

SIEMENS

Insights Hub

Settings

System Manual
03/2024

Introduction	1
User interface and User Rights	2
User Management	3
Data Access	4
Configurations	5
User Preferences	6
Appendix	7

Legal information

Warning notice system

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

DANGER

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

WARNING

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

CAUTION

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

NOTICE

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

WARNING

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

Trademarks

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

Disclaimer of Liability

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

Table of contents

1. Introduction.....	4
1.1. Introduction.....	4
2. User interface and User Rights.....	5
2.1. User interface.....	5
3. User Management.....	7
3.1. User Management.....	7
3.2. Managing user groups.....	11
3.3. Technical Users.....	15
3.4. Roles.....	18
4. Data Access.....	24
4.1. Introduction to policies.....	24
4.2. Creating a new policy.....	25
4.3. Activating or deactivating a policy.....	27
4.4. Creating a new resource group.....	27
4.5. Using subtenants.....	29
4.6. Collaborations.....	32
4.7. Customize the OS Bar with "Provider".....	34
4.8. Service Credentials.....	40
5. Configurations.....	46
5.1. Certificate Manager.....	46
5.2. Identity Provider Federation.....	47
6. User Preferences.....	52
6.1. User Preferences.....	52
7. Appendix.....	54
7.1. Appendix.....	54

Introduction

1.1 Introduction

Settings is a system tool that offers the following benefits:

- It is integrated.
- It is a trusted application.
- It provides access to system functions.

Settings handles the user management and the settings of your tenant. It allows you to customize the provider information in your tenant and create further subtenants.

Functionalities

Settings offers the following functions:

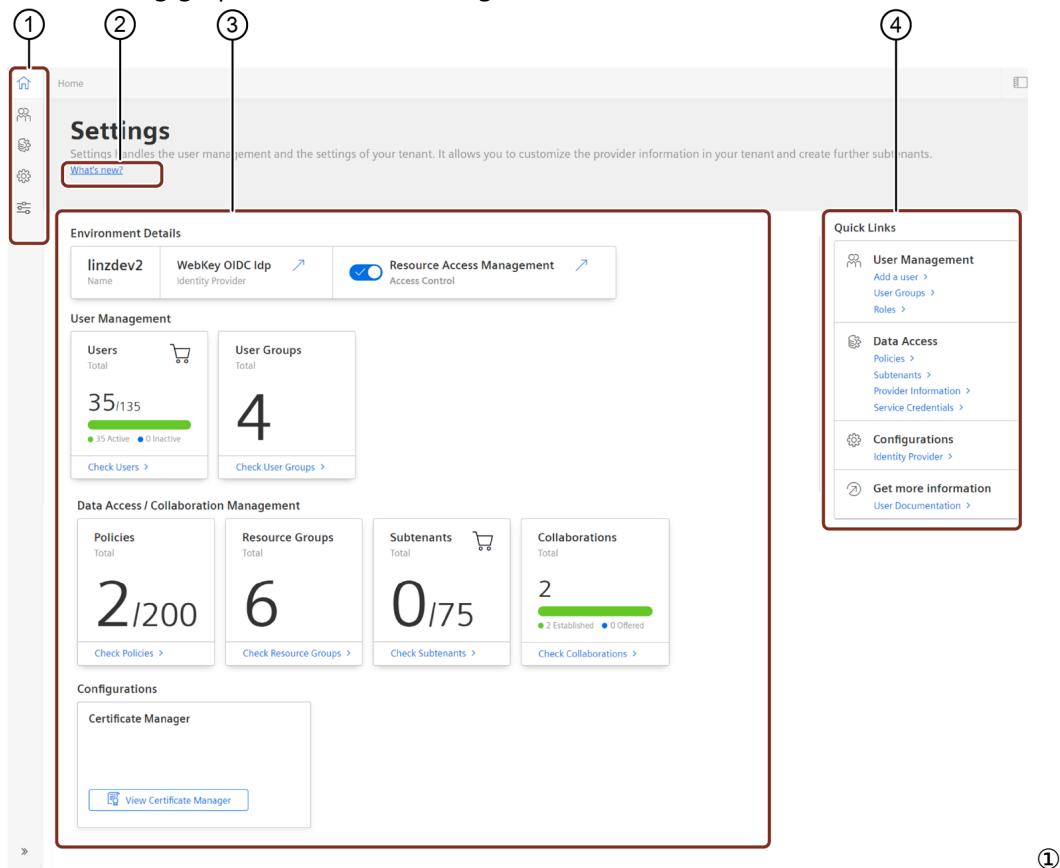
- Create, manage and delete users.
- Create and manage user groups.
- Manage roles, their users, and user groups.
- Manage company name, logo and links in OS Bar as tenant provider.
- Create and manage subtenants.
- Subscribe and Unsubscribe to receive the notifications.

User interface and User Rights

2

2.1 User interface

The following graphic shows the Settings start screen user interface:



Navigation area

- ② Link to release notes
- ③ Links to operating tabs
- ④ Quick links to navigate to the respective screens

User rights

In order to get full access to Settings you need the Settings administrator app role. If the Settings administrator role is not assigned to the user, the Settings icon is not shown to the user on the Launchpad.

You can also grant access to Settings by using the TenantAdmin standard role.

2.1 User interface

The support team creates your tenant and grants the TenantAdmin role to an authorized person in your company. The TenantAdmin can grant the TenantAdmin or Settings administrator role to other users.

User Management

3

3.1 User Management

Managing users

User types

Settings allows you to create users with their email addresses and manage their permissions. You can create the following user types in Settings:

- **Global users:** Users have access to all tenants.
- **Subtenant users:** These users are assigned to a subtenant and only have access to assets of a specific subtenant.



Subtenant user

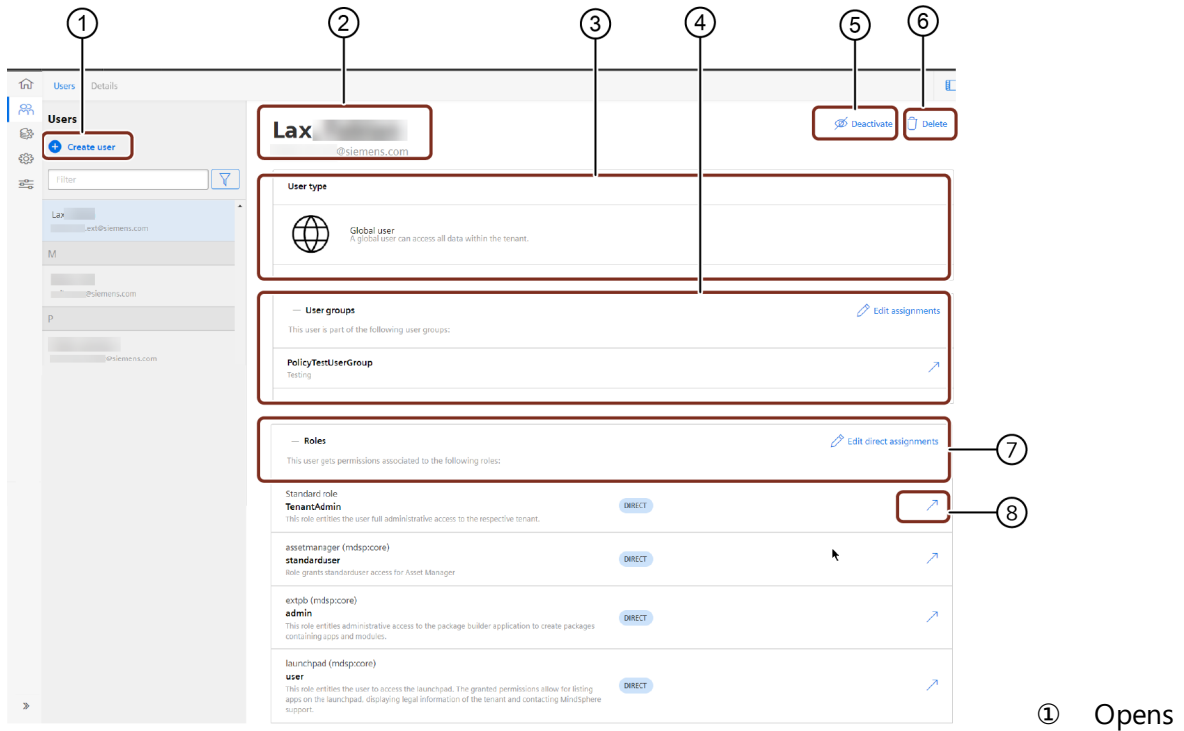
A subtenant user needs the role [mdsp:core:SubTenantUser](#) to get access to applications on the launchpad. See also

- [Standard roles](#)
- [Using subtenants](#)

For a better management of users and to assign roles to multiple users, Settings offers the creation of user groups.

User interface "Users"

The following screenshot shows the "Users" user interface:



a dialog to create a new user

- ② Shows the name and email address of the user
- ③ Shows the user type
- ④ Shows the user groups assigned to the user
- ⑤ Activates or deactivates the user
- ⑥ Deletes the selected user
- ⑦ Switches to "Roles" tab
- ⑧ Shows the roles assigned to the user

Creating users

You can create global users or subtenant users.

Quota consumption


The creation of a user reduces your quota.

Creating the subtenant

You can create a new subtenant for new users. For more information on subtenants, refer to the section Using subtenants (Page 49).

Procedure

To create a new user in Settings, proceed as follows:

1. Open the "Users" interface and click  "Create user".

- The "Create user" interface opens.
- 2. Enter a name and the email address of the user.
- 3. Select the user type "Global user" or "Subtenant user".
 - If there is no subtenant available, click "Create subtenant" and create a subtenant.
- 4. If you selected "Subtenant user", select a subtenant.
- 5. Click "Create user".
- 6. In order to assign a role to the user, click "Assign roles".
- 7. Select a role and click "Next".
 - You can find more information about roles in chapter [Standard roles](#).
- 8. In order to save the settings, click "Save".
- 9. In order to close the settings, click "Close".

Result

You have created a new user and assigned a role. The new user is now activated and will receive an email with access instructions for the tenant. After the user has logged in the first time, the first name and last name of the user is displayed in Settings.

Activate or deactivate users

You can activate and deactivate users in Settings. Activated users have access to their assigned apps and services. You may temporarily deny users access to Insights Hub and its services by deactivating them. Reactivated users obtain automatically their previously assigned permissions.

Procedure

To activate or deactivate a user, proceed as follows:

1. In the navigation area, click "Users".
2. In the selection list, select the user.
3. Click "Activate" or "Deactivate" to activate or deactivate the user.
 - The "Activate user" or "Deactivate user" dialog opens.
4. Confirm activation or deactivation.

Result

You activated or deactivated the user.

Deleting users

Procedure



Data security notice

Delete users immediately if they are no longer part of your business.

To delete a user, proceed as follows:

1. In the navigation area, click "Users".
2. In the selection list, select the user to be deleted.
3. Click "Delete" to delete the user.
 - The "Delete user" dialog opens.
4. Confirm deletion with "Yes".

Result

You deleted the user from Settings.

Edit user role assignment

You can assign roles to a user in the "User" tab or assign user to a role in the "Roles" tab. You can find more information about roles in the section [Roles](#)

Procedure

In order to assign or remove roles to a user proceed as follows:

1. In the navigation area, click on "Users".
2. Select the user in the selection list.
3. Click "Edit direct assignment".
 - A dialog box appears with a list of available roles.
4. Select or deselect the appropriate check boxes to assign or unassign roles to the selected user.
5. To confirm the changes, click "Next".
6. To save the changes, click "Save".
7. In order to close the settings, click "Close".

