PROCESS AUTOMATION

My Control System (on-premise) Operation

User Manual

Notice

This document contains information about one or more ABB products and may include a description of or a reference to one or more standards that may be generally relevant to the ABB products. The presence of any such description of a standard or reference to a standard is not a representation that all of the ABB products referenced in this document support all of the features of the described or referenced standard. In order to determine the specific features supported by a particular ABB product, the reader should consult the product specifications for the particular ABB product.

ABB may have one or more patents or pending patent applications protecting the intellectual property in the ABB products described in this document.

The information in this document is subject to change without notice and should not be construed as a commitment by ABB. ABB assumes no responsibility for any errors that may appear in this document.

Products described or referenced in this document are designed to be connected and to communicate information and data through network interfaces, which should be connected to a secure network. It is the sole responsibility of the system/product owner to provide and continuously ensure a secure connection between the product and the system network and/or any other networks that may be connected.

The system/product owners must establish and maintain appropriate measures, including, but not limited to, the installation of firewalls, application of authentication measures, encryption of data, installation of antivirus programs, and so on, to protect these products, the network, its system, and interfaces against security breaches, unauthorized access, interference, intrusion, leakage, and/or theft of data or information.

ABB performs functionality testing on the products and updates that we release. However, system/product owners are ultimately responsible for ensuring that any product updates or other major system updates (to include but not limited to code changes, configuration file changes, third-party software updates or patches, hardware change out, and so on) are compatible with the security measures implemented. The system/product owners must verify that the system and associated products function as expected in the environment in which they are deployed.

In no event shall ABB be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall ABB be liable for incidental or consequential damages arising from use of any software or hardware described in this document.

This document and parts thereof must not be reproduced or copied without written permission from ABB, and the contents thereof must not be imparted to a third party nor used for any unauthorized purpose.

The software or hardware described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license.

This product meets the requirements specified in EMC Directive 2014/30/EU and in Low Voltage Directive 2014/35/EU.

Trademarks and copyright

Release: October 2023

Document ID: 2PAA122516

Revision: V

Table of contents

1. Introduction

My Control System (on-premise) is a part of the Advanced Digital Services offering from ABB. This document is intended to provide assistance in the use of MCS-OP.

This manual does not discuss the settings and process for collecting the necessary data with the My Control System - Data Collector (MCS-DC). For details on the collection process refer to document ref. [1] & [2].

1.1. General (Introduction & main functions)

My Control System (on-premise) is a standalone secure service delivery platform that provides information in a central location.

It uses data collected during scheduled and on demand analyses for comparison against best practices and standards to detect performance irregularities and provides the user with standardized views of Key Performance Indicators (KPIs).

This comparison quickly pinpoints issues, helping to improve system reliability, availability, and performance. Automated e-mail notifications can be configured based on defined trigger situations to directly inform the users on the latest analysis results.

Depending on the available licenses different functionality is enabled within the platform. E.g. having an active Cyber Security Workplace license available for the system will enable all the relevant functionality within the platform to monitoring the most important parameters related to maintain cyber security standards in your system.

1.2. Used icons

Warning/important notice

Indicates a warning or important notice that must not be ignored.

Informational notice

Indicates additional information which should be read by the user.

1.3. Terminology

Table 1: Terminology

Term	Description
CSM	Control System Monitoring
CSWP	Cyber Security Workplace Functionality hosted by the My Control System on-premise application
DCS	Distributed Control System
ENS	McAfee Endpoint Security
ePO	McAfee ePolicy Orchestrator
FQDN	Fully Qualified Domain Name

Term	Description
KPI	Key Performance Indicator This is a basic item or elementary function of the control system which is checked. It consists of one or more values to be measured and evaluated
MCS	My Control System This is a platform hosting ABB service applications in the ABB Cloud
MCS-DC	My Control System Data Collector Software, which collects data from an installed control system
MCS-FW	My Control System – Forwarder Software, which distributes data collections of MCS-DC to consuming applications like e.g., MCS-OP
MCS-OP MCS on-premise	My Control System (on-premise) application. This is the platform hosting MCS functionality on a customer site
RAP VSE	Remote Access Platform Virtual Security Engine
SDF	System Data File This file consists of relevant raw data collected on site, which is then used to generate data sets
SEPM	Symantec Endpoint Protection Manager
SID	System identifier This is a unique serial number of control systems used by the software license register (SoFa). The system identification number is always written close to the digits, e.g. SID1234
SoFa	Software Factory Global ABB database holding detailed information on ABB software licenses
VSE	McAfee VirusScan Enterprise

1.4. Scope & Software versions

The scope of the document is for installing MCS on-premise as per the supported software versions. In general, MCS on-premise supports all control system versions as supported by the MCS Data Collector. Refer to document ref. [2] for the complete list.

The CSWP feature set supports a limited subset of the control system versions and is supporting:

- ABB System 800xA
  - System 800xA version 6.0
  - System 800xA version 6.1
- ABB Symphony Plus
  - Symphony Plus version 3
  - Symphony Plus version 2.1 and above – excluding the ABB Symphony Plus Collector function
- ABB Freelance
  - Freelance 2016
  - Freelance 2019

For a listing of all supported ABB services / service products and 3rd party products, refer to document ref.[1].

2. Using My Control System (on-premise)

2.1. Sign on to the system

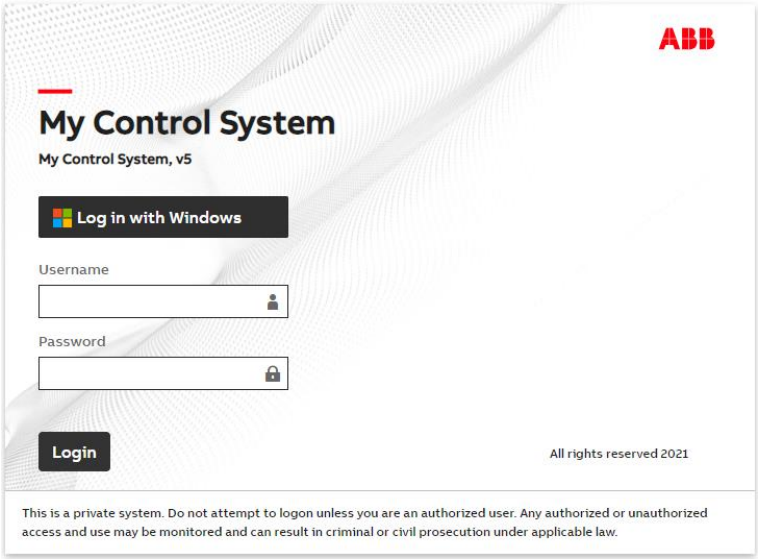


Figure 1: Login screen

When accessing MCS-OP you are asked for your login credentials.

There are 2 options to login:

- via your currently active windows user
- via a dedicated username and password

The windows user needs to be setup first in MCS-OP to be able to log in. This is only applicable for Active Directory user accounts. Refer to document ref. [1] for more information

Keep in mind that due to security reasons, you will be automatically logged out of MCS-OP after 20 minutes of inactivity

Note that the support for Internet Explorer has been dropped by end Q2 2022. We are recommending using Microsoft Edge to access the web portal.

After the successful login the MCS-OP home screen is shown.

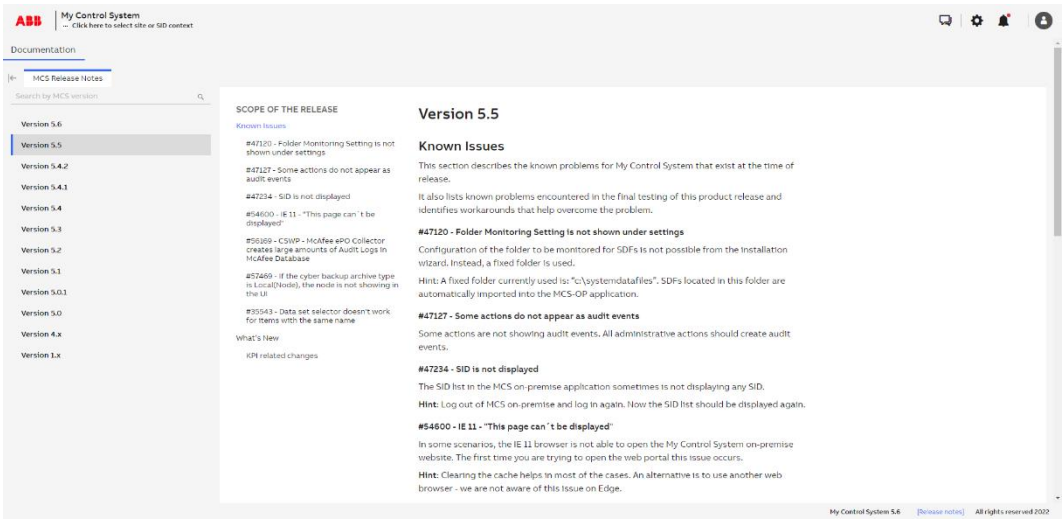


Figure 2: Home screen

Click in the upper left corner on the ABB logo to open the site/SID selector to work with MCS-OP in the correct context.

You can select either site or SID to check the details of your system.

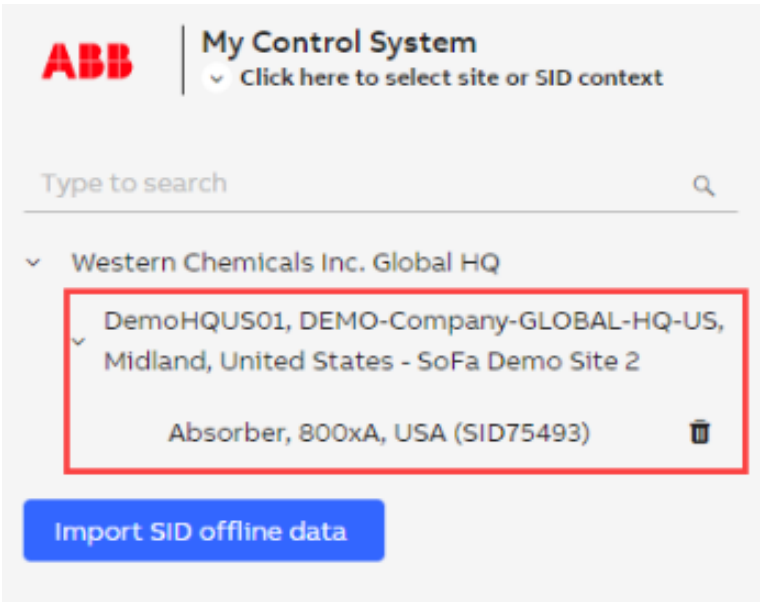


Figure 3: Site/SID selector

2.2. Overview (general layout)

The MCS-OP dashboard consists for 4 major areas:

1. Top navigation bar (Chapter 2.2.1)
2. Filter area (Chapter 2.2.2)
3. Overview area (Chapter 2.2.6)
4. Footer area (Chapter 2.2.3)

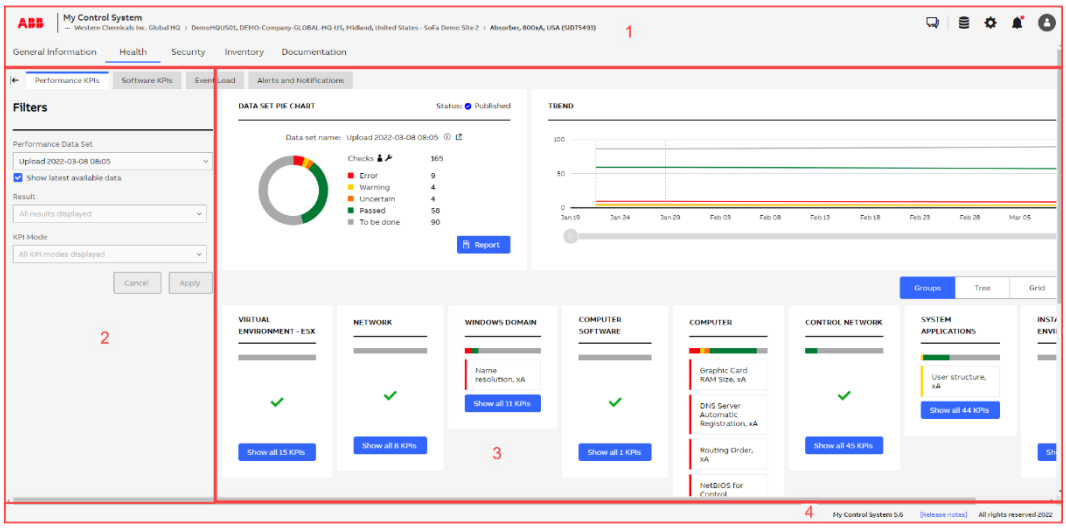


Figure 4: General layout

2.2.1. Top navigation bar

The top navigation bar consists of 3 different sections:

1. SID selector
2. Categories (Chapter 2.2.4 onwards)
3. Administration and configuration (Chapter 2.2.12)

Figure 5: Top navigation bar

Use the top navigation bar to access the different areas (e.g. “Health”). Once an area is selected a second level navigation bar will be displayed (if available for that area).

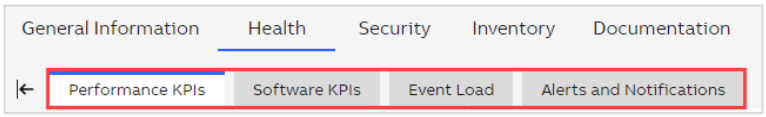


Figure 6: Second level navigation

2.2.2. Filter area

On the left side of the dashboard, you have a selection and filter area to narrow down / modify the results and content that is shown in the overview area.

By default, filter area is detached from the main view. Click on the “Show filters” icon to display it:

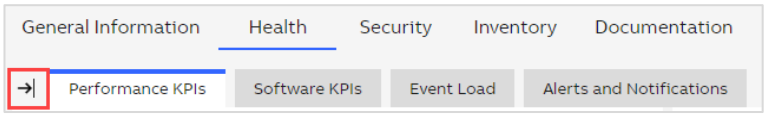


Figure 7: Show filter area

Click on the “Hide filters” icon to hide filter area:

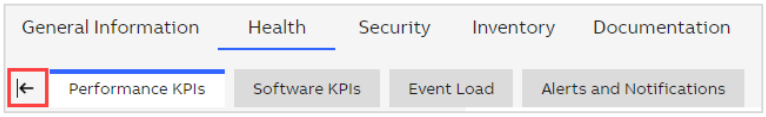


Figure 8: Hide filter area

The visibility of the filter area will be remembered when browsing the application.

Depending on the category you have selected, different filters may apply. In this example the filters for the category Health / Performance KPIs are used

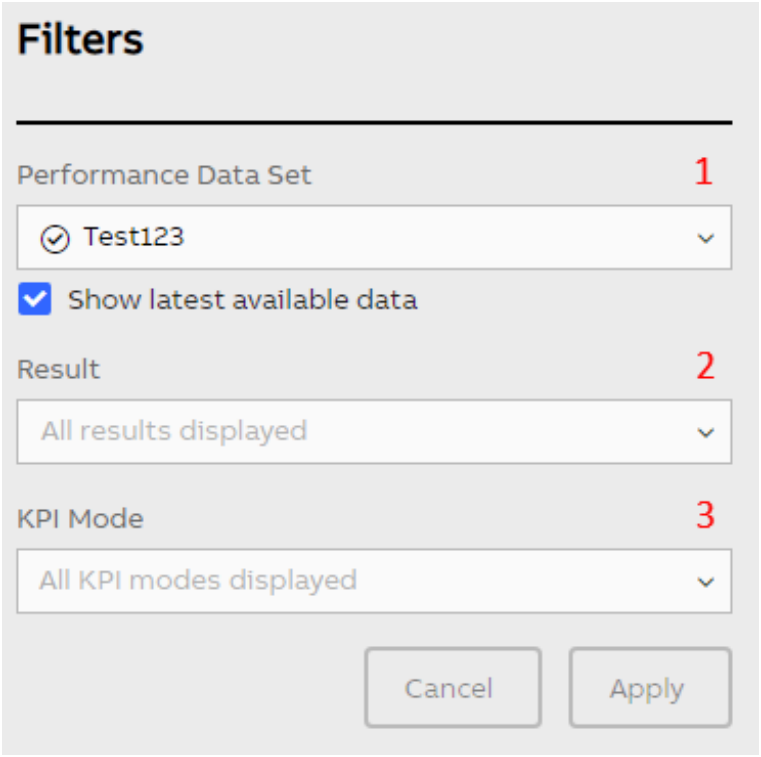


Figure 9: Filter area

1. Data Set selector: Select the data set that you would like to inspect. Only one data set can be selected at any given time. By default, the option “Show latest available data” is enabled.

This means MCS-OP will keep the selected data set when switching between the categories only if data for the category is available. Otherwise, it will automatically select the latest available data for the category, irrespective of the data set it came from. If you want to browse through one specific data set,

this option needs to be disabled. Disabling this option is only kept in the local storage of the browser.

2. Result selector: Select specific KPI results to narrow down what will be displayed in the overview area. This selector allows multiple choice, e.g., you can select “Error” and “Warning” at the same time. If the selector is left empty, all KPIs and their results will be displayed.
3. KPI Mode: Select either automated or manual KPIs. If the selector is left empty, all KPIs will be displayed. This section only appears if you have an active System Assessment license and selected data set is of type “Automated and manual KPIs”.

After you selected your filter, click “Apply”. The page will refresh and display the data you have selected. You can also click “Cancel” to revert any selection you have made to the currently displayed view.

2.2.3. Footer area

Information about the current MCS-OP version is provided in the footer area of the dashboard. In addition, the footer area provides a direct link to the Release notes to be found under category Documentation (Chapter 2.2.11)

Figure 10: Footer area

2.2.4. Categories

MCS-OP uses five different categories to structure all the information that is available for the control system.

1. General Information (Chapter 2.2.5)
2. Health (Chapter 2.2.8)
3. Security (Chapter 2.2.9)
4. Inventory (Chapter 2.2.10)
5. Documentation (Chapter 2.2.11)

2.2.5. General Information

The general information category consists of two tabs:

1. System status or Site status (high level overview about the system or site status of the installed control system)
2. Licenses and Contacts (general information about the installed control system, e.g. licenses and contacts)

2.2.5.1. System Status

The System Status tab gives you a high-level overview about the status of the control system. The KPI analysis results from all categories (Health, Security and Inventory) as well as widgets from other functions are combined within this single dashboard. The dashboard consists of

different widgets representing the different categories / functions (e.g. Performance KPI, Security KPIs, ...).

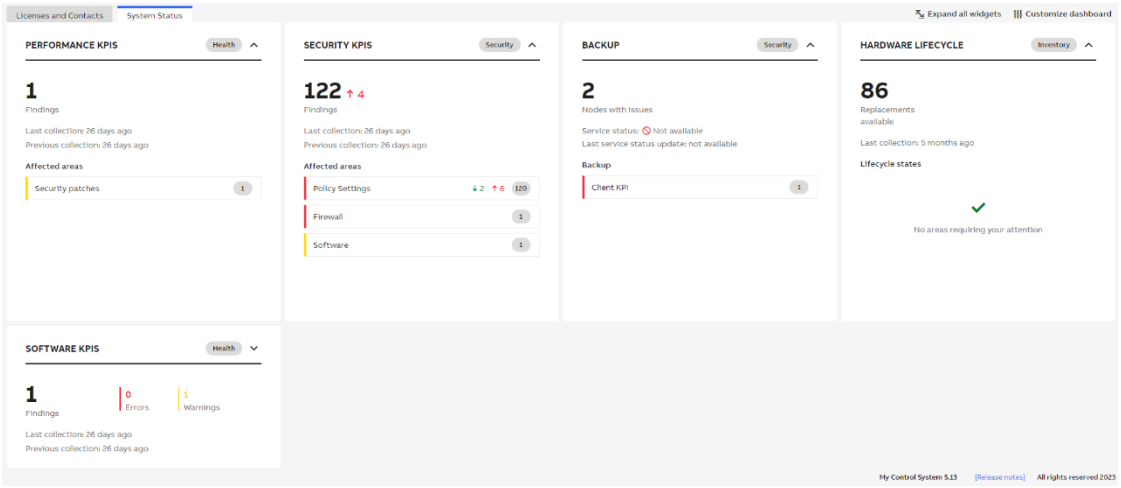


Figure 11: System Status

Each widget has two views (expanded / collapsed) showing a different level of detail. Use the toggle button to switch between the views or click on “Expand all widgets” in the upper right corner.

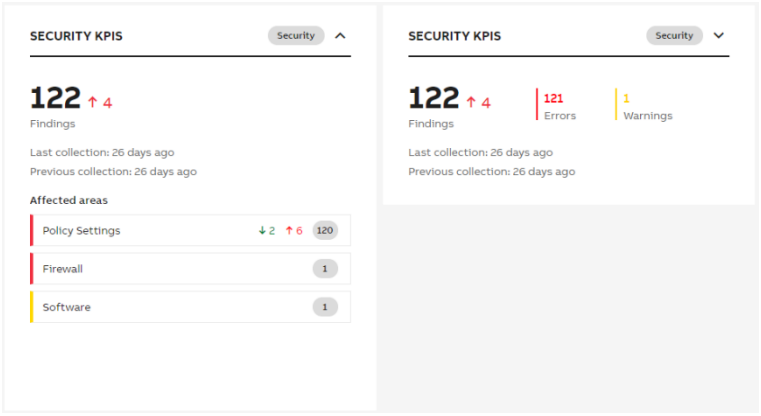


Figure 12: Expanded / collapsed view

Click either on the heading or on the number of findings, to jump to the corresponding KPI analysis of the category.

Click on one of the “Affected areas” (e.g. Firewall) to jump to the KPI analysis of the category using the “Tree view” where the affected area is automatically expanded.

Hover over the indicators in the “Affected areas” to get more information about the changes within this area.

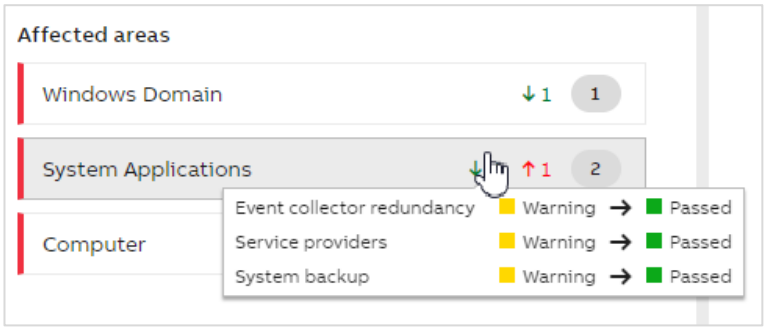


Figure 13: Changes in area

The appearance of the system status tab can be customized. Click on “Customize dashboard” in the upper right corner to start the customization. On the left side of the screen, you have an area where you can do the following adjustments:

– Dashboard Layout (3 or 4 column layout for different screen resolutions)

– Color Theme (Default or High-Performance color theme)

– Widgets (Enabling / Disabling / Expanding / Collapsing widgets)

In addition, the arrangement and order of the widgets can by changed by dragging & dropping the widget to another column or position.

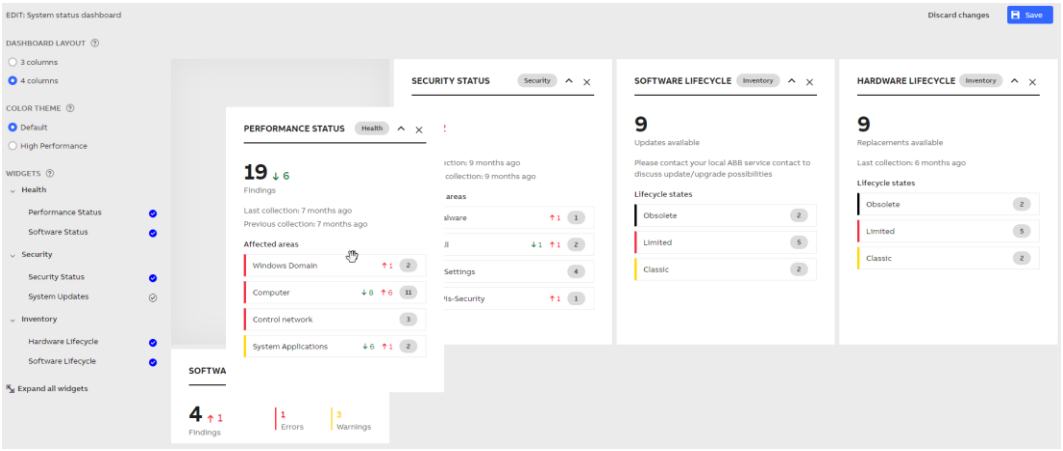


Figure 14: System status customization

2.2.5.1.1. Performance KPIs, Software KPIs and Security KPIs

[1] Performance KPIs, Software KPIs and Security KPIs widgets show the number of findings (errors or warnings) in the latest data set with the trend indicator and difference compared to the previous data set. Number of KPIs which have worsened and improved is presented in the tooltip.

[2] Information about the latest and previous collections is presented below with more details on hover.

[3] Red label next to the “Affected area” indicates there is at least 1 error whereas yellow one shows there are no errors but at least 1 warning in the specific KPI category. The number of all findings in each category is displayed in the grey label on the right side. Next to that, trend indicators and more details in the tooltip are shown.

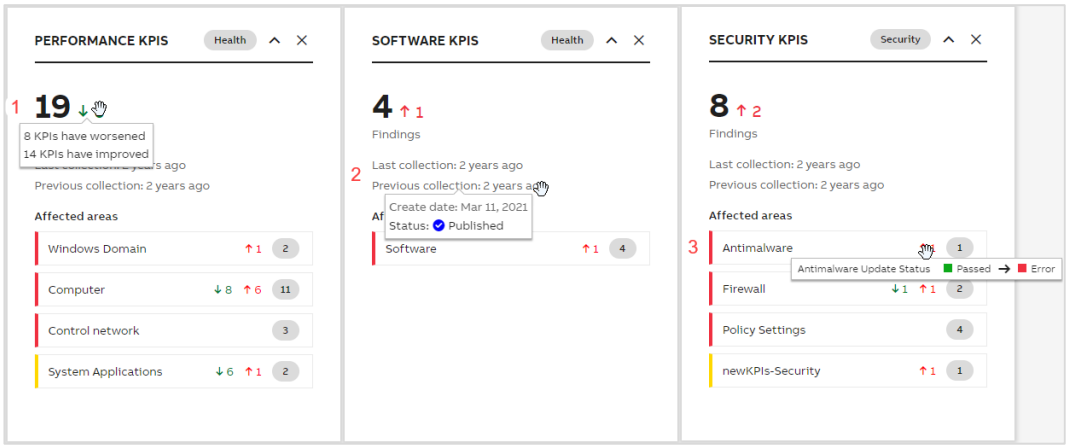


Figure 15: Performance KPIs, Software KPIs and Security KPIs widgets

2.2.5.1.2. Event Load and Alerts and Notifications

Event Load as well as Alerts and Notifications widgets present CSM data.

