

KNIME Business Hub Admin Guide

KNIME AG, Zurich, Switzerland
Version 1.10 (last updated on 2025-04-02)



Table of Contents

Introduction.....	1
KNIME Business Hub editions.....	1
Users and Consumers.....	2
Create and manage teams.....	3
Create a team.....	3
Allocate resources to a team.....	4
Manage team members.....	6
Delete a team.....	6
Execution resources.....	8
Create a shared execution context.....	9
Manage shared execution contexts.....	10
Advanced configuration of execution contexts.....	11
Users management.....	12
Delete a user.....	12
Make a user Hub admin.....	13
Provisioning users and groups with SCIM (Enterprise edition only).....	17
Create a SCIM application password.....	17
Configure Okta as a SCIM client.....	18
Configure Microsoft Entra ID as a SCIM client.....	19
Assign user to teams based on external groups.....	21
Expose external groups inside KNIME Business Hub (Standard and Enterprise editions only).....	28
External OIDC provider.....	28
LDAP federation.....	33
Enable external groups.....	37
Docker executor images.....	38
Add extensions to an existing Docker image.....	39
Python and Conda in Docker images.....	53
Delete a custom Docker image.....	55
Customization profiles.....	60
Structure of a customization profile.....	60
Variable replacement.....	61
Create a customization profile.....	62
Customization options.....	62

Upload a customization profile	69
Apply a customization profile	74
Update a customization profile	80
Detach a customization profile	84
Delete a customization profile	90
Advanced configuration	94
Configure networking	94
Configure Browser Security	98
Activate and configure Job Instrumentation Data	99
Installation of AI services (Enterprise edition only)	100
Node affinity	103
Create a collection (Enterprise edition only)	105
Administrator workflows	108
Workflows overview	108
Requirements and prerequisites	108
Discard Failed Jobs	109
Manage All Existing Jobs	112
Delete Old Versions	117
Scheduled Workflows Kick-Off Times	120
Count Workflows Running Per Day	123
Workflows' Run Time	125
Monitor Users' Usage	127
Monitoring K-AI in KNIME Business Hub	133
Data access	133
Data structure	133
Deploying the data application	134
Data application overview	135
Workflows Jobs Monitoring data application	139
Introduction	139
Data application usage	139
KNIME Business Hub API documentation	147
Support Bundles and Troubleshooting	148
Generating a support bundle (GUI)	148
Generating a support bundle (CLI)	149
Configuring redaction in support bundles	149
Inspecting support bundles	149

Maintenance operations	153
Restart a node	153
Backup and restore with Velero Snapshots and Kotsadm	154
Creating snapshot backups	154
Backup Troubleshooting	156
Restoring a snapshot	157
Changelog (KNIME Business Hub 1.10)	159
KNIME Business Hub 1.10.4	159
KNIME Business Hub 1.10.3	159
KNIME Business Hub 1.10.2	159
Important Bugfixes	160
KNIME Business Hub 1.10.1	160
KNIME Business Hub 1.10.0	161
Changelog (KNIME Business Hub 1.9)	164
KNIME Business Hub 1.9.0	164
Changelog (KNIME Business Hub 1.8)	165
KNIME Business Hub 1.8.3	165
KNIME Business Hub 1.8.2	165
KNIME Business Hub 1.8.1	166
KNIME Business Hub 1.8.0	167
Changelog (KNIME Business Hub 1.7)	169
KNIME Business Hub 1.7.0	169
Changelog (KNIME Business Hub 1.6)	170
KNIME Business Hub 1.6.0	170
Changelog (KNIME Business Hub 1.5)	173
KNIME Business Hub 1.5.2	173
KNIME Business Hub 1.5.1	173
KNIME Business Hub 1.5.0	173
Changelog (KNIME Business Hub 1.4)	175
KNIME Business Hub 1.4.2	176
KNIME Business Hub 1.4.1	176
KNIME Business Hub 1.4.0	176
Changelog (KNIME Business Hub 1.3.0)	178
KNIME Business Hub 1.3.0	178
Changelog (KNIME Business Hub 1.2.0)	179
KNIME Business Hub 1.2.0	179

Introduction

KNIME Business Hub is a customer-managed Hub instance. Once you have a license for it and proceed with installation you will have access to Hub resources and will be able to customize specific features, as well as give access to these resources to your employees, organize them into Teams and give them the ability to manage specific resources.

This guide provides information on how to administrate a KNIME Business Hub instance.

To install a KNIME Business Hub please refer to the [KNIME Business Hub Installation Guide - Embedded Cluster](#) or the [KNIME Business Hub Installation Guide - Existing Cluster](#).

A user guide is also available [here](#), which contains instructions on how to perform team administration tasks. Team admins are designated by the global Hub admin, and have control over their team's allocated resources, can add users to their team, create execution contexts and have an overview of the team's deployments. In this way the Hub administration tasks are distributed and reallocated to those users that have a better overview of their own team necessities.

KNIME Business Hub editions

KNIME Business Hub is available in three different editions:

- Basic
- Standard
- Enterprise

All the features described in this guide are available for all the editions, unless explicitly pointed out.

However, please consider that some of the features might be limited by the resources available for the different editions.

In particular the Basic edition:

- Does not allow **consumers**
- It only allows 1 execution context, which is created during the installation. It is therefore not possible to create a new one unless the other one is deleted.
- It only allows 1 team. Therefore the creation of a new team is not possible.



For an overview of the available features and resources for different KNIME Hub offerings please refer to the [pricing page](#) on the KNIME website.

Users and Consumers

- **Consumers** on KNIME Business Hub have access to specific data apps and services available on KNIME Hub. In KNIME Business Hub Basic edition there are no consumers available. Only logged-in users that are members of the team have access to the workflows, spaces and deployments of the team. Standard and Enterprise edition instead allows consumers. They will have unlimited access to the data apps and services that are shared with them.
- **Users** on KNIME Business Hub are members of a team and have access to all the workflows, spaces and deployments of their team, and to the public spaces of the other teams. In KNIME Business Hub Basic and Standard edition licenses 5 users are included, while 20 are included for Enterprise edition licenses.
- Unlicensed users, instead, do not have read access to any of the resources of the KNIME Business Hub for Basic and Standard edition licenses, while they have read access in the Enterprise edition licenses.

Create and manage teams

A team is a group of users on KNIME Hub that work together on shared projects. Specific Hub resources can be owned by a team (e.g. spaces and the contained workflows, files, or components) so that the team members will have access to these resources.

Sign in to the KNIME Business Hub instance with the admin user name by visiting the KNIME Business Hub URL.

Then click your profile picture on the right upper corner of the page and select *Administration* to go to the KNIME Business Hub Administration page. Click *Teams* in the menu on the left. Here you will be able to see an overview of the existing teams and you will be able to manage them.

Create a team

To create a new team click the yellow plus button on the right.

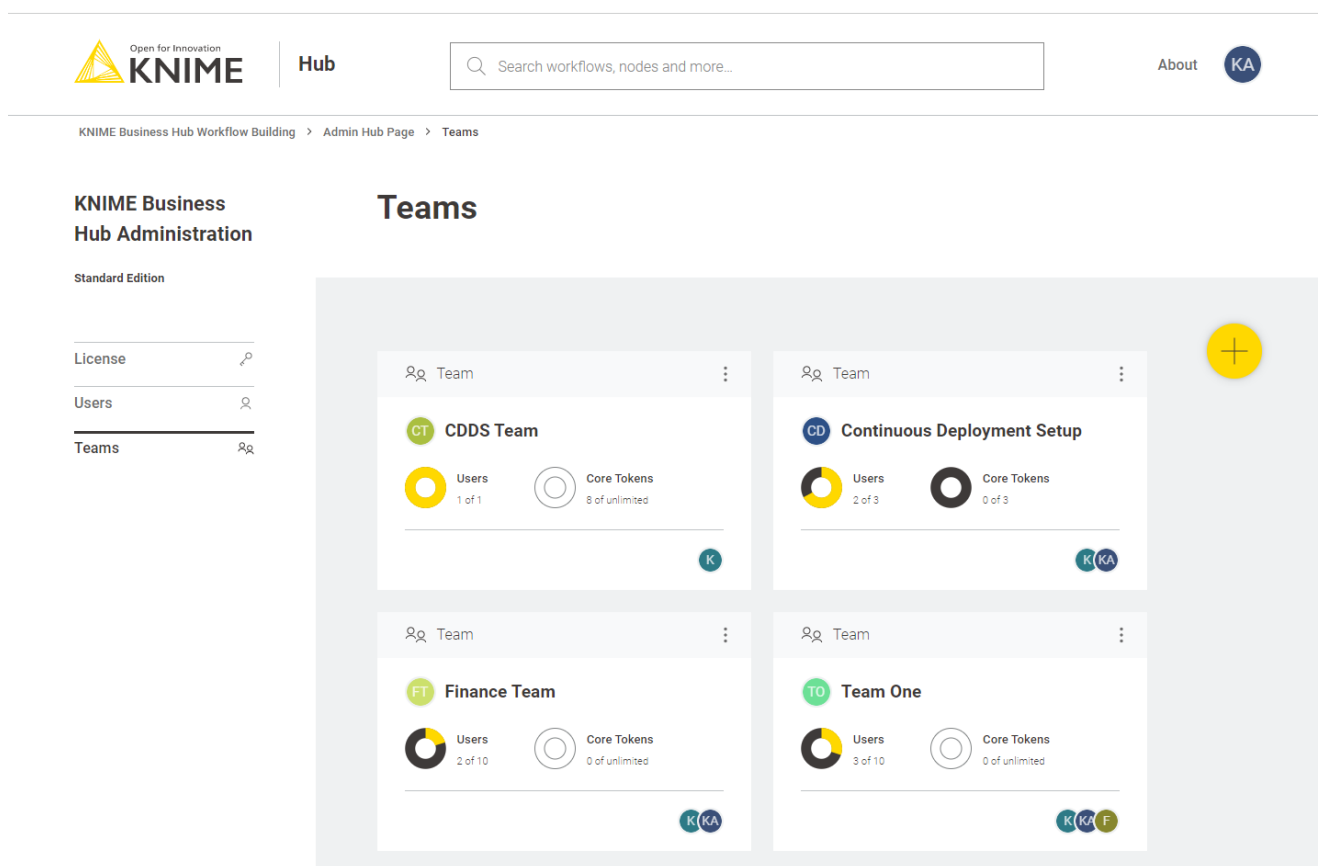


Figure 1. Create a new team in the KNIME Business Hub Administration page

After you create a new team you will be redirected to the new team's page. Here you can change the name of the team. To do so click the name of the team under the team logo on the left side of the page. The name of the team can also be changed at any point in time by

the team administrator.

From the team's page you can:

- Add members to the team
- Change their role to, for example, promote a user to team administrator role

Here you might for example want to assign the team to a team administrator. To do so click *Manage team* and enter the user name of the user you want to assign as a team administrator for the current team. Then click on the role and select *Member* and *Admin*. At the same time you might want to delete the global admin user name from the team members list. To do so click the bin icon corresponding to that user. Click *Save changes* to finalize the setting.

Allocate resources to a team

To allocate resources to a team navigate to the KNIME Business Hub Administrator page and select *Teams* from the menu on the left.

Here you can see an overview of the teams available, their allocated resourced, and of their current usage. Click the three dots on the right upper corner of the card corresponding to the team you want to allocate resources to.

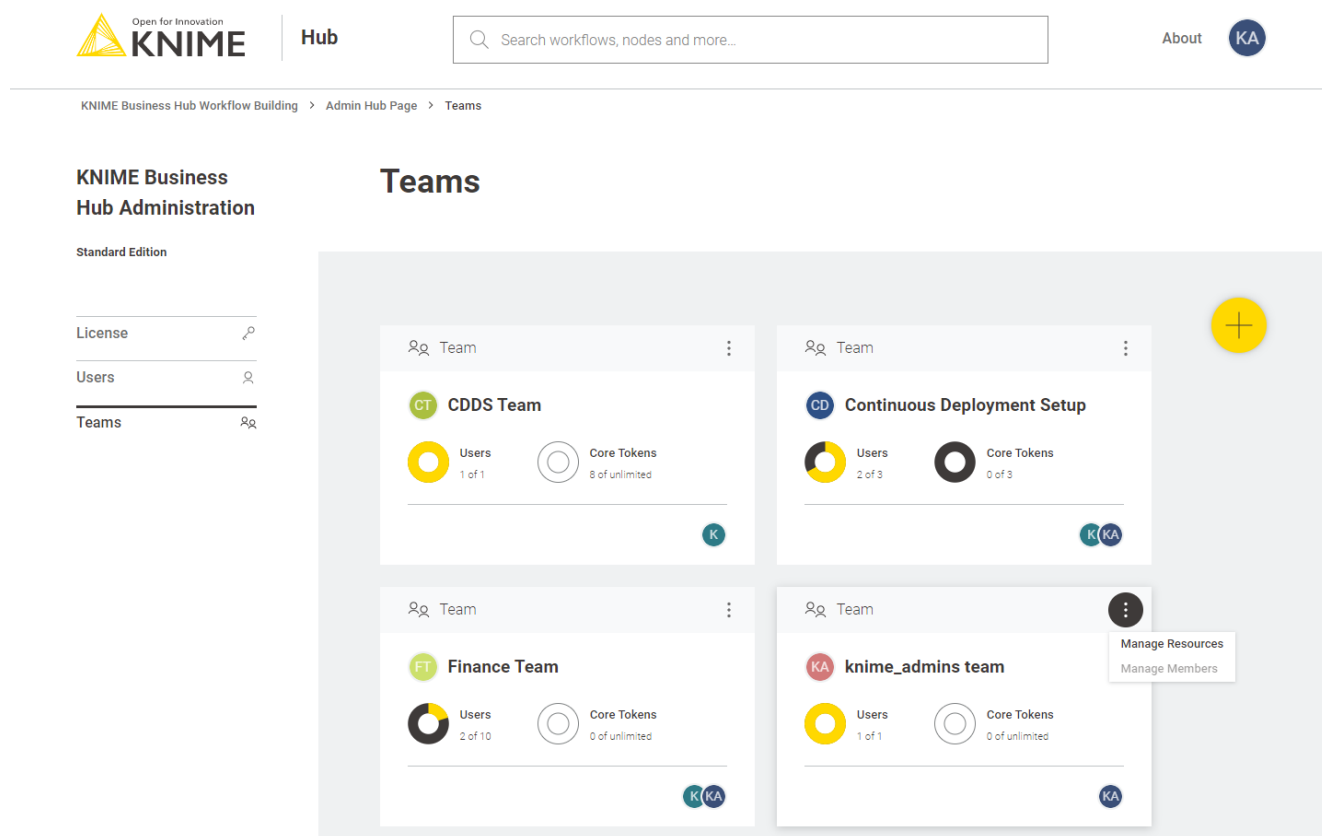


Figure 2. Manage resources of a team

Select *Manage resources* from the menu. A panel on the right will open where you can select the resources you want to allocate.

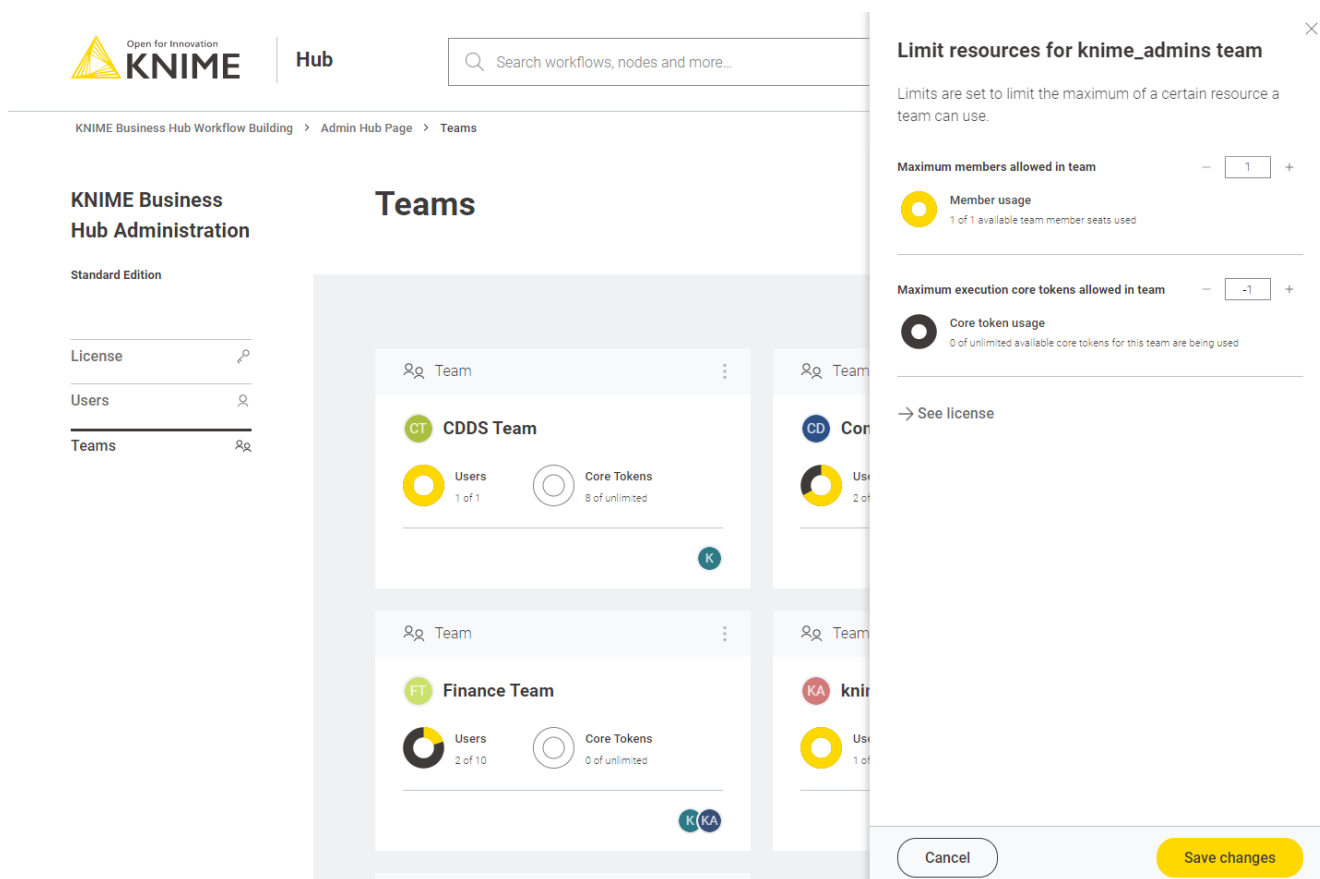


Figure 3. Allocate resources to a team

Here you can change:

- The maximum number of members allowed in that team
- The maximum number of execution vCore tokens allowed for that team

Click *Save changes* when you have set up the resources for the current team.

Manage team members

From the KNIME Business Hub Administration page you can also manage the team members.

Click the three dots on the right upper corner of the card corresponding to the team. From the menu that opens select *Manage members*. In the side panel that opens you can add members to a team, or change the team members role.

Delete a team

From the KNIME Business Hub Administration page you can also delete a team.

Click the three dots on the right upper corner of the card corresponding to the team. From the menu that opens select *Delete*. Be aware that this operation will delete also all the team resources, data and deployments.

Execution resources

As mentioned in the previous section you as an Hub admin can assign execution resources to each team.

Team admins will then be able to build execution contexts according to the execution resources that you assigned to their team. These execution contexts will then be dedicated specifically to that team.

As an Hub admin you can also create a shared execution context. Once you create one you can share it with multiple teams.

For an overview of all the available execution contexts click your profile icon on the top right corner of the KNIME Hub and select *Administration* from the drop-down.

You will be then redirected to the KNIME Business Hub administration page.

Here, select *Execution resources* from the menu on the left.

In this page you can see an overview of *All* the execution contexts available on the Hub.

From the toggle at the top you can filter to see only a specific type of execution contexts available in the Hub instance.

Select:

- *Shared*: Shared execution contexts are created by the Hub admin. They can be made available to multiple teams.
- *Dedicated*: Dedicated execution contexts are created by the team admins for their team. Dedicated execution contexts are exclusively used by a single team.




Each team can by default have a maximum of 10 execution contexts and 10000 jobs. As a KNIME Hub admin you can change these limits via a REST API call like the following:

```
``PUT https://api.<base-url>/execution/limits/{scopeId}/{limitKey}``
```

where `{scopeId}` is the team account ID and the `{limitKey}` is account-execution-contexts or account-jobs respectively.

Create a shared execution context

As an Hub admin you can create a shared execution context and make it available to multiple teams. To do so click the  button. A side panel opens where you can set up the new shared execution context.

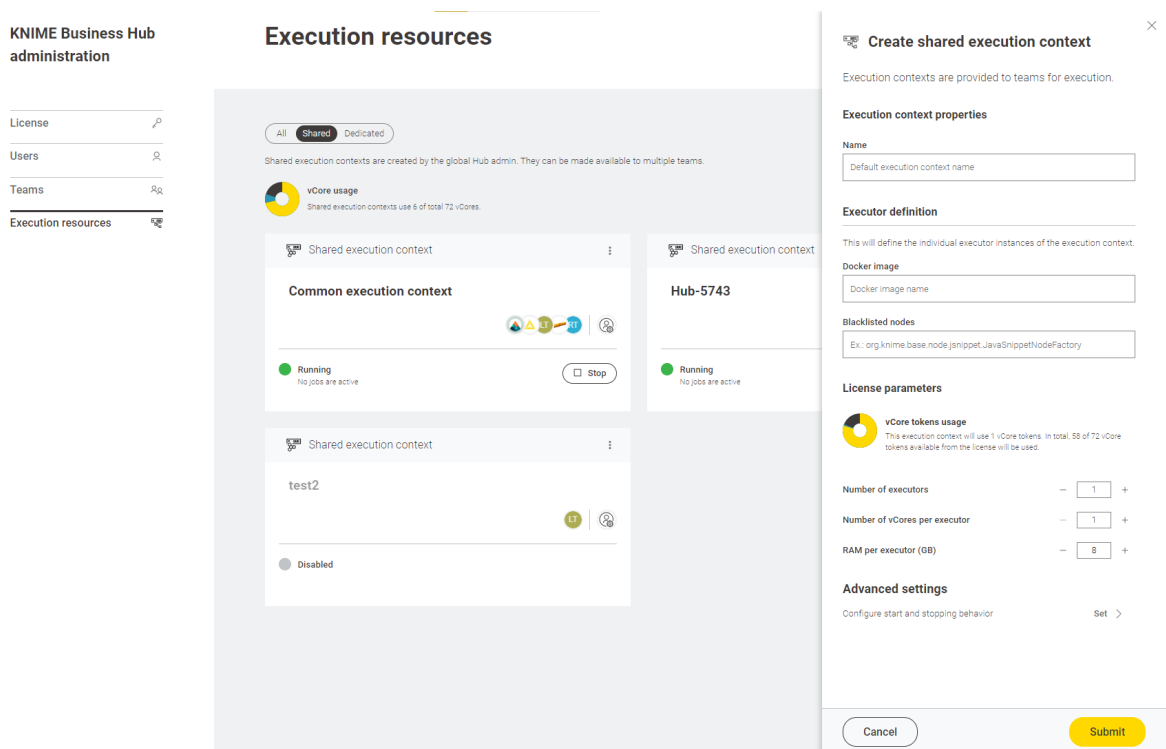


Figure 4. Create a shared execution context

Here you can give the execution context a name, set up which **Docker image** to use as the executor, give a list of blacklisted nodes, and assign the resources that the execution context will be able to use.




Find more information about how to set up the execution context in the **KNIME Business Hub User Guide**.

Finally, you can configure whether you want the execution context to automatically start and stop. To do so click *Set* under *Configure start and stop behavior* and select *On* (the setting is *Off* by default) from the toggle on top. Then you can indicate the desired inactivity time (in minutes) for the execution context to stop.

The execution context will start automatically when a queued workflow needs to run and stop automatically when there are no more active or queued workflows.

Click *Submit* to create the execution context. A notification will appear where you can click *Manage access* to share the execution context with the teams.

At any time you can also manage the access to a shared execution context by clicking the  icon in the corresponding tile and selecting *Manage access* from the menu.

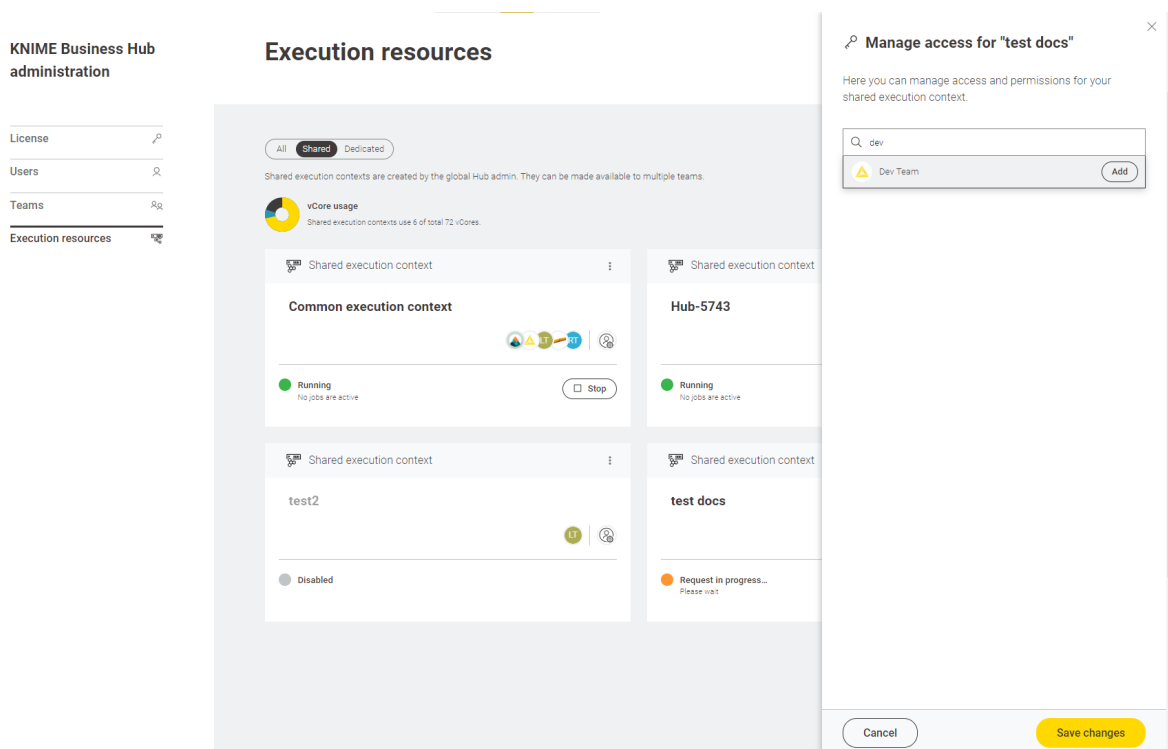



Figure 5. Manage access for a shared execution context

Manage shared execution contexts

Also from the *Execution resources* page you can have an overview about the current status of an execution context, which teams have access to it, how many jobs are running and also manage the execution context performing the following operations:

- *Start* and *Stop* an execution context by clicking the Start/Stop button in the tiles
- Click the  icon in the tile and from the menu that opens you can:
 - *Edit*: You can change the parameters and configurations in the right side panel that opens.
 - *Manage access*: Manage the access of teams to a shared execution context.
 - *Enable/Disable*: You will need first to delete the jobs associated to the execution context then proceed with disabling it.
 - *Delete*: As a Hub administrator you can delete a shared execution context. You will need to first, delete the jobs associated to the execution context then proceed with disabling it. Finally, you can delete the shared execution context.
 - *Show details*: Selecting this option will open a new page with a list of all the jobs that are running on that execution context, the usage of the execution context

(e.g. how many vCores are in use) and other information. You can also switch to the specific *Executor* tab to see more details about the executor.

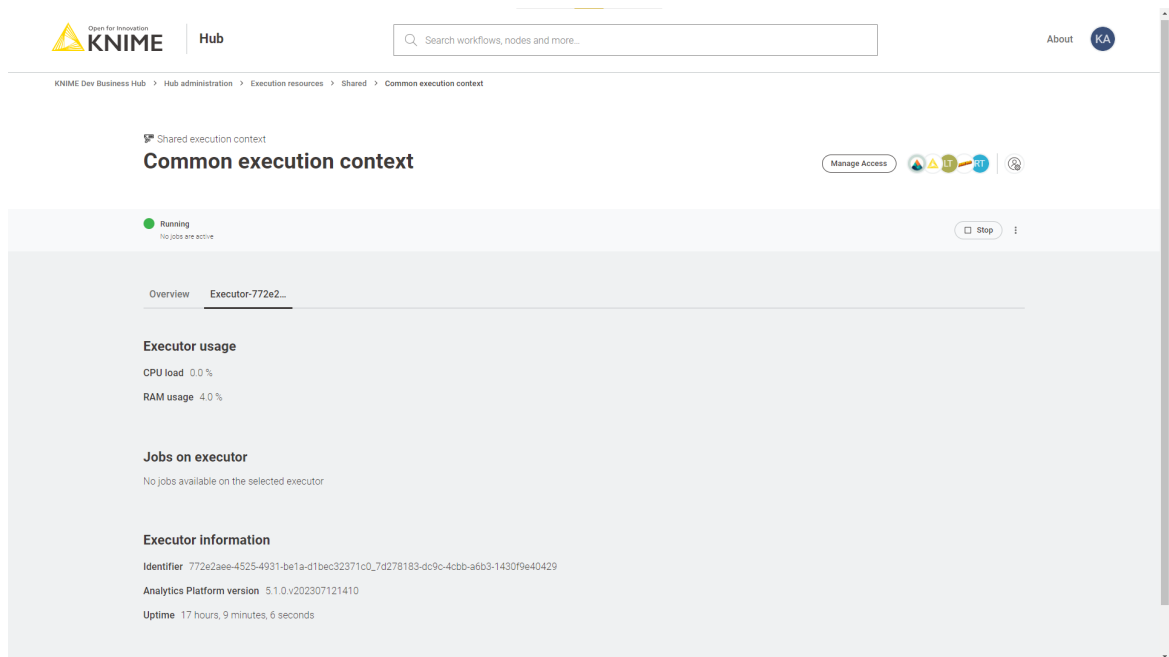


Figure 6. Additional executor information page

Advanced configuration of execution contexts

Execution contexts can be created and edited also via the Business Hub API.

Find more information on the available configurations in the [Advanced configuration of execution contexts](#) section in KNIME Business Hub User Guide.

Users management

To see a list of all the users that have access to your KNIME Business Hub instance you can go to the KNIME Business Hub Administration page and select *Users* from the menu on the left. The list shows all users that have already logged into KNIME Business Hub. Users that only exist in your identity provider are not known to KNIME Business Hub. If you want to create users before they log in, e.g. in order to assign them to groups or share deployments with them, you can provision users with SCIM. See [Provisioning users and groups with SCIM \(Enterprise edition only\)](#) below for details.

KNIME Business Hub Administration

Standard Edition

License

Users

Teams

Users

Rows: 1-4 of 4

Username ↑	Name	Type	Teams
bernd.wiswedel	-	Consumer	-
francesco	-	User	Team One
knime	-	User	Team One, Continuous Deployment S...
knime_admin	-	User	Team One, Continuous Deployment S...

Rows: 1-4 of 4

25 per page

Figure 7. Manage users on KNIME Business Hub Administration page

Here you can filter the users based on their team, the type of users and their username and name. To do so click the funnel icon in the users list. You can also search the users by using the magnifier icon and typing the keyword in the field that appears.

Delete a user

To delete a user follow these steps in this order:

1. Delete the user from the KNIME Business Hub Administration page. Click the three dots and select *Delete*. You will need to confirm the user deletion in the window that opens

by clicking *Delete user*. Be aware that this action will also delete all data from the deleted user and it will not be possible to restore the user.

2. Delete the user from Keycloak. Follow the steps in the [next section](#) to access Keycloak and manage users.

Make a user Hub admin

Users are managed in the backend via the Keycloak instance embedded in KNIME Business Hub. Therefore, the operation of promoting a registered user to the role of Hub admin is done in Keycloak.

To do so follow these steps:

1. First you will need to access the keycloak admin console. To do so you will need the credentials that are stored in a kubernetes secret called `credential-knime-keycloak` in the `knime` namespace. To get the required credentials, you need to access the instance the Business Hub is running on and run the following command:

```
kubectl -n knime get secret credential-knime-keycloak -o yaml
```

This will return a file that contains the `ADMIN_PASSWORD` and the `ADMIN_USERNAME`. Please notice that they are both base64 encrypted. In order to get the decrypted username and password, you can run the following commands:

```
echo <ADMIN_PASSWORD> | base64 -d  
echo <ADMIN_USERNAME> | base64 -d
```

2. Then go to <http://auth.<base-url>/auth/> and login.
3. In the top left corner click the dropdown and select the "Knime" realm, if you are not there already.

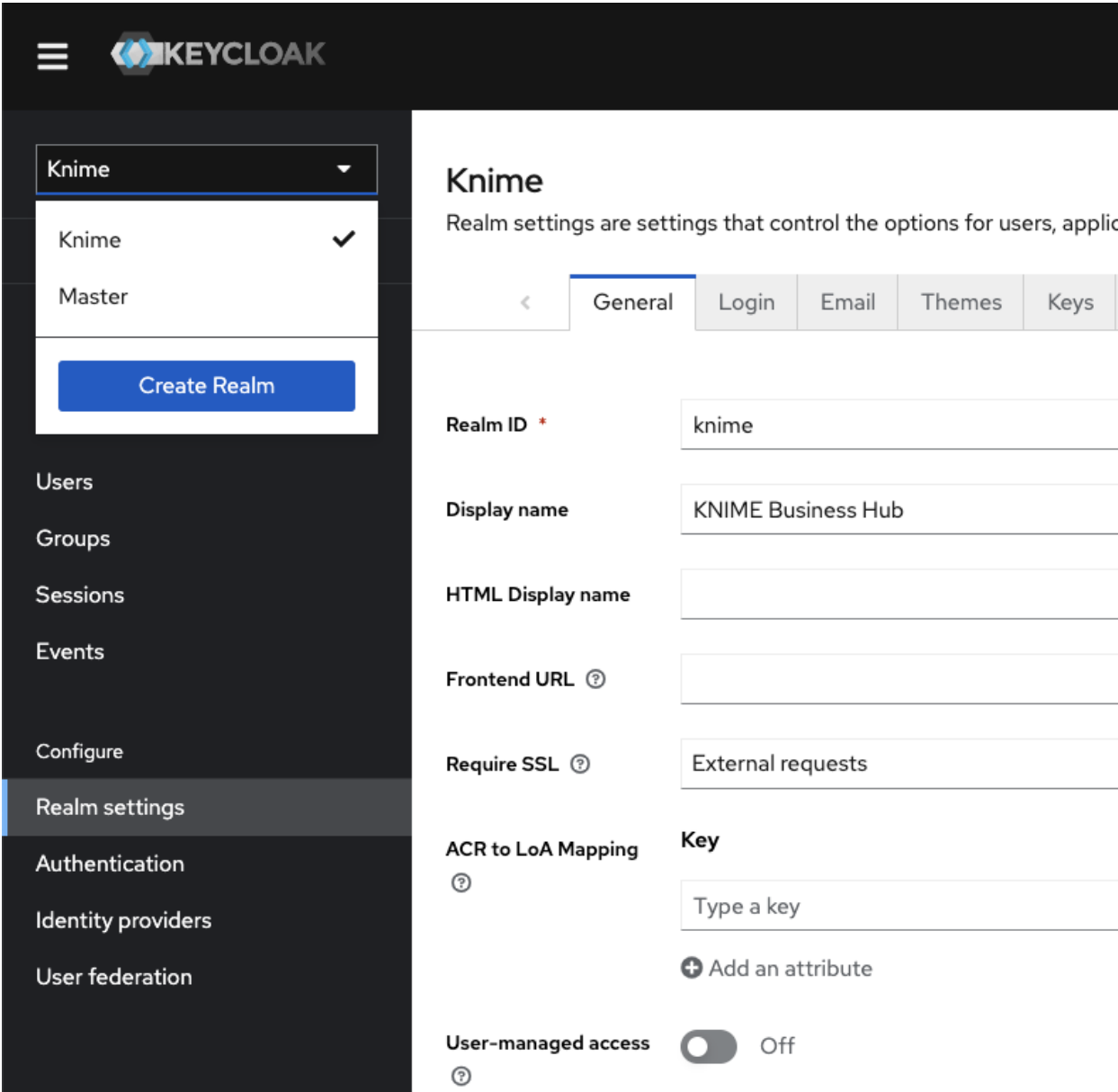


Figure 8. Select the "Knime" realm

- 4. Navigate to the *Users* menu and search for the user by name or email:

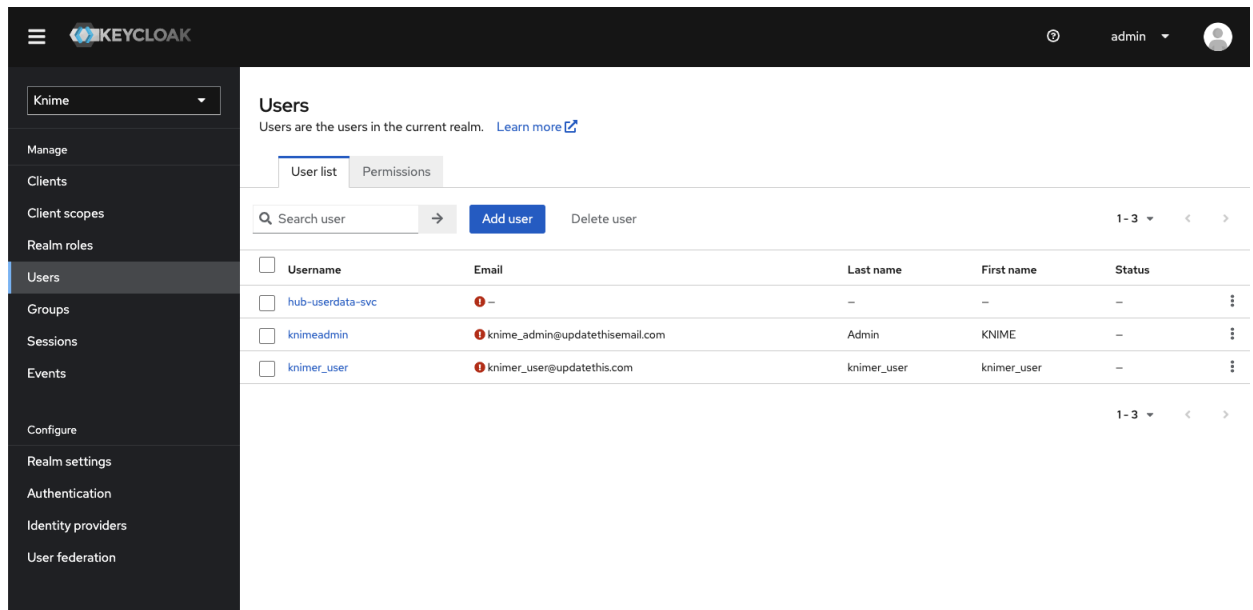


Figure 9. The Keycloak users menu



In order for a user to appear in this list, it is necessary that they have logged into your KNIME Business Hub installation at least once.

- Click the user and go to the *Groups* tab. Click *Join Group* and either expand the *hub* group by clicking it, or search for "admin". Select the admin group and click *Join*:

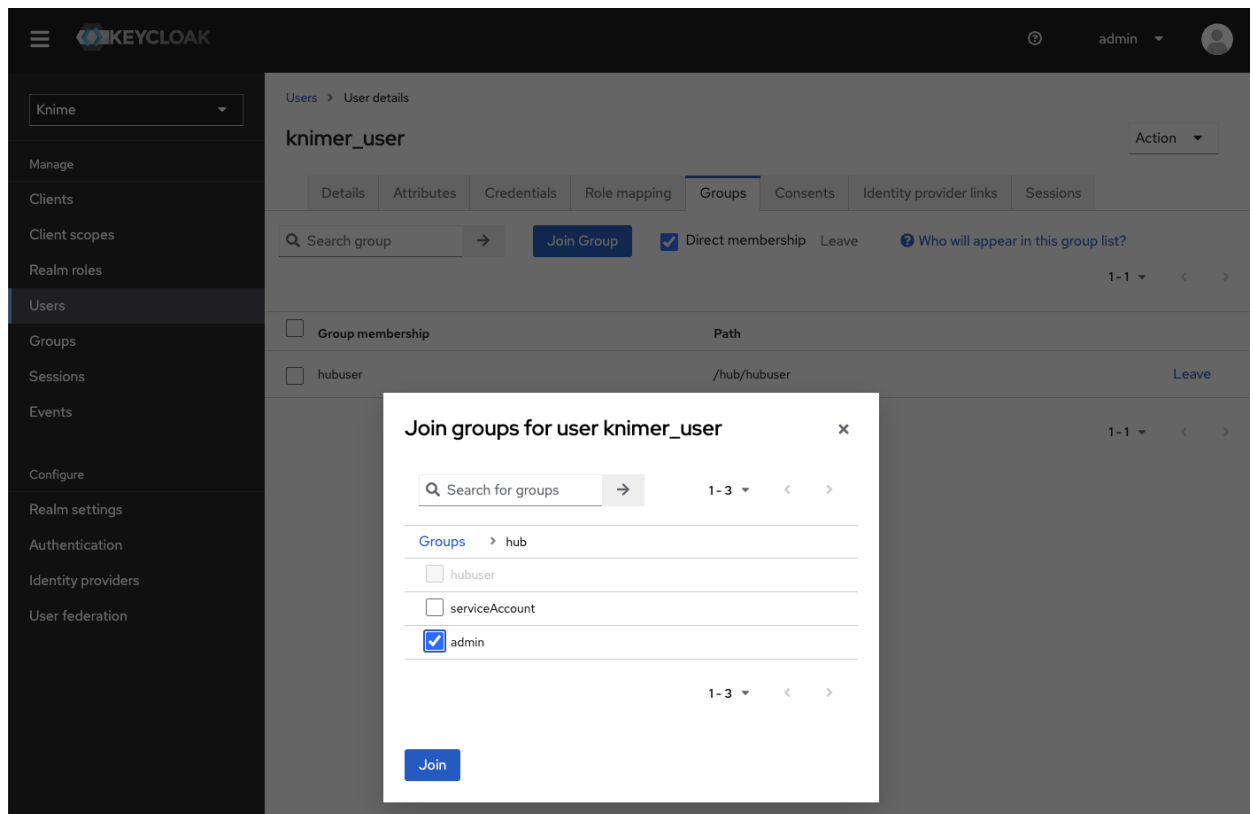


Figure 10. Making a user a Hub admin in Keycloak. If you are searching for the group then the group might show up under its full path "/hub/admin"

6. Done. The user now has the role of Hub admin, and can access the admin pages from within the Hub application to e.g., create teams or delete users.

