

# KNIME Business Hub Admin Workflows Guide

KNIME AG, Zurich, Switzerland Version 1.14 (last updated on )

# **Table of Contents**

Use cases
Monitoring
Diagnostics
Maintenance
Admin Dashboard
Setup
Workflow Jobs Monitoring
Enable Job Instrumentation data collection5
Setup
User Usage Monitoring
Keycloak Service Client configuration
Setup
Gen Al Monitoring
Enable AI Services
Setup
Executor Diagnostics
Setup
Manage Existing Jobs
Setup
Manage Workflow Versions
Setup

In this guide you will find tools that help you monitor, diagnose, and maintain your Business Hub. It is intended for anyone administrating the whole Hub or a Team on the Hub.

## Use cases

### Monitoring

- User & Team activity: Analyze how users interact with the system, including active logins, team distribution, and access methods with the Admin Dashboard for a general overview and the Monitor Users Usage data app for a detailed session investigation.
- **Resource utilization**: Assess execution contexts, workflow scheduling, and resource scaling to optimize performance with the Admin Dashboard for a general overview and the Workflow Jobs Monitoring data app for details on workflow execution.
- **Content & Storage Management**: Identify large items, popular downloads, and opportunities for space optimization with the Admin Dashboard.
- **Performance & Reliability**: Monitor workflow execution trends, failures, and overall execution efficiency with the Workflow Jobs Monitoring data app.
- Gen Al & Assistance usage: Measure engagement with K-AI, script assistance, and user support needs with the Gen Al Monitoring data app.

### Diagnostics

- List execution context capabilities: List installed extensions, nodes, conda environments, and Linux packages with the Executor Diagnostics data app.
- **Check URL accessibility:** Identify if a given URL is reachable from the execution context on the "Proxy"-perspective of the Executor Diagnostics data app.
- **Investiate network issues:** Check if the execution context is blocked for example by a faulty proxy configuration by entering a URL in the "Proxy"-perspective of the Executor Diagnostics data app.
- **Inspect active worklfow executions**: List all jobs that are still active or inspectable with the Manage Existing Jobs data app.

### Maintenance

• Free up disk space: Delete unused versions of workflows with the Manage Item Versions data app or delete old workflow executions with the Manage Existing Jobs data app.

# Admin Dashboard

The Admin Dashboard data app covers the following use cases:

- **Investigate user, item, and deployment distribution**: Analyze the distribution of users, items (workflows, components, files), and deployments in your Business Hub and across teams.
- **Trends and growth**: Monitor the growth of new users, new items, and new deployments over time.
- **Hub snapshot**: As a global admin, get a snapshot of the Hub, including anonymized information about the number of users, items, and deployments to compare growth over a longer time period or compare different Hub instances.

- 1. Download the workflow
- 2. Navigate to the space on your Hub where you want to upload the workflow to
- 3. Use the upload button to upload the workflow (learn more)
- 4. Run the workflow to start an ad hoc execution (learn more)
  - Optional: Instead, deploy the workflow as a data app to persist any configuration and make it available to others by sharing the deployment (learn how).
- 5. Optional: impersonate another user or configure another Hub in the configuration panel shown in Figure 1.
  - User application password: specify the user you want to impersonate.
    - "Current" (default) for the currently logged in user. The password is not needed.
    - Application password of the user you want to impersonate. This allows you to use permissions of another user.
  - $\,\circ\,$  Hub URL: specify the Hub you want the data app to refer to.
    - "Current" (default) for the Hub on which the execution takes place.
    - The URL of the other Hub you want to refer to.

Control the parametrization of the workflow execution.

Hub URL

Current

User application password (No password needed if "Current")

Current

Password

Figure 1. Hub URL and user application password configuration.

