REVISION 015 - 14/07/2025

Meinberg Network Management System

User Guide

TABLE OF CONTENTS

1 Installation

1.1 Installing the Meinberg Network Management System on the server

1.1.1 System requirements

1.1.1.1 Hardware requirements

Server hardware has to comply with the following requirements:

Hardware	Requirements
Processor	8 cores CPU passmark > 10K
Memory	32 GB
Hard disk	250 GB SSD + 1 TB disk for Cassandra database
Network	Throughput: 100 Mbps Latency: < 50 ms

1.1.1.2 Software requirements

The following software is required:

- Operating system: Windows Server 2012 R2 or higher
- Microsoft .NET Framework 4.6.2 or higher

WARNING: Although the use of antivirus software is supported, this will consume resources of the server. As such, it is better not to install such software if the server is in a well-protected environment. If you do install antivirus software, we recommend to:

- Minimize the impact on the resources of the server by excluding the directories *C:\Skyline DataMiner* and the data directory of the database.
- Avoid scheduled virus scans affecting the available resources for the software at certain moments in time.

1.1.2 Running the main installer

1. Log on with the "Administrator" account (not a regular user account with administrative rights).
2. Make sure the Windows setting *Fast startup* is not activated.
3. Download the DataMiner installer to the desktop. You will need a DataMiner Dojo user account in order to access it. If you do not have an account yet, create one first.

4. Double-click `Setup.exe`.
5. Click *Install*.
6. In the *DataMiner* tab, enter the DataMiner ID.

   IMPORTANT: Contact Meinberg for more details about obtaining this ID. The ID will uniquely identify the agent you are installing.

7. Click *Next*.
   The progress of the installation will be displayed. A *cancel* button in the lower right corner allows you to cancel the installation process if necessary.
8. Once the installation is complete, click *Next*.
9. Click *Go to Request.lic* to browse to the file `Request.lic`.
10. Contact Meinberg to receive the license files for the agent, and include the file `Request.lic` in your request.
11. Once you have received the license files, save these somewhere on the computer; however, not in the "Skyline DataMiner" folder.
12. In the *License* tab of the installer, click *browse and upload*, and navigate to the license files.
13. Once all files have been uploaded successfully, click *restart DataMiner*.
14. When the software has successfully restarted, click *Close*.
15. Download and install the correct DataMiner version for your Meinberg Element Manager app version.

1.1.3 Installing the Meinberg Element Manager app package

1. Download the Meinberg Element Manager package from community.dataminer.services and unzip it. This will result in a package with the .dmapp extension.
2. Double-click the Meinberg Element Manager .dmapp package.
3. In the pop-up window, click *Install*. The upgrade progress will be displayed.
4. When the upgrade is ready, click *Finished*.

1.2 Installing the client app on a client computer

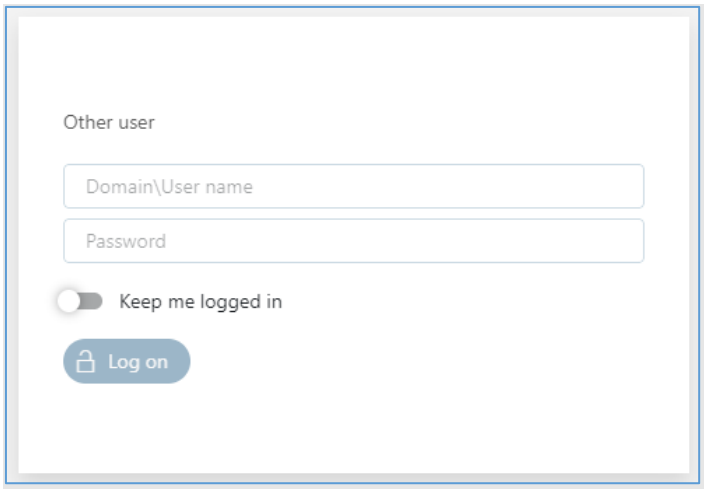
1.2.1 System requirements

The client app for the Meinberg Element Management System is available as a standalone application that can be installed on any computer that meets the following requirements:

- Processor: Min. 4 physical cores and 5000+ PassMark CPU benchmark
- Memory: 8–16 GB DDR4 RAM
- Graphics memory: 512 MB
- Operating system: Windows 10 or Windows 11
- Microsoft .NET Framework 4.7.2 or higher

1.2.2 Downloading and installing the client app

1. Configure the Windows Firewall to allow inbound TCP connections from port 49152 to 65535 for Windows Presentation Foundation Host (PresentationHost.exe).
2. Browse to the server address in any modern browser (Google Chrome, Mozilla Firefox, Microsoft Edge, etc.).
3. On the login screen, specify your username and password and click *Log on*.



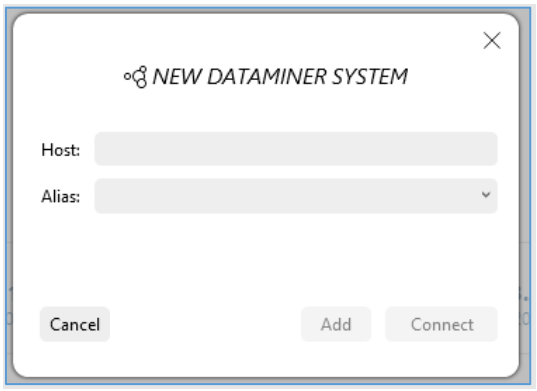
4. In the drop-down box at the top of the window, select *Install Meinberg Network Management System > Desktop installation*.
5. When the application has been downloaded, double-click the .exe file to start the installation.

2 Accessing the system with the client app

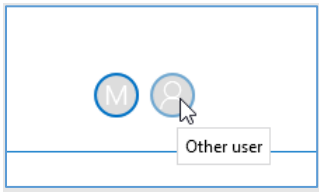
2.1 First-time access

The first time you access the system, you will need to add the host in the start window of the client app:

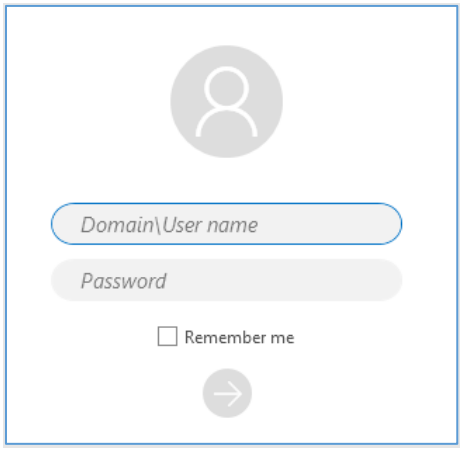
1. Double-click the DataMiner Cube shortcut on your desktop.
2. In the start window, click the + icon.
3. In the pop-up window, specify the hostname or IP of the server in the *Host* box.



4. Click *Connect*.
5. The system will automatically try to log in using your Windows credentials. If you do not have access with those credentials, a login screen will be displayed. In that case, log in as follows:
    a. At the bottom of the screen, click the other user icon.



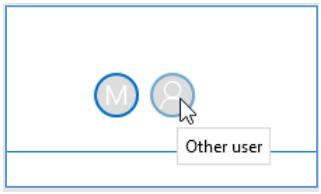
    b. Specify your username and password and click the arrow button.



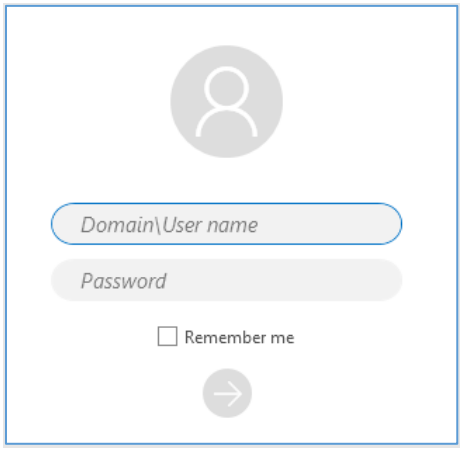
2.2 Subsequent access

If you have already used the client app to access the system on the same computer:

1. Double-click the DataMiner Cube shortcut on your desktop.
2. In the start window, click the tile containing the host name or IP of the server.
3. The system will automatically try to log in using your Windows credentials. If you do not have access with those credentials, a login screen will be displayed. In that case, log in as follows:
    a. At the bottom of the screen, click the other user icon.



    b. Specify your username and password and click the arrow button.



3 Overview of the client user interface

3.1 Terminology

Within this guide, the following terms are frequently used to refer to aspects of the user interface:

- Sidebar: The sidebar on the left or right side of the UI (depending on your user settings – see section 7.1) provides quick access to all components of the Meinberg Network Management System. See section 3.2.
- Card: When you click an item in the Surveyor or when you right-click an alarm in the alarm console (see section 4.3.3) and select *Open* > *Alarm card*, the details of that item or that alarm are displayed in a special window called a card.

  By default, such a "card" is docked within the workspace, but you can undock a card to display it in a separate window. There are several ways you can do so:

  - By dragging an open card out of the workspace.
  - By selecting *Undock* in the hamburger menu in the top left corner of an open card.
  - By holding shift when you click an item in the Surveyor to open the card.
- Alarm: An alarm indicates that an element parameter value exceeds the thresholds that have been set for its normal operation. Several severity levels are possible, indicated as follows:

  Critical alarm

  Major alarm

  Minor alarm

  Warning alarm

  No active alarms – "normal" alarm state

  Masked alarm

  Timeout alarm
- View:
  - Views function as "folders" within the Surveyor, which can for instance contain elements and subviews.
  - Views are preceded by a bar indicating their alarm state in the Surveyor. This alarm state is the most severe alarm state of all items within the view.
- Element: Elements represent devices managed by the Meinberg Network Management System.

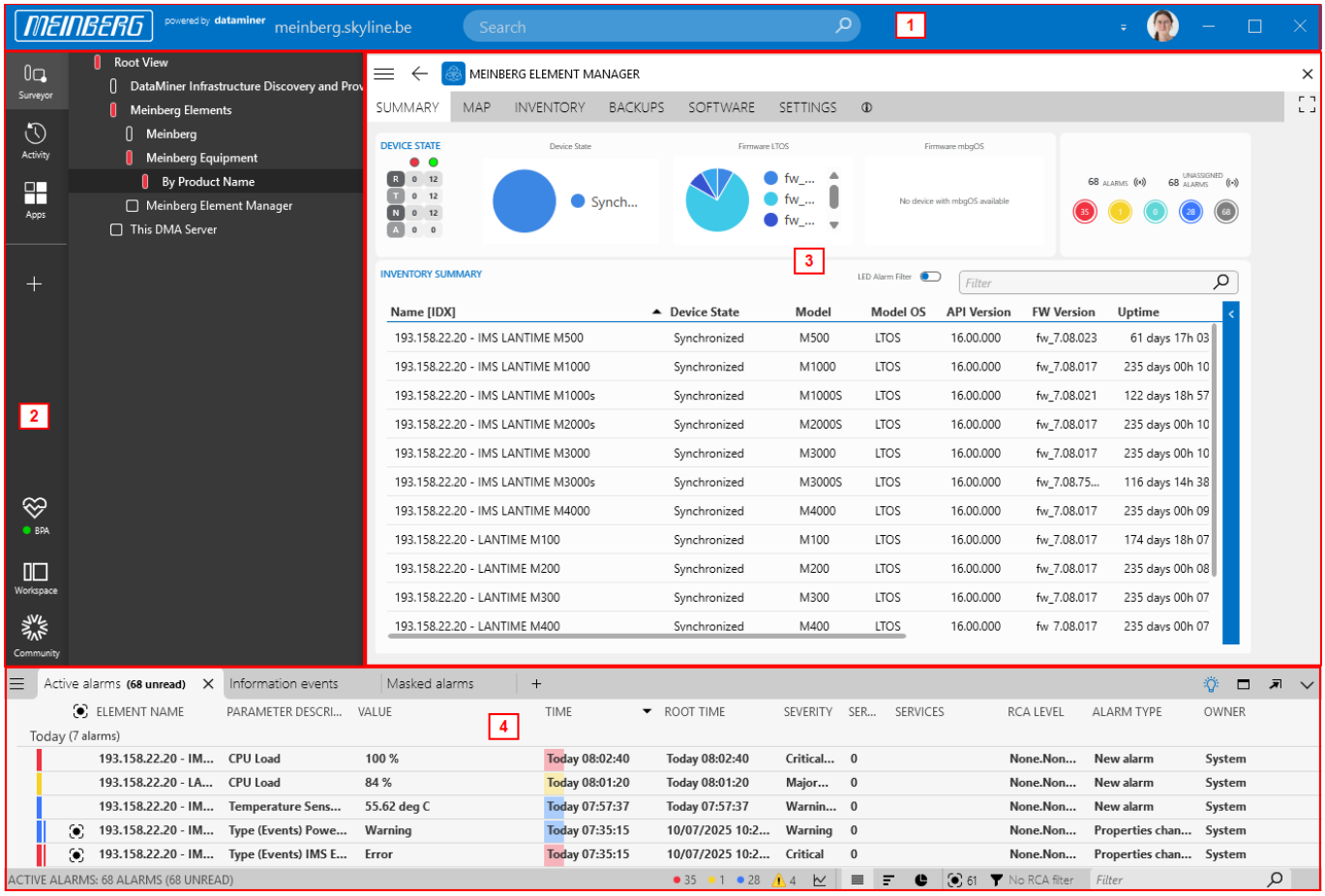
  In the Surveyor, elements are indicated with the following icon: 

- Parameter: A parameter is a variable that refers to specific data in the Meinberg Network Management System. Its value may be detected by the system or may depend on user input. Examples: the temperature of a device, the description of a location, etc.

- Protocol: Protocols are used to create elements. An overview of the protocols used in the Meinberg Network Management System is available in the Protocols & Templates module. See section 3.3.

3.2 Layout of the user interface

The client user interface consists of the components illustrated below.



(1) Header bar, consisting of (from left to right):

- The search box. Enter a term in the box and either immediately select one of the suggestions in the drop-down list below it, or select *Advanced search* to get a complete list of search results with filter options.

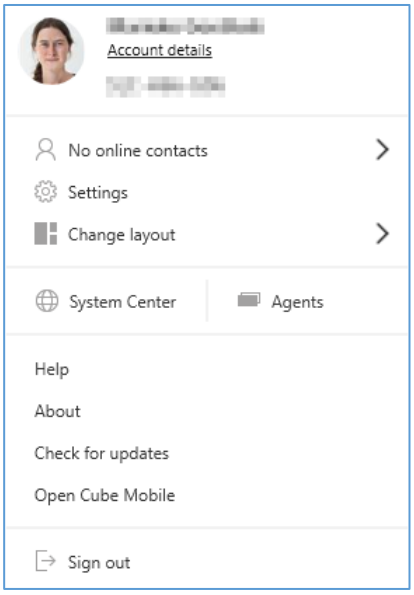
- An arrow icon that opens a drop-down menu with the following options:

  - *Show Cube sides*: Displays four blue squares, each representing one of the four client workspaces. The largest square marks the workspace that is currently displayed. Click a square to switch to a particular workspace.

  - *Show server time*: Displays the current time of the server.

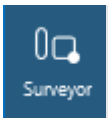
- *Show cluster name*: Displays the name of the system.

- The user icon. Click this icon to access a menu with the following options and information (from top to bottom):
  - The name of the user who is currently logged in, with a link to their account details. Below this, the server name is displayed.
  - The number of contacts who are currently connected to the system. Click this menu option to access a window where you can chat with online contacts.
  - A link to the client settings. For more information on the settings, refer to section 7.
  - The *Change layout* option, which allows you to display the cards in the workspace in different ways.
  - A link to the *System Center* module, which contains various system configuration pages, as well as logging.
  - A link to the *Agents* configuration page in System Center.
  - A link to the complete *Help*.
  - A link to the *About* page, which contains among others licensing information. See section 9 for more information.



  - The Check for updates link, which opens the Update Center, where you can download software updates if you have sufficient user permissions.
  - A link to Cube Mobile, a compact mobile app that allows you to monitor the Meinberg Network Management System from any mobile device.

(2) Sidebar, with the following buttons:



Displays the Surveyor, which shows an overview of the system, consisting of a tree view containing views, elements, etc. Alarm colors indicate when an item in a view is in a particular alarm state.

Provides quick access to items that were used recently. Items can be pinned to the top of the list. To do so, hover over the item until a pin icon appears and then click that icon.

Lists all the available applications and modules within the client app.

Allows you to save and load a workspace configuration, so that you can switch to a pre-configured set of cards with a single click.

Opens a menu with different links to the DataMiner Dojo user community, including a blog, a learning hub, a resources library and a page where you can ask questions about anything related to the software.

(3) Card area, displaying so-called "cards", which can contain an app, information on a selected element, information on a selected alarm, etc.

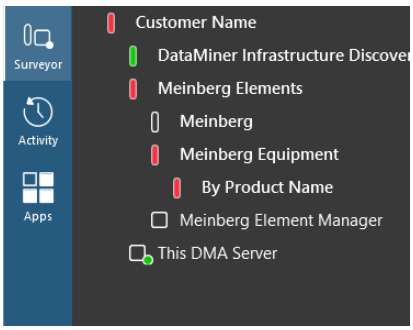
(4) Alarm console, which provides an overview of the alarms detected by the system. For more information on the alarm console, see section 4.3.3.

3.3 Meinberg Network Management System component overview

The Meinberg Network Management System makes use of the following basic components:

- Surveyor: Displays a structural overview of the system, with the following components:

  - Root view with your company name. Provides a general overview of the other available views.
  - *DataMiner Infrastructure Discovery and Provisioning*: Contains elements required for the infrastructure discovery & provisioning functionality.
  - Meinberg Elements: Contains the Meinberg Element Manager and subviews with the managed elements..



