User Guide | PUBLIC
Document Version: 2204a – 2022-04-19

Tenant Administration Apps

THE BEST RUN SAP

Content

1 Tenant Administration: Overview

Overview of the apps for organizational tenant administration

> **i** Note
>
> **Important**: All apps related to SAP IoT Tenant Administration are deprecated as of October 2021 and will be decommissioned in the future (details to be communicated as soon as possible). In case you've used any of the apps in your SAP IoT system landscape, we recommend getting in touch with SAP support in order to find an alternative solution. The following apps are affected:
>
> - Companies [page 5]
> - Persons [page 9]
> - User Groups [page 13]
> - Object Authorizations [page 17]

Introduction

Tenant Administration is the name of a group of apps that serve the purpose of covering all aspects of organizational tasks to be done during onboarding of companies and persons to the SAP IoT platform. A tenant is a technical entity offered by the platform. It is used by administrators (or automatically in the background by the *Companies* app) to establish a 1:1 relationship between a tenant and a company. For SAP IoT being a multitenancy platform where many companies are hosted on the same hardware simultaneously, it is crucial to strictly separate the data that belongs to different companies. This is accomplished with the tenant concept. The tenant serves as a container for company-specific data and isolates this data from the data of other companies.

The organizational aspects that are covered by the *Tenant Administration* apps comprise the following:

- Onboarding and maintaining companies
- Onboarding and maintaining persons (with a person always seen as a company member)
- Maintaining user groups, which serve as a connection between persons and the type of actions they can perform in the system
- Object authorizations, which define subsets of the company-specific objects that a particular user may access

In addition to these organizational aspects, there is a second area of system administration: The definition and modeling of things, that is, the digital twins of real-world objects that a company wants to manage. For this type of administrative tasks, SAP offers a second group of apps, namely the Thing Modeler apps.

Cross-App Relationships

Although the *Tenant Administration* apps are constructed as self-contained, stand-alone applications, several connections exist between them. These connections illustrate that the different apps can be seen as different

perspectives on the same subject matter, namely the organizational aspects of tenant administration. For example, from the *Companies* app, you can navigate to the persons assigned to a company in the *Persons* app as well as to the root authorization object for that company in the *Object Authorization* app.

> → Recommendation
>
> Although there is no mandatory sequence of working through the different apps that make up the *Tenant Administration* group of apps, it is a good idea to start with the *Object Authorization* app. This is because the authorization groups that you maintain in that app are referenced by all other apps, and for some entities it is even mandatory to assign an authorization group already upon creation.

Roles and Target Groups

The separation between apps for organizational versus technical aspects of tenant administration is based on the assumption that in most cases, persons with different skill sets will take care of these different aspects. While the apps for organizational aspects have managers or administration experts as their target audience, the Thing Modeler apps are addressing a more technical audience of engineers. Consequently, SAP offers different role templates with predefined authorizations that are needed to work with one of the two app groups. You can use these role templates as a blueprint for setting up custom roles according to the needs of your company.

SAP Fiori Launchpad

The apps that are provided with SAP IoT are designed for, and based on, SAP Fiori. The various apps are grouped into two main areas, *Tenant Administration* and *Thing Modeling*. Each single app has its own tile on the Fiori launchpad. For more information on how to get the best out of the SAP Fiori launchpad, see the SAP Fiori Launchpad user guide.

Related Information

Companies: Overview [page 5]
Persons: Overview [page 9]
User Groups: Overview [page 13]
Object Authorizations: Overview [page 17]

2 Companies: Overview

Overview of the Companies App

Introduction

In the SAP IoT platform, it is a basic and cross-application requirement to maintain a set of data describing the companies that have been onboarded to the platform. During the onboarding process, each company is assigned to its dedicated tenant object. The tenant serves as a container for all company-specific data, both related to persons as well as things.