# Workflow Jobs Monitoring

The Workflow Jobs Monitoring data app covers the following use cases:

- Schedule optimization: Find times where execution contexts are less busy for performant scheduling.
- **Performance & reliability**: Track workflow execution trends, identify failures, and assess overall efficiency to ensure optimal performance.
- Investigate individual jobs: Find, understand, and inspect jobs that have failed or are taking longer than expected.

### Enable Job Instrumentation data collection

The data app requires **job intrumentation data** to be collected and stored to. For that, you need to enable the job instrumentation data collection as described here.

- 1. Download the workflow
- 2. Navigate to the space on your Hub where you want to upload the workflow to
- 3. Use the upload button to upload the workflow (learn more)
- 4. *Run* the workflow to start an ad hoc execution (learn more)
  - Optional: Instead, deploy the workflow as a data app to persist any configuration and make it available to others by sharing the deployment (learn how).
- 5. Optional: impersonate another user or configure another Hub in the configuration panel shown in Figure 2.
  - User application password: specify the user you want to impersonate.
    - "Current" (default) for the currently logged in user. The password is not needed.
    - Application password of the user you want to impersonate. This allows you to use permissions of another user.
  - $\,\circ\,$  Hub URL: specify the Hub you want the data app to refer to.
    - "Current" (default) for the Hub on which the execution takes place.
    - The URL of the other Hub you want to refer to.

Control the parametrization of the workflow execution.

Hub URL

Current

User application password (No password needed if "Current")

Current

Password

Figure 2. Hub URL and user application password configuration.

# User Usage Monitoring

The User Usage Monitoring data app covers the following use cases:

- Active users: Count users actively logging in and identify unused license users (learn more about users, consumers, and unlicensed users).
- Peak login times: Identify the most active days and times.
- Access method: Determine whether users log in via the KNIME Analytics Platform, their browser, or both.

### Keycloak Service Client configuration

The data app requires **keycloak session events** to be collected and stored to monitor user usage. Here you will configure keycloak such that it stores user events, and setup a service client that has permissions to retrieve these events. This service client will be used by the data app to retrieve the session events.

- 1. Log into Keycloak Admin Console: *`https://auth.<base-url>` > Administration Console.* Learn how to retrieve the credentials here.
- 2. Select your Realm (usually knime).
- Activate Save events to save KNIME Business Hub users events at Realm Settings > Events > User events settings, as shown in Figure 3. Configure how many days to keep the session events.

		③ admin ▼	
KNIME Dev Business Hub 🔻	<b>knime</b> Realm settings are settings that control the options for us	Enabled Action •	
Manage	< General Login Email Themes k	eys <b>Events</b> Localization Security defenses Sessic	>
Clients	Event listeners User events settings Admin events	settings	
Client scopes	Save events ⑦ On		
Realm roles			
Users	Expiration ③ 30 Days		
Groups			
Sessions			
Events			
Configure	Clear user events		
Realm settings			
Authentication			
Identity providers			
User federation	Q Search saved event ty → Add saved typ	es 🖉 Refresh 1-11 🔹 🤇	
	Event saved type	Description	
	Logout	logout	

*Figure 3. Activate Save events in Realm Settings > Events > User events settings.* 

a. Select *Add saved types* and add the refresh token event to the list of events that are saved.

Add types				×
<b>Q</b> , refresh	× →	<b>∂</b> Refresh	1-2 🔻	
Event saved type		Description		
Refresh token		Refresh token		:
Refresh token error		Refresh token error		:
			1-2 🔻 <	
Add Cancel				

Figure 4. Activate Add saved types in Realm Settings > Events > User events settings.