[1] Sum of critical and high events from last 31 days.

[2] Number of critical or high events from last 31 days listed separately based on the severity.

[3] Information of the time period for which data is presented.

[4] Trend showing the number of critical (in red) and high (in orange) number of events from last 3 months

[5] Sum of notifications with critical or high severity from last 31 days

[6] List of “Affected areas” for which notification with critical (red label) or high (orange label) severity has been sent. The sum of notifications with critical or high severity in each category is displayed in the grey label on the right side.

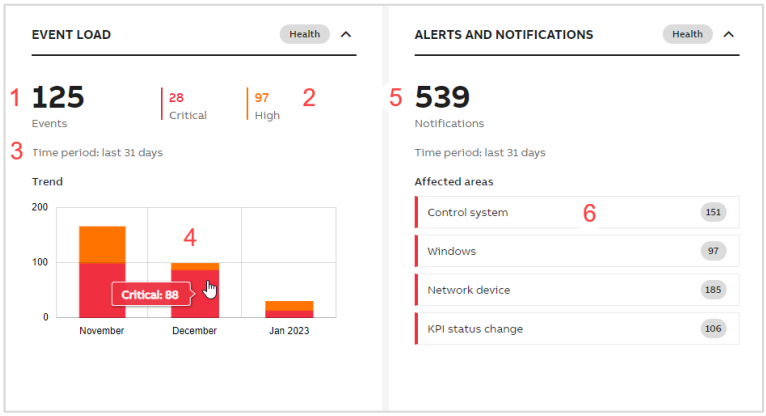


Figure 16: Event Load and Alerts and Notification widgets

2.2.5.1.3. Malware Protection, Security Updates and Backup

[1] Malware Protection, Security Updates and Backup widgets show the number of nodes with issues (errors or warnings).

[2] Information about the service status and its last update is presented below with more details on hover. If ABB My Control System – Data Collector modules (Malware Protection or Security Updates type) is enabled, this data on the respective widget is replaced with last MCS-DC collection information.

[3] Red label indicates there is at least 1 error whereas yellow one shows there are no errors but at least 1 warning in the specific KPI category. The tooltip presents the description of the KPI category. The number of all findings in each category is displayed in the grey label on the right side.

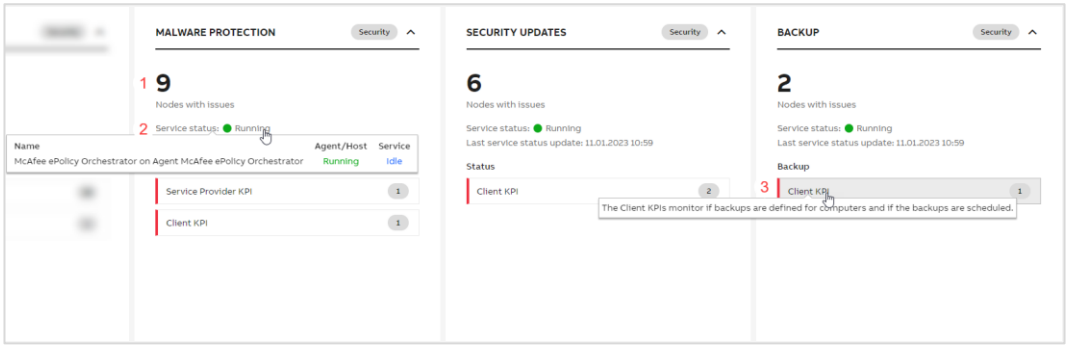


Figure 17: Malware Protection, Security Updates and Backup widgets

2.2.5.1.4. Hardware Lifecycle

[1] Hardware Lifecycle widget show the sum of devices in Obsolete, Limited or Classic lifecycle phase with available replacement.

[2] Information about the last collection is presented below with more details on hover.

[3] “Lifecycle states” section indicates the number of devices with available replacements in each lifecycle phase.

Figure 18: Hardware Lifecycle widget

2.2.5.1.5. Assets

[1] Assets widget indicates the number of active assets from the current day. This will ensure that dormant assets are picked up when becoming active again. Next to the number of active assets difference between the current day and the previous day is displayed with an arrow indicating the trend.

Total amount of assets which are detected and listed in the asset overview could be different.

[2] Activity index is displayed only in case it is critical (red) or high (orange). The thresholds can be set in the Activity index widget available on Assets tab under Settings.

[3] The service status is available with information when it was updated.

[4] The activity trend is visible in the expanded version of the widget and shows the changes from the last 15 days.

Activity index, details about the service status and activity trend are displayed in the MCS-OP if the selected SID has active Cyber Asset Inventory license and Passive Network Monitoring application has been installed.

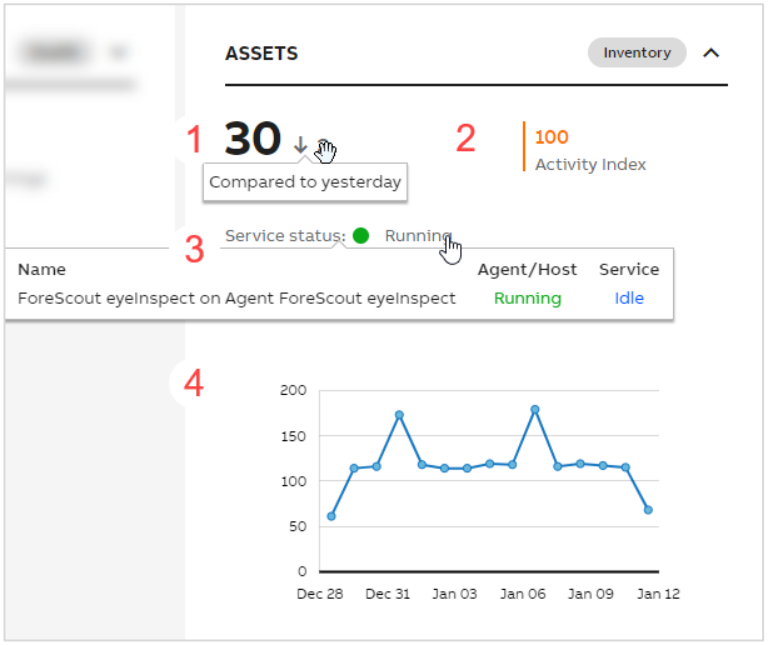


Figure 19: Assets widget

2.2.5.2. Site Status

The Site Status tab works in the similar way as System Status but gives you a high-level overview about the status of the whole site.

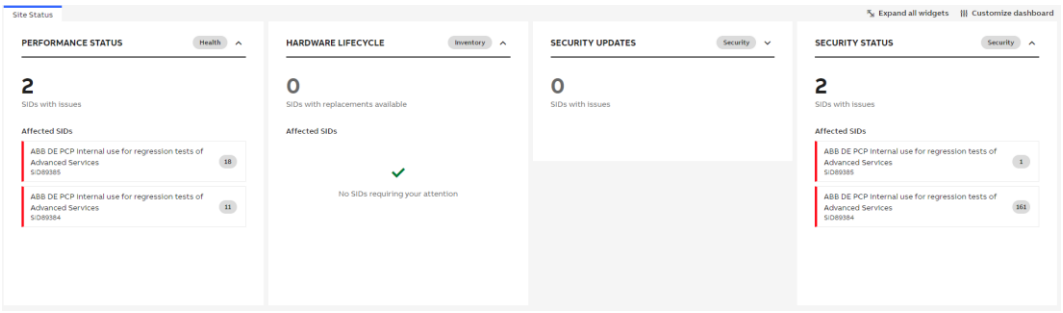


Figure 20: Site Status

Under “Affected SIDs” you will see the list of all SIDs which require your attention.

The color of the label matches the worst result for the listed SID but you can hover over the indicator with the total number of findings to check the details.

Click on one of the “Affected SIDs” (e.g. SID89385) to jump to the KPI tab of the widget’s category.

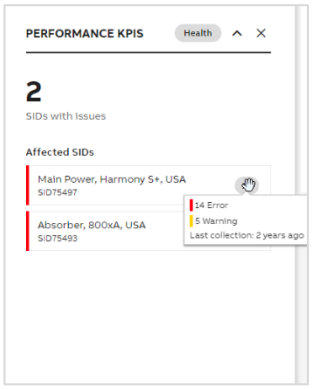


Figure 21: Site status widget

The appearance of the site status tab can be customized independently of the customization of the system status tab.

Assets widget indicates the number of SIDs with high or critical activity index. The list of these SIDs is listed in the expanded version of the widget.
For each SID information about the activity index is available (the color of the label matches the activity index and additionally, a tooltip with the activity index level is available on hover) as well as the number of active assets from the current day.

Total amount of assets which are detected and listed in the asset overview could be different.

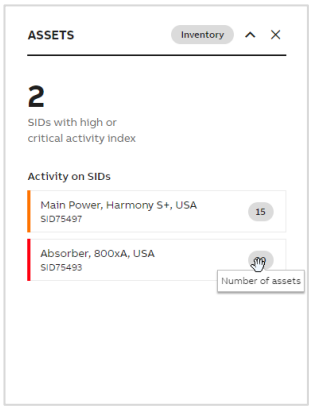


Figure 22: Assets widget

2.2.5.3. Licenses and Contacts

The licenses and contacts tab is available in SID context and consists of three different areas:

- Automation Software Maintenance widget (gives information about the status of your service contract)
- Licenses widget (lists all licenses that are registered for your control system)
- Contact widgets (lists all relevant contacts for your control system)

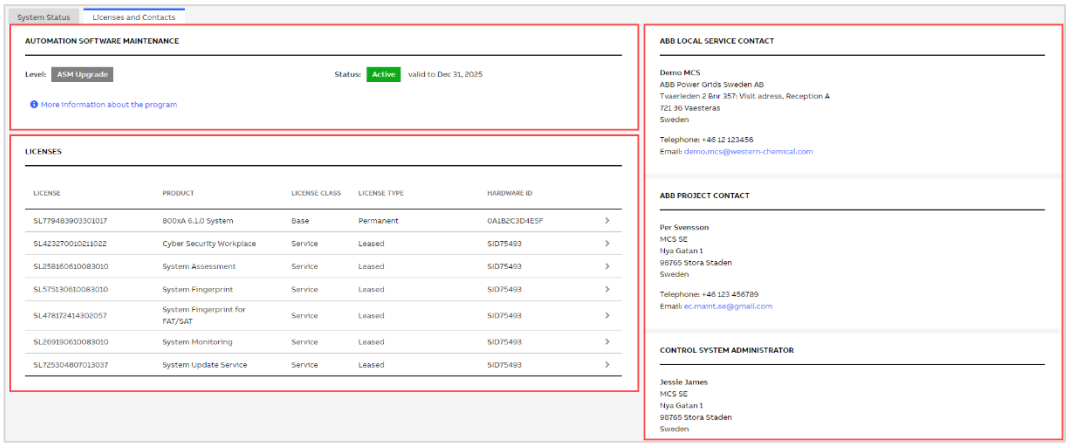


Figure 23: Licenses and Contacts

In the license widget you can expand the individual licenses to get additional information on the license details.

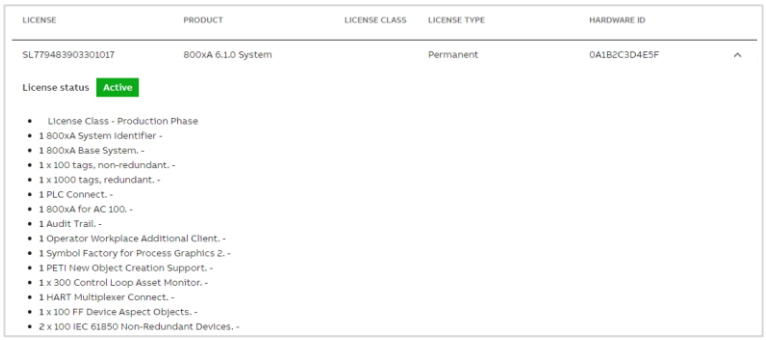


Figure 24: License details

All data in the Licenses and Contacts tab is taken from SoFa. In case something is not correct it needs to be changed in SoFa directly. Afterwards, the SID offline package needs to be downloaded from My Control System (web) again and imported into the MCS-OP to reflect the changes.

2.2.6. Overview area

The overview area gives you a quick impression about the analyzed data and the results for each category. The structure is nearly the same for all the categories. In this example the overview area for the category Security / Security KPIs is used.

Three different widgets are displayed in the overview area:

1. A pie chart in the top-left presenting all results from the selected data set in an easy and comprehensive manner. Click on the reports button to create/access reports from this category (not applicable for all categories).
2. A trend graph in the top-right giving you an overview how results changed over time.
3. KPIs at the bottom showing the results for the individual checks.

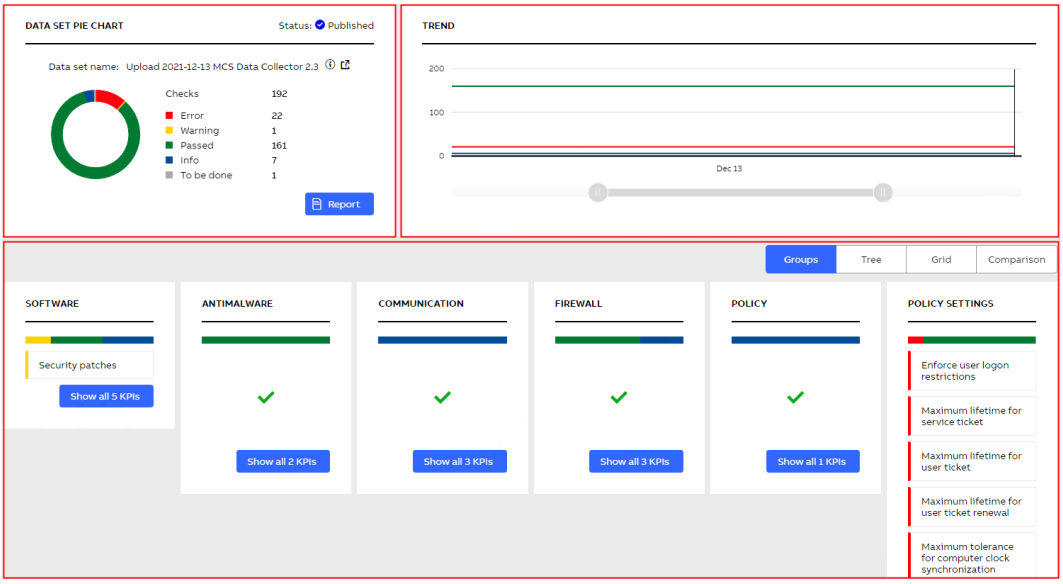


Figure 25: Overview area

The KPIs can be browsed using different views that will help you easily find the most relevant data. The different views will be described in the following chapters.

2.2.6.1. Groups view

The groups' view gives a quick basic overview about the KPIs with the worst result in the different groups. It is limited to 10 KPIs per group and displays only KPIs with the result "Error" or "Warning". Click on a KPI to access the details page (Chapter 2.2.7) of the corresponding KPI. If you want to see all KPIs of the specific group, click on the "Show all KPIs" button to view all KPIs in the Tree view.

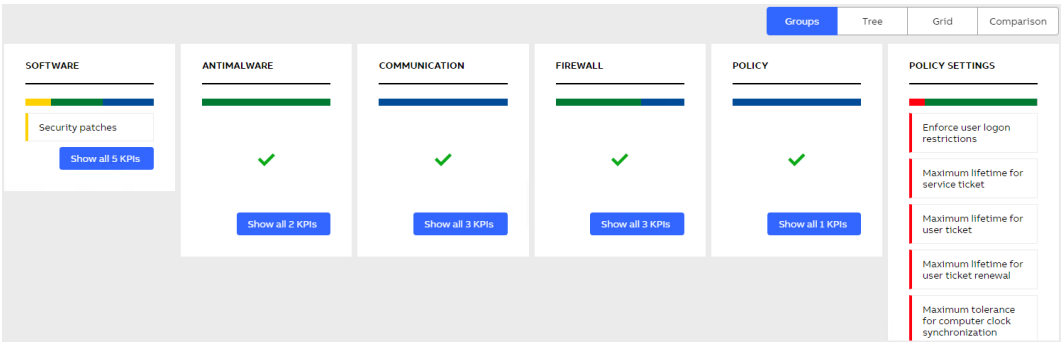


Figure 26: Groups view

2.2.6.2. Tree view

The tree view shows all the KPIs, their status and the reported result in an expandable tree.

The KPIs are grouped into main sections (e.g. Security), subsections (e.g. Software, Antimalware) and the individual KPI (e.g. Windows OS version).

Click on the KPI name to access the details page (Chapter 2.2.7) of the corresponding KPI.

The KPI mode column indicates if this KPI is an "automated KPI" (collected with the MCS-DC) or an "manual KPI" (only available with a valid System Assessment license).

The status column indicates if the KPI is already collected (either automatic or manual) or if it still needs to be done. The status "to be done" is displayed if either the data is not yet

imported, it was not possible to collect data for that specific KPI, or the manual performed KPI is not yet evaluated.

The result column shows the result of the analysis of the KPI. The result can be error, warning, uncertain, passed, info, to be done or skipped.

The user changes column allows you to filter for KPIs that either were edited, have attachments, or have user comments. All these are indicated by small icons on the KPI.

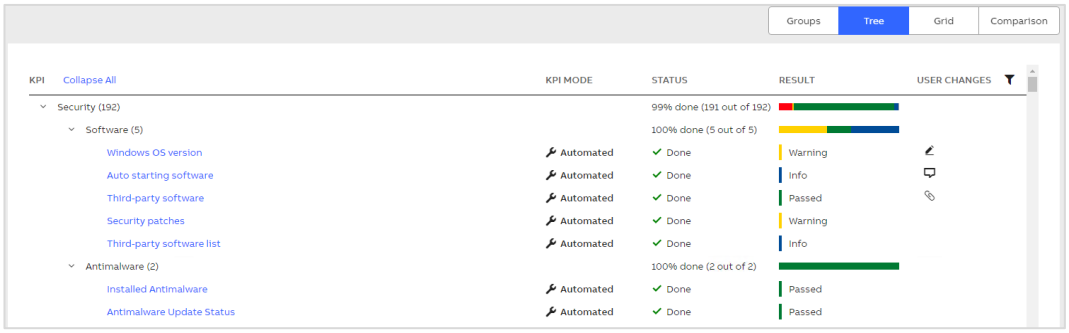


Figure 27: Tree view

2.2.6.3. Grid view

The grid view gives you an overview on the devices and their individual results. Here you can quickly check which device was causing the problem. Click on the squares to access the details page (Chapter 2.2.7) of the corresponding KPI.

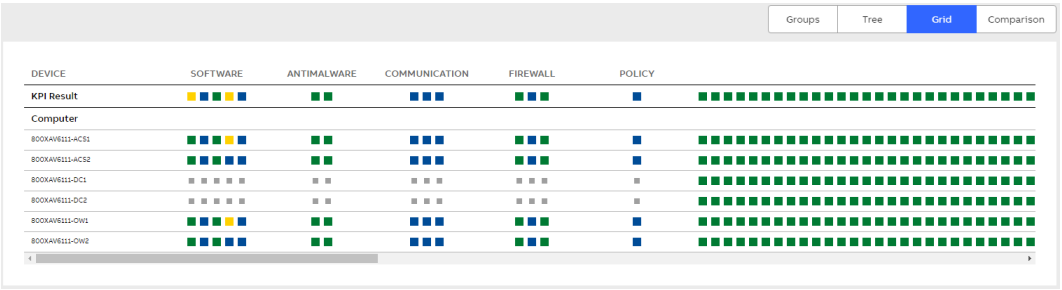


Figure 28: Grid view

2.2.6.4. Comparison view

The comparison view gives you the possibility to check which KPIs changed their status between two data sets. To do so, at least 2 data sets need to be available.

Select a data set from the “data set to compare” dropdown to compare it to the dataset you are currently looking at.

The results are divided into four sections:

1. KPIs that became worse
2. KPIs which improved
3. KPIs which did not change their results
4. KPIs which are not comparable (e.g. they were not collected before)

You can expand each result to see details on which KPIs changed. Click on the result or KPI name to access the details page (Chapter 2.2.7) of the corresponding KPI.

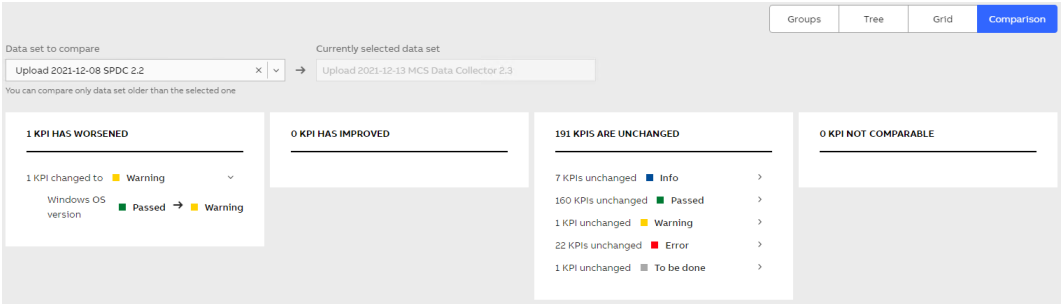


Figure 29: Comparison view

2.2.7. KPI details page

The KPI Details page shows you all relevant information concerning one specific KPI.

It consists of three different widgets:

1. KPI result
2. Suggested actions
3. Evaluation criteria

For some KPIs additional information is available via the documentation icon next to the widget name.

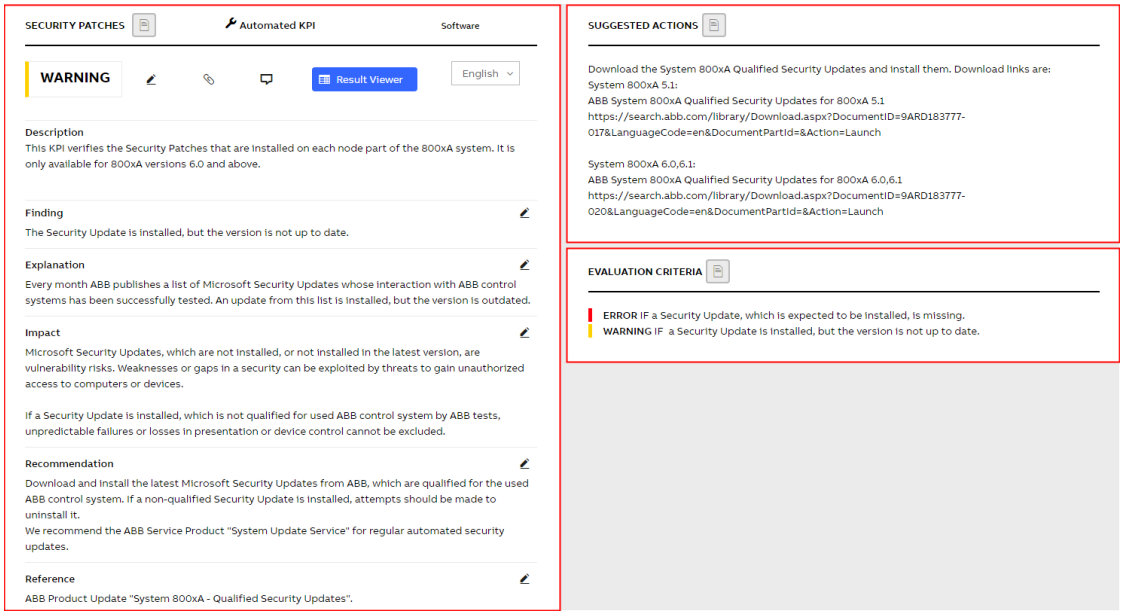


Figure 30: KPI details page

To navigate between KPIs you can use the KPI selector that is displayed in the Filters section. Keep in mind that all applied filters do have an effect on the KPIs that are displayed in the selector (e.g. if you have result filters set to Passed, only KPIs with that result will be displayed).

To go back to the overview area, click on the second item in the breadcrumbs displayed above the filter area. Click on the first item to go the default tab on the first level of navigation.

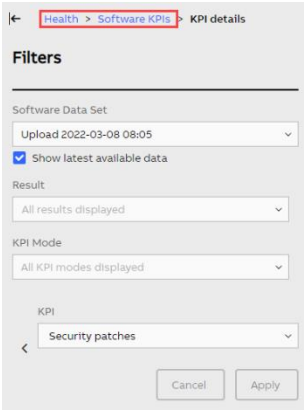


Figure 31: Filter on KPI details page

2.2.7.1. KPI result

The KPI result widget shows the actual result of the analysis. The results can be:

- Error (red)
- Warning (yellow)
- Uncertain (orange)
- Passed (green)
- Info (blue)
- To be done (light grey)
- Skipped (dark grey)

The result "Uncertain" means that no data has been collected, although expected. Possible reasons are among others:

- Checks have been selected in MCS-DC for nonexistent devices, e.g. an AC 800M controller check, but no such controller exists
- Devices are not able to deliver the data which was requested by MCS-DC. For example, an AC 800M is not loaded; or has old firmware which does not support MCS-DC collection methods
- MCS-DC has gathered collections from a computer which is not collectable or partially not collectable
- Any kind of software failure

In such cases, the cause for the failure needs to be analyzed and fixed if possible. Afterwards the data collection with the MCS-DC should be repeated for the concerned KPI. If a fix is not possible set the KPI result to "Skipped" and enter an appropriate explanation in the text field.

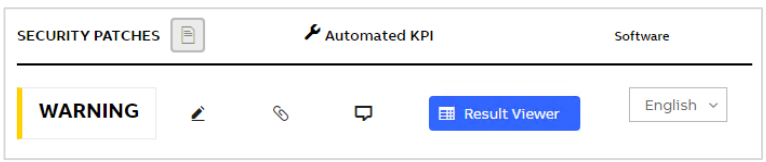


Figure 32: KPI result

You have the possibility to edit the result manually. Click on the “pencil” icon next to the result and choose the new applicable result. You will be asked to leave a comment why the result was changed. The user, the time and the comment of the changed result will be shown on the KPI details page and in the report.