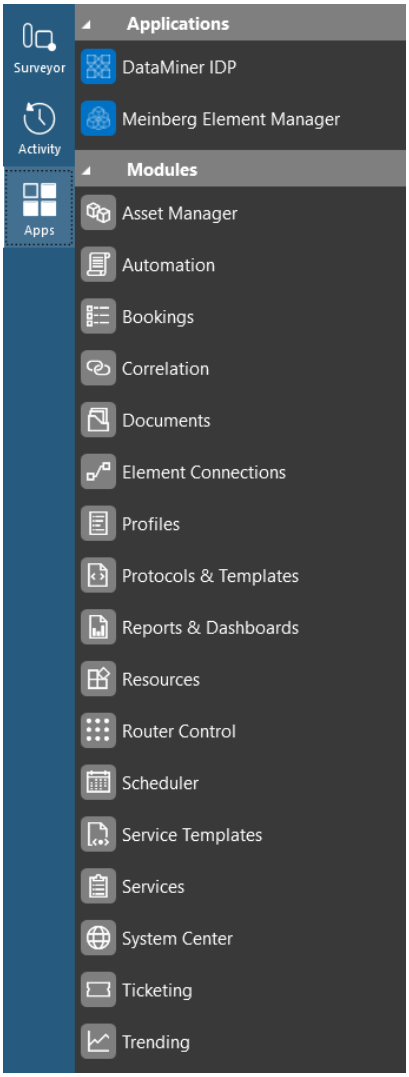
- Apps: Displays the different apps available in the system.

  - *Automation*: Provides access to automated scripts used by the app.

  - *Protocols & Templates*: Provides access to protocols, alarm templates, and trend templates. Alarm templates are used to configure monitoring; trend templates determine for which parameters trending data is collected.

  - *System Center*: Provides access to a card where you can manage the system. This includes the management of the users of the system, on the page *Users / Groups* (see section 8).

  - *Trending*: Allows you to display trend information for parameters (see section 6).



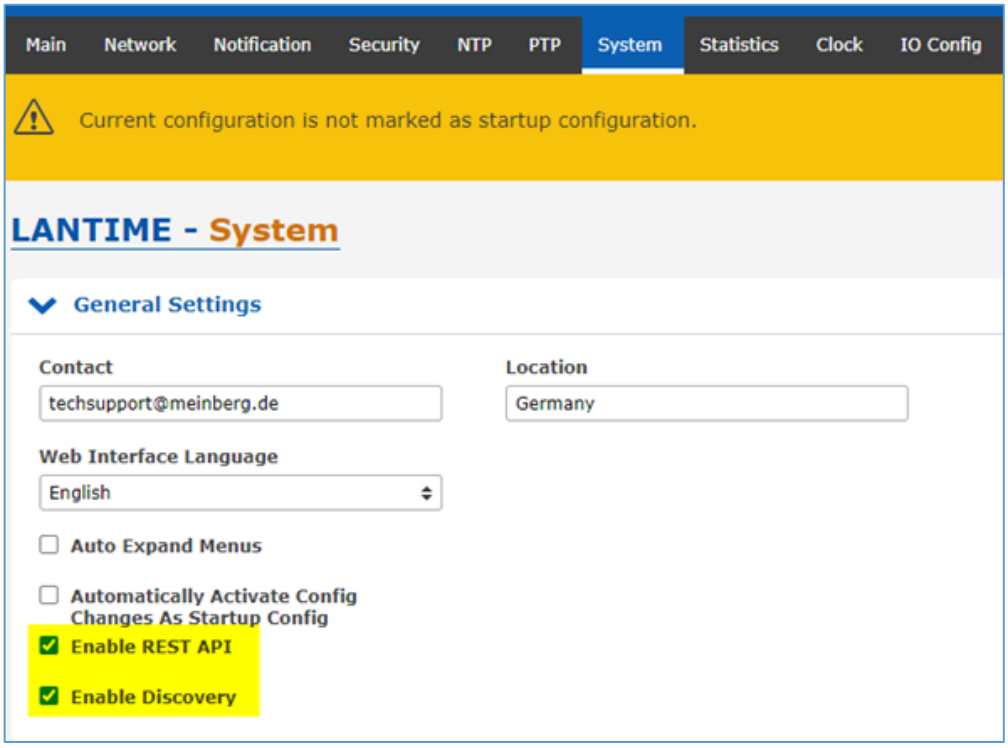
3.4 Supported devices

The Meinberg Network Management System supports both modular and non-modular devices. Non-modular devices are standalone devices. Modular devices are chassis devices and the modules they support. When modules are added to a chassis, elements representing the modules can be created automatically, depending on your settings. For more information, see section 4.3.

NOTE:

- The minimum supported version of the Meinberg firmware is 7.04.009.
- To make sure all functionality in the Meinberg Element Manager app is available for your device, in the web interface of the device, make sure the options *Enable REST API* and *Enable Discovery* are selected (under

System > General Settings).



The following devices are currently supported:

- LANTIME M100 (non-modular)
- LANTIME M150 (non-modular)
- LANTIME M200 (non-modular)
- LANTIME M250 (non-modular)
- LANTIME M300 (non-modular)
- LANTIME M320 (non-modular)
- LANTIME M350 (non-modular)
- LANTIME M400 (non-modular)
- LANTIME M450 (non-modular)
- LANTIME M600 (non-modular)
- LANTIME M1000 (modular)
- LANTIME M1000S (modular)
- LANTIME M2000S (modular)
- LANTIME M3000 (modular)
- LANTIME M3000S (modular)
- LANTIME M4000 (modular)
- LANTIME M500 (modular)

- microSync HR/RX (microSync)

The following chassis modules are supported:

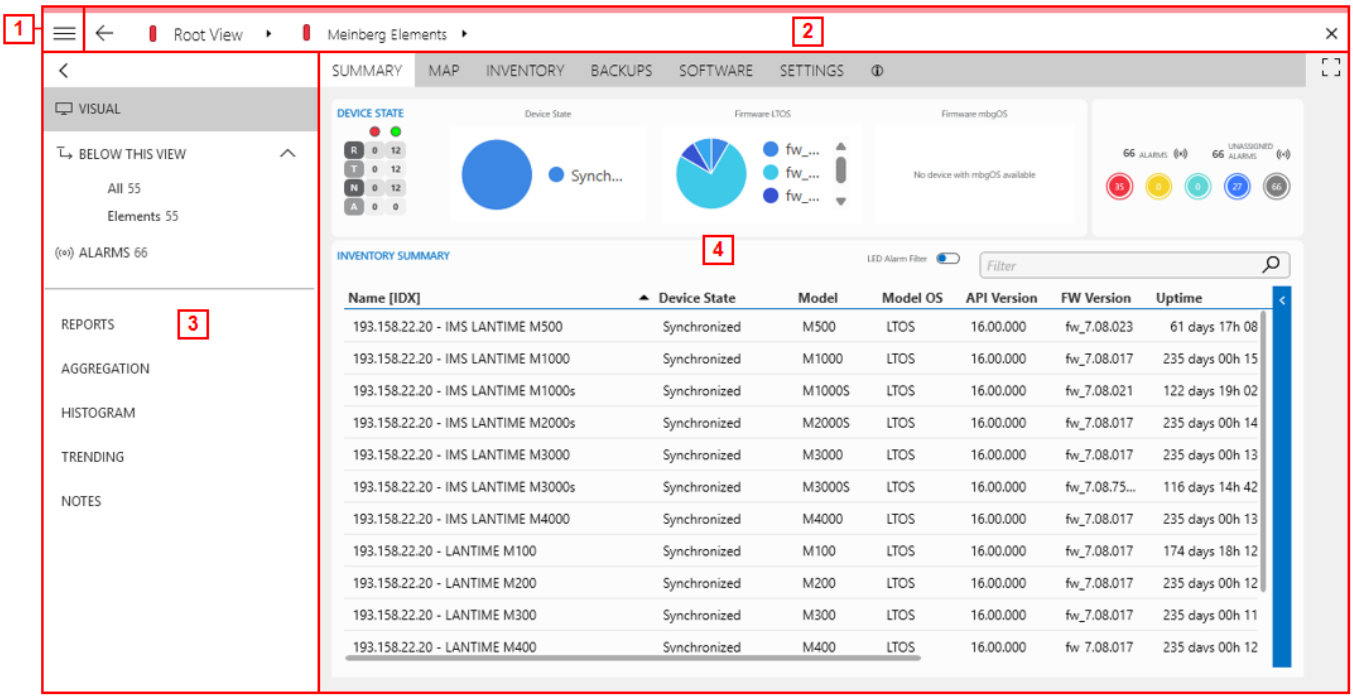
- CPU
- Fan module (supported via the CPU)
    - No separate element is created for this module
    - This module is mandatory for the M1000 and M2000, optional for the M3000 and M4000 and not used for the M500.
    - There can be at most 1 fan module
- Power supply (supported via the CPU)
    - 100-240 V AC/DC
    - 20-60 V DC
- Clock modules
    - IMS-GPS: Meinberg GPS Receiver (requires Meinberg antenna)
    - IMS-GNS: GPS/GLONASS/Galileo/BeiDou Receiver (requires L1 antenna)
    - IMS-PZF: Correlation Receiver (DCF77)
    - IMS-TCR: Time Code Reader and Generator
    - IMS-GNM: Multi-band GNSS receiver module
    - IMS-GNS-UC: GPS and Galileo satellite receiver with up-converter for Meinberg GPS antenna/converter
    - IMS-GXL: Top-End GNSS Clock for High-Security Applications
- Switchover modules
    - IMS-RSC: Signal Switchover Unit for redundant receiver configurations
- Other cards:
    - IMS-HPS: PTP/SyncE/Hardware NTP Interface with Dual-Core CPU
    - IMS-PSX210: Powerful PTP Module for Modern Bandwidth Requirements
    - IMS-LIU: Telecom Synchronization Signal Card (E1/T1 framed/unframed)
    - IMS-ESI: Input module for 2.048 MHz, 2.048 MBit/s and variable frequencies
    - IMS-SCG: Studio Clock Generator (Audio Sync: word clock or DARS generator)
    - IMS-CPE: Configurable Port Expander
    - IMS-BPE: Basic Port Expander
    - IMS-MRI: 10 MHz, PPS, IRIG, TC-AM/TC-DCLS reference signals
    - IMS-LNO: Low Noise Option (provides 10 MHz sine wave with low phase noise)
    - IMS-LSG: Line Signal Generator

4 Card panel layout

Whenever you open an element or view, a so-called card is displayed in the card area of the user interface. This is a panel that provides access to various pages with information and/or settings, depending on the configuration of the object that was opened.

4.1 General card panel layout

In general, a card consists of the following components:



(1) The card menu button. This button opens a menu with various options, depending on the type of card. The following options are available for all types of cards:

- *Back/Forward*: Allows you to navigate between the different cards you have opened.
- *Undock*: Opens the card in a separate window.
- *Dock*: Places a card that was opened in a separate window back in the card pane of the UI.
- *Pin this card*: Ensures that this card remains opened in the same position when you open other cards.
- *Close other cards/Close all docked cards/Close all undocked cards/Close all cards*: Allows you to close several cards at the same time.

(2) The card header bar. This bar shows the alarm color of the selected object at the top. The X in the top-right corner can be used to close the card.

By default, the header bar displays breadcrumbs that show the path to the selected object in the Surveyor. Click a triangle icon in the breadcrumbs path to navigate to other objects at the same level.

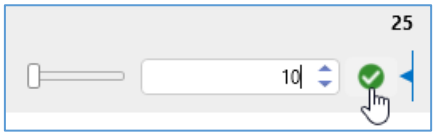
(3) The card side panel. This panel allows quick navigation between the different pages of a card. Note that for some kinds of cards, e.g. for the Meinberg Element Manager, this side panel is not shown.

(4) The main card area. This area displays the page selected in the card panel, or the default page of the card in case no page was selected.

The following pages are of specific importance for the Meinberg Network Management System:

- *Visual* pages: These pages contain a visual overview of the selected object. Depending on the selected object, the pages can have additional functionality, such as special monitoring features. For more information, see sections 4.2 and 4.3.
- *Data* pages: These pages contain detailed information on the selected object. For a view, these pages are named *Below this view*, and as the name suggests, they display lists of the items contained within the view. For an element, the different parameters of the element are displayed.

  To set the value of a parameter on a *Data* page, specify the value and then click the green check mark icon to make sure that your changes are saved.



- *Alarms* page: This page displays a list of the current alarms on the object.
- *Trending* page: This page is available on view cards and allows you to view trend information, if trending has been configured in the system. See section 6.

For certain manager elements, such as the DataMiner IDP element, the card side panel is not automatically displayed. To view the panel for such a card, click the card menu button and select *Show card side panel*.

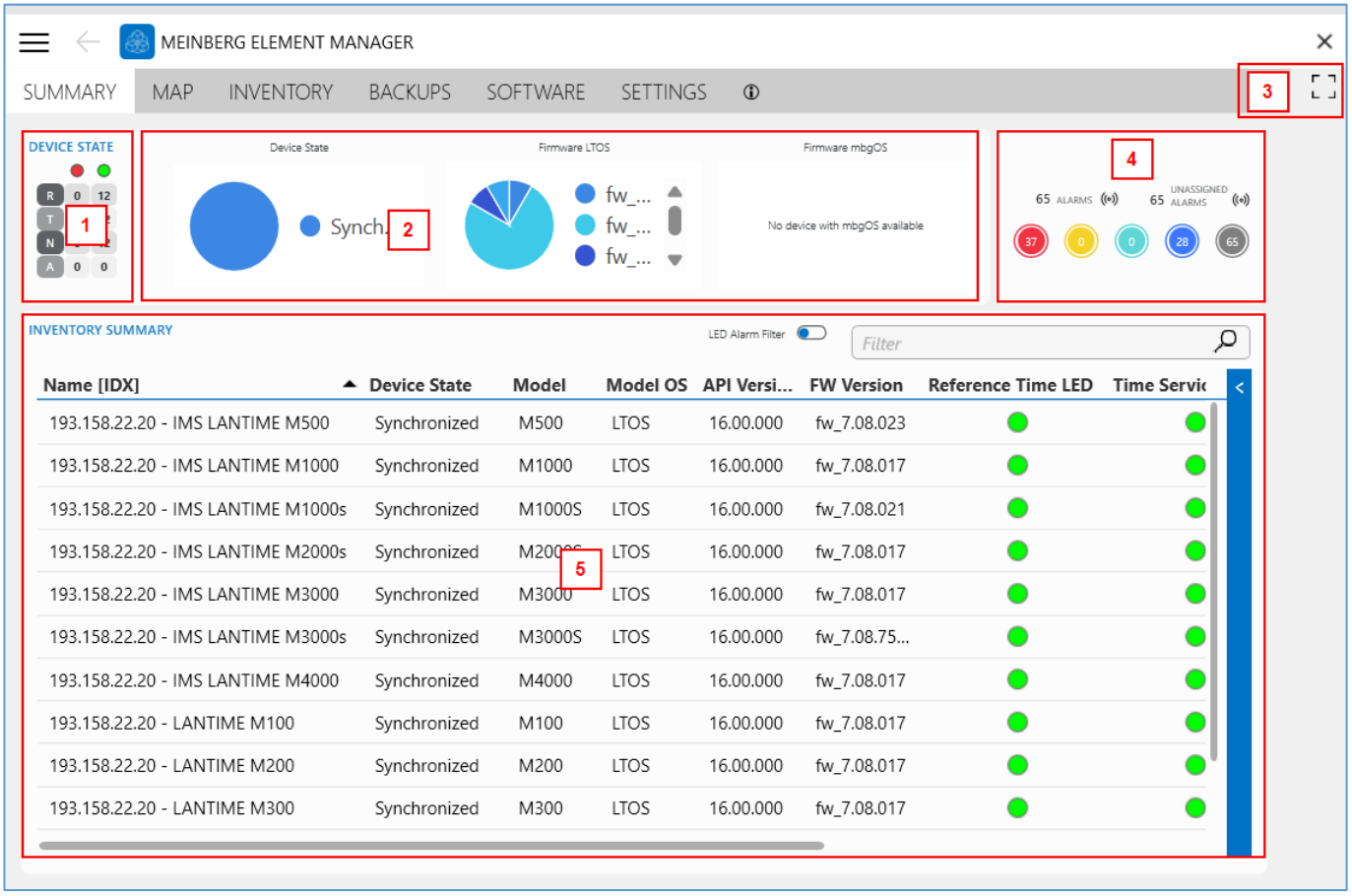
(*) A card footer bar can also be activated in the user settings (see section 7.1). This bar displays alarm information for the element or view.

4.2 Meinberg Element Manager pages

The Meinberg Element Manager has seven custom *Visual* pages: *Summary*, *Map*, *Inventory*, *Backups*, *Software*, *Settings*, and *Info*.

4.2.1 The *Summary* page

This page is available both for the Meinberg Element Manager itself and for views below this node in the Surveyor tree view.



This page consists of the following components:

(1) In the top-left corner, the device state overview shows how many LEDs of each type are in red or green state. The letters in the first column stand for Reference Time LED, Time Service LED, Network LED and Alarm LED, respectively.

(2) The graphs at the top of the page show the following information, from left to right:

- The state of each device. This shows an overview at a glance of the *Device State* column in the table below.
- The LTOS firmware versions that are currently in use.
- The mbgOS firmware versions that are currently in use, if any. Note that these devices are not yet supported in version 1.0 of the Meinberg Element Manager.

(3) The ⛶ icon in the top-right corner allows you to maximize the page, hiding all other UI elements. When the page is maximized, the ⛶ icon in the same location can be used to restore the graph to its original size.

(4) In the top-right corner, you can find an overview of the currently active alarms.

- Each colored circle represents the alarms of a specific severity level. See section 3.1.
- The gray circle represents unassigned alarms, i.e. alarms that no one has claimed ownership of yet. See section 4.3.3.
- Click one of the circles to open a filtered tab in the alarm console, showing only those alarms. For more information, see section 5.3.

(5) The table at the bottom of the page lists detailed information for all the available devices at the current level in the tree structure, including model and firmware information, the current uptime, and colored LEDs representing the different LEDs of the device.

Above the table, a *LED Alarm Filter* toggle button is available. This button determines if all devices are displayed, or only the devices of which the LEDs show an alarm.

If a device is selected in the table, the following button becomes available below *Inventory Summary*: OPEN CARD
Click this button to navigate to the element card for this device. You can also right-click the button to open a context menu that allows you to open the card as a new card or as a new undocked card. For more information about the element card, see section 4.3.

