SIEMENS

MindSphere

MindConnect IoT Extension

System Manual

07/2021
V1801.Jul/2021.1

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

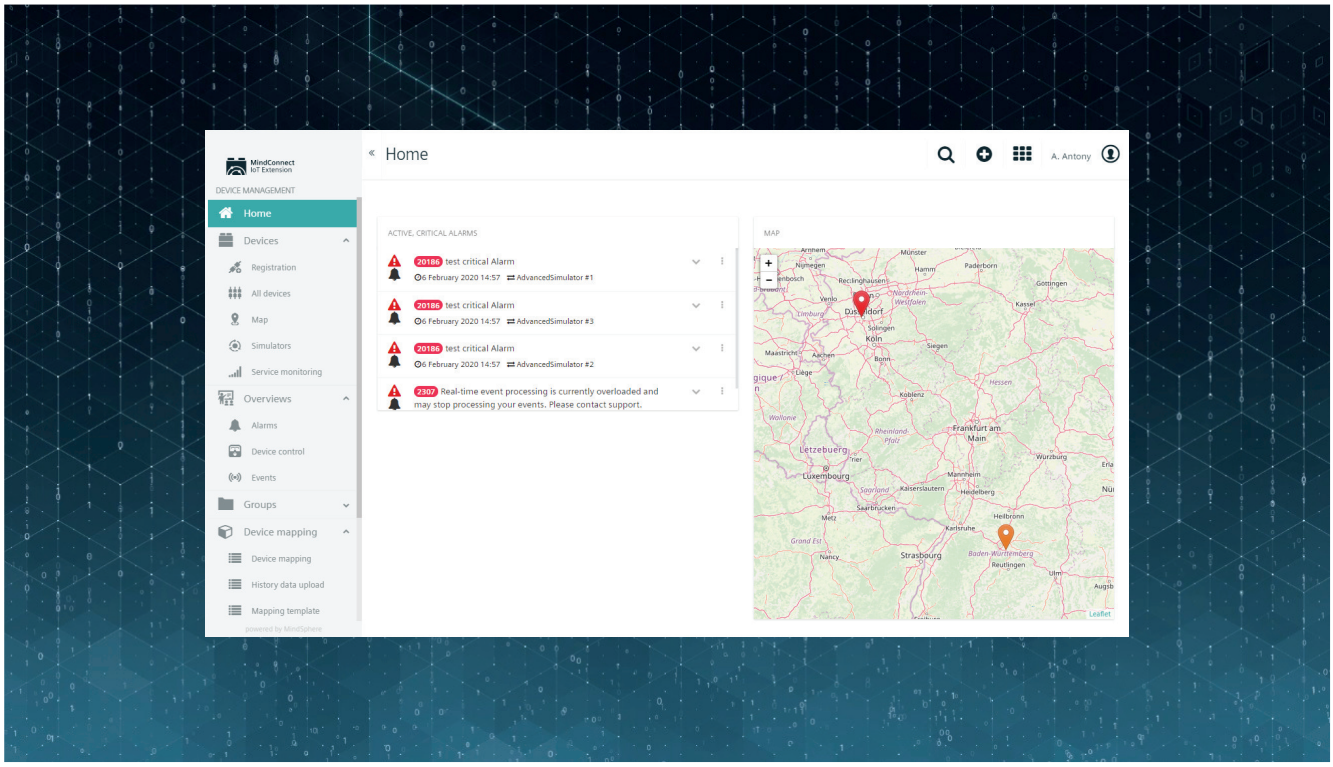
We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

V1801.Jul/2021.1
Ⓟ 07/2021 Subject to change

Table of contents

MindConnect IoT Extension is part of MindSphere, the industrial IoT platform from Siemens. MindConnect IoT Extension enables you to connect applications to MindSphere and to use software agents.



Document history

1

Document version	Product version	Date	Changes	Link
V1801.Jul/2021.1	1006.6.24	2021-7-10	Minor updates throughout the document	-
V1801.Oct/2020.1	1006.6.6	2020-10-10	Added Chapter "Firewall Settings"	Firewall Settings (Page 209)
V1801.Sep/2020.1	1006.0.9	2020-09-09	Removed "Apama" references	Managing applications (Page 31)
V1801.Aug/2020.1	1005.7.15	2020-08-08	Updated the offering information	Introduction to MindSphere IoT Extension (Page 9)
V1801.Jul/2020.1	1005.7.5	2020-07-11	Updated the Alarm mapping topic	Device Mapping (Page 91)
V1801.Apr/2020.1	1005.7.5	2020-04-18	Removed OPC UA (optional service) information	Cloud Fieldbus (Page 128)
			Removed all optional services information but Cloud Remote Access	Cloud Remote Access (Page 203)
V1801.Feb/2020.1	1005.0.7	2020-02-19	Updated screenshots	Device to asset mapping (Page 91) Device credentials (Page 127) Cockpit (Page 139)
			Updated text	AUTOHOTSPOT
V1801.Jan/2020.1	1004.6.18	2020-01-07	Added event mapping and alarm mapping information	Device Mapping (Page 91)
			Removed "LWM2M post operations" service	Device types (Page 111)
			Updated screenshots across the document	

Document version	Product version	Date	Changes	Link
V1801.Dec/2019.1		2019-12-05	Removed Chapter "Quick help".	
			Updated screenshots across the document	
			Removed "Upload micoservice" functionality	Cloud Fieldbus (Page 128)
			Added "Configure columns"	Viewing devices (Page 56)
			Replaced "Device database" with "Device protocols"	Device protocols (Page 117)
			Added event-data and metadata mappings information	Device Mapping (Page 91)
			Added "Asset quota"	Asset quota (Page 110)
V1801.Nov/2019.1		2019-11-07	Moved section "Cloud Fieldbus" from chapter "Optional Services" to "Device Management"	Cloud Fieldbus (Page 128)
			Added section "OPCUA Java gateway" in chapter "Optional Services"	OPCUA Java gateway
V1801.Mar/2019.1		2019-03-01	Notes on Subtenant use	User roles in "Visual Explorer"
			Note on data rate limitation Added information on folder structure	Creating a new datasource
V1801.CW.EU1.K1217		2018-12-18	Updated screenshots	
			Added note in chapter "Creating a new datasource"	Choose update mechanism
			Added "Support" in chapter "Further Help"	Further Help

Introduction to MindSphere IoT Extension 2

MindConnect IoT Extension gives you very fast visibility and control over your remote assets, be these houses, cars, machines or any other assets that you need to manage.

Features of MindConnect IoT Extension

MindConnect IoT Extension provides:

- Certified hardware kits and software libraries which can be used to bring your remote assets into the cloud.
- Device management, data visualization and remote control functionalities through the web.
- Rapid customization of the above through MindConnect IoT Extension Event Language rules and MindConnect IoT Extension applications.
- APIs for extending the existing functionalities or interfacing MindConnect IoT Extension with your other IT services such as ERP or CRM systems. MindConnect IoT Extension can also host your HTML5 applications.

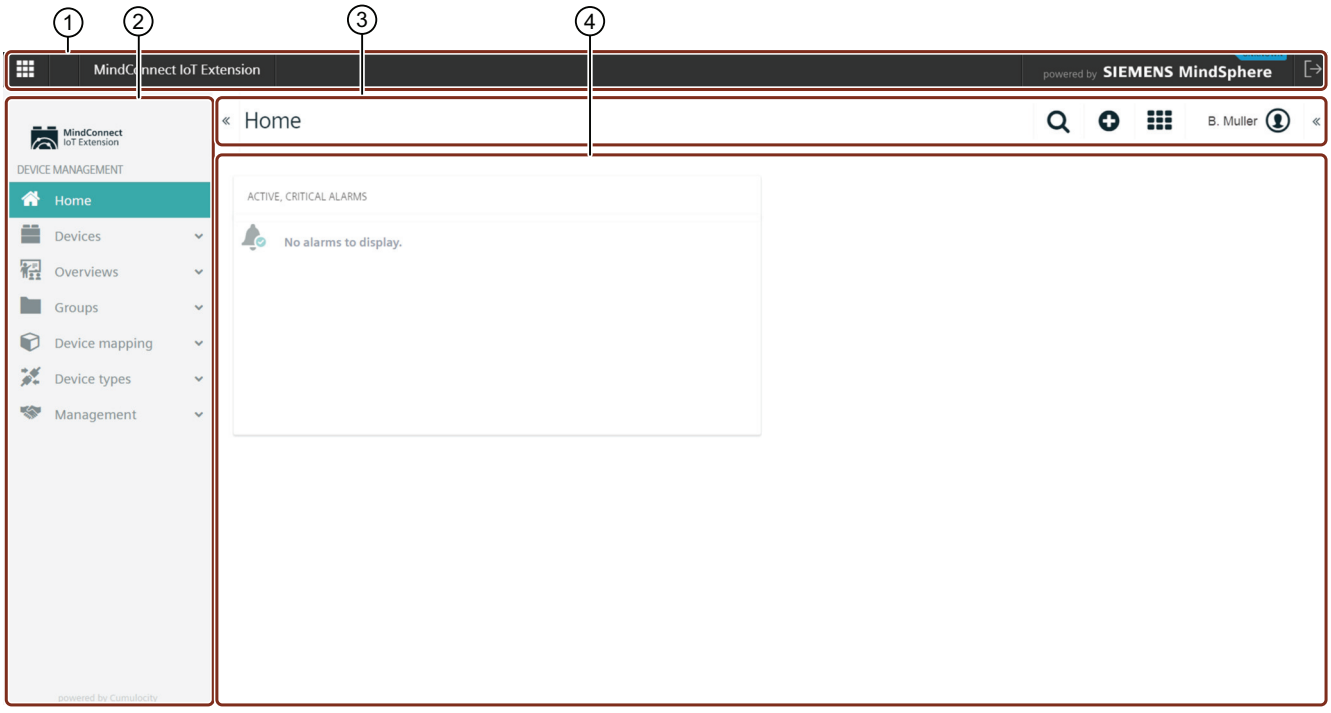
The features are provided through a cloud-based subscription service making the creation of Internet of Things (IoT) solutions with MindConnect IoT Extension fundamentally different from bespoke development and RAD (rapid application development). Once the application is bought via MindSphere store, You can start with a large amount of existing functionality. You do not need to worry about IT infrastructure (hosting, networking, security, storage and backup) and IT management (all software is available to your users). MindConnect IoT Extension also works with any network architecture, but is specifically designed to work out of the box with mobile networks.

For more information about MindConnect IoT Extension, see "https://cumulocity.com/guides/about-doc/intro-documentation/".

User Interface of MindConnect IoT Extension

3

Start screen



① MindSphere OS Bar
② Tool navigation window
③ Menu options
④ Work area

Home page navigator

The main navigator is located just below the MindSphere OS Bar as depicted in ③ in the above mentioned legend table.

The main navigation menu has the following options:

- Administration: This section enables account administrators to manage their users, roles, tenants, applications and business rules and lets them configure a number of settings for their account.
- Cockpit: Cockpit application is a dashboard which shows data for the general tenant.
- Device management: You can connect devices to your IoT Extension account either manually or by bulk-registration.

Administration

4

4.1 Overview

The "Administration" application enables account administrators to manage their users, roles, tenants, applications and business rules and lets them configure a number of settings for their account.

Overview

The following sections will walk you through all functionalities of the "Administration" application in detail. For your convenience find an overview on the content of this document below.

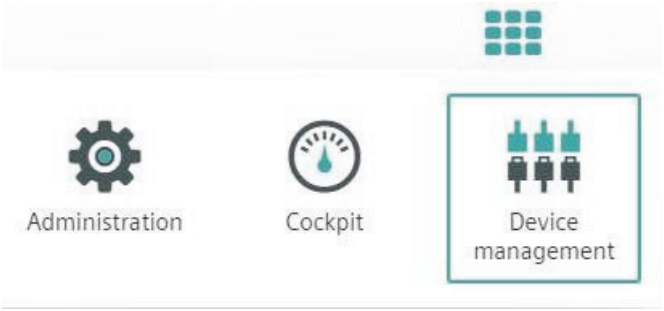
Section	Content
Home Screen (Page 13)	Providing information on your capacity usage and subscribed applications.
Managing Users (Page 15)	How to create users, edit, disable or delete them.
Managing Permissions (Page 19)	How to create and edit global roles and inventory roles, how to assign them to users, and how to grant application access.
Managing own applications (Page 31)	How to manage and configure own applications in your IoT Extension account.
Applying business rules	How to set up real-time event processing scripts and reprioritize alarms by alarm mappings.
Changing settings (Page 45)	How to change account settings like application settings or password policy and how to manage the properties library.
Managing data retention (Page 42)	How to manage and configure retention rules for your data and how to manage stored files in the file repository.

4.2 Home screen

You need to navigate from the MindConnect IoT Extension home page to access the MindConnect IoT Extension administrative page. The procedure is described below in the following section.

Navigating to administrative page

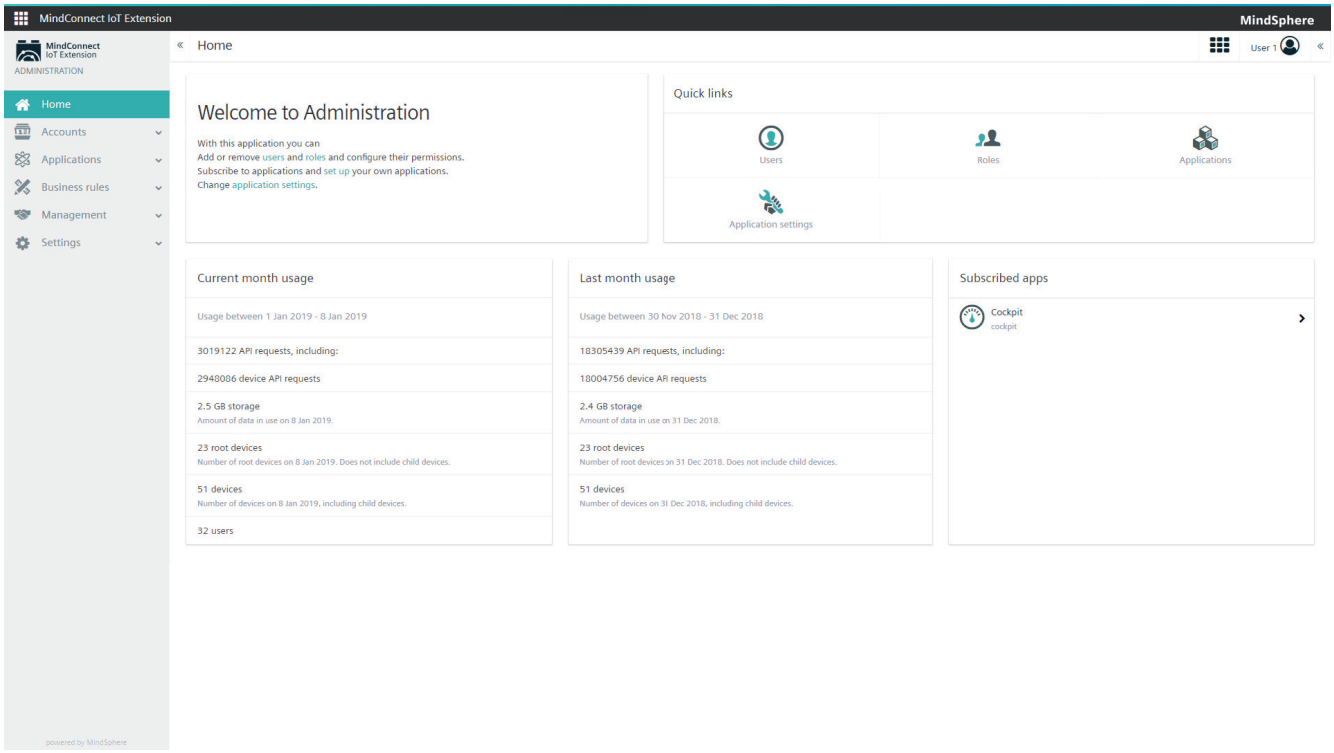
1. Click the button to navigate to the administrative page.
2. Click "Administration" from the popped up panel.



You will be redirected to the home screen of the "Administration" application.

Administration home screen UI

The "Administration" screen opens on clicking the "Home" button.



The "Home" screen of the "Administration" application provides

- A welcome message
- Quick links to the main parts of the "Administration" application

- Data consumption information for the current and for the last month
- The optional applications you are subscribed to

Dashboard information

The "Administration" home page shows information on the dashboard. These include the following:

- API requests: The total number of API requests, counting whenever some function in IoT Extension is invoked, regardless of whether the function is invoked from a device (for example, sending a measurement) or from an application (for example, viewing the list of devices).
- Device API requests: Counting only when the API is called from a device (for example, sending a measurement).
- Storage: The total amount of data stored in your account. This amount can be changed by retention policies and by the amount and size of stored files.
- Storage quota: If the storage limit per device is set, the user is restricted to a maximum data usage.
- Root devices: The number of root devices connected to your account, excluding child devices.
- Devices: The total number of devices connected to your account. This is the sum of the devices listed in the "All devices" page of the "Device Management" application and their direct and indirect child devices.
- Users: The sum of all users configured in this account - both active and inactive.

4.3 Managing users

The user management functionality allows you to manage the users within your tenant and provides the following options:

- Creating users
- Assigning user names and set passwords
- Storing user details
- Choosing basic login options

Note

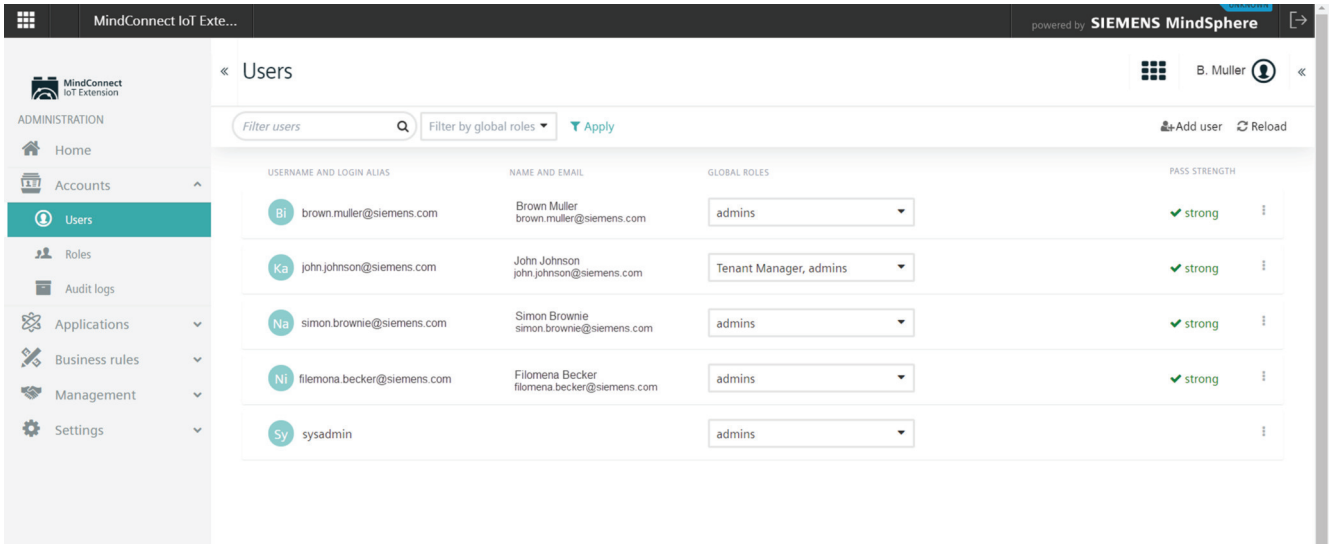
The user needs to have a role with the user management permission ADMIN or CREATE to be able to do so.

Note

MindConnect IoT Extension has a Single Sign-On feature. Users should be controlled from MindSphere Settings. For further and additional roles and permissions, you can use MindConnect IoT Extension "Users" and "Roles" tabs in the Account menu in the navigator.

Viewing users

To view all users in your tenant, click "Users" in the Account menu in the navigator.



A user list will be displayed, providing the following information for each user:

- The user name that is used to access the tenant.
- The name and email of the user, if set.
- The global roles assigned to the user.
- The strength of the password set for the user.

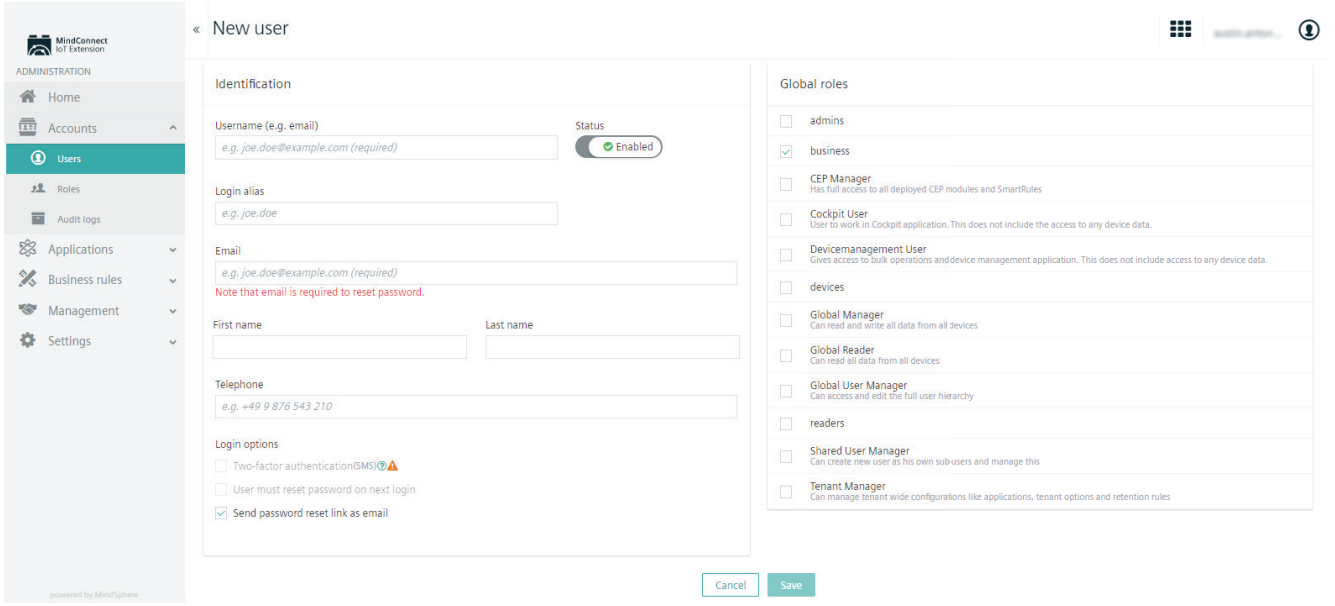
To filter the list, you can use the search field at the left of the top menu bar.

Moreover you can filter by global roles. Select the desired roles from the dropdown list and click "Apply" to limit the users shown in the list to users with the selected roles.

Initially, the User page only shows the top-level users. To see all users in your account at once, click "Expand all" at the right of the top bar. This will expand all top-level users, showing their sub-users. Click "Collapse all" to just show the top-level users again. For details on user hierarchies, refer to Managing user hierarchies.

Creating users

To add a user to your tenant, click "Add user" at the right of the top menu bar.



At the left of the "New user" window provide the following information to identify the user:

Field	Description
Username	Serves as a user ID to identify the user at the system. Note that the username cannot be changed once the user has been created. This field is mandatory.
Login alias	In addition to the user name, an optional alias can be provided to be used to log on. Other then the username, this alias may be changed if required.
Active	Enable/disable the user account here. If the user account is disabled the user cannot login.
E-mail	A valid email address. This is required to enable the user to reset the password. This field is mandatory.
First name	First name of the user. When the user is logged in, this name appears at the right of the top bar on the User button.
Last name	Last name of the user.
Telephone	A valid phone number. The phone number is required if the user is configured to use two-factor authentication.

Select the login options for the user.

- If you select "User must reset the password on next login" you need to provide a password which the user needs to reset on the next login.
  Enter a password and confirm it. While entering the password, the strength of the password will be shown.
- If you select Send password reset link as e-mail, the user will receive an email message with a link to set a password. The email will be sent to the email address configured above.

On the right of the page, select the global roles for the user. Details on global roles are described in Managing Permissions (Page 19).

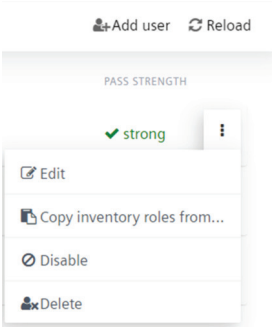
Click "Save" to create the user.

Note

By default, manually created users always have the "Own_User_Management" permissions set to active.

Modifying users

Click the menu icon at the right of a user entry to open a context menu which provides further functionalities.



Note

You need a role with user management permission to perform these options.

1. Click "Edit" to edit an existing user. All fields except "Username" and "Send password reset link as e-mail" can be modified. For details an each field, refer to "Creating users". Click "Change password" to change the password. After editing, click "Save" to apply your settings.
2. To copy roles, click "Copy inventory roles" from another user. In the upcoming window, select a user from the list and click "Copy". At the top you can select if you want to merge the roles with the existing user roles (the default) or if you want to replace the existing user roles.
3. Click "Delegate" to delegate your user hierarchies and permissions to a user, or click "Undelegate" to remove a delegation.
4. Click "Disable" to disable an active user, or click "Enable" to enable a user that has been disabled.
5. Click "Delete" to delete a user.

4.4 Managing permissions

Permissions define what a user is allowed to do in IoT Extension applications. To manage permissions more easily, they are grouped in so-called "roles". Every user can be associated with a number of roles, adding up permissions of the user.

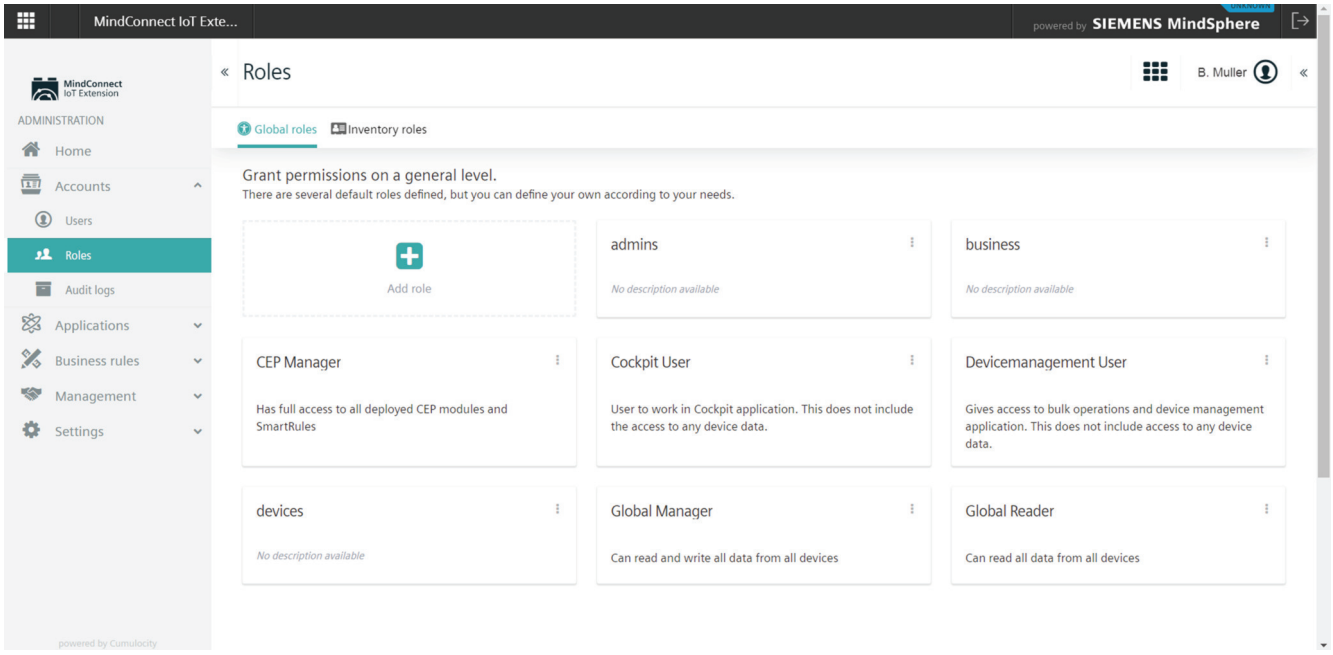
The following types of roles can be associated with users:

- "Global roles": Contain permissions that apply to all data within a tenant.
- "Inventory roles": Contain permissions that apply to groups of devices.
- "Application access": Enables a user to use an application.

Viewing global roles

Click "Roles" in the Account menu to display a list of configured roles.

In the Global roles tab you can find the roles which grant permissions on a general level. There are several default global roles defined, but you can define your own according to your needs.



The roles "admins" and "devices" have a special status:

Role	Description
admin	All permissions are enabled. The initial administrator, the first user created in a tenant, has this role.
devices	Typical permission setup for devices. After registration, a device automatically has this role. Edit this role if your devices require less or more permissions, or assign other roles to your devices.

Furthermore, the following roles are configured as a starting point:

Role	Description
CEP Manager	Can access all smart rules and event processing rules.
Cockpit User	Can access the "Cockpit" application. In addition, you should add a role providing access to devices.
Device management User	Can access the "Device Management" application. The user will be able to use the simulator and to run bulk operations. In addition, you should add a role providing access to devices.
Global Manager	Can read and write all devices.
Global Reader	Can read all devices.
Global User Manager	Can manage all users.
Shared User Manager	Can manage sub-users. The subscription plan needs to include user hierarchies to be able to manage sub-users.
Tenant Manager	Can manage tenant-wide settings, such as own applications, data brokerage, data retention, options and tenant statistics.

You may see the following legacy roles:

Role	Description
business	Can access all devices and their data but has no management permission in the tenant.
readers	Can read all data (including users, in contrast to "Global Readers").

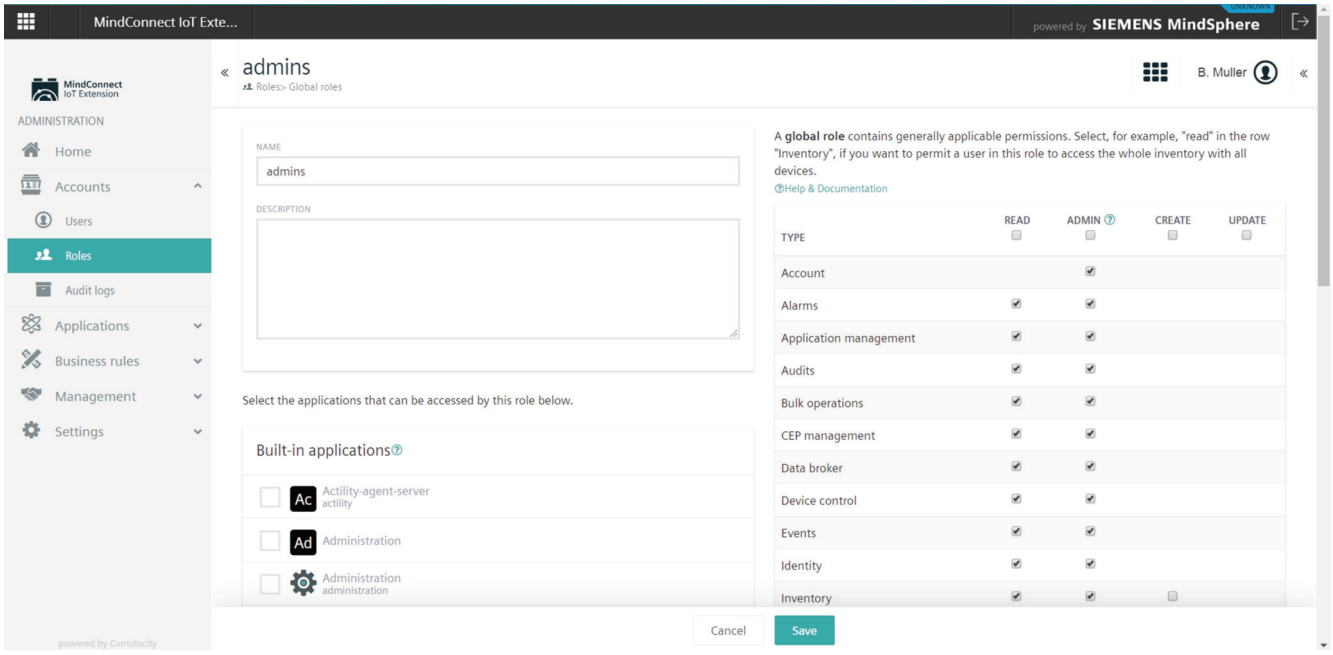
Creating and editing global roles

You can edit the existing global roles and you can create new global roles to meet your particular needs.

To edit a global role, simply click on its card. To create a new global role, click "Add Role" in the Global roles tab.

In the role page you will see a list of permission types on the left and a list of applications to be accessed on the right.

The following screenshot shows the settings for the "admins" role.



Permission levels

For each type, you can select the following permission levels:

- "Read": Read the specified data.
- "Create": Create new data like users and inventory data and edit users within your hierarchy.
- "Update": Modify and delete the specified data (not including "Read").
- "Admin": Create, update or delete the specified data.

Note

"Create" permissions are related to the concept of ownership in IoT Extension. If you have created an object, you are the owner of it and can manage it without requiring any further permissions. For example, if you have "Create" permission for "Inventory", you can create devices and groups, and fully manage these devices and groups. You cannot manage any devices or groups that you did not create yourself, unless you also have the "Change" permission or an additional inventory role (see below). This concept helps to assign minimal permissions to devices. It also enables you to limit user management permissions to sub-users, if you subscribed to user hierarchies.

Select the checkbox at the top of a column to set the respective level to all permission types.

Permission categories

The following permission categories are available by default:

Category	Description
Alarms	View or edit alarms for devices.
Application management	View or edit the applications available in this account.
Audits	View or create audit logs for devices.
Bulk operations	View or create bulk operations.
CEP management	View or edit CEP rules.
Data broker	Send data to other tenants or receive data from other tenants.
Device control	View or edit commands for devices resp. send commands to devices. Also used for device registration.
Events	View or create events for devices.
Identity	View or edit identifiers for devices.
Inventory	View or edit inventory data.
Measurements	View or create measurements for devices.
Option management	View or edit account options such as password policies.
Retention rules	View or edit retention rules.
Simulator	Configure simulated devices.
Tenant management	View, create, edit or delete subtenants.
Tenant statistics	View the usage data for this account, as shown on the Home screen of the Administration application.
User management	View or edit users, user groups and permissions.
Own user management	View or edit your own user.

There may be additional permissions visible depending on the features in your subscription plan. These are documented along with the respective feature.

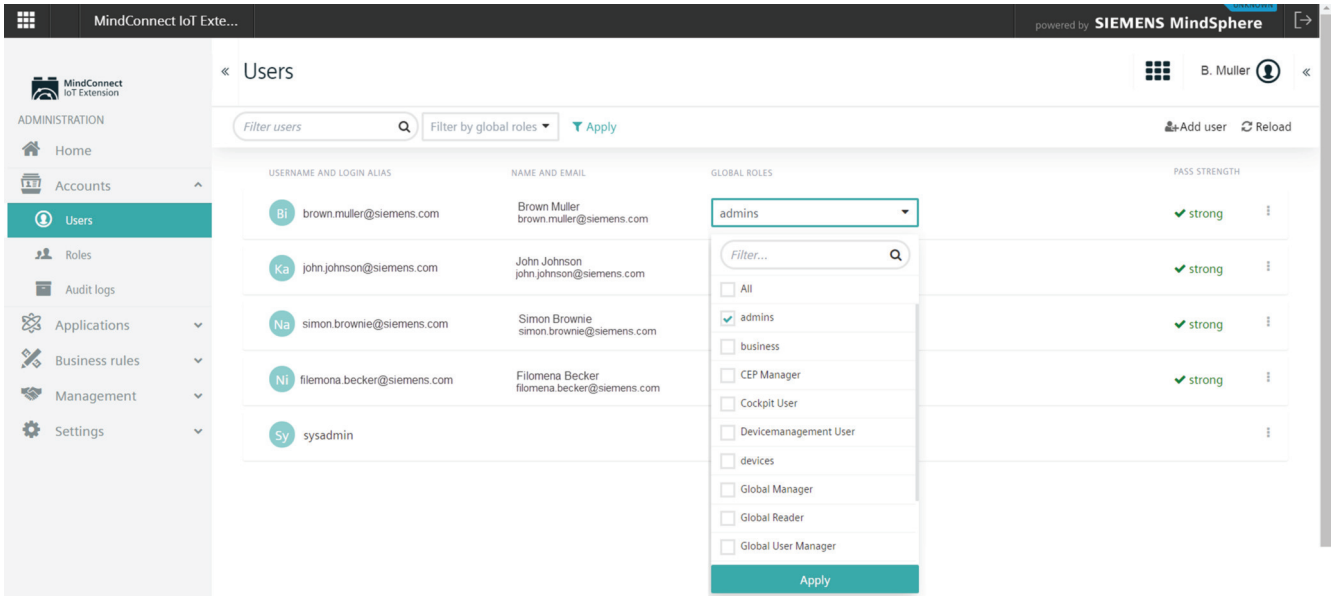
Note

When new features with new permissions are added to IoT Extension, these are not automatically added to existing roles. If you notice that you cannot use a new feature that was recently announced, check your permissions.

Assigning global roles to users

You can assign global roles to users either directly in the user list, or by opening the page for a particular user and adding them there.

In the user list, click the "Global roles" column of a particular user to open a list of global roles. Select or clear the respective checkboxes and click "Apply" to save your settings.

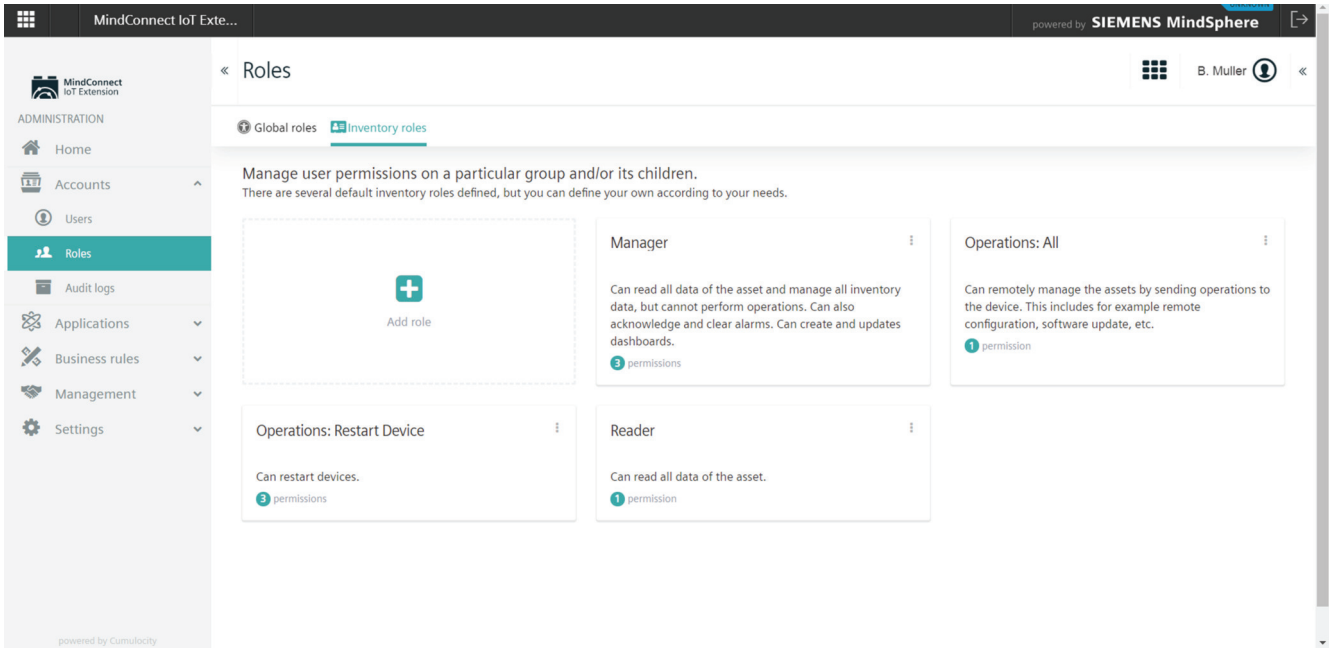


Alternatively, click on a user in the list to open its details. Select or clear the checkboxes for the relevant global roles at the right and click "Save" at the bottom of the page to save your settings.

Viewing inventory roles

Inventory roles contain permissions that you can assign to groups of devices. For example, an inventory role can contain the permission to restart a device. You can assign this inventory role to a group of devices "Region North" and to a user "smith". The result is that the user "smith" can restart all devices that are in the group "Region North" or any of its subgroups.

To view the currently configured inventory roles, click "Roles" in the Account menu and switch to the Inventory roles tab.



In the Inventory roles tab you can manage user permissions for particular groups and/or its children. There are several default inventory roles defined, but you can define your own according to your needs.

The following default inventory roles are available in new tenants as a starting point:

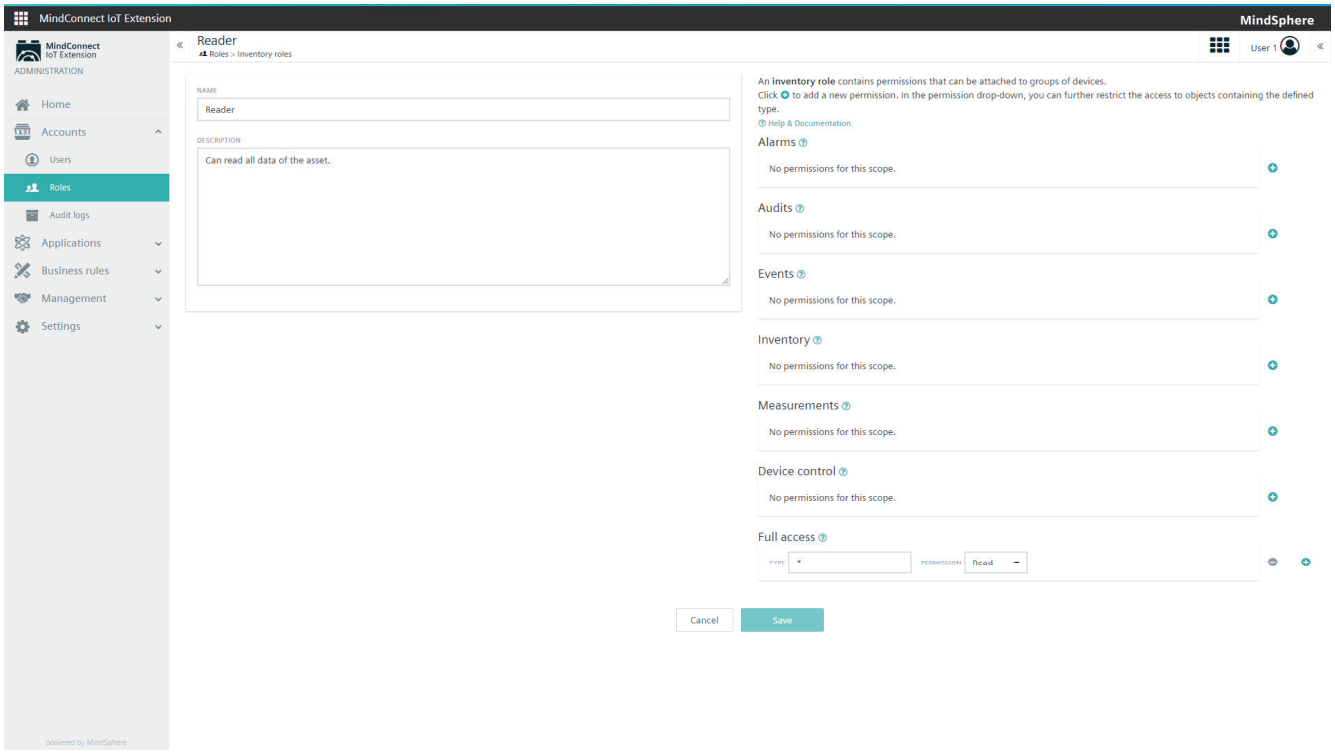
Role	Description
Manager	Can read all data of a group but cannot perform operations. In addition, can manage inventory data (including dashboards) and alarms.
Operations: All	Can send operations to devices in a group (e.g. software updates, remote configurations).
Operations: Restart Device	Can restart devices in a group.
Reader	Can read all data of a group.

Creating and editing inventory roles

You can edit the existing inventory roles and you can create new inventory roles to meet your particular needs.

To edit an inventory role, simply click on its card. To create a new inventory role, click "Add Role" in the Inventory roles tab.

At the top of the page you can edit the name of the inventory role. Click on the name, edit it and click the green checkmark to save your edits.



Permissions are grouped into the following categories:

Category	Description
Alarms	Permissions related to working with alarms from devices.
Audits	Permissions related to audit logs.
Events	Permissions related to working with events from devices.
Inventory	Permissions for viewing and editing devices.
Measurements	Permissions related to measurements.
Device control	Permissions to remote control devices.
Full access	Complete access to the associated devices, mainly to simplify configuration.

Note

Service providers will see an additional permission "Support" in their "management" tenant. This permission lets users of the service provider give support to their customer's users. See "Supporting users in other tenants" below.

Add a permission to the role by clicking the plus icon next to the desired category.

In the "Type" field, specify a type to further restrict the type of data that this permission applies to.

For example, assume that your device sends measurements related to device management, such as "c8y_SignalStrength", and actual production measurements. You want a user to only see the device management measurements. In this case, enter "c8y_SignalStrength" as type.

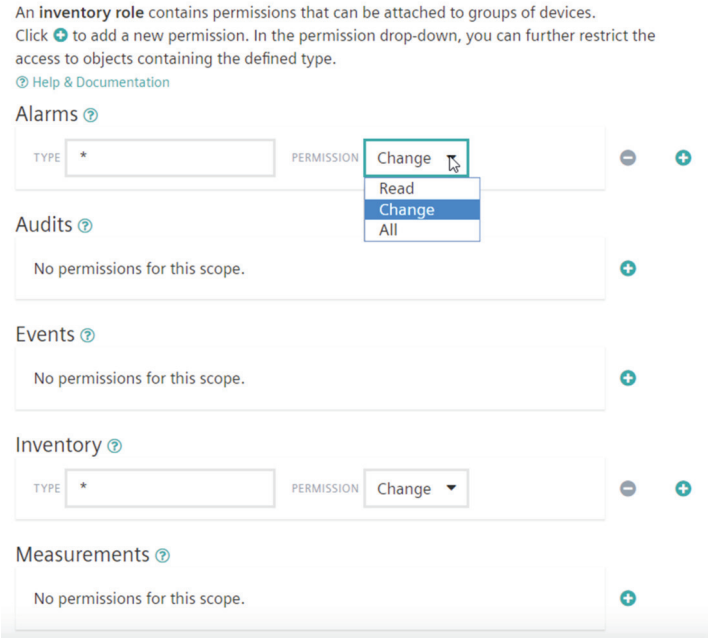
By default, the "Type" field contains an asterisk "*" selecting all types.

Note

For further information on possible types, check your device documentation, the IoT Extension sensor library or the device management library. The type being used here is the so-called "fragment type", not the "type" property. You need to enter all fragment types send in a measurement to make the measurement visible; similar for other types of data.

In the "Permission" field, select a permission level from the dropdown list:

- "Read" - to view objects
- "Change" - to modify objects (does not include "read" permission)
- "All" - to read AND modify objects



NOTICE

When you add a permission, you may see a small exclamation mark. The exclamation mark indicates that the permission that you have just added is not effective, because another, "higher" permission set for the user already includes the respective permission. Check if you have set, for example, "Full access" or if there is another permission in the same section with "*" as type and "All" as permission.

As another example, assume that you are using tracking devices. You want to allow your user to see all devices, but not to change anything. In addition, the user should be able to follow tracks of devices on a map. Tracks are recorded using an event with fragment type "c8y_Position" (see Sensor library). To do so, assign read permission on inventory as well as on events with type "c8y_Position".

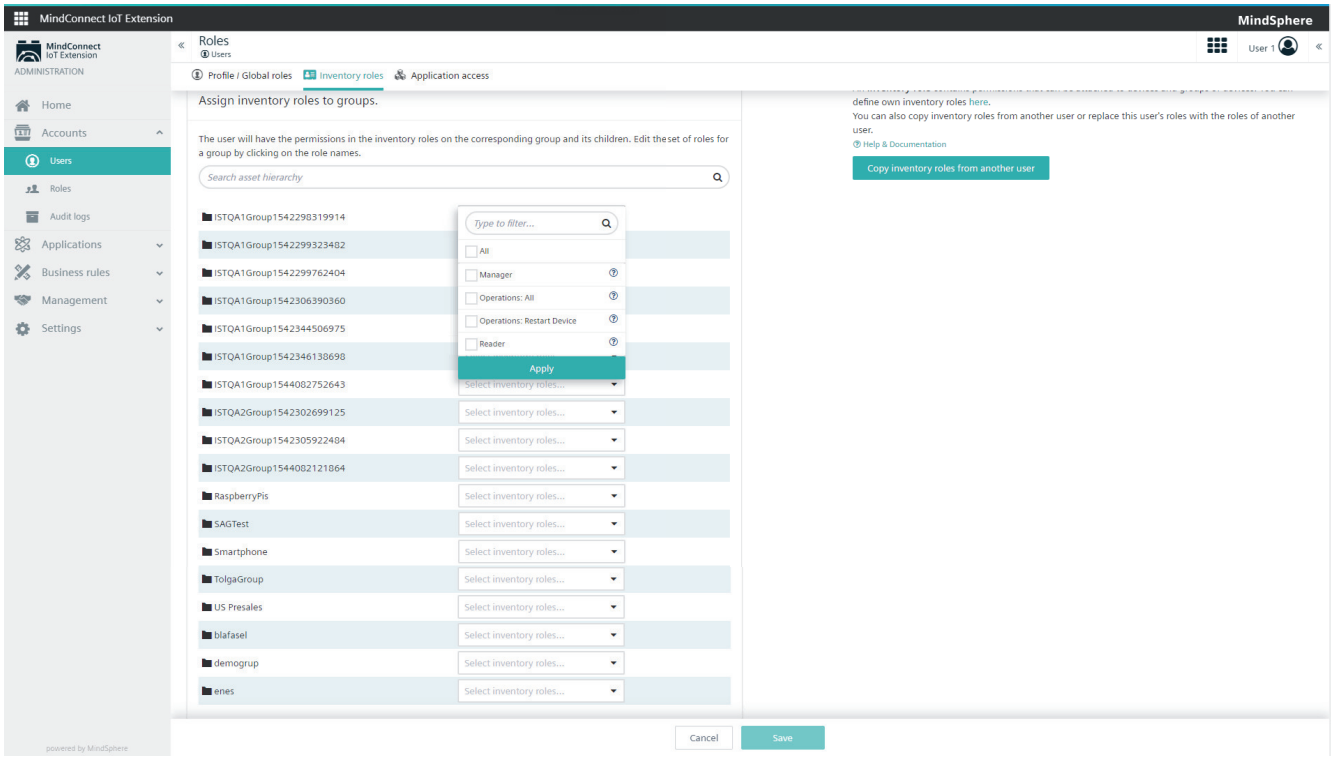
Assigning inventory roles to users

Inventory roles are assigned to a user and a group of devices.

To assign inventory roles, click "User" in the "Account" menu, select a user in the user list and switch to its Inventory roles tab.

In the Inventory roles tab you will see a tree of device groups. To assign an inventory role, click on the arrow right from a device group. Select the relevant roles and click "Apply". For details on the roles hover over the info icon next to it or refer to "Viewing inventory" roles.

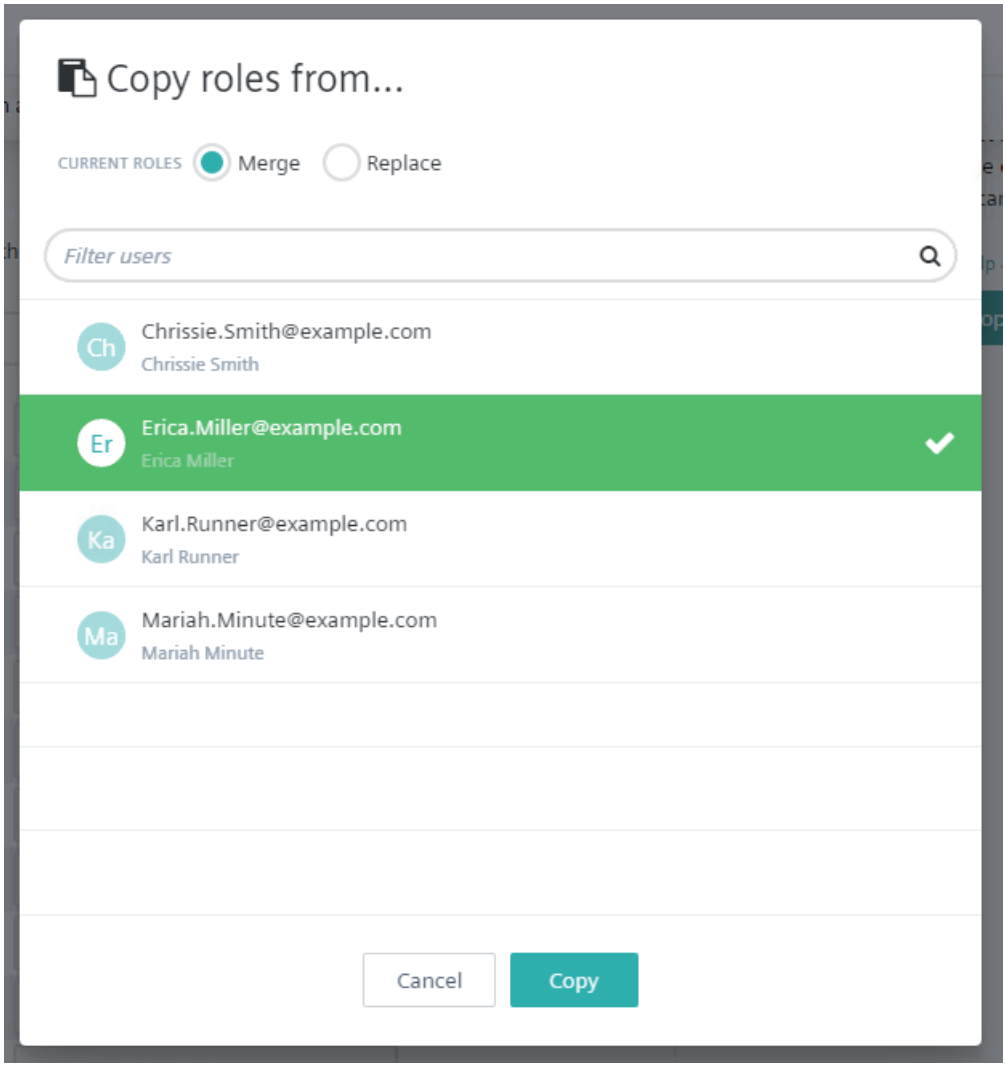
NOTICE
If a user already has a global role containing inventory permissions, the user will be able to see or change all devices regardless of what inventory roles you set here.



Inventory roles are inherited from groups to all their direct and indirect subgroups, and to the devices in these groups. If you select, for example, a role with read permissions on alarms for a group of devices, the user will be able to see alarms of all devices in this group and all its subgroups.

If a user has inventory access to a group of devices, the user will also have that access to all dashboards for that group of devices in the Cockpit application.

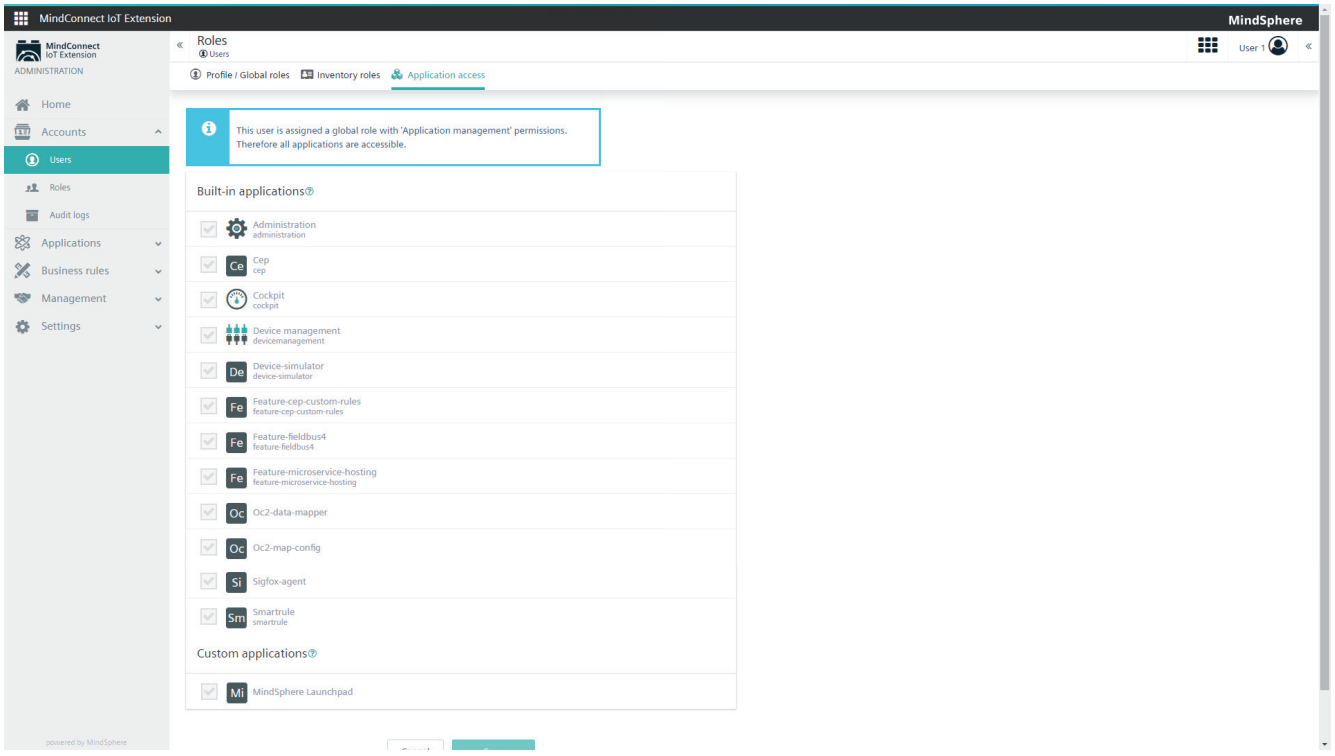
You can also copy inventory roles from another user. To copy roles, click "Copy inventory roles from another user". In the upcoming window, select a user from the list and click "Copy". At the top you can select if you want to merge the roles with the existing user roles (the default) or if you want to replace the existing user roles. Copying roles makes it easier to manage the permissions of many users as you can create a reference user and then copy the permissions from there.



Granting application access

In the Application Access tab you assign applications to the user.

The Application Access tab shows a list of all available applications in your tenant in alphabetical order. Select the applications for the user and click "Save". For more information on application management, see Managing applications (Page 31) in Administration (Page 31).



Note

If a user has global permission to read all applications, an information box will be shown.

Troubleshooting permissions

If you try to perform actions without sufficient permissions, an error message will occur.

To help troubleshooting permissions, click the "User" button at the right of the top bar. From the context menu, select "Access denied requests". In the upcoming window details on the denied accesses are provided. An administrator user or the support can help in fixing the permissions.

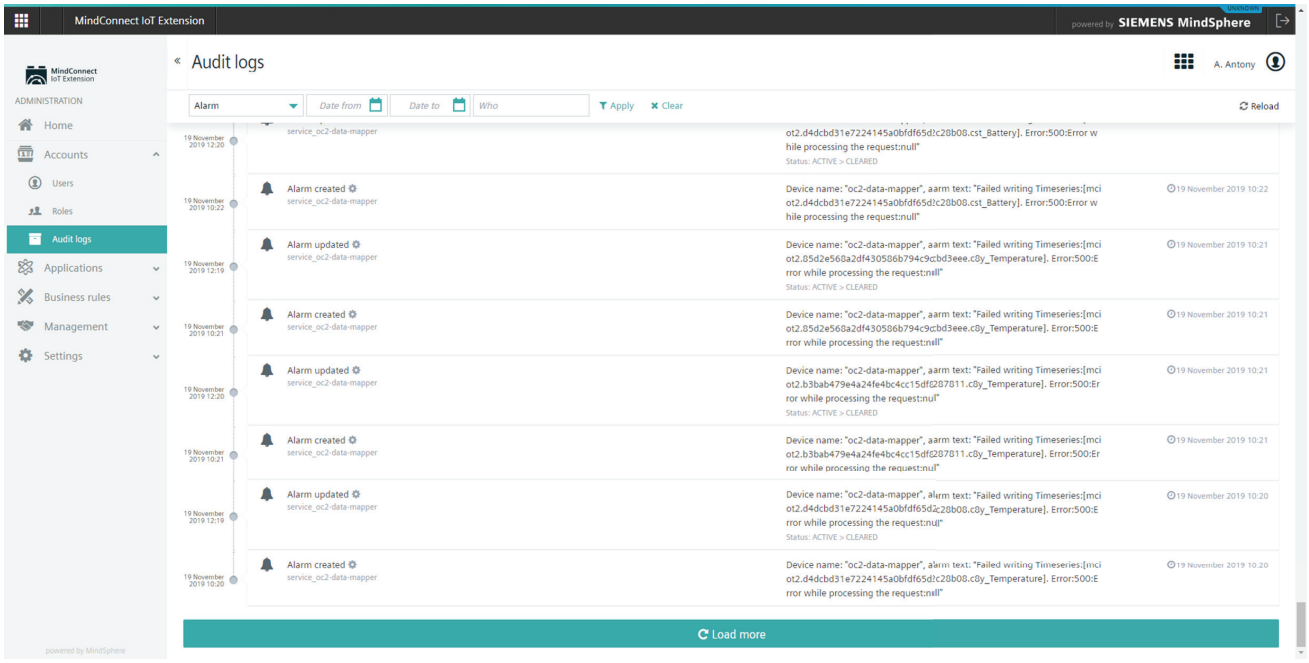
4.5 Viewing audit logs

Audit logs show the operations that users have carried out.

To view the audit log list, click "Audit logs" in the Account menu. For each log entry, the following information is provided:

Column	Description
Server time	Server time when the operation was processed.
Change	Type of operation, e.g. "Alarm created", "Smart rule deleted". Below it, the user who processed it is displayed.
Description	Provides further information depending on the operation, e.g. the device name, alarm text, operation status.
Device time	Device time when the operation was processed. This can differ from the server time.

