GSF\ecaOS\Services\AuthOtp\log
C:\Program Files (x86)\GSF\ecaOS\Services\AuthOtp\settings.conf
C:\Program Files (x86)\GSF\ecaOS\Services\AuthOtp\settings.conf.bak
C:\Program Files (x86)\GSF\ecaOS\Services\HB2Gateway\log
C:\Program Files (x86)\GSF\ecaOS\Services\HB2Gateway\settings.conf
C:\Program Files (x86)\GSF\ecaOS\Services\HB2Gateway\settings.conf.bak
C:\Program Files (x86)\GSF\ecaOS\Services\Log\log
C:\Program Files (x86)\GSF\ecaOS\Services\Log\settings.conf
C:\Program Files (x86)\GSF\ecaOS\Services\Log\settings.conf.bak
C:\Program Files\Microsoft SQL Server\MSSQL15.SQLEXPRESS\MSSQL\DATA
C:\Program Files (x86)\GSF\ecaOS\Services\Machine\log
C:\Program Files (x86)\GSF\ecaOS\Services\Machine\settings.conf
C:\Program Files (x86)\GSF\ecaOS\Services\Machine\settings.conf.bak
C:\Program Files (x86)\GSF\ecaOS\Services\WindowsServiceMonitor\log
C:\Program Files (x86)\GSF\ecaOS\Services\WindowsServiceMonitor\settings.conf
C:\Program Files (x86)\GSF\ecaOS\Services\WindowsServiceMonitor\settings.conf.bak
C:\Program Files (x86)\GSF\ecaOS\Services\SessionShield\log
C:\Program Files (x86)\GSF\ecaOS\Services\SessionShield\settings.conf
C:\Program Files (x86)\GSF\ecaOS\Services\SessionShield\settings.conf.bak
C:\Program Files (x86)\GSF\ecaOS\Services\CPUMonitor\log
C:\Program Files (x86)\GSF\ecaOS\Services\CPUMonitor\Db
C:\Program Files (x86)\GSF\ecaOS\Services\CPUMonitor\appsettings.cpu_activity.json
C:\Program Files (x86)\GSF\ecaOS\Services\MemoryMonitor\log
C:\Program Files (x86)\GSF\ecaOS\Services\MemoryMonitor\Db
C:\Program Files (x86)\GSF\ecaOS\Services\MemoryMonitor\appsettings.memory_activity.json
C:\Program Files (x86)\GSF\ecaOS\Services\NetworkMonitor\log
C:\Program Files (x86)\GSF\ecaOS\Services\NetworkMonitor\Db
C:\Program Files (x86)\GSF\ecaOS\Services\NetworkMonitor\appsettings.network_activity.json
C:\Program Files (x86)\GSF\ecaOS\Services\DiskMonitor\log
C:\Program Files (x86)\GSF\ecaOS\Services\DiskMonitor\Db
C:\Program Files (x86)\GSF\ecaOS\Services\DiskMonitor\appsettings.disk_activity.json
C:\Program Files (x86)\GSF\ecaOS\Services\DiskHealth\log
C:\Program Files (x86)\GSF\ecaOS\Services\DiskHealth\Db
C:\Program Files (x86)\GSF\ecaOS\Services\DiskHealth\appsettings.disk_health.json
C:\Program Files (x86)\GSF\ecaOS\Services\Support\log
C:\Program Files (x86)\GSF\ecaOS\Services\Support\Db
C:\Program Files (x86)\GSF\ecaOS\Services\Support\appsettings.support.json
C:\Program Files (x86)\GSF\ecaOS\Services\DiskGuard\log
C:\Program Files (x86)\GSF\ecaOS\Services\DiskGuard\Db
C:\Program Files (x86)\GSF\ecaOS\Services\Notifier\log
```

© GSF Corporation
Unit 21, Level 3A, Jalan Kenari 5, Bandar Puchong Jaya, 47170 Selangor D.E., Malaysia | +603-80908080 | info@gsfcorp.com

```
C:\Program Files (x86)\GSF\ecaOS\Services\Notifier\Db
C:\Program Files (x86)\GSF\ecaOS\Services\Dashboard\log
C:\Program Files (x86)\GSF\ecaOS\Services\Dashboard\Db
C:\Program Files (x86)\GSF\ecaOS\Services\Dashboard\appsettings.json
C:\Windows\System32\config\systemprofile\AppData\Roaming\.smartlogic
C:\Program Files\Windows Defender
C:\ProgramData\Microsoft\Windows Defender
C:\Windows\WindowsUpdate.log
C:\Windows\System32\winevt\Logs
C:\Windows\Logs
C:\Windows\assembly
C:\Windows\SoftwareDistribution
C:\Windows\MEMORY.DMP
C:\Users\localadmin\Desktop
C:\Users\localadmin\Documents
C:\Users\localadmin\Downloads
C:\Users\localadmin\Music
C:\Users\localadmin\Pictures
C:\Users\localadmin\Videos
C:\Program Files (x86)\GSF\ecaOS\ApplicationMonitor\log
C:\Program Files (x86)\GSF\ecaOS\ApplicationMonitor\settings.conf
C:\Program Files (x86)\GSF\ecaOS\ApplicationMonitor\settings.conf.bak
C:\Program Files (x86)\GSF\ecaOS\Services\Support\settings.conf
C:\Program Files (x86)\GSF\ecaOS\Services\Support\settings.conf.bak
C:\Program Files (x86)\GSF\ecaOS\Services\Support\TrueBlue\log
C:\Program Files (x86)\GSF\ecaOS\Services\Support\TrueBlue\Db
C:\Program Files (x86)\Google\Chrome Remote Desktop
C:\ProgramData\Google\Chrome Remote Desktop
```

8.5.4 Add Exclusion Files or Folder

New files or folder can be added in the Exclusion List will be allowed to be written permanently when the ‘Session Shield’ is activated.

1. Click ‘Add Exclusion‘ to add new file/folder

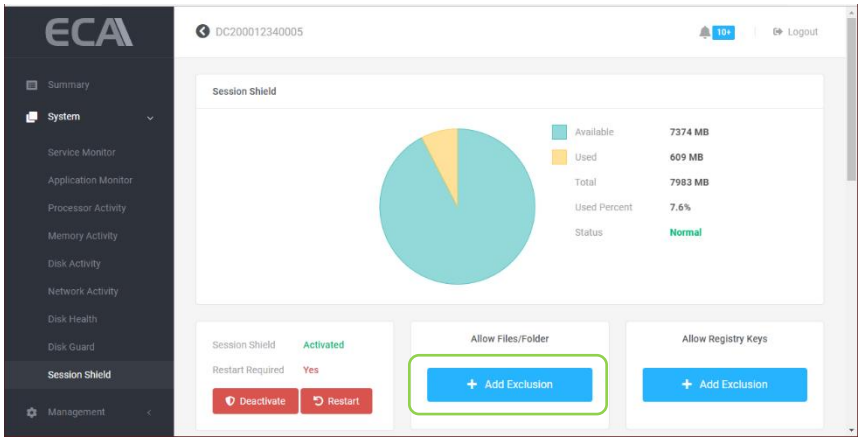


Figure 64: Allow Files/Folder (1 of 3)

2. Type or paste the new files/folder path to be include and click ‘Exclude’

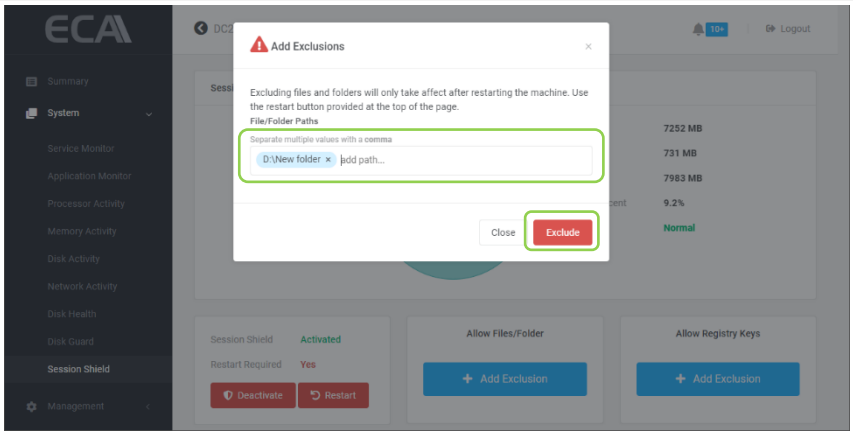


Figure 65: Allow Files/Folder (2 of 3)

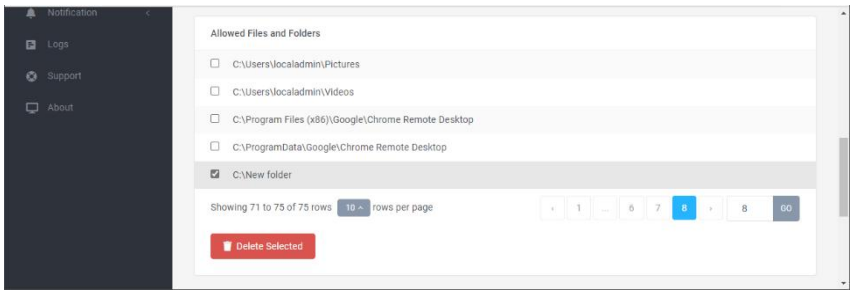


Figure 66: Allow Files/Folder (3 of 3)

8.5.5 Delete Exclusion Files or folder

1. Tick the check box which files/folder to be delete from the exclusion list and click ‘Delete Selected’

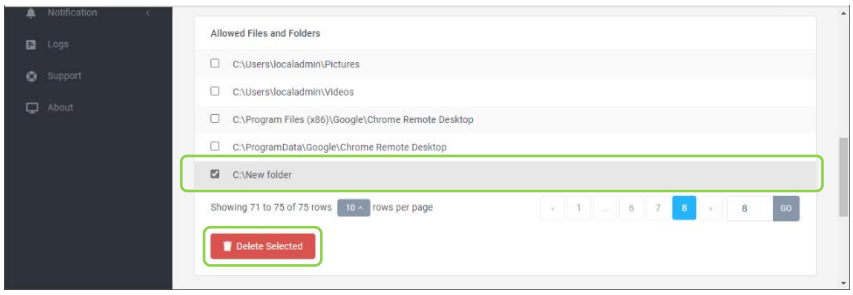


Figure 67: Delete Files/Folder (1 of 3)

2. Click ‘Delete Exclusion’ to confirm the operation

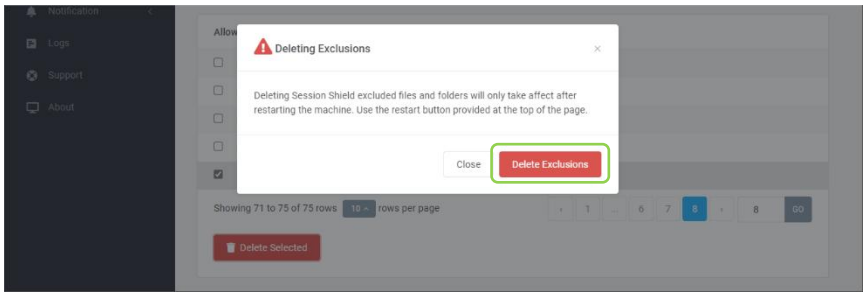


Figure 68: Delete Files/Folder (2 of 2)

8.5.6 Add Registry Keys

Allow to be written permanently when the ‘Shield’ is activated.

1. Click ‘Add Exclusion‘ to add registry keys

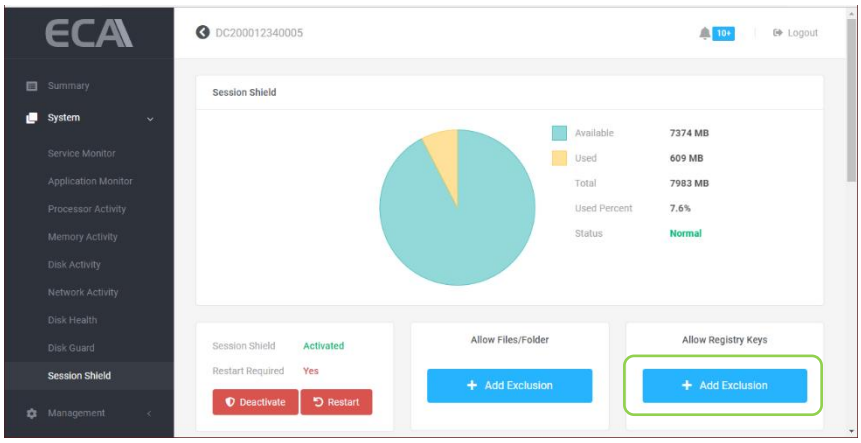


Figure 69: Allow Registry Keys (1 of 2)

2. Type or paste the registry key to be include and click ‘Exclude’

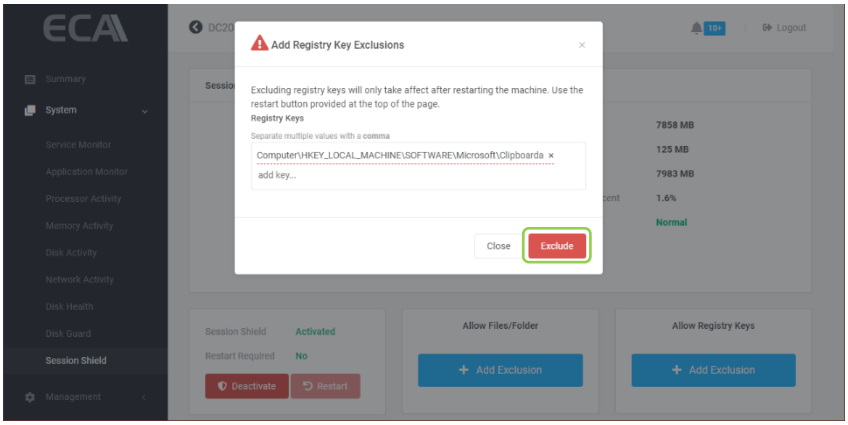


Figure 70: Allow Registry Keys (1 of 2)

8.5.7 Delete Exclusion Registry Key

1. Tick the check box which registry key to be delete from the exclusion list and click ‘Delete Selected’

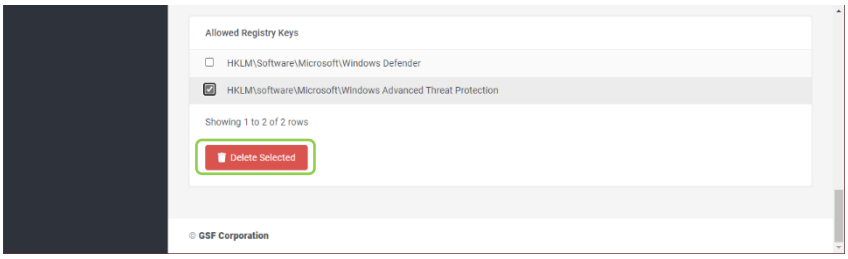


Figure 71: Delete Registry Key (1 of 2)

2. Click ‘Delete Exclusion’ to confirm the operation

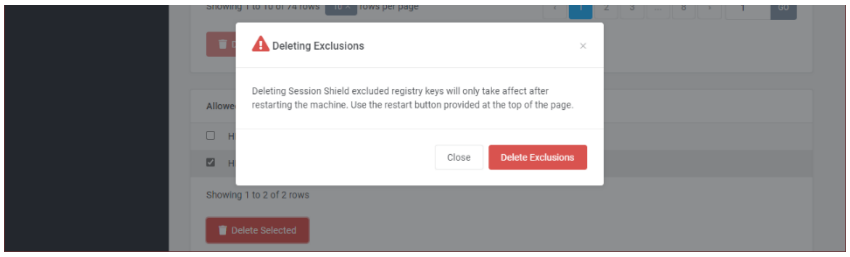


Figure 72: Delete Registry Key (2 of 2)

8.5.8 Status: Warning

Session shield status will turn to ‘Warning’ state when the used amount of space exceeds 80% of total space.

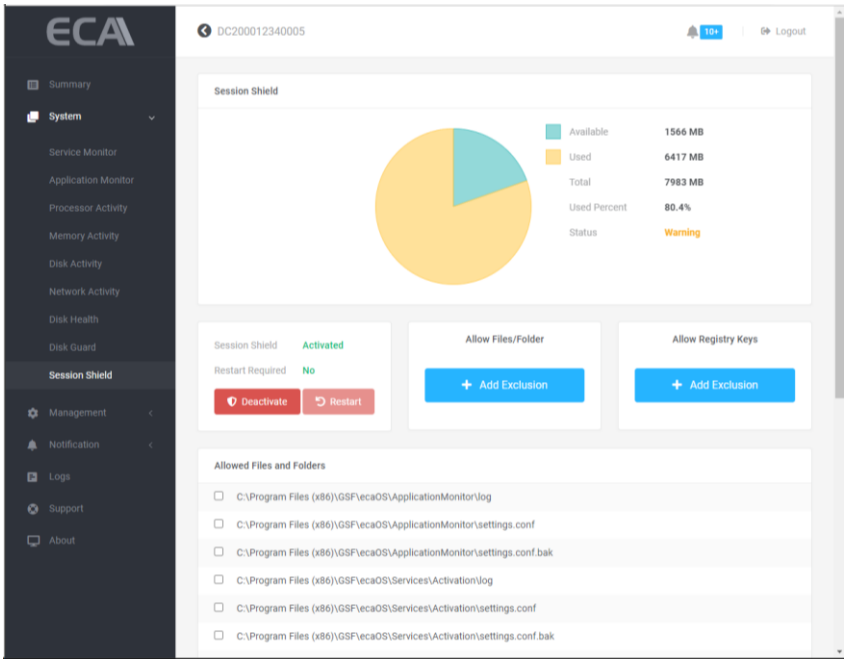


Figure 73: Warning Status

8.5.9 Status: Critical

Session shield status will turn to ‘Critical state when the used amount of space exceeds 90% of total space. The ECA will be start the counter and restart in few minutes.

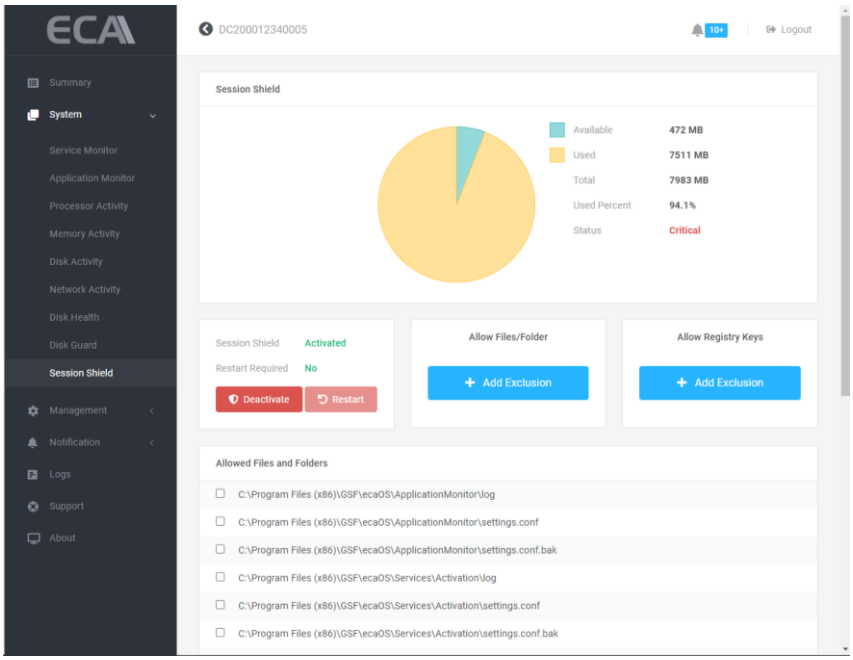


Figure 74: Critical Status

8.6 Device Monitor

Device Monitor is a tool to monitor the uptime percentage of a device of interest using HTTP, Keyword, Port or Ping methods.

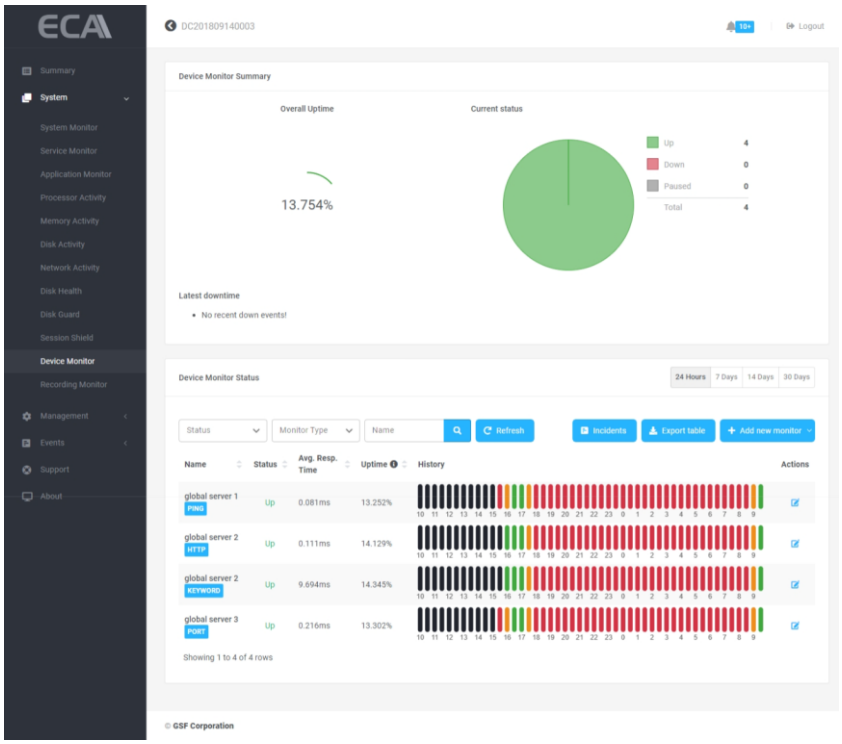


Figure 75: Device Monitor

8.6.1 Add New Monitor

1. Click the ‘Add new monitor”.

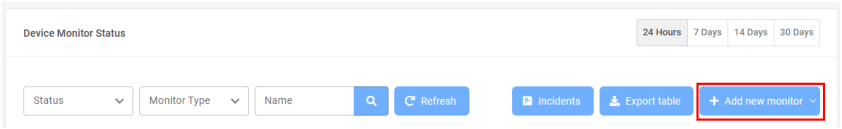


Figure 76: Add new monitor

2. Choose the desired monitor type under "Add monitor details."
3. HTTP – monitors a web server using HTTP or HTTPS. GET, POST, HEAD, and OPTIONS are supported HTTP methods.
    a. Type in the hostname or IP and monitor name.
    b. Pick the appropriate HTTP Method. (GET Method by default)
    c. Set the Monitoring Interval. (by default, five minutes)
    d. Press the Submit button.

Figure 77: Monitor type - HTTP

4. Keyword – monitors a web server (HTTP or HTTPS) using keyword.

    a. Type in the hostname or IP and monitor name.
    b. Enter a keyword to monitor. (Case-sensitive by default)
    c. Set the Monitor Up when keyword “Found or “Not Found” (default: Found)
    d. Set the Monitoring Interval. (by default, five minutes)
    e. Press the Submit button.

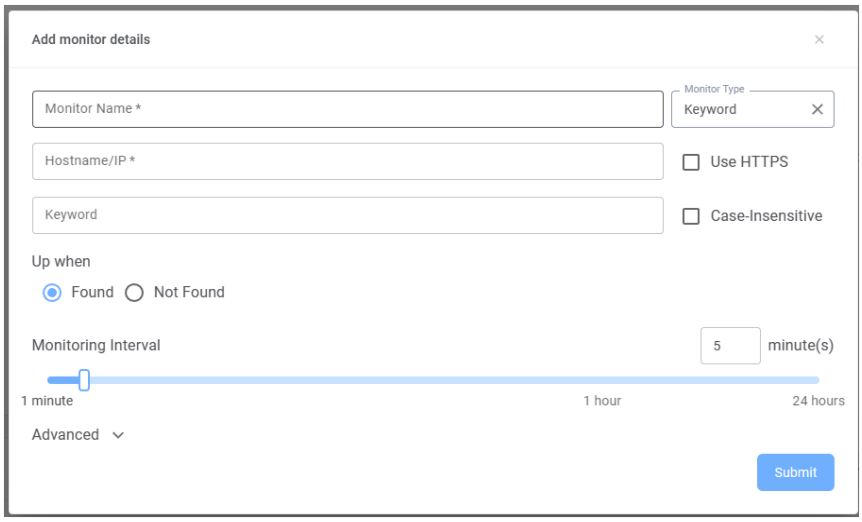


Figure 78: Monitor type - Keyword

5. Ping - sends an “ICMP” echo request ("ping") to the device to monitor its availability.

    a. Type in the Monitor name & Hostname/IP
    b. Set the Monitoring Interval. (by default, five minutes)
    c. Press the Submit button.

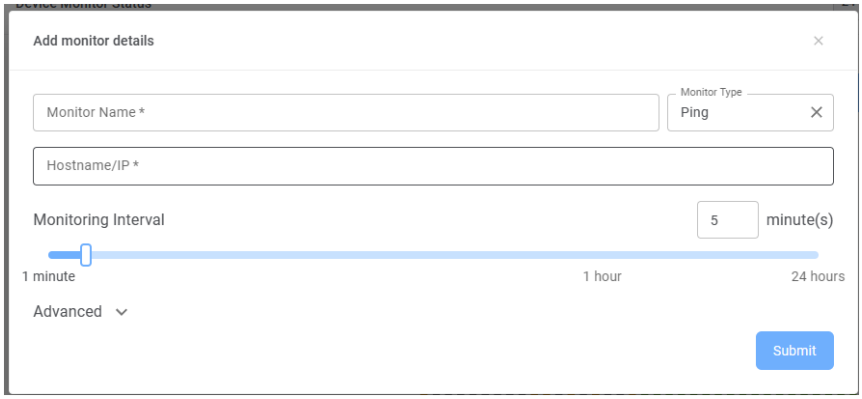


Figure 79: Monitor type - Ping

6. Port - monitors a network service by connecting to its port.

    a. Type in the Monitor name, Hostname/IP & Port number.
    b. Set the Monitoring Interval. (by default, five minutes)
    c. Press the Submit button.

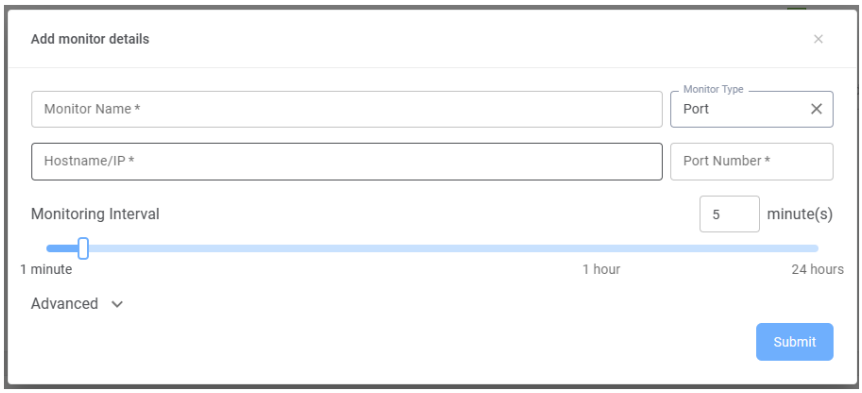


Figure 80: Add Device Monitor – Port type

8.6.2 Delete Monitor

1. Click '⌄' icon and select 'Delete monitors'.

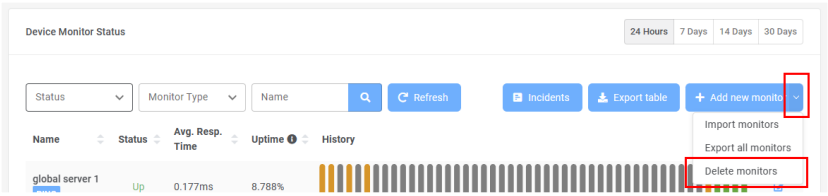


Figure 81: Delete Device Monitors (1 of 2)

2. Select the monitor to delete and type 'Delete'.
3. Press the ‘Delete’ button.

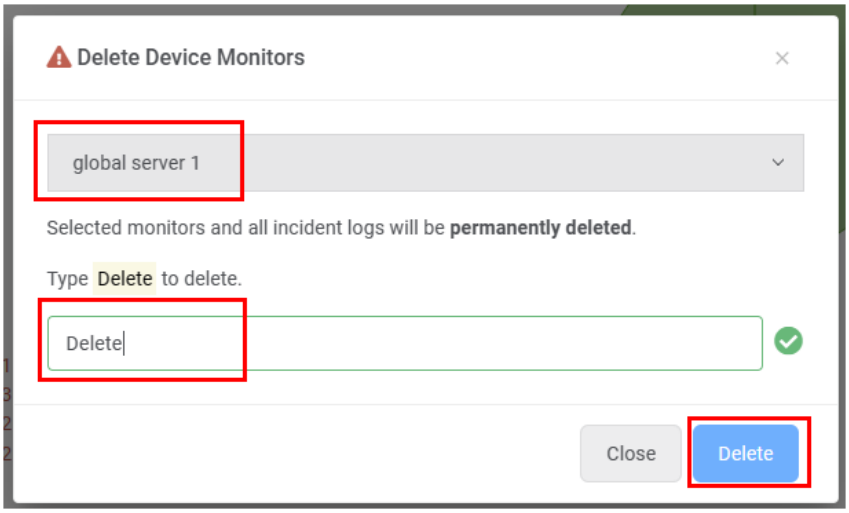


Figure 82: Delete Device Monitors (2 of 2)

8.7 Recording Monitor

The Recording Monitor is a tool for monitoring the channels recording status of the Macula VMS.

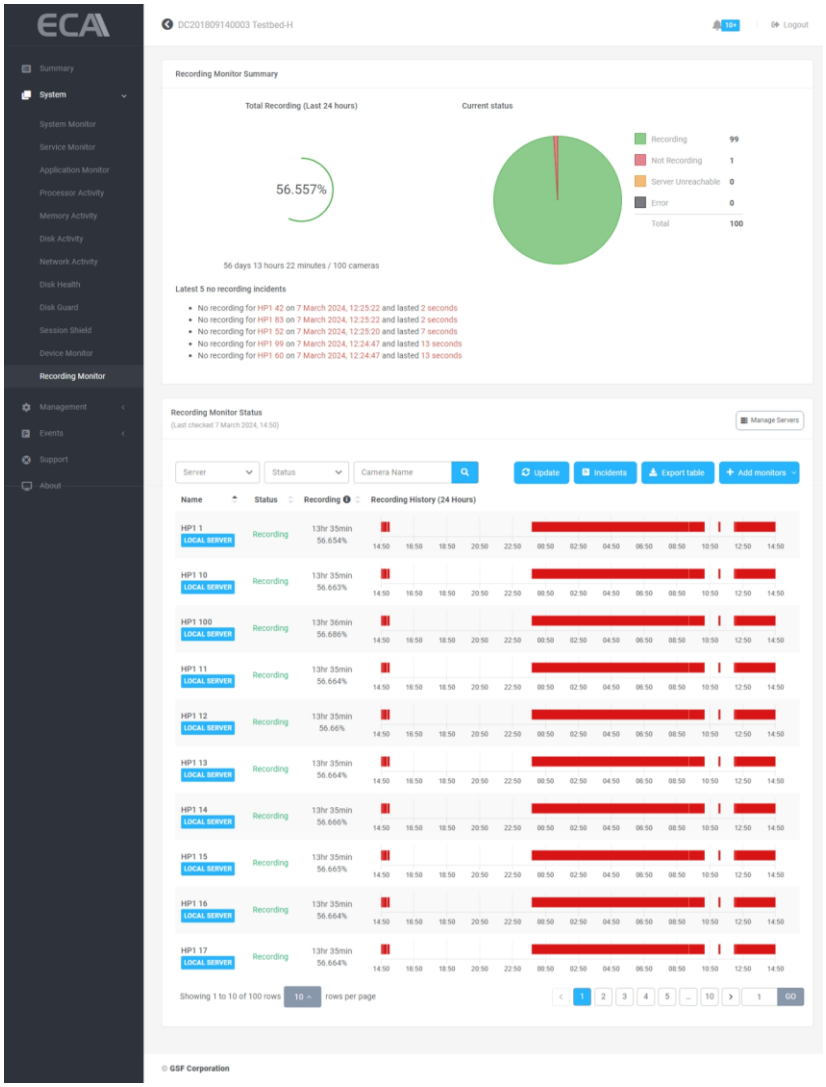


Figure 83: Device Monitor

8.7.1 Add New Monitor

1. Click ‘Manage Servers’ button.

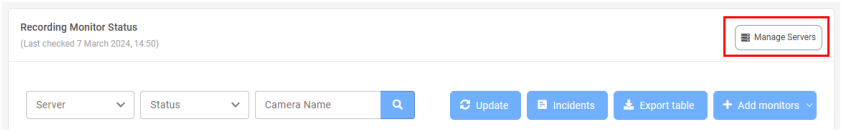


Figure 84: Add VMS server (1 of 3)

2. Click ‘Add Server’.

Figure 85: Add VMS server (2 of 3)

3. Enter VMS's hostname/IP, port, and login information. Please ensure that the user has the channel's 'video playback' and 'Login via HTTP' permissions.

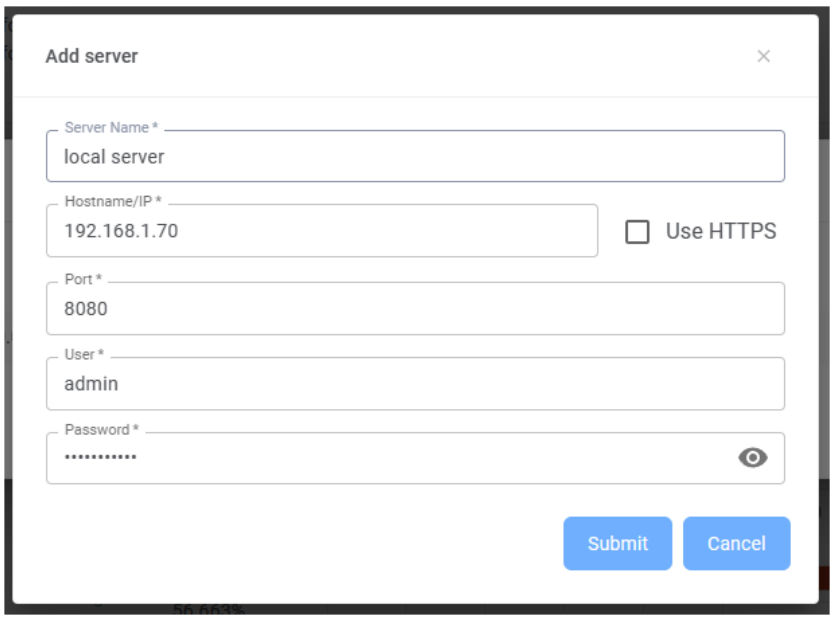


Figure 86: Add VMS server (3 of 3)

4. Click ‘Add monitors.

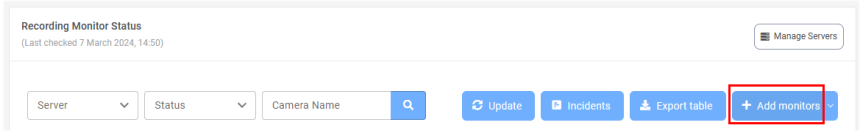


Figure 87: Add monitors (1 of 2)

5. In 'Add monitor', choose a server and channels to monitor. Then press 'Add' button.

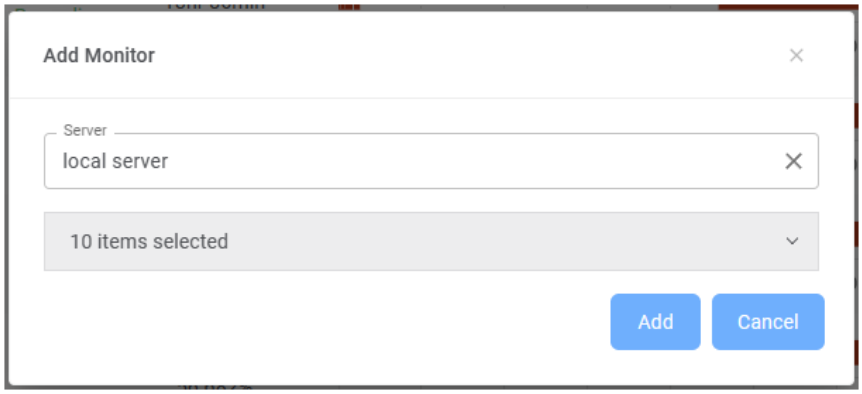


Figure 88: Add monitors (2 of 2)

8.7.2 Delete Monitors

1. Click '⌄' icon and select 'Delete monitors'.

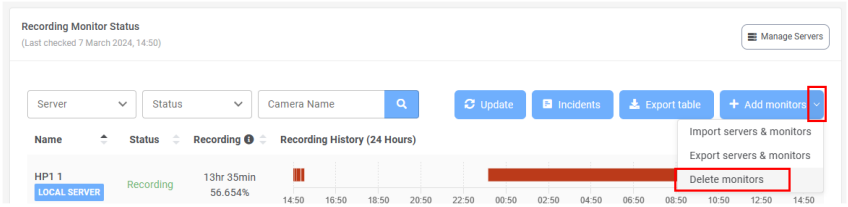


Figure 89: Delete Recording Monitors (1 of 2)

2. Select the monitor(s) to delete and type 'Delete'.
3. Press the ‘Delete’ button.

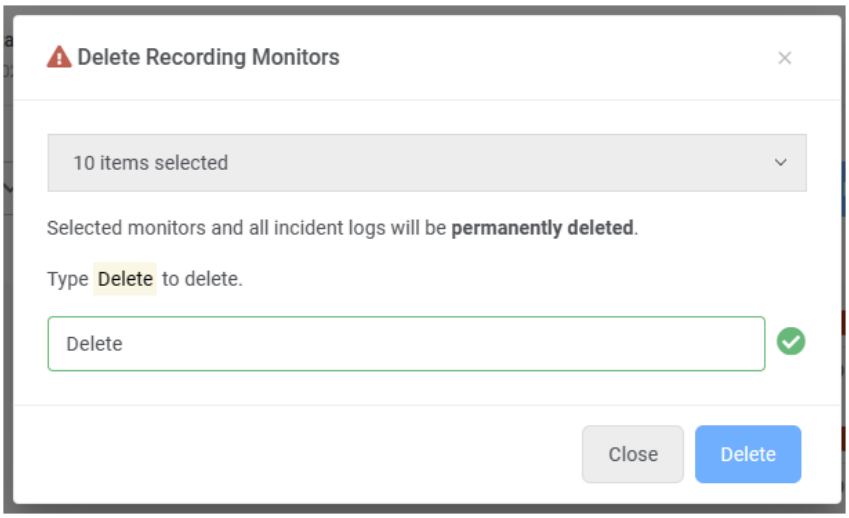


Figure 90: Delete Recording Monitors (2 of 2)

9 Management

9.1 Machine

Under Machine Control to Reboot or Shutdown ECA. Layer Management to save current layer as a backup layer. Backup layer can be deployed (Soft Reset & Hard Reset) in the future to restore previous setting.

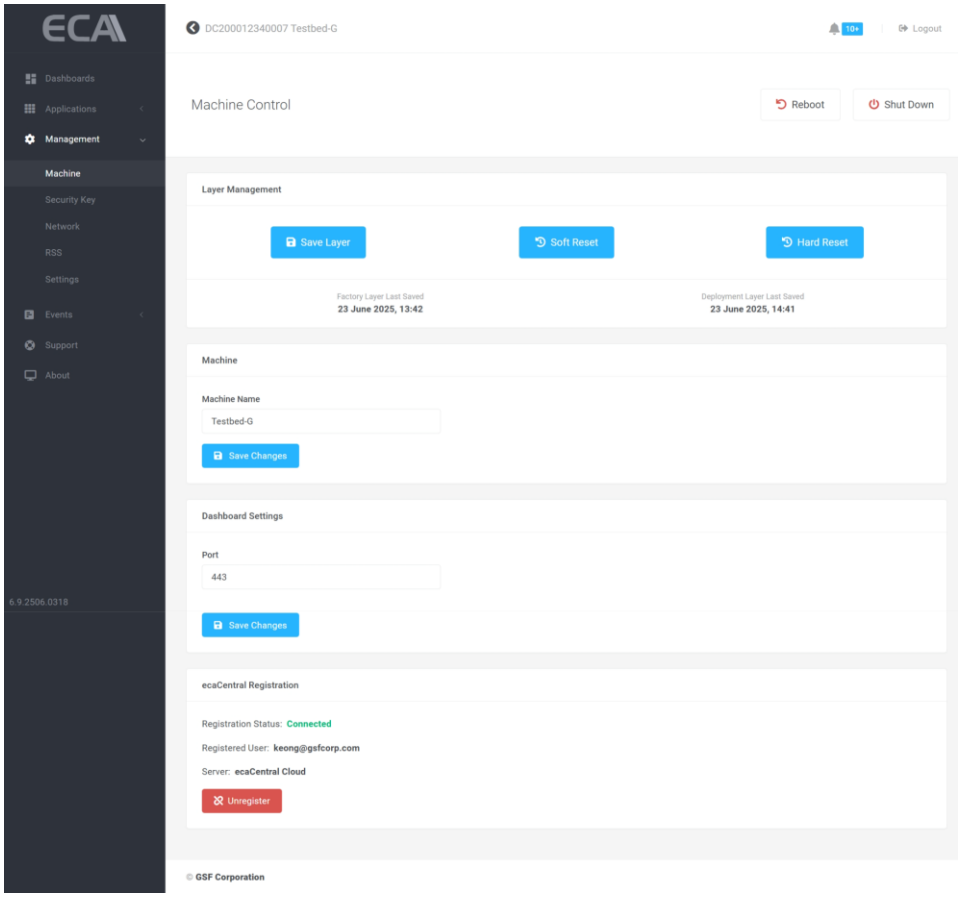


Figure 91: Machine

9.1.1 Authorize Restart

Only restart through the Dashboard will consider as authorize restart.

1. Click on ‘Restart’

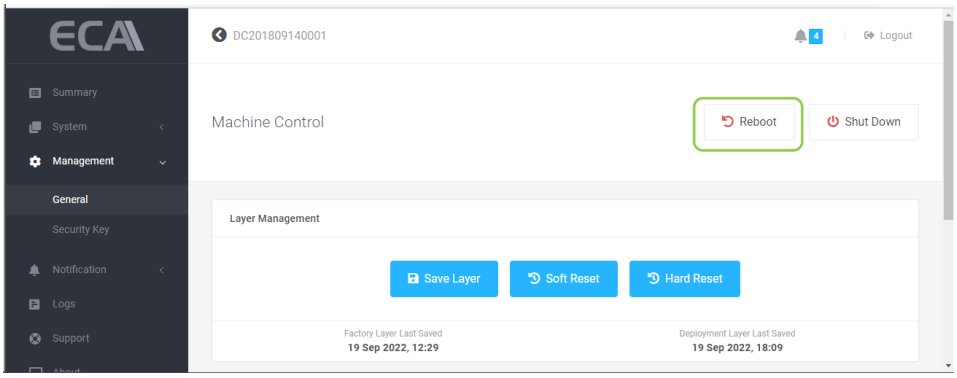


Figure 92: Authorize Restart (1 of 2)

2. Type **Restart** then click ‘Restart’ button

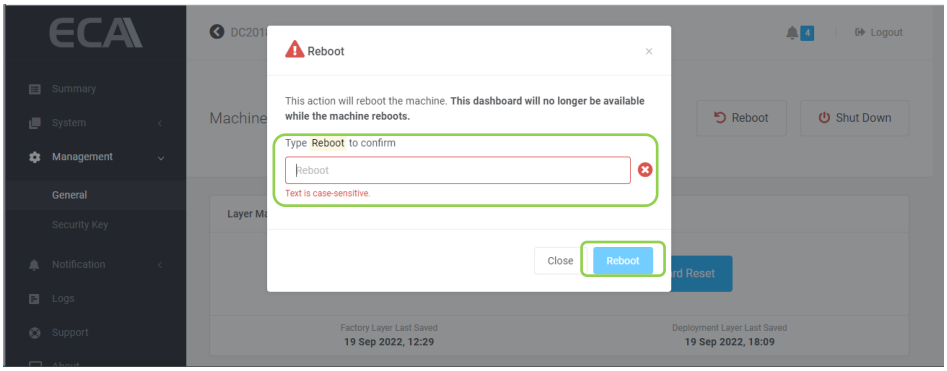


Figure 93: Authorize Restart (2 of 2)

9.1.2 Authorize Shutdown

To shutdown ECA, only through the Dashboard will consider as authorize restart. Shutdown ECA not via dashboard will consider as unauthorize shutdown. HB will reboot the ECA.

