



## Enterprise 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

<b>Table of Contents</b>	<b>3</b>
<b>INTRODUCTION</b>	<b>5</b>
<b>MANAGING TENANTS</b>	<b>6</b>
MANAGING SUBTENANTS	6
TO VIEW SUBTENANTS	6
TO CREATE A SUBTENANT	7
TO VIEW OR EDIT SUBTENANT PROPERTIES	8
TO SUSPEND A SUBTENANT	9
TO DELETE A SUBTENANT	10
SUBSCRIBING APPLICATIONS	10
OVERVIEW	10
TO VIEW SUBSCRIBED APPLICATIONS	11
TO SUBSCRIBE AN APPLICATION	12
TO UNSUBSCRIBE AN APPLICATION	12
TO MONITOR THE MICROSERVICE STATUS	12
CUSTOM PROPERTIES	12
SETTING LIMITS	13
TO LIMIT THE SUBTENANT REQUEST RATE	13
TO LIMIT THE SUBTENANT DEVICE NUMBER	13
PRODUCT EXPERIENCE TRACKING	13
TENANT POLICIES	13
TO VIEW TENANT POLICIES	14
TO CREATE A TENANT POLICY	14
TO EDIT A TENANT POLICY	15
TO DUPLICATE A TENANT POLICY	15
TO DELETE A TENANT POLICY	15
DEFAULT SUBSCRIPTIONS	15
TO VIEW DEFAULT SUBSCRIPTIONS	15
TO CONFIGURE DEFAULT SUBSCRIPTIONS	16
TO OVERRIDE DEFAULT SUBSCRIPTIONS	17
<b>MANAGING USER HIERARCHIES</b>	<b>19</b>
TO VIEW USER HIERARCHIES	19
TO CREATE A SUB-USER	20
TO DELEGATE USER HIERARCHIES TO OTHER USERS	21
To delegate permissions to a user	21
To undelegate permissions	21
TROUBLESHOOTING SUB-USERS	21
<b>CUSTOMIZING YOUR PLATFORM</b>	<b>23</b>
CONFIGURATION	23
PLACEHOLDERS	23
TWO-FACTOR AUTHENTICATION	24
SUPPORT LINK	24
PASSWORD RESET	24
EMAIL SERVER	24
DATA EXPORT	25
STORAGE LIMIT	25
SUSPENDING TENANTS	25
BRANDING	25
TO CONFIGURE BRANDING SETTINGS	26
EDITING PARAMETERS	27
DOMAIN NAME	31
TO PACKAGE THE SSL CERTIFICATE IN PKCS #12	32
DNS REQUIREMENTS FOR ENTERPRISE DOMAINS	32
TO UPLOAD THE CERTIFICATE AND ACTIVATE YOUR DOMAIN	33

---

TO UPDATE YOUR CERTIFICATE	33
TO DEACTIVATE YOUR CERTIFICATE	33
TROUBLESHOOTING	34
<b>SUPPORT USER ACCESS</b>	<b>35</b>
TO CONFIGURE SUPPORT USER ACCESS	35
<b>USAGE STATISTICS AND BILLING</b>	<b>37</b>
TO VIEW USAGE STATISTICS	37
TO EXPORT THE USAGE STATISTICS TABLE	39
Devices count details	39
MICROSERVICE USAGE	39
Billing modes	40
Isolation level	40
Resources usage assignment for billing mode and isolation level	40
Collected values	40
Scaling	41
TIMEZONE HANDLING	41
Examples	42
DAILY ROUTINE	43
LIFECYCLE	43
BILLING PRICING MODELS	45

## INTRODUCTION

An Enterprise tenant offers additional administrative functionality compared to a Standard tenant, the major difference being **multi-tenancy**.

Using an Enterprise tenant, you can:

- Create and manage subtenants.
- Manage the subscribed applications/features of the subtenants.
- Invoice subtenants based on usage statistics.

Moreover, an Enterprise tenant includes the following additional features:

- **Branding** - to configure an individual look & feel.
- **Domain name** - to provide an individual domain name.
- **User hierarchy** - to reflect entities with limited permissions to subsets of shared data.

For details on the Cumulocity tenant concept see [Tenant hierarchy](#).

## MANAGING TENANTS

### MANAGING SUBTENANTS

Using the Enterprise tenant of Cumulocity, you can make use of the tenants functionality which allows you to create and manage subtenants.

#### ✔ REQUIREMENTS

##### APPLICATION ACCESS:

The user must have access to the Administration application of an Enterprise tenant.

##### ROLES & PERMISSIONS:

The user must have at least one permission for the permission type "Tenant management":

- To view all tenants: READ permission.
- To create tenants: CREATE permission.
- To edit tenants (including subscriptions) and to suspend or activate tenants: UPDATE permission.
- To create tenants and perform activity permitted by UPDATE permission: ADMIN permission.

#### ! IMPORTANT

There is a major difference between providing several tenants and providing several users with different permissions within a single tenant. Tenants are physically separated data spaces with a separate URL, with own users, a separate application management and no sharing of data by default. Users in a single tenant by default share the same URL and the same data space. So if your users, for example, are separate customers of yours and you must strictly separate them because they may be competitors, we strongly recommend you to do so by working with tenants. For details on the role-based access approach versus multi-tenancy, see [RBAC versus multi-tenancy approach](#).

### TO VIEW SUBTENANTS

Click **Subtenants** in the **Tenants** menu to view all subtenants available in your account.

The **Tenants** page provides the following information on each subtenant:

- The name of the subtenant, for example, company name of your customer.
- The ID and domain.
- Optionally, a contact name.
- The date when the tenant was created.
- The status of the tenant, either active (indicated by a green checkmark icon ✔) or suspended (indicated by a red cross icon ✗).

#### i INFO

In the Management tenant, you also find a column with information on the parent tenant. The parent tenant is the original tenant that created the subtenants that are listed in the table.

## TO CREATE A SUBTENANT

1. Click **Create tenant** at the right of the top menu bar.

2. Provide the following properties:

Field	Description	Required
Domain/ URL	Enter a subdomain of your choice, for example "acme". The tenant's URL will be "acme.cumulocity.com" on cumulocity.com. You can only use one subdomain level. For example, you can only use "acme.cumulocity.com" on cumulocity.com. You cannot use "mycustomer.acme.cumulocity.com". This is not permitted by the TLS standard. The tenant domain may contain lowercase letters, digits or hyphens (-). It must start with a letter; hyphens are only allowed in the middle; minimum is 2 characters.	Yes
Name	The name of the tenant, for example, the company's name.	Yes
Administrator's email	A valid email address to enable users to reset their password.	Yes
Administrator's username	Username for the administrator of this tenant.	Yes
Contact name	Name of the contact.	No
Contact phone	Phone number of the contact.	Yes
Send password reset link as email	Selected by default. If you deselect this option, you must provide a password and confirm the password (see <a href="#">To change your password</a> for more information on password strength).	No


Field	Description	Required
Tenant policy	You may select a tenant policy to be applied to the tenant from the dropdown list.	No

- Click **Save** to apply your settings.

When the subtenant is created, it gets an auto-generated ID, which cannot be changed. Also, it is automatically provisioned with a first, administrative user ("Administrator's username"). This administrator can create other users and set their permissions. The first user cannot be deleted to prevent you from locking yourself out.

From the Management tenant, you can enable other tenants to create subtenants. Contact your Operations team on how to configure this setting according to your needs.

## TO VIEW OR EDIT SUBTENANT PROPERTIES

Click on the desired subtenant or click the edit icon  at the right of the subtenant entry.

In the **Properties** tab, all fields are editable except of **ID**, **Domain/ URL**, **Administrator's username** and **Administrator's email**. For details on the fields, refer to [To create a subtenant](#).

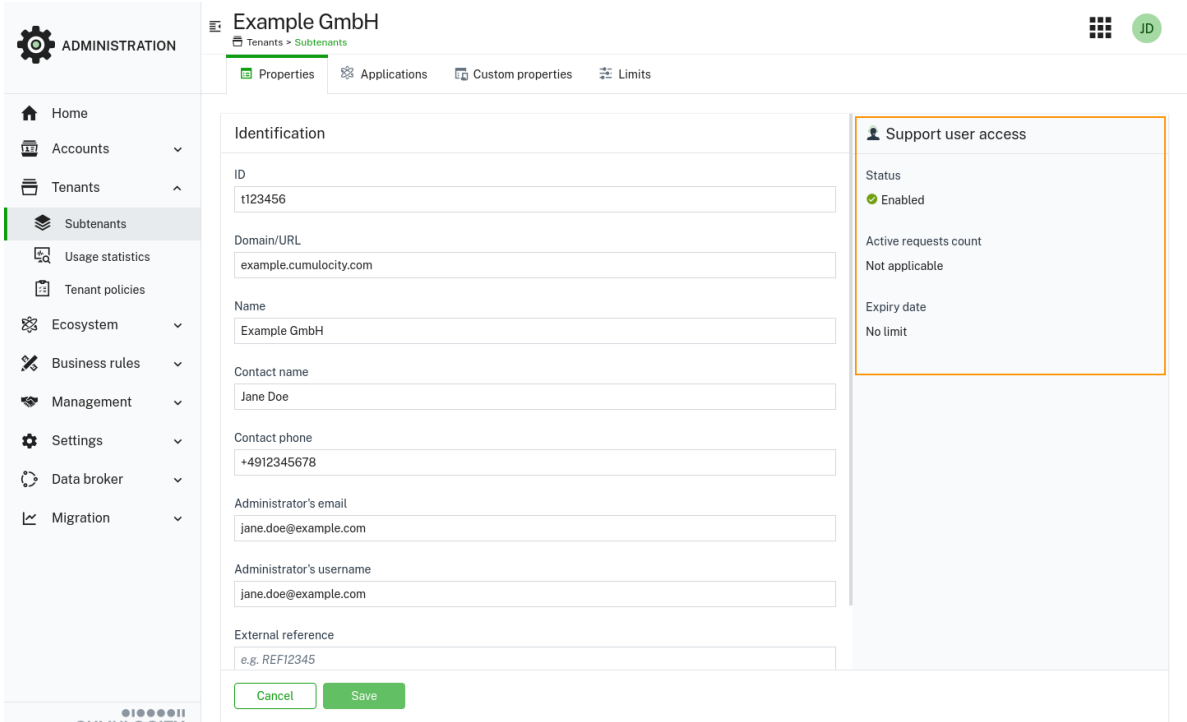
## INFO

The **Administrator's email** may be changed by logging in to the subtenant with the **Administrator's username** and changing the own email.