Only the last 100 logs are visible. Click "Load more" at the bottom of the list to view more log entries.



Note

The audit log list is not automatically refreshed after a realtime update for operations. Click "Reload" at the right of the top menu bar to update the list to the latest operations.

Filtering logs

In order to easily search through logs, you may filter logs for

- the type, i.e. alarm, operation, Smart Rule,
- a date range providing a "From" and/or a "To" date,
- the user.

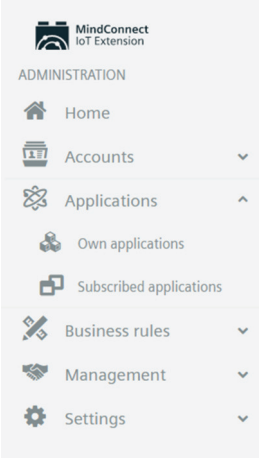
To apply filters, click the "Apply" button next to the filter fields. To discard filters, click the "Clear" button (only visible if filters are set).

4.6 Managing applications

In the IoT Extension platform we distinguish between two kinds of applications:

- Subscribed applications - all applications subscribed to the tenant (either provided by the platform or a service provider) but not owned
- Own applications - all applications owned by the tenant

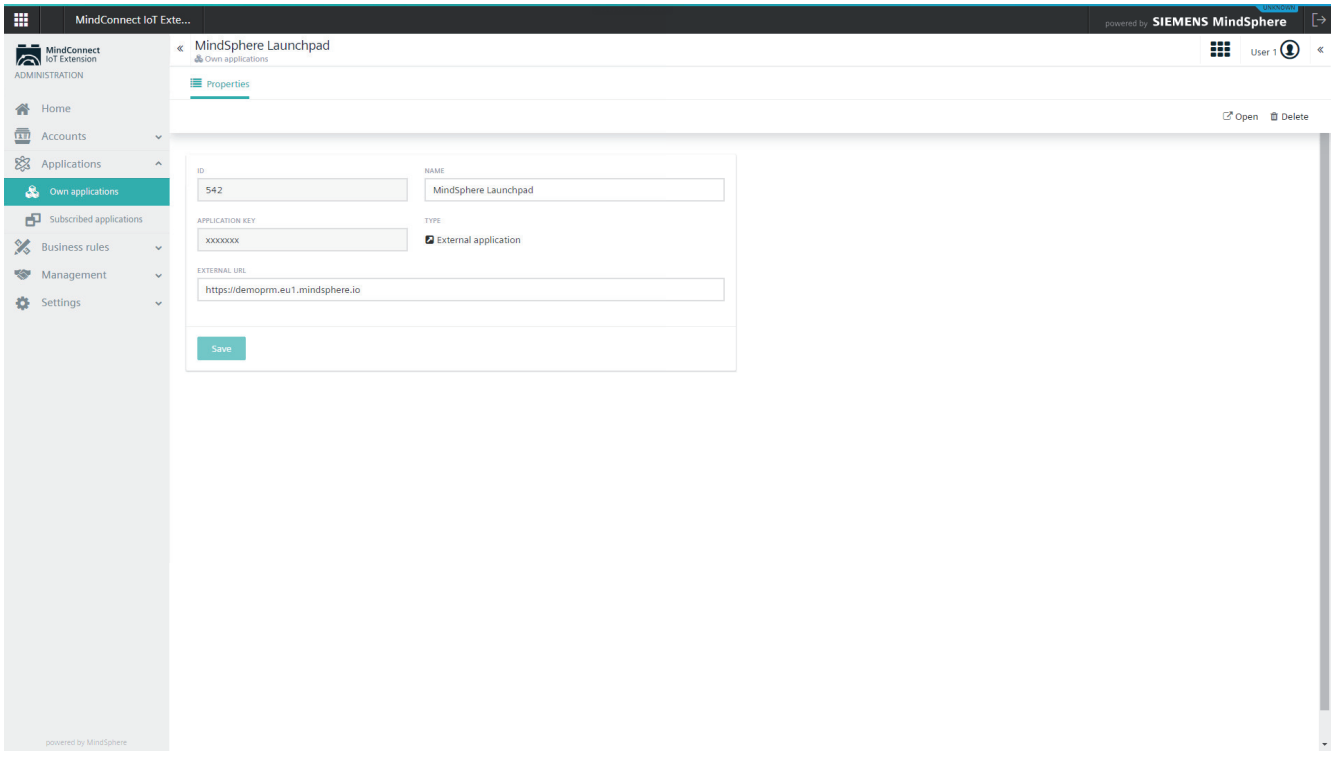
Both applications are available through the "Applications" menu in the navigator:



Subscribed applications may not be added, modified or removed by the user, while users can add custom applications in various ways as own applications.

Application properties

Click on an application card to view the application properties.



Each application will show the following properties, depending on the application type:

Field	Description	Hosted (Web app)	Microservice	External	CEP rule
ID	Unique ID to identify the application	Automatically provided	Automatically provided	Automatically provided	Automatically provided
Name	Application name. Will be shown as title of the application in the top bar and in the application switcher.	Automatically created	Automatically created, based on the zip file name	Specified by the user	Automatically created, based on the mon file name
Application key	Used to identify the application and to make the application available for subscription, see the Concepts Guide.	Automatically created	Automatically created based on the zip file name	Specified by the user	Automatically created based on the mon file name

Field	Description	Hosted (Web app)	Microservice	External	CEP rule
Type	Application type	Hosted application	Microservice	External	CEP rule
Path	Part of the URL invoking the application	Automatically created	Automatically created as .../service/<microservice name>	Specified by the user. For example, if you use "hello" as application path, the URL of the application will be "/apps/hello".	Not available

Note

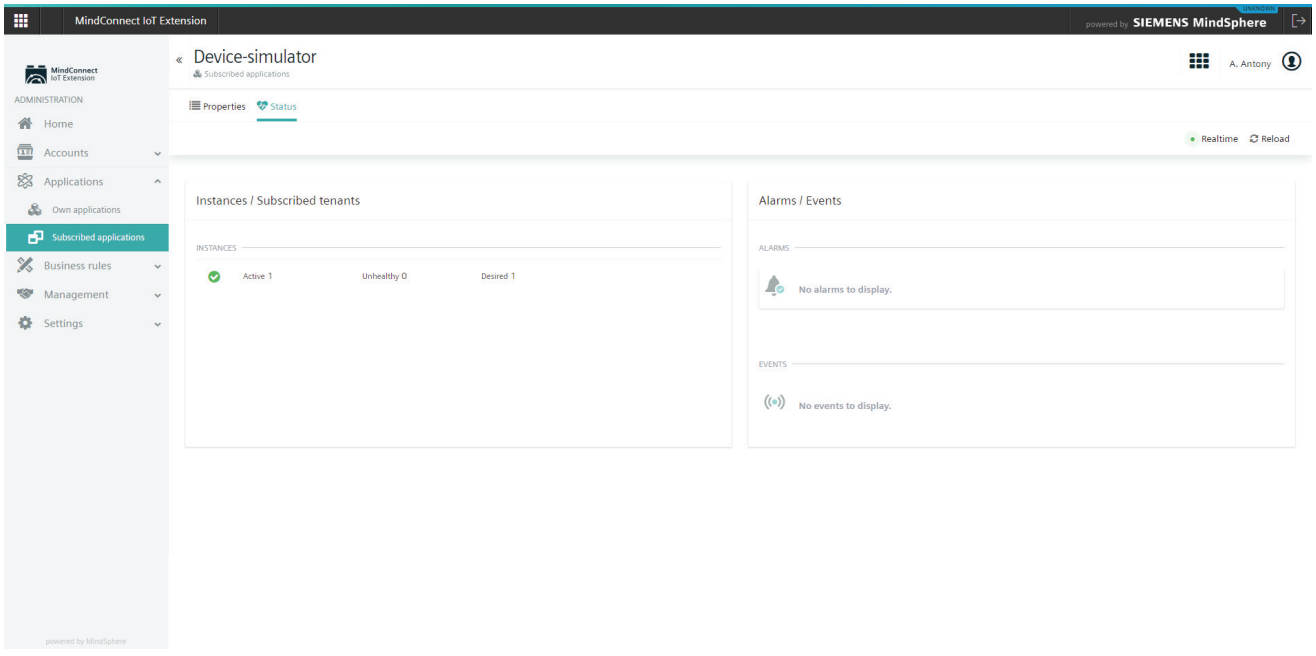
ID and type cannot be changed.

Monitoring microservices

You can monitor microservices hosted by IoT Extension in two ways:

Status information

The status of the microservice can be checked on the status tab of the respective application.



The following information is provided on the Status tab:

Sl. No.	Field name	Description
1.	Instances	Number of active, unhealthy and desired microservice instances for the current tenant
2.	Subscribed tenants	Number of active, unhealthy and desired microservice instances for all subtenants subscribed to the microservice

Sl. No.	Field name	Description
3.	Alarms	Alarms for given application, provided in realtime
4.	Events	Events for given application, provided in realtime

The status information is available for subscribed applications as well as for own applications. Information on subscribed subtenants is only visible for the application owner.

To view the status you need the following permissions:
ROLE_APPLICATION_MANAGEMENT_READ & ROLE_INVENTORY_READ

Log files

You may view logs to get more details on the status of microservices.

To view logs, open the Log tab of the respective microservice.

At the top of the page, the instance of the microservice, for which you want to view the logs, can be selected. Moreover you can adjust the font size and the theme at the right.

Initially, the Log tab shows the logs of the microservice instance for the last 10 minutes. The exact time range for which the logs are displayed is shown below the logs.

Click "Next" or "Previous" to increase or reduce the time range in 10 minutes steps.

If there have not been any logs in the selected time range, a message is shown.

To view the logs you need the permission EVENT_READ.

Own applications

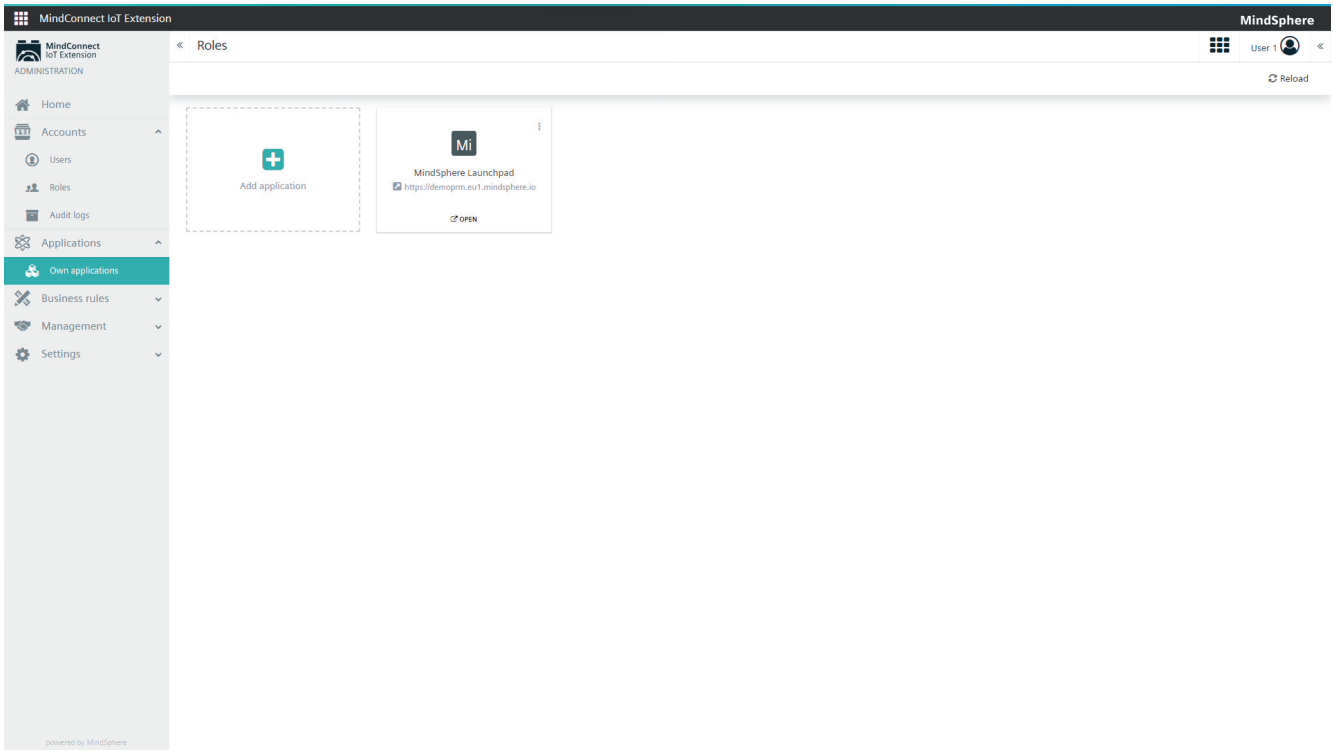
Own applications may be:

- Duplicates of subscribed applications (in order to be able to customize them)
- Web-based UI applications, either deployed as standalone applications or as plugins deployed into a specific application (e.g. a widget to the Cockpit dashboard)
- Server-side business logic deployed through microservices

Your applications are available through the application switcher in the top bar which allows to easily switch between applications.

You manage your applications under "Own applications", accessible through the "Applications" menu.

In the "Own applications" page you will find a list of the applications available in your account.



To display further information on the application, simply click its card. For details on the fields, refer to "Application properties" below.

To directly open an application from here, click "Open" on the respective application card.

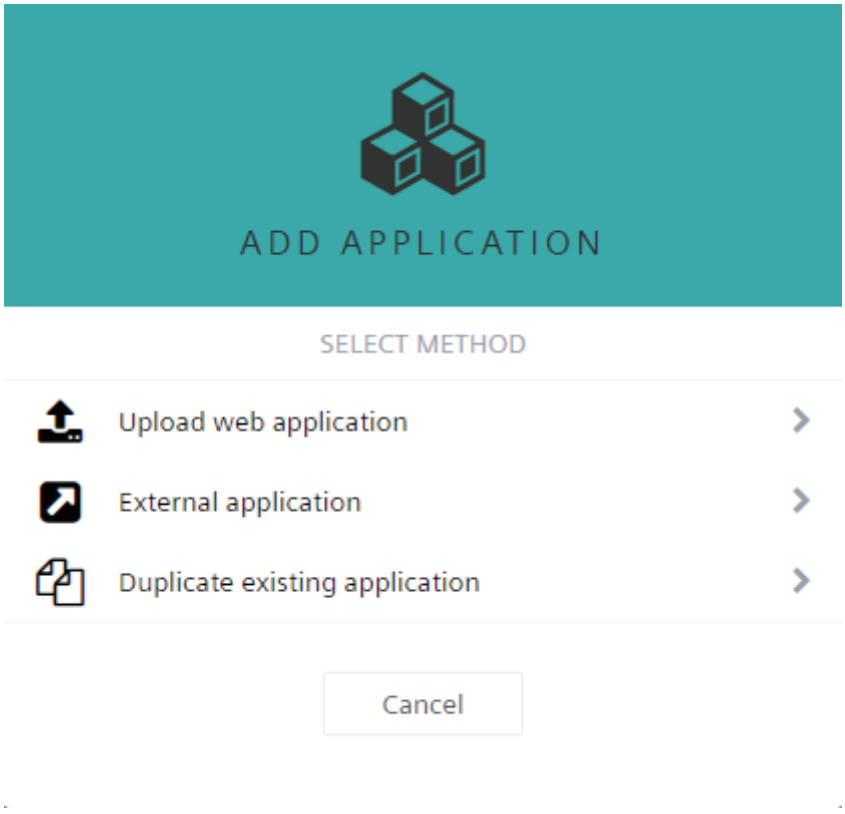
Click "Add application" in the Own applications page, to add an application to your account.

Click the menu icon at the top right of an application to open a context menu from where you can "Edit" or "Remove" an application.

Adding own applications

To add an application, click "Add application" in the "Own applications" page. In the upcoming dialog choose one of the following methods:

- uploading a web application - by dropping a ZIP file or browsing for it on your computer
- uploading a microservice - by dropping a ZIP file or browsing for it on your computer
- using an external application - by linking to an application running elsewhere
- duplicating an existing application - by creating a copy of an existing application



Uploading web applications

In order to upload a web application, follow these steps:

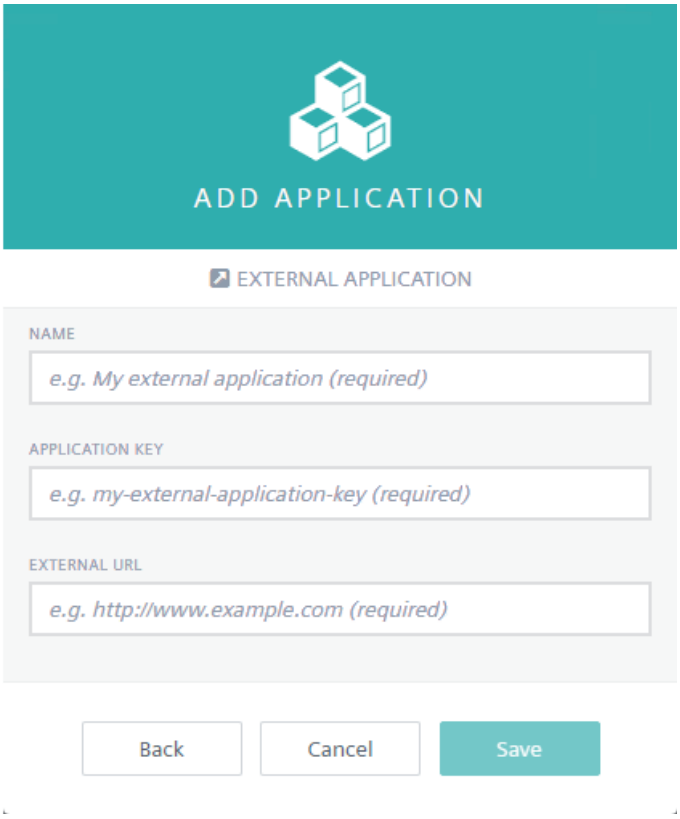
1. Click "Add application" in the "Own applications" page.
2. In the upcoming dialog, select "Upload zip file"".
3. Simply drop a zip file or browse for it on your computer.

After successfully uploading the zip file to the platform the application is being created.

Linking to external applications

In order to add an application which links to an external application, follow these steps:

1. Click "Add application" in the "Own applications" page.
2. In the upcoming dialog, select "External application".



3. In the next window, enter the name of the application. The name will be shown as title of the application.
4. Enter an application key, used to identify this application.
5. Enter the external URL where the application can be reached.
6. Finally, click "Save" to create the application.

For details on the fields, see also "Application properties" below.

Duplicating applications

Duplicating an application might be useful if you want to customize a subscribed application according to your needs.

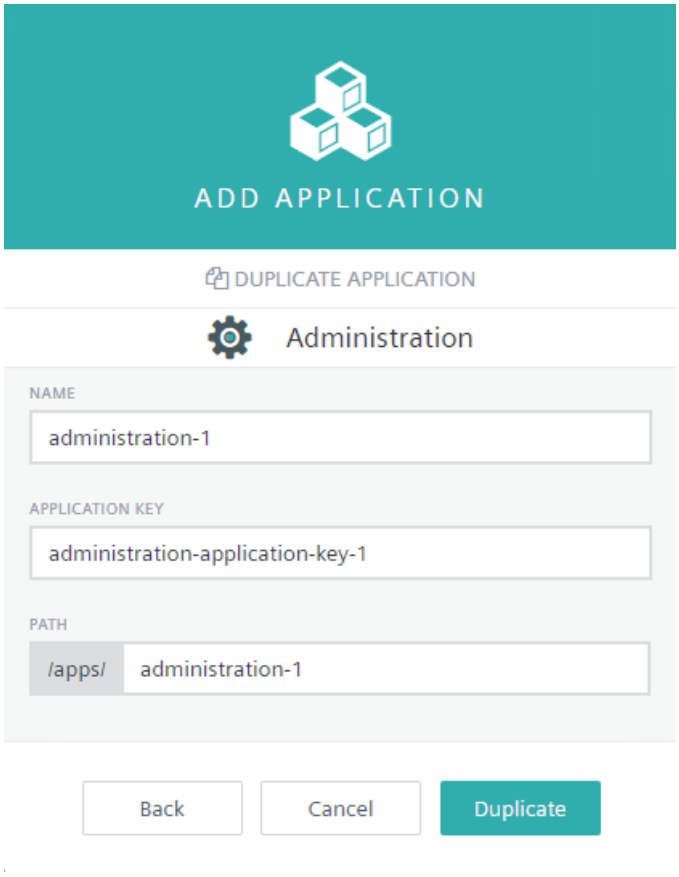
Duplicating a subscribed application creates a copy of the application as an own application, with a link to the original application.

Note

If you want your "Own application" to overrule a subscribed standard application, the path of the "Own application" needs to be set to the path of the original subscribed application.

In order to duplicate an application, follow these steps:

1. Click "Add application" in the "Own applications" page.
2. In the upcoming dialog, select "Duplicate existing application".
3. Select the desired application from the dropdown list.



4. In the next window, provide a name for the application. By default, the name of the original application is provided, extended by a number.
5. Provide an application key, used to identify this application. By default, the key of the original application is provided, extended by a number.
6. Provide the application path as part of the URL to invoke the application. By default, the path of the original application is provided, extended by a number. If you set it to the path of the original subscribed application, your own application will overrule the subscribed application.
7. Finally, click "Duplicate" to create the application.

For details on the fields, see also "Application properties" below.

Editing and removing own applications

Edit

To edit an application, simply click the application or click "Edit" in its context menu, accessible through the menu icon.

In the "Properties" tab, several fields can be modified, depending on the application type (see "Application properties").

NOTICE
Never change the system application names (e.g. "Device Management", "Cockpit"). Otherwise, tenant initialization will fail.

Remove

To remove an application, click the menu icon and from the context menu select "Remove".

If you remove an application that overwrites a subscribed application, the currently subscribed application becomes available to all users. Additionally, the users will then also benefit from future upgrades of the subscribed application.

It is not possible to remove subscribed applications. This can only be done by the owner of the subscribed application.

Adding and removing plugins

NOTICE
This plugin functionality is deprecated and only available in versions earlier then 9.16.

In order to configure and extend the functions provided with an application, you can add plugins to it.

Note

Because the application itself is modified when adding a plugin, plugins can only be added to own applications. When adding a plugin to a subscribed application, the application must be duplicated first into an own application.

To add additional plugins, click "Add Plugin" on the card of the desired application in the "Own applications" page.

The "Plugin" tab for the application will open up, showing all existing plugins and allowing to add plugins by simply dropping the respective ZIP file or browsing for it on your computer.

To remove a plugin, hover over it and click "Remove" at the right.

The following tables list the navigator and menu items with their respective plugins.

Navigator Item	Plugin
Welcome	Welcome screen
Home	Cockpit Home
Smart Rules	Smart Rules UI
Groups	Groups Hierarchy

Navigator Item	Plugin
Data Explorer	Data Point Explorer UI
Data Point Library	Data Point Explorer UI
Reporting	Reporting
Reports	Dashboard (Note: that there are two plugins with this name. Select the one with the description: "Reports are stand alone dashboards without a context".)
Alarms	Alarm Management

Menu Item	Plugin
Info	Not possible to disable
Subassets	Not possible to disable
Permissions	Device Permission Management Plugin
Data Explorer	Data Point Explorer UI

Be aware of the "UI" at the end of the plugin names.

Restoring to a previous application version

Users can restore previous versions of an application from an archive:

1. Open the application by clicking on it.
2. Switch to the Archives tab.
3. Open the context menu for the desired version by clicking the menu icon and select "Set as active" to make it the active version.
4. Click "Remove" to remove the version from the archive.

Note

The "Archive" tab is not available for subscribed applications, as only the owner of the application can perform this action.

Uploading archives

Multiple archive file versions can be stored in IoT Extension when they were created by uploading either a zip file or a mon file. Each version is called an archive. You can upload different versions at the same time and switch between these versions.

To upload an archive, follow these steps:

1. Open the application by clicking on it.
2. Switch to the "Archives" tab.
3. Click "Upload archive" and browse for the archive on your computer or simply drop the archive file.
4. Click "Upload" to upload the archive to your IoT Extension account.

Once uploaded, the recently uploaded version is automatically the active version, i.e. the version of the application that is currently being served to the users of your account. This version cannot be deleted.

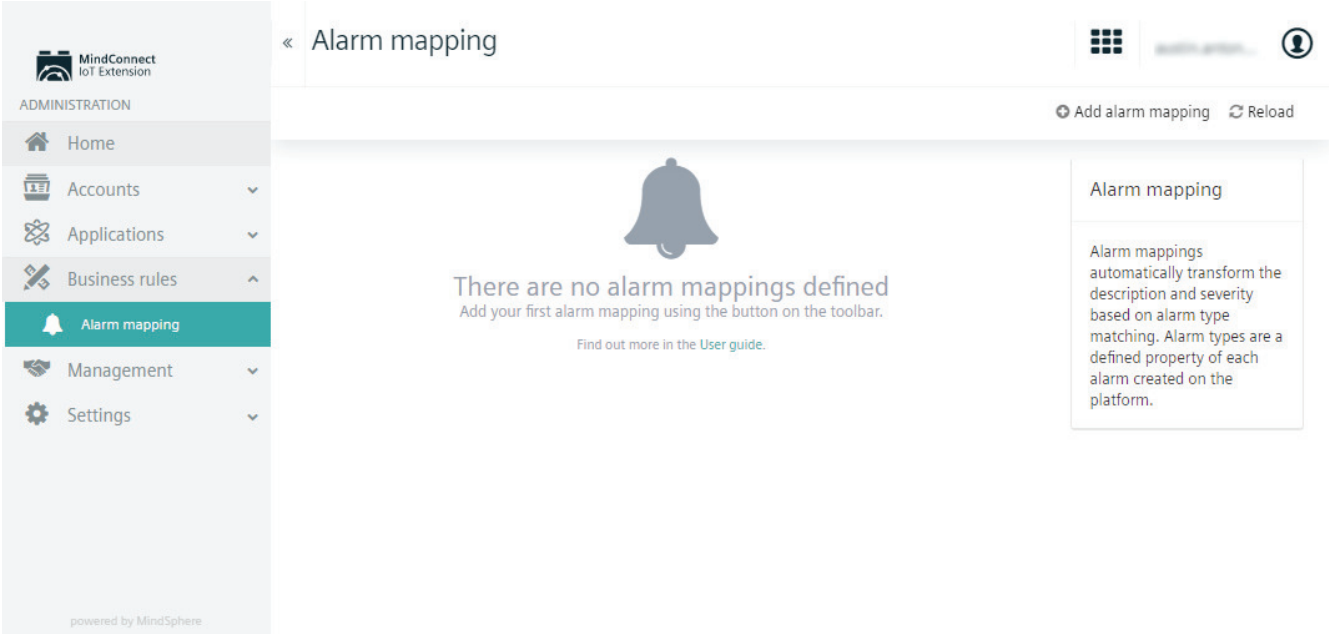
To change the active version, open the context menu in the version you want to activate and select "Set as active".

4.7 Managing business rules

Alarm mapping

Alarm mapping enables you to change the severity and text of alarms to adapt them to your business priorities. For example, a loss of the connection to a device is by default a "MAJOR" alarm but may be critical to you. To change this, add an alarm mapping to change alarms related to connection losses to CRITICAL.

Click "Alarm mapping" in the Business Rules menu to see a list of all alarm mappings.



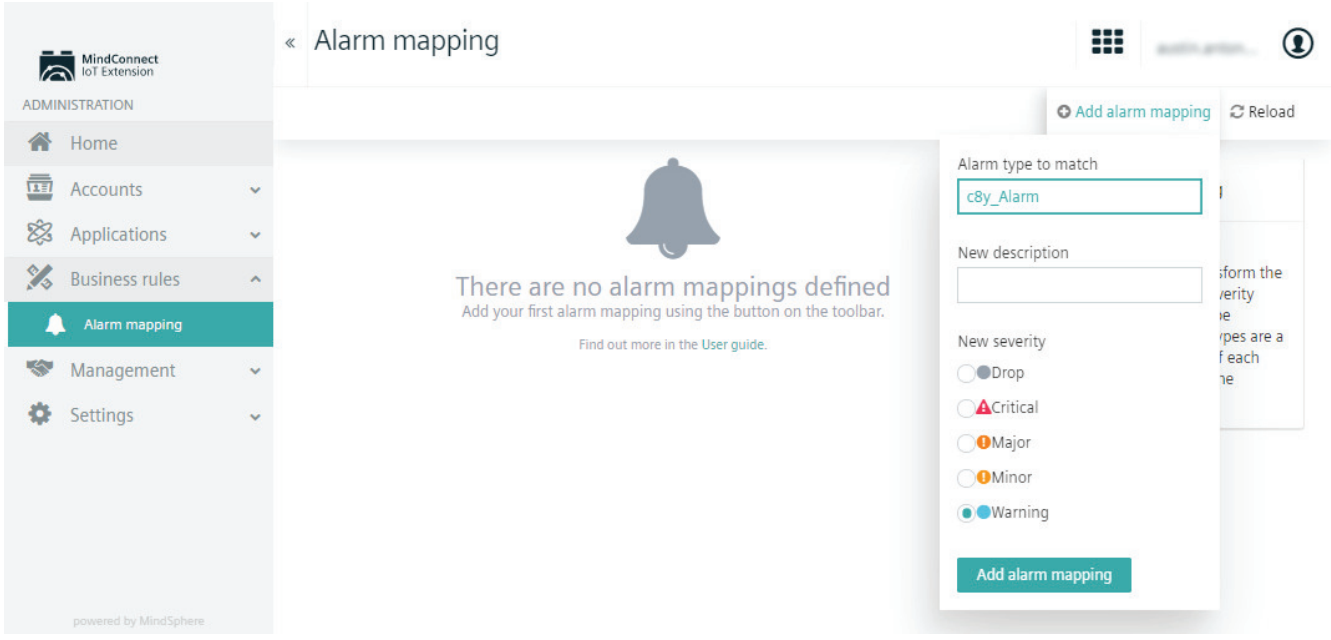
For each alarm mapping, the alarm severity and the name of the mapping is shown.

To edit an alarm mapping, simply click it.

To delete an alarm mapping, hover over it and click the "Delete" button.

Adding an alarm mapping

To add an alarm mapping, click "Add alarm mapping" in the top menu bar.



1. Enter the alarm type to be modified.
2. Optionally, enter a new text for the alarm. If you do not enter any text, the original text in the alarm will be kept.
3. Select the desired new severity, or select "Drop" to not show the alarm at all.
4. Click "Save" to save your settings.

4.8 Management

Retention rules

"Retention rules" gives you control on how long data is stored in your account. You might for example want to store measurements for 90 days, but delete alarms already after 10 days. By default, all historical data is deleted after 60 days (configurable in the system settings).

Retention rules are usually run during the night. When you edit a retention rule, you will not see an immediate effect in the Usage section on the Home screen of the Administration application.

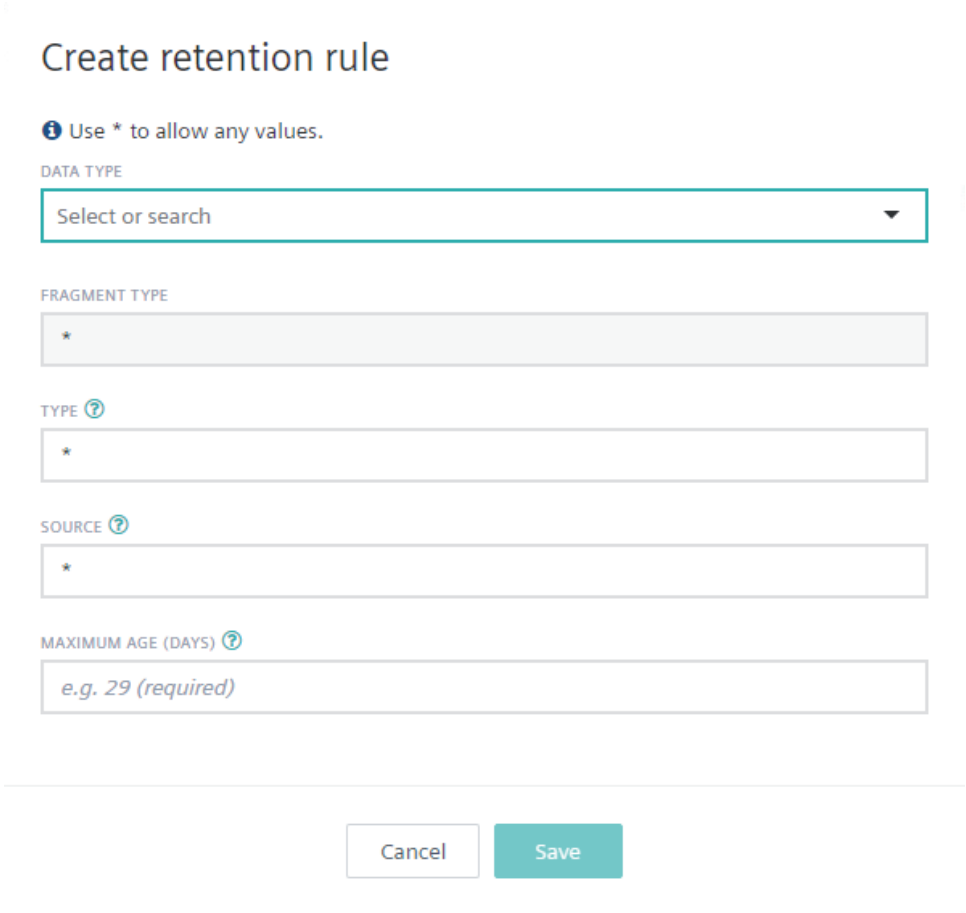
Click "Retention rules" in the Management menu to view a list of retention rules configured for your account.

For each rule, the rule name, details on the data to be deleted (fragment type, type and source, see below) and the maximum age in days is provided.

The asterisk ("*") indicates that data with any value will be cleaned up.

Creating retention rules

To add additional retention rules, click "Add rule" in the top menu bar.



Note

Per default, an asterisk ("*") is set in all fields except the "Maximum age" field, to include all values.

1. Select the type of data to be cleaned up (alarms, measurements, events, operations, audit logs or all).
2. Enter a fragment type if you want to be more specific about the data to be cleaned up. To clean up all connection loss alarms with this rule, select "alarms" and enter "c8y_UnavailabilityAlarm" as property into the "Type" field.
3. If you want to remove data only from a specific device, enter the device ID into the "Source" field.
4. Enter the "Maximum age" in days (max. allowed value is 10 years in days).
5. Click "Save" to create the rule.

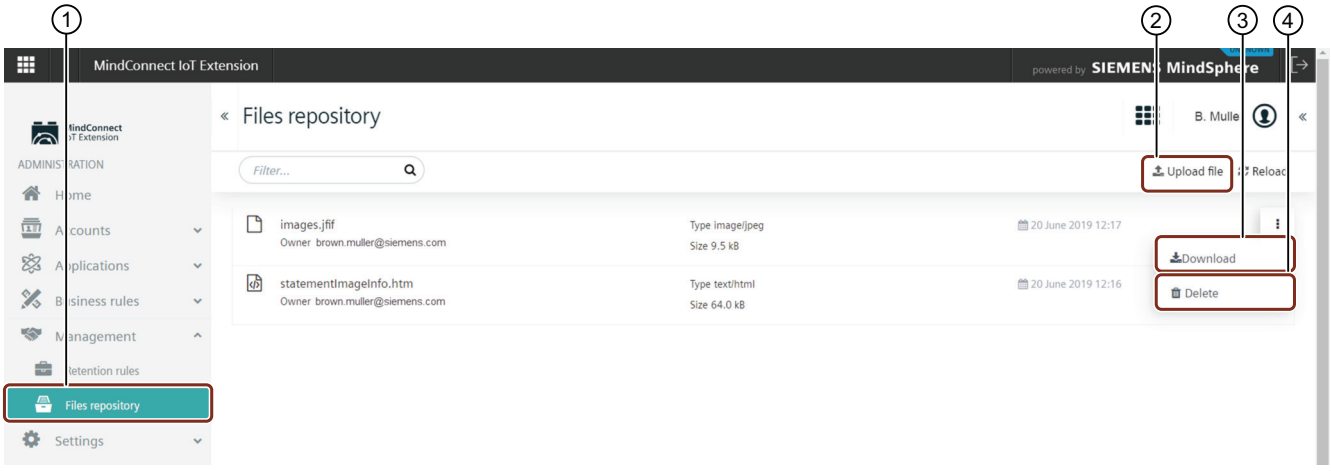
Note

Alarms are only removed if they are in CLEARED state.

To delete a rule, hover over it and click the "Delete" button at the right.

Managing files in the file repository

The file repository provides an overview of the files stored in your account.



① Files repository menu
② Upload file option
③ Download file option
④ Delete file option

Click "Files repository" in the Management menu to see a list of files.

The files listed can come from various sources. They can be software images, configuration snapshots taken from devices, log files from devices or web applications uploaded from the Own applications page.

For each file, the name of the file, its owner, the file type (i.e. image/bmp, text/csv), its size and the date when it was last updated is provided.

To **upload** a file from your computer, click "Upload file" in the top menu bar.

To **download** a file from your account, click the menu icon and from the context menu select "Download".

To **delete** a file from your account, click "Delete" in the context menu.

Note

If the file corresponds to an active application, it cannot be deleted. You first need to remove or upgrade the application to be able to delete it.

4.9 Changing settings

From the "Settings" menu, administrators can modify or manage various settings for the account as:

- Configuring single sign-on,
- Changing the application settings,
- Changing the password policy,
- Managing the properties library,
- Configure system-wide configuration properties in IoT Extension.

Configuring single sign-on

IoT Extension provides single sign-on functionality, that allows a user to login with a single 3rd-party authorization server using the OAuth2 protocol. Currently authorization code grant is supported only with access tokens in form of JWT (JSON web tokens).

Note

This feature is built on top of cookies technology. To be able to use it, you must have cookies enabled in the settings of your browser.

This feature is enabled since IoT Extension version 9.12. For correct behavior any microservice needs to use the microservice SDK with version 9.12 or later.

Before switching to the single sign-on option it is mandatory that:

- the authorization server you use supports OAuth2 authentication code grant,
- the access token is issued as JWT and you know what goes into the token content,
- the JWT must consist of a unique user identifier,
- the IoT Extension platform is in version 9.12 but preferably higher,
- all microservices are build with Microservice Java SDK 9.12.6 but preferably higher.

For on premises installation the domain-based tenant resolution is configured properly.

Changing application settings

Click "Application" in the Settings menu to change applications settings.

Under "Default application", you can select a default application from the list which will apply to all users within the tenant.

Note

All users must have access to this application.

Under Access control, administrators can enable cross-origin resource sharing or "CORS" on the IoT Extension API.

The Allowed Domain setting will enable your JavaScript web applications to directly communicate with REST APIs.

- Set it to "*" to allow communication from any host.
- Set it to "http://my.host.com, http://myother.host.com" to allow applications from http://my.host.com and from http://myother.host.com to communicate with the platform.

For further information, see http://enable-cors.org.

Changing the password policy

To change password settings, click "Password" in the Settings menu.

Under "Password expiration", you can limit the validity of user passwords by specifying the number of days after which users have to change their passwords. If you do not want to force your users to change passwords, use "0" for unlimited validity of passwords (default value).

By default, users can use any password with eight characters or more. If you select "Enforce" that all password are "strong" (green), your users must provide strong passwords.

Note

The password validity limit and the enforcing of strong passwords may not be editable, if configured by the platform administrator.

Strong (green) passwords must have "M" characters. By default, the system restricts the use of passwords already used in the past. The last "N" passwords provided by a user are remembered by the system and the system does not allow to use them. The default value for "N" is 10.

Note

"M" and "N" can be configured by the platform administrator.

Click "Save" to apply your password settings.

Managing the properties library

In the "Properties" library, accessible from the "Settings" menu, custom properties can be added to inventory objects, alarms, events and tenants.

With custom properties, you can extend the data model of IoT Extension built-in objects. You may create the following custom values:

- Custom inventory properties are used to extend the inventory data model. They can be used in the “Asset table” and “Asset properties” widgets.
- Custom tenant properties are available during tenant creation. The custom properties can be edited under Subtenants in the Custom properties tab of each tenant. Additionally, these properties can be viewed and exported in the Usage statistics.
- Custom alarm and event properties can be used as custom fields which can be added to your reports and will be available in the "Export" page in the Cockpit application.

Note

Custom properties are visible to all authenticated users of the tenant, regardless of their inventory role permission.

Adding properties to the properties library

To add a custom property, select the tab for the desired property and click "Add property".

In the upcoming form, provide a unique name as identifier and a label for the property and select its data type from the drop down list. Additionally, select validation rules for the new property:

Check box	Description
Required	If selected, the property needs to be provided, i.e. during alarm creation. Not available if the property type is "Boolean".
Default Value	Provide a default value to be automatically filled in the custom property field. Only available for properties with type "String".
Minimum	Enter a minimum integer value.
Maximum	Enter a maximum integer value.
Minimum length	Enter the minimum length required for the string.
Maximum length	Enter the maximum length required for the string.
Regular expression	Add a regular expression which will be required in order to fill the custom property field.

Click "Save" to create the new property.

Click on the name of a property in the list to open it. To edit the property, enter the desired changes and click "Save" to save the settings. Click "Remove" to delete the property.

Entering OpenIT credentials

By providing OpenIT credentials you enable the platform to utilize SMS services provided by OpenIT.

SMS are used throughout the application for various features like two-factors authentication and user notifications, i.e. on alarms.

Device Management

5

5.1 Working with the devices

5.1.1 Overview on device management

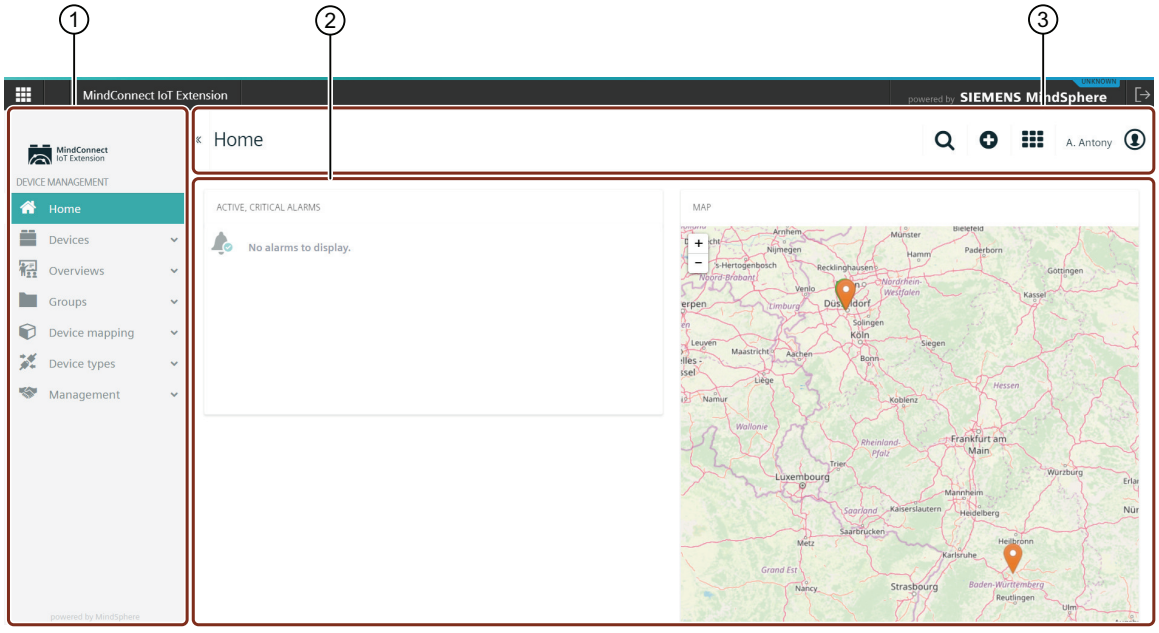
The following sections will walk you through all functionalities of the Device Management application in detail. For your convenience find an overview on the content of this document below.

Section	Content
Connecting devices (Page 51)	How to register one or more devices manually and how to bulk-register devices in order to connect devices to your account.
Viewing devices (Page 56)	What is displayed in the device list and how to sort devices by searching for devices and filtering devices.
Grouping devices (Page 85)	Why and how to group devices into top-level groups, sub-groups and smart groups.
Device details (Page 61)	Detailed description of the various kind of information available for various types of devices.
Monitoring and controlling devices (Page 75)	How to monitor the connection quality and service status of devices, how to handle alarms from devices, how to remote control and how to troubleshoot devices.
Managing device types (Page 117)	How to process data from various device types by using device protocols.
Managing device data (Page 120)	How to retrieve and manage firmware and software for devices and how to handle configuration snapshots.
Working with simulators (Page 70)	How to model devices with the simulator in order to have the same level of functionality as connected hardware devices.
Using SmartREST templates (Page 111)	How to work with SmartREST templates, a collection of request and response templates used to convert CSV data and Cumulocity Rest API calls.
Mapping devices (Page 91)	How to map devices to assets, upload history data and onboard devices.

5.1.2 User interface "Device Management"

The Device Management talks about managing devices which involves different functions like registering, connecting, monitoring, viewing and mapping devices.

Device Management UI screen



① Tool navigation window
② Work area
③ Menu options

Symbols

The following table shows the buttons of the start screen:

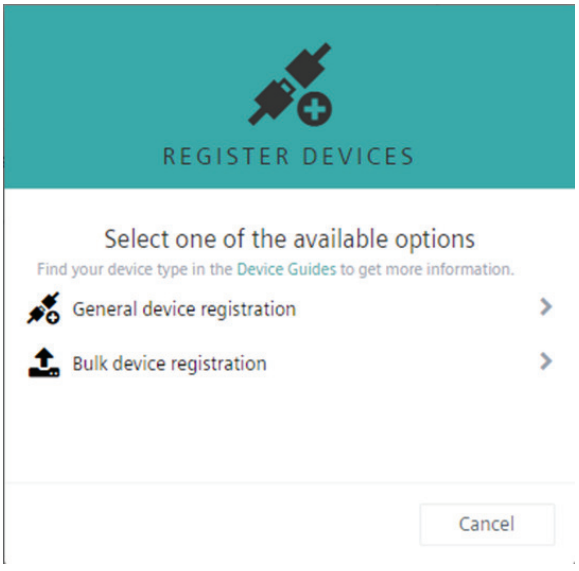
Symbol	Description
	Search bar
	Add a new group by selecting devices from the displayed device list.
Administration Cockpit Device management	Menu to select: • Administration • Cockpit • Device management
A. Antony	Current user logged in
«	Left navigation tool screen is hidden to provide you with more work-space.

5.1.3 Connecting devices

This section describes how to connect devices to your IoT Extension account either manually or by bulk-registration.

To connect devices to your IoT Extension account, follow these steps:

1. Click "Registration" in the Devices menu of the navigator and click "Register device".
2. In the "Register devices" dialog, you may choose one of the following options:
   - "General device registration" - to manually connect one or more devices
   - "Bulk device registration" - to register larger amounts of devices in one step.
3. You will see a third option "Custom device registration" for registering devices in “Cloud Remote Access” gateway if you are subscribed to such functionality. For more details, see the documentation for Cloud Remote Access.

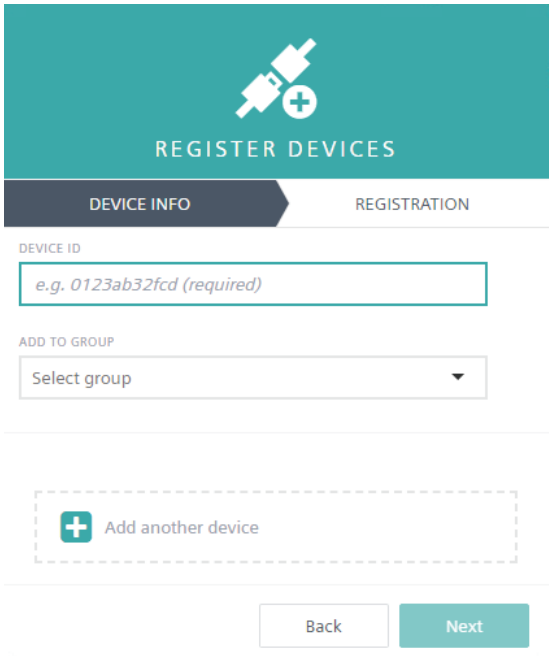


Connecting devices manually

The following process describes how to connect devices manually. Depending on the type of device you want to connect, not all steps of the process may be relevant.

To connect devices manually to your IoT Extension account, follow these steps:

1. Click "Registration" in the Devices menu of the navigator and click "Register device".
2. In the "Register devices" dialog, choose "General device registration".



3. In the "Device ID" field, enter a unique ID for the device. To determine the ID, consult the device documentation. In case of mobile devices the ID usually is the IMEI (International Mobile Equipment Identity) often found on the back of the device.
4. Optionally, select a group to assign your device to after registration. Find further information on groups assignment in "Grouping devices".
5. Click "Add another device" to register one more devices. Again, enter the device ID and optionally select a group. This way, you can add multiple devices in one step.
6. Click "Next" to register your device(s).

Note

Note that since the management tenant does not have access to the subtenant's inventory you can either register devices to a tenant OR to a group, not both.

After successful registration the device(s) will be listed in the "Device registration" page with the status "Waiting for connection".

Turn on the device(s) and wait for the connection to be established. Once a device is connected, its status will change to "Pending acceptance". Click "Accept" to confirm the connection. The status of the device will change to "Accepted".

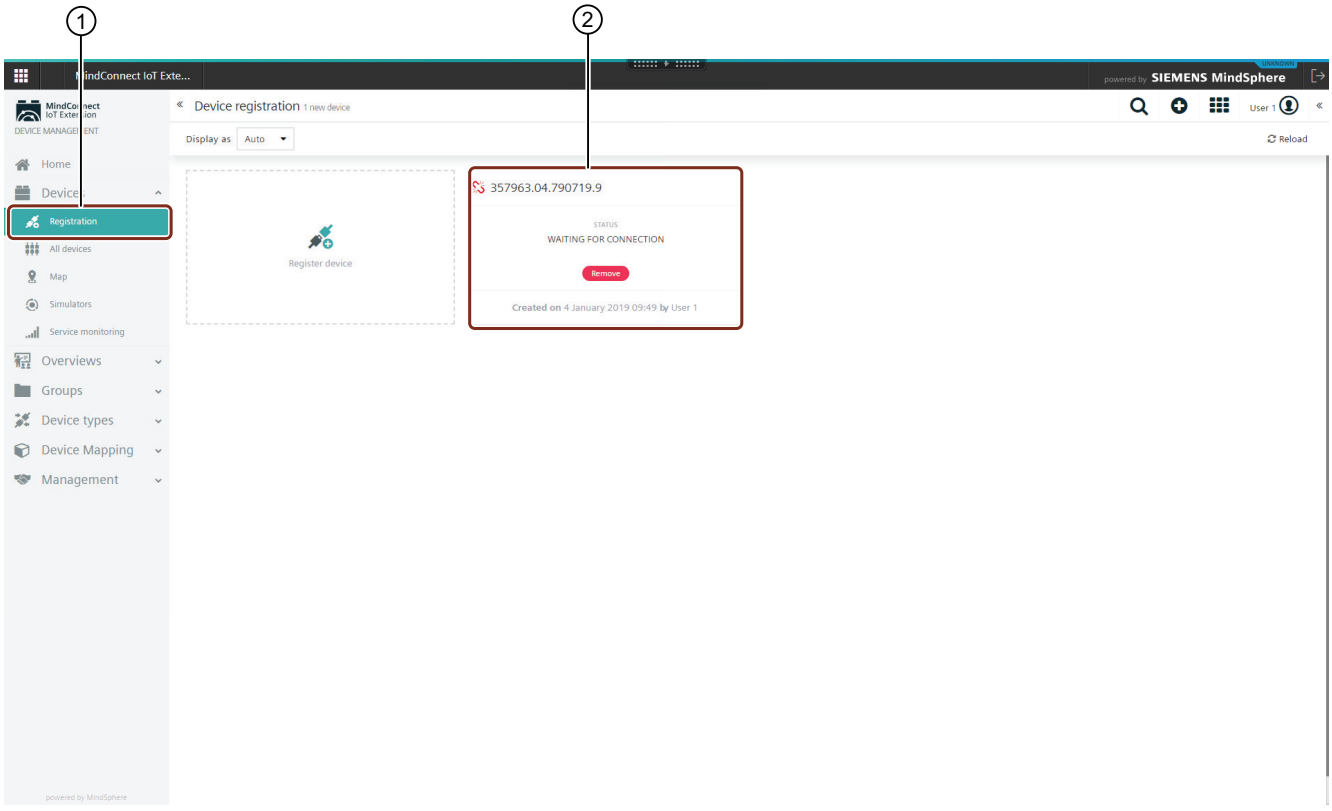
Note

In case of any issues, consult the Device guide applicable for your device type, search for your device type in the Developer Center on our website for further information, or look up the manual of your device.

5.1.4 Register devices

Device registration page

In the "Device registration" page all devices which currently are in the registration process are displayed either in a list or in a grid.



① Device registration menu

② Information displayed for each device:

- Device name specified in the registration process
- Status of the device (see below)
- Creation date
- Tenant from which the device was registered

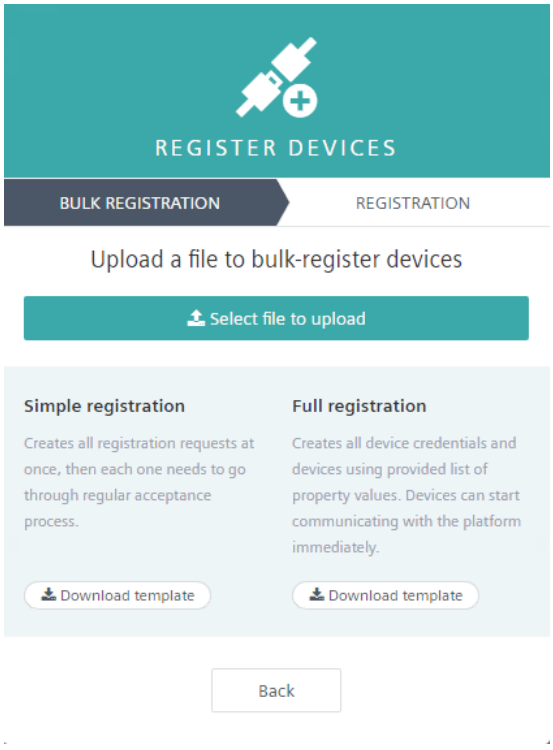
The devices may have one of the following status:

Sl. No.	Status	Description
1.	Waiting for connection	The device has been registered but no device with the specified ID has tried to connect.
2.	Pending acceptance	There is communication from a device with the specified ID, but the user doing the registration must still explicitly accept so that the credentials are sent to the device.
3.	Accepted	The user has allowed the credentials to be send to the device.

Bulk-registering devices

To connect larger amounts of devices, IoT Extension offers the option to bulk-register devices, i.e. to register larger amounts of devices by uploading a CSV file.

1. Click "Registration" in the Devices menu of the navigator and click "Register device".
2. In the upcoming window choose "Bulk device registration".



3. Click "Select file to upload" and select the CSV file you want to upload by browsing for it on your computer.

Depending on the format of the uploaded CSV file, one of the following registration types will be processed:

1. "Simple registration"
   The CSV file contains two columns: ID;PATH, where ID is the device identifier, e.g. serial number, and PATH is a slash-separated list of group names (path to the group where the device should be assigned to after registration).
2. "Full registration"
   The CSV files must contain at least the IDs as device identifier and the credentials of the devices.
   Apart from that the file can also contain other columns like ICCID, NAME, TYPE.
   To connect the devices, they are pre-registered with the relevant information. More specific, each device will be configured as follows:
   - User name - the user name for accessing IoT Extension must have the format <tenant>/device_<id>, where <tenant> refers to the tenant from which the CSV file is imported and <id> refers to the respective value in the CSV file.
   - Password - the password to access IoT Extension, equals the value "Credentials" in the CSV file.
   - Device in managed object representation - fields TYPE, NAME, ICCID, IDTYPE, PATH, SHELL in the CSV file.

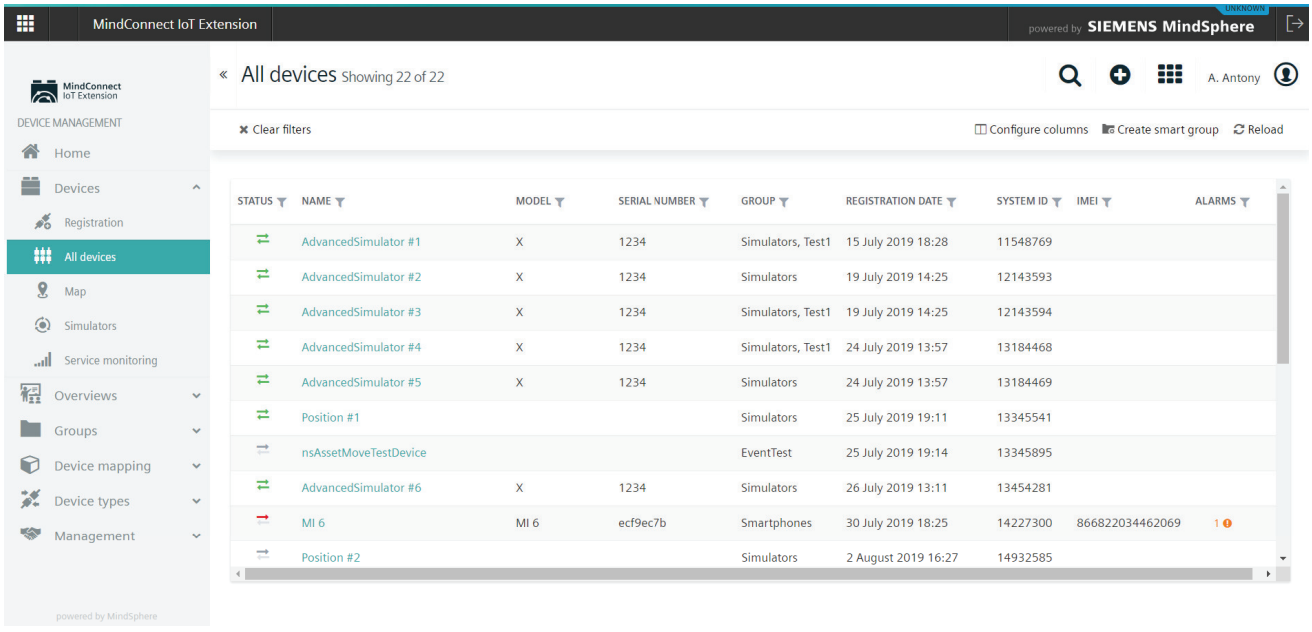
After the data is imported, you will get feedback on the number of devices that were pre-registered as well as on any potential errors that may have occurred.

For your convenience we provide template files for both formats which you can download to view or copy the structure.

5.1.5 Viewing devices

To view all devices connected to your account, click "All devices" in the "Devices" menu in the navigator.

A detailed device list will be displayed.



Device list

For each device, the device list shows the following information provided in columns:

Column	Description
Status	An icon representing the connection status. For details, see Connection monitoring.
Name	Unique name of the device.
Model	Model type of the device. Not always displayed, depends on browser width.
Serial Number	Serial number of the device. Not always displayed, depends on browser width.
Group	Group the device wherever it is assigned to.
Registration Date	Date when the device was registered to your account.
System ID	System ID of the device.
IMEI	IMEI of the device.
Alarms	The alarm status of the device, showing number and type of alarms currently unresolved for the device. See Working with alarms for further information on working with alarms.

The devices list displays up to 100 rows. If a list contains more than 100 devices, click "Load more" at the bottom of the list to display the next 100 entries.

When hovering over a row in the list, a "Delete" button appears at the right. Click it to delete the device permanently.

NOTICE
Deleting a device means to remove the device from IoT Extension database including all its generated data. Alternatively, you can arrange all retired devices in one group (see Grouping Devices (Page 85)). This ensures that all reports remain correct. To prevent alarms from being raised for the retired devices, disable connection monitoring. Deleting a device does not delete the data of its child devices.

Searching for devices

IoT Extension includes a full-text search for devices.

Click the "Search" button at the top right and enter a search term into the text-box. IoT Extension returns all devices containing this term in any property (name, model, any fragment...)

Note

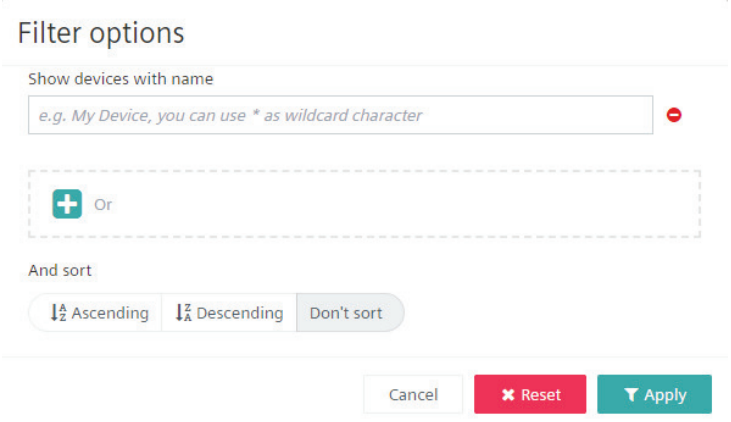
Unlike filtering, the use of wildcards in a search is not supported.

Filtering devices

The device list offers a filtering functionality to filter devices in the list for specific criteria.

Filtering is available on every column. Just click the filter icon next to the name of the column you want to set a filter for.

A window will come up in which you can specify your filter options.



Most columns represent text fields. You can filter these columns by simply entering an arbitrary text into the textbox as in the search field. Click "+ Or" to add another text-box if you want to filter for more than one term.

Apart from filtering for text there are several other options:

- In case of date fields (e.g. Registration date), you specify a date range to filter for.
- In the "Status" column you can filter for various criteria representing the send, push or maintenance status of the device.
- In the "Alarm" column the filtering options you may select correspond to the alarm types (critical, major, minor, warning, no alarms).

In the "Filter options" window, click "Ascending" or "Descending" if you want the devices to be sorted in a specific order. Finally, click "Apply" to carry out the filtering.

The devices list will now only display devices matching the filtering options.

Click "Clear filters" at the right of the top menu bar if you want to clear all filters and view all devices.