4. Create a new Client from *Clients > Create Client*.

					⑦ admin ▼	
KNIME Dev Business Hub 🛛 🕶	<b>Clients</b> Clients are applic	cations and services that ca	an request aut	hentication of a user. Learn more	• 🖒	
Manage	Clients list	Initial access token Cli	ent registratio	n		
Clients	<b>Q</b> Search for cli	ent <del>&gt;</del> Cre	ate client	Import client	h 1-39 <del>-</del> (	>
Client scopes						
Realm roles	Client ID	Name	Туре	Description	Home URL	
Users Groups		\${client_account}	OpenID Connect		https://auth.business- hubdev.cloudops.knime.com/auth [2]	:
Sessions Events		\${client_account-cons	OpenID Connect		https://auth.business- hubdev.cloudops.knime.com/auth 🗹	•••
Confiqure			OpenID Connect	Client used by account-service for		:
Realm settings		\${client_admin-cli}	OpenID Connect			:
Authentication			OpenID Connect	Service Account for ai-gateway.		:
Identity providers User federation			OpenID Connect	Service Account for ai-history-servi.		•
	ai contico		OpenID	Sonico Account for si conico		:

Figure 5. Create a new Client in Clients > Create Client.

a. Give it a Client ID (monitor-user-usage in the screenshot). Optionally, add a name and a description to make clear what this client is for.

			() a	dmin 🔻 🧕
KNIME Dev Business Hub 🔹	Clients > Create client Create client			
Manage	Clients are applications and service	es that can request authen	tication of a user.	
Clients				
Client scopes	<ol> <li>General settings</li> </ol>	Client type ③	OpenID Connect	-
Realm roles	2 Capability config	Client ID * ⑦	monitor-user-usage	>0
Users	3 Login settings			
Groups		Name 🕜		
Sessions		Description ③		
Events				<i>i</i> .
Configure		Always display in UI 🕝	Off	
Realm settings				
Authentication				
Identity providers				
User federation				

Figure 6. Give the client an ID.

b. In the Capability config section, activate Client authentication. Further, select Service account roles to allow you to authenticate this client to Keycloak and retrieve the access token dedicated to this client. The Login settings don't need to be configured.

### c. Save your new client.

				③ admin ▾
KNIME Dev Business Hub 🔻	Clients > Create client Create client Clients are applications and servic	es that can request auther	ntication of a user.	
Clients Client scopes Realm roles Users Groups Sessions Events Configure	<ol> <li>General settings</li> <li>Capability config</li> <li>Login settings</li> </ol>	Client authentication ③ Authorization ③ Authentication flow	<ul> <li>On</li> <li>Off</li> <li>Standard flow (?)</li> <li>Implicit flow (?)</li> <li>OAuth 2.0 Device</li> <li>OIDC CIBA Grant</li> </ul>	<ul> <li>✓ Direct access grants ⊚</li> <li>✓ Service accounts roles ⊚</li> <li>Authorization Grant ⊚</li> <li>⑤</li> </ul>
Realm settings Authentication Identity providers				

Figure 7. Activate Client authentication and Service account roles in Clients > Create Client.

- 5. In *Clients > Client ID (Column)*, find and click on your new Client (monitor-user-usage).
  - a. Go to the Service account roles tab and click the Assign role button.

								(?)	admin 🔻	
KNIME Dev Business Hub 👻		Client details		OpenID Conne	ct			Enabled @	Action	Ŧ
Manage	Clients a	re applicatio	ns and sei	rvices that can r	equest aut	hentication of a	user.			
Clients		Settings	Keys	Credentials	Roles	Client scopes	Service accounts roles	Sessions	Permis	>
Client scopes	🚺 To m	anage detail	and group	p mappings, clic	k on the us	ername service-	account-monitor-user-usac	je		
Realm roles	<b>Q</b> Searc	h by name		→ 🗹 Hide	inherited r	oles Assign r	ole Unassign	C Refresh		
Users										
								1.	-1 👻 👘	< >
Groups								1.	-1 👻	< >
Groups Sessions	Nan	ne			Inherited	Des	cription	1. 	-1 🔻	< >
		ne iult-roles-knim	ie		Inherited False		zription e_default-roles-knime}	1.	-1 🔻	• •
Sessions			ie					1-1		
Sessions Events			ie							:
Sessions Events Configure			ie							:
Sessions Events Configure Realm settings			ie							:

Figure 8. Assign role in Clients > Client ID (Column).

b. Via *Filter by clients*, search for view-events and assign the role to the service account associated with your client.

