

Network Management Software

Manual for u-netops

Version 1.1, October 2026

Software version 1.0.4

Weidmüller 

Network Management Software Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Copyright ©2026 Weidmüller Interface GmbH & Co. KG

All rights reserved.

Reproduction without permission is prohibited.

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Weidmüller.

Weidmüller provides this document “as is”, without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Weidmüller reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Weidmüller assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Contact Information

Weidmüller Interface GmbH & Co. KG

Postfach 3030

32760 Detmold

Klingenbergstraße 26

32758 Detmold

Germany

Phone +49 (0) 5231 14-0

Fax +49 (0) 5231 14-2083

E-Mail info@weidmueller.com

Internet www.weidmueller.com

Table of Contents

1. About u-netops	3
1.1 Functional overview	3
1.2 Conventions used in this manual	3
2. Getting Started.....	4
2.1 Requirements.....	4
2.2 Installation and uninstallation	4
2.3 Starting u-netops	4
2.4 Registration and login	5
3. User Interface	7
3.1 Header bar, main menu and list views.....	7
4. Topology View	8
4.1 Opening or creating a project.....	8
4.2 Creating a new project	8
4.3 Discovering devices	9
4.4 Topology preview	10
4.5 Topology view	11
4.6 Device tree and group tree	11
4.7 Device context menu.....	13
4.8 Edit mode	14
4.9 Notifications and disconnection events.....	15
4.10 System log in the topology view.....	16
5. Traffic Monitor	17
5.1 Real-time traffic	17
5.2 History	18
5.3 Traffic alarms (Setting).....	18
6. Host Monitor	20
6.1 “Monitor” view.....	20
6.2 Adding addresses	20
6.3 Test configuration.....	21
6.4 Running a test	22
6.5 “Message” view	22
7. Commander	23
7.1 Setting the transfer parameters	24
7.2 Running an action	25
7.3 Firmware upgrade	26
7.4 Config backup	27
7.5 Config restore.....	27
7.6 Reboot.....	27
8. MIB Browser	28

8.1 Querying an object	28
8.2 SNMP parameters	28
8.3 MIB files and result table	29
9. Backup Policy	30
9.1 Setting up the TFTP server	30
9.2 Auto Backup	31
9.3 Auto Compare	31
10. Logs	33
10.1 System Log	33
10.2 Event types and e-mail alerts	33
10.3 Syslog	34
11. Setting	35
11.1 About	35
11.2 System Config	35
11.3 Topology Config	36
12. User Menu	38
12.1 Account	38
12.2 License	39
12.3 Model	50
12.4 NTP Client	51
12.5 SMTP Setup	51
12.6 Export File and Import File	52
12.7 Logout	53
13. Typical Workflows	54
13.1 Initial setup	54
13.2 Adding a new switch to an existing project	54
13.3 Updating the firmware on several switches	54
13.4 Narrowing down the cause of a fault	54
14. Troubleshooting	55
Appendix A – System Log Event Types	56
Appendix B – Glossary	57
List of Figures	58
List of Tables	60

1. About u-netops

Weidmüller u-netops is a network management system (NMS) that graphically represents a network of Ethernet switches belonging to the Advanced & Substation Lines. It also allows all switches of the network to be monitored and configured from one central, web-based user interface.

u-netops uses SNMP for device detection and LLDP for link detection. Any third-party device that supports these protocols can therefore also be displayed in u-netops.

This manual is intended for administrators and network technicians who monitor devices, maintain network topologies, back up configurations and distribute firmware. It describes u-netops software version 1.0.4.

1.1 Functional overview

Module	Purpose
Topology View	Create projects, discover devices and display them as a network topology; live status polling of devices and links.
Traffic Monitor	Monitor and evaluate the traffic of the device ports, grouped by device type; real-time, history and traffic alarms.
Host Monitor	Check the availability of any IP device by means of test series (ICMP ping/polling).
Commander	Bulk actions on switches: reboot, firmware upgrade, configuration backup and restore.
MIB Browser	Query SNMP objects (Get, Walk, etc.) and load MIB files.
Backup Policy	Automatic configuration backup and configuration comparison via TFTP.
Logs	System log of the application and received syslog messages.
Setting	System-wide parameters: recording, polling/SNMP, topology display

Table 1: Functional overview

1.2 Conventions used in this manual

- Names of menus, buttons and fields are written as they appear in the user interface and are printed in bold, e.g. **Start Project** or **Apply settings**.
- Menu paths are shown with “→”, e.g. user menu → **Account**.
- Screenshots were taken in test environments. IP addresses, device names and – depending on the software version – some details of the screens in your installation may differ.



CAUTION: Some actions (**Reboot, Firmware Upgrade, Config Restore, Clear Log, Remove Device**) take effect on the devices immediately or delete data. Only carry out these actions within maintenance windows and after consultation with the persons responsible.

2. Getting Started

2.1 Requirements

2.1.1 System requirements

- Intel Core i5 or higher
- Monitor resolution: at least 1920 × 1080 recommended
- 4 GB RAM or higher
- 1 GB hard disk space or higher
- Windows 11 (64 bit)
- Microsoft Edge or Google Chrome (current version)
- Network access to the managed devices (SNMP UDP 161, traps UDP 162, TFTP UDP 69, syslog UDP 514)

2.1.2 Supported devices

Weidmüller u-netops supports the full range of functions – such as network status, traffic monitoring and configuration/firmware management – for Advanced and Substation Line switches.

For other SNMP-enabled devices, u-netops supports standard management functions such as link up and link down, provided that these SNMP devices also support the LLDP protocol.

u-netops can also check the availability of any device supporting ICMP (**Host Monitor**), but only for inventory purposes (device online or offline).

2.2 Installation and uninstallation

To install Weidmüller u-netops:

1. Install the **CodeMeter Runtime** included in the installation ZIP package. CodeMeter is required for license activation; without it, u-netops cannot be licensed (see section 12.2).
2. Execute the installation program.
3. During the installation, choose the directory in which u-netops will be installed or keep the default value. You can also choose whether a desktop shortcut for launching u-netops is created.
4. When the installation is complete, an information message is shown. Click **Finish** to exit the setup wizard.

After the installation, activate a license (user menu → **License**, section 12.2). [TBD: Is u-netops usable without a license, e.g. in a demo mode or with a limited number of devices?]

To uninstall Weidmüller u-netops:

1. Open the **Control Panel**.
2. Under **Programs**, click **Uninstall a program**. The screen “Uninstall or change a program” appears.
3. Select **u-netops**.
4. Click **Uninstall** (or **Uninstall/Change**) at the top of the program list.

2.3 Starting u-netops

1. Double-click the u-netops desktop shortcut. If you did not create it during the installation, click **Start** and open the u-netops program.

- The u-netops server window appears. While the server is starting, the **COPY** button is disabled. As soon as the button is enabled (after approximately half a minute), click it.

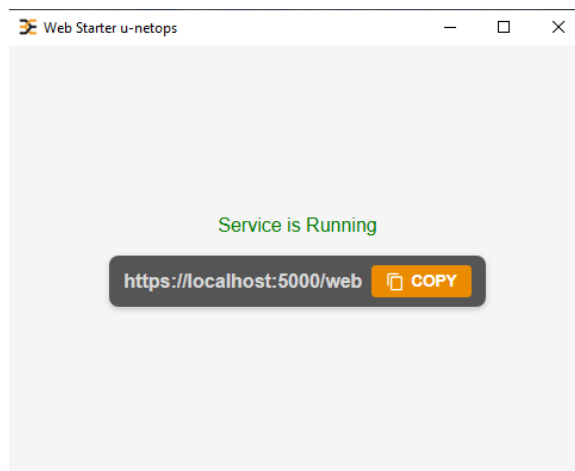


Figure 1: u-netops server window (Web Starter)

- Paste the copied address (`https://localhost:5000/web`) into the web browser. The browser warns that the connection is not private. This is because the certificate used is self-signed and not recognised by the browser; the HTTPS encryption nevertheless works and the data is protected. Click **Advanced** and then **Proceed to localhost (unsafe)**.
- The web login page is displayed.

From other computers in the network, u-netops is accessed via the address of the server, e.g. `https://<server IP>:5000/web/`.

2.4 Registration and login

When u-netops is accessed for the first time, the Administrator account must be created. The system wizard guides you through this process.



NOTE: For security reasons, the User IDs “admin” and “root” are not allowed. The password must contain at least one uppercase letter [A-Z], one lowercase letter [a-z], one number [0-9] and one special character [@\$!%#*^()/?+=&_]. The User ID of the Administrator account cannot be changed later.

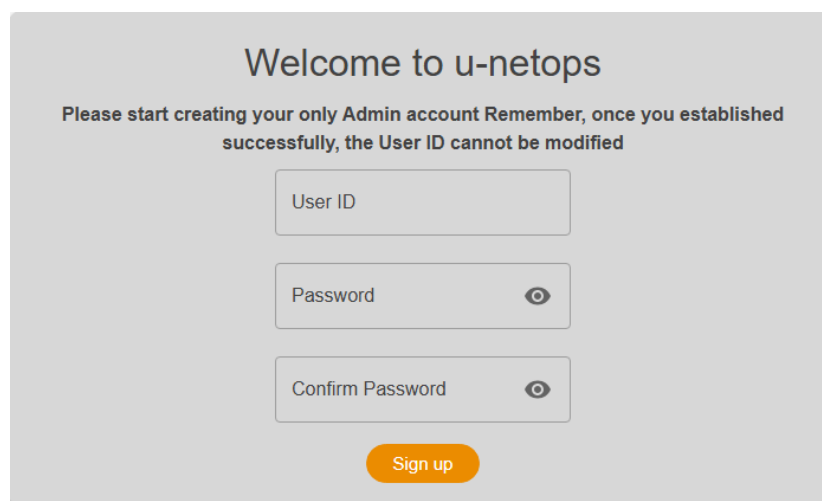


Figure 2: Creating the Administrator account

After the Administrator account has been created successfully, use these credentials to log in to u-netops. After login, the start page **Topology View** is shown. Every login and every failed login attempt is recorded in the system log (see chapter 10. Logs).

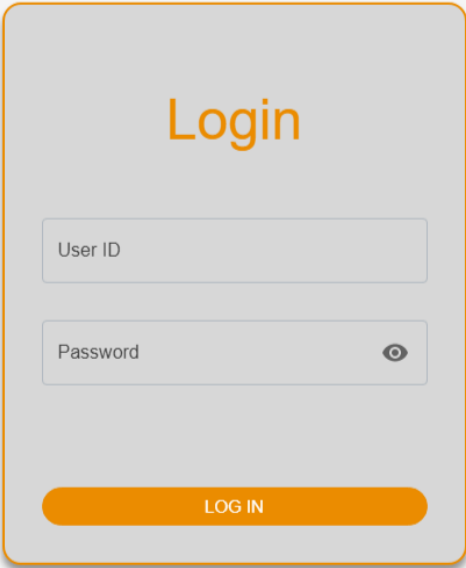
The image shows a login page with a light gray background and rounded corners. At the top, the word "Login" is displayed in a large, orange, sans-serif font. Below it, there are two input fields: the first is labeled "User ID" and the second is labeled "Password". The "Password" field includes a small eye icon on its right side to toggle visibility. At the bottom of the form, there is a prominent orange button with the text "LOG IN" in white, uppercase letters.

Figure 3: Login page

3. User Interface

3.1 Header bar, main menu and list views

The orange header bar contains the main menu with all modules: **Topology View**, **Traffic Monitor**, **Host Monitor**, **Commander**, **MIB Browser**, **Backup Policy**, **Logs** and **Setting**. On the right-hand side there are two icons:

- **Bell** – opens the **Notifications** sidebar with the current notifications. **Clear All** removes all notifications.
- **Person icon** – opens the user menu with **Account**, **License**, **Model**, **NTP Client**, **SMTP Setup**, **Export File**, **Import File** and **Logout** (see chapter 12. User Menu).

Many list views follow the same pattern: a search field, a filter icon with a selection field (defines the column that is searched, e.g. **IP**, **Device** or **System Name**), a table with check boxes for multiple selection and page navigation at the bottom.

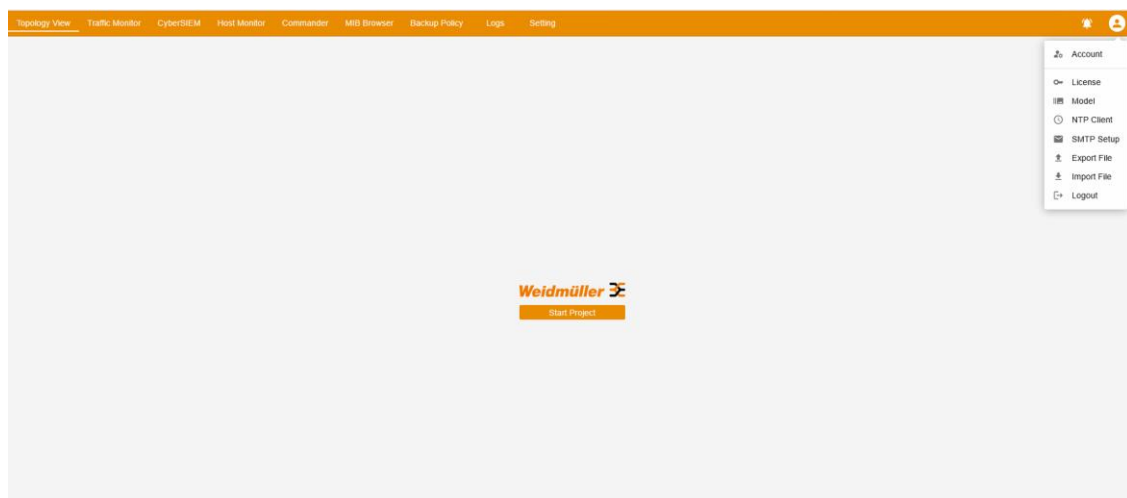


Figure 4: Header bar with main menu and opened user menu

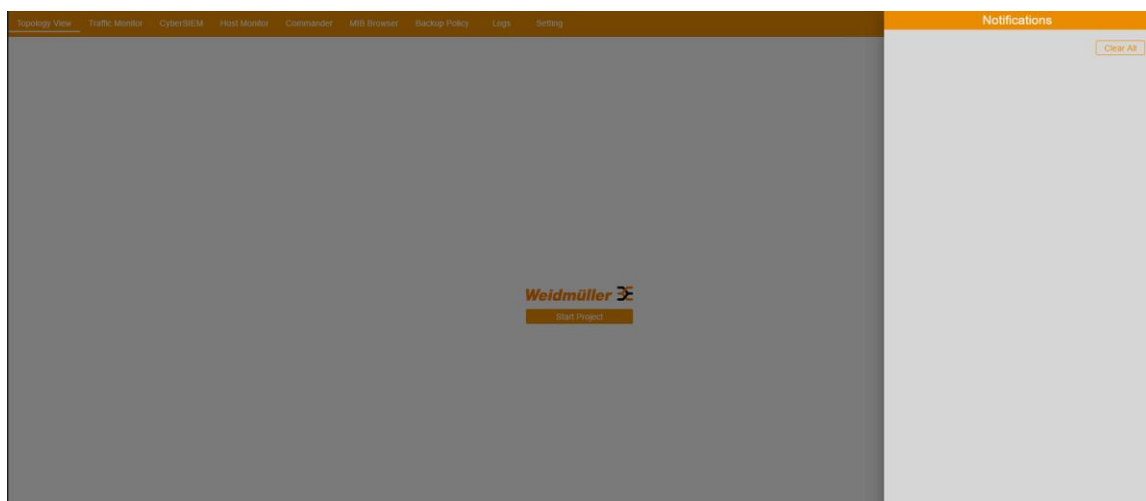


Figure 5: "Notifications" sidebar

4. Topology View

The Topology View is the starting point for working with u-netops. It finds the SNMP switches of a network, visualises the interconnections between them and notifies the user when a link goes down.

All devices are managed in **projects**. A project contains the discovered devices, their connections (edges) and the layout of the topology.

4.1 Opening or creating a project

If no project is open yet, the Topology View only shows the **Start Project** button. Clicking it opens the start dialog.

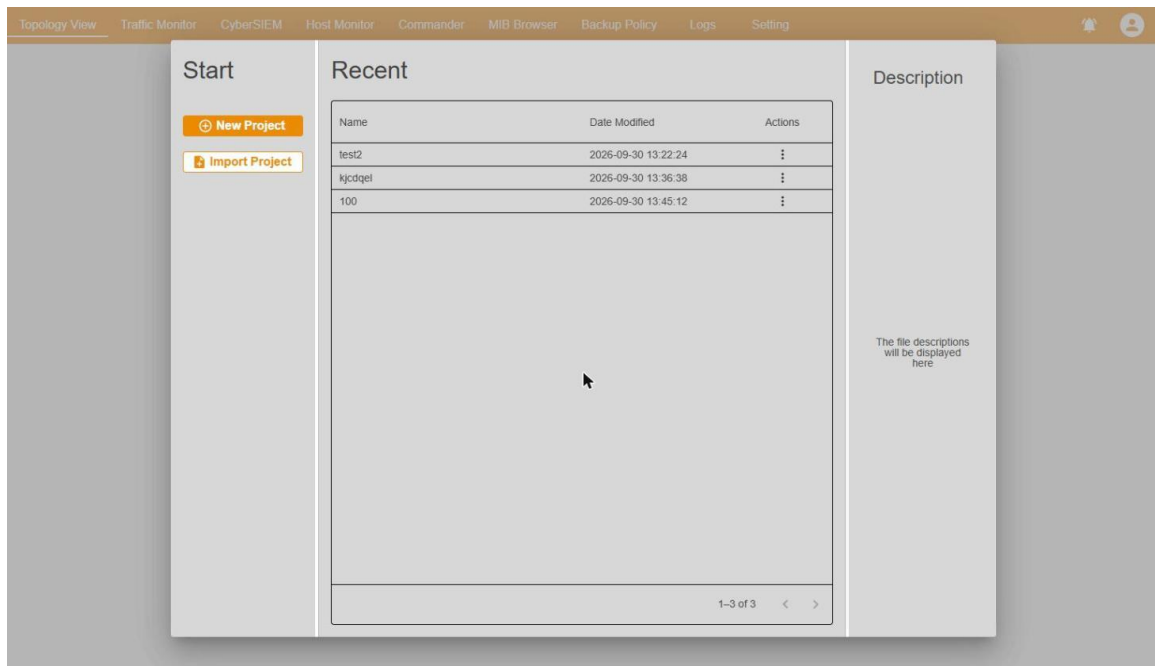


Figure 6: Start dialog with the recently used projects

Element	Function
New Project	Starts the wizard to create a new network topology by discovering devices.
Import Project	Loads an existing topology (project file, JSON) stored on the PC.
Recent	List of the existing projects with name and modification date. Clicking a project selects it; its description is shown on the right.
Open	Opens the selected project directly in the topology view.
Edit	Opens the selected project in the wizard to add devices to or remove devices from an existing network/topology.
⋮ (Actions)	Per project: Export (save the project file on the PC), Edit Info (change project name and description), Delete (delete the project).

Table 2: Opening or creating a project - Description

4.2 Creating a new project

1. In the start dialog, click **New Project**.
2. In the step **Project Settings**, enter a **Project Name** and optionally a description. Creation and modification date are set automatically. The **Next** button only becomes active once a name has been entered.

3. In the step **Device**, search for the devices (see section 4.3) and add them to the **Device List**. Continue with **Next**.
4. In the step **Topology Preview**, check the result and adjust it in **Edit** mode if necessary (see section 4.4).
5. Click **Finish** to complete the project. It is then opened as a tab in the Topology View.

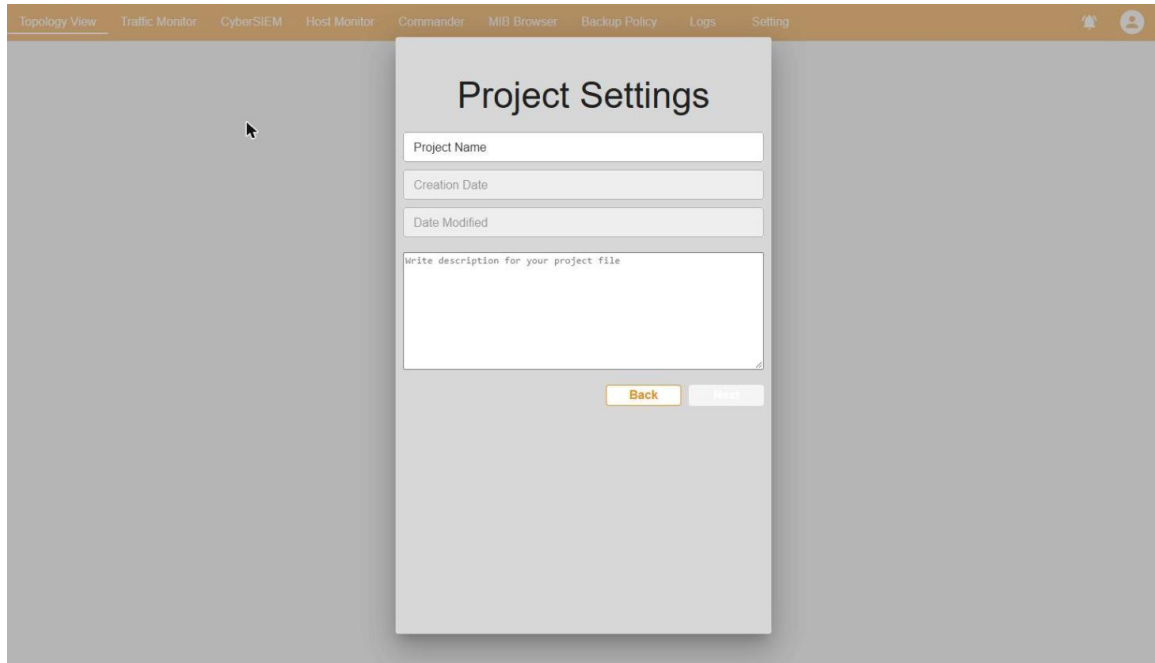


Figure 7: Wizard, step 1: Project Settings

4.3 Discovering devices

NOTE: To discover all Ethernet switches of a network properly:



- There must be IP connectivity between the PC running u-netops and the switches of the network.
- SNMP must be enabled on the switches to be discovered, and the SNMP configuration must match the one set in u-netops (**Setting** → **System Config**, see section 11.2 System Config).

NOTE: To display the existing connections between Ethernet switches properly:



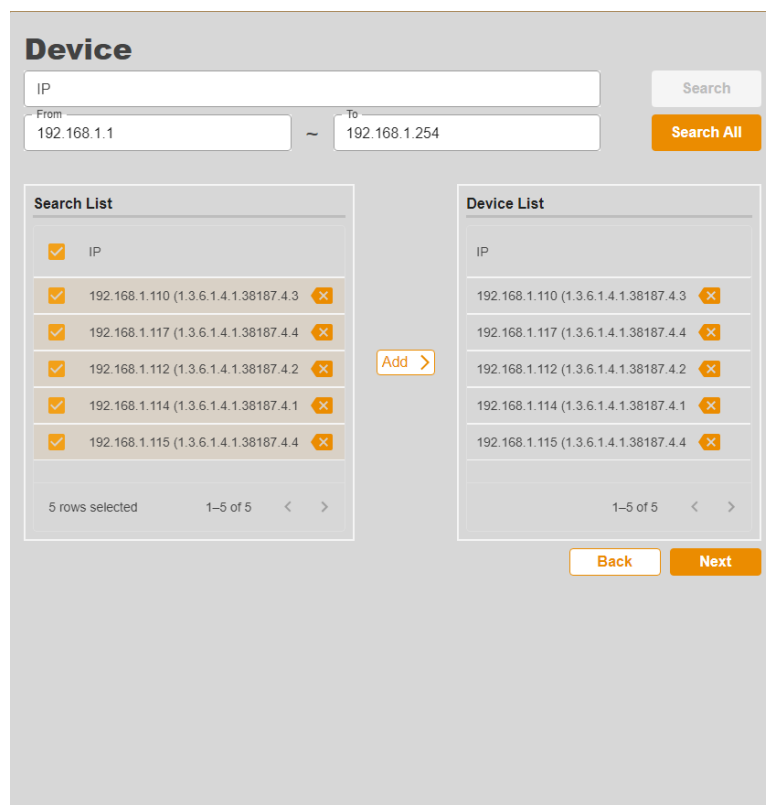
- LLDP must be enabled on all switches.
- PROFINET must be disabled on all switches that are PROFINET Conformance Class B devices.

Devices can be searched individually or via an address range:

- **Single address:** enter the IP address in the field **IP** and click **Search**.
- **Address range:** enter the start and end address in **From** and **To** and click **Search All**.
- The devices found appear in the **Search List**. Select the required entries with the check boxes (the check box **IP** selects all) and move them to the **Device List** with **Add >**.
- An entry in the Device List shows the IP address and the SNMP system OID (sysObjectID) of the device. The orange ✕ removes a device from the list again.



NOTE: Only one IP network can be entered in the IP range fields. If a router or Layer 3 switch connects devices in different IP networks, search the different IP ranges one after another to discover all devices.



Device

IP

From: 192.168.1.1 To: 192.168.1.254

Search

Search All

Search List

IP
192.168.1.110 (1.3.6.1.4.1.38187.4.3)
192.168.1.117 (1.3.6.1.4.1.38187.4.4)
192.168.1.112 (1.3.6.1.4.1.38187.4.2)
192.168.1.114 (1.3.6.1.4.1.38187.4.1)
192.168.1.115 (1.3.6.1.4.1.38187.4.4)

5 rows selected 1-5 of 5

Device List

IP
192.168.1.110 (1.3.6.1.4.1.38187.4.3)
192.168.1.117 (1.3.6.1.4.1.38187.4.4)
192.168.1.112 (1.3.6.1.4.1.38187.4.2)
192.168.1.114 (1.3.6.1.4.1.38187.4.1)
192.168.1.115 (1.3.6.1.4.1.38187.4.4)

1-5 of 5

Back Next

Figure 8: Wizard, step 2: searching and adding devices

4.4 Topology preview

When all devices to be included in the topology are in the **Device List**, click **Next** to open the **Topology Preview**.

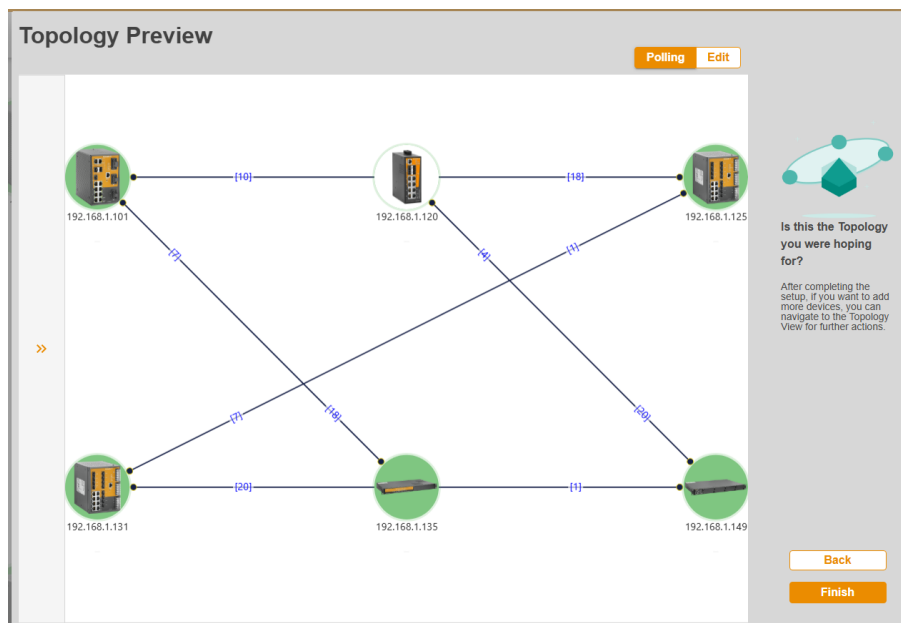


Figure 9: Wizard, step 3: Topology Preview

NOTE: Considerations about the Topology Preview:

- Advanced & Substation Line switches are displayed with their actual product images. All other (third party) devices get the same default icon, which can be changed later (user menu → **Model**, see section 12.3 Model).
- The devices and their connections are initially placed randomly. Click **Edit** and drag the devices to the desired positions. Once all devices are in their final position, click **Save File**.