Result

You have assigned or removed a role to a user.

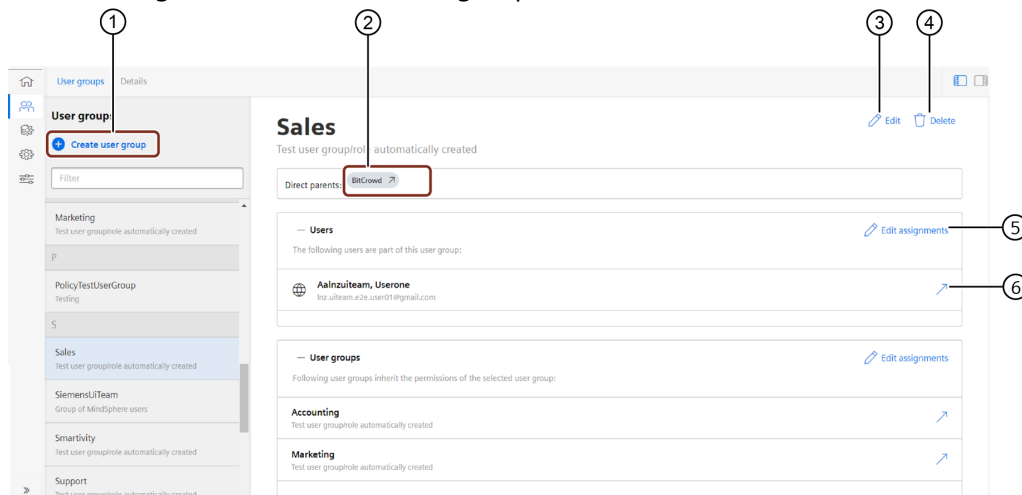


The corresponding user must log in again for the changes to become effective.

3.2 Managing user groups

User interface "User groups"

The following screen shows the user group user interface:




- ① Creates a new user group
- ② Move to superordinate user group
- ③ Edit user group
- ④ Deletes the user group
- ⑤ Opens window to edit user assignments
- ⑥ Opens user in "User" tab

Creating user groups

For a better management of users and to assign roles to multiple users, Settings offers the creation of user groups.

Procedure

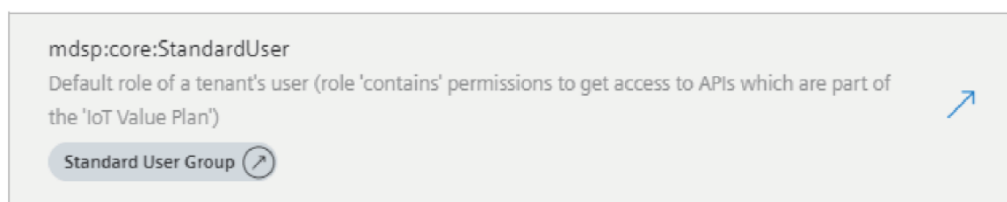
To create a new user group in Settings, proceed as follows:

1. In the navigation area open the "User group" interface and click  "Create user group".
 - The "Create user group" interface opens.

2. Enter a name and a description for the user group.
3. To create the user group, click "Create user group".
4. In order to assign users to the group, click "Add users".
5. Select the users for the new group and click "Next".
6. To save the user assignment for the group, click "Save" and "Close".
7. In order to assign other user groups. click "Assign user groups".
8. Select the user groups for the new group.
9. To save the user group assignment, click "Save" and "Close".
10. In order to assign roles to the group, click "Assign roles".
11. Select the roles for the new group and click "Next".
12. To save the role assignment for the group, click "Save" and "Close".

Result

You have created a user group with different users. All users of this group now have the assigned roles. In the "User" tab you can see the new group badge in the role assignment window:



Edit user groups

After you have created a group, you can change the user group name, description, edit user assignments and role assignments.

Prerequisite

- You have created a user group.

Edit name and description

To edit a user group, proceed as follows:

1. Select the user group in the "User groups" tab.
2. In order to edit the name and description of the user group click "Edit".
 - The edit user group popup window appears.
3. Edit the name and description and click "Save".

4. In order to edit the user or role assignments, click "Edit assignments" in the "Users" or "Roles" section.

- The edit assignment popup window appears.

5. Select the user or role you want to assign and click "Next".



You can use the filter to find the user or role faster.

6. To save the assignment, click "Save".

Result

You have edited the user group and its assignments.

Nested user groups

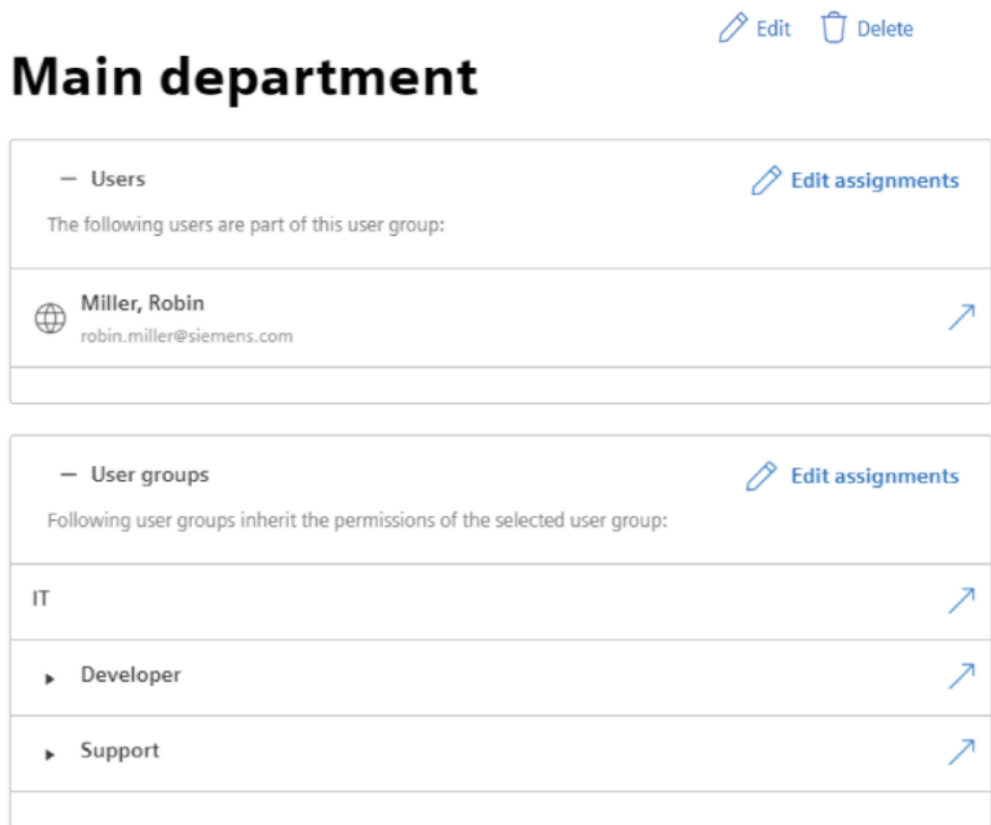
You can assign user groups to other user groups. This allows you to create nested user groups. Roles assigned to a user group are inherited to all subordinated user groups. Subordinated user groups may contain additional roles with more permissions.

Example scenario

A company creates groups for a department in the following hierarchy:

- The main department is the first level in the hierarchy.
- Under the main department is an IT area with the following divisions:
 - Developer
 - Support

The following screenshot shows the user group "main department" in Settings:



Objective

- All groups should get the StandardUser role.
- The Developer group is also to receive the DeveloperAdmin role.

Procedure

1. Open the "User groups" tab and create the user groups.
2. Select the top level group, e.g. Main department and click "Assign user groups".
3. To add the first hierarchy level assign the first user group, e.g. "IT".
4. Select the first hierarchy level in the "User group" tab. e.g. "IT".
5. To add the second hierarchy level assign the other user groups, e.g. "Developer, Support".
6. Select the main group and assign the StandardUser role.
7. Select the second hierarchy level group, e.g. "Developer" and assign the DeveloperAdminrole.

Result

- You have created a user group.
- All users of all groups have the StandardUser role.

- Only users of the Developer group have the DeveloperAdmin role.

3.3 Technical Users

Introduction

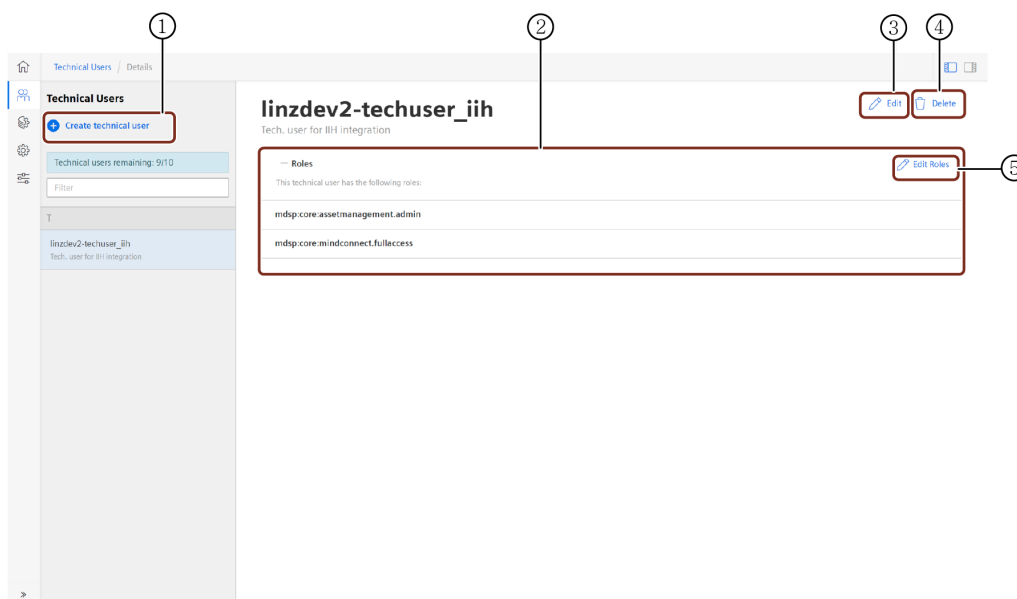
Settings allows you to create and manage Technical Users for your Insights Hub environment. They can be used for accessing Insights Hub APIs, similar to App Credentials. You can create a maximum of 10 Technical Users within the Settings application.

Prerequisite

Only the users with TenantAdmin role can create and manage Technical Users.

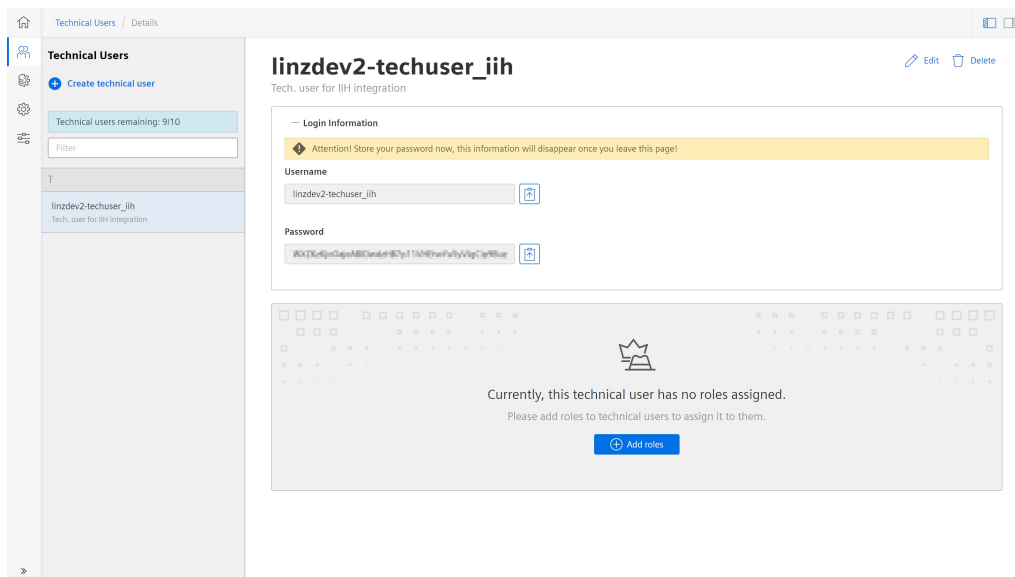
User interface

Access the "Technical Users" Tab from the left navigation. The following graphic shows the "Technical Users" section.



