PROCENTEC

Member of the HMS group.

Osiris

User manual V1.1.127
Atlas, Atlas2 Plus, Atlas2, Mercury and Osiris SaaS

Safety Guidelines

This manual contains notices which you should observe to ensure your own personal safety, as well as to protect the product and connected equipment. These notices are highlighted in the manual by a warning sign and are marked as followed according to the level of danger:

Draws your attention to important information on handling the product, a particular part of the documentation or the correct functioning of the product.

Warning

This device and its components may only be used for the applications described in this manual and only in connection with devices or components that comply with Industrial Ethernet interfaces.
This product can only function correctly and safely if it is transported, stored, set up, installed, operated and maintained as recommended. Atlas and/ or Mercury is a CE class A product. In a domestic environment it may cause radio interference in which case the user may be required to take adequate measures.

Warranty

Warranty is void if you open Atlas and/or Mercury.

Qualified Technicians

Only qualified technicians should be allowed to install and work with this equipment. Qualified technicians are defined as persons who are authorized to commission, to ground, to tag circuits and systems in accordance with established safety practices and standards. It is recommended that the technicians carry a Certified PROFINET Installer or Certified PROFINET Engineer certificate.

Disclaimer of Liability

We have checked the contents of this manual as much as possible. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the content in this manual is reviewed regularly and necessary corrections will be included in subsequent editions. Suggestions for improvements are welcome.

Important information

Purpose of the Manual

This user manual provides information how to work with Osiris on Atlas, Mercury and/or PC.

This manual does not describe the usage of the tablet itself. For the manual of the tablet, refer to the manual of FZ-M1 on the Panasonic website.

Support

In case of a defective product or unanswered questions, get in contact with the support department:

T: +31 (0)174 671 800
F: +31 (0)174 671 801
E: support@procentec.com

Recycling and Disposal

The parts of the Mercury can be recycled.

"WARNING, BATTERY INSIDE; Battery may explode if mistreated. Do not disassemble or dispose of in fire. Dispose product according to the instructions"

For further information about environment-friendly recycling and the procedure for the disposing of your old equipment, contact:

PROCENTEC
Vlasmarkt 1
3011 PW, ROTTERDAM
The Netherlands

T: +31 (0)174 671 800
F: +31 (0)174 671 801
E: info@procentec.com

Document Updates

You can obtain constantly updated information on PROCENTEC products on the Internet at www.procentec.com

Table of contents

1. Product description

1.1 Introduction

PROCENTEC's Osiris on Atlas, Atlas2, Atlas2 Plus, Mercury and PC is the solution for monitoring and diagnosing Ethernet networks, where innovative simplicity and predictive capabilities are desired. The tool is perfect for preventing unexpected and expensive downtime within PROFIBUS, PROFINET and industrial Ethernet networks.

PROCENTEC's Osiris provides unique insight in your network's health and topology. With PROCENTEC Osiris operators and engineers can easily detect problems and find their causes within your network. This prevents costly down times.

The ease of use and clear overview makes this an ideal solution for the complete understanding of networks, always and anywhere. The Atlas family is a set of compact devices that can be installed on a DIN rail and plugged in to the network for permanent network monitoring, and Mercury is the portable version. Osiris does not require additional and time-consuming software installations on the PC. You can get all the information using a custom designed web application. All the information Osiris provides can be viewed on the central, customizable dashboard page.

1.2 Your benefits

- Ease of use
- Use of Industrial Ethernet
- Topology
- Standalone device, 24/7 available
- Safe use
- Customizable dashboard
- Resistant to all environmental factors
- No software required

1.3 Product features

- Network Topology
- Customizable dashboard
- Network Quality Factor
- Alarms
- Not vendor or protocol specific

1.4 System requirements

Osiris runs on any browser-enabled computer; the interface is fully web based.
HTML5 and JavaScript must be supported by the browser.
The minimum version requirements for web browsers are:
- Chrome   version 46 or higher
- Edge   version 25 or higher
- Firefox   version 42 or higher
- Safari   version 5 or higher

For optimal experience it is recommended to use Chrome. Internet Explorer versions are not supported.

2. Getting started: Atlas

2.1 Quick Start

This checklist describes all the steps to a quick usage of Atlas, Atlas2 Plus or Atlas2.

Step: Instructions:

STEP 1   Install the device on a DIN rail.

STEP 2   Use an Ethernet cable to connect the Office port to your laptop directly and
              the Factory port to the factory network.
              The Factory port should NOT be connected to a mirror port of a switch.

STEP 3   Connect the Atlas to a power supply.
              Wait until you see the Network Status / traffic light blink yellow.

STEP 4   Set your laptops IP address to 192.168.1.1 and the netmask to
              255.255.255.0.

STEP 5   Open a web browser and go to https://192.168.1.10/. You will receive a
              warning about the certificate:
              - Chrome users should click 'ADVANCED' followed by 'Proceed ..'
              - Edge users should click 'Continue to this website ..'

STEP 6   Enter user 'admin' and password 'admin' for the first login.

STEP 7   Now complete the Setup Wizard (see chapter 5) but do not change the settings
              of the Office port yet.

STEP 8   Lastly, setup the Office port in the Settings, unplug your laptop and connect
              the Office port to the office network.

The Atlas is now operational. From here you can change settings, layout and behavior, described in .
of the Atlas. If connected to a factory network, it will start scanning and gathering information.

2.2   Atlas installation instructions

2.2.1   Location

Atlas can be installed anywhere in a non-hazardous / non-Ex area that complies with IP 20 (DIN 40 050) and the specified temperature range of -20° to +60° Celsius. Do not install the Atlas in a humid or dusty environment. To comply with UL certification regulations, in ambient temperatures higher than 55°C or 131°F it is mandatory to install the Atlas in an industrial installation cabinet with the "HOT HOUSING" warning label visible during operation.

"WARNING, HOT HOUSING. When in use at an ambient temperature higher than 55ºC or 131ºF, the housing of the Atlas will be hot. Do not touch the housing!"

To comply with UL certification regulations the Atlas is to be used at altitudes not exceeding 2000m and in non-tropical climate regions only.

2.2.2 Position

Atlas, Atlas2 and Atlas2 Plus can only be installed on a horizontal 35mm DIN rail with the front plates facing forward (see Figure 1 and Figure 2 for an example). In this position the generated heat of the module can escape through the grid in the top of the housing. It is also easier to read the status LEDs. Do not install the Atlas in any other position, this could lead to overheating of the device.

2.2.3 Power supply

The Atlas and Atlas2 contain a 3-pin screw type power connector on the front.

The layout is as follows:
1 = - (upper pin)

2 = + (middle pin)

3 = SH (lower pin)

Figure 1 - Atlas mounted on a 35mm DIN

The power supply must comply with the following specifications:

- Voltage: 12 .. 24 VDC
- Wire diameter: < 2.5 mm^2

For more information about the power supply see chapter 20 Technical specifications.

After the power has been connected, the Atlas will boot up. This process can take somewhere from 15 up to 90 seconds. When it is booted, the green RDY LED will go on. You will see the Network Status LED blink yellow as long as the Setup Wizard has not been completed and a measurement has not been started.

2.2.4 Ethernet connections

All types of Atlas devices have two physical network interfaces named Office and Factory. The networks are not connected with each other one-on-one. The scanning, measuring and reporting of the network does not occur on the Office side, only on the Factory side.

The Atlas may be connected anywhere in the Factory network. Do not connect Atlas to a mirror port, as the Topology will not be accurate.

Figure 2 – Atlas2 mounted on a 35mm DIN

Note: the web interface can be reached on the Office <u>and</u> the Factory network IP range. Therefor it does not matter where you are connected, as long as you have set the correct IP range and netmask settings of your laptop/client network card. You will only be able to scan and see the devices connected to the Factory network, not the Office network.

Pointers about the IP-address configuration:

In case your office and factory share the same (sub)network you should NOT connect and configure the Office port. Just make sure that the default Office IP-address does not exist on your network and uses a non-existing subnet. In case your company network does use the 192.168.1.0/24 subnet, change the IP-address to be part of a non-existing network, for example 192.168.100.10/24.
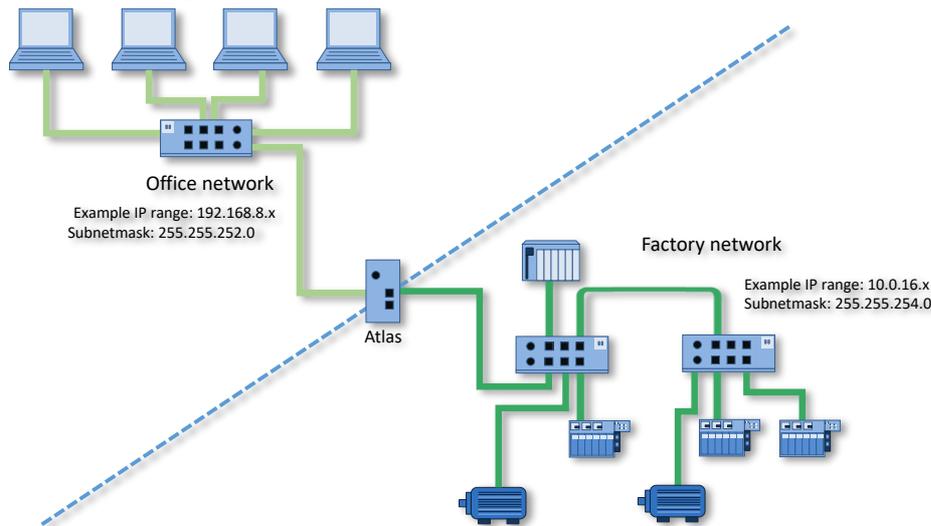
For a description on how to use Atlas, read on from chapter 6.

2.3   Atlas2 Plus and Atlas2 connections

Atlas2 Plus and Atlas2 have connections and options that the older Atlas does not have.

2.3.1   OLED display

Atlas2 Plus and Atlas2 have a display port that supports a full-color OLED display. It can be mounted on the front so it can display vital basic diagnostics and settings. This makes it easy to read problems in the network, without having to open the webserver to see what is going on.

The display covers the two LEDs on the front and replaces their function: the Power LED and the Network Status LED.

The display can be screwed on with two T10 Torx screws.

During startup, the display shows the PROCENTEC logo and it checks if there are USB updates available. When no firmware update has been found on USB, it will briefly show that on a window with blue background. When fully booted, the display shows the actual state of the Traffic Light with Network name and the state of Osiris with an uptime counter.

The display will cycle through this screen and the IP settings, on the right. This makes it easy to identify the unit and see which IP address to use to approach the webserver. On the top of the screen the device name is displayed.
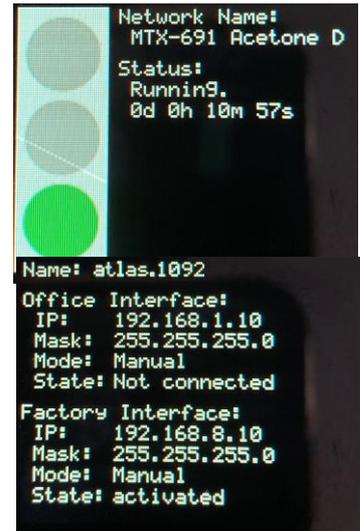
2.3.2 Micro-USB

The Micro-USB connection at the bottom of the Atlas has no purpose in normal use.

3. Getting started: Mercury

3.1 Quick Start

Step: Instructions: :

STEP 1 Switch on the Mercury by pressing the power button on the top.

STEP 2 Log in by entering your Windows username and/or password/pincode .

STEP 3 Double-click on the OsirisControl icon on the desktop. When Osiris starts, it
       will show a login window.

STEP 4 Use user 'admin' and password 'admin' for the first login.

STEP 5 Complete the Setup Wizard (see chapter 5) by entering the requested details.

STEP 6 Connect the RJ45 port of Mercury to an empty port of the factory network
       (do not use a mirror port).

Osiris on Mercury is now operational. From here you can change settings, layout and behavior. If connected to a factory network, it will start scanning and gathering information.

Warning: Do not re-install Windows or format the tablet. This will cause Osiris not to start. If problems arise, first check the FAQ on our webpage

4. Getting started: Osiris as a Software (on PC/laptop)

Osiris runs on any Windows-based PC or laptop. A license (issued by PROCENTEC) is needed to run Osiris.

4.1 System requirements

To properly install and use Osiris Software, the following requirements must be met:

Operating System	Windows 10 64bit
CPU	Intel core i5-7xxx or better
RAM	4 GB or more
LAN	100 Mbit/s or better
USB	Optional 1x USB 3.0 (required when using EtherTAP) Optional 1x USB 2.0 (required for measuring PROFIBUS)
STORAGE	25 GB free space or more (SSD optional but recommended)
Browser	Chrome, version 46 or higher. Other browsers are not fully supported.
CPU Hardware Virtualization	Enabled

It is required to have Google Chrome installed on your PC in order to use Osiris Software. Download and install the latest version of Google Chrome on your PC before the installation of Osiris Software. (Download Link: https://www.google.com/chrome/)
If you have a WiBu USB CmDongle (for example the HubDater license key) connected to your PC, remove it before installation.

Note: Hardware Virtualization
To use the underlying operating system that Osiris runs on (VirtualBox), hardware virtualization features must be available (and enabled) on the CPU. This feature is available on all modern CPUs. On most CPUs these features are also enabled. If not, then enable them via the BIOS.

4.2 Before the installation

Check if your system meets one of the following situations:

1. **There is already a version of VirtualBox installed**
   The installer for Osiris as a Software package will detect if a version of VirtualBox is already installed. If there is, the installer will ask you what to do; either use the already installed version of VirtualBox (v6.1 or higher) or install the one supplied with the installer.
   If you choose to use the already installed version, you must install the matching version of the VirtualBox Extension Pack.
   This Extension pack can be downloaded from https://www.virtualbox.org/wiki/Downloads
   Without the correct extension pack Osiris Software will not work.

2. **There is already a VirtualBox Host-Only Ethernet Adapter**
   Communication between Windows and Osiris is done using the VirtualBox Host-Only Ethernet Adapter.
   OsirisControl will create this adapter during startup when it is not available. On some systems a restart is needed before the adapter can be used.

If there already is a Host-Only Ethernet adapter available, the network settings might need to be changed. The IP address of the adapter must be set to 10.76.97.111 with netmask 255.255.255.0. The user can check these settings using Oracle VM VirtualBox Manager – Host Network Manager.

3. **You are using a firewall other than Windows Firewall**
    Update the firewall settings in order to enable communication correctly, see Note: Firewall Settings in the installation procedure (in paragraph 4.3, point 14).

4. **You have USBpcap installed on your machine**
    USBpcap is a Wireshark plugin used to analyze USB communication.
    USBpcap changes the Windows USB configuration and it is not compatible with Osiris when using ProfiCore or EtherTAP. Uninstall USBpcap before using Osiris.
    If you still have issues using ProfiCore or EtherTAP after removing USBpcap, follow this procedure:
    1. Select the 'Start' button, in the 'search programs and files' box, type 'regedit.exe'
    2. <u>**Make a backup of your registry settings**</u>
    3. Navigate the registry to this entry:
        HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{36FC9E60-C465-11CF-8056-444553540000}
    4. In the right hand side, if the value "UpperFilters" exists, delete it.
    5. Reboot Windows

    In this way Osiris will be able to communicate with the USB devices.

4.3   Preparation of the installation

Osiris comes with a quick installer, which installs all the applications necessary to run on a Windows PC. Follow the instructions to properly install Osiris on your PC.

1. Download the latest version of Osiris Software from the PROCENTEC website.
    https://procentec.nl/service-support/software-firmware/
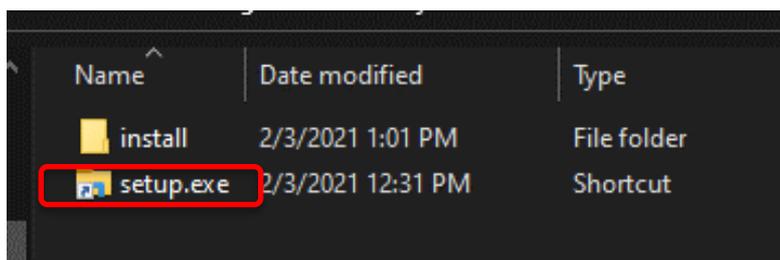
2. Connect the PC to the power supply and turn it on.

3. **Make sure that the battery is fully charged, and the sleep mode of Windows is completely disabled.**

4. Check that you do not have any pending Windows update.
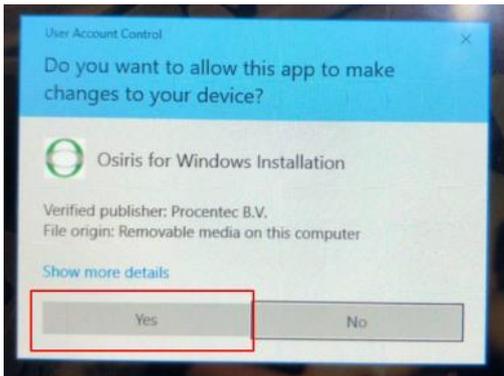   **Note: pending Windows updates can cause Osiris to not start.**

5. Open the installer folder, extract the files, and click on setup.exe

Name ^	Date modified	Type
📁 install	2/3/2021 1:01 PM	File folder
📄 setup.exe	2/3/2021 12:31 PM	Shortcut

6. When prompted, click on YES to allow the execution of the installer.

7. Click Next 2 times.

8. If you already have VirtualBox installed on your PC, you will get a pop-up for installing the VirtualBox update, click **YES**, the system will install the latest Virtualbox.
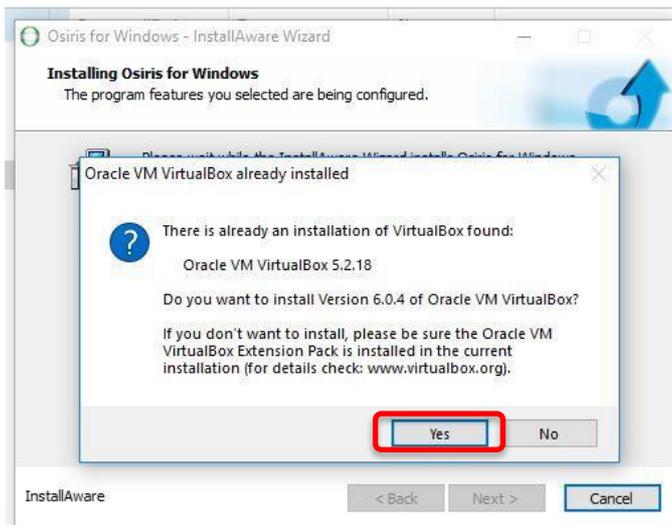
9. If you already have CodeMeter installed on your PC, you will get a pop-up for installing the CodeMeter update. Click **YES,** the system will install the newer CodeMeter.
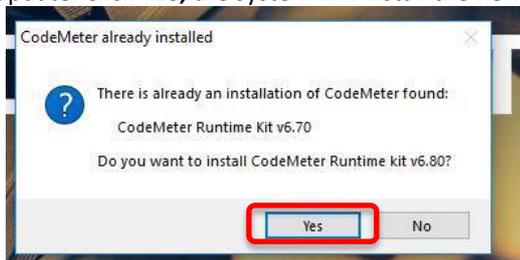
10. Follow the instructions of the CodeMeter installer (Click Next 4 times, then click Install).

11. Wait until all the installation is done.

12. When the installation is finished, make sure you have selected "Run Osiris for Windows now" and click Finish.
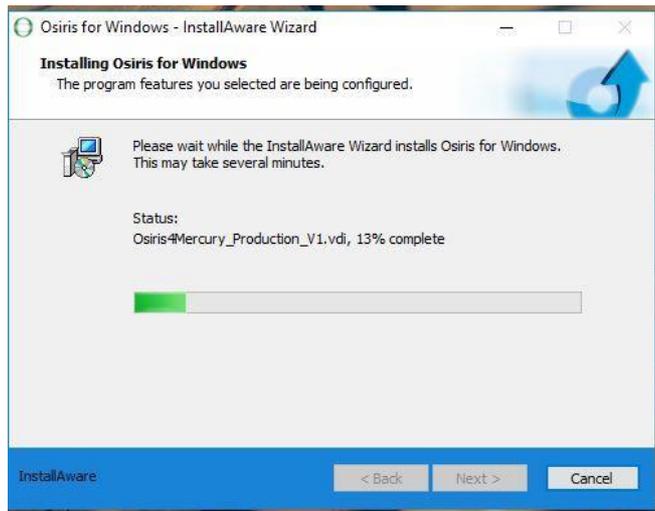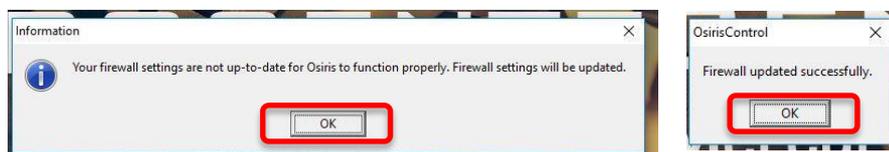

13. Wait a while, OsirisControl is now starting and preparing your system to startup.

14. If you get a firewall settings popup, click OK two times.

Important note: Firewall Settings

In order to check the license state, Osiris must be able to communicate with the CodeMeter service running on Windows. This communication is done using TCP/IP on port 22350. OsirisControl checks and configures the Windows Firewall automatically to allow incoming TCP communication on port 22350. **However, if you use a third party firewall which is not linked to the Windows firewall, you must manually open port 22350 for incoming TCP communication related to the application Codemeter, default path:**
C:\Program Files (x86)\CodeMeter\Runtime\bin\Codemeter.exe

15. Connect your PC to the internet.
    Your PC needs to be connected to the internet in order to activate your license. Connect your PC to an Ethernet/WiFi connection with internet.

16. A License pop-up will appear, click on Install.
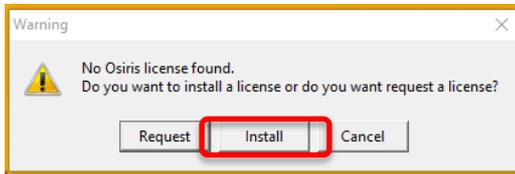
17. Insert the ticket number you received with your Osiris Software order.
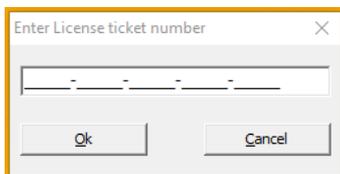
18. After some seconds you will have a license installation confirmation, click OK.
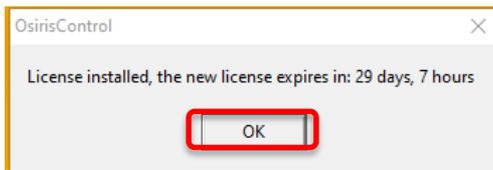
19. OsirisControl will ask you which interface you want to use for the measurement. Select the Ethernet interface you want Osiris to use for running the measurements and click OK.

20. A black popup will appear with the terms and conditions of VirtualBox, read them carefully and accept by typing "Y" and pressing Enter on the keyboard.
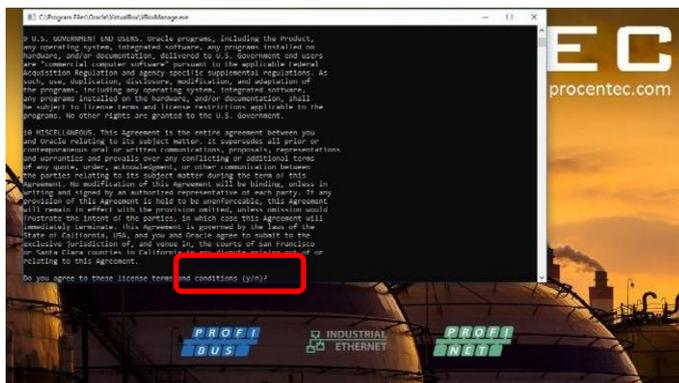
21. Osiris will now start, is it possible that at the first time you will see a "Not private connection" warning, click on 'Advanced' and 'Proceed' on the page.
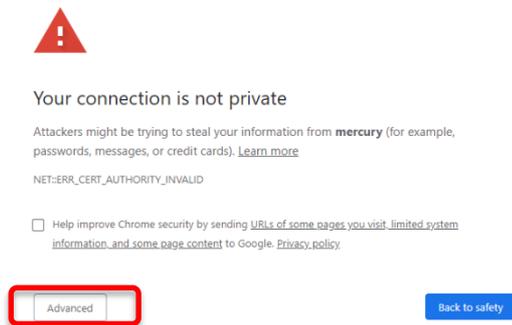
22. The Log-in page will appear, insert the default credentials (Username: admin, Password: admin).
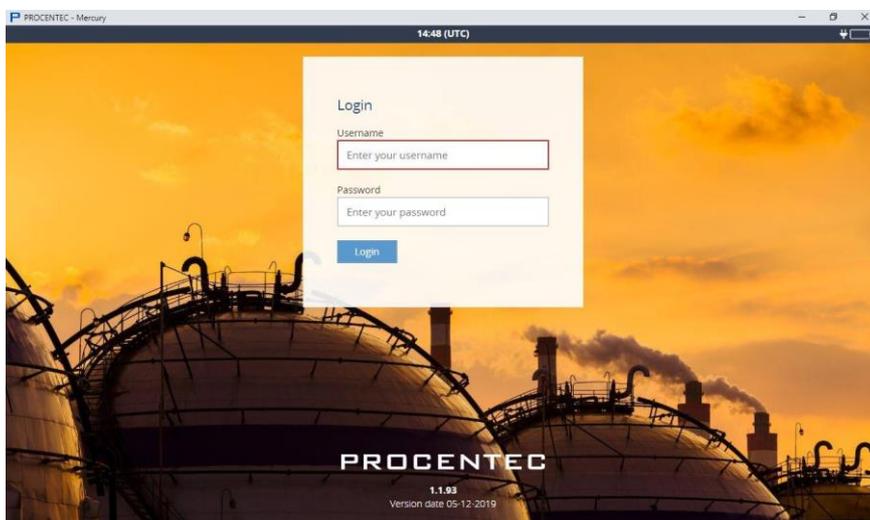
23. You can now start using Osiris Software!

4.4   Licenses

The basic license can be used for networks with up to 100 nodes. If more than 100 nodes are in the network, you can upgrade your license so that all nodes will be displayed. The notification in the System Bar will indicate if there are hidden nodes.

Contact our Sales Department for further information on upgrading your license.
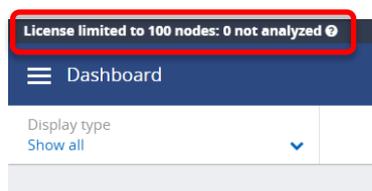
5. Setup Wizard

The Setup Wizard helps you setting up the Osiris software for use in your networks and is automatically started at first use. It can also be accessed after initial setup by clicking the Setup Wizard tile on the Dashboard. Pressing 'Change measurement settings' from the measurement button will also open the Setup Wizard on Step 2.

Step 1
Select the language. Over time, more interface languages will be released and available for download in the 'Download Software' section on www.procentec.com. Setting a language will take effect after the Setup Wizard has been completed.

Set the correct time zone. This time zone will be used to show the time in the top of the web interface (system bar) and in the reports. Automatic time (NTP) can only be used when Osiris has internet connectivity or when you manually set local time servers in the settings after the Setup Wizard has completed. See paragraph 16.1.4 for more information.

Step 2
Next, fill in the name and the location of the network. This name will be used in the web interface and reports. You can also enter optional contact details for colleagues in need of assistance.

Step 3
Then choose an Office and a Factory network IP address. The Office IP address and the Factory IP address must be set to the correct IP ranges with correct netmasks. If you do not know these, use the DHCP setting or contact your system administrator and/or the machine programmer for correct settings. Note that these two settings are independent of each other and the networks do not 'see' each other. There is no direct connection between the two ports.

Important: it is required that the office IP range and factory IP range are different from each other, and that their subnet masks do not overlap. Gateway and DNS are not mandatory, only enter one gateway, preferably the one for the office interface.
For Mercury: choose an IP address that is different from the IP address set in Windows.

Step 4
The last step asks you to enter one or more IP address scan ranges. It is important to choose scan ranges which include all the devices which you want to monitor. On the other hand, making the scan range unnecessarily large can negatively influence the Topology scan result and scan time. In case there are large gaps between devices on your network, it is advised to separate a large scan range into smaller ranges to exclude these gaps. This will speed up the scanning process.

6. Osiris User interface

Osiris displays all information by means of a web page. To access this information, simply open a web browser and type in the IP-address of your device (for the Atlas family the default address is 192.168.1.10 for the Office side and 192.168.0.10 for the Factory side; for Mercury, simply double-click on the OsirisControl icon on the desktop, Osiris webpage will appear as soon as the system has started).

6.1   Terminology and definitions

In this manual the following terms and definitions are used to refer to items in the web interface.
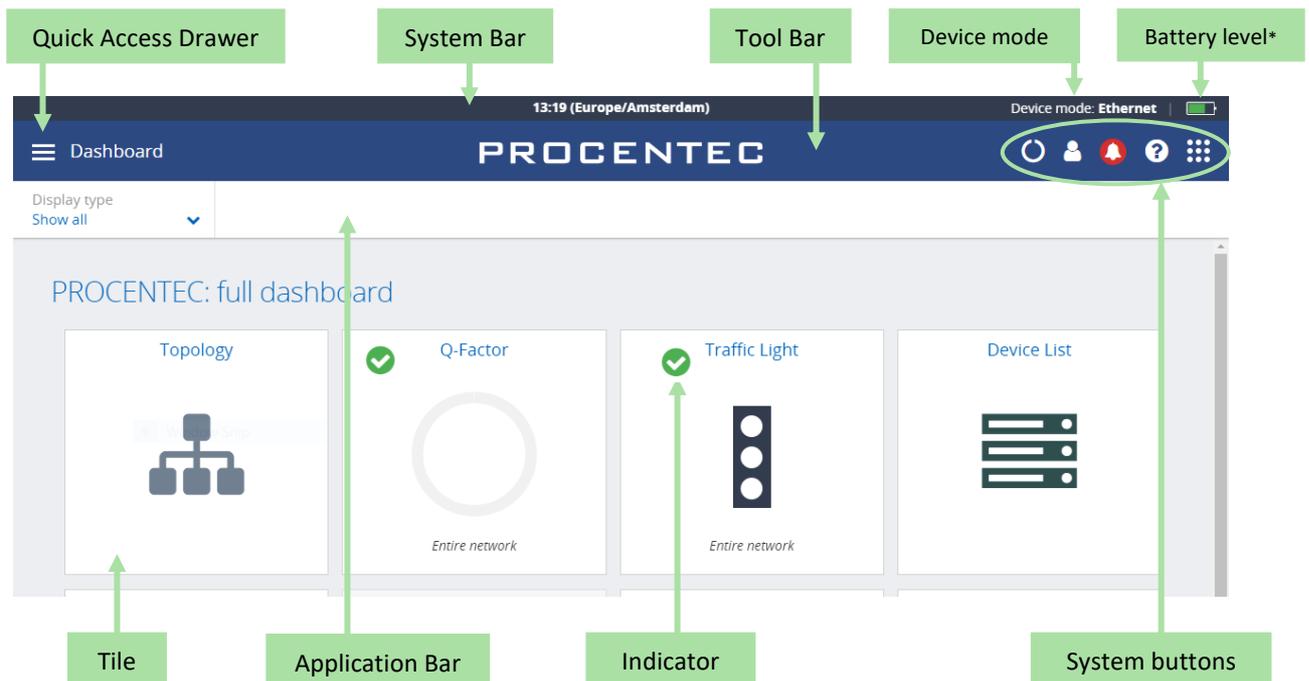
Figure 3 - Terminology used in the web interface

*Note: When using Osiris on a Mercury, a battery indicator icon will be present on the top-right corner of the System Bar. The Atlas does not have this indicator.

Figure 4 - Terminology used in the web interface (continued)

6.2 System Bar

As an admin, you can double-click on the dark blue System Bar (with the time indicator) to access shortcuts to:
- License Manager
- Settings
- Stop Osiris (safely shuts down Osiris and the underlying operating system. Not available on Atlas)
- Restart Osiris
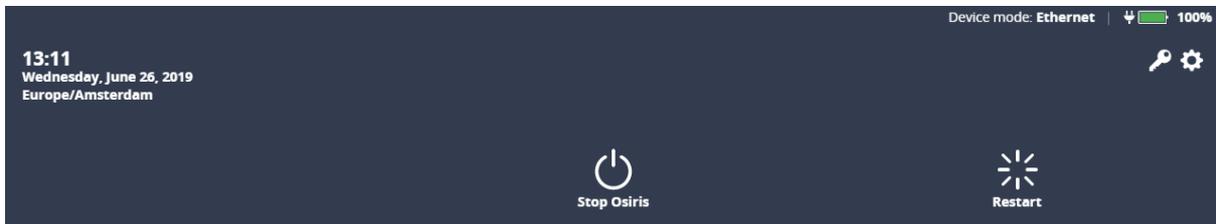
6.3 System buttons

The right upper corner of the Application Bar shows five buttons. These are the system buttons. They are all clickable and will give extra information or functionality.

Figure 5 – Explanation of system buttons in web interface

6.4 Measurement Button

When clicking the spinning measurement button, a dropdown menu appears. This dropdown shows how long the measurement has been running.

Clear data: When the Clear data button is pressed, a popup will ask you to select the types of data you wish to clear. When pressing "Confirm" all selected errors and notifications will be deleted. This will not affect the trending data related to the current measurement, system settings, configuration, custom topology views, Topology or Network snapshot, or the notifications log file.
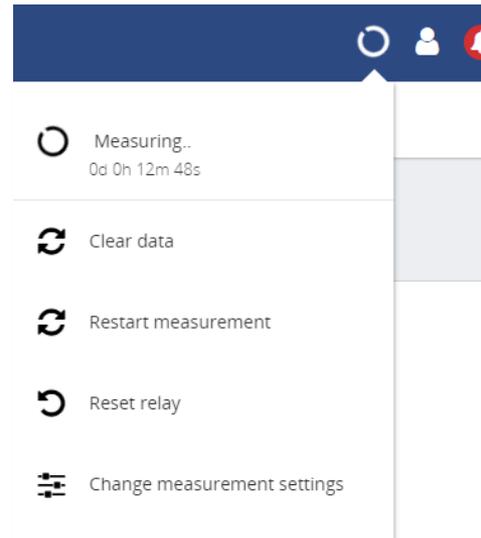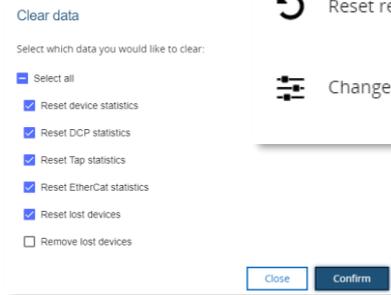
Figure 6 – Measurement button in web interface

The Restart Measurement button will clear all items listed above, including EtherTAP measurement recordings and the notifications log file. This will not affect the trending data related to the current measurement, system settings, configuration, custom topology views, Topology Snapshot or Network snapshot. After a few minutes, a new measurement will start.

The Reset Relay button (only available on Atlas) can be used to switch off the Relay when it has been triggered by an event (see 16.5.1).

The Change measurement settings button allows you to quickly change your settings by sending you to the setup wizard (see Chapter 5).