To change the tenant password, click **Change password**, enter the new password in the upcoming fields and click **Save**.

## Support user access information

At the right of the **Properties** tab, you can find information on the support user requests/access for the subtenants.



The screenshot displays the 'Example GmbH' subtenant management interface. The left sidebar contains navigation links. The main panel shows the 'Properties' tab with various identification and contact details. On the right, a 'Support user access' panel is highlighted with an orange border, showing the status as 'Enabled' and no active requests or expiry date.

The following information is displayed here:



Field	Description
Status	<p>May be either "Enabled" or "Disabled".</p> <p>"Enabled" indicates that:</p> <ul style="list-style-type: none"> <li>- Support user access has been activated globally in the Management tenant.</li> <li>- One or more subtenant users have activated support user access.</li> </ul> <p>"Disabled" indicates that:</p> <ul style="list-style-type: none"> <li>- Support user access has been deactivated globally in the Management tenant.</li> <li>- No subtenant user has currently any active support user access (that means, each support user request has either expired or has actively been deactivated).</li> </ul>
Active requests count	The number of requests currently active in the subtenant. Only displayed if support user access is not enabled globally in the Management tenant. Shown as a number in a small red dot.
Expiry date	Specifies the date on which support user access for the tenant will expire. If no date has been specified, the expiry date is set to "No limit".

## TO SUSPEND A SUBTENANT

Suspending a tenant blocks any access to this tenant, regardless whether the access is from devices, users or other applications. In addition, all its microservices are undeployed, and if the tenant is reactivated all its microservices are re-deployed.

Device-related data continues to be subject of the retention rules and will be gradually removed. The rest of the tenant's data remains in the Operational Store and can be made available later by clicking **Activate**.

Refer to [Lifecycle](#) for details on the billing perspective of suspended tenants.

### ! IMPORTANT

Suspended tenants for all Cumulocity public cloud instances will be automatically deleted after 60 days.

### i INFO

If data broker connectors are configured for a tenant, suspending this tenant results in suspending all its data broker connectors as well.

1. Click the menu icon  at the right of the respective subtenant entry and then click **Suspend**.

The screenshot displays the 'Subtenants' management page. The left sidebar is titled 'ADMINISTRATION' and lists various system components. The main area shows a table of subtenants. The first entry is 'Example GmbH' with ID 't123456', domain 'example.cumulo...', parent tenant 't41579534', contact 'Jane Doe', and creation date '13 Jan 2025, 12:53:00'. The status is 'Active' (green circle), and a 'Suspend' button is highlighted with a red box.

Tenant	ID	Domain	Parent tenant	Contact name	Created	External ref...	Status	
Example GmbH	t123456	example.cumulo...	t41579534	Jane Doe	13 Jan 2025, 12:53:00		Active	Suspend

2. In the resulting dialog box confirm the suspension by clicking **Suspend** and then entering your password.

## INFO


- As part of suspending the tenant, an email is sent to the email address that was configured for the tenant administrator.
- If you are a service provider, you can suppress this email.

## TO DELETE A SUBTENANT

### ! IMPORTANT

Deleting a subtenant cannot be reverted. For security reasons, it is therefore only available in the Management tenant. You cannot delete tenants from any tenant but the Management tenant. Contact your Operations team for further support.

Administrators in Enterprise tenants are only allowed to suspend active subtenants, but not to delete them.

Click the menu icon  at the right of the respective subtenant entry and then click **Delete** to finally delete a tenant and remove all the data of the tenant.

## SUBSCRIBING APPLICATIONS

### OVERVIEW

Cumulocity features an application marketplace that allows tenants to access and manage various applications.

Management tenants and Enterprise tenants can control application access for their subtenants. In the **Applications** tab of a tenant, they can:

- [View and manage existing application subscriptions](#)
- [Subscribe applications to tenants](#)
- [Monitor the microservice status](#)

For general information on applications as part of the Cumulocity ecosystem, refer to [Managing the ecosystem](#).

## INFO

Tenants can also create and deploy their own [custom applications](#), which can be made available to their subtenants.

## TO VIEW SUBSCRIBED APPLICATIONS

In the **Applications** tab of a tenant you can view all subscribed applications, subscribe applications to tenants, or remove the applications from the tenant. By default, the [standard Cumulocity applications](#) are subscribed to the tenant.

A tenant can have multiple available applications as displayed under **Available applications** but to use an application's functionality a subscription to the application must be established for the tenant. The list of subscribed applications is shown under **Subscribed applications**.

## INFO

Alternatively, you can retrieve the list of subscribed applications for a tenant by using the Cumulocity REST API to get [specific tenant information](#). The subscribed applications will be listed under the `applications` fragment.

[To view the application details](#)

Expanding an application entry in the **Available applications** list shows the following details:

- Availability - One of MARKET, SHARED or PRIVATE
- Type - One of HOSTED, MICROSERVICE or EXTERNAL
- Owner - Tenant that owns the application

## TO SUBSCRIBE AN APPLICATION




Hover over the application under **Available applications** at the right and click **Subscribe** on the desired application.

## TO UNSUBSCRIBE AN APPLICATION

Hover over the application under **Subscribed applications** at the left and click **Unsubscribe**.

## TO MONITOR THE MICROSERVICE STATUS

For all applications hosted as microservices by Cumulocity the status of the application is indicated next to its name by symbols. It may be in one of the following states:

-  Microservice is up and running.
-  Microservice is unhealthy.
-  Microservice is down.

You can view details on the status by expanding the respective entry.



The following information is provided:

- Active - the number of active microservice instances.
- Unhealthy - the number of inactive microservice instances.
- Desired - the number of desired microservice instances.
- Name - microservice instance name.
- Restarts - the number of microservice instance restarts.

### INFO

Information on the microservice instance name and the number of restarts is displayed in case of at least one restart.

Further details are provided on the **Status** tab of the respective microservice, see [Monitoring microservices](#).

## CUSTOM PROPERTIES

The **Custom properties** tab allows you to view and edit values of tenant custom properties defined in the [properties library](#). Such properties are also displayed as columns in the [Usage statistics](#) page.

## SETTING LIMITS

The **Limits** tab allows you to view and edit resource limits for the tenant, as well as to assign an “External reference” and to enable/disable the Gainsight product experience tracking.

### TO LIMIT THE SUBTENANT REQUEST RATE

Platform administrators can limit the request rate of each subtenant via the following properties:

- **Limit HTTP queue:** Limit of the HTTP request queue for the tenant.
- **Limit HTTP requests:** Limit of the HTTP requests for the tenant per second.
- **Limit stream queue:** Limit of the MQTT request queue for the tenant.
- **Limit stream requests:** Limit of the MQTT requests for the tenant per second.

The request throttling mechanism is only enabled when both HTTP properties (**Limit HTTP queue** and **Limit HTTP requests**) are configured. If one of the values is omitted, the other one is ignored and throttling remains disabled.

### ! IMPORTANT

Rate limiting can be an effective countermeasure against threats like brute force login attempts, API abuse and request flooding thus reducing the number of malicious/unwanted traffic. This helps in protecting against DoS (Denial of Service) attacks and saving the available bandwidth for legitimate requests.

You can also customize the buffer size for the CEP queue and the data broker queue for a particular tenant. This can be done from the Management tenant. Contact your Operations team on how to configure this setting according to your needs.

### TO LIMIT THE SUBTENANT DEVICE NUMBER

Platform administrators can limit the count of concurrently registered root devices or simply all devices (including child devices) via the property **Limit number of devices**.

You can view the peak number of concurrently registered devices, root devices and the peak value of used storage in the [Usage statistics](#) page.

## PRODUCT EXPERIENCE TRACKING

In the parent tenant, check the checkbox **Enable Gainsight product experience tracking** to enable/disable the product experience tracking through the [Gainsight PX](#) product experience software for the given child tenant.

At the tenant level, you can disable the product experience tracking by Gainsight by turning off the cookie banner on the **Branding** page. For more information, see [Branding](#).

If you activate tracking for the tenant, its users are automatically tracked. However, the nature of this tracking depends on their consent. By accepting tracking, they permit the use of Personally Identifiable Information (PII) for tracking purposes. If they decline, their data is anonymized to ensure privacy, though tracking will still capture usage data without personal identifiers. For more details, see [Accessing and logging into the platform](#).

## TENANT POLICIES

A tenant policy is a set of tenant options and retention rules. Tenant options and retention rules may be specified during tenant creation.

Creating a tenant policy with a specific set of options and rules saves time when creating multiple tenants with the same settings.

**INFO**

The options and rules are copied into the tenant. Editing the policy has no effect on tenants that have already been created.

**IMPORTANT**

Tenant options specified in a tenant policy are **not encrypted**. You should not specify or overwrite tenant options here with a "credentials." prefix, since the platform expects those options to be encrypted with data that will appear after the tenant has been created.

**TO VIEW TENANT POLICIES**

Click **Tenant policies** in the **Tenants** menu to view all available tenant policies.

For each tenant policy, the name, an optional description and the number of options and retention rules is provided, either in a list or a grid.

**TO CREATE A TENANT POLICY**

1. Click **Add policy** in the top menu bar.
2. In the resulting dialog box, enter a name and an optional description.

The screenshot shows the 'New tenant policy' dialog box. On the left is a sidebar with the 'ADMINISTRATION' menu, where 'Tenant policies' is highlighted. The main area contains the following fields and sections:

- Name:** A text input field containing 'New tenant policy'.
- Description:** A text area containing 'New tenant policy description'.
- RETENTION RULES:** A section with a table showing one rule: 'All' (Data Type) with a 'Maximum age' of '10 days'. Below the table is a green button labeled 'Add retention rule'.
- TENANT OPTIONS:** A section with a table showing one option: 'password' (Category) with 'strength.validity' (Key) and 'true' (Value). Below the table is a green button labeled 'Add tenant option definition'.
- At the bottom are 'Cancel' and 'Save' buttons.

The bottom of the sidebar shows the Cumulocity logo and the text 'powered by CUMULOCITY'.