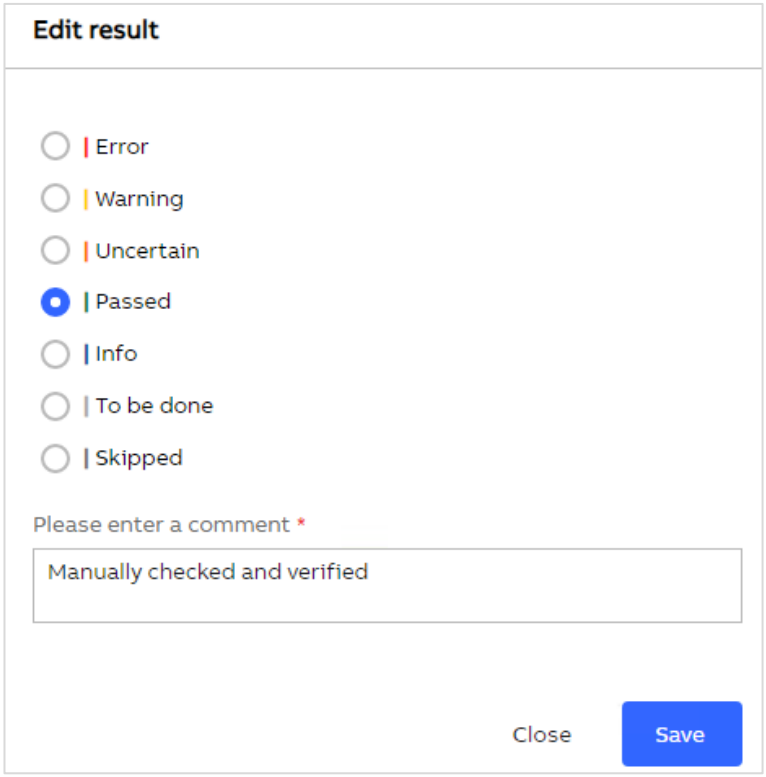


Figure 33: Edit KPI result

To be able to do any modification on the data set (e.g. renaming) or on the data within the data set (e.g. changing a KPI result) you need to be the owner of the data set. See chapter 2.2.12.2 for more information.

When editing a result only the overall KPI result is changed. The raw data will not be overwritten and still shows the original result (e.g. in the result viewer)

If you edited the result by mistake, use the “revert result” button to change the result back to its original value.

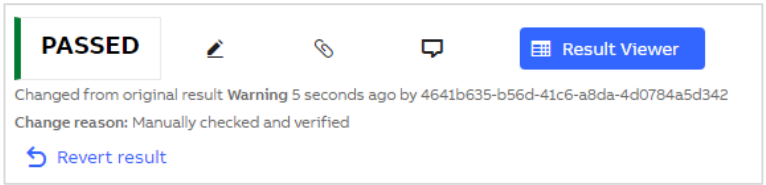


Figure 34: Revert KPI result

Additionally, you have the possibility to add multiple attachments and a comment to each KPI via the corresponding buttons. When adding an attachment, you can choose to include this in the report by enabling the respective checkmark.

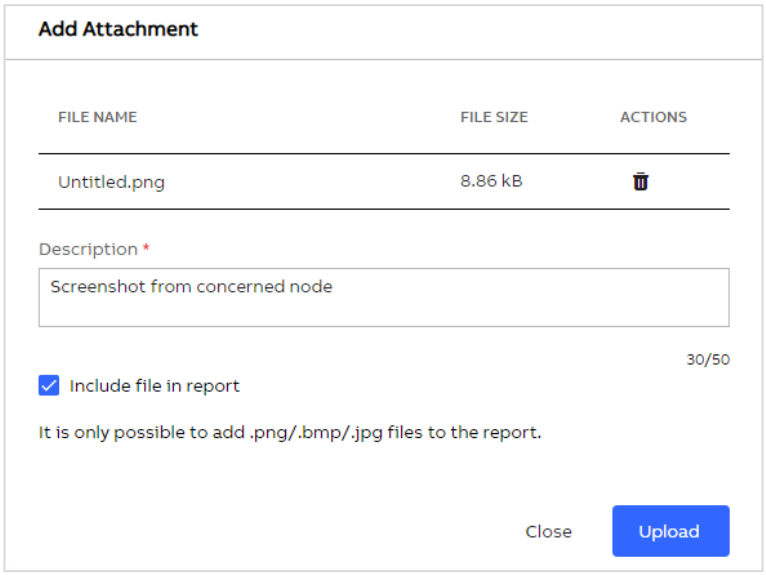


Figure 35: Add attachment

The Result viewer gives you the possibility to access the raw data of each device that was collected for the specific KPI. Use the search bar and result filter to narrow down your results. In addition, you have the possibility to export this specific KPI, all KPI from that category or all KPIs from the collection to Excel for further investigations.

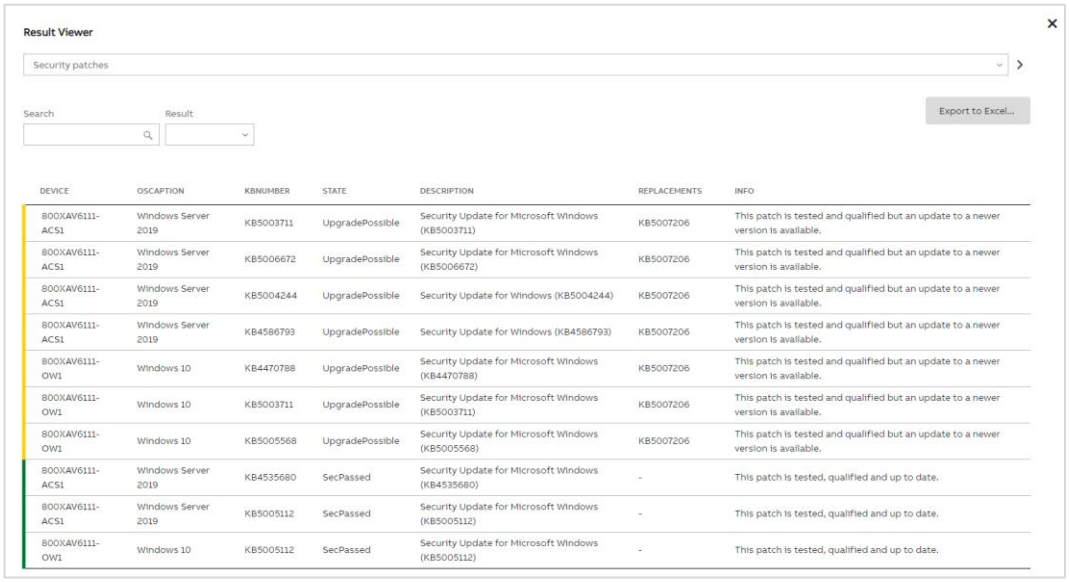


Figure 36: Result viewer

The result viewer is only available with an active System Fingerprint license

Depending on the KPI and the result, different additional text elements are available for troubleshooting the issue. These are:

- Description (general description of the KPI)
- Finding (short information about the finding)

- Explanation (detailed explanation on the finding)
- Impact (information what could be the impact if this issue is not fixed)
- Recommendation (recommended actions to be taken)
- Reference (references to e.g., manuals or web pages with additional information around the KPI)

Explanation, Impact, Recommendation and Reference are only available with an active System Fingerprint license

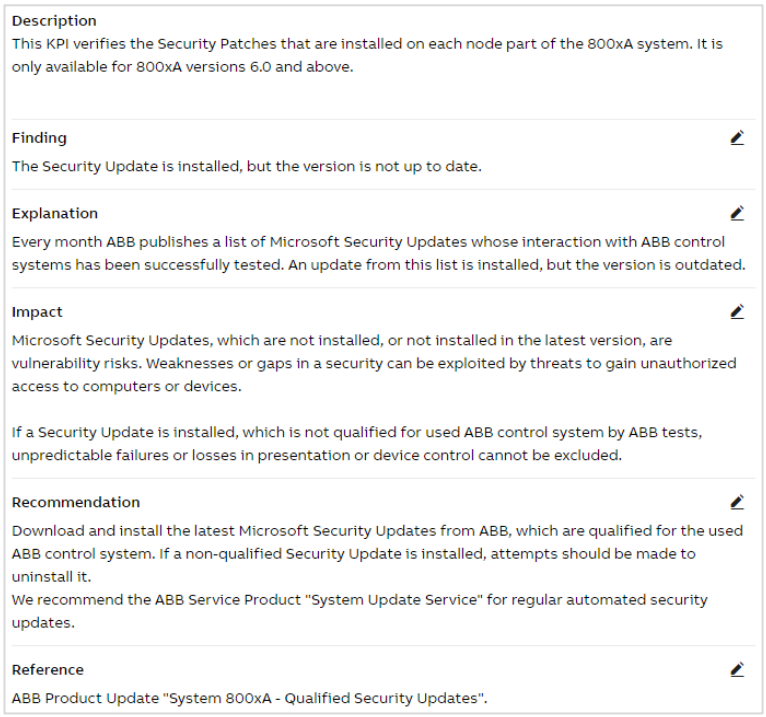


Figure 37: Additional text elements

You have the possibility to edit the pre-defined text elements by clicking on the pencil icon. If you edited the text by mistake, use the “revert text” button to change the text back to the original.

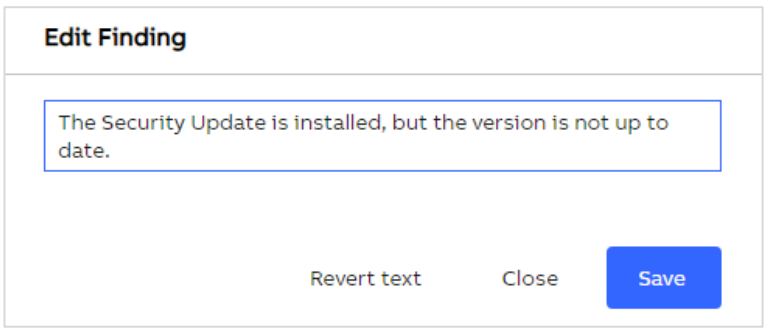


Figure 38: Edit text elements

2.2.7.2. Suggested actions

The suggested actions widget gives you detailed information about the actions to take to resolve this issue.

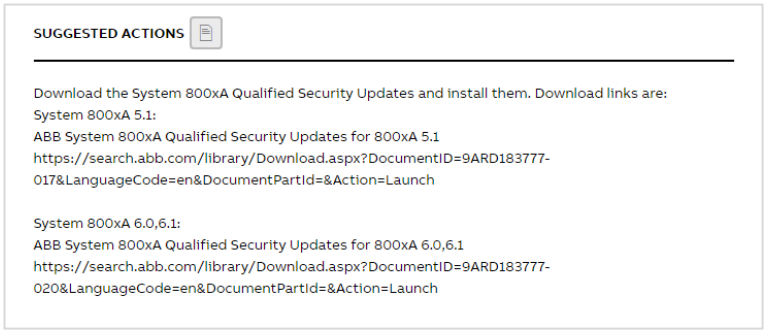


Figure 39: Suggested actions

The suggested actions widget is only available with an active System Fingerprint license

2.2.7.3. Manual check method

The manual check method widget explains how this KPI can be manually collected. This is either used when e.g., an issue was fixed and you do not want to run another MCS-DC scan. Or when performing a System Assessment where you need to collect some of the KPIs manually.

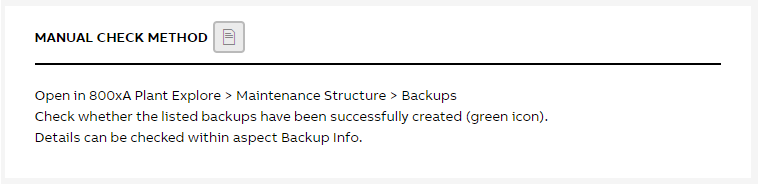


Figure 40: Manual check method

The manual check method widget is only available with an active System Fingerprint license

2.2.7.4. Evaluation criteria

The evaluation criteria widget gives you information about the evaluation criteria that were used to determine the result of the KPI.

Figure 41: Evaluation criteria

2.2.8. Health

The Health category consists of four tabs:

1. Performance KPIs (showing the results of the Performance KPI analysis)
2. Software KPIs (showing the results of the Software KPI analysis)
3. Event Load (showing the results of the System Monitoring analysis)
4. Alerts and Notifications (showing the results of the System Monitoring analysis)

Event Load and Alerts and Notifications tabs will be displayed only if a System Monitoring license is available and CSM application is installed.

2.2.8.1. Performance KPIs

As described in Chapter 2.2.6 three different widgets are displayed on the overview area:

– A pie chart in the top-left presenting all KPI results from the selected data set in an easy to comprehend manner. Click on the reports button to create/access reports from this category.

– A trend graph in the top-right giving you an overview how results changed over time.

– KPIs at the bottom showing the results for the individual checks.

For more information on navigation and the different views in the overview area, refer to Chapter 2.2.6.

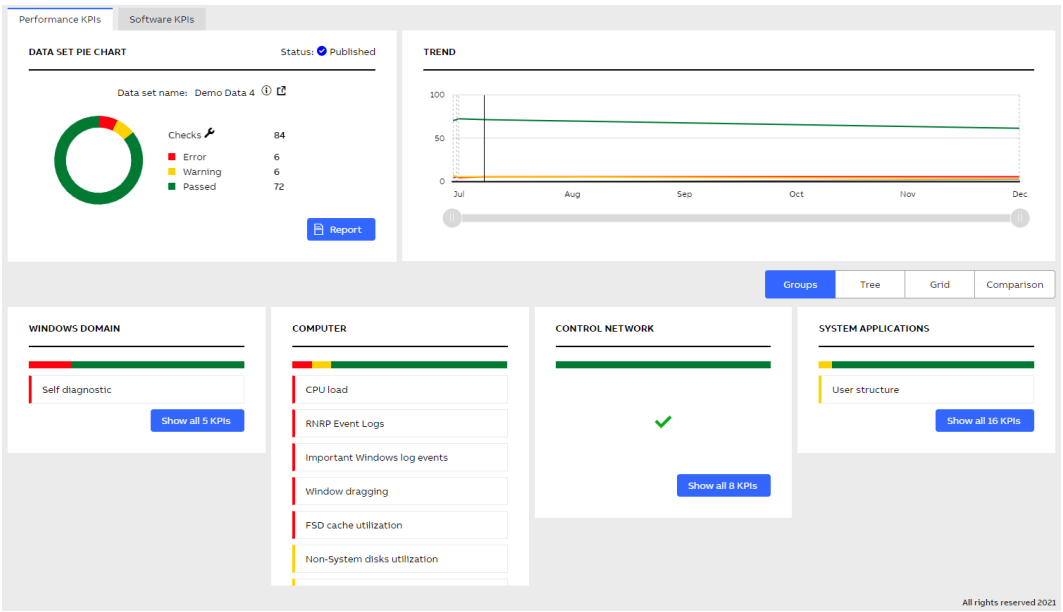


Figure 42: Performance KPIs

2.2.8.2. Software KPIs

As described in Chapter 2.2.6 three different widgets are displayed on the overview area:

– A pie chart in the top-left presenting all KPI results from the selected data set in an easy to comprehend manner. Click on the reports button to create/access reports from this category.

– A trend graph in the top-right giving you an overview how results changed over time.
– KPIs at the bottom showing the results for the individual checks.

For more information on navigation and the different views in the overview area, refer to Chapter 2.2.6.

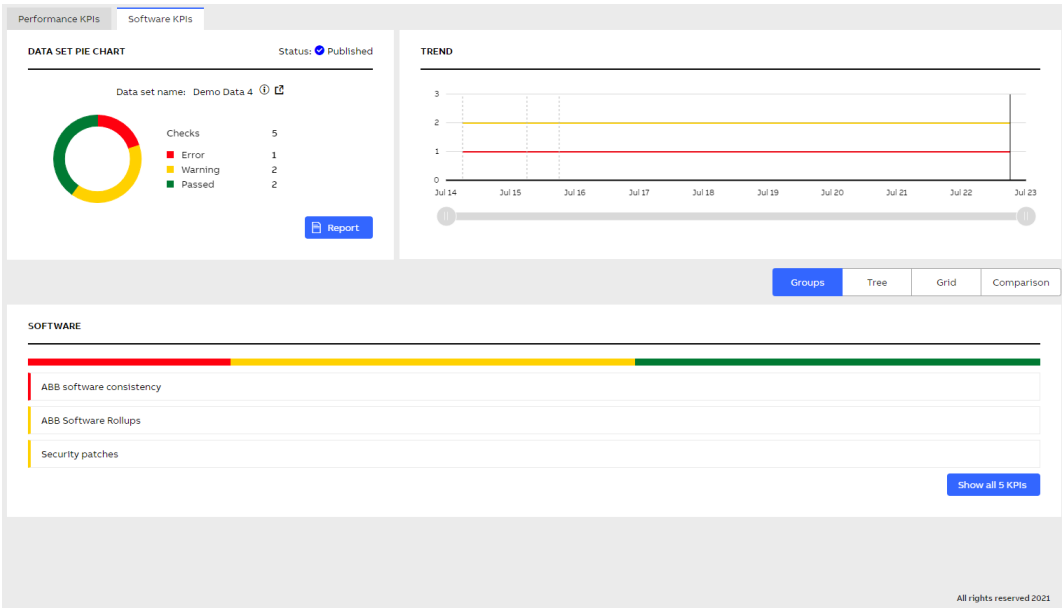


Figure 43: Software KPIs

2.2.8.3. Event Load

Event Load tab is displayed only if System Monitoring license is available for the selected SID and CSM application is installed

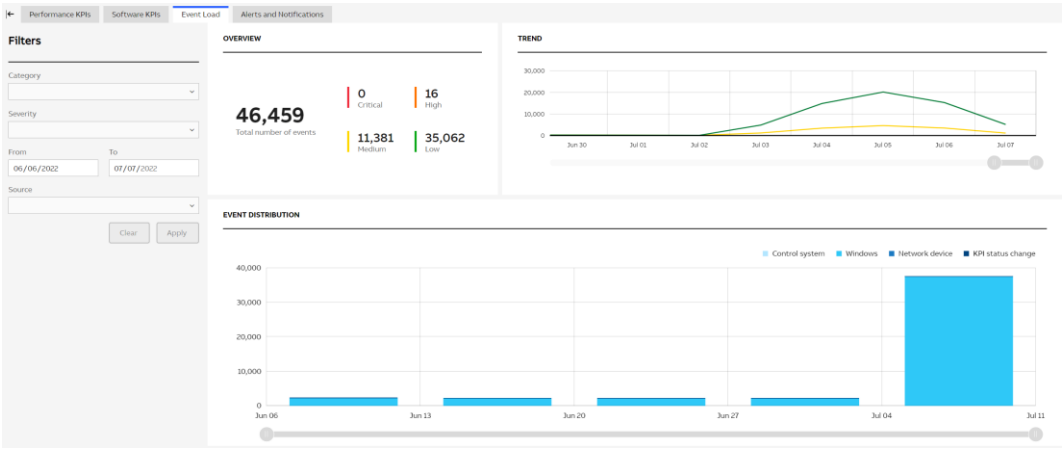


Figure 44: Event Load

A filter area and three different widgets are displayed on Event Load tab.

The following filters are available:

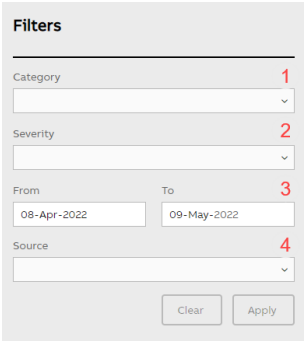


Figure 45: Filter area

1. Category: Select the category you would like to analyze. By default, data from all categories is displayed.
2. Severity: Select the severity of the events. By default, data for all severities is displayed.
3. From/To: By default, “From” filter is set to 31 days back. Date earlier than 1 year ago cannot be selected.
4. Source: Select the specific source(s) to analyze data. By default, data from all sources is displayed.

After you selected your filter, click “Apply”. The page will refresh and display the data you have selected. You can also click “Cancel” to revert any selection you have made to the currently displayed view.

The overview widget presents the total number of events (including not evaluated events) with detailed number for each severity:

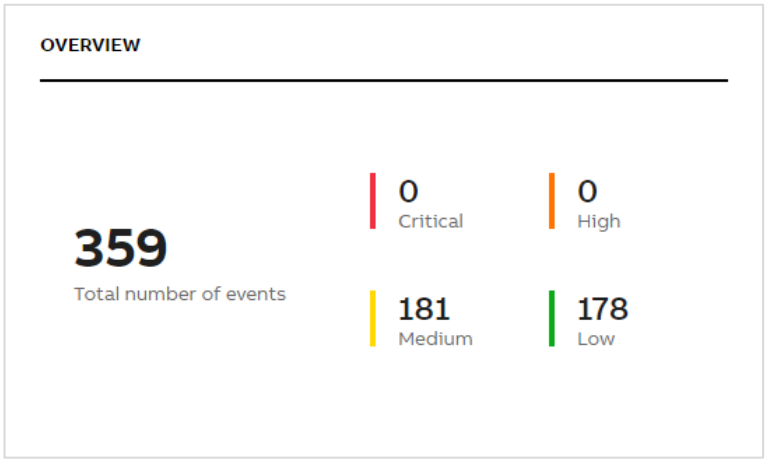


Figure 46: Overview

The trend widget shows the total number of events by the severity (color of the line matches the event severity) from the past year. Date range selected in the filter is indicated by white background and by default zoomed in. Other date range is indicated by grey background.

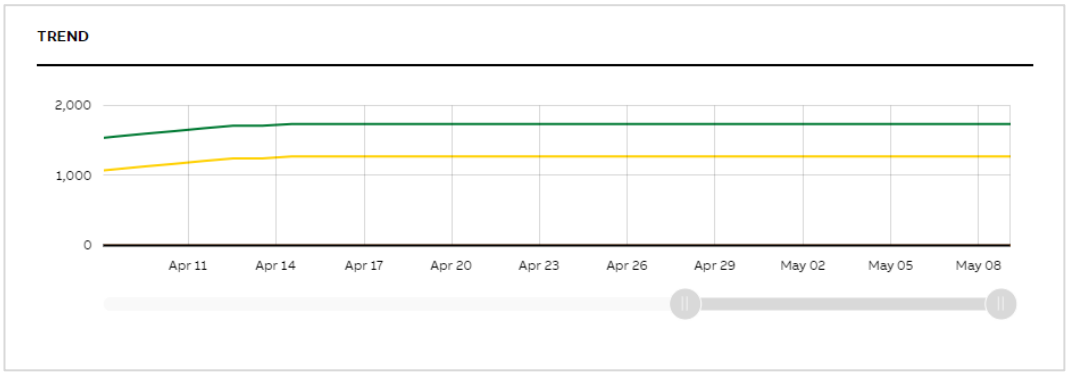


Figure 47: Trend

The Event Distribution widget presents the event distribution per category per day. For a wide range of dates a merging mechanism with the following rules has been implemented:

- If more than 31 days has been selected - data per week is shown
- If more than 31 weeks has been selected - data per month is shown

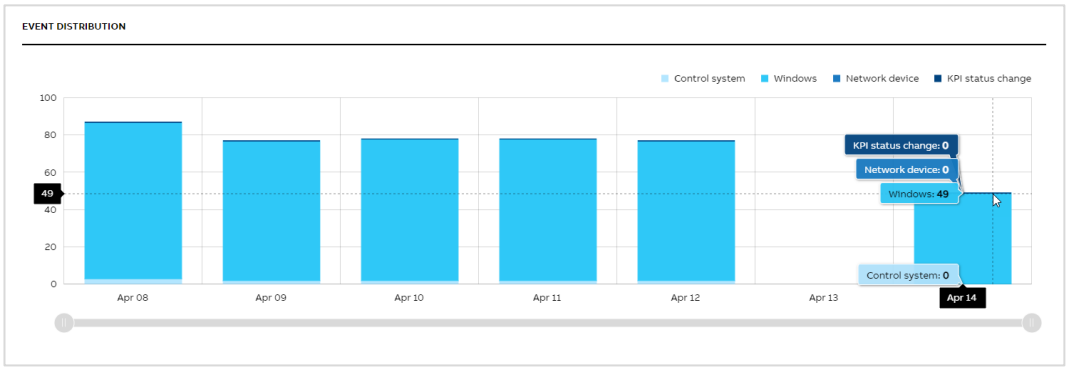


Figure 48: Event Distribution

2.2.8.4. Alerts and Notifications

The Alerts and Notifications tab is displayed only if System Monitoring license is available for the selected SID

Filter area and two different widgets are displayed on Alerts and Notifications tab:

- A trend graph giving you an overview how notifications changed over time
- Notifications at the bottom grouped by the category. Notifications can be browsed using different views (Groups, Tree or Grid).

Figure 49: Alerts and Notifications

Selecting a specific notification in any of the views (Groups, Tree or Grid) directs to the notification details page which shows all relevant information concerning one specific notification.

The notification details page consists of:

1. Notification details
2. Frequency widget

To navigate between notifications, you can use the notification selector that is displayed in the Filters sections. Keep in mind that all applied filters do influence the notifications that are displayed in the selector.

For the selected notification a frequency widget is displayed on the right side. It presents how many times the selected notification was triggered for the selected source. If the notification comes from more than one source, by default data from all sources is displayed on the graph and a dropdown with available sources is displayed (in the top right corner of the frequency widget). You can see the data from the specific source by selecting it in the dropdown. By default, data from 1 month is presented but other time frames can be selected.

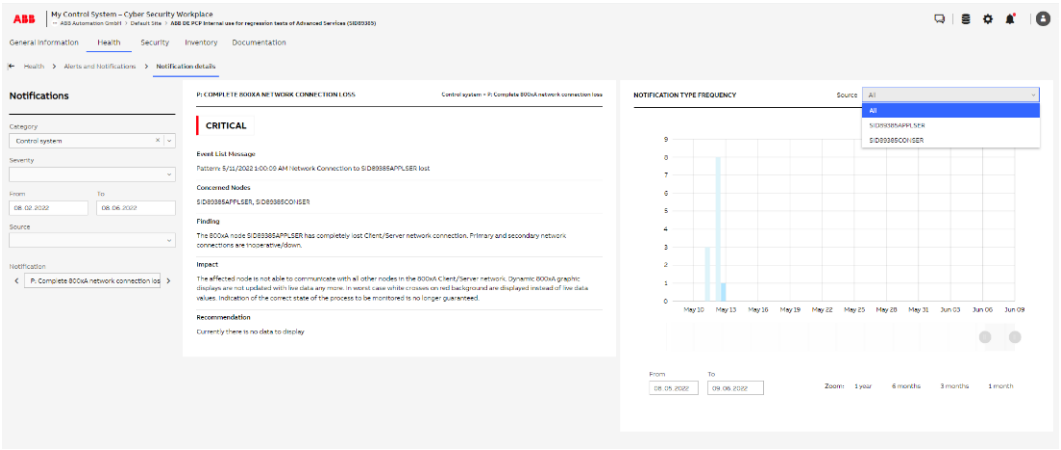


Figure 50: Notification details page

2.2.9. Security

The Security category consists of multiple tabs:

1. System Overview
2. Node Overview
3. Security KPIs
4. Security Updates
5. Malware Protection
6. Backup
7. Maintenance
8. System Tools

All tabs are part of the CSWP feature set of MCS on-premise, and will only be available if a CSWP license is available and if System Utilities application is installed. There is one exception: **Security KPIs**. This tab is generally available.