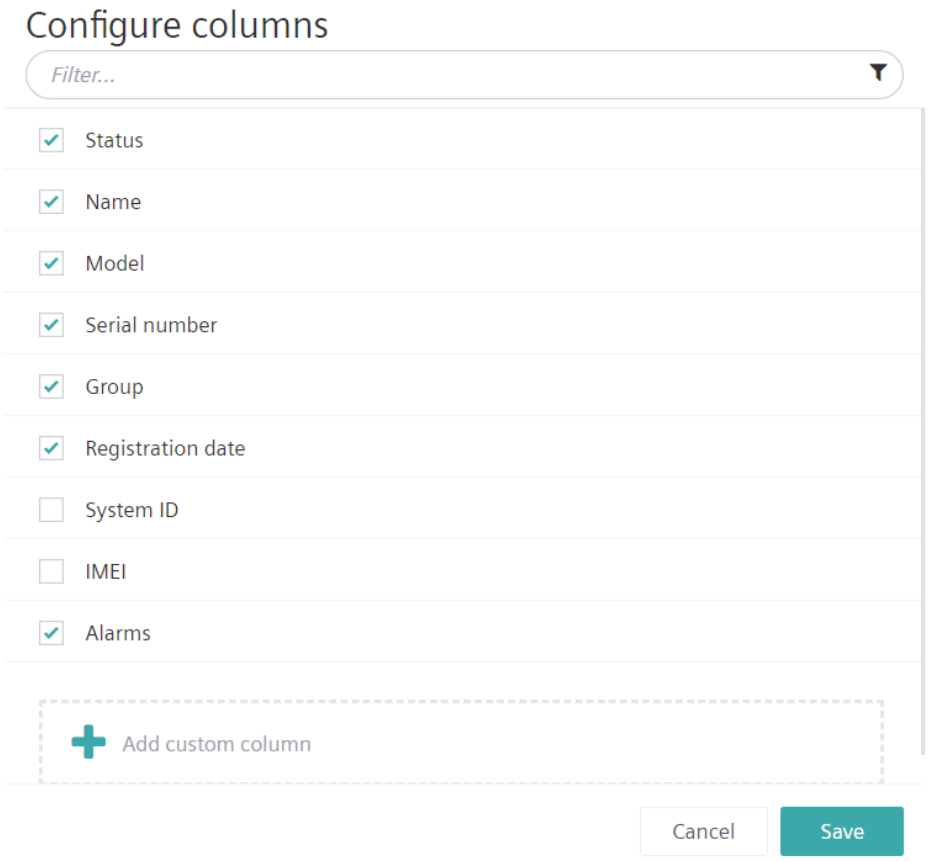
Note

If you select to sort a text field, e.g. device name, in ascending or descending order, keep in mind that the resulting alphabetical sorting is based on ASCII/UTF: A < B < ... < Z < ... < a < b ... < z. Names starting with lower case letters will be sorted below all names with uppercase letters or vice versa

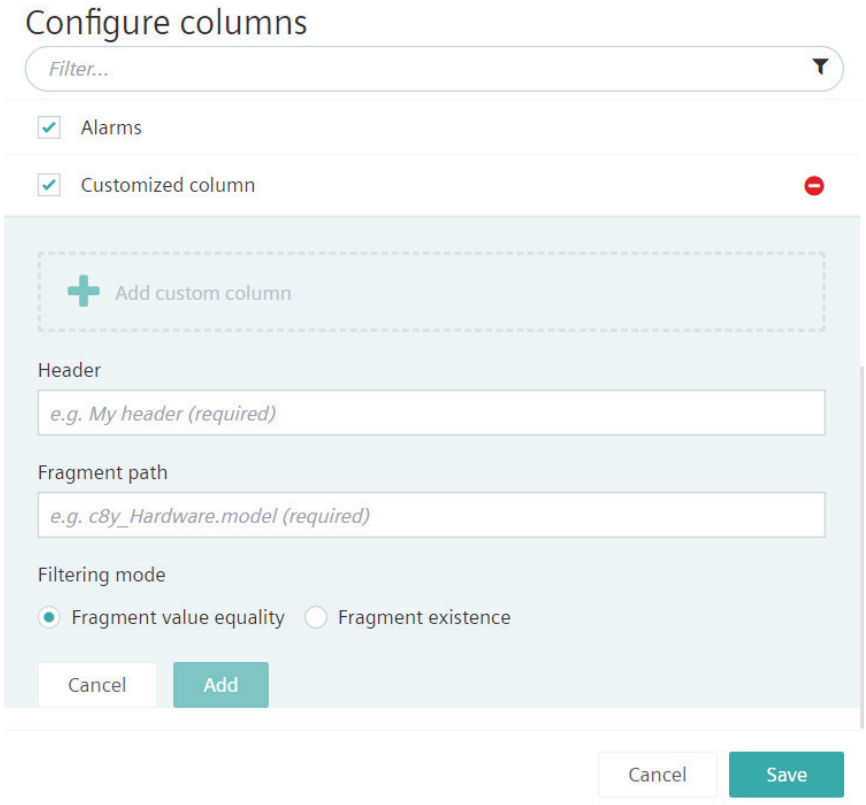
Configuring columns

You can configure the device list columns using the “Configure columns” functionality.

1. Click on the “Configure columns” function.
2. Select or deselect the columns using the checkboxes.



3. Click on the “Add custom column” function to add customized columns.
   – Enter the column “Header” and “Fragment path” values.
   – Select the “Filtering mode” (either “Fragment value equality” or “Fragment existence”).



   – Click “Add” to add your custom column.

Note

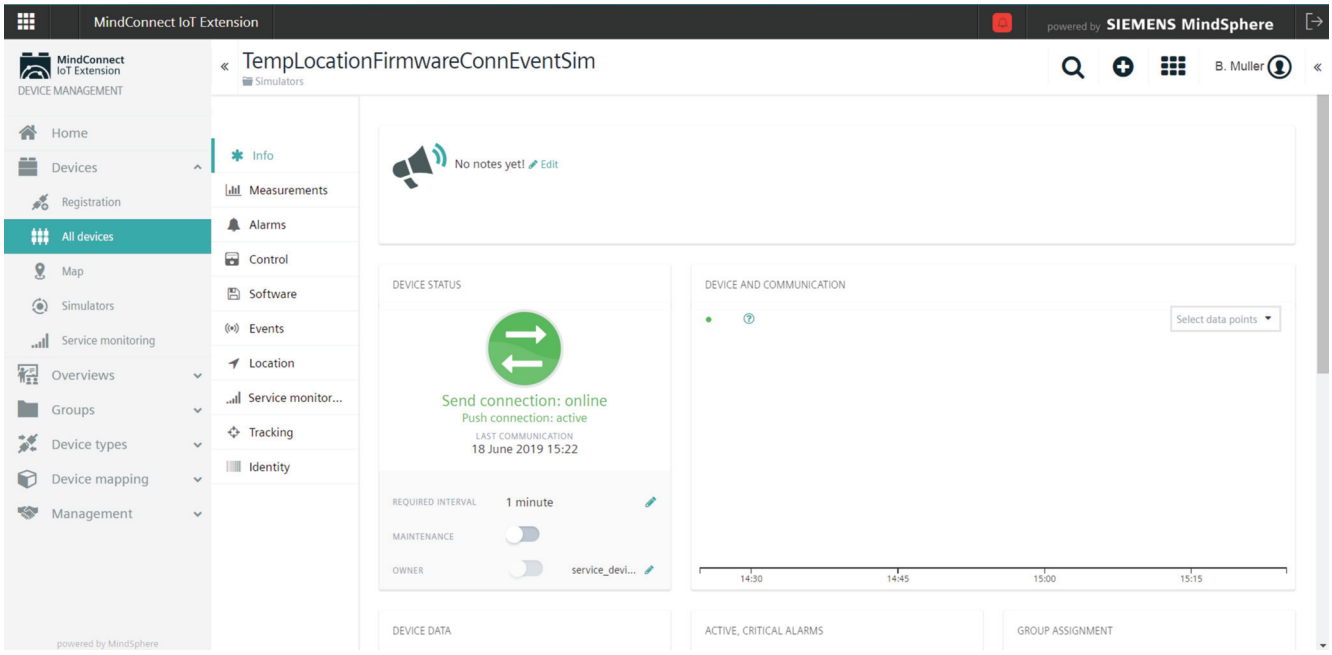
The custom columns can be removed using the delete icon.

4. Finally, click “Save” to save your settings.

5.1.6 Device details

For each device, detailed information is available. The kind of information actually provided for a device depends on the device type, device usage and the configuration of your user interface.

To view detailed information on the device, click a device in the device list.



The device details are divided into tabs. The number of tabs is dynamic and depends on the available information, i.e. tabs are only displayed if the kind of information is available for the particular device.

Initially the Info tab is shown, which offers general information on a device and is available for each device.

Each device at least shows the following tabs: "Info", "Alarms", "Control", "Events", "Service monitoring", "Identity" (also see the tab list below).

The following tabs are the most common ones, each described in detail in a separate section:

Tab	Description
Info	Provides general information on a device. Available for each device.
Child Devices	Lists devices being connected to the current device.
Measurements	Provides a default visualization of numeric data provided by the device in the form of charts.
Alarms	Provides information on the alarms for a device. See also "Working with alarms". Available for each device.
Configuration	Allows manual configuration of device parameters and settings entered in a text format. See also "Configuration Repository for binary configuration".
Control	Displays operations being sent to a device. Also refer to "Working with operations". Available for each device.
Network	Displays network information for a device.
Software	Manages firmware of a device and software installed on a device.
Events	Displays events related to a device, helpful for low-level troubleshooting. Also refer to "Troubleshooting devices". Available for each device.

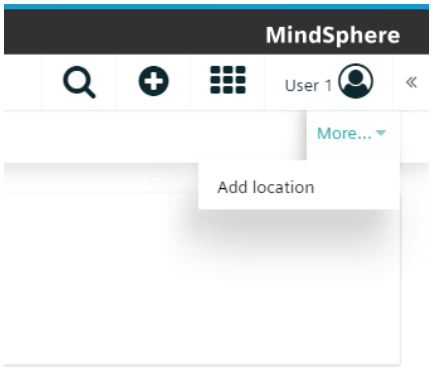
Tab	Description
Location	Shows the location of a device, if available.
Logs	Allows requesting log information for a device.
Service monitoring	Allows the service monitoring of machines. See also "Monitoring services". Available for each device.
Shell	Enables you to interact with remote devices via a command prompt.
Tracking	Shows the movement of a device, if available.
Identity	Displays identities recorded for a particular device. Available for each device.

Note

Potential individual tabs, which you do not find listed here, may be described in a different context and therefore somewhere else in the IoT Extension documentation. Use the Search function to switch to the relevant sections.

Below the name, a list of breadcrumbs is displayed. If the device is part of an asset hierarchy (such as a group), you can use the breadcrumbs to easily navigate up that hierarchy. Since devices can be part of multiple hierarchies, several rows of breadcrumbs may be shown.

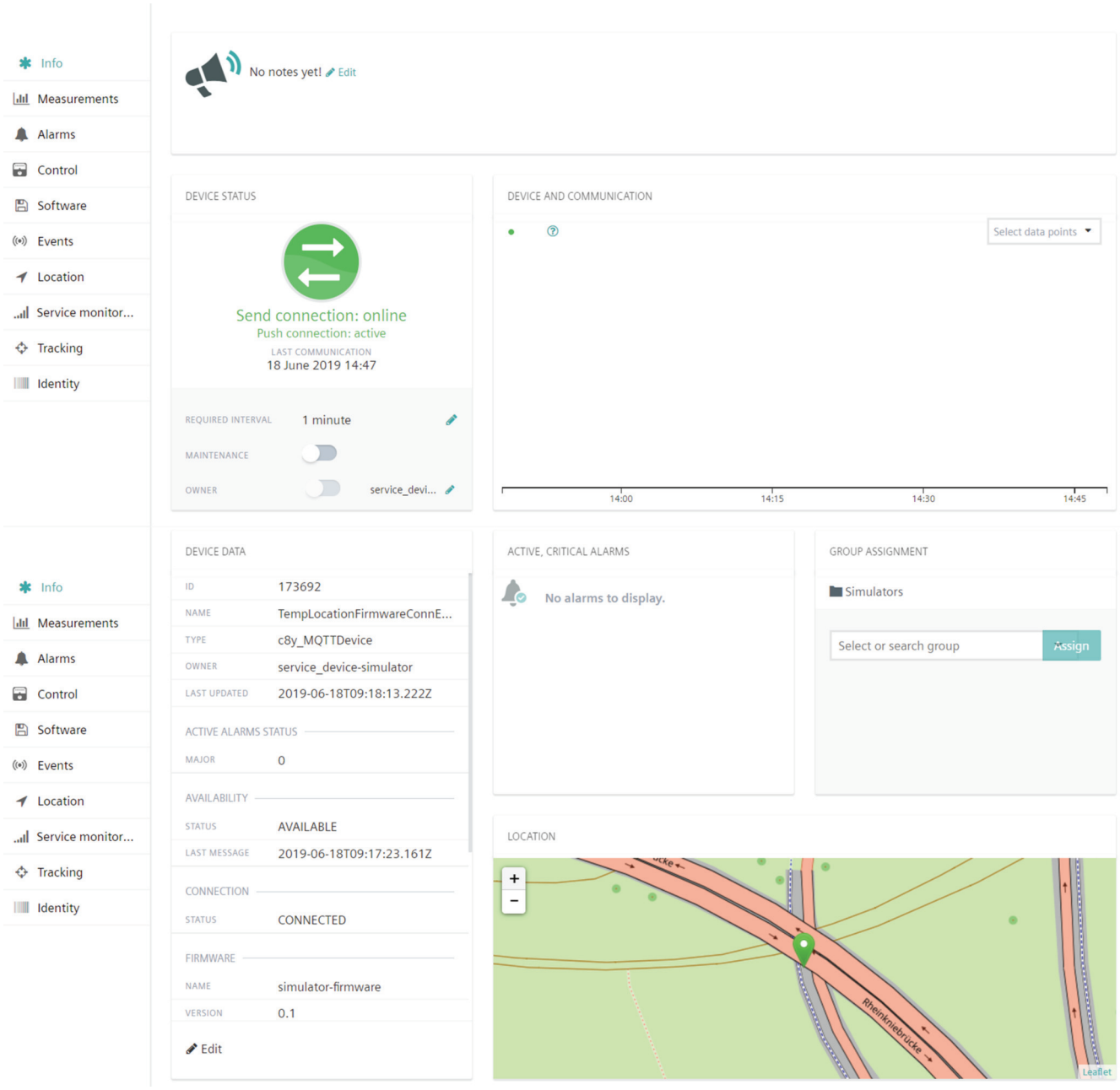
Depending of the type and usage of a device, further actions are provided in a context menu when clicking "More..." at the right of the top menu bar.



Details on these additional menu items are provided where required.

Info

The "Info" tab summarizes management-relevant device information in a dashboard.



The information is provided on the following cards:

Card	Description
Notes	Provides optional notes to inform about current activities. Notes usually may only be edited by an administrator. To add or edit a note, click "Edit", enter your note or your modifications in the text box and save your edits by clicking the green checkmark at the right of the text box.
Device status	Displays connection-relevant information.
Device and communication	Shows a data point graph displaying realtime data on particular measurements. For details on data point graphs, refer to Using the Data Explorer (Page 162) in the Cockpit documentation (Page 139).The following measurements may be shown here: Data points: c8y_Battery.level, c8y_SignalStrength.rssi, c8y_MemoryMeasurement.Used, c8y_CPUMeasurement.Workload, c8y_NetworkStatistics.Upload, c8y_SignalStrength.RCSP, c8y_SignalStrength.ber, c8y_SignalStrength.ECN0, c8y_NetworkStatistics.Download, c8y_MemoryMeasurement.TotalAlarms: c8y_UnavailabilityAlarmEvents: c8y_LocationUpdate
Device data	Displays editable information on the device (name, type, ID, owner, last updated). The fields ID and "Last updated" cannot be edited. Moreover information on hardware (editable) and firmware (not editable) is displayed here if available.
Active, critical alarms	Shows the active critical alarms for the device.
Groups assignment	Displays the groups the device belongs to. Moreover you can add the device to groups here or unassign it from groups. For details on grouping devices see Grouping devices (Page 85).
Location	Shows the location of a device on a map as reported by the device or as manually set.

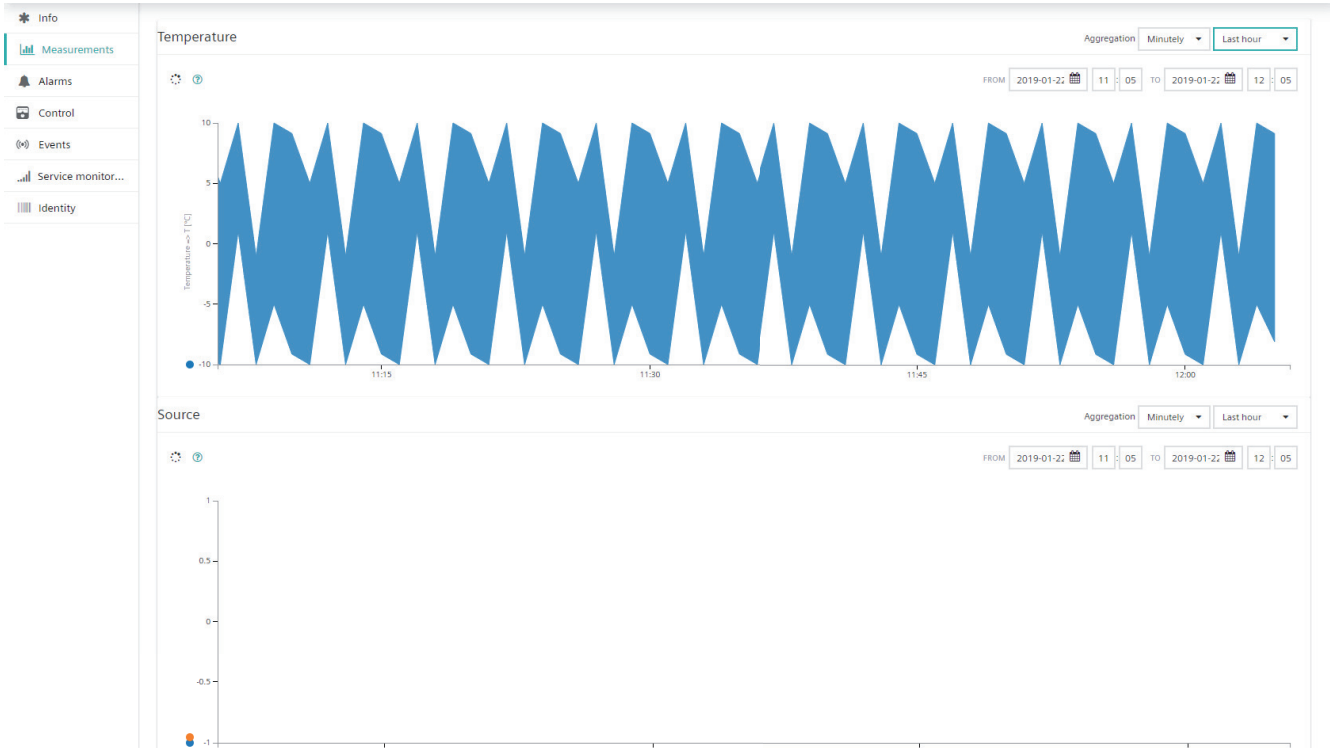
Child devices

The "Child devices" tab shows a list of devices connected to the currently displayed device. For example, if you look at a gateway, the tab lists all machines connected to the gateway.

For details provided in the child device list, refer to Viewing devices (Page 56).

Measurements

The "Measurements" tab provides a default visualization of numeric data provided by the device in the form of charts. Charts are grouped into types of measurements, which can contain multiple graphs or "series". The screenshot below, for example, shows a chart for motion measurement including graphs for acceleration in the three dimensions, and a chart with modem statistics in the form of signal strength and bit error rate.



If a chart contains graphs with different units, one Y-axis is rendered per unit. In the example above, motion measurements consist of three parameters with unit "meter per square second", so only one axis is rendered. Modem statistics consist of signal strength in decibel milliwatts and bit error rate in percent, so one axis is rendered for each graph.

To see detailed information about the measured values, hover over the chart. A tooltip will be displayed with detailed information on the measurement next to your cursor (the tooltip will "snap" to the closest measurement).

Time range and aggregation

By default, charts show the raw data of the last hour. To change the time range on the X-axis, open the "Last hour" dropdown menu at the top right and select a time range.

If you increase the time range, the value in the Aggregation field will automatically switch to "hourly" or "daily". The chart now shows ranges instead of individual raw data points. For "hourly", the chart will show a range of the minimum and maximum value measured in one hour. For "daily", the chart will show the minimum and maximum value measured over one day. Likewise, the tooltips will now show ranges of values instead of individual values.

This enables you to get an efficient overview over larger time periods. A graph will only show 5.000 data points per graph maximum to avoid overloading your desktop browser. If you select a

fine focus resulting in more than 5.000 data points, a warning message will be shown: "Truncated data. Change aggregation or select shorter date range."

Clicking "Realtime" will enable realtime user interface updates of the graphs as new data flows into the system from the connected devices.

You can influence the graphical display and axes limits by setting up so-called "KPIs", see the Administration Guide (Page 13).

Measurement format

In order to see measurement graphs, the device has to send measurements in a specified fragment format.

"fragment_name" : { "serie_name" : { "value" : ... "unit" : ... } }

Example:

"c8y_SpeedMeasurement": { "Speed": { "value": 1234, "unit": "km/h" } }

Fragment_name and serie_name can be replaced by different valid json property names, but no whitespaces and special characters like [ ],* are allowed. The structure has to be exactly as above, two-level deep json object.

Alarms

The "Alarms" tab provides information on the alarms of a device. Refer to Working with alarms (Page 75) for further information on alarms.

Configuration

The text configuration, available in the "Configuration" tab of a device, allows you to configure the parameters and initial settings of your device in a text format.

To manually add or edit a device configuration, follow these steps:

1. Open the details for your desired device.
2. Click the "Configuration" tab.
3. In the text field you can add or edit the device configuration as desired.
4. Click "Save" to save your edits.

Alternatively, you can work with configuration snapshots.

Control

The "Control" tab lists the operations being sent to a device.

Network

In the "Network" tab network settings can be configured for the device.

Software

The "Software" tab allows you to manage and update the firmware of a device and the software installed on a device.

To install a new firmware, click "Install firmware", then select a firmware image from the "Firmware repository" and click "Install".

Similarly, to install a software on the device, click "Install software", select a software package from the "Software repository" and click "Install".

Installing software and firmware usually includes a restart of the device. To monitor the progress of an installation, visit the "Control" tab.

To remove a software from a device, hover over a particular software package and click the "Delete" button.

Events

The "Events" tab displays events related to a device. This enables low-level troubleshooting of a device.

Location

The "Location" tab by default shows the location of a device on a map and as coordinates, as reported by the device. For devices that do not report a location you may manually set the location. Simply place the "pin" in the correct place of the displayed map.

The "Location" tab also shows when a device contains c8y_Position property. When you send a new c8y-position event, you can set the same c8y-Position fragment on the device and it will automatically mark its position on the map.

Logs

In the "Logs" tab you can request log information from devices. Log information can be filtered according to date ranges, log type, keywords and the maximum number of lines to transfer.

In the "Logs" tab, click "Request log file" at the right of the top menu bar.

In the upcoming window, specify the following settings for the log information:

- A date and time range.
- The type of log. The supported logs listed are usually device-specific.
- An optional text to filter the log. For example, if you enter "Users", only lines including the term "Users" will appear in the returned log information.
- The maximum number of lines to be returned (counted from the end). The default value is 1000.

Click "Request" log to request the specified log information for the device.

Note

Requesting a log from a device may take some time.

After the log has been transferred from the device to IoT Extension, it will be listed on the screen. The entry in the list includes the requested log time range.

Click on the entry in the list to show the log information in the screen.

When hovering over an entry, the "Download" and "Delete" buttons appear. Click the "Download" button to download the log excerpt to your local PC. Click the "Delete "button to delete the log file.

Service monitoring

In addition to connection monitoring, IoT Extension offers a separate service monitoring for machines.

Shell

The device shell enables you to interactively work with remote devices. Many industrial devices support some form of command language, be it AT commands for modems, CSV-style commands for many tracking devices or elaborate scripting mechanisms such as Tixi TiXML. In the shell, you can send commands in the respective language of the device and interactively view the results of the commands.

The "Shell" tab presents a command prompt to enter commands.

In the command prompt you can enter arbitrary command text. To send the command text to the device, click "Execute". This button only is activated if the device is online.

Click "View history" at the right of the top menu bar to display a list of the previously executed commands. By default, the last three commands are visible. The list displays status, date and text of a command. Clicking a list item reveals the result of the command (provided it has been executed).

For your convenience, IoT Extension provides several frequently used commands for some devices. Click "Get predefined commands" at the right of the top menu bar to open a window containing a list of available pre-defined commands. Select the command of your choice and click "Use", to copy the command to the command prompt, or "Execute", to execute the command straight away. You may also add new commands here for re-use.

Tracking

Devices can record the history of their movements in IoT Extension. This movements may be viewed in the "Tracking" tab.

Note that the "Tracking" tab only shows up when a device contains c8y_Position property.

In the dropdown list at the top right you can select a time period (or specify one by selecting Custom from the list) and visualize the movements of the device during this period. Movements are shown as red lines in the map.

Next to the map, the individual recordings with their time are listed ("location update events"). When you click a recording, a "pin" on the map will show the location at the time of the recording.

Depending on the type of device and the integration into IoT Extension, you can configure device-side geo-fencing and motion detection.

Note

When this feature is activated and the device is compatible, Cell ID information can be used to determine the position of the device. Currently, the services from Combain and Google are supported. The user can see the tracks based on both data, or filter out GPS based data or Cell ID based data.

Identity

IoT Extension can associate devices and assets with multiple external identities. For example, devices can often be identified by the IMEI of their modem, by a micro-controller serial number or by an asset tag. The Identity tab lists all the identities recorded for a particular device.

This is useful, for example, when you have non-functional hardware and need to replace the hardware without losing the data that was recorded. Just connect the new hardware to your account and modify the identity entry of the old hardware, to contain the identity of the new hardware.

5.1.7 Working with simulators

With the IoT Extension simulator all aspects of IoT devices can be simulated:

- Setting up a simulated device or a network of simulated devices
- Specify which operations the device can process
- Create work instructions based on predefined message templates or user defined templates and schedule work steps
- Create up to ten devices of a defined type
- Generate messages for measurements, alarms, events and inventory
- View simulation problems as alarms

You require Simulator admin role to access and work with simulators.

What is a simulator?

With the simulator you can create artificial devices that have the same level of functionality as connected hardware devices.

A simulator uses a playlist to simulate messages that the device sends to the IoT Extension platform. A playlist is a series of instructions that the simulator executes one after the other. When the last instruction is reached, the simulator starts again with the first one.

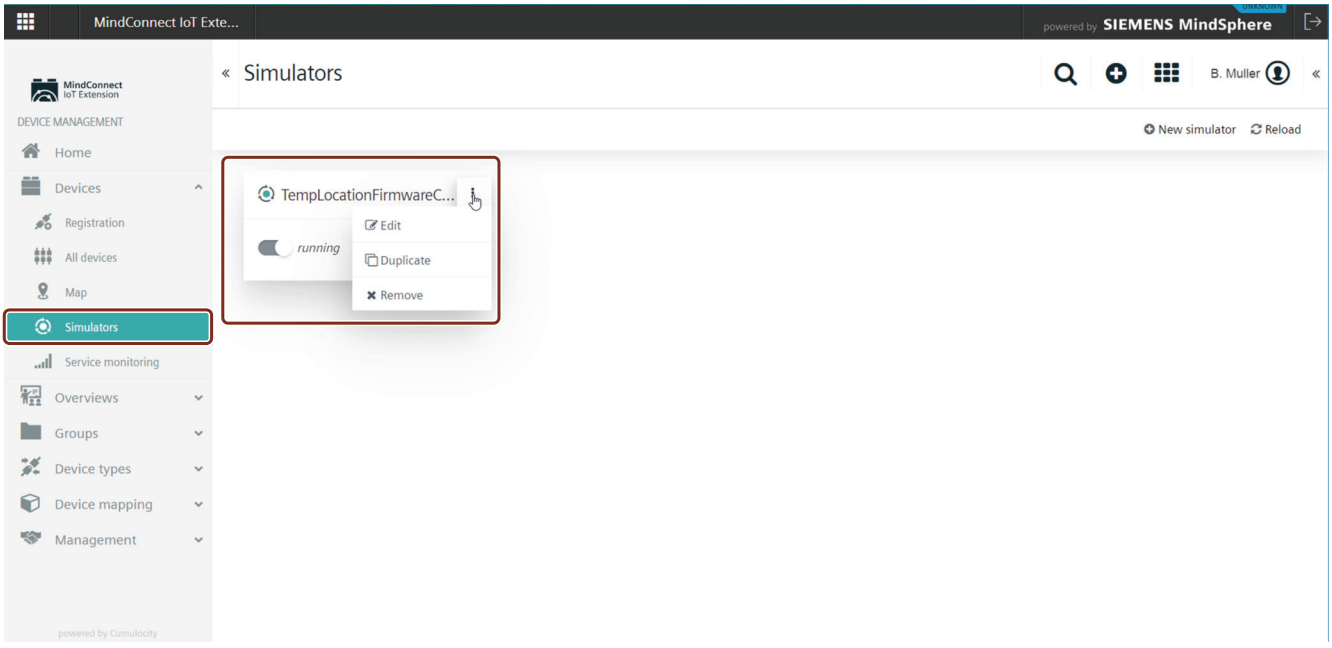
An instruction can either send a message (measurements, alarms, events and inventory) or wait for a specified time (sleep).

A message is defined by choosing a message template (like sending a temperature) and providing the values for this template (23.0 degrees). Many predefined message templates are provided, i.e. for creating a measurement, sending an event, creating and cancelling an alarm. These templates are based on MQTT static templates. Additionally, custom message templates can be defined using the SmartREST template editor.

The Simulator tab

In the navigator, click "Simulator" in the Devices menu to open the "Simulator" page.

All simulators which you can access will be listed here. Click the menu icon at the top right of a simulator card to open a context menu from where you can edit, clone or remove a simulator.



How to create a simulator

To set up a new simulator follow these steps:

1. Click New simulator at the right of the top menu bar.
2. In the upcoming window select a simulator type from the dropdown list in the "Presets" field. Select "Empty simulator" to create a simulator from scratch or select one of the sample simulators.
3. Enter a meaningful name for the simulator.
4. Select the number of instances for this simulator (up to ten).
5. Click "Continue" to proceed to the next dialog.

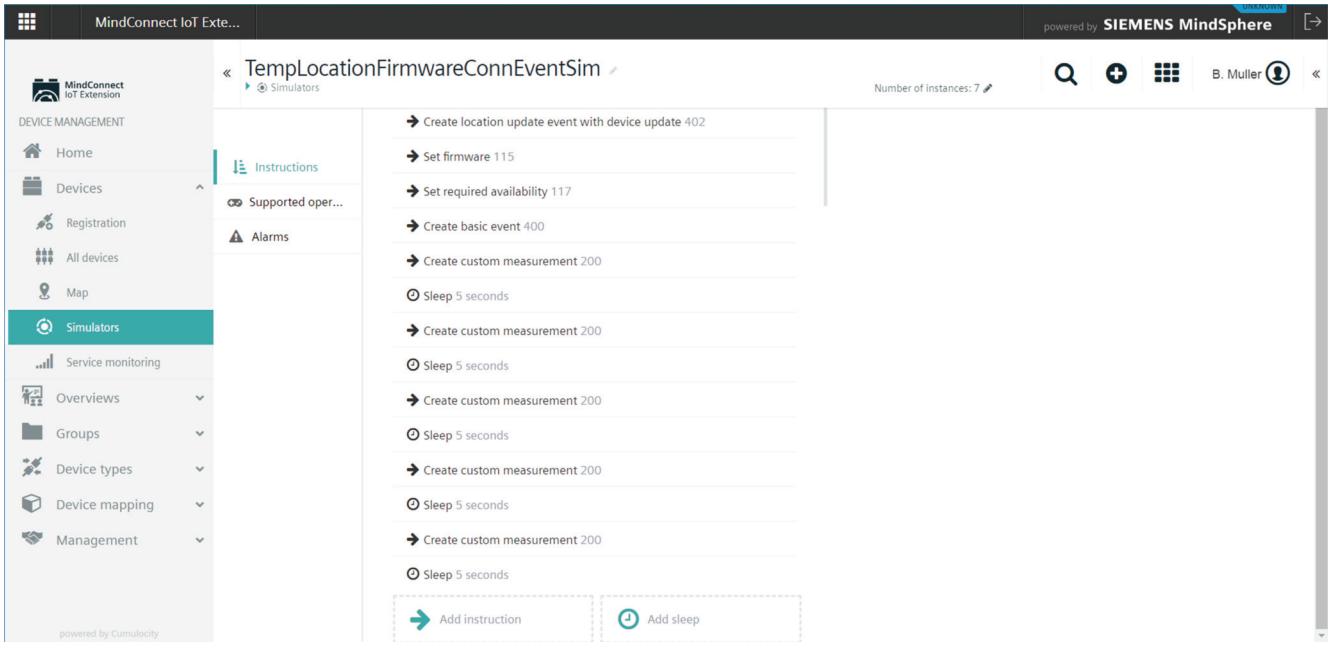
Instructions

After setting up a simulator you can add instructions which define what your simulator is supposed to do. Instructions are single tasks added to a playlist through which the simulator will work.

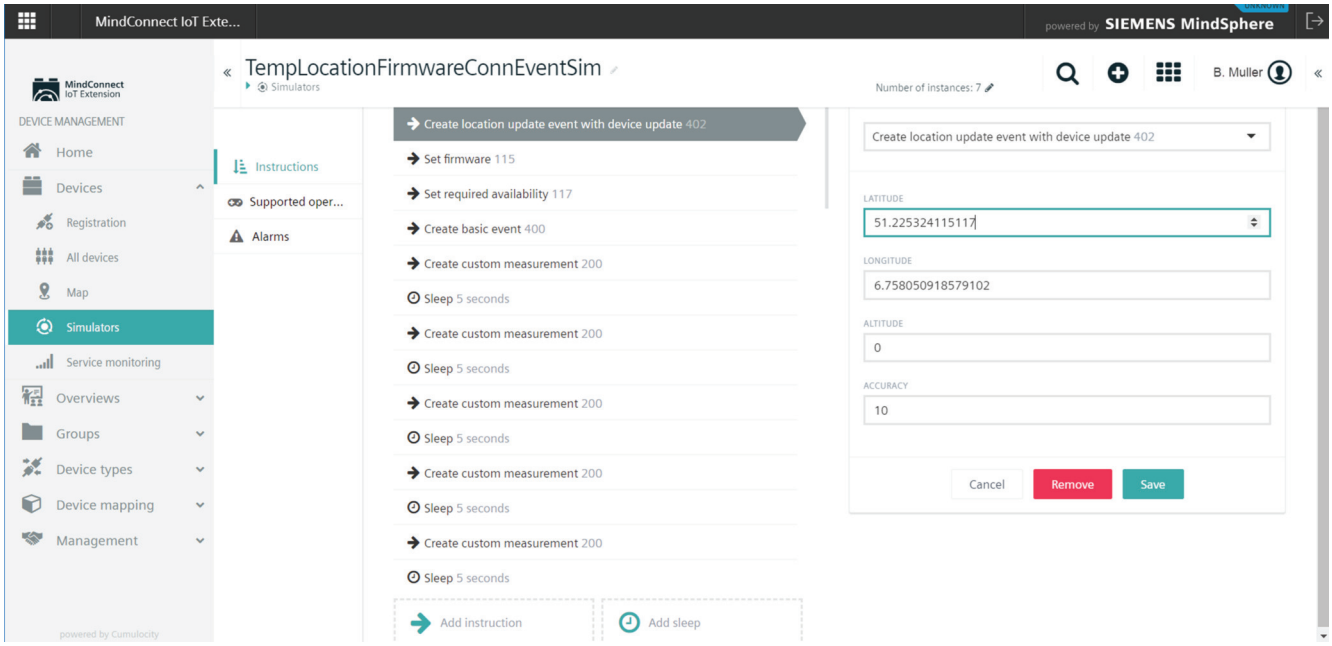
Instructions can be viewed and edited on the "Instructions" tab of the simulator.

Examples

Within the presets, samples instructions are already added. For example, the "Temperature measurement" preset already has instructions in it for the steps "Create measurement" and "Sleep".

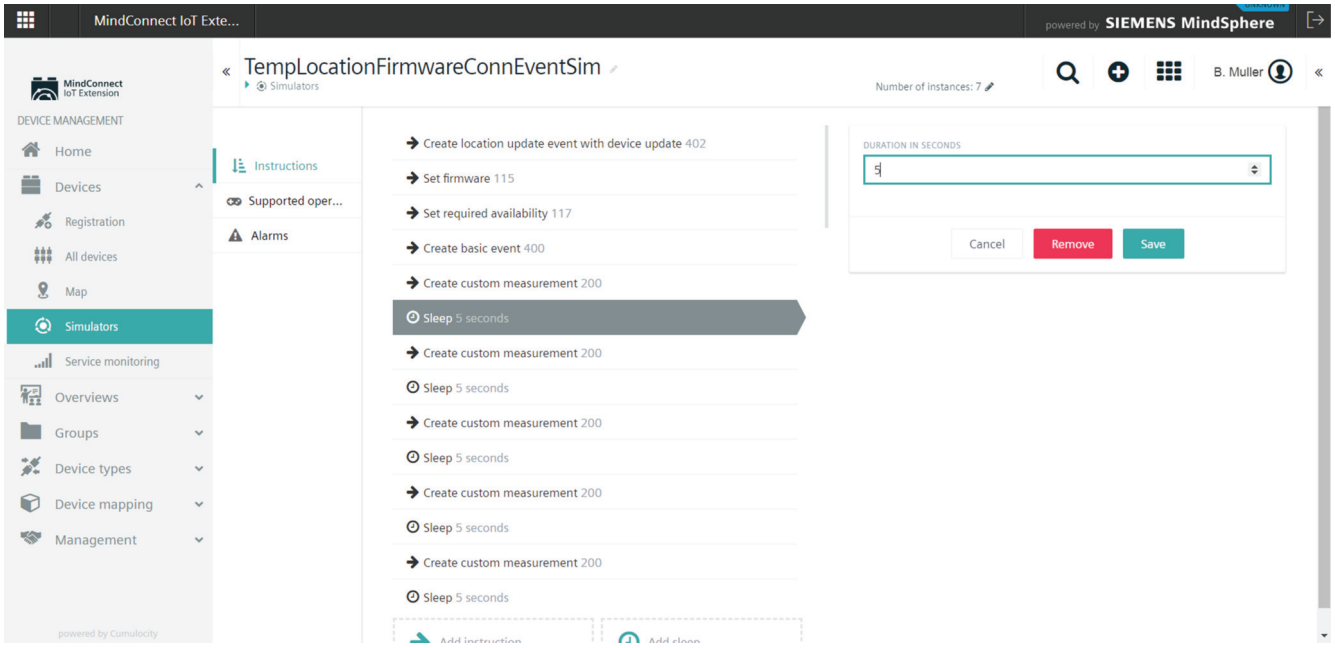


The measurement instruction refers to a fragment. Fragments are used to identify capabilities of a managed object.



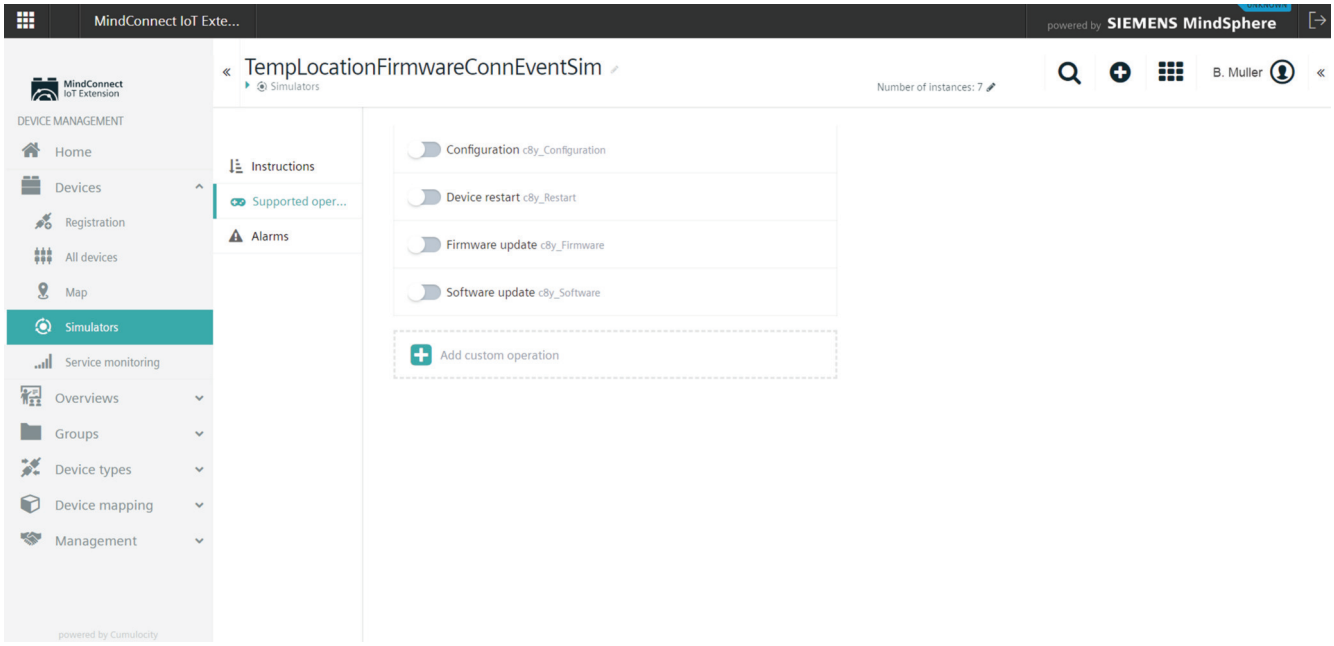
The "Sleep" instruction requires value to define its duration in seconds.

The panel on the right changes according to the type of instruction selected on the left.



Supported operations

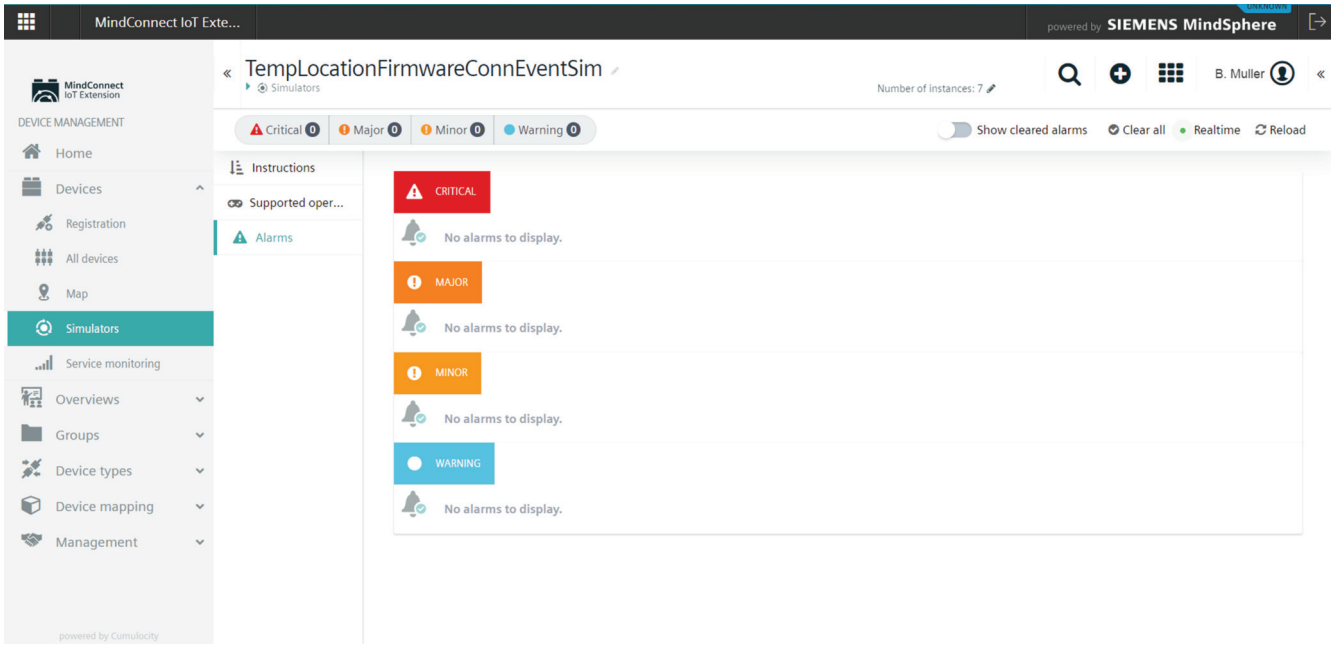
In the "Supported operations" tab of a simulator you can turn on or off specific operations like configurations or software/ firmware updates.



Click "Add custom operation" to specify a customized operation and add it to the list.

Alarms (simulator)

The "Alarm" tab of a simulator displays alarms related to the simulator itself (not to the simulated device), i.e. if the simulator itself does not work correctly, you will find alarms here. Refer to Working with alarms (Page 75) for information on alarms.



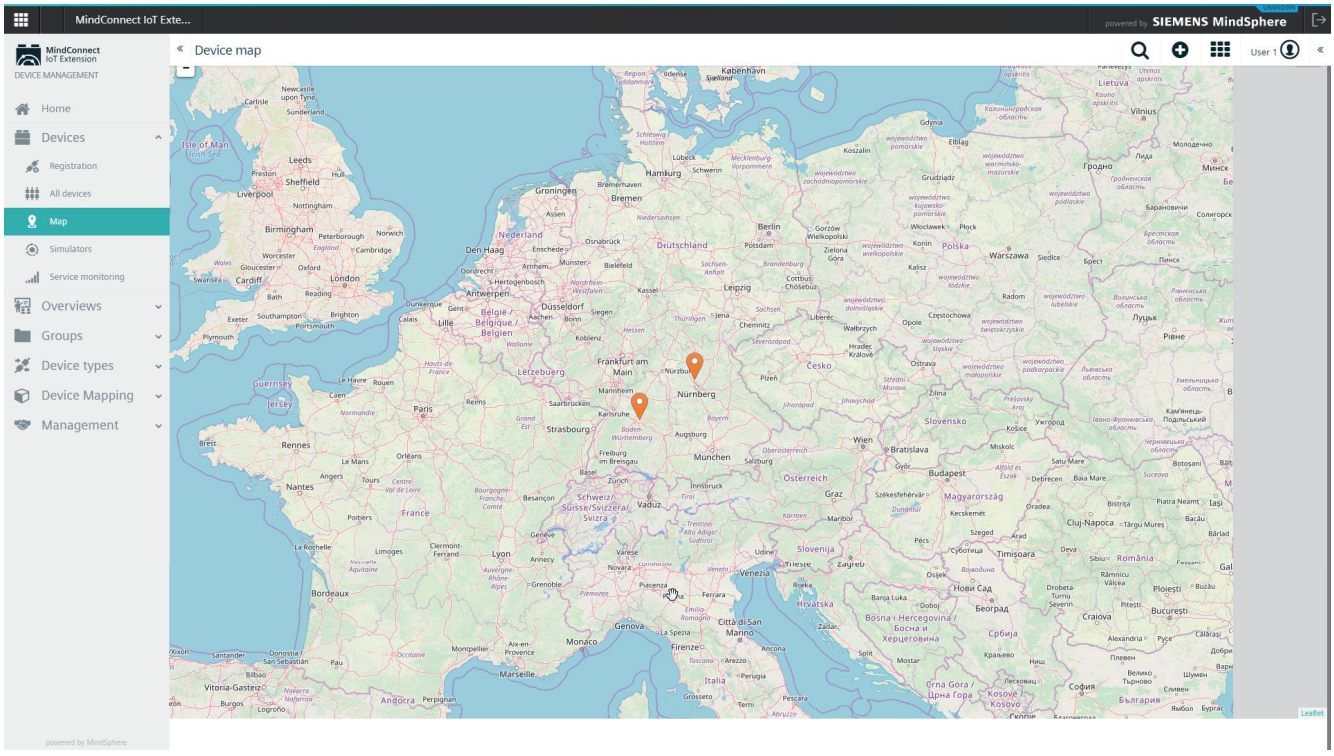
5.1.8 Monitoring and controlling devices

Locating devices

IoT Extension provides the option to view all devices in your account on a map.

Click "Map" in the Devices menu in the navigator to display a map showing all devices in realtime.

Devices are represented as "pins". Click a pin to see the name of the respective device. Click the device name to switch to the device details.



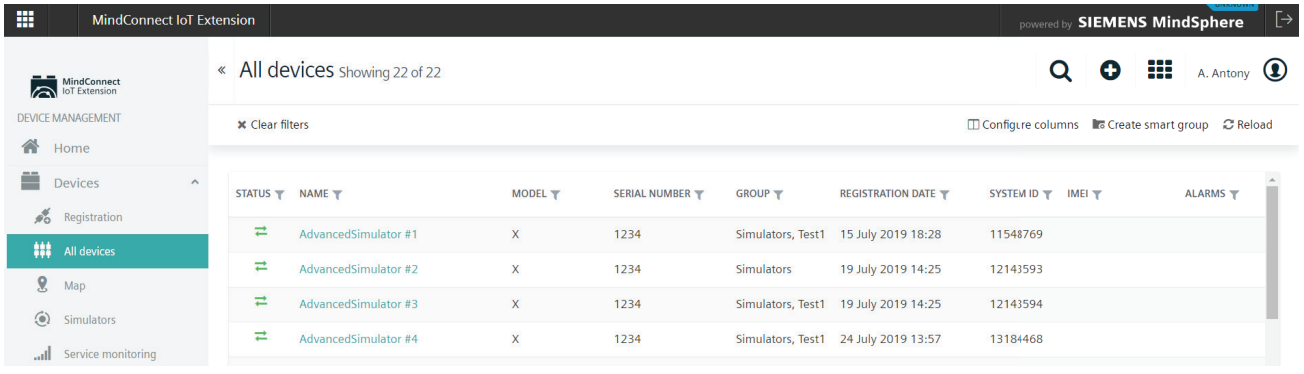
Connection monitoring

In the "Device Management" application you have the option to monitor the connections to your devices.

This can be done at the level of individual devices (see below) or across multiple devices in a list.

To monitor the connections for multiple devices, open any device list.

The connection status is represented by arrows in the "Status" column in the device list.



Send connections

The top arrow represents the "Send connection" (traffic from the device to IoT Extension). The status for the "Send connections" may be one of:

- "Online" (data was sent within the required interval)- indicated by a green arrow
- "Offline" (data was not sent within the required interval) - indicated by a red arrow
- "Unknown" or not monitored (no interval configured) - indicated by a grey arrow

Hovering over the arrow displays the timestamp of the last request from the device to the server.

When a device is detected to be offline (stops sending data within required interval and top arrow changes to red color), an unavailability alarm is created for the device reading "No data received from device within required interval".

Push connections

The bottom arrow represents the "Push connection" (from IoT Extension to the device). The status for the "Push connections" may be one of:

- "Online" (connection established)- indicated by a green arrow
- "Offline" (connection not established) - indicated by a red arrow
- Not monitored - indicated by a grey arrow

Note

The Push connection means the connection from IoT Extension to /devicecontrol/notifications API, not to realtime API.

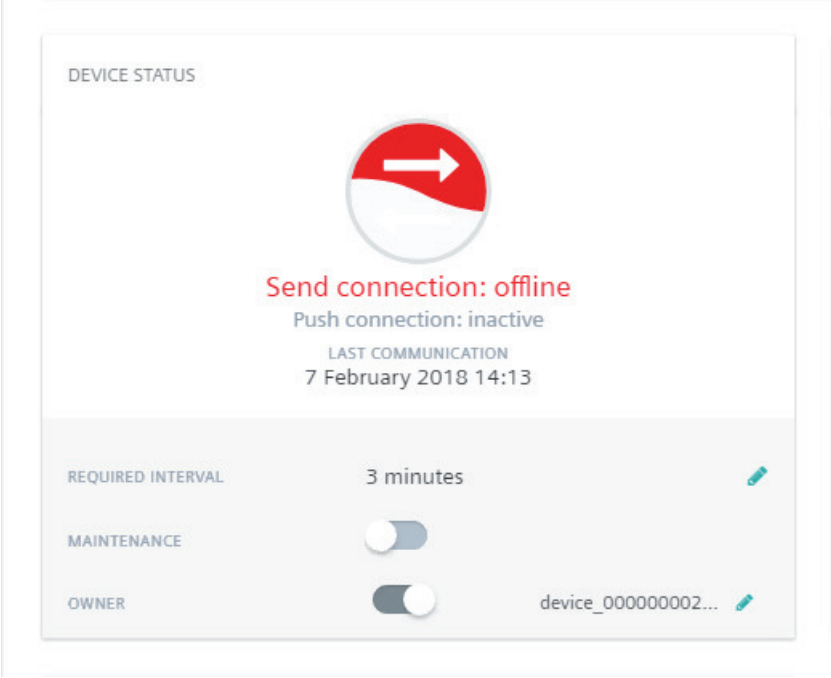
Maintenance mode

Moreover, the device may be in "Maintenance" mode, indicated by the tool icon in the Status column. This is a special connection status indicating that the device is currently being maintained and cannot be monitored. While a device is being maintained, no alarms for that device are raised.

You can turn maintenance mode on or off for a device through a slider in the "Connection monitoring" card in its Info tab.

Connection monitoring in the "Info" tab

To monitor the connections of a particular device, go to the Info tab of this device. Under "Device status", the connection status for the device is displayed.



Below the send connection and push connection status, the time of the last communication is displayed.

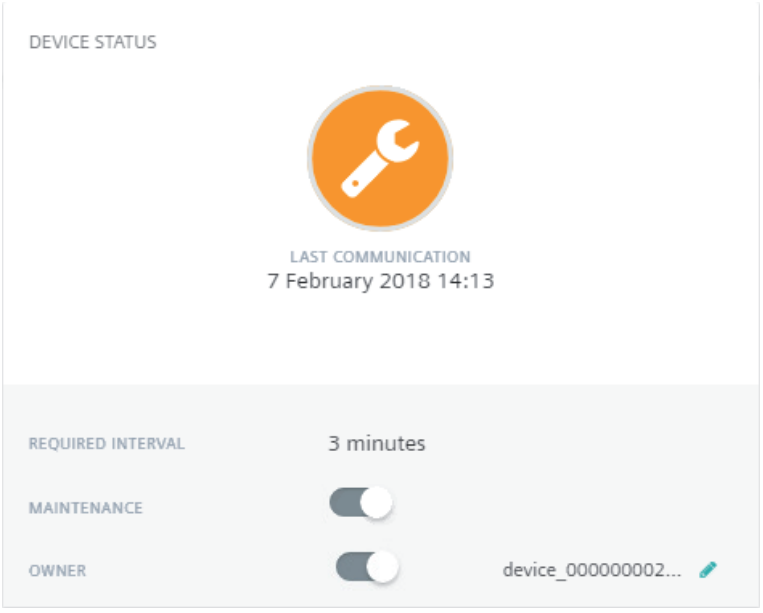
Note

"Last communication" and "Last updated" are two entirely different time stamps. "Last communication" indicates when a device has last sent data. "Last updated" indicates when the inventory entry of the device was last updated. This update may have originated from the device, from the web user interface or from another application.

In the "Required interval" field you can specify an interval. This parameter defines how often you expect to hear from the device. If, for example, you set the required interval to 60, you expect the device at least to communicate once in an hour with IoT Extension. The interval is either set by the device itself, based on the device's knowledge how often it will try to send data, or it is set manually by you.

If an interval is set, you will find the "Maintenance" slider below it.

With the "Maintenance" slider you can turn the maintenance mode for the device on or off which is immediately reflected in the connection status.



Note

Connection monitoring is not realtime. This means that the connection status will not change immediately when you switch off a device. Depending on your network, it may take about 20 minutes until a broken connection is discovered, since the network will retry sending data for a significant amount of time.

Service Monitoring

IoT Extension distinguishes between connection monitoring and service monitoring. Connection monitoring, as described in the previous section, only indicates if the device is communicating with IoT Extension, it does not automatically indicate if it is functional or not.

"Service monitoring" indicates if a device is in service. For example, a vending machine is in service if it is ready to sell goods. A vending machine can sell goods using cash money without a connection to IoT Extension. From the perspective of a merchant, it is in service. Similar, if you switch off the power on a gateway, the devices behind the gateway can still continue to work.

IoT Extension considers a device to be in service while there is no critical, unresolved alarm present for the machine. This is displayed as a share of time such an alarm was present. If a machine didn't have any critical alarms whatsoever during a time period, it was 100% in service. If half of the time there was some critical, unresolved alarm, the machine was 50% in service.

While a machine is offline, IoT Extension assumes by default

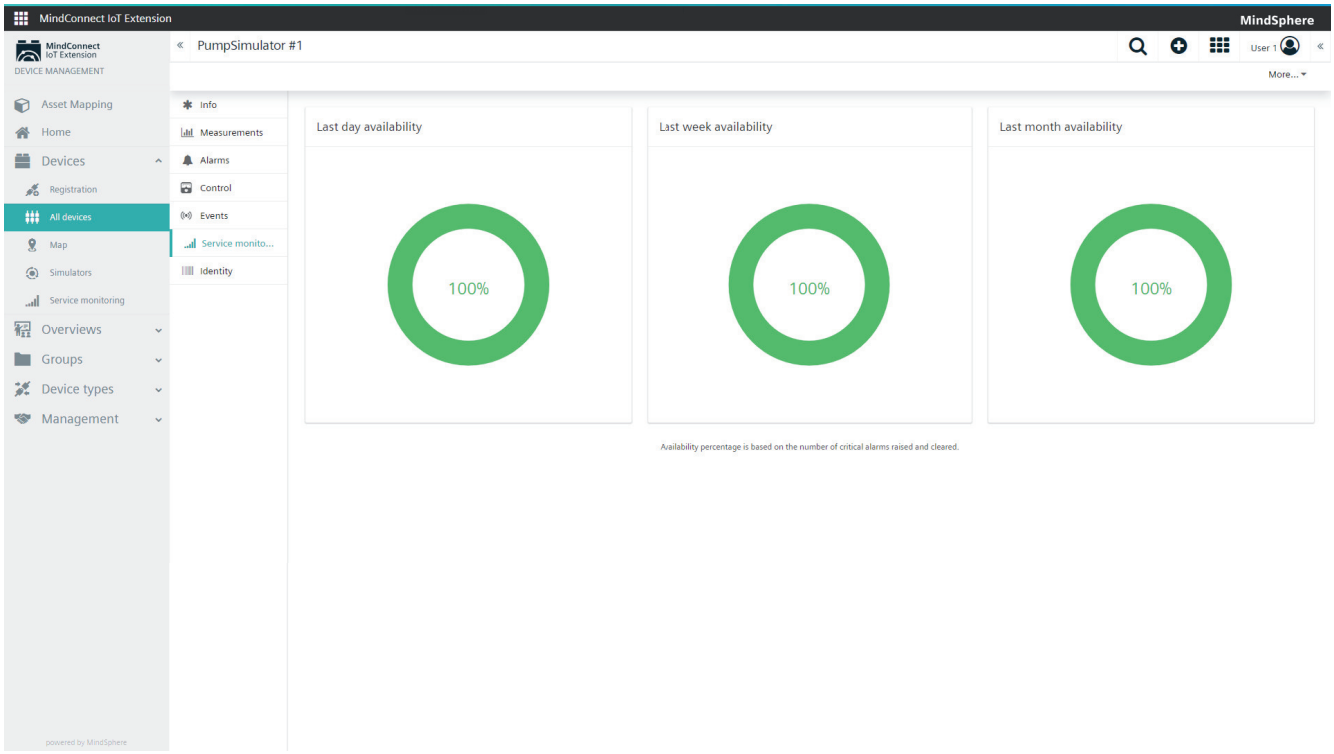
- that the machine continues to stay in service during the connection outage, if this was the status before it lost connection.
- that the machine continues to stay out of service, if this was the status before it lost connection.

There may be exceptions from this rule. If your vending machines rely exclusively on cashless payment, losing the connection to the network means that your machine is out of service and stops selling. In this case, unavailability alarms must be set in the "Administration" application which have CRITICAL severity instead of MAJOR severity.

IoT Extension displays service availability at the level of individual devices and across all devices.

To check the service monitoring of this specific device, click the "Service monitoring" tab in the details of a particular device.

To display the overall service across all devices, click "Service monitoring" in the navigator.



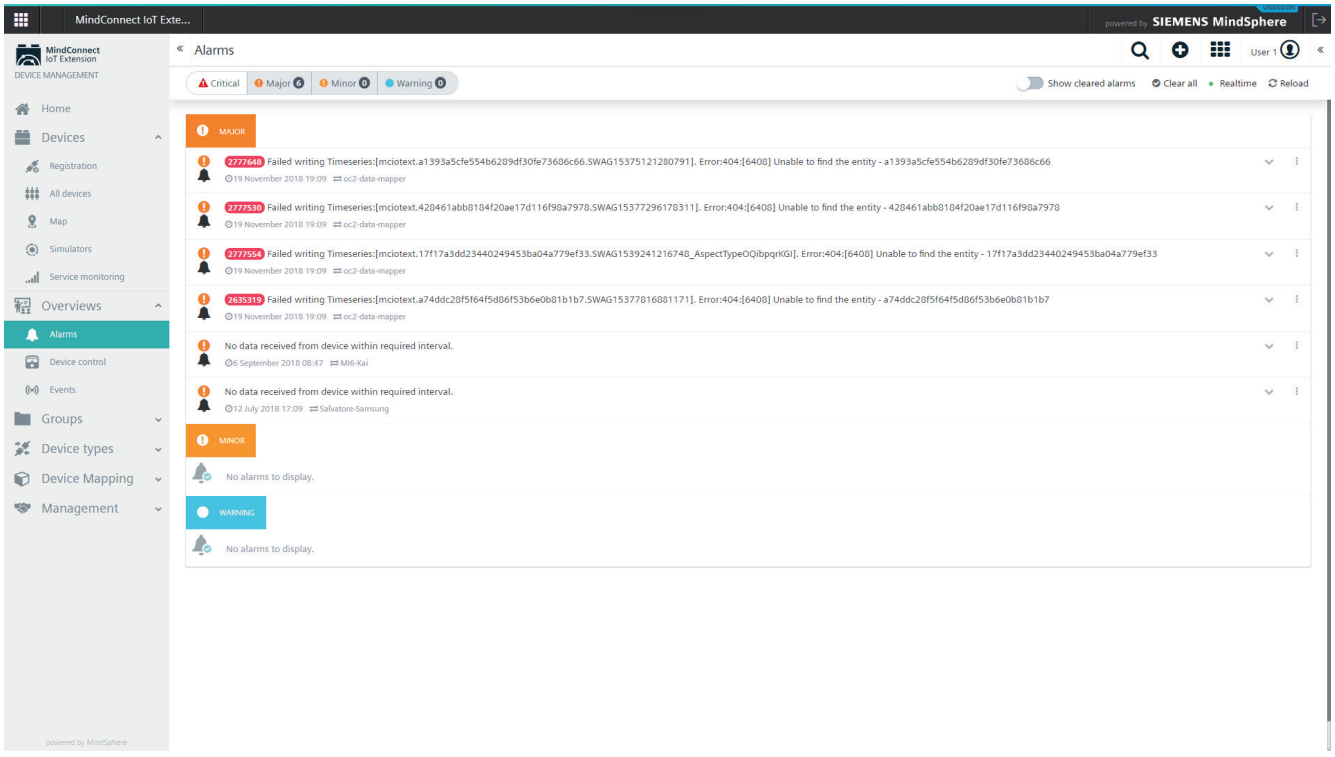
The "Service monitoring" page shows the availability percentage of devices for the last day, last week and last month.