4.2.2 The *Map* page

This page is available both for the Meinberg Element Manager itself and for views below this node in the Surveyor tree view.

On the root page, this page shows a world map with markers indicating the location of all devices that currently have active alarms. On the pages for each view below this, the map is zoomed in to the area relevant for that view, and it only shows markers for devices within the view that currently have active alarms.

When you hover the mouse pointer over a marker for a specific device, a tooltip will display information about the device.

If multiple devices are present in the same location, the markers are grouped. Click a grouped marker to zoom in further on the map. Except if the markers are in exactly the same location, the markers will then be ungrouped.

NOTE: The way the location of a device is determined depends on the device. Some devices have a GPS module and automatically provide location info, for other devices this info must be provided manually in the element properties. To do so, right-click the element and select *Properties*. Then go to the custom tab, fill in the *latitude* and *longitude* and click *OK*.

4.2.3 The *Inventory* page

This page is only available for the Meinberg Element Manager itself, not for views below this node in the Surveyor tree view. It contains information and settings related to inventory discovery and provisioning.

This page consists of the following subpages:

- **Managed**: Displays an overview of the elements managed by the inventory discovery and provisioning (IDP) component of the Meinberg Network Management System.

  At the top of the overview, the summary displays the total number of managed elements. Below this, you can find the following buttons:

  - **Open**: Navigates to the card of the selected managed element.
  - **Remove**: Removes the selected managed element.
  - **Reapply**: Applies the CI type for the managed element again. The CI type or "configuration item type" is a definition of the behavior of the element, which includes how to discover the device, provision the element, perform software and configuration management, and more. Reapplying the CI type can for example be useful to revert the element to its original configuration in case changes were made or to make the element reflect an update to the CI type. Clicking the button will open a wizard where you can select which parts of the CI type should be reapplied.
  - **Reassign**: Allows you to reassign the CI type of the element, for example in case previously a generic CI type was used for a family of devices but now a more specific CI type is available. Clicking the button opens a wizard where you can select the new CI type and then select which parts of the CI type should be applied.

- **Unmanaged**: Displays an overview of the elements available in the Meinberg Network Management System but not yet managed by its IDP component. The information on this page can for instance be useful in case for some reason an element was created manually.

  At the top of the overview, the summary displays the total number of unmanaged elements and the time when the data was last refreshed. Below this, you can find the following buttons:

  - **Refresh**: Refreshes the displayed data.
  - **Manage**: If the detected IP address and CI type are filled in for an element in the overview, click this button to add the element to the managed elements.

- **Discovered**: This page allows you to start a device discovery and manage the discovered elements. It consists of the following sections:

  - **Actions**: Allows you to start a discovery action. You can either select a scan range and click the *Discover* button on the right, or click the *Discover* page button to start a custom discovery. The section also contains the following options:
  - **Identify Unknown devices**: Disable this option if you do not want devices to be displayed if no matching CI type is found.
  - **Identify All Matching CI Types**: Enable this option if you want the discovery process to try to match all possible CI types configured in the scan range. Otherwise, the process will stop trying to match a device with other CI types once a CI type has been identified for it.
  - **Most recent discoveries**: Displays information on the most recent discovery operations.

- **Discovered elements**: Lists all discovered elements with detailed information. The buttons above the table allow you to show the responses returned by the selected device during discovery, provision the element or remove the device from the list. The toggle button on the right determines if all discovered elements are displayed, or only managed elements.

4.2.4 The *Backups* page

This page is only available for the Meinberg Element Manager itself, not for views below this node in the Surveyor tree view. It contains information and settings related to inventory discovery and provisioning.

This page consists of the following subpages:

- **Overview**: Provides an overview of the elements for which the configuration is managed. The overview includes the CI type, element name and IP address for each element, as well as the update progress of the last backup that was copied to the configuration archive, and the date and time when the last configuration change was detected.

  Below this, a list of configuration backups is shown, based on the selection in the first table. The list mentions the element name, the timestamp of the backup, the backup type, the backup size and whether a change was detected compared to the previous backup.

  Above the first overview, the following buttons are available:

  - **Backup**: Opens a wizard that allows you to create a configuration backup of the selected elements. You will first need to select the type of backup: *Startup*, *Running* or *Golden*. A golden backup is a backup that takes the rules defined on the *Rules* tab into account (see below).
  - **Show Backups**: Displays all available configuration backups from the last 30 days for the selected element on the *Backups* page.
  - **Restore**: Allows you to apply a configuration backup file to one or more elements. To do so, select the configuration backup file in Backups table, and the elements in the Elements table (keep the Ctrl key pressed to select several elements at a time). Then click the Restore button above the table.

  When you select a configuration backup in the second table, you can also use the following buttons above the table:

  - **Show content**: Displays the content of the selected configuration backup to the right of the list. Above the content, a drop-down box allows you to select whether the *Full Configuration Backup* should be displayed or the *Core Configuration Only*. This last option allows you to focus on the information that is most important for the configuration.
  - **Compare**: Starts a configuration comparison with the selected file as one of the files to be compared.
- **Compare**: Allows you to compare two configuration files. To do so:
  - First start a configuration comparison on the Overview subpage.
  - Then use the buttons above the table to select the configuration files to show on the left side and on the right side of the comparison, and click the *Compare* button to start comparing them.

- With the drop-down box in the top-right corner, you can select whether you want to compare the *Full Configuration Backup* or the *Core Configuration Only*. This last option allows you to focus on the information that is most relevant for comparison.
- To clear the current file selection, click *Clear*.

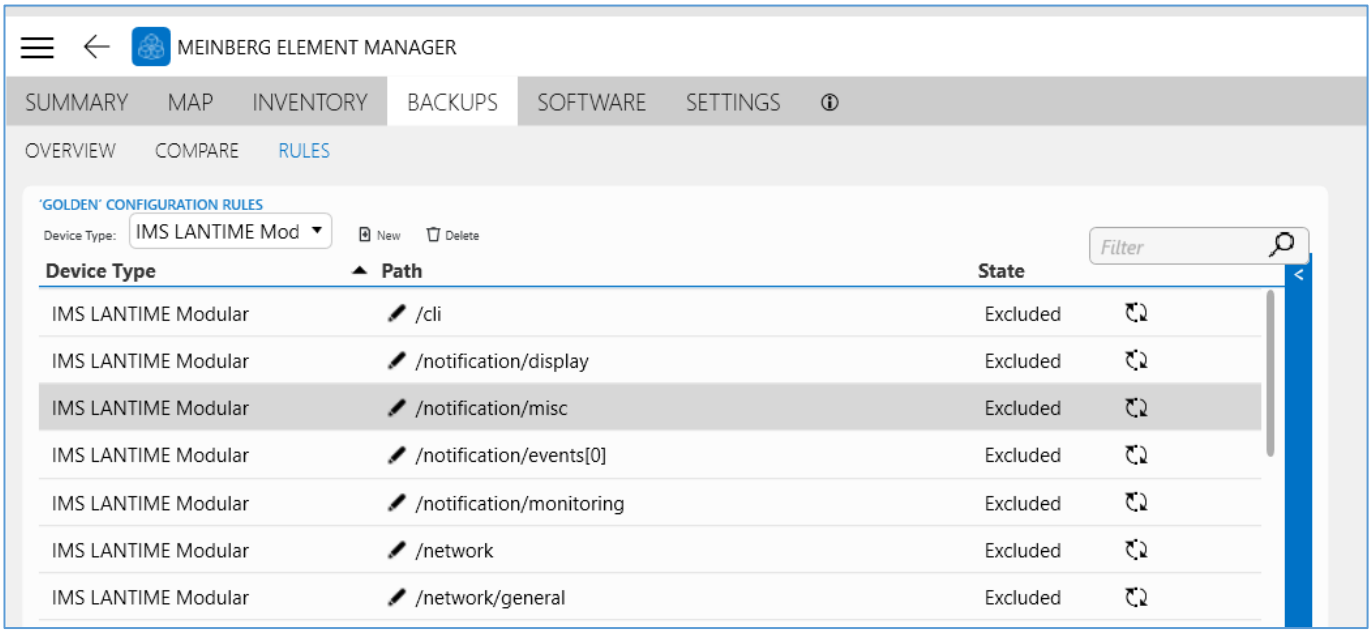
- **Rules**: Allows you to define and manage "golden" configuration rules. A golden configuration rule defines a part of the configuration that should be included in golden configuration backups. This allows you to for example ignore certain things that are device-specific, so that the configuration backup is applicable for all devices of the same type.

  To view the existing golden rules for a specific device type, select the device type in the dropdown box at the top. Via the right-click menu of the table, you can then delete, include, or exclude rules.

  To add a golden rule, use the *New* button at the top. For each rule, you need to specify the device type to which the rule applies, as well as the API path to the configuration object you want to include. Rules can be included or excluded. Only the included rules are taken into account when a backup is taken.

NOTE:

- You will need to know the API structure in order to be able to fill in the correct path. You can find more information in the web interface of the device, via `https://[device IP]/clihelp/`. The tree view on the left allows you to navigate through the objects in the API.
- For the LANTIME Modular or Non-modular, only fill in the part of the path that starts **after** `/api/configuration/`. For specific modules, only fill in the part of the path that starts **after** `/api/configuration/chassis0/slots/[slot id]/module/`.
- If you specify an incorrect path in a golden rule, the rule will be ignored. In addition, for the LANTIME Non-Modular or the LANTIME Modular itself, a path containing the *chassis0* object is ignored.



4.2.5 The *Software* page

This page is only available for the Meinberg Element Manager itself, not for views below this node in the Surveyor tree view. It contains information and settings related to inventory discovery and provisioning.

This page consists of the following subpages:

- **Overview**: Allows you to manage software updates of managed elements.

  Below this, the managed elements are listed. The following buttons are available above the list:

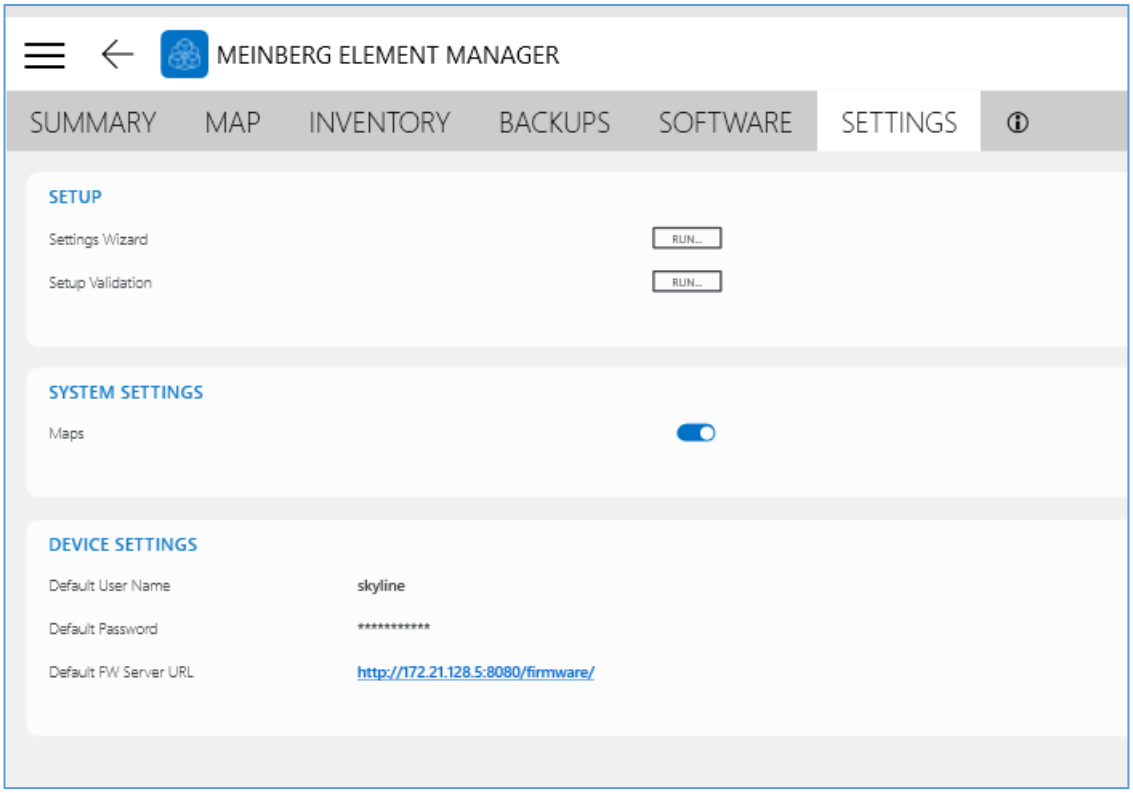
  - **Show Details**: Only available if a single element is selected. Displays the software details for the element, such as the expected software version, detected software version, software image location and deployed software version.
  - **Update**: Opens a wizard to perform a software update on the selected elements.
  - **Check compliancy**: Checks if the selected elements use the expected software version.

- **Baselines**: Allows you to view and configure the baselines for software management. For each managed element, the update image file location and version baseline are listed. If you have sufficient rights, you can click the pencil icon in the table next to a specific value in order to modify it.

NOTE:	If you upload a card firmware file to serve as the new baseline and then update the chassis to this new file, this will update all cards of the type matching the file. After this update, all cards will reboot. In the current version of the Meinberg element Manager app, updating the firmware for a single card is not yet supported.

4.2.6 The *Settings* page

This page is only available for the Meinberg Element Manager itself, not for views below this node in the Surveyor tree view. It contains a button that allows you to run the Settings Wizard script, which will configure the system and device settings displayed on this page. There is another button to run the setup validation script, which checks the default system configuration.

