IBM Enterprise Content Management System Monitor

User's Guide

IBM Enterprise Content Management System Monitor
Version 5.8.0

User's Guide

SC27-9245-09

Table of Contents

This document contains information about the use of the IBM Enterprise Content Management System Monitor after it is installed and configured. The target audience for this guide are the users of the ESM.

Preface

About this document

This document is written as plain text document and provided as html / pdf. The newest ESM related documents can be found in the help section of the console.

Who should read this guide?

The target audience for this guide are those who install or maintain ESM environments.

Every effort has been made to provide you with complete installation instructions. If information becomes available after the creation of the installation media from which you accessed this guide, we will provide an updated version of the guide on the IBM Customer Service and Support web site (https://www.ibm.com/support). As a general rule, you should refer to the IBM web site to obtain the current version of this guide.

This guide provides instructions for installing and/or upgrading IBM Enterprise Content Management System Monitor, and identifies the IBM/FileNet and 3rd Party products that are certified for the current release. Be aware that each release of IBM Enterprise Content Management System Monitor may have multiple Interim Fixes, or Fix Packs available for installation, each with potentially different dependencies and installation requirements. Therefore, before you attempt to install or upgrade IBM Enterprise Content Management System Monitor, review the list of releases and their associated dependencies on the IBM Support web site (https://www.ibm.com/support).

Before you start

Users of the guide should have knowledge about Unix and/or Microsoft Windows® operating system, web servers, database systems and middleware platforms. The configuration of managed systems (clients) requires advanced knowledge of all IBM ECM systems that should be monitored.

You should read the Upgrade Notes section below!

If you lack the requisite skill sets it is strongly recommended to have IBM Lab Services or a certified ValueNet Partner in order to install this product.

TIP

For tips and tricks regarding the configuration and maintenance of IBM Enterprise Content Management System Monitor please check the CENIT Field Guides at IBM ESM Field Guides.

The PDFs of the eGA documentation can be found on the IBM support pages. In the installed product you will always find the newest documentation.

Feedback on documentation

Send your comments by e-mail to comments@us.ibm.com. Be sure to include the name of the product, the version number of the product, and the name and part number of the book (if applicable). If you are commenting on specific text, include the location of the text (for example, a chapter and section title, a table number, a page number, or a help topic title)

IBM Enterprise Content Management System Monitor Console

This section describes the available dashboards and gives an overview of what can be done within the dashboards.

Monitoring Dashboard

The monitoring dashboard offers the possibility to create several views for the configured situations or take a look at the currently running tasks.

Adding, working with and sharing of dashboard tabs within the monitoring dashboard

Per default the monitoring dashboard has one inbuilt dashboard tab. The highlighted buttons in the screenshot below offer several options to work with the tab(s).

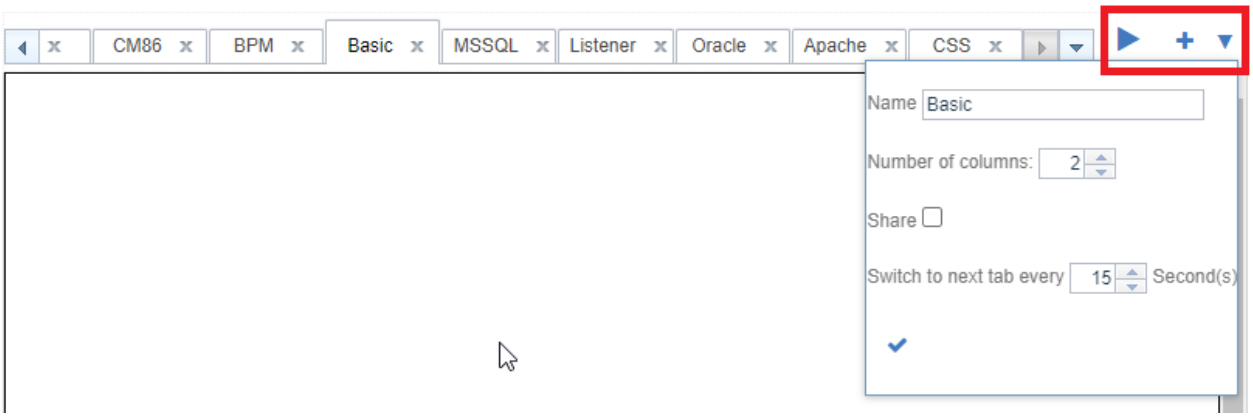

Image of Multi Tabs

Play/Pause button

If several tabs have been added, this button can be used to automatically switch between the tabs every x seconds. The seconds are defined in the options setting that pops up when clicking the drop-down button. Once activated the play button will turn in a pause button. Click on that to pause the switching again.

Plus button

Clicking on the plus button adds an additional tab in the list after the tab that is currently active.

Drop-down button

In the options setting from the drop-down, the name of the currently active tab can be adjusted. You can also define the number of columns for that tab in there. Furthermore, as admin you have the possibility to share the tab. Sharing a tab means that tab is automatically shown for all other ESM users. The background of the tab page will be highlighted and all shared tabs will be moved to the end of the tab list. As said, all of the settings in here are performed only on the active tab except the setting for the seconds between the switching which is valid for all tabs.

NOTE

Users have the possibility to customize a shared tab on their end. But the customization is only valid for the session lifetime - it is not stored. Only admins can adjust such a tab permanently.

Situations

From the sidebar choose the situation icon. This will show all available situations as a list or all situation groups, depending on which level you are.

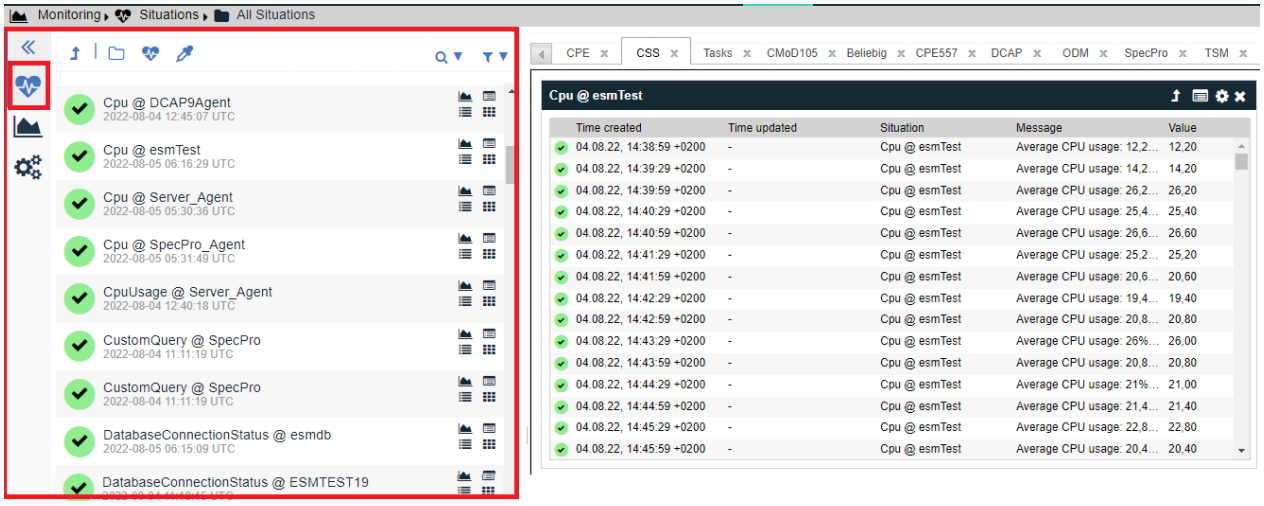

Image of Monitoring Situation List

Double-Click on a situation group

Double-clicking on a situation group will open the list with all situations from the situation group in the sidebar. This function can be used for browsing functionality.

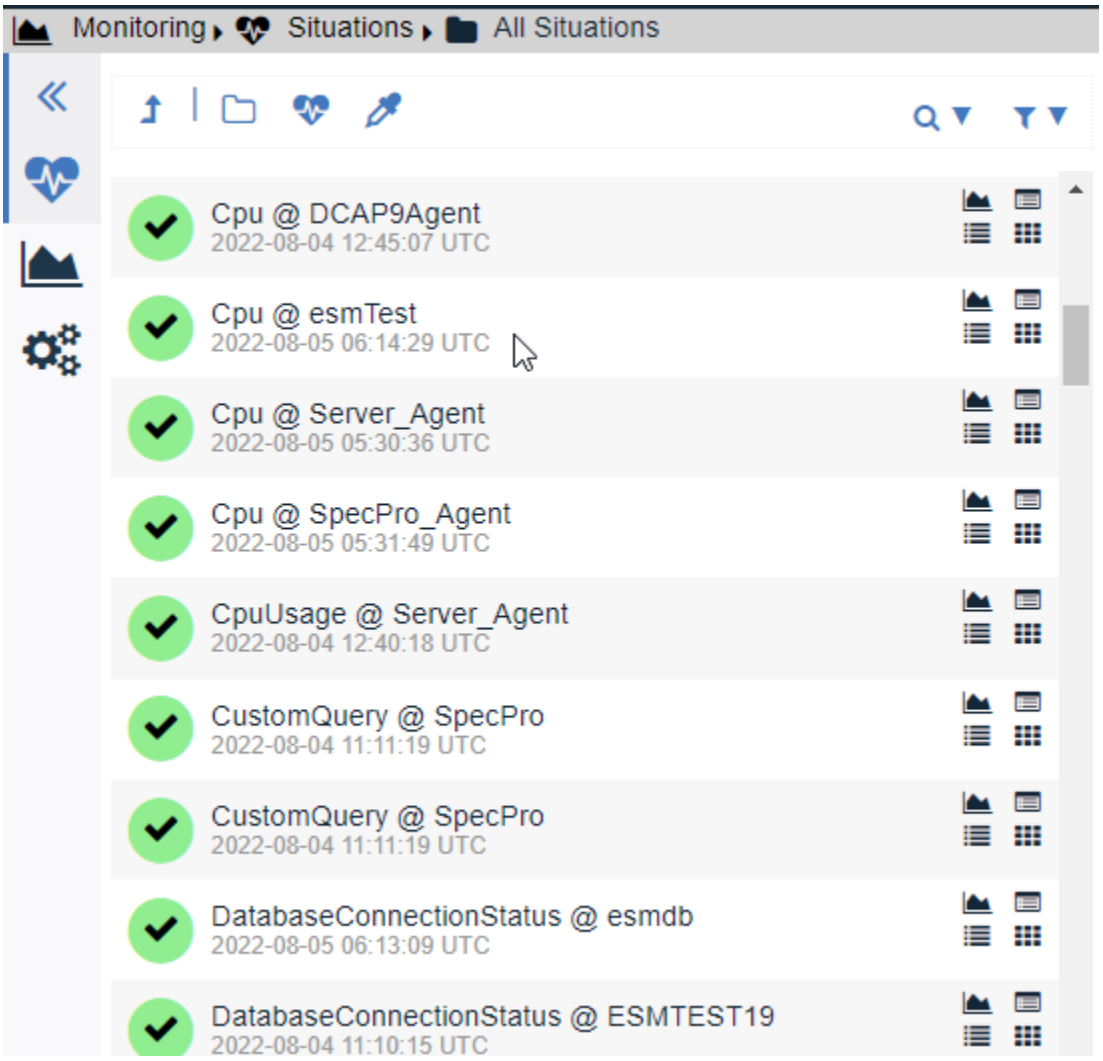

Image of List in sidebar

Choose from one of the icons next to the situation or the situation group to place it in the active monitoring dashboard.

Image of Monitoring Situation List Icons

Upper Left Icon

The upper left icon is for a graphical presentation of the sample values with a minimized list of the information from the last samples. The sample list can be hidden via a checkbox in the settings (button in the upper right corner of the portlet). After clicking the icon the situation is automatically placed at the next available slot in the active monitoring dashboard. This can be outside of the visible field. The new entry will look like this:

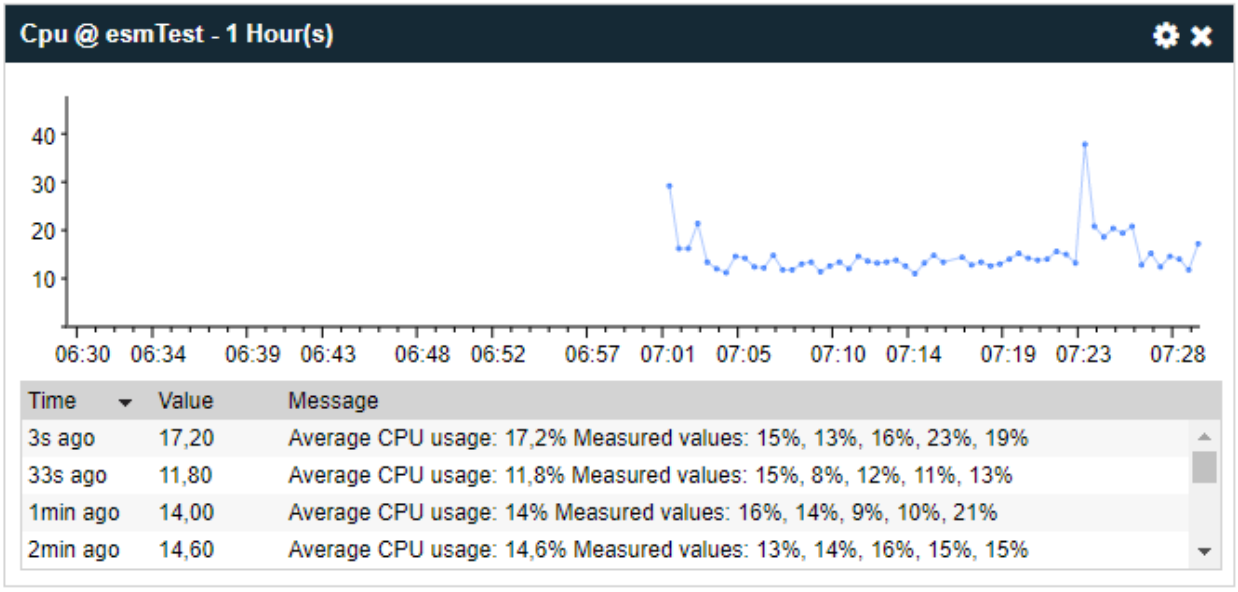

Image of Situation Graph

Upper Right Icon

The upper right icon is for an incidents details view. The view opens above the dashboard on the right. It is pre-filtered with the settings from the entry you clicked on the icon. Within the view, actions on the list (such as deleting or closing entries etc.), also more filtering can be done. This list can also be opened from the "Situation List" portlet described below. The list allows sorting via the header of the columns. The default sort order is Severity followed by Time created. The incident list will look like this:

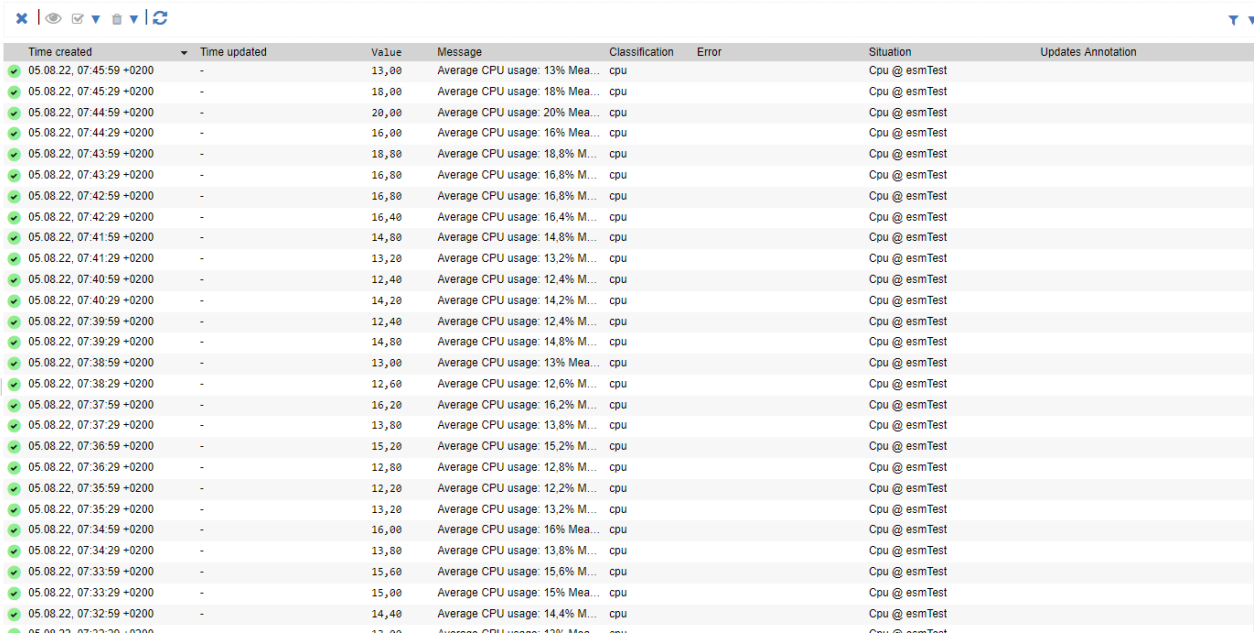

Image of Situation Graph

Lower Right Icon

The lower right icon is for a heatmap presentation of the incidents. It will create a portlet that only shows the severity as a colour and the current value. It is also automatically placed at the next available slot. There is no possibility to choose a period. By clicking on the settings icon the displayed situation can be changed. The list portlet looks like this:

Image of Situation Heat

Lower Left Icon

The lower left icon is for a list presentation of the incidents, values will only be displayed as a number in the list. It is also automatically placed at the next available slot, but it will directly open the event list. The list allows sorting via the header of the columns. The default sort order is Severity followed by Time created. Same as for the heatmap portlet, there is no possibility to choose a period. By clicking on the settings icon the displayed situation can be changed. The list entry looks like this:

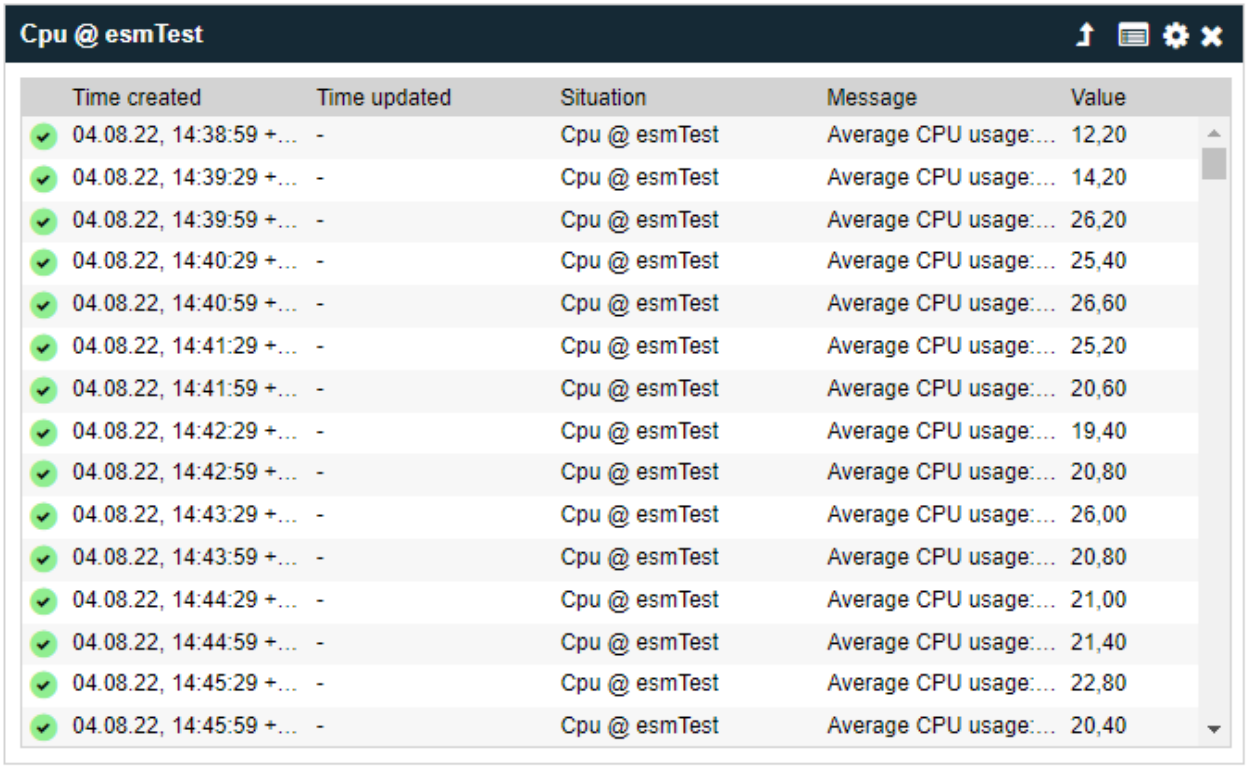

Image of Situation List

List views are best for showing samples from logfiles. Graphical views are good for samples with changing values.

NOTE Currently, a total of 16 portlets can be added to one dashboard.

Setup of the situation portlets

Each of the portlets can be adjusted. Therefore, you can use the settings icon in the top right corner of the portlet.

Settings of the graph portlet

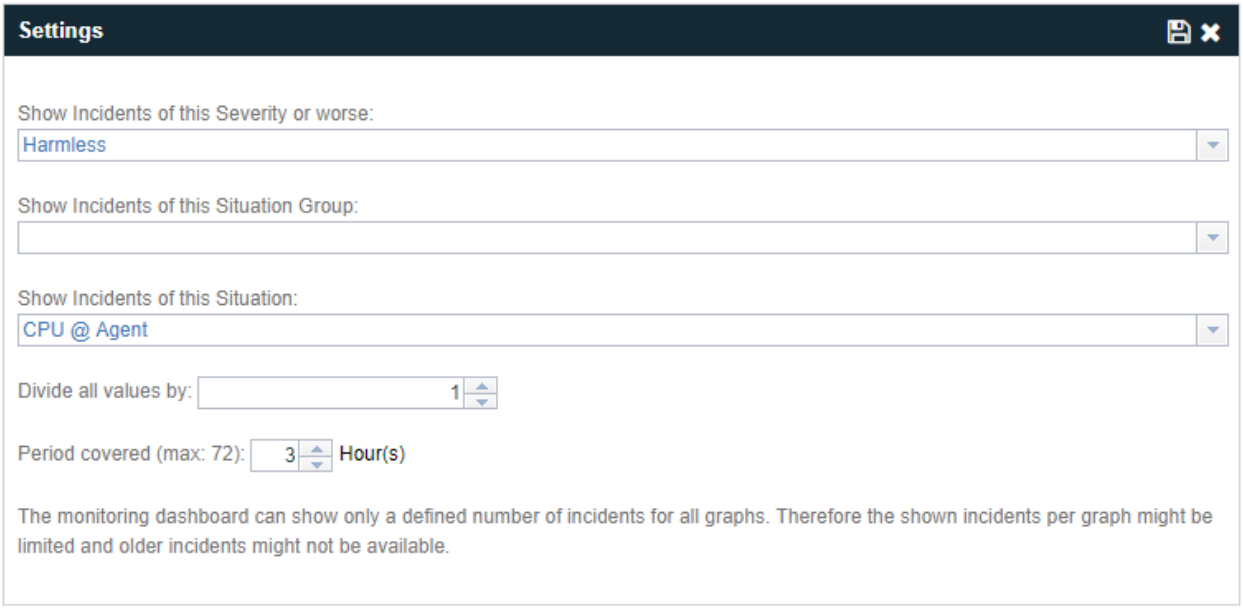

Image of graph portlet settings

NOTE Multiple (4) graphs can be shown if the parameter "Show Incidents of this Situation" is empty and the parameter "Show Incidents of this Situation Group" is used. As only 4 graphs will be shown the portlet will pick just random 4 if more than 4 situations are part of the situation group that is selected.

Show Incidents of this Severity or worse

Select the severity from the drop-down. Only incidents with this or a higher severity will be shown in the portlet.

Show Incidents of this Situation Group

Select a situation group from the drop-down. Only incidents from this situation group will be shown.

Show Incidents of this Situation

Select a situation from the drop-down. Only incidents from this situation will be shown.

Divide all values by

The user can enter a divisor not a multiplier (aka multiplicator). Up- and downscaling must be possible. The idea behind the division in comparison to the multiplication is, in the product's environment it is more common to have huge raw values, that should be scaled down instead of the opposite. But 0.001 is harder to recognize than 1000.

NOTE The scale will be shown in the title bar of the portlet as well.

Period covered (max: 72)

The default period is 3 hours, this defines the x-axes for the graph.

Settings of the heat portlet

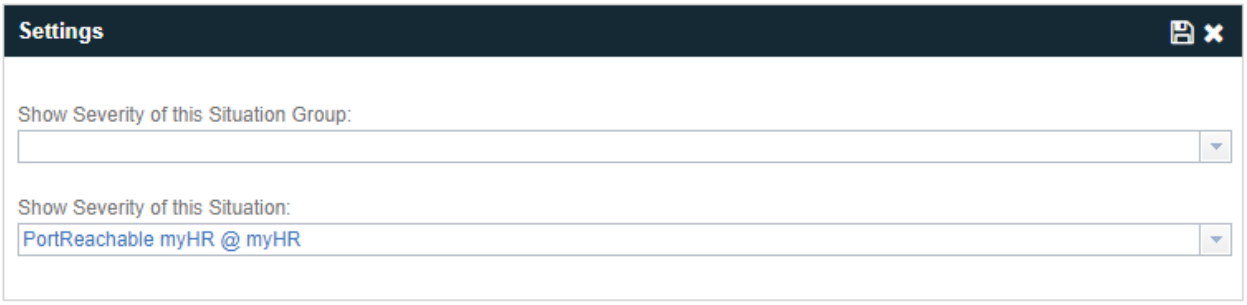

Image of heat portlet settings

Show Severity of this Situation Group

Select the situation group from the dropdown that should be used for showing the severity.

Show Severity of this Situation

Select the situation from the dropdown that should be used for showing the severity.

Settings of the list portlet

Image of list portlet settings

Show Items of this Severity or worse

Select the severity from the drop-down. Only incidents with this or a higher severity will be shown in the portlet.

Show Items of this Situation Group

Select a situation group from the drop-down. Only incidents from this situation group will be shown.

Show Items of this Situation

Select a situation from the drop-down. Only incidents from this situation will be shown.

Incidents

The portlet can have two layouts. One that shows a list where each incident is shown as new object (checked) and one that shows the Incident as a status object where only the timestamp and severity is updated (unchecked).

Divide all values by

The user can enter a divisor not a multiplier (aka multiplicator). Up- and downscaling must be possible. The idea behind the division in comparison to the multiplication is, in the product's environment it is more common to have huge raw values, that should be scaled down instead of the opposite. But 0.001 is harder to recognize than 1000.

NOTE The scale will be shown in the title bar of the portlet as well.

Buttons above the list

The buttons are used for browsing through the list or placing entries in the console.

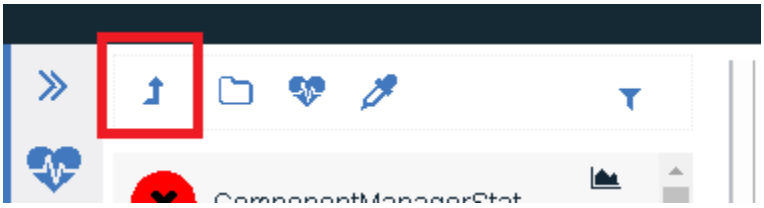

Image of sidebar button up

If you are browsing the situations in the sidebar, this button brings you one level up.