Working with alarms

Devices can raise alarms to indicate that there is a problem requiring an intervention.

IoT Extension displays alarms at the level of individual devices and across all devices:

- Click "Alarms" in the overview menu in the navigator, to check the alarms for all devices.
- Switch to the "Alarm" tab in the details of a particular device, to check the alarms of this specific device.



By default,

- only unresolved alarms are shown. If you turn on "Show cleared alarms" at the right of the top menu bar, you will see the entire alarm history.
- alarms are shown as coming in from the devices in realtime. Click "Realtime" in the top menu bar to disable realtime updates.

Alarms are classified according to their severity. IoT Extension includes four different alarm types:

Severity	Description
Critical	The device is out of service and should be fixed immediately.
Major	The device has a problem that should be fixed.
Minor	The device has a problem that may be fixed.
Warning	There is a warning.

The "Alarm" tab is split into four sections corresponding to these alarm types.

By clicking one of the buttons at the top, the corresponding section will be hidden. Click it again to show the section again.

Within each section, the alarms are sorted by their occurrence, displaying the most recent alarm first.

In each row, the following information for an alarm is provided:

Info	Description
Severity	One of "critical", "major", "minor", "warning" (see above).
Count	The number of times this alarm was sent by the device. Only one alarm of a particular type can be active for a certain device. If another alarm of the same type is sent by the device, the number is increased by 1.
Description	An arbitrary text describing the alarm.
Status	The status of the alarm. An alarm can be: • "Active": When it was raised and nobody is so far working on the alarm. • "Acknowledged": When someone changed the status to "Acknowledged" to indicate that someone is working on the alarm. • "Cleared": When either someone manually set the status to "Clear" or when the device detected by itself that the problem has gone.
Last occurrence	Timestamp of the last occurrence of the alarm (device time).
Device	The name of the device. Clicking the name leads you to the detailed view of the device.

Click the arrow on the right of a row to expand it and display further details on the alarm.

- "Status": Providing further information on the alarm status and showing the type of the alarm. The type info is used for duplicating alarms and for configuring the priority of alarms in the "Administration" application
- "Change Log": Providing the server time when the alarm was created, which may differ from the device time.

To change the status of an alarm, hover over it and click the button for the desired status or click the menu icon and from the context menu select the desired status.

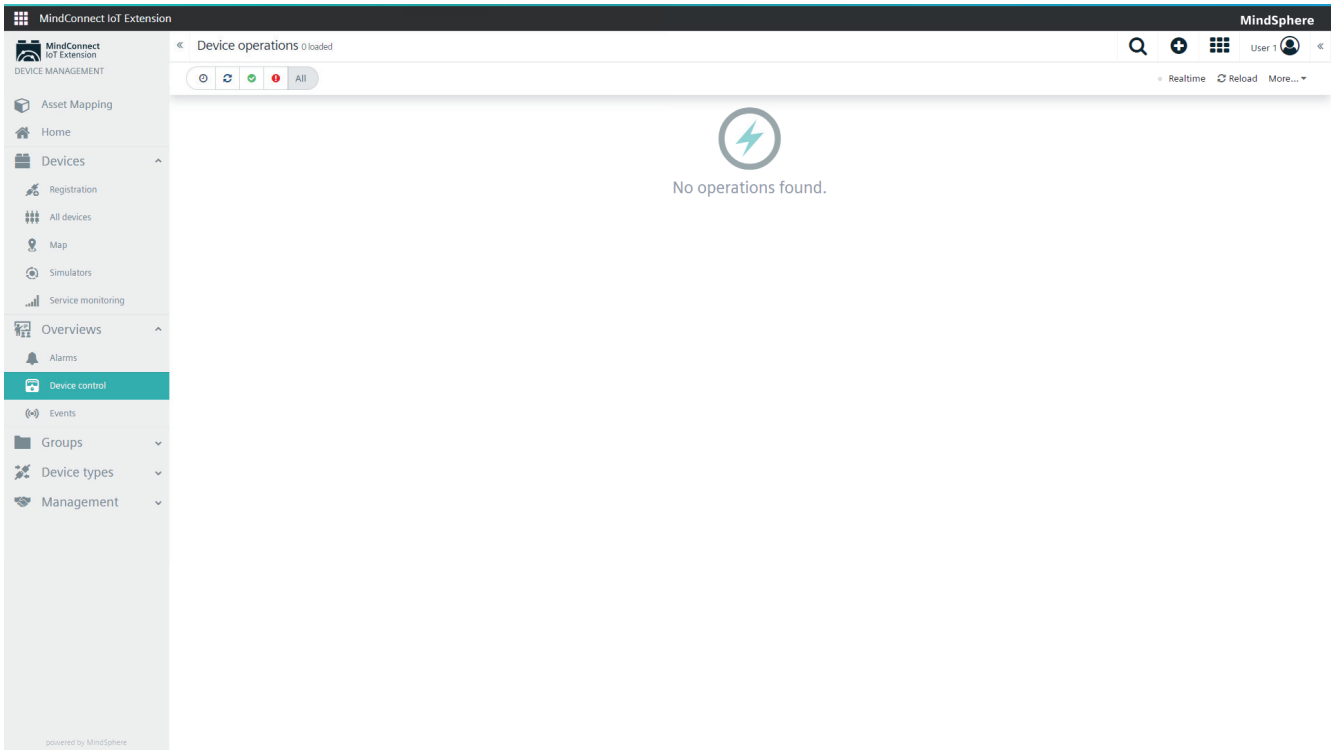
It is also possible to change the status of all alarms to "clear" at once. Click "Clear all" in the top menu bar, to clear all alarms of the selected severities.

Working with operations

Operations are used to remote control devices.

IoT Extension displays operations at the level of individual devices and across all devices:

- Click "Device control" in the Overview menu in the navigator to see the operations for all devices.
- Switch to the "Control" tab in the details of a particular device to see the operations of this specific device.



Operations can be in any of four states, indicated by meaningful icons:

State	Description
Pending	The operation has just been created and is waiting for the device to pick it up.
Executing	The operation has been picked up by the device and is being executed.
Successful	The operation has been successfully executed by the device.
Failed	The operation could not be executed by the device.

By clicking one of the state buttons at the top, the corresponding operations will be hidden. Click it again to show the operations again.

Click "Realtime" at the right of the top menu bar to see operations coming in from the devices in realtime.

Operations are listed in descending time order. Operations are executed strictly according to this order.

For each operation, the following information is provided:

Info	Description
Status	One of "pending", "executing", "successful", "failed" (see above).
Name	Name of the operation.
Device	The name of the device. Clicking the name leads you to the detailed view of the device.

Clicking a row expands it and displays further details on the operation.

- "Details": Providing information on the operation name and status. In case of status = FAILED the reason for the failure is provided.
- "History of Changes": Providing information on the past changes of the operation.

Bulk Operations

For easier handling of devices, IoT Extension offers bulk operations. With bulk operations you can at once execute operations for each device within one group.

To execute bulk operations for a group, follow these steps:

1. Select a device and open the "Control" tab.
2. Create an operation.
3. Hover over the operation you want to execute.
4. Click the menu icon.
5. In the context menu click "Execute" for whole group.

In order to view the status and progress of your operations, simply select the desired group and click the "Bulk operations" tab.

To edit a bulk operation, follow these steps:

1. Hover over the bulk operation you want to edit and click the menu icon.
2. In the context menu click "Edit operation schedule".
3. In the upcoming window you may change the "Start date" and "Delay values".
4. To change operation details, click "Show operation" details.
5. Click "Reschedule" to apply your changes.

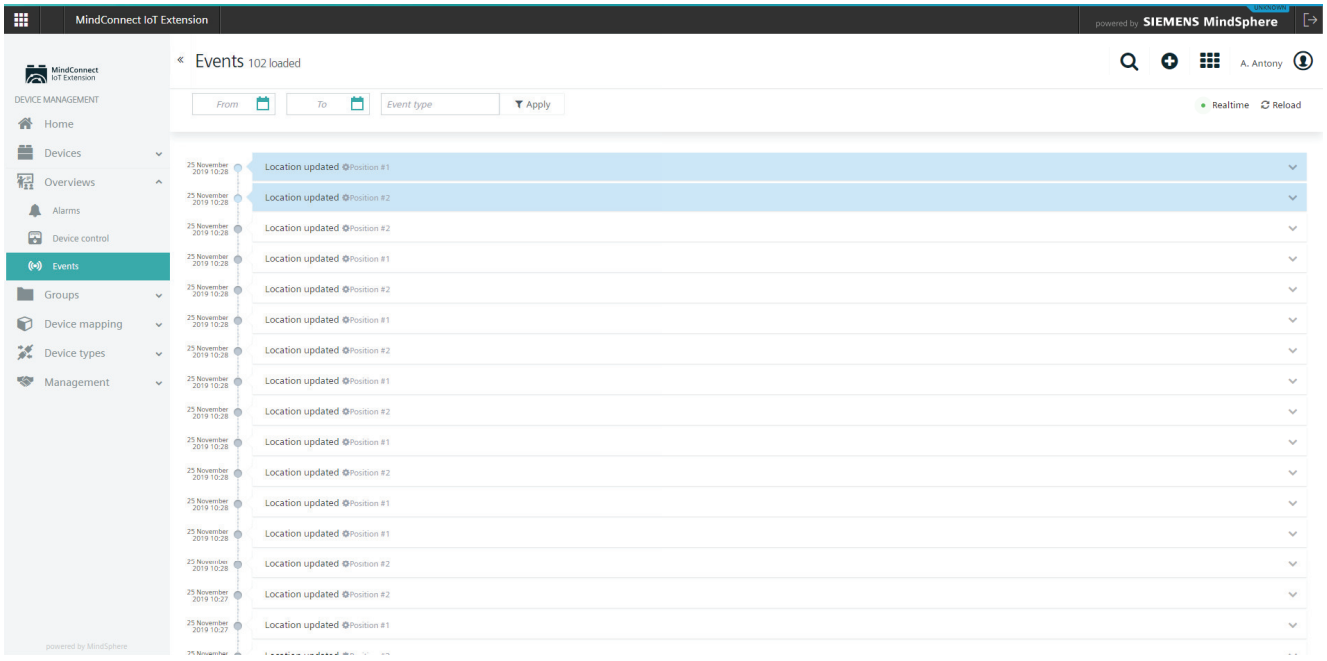
To delete a bulk operation, hover over the bulk operation you want to delete and click the menu icon. In the context menu, click "Cancel operation".

Troubleshooting devices

Troubleshooting devices at a more detailed level can be done with the help of events. Events are low-level messages sent by devices that are usually used for application-specific processing. For example, a vending device sends its realtime sales in the form of events.

IoT Extension displays events at the level of individual devices and across all devices:

- To see the events of this specific device, click the "Events" tab.
- To see the operations for all devices, click "Events" in the overview menu in the navigator.



Per default, events are shown as coming in from the devices in realtime. To disable realtime updates, click "Realtime" at the right of the top menu bar.

For each event, the following information is provided:

Info	Description
Timestamp	Timestamp when the event has been executed.
Name	Name of the event.
Device	The name of the device sending the event. Clicking the name leads you to the detailed view of the device.

In the event list the latest entry is displayed on top.

Clicking a row expands it and displays further details on the event (as type and position of the device).

Since devices may send large amounts of event data, you can filter the data to be displayed by date.

Select a start date and an end date from the fields in the top menu bar and click the "Filter" button to apply the filter. You can filter the events based on the types by entering the event type in the "Event type" field. Click the "Clear" button to clear the filter again.

5.2 Grouping devices

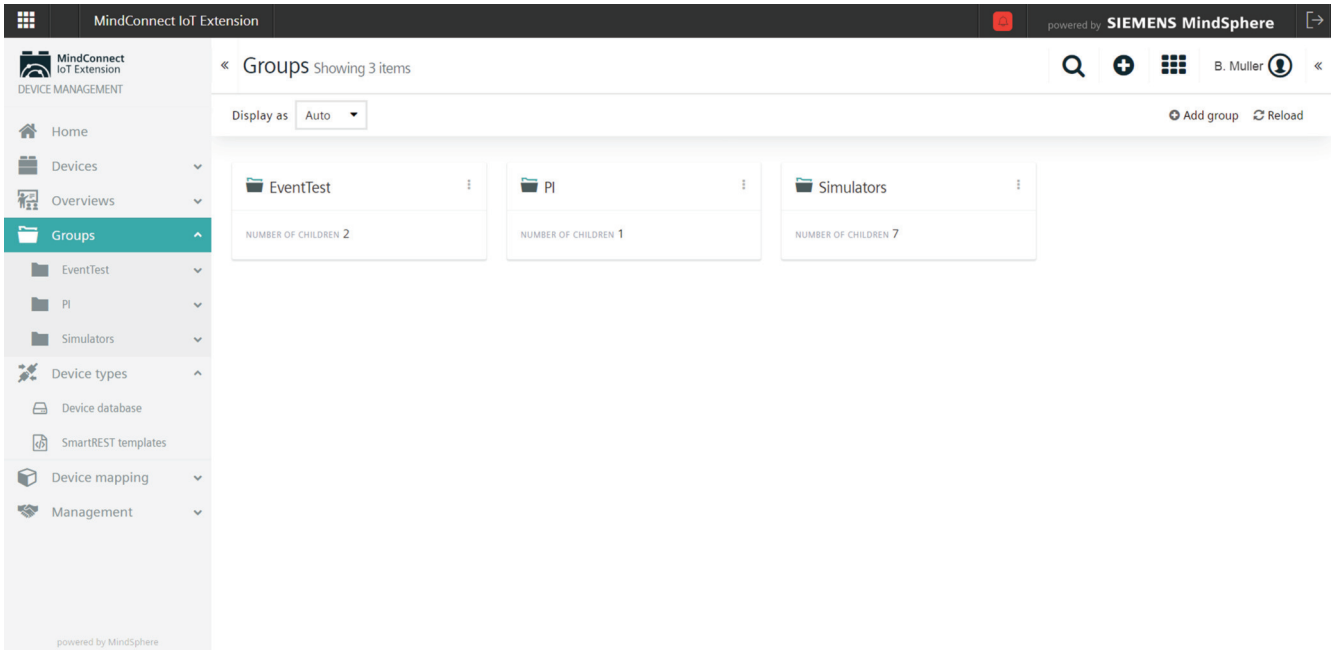
Devices can be arbitrarily grouped according to a particular use case. A device can be located in multiple groups, and groups themselves can again be part of multiple groups.

IoT Extension distinguishes between top-level groups and subgroups.

Top-level groups are shown in the "Groups" menu in the navigator at top-level. Subgroups are used to further subdivide top-level groups.

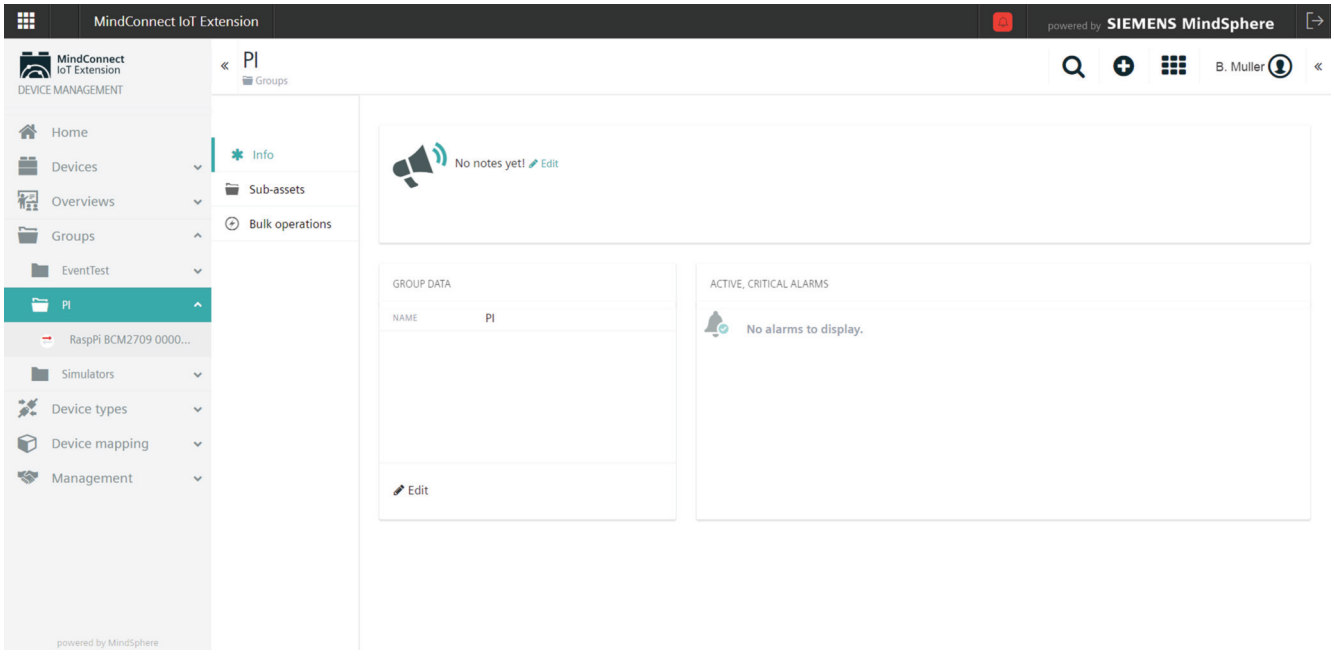
Viewing groups

To display a list of all groups in the account, click "Groups" in the navigator.



For each group, the name and the number of children is displayed.

Click a group to view its details.



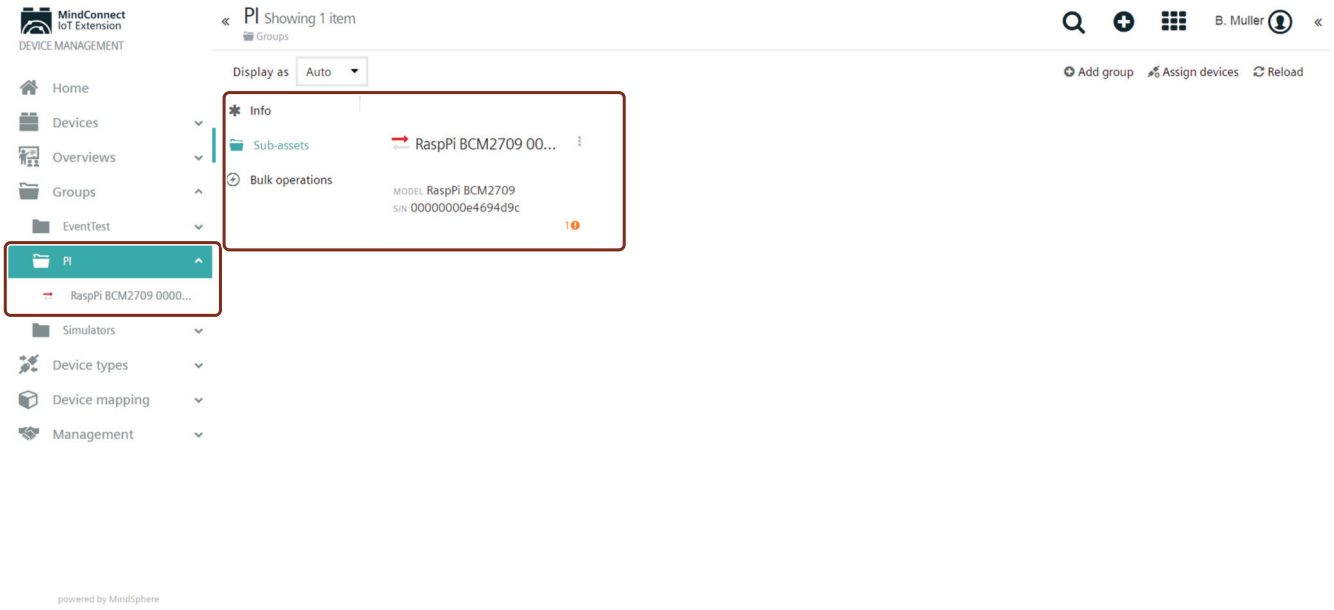
Info Tab

In the "Info" tab, the following information is provided:

Card	Description
Notes	Provides optional notes to inform about current activities. Notes usually may only be edited by an administrator. To add or edit a note, click "Edit", enter your note or your modifications in the text box and save your edits by clicking the green checkmark at the right of the text box.
Group data	Displays editable information on the group (name, description).
Active, critical alarms	Shows the active critical alarms for the devices in the group.

Sub-assets

In the "Sub-assets" tab you see a list of all devices assigned to the group. For each device, the name and the number of children is displayed.



To assign a device to a group, click "Assign devices" at the right of the top menu bar.

To unassign a device, click the menu icon in a device entry and from the context menu select "Unassign".

Bulk operations

In the "Bulk operations" tab, bulk operations created for the group can be managed. With bulk operations you can at once execute operations for each device within one group.

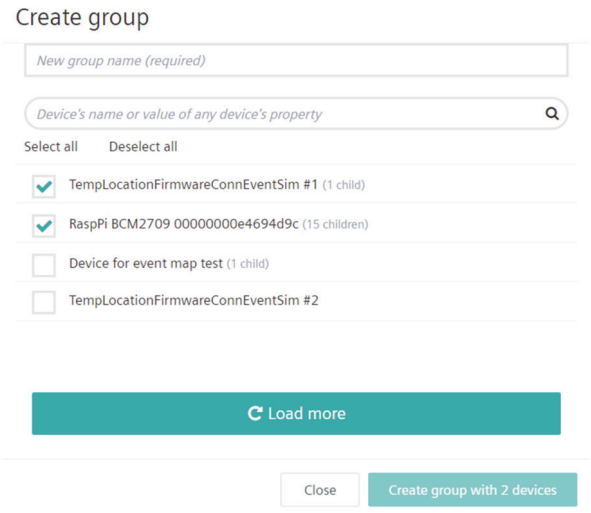
Create a new group

To create a new group follow these steps:

1. Click the "Plus" button at the right of the top bar, then select "New group" from the menu.
2. In the window that comes up enter a unique group name to identify your group.
3. In the "Device search" field, enter the search criteria for the devices you might want to add to your group (e.g. "ublox"). A list of devices that match your search criteria will be displayed.
4. Checkmark the devices you want to add from the list.
5. Click "Create group with X device(s)" to finally create your new group.

Note

A group can be created with "0" devices in it.



Assign a device to an existing group

You can assign devices to an existing group in two ways.

From the device perspective:

1. Select a device from the device list and open it.
2. In the Info tab, scroll down to the "Groups assignment" card. From the drop-down field, select the group you want to assign the device to. You can also directly enter a group name here or you can enter just parts of a name to filter the list for it and only show the matching group names.
3. Click "Assign".

If you search for a group by its name which does not exist yet, a "New" button will appear so that you can create a new group with this name from here and assign the device to that group.

In order to create a new group, the user must have the following permissions:

- ROLE_INVENTORY_CREATE
- ROLE_INVENTORY_ADMIN

From the group perspective:

1. In the navigator, select a group from the Group menu and then open the "Sub-assets" tab. In the "Sub-assets" tab, all devices that are assigned to the respective group are displayed.
2. Click "Assign devices" at the right of the top menu bar. In the upcoming window search for the devices you might want to add to your group (e.g. "ublox"). A list of devices that match your search criteria will be displayed.
3. Checkmark the devices you want to add from the list.
4. Click "Assign X device(s)" to assign the selected devices.

Create a sub-group

1. In the navigator, click a group to open it.
2. Click "Add Group" at the right of the top menu bar.
3. In the upcoming window, enter a name for the sub-group and click "Add group".

Edit a group

1. In the navigator, click a group to open it.
2. In the Info tab, click "Edit". This allows you to edit the name of the group and to assign user permissions for the group. For further information on permissions, see the Administration Guide (Page 13).

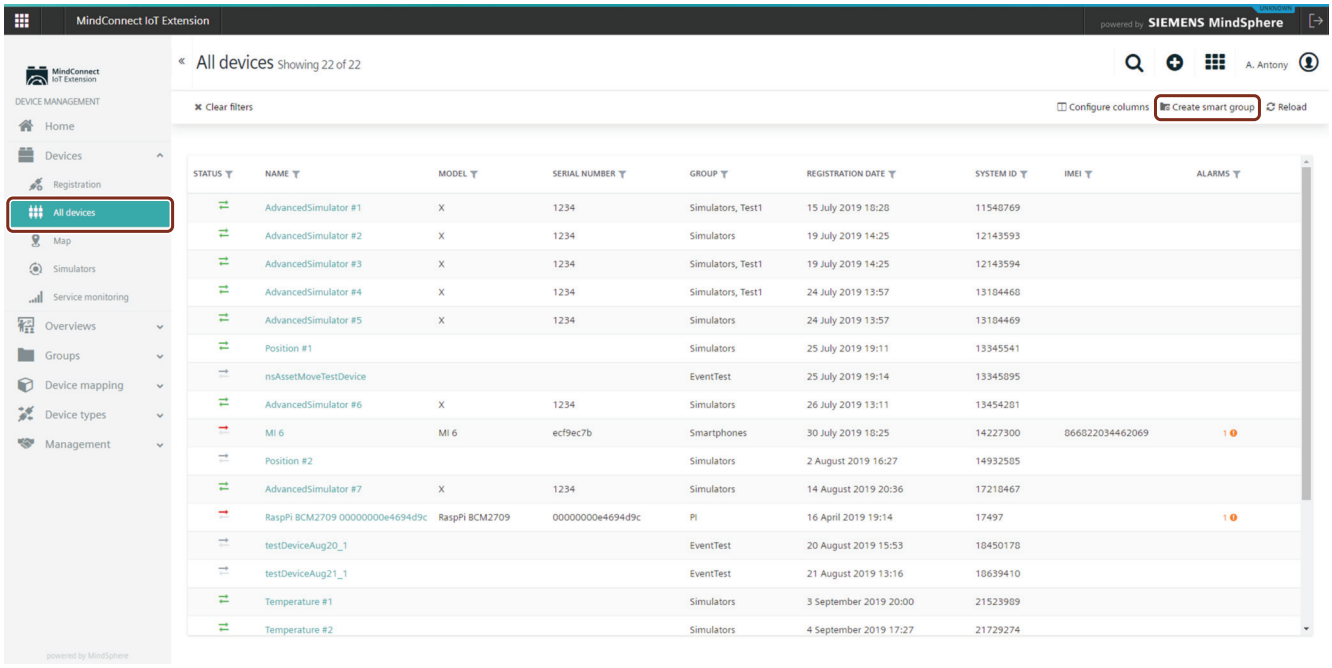
Using smart groups

Smart groups are groups dynamically constructed based on filtering criteria. They have a temporary character because the group members can change constantly. Smart groups do not have fixed member listings. They have fixed criteria instead. This type of group can be used, for example, for bulk upgrades of devices of a certain type to a new software or firmware version.

Smart groups can be created from the device list.

1. To open the device list, click "All devices" in the navigator.
2. Filter the devices in the list to select the desired devices.

3. Click "Create smart group" at the right of the top menu bar.



4. Enter a name for the group and click "Create".

The new group will appear as a top-level group in the "Groups" menu of the navigator. Smart groups can be distinguished by a small cogwheel in the folder icon.

In the "Sub-asset" tab you can adjust your selection and modify the filter settings.

To delete a smart group, click the menu icon and from the context menu select "Delete".

Note

Deleting a smart group is irreversible.

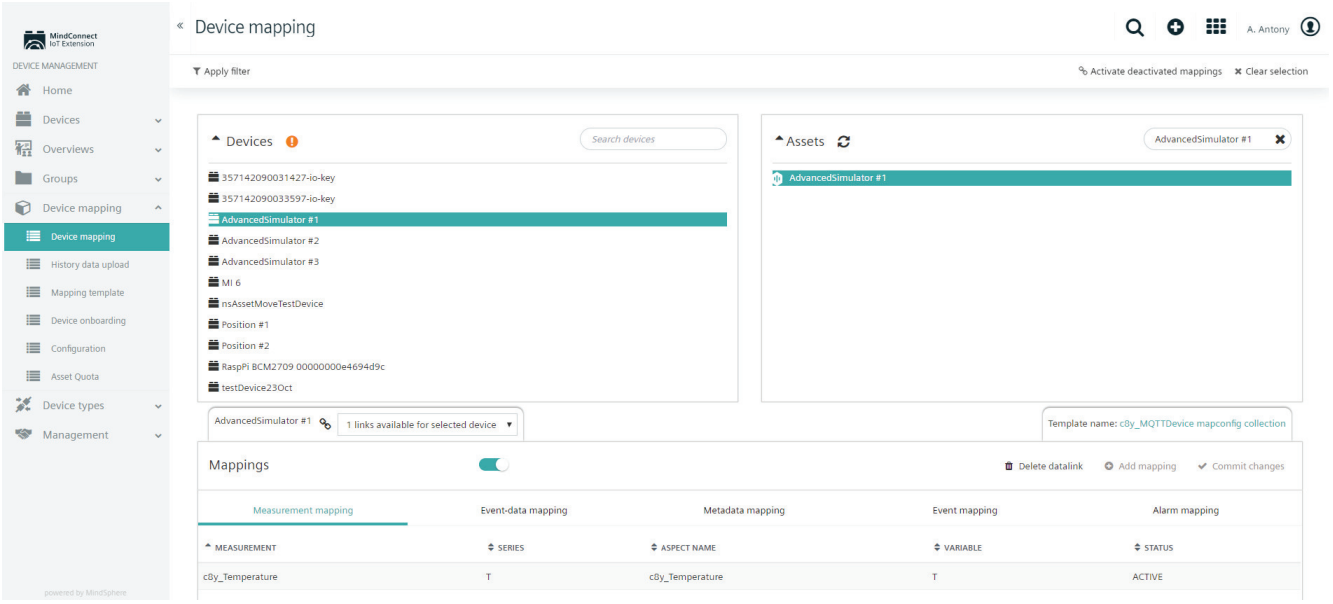
5.3 Device to asset mapping

5.3.1 Device Mapping

In order to correlate the device simulators and their measurements to MindSphere assets and their aspects you need to define a mapping. This can be done manually by "Asset Mapping" provided in the Device Management Application. Therefore, go to Device Management > Asset Mapping.

The main view is separated into two panels: Navigation (containing Devices and Assets) and Mappings area. On the navigation panel, the left side shows all available device groups and devices. The right-hand side shows all available assets of the related MindSphere tenant. A table below shows the current mappings.

On the top there are filters which can be applied to the device and asset view. Depending on the default view setting (Configuration (Page 109)), the devices are shown in a list or in a group view showing the devices within their groups. If the group view is enabled, the search applies to group names only. When devices should be searched by name, the "All devices" view can be used.



Differences among available kinds of mappings

Measurement mappings are the usually used mappings to map measurements/ data-points of a device to an (dynamic) aspect of an asset.

In case of non-number values event-data mappings can be used, if it is needed to map those non-number values like Strings to an (dynamic) aspect of an asset. In this case those values can be send by the device as an event. An event-data mapping can then be configured to take the content from the event-data mapping and transmit it to the mapped aspect.

For device information which should be transmitted to MindSphere metadata mappings can be used. Any arbitrary metadata provided in the device object can be mapped to a static aspect.

For device related events and alarms which should be transmitted to MindSphere, event mappings and alarm mappings can be used respectively. Both events and alarms can be mapped to MindSphere events.

Create a mapping

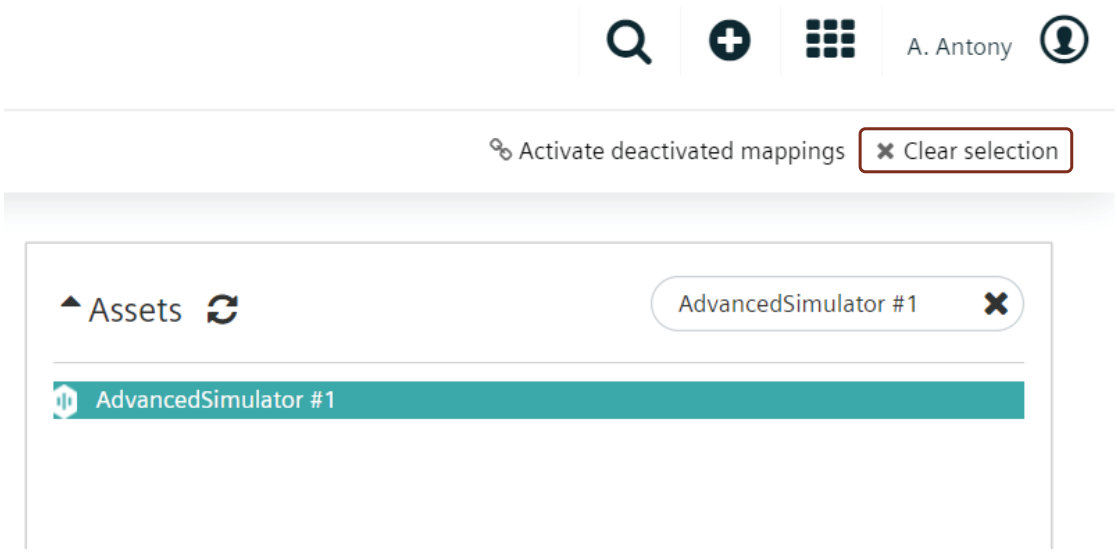
To create a mapping proceed as follows:

1. Select a device on the left-hand side of Navigation Panel. (You can see available data-links in the dropdown menu in the Mappings-Area)
2. Select an asset on the right-hand side of Navigation Panel.
3. Click "+ Add Mapping". (You can only add a new mapping when you select a device and an asset)
4. Specify mapping details in the dialog.

In case of many devices and assets, the search text fields for each section can help finding devices or assets on navigation panel.

- The search auto applies once you hit the "Return" (Enter) key.
- Also: if you delete the existing search string and click "Return", all devices and assets are shown again. (If the filter type is set to "SHOW ALL", this will show the "group view")
- Enter at least 3 characters to activate the search immediately without hitting the "Return" key.
- "Clear all" is implemented inside the search box which clears the entered text and shows the "Group view".

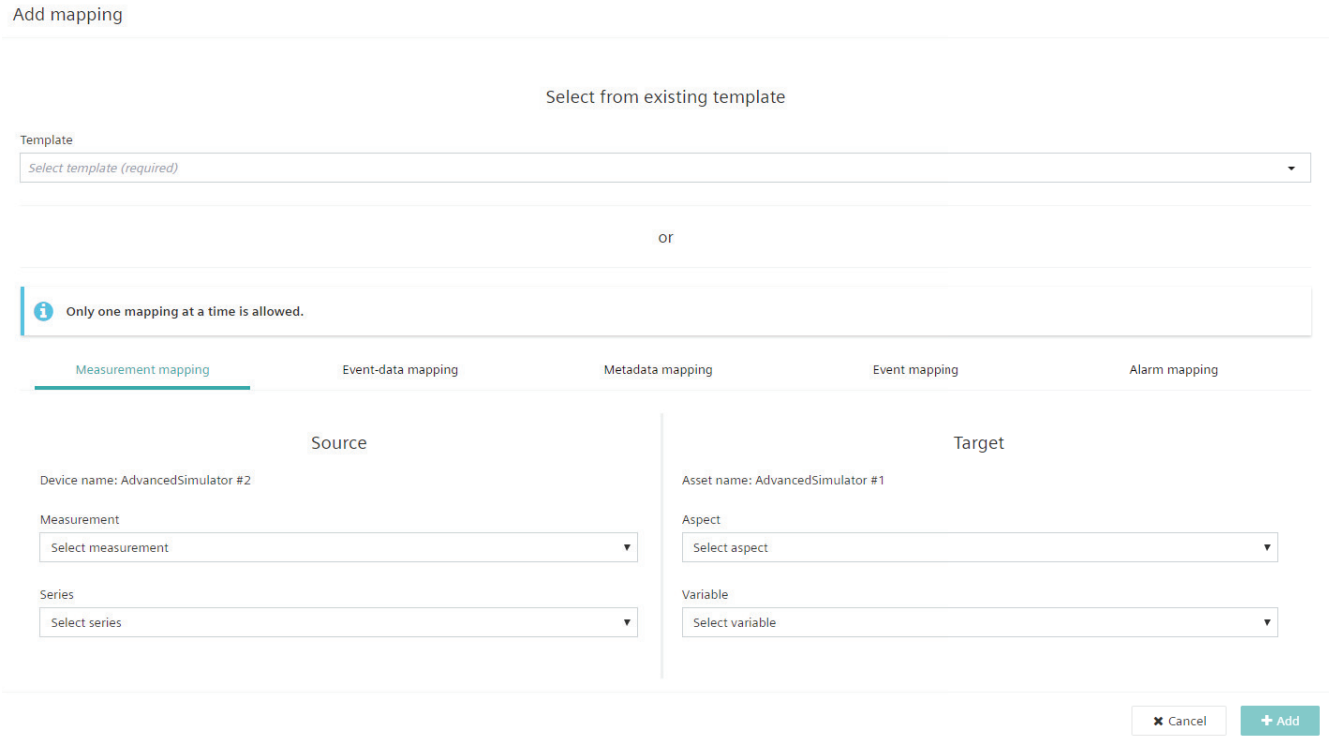
Click on "Clear selection" to clear the selection on the navigation panel.



After clicking "+ Add Mapping" a dialog appears to select the mapping information of the selected device and asset. The "+ Add Mapping" button is disabled in case the selected device and asset are mapped using a template.

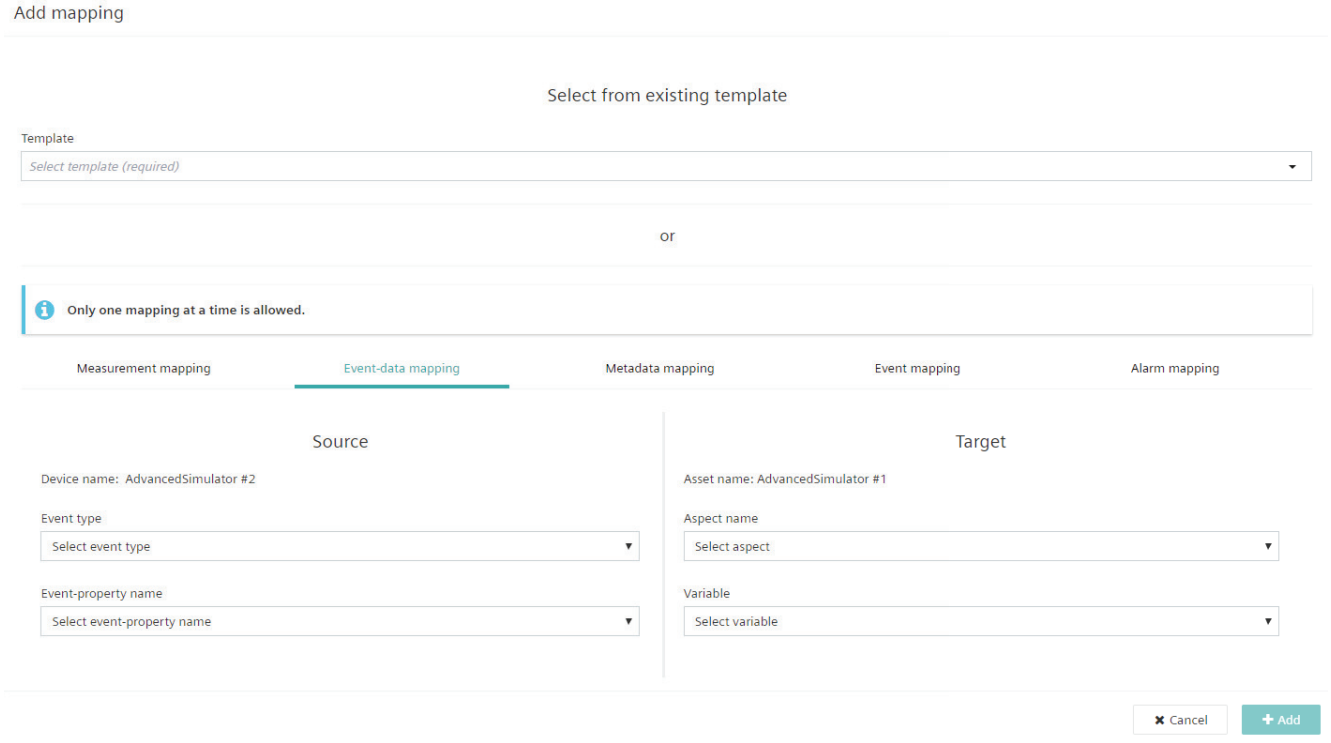
There are several options to add a mapping:

1. Choose from existing mapping template:
   - Select a template from the drop-down menu.
   - Click "+ Add" to apply this template to the selected device and asset.

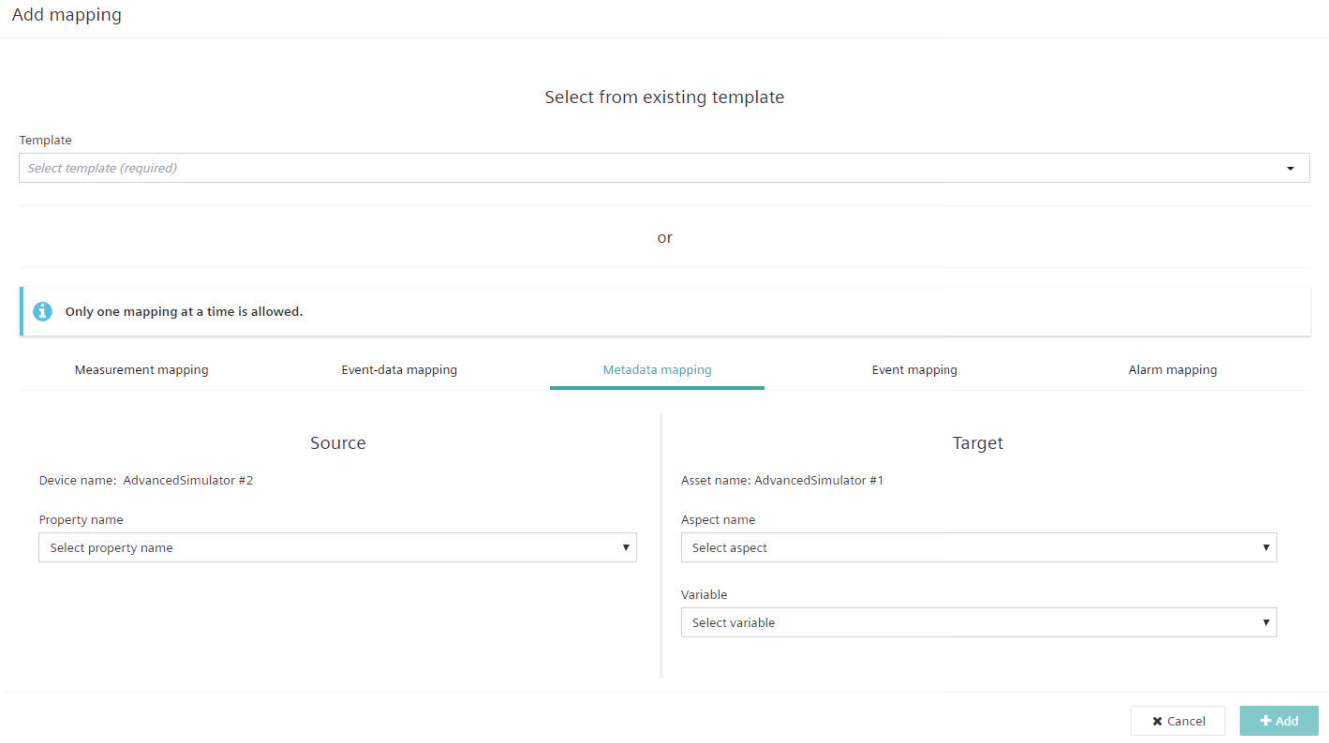


2. Add measurement (data point) mapping:
   - Select the required "Source", "Target" and "Converter" information:
     1. "Measurement": Source measurement of IoT Extension
     2. "Series": Source series within selected measurement of IoT Extension
     3. "Aspect": Target aspect of MindSphere
     4. "Variable": Target variable within selected aspect of MindSphere
     5. "Converter": Possible conversion of units of measurement from Source to Target (e.g. Celsius to Fahrenheit)

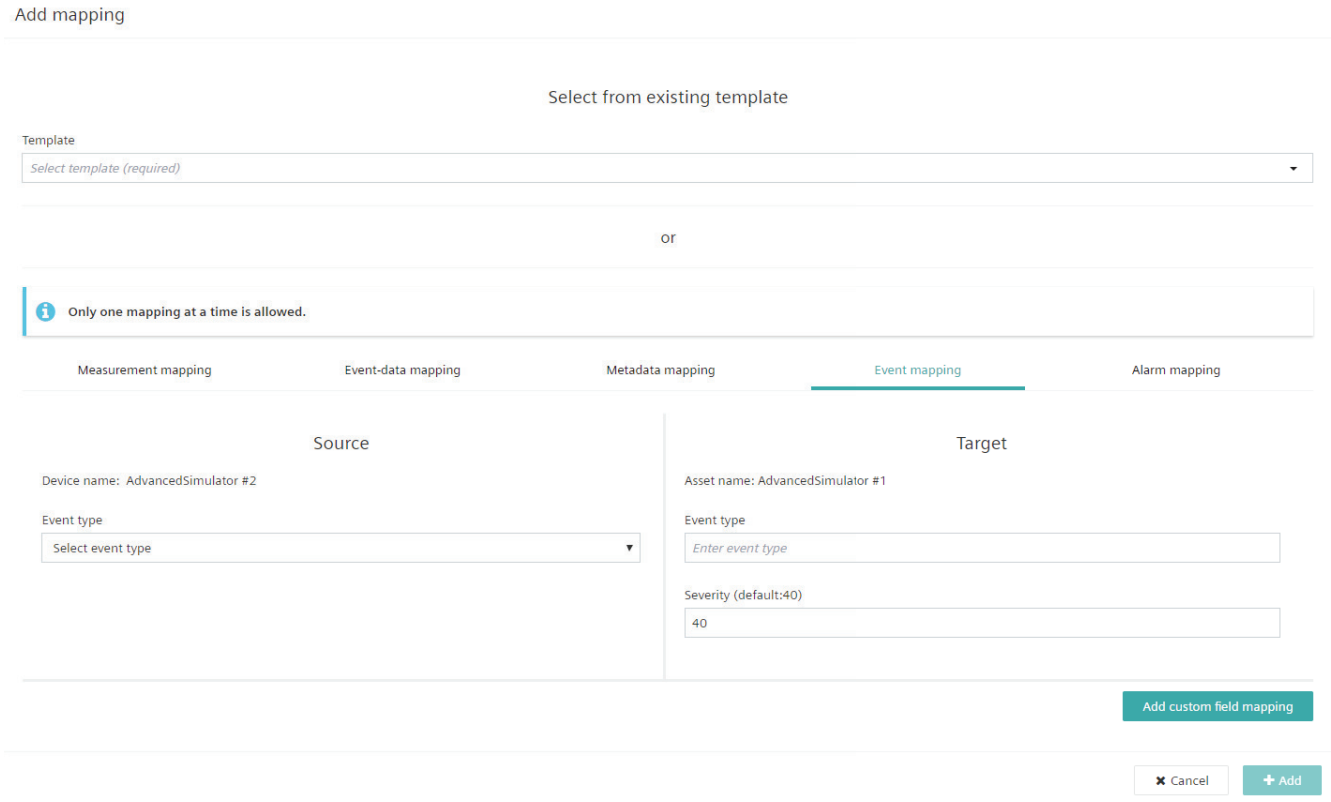
3. Add event-data mapping:
   - This process is very similar to measurement mapping.
     1. "Event Type": Select from all event types the device is sending
     2. "Event Property": (optional): Select specific property of the event
     3. "Aspect Name": Select aspect of chosen asset
     4. "Variable": Select variable of selected aspect
     5. "Converter": Possible conversion of units of measurement from Source to Target (e.g. Celsius to Fahrenheit)



4. Add metadata mapping:
   - This process is very similar to measurement mapping and event-data mapping.
     1. "Property Name": Select from all device properties
     2. "Aspect Name": Select aspect of chosen asset
     3. "Variable": Select variable of selected aspect
     4. "Converter": Possible conversion of units of measurement from Source to Target (e.g. Celsius to Fahrenheit)



5. Add event mapping:
   - Select the required "Source" and "Target" information:
     1. "Event Type": Select from all event types the device is sending.
     2. "Event Type": Type in the event type from MindSphere which should be used for event creation. After typing in first three letters, press enter. The dropdown displays the available event type starting with entered letters.
     3. “Severity”: Enter the severity of the event. By default, the severity is 40.
   - Add Custom Field Mapping (optional): Click on "Add custom field mapping" to map specific properties of the events between IoT Extension and MindSphere.
     1. “Source Property”: Select specific property of the event.
     2. “Target Property”: Select specific property of the MindSphere event to which source property should be mapped.



   It is possible to add multiple custom mappings in an event mapping.

6. Add alarm mapping:
   The creation of alarm mapping is similar to the creation of event mapping. However, in case of alarm mapping, an alarm type is mapped to an event type. Based on the created alarm mapping, a device alarm is mapped to a MindSphere event. A "1:1" mapping is maintained between an alarm in IoT Extension and an event in MindSphere based on their IDs. For a new instance of an alarm of the mapped alarm type raised in IoT Extension, a new event is created in MindSphere. Any further update to that alarm would trigger an update of the same event until the alarm is set to "CLEARED". Once an alarm is cleared, another device alarm of the same alarm type would be mapped to a new event in the MindSphere.

Note

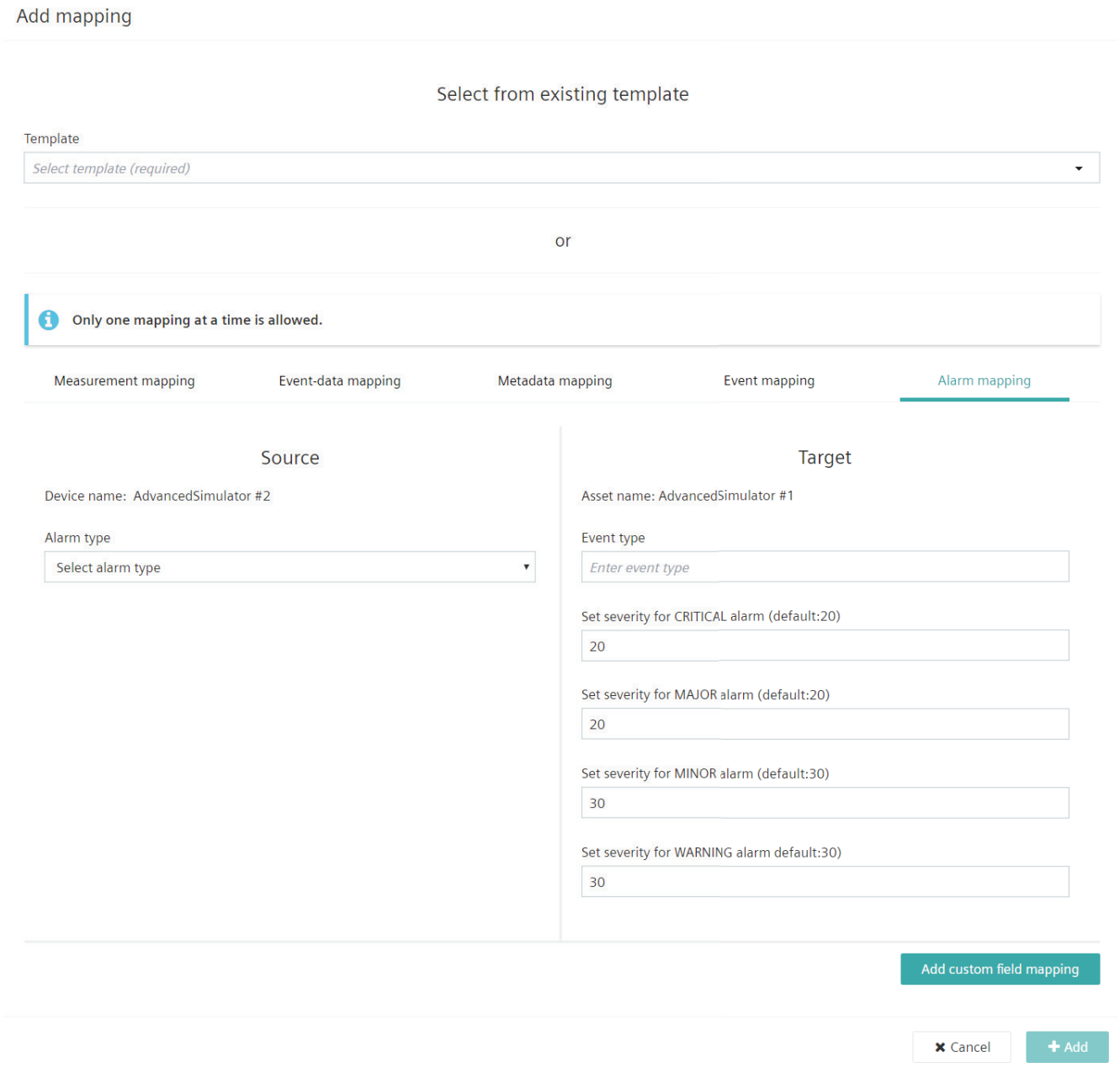
The event would always hold the timestamp once it is first created as MindSphere event does not allow updating the timestamp.

– Select the required "Source" and "Target" information:
  1. "Alarm type": Select from all alarm types.
  2. "Event Type": Type in the event type from MindSphere which should be used for event creation. After typing in first three letters, press enter. The dropdown displays the available event type starting with entered letters.
  3. "Severity": Enter the different severities of the alarm. Based on severity of the alarm selected in source, one of the four severity in target is used during event creation. By default, the severity is 20 for critical and major alarms and 30 for minor and warning alarms.

  Note

  In the source only the type of alarm is selected. However, the actual alarms in IoT Extension can be of different severity, even from the same type. For example, an alarm of type "myDeviceAlarm" can be raised with severity "Major" or "Warning". Depending on this source severity the related event in MindSphere is created with the specific target severity specified in the mapping.

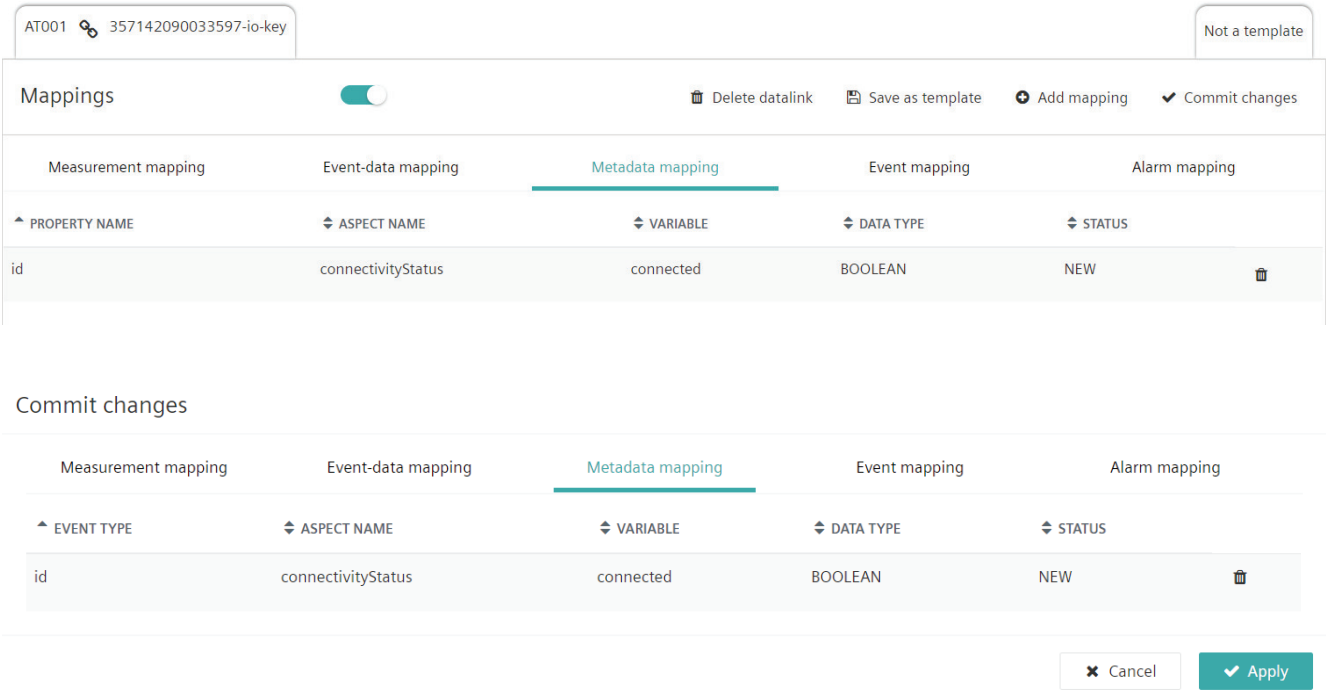
– Add Custom Field Mapping (optional): Click on "Add custom field mapping" to map specific properties of the events between IoT Extension and MindSphere.
1. “Source Property”: Select specific property of the alarm.
2. “Target Property”: Select specific property of the MindSphere event to which source property should be mapped.



It is possible to add multiple custom mappings in an alarm mapping.

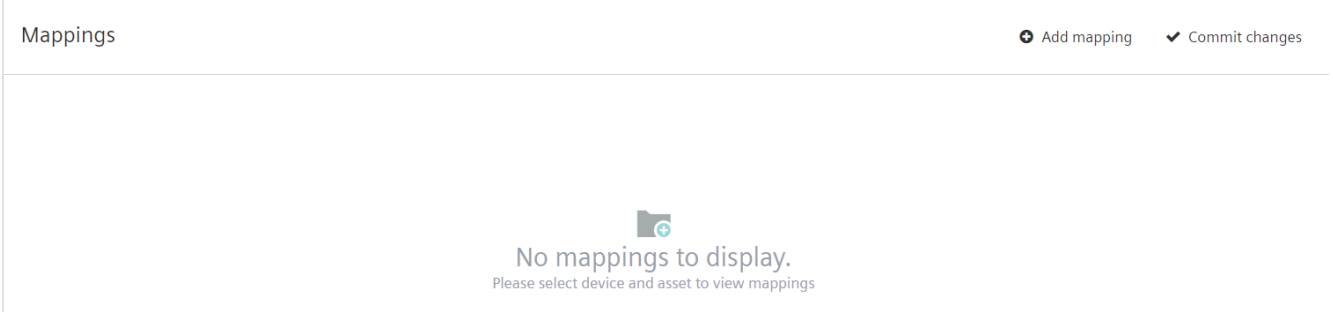
Clicking on "+ Add" creates a mapping between source and target. You can add more mappings by repeating the above steps.

At this state the mapping is not committed yet. Mappings must be committed (published) by clicking on "Commit Changes" and applying those changes in the confirmation dialog box. This action activates all mappings immediately. As long as there are no mappings to commit, nothing will be shown in "Commit Changes" pop up.