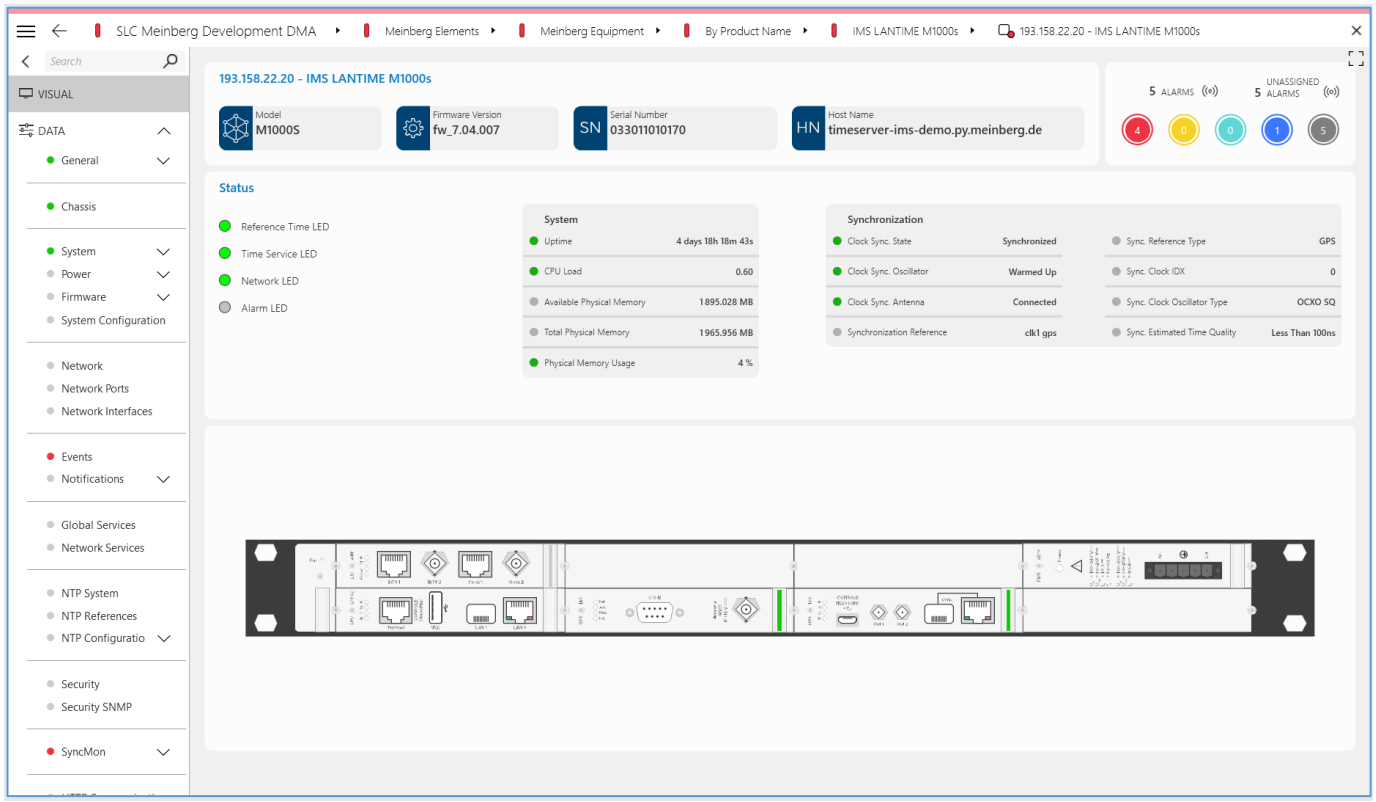


4.2.7 The *Info* page

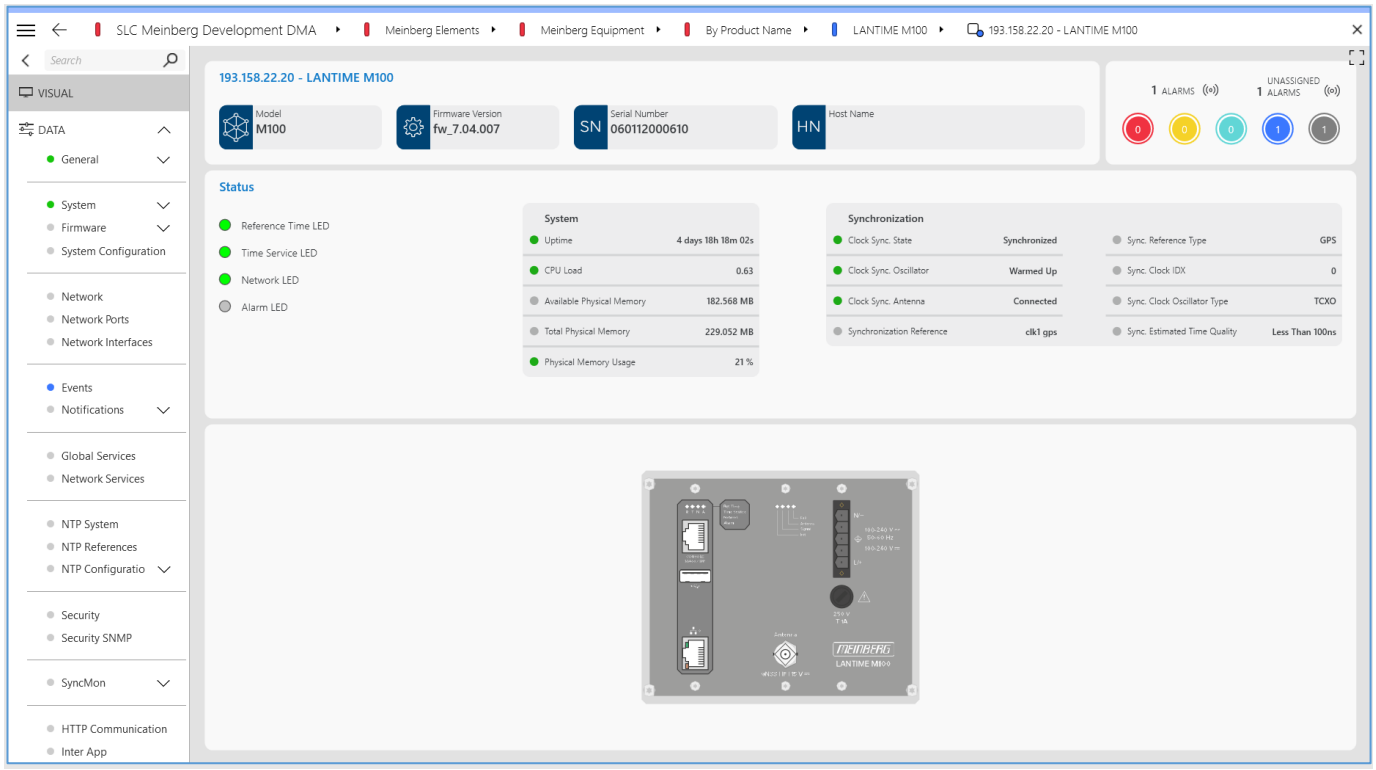
This page is only available for the Meinberg Element Manager itself, not for views below this node in the Surveyor tree view. It displays the version number of the Meinberg Element Manager and all the components it makes use of. This information can for instance be of use when troubleshooting.

4.3 Device pages

The elements representing the different devices managed by the Meinberg Network Management System also have a dedicated *Visual* page. In addition, some of the *Data* pages are of specific note. These are different depending on the type of device.



Example element card for modular device



Example element card for non-modular device

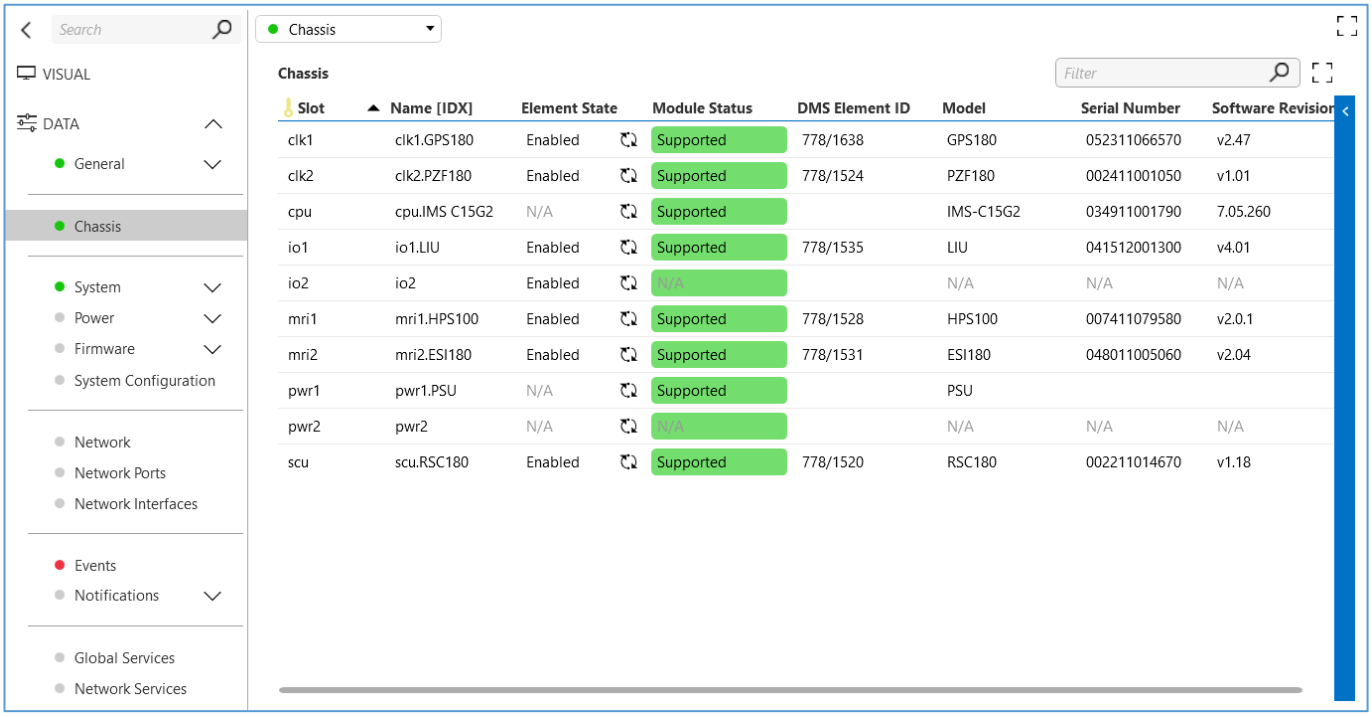
4.3.1 Visual page

The *Visual* page is similar for all devices:

- In the top-left corner, general information about the device is displayed.
- The top-right corner shows an overview of the alarms on the device, similar to that on the *Summary* page of the Meinberg Element Manager. See section 4.2.1.
- The ⛶ icon in the top-right corner allows you to maximize the page, hiding all other UI elements. When the page is maximized, the ⛶ icon in the same location can be used to restore the graph to its original size.
- The *Status* section shows an overview of the LED states and the most important KPIs of the device.
- At the bottom of the page, an image shows what the device itself looks like.

4.3.2 *Chassis* data page

The *Chassis* data page of a modular chassis device shows a table listing all modules on this device.



For each module, in the *Element State* column, a toggle button allows you to enable or disable the element for the module. If this toggle button is enabled, the module can be fully monitored as a separate element. However, the number of modules that can be monitored this way may be limited depending on your license (see section 9). By default, the element state is set to enabled for each module, but if you want to enable other elements while staying within the limitations of your license, it may be useful for you to disable some modules.

The table also displays the module status, element ID, model, serial number and software revision for each module.

4.3.3 *SyncMon* data page

The *SyncMon* data page of a (modular or non-modular) chassis element lists the available SyncMon elements. These are not monitored directly but only through the chassis.

The SyncMon elements can be enabled or disabled. By default, they are disabled. When you enable them, make sure you these additional elements are still allowed within the limitations of your license (see section 9).

4.3.4 *PTPv2* data page

For HPS cards, by default 1 element is created per PTP instance. You can enable or disable this automatic creation on the *PTPv2* data page of an HPS element.

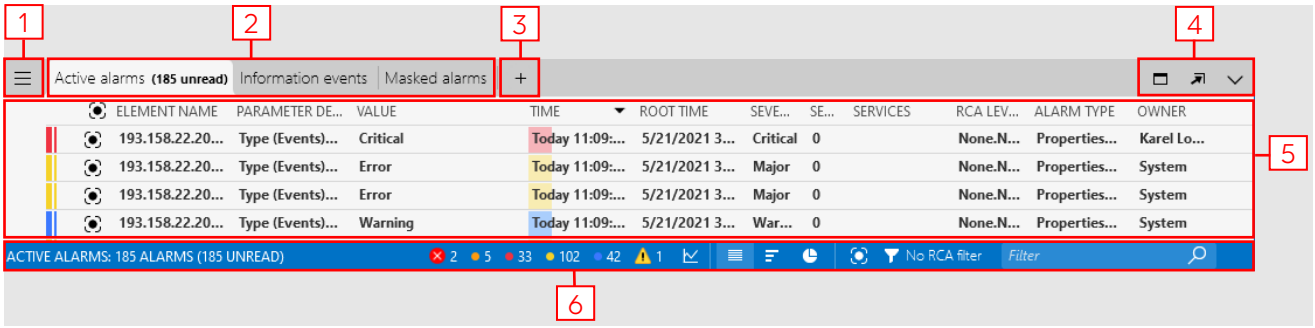
This page contains a table listing all PTP instances. For each instance, a toggle button is available that can be used to enable or disable element creation.

5 Alarm Console

In the alarm console panel, you can view information on the current and past alarms and information events. You can use this to monitor the state of all devices, both at the present time and at any point in the past.

5.1 Alarm Console overview

The alarm console consists of the components illustrated below:



(1) Menu button, which provides access to various alarm console settings. These include:

- *Text to speech*: Reads new alarm events out loud.
- *Freeze*: Keeps new alarm events from being displayed in the currently selected alarm tab.
- *Show in banner*: Displays an info banner at the top of the workspace when new alarms enter the tab.
- *Show side panel/Hide side panel*: Determines whether a side panel is shown in the alarm console, with detailed information on the currently selected alarm.
- *Delay*: Allows you to specify a delay between the creation of a new alarm and its appearance in the selected alarm tab.
- *Refresh rate*: Allows you to specify how frequently the selected tab will be refreshed. This rate will be applied from the moment this setting is set.

(2) Default alarm tabs:

- The *Active alarms* tab lists all active alarms, except information messages and masked alarms.
- The *Information events* tab lists all information messages, which for example are generated when a user logs in, when an element is created, when a script is executed, etc.
- The *Masked* alarms tab lists all alarms that are currently masked. When they are unmasked, the alarms automatically move back to the Active alarms tab.

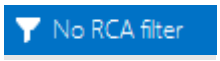
To remove a tab, select the tab and click the x next to the tab name. The tabs can be added again later at any time. For more information, refer to section 5.3.

(3) Button to add an alarm tab. This can be one of the default tabs, if they were previously removed, or a custom alarm tab, e.g. with history alarms for a particular period. See section 5.3.

(4) Buttons to maximize, undock and collapse the alarm console, respectively. If the alarm console is collapsed, only the alarm bar at the bottom is displayed, with a corresponding expand button.

(5) Alarm list, with detailed information on all the alarms in the current tab. See section 5.2.

(6) Alarm bar, consisting of (from left to right):

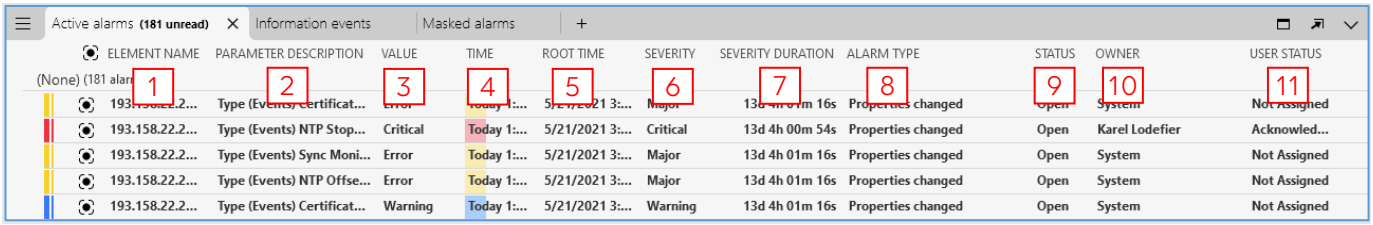
- A summary of the number of alarms.
- Severity filter buttons, which show the number of alarms for each severity, and allow you to quickly filter the alarm tab to show only this severity.
-  : A button that displays the history slider, which shows the evolution of the number of active alarms in the last 24 hours. The slider can also be used to quickly set the alarm list to display alarms for a particular time.
-  : Buttons that allow you to switch between different views:
  - List view: The default view, where all alarms are displayed in a list
  - Statistical view: Displays statistics for the alarms.
  - Report view: Displays a 24h timeline for each element or parameter in alarm, illustrating the evolution of the alarm over time (only available if the system uses a Cassandra local database).
- 

: RCA (Root Cause Analysis) filter button, which allows you to filter alarms depending on how distant they are from the suspected root cause.
- 

: Alarm list quick filter box. To filter on the content of a particular column, you can first add the column and then the content, separated by a colon, e.g. "Value:90".

5.2 Alarm list

The alarm list contains different columns with information on the alarms. Via the column header context menu, columns can be added and removed.



These are the main columns with alarm information:

(1) *Element name*: The name of the element for which the alarm record was created.

(2) *Parameter description*: The name of the parameter that triggered the alarm.

(3) *Value*: The value of the parameter at the time when the alarm was triggered.

(4) *Time*: The date and time when the current alarm event was detected.

(5) *Root time*: The time when the parameter initially entered an alarm state. In case the severity of the alarm has changed since then, this value will be different from that in the *Time* column.

(6) *Severity*: The severity level of the alarm.

(7) *Severity duration*: The length of time that the alarm has had its current severity.

(8) *Alarm type*: Indicates if this is a new alarm or an existing alarm for which a change has occurred, such as a change in severity level.

(9) *Status*: The current status of the alarm, which can have the following values:

- *Open*: The alarm is active, and the parameter that caused the alarm is currently in an alarm state.
- *Cleared*: The alarm is no longer active; the parameter that caused the alarm has returned to a normal state.
- *Masked*: The alarm is active, but is currently masked; the parameter that caused the alarm is currently in an alarm state.

(10) *Owner*: The person who has claimed ownership of an alarm. If nobody has claimed ownership of the alarm yet, the owner is "System".

(11) *User status*: The ownership status of the alarm, which can have the following values:

- *Not assigned*: No one has taken ownership of the alarm yet.
- *Acknowledged*: A user has taken ownership of the alarm.
- *Unresolved*: A user has taken ownership of the alarm and then released ownership again.

Via the context menu of the list, you can among others execute the following actions:

(1) *Open*: Allows you to open an alarm card with detailed info on the alarm or the element card containing the alarm.

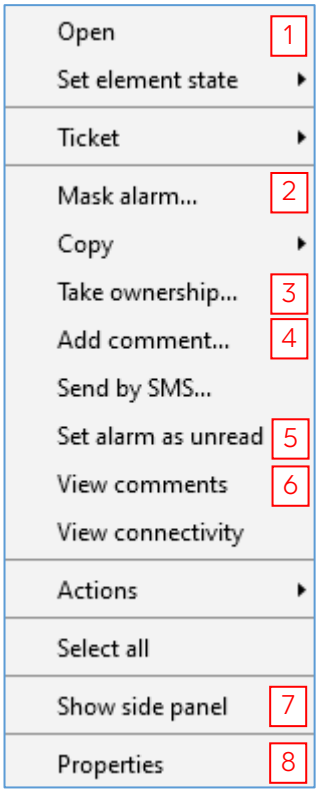
(2) *Mask alarm*: Allows you to "hide" an alarm to prevent unnecessary follow-up. For example, if a device is shut down for maintenance, you can mask the resulting alarm so that operators monitoring the network know that it does not require any intervention.

(3) *Take ownership/Release ownership*: Allows you to indicate that you take or give up responsibility for the alarm, respectively.

(4) *Add comment*: Allows you to add a comment to the alarm.

(5) *Set alarm as unread*: By default, when you select an alarm in the list, it becomes "read" and is no longer displayed in bold like unread alarms. This option allows you to set the alarm back to "unread". This is a personal setting that does not influence other users.

(6) *View comments*: Displays all comments that have been added to the alarm.

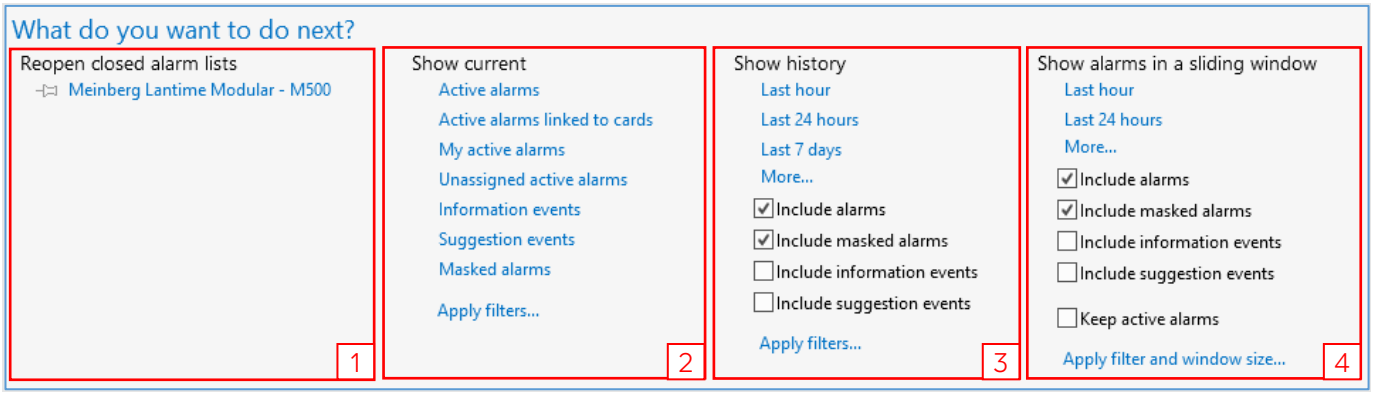


(7) *Show side panel/Hide side panel*: Shows or hides the side panel with detailed alarm information in the alarm console.