1. Click on ‘Shut Down’

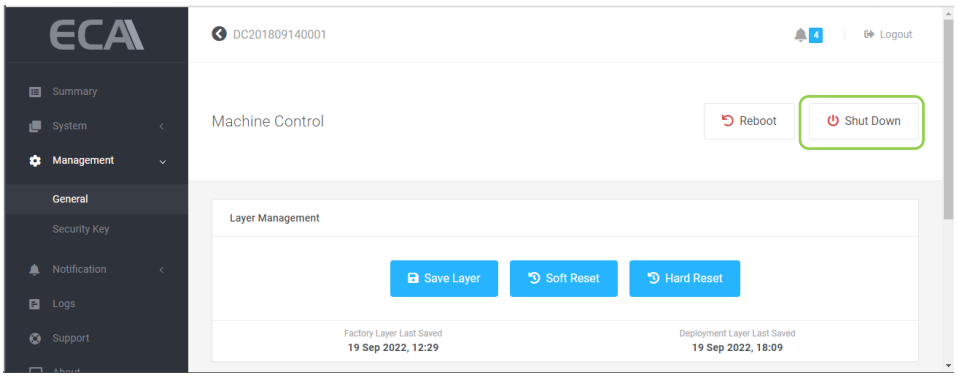


Figure 94: Authorize Shut Down (1 of 2)

2. Type **Shutdown** then click ‘shutdown’ button

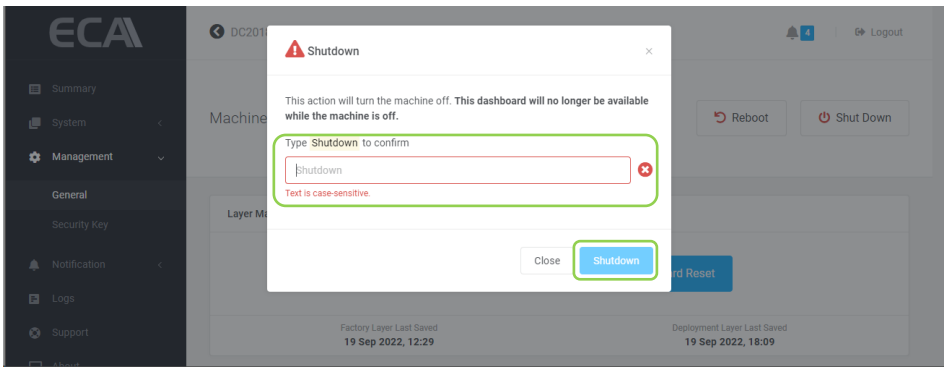


Figure 95: Authorize Shut Down (2 of 2)

9.1.3 Saving & Deploy Layer

It is recommended to perform ‘Save Layer’ for any changes under system including video management software such as added new camera.

9.1.3.1 Save Layer

Save current user working layer as a deployment layer. This layer will content all current working setting. If in the future suddenly the OS corrupt, this layer can recall (Soft Reset) to deploy previous working state.

NOTE:

Performing Save Layer, Soft Reset & Hard Reset will cause the downtime of the ECA means there will no recording & accessing to Dashboard not available during this period until the ECA complete the layer saving and reboot back to ecaOS.

1. Click on ‘Save Layer’

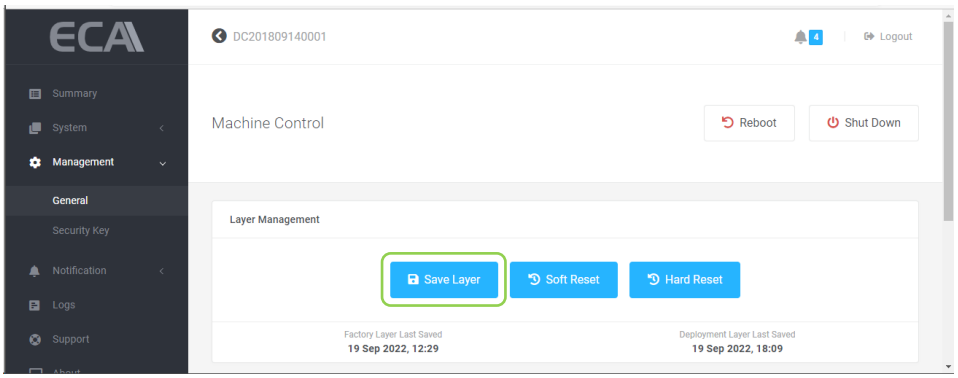


Figure 96: Save Layer (1 of 5)

2. ECA will reboot and go to Layer Manager.

Figure 97: Save Layer (2 of 5)

3. Saving layer will be start after 10 seconds countdown. To cancel the operation, click on Cancel

Figure 98: Save Layer (3 of 5)

4. Saving layer in progress show with percentage

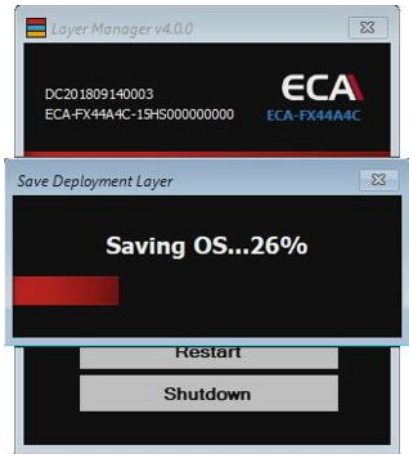


Figure 99: Save Layer (4 of 5)

5. ECA will reboot to ecaOS after complete saving layer.

Figure 100: Save Layer (5 of 5)

9.1.3.2 Soft Reset

Deploy deployment layer and replace current working with previous save setting.

1. Click on ‘Soft Reset’

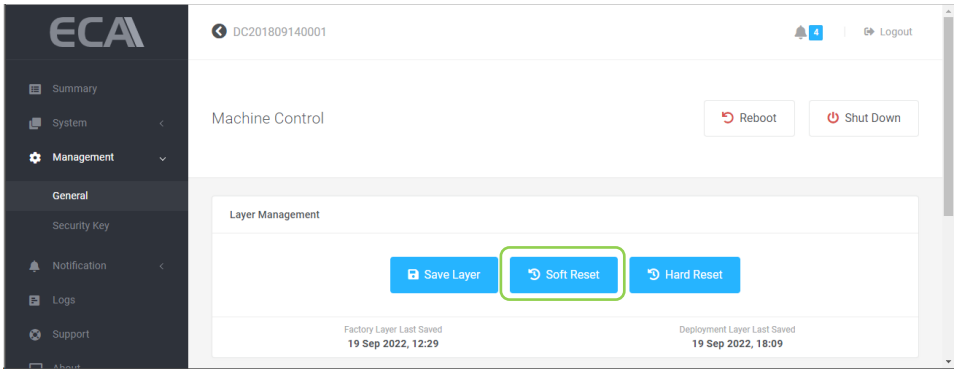


Figure 101: Soft Reset (1 of 5)

6. ECA will reboot and go to Layer Manager.

Figure 102: Save Layer (2 of 5)

7. Restoring Deployment layer will be start after 10 seconds countdown. To cancel the operation, click on Cancel

Figure 103: Save Layer (3 of 5)

8. Restoring layer in progress show with percentage

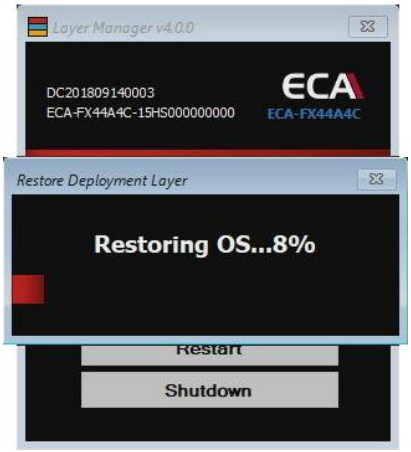


Figure 104: Save Layer (4 of 5)

9. ECA will reboot to ecaOS after complete saving layer.

Figure 105: Save Layer (5 of 5)

9.1.3.3 Hard Reset

Deploy default layer saved from factory.

NOTE: All setting previously done on site will not available after Hard Reset. Only perform Hard Reset when Soft Reset failed.

1. Click on 'Hard Reset'

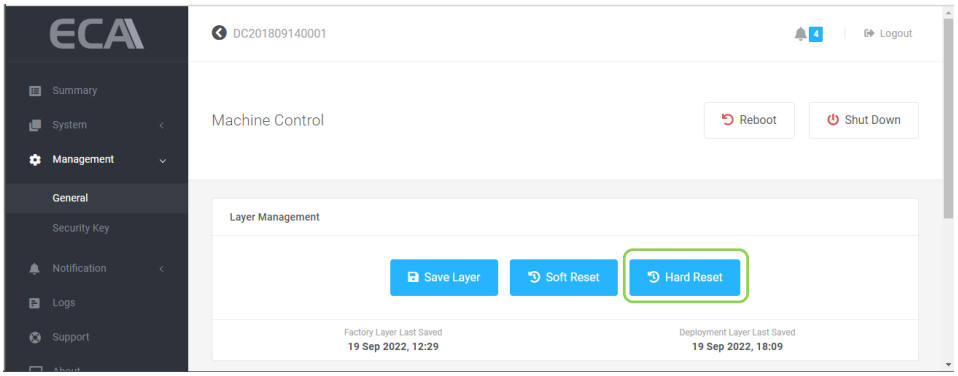


Figure 106: Soft Reset (1 of 2)

10. ECA will reboot and go to Layer Manager.

Figure 107: Save Layer (2 of 5)

11. Restoring Factory layer will be start after 10 seconds countdown. To cancel the operation, click on Cancel

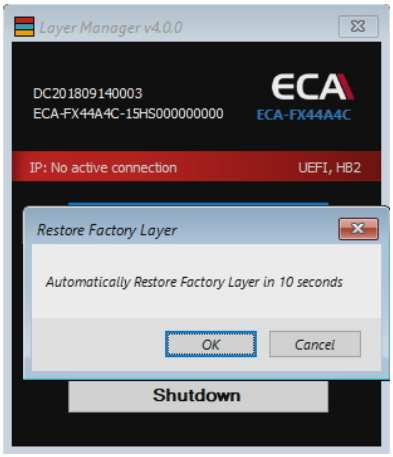


Figure 108: Save Layer (3 of 5)

12. Restoring layer in progress show with percentage

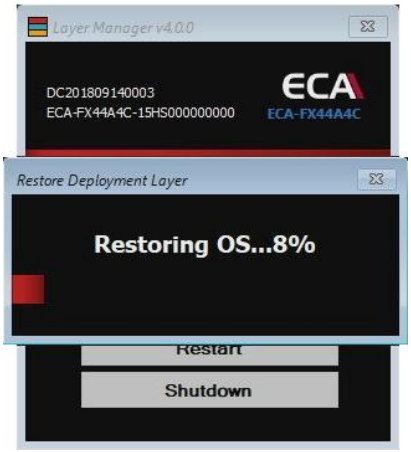


Figure 109: Save Layer (4 of 5)

13. ECA will reboot to ecaOS after complete saving layer.

Figure 110: Save Layer (5 of 5)

9.1.3.4 Last Saved Layer Information

Display the last date and time of the layer last saved

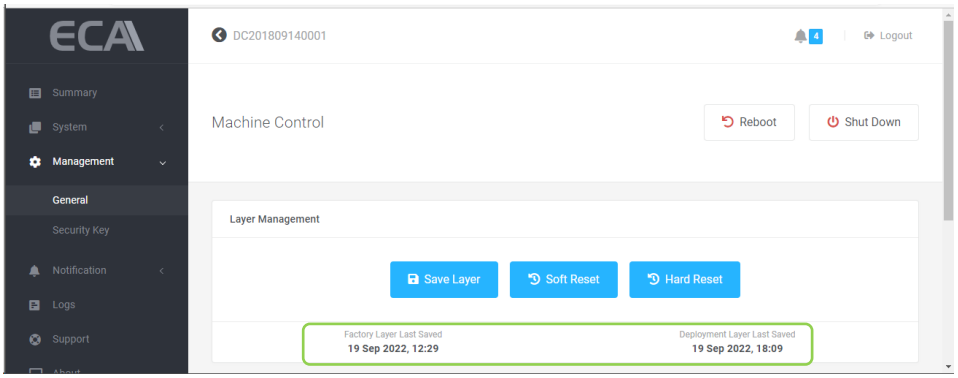


Figure 111: Information about the last saved layer

9.1.4 Machine Name

Assign your ECA a friendly name to make it easier to identify.

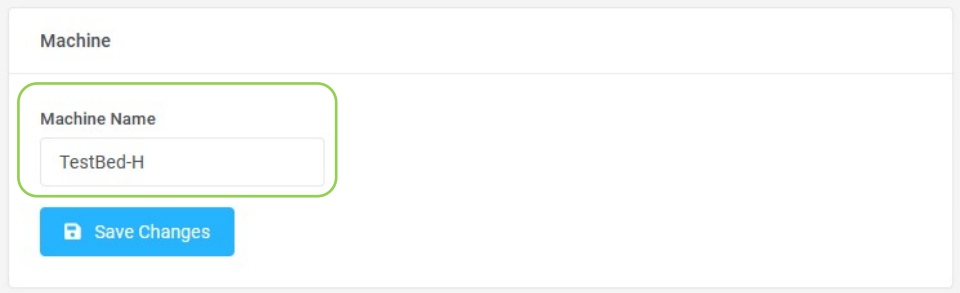


Figure 112: Machine name for ECA

9.1.5 Change Dashboard Port

By default, port 443 is used by ECA to access the dashboard remotely from a different computer connected to the same local area network. If the default ports are already being used, change this port.

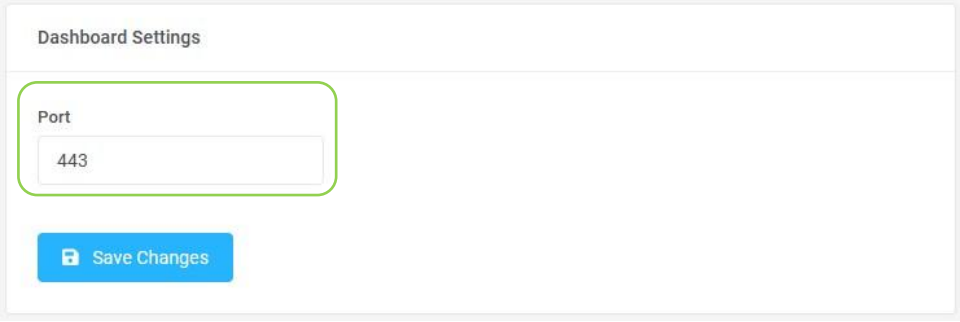


Figure 113: Port settings for Dashboard

9.1.6 ecaCentral Registration

ecaCentral is a dedicated dashboard for monitoring the health and performance of multiple ECAs using a registered email address. If any registered ECAs have anomalies, you will be notified via the ecaCentral dashboard.

Before using ecaCentral, go to the ecaOS dashboard for the ECA you want to monitor: Management > Settings > ecaCentral Registration, and enter your registered account information.

To register your ECA for this service:

- Enter the central IP address or hostname.
- Enter your registered email address.
- Click the Next button.
- Enter the access code generated from your virtual security key to verify and complete the registration.

If you have successfully connected the ecaCentral, you will see the connection status as connected.

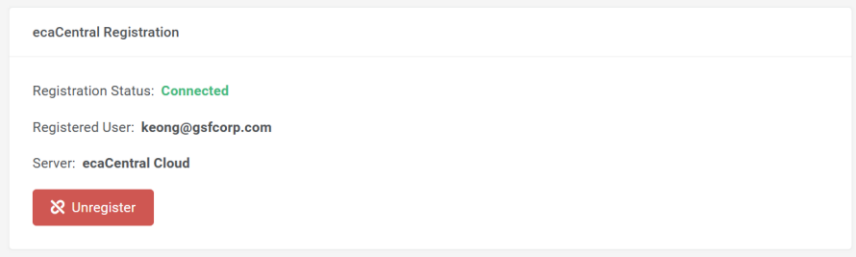


Figure 114: ecaOS Central Registration

9.2 Security Key

Each ECA will come with 1 unit of Security key. Any extra Security key or replacement unit require to register the Security Key to access Dashboard.

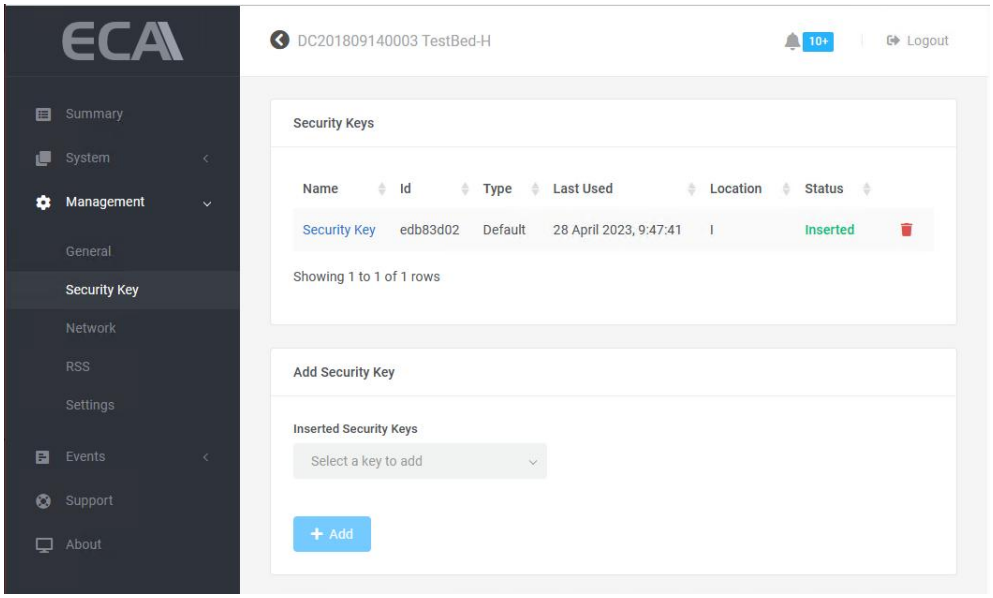


Figure 115: Security Key

9.2.1 Register Security Key

1. Insert valid Security Key in the USB on the ECA
2. Click on the drop-down list and select the key to register.

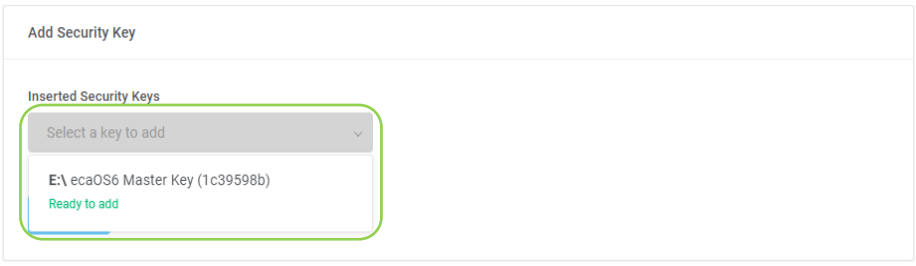


Figure 116: Register security key (1 of 3)

3. Click Add to register

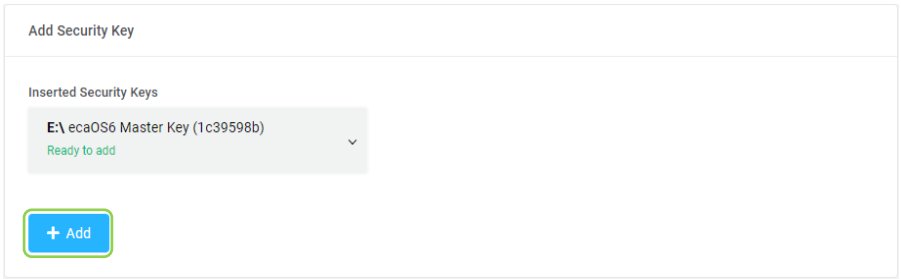


Figure 117: Register security key (2 of 3)

4. Once successfully added the Security Key. The new security key will show under ‘Security keys’

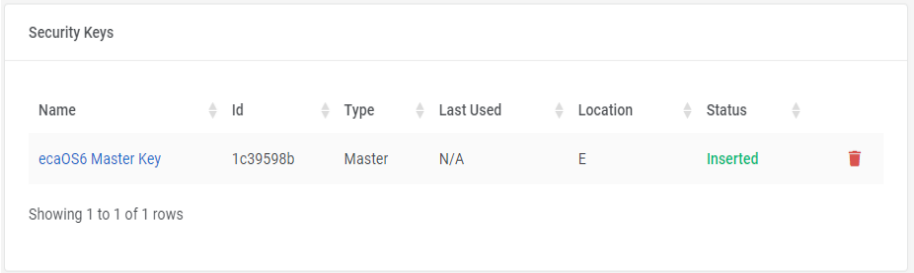


Figure 118: Register security key (3 of 3)

9.2.2 Delete Security Key

1. Click on the dustbin icon of the Security key to be delete

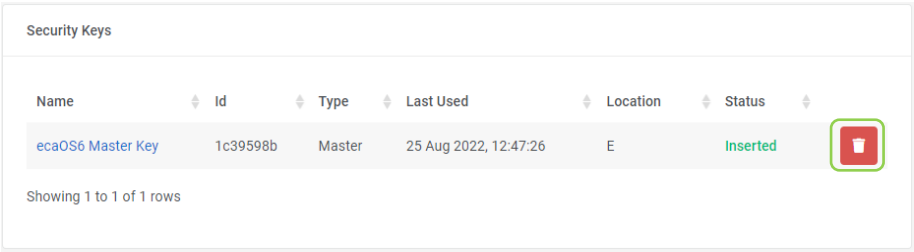


Figure 119: Delete security key (1 of 2)

2. Type in the field Security Key name and click ‘Delete Security Key’

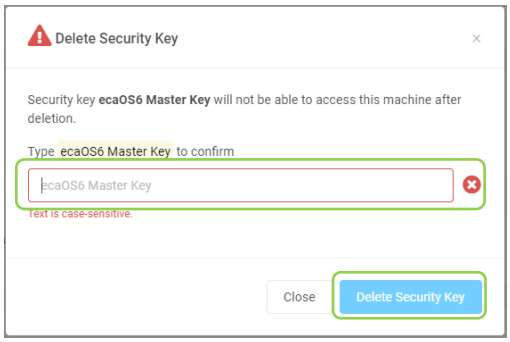


Figure 120: Delete security key (1 of 2)

9.2.3 Add Virtual Security Key

1. Click on the ‘Add’ button under Virtual Security key

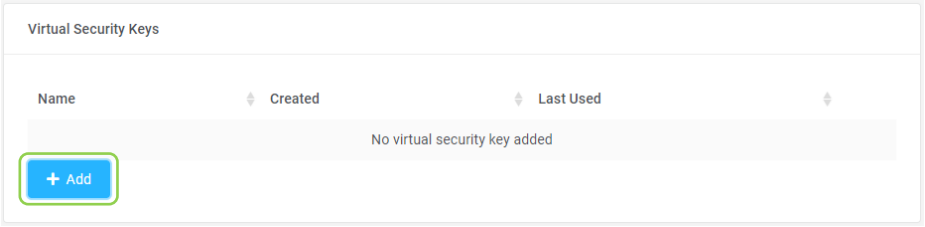


Figure 121: Add virtual security key (1 of 5)

2. Click ‘Next’ button

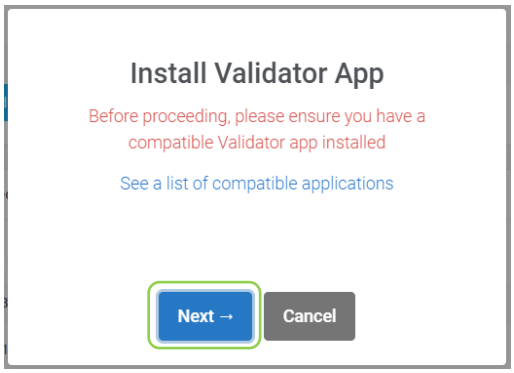


Figure 122: Add virtual security key (2 of 5)

3. Give the new virtual security key a name

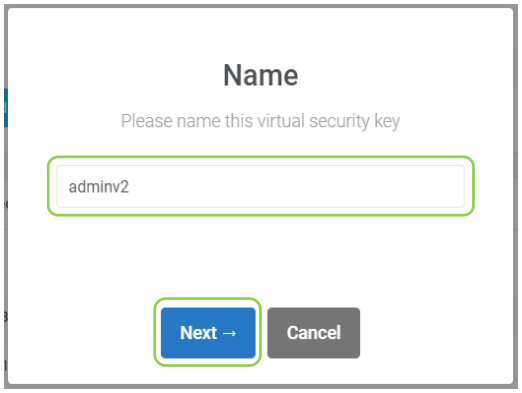


Figure 123: Add virtual security key (3 of 5)

4. Scan the QR code using authenticator application on the phone. Type the in the field and click ‘Save’ button one-time password for example 123456

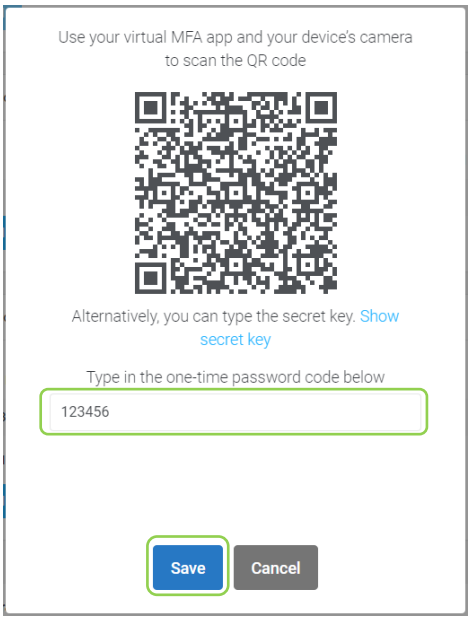


Figure 124: Add virtual security key (4 of 5)

5. The new virtual security key will show under ‘Virtual Security keys’

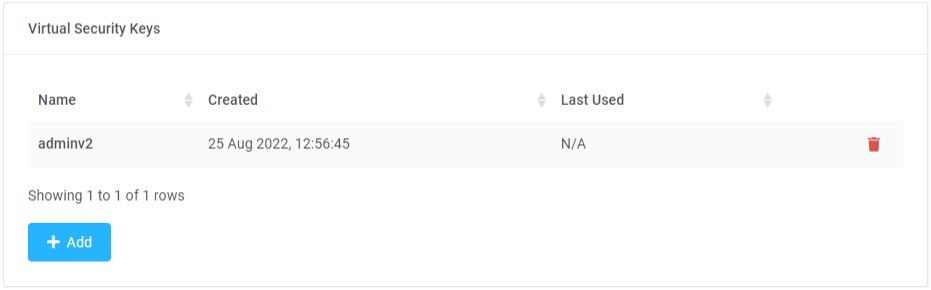


Figure 125: Add virtual security key (5 of 5)

9.2.4 Delete Virtual Security Key

1. Click on the dustbin icon the Virtual key to be delete

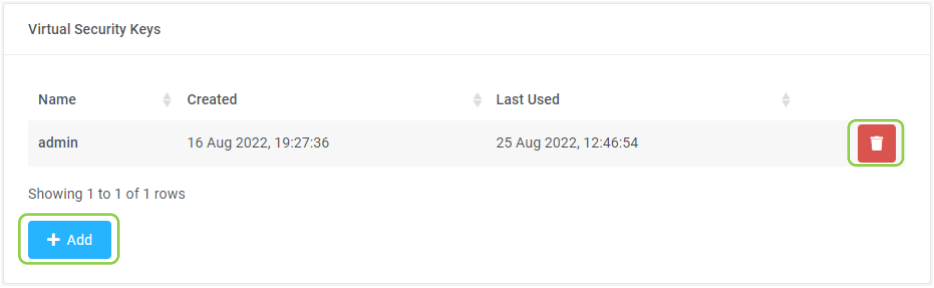


Figure 126: Delete Virtual Security Key (1 of 2)

2. Type ‘admin’ and click on ‘Delete Virtual Security Key’ button

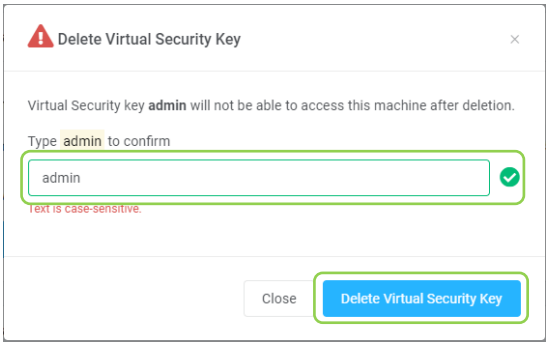


Figure 127: Delete Virtual Security Key (2 of 2)

9.3 Network

All ECA come with GSF DDNS. Network teaming groups multiple physical adapters together to provide better network fault tolerance.

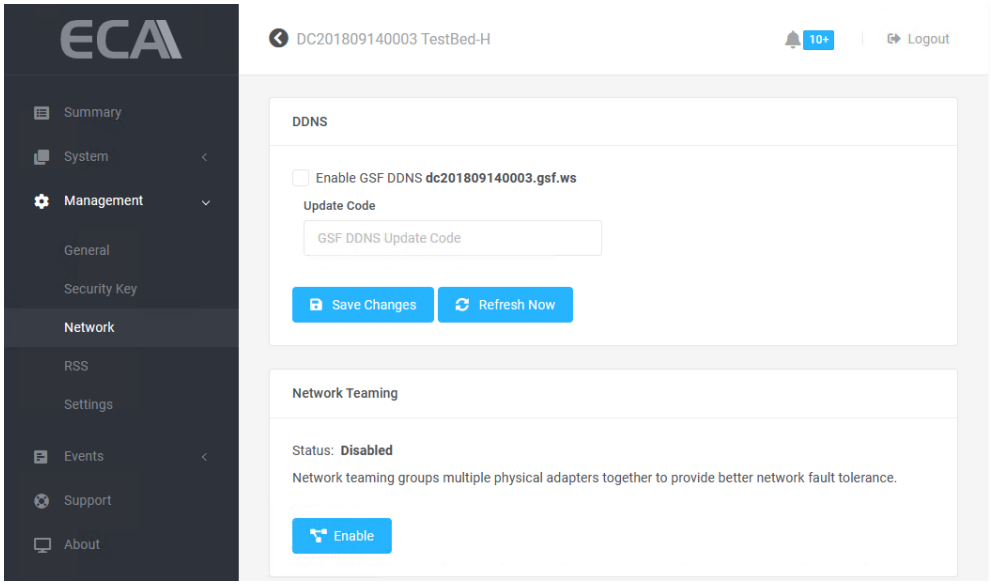


Figure 128: DDNS and Network Teaming

9.3.1 Enable DDNS

1. Enable GSF DDNS.
2. Enter the correct Update Code and click on ‘Save Changes’. Please contact GSF to obtain your update code.

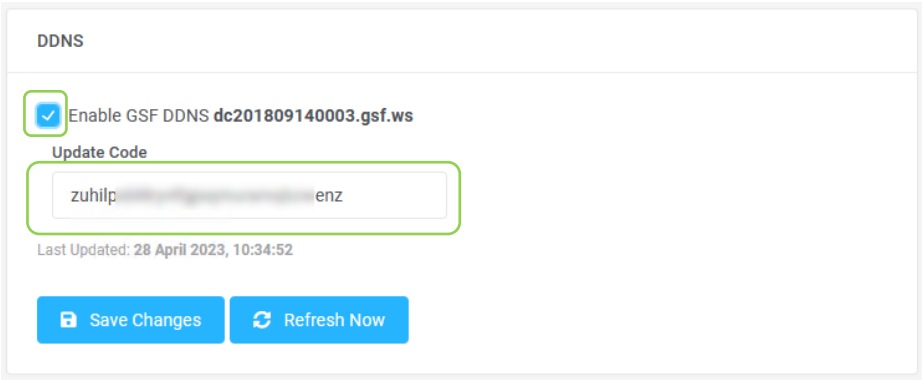


Figure 129: Enable DDNS

9.3.2 Enable Network Teaming

1. Click on the ‘Enable’ button to enable Network Teaming.

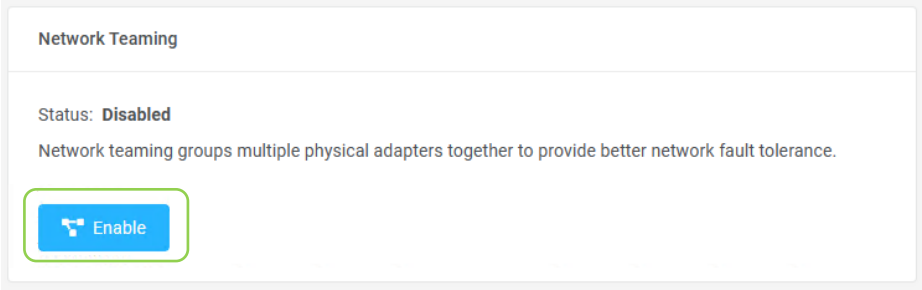


Figure 130: Enable Network Teaming

2. Type ‘Confirm and click on ‘Confirm’ button

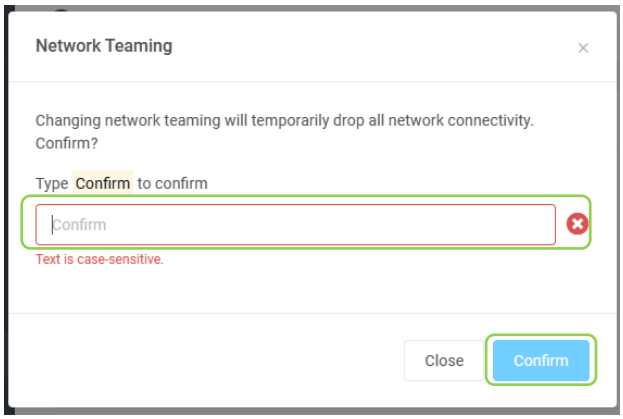


Figure 131: Confirm to enable network teaming

9.3.3 Disable Network Teaming

1. Click on the ‘Disable’ button to disable Network Teaming.

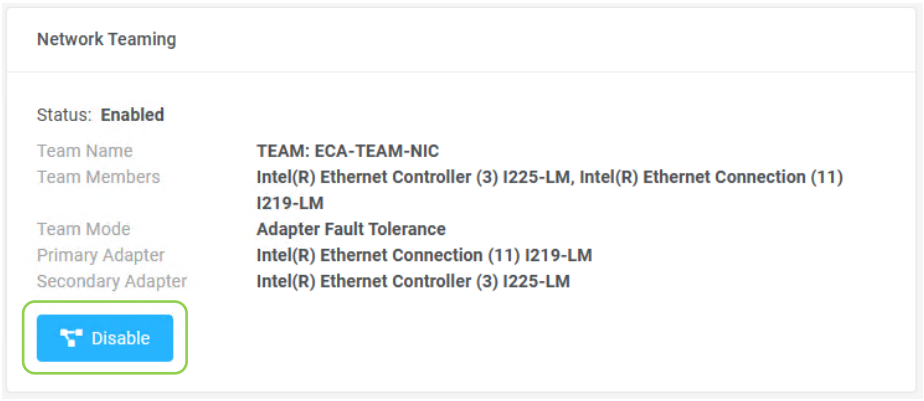


Figure 132: Disable Network Teaming

2. Type ‘Confirm and click on ‘Confirm’ button

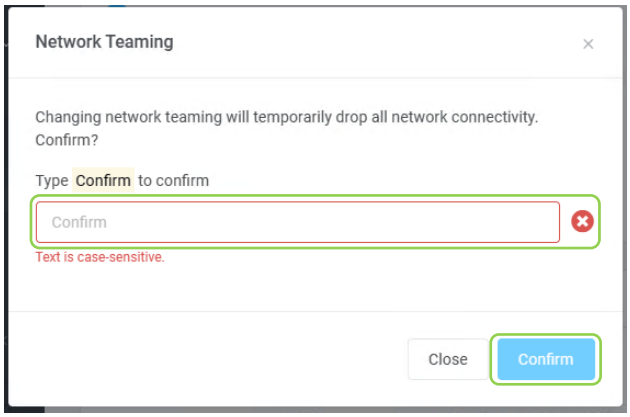


Figure 133: Confirm to disable network teaming

9.4 RSS (Redundant Storage System)

RSS can help protect your data from drive failures. It's a technology in ECA and is conceptually similar to redundant array of independent disks (RAID), implemented in software. You can use RSS to group three or more drives into a storage pool and then use capacity from that pool to create Storage Spaces. These drives typically store extra copies of your data, so if one of your drives fails, you still have an intact copy of your data.

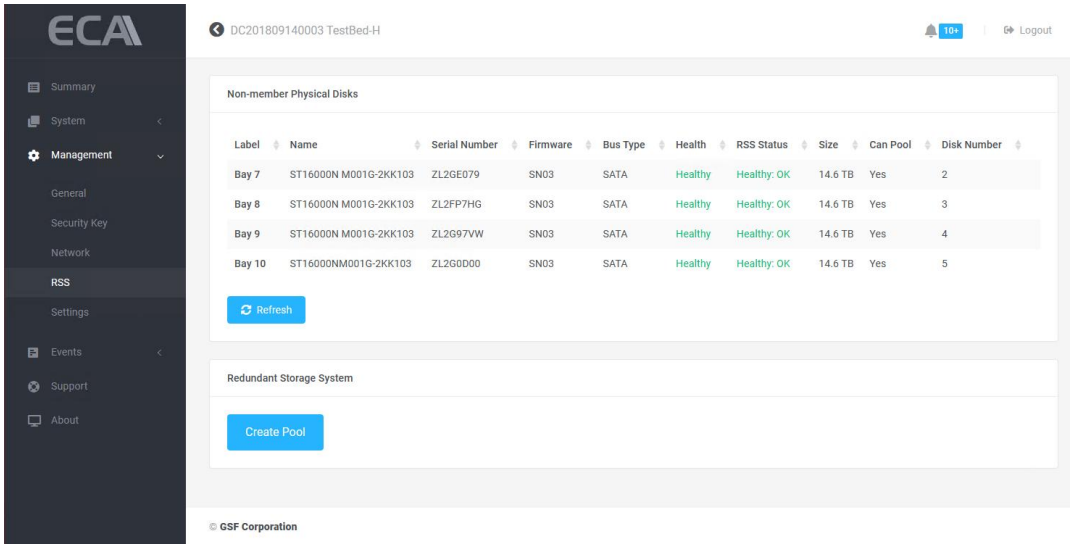


Figure 134: RSS – Redundant Storage System

9.4.1 Create Storage Pool

1. Click on the ‘Create Pool’ button to create pool.

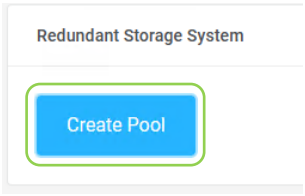


Figure 135: Create Pool

2. Name the storage pool and click on the ‘Next’ button.

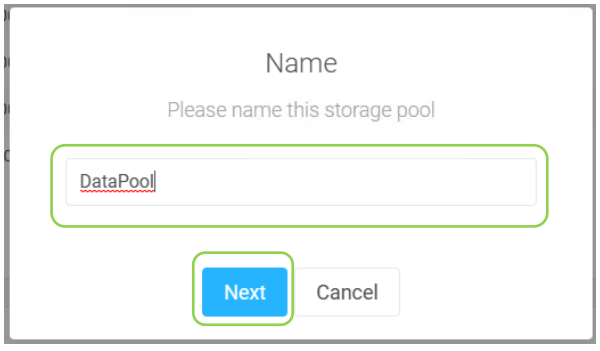


Figure 136: Name storage pool

3. Select the non-member physical disks and click on the ‘Next’ button to create pool.

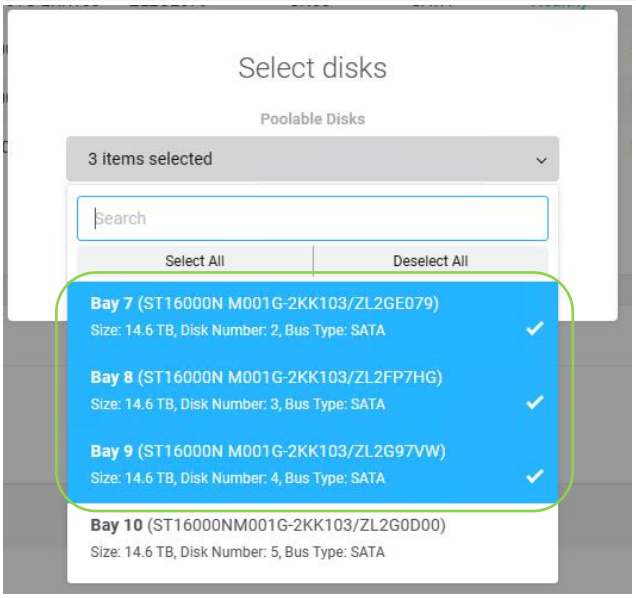


Figure 137: Select disks

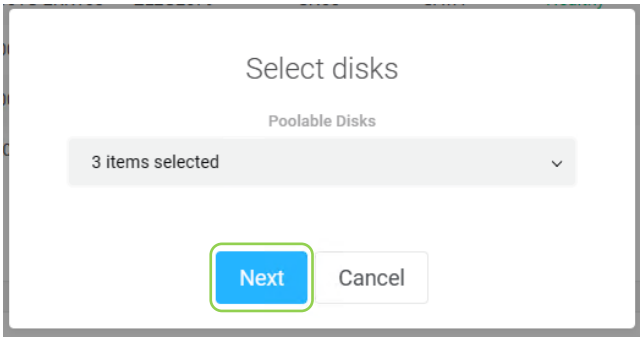


Figure 138: Select disks

4. In Virtual Disk Settings, name the virtual disk and select the Resiliency type. Click on the 'Create Volume' to create volume.