6.5 Current User

Clicking the current user button shows the current user and the logout button.
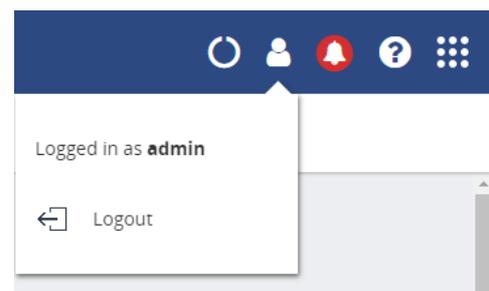
Figure 7 - User in web interface

6.6   Notifications

The color of the notification bell indicates if there are any errors or warnings to be reported. In properly working networks the bell is green. In case there are warnings, it turns orange. Error conditions on your network lead to a red bell. Clicking the icon will bring up the list of notifications. There are three types of notifications:

Figure 8 – Notifications in web interface

Non-critical user information, such as: 'Your factory network is now connected'

Warning notification, such as: 'Ping response time exceeded'

Critical errors and warnings, such as: 'Error level for Discards exceeded'

By clicking ´Clear´ all the notifications from this list are cleared. Internally the notifications are not removed and are therefore still available for CSV export.
By clicking ´Export All (CSV)´ you can download a full history of the last 50.000 notifications regardless of any previous clearings of the list. This downloadable file is in CSV format which can be directly opened in spreadsheet software like Microsoft Excel. Errors generated by ignored devices will also be in this list.

The Dashboard also features a Notification Center tile. For further information see Chapter 14.

6.7   Delphi Help

The Delphi help function provides specific help on the page you are currently viewing. This means that on the dashboard for example, it will show help information for the dashboard. This is done for the Dashboard, Topology, Q-factor, Traffic light, Device list, Trending, Commissioning Wizard, EtherTAP and OPC UA page.
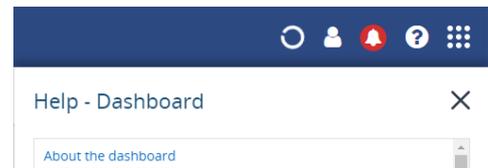
Figure 9 – Help Dashboard in web interface

6.8   Application Menu

Within the Application menu there is a function to generate a Report. See paragraph 8.10 about what the generation of the report includes.
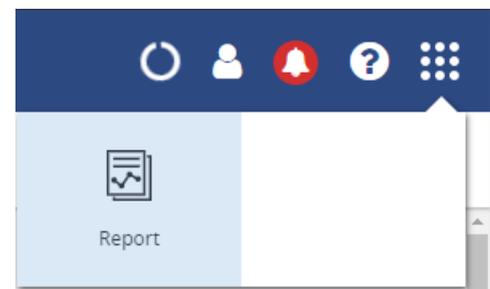
Figure 10 – Generate report in web interface

7. Device mode

Osiris has two modes; a PROFIBUS network analyzer (note: not available on Atlas), and an Industrial Ethernet analyzer. Tap on one of the options to start the preferred mode:

Figure 11 – Device mode selection in web interface

You can see the currently selected device mode in the upper notification bar on the right side.
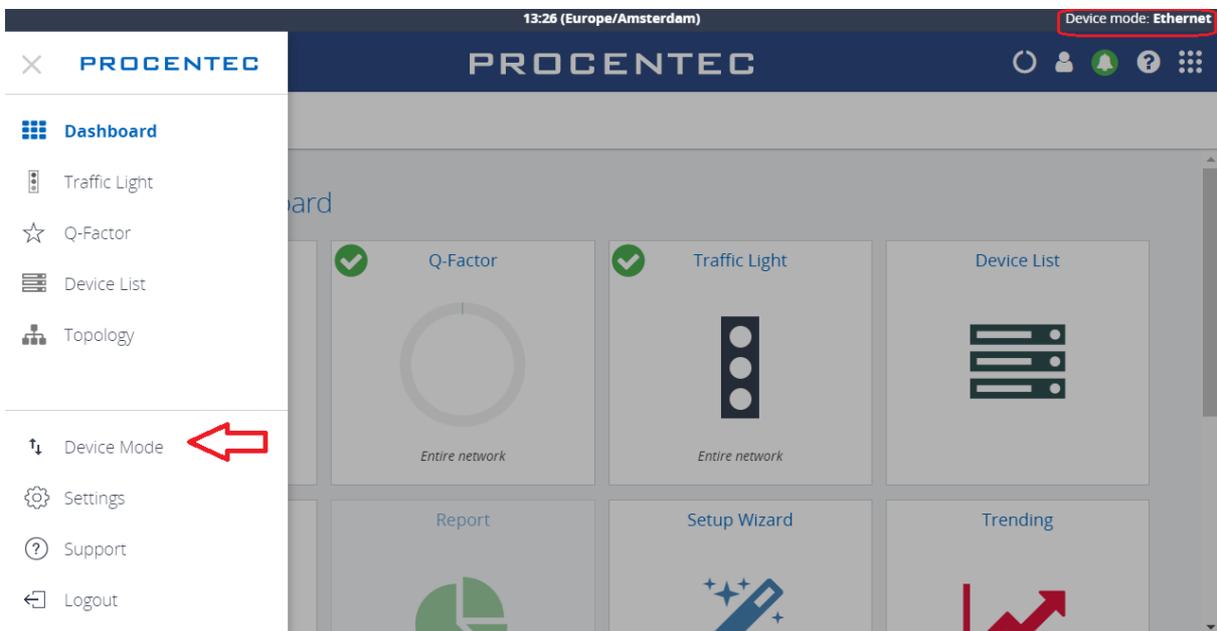
Figure 12 – Device mode in web interface (continued)

If at some point you need to change to another mode, tap the Dashboard button and click 'Device mode'. This will bring you back to the Device Mode selection screen.

For the Industrial Ethernet mode, continue on Chapter 8. For PROFIBUS mode continue on Chapter 15.

8. Device mode: Industrial Ethernet

8.1 Dashboard

The dashboard is a one-stop-shop and overview with access to all available functions through Tiles.
Tiles can be a static picture, but some are also dynamic. These dynamic tiles show an online summary of its information. This way you have a quick and intuitive way to access information. Some tiles also have a general status indication in the upper left corner of the tile (green checkmark, orange exclamation, or red cross). This is a uniform way of allowing you to see quickly if there are problems which need attention.

8.1.1 Dashboard organization

The dashboard is a matrix of tiles and can be organized in 3 different ways:

- Show all: All available tiles are shown in a fixed arrangement
- Show recommended: Only tiles are shown which PROCENTEC deems most important
- Show customized (see paragraph 8.1.2)

8.1.2 Customize Dashboard

To customize the Dashboard, follow the next steps:

- In the Dashboard, go to the upper left corner and click on 'Display type'. Then choose 'Show customized'.
- On the upper right part, select 'Edit dashboard'.
- An empty tile placeholder(s) will appear, marked with a '+' sign.
- By clicking on the '+' sign a popup window will appear.
- Select the tile you would like to place by clicking on it.
- The popup will close and the tile will be placed.
- During edit mode you can drag and drop to a desired grid location.
- By pressing the 'trashcan' icon in the lower right part of the tile you can delete the tile.
- When all changes have been made, select 'Save changes' in the upper right corner.
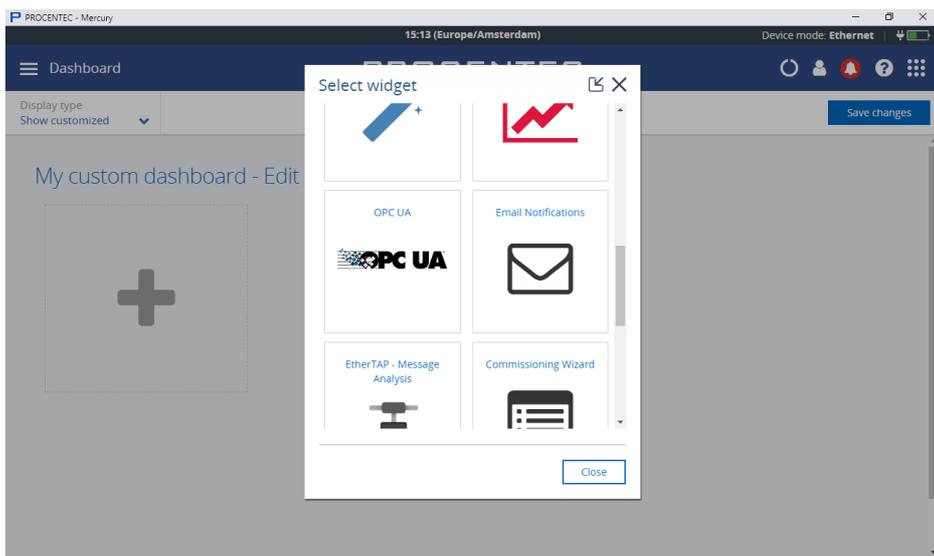
This saved personalized dashboard will remain available after a logout or restart. These settings are stored in a browser session, so this is a personalized setting for a specific user, computer and browser. Opening a customized Dashboard on a different computer or browser will result in a default view.

8.2   Starting a measurement

When Osiris has been set up and connected, start a new measurement by clicking on the round progress indicator in the System Buttons area, and click 'Start'.

To indicate the measurement is running, you will now see a spinning progress indicator.

When the measurement has collected enough information, the Topology, Q-factor, Traffic Light and Device List will become available.
Note: Atlas devices are designed to be a permanent monitoring tool, therefore is not necessary to start the measurement, as it is always running.
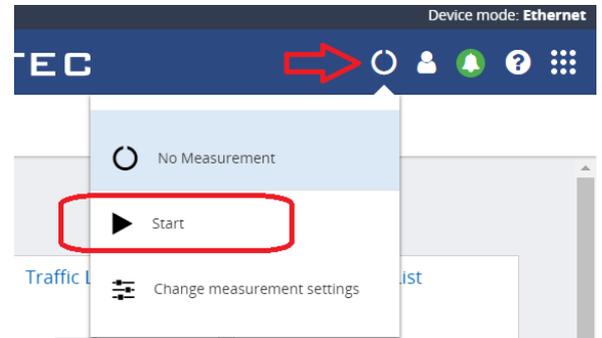
Figure 13 – Starting a measurement in web interface

8.3   Topology

The topology is a graphical and hierarchical display of a complete network. This view makes connections between devices become clear very quickly and intuitively. This view also clearly shows dependencies to easily identify/mitigate critical paths in the network, or to identify line-depths.

The underlying mechanism to be able to determine a topology is based on SNMP and, if possible, specific industrial protocol functions (e.g. LLDP for PROFINET) will also be used. Unfortunately, some devices do not (properly) supply topology information. These are connected either to a question mark icon or are placed as stand-alone devices. The devices linked to a question mark icon and then in turn to other devices means the connection information is only partly known. In many of those cases it can also be that non-managed switches are used.

There is a   Reset zoom   button in all views to set the Zoom level so that all devices fit in the screen.

8.3.1   Topology View types

There are two default views to choose from: Galaxy and Tree. Next to the default views it is possible to create custom views.

In all views, devices are connected to each other with lines. These connections between devices show how these are connected to each other and how they are co-dependent. In this overview it is much easier to understand that if a device is lost, it will affect the connection to other devices behind it. Lost devices are indicated with a red cross over the device icon.
Link problems between devices are indicated with a red cross on that particular link. The two numbers shown on both ends of the link lines, specify the port number used for this link.

8.3.1.1 Galaxy view

The Galaxy view shows a self-organizing network diagram where switches are shown as central devices. In the Galaxy view user devices can be dragged to other positions. When dragging a device to a new place, the topology will automatically be re-arranged.
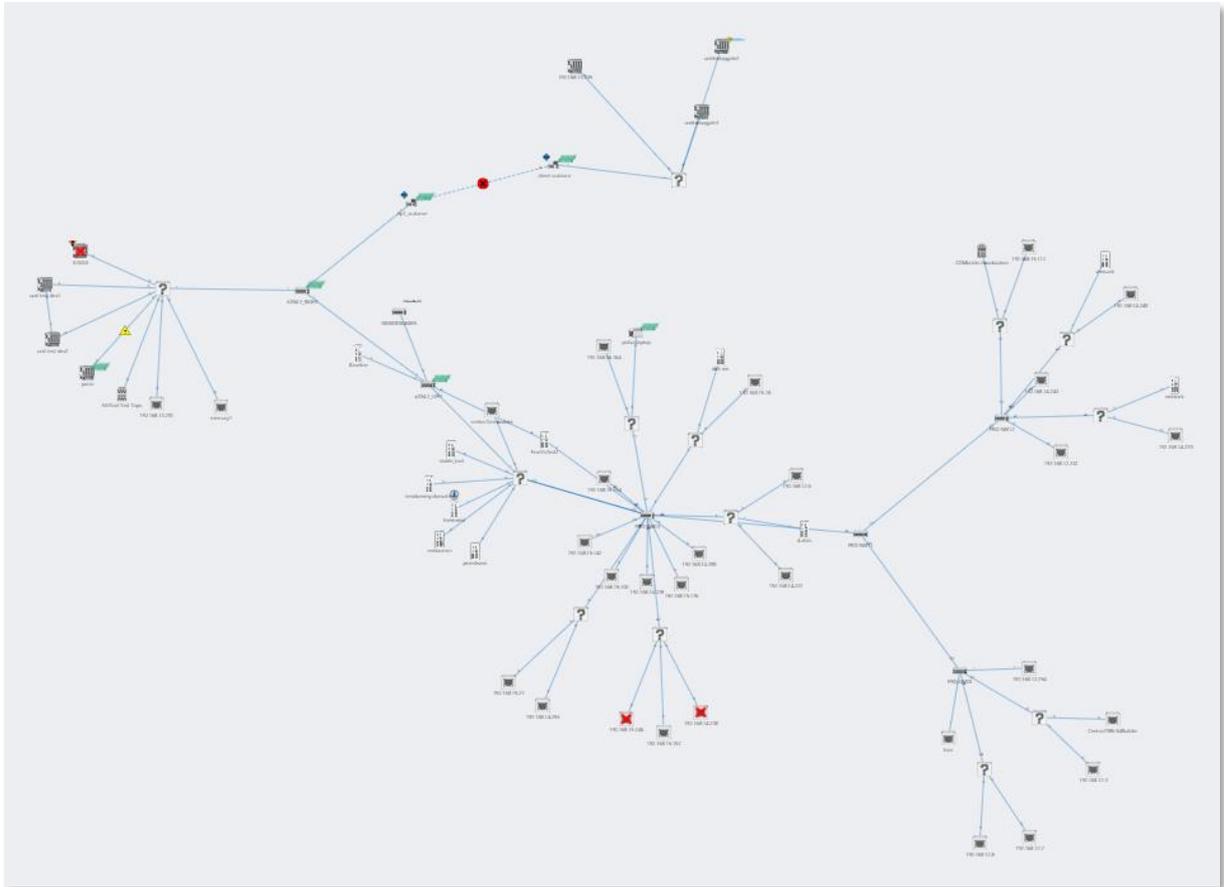
Figure 14 - Galaxy view in web interface

8.3.1.2 Tree view

The tree view shows a self-organizing layered overview using a top-down organization. In the tree view it is possible to click on a device which will show the device details panel. Within this panel there is an extra button to assign a top node. When setting a device as top node, the tree view will be re-organized with the selected device at the top.
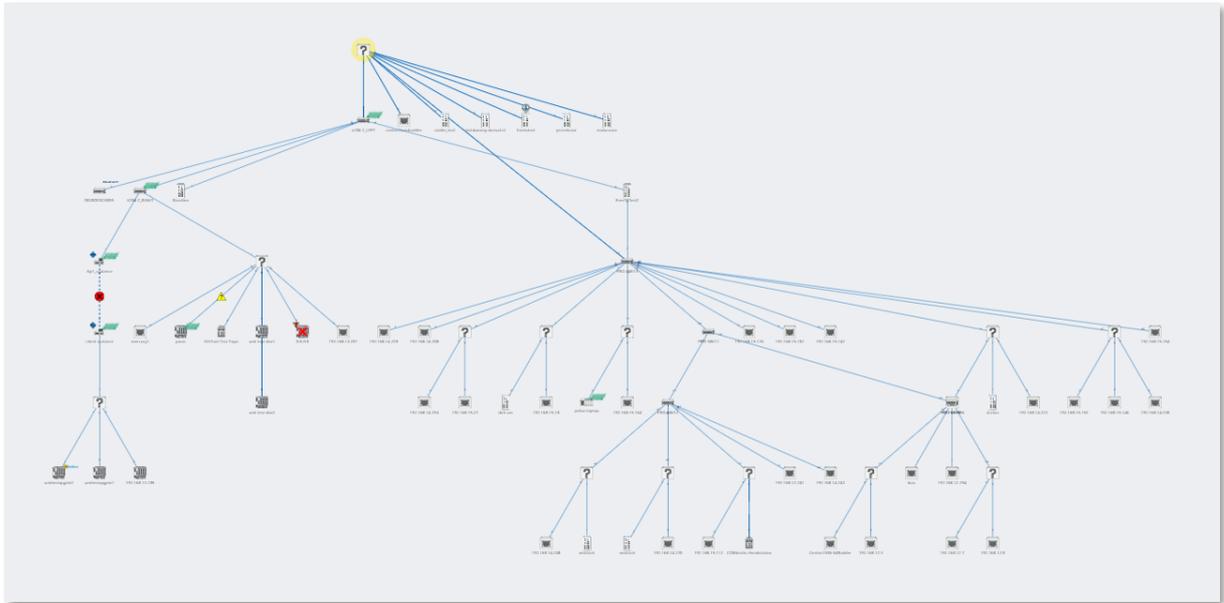
Figure 15 - Tree view in web interface

8.3.1.3   Custom view

From within the galaxy view it is possible to create custom views. Click 'Create view' and assign a name to the view. A grid appears on the background: now all devices have a fixed position which can be changed by dragging them around. The positions will be saved automatically, can be viewed and edited in multiple browsers and are persistent over a restart. It is also possible to rename or delete a custom view the Delete and Rename buttons.
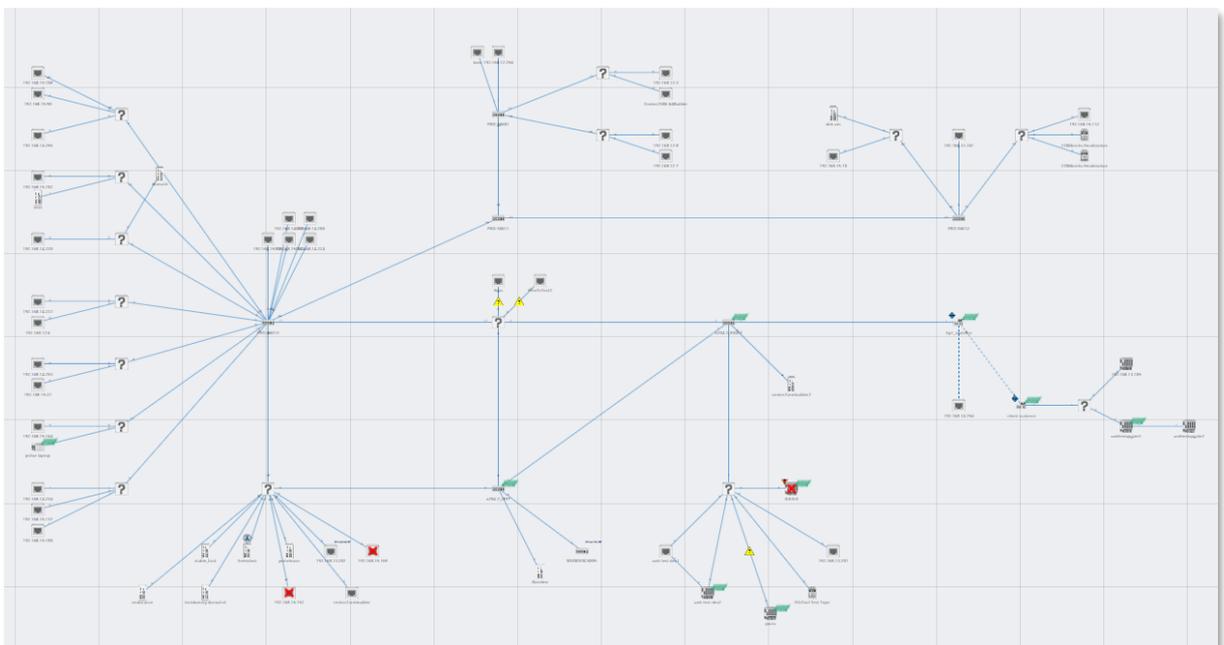
Figure 16 - Custom view in web interface

8.3.2 Topology search

To easily find devices in the Topology view, click on the magnifier icon in the top left of the Topology view. This will show an input field, where you can enter a name, IP address or MAC address of the desired device. Autocomplete will help you to quickly find the device you are looking for. When clicked on, the topology zooms in on the requested device and opens the device details.

8.3.3 Device types in the Topology view

The following icons are used for devices in the Topology view.

Icon	Meaning
	This is your current Atlas, the one on which you are currently viewing Osiris?
	This is your current Mercury, the one on which you are currently viewing Osiris?
	The yellow halo indicates the selected node.
	This is another Atlas in the network.
	This is another Mercury in the network.
	This is a tablet in the network.
	This is a laptop in the network.
	This is an I/O controller. The label next to the device indicates the supported industrial protocol.
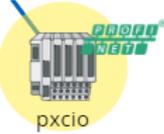
	This is an I/O device. The label next to the device indicates the supported industrial protocol.
	This is a drive / VFD / VSD.
	This is a gateway or other I/O device.
	This is a managed switch.
	This is a Wi-Fi access point.
	This is a router.
	This is a firewall.
	This is a Wi-Fi group access point, with two or more devices connected to its copper port(s).
	This is a ComBricks Head Station.
	This is a generic Ethernet node, such as a PC or laptop that does not support SNMP.
	This is a locked device.

	The devices in (and connected to) this group cannot be accurately placed in the Topology. This is because the necessary data to do so cannot be obtained. There are multiple explanations for this problem: 1 It is an unmanaged switch. This is a standard switch that does not supply data to determine the topology of the network. 2 It is a device that does not supply correct data. Note: PROFINET devices certified after v2.3 must have all the required data for Topology as defined in the PROFINET standard. This is not mandatory for other Industrial Ethernet devices. 3 It is a device outside of the scan range. The device can be found based on its MAC address but cannot be accessed via an IP address.

Device status indicators in the Topology view:

Icon	Meaning
	This indicates that the device is lost. It has been online on the network in the past, but cannot be reached now.
	This device has a different firmware version compared to other detected devices of the same type. It is recommended to set devices to the same firmware version.
	1. The IP address of this device is 0.0.0.0. This indicates it needs to be configured. 2. IP conflict: There is another device on the network with the same IP address. This could make both devices unusable. You are advised to resolve this issue immediately by changing the IP address of one of the devices. This issue may also prevent the correct visualization of the topology within Osiris.
	The device has an incorrect configuration. Click the device and investigate the device details.

8.3.4   Link indicators in the Topology view

Icon	Meaning

⚠️❓	• The port load is still acceptable but nearing unacceptable levels of 50% (20% < port load < 50%) • The link speed is not 100 Mbps full duplex (for PROFINET devices)
❌	• The port load is over 50% (port load > 50%) • The devices report different link speeds • The existence of InDiscards, OutDiscards, InErrors or OutErrors
1..28	The number on the link is the physical switch port of the device that this cable is connected to.

8.3.5 Protocol indicators in the Topology view

Icon	Meaning
PROFI NET®	This is shown for devices that support PROFINET.
PROFI BUS®	This is shown for devices that support PROFIBUS.
Modbus	This is shown for devices that support Modbus TCP.
EtherNet/IP	This is shown for devices that support Ethernet/IP.
EtherCAT.	This is shown for devices that support EtherCAT.

Note: if a device supports multiple protocols, the Protocol indicator icon is not displayed. Supported protocols are shown in the Device details.

8.3.6 Device details

By clicking on a device this item will become emphasized and a Details panel will appear on the right-hand side. Depending on the type of device, information is shown in groups:

In the Tree view (described in paragraph 8.3.1.2) you will find the button in the top to assign a device as 'Top Node'. With this functionality you can set the highest (top) device in the tree. If the selected device is already marked as Top Node, the button will state 'Top Node' and will be inactive. Otherwise, it will state 'Assign Top Node' and can be used to move the selected device to the top.

General
General information is shown for the device. For more information on the various items, check the description of the 'overview' section.

Customize: Ignore device errors
In some cases, devices generate errors which you, for different reasons, would like to ignore. Such errors can be suppressed by ignoring a device in the Device details panel (see image on the right). A drop-down box lets you choose the types of errors to ignore from this device. Ignoring a device will be done at a variety of places within Osiris; see table on the next page.

When Ignore All is selected, the device will get a checkbox in the 'Ignored' column in the Device List. If only a subset of data is selected, the rest of the data will still trigger alarms as set in the Alarm Configuration page.

Device errors will still be visible in this Device Details view but will be hidden from the Device List and Topology, and errors related to this device will not influence the Traffic Light or Q-Factor, or be displayed in the notifications log. Ignored devices are labelled in the Q-Factor. Notifications which are generated by the device are stored and downloadable as CSV but are not shown.

| Where	Effects of ignoring device errors
Device details	• Errors are <u>still visible</u> in the device details except for firmware differences
Device List	• If all errors of a device are ignored, they receive a check in the Ignore column • All errors and warnings of the device are hidden
Notifications	• New errors will not be shown • Old errors will be removed from the dropdown under the bell. This potentially means that the bell can go back to green • Errors of ignored devices <u>will still show up</u> in CSV export of the Notifications
Q-Factor	• Devices will be marked as ignored • Errors will no longer influence the Q-Factor of the device. The device will always have Q-Factor 5000 and therefore have no influence on the overall Q-Factor of the network
Report	• If all errors of a device are ignored , the device will appear in the Ignored Device list in the report
Topology	• Lost devices are still visible but the usual the red cross which indicates that the device is lost, will be faded • Double IP-addresses are ignored • Firmware difference are ignored • Link errors and warnings will not be shown if you ignore device errors of the device causing the link errors • A device with IP-address 0.0.0.0 will generate a warning. When ignoring the errors of such a device, it will not generate errors anymore • Devices which do not supply correct SNMP data will show a blue NAMUR icon. When ignoring the errors of such a device, this icon will disappear
Traffic Light	• Errors will no longer influence the traffic light (both on the web interface as on the physical Atlas or LCD display)

Notes
A device can have multiple custom notes with different types. Click the blue 'Add note' button to open the Notes window. A note can have one the following types:

- Info
- Warning
- Bug
- Environmental

After entering the note, it will appear in the Device Details list with the author name, date and time of posting.

The device icon in the Topology will have a label added to it, to indicate that a note has been added.The icon will appear at the next topology scan. This can take few seconds.
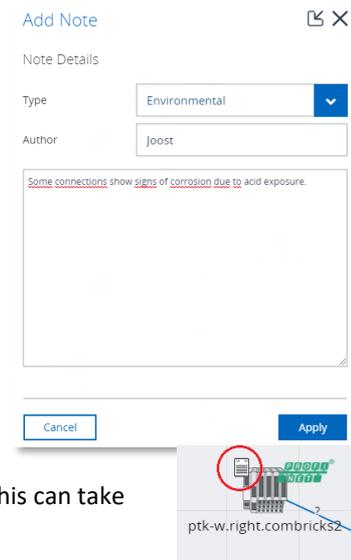
Icon
All icons in the Topology are assigned automatically by default. However, they can be changed to a custom icon when using the Custom Topology view. In the Device Details you can click on 'Change' to choose one of the custom icons (see 8.3.3 for the full list of icons).

Identification and Maintenance
Information about the device itself: the Product ID, vendor name, software and hardware version, order code and serial number. If two devices of the same ID have been found, using different firmware versions, a warning is displayed (see Figure 17).

PROFINET Configuration Status
Information about the configuration of the device; if the device reports a different configuration than what the IO-Controller expects, you can find the status of the modules in the table (see Figure 18). If a problem with a module exists, the device will show a red cross in the Topology.

Figure 17 - Firmware deviation warning
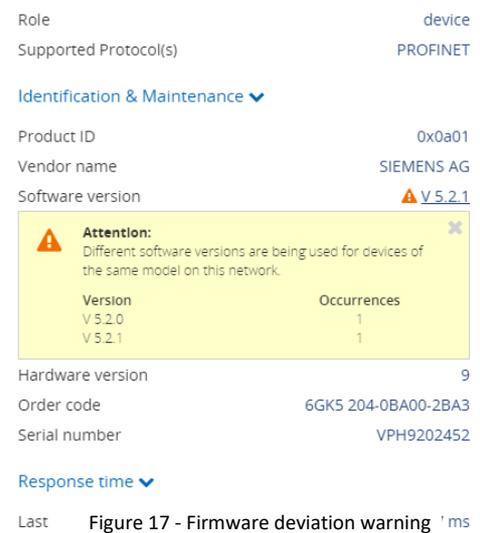
Response time
The last, min and max ping response times are shown here.

Port load
- In: for each incoming/ingress port the last, min and max port load is shown.
- Out: for each outgoing/egress port the last, min and max port load is shown.
- Warning: some devices report an incorrect link speed (e.g. 10 Mbps instead of 100 Mbps). Since the link speed is used to calculate the load, the reported load can be incorrect. If the reported load is very high, check the link speed.

Link details
By clicking on a link or line between devices an info panel will appear on the right-hand side. Depending on the type of device, information is shown in groups:

Linked devices
Device name, MAC address and port number are shown for both sides of the connection.

Load
For each direction the last and max port load is shown in %.

Figure 18 - PROFINET configuration: module 4 in error

Warning: some devices report an incorrect link speed (e.g. 10 Mbps instead of 100 Mbps). Since the link speed is used to calculate the load, the reported load can be incorrect. If the reported load is very high, check the link speed.

Link status
- General: the link speed is indicated (10Mbps/100Mbps/1Gbps) together with its operational state (up/down);
- For each direction, in and out, the 'discards', and 'errors' are shown. Discards are the number of telegrams which did not fit in the internal buffer (memory overload) and 'errors' are transmission or CRC errors.

Warning: some devices can report an incorrect link speed (e.g. 10 Mbps instead of 100 Mbps). An indication that this occurs is when two devices in a link report different link speeds. This is not possible in Ethernet connections.

8.3.7 Topology snapshot

In the upper right corner of the Topology you will find a small ⬜ icon. Pressing it will take a snapshot of the Topology as it is visualized, and saves it to memory. This makes it possible to take a snapshot of a custom Topology for example, and let that image be used by the Report Generator (see 8.10 Report). There can be only one snapshot in memory.

8.4 Q-Factor

The Q-Factor is a number that represents the quality of the network. You can choose if you want to use the 0 to 5000 range, commonly used in the Automotive industry, or a percentage.

A value of 5000 or a percentage of 100 is excellent and 0 is critical or unmeasurable. Additionally, a color coding is used to emphasize the severity. Normally the color should be green, meaning excellent or good. Yellow is subpar but not critical, e.g. attention recommended. Red means a bad, critical or urgent issue.

8.4.1 Multiple Q-Factors

There are multiple Q-Factors in use in the tool:
- A Q-Factor for each network device, which indicates the quality for a single network device. Calculation of this Q-Factor is based on a weight of:
    - Network link load: the bandwidth usage on a certain port of a device, is used to determine the value. In general, the lower the load, the higher the Q-Factor.
    - In/Out errors: the number of errors per port of a device.
    - Ping packet loss: the number of unanswered ping requests.
- A single overall Q-Factor, indicating the quality of a complete network. Currently the overall Q-Factor equals to the lowest Q-Factor of an individual network device.
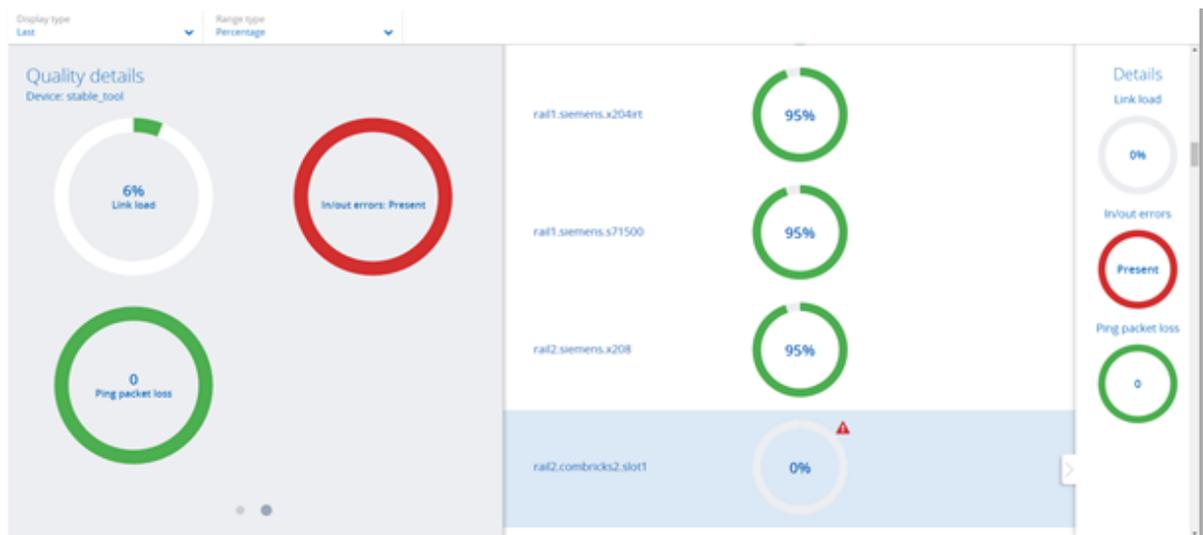

Figure 19 - Multiple Q-Factors: Overall Q-Factor on the left, individual Q-Factors in the middle and on the right

8.5   Traffic Light

The Traffic Light is an overall color coded status to indicate the degree of network status. As it so purposefully describes, the state is in the form of a traffic light. The Network indicator on the front of the Atlas unit (LEDs or LCD display) corresponds to the traffic light state in the web browser. The Traffic Light can also be read in the live tile in the Dashboard.
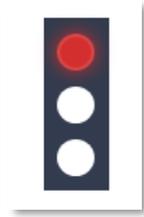
8.5.1   Traffic light state explained

- Red light: a serious problem is present in the network, user attention required.
- Yellow light: a situation is present which is important but not serious, user attention recommended.
- Green light: all seems to be working correctly, no important or critical situation.

8.5.2   Traffic light triggers

The following situations cause the traffic light to turn orange in the default setup:
- Flashing orange: no measurement is started.
- A ping response time between 250 and 500 milliseconds
- The occurrence of PROFINET alarms that are not communication alarms
- PROFINET DCP Identify Multicast (more than 1)
- PROFINET Jitter higher than 50%
- PROFINET Dropped packets
- Ethernet/IP Dead connections between 1 and 10
- Ethernet/IP Jitter higher than 50%
- Ethernet/IP dropped packets

The following situations cause the traffic light to turn red in the default setup:
- A ping response time higher than 500 milliseconds
- A device previously seen (e.g. by ping or DCP) is not responding anymore
- In or Out discards (the number of telegrams which did not fit in the internal buffer of a switch)
- In or Out Errors (transmission errors or CRC errors)
- The occurrence of PROFINET communication alarms

The behaviour of the Traffic Light is customizable; the above settings can be changed. See paragraph 16.5.

8.6   Device list

The device list shows a list of all detected network devices. Also, lost devices (detected in the past) are listed here. It provides a full overview of all the important properties of devices in the network.

The entire list is downloadable as a CSV file which can be directly opened in spreadsheet software like Microsoft Excel.

The 'View' drop-down selection box lets you choose between showing all Ethernet devices or showing only PROFINET-capable devices. If you select 'PROFINET', additional features become available which are further described in paragraph 8.6.3.