(8) *Properties*: Displays the properties that have been configured on the alarm.

5.3 Adding an alarm tab

When you click the "+" icon in the alarm console to add an alarm tab, the following options are available:



(1) *Reopen closed alarm lists*: Allows you to add any of the recently closed tabs. A pin icon is available that allows you to set a tab to always be displayed at the top of the list.

(2) *Show current*: Allows you to add default tabs with active alarms, masked alarms or information events, or to create a custom tab by applying filters.

(3) *Show history*: Allows you to add default tabs with history alarms, or to create a custom tab by applying filters.

(4) *Show alarms in a sliding window*: Allows you to add default or custom (filtered) tabs with active and history alarms in a sliding window, i.e. a time frame that moves with the current time.

NOTE: With the *Show current* > *Suggestion events* option or the *Include suggestion events* check box for history or sliding window tabs you can have a tab display special notifications indicating anomalies detected by the AI. For more information on how to configure anomaly detection, see section 5.4

You can also add a filtered tab by dragging an item from the Surveyor onto the alarm console, or by clicking specific fields in Visual Overview, such as the colored circles in the top-right corner of the Meinberg Element Manager summary page (see section 4.2.1).

5.4 Configuring alarm thresholds

Alarm thresholds determine when particular parameter values are considered abnormal. These are configured in alarm templates for each version of a protocol. The system comes with a number of predefined alarm templates, which you can adapt to match your deployment.

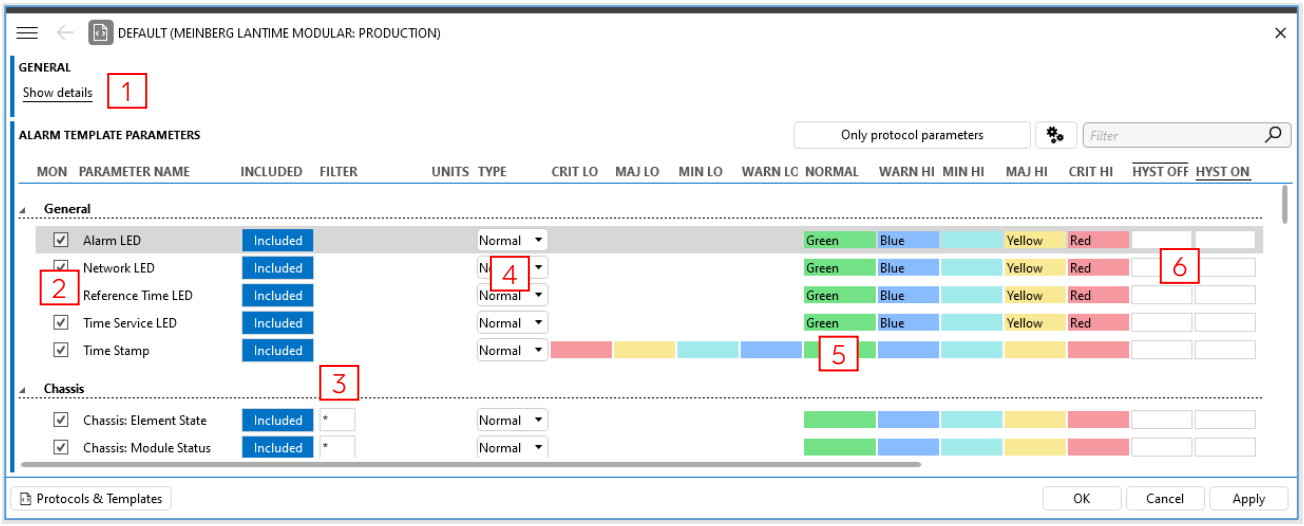
You can manage these templates via the card menu button or the Surveyor right-click menu.

To assign a different **existing alarm template** to an element, in the menu, select *Protocols & Templates* > *Assign alarm template* and select the alarm template.

To create and assign a **new alarm template**:

1. In the menu (opened either via the card menu button or by right-clicking the element in the Surveyor), select *Protocols & Templates* > *Assign alarm template* > *<New alarm template>*.
2. Specify the name of the new alarm template and click *OK*.

   This will open a blank alarm template in the *Protocols & Templates* module:



3. Optionally, you can open the *General* section (1) at the top of the editor to add a description to the template or to add a schedule, so that the template is only applied at certain times.
4. For each parameter that needs to have thresholds configured, do the following:
   a. Select the check box (2) next to the parameter name.
   b. For a table parameter, optionally specify a filter in the *Filter* column (3). The alarm thresholds will then only apply for rows in the table that match the filter. If you wish to specify multiple filters for one table parameter, hover the mouse over the parameter row and click the "+" button next to the filter. A duplicate row will then be created, where another filter can be specified.
   c. In the *Type* column (4), select the threshold type:
      - *Normal*: The default type, which requires that you enter the exact values that constitute the thresholds.
      - *Relative*: The values entered in the threshold boxes are the percentage delta with the baseline value (configured in the *Normal* column (5)).
      - *Absolute*: The values entered in the threshold boxes are the delta with the baseline value (configured in the *Normal* column (5)).
      - *Rate*: the values entered in the threshold boxes are the delta with the current value and the previously measured value.
   d. For each severity level you want to configure, specify the threshold value in the matching box:
      - For analog parameters, i.e. parameters that have a value within a predefined range delimited by a minimum and a maximum, enter the values you want for the different alarm severities. To enter multiple values for one severity level, separate the values by semicolons. In that case the existing alarm will be updated whenever one of the specified values is reached.

- For discrete parameters, i.e. parameters with a limited set of predefined values, check boxes will be displayed for the available values when you click the threshold field. Select the boxes for the value(s) you wish to use for the threshold. If multiple values are selected, the existing alarm will be updated whenever one of these values is reached.
- For hybrid parameters, which can have a value within a predefined range as well as one predefined value, a combination of the two editing methods above can be used.

e. Optionally, enter a value in the *Hyst off* or *Hyst on* column (6) to determine the number of seconds before the severity level of an alarm decreases or increases, respectively.

f. Optionally, in the *Info* column, select the check box and specify a threshold value. Whenever the parameter value crosses this threshold, an information event will be generated in the alarm console.

g. Optionally, in the *Condition* column, specify a condition to indicate that the parameter should only be monitored depending on the value or alarm state of another parameter of the element. If the condition is met, monitoring is disabled.

5. Optionally, you can also configure if and how anomaly detection should be used for the monitoring of each parameter. This feature will trigger suggestion events in the Alarm Console when an anomaly is detected. To configure anomaly detection:

   a. Click the cogwheels button in the top-right corner, next to the filter box.

   b. Select the option *Advanced configuration of anomaly detection*. Three extra columns will be displayed in the template editor.

   c. Click the toggle buttons in these columns to configure alarms for specific types of anomaly detection:

      i. *Trend monitor*: Enables or disables alarms for trend changes. These are anomalies where a value suddenly starts to increase or decrease at an unusual rate. For example, a value fluctuating around 10 (i.e. a trend slope of 0) that suddenly starts to increase by 1 unit per second (i.e. a trend slope of 1).

      ii. *Variance monitor*: Enables or disables alarms for variance changes. For example, a series like 0.5, 0.6, -0.5, -0.2, 1, ..., 5, 8, 9, -5, -6, -2.1, ... indicates a variance increase. The value is first fluctuating around 0 between 1 and -1 and then starts fluctuating around 0 between 10 and -10.

      iii. *Level shift*: Enables or disables alarms for level shift anomalies. These are anomalies where a value shifts upwards or downwards and then stays at that level, e.g. a value fluctuating around 0 that starts to fluctuate around 10.

6. When all parameters have been configured, click OK to save the template and assign it to the element.

NOTE: You can make changes to the alarm template assigned to an element by selecting *Protocols & Templates > View alarm template '...'*. This is similar to the procedure described above, except that by default only monitored parameters will be shown at first. To see other parameters as well, click the *Only monitored parameters* button and select *Only protocol parameters* or *All parameters (protocol + general)*.

---

6 Trending

For specific elements in the system, trend data can be stored and viewed.

Two types of trend data are available:

- Real-time trending: Logging of all values, in a sliding window of 24 hours.
- Average trending: Logging of the average values across larger timespans. For the past 31 days, 5-minute averages are used. Beyond that, for the last 366 days 1-hour averages are used. For each timespan, the minimum and maximum values are also stored

6.1 Configuring trending of parameters

To determine which type of trending is stored for which parameters, trend templates need to be configured.

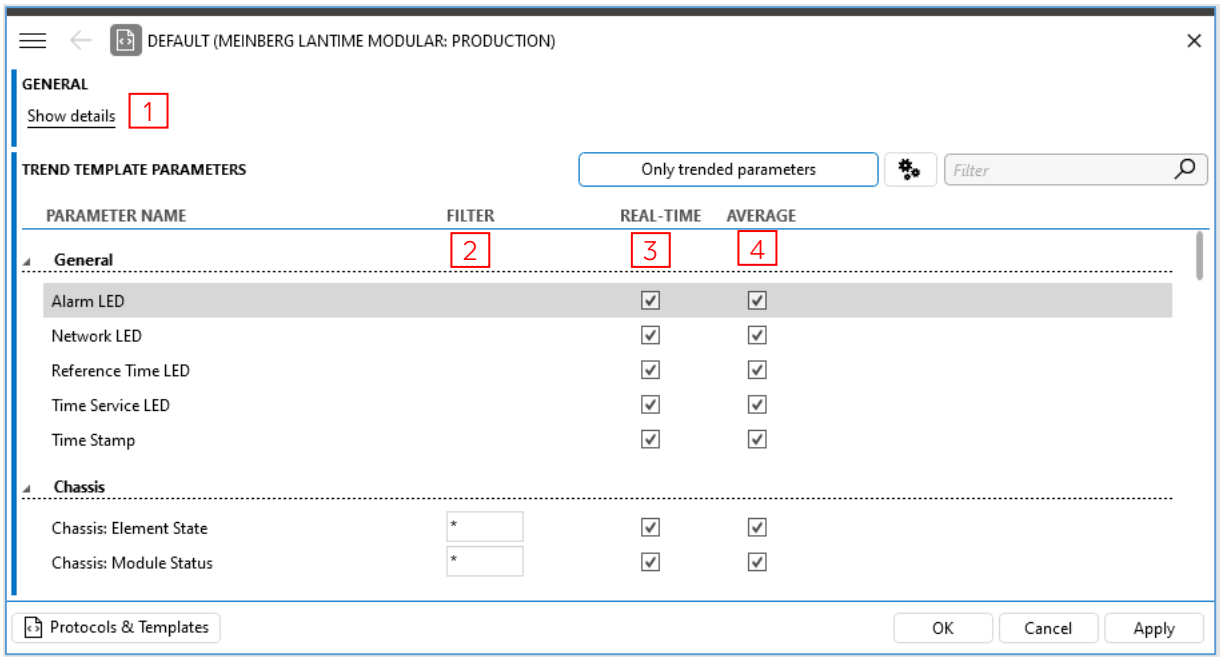
You can manage these templates via the card menu button or the Surveyor right-click menu.

To assign a different **existing trend template** to an element, in the menu, select *Protocols & Templates* > *Assign trend template* and select the trend template.

To create and assign a **new trend template**:

1. In the menu (opened either via the card menu button or by right-clicking the element in the Surveyor), select *Protocols & Templates* > *Assign trend template* > *<New trend template>*.
2. Specify the name of the new trend template and click *OK*.

   This will open a blank trend template in the *Protocols & Templates* module:



3. Optionally, click *Show Details* (1) at the top of the editor to add a description to the template.
4. Optionally, to configure trending for specific rows of a table parameter, specify a filter in the *Filter* column (2). The trending configuration will then only be applied to the rows matching the filter. If only an asterisk ("*") is specified in the filter box, the configuration will be applied to all rows.

If you wish to specify multiple filters for one table parameter, hover the mouse over the parameter row and click the "+" button next to the filter. A duplicate row will then be created, where another filter can be specified.

5. For each parameter that needs to have thresholds configured, do the following:

   To activate real-time trending for the parameter, select the check box in the *Real-time* column (3).

   To activate average trending for the parameter, select the check box in the *Average* column (4).

6. Click OK to save the template and assign it to the element.

NOTE: You can make changes to the trend template assigned to an element by selecting *Protocols & Templates* > *View trend template '...'*. This is similar to the procedure described above, except that by default only trended parameters will be shown at first. To see other parameters as well, click the *Only trended parameters* button and select *Only protocol parameters* or *All parameters (protocol + general)*.

6.2 Viewing trend information

There are several ways to access trend information:

- Click the Apps button in the sidebar and select *Trending*.
- On a view card, open the *Trending* page
- On an element card, click the trending icon for a parameter that has trending activated.

  Depending on the predicted trend, a different icon can be displayed:

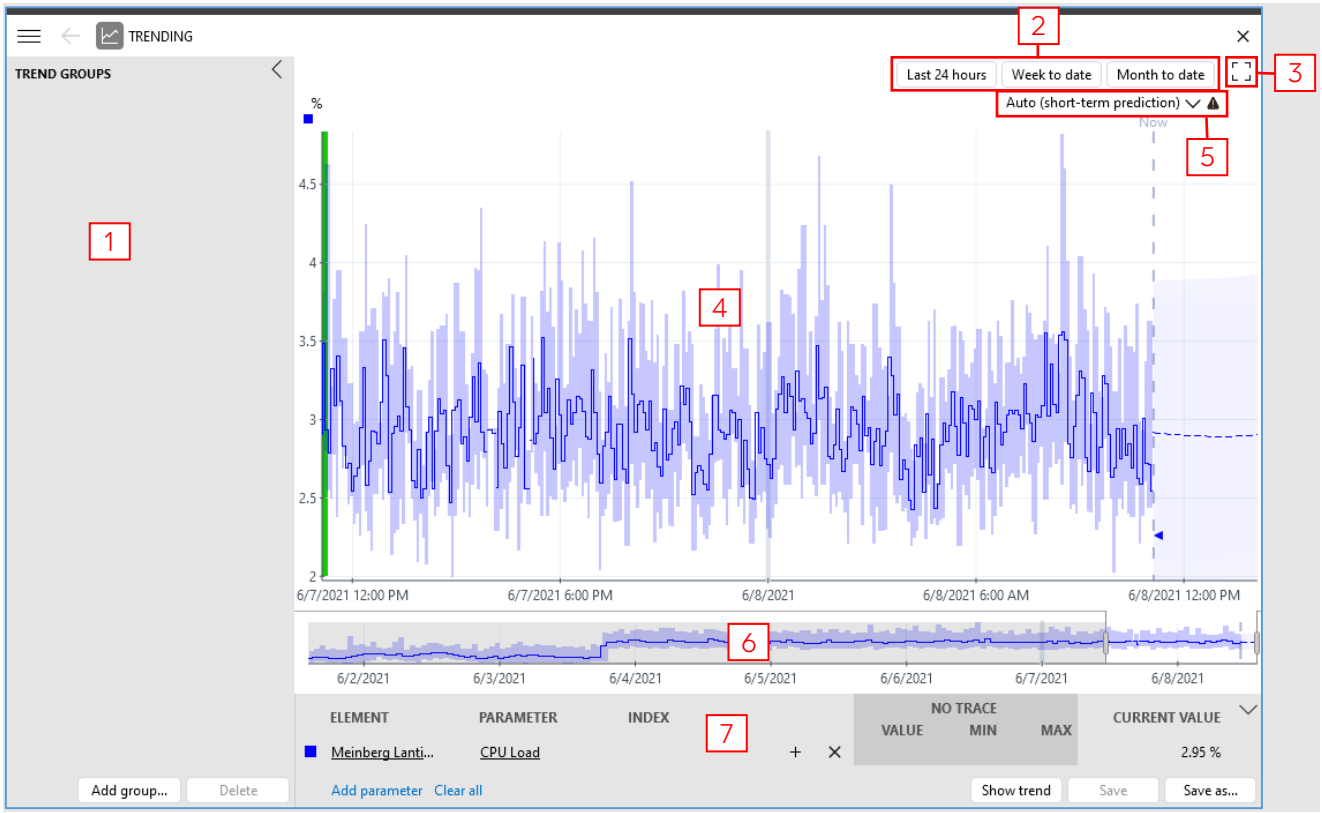
   No significant changes to the trend value are expected.

   The trend value is expected to increase.

   The trend value is expected to decrease.

   The trend behavior cannot be predicted, either because there is insufficient data, or because there is too much uncertainty in the direction of the trend during the past hour.

Regardless of where you access trending from, the user interface looks similar:



(1) Trend groups pane: This pane allows you to add a group of parameters for which trending is displayed (i.e. a "trend group") using the *Add group* button. The group should then be configured using the parameter pane (see below).

You can load a saved trend group by selecting it in the pane. This feature allows you to quickly load graphs for particular groups of parameters, without having to select all the parameters again every time.

To remove a trend group that is no longer needed, select it and click the *Delete* button.

(2) Time range buttons: These buttons allow you to quickly move to a specific time range of the graph. Additional fixed time ranges can be selected via the right-click menu of the graph.

(3) Maximize button: This icon can be used to maximize the graph, hiding all other UI elements. When the graph is maximized, the icon in the same location can be used to restore the graph to its original size.

(4) Main graph area: This area displays the selected trending information.

If average trending is configured for a parameter, this is displayed by default, with a colored background indicating the minimum and maximum values during the time intervals where the average is taken.

To view real-time trending instead, if this is available for the parameter and time period, right-click the graph and select *Show most detailed data*.

To zoom in and out on the graph, use the mouse scroll wheel. To pan the graph, drag while keeping the left mouse button clicked (note that a different button can be configured for this in the user settings – see section 7.1). Alternatively, you can also use the preview pane to manipulate the graph (see below).

Via the right-click menu of the graph, you can export the information to CSV, copy it to the clipboard, save it as an image or send it to a printer. You can also remove a curve from the graph, toggle the display of minimum and maximum values and customize the range of the Y-axis. Finally, you can also open a pop-up window with statistical info, such as the average, the mean deviation, etc.