Provisioning users and groups with SCIM (Enterprise edition only)

The **System for Cross-domain Identity Management** (SCIM) is an open industry standard for provisioning users and groups from an identity provider to an application. In contrast to authentication protocols such as OpenID/OIDC, a SCIM client in the identity provider actively pushes information about user and groups to the application.

KNIME Business Hub supports SCIM since version 1.10. This allows you to create users in KNIME Business Hub without them having to log in first. You can then assign them to teams or share deployments with them. In addition, groups can be provisioned with SCIM as well. They become *external* groups in KNIME Business Hub. In combination with the new nested groups feature they allow you to automatically assign users to teams based on group memberships in the identity provider.

You can enable SCIM on a KNIME Business Hub installation that already contains users. Existing KNIME Business Hub user accounts will be matched with accounts provisioned by SCIM based on the username and e-mail address.

If your usernames in the identity provider are e-mail addresses you likely have created a mapper in Keycloak that removes the domain part because previous KNIME Business Hub releases did not allow usernames to contain the @ character. This has changed for version 1.10 so that SCIM clients can provision users with e-mail addresses as usernames without issues. However, this also means you have to disable/remove the corresponding mapper in Keycloak, otherwise the username created by SCIM does not match the username in the authentication token provided by Keycloak. After you have removed the mapper, existing accounts in KNIME Business Hub will automatically be updated when the user logs in the next time.



We have tested and hence support SCIM with Okta and Microsoft Entra ID as SCIM clients. Other SCIM clients may work as well but as the SCIM protocol is pretty extensive therefore there may be edge-cases which we haven't covered.

Create a SCIM application password

The first step for any kind of SCIM client is to create a dedicated application password with which the SCIM client authenticates against your KNIME Business Hub installation. This must be done by an administrator and can best be performed using the Swagger UI.

1. Log into your KNIME Business Hub installation as an administrator user.

2. Open the OpenAPI documentation of the account service functionality, which is available at <https://api.<base-url>/api-doc/?service=accounts-service>
3. Go to the SCIM section, expand the POST request box, click *Try it out*, and then click *Execute*.

SCIM Requests relating to the System for Cross-domain Identity Management (SCIM). ^

GET `/scim/client-auth` Retrieves existing SCIM client authentication credentials. v

POST `/scim/client-auth` Creates new SCIM client authentication credentials. ^

Creates and returns new SCIM client authentication credentials.

Parameters Cancel

No parameters

Execute

4. The result will be displayed below the button. It contains a `pwId`, a `password`, and an `authToken`. For Okta as a SCIM client you will need the `pwId` and the `password`. For Microsoft Entra ID you will need the `authToken`. Please note down these values in a safe place because you will not be able to retrieve them again without deleting and re-creating the SCIM application password.

```
{
  "password": "8ec6NIWBX60Gj8YF9r8nAG7QBiuD74LI-DQ7YovERfwoFbFBw_5LMKfSNSB-o08Fm70hb7KsOWDg6J1jZN1mAA",
  "authToken": "UzF5QWtaZDBYRHVpOHlRUEVmSFZvRUxKSWdKRFJtZUJNRzZKV2d1bDZQdzo4ZNM2Tk1XQlg2MedqOF1G0XI4bkFHN1FCsXVENzRMSS1EUTdzb3FUmZ3b0ZiRkJ3XzVMTUtmU05TQi1vTzhGbTcwaGI3S3NPV0RnNkoxalpOMw1BQQ==",
  "id": "account:app-pw:c15f2b86-a944-494f-bac9-63b2901d6939",
  "pwId": "S1yAkZd0XDui8yQPEfHVoELJigJDRmeBMG6JWge16Pw",
  "name": "My application password name",
  "creator": "account:user:11111111-1111-1111-1111-111111111111",
}
```

Configure Okta as a SCIM client

In order to set up Okta as a SCIM client for KNIME Business Hub, follow Okta's documentation about [Adding SCIM provisioning to app integrations](#).

It is currently not possible to add SCIM to an OIDC app integration in Okta. But you can simply create a second integration for your KNIME Business Hub installation that is only responsible for provisioning via SCIM. For this create a *SWA app integration* as part of *Task 1* of the documentation.

When you configure the *SCIM Connection* of the app integration, provide the following values:

- Use `https://api.<your hub domain>/accounts/scim/v2` as the *SCIM connector base URL*.
- Use `userName` as *Unique identifier field for users*.
- Select all options for *Supported provisioning actions*.
- Select *Basic Auth* as *Authentication Mode*.
- From the application password created earlier use the `pwId` value as *Username* and the `password` value as *Password*.

The screenshot displays the 'SCIM Connection' configuration page. The left sidebar shows the navigation menu with 'Integration' selected. The main content area is titled 'SCIM Connection' and includes a 'Cancel' button in the top right. The configuration fields are as follows:

- SCIM version:** 2.0
- SCIM connector base URL:** `https://api.hub.knime.local/accounts/scim/v2`
- Unique identifier field for users:** `userName`
- Supported provisioning actions:** All five options are checked: 'Import New Users and Profile Updates', 'Push New Users', 'Push Profile Updates', 'Push Groups', and 'Import Groups'.
- Authentication Mode:** Basic Auth
- Basic Auth section:**
 - Username:** `z5kiNYTDOaDNqgv2vTZPn6pcO2q2dQAQSAbw2FruAQE`
 - Password:** Masked with dots

A 'Test Connector Configuration' button is located at the bottom right of the form.

After that you can assign users and/or groups to the application in the *Assignments* tab. Provisioning of the respective users will start automatically shortly afterwards. Likewise, group provisioning can be configured in the *Push Groups* tab.

Configure Microsoft Entra ID as a SCIM client

In order to set up Microsoft Entra ID as a SCIM client for KNIME Business Hub, follow

Microsoft's documentation about [Integrating your SCIM endpoint with the Microsoft Entra provisioning service](#).

When you configure the *Provisioning* details of the Enterprise application, provide the following values:

- Use `https://api.<your hub domain>/accounts/scim/v2` as the *Tenant URL*
- Use the `authToken` value from the application password created earlier as the *Secret Token*

No changes are required in the *Mappings* section.

The screenshot displays the 'Provisioning' configuration page in the KNIME Business Hub Admin interface. The left sidebar shows a navigation menu with 'Overview', 'Provision on demand', 'Manage', 'Provisioning' (selected), 'Users and groups', 'Expression builder', 'Monitor', and 'Troubleshoot'. The main content area has a top bar with 'Save' and 'Discard' buttons. Below this, the 'Provisioning Mode' is set to 'Automatic'. A descriptive text states: 'Use Microsoft Entra to manage the creation and synchronization of user accounts in 3rd SCIM Test by Thorsten based on user and group assignment.' The 'Admin Credentials' section is expanded, showing 'Admin Credentials' and a note: 'Microsoft Entra needs the following information to connect to 3rd SCIM Test by Thorsten's API and synchronize user data.' The 'Tenant URL' field is populated with 'https://api.hub.knime.local/accounts/scim/v2' and has a green checkmark. The 'Secret Token' field is masked with dots. A 'Test Connection' button is present. Below this, the 'Mappings' and 'Settings' sections are collapsed. At the bottom, the 'Provisioning Status' is shown as 'On' with a toggle switch.

With Entra ID provisioning can take a long time, depending on the number of users and groups. For example, 250 users and 30 groups take about 40 minutes.

If your KNIME Business Hub installation is not reachable by Entra ID due to network restrictions, you can follow Microsoft's instructions about [Configuring the connection via the provisioning agent](#)

Assign user to teams based on external groups

If you have provisioned groups from your identity provider to KNIME Business Hub you can use these external groups to manage team memberships. Once changes to group memberships in the identity provider have been provisioned to KNIME Business Hub they will immediately be reflected in team memberships. This also allows you to assign users to teams before they have logged in.

In order to assign team membership based on an external group, you have to add the external group as a *nested group* to the team's *accountMember* group.

Currently, you can accomplish this by:

1. Using **API calls**, such as through the Swagger UI that you used to create the SCIM application password.
2. By using a dedicated **data application** deployed in your KNIME Business Hub instance.

Assign users based on external groups via API calls

Follow these steps in order to add an external group as a nested group to a team group:

1. Find the team's ID. You can search teams by their name and then get the ID from the `id` field in the response.

Accounts Requests relating to accounts.

GET /accounts List all existing user or team accounts.

GET /accounts/name/{name} Returns the information of the account.

Returns the information of the account, such as name, avatar URL etc.

Parameters Cancel

Name	Description
name required	The account's name.
string (path)	
<input type="text" value="Dev Team"/>	

Execute Clear

Responses

Server response

Code	Details
200	<p>Response body</p> <pre>{ "type": "TEAM", "id": "account:team:41d128c5-8331-491f-8a1b-d8f5c843e211", "name": "Dev Team", }</pre>

2. Find the external group's ID. Since the external group's name in KNIME Business Hub may not be exactly the same as in the identity provider, the easiest way is to list all external groups, select the right one based on its `displayName`, and note down its `id`.

Accounts Requests relating to accounts.

GET /accounts List all existing user or team accounts.

GET /accounts/hub:global Returns information about this KNIME Hub installation, including external groups.

Returns information about this KNIME Hub installation such as the enabled features or groups that are associated with an external identity provider.

Parameters Cancel

No parameters

Execute **Clear**

Responses

Curl

```
curl -X 'GET' \
  'https://api.business-hubdev.cloudops.knime.com/accounts/accounts/hub:global' \
  -H 'accept: application/json'
```

Request URL

```
https://api.business-hubdev.cloudops.knime.com/accounts/accounts/hub:global
```

Server response

Code **Details**

200

Response body

```
{
  "secretStore": {
    "secretStore": {
      "groups": [
        {
          "self": {
            "href": "https://api.business-hubdev.cloudops.knime.com/accounts/accounts/hub:global/groups/cloudops",
            "isHrefTemplate": true,
            "method": "GET"
          },
          "name": "cloudops",
          "displayName": "The Cloudops",
          "id": "hub:global:group:cloudops",
          "type": "external",
          "external": true
        }
      ]
    }
  }
}
```

3. Add the external group as a member to the *accountMember* group of the desired team.

Groups

POST /accounts/{id}/groups/{name}/members Adds members to an existing group of an account

Sending this requests with a list of user account IDs and/or a list of group IDs in the request body lets you add members to a group of a team. If a user account or group in the list does not exist, or a user is not a member of the team, the whole request will fail. I.e. either all members/groups are added or none. User accounts or groups that are already group members will be silently ignored. In order to add group members the caller must have appropriate permissions for the team account.

Parameters Cancel Reset

Name	Description
id ★ required string (path)	The account's ID. Must be a team account. <code>eam:41d128c5-8331-491f-8a1b-d8f5c843e211</code>
name ★ required string (path)	The name of the group. <code>accountMember</code>

Request body application/json

The users and/or groups that should be added to this group.

```
{
  "groupIDs": [
    "hub:global:group:cloudops"
  ]
}
```

Execute

After that, the users in the external group will immediately show up as members of the respective team.

Please note that you must have enough users in your KNIME Business Hub license, otherwise this operation might fail due to insufficient users. The team size limit will be updated automatically if the external group was provisioned by SCIM.

Assign users based on external groups via Data Application



Before running this application, ensure you have provisioned groups from your identity provider to KNIME Business Hub. Once you have done this, you can use these external groups to manage team memberships.

Data Application specifications

1. The aim of this application is to allow Global Admins to manage the assignment and deletion of users to teams based on external groups without having to do it manually.
2. Hence, only KNIME Business Hub Global Admins have permission to run this data application.
3. When using the data application in KNIME Business Hub, user authentication will align with the logged-in user's permissions, eliminating the need to provide an application password.

Data Application execution

1. Download the workflow from KNIME Community Hub.



You can find the workflow in the [KNIME Community Hub](#).

2. Upload the downloaded workflow to your KNIME Business Hub instance via [KNIME Analytics Platform](#).
3. Deploy the workflow as a data application. You can learn more about how to do it [here](#).
4. Afterward, execute the newly created data application deployment.

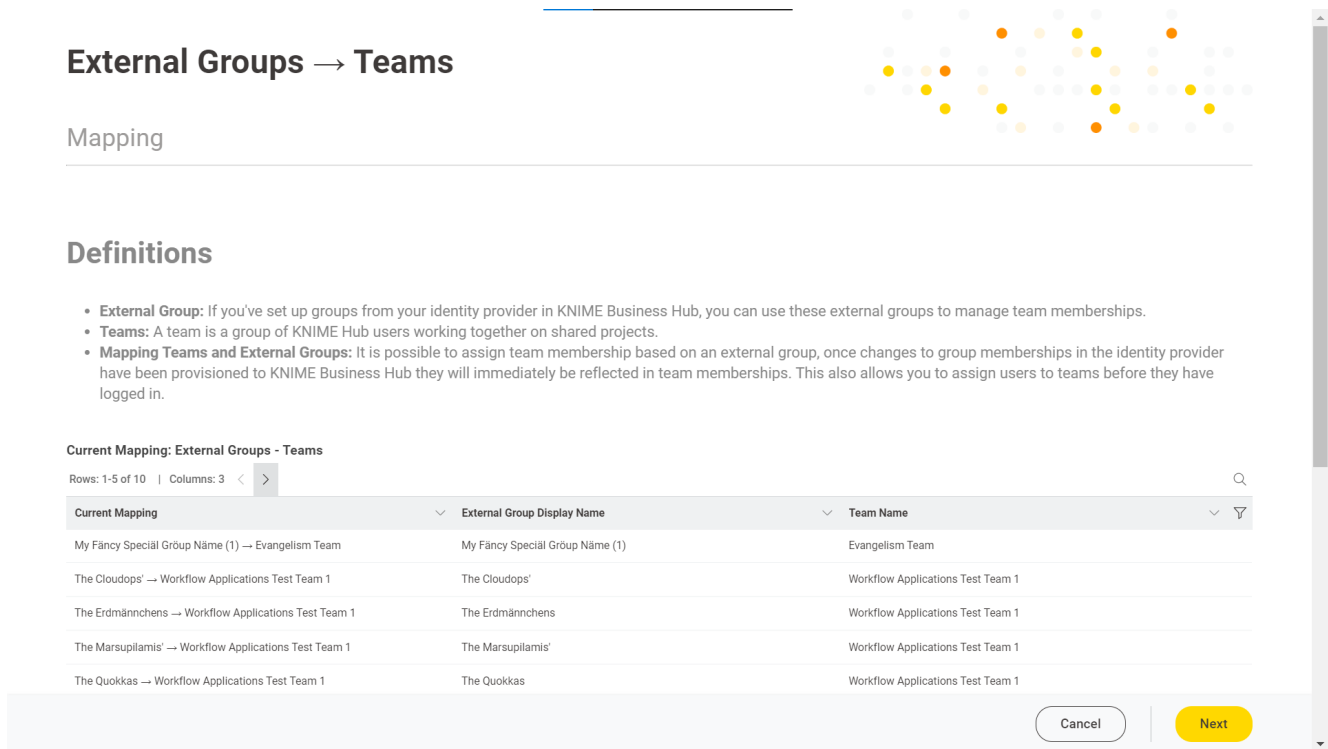
External groups - teams mapping

The one-page data application lets the Global Admin of KNIME Business Hub view the current mapping of the external groups and teams and make additions or deletions to modify it.

Current mapping

Below the main definitions is a table with three columns indicating the current mapping, the external groups, and the teams.

You can use the filters to narrow your research by team name or external group for convenience.



External Groups → Teams

Mapping

Definitions

- **External Group:** If you've set up groups from your identity provider in KNIME Business Hub, you can use these external groups to manage team memberships.
- **Teams:** A team is a group of KNIME Hub users working together on shared projects.
- **Mapping Teams and External Groups:** It is possible to assign team membership based on an external group, once changes to group memberships in the identity provider have been provisioned to KNIME Business Hub they will immediately be reflected in team memberships. This also allows you to assign users to teams before they have logged in.

Current Mapping: External Groups - Teams

Rows: 1-5 of 10 | Columns: 3 < >

Current Mapping	External Group Display Name	Team Name
My Fancy Special Group Name (1) → Evangelism Team	My Fancy Special Group Name (1)	Evangelism Team
The Cloudops' → Workflow Applications Test Team 1	The Cloudops'	Workflow Applications Test Team 1
The Erdmännchens → Workflow Applications Test Team 1	The Erdmännchens	Workflow Applications Test Team 1
The Marsupilamis' → Workflow Applications Test Team 1	The Marsupilamis'	Workflow Applications Test Team 1
The Quokkas → Workflow Applications Test Team 1	The Quokkas	Workflow Applications Test Team 1

Cancel Next

Figure 11. Table with the current external groups assigned to teams.



The table displays just five rows; use the right and left arrows to navigate.

Adding external groups to teams

Once you have a clear understanding of the current external groups assigned to teams, you can add new ones.

1. Choose the "Add external groups to teams" option to complete this task.
 - a. The central search box allows you to add the "external groups - teams" pairs.
 - b. To ease the research process, if too many options are available, you can **copy** either the *external groups* or the *team* names and paste them into the **search box**. This will display only items related to the pasted name.

What do you want to do next?

☒ Add external groups to teams
 ☐ Delete external groups from teams

Available External Groups

- My Fancy Special Group Name
- My Fancy Special Group Name (1)**
- My Fancy Special Group Name (2)
- My Fancy Special Group Name (3)
- My Fancy Special Group Name (4)
- My Fancy Special Group Name (5)
- MyExternalGroupHopefully
- The Cloudops'
- The Erdmännchens
- The Marsupiamis'

My Fancy Special Group Name (1)

- ☐ My Fancy Special Group Name (1) → Another thing
- ☐ My Fancy Special Group Name (1) → Armin and Tobis team
- ☐ My Fancy Special Group Name (1) → Data Science CoE
- ☐ My Fancy Special Group Name (1) → Data Science Team
- ☐ My Fancy Special Group Name (1) → Dev Team
- ☐ My Fancy Special Group Name (1) → Documentation team
- ☐ My Fancy Special Group Name (1) → Evangelism Team
- ☐ My Fancy Special Group Name (1) → Finance Team
- ☐ My Fancy Special Group Name (1) → Joy Division
- ☐ My Fancy Special Group Name (1) → knime_admins team
- ☐ My Fancy Special Group Name (1) → knime_admins team 1

Available Teams

- Another thing
- Armin and Tobis team
- Data Science CoE
- Data Science Team
- Dev Team
- Documentation team
- Evangelism Team
- Finance Team
- Joy Division
- LS Team

Figure 12. Copy the desired external group name and paste it into the search box.

- After adding all the desired external groups to the target teams in the search box, click "Next." After a short wait, you will see the same page with the newly added external groups. You can use the table filters to find them.
- Afterward, the users in the external group will **immediately** appear as members of the respective team.

Delete external groups from teams

To detach an external group from a specific team, you can follow these steps:

- Select the "Delete external groups from teams" option.
- Refer to the "Current Mapping: External Groups—Teams" table to determine which external groups are attached to which teams.
- In the search box, enter the name of the external group or team that you want to delete.

Current Mapping: External Groups - Teams

Rows: 1 | Columns: 3

Current Mapping	External Group Display Name	Team Name
My Fäncý Special Gróup Náme (1) → Evangelism Team	My Fäncý Special Gróup Náme (1)	Evangelism Team

What do you want to do next?

☐ Add external groups to teams ☒ Delete external groups from teams

My Fäncý Special Gróup Náme (1) → Evangelism Team X



Search by typing the team or external group in the box above.

Use the table "Current Mapping" above as a reference.

Figure 13. The external group that will be deleted from the team is added to the search box.

- Once you have added all the external groups and their corresponding teams in the search box, click "Next."



After clicking "Next", all the users in the external group will **immediately** be removed as members of the respective team.

Warnings and errors

The data application may encounter various errors or issues during execution.

- If the KNIME Business Hub API responds poorly, the data application has trouble communicating with it via REST requests. If this happens, a clear error message should be displayed to inform the user.
- If external groups have yet to be provided for the current KNIME Business Hub, you must follow **all the steps provided above** before running the data application.
- When running the data application for the first time, an information message indicates that no external groups are assigned to any team. To add them, use the search box and click "Next".

External Groups → Teams

Mapping



Definitions

- **External Group:** If you've set up groups from your identity provider in KNIME Business Hub, you can use these external groups to manage team memberships.
- **Teams:** A team is a group of KNIME Hub users working together on shared projects.
- **Mapping Teams and External Groups:** It is possible to assign team membership based on an external group, once changes to group memberships in the identity provider have been provisioned to KNIME Business Hub they will immediately be reflected in team memberships. This also allows you to assign users to teams before they have logged in.

 There are no external groups added to any team.

Current Mapping: External Groups - Teams

No data | Columns: 3



Current Mapping	External Group Display Name	Team Name
-----------------	-----------------------------	-----------

Figure 14. There are no external groups associated with teams.

4. Suppose a KNIME Business Hub team admin or member tries to run the data application. In that case, an error message will appear, telling the user that only Global Admins can execute the application.
5. If you proceed without selecting any item in the search box and click "Next", a warning message will be displayed, prompting you to return to the external groups teams mapping stage by clicking "Next" again.

Expose external groups inside KNIME Business Hub (Standard and Enterprise editions only)

In case you cannot use **SCIM**, there are two other possibilities for bringing external groups into your KNIME Business Hub installation. As a Global KNIME Hub administrator you can configure groups that are provided via an external identity provider to be exposed inside the KNIME Business Hub instance.

Two possible sources for your external groups are:

1. Groups are provided within the access token of your OIDC provider
2. Groups are imported from LDAP by federating the login

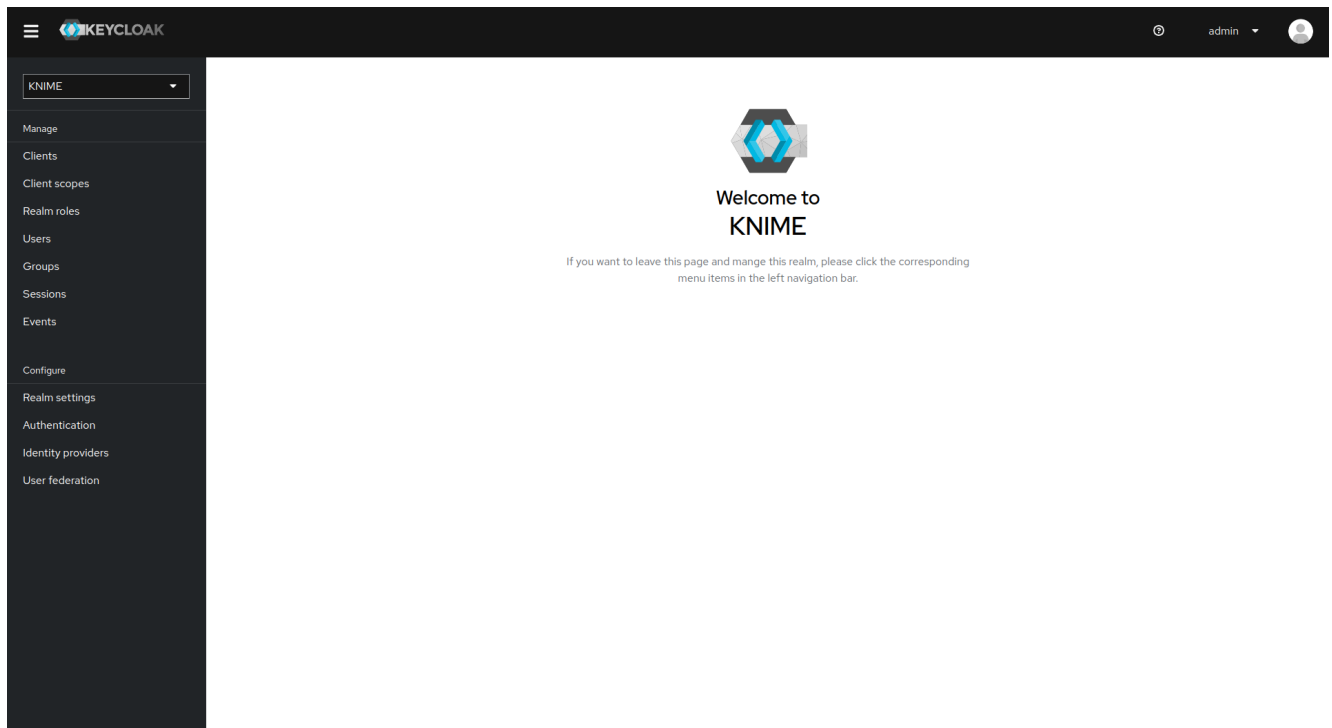
External OIDC provider

Assume you have an identity provider that provides groups through a **groups** claim in the access token.

```
{
  ...,
  "groups": [
    "finance",
    "marketing",
    "data"
  ]
}
```

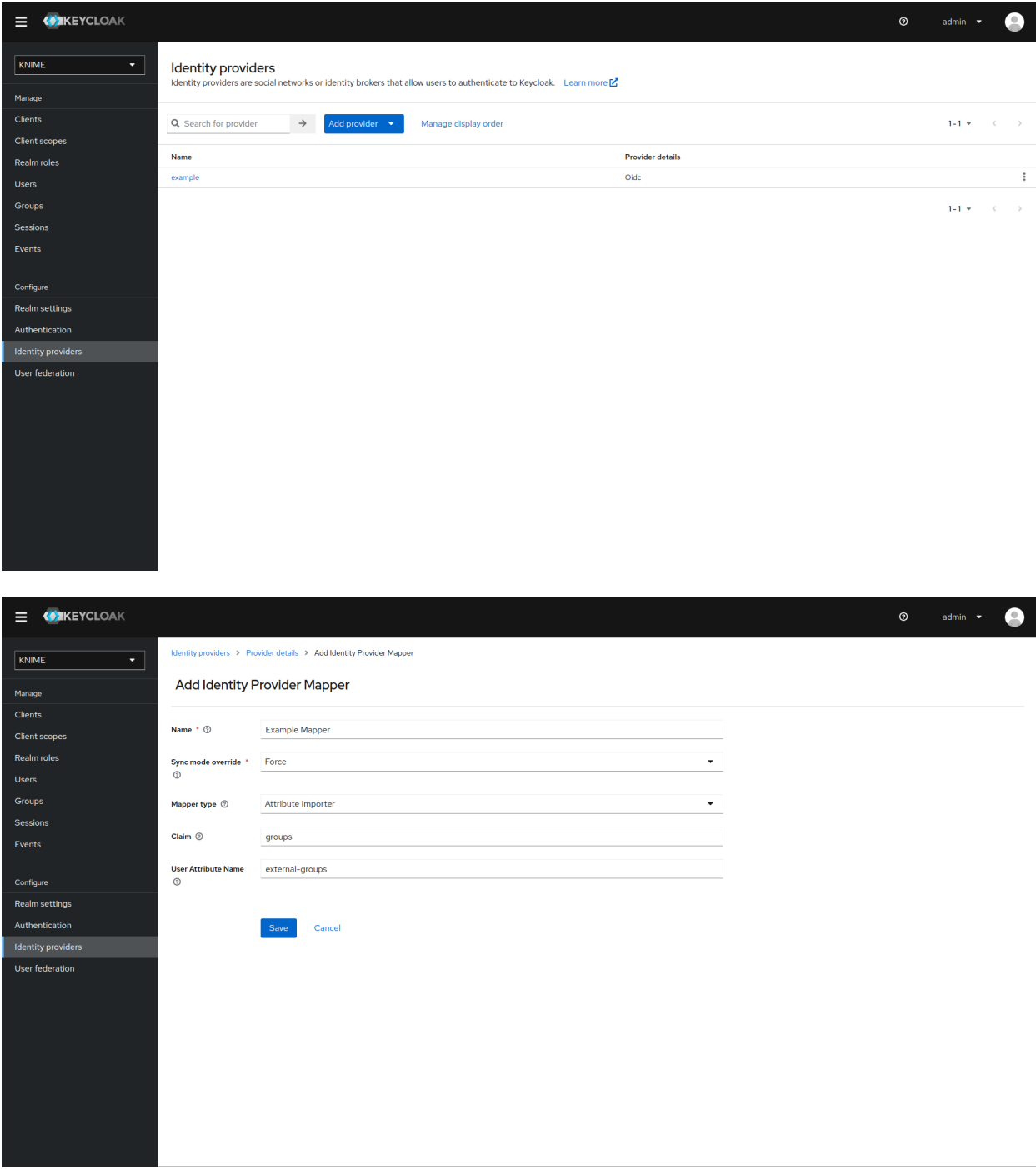
First you need to configure Keycloak in such a way that it can map these groups to a **user attribute**. The second step is to add a mapper that maps these user attributes into the Keycloak's tokens.

Your third-party identity provider should have been set up already. Keycloak has to be configured as follows:

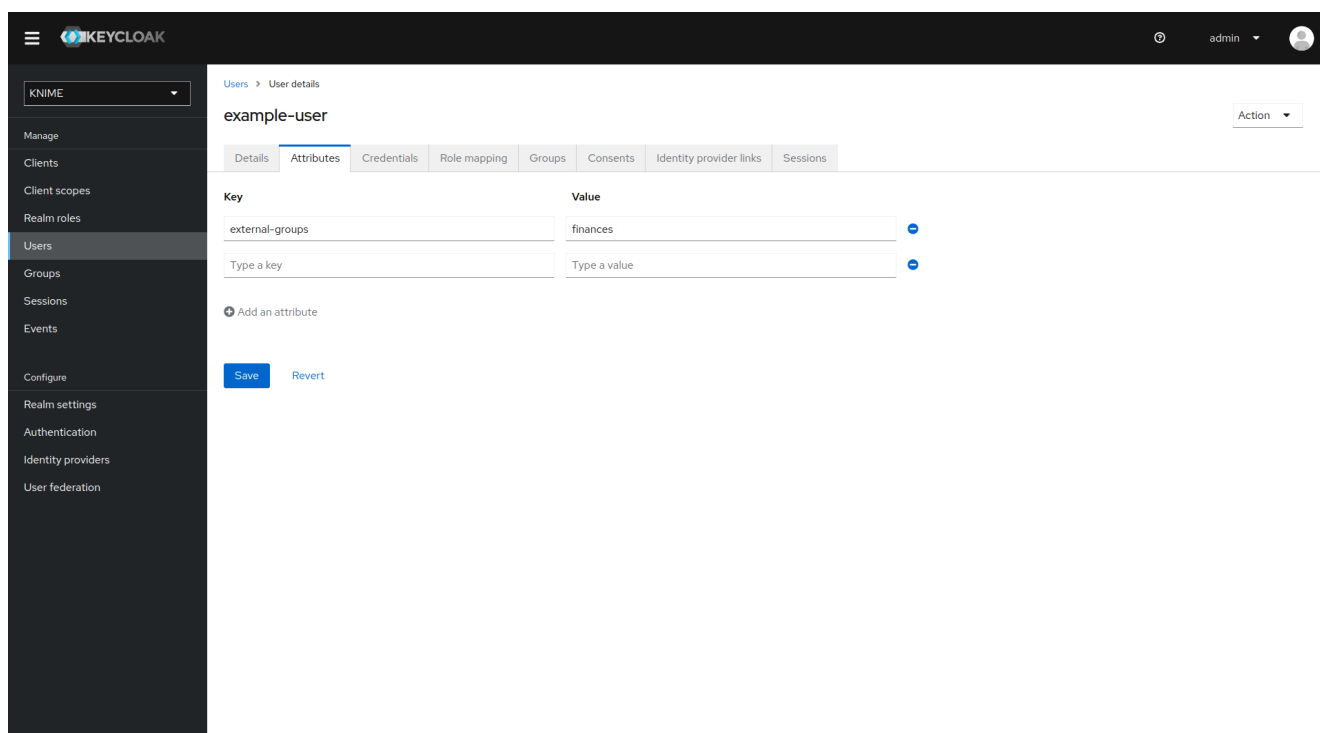


First step is to add an Attribute Importer Mapper.

1. In Keycloak select realm *Knime* in the top left dropdown menu
2. On the left tab select *Identity Providers*
3. Select your third-party provider
4. Switch to the tab *Mappers* and click on *Add mapper*
5. Provide a name for the mapper and set the *Sync mode override* to *Force* to ensure that the user's group memberships are updated upon every login
6. Set *Mapper type* to *Attribute importer*
7. Enter the *Claim* that contains the external groups in the original token (in our example *groups*)
8. In the *User Attribute Name* field enter *external-groups*
9. Click on *Save*



Now, every user in Keycloak who logged in after the mapper has been added will have an *external-groups* attribute associated like in the following picture:



Now, the external groups are known to Keycloak. To expose them inside KNIME Business Hub they need to be mapped into the access tokens issued by Keycloak. For this a second mapper needs to be added, that maps the user attribute *external-groups* to a claim in the user's access token.

To do this you need to add a client scope, which includes a mapper for the user attribute.

1. On the left tab select *Client scopes*
2. Select *groups*
3. Switch to the tab *Mappers*
4. Click on *Add mapper* > *By configuration* and select *User Attribute* from the list
5. Provide a name, e.g. *external-groups-attribute-mapper*
6. Set both fields *User Attribute* and *Token Claim Name* to *external-groups*
7. Ensure that *Add to ID token*, *Add to access token* and *Aggregate attribute values* are turned off
8. Ensure that *Add to userinfo* and *Multivalued* are turned on
9. Click on *Save*

KEYCLOAK

KNIME

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Client scopes

Client scopes are a common set of protocol mappers and roles that are shared between multiple clients. [Learn more](#)

▼ Name

Search for client scope

→

Create client scope

Change type to

1-10

<

>

<input type="checkbox"/>	Name	Assigned type	Protocol	Display order	Description	
<input type="checkbox"/>	acr	Default	OpenID Connect	–	OpenID Connect scope for add acr (authentication context class reference) to the token	⋮
<input type="checkbox"/>	address	Optional	OpenID Connect	–	OpenID Connect built-in scope: address	⋮
<input type="checkbox"/>	email	Default	OpenID Connect	–	OpenID Connect built-in scope: email	⋮
<input type="checkbox"/>	external-groups-scope	Default	OpenID Connect	–	scope for external groups	⋮
<input type="checkbox"/>	groups	None	OpenID Connect	–	–	⋮
<input type="checkbox"/>	microprofile-jwt	Optional	OpenID Connect	–	Microprofile - JWT built-in scope	⋮
<input type="checkbox"/>	offline_access	Optional	OpenID Connect	–	OpenID Connect built-in scope: offline_access	⋮
<input type="checkbox"/>	phone	Optional	OpenID Connect	–	OpenID Connect built-in scope: phone	⋮
<input type="checkbox"/>	profile	Default	OpenID Connect	–	OpenID Connect built-in scope: profile	⋮
<input type="checkbox"/>	role_list	Default	SAML	–	SAML role list	⋮

1-10<>

KEYCLOAK

KNIME

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Client scopes > Client scope details

Groups [openid-connect](#)

Action

SettingsMappersScope

Search for mapper

→

Add mapper

1-1

<

>

Name	Category	Type	Priority	
groups	Token mapper	User Realm Role	40	⋮

1-1<>

The screenshot shows the Keycloak Admin Console interface. On the left is a dark sidebar with navigation links: Manage, Clients, Client scopes, Realm roles, Users, Groups, Sessions, Events, Configure, Realm settings, Authentication, Identity providers, and User federation. The 'Clients' section is expanded, showing 'Client scopes' and 'Mapper details'. The main area is titled 'Add mapper' with a subtitle 'If you want more fine-grain control, you can create protocol mapper on this client'. The 'Mapper type' is set to 'User Attribute'. The configuration fields are: Name (external-groups-attribute-mapper), User Attribute (external-groups), Token Claim Name (external-groups), Claim JSON Type (String), Add to ID token (On), Add to access token (On), Add to userinfo (On), Multivalued (On), and Aggregate attribute values (Off). At the bottom are 'Save' and 'Cancel' buttons.

With both mappers in place, the external groups are part of userinfo response returned by Keycloak. By this, the external groups are exposed inside KNIME Business Hub. In order to enable external groups to be used for permissions and access management they need to be configured separately through the admin REST API as described in [Enable external groups](#).

LDAP federation



Before proceeding with the following steps you need to have a user federation configured for an LDAP instance.

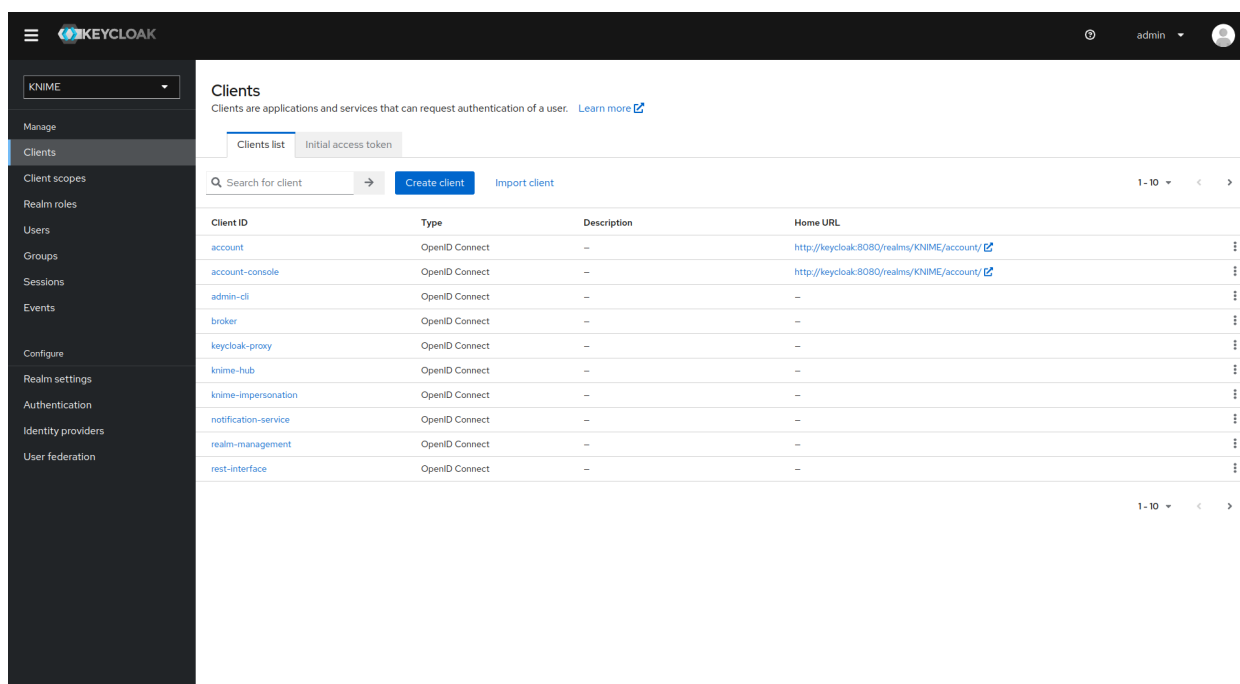
Once you have configured user federation for an LDAP instance that also supplies external group names, you need to configure mappers that map these groups into the access tokens used inside the Hub instance.

To ensure that groups from Keycloak groups and groups from LDAP are not mixed we recommend to treat external groups as realm roles.