8.6.1   Table customization

Generally, the table columns can be customized with the following features:

- The left column is pinned, meaning if the scrollbar is horizontally scrolled the leftmost column does not move.
- The list can be sorted by clicking on the column header (ascending, descending or none).
- Columns can be resized by placing the mouse between columns and then selecting/dragging the splitter.
- Columns can be hidden by selecting the ☰ icon on the far right of the table. A list will drop down in which you can select which columns are to be shown/hidden.
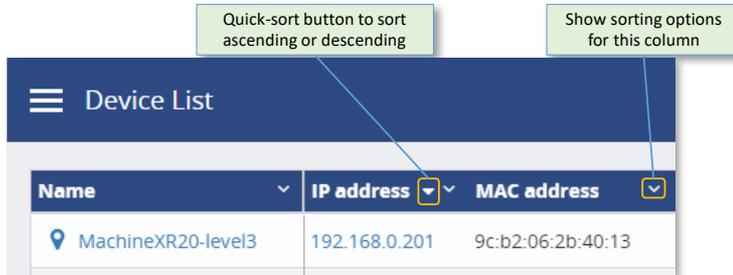

Figure 20 - Sorting

- Certain columns can be filtered (mainly text fields) by clicking on the 'sorting options' button on the right of the column, and then choosing 'Show filter'. Note: these columns can also be optionally pinned left.

- It is also possible to combine two or more filters. Simply enable a filter for each column that you want to filter, for example an IP address filter and a MAC address filter:
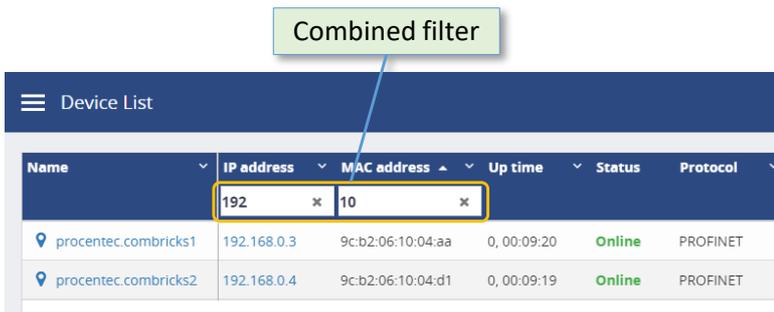
Figure 21 - Combined IP and MAC address filter

8.6.2   Available columns

Column	Description
Name	This name is retrieved from the device if it supports a protocol name identification function (e.g. DCP for PROFINET IO).
IP address	The IP address of the device. It consists of 4 numbers separated by '.' Dots. If no IP protocol is supported, it is left blank. Currently only IPV4 is supported.

MAC address	The unique Media Access Control address for the device. It consists of 6 numbers in hexadecimal format separated by colons.
Status	If a network device has been seen previously and is still being seen it remains Online (green). If it has been seen previously but not anymore lately it changes to 'Lost (red).
Last response time	The most recent reaction time measured by a 'ping' to a device and its response.
Min. response time	The fastest 'ping' reaction time.
Max. response time	The slowest 'ping' reaction time.
Last incoming load	The most recent measured network load (in %) for the incoming/ingress port. If a network device has more than one port the highest load is shown. **See note below**
Min. incoming load	The lowest measured network load (in %) for the incoming/ingress port. If a network device has more than one port the highest load of all the lowest port values is shown. **See note below**
Max. incoming load	The highest measured network load (in %) for the incoming/ingress port. If a network device has more than one port the highest load of all the highest port values is shown. **See note below**
Last outgoing load	The most recent measured network load (in %) for the outgoing/egress port. If a network device has more than one port the highest load is shown. **See note below**
Min. outgoing load	The lowest measured network load (in %) for the outgoing/egress port. If a network device has more than one port the highest load of all the lowest port values is shown. **See note below**
Max. outgoing load	The highest measured network load (in %) for the outgoing/egress port. If a network device has more than one port the highest load of all the highest port values is shown. **See note below**
Netmask	The IP netmask address of the device. It consists of 4 numbers separated by '.' Dots. If no IP protocol is supported, it is left blank. Currently only IPV4 is supported.
Gateway	The IP gateway address of the device. It consists of 4 numbers separated by '.' Dots. If no IP protocol is supported, it is left blank. Currently only IPV4 is supported.

Role	For certain industrial network protocols, a device can have a certain designated role associated with it. For e.g. PROFINET the roles device, controller and supervisor are possible.
Model	For certain industrial network protocols, a device can have a vendor designated model assignment associated with it (e.g. for PROFINET).
Device ID	For certain industrial network protocols, a device can have a certain designated Device ID assignment associated with it (e.g. for PROFINET it helps to define the product code when used in combination with a Vendor ID).
Vendor ID	For certain industrial network protocols, a device can have a certain designated Vendor ID assignment associated with it (e.g. for PROFINET each registered manufacturer has its own number).
Software version	For certain industrial network protocols, the software version can be retrieved (e.g. for PROFINET and Ethernet/IP). This can help to verify that the product has the latest or stable software version.
Hardware version	For certain industrial network protocols, the hardware version can be retrieved (e.g. for PROFINET).
Order ID	For certain industrial network protocols, the order/article number can be retrieved (e.g. for PROFINET). This can help if the product needs to be re-ordered or documented (e.g. when there is a defect, or a spare is needed).
Serial number	For certain industrial network protocols, the serial number can be retrieved (e.g. for PROFINET). A serial number sometimes contains crucial information for a vendor (production date, batch) and for a user as well (tracking/detecting replacements).
Vendor name	The vendor name is either retrieved by looking up de MAC address in a publicly registered MAC/OUI reference list or it can be retrieved by using specific network protocol functions (e.g. I&M0 for PROFINET)
Vendor name (I&M0)	Retrieved by using a specific PROFINET IO network protocol function (I&M0 Identification & Maintenance function as defined by PROFIBUS/PROFINET International)
Revision counter	A settings alteration tracking number implemented by some industrial network protocols (e.g. the I&M0 Identification & Maintenance function as defined by PROFIBUS/PROFINET International).
Tag Function (I&M1)	Also referred to as 'Plant Designation'. It describes the function or place in the process. This field can be filled in the configuration tool of the IO-Controller.
Tag Location (I&M1)	Describes the physical location in the plant. This field can be filled in the configuration tool of the IO-Controller.

Installation date (I&M2)	The Installation date of the device. This field can be filled in the configuration tool of the IO-Controller.
Descriptor (I&M3)	Additional general information. This field can be filled in the configuration tool of the IO-Controller.
Signature (I&M4)	Signature of the device.
Manufacturer data (I&M5)	Describes the manufacturer of the interface module.
Ethernet/IP Profile	Describes the type of Ethernet/IP device

Note: Some devices report an incorrect link speed (e.g. 10 Mbps instead of 100 Mbps). Since the link speed is used to calculate the load, the reported load can be incorrect. If the reported load is very high, check the link speed in the topology overview.

8.6.3   PROFINET Features

Osiris has built-in control functions specifically for PROFINET-devices. These functions are:
- Flashing the LED of a device
- Change or Clear the device name
- Change or clear the IP settings of a device (IP, netmask and gateway address)
- Perform a complete factory reset of the device

To use these features, a 'PROFINET Features' license is needed, and it is required to be logged in as the 'networkengineer' user. No other user can use these features; see 16.1.2.

In the Device List choose the view 'PROFINET' to see the 'PROFINET Features' button.

8.6.3.1   Flashing the LED of a device

This feature is useful during commissioning of a network. It allows easy and reliable identification of a device. Instead of checking the MAC address on the device itself, you can simply click a device in the Device List and choose 'Flash LED'. It continues to flash until you press the button 'Stop Flashing'.

8.6.3.2   Changing or clearing the name of a device

 WARNING: Changing the name of a device during Data Exchange will force it to go offline or out of Data Exchange. This can stop the PLC process!

If a name needs to be changed during the Commissioning phase or after a device exchange for example, the name can either be cleared or changed. There is also an option to store the name in non-volatile memory, to make the change permanent. A controller name cannot be changed.

8.6.3.3   Changing or clearing the IP settings of a device

If an IP setting (IP address, subnetmask or gateway address) needs to be changed during the Commissioning phase or after a device exchange for example, these addresses can either be cleared or changed. There is also an option to store the address in non-volatile memory, to make the change permanent.
Note: changing the IP address is not possible when the device is already in Data Exchange and the IP has been assigned by the IO-Controller.

8.6.3.4   Factory Reset

A device can be reset to factory defaults, for example if it has been tested and goes back into inventory.
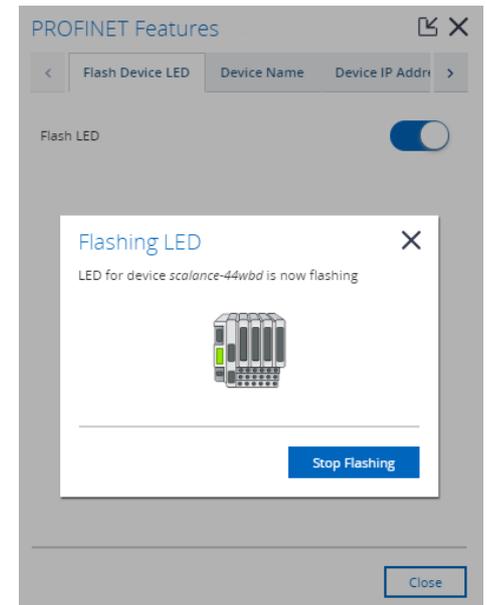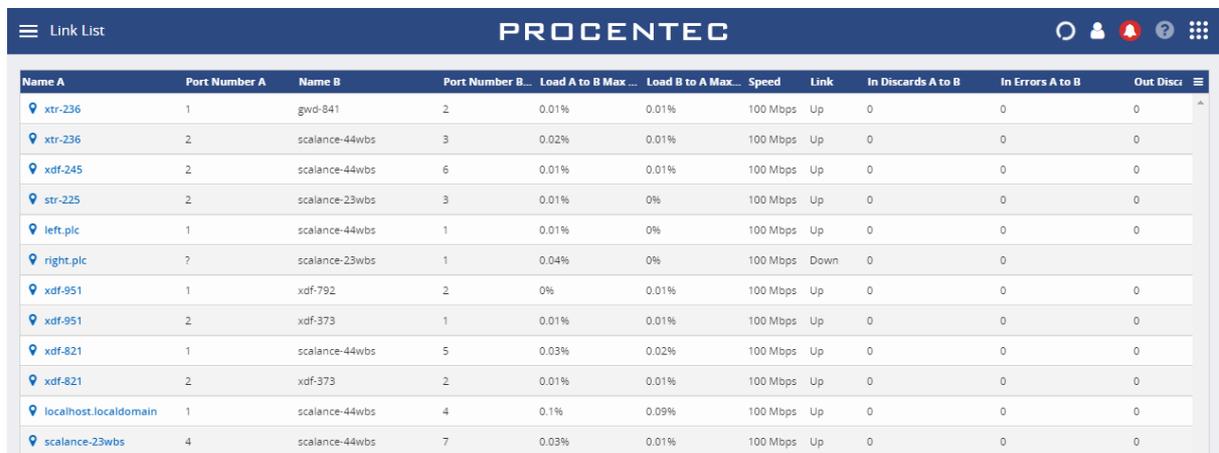
8.7 Link List

As an addition to the Device List and Topology, the Link List gives an overview of all detected connections and can display the following properties of those links:

- Name of device A and B
- MAC address of device A and B
- Port number of device A and B
- Port load from / to device A and B, last and max
- Link speed
- Link up or down
- In / Out Discards to / from A and B
- In / Out Errors to / from A and B

This list provides a complete and easy to read overview of possible link failures in the network.

The table is adjustable, by clicking on the small menu button ☰ on the right. It is also possible to drag the colums wider or narrower (in the title bar of the table), so that the screen can display more information.

The Link List is accessible by clicking on the tile on the Dashboard or in the side menu.

8.8   ComBricks Integration

Osiris can serve as a monitoring tool for one or many ComBricks sets. It can be used
to report any type of problem on PROFIBUS-level. The ComBricks measures the
physical cable or checks the telegrams, and all measurement values are sent over a
TCP-stream (port 80 only) to the Osiris platform. For more information on ComBricks
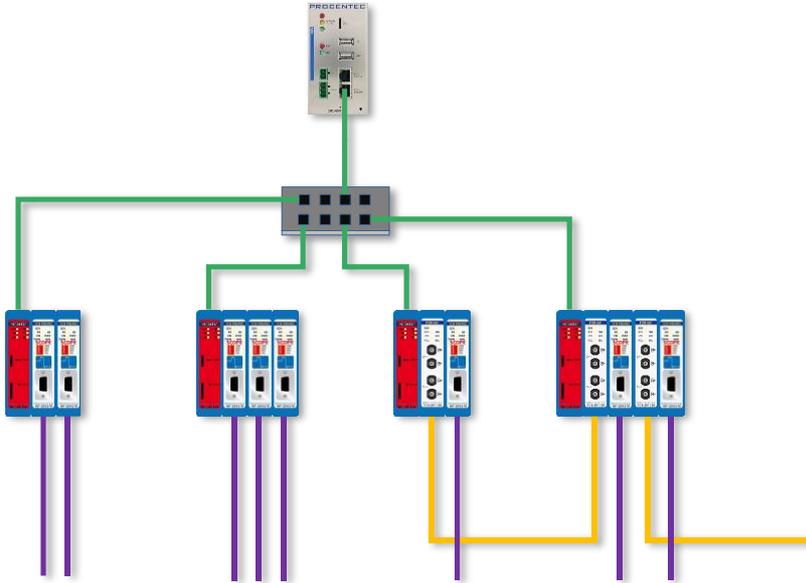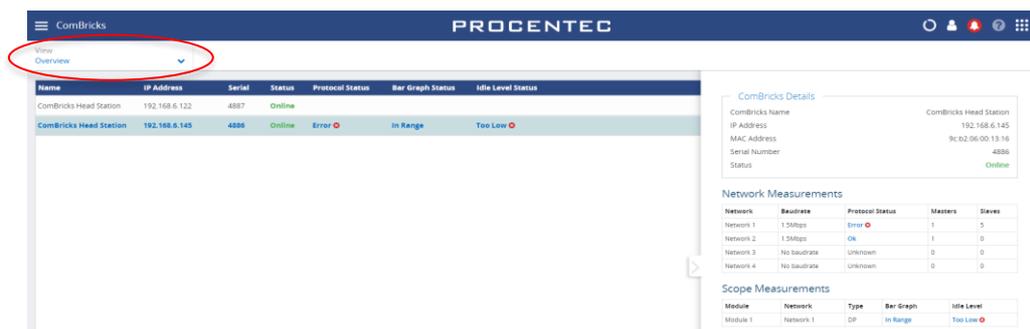see www.procentec.com/combricks.

Figure 22 - One Atlas monitoring four different ComBricks

8.8.1   Setting up ComBricks integration

Setting up the communication between Osiris and one or more ComBricks is very easy. Simply make sure that
the ComBricks Head Station is connected with an Ethernet cable in the same Ethernet network as Osiris, and
that the Head Station IP address is within the Monitoring range (see 16.3.1 how to set up the Network
Monitoring range). The rest will be handled automatically by Osiris. The only license requirement is a 1B or a 1C
license in the ComBricks. **Please note:** this feature only works when the ComBricks Web server is on the default
port 80. Currently no other ports are supported.

8.8.2   Overview

The ComBricks tile on the Dashboard gives access to all the discovered ComBricks sets within the Monitoring
range of Osiris. A brief status is provided on all found ComBricks sets in the Overview menu item:

Click a row to view more details, which will unfold on the right side of the screen.
This screen contains some basic identification information of the ComBricks, such as IP and MAC address and serial number. It also shows the networks baudrates, communication status, and number of detected masters and slaves. If the ComBricks set has one or more Scope modules, it will also show an interpretation of the Bar Graph level and Idle level.

8.8.3   Live List and Statistics

The next menu item, Live List & Statistics, shows the Live List and all details of the slaves on protocol level.
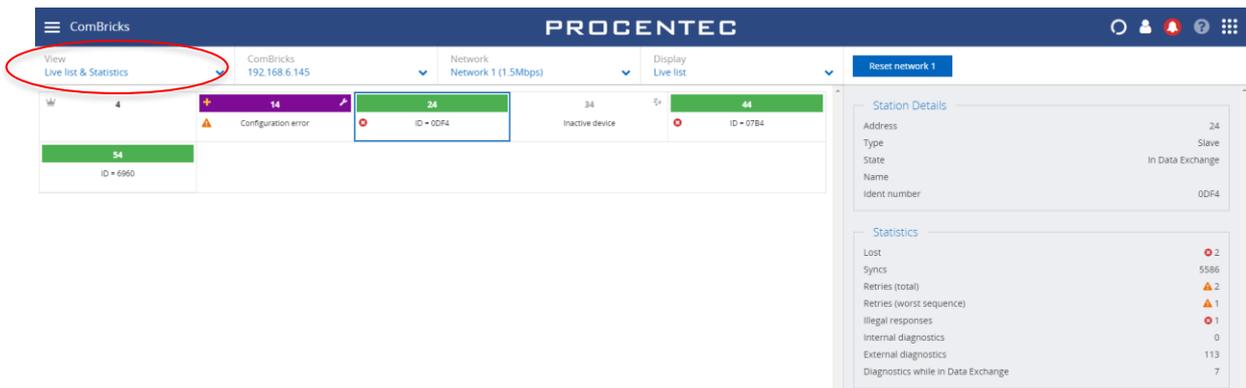
Clicking a slave shows the communication details and statistics.

   A yellow '+' appears if the device has diagnostics.
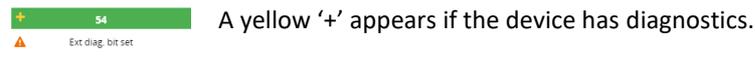
The other drop-down lists let you choose between different ComBricks sets or different networks. The last drop-down list 'Display' changes the information in the Live List from Ident numbers (if any have been read) to one of the following statistics:

- Lost
- Syncs
- Retries (total)
- Retries (worst sequence)
- Illegal responses
- Internal diagnostics
- External diagnostics
- Diagnostics while in Data Exchange

There is also a 'Reset network x' button, to reset statistics of that network. The window on the right lets you choose which items to reset; Live List stations, Ident numbers and / or station statistics.

Note: Resetting the items in Osiris will also reset these in the ComBricks.
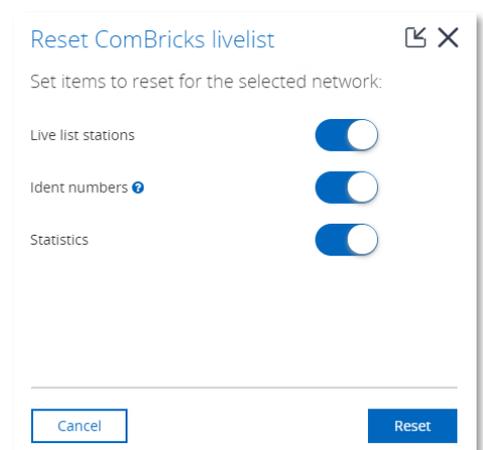
8.8.4   Bar Graph

The Bar Graph shows all devices (slaves and masters) connected to a Scope module, and displays the signal strength (amplitude) of those devices in a bar.

The bar has upper and lower limit indicators, which indicate the highest and lowest sampled amplitude.
The red line, which indicates the threshold for an alarm, can be moved up and down in the ComBricks Scope settings page.
The ComBricks unit, module and image type can be chosen from the drop-down lists.

The 'Reset module x' button can be used to clear all Bar Graph data from that module. Resetting the Bar Graph in Osiris will also reset it in the ComBricks.

8.8.5   Scope Images

The Scope Images menu item shows all devices (slaves and masters) connected to a Scope module, and displays the signals of those devices. This makes it easy to perform remote troubleshooting.

All devices on a module show in the same window.
The ComBricks unit, module and image type (Last, Min and Max) can be chosen from the drop-down lists.
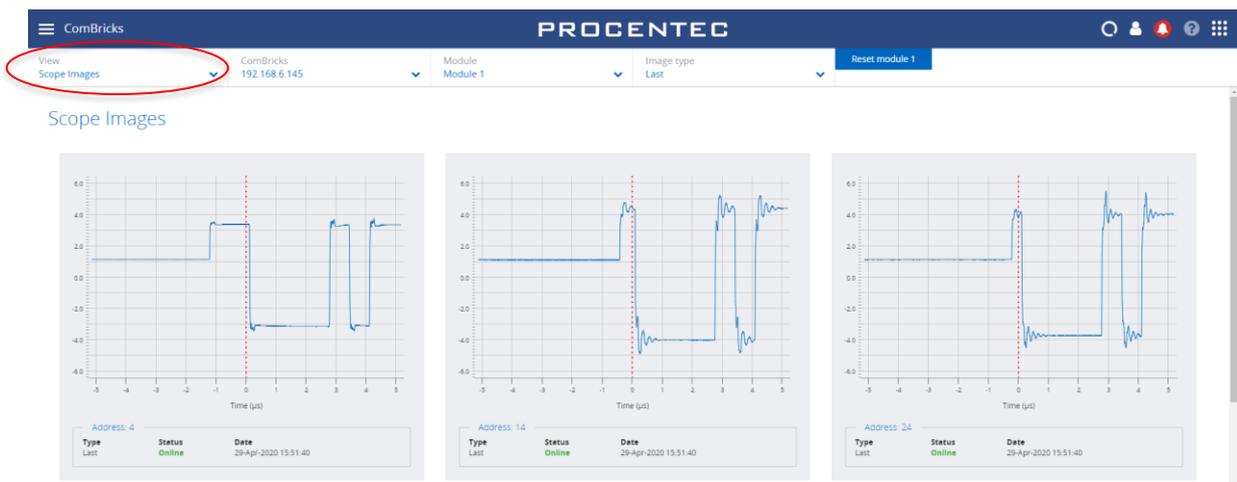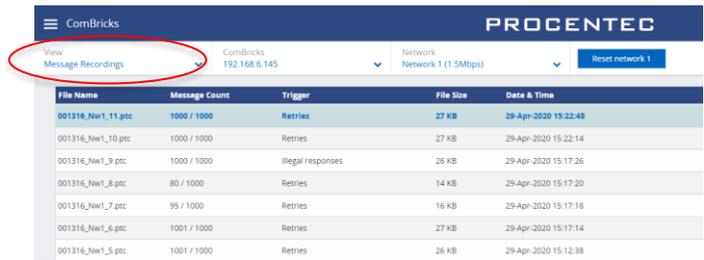

If you have a SNAP license and gateway (see chapter 12), SNAP can automatically analyze these scope images for you.

8.8.6   Message recordings

The Message Recordings menu shows a list of
all captured message files in the ComBricks.
These are recordings of messages during a
certain event. It is the same list as in 'Message
Recording' in the ComBricks webpage.

If you have a SNAP license and gateway (see
chapter 12), SNAP can automatically decode parts of the message files for you.
The 'Reset network x' lets you clear all these message files in Osiris, and you can choose if these should also be
removed from the ComBricks itself.

8.9   Trending

The Trending feature visualizes the historical data of the Q-Factor. Every 5 minutes the
Q-Factor is recorded. The minimum and maximum values of the Q-Factor during these 5
minutes are also recorded.

When you see a decline in the trend, it is safe to say the quality of the network is going
down. The steepness of the trend determines if you could schedule maintenance or if you need to act as soon
as possible. The steeper the trend becomes, the quicker you are required to act.
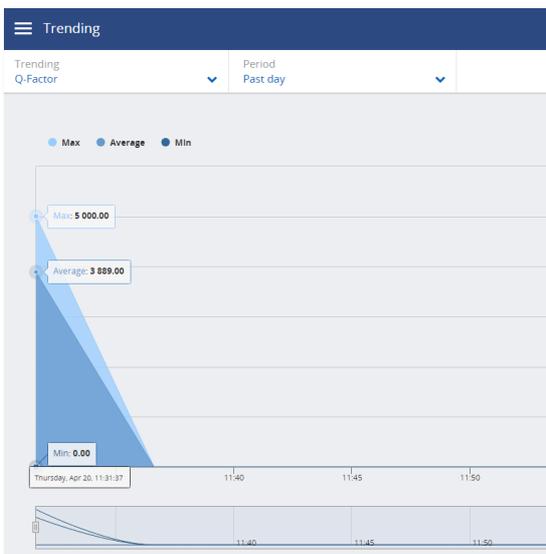
The trend also provides insight into what has happened in
the past. This could provide clues on where to look at and
what to do next to prevent it from happening again.

The legend of Trending shows the following items:

- Max: The maximum value of Q-Factor of the
  network found during the chosen period
- Average: The average value of Q-Factor during a
  period
- Min: The minimum value of Q-Factor of the
  network found during the chosen period

It is possible to select which of these values you want to
have displayed in Trending by clicking on the respective
legend items.

8.10 Report

The button for generating a Report can be found in the Application menu or by clicking the Report tile in the Dashboard. The Report feature allows you to generate a report with all relevant collected data of the network and general information:

- General network information
- Osiris information
- ComBricks overview
- Q-Factor
- Device List
- Topology
- Ignored Devices
- Traffic Light
- Firmware Differences
- TAP Analysis
- Last Commissioning Wizard results
- Security Notifications

Before generating the Report you need to fill in some mandatory details (marked in red). These details will be shown in the Report.

The Report can be customized in the following tabs:

Customize
In this tab you can choose which items are shown in the Report.
The Topology Snapshot checkbox is only available if a snapshot has been taken (see 8.3.7).
The Commissioning Wizard checkbox is only available if the Commissioning Wizard functionality was run.

Topology
Here you can preview or remove the snapshot of the image that will be included in the Report.

Logo
It is possible to insert or remove a custom logo in the report. Click the folder in the Logo tab and select an image.
The image must comply to the following rules:
- Supported image types: .png, .jpg, .jpeg, .gif
- Maximum file size: 2 MB

Please note that if you press 'Generate Report', the Report window is opened in a separate browser tab. Make sure your browser does not block opening new tabs. If you use a pop-up blocker, you can white-list the IP address of your Atlas.

8.11 OPC UA

OPC UA has been selected as the foundation of Industry 4.0 and it allows for easy integration with SCADA systems.

The OPC UA server functionality in Osiris is switched off by default.
On the OPC UA page you will see the address to connect a client to Osiris and a button to start the server. Once the OPC UA server is started the button will change into 'Stop server'. This means the OPC UA server is active.

When a connection has been established, the following information can be discovered:

- Full Device List, same as in the webserver (since version 1.1.93)
- Device information (about the Mercury or Atlas)
- Traffic Light – entire network
- Q-Factor – entire network
- PROFINET EtherTAP data
- Measurement Status
- ComBricks Measurement data

It is possible to use encrypted connections and certificates (since version 1.1.93).
It is possible to select which OPC port to use (since version 1.1.105).
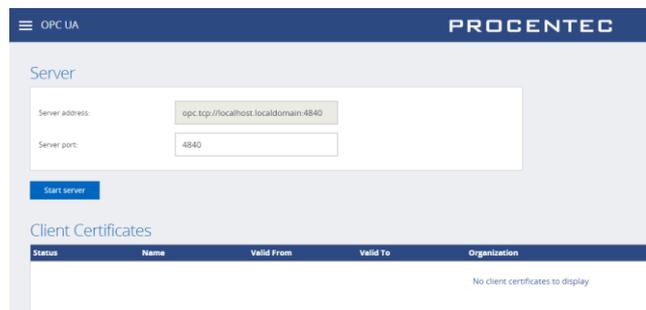
Below is an example made with UaExpert, which can be obtained from https://www.unified-automation.com/.

Before you begin, make sure the OPC UA server is started in Osiris. To start it, choose a port number (or leave it to the default port 4840) and then click the 'Start server' button.

Then open UaExpert and add a OPC UA server, according to the procedure displayed below:
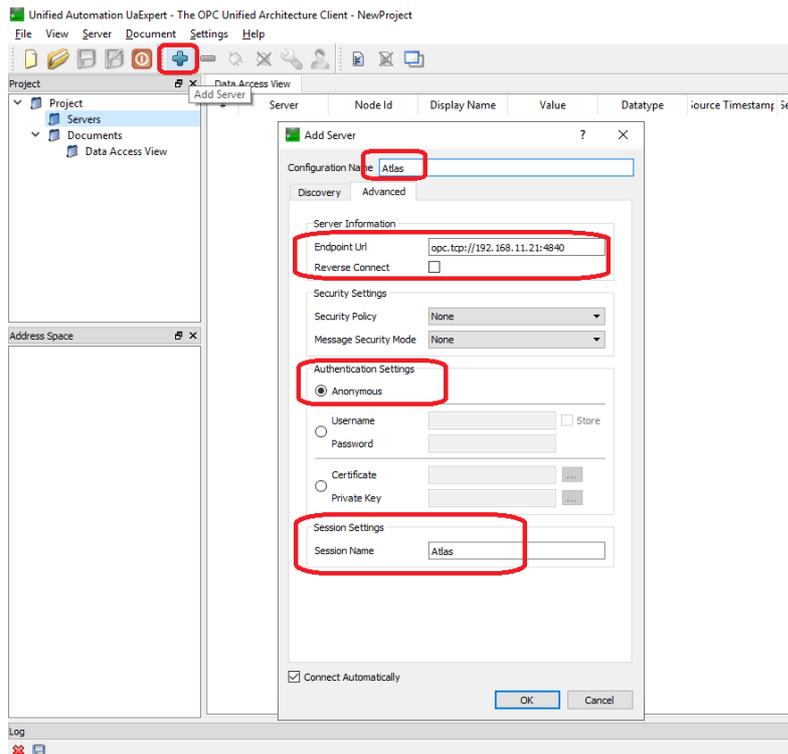
When the connection has been successfully established, you can add tags to the Data Access view by dragging and dropping the green tags on the left to the main window. Below is an example of ComBricks data tags (in blue) and some PROFINET Device data tags (in green).

8.12 MQTT

Osiris supports the MQTT connectivity protocol, which is very efficient in the sense that bandwidth usage is limited. It transports the following data from Osiris to an MQTT-broker:

- Device List (same as in the webserver)
- Traffic Light
- Q-Factor
- PROFINET EtherTAP data
- Measurement status
- Device status (of Atlas or Mercury)
- ComBricks Measurement data

The default port to connect to is 1883.

The following MQTT topics are available for subscription:

Topic	Description
/osiris/general/deviceinfo	General information regarding Osiris
/osiris/measurement/status	Status of the measurement
/osiris/measurement/ethernet/trafficlight	Status of the traffic light
/osiris/measurement/ethernet/qfactor	Q-Factor values
/osiris/measurement/ethernet/devices	Device list information

Osiris automatically subscribes to the following topic:

Topic	Description
/osiris/control/republish	When receiving data in this topic, Osiris will republish all its data to their respective MQTT Topics. Message can either be empty or have an empty JSON object. That depends on the MQTT library used by the client.

8.13 E-mail Notifications

The E-mail Notifications tile is a shortcut to the Email settings.
See paragraph 16.4.1 for more information.

9. Commissioning Wizard

The PROCENTEC Commissioning Wizard is a series of automated checks to see if the network is in compliance with the guidelines of the used protocol. The checks are based on the PROFINET Commissioning Guidelines v1.36, Ethernet/IP Commissioning Guideline v1.00 and PROCENTEC's expertise on PROFINET and Ethernet/IP networks.

Each item can be confirmed as successful or it can be declined after the checks have been performed. When the wizard has finished, an optional report can be generated. This report can also be generated later; the results are stored in memory.

9.1.1 Starting the Commissioning Wizard

Make sure a measurement is already running before starting the Commissioning Wizard; the wizard cannot run without a measurement. Also make sure to have a valid license for the protocol you want to run the wizard.

When starting the Wizard, you need to select the protocol that you wish to run the Commissioning Wizard on, and a mode. Two modes can be selected; Quickscan and Commissioning. These modes are described in the paragraphs below.

9.1.2 Quickscan

Quickscan will perform only automatic checks. No user interaction is required. Performed checks:

Check	PROFINET	Ethernet/IP
Double IP addresses	✓	✓
Firmware differences	✓	✓
Discarded packets	✓	✓
Network load	✓	✓
ARP requests	✓	✓
DCP multicasts	✓	X
IGMP multicasts	x	✓
Device names	✓	X

The Quickscan will result in a summary of scanned items, and a button to generate a report:

9.1.3 Commissioning

This wizard performs all the checks of the Quickscan and will additionally perform the following checks:

Check	PROFINET	Ethernet/IP
Topology check	✓	✓
Device details check	✓	✓
Device count check	✓	✓

At the end of the wizard you can press 'Generate Report' to create an automated report of all checked items. This is an HTML based report and can be directly printed from the browser or exported to PDF (you need to install a PDF generator first). You can also save as an HTML page. This Report also contains a section called 'Visual Inspection' with items that can be manually filled in later.

The Report can be customized; customization features are explained in detail in paragraph 8.10.

10. EtherTAP

10.1.1 EtherTAP – Message Analysis

The EtherTAP – Message Analysis feature allows you to do deep analysis of network traffic by placing an EtherTAP between devices exchanging traffic (usually between a Controller and the first switch).

EtherTAP - Message Analysis

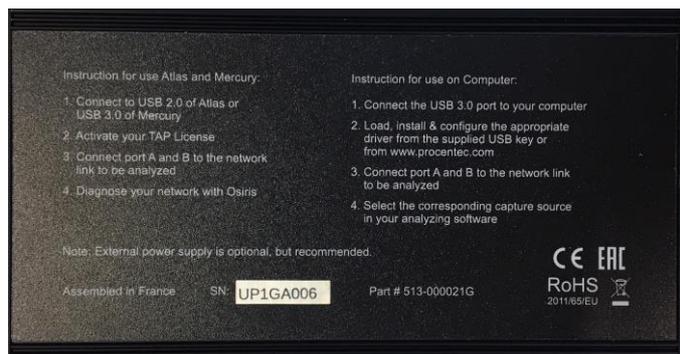TAP connected

To make tapping available make sure you have:
- A correct license
- An EtherTAP placed between two devices communicating (between a Controller and the first switch).
- A running measurement

10.1.2 Supported EtherTAP types

The supported EtherTAP types are:
- EtherTAP 10/100 (Product code 513-00011A)
- EtherTAP 1G (Product code 513-00021A)

The product number can be found on the back of the EtherTAP as depicted in the image below. Other TAPs cannot be used.

10.1.3 How to start using the EtherTAP

The EtherTAP must be connected with the supplied USB3 cable. A USB2 cable cannot be used. The USB3 cable can be connected to any port of the Atlas or to the USB 3.0 port of Mercury (on the right side), Atlas2 Plus and Atlas2. Note: do <u>not</u> use the USB 2.0 port on Mercury.

For Mercury and Osiris as a Software: Only plug in the EtherTAP USB cable after Osiris has completed booting. Otherwise the EtherTAP will not be recognized correctly.

The two RJ45 ports of the EtherTAP must be connected as follows: one cable between the Controller and the EtherTAP, and one cable between the first switch and the EtherTAP. This switch port should <u>not</u> be a mirror port.

Installing the EtherTAP means that you need to disconnect the Controller, and all the network communication will stop! Make sure this is done only with permission.

NOTE: the RJ45 connector of the scanning port of the Atlas or Mercury must <u>also</u> be connected. If this is done correctly, you should see a tile in the Dashboard with the message '**TAP** *connected'.* The tile already shows a general status of the network. Click the tile to open the EtherTAP information page.

Tapping is divided in PROFINET-specific data, Ethernet/IP specific data and generic Ethernet data. The top-left drop-down bar lets you choose the protocols.

10.2 PROFINET analysis

10.2.1 Network overview and device details

The Tapping for PROFINET requires a PROFINET Tapping license.

The PROFINET overview page lets you read out four types of data:
1. **The cycle time per device**
    PROFINET devices send data on a very periodic basis, these are called cycle times. Cycle times are defined in milliseconds.
2. **Positive and negative message jitter as a percentage of the cycle time**
    Jitter is the deviation of a message from the intended cycle time. Example: if a device sends a message every 4ms, then a delay of an additional 4ms leads to a jitter of 100%. In case the message is 1ms early then a jitter of 25% is being reported. Both messages which are early and late are reported in percentages. If the jitter percentage is 50% or higher, a ⚠ icon will appear.
3. **The number of Dropped Packets**
    Dropped packets are PROFINET messages which were missing in the communication cycle. Healthy PROFINET networks should never drop messages, too many consecutive dropped packets can cause the stop of the network. If there are 1 or more dropped packets, a ❌ icon will appear.