(5) Prediction type selector:

This selector indicates the type of trend prediction that is currently applied and allows you to select a different type. The following types can be selected:

- *Auto*: Automatically switches between the different trend prediction types as you zoom in and out on the graph
- *High-precision prediction*, *Short-term prediction*, *Mid-term prediction* or *Long-term prediction*.

However, depending on the behavior of the displayed parameter, some types of prediction may not be available. If a prediction is possible, the trend graph will be extended beyond the "Now" line with a dotted line, indicating the predicted trend.

(6) Preview pane:

This pane shows the larger context of the main graph and allows easy panning and zooming. The main graph is an enlargement of the central section of the preview pane. Drag this central section to pan the main graph, or drag the edges of the central section to zoom in or out.

(7) Parameter pane:

This panel allows you to configure for which parameter(s) trend information is displayed.

There are two ways to add a trend graph for a specific parameter to the main graph area using this panel:

- Click *Add parameter* in the panel, select the element, select the parameter, optionally (in case of a table parameter) specify the index, and then click *Show trend*.
- Drag the element containing the parameter from the Surveyor to this panel, select the parameter, optionally (in case of a table parameter) specify the index, and then click *Show trend*.

To clear the main graph area, click the *Clear all* button.

With the *Save* button, you can save changes to a trend group loaded from the trend groups pane.

With the *Save as* button, you can add the current set of parameters as a trend group in the trend groups pane, so you can easily load it again later.

7 Client settings

There are two ways to access the client settings:

- Click the Apps button in the sidebar, and select *Settings*.
- Click the user icon in the header bar, and click *Settings*.

This will open a window with two main tabs: a *user* tab and a *computer* tab. The *user* tab contains all settings specific to the current user, the *computer* tab contains all settings relevant to the computer used to access the client application.

7.1 Client user settings

The following pages with user settings are available:

- *General* page: Contains the following setting:
  - *Show DMA status messages*: Determines whether status messages are shown to inform the user of the status of the server.
- *Alarm Console* page: Contains various settings that determine how the alarm console is displayed, as well as settings to limit when alarms are displayed.
- *Card* page: Contains settings that determine how the different types of cards are displayed. This includes the following settings:
  - *Default view card page*: Determines which page is displayed by default when you open a view card.
  - *Default element card page*: Determines which page is displayed by default when you open an element card.
  - *Show footer*: Determines whether the footer of cards is displayed.
  - *Show breadcrumbs*: Determines how the path in the header of cards is displayed.
- *Connection* page: Contains the following settings:
  - *Time before automatic disconnect (minutes)*: Select this setting to enable automatic disconnection when the client application is left unattended for some time, and fill in the number of minutes after which you want automatic disconnection to occur.
  - *Automatic reconnect after connection loss*: Select this setting to ensure that the client application will automatically reconnect after the connection is lost.
- *Cube* page: Contains general settings related to the client application, such as:
  - *Never ask for confirmation after setting parameter value*: When you select this setting, no confirmation boxes will appear when a parameter value is set.
  - Mouse word highlighting in Alarm Console: This setting determines which key should be pressed in order to highlight

words in the alarm console by moving the mouse over them, with the purpose of adding them to a filter.
- *Use compact alarm banner*: If the alarms are configured to be shown in a banner (see section 5.1), this setting determines whether a full banner is displayed in the header, or only a banner containing the number of alarms and the highest severity.

- *Cube sides* page: Contains settings related to the four available workspaces of the client application:
  - *Default workspace*: Allows you to select a default workspace to load when the client application is started.
  - *# cards*: These settings determine the maximum number of cards that can be opened in each of the four workspaces.
- *Data Display* page: Contains settings that control how parameters are displayed on the Data pages of cards, such as:
  - *Parameter display mode*: With this option, you can choose whether to visualize parameter controls in Normal mode or Lite mode. When you select Lite mode, parameters will be shown in a more compact way. Several other options on this page allow you to customize Lite mode.
- *Icons* page: Contains settings that determine which icons are shown in the user interface, such as:
  - *Use modern icons*: Determines which kinds of icons are displayed. If you clear this check box, classic icons are displayed, which allow further fine-tuning with other options on this page.
  - *Element alarm level*: Determines whether the timeout state overrules the previous alarm state for elements. Set this option to *Separate from timeout* to show a timeout icon and the last-known alarm level, or to *Timeout overrules* to show a timeout icon and the timeout color.
- *Regional* page: Contains settings related to the region where the client interface is used, such as:
  - *Language of the user interface*: Allows you to select a different language for the user interface. Only a limited number of languages are supported.
  - *Regional date and time format*: Allows you to set the format of dates and times in the client application to a different culture.
- *Sidebar* page: Contains settings related to the sidebar, such as:
  - *Sidebar docking position*: Determines whether the navigation panel is displayed on the left or the right side of the screen.
  - *Link the Surveyor selection to the selected card in the workspace*: If this option is selected, the Surveyor automatically selects the item displayed in the currently selected card.
- *Trending* page: Contains various settings that allow you to customize how trend graphs are displayed, including:

- *Show alarm template colors on vertical axis*: Enable this setting to show the alarm colors next to the vertical axis of trend graphs. The setting *Display the alarm template in the trend graph* allows you to further specify how the alarm colors are displayed.
- *Show most detailed data*: If you select this option, the most detailed data available will be shown (if available), rather than average data. In order to ensure optimal performance in case a large amount of trend data must be displayed, this option is by default not selected.
- *Left/Right mouse button on graph*: These options determine which action is executed when you use the left or right mouse button on a trend graph: *Pan*, *Zoom*, *Select* or *None*.

- *Visual Overview* page: Contains settings related to Visual pages, such as:
  - *Enable coloring when severity is normal or undefined*: Select this option to ensure that elements, services and views in Visual Overview will also be colored if their alarm severity level is normal or undefined.
  - *Enable page loading message*: Determines whether a message is displayed to indicate that a Visual page is loading.
- *Advanced* page: Allows you to reset all client user settings back to the factory defaults.

NOTE:	Default client user settings can be configured for a group of users. For more information, refer to section 8.4.

7.2 Client computer settings

The following pages with computer settings are available:

- *Connection* page: Contains the following settings:
  - *Automatic log-on with saved user name and password*: Select this setting to have the client application remember your user name and password, so that you do not have to enter these except after an explicit logout.
  - *Connection type*: Allows you to select a different connection type. By default, *Auto* is selected, so that the client automatically determines which connection type to use. If you select *Remoting* instead, you will need to manually configure the destination port and polling interval. You can also select whether data compression should be enabled and specify a custom binding IP address, in case a VPN connection is used.
- *Cube* page Contains a setting that determines whether the name of the system is displayed in the client header.
- *Debug* page: Contains settings that can be used for troubleshooting purposes.

- *Performance* page: Contains settings related to the performance of the client computer:
  - *Use of animation*: Determines whether animations are used in the UI.
  - *Use hardware rendering*: Determines whether the client relies on the computer hardware for rendering, or only on the client software. In case display driver issues are encountered, it can be useful to deselect this option.
  - *Frame rate*: Determines the frame rate of all animations used in the client application.
  - *Trend update frame rate*: Determines the rate at which trend graphs are redrawn.
- *Visual Overview* page: Determines where Visual pages that you edit in Microsoft Visio® are saved on the computer.
- *Advanced* page Contains the following settings:
  - *Connection timeout (ms)*: Determines how many seconds should elapse before a connection timeout occurs when the connection fails.
  - *Factory defaults*: Allows you to reset all client computer settings back to the factory defaults.

  The page also has two subpages with settings related to logging and to communication between the server and the client. These can be of use for troubleshooting purposes.

8 Managing users and groups

To configure which users have access to which parts of the client app, an integrated security module is available. This module allows you to use user profiles to determine which actions users can perform, and also provides access to a detailed log of all user activity.

Three different concepts determine what a user can do in the Meinberg Network Management System:

- *Rights*: These are a set of user permissions that determine which actions the user can perform within the system and which parts of the system are available to them.
- *Views*: Users can be denied or granted access to individual views. If users do not have access to a particular view, they do not have access to any items within that view either, so that this way you can manage user access to particular elements.
- Access level: This is a number between 1 and 5, where 1 is the highest level with the most rights. This represents the parameter access level of the user. Access levels can be assigned to parameters within the protocol for an element, so that depending on their access level, users will only be able to access certain parameters.

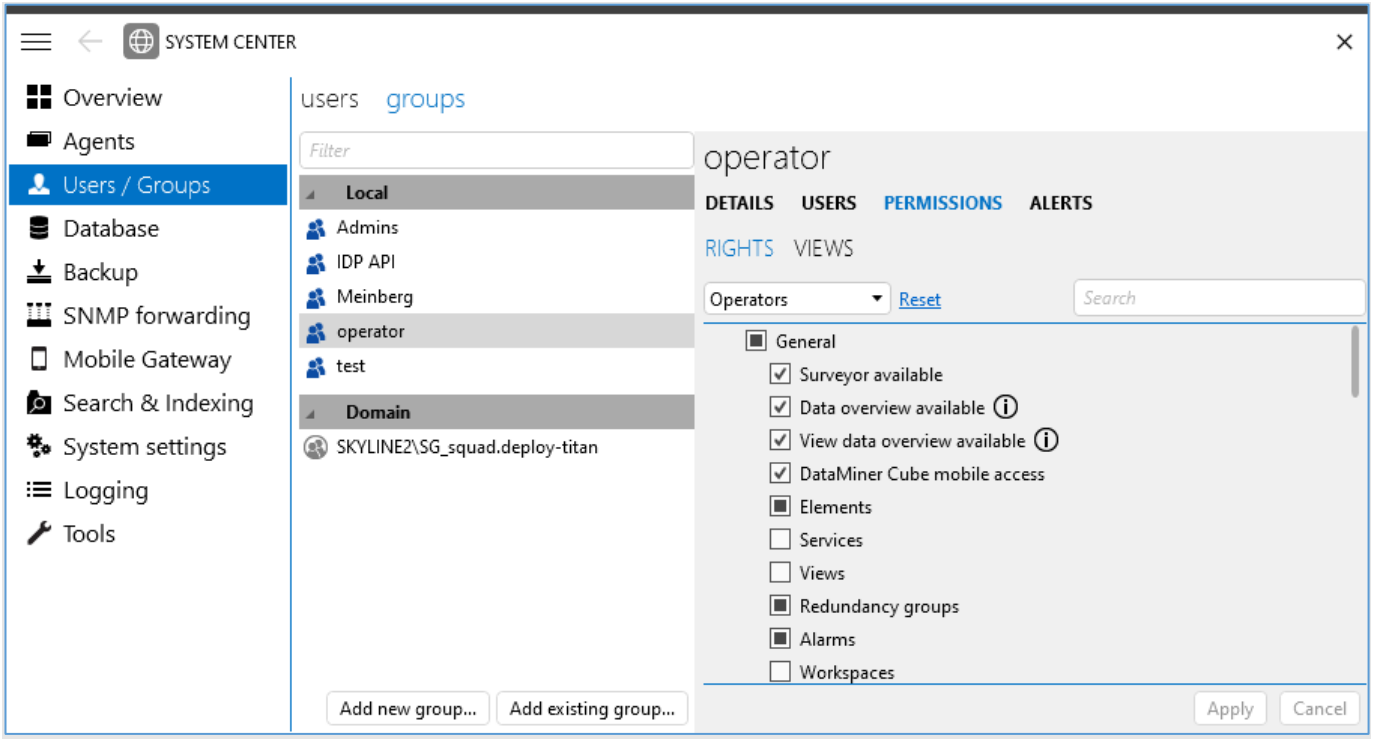
Users and user groups are managed in System Center:

- In the navigation pane, go to the apps tab and select System Center.
- In System Center, go to the page *Users / Groups*.

8.1 User group configuration

Every user must be a member of a group in order to have access to the client app.

It is at group level that user permissions and access rights are configured. To access these settings, go to the *groups* tab on the *Users / Groups* page.



To add a user group, there are two possibilities:

- To add a **new group**:
  1. Click the button *Add new group*.
  2. In the *Name* box, specify the name of the group.
  3. In the *Level* box, specify a number from 1 to 5. This represents the parameter access level of the group, where 5 is the lowest level and 1 is the highest level with the most rights.
  4. Click *OK*.
- To add an **existing group from the domain**, including its users and any subgroups it contains:
  1. Click the button *Add existing group*.
  2. Select the group you want to add. Optionally, several groups can be selected at the same time.
  3. In the *Group level* box, specify a number from 1 to 5. This represents the parameter access level of the group, where 5 is the lowest level and 1 is the highest level with the most rights.
  4. Click *OK*.

NOTE:	If you have added a domain group, personal details for the users, such as their email and password, are determined at domain level. Any changes that are made to the domain group outside of the Meinberg Network Management System, such as added or deleted users, are automatically applied in the system.

To remove a user group, right-click the group in the list and select *Delete*.

When a group is selected in the list, it can be configured in the four tabs on the right:

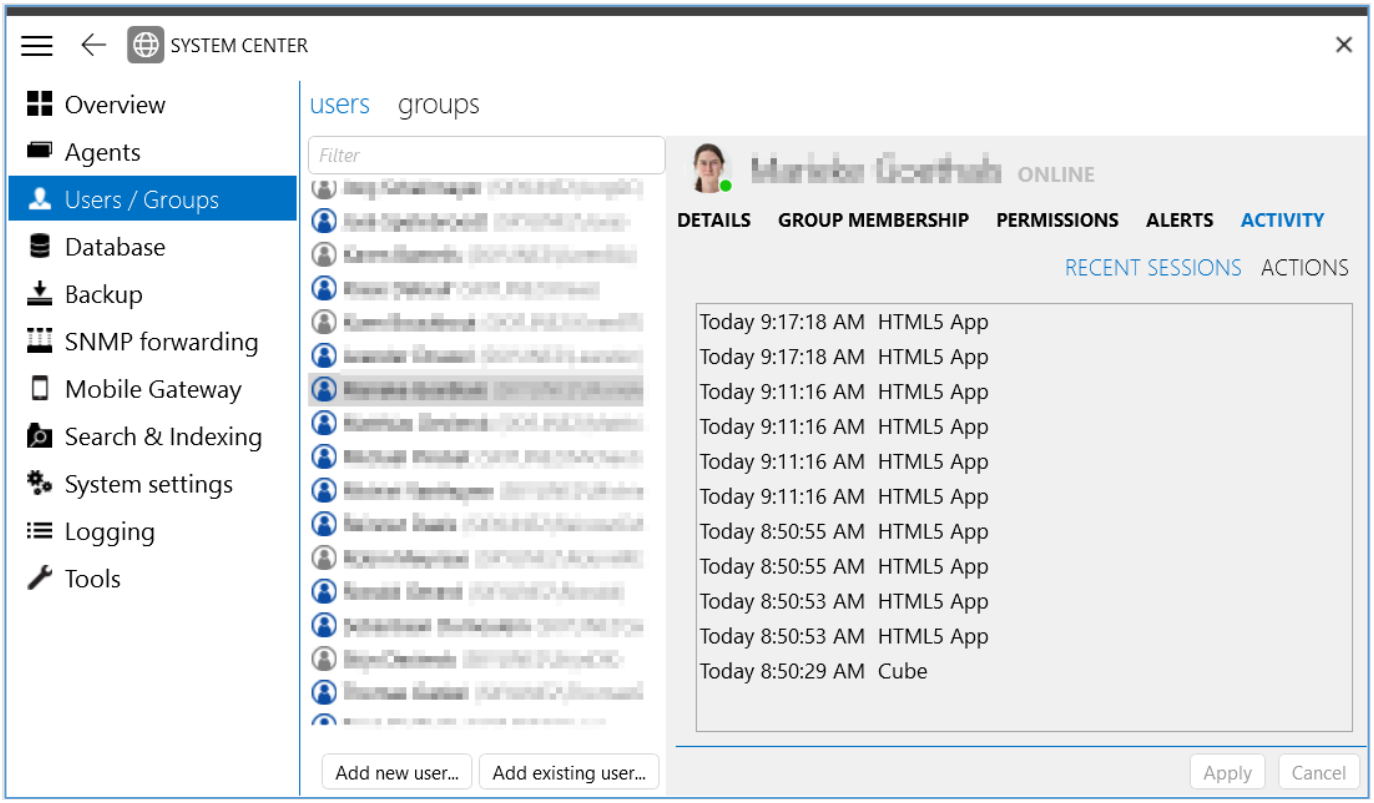
- *Details* tab: Allows you to specify the name of the group and to set a *Group level*, i.e. the parameter access level of the group, where 5 is the lowest level and 1 is the highest level with the most rights.
- *Users* tab: Allows you to add and remove users in a local group. The users in a domain group are configured at domain level, not within the Meinberg Network Management System.
- *Permissions* tab: Consists of two subtabs:
  - *Rights*: Allows you to select which aspects of the system the users in the group can use, e.g. whether the Surveyor is available to them, whether they can edit profiles in the Profile Manager module, etc. A drop-down list with presets at the top of the list allows you to quickly apply pre-configured profiles.
  - *Views*: Allows you to select which views in the Surveyor the users in the group have access to. If access is denied for a particular view, all items within that view will also be inaccessible.
- *Alerts* tab: Allows you to configure notifications for all users in the group, to warn them in case specific alarms occur. To do so:
  - In the *Delivery types* column, select *email*. SMS notifications are not supported.
  - In the *Filters* column, right-click to add an existing filter or create a new filter, which will determine when notifications are sent.

Above these columns, the *Alarm storm prevention* section allows you to customize when notifications should temporarily not be sent because there are too many alarms in a short time period. Any settings you specify there override the general alarm storm settings, which you can access via *System Center* > *System Settings* > *Notifications alarm storm prevention*.

NOTE: If you have changed any settings on this page, make sure you click the *Apply* button in the lower right corner to apply your changes.

8.2 User configuration

To some extent, individual users can also be configured outside of groups. To access these settings, go to the *users* tab on the *Users / Groups* page.



