EDM

Enterprise Diagnostics Monitor

User Guide

WWW.SYVIR.COM

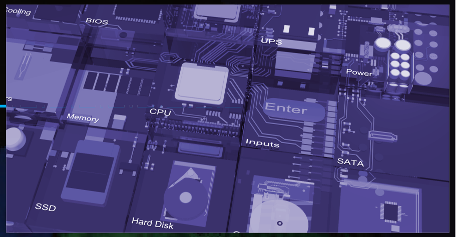
Limit of Liability and Disclaimer of Warranty: The publisher has used its best efforts in preparing this guide, and the information provided herein is provided "as is." Syvir Technologies Ltd makes no representation or warranties with respect to the accuracy or completeness of the contents of this guide and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose and shall in no event be liable for any loss of profit or any other commercial damage, including but not limited to special,incidental, consequential, or other damages.

Trademarks: This guide identifies product names and services known to be trademarks, registered trademarks, or service marks of their respective holders. They are used throughout this guide in an editorial fashion only. In addition, terms suspected of being trademarks, registered trademarks, or service marks have been appropriately capitalized, although Syvir Technologies cannot attest to the accuracy of this information. Use of a term in this guide should not be regarded as affecting the validity of any trademark, All trademarks acknowledged.

Enterprise Diagnostics Monitor

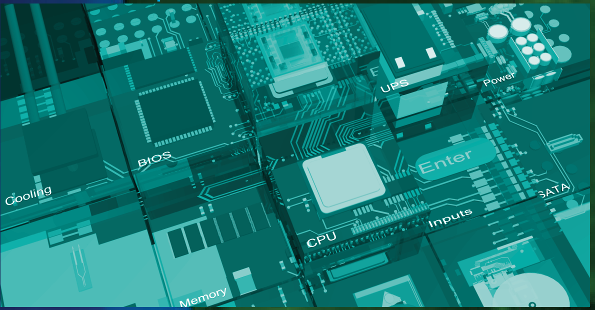
Contents

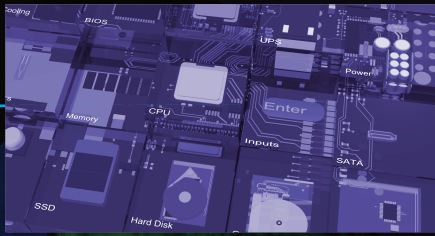
Context.



Often in the network monitoring stack, diagnostics is overlooked. Typical network monitor programs focus on performance counters for some hardware items. Performance counters return CPU load percentages or hard drive temperatures.
They often don’t return any data regarding any hardware faults or failures.

A different type of network monitoring program is required for this. With Windows the underlying subset enables us to return live and current hardware diagnostic status.

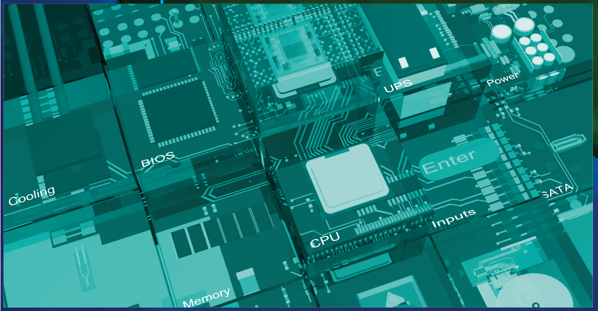




With remote working allowing staff to be located anywhere in the world this causes major issues for companies.
Clearly access to distributed endpoints can be difficult.
Sending out an engineer to employees homes can be time consuming and expensive.

Using a service probe on each machine enables diagnostic data to be sent over HTTPS to a cloud server.
Data is displayed in a web browser and alerts are sent through email to I.T staff, who can react accordingly.
All connected endpoints wherever they are in the world can return data.
Diagnostic data on hardware components in the endpoint is returned.

Enterprise Diagnostics Monitor is a windows diagnostic monitor for companies that scans for problems with hardware components.



Welcome.

Enterprise Diagnostics Monitor (EDM) is a cloud based remote network hardware monitor.
EDM is hosted by Syvir. We run the hosted server for you.
A web interface provides monitoring and configuration.

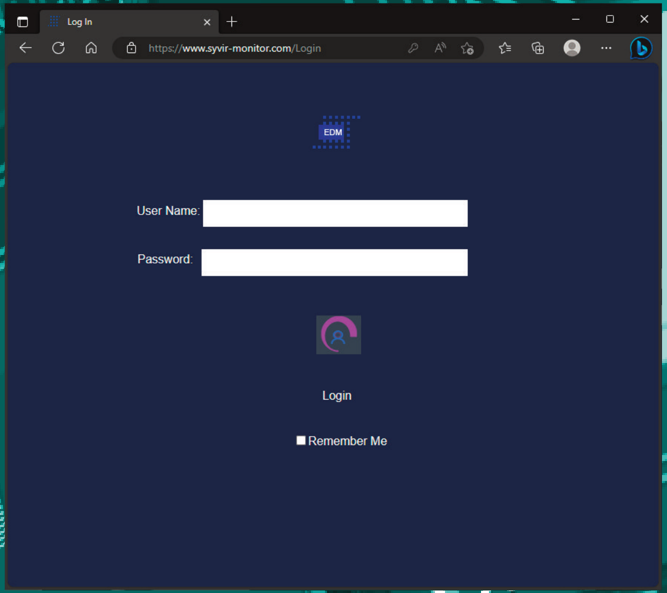
To create a hosted solution please visit www.syvir.com and start a free trial.
Syvir automatically creates a local domain name for your instance of EDM.

With your account you are assigned two usernames and passwords.

Make sure you agree to the privacy policy along with the terms and conditions.

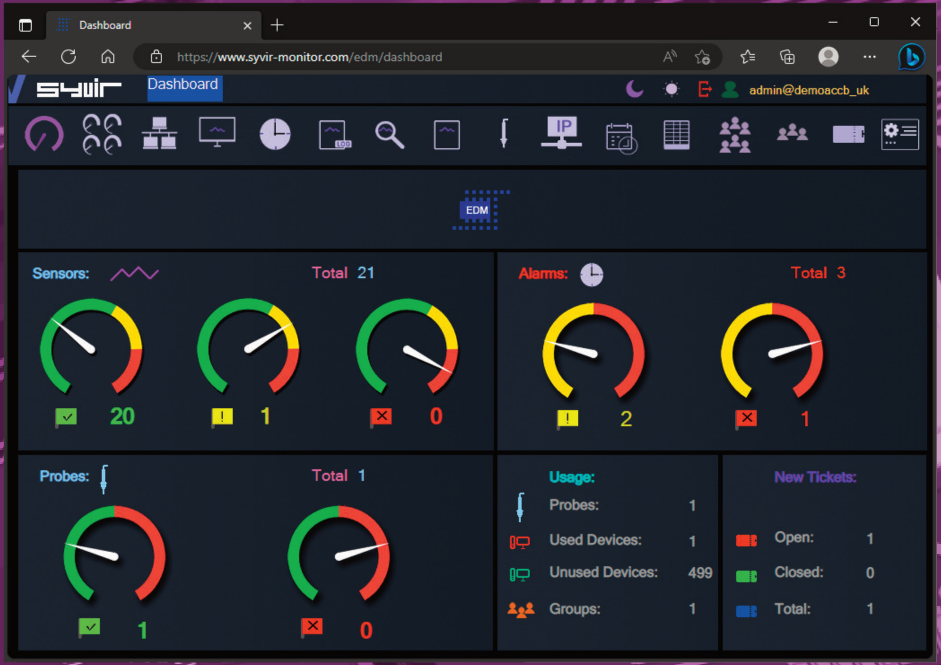
Once you have signed up you will receive a welcome email.
This contains your login information.

The site provides visual monitoring and reports of your monitored network.
Enter your credentials and click Login, to log into (EDM).



In this eBook we guide you with monitoring your network endpoints with Enterprise Diagnostics Monitor (EDM) using our cloud based monitoring system.

To begin monitoring your endpoints you will need to download software to install on your endpoints.
We advise if you are trying out EDM for the first time on a network to try the service on one machine, so you can assess the capabilities of EDM.



Sensors: Total 21
✓ 20 ! 1 ✕ 0

Alarms: Total 3
! 2 ✕ 1

Probes: Total 1
✓ 1 ✕ 0

Usage:
Probes: 1
Used Devices: 1
Unused Devices: 499
Groups: 1

New Tickets:
Open: 1
Closed: 0
Total: 1

Once this process is complete run the software using the Probe@ account and password. Other account names will not work.
Type in your Group code and select the endpoint type.
A probe will be created on the SYVIR EDM cloud.
Sensors are automatically created for the probe.
Next install the service probe, this runs on the endpoint all the time and scans WMI for diagnostic problems

Each time the system is scanned, diagnostic data is uploaded to the syvir-edm cloud.

A probe running on each monitored endpoint, connects to the EDM cloud server.
The probe is a windows service that runs all the time the endpoint is switched on.
Diagnostic data is transferred to the cloud.
Data is accessed through any device that supports a web browser.

Structure.

The structure of EDM.

Diagnostic data is gathered from the endpoint with WMI.
The sensors in the probe processes this data into channels and sets alarms if a problem is found.
Data is encrypted through SSL to the edm server.
Data is transferred through HTTPS and uses port 443
Data is stored and rendered through active server pages.

Probe

A EDM probe is a windows based service that connects to the EDM server.
Each monitored ENDPOINT has its own Probe.
This is designated by the computer name.
We recommend that each monitored Endpoint has it's own unique name, to avoid conflicts using EDM.
The hierarchical structure of EDM places the probe as the most powerful item in a Endpoint deployment.

Sensors

The probe contains Sensors that use WMI technology to monitor the current state of hardware.
Sensors are deployed to monitor hardware.
Sensors contain channels for multiple items i.e several drives etc.
Diagnostic data is received for each channel that's in use with a deployed sensor.

Channels

The sensor contains multiple channels.

For instance a USB sensor checks each usb port and assigns the port to a channel.

Properties

Diagnostic data is gathered from the endpoint with WMI.
The sensors in the probe processes this data into channels and sets alarms if an action is needed.
Data is transferred through HTTPS to the EDM Cloud.
Data is stored and rendered through active server pages.

Local installation.

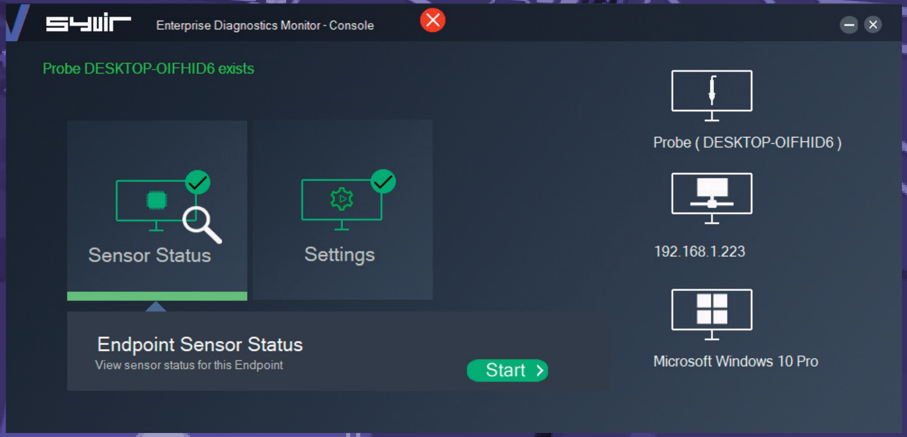
Each endpoint requires two installation processes.

One to create your machine probes profile, this will be where you enter your domain probe username and password.
These are stored locally in an encrypted file.
Select the machine type you wish to scan.

PC
Server
VMWare
Hyper-V
VMWare and Hyper-V deploy less sensors as quite a few are not detected.
In practice on Hyper-V and VMWare scans you can select PC or Server if you wish, but note you will get alot of Sensors, set to Not Detected.
Type in your username and password. For the console you need to use probe@company other logins will not work!

The second process requires installation of the Syvir - Enterprise Diagnostics Monitor service.
This service is the probe for the machine.
WMI services need to be running on each machine you wish to monitor with EDM.
Please note the account you use to monitor with WMI only requires Read permission.
Do not enable Read/Write or Write this may leave the machine open to viruses etc.
1. Install Enterprise Diagnostics Monitor - Console
2. Once the Enterprise Diagnostics Monitor - Console setup program is installed please run this.
3.Type in your username and password and Group code. This will create the probe for this machine in the EDM cloud.
4.Install Enterprise Diagnostics Monitor - probe.

Diagnostics Monitor - Probe
Once this is installed monitoring is now setup for this machine.
Repeat this process for each machine you wish to monitor.
Each endpoint requires two installation processes one to create your machine probes profile, this will be where you enter your domain probe username and password.
These are stored locally in an encrypted file.
The second process requires installation of the
The Probe service transfers non-identifiable data through HTTPS to the EDM cloud.
Once the Enterprise Diagnostics Monitor Console is installed please run this.
Enterprise Diagnostics Monitor service.
This service is the probe for the machine.
WMI services need to be running on each machine you wish to monitor with EDM.


Enterprise Diagnostics Monitor - Console

Probe DESKTOP-OIFHID6 exists

Endpoint Sensor Status
View sensor status for this Endpoint

SYVIR EDM is specially designed to check endpoints for faults.

Groups are added in the Add Group page.

To add a new group type in the groups name into the Group box.
Add a unique code for the group code.
The group code is used to separate different endpoints. This enables endpoints to be grouped together and avoid probe console name clashes.
Once you have entered these click on add.

To view a list of groups select the Group page.
To delete groups from the system click on the Delete button the click on OK. This deletes the group from SYVIR EDM.
To save a list in a .csv file, click on the download icon.

Schedule

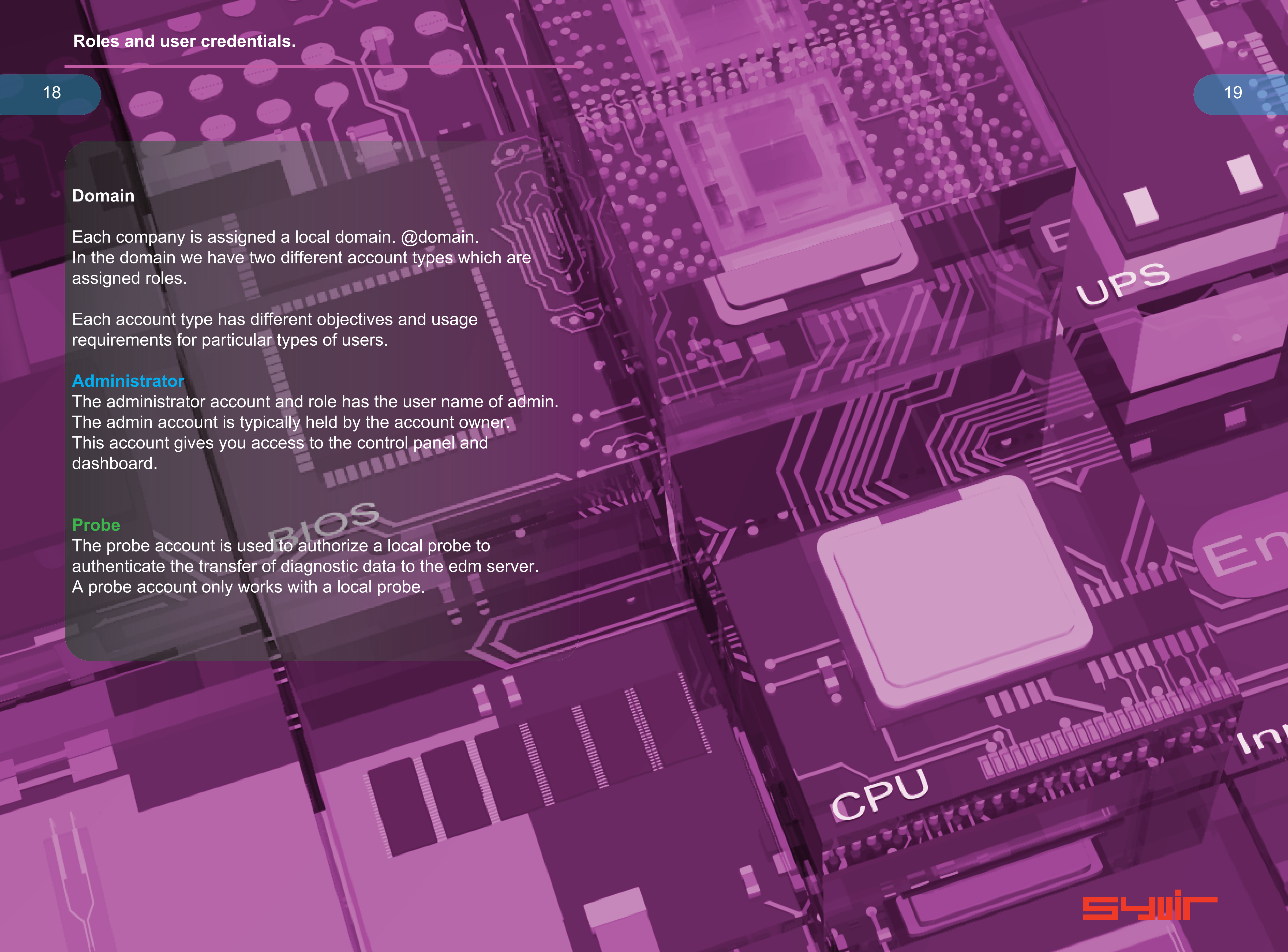
An email can be sent to each Group using Syvir EDM.
This will show that checks have been made on their systems.
The email will inform if any issues have detected with their endpoints hardware in the last 24 hours.
To enable emails alerts goto the schedule page.
1. Click on the group you wish to setup email alerts for.
2. Select the time you wish each day for the email to be sent.
3. Type in the Groups email address.
4. Check the Send Email box.
Click on save.