4. **The number of Alarms**
    PROFINET alarms are specific error messages sent by the controller or the devices using the PROFINET protocol. If there are 1 or more alarms, a ❌ icon will appear.

The image below shows the complete overview of all devices in the network, with the details described above:
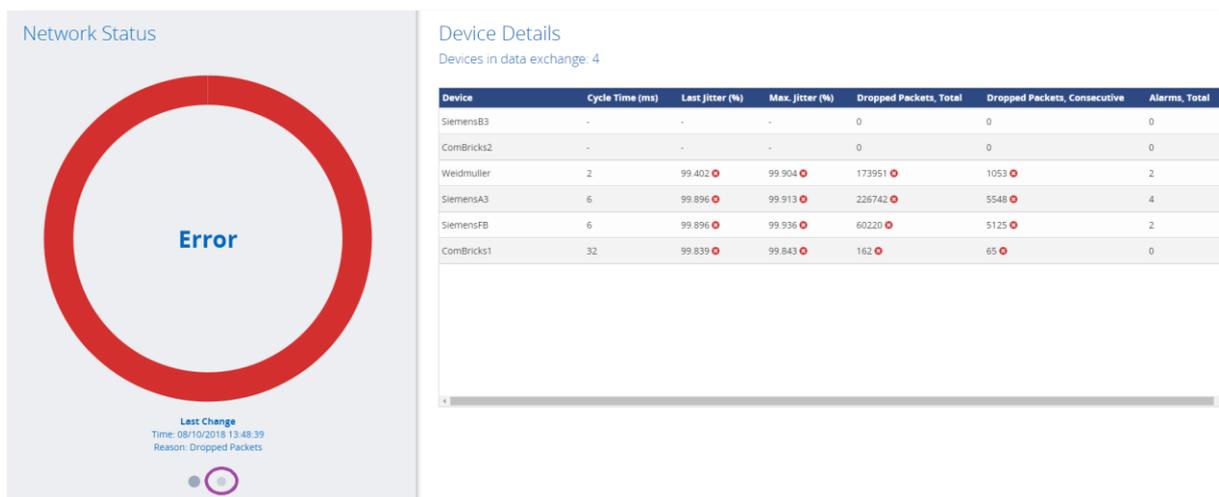
In case of errors, the large circle turns red as shown in the image. The right pane is a list of PROFINET statistics and errors per device.

By clicking the gray dot (encircled in purple) the left panel shows more details about the network:
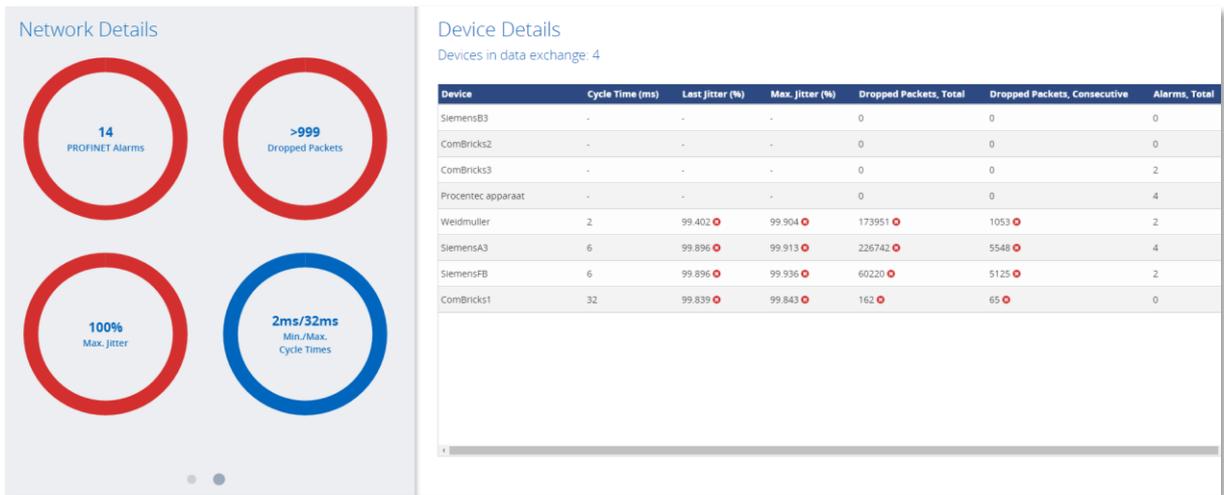
By clicking on one of the circles you can filter which columns are shown in the table on the right.

The Connection Details table can show the following icons in case of problems:
- ⚠ Jitter is 50% or higher
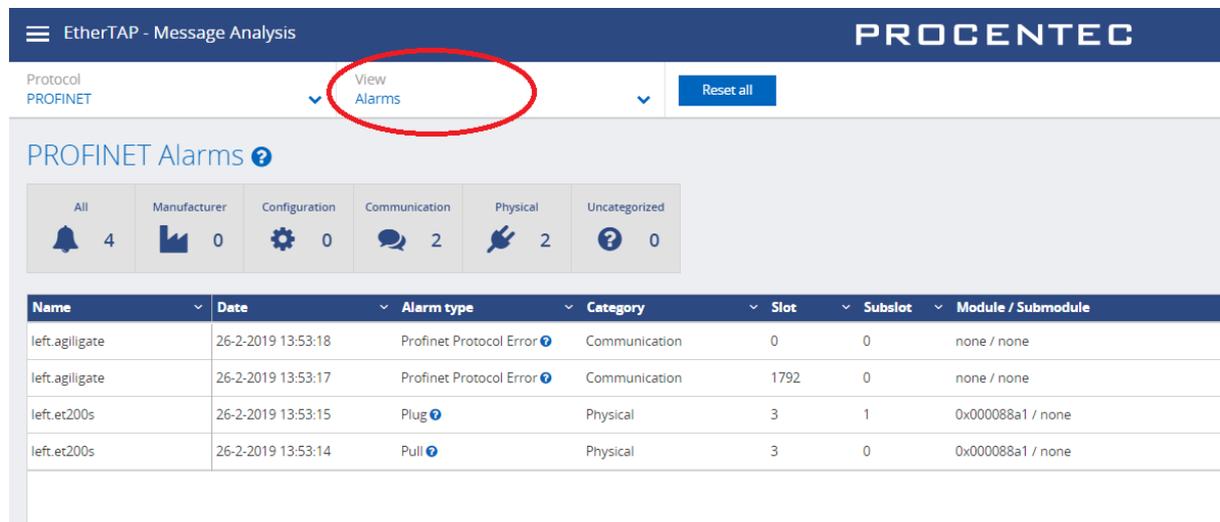- ❌ 1 or more PROFINET Alarms have been registered
- ❌ 1 or more dropped packets have been registered

10.2.2 Alarms

Clicking the 'View' pulldown menu lets you switch to the PROFINET alarms overview:

This view gives specific information about different types of PROFINET Alarms. By clicking the icons in the gray bar you can filter different types of alarms.
You can click on the question mark near the Alarm type in order to get extra information about the alarm from Delphi.

10.2.3 Message Recording

Osiris records Ethernet packets when something is wrong in the network. Recording is done in the .pcapng format, which allows easy opening in Wireshark.

Three triggers (events) can be used to record a message file:
- PROFINET Alarms
- Jitter too high
- Dropped PROFINET packets

In this overview you can see the filename and a recorded date and time, the event that triggered the recording, and a button to download or delete the recorded file.

It is possible to store up to 100 .pcapng files in Osiris. After 100 files the recording of messages will stop until the files are deleted. The number of recorded messages is shown in the top right corner of the screen.

10.3 Ethernet/IP analysis

10.3.1 Network overview and details

The Tapping for Ethernet/IP requires a specific license.

The Ethernet/IP overview page lets you read out six types of data:
1. **Connection ID**
   Every implicit CIP connection has a unique Identifier.
2. **I/O**
   The data of an implicit CIP connection can be inputs or outputs.
3. **The packet interval per device (API)**
   Ethernet/IP devices send data on a very periodic basis, these are called packets intervals and are defined in milliseconds.
4. **Positive and negative message jitter as a percentage of the packet interval**

Jitter is the deviation of a message from the intended packet interval. Example: if a device sends a message every 4ms, then a delay of an additional 4ms leads to a jitter of 100%. In case the message is 1ms early then a jitter of 25% is being reported. Both messages which are early and late are reported in percentages. If the jitter percentage is 50% or higher, a ⚠ icon will appear.

5. **The number of Dropped Packets**
   Dropped packets are Ethernet/IP messages which were missing in the communication cycle. Healthy Ethernet/IP networks should never drop messages, too many consecutive dropped packets can cause the stop of the network. If there are 1 or more dropped packets, a ❌ icon will appear.
6. **The status of Connections (active/dead)**
   Dead connections can be due to the loss of too many consecutive messages, a device has been switched off or the scanner/adapter closed the connection (i.e. new configuration, inhibit a module, etc.) If there are dead connections, a ❌ icon will appear.

The image below shows the complete overview of all devices in the network, with the details described above:

In case of errors, the large circle turns red as shown in the image. The right pane is a list of Ethernet/IP connections with statistics and errors.

By clicking the gray dot (encircled in purple) the left panel shows more details about the network:

- By clicking on one of the circles you can filter which columns are shown in the table on the right.

10.3.2 Message Recording

Osiris records Ethernet packets when something is wrong in the network. Recording is done in the .pcapng format, which allows easy opening in Wireshark.

Three triggers (events) can be used to record a message file:
- Jitter too high
- Dropped Ethernet/IP packets
- Dead connections

In this overview you can see the IP address of the involved device, the Connection ID, the I/O type of the connection, a recorded date and time, the event that triggered the recording, the file name, and a button to download or delete the recorded file.

It is possible to store up to 100 .pcapng files in Osiris. After 100 files the recording of messages will stop until the files are deleted. The number of recorded messages is shown in the top right corner of the screen.

10.4 Ethernet analysis

10.4.1 Overview

Select 'Ethernet' as the protocol in the top-left drop-down bar to view the Ethernet statistics.
These statistics are collected by the EtherTAP of the link it is currently monitoring.
Here is possible to analyze the amount of Network load and communication errors happening on the Ethernet link with the timestamp of the last change.

The EtherTAP has a Port A and Port B, which are separately listed, each with their individual statistics.

Click the blue Question Mark '?' sign for detailed information about the shown statistics.
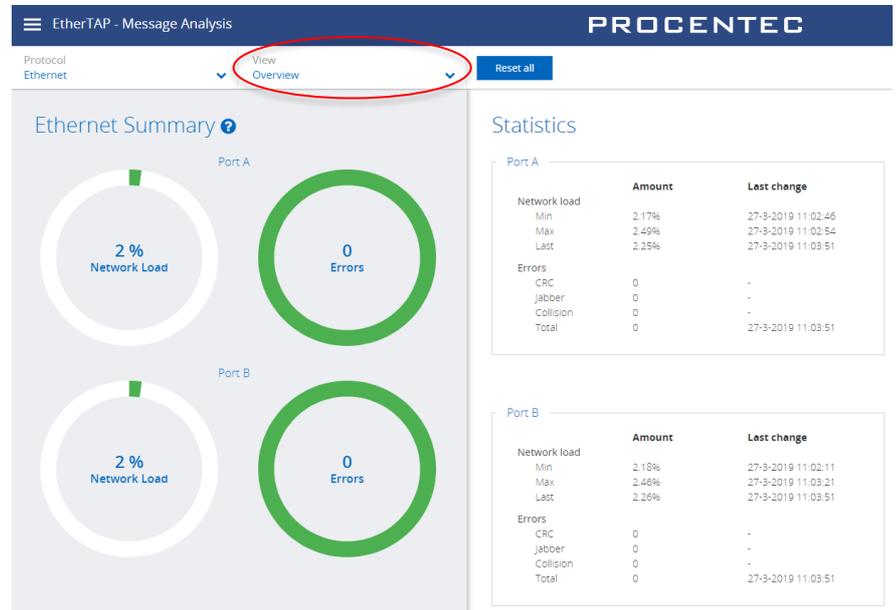
10.4.2 Trending

The information displayed in the previous chapter can also be displayed in a trending graph. This makes it clear to see when problems occurred, or when load was abnormally high or low.

The Min, Max and average load can be enabled for each port. Trending is keeping in memory the last 2h of communication, and a new sample is added every second. For detailed information refer to the Delphi Help, by clicking on the question mark '?' sign.
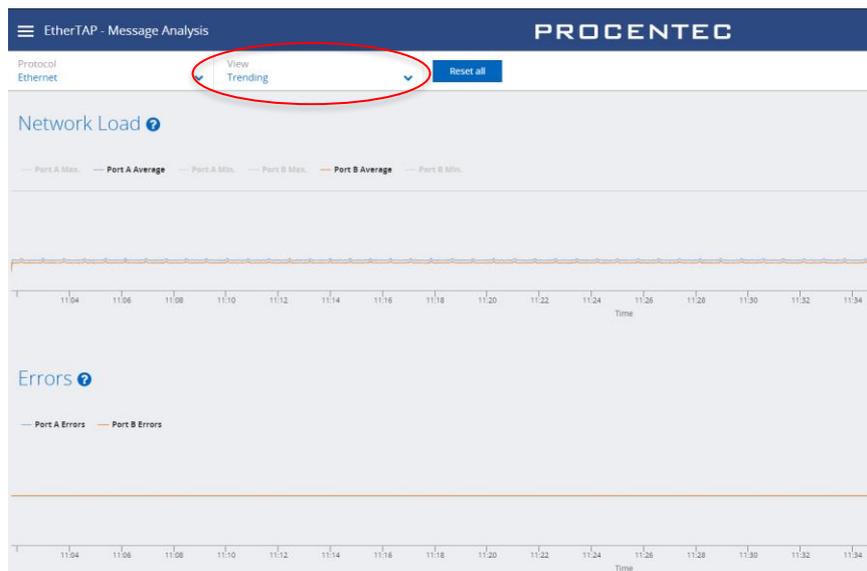
11. EtherCAT Diagnostics

The EtherCAT tile on the Dashboard makes it possible to diagnose EtherCAT networks. No special hardware is needed; Osiris makes use of the diagnostics port of the EtherCAT master.

To work with EtherCAT diagnostics, make sure you have:

- Osiris version 1.115 or higher
- An EtherCAT license for Osiris
- An EtherCAT controller with enabled Profile for Master Diagnosis Interface (ETG.1510)
- The EtherCAT controller master diagnostics port connected to the Factory network of Atlas/Mercury, within the network monitoring range of Osiris (see 16.3.1)
- A running measurement

11.1 Setting up the EtherCAT master for Diagnostics

In this chapter Twincat 3 is used as an example, other EtherCAT controllers can be connected if the support the required Profile for Master Diagnosis Interface (ETG.1510)
When using Twincat, version 3.1 build 4022.28 or higher is required.

In the Settings menu of Osiris, under 'Network' you will find an EtherCAT menu item. Here you can define the IP address of the EtherCAT Master and its Controller IP address. See paragraph 16.3.4 for more details.
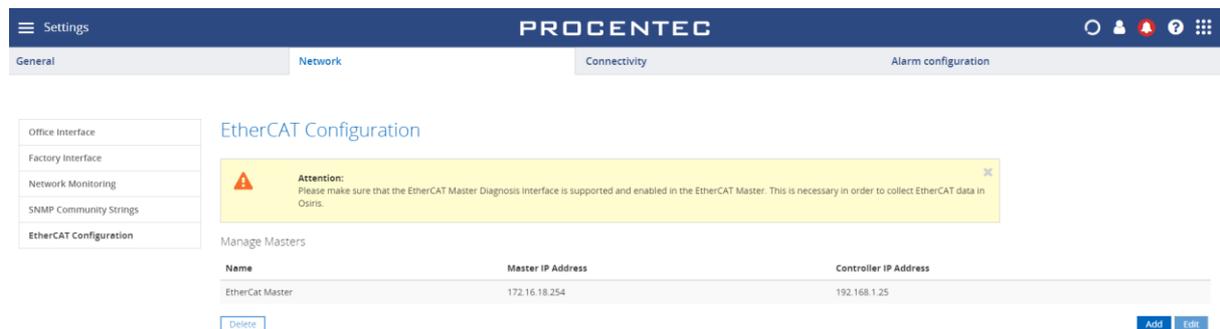
The Controller IP address must be within the Monitoring range of Osiris.

In most EtherCAT masters you can enable the diagnostics port with the help of TwinCAT 3.

1 Activate the Mailbox Gateway functionality in the master. (Red)

2   Activate the IP routing in the TwinCAT controller (Blue)
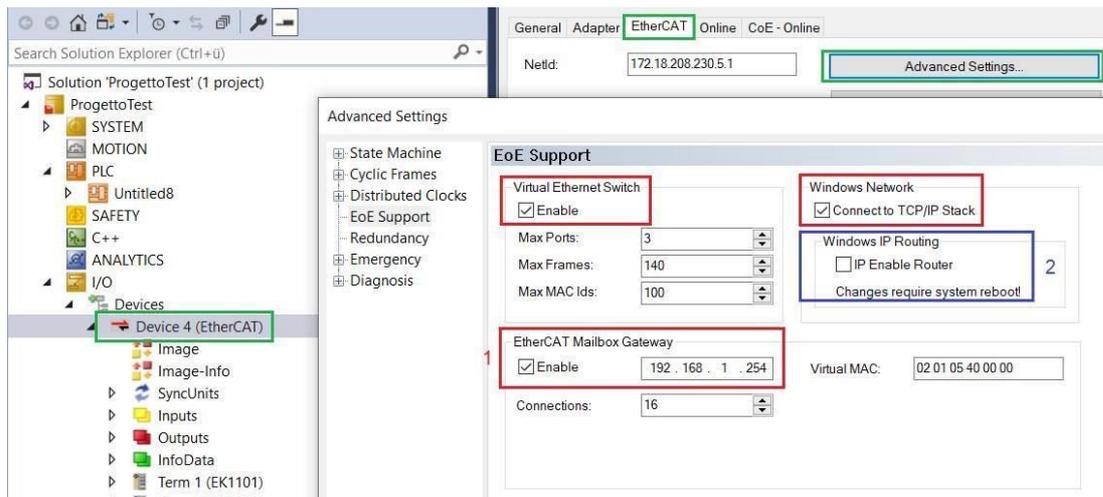
The IP address of the Mailbox Gateway/Diagnosis Interface in TwinCAT belongs to the subnet of the EtherCAT master interface, not to any LAN ports of the controller PC. The IP address of the master itself is also the gateway address to its subnet.

If the port is not open, or if there is no connection to the Diagnostics port for any other reason, the status will indicate 'Status: Error' and 'Connection status: Cannot reach master'.

If the port is correctly opened and the above conditions have been met, you can click on the EtherCAT tile in the Dashboard and will see 'Status: OK' in the top right of the screen.

11.2   Analyzing the diagnostics information

Select the Master of which you want to read out the diagnostics by choosing it in the drop-down menu on the top left. There is also a Reset-button to clear all measured data from the selected Master.

An EtherCAT network consists of one master and one or more slaves. The rows in the table represent the slaves (and their modules) connected to the master in the order they are connected in the EtherCAT line. For every slave and its modules, the following information is displayed:

Address

Address of the slave.

Name

Name of the slave.

Available

Shows if the configured slave is online and located at the expected physical network position.

Invalid Working Counter An Invalid Working Counter is incremented when inputs or outputs are not handled correctly by the slave. A possible cause can be a broken or missing cable (see image below):

Invalid Frame Counter

The invalid Counter (for each port) is incremented when an EtherCAT slave receives a corrupted incoming message. A possible cause can be that cables are not properly grounded or are too closely placed at high currents and/or high voltages, which can cause EMC problems.

AL Control

The AL Control registers contains the variable Requested State. It indicates the requested state of a slave.

Bit 7	
Bit 6	
Bit 5	
Bit 4	
Bit 3	
Bit 2	Requested State
Bit 1	
Bit 0	

AL Status

The AL Status (Application Layer Status) register consists of two variables: State and Error Indication.
The slave has to be in Operational State (State = 8) to be fully operational.

Bit 7	
Bit 6	
Bit 5	
Bit 4	Error Indication
Bit 3	State
Bit 2	
Bit 1	
Bit 0	

The slave reports an error when Error Indication has a value of one. The error can be seen in the AL Status Code column.

AL Status Code

The AL Status Code (Application Layer Status Code) shows the last detected error of a slave. Possible errors can be for instance 'Temperature too high' or 'Supply Voltage too low'.
All the AL Status Codes are defined in the EtherCAT protocol enhancements document:
https://www.ethercat.org/en/downloads/downloads_B586C0F602494A808E976CC2BD492552.htm

12. SNAP

A unique feature of Osiris is the capability of analyzing and interpreting diagnostics data independently and automatically. It provides a diagnosis in words, which is easy to understand and to follow up on.

SNAP was designed to bring automatic predictive maintenance to monitored PROFIBUS networks:
The SNAP Analysis is triggered automatically when a variation of the MIN or MAX scope images or a diagnostic message are detected. In this way the cause of the problem is provided in a matter of seconds when the issue appears on a running network.

When SNAP is activated, the SNAP status of the ComBricks overview page is provided via OPC-UA and MQTT, allowing a quick integration to SCADA systems, HMIs, and other supervision tools.

The following data is automatically interpreted:
- PROFIBUS oscilloscope waveforms
- PROFIBUS diagnostic messages

For setting up SNAP, refer to paragraph 16.4.2.

12.1 SNAP Gateway

SNAP analysis is done on our servers, where the PROFIBUS data is analyzed with an advanced AI algorithm. Osiris sends the data to be analyzed to these servers though an encrypted VPN tunnel (displayed below in grey), that is established by the SNAP Gateway.
The Gateway must be accessible from the Office interface and it requires a working Internet connection. When setup properly, the Gateway automatically starts the encrypted connection to our servers and sends the measurements.
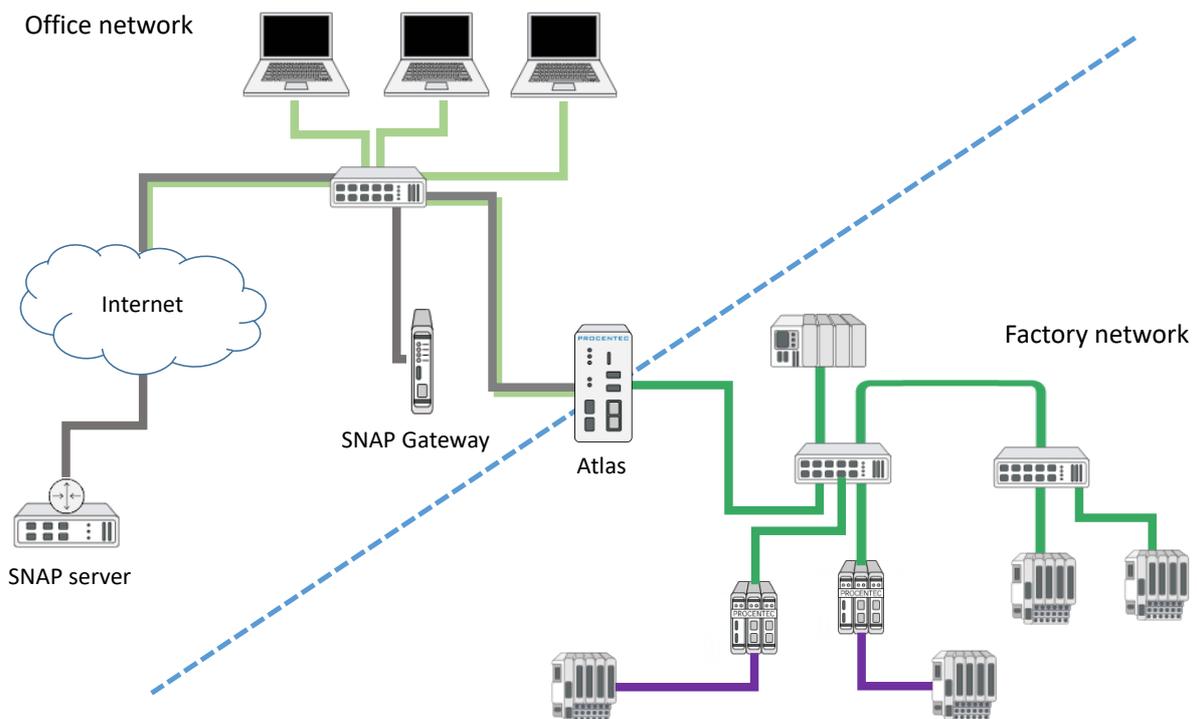
12.2 SNAP: PROFIBUS scope interpretation

If one or more ComBricks Headstations with scope modules have been found in the network, Osiris will request oscilloscope data from these. The ComBricks overview page shows if errors have been found in them by SNAP.

Clicking a line will bring up the corresponding ComBricks details:

The Scope Measurements in the Details panel indicate some problems in Network 1, module 1, 3 and 4. In module 4 for example, the analysis is 'Too many terminations'. Clicking this line opens the SNAP analysis:

In the circle you will find the most likely problem, with a percentage to indicate the certainty of the analysis. The small ? button after each possible problem takes you to the Delphi help text explaining how to fix that problem.

The 'Analyzed images' show the images that have actually been sent to the SNAP servers for analysis. Below the image you can find the distance from this device to the detected problem in meters.

Below the circle are three grey dots, indicating that there are more analysis pages. Clicking the second grey dot

shows a summary of all possible detections, a percentage of certainty and a timestamp of the last analyzed message.

The third grey dot shows all the details of the source of the images; ComBricks name, IP address and module slot number.

12.3 SNAP: PROFIBUS message decoding

SNAP can decode all standard diagnostic messages and can include useful customer specific data coming from an extensive database of devices.

If a ComBricks Headstation has recorded a message with PROFIBUS diagnostic data that can be analyzed, the diagnostic data will automatically be sent to the SNAP servers where the analysis takes

place.

After clicking a file, the analysis result appears on the right side of the screen. In the example above, the standard diagnostics has been analyzed, SNAP found the Identification number of the device in the database and shows the device name as additional information.

In the below example more information is shown about another problem; the configuration is not correct. Multiple types of PROFIBUS and Device specific messages can be decoded.

13. Security Center

The Security Center consists of a set of tools within Osiris to monitor network assets deployed in the field, protecting them from accidental or intentional changes from people who are present at the physical network. There are engineers performing work on a system, not intentionally trying to change or damage the system, but also who make improper changes to devices. This can lead to situations where the system is open to attacks, and could ultimately fail and stop.

The Security Center enables you to easily understand there is a possible attack or threat from someone at the operational network. It will utilize our existing hardware and software resources to raise an alarm when inappropriate changes occur, so they can be addressed appropriately and in a timely manner.

If there are any Security Notifications, you will see a shield in the Notification icon in the top right of Osiris:

13.1 Quiet Hours

In the Quiet Hours section, you can set times of day where no-one is expected to work on the network, for example in weekends or night hours. If any event occurs during these Quiet Hours, a notification will be sent as a Security Event Notification.

There are several ways to select Quiet Hours in the Quiet Hours Configuration table:

Click and drag to select multiple time blocks.

Click to toggle a single time block.
- Click on a day to select all its blocks (vertically)
- Click on a time to select all its blocks (horizontally)
- Use Touch & Drag on a Touch device, such as Mercury.
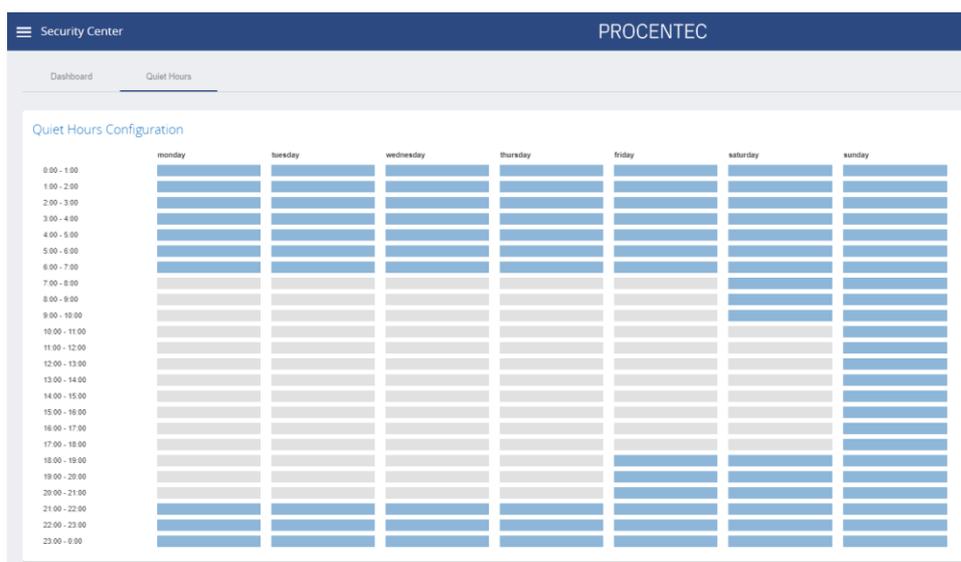
Figure 23 - Example time slots for Quiet Hours.

13.2 Maintenance Mode

To cease the Alerts generated by Osiris in case of planned maintenance, it is possible to put selected or all devices into Maintenance Mode. When this mode is activated, no Alerts will be visible in the Notification area.

It is important to realize that any changes on IO-Devices will also affect the IO-Controller, so the Controller should be put into Maintenance mode too.
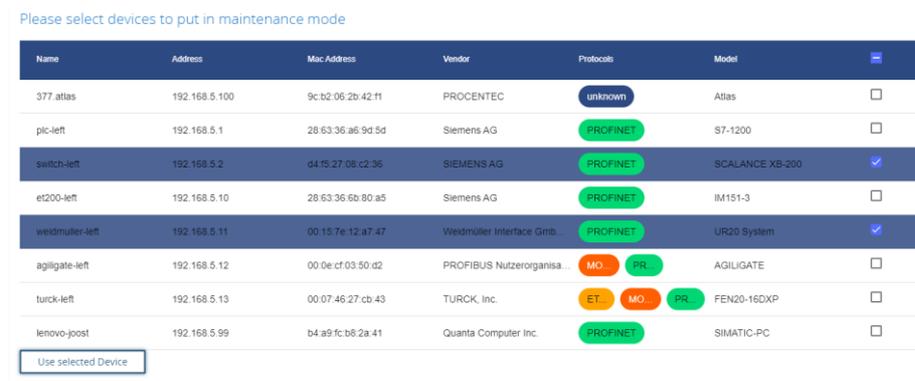
Figure 24 - Select the devices that need to be silenced during maintenance.

While the maintenance mode is active:
- Any notification about devices NOT in maintenance becomes a Security Error notification.
- Any notification about devices in maintenance becomes a Security Info notification.

If the Quiet Time is also active during Maintenance Mode, there will still be Security Alarms for the events.

13.3 SNMP Write Access Scan

While SNMP information reading is essential for good industrial network monitoring, SNMP Write access can be a security threat, as a malicious user can manipulate device configuration with SNMP messages if the SNMP Community is not adjusted. The SNMP Write Access tool scans devices for default community names and tries to write data to an SNMP object. In a secure network this should not

be possible and therefore a potential attack vector for the network. The devices in the resulting list should be changed, so that access via the mentioned community strings is no longer possible.
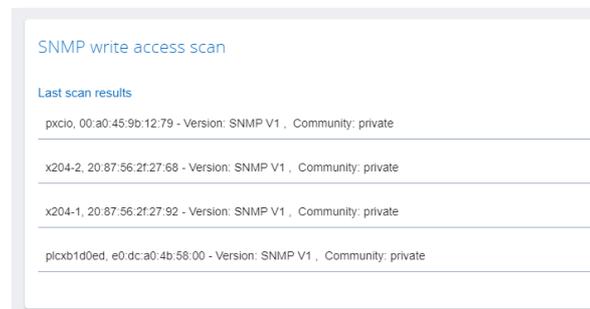
Scanning can take a few minutes, especially in larger networks.

Note: This functionality will use SNMP messages to the devices in the network, it is recommended to run this test when these type of messages on the network will not disrupt the process communication.

13.4 Port Scan

This tool scans devices for the most common open ports and tries to initiate communication on those ports. In a secure network this should not be possible, it is a potential attack vector for the network. The devices in the resulting list should be changed, so that access via the mentioned ports is no longer possible.

Currently, the Port Scan probes the following ports:

Port	Service
21	FTP
22	SSH
23	Telnet
25	SMTP
43	WHOIS
53	DNS
69	TFTP
80	HTTP
443	HTTPS
515	LDP
3306	MySQL
3389	RDP
5432	PostgreSQL
5900	VNC
5938	TeamViewer

The list will show devices with Device name, MAC address, and ports that are open.
Not every open port is a vulnerability, but it is important to have a clear overview of the open ports status. It is recommended to check if these services are in use or they can be disabled.

Scanning can take a few minutes, especially in larger networks.

Note: This functionality will use TCP messages to the devices in the network, it is recommended to run this test when these messages on the network will not disrupt the process communication.

13.5   Password Scan (Mercury / Osiris Software only)

It is recommended to change the credentials of switches and other devices in the network from default values to avoid attackers changing configuration via the web interface of devices.
Most industrial networks can have dozens of switches, and it becomes long and complicated to test all of them. With the Password Scan, Osiris can automatically test if the devices on the network are still using the default username/password set, such as "Admin/Admin".

Currently, the following device families are supported:
- Siemens X200 Switches
- Cisco IE2000 Switches

If you are interested to have this test for other type of devices, please contact us.

Note: This functionality will use HTTP messages to the devices in the network. It is recommended to run this test when these type of messages on the network will not disrupt the process communication.

13.6 Communication Baseline Scan

This tool scans the communication between two points for a certain amount of time. It therefore requires the EtherTAP to be connected, and in most situations, it should tap the communication between the IO-Controller and the switch. It gathers all the communication between all devices and creates a baseline, meaning that it allows all the communication it sees during the scan. This is comparable to white-listing in a firewall.

When the baseline scan has been completed, it can be viewed and edited by clicking the button 'Activate pending baseline'. The following window is presented:
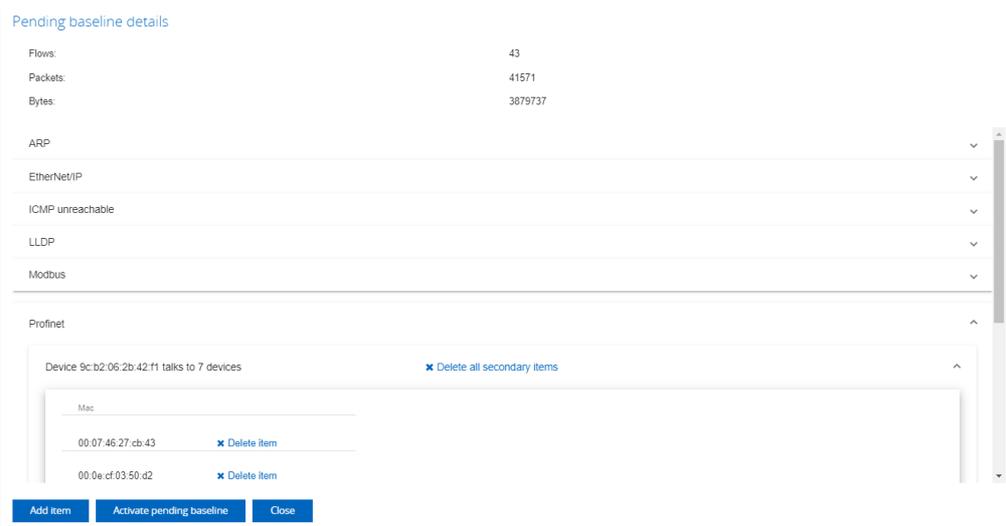
It shows all the connections, used protocols and statistics that have been observed during the baseline scan. The protocols can be expanded to view the MAC addresses that are communicating. In this window you can also add and remove items, to make sure that only the allowed devices and protocols are in the baseline scan. Adding an item requires the input of a protocol, a source, a destination MAC address and (if applicable) a source and destination IP address.