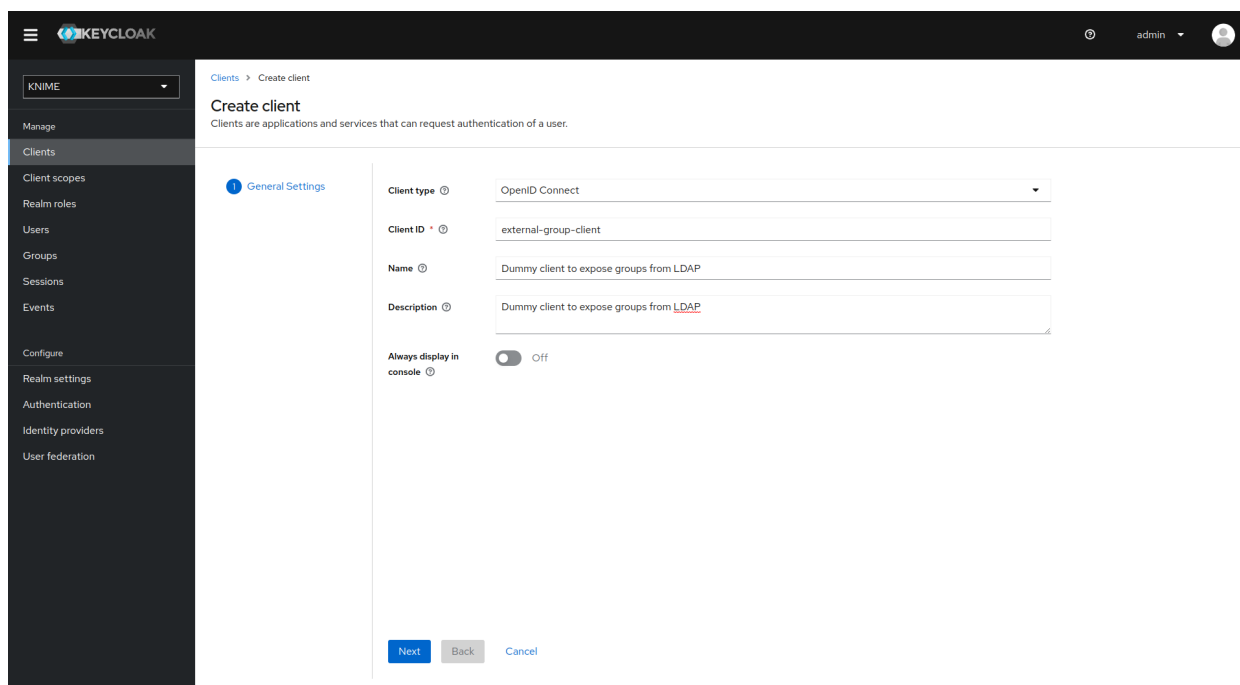
In order to do this we recommend to first create a dummy client for which roles can be created based on the LDAP groups. This will guarantee that any changes will be compatible with future changes to the KNIME Hub client in Keycloak.

To create a new client follow these steps:

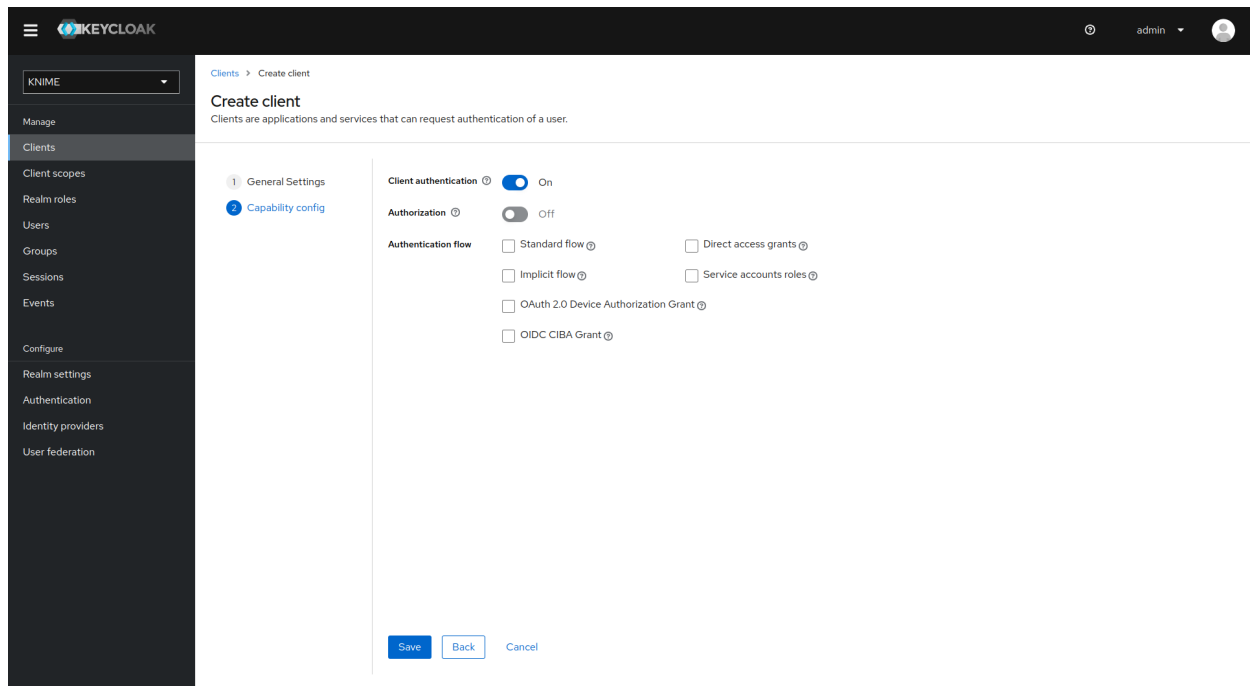
1. In Keycloak select realm *Knime* in the top left dropdown menu
2. On the left tab select *Clients* and click *Create client*



3. Set *Client type* to *OpenID Connect*
4. Enter a *Client ID* (in our example *external-group-client*), and a useful *Name* and *Description*
5. Click on *Next*



6. De-select all checkboxes of *Authentication flow* in the *Capability config* section, since this client will not require any capabilities
7. Enable *Client authentication*
8. Click on *Save*



Now that the dummy client is set up, you can proceed to create a mapper that maps the user groups from LDAP to roles inside the dummy client:

1. On the left tab select *User federation* and click on your LDAP configuration
2. Switch to the tab *Mappers*
3. Click on *Add mapper*
4. Provide a name, e.g. *ldap-group-to-dummy-client-role-mapper*
5. Set *Mapper type* to *role-ldap-mapper*
6. Setup the mapper according to your LDAP
7. Disable *User Realm Roles Mapping*
8. Set *Client ID* to the previously created dummy client (in our example *external-group-client*)
9. Click on *Save*

The screenshot shows the Keycloak Admin Console interface. On the left is a sidebar with navigation links: Manage, Clients, Client scopes, Realm roles, Users, Groups, Sessions, Events, Configure, Realm settings, Authentication, Identity providers, and User federation (which is selected). The main content area is titled 'Create new mapper' and contains a form with the following fields:

- Name: ldap-group-to-dummy-client-role-mapper
- Mapper type: role-ldap-mapper
- LDAP Roles DN: OU=groups, DC=knime, DC=com
- Role Name LDAP Attribute: CN
- Role Object Classes: groupOfNames
- Membership LDAP Attribute: member
- Membership Attribute Type: DN
- Membership User LDAP Attribute: CN
- LDAP Filter: (empty)
- Mode: READ_ONLY
- User Roles Retrieve Strategy: LOAD_ROLES_BY_MEMBER_ATTRIBUTE
- Member-Of LDAP Attribute: memberOf
- Use Realm Roles Mapping: Off (toggle)
- Client ID: external-group-client

At the bottom of the form are 'Save' and 'Cancel' buttons.

Now if a user logs in with the LDAP credentials the user's groups will be mapped to ad-hoc created client roles inside the 'external-group-client'.

Next, you need to create a mapper that maps a user's realm roles from the dummy realm to the access tokens:

1. On the left tab select *Client scopes*
2. Select *groups*
3. Switch to the tab *Mappers*
4. Click on *Add mapper* > *By configuration* and select *User Client Role* from the list
5. Provide a name, e.g. *external-ldap-client-role-mapper*
6. Set *Client ID* to the previously created dummy client (in our example *external-group-client*)
7. Set *Token Claim Name* to *external-groups*
8. Set *Claim JSON Type* to *String*
9. Ensure that *Add to ID token*, *Add to access token*, *Add to userinfo*, and *Multivalued* are turned on

10. Click on Save

The screenshot shows the Keycloak Admin Console interface. The left sidebar contains navigation links: Manage, Clients, Client scopes (selected), Realm roles, Users, Groups, Sessions, Events, Configure, Realm settings, Authentication, Identity providers, and User federation. The main content area is titled 'Add mapper' and includes a breadcrumb trail: 'Client scopes > Client scope details > Mapper details'. Below the title, there is a sub-header 'Add mapper' and a note: 'If you want more fine-grain control, you can create protocol mapper on this client'. The form contains the following fields and controls:

- Mapper type:** A dropdown menu set to 'User Client Role'.
- Name:** A text input field containing 'external-ldap-client-role-mapper'.
- Client ID:** A dropdown menu set to 'external-group-client'.
- Client Role prefix:** An empty text input field.
- Multivalued:** A toggle switch set to 'On'.
- Token Claim Name:** A text input field containing 'external_groups'.
- Claim JSON Type:** A dropdown menu set to 'String'.
- Add to ID token:** A toggle switch set to 'On'.
- Add to access token:** A toggle switch set to 'On'.
- Add to userinfo:** A toggle switch set to 'On'.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom.

Enable external groups

Once you have configured the external groups in Keycloak you need to create the groups that you want to be available inside KNIME Business Hub.

To do so you have to make a PUT request to the corresponding endpoint:

```
PUT https://api.<base-url>/accounts/hub:global/groups/<external-group-name>
```

where <external-group-name> is the name of the group and it must match the group name in the external identity provider.

Docker executor images

In order to create **execution contexts** for their teams, team admins will need to reference the Docker image of the KNIME Executor that they want to use.

Public Docker executor images are made available by KNIME which correspond to the full builds of KNIME Executor versions 4.7.4 and higher.

The currently available executor images have the following docker image name:

- `registry.hub.knime.com/knime/knime-full:r-4.7.4-179`
- `registry.hub.knime.com/knime/knime-full:r-4.7.5-199`
- `registry.hub.knime.com/knime/knime-full:r-4.7.6-209`
- `registry.hub.knime.com/knime/knime-full:r-4.7.7-221`
- `registry.hub.knime.com/knime/knime-full:r-4.7.8-231`
- `registry.hub.knime.com/knime/knime-full:r-5.1.0-251`
- `registry.hub.knime.com/knime/knime-full:r-5.1.1-379`
- `registry.hub.knime.com/knime/knime-full:r-5.1.2-433`
- `registry.hub.knime.com/knime/knime-full:r-5.1.3-594`
- `registry.hub.knime.com/knime/knime-full:r-5.2.0-271`
- `registry.hub.knime.com/knime/knime-full:r-5.2.1-369`
- `registry.hub.knime.com/knime/knime-full:r-5.2.2-445`
- `registry.hub.knime.com/knime/knime-full:r-5.2.3-477`
- `registry.hub.knime.com/knime/knime-full:r-5.2.4-564`
- `registry.hub.knime.com/knime/knime-full:r-5.2.5-592`
- `registry.hub.knime.com/knime/knime-full:r-5.2.6-758`
- `registry.hub.knime.com/knime/knime-full:r-5.3.0-388`
- `registry.hub.knime.com/knime/knime-full:r-5.3.1-498`
- `knime/knime-full:r-5.3.2-564`
- `knime/knime-full:r-5.3.3-666`



Please note that with the release of 5.2.2 KNIME executors will have HTML sanitization of old JavaScript View nodes and Widget nodes turned on by default. This ensures that no malicious HTML can be output. For more information check the [KNIME Analytics Platform 5.2.2 changelog](#).

However you might want to customize the executor image, e.g. by adding specific extensions or default conda environments.

The following section explains how to do so.

Add extensions to an existing Docker image

In order to install additional extensions and features to the KNIME Executor image, you will need to first create a `Dockerfile`, build a Docker image from it, and finally make it available by pushing it to a registry. You can do this in two ways:

1. Via a data application, provided by us and described in the [next section](#). Prerequisites:
 - The Execution Image Builder needs to be enabled: *KOTS Admin Console > Config > Execution Image Builder > check **Enable Execution Image Builder***.
 - You need global admin privileges in order to build and push the image. Deploy the data app while configuring it with an application password of the global admin to make it available for others, e.g. team admins (the application password is not visible to others that way). If you use the data app not as a global admin, you can still create the Dockerfile, but you won't be able to build and push it to the registry.
2. Via a manual approach, as described [below](#), if the Execution Image Builder service is not available. Prerequisites:
 - `docker` should be installed.



If you need to install `docker` please make sure not to install it on the same virtual machine (VM) where the KNIME Business Hub instance is installed, as it might interfere with `containerd`, which is the container runtime used by Kubernetes.

Registry Prerequisites

Enabling the Image Builder allows to build execution image in the cluster and to push it to a specified registry. There are three different scenarios where the Image Builder has access to the Embedded Docker Registry, to the registry specified in the *Registry settings* tab in the KOTS Admin Console, and to the registry defined in the *Custom Execution Image Pull Secret* that can be set in the Execution Contexts section of the Config tab in KOTS Admin Console:

1. The embedded registry (default, available only in embedded clusters). To activate it, go to *KOTS Admin Console > Config > Embedded Registry > check Enable Embedded Registry*. If you follow the manual approach, have the username and password ready that is defined in the KOTS Admin Console. See also [KNIME Business Hub Installation Guide](#) for more information.
2. The registry defined in the *Custom Execution Image Pull Secret* (if the embedded registry is not available, e.g. in non-embedded clusters). To create such a secret, go to *KOTS Admin Console > Execution Contexts > check Enable Custom Execution Image Pull Secret* and put in an *Execution Image Pull Secret* (<secret-name> in the commands below). Then, add this secret to the cluster in the name spaces hub and hub-execution via the commands

```
kubectl -n hub-execution create secret docker-registry <secret-name> --docker
-server=<registry-url> --docker-username=<username> --docker-password=<secret>
kubectl -n hub create secret docker-registry <secret-name> --docker
-server=<registry-url> --docker-username=<username> --docker-password=<secret>
```

You can use the <registry-url> in the data app. For the manual approach, you don't need to create the secret, but the URL, username, and password of the registry.

3. The registry as defined in the *KOTS Admin Console > Registry settings* (e.g. for [air gap installations](#)). If you follow the manual approach, have the username and password for this registry ready.



Building a Docker image requires enhanced container privileges. To be precise, the container needs to run as root with following capabilities:

- CHOWN
- SETUID
- SETGID
- FOWNER
- DAC_OVERRIDE

Depending on the size of the image, the build requires a lot of resources and can potentially slow down the KNIME Business Hub during the build time.

Using the Executor Image Builder data application

We provide an [Executor Image Builder](#) data application that will help you create the file, build an executor image, and push it to a registry to make it available when [creating or editing an](#)

execution context. Download the data application, upload it to your KNIME Business Hub instance, and *Run* it.



Follow the steps 1 through 3 of the [Data apps on KNIME Hub](#) for detailed instructions.

The data app consists of five steps, displayed on five pages.

First Page: Settings

First, you'll find the basic settings.

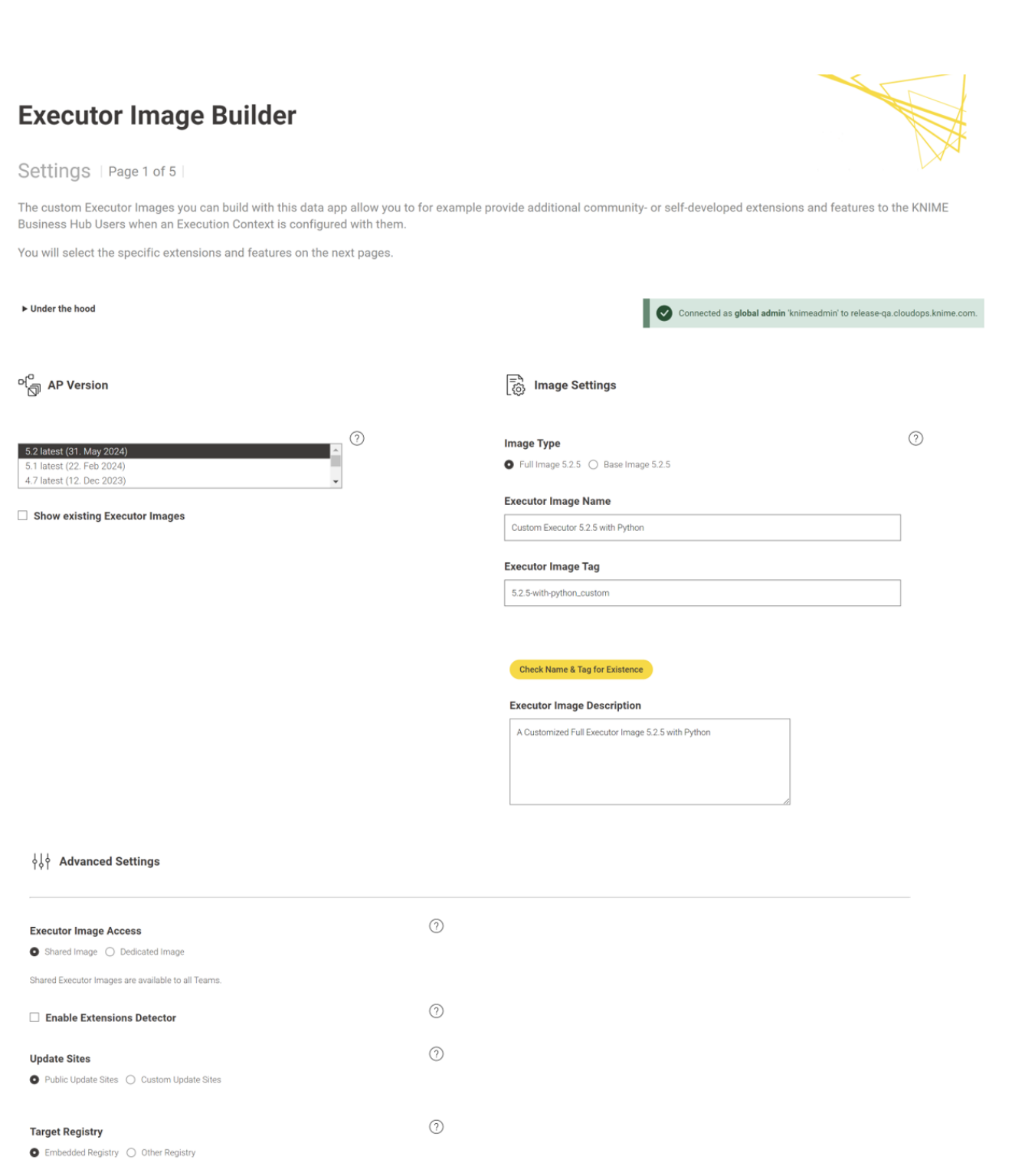
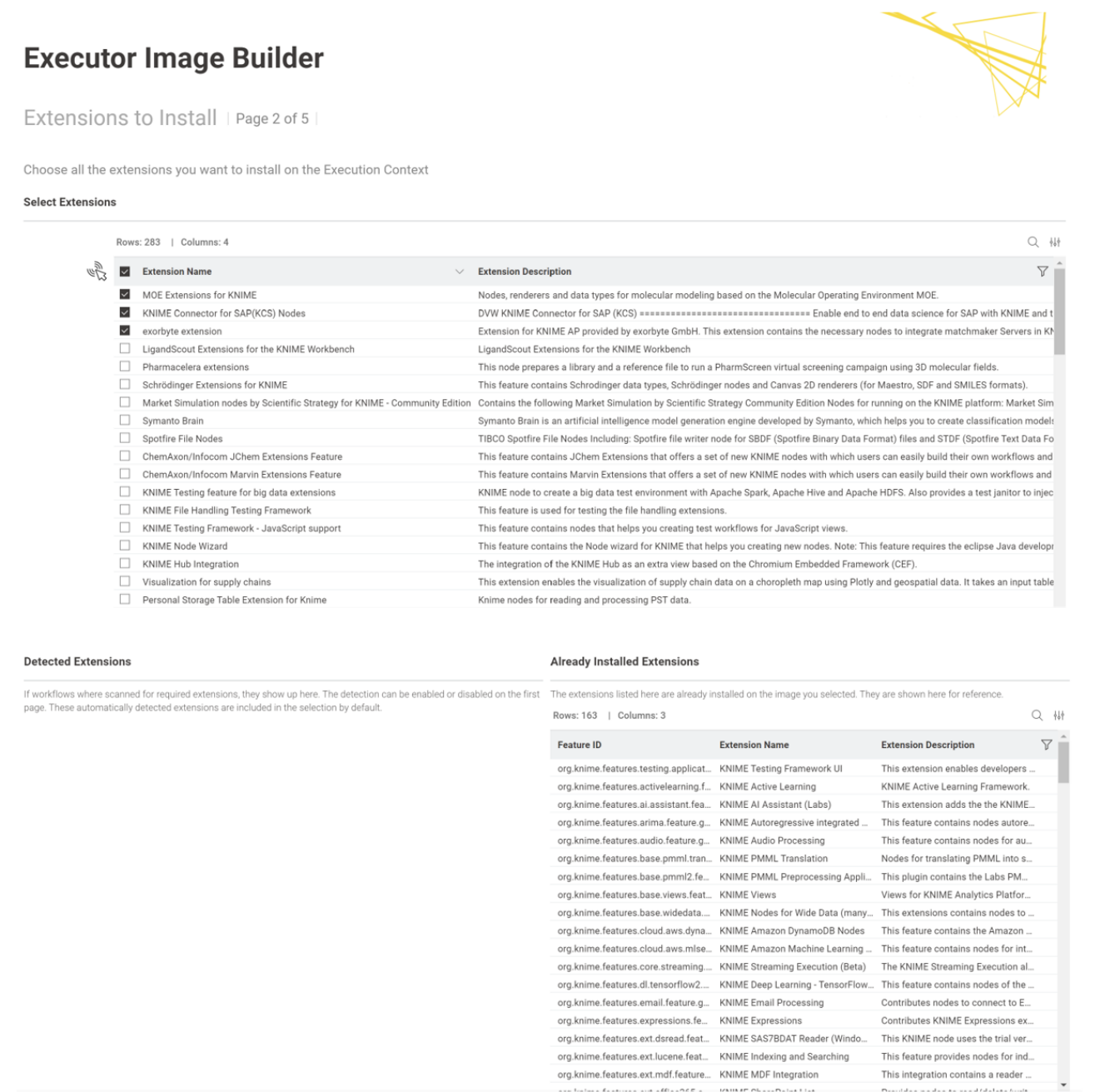


Figure 15. Executor Image Builder Settings on the first page as seen by a global admin.

If you hover over the setting or question mark in the data app, you'll find a detailed description of what each setting is for. Note that the settings related to image building and pushing are only available to global admins.

You proceed by clicking the *Next Button*.

Second Page: Extension Selection





Executor Image Builder

Conda/Python and R Integrations | Page 3 of 5 |

These integrations allow your users to use e.g. the Python Script or R Snippet Nodes.

Python Integration (Conda)

The Conda integration allows you to manage virtual environments via the Conda Environment Propagation Node that e.g. provide Python.

☐ Add Python Environment



R Integration

The R Integration feature allows you to install and use R packages in the Executor. Packages must be entered individually into the widget.

☐ Setup R



Setup Preview

Python

Conda (micromamba) included in base image
No Additional Conda Environment

R

No R Setup

Figure 17. Executor Image Builder Python and R Integration configuration on the third page.

On the third page, you decide on whether to install conda/python, respectively additional default environments to the image, or the R integration.

Python

Learn more about how the KNIME Python Integration works with the [KNIME Python Integration Guide](#)

If your choice of image type (base or full) does not already include conda (specifically: micromamba as the management software of the virtual environments), you can choose to add it here. You need this, if the workflows you run on this executor contain e.g. a [Conda Environment Propagation node](#).

If conda/micromamba is installed, you can further choose to provide a virtual environment that is already installed on the executor. This has the advantage that after a restart of the executor, the [Conda Environment Propagation node](#) executes faster, as the environment does not need to be recreated first. You add an environment by uploading a `.yaml` file, which describes the environment. You can use the following example `.yaml` file and modify it to your needs, e.g. by adding packages (and their versions) that you require:

```

name: py39_knime          # Name of the created environment
channels:                 # Repositories to search for packages
- conda-forge
dependencies:             # List of packages that should be installed
- python=3.9              # Python
- py4j                    # used for KNIME <-> Python communication
- nomkl                   # Prevents the use of Intels MKL
- pandas                  # Table data structures
- jedi=0.18.1             # Python script autocompletion
- python-dateutil         # Date and Time utilities
- numpy                   # N-dimensional arrays
- cairo                   # SVG support
- pillow                  # Image inputs/outputs
- matplotlib              # Plotting
- pyarrow=6.0             # Arrow serialization
- IPython                 # Notebook support
- nbformat                # Notebook support
- scipy                   # Notebook support
- python-flatbuffers<2.0  # because tensorflow expects a version before 2
- h5py<3.0                # must be < 3.0 because they changed whether str or byte is
returned
- protobuf>3.12           # Lower protobuf versions do not work with TensorFlow 2
- libiconv                # MDF Reader node
- asammdf=5.19.14         # MDF Reader node
- JPype1                  # Databases

```

To learn more about how to create conda environment files, visit the [conda docs](#). If you want to pre-install multiple conda environments, please edit the Dockerfile manually on the next page of the data app.



In order for the executor to find the conda installation, the execution context needs to know where to find conda. This is done as a final step and is described [below](#).


Unless modified, the path to the conda installation is `/home/knime/miniconda3/`, and the path to the environment (see below) is `<path to default conda environment dir>=<path to conda installation dir>/envs/<name of the env>`.

In the full images of KNIME Executor version 5.2 and above, where conda and Python are preinstalled, the path to conda is the same, i.e.

`/home/knime/miniconda3/` and the paths to the default environments are `/home/knime/miniconda3/py2_knime` and `/home/knime/miniconda3/py3_knime`.

You can make R available as an **integration** if the workflows are expected to contain nodes from the **KNIME R Scripting extension**. Provide a comma-separated list of additional packages in the provided input field.

Fourth Page: Dockerfile Review



Executor Image Builder

Dockerfile Check | Page 4 of 5 |

The Dockerfile was successfully generated. Please review it below and edit it to you needs, if applicable. By clicking 'Next', it will be sent to the Image Builder Service on the Hub, where the image is being built. This process might take a while.

☐ Dockerfile Edit Mode

[Download Link](#)
[? Dockerfile](#)

Dockerfile Preview

```
# Define the base image
FROM registry.hub.knime.com/knime/knime-full:r-5.2.5-592-with-python

# Define the list of update sites and features
ENV KNIME_UPDATE_SITES="https://update.knime.com/analytics-platform/5.2/5.2.5, https://update.knime.com/community-contributions/trusted/5.2, https://update.knime.com/partner/5.2, https://update.knime.com/community-contributions/5.2"

# Install features from the update sites
ENV KNIME_FEATURES="com.chemcomp.feature.group,com.dvw.knime.sap.feature.feature.group,com.exorbyte.knime.feature.feature.group"

# Install CA Certificates
USER root
RUN apt-get update && \
  apt-get install -y ca-certificates && \
  update-ca-certificates && \
  rm -rf /var/lib/apt/lists/*
USER knime

# Execute extension installation script
RUN ./install-extensions.sh

# No R Setup

# Conda (micromamba) included in base image
# No Additional Conda Environment

# user root needs to do the prestart
USER root
# pre-start executor, to improve startup time
RUN KNIME_EXECUTOR_CONNECTION_RETRIES=0 knime/knime -consolelog -nosplash -application com.knime.enterprise.slave.KNIME_REMOTE_APPLICATION; rm -rf /root/knime-workspace
USER knime
```

Figure 18. Executor Image Builder Dockerfile review on the fourth page. This is the final page for users that are not global admins.

Here you are able to review the Dockerfile and do manual edits, if needed. To do this, enable the Dockerfile Edit Mode, and change the Dockerfile based on your needs.

- If you are **not** connected as a **global admin**, you can proceed to **build** and **push** the Dockerfile manually.
- If you are the **global admin** and proceed to the next page, the Dockerfile is sent to the image builder endpoint, where the image is actually built, and then pushed to the executor image list.

Fifth Page: Dockerfile Building and Pushing

Executor Image Builder



Create Executor Image Info | Page 5 of 5 |

You can now reference the Docker Image of the Executor in the team resources page or in the Administration panel, if you are a global admin, and deploy your custom Execution Context on KNIME Business Hub.

Copy the image URL from the Table View below and paste it into the 'Docker Image' field when creating the Execution Context

Created Executor Images

Result	Image Uri	Add Execution Context	Executor Name	Team	
Executor image info created	registry.release-qa.cloudops.knime.com/knime-executor:5.2.5-with-python_custom	→ Admin Execution Resources	Custom Executor 5.2.5 with Python	A shared execution context can be used by all teams	Proces

*Figure 19. Executor Image Builder Dockerfile final page with the result of the building process. Copy the image URL and use it when **creating or editing an execution context**.*

If you didn't encounter any errors during the building phase, the final image URL is shown. You can copy this, proceed to the Execution Resources page to **create a new execution context**, or edit an existing one, and paste the URL there.

Finally, go ahead and test the execution of a workflow containing a node from the freshly installed extensions or one that uses python.

Adding extensions manually

Instead of using the data app, you can also go through the steps manually.

Create the Dockerfile

You can use the example below which demonstrates how to extend an existing executor image with a custom set of update sites and features.

```
# Define the base image
FROM registry.hub.knime.com/knime/knime-full:r-5.2.5-592

# Change to root user to be able to install system packages
USER root

# Update/upgrade package manager and install ca-certificates to enable ca certificates
that micromamba (for python) is asking for
RUN apt-get update && \
    apt-get upgrade -yq && \
    apt-get install -yq \
        ca-certificates && \
    # cleanup
    rm -rf /var/lib/apt/lists/*

# Change to knime user to handle extensions
USER knime

# Define the list of update sites and features
# Optional, the default is the KNIME Analytics Platform update site (first entry in the
list below)
ENV KNIME_UPDATE_SITES=https://update.knime.com/analytics-
platform/5.2,https://update.knime.com/community-contributions/trusted/5.2
# Install a feature from the Community Trusted update site
ENV KNIME_FEATURES="org.knime.features.geospatial.feature.group"

# Execute extension installation script
RUN ./install-extensions.sh
```

The `KNIME_UPDATE_SITES` environment variable determines the update sites that will be used for installing KNIME Features. It accepts a comma-delimited list of URLs. The `KNIME_FEATURES` environment variable determines the extensions which will be installed in the KNIME Executor. It accepts a comma-delimited list of feature group identifiers. A corresponding update site must be defined in the `KNIME_UPDATE_SITES` list for feature groups to be successfully installed. You can get the necessary identifiers by looking at *Help → About KNIME → Installation Details → Installed Software* in a KNIME instance that has the desired features installed. Take the identifiers from the "Id" column and make sure you do not omit the `.feature.group` at the end (see also screenshot on the next page). The base image contains a shell script `install-extensions.sh` which lets you easily install additional extensions in another Dockerfile.



The previous version of the Executor Image Builder allowed to create the Dockerfile, just like the [Executor Image Builder Data App](#) allows for non-global admins. You can use the resulting Dockerfile as a starting point.

Python Integration

If you want the executor to run workflows with the **Conda Environment Propagation node**, you need to install conda (respectively micromamba or any other conda environment manager). You can do so by adding the following lines to the Dockerfile:

```
# START Conda setup
# install additional packages
USER root
RUN apt-get update && \
apt-get install -y curl bzip2 && \
rm -rf /var/lib/apt/lists/*
USER knime
SHELL [ "/usr/bin/bash", "-o", "pipefail" ,"-c" ]
RUN set -x && \
mkdir -p ~/.local/bin && \
curl -Ls https://micro.mamba.pm/api/micromamba/linux-64/latest | tar -xvj -C \
${HOME}/.local/bin/ --strip-components=1 bin/micromamba && \
${HOME}/.local/bin/micromamba shell init -s bash -p ~/miniconda3
ENV MAMBA_ROOT_PREFIX=/home/knime/miniconda3
USER root
RUN ln -s /home/knime/.local/bin/micromamba /usr/local/bin/micromamba
USER knime
# legacy conda support
RUN micromamba install -y -n base conda -c conda-forge
# END Conda setup
```

If you additionally want to provide pre-installed environments, add them to the Dockerfile like below:

```
# START Python Environment Setup
RUN echo $'\
name: py39_knime          # Name of the created environment\n\
channels:                 # Repositories to search for packages\n\
- conda-forge\n\
dependencies:             # List of packages that should be installed\n\
- python=3.9              # Python\n\
- py4j                    # used for KNIME <-> Python communication\n\
- nomkl                   # Prevents the use of Intels MKL\n\
- pandas                  # Table data structures\n\
- jedi=0.18.1             # Python script autocompletion\n\
- python-dateutil         # Date and Time utilities\n\
- numpy                   # N-dimensional arrays\n\
- cairo                   # SVG support\n\
- pillow                  # Image inputs/outputs\n\
- matplotlib              # Plotting\n\
- pyarrow=6.0             # Arrow serialization\n\
- IPython                 # Notebook support\n\
- nbformat                # Notebook support\n\
- scipy                   # Notebook support\n\
- python-flatbuffers<2.0  # because tensorflow expects a version before 2\n\
- h5py<3.0                # must be < 3.0 because they changed whether str or byte is
returned\n\
- protobuf>3.12           # Lower protobuf versions do not work with TensorFlow 2\n\
- libiconv                # MDF Reader node\n\
- asammdf=5.19.14         # MDF Reader node\n\
- JPYpe1                  # Databases\n\
' > /tmp/py39_knime.yml
RUN set -x && \
micromamba env create -f /tmp/py39_knime.yml
# END Python Environment Setup
```

Learn more about the KNIME Python Integration with the [KNIME Python Integration Guide](#).



In order for the executor to find the conda installation, the execution context needs to know where to find conda. This is done as a final step and is described [below](#).

Unless modified, the path to the conda installation is `/home/knime/miniconda3/`, and the path to the environment (see below) is `<path to default conda environment dir>=<path to conda installation dir>/envs/<name of the env>`.

In the full images of KNIME Executor version 5.2 and above, where conda and Python are preinstalled, the path to conda is the same, i.e.

`/home/knime/miniconda3/` and the paths to the default environments are `/home/knime/miniconda3/py2_knime` and `/home/knime/miniconda3/py3_knime`.

Build a Docker image from the Dockerfile

Once the Dockerfile has been customized appropriately, you can build a Docker image from it by using the following command after replacing `<image_name>` and `<tag_name>` with actual values:

```
docker build -t <image_name>:<tag_name> .
```

This process can take a few minutes to be completed. In order to check if the new image has been built you can use the command `docker images`.

Push the Docker image to the Docker Embedded Registry

Finally you can push the image to the Docker Embedded Registry.

1. Authenticate against the registry with the credentials obtained from the *KOTS Admin Console > Config > Embedded Registry* via

```
docker login --username <username> registry.<base-url>
```



If TLS is not configured, the registry URL must be added as an **insecure registry**.

2. Tag the previously created image with the format of the Embedded Docker Registry

```
docker tag <old-name> registry.<base-url>/<new_name>
```

3. Push the image to the Embedded Docker Registry

```
docker push registry.<base-url>/<image_name>:<tag_name>
```

4. Now the Docker image (e.g. `registry.hub.example.com/knime-full:5.2-with-additional-extension`) is available to **create an execution context** from the Hub UI.

Push the Docker image to the Container Embedded Registry for air gap installations

For air gap installations you will need to create a custom Docker image and push it to the Container Embedded Registry using `containerd` command line (`ctr`).

As Containerd is installed as container runtime in the cluster, you can make use of the `ctr` commands to pull and push the images into the embedded registry.

1. Build the image on a machine with access to the internet and installed docker:

```
docker build . -t registry.<base-url>/<image_name>:<tag_name>
```

2. Save the Docker image as a tar file on the machine where Docker is installed:

```
docker save -o docker.tar <tag_name>
```

3. Copy the image to the machine where the Hub instance is running
4. On the machine where the Hub instance is running, import the image into containerd:

```
ctr image import docker.tar
```

5. Tag the image:

```
ctr image tag <old-image_name>[<old-tag_name>] registry.<base-url>/<image_name>:<tag_name>
```

6. Push the image to the Container Registry:

```
ctr images push --user knime -k registry.<base-url>/<image_name>:<tag_name>
```

where -k parameter is to skip the TLS check, and --user parameter is to provide the username for the registry.

7. Now you can verify that the images are available on the Container Registry using the below endpoints:

```
http://registry.<base-url>/v2/_catalog  
http://registry.<base-url>/v2/<repo>/tags/list
```

Push the Docker image to a non-embedded Registry

For non-embedded registries you will push the image from your local Docker instance to the remote registry, using the authentication required for that particular registry. Then you can use the image name to create the executor images, given that you have added the correct pull secrets to the KNIME Business Hub configuration.

Python and Conda in Docker images

When you create an Execution Context on KNIME Business Hub based on a **full build** you will have the Python environment bundled with the KNIME Python Integration available. If you need additional libraries or are using the **Python 2 (legacy) extension**, you need to create a custom Python environment to make them available on the Hub instance.

You can do this in several ways:

1. You can use the **Conda Environment Propagation node** in all your workflows using Python. To get started with the **Conda Environment Propagation node**, check out the **KNIME Python Integration Guide**. This has the advantage that no further setup is needed, and you are done with this guide. Any libraries installed using the **Conda Environment Propagation node** will be removed, however, when the executor restarts and are installed again next time the node executes, so libraries that are used often should be installed as part of the executor Docker image to save time. This is described in the following.
2. You can customize the executor image. To do so, you need to create a Docker image with Python, either via the **Executor Image Builder** data application described **above**, or by **creating (Dockerfile examples)**, **building**, and **pushing** the Dockerfile manually. Be sure to note down the paths where conda was installed, as you will need add them in the .epf file of the customization profile during the **set up of the execution context**. The default installation paths are:

```
<path to conda installation dir>      = /home/knime/miniconda3/  
<path to default conda environment dir> = <path to conda installation  
dir>/envs/<name of the env>
```

3. Use an full image of version 5.2 and above, since starting with KNIME Executor version 5.2 the KNIME Python extension is already installed in the Docker images. There are two default environments installed, py2_knime and py3_knime:

- py2_knime:

```

name: py2_knime                # Name of the created environment
channels:                      # Repositories to search for packages
  - defaults
  - conda-forge
dependencies:                  # List of packages that should be installed
  - python=2.7                # Python
  - pandas=0.23               # Table data structures
  - jedi=0.13                 # Python script autocompletion
  - parso=0.7.1               # Jedi dependency this is the last version
compatible with 2.7
  - python-dateutil=2.7       # Date and Time utilities
  - numpy=1.15                # N-dimensional arrays
  - cairo=1.14                # SVG support
  - pillow=5.3                # Image inputs/outputs
  - matplotlib=2.2            # Plotting
  - pyarrow=0.11              # Arrow serialization
  - IPython=5.8               # Notebook support
  - nbformat=4.4              # Notebook support
  - scipy=1.1                 # Notebook support
  - jpype1=0.6.3              # Databases
  - protobuf=3.5              # Serialization for deprecated Python nodes

```

◦ py3_knime:

```

name: py3_knime                # Name of the created environment
channels:                      # Repositories to search for packages
  - defaults
  - conda-forge
dependencies:                  # List of packages that should be installed
  - nbformat=4.4              # Notebook support
  - scipy=1.1                 # Notebook support
  - pillow=5.3                # Image inputs/outputs
  - cairo=1.14                # SVG support
  - ipython=7.1               # Notebook support
  - numpy=1.16.1              # N-dimensional arrays
  - python=3.6                # Python
  - matplotlib=3.0            # Plotting
  - jpype1=0.6.3              # Databases
  - pyarrow=0.11              # Arrow serialization
  - jedi=0.13                 # Python script autocompletion
  - python-dateutil=2.7       # Date and Time utilities
  - pandas=0.23               # Table data structures
  - libiconv=1.15             # MDF Reader node
  - asammdf=5.19.14           # MDF Reader node

```

If you choose to modify the executor image or use the full build of version 5.2 and above, you further need to set up the execution context for it to know where to find the conda/python installations. This is described in the section below.

Set up the execution context

Once you have created the Docker image with Conda/Python and the desired environments, [create an execution context](#) that uses the newly created Docker image.

Now you need to set up and customize the execution context. This process is described in the [KNIME Python Integration Guide](#) in detail, and the relevant parts are repeated here.

You specify the paths where the execution context will find the conda installation and environments in a [customization profile](#) applied it to the execution context.

1. Build the .epf file by following the steps in [KNIME Python Integration Guide](#) and exporting the .epf file. To export the .epf file from KNIME Analytics Platform go to *File > Export Preferences...*
2. Open the file and use only the parts related to Python/conda.

The .epf file could look like the following:

```
/instance/org.knime.conda/condaDirectoryPath=<path to conda installation dir>  
/instance/org.knime.python3.scripting.nodes/pythonEnvironmentType=conda  
/instance/org.knime.python3.scripting.nodes/python2CondaEnvironmentDirectoryPath=<path  
to default conda environment dir>  
/instance/org.knime.python3.scripting.nodes/python3CondaEnvironmentDirectoryPath=<path  
to default conda environment dir>
```

Find more details on how to setup the .epf file in the [Executor configuration](#) section of the [KNIME Python Integration Guide](#).

Now follow these steps to customize the execution context:

1. Build the .zip file containing the [customization profile](#) using the .epf file you just created.
2. Upload the [customization profile](#) .zip file to KNIME Business Hub.
3. Apply the [customization profile](#) to the execution context.

You are done, and can test the setup by running a workflow that contains a [Conda Environment Propagation node](#).

Delete a custom Docker image

You might want to remove the Images that you pushed to the Embedded Docker Registry. This is especially important since the minIO storage allocated for the registry is, by default

limited to ~30 GB.