Resiliency type	Fault-tolerance for each storage pool	Minimum number of disks	Disk space efficie
Simple	0 Disk	1	100%
Two-way Mirror	1 Disk	2	50%
Three-way Mirror	2 Disks	5	33%
Single Parity	1 Disk	3 (recommended 5disk for optimized performance)	$\frac{Disk\ Count\ -\ 1}{Disk\ Count}$
Dual Parity	2 Disks	5 (recommended 10disk for optimized performance)	$\frac{Disk\ Count\ -\ 2}{Disk\ Count}$

Figure 139: Resiliency type table

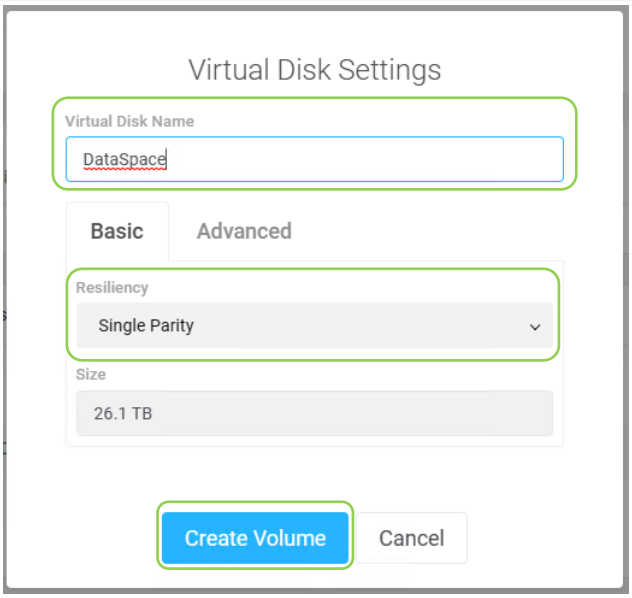


Figure 140: Create volume

5. Storage pool and virtual disk health status in RSS.

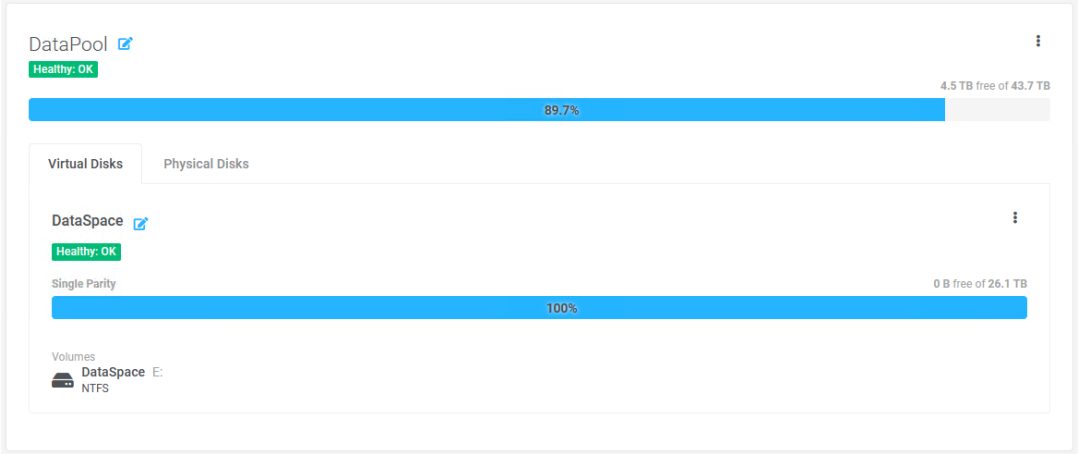


Figure 141: View storage pool, virtual disk health status

9.4.2 Delete Storage Pool

1. Click on the '⋮' and select 'Delete Pool' to delete the pool.

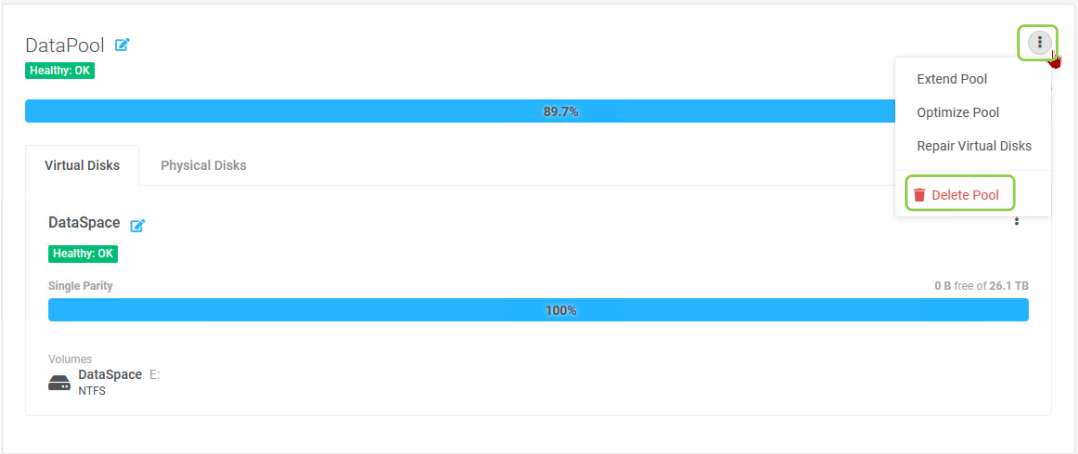


Figure 142: Delete pool

2. Enter storage pool name and click on the 'Delete Pool and Volumes' to delete the pool.

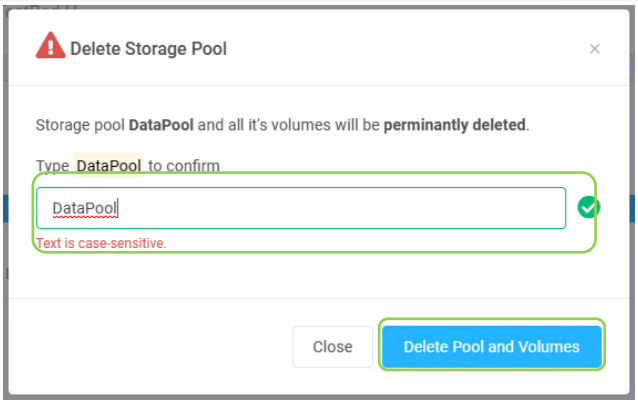


Figure 143: Confirm delete pool

9.4.3 Extend Storage Pool

Add a new non-member disk to extend the storage pool.

1. Insert a new clean disk into the ECA, it will appear under the Non-member Physical Disks list.

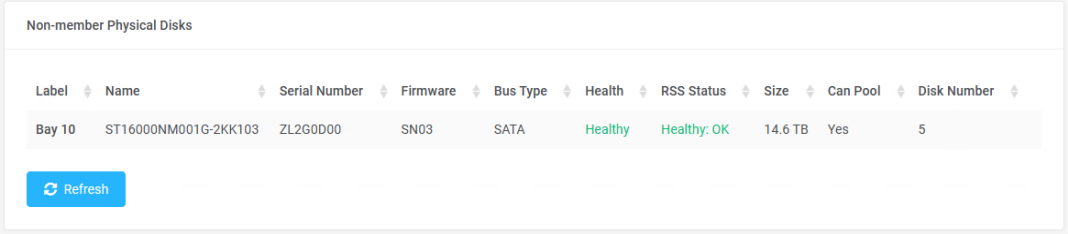


Figure 144: RSS non-member physical disks

2. Click on the '⋮' and select 'Extend Pool' to extend the pool.

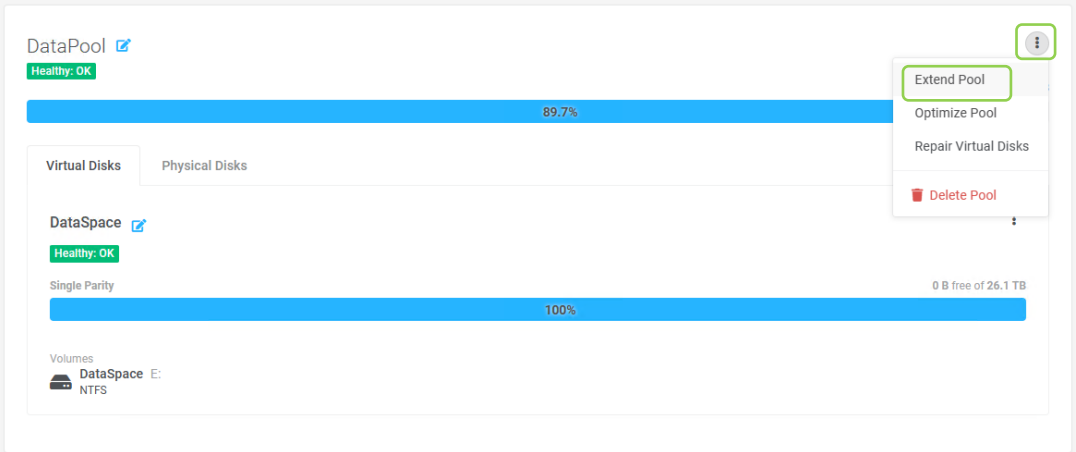


Figure 145: Extend storage pool

3. Enable Optimize storage pool and click on the 'Extend' button to extend the pool.

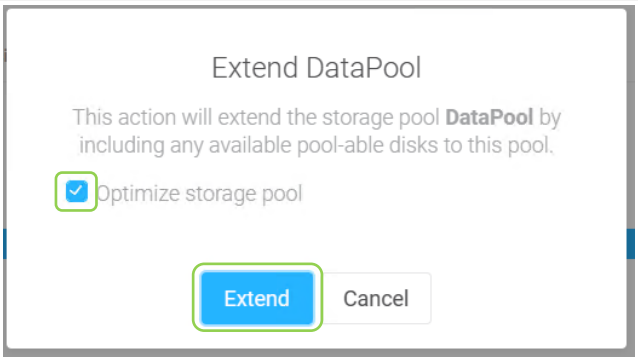


Figure 146: Optimize and extend storage pool

4. Please wait for the ECA to complete the optimization process.

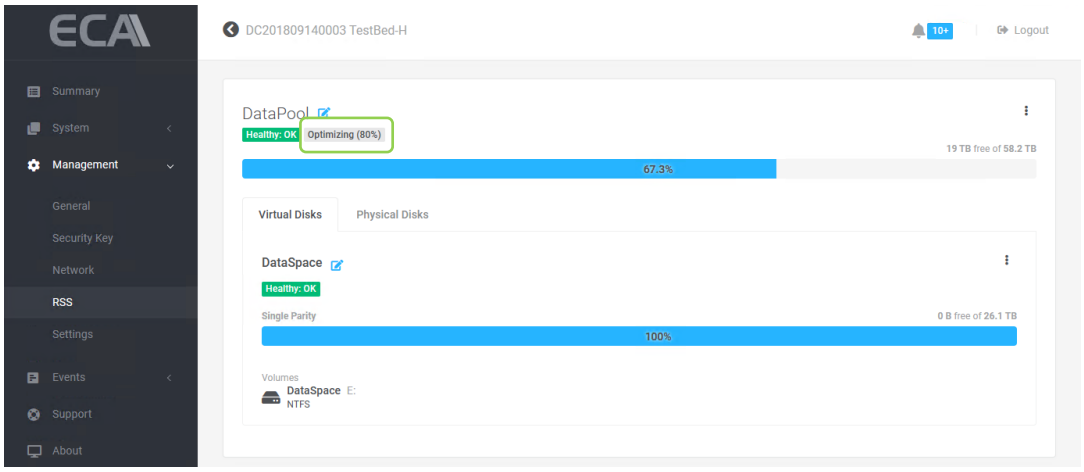


Figure 147: Optimizing storage pool

5. After the RSS optimization process is complete, go to Windows Device Manager to expand the RSS volume.

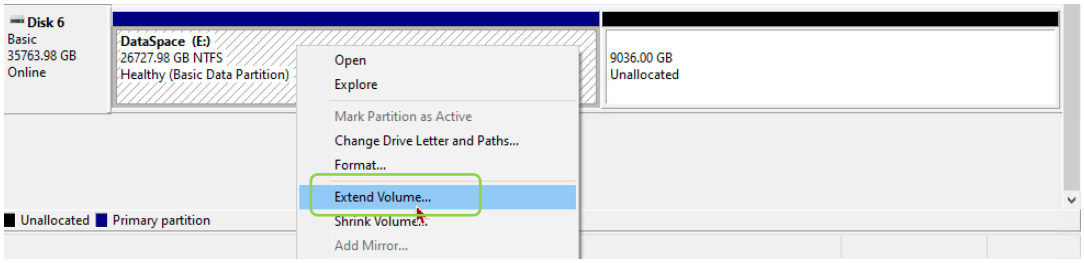


Figure 148: Extend volume in Disk Management (1 of 2)

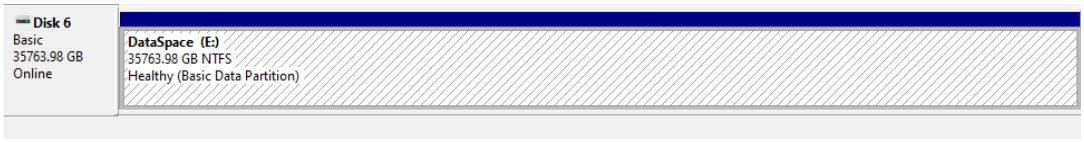


Figure 149: Extend volume in Disk Management (2 of 2)

9.4.4 Repair Storage Pool

If any of the RSS member disks are missing or faulty, ecaOS will notify you via email or desktop notification. To repair the storage pool, replace the missing or faulty disk with a new non-member disk.

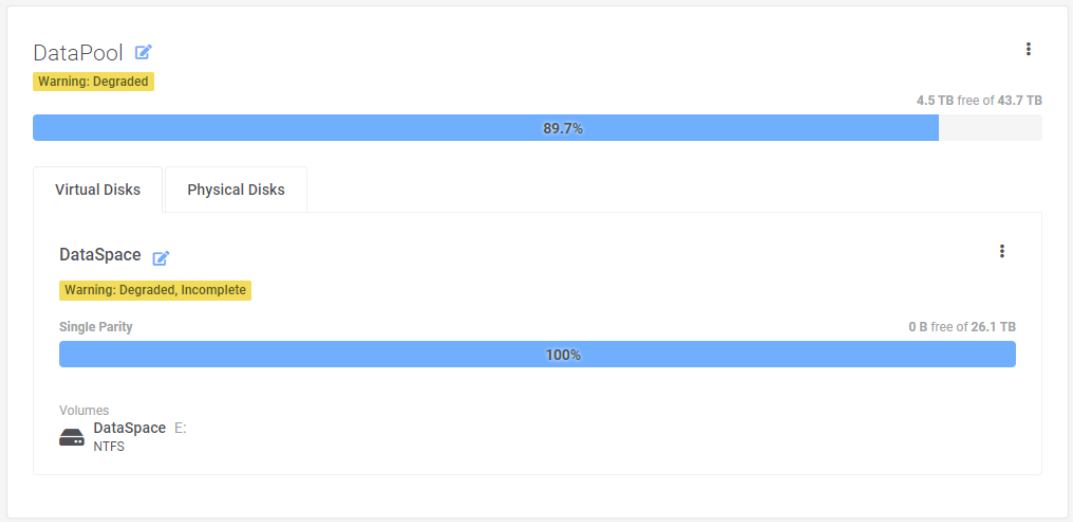


Figure 150: RSS Degraded

Figure 151: RSS Degraded Desktop notifications

1. To determine which member disks are 'Warning: lost communication,' go to the 'Physical Disks' tab. Then remove the faulty disk from the ECA.

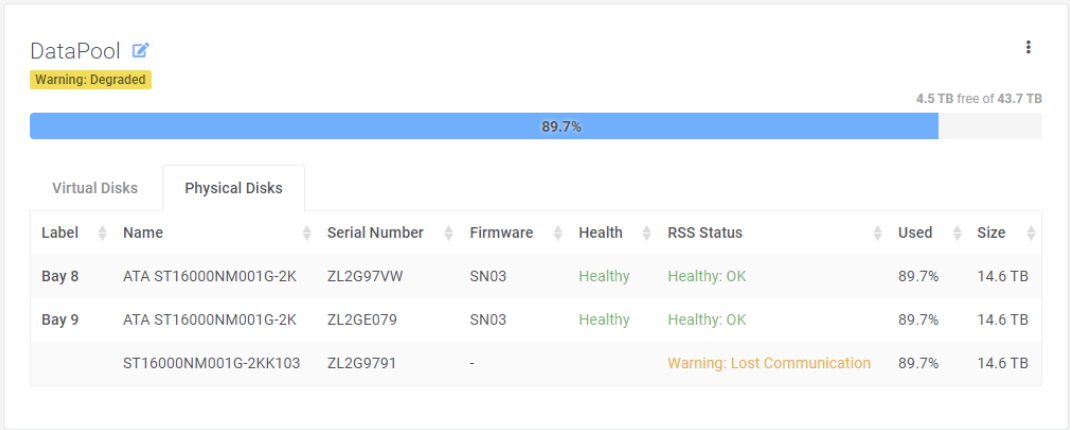


Figure 152: RSS member disk lost communication

2. Insert a new clean disk into the ECA, and then navigate to ‘System > Disk Guard’ to ‘Acknowledge’ the new replaced disk.

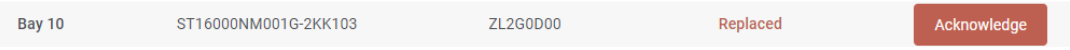


Figure 153: Acknowledge the replacement disk

3. Go to Management > RSS, the new replacement disk will be listed under Non-member Physical Disks.

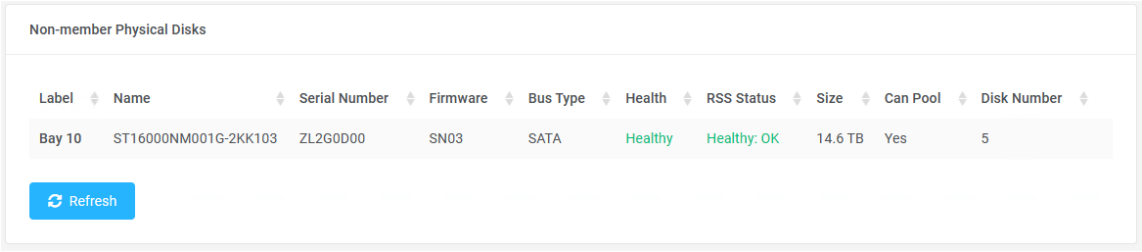


Figure 154: RSS non-member physical disks

4. Click on the '⋮' and select 'Repair Virtual Disks' to repair the virtual disk.

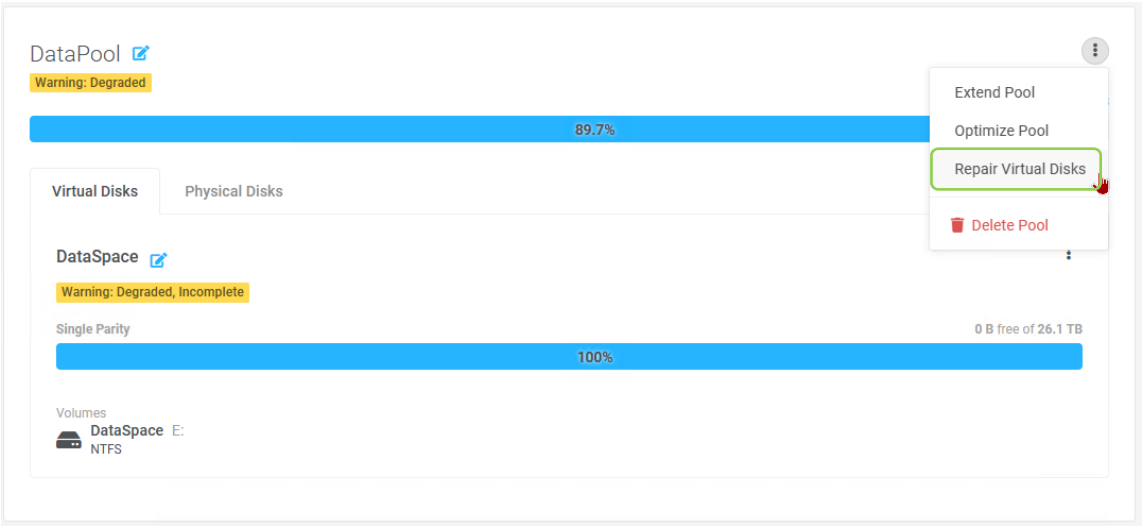


Figure 155: RSS non-member physical disks

5. Enter storage pool name and click on the 'Repair' button to start repair.

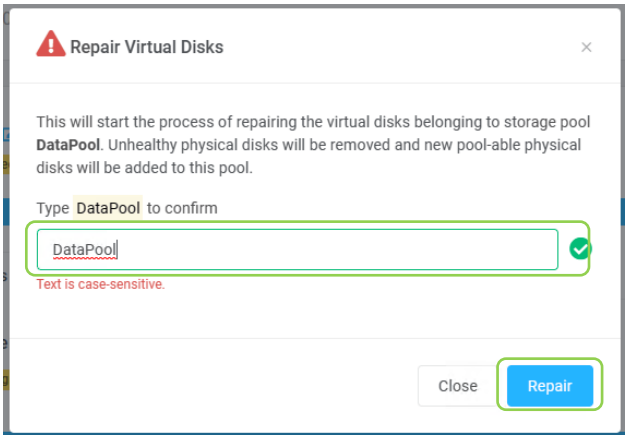


Figure 156: Confirm delete pool

6. After the RSS repair process is complete, the health of the storage pool and virtual disk will return to normal.

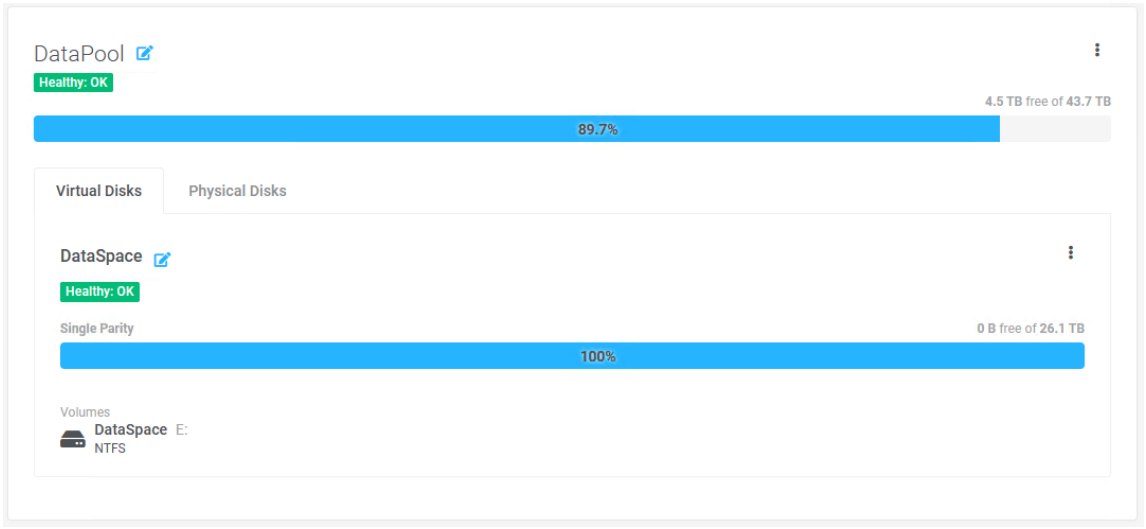


Figure 157: RSS healthy storage pool and virtual disk

9.5 Settings

Any event trigger can be set send email to respective personnel for any abnormal event.

9.5.1 Email Recipient Settings

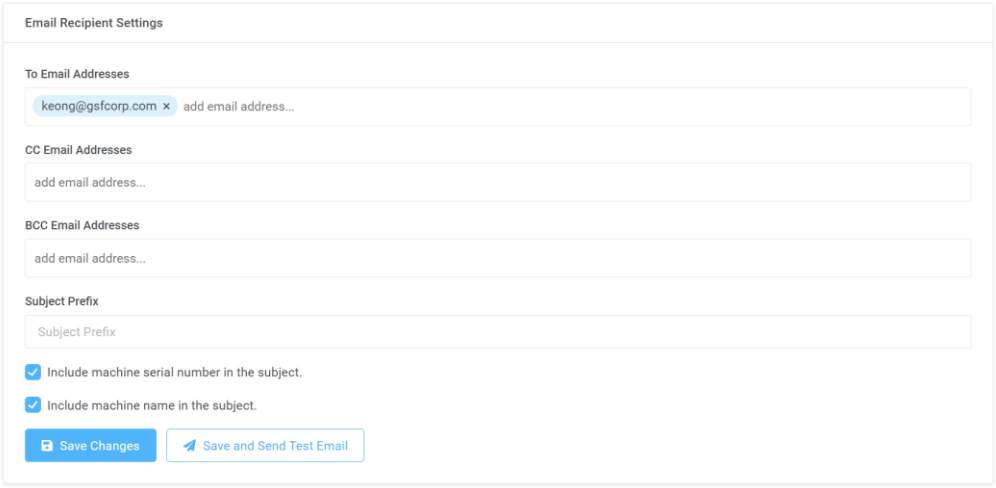


Figure 158: Email Setting (1 of 2)

9.5.2 Mail Servers

Click "+ Add Mail Server" and then follow the wizard to add a new SMTP server to add a new mail server.

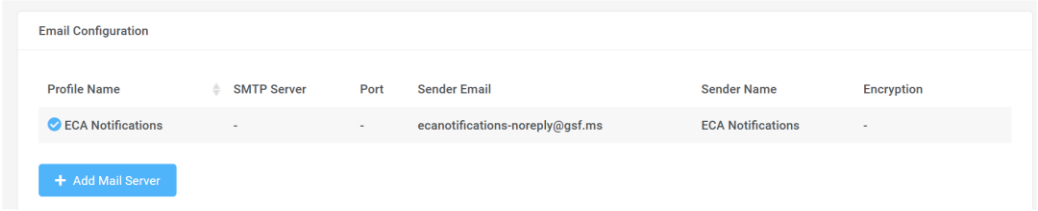


Figure 159: Email Setting (2 of 2)

9.5.3 Events

All monitoring application under System able to set notify in the desktop, send the email or both.

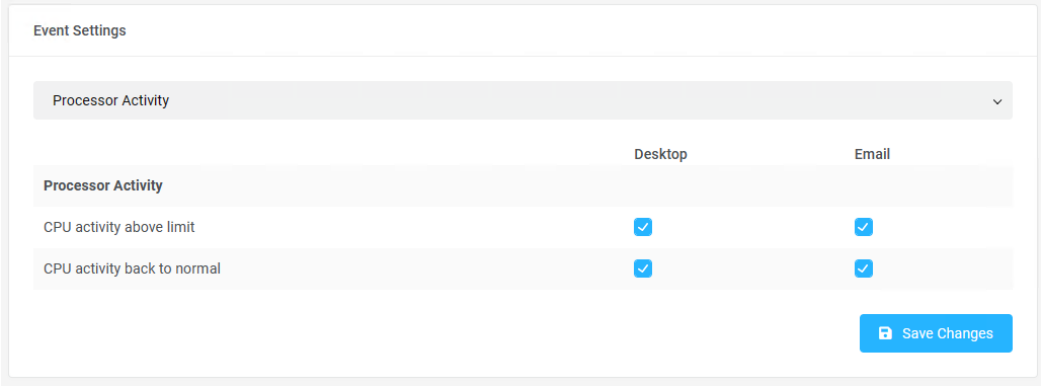


Figure 160: Events

1. Select event to be set by click drop down.

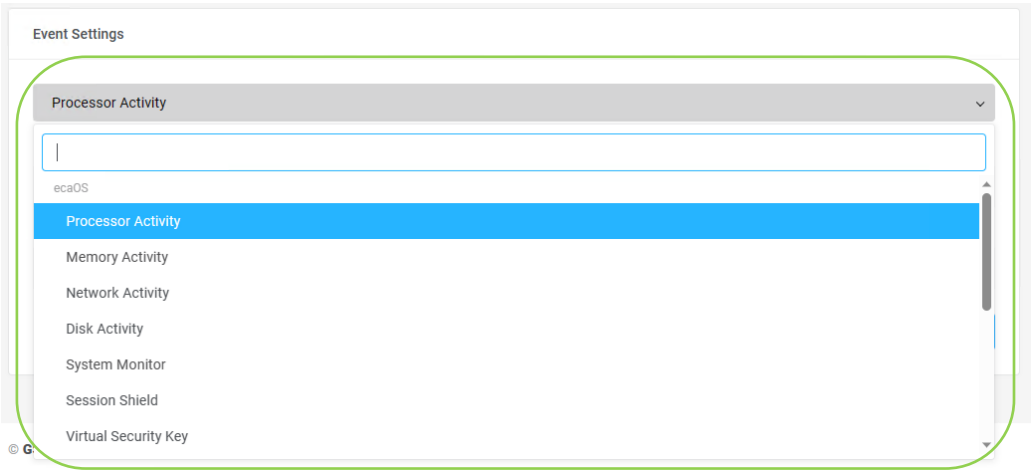


Figure 161: Select event (1 of 2)

2. Check the box to enable notification on the desktop or email and click 'Save Changes'
3. Setting below will notify user via Desktop notification and email if the memory usage above threshold limit. The user also will notify when the memory usage return to normal state

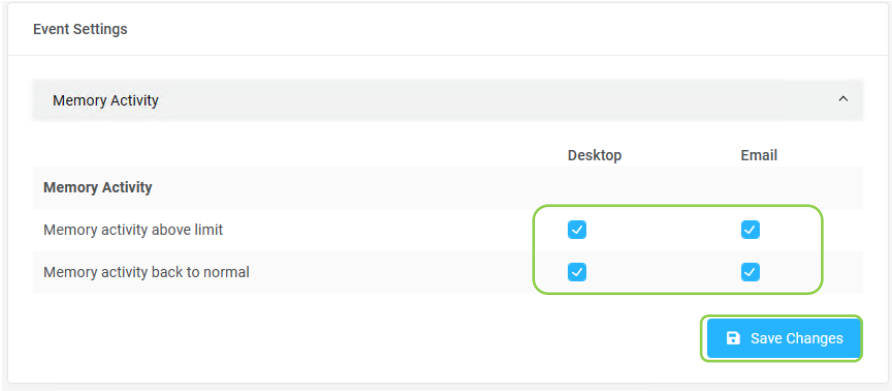


Figure 162: Select event (2 of 2)

9.5.3.1 Events List

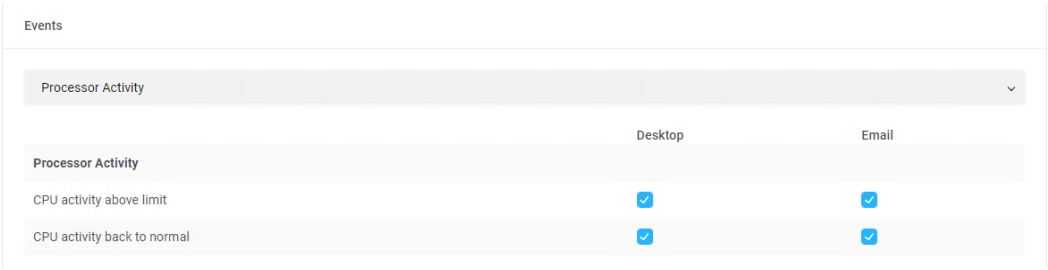


Figure 163: Processor Activity events notify setting

Figure 164: Memory Activity events notify setting

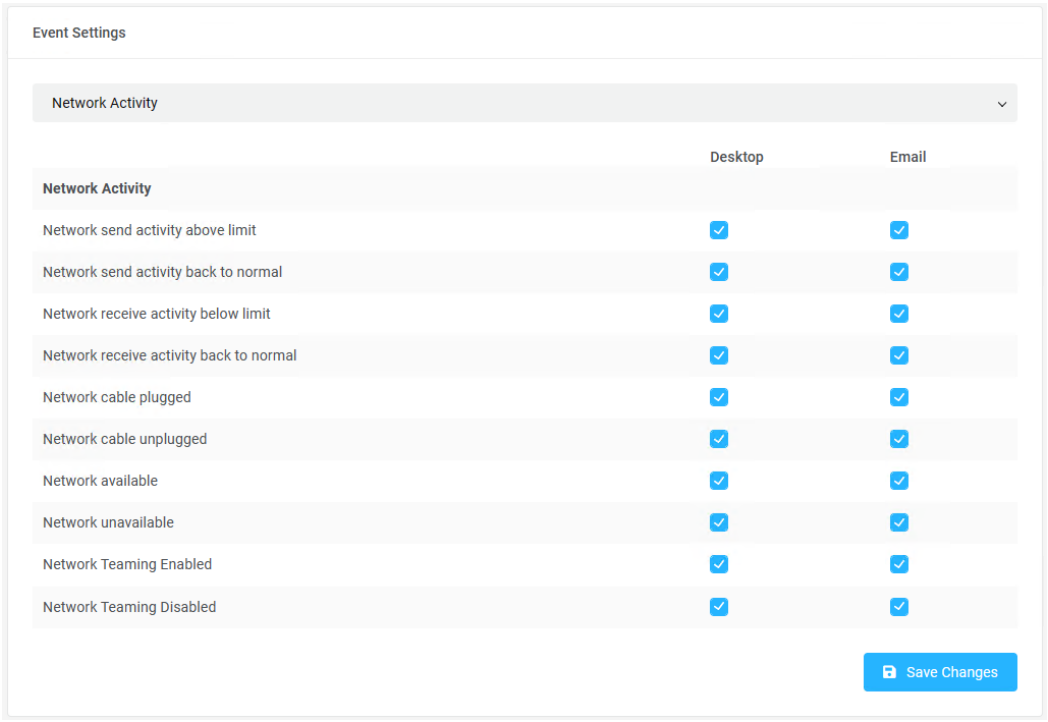


Figure 165: Network Activity events notify setting

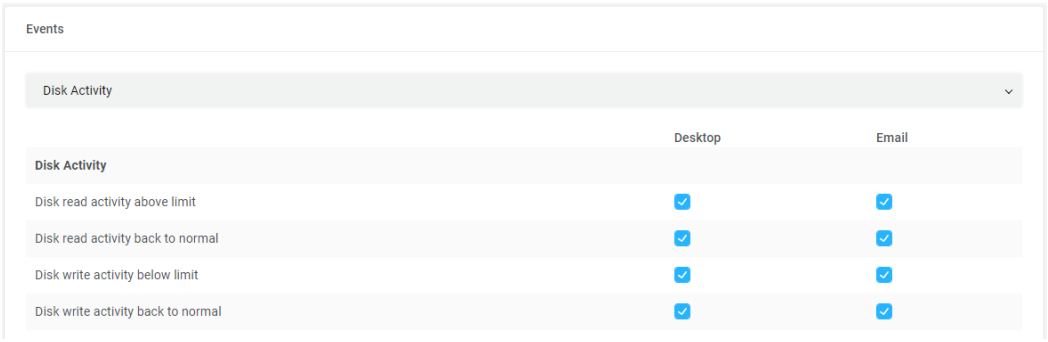


Figure 166: Disk Activity events notify setting

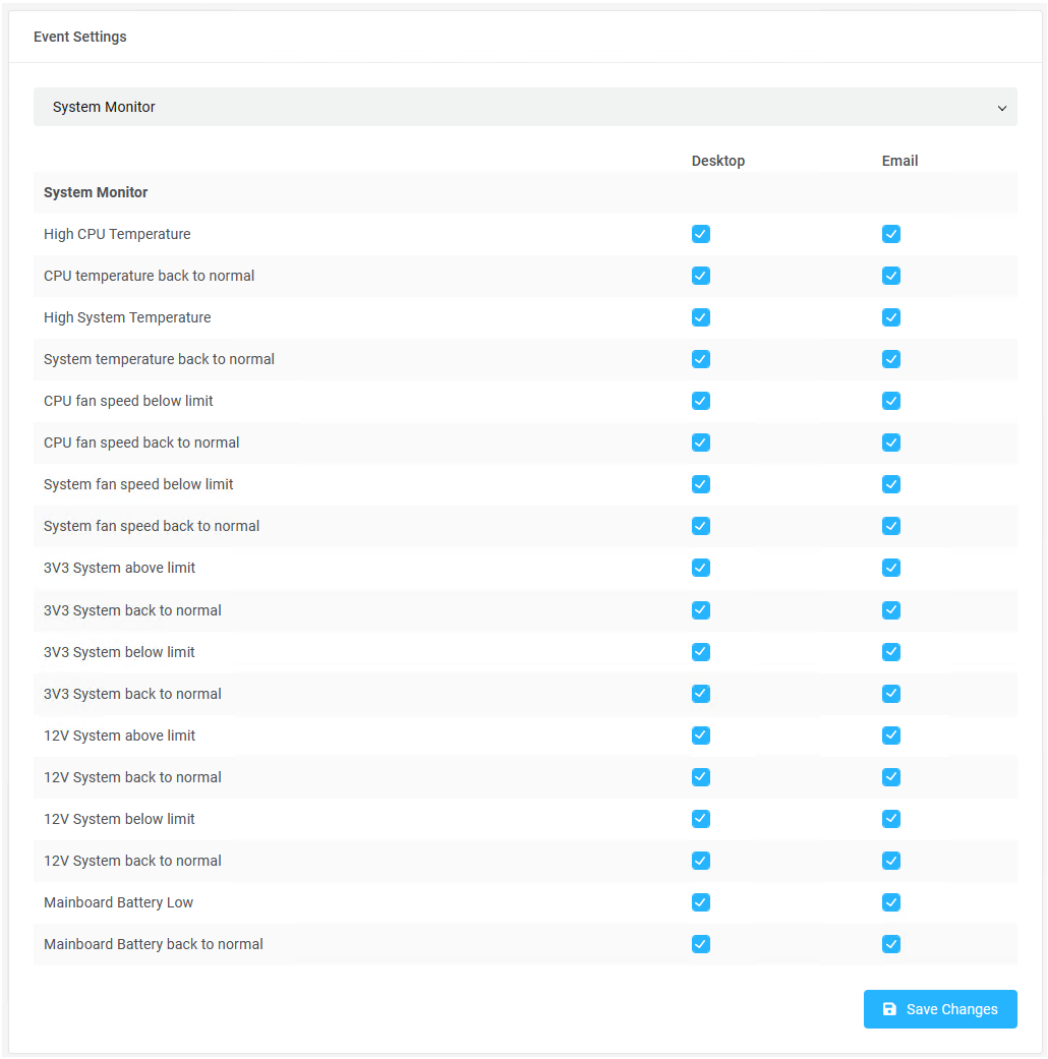


Figure 167: System Monitor events notify setting

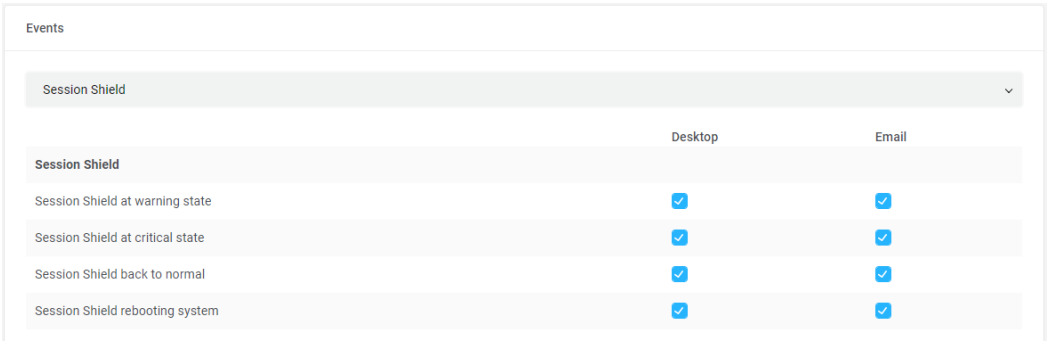


Figure 168: Session Shield events notify setting

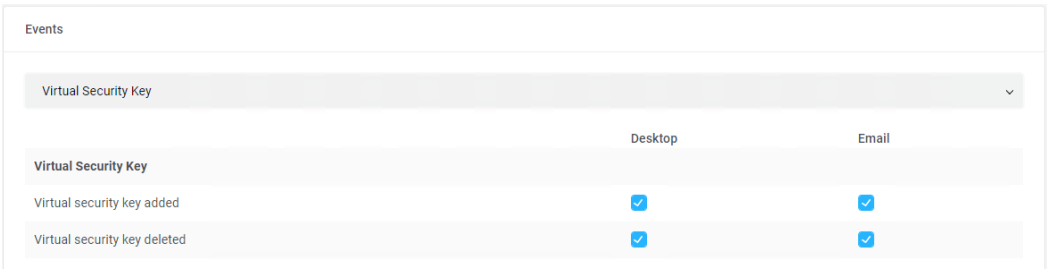


Figure 169: Virtual Security Key events notify setting

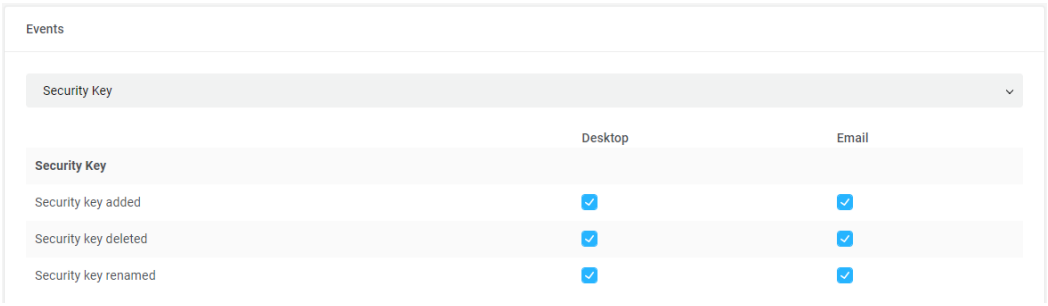


Figure 170: Security Key events notify setting

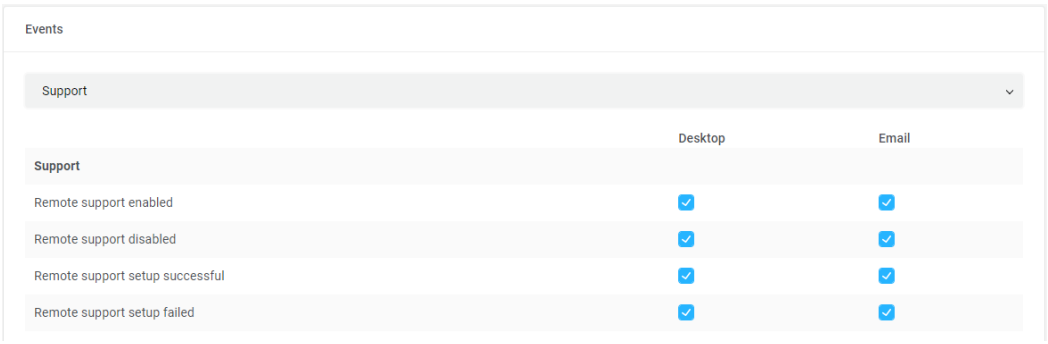


Figure 171: Support events notify setting

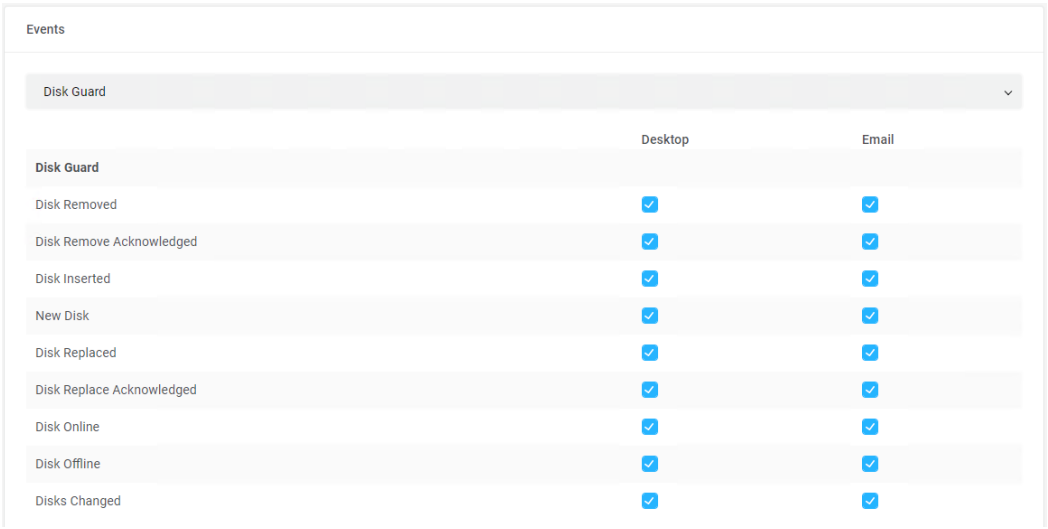


Figure 172: Disk Guard events notify setting

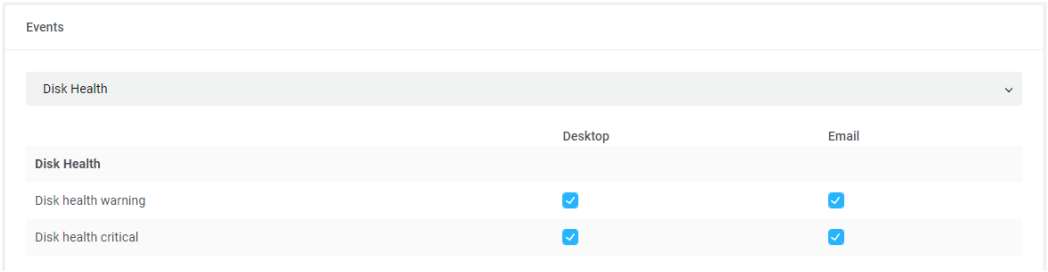


Figure 173: Disk Health events notify setting

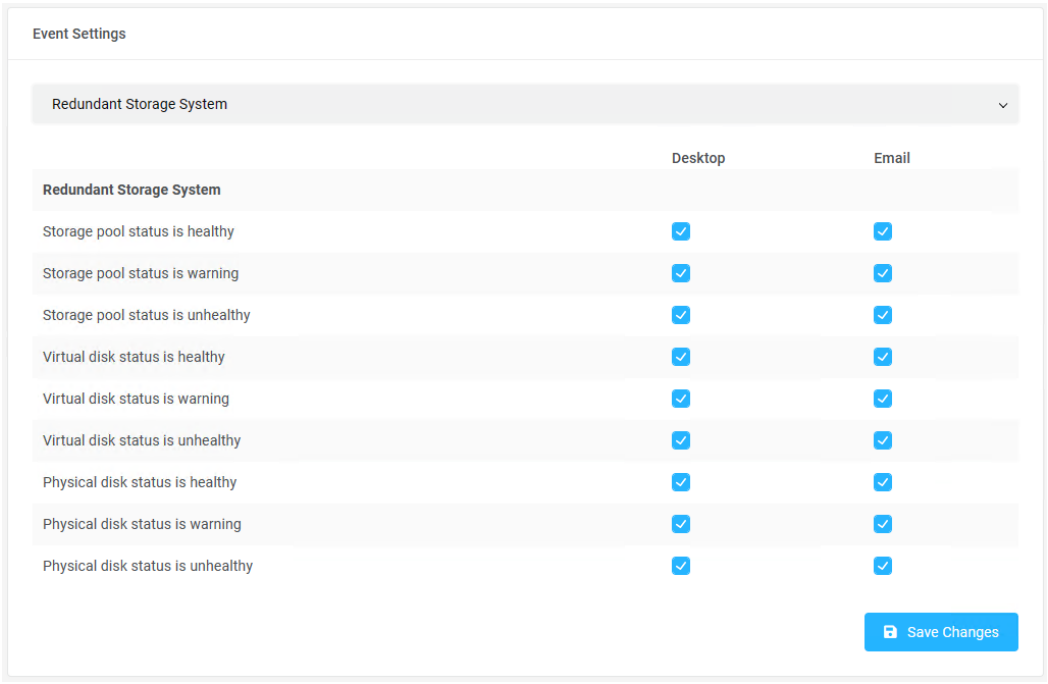


Figure 174: Redundant Storage System notify setting

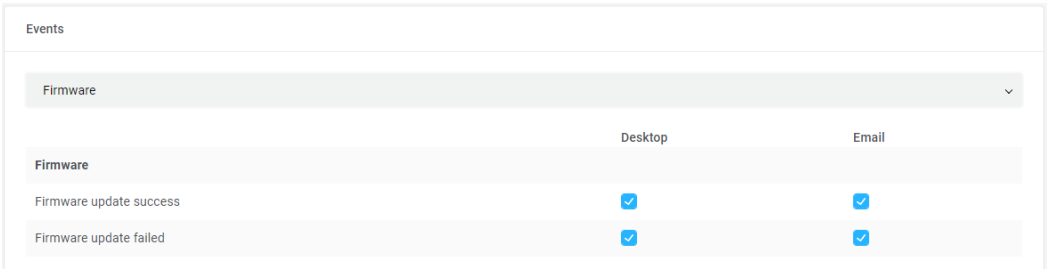


Figure 175: Heartbeat firmware events notify setting

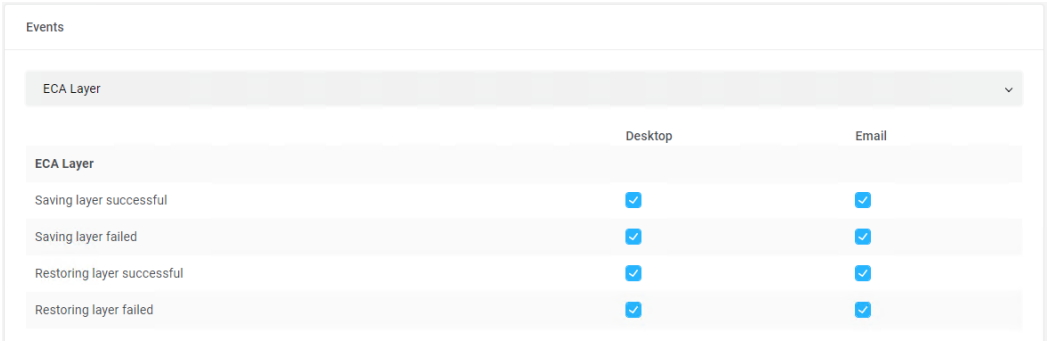


Figure 176: ECA Layer events notify setting

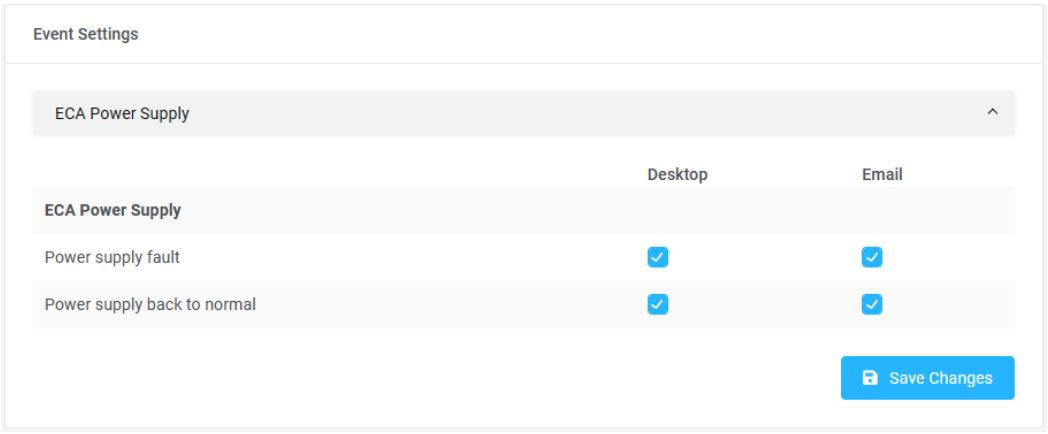


Figure 177: ECA Power Supply events notify setting (ONLY applies to ECA45 with TBSP-ECAPSU-R600 power supply unit)

9.5.4 SNMP Settings

Users can monitor ECA with network management software by using SNMP (Management > Settings > SNMP Settings). The following protocols are currently supported: SNMPv1, SNMPv2c, and SNMPv3.