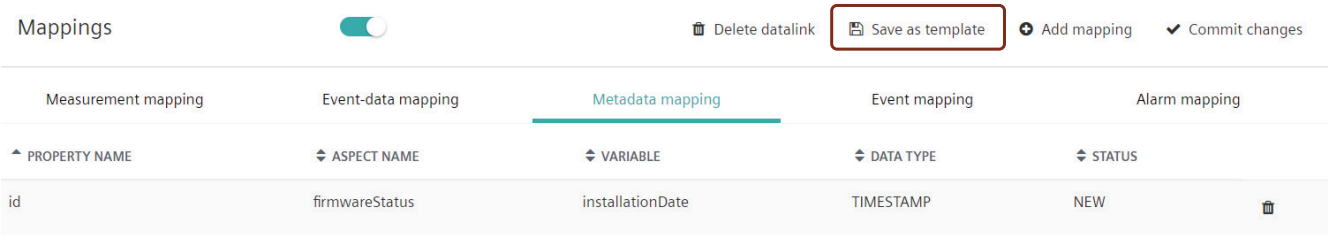


Mappings of any devices or assets are shown on demand. (No mappings will be shown unless any device / asset is selected)

- Mappings can be sorted based on the Measurement, Series, Aspect Name, Variable and Status.
- Mappings can be deleted by clicking on the "trash" icon.
- If no mapping is found for the device or asset, the following notification appears:



Existing mappings can be saved as template:



Delete a mapping

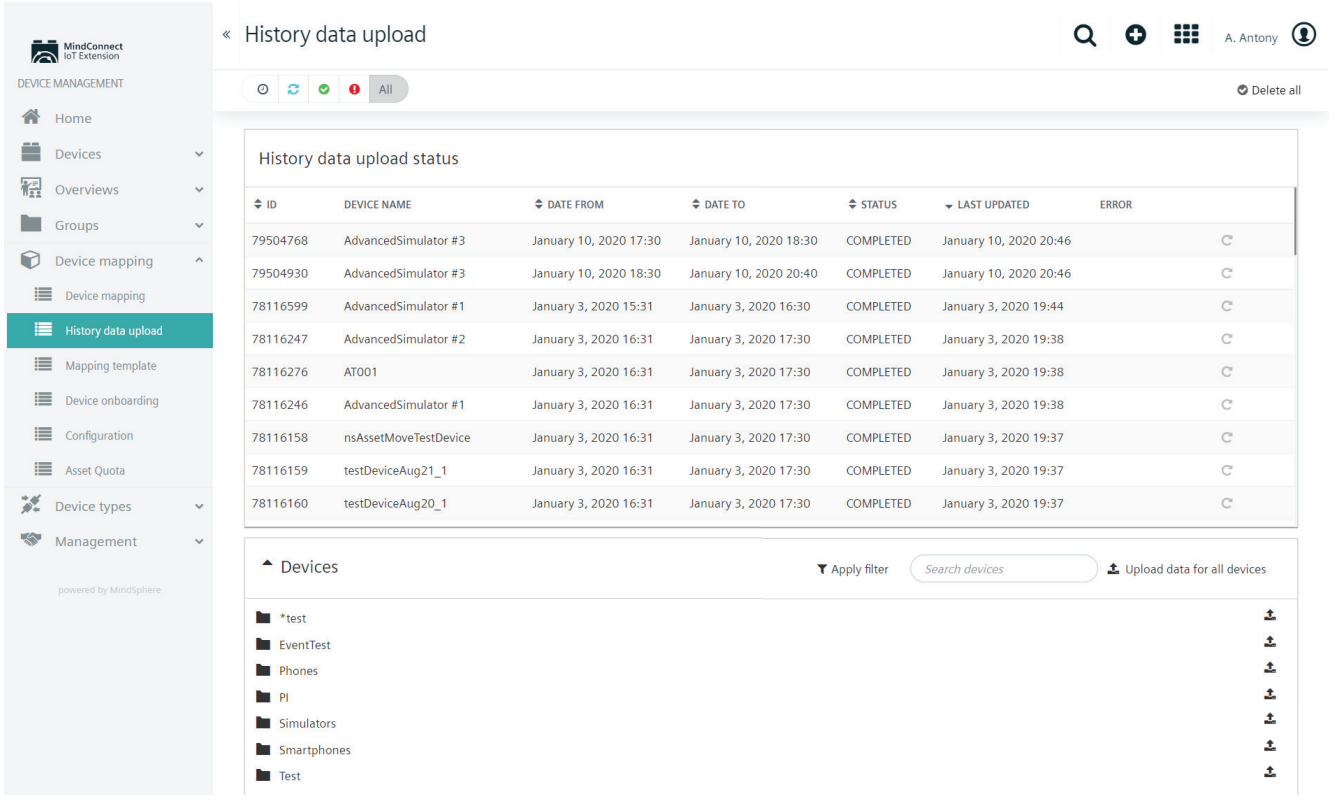
Deleting single mappings can be done as soon as a device or an asset and one of its datalinks is selected.

The datalink between a device and the onboarded asset can be deleted by selecting it and clicking on the trash-icon afterwards. We can choose whether the created MindSphere asset should be deleted or not. In any case the locked asset will be unlocked when deleting the datalink.

5.3.2 History Data Upload

History Data Upload provides the functionality to upload measurement data of specific devices in a specific time frame. This can be useful when time series data of a device should be uploaded to MindSphere before any mapping was configured for this device. The history data upload view contains two panels.

- On the top panel you can see all the upload requests for historical data and their information.
- On the bottom panel you can see the device selection with upload buttons.

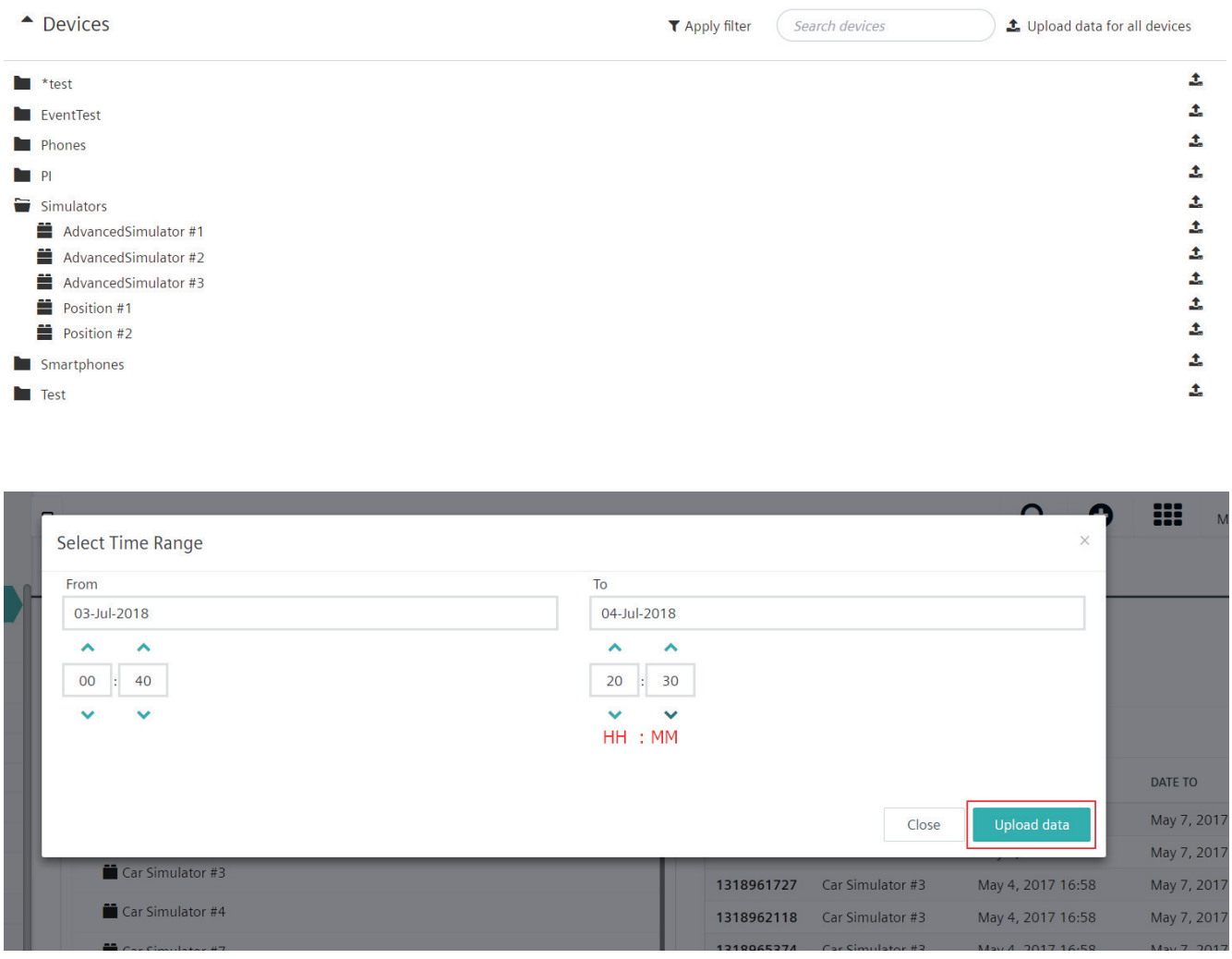


Create a new history upload request

To create a new history upload request proceed as follows:

1. Select a device group or a single device
2. Click on "Upload"
3. In the "Select Time Range" dialog
   - select the from date and time (HH:MM)
   - select date and time (HH:MM)
   - click on "Upload Data" to submit the request

The submitted request will be added to the "Upload tasks" table.



Note

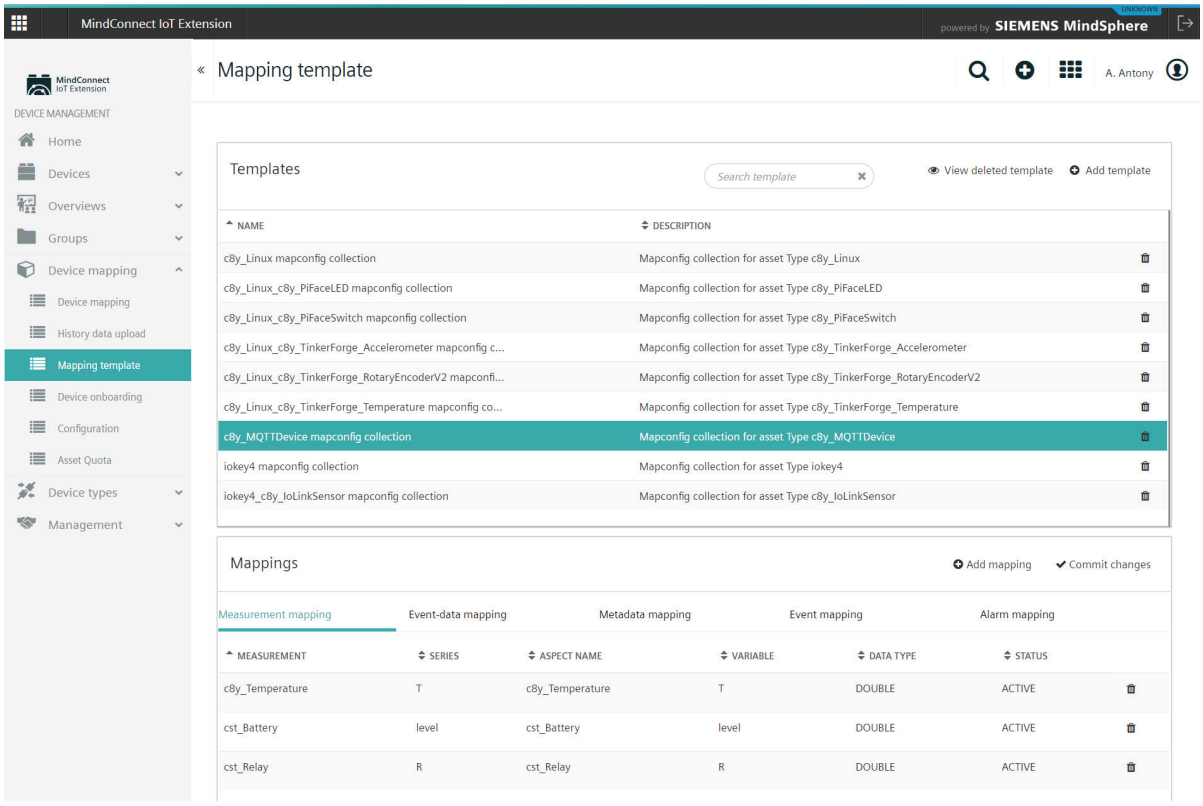
Limit on time range is 60 minutes for a single request.

5.3.3 Mapping template

Mapping templates are used to simplify the device mapping process, as they can contain a set of multiple mappings between data points. Templates are used by the automated onboarding process within its onboarding rules. However, templates can also be created manually. The mapping template view contains two panels:

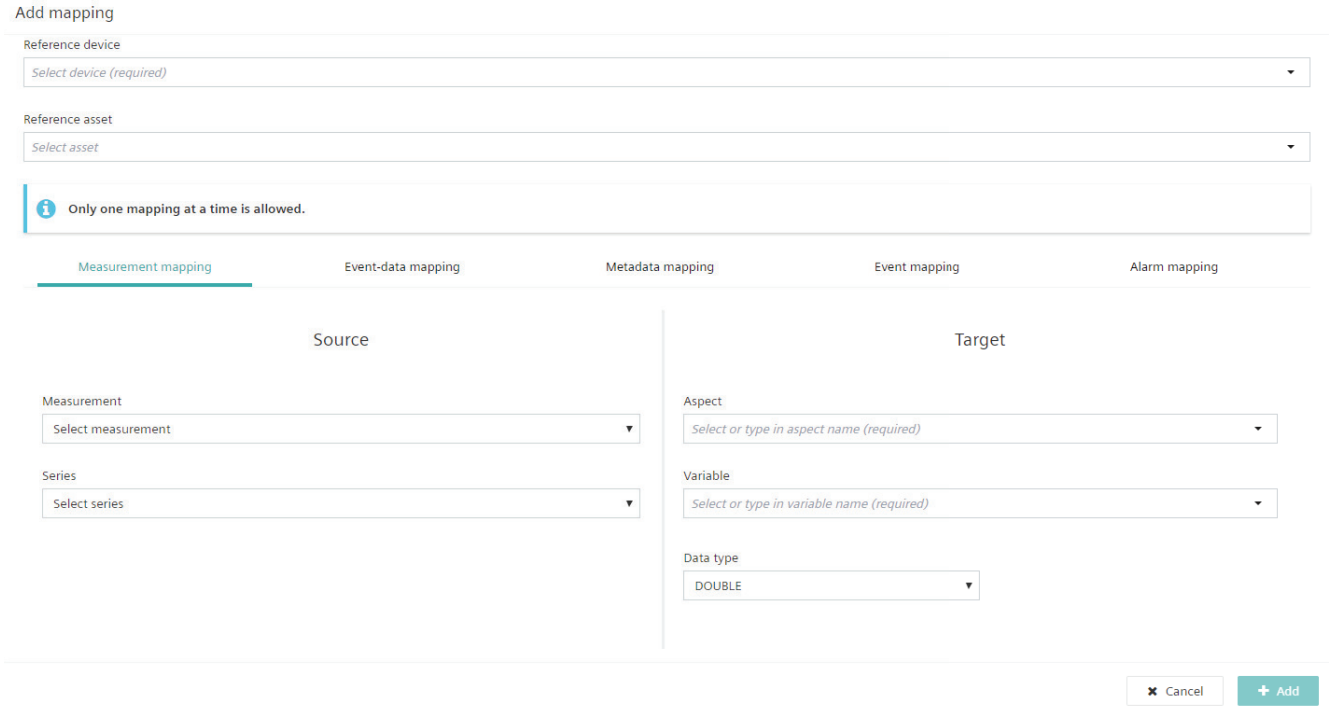
- On the top panel you can see all existing mapping templates with name and description
- On the bottom panel all mappings of a selected template are shown

You can delete a template, if it is neither referenced by any device nor referenced by an onboarding rule. Deleted templates can be viewed and restored by clicking "View deleted templates".



Creating and editing templates

You can create an empty template by clicking on "+ Add template". Any template can be modified by adding mappings. The process is similar to adding an individual mapping as described above. When adding a mapping you need to select a reference device. This reference device acts as a source provider. Any measurement/series of the reference device can be selected. For the target part you can either select an existing asset or specify an individual aspect with variable.



Note

1. All specified mappings are validated against the related assets.

2. If the modified template is part of a mapping rule the aspects and asset type get created or modified as needed. In case of a stand-alone template only a verification is performed.

5.3.4 Device Onboarding

The device onboarding view provides automated onboarding capabilities. Automated onboarding is based on a rule-concept. You can specify onboarding rules for unique device types and all devices of this type will automatically be onboarded. The automated onboarding process contains the following steps:

1. Automated onboarding
   - Creation of assets for each device of the device type
2. Automated mapping with mapping rules
   - Creation of aspect type(s) and asset type (in MindSphere) for each mapping rule/ device type
   - Automated mapping of device-asset-combinations matching the mapping rule criteria.

Right after registering/ creating a device in IoT Extension it will be automatically visible in MindSphere. Also the location of an asset (if provided) is transmitted.

Once a mapping rule is created, all devices of the specific type are mapped. Hence time series data will be transmitted to MindSphere.

Once an onboarding rule is created all devices of the specific type will be automatically be visible in MindSphere including time series data. Enabled onboarding rules are applied to all existing and new devices, which are not mapped yet to any asset. You can view, create, deactivate, activate, and delete existing onboarding rules in this view.

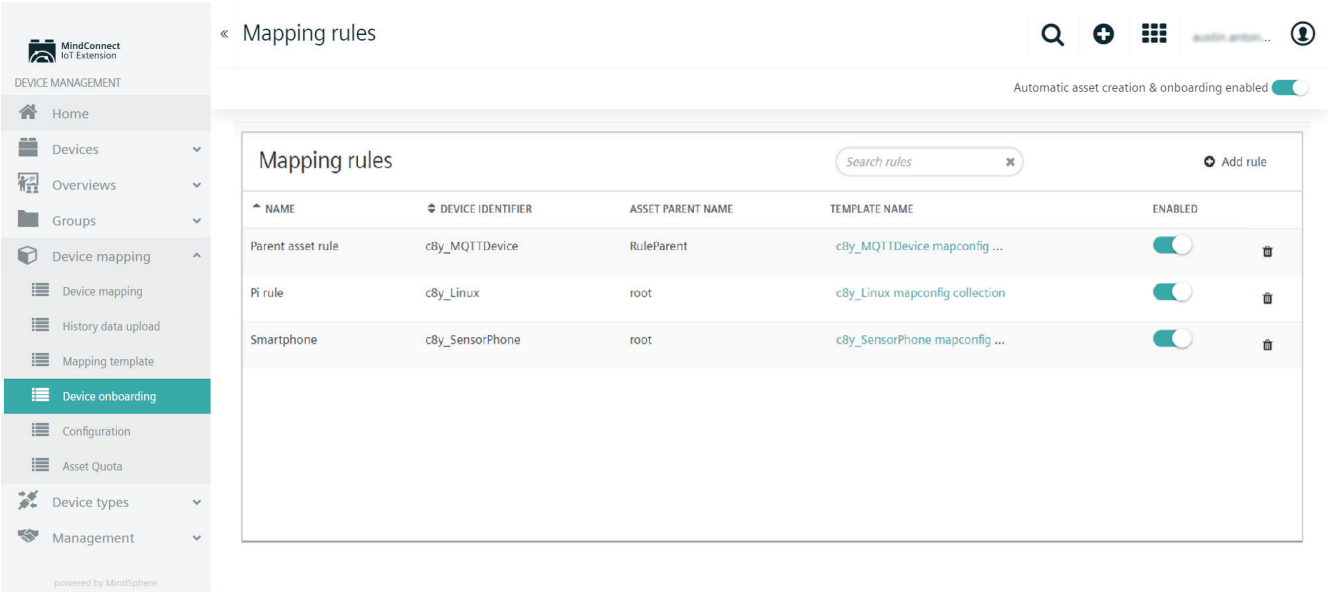
The automated asset creation and automated onboarding using the mapping rule can be deactivated for the tenant by using the "Automatic Asset Creation & Onboarding Enabled" - switch on the top right.

Note

Deleting an onboarding rule causes deletion of assets. All related entities to the onboarding rule will be deleted. This includes aspect types, asset types and assets on MindSphere side. On IoT Extension side this includes mapping templates and data-links.

Disabling automatic asset creation & onboarding affects the mapping rules.

The enabled mapping rules are not applied if the "automatic asset creation & onboarding" is deactivated.



Onboarding mapping rule creation

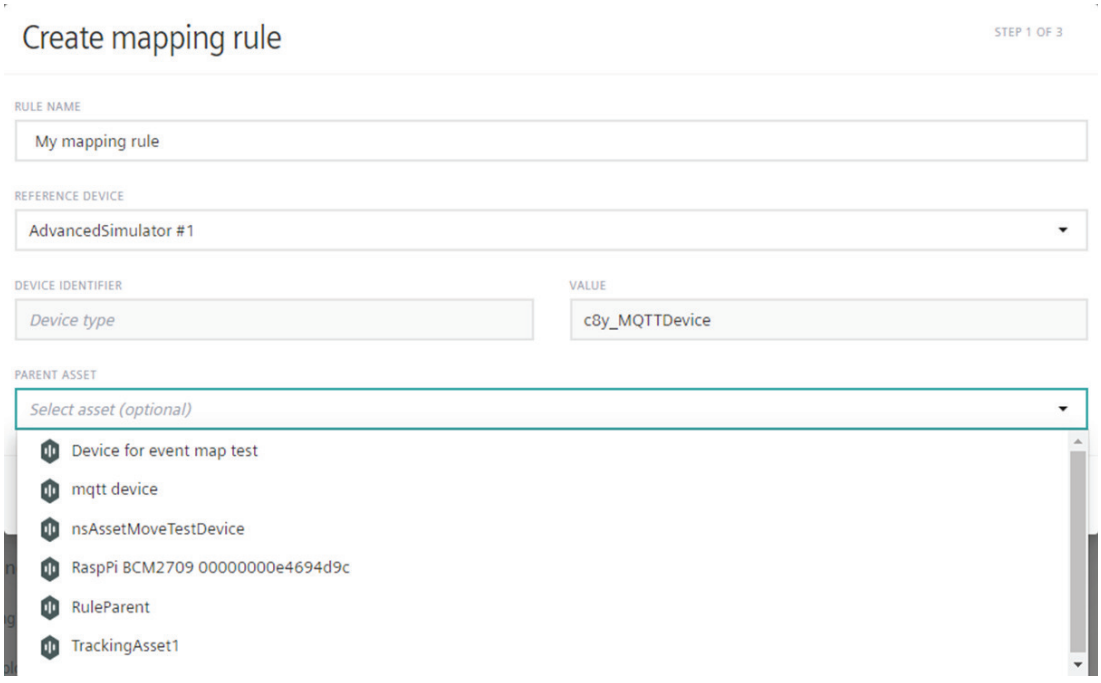
To create an onboarding mapping rule you must fulfill at least the following prerequisites:

- At least one device of a specific type (for which an onboarding rule should be created) must be registered
- At least one parent asset already exists in MindSphere
  All assets which are automatically created will be created as sub-assets of this parent asset.

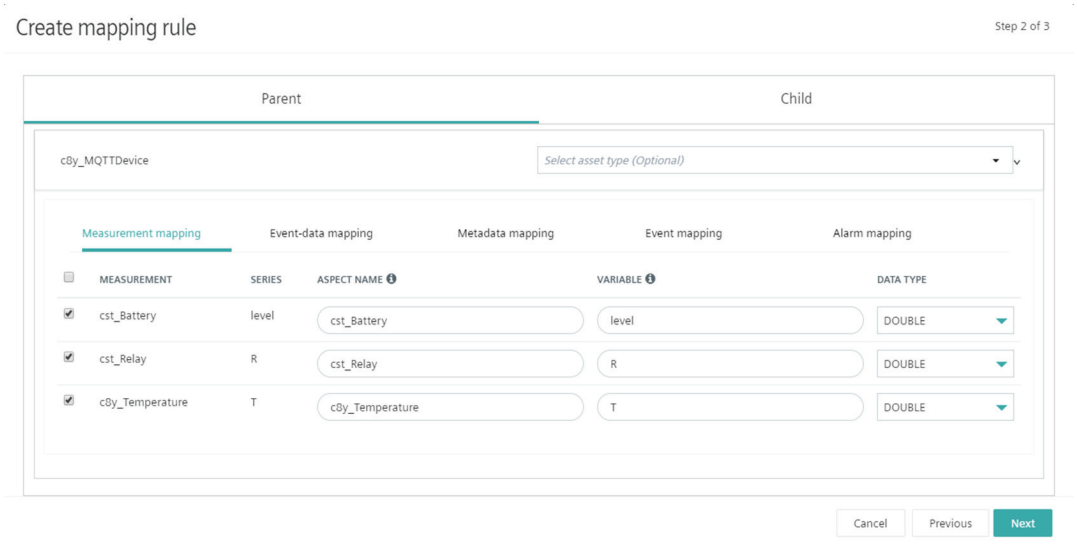
To create an onboarding mapping rule proceed as follows:

1. Click on "+ Add rule"
2. Select the reference device
   - This device is used as source provider to provide information about measurements of this device type.
   - After selecting a device its device type is presented as device identifier for this new rule

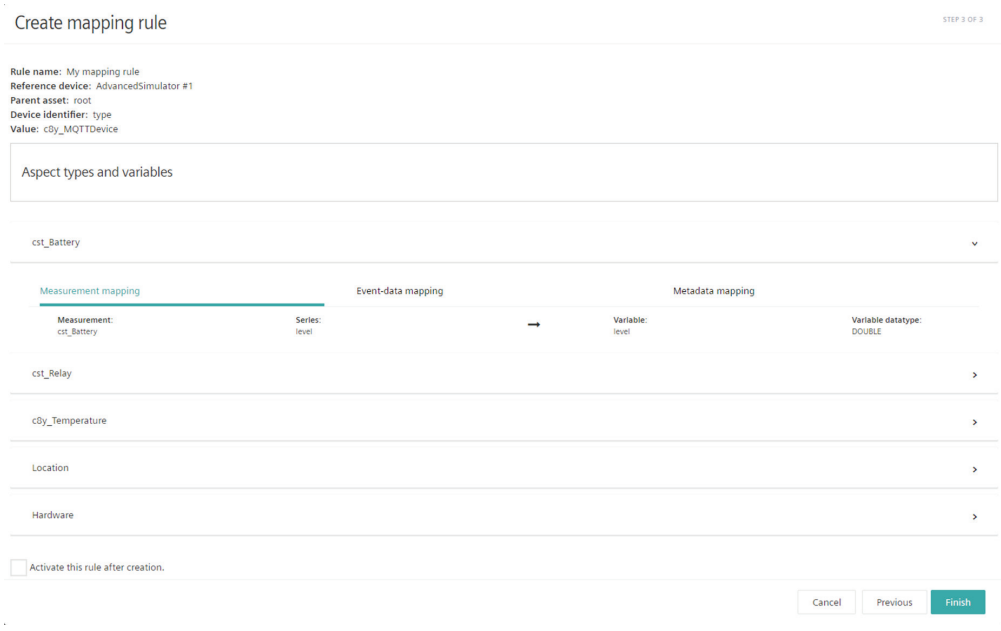
3. Select the parent asset.



4. Define the aspect name and variable names
   - Default values are automatically provided based on the source measurement
   - All existing measurements will be presented
   - For all measurements an automated mapping will be performed by the rule
   - In case the selected reference device has child devices, also measurements of the child devices are considered



5. The final step provides a preview of the new rule
6. Select if the new rule should be active after creation
   – By default new rules are not active after their creation

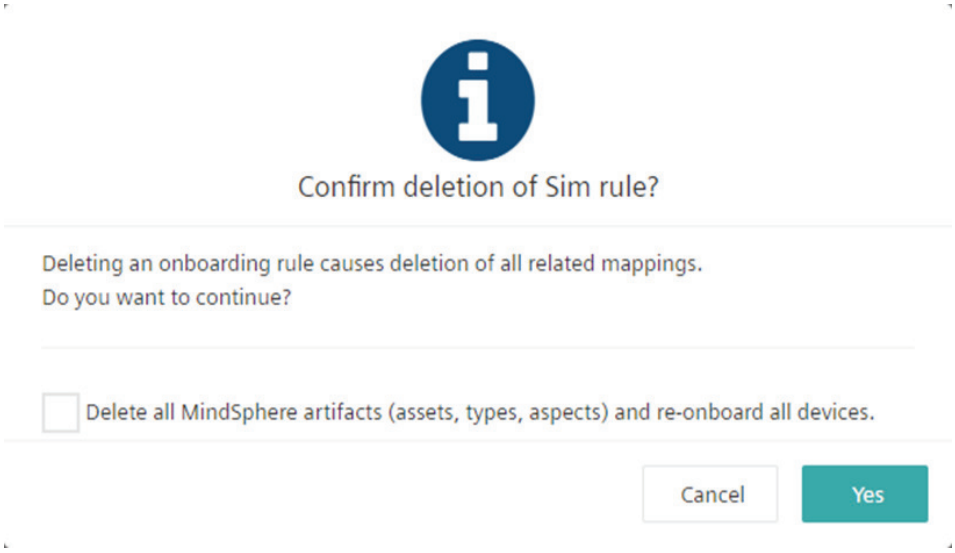


Mapping rule deletion

A mapping rule can also be deleted, but it needs to be disabled. Optionally all related MindSphere artifacts can be deleted as well.

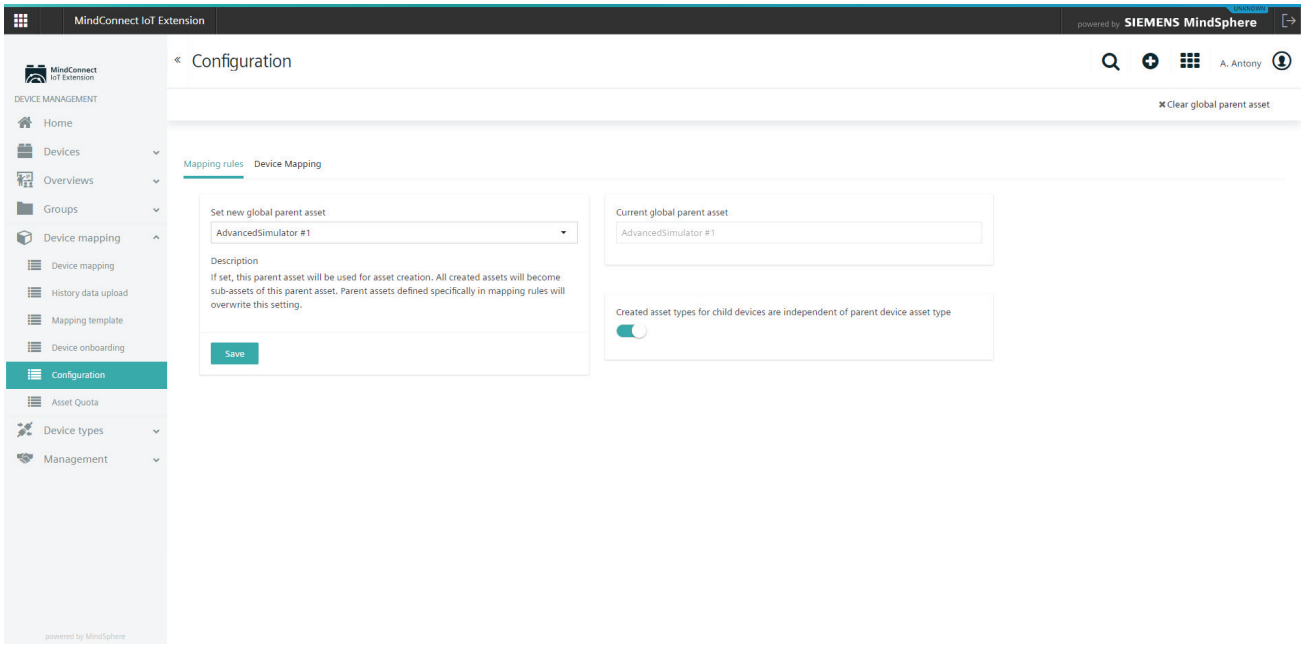
Note

If enabled, the MindSphere artifacts related entities to the mapping rule will be deleted. This includes aspect types, asset types and all assets on MindSphere.



5.3.5 Configuration

The configuration view contains the possibility to set a global, tenant-wide parent asset, which is used for asset creation. This asset is used as a parent asset for all assets which are created by IoT Extension. In case a parent asset is defined on a mapping rule specifically it has higher priority over the globally defined parent asset.



Mapping rules

To add a new global asset parent, proceed with the following steps:

1. Select the asset from the drop down menu.
2. Click "Save".

The asset will be saved and displayed in the "Current Global Parent Asset" section on the right.

If you choose a new asset and save the same, the system will overwrite the existing asset and the newly saved asset will be displayed in the "Current Global Parent Asset".

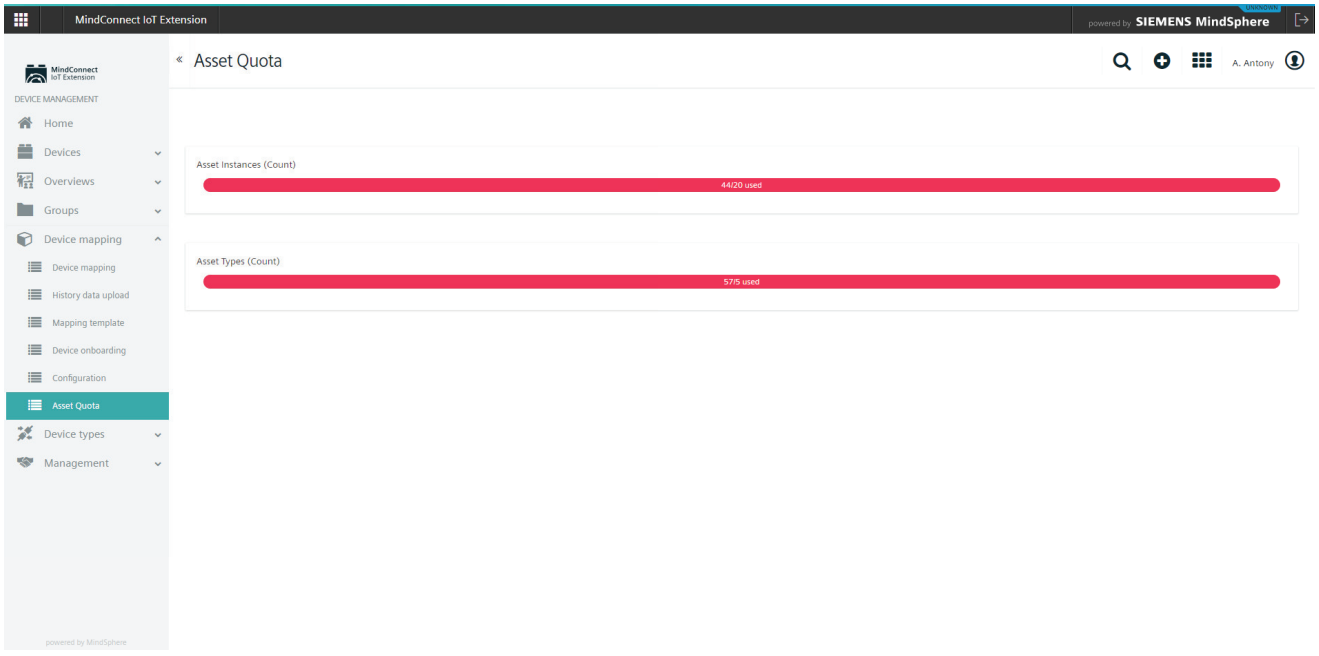
Creation of asset types for child asset types can be optionally be set as independent from the parent asset type.

Device Mapping

The default view of the device mapping can be set to either the “Group view” or “All devices”. In case the quotas are exceeded, they are highlighted in red.

5.3.6 Asset quota

The asset quota shows statistics for the usage of asset instances and asset types.



5.4 Device types

5.4.1 SmartREST templates

Introduction

SmartREST templates are a collection of request and response templates used to convert IoT Extension data and IoT Extension Rest API calls. For example, you can use SmartREST templates to easily add devices to the platform instead of manually writing the requests each time.

To ease the device integration, IoT Extension supports static templates that can be used without the need for creating your own templates. These templates focus only on the most commonly used messages for device management.

Open the SmartREST template list from the "Device Types" menu in the navigator.

For each template, the following information is provided:

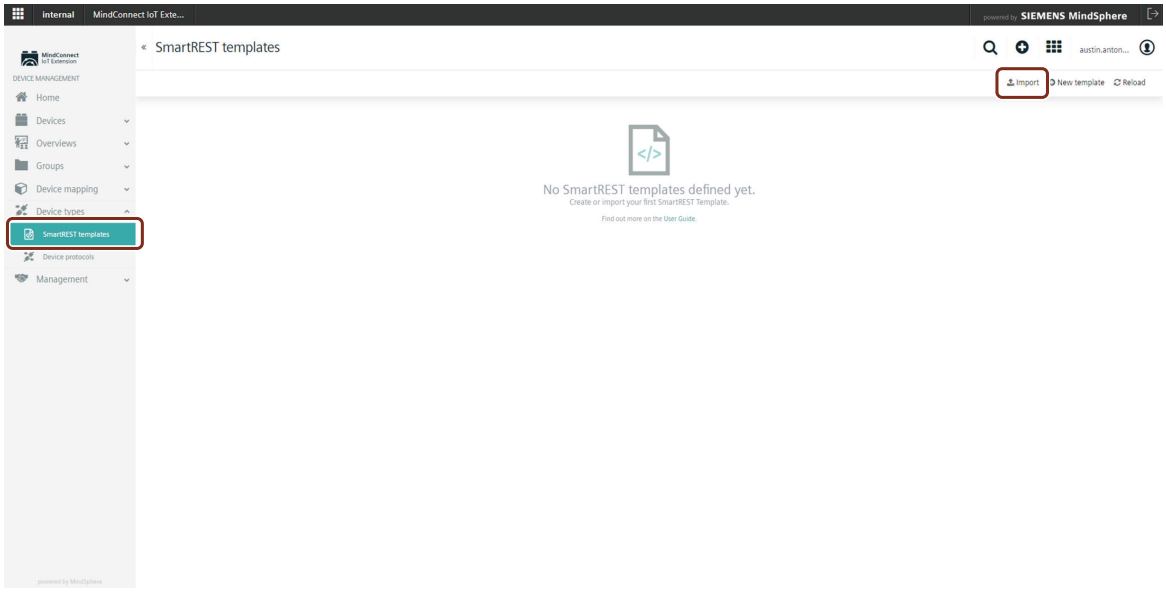
- "Template name", e.g. Camel
- "Template ID", e.g. 99
- "Number of send messages"
- "Number of responses"

There are two ways to add a SmartRest template:

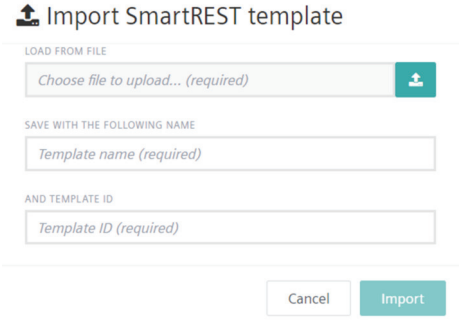
- Import an already existing template.
- Create a new template.

Import an existing SmartREST template

1. Click "Import" at the right of the top menu bar.

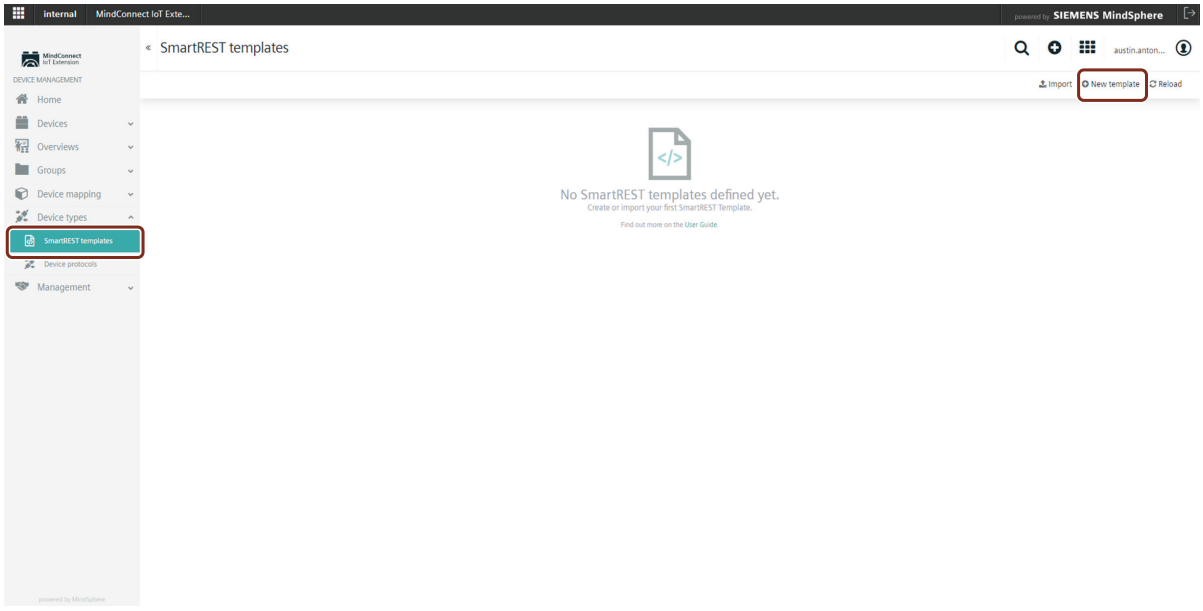


2. In the upcoming window, choose a file to upload by browsing for it.
3. Enter a template name and a unique template ID (both mandatory fields).
4. Click "Import" to import the template.

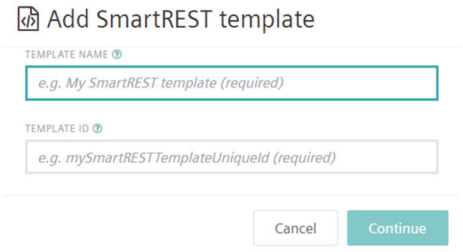


Create a new SmartREST template

1. Click "New Template" at the right of the top menu bar.

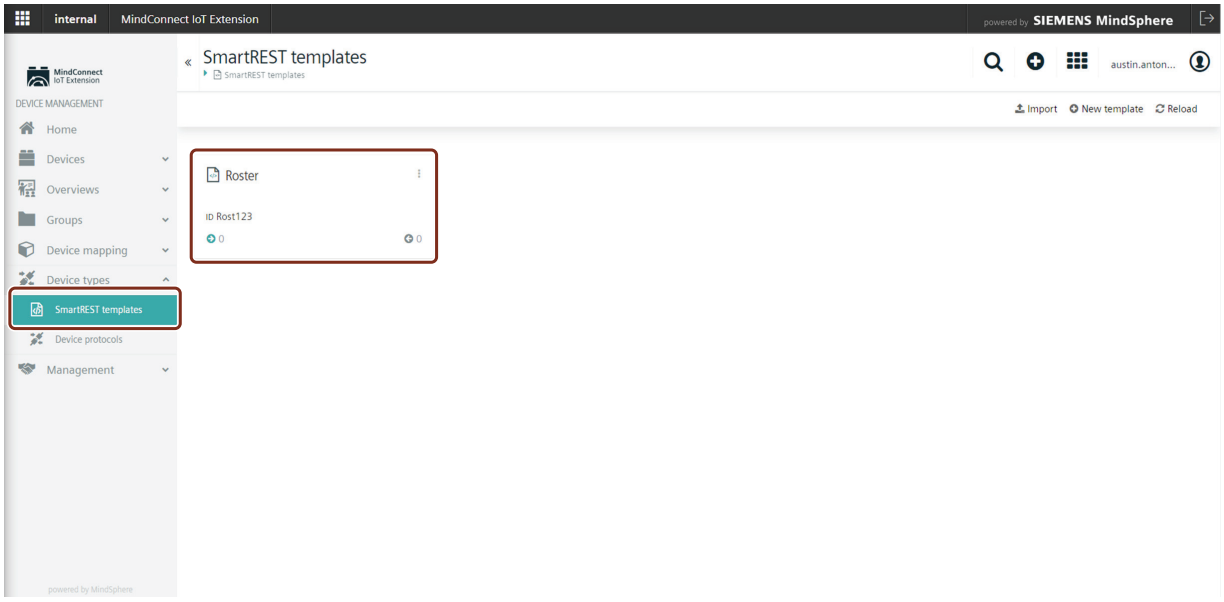


2. In the upcoming window, enter a template name and a unique template ID (both mandatory fields).
3. Click "Continue" to proceed adding messages or responses.



Add a message

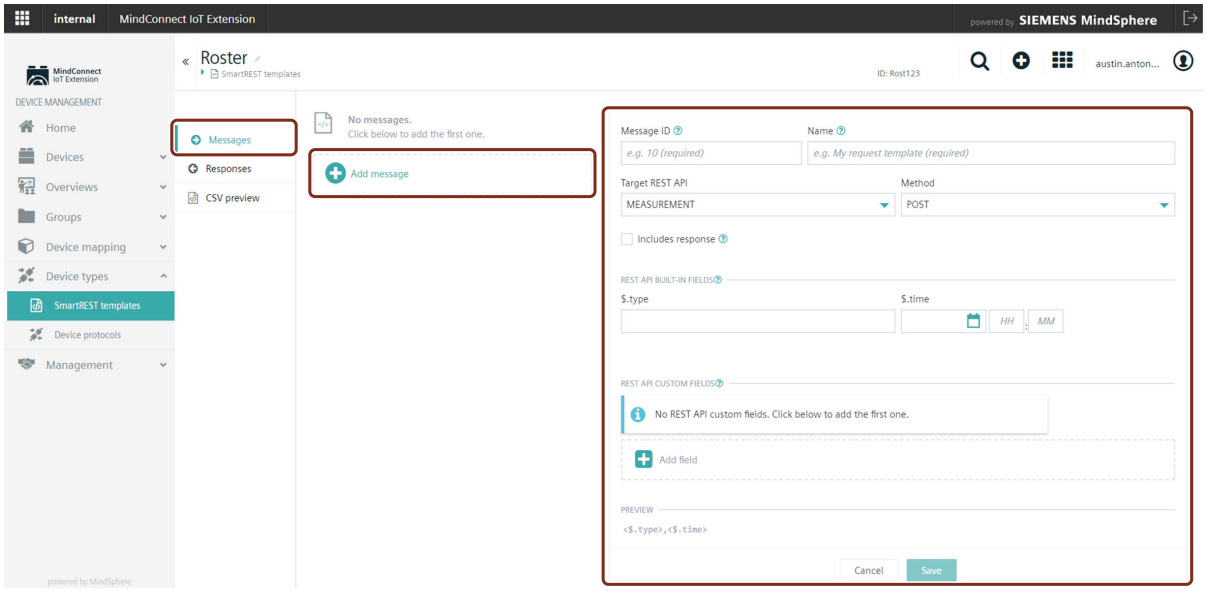
The message template contains all necessary information to convert the SmartRest request into a corresponding Rest API call which is then sent to the platform.



To add a new message, navigate to the "Messages" tab in your desired SmartREST template and click "Add message".

Thereafter, complete the following fields:

Field	Description
Message ID	Unique integer that will be used as a message identifier. It must be unique among all message and response templates.
Name	Name for the message. The is a mandatory requirement.
Target REST API	REST API for the target. Dropdown list. May be one of "Measurement", "Inventory", "Alarm", "Event", "Operation".
Method	Request method. May be one of "POST", "PUT", "GET", depending on the selected Target REST API.
Include Responses	Select this checkbox if you want to process the results of the request with response templates.
REST API built-in fields	These fields are optional and vary depending on the target REST API selected. In case no value is provided, a device will be able to set it when sending an actual message.
REST API custom fields	Additional fields can be added by clicking Add field. Enter the API key and select the desired data type.



In the "Preview" you can see the preview of your request message.

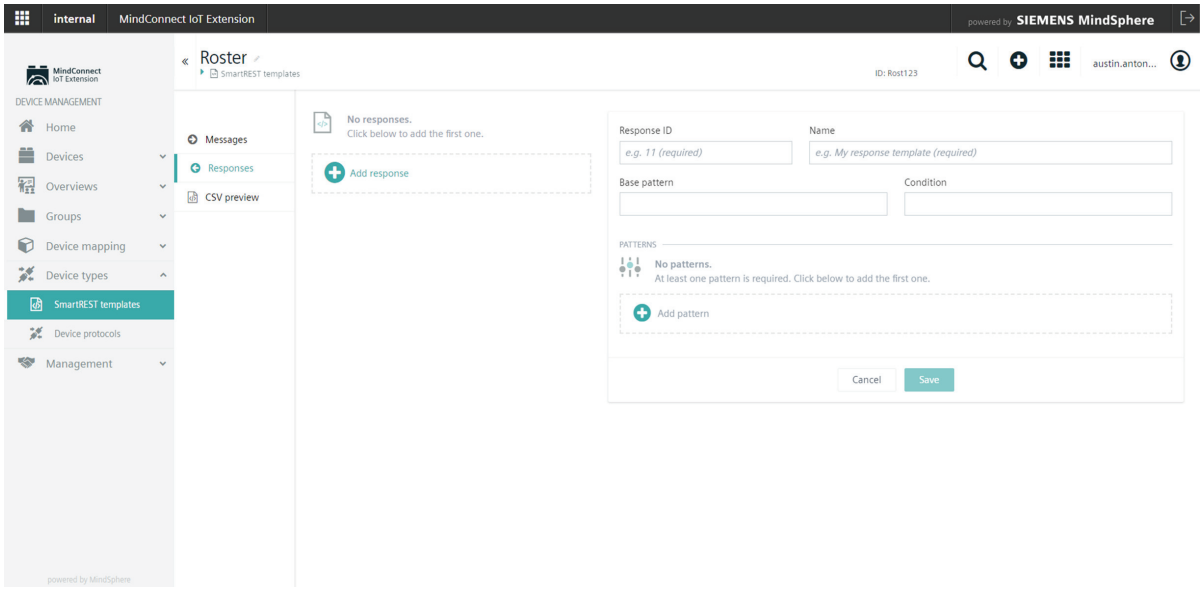
Click "Save" to save your settings.

To delete a message, open it and click "Remove" at the bottom.

Add a response

A response template contains the necessary information to extract data values from a platform REST API call response, which is then sent back to the client in a IoT Extension data format.

To add a new response, navigate to the "Response" tab in your desired SmartREST template and click "Add response". Complete the following fields:



Field	Description
Response ID	Unique integer that will be used as a response identifier.
Name	Name for the response. Mandatory.
Base Pattern	Base pattern for the response.
Condition	Condition value of the response.
Pattern	At least one pattern is required. Click Add pattern and enter a pattern value.

Click "Save" to save your settings.

To delete a response, open it and click "Remove" at the bottom.

Edit or delete a SmartREST template

To edit a SmartREST template, either click the desired template or click the menu icon and in the context menu click "Edit".

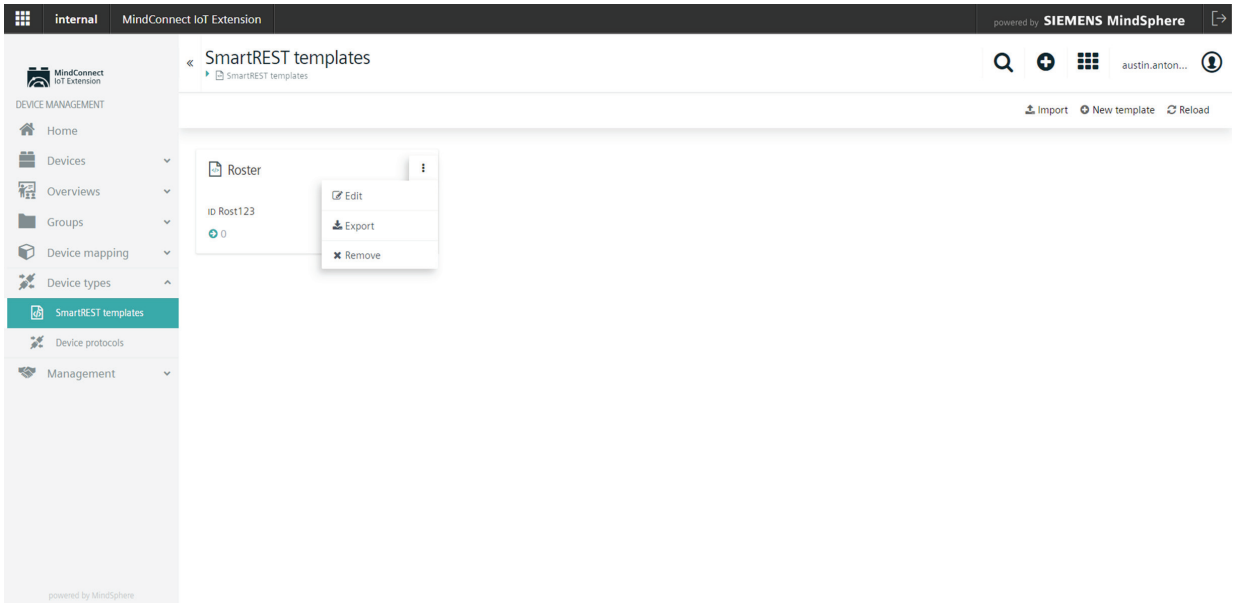
To delete a SmartREST template, click "Remove" in its context menu.

Export a SmartREST template

To export a SmartREST template, click the menu icon and in the menu click "Export". The template will automatically be downloaded.

To export a SmartREST template as IoT Extension file follow these steps:

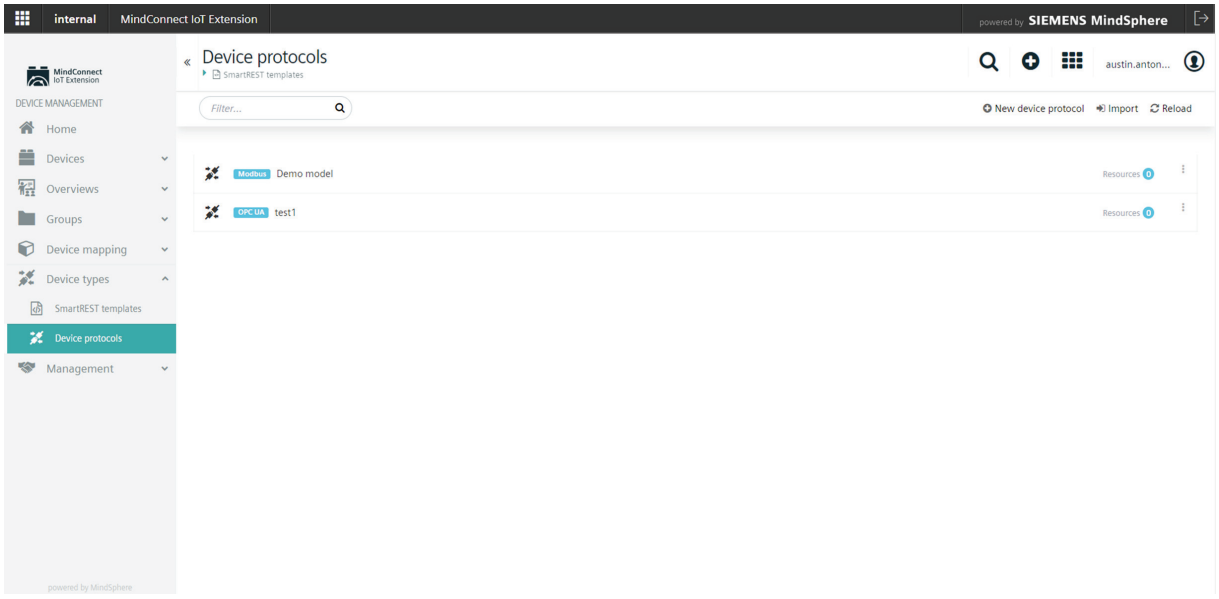
1. Open the template of your choice and select the IoT Extension preview tab.
2. In the IoT Extension preview tab which provides additional information on messages and responses, click "Export IoT Extension".
3. In the upcoming window, specify the preferred options for the field separator, decimal separator and character set.
4. Click "Download" to download the template as IoT Extension file.



5.4.2 Device protocols

To process data from various device types, IoT Extension uses device protocols.

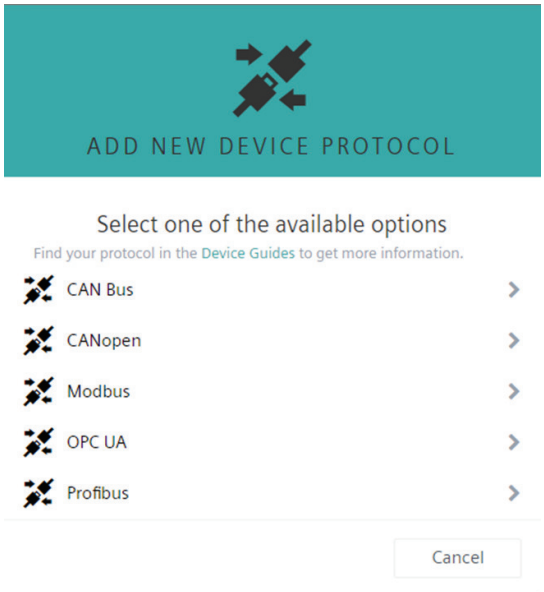
Click "Device protocols" in the "Device types" menu to access the "Device protocols" page.



In the "Device protocols" page you will find a list with all device protocols available in your account.

Add a device protocol

1. Click “New device protocol” in the top menu bar.

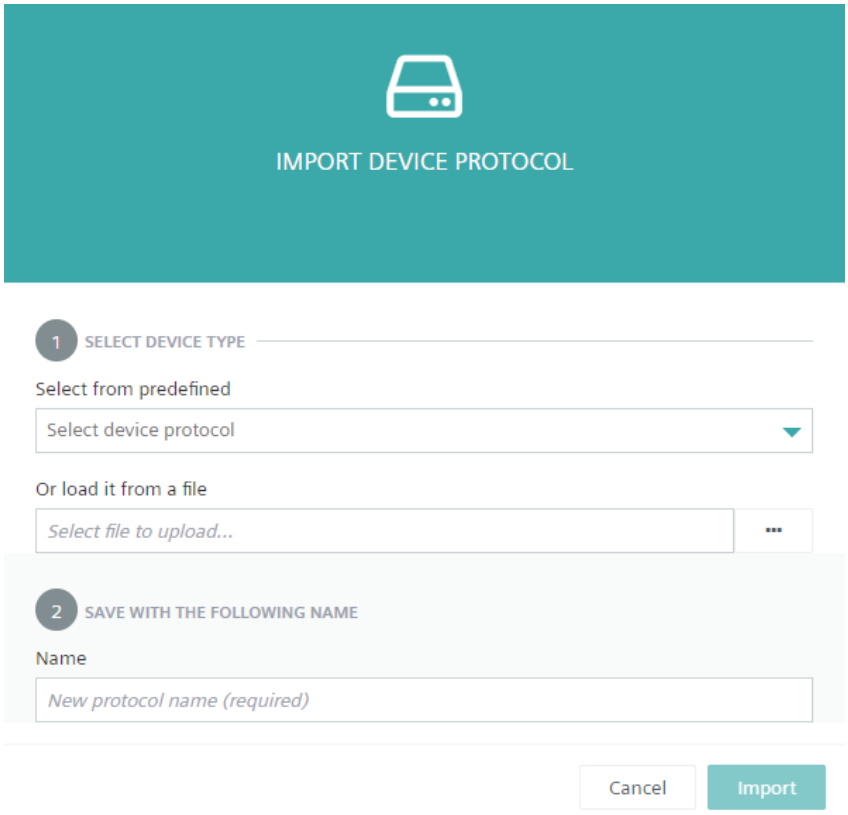


2. Select one of the available device protocol types from the list.
3. In the resulting dialog box, enter a name and an optional description for the device protocol and click “Create”.
4. Enter the configuration for the device protocol. The configuration of the device protocol depends on the protocol type.
5. For details on configuring device protocols, follow the documentation of the particular device type you want to create, see AUTOHOTSPOT.
6. Click “Save”.

Import a device protocol

To add a device protocol from an existing protocol, perform the following steps:

1. Click “Import” in the top menu bar.



2. Either select the device protocol to be imported from a list of predefined protocols or load it from a file by browsing.
3. Provide a name for the new protocol and click “Save”.
   The device protocol will be added to the device database.

Edit a device protocol

To edit a device protocol, click on the protocol or click the menu icon at the right of the row and then click “Edit”.

Details on the fields can be found in the documentation of the particular device type, see AUTOHOTSPOT.

Remove a device protocol

To remove a device protocol, click the menu icon at the right of the row and then click “Remove”.

The device protocol will be removed from the device database.

5.5 Management repositories

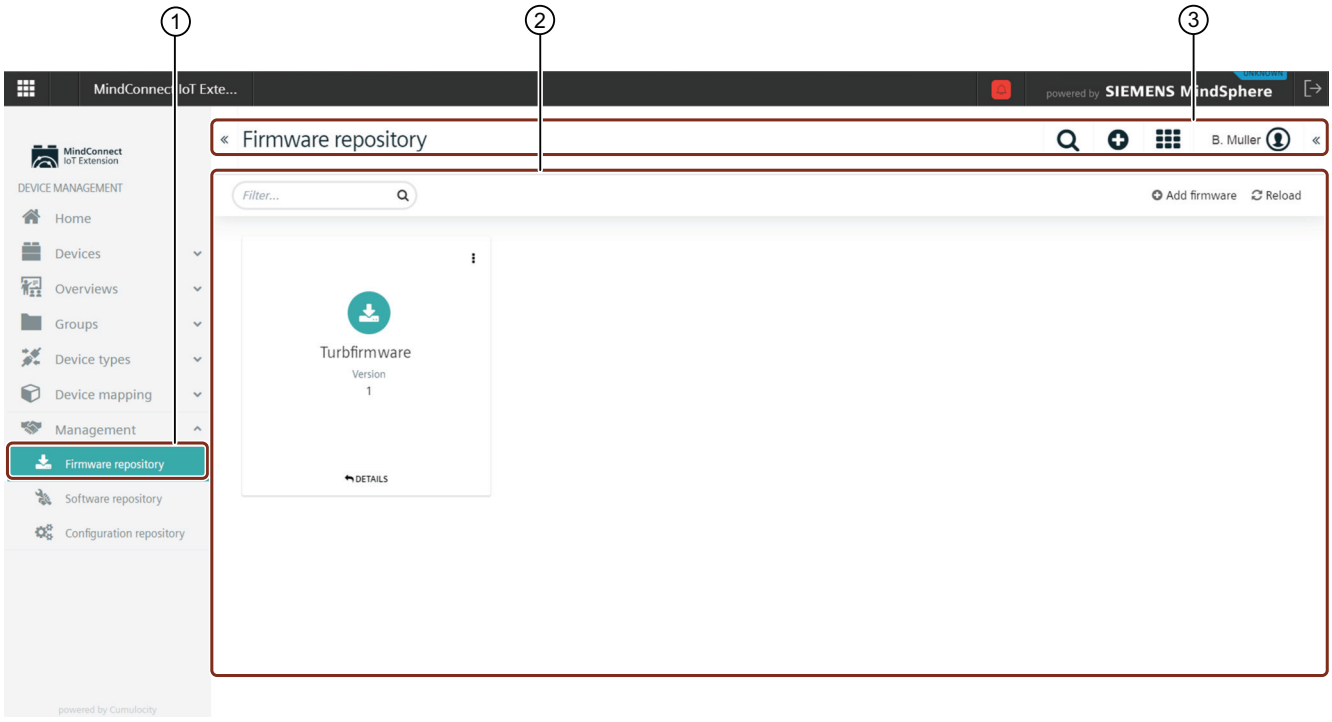
5.5.1 Firmware repository

In the "Firmware repository" and in the "Software repository" IoT Extension offers to collect reference firmware and software for devices respectively.

Managing device firmware

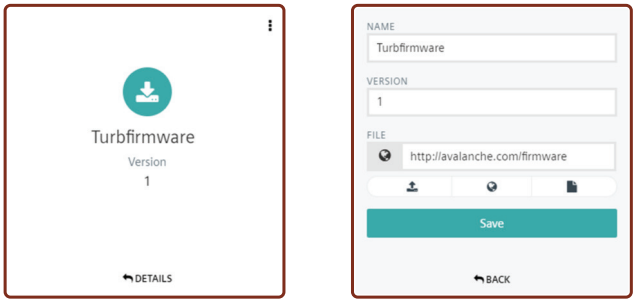
Open the "Firmware repository" from the "Management" menu in the navigator.

