



Anybus Atlas2 Plus - Next Generation

User Manual

Based on firmware v2.3.0

December 2025



About this document

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.

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.

Copyright © 2025 HMS Industrial Network

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher.

Referenced documents

HMS Industrial Networks. (u.d.). HMS Communication Guide. *1.0*.

Table of Contents

1	Getting Started	5
1.1	Quick Start	5
1.2	Atlas installation instructions	6
1.2.1	Location	6
1.2.2	Position	6
1.2.3	Power supply	6
1.2.4	Relay switch	7
1.2.5	Ethernet connections	7
1.2.6	Micro-USB	8
1.2.7	USB-A ports	8
1.2.8	OLED Display	8
1.2.9	Reset to factory defaults	8
1.2.10	Login	9
2	Setup Wizard	10
3	User interface	11
3.1	Network Status Page	11
3.2	Notifications	13
3.2.1	Muting notifications	13
3.2.2	Deleting notifications	13
3.2.3	Notification Details	13
3.2.4	Adding custom solutions to notifications	14
3.2.5	Advanced Diagnostics	14
3.3	Device List	16
3.4	Topology	17
3.5	EtherTAP	21
3.5.1	Overview	21
3.5.2	Recordings	22
3.6	Message Configuration	24
3.6.1	Global settings	24
3.6.2	Device filters	25
3.7	Reporting	26
4	Settings	27
4.1	General: User Management	28
4.2	Network: Factory and Office interface	32
4.3	Network: SNMP Communities	32
4.4	Measurement: Scan range and Blacklist	32
4.5	Connectivity: MQTT	33
4.6	Connectivity: OPC UA	35
4.7	Firmware Updates	38
4.7.1	How to find the current firmware version	38
4.7.2	Firmware Update License	38
4.7.3	Update via the web interface	39
4.7.4	Update via USB	40
4.7.5	Updating from the old User Interface	40

1 Getting Started

1.1 Quick Start

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

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 yellow traffic light.
STEP 4	Set the IP address of your laptop to 192.168.1.1 and set 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	Change the password as prompted.
STEP 8	Now complete the Setup Wizard but do not change the settings of the Office port yet.
STEP 9	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 and behavior of the Atlas. If connected to a factory network, it will start scanning and gathering information.

1.2 Atlas installation instructions

1.2.1 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 55°C or 131°F, 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.

1.2.2 Position

The Anybus Atlas 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 device 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.

1.2.3 Power supply

The Atlas contains a 3-pin screw type power connector on the front.



Figure 1

The layout is as follows:

- 1 = - (upper pin)
- 2 = + (middle pin)
- 3 = SH (lower pin)

The power supply must comply with the following specifications:

Voltage: 12 .. 24 VDC

Wire diameter: < 2.5 mm²

After the power has been connected, the Atlas will start the boot process. This can take up to 2 minutes. When it is booted, you should see the Traffic Light on the OLED display blink yellow if the Setup Wizard has not been completed, and a measurement has not been started.

1.2.4 Relay switch

The relay switch on the front is currently not implemented.

1.2.5 Ethernet connections

The Anybus Atlas has 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.

Each port has two status LEDs to indicate data being transmitted (upper LED, blinking green rapidly) and an established link (lower LED, green for 100 Mbit/s and orange for 1Gbit/s).

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.

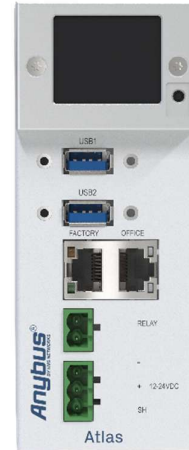


Figure 2 – Atlas2 Plus

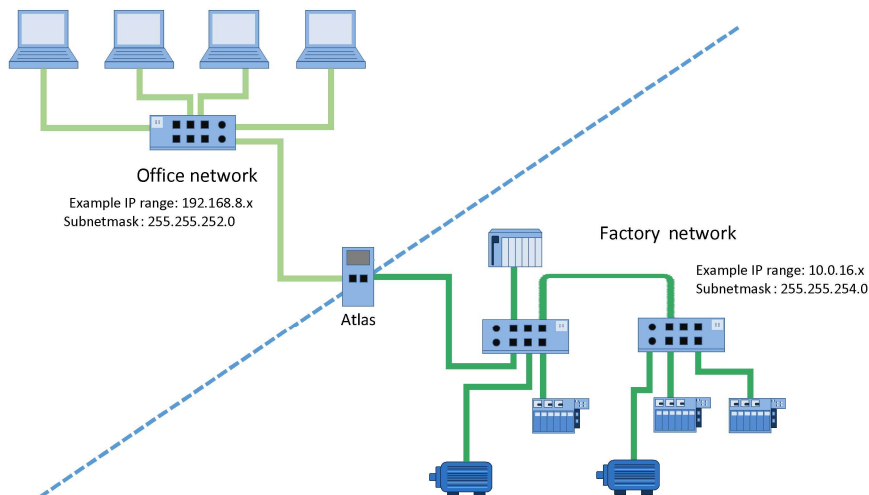


Note: the web interface can be reached on the Office and the Factory network IP range. Therefore it does not matter where you are connected, but you must use the correct IP range and netmask settings of your laptop/client network card. You will only be able to scan and see the devices connected to the 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 3.



1.2.6 Micro-USB

The Micro-USB connection at the bottom of the Atlas has no purpose in normal use. It is used to program the device.

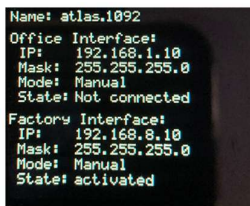
1.2.7 USB-A ports

The two USB-A ports on the front of the Atlas2 Plus can be used for connection with an EtherTap (see paragraph 3.5) and a USB flash drive for upgrading the firmware (see 4.7.4).

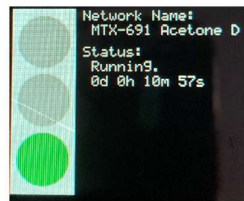
1.2.8 OLED Display

The OLED Display of the Atlas will display the following details:

- Traffic light status of the network
- Network name
- Measurement status
- Measurement time
- Atlas device name
- Factory Interface IP settings
- Office Interface IP settings



```
Name: atlas.1092
Office Interface:
IP: 192.168.1.10
Mask: 255.255.255.0
Mode: Manual
State: Not connected
Factory Interface:
IP: 192.168.8.10
Mask: 255.255.255.0
Mode: Manual
State: activated
```



```
Network Name:
MTX-691 Acetone D
Status:
Running.
0d 0h 10m 57s
```

1.2.9 Reset to factory defaults

If the device needs to be reset to factory defaults, proceed as follows:

1. Make sure the device is powered.
2. Locate the reset button on top of the device, between the ventilation ribs. The button closest to the front is the reset button. Press and hold with a small screwdriver for 20 seconds, then release. The reset procedure takes several minutes. You will not see visual feedback, just wait until the Atlas2 Plus is finished.

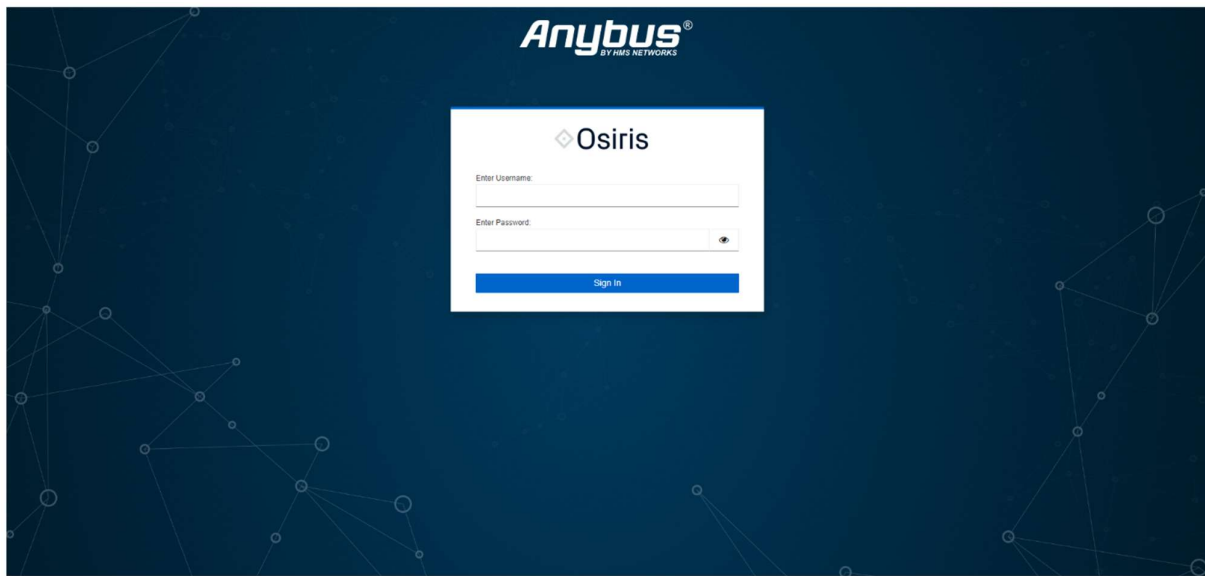
1.2.10 Login

After connecting the office interface of the Atlas to the local network you can use a browser to open the webserver on its IP address.

Default Office interface: 192.168.1.10

Default Factory interface: 192.168.0.10

The web browser will prompt you the following screen:



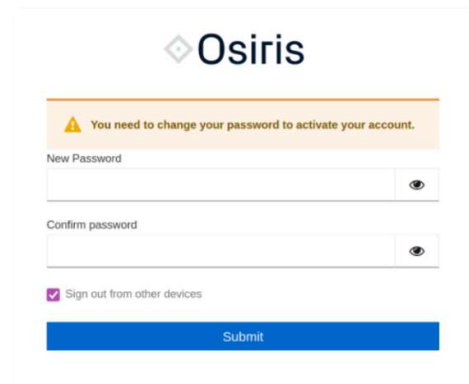
The default login credentials are:

Username: **admin**

Password: **admin**

After first login you will be prompted to change the password.

If you do not remember the admin password, see paragraph 1.2.9 to reset to factory defaults.



2 Setup Wizard

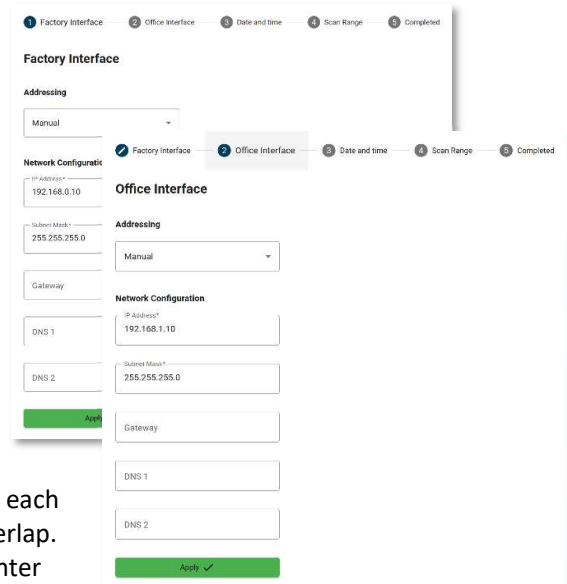
Once the password has been changed, you will be guided through the Setup Wizard, which helps you to set up the Atlas for use in your network. The Wizard is automatically started at first use.

Step 1 & 2

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.



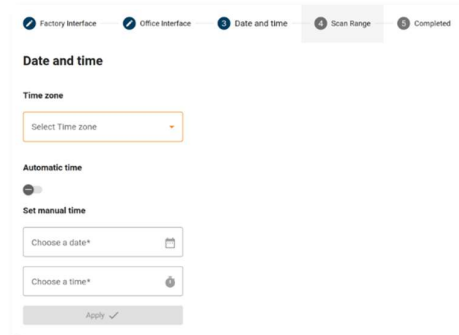
Important: it is required that the Office IP range and Factory IP range are different from each other, and that their subnet masks do not overlap. Gateway and DNS are not mandatory. Only enter one gateway, preferably the one for the Office interface.



The screenshot shows the 'Factory Interface' and 'Office Interface' configuration screens. The 'Factory Interface' screen has fields for 'Addressing' (Manual), 'IP Address*' (192.168.0.10), 'Subnet Mask*' (255.255.255.0), 'Gateway', 'DNS 1', and 'DNS 2'. The 'Office Interface' screen has similar fields for 'Addressing' (Manual), 'IP Address*' (192.168.1.10), 'Subnet Mask*' (255.255.255.0), 'Gateway', 'DNS 1', and 'DNS 2'. Both screens have an 'Apply' button at the bottom.

Step 3

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 Atlas has internet connectivity or when you manually set local time servers in the settings after the Setup Wizard has been completed.