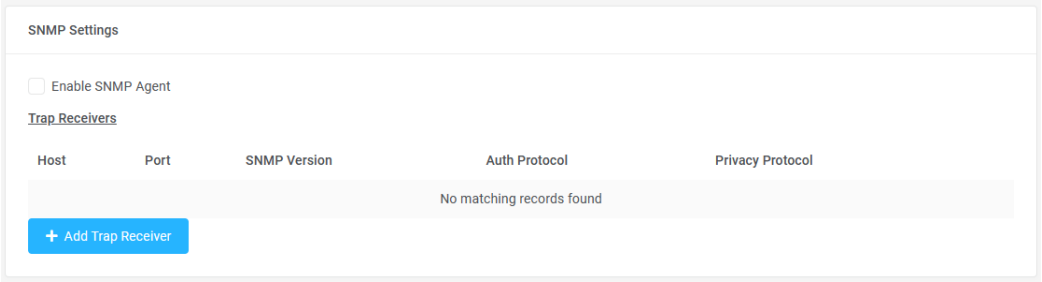


Figure 178: SNMP Settings

9.5.4.1 Enable SNMP

1. Tick Enable SNMP Agent, click the Add Trap Receiver button and follow the steps below.
    a. Enter the host IP address.
    b. Enter the port number of the host.
    c. Select the SNMP version.
    d. Enter a community name.
    e. Click the Save button.

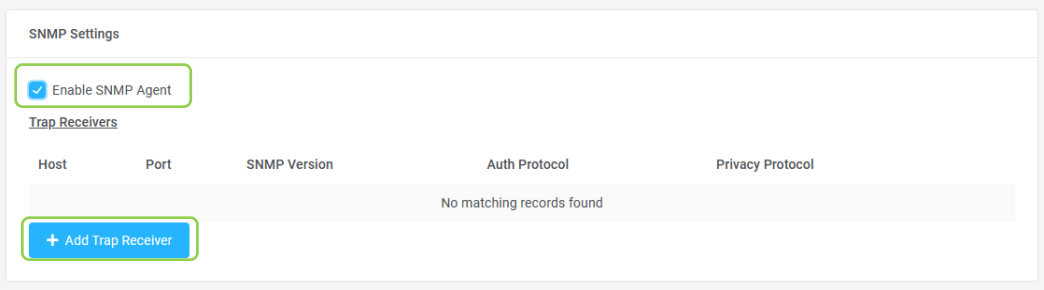


Figure 179: Enable SNMP

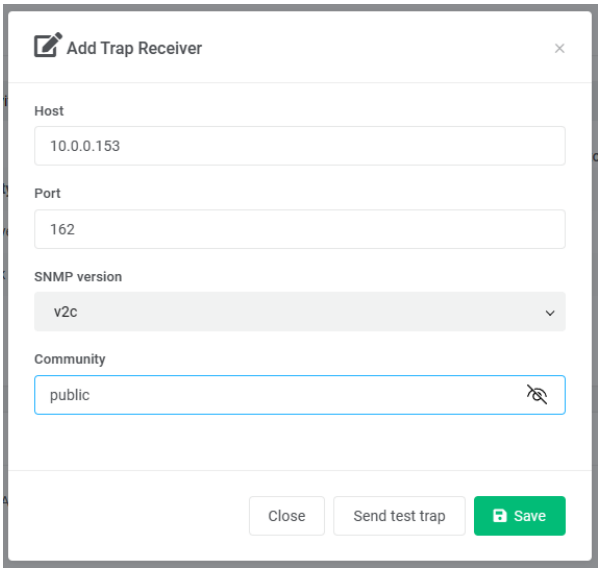


Figure 180: Add SNMP Trap Receiver

9.5.4.2 Download ECA MIB Files

GSF provides management information base (MIB) of ECA, which allows users to monitor ECA using network management systems, such as system, disk, and network statuses.

Please obtain the ECA MIB files from

“C:\Program Files (x86)\GSF\ecaOS\Services\MqttSnmpAgent\MiB.zip”.

10 Events

10.1 Notification

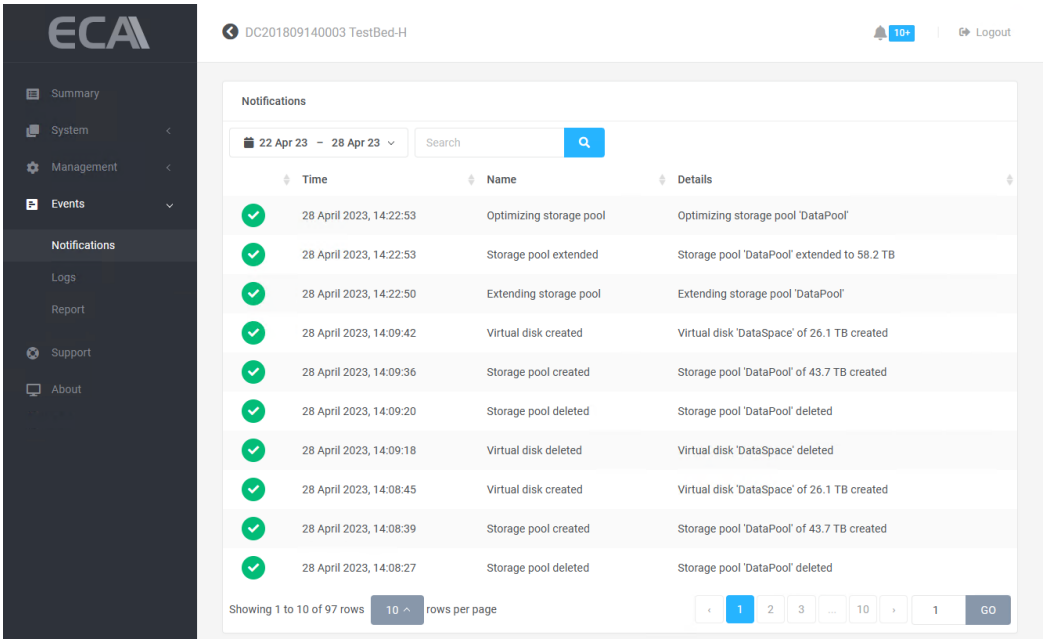


Figure 181: Notification

10.2 Logs

An event log is a file that contains information about usage, operations and activity of the ECA system. The log can be filtered by specifying data range and/or inserting keyword(s).

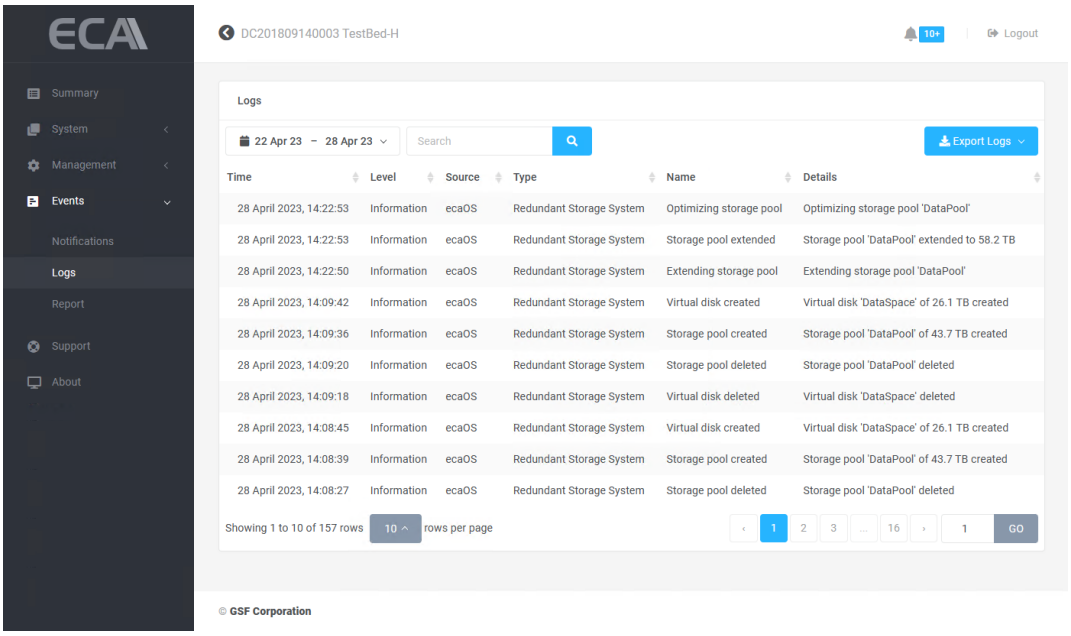


Figure 182: Log

10.2.1 Filtering Log

Filter by can choose by Today, Yesterday, Last 3 days, Last 7 Days, Last 30 Days or Custom data range.

Type any keyword and click on magnetify glass icon to start filtering. Click ‘Apply’ to filter the Logs.

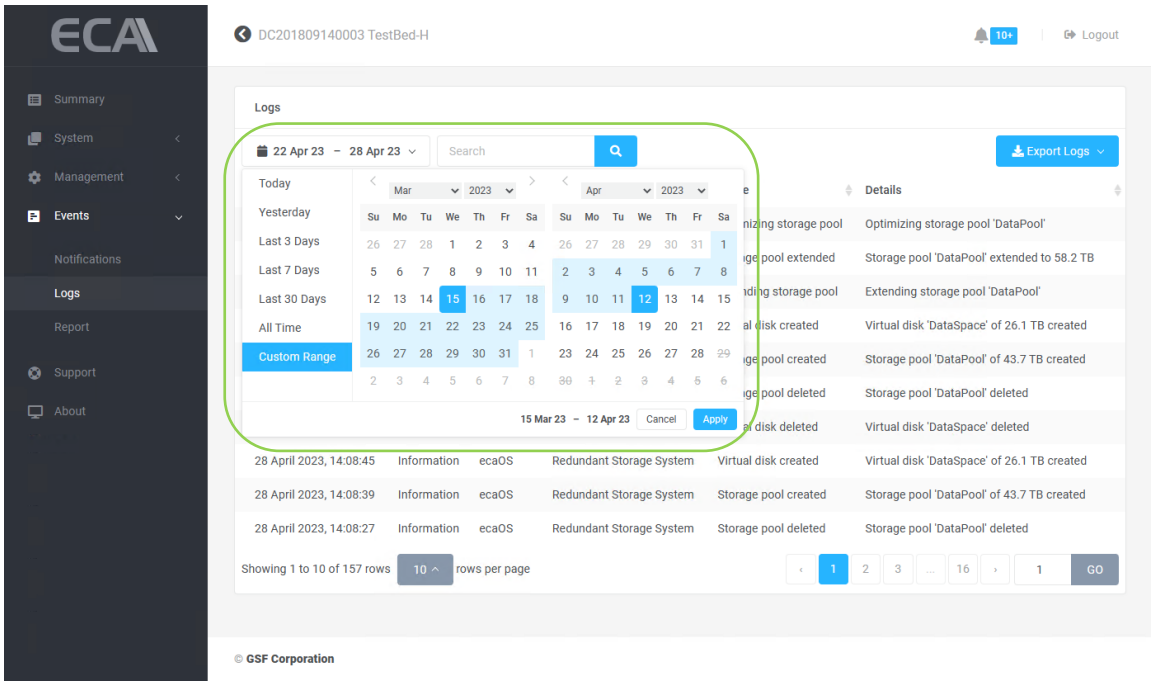


Figure 183: Filter log

10.2.2 Exporting Log

1. Click on the ‘Export Logs’ button

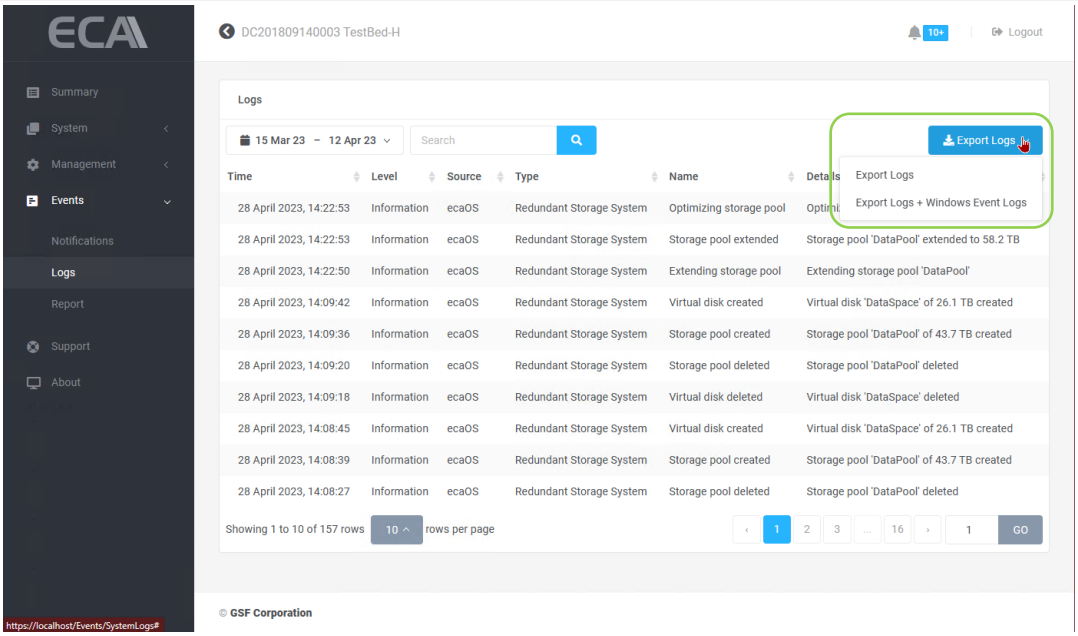


Figure 184: Export Log (1 of 8)

2. Click OK to start export the current log

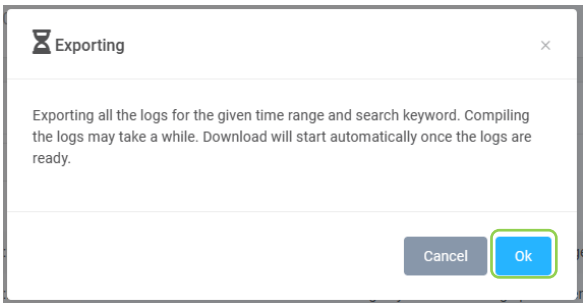


Figure 185: Export Log (2 of 8)

3. The log will export to Downloads folder in compress format

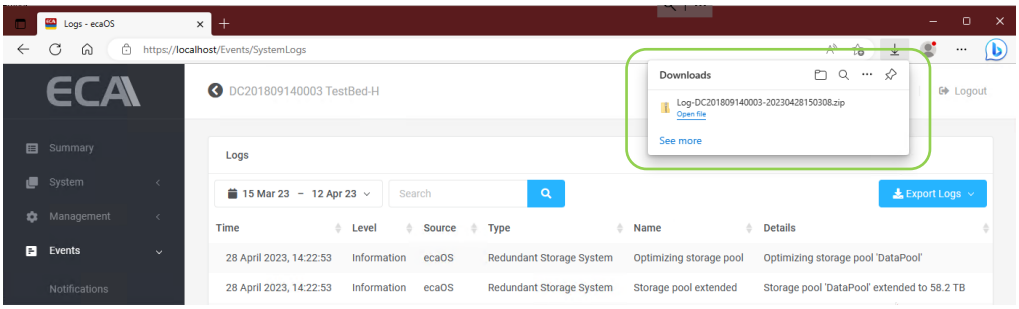


Figure 186: Export Log (3 of 8)

4. The log will be export to under Downloads. The exported log can be retrieved via Explorer.

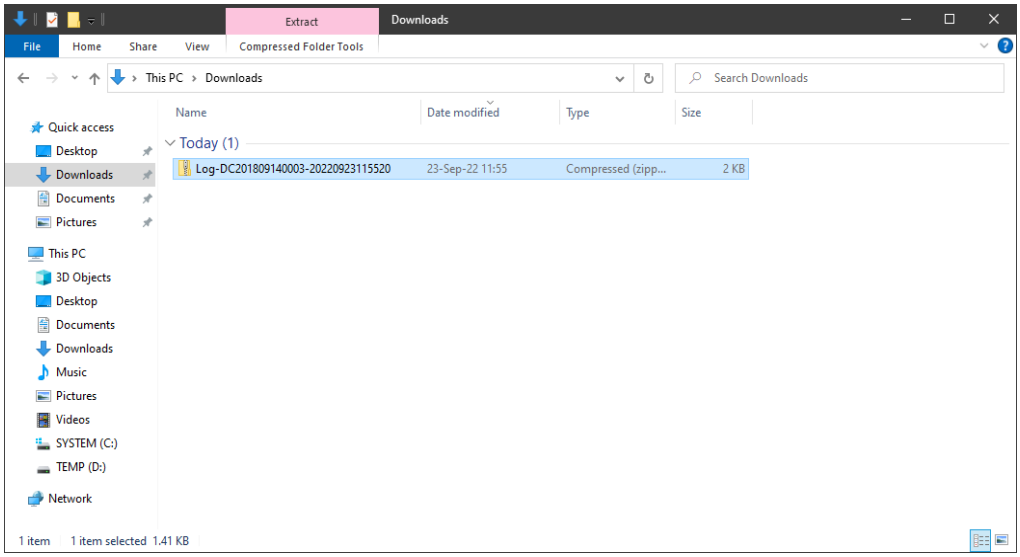


Figure 187: Exporting log (4 of 8)

5. Extract the file by right click on the file and select Extract All.

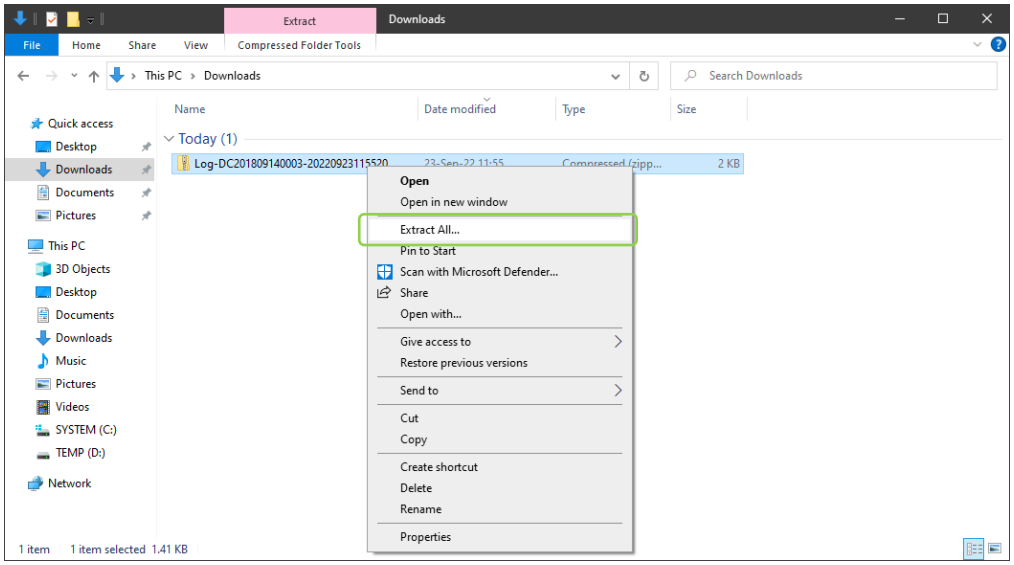


Figure 188: Exporting log (5 of 8)

6. Choose the location to extra the file and click Extract button.

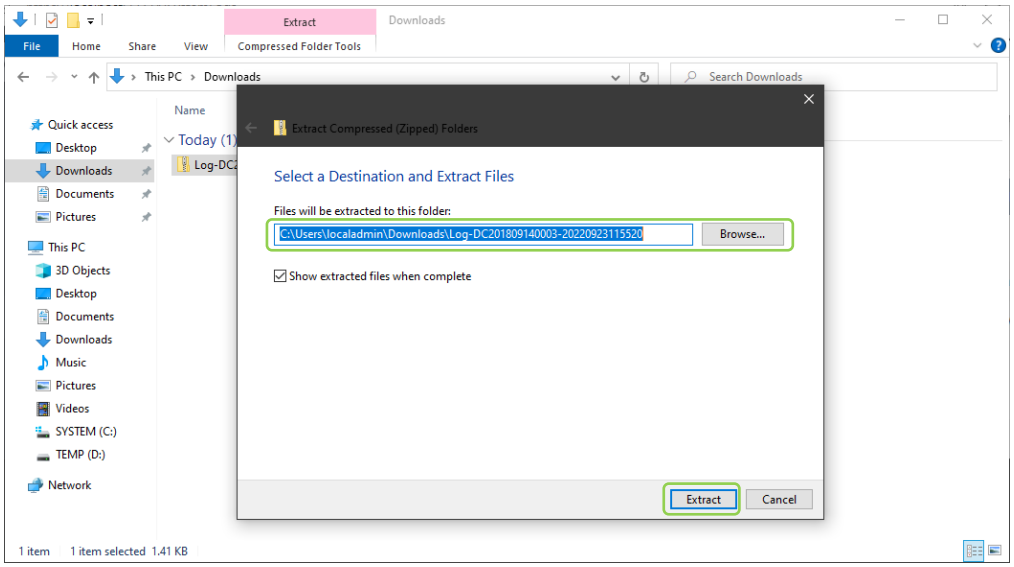


Figure 189: Exporting log (6 of 8)

7. The log file saved in comma-separated values (CSV) format.

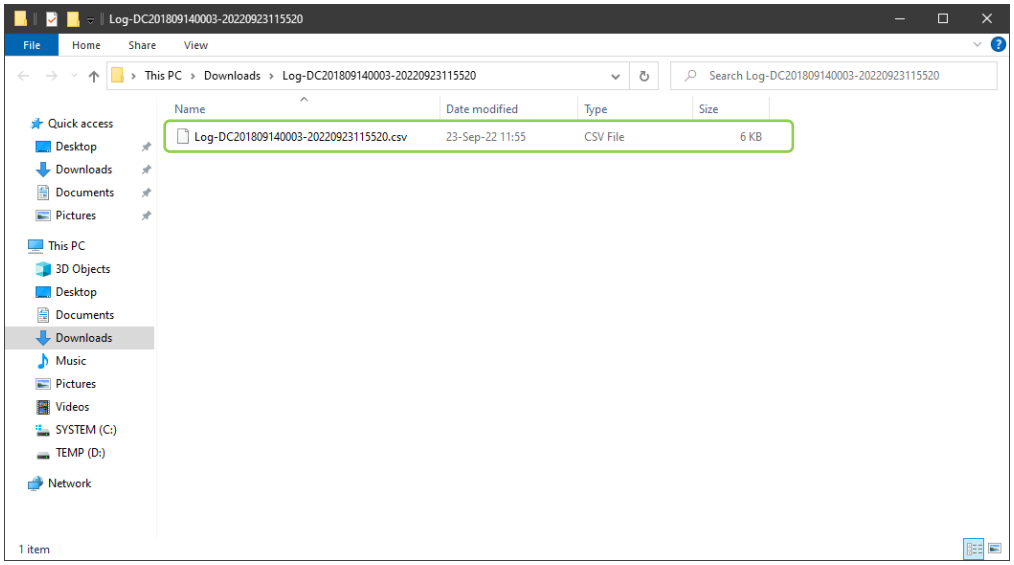


Figure 190: Exporting log (7 of 8)

8. Use Spreadsheet program to open the log file.

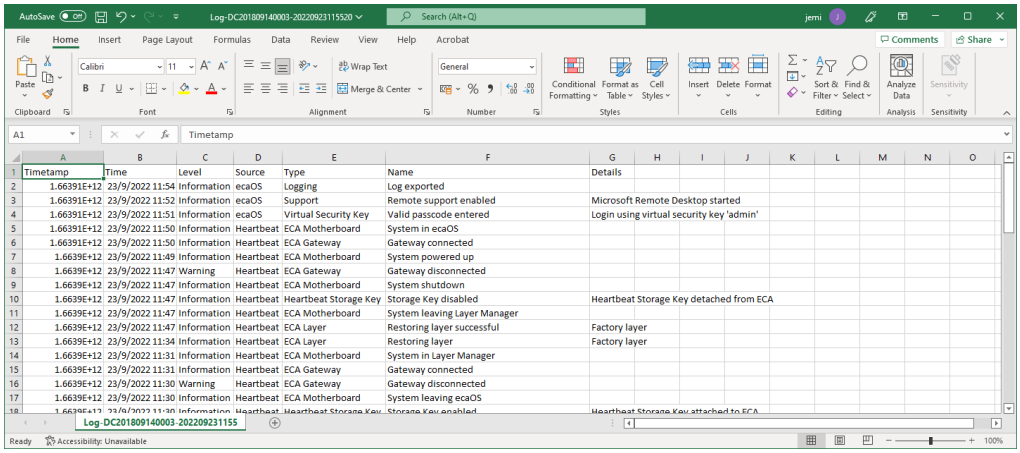


Figure 191: Exporting log (8 of 8)

10.3 Report

Report will be auto generated and sent to all recipients daily at: 23:55 or manually download by click on the ‘Download System Report’ button.

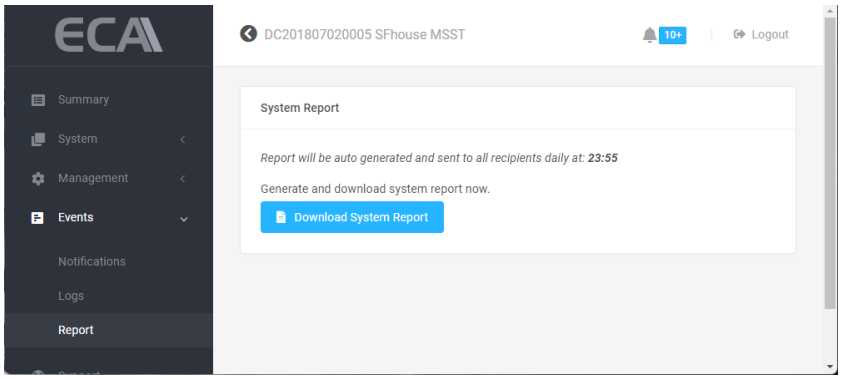


Figure 192: Manual Report Download at Events > Report section

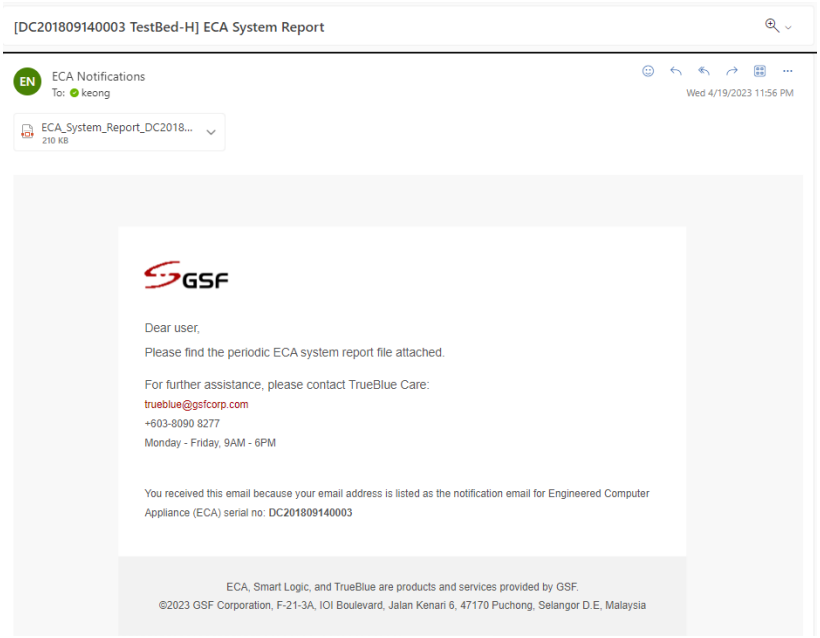
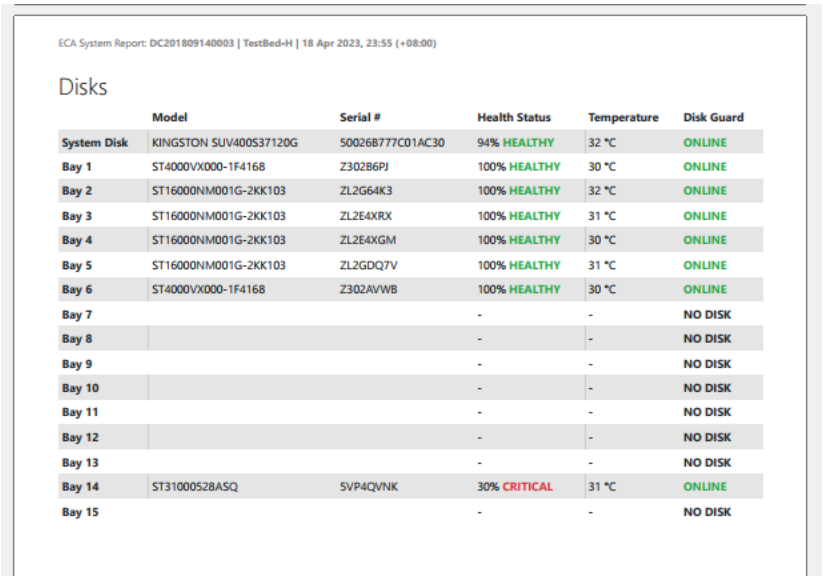


Figure160A: ECA email an ECA report



ECA System Report: DC20180914003 | TestBed-H | 18 Apr 2023, 23:55 (+08:00)

Disks

	Model	Serial #	Health Status	Temperature	Disk Guard
System Disk	KINGSTON SUV400S37120G	50026B777C01AC30	94% HEALTHY	32 °C	ONLINE
Bay 1	ST4000VX000-1F4168	Z302B6PJ	100% HEALTHY	30 °C	ONLINE
Bay 2	ST16000NM001G-2KK103	ZL2G64K3	100% HEALTHY	32 °C	ONLINE
Bay 3	ST16000NM001G-2KK103	ZL2E4XRX	100% HEALTHY	31 °C	ONLINE
Bay 4	ST16000NM001G-2KK103	ZL2E4XGM	100% HEALTHY	30 °C	ONLINE
Bay 5	ST16000NM001G-2KK103	ZL2GDQ7V	100% HEALTHY	31 °C	ONLINE
Bay 6	ST4000VX000-1F4168	Z302AVWB	100% HEALTHY	30 °C	ONLINE
Bay 7			-	-	NO DISK
Bay 8			-	-	NO DISK
Bay 9			-	-	NO DISK
Bay 10			-	-	NO DISK
Bay 11			-	-	NO DISK
Bay 12			-	-	NO DISK
Bay 13			-	-	NO DISK
Bay 14	ST31000528ASQ	5VP4QVNK	30% CRITICAL	31 °C	ONLINE
Bay 15			-	-	NO DISK

Figure 193B: Example ECA report in PDF format

11 Support

11.1 Microsoft Remote Desktop

Microsoft Remote Desktop app to connect to a remote PC or virtual apps and desktops made available by your admin.

Click on ‘Start’ button under Microsoft Remote Desktop

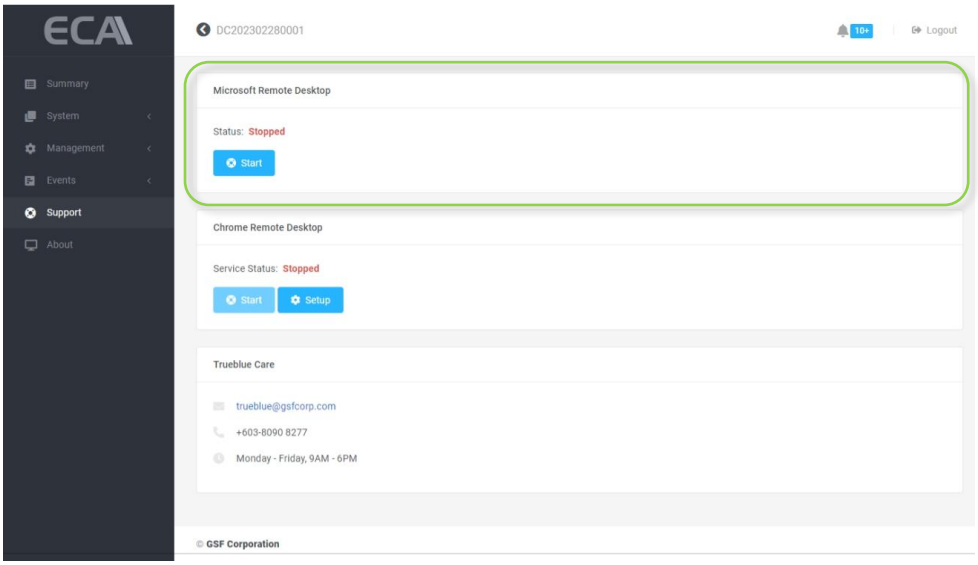


Figure 194: Microsoft Remote Support

From local PC. Enter computer name or IP address of the remote ECA.

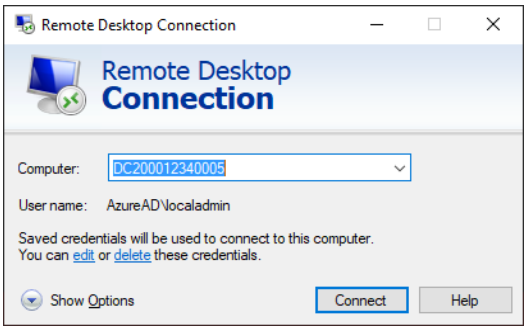


Figure 195: Trueblue Remote Support (1 of 2)

NOTE: You will require to port forward in your router to allowed Remote Desktop to be accessible via internet. Default port is 3389

11.2 Chrome Remote Desktop

This option allows you to access your ECA remotely from your PC/Laptop using your own Google account without require any port forwarding setting in the router. Before begin, Chrome Remote Desktop work in both Google Chrome or Microsoft Edge Browser, at the address bar type: https://remotedesktop.google.com/access then follow the directions to enabled Chrome Remote Desktop in your browser.