The available firmware objects will be displayed, presented as cards in a grid.



① Left navigation option menu
② Tools menu
③ Workspace

Click "Details" on a specific object to "turn around" its card and display details.



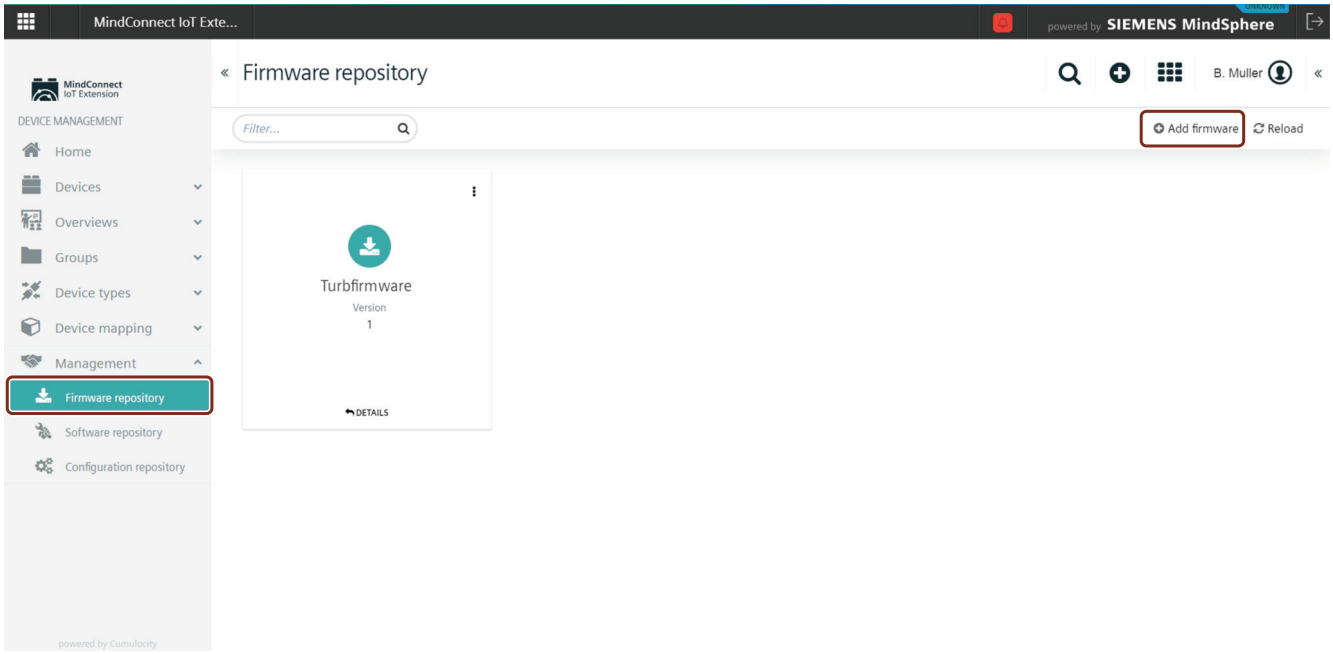
In addition to the object name and version, you will here find the name of the file containing the firmware.

Moreover, several buttons allow you to update the information (see also "Add a firmware object" below).

Add a firmware object

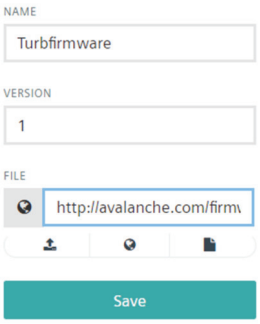
To add a firmware object, follow these steps:

1. Upload the firmware file in the "Administration" application. This step is not necessarily required since some manufacturers offer the firmware online.
2. In the Firmware repository page, click "Add firmware" at the right of the top bar menu.



3. In the pop-up window, enter a name for the firmware and its version.

4. Specify the file for the firmware by choosing or uploading it or enter the URL from which the device can download the firmware.
5. Click "Save" to save your settings.



Install a firmware on device

Open the device list by clicking "All devices" in the navigator and select a device from the device list.

Open the Software tab for the device and click "Install firmware".

For further information on these steps, refer to the description of the Software tab.

Note

To store other types of binaries in IoT Extension, switch to the Administration application.

Install firmware on multiple devices

IoT Extension offers the option to execute firmware or software updates for multiple devices at once. To do so, follow these steps:

1. Execute the software update in a single device to test that the new version works.
2. Navigate to operation and select "Execute" for the whole group.
3. Fill the form to schedule the bulk operation and click "Create".

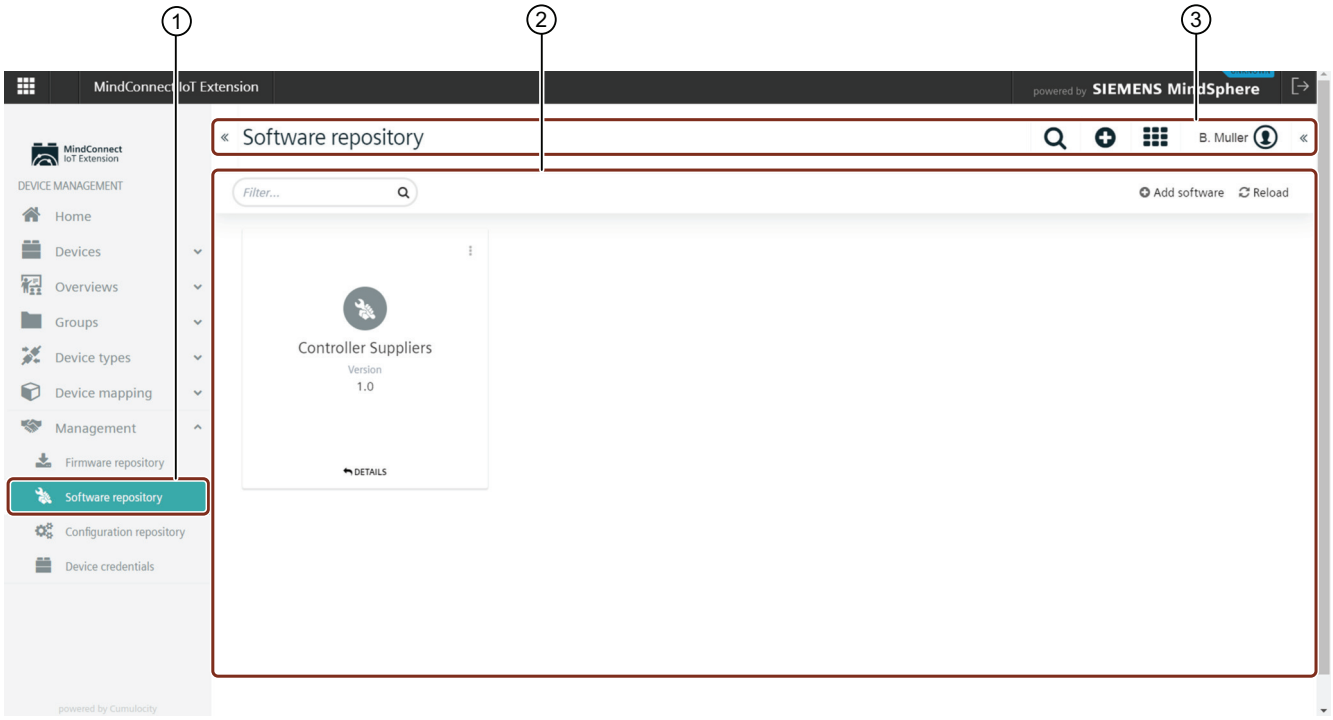
The operation status can be viewed in the "Bulk Operation" tab of the selected group.

5.5.2 Software repository

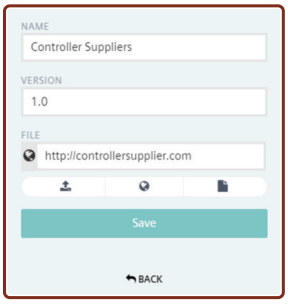
Managing device software

Open the "Software repository" from the "Management" menu in the navigator.

The available software objects will be displayed, presented as cards in a grid.



Click "Details" on a specific object to "turn around" its card and display details.



In addition to the object name and version, you will here find the name of the file containing the software.

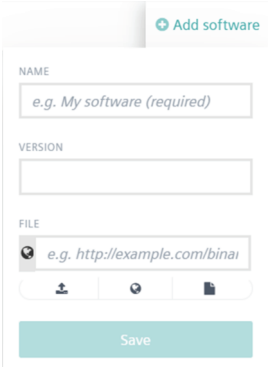
Moreover, several buttons allow you to update the information (see also "Add a new software" below).

Add a new software

To add a new software, proceed with the following steps:

1. Click "+Add software" from the top right corner of the "Software Repository" screen.
2. In the pop-up window, enter a name for the firmware and its version.

3. Specify the file for the firmware by choosing or uploading it or enter the URL from which the device can download the firmware.
4. Click "Save" to save your settings.

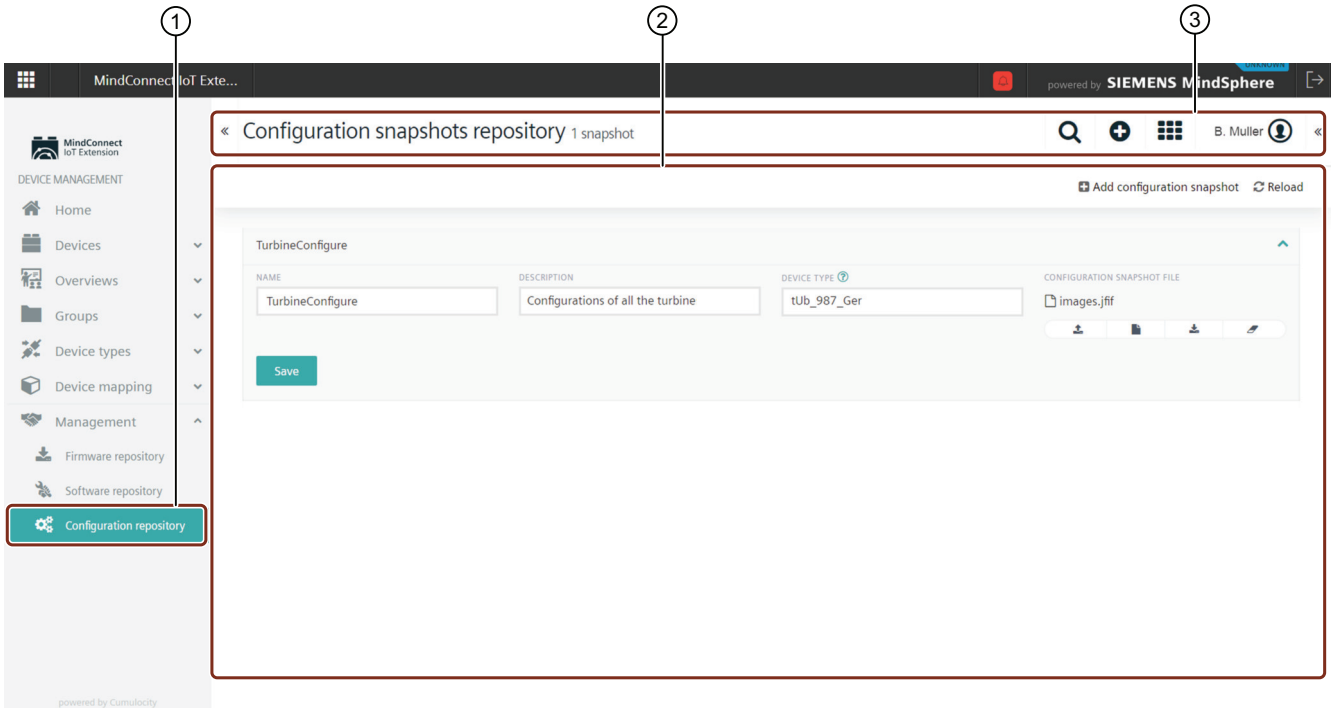


5.5.3 Configuration repository

IoT Extension allows to retrieve configuration data and store and manage it in a "Configuration repository". The configuration data contains the parameters and the initial settings of your device.

Configuration snapshots help you, for example, to apply the same configuration to multiple devices as described below.

In the "Configuration repository" page which you open from the "Management" menu in the navigator, all available configurations are listed. Each entry shows the configuration name, the device from which it has been uploaded and the upload timestamp.



① Firmware option in the navigation menu
② Display area
③ Tools menu

Parameters table

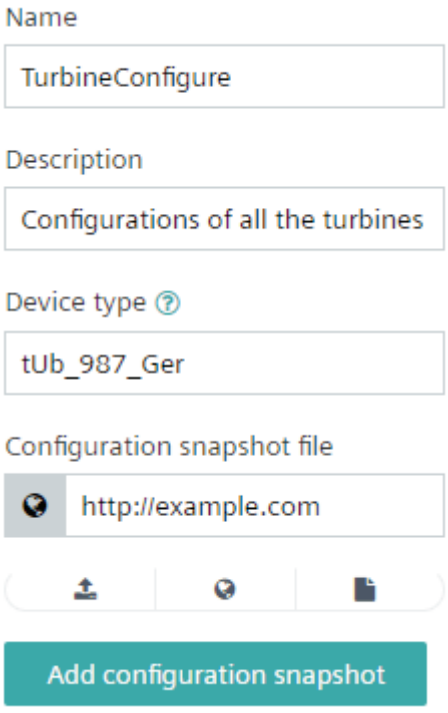
Click a configuration in the list to open it. You may modify the settings according to requirements and apply them by clicking "Save" as shown in ②. Refer to the section below for details on the fields.

Field	Description
Name	Name for the configuration snapshot. This is a mandatory field.
Description	Short summary of the configuration snapshot.
Device Type	Type of the device.
Configuration snapshot file	
Upload	Browse and upload the configuration file.
Choose file	Select files from the uploaded files if multiple files are uploaded.
Download	Download the latest upload file.
Clear	Remove all the uploaded files at once.

Add a snapshot configuration from a file

To add a new configuration from a file, follow these steps:

1. Click "Add configuration snapshot" at the right of the top menu bar.
2. In the upcoming window, enter a unique name and optional description for the configuration.
3. In the "Device type" field, enter a device type. The device type can be found in the Info tab of the target device.
4. Select the configuration snapshot file by uploading or choosing a file or providing an external URL.
5. Click "Add configuration snapshot" to save your settings.



The snapshot will be added to the "Configuration" repository.

Retrieve a current snapshot from a device

In addition to adding configurations from a file you can also add configurations by retrieving them from a device.

In order to retrieve a current configuration snapshot from a device, follow these steps:

1. Navigate to the desired device and open its "Configuration" tab.
2. Under "Configuration snapshot file", click at the top right.

The retrieved snapshot can be found in the "Configuration" repository, accessed through the "Management" menu of the navigator.

Apply a configuration snapshot to a device

In order to apply a configuration snapshot to a device, follow these steps:

1. Navigate to the desired device and open its "Configuration" tab.
2. Under "Configuration snapshot file", select a configuration from the dropdown field.
3. Click "Put new snapshot to device" to apply the selected snapshot to the device.

Apply a snapshot configuration from one device to another

In order to apply a configuration snapshot from one device to another, follow these steps:

1. Navigate to the device which has your desired configuration and open the "Configuration" tab.
2. Under Configuration snapshot, click "Get new snapshot from device" at the top right.
3. Navigate to the other device and open its "Configuration" tab.
4. Under "Configuration" snapshot, select the new configuration from the dropdown field and click "Put new snapshot to device".

Note

When you apply snapshot configuration from one device to another, the configuration may contain data which is device-specific.

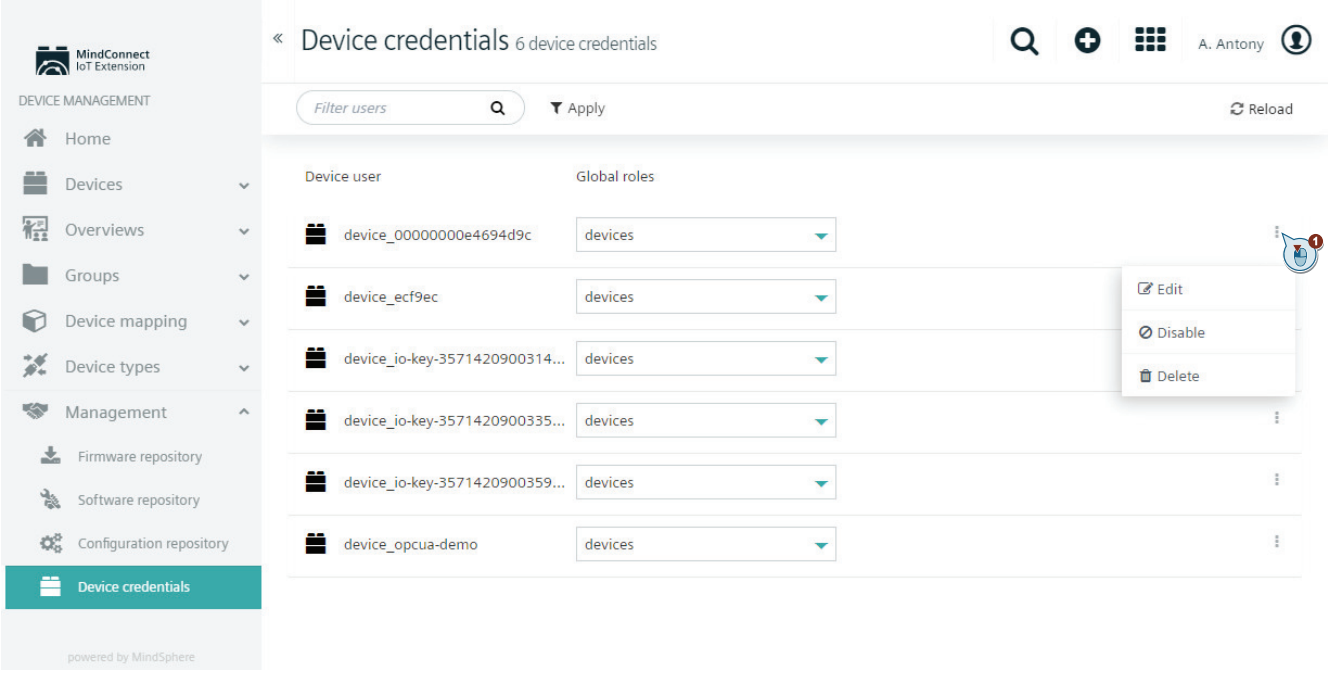
5.5.4 Device credentials

The "Device credentials" tab lists all credentials that have been generated for your connected devices. Each device that has been registered shows up here with the naming convention "device_<id>".

Click the arrow in the "Global roles" column of a device to open a list with available global roles. Assign or remove permissions for an individual device by selecting/ deselecting roles, and click "Apply" to save your settings.

Click the menu icon at the right of a device to access the following functionalities:

- "Edit" - To open the device credential details (see below).
- "Disable" - To temporarily disconnect a device.
- "Delete" - To delete the credentials of a device. This might be required if you have carried out a factory reset on a device. In this case, the device will often loose its assigned credentials. Delete it and continue with the normal registration process to re-register the device.



In the details page of any particular device credentials you can

- Disable/enable a device with the "Active" slider,
- Change the password for a device,
- Assign or remove permissions for an individual device by selecting/deselecting roles in the "Global roles" list.

5.6 Cloud Fieldbus

Cloud Fieldbus is an IoT Extension application with the ability to collect data from fieldbus devices and remotely manage them. This section describes how to

- Connect fieldbus devices.
- Manage the connected fieldbus devices.
- Configure the remote management capabilities of particular types of devices and import and export them.

It is supported out of the box by the following terminals:

- Pssystec Smartbox-Modbus for Modbus/RTU
- Netcomm Wireless NTC-6200 for Modbus/TCP and Modbus/RTU
- Cinterion Java modules for Modbus/RTU and CAN bus
- Pssystec SmartBox DP for Profibus

Connecting Fieldbus devices

For the following instructions, we assume you have a "Cloud Fieldbus" terminal available and it is registered as a device in your IoT Extension tenant. To register a terminal with IoT Extension, follow the instructions provided with the terminal.

Connecting Modbus/RTU devices

To connect a Modbus/RTU device:

1. Physically wire the Modbus/RTU device through RS/485 or RS/232 to the terminal.
2. Give the device a unique Modbus address according to the instructions provided with the Modbus device (e.g. by setting a jumper on the device).
3. Check the serial communication settings of the device according to the instructions provided with the device (i.e. baud rates and communication protocol). These have to match with all devices on the bus.
4. In the Device Management application, click "All devices" in the Devices menu in the navigator. In the device list, select the terminal and switch to the "Modbus" tab.
5. Change the communication settings shown in the section "Serial communication" to match the settings on the bus, if needed.
6. Change the transmit rate and the polling rate according to your requirements. The polling rate is the frequency at which the Modbus devices are polled for changes. The transmit rate is the frequency where measurements are sent to IoT Extension.
7. Click "Save changes" if you made changes.
8. To start communication between the terminal and the Modbus device, click "Add new device".
9. Enter a name for the device and select the type of the device from the drop-down field. To add new device types, see "Configuring Fieldbus device types" below. Set the Modbus address of the connected device.
10. Click "Add". IoT Extension will now send a notification to the Modbus terminal that a new device is ready to be managed. This may take a few seconds.

After completion, a new child device has been added to the terminal and can now be managed. You can click on the name of the device in the table to navigate to the device. If you have not yet added Modbus devices to the terminal, you may have to reload your browser window to make the "Child Devices" tab visible.

Connecting Modbus/TCP devices

To connect a Modbus/TCP device:

1. Make sure that the Modbus/TCP device is connected to the terminal, i.e. directly through an Ethernet cable or through a switch. If you are using a Modbus gateway, configure the gateway in a way it can communicate with the Modbus devices behind the gateway.
2. Check the network settings of the device using the instructions provided with the device.
3. In the Device Management application, click All devices in the Devices menu in the navigator. In the device list, select the terminal and switch to the Network tab. Verify that the LAN settings of the terminal match the settings of the device so that TCP communication can be established.
4. Switch to the "Modbus" tab.

5. Change the transmit rate and the polling rate according to your requirements. The polling rate is the frequency at which the Modbus devices are polled for changes. The transmit rate is the frequency at which measurements are sent to IoT Extension.
6. Click "Save changes" if you made changes.

Adding child devices

1. To start communication between the terminal and the Modbus device, click "Add new device".
2. Enter a name for the device and select the type of the device from the dropdown field. To add new device types, see "Configuring Fieldbus device types" below. Set the Modbus address and the IP address of the connected device.
3. Click "Add".

IoT Extension will now send a notification to the Modbus terminal that a new device is ready to be managed. This may take a few seconds.

Connecting CAN devices

To connect a CAN device:

1. Physically wire the CAN device through to the terminal.
2. Check the serial communication baud rate of the device according to the instructions provided with the device. These have to match all devices on the bus.
3. In the Device Management application, click All devices in the Devices menu in the navigator. In the device list, select the terminal and switch to the CAN bus tab.
4. Change the baud rate setting shown in the section CAN bus communication to match the settings on the bus, if needed.
5. Change the transmit rate according to your requirements. The transmit rate is the frequency where measurements are sent to IoT Extension.
6. Click "Save changes" if you made changes.

Adding child devices

1. To start communication between the terminal and the CAN device, click "Add CAN device".
2. Enter a name for the device and select the type of the device from the dropdown field. To add new device types, see "Configuring Fieldbus device types" below.
3. Click "Add".

IoT Extension will now send a notification to the Fieldbus terminal that a new device is ready to be managed. This may take a few seconds.

After completion, a new child device has been added to the terminal and can now be managed. You can click on the name of the device in the table to navigate to the device. If you have not yet added Fieldbus devices to the terminal, you may have to reload your browser window to make the "Child Devices" tab visible.

Connecting Profibus devices

Connecting Profibus differs slightly from the regular Plug & Play approach of Cloud Fieldbus. The gateway device acts as slave on the Profibus so it can easily be integrated into existing infrastructure. This means that Profibus data must be actively sent to the gateway though. Typically this is done by programming a PLC to actively send information to the gateway via it's configured Profibus slave address.

1. Physically wire the Profibus device to the terminal.
2. In the Device Management application, click "All devices" in the Devices menu in the navigator. In the device list, select the terminal and switch to the "Profibus" tab.
   Profibus settings
3. The baud rate is automatically detected by the gateway and is just being displayed here.
4. Change the transmit rate according to your requirements. The transmit rate is the interval at which measurements are sent to IoT Extension.
5. Set the slave address of the terminal.
6. Configure your Profibus Master device to communicate to that slave address. To do so, refer to the gateway manual (e.g. SmartBox DP).
7. Click "Save" to update the gateway with the new settings.

Adding child devices

1. To start communication between the gateway and the Profibus device, click "Add Profibus device".
2. Enter a name for the new device.
3. Select the type of the child device from the drop-down box. To add new device types, see "Configuring Fieldbus device types" below.
4. Click "Add" to confirm and notify the gateway.

Now a child device will be created containing the data configured in the selected device type.

IoT Extension will notify the gateway to send data for the newly created child device.

Managing Fieldbus devices

Once connected, you can now manage your device. Switch to the Child devices tab of a device to list the connected Fieldbus devices and navigate to a Fieldbus device. Depending on the capabilities of the device and its configuration in IoT Extension, you can:

- Collect measurements
- Send alarms on coil or register changes
- Log coil and register changes as events
- Monitor the status of coils and registers

Collecting measurements

If the device type of the Fieldbus device is configured to collect measurements, these will be visible in the Measurements tab. They will also be available for usage in the "Data Explorer" and in "Dashboard widgets".

Data is collected according to the interval specified in the "transmit rate" property of the terminal as described above. To optimize the data traffic, data that is exactly the same as collected previously may not be sent again.

Monitoring alarms

If the device type of the Fieldbus device is configured to send alarms, these will be visible in the Alarms tab and usable in widgets. To determine the alarm status, the Fieldbus devices are monitored for changes according to the "polling rate" setting of the terminal. If a particular coil or register is non-zero, an alarm will be raised. If the value goes back to zero, the alarm will be cleared.

Logging events

Similar to alarms, changes in Fieldbus devices can be monitored and logged as events. Each time, the value of the monitored coil or register changes, an event is created. You can see the events in the "Events" tab of the device or use them in widgets. You can inspect the new value of the monitored coil or register by clicking on the event and unfolding the event details.

Monitor a device status

The status of devices can be monitored in real time using dashboard widgets in the Cockpit application. Navigate to the Cockpit application, create a dashboard or report, and add widgets as described in the Cockpit section in the User guide. The Cloud Fieldbus has two new widgets: The "Fieldbus Device" widget and the "SCADA" widget.

Monitoring device status using the Fieldbus Device widget

The Fieldbus Device widget provides you with a tabular display of the status of a device. The status of the device can also be modified through the widget.

To use the Fieldbus Device widget, follow these steps:

1. Select a dashboard and click "Add widget" in the top menu bar.
2. Select the Fieldbus Device Widget and edit the title of the widget.
3. Choose the device that should be shown in the widget in the Target assets or devices section.
4. Select the coils and registers that should be shown on the widget.

In the widget, the selected coils and registers are grouped into display categories as configured in the device type. The Fieldbus Device Widget updates automatically as soon as there is new data available. You do not need to click on reload.

Registers and coils that can be changed are represented by active widgets. If you click a switch, an operation to change the corresponding coil or register is sent to the terminal. Similar, if you change a value and click "Set", an operation is created. The terminal will then carry out the

configuration change on the device, as requested through the operation. While the operation is being processed, a progress indicator is shown.

Monitoring status using the SCADA widget

The SCADA widget provides you with a graphic representation of the status of a device.

To use the SCADA widget, follow these steps:

1. Select a dashboard and click "Add widget" in the top menu bar.
2. Select the SCADA widget and edit the title of the widget.
3. Choose the device that should be shown in the widget in the Target assets or devices section.
4. Upload an SVG file with the graphic representation of the device. SVG files are vector graphics that have to be specifically prepared with placeholders for the status information. See Preparing SVG files for the SCADA widget below.
5. Assign placeholders to devices. Note that multiple devices can be taken as source.
6. You now need to assign each placeholder to a property of the device. Hover over each placeholder and select "Assign device property" or "Assign fieldbus property". A dialog box comes up, in which you can choose basic device properties or fieldbus properties (i.e. status coils and registers). Select the desired property and click "Select".
7. After assigning all placeholders, a preview of the widget with the current values of the properties is shown. Click "Save" to place the widget on the dashboard.

Preparing SVG files for the SCADA widget

The SCADA widgets inspect uploaded SVG files for placeholders. These placeholders are replaced by actual values from devices. Placeholders have a specific syntax and can be used anywhere in the SVG file. To add a placeholder, enter the name of the placeholder in double curly braces using your design application or a text editor.

When creating svg files, we recommend you to use "https://boxy-svg.com/". It is easy to use, quality chrome extension.

```
<text class="text" xt-anchor="middle" x="100" y="236.982125"
width="200" ...>
    {{batteryValue}}
</text>
```

Configuring Fieldbus device types

New Fieldbus device types can be set up in the Device database page which you open from the Device Types menu in the navigator.

Click "New" in the top menu bar. In the Device type field, select the protocol of your device and enter a name for it.

Now you can start adding coils and register definitions to the device type, depending on the selected protocol (see the descriptions below).

Configuring Modbus data
Adding a coil definition

Click "Add" at the top right of the Coils (discrete inputs) section, to add a coil definition. This will open a dialog to specify the coil. Enter the following information:

1. Enter the name of the coil as being displayed in the user interface.
2. Optionally, enter the display category to structure your data in widgets.
3. Enter the number of the coil in the Modbus device.
4. Select the "Show status" checkbox if you want to show the coil's current value in the Fieldbus Device Widget. In this case, you can enter the text that the Fieldbus Device Widget should show for unset and set coils.
5. Select the "Update status" checkbox if you want to be able to edit the coil from the Fieldbus Device Widget.
6. Select the "Raise alarm" checkbox if an alarm should be raised when the coil is set in the device. In this case, you can specify the type of the alarm that is raised, its text and its severity. Note that there can only be one alarm active of a particular type for a particular device.
7. Select the "Send event" checkbox if an event should be generated each time the value of the coil changes. If "Send event" is selected, you can specify the type of event and the text in the event.
8. Click "OK" to finish editing the coil.

The same functions are available for discrete inputs. However, it is not possible to update the status of a discrete input.

Adding a register definition

Click "Add" at the top right of the Holding registers section, to add a register definition. This opens a dialog to enter the details of the register definition:

1. Enter the name of the register being displayed in the user interface.
2. Optionally, enter the display category to structure your data in widgets.
3. Enter the number of the register in the Modbus device. You can indicate a subset of bits to be used from a register by providing a start bit and a number of bits. This allows you to split a physical Modbus register into a set of "logical registers".
4. To scale the integer value read from the Modbus device, you can enter a multiplier, a divisor and a number of decimal places. The register value is first multiplied by the "multiplier", then divided by the "divisor" and then shifted by the number of decimal places. Note, that the terminal may use integer arithmetic to calculate values sent to IoT Extension. For example, if you use a divisor of one and one decimal place, a value of 231 read from the terminal will be sent as 23.1 to IoT Extension. If you use a divisor of ten and no decimal places, the terminal may send 23 to IoT Extension (depending on its implementation).
5. Indicate the unit of the data, for example, "C" for temperature values.
6. Select the "Signed" checkbox if the register value should be interpreted as signed number.

7. Select the "Enumeration type" checkbox if the register value should be interpreted as enumeration of discrete values. If Enumeration type is selected, you can click "Add value" to add mappings from a discrete value to a text to be shown for this value in the widget. Click "Remove value" to remove the mapping.
8. Select the "Show status" checkbox if you want to show the current value of the register in the Fieldbus Device Widget.
9. Select the "Update status" checkbox if you want to be able to edit the register from the Fieldbus Device Widget. If Update status is selected, two additional fields Minimum and Maximum appear. Using these fields, you can constrain numerical values entered in the widget.
10. Select the "Send measurement" checkbox if you want the values of the register to be regularly collected according to the transmit interval (see above). In this case, add a measurement type and a series to be used. For each measurement type, a chart is created in the Measurements tab. For each series, a graph is created in the chart. The unit is used for labelling the measurement in the chart and in the Fieldbus Device Widget.
11. Select the "Raise alarm" checkbox if an alarm should be raised when the register is not zero in the device measurement. In this case, you can specify the type of the alarm raised, its text and its severity. Note, that there can only be one alarm active of a particular type for a particular device.
12. Select the "Send event" checkbox if an event should be generated each time the value of the register changes. If "Send event" is selected, you can specify the type of event and the text in the event.
13. Click "OK" to save your settings.

In the Options section, select the checkbox "Use server time" to create the time stamps for data on the server instead of on the terminal. If you need to support buffering of data on the terminal, leave this checkbox clear.

Finally, click "Save" to save your settings.

If you edit a device type that is currently in use, you may need to

- restart the terminals that use the device type,
- reconfigure dashboards and widgets that use the device type.

Configuring CAN bus data

CAN device types can be configured in a very similar way as Modbus device types. For more information, see "Configuring Modbus" data above. The differences are:

- Holding registers are used to describe the different pieces of data inside CAN messages.
- Enter the CAN message ID of the specific message the data should be extracted from. Use a hexadecimal number for the message ID.
- Conversion of values is extended by an offset parameter. This will be added or subtracted from the register value, depending on its sign. The offset calculation is done after applying multiplier and divisor, and before performing decimal shifting.

Configuring Profibus data

To configure a Profibus device type, select "Profibus" as device type from the dropdown list and enter a name for it.

In the Register section, click "Add" at the right to add one or more register definitions as described exemplarily for Modbus devices in "Adding a register" definition above.

In the Options section, select the checkbox Use server time to create the time stamps for data on the server instead of on the terminal. If you need to support buffering of data on the terminal, leave this checkbox clear.

Finally, click "Save" to save your settings.

If you edit a device type that is currently in use, you may need to

- restart the terminals that use the device type,
- reconfigure dashboards and widgets that use the device type.

Configuring CANopen data

There are two ways to create a new device type. Either manually from scratch via the “New” operation or via import of an EDS file for the corresponding device.

Manually creating a new device type from scratch

Navigate to the Device database page and click "New". A new window will open.

Select “CANopen” as fieldbus type and enter a name for your device type. Specific to CANopen is the CANopen device type field which accepts a hex number.

In the Variables section, you determine the CANopen variables. Variables inside the “Object Dictionary”(OD) of the CANopen device can be accessed later by adding the variables to the device type definition. Via the "Add" button at the right of the Variables section, new variables can be configured.

The following fields can be observed:

- "Name": The name of the variable.
- "Display category": This field is used to group variables into sections in the visualization.
- "Index": Index of the variable in the OD of the device.
- "Sub-index": Sub-Index of the variable in the OD of the device.
- "Data type": The type of the variable (e.g. boolean, unsigned).
- "Access type": E.g. read only, write only, etc.
- "Unit": Logical unit of the variable.
- "Show status": Defines how the variable is shown in the inventory.
- "Update status": Defines how the variable is updated in IoT Extension.
- "Send measurement": Create a measurement when the value of the variable is changed.

- "Raise alarm": Create an alarm if a given mask matches with the value of the variable ((value & mask) == mask). Therefore, it is possible to raise alarms on single bits of e.g. an Unsigned8 variable, like the Error-Register.
- "Raise event": Create an event, whenever the value of the variable is changed.

After adding variables to the new device type, they are listed in the Variables section of the device type. All variables are grouped by the given display category, i.e. variables with same category are grouped together.

After completing your configuration, click "Save" to save your settings. The device type can be used now to add CANopen devices to the platform. The device type can be updated after creation.

Importing a device type

To import a new device type, see the Exporting and importing device types section.

After importing the EDS file, all variables defined in the file are listed in the Variables section of the device type. The user can then enrich the imported variable configurations by opening the configuration dialog for each variable (e.g. the missing display category can be set or mappings can be defined).

Configuring CANopen device data

To configure CANopen device data navigate to the desired device and switch to the CANopen tab.

In the CANopen communication section, the following parameters can be configured:

- "Baud rate": This field must match with the used baud rate in the CANopen network.
- "Polling rate": The rate at which the agent sends requests to the CANopen devices. to determine changes in variables.
- "Transmit rate": The transfer rate, i.e. the rate at which the terminal sends regular measurements to IoT Extension.

In the CANopen section, up to 127 CANopen devices can be added to the gateway as child devices by giving the following parameters:

- "Name": The name of the device used for visualization.
- "Device type": The device type of the CANopen device. The user can select from a list of all CANopen device types which are stored in the device database.
- "Node ID": The CANopen node ID of the device. It is used for addressing the device inside the CANopen network.

The device type and node ID need to match with the real CANopen device, otherwise setting up the communication is not possible or wrong values will be transmitted.

Exporting and importing device types

To manage device types more conveniently, you can export device types to a file once they are edited in the user interface. The file can be re-imported to set up other IoT Extension accounts easily or to restore the types from a backup. The import functionality also supports importing ready-made device types provided by device manufacturers.

To export a device type, hover over the device type that you would like to export and click "Export". Your browser will download a file named "<device type>.json" with the device type definition.

To import a device type, click "Import" in the top menu bar. This will open a dialog that lets you choose between importing a ready-made device type and uploading a previously exported device type. You can change the name of the device type during import using the New device type name field.

Cockpit

6

6.1 Overview of Cockpit

The following sections will walk you through all functionalities of the "Cockpit" application in detail.

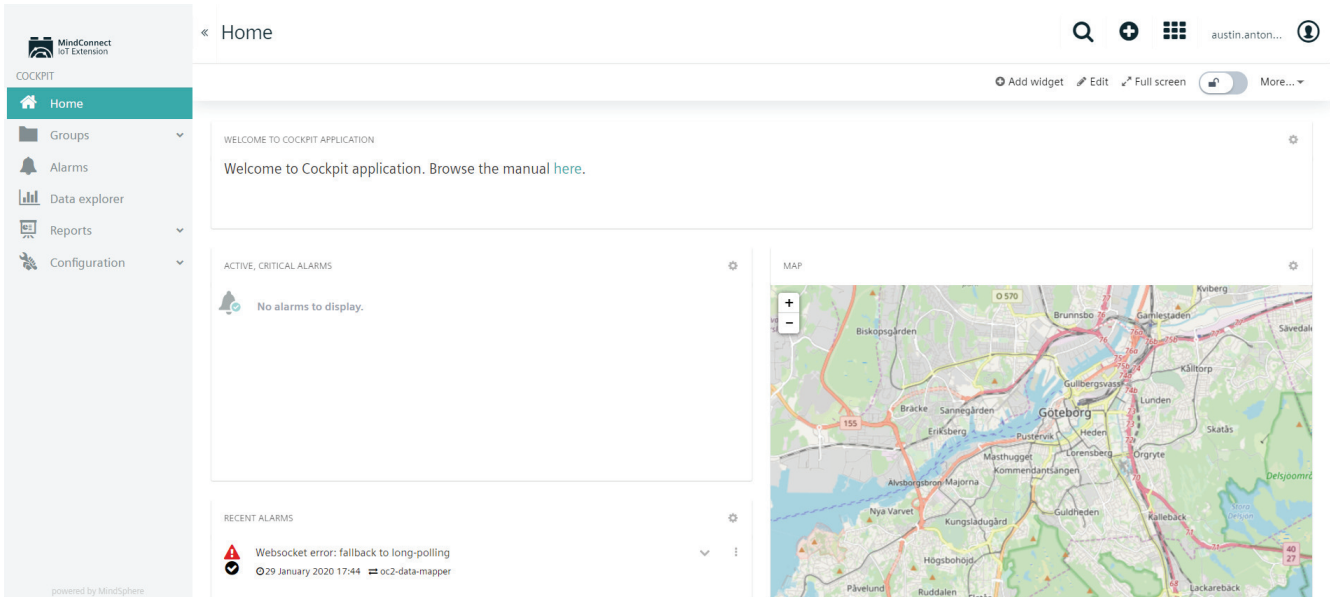
For your convenience find an overview on the content of this document below.

Section	Content
Managing assets (Page 142)	Organize assets in hierarchies by creating groups and assigning devices.
Visualizing data using the Data Explorer (Page 162)	Interactively explore, compare and visualize IoT data. Describes how to access and use the data explorer, add data points to the data explorer, customize data point properties, modify the visualization, store the data explorer as widget, and export the data.
Working with dashboards (Page 169)	Create your own analytics and monitor pages by adding and arranging widgets. Share dashboards among all devices of the same type.
Widgets collection (Page 146)	Use various types of widgets from the Widgets collection that comes with IoT Extension and configure them according your needs.
Working with alarms (Page 174)	Monitor problems of your assets using severities and workflows. Since working with alarms in the Cockpit application is actually the same as working with alarms in "Device Management", refer to "Working with alarms in Device Management".
Managing reports (Page 174)	Handle reports based on dashboard layouts, create reports for exporting data in CSV or excel format and schedule the export.
Using the Data Point Library (Page 179)	Manage default settings ("profiles") of your devices and apply them automatically using the Data Point Library.
Working with Smart Rules (Page 182)	Create and manage business rules to work on incoming data in realtime and to perform actions based on this data.
Smart Rules collection (Page 188)	Use pre-defined global Smart Rules to configure rules for geofencing, thresholds or alarm escalation and notifications (SMS/email/voice). Describes each SmartRule and its configurable parameters in detail.

If you want to learn more about general aspects of the IoT Extension platform and its applications, refer to IoT Extension Getting Started (https://documentation.mindsphere.io/resources/html/mindconnect-iot-extension-gs/en-US/index.html).

Home dashboard

The "Home" screen of the Cockpit application is a dashboard which shows data for the general tenant.



The data shown on the "Home" dashboard is shared by all users of the tenant. By default, the "Home" dashboard includes a welcome message, the active critical alarms, recent alarms and a map of all objects.

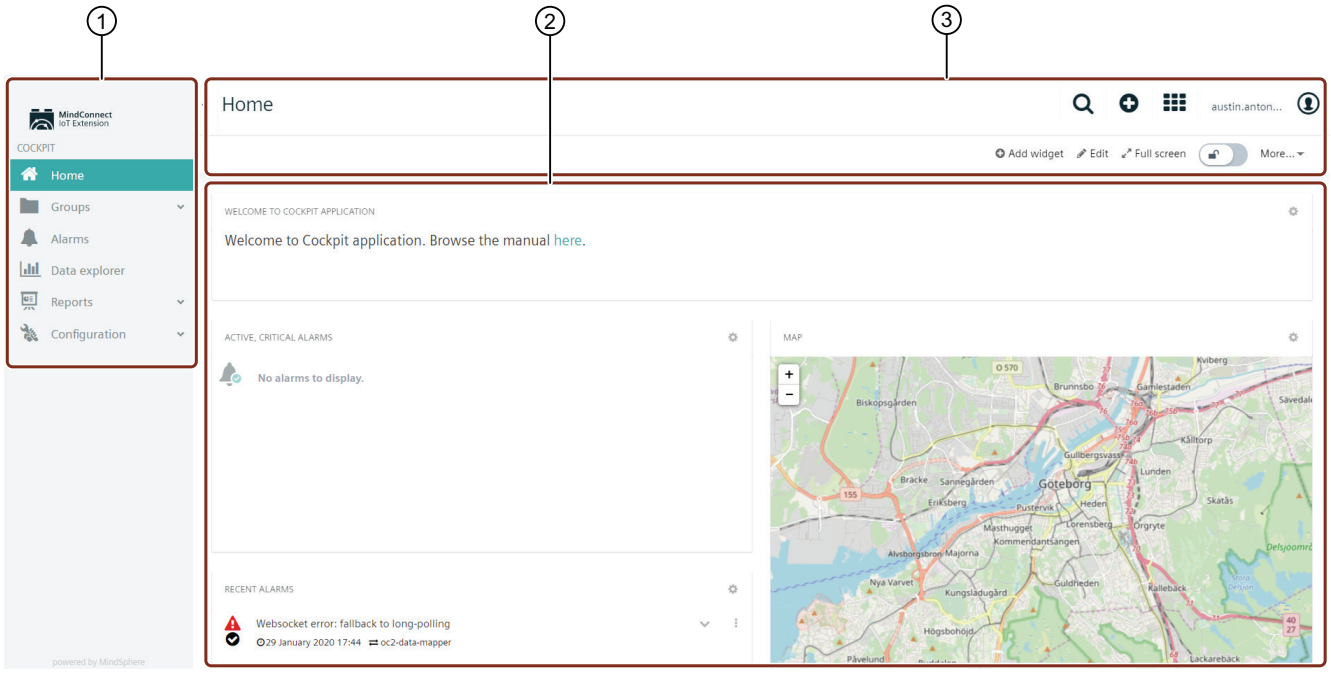
The "Home" dashboard can be edited and designed individually according to your needs. You can add, remove or change widgets being displayed here.

For details on editing a dashboard, refer to "Working with dashboards".

To reset the "Home" dashboard to its original content, click "More..." at the right of the top menu bar and from the context menu select "Restore dashboard".

6.2 User Interface "Cockpit"

Cockpit UI screen



① Tool navigation window

② Work area. The ② section provides quick links for documentation information, similar to References for user documentation.

③ Menu options

Symbols

The following table shows the buttons of the start screen:

Symbol	Description
	Search bar
	Add a new group by selecting devices from the displayed device list.
	Menu to select: • Administration • Cockpit • Device management

Symbol	Description
A. Antony 	Current user logged in
«	Left navigation tool screen is hidden to provides you with more work-space.
»	Navigates you to device management.

6.3 Managing assets

Introduction

Assets represent business objects in general like buildings, machines, production units or cars.

Assets are organized in hierarchies.

The asset hierarchy is composed of two types of objects:

- "Groups": Objects which group single devices or other groups. Groups can either be created in the Cockpit" application or in the Device Management application.
- "Devices": Devices which are linked into the asset hierarchy. Before you can use devices in the Cockpit application, they need to be connected to IoT Extension. This is done in the Device Management application. For details on connecting devices refer to Device Management (Page 49).

As an example, the group objects can represent a building asset. The device objects represent the room asset. The group names and hierarchy can be defined individually by the user. The hierarchy can have multiple levels, like region level, city level, street level, building level, floor level and room level. Any device can be part of multiple and different hierarchies, like part of regional hierarchy and part of customer hierarchy.

To position a device in the asset hierarchy, you have to "assign" the device to the respective group. See description below for details.

Note

Single devices are not managed in the Cockpit application. They are managed in the Device Management application.

Asset hierarchy versus device hierarchy

IoT Extension supports two types of hierarchies: a device hierarchy and an asset hierarchy.

The device hierarchy tracks how devices are linked to IoT Extension from a communications point of view. The asset hierarchy structures the assets that are being remotely supervised and controlled through the M2M devices.

In the Cockpit application, you construct your asset hierarchy by creating group objects and by linking devices into the hierarchy. The asset hierarchy depends on the IoT devices used. There are many types of IoT devices, but these two types are very common:

- Smart devices are self-contained devices that include sensors, actuators and a communication module. They are typically connected to a single asset. Smart devices are trackers, weather stations or general "smart" sensors with a built-in communication module.
- Gateway devices establish the communication from other devices to IoT Extension but do not include sensors or actuators. Typical gateway devices include Zigbee, Modbus, M-Bus or KNX gateways.

The following section explains how to work with smart devices and gateway devices in the Cockpit application.

Smart devices are represented in the Device Management application as top-level devices. In the Cockpit application, you can organize smart devices into groups, as the arrows indicate in the above diagram.

In the Device Management application, gateway devices are represented as top level devices. Their attached devices (like Zigbee, Modbus or KNX devices) are shown as child devices. These child devices can be organized in the asset hierarchy in the Cockpit application as shown above.

Devices can have completely different hierarchies in the Device Management application and in the Cockpit application: While inside Device Management all child devices are below the gateway device, the same child devices are organized in two different buildings in the Cockpit.

Cockpit assets versus business assets

The mapping of objects in the Cockpit asset hierarchy is a virtual hierarchy.

If you manage trucks within the IoT Extension platform, then each truck is represented via its individual tracking device communicating with IoT Extension.

For building management, it is most common that a group of sensors inside a building represents the building as a group communicating with the IoT Extension platform.

Navigating assets

In the asset hierarchy, IoT Extension distinguishes between top-level groups and subgroups, so called sub-assets.

In the navigator, top-level groups are shown in the Group menu at top-level. Sub-assets are shown in the navigator under the top-level groups or in the Sub-asset tab of a particular group.

When selecting an object in the asset hierarchy, details on the selected object are displayed at the right.

If you add a gateway device, the child devices are not shown. To show child devices, you must add them to the related asset. Details related to the child hierarchy are visible and editable in the Device Management application.

To navigate further in the asset hierarchy, use the navigator or select an object in the Sub-Asset tab. To navigate up in the asset hierarchy, use the breadcrumb entry below the name of the asset.

Asset details

Several tabs are available for each object, dependent of the object type:

Tab	Description	Availability
Info	Shows a list of Smart Rules created for the object.	Group, Device
Alarms	Displays alarms for the device. For details on alarms, refer to "Working with alarms in Device Management".	Device
Sub-assets	Shows the sub-assets of a group.	Group
Data explorer	Shows all data points of the children. For details refer to Visualizing data using the Data Explorer (Page 162).	Group, Device
Location	Shows the current location of a device.	Device

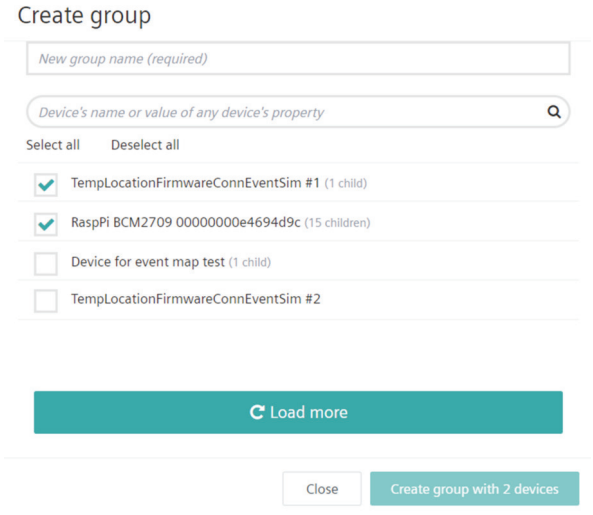
If dashboards have been created for an object, they will also be added as a tab. See Working with Dashboards (Page 169) for details.

Moreover, additional tabs may be displayed here in case the application has been extended with plugins.

Adding groups

To create a new group, follow these steps:

1. Click the "Plus" button at the right of the top bar, then select "Add group" from the menu.



2. In the window that comes up enter a unique group name to identify your group.
3. In the "Device Search" field, enter the search criteria for the devices you might want to add to your group (e.g. "ublox"). A list of devices that match your search criteria will be displayed.
4. Checkmark the devices you want to add from the list.
5. Click "Create group with X device(s)" to finally create your new group.

Note

A group can be created with "0" devices in it.

To add a new group as a child of an existing asset, navigate to its Sub-asset tab and click "Add Group" in the top menu bar.

Assigning devices to groups

Before adding a device to the asset hierarchy, it must be connected to IoT Extension. Connecting devices to the platform is done in the Device Management application. For details on connecting devices refer to Device Management.

To assign a device to a group, follow these steps:

1. In the navigator, select a group from the "Group" menu and then open the "Sub-assets" tab. In the "Sub-assets" tab, all devices that are assigned to the respective group are displayed.
2. Click "Assign devices" at the right of the top menu bar. In the upcoming window search for the devices you might want to add to your group (e.g. "ublox"). A list of devices that match your search criteria will be displayed.
3. Checkmark the devices you want to add from the list.
4. Click "Assign X device(s)" to assign the selected devices.

The devices will be shown as sub-assets in the "Sub-assets" tab.

Editing groups

To edit the name of a group, navigate to its information tab and click "Edit" next to its name. Edit the name and optionally leave some notes to be displayed in the "Info" tab. Click "Save changes" to apply your settings.

Deleting groups

To delete a top-level group from the navigator, follow these steps:

1. Click "Groups" in the navigator.
2. Click the menu icon for the group you want to delete.
3. From the context menu, select "Delete".

To delete a group from the "Sub-assets" tab of another group, follow these steps:

1. Navigate to the "Sub-assets" tab.
2. Click the menu icon for the group you want to delete.
3. From the context menu, select "Delete".

Unassigning devices

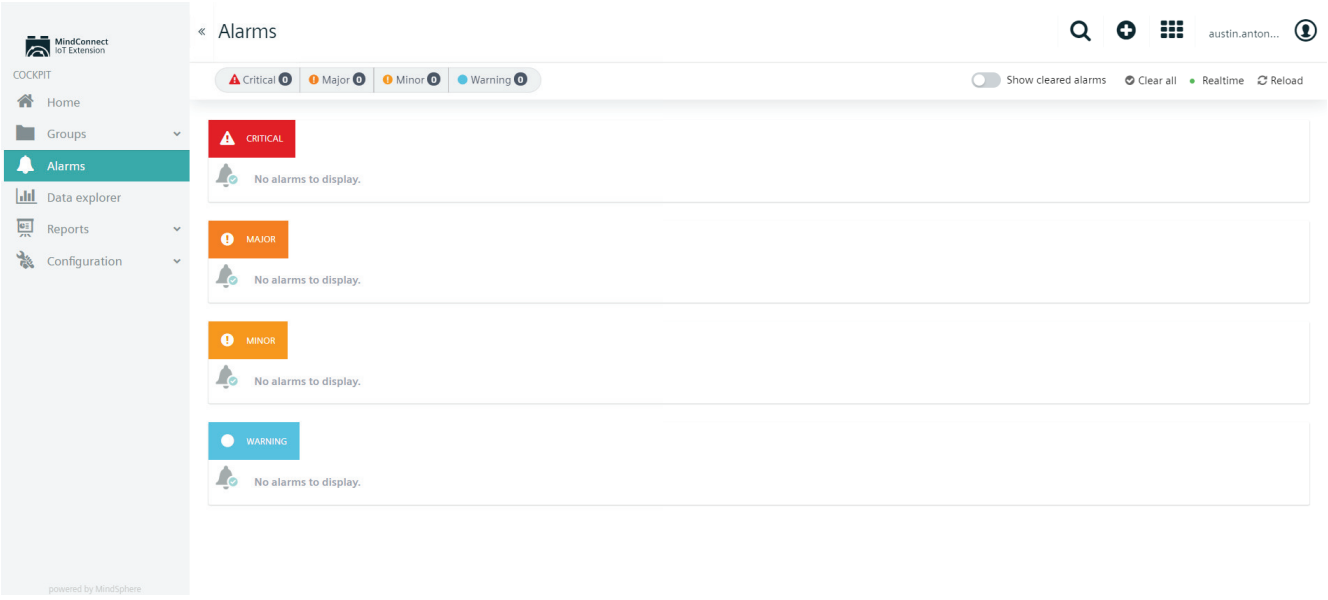
To unassign a device from a group, follow these steps:

1. Navigate to the "Sub-assets" tab of the group.
2. Click the menu icon for the device you want to unassign.
3. From the context menu, select "Unassign".

Unassigning a device does not remove the device, sub-devices or any associated data. The device is only removed from its location in the asset hierarchy. It can be assigned to this group or other groups later.

6.4 Alarms

Alarm UI screen



① Tool navigation window
② Work area
③ Menu options

6.5 Widgets collection

The "Cockpit" includes preset widget types. Each widget type provides different parameters to configure and different data to be displayed.

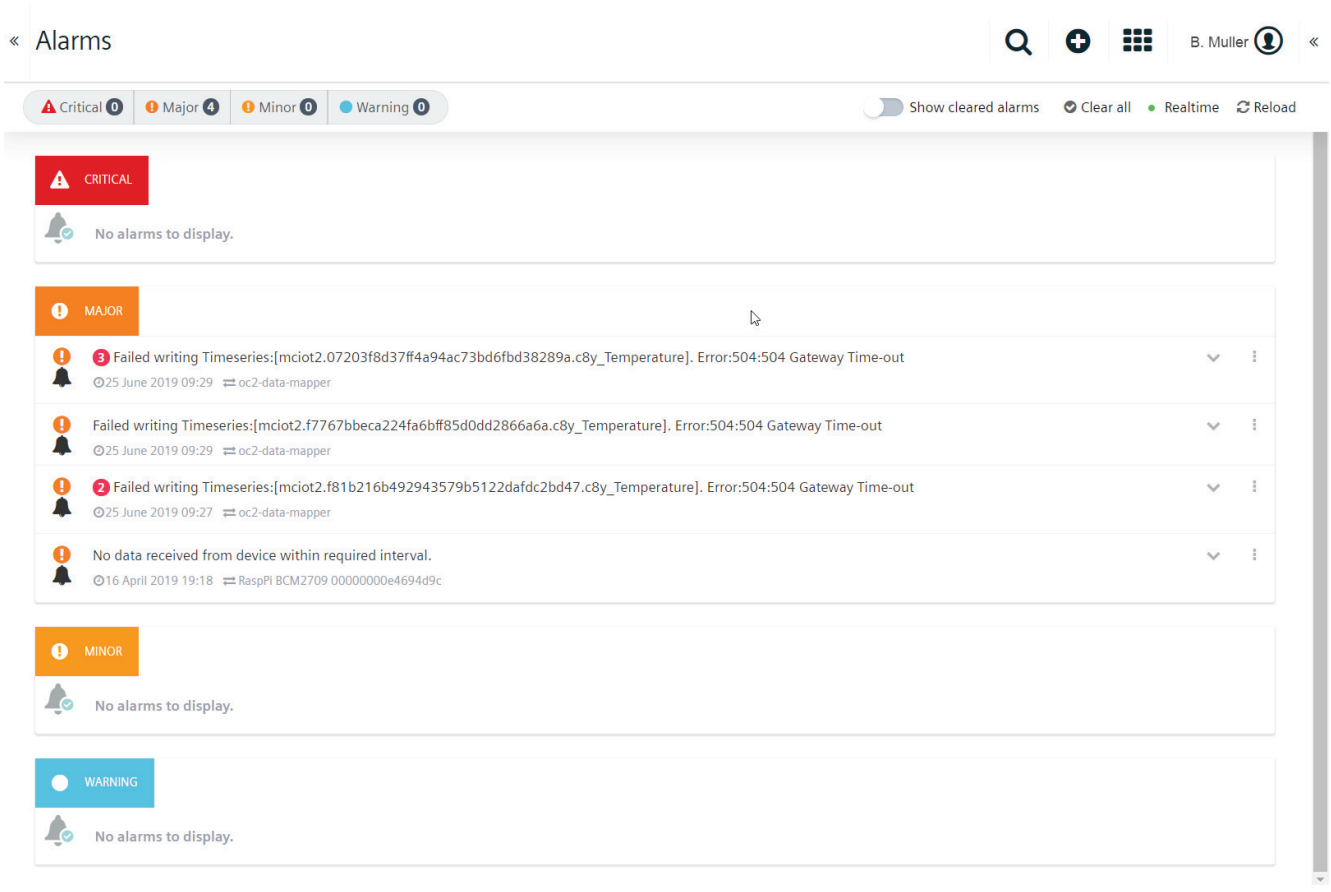
The following section describes, in alphabetical order, each available widget type and its configuration properties.

Widget "Alarm list"

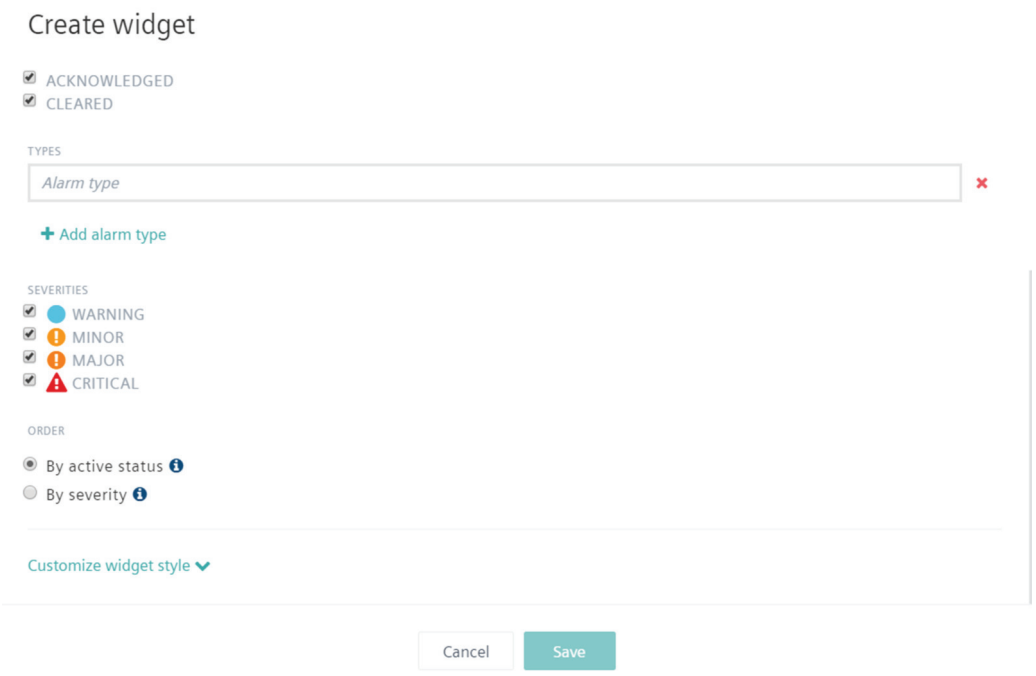
The "Alarm list" widget shows a list of alarms, filtered by objects, alarm severity and alarm status. For details on the information provided for each alarm, refer to Working with alarms (Page 75) in Device Management (Page 49).

Create a widget

To create a new widget, select "Add widget" from the "Home" tab.