Reports

A wide range of reports are available in csv file format for use in a spreadsheet.
The directory box on the left contains all your Groups, click on a Group name. On the left hand directory box is a list of that Groups probes.
With some reports you need to select a Group first.
All data for that Groups probes will be downloaded.
Some reports require the probe to be selected so individual reports on specific probes can be made.

These are the reports produced by SYVIR EDM

Sensors on the selected Group probe, that are UP.
Sensors on the selected Group probe, that are set to WARNING.
Sensors on the selected Group console probe, that are DOWN.
All Probes and Sensors on the selected Group, that are UP.
All Probes and Sensors on the selected Group, that are set to WARNING.
All Console Probes and Sensors on the selected Group, that are DOWN.
Diagnostics for the selected Group Probes sensors.
Sensors on the selected Group probe, that are set to UP, WARNING and DOWN.
All Probes and Sensors on the selected Group, that are set to UP, WARNING and DOWN.
Diagnostics for the selected Group Probes alarm.
Alarms on the selected Group probe.
Alarms on all Group probes.



Domain

Each company is assigned a local domain. @domain.
In the domain we have two different account types which are assigned roles.

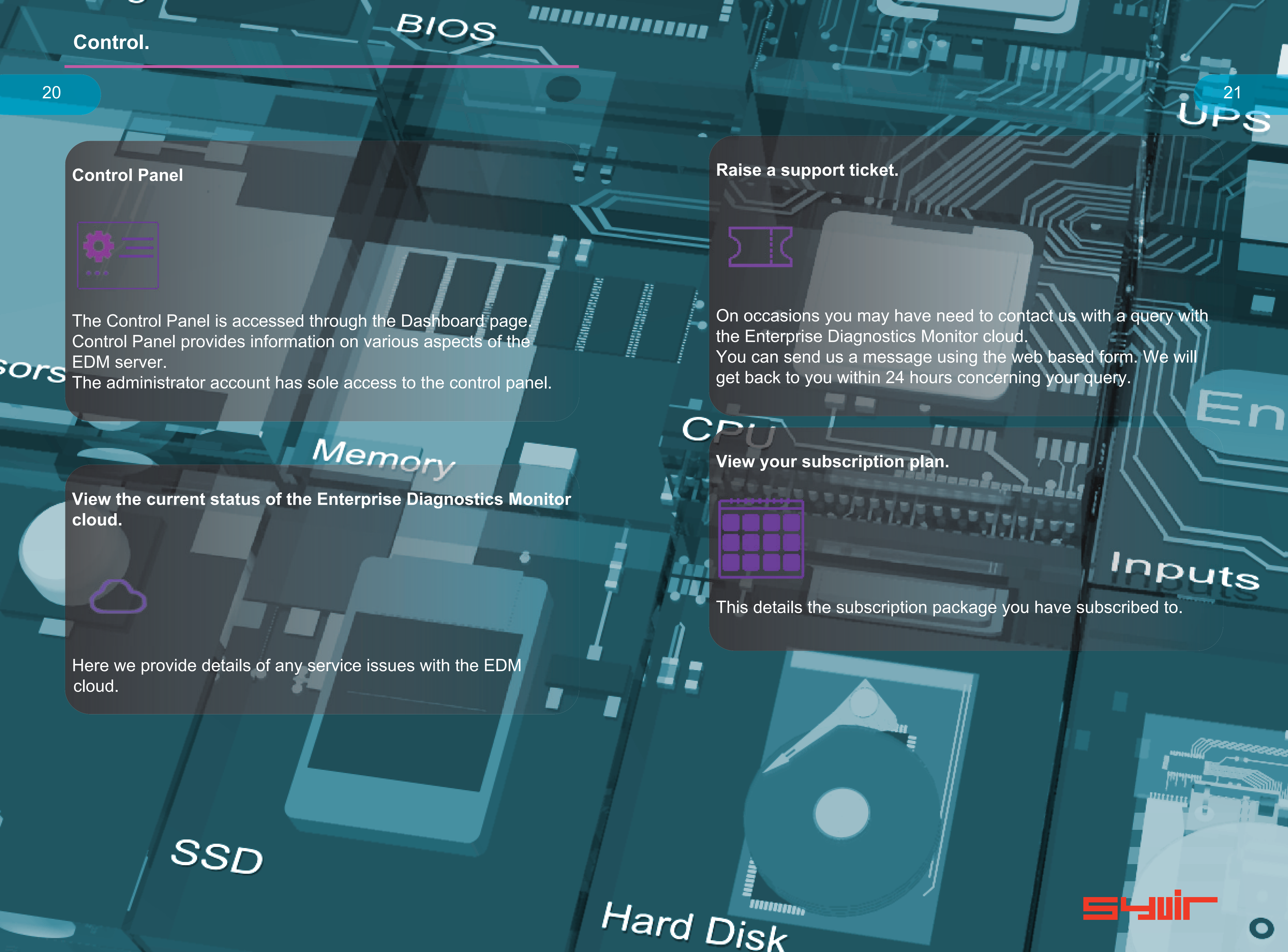
Each account type has different objectives and usage requirements for particular types of users.

Administrator

The administrator account and role has the user name of admin.
The admin account is typically held by the account owner.
This account gives you access to the control panel and dashboard.

Probe

The probe account is used to authorize a local probe to authenticate the transfer of diagnostic data to the edm server.
A probe account only works with a local probe.



Control Panel

The Control Panel is accessed through the Dashboard page. Control Panel provides information on various aspects of the EDM server.
The administrator account has sole access to the control panel.

View the current status of the Enterprise Diagnostics Monitor cloud.

Here we provide details of any service issues with the EDM cloud.

Raise a support ticket.

On occasions you may have need to contact us with a query with the Enterprise Diagnostics Monitor cloud.
You can send us a message using the web based form. We will get back to you within 24 hours concerning your query.

View your subscription plan.

This details the subscription package you have subscribed to.

Roles and user credentials.

EDM uses Roles and user credentials to determine the access that user accounts have to the EDM server.
The administrator account and role has the user name of admin.
The admin account is typically held by the account owner.
This account gives you access to the control panel and dashboard.

The probe account is used to authorize a local probe to authenticate the transfer of diagnostic data to the EDM Cloud.

Check the number of sensors deployed on your endpoints.

This number shows how many sensors assigned to the local probes on your computers.

Check the number of probes deployed on your computers.

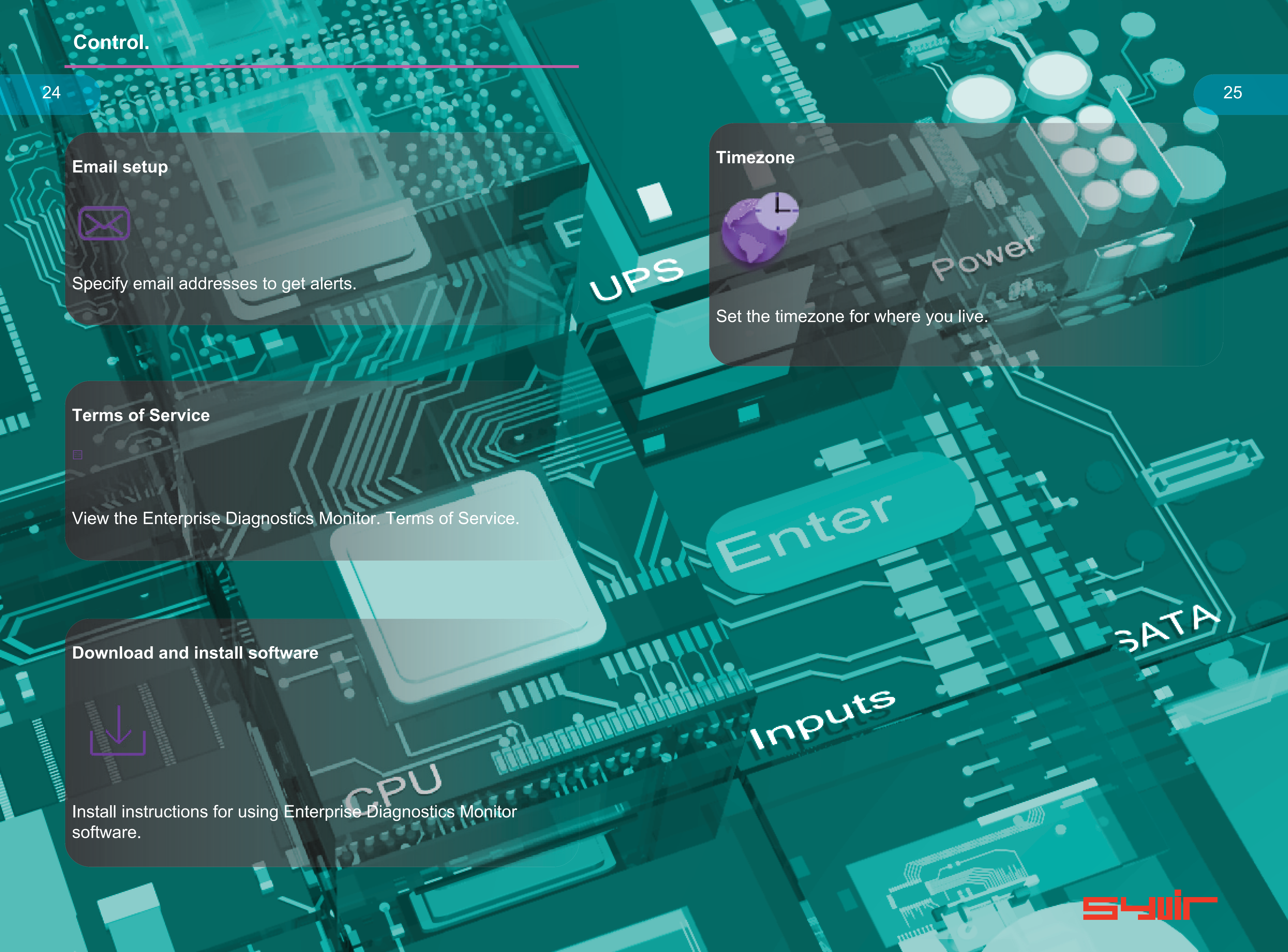
This number indicates how many probes you have installed on your network computers.

Probe Setup

Install and setup a probe on a windows endpoint.

Interval

Set the interval between scans.



Email setup

Specify email addresses to get alerts.

Terms of Service

View the Enterprise Diagnostics Monitor. Terms of Service.

Download and install software

Install instructions for using Enterprise Diagnostics Monitor software.

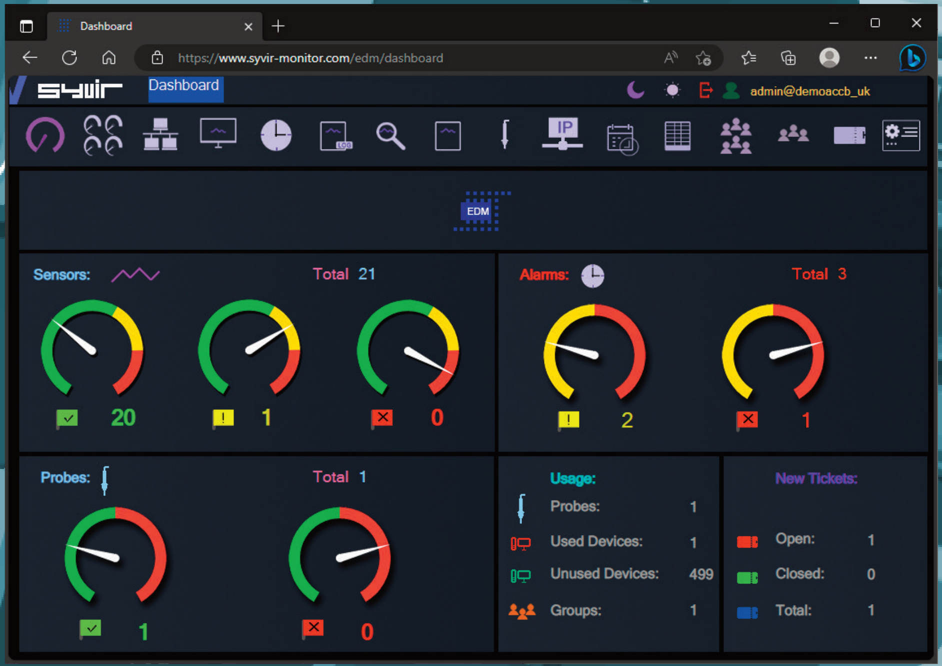
Timezone

Set the timezone for where you live.

Web.

We recommend Google Chrome and Microsoft Edge browsers.

Click on the login icon to visit the login page.
Type in your credentials that were issued to you in your welcome email.
Only administrator accounts have full access to web interface.



Usage:

Probes:	1
Used Devices:	1
Unused Devices:	499
Groups:	1

New Tickets:

Open:	1
Closed:	0
Total:	1

Dashboard.

The starting point for any web based monitoring session is the dashboard page.
This gives a quick at a glance view of the last known statuses of sensors probes and alarms.
EDM stores in the cloud the last known values from your network.
The five sensor dials cover the various states of the sensors.

Probe diagnostic sensors

UP

The sensors channels are all functioning ok.

WARNING

A problem has been detected in one of the sensors channel(s).

DOWN

A serious issue has been detected in one of the sensors channel(s).

NOT DETECTED

Not detected in some cases EDM will not be able to retrieve WMI data for a given sensor.
Sometimes WMI data is not available for hardware devices.
It can vary from each computer vendor what WMI data is available.

In a lot of situations WMI data can be retrieved with a sensor but the data for the sensors requirements is missing...

Probe.

A windows based service that connects to the EDM server.
Each monitored Endpoint has its own Probe. This is designated by the computer name.
The hierarchical structure of EDM places the probe as the most powerful item in a pc deployment.

Probe status

UP

The probe is functioning ok.

DOWN

The probe is either not running or the endpoint that the probe is on has been switched off.

Internet

Data is transferred to the EDM server using HTTPS, a constant internet connection is required to transfer data.

Delete probe

From the probe directory view open the User hierarchical structure to list Probes on your Groups network connected to the EDM cloud.
Select the probe you wish to delete.
Click on the delete probe icon.
All data will be deleted along with the sensors attached to the probe.

The probe contains Sensors that use WMI technology to monitor the current state of hardware. Sensors are deployed to monitor Groups hardware. Sensors contain channels for multiple items i.e. several drives etc. Diagnostic data is received for each channel that's in use with a sensor. The sensor contains multiple channels.
For instance a USB sensor checks each usb port and assigns the port to a channel.

Sensor Status values

UP

The sensors channels are all functioning ok.

WARNING

A problem has been detected in one of the sensors channel(s).

DOWN

A serious issue has been detected in one of the sensors channel(s). This will trigger an alarm.