- ① Create a new technical user
- ② Shows the assigned roles of the technical user
- ③ Edit the description of the technical user
- ④ Delete the technical user
- ⑤ Edit the assigned roles of the technical user

Once you have created a Technical User, the following screen with the Technical user details is shown. The password will disappear, if you refresh the page or select another technical user or move out of the current screen.



Create a new Technical User

To create a new Technical User, proceed as follows:

1. Open the "Technical User" tab and click "Create technical user".
2. Enter a user name, e.g. "robin".



- The username uses the tenant name as a prefix.

3. Enter a description for the Technical User.
4. Click "Create technical user".
 - The Login information appears.

5. To copy the username and the password into clipboard, click



- The password will disappear, if you refresh the page or select another technical user or move out of the current screen.

Result

- You have created a Technical User. It can now be used to access Insights Hub APIs.

Edit role assignment for Technical User

It is now possible to edit the role assignment of the Technical User. To edit the role assignment for the Technical User, proceed as follows:

1. Open the "Technical User" tab and select the Technical User you want to edit.
2. Click "Edit Roles" in the "Roles" tab.
3. Select the roles you want to add or deselect the role you want to remove and click "Next".
4. Click "Save".

Delete Technical User

Once you reach the maximum number of Technical Users, you can delete the Technical Users which are no longer required. To delete the Technical User, proceed as follows:

1. Open the "Technical User" tab and select the Technical User you want to delete.
2. Click "Delete".
3. To delete the Technical User, click "Delete" in the confirm dialog.

Result

- You have deleted the selected Technical User and the remaining Technical User number increases.

Obtain a token for Technical User

To directly work with Insights Hub API's you need to obtain a token using the credentials of the Technical User that you have just created.

To get a token, you have to execute a POST request using the following URL

`https://{tenantName}.piam.eu1.mindsphere.io/oauth/token?grant_type=client_credentials`.

1. Provide the client id and client secret of your Technical User as basic authentication (RFC7617)

Sample request:

```
POST https://{tenantName}.piam.eu1.mindsphere.io/oauth/token?grant_type=client_credentials HTTP/1.1
Authorization: Basic {base64 encoded client_id:client_secret}
```

Sample request using python:

```
ServiceUrl = f"https://{tenant}.piam.eu1.mindsphere.io/oauth/token?grant_type=client_credentials"
MessageBytes = str({clientId}+":{secret}").encode('ascii')
Base64Credentials = base64.b64encode(MessageBytes)
ResponseTechToken = requests.request('POST', ServiceUrl, headers={'Aut
```

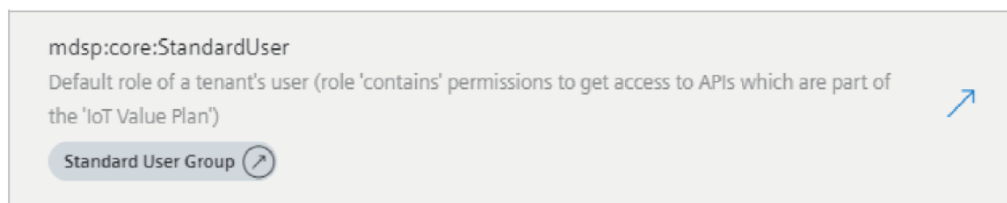
```
horization': 'Basic ' + str(Base64Credentials.decode("utf-8")), 'accept': 'application/json'})
```

Sample response:

```
{
  "access_token": "eyJhbGciOiJSUzI1NiIsImprdiSI6Imh0dHBzOi8vZWVucHlyLnBpYW0...nWf088P29u10zw",
  "token_type": "bearer",
  "expires_in": 1799,
  "scope": "mdsp:core:assetmanagement.admin",
  "jti": "da6c28e603axxxxa6b0c40a2072c9c5"
}
```

3.4 Roles

A role is a collection of permissions that can be assigned to a user or user group. When you assign a role to a user, the user receives all rights that are defined for the corresponding role. You can manage the access rights of your employees with role assignment. The role assignment in the "User" tab shows in which user group the role is included:



You can create the following types of roles:

- App roles
- Core app roles
- Custom roles
- Standard roles

App roles

Each application offers individual roles that grant access to the application. Every application in Insights Hub can have their own app roles, that can be assigned to relevant users. The app roles are either used by Insights Hub for core applications such as e. g. Asset Manager, or the developer for 3rd party applications.

Roles for other applications will be made available in Settings automatically once the app was

bought. For example, you can assign the Visual Flow Creator User role to users via Settings to grant them access to the Visual Flow Creator.

Core app roles

Core app roles are app roles of Insights Hub system tools like Asset Manager or Insights Hub Monitor.

You can identify core app roles on the prefix: mdsp:core.

You can enable core app roles in your tenant to make them available.

You can find a list of all available core app roles in chapter [core app roles](#).

Custom roles

Custom roles are flexible roles that you can define.

With custom roles you can bundle roles from each role category like default roles, app roles or custom roles into a new role. This enables you to assign individual combinations of permissions to users and user groups.

Standard roles

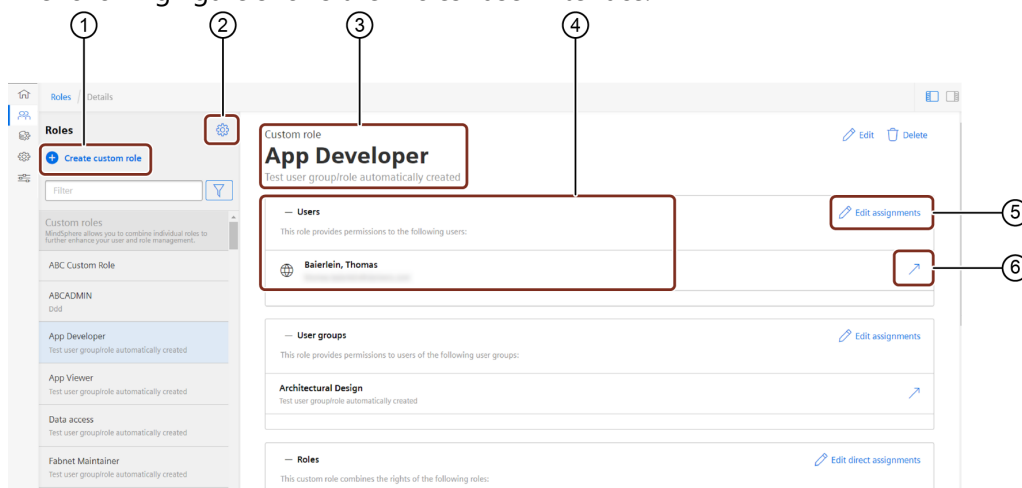
A standard role is a set of app roles.



You can use the core app roles for the assignment of single apps like Insights Hub Monitor. Please also assign the Launchpad role for accessing apps.

User interface "Roles"

The following figure shows the "Roles" user interface:

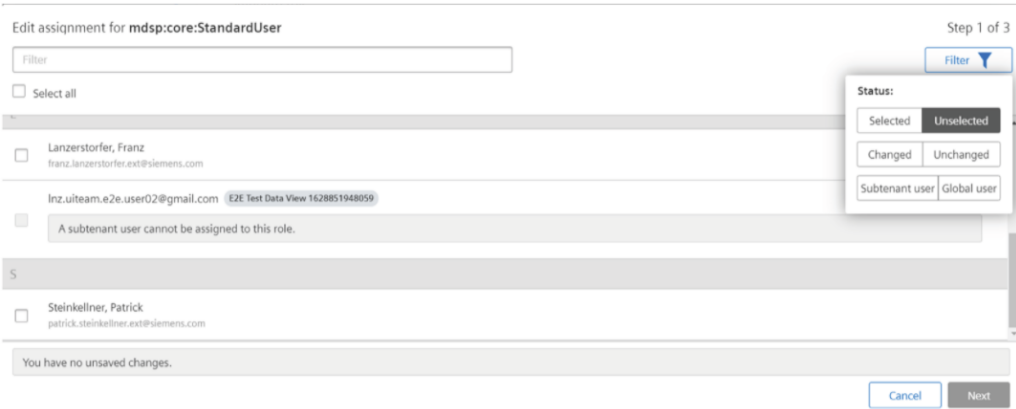


① Create a new custom role

- ② Opens core app role configuration window
- ③ Role details:
 - Name of the role
 - Description of the role
- ⑤ List of all users assigned to the role
- ⑥ Click on "Edit user assignment" to assign or remove users to the role
- ⑦ Click on the arrow to change to the "Users" interface

Edit assignment screen

The "Edit assignment" screen allows you to assign or remove users to the role. You can filter users according to fixed parameters.



Filter parameter of "Edit assignment"

You can use filter and combine the parameter to find sought user. The following table shows the filter parameter:

Filter	Description
Selected	Shows all selected users of the "Edit assignment" screen.
Unselected	Shows all unselected users of the "Edit assignment" screen.
Changed	Shows all changed and unsaved user. The list also highlights changed user.
Unchanged	Shows all unchanged user.
Subtenant user	Shows all as subtenant user created user.
Global user	Shows all global user.

Standard roles

A standard role consists of different permissions to use particular applications in Insights Hub and can be subdivided into the following categories:

- **Administrative access:** Full use without restrictions within a tenant.
mdsp:core:TenantAdmin, mdsp:core:OperatorAdmin,
mdsp:core:DeveloperAdmin
- **Standard access:** Restricted use within a tenant. The system manuals of the apps provide detailed information about the permissions. mdsp:core:TenantAdmin,
mdsp:core:OperatorAdmin, mdsp:core:DeveloperAdmin
- **Subtenant access:** Restricted use as a subtenant user within a tenant.
mdsp:core:SubTenantUser

The system manuals of the apps provide detailed information about the permissions.

The following table describes which license you need in order to utilize the respective default role:

Standard role	Role ID
TenantAdmin	mdsp:core:TenantAdmin
StandardUser	mdsp:core:StandardUser
SubtenantUser	mdsp:core:SubTenantUser
OperatorAdmin	mdsp:core:OperatorAdmin
DeveloperAdmin	mdsp:core:DeveloperAdmin
Developer	mdsp:core:Developer

You can find detailed information to each standard role in the following sections:

Assign users to a role

You can assign a user to a role in the tab "Roles" or assign roles to a user in the tab "Users". You can find more information about users in the section [Managing users](#).

Procedure

In order to assign a user to a role proceed as follows:

1. In the navigation, click "Roles".
2. Select the relevant role in the selection list.
3. Click "Edit assignments".
 - The "Edit assignment" dialog box opens.
4. Select the users from the list.