The Security KPIs tab, the Security Update tab, the Malware Protection tab and the Backup tab have indicators to show if there are items in the tab which need attention. The table below lists the indicator and their purpose:

Table 2: Tab indicators

Indicator	Description
	There is no data available to show. This typically indicates there is no dataset available containing the data needed to show.
	The collector service is not running and the data presented in the tab is unreliable. Besides the indicator, also the background of the tab will be colored in red if it is not the active tab.
	There are KPIs or nodes on the tab which are in error. The number inside the indicator shows how many errors there are. If the number is greater than 9, it will be presented as **9+**.
	There are KPIs or nodes on the tab which are in warning and there are no KPIs or nodes in error. The number inside the indicator shows how many warnigs there are. If the number is greater than 9, it will be presented as **9+**.
	There are no errors or warnings.

The order of the table shows the order of precedence of the indicators. Only one indicator at a time will be shown.

The following chapters describe the contents of each tab in more detail.

2.2.9.1. System Overview

The System Overview tab shows the summary status for the following tabs:

– Security KPIs
– Security Updates
– Malware Protection
– Backup

[2]

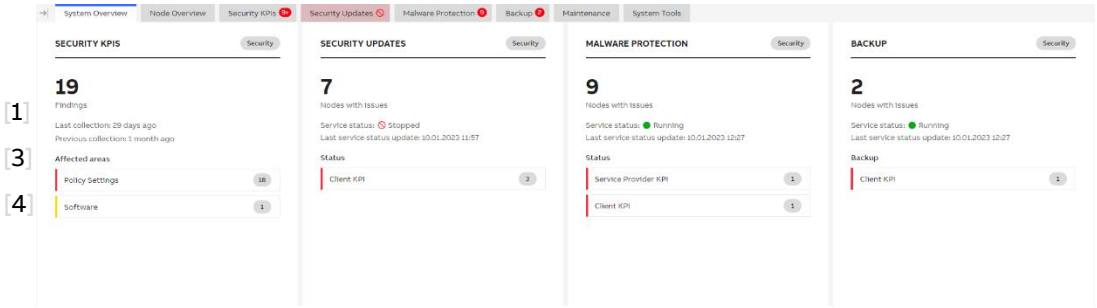


Figure 51: Summary widgets

Depending on the tab, the widget will show the total number of findings (**Security KPIs**) or the number of nodes which are having issues (**Security Updates**, **Malware Protection** and **Backup**) – see [1]. The number is always the total number, regardless of errors or warnings being present or not. Therefor the number on the tab, which is only showing the number of the most severe issue – see [2], could differ from the number shown on the summary widget.

Below the number of findings, there is an indicator – see [3] – on the “Last collection” date and “Previous collection” date for the Security Status and the collector “Service status” and the “Last service status update” date for Security Updates, Malware Protection and Backup. This information helps to determine how reliable the data on the widgets is. If ABB My Control System – Data Collector modules (Malware Protection or Security Updates type) is enabled, this data on the respective widget is replaced with last MCS-DC collection information.

Finally, the affected areas / status is shown. This shows in which KPI area’s the error(s) or warning(s) are.

2.2.9.2. Node Overview

This tab shows details information on a per node basis. Depending on the modules activated and the functionality assigned to the node, the information shown might differ per node.

On the left hand side of the tab, there is the list with the nodes configured to be part of System Utilities (see document ref.[1] for more details on configuring System Utilities). Select any node to display the details for that node:

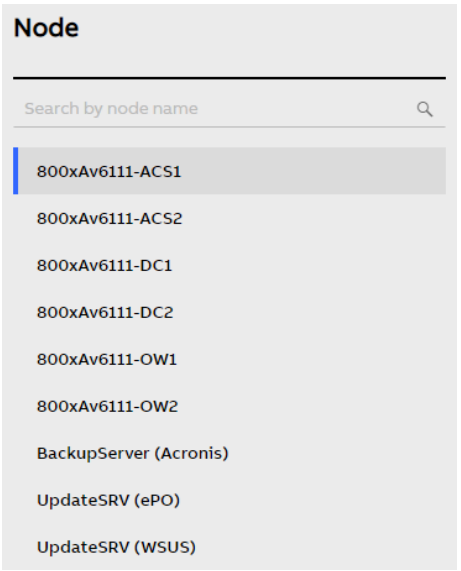


Figure 52: Node list

The details are shown in the main pane. The possible widgets shown are listed from left to right first and then from top to bottom in the following chapters.

2.2.9.2.1. Node Details

This widget is always shown.

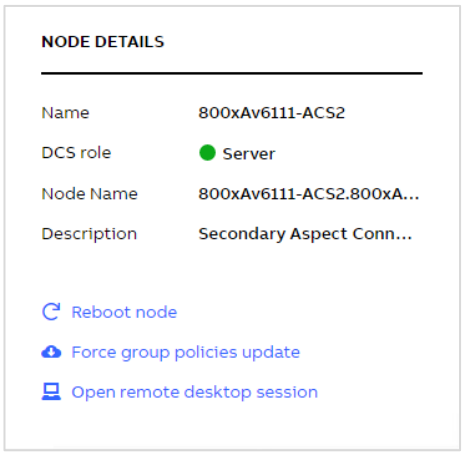


Figure 53: Node details widget

This widget shows the following information:

- Name
  the display name of the node in MCS on-premise.
- DCS role
  the DCS role of the node (only shown if applicable).
- Node name
  the FQDN name of the node.
- Description
  Description of the node as given in MCS on-premise. In case the description is too long, three dots (...) are added and a tooltip will give the entire description.

The bottom part of the widget shows the available actions for that node:

- Reboot node
  sends the reboot command to the node.
- Force group policies update
  sends the **gpupdate /force** command to the node. This is to re-apply the group policies as defined in the domain.
- Open remote desktop session
  creates the remote desktop file which can be used to setup a remote desktop connection to the node.

If an action is started, other actions will be temporary disabled until the action has completed.

2.2.9.2.2. Security Updates

This widget is only shown when the node is marked member of the WSUS module or ABB My Control System – Data Collector module (of Security Updates type) is enabled.

For WSUS module:

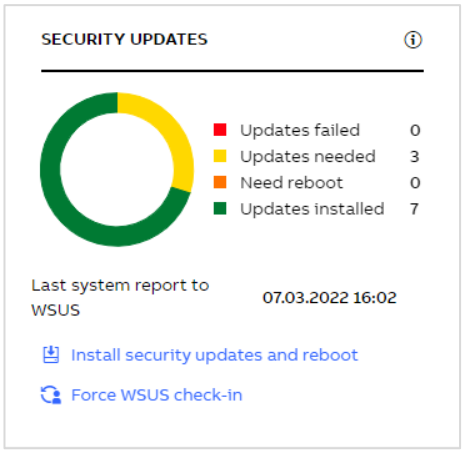


Figure 54: Security updates widget (WSUS module)

This widget shows the current security update installation status for the selected node.

It shows the following information (in order of severity):

- how many updates have failed installation
- how many updates are needed to be installed
- how many updates are installed but need a reboot to become fully active
- how many updates are successfully installed
- the date and time of the last system report to WSUS

It could be that security updates are listed to be installed, but when trying to do so on the node, it tells no updates are available. This is most likely due to the WSUS server not having downloaded the complete content of the update and thus not making it available for installation yet.

When having installed an updated successfully, it could be that the number for the successfully installed updates is not increased. This is due to the updates for Windows being cumulative updates and the installed update replaces the previously installed one.

The same text is also shown when clicking the information icon in the top-right corner.

The bottom part of the widget shows the available actions for that node:

- Install security updates and reboot
  sends the update patches and reboot once installed command to the node. Any control system services for System 800xA and Symphony Plus will be stopped first.
- Force WSUS check-in
  sends the command to report the current patch status of the node to the WSUS server to the node.

If an action is started, other actions will be temporary disabled until the action has completed.

For ABB My Control System – Data Collector module:

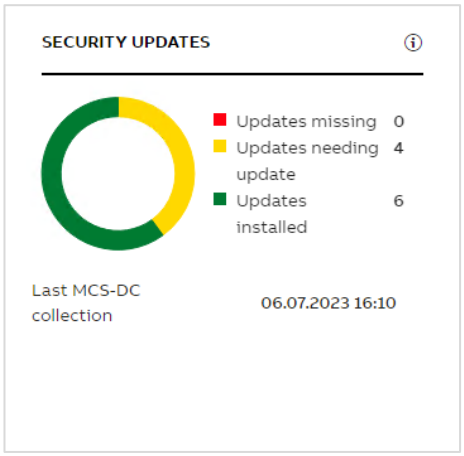


Figure 55: Security Updates widget (ABB My Control System - Data Collector module)

This widget shows the current security update installation status for the selected node.

It shows the following information (in order of severity):

- how many updates are missing
- how many updates need to be updated
- how many updates are successfully installed

Security updates need to be installed/updated manually as no centralized management system is available.

When having installed an update successfully, it could be that the number for the successfully installed updates is not increased. This is due to the updates for Windows being cumulative updates and the installed update replaces the previously installed one.

It can take up to one hour before data is presented for just created or updated nodes.

2.2.9.2.3. Malware Protection

This widget is only shown when the node is marked member of the ePO or SEPM module or ABB My Control System – Data Collector module (of Security Updates type) is enabled.

For ePO module:

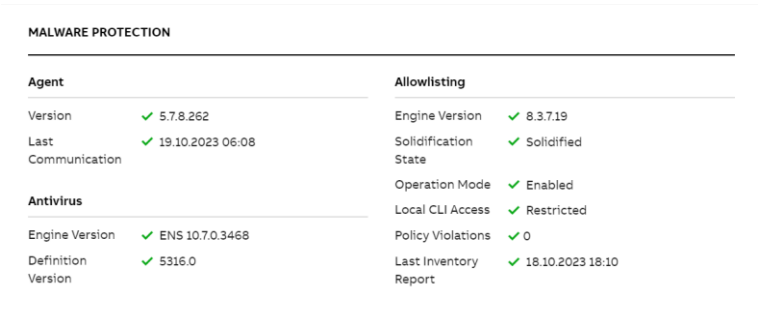


Figure 56 Malware protection widget (ePO module)

This widget shows the status of all monitored ePO managed software on the node:

- Agent
  The status of the ePO Agent deployed to the Node. The section displays the detected

version of the Agent, and when the Agent has last communicated with the ePO server.
The version is compared against the Agent version available in the local ePO Main Repository. If the versions match, the green checkmark will be shown.
For the last communication, a green checkmark will be shown if the value is not older than one hour.

– Antivirus
The status of the ePO antivirus software (VSE/ENS) on the node. This section is only displayed, if monitoring of the antivirus status was configured for the node.
The section displays the name and version of the detected antivirus engine (ENS or VSE) on the node and the version of the currently used virus definition file.
The engine version is compared the engine version available in the local ePO Main Repository. If the versions match, the green checkmark will be shown.
The definition version is either compared to the version available in the local ePO Main Repository (VSE) or to its creation date (ENS). For the version comparison, a green check mark is shown if the version matches the version in the repository, for the date comparison it is shown, if the version is not older than five days.

– Allowlisting
The status of the ePO allowlisting software (Solidcore) on the node. This section is only displayed, if monitoring of the allowlisting status was configured for the node.
The section displays the version of the detected allowlisting engine, the nodes solidification state, the operation mode of the engine, whether access to the Solidcore CLI is permitted, the number of Allowlisting policy violations in the last seven days and when the node last reported its inventory to the ePO server.
The engine version is compared the engine version available in the local ePO Main Repository. If the versions match, the green checkmark will be shown.
The Solidification State will show a green checkmark, if the state “Solidified” is detected.
The Operation Mode will show a green checkmark, if the state “Enabled” is detected.
The Local CLI Access will show a green checkmark, if the state “Restricted” is detected.
The Policy Violations will show a green checkmark, if no violations were detected within the last seven days.
The Last Inventory Report will show a green checkmark, if the value is not older than five days.

For SEPM module:

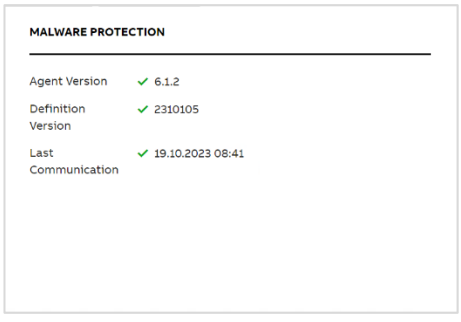


Figure 57: Malware protection widget (SEPM module)

This widget shows the status of the SEPM malware protection solution:

– Agent version
the version of the McAfee ePO or SEPM Agent installed on the node.
A green checkmark is displayed, if the SEPM Agent was detected on the node.

– Definition version
  The virus definition file. The definition file should be less than five days old to show the green checkmark.
– Last agent communication
  Date and time of the last successful communication of the agent with the management server. If the last agent communication is within the last hour the green checkmark will be shown.

For ABB My Control System – Data Collector module:

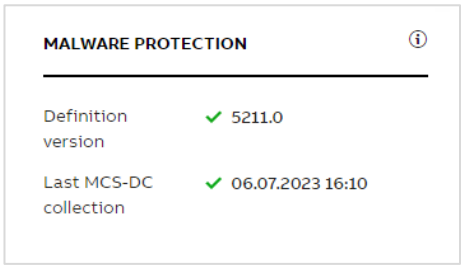


Figure 58: Malware protection widget (ABB My Control System – Data Collector module)

– Definition version
– Last MCS-DC collection

It can take up to one hour before data is presented for just created or updated nodes.

2.2.9.2.4. Backup

This widget is only shown when the node is marked member of the NetVault, Rapid Recovery or Cyber backup module.

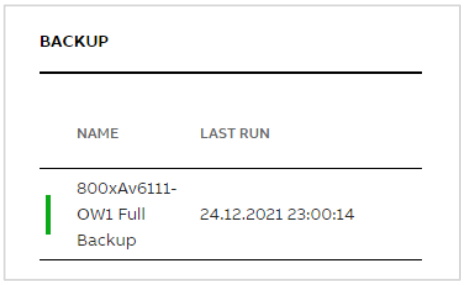


Figure 59: Backup widget

This widget shows the latest status for the backup job/plan defined for this node and when it was last executed.

2.2.9.2.5. Maintenance

This widget is always shown.

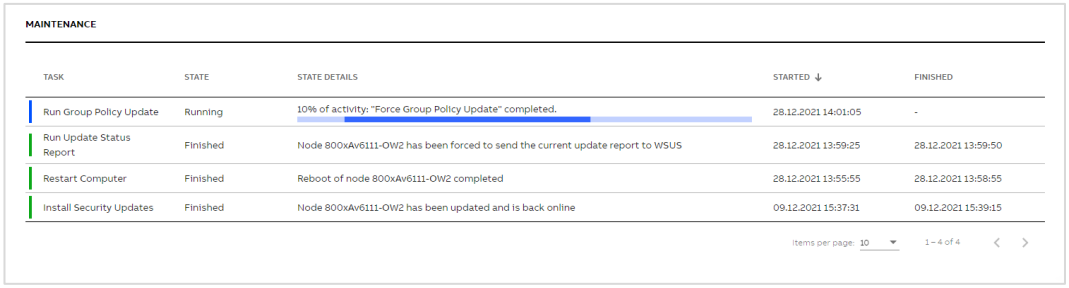


Figure 60: Maintenance widget

This widget shows the maintenance actions performed on the node, listing from left to right:

- Status
  color indication on the status of the maintenance action.
- Task
  the maintenance task executed.
- State
  the state of the maintenance task.
- State Details
  The details of the maintenance task.
- Started
  When the task was started.
- Finished
  When the task finished.

2.2.9.2.6. Aspect Directory Status

This widget is only shown for System 800xA nodes acting as Aspect Servers.

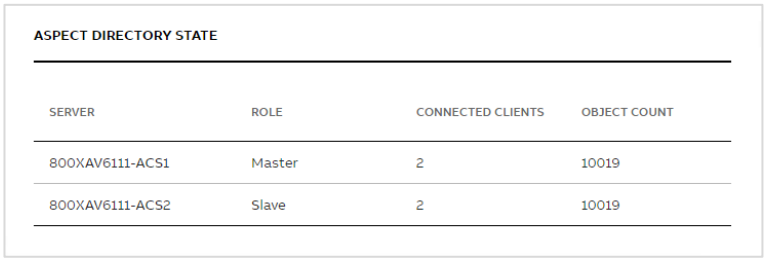


Figure 61: Aspect Directory state widget

This widget shows the start of the Aspect Directory for all Aspect Servers. It shows which server is currently active as master and which one(s) are acting as slave. It also shows the number of connected clients for each of the servers as well as the amount of aspect objects available in the Aspect Directory on each server. The number of aspect objects should be the same on all servers. If not, it indicates a problem in the Aspect System.

2.2.9.2.7. 800xA Services

This widget is only shown for System 800xA nodes marked as server and running at least one service.

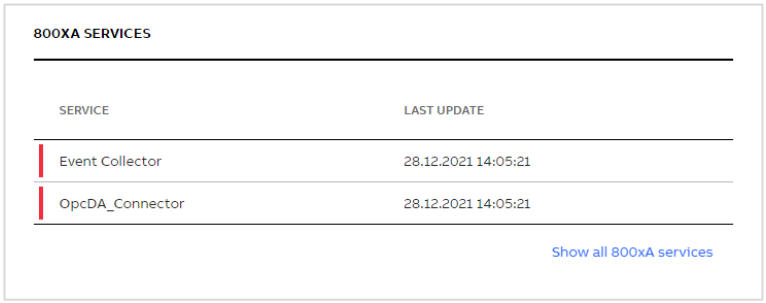


Figure 62: 800xA services widget

This widget shows the status of the 800xA services. As the list of services is long, by default only services in error are shown. Click **Show all 800xA services** to list all services in the Aspect System.

2.2.9.2.8. Basic History

This widget is only shown for System 800xA nodes providing basic history functionality.

Figure 63: Basic history widget

This widget shows the status of the basic history providers in the 800xA system. The basic history providers should always be in sync. If not, it indicates a problem with basic history in the system.

2.2.9.3. Security KPIs

The Security KPIs page has the same build up as the Performance and Health KPI's pages. Three different sections are displayed:

- A pie chart in the top-left presenting all KPI results from the selected data set in an easy to comprehend manner. Click on the reports button to create/access reports from this category.
- A trend graph in the top-right giving an overview how results changed over time.
- KPI's at the bottom showing the results for the individual checks.

For more information on navigation and the different views on the KPI tabs, refer to chapter 2.2.6 Overview area.

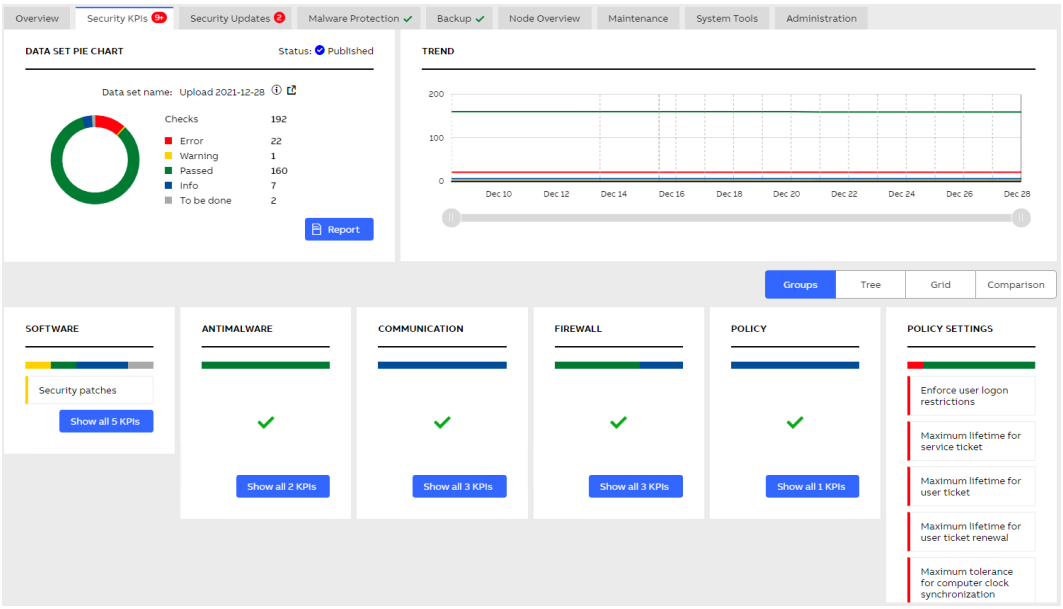


Figure 64: Security KPIs

2.2.9.4. Security Updates

Opposed to the other views in MCS on-premise, this tab shows the donut chart and trend data Node oriented, not KPI oriented.

The following information is displayed:

- A pie chart on the top-left presenting the node status from the selected data set in an easy to comprehend manner.
- A trend graph in the top-right giving an overview how the status for the nodes changed over time.
- KPI's at the bottom showing the results for the individual checks.

For more information on navigation and the different views on the KPI tabs, refer to chapter 2.2.6 Overview area.

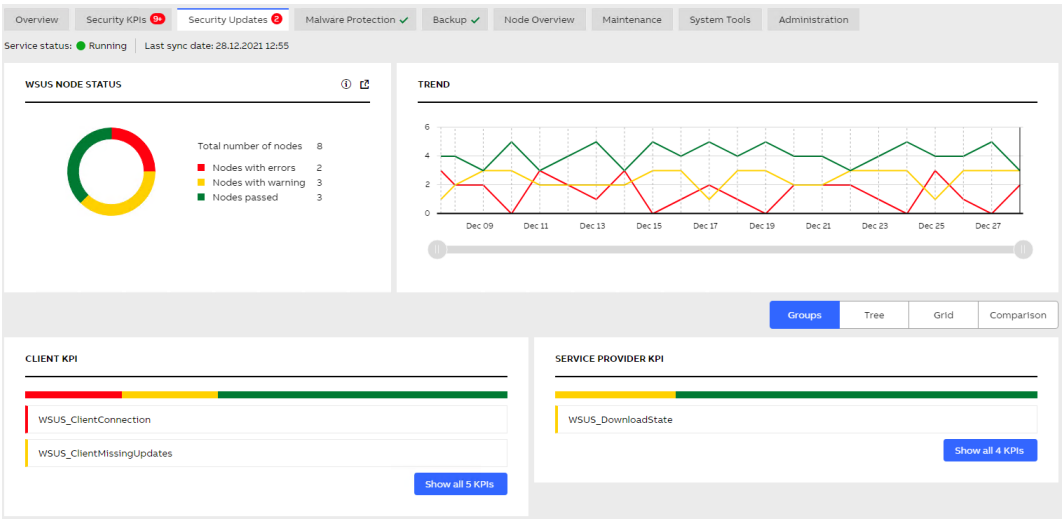


Figure 65: Security Updates

2.2.9.5. Malware protection

Opposed to the other views in MCS on-premise, this tab shows the donut chart and trend data Node oriented, not KPI oriented.

The following information is displayed:

- A pie chart on the top-left presenting the node status from the selected data set in an easy to comprehend manner.
- A trend graph in the top-right giving an overview how the status for the nodes changed over time.
- KPI's at the bottom showing the results for the individual checks.

For more information on navigation and the different views on the KPI tabs, refer to chapter 2.2.6 Overview area.

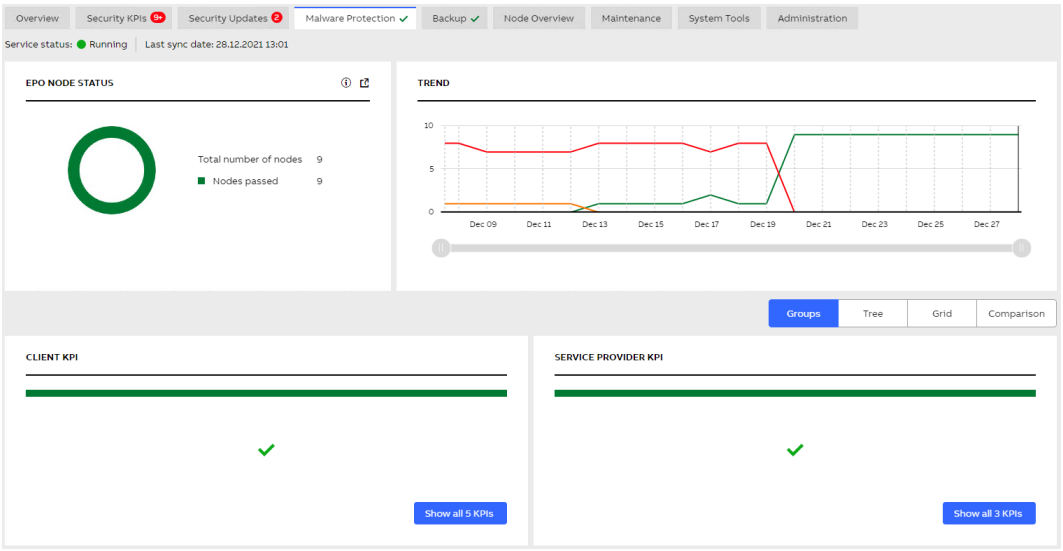


Figure 66: Malware Protection

2.2.9.6. Backup

Opposed to the other views in MCS on-premise, this tab shows the donut chart and trend data Node oriented, not KPI oriented.

The following information is displayed:

- A pie chart on the top-left presenting the node status from the selected data set in an easy to comprehend manner.
- A trend graph in the top-right giving an overview how the status for the nodes changed over time.
- KPI's at the bottom showing the results for the individual checks.

For more information on navigation and the different views on the KPI tabs, refer to chapter 2.2.6 Overview area.

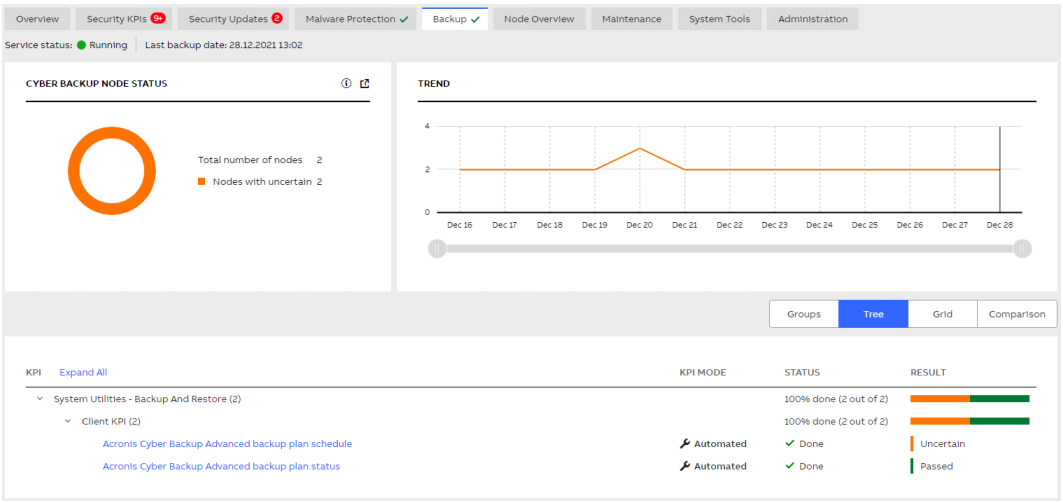


Figure 67: Backup

2.2.9.7. Maintenance

This tab shows a comprehensive overview of all nodes, showing the last action executed with its state and details and allows to take actions. The most used actions are available for direct selection, the lesser used actions are available by opening the pop-up menu using the three dots (⋮).