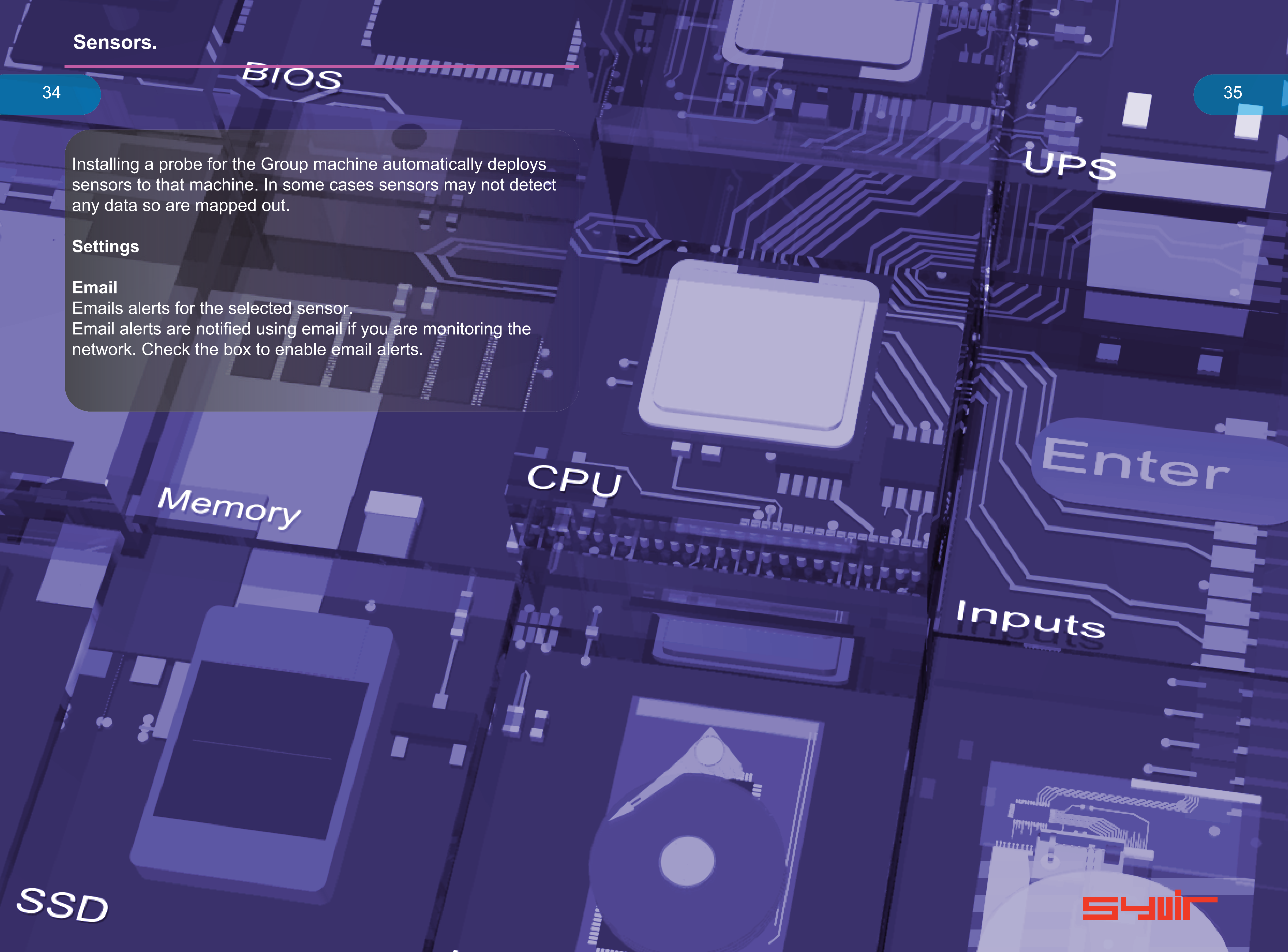
NOT DETECTED

On deployment the hardware has not been detected.
This could be for a number of reasons. i.e. the hardware doesn't exist on this system.
Other reasons for not detected status. In our experience if there is no data there, then no data will appear in the future. In a lot of situations WMI data can be retrieved with a sensor but the data for the sensors requirements is missing...
So for some deployments some sensors won't be available.

Installing a probe for the Group machine automatically deploys sensors to that machine. In some cases sensors may not detect any data so are mapped out.

Settings

Email
Emails alerts for the selected sensor.
Email alerts are notified using email if you are monitoring the network. Check the box to enable email alerts.



Alarms.

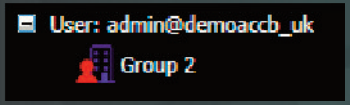
Alarms are produced when a sensor is set to WARNING or DOWN.

DOWN

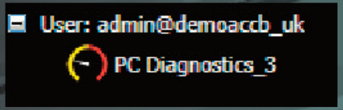
WARNING

The alarm takes the form of an email, when set, for the sensor that is changed.

View the current alarms.
From the Group directory view, select the Group you wish to view


User: admin@demoaccb_uk
Group 2

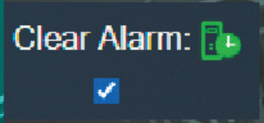
From the probe directory view open the User hierarchical structure to list alarms on Groups network connected to the EDM cloud.
Alarms are listed under each probe.


User: admin@demoaccb_uk
PC Diagnostics_3

Alarm
Once an alarm is created an email alert is sent to the designated email address.

A notification icon indicates that an email has been sent to the designated email address.

Clear Alarms

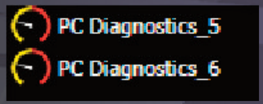

Clear Alarm: ☑

Select clear alarm and then the

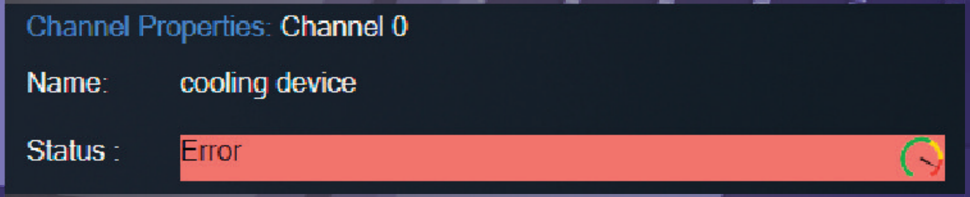
update icon. This clears the alarm.

Alarm Diagnostics.

Alarm diagnostics


PC Diagnostics_5
PC Diagnostics_6

Click on Probe Diagnostics to view the alarm status of the sensor on that probe.


Channel Properties: Channel 0

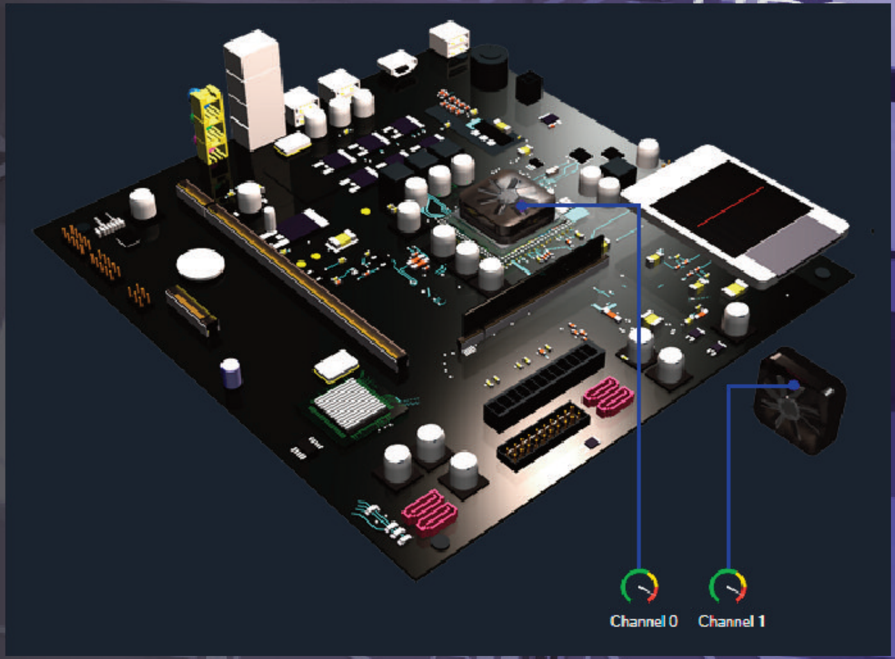
Name: cooling device

Status : Error

Click on the channel icons to retrieve diagnostic data for the particular channel. In some instances data can be basic.

In most instances you should be able to retrieve the Status of the Channel.

Usually this is a generic message of "OK"



Sensors dials are color coded to reflect the status of the sensor.
Green = UP.
Where a problem has been detected by the sensor, the dial will indicate
Yellow = Warning.
A dial that indicates Red = Down.

Click on a sensor to view channel data for the particular component.
In the system box is a generic pc view, Sensor channels are mapped to the hardware.

Properties.

Each channel has properties. Depending on the sensor.
These are the main properties...some sensors will use all of the properties, other sensors will just use one or two properties.

Status
Returns the status on the selected component.

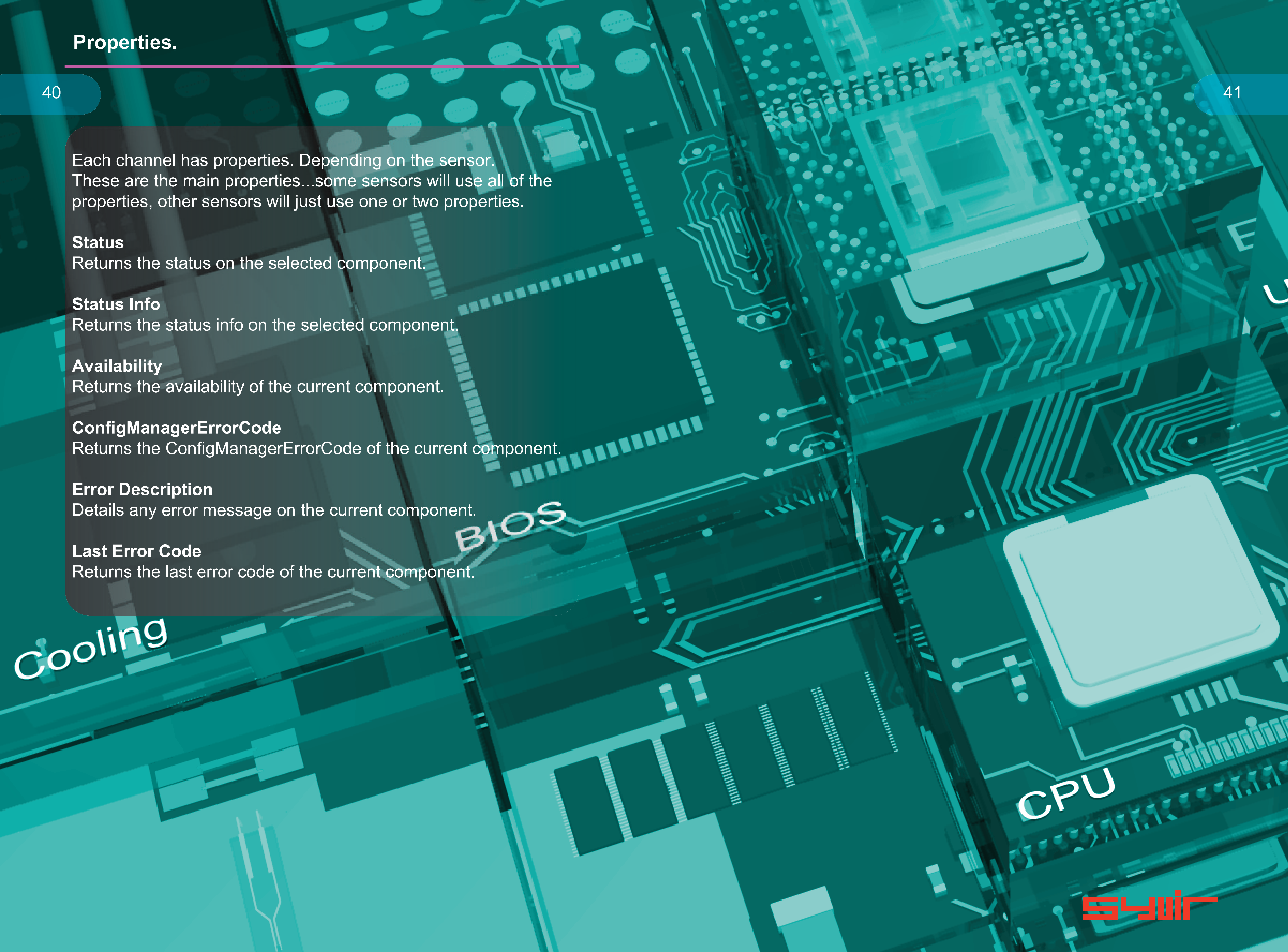
Status Info
Returns the status info on the selected component.

Availability
Returns the availability of the current component.

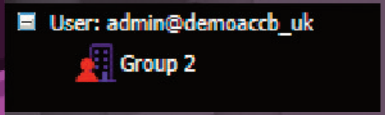
ConfigManagerErrorCode
Returns the ConfigManagerErrorCode of the current component.

Error Description
Details any error message on the current component.

Last Error Code
Returns the last error code of the current component.

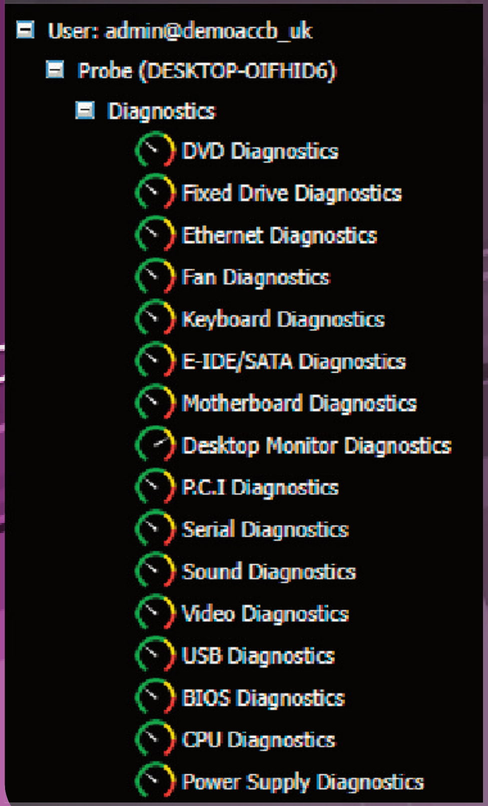


PC, Server, VMware, Hyper-V Diagnostics.
Select the Diagnostics page .
Each time the probe scans the machine, diagnostic data is retrieved for the purpose of pinpointing more accurately where a problem exists.From the Group directory view, select the Group you wish to view.



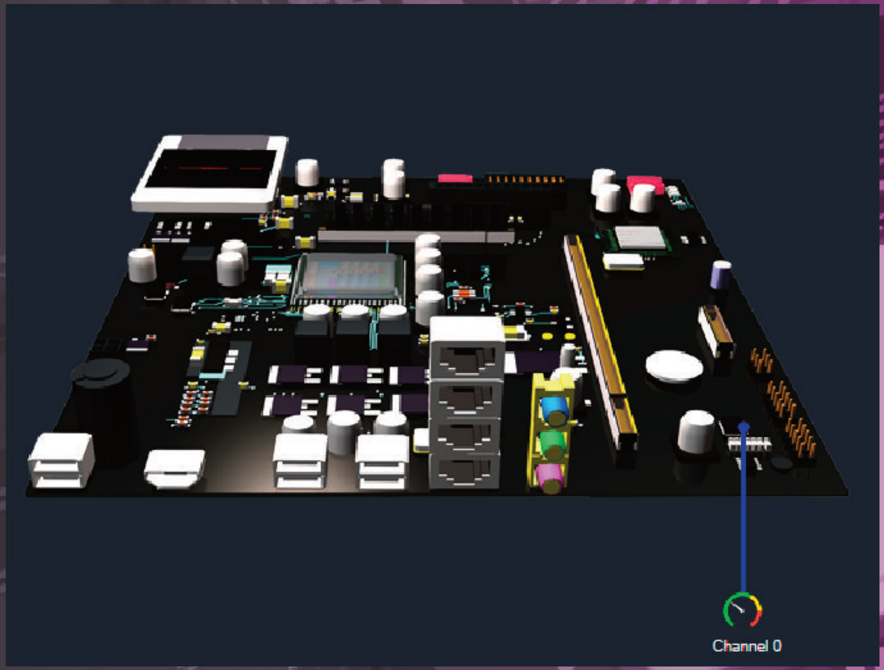
- ⊟ User: admin@demoaccb_uk
  - Group 2

From the probe directory view open the User hierarchical structure to list Console Probes created on the SYVIR EDM cloud.
Select the Console probe you wish to view.



- ⊟ User: admin@demoaccb_uk
  - ⊟ Probe (DESKTOP-OIFHID6)
    - ⊟ Diagnostics
      - DVD Diagnostics
      - Fixed Drive Diagnostics
      - Ethernet Diagnostics
      - Fan Diagnostics
      - Keyboard Diagnostics
      - E-IDE/SATA Diagnostics
      - Motherboard Diagnostics
      - Desktop Monitor Diagnostics
      - P.C.I Diagnostics
      - Serial Diagnostics
      - Sound Diagnostics
      - Video Diagnostics
      - USB Diagnostics
      - BIOS Diagnostics
      - CPU Diagnostics
      - Power Supply Diagnostics

Click on Diagnostics to view the last status of the deployed sensors on that probe.
Sensors dials are color coded to reflect the status of the sensor.
Green = UP.
Where a problem has been detected by the sensor, the dial will indicate Yellow = Warning.
A dial that indicates Red= Down.
Click on a sensor to view channel data for the particular component.



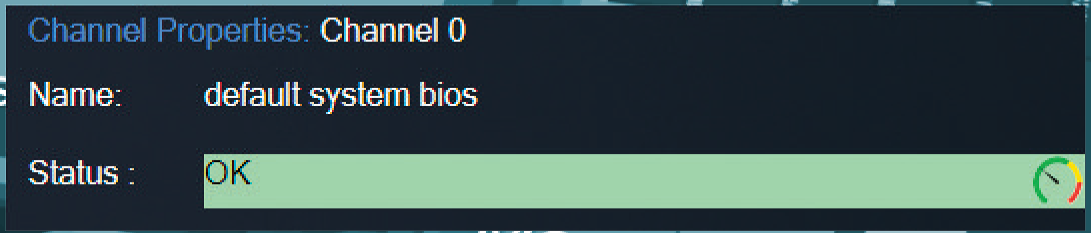
In the system box is a generic pc view, Sensor channels are mapped to the hardware.