To do so you can use the following script:

delete_registry_image.sh

```
#!/bin/bash

# exit when any command fails
set -e

registry='registry.<base-url>'

# concatenates all images listed in json file into single line string seperated with
blank
echo "Image Name:"
read images
echo "Image Tag (Space seperated for multiple tags or leave empty if all should be
deleted):"
read tags
echo "Registry User:"
read user
echo "Registry Password:"
read -s password

for image in $images; do

    if [[ -z $tags ]]
    then
        # get tag list of image, with fallback to empty array when value is null
        tags=$(curl --user $user:$password "https://${registry}/v2/${image}/tags/list" |
jq -r '.tags // [] | .[]' | tr '\n' ' ')
    fi

    echo "DELETING image: " $image
    echo "DELETING tags: " $tags

    # check for empty tag list, e.g. when already cleaned up
    if [[ -n $tags ]]
    then
        for tag in $tags; do
            curl --user $user:$password -X DELETE
"https://${registry}/v2/${image}/manifests/${
            curl --user $user:$password -I \
            -H "Accept: application/vnd.docker.distribution.manifest.v2+json" \
            "https://${registry}/v2/${image}/manifests/${tag}" \
            | awk '$1 == "docker-content-digest:" { print $2 }' \
            | tr -d '$\r' \
            )"
            echo "DELETED:" $image "with tag" $tag
        done
    fi
done
```



```

        echo "Deleted images. To free disk space run the garbage collection command
inside the registry pod: 'bin/registry garbage-collect --delete-untagged /
etc/docker/registry/config.yml'"
    else
        echo "SKIP:" $image
    fi
done

```

To run the script you will need:

1. **jq**: **jq** is a lightweight and flexible command line JSON processor that is used to format the JSON output of **curl** calls. To install it on the machine where you want to run the shell script you can use the following command:

```

sudo apt-get update
sudo apt-get -y install jq

```

2. You will need to adapt the value `registry.<base-url>` at the line 6 of the script with the `<base-url>` of your KNIME Business Hub, e.g. for `hub.example.com` will be `registry.hub.example.com`.
3. You will need to know the **Embedded Docker Registry** username and password.



If your KNIME Business Hub instance does not have TLS enabled, the script will cause SSL certificate issues.

To solve this you can:

1. Change the script where a **curl** command is calling an `https://` endpoint to call an `http://` instead, or
2. Add `--insecure` to each line of the script with a **curl** command.

Identify Docker Image names and tags

To be able to run the script you will need to know the image names and tags present on the embedded registry that you want to delete. You can for example run the following **GET** requests against the Docker Registry API. Again you will need to first adapt the `<base-url>` entries to your specific Hub URL, and use your `<username>` and `<password>` for the Embedded Docker Registry.

```

# listing images on the remote registry
$ curl -u <username>:<password> -X GET registry.<base-url>/v2/_catalog | jq

```

This should output a list of the Docker Images available:

```
{
  "repositories": ["executor-image-name1",
                  "executor-image-name2",
                  "executor-image-name3"]
}
```

Then you can run the following command for each Docker Image you are interested in, e.g. `executor-image-name1`, to retrieve the Image tag:

```
# listing tags on the remote registry
$ curl -u <username>:<password> -X GET registry.<base-url>/v2/<executor-image-
name>/tags/list | jq
```

This should output a list of the Docker Image's tags:

```
{
  "name": "executor-image-name1",
  "tags": ["tag1"]
}
```

Run the script

Now you can run the script to delete one or multiple image tags. The script will ask you to provide an Image name, one or more Image tag and the Embedded Docker Registry username and password.

```
$ ./delete-registry-image.sh

Image Name:
<image-name>
Image Tag (Space separated for multiple tags or leave empty if all should be deleted):
<image-tag>
Registry User:
<usr>
Registry Password:
<pwd>
```

Clean up directories and garbage collection

The script will only remove the tags, but the actual file folders remain.

Those need to be manually removed from the minIO storage and can be found in the `minio` pod inside the `minio` namespace under `/data/docker-registry/docker/registry/v2/repositories/`.

Lastly, one needs to run garbage collection on the `registry` pod inside the `kurl` namespace to clean up the disk space using the following command:

```
$ bin/registry garbage-collect --delete-untagged /etc/docker/registry/config.yml
```

Customization profiles

Customization profiles are used to deliver KNIME Analytics Platform configurations from KNIME Hub to KNIME Analytics Platform clients and KNIME Hub executors.

This allows defining centrally managed:

- Update sites
- Preference profiles (such as Database drivers, Python/R settings)

A profile consists of a set of files that can:

- Be applied to the client during startup once the **KNIME Analytics Platform client is configured**. The files are copied into the user's workspace.
- Be applied to the **KNIME Hub executors** of the execution contexts.

Customization profiles can be:

- Global customization profiles that need to be uploaded and managed by the Global Admin. These can be applied across teams via shared execution context or to specific teams.
- Team's customization profiles, which are scoped to the team, can be uploaded either by a Global Admin or a team admin.

Once uploaded, the customization profile can then be downloaded or used in KNIME Analytics Platform clients and executors.



The access to the customization profile is not restricted meaning that anyone with the link can download it and use it.

Currently, customization profiles can be managed on KNIME Hub via REST or using the dedicated Customization Profile data application available [here](#).

Structure of a customization profile

A customization profile minimally consists of a folder, named according to the *profile name*, containing at least one *preference file*. A preference file is a simple text file with the extension `.epf`.

Each line in a preference (`.epf`) file specifies key and value of a setting, separated by `=`.

```
<key1>=<value1>
<key2>=<value2>
# ...
```

If two lines specify identical keys, the value later in the file overrides a value specified earlier.

If the profile folder contains more than one `.epf` files, the files are read in lexicographic order.

A customization profile may contain additional arbitrary files. These are distributed as part of the profile and can be referenced in `.epf` files.

Variable replacement

It is possible to use variables inside the preference files (only those files ending in `.epf`) which are replaced on the client right before they are applied. This makes the Hub-managed customizations even more powerful. These variables have the following format:

`${prefix:variable-name}`. The following prefixes are available:

- **env:** the variable is replaced with the value of an environment value. For example, `${env:TEMP}` will be replaced with `/tmp` under most Linux systems.
- **sysprop:** the variable is replaced with a Java system property. For example, `${sysprop:user.name}` will be replaced with the current user's name. For a list of standard Java system properties see [the JavaDoc](#). Additional system properties can be defined via `-vmargs` in the `knime.ini`.
- **profile:** the variable will be replaced with a property of the profile in which the current preference file is contained in. Currently `location` and `name` are supported as variable names. For example, `${profile:location}` will be replaced by the file system location of the profile on the client. This can be used to reference other files that are part of the profile, such as database drivers:
`org.knime.workbench.core/database_drivers=${profile:location}/db-driver.jar`

In case you want to have a literal in a preference value that looks like a variable, you have to use two dollar signs to prevent replacement. For example ``${env:HOME}` will be replaced with the plain text `${env:HOME}`. If you want to have two dollars in plain text, you have to write three dollars (``${env:HOME}`) in the preference file.



Once you use variables in your preference files, they are not standard Eclipse preference files anymore and cannot be imported as they are.

Create a customization profile

Follow the steps below to create a customization profile. You can export the preference file from a KNIME Analytics Platform installation, with the needed configuration.

Then create a folder with the preference file and any additional file that you might need to distribute with the customization profile. Finally, you compress the folder to a `.zip` format and

1. Set up the needed configuration in a local KNIME Analytics Platform installation.
2. Go to *File* → *Export Preferences* and select a location.
3. Open the created `.epf` file, and look for the lines related to your needed settings. Remove all other settings (as some contain e.g. local paths on your machine, which will inevitably cause issues when applying to another installation). You can also further modify the file with the [customization options](#) below.
4. Place the `.epf` file in a folder, together with any additional files that need to be distributed along the profile (e.g. database drivers).
5. Create a `.zip` from that folder.

Finally you can proceed with the next step, and [upload the file](#) to the KNIME Hub instance.



When creating a zip file on macOS using the built-in functionality, two files are automatically added that cause the next steps (i.e. applying the profile in Analytics Platform) to fail. There is a way to prevent creation of these files if creating the `.zip` via command line, see [here](#). If in doubt, use a Windows or Linux machine to create the `.zip` file.



The customization profiles on the KNIME Hub instance are going to be accessible without user authentication. Therefore, they shouldn't contain any confidential data such as passwords.

For further details and an example on how to distribute JDBC driver files, go to the Hub-managed customization profiles section of the [KNIME Database Extension Guide](#).

Customization options

Besides the preferences that are [exportable by KNIME Analytics Platform](#), there are additional settings that can be added to the preference files to customize clients.

Since KNIME Analytics Platform 5.3, some complex settings can be specified in YAML

format.

1. Create a file `<filename>.yaml` in the **profile directory**.
2. Reference the file in a preference (`.epf`) file by setting the following:

```
/instance/org.knime.core/knime.core.ap-customization-configuration=${profile:location}/<filename>.yaml
```

where `<filename>.yaml` is the name of the YAML file you created.



The YAML file should declare the document version at the beginning of the file, i.e. `version: 'customization-v1.0'`. This is to ensure that the document can still be read in the future even if the format changes.

Restrict access to nodes

The property path `nodes.filter` allows to configure a sequence of *filters* which are evaluated on startup of the KNIME Analytics Platform.

The *scope* of a filter expresses to what extent access is restricted by this filter.

1. *view*: If a node does not match all filters with *view* scope, it can be loaded, configured and executed as part of a workflow, but it will not be presented as a choice in the node repository or similar places.
2. *use*: If a node does not match all filters with *use* scope, it will not be loaded and will not appear as a choice.



use takes over *view*. Meaning that a node that cannot be used can also never be viewed, regardless of whether it matches filters with the *view* scope.

Whether a node matches a filter is defined by its *predicate*, consisting of one or several regular expressions. The regular expression patterns are evaluated against the node factory class name. The value of *rule* (*allow* or *deny*) specifies whether the predicate is applied as-is or inverted.

Examples

- Completely ignore any Java Snippet or Row Filter nodes. Any other nodes are not affected.

```
version: 'customization-v1.0'
nodes:
  filter:
    - scope: use
      rule: deny
      predicate:
        type: pattern
        patterns:
          - .+JavaSnippet.+
          - .+RowFilter.+
        isRegex: true
```

- Completely ignore any Java Snippet node. Restrict node repository and related user interface elements to nodes from given modules.

```
version: 'customization-v1.0'
nodes:
  filter:
    - scope: use
      rule: deny
      predicate:
        type: pattern
        patterns:
          - .+JavaSnippet.+
        isRegex: true
    - scope: view
      rule: allow
      predicate:
        type: pattern
        patterns:
          - org\.<vendor>\.<package>\.+
          - org\.<vendor>\.<package>\.+
        isRegex: true
```

Custom UI menu entries

In the YAML customization file, use the property `ui.menuEntries` as illustrated by the following example.


```
version: 'customization-v1.0'
ui:
  menuEntries:
    - name: "My custom entry"
      link: "https://help.company.com/knime"
    - name: "Another entry"
      link: "https://support.company.com/contact"
```

These entries will appear in the *Help* menu revealed by the button at the top-right of the KNIME Analytics Platform user interface.

To configure custom menu entries in the **classic user interface**, use the following settings in a preference (.epf) file.

`/instance/com.knime.customizations/helpContact.buttonText=<label>`

If set together with `/instance/com.knime.customizations/helpContact.address` a button with the provided label will occur under Help in KNIME Analytics Platform. Clicking on the button will, depending on the `helpContact.address`, either open the default mail client or the default browser with the provided address.

`/instance/com.knime.customizations/helpContact.address=<uri>`

Sets the address of the support contact, e.g. `mailto:support@company` or `https://company/support`.

This option only takes effect in combination with

`/instance/com.knime.customizations/helpContact.buttonText`.

`/instance/com.knime.customizations/documentation.buttonText=<label>`

Sets the label of the documentation button that can be found under Help in KNIME Analytics Platform. Clicking on the button will open the default browser and navigate to the documentation. If set to - the button will be hidden.

`/instance/com.knime.customizations/documentation.address=<uri>`

Sets the address of the documentation, e.g. `https://company/documentation` or `file:///sharedSpace/documentation`.

By default, the documentation address points to the KNIME Analytics Platform documentation.

Restrict which KNIME Hubs the KNIME AI Assistant is allowed to connect to

The `kai.hub.filter` property allows you to configure a sequence of filters that are evaluated on startup. These filters determine which KNIME Hubs can be selected as the backend for K-AI on the KNIME AI Assistant preference page. This is similar to the `nodes.filter` property but with two key differences:

- **Filter target:** The filters match the host URL of a Hub (e.g., `hub.knime.com` for the KNIME Community Hub).
- **Scope:** There is no scope property as the filters only control which hubs K-AI is allowed to connect to.

Examples

- Prevent K-AI from connecting to KNIME Community Hub.

```
version: 'customization-v1.0'
kai:
  hub:
    filter:
      - rule: deny
        predicate:
          type: pattern
          patterns:
            - hub.knime.com
          isRegex: false
```

- Allow only hubs of a certain domain.

```
version: 'customization-v1.0'
kai:
  hub:
    filter:
      - rule: allow
        predicate:
          type: pattern
          patterns:
            - .+\.<custom domain>\.com
          isRegex: true
```

Mountpoints

```
/instance/org.knime.workbench.explorer.view/defaultMountpoint/defaultMountpoints
=<mount id1>,<mount id2>,...
```

A comma separated list of default mountpoints that should be loaded, e.g. LOCAL, EXAMPLES, My-KNIME-Hub. Changes to this list only affects new workspaces, i.e. workspaces which already contain default mountpoints will still contain them even though they haven't been defined here. If this option is absent and defaultMountpoint/enforceExclusion isn't set to true then all default mountpoints will be added. The current default mountpoints are LOCAL, EXAMPLES, and My-KNIME-Hub.

```
/instance/org.knime.workbench.explorer.view/defaultMountpoint/enforceExclusion=<
true|false>
```

If set to true then all default mountpoint not defined by /instance/org.knime.workbench.explorer.view/defaultMountpoint/defaultMountpoints will be removed on start up. Please note that if you want to use this option, the default mountpoints you want to include should **only** be listed in /instance/org.knime.workbench.explorer.view/defaultMountpoint/defaultMountpoints, and **not** in their full definition like when exporting the preferences.epf file from a KNIME Analytics Platform.

Update Sites

```
/instance/com.knime.customizations/updateSite.uris=<uri>,<uri>,...
```

Adds the provided addresses to the update sites.

```
/instance/com.knime.customizations/updateSite.names=<name>,<name>,...
```

The names that are shown under Available Software Sites for the provided update sites. Note that the number of names must match the number of provided URIs.

```
/instance/com.knime.customizations/updateSite.default.disable=<true|false>
```

Disables the default update sites added by KNIME after a fresh installation or update. If a user enables these update sites again they will remain enabled.

```
/instance/com.knime.customizations/updateSite.default.forceDisable=<true|false>
```

Disables the default update sites added by KNIME after a fresh installation or update. If a user enables these update sites again they will be disabled with the restart of their client.

Columnar Backend Memory configuration

The columnar backend makes use of off-heap memory to store data tables. The memory is managed by the columnar backend and is not part of the Java heap (which is configured via the Xmx setting). Therefore, the memory configured for the columnar backend must be taken into account to avoid out-of-memory errors.

Depending on the executor version, different preferences can be set.

KNIME Analytics Platform version 4.7.x

```
/instance/org.knime.core.data.columnar/knime.core.data.columnar.use-  
defaults=<true|false>
```

If true, the other preferences in this section are ignored.

```
/instance/org.knime.core.data.columnar/knime.core.data.columnar.small-cache-  
size=<size>
```

Size of cache for tables smaller than 1MB in MB. Example value: 32.

```
/instance/org.knime.core.data.columnar/knime.core.data.columnar.data-cache-  
size=2048
```

Size of cache for other tables in MB. Example value: 2048.

KNIME Analytics Platform version 5.x

```
/instance/org.knime.core.data.columnar/knime.core.data.columnar.off-heap-  
limit=<size>
```

Total off-heap memory limit in MB. Example value: 2048.

Make sure to configure the memory settings according to the available resources on the executor. Make sure to leave enough memory for the Java heap and other processes running on the executor.



The default configuration for 5.1.0 to 5.1.2 is to use all memory that is not reserved for the Java heap. This configuration is likely to cause the executor to crash with an Out Of Memory Exception. For the default heap size of 60% of the available memory, we recommend setting the off-heap limit to 20% of the available memory.



On executor images before 5.1.2 and 4.7.7, an unfavorable interaction between the JVM and the glibc native memory allocator can cause higher than expected memory usage when using the Columnar Table Backend. Set the environment variable `MALLOC_ARENA_MAX=1` to prevent this issue. Also see, [Columnar Backend High Memory Usage on Linux](#).

Upload a customization profile

After [creating a customization profile](#), you need to upload it to KNIME Business Hub. You can do it [via REST](#) or [via data application](#).

Upload via Data Application

1. If you have not done so already, on KNIME Business Hub, create an [application password](#) for the user uploading the profile.
 - a. For global customization profiles, use a global admin user.
 - b. For team's customization profiles, the user can be either a global admin user or a team admin user.

2. Download the workflow:



Click [here](#) and download the workflow to your KNIME Analytics Platform.

3. Upload the downloaded workflow to your KNIME Business Hub instance via [KNIME Analytics Platform](#).
4. Deploy the workflow as a data application. You can learn more about how to do it [here](#).
5. The first step to begin using the data application is establishing a **connection** with the Hub instance. You must enter your Hub URL and application password in the data app to connect to your KNIME Business Hub instance.

Customization Profile
Hub connection

Hub Credentials

Application password ID

Password

Hub Location

https://your-business-hub.com

Connect to Hub

Could not connect to Hub. Make sure the entered information are correct

Figure 20. The Hub connection step.

6. Select *Upload a New Customization Profile* in the *Action Selection* menu and click *Next*. You can upload multiple customization profiles to your KNIME Business Hub instance.

Customization Profile
Action selection

Please choose the action you wish to perform.

Upload a new customization profile

Figure 21. The upload option is selected in the action selection step.

7. In the next step, select the customization profile **file** previously created, give it a name, and define its scope.
 - a. **Global Admin:** You can choose the customization profile scope if logged in to the Data App as a Global Admin.
 - i. *Global scope:* After being uploaded to KNIME Business Hub, the global customization profile can be applied to a shared or a team execution context.
 - ii. *Team scope:* When a customization profile with team scope is uploaded, it can be applied to the team's executors. It is possible to upload the same customization profile to multiple teams. The Global Admin can upload the customization profile to any team.

Figure 22. Global Admin executing the data app

- b. **Team Admin:** If you're logged in as a team admin, you can only upload the customization profile as a team-scoped type. You can upload the same customization profile for multiple teams. The availability of teams is determined by the permissions of the user who is logged in.
 8. In the Upload Results step, a table displays the results of the customization profile upload operation, along with a legend.
- If everything goes well, the green light means your customization profile has been successfully uploaded to the KNIME Business Hub. You can now apply it to a **KNIME Analytics Platform installation** or to a **KNIME Business Hub executor**.
9. **Error Handling:** The data application is designed to handle two types of errors:
 - a. Missing customization profile file.

Figure 23. This error occurs when no customization profile file is provided.

- b. No team selection (for team-scoped customization profiles).

If you encounter an error message, click *Next* and select the *Turn back to the*

choose *action menu* option. Repeat the operation, fixing the error.



Figure 24. Turn back to the action menu and repeat the operation.

10. Click *Next* to finish the operation. You can return to the *Action Selection* menu to perform additional actions or close the data application directly.

Upload via REST request

1. If you have not done so already, on KNIME Business Hub, create an **application password** for the user uploading the profile.
 - a. For global customization profiles, use a global admin user.
 - b. For team's customization profiles, the user can be either a global admin user or a team admin user.
2. Send a POST request to `https://api.<base-url>/execution/customization-profiles` with the following set up:
 - a. Authorization: select Basic Auth, using username and password from the created application password
 - b. Body: select form-data as request body type and add the following entries:
 - i. Add a new key, set content to "File". Name of the key needs to be "content". The value of the key is the .zip file containing the profile, and the content type is `application/zip`.
 - ii. Add a new key, set content to "Text". Name of the key needs to be "metadata".

A. The value of the key is:

For global customization profiles enter:


```
{
  "name": "<profile_name>",
  "scope": "hub:global"
}
```

For team's customization profiles you first need to obtain the `<team_ID>` of the team you want to upload the customization profile to. To do so you can use the following GET request:

```
GET api.<base-url>/accounts/identity
```

You will find the `<team_ID>` in the body response under `teams`:

```
...
  "teams": [
    {
      "id": "account:team:<team_ID>",
      "name": "<team_name>",
      ...
    }
  ]
...
```

Then the value of the key is:

```
{
  "name": "<profile_name>",
  "scope": "account:team:<team_ID>"
}
```

- B. Set the content type for the second key to `application/json`
 - c. When using Postman there is no need to manually adjust the headers
3. Send the request

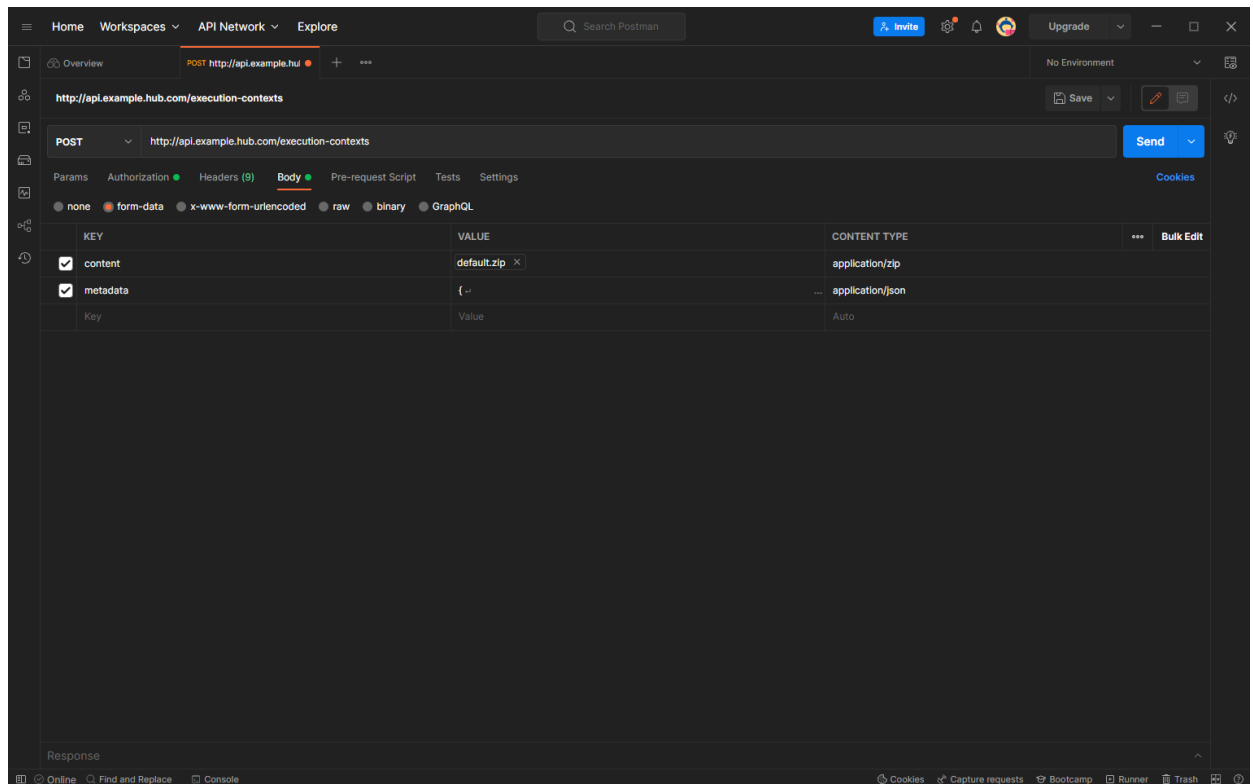


Figure 25. Set up Postman for a REST call to upload a customization profile to a KNIME Hub instance

- If successful, you will receive a 201 status response. Make note of the created `<profile_ID>`, as this will be used to refer to the profile when requesting it.



You can refer to the API documentation at the following URL for more details about the different calls you can make to the Customization Profiles endpoint.

`http://api.<base-url>/api-doc/execution/#/Customization%20Profiles`

Apply a customization profile

Apply a customization profile to KNIME Hub executor

Apply via Data App

To apply a customization profile to all executors running in a KNIME Business Hub **execution context**, we can use the data application. However, the type of user logged in affects the operations that can be performed. Refer to the table below for a comprehensive overview.

Table 1. Apply customization profile: user rights

User type	Eligible customization profile	Customization profile type	Eligible Execution Context
Global Admin	All uploaded within the KNIME Business Hub instance	Global	Shared and any team specific execution context
		Team-scoped	Any team execution contexts
Team admin	Only those uploaded in teams in which the user has team admin rights	Team-scoped only	Only the team execution contexts where the customization profile was uploaded. Shared execution contexts are not eligible

To provide a better understanding of the table, here are some examples to demonstrate its functionality:

- A Global Admin can choose one team-scoped customization profile and apply it to any team-scoped execution context within the KNIME Business Hub instance. For instance, the Global Admin can apply *Team A's customization profile* to the execution context of *Team B*, i.e., execution context B.1.
- A Global Admin can also select a **Global** customization profile and apply it to any shared and team-scoped execution context within the KNIME Business Hub instance.
- A team admin can **only** choose team-scoped customization profiles uploaded within the teams with admin rights. For example, they can only apply a customization profile uploaded in *Team A* within the Team A execution contexts.

1. Learn how to download the data app from Community Hub, upload and deploy it in KNIME Business Hub, and authenticate with your application password in the [Upload a customization profile](#) section.
2. Select *Apply an existing Customization Profile* in the *Action Selection* menu to apply a Customization Profile.
3. Choose the desired customization profile from the table and click *Next*. In the table, if

the *Team name* column has a value of *Any*, the customization profile has a global scope and can be applied to any team.

Customization Profile
Action selection

Please choose the action you wish to perform.

Apply an existing customization profile

Select one of the customization profiles that already exists
The customization profile can be applied to a KNIME Business Hub Executor or a KNIME Analytics Platform client.

Show 5 entries Clear Sorting

	Custom profile name	Custom profile type	File uploaded	Created at	Updated at	Team name
<input type="radio"/>	Python profile	Team	windows.zip	2023-11-08	2023-11-08	Dev Team
<input type="radio"/>	Python profile	Team	windows.zip	2023-11-08	2023-11-08	Data Science Team
<input checked="" type="radio"/>	DB configuration	Global	default.zip	2023-11-08	2023-11-08	Any

Previous 1 Next

Filter teams

Excludes

No entries in this list

Includes

- Dev Team
- Data Science Team
- Any

Customization profile scope

☒ Global ☐ Team

Figure 26. A Global Admin could select a global or team-scoped customization profile.



It is only possible to apply one customization profile at a time. To apply multiple customization profiles, repeat the operation.


- When you reach the *Apply customization profile* step, choose the option *Apply one customization profile to KNIME Hub Executor*. You'll see a table that shows the available execution contexts based on your user type and the previously selected customization profile scope.



Applying a new customization profile with the same name as an existing one to an execution context causes an internal error. Check the "Existing customization profiles name" column to avoid this.

Select one or more execution contexts from the table where you want to apply the customization profile and click *Next*.

Customization Profile
Apply customization profile



What do you want to do next?

☐ Apply one customization profile to KNIME Analytics Platform client
☒ Apply one customization profile to KNIME Hub executor
☐ None of the above. I am fine for now.

Select to which execution contexts apply the customization profile.

Since the customization profile is team-based, it can only be applied to team-scoped execution contexts.

<input type="checkbox"/>	Team name	Execution context name	Execution context scope	Disabled	Existing customization profiles name
<input type="checkbox"/>	Dev Team	4.7.x stable	Team	true	Missing
<input type="checkbox"/>	Dev Team	Moritz local executor	Team	true	Missing
<input type="checkbox"/>	Dev Team	QA-5.1.1	Team	false	Missing
<input type="checkbox"/>	Dev Team	official-nightly	Team	false	Missing
<input type="checkbox"/>	Dev Team	test EC for docs	Team	false	Missing

Warning: When a new customization profile is added to an execution context with existing ones, it is attached to the execution context along with the existing ones.

Filter by teams
Dev Team

☒ Include disabled execution contexts


Previous 1 Next

Figure 27. The team admin can apply a customization profile uploaded to the Dev Team to the team-scoped execution contexts.

- In the *Application Results* step, a table displays the results of the customization profile application operation, along with a legend.



If everything goes well, the green light indicates that your customization profile has been successfully applied to KNIME Business Hub executors for the selected execution contexts.

Customization Profile
Application results



Customization profile application results

The customization profile "Python profile" has been applied with Team scope to the following execution contexts:

	Team name	Execution context name	Execution context scope	Results
	Dev Team	QA-5.1.1	Team	The customization profile has been applied to the execution context
	Dev Team	official-nightly	Team	The customization profile has been applied to the execution context



Result legend
 The customization profile has been applied to the execution context
 It has not been possible to apply the customization profile to the selected execution contexts. See the results column for further details

Figure 28. The team admin has applied the Python profile to two different execution contexts for the same team.

- Error Handling:** The data application handles two types of errors for the application branch.:
 - No customization profiles were uploaded to the KNIME Business Hub.

- b. Attempting to apply a customization profile to an execution context with a customization profile with the same name.

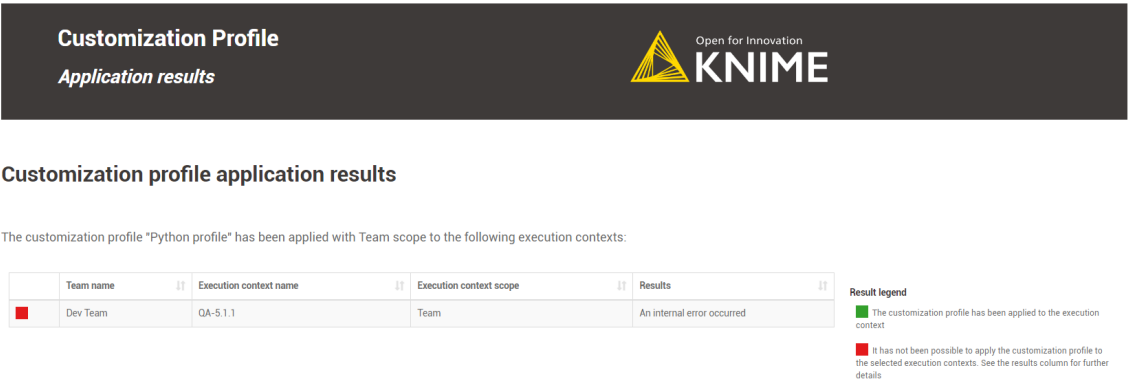


Figure 29. A view of the error.

- c. No customization profile was selected.
- d. When no execution contexts were chosen to apply the customization profile.

If you encounter an error message, click *Next* and select the *Turn back to the choose action menu* option. Repeat the operation, fixing the error.



Figure 30. Turn back to the action menu and repeat the operation.

- 7. Click *Next* to finish the operation. You can return to the *Action Selection* menu to perform additional actions or close the data application directly.

Apply via REST request

In order to apply a customization profile to all executors running in a KNIME Business Hub **execution context**, you will need to send a request to the execution context endpoint.

First you need to get the execution context ID. To do so you can use the following GET request to get a list of all the execution contexts that are owned by a specific team:

```
GET api.<base-url>/execution-contexts/account:team:<team_ID>
```



If you are a global admin you can also GET a list of all the execution contexts available on the Hub instance with the call `GET api.<base-url>/execution-contexts/`.

Now you can apply the new customization profile to the selected execution context.

You will need to obtain the `<profile_ID>` using the following GET request:

1. For global customization profiles:

```
GET api.<base-url>/execution/customization-profiles/hub:global
```

2. For team's customization profiles:

```
GET api.<base-url>/execution/customization-profiles/account:team:<team_ID>
```



Refer to the [above section](#) to find out how to get the `<team_ID>`.

Then you need to update the execution context by using the following PUT request:

```
PUT api.<base-url>/execution-contexts/<execution-context_ID>
```

You need to select **Body** > **raw** > **JSON** and add the following to the request body:

```
{
  "customizationProfiles": [
    "<profile_ID>"
  ]
}
```

This will cause a restart of all executor pods of this execution context, after which the profile will be applied.



At present, this will also terminate all jobs currently running on the executor.

Update a customization profile

It is possible to update customization profiles uploaded to KNIME Business Hub. This can be done even if the customization profile *has already been applied* to the KNIME Business executor via execution context. You can update two features:

1. The customization profile **name**.
2. The customization profile zip file can be overwritten. Refer to the [create a customization profile](#) section to learn how to make one.

Update via Data Application

Users can use the customization profile data app to **update** customization profiles previously uploaded to the KNIME Business Hub.

Depending on the user's role as a Global Admin or a Team Admin, they can access and update specific customization profiles:

- **Global Admin:** can **update** all uploaded customization profiles within the current KNIME Business Hub instance, either team or global-scoped customization profiles.
- **Team Admin:** can only update team-scoped customization profiles from their own teams.

-
1. Learn how to download the data app from Community Hub, upload and deploy it in KNIME Business Hub, and authenticate with your application password in the [Upload a customization profile](#) section.
 2. Select *Update an existing Customization Profile* in the *Action Selection* menu to update a Customization Profile. Choose the desired customization profiles from the table and click *Next*.

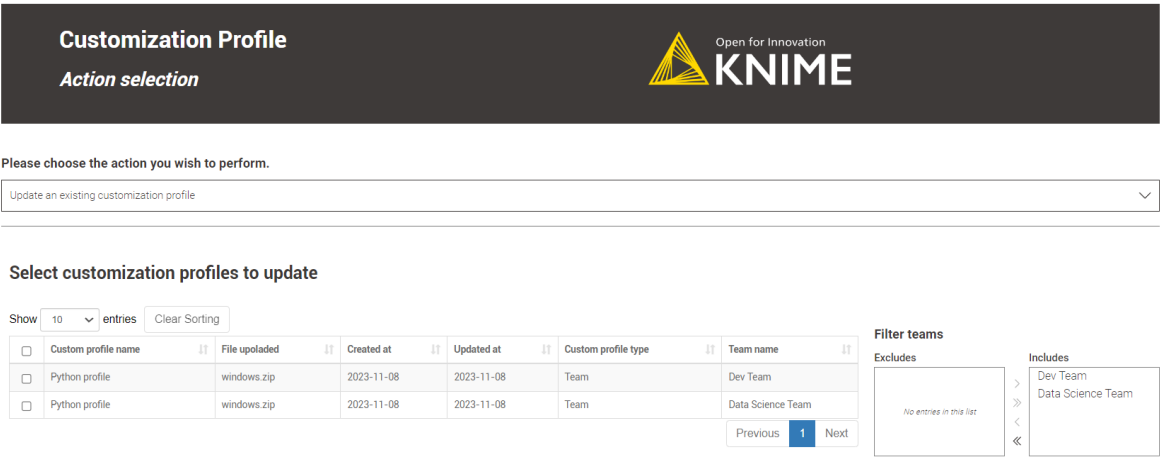


Figure 31. A team admin could select only team-scoped customization profiles.



You can choose to update multiple customization profiles at the same time.

3. In the *Update Customization Profile* step, you can change the customization profile name by **double-clicking** the corresponding table cell and uploading a new customization profile to overwrite the existing one.

Refer to the "File uploaded" column for the currently assigned customization profile file.

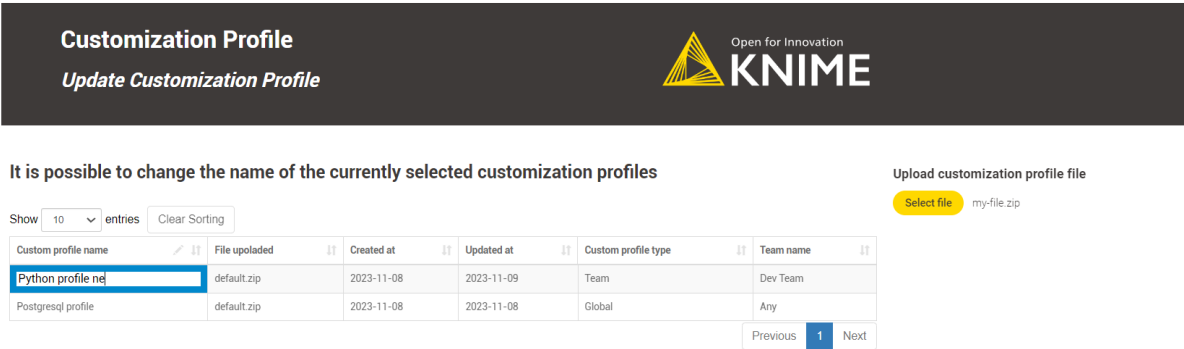


Figure 32. A Global Admin updating two customization profiles at once.




Updating multiple customization profiles at once is possible, but it's important to note that you can only upload a single customization profile file for all the customization profiles. Although each customization profile can be renamed, they will all share the same customization profile file.

4. In the *Update Results* step, a table displays the results of the customization profile updating operation, along with a legend.

If everything goes well, the green light indicates that your selected customization profiles have been successfully updated with new names and a new customization profile file.


Customization Profile

Update results




Customization profile updated details

The updated customization profiles will be automatically applied to execution contexts or KNIME Analytics Platform clients using it.

	Customization profile name	Uploaded file name	Created at	Updated at	Results
	Python profile data team	default.zip	2023-11-08 GMT	2023-11-09 GMT	The customization profile has been successfully updated.

Result legend

 The customization profile has been successfully updated


 It has not been possible to update the customization profile. See the results column for further details

Figure 33. The outcome of updating two customization profiles.




The updated customization profiles will be automatically applied to execution contexts or KNIME Analytics Platform clients using it.

5. **Error Handling:** The data application handles two types of errors for the update option:
- a. An error will occur if the user does not upload a new customization profile file during the *Update Customization Profile* step.

Customization Profile

Update results



Customization profile updated details

An error occurred: No .zip file was uploaded. Click "Next" to return to the action selection menu.

Figure 34. A view of the error.

- b. No customization profiles were selected in the *Update Customization Profile* step.

If you encounter an error message, click *Next* and select the *Turn back to the choose action menu* option. Repeat the operation, fixing the error.



Figure 35. Turn back to the action menu and repeat the operation.

6. Click *Next* to finish the operation. You can return to the *Action Selection* menu to perform additional actions or close the data application directly.

Update via REST request

Updating a customization profile is like replacing an existing profile with a new file and name.

If you want to update a customization profile via REST request, the process is similar to the [uploading process](#). The only difference is that instead of a POST Request, you need to perform a **PUT Request** and specify the ID of the customization profile.

1. If you have not done so already, on KNIME Business Hub, create an **application password** for the user uploading the profile.
 - a. For global customization profiles, use a global admin user.
 - b. For team's customization profiles, the user can be either a global admin user or a team admin user.
2. To begin, you will need to get the list of all uploaded customization profiles on KNIME Business Hub:

You can obtain the <profile_ID> using the following GET request:

For global customization profiles:

```
GET api.<base-url>/execution/customization-profiles/hub:global
```

For team's customization profiles:

```
GET api.<base-url>/execution/customization-profiles/account:team:<team_ID>
```



Refer to the [above section](#) to learn how to get the <team_ID>.

3. **Updating** a customization profile is similar to uploading it via a REST Request. However, unlike uploading, we only need to provide the name and file of the customization profile for updating. So, we don't need to provide the scope as it remains the same.

- a. Send a PUT request to `https://api.<base-url>/execution/customization-profiles/<customization-profile-ID>` with the following set up:
- b. Authorization: select Basic Auth, using username and password from the created application password
- c. Body: select form-data as request body type and add the following entries:
 - i. Add a new key, set content to "File". Name of the key needs to be "content". The value of the key is the .zip file containing the profile, and the content type is application/zip.
 - ii. Add a new key, set content to "Text". Name of the key needs to be "metadata".
 - A. The value of the key is the same for global and team-scoped customization profiles:

```
{  
  "name": "<profile_name>"  
}
```

- B. Set the content type for the second key to application/json

- d. When using Postman there is no need to manually adjust the headers

4. Send the request

Detach a customization profile

It's important to know that detaching a customization profile is not the same as deleting it. When you detach a customization profile, it isn't removed from KNIME Business Hub. Instead, it just means that the customization profile won't be applied to the KNIME Analytics Platform or the KNIME Business executors.

However, the customization profile is still available in KNIME Business Hub, so it can be reused again whenever needed.

Detach a customization profile from a KNIME Business Hub executor

Detaching a customization profile applies **only** to those customization profiles applied to a KNIME Business Hub executor via execution context. Separating a customization profile from its execution context is the prerequisite step to deleting a customization profile from a KNIME Business Hub instance.

Detaching a customization profile from an execution context can also be done if the user no longer wants to apply the customization to the executors.

Detach via Data Appliation

The data application allows users to **detach** customization profiles applied to execution contexts in KNIME Business Hub.

For instructions on how to apply a customization profile to an execution context, [refer to this section](#).

The customization profiles available for detachment depend on the user type:

- **Global Admin:** can **detach** all applied customization profiles within the current KNIME Business Hub instance, either team or global-scoped customization profiles.
- **Team Admin:** can only detach team-scoped customization profiles from their own teams.
 1. Learn how to download the data app from Community Hub, upload and deploy it in KNIME Business Hub, and authenticate with your application password in the [Upload a customization profile](#) section.
 2. Select *Detach a customization profile from an execution context* in the *Action Selection* menu to detach a customization profile. Choose the desired customization profiles from the table and click *Next*.