11.2.1 Setup ECA into your Chrome Remote Desktop

In your PC/Laptop, run Chrome/Edge and enter https://remotedesktop.google.com/headless

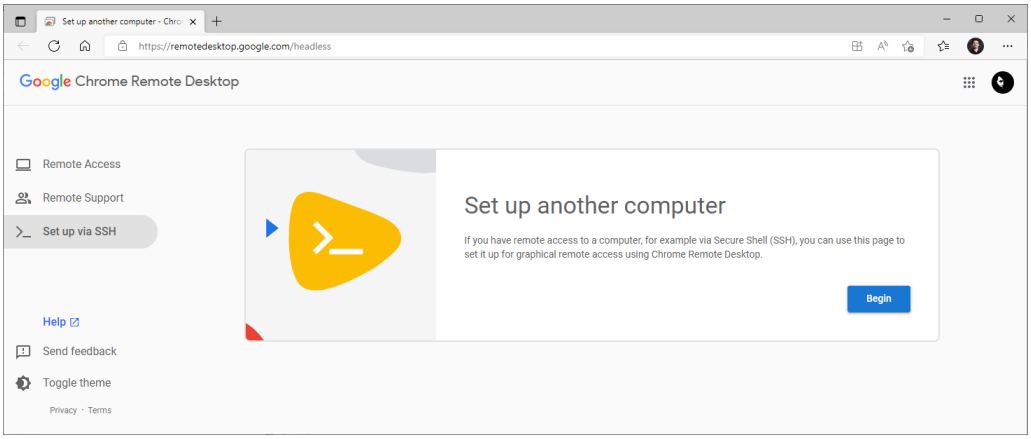


Figure 196: Chrome Remote Desktop (1 of 6)

1. Click 'Begin'

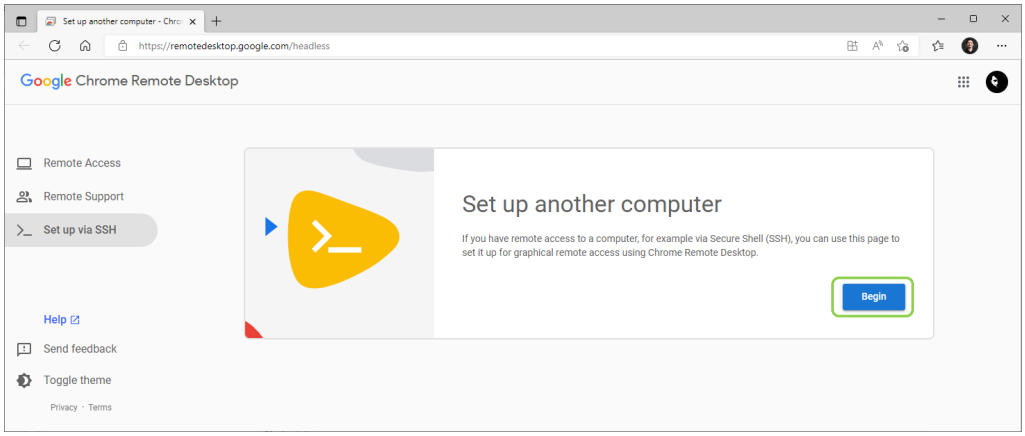


Figure 197: Chrome Remote Desktop (2 of 6)

2. Click 'Next'

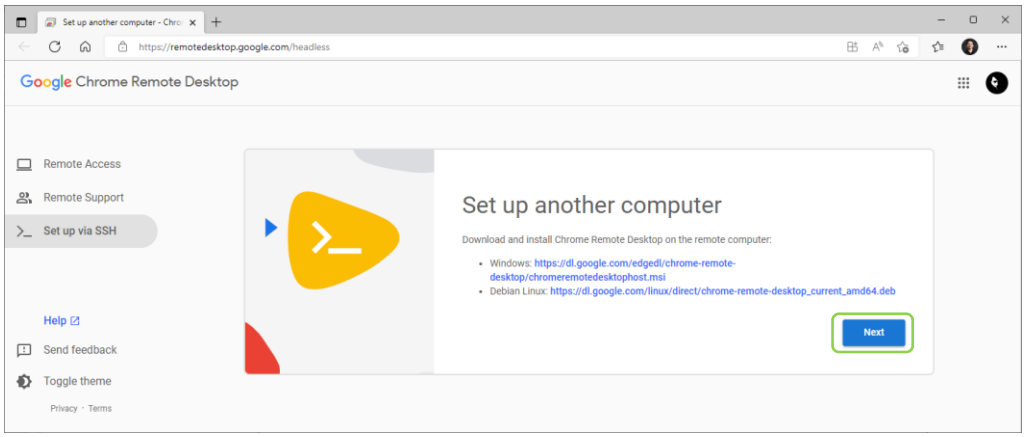


Figure 198: Chrome Remote Desktop (3 of 6)

3. Click 'Authorize'

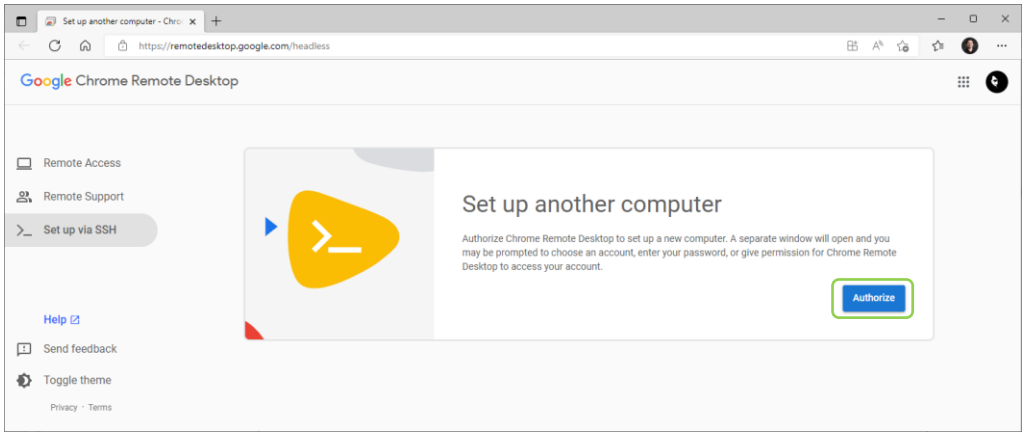


Figure 199: Chrome Remote Desktop (3 of 6)

4. Copy command for Windows (Cmd)

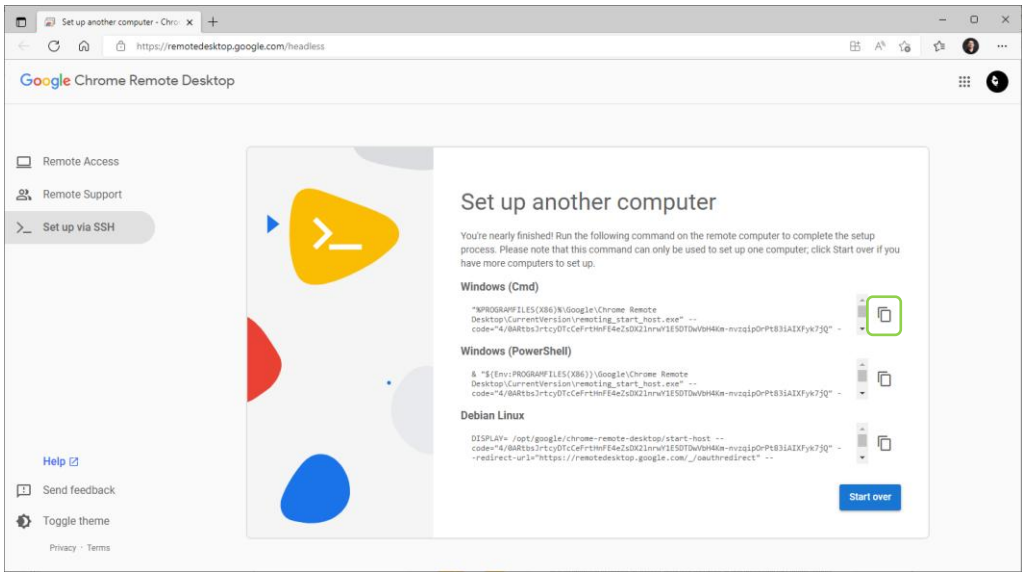


Figure 200: Chrome Remote Desktop (4 of 6)

5. From the ECA machine, go to Support. Under ‘Chrome Remote Desktop’, click setup

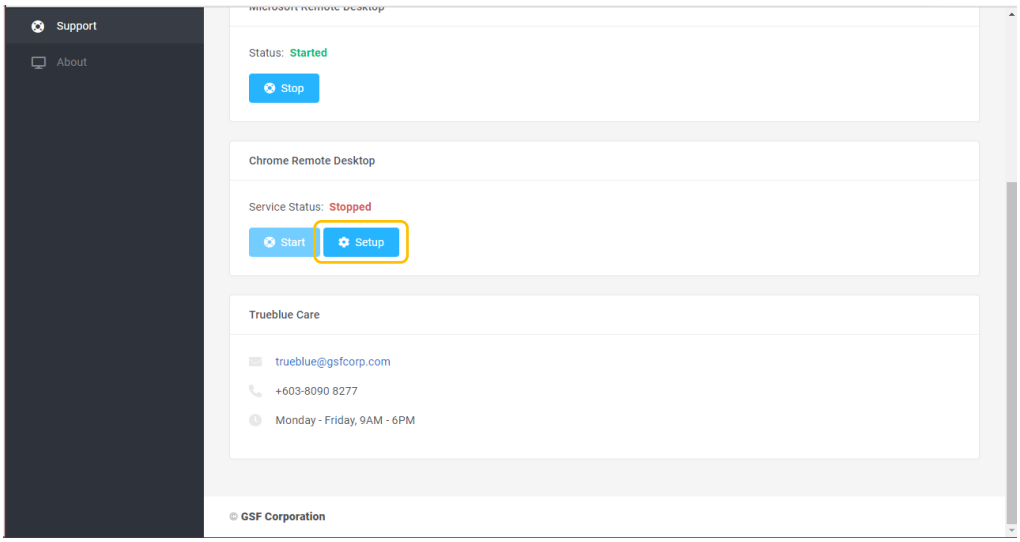


Figure 201: Chrome Remote Desktop (5 of 6)

6. Paste the command and enter 6-digit PIN number as a password.

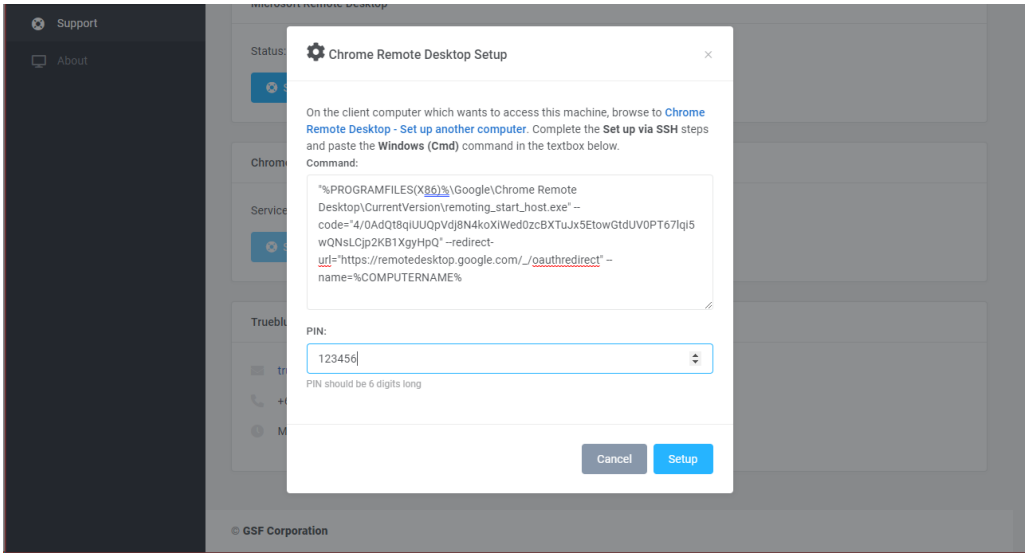


Figure 202: Chrome Remote Desktop (6 of 6)

11.2.2 Accessing ECA via Chrome Remote Desktop?

1. From the ECA will be remote. Make sure the service status Started

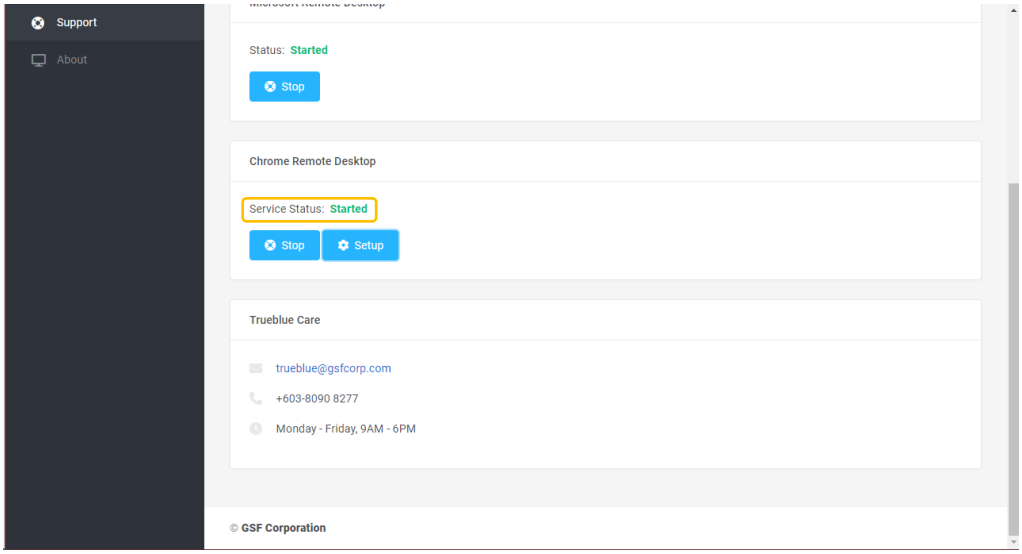


Figure 203: Accessing ECA via Chrome Remote Desktop (1 of 4)

2. From remote machine. Run web browser enter https://remotedesktop.google.com/access/. Click on remote devices.

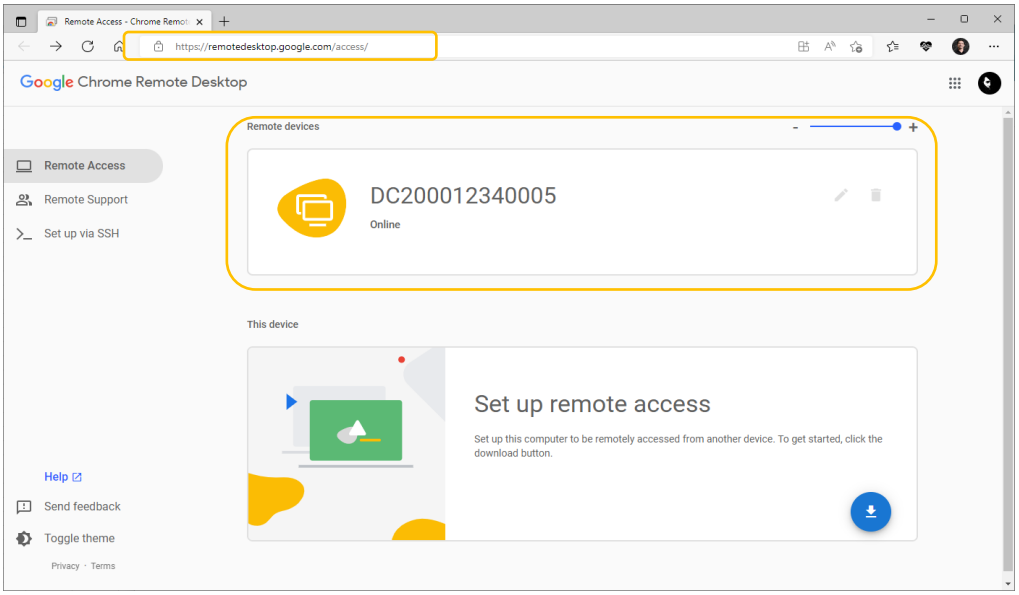


Figure 204: Accessing ECA via Chrome Remote Desktop (2 of 4)

3. Enter 6-digit PIN previously set during setup to start login

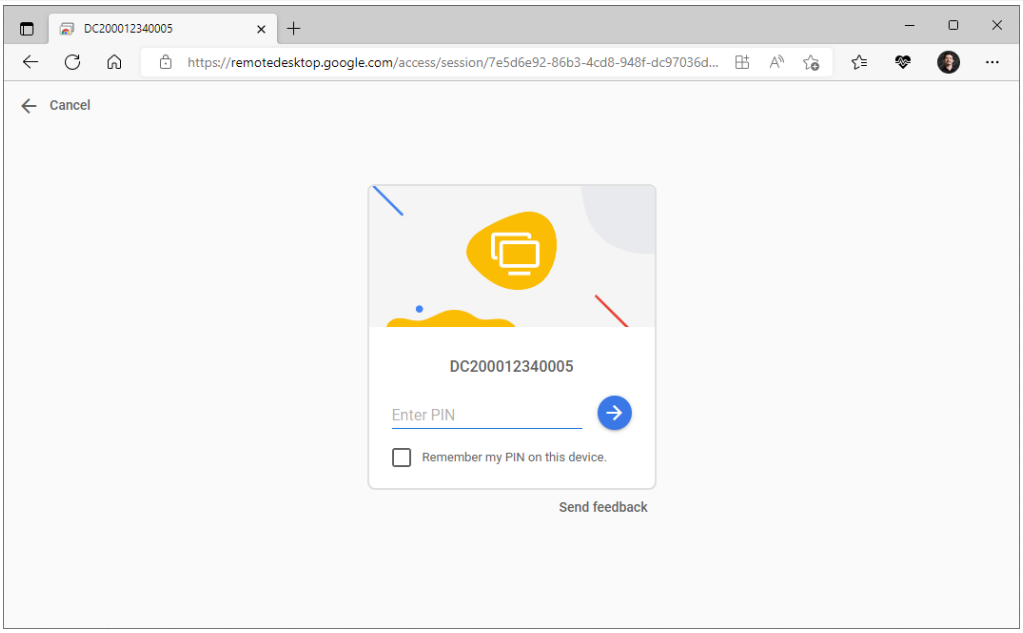


Figure 205: Accessing ECA via Chrome Remote Desktop (3 of 4)

4. Access the ECA

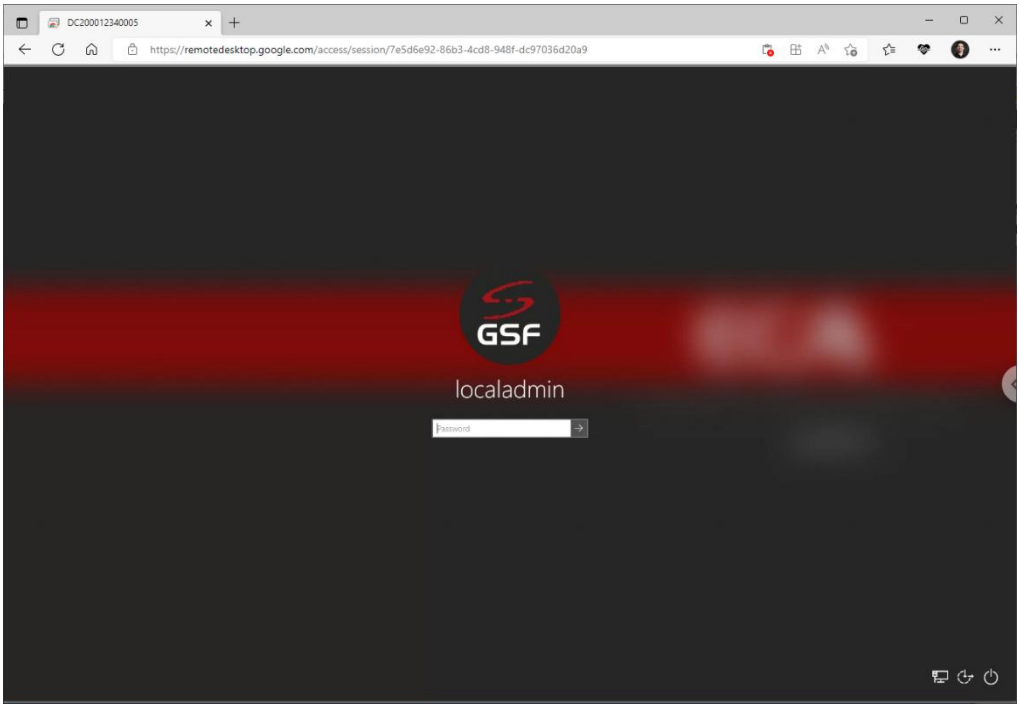


Figure 206: Accessing ECA via Chrome Remote Desktop (4 of 4)

12 About

12.1 Machine Information

The ECA information display here such as Model, Serial Number, ecaOS version, Up time, when last reboot.

The IP address will be display if the ECA connected to local LAN.

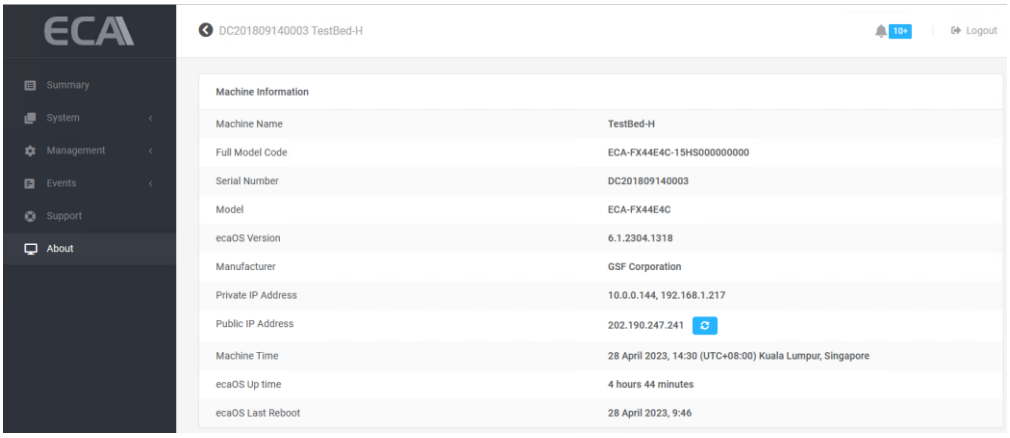


Figure 207: Machine Information

12.2 Heartbeat Information

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

‘Factory Layer Last Saved’ (Hard Reset) & Deployment Layer Last Saved’ (Soft Reset) it shows the date of the layer saved.

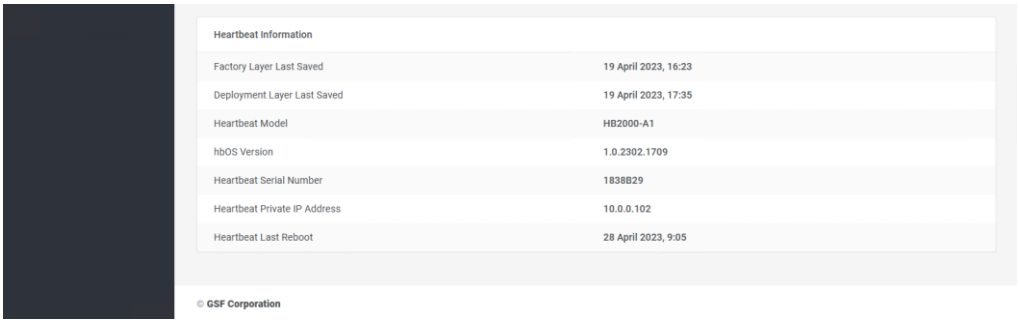


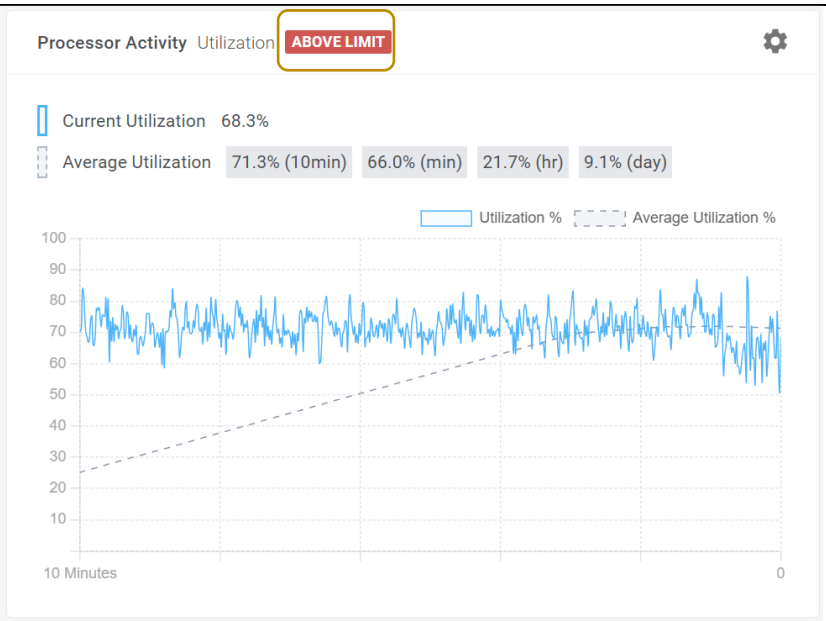
Figure 208: Heartbeat Information

13 APPENDIX

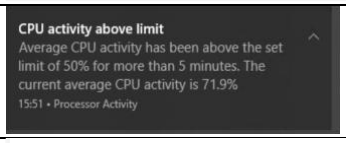
13.1 Processor Activity

13.1.1 CPU activity above limit

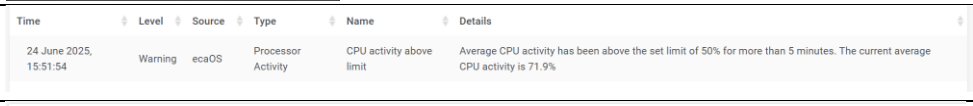
Dashboard



Notification

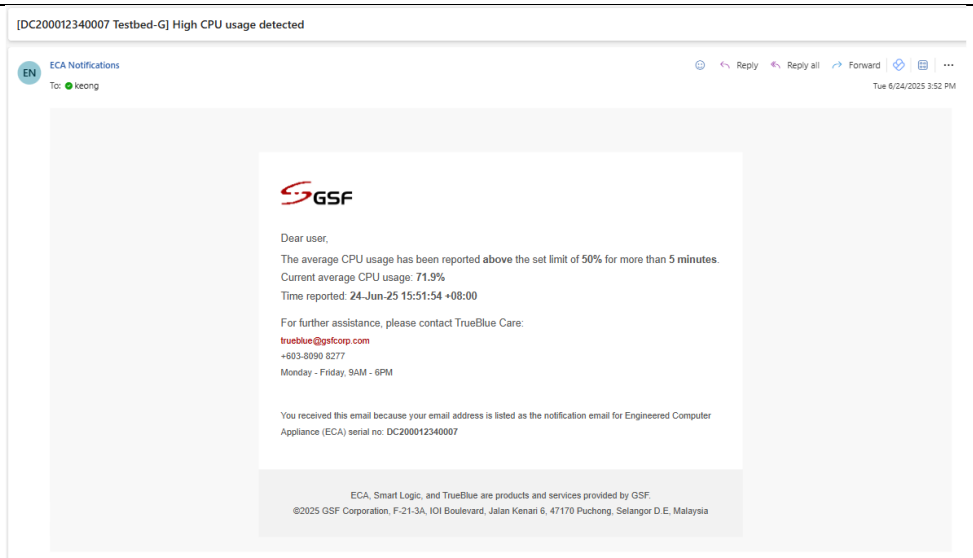


Log



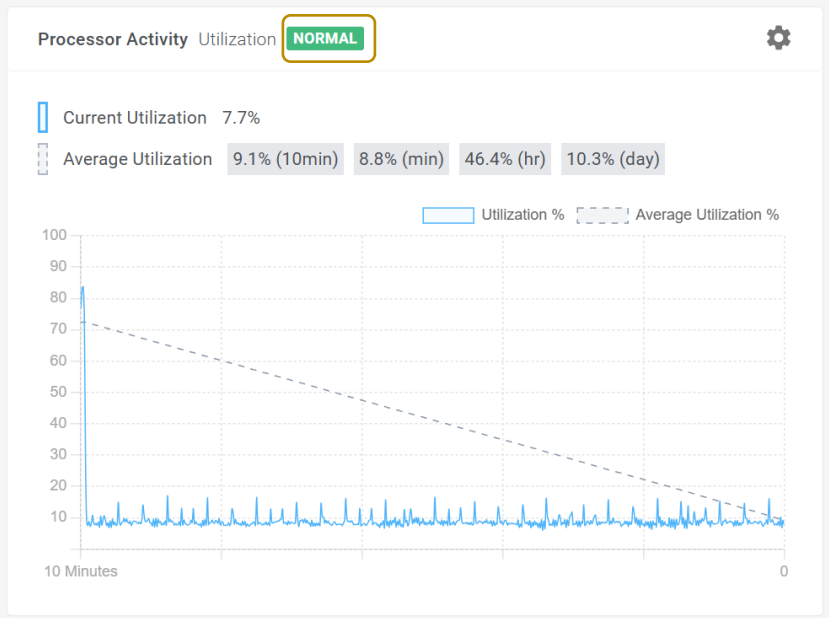
Time	Level	Source	Type	Name	Details
24 June 2025, 15:51:54	Warning	ecaOS	Processor Activity	CPU activity above limit	Average CPU activity has been above the set limit of 50% for more than 5 minutes. The current average CPU activity is 71.9%

Email

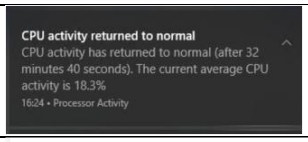


13.1.2 CPU activity back to normal

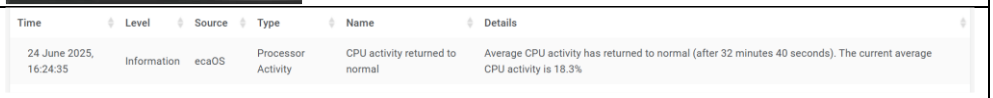
Dashboard



Notification

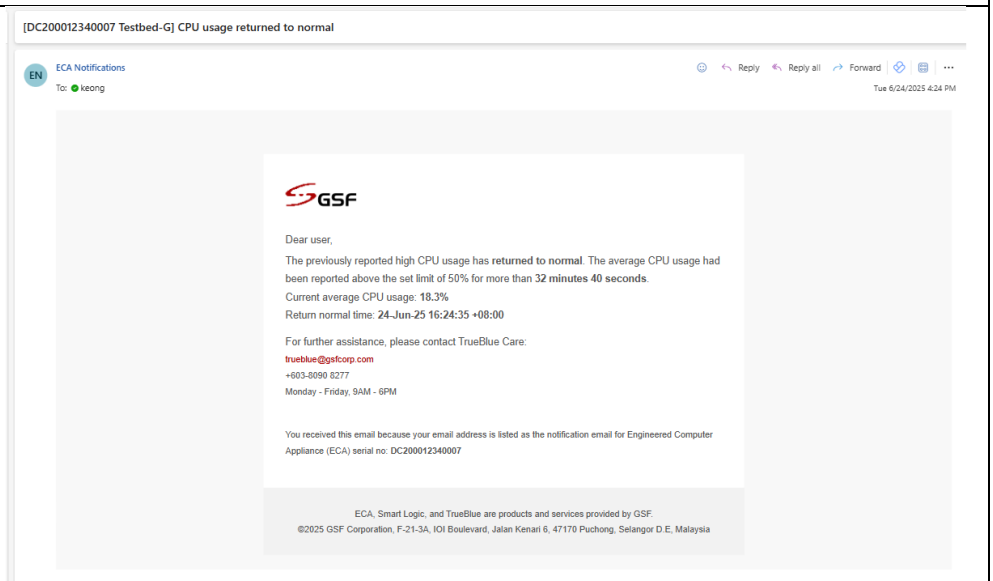


Log



Time	Level	Source	Type	Name	Details
24 June 2025, 16:24:35	Information	ecaOS	Processor Activity	CPU activity returned to normal	Average CPU activity has returned to normal (after 32 minutes 40 seconds). The current average CPU activity is 18.3%

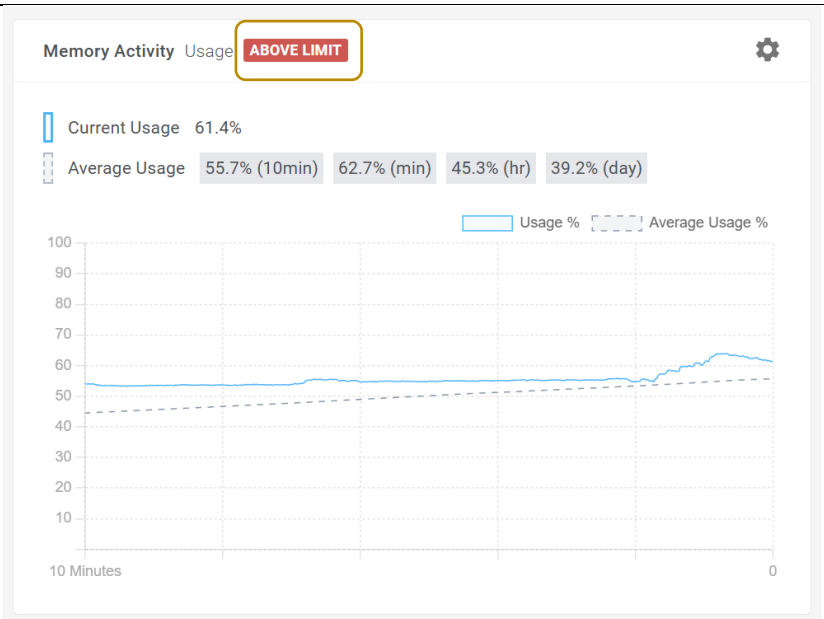
Email



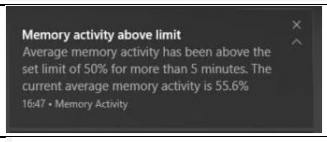
13.2 Memory Activity

13.2.1 Memory usage above limit

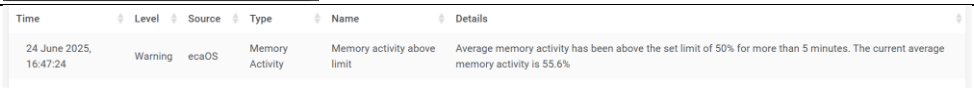
Dashboard



Notification

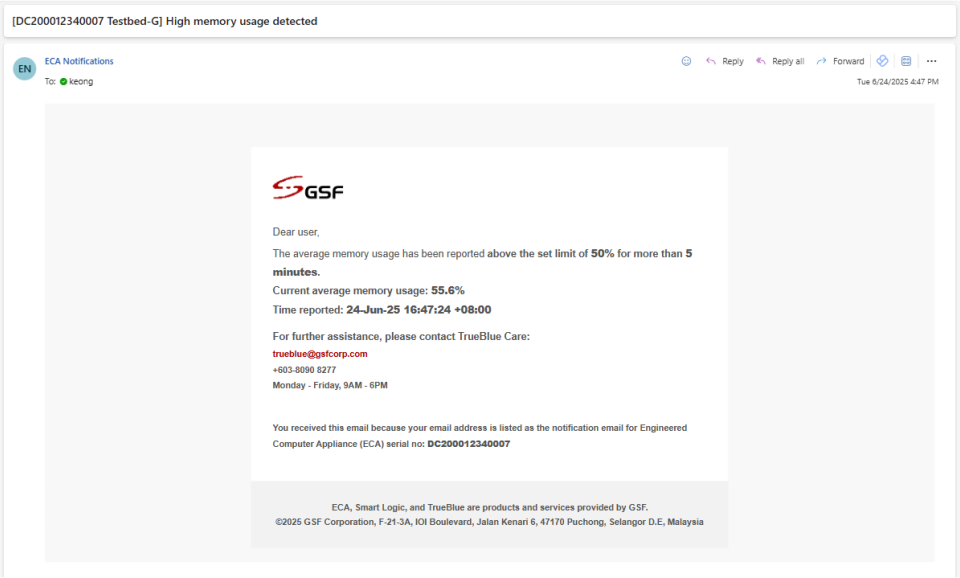


Log



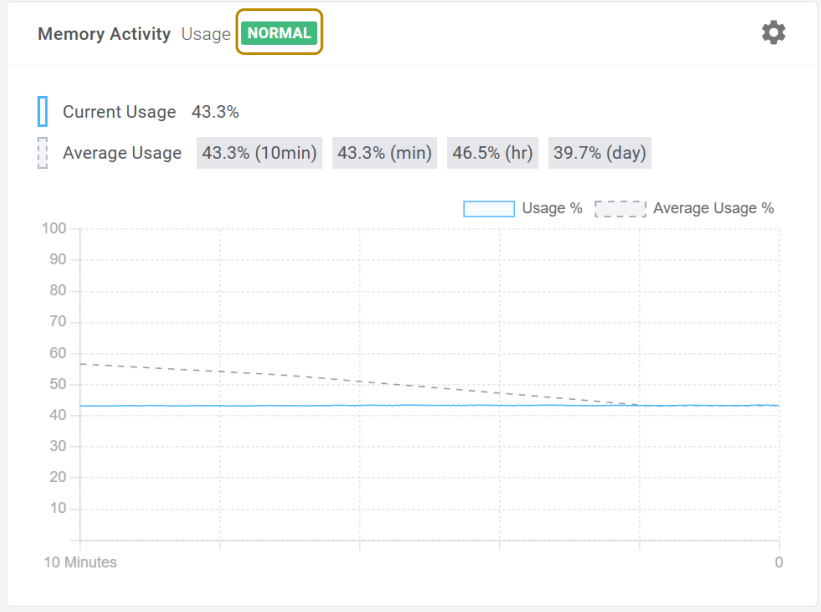
Time	Level	Source	Type	Name	Details
24 June 2025, 16:47:24	Warning	ecaOS	Memory Activity	Memory activity above limit	Average memory activity has been above the set limit of 50% for more than 5 minutes. The current average memory activity is 55.6%

Email

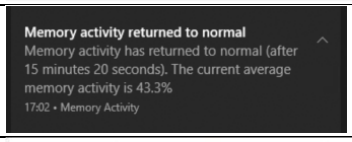


13.2.2 Memory activity back to normal

Dashboard



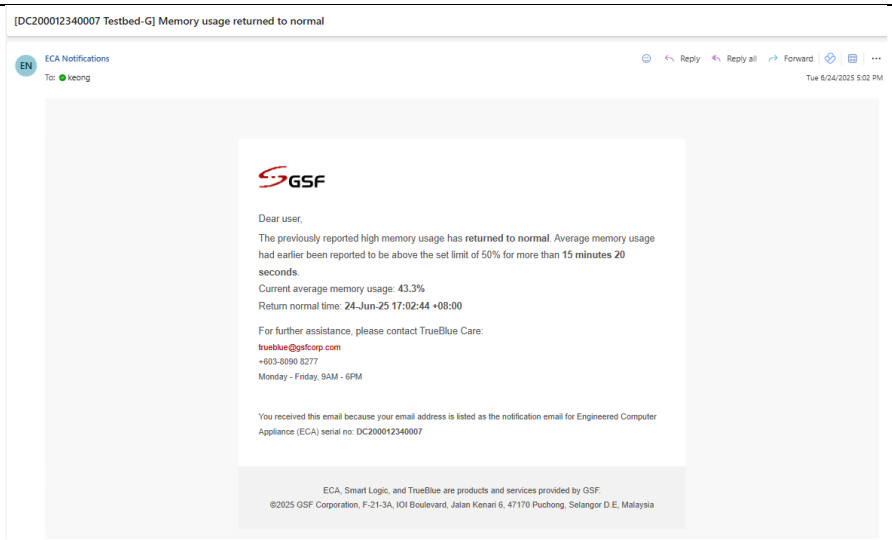
Notification



Log

Time	Level	Source	Type	Name	Details
24 June 2025, 17:02:44	Information	ecaOS	Memory Activity	Memory activity returned to normal	Average memory activity has returned to normal (after 15 minutes 20 seconds). The current average memory activity is 43.3%

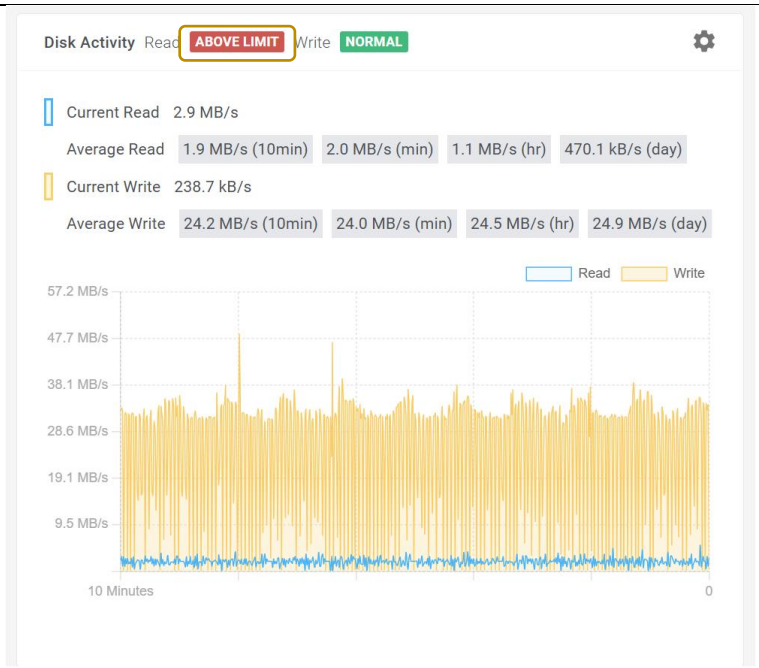
Email



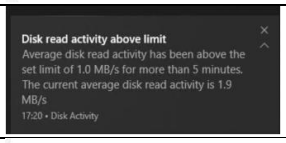
13.3 Disk Activity

13.3.1 Disk read activity above limit

Dashboard



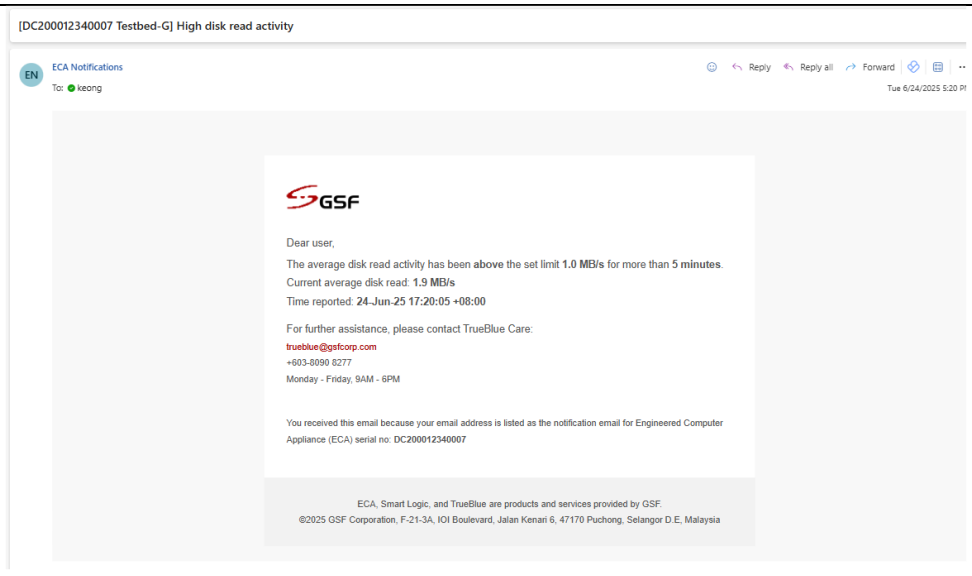
Notification



Log

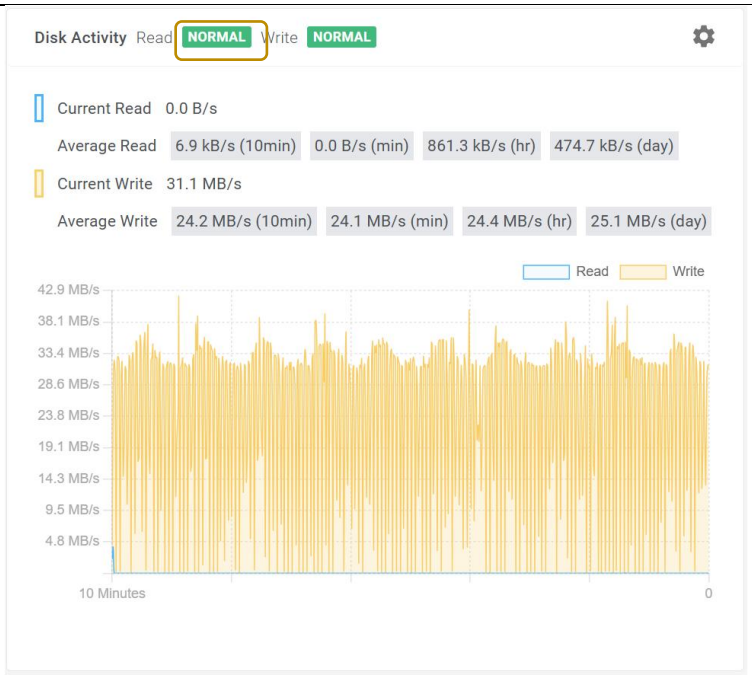
Time	Level	Source	Type	Name	Details
24 June 2025, 17:20:05	Warning	ecaOS	Disk Activity	Disk read activity above limit	Average disk read activity has been above the set limit of 1.0 MB/s for more than 5 minutes. The current average disk read activity is 1.9 MB/s

Email

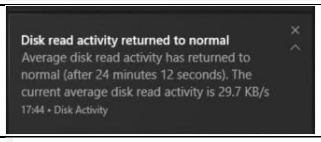


13.3.2 Disk read activity back to normal

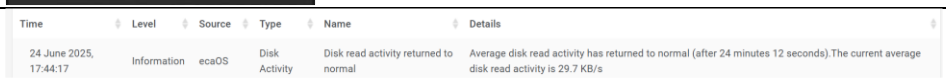
Dashboard



Notification

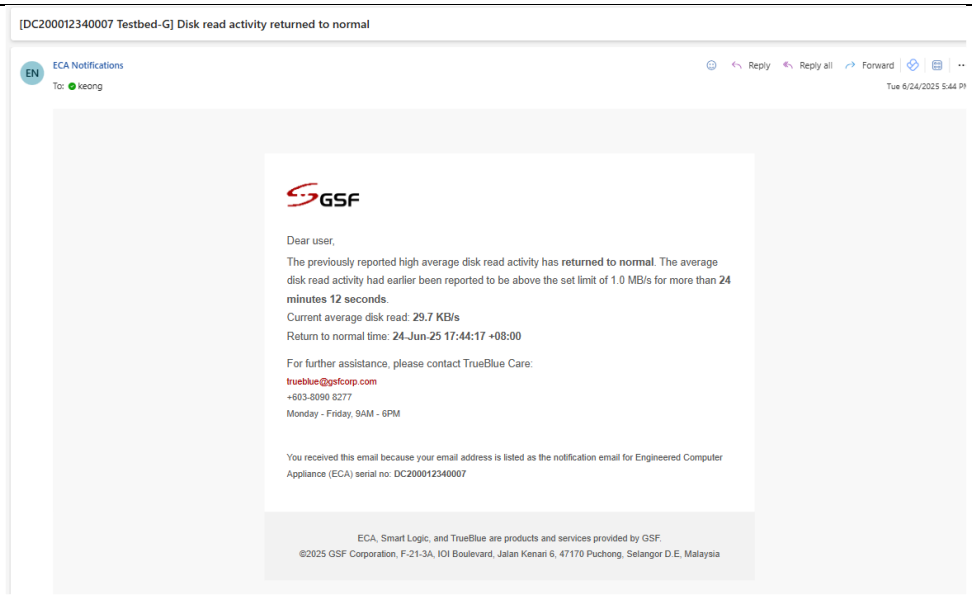


Log



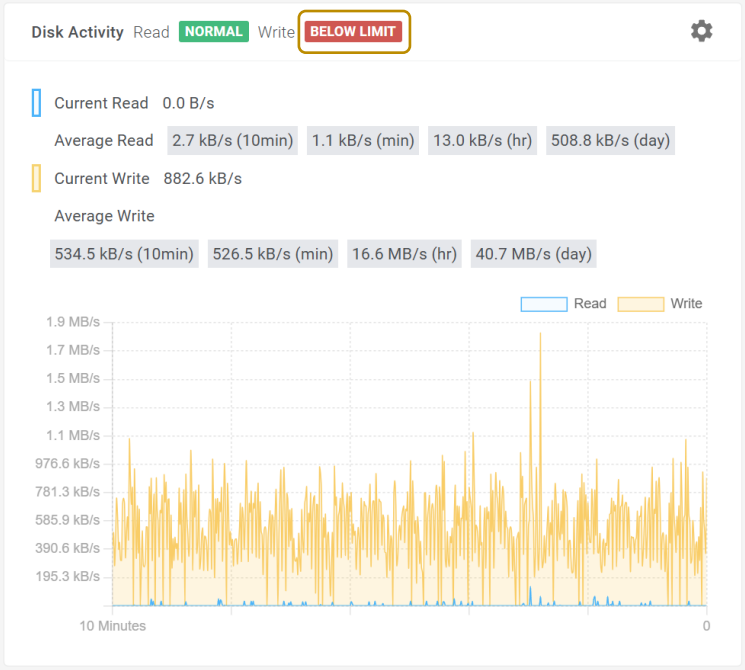
Time	Level	Source	Type	Name	Details
24 June 2025, 17:44:17	Information	ecaOS	Disk Activity	Disk read activity returned to normal	Average disk read activity has returned to normal (after 24 minutes 12 seconds).The current average disk read activity is 29.7 KB/s

Email

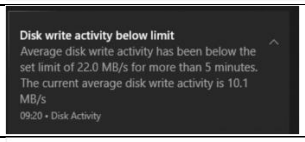


13.3.3 Disk write activity below limit

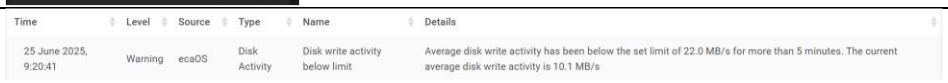
Dashboard



Notification

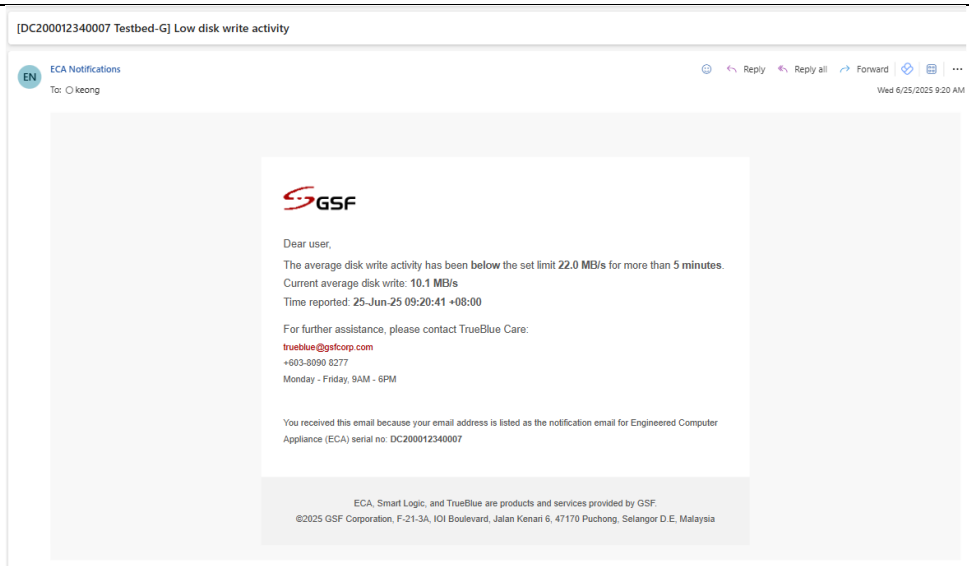


Log



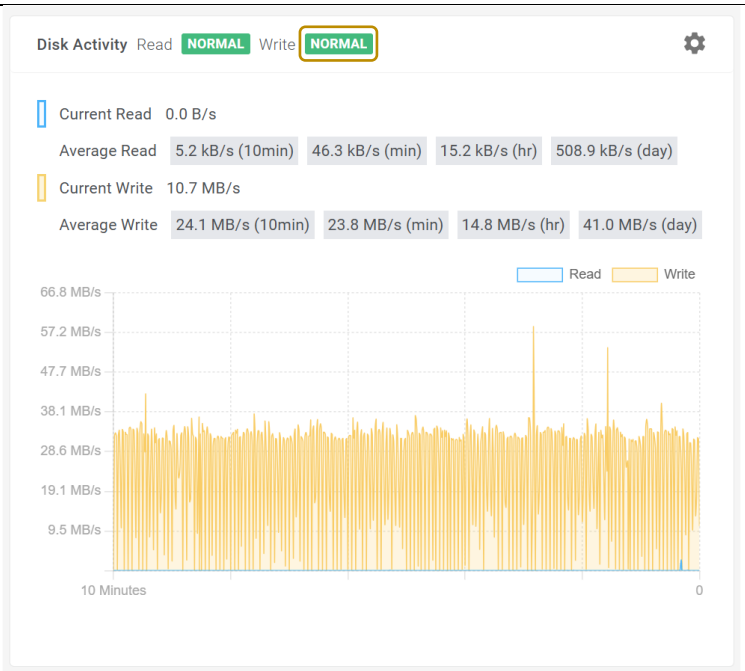
Time	Level	Source	Type	Name	Details
25 June 2025, 9:20:41	Warning	ecaOS	Disk Activity	Disk write activity below limit	Average disk write activity has been below the set limit of 22.0 MB/s for more than 5 minutes. The current average disk write activity is 10.1 MB/s