> **i** Note
>
> Setting up a company is a prerequisite for a complete onboarding of the persons that belong to the company. This is because during person onboarding, you have to assign each person to a company.

For each company, you can maintain data belonging to the following categories:

- Basic Data
- Contact Data
- Authorization Group Assignment

Here, the last category, *Authorization Group Assignment*, is of special interest. In this category, the app lets you navigate to the Object Authorizations app where you can define a root authorization object for the current company. Based on this root authorization, an administrator can build a hierarchy of derived authorizations that control the access permissions based on object instances, that is, the things that are assigned to a company.

With this app, you can perform the following activities:

- Creating companies
- Maintaining companies
- Deleting companies

Related Information

Persons: Overview [page 9]
Object Authorizations: Overview [page 17]

2.1 Create a Company

Process steps for creating a company manually

Context

You want to create a new company that shall be entitled to manage its assets as things with the SAP IoT platform.

Procedure

1. From the launchpad, start the *Companies* app.

   The system displays the list of companies that are already stored in the system.
2. In the upper right corner of the screen, choose + *Add*.

   You are now navigating to the *New Company* data entry form.
3. Enter the data into the respective fields. Note that the following fields are mandatory: *Company Name*, *E-Mail*, and *Authorization Group*.
4. Once you are done, choose *Save*.

   Note that the *Save* button is active only if you have entered all required data, and if the e-mail address is formally correct.
5. If you need to create more companies, you can accomplish this by navigating < *Back* back to the list of companies and repeat the previous steps.

Results

The new company has been added to the database and is displayed in the list of companies on the entry screen.

2.2 Maintain a Company

Process steps for maintaining company data

Context

As an administrator, you want to modify the data that has been entered for a company that has been onboarded on the SAP IoT platform.

Procedure

1. From the launchpad, start the *Companies* app.

   The system displays the list of companies that are already stored in the system.
2. From the list of companies, choose the one you want to maintain. If you don't see the company that you want to change, use the *Search* or the *Filter* to narrow down the number of companies presented in the list.

   You are now navigating to the *Edit Company* data entry form.
3. Modify the field values as needed.
4. Choose *Save*.

   The *Save* button remains inactive as long as the data shown for the company is identical to the data that is already stored in the database.

Results

The changes are stored in the database, and the system takes you back to the entry screen with the list of companies.

2.3 Delete a Company

Process steps for deleting a company from the system

Context

As an administrator, you want to delete a company from the system, for example, because that company has been acquired by another company and is therefore no longer entitled to use the SAP IoT platform.

Procedure

1. From the launchpad, start the *Company* app.

   The system displays the list of companies that are already stored in the system.
2. From the list of companies, choose the one you want to delete. If you don't see the company you are looking for, use the *Search* or the *Filter* to narrow down the number of companies presented in the list.

   You are now navigating to the *Edit Company* data entry form.
3. Make sure the currently displayed company is in fact the one that you want to delete. Once you are sure, choose *Delete*.

   The system presents a confirmation dialog where you have to confirm your decision to delete the company.
4. Confirm your decision.

Results

The company is deleted from the database. The system takes you back to the entry screen with the list of companies.

> **i** Note
>
> Together with the company, the system deletes all persons that have been assigned to that company.

3 Persons: Overview

Overview of the Persons App

Introduction

In the SAP IoT platform, it is a basic and cross-application requirement to maintain a set of data describing the persons who are allowed to log on to the platform and access the objects for which they are responsible to the extent of the set of permissions that they have been granted. As a part of a person's data record, you assign an authorization group to the person. This authorization group can then be used to grant other users access to the data of that person. Similarly, the scope of allowed operations that the person can perform on certain objects is something that you define by assigning the person to a user group.