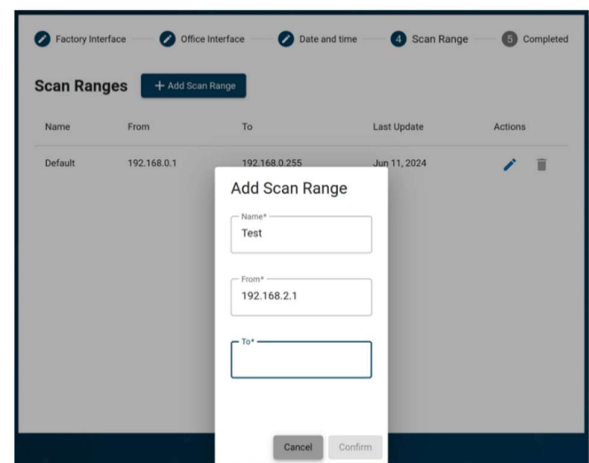


The screenshot shows the 'Date and time' configuration screen. It has a 'Time zone' dropdown menu with 'Select Time zone' as the selected option. Below it, there is a section for 'Automatic time' with a toggle switch. Underneath, there is a 'Set manual time' section with 'Choose a date*' and 'Choose a time*' dropdown menus. An 'Apply' button is at the bottom.

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.

For more information, see paragraph 4.4.



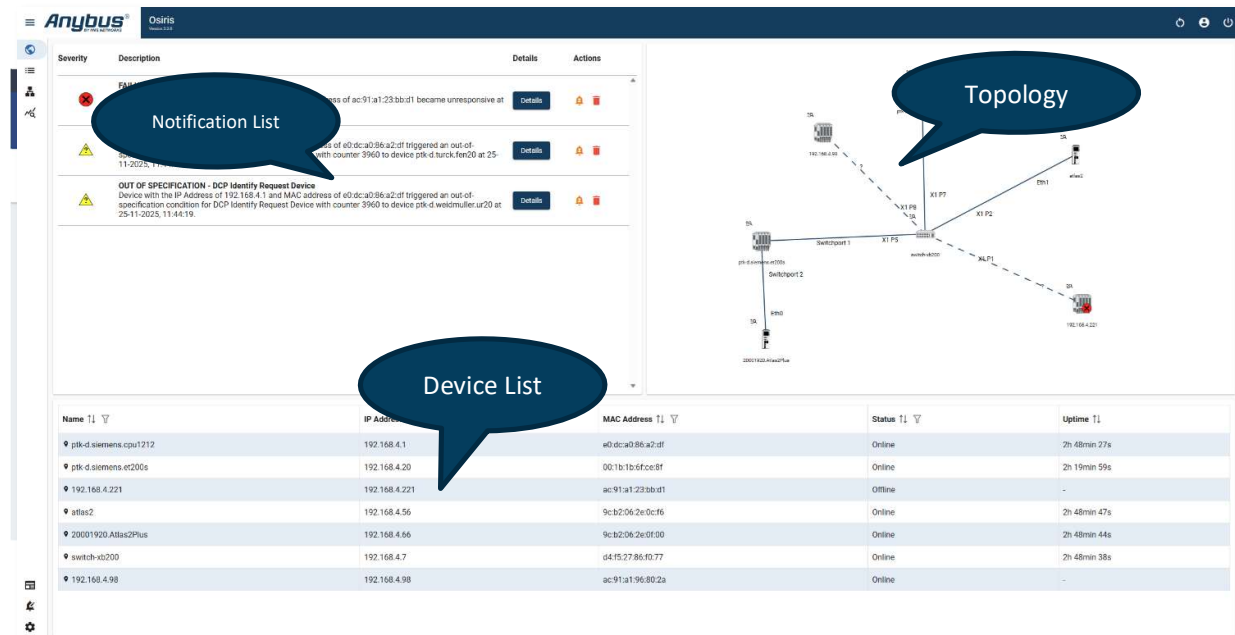
The screenshot shows the 'Scan Ranges' configuration screen. It has a table with columns: Name, From, To, Last Update, and Actions. The table contains one row: Default, 192.168.0.1, 192.168.0.255, Jun 11, 2024. There is an 'Add Scan Range' button at the top right. A modal window titled 'Add Scan Range' is open, showing fields for 'Name*' (Test), 'From*' (192.168.2.1), and 'To*'. There are 'Cancel' and 'Confirm' buttons at the bottom of the modal.

3 User interface

The user interface 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. The default address is 192.168.1.10 for the Office connection and 192.168.0.10 for the Factory connection.

3.1 Network Status Page

The opening window of the user interface is called the “Network Status Page”. It contains three main elements, allowing you to get quick access to data regarding troubleshooting a network.



Name	IP Address	MAC Address	Status	Uptime
pk-d.siemens.cpu1712	192.168.4.1	e0:dc:a0:86:a2:df	Online	2h 48min 27s
pk-d.siemens.ec200s	192.168.4.20	00:1b:1b:8f:ce:8f	Online	2h 19min 59s
192.168.4.221	192.168.4.221	ac:91:a1:23:bb:d1	Offline	-
ytas2	192.168.4.56	9c:b2:06:2e:0c:f6	Online	2h 48min 47s
20001920.Atlas2Plus	192.168.4.66	9c:b2:06:2e:0f:00	Online	2h 48min 44s
switch-xb200	192.168.4.7	d4:15:27:86:f0:77	Online	2h 48min 38s
192.168.4.98	192.168.4.98	ac:91:a1:96:80:2a	Online	-

Notification List

This list displays all notifications. The notifications are sorted in order of severity. You can mark a notification as “Solved”. By doing so the notification will be removed from the list until it happens again on another device.

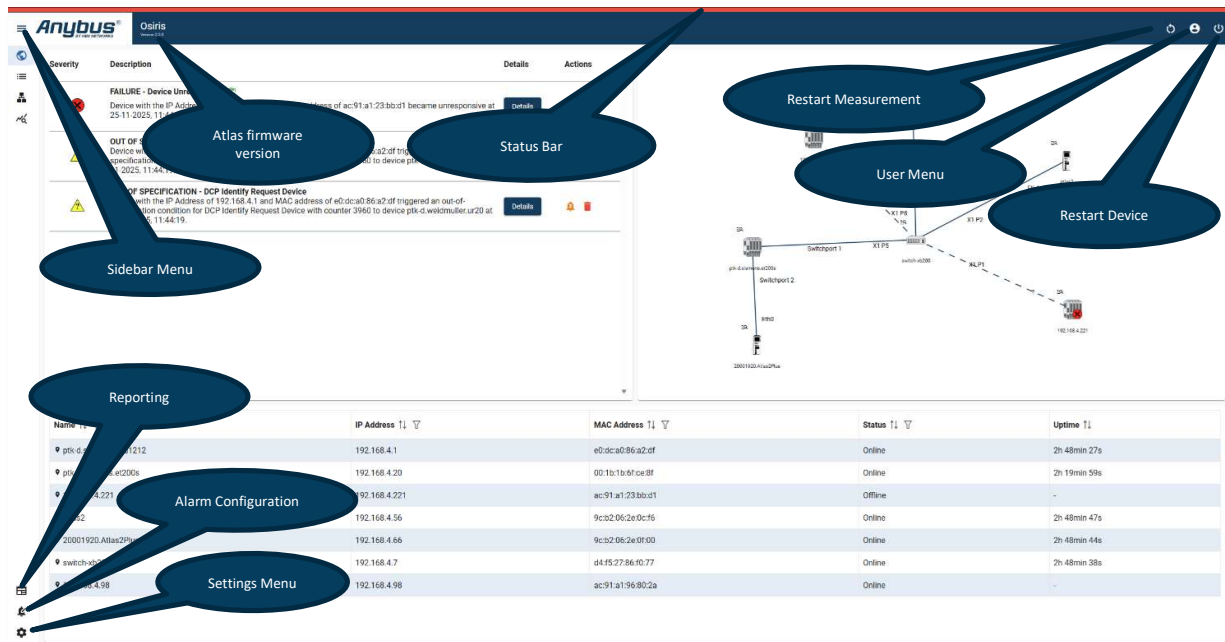
Topology

A small (zoomable) visualization of the graphical topology of the network.

Device List

A concise version of the device list, allowing you to quickly identify any troublesome devices in the network.

Other items on the Network Status Page are:



Atlas Firmware version

The currently running firmware version of Atlas2 Plus is displayed here.

Status Bar

The Status Bar shows the network condition based on a traffic light coloring system. The bar can be green, blue, orange or red. The colors correspond to the notification levels described in 3.2.

Restart Measurement

Use this button to reset the measurement and all recorded data.

Restart Device

This option will perform a restart of the Atlas2 Plus operating system. Recorded information will not be deleted, except for any recorded PCAP files in the EtherTAP section.

User Menu

Access this menu to change the password or sign out of the Atlas2 Plus webpage.

Report

Create a report of all findings of the measurement, in PDF format.

Alarm Configuration

This will bring up the Alarm Configuration page where you can modify the thresholds and triggers of the alarms and notifications.

Settings

You can open the settings menu here.

Sidebar Menu

Allows you to expand/fold the sidebar menu.

3.2 Notifications

The colour of the status bar indicates if there are any errors or warnings to be reported. In case of no notifications: the bar will be green. In other conditions it can turn into one of the following colours.



Maintenance Required



Out of Specification



Failure

The icons in the notification list have the same corresponding colour as the status bar.

Notifications are sorted by severity and time, so you will find all 'Failures' on top, which are sorted by newest to oldest. Below that are all 'Out of Specification' notifications, also sorted by newest first.

Each notification row can be clicked, which filters for the IP or MAC address mentioned in that notification. This allows you to see all notifications for that specific device. Click again to see all notifications.

3.2.1 Muting notifications

The orange bell  on the right of a notification allows you to mute this type of notification. It disables the specific notification for a specific device, depending on the type of notification.

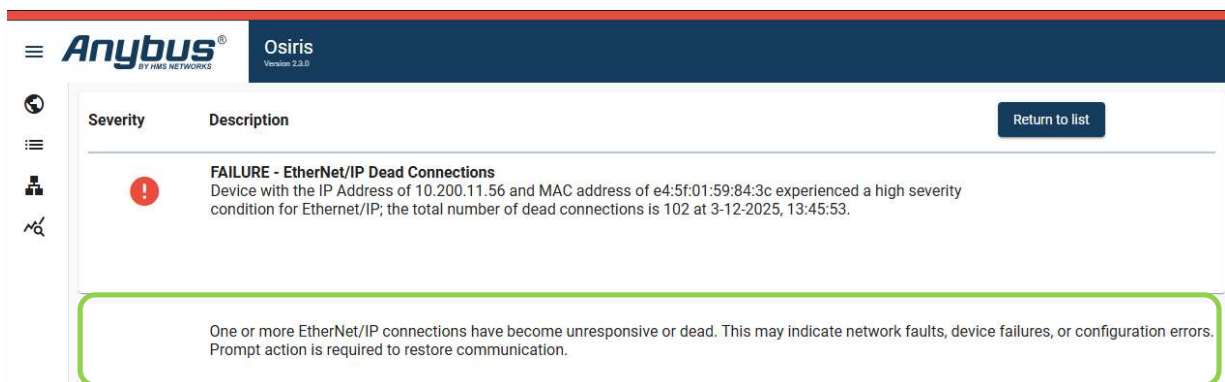
An overview of all muted notifications is listed in the Message Configuration, under 'Device filters' tab. See paragraph 3.6.2. You can also remove these filters there.

3.2.2 Deleting notifications

Click the red trash can  on the right of a notification to remove it. This is different from the Mute button, because it will only remove that specific entry. When the same problem reoccurs, the notification will show again.