- In order to find the searched users faster you can use the filters. You can find more information about filter in the chapter [User interface "Roles"](#).
5. Select or clear the appropriate check boxes to assign or unassign users to the role.
 6. To approve the changes, click "Next".
 7. To save the changes, click "Close".

Result

You have assigned a user to a role. The corresponding user must log in again for the changes to become effective.




After reassigning roles, you need to log out and log in for these changes to take effect.

Create custom roles

Procedure

In order to create a custom role proceed as follows:

1. In the navigation, click "Roles".
2. To create a custom role click  or "Create custom role".
3. Enter a name and description.
4. To save the new custom role click "Create custom role".

Result


- You have created a new custom role.
- The new role appears in the custom role list.
- You can customize the new role by adding roles, users and user groups.

Configure core app roles

You can enable core app roles in your tenant to use them for finer grained access control.

Procedure

In order to enable core app role proceed as follows:

1. In the navigation, click "Roles".
2. To open the core app roles configuration click .
3. Select the core app roles you want to use in your tenant and click "Next".
4. To use the core app roles in your tenant and save the settings click "Save".



Disable core app roles

You can also disable a core app role by deselecting it. Disabling a core app role removes the role from all assigned users, user groups and roles. Please note that associated permissions granted to your user will be removed.

Result

- You can now use the added core app roles in your tenant.
- You can add the core app roles to a custom role.

Data Access

4

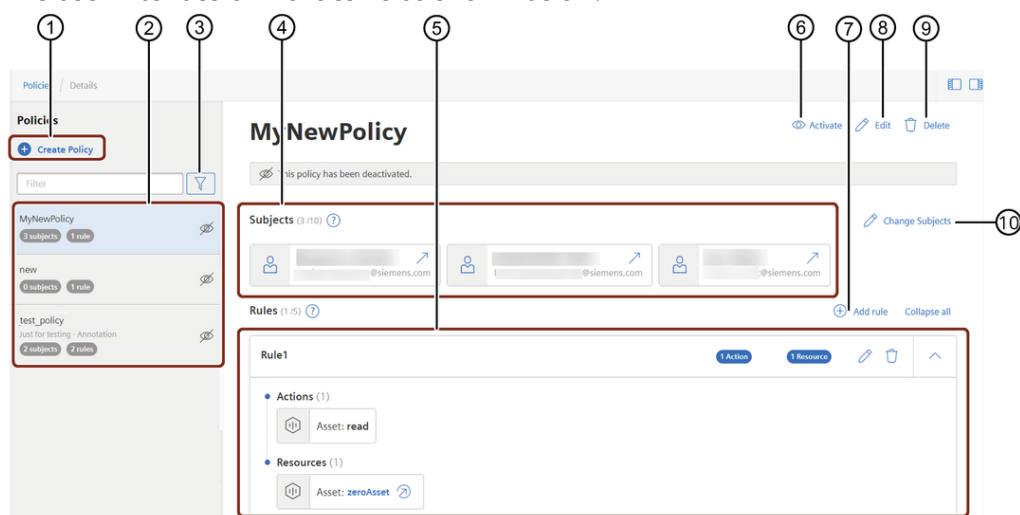
4.1 Introduction to policies

A policy describes a given set of subjects and is allowed to perform a given set of actions on a specified set of resources or resource groups. Set of actions, and resources are bound by a rule, and a policy can have multiple rules.

Subjects are users or user groups who are allowed to perform certain actions on certain resources.

A rule is just a container that holds tuple of *actions* and *resources / resource groups*. A policy can contain multiple rules. For more information on Resource Groups, please refer to [Creating a new Resource group](#)

The user interface of "Policies" is as shown below:



- ① Opens a new window to create a new policy
- ② List of available policies for the tenant
- ③ Filter icon to filter the available policies. The available filter options are: Active and Inactive
- ④ Subjects assigned to the selected policy. Subjects can be Users or User groups
- ⑤ Rules created for the selected policy
- ⑥ Activate/Deactivate the selected policy
- ⑦ Add new rule for the selected policy
- ⑧ Edit the selected policy
- ⑨ Delete the selected policy
- ⑩ Change the subject for the selected policy. The available options are: Change assigned users and change assigned user groups

For more information on Policies, please refer to [Resource Access Management](#).

4.2 Creating a new policy

Pre-requisites

For creating a policy, ensure that you have tenantadmin role assigned.

Creating a new policy

To create a policy, proceed with the following steps:

1. In the "Settings" application, click "Policies" tab in the left navigation.
2. Click "Create Policy".
3. Enter the policy name and description.
4. Click "Create policy".

Create Policy
Create a policy, to provide asset access to users and user groups.

Policy name: *
test-policy
Please enter a policy name.


Description:
This is for testing
Please enter a description text.

* Required input field

Create policy Cancel

Assigning users or user groups to the policy

To assign users or user group to the created policy, proceed with the following steps:

1. In the "Policies" screen, select the policy for which you want to assign users or user groups.
2. To add users, click "Add users" and to add user groups, click "Add user groups".
3. In the "Edit assignment" window, select the users/user groups to be assigned to this policy and click "Next".
4. Click "Save".
5. To activate the policy, click  Activate .

The selected users/ user groups are successfully added to the policy.

Adding rules to the policy

To add rules to the policy, proceed with the following steps:

1. In the "Policies" screen, select the policy for which you want to add rule.
2. Click "Add rule".
3. In the "Resource selection" step, select Assets, IDL Folders or Resource groups and click "Next".

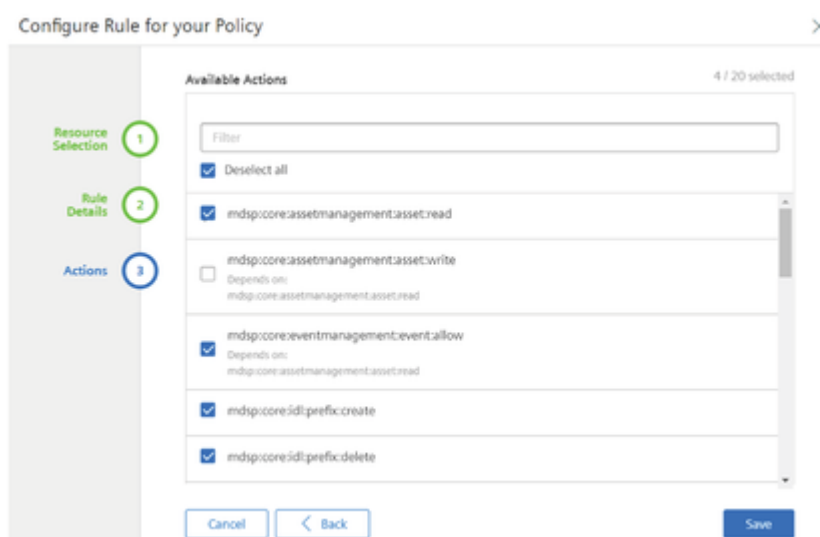
The screenshot shows the 'Configure Rule for your Policy' dialog with the 'Resource Selection' step highlighted. On the left, a sidebar shows three steps: 'Resource Selection' (1), 'Rule Details' (2), and 'Actions' (3). The main area is divided into 'Assets' and 'Resources'. Under 'Assets', there is a 'Filter' input, a 'Deselect all' checkbox, and a list of assets: 'bergTest' (checked), 'fablasset4' (checked), 'fabirout' (unchecked), 'landTestArea' (unchecked), and 'landTestWeather' (unchecked). Under 'Resources', there is a list showing '2 / 20 selected' with 'bergTest' and 'fablasset4' listed. At the bottom, there are 'Cancel' and 'Next >' buttons.

4. In the "Rule Details" step, select the propagation depth and click "Next". The available options are: "Only selected", "Direct children" and "All children".

The screenshot shows the 'Configure Rule for your Policy' dialog with the 'Rule Details' step highlighted. The sidebar shows 'Resource Selection' (1), 'Rule Details' (2), and 'Actions' (3). The main area has a 'Name' field with the value 'test-doc-rule' and a note: 'Name will be generated automatically if field is left empty.' Below this is the 'Propagation Depth' section with three radio button options: 'Only selected' (unchecked, with subtext 'Only the selected resources are accessible.'), 'Direct children' (checked, with subtext 'The selected resources and its next successors are accessible.'), and 'All children' (unchecked, with subtext 'The selected resources and all its successors are accessible.'). At the bottom, there are 'Cancel', '< Back', and 'Next >' buttons.

5. In the "Actions" step, select the required actions that needs to be enabled for the assigned users/user groups.

6. Click "Save".




The policy needs to be activated for it to be available for the assigned users/user groups with the configured rules. For steps to activate the policy, refer [Activating or deactivating a policy](#).

It is possible to edit or delete the policy by clicking "Edit" and "Delete" button respectively.

For more information on policies, please refer to [Resource Access Management](#).

4.3 Activating or deactivating a policy

To activate or deactivate a policy, proceed with the following steps:

1. In the "Settings" application, click "Data Access" from left navigation and click "Policies".
2. From the list of available policies, click on the policy which needs to be activated or deactivated.
3. Click  Activate to activate the policy, or click "Deactivate" to deactivate the policy.

After activating the created policy, the users/user groups assigned to this policy will now be able to view the assigned assets in their tenant. The rule configured for the policy will be applicable for the assigned users/user groups.

For more information on policies, refer "Resource Access Management" section in [Developer Documentation](#).

4.4 Creating a new resource group

Pre-requisites

For creating a resource group, ensure that you have tenantadmin role assigned.

Creating a new resource group

- To create a resource group, proceed with the following steps:
1. In the "Settings" application, click "Resource groups" tab in the left navigation.
 2. Click "Create resource group".
 3. Enter the resource group name and description.
 4. Click "Create resource group".

Create resource group

Enter basic resource group information here.

Resource group *

MyFirstResourceGroup

Please enter a resource group name.

Description

This is my first resource group

Please enter a description text.

* Required input field

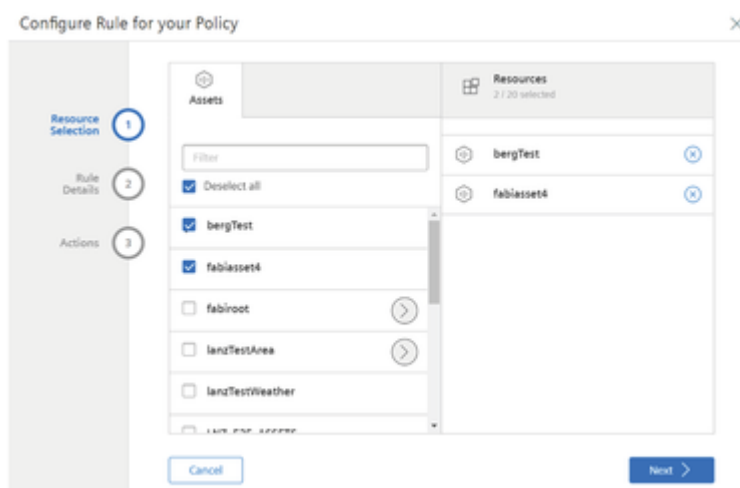
Create resource group

Cancel

Adding resources to the resource group

- To add resources to the resource group, proceed with the following steps:
1. In the "Resource groups" screen, select the resource group for which you want to add resources.
 2. Click "Add resources".

3. In the "Resource selection" step, select Assets or IDL Folders.



4. Click "Save".

It is possible to edit or delete the resource groups by clicking "Edit" and "Delete" button respectively.

For more information on "Resource Access Management", please refer to [Resource Access Management](#).