To give you a better idea of how the different entities in the Tenant Administration apps are related with each other, just have a look at the following graphic. The graphic presents a scenario where an administrator ("Person A") needs to access the data of another user ("Person B"):

> **i Note**
>
> In this app, you can only assign a person to both an authorization group and a user group. The definition, however, of these two types of groups is subject to two separate dedicated apps, Object Authorizations and User Groups. Setting up authorization groups and user groups is therefore a prerequisite for a fully qualified person record. However, if the appropriate authorization groups or user groups are not yet available, you can still start creating new, and maintaining existing person records. You can easily make the relevant group assignments at a later point in time.

There is one more relationship between the Persons app and another app, namely the Companies app. With the Companies app, you can define the companies that are known to the system and that you assign to a person.

For each person, you can maintain data belonging to the following categories:

- Name
- Address
- Contact
- User

Here, the last category, *User*, is of special interest. It is possible to maintain the basic data for a person in the system without granting him or her the permission to log on to the system or to access any objects that are handled by the system. This is only possible for persons who have also a user assigned, and this user must be flagged as active.

With this app, you can perform the following activities:

- Creating persons
- Maintaining persons
- Deleting persons

Related Information

User Groups: Overview [page 13]
Object Authorizations: Overview [page 17]
Companies: Overview [page 5]

3.1 Create a Person

Process steps for creating a person manually

Context

You want to create a new person who shall be entitled to log on to the SAP IoT Application Services platform and to access a well-defined set of things.

Procedure

1. From the launchpad, start the *Persons* app.

   The system displays the list of persons who are already stored in the system.
2. In the upper right corner of the screen, choose + *Add*.

   You are now navigating to the *New Person* data entry form.
3. Enter the data into the respective fields. Note that the following fields are mandatory: *First Name*, *Last Name*, *E-Mail*, and *Authorization Group*.

   The system assigns the company to which the logged-on user belongs to the new person as well. A reference to this company is automatically added to the person data. It is possible to manually assign a different company at a later point in time. However, this may lead to authorization inconsistencies that need to be adjusted manually as well.
4. Once you are done, choose *Save*.

   Note that the *Save* button is active only if you have entered all required data, and if the e-mail address is formally correct.

5. If you need to create more persons, you can accomplish this by navigating < *Back* back to the list of persons and repeat the previous steps.

3.2 Maintain a Person

Process steps for maintaining person data

Context

You want to modify the data that has been entered for a person who is entitled to log on to the SAP IoT platform and to access a well-defined set of things.

Procedure

1. From the launchpad, start the *Persons* app.

   The system displays the list of persons who are already stored in the system.
2. From the list of persons, choose the one whose data you want to maintain. If you don't see the person that you want to change, use the *Search* or the *Filter* to narrow down the number of persons presented in the list.

   You are now navigating to the *Edit Person* data entry form.
3. Modify the field values as needed.
4. Choose *Save*.

   The *Save* button remains inactive as long as the data shown for the person is identical to the data that is already stored in the database.

Results

The changes are stored in the database, and the system takes you back to the entry screen with the list of persons.

3.3 Delete a Person

Process steps for deleting a person from the system

Context

You want to delete a person from the system, for example, because that person has left your company and is therefore no longer entitled to log on to the SAP IoT platform and to access any things.

Procedure

1. From the launchpad, start the *Persons* app.

   The system displays the list of persons who are already stored in the system.
2. From the list of persons, choose the one you want to delete. If you don't see the person you are looking for, use the *Search* or the *Filter* to narrow down the number of persons presented in the list.

   You are now navigating to the *Edit Person* data entry form.
3. Make sure the currently displayed person is in fact the one that you want to delete. Once you are sure, choose *Delete*.

   The system presents a confirmation dialog where you have to confirm your decision to delete the person.
4. Confirm your decision.

Results

The person is deleted from the database and can no longer access any data that is stored in the system. The system takes you back to the entry screen with the list of persons.

> **i** Note
>
> If you plan a mass deletion of all persons that are assigned to a particular company, it is much easier to delete the company with the help of the Companies app. Together with the company, all the persons that are assigned to that company are automatically deleted by the system.