When all devices are in the desired position and the topology has been saved (**Save File**), click **Finish** to go to the main topology view.

4.5 Topology view

Opened projects are shown as tabs below the header bar. **Add Project** opens a further project; the × on a tab closes the project (the project is not deleted).



Figure 10: Topology View in “Polling” mode

The topology view has two operating modes:

- **Polling** – mode for normal operation. The status of devices and links is continuously monitored by u-netops.
- **Edit** – mode for changing and updating the topology (see section 4.8 Edit mode).

Element	Function
Polling / Edit	Switches between monitoring mode (Polling) and editing mode (Edit).
Bell (in the view)	Opens the Disconnection Event sidebar with link disconnections; with search field (see section 4.9).
Clock icon	Opens the System Log as a sidebar (same content as Logs → System Log).
» (left edge)	Expands the sidebar with the device and group tree; < collapses it again.
Toolbar bottom right	Undo, redo, zoom in, zoom out and Fit (show the entire topology).

Table 3: Topology View in “Polling” mode

4.6 Device tree and group tree

The sidebar on the left offers two views:

- **Device Tree** – lists all devices and connections (edges) of the project with their number. Each device has a switch in front of it and a status dot behind it. Clicking a device or a connection highlights it in the topology.
- **Group Tree** – shows the devices in groups (default: **Main**).

- The pencil icon at the top right of the sidebar is used to edit the tree or the groups.

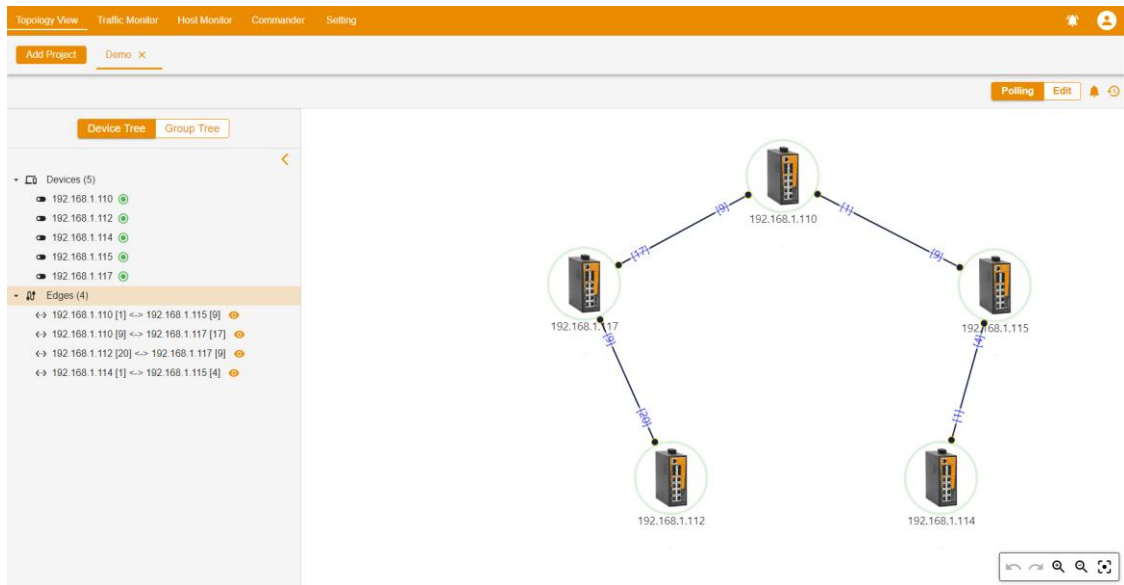


Figure 11: Sidebar with Device Tree

In the group view, the **Group Management** dialog is used to organise devices in groups. **Add Group** creates a new group (only the group name is required); the devices that belong to the group are then selected and moved to it with **Move to group**.

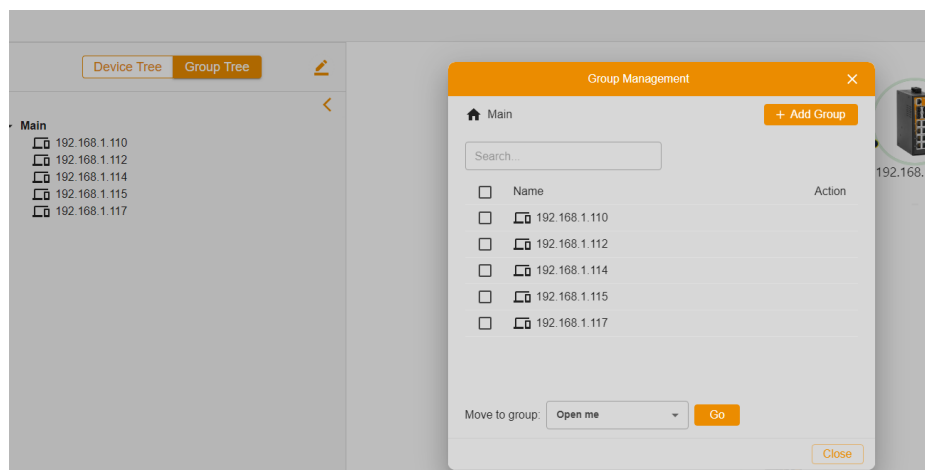


Figure 12: Group Management dialog

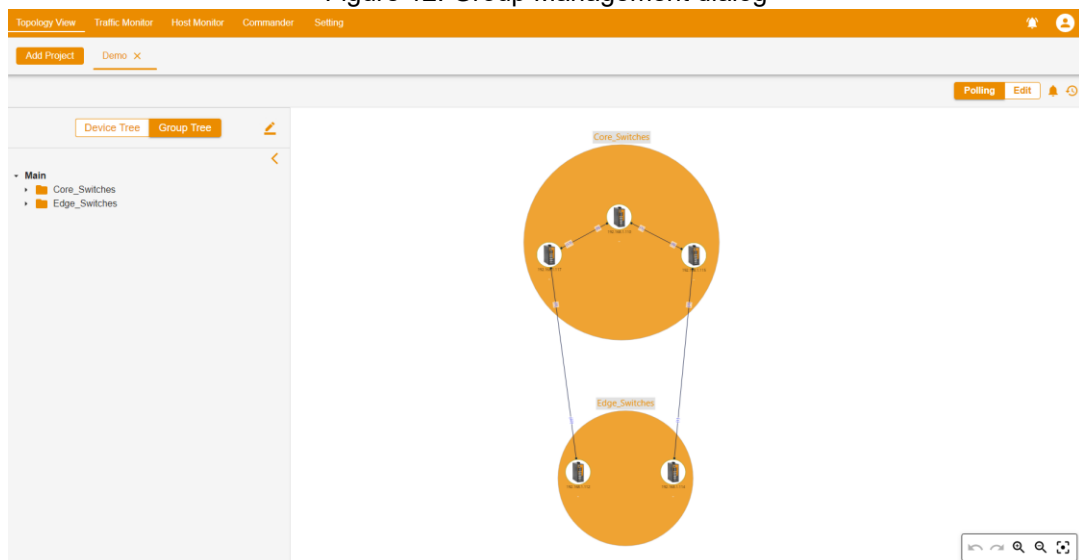


Figure 13: Example of a topology with two groups of devices

4.7 Device context menu

A right-click on a device icon opens the context menu:

Entry	Function
Ports Information	Opens the Device Information dialog with port, WAN, mobile, WLAN and DS serial information (quick view of the status of all ports).
Open in Web	Opens the web interface of the device (HTTPS) in a new browser tab.
Open SSH	Opens the command line interface of the device using the OpenSSH client of Windows (OpenSSH version 8.5 or higher).
Open Ping	Sends ping messages to the device to check connectivity.
Local Alert	Enable switch localization (front LEDs flash and an audible signal is generated via the output relay).
SNMP Test	Checks whether the device can be reached via SNMP.
Event Log in Web	Opens the event log of the device in its web interface.
Remove Device	Removes the device from the project.

Table 4: Device context menu



Figure 14: Context menu of a device

On the tab **Port Information**, the **Device Information** dialog shows the columns Port, Status, IP, MAC, Connected Port and System Name. **Refresh** queries the data again. For devices that cannot be reached, the table remains empty.

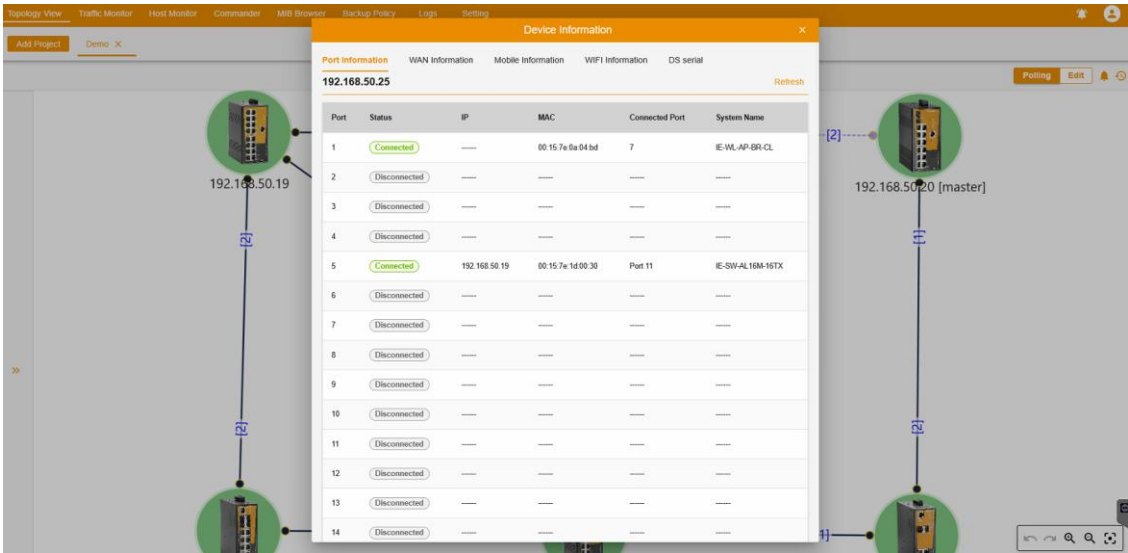


Figure 15: “Device Information” dialog

4.8 Edit mode

After switching to **Edit**, an additional toolbar appears:

Button	Function
+ Add Background	Adds a background to the topology, e.g. a different colour, a map or an image (hall or cabinet plan). Opens the file selection.
+ Add Device	Adds a single device manually (dialog New Device).
+ Add Edge	Adds a connection between two devices manually (dialog New Edge).
Refresh	Reads in the topology again immediately, e.g. after a new connection has been established.
Save File	Saves the changes to the project.

Table 5: Edit mode

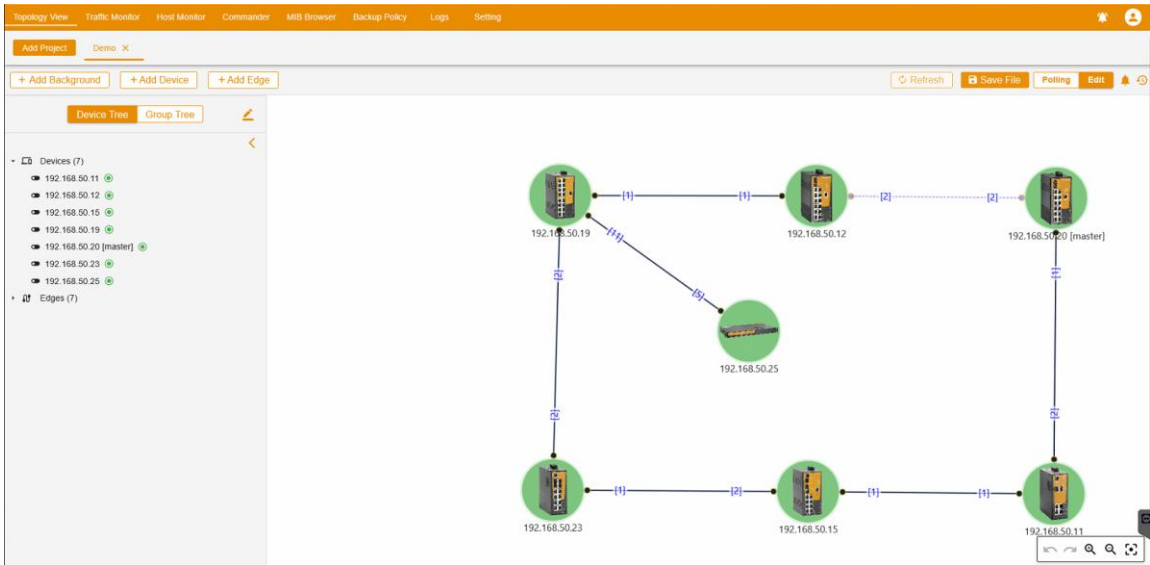


Figure 16: Topology View in “Edit” mode

Adding a device manually

1. Click **+ Add Device**.
2. Enter the **IP** of the device and select the device model under **Assign Model**.
3. Enable **SNMP Enable** and **ICMP Enable** as required (default: both enabled).

4. Define the **SNMP Version** (v1, v2c or v3), the **SNMP Port** (default 161) as well as **Read Community** and **Write Community**.
5. Confirm with **Add Device** and then save the project with **Save File**.

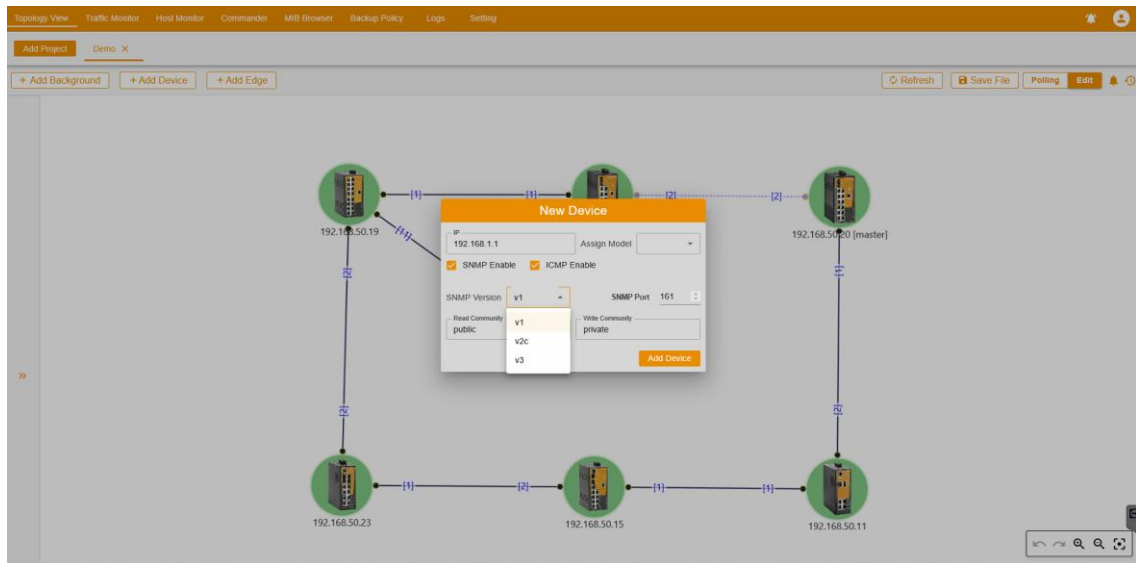


Figure 17: "New Device" dialog

Adding a connection (edge) manually

1. Click **+ Add Edge**.
2. Under **From**, enter the IP address and port of the first device.
3. Under **To**, enter the IP address and port of the second device.
4. Confirm with **Add Edge** and save with **Save File**.

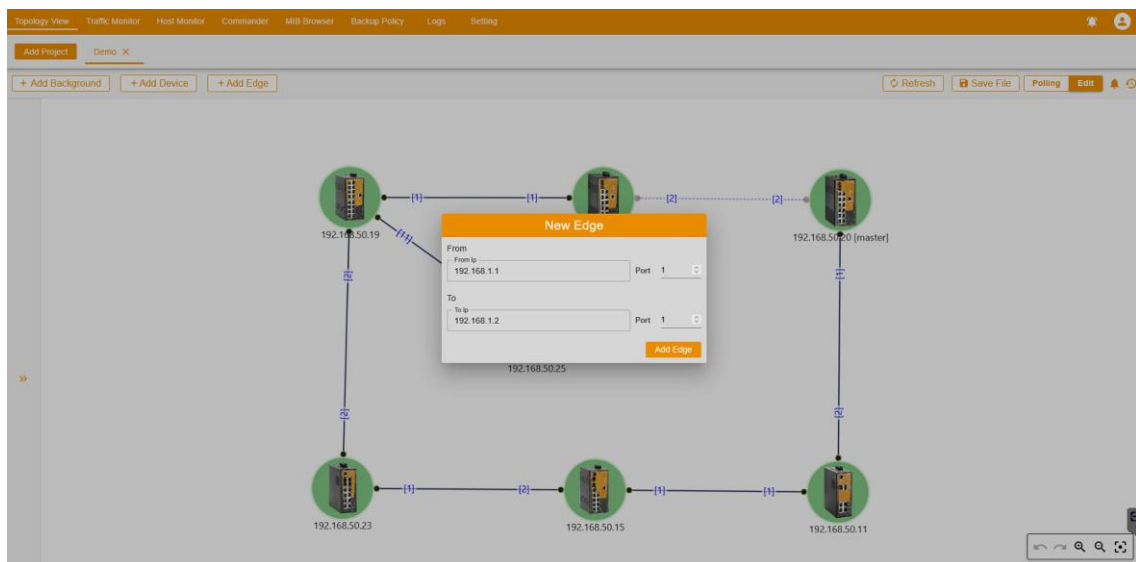


Figure 18: "New Edge" dialog



NOTE: Changes made in Edit mode are only saved permanently with **Save File**. A dialog can be closed without applying the changes using the Esc key.

4.9 Notifications and disconnection events

u-netops always notifies link disconnections in two ways:

1. The link that has gone down changes its colour (default: red).
2. A notification is shown at the bell next to the **Polling/Edit** switch.

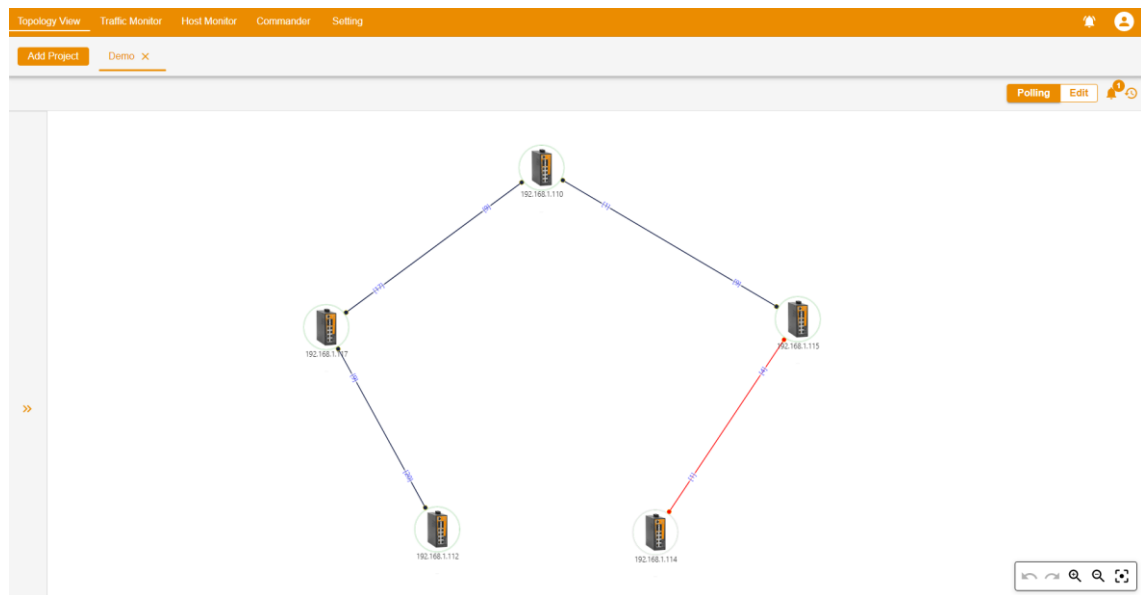


Figure 19: Disconnected link shown in red

Click the bell to display the disconnection message. It shows the date and time as well as the history of the link. The message can simply be closed or acknowledged (**Check All**). Acknowledged messages are no longer shown in the **Disconnection Event** list.

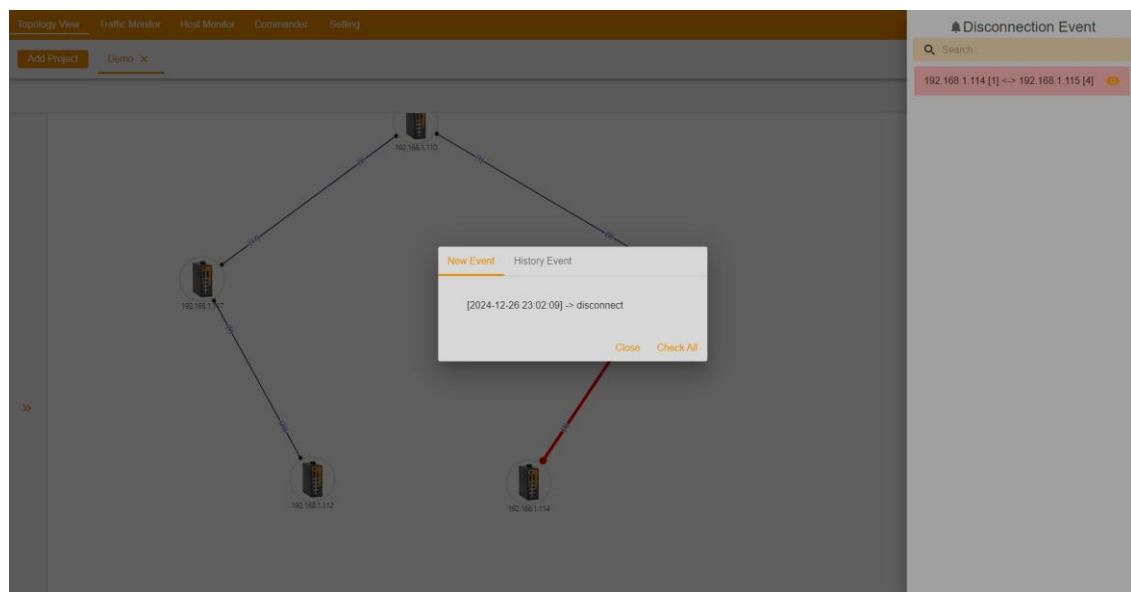


Figure 20: Disconnection event message

When a disconnected link is connected again, u-netops shows it in yellow as long as the disconnection event has not been acknowledged. If the event has already been acknowledged, the link returns to its normal colour when communication is restored. A yellow link is therefore healthy, but was disconnected at some point. The link colours can be changed under **Setting** → **Topology Config** (section 11.3 Topology Config).

4.10 System log in the topology view

The clock icon next to the bell displays the system log of u-netops as a sidebar. It shows all actions performed by the users with date and time. The system log is described in detail in section 10.1 System Log.

5. Traffic Monitor

The Traffic Monitor shows the traffic of the monitored devices. Any port of any device found in the Topology View can be selected. On the left there is a tree that groups the devices by model under **Main** → **Devices Types** (the number in brackets is the number of devices per model).

1. Open **Traffic Monitor** in the main menu.
2. In the tree, expand **Devices Types** and then the required model with **+**.
3. Select the device (IP address). The traffic data appears in the right-hand area.

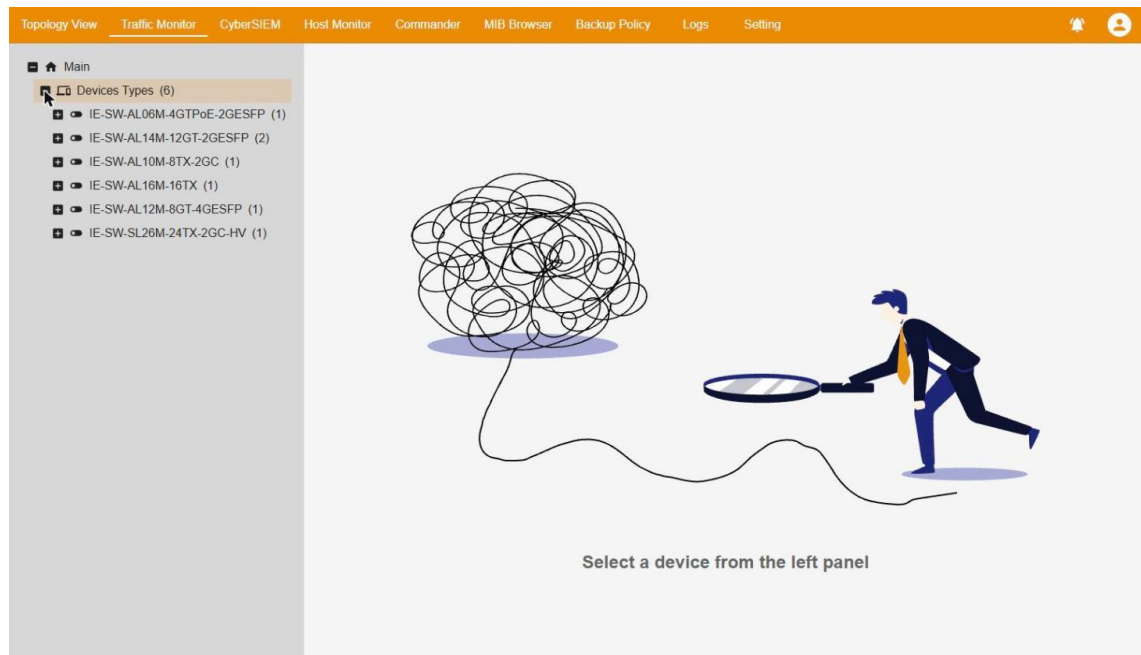


Figure 21: Traffic Monitor with expanded device tree



NOTE: As long as no device is selected or no data is available, the right-hand area shows “Select a device from the left panel”. Historical traffic data is only recorded if **RECORD TRAFFIC ENABLE** is active under **Setting** → **About** (see section 11.1 About).