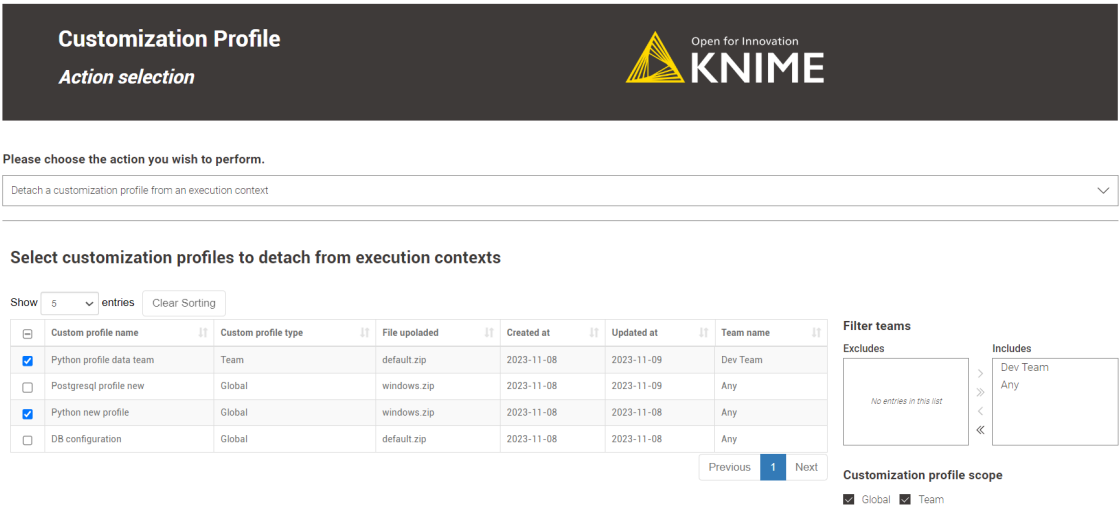


Figure 36. A Global admin is able to detach either team or global-scoped customization profiles.

i You can choose to detach multiple customization profiles at the same time.

- 3. Once you click on *Next*, a table will be displayed showing all the execution contexts where the selected customization profiles have been applied.
- 4. At this point, you can choose multiple execution contexts to detach the customization profile.
- 5. Notice that for execution contexts with `global` scope, all teams where they are in use are listed in the column *Team name*. By detaching the customization profile from such an execution context, you will detach it from all the teams where the execution is being applied.

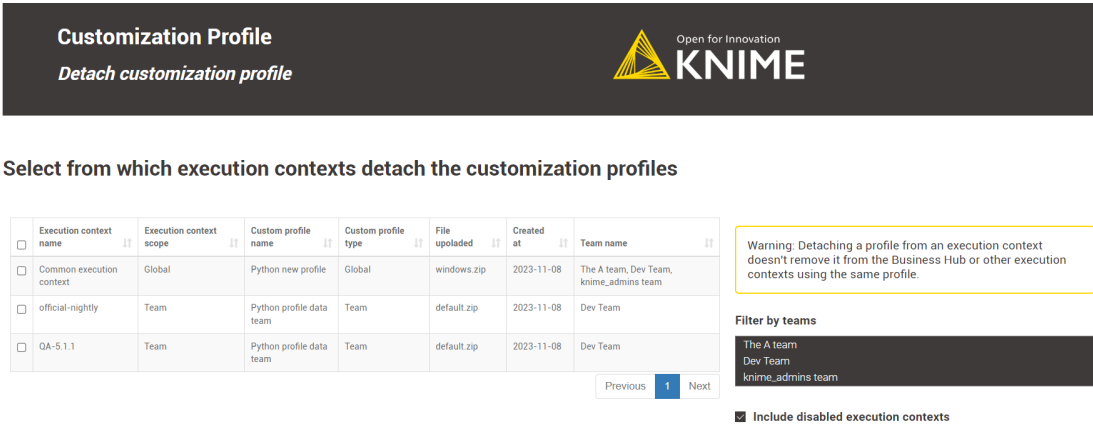


Figure 37. Here's an example of a global execution context shared between three teams.

6. After you perform the *Detach Results* step, a table will appear showing you the customization profile detach operation results.

If everything goes well, the green light indicates that your selected customization profiles have been successfully detached from the selected execution contexts.

Customization Profile							
Detach results							
Customization profile detached from the following execution contexts							
Execution context name	Execution context scope	Team name	Custom profile name	Custom profile type	File uploaded	Created at	Results
Common execution context	Global	The A team, Dev Team, knime_admins team	Python new profile	Global	windows.zip	2023-11-08	The customization profile has been detached from the execution context
QA automation	Team	QA automation team	DB configuration	Global	default.zip	2023-11-08	The customization profile has been detached from the execution context

Result legend

■ The customization profile has been detached from the execution context

■ It has not been possible to detach the customization profile from the selected execution contexts. See the results column for further details

Figure 38. The outcome of detaching two customization profiles.



Detaching a customization profile from an execution context doesn't remove it from the Business Hub or other execution contexts using the same profile.

7. **Error Handling:** The data application handles three types of errors for the detach option:
- An error will occur if no customization profiles are applied to any KNIME Business Hub execution context. In this case, you must select the option to **Apply an existing customization profile**.
 - An error is raised if the user:
 - Does not select any customization profile to detach.
 - If there are no execution contexts selected from where to detach the customization profiles.



Figure 39. A view of one of the possible errors.

If you encounter an error message, click *Next* and select the *Turn back to the choose action menu* option. Repeat the operation, fixing the error.



Figure 40. Turn back to the action menu and repeat the operation.

8. Click *Next* to finish the operation. You can return to the *Action Selection* menu to perform additional actions or close the data application directly.

Detach via REST request

You can detach a customization profile from a KNIME Business Hub execution context, which is the inverse of applying it. The steps for detaching a customization profile are similar to applying one.

To detach a customization profile from all executors running in a KNIME Business Hub **execution context**, you must send a request to the execution context endpoint, not including the customization profile ID that you want to detach.

1. If you have not done so already, on KNIME Business Hub, create an **application password** for the user uploading the profile.
 - a. For global customization profiles, use a global admin user.

- b. For team's customization profiles, the user can be either a global admin user or a team admin user.
2. First, you need to get the execution context ID. To do so, you can use the following GET request to get a list of all the execution contexts that are owned by a specific team:

```
GET api.<base-url>/execution-contexts/account:team:<team_ID>
```



If you are a Global Admin you can also GET a list of all the execution contexts available on the Hub instance with the call GET api.<base-url>/execution-contexts/.

3. Retrieve the existing customization profiles in the execution context from the above Get Request response. Look for a key in the JSON body similar to:

```
"customizationProfiles" : [ "<customization-profile-ID_1>",<customization-profile-ID_2>" ]
```

4. Now, you can detach the target customization profile from the selected execution context. To do so, you need to update the execution context by using the following PUT request:

```
PUT api.<base-url>/execution-contexts/<execution-context_ID>
```

5. To detach a customization profile, e.g. <customization-profile-ID_1>, from the target execution context, follow these steps. Select Body > raw > JSON and ensure you do not include the customization profile you wish to remove. Use the syntax of the request body shown below:

```
{
  "customizationProfiles": [
    "<customization-profile-ID_2>"
  ]
}
```

6. If the target execution context has only **one** customization profile attached, you can detach it by doing an empty request.

```
{
  "customizationProfiles": []
}
```

Delete a customization profile

Deleting a customization profile from KNIME Business is a straightforward operation, and you can do it either through a REST request or the data application. Please follow the step-by-step guide below to understand how it works.

Please note that the type of user determines which customization profiles they can delete:

- **Global Admin:** can **delete** all customization profiles within the current KNIME Business Hub instance, either team or global-scoped customization profiles.
- **Team Admin:** can only **delete** team-scoped customization profiles from their own teams.



Deleting a customization profile from KNIME Business Hub requires first **detaching** it from any execution context where it was applied.

Please refer to the [Detach a customization profile from a KNIME Business Hub executor](#) section to understand how to detach a customization profile.

Delete via Data Application

1. Learn how to download the data app from Community Hub, upload and deploy it in KNIME Business Hub, and authenticate with your application password in the [Upload a customization profile](#) section.
2. Select *Delete a customization profile from your Business Hub instance* in the *Action Selection* menu to delete a customization profile. Choose the desired customization profiles from the table and click *Next*.

Customization Profile
Action selection

Please choose the action you wish to perform.

Delete a customization profile from your Business Hub instance

Select customization profiles to delete

Show 5 entries Clear Sorting

<input checked="" type="checkbox"/>	Customization profile name	Customization profile type	File uploaded	Created at	Updated at	Team name
<input checked="" type="checkbox"/>	Python profile data team	Team	default.zip	2023-11-08	2023-11-09	Dev Team

Previous 1 Next

Filter teams

Excludes

Includes

Dev Team

No entries in this list

Figure 41. Team admins can only delete customization profiles from teams they are admin of.



You can choose to delete multiple customization profiles at the same time.

- As deleting is a delicate operation, in the next step, we offer a preview of the selected customization profiles to be deleted to ensure the user is performing the desired action.

Customization Profile
Discard Customization Profiles

Below are the custom profiles selected for deletion

Click "Next" to confirm deletion

Show entries

Customization profile name	Customization profile type	File uploaded	Created at	Updated at	Team name
Python profile data team	Team	default.zip	2023-11-08	2023-11-09	Dev Team

Previous
1
Next

Figure 42. Preview of the selected customization profile.



Clicking *Next* will delete the customization profile directly.

- The *Discard results* section displays a table with a legend indicating the success or failure of deleting a customization profile. Green means success, red means failure, and orange means you need to detach the customization profile from the execution contexts first.

Customization Profile
Discard results

Discarded customization profiles

Customization profile name	Customization profile type	File uploaded	Created at	Updated at	Results
Postgresql profile new	Global	windows.zip	2023-11-08	2023-11-09	The customization profile has been discarded

Previous
1
Next

Result legend


- The customization profile has been discarded
- It has not been possible to discard the customization profile. See the results column for further details
- It has not been possible to discard the customization profile. It is already attached to an execution context

Figure 43. The deletion of a customization profile from KNIME Business Hub was successful.


- Error Handling:** The data application handles two types of errors for the delete option:
 - If the user doesn't select any customization profile.

- b. When deleting a customization profile still attached to an execution context, reference the [Detach a customization profile from a KNIME Business Hub executor](#) section for resolution.




Customization Profile
Discard results



Discarded customization profiles

	Customization profile name	Customization profile type	File uploaded	Created at	Updated at	Results
	Python profile data team	Team	default.zip	2023-11-08	2023-11-09	The customization profile is attached to an execution context. Please return to the menu and detach it before deleting it.

Result legend

-  The customization profile has been discarded
-  It has not been possible to discard the customization profile. See the results column for further details
-  It has not been possible to discard the customization profile. It is already attached to an execution context

Previous
1
Next

Figure 44. A view of one of the possible errors.

If you encounter an error message, click *Next* and select the *Turn back to the choose action menu* option. Repeat the operation, fixing the error.

Customization Profile
Action selection



Please choose the action you wish to perform.

☒ Turn back to the choose action menu
☐ I'm ok, I want to close the data application

Figure 45. Turn back to the action menu and repeat the operation.

6. Click *Next* to finish the operation. You can return to the *Action Selection* menu to perform additional actions or close the data application directly.

Delete via REST request

Deleting a customization profile from KNIME Business Hub is possible via a REST request.

Below are the steps to accomplish this:

1. If you have not done so already, on KNIME Business Hub, create an [application password](#) for the user uploading the profile.

- a. For global customization profiles, use a global admin user.
 - b. For team's customization profiles, the user can be either a global admin user or a team admin user.
2. To start, you need to retrieve the list of the uploaded customization profiles to KNIME Business Hub:

You can obtain the <customization_profile_ID> using the following GET request:

For global customization profiles:

```
GET api.<base-url>/execution/customization-profiles/hub:global
```

For team's customization profiles:

```
GET api.<base-url>/execution/customization-profiles/account:team:<team_ID>
```



Refer to the [above section](#) to find out how to get the <team_ID>.

3. Once you have the <customization-profile-ID> that you want to delete, perform a DELETE Request.
 - a. Send a DELETE request to `https://api.<base-url>/execution/customization-profiles/<customization-profile-ID>` with the following set up:
 - i. Authorization: select Basic Auth, using username and password from the created application password

After a successful deletion, you will receive a 20* status code.

Advanced configuration

This section covers some of the configuration settings that are available for your KNIME Business Hub instance.

The following configurations are available in the KOTS Admin Console and can be changed after the installation and first minimal configuration steps are concluded successfully.

You can access the KOTS Admin Console via the **URL and password** you are provided in the output upon installation.

Configure networking

In the "Networking" section of the KOTS Admin Console you can:

- Deploy an external load balancer for traffic ingress: this feature takes effect only if your cloud provider and kubernetes distribution support automatic load balancer provisioning.
- Enable Transport Layer Security (TLS): the encryption protocol that provides communications security is highly recommended especially for KNIME Business Hub instances deployed in a production environment.



Please, be aware that if TLS is not enabled some HTTPS-only browser's features will not be available. For example, it will not be possible for a user to copy generated **application passwords**.

- Enable advanced ingress configuration: you can customize the ingress proxy behavior, for example configuring the read/send/connect timeouts.

Networking

Configuration for external load balancer and TLS.

☐ **Deploy Load Balancer**

Deploy an external load balancer. Your cloud provider and kubernetes distribution (e.g., AWS EKS or Azure AKS) must support automatic load balancer provisioning in order for this feature to take effect. See [kubernetes documentation](#) for more.

☐ **Enable TLS** Recommended

Enable Transport Layer Security (TLS). This option is highly recommended for any KNIME Business Hub deployed in a production environment. A certificate must be created for all URLs configured above, including a wildcard certificate for `hub.example.com` and `*.hub.example.com`.

☐ **Enable Advanced Ingress Configuration**

Customize the ingress proxy behavior such as read/send/connect timeouts. Changes to these settings require a restart of the `ingress-nginx-controller` pod before taking effect.

☐ **Enable Custom Certificate Authority (CA) Certificate**

Enable the addition of a custom CA certificate. Some organizations may use their own CA, and adding it here will allow certain KNIME Business Hub services to communicate with external resources that require a custom CA.

Configure TLS

If you enable the Transport Layer Security (TLS) you need to have a certificate that is valid for all the **URLs defined during the installation**. We recommend to create a wildcard certificate for `<base-url>` and `*.<base-url>`, e.g. `hub.example.com` and `*.hub.example.com`.

Check *Enable TLS* in the "Networking" section of the KOTS Admin Console.

- **Upload your own certificate:** Select *Upload your own certificate* to be able to upload the certificate files.

You will need an unencrypted private key file and a certificate file that contains the full certificate chain. In the certificate chain the server certificate needs to be the first in the PEM file, followed by the intermediate certificate(s). You usually can get a certificate from your company's IT department or Certificate Authority (CA).

Another possibility, if you have a public domain name, is to use letsencrypt to obtain a certificate.

Both certificates need to be PEM formatted as requested by the `ingress-nginx-controller` (see the relevant documentation [here](#)).

Networking

Configuration for external load balancer and TLS.

☐ Deploy Load Balancer

Deploy an external load balancer. Your cloud provider and kubernetes distribution (e.g., AWS EKS or Azure AKS) must support automatic load balancer provisioning in order for this feature to take effect. See [kubernetes documentation](#) for more.

☒ Enable TLS Recommended

Enable Transport Layer Security (TLS). This option is highly recommended for any KNIME Business Hub deployed in a production environment. A certificate must be created for all URLs configured above, including a wildcard certificate for `hub.example.com` and `*.hub.example.com`.

Certificate Authority

Select the TLS certificate authority to use for KNIME Business Hub.

☒ Upload your own certificate ☐ Existing TLS Secret ☐ AWS ACM Certificate

Private Key File

The private key file should be pem formatted.

Upload a file

 Browse files for Private Key File

Certificate File

The certificate file should be the full certificate chain in pem format.

Upload a file

 Browse files for Certificate File

☐ Enable Advanced Ingress Configuration

Customize the ingress proxy behavior such as read/send/connect timeouts. Changes to these settings require a restart of the `ingress-nginx-controller` pod before taking effect.

☐ Enable Custom Certificate Authority (CA) Certificate

Enable the addition of a custom CA certificate. Some organizations may use their own CA, and adding it here will allow certain KNIME Business Hub services to communicate with external resources that require a custom CA.

- **Existing TLS Secret:** Select *Existing TLS Secret* to specify the name of of an existing Secret of type `kubernetes.io/tls` in the `knime` namespace. It needs to have keys `tls.crt` and `tls.key`, which contain the PEM formatted private key and full chain certificate.

This option is recommended if you have an automatic process that can create and renew `kubernetes.io/tls` Secrets in the cluster, like the [cert-manager project](#).

See [ingress-nginx](#) and [kubernetes documentation on TLS secrets](#) for more details.

Networking

Configuration for external load balancer and TLS.

☐ Deploy Load Balancer

Deploy an external load balancer. Your cloud provider and kubernetes distribution (e.g., AWS EKS or Azure AKS) must support automatic load balancer provisioning in order for this feature to take effect. See [kubernetes documentation](#) for more.

☒ Enable TLS Recommended

Enable Transport Layer Security (TLS). This option is highly recommended for any KNIME Business Hub deployed in a production environment. A certificate must be created for all URLs configured above, including a wildcard certificate for `hub.example.com` and `*.hub.example.com`.

Certificate Authority

Select the TLS certificate authority to use for KNIME Business Hub.

☐ Upload your own certificate ☒ Existing TLS Secret ☐ AWS ACM Certificate

Existing TLS Secret

Specify the name of an existing Secret of type `kubernetes.io/tls` in the `knime` namespace. It needs to have keys `tls.crt` and `tls.key`. See [ingress-nginx](#) and [kubernetes documentation](#) for more. This option is recommended if you have an automatic process that can create and update `kubernetes.io/tls` Secrets in the cluster.

business-hub-crt-secret

☐ Enable Advanced Ingress Configuration

Customize the ingress proxy behavior such as read/send/connect timeouts. Changes to these settings require a restart of the `ingress-nginx-controller` pod before taking effect.

☐ Enable Custom Certificate Authority (CA) Certificate

Enable the addition of a custom CA certificate. Some organizations may use their own CA, and adding it here will allow certain KNIME Business Hub services to communicate with external resources that require a custom CA.

- Select *AWS ACM Certificate* if, instead, you have deployed an AWS Elastic Load Balancer (ELB). In this case you can use AWS Certificate Manager (ACM) and set the certificate as an annotation directly on the loadbalancer. You can find more information in AWS documentation for ACM [here](#).

Once you obtained the certificate Amazon Resource Name (ARN) in the form `arn:aws:acm:<region>:<account-id>:certificate/<certificate-id>`, insert the ARN in the corresponding field as shown in the image below.

Networking

Configuration for external load balancer and TLS.

☐ Deploy Load Balancer

Deploy an external load balancer. Your cloud provider and kubernetes distribution (e.g., AWS EKS or Azure AKS) must support automatic load balancer provisioning in order for this feature to take effect. See [kubernetes documentation](#) for more.

☒ Enable TLS Recommended

Enable Transport Layer Security (TLS). This option is highly recommended for any KNIME Business Hub deployed in a production environment. A certificate must be created for all URLs configured above, including a wildcard certificate for `hub.example.com` and `*.hub.example.com`.

Certificate Authority

Select the TLS certificate authority to use for KNIME Business Hub.

☐ Upload your own certificate ☐ Existing TLS Secret ☒ AWS ACM Certificate

AWS Certificate Manager ARN

When deploying in an existing AWS EKS cluster, and selecting the loadbalancer option above, you can attach a certificate from the AWS Certificate Manager to the loadbalancer here. Set the certificate ARN below in the format: `arn:aws:acm:<region>:<account-id>:certificate/<certificate-id>`

`arn:aws:acm:<region>:<account-id>:certificate/<certificate-id>`

☐ Enable Advanced Ingress Configuration

Customize the ingress proxy behavior such as read/send/connect timeouts. Changes to these settings require a restart of the `ingress-nginx-controller` pod before taking effect.

☐ Enable Custom Certificate Authority (CA) Certificate

Enable the addition of a custom CA certificate. Some organizations may use their own CA, and adding it here will allow certain KNIME Business Hub services to communicate with external resources that require a custom CA.

Configure Browser Security

In the "Browser Security" section of the KOTS Admin Console you can:

- Specify a custom Content Security Policy for Data App execution. It may be necessary to override the default if you are using custom JavaScript views that load external resources. The default works for all standard KNIME views. For more information about how to write the CSP statement, please refer to this [resource](#).
- Configure the X-Frame-Options header being set by webapps. This header is used to avoid click-jacking attacks, by ensuring that the sites content is not embedded into other sites. See [here](#) for more information.

Browser Security

This section contains settings for browser security.

☒ Enable Content Security Policy for Data Apps

Enabling this option allows you to set a custom Content Security Policy for Data Apps below. If disabled, no Content Security Policy header is set.

Content Security Policy for Data Apps

Specifies a custom Content Security Policy for Data App execution. It may be necessary to override the default if you are using BIRT report generators or custom JavaScript views that load external resources. The default works for all standard KNIME views. For more information about how to write the CSP statement, please refer to this [resource](#).

```
default-src 'self'; script-src 'unsafe-inline' 'unsafe-eval' 'self'; style-src 'unsafe-inline' 'self'; img-src 'self' data:; font-src 'self'
```

Default value: `default-src 'self'; script-src 'unsafe-inline' 'unsafe-eval' 'self'; style-src 'unsafe-inline' 'self'; img-src 'self' data:; font-src 'self' data;;`

X-Frame-Options Header

Sets the `X-Frame-Options` header to the selected option, or doesn't set the header if `none` is selected. This header is used to avoid click-jacking attacks, by ensuring that the sites content is not embedded into other sites. See [here](#) for more information.

☒ SAMEORIGIN ☐ DENY ☐ none

Activate and configure Job Instrumentation Data

To make use of the service that stores job's data you need to check the relative option in the "Job Instrumentation Data" section of the KOTS Admin Console. By default the collected data are deleted after 30 days. Here, you can also change this value to the amount of desired days.



You can use the Workflows Jobs Monitoring data application for obtaining insights about the status of workflow executions, usage of execution resources across different teams, or identify faulty jobs.

Job Instrumentation Data

KNIME Business Hub can collect instrumentation data on workflow executions.

☒ Do you want to collect job instrumentation data?

Job Info Expiration

How long instrumentation data about a job is stored, in days.

Default value: 30

Installation of AI services (Enterprise edition only)

The AI service is a Business Hub Enterprise feature that enables end-users to connect the **AI features** of their Analytics Platform (such as the KNIME AI Assistant and Code Generation) to KNIME Business Hub.

The AI service is configured via the KOTS Admin Console.

The configuration consists of three parts:

- LLM provider
- Disclaimer & welcome messages
- AI history access groups

LLM provider

Currently, it is possible to configure the AI service to use either OpenAI or Azure OpenAI as backend.

To configure OpenAI as LLM provider do the following steps:

1. Create an OpenAI account
2. Generate an API key on the **API keys page**. It is recommended to create a fresh API key that is used exclusively by the AI service.

To configure Azure OpenAI as LLM provider do the following steps:

1. Create an Azure account and get access to Azure OpenAI

2. Create an Azure OpenAI resource to be used by the service and enter it in the KOTS Admin Console. It is recommended to create a separate resource that is used exclusively by the AI service to avoid any interference with other applications. See the [Azure OpenAI documentation](#) to learn how to create a resource.
3. Deploy a GPT 3.5 Turbo, a GPT 4 and an embeddings model with API version 2023-07-01-preview or newer. The embeddings model must be a text-embedding-ada-002 for the AI service to function properly. See the [Azure OpenAI documentation](#) for more details.

Models usage

The GPT 3.5 Turbo and the embeddings model are used for the Q&A mode of the KNIME AI Assistant.

The GPT 4 model is used for code generation and the build mode of the KNIME AI Assistant.

The reason for this distinction is that the GPT 4 model is more capable than the GPT 3.5 Turbo model but also much slower to respond and more expensive. If response time and cost are no concerns, GPT 4 can also be used for the Q&A mode.

Disclaimer & welcome messages

The KOTS Admin Console also allows to customize the initial messages displayed by the KNIME AI Assistant. The disclaimer is not shown by the KNIME AI Assistant if it is left empty.

AI history access groups

The AI service also exposes an endpoint that allows to retrieve the requests that were made to the AI service via the KNIME AI Assistant. The KOTS Admin Console allows to configure which Keycloak groups can access the endpoint.

It is recommended to only give access to admins.

The address depends on the hub but it is typically located at <https://api.<base-url>/ai-history/kai>.

GET requests to this endpoint need to have the authorization header set with a valid bearer token from the Hub.

You have the possibility to filter data by date directly within the endpoint, for instance:

```
https://api.<base-url>/ai-history/code/python?start_time=2023-12-31T00:00:00&end_time=2024-04-10T00:00:00
```

The format of the parameters `start_time` and `end_time` needs to be `yyyy-mm-ddThh:mm:ss` as in the example above.



A **data application** is available to help you monitor and govern K-AI usage in your KNIME Business Hub instance. Find more information and a step-by-step guide [here](#).

Node affinity

Node affinity makes it possible to ensure that cluster resources intended for a specific task, e.g. execution resources, run on a specific set of nodes. There are two roles that each pod is grouped into: `core` and `execution`. Pods in the `core` group consist of KNIME Business Hub control plane resources, and pods in the `execution` group relate to execution contexts.

In order to use the node affinity feature in your KNIME Hub cluster, you can apply one or both of the following labels to nodes within your cluster:

- `hub.knime.com/role=core`
- `hub.knime.com/role=execution`

To label a node, you can execute the following command (where `<node-name>` is the name of the node you want to label):

```
kubectl label node <node-name> hub.knime.com/role=core
```



For more information about labeling nodes, see the [Kubernetes documentation](#).

Pods will have to be restarted in order to be rescheduled onto labeled nodes. You can use the following example commands to restart the pods in a live cluster:

- `kubectl rollout restart deployment -n istio-system`
- `kubectl rollout restart deployment -n hub`
- `kubectl rollout restart deployment -n knime`
- `kubectl delete pods --all --namespace hub-execution`



This command will restart all execution context pods.

There are a few things to note about the behavior of this feature:

- Node affinity uses a "best effort" approach to pod scheduling.
 - If one or both of the `hub.knime.com/role` labels are applied, cluster resources will attempt to be scheduled onto the nodes based on their role.
 - If no nodes have a `hub.knime.com/role` label, pods will be scheduled onto any available node.
 - If labeled nodes reach capacity, pods will be scheduled onto any available node.

- If a labeled node is shut down, pods will be rescheduled onto other nodes in the cluster with a preference towards using nodes that have a matching label.
- Node affinity for KNIME Business Hub uses the `preferredDuringSchedulingIgnoredDuringExecution` approach (see the [Kubernetes documentation](#) for more details).
- It is possible to use only one of the labels above, e.g. labeling nodes for the `execution` role but not specifying any node labels for the `core` role.

Create a collection (Enterprise edition only)

It is possible to create collections on your KNIME Business Hub instance.

KNIME Collections on KNIME Hub allow upskilling users by providing selected workflows, nodes, and links about a specific, common topic.

One example of a collection can be found on KNIME Community Hub [here](#).



This is a feature of KNIME Business Hub - Enterprise edition.

In order to create a new collection page you need to be a global admin of your KNIME Business Hub instance.

The creation of a collection is possible via REST API, and a description of the different configurations can be found in your KNIME Business Hub API doc at the following URL:

```
api.<base-url>/api-doc/?service=catalog-service#/Collections
```

e.g. `api.hub.example.com/api-doc/?service=catalog-service#/Collections`.

In order to create a collection the items (i.e. workflows and nodes) that are collected need to be stored and accessible on the same KNIME Business Hub instance where collection is created.

To create the collection you will need then to build a json file with the schema that is available in the API doc in the Collections section, under the POST `/collections` request description.

The following is an example that would allow you to build a collection, similar to the one available on KNIME Community Hub [here](#).

In the first section you can for example set up a title, a description, a so-called hero, which is the banner image at the top right of the example collection page, and tags:

```
{
  "title": "Spreadsheet Automation",
  "description": "On this page you will find everything to get started with spreadsheet automation in KNIME",
  "ownerAccountId": "account:user:<global-admin-user-id>",
  "hero": {
    "title": "New to KNIME?",
    "description": "Get started with <strong>KNIME Analytics Platform</strong> to import all the examples and nodes you need for spreadsheet automation right now!",
    "actionTitle": "Download",
    "actionLink": "https://www.knime.com/downloads"
  },
  "tags": [
    "Excel",
    "XLS"
  ],
}
```

Next you can add different sections and subsections, each with a title and a description, choose a layout, and select the `itemType` such as *Space*, *Component*, *Workflow*, *Node*, *Extension*, or *Collection*. For each of these items you will need to provide the `id` under which they are registered in your Business Hub installation.

The `id` for workflows, spaces, components, and collections can be build by taking the last part of their URL, after the `~`, and adding a `*` at the beginning. For example, the following workflow on the KNIME Community Hub has URL `https://hub.knime.com/-/spaces/-/latest/~1DCip3Jbxp7BWz0f/` so its `id` would be `*1DCip3Jbxp7BWz0f`. The `id` for node and extensions instead needs to be retrieved with a REST call, for example to the `search` endpoint of your KNIME Business Hub instance.

```

"sections": [
  {
    "title": "Workflow examples",
    "description": "Some subtitle text here. Can have <strong>bold format</strong>",
    "iconType": "Workflow",
    "subsections": [
      {
        "title": "How to do basic spreadsheet tasks in KNIME",
        "description": "Some examples on how to do common things",
        "layout": "SingleColumn",
        "numberOfTeaseredItems": 2,
        "items": [
          {
            "title": "Click Here!",
            "itemType": "Link",
            "absoluteUrl": "https://knime.com"
          },
          {
            "id": "*SJW5zSkh1R3T-DB5",
            "itemType": "Space"
          },
          {
            "id": "*vpE_LTbA0n96Z0g9",
            "itemType": "Component"
          },
          {
            "id": "*MvnABULB035AQcAR",
            "itemType": "Workflow"
          },
          {
            "showDnD": true,
            "id": "*yiAvNQVn0sVwCwYo",
            "itemType": "Node"
          },
          {
            "id": "*bjR3r1yW0znPIEXS",
            "itemType": "Extension"
          },
          {
            "id": "*QY7INTkMW6iDj7uC",
            "itemType": "Collection"
          }
        ]
      }
    ]
  }
]

```

Administrator workflows

The workflows described in this section of the documentation aim to support KNIME Business Hub administrators, or heavy KNIME Business Hub users, to configure, clean up, monitor and better administrate their Business Hub instance.

The functionalities provided are a time saver for monitoring or administrating KNIME Business Hub, eliminating the need for manual work and centralizing information from various applications.

Workflows overview

The user can access the workflows on the KNIME Community Hub in a [public space](#) owned by KNIME. Additionally, the user can find them on a dedicated [collection page](#). To use them, download the workflows from the Community Hub and upload them into an existing team space in your KNIME Business Hub installation.

Business Hub has three types of user roles (global admin, team admin, and team member). All the users with access to the “Admin Space” can run the workflows. The user’s role defines their allowed actions when running the different workflows.

The workflows can be run as data applications on-demand or directly scheduled using the Business Hub UI. First, you must deploy the workflows as a Data app or Schedule.

Below the list of workflows within the “Admin Space”, click on them to read further details:

- [Discard Failed Jobs](#)
- [Manage All Existing Jobs](#)
- [Delete Old Versions](#)
- [Scheduled Workflows Kick-Off Times](#)
- [Count Workflows Running Per Day](#)
- [Workflows' Run Time](#)
- [Monitor Users' Usage](#)

Requirements and prerequisites

Requirements

- The user needs to exist and be at least a Team member (no matter the user's role) where the "Admin Space" is located
- Also, the user needs at least view access to the "Admin Space."

Prerequisites

- The user should be familiar with new concepts on the Hub. See the KNIME Business Hub User Guide.
- The user needs to create an application password specific to her account on KNIME Business Hub that most applications will use.

Discard Failed Jobs

Overview

This workflow aims to keep "clean" the KNIME Business Hub installation by discarding failed jobs from any kind of execution run by the KNIME Business Hub users.

Workflow specs

Without applying any time range, the workflow discards all failed jobs for the following execution types: **ad-hoc executions**, **triggers**, **data apps**, **schedules** or **shared deployments**.

We consider as failed jobs all those with any of the following states after execution: "Execution_Failed", "Execution_Failed_With_Content", "Execution_Canceled", or "Vanished".

The failed jobs a user can discard depend on the role of the user running the workflow:

Global admin: can discard all failed jobs in any team and space from any execution type.

Team admin: can discard all failed jobs of the teams of which it is an admin from any execution type.

Team member: can discard only self-generated failed jobs from any execution type, any team and space of which it is a member (no matter the **user's right's** on space items). It also includes deployments shared with the user from teams where the user is not a member.

Deployment configuration

This workflow can be deployed as a **data app** or **schedule** deployment.

In both cases, you can provide the following information to deploy the workflow:

1. Hub URL: The URL of your KNIME Business Hub instance, e.g. "https://my-business-hub.com".
2. Application Password ID: User-associated application password ID.
3. Application Password: User-associated application password.

If you want to know how to create an application password, follow **these steps**.

Data app


After deploying the workflow as a Data App, you can run it. To do so, follow **these instructions**.

Below are the steps for the data app:

1. **Business Hub connection:** you need to connect to the KNIME Business Hub instance through the previously generated application password.
2. **Select Job State:** it is possible to customize which types of failed jobs you want to discard. Max 4 job states should be available: "Execution_Failed", "Execution_Failed_With_Content", "Execution_Canceled", or "Vanished".
3. **Discard Results:** A table with the discard jobs results is displayed by default. There is also the possibility to see an illustrated version of the table by selecting the "Switch to charts" option.





Discard Failed Jobs

Discard Results





Discard Jobs Results

☐ Switch to charts

	Execution name	Execution type	Workflow path	Space	Results
	Scheduled job 2023-04-07 03.58.00	schedule	/Users/Continuous Deployment Setup/Public test environment/Faling deployments/failing_workflow	Public test environment	The job has been discarded
	Scheduled job 2023-04-10 03.58.00	schedule	/Users/Continuous Deployment Setup/Public test environment/Faling deployments/failing_workflow	Public test environment	The job has been discarded
	Scheduled job 2023-04-10 23.58.00	schedule	/Users/Continuous Deployment Setup/Public test environment/Faling deployments/failing_workflow	Public test environment	The job has been discarded
	Scheduled job 2023-04-07	schedule	/Users/Continuous Deployment Setup/Public test environment/Faling	Public test environment	The job has been

Result legend

 The job has been discarded

 It has not been possible to discard the job. See the results column for further details


Team filter

☒ Continuous Deployment Setup

← Back

Discard Failed Jobs

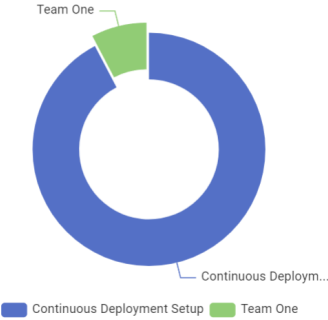
Discard Results



Discard Jobs Results

☒ Switch to charts


Count of Jobs by team



Team One

Continuous Deployment Setup

Count of jobs for Team One spaces



Team member Space

Team One Spaces

Team filter

☒ Team One

☒ Continuous Deployment Setup

← Back

Schedule

- 1. Define when the workflow should be executed through the schedule options. For more information, follow [this guide](#).
- 2. Ensure the Schedule Deployment is active (*Status* column).
- 3. In the Team Deployments page or the workflow page, Deployments section, you can

check the number of executions and their status.

Deployments

Rows: 10 All time

Type of deployment	Name	Workflow	Version	Date of creation	Execution context	Status
Schedule	Schedule - Dis...	...rd Failed Jobs/	Testing links in...	Apr. 12, 2023, ...	4.7.1 Context	On

Rows: 1-2 of 2

Created at	Owner	State	Node messages
Apr. 12, 2023, 12:54	diego	Execution finished	12 Messages
Apr. 12, 2023, 12:53	diego	Execution finished	12 Messages

Manage All Existing Jobs

Overview

Job definition: Whenever a workflow is executed on KNIME Business Hub, it creates a job. Jobs can come from ad-hoc executions or deployments. The Hub's user interface allows users to explore these jobs from different touchpoints, including the Execution Resources and Deployment pages within each team, or the Administration panel for global admins.

The "Manage All Existing Jobs" workflow, deployed as a data application in KNIME Business Hub, displays **all existing** jobs, allowing users to select and delete them. Existing jobs are those in either the executor's memory or the object store (i.e. swapped).

Global or team admins can use the data application to **automate job management** across multiple execution contexts.



You can download the workflow from the [KNIME Community Hub](#). After downloading, upload the workflow to your KNIME Business Hub instance and run it as a **data app**.

Workflow specs

Without applying any time range, the data application lists all existing jobs accessible to the user for the following execution types: **ad-hoc executions**, **triggers**, **data apps**, **schedules** or **shared deployments**.

The data application lists all types of job statuses, including the ones that have failed. For a detailed list click [here](#).

The jobs a user could retrieve depends on the user role:

- **Global admin:** can recover all jobs in any team and space.
- **Team admin:** can recover all jobs within the team where it is an admin.
- **Team member:** can recover jobs from any team and space where it is a member (no matter the **user's rights** on space items). It also includes shared deployments from teams where the user is not a member.

The user's ability to delete jobs is determined by their role:

- **Global admin:** can delete all jobs in any team and space from any execution type.
- **Team admin:** can delete all jobs of the teams of which it is an admin from any execution type.
- **Team member:** can delete only self-generated jobs from any execution type, team and space of which it is a member (no matter the user's right on space items). It also includes deployments shared with the user from teams where the user is not a member.

Deployment configuration

This workflow must be deployed as a **data app**.

You can provide the following information to deploy the workflow:

1. **Hub URL:** The URL of your KNIME Business Hub instance, e.g. "https://my-business-hub.com".



It is possible to use the current Hub authentication by using the default value to "Use current Hub." This option bypasses the need to input the Hub URL and the application password. The user must have the correct rights to access the data.

2. **Username:** User-associated application password ID.
3. **Password:** User-associated application password.

Edit data app for Manage All Existing Jobs

Create a data app to interact with the workflow via a user interface.

Configuration options

Control the parametrization of the workflow execution.

Application password

Username

Password

Default Hub URL (Please use 'Use current Hub' to bypass credential input)

Use current Hub

Advanced settings

Change job lifecycle behavior, timeouts, ... Set >

Cancel Save changes

Figure 46. "Use current Hub" in the deployment configuration dialogue

If you want to know how to create an **application password**, follow [these steps](#).

Data app

After deploying the workflow as a Data App, you can run it. To do so, follow the [instructions](#).

Below is a brief description of each page in the data application:

1. **Available Jobs:** This feature provides a list of jobs with detailed information, including workflow name, team, job state, execution context, deployment type, duration, and execution timestamp. Users can open the job in the new Job Viewer. If the job is a data app in the "Interaction Required" state, users can reopen or terminate the data app as needed.

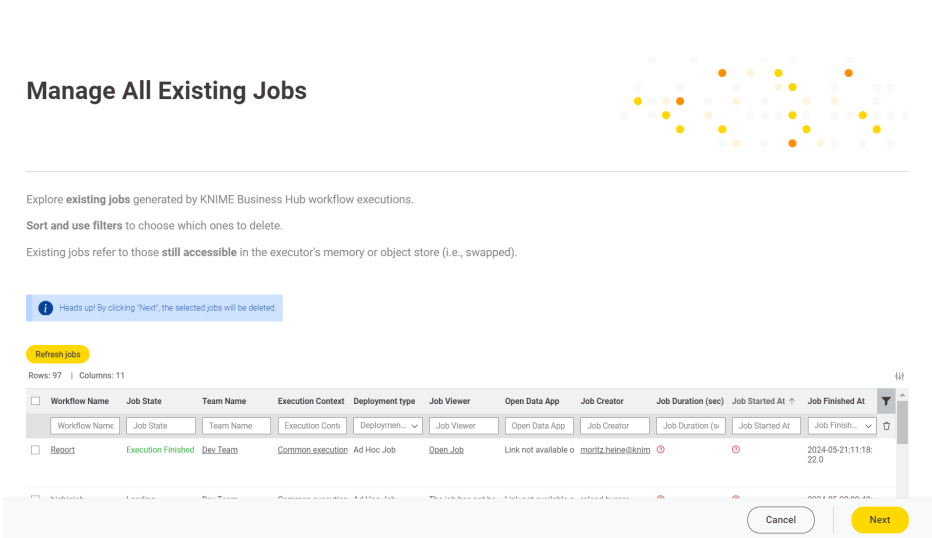


Figure 47. Available jobs table in the data app

- a. As shown in the image above, you can use the table **filters** to narrow your research and **sort** the columns by clicking the column header.
- b. By selecting the jobs from the table and clicking the "Next" button, the application will attempt to delete them in the next step.

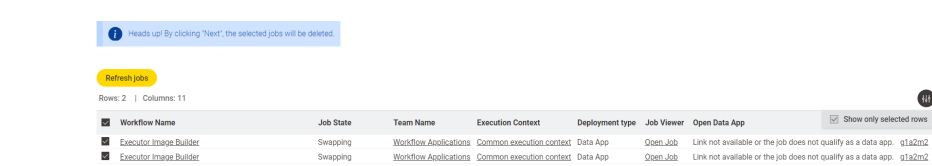


Figure 48. The selected jobs will be deleted after clicking the "Next" button.

- c. There is a **"Refresh jobs"** button to fetch the latest status of the KNIME Business Hub instance, as more jobs could be produced during the data application's execution.
- d. The table displays **100 jobs**. Use the pagination arrows at the top to navigate the table.
- e. Two exceptions related to the job's deployment information:
 - i. When you run a workflow in KNIME Business Hub using the Run button, it generates a job, but the deployment name is unavailable. Therefore, the deployment type is "Ad Hoc Job."

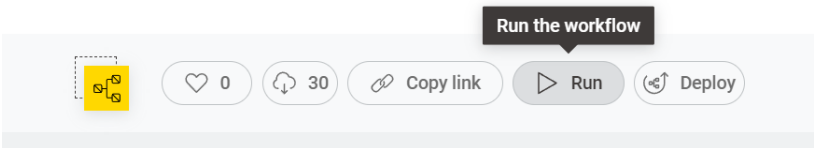


Figure 49. Ad-hoc execution via the Run button.

