



Standard tenant administration

Last updated: 03/03/2026

This content applies to the latest CD version of Cumulocity.

Specifications contained herein are subject to change and these changes will be reported in subsequent versions.

Copyright © 2026 Cumulocity GmbH.

The name Cumulocity GmbH and all Cumulocity GmbH product names are either trademarks or registered trademarks of Cumulocity GmbH and/or its subsidiaries and/or its affiliates and/or their licensors. Other company and product names mentioned herein may be trademarks of their respective owners.

This software may include portions of third-party products. Third-party terms are set out in a 3rd-party-licenses file linked to or included with each installation package.

Table of Contents

Table of Contents	3
INTRODUCTION	6
HOME SCREEN	7
MANAGING USERS	9
TO VIEW USERS	10
TO ADD A USER	10
TO EDIT A USER	12
TO COPY INVENTORY ROLES	12
TO DELEGATE/UNDELEGATE USER HIERARCHIES	12
TO DISABLE/ENABLE A USER	12
TO DELETE A USER	13
TO LOG OUT ALL USERS	13
MANAGING PERMISSIONS AND ROLES	14
GLOBAL ROLES	15
TO ADD A GLOBAL ROLE	16
TO ASSIGN GLOBAL ROLES	18
INVENTORY ROLES	19
TO VIEW INVENTORY ROLES	19
TO ADD AN INVENTORY ROLE	19
TO ASSIGN INVENTORY ROLES TO USERS	24
GRANTING APPLICATION ACCESS	24
TROUBLESHOOTING PERMISSIONS	24
IMPROVING THE PERFORMANCE	24
LIMITATIONS OF INVENTORY ROLES BASED ACCESS	25
OPTIMIZED	25
LEGACY	25
MANAGING THE ECOSYSTEM	26
MANAGING APPLICATIONS	27
TO VIEW APPLICATIONS	27
TO EDIT AN APPLICATION	27
TO DELETE AN APPLICATION	28
FEATURES	28
SUBSCRIBED APPLICATIONS	28
APPLICATIONS SUBSCRIBED BY DEFAULT	29
CUSTOM APPLICATIONS	29
TO UPLOAD A WEB APPLICATION	30
TO LINK TO AN EXTERNAL APPLICATION	30
TO INSTALL AN APPLICATION FROM A BLUEPRINT	30
TO DUPLICATE AN APPLICATION	30
APPLICATION PROPERTIES	31
EXTENSIONS	33
EXTENSIONS	33
PLUGINS	35
UPLOADING ARCHIVES	36
TO UPLOAD AN ARCHIVE	36
TO RESTORE AN OLDER APPLICATION VERSION	37
TO REACTIVATE A SINGLE APPLICATION	37
MANAGING MICROSERVICES	37
SUBSCRIBED MICROSERVICES	37
CUSTOM MICROSERVICES	38
MICROSERVICE PROPERTIES	38
MICROSERVICE PERMISSIONS	39
MONITORING MICROSERVICES	39

STATUS INFORMATION	40
LOG FILES	40
MONITORING	42
AUDIT LOGS	42
TO VIEW AUDIT LOGS	42
TO FILTER LOGS	43
AUDIT LOG TYPES	43
MESSAGING SERVICE	46
TO VIEW THE TOPICS	46
TO VIEW THE TOPIC DETAILS	48
MONITORING NOTIFICATIONS 2.0	48
MONITORING THE MQTT SERVICE	49
FREQUENTLY ASKED QUESTIONS (FAQ)	50
ALARM MAPPING	51
TO VIEW ALARM MAPPINGS	51
TO ADD ALARM MAPPING	52
TO EDIT AN ALARM MAPPING	52
TO DELETE AN ALARM MAPPING	52
MANAGING DATA	53
RETENTION RULES	53
TO VIEW RETENTION RULES	53
DATA TYPES	54
TO ADD A RETENTION RULE	54
TO EDIT A RETENTION RULE	55
TO DELETE A RETENTION RULE	55
EXECUTION EXAMPLES	55
FILE REPOSITORY	55
TO UPLOAD A FILE FROM YOUR FILE SYSTEM	56
TO DOWNLOAD A FILE FROM YOUR ACCOUNT	57
TO DELETE A FILE FROM YOUR ACCOUNT	57
LATEST MEASUREMENT VALUES	57
HOW TO ENABLE IT	57
HOW IT WORKS	57
PREVIOUS MEASUREMENTS VALUES	59
IMPLICATIONS & PRECONDITION	60
LIMITATIONS	60
CHANGING SETTINGS	61
APPLICATION	61
TO CHANGE APPLICATION SETTINGS	61
PROPERTIES LIBRARY	62
TO ADD A CUSTOM PROPERTY	63
TO EDIT A CUSTOM PROPERTY	63
TO REMOVE A CUSTOM PROPERTY	63
SMS PROVIDER	64
TO ENTER SMS PROVIDER CREDENTIALS	64
CONNECTIVITY	64
TO PROVIDE OR REPLACE CREDENTIALS	65
LOCALIZATION	65
TO ADD NEW IDENTIFIER FOR TRANSLATIONS	65
TO ADD AND EDIT TRANSLATIONS	66
ENHANCED TIME SERIES SUPPORT	67
GENERAL CONFIGURATION	67
TO CONFIGURE TIME SERIES SUPPORT	67
IMPLICATIONS OF THE CONFIGURATION	67
UNSUPPORTED APIS	68

TO CHECK WHETHER TIME SERIES COLLECTIONS ARE ENABLED	68
MIGRATION PROCESS DESCRIPTION	68
TO TRIGGER TIME SERIES MIGRATION	69
MIGRATION STATES	70
DESCRIPTION AND PROGRESS MONITORING	70

INTRODUCTION

In the administration application, account administrators can manage numerous functions and settings for their account.

On Standard tenant level, administrators can manage [users](#), [permissions](#), [applications & microservices](#), and more. Moreover they can configure various settings for their account.

Refer to [Enterprise tenant administration](#) for information on the configuration of additional functionalities available in Enterprise tenants.

For details on authentication settings, refer to [Authentication](#).

HOME SCREEN

✓ REQUIREMENTS

APPLICATION ACCESS:

The user must have access to the Administration application.

ROLES & PERMISSIONS:

- To see usage statistics for the current tenant: READ permission for the permission type "Tenant statistics".
- To view subscribed applications: READ permission for the permission type "Application management".

The Home screen of the Administration application provides the following content:

- A welcome message
- Quick links to the main parts of the Administration application
- Your capacity usage for the current and for the last month
- The optional applications you are subscribed to

The screenshot shows the Administration application's Home screen. On the left is a sidebar with a gear icon labeled 'ADMINISTRATION' and a list of navigation items: Home, Accounts, Tenants, Ecosystem, Business rules, Management, Settings, Data broker, and Migration. The main content area has a header with a hamburger menu, 'Home', and a user profile icon 'JD'. Below the header, there's a 'Welcome to Administration' section with a message about adding/removing users and roles, and links to subscribe to applications and change settings. To the right is a 'Quick links' section with icons for Users, Roles, Applications, Application settings, and Usage statistics. Below this are three sections: 'Current month usage' (usage between 1 Feb 2025 - 8 Feb 2025), 'Last month usage' (usage between 31 Dec 2024 - 31 Jan 2025), and 'Subscribed apps' (listing Cockpit, Device Management, and Digital Twin Manager). The bottom of the sidebar shows 'powered by CUMULOCITY'.

The capacity sections show:

- API requests - the total number of API requests, counting whenever some function in Cumulocity 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 rules](#) and by the amount and size of [stored files](#).
- 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, active and inactive.

 > Standard tenant administration > Home screen

MANAGING USERS

The **user management feature** allows you to manage the users within your tenant, that is create users, store user details, or configure login and security options.

✔ REQUIREMENTS

ROLES & PERMISSIONS:

“User management” permission type:

- To view users: READ permission
- To manage (create, edit, delete, disable/enable, delegate, manage permissions) all existing users: ADMIN permission
- To create users: CREATE permission

“Own user management” permission type (has no influence on user management capabilities):

- To view the own user: READ permission
- To edit the own user: ADMIN permission

Note that each user created on the platform can edit its own information by default, regardless of the “Own user management” permissions. The purpose of the “Own user management” permission is to manage specific users created for technical purposes, for example, by microservices, and determine whether such users can be managed by respective services.

On tenant creation, there are default roles available that can be used as a sample configuration for the above mentioned permissions:

- Global User Manager - Can access and modify the full user hierarchy
- Shared User Manager - Can create new users as his own subusers and manage them (“feature-user-hierarchy” application subscription required)

Note that when subscribed to the “feature-user-hierarchy” application, the CREATE permission allows to manage (display, create, edit, delete, disable/enable, delegate, manage permissions) underlying users. For details see [Managing user hierarchies](#).

For users created via an external authorization server, updating the following settings in Cumulocity will have no effect (will be reset on the next user re-login):

- user info (login alias, email, first name, last name, telephone)
- global roles - configurable via SSO access mapping
- application access - configurable via SSO access mapping
- inventory roles assignments - configurable via SSO access mapping

Moreover, password reset in Cumulocity is disabled for users created through an external authentication server.

i INFO

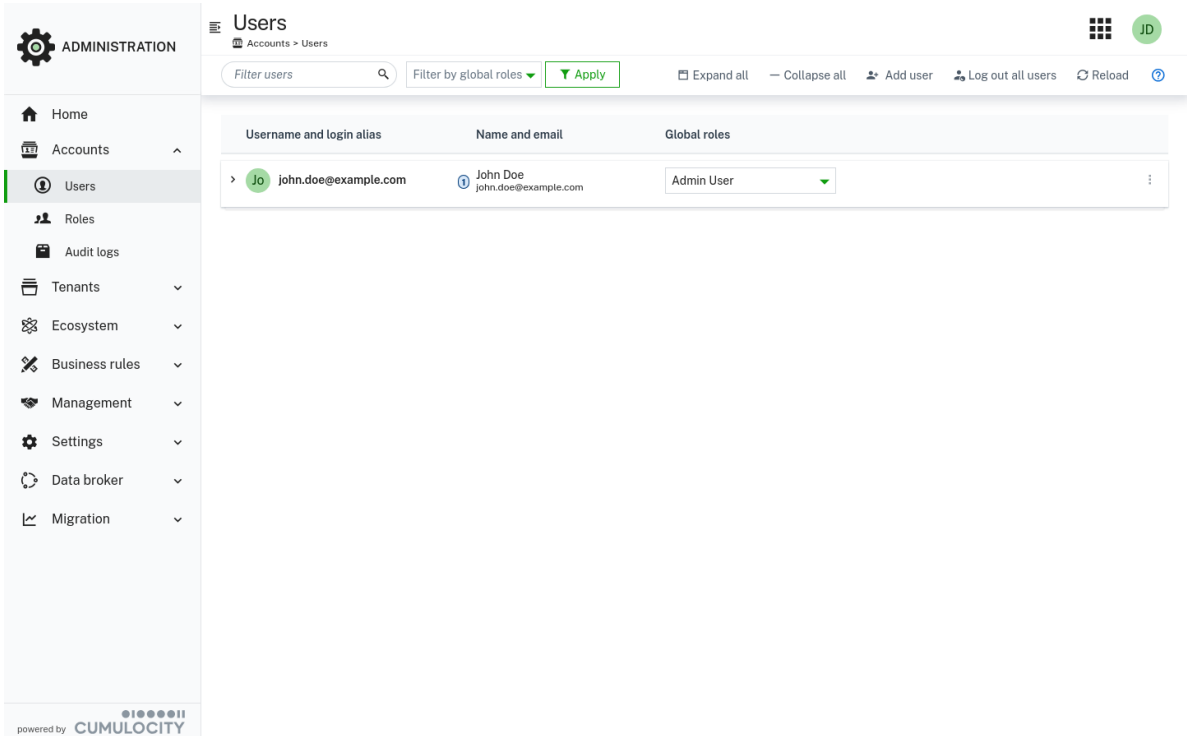
Users which are using single sign-on cannot change the password of users which are managed by the platform.

RELATED TOPICS

- [Platform administration > Standard tenant management > Managing permissions](#) for details on assigning roles and permissions to users.
- [Getting started > Technical concepts > Tenant hierarchy](#) for information on the concept of multi-tenancy as opposed to user access control.
- [Users](#) in the Cumulocity OpenAPI Specification for managing users via REST.

TO VIEW USERS

To view all users in your tenant, click **Users** in the **Accounts** menu in the navigator.



The screenshot shows the Cumulocity Users management interface. On the left is a sidebar with the 'ADMINISTRATION' menu, where 'Users' is selected. The main content area is titled 'Users' and shows a table of users. The table has three columns: 'Username and login alias', 'Name and email', and 'Global roles'. One user is listed with the username 'john.doe@example.com', name 'John Doe', and role 'Admin User'. Above the table are search and filter controls, including a 'Filter users' search bar, a 'Filter by global roles' dropdown, and an 'Apply' button. There are also buttons for 'Expand all', 'Collapse all', 'Add user', 'Log out all users', 'Reload', and a help icon. The bottom of the sidebar shows 'powered by CUMULOCITY'.

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

- The username 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 by username, you can use the filter field at the left of the top menu bar. With the dropdown list you can filter by global roles. For details on filtering, see [Filtering](#).

In order to apply the selected filters click **Apply**.

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](#).

TO ADD A USER

1. Click **Add user** at the right of the top menu bar.

INFO

If single sign-on is enabled for your tenant, a message will show up which reminds you that you are about to create a local user which will not be able to login via single sign-on.

- At the left of the **New user** window, provide the following information to identify the user:

Field	Description
User name	Serves as a unique 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 username, an optional alias can be provided to be used to log on. In contrast to the username, this alias may be changed if required. The login alias cannot be the same as the username. Note that the login alias is not supported for devices.
Status	Enable/disable the user account here. If the user account is disabled the user cannot login.
Email	A valid email address. This field is mandatory.
First name	First name of the user.
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.
Owner	Another user that manages ("owns") the new user. Select a user from the dropdown list and click Done to confirm. Refer to Managing user hierarchies for details on user hierarchies.
Delegated by	Can be activated to delegate user hierarchies and permissions to the user. Refer to Managing user hierarchies for details on delegation.

For additional information see [User options and settings](#).

- Select the login options for the user.

If TFA authorization via SMS is enabled for the tenant:

- **Two-factor authentication (SMS)** - If selected, the user will receive a verification code via SMS which is required to complete the authentication. The SMS will be sent to the phone number configured above. For details refer to [Two-factor authentication](#).

If TFA authorization via TOTP is enabled for the tenant:

- **Two-factor authentication (TOTP)** - If selected, the user must provide TOTP from a third-party authentication application to complete the authentication. For details refer to [Two-factor authentication](#).
- **Enforce TOTP setup for the user** - If selected, the user must setup TOTP on the first login. For details refer to [Two-factor authentication](#).

4. Select the password options for the user.

- **Send password reset link as email** - If selected, 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. This option is only available during user creation.
- **Set password that must be changed on the first login** - If selected, you must provide a password which the user must reset on the next login.
- **Set password for the user (no change required)** - If selected, you must provide a password. A password change is not required by the user.

INFO

While entering the password, the strength of the password is checked. See [To change your password](#) for further information on password reset and strength.

5. On the right of the page, select the global roles for the user. Details on global roles are described in [Managing permissions and roles](#).


6. Click **Save** to save your settings.

The new user will be added to the user list.


INFO

By default, manually created users always have the “Own user management” permissions set to active.

TO EDIT A USER


1. Click the menu icon  at the right of the respective row and then click **Edit**. All fields except **Username** and **Send password reset link as email** can be changed. For details on the fields, see [To add a user](#).
2. Click **Change password** to change the password.
3. Click **Save** to apply your settings.