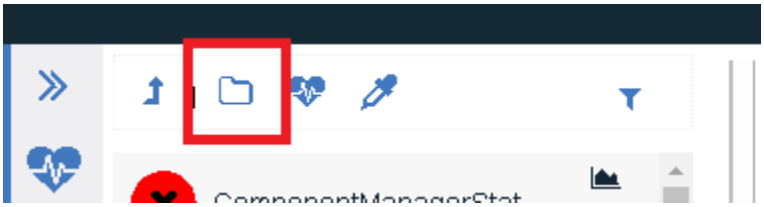

Image of placing all situation groups

Once the button is clicked a portlet containing all situation groups is added to the console on the right. See next screenshot.

Image of portlet with all situation groups

Clicking on the settings icon opens the configuration for this portlet. You can select a severity level for the shown items, which groups should be shown and which items of the groups should be shown. Save the settings by clicking on the disk icon.

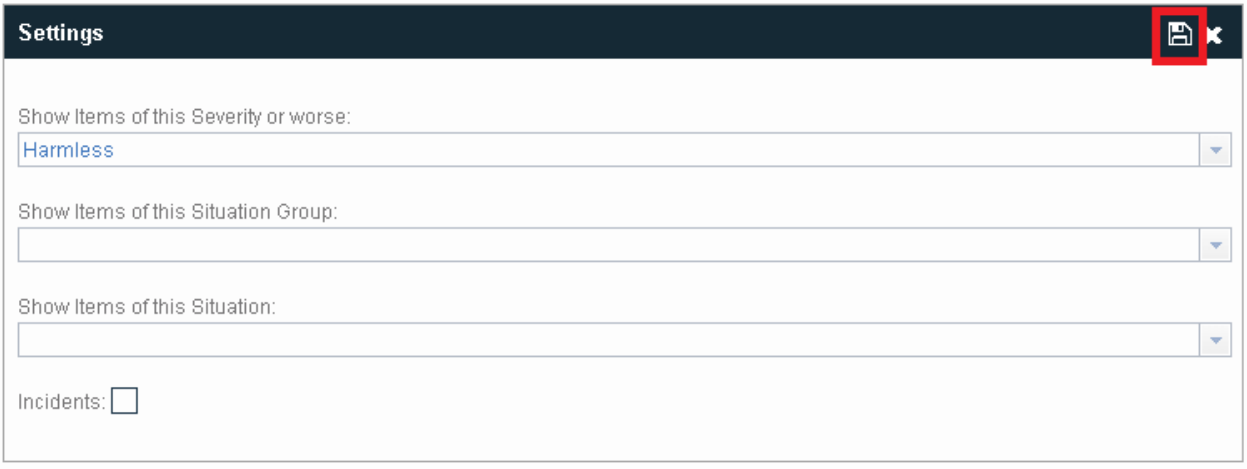

Image of portlet settings for situation group portlet

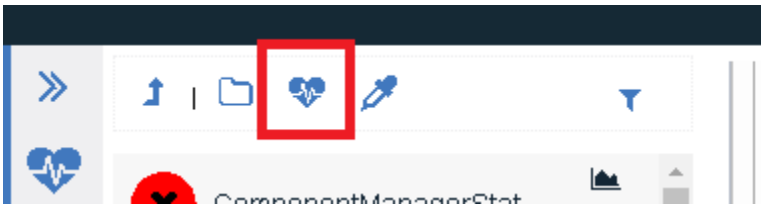

Image of button for placing empty situation portlet

The button places an empty portlet for situations on the right in the console. This portlet can be configured to show incidents of a certain situation (drop-down). Also, the period that should be covered can be adjusted. Afterwards click on save icon to show the graph.

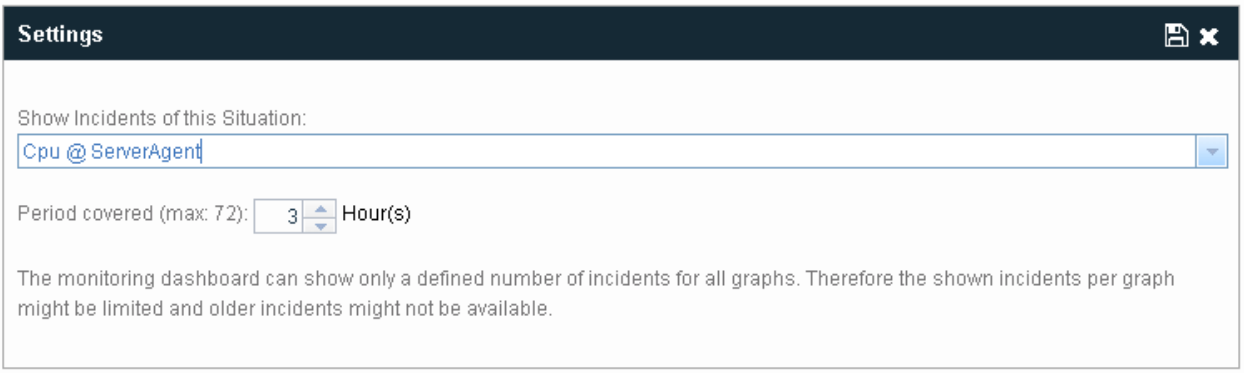

Image of empty portlet

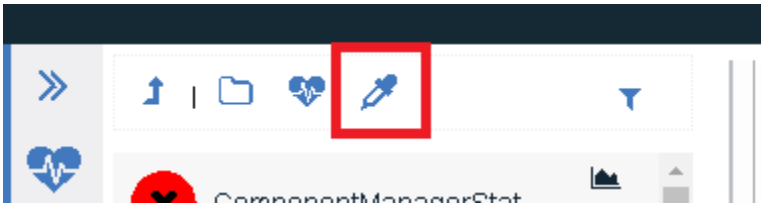

Image of button for placing empty samples portlet

The button places an empty portlet for samples on the right in the console. This portlet can be configured to show a list with samples of a certain probe (drop-down). Also, the period that should be covered can be adjusted. Afterwards click on save icon to show the list.

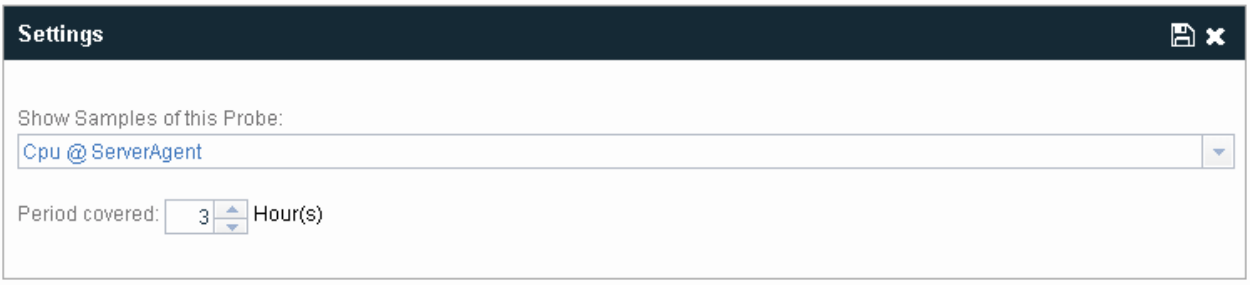

Image of empty samples portlet

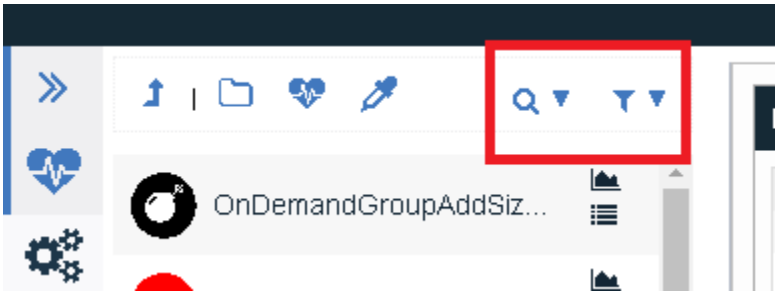

Image of filter button for list

The listed entries in the sidebar can be filtered using these buttons. The first one (search option) is for filtering the objects based on the name. The search is not case-sensitive. Also tags can be added which are taken into account when the search is performed. Click on "Filter" to apply the settings, click on "Reset" to remove the filter once it has been applied.

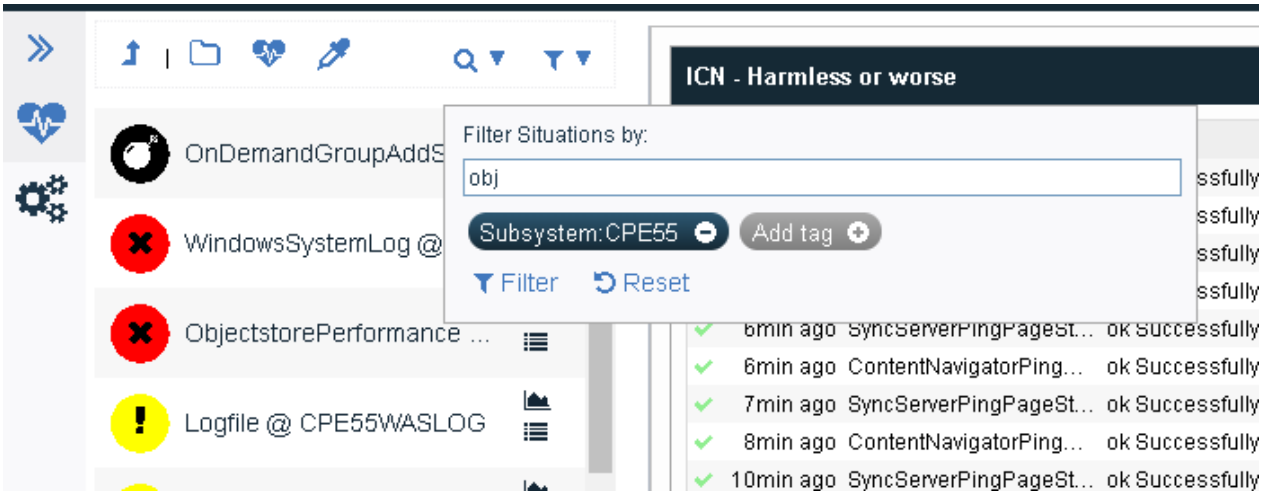

Image of filter setting for the list based on object name and tag

The second one is for a filter based on the severity. Once the button is clicked an overlaying window opens. You can select the severity from the drop-down. The filter is applied automatically.

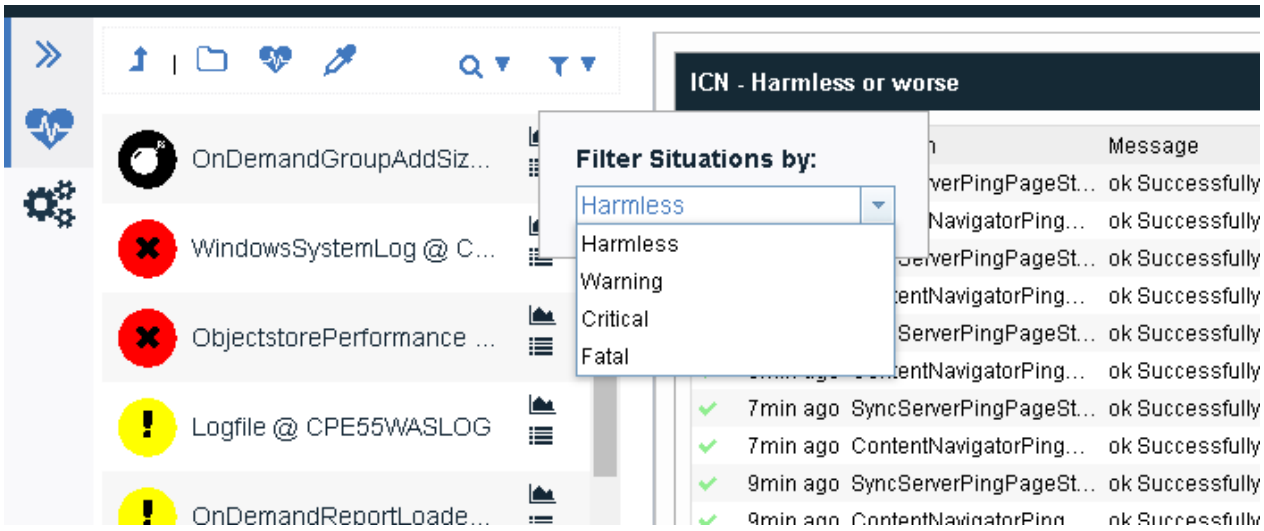

Image of filter setting for the list based on the severity

NOTE Situations with unknown severity will always be shown.

Incident list and details of an incident

A list for getting all incidents is available.

This list uses lazy loading.

Filtering by the combination of the following criteria is possible.

- Least severity (= severity x or worse)
- Situation Group
- Situation

The filters are defined in the portlet criteria. The portlet can show a high level view e.g. "Situation Groups", but the list will show the incidents of the "Situation Groups".

This list shows the following information in the given order in a row per incident:

- Severity (Icon)
- Timestamp (in ISO format)
- Value
- Message
- Classification
- Error
- Situation Name

The default sorting is by descending timestamp (oldest at the bottom, newest at the top of the list).

The list can be reached by clicking in the list icon in any of the portlets.

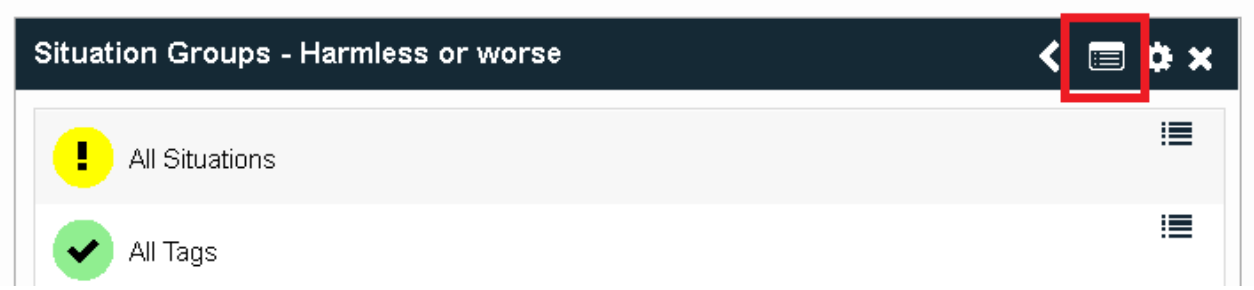

Image of list icon in portlet

Detailed information about an incident can be shown by selecting an entry in the incident list - The details are also available when double-clicking on an incident directly in the portlet.

The following image shows the incident list including the details of a selected incident. The details section is automatically opened once an entry from the list is selected. The section will close once you click on the same entry again. Selecting any other entry will open the details for this one. The selected entry is highlighted in the list.

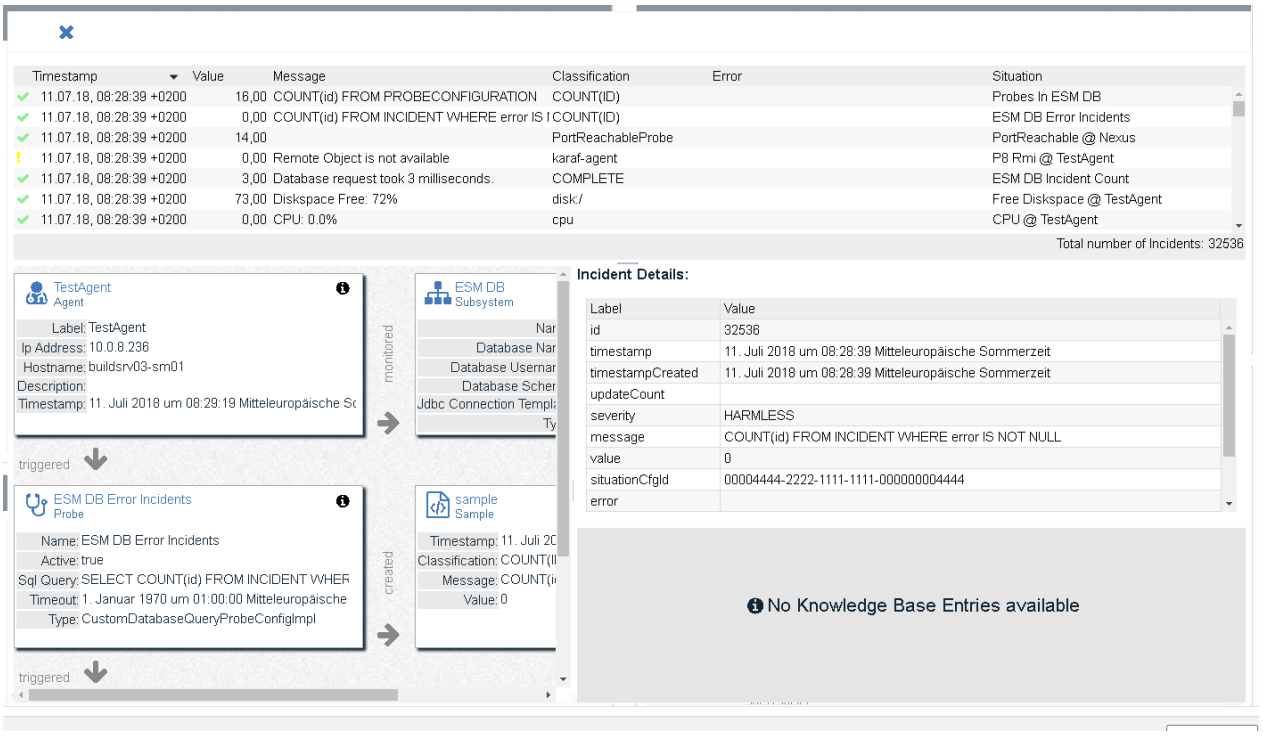

Image of Incident list including details of a selected incident

Incident handling

Within the history view of each portlet, ESM offers possibilities to handle events. Therefore, some buttons are available at the top in this view.

Image of Top Buttons in History

Functions of the buttons from left to right:

1. Leave this view
2. Acknowledge the selected entry. The user can add some text e.g. that he is working on this entry. - Acknowledging can be overwritten by clicking the button again.
3. Close the selected incident. For closing all incidents of the current list, select the drop-down button next to it on the right side. (Incident will not be shown in the portlet anymore) - This can be undone by doing the same again.
4. Delete the selected incident, For deleting all incidents of the current list, select the drop-down button next to it on the right. (The Incident is completely removed - deleted from DB) - This cannot be undone.
5. Reload/Refresh the list

Incident filtering

The history view also offers the possibility to filter for certain incidents.

Image of Filter Buttons in History

Clicking on the buttons opens the filter editor.

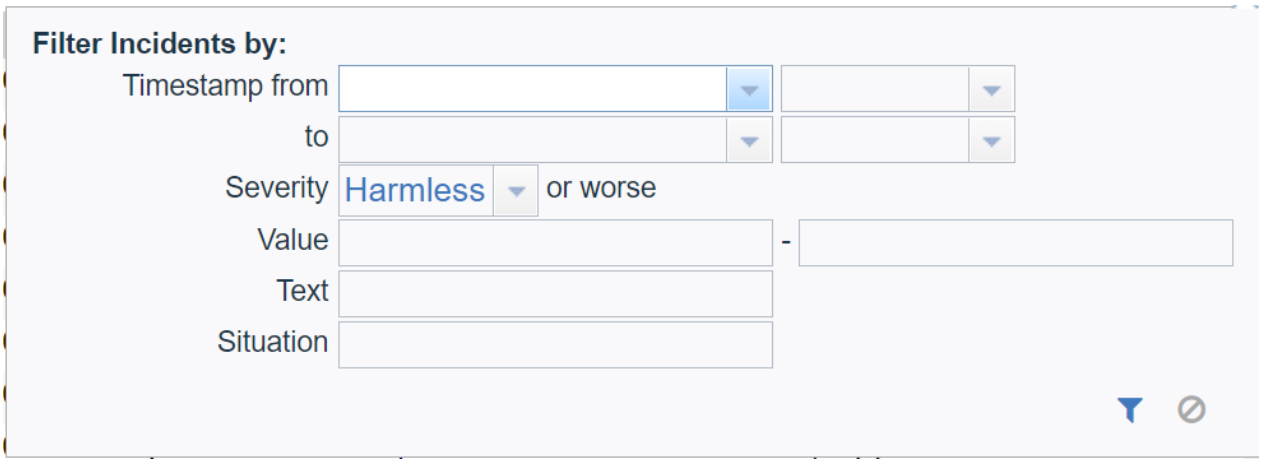

Image of Filter Editor in History

It is possible to set several of the filters at the same time. Filter settings can be adjusted and submitted again. Possible filters are:

- Timestamp (Date and Time), from and to
- Severity, filters for the severity that is given and worse
- Value, from - to
- Text, searches for the given string in Message, Classification, Error and Annotation.
- Situation, searches for the given string in Situation.

Depending on the filters the search context might get complex and therefore the search can take some time.

The filter is submitted/activated by clicking on the filter icon in the bottom right corner in the editor. It can be deactivated by clicking on the deactivate button next to it. The filter editor stores the last filter setup until the history view is closed. Even if the filter editor is closed, the filter is still maintained.

Report Portlets

From the sidebar choose the task portlet icon. This will open a list with the available reports. Reports from the type aggregation can be added as portlet with the button on the right of the entry.

The portlet will show the latest available instance of this report - every time the report is created due to the schedule, the portlet will be updated as well.

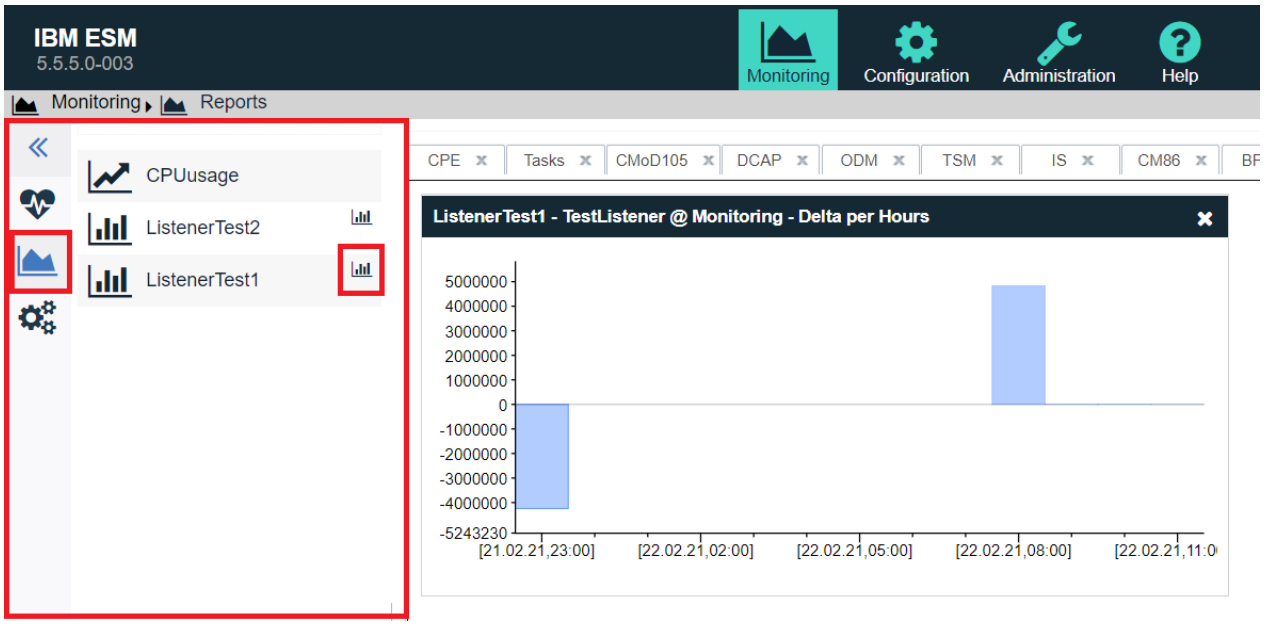

Image of Monitoring Report Portlet

Task Portlets

From the sidebar choose the task portlet icon. This will show the recent tasks as a list.

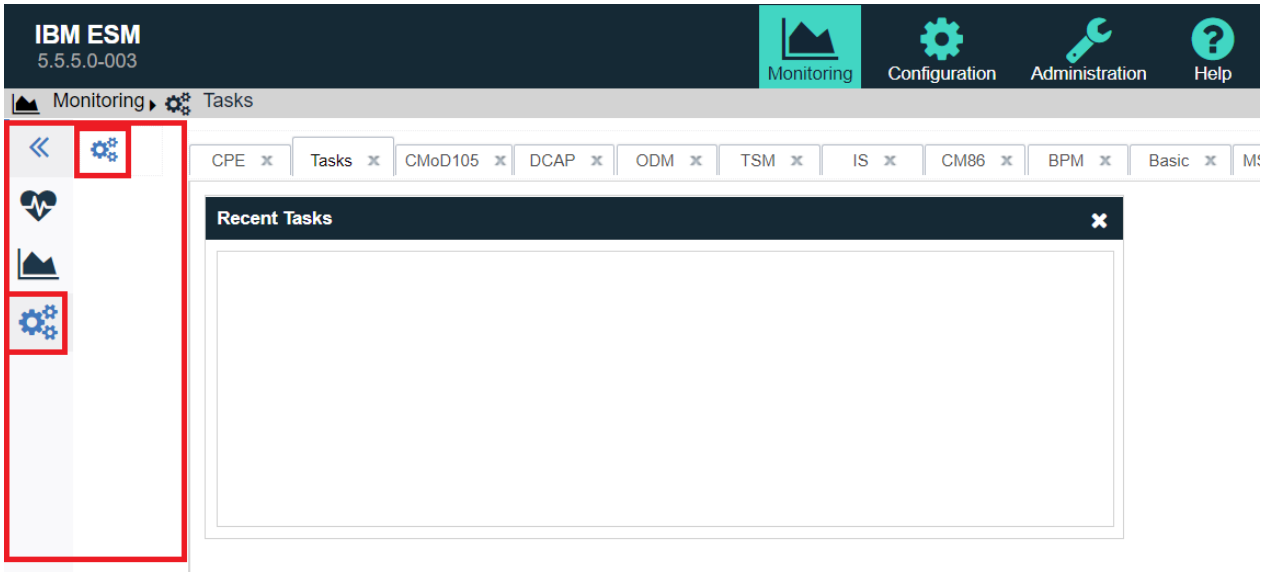

Image of Monitoring Task Portlet

Double-click on the button to add the "Recent Task" portlet on the next available slot in the monitoring window. This can be outside of the visible field. The portlet contains a list and will look like this:

Image of Monitoring Recent Tasks List

Configuration Dashboard

The configuration dashboard offers the possibility to configure ESM based on your needs. Within the configuration you can review the agents, configure your subsystems, situation groups and task or browse and adjust the knowledgebase.

Agents

Choose the agent icon from the sidebar. This will open a list with all agents. Also, the status of the agent is displayed.