4.5 Using subtenants

Environments and subtenants in "Settings"

Environments

An environment is the digital representation of a real organization. An environment contains users, data, assets and other properties.

An environment groups the users and offers them access to Insights Hub. All users within an environment have a common view of the saved data. By default, users only see the data of the assigned environment.

Subtenants

You can create and manage additional so-called subtenants within an environment. The subtenants can represent additional organizations or departments.

You can assign multiple users to a subtenant. Users of a subtenant only see the associated assets and data of the subtenant in the respective Insights Hub application.

You can find additional information on viewing assets and user rights of subtenants in the [Asset Manager](#) documentation .

Assignable roles to subtenant users

Only specific roles are useful or even allowed for a subtenant user. To protect the administrator from misconfiguration, certain core roles are blocked for assignment to subtenant users.

This blocking works in all directions:

- Subtenant user cannot be assigned to user groups which have a not assignable role.
- Roles cannot be assigned to user groups which have subtenant users assigned.

You can assign the following roles to a subtenant user:

- mdsp:core:SubTenantUser,
- mdsp:core:fleetmanager.subtenantuser
- mdsp:core:va.subtenantusage
- mdsp:core:visualexplorer.viewer,
- mdsp:core:vfc.admin
- mdsp:core:vfc.user
- mdsp:core:vfc.viewer

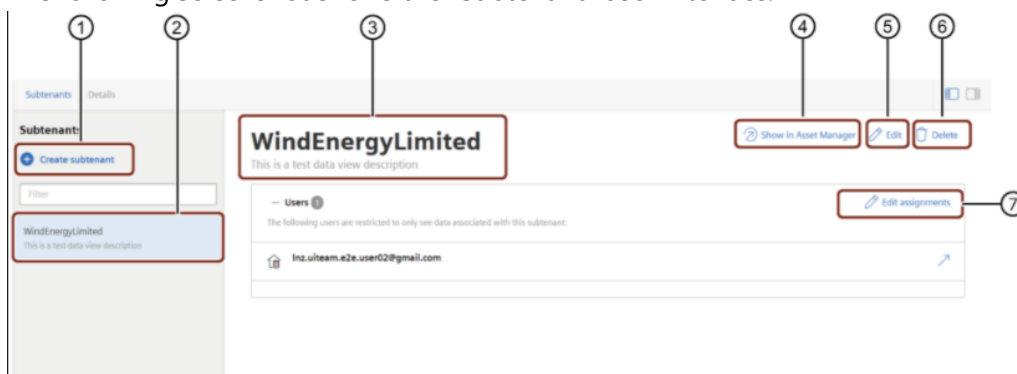
Only Insights Hub core roles (mdsp:core:*) are blocked and explicitly unlocked for subtenants. All other roles are always unlocked.



As administrator, you should always be careful with the assignment of users to roles and user groups.

"Subtenant" user interface

The following screenshot shows the "Subtenant" user interface:



- ① Creates a new subtenant
- ② List of created subtenants
- ③ Subtenant name and description
- ④ Shows the subtenant assets in Asset Manager

- ⑤ Opens a dialog to edit the subtenant name and description
- ⑥ Deletes the subtenant
- ⑦ Opens a dialog to edit the assignments for the selected subtenant.



Operator tenants do not support the subtenant functionality

The subtenant option is not available in Operator tenants. Settings in Operator tenants do not display the tab "Subtenants".

Create new subtenant

Prerequisite

You can only create a subtenant, if you initially have generated the provider information. With the initial design of the provider information, you read confirm the provider information. Additionally you agree with the terms and conditions associated with it. You must not enter the basic information or formulate tenant provider links necessarily to create a subtenant.




Quota consumption

The creation of a new subtenant reduces your quota.

Procedure

To create a new subtenant, proceed as follows:

1. Click on "Subtenant" in the navigation.
2. Click on  "Create subtenant".
 - The "Create subtenant" dialog opens.
3. Add a subtenant name.
4. Add a description for the subtenant.
5. Click "Create".

Result

You have created a new subtenant.

Assign users to a subtenant

You can assign a user to a subtenant when creating the user by choosing the user type.

Prerequisite

- You have created a subtenant.

- You have created a subtenant user.

Procedure

To assign a user to a subtenant, proceed as follows:

1. In the navigation area, click "Subtenant".
2. Select the desired subtenant in the selection list.
3. Click "Assign users".
 - The "Assign users to:<SubtenantName>" dialog opens.
4. Select the user you want to assign in the list and click "Next".
5. To save the configuration, click "Save".
6. In order to close the settings, click "Close".

Result

You assigned the user to the subtenant.

Remove user from a subtenant

Procedure

To remove a user from a subtenant, proceed as follows:

1. In the navigation area, click "Subtenant".
2. Select the desired subtenant in the selection list.
3. Click "Assign users".
 - The "Assign users to:<SubtenantName>" dialog opens.
4. Select the user you want to remove in the list "Available users".
5. To remove the user of the subtenant, click .
6. To save the configuration, click "Close".

Result

You removed the user from subtenant.

4.6 Collaborations

You can request collaborations with other tenants in Settings. This gives you the opportunity to share your assets with other tenants by using Cross-Tenancy. You can find more information about sharing assets in the Asset Manager documentation. In order to perform a collaboration, you need to know the name of your partner's tenant ID for the handshake procedure. Each party may refuse a request or end an existing collaboration at any time. The collaboration UI provides an overview of all existing and requested collaborations.

Offer collaboration

You can offer a collaboration with all tenants in the same region. Your collaboration offer needs to be accepted by the receiving tenant.

Revoke pending collaborations

You can revoke a pending offered collaboration as long as the collaboration has not yet been confirmed by the receiving tenant.

Terminate collaborations

The "Collaboration" section shows all existing collaboration. You can terminate a collaboration at any time.

Offering a new collaboration

In order to start a new offer for a collaboration proceed as follows:

1. In the main navigation, click "Collaborations".
2. In order to start a new offer, click "Offer Collaboration".
3. Enter the tenant ID of your collaboration partner.
 - You have to request the respective tenant ID from your collaborative tenant.
4. To accept the legal notice, activate the checkbox.
5. To start the request, click "Offer".

Your request will be shown in the "Offered Collaborations" section as pending. The receiving tenant can see the number of pending collaboration offers in its collaboration section.

- As long as the receiving tenant has not accepted your offer, you can revoke the offer by clicking "Revoke".
- After the receiving tenant has accepted the offer, your collaboration will appear below in the "Collaboration" section.

4.7 Customize the OS Bar with "Provider"

Overview of OS Bar

The OS Bar provides the following information:

- Company and tenant information
- Application information
- Insights Hub information

The information varies whether you are looking at the OS Bar from the Launchpad or in the application. In order to view the information, click on respective name in the OS bar. The information is displayed as a drop down menu.

Company and tenant information

You can customize the following company information in Settings:

- Your company logo
- Your company name
- Tenant provider links

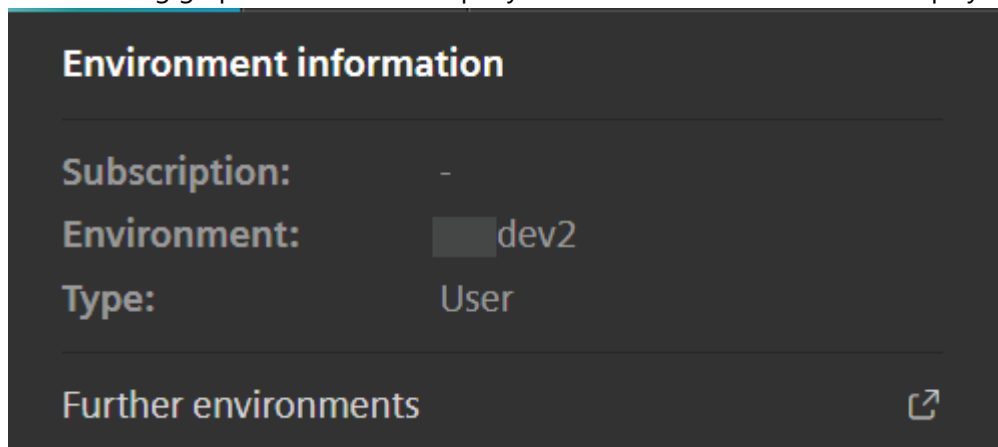
You can edit the tenant provider links in different languages.

Furthermore, the following information is displayed:

- Environment name
- Environment type
- Subscription
- Further environments

You can specify this information when ordering the environment. In Settings this information cannot be edited.

The following graphic shows the company and environment information displayed in the OS Bar:



Application information

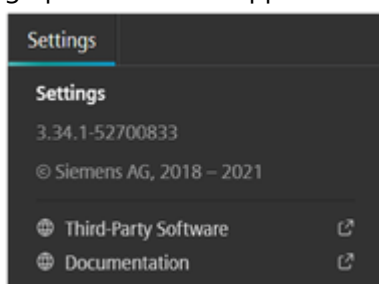
The following information is displayed in the application information:

- Name of the application
- Version number

Further information can be provided by the developer via Developer Cockpit, for example:

- Third-Party Software
- Documentation

Application information cannot be edited via Settings. You can find more information about how to edit the application information in [OS Bar](#) in the developer documentation . The following graphic shows the application information displayed in the OS Bar:



Insights Hub information

The "powered by {{ whitelabel.companyName }} Xcelerator" displays the following general information:

- Current Insights Hub version
- Link to the Industrial IoT Store
- Link to status page with the latest information on updates and maintenance

Tenant-specific adjustments

With the "Provider" function you can customize your tenant by providing basic information about the company. Furthermore, you can define links that provide custom information. Links to custom pages link to the corporate information or the support page of your company. These links can be seen in the OS Bar on the Launchpad. If you do not create your own specifications, the {{ whitelabel.companyName }} default information is displayed. With the "Provider" function, you have the option for every tenant to individually configure the following:

- Contact information
- Company information
- Links to additional information
- Tenant provider links in different languages
- Regions which contain several countries (only available within an Operator tenant)

- Basic tenant information

The company-specific links are only visible to users that do not have the TenantAdmin role. Users with the TenantAdmin role continue to see the default information.

Support of multilingualism

Every tenant is assigned to only one country. Nevertheless, users from other countries can access a tenant. Users from other countries usually have their browsers set to the regional language.

The OS Bar of a tenant displays company-specific links. You can configure these links in different languages in the "Provider" function, to support users from other countries. If the set browser language is not configured, the links are shown in the "default" language. You cannot edit or configure the "default" language.

After the configuration of a new language in the "Provider" function, the user sees the company specific links in the language set in the browser.