Next, click on 'Activate pending baseline'. From then on, any communication that was not seen during the baseline scan, will be considered Unauthorized, and will be displayed in the Security Notifications list (see paragraph 13.7).
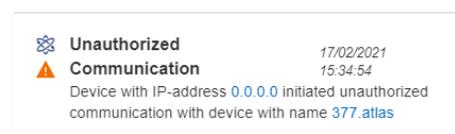
13.7 Security Notifications

The right side of the Security Center features a Notification area. Here, all notifications generated by the Security Center are displayed. These are the same as the Notification Panel (see paragraph 6.6) and the Notification Center (see Chapter 14), but without the General notifications.

14. Notification Center

The Notification Center, accessible from the tile on the Dashboard, shows the last 1000 notifications and security warnings from the start of the measurement. They are the same as in the Notification Panel, but the difference is that the items in the Notification Panel can be cleared, and that the Notification Panel only shows the last 50 notifications.
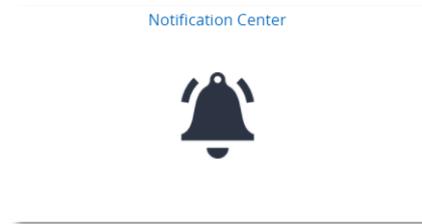
The information in the Notification Center cannot be cleared unless the 'Clear Data' feature is used.
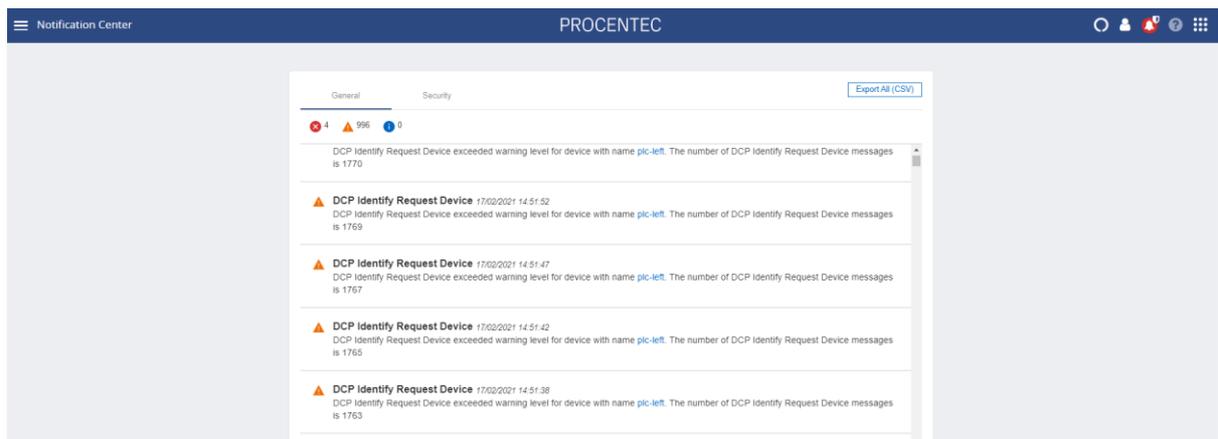
The Notification Center has an 'Export All' button to easily save all last 50000 messages in CSV format. The file will be downloaded to the 'Downloads' folder of the client system.

The icons in the General tab and the Security tab indicate the number of messages of a certain type. Clicking the icon will apply a filter for only that message type. The following types are available:

9   Maintenance related

6   Security related

0   Password and SNMP related

0   Quiet time related

0   Security error related

15. Device mode: PROFIBUS (Not available on Atlas)

To begin using Osiris in PROFIBUS mode, first make sure to connect a ProfiCore Ultra to one of the USB ports of the Mercury or laptop (this feature is not available on Atlas). When the Mercury, PC or laptop has been set up and connected, start a new measurement by clicking on the round progress indicator in the System Buttons area, and click 'Start'.
To indicate the measurement is running, you will now see a spinning progress indicator.
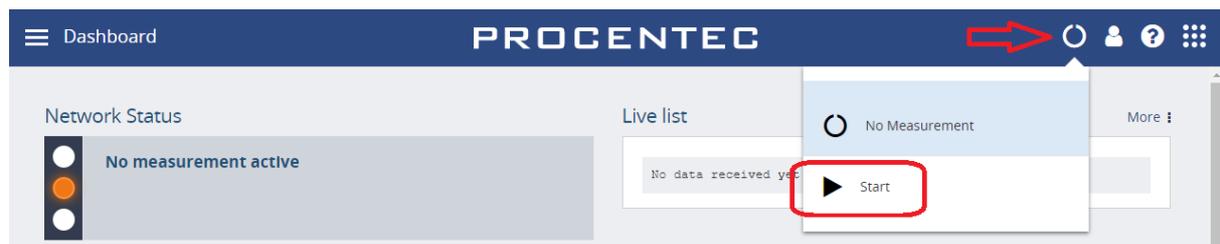
For each menu item, the Delphi Help can be viewed by pressing the   [?]   button.

15.1 Dashboard

The Dashboard gives a clear overview of the Network status of the network (Traffic Light style), a Live list, and a Network summary of all collected data.

15.1.1 Network status

The Network Status indicator or Traffic Light will turn yellow or red if problems or errors occur. The errors that have occurred can be found in the 'Device errors' tab.

When the PROFIBUS network is running without any problems, the Traffic Light will be green. In the following situations the color of the traffic light will change:

Warning/event	Traffic light state
Idle voltage low (0,9 V to 0,3 V)	🟡
Critical diagnosis (Ext-diag)	🟡
Configuration error	🟡
Parameter error	🟡
Risk margin low (60 to 40)	🟡
Slave amplitude low (just above limit 2.5 V)	🟡
Repeats	🟡
Syncs	🟡
Idle voltage below limit (< 0,3 V)	🔴
Risk margin below limit (< 40)	🔴
Slave amplitude below limit (< 2,5 V)	🔴

Slave edge steepness below limit (< 1/16 tBit)	🔴
Illegals	🔴
Slave lost	🔴

15.1.1.1   Network summary

The Network summary gives a clear overview of currently detected network settings, statistics and measurements:

Network summary item	Meaning
Baudrate	The detected bus speed of this PROFIBUS network.
HSA	The Highest Station Address, the highest possible master node in this network.
Masters	Number of detected masters.
Slaves	Number of detected slaves.
In Data Exchange	Number of detected slaves in Data Exchange with a master.
Tslot	The maximum allowed response time for a slave.
MinTSDR	The required waiting time for a slave before it can respond. (only visible when a parameter message has been sent by the master)
MaxTSDR	The maximum time for a slave before it times out.
Tid1	Idle time; the minimum waiting time for the master before it can send a new message.
Watchdog	The safety time-out for a slave. (only visible when a parameter message has been sent by the master)
Actual idle voltage	The voltage on the bus when no node is sending.
Min idle voltage	The lowest recorded idle voltage on the bus when no node is sending.
Max idle voltage	The highest recorded idle voltage on the bus when no node is sending.

The Live List below the Network Summary is explained in detail in paragraph 15.1.1.2. To get to the LiveList, click upper left menu button.
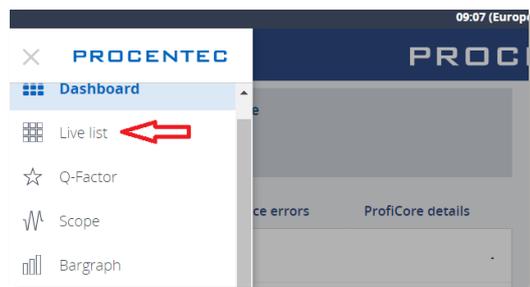
15.1.1.2   Live list

The live List in the Dashboard shows all the nodes that are present on the bus. Masters have a small crown icon, slaves have colored backgrounds if they are communicating. Below is a full list of possible indications:

Live List indication	Meaning
	Active master.
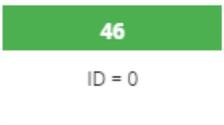
46 ID = 0	Slave in data exchange with a master, no ident number captured.
10 ID = 05FB	Slave in data exchange with a master, ident number captured.
5 ID = 0	Idle slave, not assigned to any master.
125 Zz ID = 0	Slave configured, but not reachable by the master.
10 (x) ID = 806A	This slave has been incorrectly parameterized by the master. Possibly a wrong address or a wrong GSD has been used.
36 🔧 ID = 806A	This slave has been incorrectly configured by the master, or the hardware modules in the slave are not correct.

Above the Live List is a button to control the device statistics of the Live List. The Device Statistics button default setting shows the slave model name, if the Ident number has been captured. This only occurs during master or slave startup, or when diagnostic messages are sent from the slave. Another prerequisite is that the GSD file is listed in the library of the Mercury. For more information on this, see paragraph 15.1.6.

The Live List can be 'paused' by switching the 'Auto Update' button to off. No changes will be visible.

15.1.1.3   Info Panel

Under the Live List is the Info Panel. This shows issues that have been detected on the network. If no issues have been detected, this panel will be empty . You can click on an address to see the details and any recorded problems, divided over four tabs; General, Diagnostics, Parameter and Configuration. These are shown on the following pages.
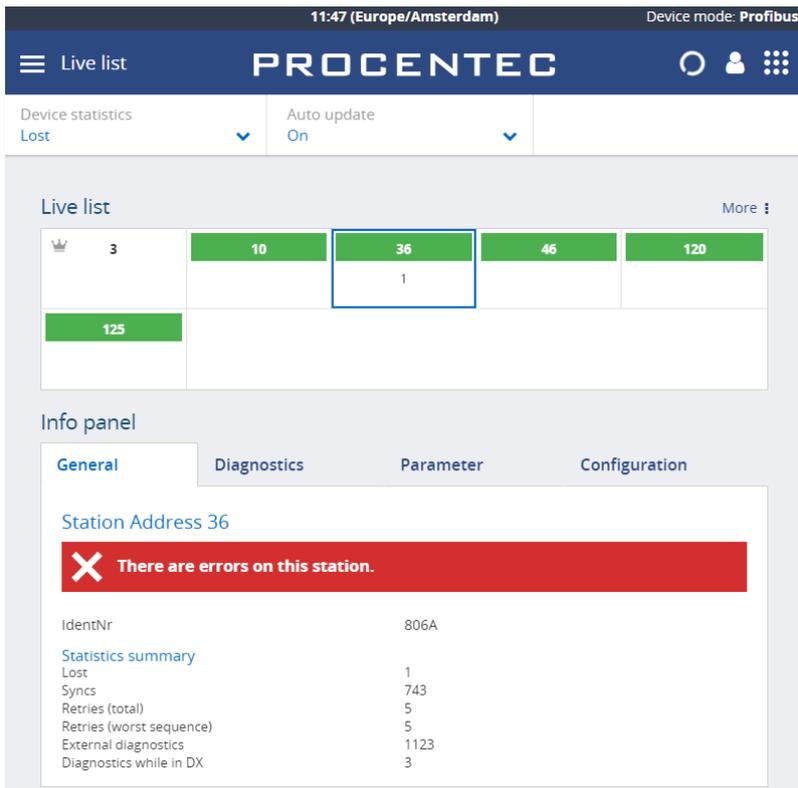
Figure 25 - General errors of the selected station
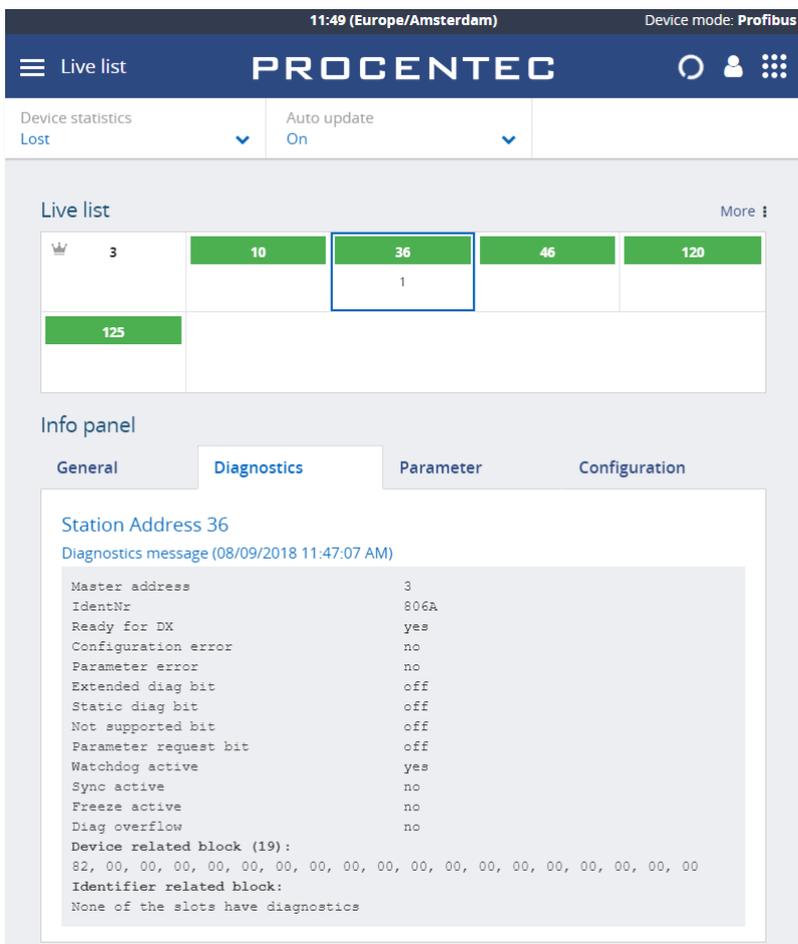
Figure 26 - Diagnostic information from the selected station

Figure 27 - Parameter information from the selected slave

Figure 28 - Configuration of the selected slave.

15.1.2 Q-Factor

The Q-Factor is a number that represents the quality of the network.

A value of 5000 is excellent and 0 is critical or unmeasurable. Additionally, a color coding is used to emphasize the severity. Normally the color should be green, meaning excellent or good. Orange is below average but not critical, e.g. attention recommended. Red means a bad, critical or urgent issue.

There are multiple Q-Factors in use in the tool:
- A Q-Factor for each network device, which indicates the quality for a single device. Calculation of this Q-Factor is based on a weight of:
  - Measured voltage, or amplitude
  - Edge steepness
  - Risk margin
- A single overall Q-Factor, indicating the quality of a complete network. Currently the overall Q-Factor equals to the lowest Q-Factor of an individual network device.
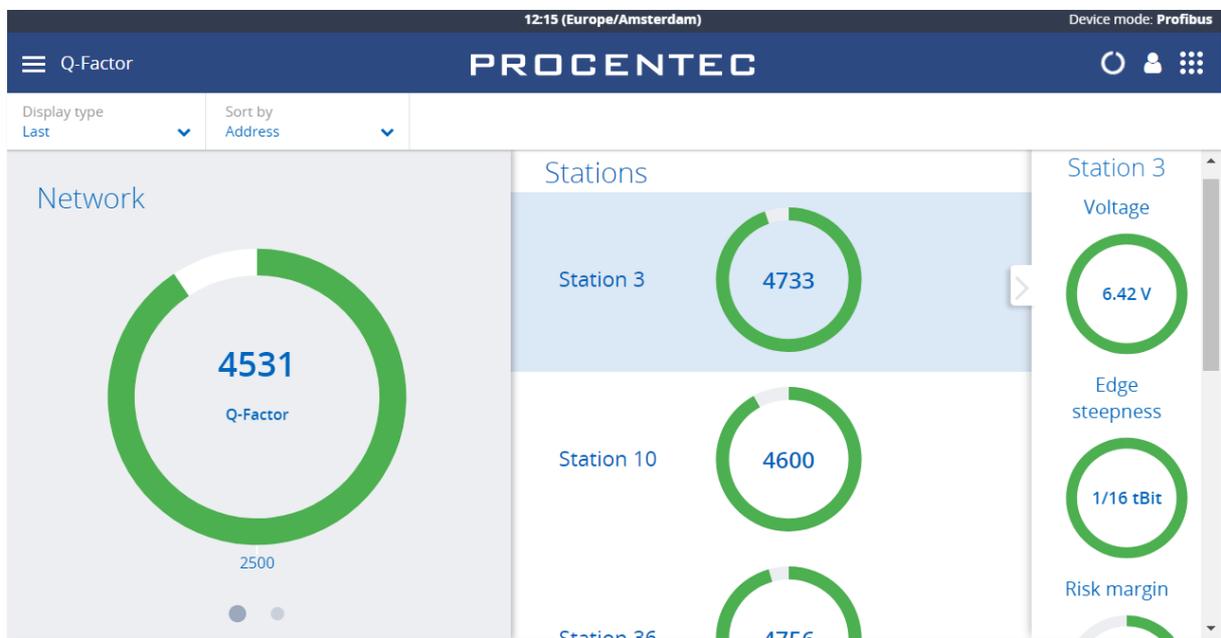
Figure 29 - The Q-Factor

The buttons on top can be used to view the last, best or worst values. Swiping the main Q-factor to the left shows a more detailed Q-factor. Clicking a station Q-factor brings up a detailed measurement column on the right.

15.1.3 Scope

The Scope view shows a detailed live oscilloscope waveform of a specific device, and is one of the most important items to check during commissioning or troubleshooting because it gives an accurate view of the health of the network.
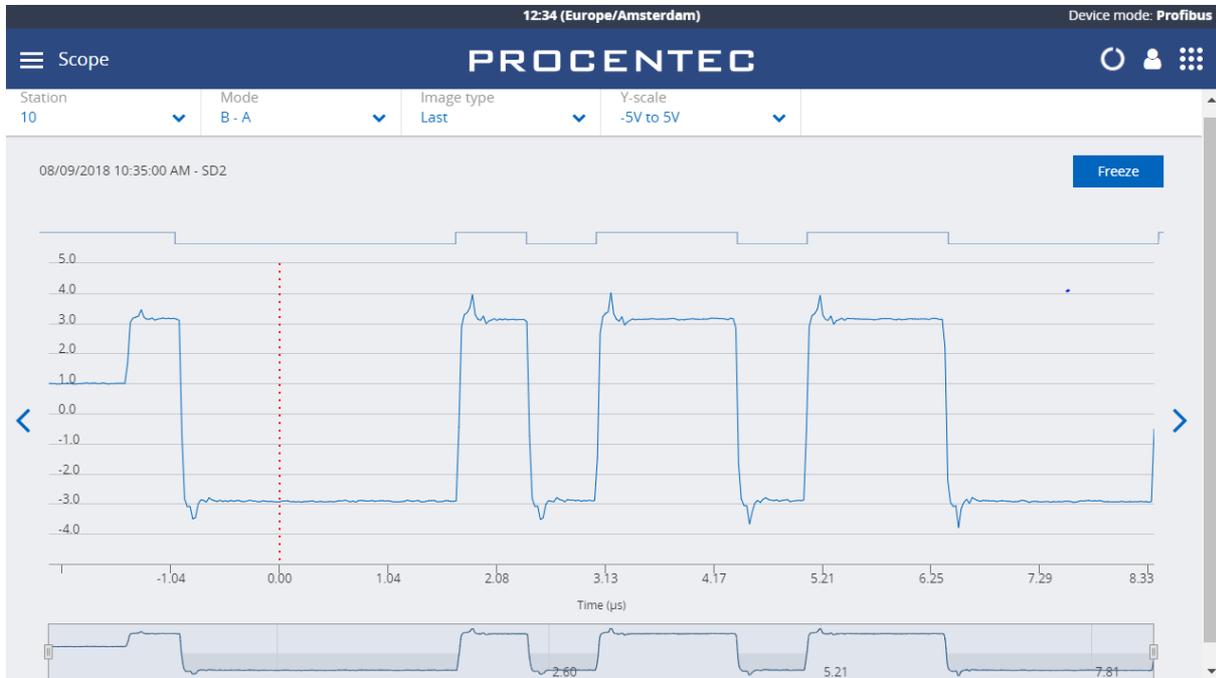
Figure 30 - Normal oscilloscope image of device 10

Use the Station selector in the top left to choose another device or use the '<' and '>' on the left and right to easily cycle through all available addresses.

The 'Mode' button lets you switch between B-A differential mode, the A or B line separately, or both A and B simultaneously. This is useful when troubleshooting a wire break, short circuit with shield or poor connection of one of the wires.

The 'Image type' button allows you to see the last, lowest (minimum) or highest (maximum) measured value. These values are stored in memory from the beginning of the measurement. Leaving the Mercury running for a longer period of time gives a good indication of the lowest / worst oscilloscope signal.
There is also an 'Error' image, this shows the last detected corrupt frame. This only works if the mode is set to 'Error' at the time of the error, so it cannot detect error signals in the background.

Above the oscilloscope image there is a digital representation of the measured signal. This can help determining if there are actual problems with the signal.

Below the oscilloscope image there is a timeline that can be used to scroll left and right in a scope image. On mercury you can use two fingers to 'pinch' the screen on the oscilloscope line, which zooms in or out. Move the timeline with one finger to scroll.

There is a 'Freeze' button on the top right to stop the screen, to be able to analyze a specific signal.

15.1.4 Bargraph

The Bar graph illustrates the average signal strength from all available devices. It is a helpful utility to get an impression of the overall signal quality of the network.

Figure 31 - Good bargraph levels

The average amplitude should be around 5 V. When there are bus problems the Bar graph will display different voltage levels and the color of the bars will change.

Each bar has a Min and Max level, indicated with blue lines on the bars. These indicate the highest and lowest measured amplitudes, corresponding with the Min and Max levels in the oscilloscope images.
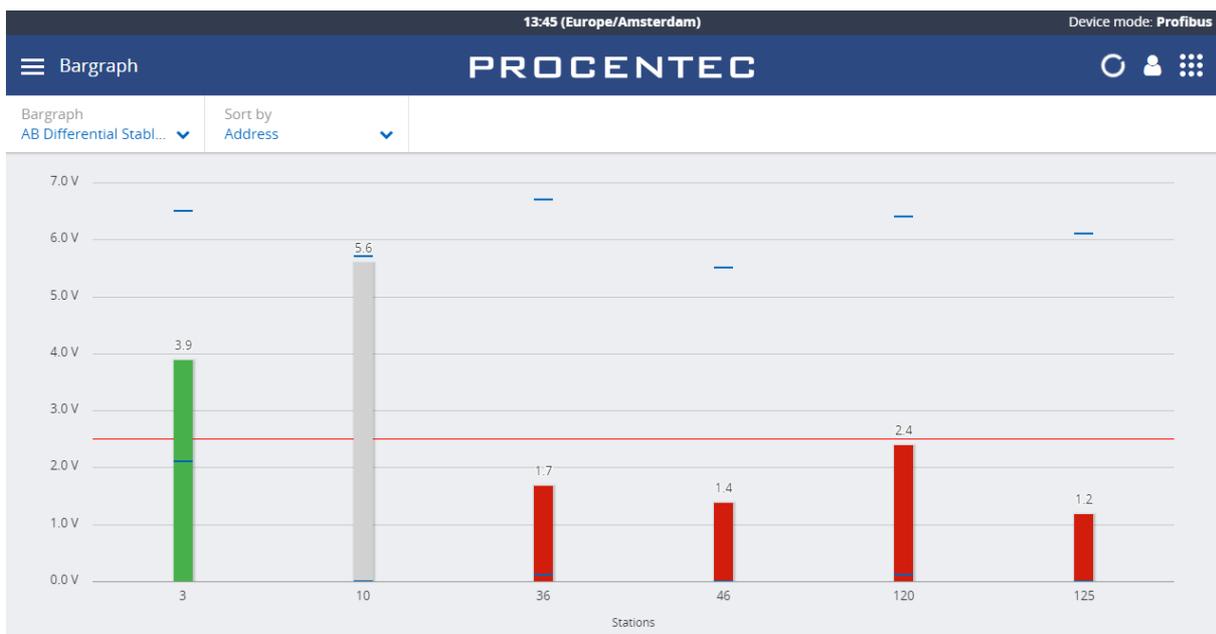
Figure 32 - Inactive and low bars

If a station is not active during the defined time-out (5 seconds), the bar of that station will become grey to indicate inactivity. This can also happen when the signal of this station is so bad that Mercury cannot decode the message.

The bars turn orange when the measured amplitude is between 2.5 V and 3 V. Below 2.5 V the bar turns red. These threshold values can be changed in the settings.

15.1.5 Messages

Message recording lets you record the actual data that is sent over the bus.
Simply press 'Record', and it will record 20000 messages and then stops recording, or press 'Stop' before the 20000 messages are recorded.

The columns have the following meaning:

Column	Description	Units
Nr.	The Nr. header specifies the line number in the respective view. This line number is independent of settings, filtering and such.	
Attention	The Attention header gives more information on the message or possible reason for a disturbance or error in the recorded message. (Messages with an "attention" message are tagged with a cross red icon).	
Idle time	The Idle Time is the inactivity between 2 messages. It refers to the time that has elapsed between the end of the previous message and the start of the current message . If the current message is a response, it is called the slave Tsdr (slave response time).	Bit Time
Delta time	This is the time from the first start-bit of the previous message to the first start-bit of the current message.	Bit Time
Address	The 'Address' column specifies the source and destination address of the message. Requests: Source -> Destination Responses: Destination <- Source	Decimal

Column	Description	Units
	An ACK message does not contain addresses, so this field will be empty.	
Msg Type	The Msg Type column specifies the higher level DP, DP-V1 and DP-V2 messages.	
Service	The Service column specifies the type of service of a message. The information is extracted from the FC byte when available (only valid for SD1,SD2 or SD3 messages).	
Type	The Type column indicates a request or response message.	• Req • Res
Frame	The 'Frame' specifies the frame type of the message.	• SD1 • SD2 • SD3 • SD4 • ACK
FC	Frame Control byte of the message.	Hex
Timestamp	The timestamp is calculated on the basis of a starting moment the user has defined and subsequent messages add to a delta-bittime to this beginning. This means that the timestamp internally consists of 2 parts: the time/date and the delta-bittimes that have passed.	
SAPs	The SAPs column specifies the source and destination SAP of the message. Requests: Source SAP -> Destination SAP Responses: Destination SAP <- Source SAP	Decimal
Length	The Length column specifies length of the user data of a message (only valid for SD2 and SD3 messages and does not include SAPs).	Decimal
Data	The Data column contains the USER DATA or Outputs and Inputs of messages.	Hex
Station	Model name of the device. Can only be displayed if the ident number was captured and the GSD is known (paragraph 15.1.6)	

15.1.6 GSD Management

Mercury features a GSD library with all relevant information from PROFIBUS slaves, such as the device capabilities, device name, manufacturer, version, diagnostic information and possible configurations. This information is used in other parts of the Mercury.

Press the Upload button to select a folder containing GSD files.
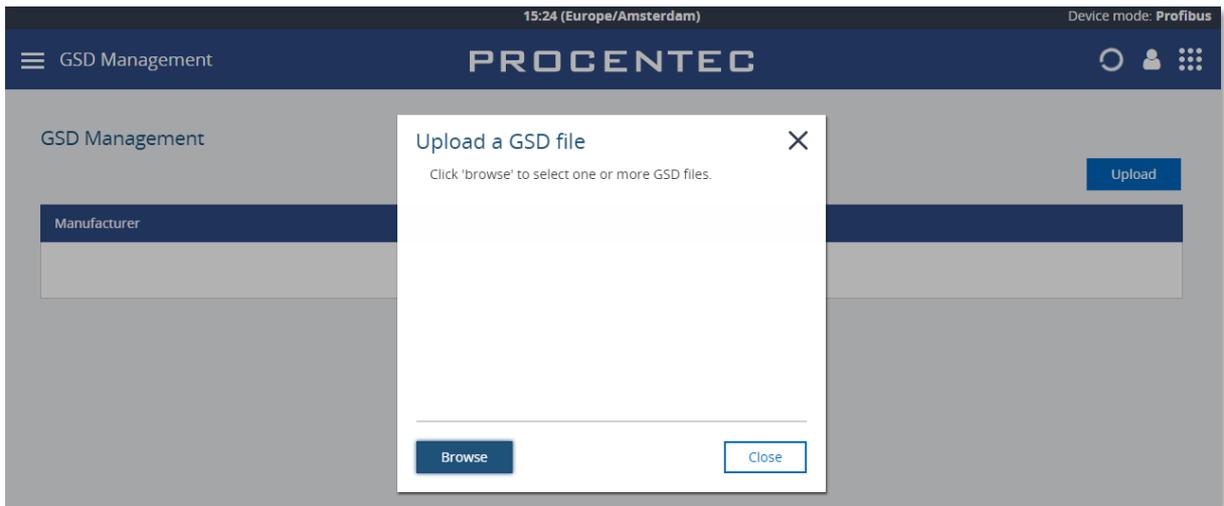
Figure 33 - Click Browse to select a folder containing GSD files

Then click 'Upload' to copy all the selected GSD files to the Mercury. Depending on the number of files, this can take some time. The Mercury automatically makes a library of all GSD files.

The GSD files are then sorted on Manufacturer name and the information in the GSDs is available in the other features of Mercury.

16. Settings

Most of the Osiris settings can be changed manually instead of using the Setup Wizard. Click the Settings tile on the Dashboard, or use the Menu button and select 'Settings'.

16.1 General

The General settings page shows the following items:
- The Device name: this is the hostname of device. It cannot be changed.
- Select your language: the interface language.
- The Network name is displayed on the dashboard.

16.1.1 User administration

Osiris can be protected against unauthorized access or changing of settings. With means of user rights administration you can control the level of authentication a certain user (or group of users) has.

The default password for an account is the same as the username. So the password for the admin account is admin. All letters are lowercase, also for the username.

The default passwords can be changed in the Settings menu. Click on the Quick Drawer Access button ☰ , click 'Settings' or double-click on the System Bar (admin only) and click on the ⚙ icon. in the 'General' tab you can select 'User from the menu on the left. Then choose the user from the drop-down list to change the password.
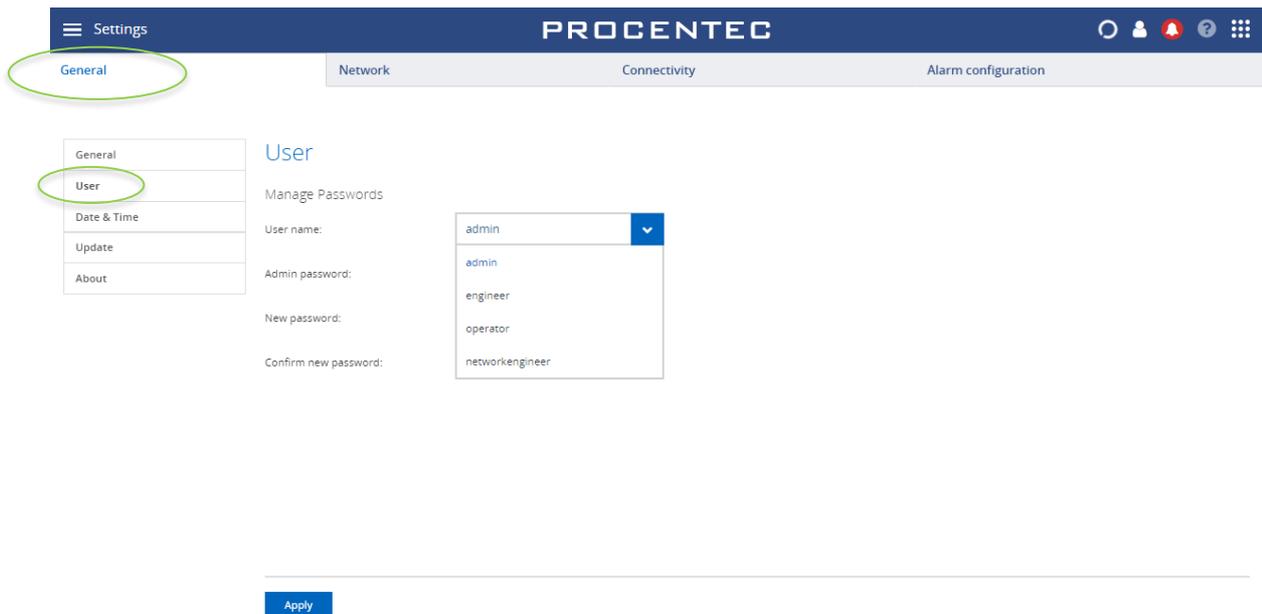
16.1.2 The account 'networkengineer'

This account, added since firmware version 1.1.105, is required for using the PROFINET Features in the Device List (see 8.6.3). It has the same rights as the 'engineer' account and is additionally allowed to use the PROFINET features.
This account is disabled by default and must be activated by entering a password for the account. Only the admin can do this.

The idea behind this approach is that this feature cannot be used without setting a customized password. The account 'admin' has an easy default password, and if this password is not changed, then anyone with remote access could also use the PROFINET features. This can unknowingly or deliberately stop a running installation.

16.1.3 Default users

There are four default usernames: admin, networkengineer, engineer and operator. They have the following rights, restrictions and capabilities for the Ethernet device mode. All user types have access rights for all the pages inside the PROFIBUS device mode.

Action	admin	networkengineer (disabled by default)	engineer	operator
View the Traffic Light	Yes	Yes	Yes	Yes
View the Notifications	Yes	Yes	Yes	Yes
View the Settings	Yes	Yes	Yes	Yes
View/use the Commissioning Wizard	Yes	Yes	Yes	Yes
View/use the EtherTAP page	Yes	Yes	Yes	Yes
View/use the Email settings	Yes	Yes	Yes	Yes

View/use the ComBricks page	Yes	Yes	Yes	Yes
View/use the Link List page	Yes	Yes	Yes	Yes
View/use the MQTT page	Yes	Yes	Yes	Yes
View/use the EtherCAT page	Yes	Yes	Yes	Yes
Clear the Notifications	Yes	Yes	Yes	No
Clear the Measurement Data	Yes	Yes	Yes	No
Customize the Dashboard (add/remove tiles)	Yes	Yes	Yes	No
View/use the Trending page	Yes	Yes	Yes	No
View/use the OPC UA page	Yes	Yes	Yes	No
View/use the Topology page	Yes	Yes	Yes	No
View/use the Q-Factor page	Yes	Yes	Yes	No
View/use the Device List page	Yes	Yes	Yes	No
Use the PROFINET features button	No	Yes	No	No
View/use the 'Factory Reset' button	Yes	No	No	No
View/use the System Bar	Yes	No	No	No
View/use the Setup Wizard	Yes	No	No	No
Edit the users and passwords	Yes	No	No	No
Edit Osiris settings	Yes	No	No	No

16.1.3.1 Password best practice

We encourage you to change the default Administrator password after purchase.

- Change the password(s) immediately after installation or at the office before it is transported to the final destination.
- Never share passwords with anyone.
- Always use strong passwords. Avoid: *test, 123456, <your company name>, <your first name>, Atlas, PROCENTEC, etc.*
- Change passwords immediately if they may have been compromised.
- If passwords must be written down, store it in a secure place and destroy it when it is no longer needed.
- Be careful about where passwords are saved on computers. Some dialog boxes, such as those for remote access, present an option to save or remember passwords. Selecting this option poses a potential security threat.

16.1.4 Date & time

The Timezone selection field allows you to select the time zone of the physical location.

Atlas only: When choosing automatic time, Osiris will try to connect to one of the given NTP servers which require internet connectivity. In case you have a local NTP server(s) then you can remove and replace these defaults servers.
In case you do not want to use automatic time, you can turn it off and manually set the time.

Note: Mercury and Osiris on laptop or PC will use the Windows time. Adjust the time in the Windows host to apply changes in Osiris too.

16.1.5 System

16.1.5.1   Enable USB ports (Atlas only)

Note: This option is only available in Atlas.