You can use the buttons above the agents list to restart an agent (only if online), delete offline agents or mark timed-out agents as offline in the DB.

NOTE

- Agents can only be deleted if there are no probes assigned to run at the agent that should be deleted.
- Setting an agent to offline only marks the agent as offline, it is not shutting down the agent. The status is only kept until the agent is sending heartbeat information again, if any. Afterwards the agent can be shown as online, timed-out or outdated again. This button serves the purpose to set the status of an agent to a defined state on the server.

In addition, there is a button that can be used to update the selected agent from this console (see below).

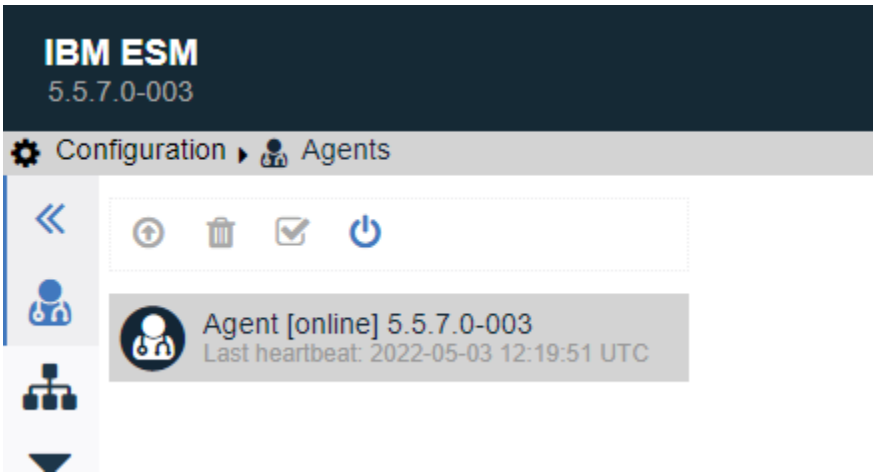

Image of Configuration Agent

Updating Agents from the Console

IMPORTANT The update cannot be performed on agents that run as a docker container. Docker containers should be updated via the usual platform mechanisms.

NOTE If you are updating an agent via the ESM web-UI, under rare conditions it is possible an already existing `<agent-installation-directory>/update` directory causes issues that will prevent the update to proceed. If so, please delete that `update` directory and try again.

IMPORTANT If the agent is not installed as a service, it can be updated via the console, but it will not restart automatically after the update is complete. Such an agent must be started manually in order to reconnect to the server.

Requirements

- Agent is on ESM version 5.5.5.7-003 or later.
- Agent status is outdated.
- The corresponding agent installer must exist on the ESM Server in <Install-Dir>karaf/agent/installers/<currentVersion>/<matchingOS>
- On Windows OS: The following commands must exist and be executable for the agent`s service account (Local System per default)
  - C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

- C:\Windows\System32\xcopy.exe
- C:\Windows\System32\cmd.exe
- C:\Windows\System32\net.exe
- C:\Windows\System32\taskkill.exe

- On Linux/Unix OS: The following commands must exist and be executable for the account the agent runs under.
  - /bin/bash
  - systemd-run
  - kill
  - nohup

Update process

- Select the agent you want to update from the agent list and click on the update button.
- The Agent should change it`s status to updating.
- After some minutes (depending on the performance) the agent should be having the status online again.

NOTE

If an agent is updated via the web-UI and during the first installation no automatic start for the agent after installation was selected, this setting will be overwritten. That must be done, so the agents starts after the update process and no interaction on the system itself must be done.

Subsystems

Choose the subsystem icon from the sidebar. This will open a list with the already configured subsystems. You have the possibility to create a new subsystem, add a probe to the selected subsystem, modify the selected subsystem or delete the selected subsystem.

For more details please refer to the "Configuration Guide for ESM 5.8.0".

Image of Configuration Subsystem

Sample Filtering

The sample filtering is a mechanism to filter sample depending on certain criteria. If samples match the criteria, they will directly be filtered on the agent.

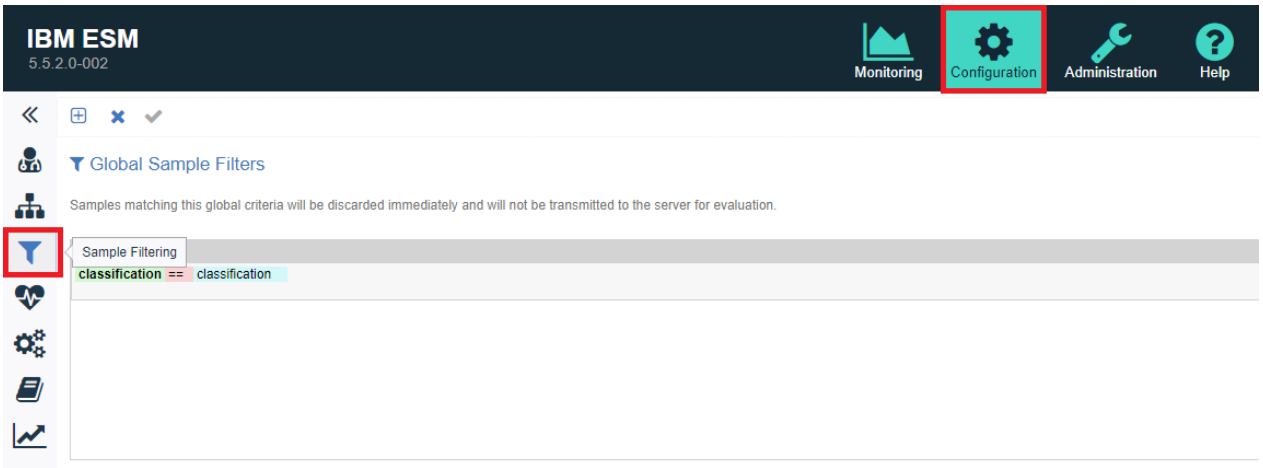

Image of Configuration Sample Filtering

Situation Groups

Choose the situation icon from the sidebar. This will open a list with the already configured situations. You have the possibility to create a new situation, duplicate, modify or delete the selected situation, or do the same with so-called situation groups. Situations that contain a deactivated probe are highlighted with a different color.

For more details please refer to the "Probes and Situation Guide for ESM 5.8.0".

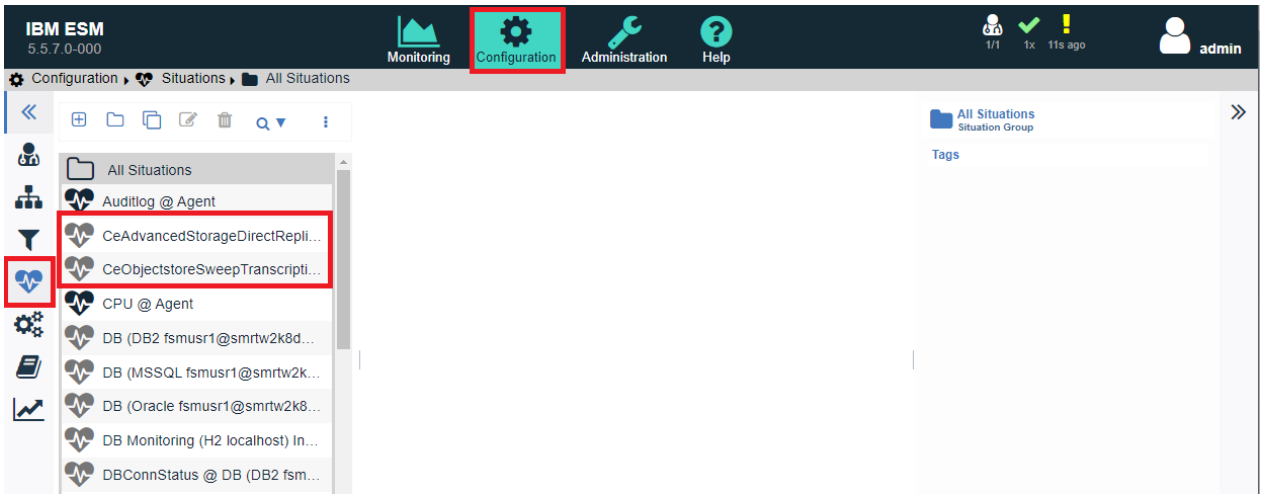

Image of Configuration Situation

Furthermore, detailed information about the selected entry is given at the bottom of the list.

Task Configuration

Choose the task icon from the sidebar. This will open a list predefined task types. You have the possibility to create a new task, duplicate, modify or delete the selected task.

For more details please refer to the "Task Guide for ESM 5.8.0".

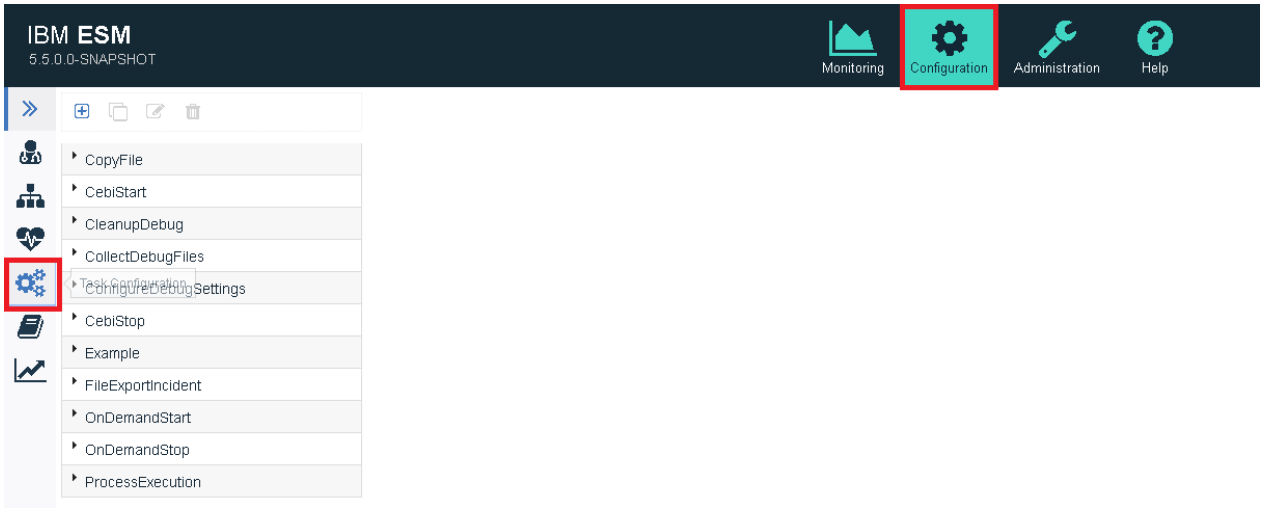

Image of Configuration Task

Furthermore, detailed information about the selected entry is given at the bottom of the list.

Knowledge Base

Choose the knowledge base icon from the sidebar. This will open a list containing all available entries. You have the possibility to create a new entry, duplicate or delete a custom entry.

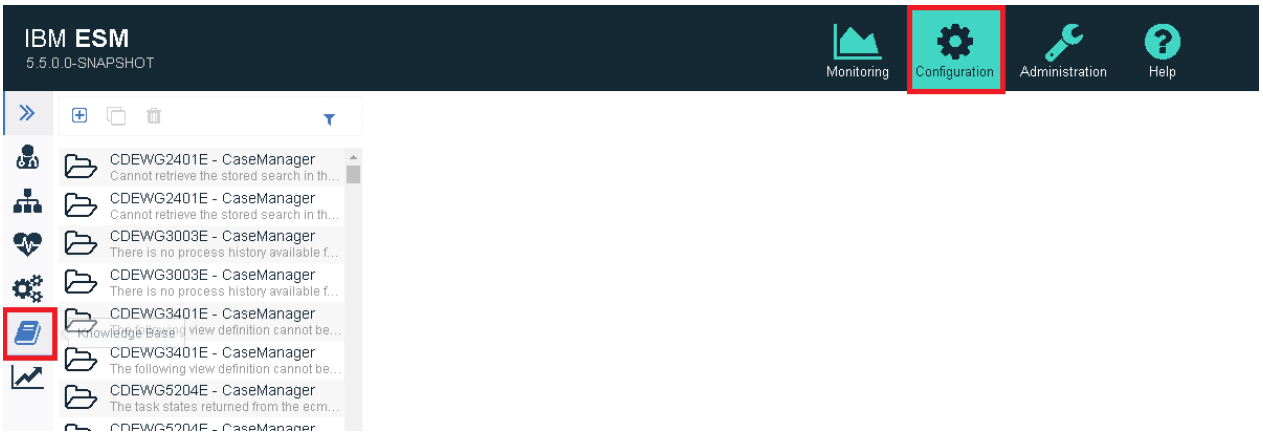

Image of Configuration Knowledge Base

Furthermore, a possibility to filter the list based on ErrorID or subsystem is available. Either search for a snippet of the ErrorID or select the subsystem. A combination of both is also possible.

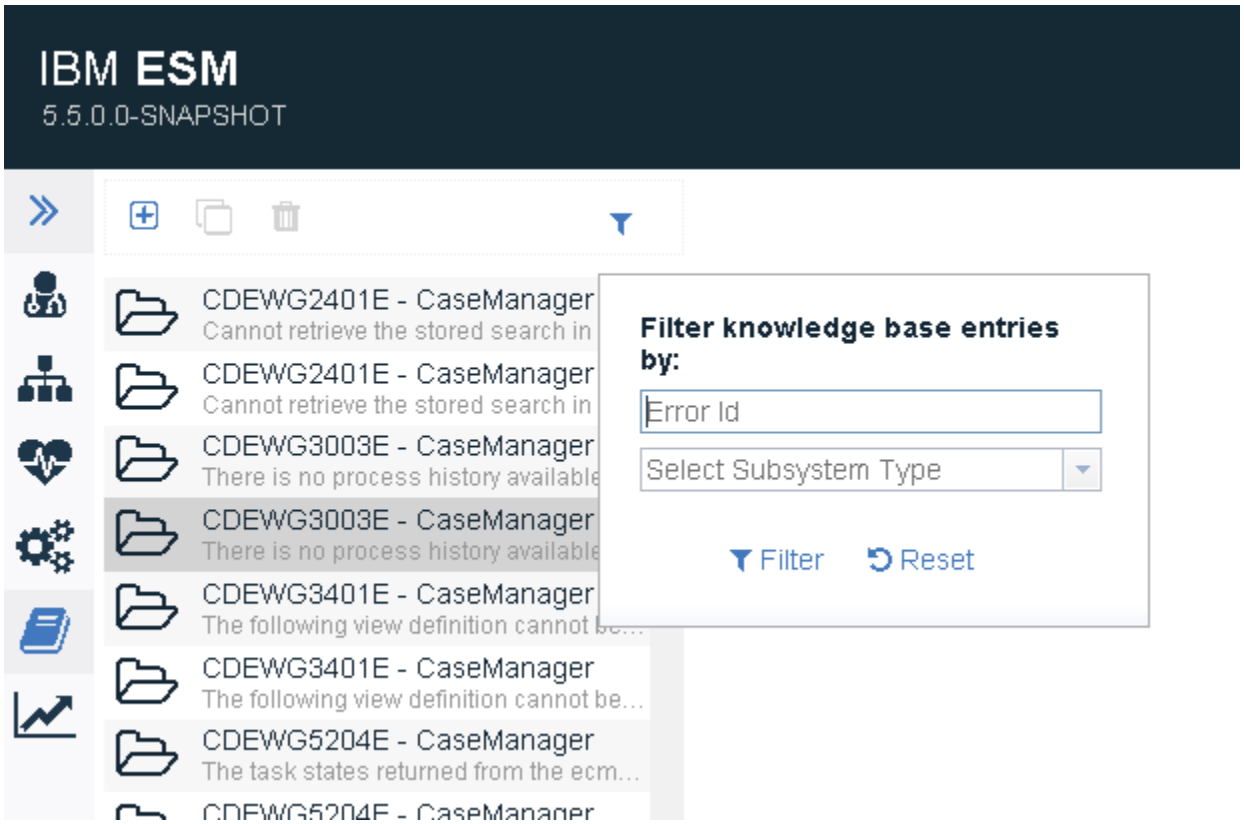

Image of Configuration Knowledge Base Filter

The filter is saved throughout the search and can be enhanced. A reset by using the reset button is also possible.

Double-click an entry to see more details like message, cause, corrective action and custom info. This information is also available at the bottom of the list.

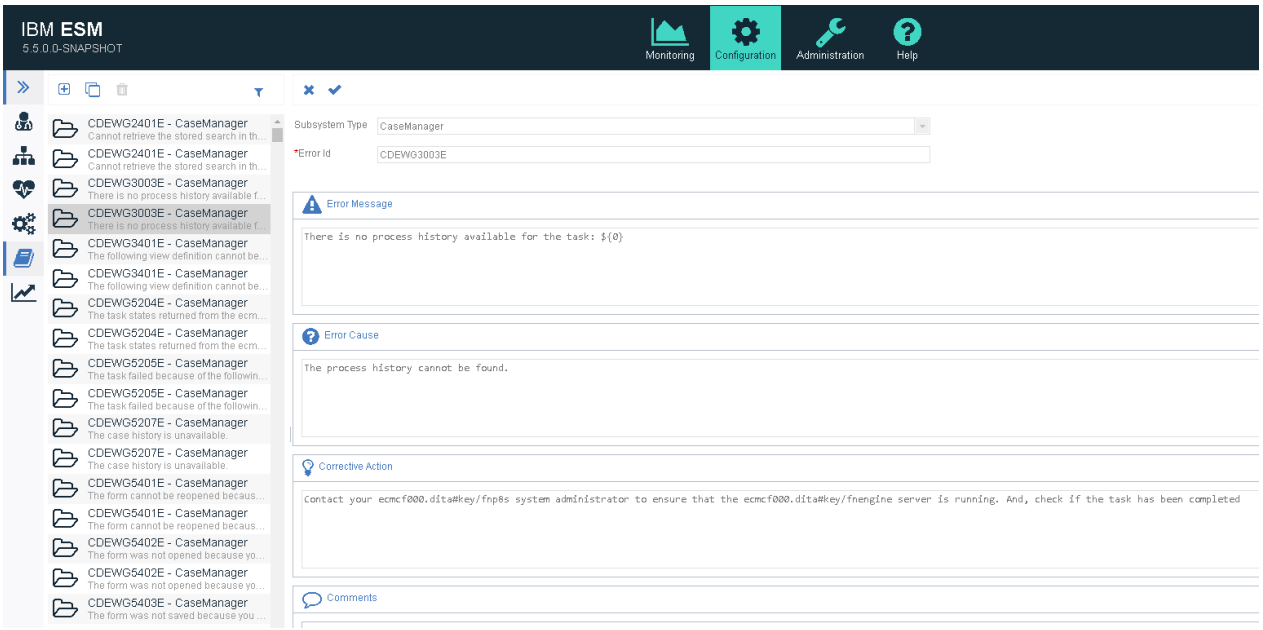

Image of Configuration Knowledge Entry

Reporting Configuration

Choose the reporting configuration from the sidebar. This will open a list with the already configured reports. You have the possibility to create new reports or delete the selected report.

For more details please refer to the "Configuration Guide for ESM 5.8.0".

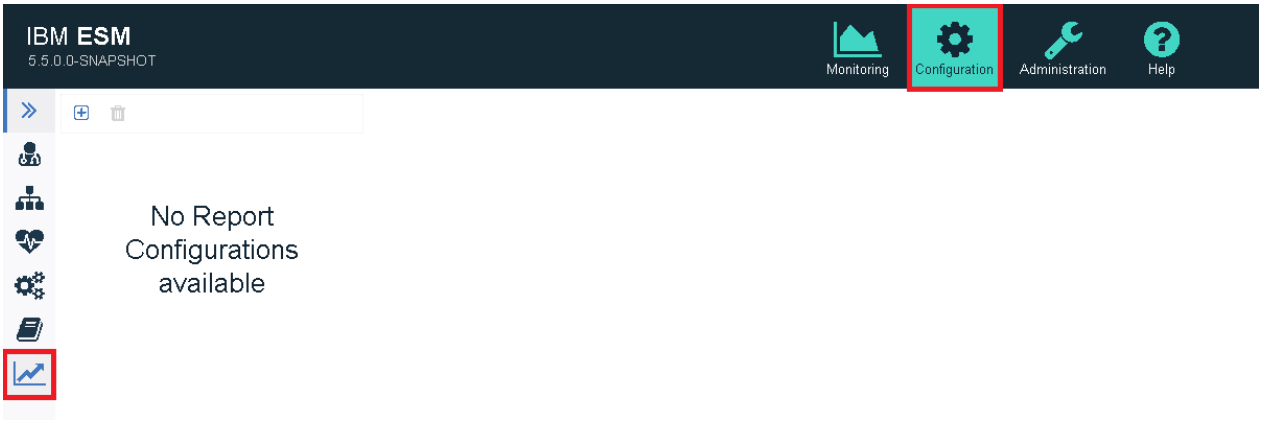

Image of Configuration Reporting

Administration Dashboard

The administration dashboard offers the possibility to adjust Server Settings, review the audit log, manage users and login modules, such as LDAP integration and administrate SMTP forwarding.

Server

Once you have selected the server icon on the left, two options are offered. You can either adjust server settings or review the audit log.

Settings

Double-click on the Settings button to open the Server Settings. Currently, you can enable or disable the automatic deployment of the base monitoring for new agents and adjust the Database Cleanup configuration as well as user time out settings.

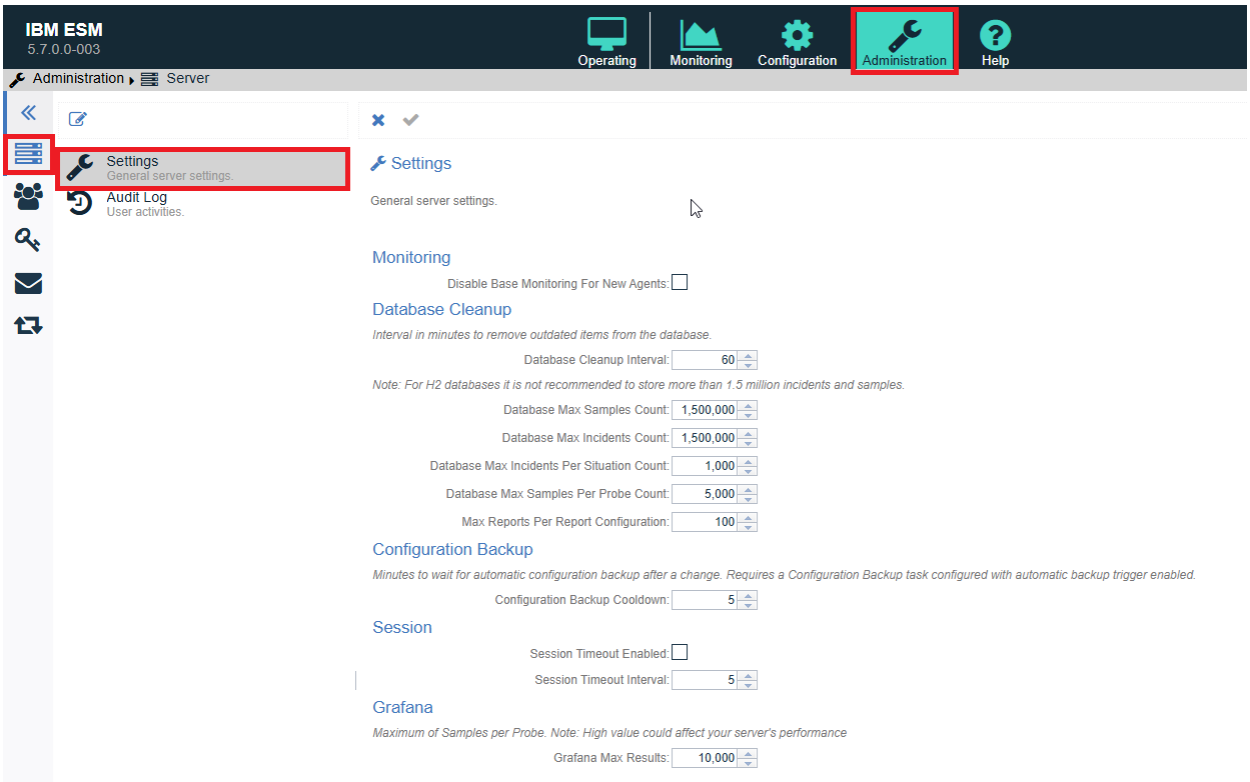

Image of Administration Server Settings

Audit Log

Choose the audit log icon from the sidebar. This will open the audit log on the right side of the sidebar.

You have the possibility to reload the audit log.

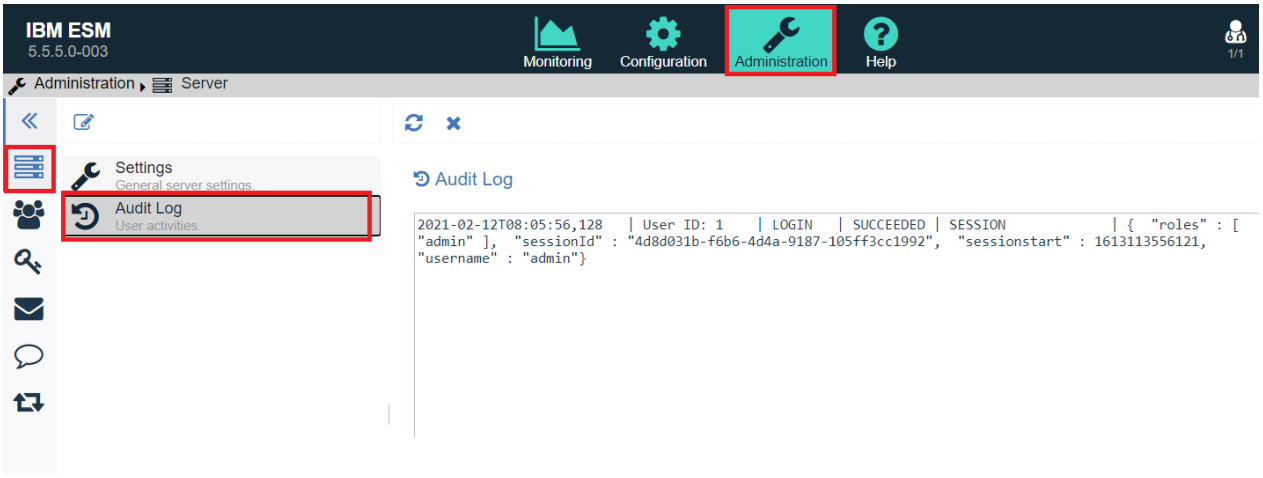

Image of Administration Server Audit Log

User Management

Choose the user management icon from the sidebar. This will open a list containing all users. Per default only the admin account exists.

You have the possibility to create an internal or external user, remove the selected user or unlock a locked account.

For more details please refer to the "Configuration Guide for ESM 5.8.0".

Image of Administration Users

Login Module

Choose the login module icon from the sidebar. This will open a list of already created login modules. Per default no login module is available.

You have the possibility to create a new login module or remove the selected login module.

For more details please refer to the "Configuration Guide for ESM 5.8.0".

Image of Administration Login Module

Mail Server administration

Choose the Mail Server administration icon from the sidebar. This will open a list of already created mail server setups.

You have the possibility to create a new mail server setup or remove the selected setup.