Email

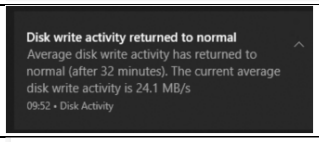


13.3.4 Disk write activity back to normal

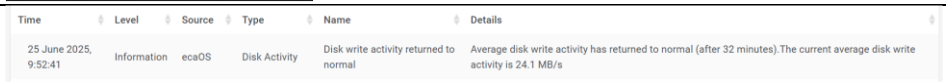
Dashboard



Notification

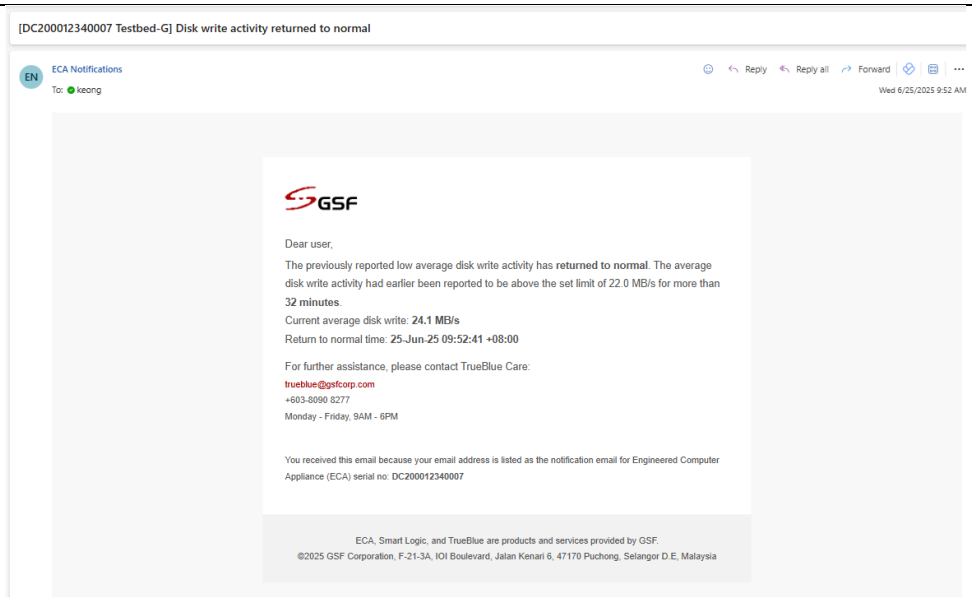


Log



Time	Level	Source	Type	Name	Details
25 June 2025, 9:52:41	Information	ecaOS	Disk Activity	Disk write activity returned to normal	Average disk write activity has returned to normal (after 32 minutes).The current average disk write activity is 24.1 MB/s

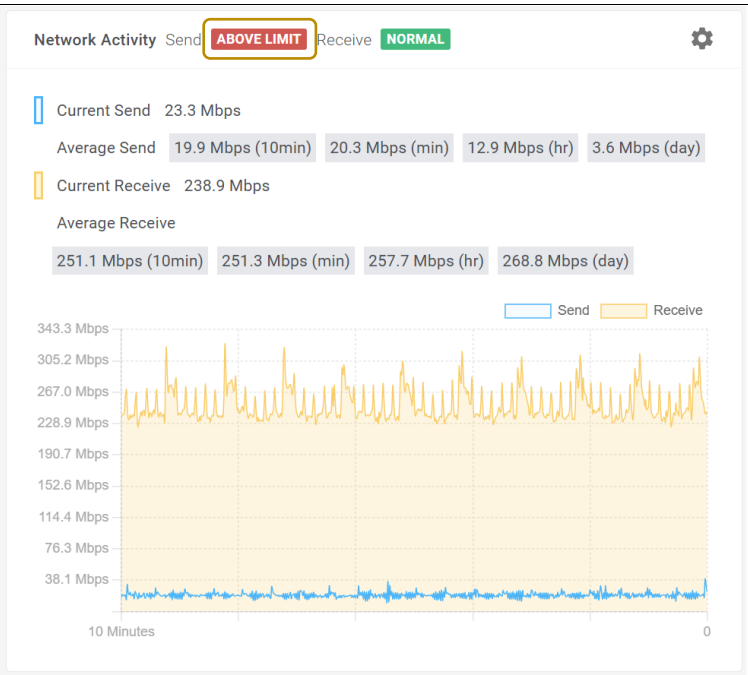
Email



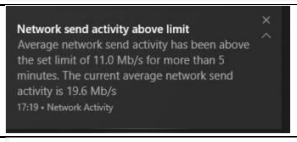
13.4 Network Activity

13.4.1 Network send activity above limit

Dashboard



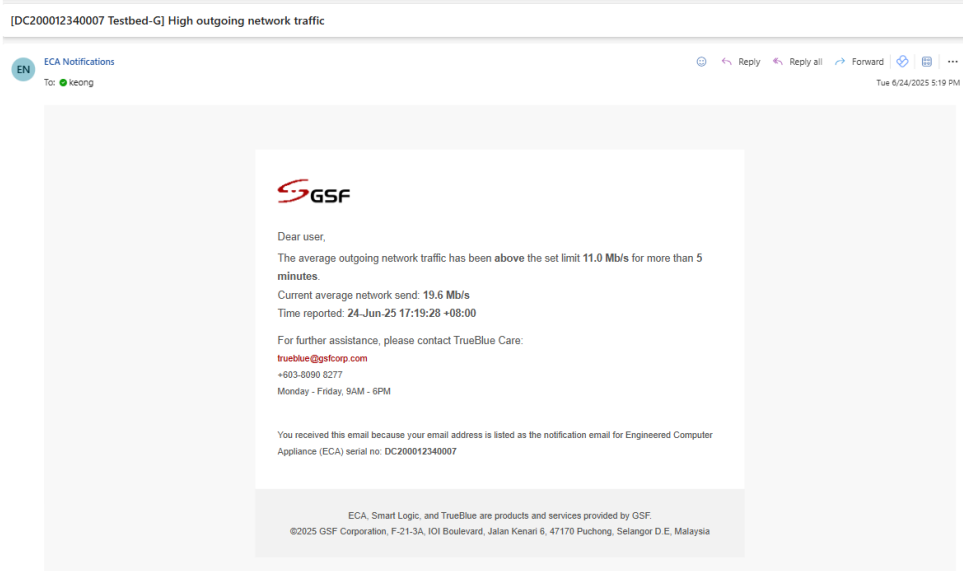
Notification



Log

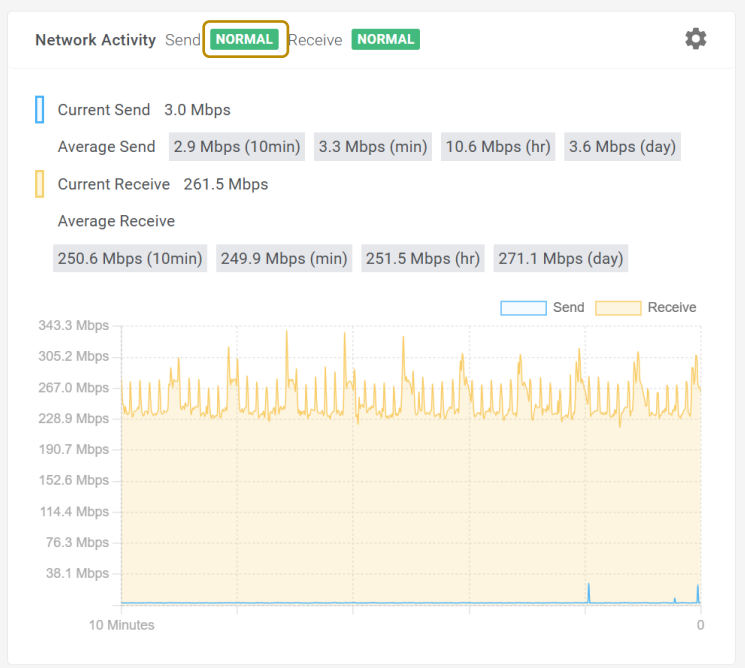
Time	Level	Source	Type	Name	Details
24 June 2025, 17:19:28	Warning	ecaOS	Network Activity	Network send activity above limit	Average network send activity has been above the set limit of 11.0 Mb/s for more than 5 minutes. The current average network send activity is 19.6 Mb/s

Email

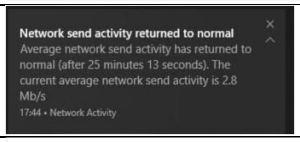


13.4.2 Network send activity back to normal

Dashboard



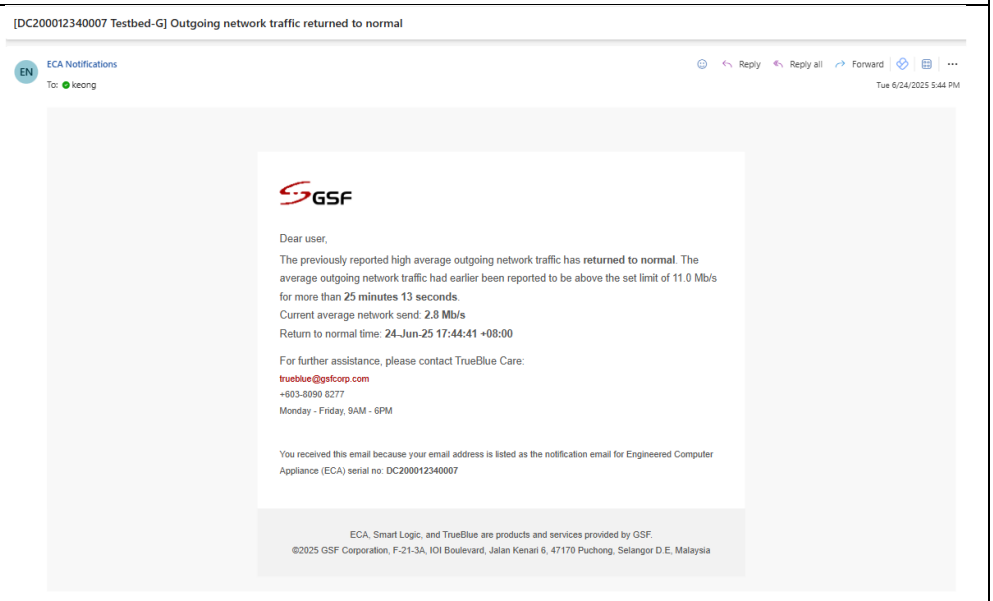
Notification



Log

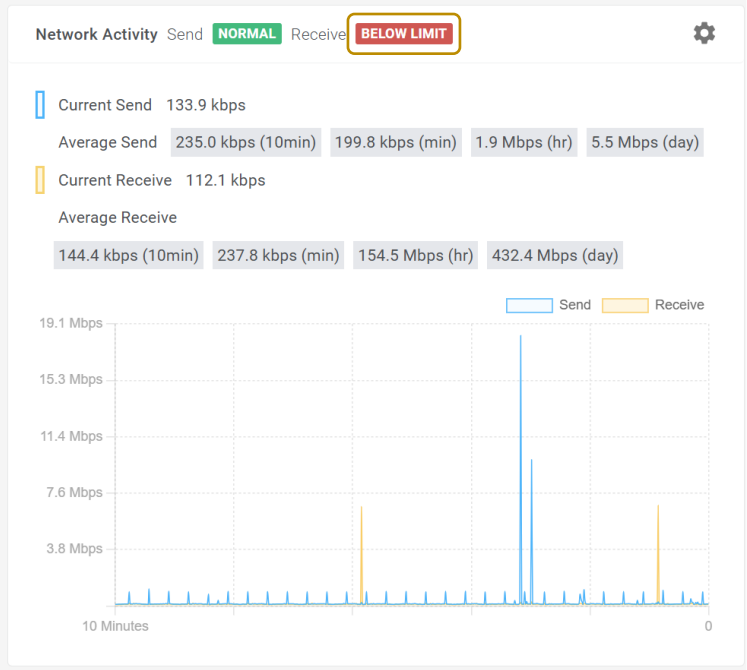
Time	Level	Source	Type	Name	Details
24 June 2025, 17:44:41	Information	ecaOS	Network Activity	Network send activity returned to normal	Average network send activity has returned to normal (after 25 minutes 13 seconds).The current average network send activity is 2.8 Mb/s

Email



13.4.3 Network receive activity below limit

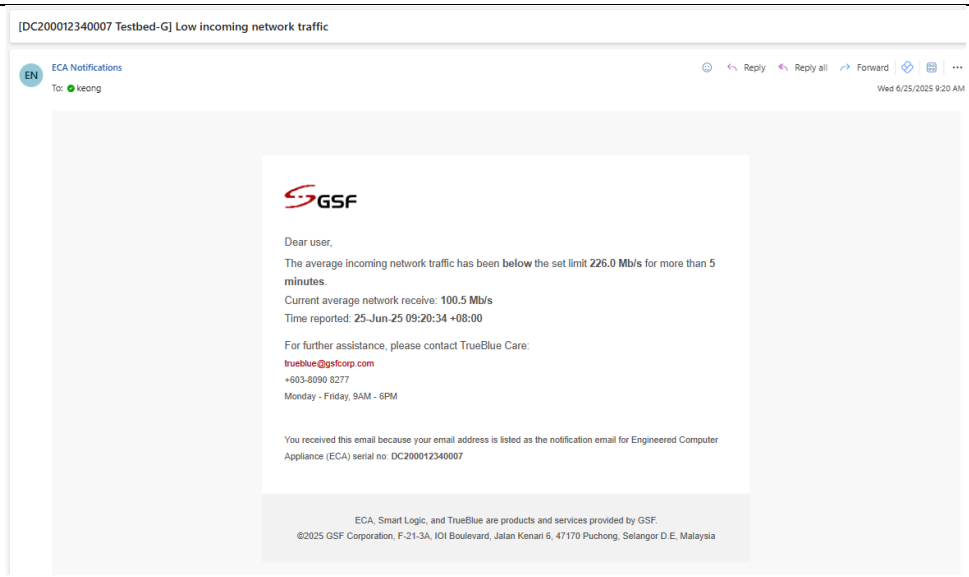
Dashboard



Notification

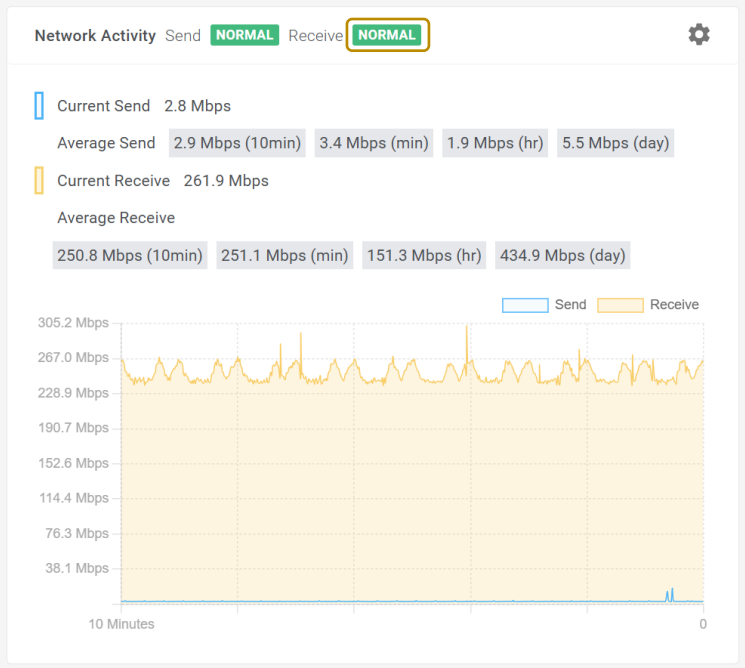
Log

Email



13.4.4 Network receive activity back to normal

Dashboard

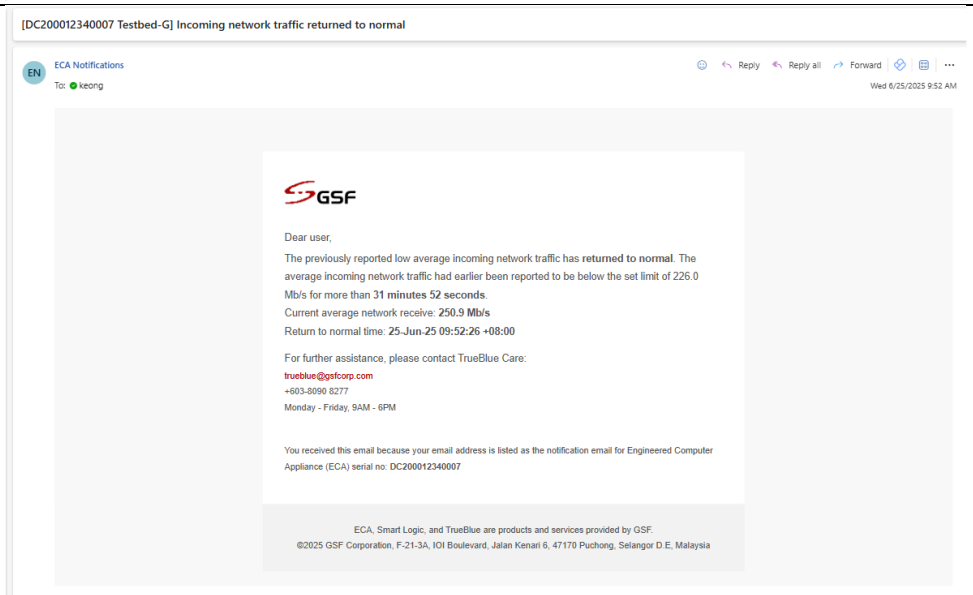


Notification

Log

Time	Level	Source	Type	Name	Details
25 June 2025, 9:52:26	Information	ecaOS	Network Activity	Network receive activity returned to normal	Average network receive activity has returned to normal (after 31 minutes 52 seconds).The current average network receive activity is 250.9 Mb/s

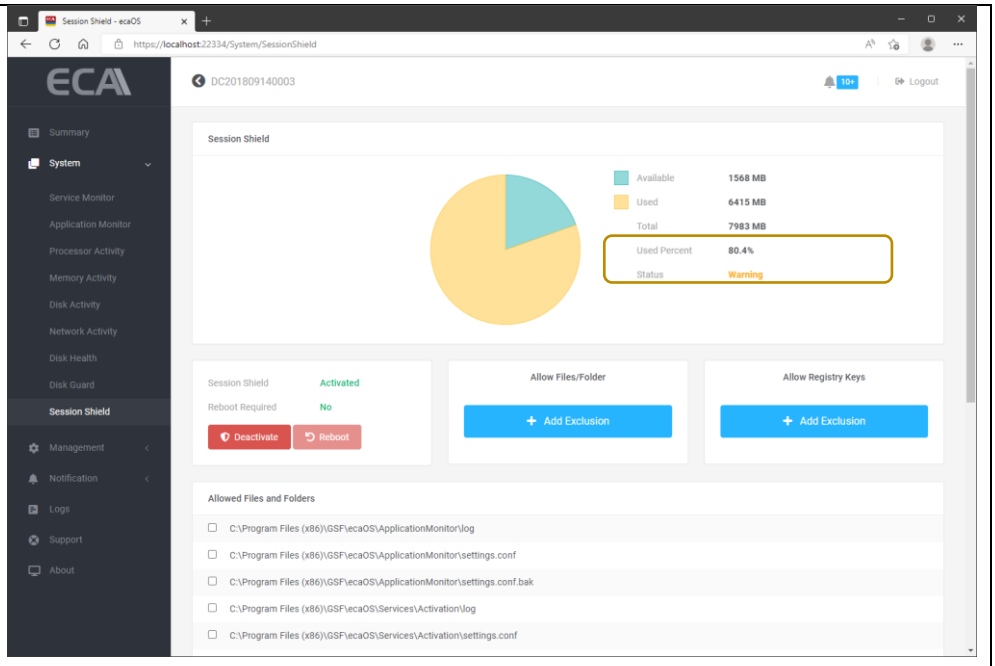
Email



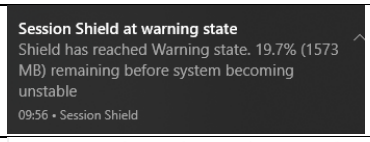
13.5 Session Shield

13.5.1 Warning Status

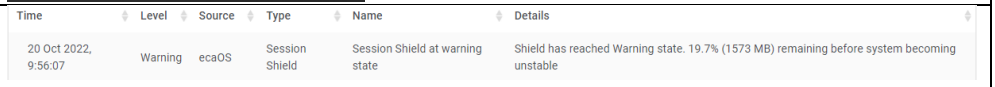
Dashboard



Notification

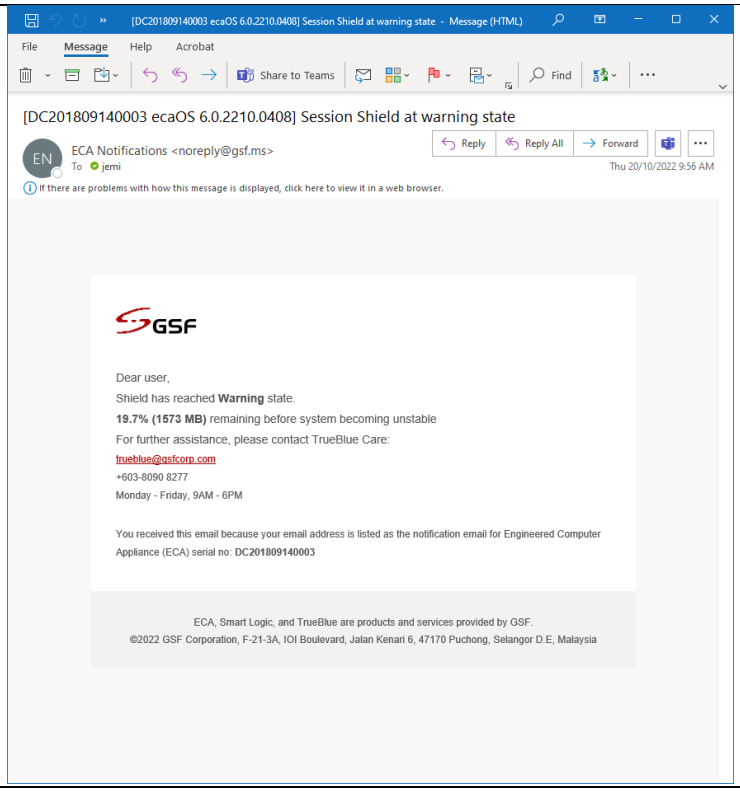


Log



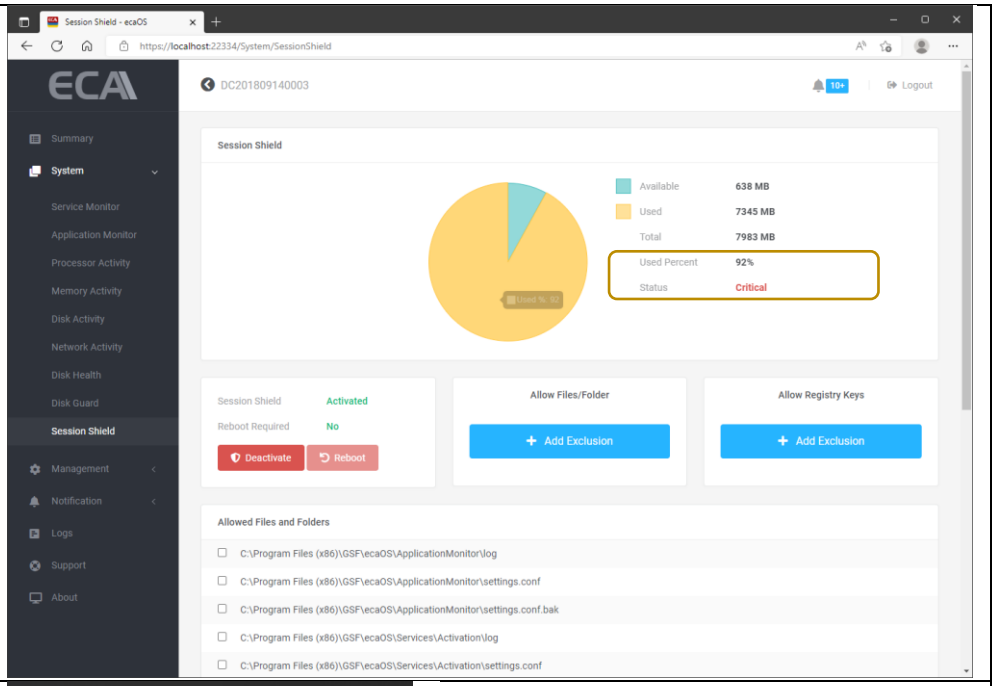
Time	Level	Source	Type	Name	Details
20 Oct 2022, 9:56:07	Warning	ecaOS	Session Shield	Session Shield at warning state	Shield has reached Warning state. 19.7% (1573 MB) remaining before system becoming unstable

Email

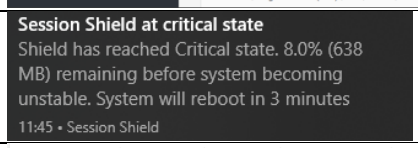


13.5.2 Critical Status

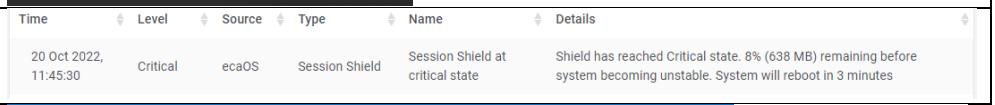
Dashboard



Notification

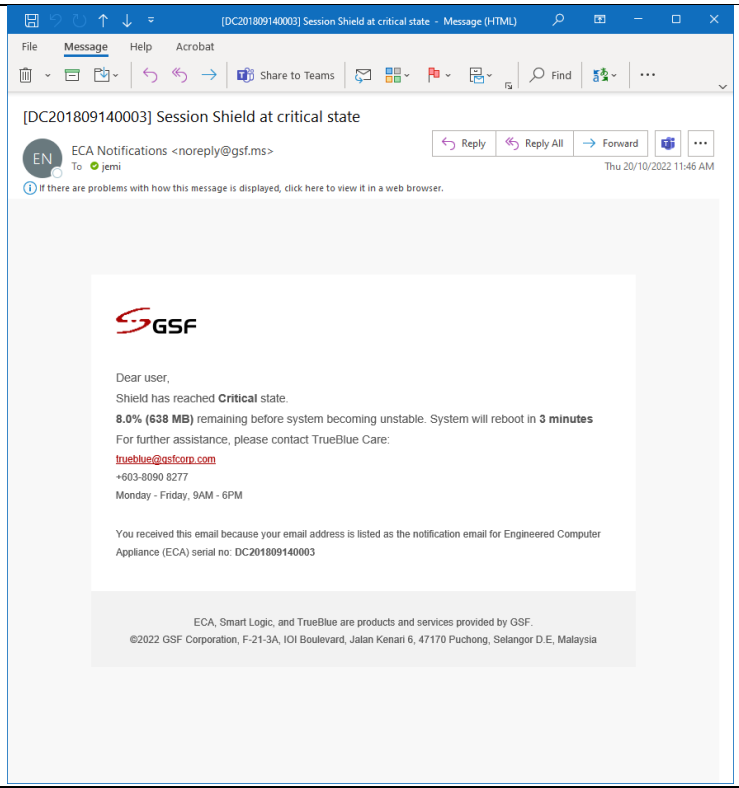


Log



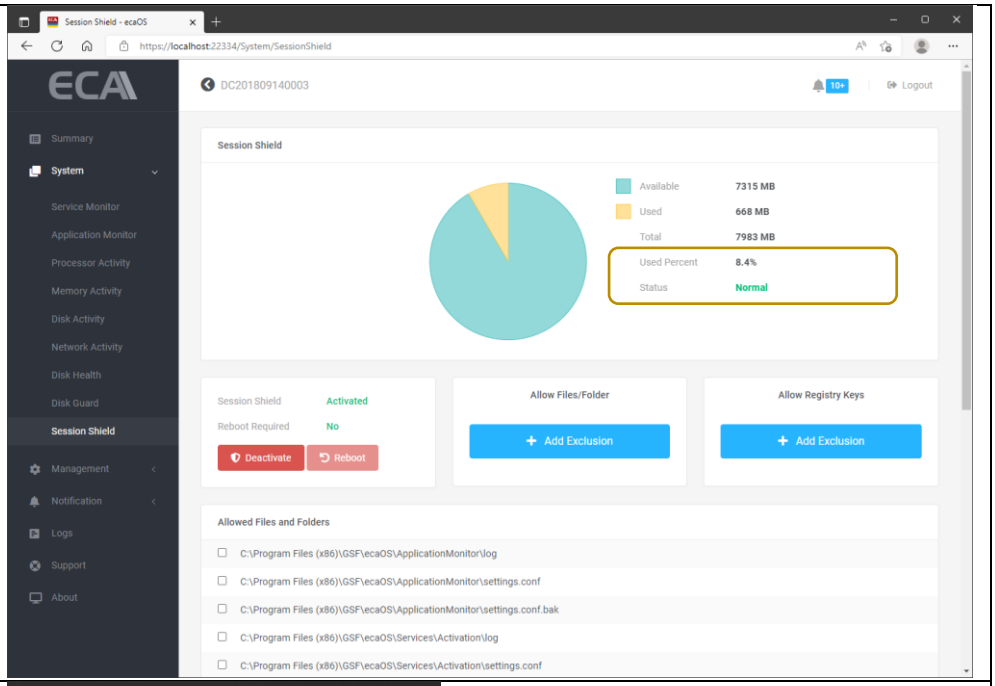
Time	Level	Source	Type	Name	Details
20 Oct 2022, 11:45:30	Critical	ecaOS	Session Shield	Session Shield at critical state	Shield has reached Critical state. 8% (638 MB) remaining before system becoming unstable. System will reboot in 3 minutes

Email

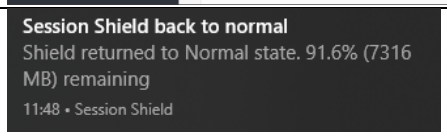


13.5.3 Status back to normal

Dashboard



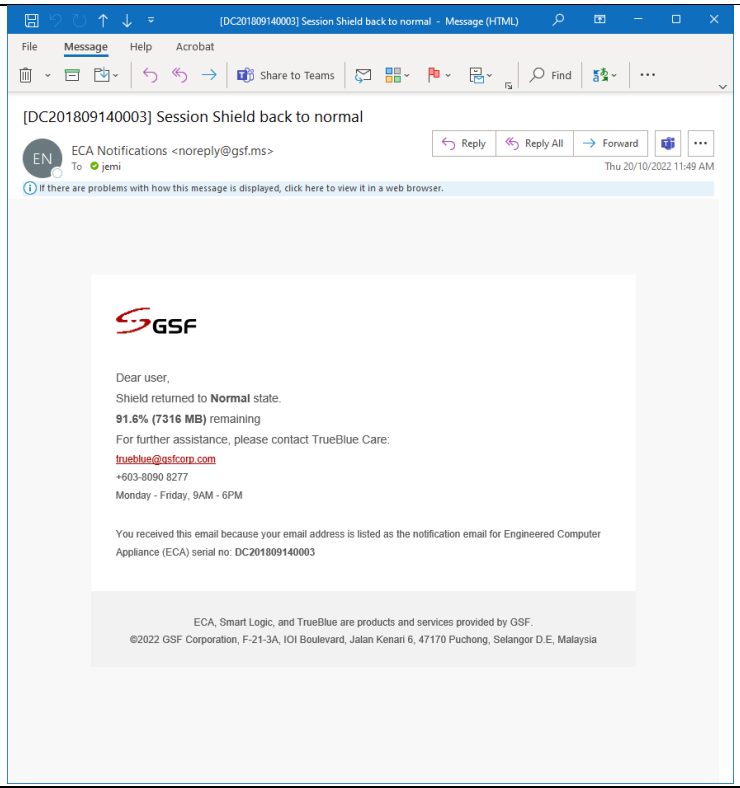
Notification



Log

Time	Level	Source	Type	Name	Details
20 Oct 2022, 11:48:52	Information	ecaOS	Session Shield	Session Shield back to normal	Shield returned to Normal state. 91.6% (7316 MB) remaining

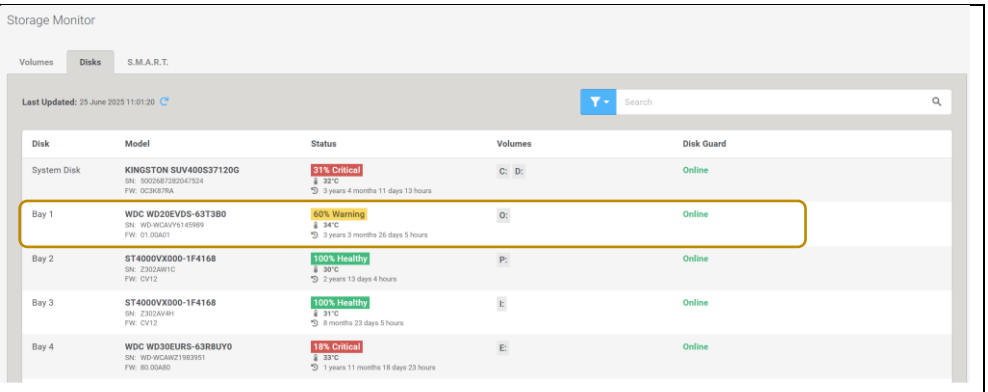
Email



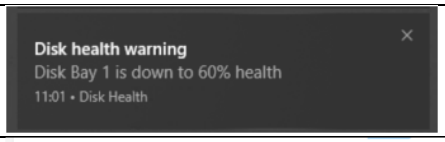
13.6 Disk Health

13.6.1 Warning Status Disk

Dashboard



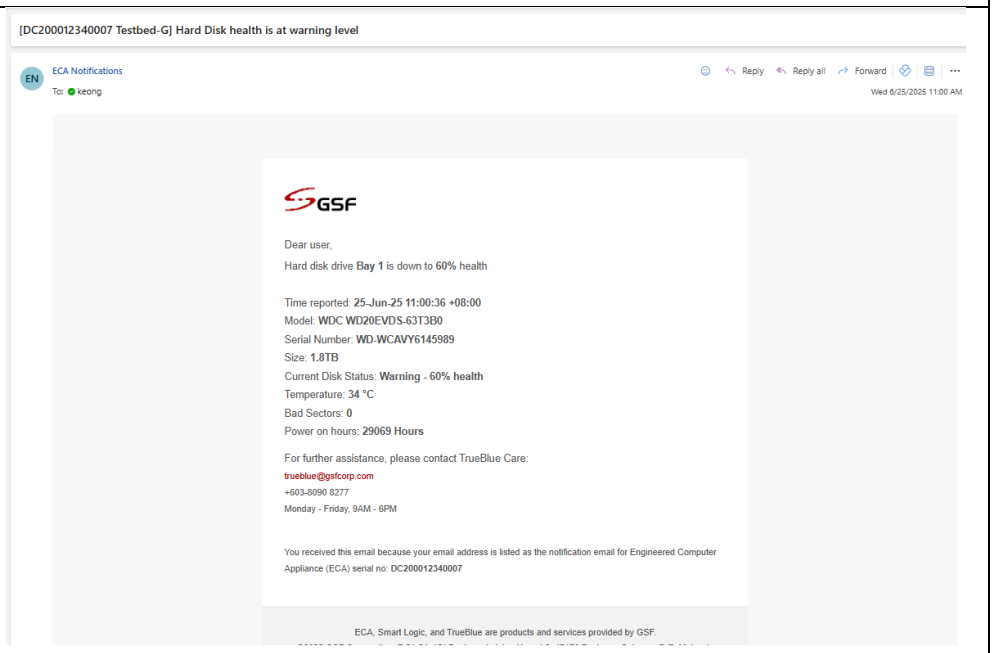
Notification



Log

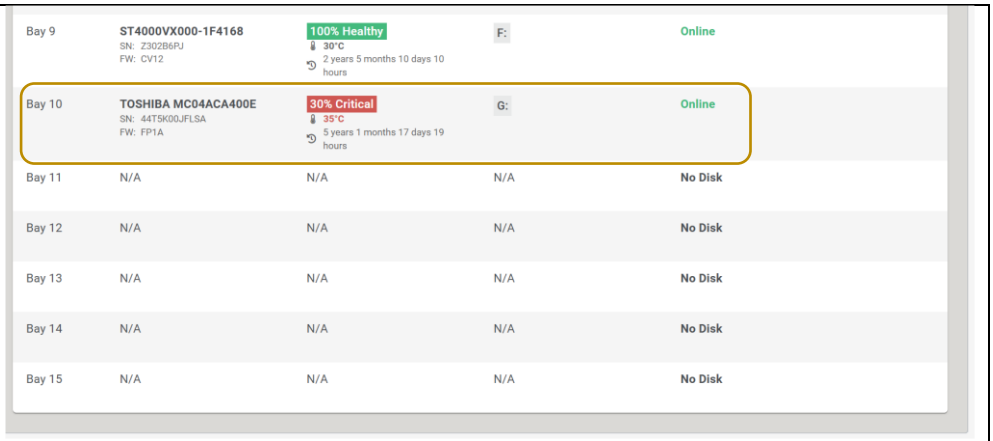
Time	Level	Source	Type	Name	Details
25 June 2025, 11:01:06	Warning	ecaOS	Disk Health	Disk health warning	Disk Bay 1 is down to 60% health

Email

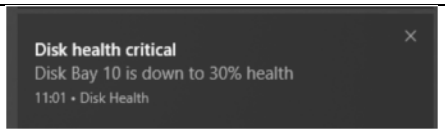


13.6.2 Critical Status Disk

Dashboard



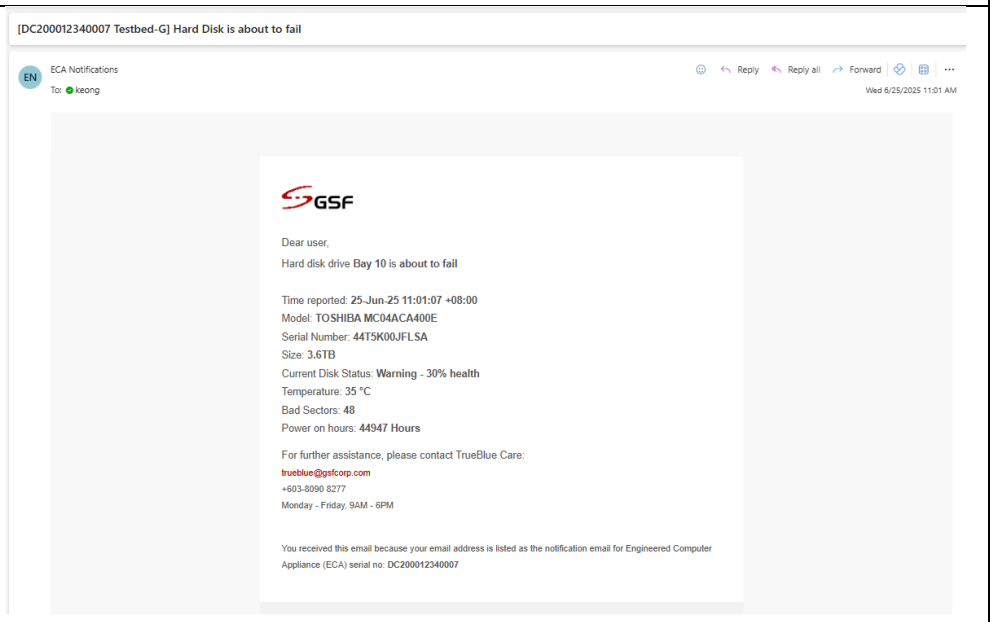
Notification



Log

Time	Level	Source	Type	Name	Details
25 June 2025, 11:01:07	Warning	ecaOS	Disk Health	Disk health critical	Disk Bay 10 is down to 30% health

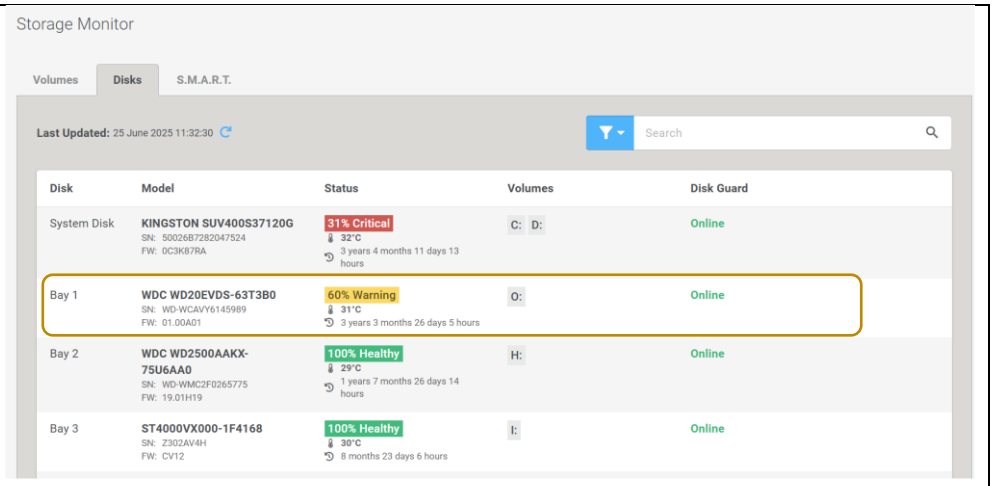
Email



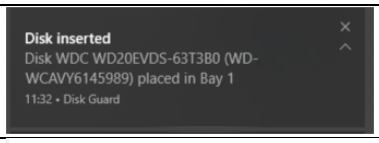
13.7 Disk Guard

13.7.1 New disk / Disk Inserted

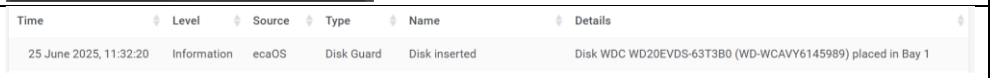
Dashboard



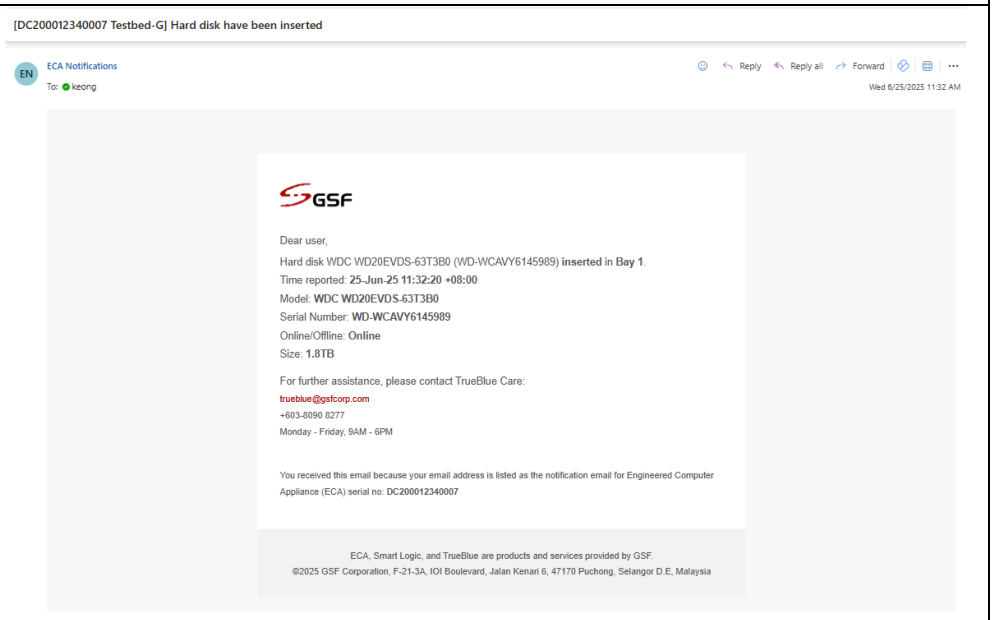
Notification



Log

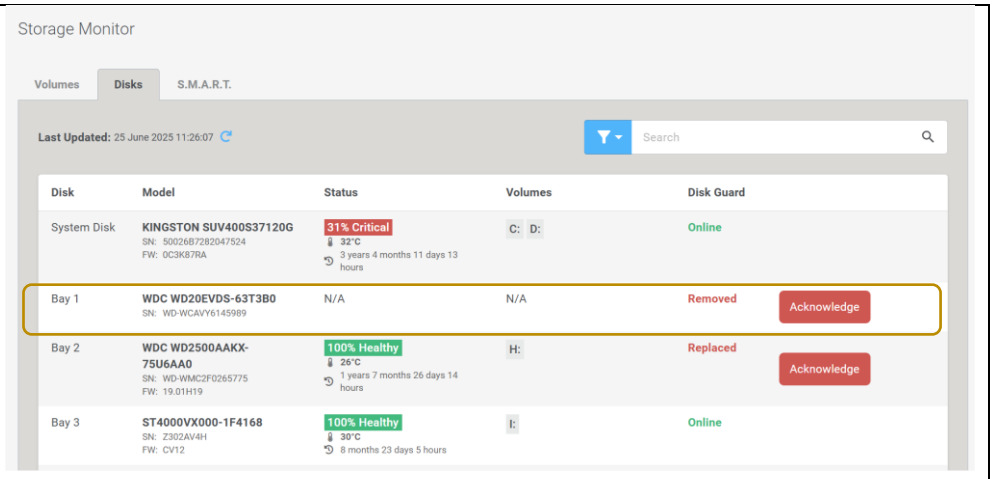


Email

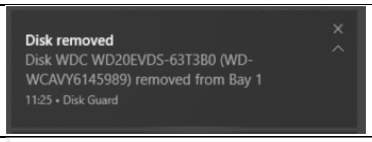


13.7.2 Disk Removed

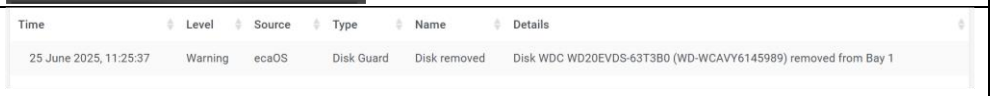
Dashboard



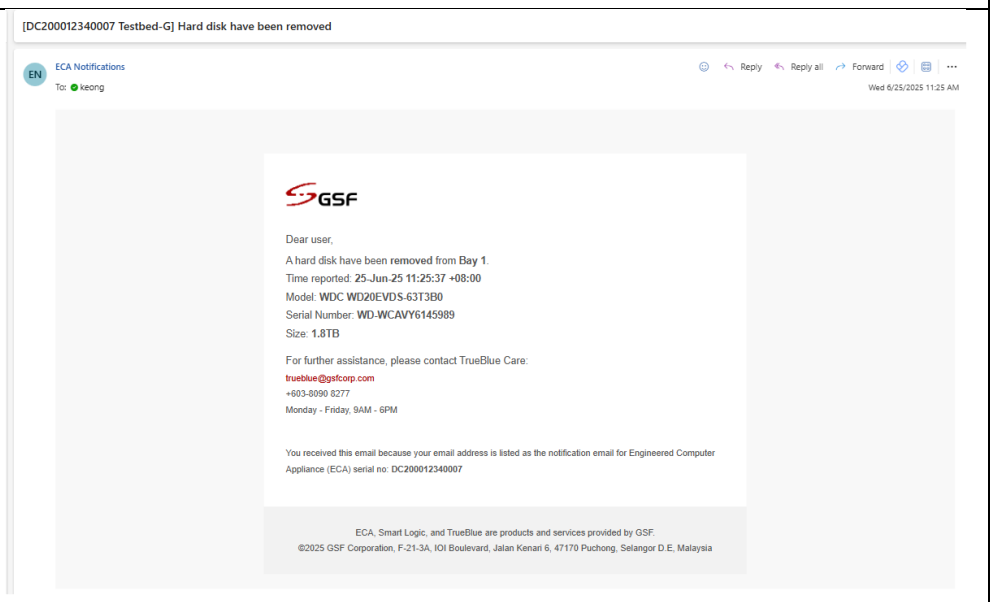
Notification



Log

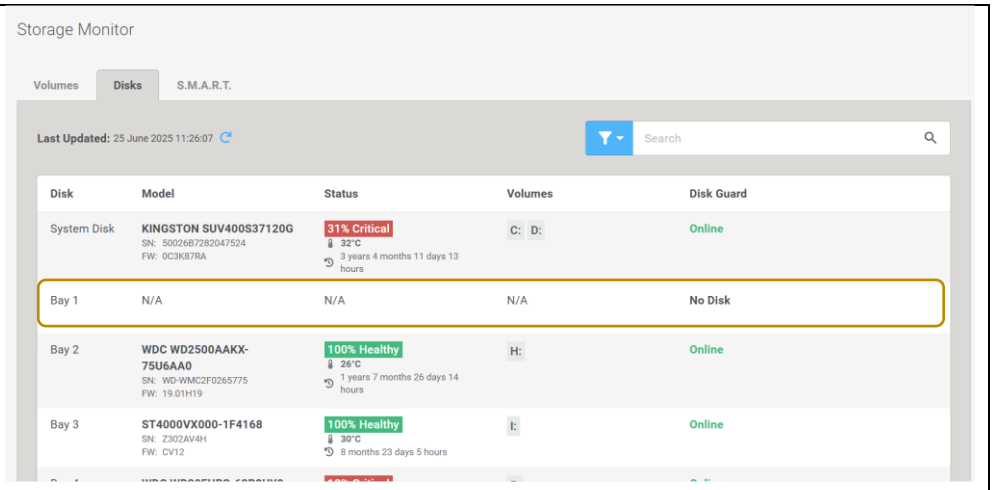


Email

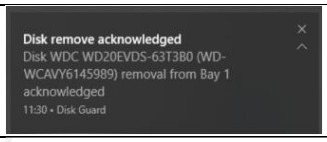


13.7.3 Disk Removed Acknowledge

Dashboard

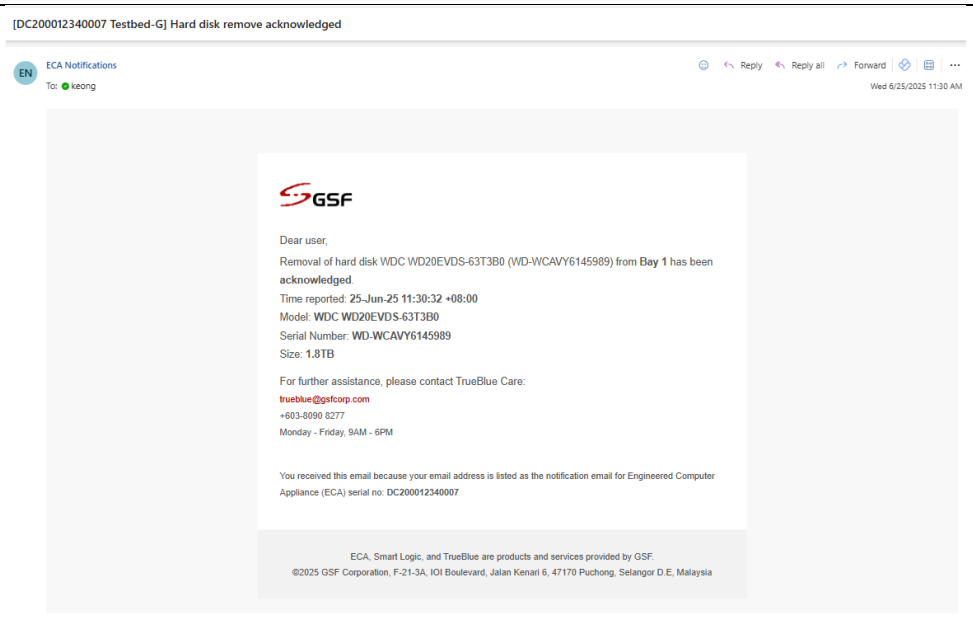


Notification



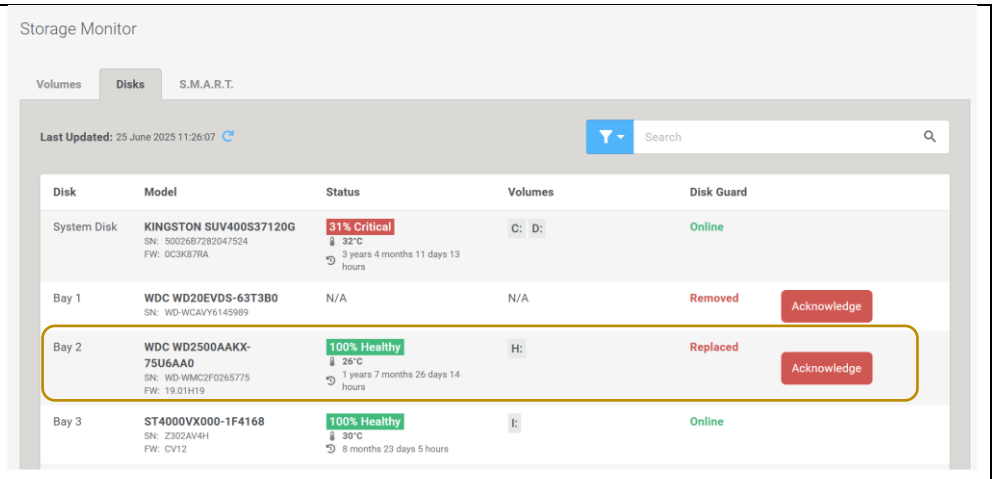
Log

Email

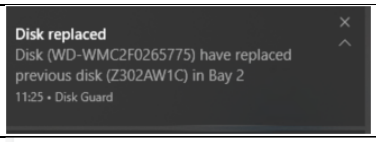


13.7.4 Disk Replaced

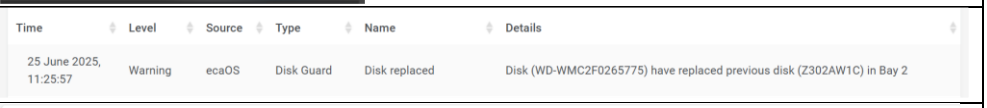
Dashboard



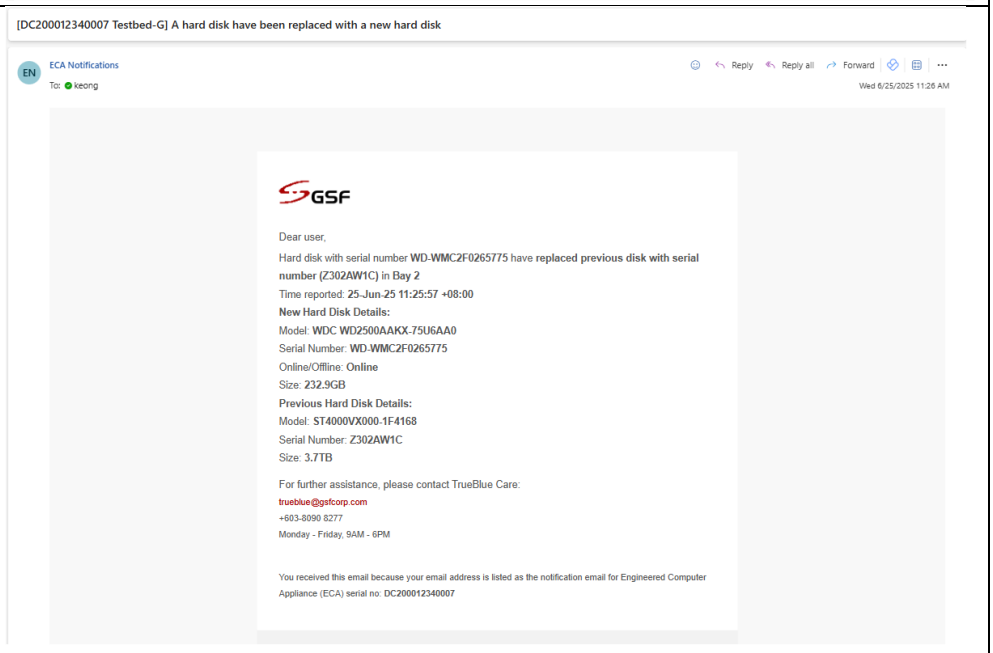
Notification



Log

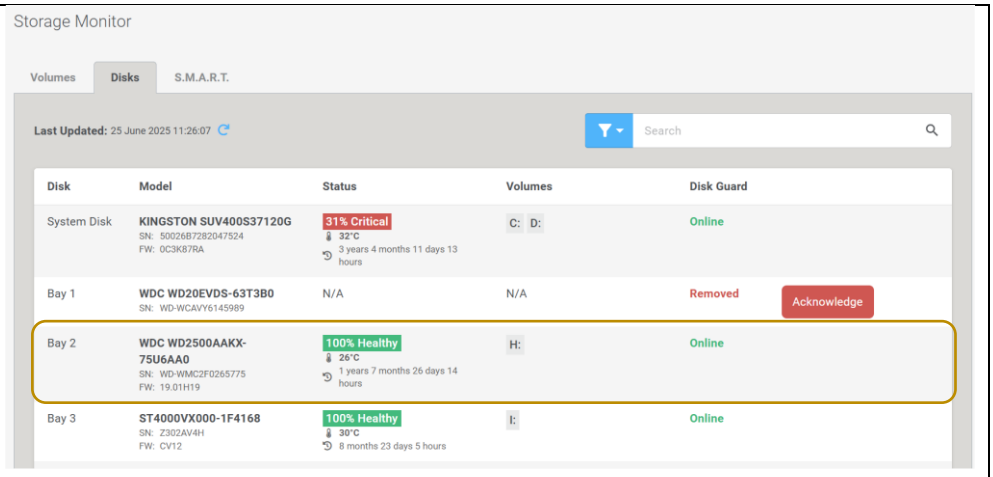


Email

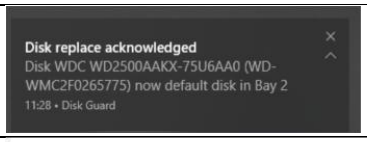


13.7.5 Disk Replaced Acknowledge

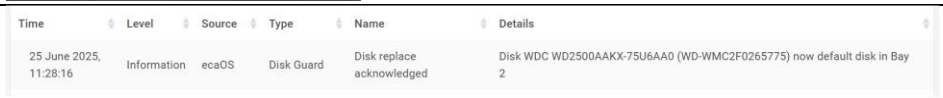
Dashboard



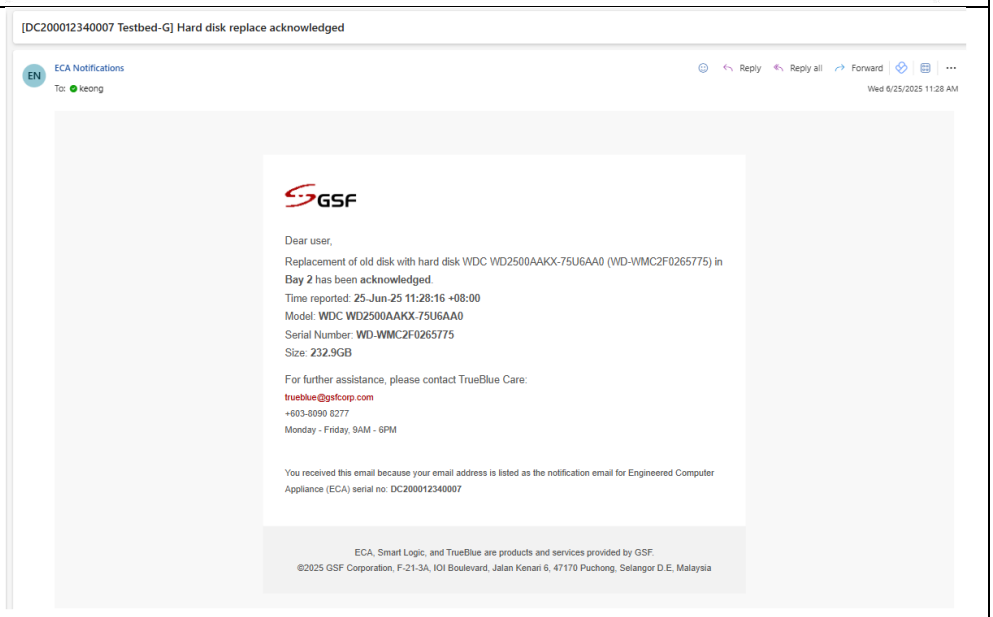
Notification



Log



Email



13.8 Log

13.8.1 ECA reboot more than 3 times

Figure 209 Show chronological events in log when ECA reboot more than 3 times within 1 hour

Time	Level	Source	Type	Name	Details
21 Oct 2022, 17:15:16	Information	Heartbeat	I/O	DO0 output set to high	
21 Oct 2022, 17:15:15	Warning	Heartbeat	ECA Controller	Unauthorized system reboot	
21 Oct 2022, 17:15:14	Warning	Heartbeat	ECA Controller	Alert on: System repetitive reboot	

Figure 209

13.8.2 AC Power loss

Figure 210 Show chronological events in log when AC power loss.