3. Add at least one retention rule. For details on creating retention rules, see [Retention rules](#).
4. Optionally, add a tenant option.
5. Click **Save**.


The tenant policy will be added to the tenant policies list.

**IMPORTANT**


When defining the retention rules and options you can select a checkbox to allow subtenants to modify definitions of these rules or options. By default, this checkbox is not activated. Be aware that if you do not

select this checkbox after creating the subtenant you must run an update from the Management tenant in order to edit those rules and options.


### TO EDIT A TENANT POLICY

Click the respective policy entry or click the menu icon  at the right of the policy entry and then click **Edit**.


In the resulting dialog box, make your edits and click **Save** to save your settings.

To delete a retention rule or a tenant option from a policy, hover over it and click the remove icon .

### TO DUPLICATE A TENANT POLICY

Click the menu icon  in the policy entry you want to duplicate and then click **Duplicate**.

### TO DELETE A TENANT POLICY

Click the menu icon  in the policy entry you want to delete and then click **Delete**.

## DEFAULT SUBSCRIPTIONS

In the Cumulocity platform, you can configure which applications and microservices are subscribed to a tenant on tenant creation. When you create a new tenant, the specified applications and microservices automatically get subscribed to it.

In addition, you can specify which applications and microservices are subscribed to a tenant when the system is upgraded. This list might differ from the default subscriptions on tenant creation. For example, certain default applications might have been unsubscribed from a tenant after creation and you may not want these applications to be subscribed to it again or you may want to subscribe different ones to it.

### TO VIEW DEFAULT SUBSCRIPTIONS

In the **Default subscriptions** page, you can configure two separate lists of applications. These will be subscribed by default to:

- Every new tenant on its creation.
- Every existing tenant on platform upgrade.

#### INFO

These default lists can be overridden for particular subtenants by setting additional tenant options, for example via tenant policy. For details, see [Overriding default subscriptions](#) or the [Tenant API](#) in the Cumulocity OpenAPI Specification.

On the left, the list of subscribable applications (both web applications and microservices) is displayed, which consists of:

- All own applications.
- All subscribed applications which have different names than the own applications.

#### INFO

In order to help you to distinguish which application is owned and which is subscribed, the tenant ID of the

owner is displayed.

On the right, you see the **Subscribed on tenant creation** and the **Subscribed on platform upgrade** columns.

Initially, the lists show the default subscriptions inherited from the tenant hierarchy.

ADMINISTRATION

Home

Accounts

Tenants

Ecosystem

Applications

Extensions

Microservices

Default subscriptions

Business rules

Management

Settings

Data broker

Migration

Default subscriptions

Ecosystem > Default subscriptions

JD

Applications










Configure default subscriptions in the platform, both for tenant creation and for platform upgrade. To display a full list of available applications, override inherited settings.

Subscribed on tenant creation

Override inherited

Subscribed on platform upgrade

Override inherited

 Administration administration	TENANT ID management	<input checked="" type="checkbox"/>	<input type="checkbox"/>
 Advanced-software-mgmt advanced-software-mgmt	TENANT ID management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 Apama-ctrl-smartrulesmt cep	TENANT ID management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 Cockpit cockpit	TENANT ID management	<input checked="" type="checkbox"/>	<input type="checkbox"/>
 Device Management devicemanagement	TENANT ID management	<input checked="" type="checkbox"/>	<input type="checkbox"/>
 Device-simulator device-simulator	TENANT ID management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 Digital Twin Manager digital-twin-manager	TENANT ID management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 Dtm dtm	TENANT ID management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 Feature-cep-custom-rules feature-cep-custom-rules	TENANT ID management	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Save

TO CONFIGURE DEFAULT SUBSCRIPTIONS

You can override both lists by switching the corresponding toggle. This will reveal all available applications (initially, unselected ones are hidden) but the selection will remain the same.

Next, adjust the lists to your needs by selecting additional applications to be subscribed by default or deselect applications you do not want to be subscribed.

You may also deselect all of them if you don't want any subscriptions to be executed on tenant creation and/or platform upgrade.



ADMINISTRATION
 

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

## Default subscriptions

Ecosystem > Default subscriptions

Applications

Configure default subscriptions in the platform, both for tenant creation and for platform upgrade. To display a full list of available applications, override inherited settings.

Subscribed on tenant creation

Override inherited

Subscribed on platform upgrade

Override inherited

Activity activity	TENANT ID: management	<input type="checkbox"/>	<input type="checkbox"/>
Administration administration	TENANT ID: management	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Advanced software mgmt advanced-software-mgmt	TENANT ID: management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Apama-ctrl-smartrulesmt cep	TENANT ID: management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cloud-remote-access remoteaccess	TENANT ID: management	<input type="checkbox"/>	<input type="checkbox"/>
Cockpit cockpit	TENANT ID: management	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Connectivity-agent-server connectivity	TENANT ID: management	<input type="checkbox"/>	<input type="checkbox"/>
Databroker-agent-server databroker-agent-server	TENANT ID: management	<input type="checkbox"/>	<input type="checkbox"/>
Device Management devicemanagement	TENANT ID: management	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Save

If you want to return to the settings inherited from the tenant hierarchy, just switch the corresponding toggle again.

Save the settings by clicking **Save** at the bottom of the page.

## INFO

Obsolete entries not matching any existing applications are removed on save. If an application selected in one of the lists has been removed, it will be silently ignored during tenant creation and/or platform upgrade. If another application with the same name is created afterwards (but before the settings on this page are saved again, which will remove the obsolete entry), the new application will be subscribed instead of the previous one.

## TO OVERRIDE DEFAULT SUBSCRIPTIONS

The default subscriptions can be overridden for subtenants by setting up a tenant policy with the following options:

- To define default web applications subscribed to new tenants on creation:
  - category: configuration
  - key: default.tenant.applications
  - value: comma-separated list of application names, for example, administration,devicemanagement,cockpit,feature-microservice-hosting,feature-cep-custom-rules
- To define default microservices subscribed to new tenants on creation:
  - category: configuration
  - key: default.tenant.microservices
  - value: comma-separated list of microservice names, for example, device-simulator,report-agent,sms-gateway
- To use a different list of web applications to be subscribed to existing tenants on platform upgrade:
  - category: configuration
  - key: on-update.tenant.applications.enabled
  - value: true/false (when false or not set, the same list from default.tenant.applications will be used)
- To define default web applications subscribed to existing tenants on platform upgrade:
  - category: configuration
  - key: on-update.tenant.applications
  - value: comma-separated list of application names, for example, administration,devicemanagement,cockpit,feature-microservice-hosting,feature-cep-custom-rules
- To use a different list of microservices to be subscribed to existing tenants on platform upgrade:
  - category: configuration
  - key: on-update.tenant.microservices.enabled

- value: true/false (when false or not set, the same list from default.tenant.microservices will be used)
- To define default microservices subscribed to existing tenants on platform upgrade:
  - category: configuration
  - key: on-update.tenant.microservices
  - value: comma-separated list of microservice names, for example, device-simulator,report-agent,sms-gateway

## MANAGING USER HIERARCHIES

With user hierarchies you can model the structure of organizational entities in your company which share the same database in Cumulocity platform. These entities can have limited permissions to subsets of the shared data and can manage their own sub-users.

### ✔ REQUIREMENTS

#### SUBSCRIPTIONS:

The tenant must be subscribed to the application "feature-user-hierarchy".

#### APPLICATION ACCESS:

The user must have access to the Administration application.

#### ROLES & PERMISSIONS:


The user must have one or more of "User management" permissions:

- To view all users: READ permission.
- To manage all users: ADMIN permission.
- To create users: CREATE permission. By assigning this permission you can create own sub-users and manage the underlying hierarchy of users.

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

- Global User Manager - Can access and modify the full user hierarchy (all users).
- Shared User Manager - Can create new own sub-users and manage the underlying user hierarchy.

## TO VIEW USER HIERARCHIES

In the **Users** page, user hierarchies are indicated by an arrow left  from the user icon. Clicking on the arrow unfolds the user hierarchy. You can also fold and unfold the entire user hierarchy using the **Expand all** and **Collapse all** links at the right of the top menu bar.

A small number next to the username shows how many direct sub-users a user has. Sub-users are users that can be managed by their respective parent user and that have at most the permissions of that parent user. In the example below, the user "Demo user" has one direct sub-user.

**ADMINISTRATION**

**Users**  
Accounts > Users

Filter users  Filter by global roles

Username and login alias	Name and email	Global roles
Jo john.doe@example.com	John Doe john.doe@example.com	Admin User
Su subuser1@example.com	Subuser One subuser1@example.com	-----

powered by CUMULOCITY

## TO CREATE A SUB-USER

User hierarchies are created by assigning an “owner” to a user. The owner can manage the user. The user can have at most the same permissions as the owner.

1. Select the user in the **Users** page.
2. In the **Owner** field, select the user you want to assign as owner from the dropdown list.
3. Click **Done** to confirm.

**ADMINISTRATION**

**subuser1@example.com**  
Accounts > Users

**Identification**

Username: subuser1@example.com **Status:** ☒ Enabled

Login alias: e.g. joe.doe

Email: subuser1@example.com

First name: Subuser Last name: One

Telephone: e.g. +49 9 876 543 210

Owner: john.doe@example.com

Delegated by: No delegation

**Global roles**

- ☐ Admin User  
Enables administrative permissions. The first user created for the tenant receives this role.
- ☐ Business User  
Can access all devices and their data but has no management permission in the tenant.
- ☐ CEP Manager  
Has full access to all deployed CEP modules and smart rules.
- ☐ Cockpit User  
User to work in Cockpit application. This does not include the access to any device data.
- ☐ Device Management User  
Gives access to bulk operations and Device Management application. This does not include access to any device data.
- ☐ Device User  
A role marker for device users. After registration, a device automatically has this role.
- ☐ Global Manager  
Can read and write all data from all devices.
- ☐ Global Reader  
Can read all data from all devices.
- ☐ Global User Manager  
Can access and edit the full user hierarchy.
- ☐ Reader User  
Can read all data (including users, in contrast to "Global Reader").


powered by CUMULOCITY

## INFO

When creating a new user, the owner is automatically set to the user who is logged in if the logged-in user has only “User management” CREATE permission. The owner can be changed later, but only by a user with “User management” ADMIN permission.