For more details please refer to the "Configuration Guide for ESM 5.8.0".

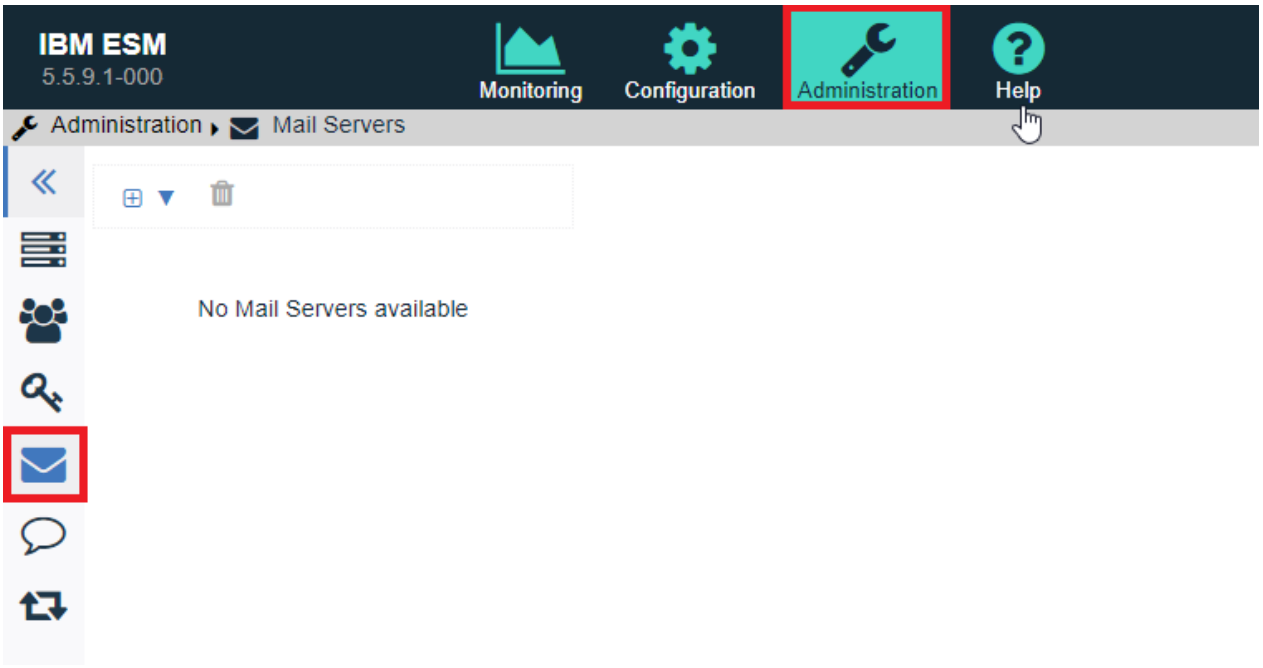

Image of Administration SMTP

Help Dashboard

The help dashboard offers the documentation as html. Select from one of the available documents on the left site:

- IBM Enterprise Content Management System Monitor Release Notes
- IBM Enterprise Content Management System Monitor User's Guide
- IBM Enterprise Content Management System Monitor Installation Guide
- IBM Enterprise Content Management System Monitor Configuration Guide
- IBM Enterprise Content Management System Monitor Probes and Situations Guide
- IBM Enterprise Content Management System Monitor Tasks Guide

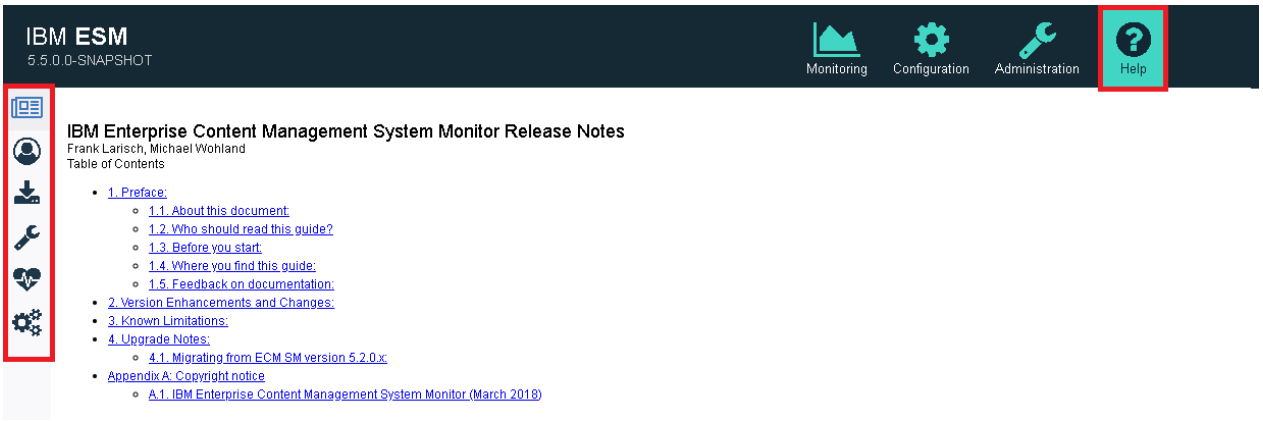

Image of Help

Information Sidebar

In the Configuration and Administration a sidebar on the right side is available. The sidebar can be toggled.

Depending on the selection of the left bar, different kind of information are shown in here. In some cases it is also possible to switch to related objects like subsystems or situations by double-clicking on the object name.

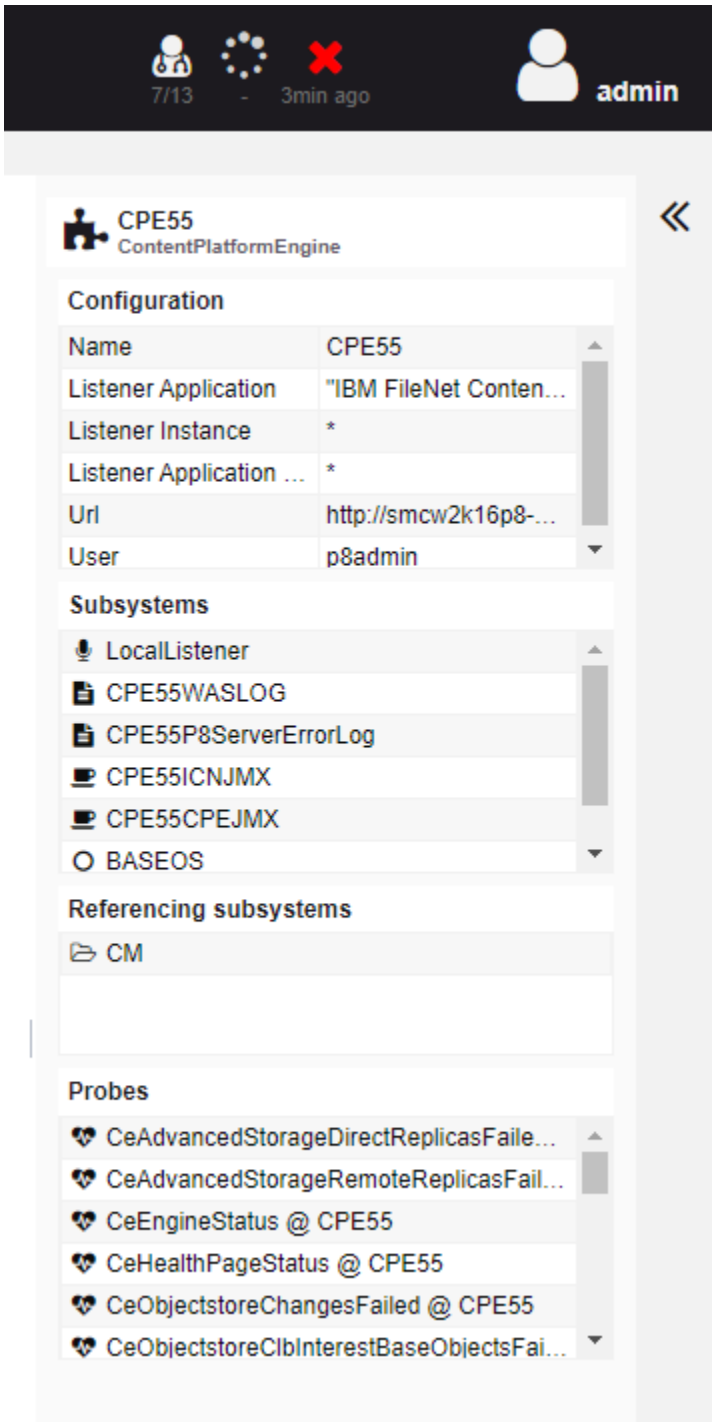

Image of Sidebar Right

ESM Operating Console

This section describes the "Operating Console" and the possibilities within this console.

Wordings

Probe

Script that is executed or continuously reader for gathering information on the agent.

Sample

Information that has been created during the execution of a probe. The sample is created on the agent and sent to the server.

Event

Evaluated information that has been created out of a sample and has a severity.

Incident

A subset of events, all events with a severity of at least warning level.

Operating Console - Status Overview

When opening the Operating Console per default the Status Overview will be shown. This view is a highlevel overview over the monitored environments and can be used e.g. to keep it on a big screen in the office. Information about the systems, agents and possible maintenance windows is displayed.

Furthermore Common Steps and News and Noteworthy information are displayed.

Clicking on the blue highlighted "Show Incidents" button redirects you to Systems Overview which is described below.

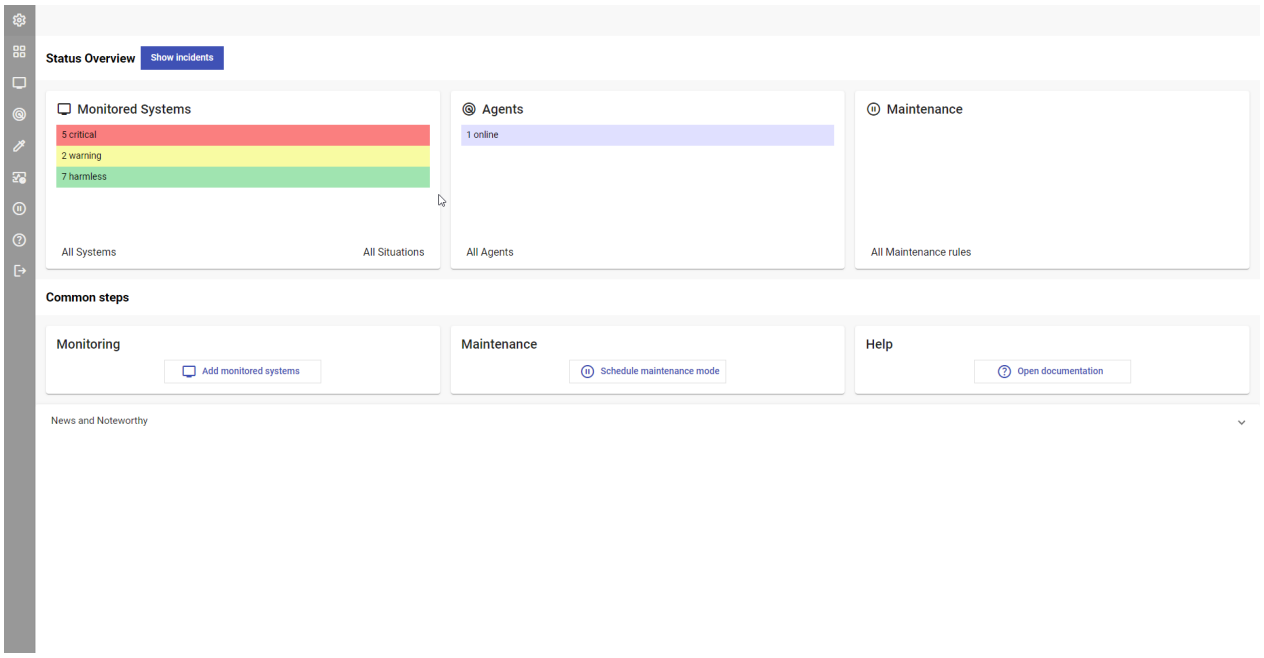

Image of Operational Console Status Overview

Operating Console areas

The default console when opening looks like the screenshot below. It has various sections.

- The Main Menu (on the left)
- The sidebar (list/tree of sections' items)
- The Main View (Content like overview or item details)

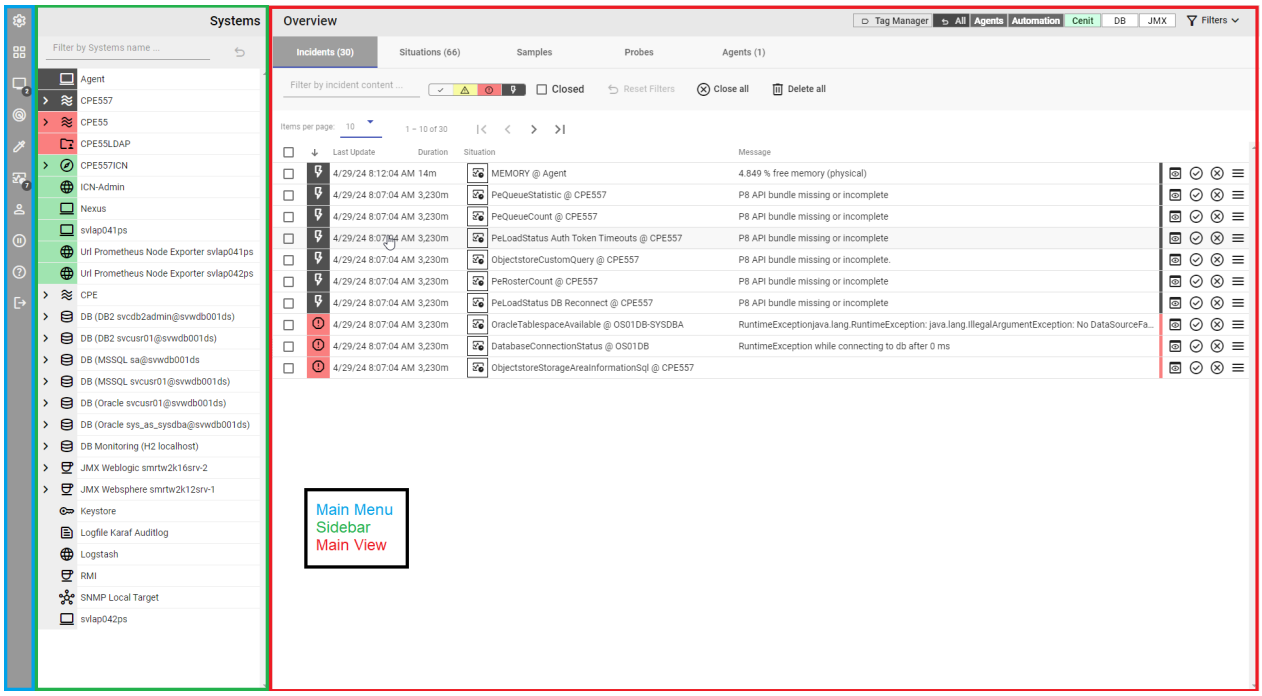

Image of Operational Console Description Overview

The Main Menu

On the left in this console is a main menu. The main menu automatically expands once the mouse is over it. It has several entries (buttons) which mainly can be used to control the information that is shown in the sidebar.

- The Configuration button is used to switch back to the ESM Service Monitor Console.
- The Status button is used to switch to the above described Status Overview.
- The next three buttons (Systems, Agents and Probes) are for the corresponding parts in the sidebar.
- The Maintenance button contains setting possibilities for maintenance.
- The Help button opens the documenation in which you can find the same documentation as in the already described Help Dashboard.
- The Logout button logs out of the system.

Furthermore you will find badges from time to time. This should bring up your attention to important information at this part.

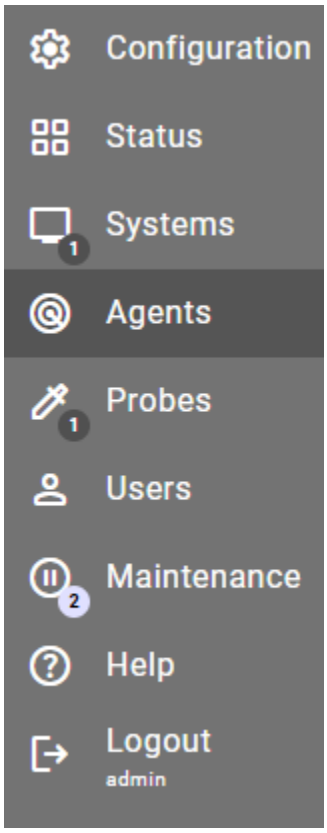

Image of Operational Console main menu

The sidebar

Depending on the selection from the main menu, the sidebar shows different information. Always at the top of the sidebar you have to possibility to use a textual filter for the list. Just enter your search criteria and the list will be filtered with a short delay - so a short pause during typing is also possible.

The Systems sidebar

Within the systems sidebar you can find all of your configured systems. The list is automatically sorted by severity - meaning the system with the highest severity is always at the top. Within the same severity, the list is in alphabetical order.

A system set that consists of several referenced subsystems can be expanded. In front of such a system set you might see two different colours. A "bubble" function that shows the highest severity of all of the systems (that are part of the system set - including the top level system) has been implemented. The first colour is always the highest severity of the set. The second colour, is the one of the entry itself. You can see an example in the screenshot below.

Systems that are shown in grey colour, currently do not have any kind of events.

Also you may find systems that have a "pause" symbol attached in the icon. These systems are currently affected by an active maintenance rule.

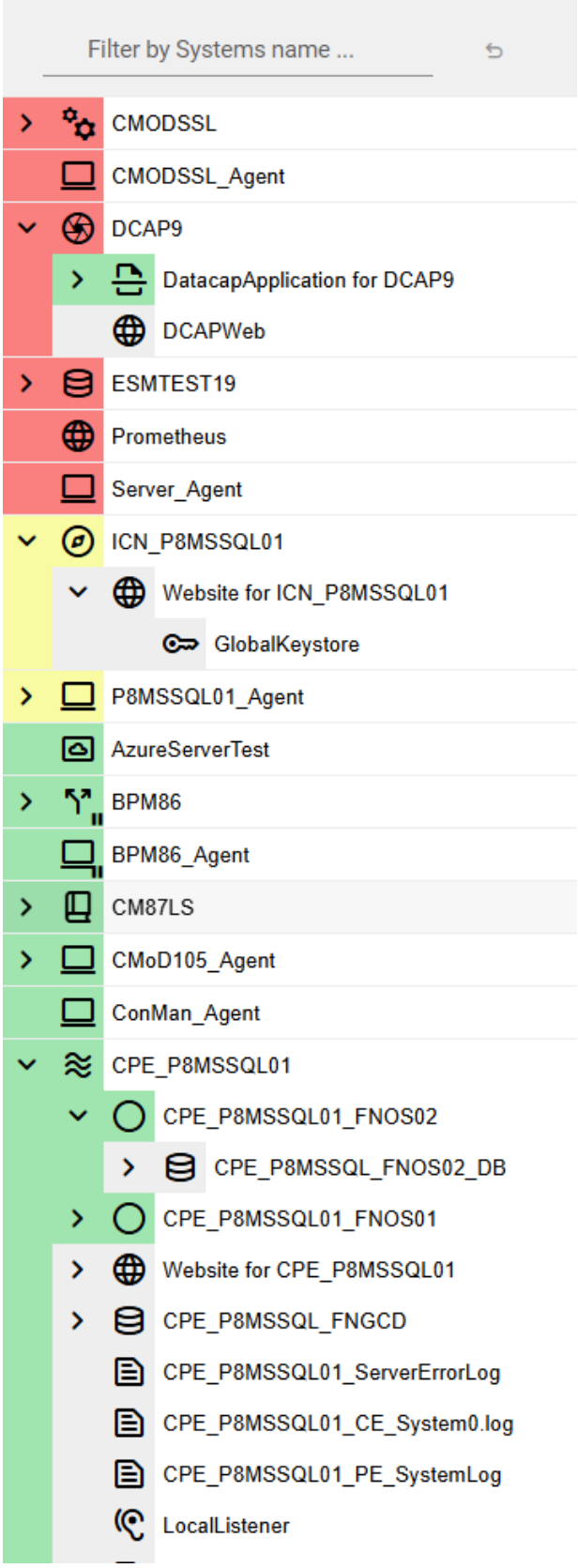

Image of Systems sidebar

The Agents sidebar

Within the agents sidebar you can find all agents that are or have been connected. The list is sorted in alphabetical order. The icon in front of an agent will be highlighted depending on the current status of the agent.

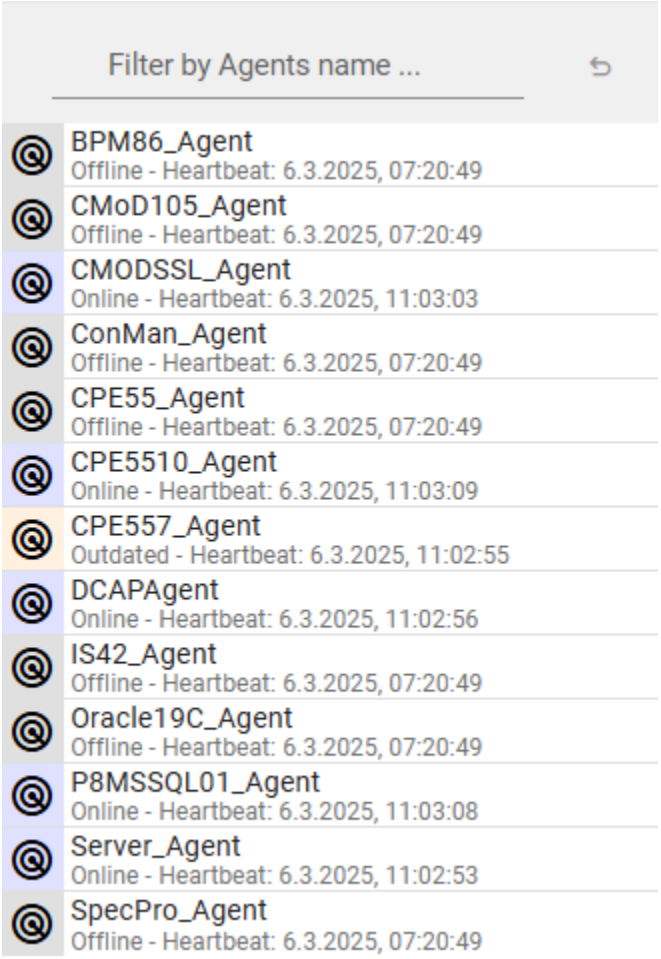

Image of Agents sidebar

The Probes sidebar

Within the probes sidebar you can find all probes that are set up. The list is sorted by name, active probes are on the top. The icon in front of the entry shows the current severity status of the probe.

Also you may find probes that have a "pause" symbol attached in the icon. These probes are currently paused due to an active maintenance rule.

Above the list you have the possibility to add a "new" probe configuration by clicking on the + next to the "Filter by …" section.

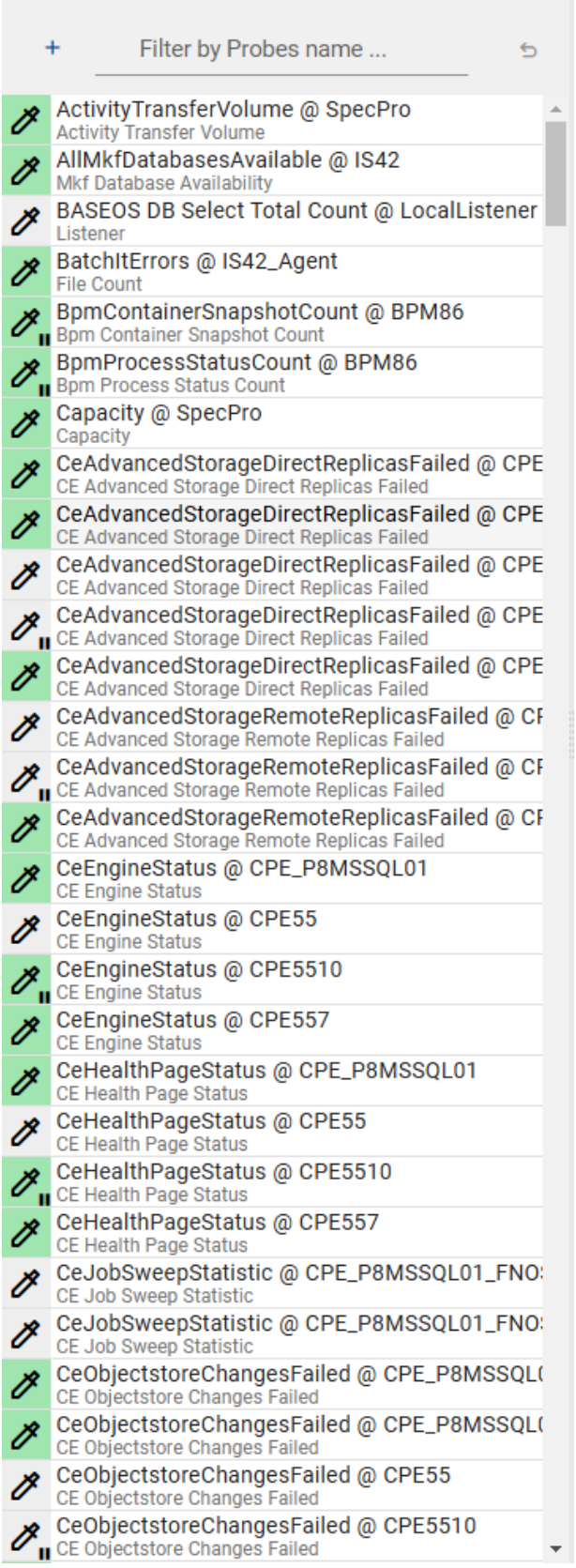

Image of Probes sidebar

The Users sidebar

At the top of the sidebar, you have the possibilty to add a new user or search for users by specifying a filter criteria. The list shows the already existing users. Per default one user for each role exists - admin, operator and guest.

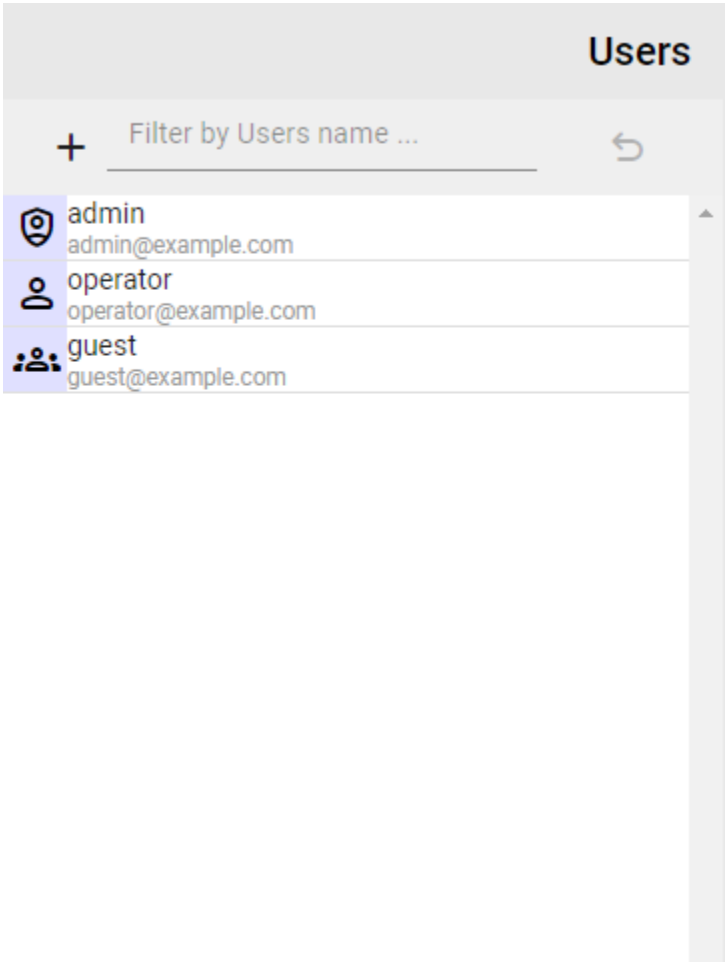

Image of Users sidebar

The Maintenance sidebar

At the top of sidebar, you have the possibilty to add a new maintenance rule using the + button. This will open the editor for creating a new rule - Take a look in the configuriation guide for more information about setting up maintenance rules.