The menu item 'System' under the General tab allows you to disable the USB ports for security reasons or company policy compliance.
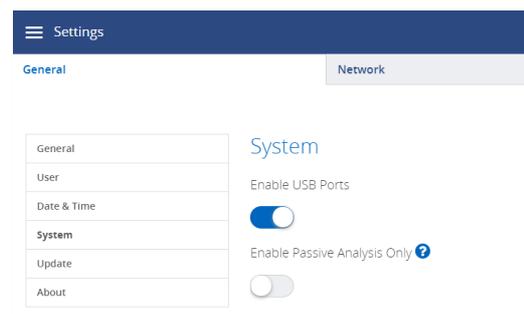
16.1.5.2   Passive Analysis Only

This feature allows the use of Osiris EtherTAP Message Analysis functionalities without sending any data on the network.

When this functionality is enabled, Osiris will only analyze the data coming from the connected EtherTAP. This allows pure passive analysis of the network without the need of connecting the Factory Interface for scanning.

All the active scanning functionalities are disabled, therefore all the data coming from active analysis (such as Device list, Topology, etc.) will not be available.

This functionality is recommended only for security reasons or company policy compliance.

A reboot of the device is required for the setting to take effect.

16.1.6 Updates

New firmware can be downloaded from the <u>PROCENTEC</u> website and uploaded in the Updates menu item. More instructions about updating can be found in chapter 17.

16.1.7 About

The About menu item features the following:
- The current version
- Factory reset (see 18.4).
- Licenses: an overview of the current licenses for specific features. See 16.1.8 and 16.1.9.
- Third-party licenses: a list of third-party open source licenses.

16.1.8 License Manager

Features within Osiris are license based. There is a License Manager available to see which features are enabled or to upload a new license. The license manager can be reached via the 'Atlas/Mercury licenses' button within the About menu item on the Settings page. Another way of opening the License Manager is to double-click or drag down the dark blue bar on top (admin only). In the right upper corner there is an icon of a key which opens the License Manager.
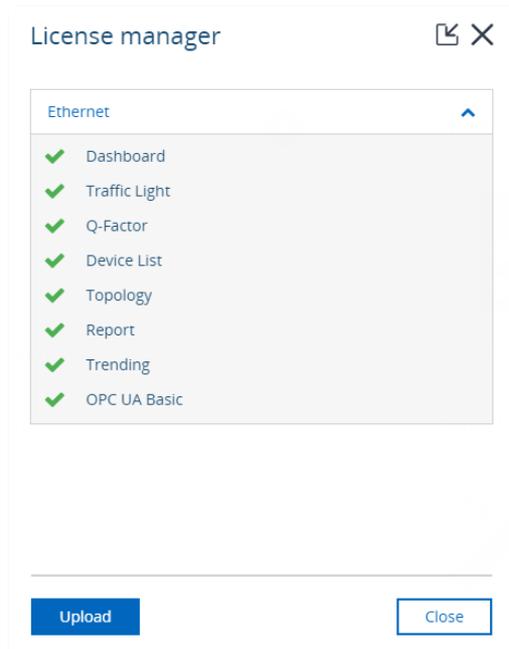
The upload license button will enable the selection of a new license file (see also 16.1.9). During the upload of a new license file, the file is checked and if the file is not valid the old license will be restored - an error will be shown.

16.1.9 How to upload a new license file

Before you can upload a new license, first make sure you obtain one. To do this, get in contact with your local distributor where you purchased the device, and keep your serial number ready. The serial number of the Atlas can be found at the side of the unit, or check the 'Device name' of the General tab of the settings.

The serial number of the Mercury and Osiris as a Software are based on two keys: the license serial number and the license ticket number (both can be found in the top of Osiris Control window). It can be downloaded automatically by Osiris if it has a working Internet connection. To do this, right-click the Osiris icon in the Windows system tray and choose 'License information'. It will pop up the window shown on the right. Click 'Check for license updates' and the new license will be installed automatically.
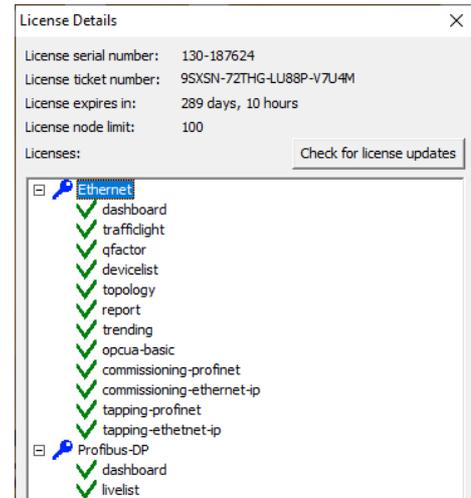
For Atlas, follow this procedure:

- Open the License manager, this can be done in two ways:
    - Double click or drag down the dark blue top bar containing the time. Click on the key icon located at the right side.

    - From within the Settings page go to the 'About' menu item. Click on the 'Osiris licenses' button.
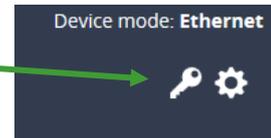
- Click the "Upload" button
- Click the folder icon
- Browse to and open your new license file
- Click the "Upload" button
- When you press the Upload button the system will check if your license is valid. If this check fails then make sure you upload the license to the correct device (check the serial number). If this keeps failing, contact PROCENTEC.
- When the correct license is uploaded you will be automatically logged out. After logging in again, your new license will take effect.
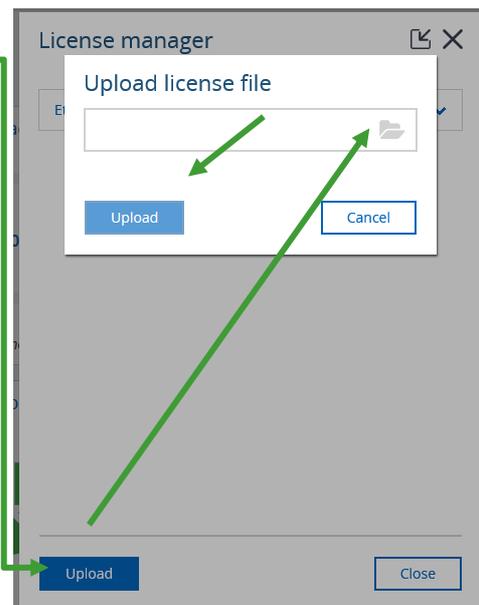
In the License manager you can now check which new features are enabled.
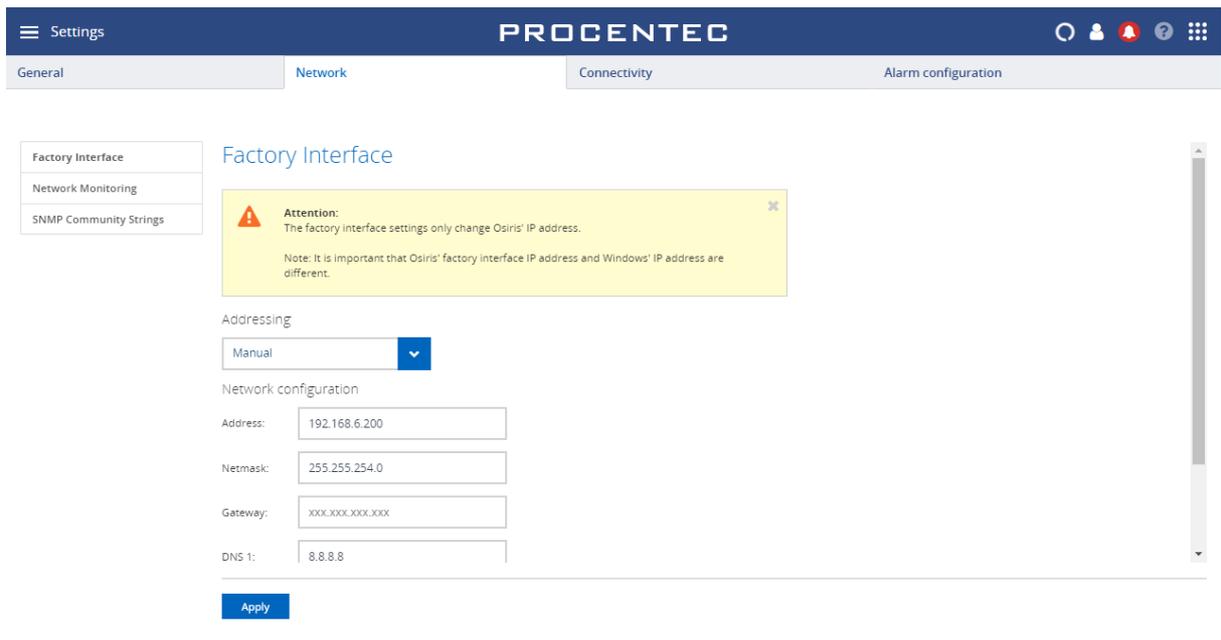
16.2 Licensing Update on Atlas2 and Atlas2 Plus

There are 3 options for updating a license on Atls2 and 2+, go to the license manager:
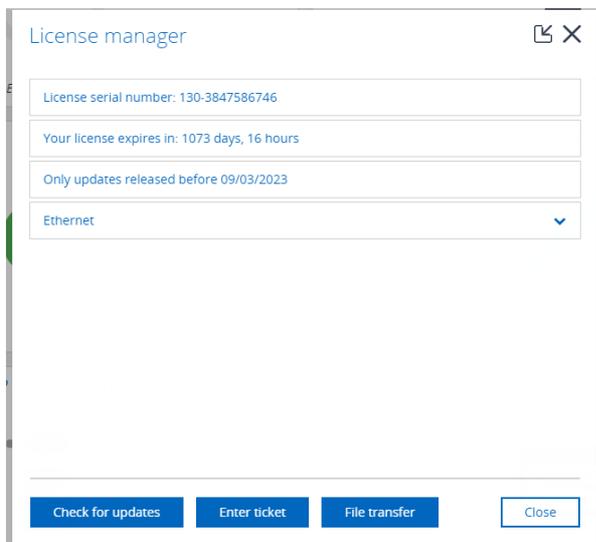
- Check for updates, can be used when the device is connected to internet and there is already a license installed.
- Enter ticket, can be used when the device is connected to internet and the user has got a ticket from Procentec.
- File transfer, can be used when the device is not connected to internet, please see your mail for more details.

For the offline File Transfer:

Transfer license file

| Request license | Update license |

Download request file   Close
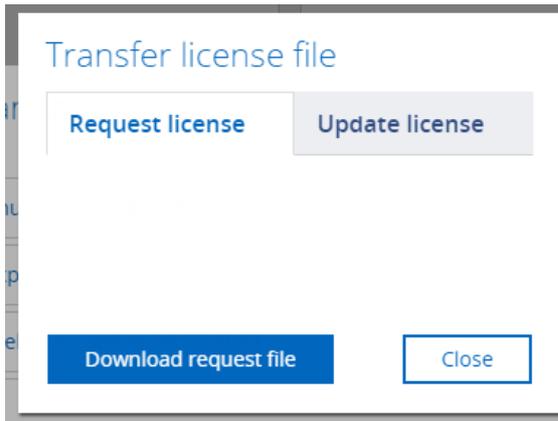
- Download the request file from the licence page "Request License"
- Open the link that Procentec provided, something like this:
  http://lc.codemeter.com/86969/depot/get.php?id=ticket number
- Upload the Atlas2 file on the WIBU webpage, WIBU will create a new license update file
- Upload the license file on Atlas2
- Atlas2 will provide a confirmation file, download it.
- Upload the confirmation file on the WIBU website.

When the entire procedure is done, both the license on Atlas and the WIBU servers will be synchronized.

16.3 Network: Office (Atlas only) & Factory interface

The Factory and Office interface can be configured manually or automatically using DHCP. Mercury does not have an Office interface.

In case you configure the interface manually and you would like to make use of automatic time (via the internet) you should enter the Gateway and DNS servers. Make sure to only enter one Gateway; do not use gateways in both interfaces.

Important note: make sure that the Office and Factory interface are set to different IP ranges. Having both interfaces configured in the same IP range will cause Atlas to not work properly.
Also, it is required to have only one gateway set. This can be either in the Office interface or in the Factory interface, but not both.

If you are using a Mercury or PC-license, the 'Office' interface is not available.

16.3.1 Network Monitoring

In this menu item you can specify up to ten IP address ranges of devices you would like to scan. Each scan range must be given a name. The order of scan ranges is irrelevant.

If there are large gaps between devices on your network, it is advised to separate a large scan range into multiple smaller ranges. This will speed up the scanning process.
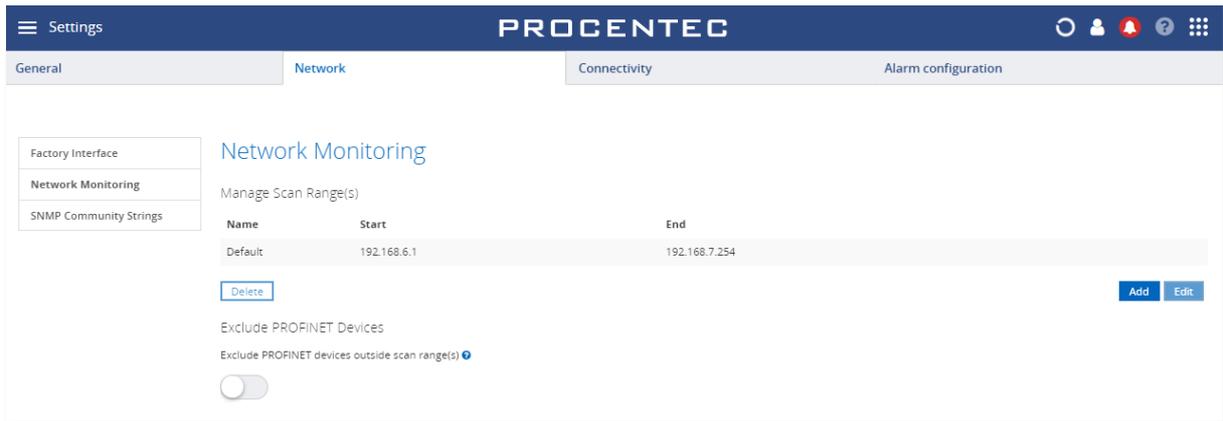
The network monitoring is performed on the Factory network interface, so it is important that the entire specified IP address ranges are reachable by Osiris through its Factory interface. To do this make sure your scan ranges falls within the subnet of the Factory interface.
If your IP/subnet configuration is not correct for the specified scan ranges, a notification pop-up will appear.

You can delete or edit a scan range by clicking it first and then click Delete or Edit respectively.

Devices which are not within the scan range can be excluded from appearing in the Device list, Topology, Commissioning Wizard and EtherTAP by enabling the 'Exclude PROFINET Devices' slider. These devices are typically PROFINET devices that respond to DCP broadcasts, even when they are outside the scan range.

16.3.2 Network Snapshot

Osiris offers the possibility of creating a snapshot of the monitored network, and then receive a notification if something has changed. This makes it possible to improve the monitoring of a network and to address any sudden, potentially critical changes.

You can create and delete a network snapshot, which contains a baseline of the active monitored Ethernet network.

The deviations in the network are reported in several outputs, like Notifications, Traffic Light and Email. These outputs are configurable in the Alarm configuration tab in Settings (see 16.5).

Network Compare	Warning	Error	Notifications	Traffic Light	Email	MQTT	OPC-UA	Relay
Missing Device	⊘	⊘	✔	✔	✔	✔	✔	✔
New Device	⊘	⊘	✔	✔	✔	✔	✔	✔
Different Firmware	⊘	⊘	✔	✔	✔	✔	✔	✔
Different Name	⊘	⊘	✔	✔	✔	✔	✔	✔
Different IP Address	⊘	⊘	✔	✔	✔	✔	✔	✔

Figure 34 - The network properties stored in a Network Snapshot. The alarms can be customised.

A Network Snapshot will show the following details:
• **Date**: shows the date and time when the Network Snapshot was created.
• **Number of devices**: shows the number of devices in your network when the Network Snapshot was created.
• **Scan range**: shows the scan range(s) set in Osiris when the Network Snapshot was created (see 16.3.1).
Only one Network Snapshot is available.
It is possible to create and delete a Network Snapshot.

Creating a new snapshot will overwrite any existing snapshot.

A Network Snapshot can only be created with the measurement running.

A Network Snapshot can only be created after the network is fully scanned. Depending on network size this can take a while.

After changing a scan range, create a new Network Snapshot to avoid Network Compare alarms.

16.3.3 SNMP configuration

16.3.3.1 SNMP version

You can choose the version for retrieving SNMP data. The following versions are supported:
- SNMPv1
- SNMPv2c
- SNMPv3

SNMPv1 does not require any login and offers no encryption or security. This is suitable for most applications.

SNMPv2c supports more values as it can use 64 bit counters.

SNMPv3 has a login and encryption feature, where you can choose the following security levels:

- No Authentication required, no private key required
    - o Only a username is needed to login.
- Authentication required, no private key required
    - o A username and correct password are needed to use SNMPv3. MD5 and SHA authorization algorithms are supported.
- Authentication and private key both required
    - o A username, correct password and a private key are needed to use SNMPv3. MD5 and SHA authorization algorithms are supported.

The authentication password and private key must match the credentials entered in the SNMP hosts (e.g. switches or firewalls).
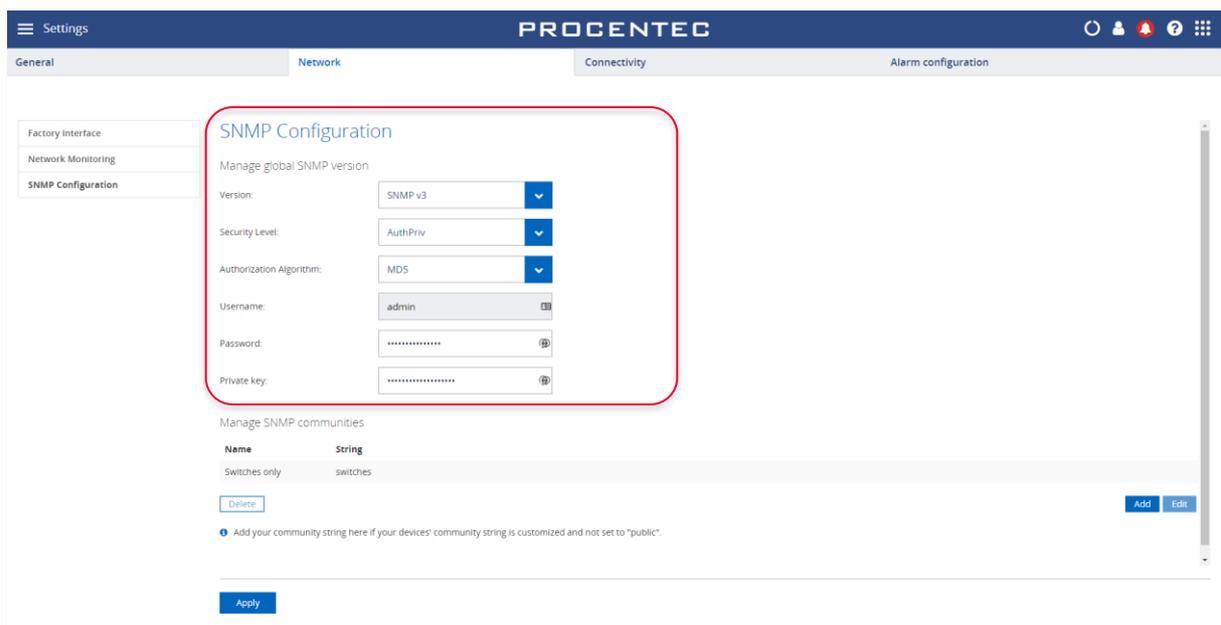
16.3.3.2 SNMP Community strings

The SNMP Community String is similar to a user ID or password that allows access to the statistics of a switch or device. If the correct community string is provided, the device responds with the requested information. If the community string is incorrect, the device will discard the request and does not respond. This results in missing information and a wrong Topology where devices are centered around a ⏣ icon.

If the Community String in the switch(es) is not 'public', you can change it to another string here:
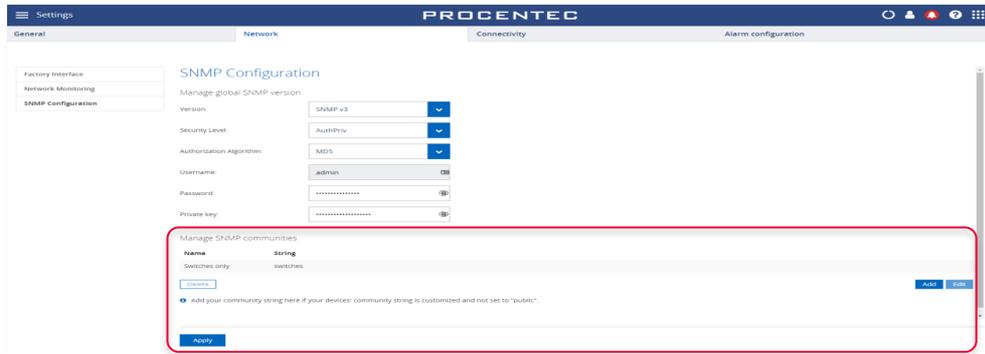
16.3.4 EtherCAT configuration

If you have an EtherCAT license installed, you can setup the configuration here.
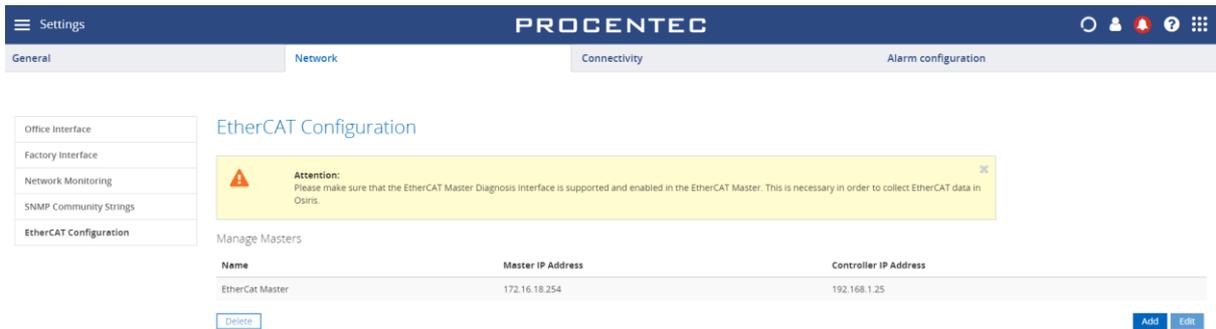
Click ' Add' to enter the IP address of a new EtherCAT master.

· **Name:** This name will be used in the EtherCAT page to display the master information.
· **Controller IP Address:** The IP address of the LAN interface of the physical controller
· **Use as gateway:** When using TwinCAT controllers, this option must be disabled.
· **Master IP Address:** The IP address of the Mailbox gateway of the EtherCAT Master

Press Apply.
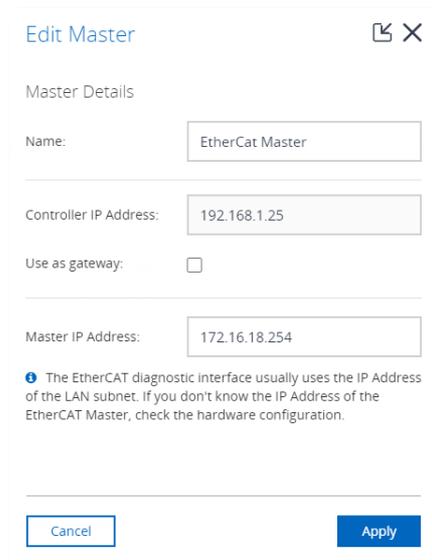
16.3.5 EtherTAP configuration

In the EtherTAP Configuration tab in the settings it is possible to:

• Enable or Disable PROFINET tapping
• Enable or Disable Ethernet/IP tapping
• Enable or Disable Security Tapping.

For better performance, it is recommended to disable functionalities that are not used.
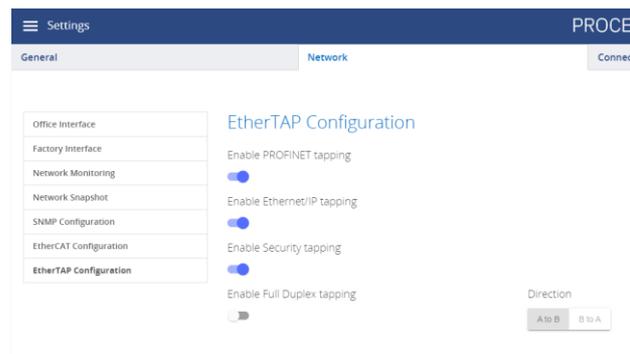
By disabling Full Duplex tapping, it is possible to maximize TAP performances on a high load network by selecting to TAP and analyze only one direction at the time. In this way, all the processing power will be dedicated to one communication direction, allowing Osiris to achieve better performance on very high load networks.

16.4 Other Connectivity

16.4.1 E-Mail

Osiris allows you to be alerted by e-mail about changes in the properties of your network and/or devices (this is configurable in the Alarm Configuration tab, see 16.5):

The e-mail settings menu item allows you to specify an SMTPS (secure) or SMTP (not secure) server, login credentials and a list of recipients which will be used for the delivery of the alerts. The interval is the minimum number of minutes between two e-mail alerts.

Before you save your settings, you are advised to test them first by clicking the **Send test email** button. All the recipients will receive this test e-mail.

16.4.1.1 Google Gmail-account

Use the settings in the image above for Gmail accounts. Then go into your Google account to allow the Atlas to send emails (this is disabled in Gmail by default, and must explicitly be enabled). Search in your account for 'Less secure app access' and enable this feature.
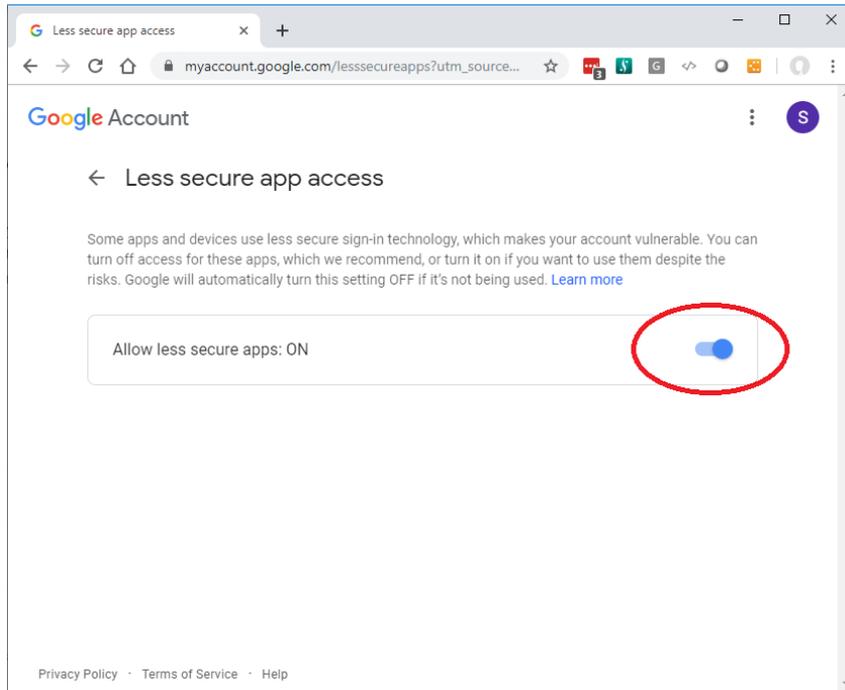
16.4.2 SNAP

You can enable and setup the SNAP functionality here.
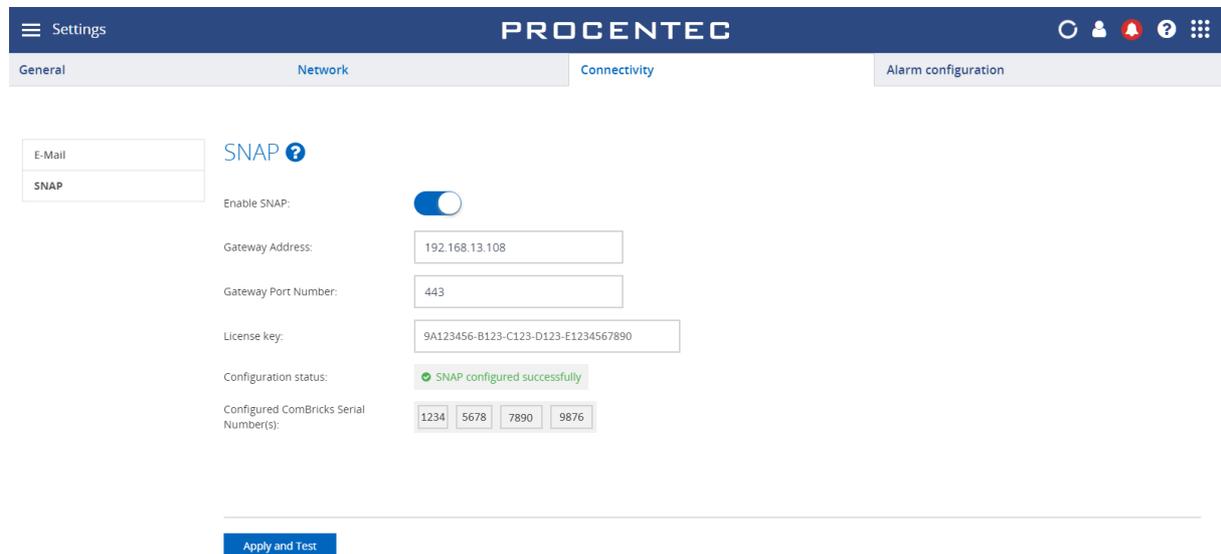
If you are interested in the SNAP functionality, contact your PROCENTEC sales representative, all the configuration steps required will be provided by our technicians.

16.5 Alarm configuration

The Alarm configuration screen lets you configure warnings, errors, notifications, Traffic Light, emails, and the Relay (Atlas family only) in a flexible way. All items can be enabled or disabled, and thresholds can be changed to suit your desired level of alarms.

To change a line, select it and click the 'Edit' button in the bottom of the window.
In the example below, the Ping Packet Loss alarms have all been disabled:

Use the switch buttons to enable or disable the types of alarms.

Atlas has an additional switch button to enable or disable the Relay for events (see16.5.1).

16.5.1 Relay (Atlas only)

A unique feature of the Atlas is the Alarm Relay (indicated as RL on the front of the housing). The behaviour can be adjusted in the Alarm Configuration tab of the Settings. The Relay switches from ON (it is a Normally Closed contact) to OFF after successful startup. By default, it switches ON whenever one of the following events occurs:

- Ping packet response warning or error
- Ping packet loss detected
- Lost device detected
- In or out errors detected
- In or out discards detected
- PROFINET broadcasts (DCP Identify)
- Alarms or Dead Connections (PROFINET or Ethernet/IP)
- Max. Jitter reached (PROFINET and Ethernet/IP)
- Dropped packets detected (PROFINET and Ethernet/IP)
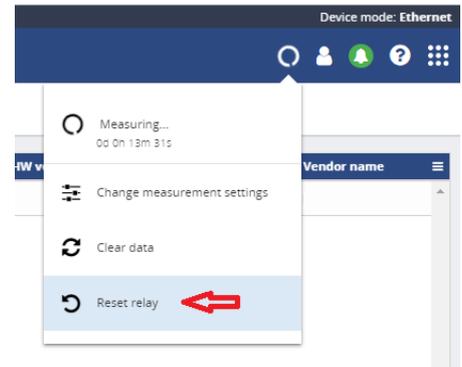
When the Relay has been triggered by an event, you can easily reset it in the Measurement menu (round spinning icon in the Icon bar), by clicking the 'Reset relay' menu item.

17. Updating the firmware

Osiris, the application running on Atlas/Mercury, will be regularly updated by PROCENTEC. Such an update may include the addition of new valuable features for users, fixes for issues encountered in the field or updates to the underlying operating system.

Whenever an update becomes available it will be announced on the website of PROCENTEC and by means of our newsletter. PROCENTEC will provide details regarding the update and indicate whether or not the update is regarded as being a critical update.

Before reporting a bug, make sure to update your Atlas/Mercury to the latest version and check if the problem is still happening.

To start with the update process its first important to see what the current version is and if it can be updated.

WARNING: IT IS IMPORTANT TO FOLLOW THE UPDATE PROCEDURE STEP BY STEP. A WRONG UPDATE PROCEDURE CAN LEAD TO A NON-FUNCTIONING DEVICE.

Administrators can update the firmware by uploading it using the 'Update' menu in the General Settings tab. The process of updating the firmware is detailed in the following steps.

17.1 How to find your current version

To find the current Osiris version, check the login screen:

On the bottom of the screen you should see the name PROCENTEC. Underneath it you will find the current version number. You can ignore the fourth number.
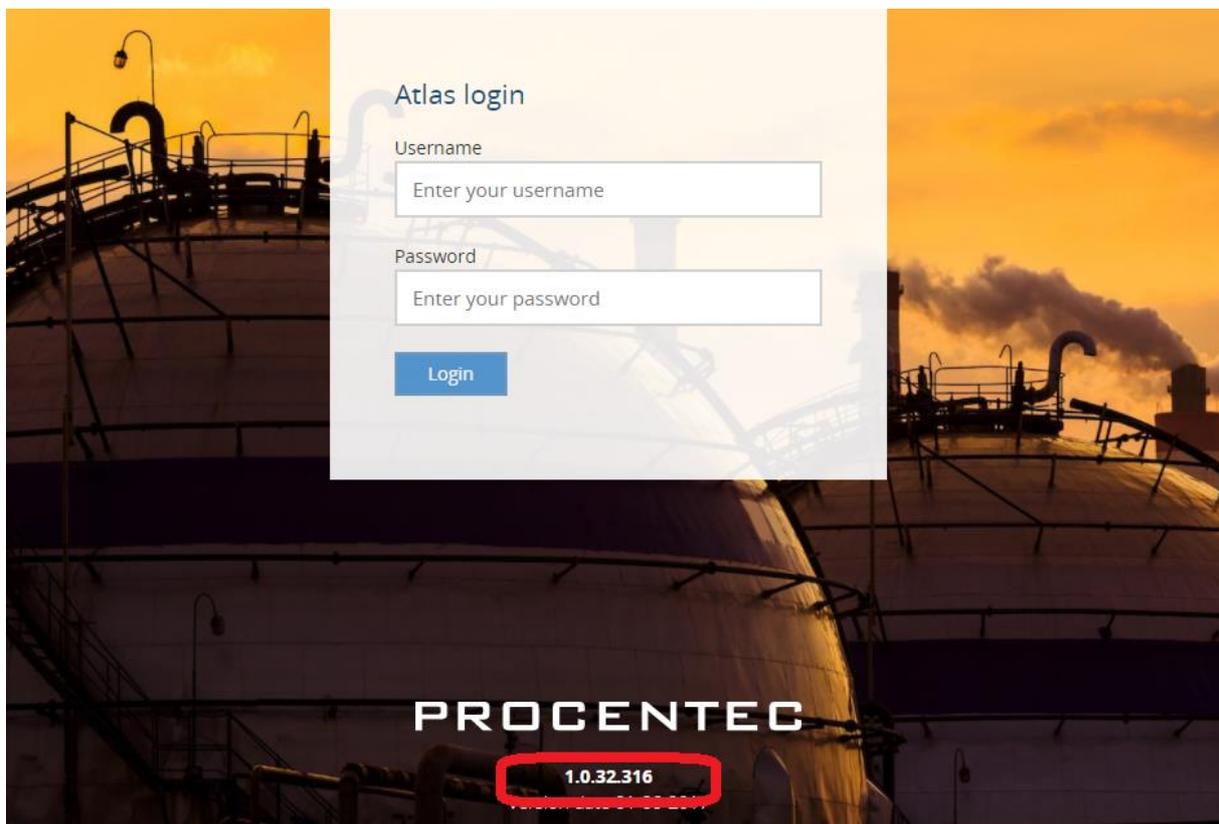
17.2 How to update

For Atlas version newer than 1.0.32, follow instructions at paragraph *Updating Atlas(> 1.0.32)*.
For Mercury, follow instructions at paragraph *Updating Mercury.*
For Atlas version 1.0.32: follow instructions at paragraph *Updating Atlas Version 1.0.32.*

17.3 Updating Atlas Version 1.0.32

For this version of Atlas the update of the firmware is only possible by means of a USB-stick. The process of updating the firmware is detailed in the following steps:

1. Download the latest firmware for Atlas from the PROCENTEC website.
   support.procentec.com

2. Copy the downloaded firmware package onto a USB-stick.
   Note: make sure the USB-stick is formatted according the FAT filesystem.