If you want an owner to manage only their sub-users, make sure that the owner does not have a global role with “User management” permission for all users.

### Example


A user A has the role “business”. User A becomes the owner of a new user B. User B can then only get a business role assigned (and not for example an admin role) as the user cannot have higher permissions than the owner. If you try to assign any other role except “business” for user B, then the role will be unavailable for subscription and will be indicated by a warning icon  with a notification that this operation is not permitted.

## TO DELEGATE USER HIERARCHIES TO OTHER USERS


In Cumulocity, users can delegate their user hierarchies and permissions to another user. The delegated user then has the same user management permissions as the user who activated the delegation. To do user management, the delegated user must have CREATE permission for the “User management” permission type, which can be granted by assigning a predefined global role “Shared User Manager” or by assigning a custom global role with this permission.

You may of course also delegate on a temporary basis, for example if you are temporarily unavailable.

### To delegate permissions to a user

Either open the user and click the delegate icon  in the **Delegated by** field, or click the menu icon  at the right of the user entry in the user list and from the context menu, select **Delegate**.

### To undelegate permissions

Remove the delegation in the **Delegate by** field, or click the menu icon  in the user list and from the context menu, select **Undelegate**.

If the delegated user must also manage specific devices, the admin user must assign this device permissions (inventory roles) directly to the intended user. This can be done by using **Copy inventory roles from another user**. For details refer to [Assigning inventory roles to users](#).

## INFO
















Delegation works only inside user management and does not have any implication to other places.

## TROUBLESHOOTING SUB-USERS

In the example below the user cannot change the access to the Administration application, because the owner of the user has no “User management” permission. As a result, the owner user can not assign built-in applications (and the owned user cannot use them).

Application access

SUBSCRIBED APPLICATIONS

	 Digital Twin Manager digital-twin-manager		<div>This application is not accessible by the owner.</div>
	 Feature-branding feature-branding		
	 Feature-broker feature-broker		
	 Feature-cep-custom-rules feature-cep-custom-rules		
	 Feature-fieldbus4 feature-fieldbus4		

## CUSTOMIZING YOUR PLATFORM

With the Enterprise tenant of Cumulocity, you can customize your platform in various aspects and according to your requirements.

Apart from various [configuration](#) settings, you can use your individual [branding](#) and your individual [domain name](#).

Click **Enterprise tenant** in the **Settings** menu to access these settings.

## CONFIGURATION

On the **Configuration** tab, you can configure various properties for your tenant.

### ✔ REQUIREMENTS

#### APPLICATION ACCESS:

Users must have access to the Administration application of the Enterprise tenant.

#### ROLES & PERMISSIONS:

- To view settings: READ permission for the "Options management" permission type
- To manage (create, edit, update) all existing settings: ADMIN permission for the "Options management" permission type

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

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

### i INFO

In some of the properties you can configure email templates for various purposes. Be aware that the corresponding emails are sent with "text/html" as content type.

## PLACEHOLDERS

The following placeholders can be found in the **Configuration** tab:

Placeholder	Description
{host}	The value of this placeholder is "https://" + "<<tenantId>>" + "<<base-domain>>". For example, if "tenantId" is auto-generated, the host will be <a href="https://t12345678.cumulocity.com">https://t12345678.cumulocity.com</a> .

Placeholder	Description
{tenant-domain}	This is the location in which a tenant can be accessed. It is equal to "https://" + "<<tenantDomainName>>". For example, {tenant-domain} can be <code>https://myTenant.cumulocity.com</code> . In case of an Enterprise tenant, the {tenantDomain} placeholders can have different values. An example tenant domain is <code>https://myTenant.myhost.com</code> .
{token}	An automatically generated system token for password reset purposes. When a user requests a password reset, a new random token will be generated. This token will be associated only with the particular user and will allow for a single password reset action. The standard way of using this placeholder is along with the {tenant-domain} property as "{tenant-domain}?token={token}".
{email}	Will be replaced with the email address of the recipient user as stored in the user settings. Some views in the UI recognize this parameter and prefill the respective field with this value, for example, during the process of password reset.
{username}	Will be replaced with the value of the username property specified in the user configuration, see <a href="#">User options and settings</a> .
{binaryId}	Will be replaced with the respective <code>binaryId</code> for the binary artefact to be used in the download link.
{exportApi}	Will be replaced with the respective API in which the error occurred.
{size}	Will be replaced with the storage usage percentage value.

## INFO

The above mentioned placeholders might not be applicable to certain templates. While preparing content, note the information provided in the UI.

## TWO-FACTOR AUTHENTICATION

Under **Two-factor authentication**, you can change the SMS template which is sent to the users.

## SUPPORT LINK

In the **Support link** section, you can provide a URL which is then used as default link for the **Request support** option in the user menu. If you set this value to "false", then the **Request support** option in the user menu will be hidden. If you leave the **Support link** field empty, the URL for the link will be taken from the tenant options. However, an application can override this setting by defining the "supportUrl" application option.

## PASSWORD RESET

In the **Password reset** section you can change all settings related to password reset email templates.

At the top you can select if you want to allow sending emails to unknown email addresses.

In the **Password reset email template** fields, provide an email template to be used when the address is known and one to be used when the address is unknown. The link to reset the password might for example be: {tenant-domain}/apps/devicemanagement/index.html?token={token}&email={email}.

In the **Email subject** field, provide a subject for all password reset related emails.

In the following two fields provide an email template to be used on password change confirmation and a template for the invitation email.

## EMAIL SERVER



In the **Email server** section, you can configure custom email server settings.

In the **Protocol and encryption** field, select a protocol/encryption type from the dropdown list. May be one of:

- SMTP (no encryption): email.protocol=smtp and email.connection.encrypted=false
- SMTP (STARTTLS): email.protocol=smtp and email.connection.encrypted=true
- SMTPS (SSL/TLS): email.protocol=smtps and email.connection.encrypted=true

Provide the host, port, username, password, and sender address for the email server. The empty password configuration is supported for the Enterprise tenant.

## DATA EXPORT

In the **Data export** section, you can set the email subject and email template for data export and specify the **User unauthorized error message**.

## STORAGE LIMIT

In the **Storage limit** section, you can specify the email subject and email template for emails being send *before* data is removed on exceeding the storage limit (warning) and *after* data removal is performed (limit exceeded).

## SUSPENDING TENANTS

In the **Suspending tenants** section, you can provide settings for emails being send on tenant suspension.

At the top you can select if you want to send the email to the suspended tenant's administrator and specify an additional email receiver. Below you set the subject and template for the tenant suspended email.

Click **Save configuration** at the bottom to save your settings.

### INFO

Some additional configuration settings can be specified globally in the Management tenant. Contact your Operations team for further details.

## BRANDING

With the Branding feature, you can fully customize the look of your tenant to your own preferences.

### REQUIREMENTS

#### APPLICATION ACCESS:

The branding feature comes as default with the Enterprise tenant and is available in the Administration application.

The branding functionality is enabled by subscribing to the “feature-branding” application.

#### ROLES & PERMISSIONS:

- To manage and apply the branding configuration:
  - READ, ADMIN permission for the “Application management” permission type

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

above-mentioned permissions:

- **Tenant Manager** - manages tenant-wide configurations like applications, tenant options and retention rules

## TO CONFIGURE BRANDING SETTINGS

In the **Branding** page, you can maintain multiple branding variants. One of the branding variants is always configured as the global branding. The global branding will by default apply to all apps on your tenant and your subtenants.

The screenshot shows the 'Branding' page in the administration interface. The left sidebar contains the 'ADMINISTRATION' menu with options like Home, Accounts, Tenants, Ecosystem, Business rules, Management, Settings, Authentication, Remote access, Application, Properties library, Enterprise tenant, SMS provider, Branding (selected), Connectivity, Localization, and Data broker. The main content area displays a table of branding variants. The table has columns: Name, Applied to, Owner, and Last updated. There are two variants: 'default' (Global) and 'custom' (Cockpit, Device Management). The 'default' variant is the global branding. The 'custom' variant is applied to specific applications. The table also shows the owner 'john.doe@example.com' and the last updated time '1 Sept 2024, 12:10:00' and '1 Sept 2024, 12:12:00'.

Name	Applied to	Owner	Last updated
default	Global	john.doe@example.com	1 Sept 2024, 12:10:00
custom	Cockpit, Device Management	john.doe@example.com	1 Sept 2024, 12:12:00

In addition to the global branding, there can also be branding variants that apply only to specific applications. This allows to brand applications differently.

For each branding variant, you can configure various parameters like logos, colors and font types used throughout the platform. The [parameters](#) can be configured through the multiple tabs available on the **Branding** page. Most of the parameters are immediately applied to your current window as a preview.

If you want to make changes to one of your branding variants, we recommend you to duplicate the corresponding branding variant first and to make your changes on the duplicated variant as any saved changes would immediately be applied. This way you can review and edit the preview of your branding variant first across all applications before it is set as global branding and/or applied to your target applications.

To edit a branding variant you can configure the following tabs:

- **Generic:** Allows you to change generic parameters of your branding that are the same across all themes.
- **Light theme:** Allows you to edit the branding parameters for the light theme.
- **Dark theme:** Allows you to edit the branding parameters for the dark theme. The dark theme support needs to be enabled first in the **Generic** tab.
- **Custom CSS:** Allows you to customize the looks of your applications even more by providing your own Cascading Style Sheets.
- **Advanced branding:** Allows you to make direct changes to the branding JSON object via a text editor. This can be useful to set some of the [ApplicationOptions](#) the [Web SDK](#) provides which are not immediately supported by the branding editor.

For a more detailed preview of your settings, click **Open preview** to check the look and feel of your branding settings in the overall platform. You may interact and even switch applications in the preview. Every change that you make in the **Branding** page is immediately applied to the **Preview** page after you click **Save**.

Click **Save** at the bottom to save your final branding settings to your tenant. This applies them to the places your branding variant applies to.

To revert back to the default settings, click **Delete all variants** in the in the top menu bar. With this action all branding variants are deleted. We therefore recommend you to export your existing variants beforehand.

## EDITING PARAMETERS

Each branding parameter can be configured in multiple ways.

### Generic tab

In the **Generic** tab, you can edit the generic settings of your branding variant that will apply to all of your branding themes.