TO COPY INVENTORY ROLES

1. Click the menu icon  at the right of the respective row and then click **Copy inventory roles from another user**.
2. In the resulting dialog box, select if you want to merge the roles to be copied with the existing user roles (the default) or if you want to replace the existing user roles.
3. Select the user from which you want to copy roles from the dropdown list.
4. Click **Copy**.

The inventory roles will be copied from the selected user.


TO DELEGATE/UNDELEGATE USER HIERARCHIES

Click the menu icon  at the right of the respective row and then click **Delegate** to delegate your user hierarchies and permissions to a user.


Click **Undelegate** to remove a delegation.

Refer to [Managing user hierarchies](#) for details on delegation.

TO DISABLE/ENABLE A USER

Click the menu icon  at the right of the respective row and then click **Disable** to disable an active user, or click **Enable** to enable a user that has been disabled.

TO DELETE A USER

Click the menu icon  at the right of the respective row and then click **Delete**.

TO LOG OUT ALL USERS

In the event of a security incident involving the session tokens of your tenant's users, you can invalidate any tokens currently in use.

To log out all users click **Log out all users** at the right of the top menu bar. This logs out all users currently logged in via OAI-Secure or single sign-on redirect. JWT tokens retrieved by all devices in the current tenant are also invalidated.

Note that, if basic authentication is used, users logged in via base64 token are not logged out.

REQUIREMENTS

To log out all users, you must have ADMIN permission for the permission type "User management".

MANAGING PERMISSIONS AND ROLES

Permissions define what a user is allowed to do in Cumulocity applications.

Permissions are not assigned to users directly. To manage permissions more easily, they are grouped into roles (global and inventory roles). Every user can be associated with a number of roles, adding up permissions of the user.

INFO

In the Cumulocity API, each granular permission is identified by a unique “permission” string, which is prefixed with `ROLE_` (for example, `ROLE_ALARM_READ` , `ROLE_INVENTORY_ADMIN`). Therefore, permissions are frequently referred to as “roles” throughout the API as well as in the configuration files. See also the glossary for the usage of the terms [permission](#) and [role](#) in the Cumulocity context.

REQUIREMENTS

ROLES & PERMISSIONS:

- To view global roles, inventory roles, applications: READ permission for the “User management” permission type.
- To manage global roles (assign to users, unassign from users), to manage inventory roles, to manage application access: ADMIN permission for the “User management” permission type.
- To assign owned roles to users (“feature-user-hierarchy” application subscription required): CREATE permission for the “User management” permission type.
- To create new roles with available (owned) permissions: CREATE and ADMIN permission.

The above permissions can be used to create roles for robust user management. Every new tenant has these roles by default:

- Global User Manager - Can access and modify the full user hierarchy
- Shared User Manager - Can create new own sub-users and manage them (“feature-user-hierarchy” application subscription required)

RELATED TOPICS

- [Platform administration > Standard tenant management > Managing users](#) for information on managing users in general.
- [Platform administration > Standard tenant management > Managing applications](#) for more information on managing applications.
- [Platform administration > Enterprise tenant administration > Managing user hierarchies](#) for more information on managing user hierarchies.
- [Device management & connectivity > Device integration > Fragment library](#) for further information on fragment types.
- [Roles](#) and [Inventory Roles](#) in the Cumulocity OpenAPI Specification for managing permissions via REST.

GLOBAL ROLES

Click **Roles** in the **Accounts** menu to display a list of configured roles.

The screenshot shows the 'Roles' management page. On the left is a sidebar with navigation options: Home, Accounts, Users, Roles (selected), Audit logs, Tenants, Ecosystem, Business rules, Management, Settings, Data broker, and Migration. The main content area is titled 'Roles' and has a breadcrumb 'Accounts > Roles > Global roles'. Below the title are tabs for 'Global roles' and 'Inventory roles'. A 'Display as' dropdown is set to 'Auto', and there is a 'Filter...' search bar. A '+ Add global role' button is in the top right. The roles are displayed in a grid of 12 cards, each with a role icon, name, and description. The roles are: Admin User, Business User, CEP Manager, Cockpit User, Device Management..., Device User, Global Manager, Global Reader, Global User Manager, Reader User, Shared User Manag..., and Tenant Manager. Each card has a 'DESCRIPTION' section with details about the role's permissions.

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

INFO

The pre-defined roles are configured as samples for a particular purpose. You may use them as a starting point and further adapt them to your individual needs.

On creating a new user, make sure that the global roles you assign to the user contain all necessary permissions relevant for this particular user in either of those roles assigned. Permissions from different roles are merged together when assigned to the same user. If, for example, a user only has the role “Cockpit User” (see below), the user is only able to access the Cockpit application and nothing more. But if you also assign inventory permission via some of the available roles, the user will get access to the whole inventory, such as devices, groups, and configurations.

The roles “admins” and “devices” have a special status:

Role	Description
admins	Administrative 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 pre-configured roles are initially provided.

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.
Devicemanagement 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 data from all devices.
Global Reader	Can read all data from all devices.
Global User Manager	Can manage all users.
Shared User Manager	Can manage sub-users. The subscription plan must 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 also 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”).

TO ADD A GLOBAL ROLE

Click **Add global role** in the **Global roles** tab. In the **New global role** page you will see a list of permission types at the left and a list of applications to be accessed at the right. The following screenshot shows the settings for the “admins” role.

The screenshot displays the 'New global role' configuration page. On the left is a navigation sidebar with 'ADMINISTRATION' and various menu items. The main content area is titled 'New global role' and includes a breadcrumb 'Accounts > Roles > Global roles'. The configuration is divided into three main sections:

- Global role:** Contains input fields for 'Name' (pre-filled with 'New global role') and 'Description'.
- Permissions:** A table with columns for 'TYPE', 'READ', 'ADMIN', 'CREATE', and 'UPDATE'. It lists various system components with checkboxes to assign permissions.
- Application access:** A section titled 'SUBSCRIBED APPLICATIONS' with a list of applications and checkboxes to grant access. Below this is a 'CUSTOM APPLICATIONS' section with 'Administration' and 'Cockpit' listed.

At the bottom of the form are 'Cancel' and 'Save' buttons. The footer of the interface shows 'powered by CUMULOCITY'.

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 - change and delete the specified data (not including READ).
- ADMIN - create, update or delete the specified data.

INFO

CREATE permissions are related to the concept of ownership in Cumulocity. 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 UPDATE 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.
Application management	View or edit the applications available in this account.
Audits	View or create audit logs.
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.
Global smart rules	Configure global smart rules.
Identity	View or edit identifiers for devices.
Inventory	View or edit inventory data.
Measurements	View or create measurements.
Option management	View or edit account options such as password policies.
Retention rules	View or edit retention rules.

Category	Description
Schedule reports	Manage the schedule of report exporting.
Simulator	Configure simulated devices.
Sms	Configure SMS.
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, global roles and permissions.
Own user management	View or edit your own user. Note that this permission may only be applicable to technical users.

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

❗ IMPORTANT

When new features with new permissions are added to Cumulocity, 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.

TO ASSIGN GLOBAL ROLES

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

❗ IMPORTANT

By default it is not possible to change roles of SSO users (created automatically during SSO login) as those would be overridden by dynamic access mapping. However this behaviour can be changed. For more information refer to [Custom template configuration](#).

To assign global roles from the user list

1. Click the **Global roles** column of a particular user to open a list of global roles.
2. Select or clear the respective checkboxes.
3. Click **Apply** to save your settings.

To assign global roles from the user page

1. Click on the row of the respective user in the user list.
2. In the user page, select or clear the checkboxes for the relevant global roles at the right.
3. Click **Save** to save your settings.

❗ IMPORTANT

Users who are logged in via OAI-Secure will be forced to log out of the platform after switching roles. Role

changes require confirmation by an administrator.

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 INVENTORY ROLES

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

The screenshot shows the 'Roles' management page with the 'Inventory roles' tab selected. The sidebar on the left contains the 'ADMINISTRATION' menu with options: Home, Accounts, Users, Roles (selected), Audit logs, Tenants, Ecosystem, Business rules, Management, Settings, Data broker, and Migration. The main content area is titled 'Roles' and shows the breadcrumb 'Accounts > Roles > Inventory roles'. It features a 'Global roles' and 'Inventory roles' tab, a 'Display as' dropdown set to 'Auto', and a search filter. Below these are four role cards: 'Asset Manager' (description: Can read all data of the asset and manage all inventory data, but cannot perform operations. Can also acknowledge and clear alarms. Can create and updates dashboards. permissions: 3), 'Operations: All' (description: Can remotely manage the assets by sending operations to the device. This includes remote configuration, software update and more. permissions: 1), 'Operations: Restart ...' (description: Can restart devices. permissions: 3), and 'Reader' (description: Can read all data of the asset. permissions: 1). The bottom of the sidebar indicates 'powered by CUMULOCITY'.

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 initially available in new tenants:

Role	Description
Manager	Can read all data of the asset and manage all inventory data but cannot perform operations. In addition, can manage inventory data (including dashboards) and alarms.
Operations: All	Can remotely manage the assets by sending operations to a device (for example software updates, remote configurations).
Operations: Restart Device	Can restart devices.
Reader	Can read all data of the asset.


TO ADD AN INVENTORY ROLE

Click **Add inventory role** in the **Inventory roles** tab. In the **New inventory role** dialog, provide a **name** and a **description**, and assign the **permissions** for the new inventory role.

The screenshot shows the 'New inventory role' dialog. The 'Inventory role' section contains a 'Name' field with the value 'New inventory role' and a 'Description' text area. The 'Permissions' section lists several categories: Alarms, Audits, Events, Inventory, and Measurements. Each category has a 'No permissions for this scope.' message and a green plus icon to add permissions. The 'Alarms' category is expanded, showing a 'Type' field with an asterisk, a 'Permission' dropdown set to 'Read', and red minus and green plus icons. At the bottom are 'Cancel' and 'Save' buttons. The left sidebar shows the 'ADMINISTRATION' menu with 'Roles' selected. The top right shows a user profile 'JD'.

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.

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

In the **Type** field, specify a fragment to further restrict the types of data that this permission applies to. Access will only be granted to objects that contain exactly the specified fragment types. If the selected object contains more fragment types than those defined in the inventory roles configuration, in order to display it, they also must be added to the inventory role configuration.

For example, assume that your device sends measurements related to device management, such as "c8y_SignalStrength" but the measurement itself also has "c8y_Temperature" which you are not interested in. For the selected device, there are also measurements containing only the "c8y_Temperature" fragment.

```

POST /measurement/measurements
...
{
  "source": { "id": "2480300" },
  "time": "2013-07-02T16:32:30.152+02:00",
  "type": "SignalStrength",
  "c8y_SignalStrength": {
    "rssi": { "value": -53, "unit": "dBm" },
    "ber": { "value": 0.14, "unit": "%" }
  },
  "c8y_Temperature": {
    "T": { "value": 10, "unit": "C" }
  }
}
POST /measurement/measurements
...
{
  "source": { "id": "2480300" },
  "time": "2013-07-02T16:32:30.152+02:00",
  "type": "SignalStrength",
  "c8y_Temperature": {
    "T": { "value": 10, "unit": "C" }
  }
}

```

You want a user to only see the device management measurements which have a fragment "c8y_SignalStrength".

In the default configuration for inventory roles we must provide access to all fragments that the measurement has, that is, "c8y_SignalStrength" and "c8y_Temperature".

Note that if a measurement also contains other fragment types, they must also be added in the inventory role configuration, and they are also returned in the response.

Otherwise such measurements are not returned because they contain fields to which the user has not been granted access.

The response looks like below:

```

GET /measurement/measurements
...
{
  "source": { "id": "2480300" },
  "time": "2013-07-02T16:32:30.152+02:00",
  "type": "SignalStrength",
  "c8y_SignalStrength": {
    "rssi": { "value": -53, "unit": "dBm" },
    "ber": { "value": 0.14, "unit": "%" }
  },
  "c8y_Temperature": {
    "T": { "value": 10, "unit": "C" }
  }
}

```

The tenant option `acl.measurement.only-accessible-fragments` in the category `configuration` can be used for measurements.

To enable it set the option value to "true" as below.

```
POST /tenant/options
...
{
  "category": "configuration",
  "key": "acl.measurement.only-accessible-fragments",
  "value": "true"
}
```

After setting the tenant option value to true, in order to have access to a single measurement fragment like "c8y_SignalStrength", you do not have to grant access to all fragments types that the measurement has.

For example, assume that your device sends measurements such as those in the previous example, including "c8y_SignalStrength" and "c8y_Temperature" and other measurements with "c8y_Temperature" only.

```
POST /measurement/measurements
...
{
  "source": { "id": "2480300" },
  "time": "2013-07-02T16:32:30.152+02:00",
  "type": "SignalStrength",
  "c8y_SignalStrength": {
    "rssi": { "value": -53, "unit": "dBm" },
    "ber": { "value": 0.14, "unit": "%" }
  },
  "c8y_Temperature": {
    "T": { "value": 10, "unit": "C" }
  }
}
POST /measurement/measurements
...
{
  "source": { "id": "2480300" },
  "time": "2013-07-02T16:32:30.152+02:00",
  "type": "SignalStrength",
  "c8y_Temperature": {
    "T": { "value": 10, "unit": "C" }
  }
}
}
```

HTTP/1.1 201 Created

You want a user to only see the device management measurements which have a fragment "c8y_SignalStrength". After changing the tenant option, we can specify only the types of fragments that interest us.

Measurements ?

Type	Permission
c8y_SignalStrength	Read
c8y_Temperature	

Device control ?

Note that only measurements that have a defined set of types are returned, and additional types not listed in the inventory role configuration are removed from the returned measurements.

The response looks like below:

```
GET /measurement/measurements
...
{
  "source": { "id": "2480300" },
  "time": "2013-07-02T16:32:30.152+02:00",
  "type": "SignalStrength",
  "c8y_SignalStrength": {
    "rssi": { "value": -53, "unit": "dBm" },
    "ber": { "value": 0.14, "unit": "%" }
  }
}
...
```

This allows the user to see measurements that contain only the defined types, without the additional need to configure other types of fragments that the measurement has.

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

INFO

For further information on possible types, check your device documentation or the [fragment library](#). The type being used here is the so-called "fragment type", not the "type" property. You must 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

IMPORTANT

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 [fragment library](#). To do so, assign READ permission on inventory as well as on events with type "c8y_Position" as shown in the image below.

The screenshot shows a user interface for configuring permissions. It consists of two main sections, each with a title and a search icon (a circle with a question mark).

- Events**: The 'Type' field contains 'c8y_Position'. The 'Permission' dropdown is set to 'Read'. To the right of the dropdown are three buttons: a green downward arrow, a red minus button, and a green plus button.
- Inventory**: The 'Type' field contains an asterisk '*'. The 'Permission' dropdown is set to 'Read'. To the right of the dropdown are three buttons: a green downward arrow, a red minus button, and a green plus button.

TO ASSIGN INVENTORY ROLES TO USERS

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

To assign inventory roles, click **Users** in the **Accounts** 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, open the dropdown at the right of the group row. Select the relevant roles and click **Apply**. For a detailed description of a role click the info icon next to it.

IMPORTANT

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

The **Application Access** tab shows a list of all available applications in your tenant in alphabetical order.

To assign applications to the user, simply select the respective applications and click **Save**.

For more information on application management, see [Managing applications](#).

INFO

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 (showing the current username) at the right of the top bar. From the context menu, select **Access denied requests**. In the resulting window details on the denied accesses are provided. An administrator user or the [product support](#) can help in fixing the permissions.