Related Information

Delete a Company [page 7]

4 User Groups: Overview

Overview of the User Groups app

> **i** Note
>
> Due to a change in the tenant administration concept, the User Groups app is no longer needed for newly created tenants. Consequently, the app checks the tenant status upon startup:
>
> - For legacy tenants, the app starts and lets you define user groups.
> - For newer tenants, the app is not needed and only displays an information message before automatically shutting down.

Introduction

In SAP IoT the concept for granting or restricting access permissions to the available objects and services has two aspects:

- Defining a hierarchy of objects with a set of capabilities defining the allowed actions (read, write, delete) with respect to a given object hierarchy.
- Defining user groups that relate a single user (as a member of the user group) with the object-specific access rights that are granted to the user group.

While the object-specific access rights are defined with the help of the Object Authorizations app, you use the User Groups app to define the user groups that bring together object authorizations, service authorizations, and users.

Features

Service Authorizations

A service authorization is a set of one or more role collections, which in turn is a set of one or more roles. The predefined roles that are provided by SAP are oriented at certain profiles of a user who is in charge of performing certain tasks in the system. For example, the `Thing_Editor` role combines a number of functional authorizations for full access to things, events, and authorizations in the SAP IoT platform.

Object Authorizations

In this section of the User Groups app, you assign the object-specific authorizations defined in the Object Authorizations app to the user group that you are currently working on. In other words, this is the place where you define the set of objects that users in the current user group may access.

Persons

In this section of the User Groups app, you specify a set of persons that you have created with the help of the Persons app. All persons that you bring together in one user group have the same access rights with regard to

the objects that you have specified in the *Object Authorization* section. If a person is assigned to more than one user group, the resulting access rights for that person are the superset of all access rights granted by all assigned user groups.

Related Information

Object Authorizations: Overview [page 17]
Persons: Overview [page 9]

4.1 Create a User Group

Process steps for creating a user group

Context

As an administrator, you want to define a group of users who shall all be granted the same access rights for the same set of objects.

Procedure

1. From the launchpad, start the *User Groups* app.

   The system presents the list of available user groups.
2. At the top of the list of user groups, choose + *Add*.

   The system navigates you to the *Basic Data* section.
3. Enter a technical name for the new user group. In addition, you can also enter a description of the purpose of the user group.

   For the name, only a restricted set of characters is allowed. The system alerts you in case you enter any unallowed characters.
4. Choose *Service Authorizations*.
5. At the top of the list of role collections, choose + *Add*.

   The system presents a list of available role collections.
6. Tick the checkbox of all role collections that you want to include in the new user group and choose *OK*.

   The system adds all selected role collections to the list of service authorizations of the new user group. You can expand each role collection to see the individual roles contained in each collection. You can even drill down one more level by clicking the role names. The system then presents the list of single capabilities that are combined in that role.

7. Once you are done with adding service authorizations, choose *Object Authorizations*.
8. At the top of the list of capabilities, choose + *Add*.
   The system presents a list of available capabilities.
9. Tick the checkbox of all capabilities that you want to include in the new user group and choose *OK*.
   The system adds all selected capabilities to the list of object authorizations of the new user group.
10. Once you are done with adding object authorizations, choose *Persons*.
11. At the top of the list of assigned persons, choose + *Add*.
    The system presents a list of available persons.
12. Tick the checkbox of all persons that you want to include in the new user group and choose *OK*.
    The system adds all selected persons to the list of assigned persons of the new user group.
13. Choose *Save*.

4.2 Maintain a User Group

Process steps for maintaining a user group

Context

As an administrator, you want to modify an existing user group. This is a quite common task because, for example, in daily business it is quite normal that new employees take over new tasks and have to be added to an existing user group. Also, when new assets have been taken into production mode and are modeled as things, the necessary authorizations for such new things require adjustments of the access rights defined in a user group.