3. Insert the USB-stick into a USB port of Atlas.

4. Wait at least 20 seconds and then remove the USB-stick.

5. Wait 10 seconds and then insert the USB-stick again into the same USB port of Atlas as used at step 3.

6. Wait 3 minutes and then remove the USB-stick.

7. Log in as administrator, double click the top bar and then press the restart button.

8. Now wait until the RDY led turns on.
   !!! IT WILL TAKE ±60 MINUTES TO COMPLETE THE UPDATE PROCESS. DO NOT UNPLUG THE POWER SUPPLY DURING THE UPDATE PROCESS !!!

9. Check the version number again.
   Note: for version 1.0.35 it will show the number 1.0.34.417

17.4 Updating Atlas(> 1.0.32)

Update via web interface:
1. Log-in in Osiris as Admin (only the admin user can update the firmware).
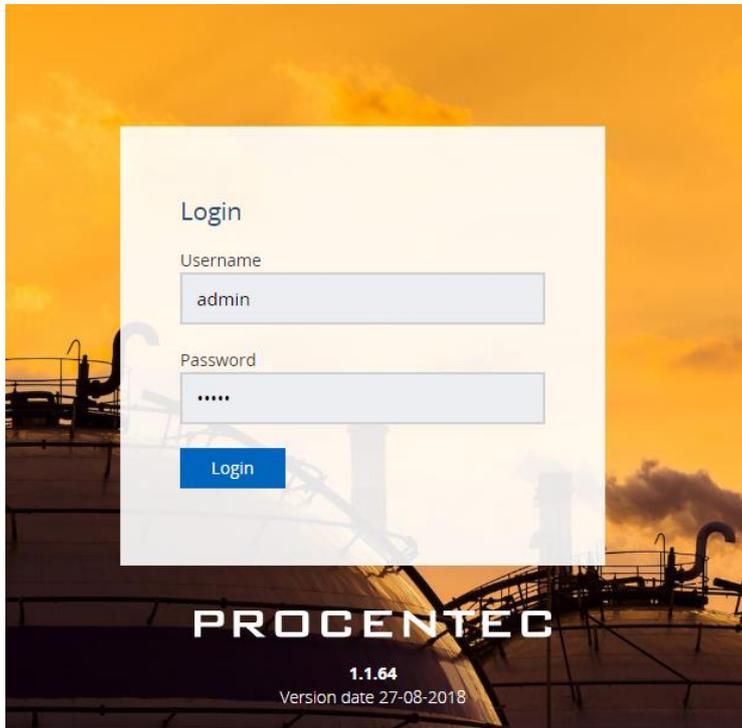
2. Go to Settings > Updates
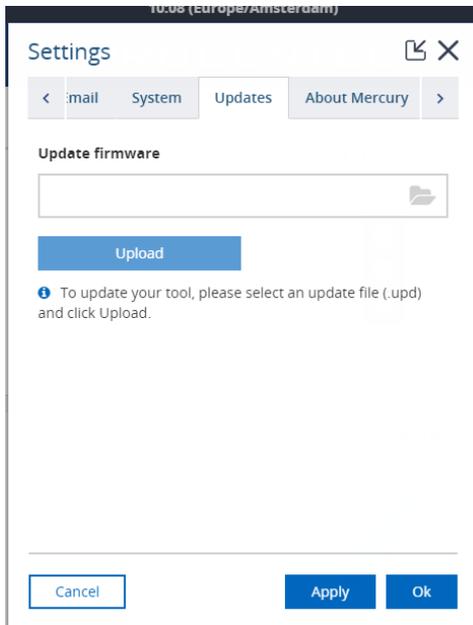
3. Select the update file .upd
   Atlas and Mercury updates have different .upd files, use the specific Atlas update file!

4. Press upload

5. Wait until the file is uploaded – this usually takes about 10 minutes. If it is still loading after an hour, try again.

6. When the update is loaded, a green message will appear, press OK
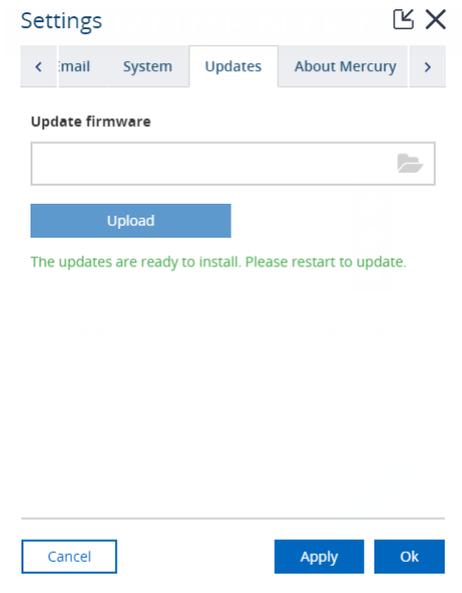
7. A reboot button on the system clock will appear. Click on **Restart to Update** and click on yes on the popup.
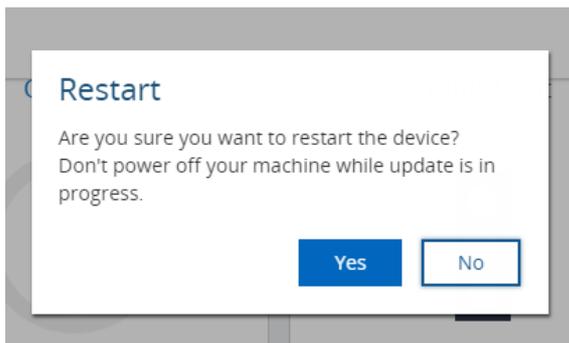
8. The screen will change to the Restarting page.
   If after 5 minutes you do not see the restart page appearing, it is needed to manually power off and on the unit. After power on, wait up to an hour for the update, then manually browse to the Atlas IP address.
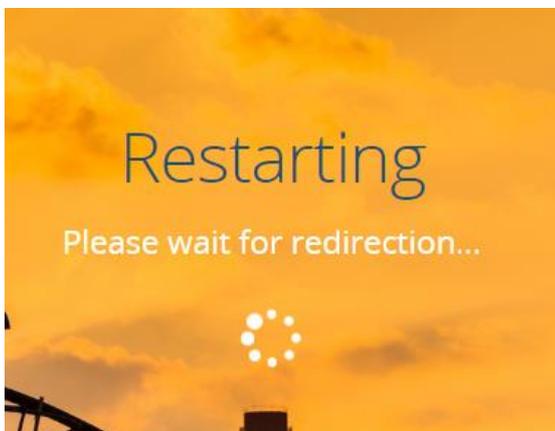
9. Wait until Osiris is back online. This can take up to one hour, the entire OS and the software will be updated. **DO NOT POWER OFF THE ATLAS. POWERING OFF WILL DAMAGE THE UPDATE AND THE ATLAS.**

10. Once the update is done you will see the login page. Log in and go to settings, where you should see the newest version. If it still shows the previous version, try to refresh the page:
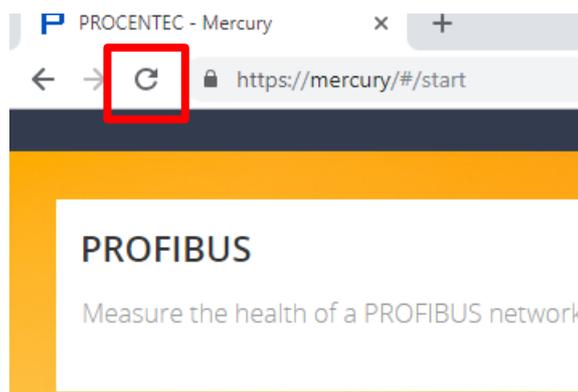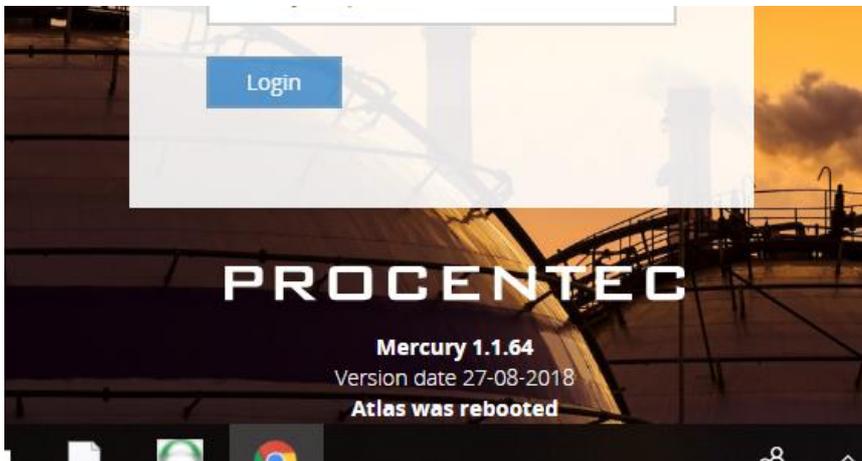
Your Atlas is now updated, enjoy the new functionalities!

17.5 Updating Atlas2 Plus and Atlas2

The Atlas2 Plus and Atlas2 can be updated via the webserver as described in 17.4, but it can also receive an update via USB. Copy the new firmware file with extension .upd to the root of a USB drive and insert the USB drive in one of the two available USB ports of the unit.

Note on Downgrading the firmware on Atlas2 Plus and Atlas2:
After downgrading the Osiris software running in your unit a factory reset is required.
This is only needed when downgrading, not for upgrading.

17.6 Updating Mercury and Osiris as a Software on PC

Since V1.93, Mercury is updated via a new windows installer, which contains and takes care of all the changes and updates automatically.
After the update, some settings will be reset to default. Take note of your current settings before applying the update.
Stop Osiris before installing the update.

DICSONNECT ANY USB DEVICE CONNECTED TO MERCURY (i.e. EtherTAP) BEFORE STARTING THE UPDATE.

YOUR MERCURY NEEDS TO BE CONNECTED TO THE INTERNET IN ORDER TO ACTIVATE YOUR LICENSE.
CONNECT YOUR MERCURY TO AN ETHERNET/WIFI CONNECTION WITH INTERNET BEFORE STARTING THE UPDATE.

1. Download the latest firmware for Mercury from the PROCENTEC website.
   support.procentec.com
   Please note: the firmware update file for Mercury is a different file than for Atlas.
2. Connect Mercury to the power supply and turn it on
3. Make sure that the battery is fully charged and the sleep mode of Windows is completely disabled. If Windows is switched off or goes in sleep mode during update the entire device can be damaged.
4. Check that you do not have any pending Windows update. **Note: pending Windows updates can cause Osiris to not start.**
5. Open the update folder, extract the files and click on OsirisForWindows.exe
   Note: Make sure you start the .exe file, do not start the .msi file in the directory.
6. When prompted, click on YES to allow the execution of the installer.
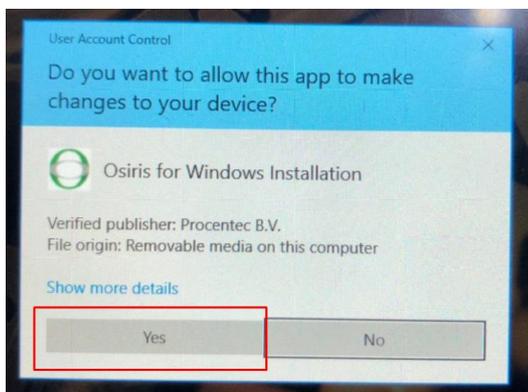
7. If you had Osiris already installed on your system, the following windows will appear:

Select Uninstall and press next, then press finish.

Then open OsirisForWindows.exe again.

8. Click Next 2 times
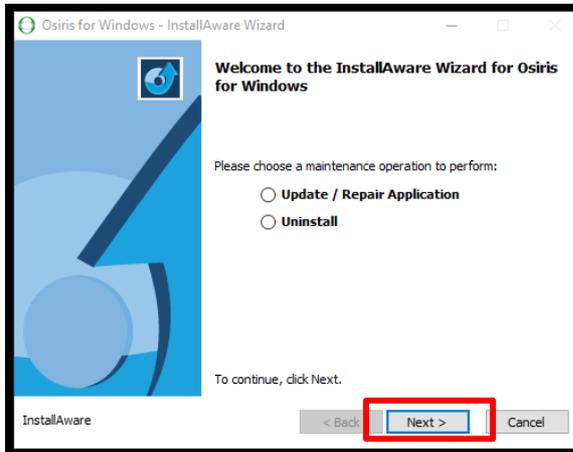
9. You will get a pop-up for installing the VirtualBox update, click **YES**, the system will install virtualbox V6.04
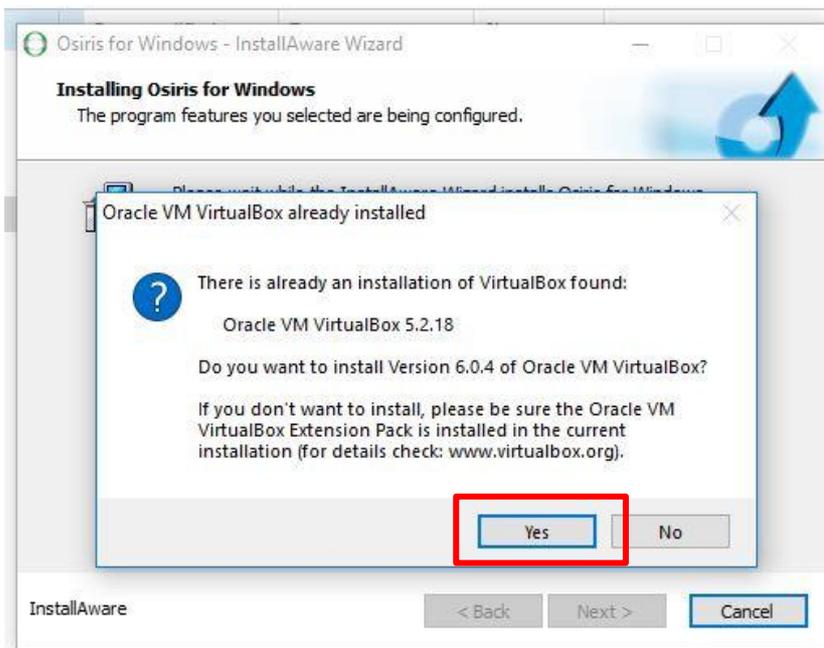
10. You will get a pop-up for installing CodeMeter update, click **YES,** the system will install CodeMeter V7.10a
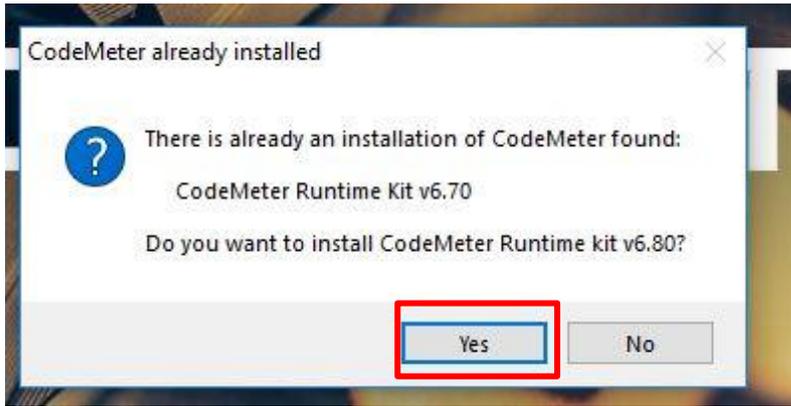
11. If the installer is showing the following screen:
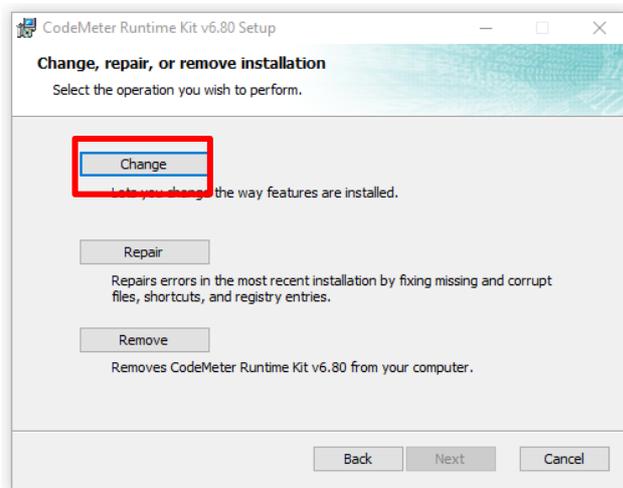
Select **Change**.

12. Follow the instructions of the CodeMeter installer (Click **Next** until the installer is ready to install CodeMeter, then click **Install/Change**, then wait until the installation is done).
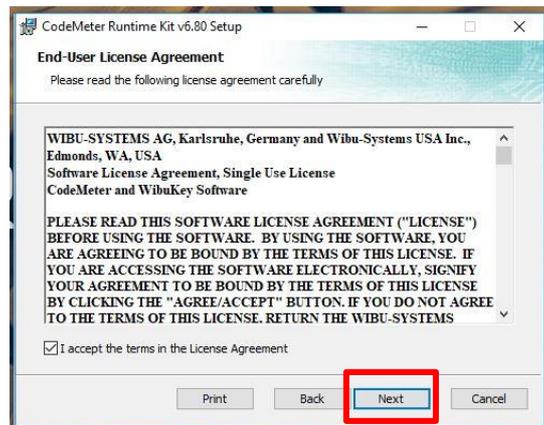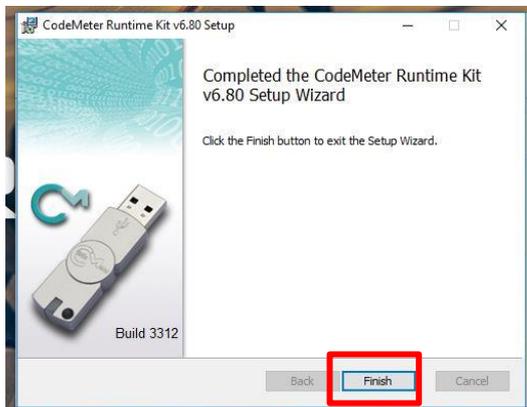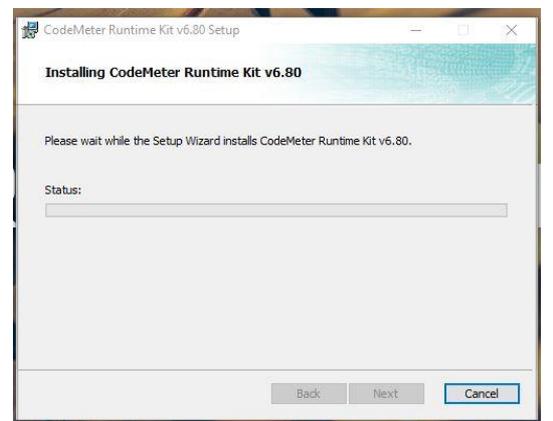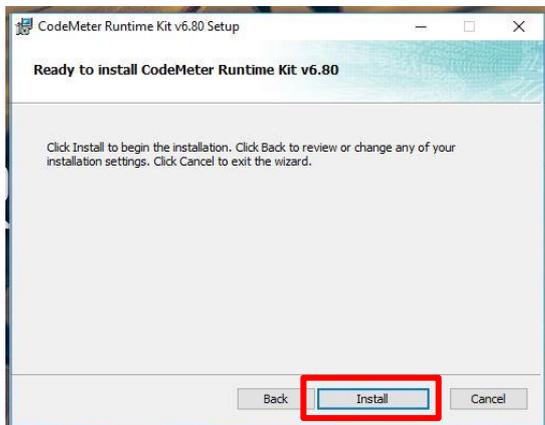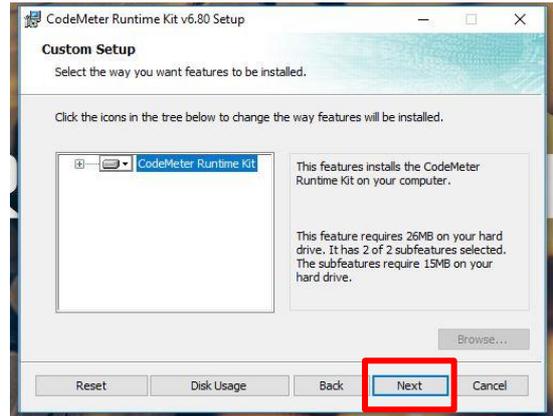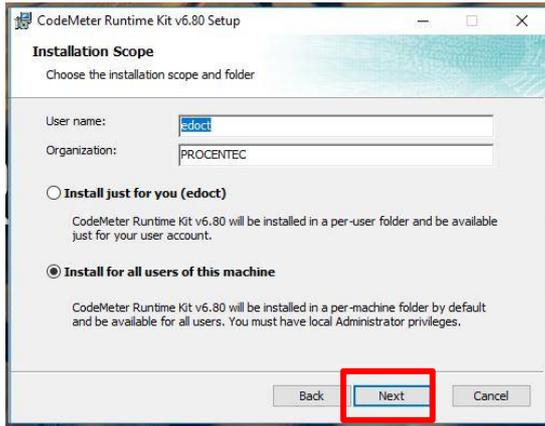
13. Wait until all the installation is done
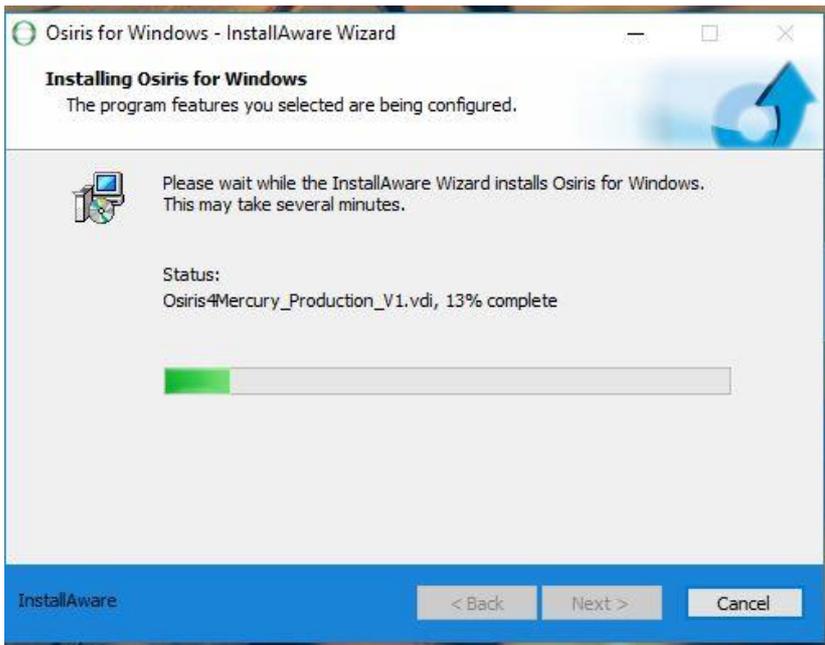
14. When the installation is finished, make sure you have selected "Run Osiris for Windows now" and click finish.
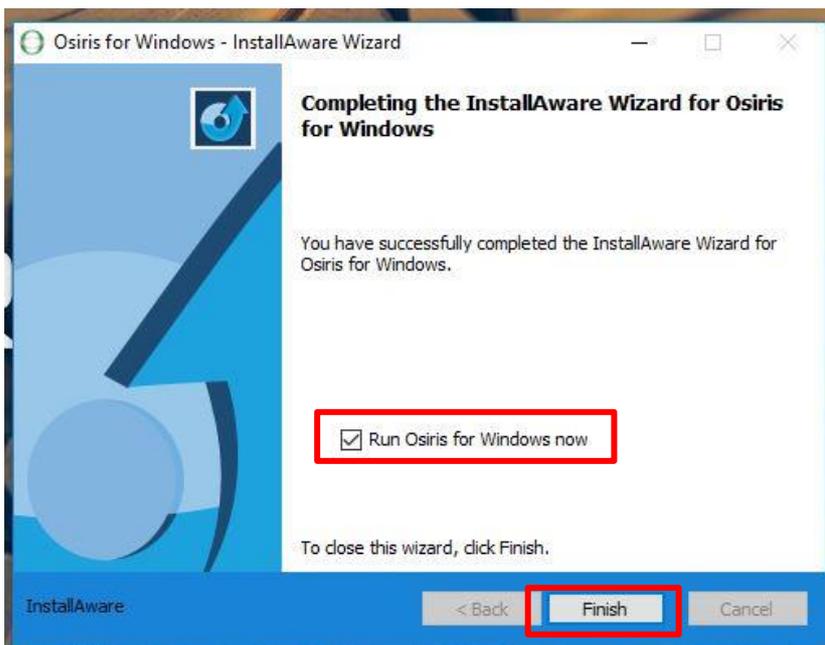
15. **If you are updating from mercury 1.83 or older**: wait a while, OsirisControl is now starting and preparing your system for the update.
    If you are updating from mercury 1.93: you need to manually run OsirisControl from your desktop in order to start it.

16. If you get a firewall settings popup, click <u>OK</u> two times
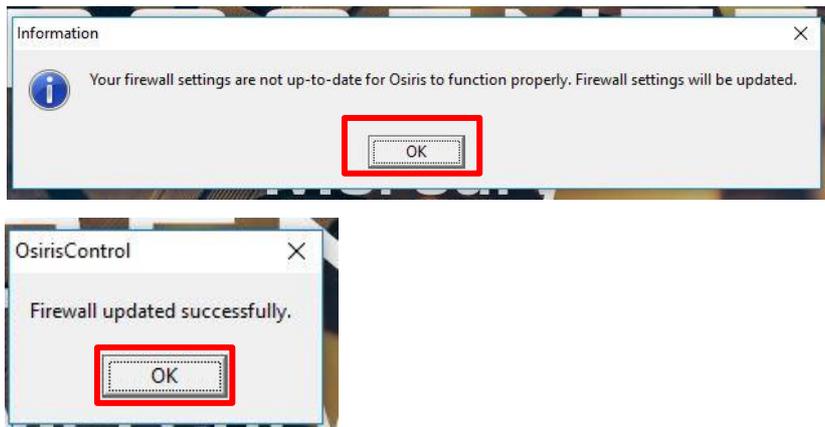
17. After some seconds you will have a license update confirmation, click OK
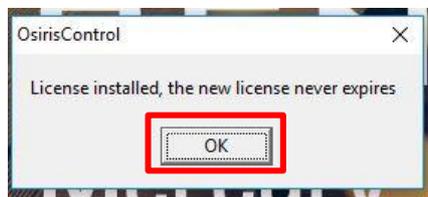
18. OsirisControl will ask you which interface you want to use for the measurement, select *"Realtek USB FE Family Controller"* and click OK
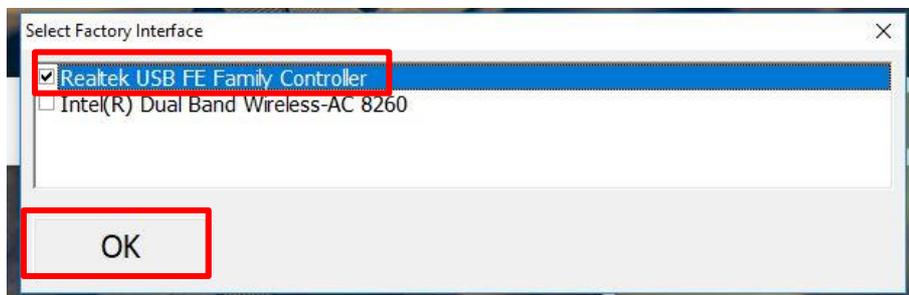
19. A black popup will appear with the terms and conditions of the new VirtualBox, read them and accept by typing "Y" and pressing enter in the keyboard
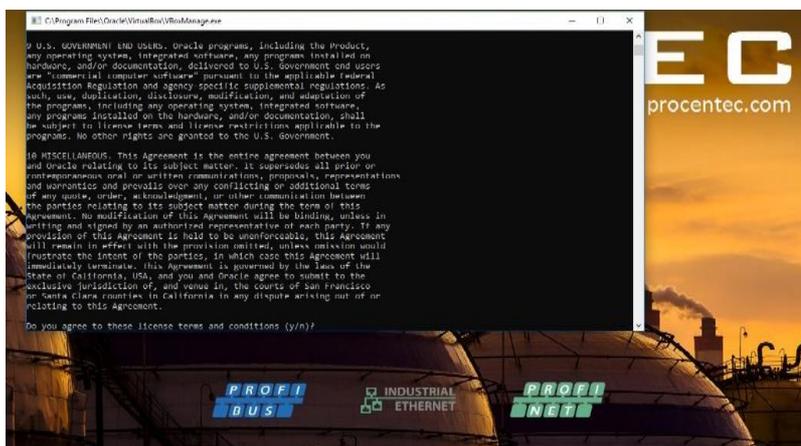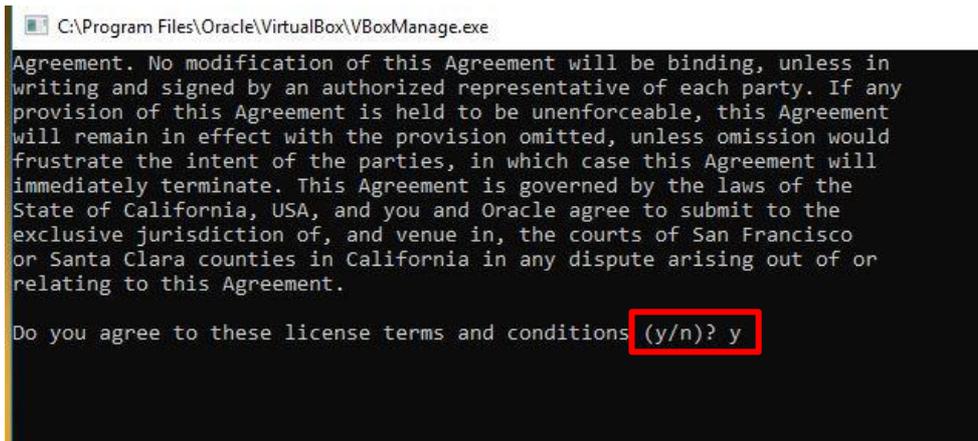
20. Osiris will now start, you will see the Log-in page appearing with the new version number at the bottom.
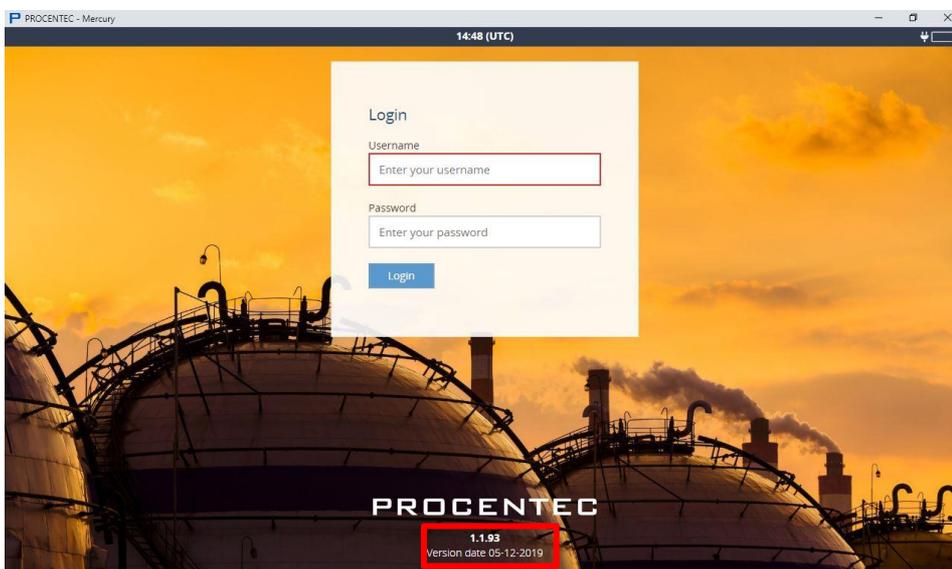
21. Follow the configuration guide and add your network information
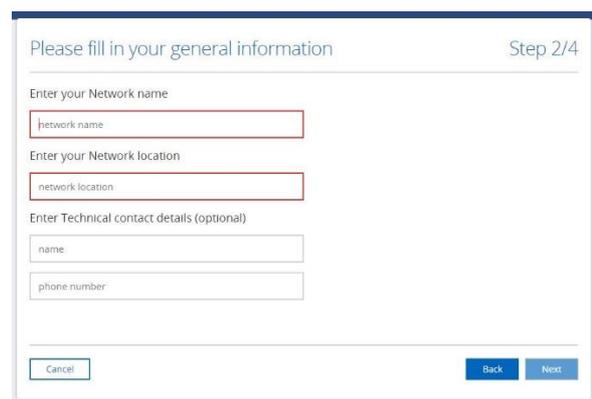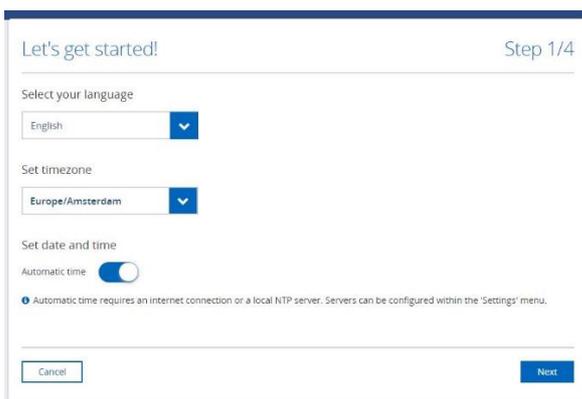
22. You can now start using the new version of Osiris! Enjoy the new features!

If you get old data in your notification, just run *"Clear all Data"* to start from scratch

18. Resetting Osiris to factory defaults

If Osiris becomes unreachable due to any reason, you can reset the device to factory settings.

Warning: this will reset all settings, clear all measurement data and will restore both the network interfaces to their initial IP address (Factory: 192.168.0.10; Office: 192.168.1.10)

18.1 On Atlas

The Atlas has a reset button at the front, as shown in Figure 3532. You can use a small object, such as an unfolded paperclip, to reach the button behind the small hole in the front. Press it for 10 seconds during operation and then release it. Do NOT press too hard; the button requires little pressure. After 10 seconds, the device will start a factory reset which will take approximately 2 minutes.
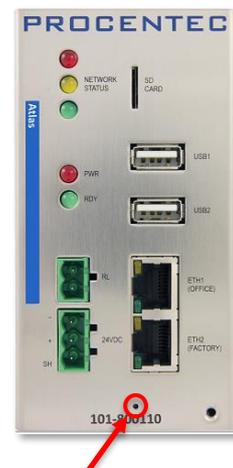
Figure 35 - Factory reset button

After the reset, it will reboot and be reachable on the default IP addresses again. You need to fill out the Setup Wizard before the Atlas can continue normal operation again (see 2.1 for setting up the Atlas). Until that time the yellow traffic light and the green RDY LED will blink.

18.2 On Atlas2 Plus and Atlas2

Osiris on Atlas2 Plus and Atlas2 has two ways of being restored. On the top of the housing, between the ventilation grid, are two buttons. The buttons have the following functions:

Button 1: Re-load latest working firmware
This will write the latest working firmware into memory. It can be used if the device becomes unresponsive for whatever reason.
This mode does not clear IP addresses or passwords; they remain the same as before.