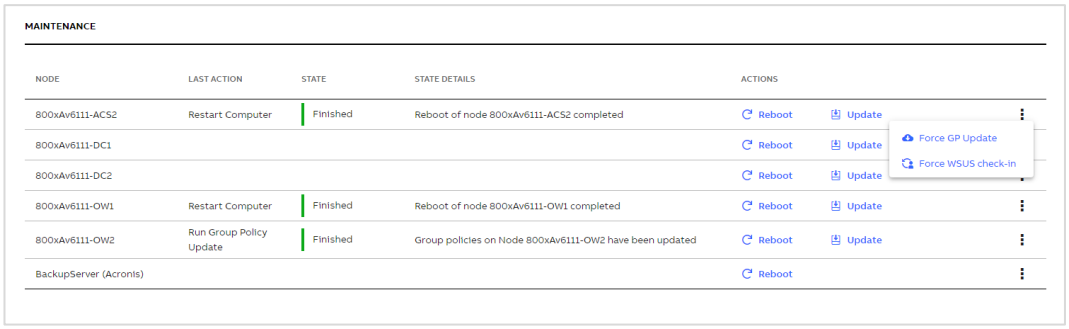


Figure 68: Maintenance

2.2.9.8. System tools

This tab provides the following functions:

2.2.9.8.1. System remote access

This allows for enabling predefined users in the domain, which can be used for remote access.

Figure 69: System remote access widget

From left to right, the widget shows:

- Account name
  the account name for the remote access user.
- Status
  if the account is locked or enabled.
- Password
  the temporary password for the account.
- Expiration
  how much time left until the account expires
- Actions
  actions to **Activate** or **Deactivate** the account.

When clicking activate, a confirmation dialog will be shown:

Figure 70: Activate account confirmation dialog

If **Activate account** is clicked, it will enable the locked account and a **new** password will be generated for this account. The length of the newly password generated is per the settings for the SystemAccessAction service. Also, an expiration timer will be started. The time used for expiration is as set in the System Remote Access module settings.

Once an account is activated, additional actions can be taken for this account:

Table 3: System Remote Access action icons

Action	Description
	Show generated password
	Hide generated password
	Copy the password to the clipboard
Extend	Extend the time left until expiration till the maximum configured for this account

The link to the remote access web interface, typically the RAP VSE web interface, is located at the top-right corner of the widget. Clicking this link, **Open Remote Access Web Interface** will show the URL which will be opened before opening it:

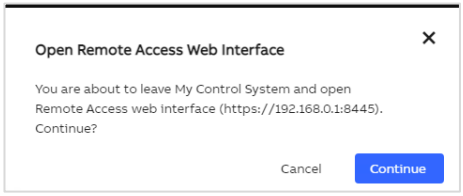


Figure 71: Open Remote Access Web Interface confirmation dialog

Clicking **Continue** will open the web interface in a new tab in the browser.

2.2.9.8.2. Plant isolation

This widget allows the user to put the adapter into or to take it out of isolation mode. If communication is currently allowed (the adapter is not in isolation mode), it is shown with a green label:

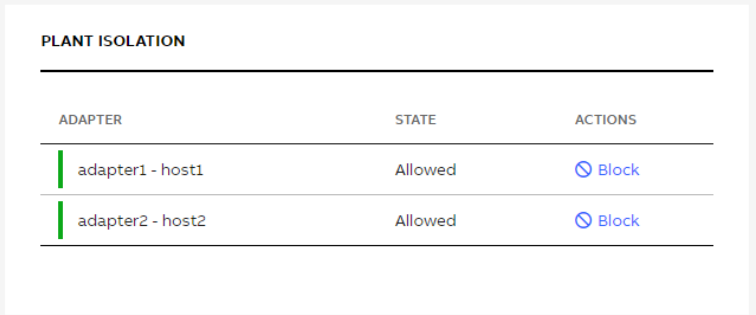


Figure 72: Network communication is allowed

Clicking **Block** will put the adapter in isolation mode by disabling the network communication to the control system. Once in isolation mode, the status on the widget is updated accordingly.

Click **Allow** to enable the network communication.

Depending on the configuration of Plant isolations, blocking the Network Communication can affect System Operations

2.2.10. Inventory

The Inventory category consists of four tabs:

1. Hardware Lifecycle (showing the results of the Hardware lifecycle analysis)
2. Assets (showing an overview about all assets with details and analysis results of the different categories
3. Control Structure (showing an overview about controllers)
4. Software (showing all computers with installed ABB and third-party software)

2.2.10.1. Hardware Lifecycle

The Hardware Lifecycle tab shows all results of the lifecycle analysis.

The overview area consists for two different widgets:

– A pie chart in the top-left presenting all lifecycle phases from the latest inventory information in an easy to comprehend manner. Click on the reports button to create/access reports from this category.

– KPIs at the bottom showing the lifecycle phases for the individual components.

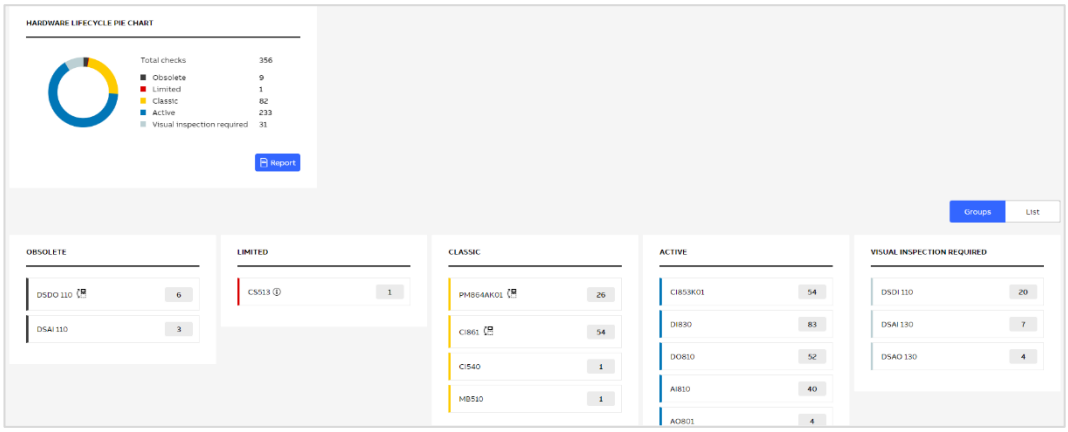


Figure 73: Hardware Lifecycle - groups view

The groups' view classifies the devices according to their current lifecycle status (Active, Classic, Limited, Obsolete). Devices that cannot be determined completely are classified as "visual inspection required". See chapter 0 for more information on how to set the device type for visual inspection required modules.

In every group the name of the device and the number of devices that were found is listed. In addition, indicators show you for which device a replacement is available.

In case the exact module version could not be identified but all module versions have the same lifecycle status, an indicator is displayed next to the device name with tooltip on hover.

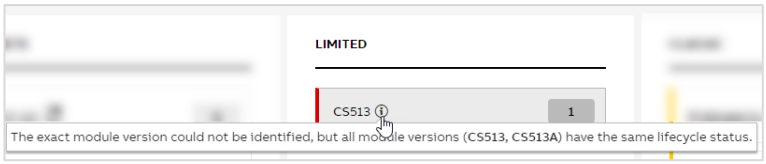


Figure 74: Hardware Lifecycle tooltip

Click on the devices to open a pop-up with additional information.

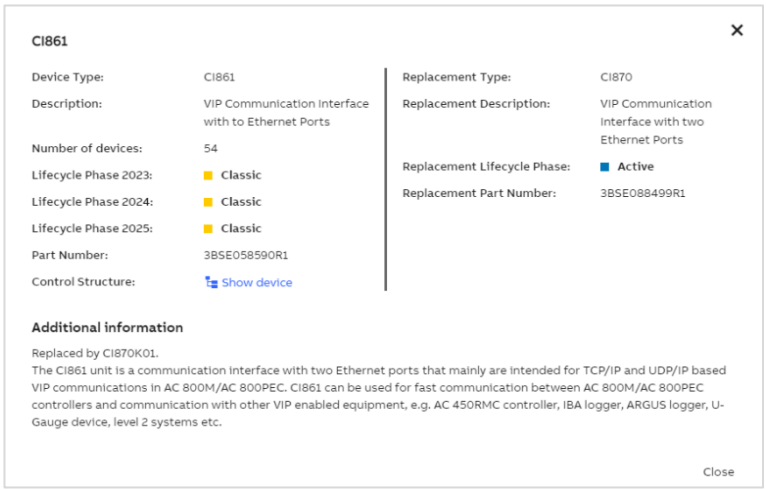
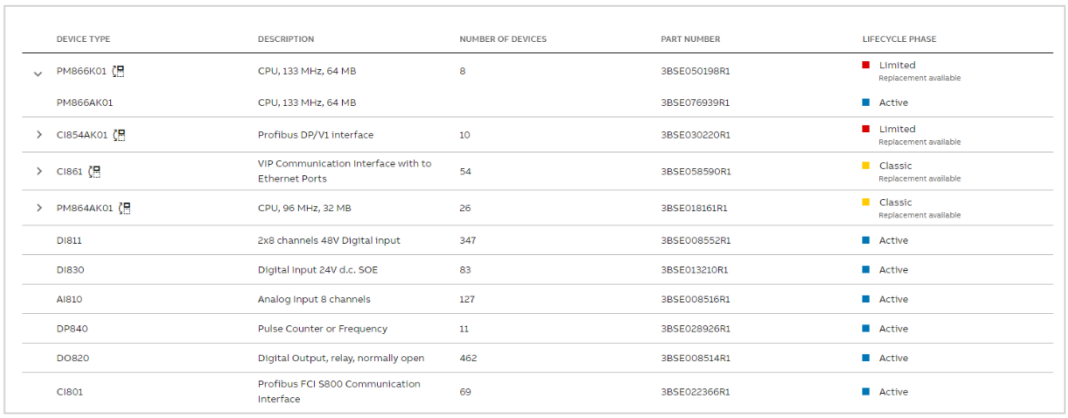


Figure 75: Hardware Lifecycle - Pop-up

The list view shows all devices and additional information in one combined list. The list is sorted descending with the device with the worst lifecycle status (Obsolete) and highest number of devices listed on top.

Click on the device name to open a pop-up with additional information.



DEVICE TYPE	DESCRIPTION	NUMBER OF DEVICES	PART NUMBER	LIFECYCLE PHASE
PM866K01	CPU, 133 MHz, 64 MB	8	3BSE050198R1	Limited Replacement available
PM866AK01	CPU, 133 MHz, 64 MB		3BSE076939R1	Active
CI854AK01	Profibus DP/V1 interface	10	3BSE030220R1	Limited Replacement available
CI861	VIP Communication Interface with to Ethernet Ports	54	3BSE058590R1	Classic Replacement available
PM864AK01	CPU, 96 MHz, 32 MB	26	3BSE018161R1	Classic Replacement available
DI811	2x8 channels 48V Digital Input	347	3BSE008552R1	Active
DI830	Digital Input 24V d.c. SOE	83	3BSE013210R1	Active
AI810	Analog Input 8 channels	127	3BSE008516R1	Active
DP840	Pulse Counter or Frequency	11	3BSE028926R1	Active
DO820	Digital Output, relay, normally open	462	3BSE008514R1	Active
CI801	Profibus FCI S800 Communication Interface	69	3BSE022366R1	Active

Figure 76: Hardware Lifecycle - list view

In case the asset inventory data does not match your current installation on site, clear inventory data and re-upload your latest collection file. Click on the banner displayed on the top of this tab or go directly do the Inventory data sets tab to initiate the process.

Figure 77: Banner for incorrect asset inventory data

2.2.10.2. Assets

The Assets tab gives you an overview about all found assets in the control system and their status in the different KPI categories (Performance, Software, Security). The overall result for each category is a sum of error and warnings with the label which matches the color of the worst result. To see the exact number of errors and warnings separately, hover over the number of findings. Only error and warnings are shown in this view. If there are no errors or warnings a green checkmark is displayed. Click on the number of findings to directly jump to the KPI analysis of the respective category and view the KPIs in the grid view.

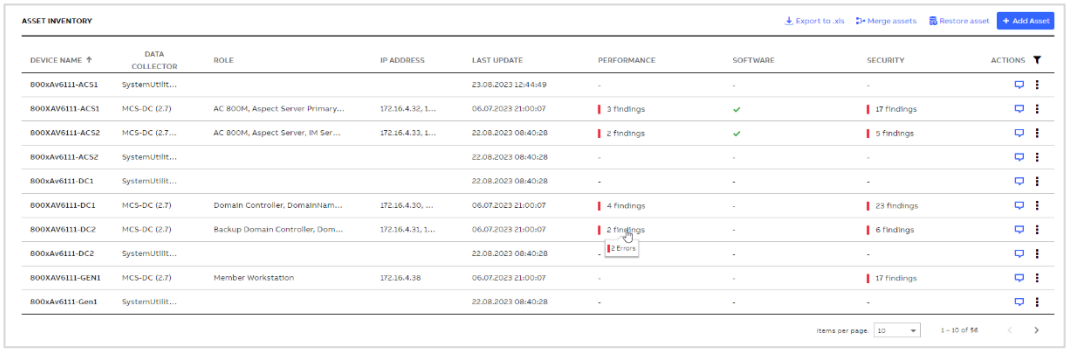


Figure 78: Asset Inventory widget

Some assets might be shown in the widget multiple times (due to changes that happened over time with them). In order to clean up the list, the following options are available:

1. Delete them individually
2. Use “Clear inventory data” function (Chapter Inventory2.2.12.2.2) to delete all assets

Filters are available to narrow down displayed items.

- Click on the filter icon to expand or clear and hide filters
- Apply filters in each column to narrow down displayed items
- Click on “x” icon to clear all filters

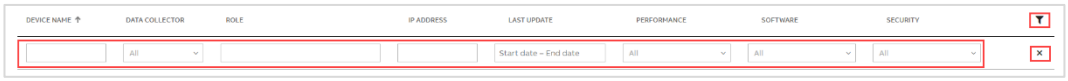


Figure 79: Filters

The following options are available under the additional menu for a single asset:

- Comment
- Edit asset details – you will be redirected to the asset details view with edit mode enabled
- Merge with another asset – this option is not available for assets added manually
- Edit merging – this option is displayed for assets which have already been merged with another item
- Delete – allows you to remove an asset from the system

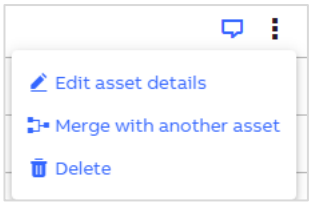


Figure 80: Asset options

An empty comment icon indicates that there is a possibility to add a comment whereas a filled in icon shows that the comment has already been added. Hover over the icon to see the tooltip with the comment.

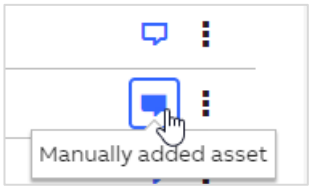


Figure 81: Asset comment

Click on the empty comment icon to add a comment.

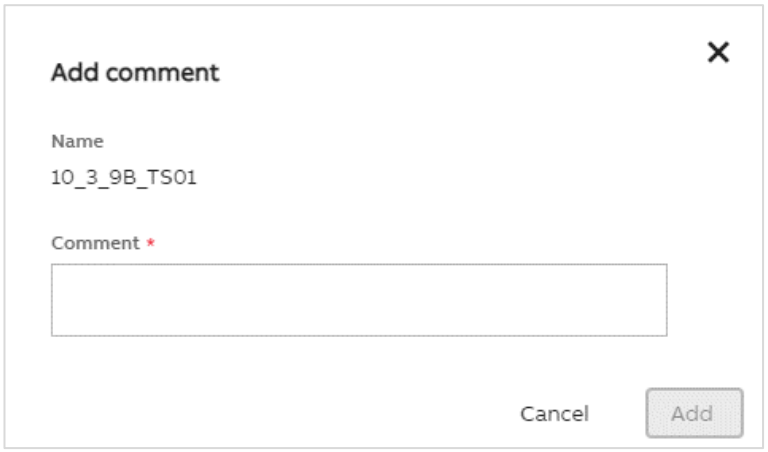


Figure 82: Add comment

Click on the filled in comment icon to check who and when updated the comment or to update it.

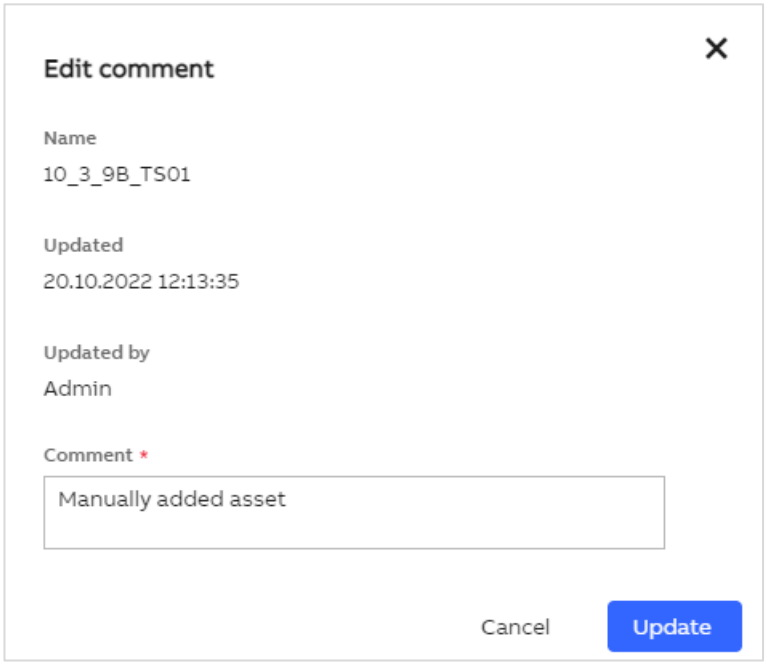


Figure 83: Edit comment

After choosing the “Merge with another asset” option, you will see the details of the selected asset and a dropdown with the lists of assets with which a merge can be done. Select an asset in the dropdown and click on “Merge”. Selected asset will be displayed in the summary section. An asset which is a master is marked with the blue label displayed next to the asset’s name.

Use “set as master” button if another asset should be set as a master. If MCS-DC asset(s) is among assets which should be merged, only this one can be set as a master. System Utilities asset cannot be set as a master.

Use “x” icon to remove an asset and not merge it.

Confirm your selection by clicking on “Save”.

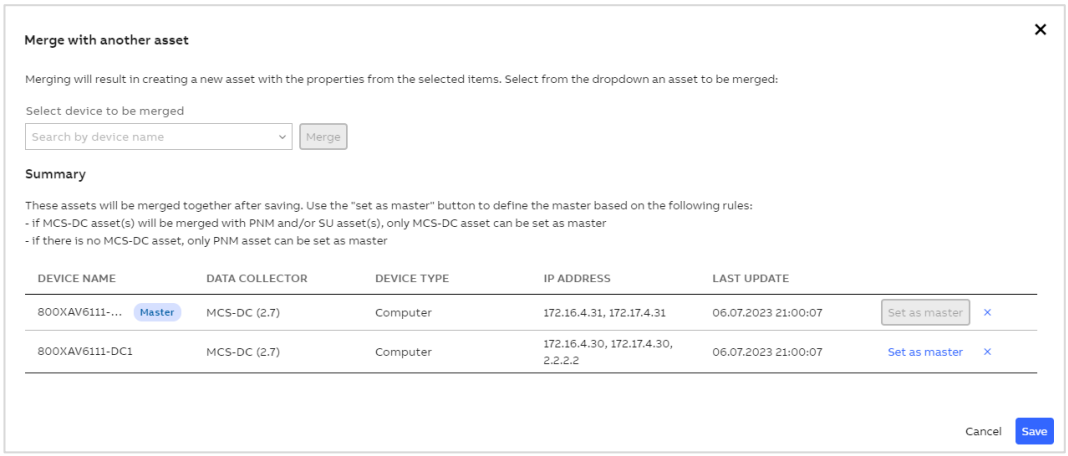


Figure 84: Merge with another asset

If assets have already been merged together, “Edit merging” option is displayed.

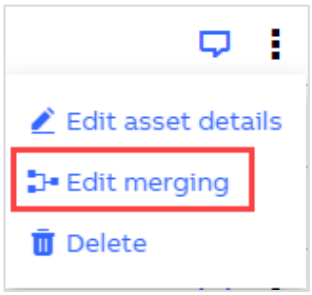


Figure 85: Edit merging

All options which are available for “Merge with another asset” are here as well. Additionally, it is possible to unmerge all assets using “unmerge all assets” button:

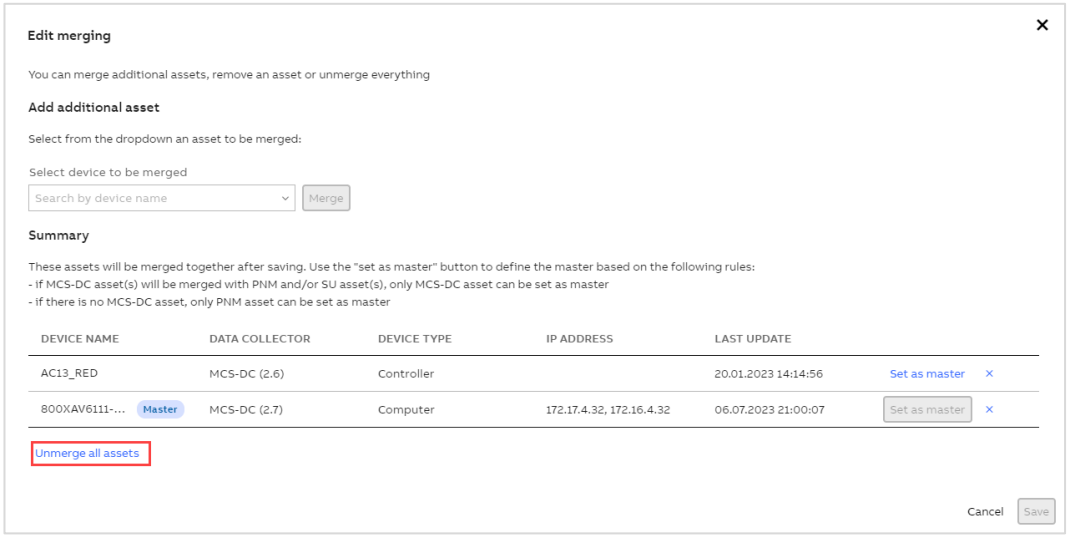


Figure 86: Edit merging dialog and unmerge all assets option

Additional options are available in the top right corner of the Asset Inventory widget:

1. Export to .xls

2. Merge assets
3. Restore asset
4. Add asset

Figure 87: Additional options

To export the list of all assets, click on “Export to .xls” button. A file containing all assets and their details will be generated.

Under “Merge assets” button, the list of merging suggestions are listed. This option is not displayed if “Perform automatic asset merging” is selected in the assets merging setting. If there are no suggestions, the button is disabled with a tooltip indicating the reason.

The table displays all merging suggestions. Expand the assets to see the details. Use check-boxes on the left side and “Accept selected” to accept only specific suggestions or “Accept all”.

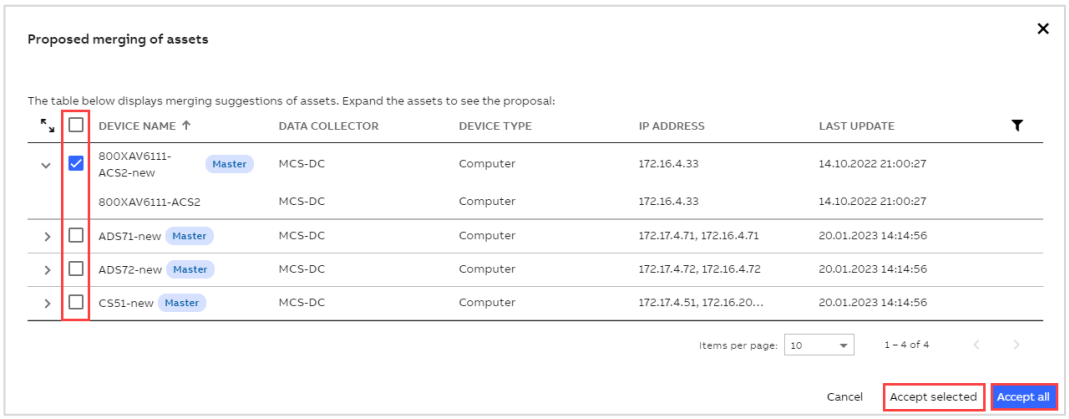


Figure 88: Proposed merging of assets

Each device which has not yet been permanently deleted can be restored using “Restore asset” button available in the top right corner of Asset Inventory widget. Click on the button to see the list of assets which can be restored.

Select assets which you would like to restore and click on “Restore selected”.

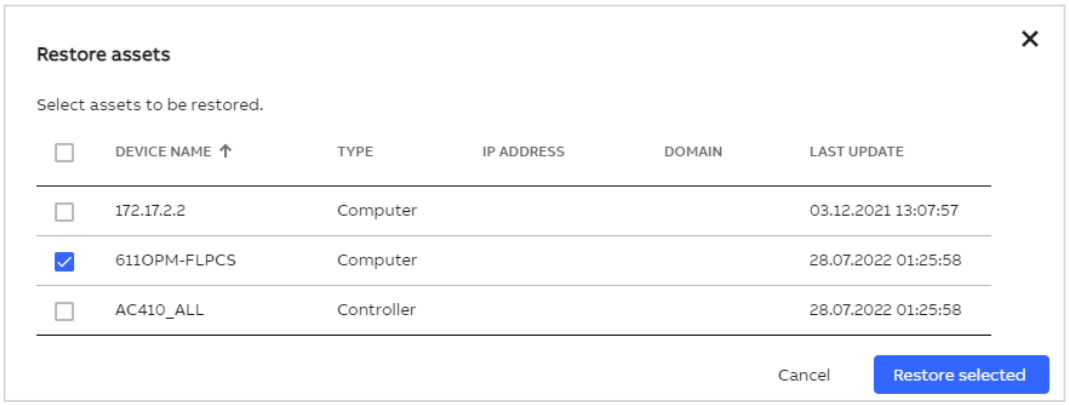


Figure 89: Restore selected

To add an asset manually, click on “Add asset” button and provide all required data. Click on “Add” button to confirm. Newly added asset will be listed on the Asset Inventory widget.