5.1 Real-time traffic

When a switch is selected, all its ports are shown in the following colours:

- **Green:** the port is up (connected)
- **Grey:** the port is down (disconnected)
- **Red:** the port is disabled

Clicking a green port displays the real-time input and output traffic of this port. The traffic can be analysed in more detail by displaying the corresponding **Unicast**, **Multicast**, and **Broadcast** traffic values for the selected port.

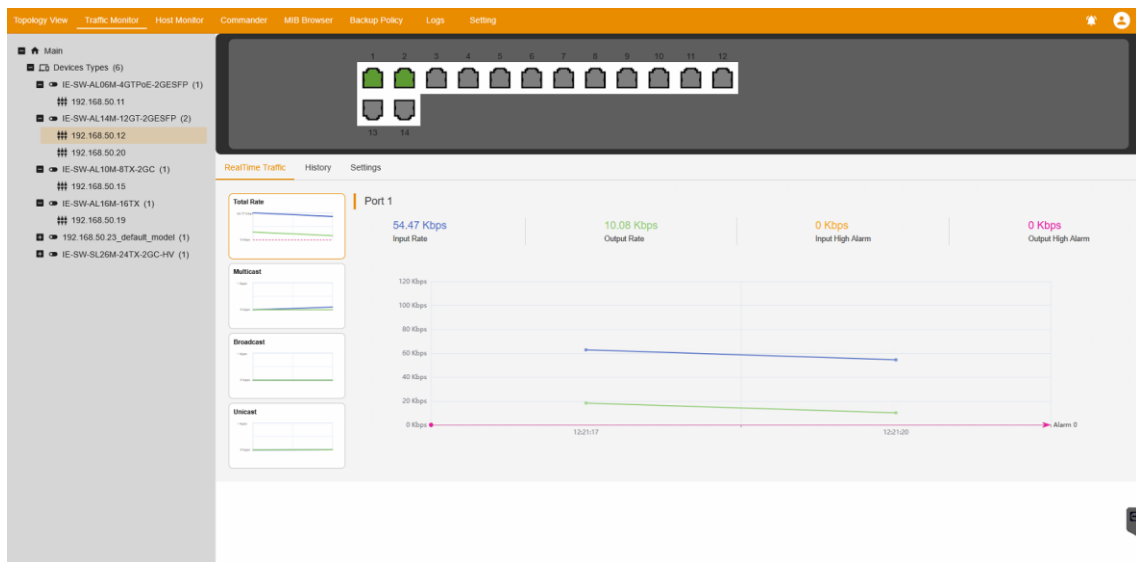


Figure 22: Real-time traffic of a port

5.2 History

On the **History** tab, the latest historical traffic records of a port can be displayed. One record corresponds to one minute. Select the number of latest records (between 5 and 15, i.e. up to the last 15 minutes) and click **Search**.

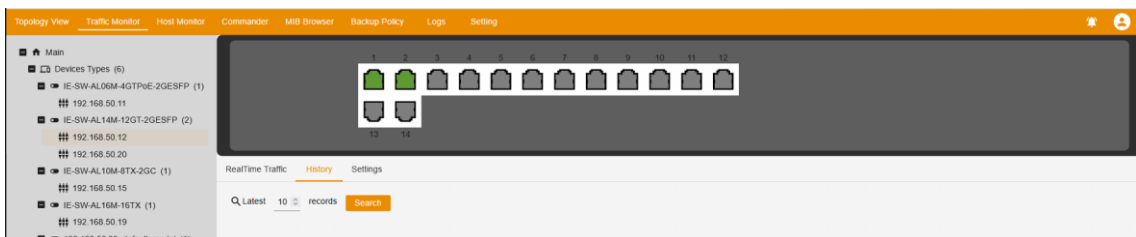


Figure 23: Traffic history

5.3 Traffic alarms (Setting)

On the **Setting** tab, thresholds for high-traffic notifications can be defined for the input and output traffic of every port. Select the **Alarm** check box(es) of the required port(s), enter the thresholds and click **Save Setting**.

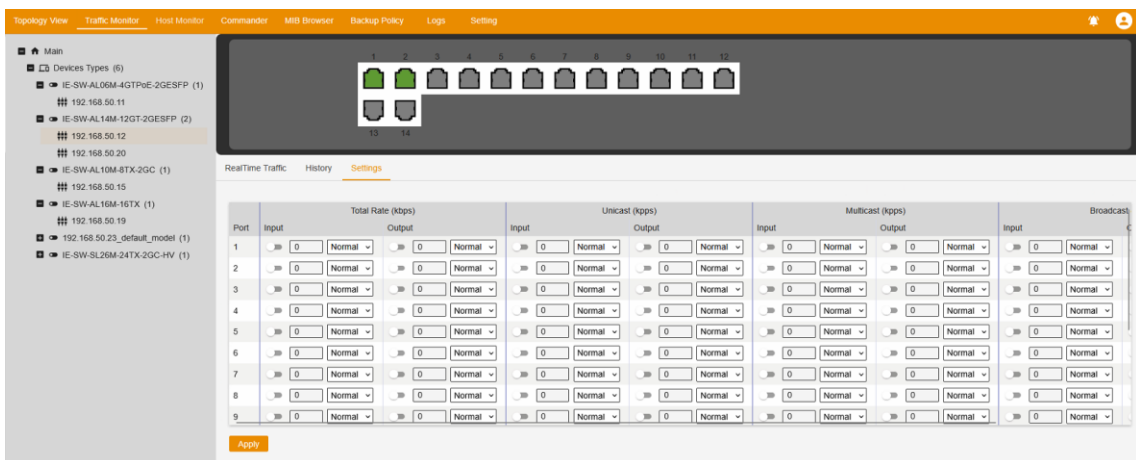


Figure 24: Defining traffic alarm thresholds

Once a traffic alarm is configured, the threshold is shown in the real-time traffic view. If the traffic exceeds the threshold for at least one minute, a high-traffic notification is generated at the bell in the upper right corner.

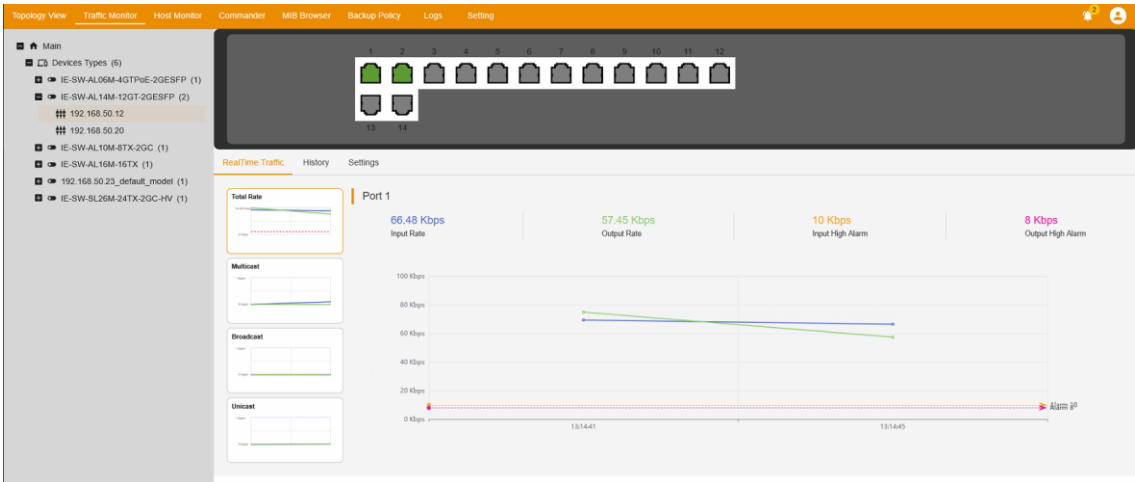


Figure 25: Threshold displayed in the real-time view

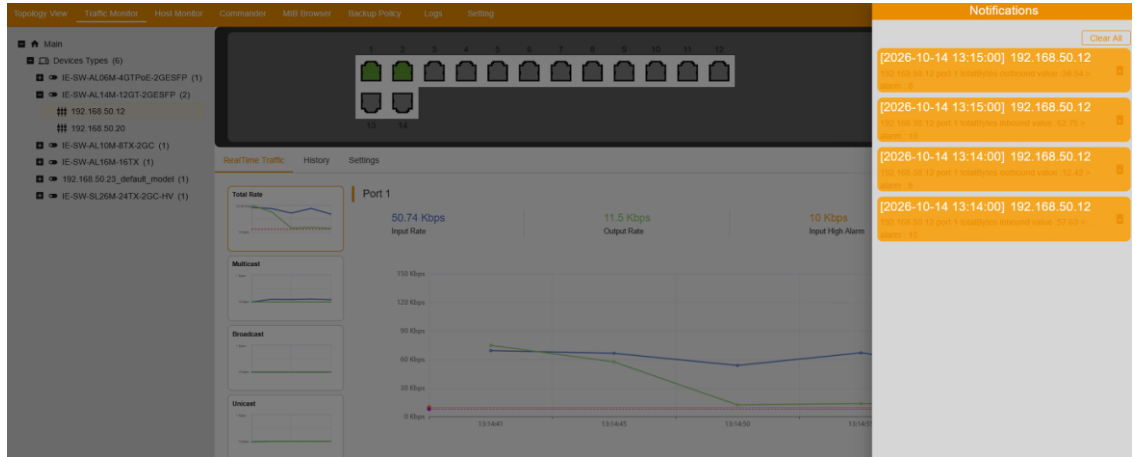


Figure 26: High-traffic notifications

Notifications can be deleted from the notification list; they remain available in the system log of u-netops.

6. Host Monitor

The Host Monitor provides an inventory of IP devices and checks their availability via ICMP (ping) in repeated test rounds with a single action. It is useful, for example, to check the availability of an entire address range after maintenance work.

6.1 “Monitor” view

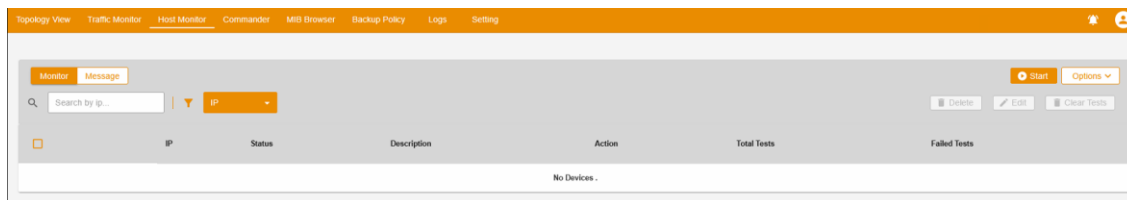


Figure 27: Host Monitor, “Monitor” view

Column / Element	Meaning
Monitor / Message	Switches between the inventory with the test results (Monitor) and the message panel with the test log (Message , section 6.5 “Message” view).
IP	Monitored address.
Status	Online or Offline .
Description	Optional description (can be changed with Edit).
Action	State of the test series, e.g. finish .
Total Tests / Failed Tests	Number of tests performed and failed.
Search / filter	Search the inventory filtered by IP, Status, Description or Action.
Start	Starts the test series for the monitored addresses.
Delete / Edit / Clear Tests	Active as soon as entries are selected: delete entries, edit the description (one entry), reset the test counters.
Options	Add Device, Configuration, Restart (restart the test series).

Table 6: Host Monitor, “Monitor” view

6.2 Adding addresses

1. Select **Options** → **Add Device**.
2. Enter a single address in the field **IP** and click **Add** – or enter a range in **From** / **To** and click **Add All**.
3. The addresses appear in the **Search List**. At this point, u-netops does not yet check whether they are reachable. Select them and move them to the **Device List** with **Add >**.
4. Save with **Submit** (or discard with **Cancel**).

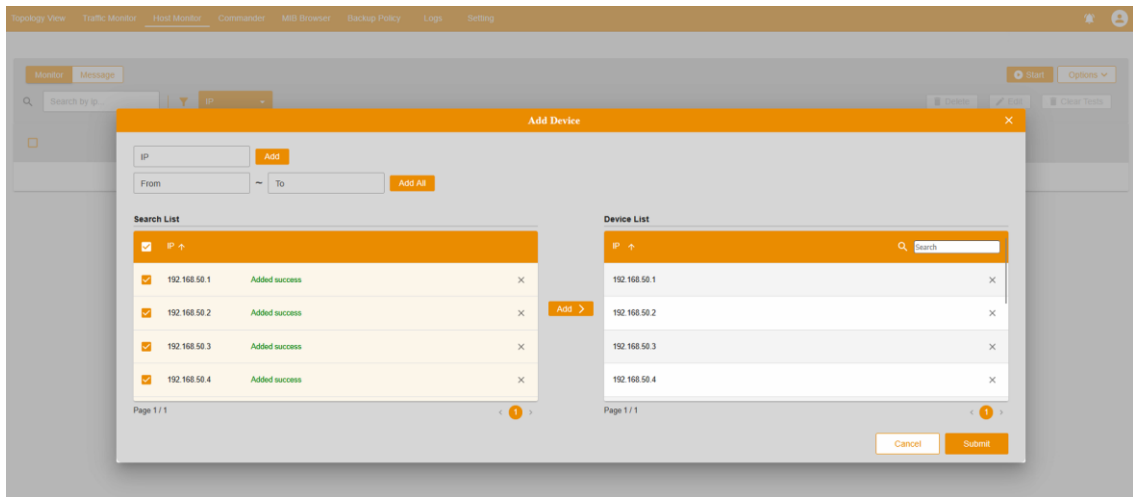


Figure 28: Host Monitor, "Add Device" dialog

To add a description, select a device in the list and click **Edit**.

6.3 Test configuration

Options → **Configuration** defines how long or how often the test is carried out:

- Tab **Mode**: **Timer** – stops after a number of minutes (stop after (minutes), default 5); **Test limit** – stops after a number of rounds (rounds, default 100).
- Tab **Polling settings**: **Polling Interval (ms)** (at least 500 ms, default 2000) and **Timeout (ms)** after which a device is considered unavailable (at least 100 ms, default 500).
- **Confirm** applies the values, **Reset to Default** restores the default values.

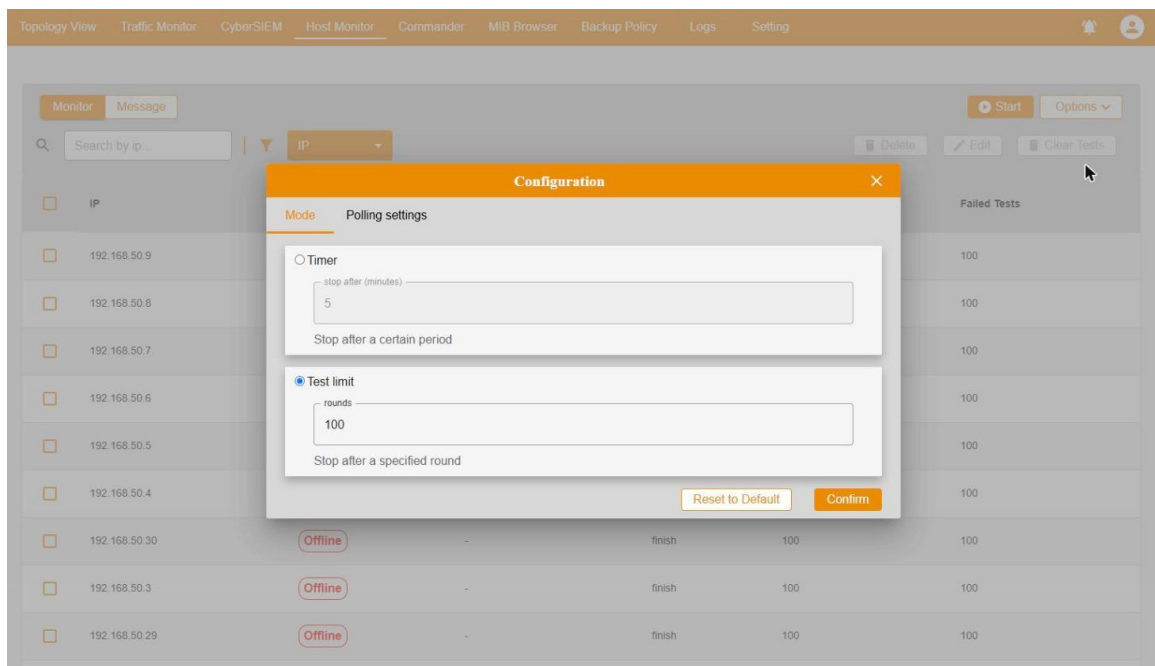


Figure 29: Configuration, "Mode" tab

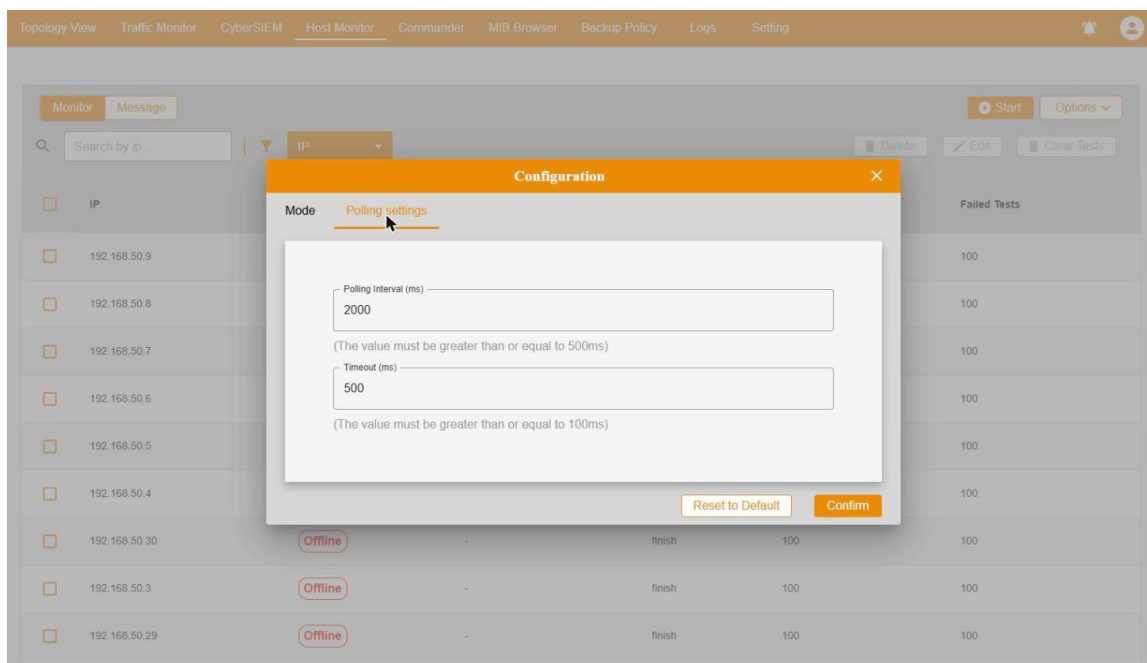


Figure 30: Configuration, “Polling settings” tab

6.4 Running a test

Select a single device or all devices (check box **IP**) and click **Start**. u-netops runs the test series and immediately shows whether the devices are **Online** or **Offline**, together with the total number of tests and the number of failed tests.

6.5 “Message” view

The **Message** view shows the result log of the tests with IP, time and message (e.g. connect success / connect failed). The list can be saved with **Export as CSV**, loaded with **Import as CSV** and emptied with **Clear log** (Administrator and Manager only).

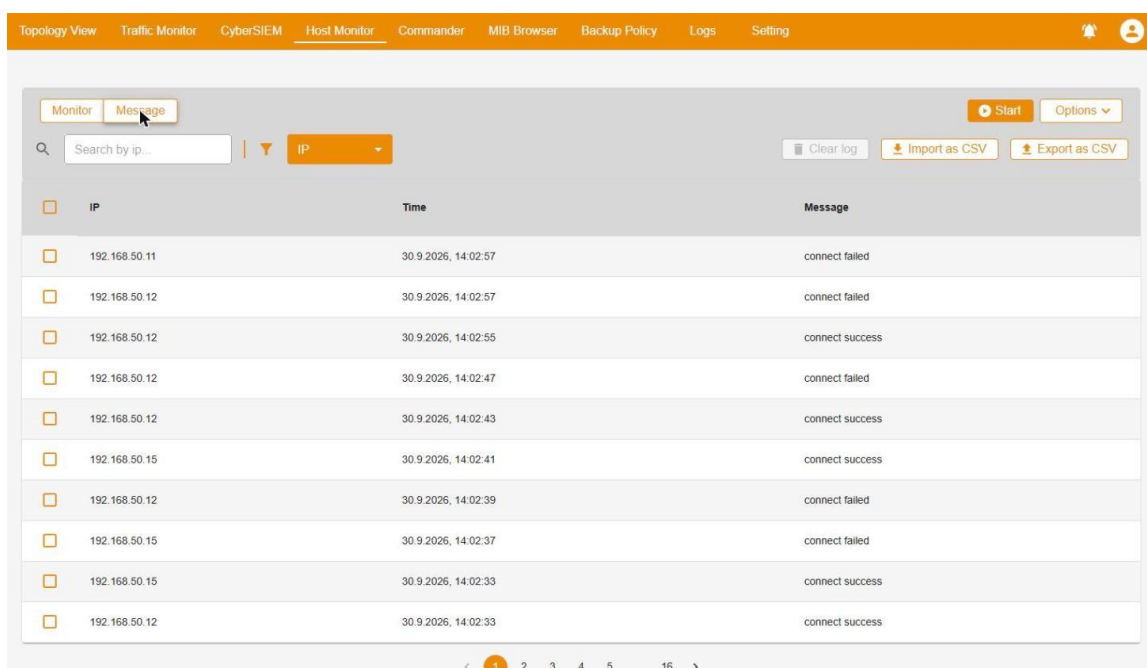


Figure 31: Host Monitor, “Message” view

7. Commander

The Commander is only applicable to switches of the Advanced and Substation Lines. It performs actions on one or several devices of the same model simultaneously:

- Firmware upgrade
- Configuration backup (get the configuration file of a switch)
- Configuration restore (load a configuration file onto a switch)
- Reboot

NOTE: The Commander functions require a minimum firmware version (also indicated in the user interface):



- IE-SW-AL/SL Full Gigabit series: firmware 1.38 or higher
- IE-SW-AL/SL Fast Ethernet series: firmware 1.18 or higher
- IE-SL-AL Lite Managed models: firmware 1.20 or higher

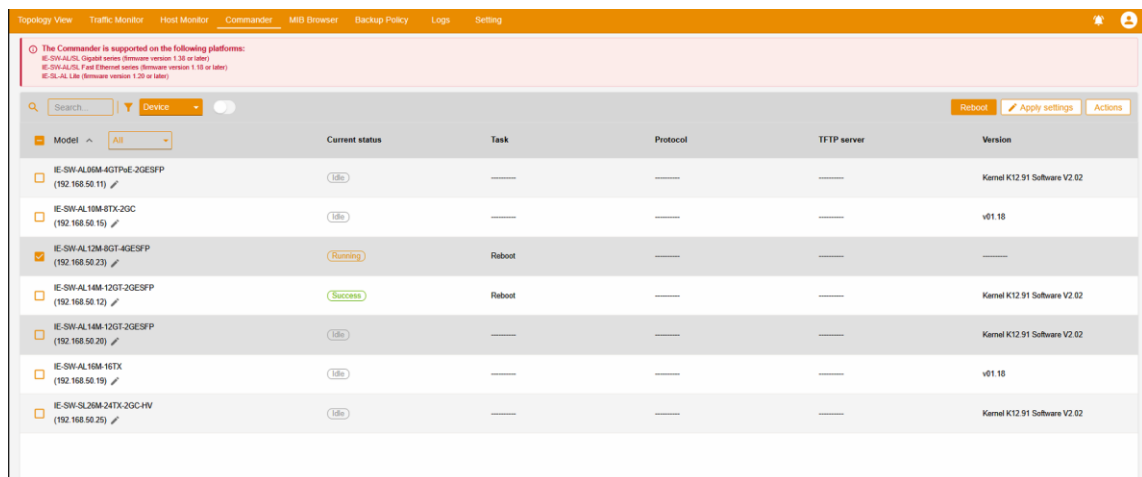


NOTE: Firmware upgrade as well as configuration backup and restore require an external TFTP server.



CAUTION: Firmware upgrade, config restore and reboot interrupt the operation of the switches concerned. Create an up-to-date configuration backup beforehand.

When **Commander** is selected, all devices found in the Topology View are listed. The list can be searched and filtered (e.g. by device name, status or version) and restricted to one model.



Model	Current status	Task	Protocol	TFTP server	Version
IE-SW-AL16M-40TPE-2GESFP (192.168.50.11)	Idle	---	---	---	Kernel K12.91 Software V2.02
IE-SW-AL16M-8TX-2GC (192.168.50.15)	Idle	---	---	---	v01.18
IE-SW-AL12M-8GT-4GESFP (192.168.50.23)	Running	Reboot	---	---	---
IE-SW-AL14M-12GT-2GESFP (192.168.50.12)	Success	Reboot	---	---	Kernel K12.91 Software V2.02
IE-SW-AL14M-12GT-2GESFP (192.168.50.20)	Idle	---	---	---	Kernel K12.91 Software V2.02
IE-SW-AL16M-16TX (192.168.50.19)	Idle	---	---	---	v01.18
IE-SW-SL26M-24TX-2GC-HV (192.168.50.25)	Idle	---	---	---	Kernel K12.91 Software V2.02

Figure 32: Commander device list

Column / Element	Meaning
Model	Device model and IP address. The selection field All filters by model.
Pencil icon	Opens the Information dialog with the device-specific transfer data.
Current status	State of the last action, e.g. Idle , Success or Failed .
Task	Last action performed, e.g. Reboot .
Protocol / TFTP server / Version	Stored transfer parameters and firmware version.
Reboot	Restarts the selected devices.

Column / Element	Meaning
Apply settings	Sets the transfer parameters for all selected devices at the same time.
Actions	Firmware Upgrade, Config Backup, Config Restore.

Table 7: Commander device list

7.1 Setting the transfer parameters

Before an action, the transfer data must be defined for each device. Otherwise the confirmation dialog reports “Some devices have missing or empty information” and **Confirm** remains disabled.

1. Select the devices concerned with the check boxes.
2. Click **Apply settings**.
3. Select the **Protocol** (currently only **TFTP**) and enter the **TFTP server IP address**.
4. Enter the file name under **Firmware upgrade file** and/or **Restore configuration file** (maximum 30 characters) according to the table below.
5. Apply with **Confirm**.