Create regions

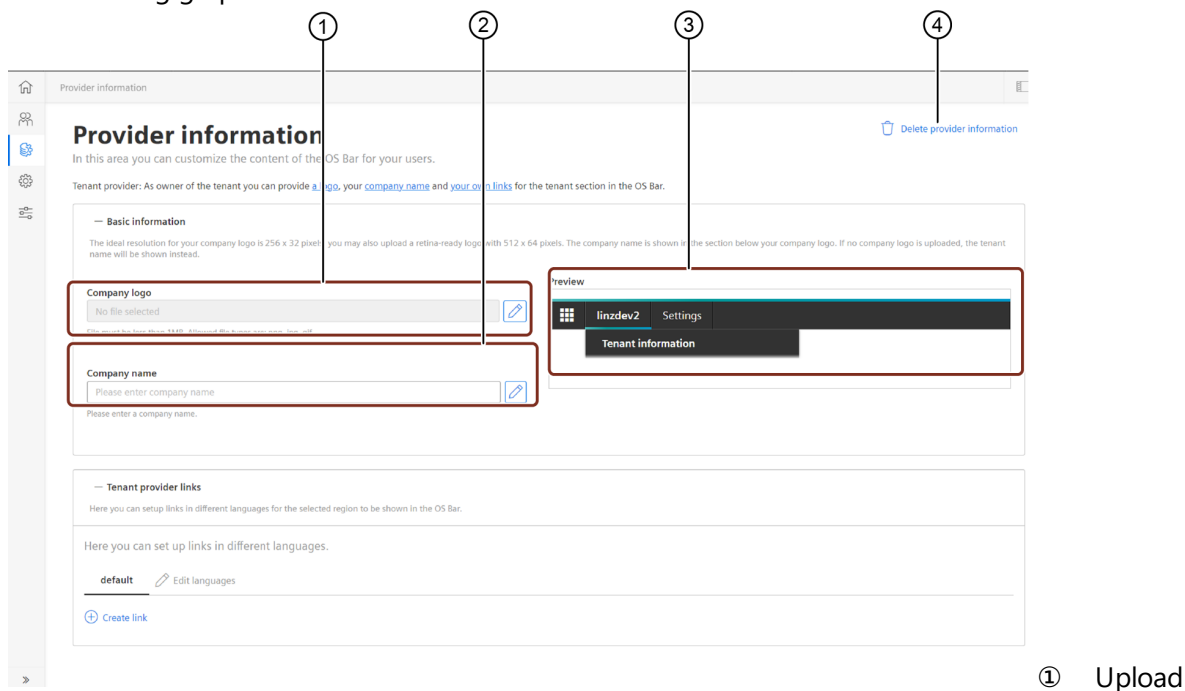
!!! note

The "create regions" functionality is only supported in Operator tenants.

"Provider information" offers the option to configure your own regions. With "Create regions" you can specify links for a certain region with several countries. A region can be, for example, South America. For this region, you can add the respective countries and configure the language of the links as needed. This case occurs when different regions or countries have different legal requirements for links. For example, a tenant in South America can see different information than a tenant in Europe.

User interface "Provider"

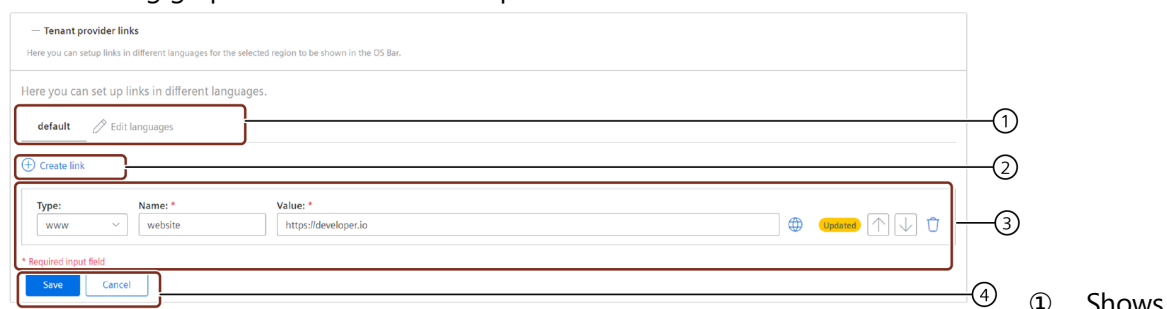
The following graphic shows the "Basic information" area within the "Provider" interface:



or edit your company logo

- ② Add or edit your company name
- ③ Shows a preview of the added information
- ④ Delete the provider information

The following graphic shows the "Tenant provider links" area within the "Provider" user interface:



the default language which is adopted from the set browser language as well as the option to add more languages with "Edit language"

- ② Creates a new bar to add the link details
- ③ Shows the link parameters and buttons for adjustments
- ④ Save or cancel settings

Parameter for links







The following table shows a description of the link parameters:

Parameter	Description
Type	Select the link type: E-mail address, Web link, Telephone number
Name	Add an individual name for the link.

Parameter	Description
Value	Add a specific value for the link type: E-mail address, for example contact@mindsphere.io ; URL, for example https://www.mindsphere.io ; Telephone number

Symbols

The following table shows the buttons of the link parameter area:

Symbol	Description
	Opens the URL to check if it is correct.
	Opens your local e-mail client to check if it works.
	Opens a telephone app and asks if number shall be called.
	Moves the link downwards.
	Moves the link upwards.
	Deletes the link.

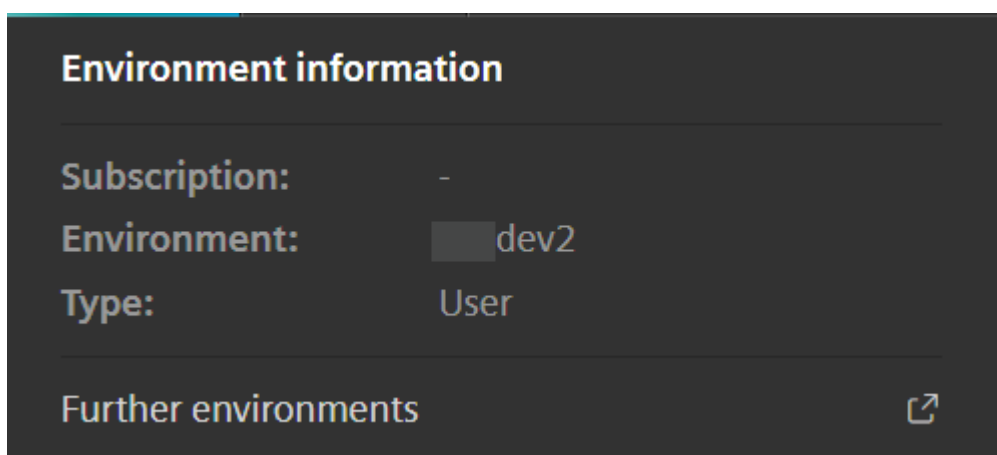
Edit tenant basic information

Procedure

- To create the basic information, proceed as follows:
1. In the navigation area, click "Provider".
 2. Open the area "Basic information".
 3. Upload your company logo as a png, gif or jpg with file size less than 1 MB.
 4. Enter your company name.
 - The changes are saved automatically.
 5. In order to confirm your changes, click the check or press enter.

Result

The "Basic information" area shows a preview of your company logo and company name in the OS Bar. The following graphic shows the result in the OS Bar:



Creating links for different languages

The following example shows how you can define own provider links in Settings.

Example scenario

The MindEdge Corporation, based in Germany, has a tenant with users from Spain. The links in the OS Bar should be displayed in the regional language Spanish for the Spanish users.


Objective

- The new language "Spanish (es)" should be set.
- The defined links should be displayed in the OS Bar in Spanish for Spanish users.

Procedure

In order to create a new link for a new language proceed as follows:

1. In the navigation area, select "Provider".
 - The "Provider information" interface opens.
2. To open the "Tenant provider links" area, click on **+**.
3. Select "Edit languages".
 - The "Edit languages" dialog box opens.
4. Select the language that need to be configured for the translation of the links and click **>**, e.g. "Spanish: Castilian".
5. To save the selected language and close the dialog, click "Save".
6. In order to create a new link, select the language and click "Create link".
 - A new row with input boxes appears.
7. Select the type of the link in the "Type" box, for example "www".
8. Enter an individual name in the "Name" box, e. g. "Spanish support" .

9. Enter a valid URL in the "Value" box, e. g. "<https://www.mindsphere-support.es>".
10. To test the link, click .
11. To save the settings, click "Save".

Result

The new language "es" is displayed in addition to the default language "default":



The new link for a new language Spanish was created in Settings. Spanish users will now see the Spanish link in their Launchpad and will be redirected to the set URL.



Create new regions

!!! note

The function "create regions" is only available in Operator tenants.

Procedure

To define a new region, proceed as follows:

1. In the navigation area, click "Provider".
 - The "Provider information" interface opens
2. To open the "Tenant provider links" area click on .
3. Click on "Create region".
 - The dialog "Create region" opens.
4. Add an individual region name.
5. Select the countries from the list "Available countries" as needed.
6. To assign the countries click .
7. To save the configuration click "Create".

Result

The new region has been created.

4.8 Service Credentials

Introduction Service Credentials

Settings allows you to create Service Credentials for your Insights Hub environment. Within the "Service Credentials" tab you can create a maximum of 3 Service Credentials. Service Credentials are valid for Cloud Foundry and cannot be used for Insights Hub APIs. The Org Manager and Space Developer role from Cloud Foundry is supported. You can find more information in the Cloud Foundry documentation.

(<https://docs.cloudfoundry.org/concepts/roles.html>)

Requirements

You can access the Service Credentials tab in an operator or a developer tenant. In order to get access to the Service Credentials tab and to create Service Credentials you need one of the following roles:

- TenantAdmin
- OperatorAdmin
- DeveloperAdmin
- ServiceCredentialAdmin

Service Credential status

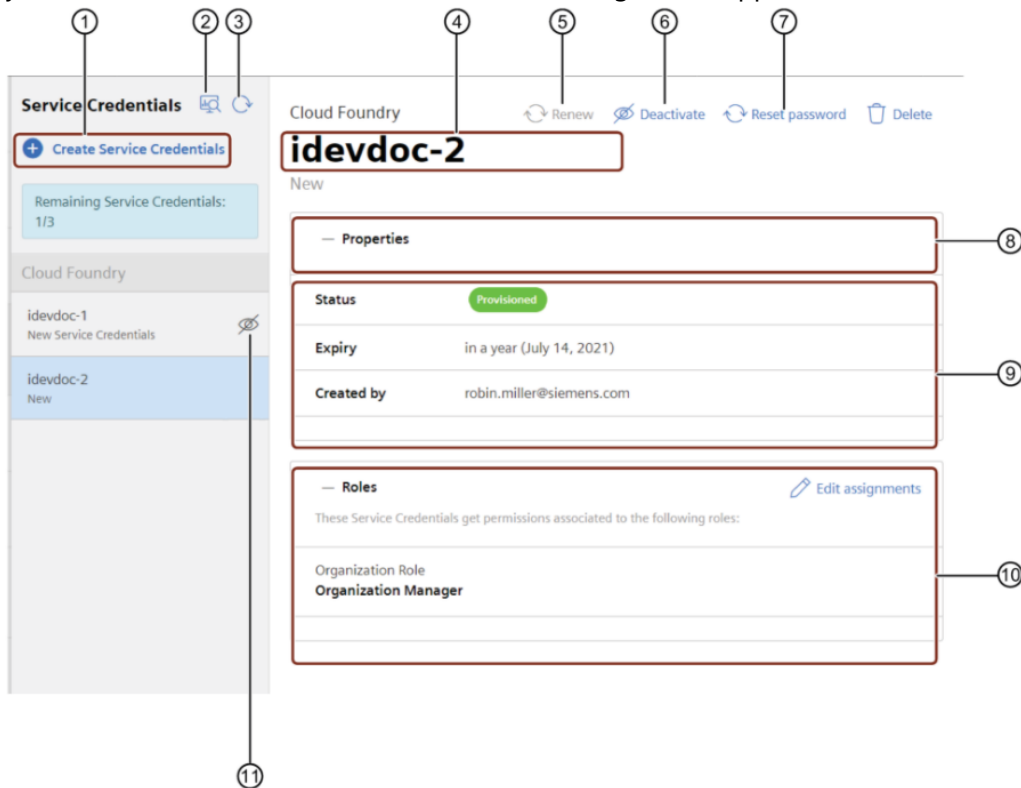
Your Service Credentials can have the following status:

Status	Description
Activating	Shows that the Service Credentials are activated.
Deactivated	Shows that the Service Credentials are deactivated.
Deactivating	Shows that the Service Credentials are currently deactivated.
Expired	Shows that the Service Credentials expiry date has been exceeded.
Provisioned	Shows that the Service Credentials were provisioned and are ready to use.
Provisioning	Shows that the Service Credentials are currently provisioned.
Provisioning failed	Shows that the Service Credentials provisioning failed.
Deprovisioning	Shows that the Service Credentials are deleted.
Renewing Credentials	Shows that the Service Credentials are renewed.
Resetting	Shows that the password of the Service Credentials gets reset.
Updating	Shows that Service Credentials are currently updated.