IMPROVING THE PERFORMANCE

The Cumulocity platform provides optimized UI performance for users with inventory roles access. In particular, requests for tenants with large inventory hierarchies are faster.

The performance of the following UI pages is improved:

- In the device details view, the tabs **Info, Measurements, Alarms, Events** and **Control**.
- Pages with aggregated alarm views from multiple devices, if the number of alarms in the system is low, for example, Cockpit > Home dashboard, Cockpit > Alarms and Device management & connectivity > Home.
- Pages with aggregated events from multiple devices, if the number of events is low, for example, Device management & connectivity > Events.
- Pages with aggregated operations from multiple devices, if the number of operations is low, for example, Device management & connectivity > Device control > Single operations.

As an administrator, you can disable the performance feature by doing the following:

- On platform level via the configuration file (only available for platform administrators, see the *Cumulocity - Operations guide* for details).
- On tenant level via a tenant option. The tenant option has 2 possible values: LEGACY/OPTIMIZED, where OPTIMIZED is the global default.

The option looks like the following in the REST API (see also the [Cumulocity OpenAPI Specification](#)):

```
{"category": "configuration", "key": "acl.algorithm-version", "value": "LEGACY"}
```

The setting on tenant level has priority over the setting on platform level.

By default, this option is enabled.

LIMITATIONS OF INVENTORY ROLES BASED ACCESS

The Cumulocity inventory roles based access has some limitations and may change the behavior of the REST API.

OPTIMIZED

The [optimized performance](#) can be applied only when:

- The total number of items matching the filters is lower than **2000**. For example, if you are searching only active alarms with a given type and the number of such alarms is below 2000.
- You are fetching measurements, alarms, events, and control for a specific device.

In all other cases Cumulocity will apply the legacy search algorithm.

LEGACY

The legacy algorithm provides the following implications for the REST API:

- The `currentPage` query parameter will act as offset of scanned documents.
- The REST API may return empty pages. Cumulocity searches the items that are accessible for the user but the scan has a limit per request. If there is no accessible element in the scanned items, the platform will result an empty list. In such case, the `statistics.next` URL should be used to perform a scan of the next chunk. Cumulocity will return `statistics.next` until there are items to scan.

MANAGING THE ECOSYSTEM

The Cumulocity platform distinguishes between applications and microservices:

- [Applications](#) - all web applications either subscribed to the tenant or owned by the tenant.
- [Microservices](#) - server-side applications used to develop further functionality on top of Cumulocity.

Both can be accessed via the **Ecosystem** menu in the navigator.

Additionally, in Enterprise tenants, it is possible to configure **Default subscriptions**, that means you can specify a list of applications that are subscribed by default to every new tenant on creation and/or to all existing tenants on platform upgrade. For details, see [Default subscriptions](#).

✓ REQUIREMENTS

ROLES & PERMISSIONS:

- To view applications and microservices: READ permission for the “Application management” permission type
- To manage applications and microservices (create, update, copy, delete): ADMIN permission for the “Application management” permission type

On tenant creation there are default roles available that can be used as sample configuration for the above mentioned permissions:

- Tenant Manager - manages tenant-wide configurations like applications, tenant options and business rules.

Note that for complete application management some additional permission types with different permission levels might be required per feature, for example:

- [Default subscriptions](#) for the Enterprise tenant additionally requires READ and ADMIN permissions for the “Option management” permission type.
- [Subscribing applications](#) for the Enterprise tenant additionally requires READ and ADMIN permissions for the “Tenant management” permission type.

i RELATED TOPICS

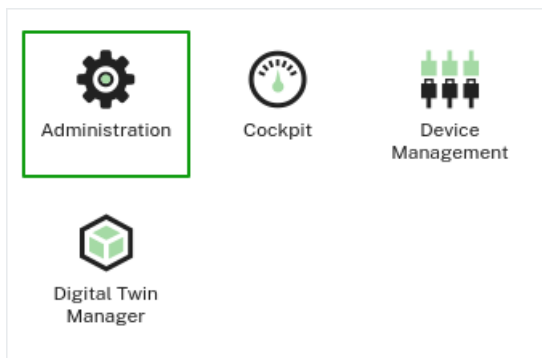
- [Platform administration > Standard tenant administration > Managing permissions](#) for details on assigning roles and permissions for the usage of Cumulocity applications.
- [Platform administration > Standard tenant administration > Changing settings > Application](#) for information on changing the application settings for your account.
- [Platform administration > Enterprise tenant administration > Managing tenants > Subscribing applications](#) for information on application subscriptions on tenant level.
- [Application enablement & solutions > Introduction > Application enablement](#) for an overview on the basic concepts of applications in Cumulocity.
- [Application enablement & solutions > Web SDK](#) for information on how to develop web applications on top of Cumulocity and how to [customize](#) existing applications.
- Refer to the [Cumulocity Tech Community](#) for a tutorial on how to extend an existing application using the Web SDK.
- [Application enablement & solutions > Microservice SDK](#) for general aspects of using microservices on top of Cumulocity and information on developing and deploying microservices using our SDKs or the REST interface.
- [Applications](#) in the Cumulocity OpenAPI Specification for managing applications via REST.

MANAGING APPLICATIONS

There are two types of availability for applications:

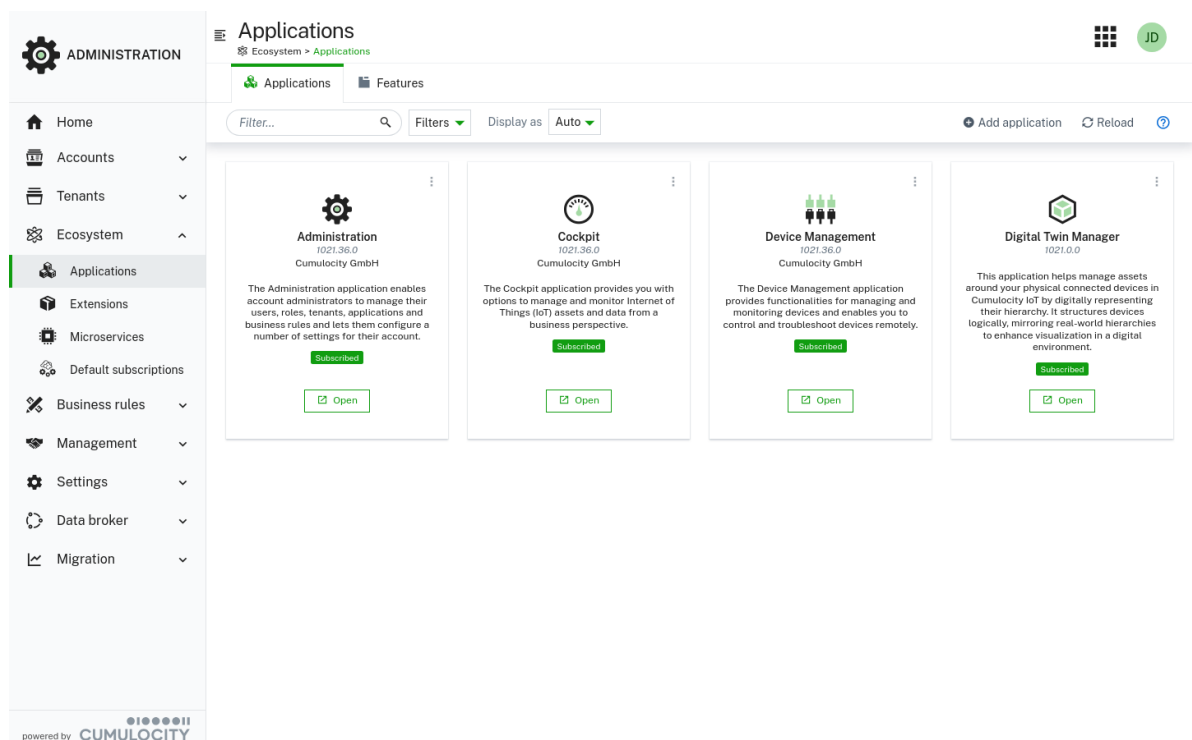
- **Subscribed** - applications subscribed to the tenant, either provided by the platform (as default applications) or by a service provider.
- **Custom** - applications owned by the tenant. You can [add custom applications](#) in various ways as own applications.

Your applications are available through the application switcher in the top bar.



TO VIEW APPLICATIONS

Click **Applications** in the **Ecosystem** menu in the navigator to display a list or grid of all applications in your account.



In the **Applications** tab, you can see all applications available in your tenant.

Applications can be filtered by name or by availability.

TO EDIT AN APPLICATION


Click the application or click the menu icon  at the right of an entry and then click **Edit**.

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

IMPORTANT

Never change the system application names (such as “Device Management”, “Cockpit”). Otherwise, tenant initialization will fail.

TO DELETE AN APPLICATION

Click the menu icon  at the right of an entry and then click **Delete**. You can also delete an application directly from the **Properties** tab in the application details.

If you delete 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 delete subscribed applications. This can only be done by the owner of the subscribed application.

FEATURES

Features are applications which are built-in and not represented by an explicit artifact (like microservices or web applications).

In the **Features** tab, you will find a list of all features subscribed in your tenant. In an Enterprise tenant, the following features are available by default:

Name in the UI	Functionality	Identification in the API	Availability
Feature-branding	Customize the look of your tenants to your own preferences	feature-branding	Enterprise tenant
Feature-broker	Share data selectively with other tenants	feature-broker	Enterprise tenant
Feature-user-hierarchy	Reflect independent organizational entities in Cumulocity that share the same database	feature-user-hierarchy	Enterprise tenant

INFO

All applications listed here are of the type “Feature”.

Other features may show up, depending on the individual subscriptions of your tenant.

SUBSCRIBED APPLICATIONS

Cumulocity provides a variety of applications for different purposes. Depending on your installation and/or optional services your tenant will show a selection of the potentially available applications.

INFO

In the **Applications** tab, subscribed applications are labeled as “Subscribed”. Subscribed applications may not be added, modified or removed by the user but only by a tenant administrator.

Below all applications are listed which are by default available in the Standard tenant or Enterprise tenant. In addition, numerous optional applications might be subscribed to your tenant.

APPLICATIONS SUBSCRIBED BY DEFAULT

Name in the UI	Functionality	Identification in the API	Technical type	Availability
Administration	Lets account administrators manage users, roles, tenants and applications	administration	Web application	Standard tenant, Enterprise tenant
Cockpit	Manage and monitor IoT assets and data from a business perspective	cockpit	Web application	Standard tenant, Enterprise tenant
Device Management	Manage and monitor devices, and control and troubleshoot devices remotely	devicemanagement	Web application	Standard tenant, Enterprise tenant
Streaming Analytics	Manage and edit Analytics Builder models and EPL apps (if enabled)	Streaming Analytics	Web application	Standard tenant (limited version for Analytics Builder), Enterprise tenant (full version)
Digital Twin Manager	Create and manage basic building blocks for Digital twins: Assets, Asset models and Asset properties	digital-twin-manager	Web application	Standard tenant, Enterprise tenant
Time Series Migration	The application facilitates the migration of tenant data from legacy measurements to the new time series storage	timeseries-migration	Microservice	Standard tenant, Enterprise tenant

CUSTOM APPLICATIONS

Custom applications may be:

- Web-based UI applications, either deployed as standalone applications or as plugins deployed into a specific application (for example, a widget to the Cockpit dashboard).
- Links to an application running elsewhere.
- Duplicates of subscribed applications (in order to be able to customize them).

INFO

In the **Applications** tab, custom applications are labeled as “Custom”.

Click **Add application** at the top right of the **Applications** tab to add a custom application.

In the resulting dialog box, select one of the following methods:

- [Upload web application](#) - drop a ZIP file or browse for it in your file system.
- [External application](#) - link to an application running elsewhere.
- [Install from available packages](#) - select a package blueprint.
- [Duplicate existing application](#) - create a copy of an existing application.

TO UPLOAD A WEB APPLICATION

1. Click **Add application** at the top right of the **Applications** tab.
2. Select **Upload web application**.
3. In the resulting dialog box, drop a ZIP file or browse for it in your file system.

The application is created once the ZIP file has been successfully uploaded.

IMPORTANT

The ZIP file must contain the *index.html* and *cumulocity.json* in its root directory, otherwise the application will not work.

TO LINK TO AN EXTERNAL APPLICATION

1. Click **Add application** at the top right of the **Applications** tab.
2. Select **External application**.
3. In the resulting dialog box, 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. Click **Save** to create the application.

For details on the fields, see also [Application properties](#) below.

TO INSTALL AN APPLICATION FROM A BLUEPRINT

1. Click **Add application** at the top right of the **Applications** tab.
2. Select **Install from available packages**.
3. Select the desired package.
4. In the resulting dialog box, enter the name of the application. The name will be shown as title of the application.
5. Enter an application key, used to identify this application.
6. Enter the path where the application can be reached.
7. Click **Save** to create the application.

For details on the fields, see also [Application properties](#) below.

TO DUPLICATE AN APPLICATION

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.

1. Click **Add application** at the top right of the **Applications** tab.
2. In the upcoming dialog, select **Duplicate existing application**.
3. Select the desired application from the dropdown list, for example "Cockpit".
4. In the next window, provide a name for the application, an application key to identify the application, and a path as part of the URL to invoke the application. Finally select an icon for the new application from the available icons. Per default, the values of the original application are provided, extended by a number. If you set the path to the path of the original subscribed application, your own application will overrule the subscribed application.

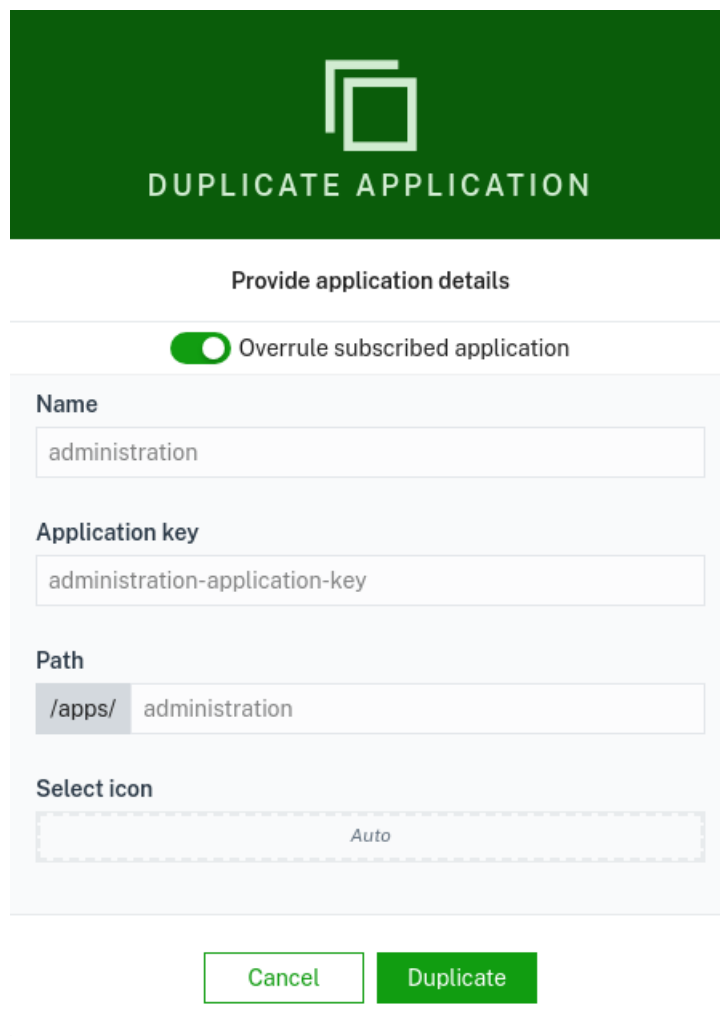
INFO

The platform restricts the use of the prefix “feature-” in the **Name** field. You cannot create applications using this prefix in the application name. This also applies to existing applications in cases where the duplicate application feature is used.