Field	Firmware Upgrade	Config Backup	Config Restore
Protocol	TFTP	TFTP	TFTP
TFTP server IP address	Server on which the firmware file is stored	Server on which the backup file will be stored	Server on which the configuration file is stored
Firmware upgrade file	Complete name of the firmware file	leave empty	leave empty
Restore configuration file	leave empty	leave empty	Complete name of the configuration file to be loaded

Table 8: transfer parameters

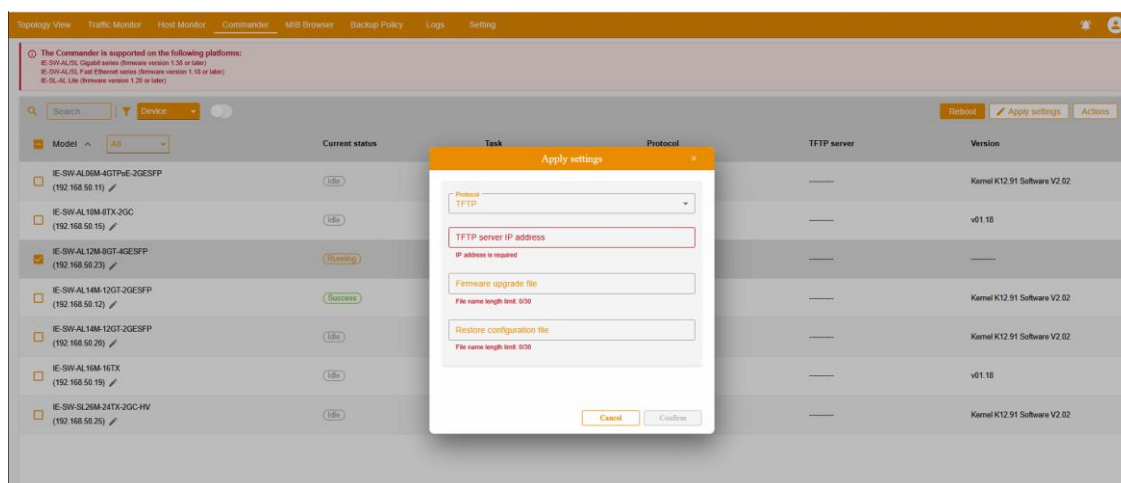


Figure 33: “Apply settings” dialog

For a single device, the values can be edited with the pencil icon in the **Information** dialog. There, **System Name** and **Restore folder** are also available.

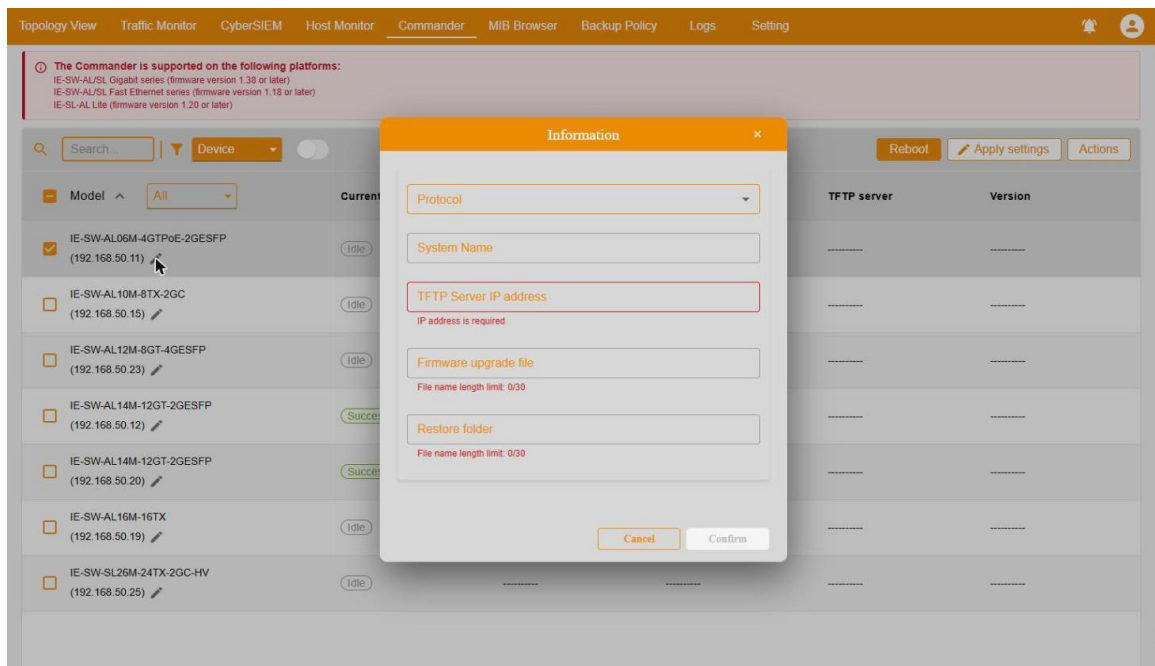


Figure 34: “Information” dialog of a single device

7.2 Running an action

1. Select the devices.
2. Open **Actions** and select **Firmware Upgrade**, **Config Backup** or **Config Restore** – or click **Reboot**.
3. Check the device list in the confirmation dialog and execute with **Confirm** (or abort with **Cancel**).
4. Follow the progress in the columns **Current status** and **Task**. When the process is finished, all devices should show **Success**; if a problem occurs on a device, **Failed** is shown.

The confirmation dialog offers two display modes (switch at the top right):

- **Simplified view** – only the list of devices with OID and IP address; a tooltip shows additional information.
- **Detailed view** – IP addresses of the devices together with the file name and the TFTP server IP address.

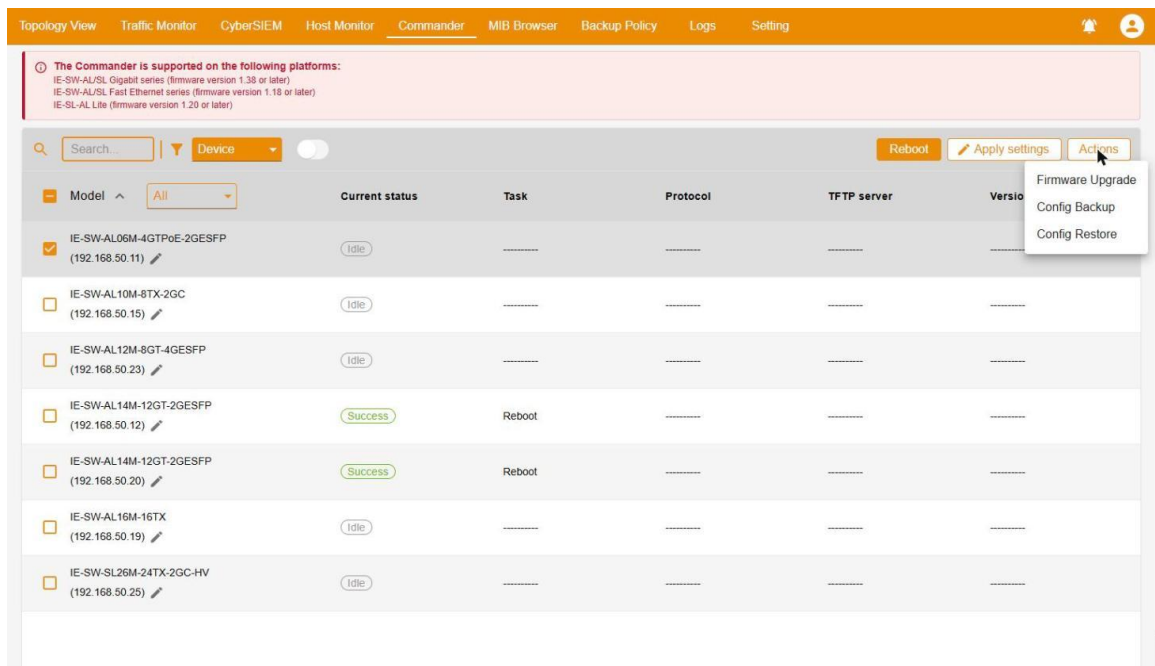


Figure 35: “Actions” menu with a selected device

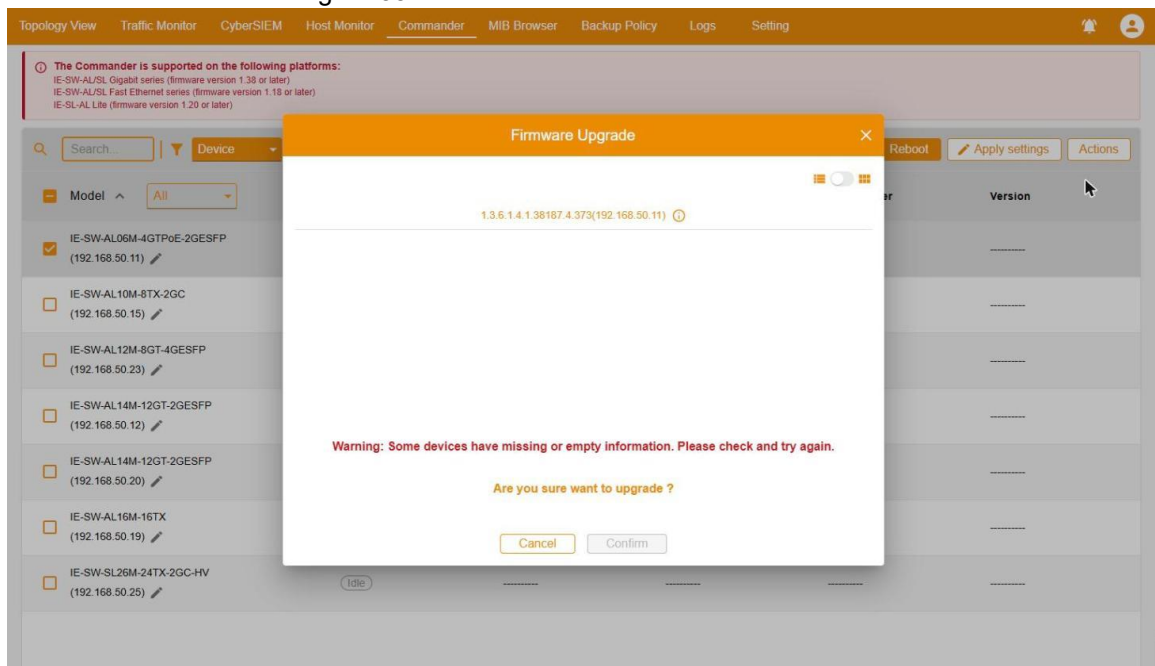


Figure 36: “Firmware Upgrade” confirmation dialog with warning about missing data

7.3 Firmware upgrade

Define the TFTP server and the firmware file (section 7.1 Setting the transfer parameters), then select **Actions** → **Firmware Upgrade** and confirm. The upgrade process starts and its progress is shown in **Current status**.

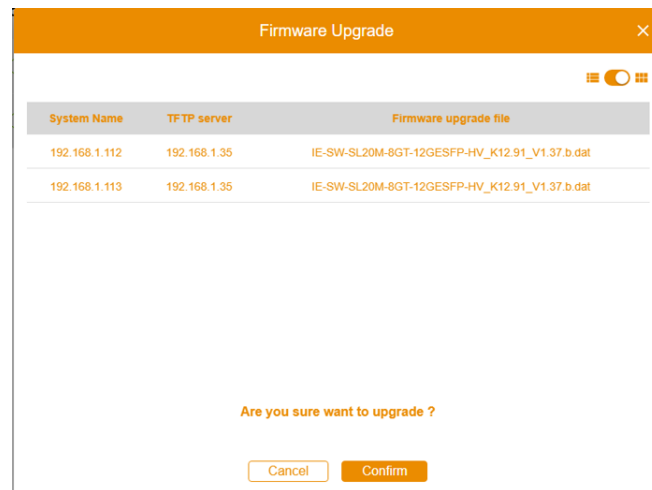


Figure 37: Firmware upgrade confirmation, detailed view



NOTE: The devices are not rebooted automatically after the firmware upgrade in order to avoid communication losses in the network. The new firmware only becomes active after the device has been rebooted (**Reboot**, section 7.6 Reboot).

7.4 Config backup

Define the TFTP server (section 7.1 Setting the transfer parameters), then select **Actions** → **Config Backup** and confirm. The backup file is stored on the TFTP server with the name **DeviceName_IPaddress_datetime.cfg**, e.g. IE-SW-SL20M-8GT-12GESFP-HV_192_168_1_112_20250104212008.cfg.



NOTE: For Full Gigabit switches, the backup contains the running configuration. For Fast Ethernet switches and Lite Managed models, it contains the configuration saved in the flash memory.

7.5 Config restore

Define the TFTP server and the configuration file (section 7.1 Setting the transfer parameters), then select **Actions** → **Config Restore** and confirm. The restore process starts and its progress is shown in **Current status**.



NOTE: On Full Gigabit switches, the loaded configuration is saved in both the running and the startup configuration. Fast Ethernet switches and Lite Managed models must be rebooted after a restore; the loaded configuration only becomes active after the reboot.

7.6 Reboot

Select the device(s) and click **Reboot**. After confirming with **Yes**, the reboot starts and its progress is shown in **Current status**.

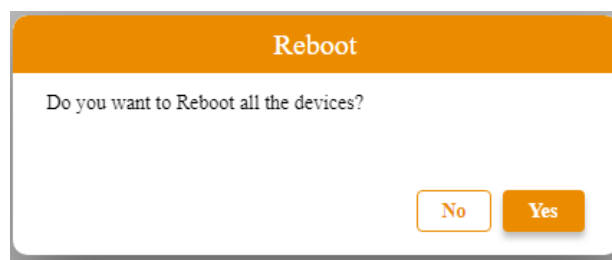


Figure 38: Reboot confirmation

8. MIB Browser

The MIB Browser queries SNMP objects directly from a device. It consists of the **MIB Tree** (left), a detail table for the selected object (bottom left) and the query area with the result table (right).

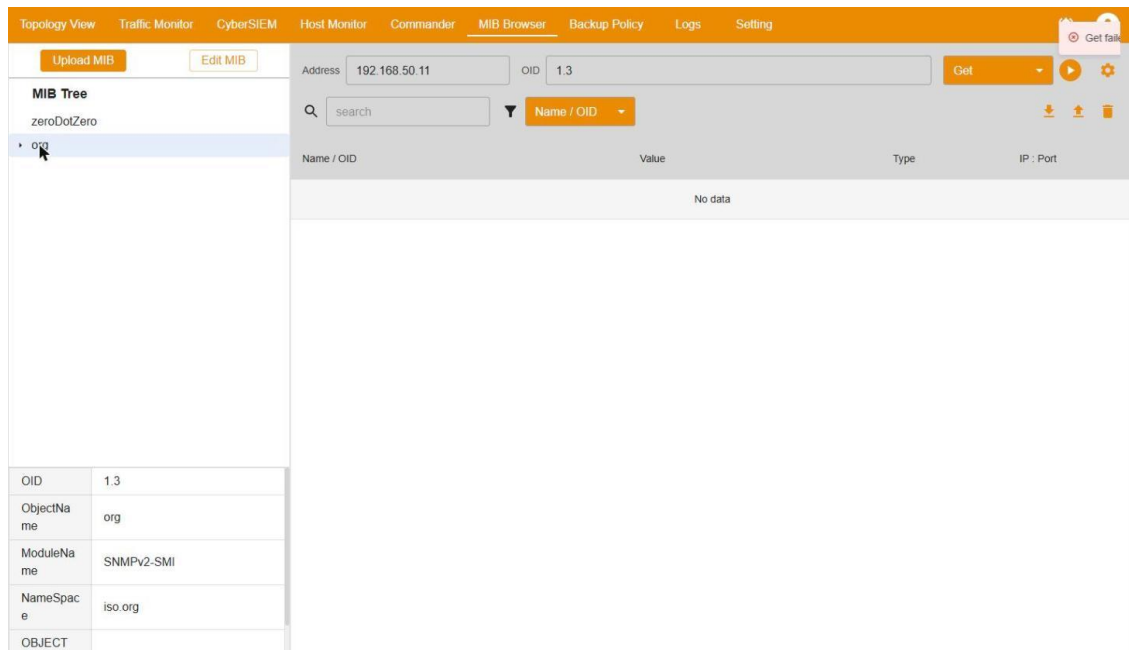


Figure 39: MIB Browser with the node “org” selected

8.1 Querying an object

1. Enter the IP address of the device in the field **Address**.
2. Click a node in the **MIB Tree** – the **OID** is taken over and OID, ObjectName, ModuleName, NameSpace etc. are shown at the bottom left. Alternatively, enter the OID directly.
3. Select the operation in the selection field: **Get**, **Get Next**, **Get Bulk**, **Subtree**, **Walk**, **Set** or **Table View**.



CAUTION: The **Set** operation writes values directly to the device and takes effect immediately. Incorrect values can change the device configuration or interrupt network operation. Only use **Set** if you know the meaning of the object, and only within maintenance windows. A **Write Community** with write access is required.

4. Execute with the round start button (▶). The results are shown with Name/OID, Value, Type and IP:Port.



NOTE: Double-clicking a node in the MIB Tree executes the selected operation immediately. Without an address, the message “Address is empty. Please enter a valid IP address.” appears.

8.2 SNMP parameters

The gear icon (**Advanced Properties of SNMP**) opens the connection parameters for the address entered: **Port** (default 161), **Read Community**, **Write Community** and **SNMP Version**. Apply them with **Apply**.

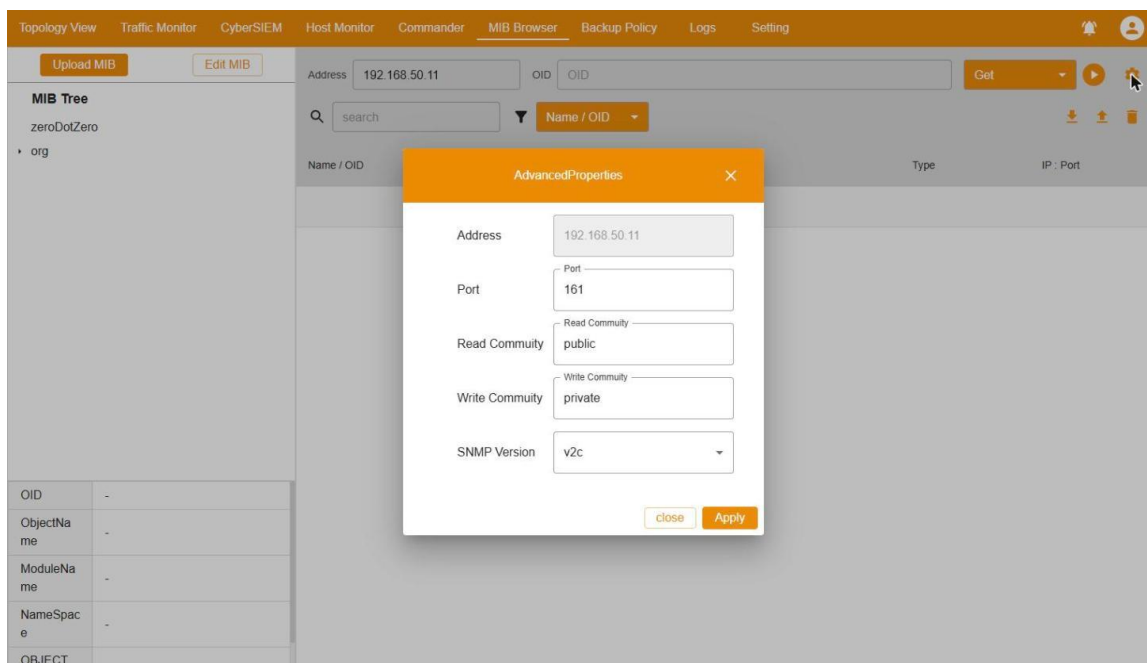


Figure 40: “AdvancedProperties” dialog

8.3 MIB files and result table

- **Upload MIB** loads vendor-specific MIB files, which then appear in the MIB Tree.
- **Edit MIB** lists the loaded MIB modules; individual modules can be removed, or all with **Remove all MIB**.
- The icons above the result table download the table, upload a table (**Upload Table**) or clear it (**Clear Table**).
- The search field with the selection **Name / OID** filters the result table.

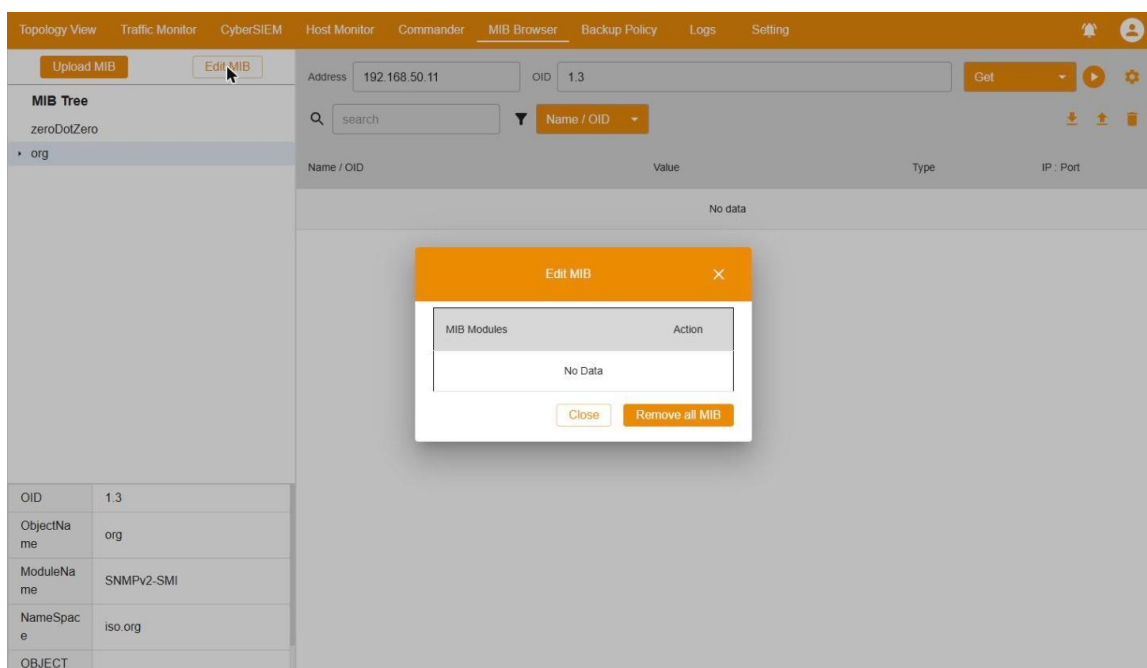


Figure 41: “Edit MIB” dialog

9. Backup Policy

Backup Policy backs up device configurations automatically and compares them with a reference (baseline). Both functions require a configured TFTP server; as long as none is configured, the page shows the message “Backup and Compare require a configured TFTP server.” and the action buttons are disabled.

9.1 Setting up the TFTP server

1. Click **TFTP Setting**.
2. Enter the **Host IP** and **Port** (default 69) of the TFTP server.
3. Save with **Save**. The header line then shows the server address.

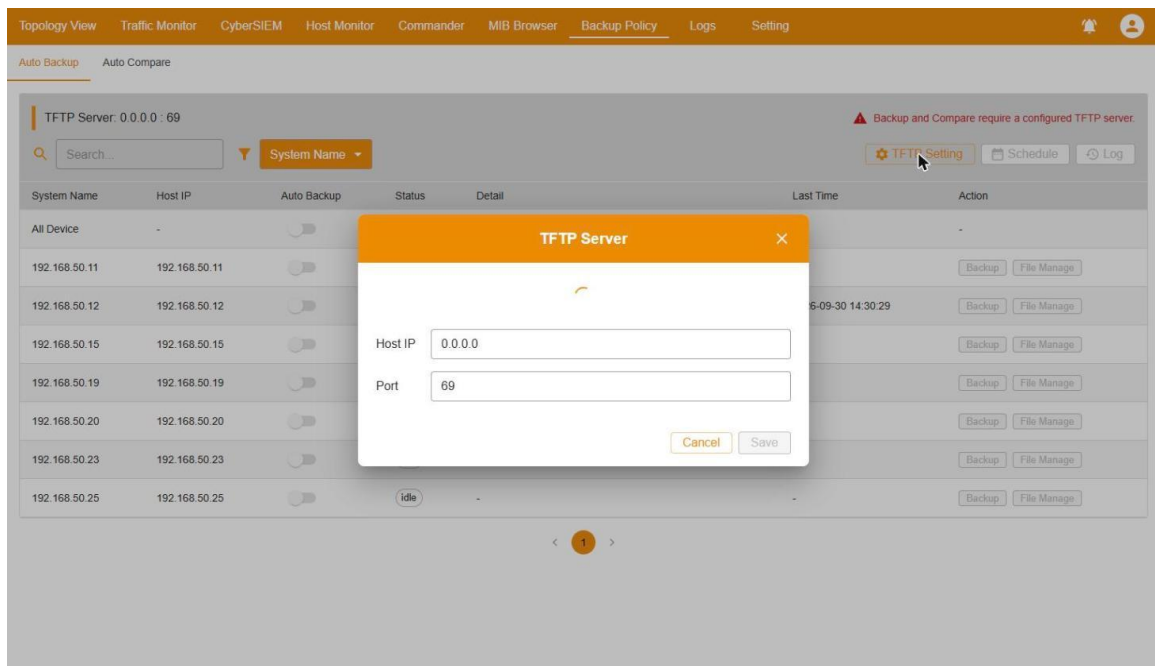


Figure 42: “TFTP Server” dialog

9.2 Auto Backup

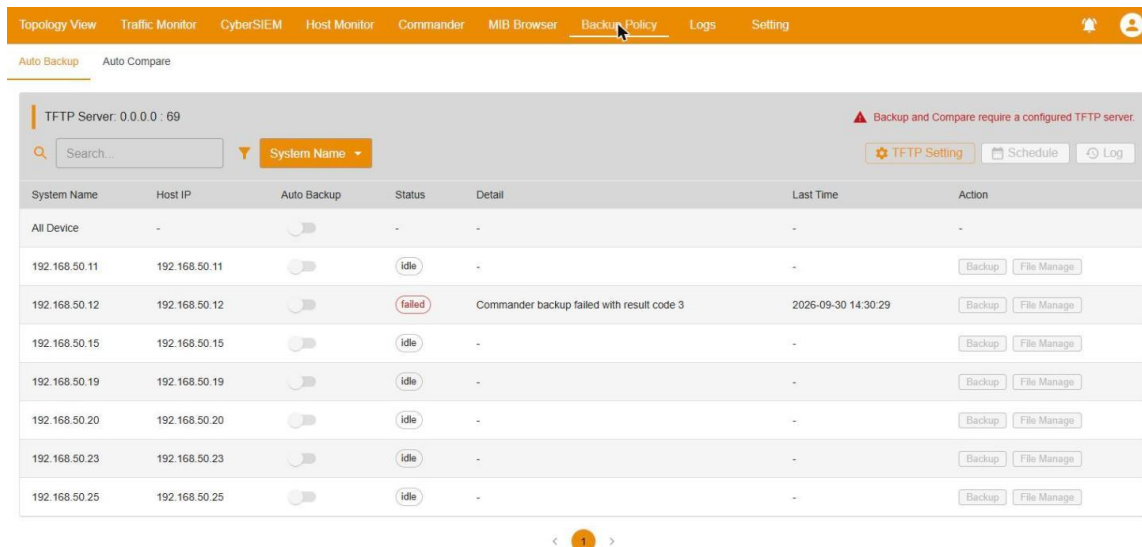


Figure 43: Auto Backup

Element	Function
Auto Backup (switch)	Enables automatic backup per device; the row All Device switches all devices together.
Status / Detail / Last Time	Result of the last backup (idle, failed ...), error message and time.
Backup	Backs up the configuration of the device immediately.
File Manage	Manages the stored backup files of the device.
Schedule	Defines the schedule for automatic backups.
Log	Shows the log of the backup operations.

Table 9: Auto Backup

Setting up an automatic backup

Make sure the TFTP server is configured (section 9.1).

Click Schedule and define [TBD: options, e.g. daily/weekly, time, interval]. Confirm with [TBD].

Enable the Auto Backup switch for the required devices, or for all devices with All Device.