Furthermore the list shows the already created rules. If rules have been created for a single run (One-time event), they will be removed shortly after the execution time has passed. Only rules that are set and shown as enabled will be executed. Currently runing rules are highlighted. The list is sorted, first the currently running rules are shown, then the rules that are enabled. At the end you will find the rules that are deactivated.

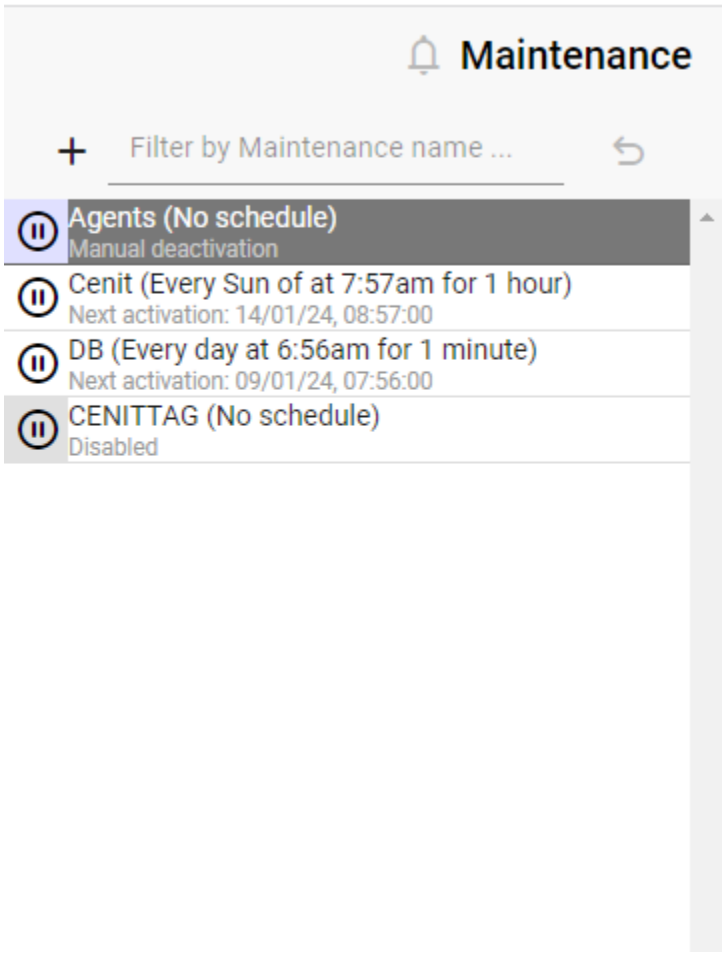

Image of Maintenance sidebar

The Help sidebar

Within the help sidebar you can find the documentation of ESM. The list is sorted in alphabetical order.

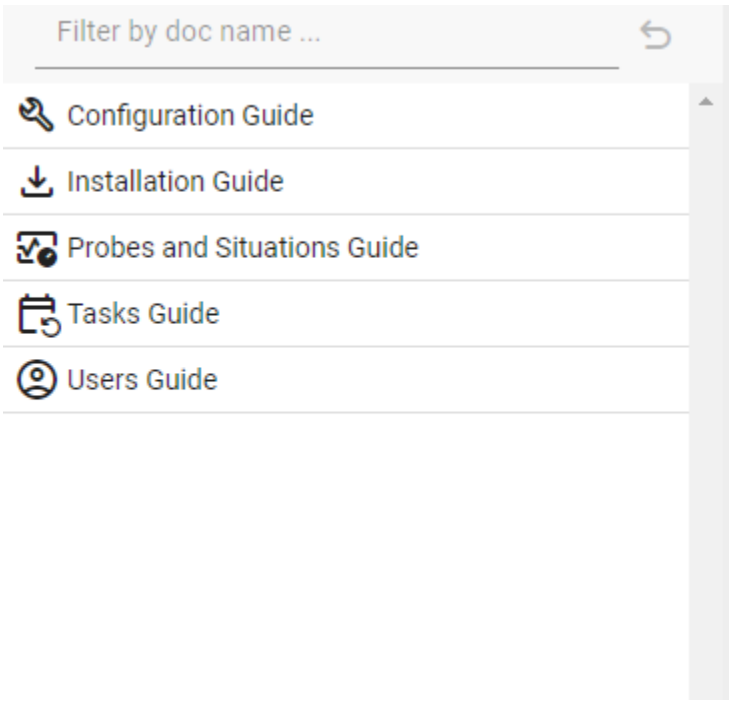

Image of Help sidebar

The Main View

The information that is shown in the main view depends on the selection of the main menu and the sidebar. Per default and when selecting anything from the main menu, but nothing from the sidebar, the "Overview" will be shown in this area. Once selecting something from the sidebar, more specific information about the selection from the sidebar will be shown.

Overview

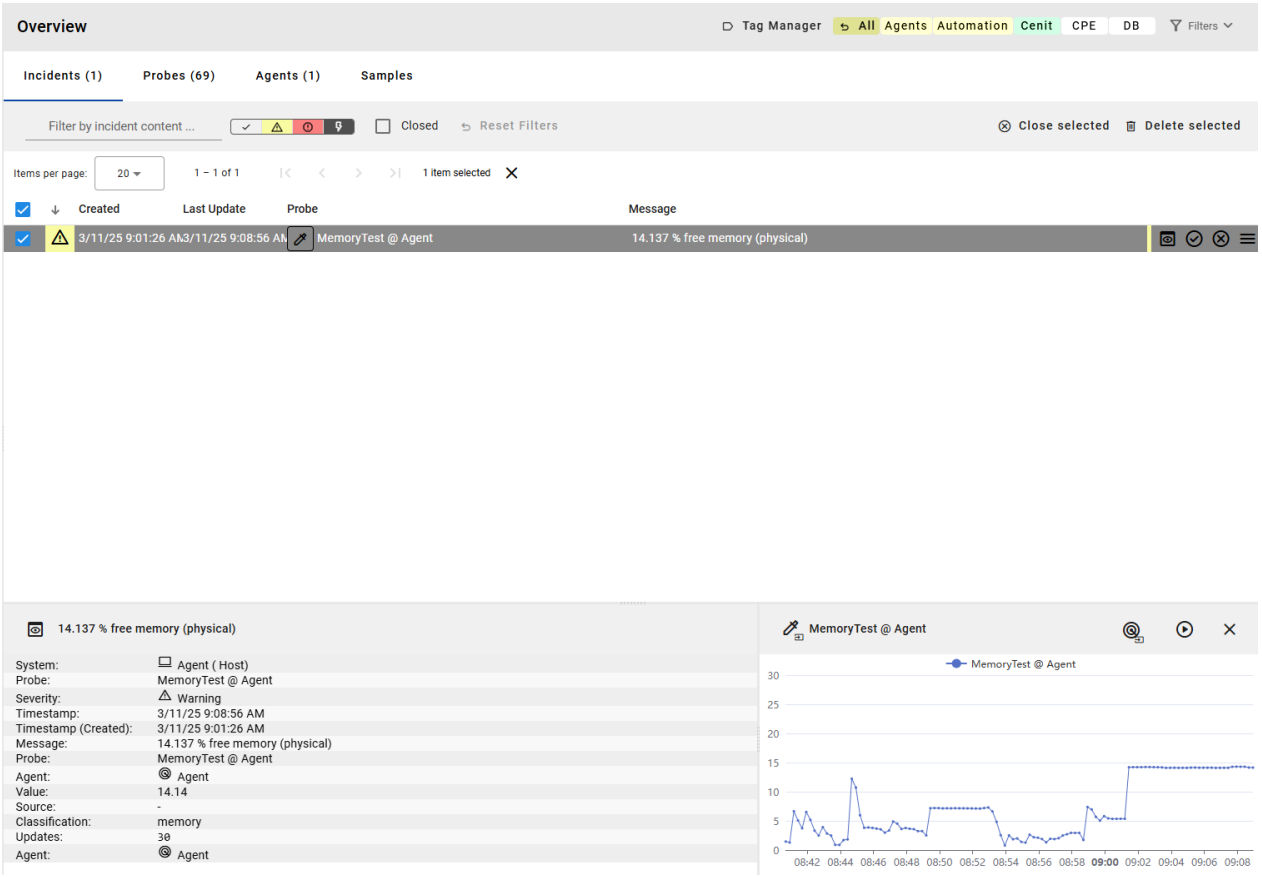

Image of Overview

The overview for Systems, Agents and Probes focuses on the same points and look similar. Only the Probes overview misses the Agents tab.

The overview for maintenance and help differs and will be described at the bottom of this section as separate information.

In the overview for Systems, Agents and Probes there are two sections.

Global Filter Section

At the top there is a global filter section. These filters define which information is available in the information section. You have the possibility to click on a tag. That will define the information that is available in the information section. Furthermore, can click on "Filters" and select one or several entries of a certain type from Probe type, System type, System and Agent.

NOTE

The selection within a type is a disjunction. The selection between several types is a conjunction. Between type and tag it's also a conjunction. Only the matching entries will be shown in the information section.

Information Section

In the information section you can find a total of 4 (or 3) tabs - Incidents, Probes, Agents and Sample. Those can be used to browse the information from different point of views. Also the per default active tab depends on which selection you made in the main menu:

Table 1. Combination of main menu selection and Active Tab

Main menu	Active Tab
Systems	Incidents
Agents	Agents
Probes	Probes

Incidents Tab

The number in brackets behind the tab reflects the amount of shown events depending of your selection.

In the incident tab there are more (local) filter possibilities.

- First you can use a textual filter, the function is the same as in the sidebar but the full content of the incidents is browsed for matching the criteria.
- You can use the severity filter to either show all events (Harmless and above) or Incidents when using a severity greater or equal to Warning. Just click on the Severity on the "slider".
- Use the check button in front of Closed to also list closed events.

Furthermore there are two buttons to either close all or delete all entries that are currently available in this information section. Although the list only shows a maximum of 10 entries, all are affected.

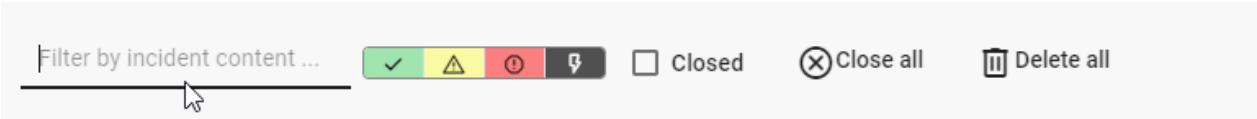

Image of Overview Incident Filter

The list of incident can be sorted by clicking on the headers of the list columns.

A single click on an entry in the list, opens detail information at the bottom of this section.

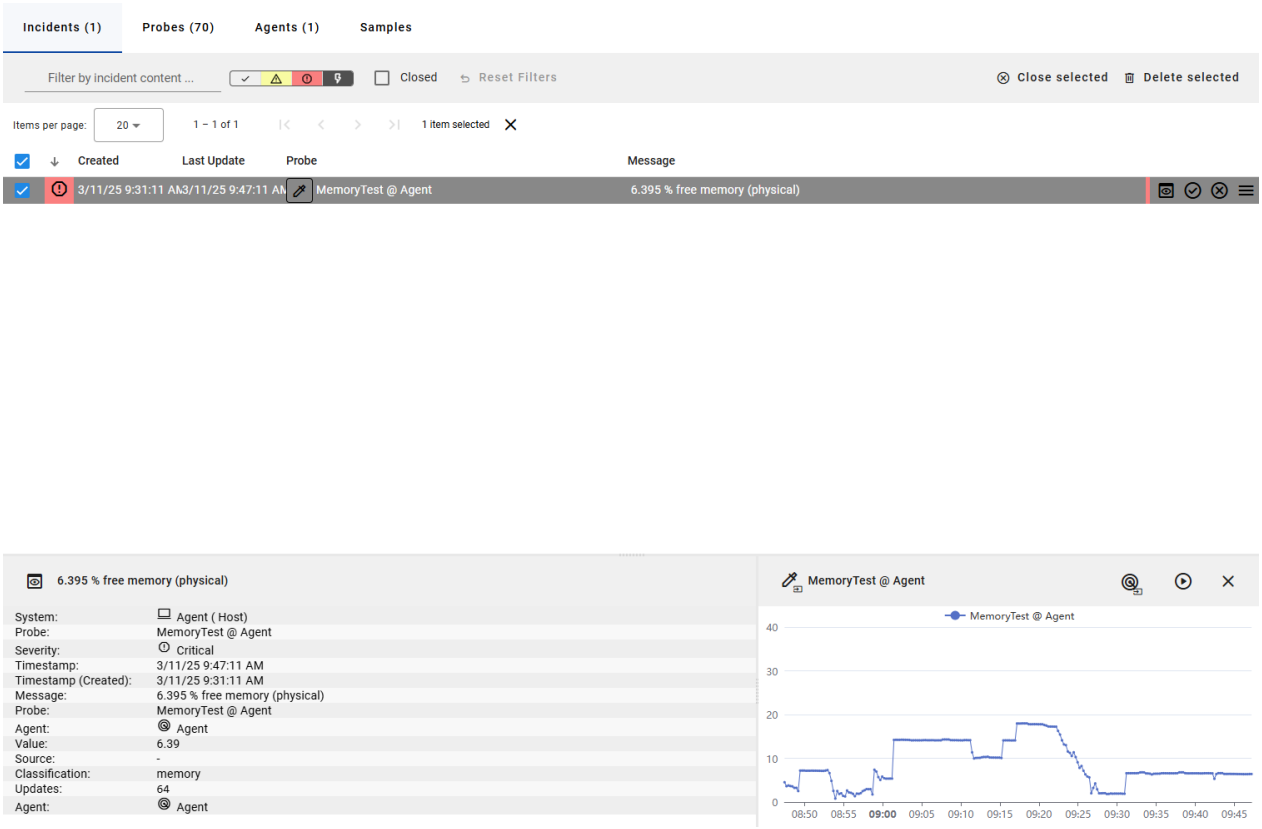

Image of Overview Incident Details

A double click on an entry opens the context view. This pops up in front of the full console. It has cross references to Subsystem, Probe and Agent. You can review these information directly by clicking on the text of the tab or go to the corresponding settings by clicking to the icon next to the text of the tab. Also you can review Incident details incl. a graph. In this view you do have the possibility to analyze the incident with an AI Analysis. The button is available once a OpenAI API subsystem has been created. A click on the button provides a pre defined prompt in the view which can be used for starting the analyzation.

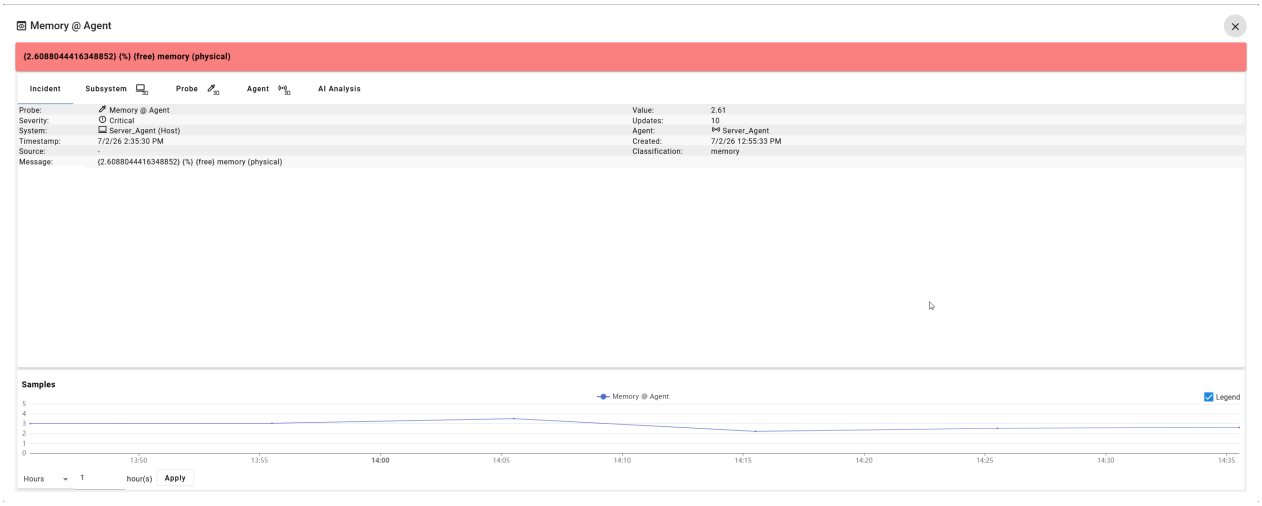

Image of Overview Incident Context

In each event line you can find several buttons. The first one is next to the probe information and will cause a switch to the probe main menu along with the selection of the probe in the main menu.

At the end of the line you find 4 more buttons. The first one is the same as the double click and opens the context view. With the second one you can acknowledge the entry and add an annotation. Only one annotation at a time is possible, the annotation is overwritten with each new acknolwgement. It is also shown in the incident details. The third button is for closing the event. The last one opens a menu with further possibilities. Xou can only delete the event here or also start a AI analysis of the incident. The AI analysis is only available once a OpenAI API subsystem has been created.

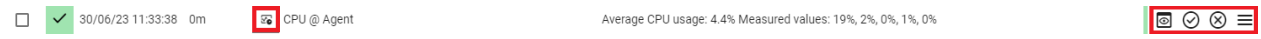

Image of Overview Incident Entry Buttons

NOTE

Per default the incidents tab only shows incidents and not all events. The is due to the severity filter which is set per default to Warning and above in this tab.

Probes Tab

You have the possibility to add a new probe configuration from this view.

Also there are more (local) filter possibilities.

- First you can use a textual filter, the function is the same as in the sidebar. In this case the probe name is browsed for matching the criteria.
- You can use the status filter to either show all or only active/inactive probes.

And within the tab you can distinguish between a list (default) or a tiles view.

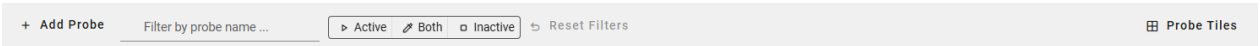

Image of Overview Probes Filter

The list view lists all probes. Selecting an entry from the list, will open a context information at the bottom that shows the graph.

At the end of each entry you have three options. The first is a slider button to de-/activate the probe. The second option is a button for opening the probe editor and the third can be used to execute the probe adhoc.

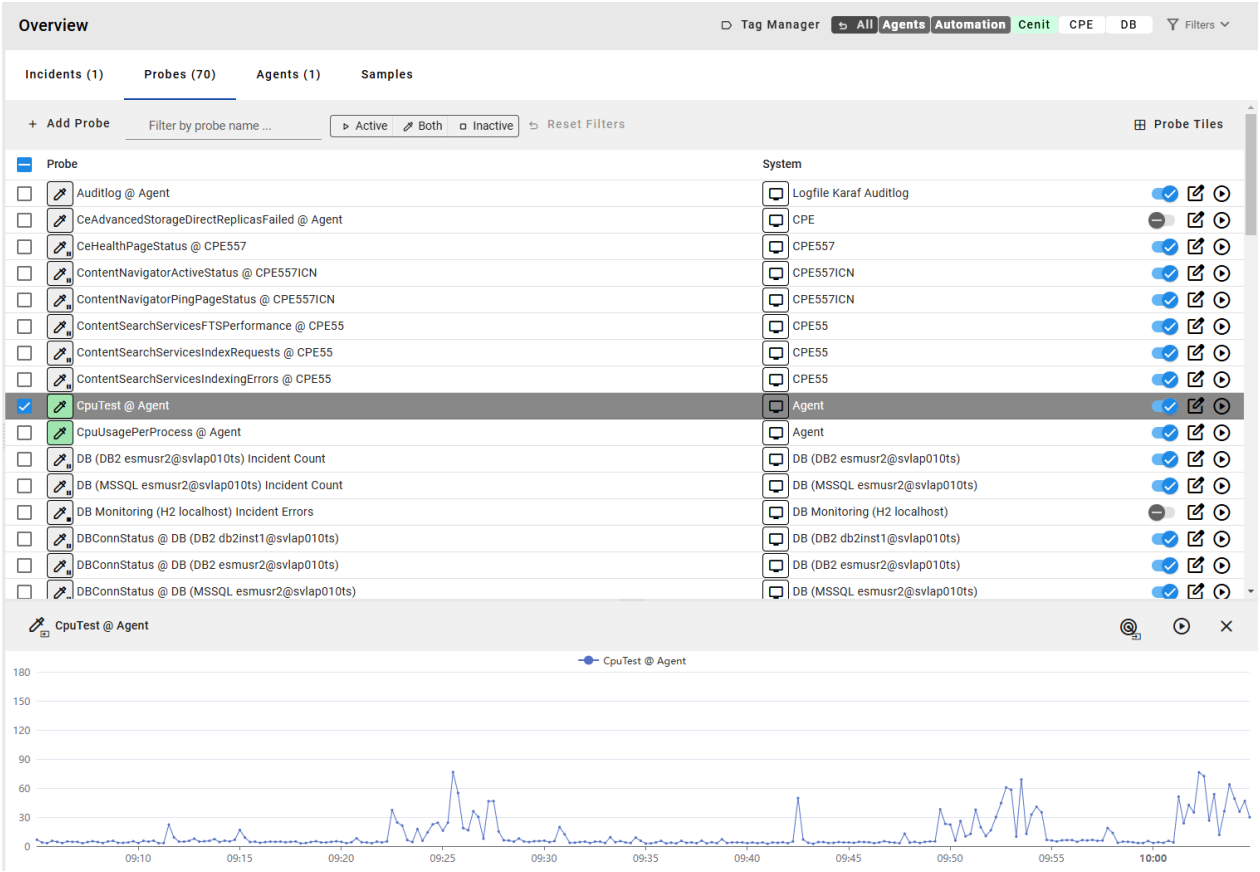

Image of Overview Probes Details List

The tiles view shows a heat map for all probes. Selecting an entry from the tiles, will open a context information at the bottom that shows the graph.

When hovering over an entry a slider button to deactivate the probe and an execution button for adhoc execution of the probe appear.

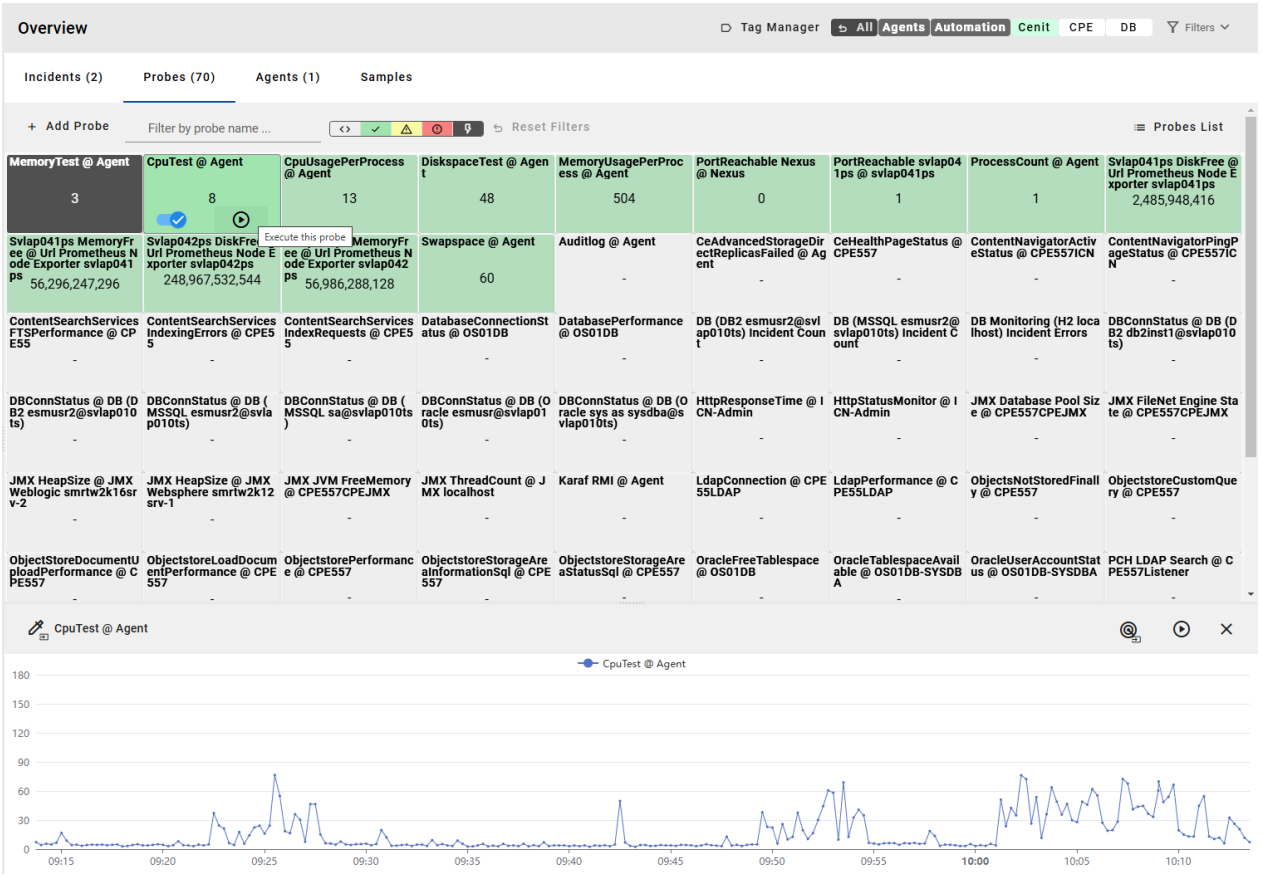

Image of Overview Probes Details Tiles

Agent Tab

The Agents Tab offers a "Update All" functionality. This can be used to update all outdated agents. The button is only available for admins and only active when the following requirements are given.

- Outdated agents are available
- The corresponding agent installers are available in <Server-Install-Dir>/karaf/agent/installers/<Version>/<OS>

In the agents tab you can textually filter for agent label.

Image of Overview Agents Filter

Furthermore the agents along with severity of agent basic probes are shown as a map.