Channel.

Click on the channel icons to retrieve properties for the particular channel.
Properties diagnostics are available for each channel.

In some instances data can be basic.
In most instances you should be able to retrieve the Status of the Channel.
Usually this is a generic message of "OK"

A support engineer will require details of any problems found.



Channel Properties: Channel 0

Name: default system bios

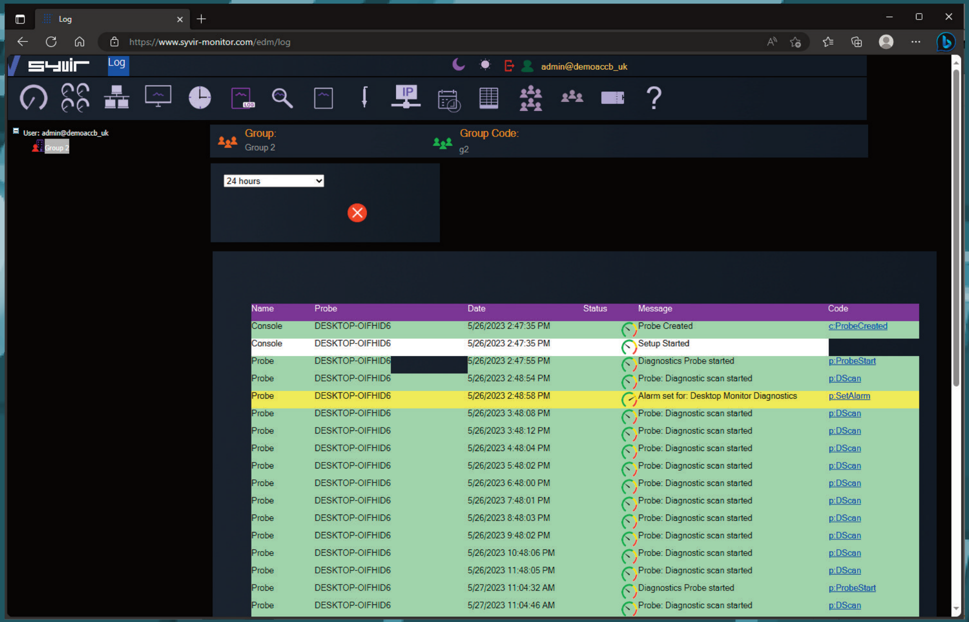
Status : OK

Reporting diagnostic problems.
With EDM its possible to email a front line engineer a report on the problem that is flagged up.
Click on the email icon.
The report shows any problems found with the channels properties diagnostics.
This report can than be emailed.

Log and Reports.

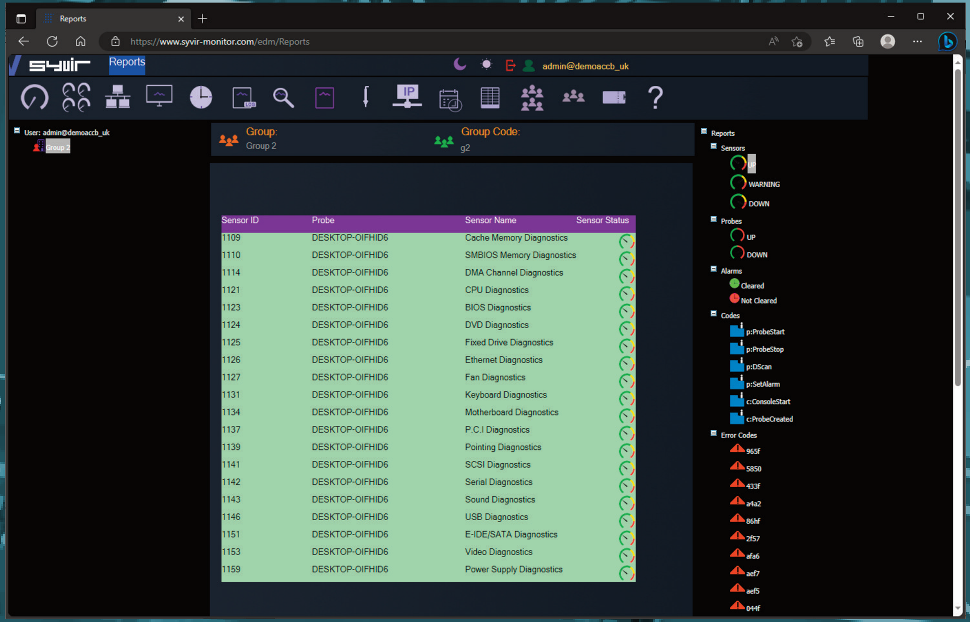
Log messages are produced by the local service probe each time a specific action such as a diagnostic scan is started.
Error messages produced by the local service probe are stored in the edm server.

These messages are accessed through the Log page.
Each log entry provides details of the message and status of the probe.
A code is produced that hyperlink to further details of the log entry.



Name	Probe	Date	Status	Message	Code
Console	DESKTOP-OIFHID6	5/26/2023 2:47:35 PM		Probe Created	c:ProbeCreated
Console	DESKTOP-OIFHID6	5/26/2023 2:47:35 PM		Setup Started	
Probe	DESKTOP-OIFHID6	5/26/2023 2:47:55 PM		Diagnostics Probe started	p:ProbeStart
Probe	DESKTOP-OIFHID6	5/26/2023 2:48:54 PM		Probe: Diagnostic scan started	p:DScan
Probe	DESKTOP-OIFHID6	5/26/2023 2:48:58 PM		Alarm set for: Desktop Monitor Diagnostics	p:SetAlarm
Probe	DESKTOP-OIFHID6	5/26/2023 3:48:08 PM		Probe: Diagnostic scan started	p:DScan
Probe	DESKTOP-OIFHID6	5/26/2023 3:48:12 PM		Probe: Diagnostic scan started	p:DScan
Probe	DESKTOP-OIFHID6	5/26/2023 4:48:04 PM		Probe: Diagnostic scan started	p:DScan
Probe	DESKTOP-OIFHID6	5/26/2023 5:48:02 PM		Probe: Diagnostic scan started	p:DScan
Probe	DESKTOP-OIFHID6	5/26/2023 6:48:00 PM		Probe: Diagnostic scan started	p:DScan
Probe	DESKTOP-OIFHID6	5/26/2023 7:48:01 PM		Probe: Diagnostic scan started	p:DScan
Probe	DESKTOP-OIFHID6	5/26/2023 8:48:03 PM		Probe: Diagnostic scan started	p:DScan
Probe	DESKTOP-OIFHID6	5/26/2023 9:48:02 PM		Probe: Diagnostic scan started	p:DScan
Probe	DESKTOP-OIFHID6	5/26/2023 10:48:06 PM		Probe: Diagnostic scan started	p:DScan
Probe	DESKTOP-OIFHID6	5/26/2023 11:48:05 PM		Probe: Diagnostic scan started	p:DScan
Probe	DESKTOP-OIFHID6	5/27/2023 11:04:32 AM		Diagnostics Probe started	p:ProbeStart
Probe	DESKTOP-OIFHID6	5/27/2023 11:04:46 AM		Probe: Diagnostic scan started	p:DScan

Various reports about your Endpoint sensors and probes, alarms along with codes and error codes.



Sensor ID	Probe	Sensor Name	Sensor Status
1109	DESKTOP-OIFHID6	Cache Memory Diagnostics	
1110	DESKTOP-OIFHID6	SMBIOS Memory Diagnostics	
1114	DESKTOP-OIFHID6	DMA Channel Diagnostics	
1121	DESKTOP-OIFHID6	CPU Diagnostics	
1123	DESKTOP-OIFHID6	BIOS Diagnostics	
1124	DESKTOP-OIFHID6	DVD Diagnostics	
1125	DESKTOP-OIFHID6	Fixed Drive Diagnostics	
1126	DESKTOP-OIFHID6	Ethernet Diagnostics	
1127	DESKTOP-OIFHID6	Fan Diagnostics	
1131	DESKTOP-OIFHID6	Keyboard Diagnostics	
1134	DESKTOP-OIFHID6	Motherboard Diagnostics	
1137	DESKTOP-OIFHID6	P.C.I Diagnostics	
1139	DESKTOP-OIFHID6	Pointing Diagnostics	
1141	DESKTOP-OIFHID6	SCSI Diagnostics	
1142	DESKTOP-OIFHID6	Serial Diagnostics	
1143	DESKTOP-OIFHID6	Sound Diagnostics	
1146	DESKTOP-OIFHID6	USB Diagnostics	
1151	DESKTOP-OIFHID6	E-IDE/SATA Diagnostics	
1153	DESKTOP-OIFHID6	Video Diagnostics	
1159	DESKTOP-OIFHID6	Power Supply Diagnostics	

Tickets.

Tickets by default are produced when a sensor is set to WARNING or DOWN.

Tickets are accessible from the tickets page.

View tickets.
From the Drop-Down box select the period you wish to view Tickets from. Select 24 Hours.
Tickets from the last 24 hours are listed.

Edit a ticket.
Select the ticket by checking the edit checkbox.

Click on the Edit button.
In this mode we have three options.

Ticket
Shows the sensor details when the ticket was created by the probe.

Live
Shows the sensor details from the last scan by the probe.

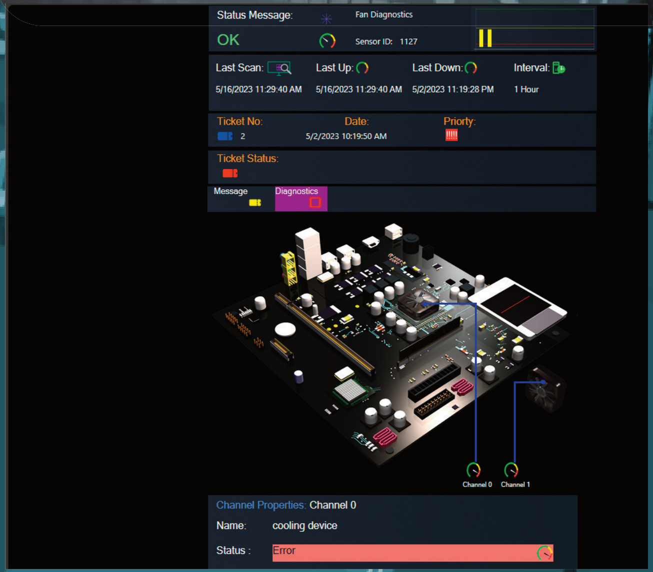
Edit
Edit details such as Priority and Ticket Status.

Priority
By default the probe defines a WARNING status as Priority 4 and DOWN as priority 5.
You can change these by selecting priority Drop-Down box.
Click on Save.

Ticket Status
By default, the probe defines a tickets status as Open, to close a ticket select Closed form the Change status drop down box.

Click on Save.
To view the diagnostic state of the sensor at the time the probe created the ticket. Click on Ticket and Diagnostics.
Click on Channel icons for diagnostic data for each Channel(s)
To view the diagnostic state of the sensor at the last scan by the probe. Click on Live and Diagnostics.
Click on Channel icons for diagnostic data for each Channel(s)

Create your own Tickets.
Select the ticket by checking the edit checkbox.
Click on the New button.
Select the Group and the probe and sensor.
Type in a subject and message.
Click on Save.



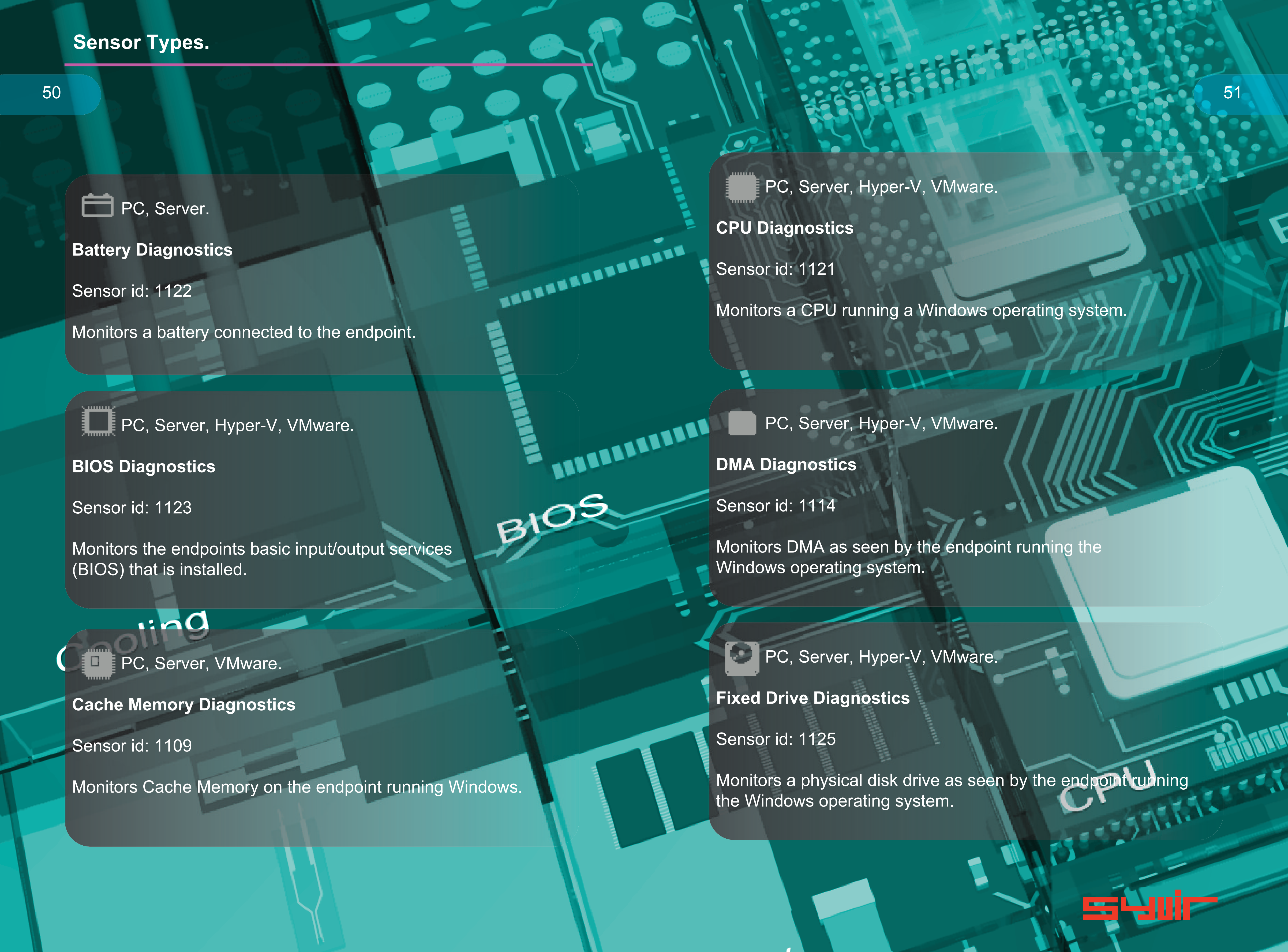
Status Message: Fan Diagnostics
OK Sensor ID: 1127

Last Scan: 5/16/2023 11:29:40 AM
Last Up: 5/16/2023 11:29:40 AM
Last Down: 5/2/2023 11:19:28 PM
Interval: 1 Hour

Ticket No: 2
Date: 5/2/2023 10:19:50 AM
Priorty: !!!!!

Ticket Status:

Channel Properties: Channel 0
Name: cooling device
Status : Error



PC, Server.

Battery Diagnostics

Sensor id: 1122

Monitors a battery connected to the endpoint.

PC, Server, Hyper-V, VMware.

BIOS Diagnostics

Sensor id: 1123

Monitors the endpoints basic input/output services (BIOS) that is installed.

PC, Server, VMware.

Cache Memory Diagnostics

Sensor id: 1109

Monitors Cache Memory on the endpoint running Windows.

PC, Server, Hyper-V, VMware.

CPU Diagnostics

Sensor id: 1121

Monitors a CPU running a Windows operating system.

PC, Server, Hyper-V, VMware.