Parameters to configure

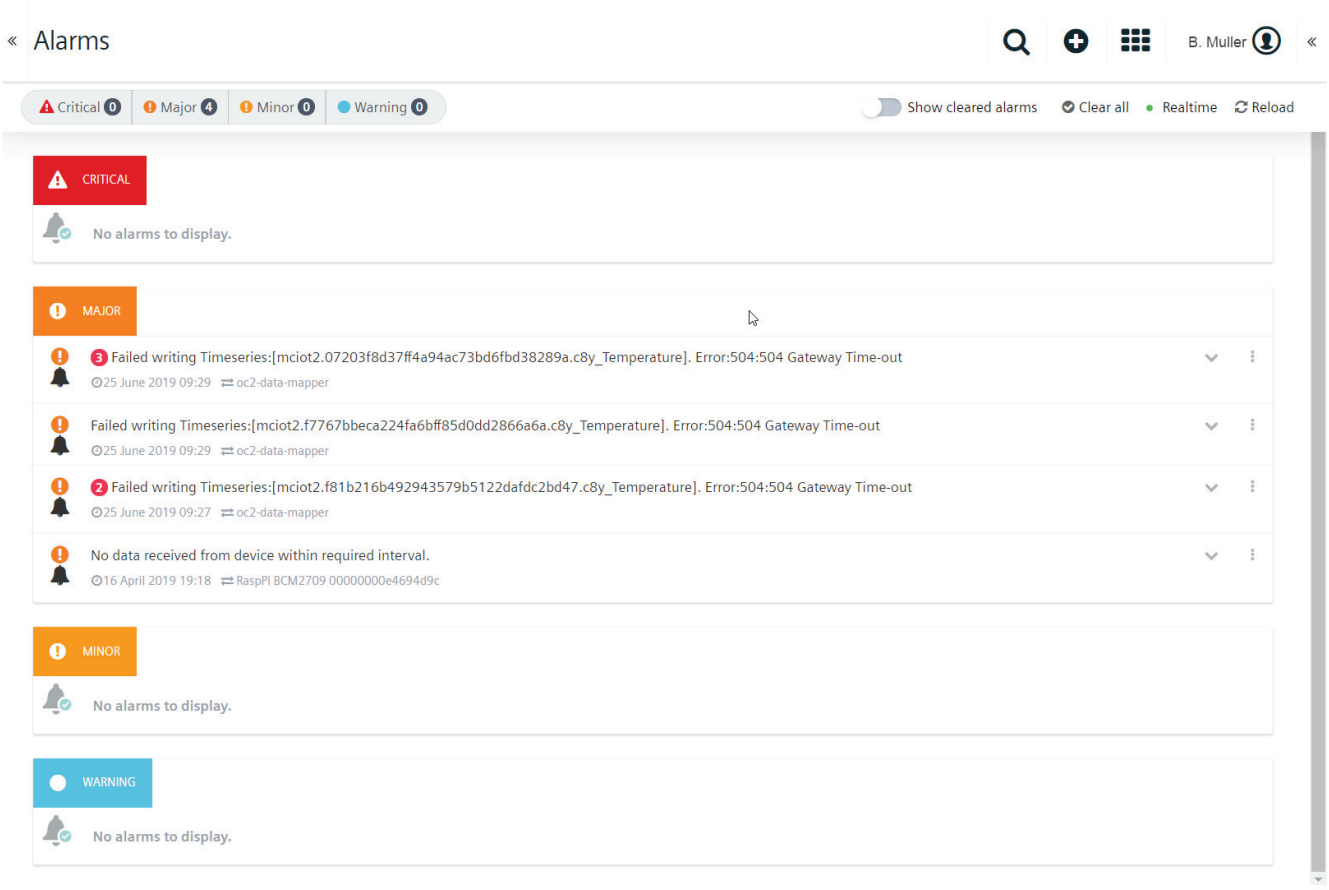


Field	Description
Title	By default, the widget type is simply used as title.
Target assets or devices	Select groups or devices, optional HTML expressions which should be evaluated.
Status	Only show devices with alarms of the selected alarm status.
Type	Only show alarms of the specified type(s). Details can be seen when clicking once on an alarm.
Severities	Only show alarms of the selected alarm severity.
Order	Alarms may be ordered by the active status (followed by severity and time, the default) or the severity (followed by time).

Widget "All critical alarms"

The "All critical alarms" widget shows all objects with a critical alarm. There are no additional parameters to be configured.

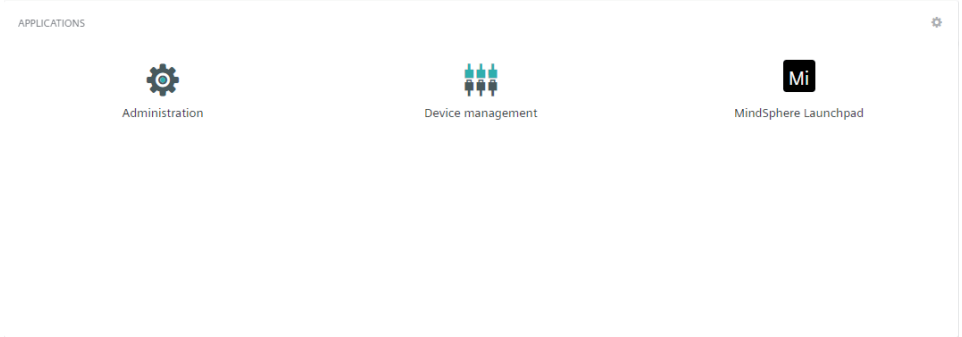
For details on alarms, refer to Device Management (Page 49).



Widget "Applications"

The "Applications" widget shows a list of links to all available applications. There are no additional parameters to be configured.

For details on applications, refer to Managing Applications (Page 31) in Administration (Page 13).



Widget "Asset notes"

The "Asset notes" widget displays messages provided by the administrative user to all owners of the current widget.

Only users with the permission to edit the home dashboard will be able to provide this message.

Widget "Asset properties"

The "Asset properties" widget displays a user-defined list of attributes of the current object. The current object can be a device or a group.

Parameters to configure

Field	Description
Title	By default, the widget type is simply used as title.
Target assets or devices	Select groups or devices.
Properties	List of properties, see Widget "Asset table".

Note

In the view mode, this widget only displays the properties which are not empty.

Widget "Asset table"

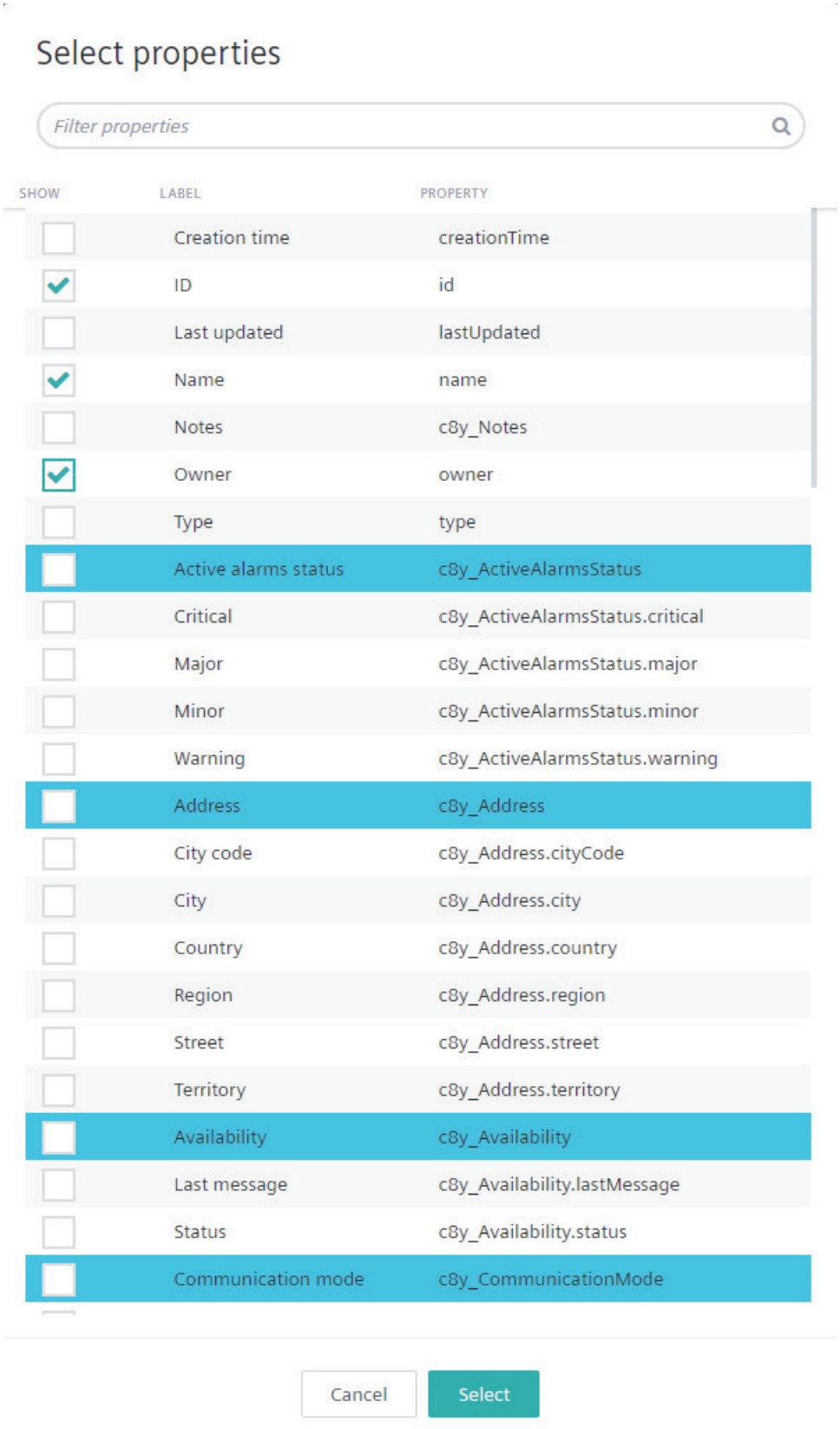
The "Asset table" widget shows details of all child devices in a table. This is a very powerful widget, allowing to arrange selected properties of objects in a table.

Parameters to configure

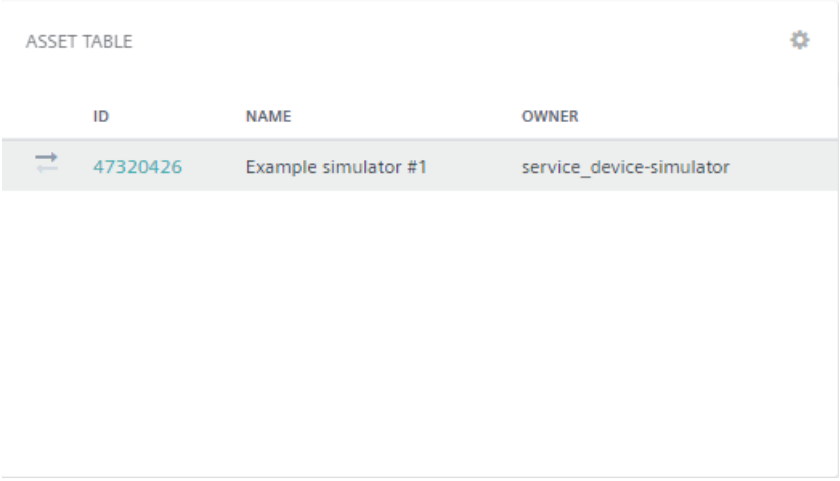
Field	Description
Title	By default, the widget type is simply used as title.
Target assets or devices	Select for which object all child devices should be shown. This is typically a group object.
Properties	Select properties or actions of an object to visualize them as columns in the table.

Example

In the following screenshot, three columns are configured:


Select properties
Filter properties
SHOW
LABEL
PROPERTY
Creation time
creationTime
ID
id
Last updated
lastUpdated
Name
name
Notes
c8y_Notes
Owner
owner
Type
type
Active alarms status
c8y_ActiveAlarmsStatus
Critical
c8y_ActiveAlarmsStatus.critical
Major
c8y_ActiveAlarmsStatus.major
Minor
c8y_ActiveAlarmsStatus.minor
Warning
c8y_ActiveAlarmsStatus.warning
Address
c8y_Address
City code
c8y_Address.cityCode
City
c8y_Address.city
Country
c8y_Address.country
Region
c8y_Address.region
Street
c8y_Address.street
Territory
c8y_Address.territory
Availability
c8y_Availability
Last message
c8y_Availability.lastMessage
Status
c8y_Availability.status
Communication mode
c8y_CommunicationMode
Cancel
Select

The resulting table is visualized as follows:



Adding properties

To add a property, click "+Add Properties" and select one or more properties to be added.

Note

The property "Active alarm status" shows active alarms as icons in the table. If you select this property, you also need to configure the renderer "Active Alarm Status" in the list of columns.

Adding actions

To add an action, click "+Add Action". Select Toggle maintenance mode to add the predefined action to toggle the maintenance mode. Or select "Create operation" to create a button that will execute a shell command. In the following dialog you can then enter the label for the button and the shell command to be executed.

Note

The dialog shows the predefined shell commands of the first device that supports shell commands. The list is empty if there is no such device.
You can also enter the JSON format for the operation that will be sent to the device. For details, contact the device vendor for supported operations.

Modifying the table

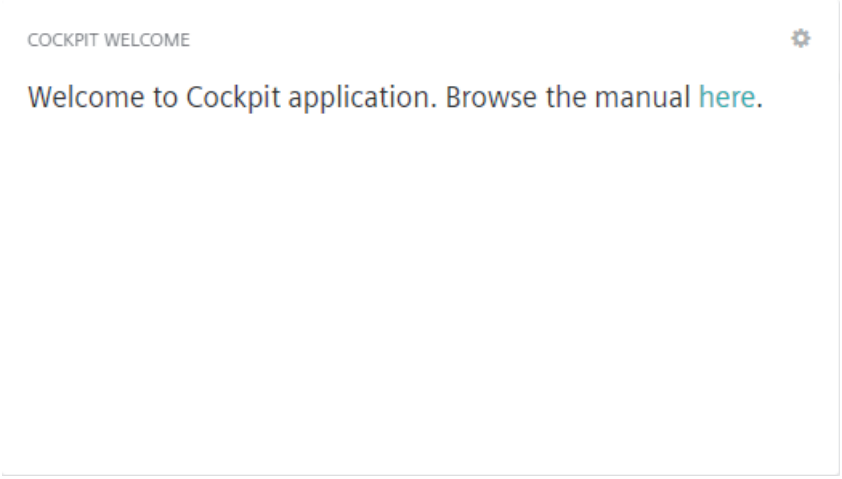
To edit the header of a column, click on its value in the "Label" column and edit the label.

You can rearrange the columns by clicking the icon at the very left of a row and dragging and dropping the entry.

To remove a property or an action, hover over the respective row and click "Delete" at the right.

Widget "Cockpit welcome"

The "Cockpit welcome" widget lets you display a welcome message to the "Welcome" screen. There are no additional parameters to be configured.



Widget "Data point graph"

The "Data point graph" widget shows a data point (measurement) in a graph. The visualization is the same as in the data explorer.

The easiest way to create a "Data point graph" widget is to navigate to the data explorer, click the "More..." button in the top menu bar and select "Send as widget to dashboard".

Refer to Visualizing data using the data explorer (Page 162) for further details on the parameters to be configured.

Widget "Data point list"

The "Data point list" widget shows data points (measurements), one in each row, with current values and data point properties.

Parameters to configure

Field	Description
Title	Widget title. By default, the widget type is simply used as title.
Data point	Shows a list of available data points. You must enable at least one data point. Click "Add data point" to add a data point to the list.
Column visibility	Select which columns should be visible: Label: Label of the data point. See Visualizing data using the data explorer (Page 162) for details. Target: Target value. Can be configured in the data explorer or Data Point Library. Current: Current value. Diff: Absolute difference between current value and target value. Diff %: Percentage of difference between current value and target value. Asset: Name of the device or group of the data point.

Widget "Data point table"

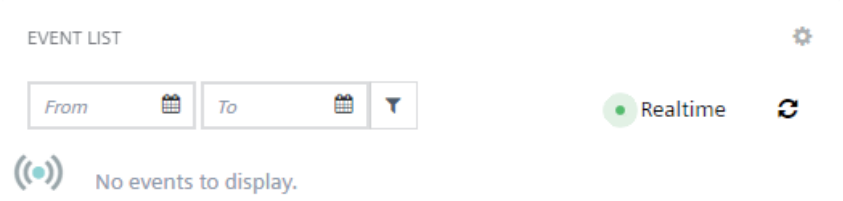
The "Data point table" widget configuration is similar to the "Data point graph" widget, but instead of visualizing the data as a line-chart, data is visualized as a table.

The "Data point table" widget displays data based on selected data points, time interval and aggregation.

Out of range values, based on configured yellow and red ranges, are highlighted in the table.

Widget "Event list"

The "Event list" widget lets you monitor events for a selected device.



Additionally, a specific date range can be set and the events can be monitored in realtime.

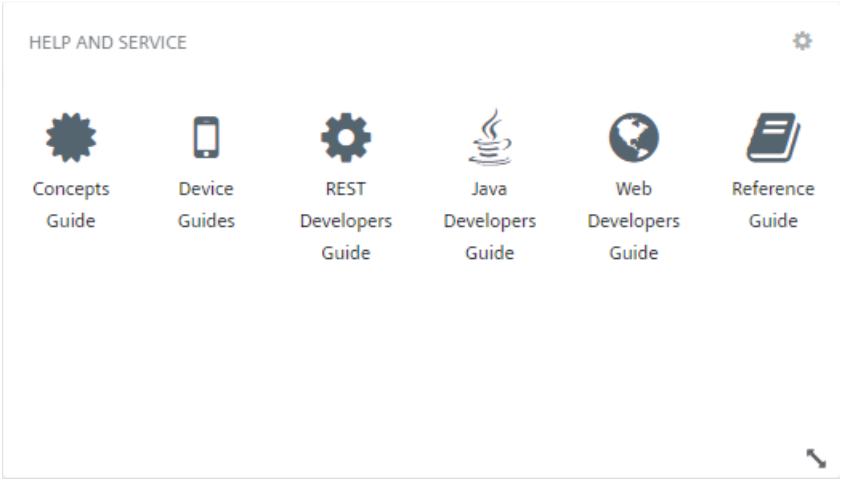
Widget "Fieldbus device"

The "Fieldbus device" widget lets you see the status of a modbus device and operate it.

For details on the "Fieldbus device" widget, refer to Cloud Fieldbus (Page 128) in Device Management (Page 49).

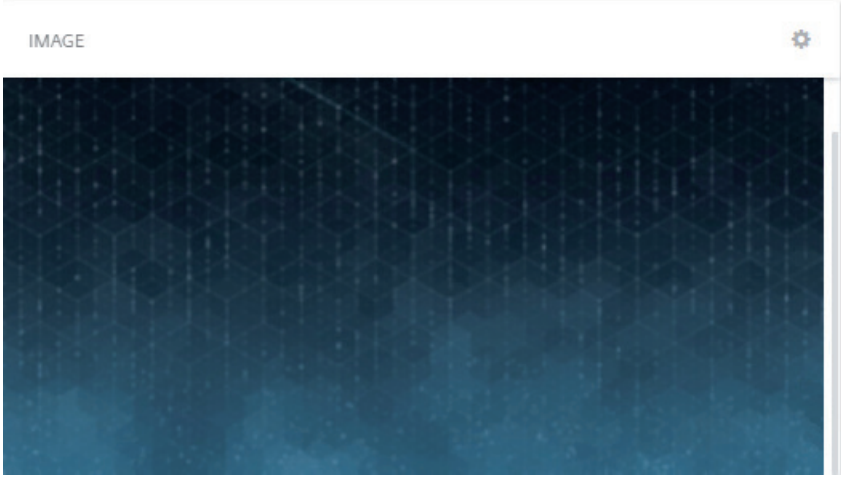
Widget "Help and service"

The "Help and service" widget displays links to help and service resources. There are no additional parameters to be configured.



Widget "Image"

The "Image" widget lets you display a single image to be selected from your computer by browsing. There are no additional parameters to be configured.



Widget "Info Gauge"

The "Info gauge" widget visualizes one data point in form of a radial gauge and multiple data points as labels.

You can select one data point for the gauge, and multiple data points shown with labels on the left side.

You must enable at least one data point in each section to create the "Info gauge" widget.

Widget "HTML"

The "HTML" widget shows user-defined content. The content can be formatted using HTML.

Parameters to configure

- Target assets or devices: Select the objects for which optional HTML expressions are evaluated.
- HTML code

The following variables can be used inside the HTML content:

- {{devicesCount}}: Total number of devices.
- {{usersCount}}: Total number of users.
- {{deviceGroupsCount}}: Total number of groups.
- {{device.name}}: The name of the device.
- {{device.property}}: More general form of the above. You can address any property of the device.
- {{device.c8y_Hardware.model}}: The model of the device.
- {{device.fragment.property}}: More general form of the above. You can address any property of any fragment of the device.

Note

"Device" refers to the target device, as selected in the widget configuration parameter. fragment.property refers to the properties of the respective device. To see the available property names, you can use the "Asset property" or “Asset table” widget and click "+Add property" in the widget configuration. This will show a table of supported properties. You can copy and paste the values from the column “Property”. Generated properties of these widgets are not available in the HTML widgets.

Widget "Linear Gauge"

The "Linear gauge" widget visualizes data points in form of a linear gauge. Min and max target values are shown on the gauge as well.

Note

If a label is not properly readable, you can help yourself by increasing the min and max value of the data point to move the label into the readable range.

You must enable at least one data point to create the "Linear gauge" widget.

Widget "Map"

The "Map" widget shows the location of a device or all devices of a group.

You can drag the map and move its content, and you can zoom in and out by using the "Plus and Minus" buttons.

The icons representing the devices are color-coded. The color used follows these rules:

- Red = At least one critical alarm
- Orange = At least one major alarm
- Yellow = At least one minor alarm
- Blue = At least one warning
- Green = No alarm

Click a device icon, to open popup with the following information:

- The device name. When clicked, the application navigates to the device.
- The date at which the device last reported its location, if available.
- A slider to show/hide the device tracks for the previous and current days.

Parameters to configure

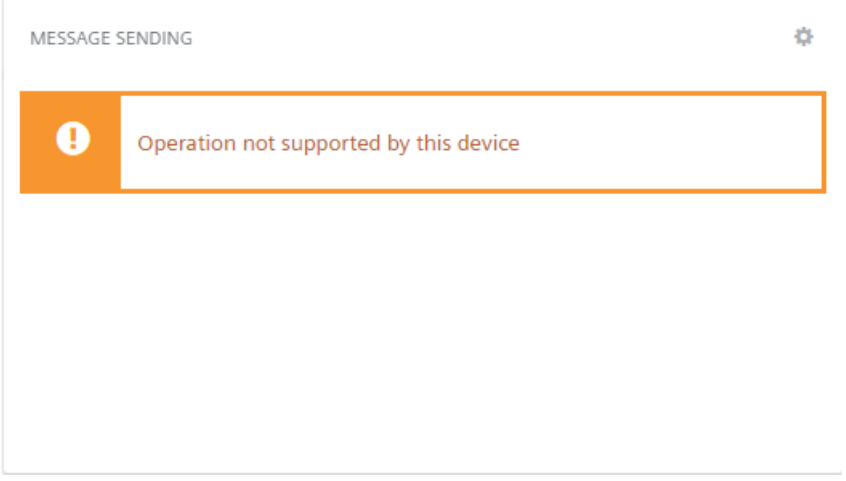
Target assets or devices: Select which devices are shown on the map. If a group is selected, all devices in that group (but not in any subgroups) are visible.

Note

If none of the target device(s) has a known location, then the widget shows a world map without icons.

Widget "Message sending"

The "Message sending" widget sends a message to a device. The behavior of the device itself is device-dependent. Only available for devices that support this type of operation.



Widget "Pie chart"

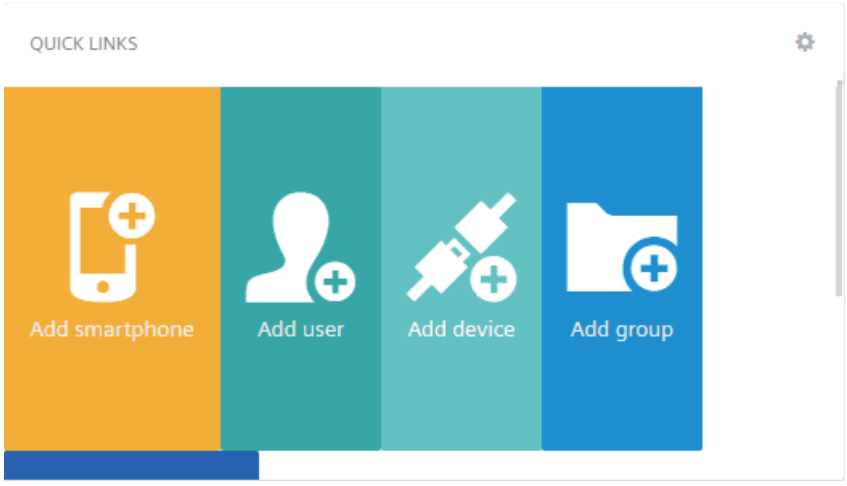
The "Pie chart" widget displays data points (measurements) with current values in a pie chart presentation.

Parameters to configure

Field	Description
Title	Widget title. By default, the widget type is simply used as title.
Pie chart options	Select from the options to show tooltips, percentages, legends in the pie chart.
Data point	Shows a list of available data points. You must enable at least one data point. Click "Add data point" to add a data point to the list.

Widget "Quick links"

The "Quick links" widget displays several quick links to relevant operations. There are no additional parameters to be configured.



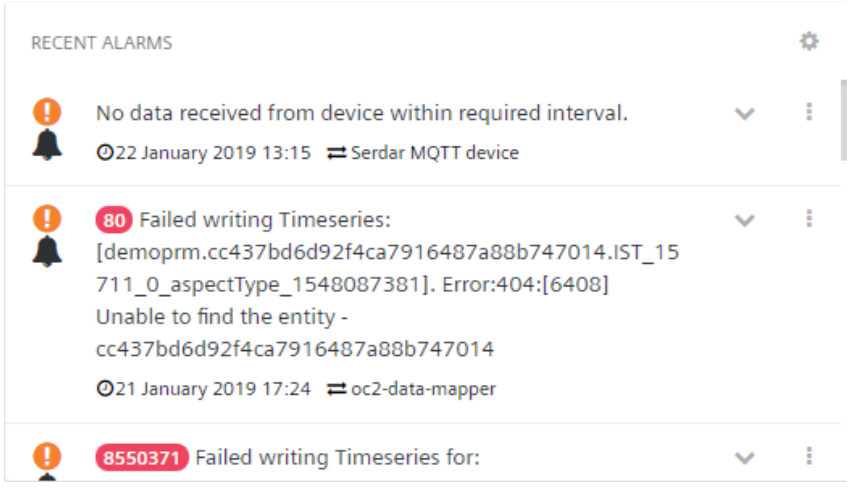
Widget "Radial Gauge"

The "Radial gauge" widget visualizes data points in form of a radial gauge.

You must enable at least one data point to create the "Radial gauge" widget.

Widget "Recent alarms"

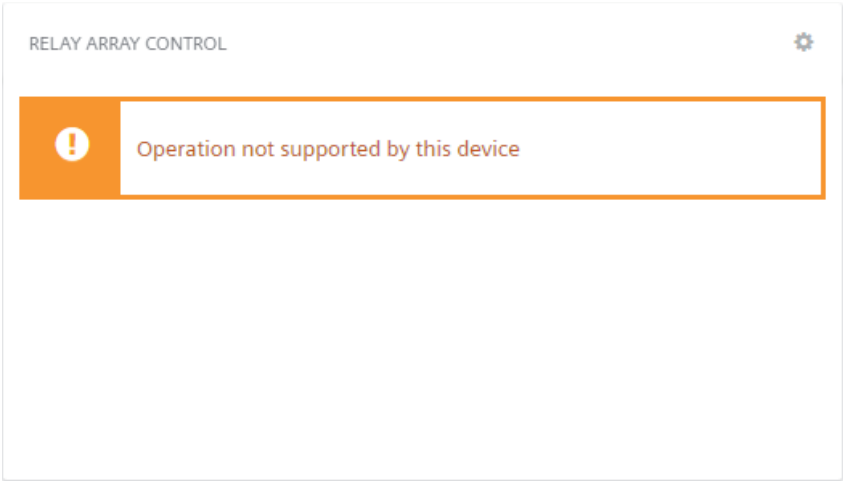
The "Recent alarms" widget shows all alarms of all severity sorted by time. There are no additional parameters to be configured.



For details on alarms, refer to Device Management (Page 75).

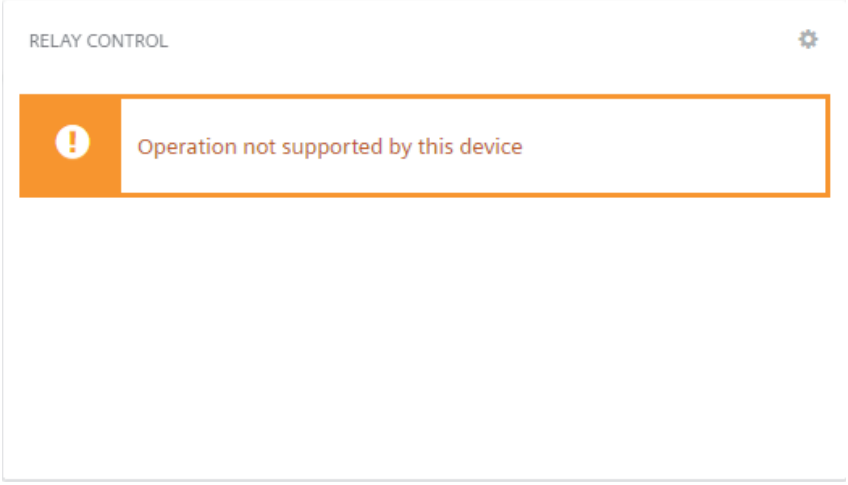
Widget "Relay array control"

The "Relay array control" widget lets you switch relays on or off independently in an array of relays. Only available for devices that support this type of operation.



Widget "Relay control"

The "Relay control" widget allows you to switch a device relay on or off. Only available for devices that support this type of operation.



Widget "Rotation"

The "Rotation" widget lets you render an object model of a device.

Parameters to configure

Field	Description
Title	By default, the widget type is simply used as title.
Target assets or devices	Select group or device to be displayed.
Object model for rendering	Select an object model type for rendering. May be one of "Box model" or "Phone model".
Wireframe	Turn "Wireframe" on or off (default = on). The "wireframe" mode displays the object in a skeletal representation.
Camera type	Select the type of camera to be used. May be one of "Orthographic camera" or "Perspective camera".

In the "Rotation" widget you can rotate the object by dragging and moving it around. Zoom in and out by using the mouse.

Widget "SCADA"

The "SCADA" widget provides a graphic representation of the status of a device.

For details on the "SCADA" widget, refer to "Optional Services" > "Cloud Fieldbus" > "Monitoring status using the SCADA widget".

Widget "Silo"

The "Silo" widget displays data points (measurements) with current values in a silo presentation.

Parameters to configure

Field	Description
Title	Widget title. By default, the widget type is simply used as title
Data point	Shows a list of available data points. You must enable at least one data point. Click "Add data point" to add a data point to the list.

Widget "Traffic light"

The "Traffic light" widget visualizes the states of a device as traffic light.

Parameters to configure

Field	Description
Title	Widget title. By default, the widget type is simply used as title.
Target assets or devices	Select group or device to be displayed.
States mapping	Select a property for each light. The value of the property has to be one of the following to have the respective light on: true, 1, any non-empty string, any non-null number.

Widget "Twitter News"

The "Twitter news" widget displays tweets from Twitter's embedded timeline widget.

Parameters to configure

Field	Description
Title	By default, the widget type is simply used as title.
Twitters's username	User name for the Twitter account being displayed.
Twitter's widget ID	ID for the Twitter widget. You can obtain the ID from widgets settings.
Options	Select if you want to display a header, footer, borders or transparency.

6.6 Data explorer

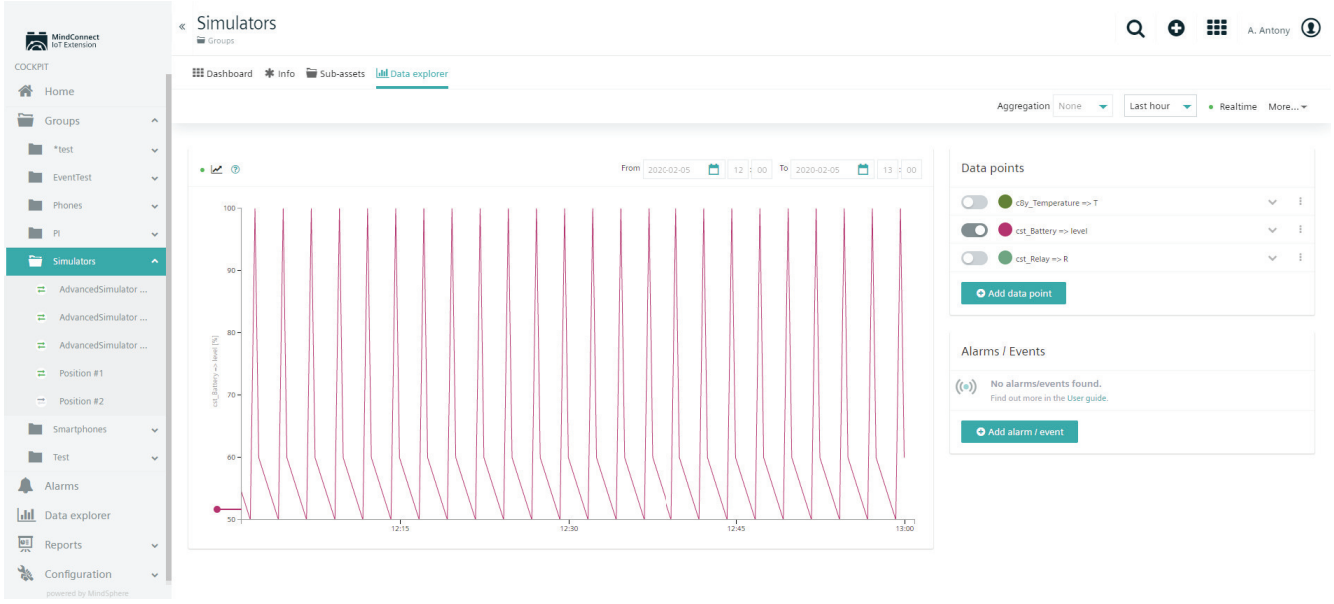
In the data explorer, data points, i.e. measurements or sensor data, can be visualized.

The data explorer is available for all assets or just for a particular asset.

- Click "Data explorer" in the navigator to visualize all data points of all assets.
- Navigate to a particular asset and switch to the Data explorer tab to visualize all data points of this particular asset and its sub-assets.

In the data explorer, you see a list of available data points on the right. The first five data points of the selected device or group are shown by default.

On the left, in the main card, you see its visualization.

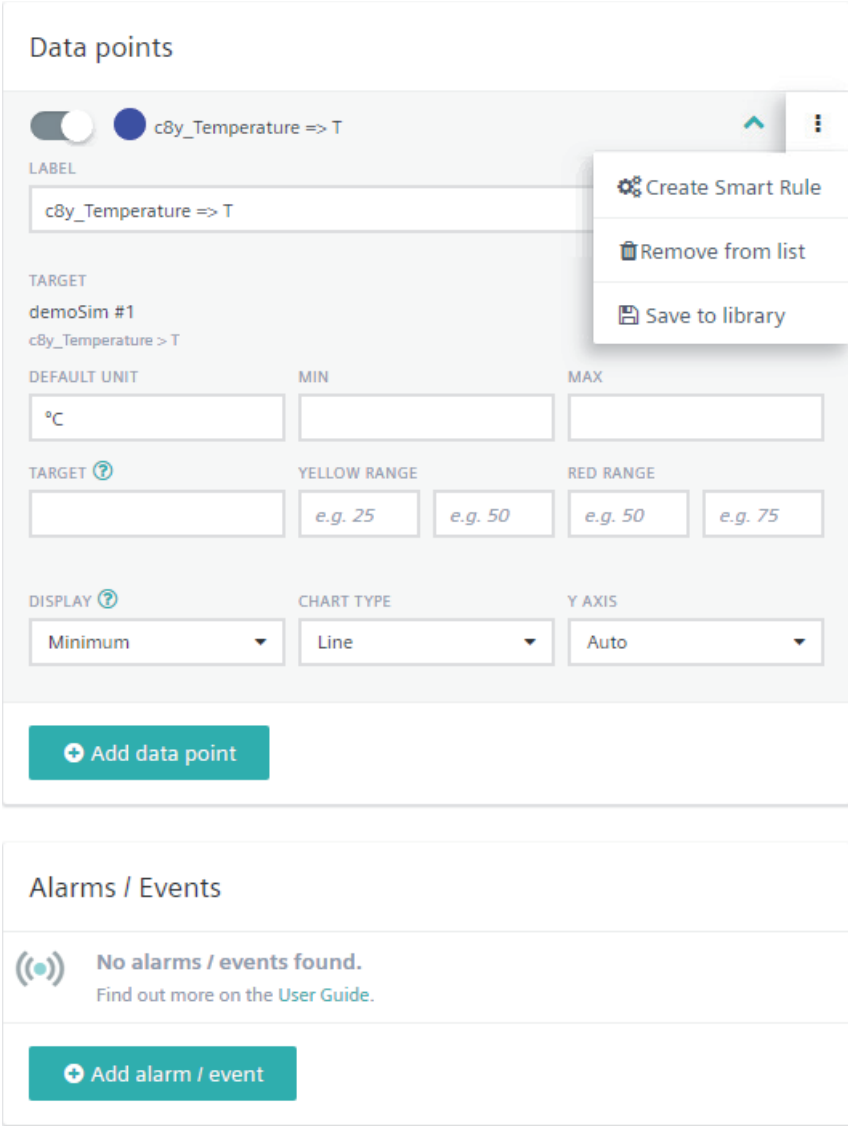


The visualization is generated based on data point properties.

The data points properties are pre-filled as follows:

- If these properties have been customized previously, these values are used, see "Customizing data point properties".
- If the data points have a matching definition in the "Data Point Library", the values from the "Data Point Library" are used.

There can be more than one matching data point entry in the "Data Point Library". In this case, the first one is selected automatically by the system. You can overwrite this selection by clicking the menu icon of the respective data point and selecting Load [NAME] from Library.



Note

Data points are visible to all authenticated users of the tenant, regardless of their inventory role permission.

Changing data explorer visualization

To change the visualization in the data explorer, you can modify several properties.

Time range

You can change the time range being shown. By default, you see the values for the last hour.

To change the time range on the X-axis,

- select a different time range from the dropdown list in the top menu bar,
- enter a custom time range into the "From" and "To" fields in the data explorer,
- drag the X-axis and move of left or right to move the time period,
- double-click into the data explorer to zoom out.

Note

Real-time updates will be switched off if you set a time range in the past.

Aggregation

You may aggregate the data being displayed to get an efficient overview over larger time periods.

By default, aggregation is set to "None". This value may be changed in the "Aggregation" field in the top menu bar. Available values are "Minutely", "Hourly" or "Daily", depending on the selected time range.

Realtime updating

By default, realtime updating is enabled which means that the data being shown is updated as new data flows into the system from the connected devices.

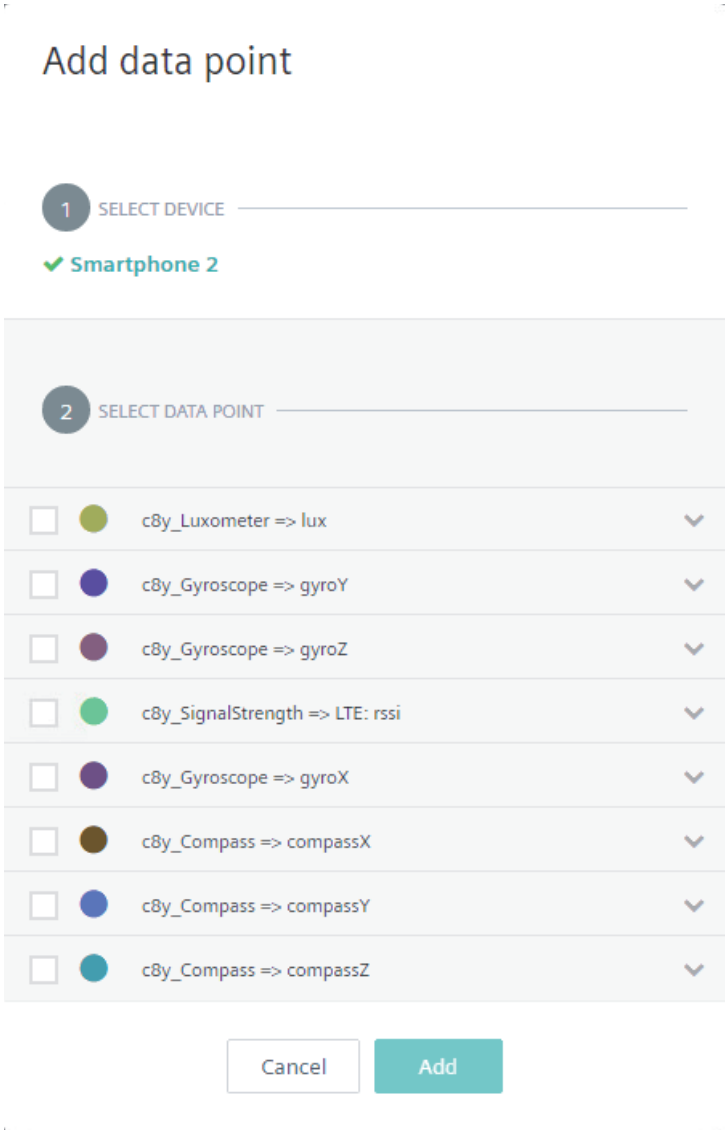
To turn realtime updating on or off, click "Realtime" in the top menu bar. A green light indicates, that realtime updating is enabled.

Data point visibility

For each datapoint, its visibility can be switched on or off by using the slider left from the data point name.

Adding data points

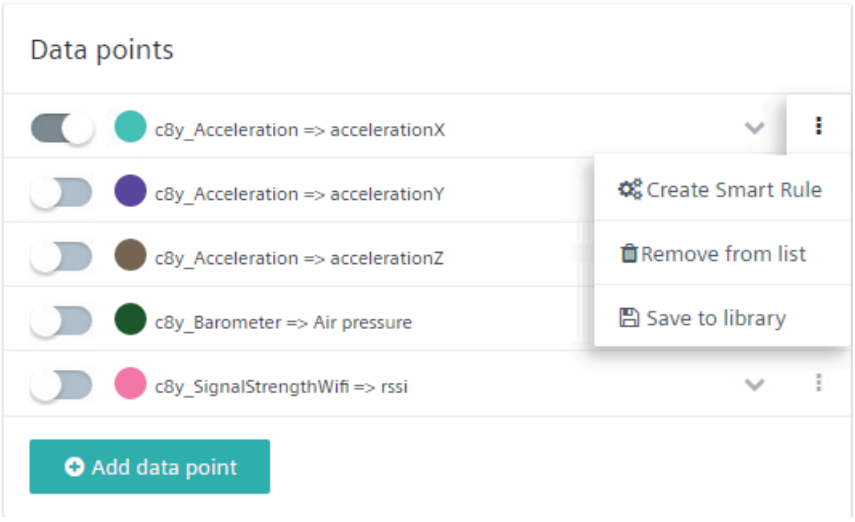
To add a data point to the data explorer, click "Add data point" at the bottom of the Data points card.



In the top of the dialog, select a device from the asset hierarchy. Only the asset hierarchy below the objects selected in the navigator is visible. If "Data explorer" in the navigator was selected, the complete asset hierarchy is visible.

The bottom of the dialog shows all data points of the selected object. Select the data points you want to show in the data explorer. Click "Add" to add all selected data points to the list of data points.

To save the data point to the Data Point Library, click the menu icon of the data point and from the context menu select "Save" to library.



For details on the "Data Point Library" refer to "Using the Datapoint Library".

To remove a data point from the data point list, click the menu icon and select "Remove" from list.

Customizing data point properties

You can customize the visualization of a particular data point to your preferences. To do so, expand the data point entry in the data point list.

The following fields my be modified:

Field	Description
Label	Name of the data point, displayed on the y-axis to identify the data point. Below the label, the target is displayed, showing the name of the asset and the internal name of the data point (measurement fragment and series). This information is not editable.
Unit	Unit used on the y-axis.
Min/Max	Range shown on the y-axis.
Target	The target value is currently not shown in the diagram. The value is used in the "Data Point List" widget.
Yellow range min/max	Defines the range when MINOR alarms should be raised by threshold rule.
Red range min/max	Defines the range when CRITICAL alarms should be raised by threshold rule.
Display	Value displayed when data is aggregated. May be "Minimum", Maximum", Minimum and maximum".
Chart type	The type of chart used for the visualization. May be one of "Line", "Points", "Line and points", "Bars", "Step before" (alternating between vertical and horizontal segments, as in a step function) or "Step after" (alternating between horizontal and vertical segments). Default value is "line".
Y axis	Defines where the y-axis is shown. May be one of "Auto", "Left", "Right". Default value is "Auto".

After customizing the properties of a data point, you can save the modified settings to the Data Point Library. Click the menu icon and from the context menu select "Update [NAME] to library".

To return to the properties stored in the Data Point Library to a data point, select "Load [NAME]" from library.

Y-axis behavior

Per default, the first data point is positioned to the left y-axis and the remaining data points to the right. This behavior can be changed by modifying the respective value "Y-axis" for a particular data point (to "Left" or "Right", see above).

Each data point is shown on its own y-axis, unless the following condition is met:

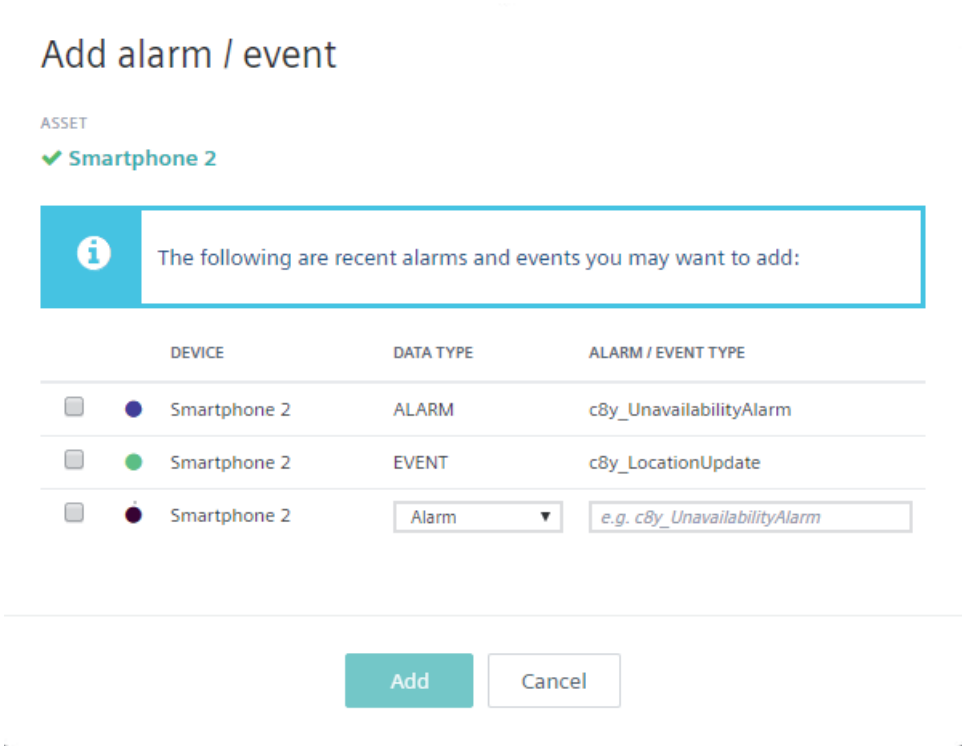
- Two data points having the same minimum and the same maximum value.

In this case, both data points share the same y-axis. This y-axis only shows the unit (or multiple units, in case they are different). The label is not shown.

Adding alarms or events

In addition to data points you can also add alarms or events to the data explorer.

In the "Alarms/ Events" card, click "Add alarm/ event" to add an alarm or event.



In the upcoming dialog, you can select an alarm or event from the list of recent alarms and events. Click "Add" to add your selection.

Expand an event to modify its properties.

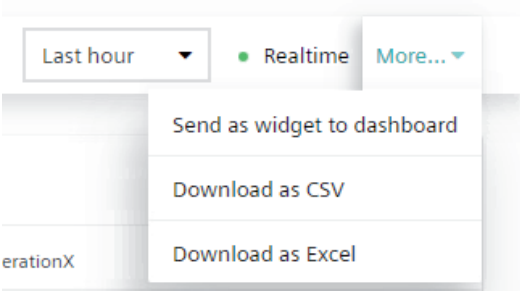
Click the menu icon and in the context menu select "Remove", to remove the entry from the list.

As with data points, you can turn the visibility of an alarm/ event in the data explorer on and off by moving the slider.

Creating widgets from the data explorer

If you want to keep your current configuration in the data explorer for later usage, save it as a widget.

To create a widget from the data explorer of a particular asset, click "More..." in the top menu bar and select "Send as a widget to dashboard" from the context menu.



In the upcoming dialog, select one of the dashboards available for the current object and click "Select" to add the data explorer as widget to the selected dashboard.

Note

To use this function, first a dashboard has to be created. For details on dashboards, refer to "Working with Dashboards".

Send as widget to report

To create a widget from the data explorer of in the navigator, click "More..." in the top menu bar and select "Send as a widget" to report from the context menu.

In the upcoming dialog, select one of the reports available and click "Select to add the data explorer as widget to the selected report".

Note

To use this function, first a report has to be created. For details on reports, refer to Working with Dashboard reports (Page 174).

Exporting measurement data

You may download measurement data as CSV or Excel files. The exported data shows the following information, divided into columns:

- Time when the specific measurement was taken
- Source of the measurement
- Name of the device being used
- Fragment series (e.g. c8y_SpeedMeasurement)
- Value of the measurement
- Unit used for a particular measurement (e.g. "C", "km/h", "sec")

To export measurement data, click the "More..." button in the top menu bar and select either "Download as CSV" or "Download as Excel", according to your preferences.

The download will be generated, as shown in the upcoming dialog. This make take a while, depending on the number of data points added to the data explorer. Once the loading has been completed, click "Download".

6.7 Dashboards

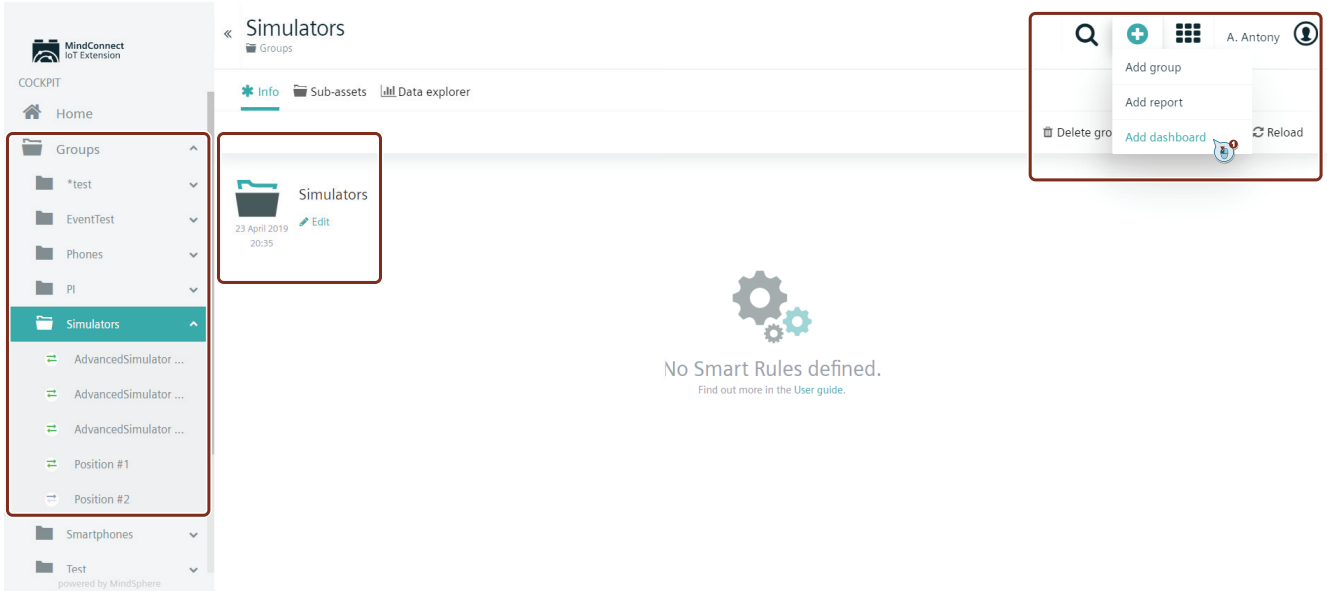
"Dashboards" provide you with a customized visualization of your data by using a set of widgets. Widgets can display maps, images, graphs, tables and other graphic representations of data.

IoT Extension comes with a number of preset widgets, see Widgets Collection (Page 146) for details. You can also develop your own widgets and add them to your IoT Extension account.

Creating a dashboard

Select the "Group" option from the left navigator and choose a displayed group from the display area.

Click the "Plus" button in the top bar and from the context menu select "New dashboard".



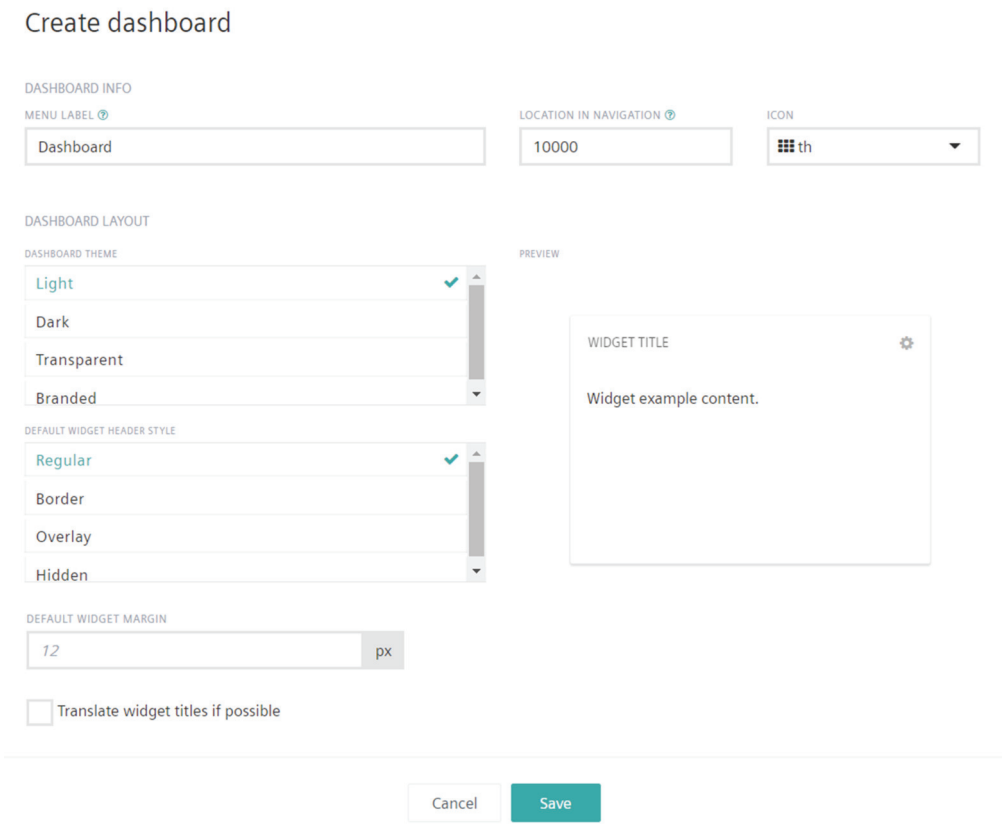
In the "Dashboard" info section of the dashboard editor, provide the following information:

- A menu label to be used as the name of the dashboard
- The location of the dashboard in the navigator, with "10000" being ordered first and "-10000" last
- An icon which is shown next to the dashboard name in the navigator

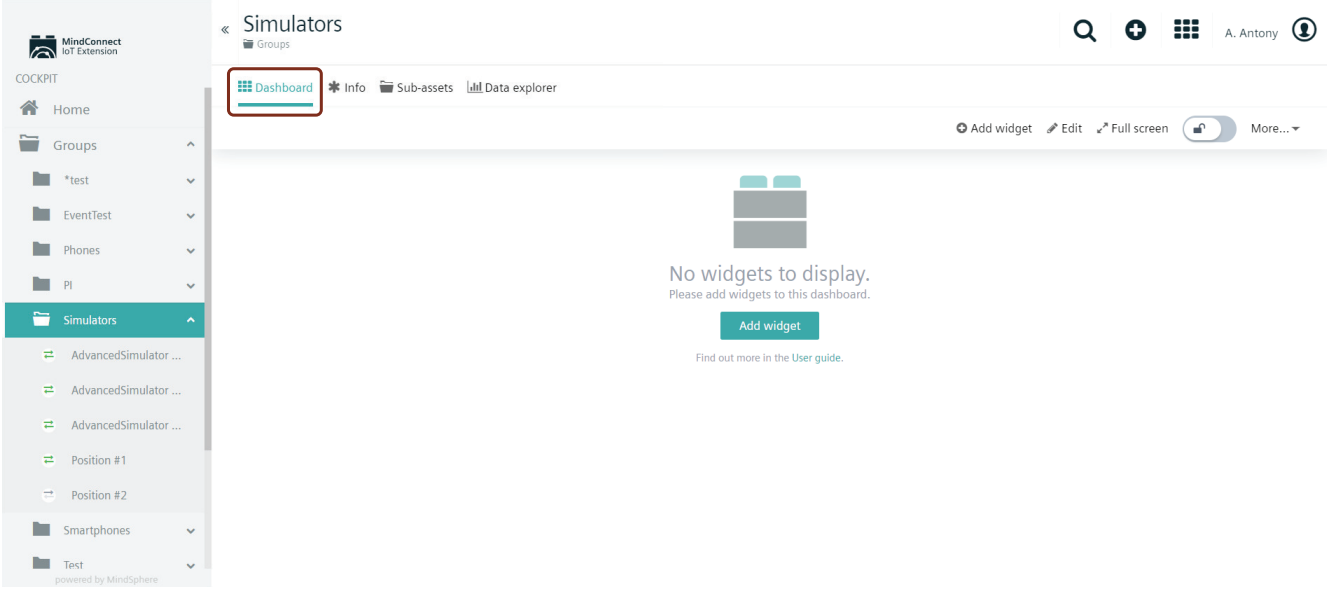
In the "Dashboard" layout section you can select a theme for the dashboard (one of "Light", "Dark", "Transparent" or "Branded") and a default header style for the widgets (one of "Regular", "Border", "Overlay", or "Hidden"). Moreover, you can change the default widget margin (default value is 15 px).

A preview of the selected layout settings is immediately displayed in the "Preview" section at the right to visualize your selections.

Click "Save" to create and open the dashboard.

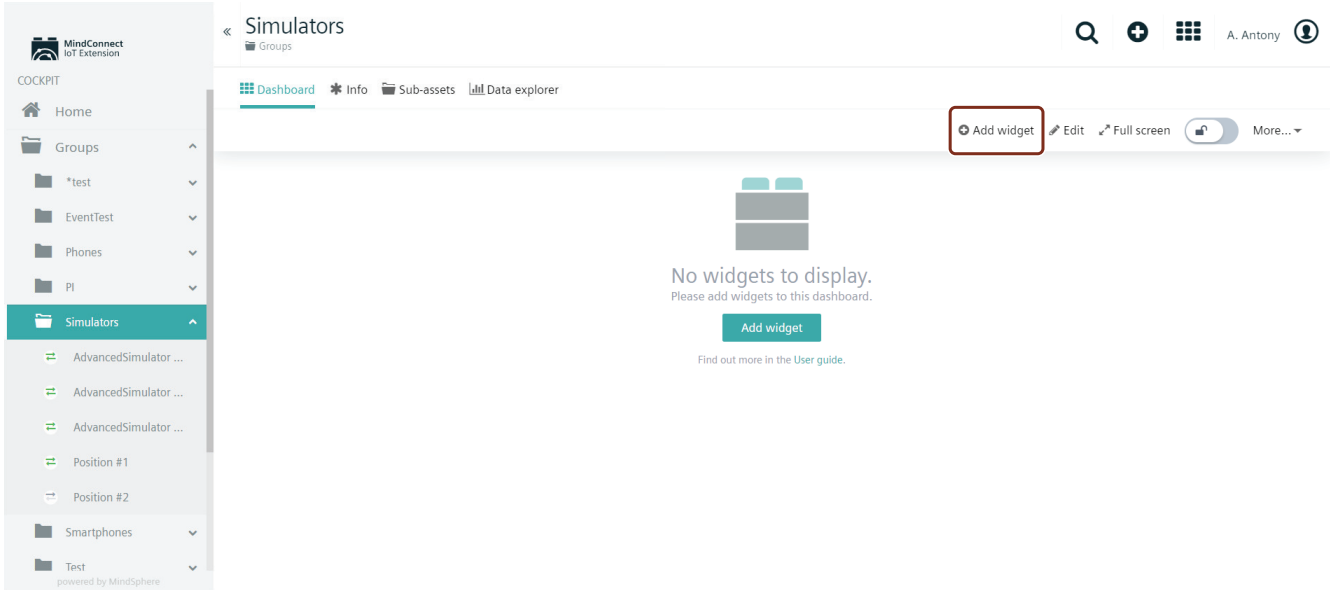


Once you add a dashboard, you will be able to view the "Dashboard" option in the working UI.

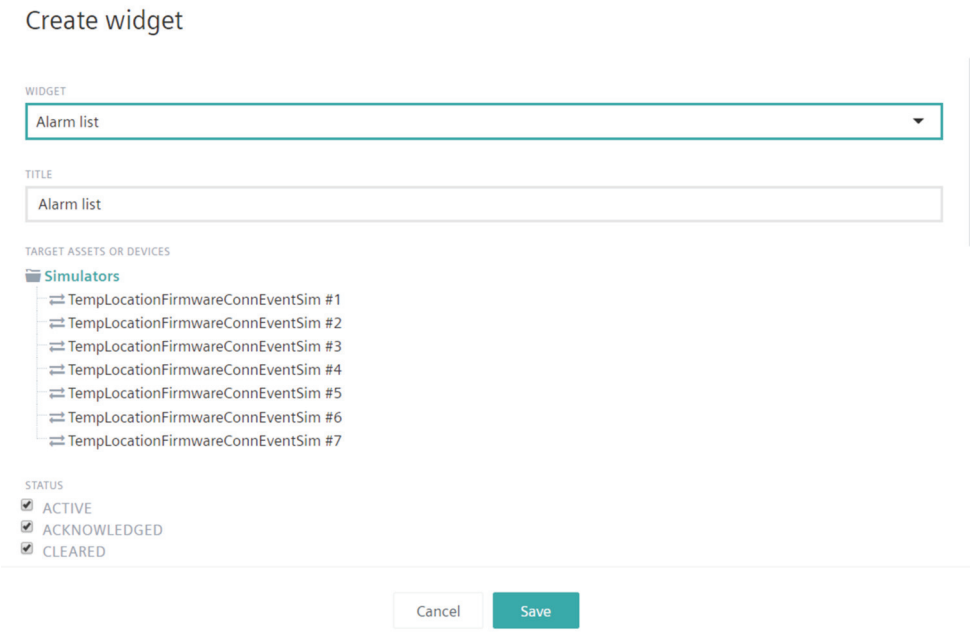


Adding a widget to a dashboard

If there will be no widgets on the dashboard, you will see an "Add Widget" button instead.