To add an individual user, two buttons are available:

- *Add new user*: Adds a new local user. Clicking the button will open a window where you need to specify at least the *Name*, *Password* and *Confirm password* fields.
    - User names may not start or end with a backslash "\" character. They may also not contain more than one percentage "%" character.
    - The maximum length of a user name is 20 characters.
    - User name validation is not case sensitive. If, for example, a user named "John" has already been added, it will not be possible to add another user named "john" or "JOHN".
    - The *Email* must be filled in for the user to be able to receive email notifications or automated email messages.

- The *Level* field determines the user's parameter access level, in case this is different from the user's group access level. Access levels range from 1 (highest level) to 5 (lowest level).
- To force the user to change the password the next time they log on to the system, select *User must change password at next login*.
- If you want to prevent the password from being changed, select *User cannot change password*.
- To ensure that the password does not expire, select *Password never expires*.

- *Add existing user*: Adds an existing user from the domain. Clicking the button will open a window where you need to select the user or users you wish to add. Personal details for existing users, such as the email and password, are determined at domain level.

The different kinds of users are indicated with different icons in the list of users:

Local user: Entirely managed via the client app.

Domain user. If the user was added by adding the domain group, all personal details for this user are managed by the domain. If the user was added individually, only the user name and password are managed by the domain, while other personal details, such as email and telephone number, can be managed in the client app.

To remove a user, right-click the user in the list and select *Delete*. This is only possible for individually added users.

When a user is selected, five tabs with settings and information are available for this user:

- *Details* tab: This tab displays the personal settings for the user, including the full name, email, and password. For individually added users, these settings can be modified. For all users, you can also specify an access level of 1 to 5 in the *Override level* box, in order to override the group access level for this user.
- *Group membership* tab: In this tab, you can view and change the group or groups the user is a member of. To make changes, select a group in the *Available groups* or *Included in groups* column and use the *Add* or *Remove* button to move it to the other column.
- *Permissions* tab: Consists of two subtabs with information:
  - *Rights*: Shows which aspects of the system the user has permission to use, e.g. whether the sidebar is available to them, whether they can edit alarm templates, etc.
  - *Views*: Shows which views in the Surveyor the user has access to.

  The information in this tab depends entirely on the configuration of the group or groups the user is a member of, and can only be modified at group level.
- *Alerts* tab: Allows you to configure notifications for this user only, to warn them in case specific alarms occur. To do so:
  - In the *Delivery types* column, select *Alerter*, *email*, or *SMS*. Depending on your setup, some delivery types may not be available. (For more information on Alerter, see section 9.2)

- In the *Filters* column, right-click to add an existing filter or create a new filter, which will determine when notifications are sent.

  Above these columns, the *Alarm storm prevention* section allows you to customize when notifications should temporarily not be sent because there are too many alarms in a short time period. Any settings you specify there override the alarm storm settings for the group and the general alarm storm settings, which you can access via *System Center* > *System Settings* > *Notifications alarm storm prevention*.

- *Activity* tab:

  This tab consists of two subtabs.

  - *Recent sessions* shows when the user has logged on to the system and which application was used.
  - *Actions* shows a detailed log of all actions the user has taken.

NOTE:	If you have changed any settings on this page, make sure you click the *Apply* button in the lower right corner to apply your changes.

8.3 Disconnecting a user

Users who have been granted the permission *Disconnect other users* can disconnect other users from the system.

To do so:

1. Click the current user in the top-right corner of the screen.
2. In the *Contacts* list, right-click the user you want to disconnect.
3. In the shortcut menu, select either to disconnect either one specific session or to disconnect all sessions of the user.
4. In the *Motivation* box, enter the reason why the user is disconnected, and click *OK*.

8.4 Assigning user settings to a user group

All users who log on to the client app can personalize their client user settings. However, default settings can be assigned to a group of users, and optionally some settings can be hidden or locked at group level, so that users within that group cannot see or change these settings.

To assign settings to a group of users:

1. In the client user interface, open the *Settings* window in one of the following ways:
   - Click the Apps button in the sidebar, and select *Settings*.
   - Click the user icon in the header bar, and click *Settings*.
2. In the lower-left corner of the *Settings* card, click the button *Configure group*. This button is only displayed if you have the necessary permissions to configure groups.
3. In the *Group settings* dialog box, select the group to which you want to assign settings, and click *Assign*.

4. In the *Create settings for group* dialog box, you can either:
    - Select *New settings*, if you want to assign a new set of user settings containing only factory defaults.
    - Select *Copy settings from* and select a user group from the list, if you want to copy the set of user settings from that user group to the user group you selected earlier.
5. Click *OK* to close the dialog box.

In the *Group settings* dialog box, you can then configure the settings assigned to the group:

1. Select the group for which you want to configure the settings, and click *Open*.
2. Go through the pages of the group settings, and set the settings to the default value you want to apply to the group. The following options are also available:
    - Click the lock icon next to a setting to make sure users will not be able to change this setting.
    - Click the eye icon next to a setting to hide the setting from the users. When the icon shows a line across the eye, the setting is hidden.
    - For the alarm console, you can select the option *Enforce Alarm Console pages*. When you do so, users will not be able to remove the enforced tab pages or change any filters that are applied to them, but they will be able to change settings via the alarm console menu. If you do not want them to be able to change these settings either, also select the check box *Enforce Alarm Console tab page settings*.
3. Click *OK* to close the window and apply the settings to the group.

NOTE: For more information on the different settings, refer to section 7.1.

---

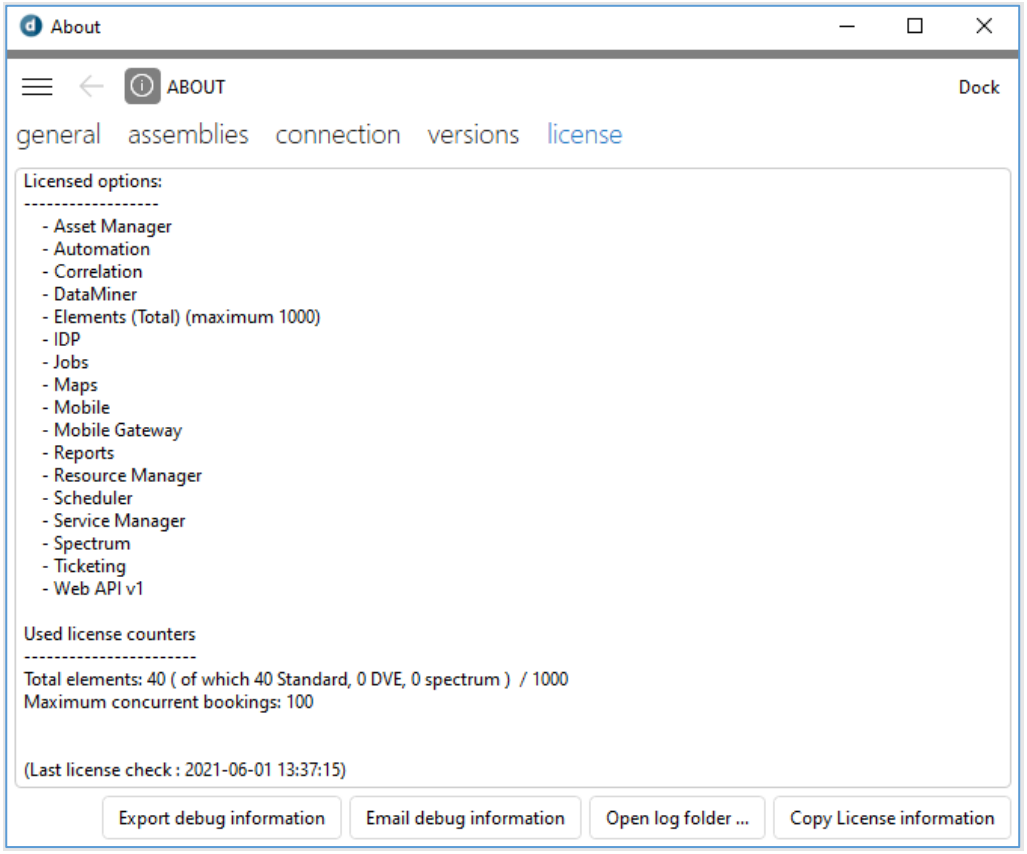
9 Miscellaneous

9.1 Consulting licensing information

As the license only supports a limited number of elements, it can be useful to check the licensing information in order to see how many elements you can still add to the Meinberg Network Management System.

To view license information:

1. Click the user icon in the header bar, and click *About*
2. In the *About* window, go to the *license* tab.



At the top of the window, the *Licensed options* are listed, i.e. the optional modules of the client software for which a license is available. Below this, the used license counters

Below this, the *Used license counters* section displays both the total number of items supported by your license and the current number of items.

Whether a device is included in the license count depends on the type of device and the configuration:

- For the LANTIME non-modular series, each device corresponds with a DataMiner element that is included in the license count. The same goes for the microSync HR/RX series.
- For the LANTIME modular series, only the chassis and the managed cards are included. This means that when you activate a card, it is included in the license count, but it is removed if you deactivate it.

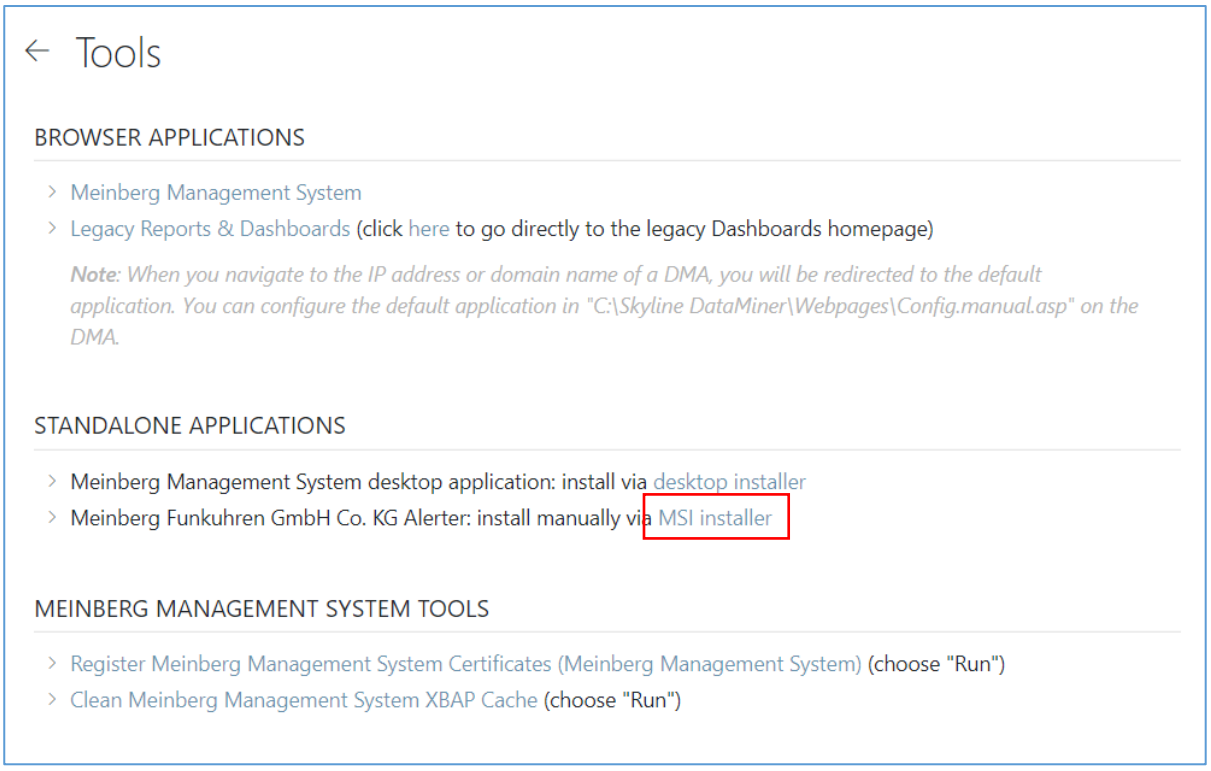
9.2 Working with the Alerter app

Alerter is a small application that can be installed on a client machine. It installs an icon in the system tray and maintains a lifeline with the Meinberg Network Management System. It will make sure you are notified whenever relevant events occur in the system.

9.2.1 Installing the Alerter app

To install the app:

1. Browse to *http://[your Meinberg server]/tools*.
2. Click the MSI installer link for Alerter.



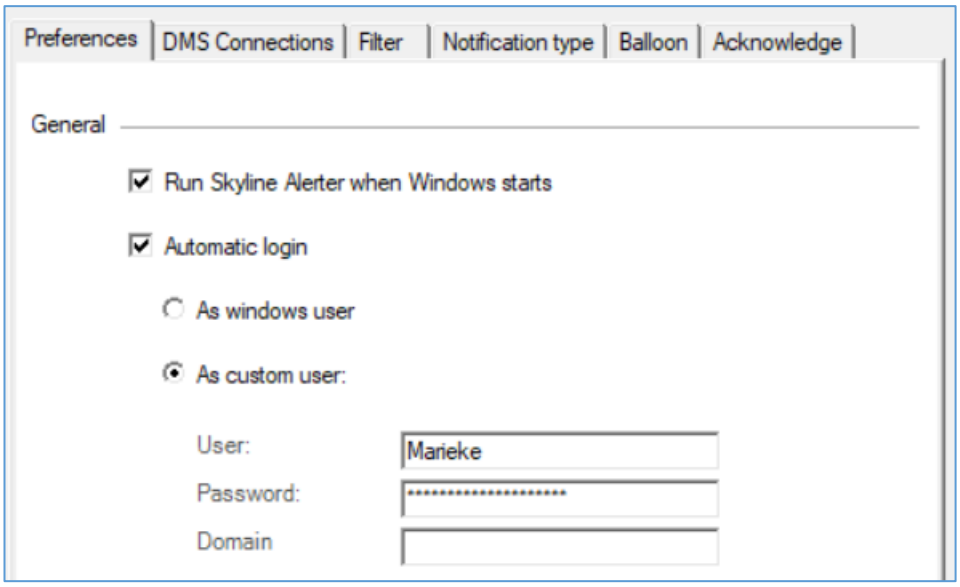
3. Open the downloaded file.
4. In the wizard, click *Next*.
5. Specify the installation folder, select whether only you should have access to the application or other users as well, and click *Next*.
6. Click *Next* again to start the installation.
7. When the installation is complete, click *Close* to exit the wizard.

9.2.2 Setting up the Alerter app

When you first open the app, you will need to specify the server you want to connect to as well as the credentials you will use to connect to it.

Once that is done, you can further configure the Alerter settings by clicking *Settings* in the top right corner. This will open a window with 6 tabs. Configure the settings in these tabs according to your preferences, and then click *OK* to close the window.

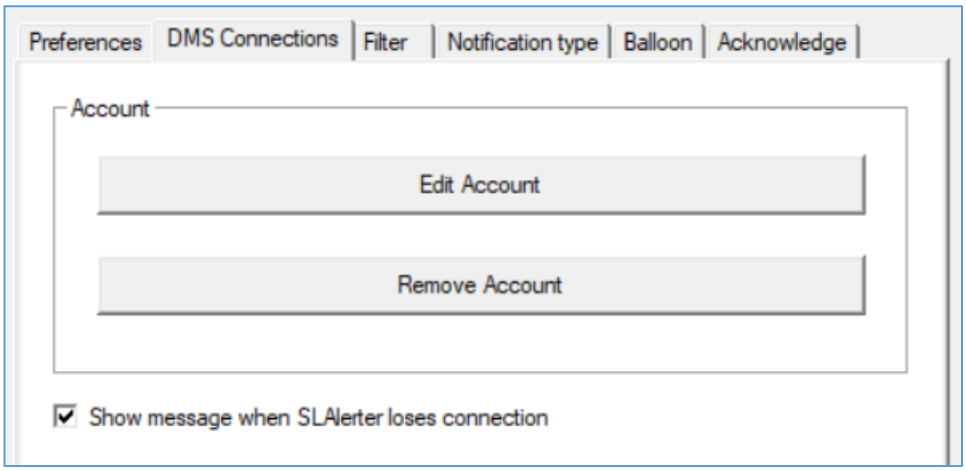
9.2.2.1 The Preferences tab



This tab allows you to configure your startup preferences for the app:

- *Run Skyline Alerter when Windows starts*: Select this checkbox to start the app automatically when your computer starts up.
- *Automatic login*: Select this option to automatically log in. If you select *As windows user*, your Windows credentials will be used. Otherwise, custom credentials will be used.

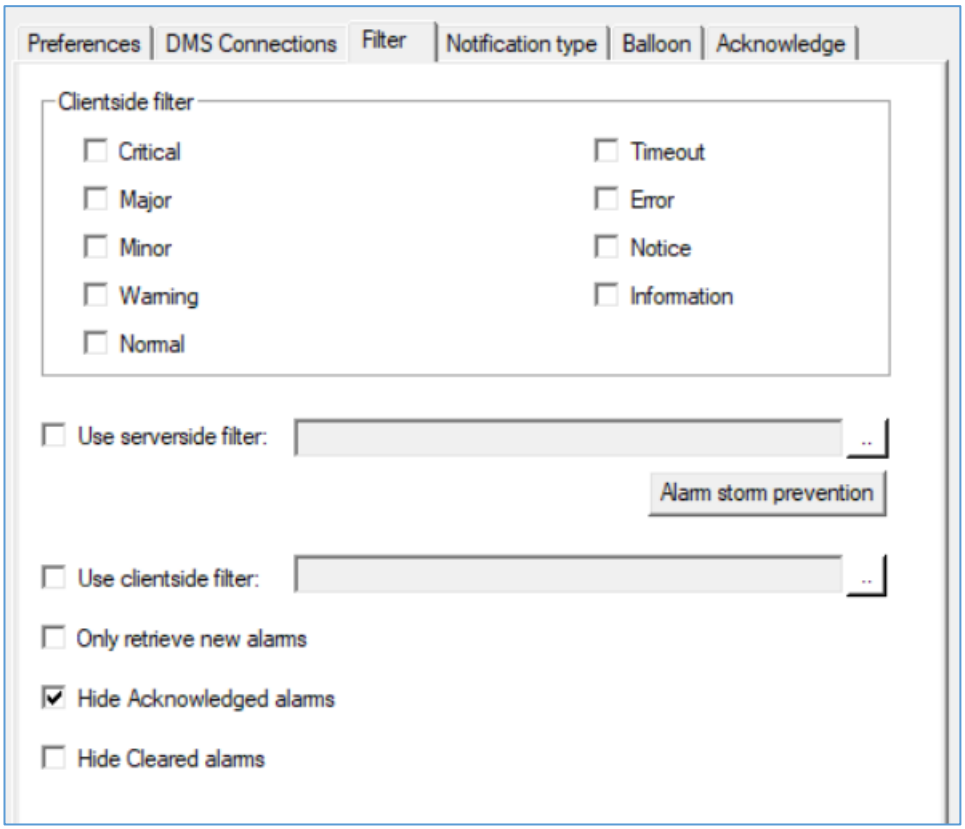
9.2.2.2 The DMS Connections tab



This tab allows you to change how you connect to the system.