Check the result in Status, Detail and Last Time. The Log button shows the history of all backup operations.

The backup files are stored on the TFTP server.

Managing backup files

File Manage lists the stored backups of a device with [TBD: columns]. Backups can be downloaded and deleted there.

9.3 Auto Compare

Auto Compare regularly compares the current device configuration with a stored **Baseline File**. Unexpected configuration changes are detected in this way.

1. Open the **Auto Compare** tab.
2. Upload a reference configuration (baseline) for the device with **File Upload**.
3. Enable the **Auto Compare** switch and define the schedule with **Schedule** – or compare immediately with **Compare**.

4. Check the result in **Status**, **Detail** and **Last Time**.

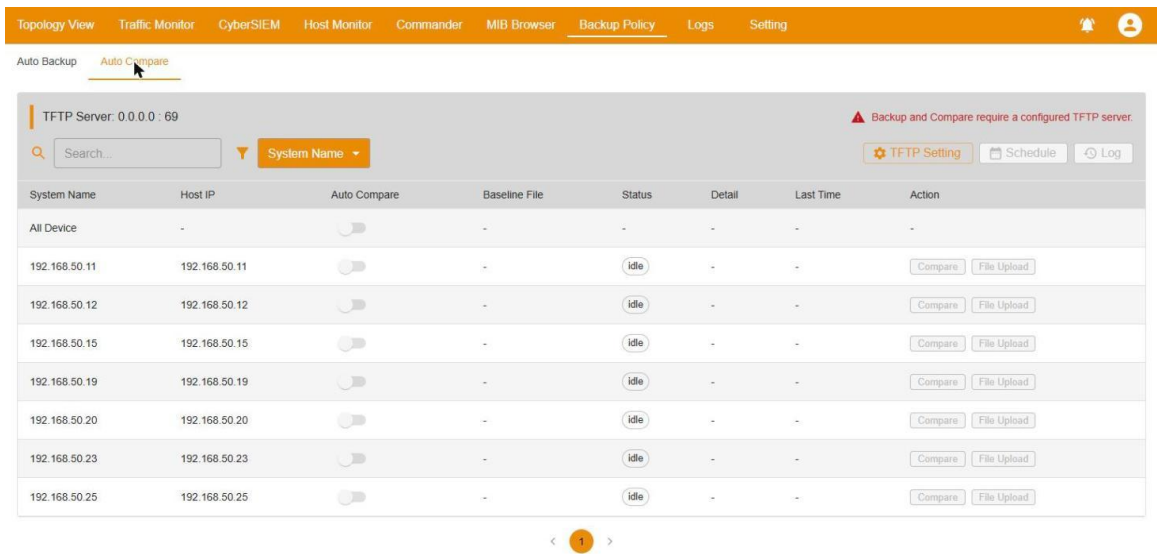
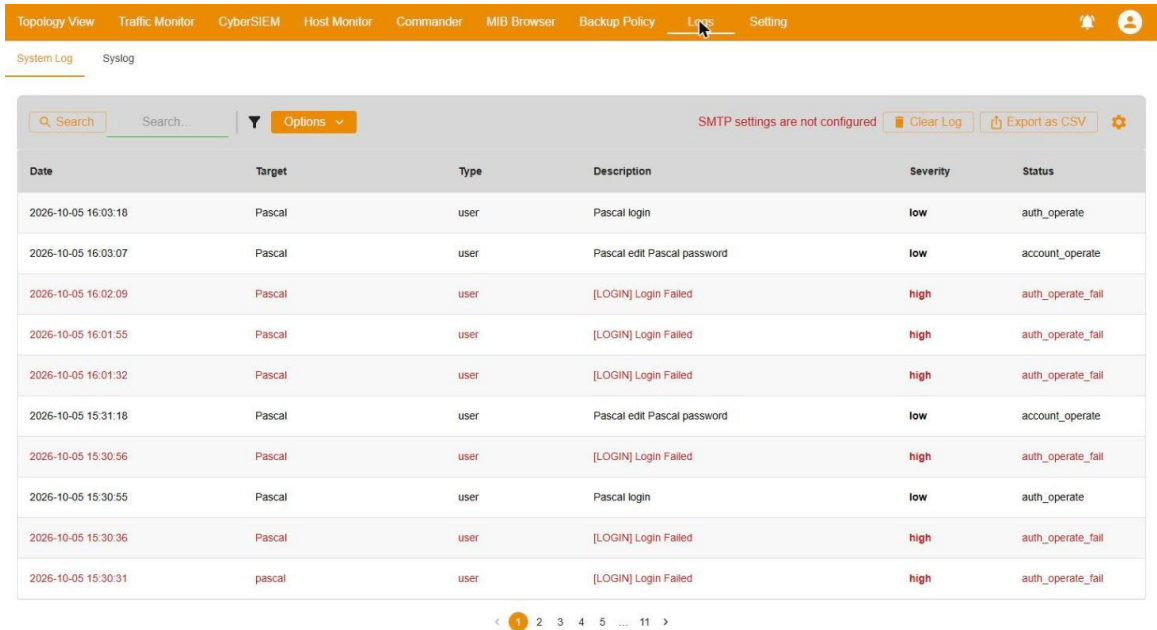


Figure 44: “Auto Compare” tab

10. Logs

10.1 System Log

The System Log records all events of the application: logins and logouts, configuration changes, device status and all other actions of the users, each with date and time. Entries with severity **high** are shown in red. Users with the Administrator or Manager profile can clear the system log.



Date	Target	Type	Description	Severity	Status
2026-10-05 16:03:18	Pascal	user	Pascal login	low	auth_operate
2026-10-05 16:03:07	Pascal	user	Pascal edit Pascal password	low	account_operate
2026-10-05 16:02:09	Pascal	user	[LOGIN] Login Failed	high	auth_operate_fail
2026-10-05 16:01:55	Pascal	user	[LOGIN] Login Failed	high	auth_operate_fail
2026-10-05 16:01:32	Pascal	user	[LOGIN] Login Failed	high	auth_operate_fail
2026-10-05 15:31:18	Pascal	user	Pascal edit Pascal password	low	account_operate
2026-10-05 15:30:56	Pascal	user	[LOGIN] Login Failed	high	auth_operate_fail
2026-10-05 15:30:55	Pascal	user	Pascal login	low	auth_operate
2026-10-05 15:30:36	Pascal	user	[LOGIN] Login Failed	high	auth_operate_fail
2026-10-05 15:30:31	pascal	user	[LOGIN] Login Failed	high	auth_operate_fail

Figure 45: Logs → System Log

Element	Function
Search / Options	Search; Options selects the search column (Target, Type, Description, Severity, Status, Date).
Clear Log	Deletes the system log.
Export as CSV	Saves the log as a CSV file.
Gear icon	Opens System Log Settings (severity and e-mail alert per event type).
Columns	Date, Target, Type, Description, Severity, Status.

Table 10: Logs → System Log

10.2 Event types and e-mail alerts

In **System Log Settings**, the severity (**Low**, **Normal**, **High**) is defined for each event type and the **Email Alert** can be enabled. Save with **Save**, reset with **Reset to Default**. A complete list of the event types is given in Appendix A.

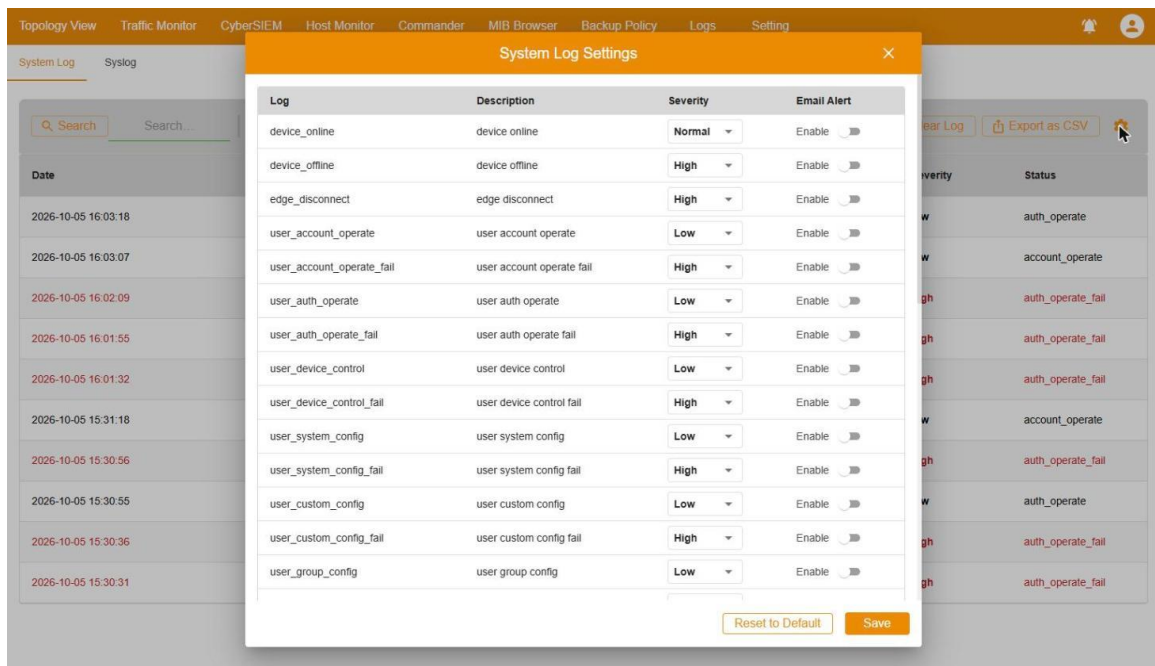


Figure 46: “System Log Settings” dialog



NOTE: E-mail alerts require a configured SMTP server (user menu → **SMTP Setup**, section 12.5 SMTP Setup). Otherwise the log shows the message “SMTP settings are not configured”.

10.3 Syslog

The **Syslog** tab shows the syslog messages sent by the devices to u-netops (columns IP, Message, Time). The search can be restricted to one column; **Export Log** saves and **Clear Log** empties the list. For messages to appear, u-netops must be configured as syslog server in the switches.

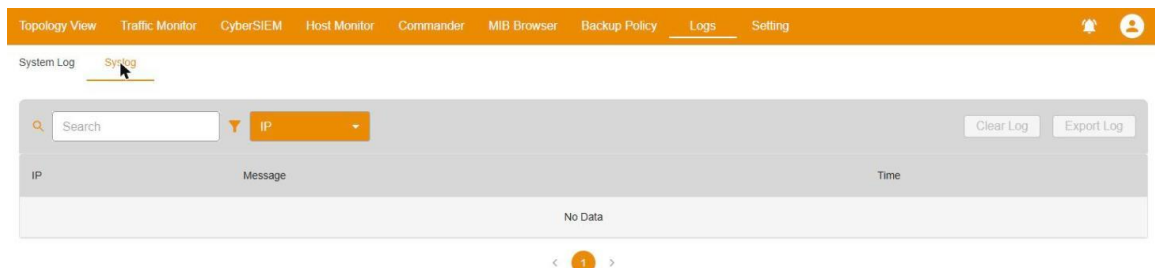


Figure 47: Logs → Syslog

11. Setting

The **Setting** menu contains the system-wide parameters of u-netops.

11.1 About

Shows the current **App Version** and the recording options:

- **RECORD TRAFFIC ENABLE** – records traffic data so that historical information of all switch ports can be displayed in the Traffic Monitor (section 5.2). Disabled by default.
- **RECORD SYSTEM ENABLE** – records system data and events. Enabled by default.
- **RECORD EXPIRED** – retention period of the records in days (example: 60).

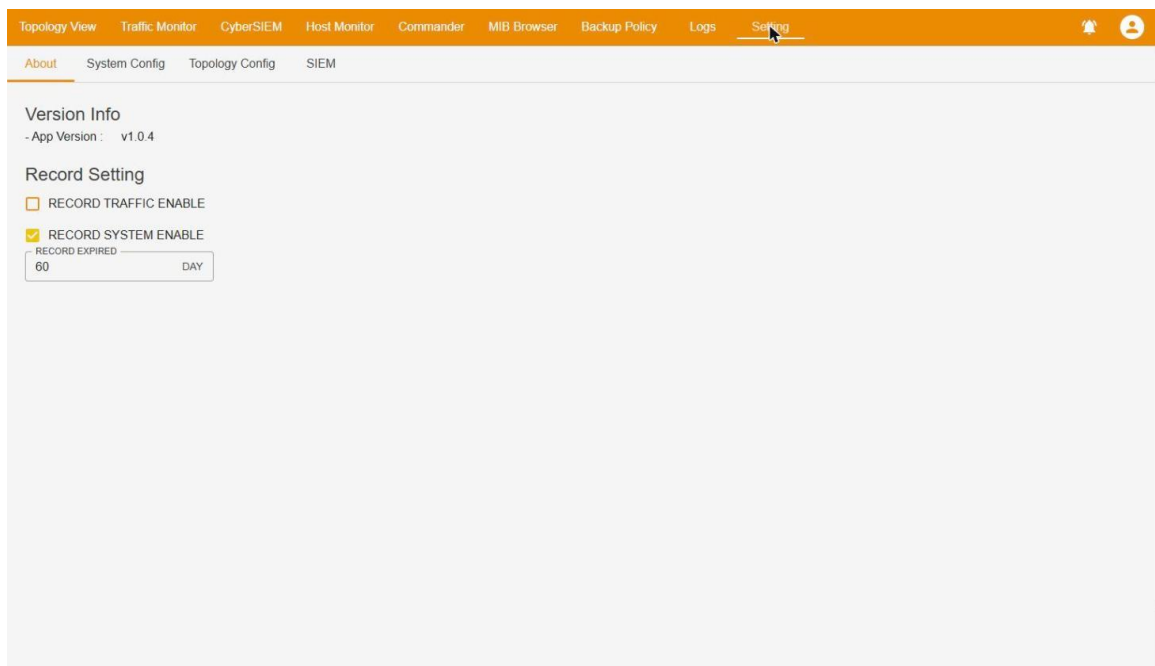


Figure 48: Setting → About

11.2 System Config

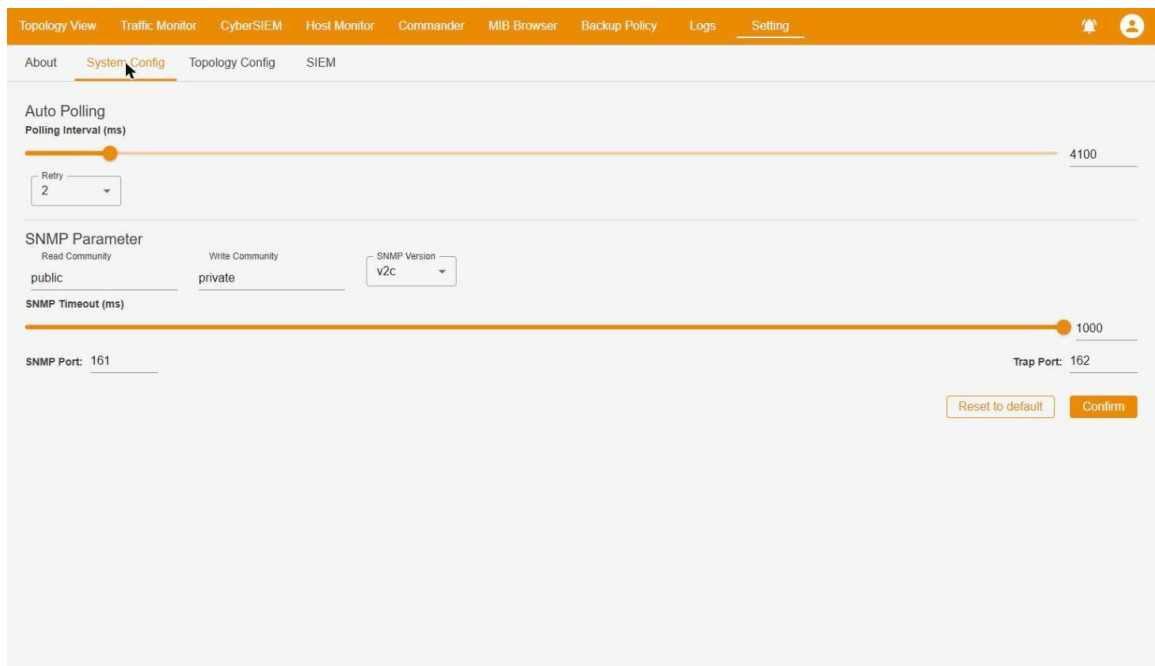
Global polling and SNMP parameters. Apply changes with **Confirm**; **Reset to default** restores the default values.

Parameter	Meaning
Polling Interval (ms)	Interval of the automatic status queries (Auto Polling; slider or input).
Retry	Number of retries before a device is considered unreachable.
Read / Write Community	Default community strings for SNMP v1/v2c (defaults: public / private).
SNMP Version	Default SNMP version for new devices.
SNMP Timeout (ms)	Waiting time for an SNMP response.
SNMP Port / Trap Port	Ports for SNMP queries (default 161) and for receiving traps (default 162).

Table 11: System Config



NOTE: The default communities **public** and **private** are widely known. For security reasons, change them on the switches and in u-netops, or use SNMPv3 with **AuthPriv**.

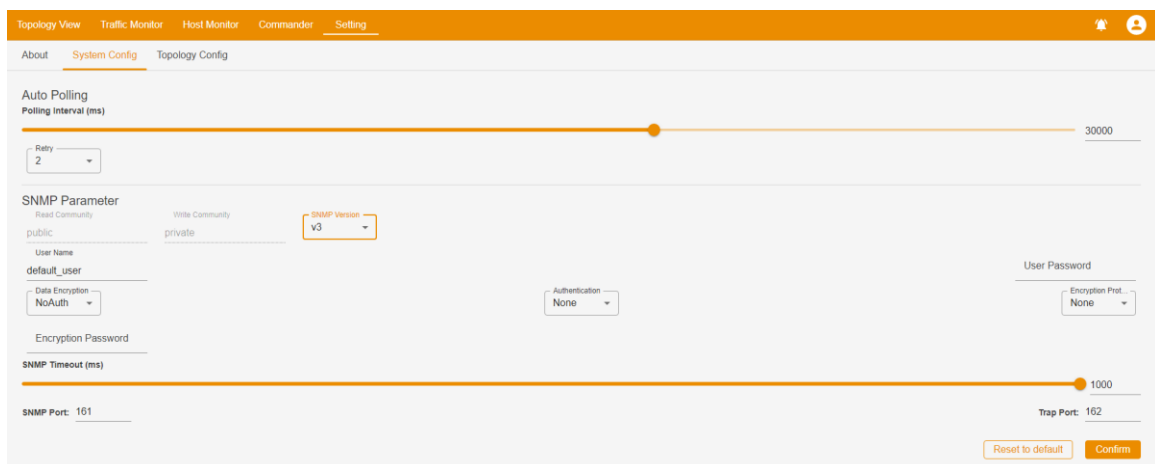


The screenshot shows the 'System Config' page in the u-netops interface. The 'Auto Polling' section has a 'Polling Interval (ms)' slider set to 4100 and a 'Retry' dropdown set to 2. The 'SNMP Parameter' section includes 'Read Community' (public), 'Write Community' (private), and 'SNMP Version' (v2c). The 'SNMP Timeout (ms)' slider is set to 1000. The 'SNMP Port' is 161 and the 'Trap Port' is 162. There are 'Reset to default' and 'Confirm' buttons at the bottom right.

Figure 49: Setting → System Config

With SNMPv3, a user name and password are configured as well as the authentication and encryption protocols:

- **Data Encryption (security level):** the default value is **NoAuth**. It is highly recommended to select **AuthPriv**, so that both authentication and encryption are required. With **AuthNoPriv**, only authentication is required, without encryption.
- **Authentication:** MD5 or SHA.
- **Encryption:** AES.



This screenshot shows the 'System Config' page with SNMPv3 parameters. The 'Auto Polling' section has a 'Polling Interval (ms)' slider set to 30000 and a 'Retry' dropdown set to 2. The 'SNMP Parameter' section includes 'Read Community' (public), 'Write Community' (private), and 'SNMP Version' (v3). Below these, there are fields for 'User Name' (default_user), 'Data Encryption' (NoAuth), 'Authentication' (None), 'Encryption Password', and 'User Password'. The 'SNMP Timeout (ms)' slider is set to 1000. The 'SNMP Port' is 161 and the 'Trap Port' is 162. There are 'Reset to default' and 'Confirm' buttons at the bottom right.

Figure 50: SNMPv3 parameters in System Config



NOTE: The SNMP parameters configured in u-netops (v1, v2c or v3) must match those configured on the Ethernet switches to be managed.

11.3 Topology Config

Display settings of the topology view. Apply with **Apply**.

- **Device Display Option** – label of the devices with **IP** and/or **System Name**.

- **View Option – Edge size** (thickness of the links) and **Font size** (size of the labels such as IP address, port number or switch role in a redundant topology).
- **Link Option** – colours of the links: Normal, Issues Remain (link restored, disconnection not yet acknowledged), Backup, Disconnect.
- **State Option** – colours of the device states: Online, Offline, Focus (switch selected), Buzzer (local alert enabled).

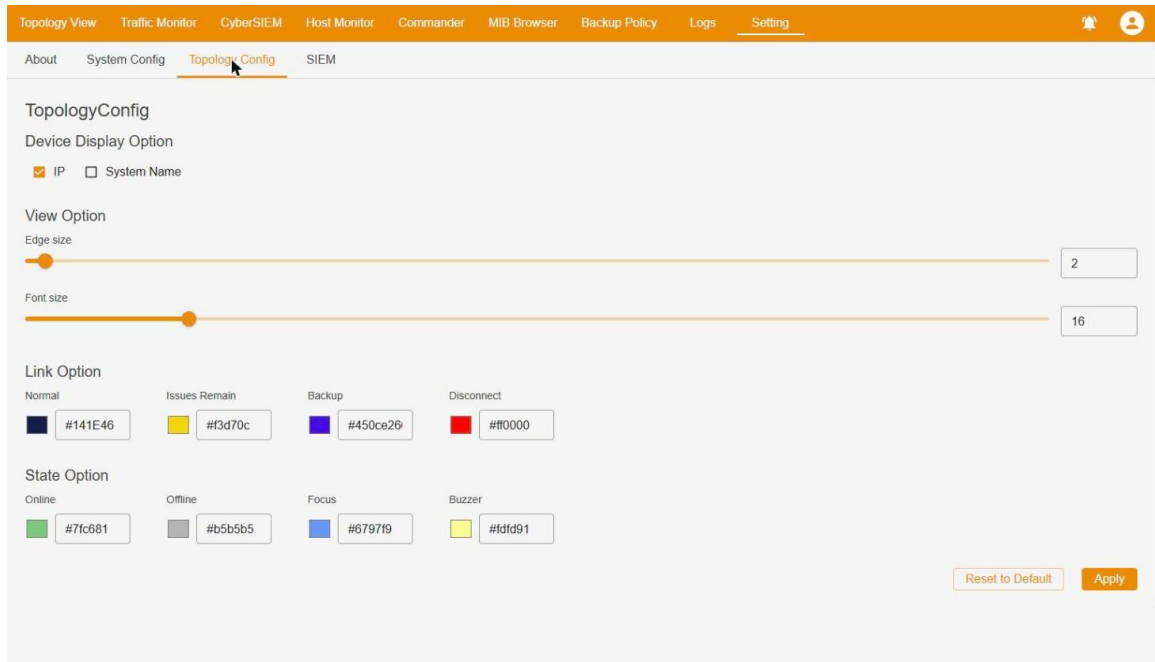


Figure 51: Setting → Topology Config

12. User Menu

The person icon in the upper right corner opens functions for users, licences and system services.



NOTE: These options are only available to the Administrator. Users with the Manager or User profile only see **Logout** in the user menu.

12.1 Account

Account Management lists the users by role (**Administrator**, **Manager**, **User**) with login ID and last activity. The pencil icon edits an account (e.g. to change the password). The Administrator can also delete users and reset their passwords.

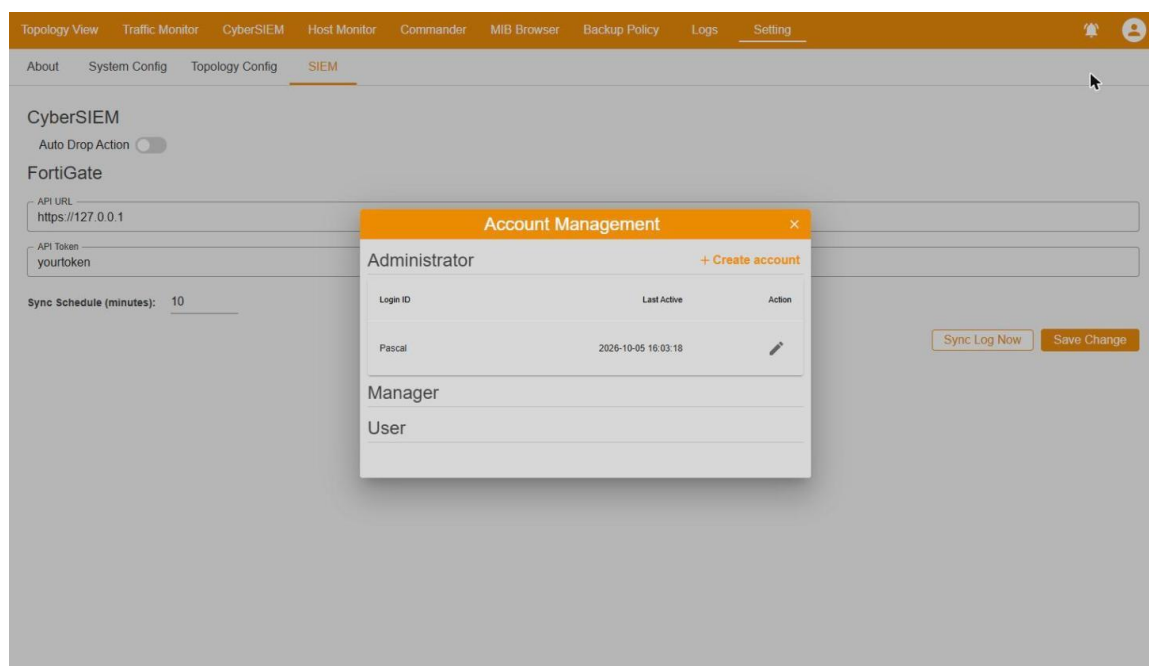


Figure 52: “Account Management” dialog

Role	Rights
Administrator	Full access. Created when u-netops is accessed for the first time (section 2.4); manages users and has access to the user menu.
Manager	Same rights as the Administrator in the main modules (e.g. Topology View, Traffic Monitor, Host Monitor, Commander). In Setting , only Topology Config can be modified; no access to the user menu (except Logout).
User	Monitoring only. Cannot modify settings or acknowledge disconnection events.

Table 12: “Account Management” dialog

Creating a user

1. Click **+ Create account**.
2. Enter a **Login ID**.
3. Enter the password in **password** and **confirmPassword** – or generate a secure password with **Generate password** and copy it with the copy icon. The password rules of section 2.4 apply.
4. Select the role **Manager** or **User** under **Role**.
5. Create the account with **Create**.