- ii. If the deployment that generated a job is no longer available in the KNIME

Business Hub at the time the current data application is executed (due to deletion or the end of a scheduled deployment), it will not be possible to retrieve the deployment information. Instead, a message will be displayed in the "Deployment type" column: "Not Available."

- 2. **Deletion Results:** The table displays job deletion results, including job name, deletion result, team name, deployment type, and workflow name.

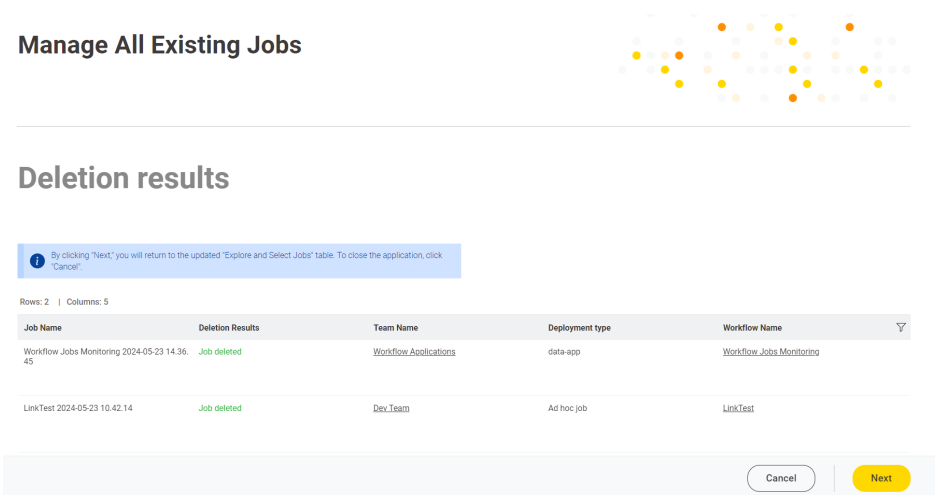


Figure 50. Deletion results table in the data app

- a. If the data application cannot delete a job, an error message will be displayed in the deletion result column.

Rows: 1 Columns: 5				
Job Name	Deletion Results	Team Name	Deployment type	Workflow Name
Manage All Existing Jobs 2024-05-28 09:49:3	User is not allowed to delete job '65952e06-fd53-4a37-a5ee-e88ca4a5314d'	Workflow Applications	data-app	Manage All Existing...

Figure 51. The logged users has insufficient rights to delete the job.

- b. By clicking the "Next" button, the user will return to the updated "Explore and Select Jobs" table. To close the application, click "Cancel".

3. **Warnings and errors:**

- a. The data application interacts with the KNIME Business HUB API using GET requests to fetch the jobs and DELETE requests to delete them. It also ensures that a meaningful error is displayed in case of server-side issues or problems with the API call.

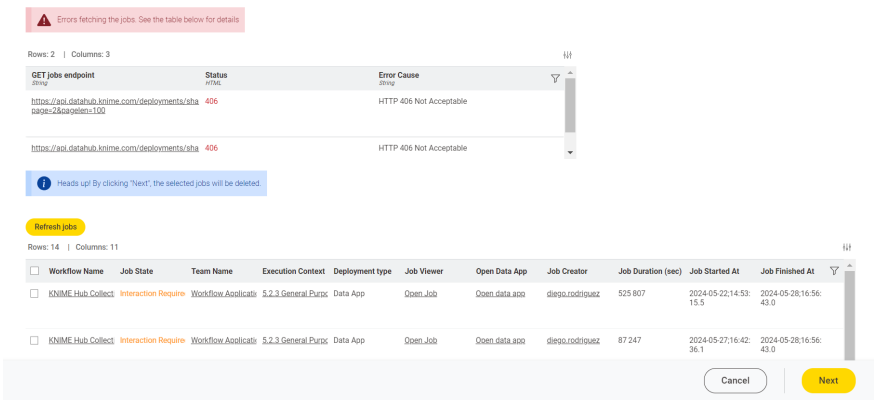


Figure 52. GET Request error displayed in the data app

- b. If the user doesn't select any jobs in the "Explore and Select Jobs" table and then clicks "Next", the data application will display a warning on the "Deletion Results" page. Clicking "Next" again redirects you to the "Explore and Select Jobs" table.

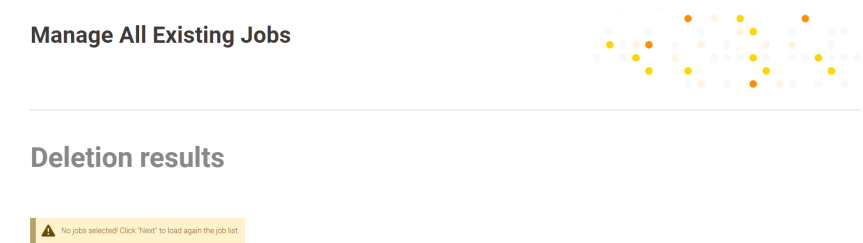


Figure 53. Warning message displayed in the data app

- c. Also if no jobs are available in the KNIME Business Hub instance for the logged user, a message will be displayed.

Delete Old Versions

Overview

The workflow aims to delete old item versions that aren't involved in any deployment. The sought effect of this operation is to avoid a massive proliferation of item versions within the Business Hub installation, impacting disk space.

Workflow specs

The workflow deletes all item versions older than the specified number of days, e.g. older than seven days.

The deletion will only be applied to the selected teams and spaces using the workflow as a data app or schedule deployment.

In cases where a rule applies to all versions in a space, the latest version will not be deleted, even if it is affected by the rule. Additionally, item versions that are involved in deployments are exempt from the rule.

Depending on your user role on the KNIME Business Hub, if you execute this workflow, you will have the following permissions:

Global admin: Can delete every item version not used in any deployment from any team on the KNIME Business Hub instance.

Team admin: Can only delete the item versions not involved in any deployment in the team where it's an admin.

Team member: Can only delete the item versions not involved in any deployment in the teams where it's a member. The Team member must have "Edit" permissions for the targeted spaces to perform the version deletion.

Deployment configuration

This workflow can be deployed as a **data app** or **schedule** deployment.

You need to provide the following information to deploy the workflow as a data app or to schedule it:

1. Hub URL: The URL of your KNIME Business Hub instance, e.g. "https://my-business-hub.com".
2. Application Password ID: User-associated application password ID.
3. Application Password: User-associated application password.
4. Team name: Use "*" to select all and "/" to choose a subset: "Team1/Team2".
5. Space name: Use "*" to select all and "/" to choose a subset: "Space1/Space2".
6. The number of days: All item versions older than that will be deleted (default is 30 days).

To create an application password, follow **these steps**.

Data app


After deploying the workflow as a data app, you can run it. To do so, follow these **instructions**. Below are listed the steps for the data app::

1. **Business Hub connection:** You need to connect to the KNIME Business Hub instance through the application password generated previously.
2. **Team and Space selection:** Select the teams and associated spaces from which the workflow should delete the old versions.
3. **Define version deletion rule:** Here, you can set a version deletion rule. All versions older than the given number of days will be deleted.
4. **Deletion result:** A table showing the deletion result with the version information will appear by default.

Switching to a chart view is possible using the “Switch to charts” option.

Delete Old Item Versions

Deletion results



Deleted versions

Team






Workflow Building
▼

Space

☒ Migration Workflow Updated with Item Versioning
☐ Trigger Demo 2
☒ Trigger Demo


☐ Switch to charts


Show 5 entries

	Item path	Creation date	Version details	Results
	/Users/Workflow Building/Migration Workflow Updated with Item Versioning/KNIME Server to KNIME Hub Migration	2023-07-04 UTC	Version title: latest - Version index: 1 - Version description :	Item version deleted
	/Users/Workflow Building/Trigger Demo/Training Workflow	2023-04-03 UTC	Version title: Version created by Trigger Deployment (migrated from space version 35) - Version index: 35 - Version description :	Item version deleted
	/Users/Workflow Building/Trigger Demo/Training Workflow	2023-04-03 UTC	Version title: Version created by Trigger Deployment (migrated from space version 34) - Version index: 34 - Version description :	Item version deleted
	/Users/Workflow Building/Trigger Demo/Training Workflow	2023-04-03 UTC	Version title: Version created by Trigger Deployment - Version index: 33 - Version description :	Item version deleted
	/Users/Workflow Building/Trigger Demo/Training Workflow	2023-04-03 UTC	Version title: Version created by Trigger Deployment - Version index: 32 - Version description :	Item version deleted

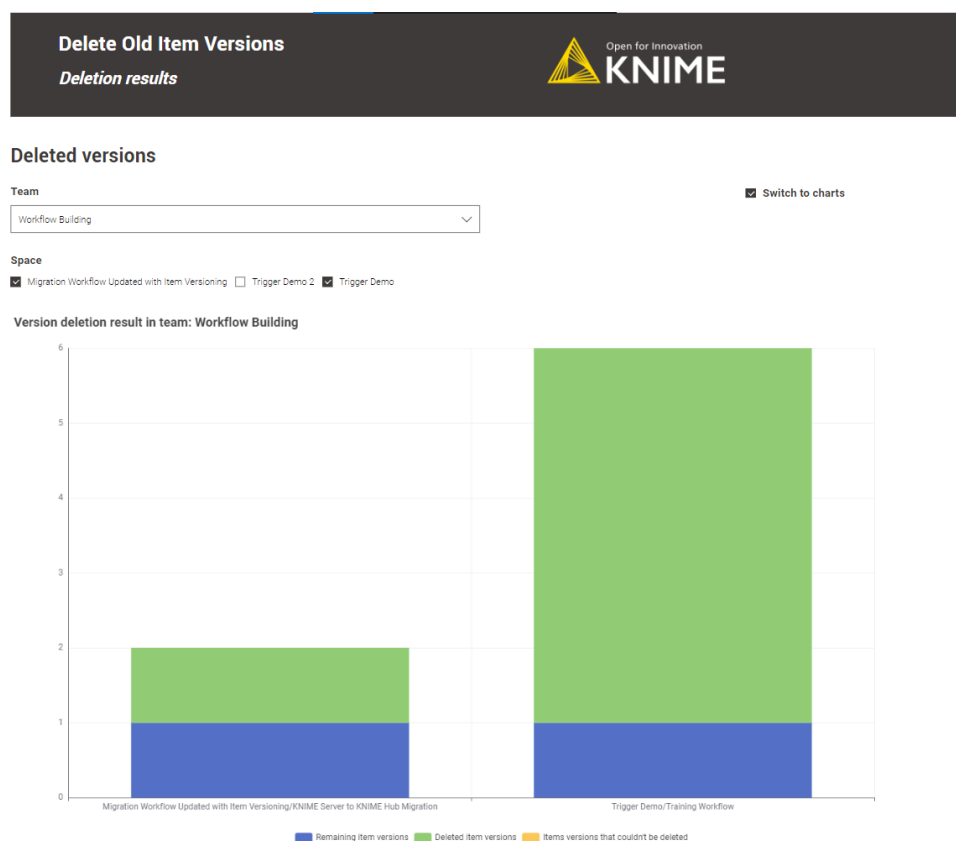
Previous
1
2
Next

Result legend


The item version has been deleted successfully.


Something went wrong. See the *Results* column in the table for further details.

← Back



Schedule

1. Define when the workflow should be executed through the schedule options. For more information, follow [this guide](#).
2. Ensure the Schedule Deployment is active (*Status* column).
3. In the Team Deployments page or the workflow page, Deployments section, you can check the number of executions and their status.

Scheduled Workflows Kick-Off Times

Overview

The workflow aims to prevent scheduled deployments from overlapping and, consequently, helps to avoid overloading KNIME Business Hub executors.

Running on demand as a data app offers the user a visual overview of the scheduled deployments within the given number of days by team and execution context.

Workflow specs

The workflow visualizes all the scheduled deployments by KNIME Business Hub execution context and team in the following days. Notice that the maximum number of days is set up to seven.

The workflow shows only those schedules whose deployment is active and has not been disabled via the KNIME Analytics Platform and those with a valid next execution date.

Depending on the user role, you can view the following schedules:

Global admin: monitor the scheduled workflows of any team and any KNIME Business Hub execution context.

Team admin: monitor the scheduled workflows for any KNIME Business Hub execution context in the team.

Team member: monitor the scheduled workflows for any KNIME Business Hub execution context in the team.

Deployment configuration

This workflow can be deployed as a **data app**.

You can provide the following information to deploy the workflow as a data app:

1. **Hub URL:** The URL of your KNIME Business Hub instance, e.g. "https://my-business-hub.com".
2. **Application Password ID:** User-associated application password ID.
3. **Application Password:** User-associated application password.

To create an application password, follow **these steps**.

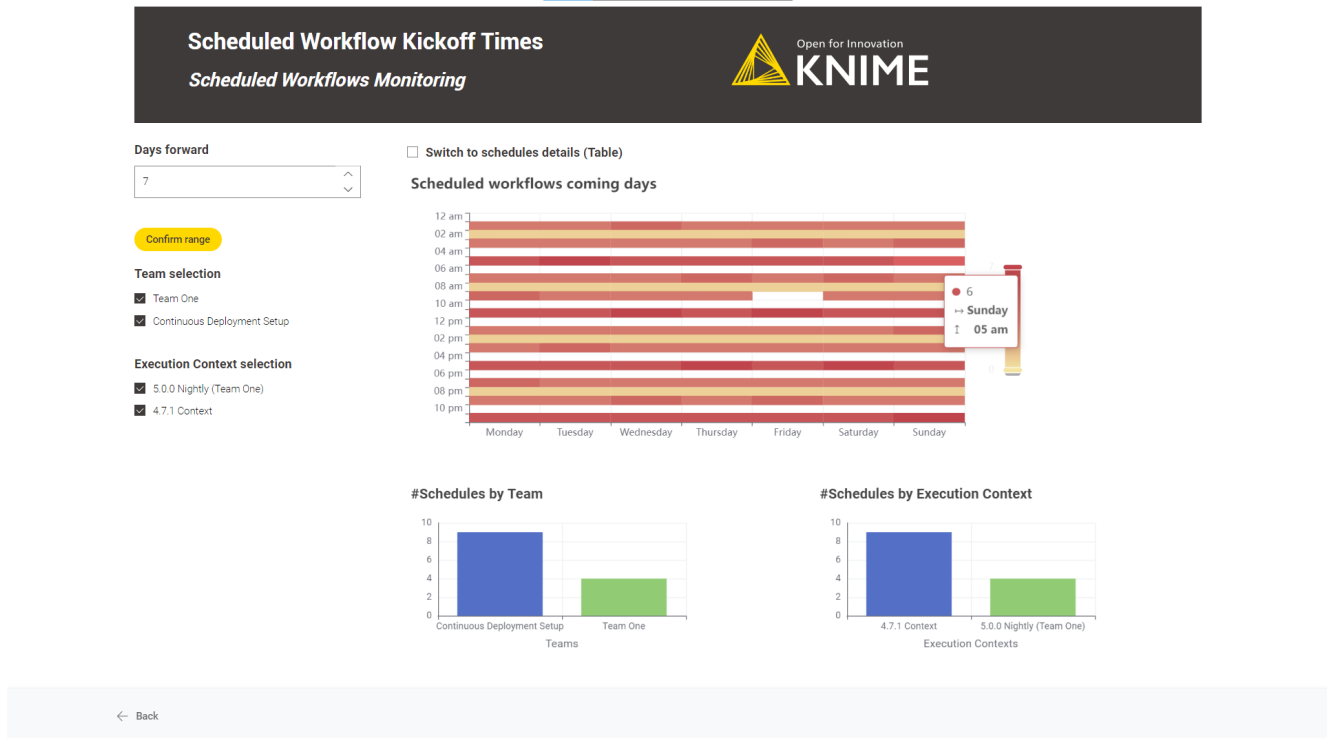
Data app

After deploying the workflow as a data app, you can run it. To do so, follow these **instructions**. Below are the steps for the data app:

1. **Business Hub connection:** You need to connect to the KNIME Business Hub instance through the application password generated previously.
2. **Scheduled Workflows Monitoring:** By default, it visually represents the scheduled workflows in the coming days.

The number of scheduled workflows per day and hour and the number of schedules by team and execution context are represented.

Diving deep into each scheduled deployment is possible by switching to a “Table” mode. Use the “Switch to schedules details (Table)” option.



Scheduled Workflow Kickoff Times
Scheduled Workflows Monitoring

Open for Innovation
KNIME

Days forward: 7

☒ Switch to schedules details (Table)

Schedule name	Created by	Workflow path	Running each	Running times filter	Running days of week filter	Running days filter	Running months filter
ETL workflow	knime	/Users/Team One/Team member Space/failing_workflow	6 hours	[{"start": "00:00", "end": "23:59:59"}]	[MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, SATURDAY, SUNDAY]	[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31]	[JANUARY, FEBRUARY, MARCH, APRIL, MAY, JUNE, JULY, AUGUST, SEPTEMBER, OCTOBER, NOVEMBER, DECEMBER]
knime_user_failing_workflow	knime	/Users/Continuous Deployment Setup/Public test environment/failing deployments/failing_workflow	2 hours	[{"start": "00:00", "end": "23:59:59"}]	[MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, SATURDAY, SUNDAY]	[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31]	[JANUARY, FEBRUARY, MARCH, APRIL, MAY, JUNE, JULY, AUGUST, SEPTEMBER, OCTOBER, NOVEMBER, DECEMBER]
Schedule - ETL Workflow	knime	/Users/Continuous Deployment Setup/Team admin space/failing_workflow	3 hours	[{"start": "00:00", "end": "23:59:59"}]	[MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, SATURDAY, SUNDAY]	[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31]	[JANUARY, FEBRUARY, MARCH, APRIL, MAY, JUNE, JULY, AUGUST, SEPTEMBER, OCTOBER, NOVEMBER, DECEMBER]
Schedule - Workflow for ETL Basics Operations	knime	/Users/Continuous Deployment Setup/Public test	2 hours	[{"start": "00:00", "end": "23:59:59"}]	[MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, SATURDAY, SUNDAY]	[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31]	[JANUARY, FEBRUARY, MARCH, APRIL, MAY, JUNE, JULY, AUGUST, SEPTEMBER, OCTOBER, NOVEMBER, DECEMBER]

← Back

Count Workflows Running Per Day

Overview

After a while, the KNIME Business Hub instance automatically discards already executed workflow jobs. KNIME Business Hub administrators can define this time window until a specific period, but it is not infinite.

The workflow scope is to go beyond this automatic discard timeline creating a historical file with all the workflow execution information for further consultation.

Workflow specs

The workflow saves in the root level of an existing team space a CSV file of the jobs information of any state ("Executed", "Failed", etc.) and from any execution type (Deployments and Ad-hoc executions).

The workflow job information a user could retrieve depends on the user role running the deployed workflow:

Global admin: can recover all workflow jobs in any team and space.

Team admin: can recover all workflow jobs within the team where it is an admin.

Team member: can recover workflow jobs from any team and space where is a member (no matter the **user's right's** on space items). It also includes shared deployments from teams where the user is not a member.

The team space where the CSV file can be saved depends on the user role running the deployed workflow:

Global admin: can save workflow job information in any team space.

Team admin: can save workflow job information in every team space where it is an admin.

Team member: can save workflow job information in every team space where it is a member and it has edit permissions.

The user must define the number of backward days you want to retrieve the workflow job information, e.g. last five days.

If you repeatedly target the same team space executing this workflow, the workflow will append the new information to the master file.

Deployment configuration

This workflow can be deployed as a **data app** or **schedule** deployment.

You can provide the following information to deploy the workflow as a data app or schedule it:

1. Hub URL: The URL of your KNIME Business Hub instance, e.g. "https://my-business-hub.com".
2. Application Password ID: User-associated application password ID.
3. Application Password: User-associated application password.
4. Last n days filter: Save job information of all jobs from the last n days.
5. Select the destination Team: The team in which the job information will be saved.
6. Select the destination Space: The space in which the job information will be saved.

To create an application password, follow **these steps**.

Data app

After deploying the workflow as a data app, you can run it. To do so, follow these **instructions**. Below are the steps for the data app:

1. **Business Hub connection:** You need to connect to the KNIME Business Hub instance through the previously generated application password.
2. **Set rule and file destination:** Select the last n days to save the workflow job information. And choose the destination team and space where this file will be saved.
3. **File location link and preview:** You can find the link to the destination space and a preview of the saved job information.

Workflows running per day

File location link and preview



You can find the file with the workflows running per day here: [User space](#)

Workflows running per day preview

Execution name	Execution type	Team	Hub path	Job state	Timestamp
Scheduled job 2023-04-18 07.34.00	schedule	Continuous Deployment Setup	/Users/Continuous Deployment Setup/Public test environment/Scheduled deployments/flyweight-execution-workflow	EXECUTION_FINISHED	2023-04-18
Scheduled job 2023-04-21 11.33.00	schedule	Continuous Deployment Setup	/Users/Continuous Deployment Setup/Public test environment/Scheduled deployments/middleweight-execution-workflow	EXECUTION_FINISHED	2023-04-21
Scheduled job 2023-04-17 07.34.00	schedule	Continuous Deployment Setup	/Users/Continuous Deployment Setup/Public test environment/Scheduled deployments/flyweight-execution-workflow	EXECUTION_FINISHED	2023-04-17
Scheduled job 2023-04-18 15.34.00	schedule	Continuous Deployment Setup	/Users/Continuous Deployment Setup/Public test environment/Scheduled deployments/flyweight-execution-workflow	EXECUTION_FINISHED	2023-04-18
Scheduled job 2023-04-18 21.33.00	schedule	Continuous Deployment Setup	/Users/Continuous Deployment Setup/Public test environment/Scheduled deployments/middleweight-execution-workflow	EXECUTION_FINISHED	2023-04-18

Job state filter

- ☒ EXECUTION_FINISHED
- ☐ EXECUTION_FAILED
- ☐ INTERACTION_REQUIRED

[← Back](#)

Schedule

1. Define when the workflow should be executed through the schedule options. For more information, follow [this guide](#).
It is recommended to adjust the last n days' field to the chosen schedule option, e.g. if the workflow is scheduled every seven days, set the last n days to seven to avoid duplicate information in the CSV file.
2. Ensure the Schedule Deployment is active (*Status* column).
3. In the Team Deployments page or the workflow page, Deployments section, you can check the number of executions and their status.

Workflows' Run Time

Overview

This workflow aims to list all the workflows sorted by the average execution time (the greater the first) for the last n days.

Workflow specs

We calculate the run time by solely considering the deployed schedules, as monitoring the

execution time of other deployment types is not meaningful. For example, a user could play around one hour or five minutes with a data app.

The average workflow execution time and the standard deviation are calculated for the given period.

Be aware that the number of days a workflow deployment's job is available depends on the KNIME Business Hub instance's configuration, e.g. a common value would be seven days. After that period, all jobs would be discarded automatically.

The average jobs run time, which a user can monitor, depends on the role of the user running the deployed workflow:

Global admin: can monitor the run time of all deployed schedules in any Team and Space.

Team admin: can monitor the run time of all deployed schedules within the Team where it is an admin.

Team member: can monitor the run time of all deployed schedules within the Team where it is a member.

Deployment configuration

This workflow is designed to be deployed only as a **data app**.

You can provide the following information to deploy the workflow:

1. Hub URL: The URL of your KNIME Business Hub instance, e.g. "https://my-business-hub.com".
2. Application Password ID: User-associated application password ID.
3. Application Password: User-associated application password.
4. Last n days filter: number of days from calculating the average execution time, e.g. last seven days.

If you want to know how to create an application password, follow **these steps**.

Data app

After deploying the workflow as a data app, you can run it. To do so, follow these **instructions**. Below are the steps for the data app:


1. **Business Hub connection:** You need to connect to the KNIME Business Hub instance

through the application password generated previously.

2. **Workflow performances:** A performance overview of the deployed workflows for the last n days. Diving deep into any workflow performance is possible by selecting the workflow and clicking the “workflow details” button. When diving deep into the workflow, each workflow’s average run time calculation is calculated per day (stacked area chart).

Workflows' Run Time

Workflow performances



Last n days filter

^
v

[Filter by days](#)

Workflow execution time

<input type="checkbox"/>	Workflow name	Mean (seconds)	Stand. dev. (seconds)
<input type="checkbox"/>	Discard Failed Jobs	3.6	0.548
<input type="checkbox"/>	flyweight-execution-workflow	0	0

[Previous](#)
[1](#)
[Next](#)

Teams' filter

☒ Continuous Deployment Setup

[Workflow details](#)

[← Back](#)

Monitor Users' Usage

Overview

The workflow aims to track KNIME Business Hub user logins to better manage the KNIME Business Hub users' quantity and instance usage.

Workflow specs

You need access to the Keycloak instance embedded in KNIME Business Hub to generate the Client Id and Secret necessary to access the KNIME Business Hub user information.

The workflow shows information about two users type: active and inactive.

Inactive users: those who have never logged into the KNIME Business Hub instance since their creation date.

Active users: those who logged into the KNIME Business Hub instance in the last n days.

It is possible to analyse the session length for actively engaged users. However, it's important to note that if a user doesn't log out after each session, it could impact the accuracy of the KPI calculation. As a result, this metric cannot be considered completely dependable.

Deployment configuration

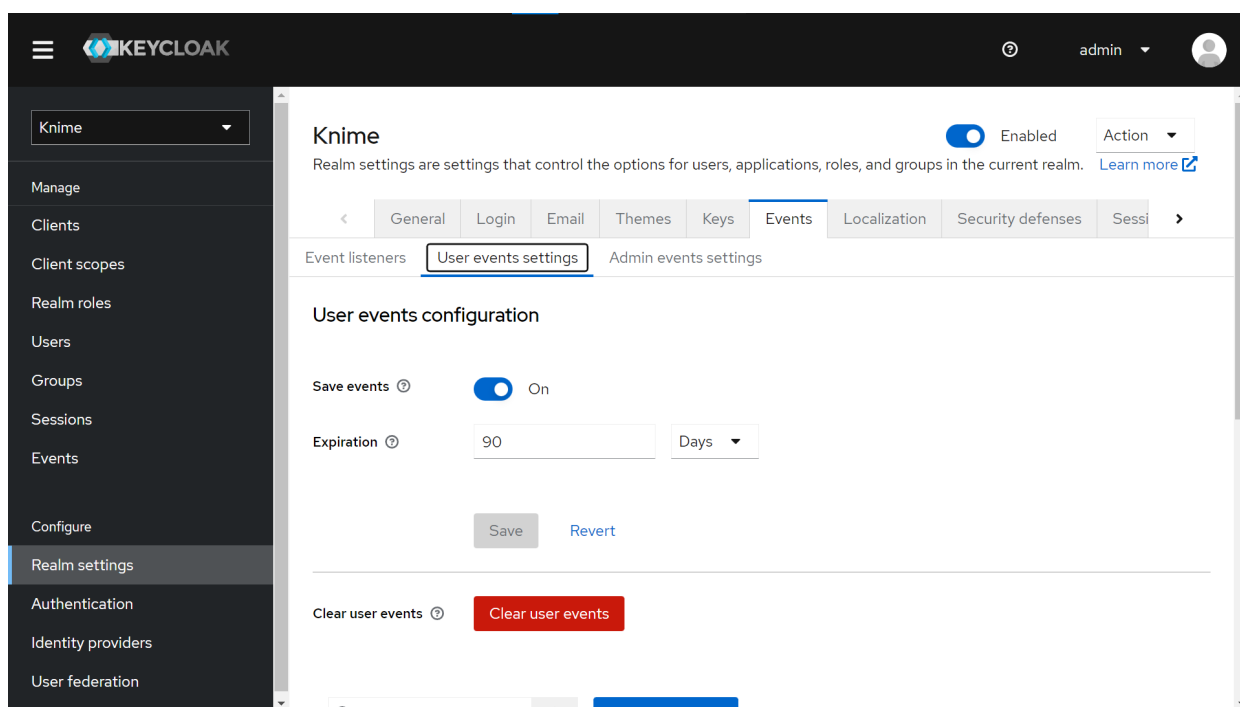
This workflow is designed to be deployed only as a **data app**.

You can provide the following information to deploy the workflow:

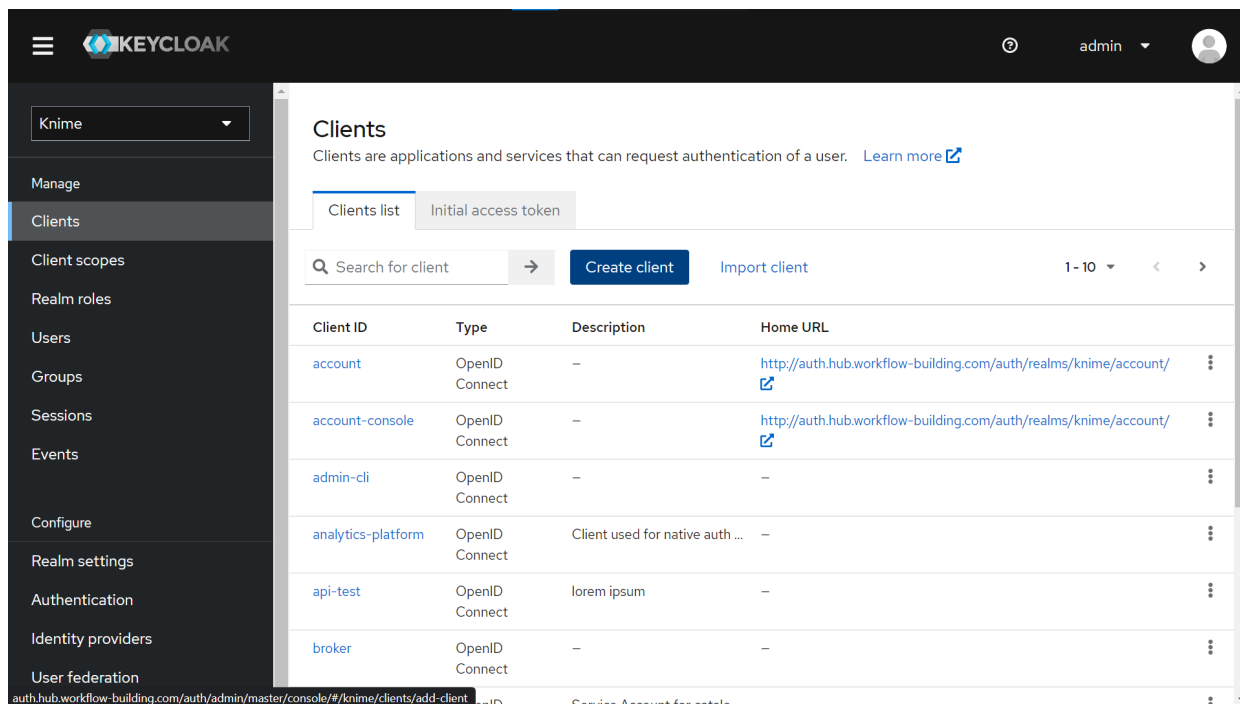
1. Hub URL: The URL of your KNIME Business Hub instance, e.g. "https://my-business-hub.com".
2. Keycloak Client ID: your-ClientId from Keycloak.
3. Keycloak Client Secret: your-Client-Secret from Keycloak.

To generate a Keycloak Client ID and Client Secret:

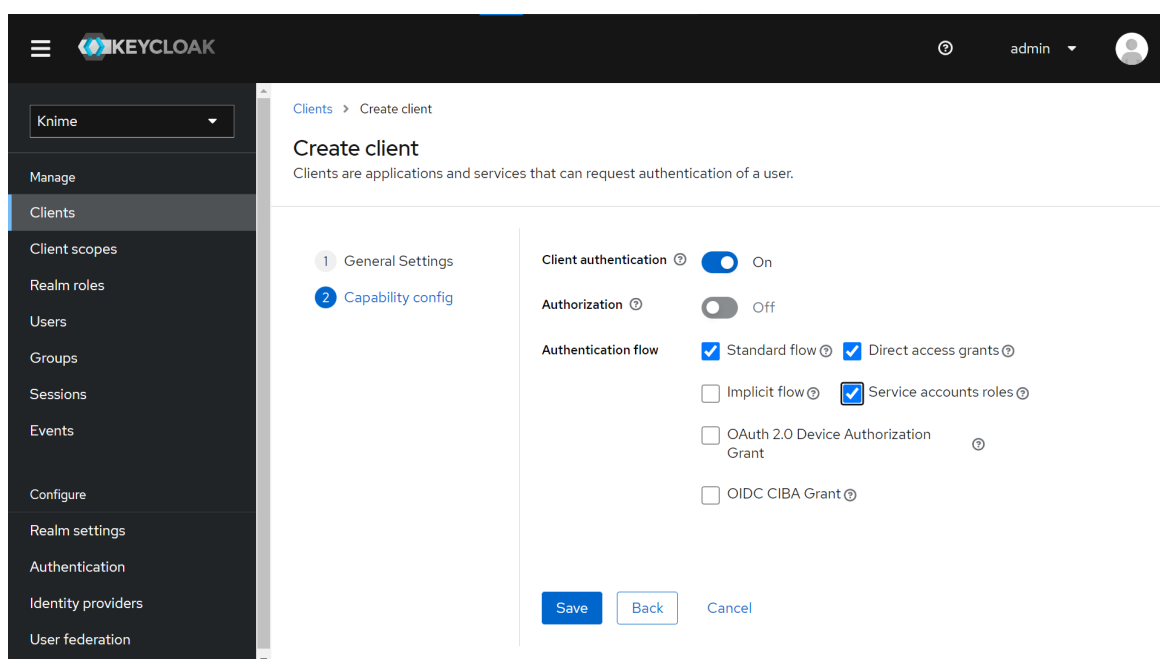
1. Login into Keycloak Admin Console: "https://auth.my-business-hub.com > Administration Console".
2. Select your Realm, and from "Realm Settings > Events > User events settings", activate "Save events" to save KNIME Business Hub Users events. You can configure how many days to keep the user's events.



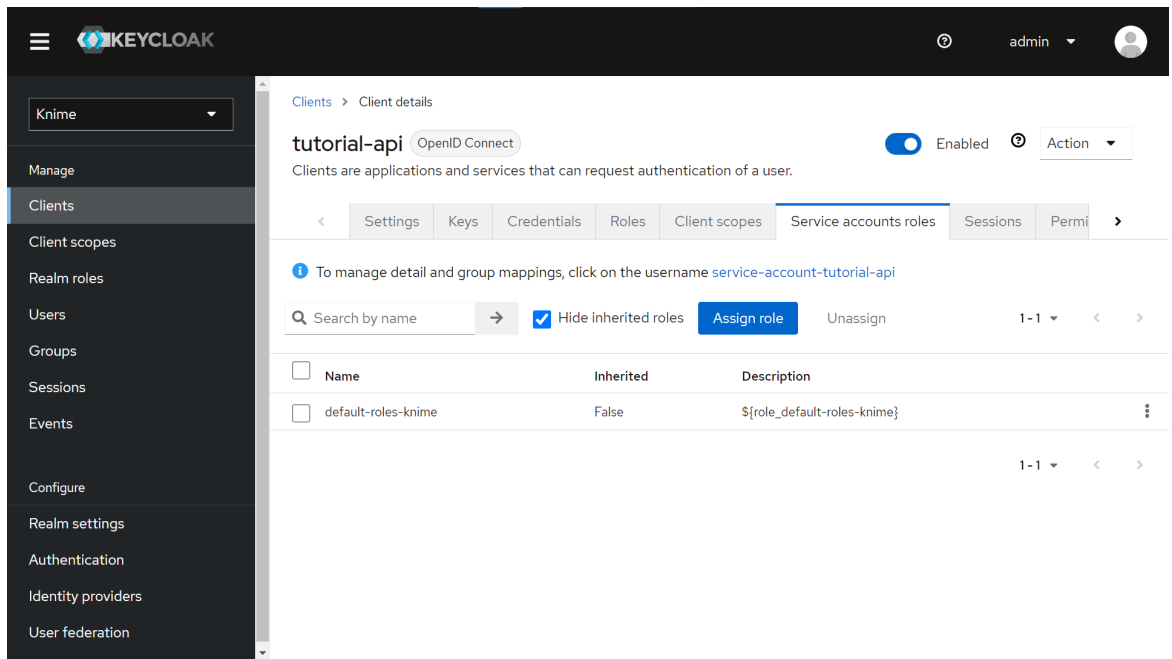
3. Create a new Client from “Clients > Create Client”. Give it a Client ID (tutorial-api in our example), a name (tutorial) and a description (lorem ipsum).



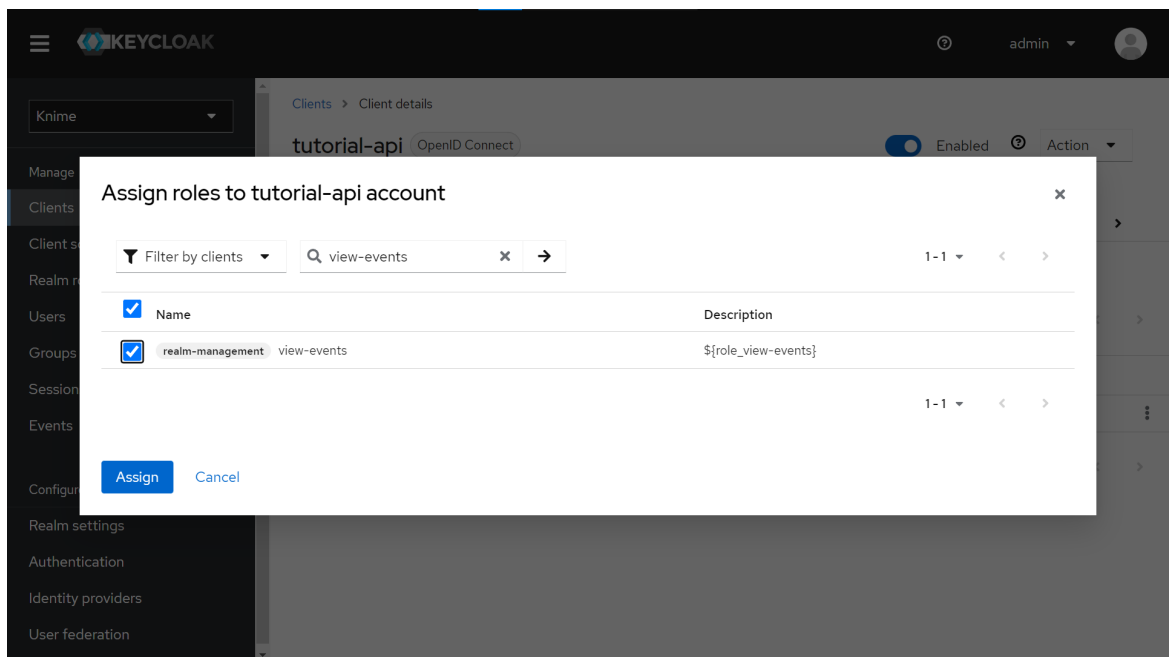
- a. In the “Capability config” section, activate “Client authentication”.
- b. Select “Service account roles” to allow you to authenticate this client to Keycloak and retrieve the access token dedicated to this client.
- c. Save your new client.



4. Click on your new Client (tutorial-api) from “Clients > Client ID (Column)”.
 - a. Go to the “Service account roles” tab > Click the “Assign role” button.

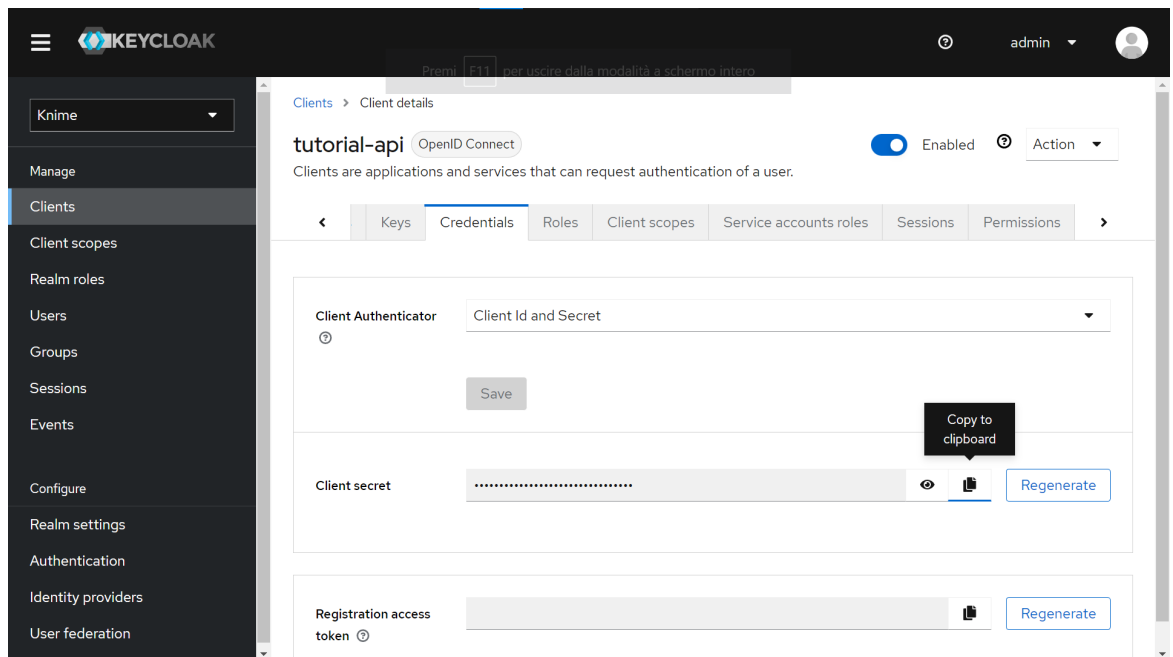


- b. Click “Filter by Roles” and select “Filter by clients”.
- c. Search for “view-events” and for “manage-users” and assign both roles to the Service account associated with our client.