> **i** Note
>
> You should keep in mind the following aspects:
>
> - You cannot change the name of a user group. This is because the name is used as a unique technical identifier by the system.

Procedure

1. From the launchpad, start the *User Groups* app.
   The system presents the list of available user groups.
2. Search the user group that you want to change and click on its entry in the list.
   The system navigates you to the *Basic Data* section of the user group.
3. Choose any of the available sections for the user group (*Basic Data*, *Service Authorizations*, *Object Authorizations*, *Persons*) and modify the existing assignments as required.

4. Once you are done, choose *Save* to make all changes you have made effective with one single click.

4.3 Delete a User Group

Process steps for deleting a user group from the system

Context

As an administrator, you want to delete a user group from the system. Deleting a user group is an action that can have a major impact on the processes in your company. You should therefore be extra careful before you delete a user group. You should be aware of the following aspects:

- Access to all objects that are assigned to the user group will no longer be possible for the members of the group.
- On the other hand, it is still possible that certain group members can access all or some of the objects in question if they are assigned to one or more other user groups granting similar, or overlapping, access rights.

Procedure

1. From the launchpad, start the *User Group* app.

   The system presents the list of available user groups.
2. Search the user group that you want to delete and click on its entry in the list.

   The system navigates you to the *Basic Data* section of the user group.
3. Make sure that the currently displayed user group is in fact the one that you want to delete. Once you are sure, choose *Delete*.

   The system presents a confirmation dialog where you have to confirm your decision to delete the user group.
4. Confirm your decision.

Results

The user group is deleted from the database. The system takes you back to the entry screen with the list of user groups. The persons and onject authorizations that have been collected in the user group are **not** affected by this operation and remain untouched in the system.

5 Object Authorizations: Overview

Overview of the Object Authorizations app

Introduction

In the SAP IoT platform, one of the most important and critical administrative activities is defining and assigning access authorizations. This is because the platform is designed as a multitenancy environment, where different customers manage their assets (that is, the "things") in one shared system. It is therefore crucial for an administrator to properly define the access rights with respect to the assets that are onboarded.

However, there is more to authorization than things (that's why we are speaking of **object** authorizations in a more general sense). For persons acting in the role of an administrator, it is also important to enable or restrict access to onboarded persons as well as organizations.

> ✤ Example
>
> After the initial onboarding of a new customer has been done by a system administrator, the customer needs to be able to manage not only its assets like buildings, vehicles, or machines. Rather, the customer must be able to manage also the organizational aspects within its own area of responsibility. For example, a person who was initially onboarded might leave the company and needs to be replaced by a new hire. Or another person may be promoted to a new job level or function and needs a different set of authorizations assigned. This kind of administrative tasks can (and should) be taken care of by the customer itself without involving the platform host administrators.

Features

The Object Authorizations app offers a number of interwoven settings, which, as a whole, make up the access authorization management of the platform. These settings comprise the following:

- *Authorization Groups*
  Authorization groups serve the purpose of defining access rights with respect to particular objects (things, persons, companies). They are organized in a hierarchical structure with a single root authorization for each customer (or, from a technical point of view, for each tenant). Authorization groups are the answer to the question "authorization for what object?"
- *Capabilities*
  With capabilities, you define the actions that a user may perform when accessing a particular object. These actions are read, write, and delete. So, capabilities answer the question "authorization for which activity?"
- *Collections*
  Collections are used to assign the object instance-based authorizations that you define with authorization groups and capabilities to a particular user group. As a result, a user who is a member of a user group is permitted to access the set of objects in the way defined by the capabilities. With that, you have the answer to the question "authorization for whom?"

5.1 Create a Capability

Process steps for creating a capability for granting certain operations on objects

Context

As an administrator, you want to define the types of actions (read, write, delete) that are permitted when a user tries to access a particular object (thing, person, organization). A capability is therefore a set of attributes defining the allowed actions for a set of authorization groups (where the latter implicitly define the objects to be accessed) or for a set of specified object instances. In a final step, capabilities are assigned to one or more user groups in the *User Groups* app so that all users belonging to that group can perform the actions permitted by the capability.