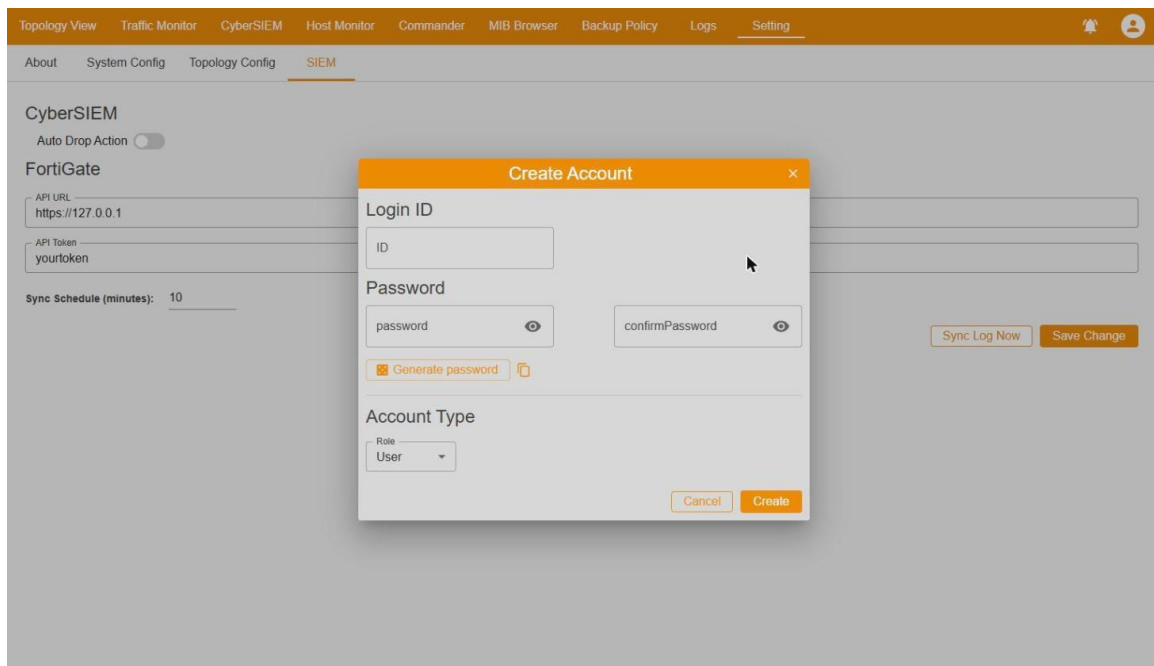


Figure 53: "Create Account" dialog

12.2 License

The License Management dialog provides an overview of all activated licenses and the current license usage.

It displays:

- The number of currently used devices compared to the maximum licensed devices (for example, 7 / 50).
- The current CodeMeter Status.
- A list of all available licenses including:
 - License name
 - Additional device count
 - Expiration date
 - License status

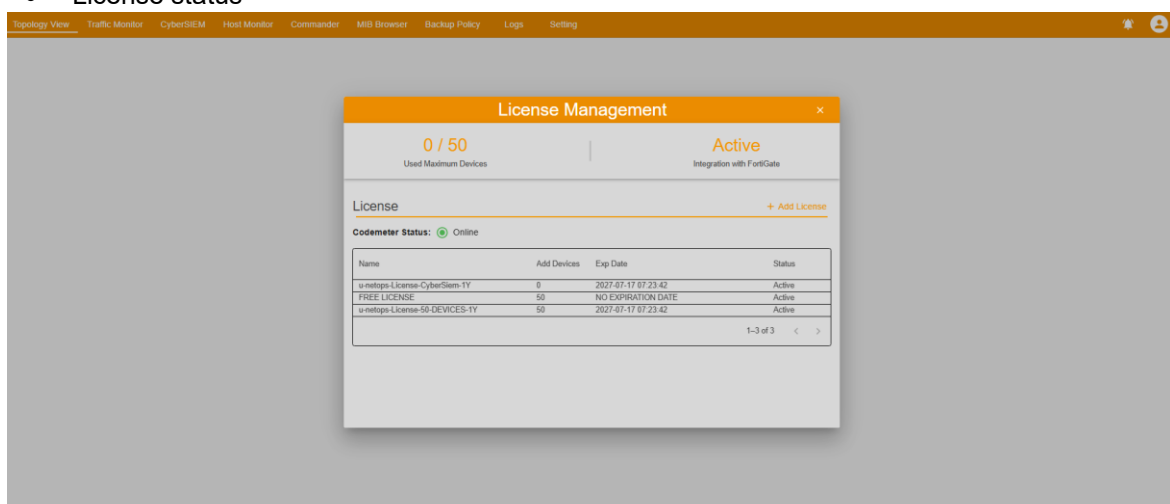


Figure 54: "License Management" dialog

The **+ Add License** button is used to activate a new license.

When adding a license, the wizard prompts you to select an activation mode:

- **Online:** Select this option if the computer has internet access. Clicking Next opens the CodeMeter License Central WebDepot in a web browser.

- **Offline:** Select this option if the target computer does not have internet access. The activation is performed using activation files.

CodeMeter Requirement

u-netops uses **CodeMeter** from WIBU-Systems for license management and activation.

The CodeMeter Runtime is included in the provided installation ZIP package and must be installed before a license can be activated. Without a valid CodeMeter installation, license activation is not possible.

Add License online

Step 1: Select Online Mode

Open the License Management dialog and click + Add License.
Select Online and continue with Next.

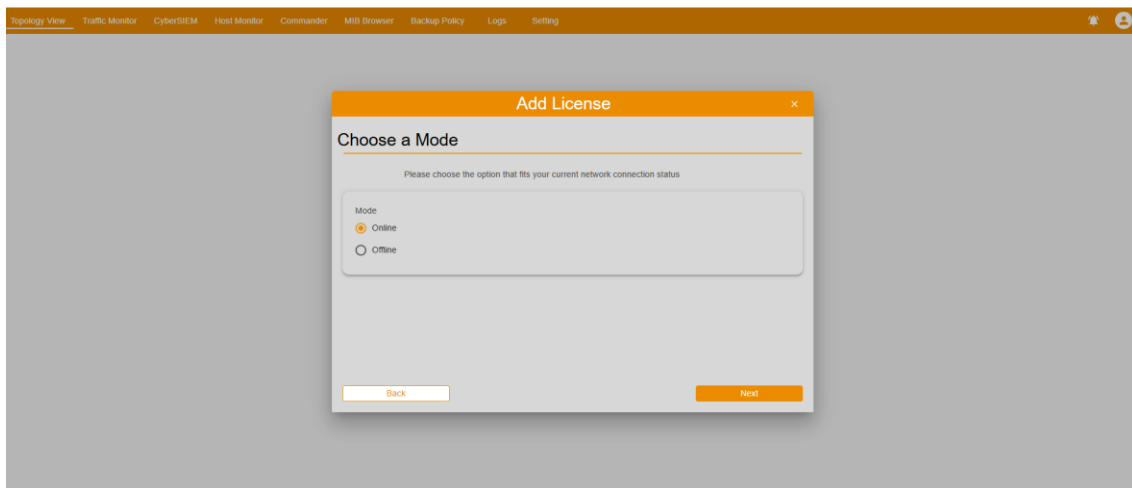
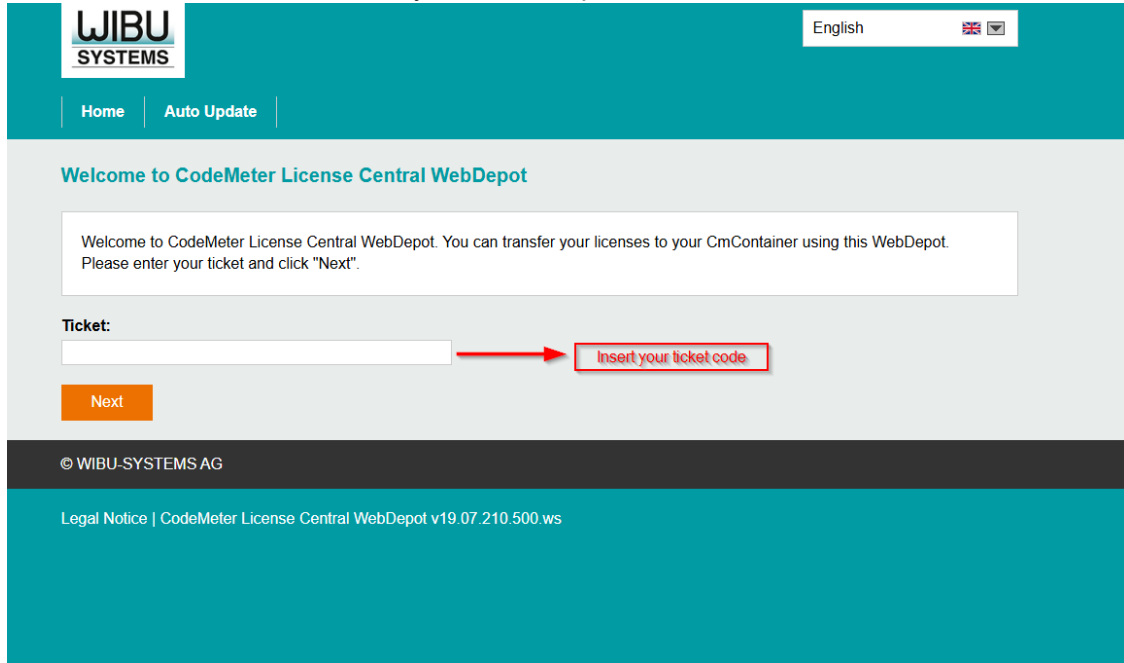


Figure 55: Selecting the activation mode (Online)

Step 2: Enter the Ticket Code

Enter the ticket code received with your software purchase.



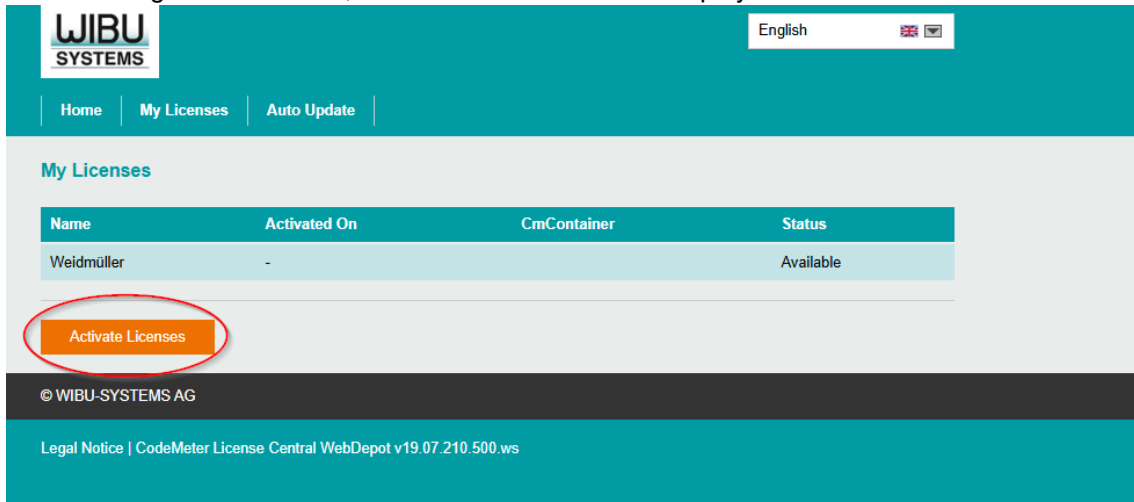
The screenshot shows the WIBU SYSTEMS CodeMeter License Central WebDepot interface. The header includes the WIBU SYSTEMS logo, a language selector set to 'English', and navigation links for 'Home' and 'Auto Update'. The main content area displays a welcome message: 'Welcome to CodeMeter License Central WebDepot. You can transfer your licenses to your CmContainer using this WebDepot. Please enter your ticket and click "Next".' Below this, there is a 'Ticket:' label, a text input field, and a red arrow pointing to a button labeled 'Insert your ticket code'. An orange 'Next' button is also visible. The footer contains the copyright notice '© WIBU-SYSTEMS AG' and a link to the 'Legal Notice | CodeMeter License Central WebDepot v19.07.210.500.ws'.

Figure 56: Insert your ticket code

The ticket code uniquely identifies your purchased license and is required for activation.

Step 3: Activate the License

After entering the ticket code, the available licenses are displayed.



The screenshot shows the 'My Licenses' section of the WIBU SYSTEMS CodeMeter License Central WebDepot interface. The header includes the WIBU SYSTEMS logo, a language selector set to 'English', and navigation links for 'Home', 'My Licenses', and 'Auto Update'. The main content area displays a table with the following data:

Name	Activated On	CmContainer	Status
Weidmüller	-		Available

Below the table, there is an orange button labeled 'Activate Licenses' which is circled in red. The footer contains the copyright notice '© WIBU-SYSTEMS AG' and a link to the 'Legal Notice | CodeMeter License Central WebDepot v19.07.210.500.ws'.

Figure 57: Activate License

Step 4: Available License Types

Available Licenses - Select the binding for Your Licenses

You can bind your licenses either to a computer (**CmActLicense**) or to a dongle (**CmDongle**).

- When binding to a computer, the licenses are transferred to that machine. The licenses are associated with some properties of this computer.
- When binding to a CmDongle, the licenses are fully transferred into this dongle. This allows you to use these licenses on different computers.



I want my licenses on one computer (**CmActLicense**).
Firm Code: 6000276 | CmContainer: Weidmüller Interface GmbH & Co.KG (200A)



I want my licenses on one computer (**CmActLicense**).
Firm Code: 6000276 | CmContainer: Weidmüller Interface GmbH & Co.KG (VM) (200C)

Figure 58: Available license types

Parameter	Meaning
CMContainer: Weidmueller Interface GmbH & Co. KG (200A)	License for a physical PC running Windows directly on bare-metal hardware.
CMContainer: Weidmueller Interface GmbH & Co. KG (VM) (200C)	License for a virtual machine (VM) running Windows within a virtualization environment.

Table 13: Available license types

Select the appropriate license type depending on the deployment environment of u-netops.

Step 5: Confirm Activation

Select the desired license and click Activate Selected Licenses Now.

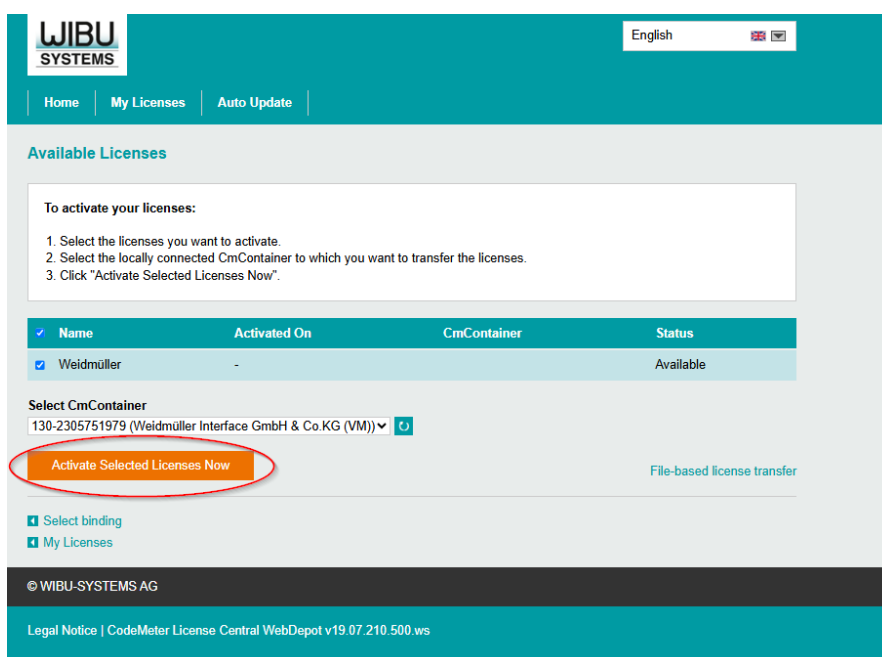


Figure 59: Activate Selected Licenses Now

The license is downloaded and transferred automatically to the local CodeMeter container.

Step 6: License Transfer Completed

After successful activation, the license appears in the License Management overview.

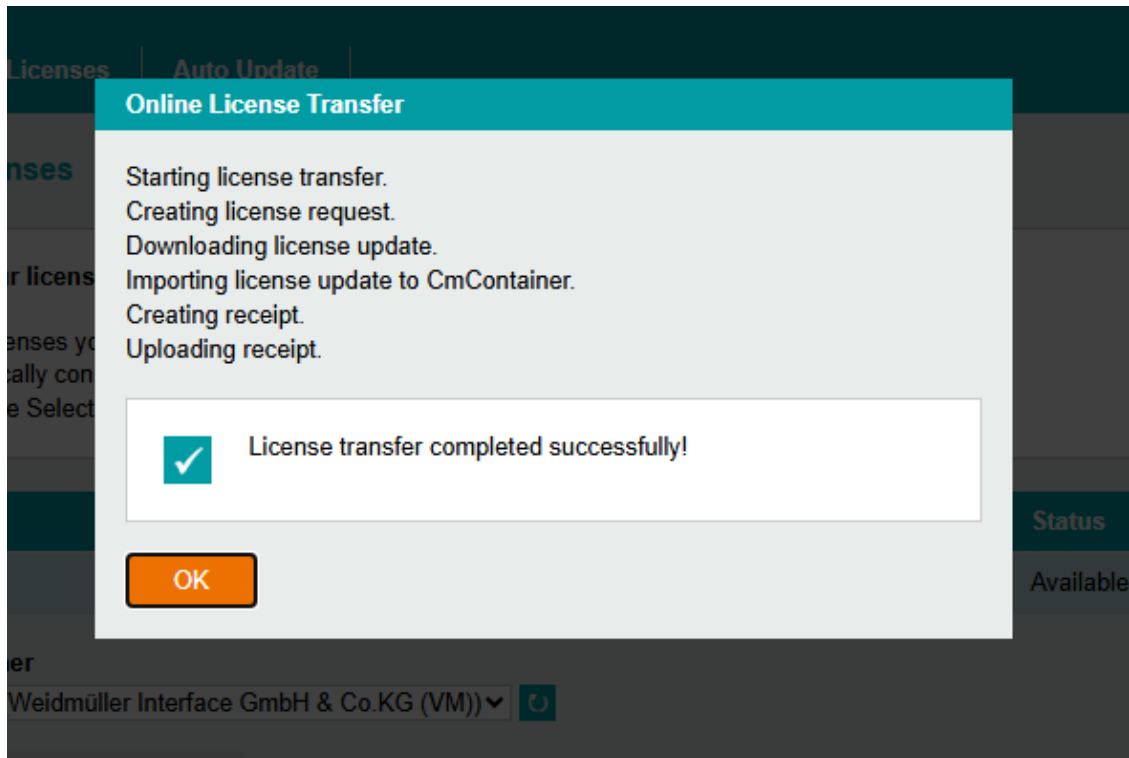


Figure 60: Online License Transfer

The license can now be used immediately.

Add License offline

Offline activation is intended for systems without internet connectivity.

The offline activation process consists of three stages:

1. Create an activation request.
2. Generate the license on an internet-enabled computer.
3. Import the license and upload the receipt.

Step 1: Select Offline Mode

Open the **License Management** dialog and select **Offline**.

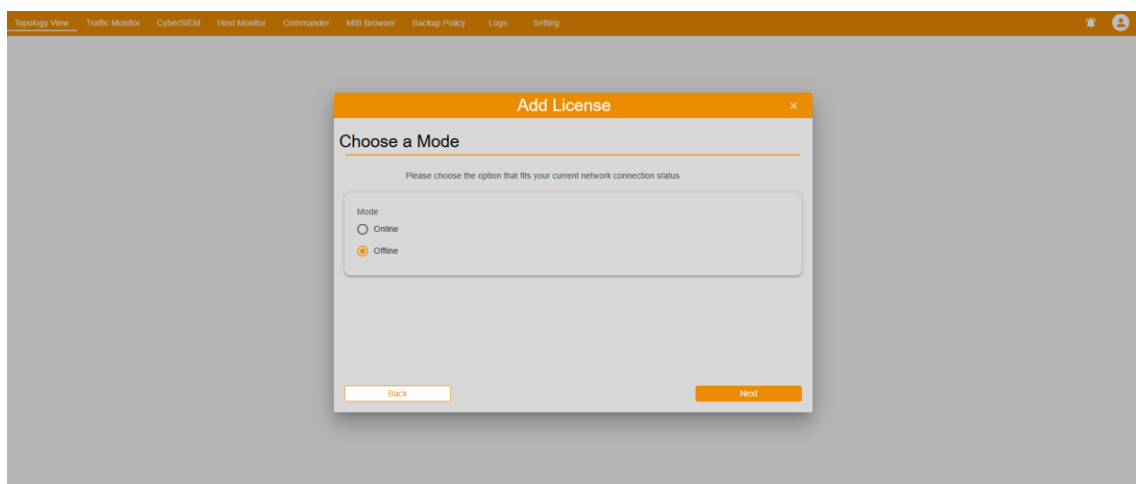


Figure 61: Adding a license: choosing the mode (offline)

Step 2: Create and Download the License Request File

Generate and save the activation request file.

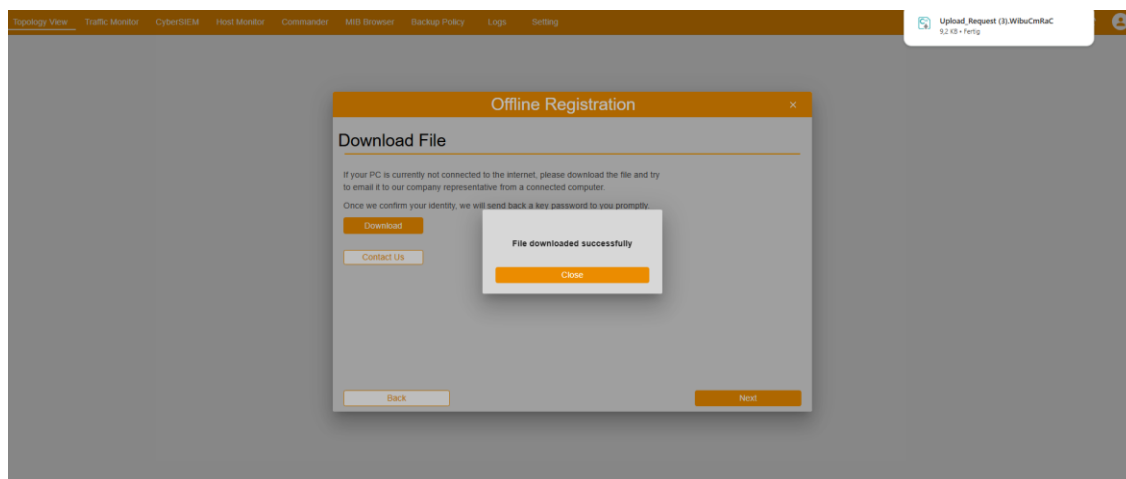


Figure 62: Offline Registration

Copy this file to a computer with internet access.

Step 3: Open the CodeMeter WebDepot

On the internet-enabled computer, open the CodeMeter WebDepot (<https://lc.codemeter.com/31868/depot/index.php>), enter the ticket code and select the license type. These steps are identical to online activation, steps 2 to 4 (Figures 56–58, Table 13).

Step 4: Generate the License File

Click File-based license transfer

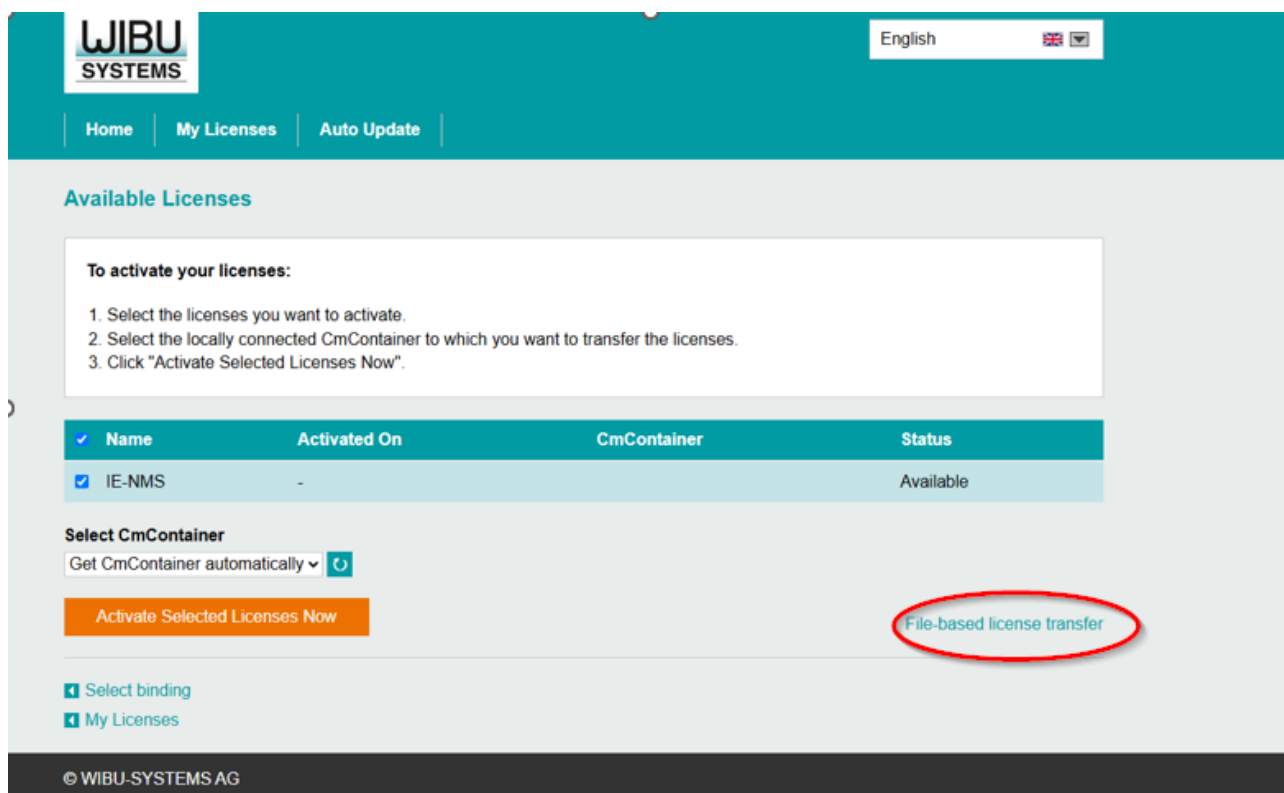


Figure 63: File-based license transfer

Upload the activation request file previously generated by u-netops.