To add a widget to a dashboard, click "Add widget" in the top menu bar.



In the upcoming dialog, select a widget type from the dropdown list. Depending on the widget type selected, additional fields and checkboxes will be displayed to be filled in or selected. For details on all widgets refer to Widgets Collection (Page 146).

Click "Customize widget style" to customize the content and header style for the widget individually, similar to specifying the general layout in the dashboard editor.

Click "Save" to add the widget to the dashboard.

Modifying widgets on a dashboard

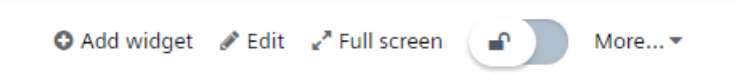
Widgets may be rearranged on the dashboard. By dragging and dropping you can move the widget to another position.

By dragging the arrows on the bottom right corner of a widget, you can resize it.

To edit the properties of a widget on a dashboard, click the cogwheel icon at the top right corner of the widget and from the context menu select "Edit".

To delete a widget from a dashboard, click the cogwheel icon at the top right corner of the widget and from the context menu select "Remove".

Widgets can only be modified, if the dashboard is unlocked. To lock/unlock a dashboard, use the slider with the lock icon on the top menu bar.



Note

On touch devices like smartphones or tablets some functions may not be supported.

Sharing dashboards

You can create one dashboard and share it with all devices of a specific type. To do so, select the option "Apply dashboard to all devices of type [TYPE]" ([TYPE] is replaced with the type of the device that is currently selected).

Changes made to this dashboard are automatically applied to all dashboard instances.

Note

You can only add widgets and data to the dashboard for the device itself. It is not possible to add data from child devices because the structure of these devices might be different from device to device.

Editing dashboard properties

To edit a dashboard, click "Edit" in the top menu bar. The dashboard editor will open up.

Copying dashboards

To copy a dashboard from one object to another, click "More..." in the top menu bar and from the context menu select "Copy dashboard".

Next, navigate to the object you want to copy the dashboard to and from the context menu select "Paste dashboard [NAME]" to insert the dashboard.

An alternative way to copy a dashboard is to use the "dashboard per type" approach. With the "dashboard per type" approach you share the dashboard from one object with all objects of the same type.

Removing dashboards

To delete a dashboard from an object, click "More..." in the top menu bar and from the context menu select "Remove dashboard".

6.8 Managing reports and exports

Managing reports

Dashboard reports enable you to track applications, alarms, assets, events and many other widgets.

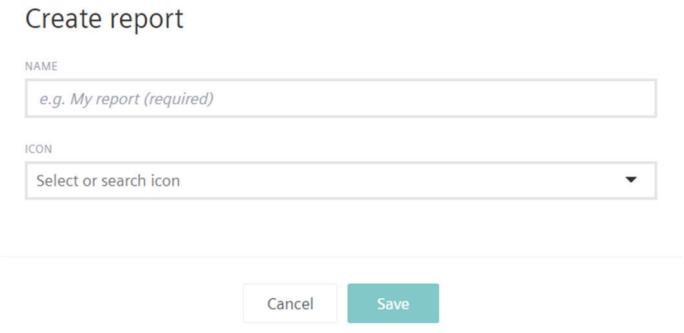
Dashboard reports are global dashboard pages, regardless of the asset hierarchy.

To see all existing reports, expand the "Reports" menu in the navigator.

To view a specific report, click the report in the navigator to open it.

Creating new reports

To add a new report, click the "Plus" button in the top bar and from the context menu select "Create new report".



Enter a name for the report and optionally select an icon from the dropdown list. Click "Save" to save your settings.

Next, widgets can be added to the report.

Adding widgets to reports

You can add widgets to reports in the same way as adding widgets to dashboards.

Click "Add widget" in the top menu bar and select a widget type from the list. For details on all widgets types available, refer to Widgets collection (Page 146).

Deleting reports

To delete a report, open the report and click "More..." at the right of the top menu bar. From the context menu, select "Remove report".

Exporting data

The export functionality lets you export specific data to either CSV or Excel files.

With this feature, you can request data for the whole tenant. Additionally, you can choose to filter for specific devices, time ranges or fields. The export data contains information about all specified filters and enabled fields.

Note

The maximum number of documents that can be exported into a single file is 1 million. If the number of documents for defined filters exceeds this limit, only first 1 million documents will be taken.

To show all exports, click "Export" in the "Reports" menu.

In the "Export" page you will find a list displaying all exports with their names and time range.

Adding exports

To create an export, click "Add export" in the top menu bar.

Enter a name for the export and select the file type (CSV or xlsx).

Filters

In the Filter section, you can select filters to request object- or time-specific data.

To filter for a particular object, enter a name or property value into the search field and click the search icon. All matching devices or groups will be displayed below the Value field. Click a device to select it (highlighted in green).

The "Time range" filter can filter data for a specific time range. Select a time range from the dropdown field. This may be one of "Last year", "Last month", "Last week" or select "Custom" and enter a custom from/to range in the additional fields.

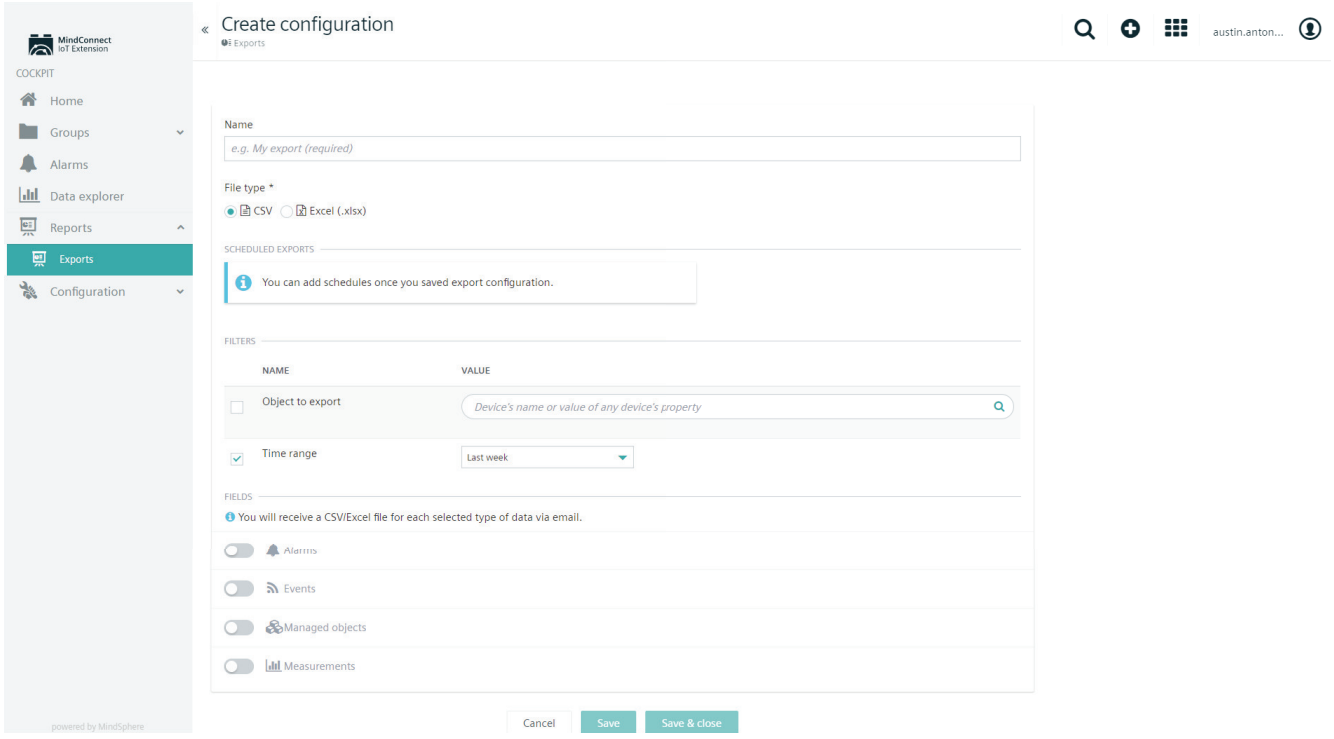
Select the checkbox in front of the filter name to enable the filter.

Fields

Apart from object- and time-specific filtering you may filter data for specific fields:

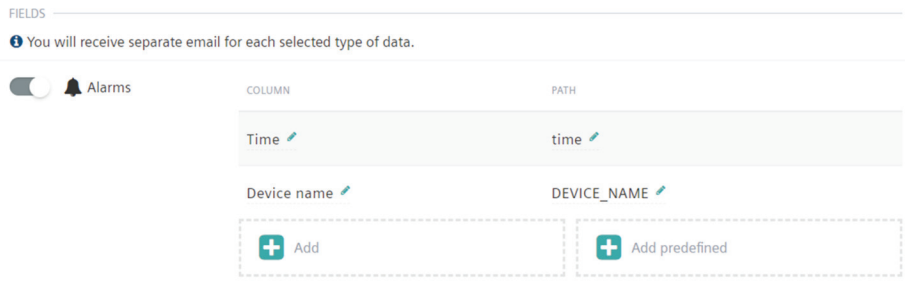
- "Alarms"
- "Events"
- "Managed objects"
- "Measurements"

Use the slider to enable/disable a field.



Note

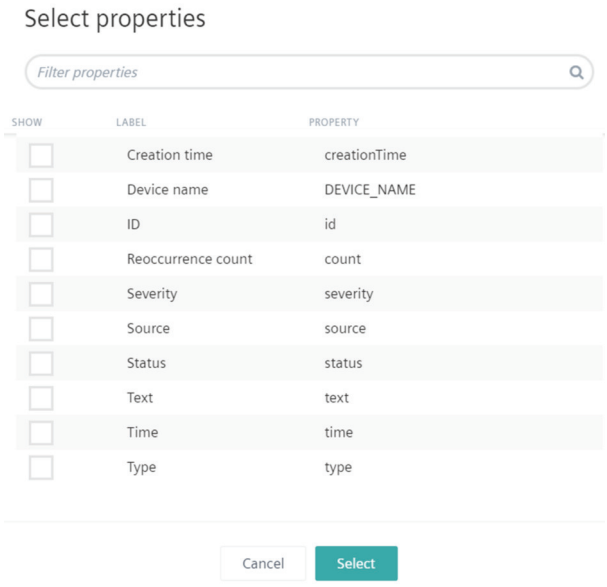
The time range filter only applies to alarms, events and measurements but not to managed objects. If selected, managed objects will appear in the export, regardless of any specified time range.



When a field is enabled, predefined or empty properties can be added.

Click "Add" to add empty properties. To enter a label or path, click "Column" or "Path" and edit the field. For example, if you enable the "Alarms" field you could enter "Severity" in column and path to receive data for alarm severities.

Click "Add predefined" to add predefined properties. Simply select the desired properties from the list and click "Select". Use the search field at the top to search for a specific property.



If you have at least one field that is not originating from the "Add predefined" list but defined as a custom property, then you need to set up at least one property for the custom values to appear in the export.

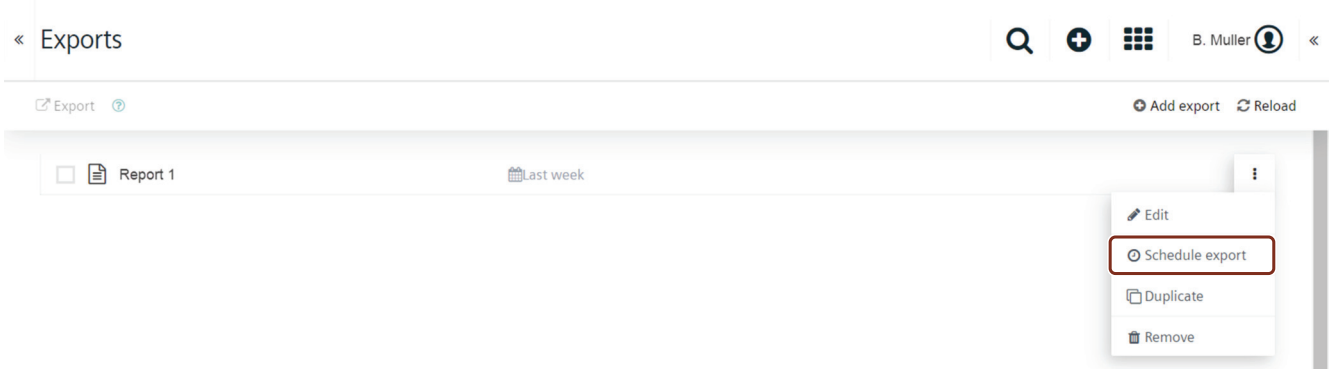
Example: An export has 4 fields defined: time range, device name, type and c8y_SpeedMeasurement.speed.value. The first 3 are predefined properties, while the last one is a custom property. If any measurement for export does not have a custom property c8y_SpeedMeasurement.speed.value, then it will not appear in the export file.

If your field is a valid.key.with.dot then refer to it as ['fragment.key.with.dot'] in the path, e.g.: ['fragment.key.with.dot'].series.value

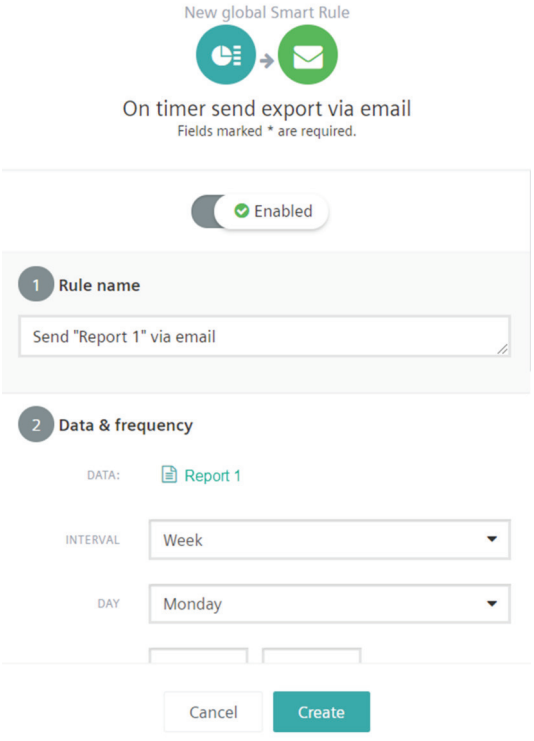
In case of "Measurements" enabled, you can also choose "Add from data point".

Scheduling exports

To schedule the export to a CSV or Excel file to any point in time, click the menu icon at the end of the row and from the context menu select "Schedule export".



In the upcoming window you can customize the Smart Rule "On timer send export via email" according to your needs.



1 - Rule name

The rule name is pre-filled, providing the name of the export, but may be modified.

2 - Data & frequency

Define the frequency for sending the export, i.e. every hour, day, week, month or year. Depending on the frequency selected, provide additional timing information. For example, if you have selected "every month", provide the day of month, hour and minute.

3 - Send email

Complete the email information.

In the "Send to" field, provide the email address of the receiver. This field is mandatory. Optionally, you can provide email addresses for sending CC or BCC and add the email address of the sender for reply.

Specify the subject of the email. This field is pre-filled, but may be modified.

Enter the actual email message. Available placeholders are {host}, {binaryId}. The default value is "File with exported data can be downloaded from {host}/inventory/binaries/{binaryId}".

Click "Create" to create the customized Smart Rule "On timer send export via email".

The Smart Rule will be added to the export details.

Exporting data

To export data to a CSV or xlsx file, select the checkbox in front of the export in the list and at the left of the top menu bar click "Export".

You will receive an e-mail containing links to each export file.

Standard time properties of documents (like time or creationTime in alarms) are exported to
•xlsx file in the format: 03/13/2016 00:00:24
•CSV file in the format: 2016-03-13T00:01:24.000Z

Only CSV time contains milliseconds and timezone.

Editing exports

To edit an export, just click the respective row or click the menu icon at the end of the row and from the context menu select "Edit".

Duplicating exports

To duplicate an export, click the menu icon at the end of the row and from the context menu select "Duplicate". Modify at least the name and click "Save & close" to save the export and return to the export list.

Removing exports

To remove an export, click the menu icon at the end of the row and from the context menu select "Remove".

6.9 Data Point Library

The Data Point Library provides a collection of data points with default values for data point properties.

Data point properties are similar to "paragraph formats" in word processing applications: You do not want to format each paragraph individually. Instead you want to define a set of default formats and apply them to your paragraphs in your document.

The Data Point Library provides the same functionality for data points: It provides a number of default data point templates that can be applied easily to your data points from different devices.

How does the Cockpit application use the data point library? To find the default visualization for a data point like color or label, Cockpit searches the data point library and tries to find a matching entry. An entry is considered as "matching", if the values for fragment and series in the data point library match those of the measurement. If a matching entry is found, the corresponding data point properties are used for a default visualization.

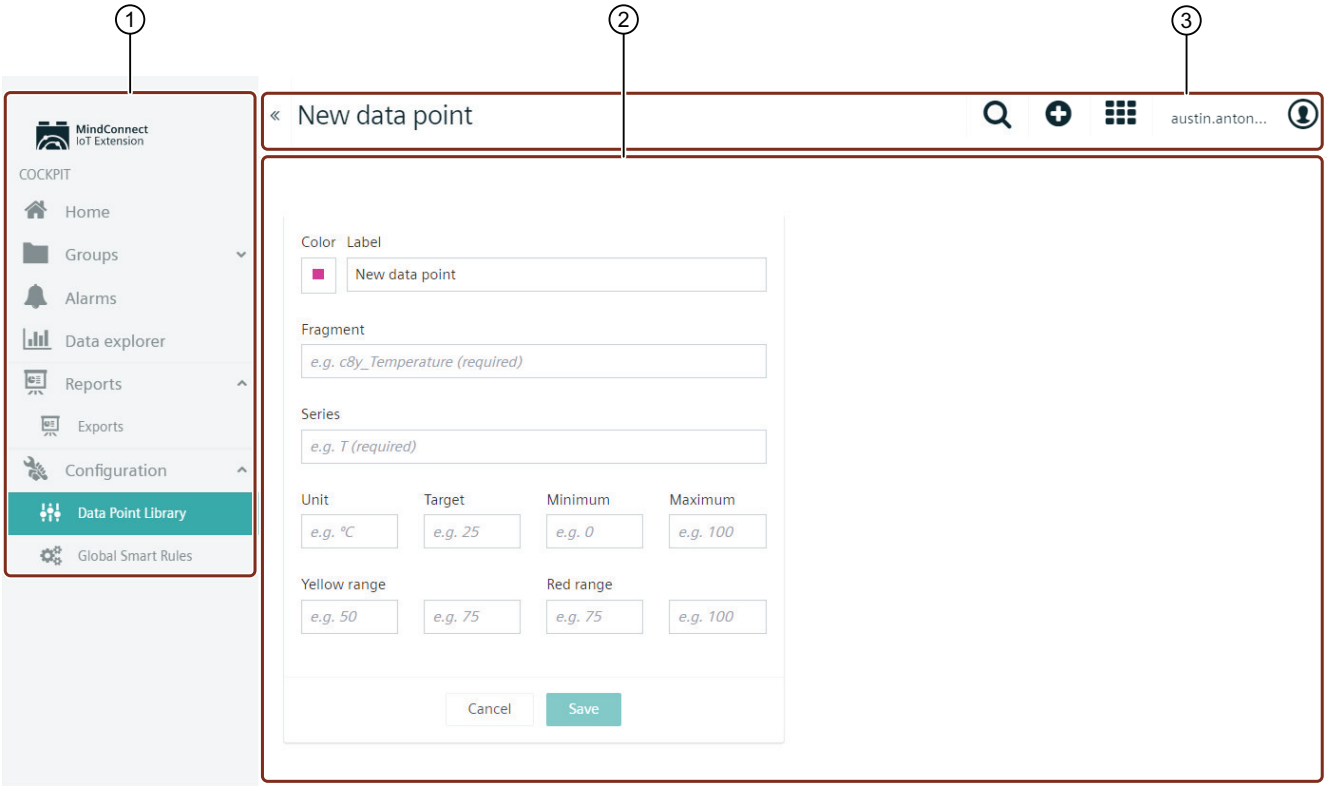
Additionally, the properties of the Data Point Library are used by threshold business rules: The red and yellow values configured in the Data Point Library are used by the threshold rules to raise alarms.

To open the Data Point Library, click "Data Point Library" in the Configuration menu of the navigator.

A list of available data points will be opened. For each data point, the following information is provided in the list:

- Color and label for the data point
- Fragment name and series
- Measurement unit

Data Point Library UI



① Tool navigation window
② Work area
③ Menu options

Adding a data point to the library

To add a new data point to the library, click "Add data point" in the top menu bar.

Provide the following information:

Field	Description
Color	Color for the data point visualization.
Label	Label to identify the data point.
Fragment	Name of the fragment.
Series	Name of the series.
Unit	Unit used for the measurement.
Target	Target value.
Minimum	Minimum value shown on the y-axis.
Maximum	Minimum value shown on the y-axis.

Field	Description
Yellow range	Minimum/maximum values for the yellow range (MINOR alarms).
Red range	Minimum/maximum values for the red range (CRITICAL alarms).

Click "Save" to add the data point to the library.

Editing or removing data points

To edit a data point, simply click the respective entry in the list or click the menu icon at the right of an entry and in the context menu click "Edit".

To remove a data point, click "Remove" in the context menu.

6.10 Smart rules

IoT Extension includes a rule engine to analyze data in realtime and to perform actions based on data. These rules are specified in a scripting language and are managed in the Administration application.

To easily create rules, the Cockpit application includes a Smart Rules builder which allows you to create rules from templates (so-called smart rule templates).

Note

Smart Rules are only visible, if the tenant is subscribed to the Smart Rule application. To manage "Smart Rules", the user has to have INVENTORY CREATE permission and either SMART RULE permission or CEP MANAGEMENT permission.

Smart Rules are parameterized. There are two sources for parameters:

Rule Parameters are provided by the user when creating a Smart Rule from a template. Examples are email addresses and alarm texts.

Object Parameters are stored in the group or device. These parameters can be edited after the Smart Rule has been created. An example includes min and max values for thresholds.

Smart Rules can be seen

- in the Info tab of a device or group,
- in the Smart Rules page accessible from the Configuration menu.

There are two different kinds of Smart Rules:

- Local: Smart Rules created in either a group or a device. They are visible to everyone with access to the group/device.
- Global: These Smart Rules are created in a global context (Smart Rules page, alarms, data explorer, etc...). They are only visible to users with the relevant permissions.

In the Smart Rules page, only the global smart rules are shown.

In a local context (group or device) and without the relevant permissions, only the local Smart Rules are shown. If the user has the relevant permissions, both local and global Smart Rules are shown.
The permissions required in order to see the global Smart Rules are:

- Smart rule READ
- Smart rule ADMIN
- CEP management ADMIN

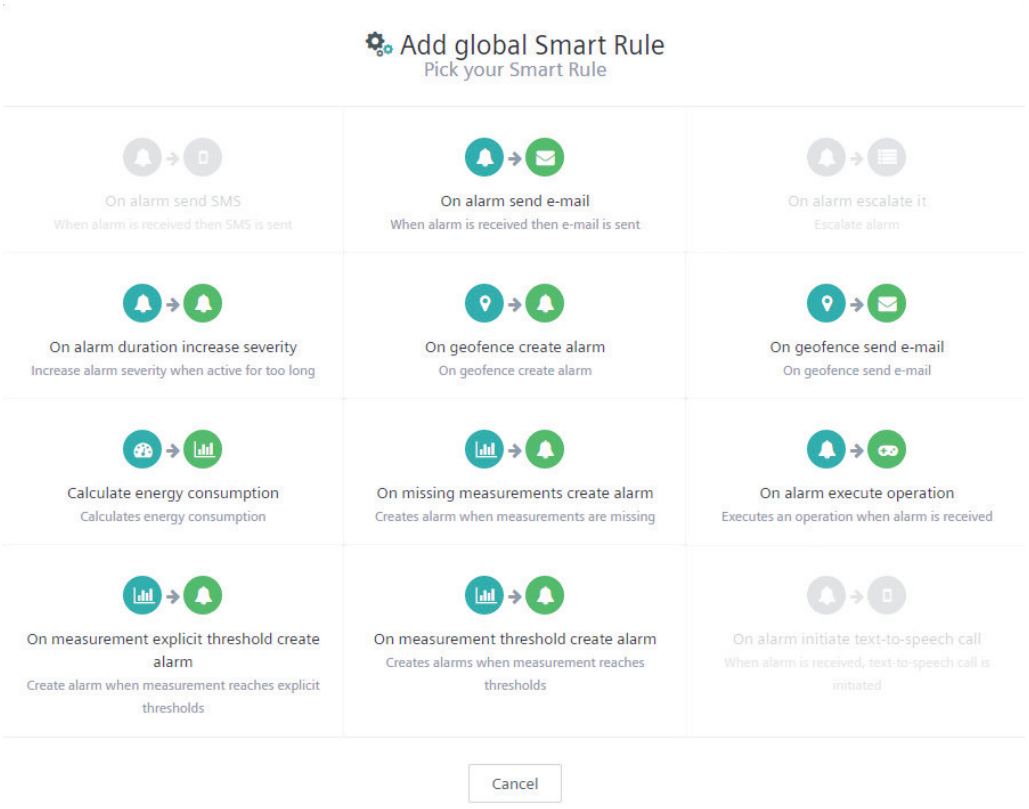
Creating Smart Rules

"Smart Rules" can be created either in the "Smart Rules" page, accessible from the "Configuration" menu in the navigator, or in the Info tab of a group or a device.

To create a "Smart Rule", follow these steps:

1. Click "Add Smart Rule" in the top menu bar.
2. Select a "Smart Rule" template from the list.
3. In the upcoming window, use the slider to select if the rule will be enabled or disabled.
4. Next, configure the rule parameters. The parameters differ from rule to rule, for details see individual rule descriptions below.
5. In the target asset or devices field, you can optionally activate the current "Smart Rule" for specific devices or assets.
6. Click "Create" to create the "Smart Rule".

A list of "Smart Rules" is shown below. Note that this list might differ based on your installation.



If the new rule was set to "enabled" and was not activated for specific objects, the rule will be active for all devices and groups. See next section on how to deactivate a smart rule for specific objects.

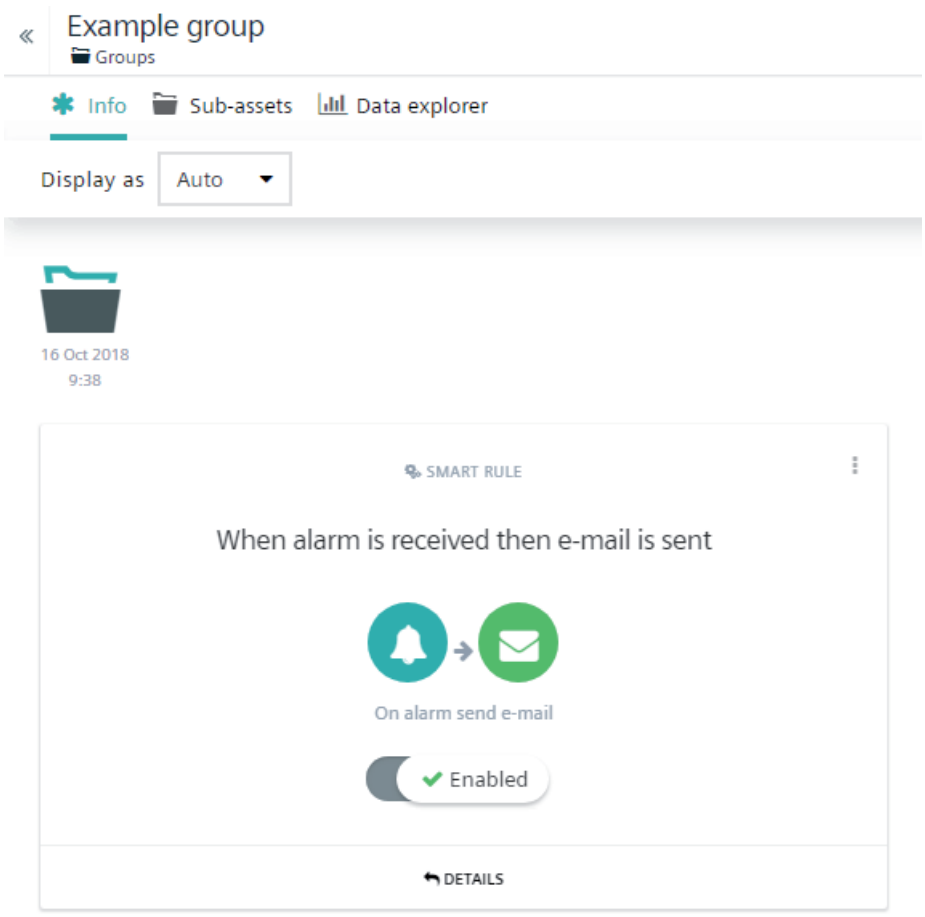
To avoid confusion, disabled "Smart Rules" are not displayed in group menus or device menus.

Smart Rules can be instantiated multiple times.

Activating or deactivating Smart Rules

A "Smart Rule" can be activated (switched on) and deactivated (switched off) for a single object (group or device). For example, if a device is generating too many threshold alarms, you can deactivate the rule for this single object. The rule is still active for all other objects.

To deactivate or activate a "Smart Rule" for a group or device, navigate to the Info tab of the group or device and enable/disable the respective rule using the slider.



Editing Smart Rules

To edit a "Smart Rule", just click the respective row or click the menu icon at the end of the row and from the context menu select "Edit".

Duplicating Smart Rules

To duplicate a "Smart Rule", click the menu icon at the end of the row and from the context menu select "Clone". Modify at least the name and click "Save & close" to save the "Smart Rule" and return to the "Smart Rule" list.

Removing Smart Rules

To remove a "Smart Rule", click the menu icon at the end of the row and from the context menu select "Remove".

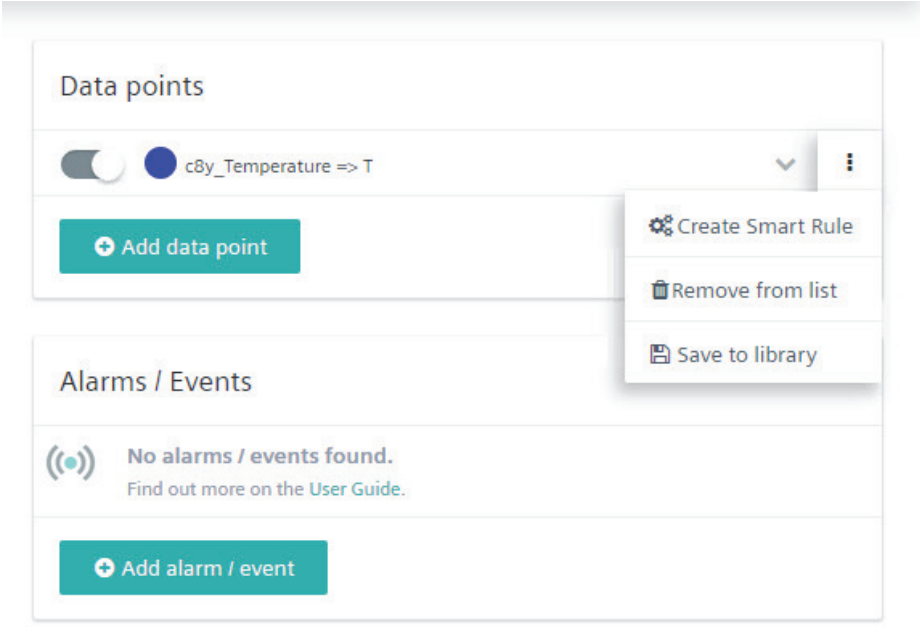
Debugging Smart Rules

For easier debugging, there is a direct link from a "Smart Rule" to the corresponding event processing module. Click the menu icon at the end of the row and from the context menu select "Inspect" to use this link.

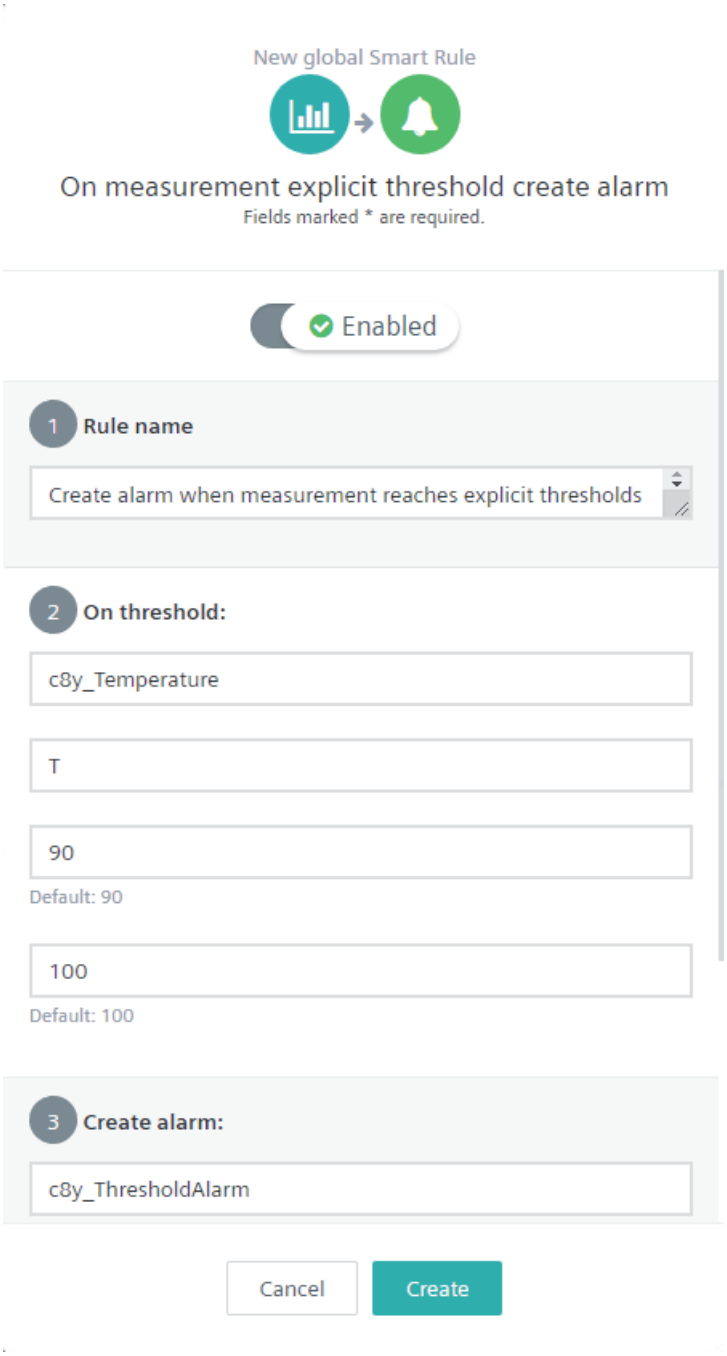
Example: Defining explicit thresholds

To define a threshold rule follow these steps:

1. In the navigator, select the desired group or device to apply a threshold to.
2. Switch to the "Data explorer" tab.
3. If the data point that should raise the threshold is not visible by default, select "Add data point" and add a data point.
4. Click the menu icon at the end of the row of the respective data point and select "Create Smart Rule".



5. Select the Smart Rule "On measurement explicit threshold create alarm".



6. Fill in the red range minimum and red range maximum value. When the measurement value enters or leaves the RED range, an alarm is created or respectively cleared. For details, see the description of the rule "On measurement explicit threshold create alarm" in the Smart rules collection (Page 188).
7. Under "Create Alarm" you can optionally edit the alarm type and the alarm text.
8. Under "Target assets" or devices you can select the object this rule will be applied to.
9. Click "Create" to create the Smart Rule.

The rule will automatically be set to active and alarms appear if they arise.

Chain rule execution

Smart Rules can create a new data item on the platform. For example, the threshold rule creates new alarms. This new data can be handled further by selected "Smart Rules", for example, by an "On alarm send e-mail" rule.

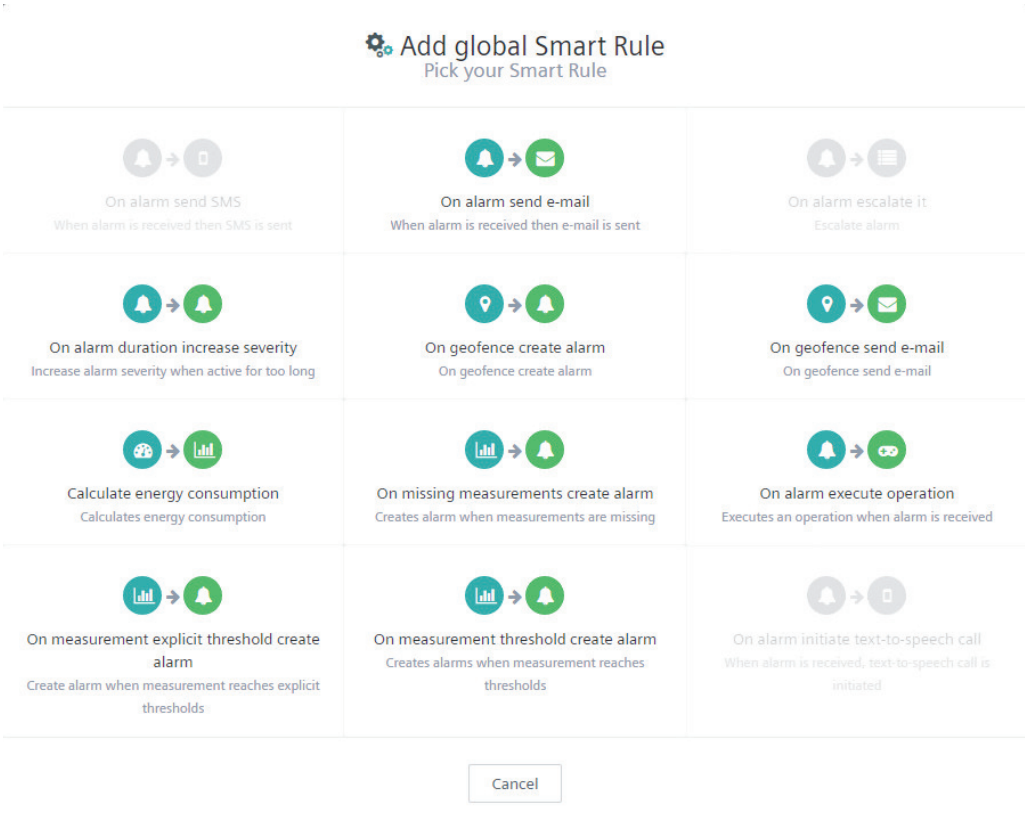
Using this mechanism, it is possible to create a chain of smart rules.

Note

If you create a rule chain keep in mind how much data will be created to avoid overload or excessive amount of data.

6.11 Smart rules collection

IoT Extension includes preset global Smart Rule types.



Each global Smart Rule type provides different parameters to configure.

The following section describes each available type and its configuration properties.

On alarm send SMS

Functionality

When an alarm is created, a SMS is sent.

Note

This rule is only available if your tenant has a configured SMS provider.

Parameters

The rule uses the following parameters:

Step	Field	Description
1	Rule name	Pre-filled with the name of the rule template. Can be modified according to your needs.
2	On alarm matching	The types of alarms triggering the rule. For each newly created alarm with one of these types in the list the rule is triggered.
3	Send SMS	"Phone number": Target phone number. It is recommended to include mobile country code for all numbers, e.g. "+49" or "0049" for Germany. Multiple numbers can be separated by a comma (",", do not use a space!). "Message": Text of SMS with max. 160 characters. You can use variables of the form #{name}. Supported variables are listed under "Smart Rule Variables" below.
4	Target asset or devices	Groups or devices the rule shall be applied to.

Troubleshooting

- Verify that the alarm was created and not duplicated from somewhere.
- Check if the device is in maintenance mode. In this case no new alarm will be created because of suppression policy.
- If you have configured an alarm mapping rule which changes the alarm severity, the alarm may have different severity than expected.

NOTICE
There is a limit of 160 characters as a total count. If you use variables and after applying the variables the text counts more than 160 characters the SMS will not be sent.

On alarm send e-mail

Functionality

When an alarm is created, an email is sent.

Parameters

The rule uses the following parameters:

Step	Field	Description
1	Rule name	Pre-filled with the name of the rule template. Can be modified according to your needs.
2	On alarm matching	The types of alarms triggering the rule. For each newly created alarm with one of these types in the list the rule is triggered.
3	Send e-mail	"Send to:/Send CC to:/Send BCC to": Email addresses for sending the e-mail to. Multiple addresses can be separated by a comma (",", do not use a space!). "Reply to": Address to be used to reply to the message. "Subject": Subject of e-mail. You can use a variable of the form #{name}. Supported variables are listed under "Smart Rule Variables" below. "Message": Text of the e-mail. You can use a variable of the form #{name}. Supported variables are listed under "Smart Rule Variables" below.
4	Target asset or devices	Groups or devices the rule shall be applied to.

Troubleshooting

- Verify that the alarm was created and not duplicated from somewhere.
- Check if the device is in maintenance mode. In this case no new alarm will be created because of suppression policy.
- If you have configured an alarm mapping rule which changes the alarm severity, the alarm may have different severity than expected.
- Check your spam folder.

On alarm escalate it

Functionality

When an alarm is created, sends e-mail, sms, and/or initiates text-to-speech.

Parameters

The rule uses the following parameters:

Step	Field	Description
1	Rule name	Pre-filled with the name of the rule template. Can be modified according to your needs.
2	On alarm matching	The types of alarms triggering the rule. For each newly created alarm with one of these types in the list the rule is triggered.
3	Escalate as follows	Escalation steps processed in a chain. Click Add step to define at least one step: Type: Type of action executed in the step. Possible values are: Email (see "On alarm send e-mail" rule for parameter descriptions). SMS (see "On alarm send SMS" rule for parameter descriptions). Phone (see "On alarm initiate text-to-speech call" rule for parameter descriptions). Condition: The condition applied when the rule will be executed. Possible values are: Always: Action will always be executed. * Always: If step N failed. Only phone steps may fail. The step is marked as failed once all retries have been made without a successful call. This option only appears if there already is a phone step configured that can be referred to.
4	Target asset or devices	Groups or devices the rule shall be applied to.

Troubleshooting

- Verify that the alarm was created and not duplicated from somewhere.
- Check if the device is in maintenance mode. In this case no new alarm will be created because of suppression policy.
- If you have configured an alarm mapping rule which changes the alarm severity, the alarm may have different severity than expected.

On alarm duration increase severity

Functionality

If an alarm is active for a certain time, the severity is increased.

Parameters

The rule uses the following parameters:

Step	Field	Description
1	Rule name	Pre-filled with the name of the rule template. Can be modified according to your needs.
2	On alarm matching	The types of alarms triggering the rule. For each newly created alarm with one of these types in the list the rule is triggered.
3	Increase alarm severity	Duration, an alarm must be active, before increasing the severity.
4	Target asset or devices	Groups or devices the rule shall be applied to.

Description

When a configured type of alarm is raised, it starts monitoring how long the alarm stays active.

If the alarm is still active after the specified duration, the severity will be increased one level, e.g. from MINOR to MAJOR.

If the alarm has reached CRITICAL, it will stop monitoring because there is no further action possible.

Note

The rule checks once a minute if the configured duration has been exceeded. Therefore it might happen that the alarm severity won't change in the second it exceeds the duration but only after the following check.

On geofence create alarm

Functionality

If a geofence border is crossed, an alarm is created.

The rule can be configured for entering or leaving the geofence, or both. Existing alarms are cleared when the opposite condition is true again, e.g. if a tracked car which has left the geofence area is re-entering the geofence area.

Parameters

The rule uses the following parameters:

Step	Field	Description
1	Rule name	Pre-filled with the name of the rule template. Can be modified according to your needs.
2	On geofence violation	Polygon that defines the borders of an area. Click Edit geofence and set the area. Double-click to add points and click and drag them to adjust.
3	Create alarm	Reason for triggering the alarm: "On entering", "On leaving" (the default), "On entering and leaving". Type of alarm being raised. Severity of alarm being raised. Alarm text.
4	Target asset or devices	Groups or devices the rule shall be applied to.

Note

In order to raise an alarm the device had to be inside the geofence at least once after creating the rule.

Troubleshooting

- Make sure the device was inside the geofence at least once after creating/activating the rule.
- Check if the device is in maintenance mode. No new alarm will be created because of suppression policy.
- If you have configured an alarm mapping rule which changes the alarm severity, the alarm may have different severity than expected.

On geofence send e-mail

Functionality

If a geofence border is crossed, an email is sent.

The rule can be configured for entering or leaving the geofence, or both.

Parameters

The rule uses the following parameters:

Step	Field	Description
1	Rule name	Pre-filled with the name of the rule template. Can be modified according to your needs.
2	On geofence violation	Polygon that defines the borders of an area. Click Edit geofence and set the area. Double-click to add points and click and drag them to adjust.
3	Send e-mail	Send to:/Send CC to:/Send BCC to: Email addresses for sending the e-mail to. Multiple addresses can be separated by a comma (",", do not use a space!). Reply to: Address to be used to reply to the message. Subject: Subject of e-mail. You can use a variable of the form #{name}. Supported variables are listed under "Smart Rule Variables" below. Message: Text of the e-mail. You can use a variable of the form #{name}. Supported variables are listed under "Smart Rule Variables" below.
4	Target asset or devices	Groups or devices the rule shall be applied to.

Note

In order to raise an alarm the device had to be inside the geofence at least once after creating the rule.

Troubleshooting

- Make sure the device was inside the geofence at least once after creating/activating the rule.
- Check your spam folder.

Calculate energy consumption

Functionality

Creates consumption data point based on data from an electric-, gas-, water- meter.

Parameters

The rule uses the following parameters:

Step	Field	Description
1	Rule name	Pre-filled with the name of the rule template. Can be modified according to your needs.
2	Monitored measurement	**Fragment/Series**: Name of the measurement fragment and series. The incoming measurement must have exactly the same fragment/series name as configured. When creating a rule from the data explorer, these fields are already filled in. **Time interval**: Interval in which consumption values shall be calculated. Specifies how often per hour the consumption is calculated.
3	Energy consumption measurement	Name of the measurement fragment and series that shall be generated.
4	Target asset or devices	Groups or devices the rule shall be applied to.

The unit of the consumption measurement is always per hour (i.e. if the measurements are in "kg" the consumption will be in "kg/h").

The rule takes the last two measurements for a specified time, calculates the difference in value and time and then calculates the consumption per hour.

Example

The rule is configured to calculate every 20 minutes. The following measurements are coming in: 100 kg at 11:59 and 200 kg at 12:14. At 12:20 the rule is triggered, taking the last two measurements. It calculates value and time difference. The consumption measurement created at 12:20 will therefore be 400 kg/h. If no new measurement was created in the last period a measurement with consumption 0 will be created.

On missing measurements create alarm

Functionality

If no new measurement data has been received for a specified time, an alarm is created.

Parameters

The rule uses the following parameters:

Step	Field	Description
1	Rule name	Pre-filled with the name of the rule template. Can be modified according to your needs.
2	Monitored measurement	Type: Type of measurement. The incoming measurement must have the same type as configured. When creating a rule from the data explorer, the type is already filled in. Time interval: Interval for calculating consumption values.
3	Create alarm	Type of alarm being raised. Severity of alarm being raised. Alarm text.
4	Target asset or devices	Groups or devices the rule shall be applied to.

Note

The rule checks once a minute if the configured time interval was exceeded. Therefore it can take up to one minute to create the alarm after the time interval was exceeded. To check if the time interval was exceeded there must be at least one incoming measurement after the activation of the rule.

On alarm execute operation

Functionality

If a certain alarm occurs, the specified operation will be send to the device.

Parameters

The rule uses the following parameters:

Step	Field	Description
1	Rule name	Pre-filled with the name of the rule template. Can be modified according to your needs.
2	On alarm matching	The types of alarms triggering the rule. For each newly created alarm with one of these types in the list the rule is triggered.

Step	Field	Description
3	Execute operation	The operation that will be sent. The operation is provided as JSON description. Some standard operations can be selected below the Operation field. To use a standard operation, select one, and press the arrow button on the right. This will insert the JSON of the selected operation.
4	Target asset or devices	Groups or devices the rule shall be applied to.

On measurement threshold create alarm

Functionality

When the measurement value enters or leaves the RED/YELLOW range, an alarm is created or respectively cleared.

The severity of alarm is determined as follows:

- If the measurement value moves into RED range, then the severity is CRITICAL.
- If the measurement value moves into YELLOW range, then the severity is MINOR.
- If the measurement value moves into GREEN range, the alarm is cleared.

The rule uses the following parameter from the device object or data point library:

- Object red range: Range when the system should create CRITICAL alarms. These values can be edited in the data explorer for each data point.
- Object yellow range: Range when the system should create MINOR alarms. These values can be edited in the data explorer for each data point.
- Data Point Library red/yellow range: When there is no red/yellow range stored in the respective object, then the Data Point Library is searched for the configured data point entry and the related red/yellow range is used.

Using this mechanism, you can configure global threshold ranges in the Data Point Library. These global values can then be overridden for specific objects on a case-by-case basis.

Parameters

The rule uses the following parameters:

Step	Field	Description
1	Rule name	Pre-filled with the name of the rule template. Can be modified according to your needs.
2	On threshold	Fragment/Series: Name of the measurement fragment and series. The incoming measurement must have exactly the same fragment name as configured. When creating a rule from the data explorer, these fields are already filled in. Data Point Library entry: Name of the entry in the Data Point Library. This is used to find the default values for red and yellow ranges in case they are not configured for an individual object.
3	Create alarm	Type: Type of alarm being raised. Text: Alarm message.
4	Target asset or devices	Groups or devices the rule shall be applied to.

Description

For each incoming measurement value, the rule performs the following steps:

- Check, if the measurement includes data for the fragment and series (rule parameter).
- Check, if the rule is activated for the source object.
- The data of the red and yellow range is collected from either:
- the source object (the measurement),
- the Data Point Library (control parameter).

If no red/yellow ranges are defined, no alarms are generated.

Note

Range values defined in the source object have a higher priority than those defined in the Data Point Library. You can also just overwrite a single value (e.g. yellow range max) by setting it in the source object. The other values will then be taken from the Data Point Library.

- Incoming value inside the yellow range:
  If there is an active alarm of given type for the object, set severity to MINOR. Otherwise create new MINOR alarm with given parameters.
- Incoming value inside the red range:
  If there is an active alarm of given type for the object, set severity to CRITICAL. Otherwise, create new CRITICAL alarm with given parameters.
- Measurement outside of yellow and red range:
  If there is an active alarm of given type for the object, clear the alarm.

Troubleshooting

- Verify that the alarm was created and not duplicated from somewhere.
- Check if the device is in maintenance mode. In this case no new alarm will be created because of suppression policy.
- If you have configured an alarm mapping rule which changes the alarm severity, the alarm may have different severity than expected.
- Check if an alarm was already cleared by the next scheduled measurements with resulting value in a green range.

Note

If you clear an alarm, you state that the alarm is resolved. A new alarm is not raised unless the device changes its state and exceeds the thresholds again.

On measurement explicit threshold create alarm

Functionality

When the measurement value enters or leaves the RED range, a CRITICAL alarm is generated or cleared.

The severity of alarm is determined as follows:

- If the measurement value moves into RED range, then the severity is CRITICAL.
- If the measurement value moves into GREEN range, the alarm is cleared.

Note

This rule is similar to the rule "On measurement threshold create alarm". However, in this rule here the RED threshold value is provided explicitly. The threshold rule "On measurement threshold create alarm" extracts the thresholds values from the device or "Data Point Library".

Parameters

The rule uses the following parameters:

Step	Field	Description
1	Rule name	Pre-filled with the name of the rule template. Can be modified according to your needs.
2	On threshold	Fragment/Series: Name of the measurement fragment and series. The incoming measurement must have exactly the same fragment name as configured. When creating a rule from the data explorer, these fields are already filled in. Minimum, Maximum: When a value is in the specified range [minimum; maximum], the configured alarm is raised.
3	Create alarm	Type: Type of alarm being raised. Text: Alarm message.
4	Target asset or devices	Groups or devices the rule shall be applied to.

Troubleshooting

- Verify that the alarm was created and not duplicated from somewhere.
- Check if the device is in maintenance mode. In this case no new alarm will be created because of suppression policy.
- If you have configured an alarm mapping rule (see Administration > Reprioritizing alarms) which changes the alarm severity, the alarm may have different severity than expected.
- Check if an alarm was already cleared by the next scheduled measurements with resulting value in a green range.

Note

If you clear an alarm, you state that the alarm is resolved. A new alarm is not raised unless the device changes its state and exceeds the thresholds again.

On alarm initiate text-to-speech call

Functionality

When an alarm is created, it initiates a text-to-speech call.

Parameters

The rule uses the following parameters:

Step	Field	Description
1	Rule name	Pre-filled with the name of the rule template. Can be modified according to your needs.
2	On alarm matching	The types of alarms triggering the rule. For each newly created alarm with one of these types in the list the rule is triggered.
3	Text-to-speech	Phone number: Valid international phone number. Use country codes in the format "+49" (as an example for Germany). Message: The text read out by the rule. Retries: The number of retries to reach the target phone number if not successful (default is "0", max is "20"). Interval: The time interval between the retries in minutes (default is "5"). Acknowledgment: If selected the receiver of the call has to acknowledge the call (a call not acknowledged will not count as successful) Acknowledgment text: The acknowledgment message which will be read after the main message, for example: "Please acknowledge this call by pressing the button 5". Acknowledgment number: The number of the button the receiver has to push to acknowledge. If the button has been pushed, the call will be successful and the alarm status will be changed to acknowledged.
4	Target asset or devices	Groups or devices the rule shall be applied to.

Troubleshooting

- Make sure that the alarm was created and not duplicated from somewhere.
- Check if the device is in maintenance mode. No new alarm will be created because of suppression policy.
- If you have configured an alarm mapping rule (see Administration > Reprioritizing alarms) which changes the alarm severity, the alarm may have different severity than expected.

Smart Rule Variables

In certain rule parameters, variables can be used. When a rule is triggered, the variables are replaced by their actual values. You can use this mechanism to insert device names or alarm text into various outputs (email, SMS, text-to-speech). You can include any information of the triggering event (like the alarm) and its source device.

The following table lists example variables:

Variable	Content
#{creationTime}	Time when the alarm was created in the database.
#{type}	Type of the alarm.
#{time}	Time of alarm, as provided by the alarm.
#{text}	Textual description of the alarm.
#{source.name}	Name of the device.
#{source.c8y_Hardware.serialNumber}	Serial number of the device.
#{source.c8y_Notes}	Note field of the device.
#{status}	Status of the alarm: "ACTIVE", "ACKNOWLEDGED" or "CLEARED".
#{severity}	Severity of the alarm: "CRITICAL", "MAJOR", "MINOR" or "WARNING".
#{count}	Number of alarm messages for this device: Repeating messages for the same device and same alarm type are de-duplicated into one alarm.
#{source.c8y_Address.street}	Street of the device.
#{source.c8y_Address.cityCode}	ZIP code of the device.
#{source.c8y_Address.city}	City of the device.

Note

In case the variable does not exist or is misspelled, the generated content is displayed.

Cloud Remote Access

7

Overview

The IoT Extension Cloud Remote Access feature allows you to remotely access operating panels and other devices via a web browser.

The remote-controlled device runs a VNC, SSH or Telnet server and is connected to a gateway compatible with Cloud Remote Access. This gateway must be registered as a device within the Device Management application in IoT Extension. More information about registering devices and instructions can be found in Device Management > Device Registration.

With Cloud Remote Access users can

- view status visualizations and track updates of remote devices immediately as if the user were at the device location,
- connect to remote devices easily as complex VPN setups are not required,
- establish connection via Telnet or SSH to the gateway itself or to any device in the local area network.

The connection to remote devices is securely encrypted through TLS technology. Additionally, passwords are encrypted in your IoT Extension account, so that you do not need to manage them elsewhere.

Using Cloud Remote Access

Cloud Remote Access is available in the Device Management application.

To use Cloud Remote Access, the following prerequisites have to be met:

- a Cloud Remote Access compatible gateway connected to your IoT Extension account;
- a device with a VNC, SH or Telnet server that is connected to the gateway and reachable from the gateway.

Click "All devices" and select the desired gateway from the device list.

When you open the device you will find the Remote access tab in the tab list of the device.

Note

The Remote Access tab is visible only if your device/gateway supports the Remote Access functionality.

In the Remote Access tab, you can configure devices for remote control, so-called "endpoints", and connect to a device.

Connections can be established to the gateway itself (localhost) or to any device in the local area network reachable by the device.

Note

If the prerequisites are met and you do not see the Remote access tab in the tab list of your gateway, please contact sales@IoT Extension.com.
If you are a gateway manufacturer and would like to support Cloud Remote Access on your gateway, please contact support@IoT Extension.com.

Configuring endpoints

The "endpoint" is the IP address and port of the VNC, SSH or Telnet server running on the device. The IP address and port need to be reachable from the gateway.

To configure new remote devices, click "Add endpoint". Follow the descriptions below for configuring the various kind of endpoints.

Note

To be able to configure an endpoint, you need "Admin" permission for "Remote access" and "Device control". To read data, a “Read” permission is sufficient. For more information on permissions, refer to Managing permissions (Page 19) in Administration (Page 13).

Adding remote access endpoints via VNC

To configure a remote access endpoint via VNC, enter a description for the remote access endpoint, the IP address and port, and the password of the VNC server. Click "Save" to add the endpoint to the list.

Once the connection is established, a new browser tab will open displaying the front screen or operating panel of the device you are connected to. The top bar of the screen will show “starting VNC handshake” when the process is starting.

Adding remote access endpoints via Telnet

Enter the name of the endpoint. Select the Telnet protocol from the dropdown menu. Enter the IP address and the port. When ready, click "Save".

NOTICE
Be aware, that Telnet is considered to be an insecure protocol lacking built-in security measures. For network communication in a production environment we highly recommend to use the SSH protocol instead.

Adding remote access endpoints via SSH

To configure a remote access endpoint via SSH, enter the name of the endpoint, select the "SSH" protocol from the dropdown list, and enter the IP address and the port. There are two Sign-in methods to be selected:

- Username and password: If this method is selected, it is mandatory to enter username and password.
- Public/private keys: Automatically generate public and private keys or simply paste pre-generated keys. The keys can also be uploaded from a file.

Note

The public key needs to be installed on the device as authorized_key.

Optionally, you can also add a host key to ensure connection to the correct device. This key can also be uploaded from a file.

Click "Save" to save your settings.

The following formats are supported when adding new keys:

- OpenSSHv1
- OpenSSHv2
- PEM
- SSH2

The following algorithms are supported when adding new keys:

- RSA
- DSA
- ECDSA
- ED25519

Editing or removing endpoints

To edit or remove an endpoint, click the menu icon at the right of a row and select "Edit" or "Remove" from the context menu.

Connecting to endpoints

To connect to configured endpoints, choose an endpoint in the Remote access tab and click "Connect". The connection to the configured device is established and the VNC, SSH or Telnet screen is shared in the client area.

To terminate the connection, click "Disconnect".

Displaying the audit logs

Audit logs are displayed for each device.

For each connection the Cloud Remote Access microservice creates an operation in scope of the current user. The operation then will be updated by the device to reflect the current status. Finally the operation will be in state SUCCESSFUL or FAILED.

The audit logs can be found in the Control tab of the device.

Compatibility and limitations

VNC protocol

The following versions of the VNC protocol are currently supported:

- RFB 003.003
- RFB 003.007
- RFB 003.008

The functionality has been tested on the following VNC servers:

- Real VNC 5.3.2
- Tiger VNC 1.6.0/1.7.0
- TightVNC 1.3.9
- EfonVNC 4.2
- Vino

The following operating systems/browsers are currently supported:

Operating System	Browser	Touch	Swipe	Keyboard	Pointer
Windows 10	Edge 38	Yes	Yes	Yes	Minor
Windows 10	Internet Explorer 11.5.6.7	Yes	Yes	Yes	Minor
Windows 10	Firefox 51	Yes	Yes	Yes	Yes
Ubuntu 16.04	Chrome 56	Minor	Yes	Yes	Yes
Ubuntu 16.04	Firefox 51	Minor	Yes	Yes	Yes
MacOS	Safari	Yes	Yes	Yes	Yes
iOS 10.2.1	Safari	Yes	Minor	No	n/a
Android 6.0.1	Chrome	Yes	Minor	No	n/a
Android 6.0.1	Stock browser 5.0	Yes	Minor	No	n/a

Telnet protocol

The following limitations apply to Cloud Remote Access for Telnet:

Area	Scrolling	Reflow on width change	Bitmap fonts	Vector fonts	Mouse tracking	Applica-tion key-pad	Tabs	Split screen
Console	Yes	No	Yes	Yes	Yes	Yes	?	Yes
xterm	Yes	No	Yes	Yes	Yes	Yes	No	No

SSH protocol

For Cloud Remote Access for SSH the same limitations as mentioned for Telnet apply (see above). Also the following additional limitations are known:

- International characters are not to be supported yet.
- Only limited number of control characters are working. For example interrupt (ctrl+c) is not working yet.
- Mouse movements are not supported.
- Only SSHv2 protocol is supported.

Troubleshooting

If you cannot set up new endpoints, check if you have sufficient permissions.

To set up new endpoints, you need "Admin" permission for "Device control" to be able to register a device and “Admin” permission for "Remote access" to be able to add an endpoint.

To establish a connection to a remote operating panel, a “Read” permission for "Remote access" is sufficient.

For more information on permissions, refer to Administration (Page 13) > Managing permissions (Page 19).

The connection via a gateway to a remote VNC, SSH or Telnet server can fail because of network problems. In this case you need to contact your network administrator.

Firewall Settings

8

The IP address currently used to connect with MindConnect IoT Extension is `35.157.191.77`. Since this is a public IP and it may change, it is recommended to apply the rules based on DNS entries as given below:

```
$ host 35.157.191.77
77.191.157.35.in-addr.arpa domain name pointer ec2-35-157-191-77.eu-
central-1.compute.amazonaws.com
```