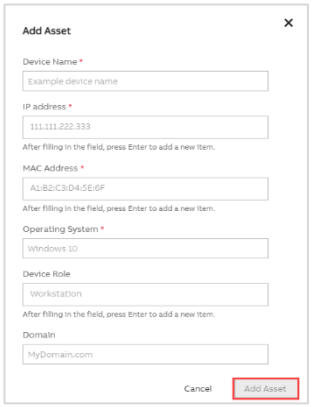


Figure 90: Add asset

Click on the device name in the Asset Inventory widget to jump to the overview of the selected asset. Items displayed in the menu on the left side, depends on the selected asset.

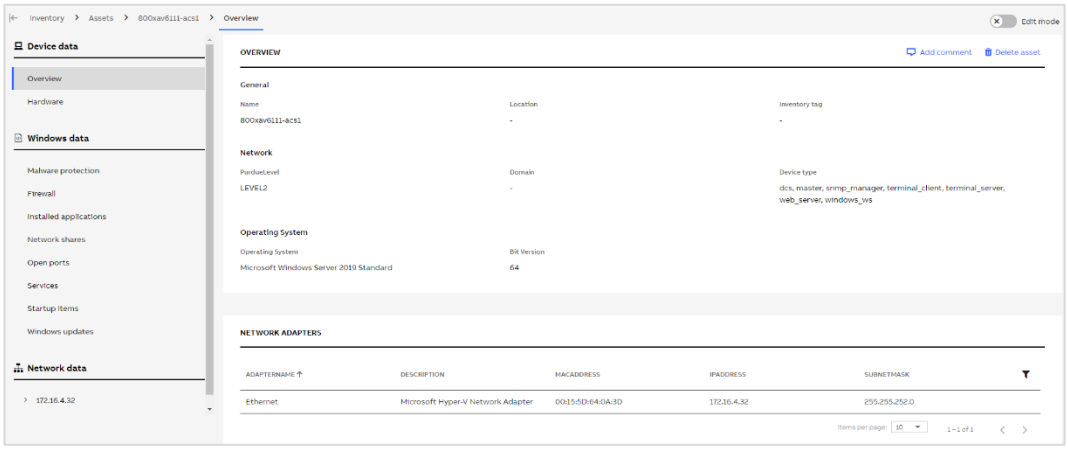


Figure 91: Asset details

If selected asset is a controller, control structure is displayed in the left pane instead of the navigation tabs. Click on the device name in the left pane to switch between the details views of the control structure.

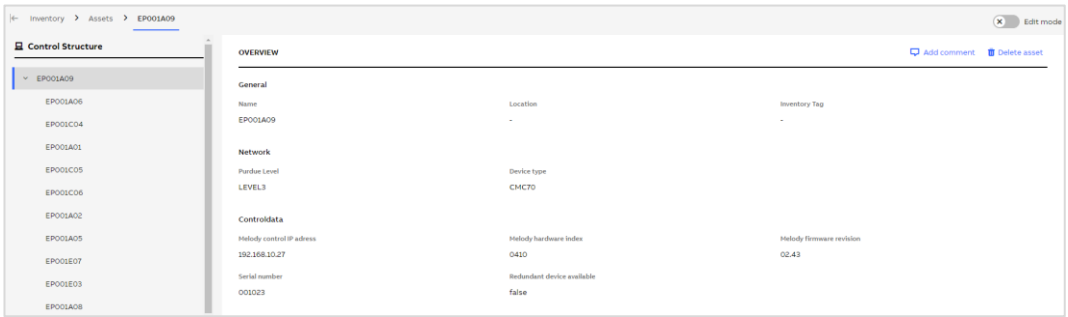


Figure 92: Controller details on Asset tab

Only the root items of the control structure can be found on the Assets tab. All items are listed on the Controllers widget on the Control Structure tab.

To edit data, enable edit mode using the switch located in the top right corner of the asset details page. “Discard changes” and “Save changes” buttons will be enabled once you modify any field.

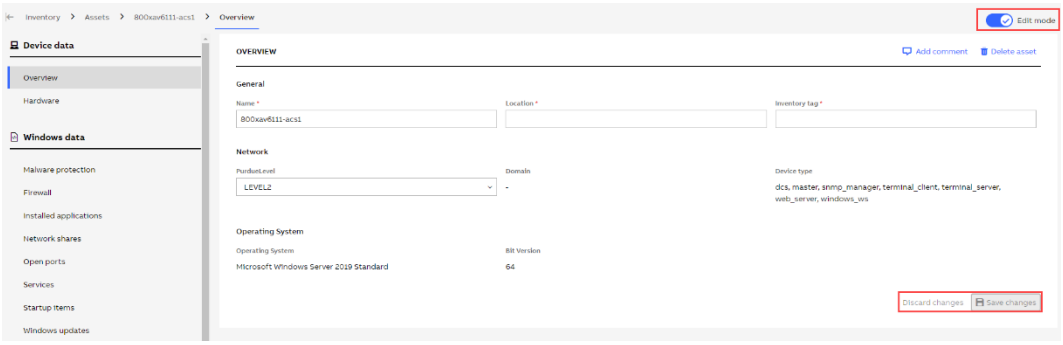


Figure 93: Edit mode

Options to add or update comment or delete asset are also available on asset overview tab.

Figure 94: Asset details - comment or delete asset

Add, merge with another asset, undo merge, delete, edit or restore asset actions on Asset Inventory widget and asset details in the MCS on-premise application are only visible for logged in users having the “Administrator” or “Asset Inventory Administrator” user role assigned.

In case the asset inventory data does not match your current installation on site, clear inventory data and re-upload your latest collection file. Click on the banner displayed on the top of this tab or go directly do the Inventory data sets tab to initiate the process.

Figure 95: Banner for incorrect asset inventory data

2.2.10.3. Control Structure

The Control Structure tab gives an overview of all controllers in the control system, their device type, hardware and firmware revision as well as IP address, position and their lifecycle phase.

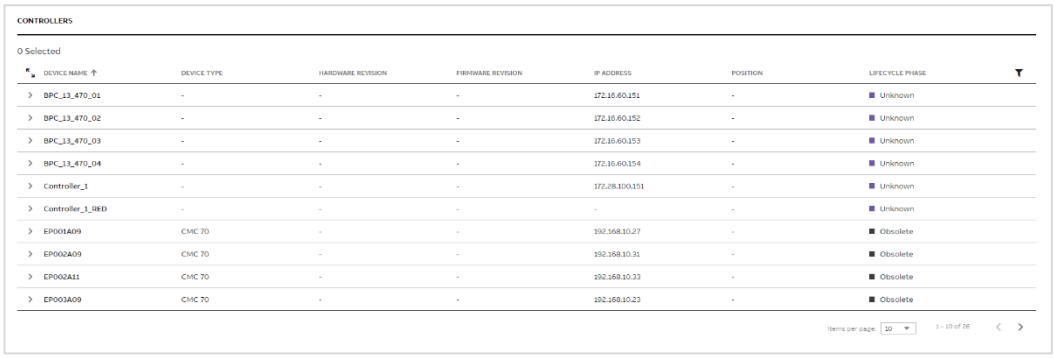


Figure 96: Control Structure widget

In case the device type could not be identified and an “visual inspection is required”, use the edit icon displayed next to the lifecycle phase of the specific item or select checkbox(es) next to the device name and then click on “Specify device type” button on the top of the widget to specify the device type.

Figure 97: Specify device type for single item

When using the checkboxes, only items with the same device type can be selected.

Figure 98: Specify device type for one or multiple items

Select the device type in the dropdown and click “Save” to confirm.

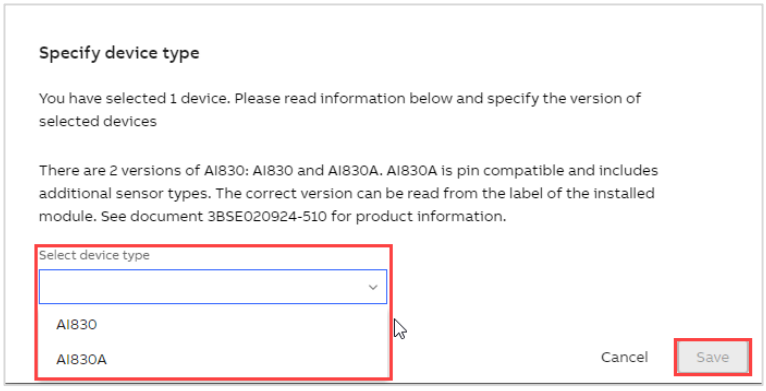


Figure 99: Specify device type dialog

If the device type has been selected manually, this action can be reverted. Click on the edit icon next to the lifecycle phase. Information what was the original device type as well as who and when modified it is displayed in the dialog. Click on “Revert changes” to bring back the original value.

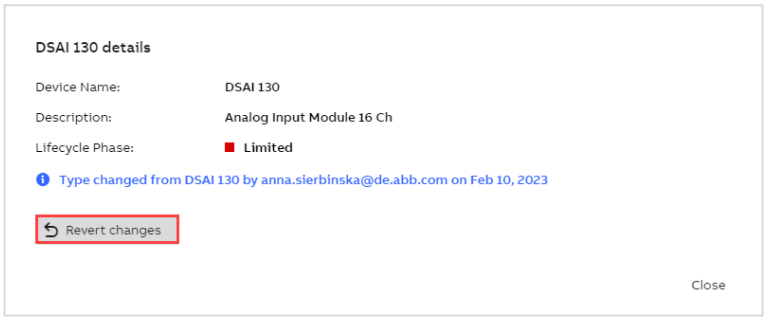


Figure 100: Revert changes dialog

Click on the device name in the Controllers widget to jump to the overview of the selected item. The structure of the controller is displayed in the left pane to allow switching between the detail views of the devices.

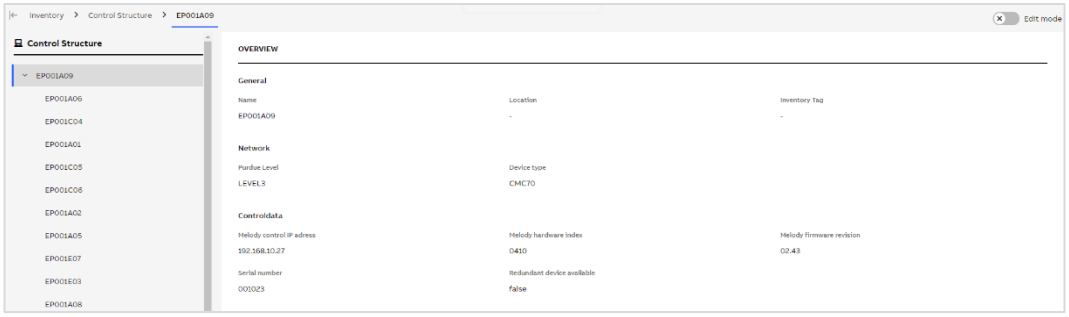


Figure 101: Controller details

To edit data, enable the edit mode using the switch located in the top right corner of the controller details page. “Discard changes” and “Save changes” buttons will be enabled once you modify any field.

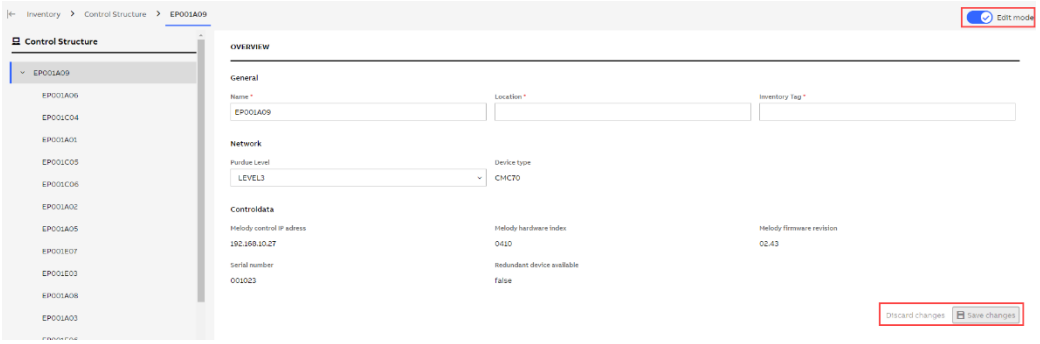


Figure 102: Edit mode

Edit action on the controller details view as well as options to specify the device type or revert this change in the MCS on-premise application is only visible for logged in users having the “Administrator” or “Asset Inventory Administrator” user role assigned.

2.2.10.4. Software

The Software tab shows a list of all installed software.

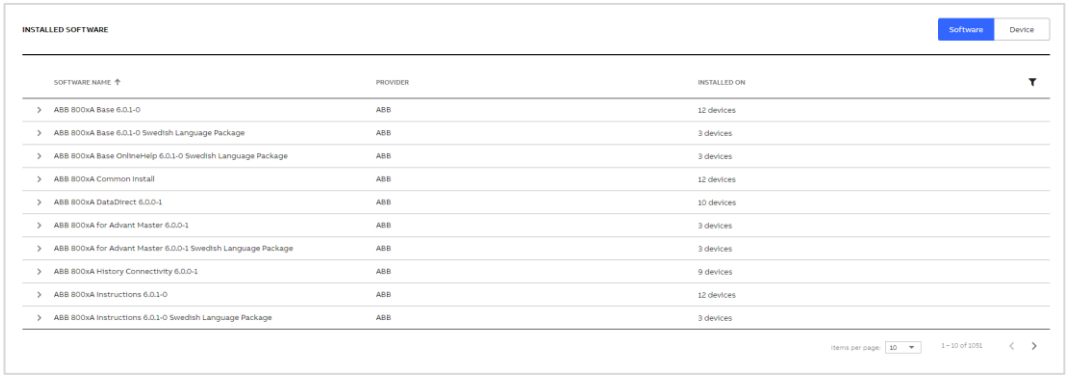


Figure 103: Installed software – software view

Click on the expand icon next to the software name to see all the computers where this software is installed on.

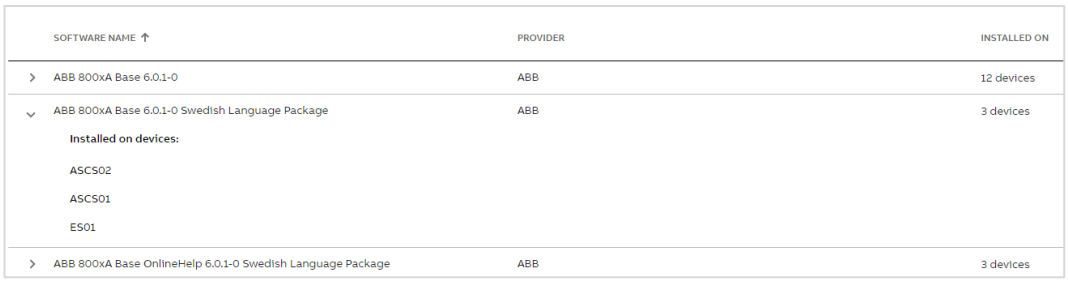


Figure 104: Installed on devices

Use the switch in the top right corner to see the list of all computers in the control system with software installed.

Figure 105: Software/Device view switch

Click on the expand icon next to the device name to see the software installed there.

Figure 106: Installed software - device view

On both software and device views, filters can be used to find out on which computer a specific software is installed.

2.2.11. Documentation

You have the possibility to view the release notes information as part of the application for the respective released version.

The following three release notes information categories are published:

– What's new

– Fixed Issues

– Known Issues

The **What's new** section provides information about newly added, enhanced, or modified functionality. Under section **Fixed Issues**, we are listing solved product issues and the **Known Issues** section always contains the list of known issues for the particular version released.

The release notes information is accessible either using the quick link available in the footer section of the application called "[Release Notes]" (Chapter 2.2.3) or by direct navigation to the Documentation/MCS Release Notes section.

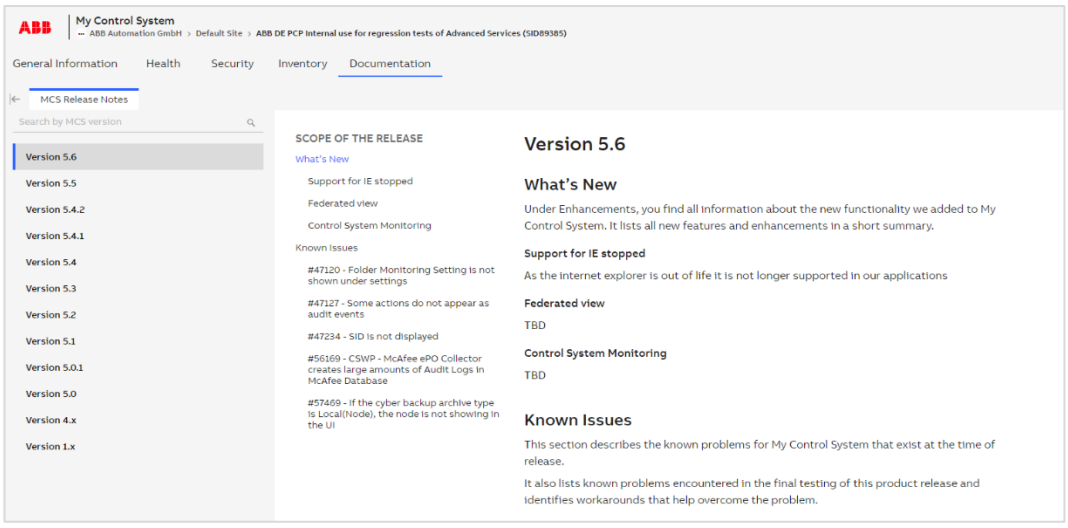


Figure 107: Release Notes Information

2.2.12. Administration and Configuration Area

The Administration and Configuration area of the MCS-OP dashboard is in the upper right corner and consists of a couple of icons used to administrate the operational environment of your MCS-OP application. These icons provide access to the functionalities described in the following chapters:

1. Contact ABB section: Please refer to chapter 2.2.12.1 for details

2. Data set management section: Please refer to chapter 2.2.12.2 for details

3. Settings section: Please refer to chapter 2.2.12.3 for details
4. Notifications section: Please refer to chapter 2.2.12.4 for details
5. User section: Please refer to chapter 2.2.12.5 for details

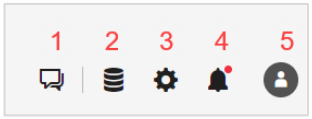


Figure 108: Icons of the Administration and Configuration area

2.2.12.1. Contact ABB section

The “Contact ABB” section of the Administration and Configuration area is intended to be used in case the user might need support from ABB experts to either configure his/her local MCS-OP environment to his/her needs or to report an issue.

The “Contact ABB” icon is only visible for logged in users having either the “Administrator” or the “Contact ABB Operator” user role assigned.

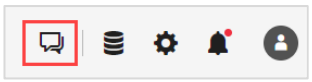


Figure 109: Contact ABB section of Administration and Configuration area

Please provide following information in the upcoming contact form before sending your request to ABB support via E-mail:

- Personal information like name, e-mail address and phone number
- Company information
- Used ABB product family and version
- Plant name and SID
- Desired Reaction Time (select from drop down menu). Only visible in case this setting has been preconfigured in the “Contact ABB” settings, chapter 2.2.12.3.5
- Request details

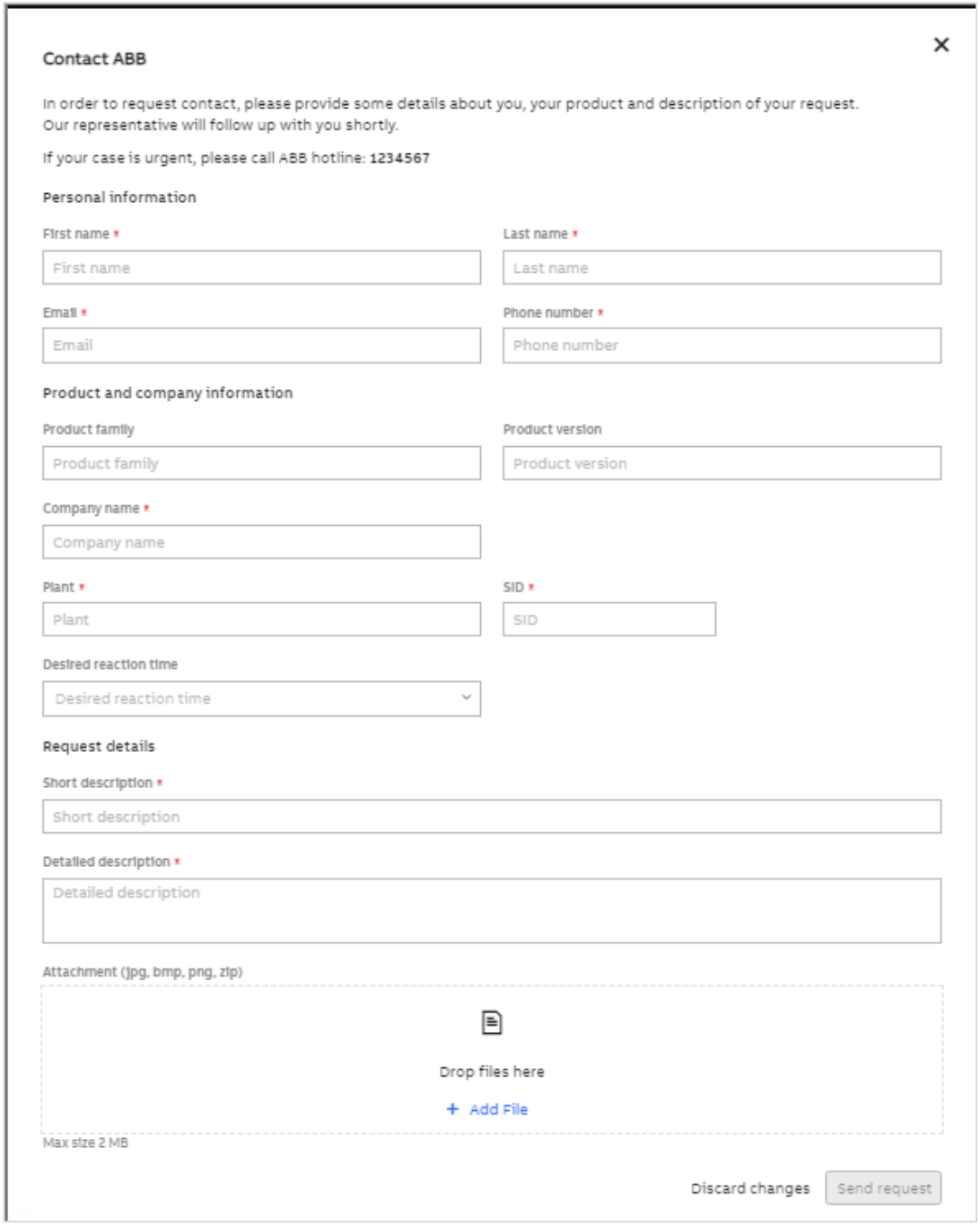


Figure 110: Contact ABB form

By selecting the “Send request” button on this form an E-mail containing the provided information is sent out to a preconfigured ABB recipient.

A detailed description on how to configure the recipient of this E-mail and the desired reaction time as well as on how to setup an E-mail SMTP server is provided in chapter 2.2.12.3.5 “Contact ABB tab” of this manual.

2.2.12.2. Data set management section

The data set management section of the Administration and Configuration area provides the needed functionality to manage previously collected data sets.

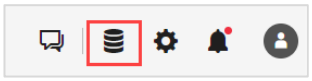


Figure 111: Data Sets Management section of Administration and Configuration area

Data sets management section consists of two tabs:

- KPI
- Inventory

2.2.12.2.1. KPI

To prevent any unauthorized data modification, a newly created data set is locked to the user or instance (e.g. MCS-OP) that created it. To be able to do any modification on the data set (e.g. renaming) or on the data within the data set (e.g. changing a KPI result) you need to take over the data set. Click on the “lock” icon next to the data set name to take over the data set.

The main dashboard of this section displays all previously collected data sets with their details, namely:

- Data set name
- Creation date
- User who created the data set
- Collected KPI categories (Performance, Software, Security)

Blue checkmarks indicate which category has been collected.

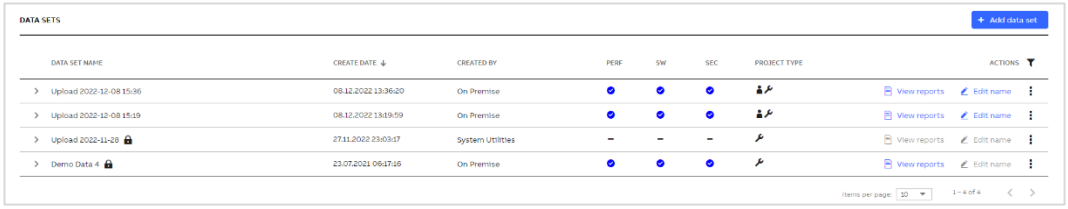


Figure 112: Data set management

Depending on the enabled functions data sets with different content are created.

Data collected via the MCS-DC will result in a data set created by “On Premise”, while data collected with CSWP functionalities will result in a data set created by “SystemUtilities”.

Actions and Options might vary between the different data set contents.
E.g. Reports are not available for “SystemUtilities” data sets.

By selecting the Reports icon all already generated reports related to the selected data set can be displayed.

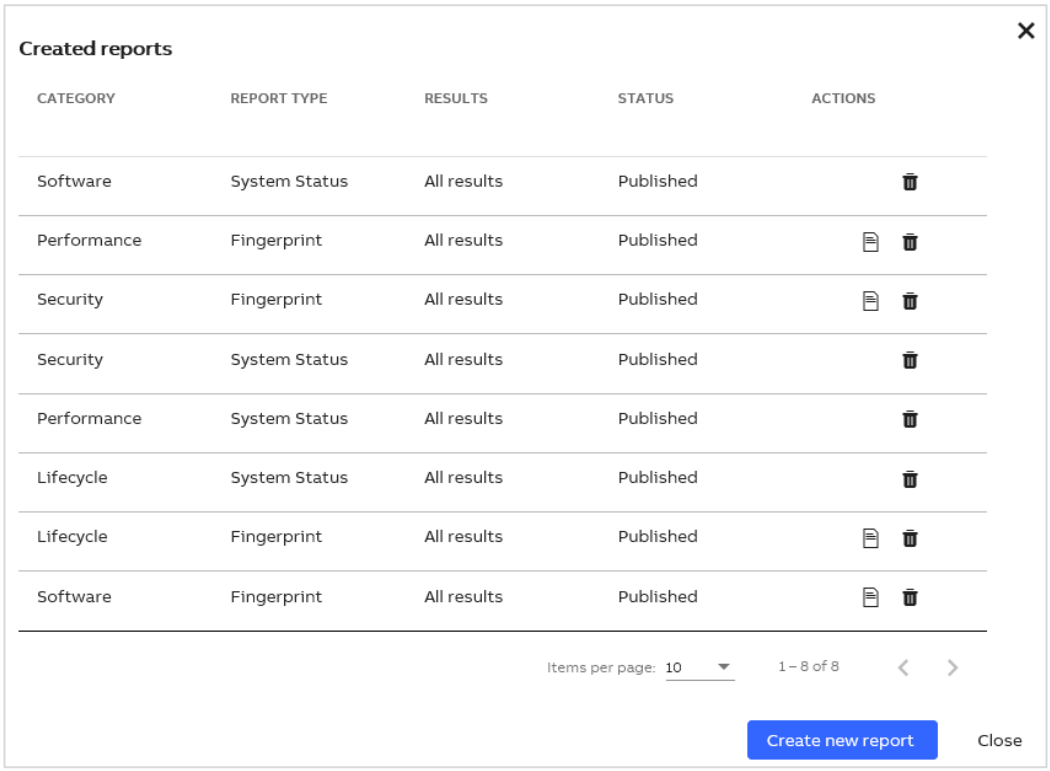


Figure 113: Created reports list

The Actions section provides all necessary functionalities to manage and edit your data sets. These functionalities are described in detail in the following chapters.