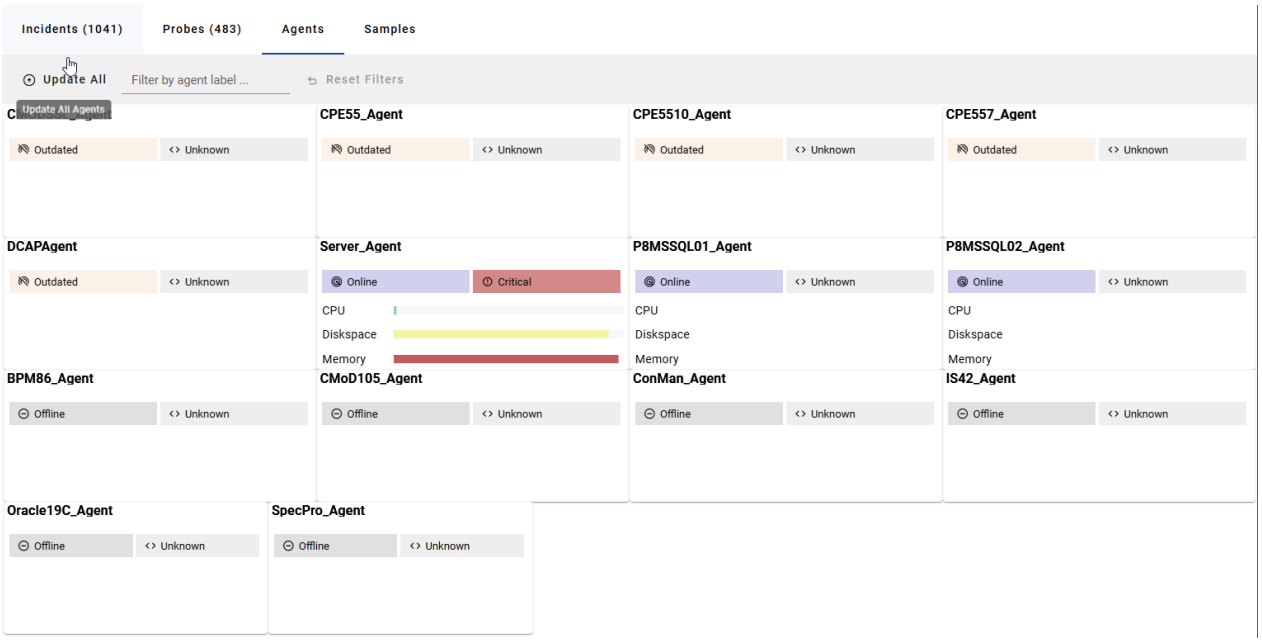

Image of Overview Agents Details

NOTE In this tab no additional details when selecting an agent are shown.

Samples Tab

In the samples tab there is no local filter option. The list shows the latest samples with a maximum of ten entries per page. The list is automatically updated and sorted by the timestamp per default.

Selecting an entry from the list, will open a context information at the bottom along with cross references to the Incident Context and Probe Details. Also the probe can be executed adhoc from here.

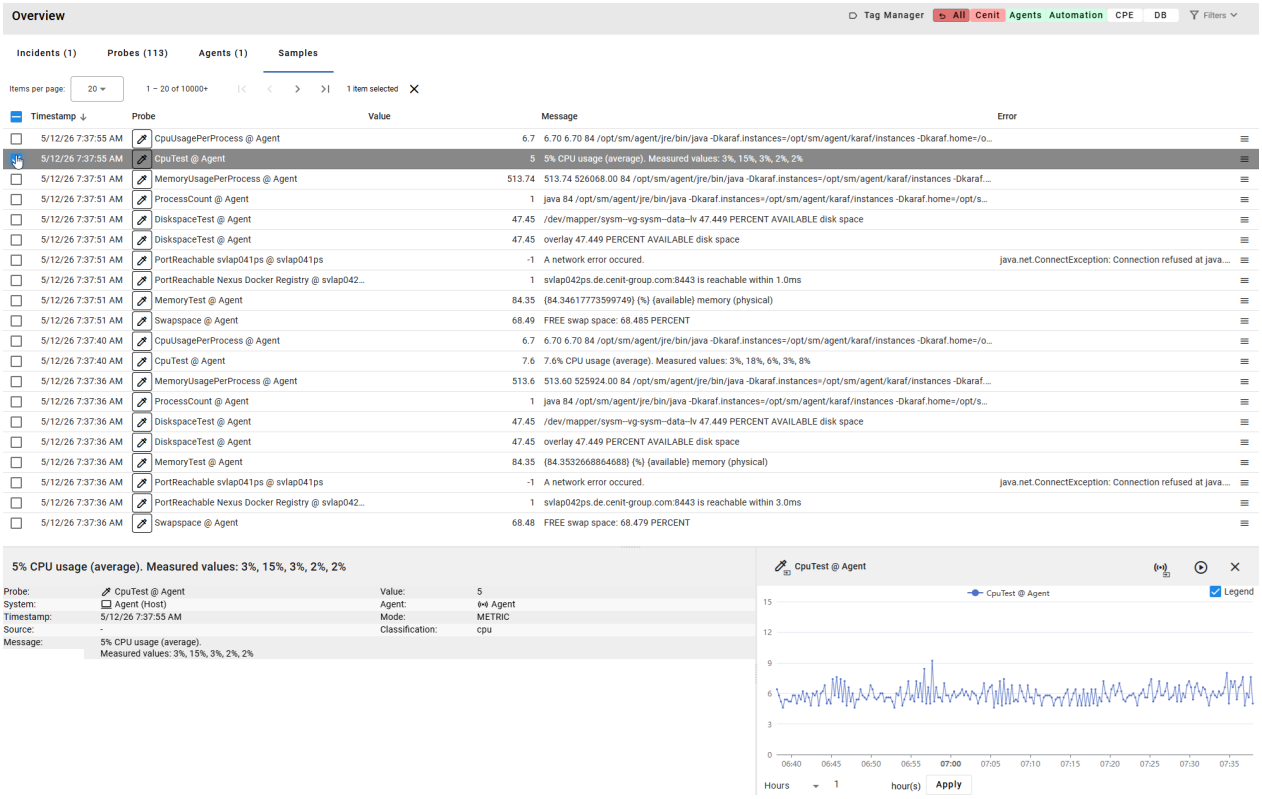

Image of Overview Samples Details

NOTE The selected list entry can disappear from the list due to updates, but the context will stay available.

Multiselection within the tabs

In the Incident, Probes and Samples tab you can multiselect entries by holding the CTRL key on your keyboard and selecting the entries with the mouse or selecting the entries with the check at the beginning of the lines.

For all selected entries a graph is shown in the section below the list. If several entries are selected, the details part will disappear. See example screenshot below.

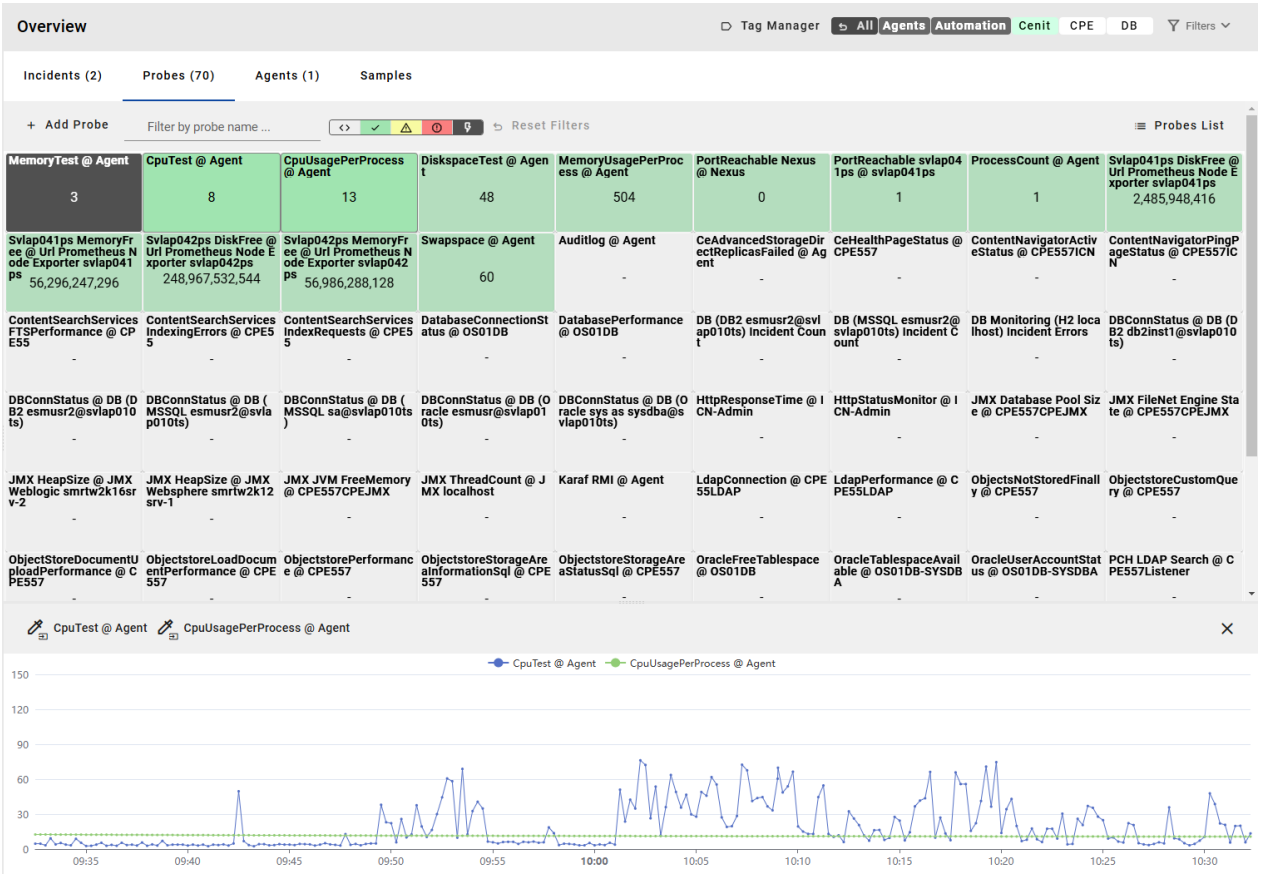

Image of Overview Multiselect

Overview for Users

The overview for Users lists all configured users. For each user entry buttons at the end of the line are available. You can use them to edit, delete, unlock or enable/disable the account.

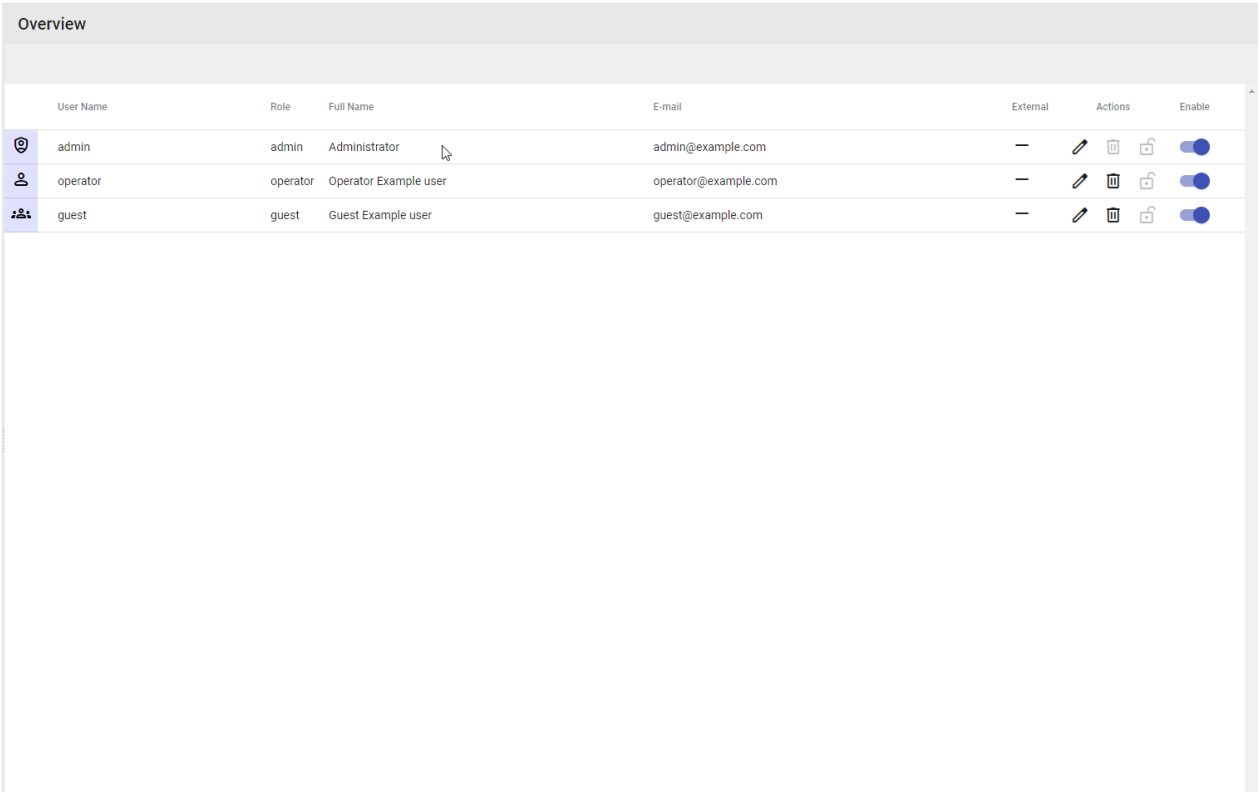

Image of Overview Users

Overview for Maintenance

The overview for Maintenance shows the currently configured maintenance rules along with some additional information. Such as state, tags used for the rule, schedule, duration and unit, start and end time and next activation/deactivation. Also at the end of each entry is a button for deleting the rule. When selecting a entry from the list more information about the affected situations (Name, System and Tags) are shown at the bottom. Doubleclicking an entry will open the specific information view for this rule, same as when selecting the entry from the sidebar.

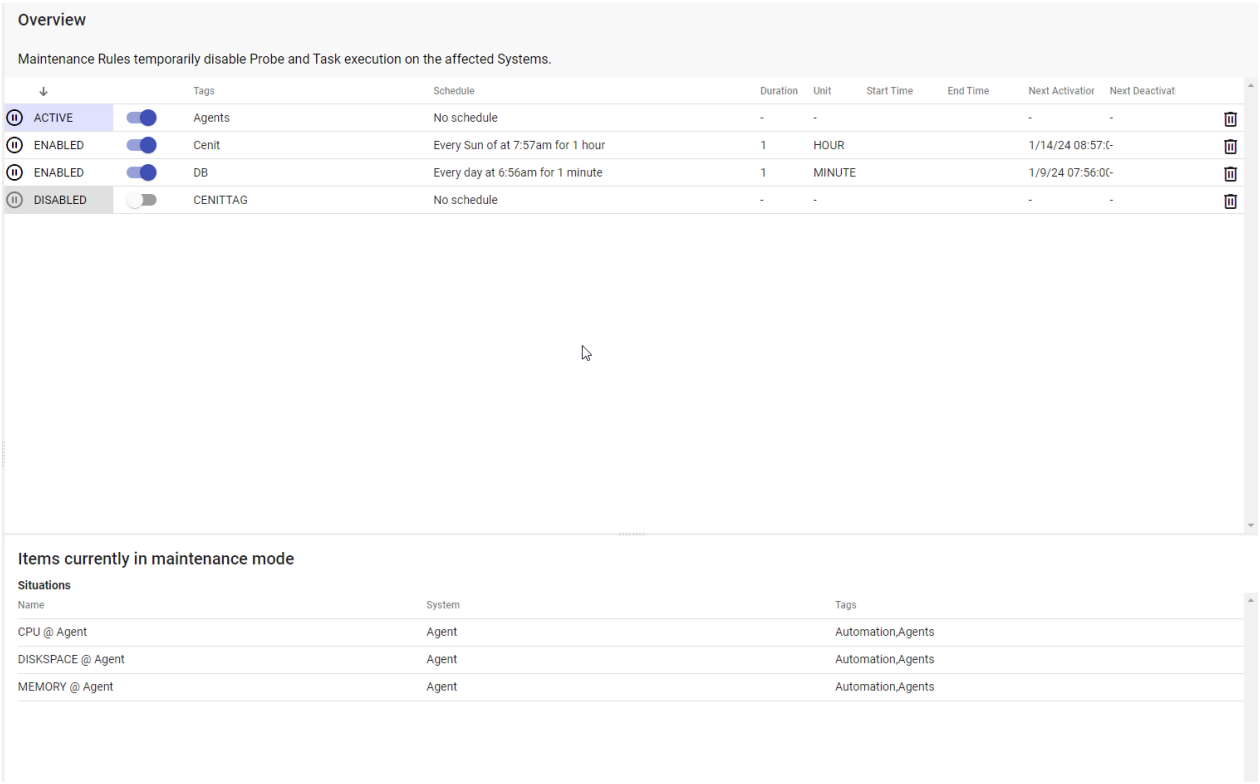

Image of Overview Maintenance

Overview for Help

This view is empty by default.

Specific Information Views

The following Views are shown, once a specific entry from the sidebar is selected.

Detailed View for System

The detailed view for a selected System almost looks like the "Overview". The filter at the top are missing but you can find a summary information instead. The content of "Subsystems" can also be used to browse between the specified subsystems. The summary can be minimized if not needed.

The Incidents and Probes tab are the same as in the overview, the content is already filtered and only shows the information of the selected sidebar system.

As you can see in the screenshot below, there are no Incidents for the selected system CPE_P8MSSQL01, neither CPE_P8MSSQL01 has one, nor any of the referenced systems. All checks are marked as OK.

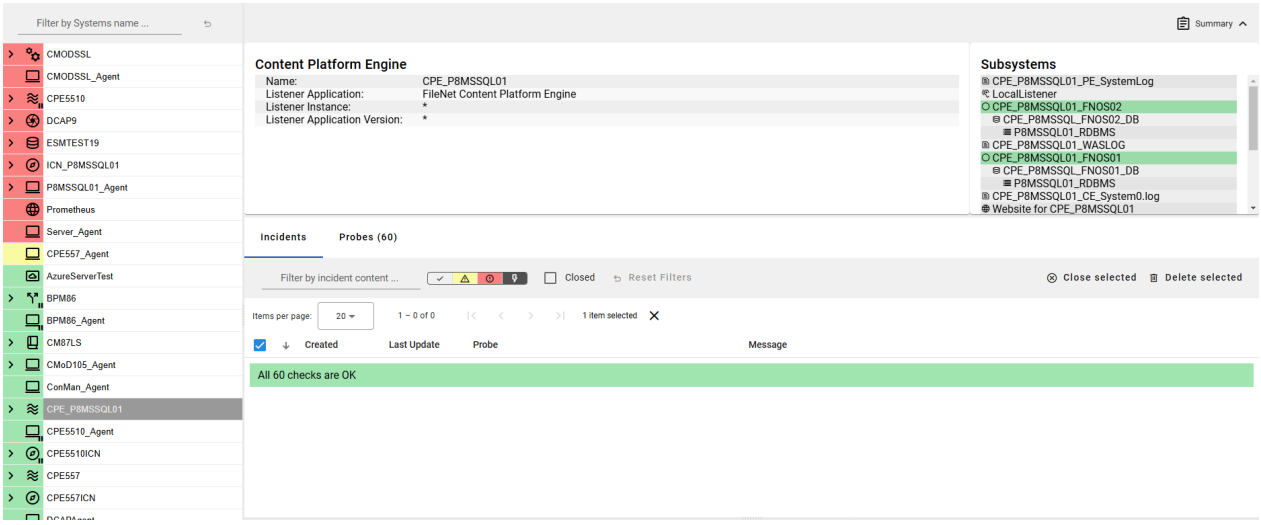

Image of Details View for Systems

Detailed View for Agents

The detailed view for a selected Agent also has a summary part at the top. The summary lists the Health Status of the Agent (CPU, Diskspace and Memory information are used for that).

The recent tasks that have been executed on this agent are shown. You can review the task context via double click on the entry. A pop-up will open containing the task context information. Of course this can be closed.

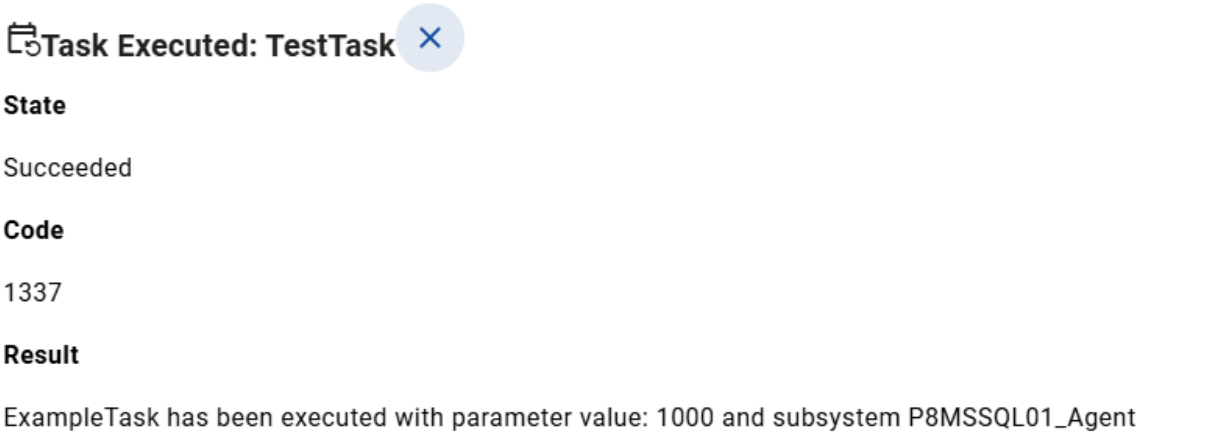

Image of Details View for Agents Task Context

Furthermore you can see detailed Agent information.

At the bottom of the view you find the already known information from the Probes tab. In this case the list

is filtered already and only shows the probes of the selected agent.

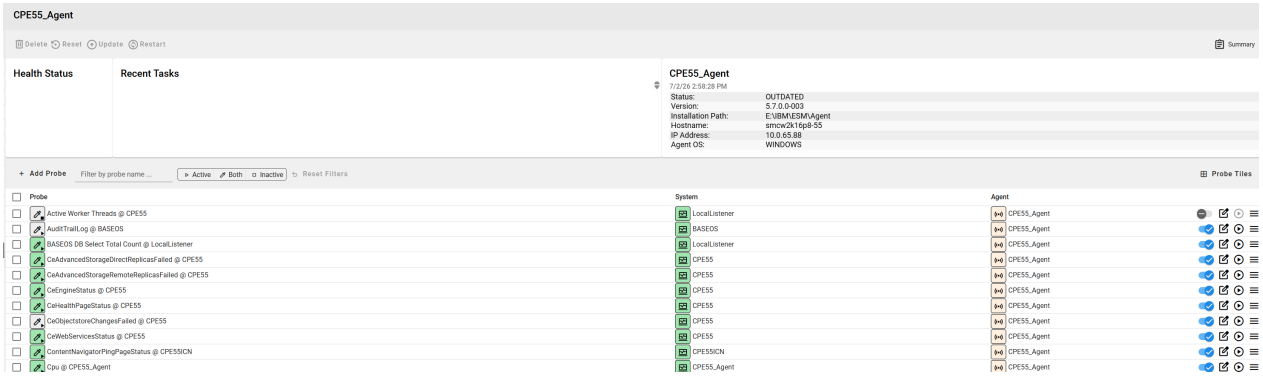

Image of Deatils View for Agents

Some action buttons are available. If the agent is offline you can delete it. If the agent is timed out you can reset it to offline. With the update button you can update the agent if it is outdated. The button is only available for admins and only active when the following requirements are given.

- Agents is outdated
- The corresponding agent installer is available in <Server-Install-Dir>/karaf/agent/installers/<Version>/<OS>

The Restart button can be used to restart the bundles of an online agent.

NOTE The Update and Restart button does not work on container agents.

Detailed View for Probes

Above the summary part at the top you can activate/deactivate the probe or start an adhoc execution.

In the summary you can see information about the probe setup. Such as the parameters that are used, the schedule and the evaluation information.

Along with that you can see a list of samples or incidents (if you switch the tab) from the probe and a graph for the values of the last hour is shown.

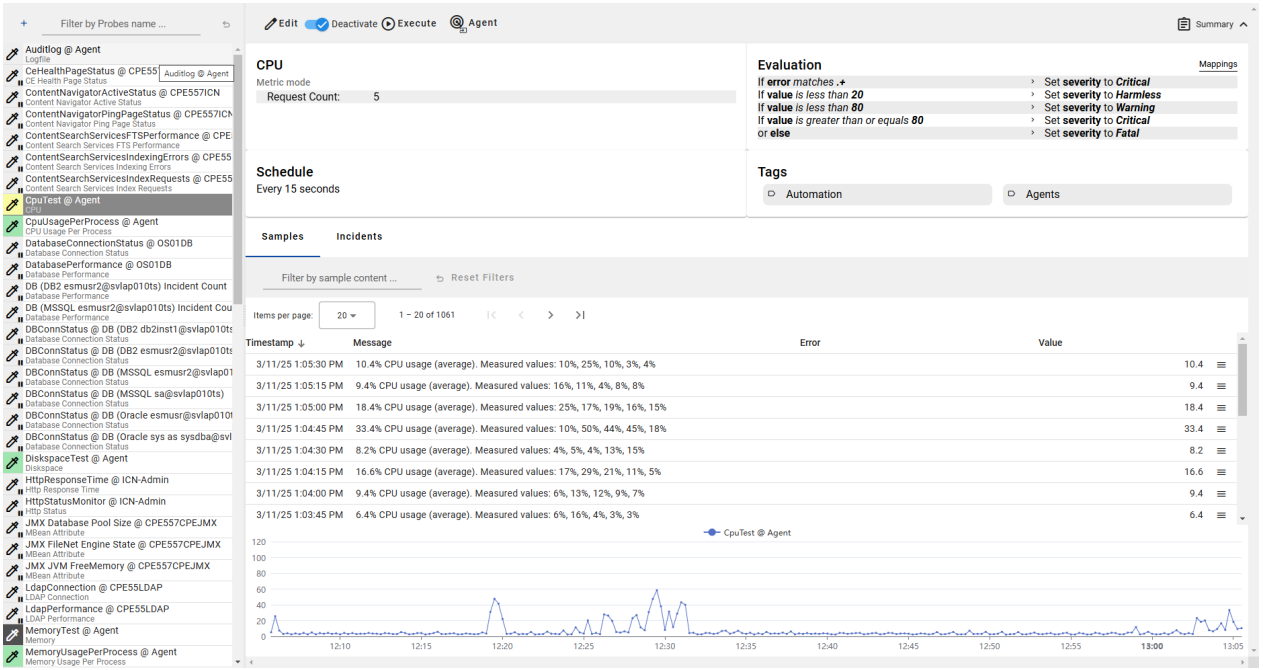

Image of Details View for Probes

Detailed View for Users

When selecting an user from the sidebar, the details view for the user is opened. Within the view buttons for editing, deleting unlocking and enabling/disabling are shown.

Furthermore, the view offers additional (detailed) information for the user - account and contact information.