You can see the status and the types of change in the history.

User interface "Service Credentials"

You can access Service Credentials via the "Service Credentials" tab inside the Settings app. After you have created a Service Credential the following screen appears:



- ① Create new Service Credentials
- ② Opens the history of all changes made in the last 90 days
- ③ Refreshes the site
- ④ Shows the Service Credentials name
- ⑤ Renews the Service Credentials
- ⑥ Activates or deactivates selected Service Credentials
- ⑦ Reset the password
- ⑧ Shows the login information with username and password until the site gets refreshed
- ⑨ Shows the properties of the selected Service Credentials
- ⑩ Shows the assigned role to the Service Credentials
- ⑪ Shows an error and that the Service Credentials are not active

Create new Service Credentials

Requirement

You have one of the following roles:

- OperatorAdmin
- DeveloperAdmin

Procedure


In order to create new Service Credentials proceed as follows:

1. Open the "Service Credentials" tab and click "Create Service Credentials".
2. Enter a client ID, e.g. "robin".



- The username uses the tenant name as a prefix.
- Only a-z and 0-9 are allowed as characters.

3. Enter a description for the Service Credentials.
4. Enter an expiry date for the Service Credentials. The default expiry date is one year.
5. Assign a role to the Service Credentials.
6. Click "Create Service Credentials".
 - The Login information window appears.

7. To copy the username and the password into clipboard, click  .



- The password will disappear after refreshing the page.
- You can reset the password later.

Result

- You have created Service Credentials.
- After refreshing the site the "Properties" status switches from "Provisioning" to "Provisioned". This credential is now ready for use.
- You can now log in into your Cloud Foundry account with these credentials.

Edit role assignment for Service Credentials

You can edit the role assignment of your Service Credentials.

Procedure

To edit the role assignment for Service Credentials proceed as follows:

1. Open the "Service Credentials" tab and select the Service Credentials you want to edit.
2. Click "Edit assignment" in the "Roles" tab.
3. Select the roles you want to add or deselect the role you want to remove and click "Next".
4. To save the changes, click "Save".

Deactivate Service Credentials

You can deactivate Service Credentials to temporarily revoke access for a user.

Requirement

You have created Service Credentials.

Procedure

To deactivate Service Credentials proceed as follows:

1. Open the "Service Credentials" tab and select the Service Credentials you want to deactivate.
2. Click "Deactivate Service Credentials".
 - The status changes to "Deactivating"
3. To update the provisioning status, click "Refresh".

Result

- You have deactivated the selected Service Credentials. You can not log in to Cloud Foundry with this credential.
- You can activate the Service Credentials using the same procedure.

Delete Service Credentials

You can delete Service Credentials or if you reach your limit of remaining Service Credentials or when you no longer need them.

Requirement

You have created Service Credentials.

Procedure

To delete Service Credentials proceed as follows:

1. Open the "Service Credentials" tab and select the Service Credentials you want to delete.
2. Click "Delete Service Credentials".
3. To delete the Service Credentials, click "Delete".

Result

- You have deleted the selected Service Credentials.
- The remaining Service Credentials number increases.

Renew Service Credentials

You can renew expired Service Credentials. By default, the Service Credentials are valid for one year.


Requirement

- You have created Service Credentials.
- The Service Credentials have the status "Expired".

Procedure

To renew expired Service Credentials proceed as follows:

1. Open the "Service Credentials" tab and select the Service Credentials you want to renew.
2. Click "Renew Service Credentials".
3. Enter the new expiry date for the Service Credentials and click "Renew Service Credentials".

4. To copy the username and the password into clipboard, click  .

Result

- You have renewed the expired Service Credentials. The password has been changed. You need to update your local configurations in which you used these Service Credentials.
- The status changes to "Renewing Credentials".

5.1 Certificate Manager

Introduction Certificate Manager

You can upload certificates into Insights Hub to improve the security level. The encryption adds an additional layer of security to MQTT with X509 client certificates. The certificate is valid for the domain of your tenant. You can access the Certificate Manager via the navigation area in Settings.

With the Certificate Manager you can:

- Upload and manage PEM certificates on your tenant
- Download PEM or CERT certificate to install on assets

Certificate requirements

The operating system assumes no responsibility for the quality of the device certificates. Uploading the TenantCA certificate through Certificate Manager checks the following requirements for TenantCA certificates:



For violations, the upload request will be rejected. Certificate Manager users are completely responsible of the quality of certificates. We take no responsibility in certificate management processes.

Certificate requirement	Description
Certificates signing algorithm	The device certificate signature algorithm should be SHA2.
Version	The certificate version must be at version 2 (indicating X.509 v3).
Key Usage	Key Usage extension with keycert Sign bit must be set.

Certificate requirement	Description
Validity	Validity of the certificate should be valid up to one year. The current date and time should be between Not Before and Not After.
Subject	Subject Distinguished Name (DN) is required (e.g. Customer Name (CN)=Robin Miller, Organisation Unit (OU)=Unit1, Organisation (O)={{ whitelabel.companyName }}, Locality (L)=Erlangen, Country (C)=Germany).
Subject Key Identifier	Subject Key Identifier extension is required.
Basic Constraints	Basic Constraints extension is required and Certificate Authority (CA) value must be TRUE to indicate that Subject Type is CA.

Add new certificate

In order to add a new certificate to your tenant proceed as follows:

1. Click "Add certificate" in the "Certificate" tab.
2. Enter a descriptive name.
3. Upload the CA PEM Certificate.
4. Upload the Verification PEM Certificate.
5. Click "Add".

Using "Broker info"

You can download a PEM or a CERT certificate in the "Broker info" tab. After downloading the broker certificate, you can install it on your asset via USB stick, for example.

This will establish the handshake between Insights Hub and your asset, allowing your device will to validate the X509 certificate.

5.2 Identity Provider Federation

Configuring Custom IdP

Currently, WebKey is used as the default IdP for Insights Hub. This means that, for any user to access Insights Hub, it is required to log in using Webkey.

The "Identity Provider (IdP) Federation" tab in "Settings" application enables the users to create and use their own IdP. This allows the users to take control on authentication and access Insights

Hub by onboarding their own IdP.



This functionality is applicable:

- for all the environments, if you are an existing Insights Hub customer with Insights Hub offerings (MindAccess Plans, any Upgrades etc)
- For Premium tenants only, if you are a new customer with new offering structure (Capability Packages, Asset Attributes etc)
- for "TenantAdmin" only, irrespective of existing or new customers

Configuring Custom Identity Provider (IdP)

To create and configure a new custom (IdP), proceed with the following steps:

1. From the left navigation, select "Identity Provider Federation".
2. Click "Configure Custom Identity Provider".
3. Select the required IdP type and click "Next".

link'. At the bottom are 'Cancel' and 'Next >' buttons."/>

4. Follow the configuration steps in the "External Identity Provider Configuration" step and click "Next".

If "Open ID" is selected as the provider type, then the configuration screen is displayed as in the below image:


If "SAML" is

selected as the provider type, then the configuration screen is displayed as in the below image:

Type Selection 1
Prerequisites 2
Configuration 3

Prerequisites for setting your Identity Provider configuration:

You will need the following information to complete your identity provider federation.



- Make sure that your Identity Server is up and running.
- Have the current meta data of your SAML configuration from your service provider.
- Check recommended security capabilities of your IdP in the user documentation. Click Next.

Cancel < Back
Next >

5. For Open ID, enter the configuration details as shown in the below image:

Type Selection 1
Prerequisites 2
Configuration 3

Configuration

Here you can configure your OpenID Identity Provider to be used by the current account

General Settings

Identity Provider Name *

Name your identity Provider.
Description * ⓘ

Enter a meaningful description for your identity provider. (Max. 50 characters)

User Attributes Mapping

Attribute for Email * ⓘ

Enter the attribute name where email could be found in id_token claims.

Attribute for First Name * ⓘ

Enter the attribute name where first name could be found in id_token claims.

Attribute for Last Name * ⓘ

Enter the attribute name where last name could be found in id_token claims.

Attribute for User Name * ⓘ

Enter the attribute name where user name could be found in id_token claims.

Authentication Settings

Client ID *

Enter your client id.

Client Secret *

Enter your client secret.

Origin Key * ⓘ

Configure an origin key for your identity provider.

Discovery URL *

Enter a valid discovery url.

Logout URL *

Enter a valid logout url for your identity provider.

Cancel < Back
Save

For SAML, enter the configuration details as shown in the below image:

Type Selection1

Prerequisites2

Configuration3

Configuration

Here you can configure your SAML Identity Provider (SAML 2.0) to be used by the current account

General Settings

Identity Provider Name *

saml_idp

Name your Identity Provider.

Description * ?

test

Enter a meaningful description for your identity provider. (Max. 50 characters)

User Attributes Mapping

Attribute for Email * ?

email

Enter the attribute name where email could be found in id_token claims.

Attribute for First Name * ?

first name

Enter the attribute name where first name could be found in id_token claims.

Attribute for Last Name * ?

last name

Enter the attribute name where last name could be found in id_token claims.

Authentication Settings

Origin Key * ?

key

Configure an origin key for your identity provider.

Logout URL *

https://google.com

Enter a valid logout url for your identity provider.

Meta Location *

meta

Enter a valid meta location details for your identity provider.

Cancel

< Back

Save

6. Click Save.
- A pop-up window is displayed with a message that the creation of the new IdP is successful.

Activation of OIDC_TEST

Note: In order to use your newly configured identity provider, it must be activated. If you want to delay activation, click activate later.



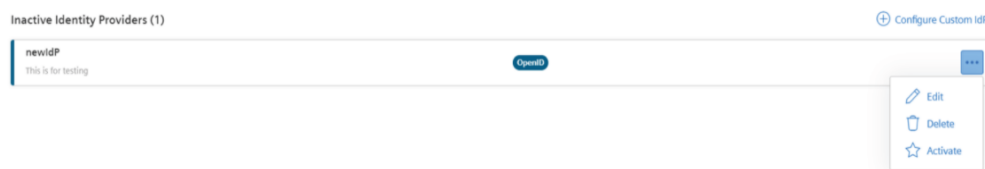
Important: When you hit the activate now button you will automatically be logged out and all other users will be unable to access the platform for a few minutes. If your configuration is unsuccessful and login is not possible the previous identity provider will be restored in a few minutes and you can login with your existing credentials.