3.2.3 Notification Details

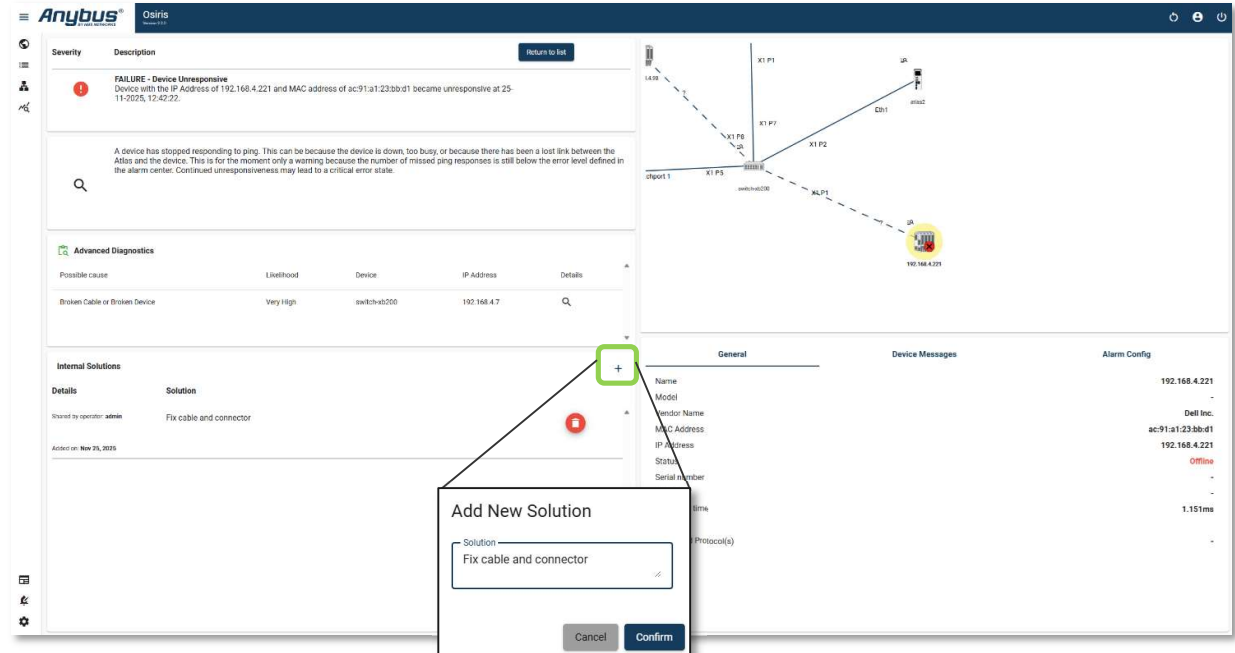
You can get more in-depth information about the notification by clicking on the "Details" button. The text explaining the notification helps to find the cause and solution for the problem.



The screenshot shows the Anybus Osiris web interface. The top header includes the Anybus logo and 'Osiris Version 2.0.0'. A sidebar on the left contains navigation icons. The main content area displays a notification table with columns 'Severity' and 'Description'. A notification with a red severity icon is shown: 'FAILURE - EtherNet/IP Dead Connections'. The description states: 'Device with the IP Address of 10.200.11.56 and MAC address of e4:5f:01:59:84:3c experienced a high severity condition for Ethernet/IP; the total number of dead connections is 102 at 3-12-2025, 13:45:53.' Below the table, a green-bordered box contains a detailed message: 'One or more EtherNet/IP connections have become unresponsive or dead. This may indicate network faults, device failures, or configuration errors. Prompt action is required to restore communication.' A 'Return to list' button is located in the top right of the notification row.

3.2.4 Adding custom solutions to notifications

Press the + sign in the Internal Solutions field to add your (custom) resolution or note to the notification. Whenever the same notification reappears, the custom solution will appear in this field, allowing you to have a much quicker insight to how to resolve the problem.



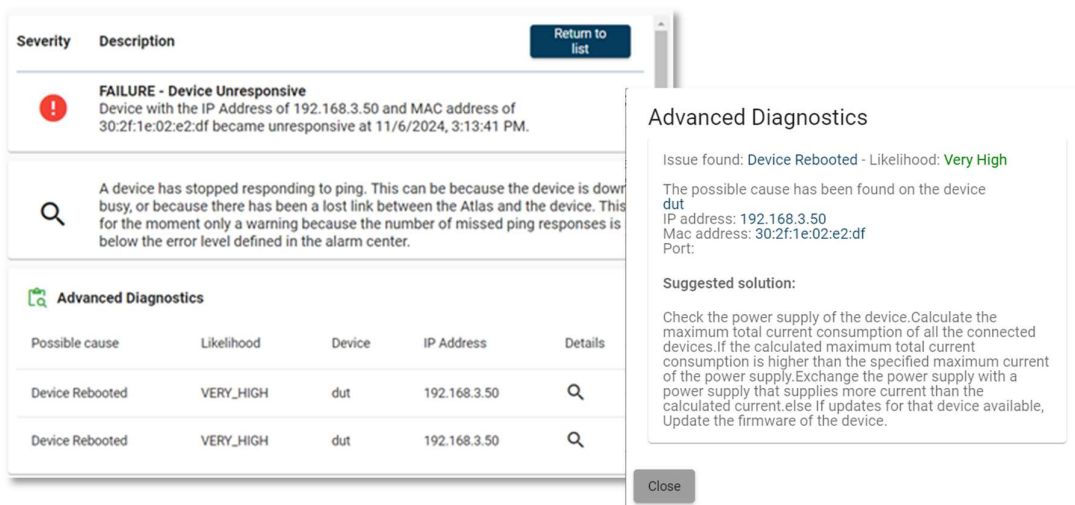
3.2.5 Advanced Diagnostics

If the Advanced Diagnostics license is installed, you see a green icon if there is further information about this type of error and if the Details page shows the Advanced Diagnostics.

Advanced Diagnostics is a feature that guides you towards the most likely cause of certain network errors.

The Atlas2 Plus takes two minutes after triggering an event to analyze the data and to provide you with feedback and directions. This is done internally in the Atlas2 Plus and does not require an internet connection.

Some examples of events explained by Advanced Diagnostics:



Severity	Description	Details	Actions
	FAILURE - Device Unresponsive Device with the IP Address of 192.168.4.221 and MAC address of ac:91:a1:23:bb:d1 became unresponsive at 25-11-2025, 11:55:07.	Details	 
	OUT OF SPECIFICATION - DCP Identify Request Device Device with the IP Address of 192.168.4.1 and MAC address of e0:dc:a0:86:a2:df triggered an out-of-specification condition for DCP Identify Request Device with counter 4232 to device ptk-d.weldmuller.ur20 at 25-11-2025, 11:55:49.	Details	 
	OUT OF SPECIFICATION - DCP Identify Request Device Device with the IP Address of 192.168.4.1 and MAC address of e0:dc:a0:86:a2:df triggered an out-of-specification condition for DCP Identify Request Device with counter 4232 to device ptk-d.turck.fen20 at 25-11-2025, 11:55:49.	Details	 

Severity

Description

Return to list

!

FAILURE - Device Unresponsive

Device with the IP Address of 192.168.4.221 and MAC address of ac:91:a1:23:bb:d1 became unresponsive at 25-11-2025, 12:34:47.

A device has stopped responding to ping. This can be because the device is down, too busy, or because there has been a lost link between the Atlas and the device. This is for the moment only a warning because the number of missed ping responses is still below the error level defined in the alarm center. Continued unresponsiveness may lead to a critical error state.

Advanced Diagnostics

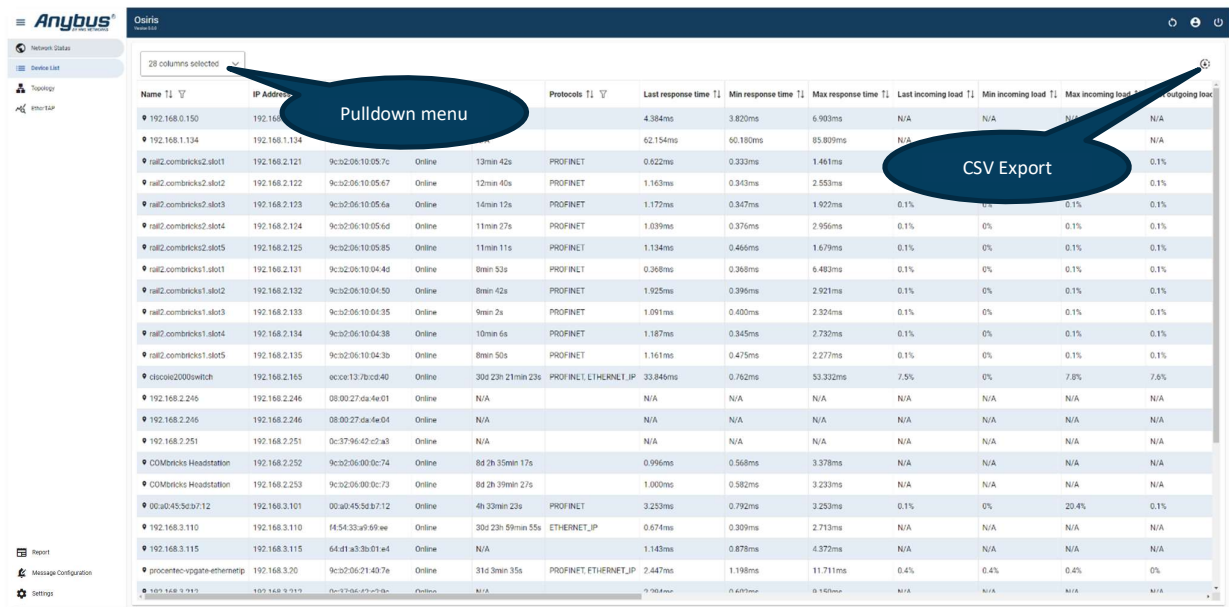
Possible cause	Likelihood	Device	IP Address	Details
Broken Cable or Broken Device	Very High	switch-xb200	192.168.4.7	

The following events can be analyzed by Advanced Diagnostics:

- Broken Cable / Broken Cable or Broken Device
- Cable Too Long
- EMC Issues
- Overloaded Device
- Port Disabled by user
- Duplex Configuration Mismatch
- MTU Configuration Mismatch
- Rebooted Device

3.3 Device List

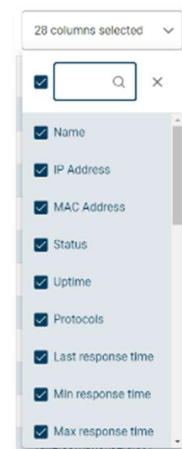
You can access the Device List through the sidebar menu. This feature gives full insight into all the devices / assets which are connected to the network, and which are discovered by the Atlas2 Plus.



The dropdown menu makes it easy to hide or show columns. Use the filter box to easily find columns you wish to select.

At the top right there is an export button to download the Device List into a .CSV formatted file. The file will appear in the Downloads folder of your browser.

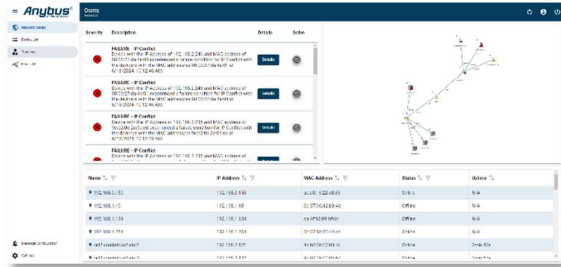
Note that there is a horizontal scrollbar at the bottom of the Device List, because there are many more columns than can fit on most screens.



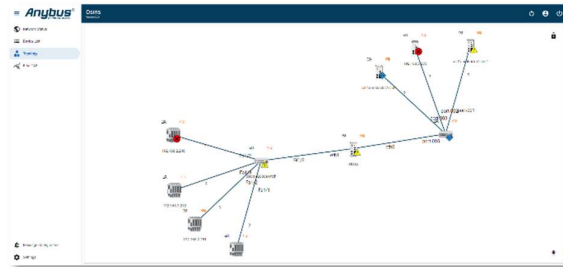
3.4 Topology

The graphical Topology can be found on two different pages:

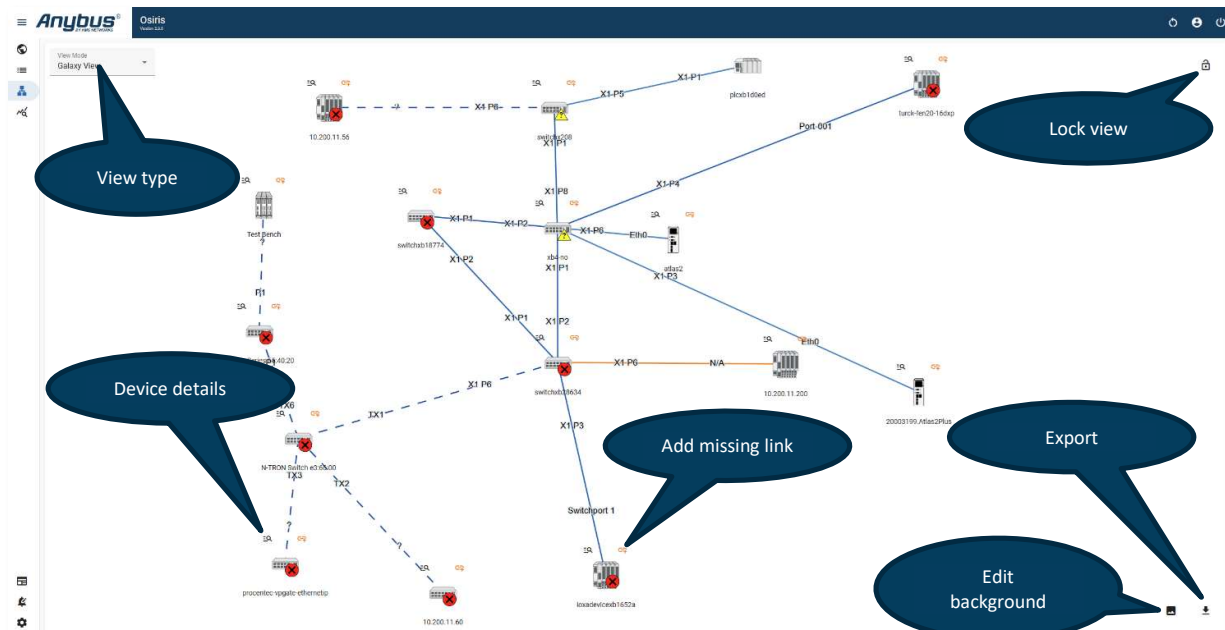
Small topology view on the Network Status page:



Full size topology view on the Topology page:



The full-size topology view has several features which are not available in the small view on the network status page.