DMA Diagnostics

Sensor id: 1114

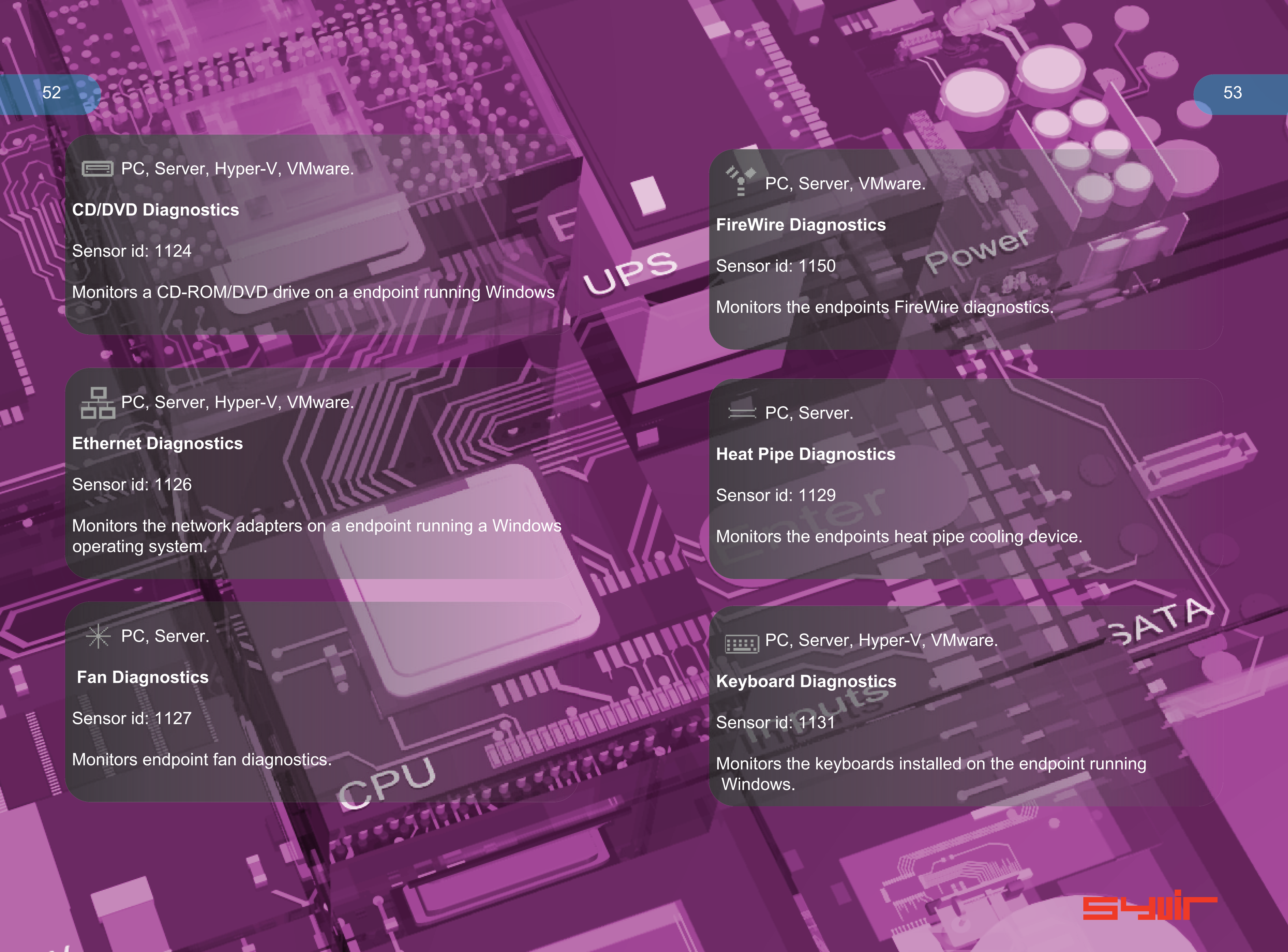
Monitors DMA as seen by the endpoint running the Windows operating system.

PC, Server, Hyper-V, VMware.

Fixed Drive Diagnostics

Sensor id: 1125

Monitors a physical disk drive as seen by the endpoint running the Windows operating system.



PC, Server, Hyper-V, VMware.

CD/DVD Diagnostics

Sensor id: 1124

Monitors a CD-ROM/DVD drive on a endpoint running Windows

PC, Server, Hyper-V, VMware.

Ethernet Diagnostics

Sensor id: 1126

Monitors the network adapters on a endpoint running a Windows operating system.

PC, Server.

Fan Diagnostics

Sensor id: 1127

Monitors endpoint fan diagnostics.

PC, Server, VMware.

FireWire Diagnostics

Sensor id: 1150

Monitors the endpoints FireWire diagnostics.

PC, Server.

Heat Pipe Diagnostics

Sensor id: 1129

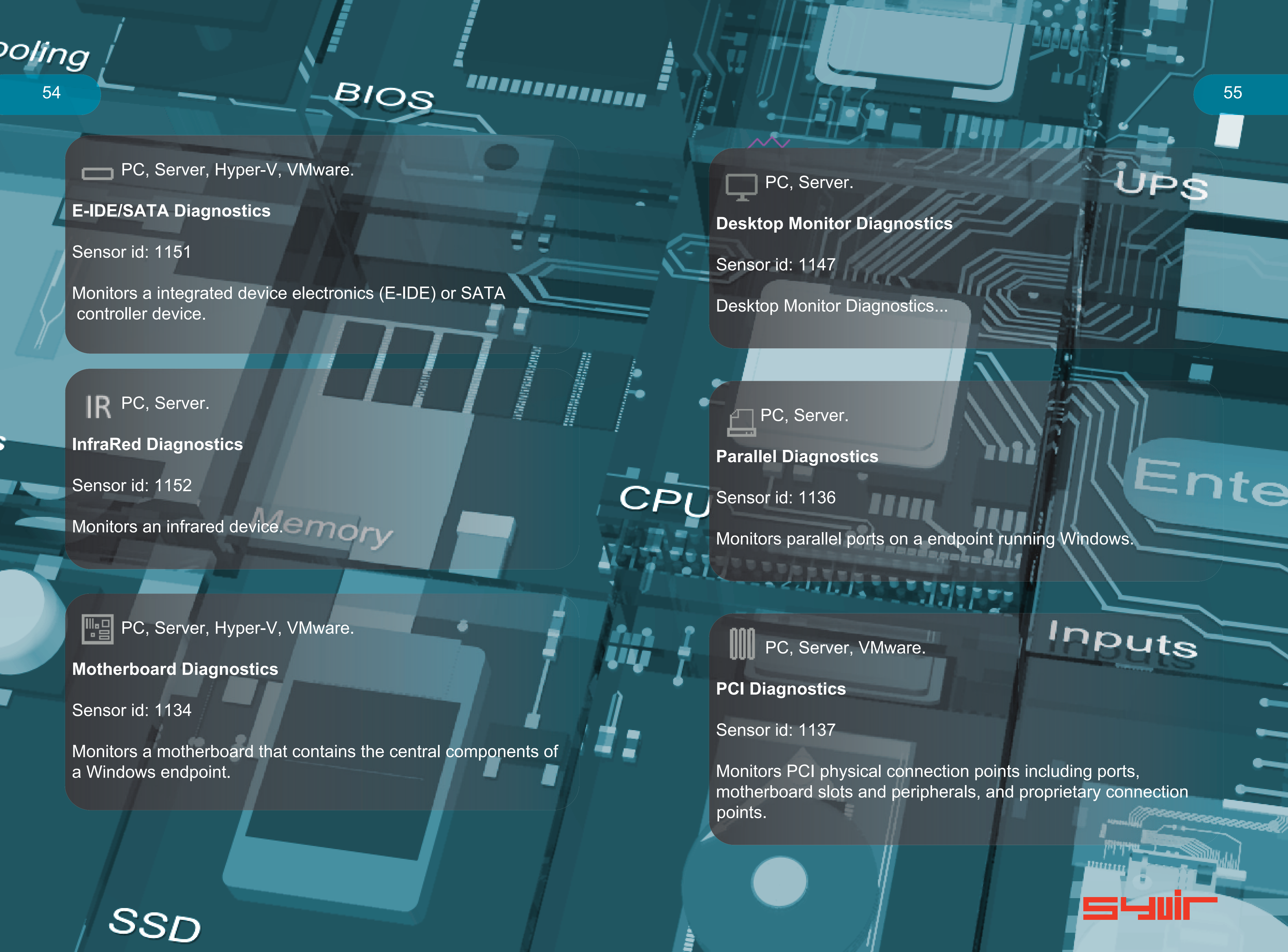
Monitors the endpoints heat pipe cooling device.

PC, Server, Hyper-V, VMware.

Keyboard Diagnostics

Sensor id: 1131

Monitors the keyboards installed on the endpoint running Windows.



PC, Server, Hyper-V, VMware.

E-IDE/SATA Diagnostics

Sensor id: 1151

Monitors a integrated device electronics (E-IDE) or SATA controller device.

IR PC, Server.

InfraRed Diagnostics

Sensor id: 1152

Monitors an infrared device.

PC, Server, Hyper-V, VMware.

Motherboard Diagnostics

Sensor id: 1134

Monitors a motherboard that contains the central components of a Windows endpoint.

PC, Server.

Desktop Monitor Diagnostics

Sensor id: 1147

Desktop Monitor Diagnostics...

PC, Server.

Parallel Diagnostics

Sensor id: 1136

Monitors parallel ports on a endpoint running Windows.

PC, Server, VMware.

PCI Diagnostics

Sensor id: 1137

Monitors PCI physical connection points including ports, motherboard slots and peripherals, and proprietary connection points.

PC, Server.

PCMCIA Diagnostics

Sensor id: 1138

Monitors Personal Computer Memory Card Interface Adapter (PCMCIA of a PC Card) controller device.

PC, Server, Hyper-V, VMware.

PC Pointing Diagnostics
Sensor id: 1139

Monitors input device used to point to and select regions on the display of a endpoint running Windows. Any device used to manipulate a pointer, or point to the display on a endpoint running Windows.

PC, Server, Hyper-V, VMware.

Power Diagnostics

Sensor id: 1159

Monitors the power supply state.

PC, Server.

Refrigeration Diagnostics

Sensor id: 1140

Monitors Refrigeration.

PC, Server, Hyper-V, VMware.

SCSI Diagnostics

Sensor id: 1141

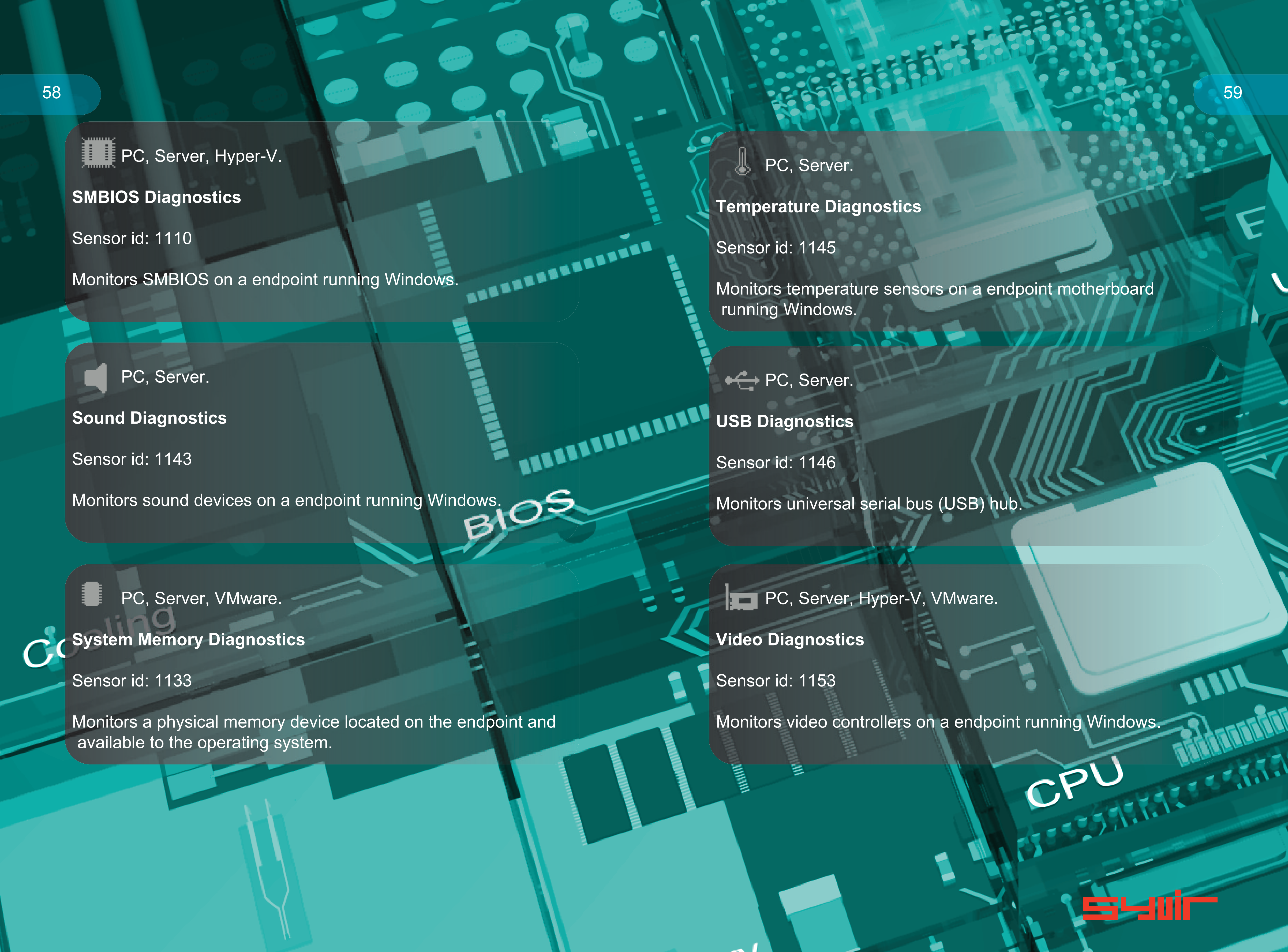
Monitors SCSI on Windows.

PC, Server, Hyper-V.

Serial Diagnostics

Sensor id: 1142

Monitors serial ports on a endpoint running Windows.



PC, Server, Hyper-V.

SMBIOS Diagnostics

Sensor id: 1110

Monitors SMBIOS on a endpoint running Windows.

PC, Server.

Sound Diagnostics

Sensor id: 1143

Monitors sound devices on a endpoint running Windows.

PC, Server, VMware.

System Memory Diagnostics

Sensor id: 1133

Monitors a physical memory device located on the endpoint and available to the operating system.

PC, Server.

Temperature Diagnostics

Sensor id: 1145

Monitors temperature sensors on a endpoint motherboard running Windows.

PC, Server.

USB Diagnostics

Sensor id: 1146

Monitors universal serial bus (USB) hub.

PC, Server, Hyper-V, VMware.

Video Diagnostics

Sensor id: 1153

Monitors video controllers on a endpoint running Windows.

PC, Server.

Voltage Diagnostics

Sensor id: 1112

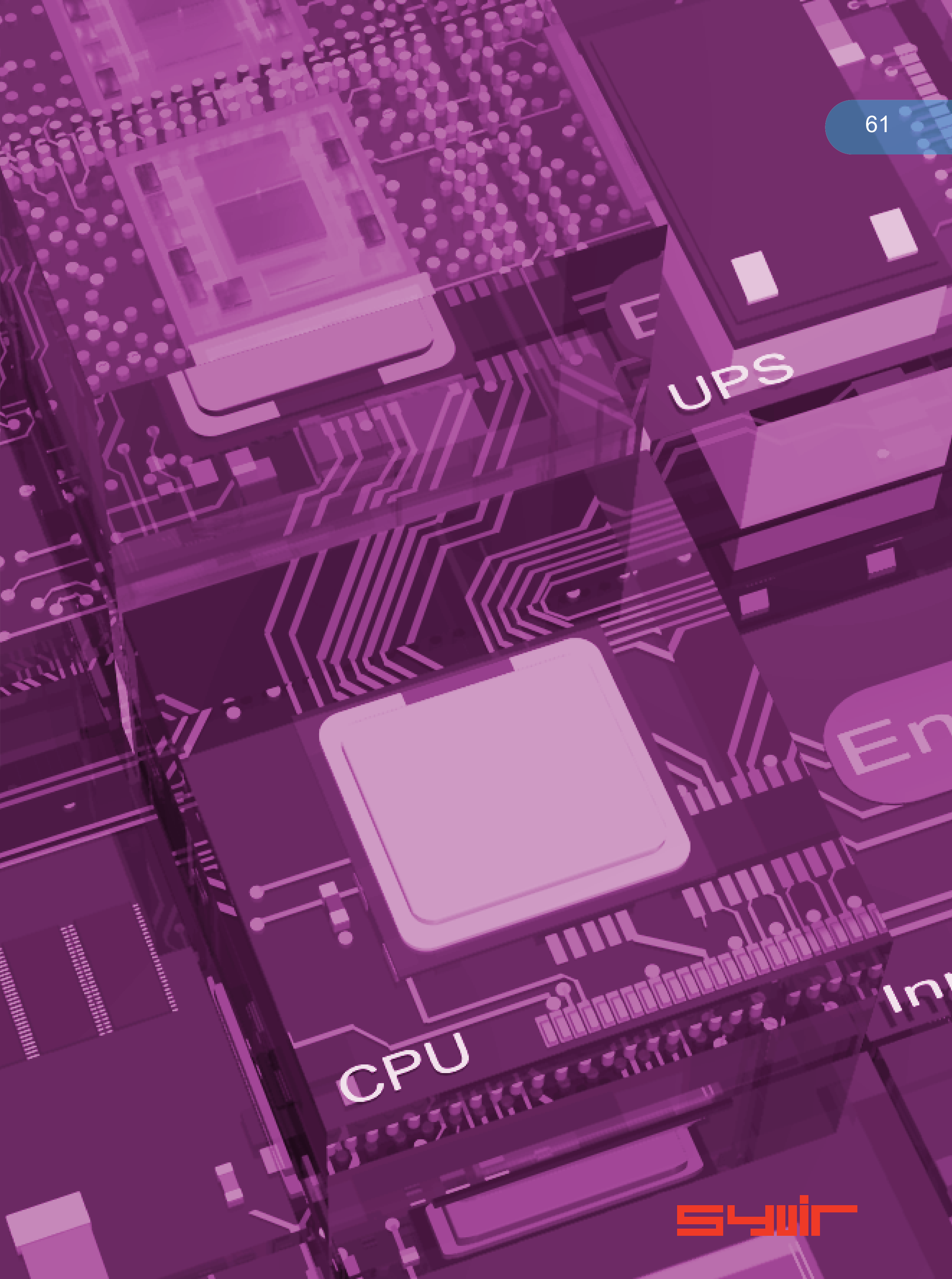
Monitors endpoint Voltage probes on a endpoint running Windows.