☒ I have read and understood these guidelines

Cancel

Activate now

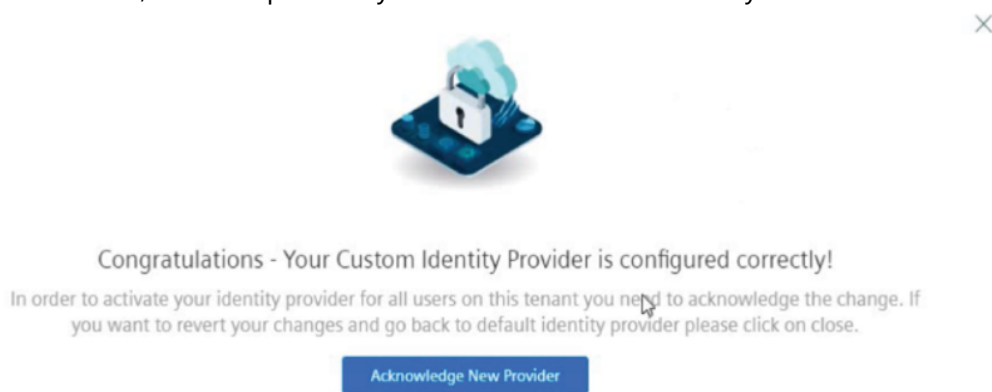
7. To activate the new IdP immediately, click "Activate Now". Otherwise, click "Activate Later". The created IdP is displayed in "Identity Provider Configuration" screen.



8. To activate the created IdP, click "Activate".

After this IdP is activated, the current session will be logged out and the new IdP will be displayed to log in to Insights Hub.

As soon as you log in with the new IdP, a pop-up will be displayed to acknowledge the new provider. Click "Acknowledge New Provider". If this action is not performed during the first login with new IdP, then the previously used IdP will be automatically activated after 5 minutes.



Security capabilities

A secure way is provided to integrate with 3rd party Identity provider (IdP) based on standard protocols and frameworks in case a custom IdP (identity provider) should be used instead of our standard IdP solution. The customer will assume responsibility for the secure operation and management of the chosen IdP including physical security, host operating system and virtualization layer, guest operating system (including updates and security patches) and network configuration according to ISO 27001 (see ISO <https://www.isms.online/iso-27001/annex-a-controls/>).

It is required to change the password regularly. For Tenant administrators, using Multi-Factor Authentication (MFA) is recommended.

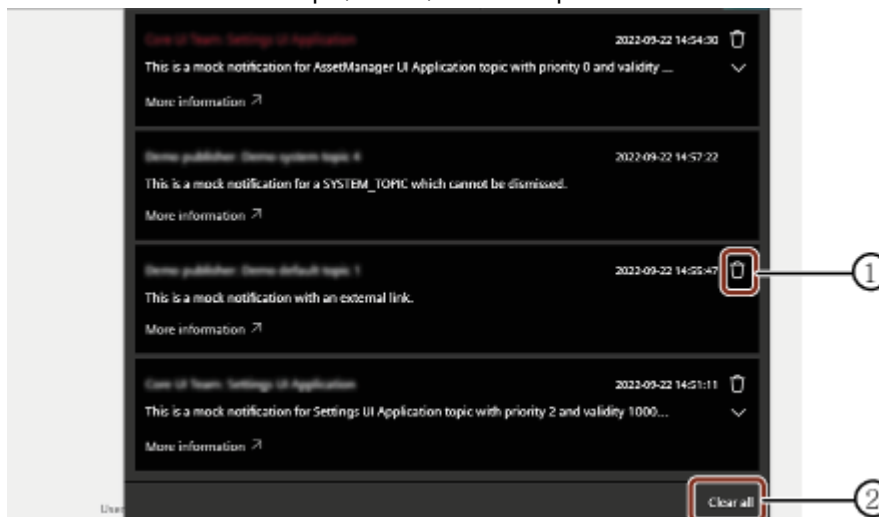
User Preferences

6

6.1 User Preferences

The OS bar of each tenant now shows the push alerts linked to the various event updates for each user. Each user can read, dismiss and redirect to other applications from these push notifications. The user must subscribe to these notifications for the relevant topic in order to receive them.

The "User Preferences" tab in the Settings application allows the users to subscribe and unsubscribe the notifications for the respective topics. These notifications contain the information about the topic, event, timestamp of the event and the link to the application.



- ① Dismisses the specific notification
- ② Dismisses all the notification

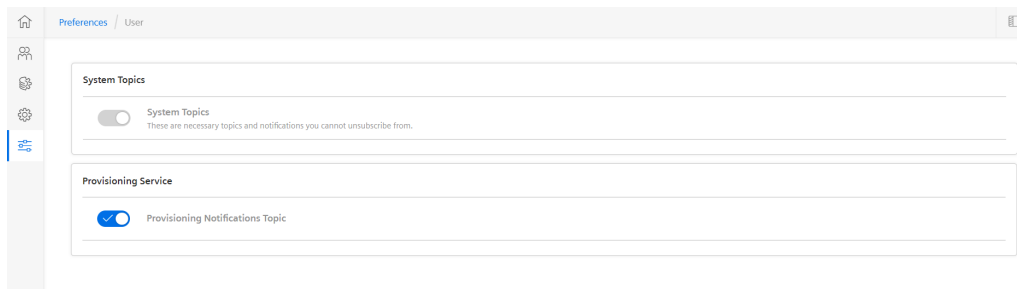


- Notifications related to the "System topic" are subscribed by default and cannot be unsubscribed.
- The notifications are currently supported only in English and German.

Subscribe and Unsubscribe the notifications

To Subscribe for the notifications, in the navigation, click "User Preference". From the list of topics, select the topic of your choice and enable the toggle button.

To Unsubscribe the notifications, in the navigation, click "User Preference". From the list of topics, select the topic of your choice and disable the toggle button.



Appendix

7

7.1 Appendix

Security settings

Change Identity Provider and configure MFA

The Insights Hub Identity Provider WebKey supports Multi-Factor Authentication (MFA). {{ whitelabel.companyName }} Business Units can also use the Corporate Entitlement Service (CES) as an Identity Provider.

Tenant administrators can enable or disable the Multi-Factor Authentication (MFA) for their tenant. You have the option to select the appropriate authentication methods:

1. Default Identity Provider configuration via WebKey with user name and password (without MFA)
2. Identity Provider configuration via WebKey with MFA (via Mail)
3. Identity Provider configuration via Corporate Entitlement Service with MFA (only for {{ whitelabel.companyName }} Business Units)

If you want to change the authentication method, please send an email to provisioning@mindsphere.io with the following content:



We recommend changing your password regularly. In addition, using MFA increases security.

Subject: *Activation of MFA for tenants*

Dear Provisioning Team

Please set the authentication method for the tenant given below to the authentication method given below.

Tenant name: <*your tenant name here*>

Authentication method: <*option: 1, 2, or 3*>

Insights Hub session handling

You can use an application up to a maximum of **12 hours** without logging in again to Insights Hub. This section describes the session handling in detail.

Session types

When a user is logged into Insights Hub, there are two types of sessions:

- The Application Session
- The Insights Hub Session

Application sessions

Each application in Insights Hub is identified by a unique host name. For Insights Hub Monitor for example: -insightshubmonitor.eu1.mindsphere.io. Every application has its own application session. In Insights Hub, the idle timeout for these application sessions is **30 minutes**.

During usage of the application, each user interaction with the application backend resets the application session idle timer. If the user does not interact with the application backend for an extended time period and this time period exceeds the idle timeout, the application session ends. A new application session needs to be established.

If the user still has a valid Insights Hub session (see below), this user will automatically receive a new application session, with no additional effort is needed. Otherwise, the user is redirected to the configured single sign-on system. This typically results in a redirection to the login page of the configured identity provider, for example WebKey.

Insights Hub session

Each authenticated user in Insights Hub has a Insights Hub session. This session is also called "Insights Hub IAM session". As long as a user has a valid Insights Hub session, changing applications is possible without re-authentication.

The Insights Hub session idle timeout is **8 hours**. The idle timeout counter is reset each time when the authenticated user contacts the Insights Hub IAM (Identity and Access Management) service. In particular, when the user switches to a Insights Hub application that has not been used for more than **30 minutes** (application session idle timeout).

The total duration of a Insights Hub session cannot exceed **12 hours**. When the Insights Hub IAM session has expired, the user is redirected to the configured single sign-on system. This typically results in a redirection to the login page of the configured identity provider, for example WebKey.

Session Persistency

The following modes of session persistency are supported:

--	--

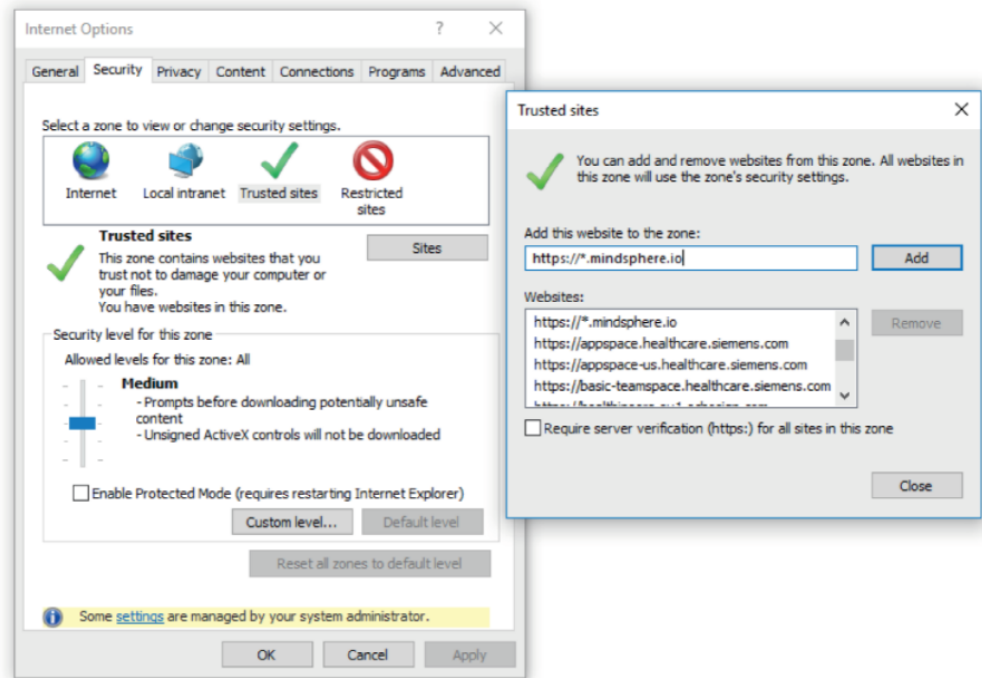
Enabled session persistency	With session persistency enabled the user session is not terminated by closing the browser window. This means there is no need re-authenticate when accessing your tenant for up to 36 hours after closing and reopening your browser. Please note that the session still expires after 12 hours of inactivity. Enabled session persistency is currently not supported for tenants with multi factor authentication enabled. Enabled session persistency is the default behavior in all tenants created as of Aug 23rd 2020 onwards.
Disabled session persistency	With session persistency disabled the user session is terminated by closing the browser window. This means that authentication is necessary each time a tenant is accessed. This can be a demand, for example, in case of increased security requirements where a computer is shared between different users. Disabled session persistency is the default behavior in all tenants created prior to Aug 23rd 2020.

To change the session persistency behavior of your tenant, please reach out to support team with the subject "Session Persistency Configuration Change". We will configure session persistency for your tenant according to your requirements.

Logout problems in IE11

Some users experience logout problems when using Internet Explorer 11. After clicking logout, they get redirected to the Launchpad and can continue working.

1. Add "https://*.mindsphere.io" to the "trusted sites" on the "security" tab and check whether logout works as expected afterwards.



2. If step1 does not work: Overwrite privacy settings as shown below ("privacy tab" → Settings "Advanced" → see screenshot of "Advanced Privacy Settings"); and check whether logout works as

expected afterwards.