The screenshot shows the 'default -- Generic' branding configuration page. The sidebar on the left lists various administration settings, with 'Branding' selected. The main content area is divided into three sections: 'Title & favicon', 'Dark theme', and 'Typography'. The 'Title & favicon' section includes a 'Title' input field and a 'Favicon' selection area. The 'Dark theme' section has a toggle for 'Enable dark theme support'. The 'Typography' section includes 'Base typography' and 'Headings & navigator' sub-sections. The 'Base typography' section has a 'Fonts URL' input field and a 'Base font stack' input field. The 'Headings & navigator' section has a 'Headings font stack' input field, a 'Navigator font stack' input field, and radio buttons for 'Match base font stack' and 'Match headings font stack'. At the bottom of the main area are four buttons: 'Cancel', 'Save', 'Open preview', and 'Set as global'.

Under **Title & favicon**, specify the following items:

- The title: This is displayed in the browser's address bar.
- The favicon: This is displayed in the browser's address bar. Click **Select** to select a file from your file system. The supported favicon format is ICO.

### Dark theme

Here you can enable the dark theme support on this branding variant. If enabled, the **Dark theme** tab is available.

### Typography

under **Typography** you specify the font settings for your brand variant.

You can select your base and headings font stack, and select an option for the navigator font stack. This is either same as base or same as headings font. You can also add a link to existing remote fonts to be used.

### Cookie banner

Under **Cookie banner** you specify the settings for the banner with the cookie usage information. If not disabled here, the banner is shown for all users of the current tenant and all subtenants until a user clicks **Agree and proceed**.

If you disable the cookie banner, this also disables the product experience tracking by Gainsight for the current tenant and all subtenants.

The following parameters can be specified:

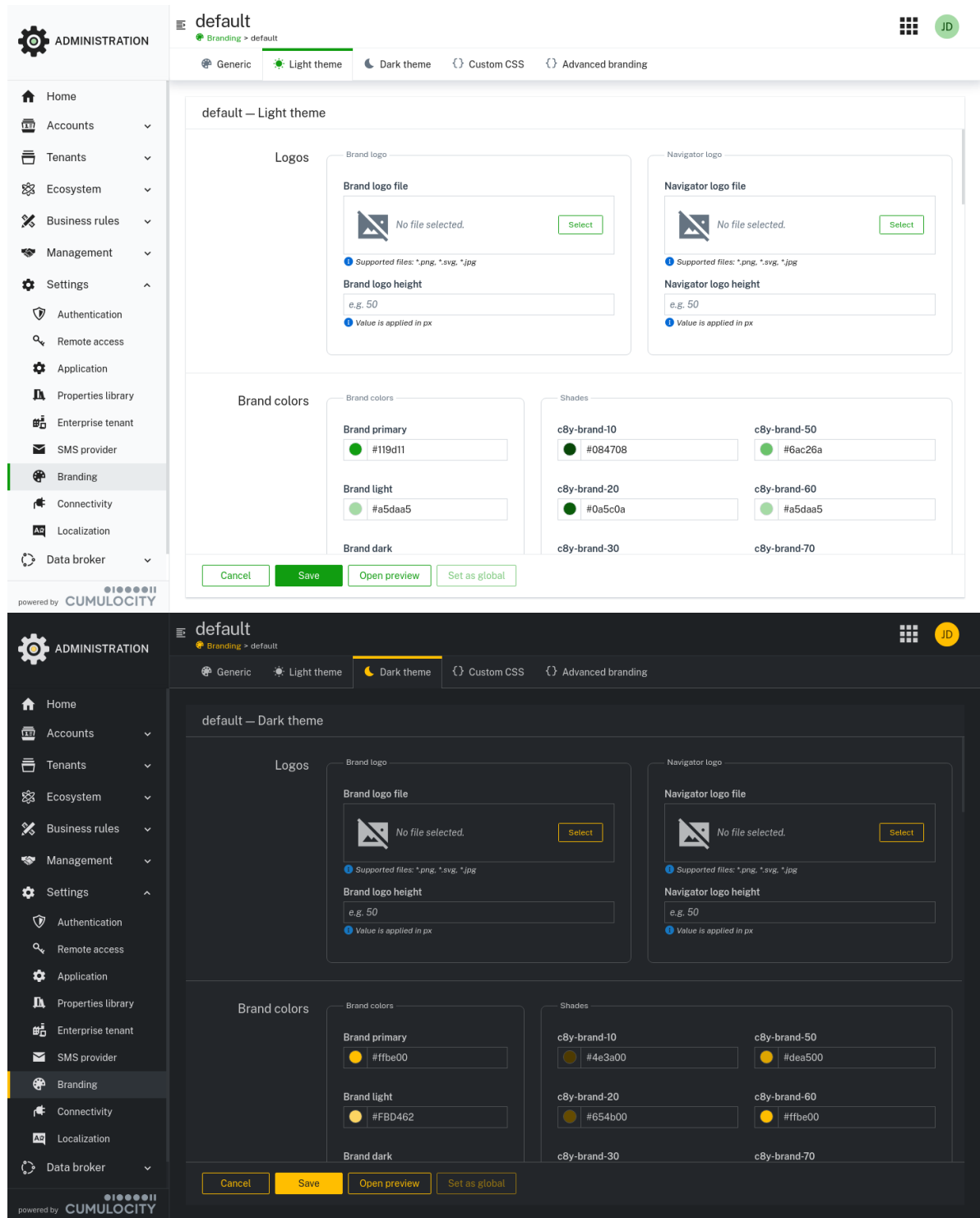
- Title: Cookie banner title.
- Text: Cookie banner text with a general statement on the cookie usage and the use cases for it.
- Link to privacy policy: A link to the page with the privacy policy.
- Version of privacy policy: A version of the privacy policy (for example, a date). In case the version changes, the consent of all

existing users is invalidated.

### Light & dark theme tab

The same set of parameters is available for both the light and the dark theme and can be changed in the corresponding tabs. Further details regarding these parameters can be found in the [Branding](#) and [Color palette](#) sections of the Codex.

The theme switcher in the right drawer allows you to switch between the light and dark theme, once you enable the dark theme on your branding variant.



### Logos

Under **Logos**, specify the following items:

- Your brand logo: This shows during the application loading. Click **Select** to select a file from your file system. The supported formats are PNG, SVG and JPG.

- The brand logo height.
- Your navigator logo: This is located on top of the navigator panel. Click **Select** to select a file from your file system. The supported formats are PNG, SVG and JPG.
- The navigator logo height.

#### Brand colors

In the **Brand colors** section you specify the colors you like to use in the branding variant.

You can configure the following parameters by providing a HEX, RGB or RGBA value:

- Brand primary.
- Brand light: Mainly used for two-color icons.
- Brand dark: Mainly used for two-color icons.
- A set of 8 shades that you can generate based on your brand primary color. To generate the shades click **Reset shades**. The shades are used in various locations in the different applications.

#### Status colors

In the **Status colors** section you specify the colors used to display the different statuses.

For each status (**Info**, **Warning**, **Danger** and **Success**) you can provide three colors ("default", "light" and "dark").

#### Generic

In the **Generic** section you specify the colors used in generic places.

The following parameters can be specified by providing a HEX, RGB or RGBA value:

- Body background color
- Text color
- Text muted color
- Link color
- Link hover color

In addition, you can also specify the **Button border-radius**.

#### Action bar

In the **Action bar** section you specify the parameters for the action bar.

The following parameters can be specified by providing a HEX, RGB or RGBA value:

- Background color
- Text color
- Icon color
- Button color
- Button hover color

#### Main header

In the **Main header** section you specify the parameters for the main header.

The following parameters can be specified by providing a HEX, RGB, or RGBA value:

- Background color
- Text color
- Button hover color

#### Navigator

In the **Navigator** section you specify the parameters for the navigator.

The following parameters can be specified by providing a HEX, RGB, or RGBA value:

- Background color
- Text and buttons color
- Separator color
- Header background color
- Title color
- Active background color: Background color of the current item in the navigator

- Active border color: Border color of the current item in the navigator
- Active text color: Text color of the current item in the navigator

#### Right drawer

In the **Right drawer** section you specify the parameters for the right drawer.

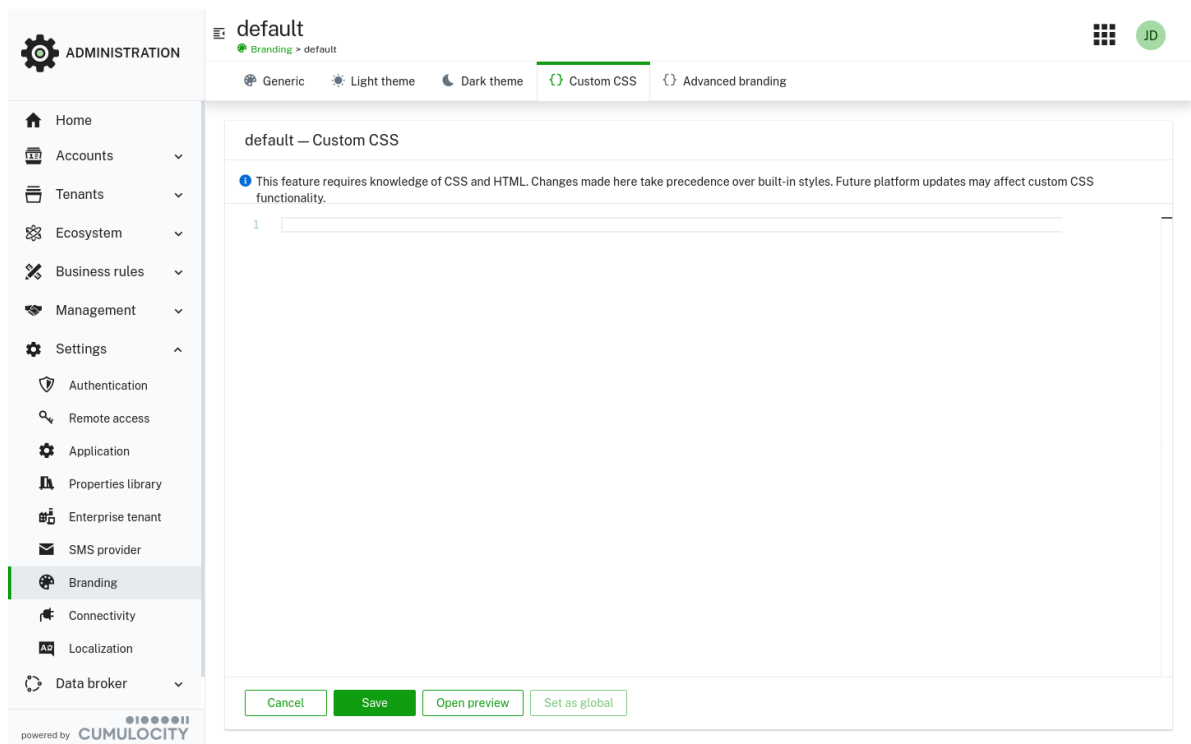
The following parameters can be specified by providing a HEX, RGB or RGBA value:

- Background color
- Text color
- Text muted color
- Separator color
- Link color
- Link hover color

#### Custom CSS

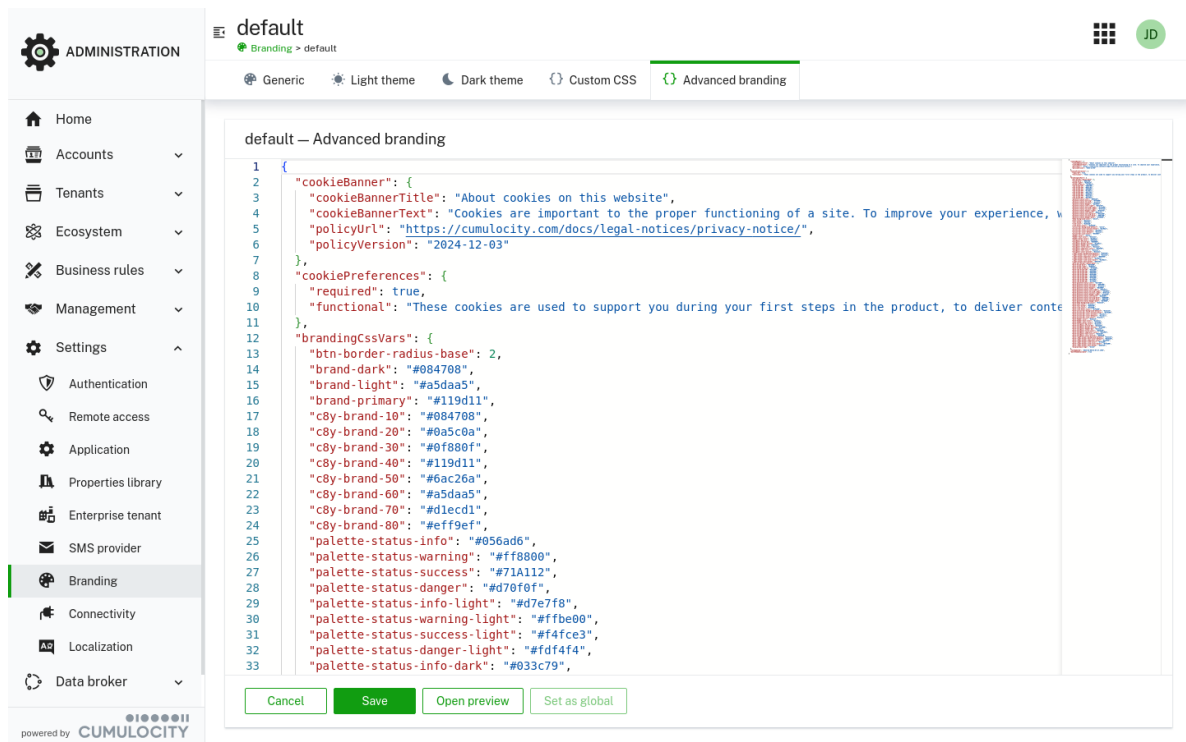
The **Custom CSS** tab allows to customize the looks of your applications even more by providing your own Cascading Style Sheets.

You can utilize this to change colors for locations that have not been covered by the dialog window provided in the [Light/Dark theme](#) tab.



#### Advanced branding

The **Advanced branding** tab allows to make direct changes to the branding JSON object, which is usually filled by the other tabs behind the scenes, via a text editor. This can be useful to set some of the [ApplicationOptions the Web SDK provides](#) which are not immediately supported by the forms the branding editor includes. More details regarding these options can also be found within [Developer Codex](#).



## DOMAIN NAME

A key feature of the Enterprise tenant is the ability to operate the Cumulocity platform using a custom domain name. This means that you can configure the platform to serve you and your customers using a host name of choice, for example \*.iot.mycompany.com rather than the default URL of Cumulocity. In addition you'll be able to create subtenants using your domain. These will be using **<subtenantName>.iot.mycompany.com** as their host names.

### 🔒 REQUIREMENTS

#### APPLICATION ACCESS:

The domain management feature comes as default with the Enterprise tenant and is available in the Administration application.

The domain management functionality is enabled by subscribing to the "sslmanagement" microservice.

#### ROLES & PERMISSIONS:

- To upload certificate:
  - READ, ADMIN permission for the "Inventory" permission type;
  - READ, ADMIN permission for the "Options management" permission type;
  - READ, ADMIN permission for the "Application management" permission type;

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

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

#### PREREQUISITES

There are three prerequisites for using a custom domain:

1. To activate your domain, a valid license that covers your wildcard domain is required. Please contact [product support](#) to install a license for your domain.
2. You've obtained a valid wildcard SSL certificate for your IoT domain, for example a certificate for *\*.iot.mycompany.com*.
3. There is a valid DNS configuration for your domain which ensures that all requests to *\*.iot.mycompany.com* are routed to Cumulocity. (see below).

## SSL CERTIFICATE REQUIREMENTS

The following criteria must be met by any SSL certificate to be used with the Enterprise tenant feature:

- The certificate is currently valid and has not expired. More specifically, `validFrom` points to a point in time in the past, and `validTo` to a point in the future.
- The certificate has been issued by a well-established certificate authority (CA). Self-signed certificates are explicitly not supported.
- The certificate is a wildcard certificate issued for your domain *\*.iot.mycompany.com*. The use of a wildcard certificate is mandatory, as it will also be used for subdomains created from your Enterprise tenant.
- Every single certificate in the chain is provided using the X509 format.
- The common name (CN) in the subject of the primary certificate (the first one in the chain) holds the value of your wildcard domain name, for example, "CN=\*.iot.mycompany.com".

Cumulocity supports a single certificate that is signed by the root CA, as well as a full chain certificate which contains one or more intermediate certificates.

## INFO

The custom domain name functionality is only available for Cumulocity cloud installations or on-prem installations which don't use a custom load balancer.

## TO PACKAGE THE SSL CERTIFICATE IN PKCS #12

In order to use an SSL certificate with Cumulocity, the certificate together with its private key must be uploaded to the platform in a single file, using the PKCS #12 file format.

Most certificate authorities deliver their certificates and corresponding private keys in the PEM file format, using two separate text files for the certificate chain and the private key. Make sure that the private key is not protected with a password/passphrase.

Such PEM files can easily be repackaged into #PKCS #12 using [OpenSSL](#). In the following example, OpenSSL is used to combine a certificate chain (*chain.cert*) and the corresponding key (*privkey.pem*) into a PKCS #12 keystore file (*out\_keystore.p12*) that can be used with Cumulocity.

```
openssl pkcs12 -export -out out_keystore.p12 -inkey privkey.pem -in cert.pem -certfile chain.pem
```

## DNS REQUIREMENTS FOR ENTERPRISE DOMAINS

The DNS entries for your custom domain must be configured in a way that all requests are routed to the Cumulocity platform.

We **strongly recommend** you to use a wildcard CNAME entry for this purpose. The CNAME must contain your wildcard domain from the certificate in the NAME field. The VALUE field of the CNAME entry must point to the hostname of Cumulocity. This target hostname can be easily determined by looking at your current tenant URL. If your tenant URL is *http://mytenant.cumulocity.com*, the target hostname is *mytenant.cumulocity.com*. Please also make sure to delete any conflicting A entries.

### Example:

If you want to use *\*.iot.mycompany.com* for your enterprise subtenants and if you're using the Cumulocity at *mytenant.cumulocity.com*,



the following CNAME entry must be added to your DNS zone:

NAME	TYPE	VALUE
-----		
*.iot.mycompany.com.	CNAME	mytenant.cumulocity.com.

We highly discourage any use of alternative DNS configurations for the following reasons:

- *Wildcard A entries* take the IP address of the platform in the value field and hence redirect all requests based on the given IP rather than a hostname. This results in major problems if the IP address of the IoT platform should change in the future.
- *Singular A entries or singular CNAME entries* instead of DNS wild cards require a single DNS entry for each enterprise domain being created. This is very error prone and prevents the creation of subtenants without always tampering with DNS settings.

## TO UPLOAD THE CERTIFICATE AND ACTIVATE YOUR DOMAIN

Once the DNS configuration is in place and if a certificate with the given requirements is available, it can be easily uploaded to the platform.

On the **Domain name** tab in the **Enterprise tenant** page, click **Upload certificate**. Select the certificate from your file system and click **Upload**.

Afterwards, you can activate the domain with a single click on its name. After the domain has been activated, you will be redirected to your Enterprise tenant using the new domain name. You will also receive an email with information about the activation. Note that your Management tenant domain name is static, for example, if your wildcard domain is “\*.iot.mycompany.com” then your Management tenant domain will be “management.iot.mycompany.com”.

### INFO

After the activation is completed you will no longer be able to access your tenant with the Cumulocity domain name. Instead, use your custom domain name.

## TO UPDATE YOUR CERTIFICATE

When your certificate expires, you must update your certificate with a new one with an extended validation period. When updating a certificate, you must make sure that the certificate meets the following requirements:

- It is valid, like when being uploaded for the first time.
- It is currently valid (validFrom in the past and validTo in the future).
- It has exactly the same common name (domain name) as the currently active certificate.

### INFO

Keep in mind that after replacing the certificate it may take some minutes until the new certificate has been delivered to the users/browsers.

## TO DEACTIVATE YOUR CERTIFICATE

If you wish to return to your old domain at Cumulocity, you can simply deactivate your certificate.