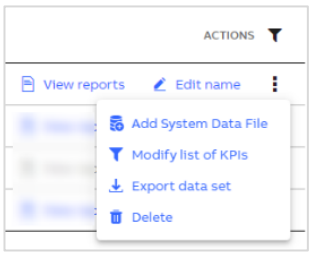


Figure 114: Actions section within Data set management

Furthermore, you can expand/collapse the selected data set to figure out the raw system data files the results displayed in the system data set are based on.

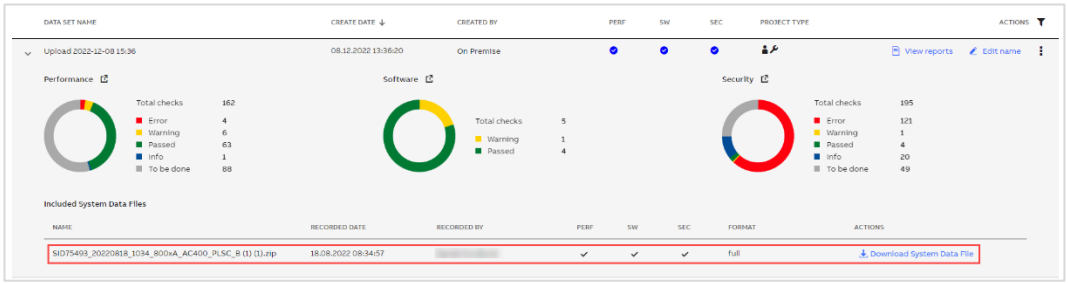


Figure 115: Expanded data set

Adding a data set

Click on the “Add data set” button located in the upper right corner of the “Data Sets” widget. A pop-up window will be displayed where you can select option to create new data set or import an existing one.

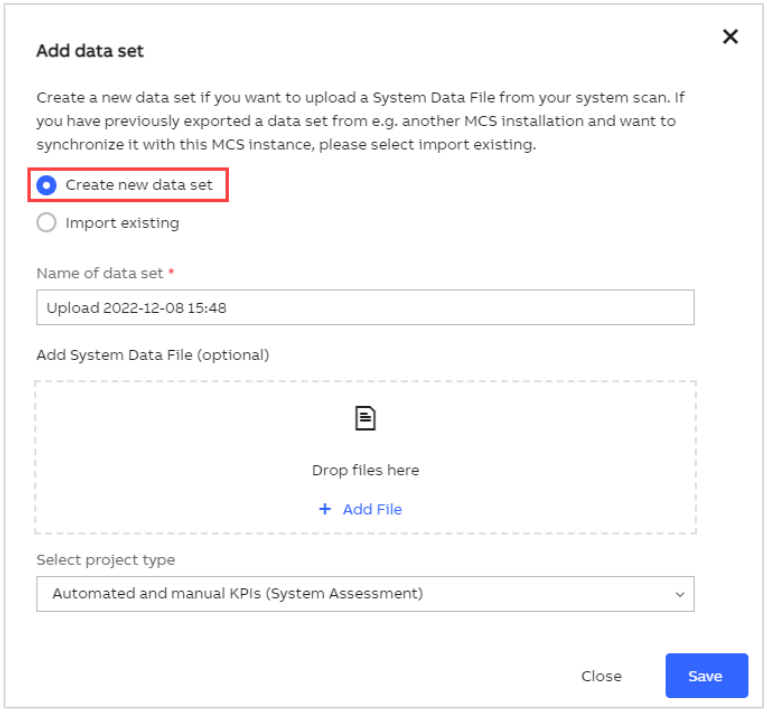


Figure 116: Create new data setWhen creating new data set, in case you have the applicable System Assessment license you can choose the project type (Automated KPIs / Automated and manual KPIs) otherwise only Automated KPIs are available. Then click on the “Save” button. After that the new created data set is displayed in the “Data sets” widget.

To import a previously exported data please select the “Import Data Set” button located in the upper right corner of the “Data Sets” widget. The following pop-up window will show up:

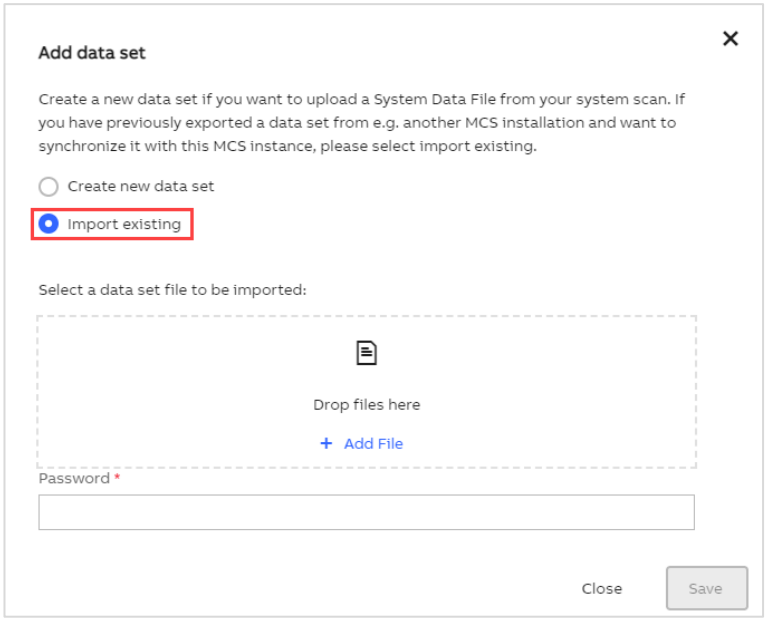


Figure 117: Import existing data set

Please select the Data Set you would like to (re-)import to your local MCS-OP application from the hard disk and place it in the respective drop field.

During the export process of the Data Set an initial password has been defined.
This process is described in detail in thischapter. . The same password needs to be used when (re-) importing this Data Set to your local MCS-OP application.

Adding a system data file

Once the new data set is saved you can manually upload the collected SDF by using the “Add File” button. A pop-up window will come up where you can select the data file. Please consider that the name of the uploaded file must begin with the SID number you want to upload to. After the file is selected, the system will automatically analyze the uploaded raw system data file. This might take some minutes to complete.

After the file has been analyzed a confirmation message stating that the pop-up window can be safely closed will be displayed. In case of issues during analysis like e.g., wrong file extension, relevant information will be displayed in the pop-up window.

Downloading a system data file

It is possible to download the SDF of a specific data set from the data set management. To do so, please expand a selected data set and then select the Download icon in the lower right corner next to the SDF name.

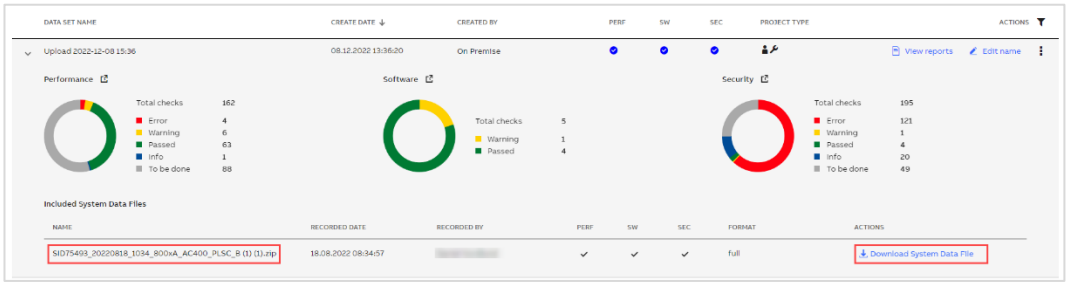


Figure 118: Possibility to download an SDF of a specific data set

Renaming a data set

You have the possibility to rename an existing data set. To do so, select the pencil icon in the Actions section and a pop-up window will be displayed where you can rename the selected data set.

Modifying the KPI list

To prevent specific sections or KPIs from being displayed in the analysis results of a specific data set you could modify its KPI list. The KPI list of a data set is created automatically based on your system configuration and the existing licenses.

To do so, please select the Filter icon from the Actions section to modify the KPI list. You can then use toggle buttons to select/deselect individual KPIs or KPI groups.

Deleting a data set

Select the trash icon from the Actions section to delete a selected data set. Please consider that all information associated with this data set, including reports, will be deleted. A pop-up window will ask you to confirm deletion.

Importing a system data file

In principle there are two different ways to import system data files generated by the MCS-DC software into your local MCS-OP application:

– Automated import via MCS-FW using shared folder
  To automatically import and analyze the collected data, a shared folder needs to be configured. The folder path of this shared folder needs to be entered in both applications, namely MCS-FW and MCS-OP during installation. System data files provided by the MCS-DC and placed in this shared folder by MCS-FW are then automatically imported and analyzed by the MCS-OP application. Please refer to document ref. [1] and [2] for detailed information on how to setup this functionality.

– Manual import
  To manually import system data files first a new Data Set must be created before the new system data file could be imported. This process is described in detail in this chapter.

Exporting a data set

To export a data set from your MCS-OP select the data set you would like to export and press the export icon in the Actions section on the right side.

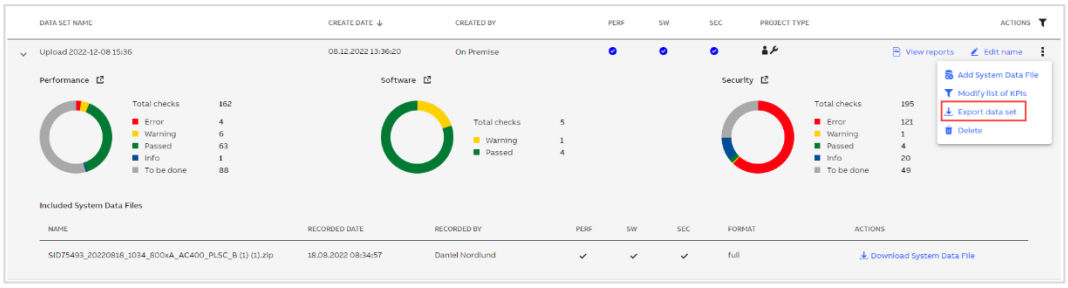


Figure 119: Exporting a Data Set via export tool

According to ABB cyber security guidelines exported customer data has to be password protected. For this reason, a new pop-up window will appear where you must specify a password for the Data Set to be exported.

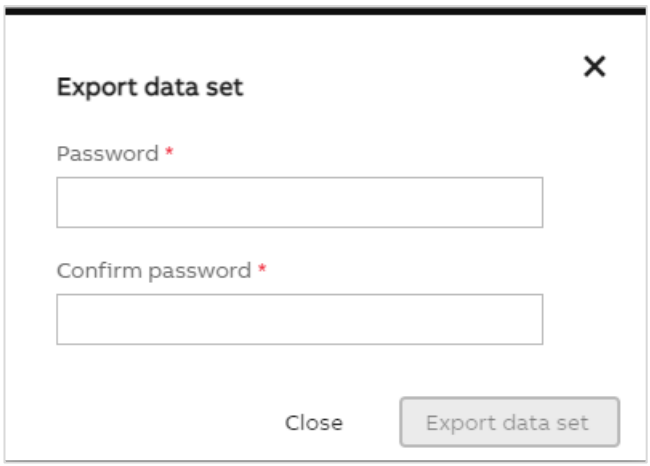


Figure 120: Specify password for exported Data Sets

The Data Set export is started by selecting the “Export Data Set” button inside this pop-up window. The Data Set export will then be stored on your local hard drive.

2.2.12.2.2. Inventory

The inventory tab is used to manage inventory reports, check data import history or clean inventory data.

In the “Inventory Reports” widget you can find the list of already generated inventory reports. Use “Create new report” button to generate new inventory or lifecycle reports.

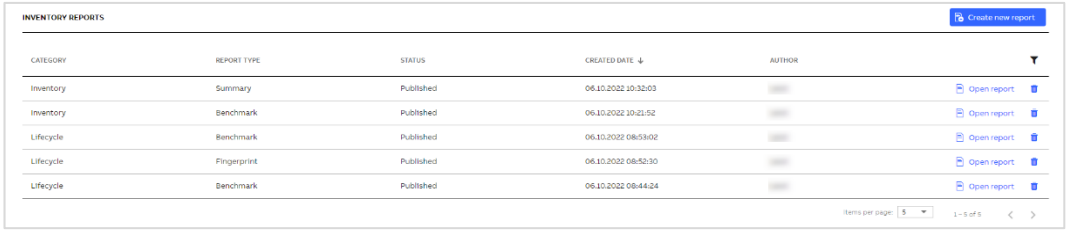


Figure 121: Inventory Report widget

The “Data import history” widget shows information about the data collector, upload date and who uploaded the data. You can also use create a new data set or import previously exported data set from this widget.

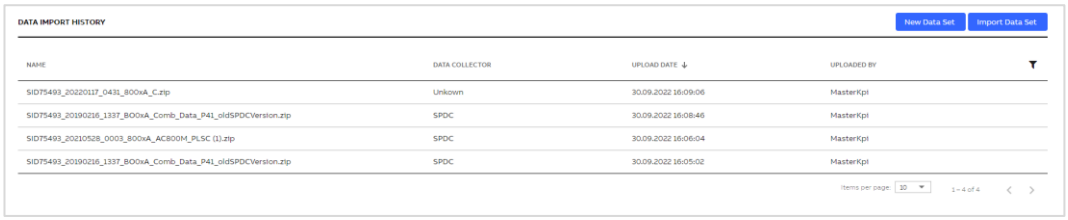


Figure 122: Data Import History

To clear all inventory data, click on the button located in the top right corner of this tab.

Figure 123: Clear inventory data

Clear inventory data in the MCS on-premise application is only visible for logged in users having the “Administrator” or “Asset Inventory Administrator” user role assigned.

2.2.12.3. Settings section

The Settings section of the MCS-OP application is used to manage and preconfigure the working environment of your MCS-OP application. This section consists of in total five tabs providing different functionalities. These functionalities are described in detail in the following chapters.

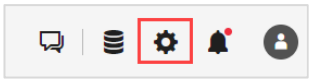


Figure 124: Settings section of Administration and Configuration area

The “Settings” section of Administration and Configuration area is only visible for logged in users having the “Administrator” user role assigned.

2.2.12.3.1. Applications tab

The management of software packages installed on the local MCS-OP application is done in the “Applications” tab of the Settings section.

The “Applications” tab provides the name of the node where MCS-OP is installed on. It also provides an overview of the currently installed software packages with their names and specific versions on the left side. On the right side there is the possibility to install additional MCS-OP feature set packages delivered together with the system software but not yet installed like e.g., the System Monitoring or the Site View feature set.

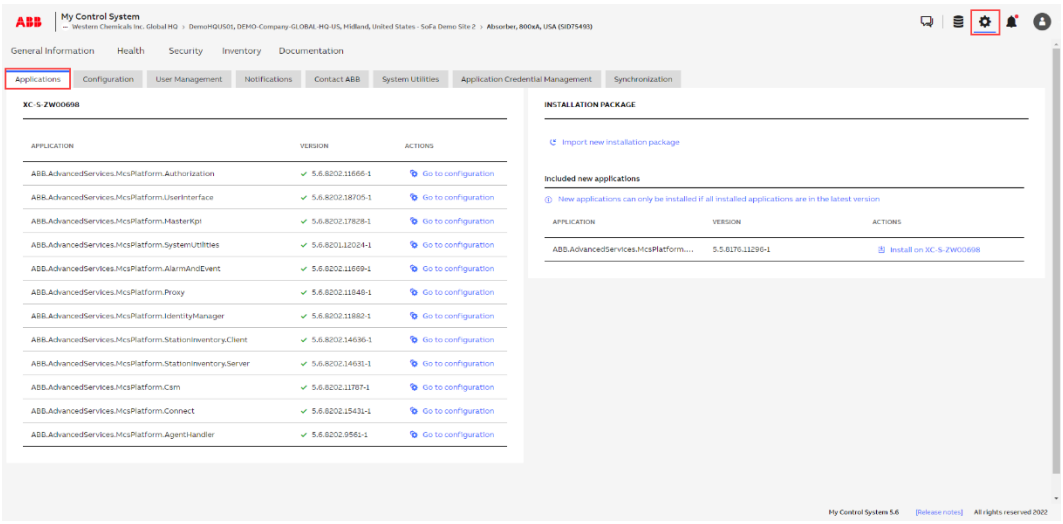


Figure 125: Applications tab – Settings section

In addition, there is a possibility to navigate to the application specific configuration.

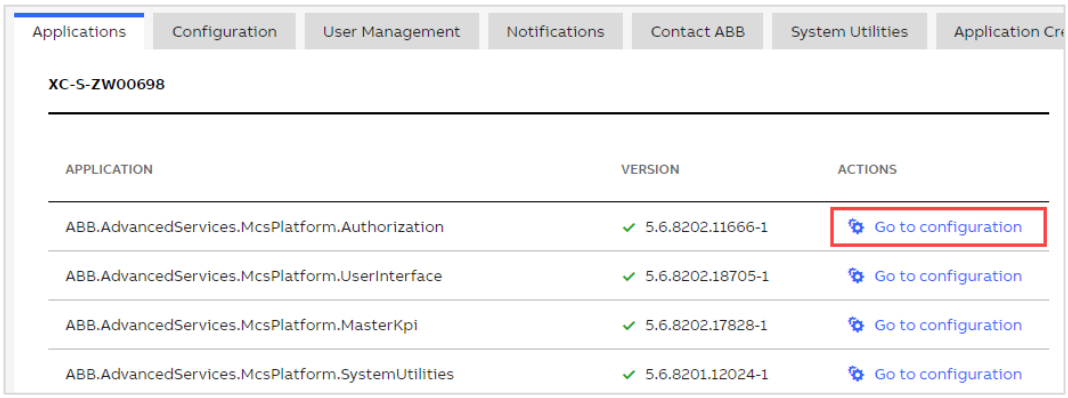


Figure 126: Application specific configuration access

MCS-OP software packages are updated on a regular basis and provided in MCS in the Web for download. Before being able to update the MCS-OP software packages installed the new versions need to be downloaded from MCS in the Web and copied to the MCS-OP hard disk.

Please refer to document ref. [1] for detailed information on the upgrade procedure.

2.2.12.3.2. Configuration tab

The Configurations tab in the Settings section provides the possibility to configure your MCS-OP platform environment and adapt it to the conditions on site. In addition to the basic settings used by the MCS-OP platform like e.g., used SID, used service account, URL of the used computer …etc. it also provides a list of dedicated settings used by individual functionalities like e.g., the Cyber Security Workplace functionality.

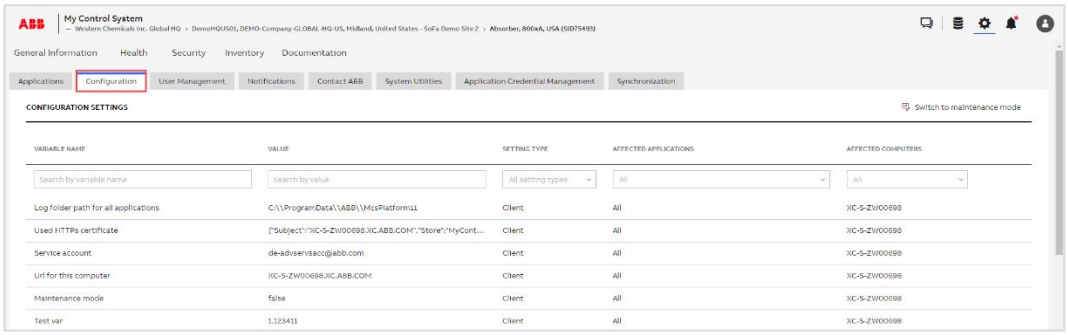


Figure 127: Overview of settings

As a prerequisite to edit configuration settings the logged in user needs to have Administrator use role granted. For details on how to setup users and assign specific user roles to them please refer to chapter 2.2.12.3.3 of this user manual.

To edit configuration settings please enable maintenance mode by selecting the “Switch to maintenance mode” button located in the upper right corner of the Configuration tab.

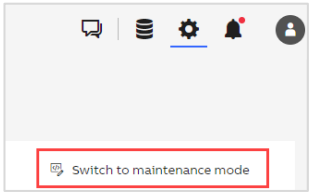


Figure 128: Enable “Maintenance mode” switch

To change a specific setting please press the pencil icon located on the right side of the selected setting. The value of the selected setting could be edited in the upcoming pop-up window. Save your configuration changes using the “Save” button.

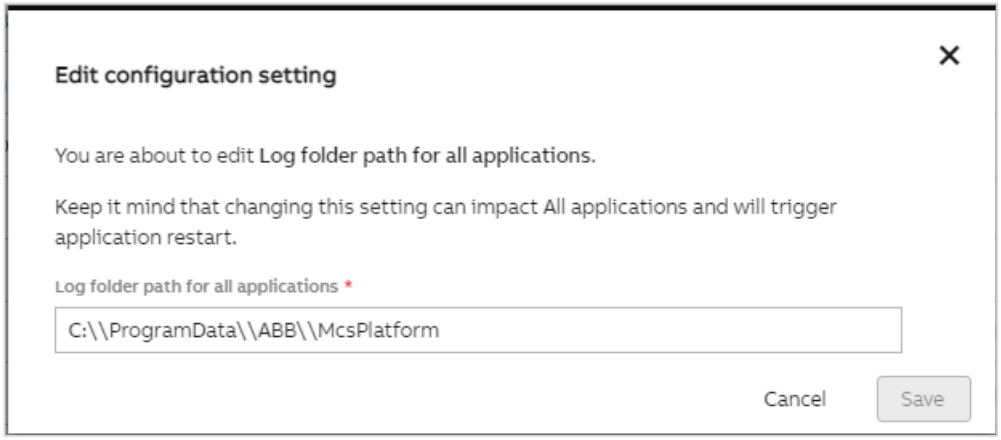


Figure 129: Edit configuration setting pop-up window

By default, the maintenance mode will be disabled after 15 minutes but could be extended with another 15 minutes using “Extend session time” button located in the banner displayed when maintenance mode is enabled.

Figure 130: “Extend maintenance mode” switch

2.2.12.3.3. User Management tab

The User management tab of the Settings section is used to configure and manage user accounts needed to access the MCS-OP application.

Within user management you have the possibility to define and configure local user accounts. In case the MCS on-premise computer is used in a Domain environment MCS on-premise supports the possibility to configure access for user accounts defined within this Domain in addition.

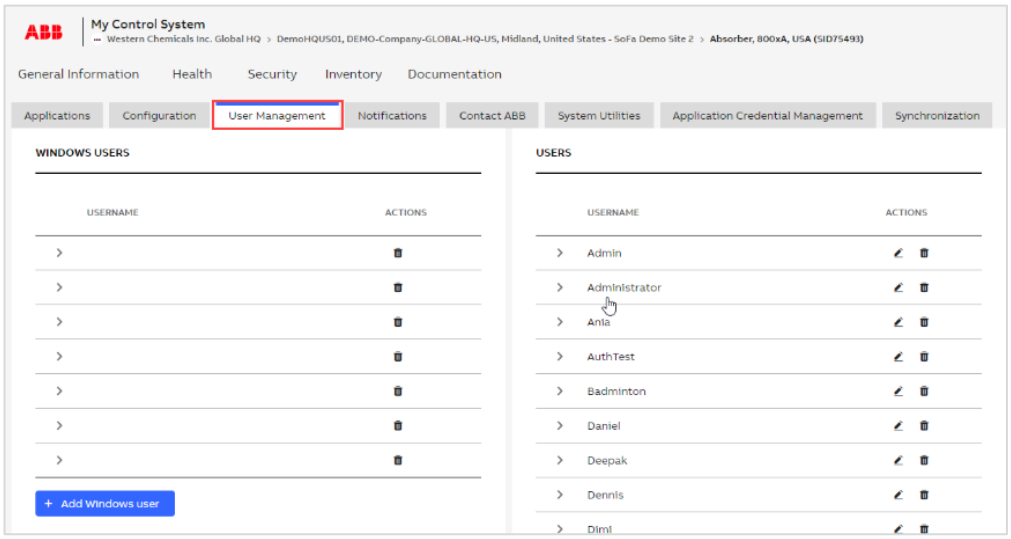


Figure 131: User Management tab in Configuration section

Please refer to document ref. [1] for detailed information on how to add/remove user accounts and on how to assign user roles to specific user accounts.

2.2.12.3.4. Notifications tab

The Notifications tab of the Settings section provides the possibility to setup and configure an SMTP E-mail server and a sender E-mail address. These settings will then be used to send user notification generated in the MCS-OP application to configured recipients.

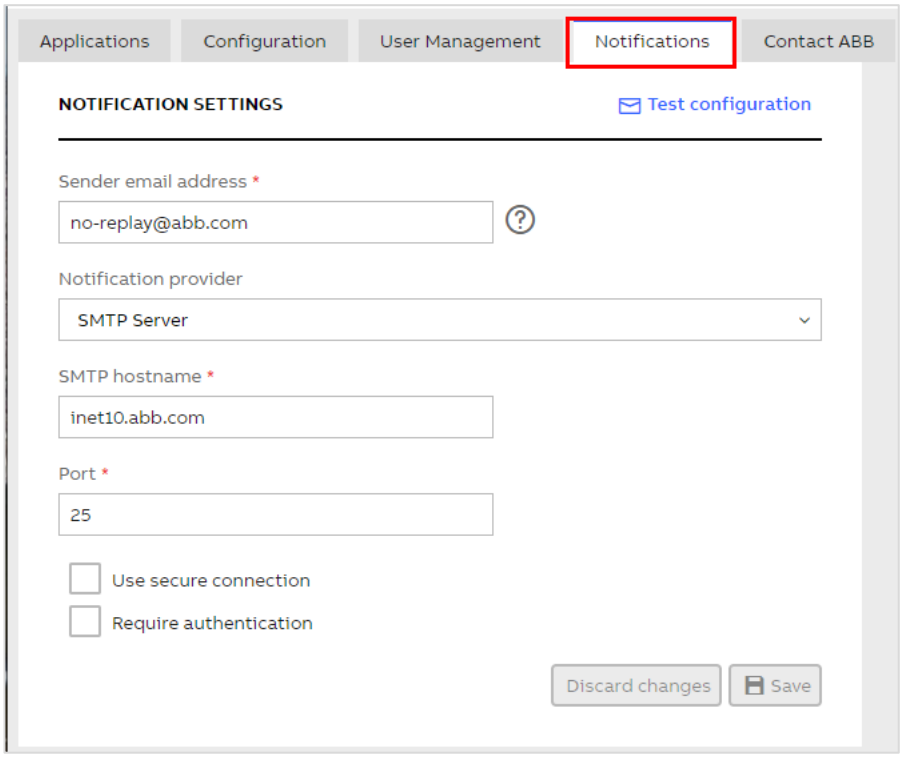


Figure 132: Notifications tab – Notification settings widget

Please refer to document ref. [1] for detailed information on how to setup an SMTP E-mail server to be used with your MCS-OP application.