Procedure

1. From the launchpad, start the *Object Authorizations* app.

   The system displays the hierarchical list of authorizations that are already stored in the system.
2. From the button bar underneath *Object Authorizations*, choose *Capabilities*.

   The system displays the list of capabilities that already exist in the system.
3. In the upper right corner of the screen, choose + *Add*.

   The system displays the *Create Capability* dialog box.
4. In the dialog box, enter the required data:
   - *Name*: Enter a name for the capability that describes the granted permissions. It may also be advisable to mention the user groups for which the capability is relevant.
   - *Capability Type*: Choose one of the predefined object types to which the new capability shall be related.
   - *Actions*: Choose one or more of the predefined types of actions that shall be permitted by the new capability.
   - *Conditions*: In this area, you specify the scope of objects for which the new capability shall grant access permissions. Here, you can follow two different approaches:
     - Apply access permissions to **all objects** matching the selected *Capability Type*: If you want users who are granted the new capability to be able to perform the allowed action types on all objects of the type specified in *Capability Type*, tick the *Unrestricted* checkbox.
     - Restrict access to **certain object instances**: Make sure the *Unrestricted* checkbox is deselected. Then, specify the conditions an object must fulfill to be subject of the new capability. Each condition may be based either on an authorization group related to the object, or on type-specific attributes of the given object type.

       > **i Note**
       >
       > You can define as many conditions as desired for a given capability. At runtime, the system combines the conditions with a logical AND. That is, the more conditions you define, the lower the number of object instances that may match all these conditions.

> **Note**
>
> Specifying individual object instances or granting unrestricted access to all object instances is mutually exclusive. In any case, you have to decide for one of the two approaches. Otherwise, the system does not allow saving the capability.

5. Once you are done, choose *Save*.

Results

The new capability is available in the system and can be assigned to one or more user groups.

Related Information

User Groups: Overview [page 13]

5.2 Maintain a Capability

Process steps for maintaining a capability

Context

As an administrator, you want to modify an already existing capability. Here are some use cases where this would be necessary:

- Extending a capability to additional user groups, or removing some of the already assigned user groups.
- Modifying the allowed activities, for example, restrict access from read/write/delete to only read/write.
- Change the set of objects covered by a capability from unrestricted access to only a clearly defined set of objects matching certain conditions.
- The settings of a capability have already been changed, but the changes still need to be reflected by an adjusted capability name.

Procedure

1. From the launchpad, start the *Object Authorizations* app.
2. From the button bar underneath *Object Autorizations*, choose *Capabilities*.

   The system displays the list of capabilities that already exist in the system.

3. From the list of capabilities, select the one you want to change.

   If you don't see the capability you are looking for, enter a part of the capability name in the *Search* field to narrow down the number of capabilities displayed.
4. Decide what kind of change you want to apply to the capability:
   - To modify the set of assigned user groups, click the number displayed in the *User Groups* column. The system takes you to the *User Groups* app where you can modify the set of assigned user groups.
   - To modify the detail settings of a capability, select its entry in the list. The system displays the *Edit Capability* screen.
5. Apply the desired changes to the capability.

   For more information on the various fields of a capability, see Create a Capability [page 18].
6. Once you are done, choose *Save*.

5.3 Delete a Capability

Process steps for deleting a capability from the system

Context

As an administrator, you may want to delete a capability for various reasons, such as:

- A capability has been created a long time ago and does not properly reflect the thing infrastructure that is in place now.
- Reorganizations of the company structure call for a new level of granularity for the capabilities in effect.
- A cloud platform consumer has decided **not** to renew their license contract. As a consequence, all the capabilities, users, and user groups related to that customer must be deleted as soon as the customer has been offboarded.