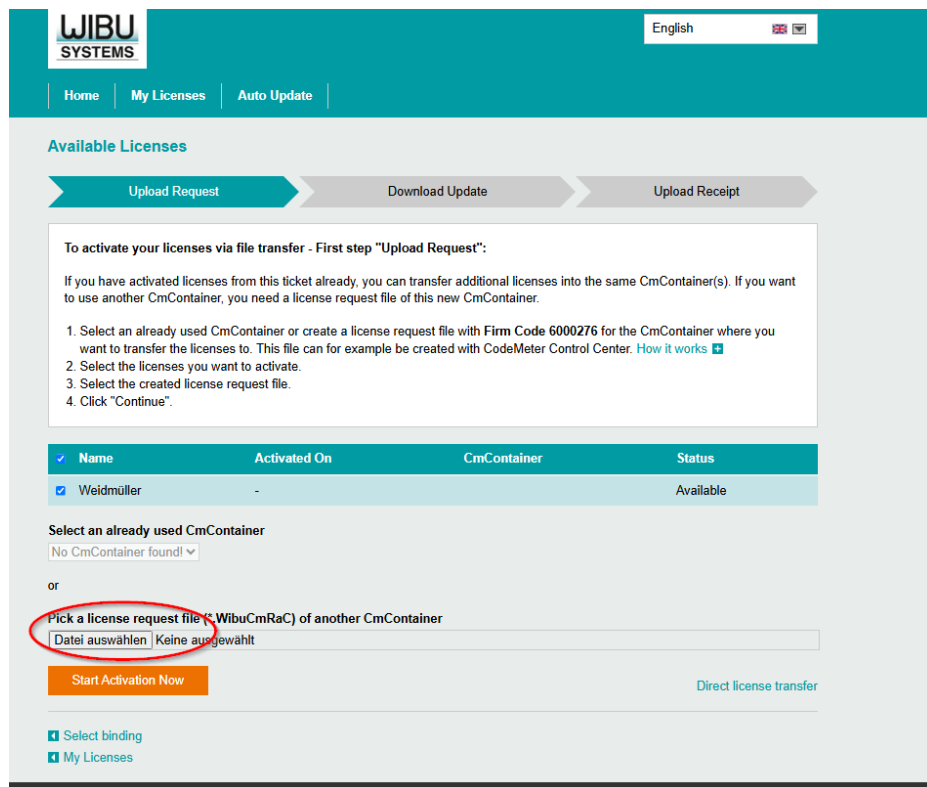


Figure 64: Upload Activation Request File

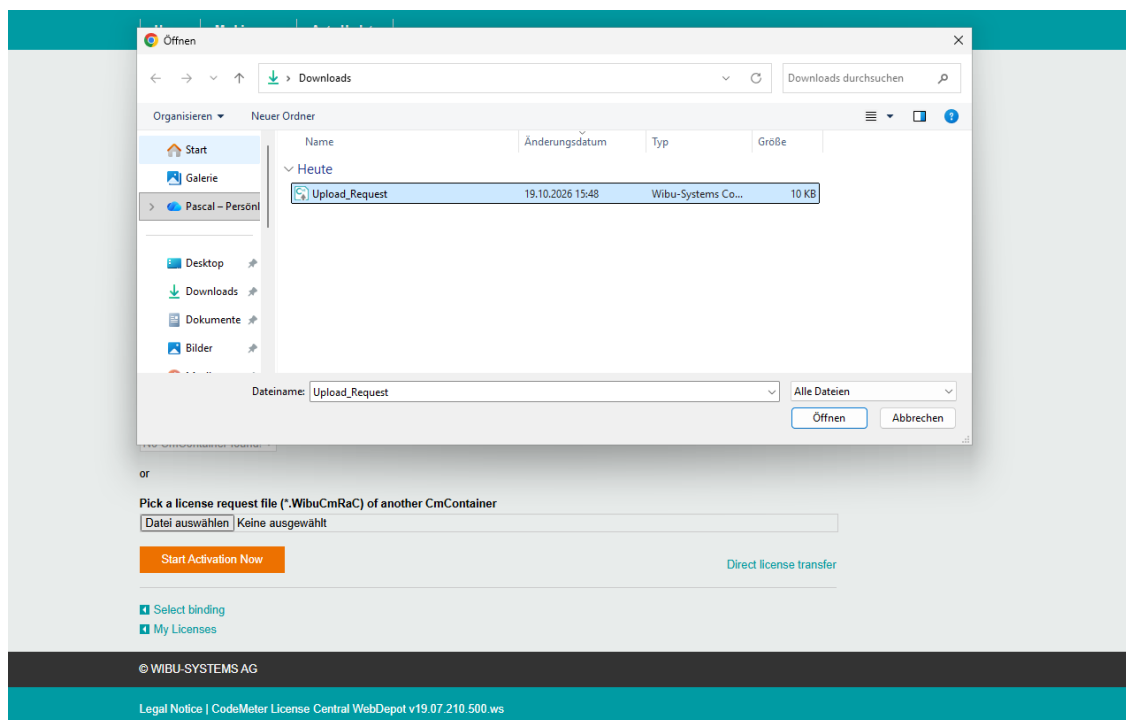


Figure 65: Insert the Download file from u-netops

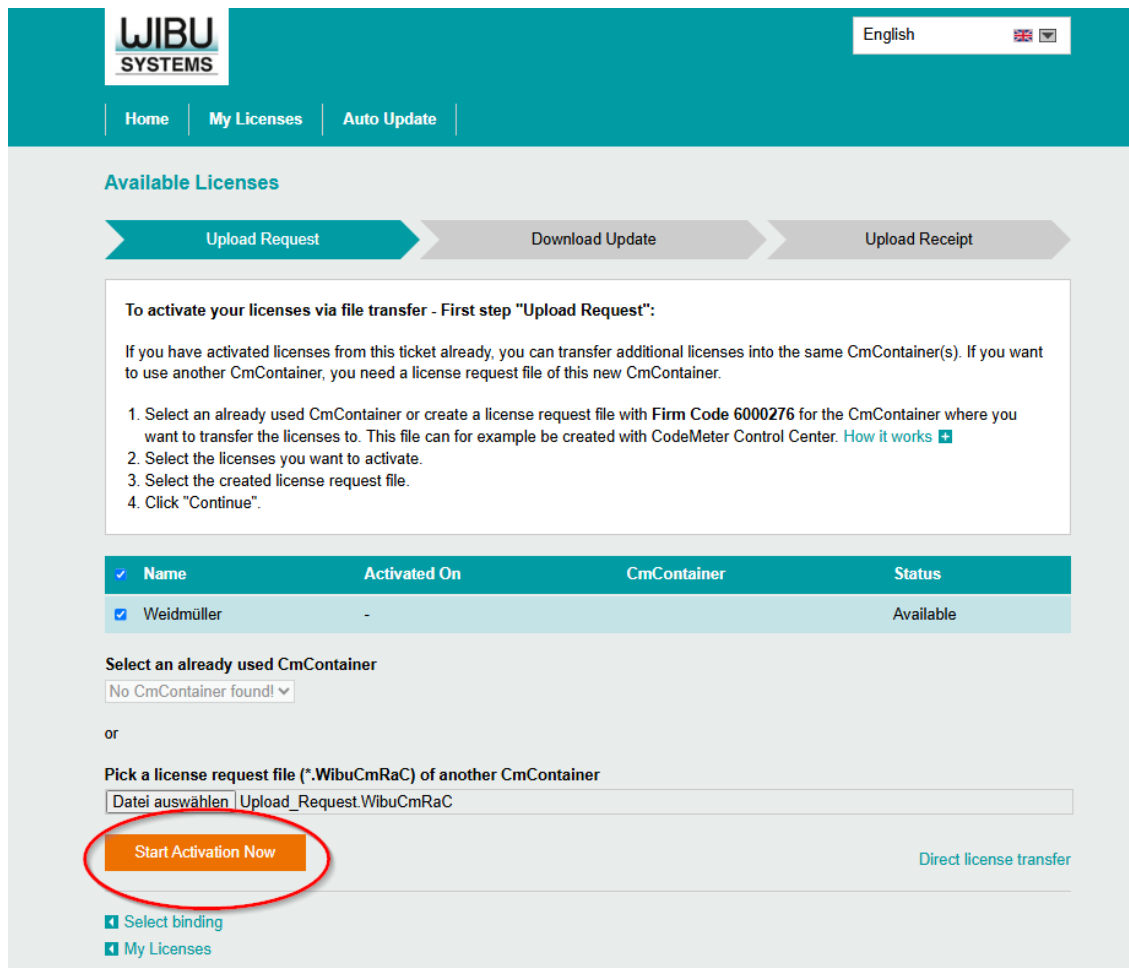


Figure 66: Activate Selected Licenses Now

The WebDepot generates a license update file that contains the activated license.

Step 5: Download the Generated License

Download the generated license file.

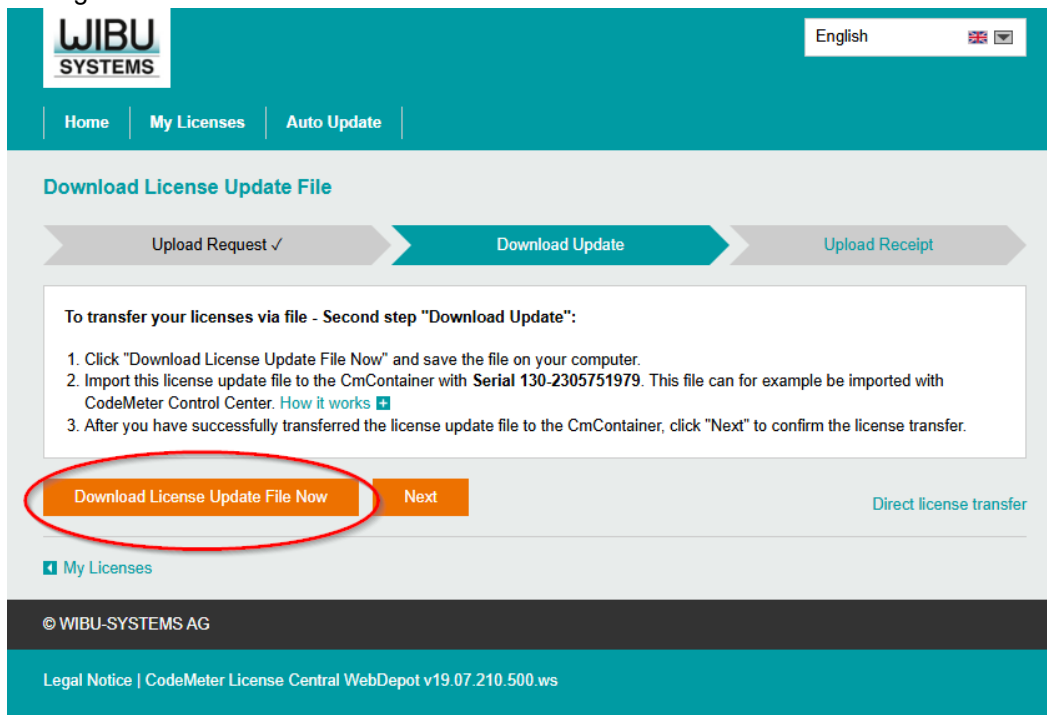


Figure 67: Download the generated license to import it into CodeMeter

Step 6: Import the License into CodeMeter

Return to the target system and import the downloaded license file using CodeMeter.

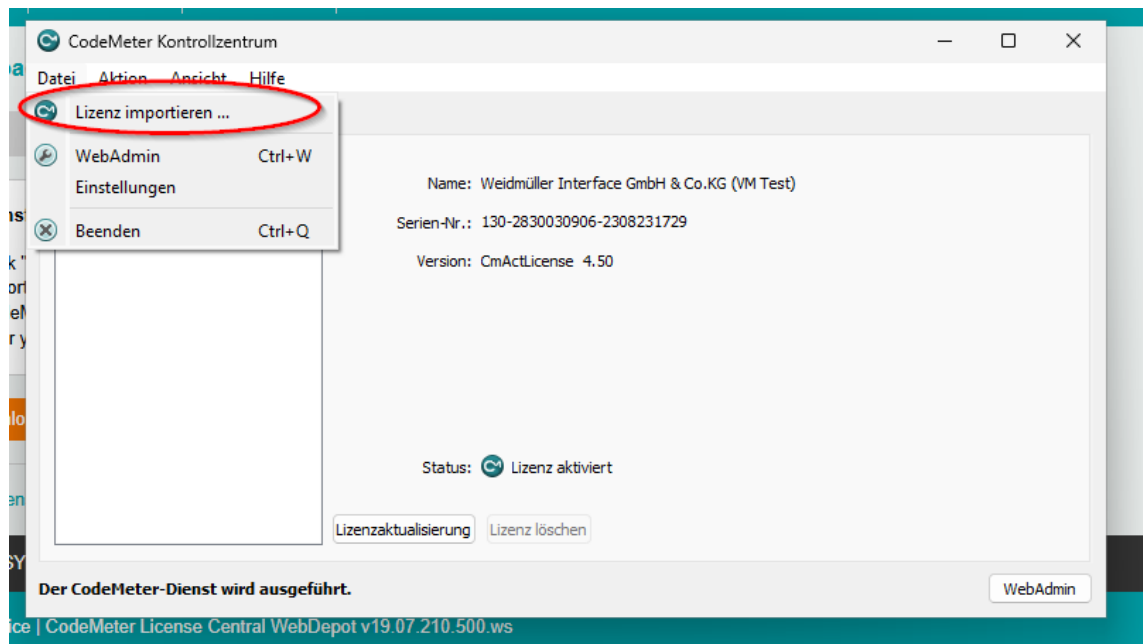


Figure 68: CodeMeter license import

Confirm the import process.

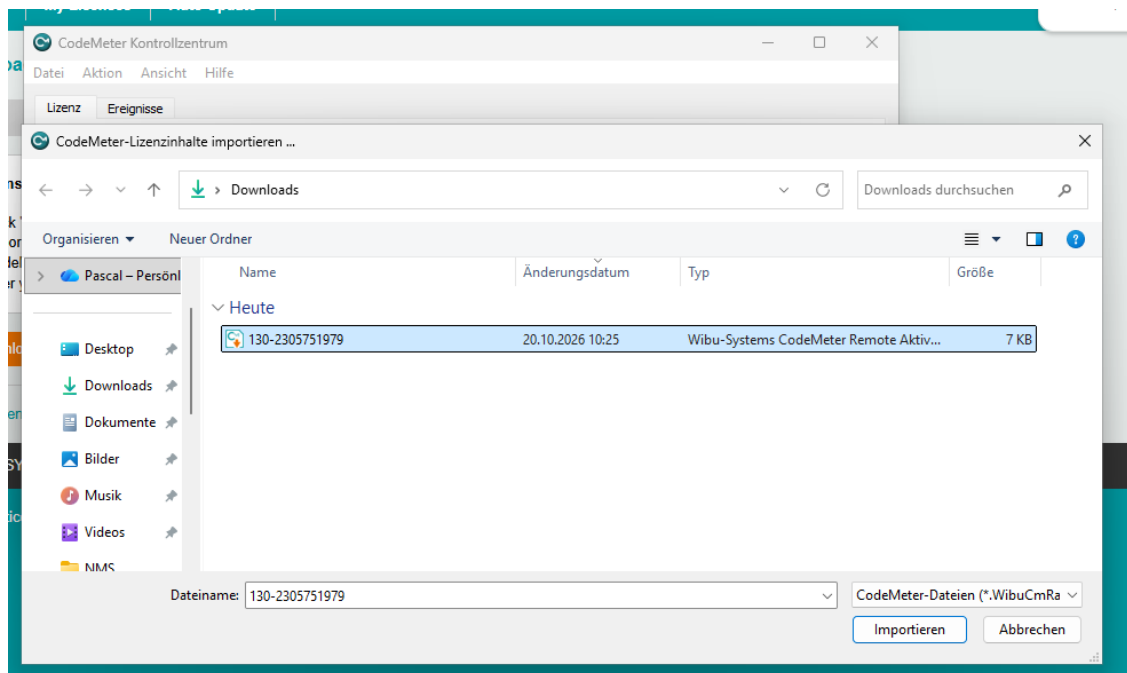


Figure 69: Import generated license

The license is now available locally.

Step 7: Create a Receipt

To complete the activation process, a receipt must be generated and uploaded.

This step informs the License Central server that the activation has been successfully completed.

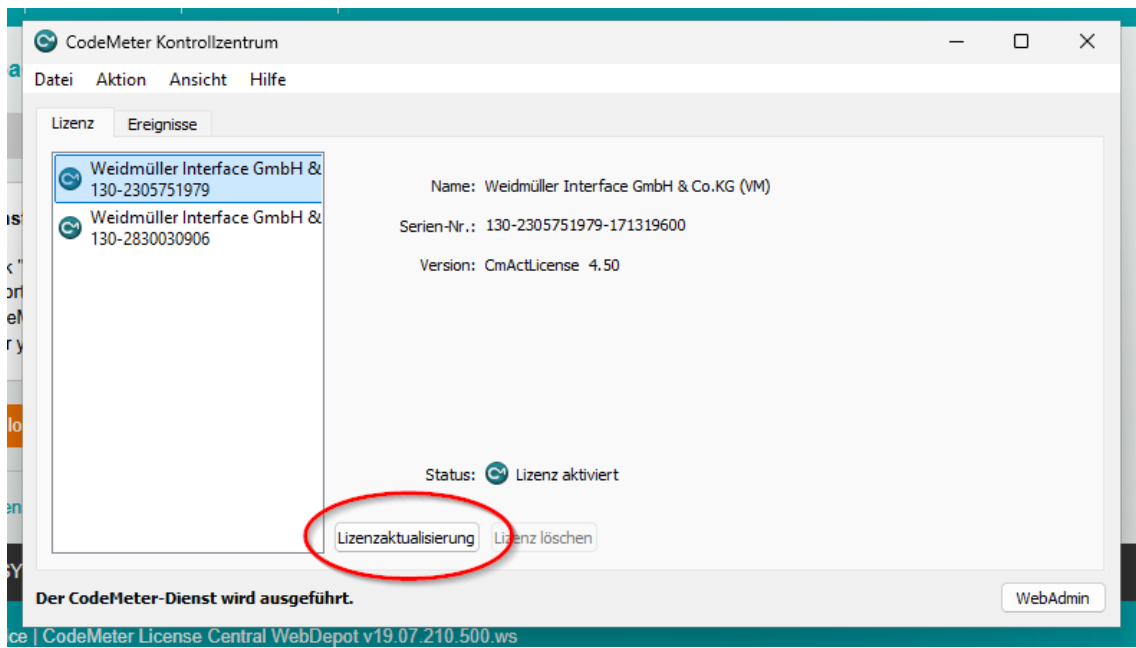


Figure 70: License Update

Click **Generate Receipt**.

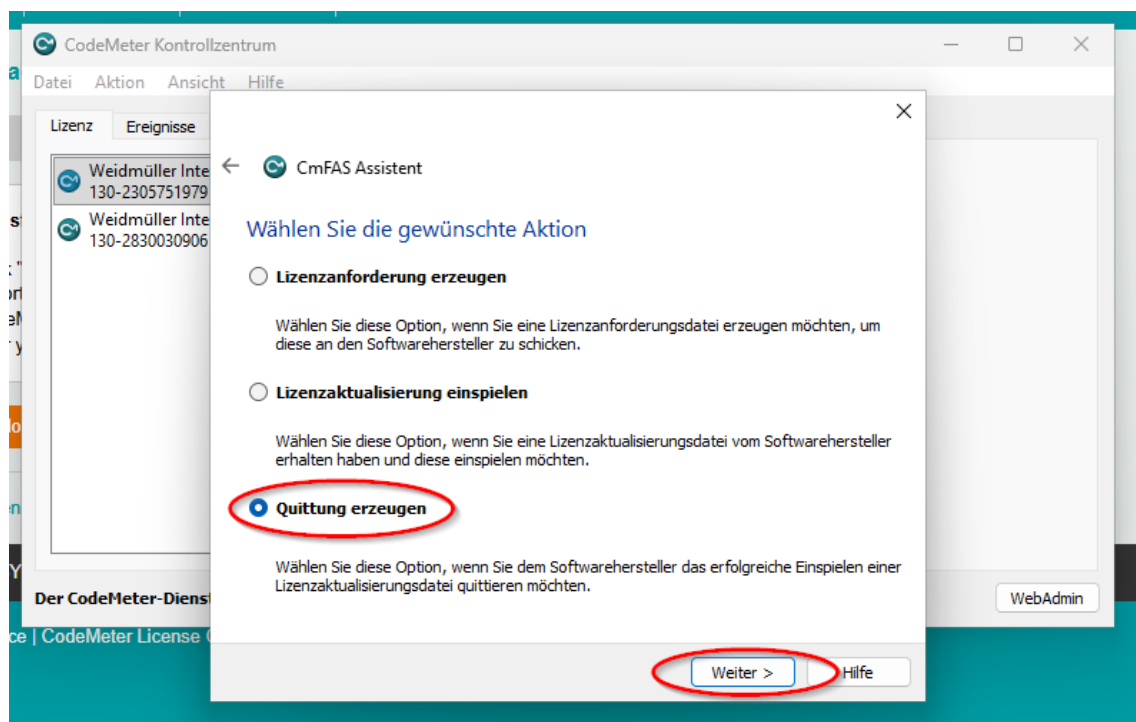


Figure 71: Generate a receipt

Save the generated receipt file.

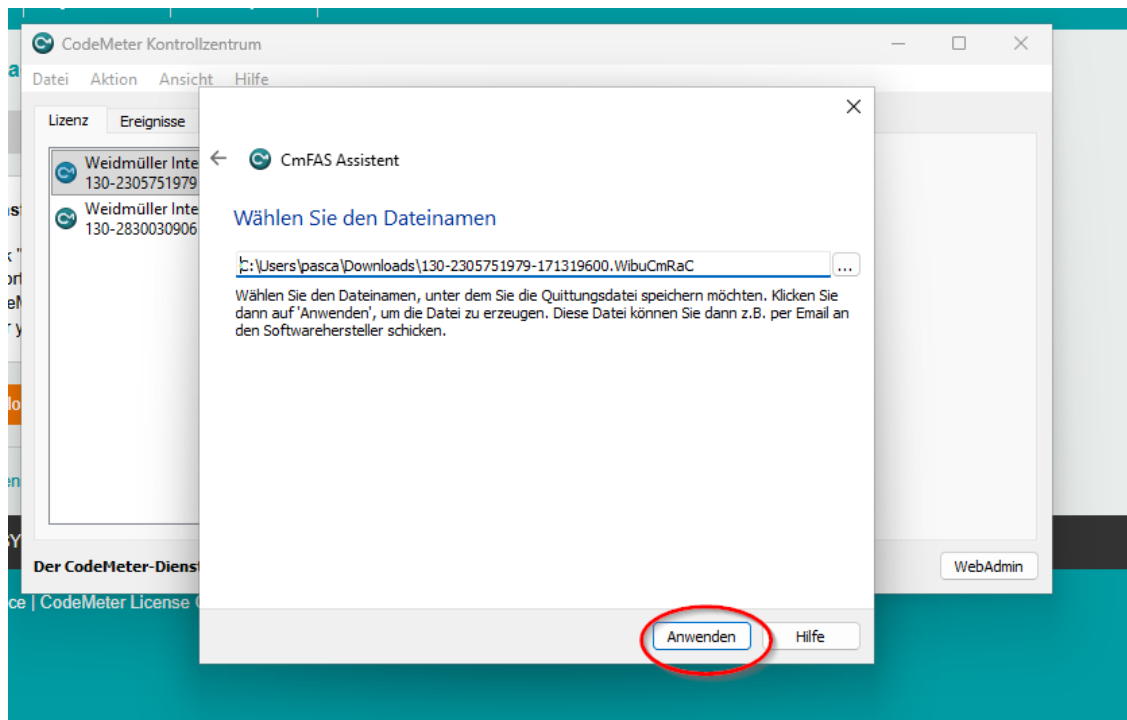


Figure 72: Save receipt

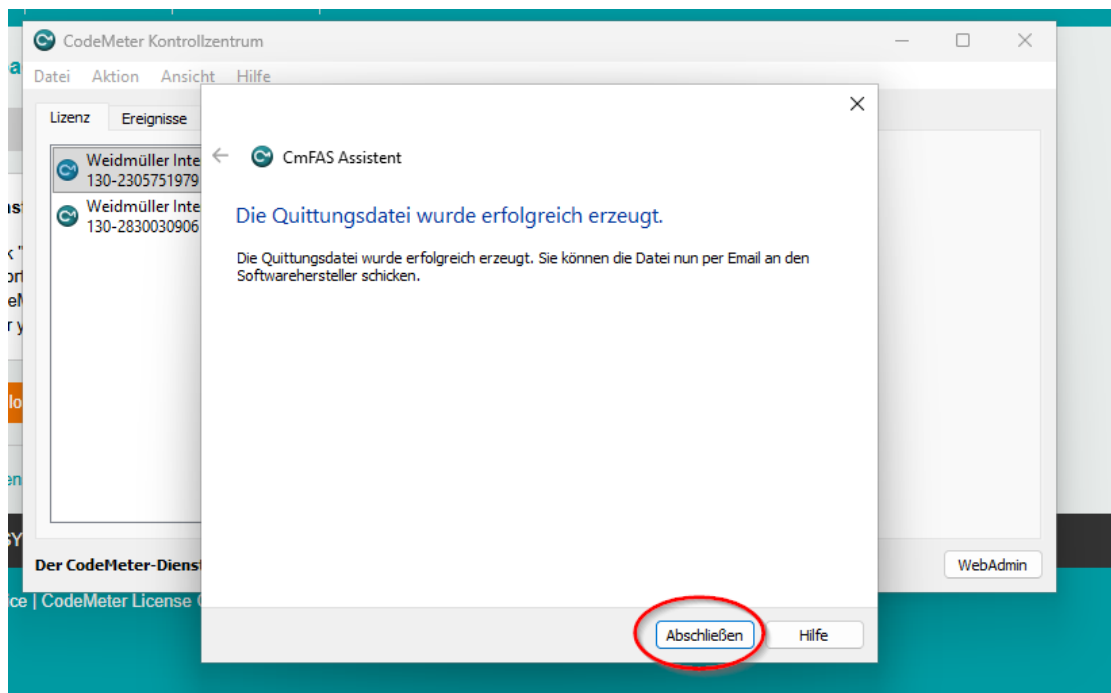


Figure 73: Finalize the receipt

Step 8: Finalize the Activation

Upload the receipt file to the CodeMeter WebDepot.

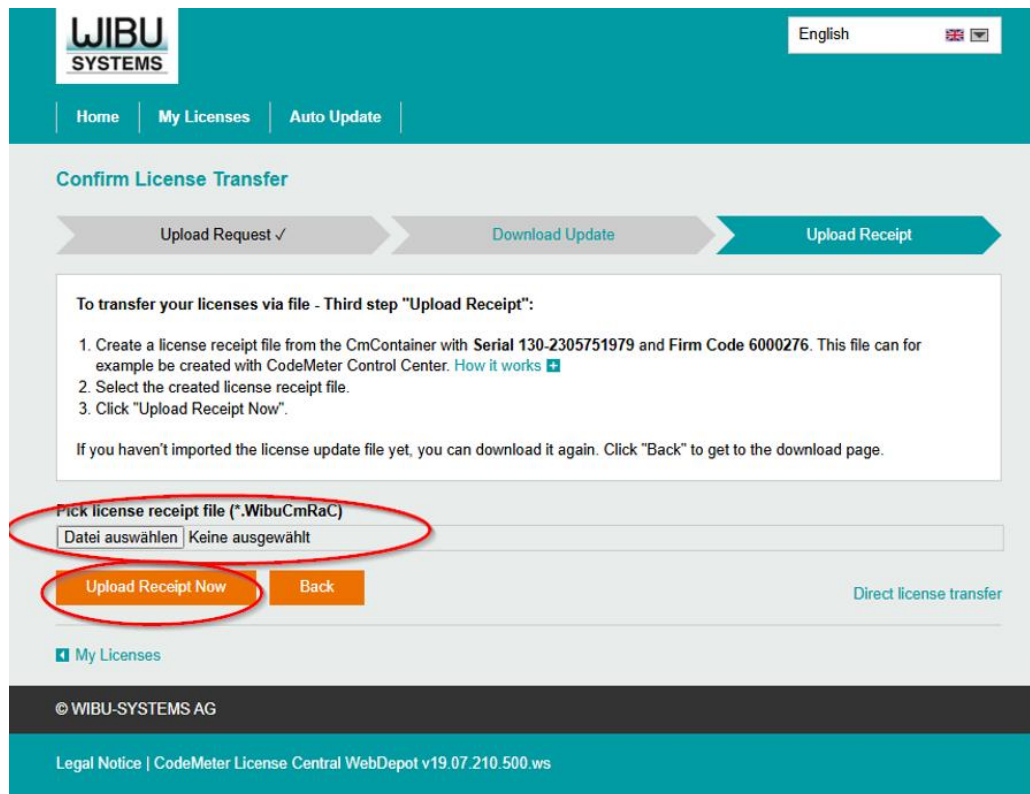


Figure 74: Upload Receipt in Wibu

After successful upload, the activation process is completed.