5. Finally, to retrieve the Client ID and Client secret:
 - a. Go to “Clients > Client ID (Column)” and choose your client (tutorial-api in our example)
 - b. Click on the “Credentials” tab
 - c. Leave as a Client Authenticator the “Client ID and Secret” option.
 - d. Copy the Client’s Secret.

- e. Copy the Client ID from the top of the tab (“tutorial-api” in the screenshot below).



Data app

After deploying the workflow as a data app, you can run it. To do so, follow these [instructions](#). Below are the steps for the data app:


Keycloak connection: the user must connect to the Keycloak instance embedded in KNIME Business Hub through the previously generated Client ID and Secret.

User login events: Select the last n days to see KNIME Business Hub active users' login count and inactive users' information. It is possible to explore the active users' session length.

Also, the user can switch to chart mode by clicking the “Switch to charts” option.

Monitor Users Usage

User Login Events



User Usage Results

Days back

15

^

v

Confirm range

☐ Switch to charts

Active Users

<input type="checkbox"/>	Username	Logins count	Days since last access
<input type="checkbox"/>	knime	62	0
<input type="checkbox"/>	knime_admin	28	0
<input type="checkbox"/>	diego	8	0
<input type="checkbox"/>	karen	3	7
<input type="checkbox"/>	simon	3	1

Previous

1

2

Next

Inactive users - No Logins

Username	Days since creation
bernd.wiswedel	162
kevinkr	149
jim.falgout	95
test_daria	155
oole	29

Previous

1

Next

Select users in the "Active users" table and click the button to display more statistics about users' activity

Check sessions' length

← Back

Monitor Users Usage

User Login Events



User Usage Results

Days back

7

^

v

Confirm range

☒ Switch to charts

Aggregated logins count



Individual logins count



Monitoring K-AI in KNIME Business Hub

A **data application** is available to help KNIME Business Hub admins monitor and govern K-AI usage.

Download the data application and upload it to your KNIME Business Hub instance and *Run* it or deploy it as a data app.



Follow the steps 1 to 3 (or 1 to 5 if you want to create a data app deployment) of the **Data apps on KNIME Hub** guide to know how to do this.

Data access

To know more about the AI history access groups, please consult the **KNIME Business Hub Admin Guide**.

Data structure

Every user on the Hub can interact with K-AI. When users open their KNIME Analytics Platform and initiate a prompt, a conversation with K-AI begins. The conversation concludes when the user closes the *Assistant* window. Each question the user asks is a prompt, and the corresponding answer is a response. This results in three distinct levels of K-AI usage data, since each user has multiple conversations consisting of several prompts and responses.

Table 2. An example of usage data for K-AI

User ID	Account created (year)	Conversation ID	User Prompt	K-AI Response	Timestamp	Tokens consumed
37373	2022	1	Hi!	Hello! How can I assist you today?	2024-01-01T00:00:00	330

User ID	Account created (year)	Conversation ID	User Prompt	K-AI Response	Timestamp	Tokens consumed
37373	2022	1	What node can I use to close a loop with the Group Loop Start node	You can use the "Loop End" node to close a loop with the "Group Loop Start" node.	2024-01-01T00:05:00	1220
37373	2022	2	How can I read an Excel file?	To read an Excel file in KNIME, you can use the "Excel Reader" node from the "KNIME Excel [...]"	2024-01-05T20:00:00	880

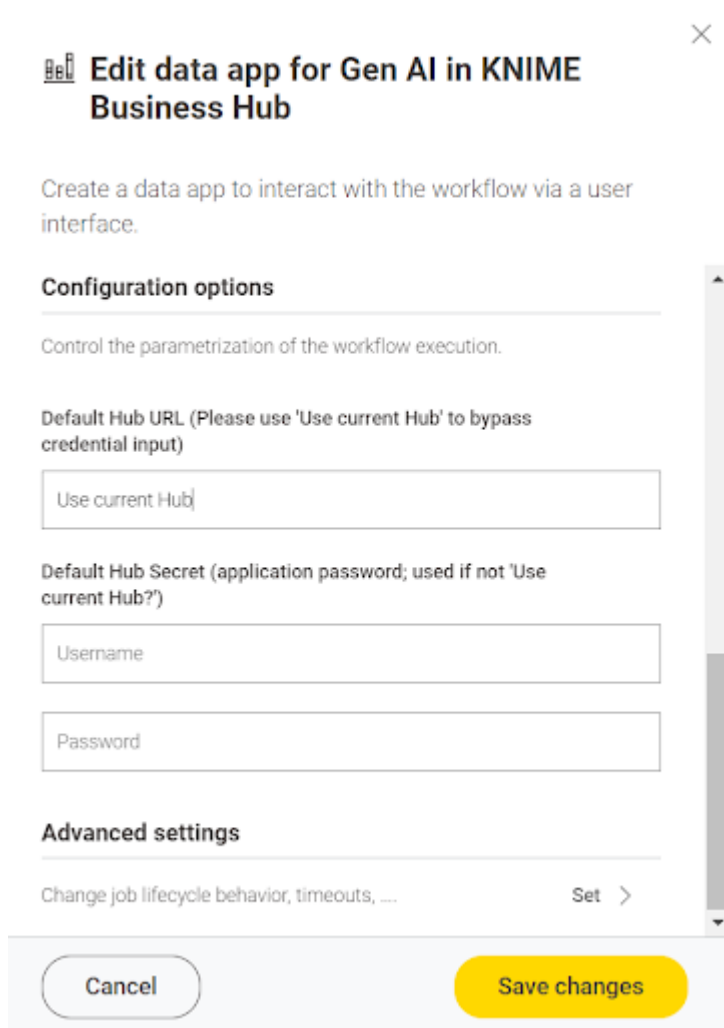
Based on the data in the table, on January 1st, 2024, a user (identified as 37373) interacted with K-AI for five minutes and made two different prompts with varying token consumption values. On January 5th, the same user issued a prompt inquiring about how to read an Excel File. This prompt was stored with a different Conversation ID, indicating that the K-AI assistant was closed between the two conversations.

Deploying the data application

To run the data application in KNIME Business Hub, it is possible to use an [Ad hoc execution](#) or run the [data application deployment](#). Please follow [this](#) link for more information about data app deployments in KNIME Business Hub.

In the data application deployment configuration, the current Hub authentication can be used if the logged user has permission for the correct rights to access the data. Otherwise, a user with permissions must provide their application password, and it is necessary to input the

Hub URL.



Edit data app for Gen AI in KNIME Business Hub

Create a data app to interact with the workflow via a user interface.

Configuration options

Control the parametrization of the workflow execution.

Default Hub URL (Please use 'Use current Hub' to bypass credential input)

Use current Hub

Default Hub Secret (application password; used if not 'Use current Hub?')

Username

Password

Advanced settings

Change job lifecycle behavior, timeouts, ... Set >

Cancel Save changes

Figure 54. Deployment using Use current Hub to bypass credential input

Data application overview

Perspective selection

The data app is divided into four different perspectives to facilitate the answer to various questions:

- **Users:** Who is using K-AI?
This perspective can answer user-related questions like “Are the new KNIME Business Hub users using K-AI?”
- **Conversations:** How are users using K-AI?
This dashboard answers questions such as how the user prompts are distributed by K-AI mode (Q&A, Workflow builder, etc.).

- **Cost:** How much does it cost to use K-AI?

The estimated cost associated with K-AI can be analyzed based on the tokens consumed.

- **All Dimensions:** This perspective combines all attributes and metrics from three previous perspectives to create a more articulated analysis.

K-AI Dashboard

Conversations | Slice and dice by conversation attributes



K-AI is an AI assistant for KNIME that supports KNIME-related questions, workflow building, and scripting nodes such as Python and Echarts. This dashboard provides four perspectives to help you gain insights into K-AI usage.

Perspective selection

☐ Users ☒ Conversations ☐ Cost ☐ All

Figure 55. Perspective selection in the K-AI Dashboard

Slice and dice

There are different slicing filters and dice attributes for every perspective. The term *Slice* refers to filtering the data by different attributes. *Dice* refers to splitting chart metrics by the same attributes. The *Slice and Dice Legend* provides a comprehensive explanation of all of them.

☐ Show slicing filters

Dice (Split by)

K-AI mode

▼ Dice and Slicing Filters Legend

The term 'Slice' refers to filtering the data by different attributes. By selecting the 'Show slicing filter' option, you access a set of filters to slice the data. This allows you to focus on specific user-, conversation-, and prompt-attributes in the current view.

The term 'Dice' refers to splitting chart metrics by the very same attributes. You select the attribute to Dice by in the Drop Down above.

Together, Slicing and Dicing by different attributes allows you to explore the data interactively.

The Dashboard handles different dimensions, each of which certain metrics are attributed to.

User Dimension: Focuses on properties of the users that interact with the AI assistant.

- **Hub Account Age Cohort:** Differentiate new and experienced users based on the year in which a user account was created. For the most recent year, the cohort is further divided into its quarters.
- **Team Memberships:** The number of teams a user is a member of.
- **Team name:** The specific team a user belongs to. Note that if a user is a member of multiple teams, the team association is grouped together.

Apply slice and dice

Figure 56. Slice and Dice Filter Legend in the K-AI Dashboard

Slicing filters

The slicing filters isolate data based on dimension attributes. For instance, from the *Conversation* perspective, you can slice the data only to analyze K-AI interactions related to Python.

☒ Show slicing filters

The Users' slicing filters will filter users and all their conversations, while the Conversations' slicing filters will filter specific conversations with all their prompts. Cost's slicing filters only apply to the prompts.

Based on the [Table 2](#), the user with ID "37373" is filtered out along with all its conversations if you slice by "Hub account age cohort," which equals 2024 in the *User* perspective. Conversation ID 1 is filtered out if you slice by "Conversation duration buckets" equals "10-20 min," and finally, if you slice by "Prompt and response token buckets" equals "1000-2000 tokens," only row 2 from the table above will be kept.

It is important to note that the slicing filters work sequentially from left to right. This means that if you select to view only K-AI interactions within Python nodes, the filtered output of the first slicing filter will be passed to the downstream filters. Please see [Figure 57](#) for a visual representation.

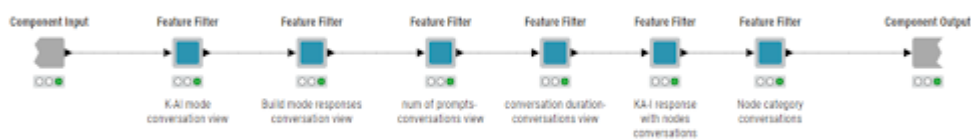


Figure 57. The slicing filters in the underlying workflow

Dice

Analyzing K-AI usage metrics by different attributes can help you understand how data trends are formed over time. For instance, in the *Conversations* perspective, you can observe the number of user prompts over time, split by "K-AI Mode" or "Conversation duration (minutes)" attributes.

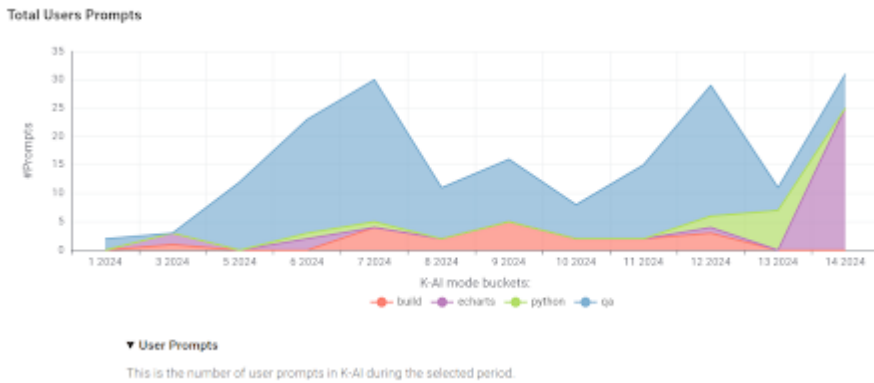


Figure 58. Total user prompts dice by K-AI mode

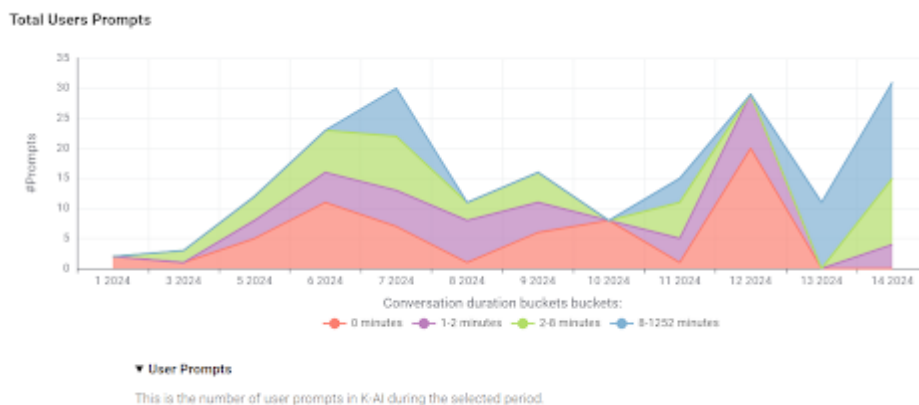


Figure 59. Total user prompts dice by Conversation duration

It is possible to select the attribute to *Dice* in the drop-down menu:

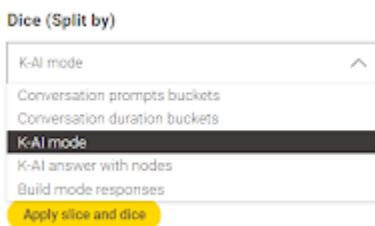


Figure 60. Dice drop-down menu

Data application usage

Please note that if you modify the time range, the data application will retrieve data from the KNIME Business Hub API endpoints again. Depending on the amount of data and the time range, it may take some time to re-execute.

Instead, the granularity feature only re-executes the charts within a different time granularity (from year to day).

When switching between perspectives, e.g., from Users to Conversations, the dice and slicing

filters are reset, and the charts are re-executed.

Customization

This workflow, is a blueprint you can customize to meet your needs. For instance, you can remove or reorganize some slicing filters, choose to have only the *Cost* perspective, eliminate other perspectives, or be inspired to create your attributes.

Workflows Jobs Monitoring data application

Introduction

Whenever an execution is requested on KNIME Business Hub, a corresponding job is created. Executions can originate from various sources such as ad-hoc executions, deployments, or through the Call Workflow node. The Hub's user interface provides access to explore these jobs from different touchpoints. For instance, you can navigate to the *Execution Resources* and *Deployment* pages within each team, or access the *Administration* panel if you are a global admin of the Hub.

However, this data app offers a deeper dive into job executions, providing insights such as:

- Status of workflow executions
- Usage of execution resources across different teams
- Trends in executions over time
- Identification of lengthy executions and faulty jobs

With this data app, you can gain a comprehensive understanding of your workflow executions and optimize processes accordingly.



This application accesses the jobs data collected when the Job Instrumentation Data service is activated for the KNIME Business Hub instance. This is managed from the KOTS Admin Console, as explained in the [Activate and configure Job Instrumentation Data](#) section.

Data application usage

The workflow is stored [here](#) and is compatible with KNIME Business Hub versions 1.10 and above. It can be executed either locally or directly on the Business Hub with executors

versions 5.2.3 and above.

If you choose to run the workflow locally, you will need to manually input the Hub URL and the <<Application Passwords in the String Configuration node.

However, if you opt to run it on the Hub, you can connect directly by selecting "Use current Hub" as the Hub URL, which is also set as the default value. Upon triggering the data app, it will initiate by downloading up to 1000 jobs metadata for each team the logged-in user is associated with.

i

We **strongly advise against** deploying this workflow with a global admin application password stored in the configuration nodes. This would grant all users running the data app access to all jobs or open the job and perform API calls with a global admin role, which leads to a potential security risk. Instead, the **recommended practice** is to deploy the data app with the default value set to "Use current Hub". By doing so, each user running the data app will only see the jobs they have permission to access.

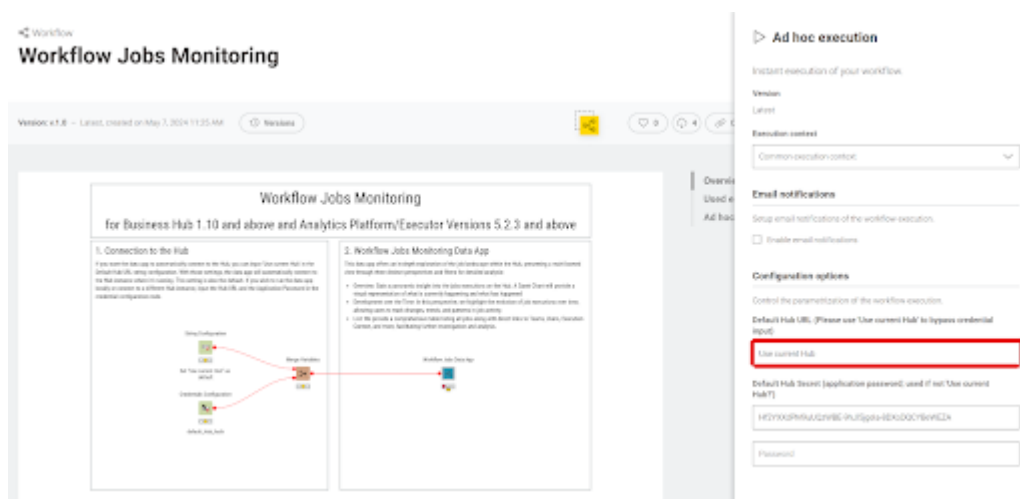


Figure 61. Configuring the Workflows Jobs Monitoring data application

Any user on the Hub can execute the data app. However, the displayed data of the fetched jobs varies significantly based on the user's role within their teams.

Job visibility permissions are structured as follows:

- Global admins have access to view all jobs across all teams on the Hub.
- Team admins are granted access to view all jobs within their respective teams.
- Team members can view all jobs they have triggered.

Once the data app is executed you will be able to see that there are three different sections:

- [Query Parameters](#),
- [Filters](#), and
- [Perspective](#).

Query Parameters

This section enables you to adjust the number of jobs fetched for each team you are a member of. Additionally, it provides connection details such as user roles, the Hub instance you are connected to, the teams you are associated with, and a summary of your permissions.

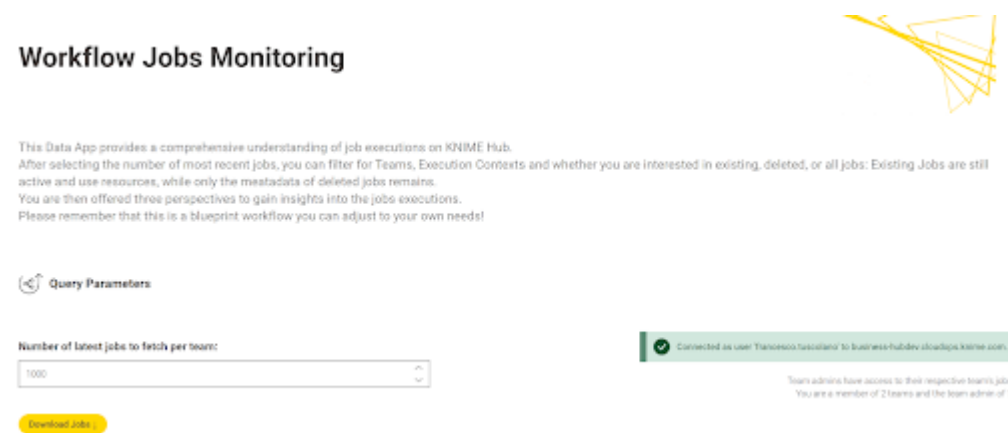


Figure 62. Query Parameters section of the Workflows Jobs Monitoring data application

Filters

This section empowers the data app with filters to slice the downloaded data, considering that users may not be interested in all teams and execution contexts they have access to. Note that the team filter is deactivated if the user can only access jobs from a single team. Additionally, users can choose to visualize all available jobs or only those that are deleted or existing. It is important to remember that deleted jobs are those that have been removed from the executor, with only metadata surviving. Existing jobs, on the other hand, can still be accessed and are retained within the Executor.

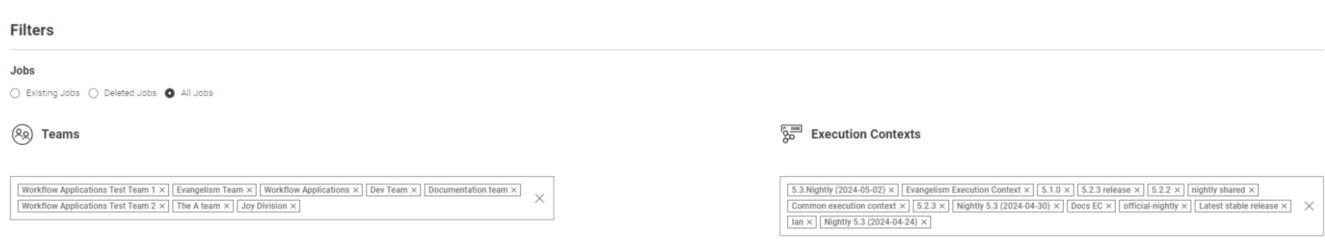


Figure 63. Filters section of the Workflows Jobs Monitoring data application

Perspective

This is the central component of the data app, offering insights into job executions. You have the flexibility to choose among three distinct perspectives, each providing a unique view of the data. While these sections use the same dataset, they are designed to shape and present the information in varied ways, ensuring a comprehensive understanding of the job executions.

Three distinct perspectives are available:

- **Overview:** Gain a panoramic insight into the jobs executions on the Hub. A Gantt Chart will provide a visual representation of what is currently happening and what has happened.
- **Development over the Time:** In this perspective, we highlight the evolution of job executions over time, allowing users to track changes, trends, and patterns in job activity.
- **List:** We provide a comprehensive table listing all jobs along with direct links to Teams, Users, Execution Context, and more, facilitating further investigation and analysis.

Overview

This section provides a concise overview and basic statistics concerning the executions. It includes counts of job states, the number and types of executions by team, the total number of fetched jobs or workflows, and other relevant metrics.

Perspective

Overview

● Overview ○ Development over Time ○ List

Overview: Summary stats and Gantt Chart show job execution details.

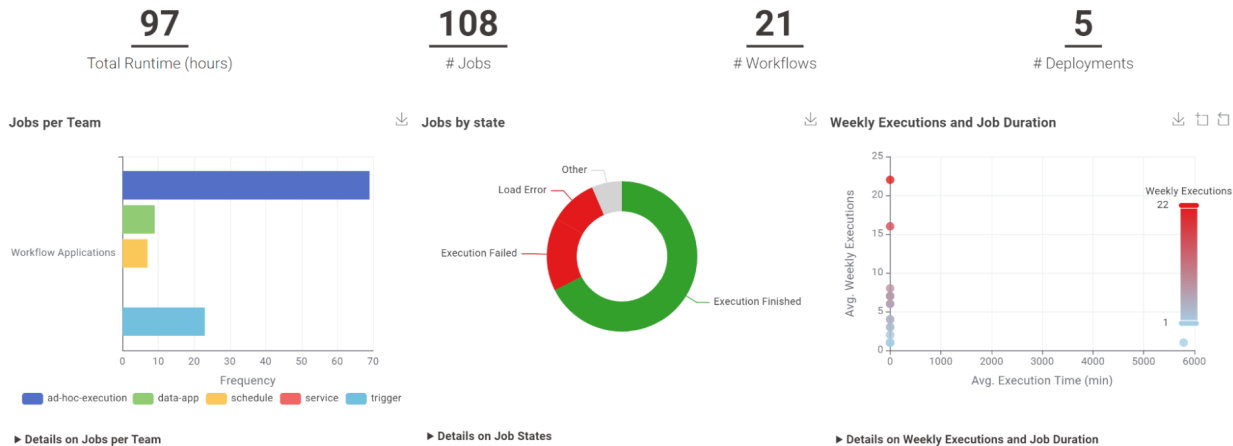


Figure 64. Overview section of the Workflows Jobs Monitoring data application

As you scroll down the Overview page, you will encounter a **Gantt Chart** visually depicting the executions on the current Hub instance. Here, the horizontal axis represents time intervals, while workflows are listed on the Y-axis. The length of each bar is proportional to the duration of the execution across the time axis. Hovering over the bars reveals additional information about the job. By default, the color of the bars corresponds to the job state, but you have the option to customize this setting and color the bars according to teams.

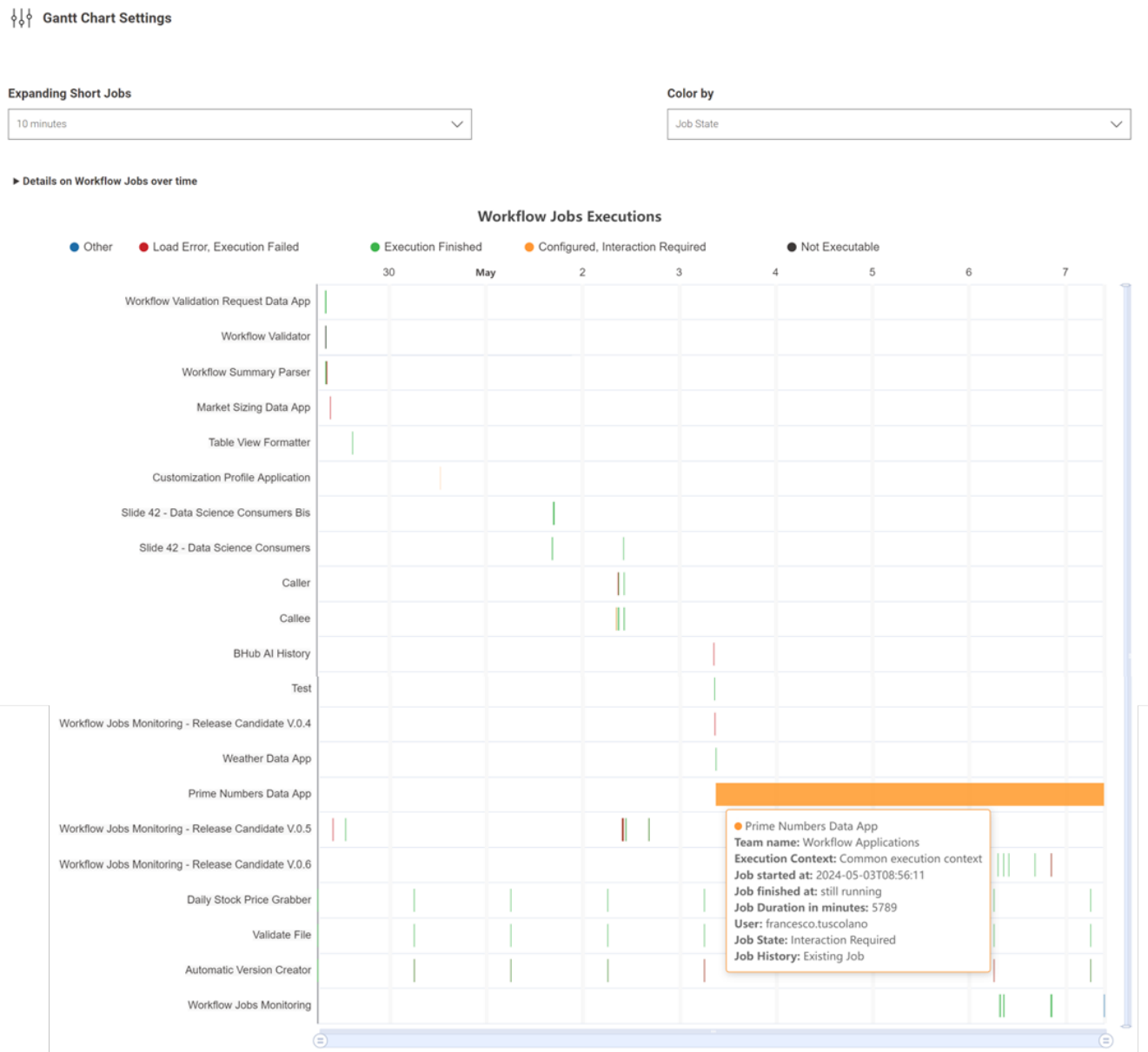
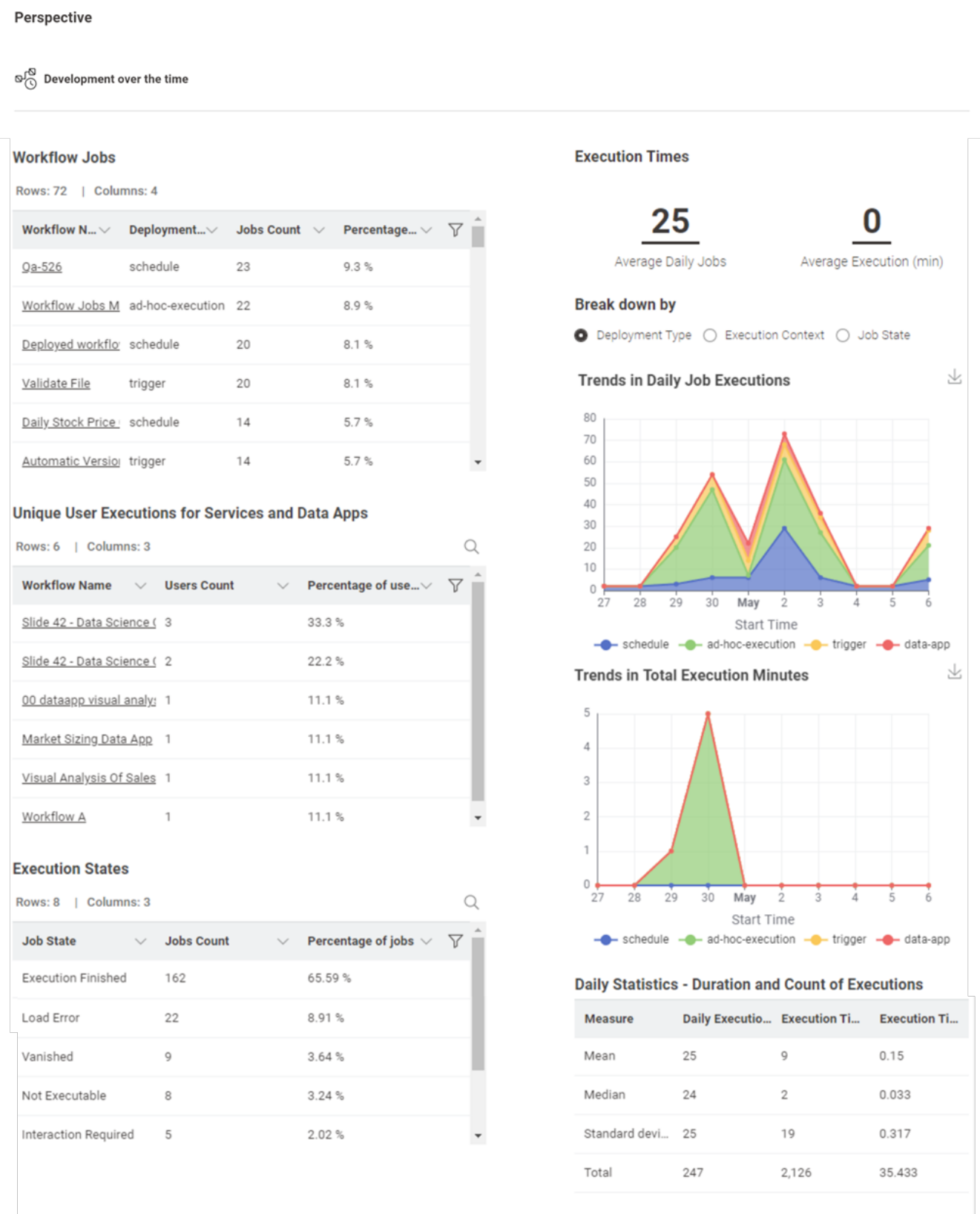


Figure 65. Gantt Chart Settings section of the Workflows Jobs Monitoring data application

Development over the time

This perspective dives deeper into job execution trends over time through a combination of tables and stacked area charts. It provides insights into execution counts, execution times, and highlights the workflows and deployments that are most frequently executed. Stacked area charts are an effective tool for identifying trends in execution. Moreover, we integrated a single selection widget that allows for the breakdown of the charts by three variables of interest, such as Execution Contexts, Deployment types, and teams, facilitating the understanding of resource allocation dynamics. Additionally, the table views feature links that redirect users to the workflows' locations on the Hub, enhancing accessibility and navigation.



List

The final perspective presents the fetched job data in a well-organized table, with all available resources linked and jobs sorted from the most recent to the earliest. This comprehensive list of jobs allows users to inspect every detail for each job, including the workflow name, team, job state, deployment type, duration, and timestamp of the execution. Moreover, if the job is still existing and accessible in the executor, users can open it in the new Job Viewer. Additionally, if the job is a data app in the "Interaction Required" state, users can reopen the data app and, if necessary, terminate the execution to free up memory.

Perspective



Overview Development over Time **List**

List: Includes relevant details for each job in a Table View

97

Total Runtime (hours)

108

Jobs

21

Workflows

5

Deployments

► Details on Job States

Rows: 108 | Columns: 12

Workflow Name	Job State	Team name	Execution Context	Deployment Type	Job Viewer	Open data app	Job Creator	Job Duration (sec)	Job H...	Job started at	
Workflow Jobs Monit...	Executing	Workflow Applic...	Common execution co	ad-hoc-execution	Open Job	Link not available o	francesco.tuscolano	2	Existing Job	2024-05-07 09:2...	Job
Automatic Version Ctr	Execution Failed	Workflow Applic...	5.1.0	trigger	Open Job	Link not available o	francesco.tuscolano	1	Existing Job	2024-05-07 06:0...	2024
Automatic Version Ctr	Execution Finished	Workflow Applic...	5.1.0	trigger	Open Job	Link not available o	francesco.tuscolano	1	Existing Job	2024-05-07 06:0...	2024
Validate File	Execution Finished	Workflow Applic...	5.3.Nightly (2024-05-0	trigger	Open Job	Link not available o	francesco.tuscolano	2	Existing Job	2024-05-07 06:0...	2024
Daily Stock Price Grab	Execution Finished	Workflow Applic...	5.3.Nightly (2024-05-0	schedule	Open Job	Link not available o	francesco.tuscolano	16	Existing Job	2024-05-07 06:0...	2024
Workflow Jobs Monit...	Execution Finished	Workflow Applic...	Common execution co	ad-hoc-execution	Open Job	Link not available o	francesco.tuscolano	7	Existing Job	2024-05-06 20:2...	2024
Workflow Jobs Monit...	Execution Finished	Workflow Applic...	Common execution co	ad-hoc-execution	Open Job	Link not available o	francesco.tuscolano	8	Existing Job	2024-05-06 20:1...	2024
Workflow Jobs Monit...	Execution Finished	Workflow Applic...	Common execution co	ad-hoc-execution	Open Job	Link not available o	francesco.tuscolano	8	Existing Job	2024-05-06 20:1...	2024
Workflow Jobs Monit...	Load Error	Workflow Applic...	5.1.0	ad-hoc-execution	The job has not i	Link not available o	francesco.tuscolano	40	Existing Job	2024-05-06 20:1...	2024
Workflow Jobs Monit...	Execution Finished	Workflow Applic...	Common execution co	ad-hoc-execution	Open Job	Link not available o	francesco.tuscolano	7	Existing Job	2024-05-06 20:09	2024
Workflow Jobs Monit...	Execution Finished	Workflow Applic...	Common execution co	ad-hoc-execution	Open Job	Link not available o	roland.burger@knime.c	13	Existing Job	2024-05-06 16:1...	2024
Workflow Jobs Monit...	Execution Finished	Workflow Applic...	Common execution co	ad-hoc-execution	Open Job	Link not available o	roland.burger@knime.c	15	Existing Job	2024-05-06 09:4...	2024
Workflow Jobs Monit...	Execution Finished	Workflow Applic...	Common execution co	ad-hoc-execution	Open Job	Link not available o	francesco.tuscolano	8	Existing Job	2024-05-06 08:2...	2024
Workflow Jobs Monit...	Execution Finished	Workflow Applic...	Common execution co	ad-hoc-execution	Open Job	Link not available o	roland.burger@knime.c	14	Existing Job	2024-05-06 08:2...	2024

Figure 67. List section of the Workflows Jobs Monitoring data application

KNIME Business Hub API documentation

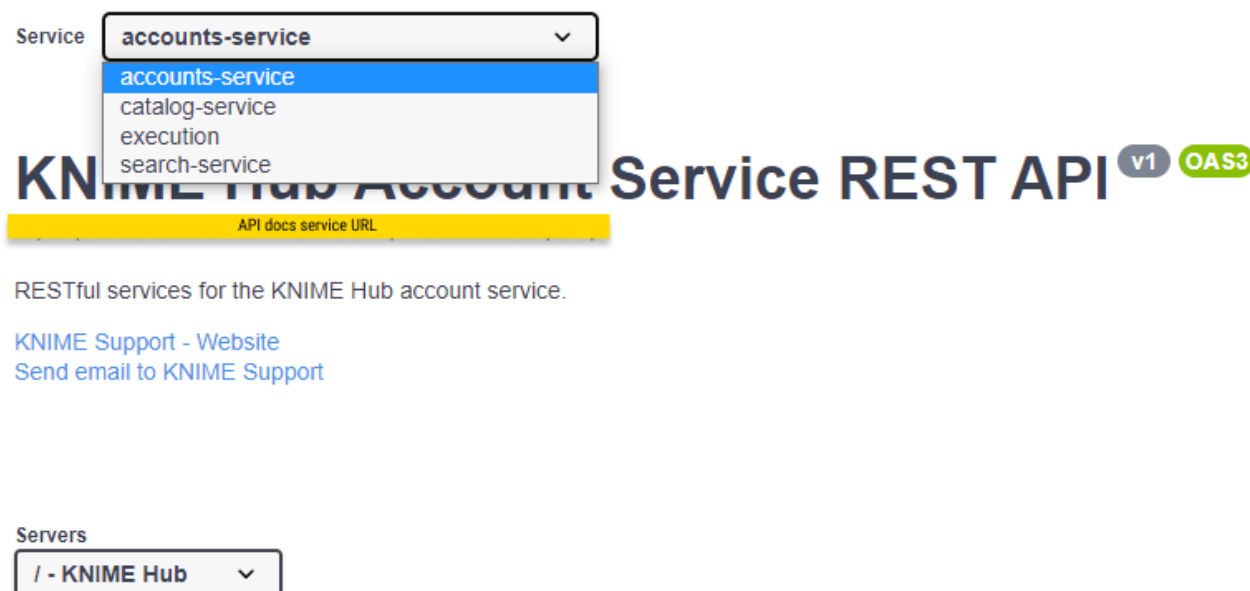
Most KNIME Business Hub functionalities are also available via REST API allowing you to perform several actions.

You can access the API documentation by navigating to the following URL:

```
api.<base-url>/api-doc
```

where `<base-url>` is your Business Hub instance URL, e.g. `hub.example.com`.

Here you can select from the drop-down menu the service you want to use.



Support Bundles and Troubleshooting

When generating a support bundle, **no data leaves the cluster**.

If necessary, you can download the support bundle and send it to KNIME for the purpose of troubleshooting. Contact us by sending an email to support@knime.com. Under extreme circumstances, the KNIME team may forward the support bundle to the Replicated support team for additional help.

When generating a support bundle, a limited amount of information will be automatically redacted (IPv4 addresses, connection strings, etc.). You can configure additional redactions and/or manually redact information prior to sending the bundle. See the **Configuring redaction in support bundles** section for more details.

KNIME Business Hub is capable of generating support bundles in a standard format, even when the admin console isn't working. This ensures that users are able to provide all of the necessary information for KNIME to be able to identify the problem and prescribe a solution.

Generating a support bundle (GUI)

In order to help troubleshoot an installation, or to simply inspect the logs of the cluster in a user-friendly format, you will need to generate a support bundle.

Simply open the KOTS Admin Console, navigate to the **Troubleshoot** pane, and click the **Generate a support bundle** button to generate a support bundle.

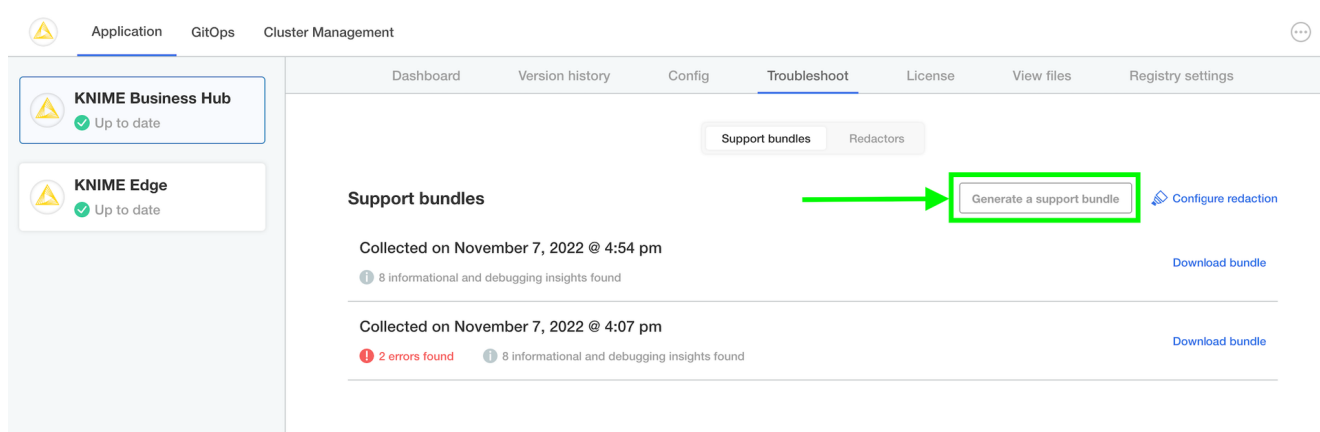


Figure 68. Generate a support bundle

All generated support bundles will display in the list above. Click the **Download bundle** button to download the bundle(s) you want to share with KNIME, and please see the **Configuring redaction in support bundles** section for information on how to redact confidential/personal information before sending.