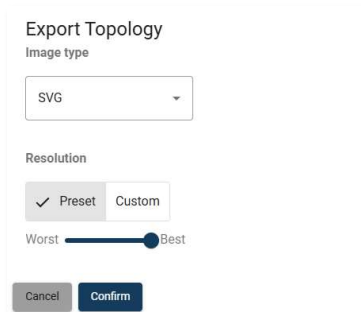


View type

There are two views for the Topology: Galaxy and Tree view. The Galaxy offers extra functionalities (Background and Lock, see below), the Tree view is a static view.

Export

You can export the Topology to an image in either a PNG, JPG or SVG format. After clicking 'Confirm' the file will be downloaded to your default browser download location.



Lock (Galaxy view only)

This locks the devices to their position. You can drag the devices around and drop them where needed. The devices will now stay in this place until the "Lock View" button is disabled.

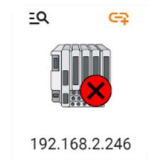
Background (Galaxy view only)

Add a background picture of a company logo or a floorplan for example. This can be very helpful when looking for the location of a certain error or device. After uploading an image you can zoom in and out, reduce or increase opacity, and save, delete or cancel the background settings.



Add Missing Link

When the physical connection of a device cannot be determined, the device will show as a disconnected device in the topology. By clicking on the orange symbol in the top right corner of a device you can manually add the link for the disconnected device.



Select port

Ports*

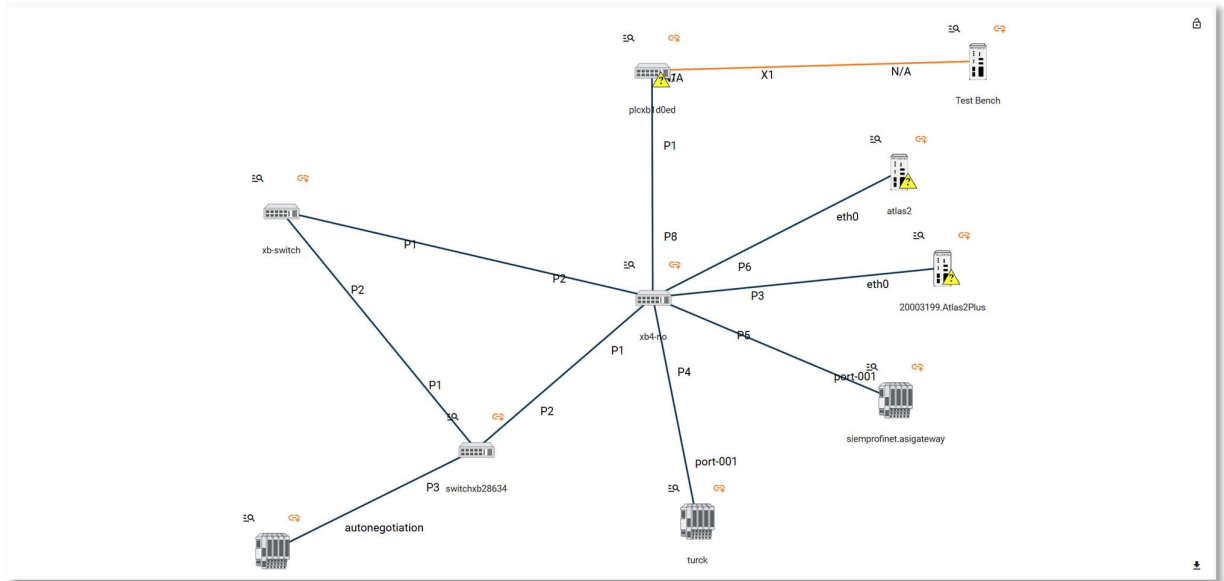
Cancel Confirm

Select which port of the device to draw the link to. When port names can be read from the device data, they will be displayed in the dropdown menu. If no port names can be read, just select the “no port” option.

Then, do the same with the device on the other end of the link. The manually added link will now appear as an orange link in the topology.

Link types

Lines (links) in the Topology can be uninterrupted lines or dotted lines. The information from uninterrupted lines is certain; it comes from SNMP data from the devices. A dotted line means the information is not certain and comes from the MAC list in the switch. It can indicate missing SNMP information and it is possible that there are more devices on that link that cannot be displayed.



The manually added links can be removed at any time by clicking on the orange link, followed by clicking on “Delete link”.

The port numbers of the devices in the topology are based on the port names in the SNMP data of the device. Therefore, this can result in port numbers being displayed in different formats as this could vary per vendor.

Device Details

The upper left corner of a device in the Topology has a magnifier icon, which, if clicked, opens the Device Details. This page has three parts:

Device details (top left), with 3 tabs

General	Device Messages	Alarm Config
Name		switchxb18774
Model		SCALANCE X-200
Vendor Name		SIEMENS AG
MAC Address		00:1b:1b:ad:88:51
IP Address		10.200.11.138
Status		Online
Serial number		VPE9128968
Uptime		15min 57s
Response time		1.185ms
Role		Device
Supported Protocol(s)		PROFINET

The left tab shows the General device details. The middle tab ‘Device Messages’ lists all events related to this device, and the right tab ‘Alarm Config’ has a customizable list of alarms, which are specific to this device. They correspond to the same alarms in the Alarm Configuration (see paragraph 3.6 and)

Topology (top-right) This shows the device in the Topology.

Port information (bottom)

The port information shows port status, connected device on the other side of the link, IP address of that device, Incoming and Outgoing port loads, connection speed, and (if available) the Cable length. This cable length can be calculated if the device supports it.

Port	Operational Status	Connected device	IP	Incoming load	Outgoing load	Speed	Cable Length
Siemens, SIMATIC NET, Ethernet Port, X1 P1 (X1 P1)	Up	switch208	10.200.11.69	0.2%	0.2%	100 Mbit/s	-
Siemens, SIMATIC NET, Ethernet Port, X1 P2 (X1 P2)	Up	Test Bench	10.200.11.5	0.2%	0.2%	100 Mbit/s	-

3.5 EtherTAP

When you connect an EtherTAP to the Atlas2 Plus, you will be able to receive additional 'passive' diagnostics data from the network. This additional data can be accessed by browsing to the EtherTAP page via the menu on the left-hand side. Passive here means that the data is simply captured and measured on the link, not retrieved from a device.

The 'View' drop-down box allows you to choose between the Overview and the Recordings.

3.5.1 Overview

This screen provides you with the following information:

The screenshot shows the Anybus EtherTAP Overview page. At the top, it displays the status 'Connected' and 'Type: EtherTAP 1G_v6'. Below this, there are two main sections: Port A and Port B. Each section contains a table for Network Load and Errors. Below these, there are two large tables: Profinet Connections and Ethernet/IP Connections. The Profinet Connections table shows details for various MAC addresses, including Source MAC, Destination MAC, Frame ID, Direction, Cycle time, Last Jitter, Max Jitter, Max Consecutive Dropped Packets, Total Dropped Packets, Processed Packets, and Last Updated. The Ethernet/IP Connections table shows details for various IP addresses, including Source IP, Destination IP, Connection ID, Direction, API (ms), Last Jitter, Max Jitter, Max Consecutive Dropped Packets, Total Dropped Packets, Processed Packets, Status, and Last Updated.

Port A		Port B	
Rule	Amount	Rule	Amount
Network Load			
Min	0.1%	Min	0.1%
Max	0.4%	Max	0.2%
Last	0.2%	Last	0.2%
Errors			
CRC	0	CRC	0
Jabber	0	Jabber	0
Collisions	0	Collisions	0
Total	0	Total	0

Profinet Connections											
Source MAC Address	Destination MAC Address	Frame ID	Direction	Cycle time (ms)	Last Jitter	Max Jitter	Max Consecutive Dropped Packets	Total Dropped Packets	Processed Packets	Status	Last Updated
8c:f3:19:12:22:3d	20:87:56:14:0a:16	0x8000	Output	128	0.015%	0.094%	0	0	5728	Alive	Dec 8, 2025, 11:09:32 AM
8c:f3:19:12:22:3d	00:1b:10:ad:68:51	0x8000	Output	128	0.009%	0.073%	0	0	5729	Alive	Dec 8, 2025, 11:09:32 AM
8c:f3:19:12:22:3d	00:1b:10:6f:cc:89	0x8000	Output	64	0.016%	0.188%	0	0	11463	Alive	Dec 8, 2025, 11:09:32 AM
20:87:56:14:0a:16	8c:f3:19:12:22:3d	0x8005	Input	128	2.742%	8.685%	0	0	5729	Alive	Dec 8, 2025, 11:09:32 AM
00:1b:10:ad:68:51	8c:f3:19:12:22:3d	0x8004	Input	128	3.741%	6.808%	0	0	5730	Alive	Dec 8, 2025, 11:09:32 AM
00:1b:10:6f:cc:89	8c:f3:19:12:22:3d	0x8001	Input	64	0.001%	0.256%	0	0	11461	Alive	Dec 8, 2025, 11:09:32 AM

Ethernet/IP Connections											
Source IP Address	Destination IP Address	Connection ID	Direction	API (ms)	Last Jitter	Max Jitter	Max Consecutive Dropped Packets	Total Dropped Packets	Processed Packets	Status	Last Updated
10.200.11.56	10.200.11.75	0x5870	Input	300.001	0.004%	0.128%	0	0	2420	Alive	Dec 8, 2025, 11:09:32 AM
10.200.11.56	10.200.11.60	0x420081	Input	10	0.192%	4.172%	0	0	72280	Alive	Dec 8, 2025, 11:09:32 AM
10.200.11.56	10.200.11.70	0x9532	Input	300	0.003%	0.157%	0	0	2420	Alive	Dec 8, 2025, 11:09:32 AM
10.200.11.56	10.200.11.65	0x040001	Input	20	0.093%	1.527%	0	0	36640	Alive	Dec 8, 2025, 11:09:32 AM
10.200.11.65	239.193.103.0	0x020001	Input	10.996	0.426%	14.814%	0	0	36640	Alive	Dec 8, 2025, 11:09:32 AM
10.200.11.60	10.200.11.56	0x0140896	Input	9.998	0.201%	21.569%	0	0	72280	Alive	Dec 8, 2025, 11:09:32 AM
10.200.11.70	10.200.11.56	0x42008570	Input	300.005	0.004%	1.305%	0	0	2420	Alive	Dec 8, 2025, 11:09:32 AM

Port A Statistics

Diagnostic details concerning Port A of the EtherTAP.

These details concern the network load and ethernet errors (CRC, Jabber and Collisions).

Port B Statistics

Diagnostic details concerning Port B of the EtherTAP.

These details concern the network load and ethernet errors (CRC, Jabber and Collisions).

PROFINET Details

The table in the center will display PROFINET details which are gathered from the EtherTAP. These are details such as Frame IDs, cycle times, jitter and dropped packets.

Ethernet/IP details

The table in the center will display Ethernet/IP details which are gathered from the EtherTAP. These are details such as Connection IDs and directions, API times, jitter, dropped packets and Connection status.

Cycle Time

Measured based on the cycle counter in PROFINET packets.

Jitter

Deviation from the expected cycle time in percentage. So if the cycle time is set to 4ms, and the jitter is 10%, the jitter is 0.4ms. Recommended maximum jitter should not be higher than 25%.