- *Edit Account*: Opens a window where you can specify a name for the connection and then change the IP or hostname you connect to. Via the *Advanced* button, you can fine-tune additional connection settings.
- *Remove Account*: Removes the account you are currently using. This means your connection will be lost, and you will need to specify the server and credentials again to access the system.
- *Show message when SLAlerter loses connection*: Select this checkbox to get a notification if the connection to the system is lost.

9.2.2.3 The *Filter* tab

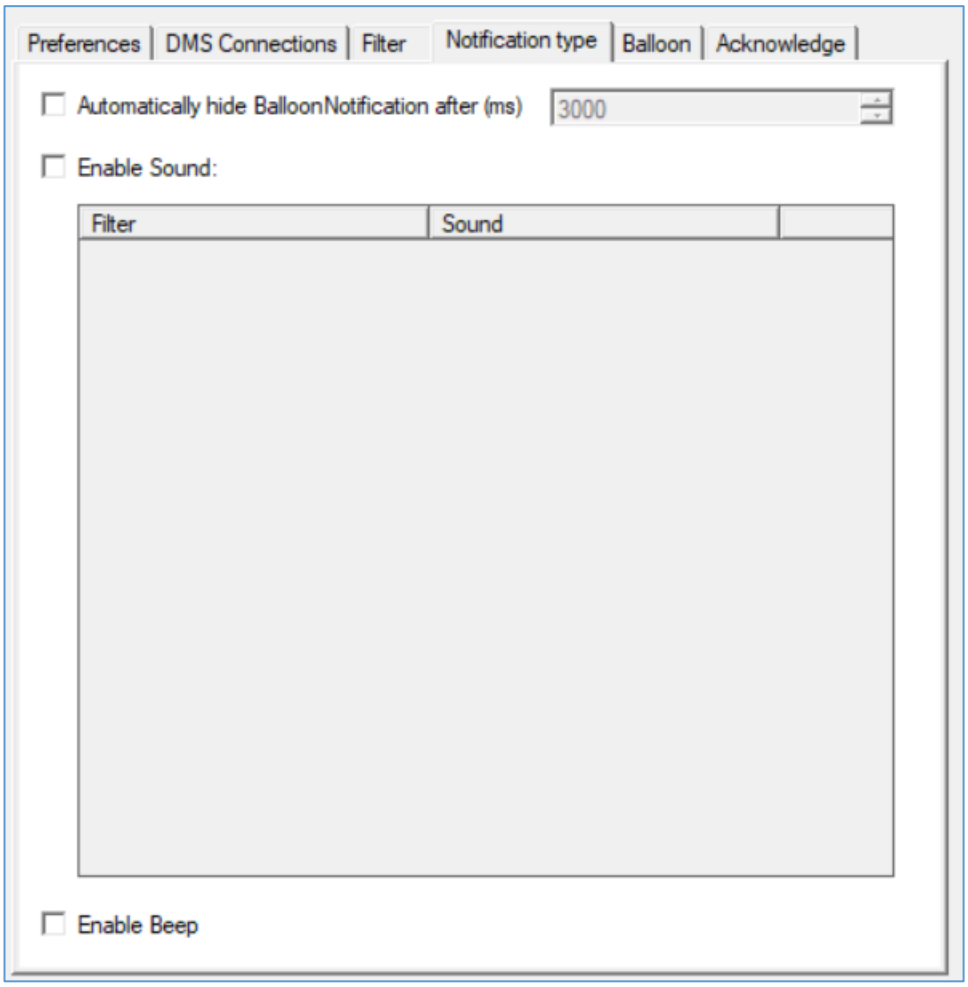


This tab allows you to fine-tune for which alarms you will receive notifications.

- *Client-side filter*: Allows you to configure a client-side severity filter, by selecting the severities for which an alert should be displayed. Though this will not stop alarms from entering the Alerter Alarms list, only the alarms with the selected severities will generate alerts.
- *Use server-side filter*: If you select this option, click the ellipsis button on the right, and select one or more of the available alarm filters. Only alarms matching the alarm filters will be sent to Alerter.
- *Use client-side filter*: If you select this option, click the ellipsis button on the right, and select one or more of the available alarm filters. Though all alarms will be sent to Alerter, only alarms matching the alarm filters will generate an alert. If you combine this option with the first *Client-side filter* option, alerts will only be generated for alarms that match the selected filters and have the selected severities.
- *Only retrieve new alarms*: Select this option to not get notified of alarms that already exist at the moment when you connect to the DMS.
- *Hide acknowledged alarms*: If you select this option, when Alerter receives an alarm that is acknowledged (i.e. an alarm that someone has taken ownership of), that alarm will still be added to the Alarms list, but no alert will be generated, even if the alarm matches the client-side filters.
- *Hide cleared alarms*: If you select this option, when Alerter receives an alarm that is cleared, that alarm will still be added to the Alarms list, but no alert will be generated, even if the alarm matches the client-side filters.

NOTE: Alerter never displays notifications for masked alarms.

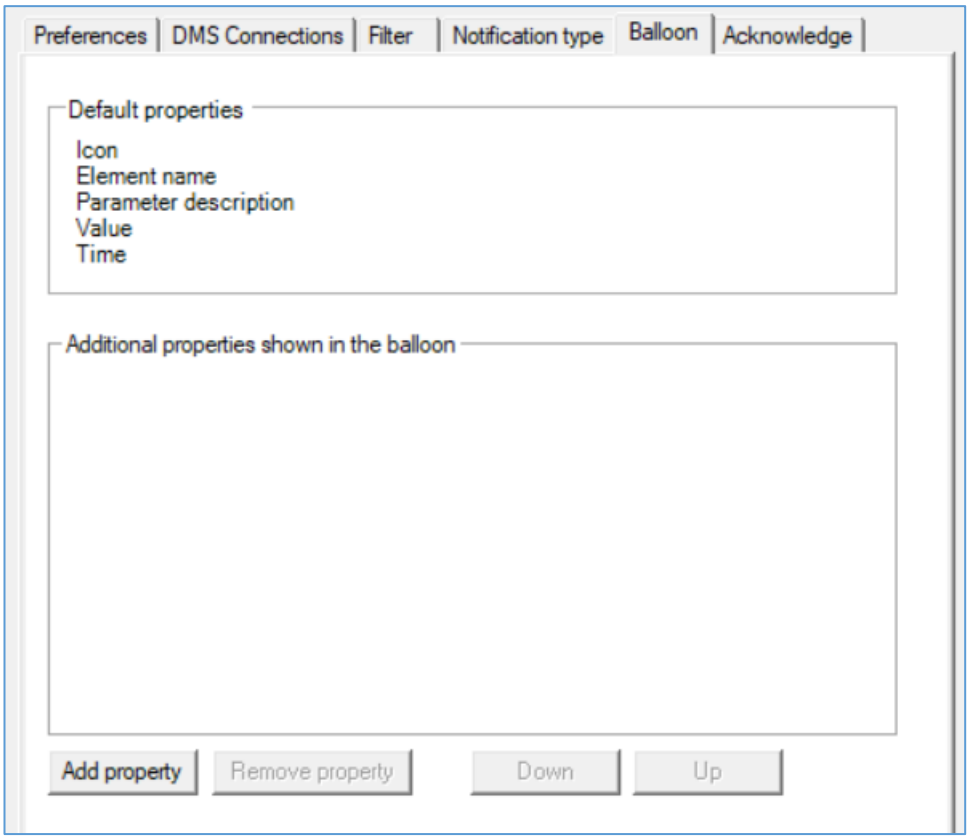
9.2.2.4 The Notification type tab



This tab allows you to customize the Alerter notifications:

- *Automatically hide balloon notification*: Select this option to make the notifications disappear after the specified number of milliseconds.
- *Enable Sound*: To play a custom sound for specific notifications, select this option and use the right-click menu to add a filter and corresponding .wav file.
- *Enable Beep*: Select this option to hear a generic beep whenever a notification appears.

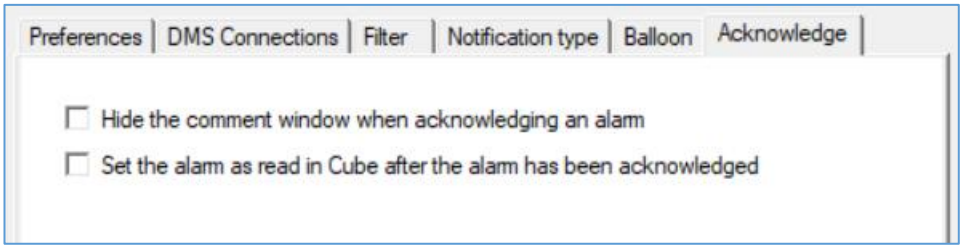
9.2.2.5 The *Balloon* tab



This tab allows you to add additional properties to the notifications and customize the order in which these are shown.

The default properties displayed at the top of the tab cannot be modified.

9.2.2.6 The Acknowledge tab

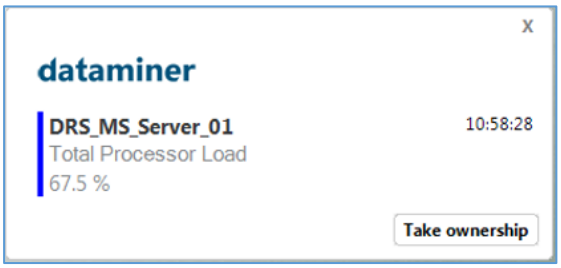


This tab allows you to fine-tune what happens when an alarm is acknowledged via an Alerter notification:

- *Hide the comment window when acknowledging an alarm*: Select this option if you do not want the default comment window to be displayed when you take ownership of an alarm.
- *Set the alarm as read in Cube after the alarm has been acknowledged*: Select this option to display the alarm as read in the Meinberg Network Management System if you take ownership of it using Alerter.

9.2.3 Working with Alerter notifications

The Alerter app will display a notification box whenever an alarm occurs in the system that matches the configured filters in the Alerter settings.



The notification displays the severity of the alarm with a colored bar on the left. For more information on the severity levels, see section 3.1.

It will also display the different properties of the alarm, as configured in the Alerter settings.

Each notification contains a *Take ownership* button. Click this button to immediately acknowledge the alarm and signal to other users that you intend to take care of the problem.

9.3 Support procedure

To raise a support ticket, you will first need to gather the necessary information and then send an email to the correct addresses.

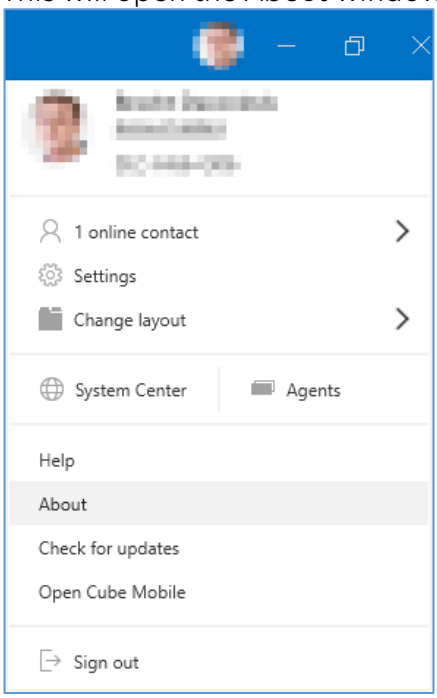
9.3.1 Collecting the necessary information

You will need to gather both information about DataMiner and about the Meinberg Network Management System.

DataMiner information

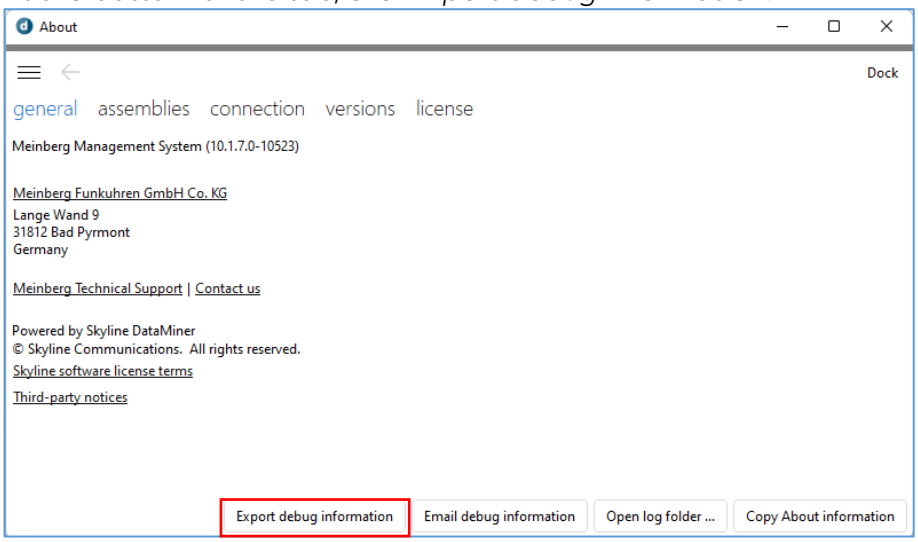
Collect the necessary DataMiner information by following the steps below.

1. Log in to DataMiner Cube.
2. In the header bar, click the user icon and select *About*.
   This will open the *About* window.

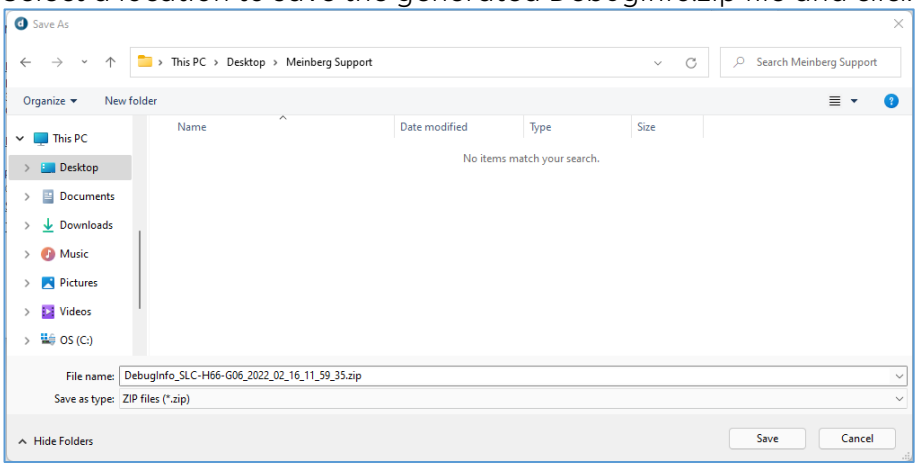


3. In the *About* window, go to the *general* tab.

4. At the bottom of the tab, click *Export debug information*.



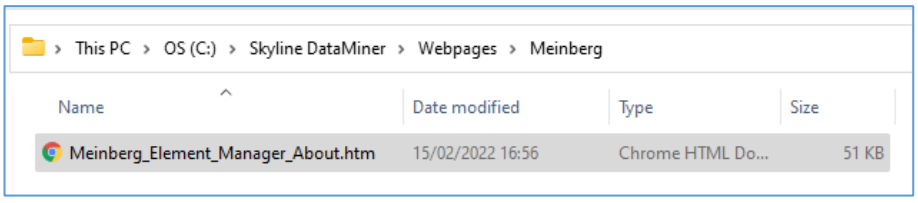
5. Select a location to save the generated DebugInfo.zip file and click *Save*.



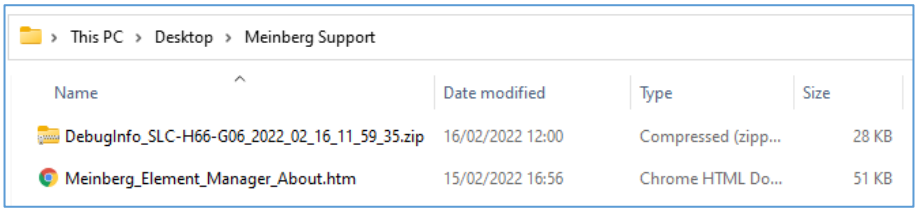
Meinberg Network Management System information

Collect the necessary mbgNMS information by following the steps below.

1. On the DataMiner server, locate the *Meinberg_Element_Manager_About.htm* file. This file is usually located in the folder *C:\Skyline DataMiner\Webpages\Meinberg*.



2. Copy the *Meinberg_Element_Manager_About.htm* file to the location where you saved the DataMiner information.



9.3.2 Raising a ticket

To raise a ticket:

1. Include all the information gathered in the previous section in an email.
2. Send the email to support@meinberg.de, with the following address in cc: meinberg.dataminer.team@skyline.be.

10 Recent changes

REV007	Required software version changed to 10.1.7 in installation procedure.
REV008	Support procedure added.
REV009	Required DataMiner version replaced with link to DataMiner Dojo page containing this info for all Meinberg Element Manager versions.
REV010	Updated installer download link. Added LANTIME M150/M250/M320/M350/M450 to supported devices.
REV011	Updated system requirements to install client app on client computer.
REV012	microSync added to supported devices
REV013	IMS-GXL and IMS-PSX210 added to supported devices
REV014	- Installation procedure updated - Supported devices updated: format module names corrected and IMS-LSG added - *Settings* page info for Meinberg Element Manager updated
REV015	Meinberg Element Manager pages updated to new page structure