Time	Level	Source	Type	Name	Details
21 Oct 2022, 17:10:44	Information	Heartbeat	ECA Motherboard	System in ecaOS	
21 Oct 2022, 17:10:43	Information	Heartbeat	ECA Gateway	Gateway connected	
21 Oct 2022, 17:10:24	Information	Heartbeat	I/O	DO0 output set to low	
21 Oct 2022, 17:10:23	Information	Heartbeat	ECA Controller	Alert off: Unexpected system power loss	
21 Oct 2022, 17:10:23	Information	Heartbeat	ECA Motherboard	System powered up	
21 Oct 2022, 17:10:21	Information	Heartbeat	Battery	Battery charging	
21 Oct 2022, 17:10:18	Information	Heartbeat	Battery	Charger power resumed	
21 Oct 2022, 17:10:18	Information	Heartbeat	ECA Motherboard	AC power resumed	
21 Oct 2022, 17:10:17	Warning	Heartbeat	ECA Gateway	Gateway disconnected	
21 Oct 2022, 17:10:16	Warning	Heartbeat	Battery	Charger power loss	
21 Oct 2022, 17:10:15	Information	Heartbeat	Battery	Battery discharging	
21 Oct 2022, 17:10:10	Information	Heartbeat	I/O	DO0 output set to high	
21 Oct 2022, 17:10:09	Warning	Heartbeat	ECA Controller	Alert on: Unexpected system power loss	
21 Oct 2022, 17:10:09	Warning	Heartbeat	ECA Motherboard	AC power loss	
21 Oct 2022, 17:05:32	Warning	Heartbeat	ECA Controller	Unauthorized system reboot	

Figure 210

13.8.3 Unauthorize ECA Reboot

Figure 211 Show chronological events in log when ECA reboot does not through Dashboard.

Time	Level	Source	Type	Name	Details
21 Oct 2022, 17:05:32	Warning	Heartbeat	ECA Controller	Unauthorized system reboot	
21 Oct 2022, 17:05:27	Information	Heartbeat	ECA Motherboard	System in ecaOS	
21 Oct 2022, 17:05:25	Information	Heartbeat	ECA Gateway	Gateway connected	
21 Oct 2022, 17:05:11	Warning	Heartbeat	ECA Gateway	Gateway disconnected	
21 Oct 2022, 17:04:59	Information	Heartbeat	ECA Motherboard	System leaving ecaOS	

Figure 211

13.8.4 Unauthorize ECA Shutdown

Figure 212 Show chronological events in log when ECA shutdown does not through Dashboard.

Time	Level	Source	Type	Name	Details
21 Oct 2022, 17:00:06	Information	Heartbeat	ECA Motherboard	System in ecaOS	
21 Oct 2022, 17:00:03	Information	Heartbeat	ECA Gateway	Gateway connected	
21 Oct 2022, 16:59:49	Information	Heartbeat	ECA Motherboard	System powered up by Heartbeat	
21 Oct 2022, 16:59:43	Warning	Heartbeat	ECA Controller	Unauthorized system shutdown	
21 Oct 2022, 16:59:43	Information	Heartbeat	ECA Motherboard	System shutdown	
21 Oct 2022, 16:59:42	Warning	Heartbeat	ECA Gateway	Gateway disconnected	
21 Oct 2022, 16:59:32	Information	Heartbeat	ECA Motherboard	System leaving ecaOS	

Figure 212

13.8.5 Authorize ECA Shutdown

Figure 213 Show chronological events in log when ECA shutdown through Dashboard.

Time	Level	Source	Type	Name	Details
21 Oct 2022, 16:53:08	Information	Heartbeat	ECA Motherboard	System shutdown	
21 Oct 2022, 16:53:07	Warning	Heartbeat	ECA Gateway	Gateway disconnected	
21 Oct 2022, 16:52:56	Information	Heartbeat	ECA Motherboard	System leaving ecaOS	
21 Oct 2022, 16:52:50	Information	ecaOS	System	Shutdown system	

Figure 213

13.8.6 Authorize ECA Reboot

Figure 214 Show chronological events in log when ECA reboot through Dashboard.

Time	Level	Source	Type	Name	Details
21 Oct 2022, 16:58:11	Information	Heartbeat	ECA Motherboard	System in ecaOS	
21 Oct 2022, 16:58:09	Information	Heartbeat	ECA Gateway	Gateway connected	
21 Oct 2022, 16:57:54	Warning	Heartbeat	ECA Gateway	Gateway disconnected	
21 Oct 2022, 16:57:42	Information	Heartbeat	ECA Motherboard	System leaving ecaOS	
21 Oct 2022, 16:57:39	Information	ecaOS	System	Reboot system	

Figure 214

13.8.7 Power up ECA by pressing power button

Figure 215 Show chronological events in log when ECA power up by pressing power button

Time	Level	Source	Type	Name	Details
21 Oct 2022, 16:53:41	Information	Heartbeat	ECA Motherboard	System in ecaOS	
21 Oct 2022, 16:53:39	Information	Heartbeat	ECA Gateway	Gateway connected	
21 Oct 2022, 16:53:25	Information	Heartbeat	ECA Motherboard	System power button released	
21 Oct 2022, 16:53:24	Information	Heartbeat	ECA Motherboard	System powered up	
21 Oct 2022, 16:53:19	Information	Heartbeat	ECA Motherboard	System power button pressed	

Figure 215

13.8.8 Force shutdown by pressing power (heartbeat) button

Figure 216 Show chronological events in log when force shutdown by long pressed power button

Time	Level	Source	Type	Name	Details
21 Oct 2022, 16:51:40	Information	Heartbeat	ECA Motherboard	System in ecaOS	
21 Oct 2022, 16:51:37	Information	Heartbeat	ECA Gateway	Gateway connected	
21 Oct 2022, 16:51:22	Information	Heartbeat	ECA Motherboard	System powered up by Heartbeat	
21 Oct 2022, 16:51:19	Warning	Heartbeat	ECA Gateway	Gateway disconnected	
21 Oct 2022, 16:51:12	Warning	Heartbeat	ECA Controller	Unauthorized system shutdown	
21 Oct 2022, 16:51:12	Information	Heartbeat	ECA Motherboard	System power button released	
21 Oct 2022, 16:51:12	Information	Heartbeat	ECA Motherboard	System forced shutdown	

Figure 216

13.8.9 Accessing Dashboard using Security Key

Figure 217 Show chronological events in log when accessing dashboard using security key

Time	Level	Source	Type	Name	Details
21 Oct 2022, 16:46:02	Information	ecaOS	Security Key	Paired security key inserted	Paired security key 'Security Key' (56a30456) was inserted
21 Oct 2022, 16:46:02	Information	ecaOS	Security Key	Security key inserted	Security key 'Security Key' (56a30456) was inserted

Figure 217

13.8.10 Accessing Dashboard using Virtual Security Key

Figure 218 Show chronological events in log when accessing dashboard using Virtual security key

Time	Level	Source	Type	Name	Details
21 Oct 2022, 16:29:32	Information	ecaOS	Virtual Security Key	Valid passcode entered	Login using virtual security key 'admin'

Figure 218

13.8.11 Add new Security Key

Figure 219 Show chronological events in log when add new security key.

Time	Level	Source	Type	Name	Details