5. Finally, click **Duplicate** to create the application.

i INFO

In case the application has been subscribed to the tenant, there is an additional toggle **Override subscribed application**. If you turn this toggle on, the values for name, key and path will be inherited from the original application and your duplicated application will overrule the subscribed application. Turn it off, to modify the values.



The image shows a 'Duplicate Application' dialog box. At the top is a green header with a white icon of two overlapping squares and the text 'DUPLICATE APPLICATION'. Below the header is a section titled 'Provide application details'. Inside this section is a toggle switch labeled 'Override subscribed application', which is currently turned on (green). Below the toggle are four input fields: 'Name' with the value 'administration', 'Application key' with the value 'administration-application-key', 'Path' with a dropdown menu showing '/apps/' and a text field with 'administration', and 'Select icon' with a dashed box containing the word 'Auto'. At the bottom of the dialog are two buttons: 'Cancel' (white with a green border) and 'Duplicate' (solid green).

For details on the fields, see also [Application properties](#) below.

APPLICATION PROPERTIES

To display further details on an application, click it to open its **Properties** tab.



Administration

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.

[Custom](#)

 VERSION: **1021.36.0**

CREATION TIME: ---

[Open](#)
ID

3

Name

administration

Application key

administration-application-key

Type

HOSTED

Path

/apps/ administration

Select icon

Auto

[Cancel](#)
[Delete](#)
[Save](#)

In the **Properties** tab, each application will show the following information, depending on the application type (hosted or external):

Field	Description	Hosted (web application)	External
ID	Unique ID to identify the application	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	Specified by the user
Application key	Used to identify the application and to make it available for subscription	Automatically created	Specified by the user
Type	Application type	Hosted	External
Path	Part of the URL invoking the application	Automatically created	Specified by the user; for example, if you use "hello" as application path, the URL of the application will be "/apps/hello"

Field	Description	Hosted (web application)	External
Select icon	Provides a variety of icons from which an icon for the application can be selected.	Automatically created	Specified by the user

INFO

The icon selector is only available for custom application.

EXTENSIONS

EXTENSIONS

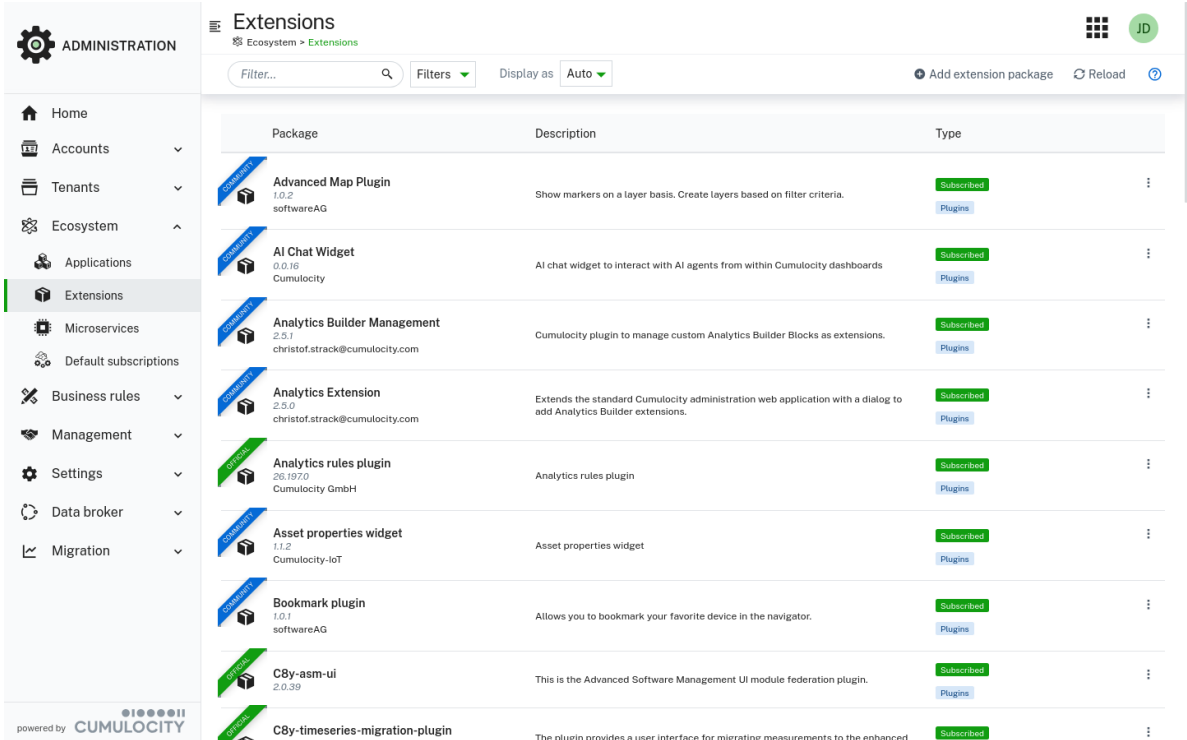
Extension packages are combinations of plugins and blueprints which can be packed together into a single file and then be deployed to the platform. Thus, they offer better shareability and reusability of UI features across different applications and allow to add UI features to applications without coding knowledge.

Extension packages can contain two types of content:

- **Plugins** can be used to extend existing applications without the need of re-building the application.
- **Blueprints** are combinations of multiple UI functionalities which can be hosted by the platform and can be used to create a new application from scratch.

Blueprint applications must be deployed, while plugins are added to other applications. This allows you to scaffold entire solutions or to extend existing ones. Due to the micro frontend technology, this can happen at runtime without rebuilding.

Packages can be located on the **Extensions** page.



The screenshot shows the 'Extensions' page in the Cumulocity interface. On the left is a sidebar with navigation options: ADMINISTRATION, Home, Accounts, Tenants, Ecosystem, Applications, Extensions (selected), Microservices, Default subscriptions, Business rules, Management, Settings, Data broker, and Migration. The main content area is titled 'Extensions' and includes a search bar, filters, and a 'Display as' dropdown set to 'Auto'. Below this is a table of extension packages:

Package	Description	Type
Advanced Map Plugin 1.0.2 softwareAG	Show markers on a layer basis. Create layers based on filter criteria.	Subscribed Plugins
AI Chat Widget 0.0.16 Cumulocity	AI chat widget to interact with AI agents from within Cumulocity dashboards	Subscribed Plugins
Analytics Builder Management 2.5.1 christof.strack@cumulocity.com	Cumulocity plugin to manage custom Analytics Builder Blocks as extensions.	Subscribed Plugins
Analytics Extension 2.5.0 christof.strack@cumulocity.com	Extends the standard Cumulocity administration web application with a dialog to add Analytics Builder extensions.	Subscribed Plugins
Analytics rules plugin 26.197.0 Cumulocity GmbH	Analytics rules plugin	Subscribed Plugins
Asset properties widget 1.1.2 Cumulocity-IoT	Asset properties widget	Subscribed Plugins
Bookmark plugin 1.0.1 softwareAG	Allows you to bookmark your favorite device in the navigator.	Subscribed Plugins
C8y-asm-ui 2.0.39	This is the Advanced Software Management UI module federation plugin.	Subscribed Plugins
C8y-timeseries-migration-plugin	The plugin provides a user interface for migrating measurements to the enhanced	Subscribed

Packages can be filtered by name, creator type, availability and type of content.

To add a new extension package, click **Add extension package** at the top right. Like for applications, the availability of extension packages can either be **subscribed** or **custom**. While **subscribed** extensions are mostly shared from the management tenant, **custom** ones are private to the current tenant. On upload, the availability of the extension can be selected:

- **PRIVATE:** This extension package is only available on the current tenant.
- **MARKET:** Allows to create a subscription model for the extension. Only the current tenant and tenants to which the extension is subscribed can use the extension.
- **SHARED:** Every subtenant and the current tenant can install the extension.

In general, you provide an extension as **SHARED** to make it available across the tenant hierarchy. However, it is important to “scope” such applications, that is, prefix the application name, context path, and key with a company shortcode. For example, Cumulocity packages are always prefixed with **c8y-** as Cumulocity might automatically deploy an extension, which will fail if you upload your own package to the management tenant.

By clicking on a package, you can see the package details such as **Extension package overview** which includes a description and images as well as some meta information which is taken from the *package.json*.

Additionally, it is possible to view all available plugins within the selected package at the right. To install a plugin click **Install plugin** and select the desired application.

The screenshot displays the Cumulocity community plugins interface. On the left, the 'ADMINISTRATION' sidebar is visible with 'Extensions' selected. The main content area shows the 'Cumulocity community plugins' package details, including its author (Cumulocity-IoT), license (Apache-2.0), and latest version (3.6.0). The 'Extension package overview' section describes the package and lists compatible Cumulocity UI app versions. Below this, a 'DATA POINTS GRAPH' visualization is shown. On the right, the 'Package plugins' section lists four plugins: 'Example widget plugin', 'Data points graph', 'Advanced simulator', and 'Application builder dashboard migration', each with 'Uninstall plugin' and 'Install plugin' buttons.

In the **Versions** tab, you see all previously uploaded binaries related to the current package. The binaries displayed on this tab can be downloaded via the context menu next to each package version entry.

Cumulocity community plugins

Ecosystem > Extensions > Cumulocity community p... > Versions

Extension package Versions Change log

Versions

Version	Tag
VERSION 3.7.0	latest
VERSION 3.6.0	
VERSION 3.5.0	
VERSION 3.4.0	
VERSION 3.2.2	
VERSION 3.1.0	
VERSION 3.0.1	
VERSION 2.1.6	

Version 3.7.0 package contents

Author: Cumulocity GmbH
Homepage: --
Keywords: --
License: Apache 2.0
Source: --
Latest version: 3.7.0

APPLICATION

Cumulocity community plugins
This is a set of plugins developed and maintained by the community.

PLUGINS

- Example widget plugin**
Adds a custom widget to the shell application.
COMMUNITY
- Data points graph**
Adds data points graph widget to the shell application.
COMMUNITY
- Advanced simulator**
Allows to generate simulators with the help of AI.
COMMUNITY
- Application builder dashboard migration**
Allows to migrate dashboards generated via application builder to be migrated into cockpit reports.
COMMUNITY

powered by CUMULOCITY

You can select or upload different versions. Versions indicate the state of the package. They can be used to verify whether a certain package is outdated and must be updated. By clicking on a version additional information is provided such as package contents, applications or plugins. Tags can be used to give versions meaningful names. The “latest” tag is used to indicate the default version which will be selected in case no tag is provided. The “latest” tag is set by default to the latest version whenever a version is uploaded without a given tag.

To switch to a different version open the context menu for the desired version and click **Set as latest**. To delete a version click **Delete**.

PLUGINS

Switch to the **Plugins** tab of an application to view all plugins installed on an application.

Administration

Ecosystem > Applications > Administration > Plugins

Properties Plugins

Install plugins Reset to default

Installed plugins 6 of 6 items No filters

Configure columns Reload Search...

Plugin name	Version	Tag	Description	Source	Status
<input type="checkbox"/> Branding base editor	1021.52.0		Allows to make basic changes to the tenants branding.	administration	LATEST
<input type="checkbox"/> Branding dark theme editor	1021.52.0		Allows editing the dark theme variables.	administration	LATEST
<input type="checkbox"/> Branding custom CSS editor	1021.52.0		Allows to add and edit a custom style sheet to the branding.	administration	LATEST
<input type="checkbox"/> Branding JSON editor	1021.52.0		Allows to edit the plain JSON of the branding.	administration	LATEST
<input type="checkbox"/> Translation editor	1021.52.0		Allows to edit translations.	administration	LATEST
<input type="checkbox"/> Timeseries migration module	1.0.326	1021-stable	Provides interface for performing timeseries migration	c8y-timeseries-migration-plugin	AUTO

1-6 of 6

powered by CUMULOCITY

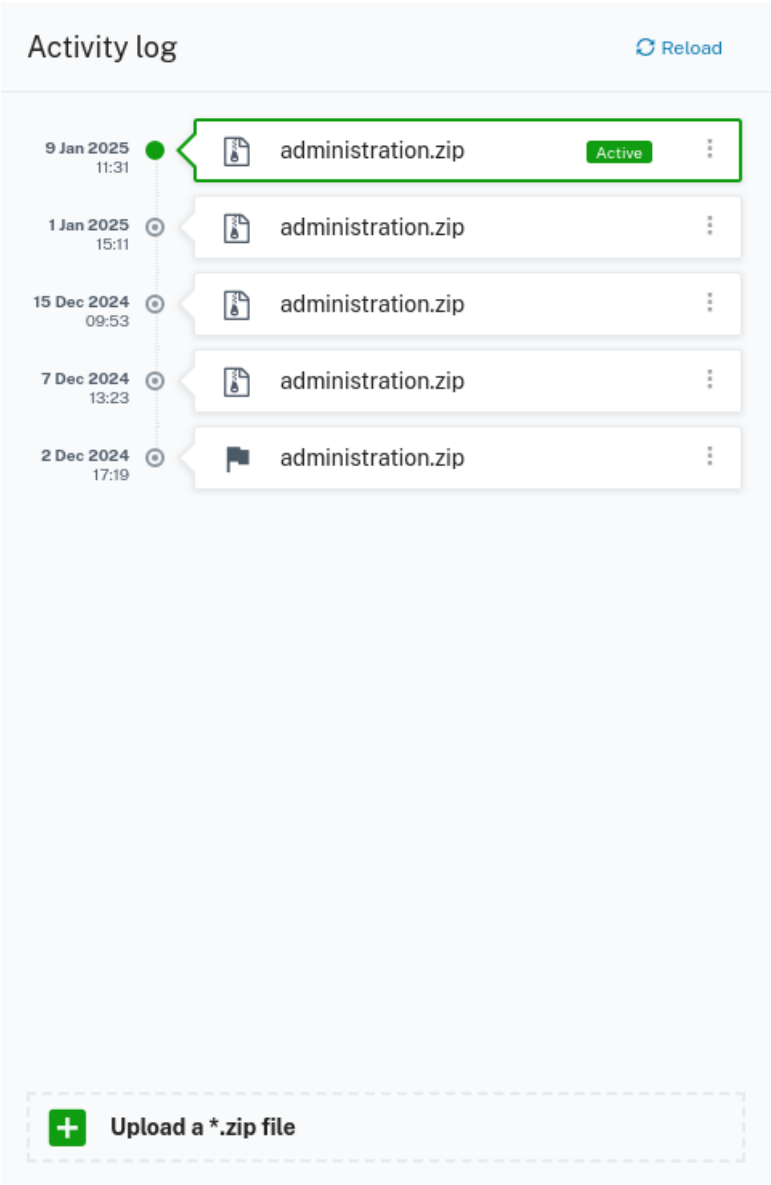
In the **Plugins** tab you can add and remove plugins. Additionally, you can install plugins to an application.

UPLOADING ARCHIVES

For custom applications, multiple file versions can be stored in Cumulocity 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

1. Open the application properties for the respective application by clicking on it.
2. Click the plus button at the bottom of the **Activity log** section and browse for the archive in your file system or simply drop the archive file.
3. Click **Upload** to upload the archive to your Cumulocity account.




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

INFO

The archive functionality is not available for subscribed applications, as only the owner of the application can perform these actions.


TO RESTORE AN OLDER APPLICATION VERSION

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

1. Open the application properties for the respective application by clicking on it.
2. In the **Activity log** section, open the context menu for the desired version by clicking the menu icon  and select **Set as active** to make it the active version.

TO REACTIVATE A SINGLE APPLICATION


If a hosted application is not deployed correctly, users may reactivate it.