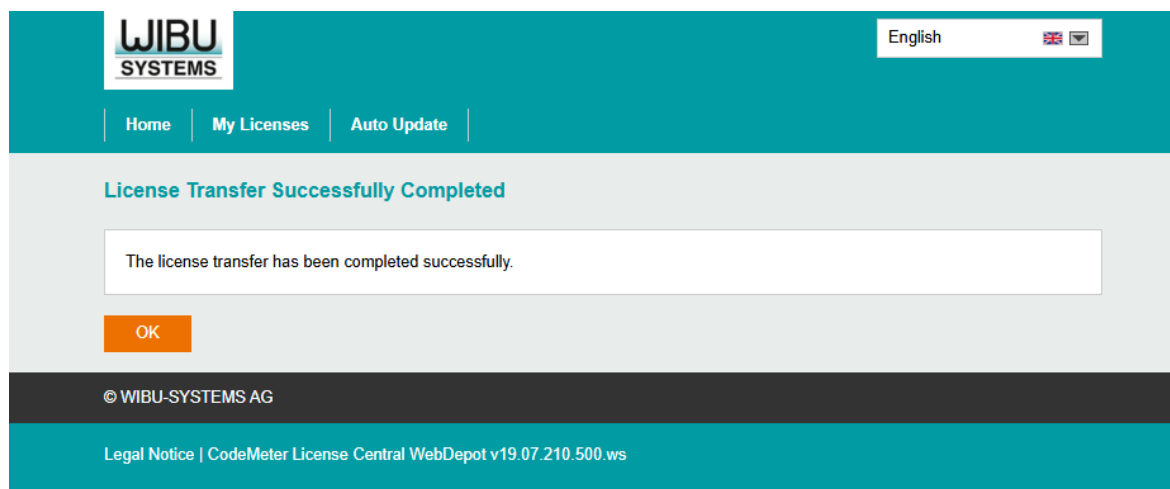


Figure 75: Successful Licensing Completed



NOTE: The receipt upload is mandatory. If the receipt is not uploaded, future license updates, transfers, or returns may not be possible because the License Central database is not synchronized with the activation state of the target system.

12.3 Model

Model Management manages the known device models. Each model is assigned to a model name and a device image via its SNMP system OID (e.g. 1.3.6.1.4.1.38187.4.88). Based on this assignment, u-netops recognises devices and displays them with the matching image.

- Discovered third-party SNMP devices get a default icon. Click the image of a model to upload a different image stored on the PC.

- New model: enter the name in the field **Model Name** and click **+ Add**. Models can be added before a search so that the devices are displayed with the right image directly.
- Search via the search field; select the search column via the selection field (e.g. **OID**).
- Pencil icon: edit the model; bin icon: delete the model.

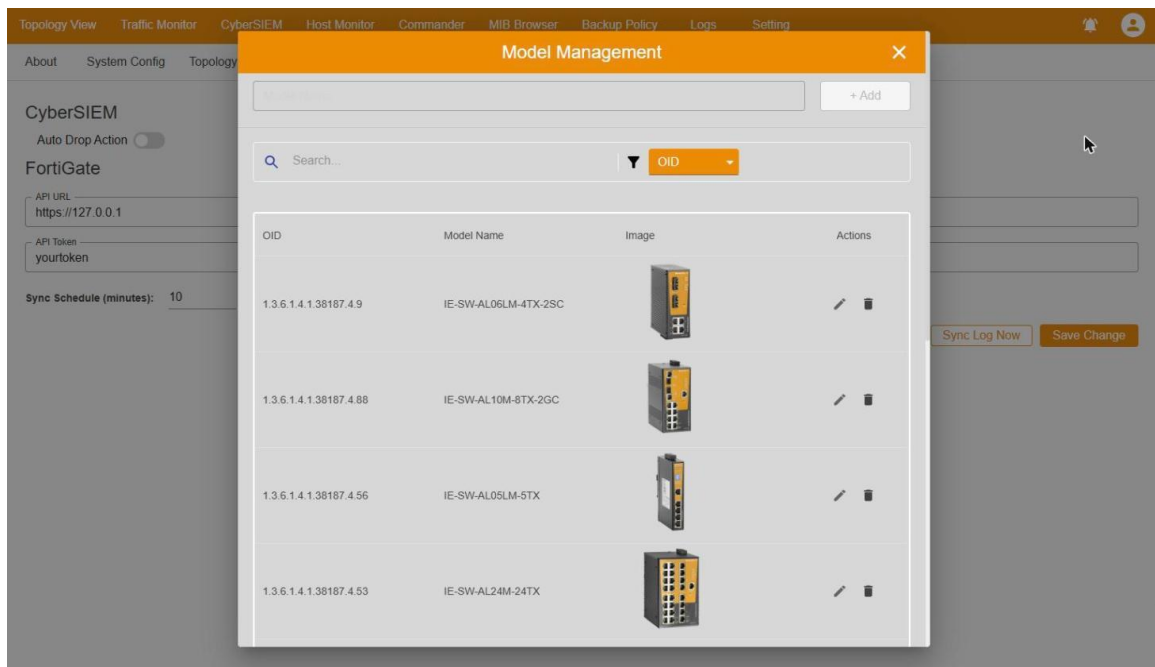


Figure 76: "Model Management" dialog

12.4 NTP Client

Time synchronisation of the u-netops server. Enable **Enable NTP Client**, enter the NTP server under **Server Host** and save with **Save**. **Last synced at** shows the last successful synchronisation.

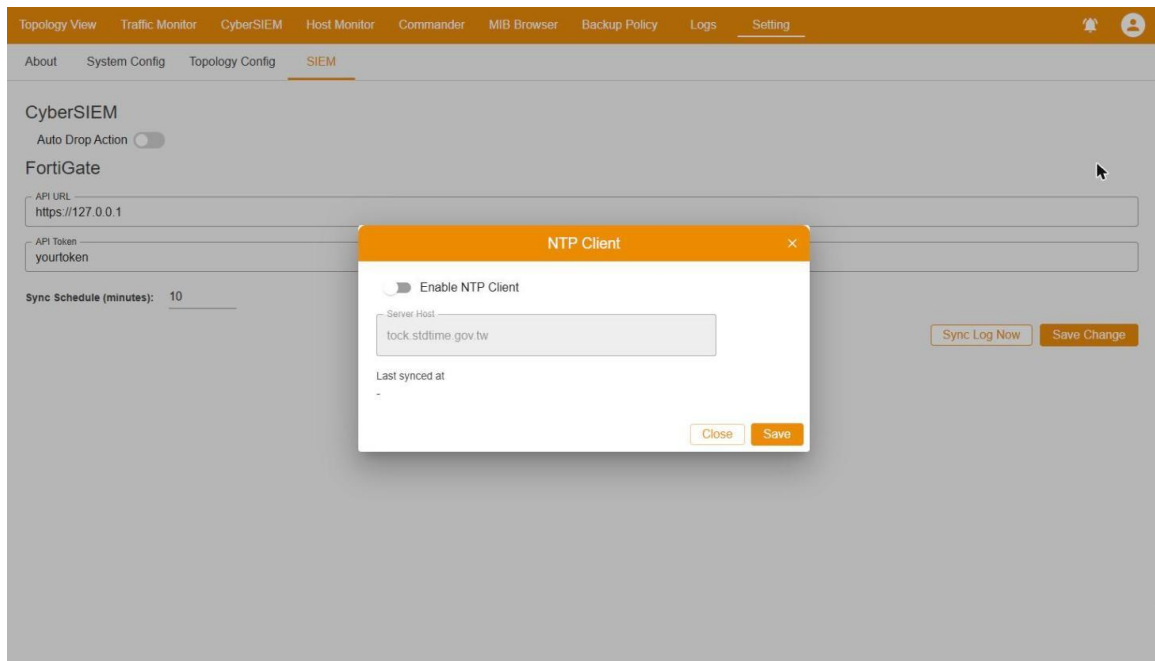


Figure 77: "NTP Client" dialog

12.5 SMTP Setup

Sending e-mails is required for alarm messages (section 10.2 Event types and e-mail alerts).

- Tab **SMTP Server**, option **SMTP Server**: enter **SMTP Server**, **Port**, **User Name** and **Password** and save with **+ Add**.
- Option **Gmail**: only enter **User Name** and **Password** of the Gmail account.
- Tab **Receiver**: enter recipients with **Name** and **Email** and add them with **Add**. The table lists all recipients; they can be edited or removed via **Actions**.

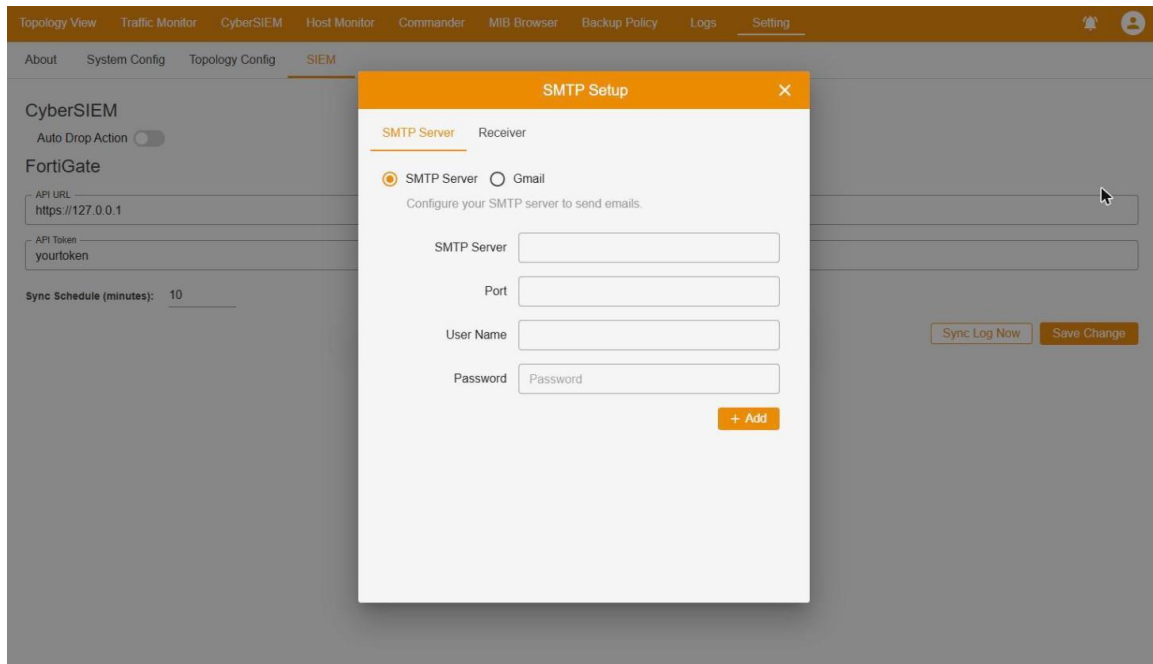


Figure 78: SMTP Setup, “SMTP Server” tab

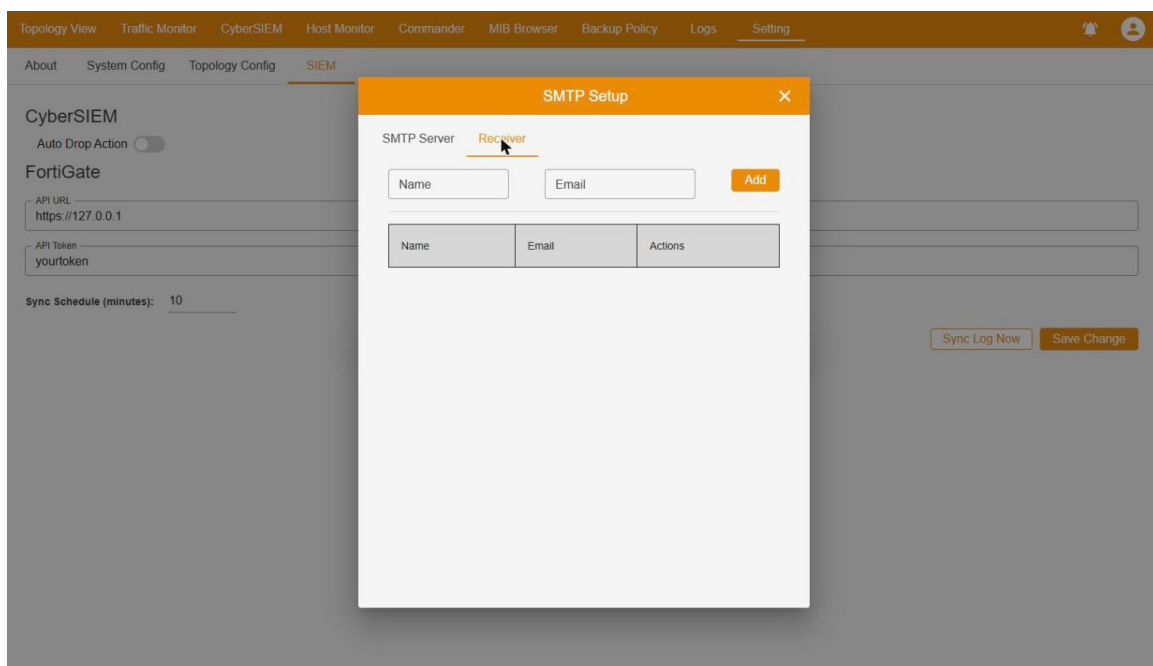


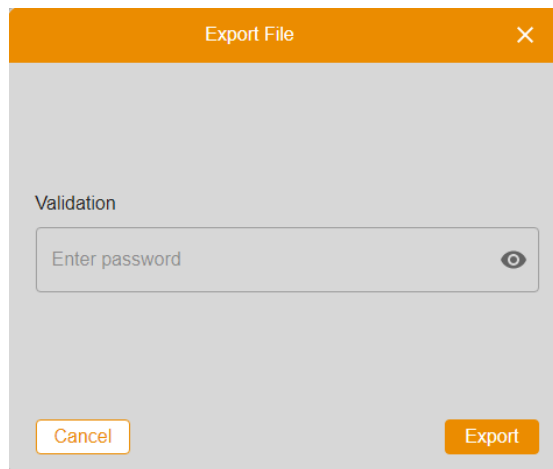
Figure 79: SMTP Setup, “Receiver” tab

12.6 Export File and Import File

Export File saves the entire u-netops configuration on the connected PC; **Import File** loads a complete configuration from a previously exported file. Both actions require the password to be entered.

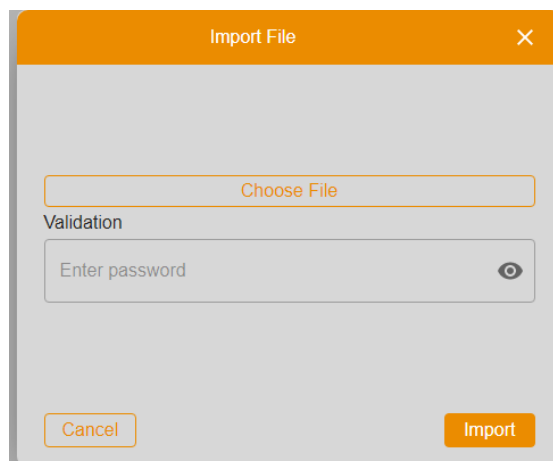
Difference from exporting/importing projects in the Topology View:

- **Export/Import Project (Topology View):** JSON file containing only the network topology of one project.
- **Export/Import File (user menu):** ZIP file containing all project files and system settings (excluding account information and the log of events). This option is mainly intended for system recovery or for migration to another server.



The "Export File" dialog box has an orange header bar with the title "Export File" and a close button (X). The main area is light gray. It contains a "Validation" section with a text input field labeled "Enter password" and a toggle icon (an eye) to its right. At the bottom, there are two buttons: "Cancel" on the left and "Export" on the right.

Figure 80: "Export File" dialog



The "Import File" dialog box has an orange header bar with the title "Import File" and a close button (X). The main area is light gray. It contains a "Choose File" button at the top. Below it is a "Validation" section with a text input field labeled "Enter password" and a toggle icon (an eye) to its right. At the bottom, there are two buttons: "Cancel" on the left and "Import" on the right.

Figure 81: "Import File" dialog

12.7 Logout

Logout ends the session and leaves the web management of u-netops.

13. Typical Workflows

13.1 Initial setup

1. User menu → **License**: activate the license (online or offline, see section 12.2). The number of licensed devices limits how many devices can be added to projects.
2. User menu → **NTP Client**: enable time synchronisation.
3. **Setting** → **System Config**: adapt SNMP communities and version to the switches.
4. User menu → **SMTP Setup**: enter mail server and recipients.
5. **Logs** → **System Log** → gear icon: enable e-mail alerts for important events (e.g. device_offline).
6. **Backup Policy** → **TFTP Setting**: enter the TFTP server.
7. **Topology View** → **Start Project** → **New Project**: search the network and create the project.
8. User menu → **Account**: create further users with the appropriate role.

13.2 Adding a new switch to an existing project

1. **Topology View** → **Add Project** or **Start Project**, select the project and click **Edit**.
2. In the step **Device**, search for the IP of the new switch and add it with **Add >**.
3. Continue to the preview with **Next** and complete with **Finish**.
4. Alternatively, use **+ Add Device** in Edit mode and save with **Save File**.

13.3 Updating the firmware on several switches

1. Provide the firmware file on the TFTP server.
2. **Backup Policy**: create an up-to-date **Backup** for the devices concerned.
3. **Commander**: select the devices, open **Apply settings**, enter the TFTP server IP and the firmware file name, **Confirm**.
4. Select **Actions** → **Firmware Upgrade**, check the device list, **Confirm**.
5. Follow the progress in **Current status**; then reboot the devices (**Reboot**) and check the version in the **Version** column.

13.4 Narrowing down the cause of a fault

1. **Topology View**: identify offline devices by their status colour; check **Disconnection Event** (bell).
2. Right-click the device → **Open Ping** or **SNMP Test**.
3. Search **Logs** → **System Log** for the device (search column **Target**).
4. If several addresses are affected, start the **Host Monitor** for the range and evaluate the **Message** view.

14. Troubleshooting

Message / symptom	Cause and remedy
"SMTP settings are not configured"	No mail server configured. Fill in user menu → SMTP Setup .
"Backup and Compare require a configured TFTP server." / "Failed to fetch TFTP server status"	TFTP server missing or not reachable (display 0.0.0.0:69). Check Backup Policy → TFTP Setting .
"Some devices have missing or empty information" (Commander)	TFTP server or file name is missing for at least one selected device. Complete it via Apply settings or the pencil icon.
"Commander backup failed with result code 3"	Backup via TFTP failed. Check the TFTP server, its reachability and write permissions.
"Address is empty. Please enter a valid IP address." (MIB Browser)	Enter an IP address in the field Address before the query.
"Get failed" (MIB Browser)	The device does not respond. Check address, community and SNMP version under Advanced Properties .
Port Information remains empty	The device is offline or cannot be reached via SNMP. Check with SNMP Test .
Devices or links are not discovered	Check IP connectivity, SNMP settings (section 11.2 System Config) and LLDP on the switches; disable PROFINET on Conformance Class B devices (section 4.3).
Traffic Monitor shows no data	Enable traffic recording (Setting → About → RECORD TRAFFIC ENABLE) and select the device in the tree.
Browser warns "connection is not private"	Self-signed certificate of u-netops. Click Advanced → Proceed (section 2.3).
Next disabled in the project wizard	No Project Name has been entered yet.

Table 14: Troubleshooting

Appendix A – System Log Event Types

Default severities according to **System Log Settings**. An e-mail alert can be enabled for each type. For the “_fail” variants, the severity is given in brackets.

Event type	Meaning	Severity
device_online	Device is online	Normal
device_offline	Device is offline	High
edge_disconnect	Link disconnected	High
edge_reconnect	Link restored	Normal
device_snmp_trap	SNMP trap received	Normal
device_syslog_message	Syslog message received	Normal
device_traffic_anomaly	Abnormal traffic	High
user_account_operate (_fail)	User account edited (failed)	Low (High)
user_auth_operate (_fail)	Login (failed)	Low (High)
user_device_control (_fail)	Device control, e.g. reboot (failed)	Low (High)
user_system_config (_fail)	System setting changed (failed)	Low (High)
user_custom_config (_fail)	Custom setting changed (failed)	Low (High)
user_group_config (_fail)	Groups changed (failed)	Low (High)
user_device_operate (_fail)	Device management (failed)	Low (High)
user_topology_operate (_fail)	Topology edited (failed)	Low (High)
user_mib_file_operate (_fail)	MIB file edited (failed)	Low (High)
user_license_operate (_fail)	Licence edited (failed)	Low (High)
user_edit_traffic_operate (_fail)	Traffic settings edited (failed)	Low (High)
user_edit_host_monitor (_fail)	Host Monitor edited (failed)	Low (High)
user_check_notification	Notification read	Normal
edge_check_notification	Link notification read	Normal
user_forget_password	Password forgotten	Normal

Table 15: System Log Event Types

Appendix B – Glossary

Term	Explanation
Baseline	Reference configuration for the automatic comparison (Auto Compare).
CodeMeter	Licence management system by Wibu-Systems used by u-netops for licensing.
Community	Access password for SNMP v1/v2c (Read = read access, Write = write access).
Edge	Connection between two devices in the topology (cable between two ports).
ICMP	Internet Control Message Protocol; used by ping to check whether a device is reachable (Host Monitor).
LLDP	Link Layer Discovery Protocol; used by u-netops to detect the links between devices.
MIB	Management Information Base; describes the SNMP objects a device provides.
NMS	Network Management System; software for monitoring and managing network devices centrally.
OID / sysObjectID	Unique SNMP object identifier; the sysObjectID identifies the device model.
Polling	Cyclic query of the device status by u-netops.
SNMP Trap	Message sent by a device on its own initiative to report an event (default port 162).
Syslog	Standard protocol for sending log messages from devices to a central server.

Table 16: Glossary

List of Figures

Figure 1: u-netops server window (Web Starter)	5
Figure 2: Creating the Administrator account	5
Figure 3: Login page	6
Figure 4: Header bar with main menu and opened user menu	7
Figure 5: “Notifications” sidebar	7
Figure 6: Start dialog with the recently used projects	8
Figure 7: Wizard, step 1: Project Settings	9
Figure 8: Wizard, step 2: searching and adding devices	10
Figure 9: Wizard, step 3: Topology Preview	10
Figure 10: Topology View in “Polling” mode	11
Figure 11: Sidebar with Device Tree	12
Figure 12: Group Management dialog	12
Figure 13: Example of a topology with two groups of devices	13
Figure 14: Context menu of a device	13
Figure 15: “Device Information” dialog	14
Figure 16: Topology View in “Edit” mode	14
Figure 17: “New Device” dialog	15
Figure 18: “New Edge” dialog	15
Figure 19: Disconnected link shown in red	16
Figure 20: Disconnection event message	16
Figure 21: Traffic Monitor with expanded device tree	17
Figure 22: Real-time traffic of a port	18
Figure 23: Traffic history	18
Figure 24: Defining traffic alarm thresholds	18
Figure 25: Threshold displayed in the real-time view	19
Figure 26: High-traffic notifications	19
Figure 27: Host Monitor, “Monitor” view	20
Figure 28: Host Monitor, “Add Device” dialog	21
Figure 29: Configuration, “Mode” tab	21
Figure 30: Configuration, “Polling settings” tab	22
Figure 31: Host Monitor, “Message” view	22
Figure 32: Commander device list	23
Figure 33: “Apply settings” dialog	24
Figure 34: “Information” dialog of a single device	25
Figure 35: “Actions” menu with a selected device	26
Figure 36: “Firmware Upgrade” confirmation dialog with warning about missing data	26
Figure 37: Firmware upgrade confirmation, detailed view	27
Figure 38: Reboot confirmation	27
Figure 39: MIB Browser with the node “org” selected	28
Figure 40: “AdvancedProperties” dialog	29
Figure 41: “Edit MIB” dialog	29
Figure 42: “TFTP Server” dialog	30
Figure 43: Auto Backup	31
Figure 44: “Auto Compare” tab	32
Figure 45: Logs → System Log	33
Figure 46: “System Log Settings” dialog	34
Figure 47: Logs → Syslog	34
Figure 48: Setting → About	35
Figure 49: Setting → System Config	36
Figure 50: SNMPv3 parameters in System Config	36
Figure 51: Setting → Topology Config	37
Figure 52: “Account Management” dialog	38
Figure 53: “Create Account” dialog	39
Figure 54: “License Management” dialog	39

Figure 55: Selecting the activation mode (Online)	40
Figure 56: Insert your ticket code	41
Figure 57: Activate License	41
Figure 58: Available license types	42
Figure 59: Activate Selected Licenses Now	42
Figure 60: Online License Transfer	43
Figure 61: Adding a license: choosing the mode (offline)	43
Figure 62: Offline Registration	44
Figure 66: File-based license transfer	44
Figure 67: Upload Activation Request File	45
Figure 68: Insert the Download file from u-netops	45
Figure 69: Activate Selected Licenses Now	46
Figure 70: Download the generated license to import it into CodeMeter	46
Figure 71: CodeMeter license import	47
Figure 72: Import generated license	47
Figure 73: License Update	48
Figure 74: Generate a receipt.....	48
Figure 75: Save receipt.....	49
Figure 76: Finalize the receipt	49
Figure 77: Upload Receipt in Wibu	50
Figure 78: Successful Licensing Completed	50
Figure 79: "Model Management" dialog.....	51
Figure 80: "NTP Client" dialog	51
Figure 81: SMTP Setup, "SMTP Server" tab	52
Figure 82: SMTP Setup, "Receiver" tab	52
Figure 83: "Export File" dialog	53
Figure 84: "Import File" dialog	53

List of Tables

Table 1: Functional overview	3
Table 2: Opening or creating a project - Description	8
Table 3: Topology View in “Polling” mode	11
Table 4: Device context menu	13
Table 5: Edit mode	14
Table 6: Host Monitor, “Monitor” view	20
Table 7: Commander device list	24
Table 8: transfer parameters	24
Table 9: Auto Backup	31
Table 10: Logs → System Log	33
Table 11: System Config	35
Table 12: “Account Management” dialog	38
Table 13: Available license types	42
Table 15: Troubleshooting	55
Table 16: System Log Event Types	56
Table 17: Glossary	57