### IMPORTANT

Use with care. Your customers will not be able to access their subtenants anymore.

## TROUBLESHOOTING

In case you cannot reach Cumulocity using your custom domain, we recommend you to perform the following checks to verify your DNS setup.

### Check if the DNS entry is correct

Execute the following command:

```
host management.<your domain name>
```

The following result should be returned:

```
management.<your domain name> is an alias for <instance domain name>
<instance domain name> has address <ip address>
```

### Check if the API is responding

Execute the following command:

```
curl -v -u '<tenant ID>/<your user>:<your password>' --head http://management.<your domain name>/inventory/managedObjects
```

The following result should be returned:

```
...
HTTP/1.1 200 OK
...
```

## INFO

Keep in mind that after changing the DNS entry it might take up to 24 hours until the new entry has been propagated.

## SUPPORT USER ACCESS

### ✔ REQUIREMENTS

To allow support users to log in as a user of your tenant, **support user access** must be enabled. This option is available at tenant level and applies to all users of the tenant.

The support user access feature enables Cumulocity platform providers (Cumulocity in case of the public cloud instances or service providers in case of individual on-prem installations) to support their customers by accessing their users using a support user. A support user is a user in the Management tenant that has specific permissions, that is, to access subtenant users in case of any issues.

### ✔ REQUIREMENTS

To use this feature, support user access must be configured and the required support users must be created in the Management tenant. Contact your Operations team on how to configure this feature according to your needs.

On the Cumulocity public cloud instances, the support user functionality can only be used by the Cumulocity team for providing customer support. It is not available for Enterprise tenant customers to support their customers/subtenants.

## TO CONFIGURE SUPPORT USER ACCESS

Support user access can either be:

- Activated for all subtenants by default.
- Deactivated for all subtenants, but explicitly be enabled by a user for their tenant.

This is configured globally in the Management tenant. Contact your Operations team on how to configure the settings according to your needs.

If activated globally, the support user can log in to all allowed subtenants as any user without restriction.

If deactivated globally, support user access can still be enabled by a subtenant user if required. This is done by clicking **Enable support** in the **User** menu, see [User options and settings](#). The support access is not restricted to the user who activated it but applies to all users of the tenant. This is necessary for retracing of role/right issues.

After a user has activated support access, the menu item changes to **Disable support**, so that the user can disable a pending support request which has been resolved actively before it expires.

### i INFO


If you don't see either the **Enable support** or **Disable support** button in the **User** menu, support user access has been activated globally. Contact [product support](#) or your Operations team for more details.

If a user with tenant management admin permission disables the support request, *all* support requests for the tenant will be disabled.

The duration of the active support request can be globally configured in the Management tenant (default is 24 hours). Contact your Operations team on how to configure this setting according to your needs.

Each new support request will prolong the support duration for the specified number of hours. After the last support request in a subtenant has expired or has been actively disabled by the user, the support user access for the subtenant will immediately be disabled (if not activated globally).

Details on the status of support requests and support user access for a tenant can be found in the **Properties** tab of the tenant, see [Managing tenants](#).

 > Enterprise tenant > Support user  
access

# USAGE STATISTICS AND BILLING

## TO VIEW USAGE STATISTICS

### ✔ REQUIREMENTS

#### APPLICATION ACCESS:

The user must have access to the Administration application of a Management tenant or an Enterprise tenant.

#### ROLES & PERMISSIONS:

- To view tenants usage statistics: READ permission for the permission type “Tenant management”.

The **Usage statistics** page provides statistical information on each subtenant.

ADMINISTRATION

Home

Accounts

Tenants

Subtenants

Usage statistics

Tenant policies

Ecosystem

Business rules

Management

Settings

Data broker

Migration

Usage statistics 1 tenant

Tenants > Usage statistics

01/01/202502/01/2025ApplyClear

Export CSVReload

TENANT	ID	DOMAIN	API REQUESTS	DEVICE API REQUESTS	STORAGE (MB)	PEAK STORAGE (MB)	ROOT DEVICES
Example GmbH	t123456	example.cumulocity.com	41799	28	41.16	41.16	3

powered by CUMULOCITY

The following information is provided for each subtenant (not completely visible in the screenshot above due to space restrictions):

Field	Description
ID	ID of the subtenant
Tenant	Name of the subtenant
API requests	Total number of API requests, including requests from devices and applications

Device API requests	Number of API requests from devices
Storage (MB)	Amount of data stored in your account
Peak storage (MB)	Peak value of storage
Root devices	Number of root devices excluding child devices, see also <a href="#">Devices count details</a>
Peak root devices	Peak number of root devices, excluding child devices
Devices	Total number of devices connected to the subtenant, including child devices
Peak devices	Peak number of devices, including child devices
Endpoint devices	Leaf machines, without gateways and edges
Subscribed applications	Number of applications that the subtenant is subscribed to
Creation time	Date and time of the creation of the subtenant
Alarms created	Number of alarms created
Alarms updated	Number of updates on alarms
Inventories created	Number of managed objects created
Inventories updated	Number of updates on managed objects
Events created	Number of events created
Events updated	Number of updates on events
Measurements created	Number of measurements created
Operations created	Number of operations created
Operations updated	Number of updates on operations

Total inbound transfer	Sum of all inbound transfers (alarms created, alarms updated, events created, events updated, inventories created, inventories updated, measurements created, operations created, operations updated)
CPU (M)	Microservice CPU usage, specified in CPU millicores, see <a href="#">Microservice usage</a> for details
Memory (MB)	Microservice memory usage, see <a href="#">Microservice usage</a> for details
Parent tenant	Name of the parent tenant (available only for Management tenant)
External reference	This field is for individual usage, for example, you can add a link to the CRM system here or an internal customer number


Moreover custom properties are displayed, if configured.

Custom properties may be defined in the [properties library](#) and then set their values in the [Custom properties](#) tab of the tenant.

You can filter the usage statistics list for a time period by adding the start and end date in the top menu bar and click **Apply**. The **Usage statistics** page will show the numbers for all subtenants for this time period.

## INFO

If a tenant was created after the selected time period, it will show up but the numbers are "0".

You can also filter and sort the list on any column by clicking the filter icon  next to the column name and providing the filtering criteria. See also [Filtering](#).

## IMPORTANT

The date/time range used here might differ from your server time due to different time zones.

## TO EXPORT THE USAGE STATISTICS TABLE

1. Click Export CSV at the right of the top menu bar to export the current view of the statistics table to a CSV file.
2. In the resulting dialog box you can customize the CSV output by specifying a field separator, decimal separator and charset.
3. Click **Download** to start the export.

The CSV file will be downloaded to your file system.

### Devices count details

The device count calculations assume that only top-level devices are marked with the [device marker](#) fragment `c8y_IsDevice`. Accordingly, the following formulas are used in the calculations:

- root devices - all devices with the `c8y_IsDevice` fragment
- all devices - all devices with the `c8y_IsDevice` fragment and their children from the whole device hierarchy
- leaf devices - only leafs of the device hierarchies starting from devices with the `c8y_IsDevice` fragment

If child devices are also marked with the `c8y_IsDevice` fragment, the calculation results may look different than expected.

## MICROSERVICE USAGE

The microservice usage feature gathers information on the resource usage per subtenant for each microservice. This enables Enterprise

tenants and service providers to charge tenants not only based on subscriptions but also based on resources usage.

### Billing modes

Cumulocity offers two billing modes:

- **Subscription-based billing** - charges a constant price when a tenant is subscribed to a microservice while resource usage is assigned to the owner.
- **Resource-based billing** - exposes the number of resources used by a microservice to calculate billing.

The billing modes are specified per microservice in the [microservice manifest](#) and are set in the field "billingMode".

**RESOURCES:** Sets the billing mode to resources-based. This is the default mode and will be applied to all microservices that are not explicitly switched to subscription-based billing mode.

**SUBSCRIPTION:** Sets the billing mode to subscription-based.

### Isolation level

Two isolation levels are distinguished for microservices: per-tenant isolation and multi-tenant isolation.

In case of subscription-based billing, the entire resources usage is always assigned to the microservice owner, independent of the isolation level, while the subscribed tenant will be billed for the subscription.

In case of resources-based billing, charging depends on the isolation level:

- Per-tenant - the subscriber tenant is charged for used resources.
- Multi-tenant - the owner of the microservice is charged for used resources.

In case of multi-tenant isolation level, the owner of a microservice (for example the Management tenant of an Enterprise tenant or a service provider) is charged for the used resources of the subtenants. The subtenants should be charged based on the subscription according to the agreement between the microservice owner and the subscribed tenant. The list of subscribed applications is available as part of the [tenant applications](#) as `subscribedApplications`.

### Resources usage assignment for billing mode and isolation level

Billing mode	Microservice Isolation	Resources usage assigned to
Subscription-based	Per-tenant	Owner
Subscription-based	Multi-tenant	Owner
Resources-based	Per-tenant	Subscriber
Resources-based	Multi-tenant	Owner

### Collected values

The following values are collected on a daily base for each tenant:

- CPU usage, specified in CPU millicores (1000m = 1 CPU)
- Memory usage, specified in MB

Microservice resources are counted based at limits defined in the microservice manifest per day. At the end of each day, the information about resource usage is collected into the tenant statistics. It is also considered that a microservice might not be subscribed for a whole day.

### Example

If a tenant was subscribed to a microservice for 12h and the microservice has 4 CPU and 4 GB of memory it should be counted as 2000 CPU millicores and 2048 MB of memory.

For billing purposes, in addition to CPU usage and memory usage the cause for the billing is collected (for example owner, subscription



for tenant):

```
{
  "name": "cep",
  "cpu": 6000,
  "memory": "20000",
  "cause": "Owner"
},
{
  "name": "cep-small",
  "cpu": 1000,
  "memory": "2000",
  "cause": "Subscription for tenant"
}
```

The information on the microservice usage is presented in the **Usage statistics** page.

The screenshot displays the 'Usage statistics' page for a single tenant. The left sidebar contains the 'ADMINISTRATION' menu, with 'Usage statistics' selected. The main content area shows a table with the following data:

TOTAL INBOUND TRANSFER	CPU (M)	MEMORY (MB)	ENABLE GAINSIGHT PRODUCT EXPERIENCE TRACKING	EXTERNAL REFERENCE	LIMIT CEP SER
0	30000	32220			

The 'CPU (M)' and 'MEMORY (MB)' columns are highlighted with orange boxes. The top of the page includes filters for dates (01/01/2025 to 02/01/2025) and buttons for 'Apply' and 'Clear'. The bottom of the page shows the 'powered by CUMULOCITY' logo.