1. Open the application properties for the respective application by clicking on it.
2. In the **Activity log** section, open the context menu for the desired version by clicking the menu icon  and select **Reactivate archive**.


The selected application will be reactivated by removing the respective files from the application directory and unpacking the web application package again.


MANAGING MICROSERVICES























Click **Microservices** in the **Ecosystem** menu in the navigator to display a list or grid of all microservices subscribed to your account.



ADMINISTRATION

 Home
  Accounts
  Tenants
  Ecosystem
  Applications
  Extensions
  **Microservices**
 Default subscriptions
  Business rules
  Management
  Settings
  Data broker
  Migration


Microservices

 Ecosystem > **Microservices**

Microservice	Description	Type
 Activity	No description available.	 Subscribed
 Advanced-software-mgmt 2.0.6	No description available.	 Subscribed
 Apama-ctrl-smartrulesmt 26.33.0	The multi-tenant Streaming Analytics microservice lets you use smart rules for real-time analytics.	 Subscribed
 Cloud-remote-access 2.0.4	No description available.	 Subscribed
 Connectivity-agent-server 1.12.0	No description available.	 Subscribed
 Databroker-agent-server 2025.50.0	No description available.	 Subscribed
 Device-simulator 2.0.2	No description available.	 Subscribed
 Dtm 1021.0.0	No description available.	 Subscribed
 Loriot-agent 3.0.4	No description available.	 Subscribed
 Lwm2m-agent	No description available.	 Subscribed
 Opcua-mgmt-service	No description available.	 Subscribed

powered by  **CUMULOCITY**

Microservices can be filtered by name and availability.

A microservice is a specific type of application, that is a server-side application used to develop further functionality on top of Cumulocity. As web applications, microservices can either be subscribed to your tenant by the platform or by a service provider, or they can be owned by you as custom applications. see [Custom microservices](#).

SUBSCRIBED MICROSERVICES

Cumulocity provides a variety of microservice applications for different purposes. Depending on your installation and/or optional services your tenant will show a selection of the potentially available applications.

Below you find a list of all microservices which are by default subscribed in a Standard tenant and/or Enterprise tenant. In addition,

numerous optional microservices might be subscribed to your tenant.

Microservices subscribed by default

Name in the UI	Functionality	Identification in the API	Availability
Apama-ctrl-*	Streaming Analytics microservices, including runtime for Analytics Builder, EPL apps and smart rules. Capabilities and resources vary depending on the microservice variant used	apama-ctrl-*	Standard tenant, Enterprise tenant
Device-simulator	Simulate all aspects of IoT devices	device-simulator	Standard tenant, Enterprise tenant
Report agent	Schedule data exports from within the Cockpit application	report agent	Standard tenant, Enterprise tenant
Smartrule	Use the smart rules engine and create smart rules to perform actions based on realtime data. Requires a variant of the Apama-ctrl microservice	smartrule	Standard tenant, Enterprise tenant
Sslmanagement	Activate your own custom domain name by using an SSL certificate	sslmanagement	Enterprise tenant

INFO

All applications listed here are of the type "Microservice".

CUSTOM MICROSERVICES

To add a microservice as custom application

1. Click **Add microservice** at the top right.
2. In the resulting dialog box, drop a ZIP file or browse for it in your file system. Note that the size limit of the file to be uploaded is 500 MB.
3. The microservice application is created once the ZIP file has been successfully uploaded.

IMPORTANT

The ZIP file must contain the application manifest and the Docker image of the microservice. Refer to [General aspects](#) for information on preparing and deploying the microservice package. You can provide the name of the microservice in its manifest file. If no name is provided in the file, the platform will derive it from the ZIP file name by removing the recognized version suffix. In any case the length of the resulting name must not exceed 23 characters.

MICROSERVICE PROPERTIES

To display further details on a microservice, click it to open its **Properties** tab.

In the **Properties** tab, each microservice will show the following information:

Field	Description	Comment
ID	Unique ID to identify the microservice	Automatically provided
Name	Application name; will be shown as title of the microservice application in the top bar	Automatically inferred from the ZIP file name (recognized version number is dropped), unless provided in the microservice's manifest file
Application key	Used to identify the microservice application and to make it available for subscription	Automatically created, based on the ZIP file name
Type	Application type	Microservice
Path	Part of the URL invoking the application	Automatically created as <code>/service/<microservice-name></code>

Below, you will additionally find information on the microservice version, as well as on its isolation level and billing mode, see [Microservice usage](#) for details on these parameters.

Microservice subscription

At the top right of the **Properties** tab, you find a toggle to subscribe to or unsubscribe from a microservice.

Changing the subscription is only possible for custom microservices, that is microservices being owned by you.

MICROSERVICE PERMISSIONS

In the **Permissions** tab you can view the permissions required for the respective microservice, and the roles provided for it.

MONITORING MICROSERVICES

You can monitor microservices hosted by Cumulocity in two ways.

STATUS INFORMATION

The status of the microservice can be checked in the **Status** tab of the respective microservice application.

The screenshot displays the Cumulocity Administration interface. On the left is a sidebar with navigation links: Home, Accounts, Tenants, Ecosystem, Applications, Extensions, Microservices (highlighted), Default subscriptions, Business rules, Management, Settings, Data broker, and Migration. The main area shows the 'Status' tab for a microservice. It includes a breadcrumb trail: Ecosystem > Microservices > Report-agent > Status. Below this are tabs for Properties, Logs, Permissions, and Status (active). The Status tab contains several sections: 'Instances' with a table showing 0 Active, 0 Unhealthy, and 0 Desired instances; 'Subscriptions' with a table showing 1 subscription for tenant t123456 with 0 Active, 0 Unhealthy, and 0 Desired instances; 'Events' showing 'No events to display'; 'Alarms' showing 'No alarms to display'; and 'Smart rules' showing three rules: 'Calculates energy consumption', 'Creates alarm when measurements are missing', and 'Executes an operation when alarm is'.

To view the status you need the following permissions: READ permission for “Application management” and “Inventory”.

The following information is provided on the **Status** tab:

- Instances - number of active, unhealthy and desired microservice instances for the current tenant.
- Subscriptions - number of active, unhealthy and desired microservice instances for all subtenants subscribed to the microservice.
- Alarms - alarms for given application, provided in realtime.
- Events - events for given application, provided in realtime.
- Smart rules - list of applicable smart rules.

Alarms and events

Most of the alarms and events visible in the **Status** tab are strictly technical descriptions of what's going on with the microservice.

There are two user-friendly alarm types:

- **c8y_Application_Down** - critical alarm which is created when no microservice instance is available.
- **c8y_Application_Unhealthy** - major alarm which is created when there is at least one microservice instance working properly, but not all of them are fully operating.

User-friendly alarms are created for the microservice owner tenant only. They are also automatically cleared when the situation gets back to normal, that is all the microservice instances are working properly.

User-friendly alarms can be used to create smart rules. For details on creating smart rules of various types, see [Smart rules](#).

For example, to send an email, if a microservice is down, create an “On alarm send email” smart rule.

In the **On alarm matching** section, use **c8y_Application_Down** as an alarm type. As a target asset select the microservice which you would like to monitor, for example “echo-agent-server”.

LOG FILES

Cumulocity offers viewing logs which provide more details on the status of microservices owned by the tenant.

To view logs, open the **Logs** tab of the respective microservice.

At the top of the page, you can select the instance of the microservice, for which you want to view the logs.

INFO

If your microservice was re-scaled into two instances you should be able to switch between them, but it is not possible to see the logs from both instances at once.

Next to the instance dropdown you can select the time range for the log entries to be shown by selecting a date from the calendar and entering a time.

INFO

The time entered here may differ from the server time due to different time zones.

At the top right, additional functionality is provided:



- **Download** - to download the log data for a specified time range.
- **Dark theme** - to turn dark theme on or off.
- **Auto refresh** - to activate the auto refresh functionality. If activated, the displayed log data will automatically be refreshed every 10 seconds.

Initially, the **Logs** tab shows the latest logs of the microservice instance.

At the bottom right you find navigation buttons:

- **First** - directly navigates to the oldest available log entries for the microservice after its restart (maximum capacity 35 MB of logs).
- **Previous** - increases the time range in 10 minutes steps.
- **Next** - reduces the time range in 10 minutes steps.
- **Last** - directly navigates to the latest available log entries.

If no logs are available in the selected time range, a message is shown accordingly:

 **No logs available from 1 June 2022, 00:00:00, instead loaded closest logs from 4 June 2022, 00:51:49.** 

INFO

There is no possibility to see the logs from the previously running instances or from previously rotated logs exceeding 35 MB. However, inside the instance there is a Docker container running, and if only this one was restarted (not the whole instance) you should see the logs from the currently running and also lately terminated Docker container.

Logs are always loaded from the Docker container using both `stdout` and `stderr` sources, and there is no possibility to distinguish/filter by the source.

MONITORING

Monitoring covers operational health and user activity tracking. This helps administrators to proactively manage the system, ensure stability, maintain security, and diagnose issues efficiently across different components.

AUDIT LOGS

Audit logs show security-relevant operations a user has processed. For example, an audit log is generated when a user logs into a gateway.

✔ REQUIREMENTS

ROLES & PERMISSIONS:

- To view audit logs: READ permission for permission type "Audit"
- To create audit logs you need Admin permission for the permission type "Audit". Note however, that you cannot create audit logs from the UI. For details on how to create audit logs via REST refer to [Audits](#) in the Cumulocity OpenAPI Specification.

ℹ RELATED TOPICS

- [Getting started > Technical concepts > Security aspects > Management security](#) for general aspects of audit logging.
- [Audits](#) in the Cumulocity OpenAPI Specification for details on managing audit records via REST.

TO VIEW AUDIT LOGS

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

Column	Description
Server time	Server time when the operation was processed.
Event	Type of operation, for example "Alarm created", "Smart rule deleted". Below it, the user who processed it is displayed.
Description	Provides further information depending on the operation, for example, 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. Scroll down the page to **Load more** to view more log entries.

ADMINISTRATION

Home

Accounts

Users

Roles

Audit logs

Tenants

Ecosystem

Business rules

Management

Settings

Data broker

Migration

Audit logs

Accounts > Audit logs

All typesDate fromDate toWhoApply filters

Reload

Device time	Event	Description
Jan 28, 2025, 9:49:40 AM	User login	"john.doe@example.com" user logged in to the platform with OAI-Secure login mode
Jan 27, 2025, 4:37:58 PM	Application subscribed	Application "administration" subscribed
Jan 26, 2025, 3:40:32 PM	Inventory Role created	Inventory Role Elevated reader created
Jan 25, 2025, 3:45:31 PM	Tenant activated.	Tenant "t123456" activated.
Jan 24, 2025, 1:45:16 PM	Tenant suspended	Tenant "t123456" suspended.

powered by CUMULOCITY


INFO

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.

TO FILTER LOGS

In order to easily search through logs, you can filter logs by:

- Type (alarm, operation, smart rule, and so on)
- Device time (provide a date range in "From" and/or "To" inputs)
- User

To apply a filter, click the **Apply** button next to the respective filter field. To discard filters, click the clear icon  next to the **Apply** button (only visible if filters are set).

AUDIT LOG TYPES

Audit type	Actions
Alarm	<ul style="list-style-type: none">• Alarm created• Alarm updated

Audit type	Actions
Application	<ul style="list-style-type: none"> • Application activated • Application subscribed • Application unsubscribed • Application deployed • Application deployment failure • Application undeployed • Application rescaled • Application deleted <p>This type of audit logs may be created for both hosted applications and microservices.</p>
Bulk operation	<ul style="list-style-type: none"> • Bulk operation created • Bulk operation updated • Bulk operation deleted
Data broker connector	<ul style="list-style-type: none"> • Connector created • Connector updated • Connector deleted
Devices availability monitoring	<ul style="list-style-type: none"> • Device availability enabled • Device availability disabled • Device availability interval updated • Device put into maintenance state
Global role	<ul style="list-style-type: none"> • Global role updated • Global role authorities updated • Global role device permissions updated
Inventory	<ul style="list-style-type: none"> • Managed object deleted • Device registration failed due to missing token • Device registration failed due to invalid token • Device registration max number of failed attempts reached
Inventory role	<ul style="list-style-type: none"> • Inventory role created • Inventory role updated • Inventory role deleted
Operation	<ul style="list-style-type: none"> • Operation created • Operation updated
Option	<ul style="list-style-type: none"> • Option created • Option updated • Option deleted
Reliable notification	<ul style="list-style-type: none"> • Reliable notification token created • Reliable notification subscription created • Reliable notification subscription deleted
Report	<ul style="list-style-type: none"> • Test tenant statistics accessed • Real tenant statistics accessed

Audit type	Actions
Single sign-on	<ul style="list-style-type: none"> • SSO login • SSO logout • SSO logout failed
Smart rule	<ul style="list-style-type: none"> • Smart rule created • Smart rule updated • Smart rule enabled • Smart rule disabled • Smart rule deleted
Tenant	<ul style="list-style-type: none"> • Tenant created • Tenant updated • Tenant suspended • Tenant activated • Tenant deleted
Tenant auth configuration	<ul style="list-style-type: none"> • Authentication configuration added • Authentication configuration updated • Authentication configuration deleted
Trusted certificate	<ul style="list-style-type: none"> • Trusted certificate uploaded • Trusted certificate updated • Trusted certificate deleted
Tenant Certificate Authority	<ul style="list-style-type: none"> • Tenant certificate authority(CA) created • Tenant certificate authority(CA) renewed • Tenant certificate authority(CA) renewal failed • Tenant certificate authority(CA) signed certificate
User	<ul style="list-style-type: none"> • User created • User updated • User username updated • User password updated • User roles updated • User groups updated • User delegation updated • User owner updated • User inventory assignment updated • User device permissions updated • User deleted • User device provisioned certificate created • User device provisioned certificate deleted
User login	<ul style="list-style-type: none"> • User login • User logout

Note that entries of this type are not created when using Basic authentication.

INFO

See also [Audit logs for Streaming Analytics](#) and [Audit logs for Cumulocity DataHub](#).

MESSAGING SERVICE

FEATURE PREVIEW

This feature is in **Public Preview** status, that is, it is not enabled by default and may be subject to change in the future.

The feature can be enabled for your tenant using the **Manage preview features** option in the right drawer in the **Administration** application.

The messaging-management microservice must be subscribed to your tenant. This should happen automatically, but if the feature is not accessible after enabling it in **Manage preview features**, verify the microservice subscription. To do this, open the Administration application and navigate to **Ecosystem > Microservices**. If you do not see the messaging-management microservice listed, contact [product support](#) to request the subscription for your tenant.

REQUIREMENTS

ROLES & PERMISSIONS:

- To view Messaging Service data: READ permission for permission type "Tenant statistics"
- To perform any action on a topic or subscriber: ADMIN permission for permission type "Tenant management"

The **Messaging Service** is a [publish/subscribe messaging](#) and message streaming component embedded in the Cumulocity platform. It provides asynchronous communication between platform components and user-facing features for moving real-time data into and out of the platform. The features that use the Messaging Service include the microservice-based data broker, Notifications 2.0, and the MQTT Service.

Topics are the core concept underlying all of the features using the Messaging Service. A topic is a logical channel for delivering messages from publishers to subscribers. Each topic may have any number of publishers and subscribers, and in general, every subscriber to a topic receives the messages sent by every publisher to that topic. All subscribers of a topic receive the published messages in the same order. The topic persistently stores published messages until every subscriber has acknowledged that they have successfully received them. This means that the Messaging Service can guarantee the delivery of every published message to every subscriber.

The following sections show how to monitor your tenant's usage of the Messaging Service for each of the services that use it.