Generating a support bundle (CLI)

See [Replicated documentation](#) for instructions on how to generate a support bundle via the Replicated CLI.

Configuring redaction in support bundles

When generating a support bundle, a limited amount of information will be automatically redacted (IPv4 addresses, connection strings, etc.) but it is not guaranteed to be a comprehensive set of redactions. You may have additional information in your logs or configuration that you do not wish to share with the KNIME engineering team.

One option is to unzip the generated .zip support bundle and manually review/redact information prior to sending the bundle to KNIME. However, there is a lot of information to review and the redaction of certain information can be automated fairly easily. The ideal option is to configure automated redactions via [Redactor](#) resources, which will automatically redact information for all future support bundles.

In order to configure automated redactors, first open the KOTS Admin Console. Navigate to the **Troubleshoot** pane and click **Configure Redaction**.

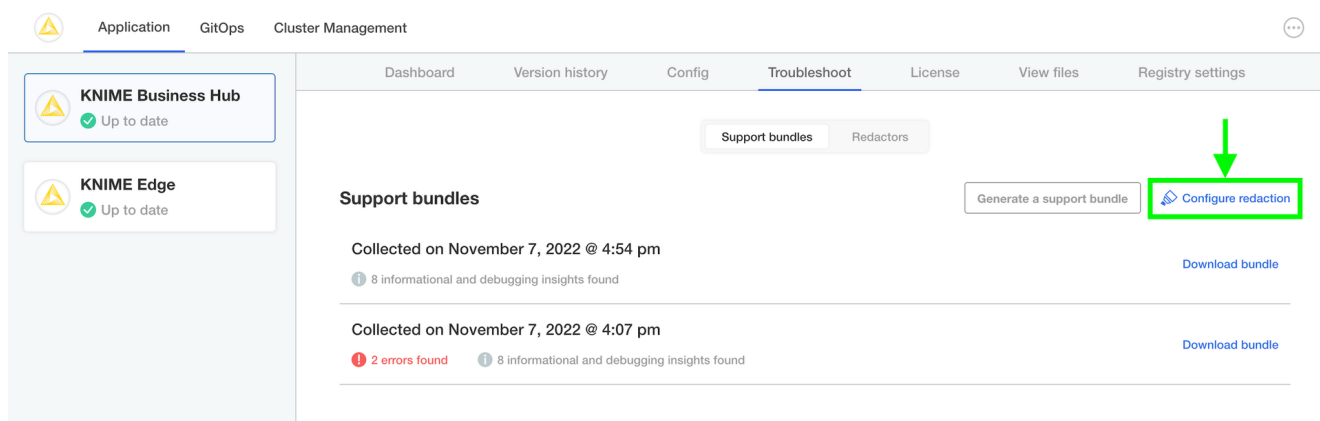


Figure 69. Configure Redaction

If you have configured your own custom redactions that you feel would be valuable to other users of KNIME Business Hub, please feel encouraged to share the configuration with KNIME so that it can be considered & potentially added to future releases.

See [this link](#) and [this link](#) for more information.

Inspecting support bundles

There are quite a number of files generated in a support bundle. Not necessarily every file

is useful for every problem. However, by collecting the same information in the same way each time, KNIME can ensure the best quality support possible for customers.

It is possible to inspect a support bundle entirely in the admin console. See below for an example screenshot.

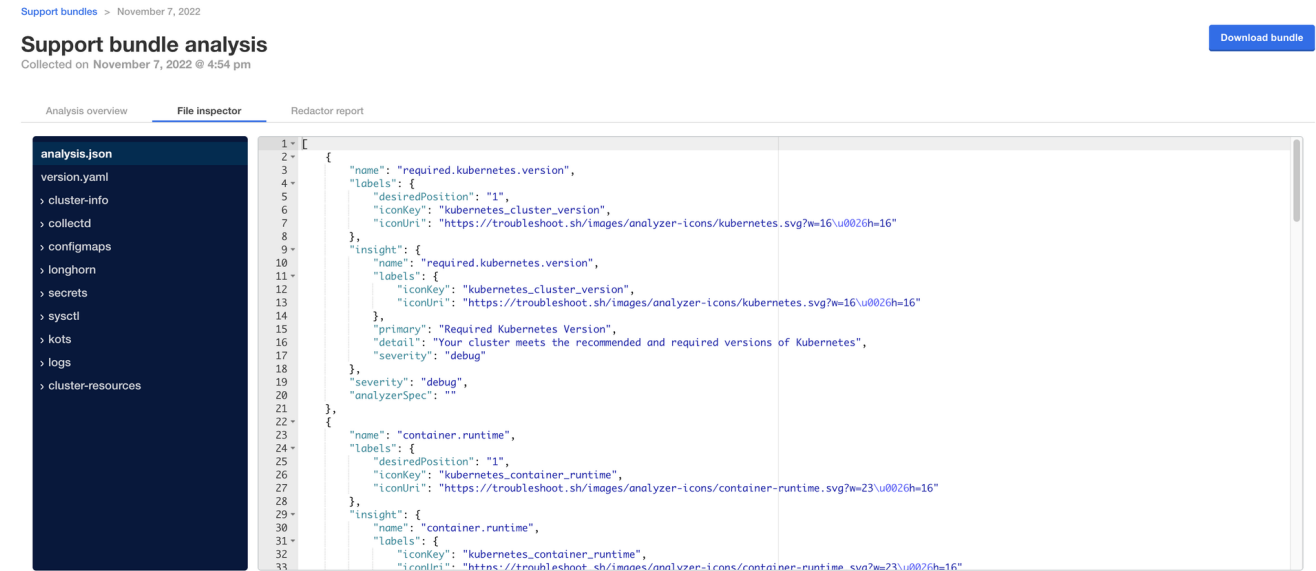


Figure 70. Inspect a support bundle in the admin console

Here are the most important folders/files and their purposes:

Path	Purpose	Example (may have properties omitted)
./analysis.json	<ul style="list-style-type: none"> Collects the highest-level insights possible for the installation. Often times, the issue and/or resolution may be identified in this file by inspecting the <code>[] .name.insight.detail</code> property. 	<pre>[{ "name": "kotsadm.status", "insight": { "name": "kotsadm.status", "primary": "kotsadm Status", "detail": "At least 1 replica of the Admin Console API is running and ready", "severity": "debug" }, "severity": "debug", "analyzerSpec": "" }]</pre>
./logs	<ul style="list-style-type: none"> Contains logs of individual pods. Execution Context logs are stored in <code>./logs/execution-contexts</code>. 	(typical application logs)

Path	Purpose	Example (may have properties omitted)
<code>./cluster-resources</code>	<ul style="list-style-type: none">• Contains the configuration of each visible resource in the cluster.• For example, to see all pods in the cluster, navigate to the <code>./cluster-resources/pods</code> directory which contains one file per namespace in the cluster.	<pre>{ "kind": "PodList", "apiVersion": "v1", "metadata": { "resourceVersion": "1686941" }, "items": [...] }</pre>

Maintenance operations

Restart a node

You might need to reboot a node if you are performing maintenance on the operating system level of the node, e.g. after a kernel update, rebooting the node will apply the changes.

Before rebooting a node on a cluster managed by kURL please call the shutdown script on the node:

```
/opt/ekco/shutdown.sh
```



See more documentation on rebooting nodes [here](#).

Otherwise, after a VM restart old pods might be in `Failed` or `Shutdown` state.

In case that happens, delete the failed pods after the restart with the following command:

```
kubectl delete pod --field-selector=status.phase==Failed --all-namespaces
```

Backup and restore with Velero Snapshots and Kotsadm

Snapshot backups and restore features are available into Replicated deployments via Velero, a tool for backing up Kubernetes cluster resources and persistent volumes.

One-time snapshots as well as automated scheduled snapshots can be managed from the *Snapshots* panel within your Kotsadm dashboard at <https://<base-url>:8800/app/knime-hub>.



Snapshot creation and restoration are disruptive processes. KNIME applications, and Replicated admin access may be unavailable during an active backup or restore operation.

Creating snapshot backups

1. First, configure storage for your backups. Navigate to the *Snapshots* tab of your Kotsadm dashboard. Click the 'Settings' button to edit backup settings where you'll be able to add a storage target.

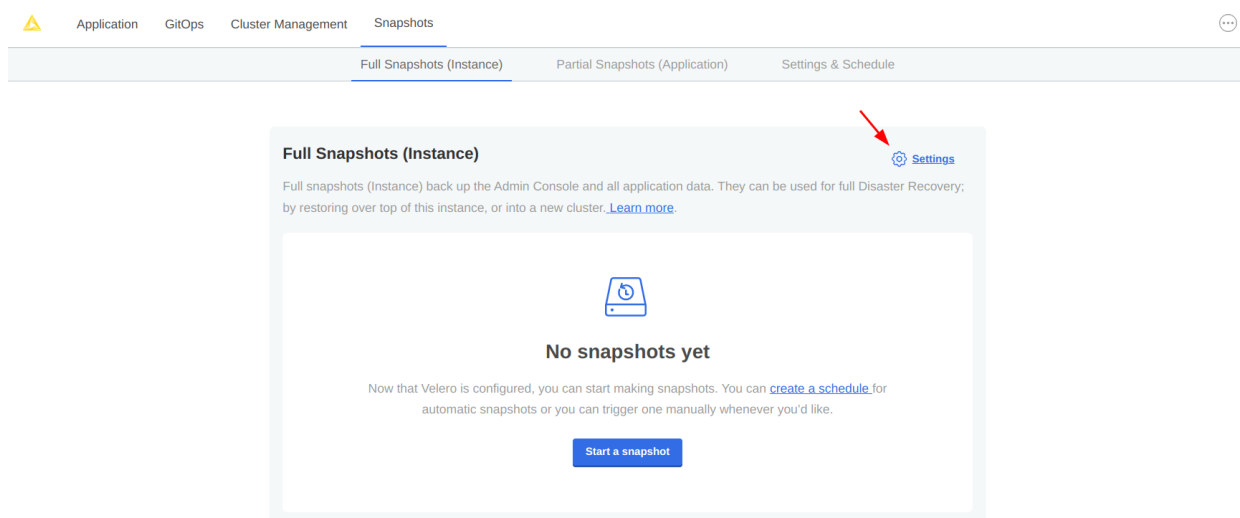


Figure 71. Snapshots tab with settings link

2. Velero supports local storage (not recommended), Amazon S3, Azure Blob Store, Google Cloud Storage, and S3 API compatible storage endpoints such as Minio. Select your preferred snapshot storage type from the 'Destination' drop-down menu, and fill in the required fields with parameters specific to your storage endpoint. Click the 'Update storage settings' button and wait for Velero to verify backup storage access.

Snapshot settings [+ Add a new destination](#)

Full (Instance) and Partial (Application) snapshots share the same Velero configuration and storage destination.

Destination

Amazon S3

Bucket **Region**

business-hub-snapshots us-east-1

Path

/snapshots/

☒ Use IAM Role

[+ Add a CA Certificate](#)

[Update storage settings](#)

All data in your snapshots will be deduplicated. To learn more about how, [check out our docs](#).

Automatic snapshots

Set up a custom schedule and retention policy for automatic snapshots of the Admin Console and all application data.

Full snapshots (Instance) **Partial snapshots (Application)**

☐ Enable automatic scheduled snapshots

Retention policy

The Admin Console can reclaim space by automatically deleting older scheduled snapshots.

Snapshots older than this will be deleted.

1 Months

[Update schedule](#)

Figure 72. Snapshots destination settings for AWS S3 storage

3. With a valid backup storage configured, you can create a Snapshot of your KNIME deployment by clicking the *Full Snapshots* tab, and then the *Start a snapshot* button. This may take a few minutes to complete.
4. Once your snapshot is complete, from the same *Full Snapshots* screen, you can click the 'Settings' button to manage snapshot retention, or configure automatic snapshots by checking the *Enable automatic scheduled snapshots* box and setting a schedule using a CRON expression.

Automatic snapshots

Set up a custom schedule and retention policy for automatic snapshots of the Admin Console and all application data.

Full snapshots (Instance)**Partial snapshots (Application)**

☒ Enable automatic scheduled snapshots

Schedule

Weekly

At 12:00 AM, only on Monday

Cron expression

0 0 * * MON

Retention policy

The Admin Console can reclaim space by automatically deleting older scheduled snapshots.

Snapshots older than this will be deleted.

1

Months

Update schedule

Figure 73. Example automatic snapshot scheduled to run at 12:00am weekly with a 1 month retention policy.

Backup Troubleshooting

Velero is installed into the embedded Kurl Kubernetes cluster with default settings and resource allocations.

© 2023 KNIME AG. All rights reserved.

156

As the number of objects or overall size of data to be backed up increases, it may eventually occur that the CPU and memory resources allocated for Velero processes are no longer sufficient to successfully complete the backup.

In the event that backup failures are encountered, it is recommended to increase the CPU and memory allocation **directly** to the Velero's node agent process via `kubectl`.

```
$ kubectl patch daemonset node-agent -n velero --patch \
'{"spec":{"template":{"spec":{"containers":[{"name": "node-agent", "resources":
{"limits":{"cpu": "2", "memory": "2048Mi"}, "requests": {"cpu": "1", "memory":
"512Mi"}}}]}}}}'
```

The CPU and memory resources and limit values can be adjusted as needed to find sufficient values for backup process. Typically, only the **limit** values will need to be increased.



At this time, the resource allocation override to Velero will **revert** after a Kurl upgrade has been performed. Please ensure any changes to the Velero node agent are reapplied after any Kurl cluster-level upgrades.

Restoring a snapshot

1. Navigate to the list of available snapshot restore points from your Kotsadm dashboard by browsing to *Snapshots* → *Full Snapshots*. From this screen, identify the snapshot instance you would like to use, and take note of the instance ID.

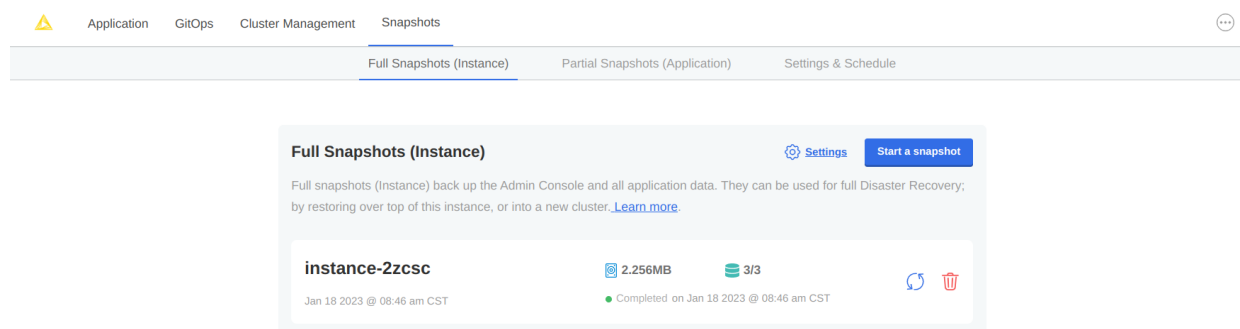


Figure 74. In this example, there is only one snapshot available and its ID is instance-2xcsc

A list of snapshots can also be retrieved by command line:

```
$ kubectl kots get backups
```

NAME	STATUS	ERRORS	WARNINGS	STARTED
instance-2zcsc	Completed	0	0	2023-01-18 14:46:26 +0000 UTC
2023-01-18 14:46:53 +0000 UTC		29d		

2. Now, restore the snapshot using a single CLI command.

```
$ kubectl kots restore --from-backup {Snapshot ID}
```

3. Next, redeploy the Hub instance from the KOTS Admin Console and trigger the restart of all executors by performing any change to each execution context in the Hub UI, e.g. decreasing/increasing the memory.
4. Finally, assuming the restore completed without errors, you can verify your Hub installation is functioning as expected.

Changelog (KNIME Business Hub 1.10)

KNIME Business Hub 1.10.4

(released March 28, 2025)

Security fix

This release resolves a security vulnerability in all prior versions of KNIME Business Hub.

On March 24, 2025, a high-severity vulnerability in the widely used ingress-nginx component for Kubernetes was publicly disclosed. By sending specially crafted HTTP requests from within the cluster to the ingress-nginx controller, attackers could achieve remote code execution. Since ingress-nginx holds access to all cluster credentials, this vulnerability could lead to a full cluster takeover.

For full details, refer to the [KNIME Security Advisory: CVE-2025-2787](#).

KNIME Business Hub 1.10.3

(released March 20, 2025)

Security fix

This release addresses a security vulnerability affecting all previous versions of KNIME Business Hub. We've identified that the existing Kubernetes secret configuration could potentially allow parties with specific credential knowledge to interact with job-related data on accessible KNIME Business Hub installations.

For more details, see the [KNIME Security Advisory: CVE-2025-2402](#).

KNIME Business Hub 1.10.2

(released July 9, 2024)



Important note: Updates from Business Hub 1.10.x versions are **highly** recommended, as critical issues were fixed in this release.

Important Bugfixes

- Fixed an issue with memory allocation to Artemis (managing job queues for execution) that could cause failure of Business Hub.
- Fixed an issue where jobs instrumentation (historical job collection) could fail because of late messages and cause failure of Business Hub.

KNIME Business Hub 1.10.1

(released June 4, 2024)

Improvements

Data App: Manage All Existing Jobs

- Data App to list all existing jobs with the possibility to delete them as well. Can be used to monitor the current execution situation on the Hub.
- Data App: https://hub.knime.com/-/spaces/-/~hOk0b0SsNX6_eAoh/most-recent/
- Docs: https://docs.knime.com/latest/business_hub_admin_guide/index.html#manage-all-existing-jobs

Data App: Assign Users to Teams based on External Groups

- Convenience Data App to link Groups (e.g. managed by SCIM) to Teams.
- Data App: <https://hub.knime.com/-/spaces/-/~aRbyzgd02lkbB60j/most-recent/>
- Docs: https://docs.knime.com/latest/business_hub_admin_guide/index.html#scim-users-teams-data-application



Users sync from identity provider to Hub teams via SCIM is an Enterprise edition only feature.

Data App: Executor Image Builder

- As the successor of the Execution Context Dockerfile Builder, the **Executor Image Builder Data Application** is designed to further ease the creation of Executor Images by employing the Image Builder Service that comes with KNIME Business Hub 1.10. This eliminates the need for manual docker image building on local machines, and instead

allows easy installation of extensions or additional software like python to an Executor Image. The Executor Image is automatically pushed to a given registry (embedded, or configured in the Admin Portal) so that it is available for Global Admins and Team Admins so that they can create Execution Contexts from the Image. Detailed [documentation](#) can be found in the Docker executor images section of the KNIME Hub Admin Guide.

Other

- Airgapped bundles now come with KNIME Analytics Platform 5.2.5 as executor.

Bugfixes

- Fixed a bug where the job viewer feature doesn't work on certain domains
- Added license support for GCP marketplace images
- Fixed a bug when sharing a secret with a team
- Fixed a bug in Kerberos impersonation when connecting to an on-premise cluster

KNIME Business Hub 1.10.0

(released May 22, 2024)

Important changes (please read carefully)

- The KOTS App Manager is now on version 1.108.9. This new version fixes an important CVE and provides new functionalities, so it has to be updated **before** updating to KNIME Business Hub version 1.10.
 - To do so use the following command: `curl -sSL https://curl.sh/knime-hub | sudo bash.`
- The Kurl update will result in a **downtime of approximately 60 min.** Please plan your update window accordingly.
- Email addresses are now allowed as usernames. In case you had a Keycloak mapper configured that strips the domain portion of the username, this mapper can now be removed.
 - **Caution:** For the time being, do not remove the mapper if you are using Kerberos authentication in KNIME Analytics Platform. A fix for this will be provided in the next feature or bugfix release.

- We changed the way groups in teams are managed. This change is only important for customers who added "guest members" to their teams to grant them access to individual spaces. If you are **not** doing this, please just skip the bullet point below.
 - Previously, it was possible for a user to be in a team without belonging to any of the team's groups ("admin" and "member" by default). Now, a user is considered a part of a team as long as they are in **any** of the team's groups. Therefore, having guest members by simply adding a user to a team, and then removing them from all groups is not possible anymore. To still achieve the same result, you need to add a new custom group to your team, to which the guest users are then added. Please reach out to support@knime.com to get assistance with this.
- In case you are updating from Business Hub 1.8.x, Keycloak will be updated as well, resulting in a changed password to access the Keycloak admin portal. Please find the new password in a Kubernetes secret called credential-knime-keycloak in the knime namespace. If you have created additional Keycloak admins, they will be deleted as part of the update.
- For customers using the external group sharing feature, the user-attribute mapper for external groups needs to be switched to userinfo-only. Please refer to the [updated documentation](#).
- Airgapped bundles now come with KNIME Analytics Platform 5.2.3 as executor.

Improvements

- Group-to-team sync via SCIM (Enterprise edition only): Automatically sync groups from your identity provider to Business Hub teams. Changes on the identity provider side will reflect in Business Hub, making it easier for IT to onboard many users. ([See documentation](#))
 - **Note:** In case you are using Kerberos authentication in KNIME Analytics Platform and if you are using a Keycloak mapper that strips the domain part from user names, do not set up SCIM yet. A fix for this will be provided in the next release.
- Job instrumentation: This feature keeps a record of every single job that is executed on Business Hub, allowing users to analyze Hub usage over time. By default, records are kept for 30 days. This value can be adjusted in the KOTS admin console. ([See documentation](#))
 - A data app to access this data is published [here](#). Please upload this to your own Business Hub installation.
- Job viewer: Users are able to inspect a job at its current state in a browser based read only mode, without the need to open their local KNIME Analytics Platform. This is possible for jobs that were created by an "Ad hoc execution" as well as from a

“Deployment”. Usage of this features requires a KNIME Analytics Platform 5.2.3 or newer to be used as hub executor. ([See documentation](#))

- **Note:** In order to use the job viewer feature, load balancers / proxies in front of Business Hub need to be websocket compatible, and the ws.<baseurl> DNS entry needs to be set up as its shown on the KOTS admin console.
- Scalable data app sharing: Share data apps at scale via a special link and run them without the need to log in for end users. ([See documentation](#))
- Secret store adds a new secret type for secure sharing of files e.g. ssh key files. ([See documentation](#))

Security Updates

- Minimal RBAC Kots install supported ([See documentation](#))
- Advanced installation now supports setting up Kots with limited RBAC permissions
- PostgreSQL no longer requires privilege escalation to be enabled
- fsGroups and supplementalGroups are now set for every container (exceptions are PostgreSQL, Istio and Ingress-Nginx)
- Namespace-metadata-reader Cluster Role converted into a Role

Kurl update

- Kurl stack updated
- Contains various CVE fixes
- Embedded clusters updated to Kubernetes version 1.27.12

Support bundle updates

- Support bundles now indicate missing required resources in the Hub cluster

Important Bug Fixes

- Fix showing a correct “License expired” message in the UI
- Fixed a bug where application password creation for consumers was broken
- Infrastructure fixes:
 - Excluding Istio from the install (for provided Istio / OpenShift Service Mesh) no

longer requires a developer license

- Fixed a bug where some init containers weren't compatible with Istio CNI
- Fixed a copy permission error in the Keycloak init container that caused issues with updates to Business Hub version 1.9.0
- Backup / Restore fixes:
 - Postgres admin password wasn't restored in some cases
 - Timeouts increased for large data volume backups / restores
- Fixed a bug where Keycloak wasn't compatible with custom certificate authorities
- Fixed a bug where the ImagePullSecret was not set for Keycloak in some air gapped, embedded cluster installations
- Keycloak migration improved when updating from Business Hub 1.8.3 or lower versions
- Various fixes for OpenShift installs
- Compatibility with OpenShift Service Mesh improved

Changelog (KNIME Business Hub 1.9)

KNIME Business Hub 1.9.0

(released April 10, 2024)

Installation notes

Due to the Keycloak version update, Keycloak admin credentials will change during the update process.

The new credentials can be retrieved from the same secret as during the first install of Business Hub: [KNIME Business Hub Installation Guide](#)



KNIME Business Hub 1.9.0 includes the Docker executor image:
`registry.hub.knime.com/knime/knime-full:r-5.2.3-477.`

Improvements

- Expanded support for secret types, including OAuth2 and authentication mechanisms from Box, Google, and Microsoft

- New landing page that highlights relevant links for faster onboarding of users
- ElasticSearch has been updated to 8.5.1
- Keycloak has been updated to 23.0.5
- Added support for installing Business Hub on OpenShift
- Added support for Kubernetes 1.29
- Migrated UI framework to nuxt3

Changelog (KNIME Business Hub 1.8)

KNIME Business Hub 1.8.3

(released March 26, 2024)

Improvements

- Update Artemis to 2.32.0

Important Bug Fixes

- Fixed a bug where Image pull secret are not set anymore for executors in embedded registry
- Fixed license check for Azure marketplace images
- Fixed exposing of workflow paths in shared deployments

KNIME Business Hub 1.8.2

(released March 05, 2024)

Installation notes

- During the update a short downtime is expected (5-10 minutes).

Improvements

- In existing cluster installations Kubernetes Namespaces can now be created before the installation happens, in compliance with IT security standards.
- Enabled additional security context policies for multiple 3rd party tools. List of policies enabled:
 - require-node-affinity
 - disallow-capabilities
 - disallow-host-namespaces
 - disallow-host-path-volumes
 - disallow-host-ports
 - disallow-privileged-containers
 - require-non-root-groups
 - require-run-as-nonroot
 - disallow-host-process
 - disallow-latest-tag
 - disallow-proc-mount
 - require-drop-all-capabilities
 - require-read-only-root-filesystem

Important Bug Fixes

- Fixed a bug where the Velero restore process could show incomplete because of timing issues with Minio.
- Fixed a bug where editing a schedule that has credentials stored corrupted the credentials

KNIME Business Hub 1.8.1

(released February 15, 2024)

Improvements

Allow routing temp data to customer-defined volume

- Helps eliminate disk pressure in situations where large amounts of data need to be cached from jobs during execution.

Optionally set node affinity to required

- Set node affinity to be required so that users can ensure that no hub components are scheduled onto a node that does not have a particular label.

Enable Rook on Airgap HA installation

- Airgap installations now support multi-node setups with Rook.

Support external groups sharing for users in more than 200 groups

- AAD removes groups from the access token of the user is in more than 200 groups. This feature allows customers to still retrieve the groups in these cases.

Important Bug Fixes

- Fixed a bug that occurred when multiple accounts are created concurrently
- Fixed various bugs that impaired first installs on airgapped environments

Important Notes

- Some advanced settings are now hidden in the KOTS Admin Console config by default. To view them enable the *View Advanced Settings* option in the Global section at the top.

KNIME Business Hub 1.8.0

(released December 20, 2023)



KNIME Business Hub 1.8.0 includes the Docker executor image:
`registry.hub.knime.com/knime/knime-full:r-5.1.2-433`.

New features

AI Service (Business Hub Enterprise)

- Gives you control over, who the data going through the KNIME AI Assistant is shared with.
- Configured via the KOTS Admin Console
- Supports OpenAI and Azure OpenAI as LLM provider
- No data is shared with KNIME
- AP Users can connect their KNIME AI Assistant to the AI Service of a Business Hub via the KNIME AI Assistant preference page
- AI history service grants admins access to all requests made by their AP users to the KNIME AI Assistant
- Documentation: [KNIME Business Hub Installation Guide](#)

Secret Store (Business Hub Standard & Enterprise)

- Central location to manage personal and team secrets
 - Sharing of team secrets with other users or teams
 - No more logins stored in KNIME workflows
 - Secret management is done in the KNIME Business Hub
 - Secret Retriever node allows users to use secrets within KNIME workflows
- Documentation: [KNIME Business Hub User Guide](#)

Start data apps with parameters via URL

- Send customized data app links that trigger link/user-specific behavior inside the data app
- Needs a Container Input (JSON) node inside the workflow
- Documentation: [KNIME Business Hub User Guide](#)

Infrastructure updates

Minimize use of cluster roles

- There are no more cluster roles in services developed by KNIME
- Circumventing the use of cluster roles in 3rd party tools used by Business Hub will be introduced in a later release (where possible)

Backup / restore via Velero

- Stability improvements

Improvements

- Added display of CPU and RAM usage of execution contexts
- Search results indicate versioned and draft items
- Admin console now displays Business Hub version

Important bug fixes

- Date-times are now displayed in the browser's timezone
- Execution context selection list not showing all available execution contexts for deployments and ad-hoc execution, improved UX
- Fixed download button for previous workflow versions
- Fixed a bug where in some cases endless loading state could occur while editing schedules
- Fixed a bug where in some scenarios deployments could be created on disabled execution contexts
- Various other bug fixes

Changelog (KNIME Business Hub 1.7)

KNIME Business Hub 1.7.0

(released November 06, 2023)

Important installation notes

Kubernetes version 1.25-1.27 is required for Business Hub 1.7.0. Pre-flight checks in the installer make sure that the correct version is available.

Infrastructure and security updates

Support provided ingress-nginx deployments

- In existing clusters creating own ingress-nginx deployments before the installation of Hub is now enabled. Whether the Hub install process deploys the inbuilt ingress-nginx can be configured on the Kots Admin dashboard.

Security context update

- Security contexts updated for pods, containers and jobs in the hub, knime and knime-execution namespaces.

Bug Fixes

- Fixed a bug where schedules edited with KNIME Analytics Platform didn't respect job discard settings.
- Fixed a bug where saving executed job as workflows didn't work in case workflow size was larger than 50 MB.
- Fixed a bug where under certain circumstances jobs were shown duplicated in the AP explorer.
- Fixed a bug where schedules in all teams connected to a user were deactivated when the user left any team.
- Various smaller fixes.

Changelog (KNIME Business Hub 1.6)

KNIME Business Hub 1.6.0

(released September 22, 2023)

Important installation notes

Business Hub 1.6.0 comes with Kubernetes 1.25 for the embedded clusters.

We recommend updating by running the Kubernetes installer command:

```
curl -sSL https://kurl.sh/knime-hub | sudo bash
```



Run the command only when updating from KNIME Business Hub version 1.5.2 or higher, or **after** you updated to version 1.6.0.

All pods will restart during the update, some downtime is expected. Creating a backup before upgrading is recommended.

New Features

Save jobs to spaces

- Jobs on KNIME Business Hub can now be saved any space where the user has permissions. Great feature to utilize for fixing a faulty job and saving the results for the future.
- Documentation: [KNIME Business Hub User Guide](#)

Shared execution contexts

- Create shared execution contexts, that allow sharing execution resources between multiple teams. Shared execution contexts are setup and maintained by the Hub admin and utilized on Team level.
- Documentation: [KNIME Business Hub Admin Guide](#)

Execution context redesign

- Improved usability of execution resource management based on customer feedback. Current job list is now available on execution context and executor level.

Auto start-stop of execution contexts

- Save money on infrastructure costs by only starting up your execution resources when they are actually used, and by shutting them down afterwards.

- Auto start-stop can be enabled for each execution context separately.

Download job logs

- Downloading job logs is now available from the Hub user interface.
- To use this feature an executor based on KNIME Analytics Platform version > 5.1 is necessary.
- Documentation: [KNIME Business Hub User Guide](#)

Improvements

Triggers listening to version creation

- It is now possible to trigger deployments when a new workflow version is created.
- Documentation: [KNIME Business Hub User Guide](#)

Deprecated nodes are not part of search results

Infrastructure updates

Embedded clusters updated

- New Kubernetes version for embedded clusters is 1.25

Kubernetes node affinity

- Node affinity available to separate execution resources from Hub core services
- Documentation: [KNIME Business Hub Admin Guide](#)

Important Bug Fixes

- Fixed a bug where two trigger deployments triggered at the same time could produce inconsistent results
- Fixed faulty URLs on the API documentation

- Fixed KNIME AP mount point registration https problem
- Fixed an issue where global proxy settings could break executor functionality
- Fixed an issue where Hub could get into a crash loop with many APs connected and large files being uploaded / downloaded at the same time

Changelog (KNIME Business Hub 1.5)

KNIME Business Hub 1.5.2

(released Aug 14, 2023)

Important installation notes

Postgres will restart during the update, short downtime is expected.

Infrastructure updates

KNIME Business Hub is now compatible with Kubernetes 1.25.

KNIME Business Hub 1.5.1

(released July 27, 2023)

Important Bugfixes

- **HUB-5628** Fixed an issue that prevented the creation of disabled schedules. Impacting KNIME Server to Hub migration.
- **HUB-5649** Fixed a bug that prevented notification service updates when a subscription for a deleted user was present.
- Fixed a configuration issue that caused the trigger-service to not start up in some scenarios.

KNIME Business Hub 1.5.0

(released July 17, 2023)

Important installation notes

All executor pods will restart during the update, some downtime is expected. Creating a backup before upgrading is recommended.

New Features

Item level versioning

- Item level versioning has been introduced with Hub 1.5.0
- Users can create / restore / delete versions of individual items
- Item versions can be utilized in Ad hoc execution, Deployments
- Using KNIME Analytics Platform 5.1 users can leverage item level versioning for Ad hoc execution, sharing component links and use new nodes like the "Version Creator"
- Space level versioning has been deprecated
- All items in previously versioned spaces are automatically migrated to be versioned on item level upon updating

Volume Mount support for Execution Contexts

- Kubernetes volumes can now be attached to Execution Contexts by editing the custom resource definition.
- This allows attaching secrets and config maps as files to Execution Contexts.

Improvements

Keycloak enforces username validation

- Username restrictions described in the [KNIME Business Hub Installation Guide](#) are now enforced by KNIME Business Hub's identity provider Keycloak. Preventing problems where users could be synced into Hub but they could not login with their credentials.

Notifications redesign

- KNIME Business Hub UI notifications were redesigned to be less intrusive and to be more convenient for users.

Schedule deployment

- Initial start date of schedules can no longer be in the past.

Space permissions

- Users with viewer permission can no longer delete spaces

Infrastructure updates

Artemis update

- Artemis version has been updated to 2.29.0

Quarkus update

- Quarkus has been updated to 3.1.1 in the execution services

Execution Context security hardening

- Execution Contexts now have a more restrictive security context to help prevent containers from escalating privileges and prevent running as root user. This increases compliance with typical enterprise cluster security policies enforced with tools such as Kyverno.

Important BugFixes

- **HUB-4991** - Fixed a bug where users were not able to execute deployments shared with them, if they didn't have access to the deployed workflow.
- **HUB-5396** - Fixed the state persistor issue that could result in timeouts and various problems in workflow execution on the Hub.

Changelog (KNIME Business Hub 1.4)

KNIME Business Hub 1.4.2

Main motivation for the 1.4.2 KNIME Business Hub release is to prepare for the upcoming 5.1 KNIME Analytics Platform release. It is an optional update as 1.5.0 Business Hub is coming out with all new features before AP 5.1.

Improvements

Support for using KNIME Analytics Platform 5.1 as a workflow editor. Compatibility with uploading workflows to the Hub using KNIME AP 5.1.

Important Bugfix

- **HUB-5396** - Fixed the state persistor issue that could result in timeouts and various problems in workflow execution on the Hub.

KNIME Business Hub 1.4.1

Important Bugfixes

- **Fix Bug** disabled functionalities for interacting with components in the HUB from AP versions (4.7.0, 4.7.1, 4. 7.2, 4.7.3, 5.0.0) affected by a bug in which saving shared components might delete local workspaces
- Listing HUB spaces from affected AP versions will return the components as data objects, which don't have the potential to trigger the bug, but limits the use of components.
- Changed file extension for downloading components from .knwf to .knar.

KNIME Business Hub 1.4.0

Important installation notes

Please calculate with some downtime during which some services might not be available.

New Features

Data apps

Share data app deployments with "any signed in user"

You can now share your data apps with every Hub user in your company with one setting. Data app deployments shared this way will be available in every user's data apps portal.

Share data app deployments with external groups

Sharing data app deployments with users from externally managed groups (e.g. LDAP/AD groups) is now available. This is done by either importing LDAP groups to Keycloak, or by connecting Keycloak to an external OIDC provider, which provides groups through the access token. Usage of such external groups is for sharing of data app deployments only. The actual users who run the deployments are still managed within KNIME Business Hub.

Data Apps Portal UX enhancements

Enhanced the visual design and user experience of the data apps portal, enabling the addition of categories and descriptions to data apps. This enhancement allows data app consumers to effortlessly filter and identify relevant data apps based on their category and description.

Content Security Policy for data apps

Admins of KNIME Business Hub can now set custom Content Security Policies for data apps, to restrict which resources, from where can be loaded into the data app's user's browser. See more in: [Business Hub Admin Guide](#).

Deployments

Editing deployments

Recreating deployments is no longer needed just to change their configuration.

Admin functionality

Backup / restore via Velero

KNIME Business Hub is now complemented with the widely used, open-source backup / restore tool: Velero. You can mitigate the risk of serious data loss by setting up a backup schedule. The backup process does not require any downtime.

X-Frame-Options Header

Now admins can also select from different X-Frame-Options header options, to prevent clickjacking attacks. See more in: [Business Hub Admin Guide](#).

Security

Improved security by removing sensitive information shown in the HTML source code.

Edge

KNIME Edge integration

KNIME Edge 1.3 is now compatible with KNIME Business Hub 1.4.

Important Bugfixes

- HUB-4774: Next execution time for schedules repeating every 24 hours cannot be computed
- HUB-5093: Heap size calculation doesn't work on Ubuntu 22.04 (Cgroups V2), leading to a too low limit being set for various services

Changelog (KNIME Business Hub 1.3.0)

KNIME Business Hub 1.3.0

(released April 03, 2023)

Important installation notes

- With the release of KNIME Business Hub 1.3.0 new security features are introduced regarding executor communication. For this reason, KNIME Business Hub requires every executor to be on Analytics Platform version 4.7.1 or higher. You can find a list of the available executor images [here](#).
- With this release we changed the istio configuration of two services, to allow them to see the IP of the caller if the request is coming from within the cluster. This can cause those two services (`keycloak-proxy`, `s3-proxy`) to not start up in some scenarios, with a "too many open files" error in the istio-proxy container of those pods. This can be fixed by increasing the open file limit on the host VM, e.g. by running the following command:
`sudo sysctl fs.inotify.max_user_instances=8192.`
- The KOTS App Manager is now on version 1.96.3. This new version fixes an important bug, so it should be updated before updating to KNIME Business Hub version 1. 3. To do so use the following command:
`curl -sSL https://kurl.sh/knime-hub | sudo bash.`

- If you haven't updated to KNIME Business Hub 1.2.0, yet, you need to follow update guide in the [changelog](#) for 1.2.0 before updating to 1.3.

New Features

Molecule sketcher

Use the new Molecule Widget (Labs) node to accept molecule input from your users. With this new node we made the integration of different sketchers easier and allowed to provide different sketchers also for the KNIME Analytics Platform. In this release the ketcher sketcher is included. Additional sketchers will follow in the upcoming releases.

Collections

Introduce your users to a topic using collection pages. Collection pages serve as a starting point for your users to explore examples and building blocks related to your chosen topic, facilitating their onboarding process. To start creating collections read our guide [here](#).

KNIME Analytics Platform customization profiles

Use Business Hub to distribute preference profiles to either local Analytics Platform clients or to KNIME Hub executors. This can be used to e.g. easily ship database drivers. More information about Analytics Platform customization profiles [here](#).

Trigger deployment

Trigger is a powerful new type of deployment which allows automating workflow execution based on specific conditions, such as another workflow or component being added or removed to a space. To get started with Triggers, check out our documentation [here](#).

Changelog (KNIME Business Hub 1.2.0)

KNIME Business Hub 1.2.0

(released March 13, 2023)

KNIME Business Hub 1.1.1 to 1.2.0 Upgrade

- KNIME Business Hub 1.2.0 is expected to run in a Kubernetes 1.23.x cluster. Prior versions of KNIME Business Hub ran in Kubernetes 1.21.x clusters.
- For embedded kurl cluster installations, the cluster update process is to:

- First, check for updates in KOTS Admin Console.
- Once the KNIME Business Hub 1.2.0 update has been identified and preflight checks have been run, trigger the deployment.
- After the deployment process has completed, run the following command in the terminal of the host machine to upgrade the Kubernetes cluster version (among other components):
 - `curl -sSL https://kurl.sh/knime-hub | sudo bash`
 - You will have to enter y to various yes/no prompts during this upgrade process.

New Features

- New supported Kubernetes versions: 1.22, 1.23, 1.24
- Keycloak version updated to 19.0.3, see Keycloak documentation: https://www.keycloak.org/docs/19.0.3/server_admin/
- Support for airgapped environments: Installing KNIME Business Hub in environments with no internet connection. Install instructions: https://docs.knime.com/latest/business_hub_installation_guide/index.html#_introduction
- Embedded docker registry for custom executor images: Embedded cluster installations using kURL now contain an embedded docker registry for storing custom executor images. Documentation: https://docs.knime.com/latest/business_hub_installation_guide/index.html#embedded-docker-registry-configuration
- Recreate strategy for Execution contexts: For upgrading execution contexts now rolling updates and recreate strategies are both available.
- Support for custom certificate authorities

Bugfixes

- Removed the unused ipv6 listener in the Business User Portal container, that could cause crashes in some environments

KNIME AG
Talacker 50
8001 Zurich, Switzerland
www.knime.com
info@knime.com