Figure 36 - Atlas2 reset buttons

To activate this button, perform the following actions:
- Remove the power from the Atlas
- Press and hold down button 1
- Apply power while pressing the button
- When the power has been applied, release the button.
This operation takes several minutes; do not remove power.

Button 2: Reset to factory defaults
This will clear all the settings and passwords.
To activate this button, perform the following actions:
- While the device is running, press the button for 10 seconds
- Remove the power from the Atlas and re-apply power after 10 seconds
This operation takes no longer than the normal boot time (15-30 seconds).

After the reset, the Atlas will reboot and be reachable on the default IP addresses again. When the device is started , you need to fill out the Setup Wizard before the Atlas can continue normal operation again (see 2.1 for setting up the Atlas). Until that time the yellow traffic light will blink.

18.3   On Mercury or PC

Osiris on Mercury or PC can be reset to factory defaults. First, make sure the OsirisControl application is running. Then press the Windows logo button   below the screen. This will bring up the Windows taskbar and system tray.

Click the UP arrow in the system tray once, then press on the Osiris icon for about 1 second. A small menu appears, then click 'Factory Reset'.
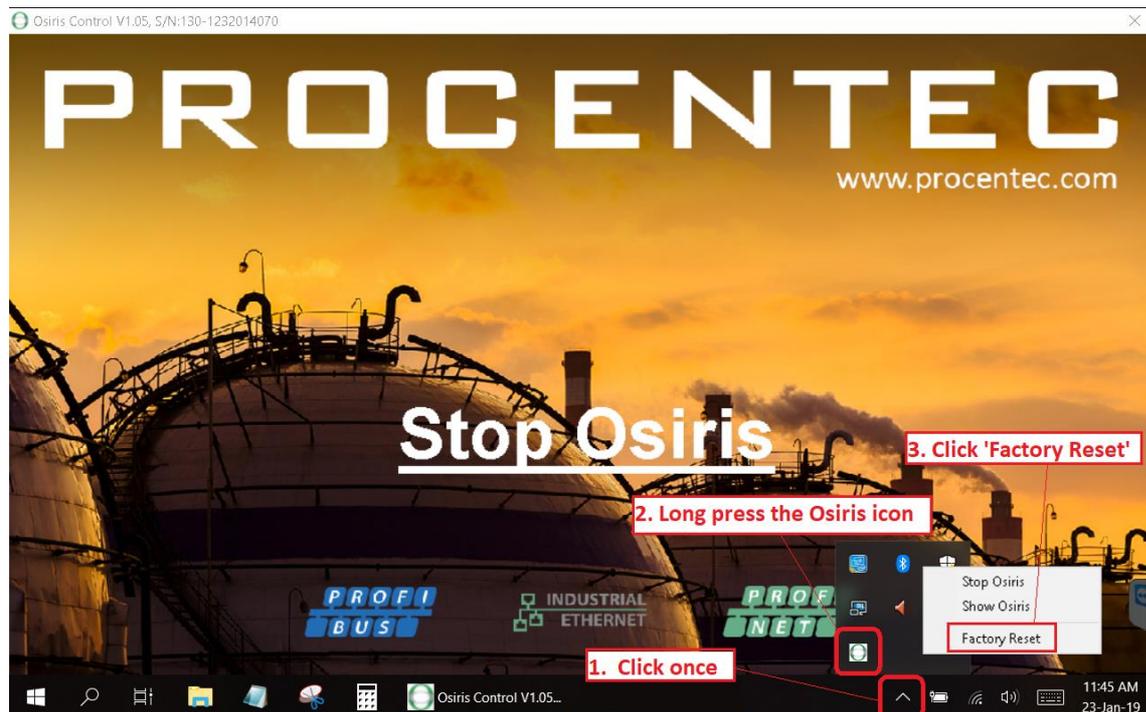
18.4   Using the Settings in the web interface

The other way to factory reset the device is through the web interface. In the 'Settings' page, go to the first tab 'General'. In this tab, click 'About' in the left menu. You can find a button 'Factory reset'. Clicking this button will bring up a confirmation window, where you can confirm the factory reset. The device will start a reload procedure that will take approximately 2 minutes.
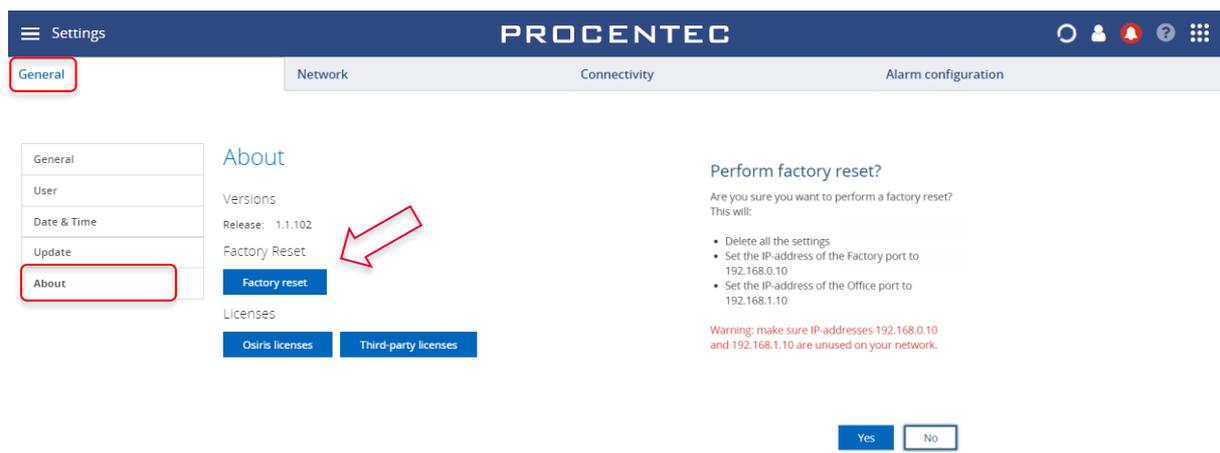
After the reset, it will reboot and be reachable on the default IP addresses again. You need to fill out the Setup Wizard before Osiris can continue normal operation again. Until that time, the yellow traffic light and the green RDY LED will blink on Atlas.

Warning: Do not re-install Windows or format the tablet. This will cause Osiris not to start. If problems arise, first check our FAQs on the website.

19. Firewall settings

Osiris uses the following network ports.

Port number/protocol	Description	Office interface (Atlas only)	Factory interface
80/TCP	HTTP	Used to redirect to HTTPS.	
137/UDP	NetBIOS	To report the hostname to Windows machines.	
161/UDP	SNMP	To report status information to external devices.	To collect topology data from the devices on the factory network.
443/TCP	HTTPS	Used for the web interface.	
502/TCP (OUT)	ModBus/TCP	Closed	Used to find devices supporting Modbus/TCP.
34964/UDP (OUT)	PROFINET-I&M/RPC	Closed	Used to collect PROFINET specific information.
44819/UDP (OUT)	EtherNet/IP	Closed	Used to find devices supporting EtherNet/IP.
1883/TCP	MQTT	Only used when the MQTT service is started.	
8883/TCP	MQTT over TLS	Only used when the MQTT service is started.	
4840/TCP	OPC UA	Only used when the OPC UA service is started.	
5353/UDP	MDNS/Avahi	To report the hostname to Apple machines.	

20. Technical specifications Atlas

Technical Data - Atlas in general	
Dimensions, weight and mounting	
Dimensions D x W x H (mm)	120 x 65 x 120 (width without side cover: 58 mm)
Weight	680 grams (*excluding plug-able connectors, packing material*)
DIN-rail	35 mm (minimum width 65 mm)
Ambient conditions	
Operating temperature	-20º .. +60º Celsius ⚠ **"WARNING, HOT HOUSING. When in use at an ambient temperature higher than 55ºC or 131ºF, the housing of the Atlas will be hot. Do not touch the housing!"**
Storage temperature	‑20° .. +85° Celsius
Relative air humidity	Maximum 98%
Ingress protection	IP 20 (DIN 40 050)
Power supply	
Pluggable power supply connector	Pin - : 0 V Pin + : +24 VDC Pin SH : Shield
Nominal power supply voltage	12 .. 24 VDC
Absolute maximum rated voltage	9 .. 32 VDC
Nominal power use	4.5 W
Maximum power use	20 W
Current consumption (12VDC)	Max. 1.4A
Reverse polarity protection	Yes
Redundant power supply	No
Wire diameter	<2.5 mm^2 Installation notes: The device shall be powered with a correct power supply: • For North America the power supply shall be listed and meet the requirements for class 2 • For the rest of the world the power supply shall meet the requirements for limited power sources as defined in IEC/EN 60950-1 cl. 2.5 Possible power supplies: Phoenix STEP-PS series Traco power TCL series XP-power DNR120-480 series

Ethernet	
Connector (Factory and Office)	RJ-45
Maximum cable length	100 m
Link speed	10/100/1000 Mbps
MAC address	Range: 9C:B2:06:2B:40:00 - 9C:B2:06:2D:3F:FF
Supported protocols	OPC UA, PROFINET (detect only), PROFINET I&M0, Modbus TCP (detect only), Ethernet/IP (detect only)
Protocols used	ARP, ICMP, DCP, SNMP, PROFINET I&M0
Default IP address after reset/purchase	Factory: 192.168.0.10 Office: 192.168.1.10
Default login / password	admin / admin
Connections	Up to 20 concurrent web clients

Relay contact	
Resistance	100 .. 150 mΩ (including plug)
UL maximum contact rating	max. 10W 24VDC, 400mA

SD card	
Supported types	SD and SDHC
Size	Maximum 32 GB

USB ports	
Type	USB 2.0
Maximum output power	500 mA per port

Others	
MTBF	To be defined

21. Technical specifications Atlas2 Plus and Atlas2

Atlas2 Plus and Atlas2 Technical Data	
Dimensions, weight and mounting	
Dimensions D x W x H (mm)	130 x 52 x 117 (*Display height included; plug-able connectors as mounted in installations excluded*)
Weight	510 grams (*excluding plug-able connectors, packing material*)
DIN-rail	35 mm (*minimum width 65 mm*)
Ambient conditions	
Operating temperature range	-20º to +60º Celsius
	⚠ "WARNING, HOT HOUSING. When in use at an ambient temperature higher than 55ºC or 131ºF, the housing of the Atlas will be hot. Do not touch the housing!"
Storage and shipping conditions	-20º to +85° Celsius
Relative air humidity	Maximum 98%
Ingress protection	IP 20 (*IEC/EN 60529, DIN 40 050*)
Power supply	
Pluggable power supply connector	Pin -: 0 V Pin +: 12 to 24 VDC Pin SH: Shield
Nominal power supply voltage	12 to 24 VDC
Nominal power use	10 W
Maximum power use	24 W
Current consumption (@12VDC)	Max. 2A
Reverse polarity protection	Yes
Redundant power supply	No
Wire diameter	Max. AWG 14 (*max area 2.5 mm^2*) Installation notes: The device shall be powered with a correct power supply: • For North America, the power supply shall be listed and meet the requirements for class 2 • For the rest of the world the power supply shall meet the requirements for limited power sources as defined in IEC/EN 60950-1 cl. 2.5 Possible power supplies: Phoenix STEP-PS series Traco power TCL series XP-power DNR120-480 series
Ethernet	
Connector (Factory and Office)	RJ-45
Maximum cable length	100 m
Link speed	10/100/1000 Mbps
Atlas2 Plus MAC address range	9C:B2:06:2E:00:00 - 9C:B2:06:35:7F:FF
Atlas2 MAC address range	9C:B2:06:35:80:00 - 9C:B2:06:3C:FF:FF

Supported protocols	OPC UA, MQTT, PROFINET (detect only), PROFINET I&M0, Modbus TCP (detect only), Ethernet/IP (detect only)
Protocols used	ARP, ICMP, DCP, SNMP, PROFINET I&M
Default IP address after reset/purchase	Factory: 192.168.0.10 Office: 192.168.1.10
Default login / password	admin / admin
Connections	Up to 20 concurrent web clients

Relay contact	
Resistance	100 to 150 mΩ (including plug)
UL maximum contact rating	max. 10W 24VDC, 400mA

Processor	
Atlas2 Plus	NXP iMX8 QuadMax 4 GB LPDDR4 Memory 16GB eMMC Storage memory Passive Cooling (Fanless)
Atlas2	NXP iMX8M Quad 2 GB LPDDR4 Memory 8 GB eMMC Storage memory Passive Cooling (Fanless)

USB ports	
Type	2x USB3.0; Type A; 900mA per port *(one used for Atlas2 TAP)* 1x USB2.0; Micro type B; 500mA *(recovery channel)*

Display	
OLED (add-on)	PM-OLED 1,45 inch, 160RGBx128 Dots, 262 Colors

LEDs	
Power LED	Green - Power Ok
Network Status (Multi color LED)	Blue - During detection of available updates on USB. Green - All seem to be working correctly. Orange - A situation is present which is important but not serious, user attention recommended. Red - A serious problem is present in the network, user attention required.

Push Buttons	
Factory Reset	Default settings *(first push button at the top of the module, press for 10 seconds)*
System Recovery	Activate firmware programming on USB recovery port *(second push button at the top of the module; push button while connecting Power supply)*

Standards and Approvals	
CE	EMC Directive 2014/30/EU, class B RoHs Directive 2011/65/EU Emission: CISPR32 Immunity: CISPR35
FCC	47 CFR 15 & ICES-003 (Issue 6), class B

22. Technical specifications Mercury

Technical Data - Mercury in general	
Mobile Computing Platform	
Manufacturer, type	Panasonic FZ-M1
Processor	Intel® Core™ i5-7Y57 vPro™ processor
Operating System	Windows 10 Pro
RAM	4 GB (Max. 8 GB)
Graphic Chip	Intel® HD Graphics 615
Camera	Front: 2 MPixel
	Rear: 8 Mpixel with autofocus and LED flash
Storage	128 GB Solid State Drive (Serial ATA)
LCD	7" sunlight-viewable WXGA Active Matrix (TFT) IPS LCD
Touchscreen	10 finger capacitive multi-touchscreen
Bluetooth	Version 4.1 + EDR Class 1
WLAN	Intel® Dual Band Wireless-AC 8265
USB ports	USB 3.0 (1x)
	USB 2.0 (1x)
Expansion slot	Micro SD/SDXC Memory Card
Dimensions, weight and mounting	
Dimensions D x W x H (mm)	203 x 18 x 132 mm
Weight	540 grams
DIN-rail	No, handheld (handstrap and stylus supplied)
Ambient conditions	
Operating temperature	-29º .. +60º Celsius
Storage temperature	– 51° .. +71° Celsius
Relative air humidity	Maximum 98%
Ingress protection	IP 65 (MIL STD 810G and IEC 60529)
Gravity drop resistance test	180 cm
Power supply	
Power supply	Supplied in box. Rated IP 20
Input	100 – 240 VAC
	1.5 A – 0.8 A
Output	16 VDC
	1.75 A
	1.76
Plug	Middle = +
	Outer ring = -
Battery	Lithium-Ion (7.2 V, 3220 mAh)
Ethernet	
Connector	RJ-45
Maximum cable length	100 m
Link speed	10/100/1000 Mbps

Supported protocols	OPC UA, PROFINET (detect only), PROFINET I&M0, Modbus TCP (detect only), Ethernet/IP (detect only)
Protocols used	ARP, ICMP, DCP, SNMP, PROFINET I&M0
Default IP address after reset/purchase	Factory: 192.168.0.10
Default login / password	admin / admin

23. Order codes

Component	Order code	Remarks
Atlas	101-800110	Atlas main unit including mounting materials
ATLAS: PROFINET Permanent Monitoring Kit 100	101-800210	1 x Atlas (101-800110), 1 x EtherTAP: PROFINET Analysis License, (101-700204) , 1 x EtherTAP 10/100 (513-00011A), 1 x TAP Din Rail Mount (UTA 107)
Mercury IE Reliability Solution FZ-M1	101-820220	Panasonic ToughPAD FZ-M1 with Intel Core 5 Processor 4GB of RAM - 128GB SSD, Wifi ONLY, Bluetooth, 1x USB 3.0, 1 X USB 2.0, 1 X RJ45 LAN Port, 1 X SD Card, Front & Rear Camera with stylus pen & standard. Windows 10. Handstrap- 3 year warranty including 5 day pick up and return repair service. WITH OSIRIS STANDARD LICENSE (101-700100)
Mercury IE Reliability Solution FZ-M1	101-821220	PROCENTEC Mercury Standard Kit Includes 1 x Mercury Rugged Tablet (101-820220) , 1 x 360 degree strap (101-820221) , 1 x Carrying Case (101-820222) , 1 x RJ45 to RJ45 3 Meter Cable (123-637GRR3) , 1 x RJ45 to M12 3 Meter Cable (123-642EMR3) , 1 x PROFICORE USB Cable (60010003) OSIRIS Software Standard Package (101-700100) pre-installed and tested.
Mercury IE Reliability Solution FZ-M1	101-822220	PROCENTEC Mercury Plus Kit Includes 1 x Mercury Rugged Tablet (101-820220) , 1 x 360 degree strap (101-820221) , 1 x Carrying Case (101-820222) , 1 x RJ45 to RJ45 3 Meter Cable (123-637GRR3) , 1 x RJ45 to M12 3 Meter Cable (123-642EMR3) , 1 x PROFICORE USB Cable (60010003), 1 X ProfiCore Ultra 2 (10020), 1 X ProfiCore TAP Connectors (13020)

		OSIRIS Software Standard Package (101-700100) pre-installed and tested.
Mercury IE Reliability Solution FZ-M1	101-823220	PROCENTEC Mercury PRO Kit Includes 1 x Mercury Rugged Tablet (101-820220) , 1 x 360 degree strap (101-820221) , 1 x Carrying Case (101-820222) , 1 x RJ45 to RJ45 3 Meter Cable (123-637GRR3) , 1 x RJ45 to M12 3 Meter Cable (123-642EMR3) , 1 x PROFICORE USB Cable (60010003), 1 X ProfiCore Ultra 2 (10020), 1 X ProfiCore TAP Connectors (13020), 1 X ProfiTrace 2 Software (22020), 1 x ProfiTrace SCOPE ware (23010), 1 X ProfiCaptain (22020), 1 x Netilities (39020) OSIRIS Software Standard Package (101-700100) pre-installed and tested.
Mercury: PROFINET Troubleshooting Kit 100	101-824220	1 x Mercury (101-800110), 1 x PN Commissioning Wizard (101-700201), 1 x EtherTAP: PROFINET Analysis License (101-700204) , 1 x EtherTAP 10/100 (513-00011A), 1 x Netilities (39020), 1 x TAP Din Rail Mount (uta 107), 1 x RJ45 to RJ45 3 meter Cable (123-637GRR3), 1 x RJ45 to M12 3 meter Cable (123-642EMR3), 1 x 360 degree hand strap (101-820221), 1 x Carrying Case (101- 820222), 1 x Osiris Software (101-700100) OSIRIS Software Standard Package (101-700100) pre-installed and tested.
Accessories	**Order code**	**Remarks**
Mercury: Optional Panasonic DC Car Charger 12V-32V / 80W	101-820321	Mercury Optional DC powered Car Charing unit for Panasonic Tough PAD 12V-32V/80W
Mercury: Optional Desktop Cradle: Full Version	101-820322	Mercury Optional Desktop Cradle Full Version with: 2 x USB 2.0, 1 x VGA, 1 x HDMI, 1 x LAN RJ45, 1 x Serial

Mercury: Optional Desktop Cradle: Lite Version	101-820323	Mercury Optional Desktop Cradle Lite Version with: 2 x USB 2.0 & 1 x LAN RJ45
Mercury: Optional 4 Bay Battery Charger	101-820324	Mercury Optional 4-Bay Battery Charger (ac adapter is not included. CF-AA5713AG or CF-AA6502A2 is required)
Mercury: Optional EU Plug: AC Charger 220V	101-820325	Mercury Optional Cable for AC Charger that has 220V EU Plug
Mercury: Optional 2-Cell Li-ION Battery	101-820326	Mercury Opional Cell Li-ION Battery for FZ-M1
Mercury: Optional Capacative Stylus PEN FZ-M1	101-820327	Mercur Optional Capacaive stylus pen for FZ-M1
Mercury: Optional Cleaning Cloths	101-820328	Mercury Optional Cloths (tissue) to clean Touchscreen MOQ
Mercury: Optional Protective Screen Films	101-820329	Mercury Optional Protective Film for FZ-M1
Mercury: Power Plug: Australian	101-820330	Mercury Optional replacement power plug: Australian
Mercury: Power Plug: China	101-820331	Mercury Optional replacement power plug: China
Mercury: Power Plug: India/South Africa	101-820332	Mercury Optional replacement power plug: India/South Africa
Mercury: Power Plug: Brazil	101-820333	Mercury Optional replacement power plug: Brazil
Mercury: Power Plug: Italian	101-820334	Mercury Optional replacement power plug: Italian
Mercury: Power Plug: U.K.	101-820335	Mercury Optional replacement power plug: U.K

Mercury: Power Plug: US	101-820336	Mercury Optional replacement power plug: US
Osiris as a Software (on Windows 10)	101-710100	Osiris PC/Laptop

24. Certificates

QualityMasters
Certificering

QualityMasters hereby declares that

Procentec B.V.
Wateringen

has a management system that meets the requirements of the standard

NEN-EN-ISO 9001:2015

for the scope

Providing training courses, technical support, product development, product sales and the exploitation of the test laboratory.

Date of original approval	10-02-2003
Date of issue	14-12-2018
Valid until	10-02-2022
Certificate number	NL 6957-uk

On behalf of QualityMasters,

N.B. The failure to meet the conditions as set forth in the certification agreement, or non-compliance with the given standard and/or guidelines, may lead to the suspension or cancellation of the certificate.
This certificate remains the property of QualityMasters Certificering B.V., Nieuwland Parc 157, 3351 LJ Papendrecht.

CONTROLLED
COMMISSIE
WAARBORGING
ONPARTIJDIGHEID
573324

Iso9001 certificate

25. Sales offices and distributors

HEADQUARTERS	
PROCENTEC Vlasmarkt 1 3011 PW, Rotterdam Netherlands	T: +31-(0)174-671800 F: +31-(0)174-671801 E: info@procentec.com I: www.procentec.com

ARGENTINA	
eFALCOM Alcorta 2411 B1744 - Moreno Buenos Aires Argentina	T: +54 237 46 31 151 F: +54 237 46 31 150 E: santiago.falcomer@efalcom.com I: www.efalcom.com.ar

BELGIUM and LUXEMBOURG	
Bintz Technics N.V. Brixtonlaan 23 B-1930 Zaventem Belgium	T: +32 2 720 49 16 F: +32 2 720 37 50 E: bloemen@bintz.be I: www.bintz.be

BRAZIL	
Westcon Instrument. Indl Ltda Rual Alvaro Rodrigues, 257 São Paulo – SP Brazil - CEP 04582-000	T: +55 11 5561-7488 F: +55 11 5093-2592 E: paolo@wii.com.br I: www.wii.com.br

CANADA	
Streamline Process Management Inc. #3, 4351 – 104 Ave SE Calgary, Alberta T2C 5C6 Canada	T: +1 403 225 1986 F: +1 587 585 2828 E: admin@streamlinepm.com I: www.streamlinepm.com
JCom Automation 1115 Whitefield Dr. K9J 7P4, Ontario Canada	T: 1 705 868 8745 i: www.jcomautomation.ca

CHILE	
RP Ingenieria Limitada Tucapel 92 oficina 52 Concepción Chile	T: +56-(0)41-2469350 F: +56-(0)41-2522592 E: rodrigopinto@rpingenieria.cl I: www.rpingenieria.cl

CHINA	
PROCENTEC Beijing Room E-1115 WangJingYuan YouLeHui ChaoYang Beijing China	T: +86(10)84766911 or 84787311 F: +86(10)84766722 E: info@procentec.net I: www.procentec.net

CZECH REPUBLIC	
FOXON s.r.o. Polní 367 460 01 Liberec 12 Czech Republic	T: +420 484 845 555 F: +420 484 845 556 E: foxon@foxon.cz I: www.foxon.cz

DENMARK

ProSaiCon	T: +45 70 20 52 01
Jernbanegade 23B	F: +45 70 20 52 02
DK 4000 Roskilde	E: hfj@prosaicon.dk
Denmark	I: www.prosaicon.dk

EGYPT

MTSE	T: +20 2 241 475 07
7, Amin Annis St., 4th Sec.	F: +20 2 229 031 60
11341 Cairo	E: hassan.mahdy@mtse.com.eg
Egypt	I: www.mtse.com.eg

ESTONIA

Saksa Automaatika OU	T: +372 605 2526
Peterburi Tee 49	F: +372 605 2524
Tailinn	E: info@saksa-automaatika.ee
EE-11415 Estonia	I: www.saksa-automaatika.ee

FINLAND

Hantekno Oy	T: +358 40 8222 014
Kalliotie 2	E: info@hantekno.com
04360 Tuusula	I: www.hantekno.fi
Finland	

FRANCE

AGILiCOM	T: +33 247 76 10 20
Bâtiment B	F: +33 247 37 95 54
1, rue de la Briaudière	E: jy.bois@agilicom.fr
Z.A. La Châtaigneraie	I: www.agilicom.fr
37510 BALLAN-MIRE	
France	

GERMANY

PROCENTEC GmbH	T: +49-(0)721 831 663-0
Rittnertstraße 19	F: +49-(0)721 831 663-29
D-76227 Karlsruhe	E: info@procentec.de
Germany	I: www.procentec.de

GREECE

ETA ENERGEIA Ltd	T: +30 6945670846
165 Philadelphias str.	F : +30 2310517103
Acharnai ,Athens	E: info@eta.gr
Greece	I: www.eta.gr/en

INDIA

UL Engineering Services & Software Pvt Ltd	T: +91-202 696 0050
Nirman Classic,	F: +91-202 696 2079
Katraj-Kondhwa Road,	E: dileep.miskin@ulepl.com
Katraj, Pune-411046	I: www.ulepl.com
India	

Automation Combine	T: +98 452 84550
B.R House, 4th Floor	F: +93 421 37534
Hennur Main Road	W: www.automationcombine.in
Bangalore 560043, India	

IRELAND

PROFIBUS Ireland
Automation Research Centre
University of Limerick
National Technology Park, Plassey
Limerick
Ireland

T: +353-61-202107 or +35361240240
F: +353-61-202582
E: info@profibus.ie
I: www.profibus.ie

ISRAEL

Instrumetrics Industrial Control
8 Hamlacha St.
New Industrial Zone
Netanya, 42170
Israel

T: +972-9-8357090
F: +972-9-8350619
E: info@instrumetrics-ic.co.il
I: www.inst-ic.co.il

ITALY

PROCENTEC Italy
Via Branze n. 43/45
25123 Brescia
Italy

T: +39 030 200 8610
F: +39 030 238 0059
E: www.procentec.it
W: www.procentec.it

JAPAN

TJ Group
C/O Japanese PROFIBUS Organisation
West World Building 4F
3-1-6 Higashi-Gotanda,
Shinagawa-ku,
Tokyo, 141-0022
Japan

T: +81-3-6450-3739
F: +81-3-6450-3739
E: info@profibus.jp

KOREA

Hi-PRO Tech. Co., Ltd.
#2802, U-Tower, 1029
Youngduk-dong, Giheung-gu
Yongin-Si, Kyunggi-do,
446-908 Korea

T: +82 82-31-216-2640
F: +82 82-31-216-2644
E: chays@hiprotech.co.kr
I: www.profibus.co.kr

MEXICO

F&G GLOBAL Equipment
Rómulo Garza 205
Col. Industrias del Vidrio
San Nicolas de los Garza, NL

T: +81 1933 7754
E: ventas@FGequipment.com
W: www.fgequipment.com

NETHERLANDS

PROCENTEC B.V.
Klopperman 16
2292 JD Wateringen
Netherlands

T: +31 (0)174 671800
F: +31 (0)174 671 801
E: info@procentec.com
I: www.procentec.com

NEW ZEALAND

Mantis Systems
34 Glasgow St.
Dunedis
New Zealand

T: +643 455 6072
F: +31 (0)174 671 801
E: tbaldock@mantis-sys.co.nz
I: www.mantis-sys.co.nz

NORWAY

Nortelco Automation AS	T: +47 22 57 61 00
Johan Scharffenbergs vei 95	E: post@nortelcoautomation.no
N-0694 Oslo	I: www.nortelcoautomation.no
Norway	

PAKISTAN

OTC	T: +92 42 3587 2667-9 Ext. 117
Suite No. 4, 1st Floor Liberty Heights	F: +92 42 3587 2670
Main Boulevard Gulberg	E: nsm@otc.com.pk
Lahore - 54660	I: www.otc.com.pk
Pakistan	

PERU

ControlWare	T: +51 1637 3735
Jr. Los Silicios 5409	F: +51 1528 0454
Los Olivos - L39	E: info@controlware.com.pe
Peru	I: www.controlware.com.pe

POLAND

INTEX Sp. z o.o.	T: +48 32 230 75 16
ul. Portowa 4	F: +48 32 230 75 17
44-102 Gliwice	E: intex@intex.com.pl
Poland	I: www.intex.com.pl

PORTUGAL

IndustrialSys	T: +351 96 716 1605
Rua Alexandre Herculano	I: www.iindustrialsys.pt
Nº25,3530-144 Mangualde	E: joao.costa@industrialsys.pt
Portugal	

ROMANIA

S.C. SVT Electronics S.R.L.	T: +40 365 809 305
Brăila 7	F: +40 365 809 305
540331 Tg-Mure	E: sajgo.tibor@svt.ro
Romania	I: www.svt.ro

RUSSIA

Diagnostics and Monitoring	T: +7 910 251 66 74
St. Lutova 4 – 60	E: rubanova.oi@gmail.com
398036, Lipetsk	
Russia	

SAUDI ARABIA

ASM Process Automation	T: +966 2 691 2741
Al-Zahra Dist. – Attas st.	F: +966 2 682 8943
cross section with helmy Kutby St.	E: info@asmestablishment.com
Villa no.25	I: www.asmestablishment.com
Jeddah-21553	
Saudi Arabia	

SERBIA

MR Process Equipment	T: +381 60 5140 513
Tribalska 15	
11050 Zvezdara	E: mr@mrprocessequipment.com
Serbia	I: www.mrprocessequipment.com

SINGAPORE / SOUTH EAST ASIA

Allegro Electronics
236 Serangoon Avenue 3 07-98
Singapore 550236

T: +65 628 780 63
E: sales@allegro.com.sg
I: www.allegro.com.sg

Gissmatic Automatisierung Pte Ltd (Malaysia)
318 Tanglin Road 01-34
Singapore 247979

T: +65 900 912 76
E: sales@gissmatic.com
I: www.gissmatic.com

SLOVAKIA

FOXON s.r.o.
Polní 367
460 01 Liberec 12
Czech Republic

T: +420 484 845 555
F: +420 484 845 556
E: foxon@foxon.cz
I: www.foxon.cz

SOUTH AFRICA

IDX
1 Weaver Street
Fourways
Johannesburg
South Africa - 2191

T: +27(11) 548 9960
F: +27(11) 465-8890
E: sales@idxonline.com
I: www.idxonline.com

SPAIN

LOGITEK, S.A
Ctra. de Sant Cugat, 63 Esc. B Planta 1ª
Rubí (BARCELONA), 08191
Spain

T: +34 93 588 6767
E: xavier.cardena@logitek.es
I: www.logitek.es

SWEDEN

Nortelco Automation AS
Johan Scharffenbergs vei 95
N-0694 Oslo
Norway

T: +47 22 57 61 00
E: post@nortelcoautomation.no
I: www.nortelcoautomation.no

SWITZERLAND

EME AG
Lohwisstrasse 50
CH-8123 Ebmatingen
Switzerland

T: +41 44 982 11 11
E: mhauri@eme.ch
I: www.eme.ch

TAIWAN

Orion Energy Technology
3F, No. 2, Aly. 6, Ln. 109, Sec. 2, Huanshan Rd.
Neihu District, Tapei City
114, Taiwan

T: +886 9 370 270 96
E: jackychiu76@gmail.com

TURKEY

Emikon Otomasyon
DES Sanayi sitesi 103 sokak
B-7 blok No:16 Yukari Dudullu / Umraniye
Istanbul 34776
Turkey

T: +90 216 420 8347
F: +90 216 420 8348
E: tolgaturunz@emikonotomasyon.com
I: www.emikonotomasyon.com

UNITED ARAB EMIRATES

Synergy Controls
907, IT Plaza Silicon Oasis :
Dubai
United Arab Emirates

T: +971 4 3262692
F: +971 4 3262693
E: sales@synergycontrols.ae

PROCENTEC UK
Digital World Center
1 Lowry Plaza, Suite 620
The Quays, Salford
M50 3UB Manchester
United Kingdom

T: +44-(0)753 430 7696
E: info@procentec.com
I: www.procentec.co.uk

iTech
Unit 1
Dukes Road
Troon
Ayrshire KA10 6QR
United Kingdom

T: +44 (0)1292 311 613
F: +44 (0)1292 311 578
E: sales@itech-troon.co.uk
I: www.itech-troon.co.uk

Parkelect Ltd.
84 Dargan Road
Belfast
BT3 9JU
N. Ireland

T: +44 2890 777743
F: +44 2890 777794
E: jgillan@parkelect.co.uk
I: www.parkelect.co.uk

Grid Connect Inc.
1630 W. Diehl Road
Naperville, Illinois 60563
USA

T: +1 630 245-1445
F: +1 630 245-1717
E: sales@gridconnect.com
I: www.gridconnect.com/procentec.html

Bavitech Corporation
42 Truong Son Street
Ward 2, Tan Binh District
Ho Chi Minh City
Vietnam

T: +84-8-3547 0976
F: +84-8-3547 0977
E: hai.hoang@bavitech.com
I: www.bavitech.com

For the up to date list of the Sales Offices and Distributors see www.procentec.com/company/distributors/. If your country or region is not listed, please contact us. We are still searching for distributors who can cover complete areas or countries.

26. About PROCENTEC

PROCENTEC are an independent Dutch company that supply products, training and consultancy to the Industrial Automation Market. Of primary focus is the development and manufacturing of automation products for PROFIBUS, PROFINET and Industrial Ethernet.

Some of our products are the most recognized solutions on the Market today. **ProfiTrace**, our mobile troubleshooting and maintenance tool has established itself as one of the most pioneering, yet essential tools available to engineers. In contrast our robust **ProfiHub** has, over the last decade, established itself as the go-to solution for ensuring a reliable network infrastructure. The combination of these products within our **ComBricks** solution has seen PPROCENTEC become the primary manufacturer of network components with the integrated capability for remote monitoring and remote asset-management.

Our training facility, the **PROCENTEC Academy**, has certified over 4000 engineers to implement and maintain their PROFIBUS and PROFINET networks to the highest standards available.

The PROCENTEC **Competence Centre** has established itself as the leading consultancy on PROFIBUS and PROFINET projects worldwide, advising on architecture, engineering, training and commissioning. Once a network is commissioned, we have experts available 24/7, to answer questions with maintenance or help troubleshooting a problem.

Products
- Osiris SaaS, Atlas, Mercury
- EtherTAP and EtherMIRROR
- ProfiHub
- ProfiTrace
- ComBricks
- VPGate
- PROFINET tools
- Cables & Connectors

Services
- On-site & Online Support
- Network Audit
- Network Certification
- Consultancy
- Testlab & Democenter
- Competence Center

Training
- PROFIBUS training courses
- PROFINET training courses
- Product training courses

27. Notes

PROCENTEC

Member of the HMS group.

Your network partner.

PROCENTEC Commercial Office
Vlasmarkt 1
3011 PW, Rotterdam

PROCENTEC Delft
Stationsplein 10
2611 BV, Delft

Tel.	0174-671 800
Fax	0174-671 801
Email	info@procentec.com