TO VIEW THE TOPICS

Click **Messaging Service** in the **Monitoring** menu in the navigator to display a list of all features that use the Messaging Service. Next to the feature name, you see basic information on the feature's usage of the Messaging Service, such as the number of topics, publishers, and subscribers. Select a feature and click it to see the details. This displays a list of all topics used by the feature and the limits that are applied for each of these topics.

ADMINISTRATION

Notifications 2.0

Monitoring > Messaging service > Notifications 2.0

Service usage/limits

Topics	32 / Unlimited
Subscribers	33
Publishers	12

Service message backlog limits

Backlog quota (per topic)	26 MB
Backlog time to live (TTL)	1 day 12 hours

Topics 32 of 32 items No filters

Name	Message rate in (msg/s)	Message rate out (msg/s)	Subscribers	Message backlog	Used backlog
Device195245Subscrip...	6.034	0	1	1.08 MB	4.14%
Device844224Subscrip...	4.72	0	1	904.25 kB	3.45%
alarmServiceSubscription	6.048	3.95	2	681.29 kB	2.6%
temperatureDeviceSubs...	4.727	3.967	1	1.31 kB	0%
Device464218Subscrip...	0	0	1	0 bytes	0%
Device654209Subscrip...	0	0	1	0 bytes	0%
Device364216Subscrip...	0	0	1	0 bytes	0%
Device673244Subscrip...	0	0	1	0 bytes	0%

1-25 of 32 Items per page 25

Topic list

The topic list shows the following information for each topic:

Column name	Description	Unsafe range
Name	Topic name. See the feature-specific documentation below for more information on mapping this to a specific source.	-
Message rate in (msg/s)	Total rate of messages published on the topic per second.	-
Message rate out (msg/s)	Total rate of messages dispatched to the subscribers for the topic per second. Dispatch includes additional batching and queuing mechanisms, so this rate could differ from the subscriber acknowledgment rate.	-
Subscribers	Total number of registered subscribers. This includes both actively consuming subscribers and those that are currently disconnected and not consuming any messages.	> 5
Message backlog	Backlog size in bytes which corresponds to the size occupied by unconsumed messages.	> 20 MB
Used backlog	Percentage usage of the backlog quota limit.	> 80%

Refer to the feature-specific documentation below for more information on how to map the topic name to the source and how to clear the backlog when reaching the unsafe range.

Messaging Service limits

All the backlog limits visible at the top of the topics list view are applied per topic. This means if the backlog quota is set to 25MB, each topic will queue messages until it reaches the configured limit. Limits are Cumulocity platform wide, and only the Operations team can

change them.

TO VIEW THE TOPIC DETAILS

Click on a selected topic name to navigate to the topic details view. The view contains information about the topic at the top and the list of all subscribers for that topic below.

The screenshot shows the 'alarmServiceSubscription' topic details page. The left sidebar contains navigation links: ADMINISTRATION, Home, Accounts, Ecosystem, Business rules, Management, Settings, Monitoring, Messaging service, MQTT Service, Notifications 2.0 (selected), and Migration. The main content area displays the topic name 'alarmServiceSubscription' and a breadcrumb trail: Monitoring > Messaging service > Notifications 2.0 > alarmServiceSubscription. A 'Reload' button is in the top right. The topic details are divided into two sections: 'Topic usage' and 'Topic message backlog'. The 'Topic usage' section shows: Active subscribers (1), Total subscribers (2), Total unacknowledged messages (1,477), Message rate in (6.048 msg/s), and Message rate out (3.95 msg/s). The 'Topic message backlog' section shows: Backlog usage (2.7% used, 7071 kB) and Backlog quota (26.2 MB). Below these is a 'Subscribers' table with 2 items. The table has columns: Name, Connected clients, Acknowledgment rate, Last acknowledged, Unacknowledged messages, and Used backlog. The subscribers listed are 'hZtnCEeHnfAFzXF' and 'alarmServiceConnector'. The bottom of the page shows '1 - 2 of 2' and 'powered by CUMULOCITY'.

Subscriber list

The subscriber list shows the following information for each subscriber:

Column name	Description	Unsafe range
Name	Subscriber name. See the feature-specific documentation below for more information on mapping this to a specific destination.	-
Connected clients	Number of clients that are currently connected and consuming messages.	-
Acknowledgment rate (msg/s)	Current rate per second of messages fully processed (consumed, processed, and acknowledged) by the consumers.	-
Last acknowledged	Latest timestamp when a message was fully processed by the consumer.	>= 1 day
Unacknowledged messages	Number of unconsumed messages for this subscriber.	> 1000
Used backlog	Percentage usage of the backlog quota limit by the subscriber.	> 80%

Refer to the feature-specific documentation below for more information on how to map the subscriber name to the destination and how to clear the backlog when reaching the unsafe range.

MONITORING NOTIFICATIONS 2.0

Topic and subscriber

The topic name is the same as the `subscription` field used in the [Notifications 2.0 Subscriptions API](#) and the [Notifications 2.0 Tokens API](#).

The subscriber name is the same as the `subscriber` field used in the [Notifications 2.0 Tokens API](#).

The subscriber is created the first time that a Notifications 2.0 WebSocket connection is established using a token with given subscription and subscriber names. The topic itself is created the first time that *any* Notifications 2.0 WebSocket connection is established using a token with the given subscription name. However, once the subscriber is created it will not be deleted even if the WebSocket connection is disconnected. That is, the Messaging Service will collect and persist the messages under the given topic until either they are consumed, they reach the configured time-to-live (TTL) interval, or the [subscriber is explicitly unsubscribed](#) from the topic. Refer to the [consumer lifecycle](#) for more details.

Clear the backlog

When the Messaging Service backlog is full, no new messages can be added to the backlog until it is cleared. REST requests that are also supposed to produce a notification will fail with a 500 status code and a message saying that the backlog quota has been reached. Clients working with Cumulocity must be aware of this situation and handle the error appropriately. In this situation, the backlog must be cleared before continuing work. There are various ways to clear the backlog from Notifications 2.0 topics.

Consume messages

If the topic and subscriber were created, there are probably also valuable messages stored in the Messaging Service that should be consumed. To consume and acknowledge the messages for a given topic and subscriber:

- Create the [Notifications 2.0 Token](#) for the selected topic and subscriber.
- Use the token to create a [Notifications 2.0 WebSocket connection](#) to the topic.
- Process and [acknowledge](#) all the messages received via the WebSocket connection.

This will remove the messages from the Messaging Service and clear the backlog for the given topic and subscriber, but the action is not permanent. Since the Notifications 2.0 subscription and the subscriber still exist, the backlog can fill again with new messages if they are not consumed continuously.

Unsubscribe the subscriber using Notifications 2.0 API

If the subscriber is not needed anymore and there are no valuable messages that should be consumed, the subscriber can be unsubscribed. To do this:

- Create the [Notifications 2.0 Token](#) for the selected topic and subscriber.
- Use the token to unsubscribe the subscriber from the topic by calling the [Notifications 2.0 Token Unsubscribe API](#).

This will remove the subscriber from the Messaging Service and clear the backlog for the given subscriber, and potentially the whole topic if there are no more subscribers with unconsumed messages. If the subscriber is not recreated by establishing a [Notifications 2.0 WebSocket connection](#) to the topic, this action is permanent, meaning the backlog won't grow again. If there are no more active subscribers for the topic, it is also recommended to delete the [Notifications 2.0 Subscription](#).

Unsubscribe the subscriber via the UI

If the subscriber is no longer needed and there are no valuable messages that should be consumed, the subscriber can be unsubscribed directly from the UI. To do this, select the subscriber from the subscriber list in the **Messaging Service** page and click the unsubscribe icon. This action is equivalent to [unsubscribing the subscriber using Notifications 2.0 API](#). All information about this being a permanent action and clearing the backlog is the same as described above.

MONITORING THE MQTT SERVICE

Topic and subscriber

The topic name is mapped 1:1 to the topic name used by the MQTT Service client.

When working with the [MQTT Service SDK](#), the subscriber name is the same as the name defined in the [subscriber configuration](#).

Subscribers created by MQTT clients are deleted automatically once the client disconnects, so it is unlikely that they will persist for a long time and require manual cleanup.

Clear the backlog

When the Messaging Service backlog is full, no new messages can be added to the backlog until it is cleared. In this situation, client behavior depends on the MQTT protocol version used:

- An MQTT client using protocol version 3.1.1 will simply be disconnected.
- An MQTT client using protocol version 5 will get negative PUBACK response with `0x97` (quota exceeded) reason code, but it will still remain connected.

Implementations connecting to the MQTT Service must be aware of this and handle these errors appropriately. In either case, the backlog must be cleared before continuing work. There are various ways to clear the backlog from MQTT Service topics.

Consume messages

If the topic and subscriber were created, there are probably also valuable messages stored in the Messaging Service that should be consumed. Use the [MQTT Service SDK](#) to consume and acknowledge the messages for a given topic and subscriber.

After consuming all the messages, the backlog is cleared, and the topic is ready to store new messages.

Unsubscribe the subscriber using the MQTT Service SDK

If the subscriber is no longer needed and there are no valuable messages that should be consumed, the subscriber can be unsubscribed. Use the [unsubscribe action](#) from the MQTT Service SDK. This will remove the subscriber from the Messaging Service and clear the backlog for the given subscriber, and potentially the whole topic if there are no more subscribers with unconsumed messages.

Unsubscribe the subscriber via the UI

If the subscriber is no longer needed and there are no valuable messages that should be consumed, the subscriber can be unsubscribed directly from the UI. To do this, select the subscriber from the subscriber list in the **Messaging Service** page and click the unsubscribe icon. This action is equivalent to [unsubscribing the subscriber using the MQTT Service SDK](#).

FREQUENTLY ASKED QUESTIONS (FAQ)

What should I do when encountering a high number of topics?

A high number of topics could be normal behavior when dealing with many devices, but there could also be a situation where new topics are generated unnecessarily:

- Test topics that were never cleared - check for unused topics that can be cleaned up.
- Topics carrying the same data - topic names should be reused where possible to avoid unnecessary resource consumption. If you have multiple topics carrying the same data, consider merging them into a single topic.

What should I do when encountering a high number of subscribers?

If you have a single microservice or a single client consuming messages from the Messaging Service, you should typically only have a single subscriber. Check if the subscriber name used by your client is unique and reused consistently when connecting to the Messaging Service. A common pitfall is generating a random subscriber name each time a new connection to the Messaging Service is established.

Multiple subscribers are expected when multiple distinct clients consume from the same topic or when using [shared consumer tokens](#).

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.

✔ REQUIREMENTS

ROLES & PERMISSIONS:

- To view alarm mappings: READ permission for the permission type "Option management".
- To manage (create, edit, or delete) alarm mappings: ADMIN permission for the permission type "Option management".

For easier user access management, the above permissions are included in the global role created by default in every new tenant:

- Tenant Manager - manages tenant-wide configurations like applications, tenant options and business rules.

i RELATED TOPICS

- [Device management & connectivity > Device Management application> Monitoring and controlling devices > Working with alarms](#) for information on working with alarms in general.
- [Alarms](#) in the Cumulocity OpenAPI Specification for details on managing alarms via REST.

TO VIEW ALARM MAPPINGS

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

ADMINISTRATION

- Home
- Accounts
- Tenants
- Ecosystem
- Business rules
- Alarm mapping**
- Management
- Settings
- Data broker
- Migration

powered by CUMULOCITY

Alarm mapping 3 mappings

Business rules > Alarm mapping

Filter...

Add mapping Reload

Alarm type	Description	Severity
cBy_Pressure	Critical pressure change	critical
<p>Alarm type to match: cBy_Pressure</p> <p>New description: Critical pressure change</p> <p>New severity: <input type="radio"/> Drop <input checked="" type="radio"/> Critical <input type="radio"/> Major <input type="radio"/> Minor <input type="radio"/> Warning</p> <p>Save</p>		
cBy_Speed	Ignore speed change	drop
cBy_Temperature	<kept as is>	warning

For each alarm mapping, the alarm severity, the alarm type and a description (optional) are shown.

TO ADD ALARM MAPPING

1. Click **Add alarm mapping** in the top menu bar.
2. Enter the alarm type to be modified.
3. In the **New description** field, optionally enter a new description for the alarm. If you leave this field empty, the original text from the alarm will be kept.
4. Select the desired new severity, or select "Drop" to not show the alarm at all.
5. Click **Save** to save your settings.

INFO

The alarm type provided as an alarm mapping is interpreted as alarm type prefix: "<type-prefix>*". If you create, for example, an alarm mapping to address alarms of type "crit-alarm", the mapping is effective for any type of alarm that starts with this value, for example, "crit-alarm-1", "crit-alarm-2", or "crit-alarm-xyz".


TO EDIT AN ALARM MAPPING

Expand an alarm mapping to edit it. You may modify the description and the alarm severity. The alarm type is not editable.

INFO

Refresh the list to discard any changes without saving.

TO DELETE AN ALARM MAPPING

To delete an alarm mapping, hover over it and click the remove icon  which appears on hovering over the row.

MANAGING DATA

RETENTION RULES

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

✔ REQUIREMENTS

ROLES & PERMISSIONS:

- To view retention rules: READ permission for the permission type "Retention rules"
- To manage retention rules (create, update, delete): ADMIN permission for the permission type "Retention rules"

The above permissions can be used to create roles for robust user management. Every new tenant have specified typical roles by default:

- Tenant Manager - Can manage tenant wide configurations like applications, tenant options and retention rules.

ℹ RELATED TOPICS

- [Platform administration > Enterprise tenant administration > Managing tenants > Tenant policies](#) for details on the creation of tenant policies and retention rules on tenant level.
- [Retention rules](#) in the Cumulocity OpenAPI Specification for details on managing retention rules via REST.

ℹ INFO

Retention rules are usually run once per calendar day. When you edit a retention rule you don't see an immediate effect in the **Usage** section on the Home screen of the Administration application.

TO VIEW RETENTION RULES

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

ADMINISTRATION

- Home
- Accounts
- Tenants
- Ecosystem
- Business rules
- Management
- Retention rules**
- Files repository
- Settings
- Data broker
- Migration

powered by CUMULOCITY

Retention rules

Management > Retention rules

Filter...

Add rule Reload

Data type	Fragment type	Type	Source	Maximum age
*	*	*	*	60 days
MEASUREMENT	*	*	*	60 days
EVENT	*	*	*	30 days

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.

DATA TYPES

The following data types are covered under retention rules:

- Alarms
- Audits
- Bulk operations
- Events
- Measurements
- Operations

INFO

Retention rules do not apply to files stored in the files repository.

TO ADD A RETENTION RULE

1. Click **Add rule** in the top menu bar.
2. In the resulting dialog box, select the type of data to be cleaned up (alarms, measurements, events, operations, audit logs or all).
3. Optionally, enter a type or a fragment type to further restrict the data to be cleaned up. The type refers to the value of the object's top-level **type** field and identifies the specific kind of object within the selected data type. The fragment type refers to the name of a JSON property contained in the object. An object has one type but can contain multiple fragments.
4. If you want to remove data only from a specific device, enter the device ID into the **Source** field.
5. Enter the **Maximum age** in days (max. allowed value is 10 years in days).
6. Click **Save** to save your settings.

The retention rule will be added to the list.

INFO


Per default, an asterisk * is set in all fields except the **Maximum age** field, to include all values. Alarms are only removed if they have a status of CLEARED.

TO EDIT A RETENTION RULE

Simply click the row of the rule you want to edit.

For details on the fields, see [To add a retention rule](#).

TO DELETE A RETENTION RULE

Hover over the row with the rule you want to delete and click the remove icon  that appears on the right.

EXECUTION EXAMPLES

All retention rules are executed sequentially and independent of each other.