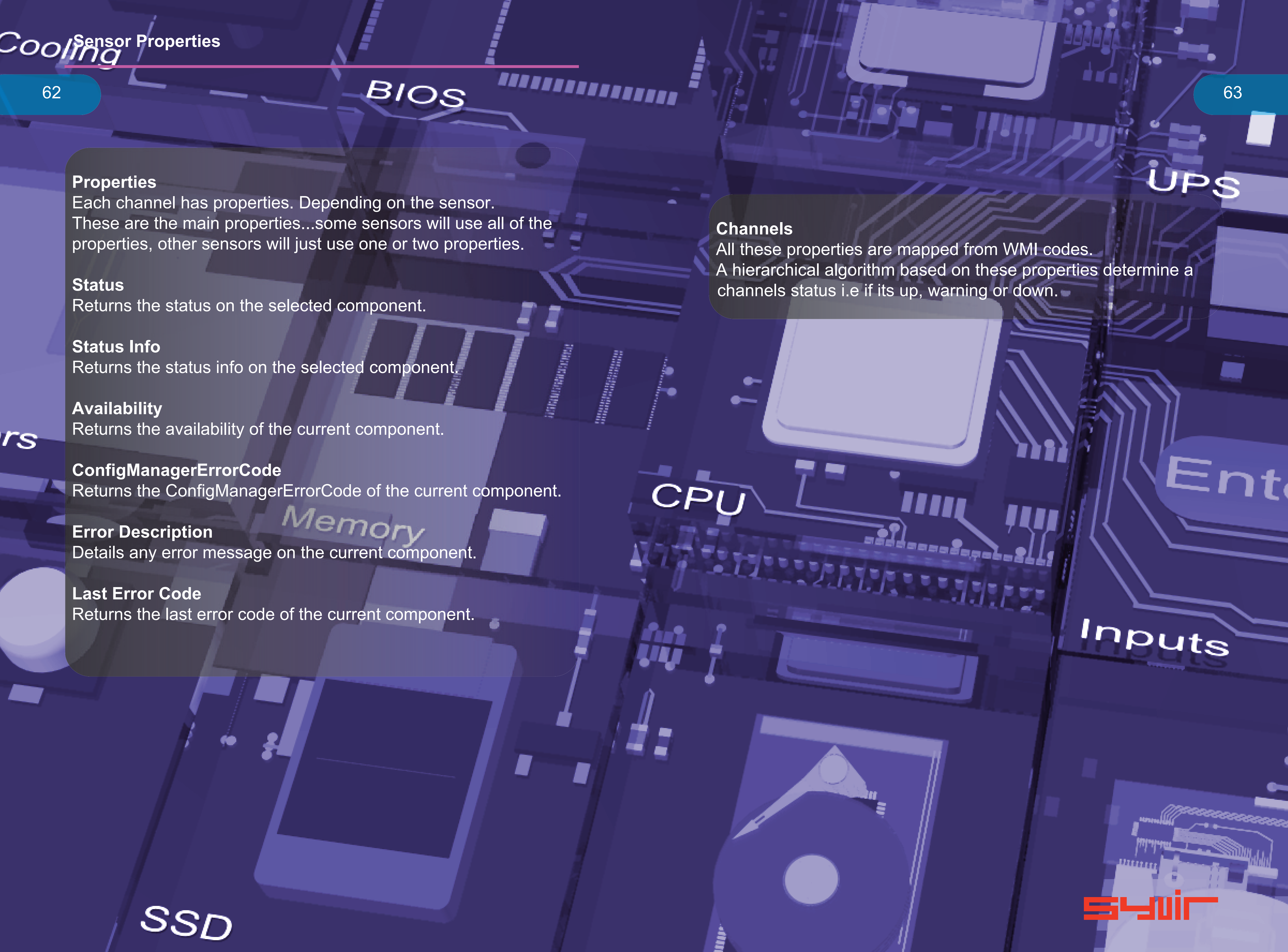
PC, Server.

Wireless Diagnostics

Sensor id: 1154

Monitors wireless diagnostics.





Properties
Each channel has properties. Depending on the sensor.
These are the main properties...some sensors will use all of the properties, other sensors will just use one or two properties.

Status
Returns the status on the selected component.

Status Info
Returns the status info on the selected component.

Availability
Returns the availability of the current component.

ConfigManagerErrorCode
Returns the ConfigManagerErrorCode of the current component.

Error Description
Details any error message on the current component.

Last Error Code
Returns the last error code of the current component.

Channels
All these properties are mapped from WMI codes.
A hierarchical algorithm based on these properties determine a channels status i.e if its up, warning or down.

Battery Diagnostics

Sensor id: 1122
Status. Status Info. Availability.ConfigManagerErrorCode.
Error Description. Last Error Code.

BIOS Diagnostics

Sensor id: 1123

Status.

Cache Memory Diagnostics

Sensor id: 1109

Status. Status Info. Availability.ConfigManagerErrorCode.
Error Description. Last Error Code.

CPU Diagnostics

Sensor id: 1121

Status. Status Info. Availability.ConfigManagerErrorCode.
Error Description. Last Error Code.

DMA Diagnostics

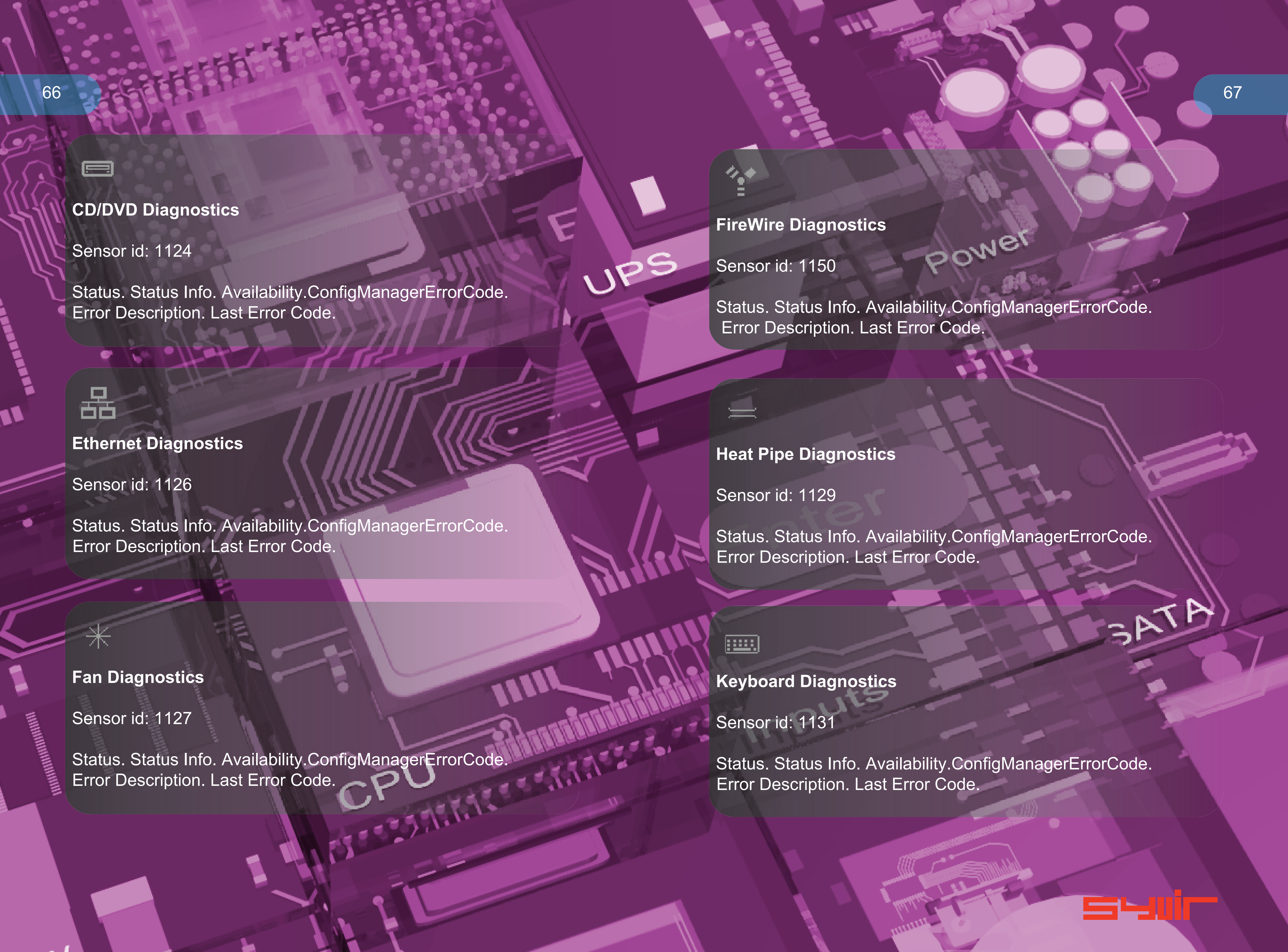
Sensor id: 1114

Status.

Fixed Drive Diagnostics

Sensor id: 1125

Status. Status Info. Availability.ConfigManagerErrorCode.
Error Description. Last Error Code.



CD/DVD Diagnostics

Sensor id: 1124

Status. Status Info. Availability.ConfigManagerErrorCode. Error Description. Last Error Code.

Ethernet Diagnostics

Sensor id: 1126

Status. Status Info. Availability.ConfigManagerErrorCode. Error Description. Last Error Code.

Fan Diagnostics

Sensor id: 1127

Status. Status Info. Availability.ConfigManagerErrorCode. Error Description. Last Error Code.

FireWire Diagnostics

Sensor id: 1150

Status. Status Info. Availability.ConfigManagerErrorCode. Error Description. Last Error Code.

Heat Pipe Diagnostics

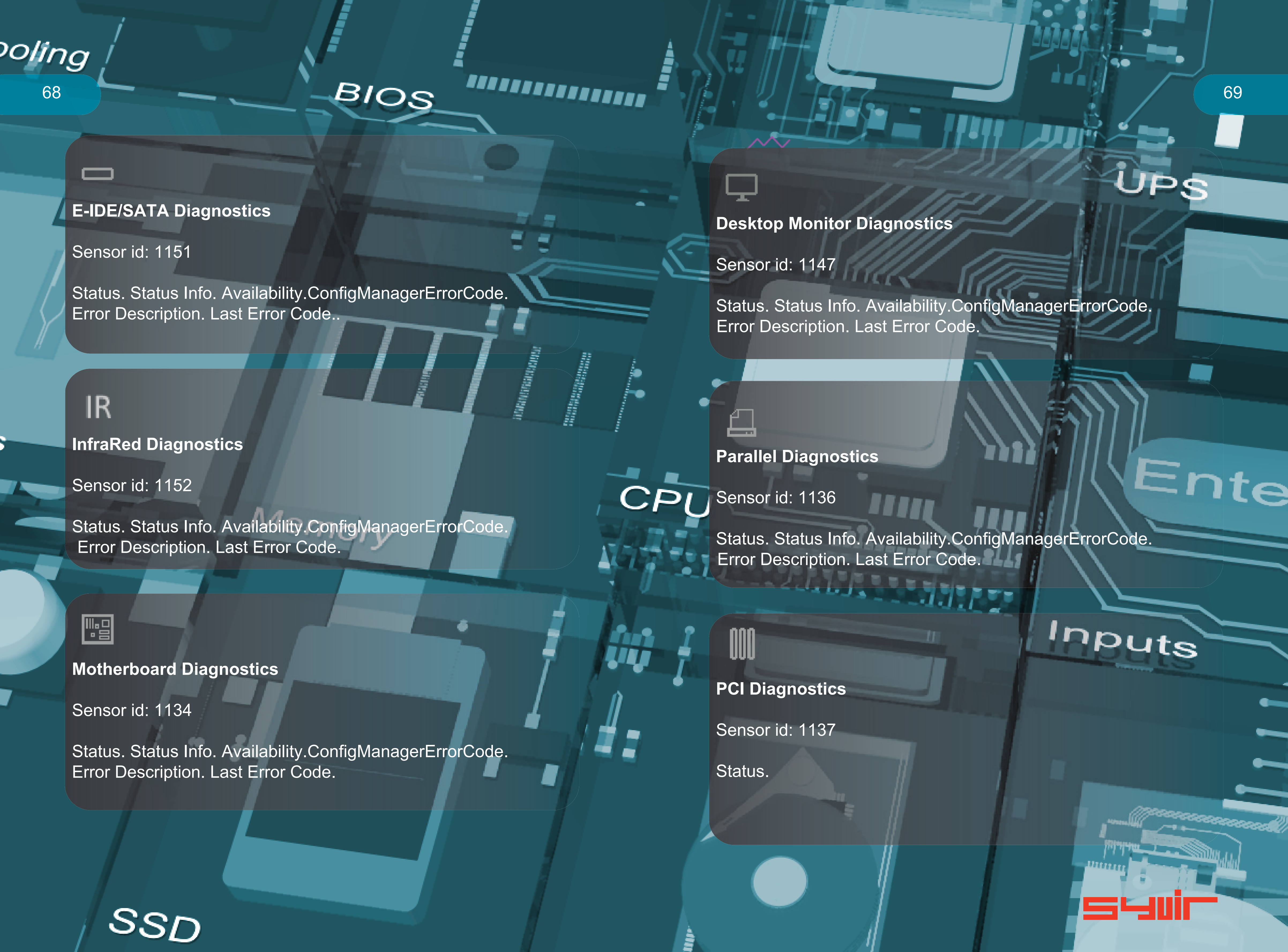
Sensor id: 1129

Status. Status Info. Availability.ConfigManagerErrorCode. Error Description. Last Error Code.

Keyboard Diagnostics

Sensor id: 1131

Status. Status Info. Availability.ConfigManagerErrorCode. Error Description. Last Error Code.



E-IDE/SATA Diagnostics

Sensor id: 1151

Status. Status Info. Availability.ConfigManagerErrorCode. Error Description. Last Error Code..

InfraRed Diagnostics

Sensor id: 1152

Status. Status Info. Availability.ConfigManagerErrorCode. Error Description. Last Error Code.

Motherboard Diagnostics

Sensor id: 1134

Status. Status Info. Availability.ConfigManagerErrorCode. Error Description. Last Error Code.

Desktop Monitor Diagnostics

Sensor id: 1147

Status. Status Info. Availability.ConfigManagerErrorCode. Error Description. Last Error Code.