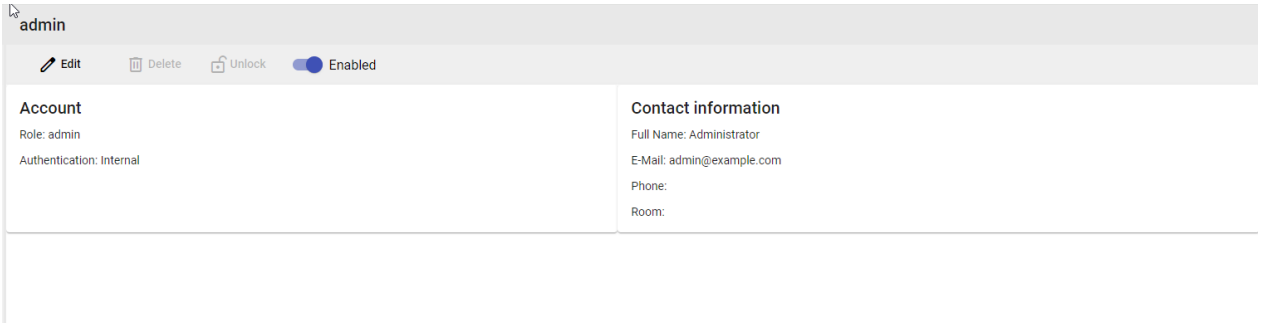

Image of Details View for Users

Detailed View for Maintenance

The summary part in the detailed view for a maintenance rule has an edit and delete button, as well as a slider button for enabling/activating or deactivating the rule. The edit button will open the editor for this rule - Take a look in the configuration guide for more information about setting up maintenance rules. The slider will distinguish the state active or enabled by the schedule. If no schedule is used, the rule will become directly active, if a schedule is used that does not fit the current time, the rule will be enabled. Disabled is used for keeping the rule stored without execution.

Furthermore some sections for the tags used in this rule, the schedule information and next activation (if rules is enabled) are shown. The lower part shows more information about the affected situations (Name, System and Tags).

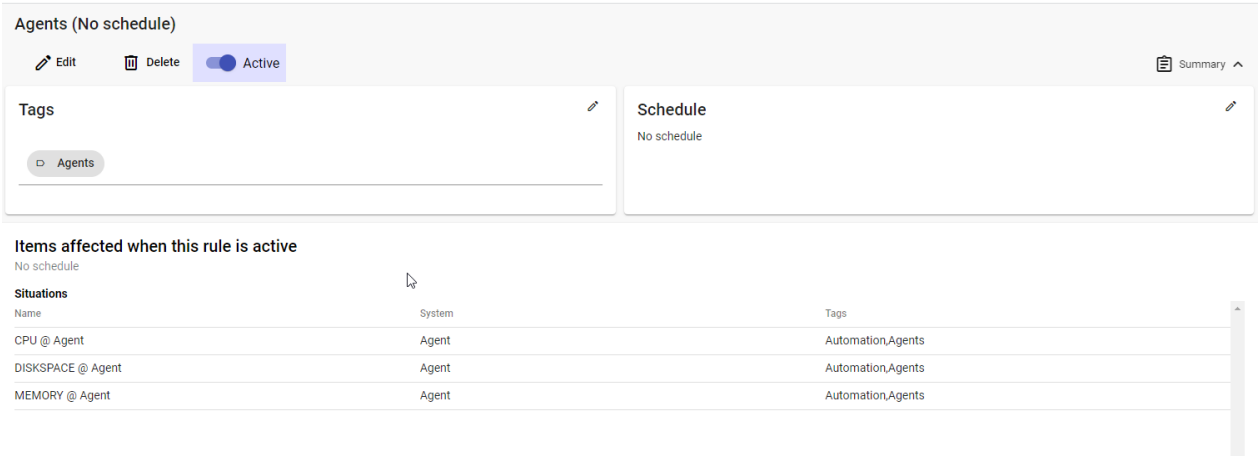

Image of Details View for Maintenance Rule

Probe Management

Clicking on the + above the sidebar in the probe menu or using the edit functionality for an existing probe opens the probe editor. Within the editor you can:

- Adjust the probe parameter(s)
- Define the schedule for the probe
- Create a meaningful evaluation, or use/share an evaluation
- Add a tag
- Setup automation by using/adding task triggers

You can switch between the steps by selecting the step at the top. If a step is missing required information, the step is highlighted in red colour. The setup cannot be saved as long as required information is missing.

Probe setup step

Within this step you can select the (sub)system and one of the corresponding probe types. Also you assign the agent on which the probe should be executed.

The Name will be given based on the system and probe type but can be adjusted.

At the end you can set the probe as active and define the parameters.

Help information is shown on the right side.

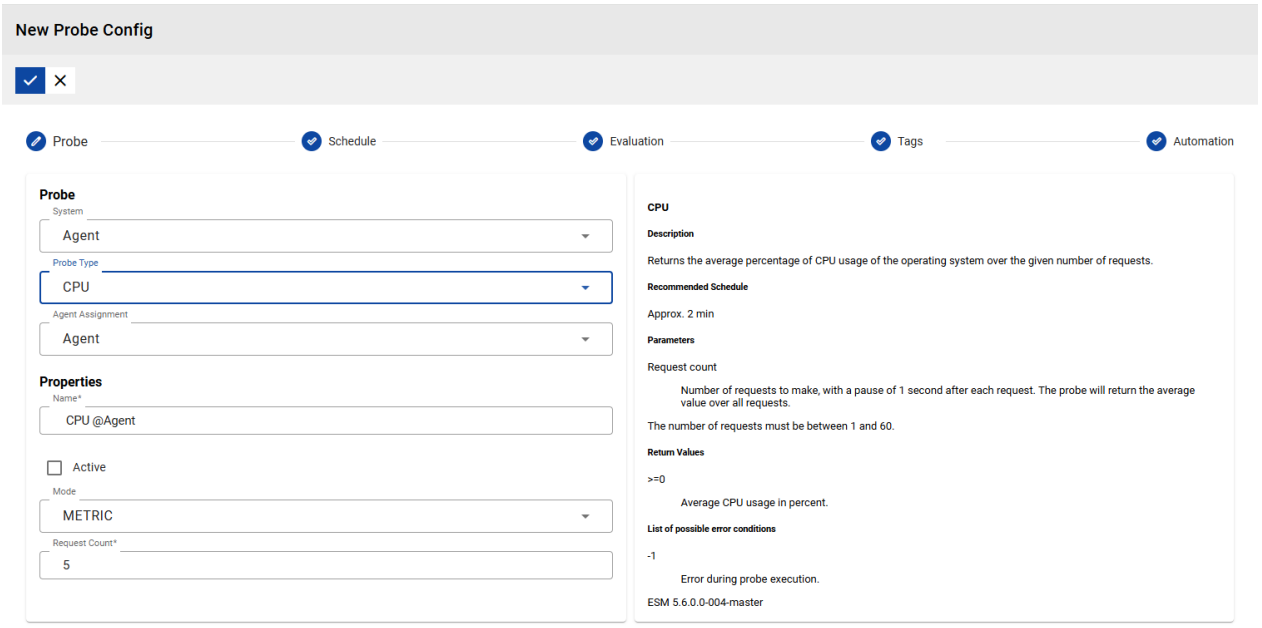

Image of Details View for Probe Probe Setup

Schedule setup step

NOTE This step is not available for all probe types. E.g. Logfile probes will not show this step.

Within this step you can select between a simple interval execution or pre-/selfdefined cronjob options.

For a simple interval you also have the possibility to define a start and end date/time.

Typically recommended schedule information is provided in the help information in the probe setup step.

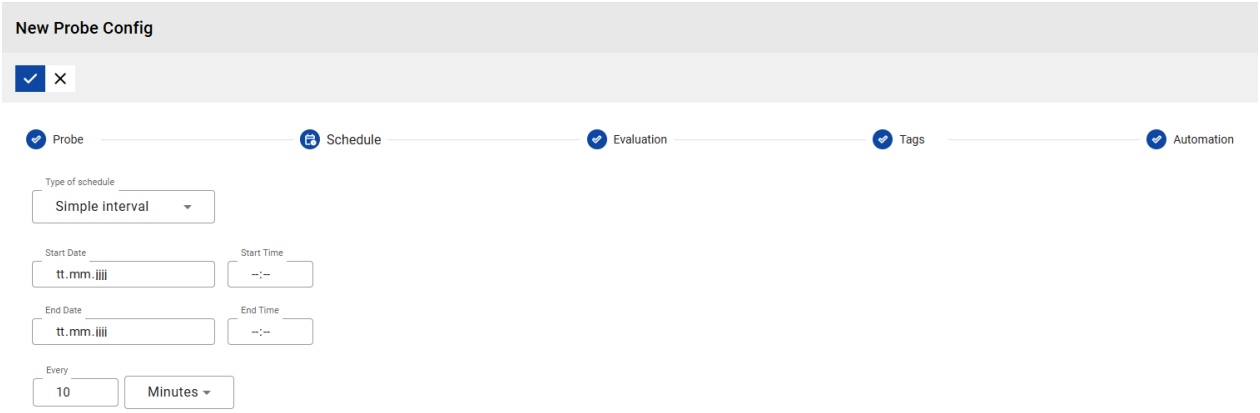

Image of Details View for Probe Schedule Setup

Evaluation setup step

In the evaluation the incident rules for a probe will be defined. Depending on different conditions different statements can be executed. E.g. severity can be set etc.

An evaluation setup has two parts, the "condition and statement" section and the "escalation and duplicate filter" section.

The "escalation and duplicate filter" is not used in this example scenario for the configured CPU probe:

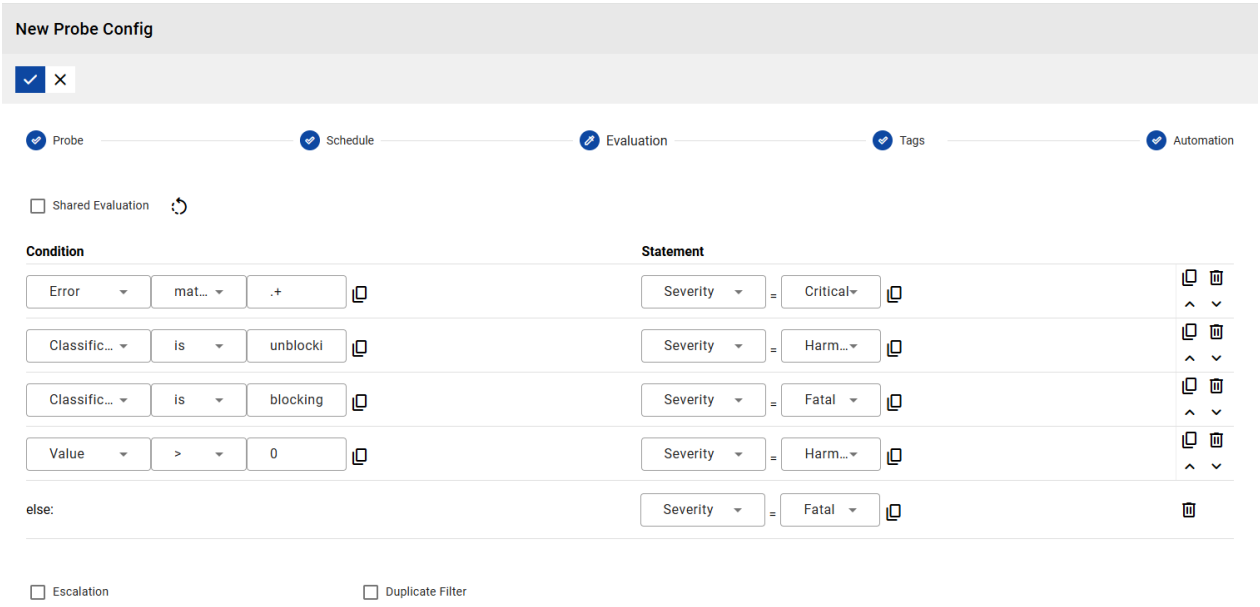

Image of Details View for Probe Evaluation Setup

Conditions

IMPORTANT The first condition that matches wins.

You can choose between the following sample fields for the condition:

- value = return value of the sample.
- error = error id included in the sample.
- message = message text of the sample.
- classification = classification text of the sample.
- timestamp = timestamp of the sample.
- source = source text of the sample.

The following operators are available:

- "! =" = not equals

- "= =" = equals
- "<" = smaller than
- ">" = greater than
- "< =" = equal or smaller than
- "> =" = equal or greater than
- "contains" = containing the followed expression
- "matches" = matching the followed expression

MultiPartConditions

You can create MultiPartConditions by clicking into the cell of a condition and then clicking on the "Copy" icon that appears to the right of the condition.

Image of Details View for Probe Evaluation MultiPartCondition

Statements

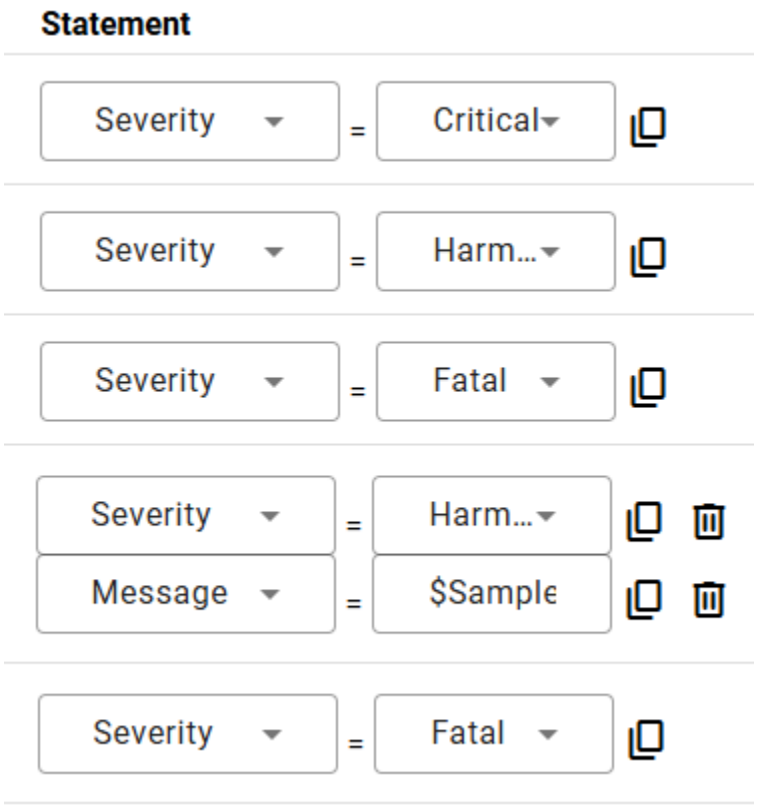

Image of Details View for Probe Evaluation Statements

It is possible to use either one (single) statement or several (multiple) statements per condition. Clicking on the copy button next to the statement adds an additional line.

Statements for the following slots can be used:

- classification
- error
- message
- severity
- source
- value

For the Severity the content is predefined and can only be selected from a drop-down. For all others the content is plain text which can be either self created or the content of the sample slots can also be used by specifying e.g. $Sample.value as shown in the screenshot.

Escalation and Duplicate Filter

The Escalation and Duplicate Filter function is used to act on a certain amount of incidents from the same type in a certain period.

NOTE The duplicate detection will have no effect for metric mode samples. This is because the metric mode implies per definition an active duplicate detection all the time.

A duplicate incident is identified by the fields:

- Classification
- Severity
- First x characters of message text (select able)
- First x characters of error text (select able)

The default setup looks like this:

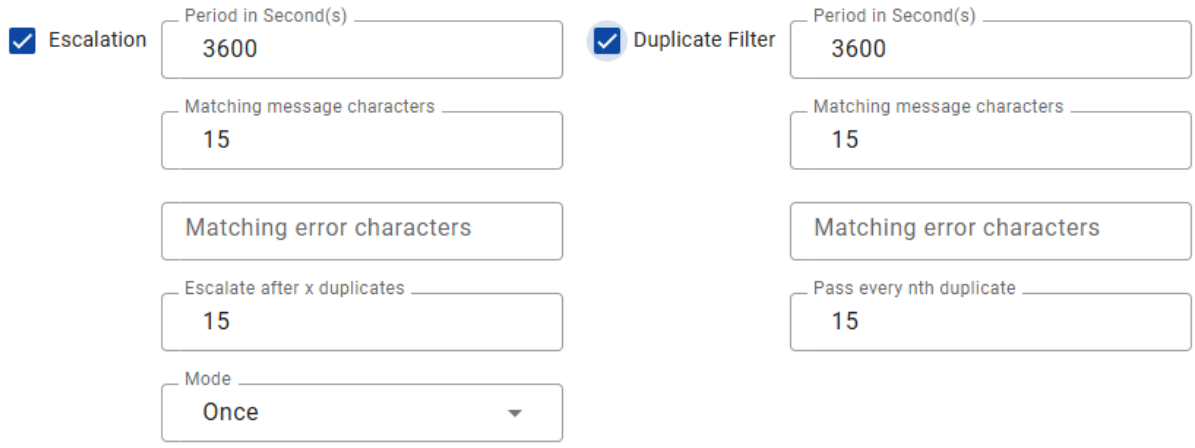

Image of Details View for Probe Escalation Setup

NOTE Only one setup per probe is possible - all incidents are handled with the same settings.

Description of the parameters

Checkboxes

Check the box to set active.

NOTE If both is selected, the escalation is done before the filtering of the duplicate!

Period

Specify the period for checking as a duplicate in seconds.

Matching message characters

Specify the amount of matching character for identify as a duplicate. The first x characters are compared. 0 means no characters are compared, empty means all characters will be compared.

Matching error characters

Specify the amount of matching character for identify as a duplicate. The first x characters are compared. 0 means no characters are compared, empty means all characters will be compared.

Escalate after x duplicates

If x duplicates appeared in the specified period, the current incident is escalated.

Pass every nth duplicate

The x duplicate is passed as a new incident to the console.

Mode

Once → Only escalated one time, the severity can only be raised to the next level.
Multiple → Escalation can happen several times over several levels.

Escalation and Filter Mechanism - How does it work

Once a sample is received at the server, the processing of the sample starts. The processing reviews the amount of already received samples for the given period.

For escalation: If the amount is less than the specified amount, the new incident stays at same level.
If the amount is equal or higher, the level is raised.

For filtering: If the amount is less than the specified amount, the new incident is discarded.
If the amount is the same, a new incident is created.

NOTE For now, HARMLESS and FATAL incidents do not get escalated. The behavior for HARMLESS might change in the future.

Shared Evaluation

For sharing or using a existing shared evaluation you have to check the button in front of "Shared Evaluation". A field is added that shows that a shared evaluation is required. You can now enter a name for a new shared evaluation or click in the field to select one of the already existing.

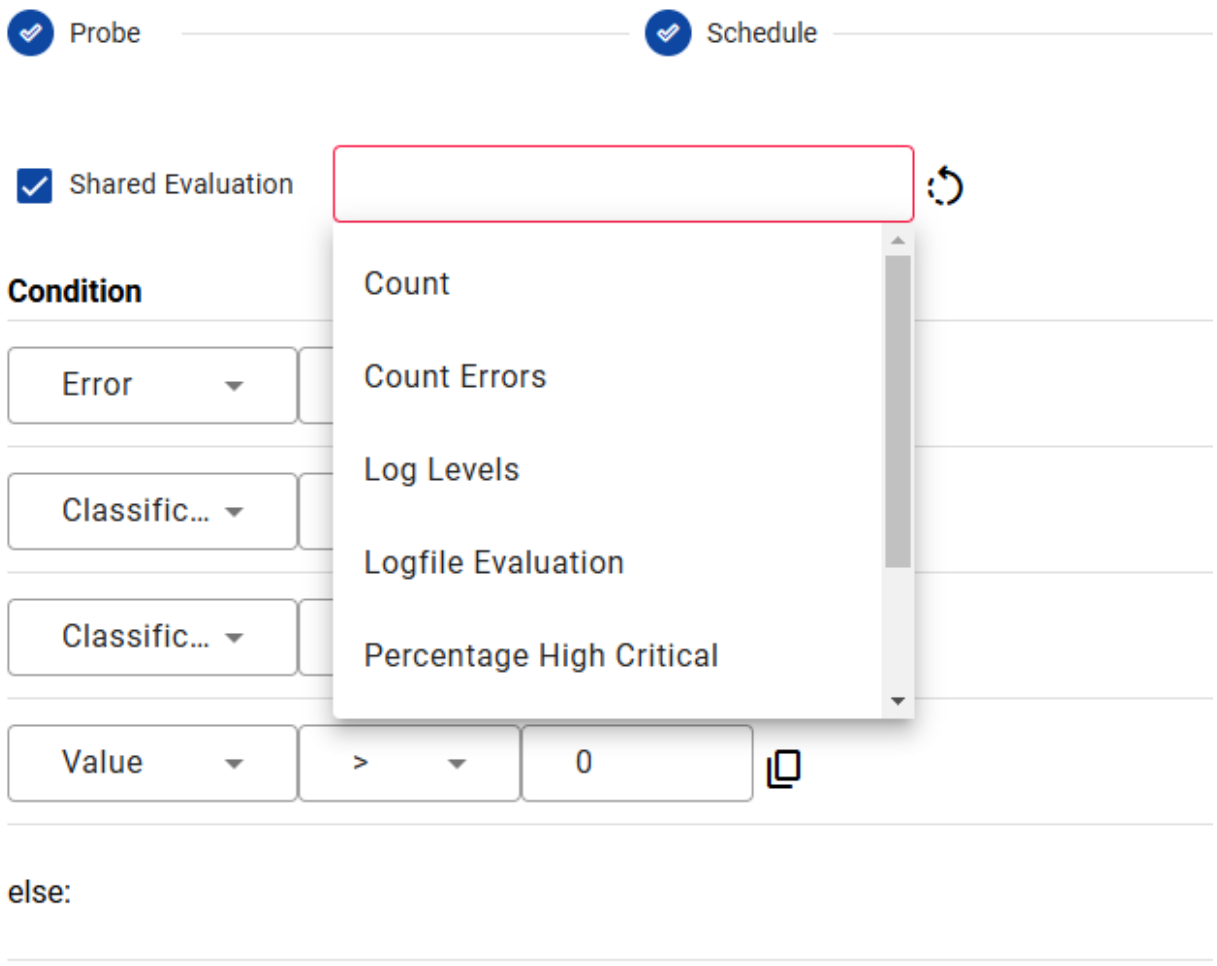

Image of Details View for Probe Shared Evaluation Setup

By default the following predefined shared evaluations are available:

- Count
  - error: FATAL
  - >=0: HARMLESS
- Count Errors
  - error: FATAL
  - >0: CRITICAL
  - 0: HARMLESS
- Log Levels
  - error: FATAL
  - classification: BLOCKING: FATAL / UNBLOCKING: HARMLESS
  - 10: HARMLESS
  - 20: WARNING

- 30: CRITICAL
- 40: FATAL

- Percentage Low Critical
  - error: FATAL
  - >=20 HARMLESS
  - >=10 WARNING
  - <10: CRITICAL
- Percentage High Critical,
  - error: FATAL
  - ⇐80 HARMLESS
  - ⇐90 WARNING
  - >90 CRITICAL
- Status
  - error: FATAL
  - 1: HARMLESS
  - 0: CRITICAL

Deleting shared evaluations

Shared evaluations can also be deleted if they are no longer needed. The "Delete the selected shared Evaluation" button - first button on the right to the drop-down - is enabled if the selected evaluation is only "shared" in the current situation setup. If it is shared in others as well, the button is disabled.

Switching to other Probe editor using shared evaluations

If a situation is shared an you want to review one of the other probes that use this shared evaluation, this can be done directly from this console.

Simply click on the link that mentions "Cahnges to this shared …" and a drop down will open that list the other probes. Select the probe you wan to switch to.

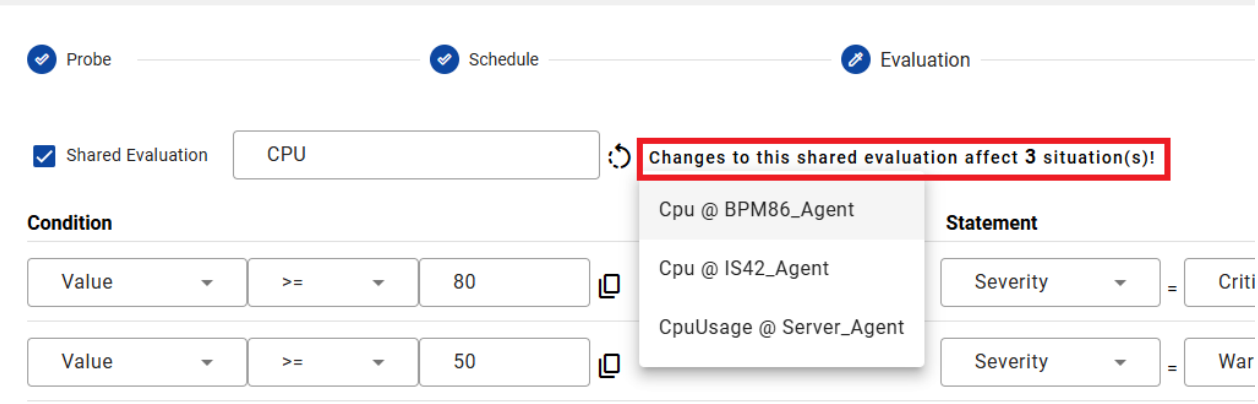

Image of Details View for Probe Shared Evaluation Probe Switch

Tag setup step

By clicking on "Add tag", you can select an already existing tag from the drop down that opens, or you can key in a new tag. Save the new tag with the "Return" key. You can add several tags if you like.

In case of editing a probe, already existing tags are shown.

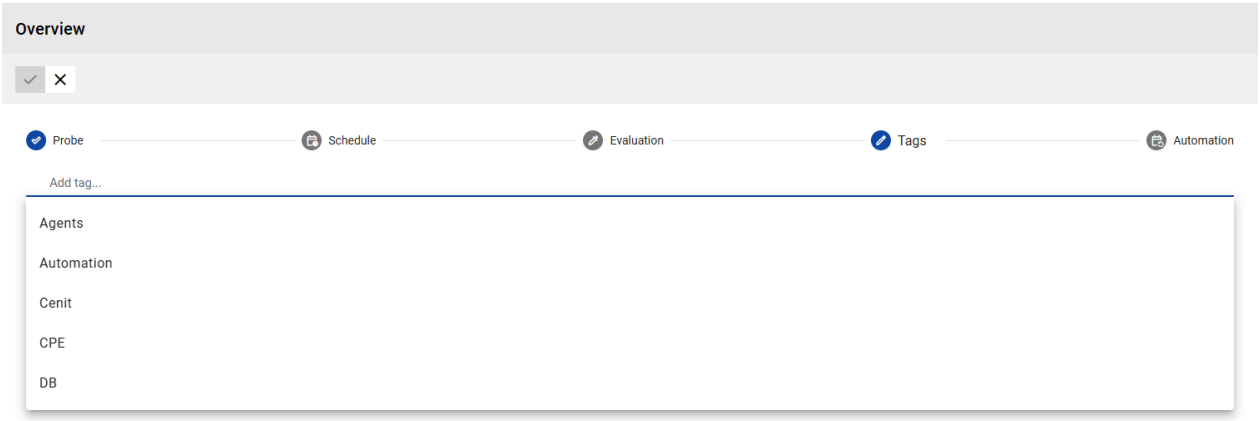

Image of Details View for Probe Tag Setup

Automation setup step

In automation, tasks can be configured based on conditions. Click on "Add task trigger" to add an entry.