API

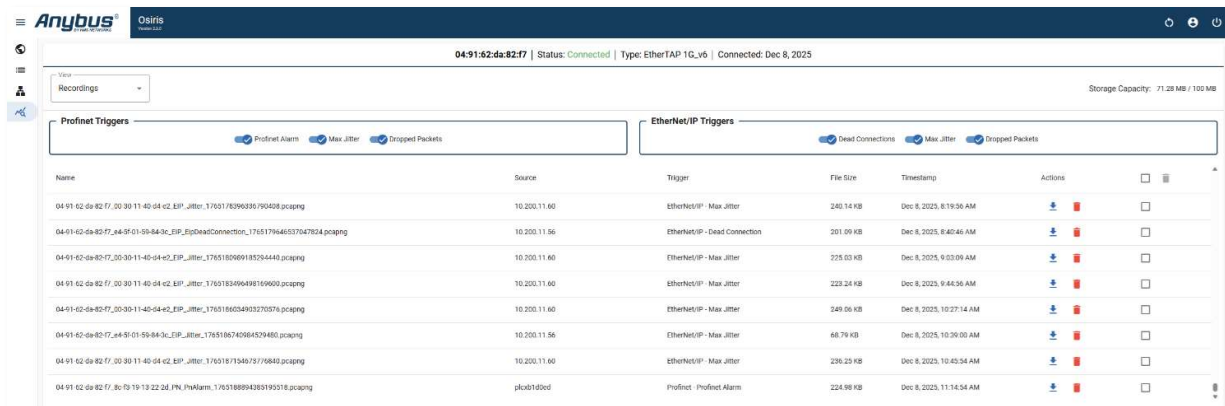
Actual Packet Interval. This is the measured interval between packets on Ethernet/IP devices.

Dropped packets

The EtherTap detects missing packets by looking at the cycle counter inside the data, and shows them as dropped packets.

3.5.2 Recordings

This screen shows all automatically recorded events and has a manual recording feature. The recorded files are recordings of all packets during a certain triggered event, and can be viewed with a packet analyzer (e.g. Wireshark).



The event triggers can be switched on or off, and are divided in Profinet and Ethernet/IP events.

The columns 'Source' and 'Timestamp' can be sorted up/down, to help finding certain recordings easier.

The download icon allows you to download the file, and the red Trash Can icon will delete the recording. It is possible to select multiple or all files for deletion with the checkbox on the right, and delete them in one action.

Manual Recording

This feature allows you to capture a recording of all traffic passing through the EtherTAP. The slider on the left lets you configure the file size of the captured recording file. This can vary between 1 MB and a maximum of 25 MB. Once the recording has stopped, a .PCAP file becomes available for download. The recorded .PCAP file will not be stored automatically and will be lost when refreshing the page or when navigating to a different page. The existing file will also be overwritten when a new recording is started.



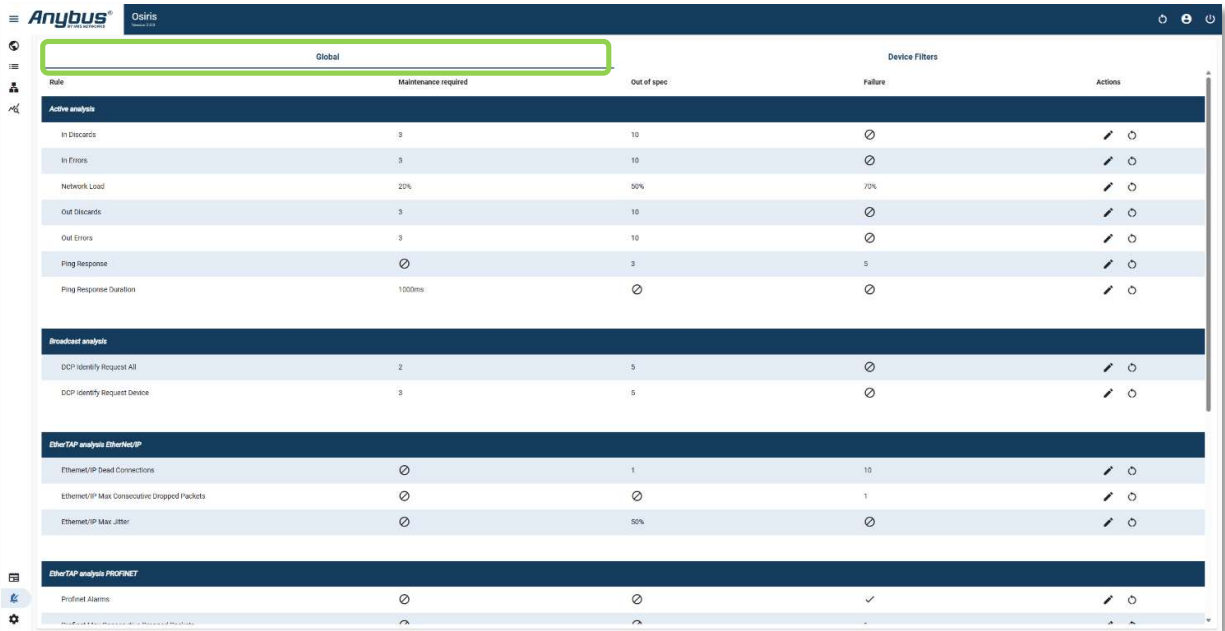
When the recording is finished, or if you click on 'Stop recording', the file is available for download in the list above, with timestamp and file size.

Note that in the top right corner you can find the Storage Capacity. A total of 100 MB is available for recordings. If the buffer is full, and new recordings are added (either manually or triggered), the first entry or entries will be deleted to make space for the new recording.

3.6 Message Configuration

3.6.1 Global settings

The Atlas2 Plus comes with a default set of triggers and thresholds for notifications. These thresholds can be modified and customized to be most efficient and meet demands of the specific network it is connected to. Each type of notification can be modified for each level of notification.



Rule	Maintenance required	Out of spec	Failure	Actions
Active analysis				
In Discards	3	10	⊗	✎ ⊗
In Errors	3	10	⊗	✎ ⊗
Network Load	20%	50%	70%	✎ ⊗
Out Discards	3	10	⊗	✎ ⊗
Out Errors	3	10	⊗	✎ ⊗
Ping Response	⊗	3	5	✎ ⊗
Ping Response Duration	1000ms	⊗	⊗	✎ ⊗
Broadcast analysis				
DCP Identify Request All	2	5	⊗	✎ ⊗
DCP Identify Request Device	3	5	⊗	✎ ⊗
EtherTAP analysis Ethernet/IP				
Ethernet/IP Dead Connections	⊗	1	10	✎ ⊗
Ethernet/IP Max Consecutive Dropped Packets	⊗	⊗	1	✎ ⊗
Ethernet/IP Max Jitter	⊗	50%	⊗	✎ ⊗
EtherTAP analysis PROFINET				
Profinet Alarms	⊗	⊗	✓	✎ ⊗

If needed, they can also be easily reset to the default settings by clicking on the Reset button on the far-right side of each type of notification.

The following alarms can be monitored with the Atlas2 Plus:

In/Out Errors: if a device detects an incorrect frame when receiving/sending an ethernet frame, it will increase the In/Out Error counter by one.

In/Out Discards: if a device needs to discard incoming/outgoing message due to lack of space in the internal buffers, it will increase the In/Out Discard by one.

Network Load: maximum load on link detected during (active) analysis in the current measurement.

Ping Response: If a device is not answering to a discovery message, the ping packet loss counter will be increased.

Ping Response Duration: This is the response time of the device during the discovery cycle of Osiris.

DCP Identify Request All: number of DCP Multicast All messages sent by a device (usually a Profinet Controller).

DCP Identify Request Device: number of Profinet DCP Multicast messages sent to a single device.

Ethernet/IP Dead Connections: When a connection stops, it is declared dead after some time.

Ethernet/IP Max Consecutive Dropped Packets: Missing consecutive packets.

Ethernet/IP Max Jitter: The maximum allowed deviation from the API in percentage.

Profinet Alarms: Alarms sent to/from a Controller.

Profinet Max Consecutive Dropped Packets: Missing consecutive packets.

Profinet Max Jitter: The maximum allowed deviation from the Cycle Time in percentage.

Siemens SFP Current: The current draw of the SFP in the Siemens switch.

Siemens SFP RX Power: The Receiving power of the SFP in the Siemens switch.

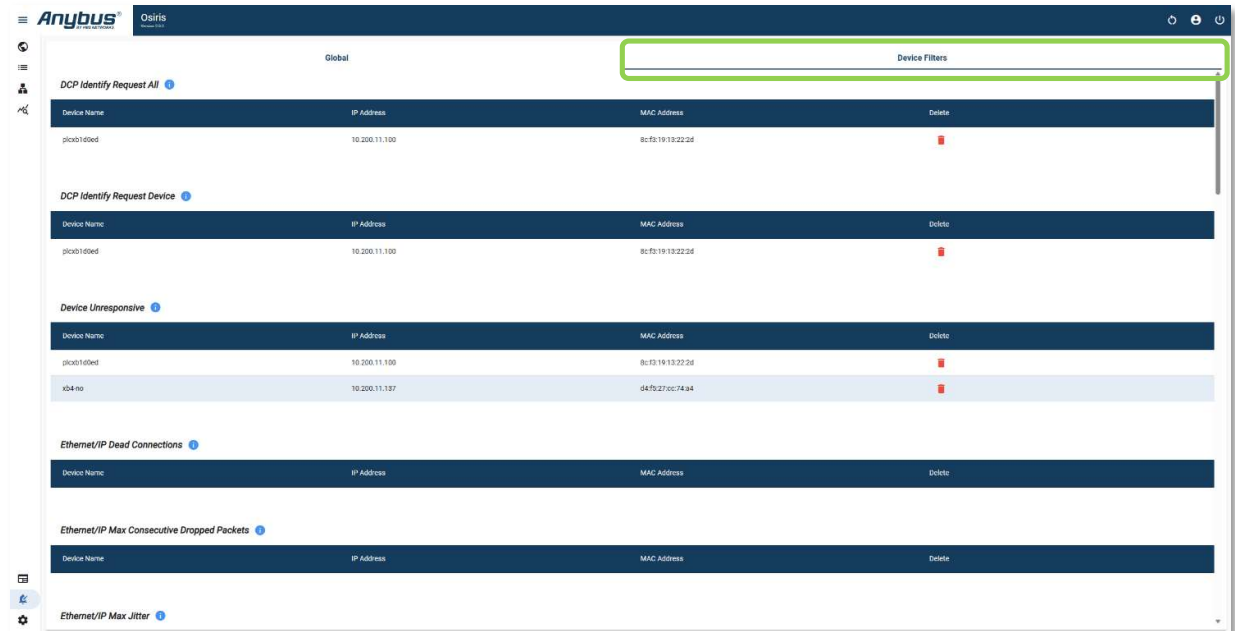
Siemens SFP Temperature: The temperature of the SFP in the Siemens switch.

Siemens SFP TX Power: The Transmit power of the SFP in the Siemens switch.

Siemens SFP Voltage: The Voltage of the SFP in the Siemens switch.

3.6.2 Device filters

Each item in the paragraph above can be filtered out individually. Device filters that have been set by the 'mute notification' feature (see 3.2.1) can be administered here. For each filter type there is a separate header, and a device is listed here if a filter rule has been assigned to it.



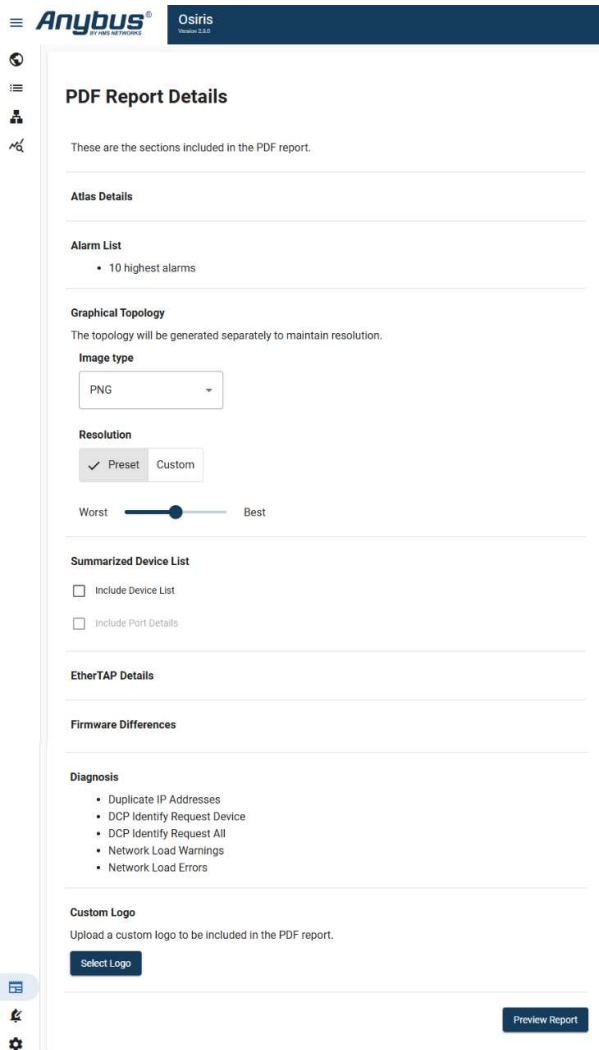
The screenshot shows the 'Anybus' web interface with the 'Device Filters' tab selected. The interface displays a list of filters with columns for 'Device Name', 'IP Address', 'MAC Address', and 'Delete'. The filters are categorized by type: 'DCP Identify Request All', 'DCP Identify Request Device', 'Device Unresponsive', 'Ethernet/IP Dead Connections', 'Ethernet/IP Max Consecutive Dropped Packets', and 'Ethernet/IP Max Jitter'. A green box highlights the 'Device Filters' tab at the top.