Procedure

1. From the launchpad, start the *Object Authorizations* app.
2. From the button bar underneath *Object Autorizations*, choose *Capabilities*.

   The system displays the list of capabilities that already exist in the system.

   If you don't see the capability you are looking for, enter a part of the capability name in the *Search* field to narrow down the number of capabilities displayed.
3. From the list of capabilities, select the one you want to delete.

   The system displays the *Edit Capability* screen.
4. Make sure the currently displayed capability is in fact the one that you want to delete. Once you are sure, choose *Delete*.

The system presents a confirmation dialog where you have to confirm your decision to delete the capability.

5. Confirm your decision.

5.4 Create an Authorization Group

Process steps for creating an authorization group and related objects

Context

As an administrator, you want to define an authorization that is related to a particular object instance (a thing, a person, or a company) and that can later be granted to users in a particular user group.

Procedure

1. From the launchpad, start the *Object Authorizations* app.

   The system displays the hierarchical list of authorizations that are already stored in the system. Even if the system has just been installed, there is always the top-level node called `HIERARCHY_ROOT`which serves as the ultimate anchor point for all custom authorization groups. It is provided automatically and cannot be deleted.

2. Choose any node in the hierarchy that you want to refine with a subordinate authorization group.

   Make sure the checkbox in the first column is selected for the respective entry so that the system knows the focus for the subsequent actions. Also, please make sure there is **only one** row selected. Otherwise, the next step cannot be performed because the + *Add* button will be deactivated.

3. In the upper right corner of the screen, choose + *Add*.

   The system inserts a new line underneath the previously selected entry.

4. Enter the name for the new authorization group into the entry field.

   Note that authorization groups with the same parent element must have unique names.

5. Once you are done, choose *Save*.

Results

The new authorization group has been added to the database and is displayed in the hierarchy of authorization groups on the entry screen.

5.5 Maintain an Authorization Group

Process steps for maintaining authorization groups

Context

As an administrator, you want to modify the current hierarchy of authorization groups. Note that you can only modify the name of an authorization group and its hierarchical level within the hierarchy of authorization groups.

Procedure

1. From the launchpad, start the *Object Authorizations* app.

   The system displays the hierarchical list of authorizations that are already stored in the system.
2. Expand the tree of authorization groups until you see the authorization group that you want to maintain.
3. For changing the name of an authorization group, simply click into the name and change it as desired. For changing the hierarchy level of an authorization group, tick the checkbox left to its name and click ← *Outdent*

   Note that you can move a group to a higher level in the hierarchy. Should you need to put the group at a lower level, or at a completely different position in the hierarchy, you have to create it anew at the desired position.
4. Once you are done, choose *Save*.

5.6 Delete an Authorization Group

Process steps for deleting an authorization group from the system

Context

As an administrator, you want to delete an authorization group from the system, for example, because you have decided to reorganize your authorization strategy within in the SAP IoT platform and you don't want to run into problems caused by legacy authorizations.

> ⚠ Caution
>
> When you delete an authorization group for which subordinate authorization groups have been defined, all these lower-level authorization groups are deleted along with the group that you have selected for deletion.

Procedure

1. From the launchpad, start the *Object Authorizations* app.
2. Expand the tree of authorization groups until you see the authorization group (or groups, in case you want to delete several groups at once) that you want to delete.
3. For all authorization groups you want to delete, tick the checkbox left to their names and click — *Delete Authorization Group*.

   The system presents a confirmation dialog where you have to confirm your decision to delete the authorization groups .
4. Confirm your decision.

Results

The authorization group is deleted from the database.

5.7 Create a Collection

Process steps for creating a collection of authorization groups

Context

As an administrator, you want to create a collection that serves as a combined set of individual authorization groups.

> **i** Note
>
> Before you start creating collections, make sure that there are already authorization groups maintained in the system.