Parallel Diagnostics

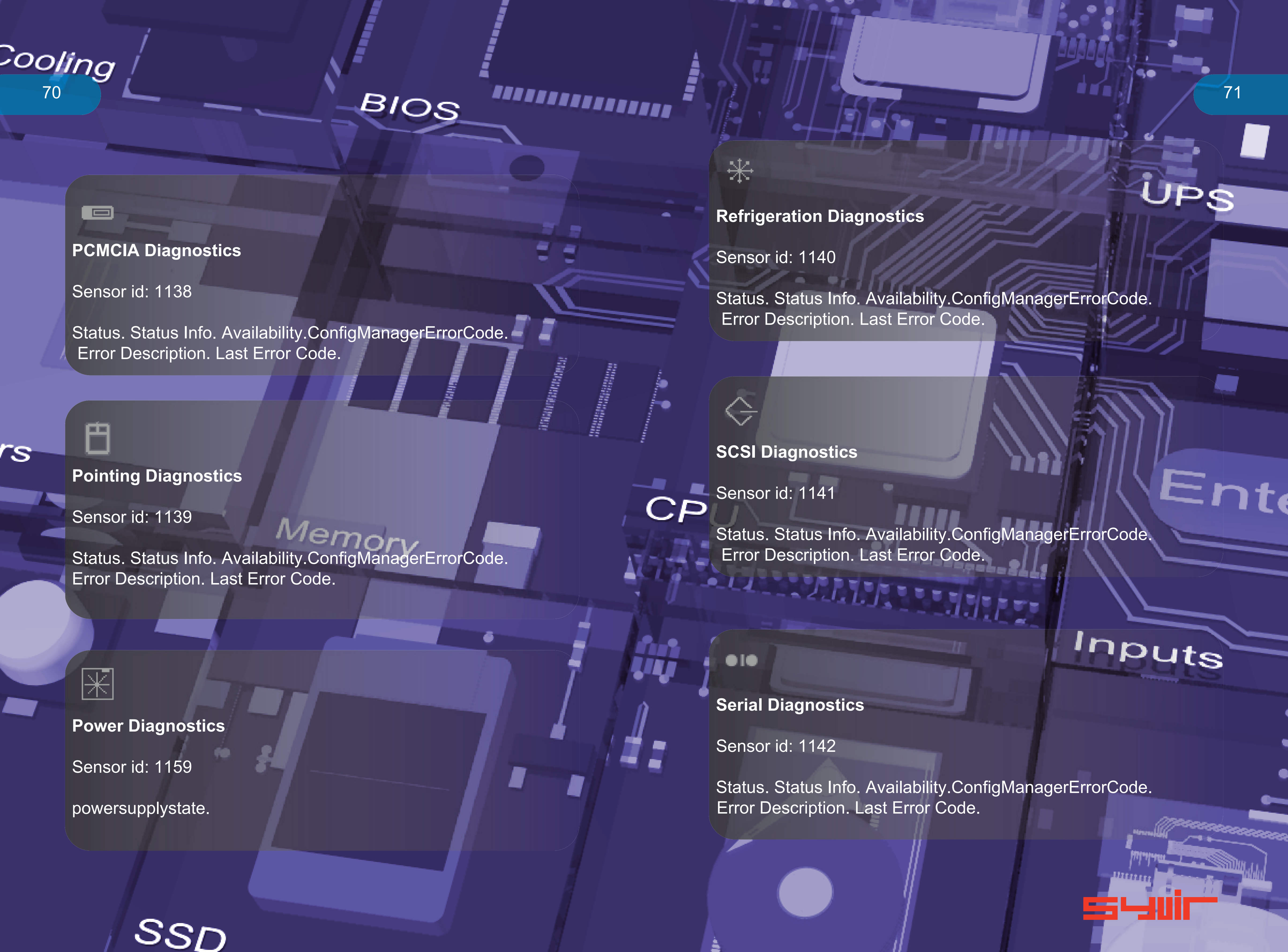
Sensor id: 1136

Status. Status Info. Availability.ConfigManagerErrorCode. Error Description. Last Error Code.

PCI Diagnostics

Sensor id: 1137

Status.



PCMCIA Diagnostics

Sensor id: 1138

Status. Status Info. Availability.ConfigManagerErrorCode.
Error Description. Last Error Code.

Pointing Diagnostics

Sensor id: 1139

Status. Status Info. Availability.ConfigManagerErrorCode.
Error Description. Last Error Code.

Power Diagnostics

Sensor id: 1159

powersupplystate.

Refrigeration Diagnostics

Sensor id: 1140

Status. Status Info. Availability.ConfigManagerErrorCode.
Error Description. Last Error Code.

SCSI Diagnostics

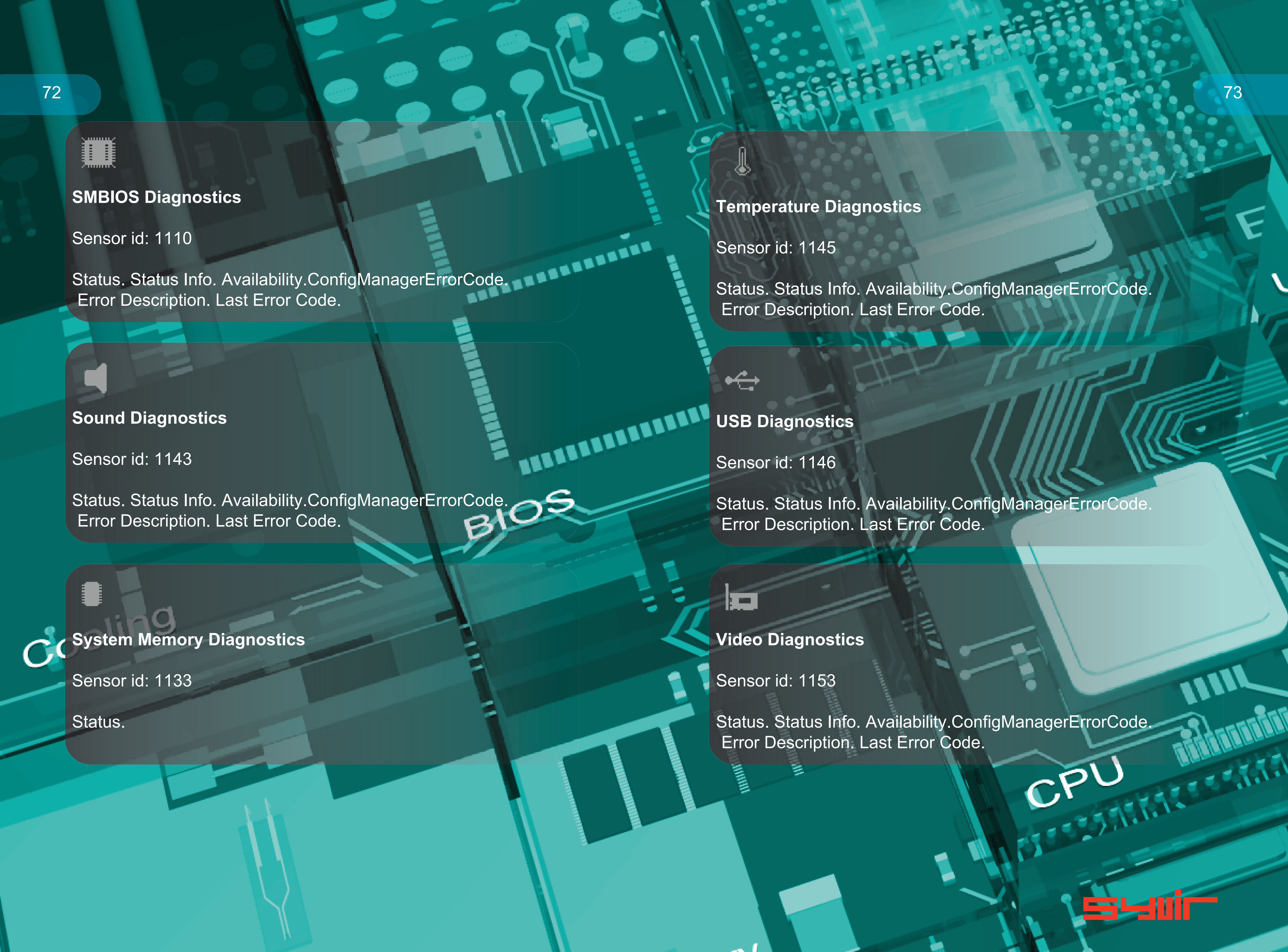
Sensor id: 1141

Status. Status Info. Availability.ConfigManagerErrorCode.
Error Description. Last Error Code.

Serial Diagnostics

Sensor id: 1142

Status. Status Info. Availability.ConfigManagerErrorCode.
Error Description. Last Error Code.



SMBIOS Diagnostics

Sensor id: 1110

Status. Status Info. Availability.ConfigManagerErrorCode. Error Description. Last Error Code.

Sound Diagnostics

Sensor id: 1143

Status. Status Info. Availability.ConfigManagerErrorCode. Error Description. Last Error Code.

System Memory Diagnostics

Sensor id: 1133

Status.

Temperature Diagnostics

Sensor id: 1145

Status. Status Info. Availability.ConfigManagerErrorCode. Error Description. Last Error Code.

USB Diagnostics

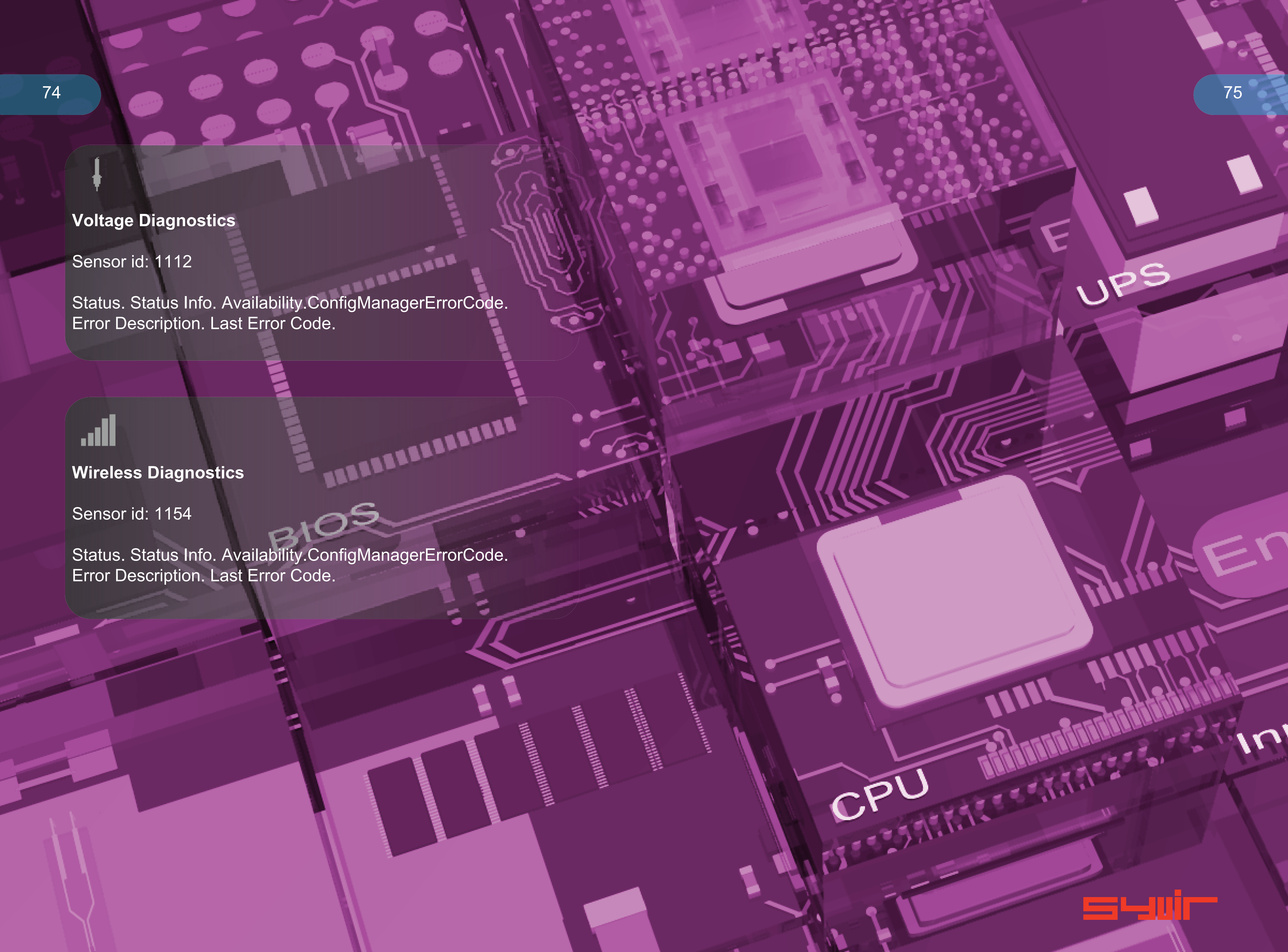
Sensor id: 1146

Status. Status Info. Availability.ConfigManagerErrorCode. Error Description. Last Error Code.

Video Diagnostics

Sensor id: 1153

Status. Status Info. Availability.ConfigManagerErrorCode. Error Description. Last Error Code.



Voltage Diagnostics

Sensor id: 1112

Status. Status Info. Availability.ConfigManagerErrorCode. Error Description. Last Error Code.

Wireless Diagnostics

Sensor id: 1154

Status. Status Info. Availability.ConfigManagerErrorCode. Error Description. Last Error Code.

Status.

ok
The device is functioning ok.

error
The device has produced an error.

degraded
The device has been degraded.

unknown
The status of the device is unknown. This doesn’t mean a failure, just the status is unknown of the device.

pred fail
The device is predicted to fail.

starting
The device is starting.

stopping
The device is stopping. This doesn’t mean a failure, just the device is stopping.

service

stressed
The device is stressed.

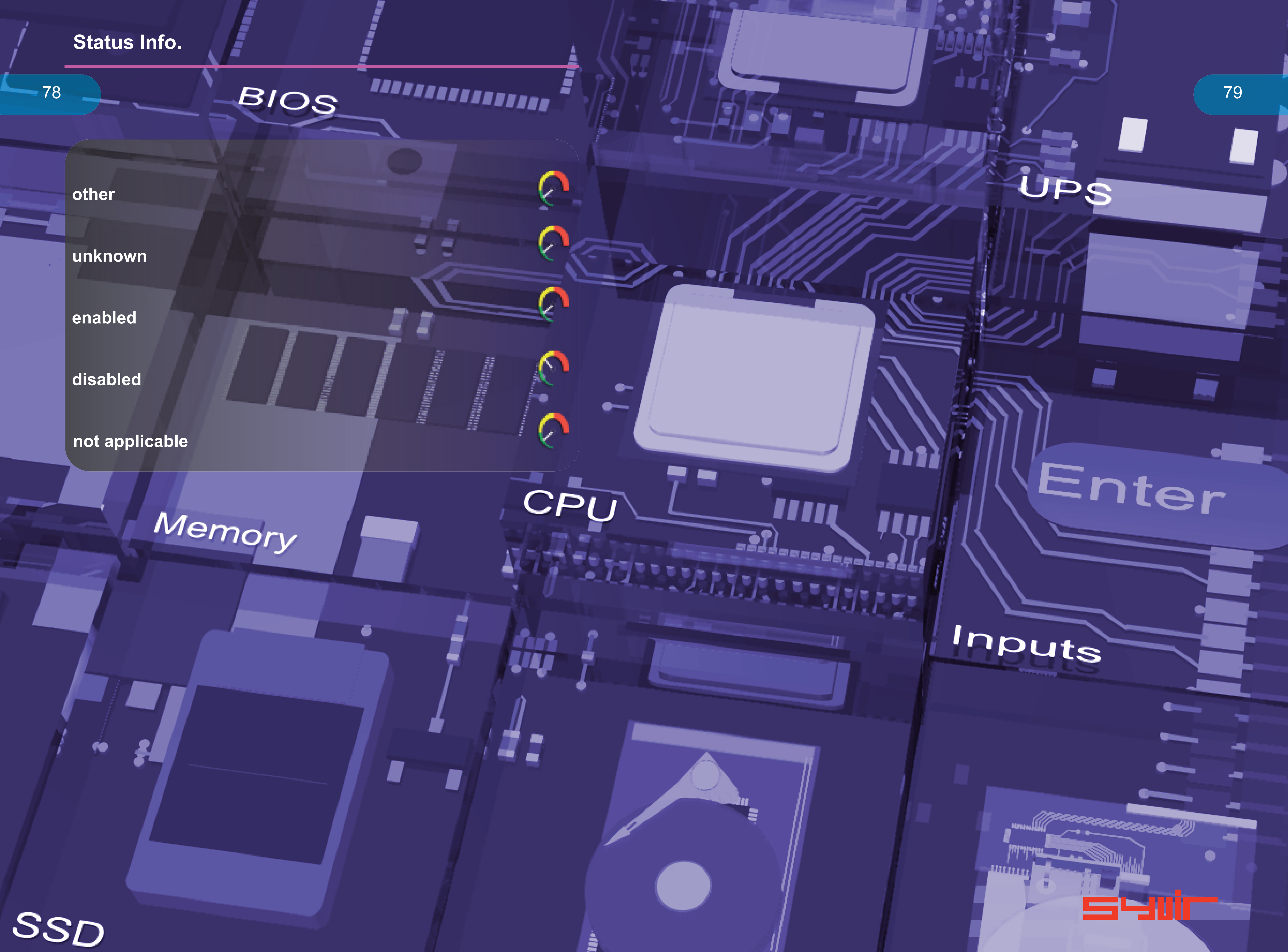
nonrecover
The device is non recoverable.

no contact
There is no contact with the device. This doesn’t mean a failure, just that there is no contact with the device.

lost comm
Communication with the component has been lost. This doesn’t mean a failure, just that there is no contact with the device.

Status Info.

- other
- unknown
- enabled
- disabled
- not applicable



ConfigManagerErrorCode

Device is working properly.
The device is working and functioning properly.

Device is not configured correctly.
The device is not configured correctly.

Windows cannot load the driver for this device

The driver for this device might be corrupted, or your system may be running low on memory or other resources.

This device is not working properly.
One of its drivers or your registry might be corrupted.

The driver for this device needs a resource that Windows cannot manage.