21 Oct 2022, 15:47:38	Information	ecaOS	Security Key	Security key added	New security key 'Security Key' (56a30456) was added

Figure 219

13.8.12 Delete paired Security Key

Figure 220 Show chronological events in log when paired Security Key deleted.

Time	Level	Source	Type	Name	Details
21 Oct 2022, 15:47:29	Information	ecaOS	Security Key	Security key deleted	Security key 'Security Key' (56a30456) was deleted

Figure 220

13.8.13 Delete Virtual Security Key

Figure 220 Show chronological events in log when existing Virtual Security Key deleted.

Time	Level	Source	Type	Name	Details
21 Oct 2022, 15:53:02	Information	ecaOS	Virtual Security Key	Virtual security key deleted	Virtual security key 'admin' was deleted

Figure 221

13.8.14 Add Virtual Security Key

Figure 220 Show chronological events in log when new Virtual Security Key added.

Time	Level	Source	Type	Name	Details
25 Aug 2022, 12:56:45	Information	ecaOS	Virtual Security Key	Virtual security key added	New virtual security key 'adminv2' was added

Figure 222

13.8.15 Open ECA cover chassis

Figure 219 Show chronological events in log when ECA top cover open.

Time	Level	Source	Type	Name	Details
21 Oct 2022, 15:57:58	Information	Heartbeat	I/O	DO0 output set to high	
21 Oct 2022, 15:57:58	Warning	Heartbeat	ECA Controller	Alert on: Unauthorized chassis opened	
21 Oct 2022, 15:57:58	Warning	Heartbeat	ECA Motherboard	System chassis opened	

Figure 223

13.8.16 Close ECA cover chassis

Figure 219 Show chronological events in log when ECA top cover close.

Time	Level	Source	Type	Name	Details
21 Oct 2022, 16:38:20	Information	Heartbeat	I/O	DO0 output set to low	
21 Oct 2022, 16:38:15	Information	Heartbeat	ECA Controller	Alert off: Unauthorized chassis opened	
21 Oct 2022, 16:38:15	Information	Heartbeat	ECA Motherboard	System chassis closed	

Figure 224

13.8.17 PSU Status

Figure 219 Show chronological events in the log when a power supply fault is detected and the power supply is restored to normal.

Time	Level	Source	Type	Name	Details
22 Jan 2024, 12:11:02	Warning	Heartbeat	ECA Power Supply	Power supply fault	PSU 2 fault detected
22 Jan 2024, 12:10:02	Information	Heartbeat	ECA Power Supply	Power supply back to normal	
22 Jan 2024, 12:09:02	Warning	Heartbeat	ECA Power Supply	Power supply fault	PSU 1 fault detected
22 Jan 2024, 12:08:02	Information	Heartbeat	ECA Power Supply	Power supply back to normal	

Figure 225

13.9 ecaOS SNMP Notification

13.9.1 CPU Activity

- CPU activity above limit

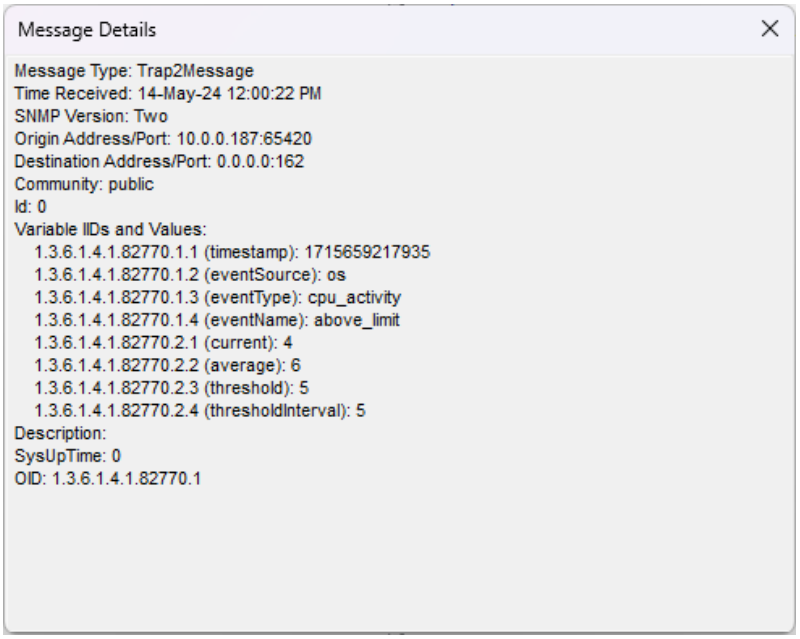


Figure 226

- CPU activity back to normal

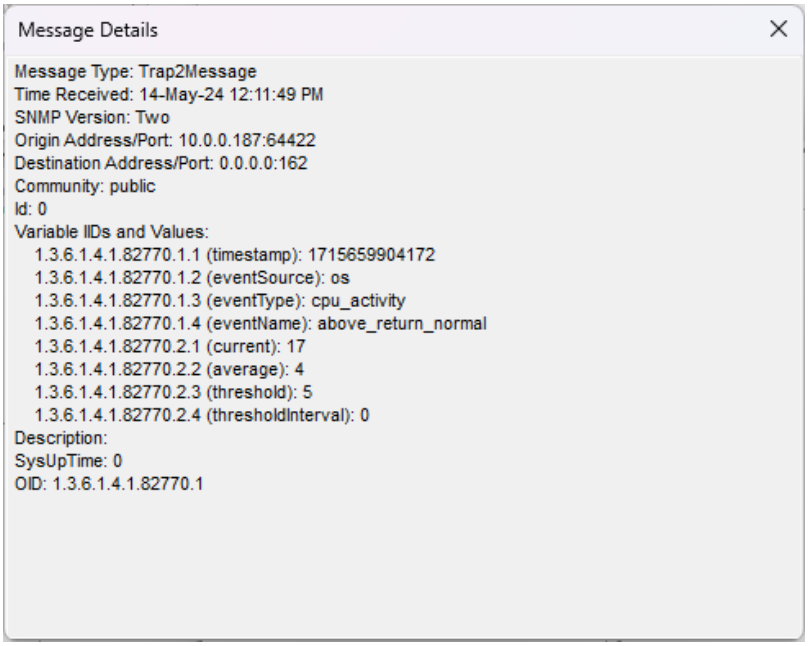


Figure 227

13.9.2 Memory Activity

- Memory activity above limit

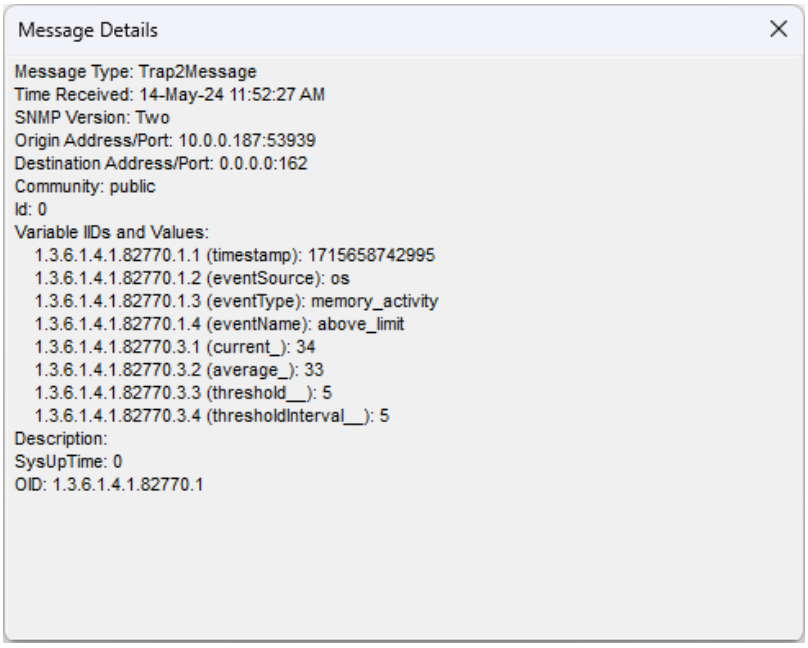


Figure 228

- Memory activity back to normal

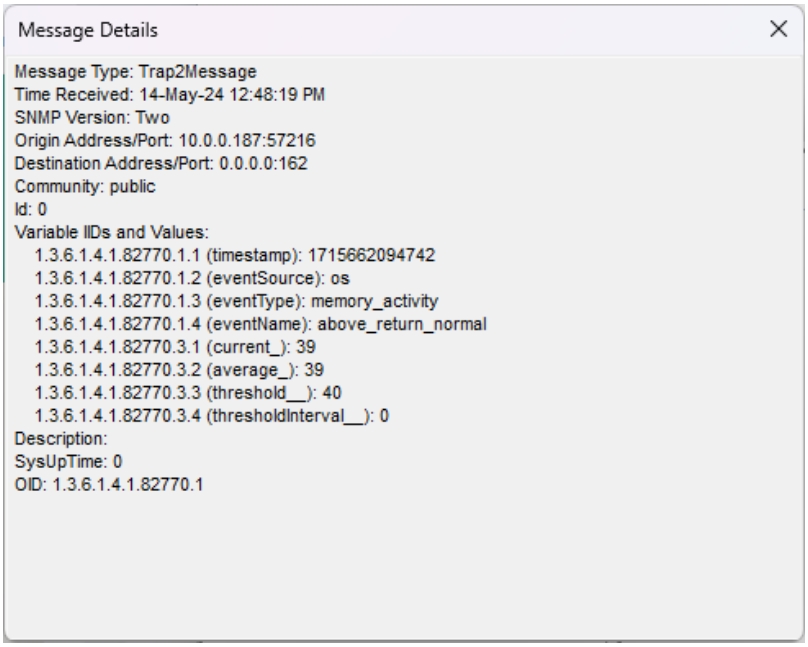


Figure 229

13.9.3 Disk Activity

- Disk read activity above limit

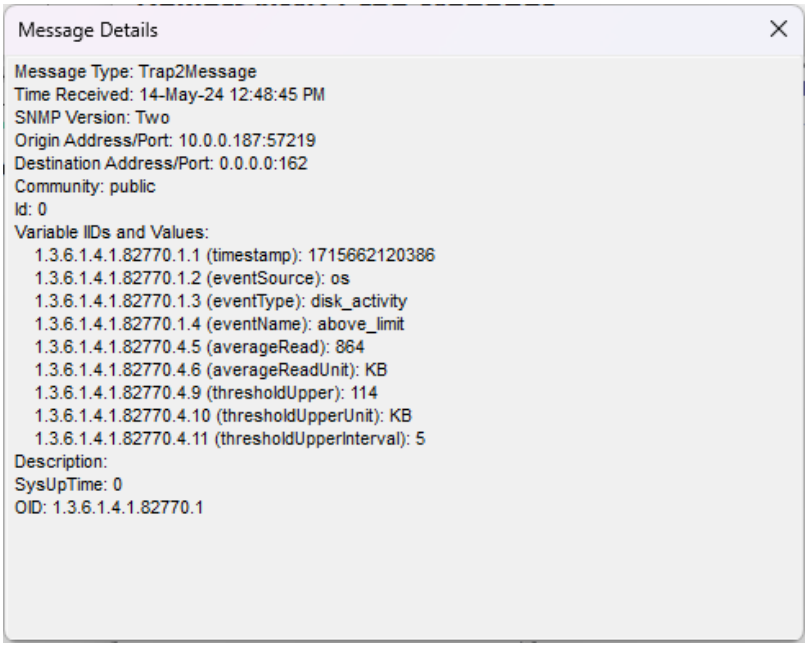


Figure 230

- Disk read activity back to normal

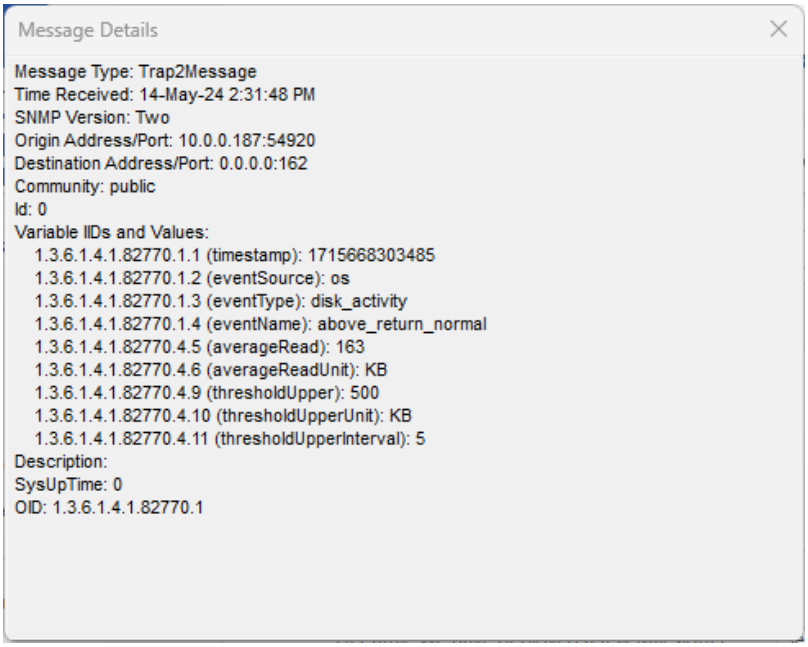


Figure 231

- Disk write activity above limit

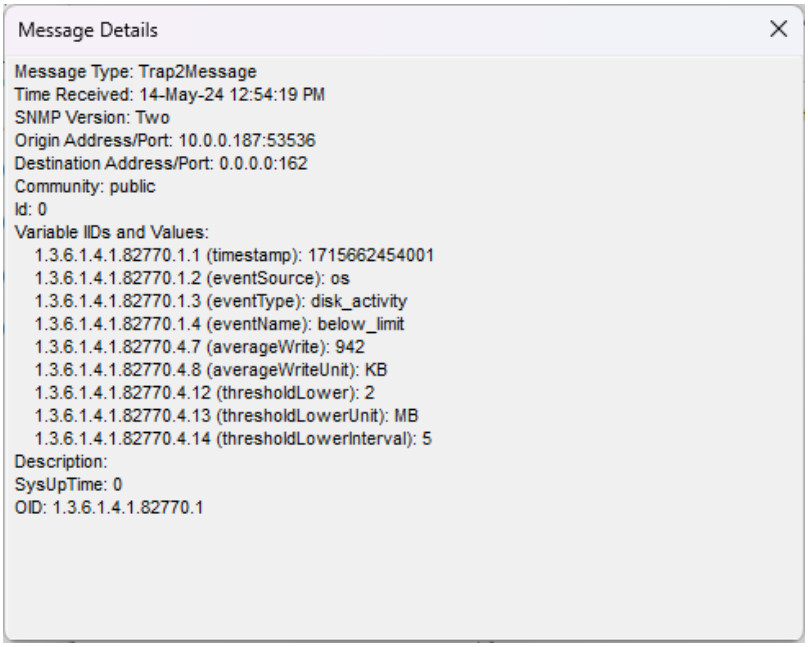


Figure 232

- Disk write activity back to normal

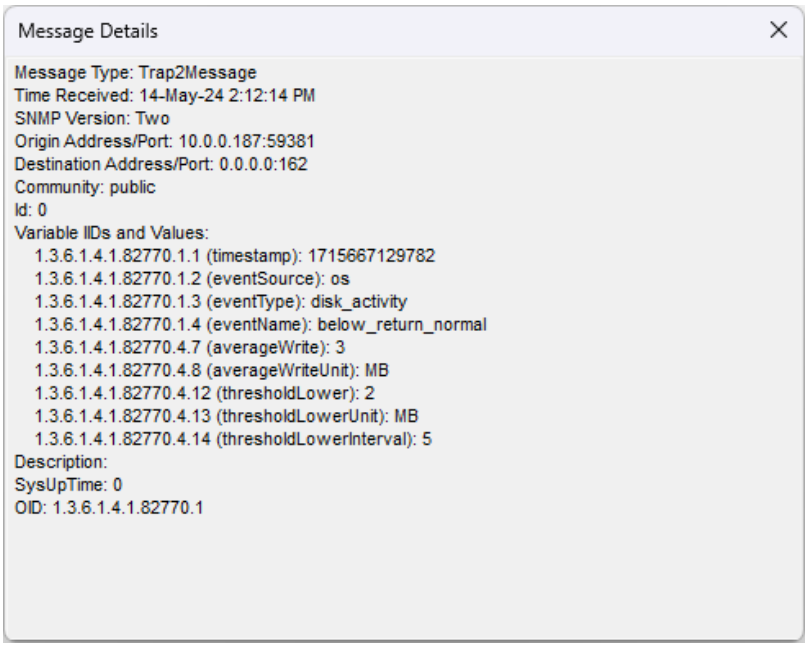


Figure 233

13.9.4 Network Activity

- Network send activity above limit

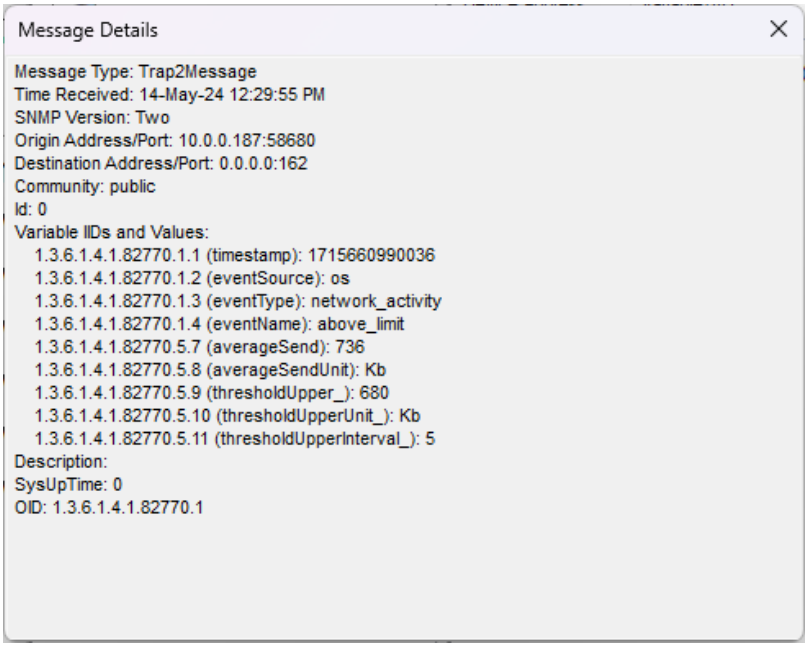


Figure 234

- Network send activity back to normal

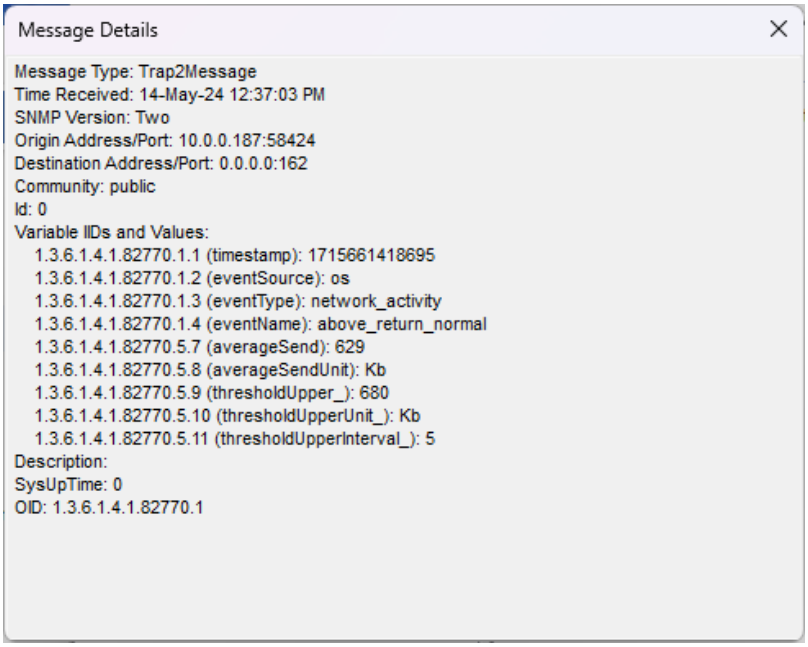


Figure 235

- Network receive activity above limit

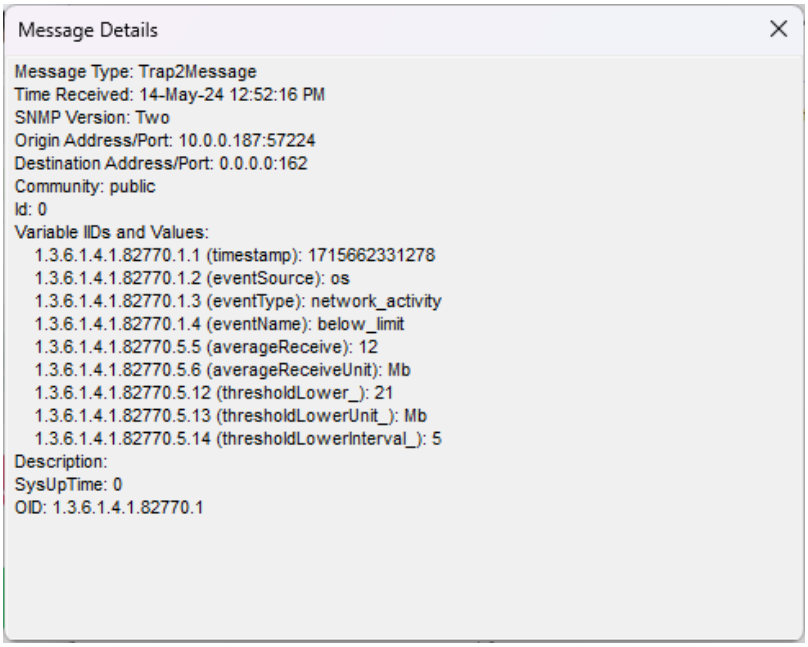


Figure 236

- Network receive activity back to normal

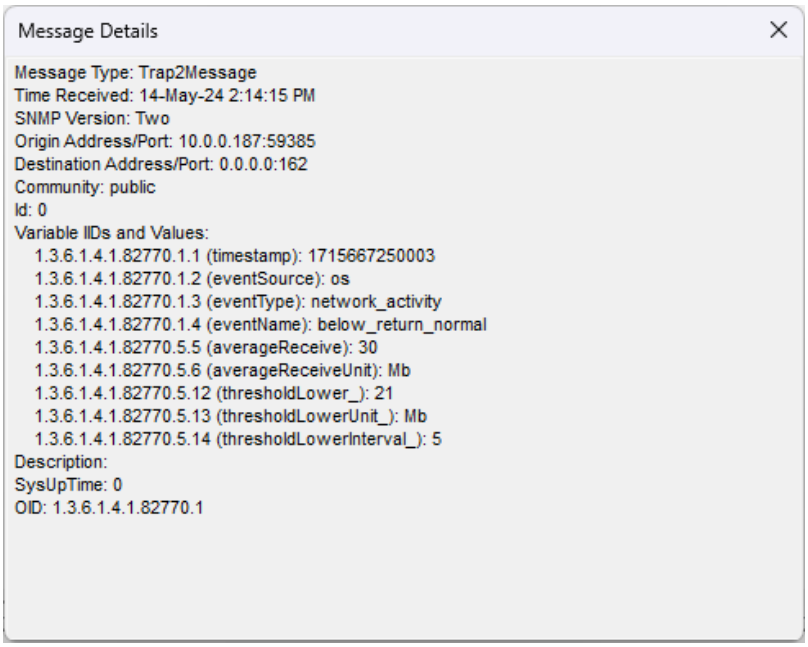


Figure 237

- Network cable unplugged

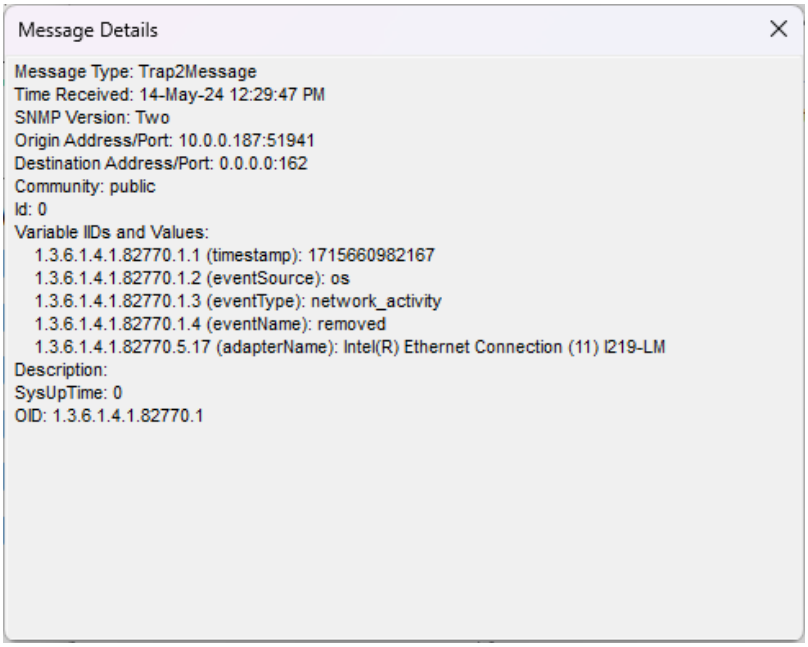


Figure 238

- Network cable plugged

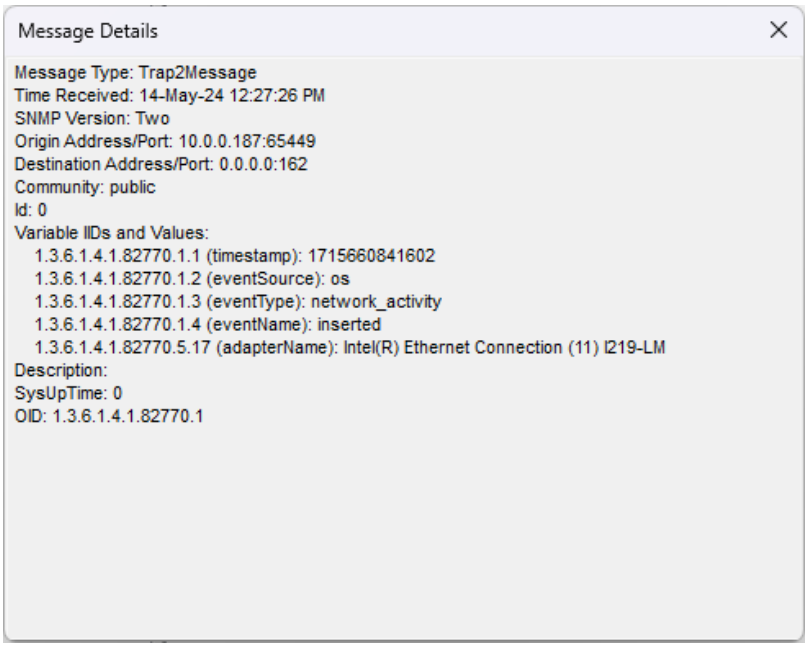


Figure 239

13.9.5 Disk Guard

- Disk removed

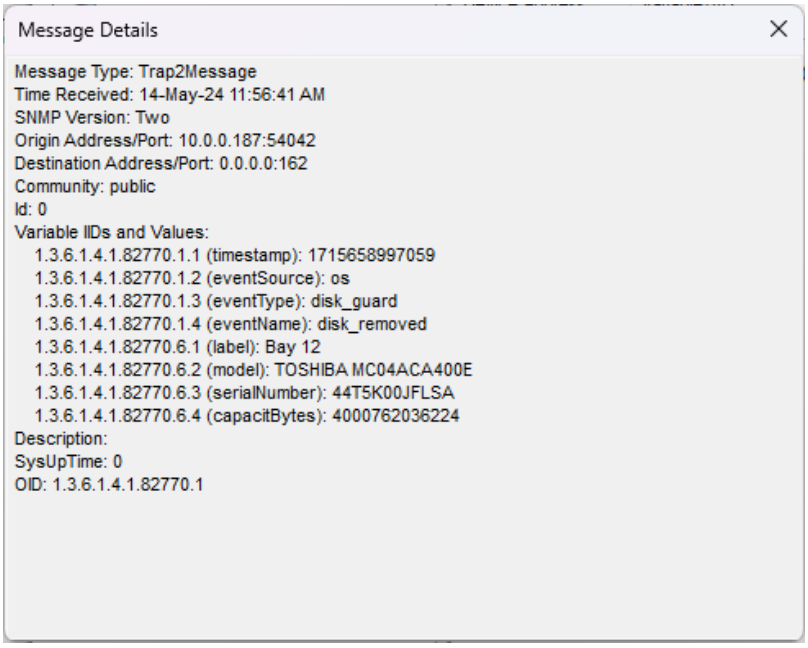


Figure 240

- Disk remove acknowledged

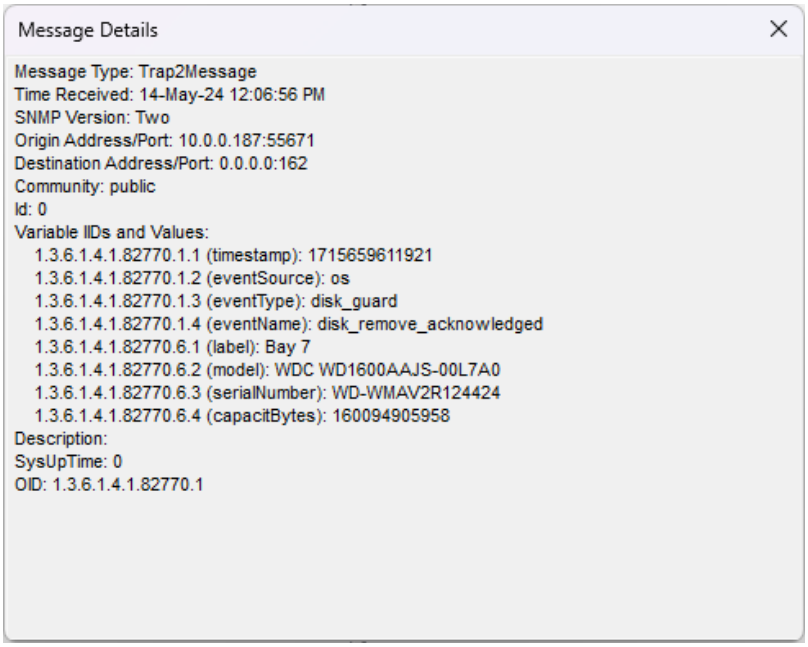


Figure 241

- Disk replaced

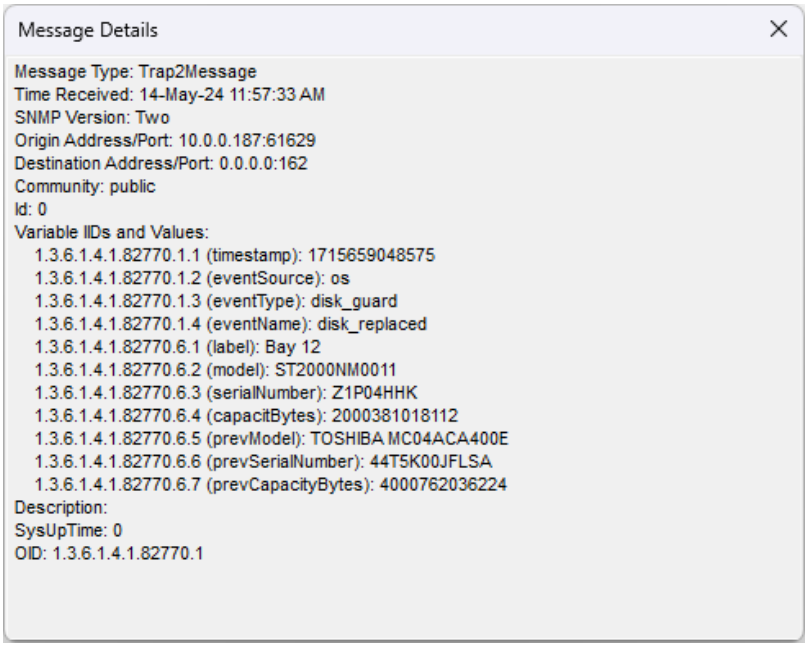


Figure 242

- Disk replace acknowledged

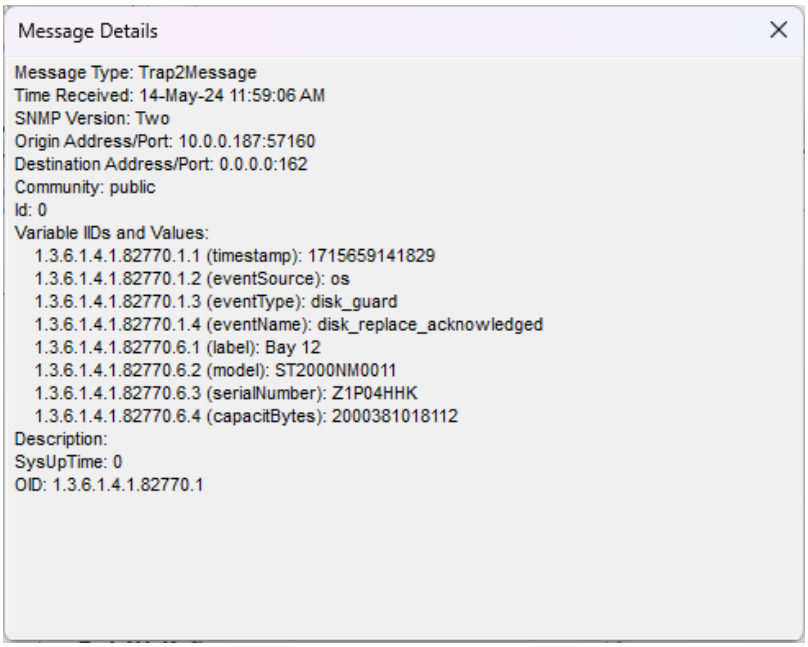


Figure 243

- Disk inserted

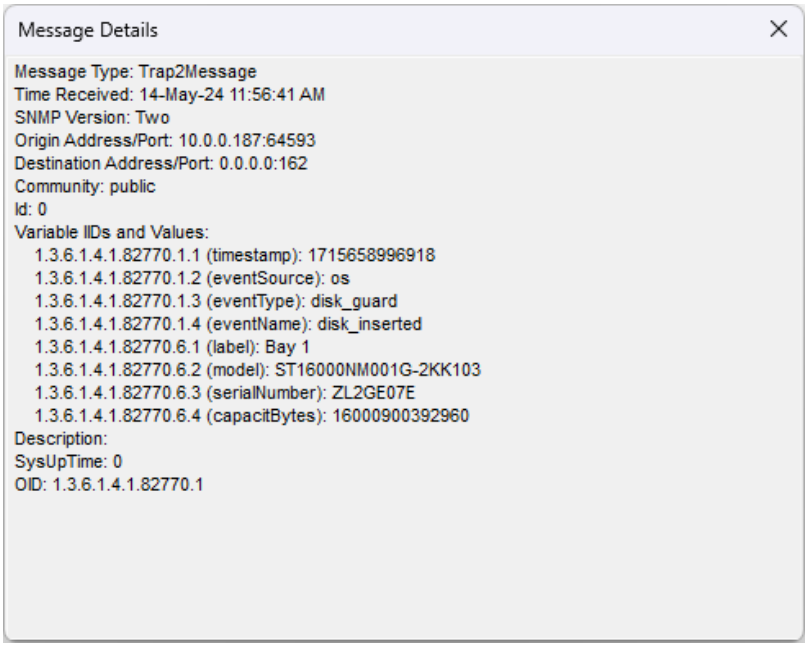


Figure 244

13.9.6 Disk Health

- Disk health status is warning

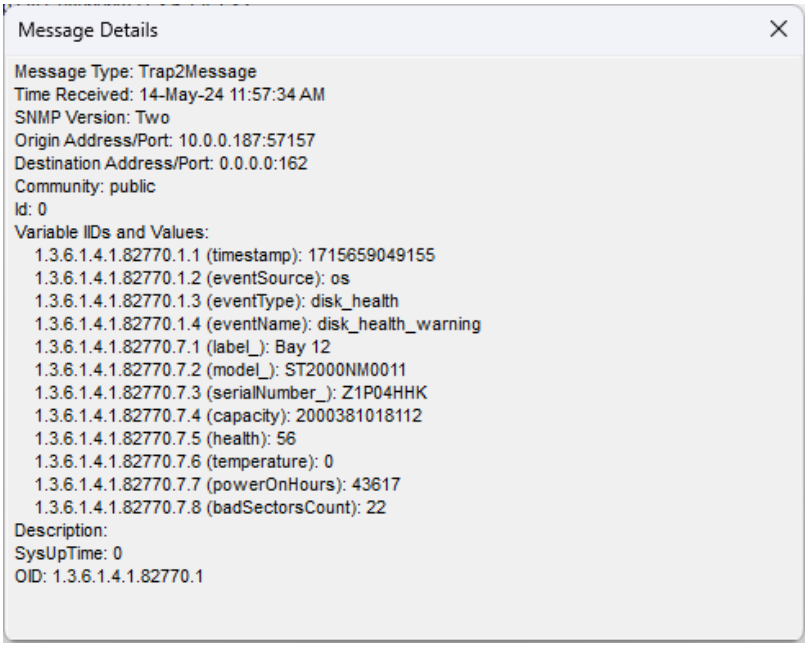


Figure 245

- Disk health status is critical

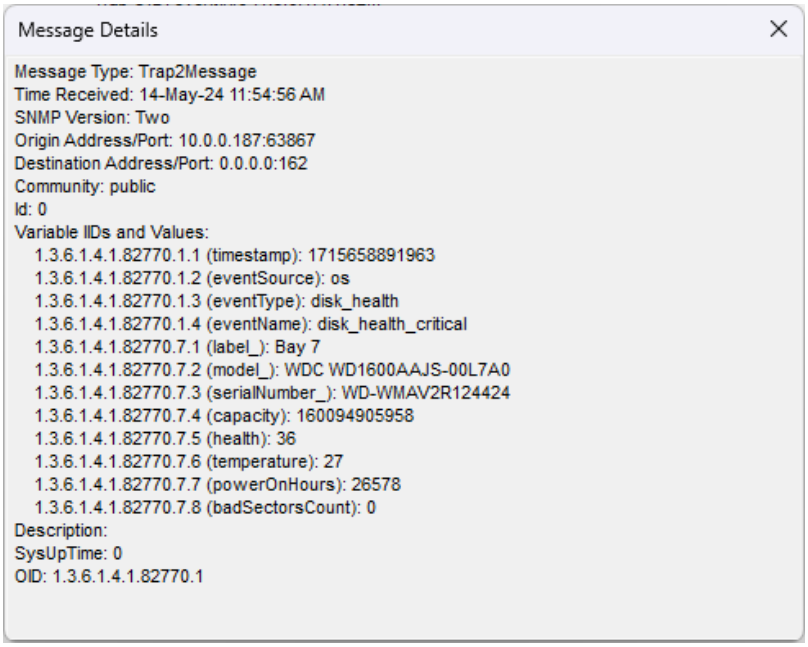


Figure 246

13.9.7 Hardware Monitor

- Fan status below limit

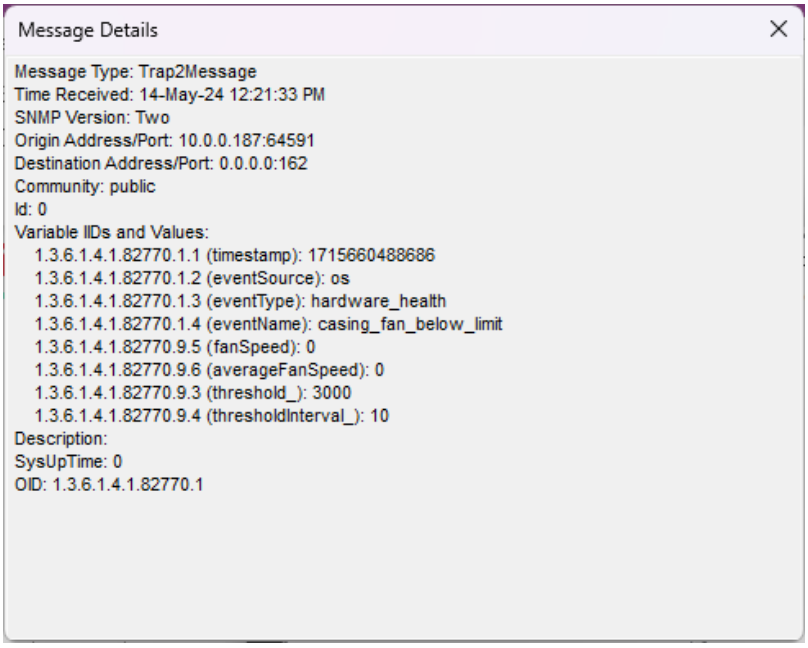


Figure 247

- Mainboard battery status below limit

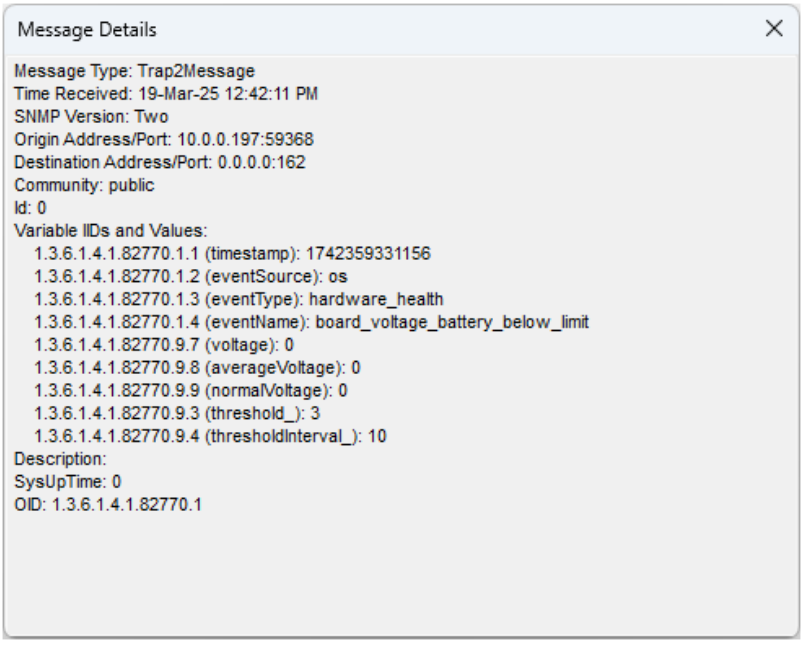


Figure 248

13.9.8 Session Shield [Only available in Windows Client]

- Session Shield status is warning

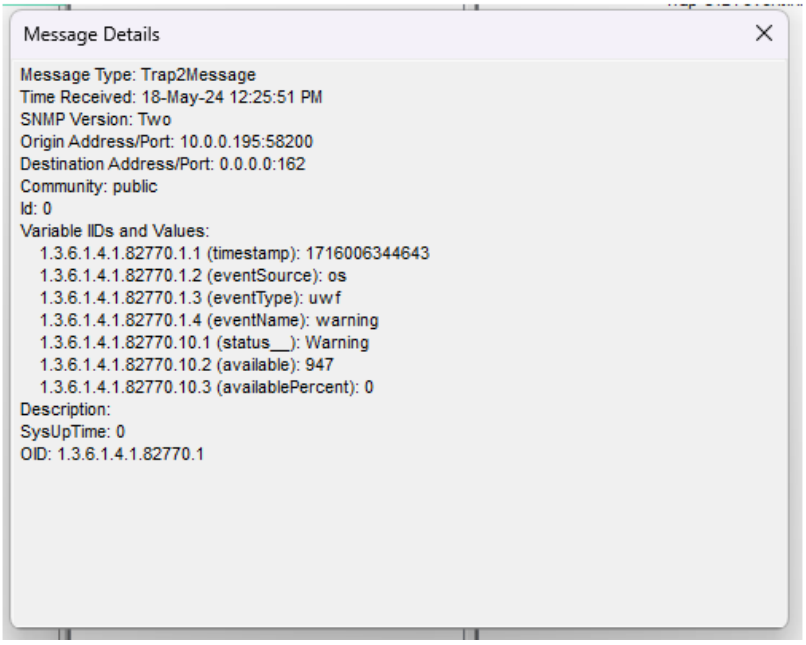


Figure 249

- Session Shield status is critical

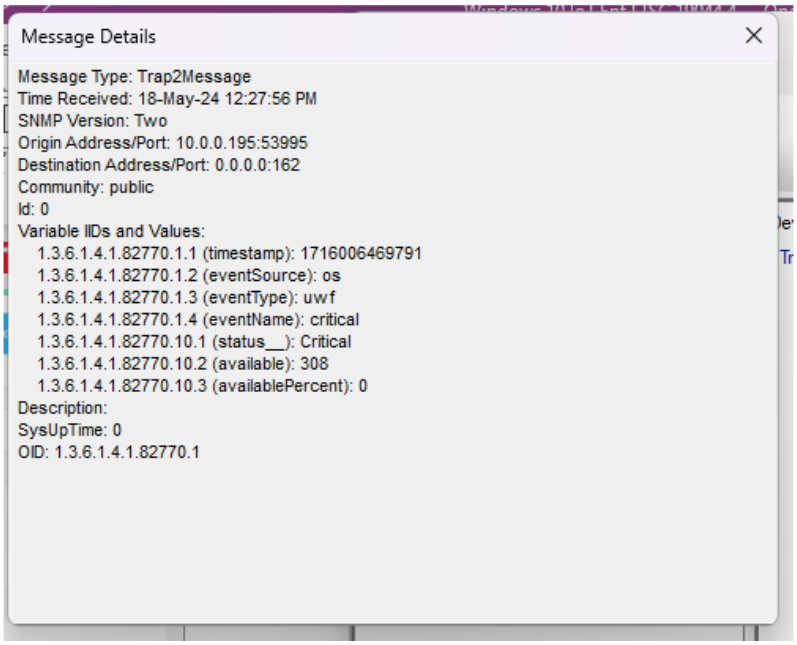


Figure 250

13.9.9 Application Monitor

- Application started

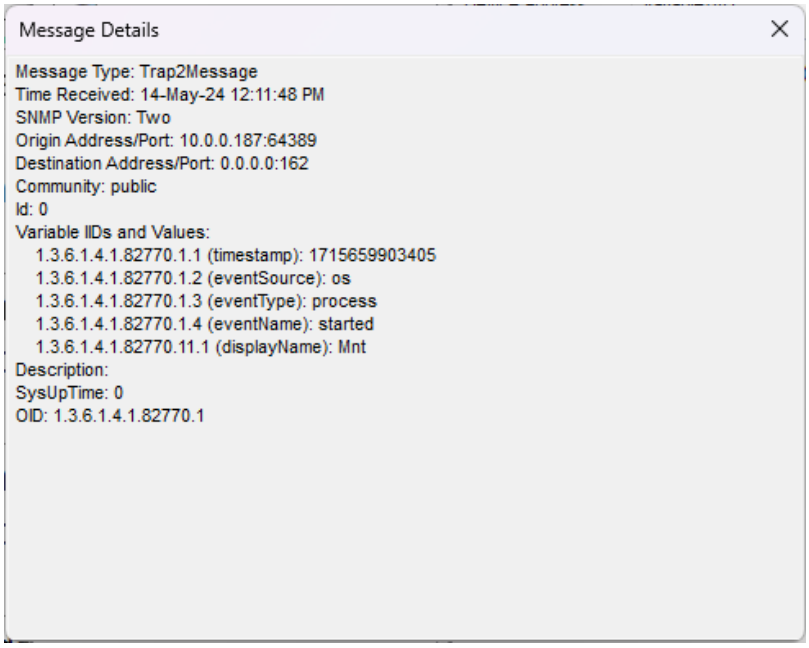


Figure 251

- Application stopped

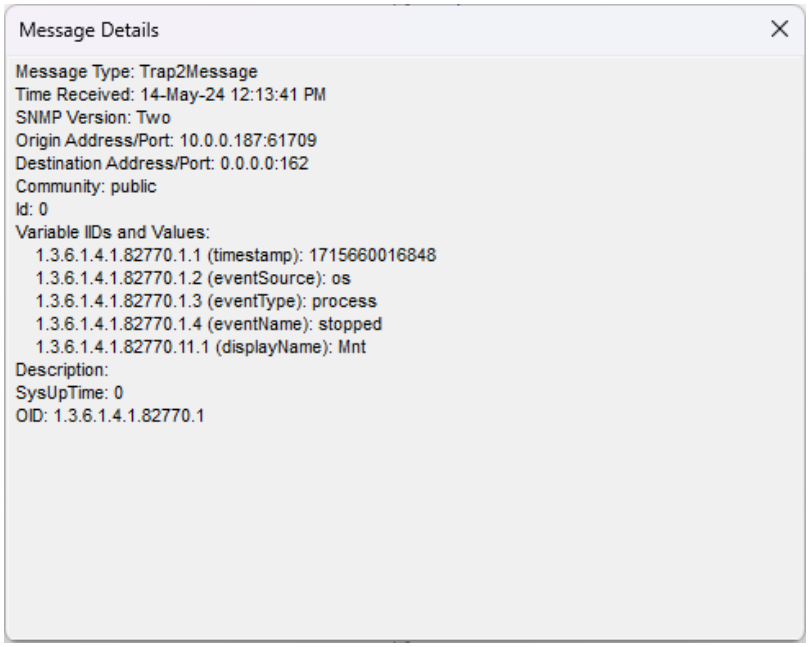


Figure 252

13.9.10 Redundant Storage System

- Storage pool status is healthy

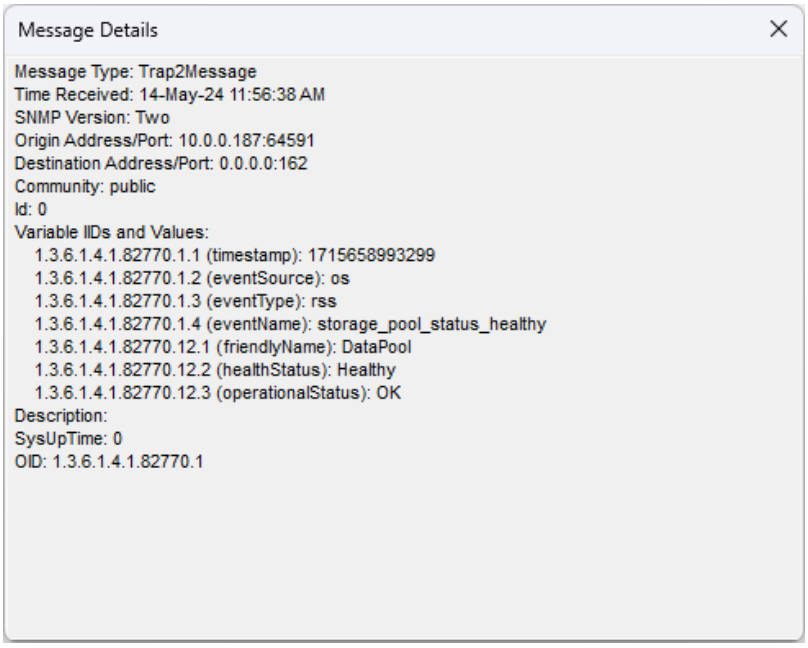


Figure 253

- Storage pool status is warning

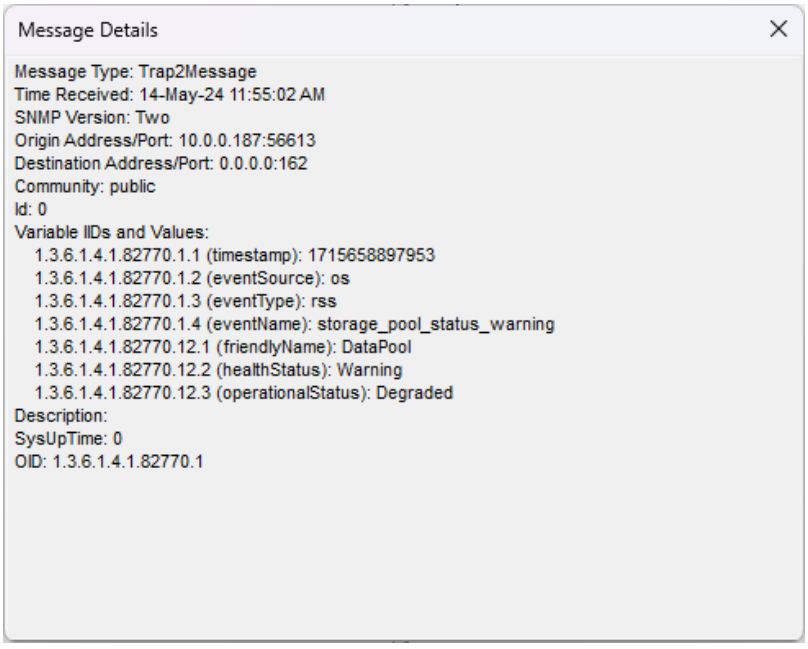


Figure 254

- Storage pool status is unhealthy

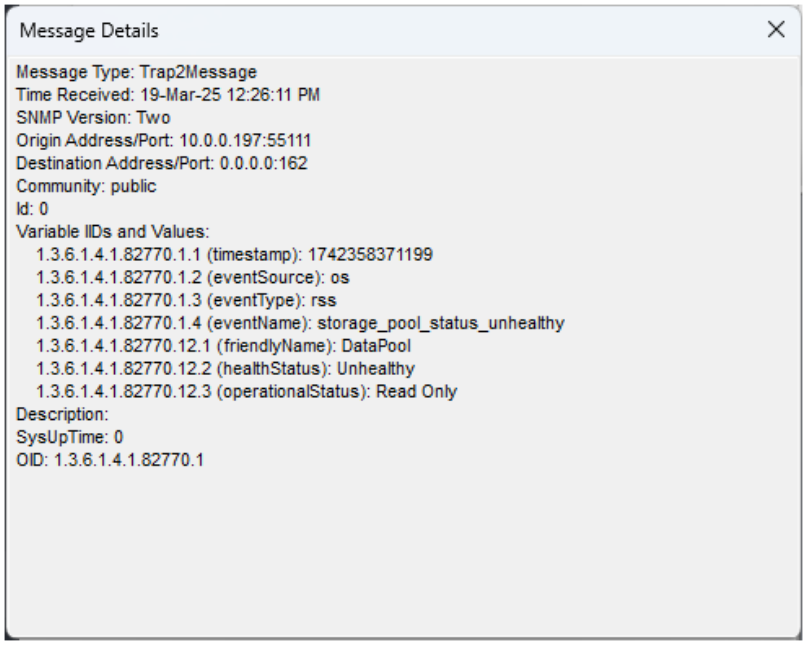


Figure 255

- Virtual disk status is healthy

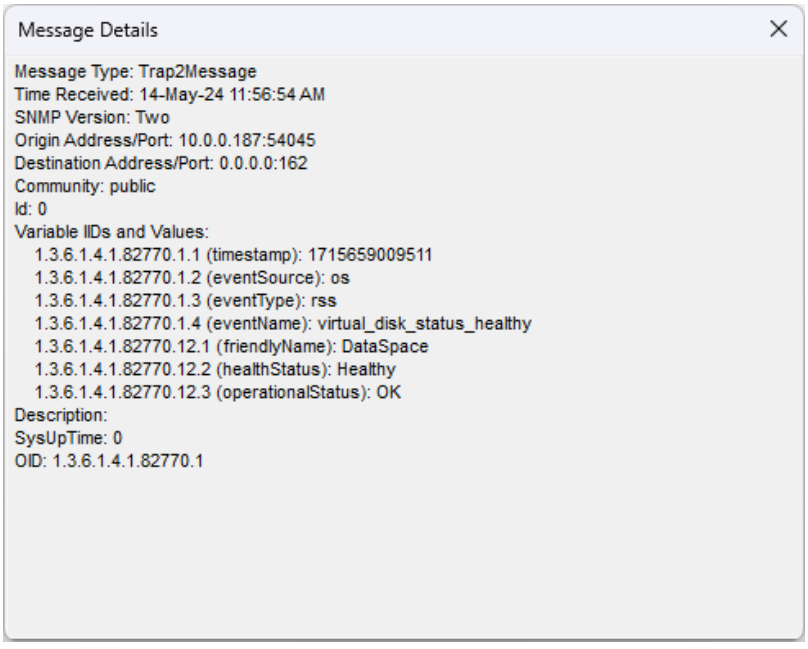


Figure 256

- Virtual disk status is warning

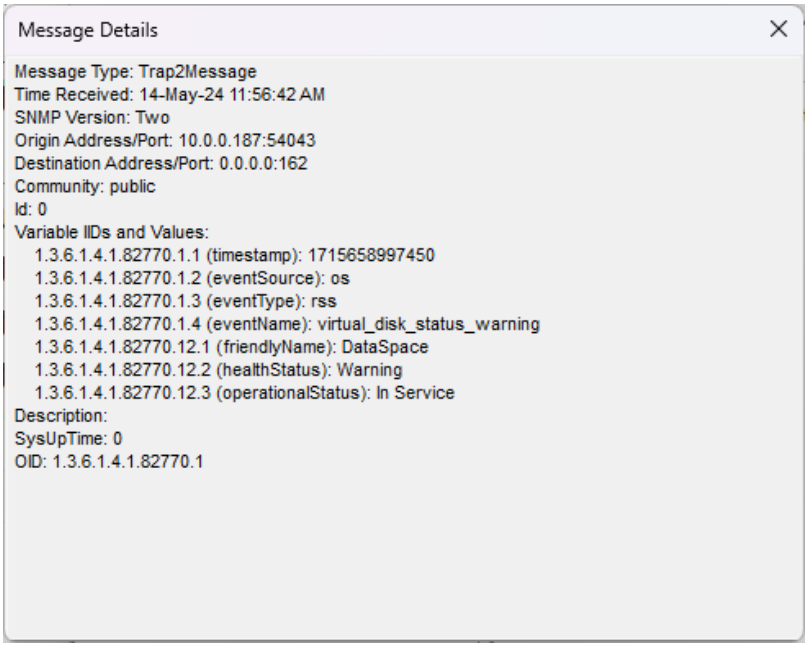


Figure 257

- Virtual disk status is unhealthy

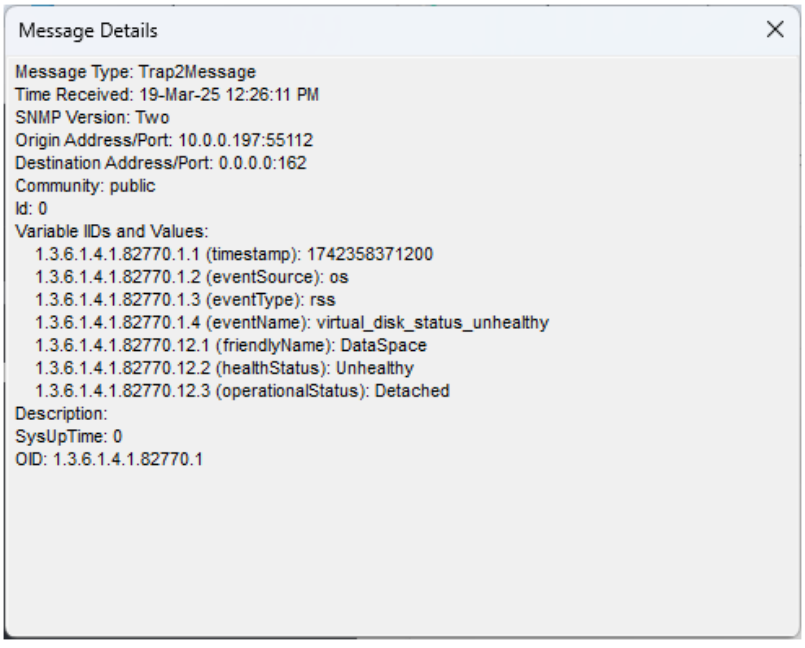


Figure 258

Trust our passion that brings us forward. Keep going!

https://gsfcorp.com/downloads/ecaosuserguide.pdf

© GSF Corporation
Unit 21, Level 3A, Jalan Kenari 5, Bandar Puchong Jaya, 47170 Selangor D.E., Malaysia | +603-80908080 | info@gsfcorp.com