You can delete a filter by clicking the red Trash Can icon.

Please note that these filters are the same as the filters in the Device Details view in the Topology. Clearing them here will also clear them in the Device Details Alarm list.

3.7 Reporting

The Reporting feature makes it easy to export all measured items to a PDF. The Report is configurable:



The screenshot shows the 'PDF Report Details' configuration page in the Anybus Osiris interface. The page is titled 'PDF Report Details' and lists the sections included in the PDF report. The sections are: Atlas Details, Alarm List (10 highest alarms), Graphical Topology (The topology will be generated separately to maintain resolution.), Image type (PNG), Resolution (Preset, Custom), Summarized Device List (Include Device List, Include Port Details), EtherTAP Details, Firmware Differences, and Diagnosis (Duplicate IP Addresses, DCP Identify Request Device, DCP Identify Request All, Network Load Warnings, Network Load Errors). There is a 'Custom Logo' section with a 'Select Logo' button. A 'Preview Report' button is located at the bottom right.

A custom logo can be added to the report by selecting an image. Most common image formats are supported.

When you are done customizing the report, click on 'Preview Report'. A pop-up shows the preview and a 'Generate PDF Report' button. Click it to download the PDF and Topology image to your local hard drive; these will be available in the default download folder of your browser.

Please note that the Topology is not included in the report, but is generated separately. It is downloaded as a separate file by the browser. If the second file is blocked by your browser, please try Chrome or Firefox.

4 Settings

Use the Settings Menu at the bottom left of the screen to access several settings.

Date and time

Set/change the date and time of the Atlas2 Plus.

Upgrade

Upload a newer firmware package and perform a firmware update. It is also possible to downgrade to a lower version 2.x. It is not possible to downgrade to 1.x versions. See 4.7 for more information.

License Manager

Check current license details, check for updates and perform an online and/or offline license update.

Users

Open the User Management Administrator Console to add, edit or remove users and credentials. See 4.1 for more information.

User Management

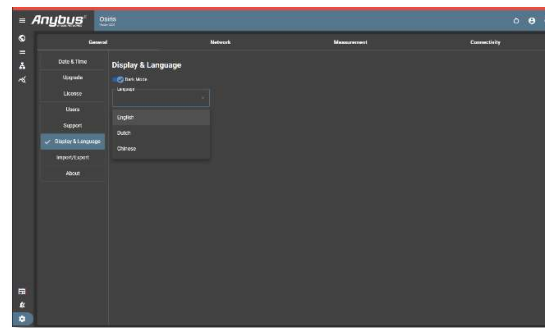
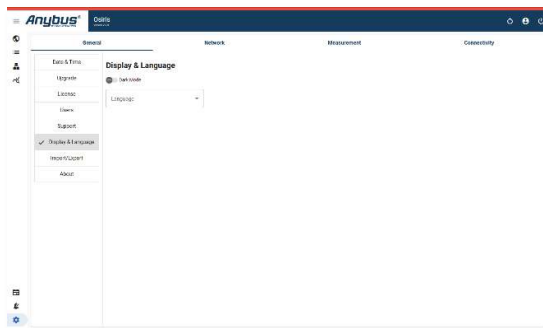
Administrator Console

Support

Generate a Diagnostic Dump file. This can be used by our R&D engineers for device diagnostics or scan information.

Display & Language

Switch between light mode and dark mode of the user interface and choose a language. More languages will be added in later firmware versions.



Import/Export

Save the settings of the Atlas2 Plus by clicking the 'Download' button. It will prompt you to enter a password, because the information is stored in an encrypted ZIP file. This file can later be imported. This restores all settings. After importing the settings, the Atlas2 Plus will reboot to load all the settings.

About

Displays the current firmware revision and serial number of the device. You can also assign a name to the Atlas2 Plus.

It also has a Rollback feature to revert to the previously installed firmware package. After clicking on the Rollback button, you will have to confirm the Rollback procedure before continuing as the rollback procedure is irreversible.

Rollback

This action will rollback the current version of Osiris to the previous one.

This operation is irreversible.

Please insert the word "rollback" in the field below to confirm the operation.

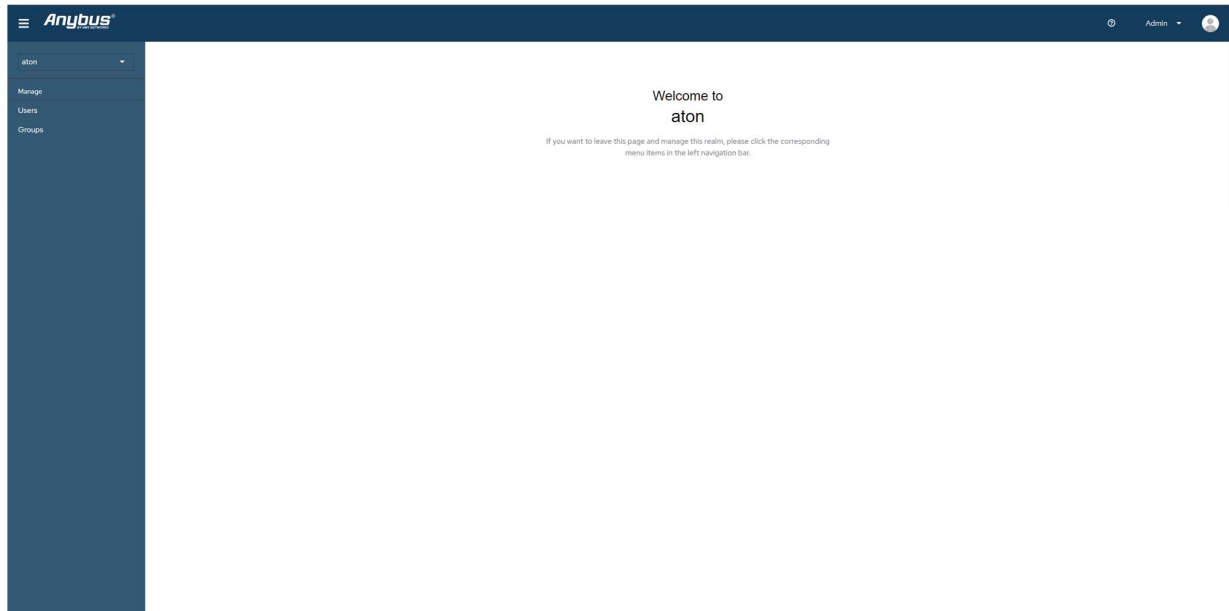
Type "rollback" to confirm*

Cancel

Confirm

4.1 General: User Management

The User Management Administrator Console allows you to add, edit or remove users and respective roles. It is opened in a new tab in the browser:



Via this menu you will be able to manage, add and customize different user accounts.

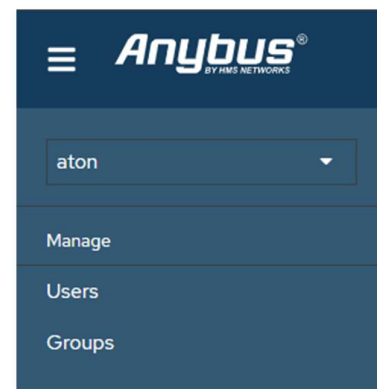
The menu on the left-hand side shows three different options:

Dropdown Menu

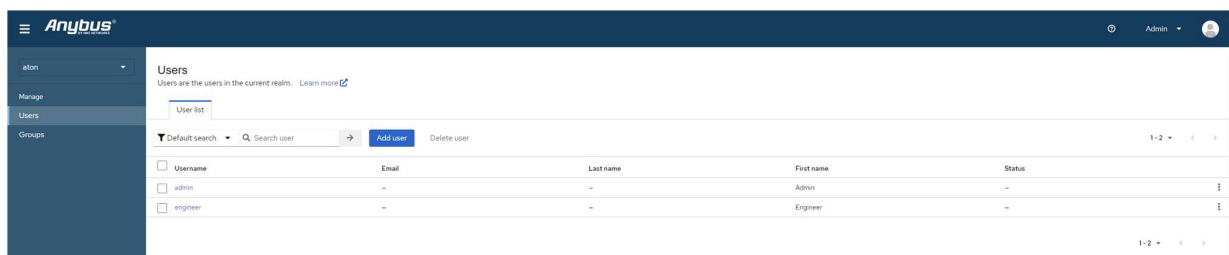
This dropdown menu shall not be used and should always be set to "Aton".

Users

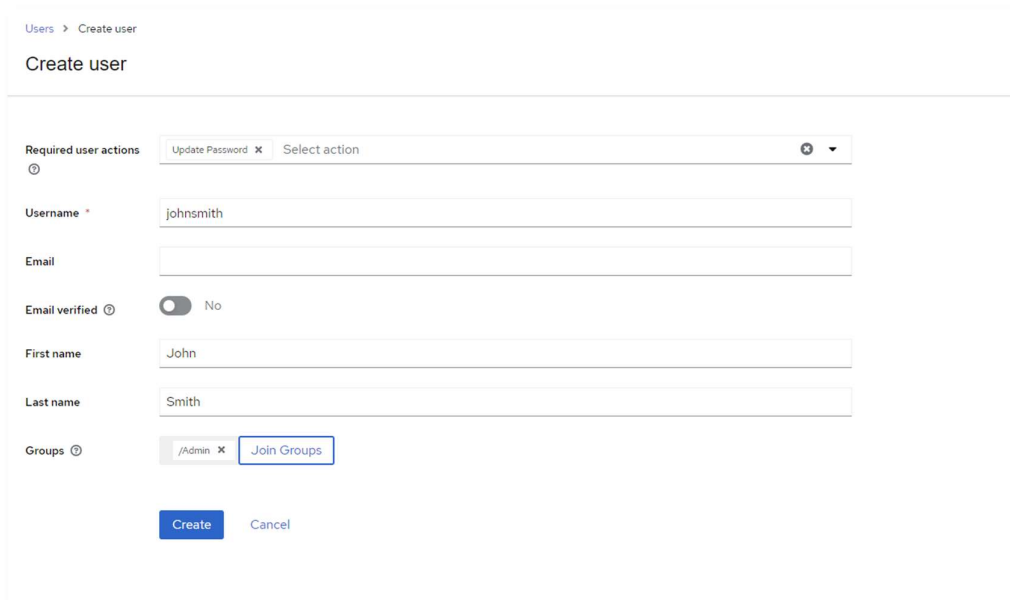
This menu allows you to add, modify or remove user accounts for the Atlas2 Plus web interface.



By default, the Atlas2 Plus has two different user accounts: Admin and Engineer. Through the Users menu new user accounts can be easily added:



Click on Add user. This will bring you to a different view.

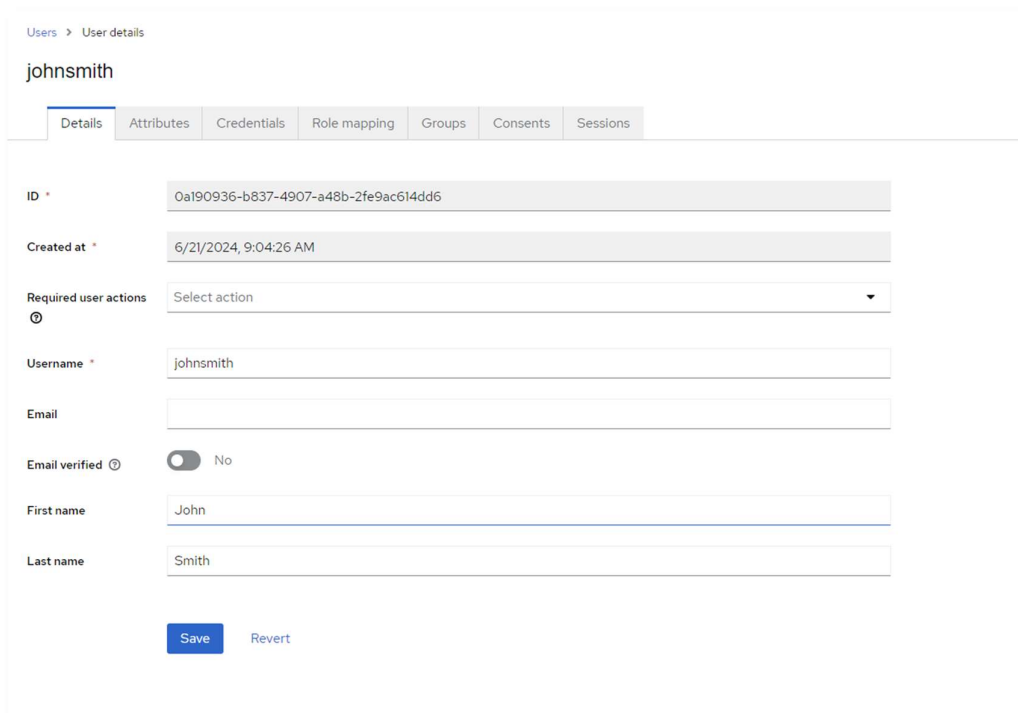


The screenshot shows the 'Create user' form. At the top, there is a breadcrumb 'Users > Create user' and a title 'Create user'. Below this, there is a 'Required user actions' section with a dropdown menu showing 'Update Password' and a 'Select action' button. The form fields include: 'Username' (johnsmith), 'Email' (empty), 'Email verified' (toggle set to 'No'), 'First name' (John), 'Last name' (Smith), and 'Groups' (a dropdown showing '/Admin' and a 'Join Groups' button). At the bottom, there are 'Create' and 'Cancel' buttons.