The boot configuration for this device conflicts with other devices.

Cannot filter.

The driver loader for the device is missing.

This device is not working properly because the controlling firmware is reporting the resources for the device incorrectly.

Device cannot start.

Device failed.

Device cannot find enough free resources that it can use.

Windows cannot verify this device's resources.

Device cannot work properly until the computer is restarted.

Device is not working properly due to a possible re-enumeration problem.

Windows cannot identify all of the resources that the device uses.

Device is requesting an unknown resource type.

Device drivers must be reinstalled.

Failure using the VxD loader.

Your registry might be corrupted.

System failure: Try changing the driver for this device.
If that does not work, see your hardware documentation.
Windows is removing this device

This device is disabled.

System failure. If changing the device driver is ineffective, see the hardware documentation.

Device is not present, not working properly, or does not have all of its drivers installed.

Windows is still setting up the device.

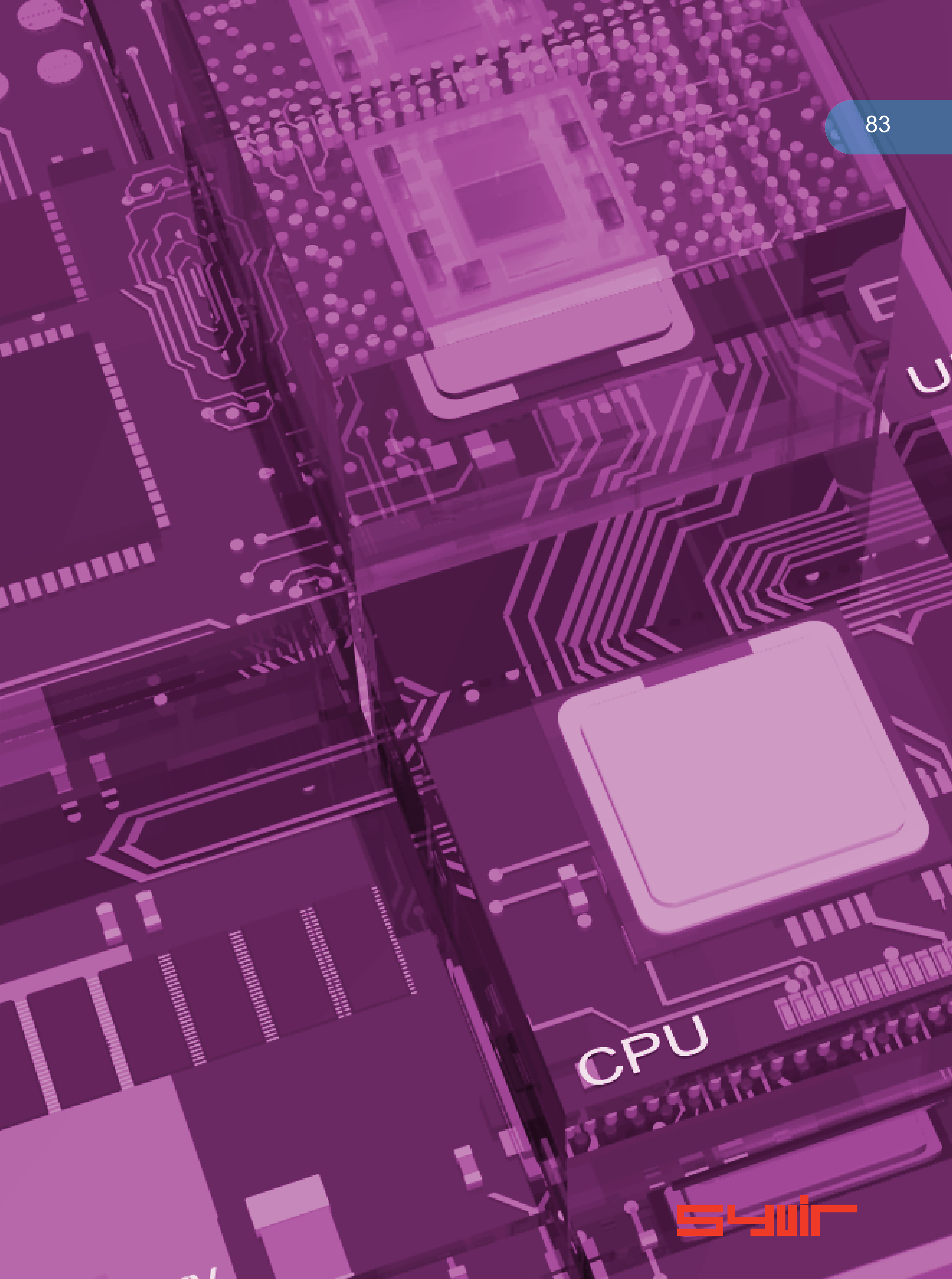
Device does not have valid log configuration.

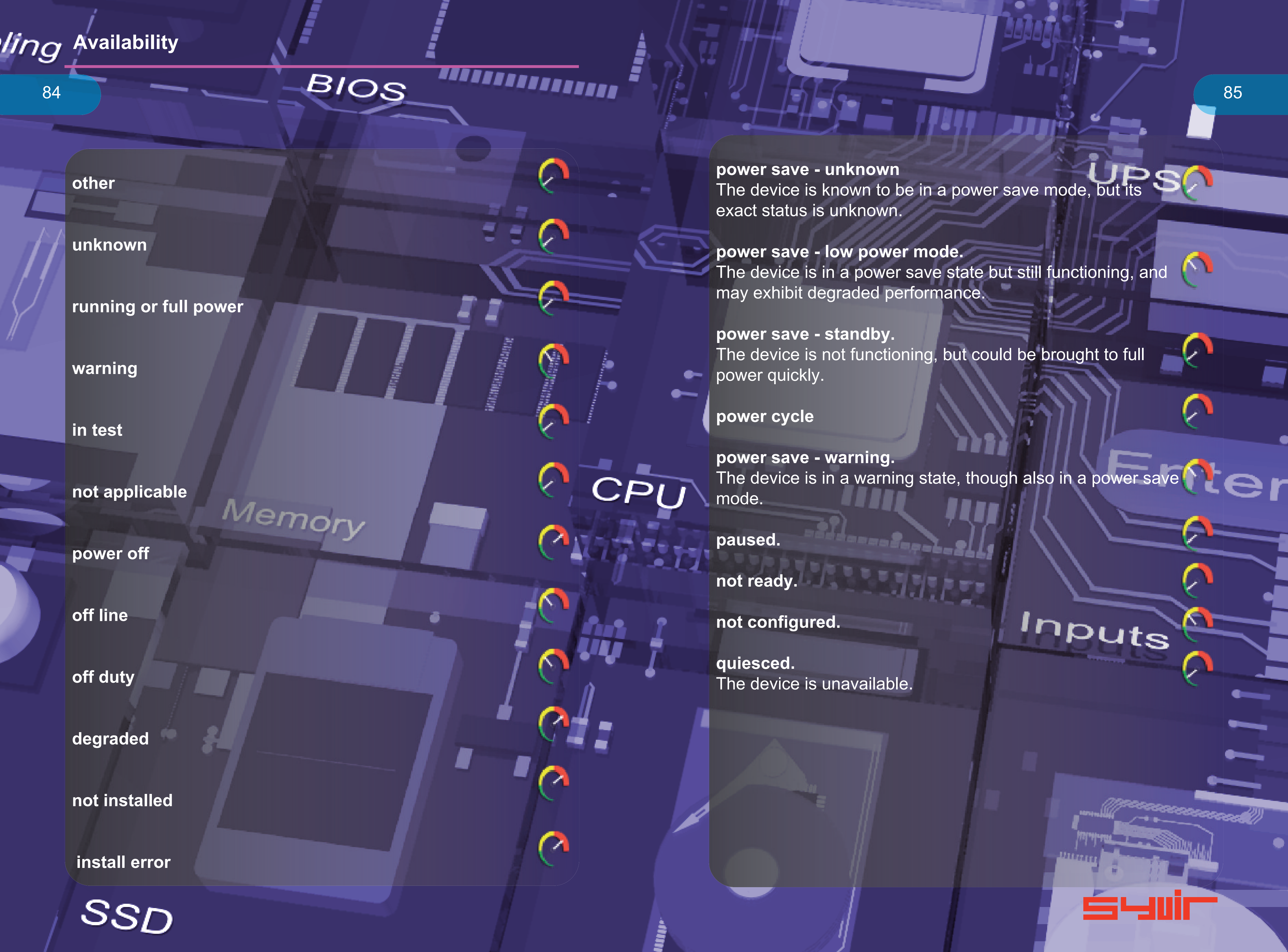
Device drivers are not installed.

Device is disabled. The device firmware did not provide the required resources.

Device is using an IRQ resource that another device is using.

Device is not working properly. Windows cannot load the required device drivers.





other

unknown

running or full power

warning

in test

not applicable

power off

off line

off duty

degraded

not installed

install error

power save - unknown
The device is known to be in a power save mode, but its exact status is unknown.

power save - low power mode.
The device is in a power save state but still functioning, and may exhibit degraded performance.

power save - standby.
The device is not functioning, but could be brought to full power quickly.

power cycle

power save - warning.
The device is in a warning state, though also in a power save mode.

paused.

not ready.

not configured.

quiesced.
The device is unavailable.

PowerSupplyState

other

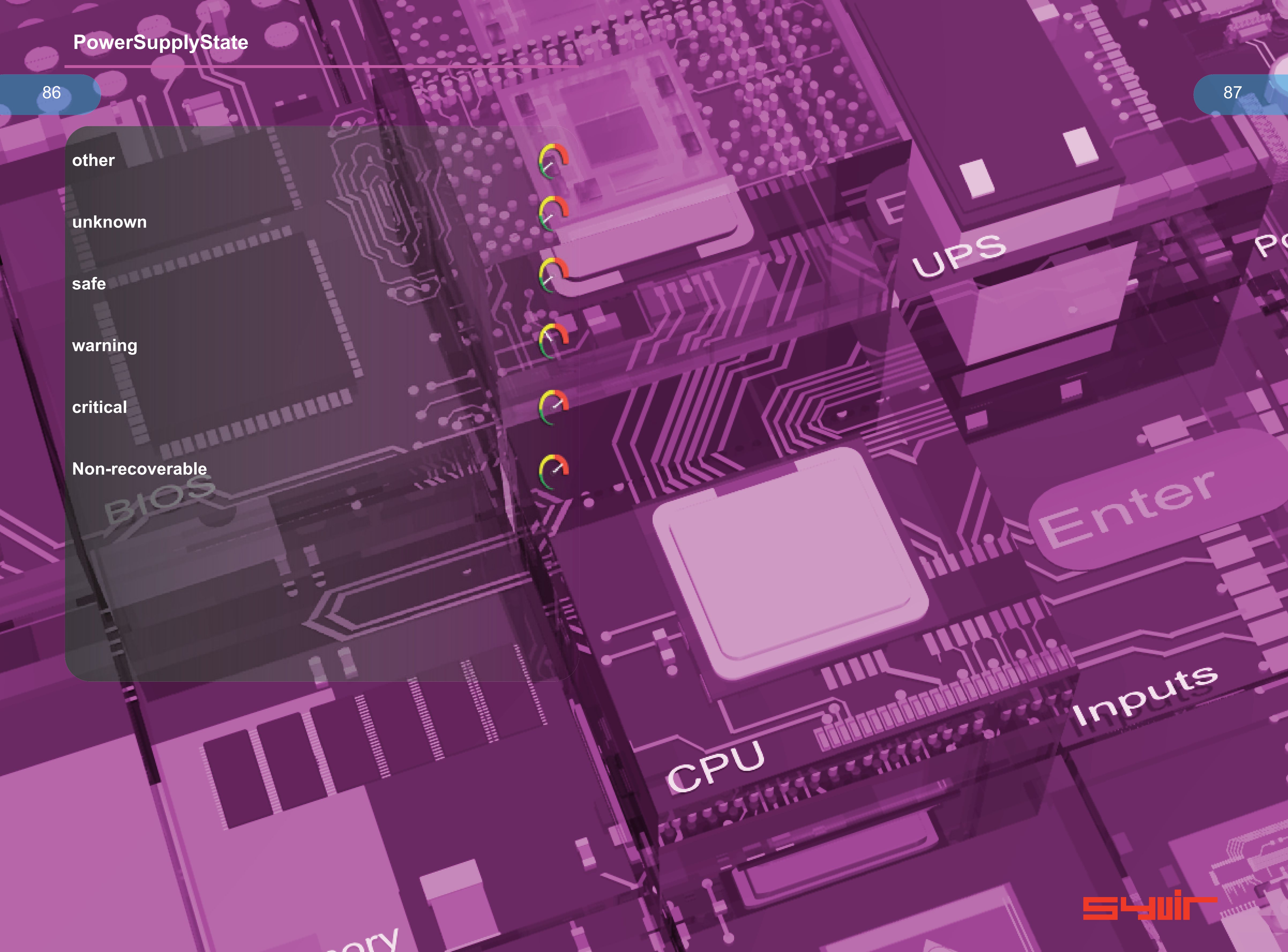
unknown

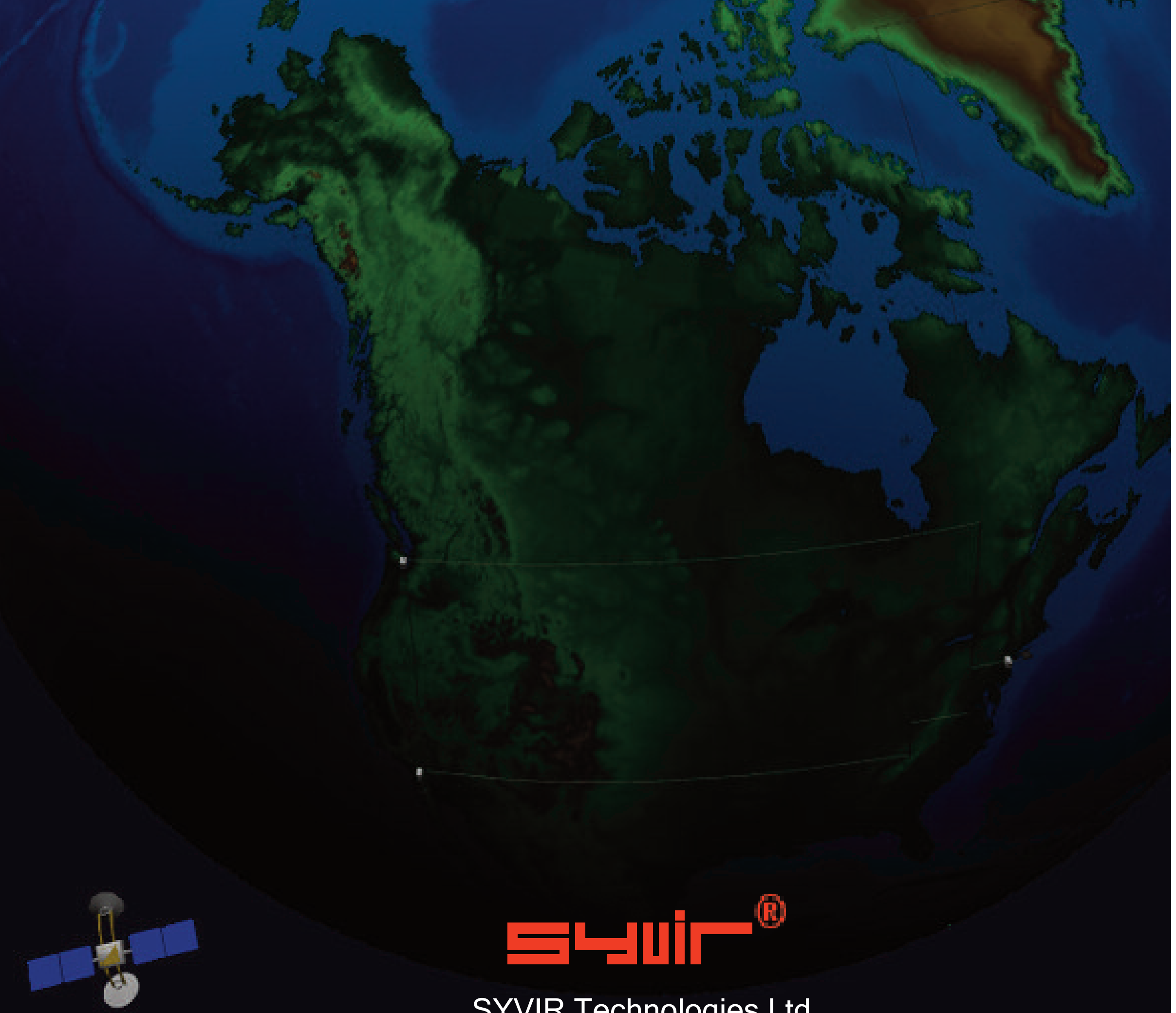
safe

warning

critical

Non-recoverable





SYVIR Technologies Ltd
184 Cambridge Science Park
Cambridge
CB4 0GA
U.K

sales@syvir.com

WWW.SYVIR.COM