For more details, refer to [Tenants](#) in the Cumulocity OpenAPI Specification. Note that details are available only for daily usage. For a summary query only the sum of all issued requests is returned.

### Scaling

Auto-scaling monitors your microservices and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. It is easy to configure the microservice scaling by setting the property `scale` in the [Microservice manifest](#).

For instance, when you have a microservice with scale policy set to AUTO and the CPU usage points that it is needed to start a new microservice instance for three hours, the billing logs:  $(24/24 + 3/24) * \text{consumed resources}$ .

- 24/24 - one instance active for the whole day
- 3/24 - second instance active only three hours

Note that an audit record is created for every change of the number of instances.

For more information, refer to [Audits](#) in the Cumulocity OpenAPI Specification.

### TIMEZONE HANDLING

## ❗ IMPORTANT

Cumulocity platform servers by default work at UTC timezone. Other time zones are also supported by the platform and can be selected by the service provider at installation time. Thus, the general metering functionality is also guaranteed for non-UTC server time zones.

The tenant usage statistics are collected on a daily base according to the beginning of day ( **BOD** ) and the end of day ( **EOD** ), which are defined by the server timezone. As a result, if the local time zone of a user is different from the server timezone, an operation triggered by the user may be assigned to a different day according to the server time.

### Examples

#### Request counting - Example 1

	Device	Server
Time zone	CEST +2h	UTC
Send measurement time	26.08.2020T01:30:00+02:00	25.08.2020T23:30:00Z

#### Result:

The request will be billed to the day 25.08.2020 as this is the server time of the request handling.

#### Request counting - Example 2

	Device	Server
Time zone	UTC	UTC
Send measurement time	26.08.2020T01:30:00Z	26.08.2020T01:30:00Z

#### Result:

The request will be billed to the day 26.08.2020 as the server time is the same as the device time.

#### Microservice resource billing - Example 1

	User	Server
Time zone	CEST +2h	UTC
Subscribe time	26.08.2020T12:00:00+02:00	26.08.2020T10:00:00Z
Unsubscribe time	27.08.2020T12:00:00+02:00	27.08.2020T10:00:00Z

#### Result:

The resources will be assigned mainly to the day 26.08.2020 as according to the UTC time zone the microservice was active for 14 hours that day and for 10 hours the next day. This might be a bit different from what a user expects as from his perspective the microservice was active for 12 hours each day.

#### Microservice resource billing - Example 2

	User	Server
Time zone	KI +14h (Kiribati Islands)	UTC
Subscribe time	26.08.2020T12:00:00+14:00	25.08.2020T22:00:00Z
Unsubscribe time	26.08.2020T20:00:00+14:00	26.08.2020T06:00:00Z

**Result:**

From the user perspective the microservice was subscribed for 8 hours at 26.08.2020 but at server time it was 2 hours before EOD of 25.08.2020 and 6 hours after BOD at 26.08.2020.

## Microservice resource billing - Example 3

	User	Server
Time zone	CEST	AS -11h (American Samoa)
Subscribe time	26.08.2020T12:30:00+2:00	25.08.2020T23:30:00Z
Unsubscribe time	26.08.2020T13:00:00+2:00	25.08.2020T24:00:00Z

**Result:**

In this case we have a big time shift between the server and the user time. All resources will be billed to the day 25.08.2020 according to the server time.

**DAILY ROUTINE**

Usage statistics consist of values that are progressive like the request count and values that are snapshots of a state at a given time period. In case of the second type of data, values are refreshed several times each day but the value from EOD is the value that is assigned for the given day.

Value type	Refreshed
Request count flush	Every 5 minutes
Used storage	9, 17 and EOD
Device count	9, 17 and EOD
Subscribed applications	9, 17 and EOD
Microservice resources	9, 17 and EOD

**LIFECYCLE****Tenant**

A Cumulocity platform tenant can have several states:

- Active - the common state when the tenant can interact with the platform. In that state all billing values are stored and updated.
- Suspended - suspended tenants are not billed for request count and microservice resources, the only value that is still counted is the existence of the tenant and the storage size. The microservice resource usage is billed as "used", that means, when the tenant is switched to suspended state all microservices are stopped so there are no resources to bill.
- Deleted - this is the point of no return. The tenant is not billed for any resources but there is no way of restoring the data also.

## Microservice

Any extension deployed to the platform as a microservice is billed as “used” and the billing starts according to the begin of usage. After the application is subscribed to the tenant a process of application startup is triggered which will go through several high level phases:

- Pending - the microservice has been scheduled to be started but the Docker container is not running yet. In this state the microservice is not yet billed.
- Scheduled - the microservice has been assigned to a node, the Docker container initialization has been started. The resources for the microservice have already been allocated so billing is started.
- Not ready - the microservice container is not ready yet to handle incoming traffic but the application is already running.
- Ready - the microservice container is ready to handle incoming traffic. “Ready” is resolved based on liveness and readiness probes defined in the [microservice manifest](#). If probes are not defined then the microservice is immediately ready.

A tenant that is billed for resources can view the point in time when the microservices billing has been changed in [the audit logs](#). The audit log entries, for example “Scaling application ‘...’ from X to Y instances” contain the information about the changes of instances and resources consumed by the microservice.

Tenants should also be able to see the full application lifecycle in the application details. In the **Status** tab, you can see an **Events** section that is showing very low level stages of the application startup. Some of the most important are:

- **Pod "apama-ctrl-starter-scope-..." created.** - a new microservice instance has been scheduled to be started for the tenant. This means that the resource allocation has been successful but the application is not running yet (maps to the state “Scheduled”).
- **Pulling image "apama-ctrl-starter-scope-..."** - the microservice initialization process has been started and the Docker image download is already in progress (state “Scheduled”).
- **Container created.** - the microservice container has been created but not started yet (state “Scheduled”).
- **Container started.** - the microservice container is started but not ready yet to handle incoming traffic (state “Not ready”).

## INFO

There is no event in the **Events** section when the microservice has reached the state “Ready” as this happens according to the readiness probe.

The screenshot shows the Cumulocity Administration interface. On the left is a sidebar with navigation options: Home, Accounts, Tenants, Ecosystem, Applications, Extensions, Microservices (highlighted), Default subscriptions, Business rules, Management, Settings, Data broker, and Migration. The main content area is titled 'Ecosystem > Microservices > Report-agent > Status'. Below this are tabs for Properties, Logs, Permissions, and Status (selected). The Status tab displays three main sections: 'Instances' with a table showing 0 Active, 0 Unhealthy, and 0 Desired instances; 'Events' with a message 'No events to display'; and 'Alarms' with a message 'No alarms to display'. Below these is a 'Subscriptions' table with one entry for tenant 't123456' showing 0 Active, 0 Unhealthy, and 0 Desired subscriptions. On the right side, there is a 'Smart rules' section with three rules: 'Calculates energy consumption', 'Creates alarm when measurements are missing', and 'Executes an operation when alarm is triggered'. The bottom of the sidebar indicates 'powered by CUMULOCITY'.

Audit logs and events are stored at tenant space according to the isolation level. For multi-tenant isolated microservices this is the tenant that is the owner of the microservice and in case of per-tenant isolation level it is the subscribed tenant.

## BILLING PRICING MODELS

The Cumulocity platform collects a lot of different usage statistics data which is used for billing customers.

Based on the contract, there are two pricing models for billing:

- Tenant usage pricing model - based on tenant usage statistics
- Device pricing model - based mostly on device statistics and microservice resource usage

The table below presents which values are used in each model for billing purposes:

Source	Name	Tenant usage pricing model	Device pricing model
<a href="#">TenantUsageStatistics</a>	ID	x	x
<a href="#">TenantUsageStatistics</a>	Tenant	x	x
<a href="#">TenantUsageStatistics</a>	API requests	x	
<a href="#">TenantUsageStatistics</a>	Device API requests	x	
<a href="#">TenantUsageStatistics</a>	Storage	x	x
<a href="#">TenantUsageStatistics</a>	Peak storage	x	
<a href="#">TenantUsageStatistics</a>	Root device	x	
<a href="#">TenantUsageStatistics</a>	Peak root device	x	
<a href="#">TenantUsageStatistics</a>	Devices	x	x
<a href="#">TenantUsageStatistics</a>	Peak devices	x	
<a href="#">TenantUsageStatistics</a>	Endpoint devices	x	
<a href="#">TenantUsageStatistics</a>	Subscribed applications	x	
<a href="#">TenantUsageStatistics</a>	Creation time	x	x
<a href="#">TenantUsageStatistics</a>	Alarms created	x	
<a href="#">TenantUsageStatistics</a>	Alarms updated	x	
<a href="#">TenantUsageStatistics</a>	Inventories created	x	
<a href="#">TenantUsageStatistics</a>	Inventories updated	x	
<a href="#">TenantUsageStatistics</a>	Events created	x	
<a href="#">TenantUsageStatistics</a>	Events updated	x	
<a href="#">TenantUsageStatistics</a>	Measurements created	x	
<a href="#">TenantUsageStatistics</a>	Operations created	x	
<a href="#">TenantUsageStatistics</a>	Operations updated	x	
<a href="#">TenantUsageStatistics</a>	Total inbound transfer	x	

Source	Name	Tenant usage pricing model	Device pricing model
<a href="#">TenantUsageStatistics</a>	Parent tenant	x	x
<a href="#">TenantUsageStatistics</a>	Tenant domain		x
<a href="#">TenantUsageStatistics</a>	Can create subtenants		x
<a href="#">TenantUsageStatistics</a>	External reference	x	x
<a href="#">TenantUsageStatistics</a>	Total microservice CPU usage	x	
<a href="#">TenantUsageStatistics</a>	Total microservice memory usage	x	
<a href="#">MicroserviceUsageStatistics</a>	Per microservice CPU usage		x
<a href="#">MicroserviceUsageStatistics</a>	Per microservice memory usage		x
<a href="#">DeviceStatistics</a>	Monthly measurements, events and alarms created and updated per device		x