If we have two retention rules, a more specific one with a greater maximum age that defines a subset of the documents that are defined by a more common rule with a lower maximum age, then effectively it will work as if we had a single, more common rule.

For example, given the two following rules:

Data type	Fragment type	Type	Source	Maximum age
MEASUREMENT	*	c8y_Temperature	*	30 days
MEASUREMENT	*	c8y_Temperature	12345	60 days

All measurements with the type `c8y_Temperature` which are older than 30 days will be removed, including those where the source equals `12345`.

On the other hand, when we have the following retention rules defined:

Data type	Fragment type	Type	Source	Maximum age
MEASUREMENT	*	c8y_Temperature	*	30 days
MEASUREMENT	*	*	*	60 days

The retention process removes the measurements with the type `c8y_Temperature` which are older than 30 days, all other measurements will be removed when they are older than 60 days.

INFO

The source parameter is the ID of the device. When it is defined, the retention process only removes the documents directly related to the device represented by the source, not its children or groups it belongs to.

FILE REPOSITORY

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

✓ REQUIREMENTS

ROLES & PERMISSIONS:

- To view files in the files repository: READ permission for the permission type "Inventory". You can remove owned files with this permission but you cannot remove files of other users.
- To upload files to the files repository: CREATE permission for the permission type "Inventory".
- To upload and manage files of all owners in the files repository: ADMIN permission for the permission type "Inventory".

The above permissions can be used to create roles for robust user management. Every new tenant have specified typical roles by default:

- Global Manager - Can read and write all data from all devices
- Global Reader - Can read all data from all devices

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 **All applications** page.

For each file, the name of the file, its owner, its type (for example, image/bmp, text/csv), its size and its last update date are displayed. If file type is supported, you can click a magnifier icon next to the file name to preview it. You can download or delete a file by clicking action buttons which appear when hovering over the file row. Note that some files (for example, application archives) cannot be deleted from this page.

You can use filters or search input to look for particular files, see [Search and filter functionality](#) for details. By default, files are sorted by **File name**. To change the sorting, remove the default filter and define your own criteria for filtering the list.


The screenshot shows the 'Files repository' management interface. The left sidebar contains a menu with items: Home, Accounts, Tenants, Ecosystem, Business rules, Management, Retention rules, Files repository (highlighted), Settings, Data broker, and Migration. The main content area is titled 'Files repository' and shows a table of files. The table has columns: Name, Type, Size, Owner, and Last update. There are three files listed: cloud.jpeg, Screenshot.png, and logo.svg. Each file row has a magnifying glass icon for preview and a download icon. The interface includes a top navigation bar with 'ADMINISTRATION' and 'Files repository' tabs, and a bottom status bar indicating 'powered by CUMULOCITY'.

Name	Type	Size	Owner	Last update
cloud.jpeg	image/jpeg	19.7 kB	john.doe@example.com	16 Jan 2024, 08:55:42
Screenshot.png	image/png	1.9 MB	john.doe@example.com	24 Jan 2024, 19:57:42
logo.svg	image/svg+xml	6.4 kB	john.doe@example.com	13 Jan 2024, 13:17:42


TO UPLOAD A FILE FROM YOUR FILE SYSTEM

Click **Upload files** in the top menu bar. In the resulting dialog box, select the files to be uploaded by browsing your file system or dropping the files. You can review the selected files in the displayed list and confirm the upload by clicking **Upload**.

TO DOWNLOAD A FILE FROM YOUR ACCOUNT

Click the download icon  at the right of the respective row.

TO DELETE A FILE FROM YOUR ACCOUNT

Hover your mouse over the row containing the file you want to delete, then click the delete icon  at the right.

To delete multiple files

Select the checkbox next to each file you want to delete, or click the checkbox at the top of the table to select all displayed files. The table header shows the number of files selected and available actions. Click **Delete** and confirm the deletion.

INFO

- If a file is an application archive, you cannot delete it from the files repository. Instead, you must delete this file from the applications details.
- If you delete files in bulk and your selection contains files not eligible for removal, the deletion will proceed while ignoring the files that cannot be deleted.

LATEST MEASUREMENT VALUES

This section describes how to create a configuration for automated persistence of measurement values under the `c8y_LatestMeasurements` fragment.

HOW TO ENABLE IT

Use the tenant options to create a category named `measurement.series.latestvalue` with a PUT request to a [tenant options category](#). Example:

```
PUT /tenant/options/measurement.series.latestvalue
{
  "c8y_Humidity.H":""," // to enable single series c8y_Humidity.H
  "c8y_Temperature.*":""," // to enable series under fragment c8y_Temperature
  // or "*" to enable all
}
```

where the key is a filter of measurement series that must be persistent and its value must always be an empty string (left for a future use case).

IMPORTANT

Property names used for fragment and series must not contain whitespaces nor the special characters `$ & + , / : ; = ? @ " < > # % { } | \ ^ ~ [] ` .` This is necessary to ensure the new tenant option is processed correctly and saved successfully.

HOW IT WORKS

If a measurement is created with a series that matches the configuration the device managed object is updated with the last series sent to the platform. Example:

If you send

```
POST /measurement/measurements
{
  "source": "5413"
  "time": "2024-02-01T10:00:00Z"
  "c8y_Temperature": {
    "T": {
      "value": 15,
      "unit": "C"
    }
  }
  "c8y_Speed": {
    "S": {
      "value": 15,
      "unit": "m/s"
    }
  }
}
```

then, considering the example configuration, only `c8y_Temperature.T` is stored as part of the device, while `c8y_Speed.S` is ignored. This means, that the measurement is stored like before, only the state update is skipped. To read the latest values on device level you must use the Inventory API and explicitly specify the `withLatestValues` parameter. For more information refer to the [Cumulocity OpenAPI Specification](#). To get a single device:

```
GET /inventory/managedObjects/5413?withLatestValues=true
{
  ...
  "c8y_LatestMeasurements": {
    "c8y_Temperature": {
      "T": {
        "value": 15,
        "time": "2024-02-01T10:00:00Z",
        "unit": "C"
      }
    }
  }
}
```

To get a list of devices matching the expected criteria, for example, get all devices which have a reported temperature higher than 10 degrees:

```
GET /inventory/managedObjects?withLatestValues=true&query=$filter=c8y_LatestMeasurements.c8y_Temperature.T.value+gt+10
{
  managedObjects: [
    {
      ...
      "c8y_LatestMeasurements": {
        "c8y_Temperature": {
          "T": {
            "value": 15,
            "time": "2024-02-01T10:00:00Z",
            "unit": "C"
          }
        }
      }
    }
  ]
}
```

In scenarios where measurements are delayed in arriving (due to network latency or other factors), the system may incorrectly display them as the latest measurement, even though they are technically out of order.

To address this, the toggle `strongConsistency` is provided. When this value is set, the out-of-order measurements will not be shown as the latest data for the device, regardless of when they were actually received. Instead, only measurements that arrive in the correct order will be treated as the latest, ensuring that the most accurate, timely data is always presented.

The toggle can be set individually for each measurement fragment to allow fine-grained control over which measurement fragments are affected:

```
PUT /tenant/options/measurement.series.latestvalue
{
  "c8y_Humidity.H": "",
  "c8y_Temperature.*": "strongConsistency"
}
```

or it can be set globally, which will apply the setting to all measurement fragments from the device:

```
PUT /tenant/options/measurement.series.latestvalue
{
  "c8y_Humidity.H": "",
  "c8y_Temperature.*": "",
  ".*": "strongConsistency"
}
```

It's important to note that setting `strongConsistency` may slightly slow down the measurement injection process, as the system now needs to check the arrival time of each measurement to determine if it is delayed. This ensures that outdated or late data does not interfere with the integrity of the latest measurement display.

PREVIOUS MEASUREMENTS VALUES

How to configure it

This functionality enables the storage and querying of measurement values that have the second most recent arrival time. Retrieving not only the most recent value but also the one before is often necessary — for example, to calculate trends or detect changes over time. By default, this feature is enabled globally, but it can be configured at the tenant level via an API request.

To manage automated persistence of previous measurement values on tenant level use the tenant options to create a new category named `measurement.series.previousvalue.enabled` with a PUT request to a [tenant options category](#). Example:

```
POST /tenant/options/
{
  "category": "configuration",
  "key": "measurement.series.previousvalue.enabled",
  "value": "true" //or "false" if the functionality needs to be disabled for a specific tenant
}
```

How it works

To retrieve previous values at the device level, you must use the Inventory API and explicitly include the `withLatestValues` parameter. For more information refer to the [Cumulocity OpenAPI Specification](#). The measurements returned belong to a series that matches the configuration of the latest values, allowing you to access both the most recent and previous measurements within the same series:

```
GET /inventory/managedObjects/5413?withLatestValues=true
{
  ...
  "c8y_LatestMeasurements":{
    "c8y_Temperature":{
      "T":{
        "value":15,
        "time":"2024-02-01T10:00:00Z",
        "unit":"C"
      }
    }
  },
  "c8y_PreviousMeasurements": {
    "c8y_Temperature": {
      "T": {
        "value": 30,
        "time": "2024-02-01T09:00:00Z",
        "unit": "C"
      }
    }
  }
}
```

IMPLICATIONS & PRECONDITION

This feature introduces an additional operation upon measurement creation. This results in performance degradation, depending on the number of series stored per measurement, reaching from 5% for single series in each measurement to more than 20% in case of 50 series per measurement. Such drawback applies if the text index is disabled. In other cases, the performance degradation can be much higher, up to more than 100%. Therefore disabling the text index is considered as a precondition.

LIMITATIONS

Security

The latest measurement values are part of the managed object and they follow the managed object inventory role permissions instead of respecting the inventory roles for measurements.

Data model

The latest measurements do not store the measurement type. This information can be obtained using the [Measurements API](#).

Last value

The value stored in the device managed object is the last value sent to the platform. If measurements are delivered to the platform in a different order than their creation time, then the latest values may be affected — unless the [strongConsistency](#) toggle is enabled.

CHANGING SETTINGS

From the **Settings** menu, administrators can manage various settings for the account:

- Change the [application settings](#).
- Manage the [properties library](#).
- Provide [SMS provider credentials](#).
- Manage the [connectivity settings](#).
- Change the [localization settings](#).

APPLICATION

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

ADMINISTRATION

- Home
- Accounts
- Tenants
- Ecosystem
- Business rules
- Management
- Settings
- Authentication
- Remote access
- Application**
- Properties library
- Enterprise tenant
- SMS provider
- Branding
- Connectivity
- Localization
- Data broker

powered by CUMULOCITY

Application

Settings > Application

Default application

The default application specifies the application that shows up per default when logging into the platform. It applies to all users of the tenant. Select an application from the list below and make sure that all users can access this application.

- ☐ Administration
- ☐ Cockpit
- ☐ Device Management
- ☐ Digital Twin Manager

Save default application

Access control

The "Allowed domain" setting allows your JavaScript web application to directly communicate with the REST API.

Options:

- Enter "*" to allow communication from any host,
- enter "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,
- leave the field blank to allow access only from your tenant's domain.

For more information, check [enable-cors.org](#)

Allowed domain

e.g. *

Be careful not to lock yourself out of the platform.

Save access control

TO CHANGE APPLICATION SETTINGS

Under **Default application**, you can select a default application from the list which will apply to all users within the tenant. Whenever the platform is accessed, for example, by domain name only, without mentioning a specific application, the application selected as default application is used as default landing page.

INFO

All users must have access to this application.

Under **Access control**, administrators can enable cross-origin resource sharing or "CORS" on the Cumulocity 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>.

RELATED TOPICS

- [Platform administration > Standard tenant administration > Managing applications](#) for general information on managing applications.
- [Platform administration > Standard tenant administration > Managing users](#) for general information on managing users.

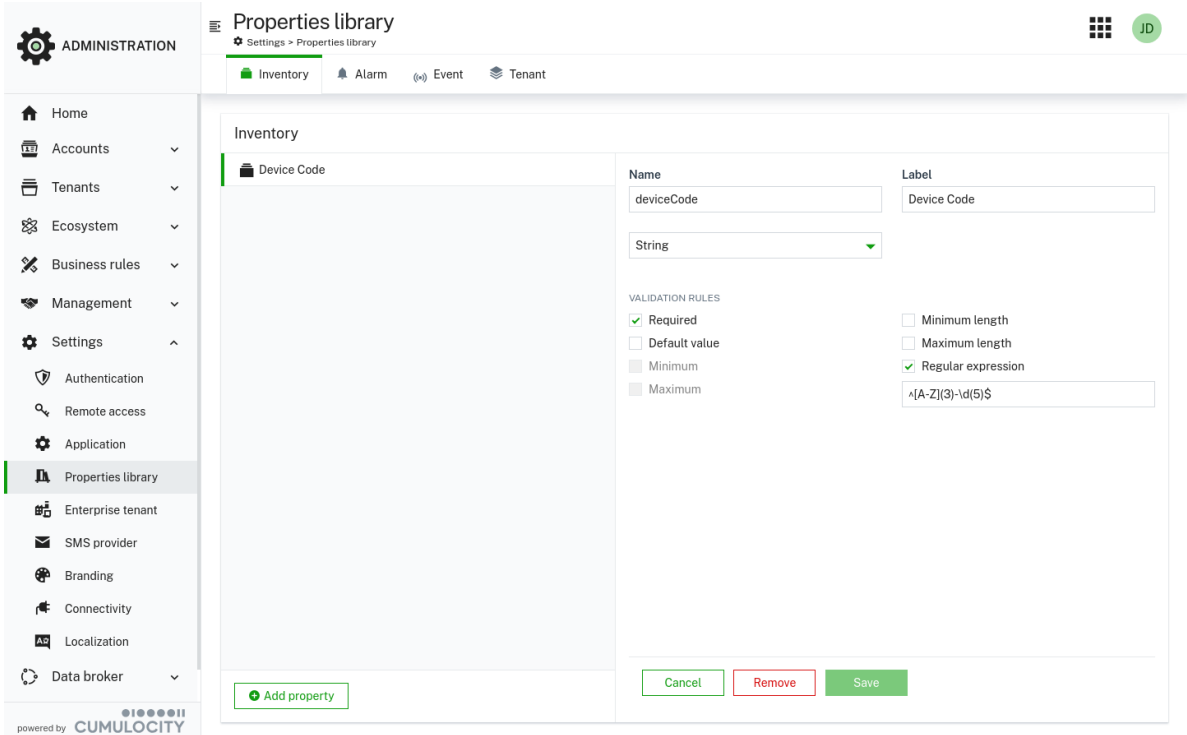
PROPERTIES LIBRARY

REQUIREMENTS

ROLES & PERMISSIONS:

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

Click **Properties library** in the **Settings** menu, to add custom properties to inventory objects, alarms, events and tenants.



ADMINISTRATION

- Home
- Accounts
- Tenants
- Ecosystem
- Business rules
- Management
- Settings
- Authentication
- Remote access
- Application
- Properties library**
- Enterprise tenant
- SMS provider
- Branding
- Connectivity
- Localization
- Data broker

Properties library

Settings > Properties library

Inventory Alarm Event Tenant

Inventory

Device Code

Name: deviceCode

Label: Device Code

Type: String

VALIDATION RULES

- ☒ Required
- ☐ Default value
- ☐ Minimum
- ☐ Maximum
- ☐ Minimum length
- ☐ Maximum length
- ☒ Regular expression: `^[A-Z]{3}-d(5)$`

Buttons: Add property, Cancel, Remove, Save

powered by CUMULOCITY

With custom properties, you can extend the data model of Cumulocity 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 widget](#) and [Asset properties widget](#).
- 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.