Procedure

1. From the launchpad, start the *Object Authorizations* app.

   The system displays the hierarchical list of authorizations that are already stored in the system. Even if the system has just been installed, there is always the top-level node called `HIERARCHY_ROOT` which serves as the ultimate anchor point for all custom authorization groups. It is provided automatically and cannot be deleted.

2. From the button bar underneath *Object Autorizations*, choose *Collections*.

   The system displays the list of collections that already exist in the system.
3. In the upper right corner of the screen, choose + *Add*.

   The system displays the *New Authorization Group Collection* view.
4. In the *Collection Name* field, enter the name for the new collection.
5. In the *Assigned* column, tick the checkbox for each authorization group that you want to include in the new collection.

   If you select an authorization group for which sub-authorizations have been defined, all subordinate authorizations are automatically selected together with the top-level node. If this is **not** what you intended, you may deselect any unwanted authorizations manually.
6. Once you are done, choose *Save*.

5.8 Maintain a Collection

Process steps for maintaining a collection of authorization groups

Context

As an administrator, you want to adjust the set of authorization groups that are bundled in a particular collection. Also, you may change the collection name, for example, to adapt an existing collection to a newly introduced naming convention.

Procedure

1. From the launchpad, start the *Object Authorizations* app.
2. From the button bar underneath *Object Autorizations*, choose *Collections*.

   The system displays the list of collections that already exist in the system.
3. From the list of collections, select the one you want to change.

   If you don't see the collection you are looking for, enter a part of the collection name in the *Search* field to narrow down the number of collections displayed.
4. Click the desired collection.

   The system displays the *Collection Details* screen.
5. Change the collection name as desired, or modify the existing authorization group assignments.
6. Once you are done, choose *Save*.

   The *Save* button remains inactive as long as the data shown for the collection is identical to the data that is already stored in the database.

5.9 Delete a Collection

Process steps for deleting a collection of authorization groups from the system

Context

As an administrator, you may want to delete an authorization group collection for various reasons, such as:

- The combination of authorization groups bundled in a collection is not permitted.
- The combination of authorization groups bundled in a collection is not useful.
- The combination of authorization groups bundled in a collection already exists in another collection, and you want to remove the duplicate.

Procedure

1. From the launchpad, start the *Object Authorizations* app.
2. From the button bar underneath *Object Autorizations*, choose *Collections*.

   The system displays the list of collections that already exist in the system.
3. From the list of collections, select the one you want to delete.

   If you don't see the collection you are looking for, enter a part of the collection name in the *Search* field to narrow down the number of collection displayed.
4. Click the desired collection.

   The system displays the *Collection Details* screen.
5. Make sure the currently displayed collection is in fact the one that you want to delete. Once you are sure, choose *Delete*.

   The system presents a confirmation dialog where you have to confirm your decision to delete the collection.
6. Confirm your decision.

Results

The collection is deleted from the database and can no longer be used for granting access to the objects referenced by the authorization group.

6 Tenant Configuration: Overview

Introduction

In SAP IoT, some scenarios require the activation of certain features that aren't active out of the box. A reason for such an inactive default status of a feature could be that the activation itself might already cause cost in the background. Therefore, in such cases, activating a feature should always be subject to a conscious decision by an authorized person at customer site.

Authorizations

The following authorizations provided by roles are required:

- For the activation of specific new features such as the integrated IoT Edge Platform, you need the `Tenant_Configuration_Admin` role assigned to your user.
- To get a read-only overview of the current feature activation status via the app, the `Tenant_Configuration_Viewer` role is required. This role is contained in the standard role collection `iot_role_collection`, which is set up during the onboarding to SAP IoT.

In the *Tenant Configuration* app you can activate the following features:

- IoT Edge Platform
  The integrated IoT Edge Platform supports scenarios such as the Smart Sensing scenario, which involves the setup and communication with an Edge node. For more information, see Smart Sensing: Overview.

Related Information

Providing Authorizations

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

THE BEST RUN SAP