Condition

The available conditions are the same as in the evaluation, but it must not use the same settings. Furthermore all matching entries will be processed. Not only the first one.

Mode

Two modes are available, Always and First. Always: Anytime the condition matches the task is triggered. First: Only the first time (on change) the condition matches the task is triggered.

Task

Choose from the available tasks in the drop-down.

Action buttons on the right

- An entry can be copied.
- An entry can be deleted.

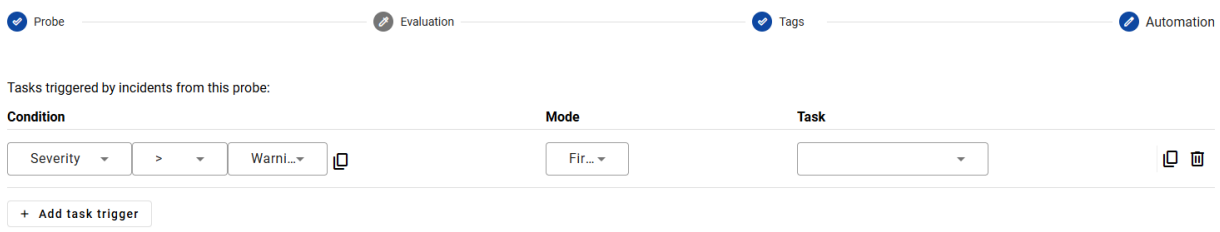

Image of Details View for Probe Automation Setup

User Management

Clicking on the + above the sidebar in the users menu or using the edit functionality for an existing users opens the user editor. Within the editor you can:

- Specify the account name
- Select which role the account should have
- Enter an e-mail address (optional)
- Specify and confirm the password (if the account is internal - otherwise greyed out)

- Give a full name, phone number and room (optional)
- Enable/disable the account
- Select if the account should have the session timeout enabled
- Select if the account is authenticated externally

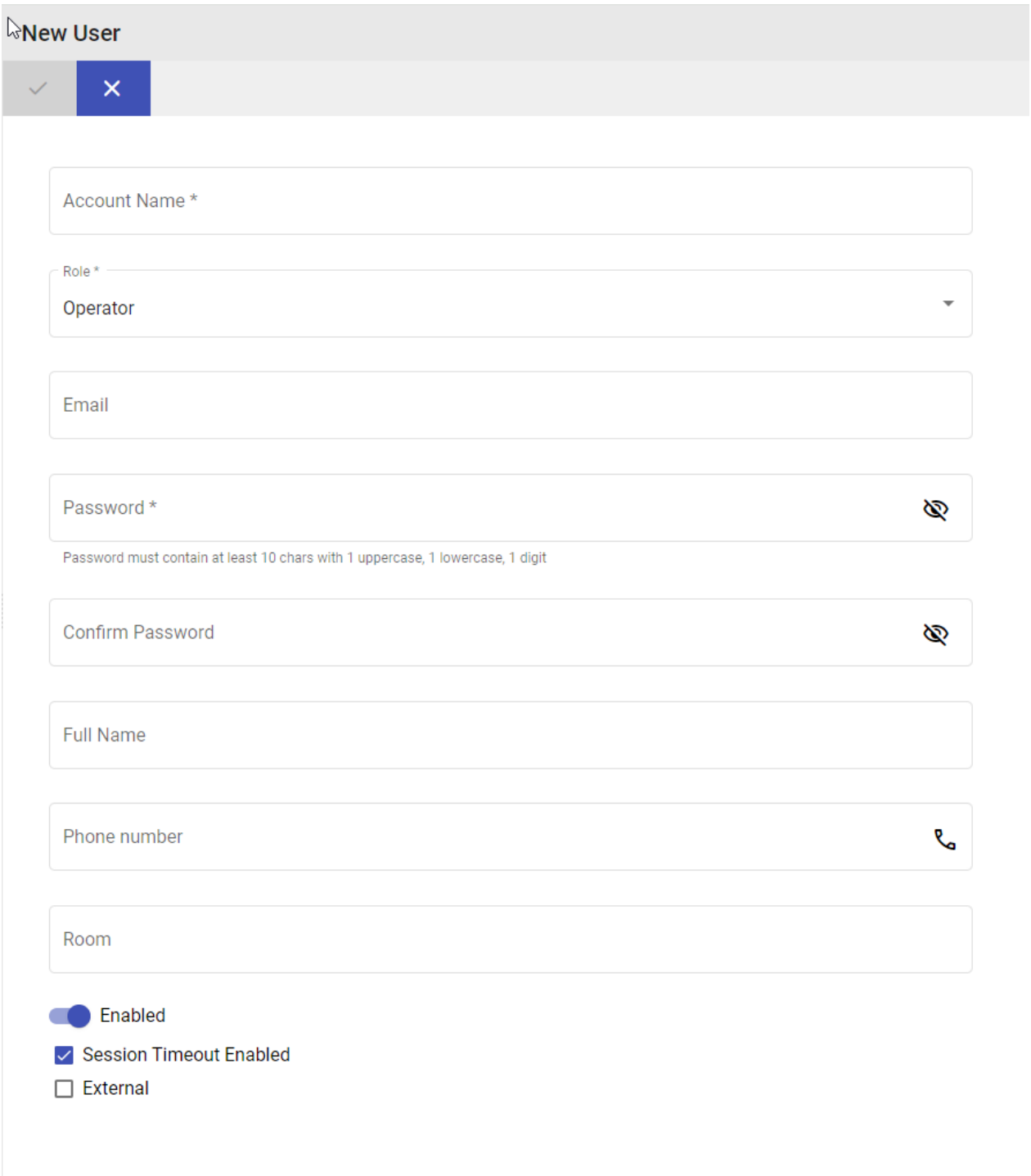

Image of User Editor

Tag Manager

The Tag Manager can be opened by clicking on the word "Tags" next to the tags and filter section in the Overview.

The Tag Manager opens as a pop up in front of the console and looks like this:

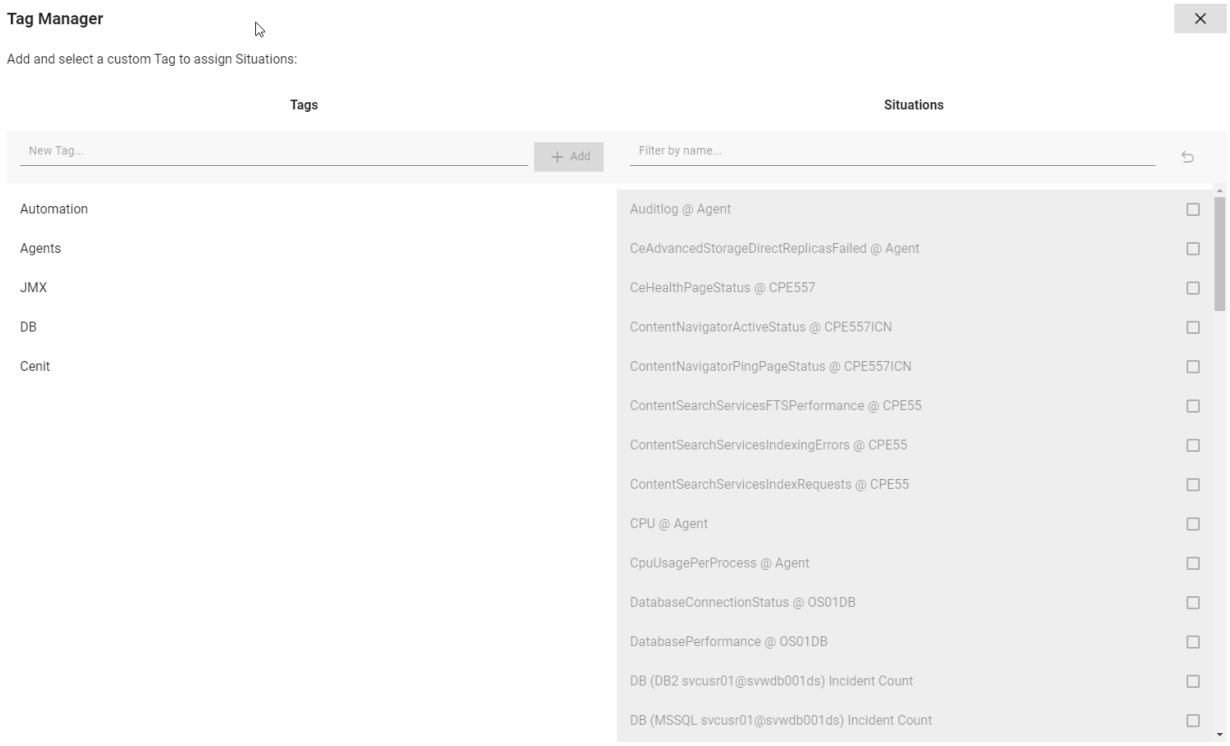

Image of Tag Manager

Adding new tag

Before a tag can be assigned to a situation, it has to be added. Therefore click in the field that says "New Tag…" and enter the tag name. Click on the "+ Add" button afterwards to add the tag to the tag list.

Assigining a tag to a situation

After a tag is created it can be selected in the tag list. Once a tag is selected, the situation list becomes active. Already assigned situations will be shown at the top of the list and the list is sorted in alphabetical order. You can assign new or additional situation by clicking on the checkbox next to the situation. Once clicked, the assignment is directly activated and the situation will also be shown at the top of the list.

Removing a tag

For removing a tag simply remove all assignment. If a tag is not assigned within any situation, it will automatically be deleted when you leave the Tag Manager.

Filtering the situation list

You can filter the situation list by using the text field above the list. Just type the search string in the filter. Only the situation where the string matches will be shown.

Reporting of Backend Errors

In the console you can see if errors in the backend occur or if the backend is not reachable. A banner at the top of the page will appear that lists the error.

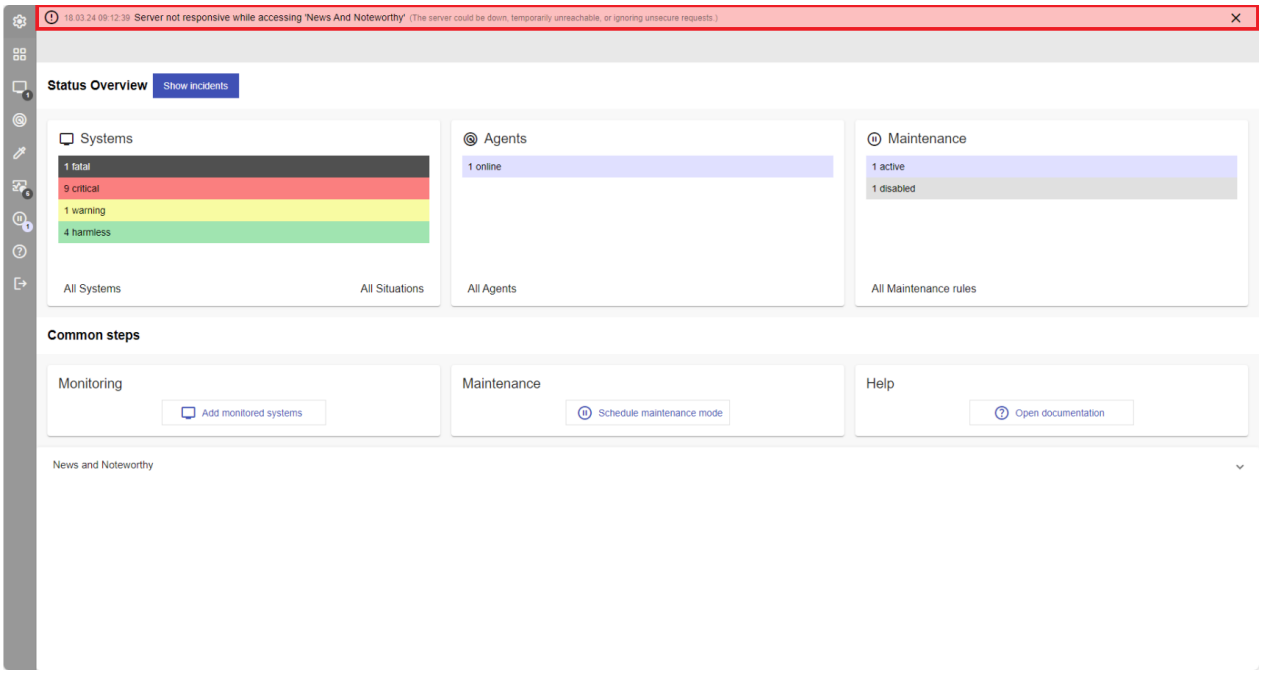

Image of Backend Error

Functions within the console

Creating/Adding an Evaluation Mapping from Sample List

For the evaluation of the incidents a mapping is used in the probe configuration. Sometimes shared mappings are used and sometimes self defined mappings are used. Also pre-defined shared evaluations are available. It is possible that some of the mappings (e.g. the pre-defined shared evaluation named "Log") do not create an incident. In this specific case this is a wished behaviour as the user/admin should create a mapping based on the required log entries only.

To add such mappings to an evaluation a function within the sample list is available. The sample list can be open via the system, probe and agent sidebar entry and selecting the list in the main view.

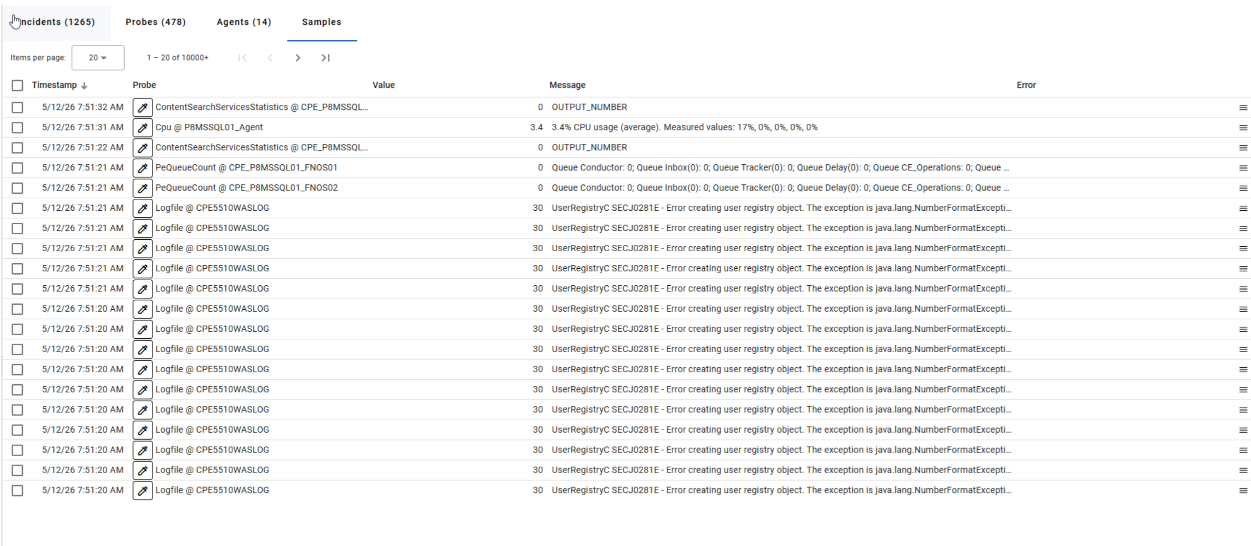

Image of Samples List

In the "hamburger menu button on the right of each list entry you will find a button for adding a new evaluation mapping.

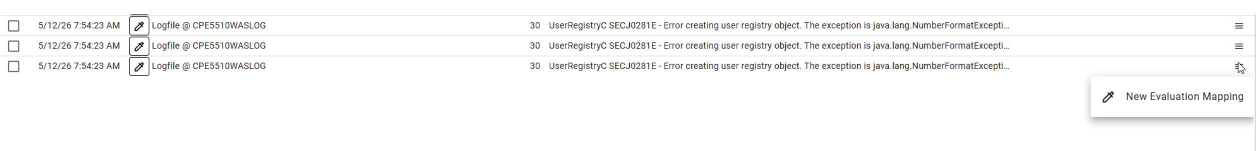

Image of Samples List New Evaluation Mapping

When clicking on the button you will be automatically redirected to the evaluation of the probe configuration that is matched with this sample. Within the evaluation a new entry was created that contains a mapping for "All of" → "Classification", "Value" and "Message" and the severity is set to "HARMLESS". You can now adjust this entry for your requirements and save the new setup afterwards.

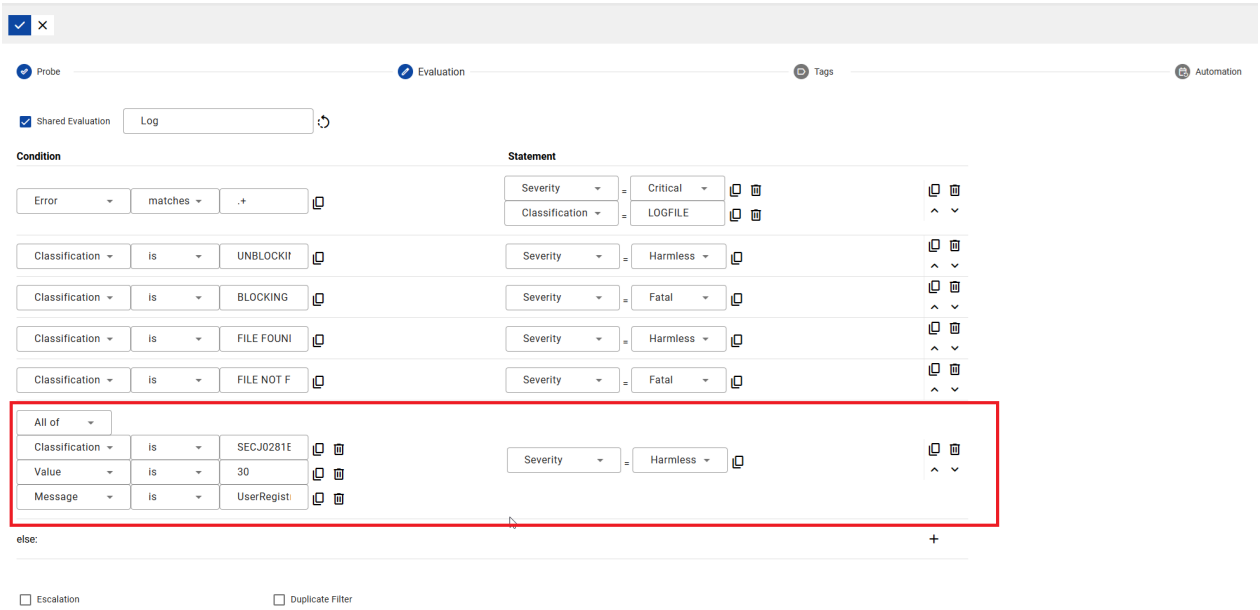

Image of Probe Configuration Added Evaluation

Messages and Error Codes

Table 2. List of possible errorcodes

Source	Formatted LogId	Explanation	Action
LogIdAccess	CDESD6501I or W or E	The user has no permission to execute the requested action.	Please check your permissions or ask your administrator to change them.
	CDESD6502I or W or E	The user has permission to execute the requested action.	Informs about successful authorization.
LogIdAgent	CDESA5501I or W or E	Adding one or more new agents failed.	Check the detailed error message for the specific reason.
	CDESA5502I or W or E	Runtime Fault.	Verify if there are any other previous messages, leading to this exception.
	CDESA5503I or W or E	No Data Available.	Check the input. However, it is not necessarily a mistake.
LogIdArgs	CDESC2501I or W or E	Incorrect or missing argument.	This should not happen in production code. Search the log for a hint what went wrong, but it is possible, there is no such log entry.
LogIdConfig	CDESD2001I or W or E	Invalid configuration was provided.	Please check the product configuration.
	CDESD2002I or W or E	Reading configuration was successful.	Informs about successful configuration import/loading.
	CDESD2003I or W or E	Reading configuration failed.	Please check the product installation.
	CDESD2004I or W or E	Saving configuration was successful.	Informs about successful configuration export/saving.
	CDESD2005I or W or E	Saving configuration was failed.	Please check the product installation.
	CDESD2006I or W or E	A configuration could not be removed.	Verify if the format of the configuration was correct and the configuration which should be removed exists.
	CDESD2007I or W or E	A property was supposed to be set, but failed.	Please check the product's configuration.
	CDESD2008I or W or E	A property was tried to be loaded, but failed due to unknown reasons.	Please check the product's configuration.
	CDESD2009I or W or E	A problem occured while trying to send a email.	Please make sure the configuration is valid.
	CDESD2010I or W or E	Configuration was not found.	Please check the product's installation.
LogIdDb	CDESD6001I or W or E	Connection failed.	Please check your DB configuration.

Source	Formatted LogId	Explanation	Action
	CDESD6002I or W or E	Updating the database failed.	Probably a problem occurred by modifying the request.
	CDESD6003I or W or E	An error occured while trying to write to the database.	Please make sure the database is available and check it's configuration.
	CDESD6004I or W or E	An error occured while trying to read from the database.	Please make sure that the database is available and check its configuration.
	CDESD6005I or W or E	There was a locking issue, while trying to perform a transaction.	Verify if another process locks the specific database resource and free it.
	CDESD6006I or W or E	A previous transaction failed. A database rollback will be performed.	Check previous log messages to find out the reason of the rollback.
	CDESD6007I or W or E	A relation between two or more database items did not exist.	Check the request and verify if the requested items hava a relation to each other, via your database management console.
	CDESD6008I or W or E	A database action was about to be performed, but a required property of the query was not set.	Check the query and verify which item was missing.
	CDESD6009I or W or E	An item was added / moved / updated. This message informs the user about the performed action.	Nothing to be done.
	CDESD6010I or W or E	There was an exception, related to a specific JPA component, whose reason was not further specified.	Read the print of the stack trace in the log file to get further information.
	CDESD6011I or W or E	An error occured while trying to remove an item from the database.	Please make sure the database is available and check it's configuration.
LogIdIo	CDESC3501I or W or E	File already exists.	Change the name of the file being created or delete the file that is already there.
	CDESC3502I or W or E	A file (or directory) cannot be created/removed.	Verify if the file or directory which was about to be created, exists and can be accessed.
	CDESC3503I or W or E	A file (or directory) is of an invalid type or {@code null}.	Please check that the file or directory is valid.
	CDESC3504I or W or E	Attempting to open a file or resource failed.	Please check that the file or resource is in the proper directory and can be accessed.
	CDESC3505I or W or E	Attempting to delete a file or resource failed.	Please check that the specified file is not in use.
	CDESC3506I or W or E	Attempting to close a file or resource failed.	Please check that the specified file is not in use and your current OS user has the rights to access the file.

Source	Formatted LogId	Explanation	Action
	CDESC3507I or W or E	Attempting to write a file or resource failed.	Please check that the specified file is not in use and your current OS user has the rights to access the file.
	CDESC3508I or W or E	Attempting to read a file or resource failed.	Please check that the specified file is not in use and your current OS user has the rights to access the file.
	CDESC3509I or W or E	Could not reach the destination via network.	Please make sure that networking is configured and the host is reachable.
	CDESC3510I or W or E	Character encoding problems.	Probably the character encoding is not supported.
	CDESC3511I or W or E	General I/O Error.	There can be several reasons why this I/O error occurred, please contact support.
	CDESC3512I or W or E	A connection to the requested system could not be established.	Please make sure that you have entered the correct connection parameters. Refer to the documentation of the system, you want to connect to.
	CDESC3513I or W or E	A connection was successfully established.	Informational message about a successful connection.
	CDESC3514I or W or E	A connection was or is about to be closed.	Informational message about a connection closing process.
	CDESC3515I or W or E	A connection was unintendedly lost.	The connection to the system was unexpectedly lost. Verify if the system is available.
LogIdOsgi	CDESC4001I or W or E	Attempting to look up the service failed.	Open the OSGi console to check if the service is available.
	CDESC4002I or W or E	A service could not be started.	Please check the log message for missing dependencies or runtime exceptions.
	CDESC4003I or W or E	A service could not be reinitialized.	Verify if dependent services are available or if another required component is missing.
LogIdReflection	CDESC4501I or W or E	A requested method was not found via Java reflection.	Please change method name configuration if possible.
	CDESC4502I or W or E	The security manager denied the execution.	Please configure the security manager appropriately.
	CDESC4503I or W or E	A requested class was not found.	Please configure the classpath appropriately and check if the JAR files have the latest version.
	CDESC4504I or W or E	The internal object could not be copied.	Please contact the support.
LogIdSecurity	CDESC7001I or W or E	The user does not exists	Create user.

Source	Formatted LogId	Explanation	Action
	CDESC7002I or W or E	The user account is deactivated	Activate the user account.
	CDESC7003I or W or E	The user account is locked	Unlock the user account.
	CDESC7004I or W or E	User account was locked because the maximum failed login attempt of was reached.	Unlock the user account.
LogIdTask	CDESC6001I or W or E	A task could not be executed successfully	Depending on the task's logic this could be a technical or a user input issue.
LogIdThread	CDESC5001I or W or E	An error occurred while trying to access another thread.	Please restart the service and try again. If the error persists, please contact support.
	CDESC5002I or W or E	A thread was interrupted.	Please restart the service and try again. If the error persists, please contact support.
	CDESC5003I or W or E	An unspecified runtime exception occurred.	Verify if there are any other previous messages, leading to this exception.
LogIdValidation	CDESM3001I or W or E	A validation check succeeded.	Informal message; nothing else is to do.
	CDESM3002I or W or E	A validation check did not succeed, but this is valid.	Informal message; nothing else is to do.
	CDESM3003I or W or E	A validation check did not succeed, but was expected to succeed.	Informal message; nothing else is to do.
	CDESM3004I or W or E	A URL which was about to be parsed, did not have the correct format.	Verify in the log file, what the URL looked like and enter the URL in the correct format.
	CDESM3005I or W or E	A String object did not have the correct format.	Verify in the log file, what the string looked like and enter the String in the correct format.
	CDESM3006I or W or E	A value which was supposed to be created, already exists.	Decide whether to override the already existing value or to leave it.
	CDESM3007I or W or E	A value which was supposed to be from a specific datatype, had a different datatype.	This is an internal issue and should be reported to the distributor of the software.
	CDESM3008I or W or E	A numeric value was supposed to be transformed to a string, but had a incorrect format.	Verify if the given value had a valid number format.

Accessibility conform Controls

ESM can be controlled only with the keyboard, no mouse is needed. The following shows the list of shortcuts and control keys:

- The "Tab" key can be used to browse through the different available entries inside the console.
- Arrow keys, page up and down or pos1 and end are used to select an entry within the favored grid (e.g. a list or line). In nested lists the list can only be browsed using arrow up and down. Page up and down and pos1 and end will not work.
- Use space or ctrl + space to select or deselect an entry in the list or the line.
- Enter is the same as double-click on a selected entry (mostly this opens an editor).
- Alt + c means cancel within an editor (valid for Chromium-based browsers).

Encryption mechanism in ESM

ESM uses JAVA based encryption mechanisms. These mechanisms are FIPS 140-2 conform.

Appendix A: Copyright notice

IBM Enterprise Content Management System Monitor

Appendix B: Notices

This information was developed for products and services offered in the U.S.A.

IBM® may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Appendix C: Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others

Product Number: 5724-R91

Printed in USA

SC27-9245-09