2.2.12.3.5. Contact ABB tab

The Contact ABB tab of the Settings section is used to preconfigure general information which then is used as a default configuration for the form in Contact ABB section.
One of these preconfigured settings is for example the ABB Helpline number. This has only to be configured once and is then used for all E-mail communication.

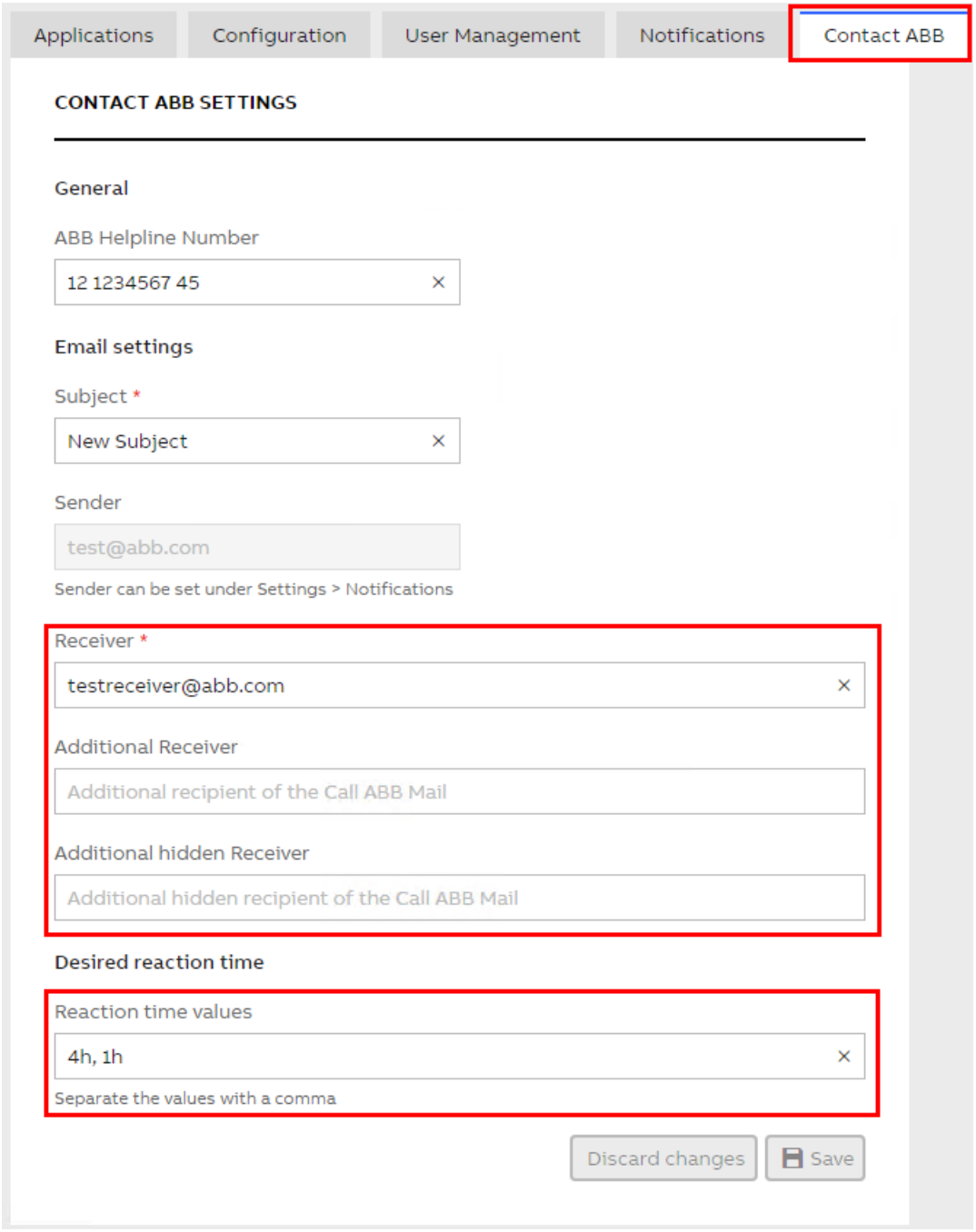


Figure 133: Contact ABB tab - Contact ABB settings form

Furthermore, the user can configure additional E-mail receivers and a desired reaction time in which ABB contacts should react on the E-mail request.

2.2.12.3.6. System Utilities tab

The System Utilities tab allows to configure the modules, services, nodes and network layers which are part of the CSWP feature set of MCS on-premise. For details on how this is done, refer to document ref.[1].

2.2.12.3.7. Application Credential Management tab

The Application Credential Management tab allows to add new service users to make services fully functional. For details on how this is done, refer to document ref.[1].

2.2.12.3.8. Synchronization tab

The Synchronization tab allows to configure how data between multiple MCS-OP instances needs to be exchanged. For details on how this is done, refer to document ref.[1].

2.2.12.3.9. Agent Management tab

The Agent Management tab allows to configure agents and services. For details on how this is done, refer to document ref.[1].

2.2.12.3.10. Assets tab

The Assets tab allows to configure activity index, time before permanent asset deletion, settings for assets merging and map sensors. For details on how this is done, refer to document ref.[1].

2.2.12.4. Notifications section

The Notifications section in the Administration and Configuration area of the MCS-OP application is used to configure and display incidents on the status of specific KPIs or on the status of the MCS-OP platform itself that might require the user's attention.

A red dot indicates if there are active or unacknowledged alarms within the system. Hovering over the icon a tooltip shows the exact number of unacknowledged and active alarm.

Figure 134: Notifications section of Administration and Configuration area

This section consists of in total three tabs, namely:

- Alarms tab
- Events tab
- Notification Management tab

The provided functionalities in these tabs are described in detail in the following chapters.

2.2.12.4.1. Alarms tab

The Alarms tab of the Notifications section is used to display occurring incidents of type "Condition" leading to a user notification. These type of incidents (called: "Alarms") require special attention as they might have a direct impact on the functionality and performance of your MCS-OP application.

They are presented in a list view with their event time, message text, incident type, rated severity, actual status and active time. All displayed events are sorted by their event time in descending order but can be sorted in descending or ascending order by message, severity, type or active time by clicking on the specific column label

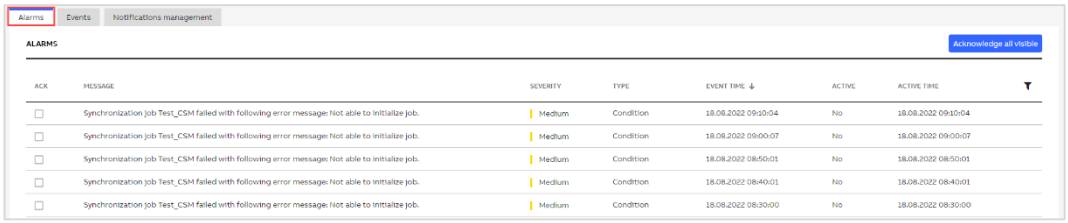


Figure 135: Alarms tab – Notification section

Since displayed alarms are of high importance the user must actively confirm that he/she has noticed them by selecting the ACK switch at the beginning of every alarm line.
Alternatively, he/she can acknowledge all visible alarms from the list at once by selecting the “Acknowledge all visible” button in the upper right corner of the Alarms tab.

Acknowledged alarms still having the status “Active == Yes” will stay in this list as long as their status does not change to status “Active == No”. As soon as the status of an acknowledged alarm changes to status “Active == No”, the affected alarm will disappear from this alarm list.

Filters are available to narrow down displayed items.

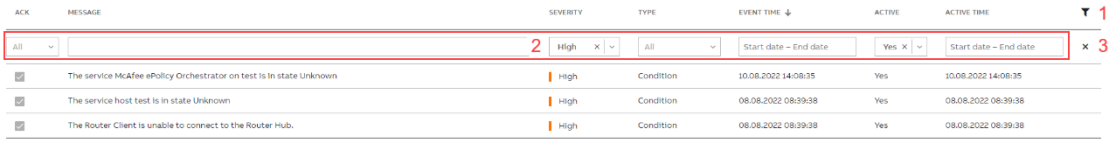


Figure 136: Alarms tab – Filters

1. Click on the filter icon to expand or clear and hide filters
2. Apply filters in each column to narrow down displayed items
3. Click on “x” icon to clear all filters

2.2.12.4.2. Events tab

The Events tab of the Notifications section is used to display all occurring incidents of any type leading to a user notification, including the ones of type “Condition”. These incidents (called: “Events”) are presented in a list view with their event time, message text, incident type and rated severity. All displayed events are sorted by their event time in descending order but can be sorted in descending or ascending order by message, severity, type or active time by clicking on the specific column label. It is also possible to apply filters.

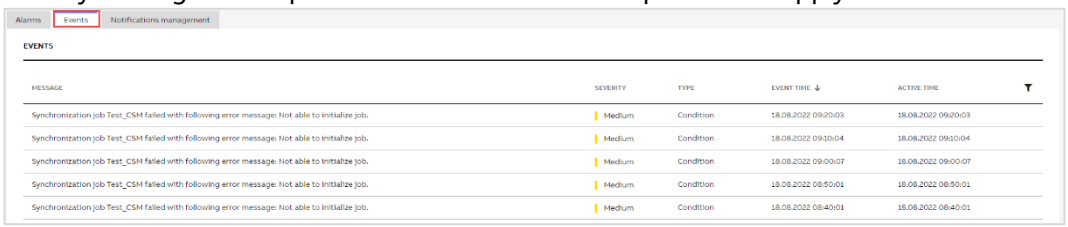


Figure 137: Events tab – Notification section

2.2.12.4.3. Notifications management tab

E-mail notifications are handled via the Notification Management tab of the Notifications section. From here you can set up a new user notification or edit your already existing notifications.

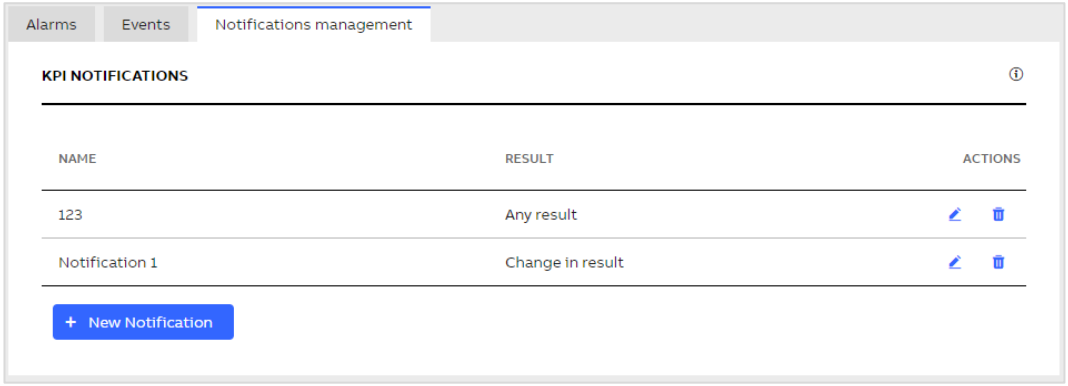


Figure 138: Notification management tab – KPI Notifications section

Please select the “New Notification” button to set up a new notification following the steps below.

1. Enter a name and the recipient(s) for the notification
2. Select if all KPIs or only specific KPIs shall be included (e.g. all Performance KPIs)
3. Select if all results, a change in the result (compared to the last analysis) or only specific result(s) should be included (e.g. only Errors)
4. Click on “Save” button

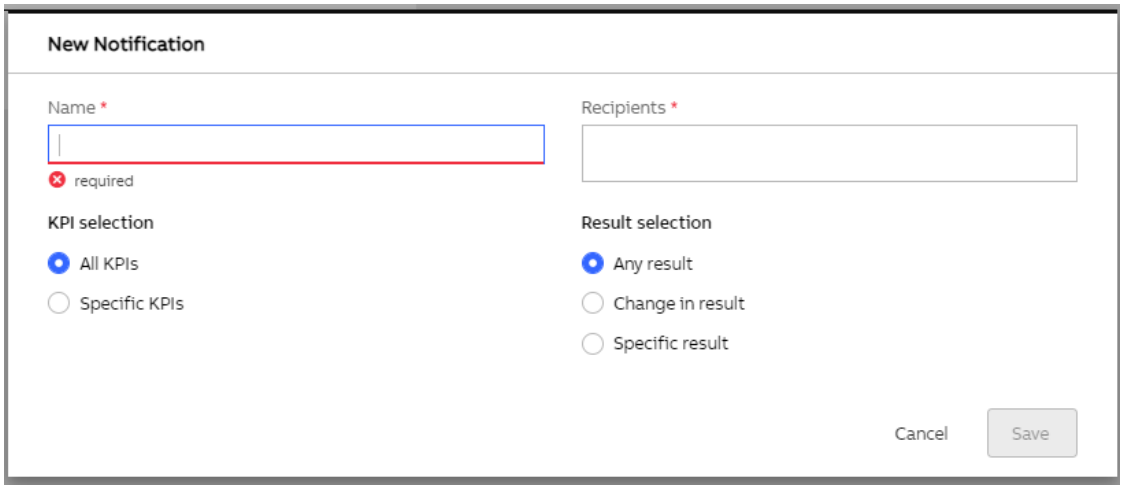


Figure 139: Configure a new notification

You can have multiple notifications with different content at the same time. They will be bundled in one common notification E-mail in case the rules apply.

System Monitoring Mail Recipients widget allows users with administrator role to configure or edit the recipients of notifications generated by the System Monitoring feature set. This widget will be displayed only if a System Monitoring license is available and CSM application is installed.

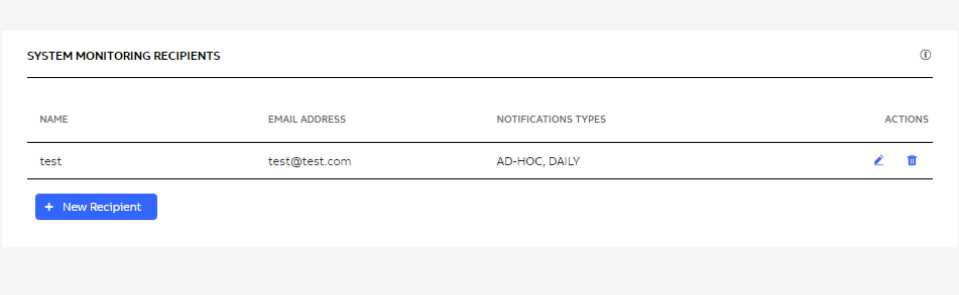


Figure 140: System Monitoring Mail Recipients

Select the “New Mail Recipient” button to set up a new recipient following the steps below.

1. Enter a name and e-mail address of the recipient
2. Select one or more notification types
3. Click on “Save” button.

Figure 141: Configure a new recipient

The following notification types are available:

– "Ad-Hoc": Generated immediately upon detection of certain notification condition
– "Daily": Summary of all notifications (independent of their severities) present in the past 24 hours
– "Monthly": Summary of all notifications (independent of their severities) present in the past calendar month

2.2.12.5. User section

The user section in the Administration and Configuration area displays information about the current user logged in to your MCS-OP application.

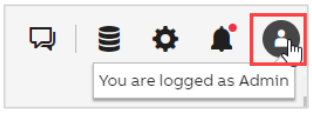


Figure 142: User section of Administration and Configuration area

It also provides the possibility to change the password or to log out the current user.

2.3. Reports

My Control System gives you the possibility to create and download all the analysis results and text elements via dedicated reports.

Following report types are available:

- Summary (provides a short overview about the overall KPI results)
- Reduced (provides a general overview about the individual KPI result of each collected device)
- Detailed (provides in-depth information about the individual KPI result of each collected device and descriptive text elements for each finding)
- Complete (provides in-depth information about the individual KPI result for each collected device, descriptive text elements for each finding and an appendix with all data points that were used for the analysis)
- Benchmark (legacy report type that is comparable to the new “Reduced Report” type)
- Fingerprint (legacy report type that is comparable to the new “Detailed Report” type)
- Assessment (legacy report type that is comparable to the new “Complete Report” type)

Report types Detailed, Complete and Fingerprint are only available with an active System Fingerprint license. Report type Assessment is only available with an active System Assessment license.

The report functionality is not available for “SystemUtilities” data sets.

2.3.1. Accessing reports

Reports can be created/accessed in three different places:

- On the data set management page (KPI tab) via the “Actions”, where you can browse reports grouped by data set (see Chapter 2.2.12.2.1)
- On the data set management page (Inventory tab) via the “Inventory Reports” widget where you can browse Inventory and Lifecycle reports (see chapter 2.2.12.2.2)
- In the pie chart widget on the KPI analysis tab of each category, where you will find reports for specific category (see Chapter 2.2.6)

Either a popup is opened where you can see already created reports or create a new one

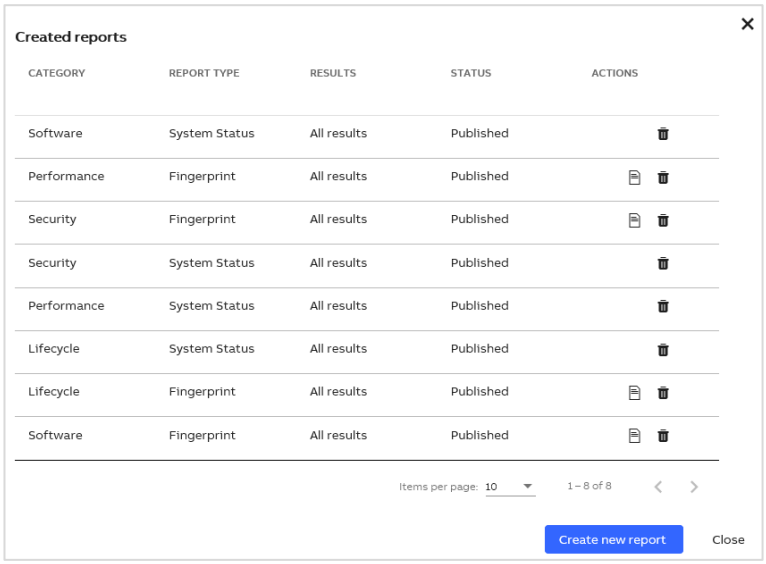


Figure 143: Created reports

or (as on Inventory tab under data set management) already created reports are listed directly in the widget.

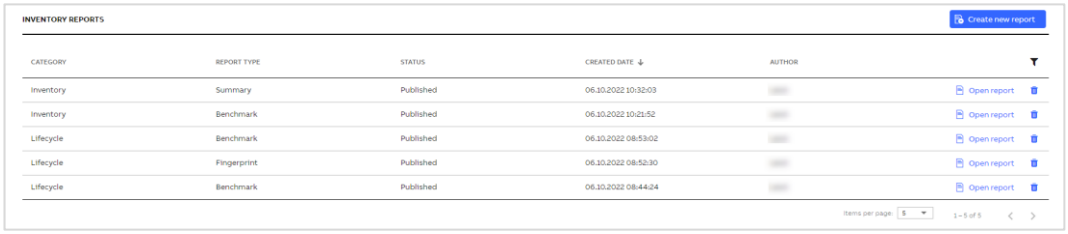


Figure 144: Created inventory reports

For already created reports, there are two actions available:

- Open report (opens the PDF version of the report in a new browser tab)
- Delete (deletes the report)

2.3.2. Generating reports

New reports can be generated by clicking the "Create new report" button. Clicking that button will open a wizard that will guide you through the process of report generation.

Following steps need to be done in the wizard:

- Select the category (if the wizard was opened from one of the category tabs, that category will be pre-selected in the drop down)
- Select the report type (keep in mind that some report types may be unavailable based on the selected category)
- Select the result filter (keep in mind that some filters may be unavailable based on the selected report type)
- Select additional options (language)

When all selections are made, click on the "Create report" button. The report will be displayed on top of the created reports list. For as long as the report is being generated, no actions will be available for that report.

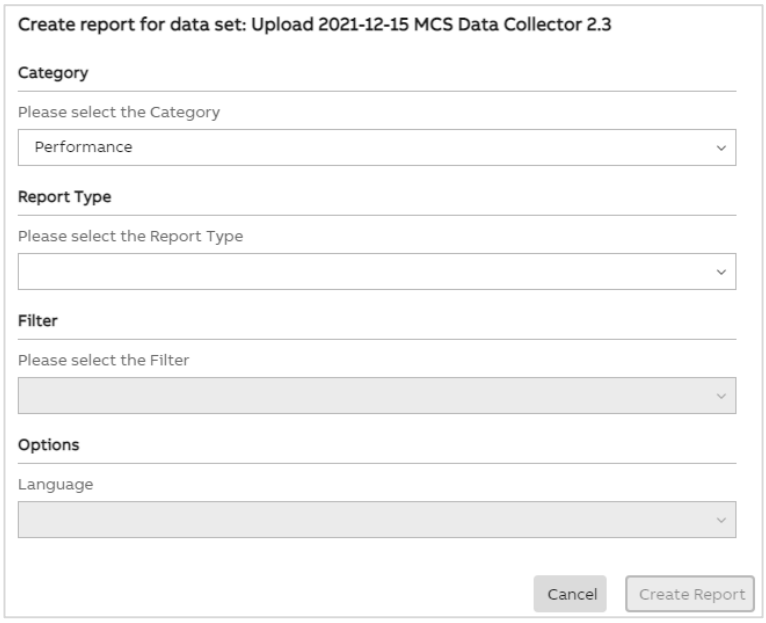


Figure 145: Create new report

3. Additional Information

3.1. Listing of Related Documents

	Document Kind, Title	Document No.
1	My Control System (on-premise) - Installation and Configuration Manual	2PAA121208
2	My Control System - Data Collector - User manual	2PAA120980-200
3	My Control System - Forwarder - User Manual	7PAA001522
4	My Control System (on-premise) - Hardening Guide	7PAA002031

4. Revisions

4.1. Revision History

Rev.	MCS Version	Page (P) Chapt. (C)	Description	Date Dept./Init.
A			New document	2020-01-30 IA PCP
B		ALL	Convert into Markdown documentation	2020-03-18 IA PCP
C		ALL	Small bug fixes	2020-12-17 IA PCP
D	5.0	ALL	Complete document is updated for the new MCS (on-premise) version, with the CSWP feature set Applied new template	2022-01-13 PA PCP
E	5.1	(C) 2.2.4.1, 2.2.10.2, 2.2.10.4 (C)1.4	Information about locked data sets added, Text and Picture update (Alarm Status indicator) Updated chapter ‘Scope and Software’ for S+ Operations 2.1 and above	2022-02-11 PA PCP
F	5.2	(C) 2.2.4, 2.2.9, 2.2.11, 2.2.12.3.6	Footer area description added Tabs renamed and rearranged Documentation section added System Utilities tab added	2022-03-10 PA PCP
G	5.3	(C) 2.2.9.2.4	Added Quest Rapid Recovery as supported Backup solution	2022-04-08 PA PCP
H	5.4	(C) 2.2.2	Added hideable filter area description	2022-05-07 PA PCP
I	5.6	(C) 2.1 (C) 2.2	Updated chapter ‘Sign on to the system’ Updated chapter ‘Overview (general layout)’	2022-07-01 PA PCP
J	5.7	(C) 2.2.7.1	Updated chapter ‘General’	2022-07-29 PA PCP
K	5.8	(C) 2.2.12.4	Updated chapter ‘Notifications section’	2022-08-26 PA PCP
L	5.9	(C) 2.2.12.3.3	Updated chapter ‘User Management tab’	2022-09-23 PA PCP
M	5.10	(C) 2.2.10, (C) 2.2.12.2 (C) 2.2.12.3.9 (C) 2.2.12.3.10 (C) 2.3.1	Updated chapter ‘Inventory’ Updated chapter ‘Data set management section’ Added chapter ‘Agent Management tab’ Added chapter ‘Assets tab’ Updated chapter ‘Accessing reports’ Added information about MCS version in the revision history	2022-10-21 PA PCP
N	5.11	(C) 2.2.10.2	Updated chapter ‘Assets’	2022-11-18 PA PCP

Rev.	MCS Version	Page (P) Chapt. (C)	Description	Date Dept./Init.
O	5.12	(C) 2.2.10.1 (C) 2.2.10.1 (C) 2.2.12.2.1	Updated chapter ‘Assets’ Updated chapter ‘Hardware Lifecycle’ Updated chapter ‘KPI’	2022-12-16 PA PCP
P	5.13	(C) 2.2.7 (C) 2.2.9.1 (C) 2.2.10	Updated chapter ‘General Information’ Updated chapter ‘System Overview' Updated chapter ‘Inventory’	2023-01-20
Q	5.14	(C) 2.2 (C) 2.2.7.3 (C) 2.2.10.1 (C) 2.2.10.3	Rearranged order of chapters in ‘Overview (general layout)’ Newly added chapter on suggested actions Images updated in ‘Hardware Lifecycle’ Added chapter ‘Control Structure’	2023-02-17
R	5.15	(C) 2.2.10.1 (C) 2.2.10.2	Updated chapter ‘Hardware Lifecycle’ Updated chapter ‘Assets’	2023-03-17
S	6.0	(C) 2.2.9.8.2	Updated chapter ‘Plant isolation’	2023-06-07
T	6.2	(C) 2.2.10.2 (C) 2.2.12.3.10	Updated chapter ‘Assets’ Updated chapter ‘Assets tab’	2023-08-11
U	6.3	(C) 2.2.5.1.3 (C) 2.2.9 (C) 2.2.10.2	Updated chapter ‘Malware Protection, Security Updates and Backup’ Updated chapter ‘Security’ Updated chapter ‘Assets’	2023-09-01
V	6.5	(C) 2.2.2 (C) 2.2.9.2.3 (C) 2.2.6.4	Updated chapter ‘Filter area’ Updated chapter ‘Malware Protection’ Updated chapter ‘Comparison view’	2023-10-19

Visit us

www.abb.com/controlsystems