Here the new user account can be set up.

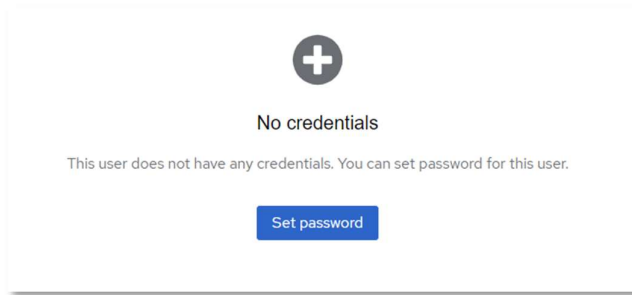
Under the “Join Groups” button you can select whether the new account should be configured as an Admin role (full access) or as an engineer role (read only).

Click on Create, followed by clicking on the “Credentials” tab at the top of the screen.



The screenshot shows the 'User details' page for 'johnsmith'. At the top, there is a breadcrumb 'Users > User details' and a title 'johnsmith'. Below this, there is a tabbed interface with tabs: 'Details', 'Attributes', 'Credentials', 'Role mapping', 'Groups', 'Consents', and 'Sessions'. The 'Details' tab is active. The form fields include: 'ID' (0a190936-b837-4907-a48b-2fe9ac614dd6), 'Created at' (6/21/2024, 9:04:26 AM), 'Required user actions' (dropdown showing 'Select action'), 'Username' (johnsmith), 'Email' (empty), 'Email verified' (toggle set to 'No'), 'First name' (John), and 'Last name' (Smith). At the bottom, there are 'Save' and 'Revert' buttons.

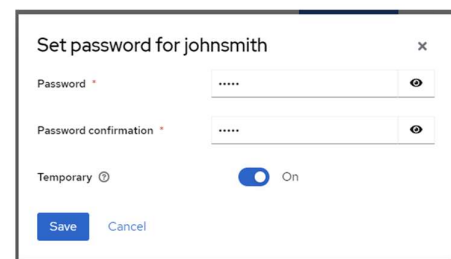
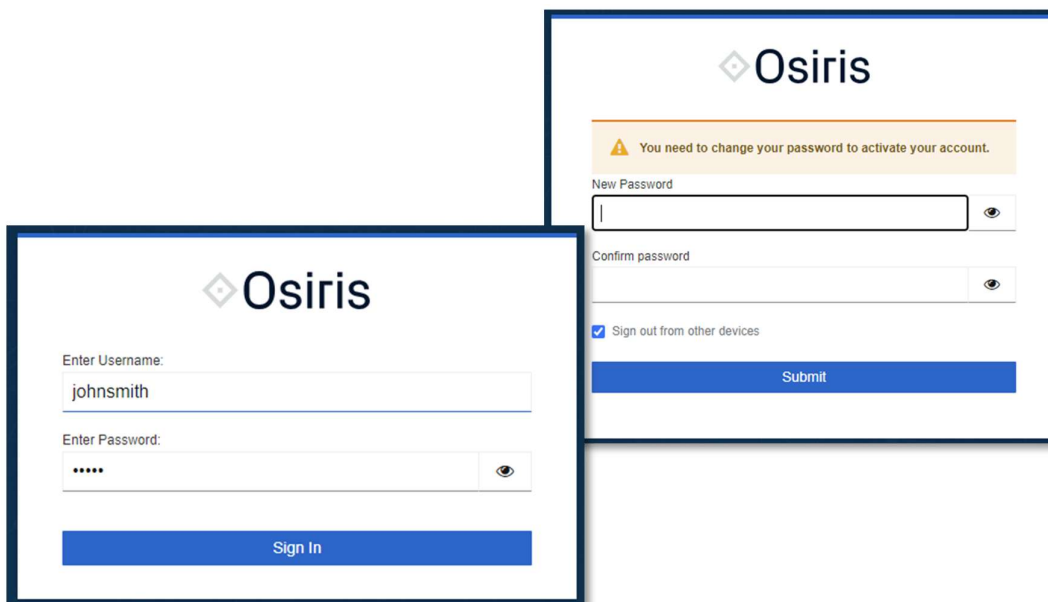
The Credentials tab is where you will have to configure the password for the new user account.



You can configure any password without restrictions.

By enabling the “Temporary” checkbox, the new user will be prompted to change the password after first log in. After saving the password the account is ready for use.

The new user can now log in with the newly created user account, and because the password was set to Temporary, the new user will be forced to change the password after first log in.

Groups

By default, Atlas2 Plus comes with two different user groups: Admin and Engineer. Accounts which are assigned to the Admin group will have full read & write access to the Atlas2 Plus measurement data and settings. The Engineer group will only have read access and will not be able to change any settings of the Atlas2 Plus. If required more user groups can be added with customizable names and privileges.



4.2 Network: Factory and Office interface

The Factory interface is used for connection to the network that needs to be scanned and analyzed. It is different from the Office interface and has its own set of IP settings. The Factory and Office IP range may not overlap.

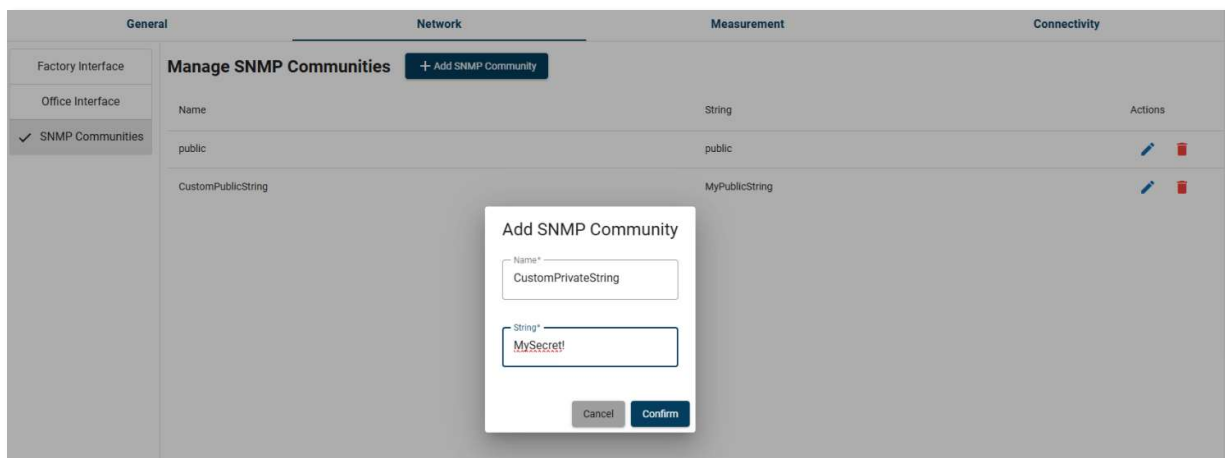
The Gateway and DNS settings are used only if you need to connect to another network or Internet. It is recommended to leave the Gateway and DNS of the Factory interface empty and only use the Office gateway for these purposes.

The Factory interface has a 'Disable HTTP Access' button, to disable webserver access on that port. If this is on, you can only connect to the webserver of the Atlas2 Plus through the Office port.

4.3 Network: SNMP Communities

The default community strings used by the Atlas are 'public' and 'private'. This may not be the right setting for your equipment. You can add custom community strings so that SNMP data can be retrieved correctly.

Simply add a string for either private or public strings:



4.4 Measurement: Scan range and Blacklist

This is an essential setting for the Atlas2 Plus. It determines the IP range for the active scanning. If this is set incorrectly, the Atlas will not work as expected.

The wizard (see chapter 2) will guide you through this, and you can also add or remove ranges here.

The scan range needs to fall within the range of the Atlas2 Plus subnet mask; it cannot scan outside of its own reachable range.

Scan Ranges + Add Scan Range

Name	From	To	Last Update	Actions
Machine ABC	192.168.4.1	192.168.4.20	Dec 12, 2025	 
Machine DEF	192.168.4.40	192.168.4.60	Dec 12, 2025	 
Machine GHI	192.168.4.100	192.168.4.150	Dec 12, 2025	 

The Blacklisted IP feature allows you to skip certain IP addresses; these will not be included in the scan or report.

Blacklisted IP + Add Blacklisted IP

Osiris will ignore these IP

192.168.4.15 

192.168.4.16 

4.5 Connectivity: MQTT

Atlas supports the MQTT connectivity protocol, a low-bandwidth and low-resource IoT-protocol. It sends the following data from Atlas to an MQTT broker:

- Device list
- Topology
- EtherTAP data
- Notifications / alarms
- Atlas details
- Network status

All data in the above topics are sent as .json data.

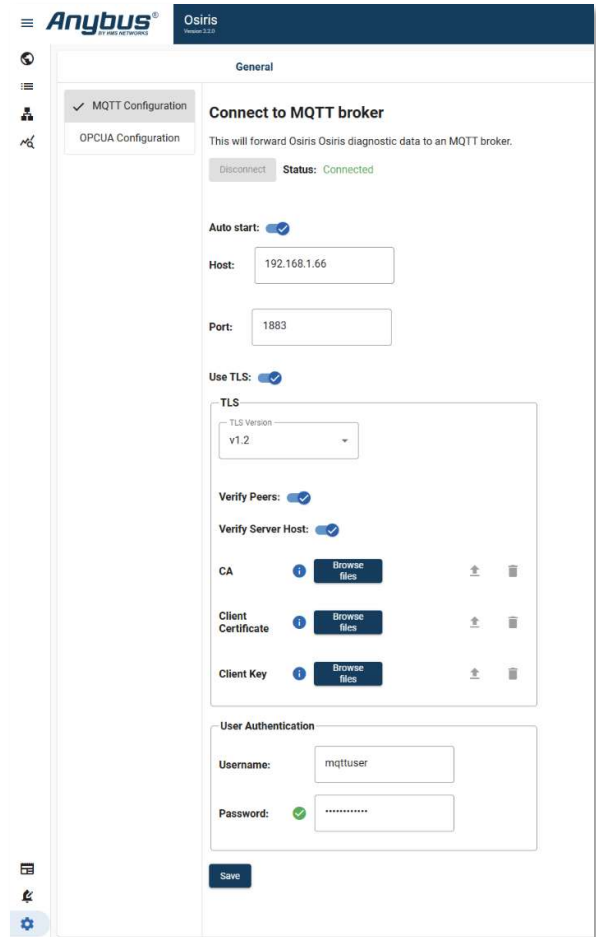
The default port to connect to is 1883.

The following settings can be configured:

Host: Server address of the Broker to connect to

Port: Port of the Broker to connect to

TLS: TLS (Transport Layer Security) aims to primarily provide privacy and data integrity between two or more communicating computer applications.



The screenshot shows the 'MQTT Configuration' tab in the Anybus Osiris interface. The 'Connect to MQTT broker' section is active, showing a 'Status: Connected' indicator. The configuration includes fields for 'Host' (192.168.1.66), 'Port' (1883), and 'Use TLS' (checked). Below this, there are sections for 'TLS' (version v1.2), 'Verify Peers' (checked), 'Verify Server Host' (checked), and 'User Authentication' (Username: mqttuser, Password: masked). There are also 'Browse files' buttons for CA, Client Certificate, and Client Key. A 'Save' button is at the bottom.

TLS Verify peer: Sets whether it should carry out post-connect checks, including that a certificate matches the given host name.

TLS Verify server: Enables or disables verification of the server certificate

TLS CA: Sets the file containing the public digital certificates trusted by the client. The file in PEM format containing the public digital certificates trusted by the client.

TLS Client Cert: Sets the file containing the public certificate chain of the client. The file in PEM format containing the public certificate chain of the client. It may also include the client's private key.

TLS Client Cert Key: Sets the file containing the client's private key. This is the file in PEM format containing the client's private key.