RELATED TOPICS

- [Application enablement & solutions > Cockpit > Widgets collection](#) for further information on the usage of properties in the "Asset table" and "Asset properties" widgets.
- [Application enablement & solutions > Cockpit > Managing exports](#) for further information on the usage of properties in reports and exports.
- [Platform administration > Enterprise tenant administration > Managing tenants > To create a subtenant](#) for further information on custom tenant properties.

TO ADD A CUSTOM PROPERTY

1. Select the tab for the desired property and click **Add property**.
2. In the resulting dialog box, provide a unique name as identifier and a label for the property and select its data type from the dropdown list.
3. Additionally, select validation rules for the new property:

Checkbox	Description
Required	If selected, the property must be provided, for example, 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.

4. Click **Save** to create the new property.

TO EDIT A CUSTOM PROPERTY

1. Click on the name of a property in the list to open it.
2. Do your edits. For details on the fields see [To add a custom property](#).
3. Click **Save** to save your settings.

TO REMOVE A CUSTOM PROPERTY

1. Click on the name of a property in the list to open it.
2. Click **Remove** to delete the property.

SMS PROVIDER

✔ REQUIREMENTS

ROLES & PERMISSIONS:

To view SMS provider configurations: READ permission for the permission type "SMS" To set or remove SMS provider configurations: ADMIN permission for the permission type "SMS"

SMS are used throughout the platform for various features like [two-factor authentication](#) and user notifications, for example, on alarms.

By providing your credentials you enable platform features that utilize SMS services.

TO ENTER SMS PROVIDER CREDENTIALS

1. Click **SMS provider** in the **Settings** menu.
2. In the **SMS provider** page, select one of the available SMS providers from the **SMS provider** dropdown field. You can start typing to filter items and more easily find your preferred provider.
3. In the resulting dialog, enter the required credentials and properties or specify optional settings, which differ depending on the provider you selected.
4. Click **Save** to save your settings.

i INFO

OpenIT does not serve new customers anymore and is in the process of shutting down their SMS provider business. We therefore recommend you to select one of the other SMS providers.

CONNECTIVITY

In the **Connectivity** page, you can manage credentials for different providers. In order to add or replace credentials ADMIN permissions are required.

✔ REQUIREMENTS

ROLES & PERMISSIONS:

The **Connectivity** menu item is only available if you are logged in to the Cumulocity platform as administrator and if you have READ or ADMIN permission for the permission type "Connectivity".

To view connectivity settings: READ permission for the permission type "Connectivity" To set or remove connectivity provider configurations: ADMIN permission for the permission type "Connectivity"

The following provider settings may currently be specified:

- [Activity LoRa](#)
- [Sigfox](#)
- [SIM](#)

TO PROVIDE OR REPLACE CREDENTIALS

1. Switch to the tab of your desired provider.
2. Enter the URL of the provider.
3. Enter the credentials of your provider platform. Depending on the provider, these credentials will be either the credentials of your account in the provider platform or the credentials with which you can register in the Cumulocity connectivity page, will be displayed in your account in the provider platform.
4. Finally, click **Save** to save your settings.

Depending on the provider you have selected, there may be additional fields, which will be explained in the respective agent documentation, see [Device integration](#).

LOCALIZATION

Using the **Localization** functionality you can add custom translations for existing static text in the UI.

✓ REQUIREMENTS

- To view the **Localization** page: READ permission for permission type "Application management"
- To add/update/delete localization identifiers: ADMIN permission for permission type "Application management"
- Your user must have a role with READ permission for "Application management". See [Managing permissions and roles](#) for more information.

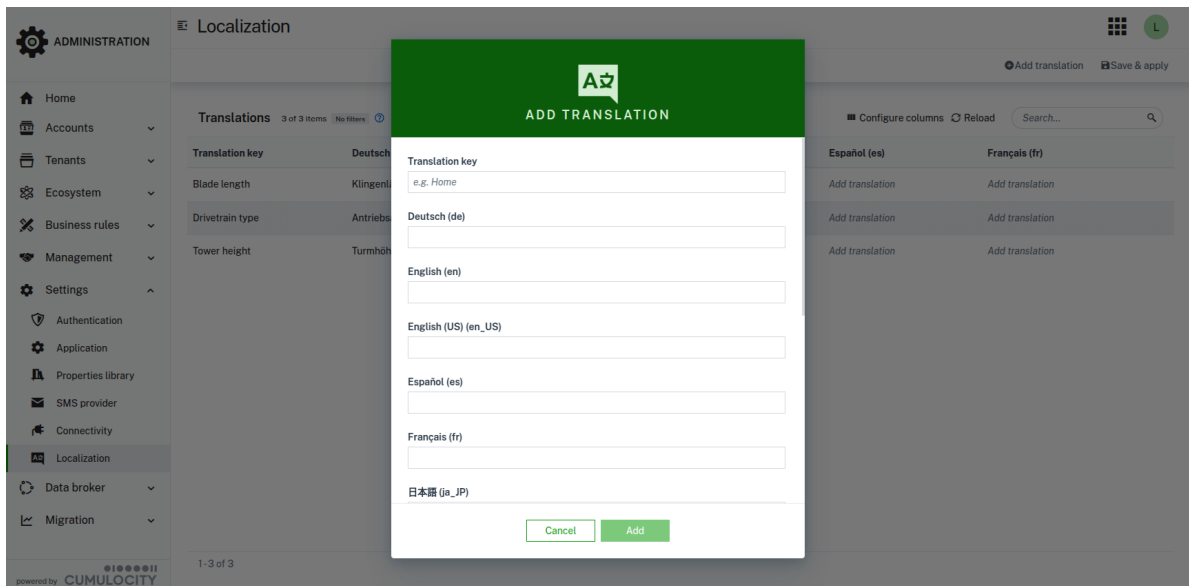
Click **Localization** in the **Settings** menu in the navigator to open the translation editor.

The screenshot shows the Cumulocity Localization settings page. The left sidebar contains the 'ADMINISTRATION' menu with options like Home, Accounts, Tenants, Ecosystem, Business rules, Management, Settings, Authentication, Application, Properties library, SMS provider, Connectivity, Localization, Data broker, and Migration. The 'Localization' option is selected. The main content area is titled 'Localization' and displays a table of translations for three items: Blade length, Drivetrain type, and Tower height. The table has columns for Deutsch (de), English (en), English (US) (en_US), Español (es), and Français (fr). Each cell contains either the translated text or a link to 'Add translation'. At the bottom, it says '1-3 of 3'.

Translation key	Deutsch (de)	English (en)	English (US) (en_US)	Español (es)	Français (fr)
Blade length	Klingenlänge	Blade length	Add translation	Add translation	Add translation
Drivetrain type	Antriebsart	Drivetrain type	Add translation	Add translation	Add translation
Tower height	Turmhöhe	Tower height	Add translation	Add translation	Add translation


TO ADD NEW IDENTIFIER FOR TRANSLATIONS

1. Click **Add translation** on the top menu bar.
2. In the resulting dialog box, add a name for the new translation key.
3. Optionally, add translations in the respective fields.
4. Click **Add** to close the translation editor.
5. Click **Save & apply** in the top menu bar to save the new translation identifier and apply it to the UI.




TO ADD AND EDIT TRANSLATIONS

You can add or edit translations for every identifier in two ways:

1. Hover over the respective column to display the edit icon .
2. Click the edit icon next to the field you want to edit.
3. Add or edit the translation.
4. Click the green checkmark to save the translation.
5. Click **Save & apply** to apply the changes.

Or:

1. Click the edit icon  in any row to open the translation editor for the respective identifier.
2. Add or edit the translations.
3. Click **Add** to close the translation editor.
4. Click **Save & apply** to apply the changes.

To view the added or modified translations in the UI, change the language from the user menu, see [To change user settings](#).

ENHANCED TIME SERIES SUPPORT

GENERAL CONFIGURATION

The Cumulocity Operational Store provides an enhanced time series support (so-called time series collections) for measurements data. The following section summarizes how to enable/disable this feature.

INFO

The enhanced time series support might be enabled for new tenants by default from a platform administrator.

TO CONFIGURE TIME SERIES SUPPORT

The enhanced time series support can be configured via a REST API as a tenant configuration. The following example illustrates how to **enable** time series collections for a subtenant:

```
POST {sub-tenant-url}/tenant/options
Content-Type: application/json
{
  "category": "configuration",
  "key": "timeseries.mongodb.collections.mode",
  "value": "ENABLED"
}
```

The following example illustrates how to **disable** time series collections for a subtenant:

```
POST {sub-tenant-url}/tenant/options
Content-Type: application/json
{
  "category": "configuration",
  "key": "timeseries.mongodb.collections.mode",
  "value": "DISABLED"
}
```

INFO

Tenant options are not inheritable from the parent tenant, that is, enabling the property on the Enterprise tenant does not affect the subtenants.

IMPLICATIONS OF THE CONFIGURATION

The configuration affects the collection that stores measurement data. By enabling or disabling the property, the system switches collections in the background. This can lead to a situation where data resides in multiple collections.

The Time series migration microservice ensures data consistency and prevents scenarios where data is distributed across multiple collections. As a best practice, the property should be configured only at the beginning of a tenant setup, ideally when no measurement data is stored yet.

❗ IMPORTANT

Once enabled, avoid switching the property back to **DISABLED** as this can lead to experience data loss. Do this only in case of an issue or emergency.

UNSUPPORTED APIS

The following APIs are not supported and do not have a replacement:

- `GET /measurement/measurements/{id}`

Alternatively, you can use the `GET /measurement/measurements` API to retrieve a list of measurements. By specifying the device (source) ID and the exact point in time when the measurement was sent by the device, the result set can be reduced significantly. Note that every returned measurement document still contains an identifier.

The following API is partially supported:

- `DEL /measurements/measurement/`

The parameters `dateFrom` and `dateTo` are supported and must be truncated to full hours (for example, `2022-08-19T14:00:00.000Z`), otherwise an error is returned.

TO CHECK WHETHER TIME SERIES COLLECTIONS ARE ENABLED

With the following request, you can check the value of the time series collections property:

```
GET /tenant/options/configuration/timeseries.mongodb.collections.mode
Content-Type: application/json
```

An example response if the configuration is enabled:

```
{
  "category": "configuration",
  "key": "timeseries.mongodb.collections.mode",
  "value": "ENABLED"
}
```

If the configuration is not set for the tenant at all, you will get a 404 response code for the request above.

MIGRATION PROCESS DESCRIPTION

Tenant administrators can schedule their tenant or any subtenant for time series collection migration. The time series format of measurements brings the following benefits:

- better performance for measurements queries,
- less storage consumption.

Note that certain limitations are induced in the API which are described in [General configuration](#).

✔ REQUIREMENTS

To have this functionality available the tenant must be subscribed to the Timeseries-migration microservice. The Administration application must have subscribed the extension `c8y-timeseries-migration-plugin`.

The user must have the following permissions for the permission type “Tenant management”:

- To view migration status for all subtenants: READ permission.
- To perform migration activity: ADMIN permission.
- The tenant’s status must be **ACTIVE**. Tenants with status **SUSPENDED** cannot be scheduled for migration.

If attempted via API, the request fails with **422 Unprocessable Entity** and the message:

`Tenant <tenantId> is suspended. Migration actions are not permitted.`

TO TRIGGER TIME SERIES MIGRATION

To start the tenant migration follow the steps below:

1. Navigate to **Migration > Time series** in the application where the plugin is installed. By default this is the Administration application.
2. Select the tenant you want to trigger the migration for from the list of available tenants.
3. Hover over the row of the tenant in the tenant list, then click **Add to queue** and confirm the operation. The tenant migration status should be updated to **Queued**, which means that tenant is added into the migration queue.

! IMPORTANT

You can add more than one tenant into the migration queue, but the migration is executed only for one tenant at a time. The migration of the next tenant in the queue will not start until you approve the previously migrated tenant.

4. When the migration process is triggered its status for the tenant changes from **Queued** to **In progress**. After the data is processed, verified and migrated to the new collection the status of the migration changes to **Verified** and the **Approve and finish migration** button is visible in the **Ongoing migration** section and in the tenant list on hovering over the tenant row. Click **Approve and finish migration** to confirm the process.
5. A confirmation pop-up shows up providing the following information:
 - The new format for time series measurements, which is used after confirming the data migration process.
 - That after seven days the legacy collection is removed. Click **Confirm**. This will change the status of the migration to **Approved**.

! IMPORTANT

The approval is irreversible. Once the migration has been confirmed and the status changes to **Approved** it is no longer possible to switch back to the legacy data format without data loss in case of an issue with the new data format. The enhanced time series support feature is fully enabled with all implications mentioned above.

- Until this point in time billing metrics are computed based on the data stored in the legacy data format. After confirmation, billing metrics are computed based on the new time series optimized data format.
6. After seven days the legacy measurements collection is deleted and the migration status changes to **Completed**.

i INFO

The migration of measurements can be cancelled when a tenant has the status **Queued**. After the status is changed to **In progress**, the process can no longer be stopped until it reaches **Verified** state and waits for user confirmation.

MIGRATION STATES

Status	Manageable by user	Description
Not migrated	yes	Indicates that the tenant has not been migrated yet. If the tenant uses legacy measurements, it will be scheduled for migration. Note: Tenants with status SUSPENDED cannot be queued.
Queued	yes	Indicates that the tenant is added to the migration queue. Tenants in this state can be picked up for migration. It is possible to Cancel migration from this state.
In progress	no	Indicates that the migration of the measurements collection is currently in progress.
Migrated	no	Indicates that the migration of the measurements collection is done.
Verifying	no	Indicates that the verification of the migrated data is in progress.
Verified	yes	Indicates that all migration processes are completed and user approval is required.
Approved	no	Indicates that the migration is completed and the legacy collection will be removed in 7 days.
Completed	no	Indicates that the migration is completed and the legacy collection is removed.
Failed	no	Indicates that an error occurred during the migration process. The information provided in the error message should be forwarded together with the support ticket.

DESCRIPTION AND PROGRESS MONITORING

The **Time series migration** page is divided into 2 sections. The top one is called **Ongoing migration** and displays the current state of the ongoing migration for the respective tenant. This section provides control over the active process. The information is displayed only after the migration has started and is in one of the progressing states (In progress, Migrated, Verifying, Verified).

Here you can see the following information:

- **Tenant** - Tenant name of the tenant the migration process is triggered for.
- **Requested by** - Name of the user that started the migration.
- **Migration range** - Date range. Start date is the date of the oldest measurement to be migrated and end date is the date of the newest measurement. This is also the point in time when the migration has started. **Migration status** - This bar displayed at the right has various functions. Depending on the state it provides either visual information on the current state of the ongoing process or allows to control certain process states. For details of states, see [Migration states](#).

The second section shows the **List of tenants** with the following information for each tenant:

- **Tenant** – Tenant name.
- **ID** – Tenant ID.
- **Domain** – Tenant domain.
- **Parent tenant ID** – Parent tenant ID.
- **Requested by user** – Name of the user that requested the migration.
- **Approved by user** – Name of the user that approved the migration.
- **Tenant status** – Current status of the tenant (for example, ACTIVE or SUSPENDED).
- **Migration status** – Current migration state for the tenant (for example, Queued, In progress, Verified).

On hovering over a tenant row, you see one of the following buttons according to the migration state. Actions are only available for tenants with status **ACTIVE**:

- **Add to queue** – Assign the tenant to the migration queue when it is in **Not migrated** state.
- **Cancel migration** – Remove the tenant from the migration queue when it is in **Queued** state. If progress has already started, it is not possible to resign from migration.
- **Approve and finish migration** – Approve the migration when it is in **Verified** state. No other migration starts if there is a tenant pending acceptance.

[🏠](#) > [Standard tenant administration](#) > [Enhanced time series support](#)