The following MQTT topics are available for subscription:

Topic	Description
anybus/osiris/export/network-status	Network Status
anybus/osiris/export/devices	Device List
anybus/osiris/export/device-ports	Device Ports
anybus/osiris/export/messages	Alarm messages / notifications
anybus/osiris/export/topology	Topology
anybus/osiris/export/tap-data	EtherTAP data
anybus/osiris/export/tap-devices	EtherTAP devices
anybus/osiris/export/tap-statistics	EtherTAP statistics

4.6 Connectivity: OPC UA

OPC UA is part of the foundation of Industry 4.0 and it allows for easy integration with SCADA systems.

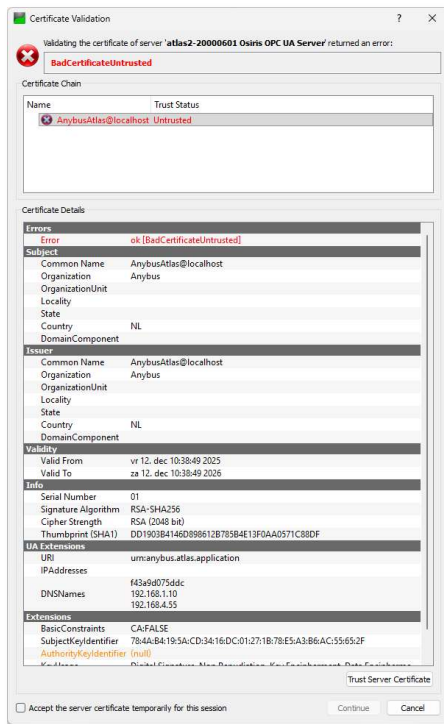
The OPC UA server functionality in Atlas is switched off by default.

On the OPC UA page you will see the address (Office IP range) 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. An OPC UA client needs to connect to the Office side.

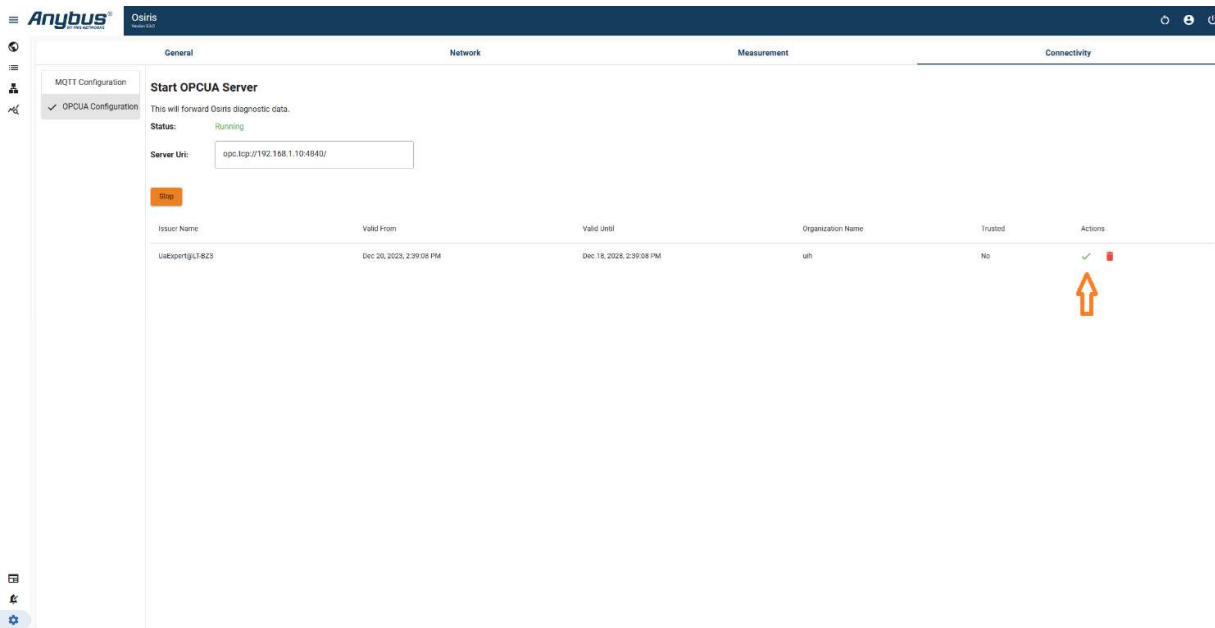


Please note that the default state of the server is 'stopped'. You need to start the server every time you reboot the Atlas.

When the server is running, you can connect an OPC-UA client to the IP address. The client will ask you to accept the certificate:



In the OPC-UA settings of the Atlas, you also need to accept the certificate. Press the green checkbox mark:



Next, you can initialize the OPC-UA connection.

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

- Atlas details
- Device list
- Messages/Notifications
- Topology
- EtherTAP data
- Network status

All items can be retrieved as individual tags or combined as Extension Objects (in JSON format).

An overview of all available OPC UA tags is available on the next page.

Description	Tag
Atlas Details:	AtlasDetails: ns=2;s=AtlasDetails MeasurementFolder: ns=2;s=MeasurementFolderId
Network Status:	NetworkStatus: ns=2;s=MeasurementNetworkStatus
Device List:	<i>Remark: {} should be replaced by the mac address of the device</i> DeviceListFolder: ns=2;s=DeviceListFolderId DeviceListFolder.DeviceFolder: ns=2;s=DeviceListFolderId_{} DeviceListFolder.DeviceFolder.DeviceDetails: ns=2;s=Device_{} DeviceListFolder.DeviceFolder.Ports: ns=2;s=Device_{}_Ports
Notifications / Alarms:	<i>Remark: {} should be replaced by the message ID (number starting from 0)</i> MessagesFolder: ns=2;s=MessagesFolderId MessagesFolder.Message: ns=2;s=UaAlarmMessage_{} ns=2;s=UaAlarmMessage_10
EtherTAP Data:	<i>Remark: {} should be replaced by the MAC address of the EtherTAP</i> TapFolder: ns=2;s=TapFolderId TapFolder.TapDeviceFolder: ns=2;s=Tap_{} TapFolder.TapDeviceFolder.TapData: ns=2;s=TapData_{} TapFolder.TapDeviceFolder.TapDetails: ns=2;s=TapDevice_{} TapFolder.TapDeviceFolder.TapStats: ns=2;s=TapStatistics_{}
Topology:	TopologyFolder: ns=2;s=TopologyFolderId TopologyFolder.Links: ns=2;s=TopologyLink TopologyFolder.Nodes: ns=2;s=TopologyNode

4.7 Firmware Updates

The application running on the Atlas2 Plus will be regularly updated. 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.

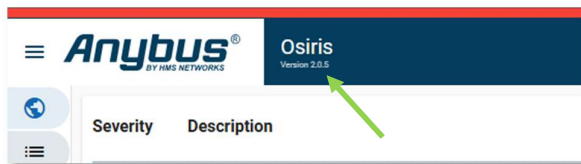
Whenever an update becomes available it will be announced on the website of HMS Networks. HMS Networks will provide details regarding the update and indicate whether the update is regarded as being a critical update.

Before reporting a bug, make sure to update your Atlas2 Plus to the latest version and check if the problem persists.

Admins 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.

4.7.1 How to find the current firmware version

To find the current version of the Atlas' firmware, check the top bar of the dashboard:



Next to the Anybus® logo you will find 'Osiris' and the firmware version which is currently installed on your Atlas2 Plus.

4.7.2 Firmware Update License

To be able to install firmware updates, the Atlas2 Plus needs an additional Firmware Update License for either three (3) years or for (product) lifetime (15 years).

The validation of the Firmware Update License can be verified under the 'General' tab of the settings menu.

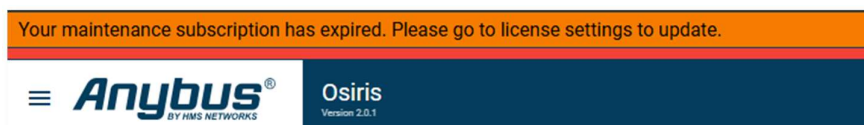
License Manager

License Number: 130-
Update Expiration: November 8, 2039

- ✓ advancedDiagnostics
- ✓ tapEthernetIp
- ✓ tapProfinet

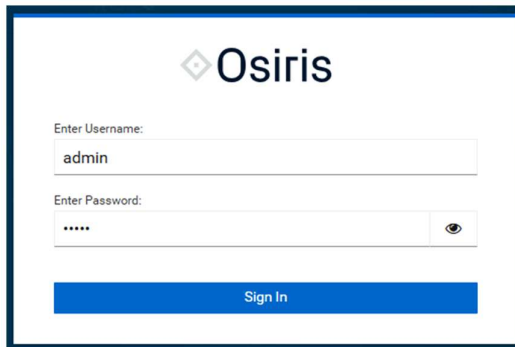
You will be notified about the upcoming expiration date one month prior to the actual expiration date through a notification on the dashboard.

Once the Firmware Update License has expired, you will be notified through the dashboard again:

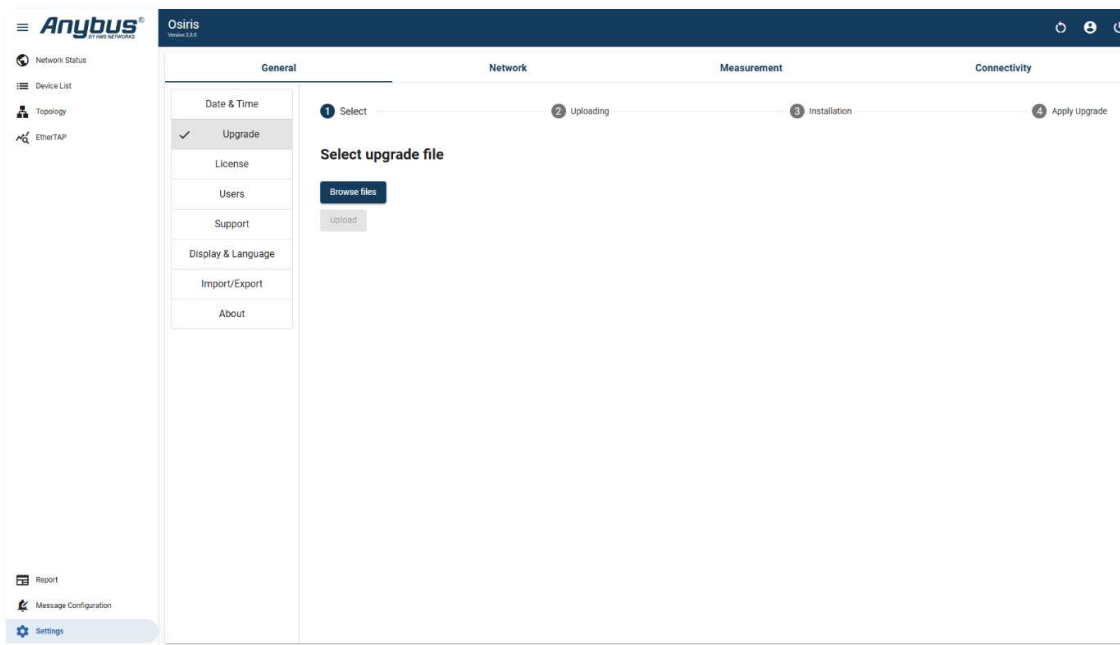


4.7.3 Update via the web interface

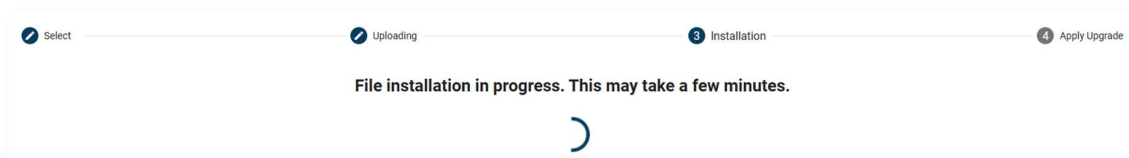
1. Log in as Admin or with an account which is assigned with an Admin role.



2. Go to Settings > Upgrade



3. Select the update file [.upd]
4. Press 'Upload'.
5. Wait until the file is uploaded.
This usually takes a few minutes.



6. Apply the upgrade by restarting the device when prompted. This will take another 5 to 10 minutes.
7. The firmware update is now successfully installed, and the device will reboot. Wait until the services are restarted.

4.7.4 Update via USB

The Atlas2 Plus can also receive an update via USB. The procedure is as follows:

1. Download the latest firmware for Atlas from the HMS website
www.hms-networks.com
2. Copy the new firmware file with the extension .upd to the root of a USB drive and insert the drive into one of the two available USB ports of the Atlas2 Plus.
3. Power down the device and power it up again to start the update.
4. The LED inside the unit will turn blue and the screen will indicate the update being installed.
5. When the update is completed, the internal LED will turn green (success) or red (failure). In case of failure, the old firmware version will remain on the system.
6. Remove the USB drive. When the drive is removed, the operating system will restart.

4.7.5 Updating from the old User Interface

For users who are updating their Atlas2 Plus from a firmware version with the old user interface (firmware V1.1.xxx): please follow the USB update procedure as described in 4.4.4.