Assign roles to monitor-user-usage	×
▼ Filter by clients       ▼       Q, view-eve       X       →       C Refresh	1-1 ▾ < >
Name	Description
realm-management view-events	\${role_view-events}
	1-1 + < >
Assign Cancel	

Figure 9. Assign the view-events role to the service account.

c. Add the manage-users role in a similar fashion.

Assign roles to monitor-user-usage	×
▼ Filter by clients       ▼       Q manage-use       ×       →       2 Refresh	1-1 + < >
Name	Description
realm-management manage-users	\${role_manage-users}
	1-1 ★ < >
Assign Cancel	

Figure 10. Assign the manage-users role to the service account.

- 6. Finally retrieve the Client ID and Client secret:
  - a. Go to Clients > Client ID (Column) and choose your client (monitor-user-usage)
  - b. Click the Credentials tab
  - c. Leave as a Client Authenticator the Client ID and Secret option.
  - d. Copy the Client ID from the top of the tab (monitor-user-usage in the screenshot below).
  - e. Copy the Client's Secret.

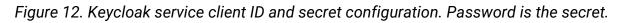
		⑦ admin ▼
KNIME Dev Business Hub 👻	Clients > Client details <b>monitor-user-usage</b> OpenID Connect Clients are applications and services that can request authentication of a user.	Enabled O Action 🗸
Manage Clients	Settings         Keys         Credentials         Roles         Client scopes         Service accounts role	s Sessions Permis >
Client scopes		
Realm roles	Client Authenticator Client Id and Secret	
Users		
Groups		
Sessions	Save Copy to	
Events	clipboard	
	Client Secret 🛛 🔐 👔	Regenerate
Configure		
Realm settings		
Authentication		
Identity providers	Registration access	🕒 Regenerate
User federation		

Figure 11. Retrieve the Client ID and Client secret.

Use the retrieved client ID and secret in the data app deployment of the User Usage Monitoring data app, as described below.

- 1. Download the workflow
- 2. Navigate to the space on your Hub where you want to upload the workflow to
- 3. Use the upload button to upload the workflow (learn more)
- 4. *Run* the workflow to start an ad hoc execution (learn more)
  - Optional: Instead, deploy the workflow as a data app to persist any configuration and make it available to others by sharing the deployment (learn how).
- 5. Configure the keycloak service client ID and secret as retrieved above in the configuration shown in Figure 12.

# Configuration options Control the parametrization of the workflow execution. Keycloak Credentials monitor-user-usage Password



# Gen Al Monitoring

The Gen Al Monitoring data app covers the following use cases:

- Investigate gen Al assistance usage: Measure engagement with K-Al, script assistance, and user prompts.
- Gen Al usage cost: Analyze the cost associated with Gen Al usage.

### **Enable AI Services**

The data displayed by this data app is only available when the AI Service is enabled, as described here.

- 1. Download the workflow
- 2. Navigate to the space on your Hub where you want to upload the workflow to
- 3. Use the upload button to upload the workflow (learn more)
- 4. Run the workflow to start an ad hoc execution (learn more)
  - Optional: Instead, deploy the workflow as a data app to persist any configuration and make it available to others by sharing the deployment (learn how).
- 5. Optional: impersonate another user or configure another Hub in the configuration panel shown in Figure 13.
  - User application password: specify the user you want to impersonate.
    - "Current" (default) for the currently logged in user. The password is not needed.
    - Application password of the user you want to impersonate. This allows you to use permissions of another user.
  - $_{\circ}\,$  Hub URL: specify the Hub you want the data app to refer to.
    - "Current" (default) for the Hub on which the execution takes place.
    - The URL of the other Hub you want to refer to.

Control the parametrization of the workflow execution.

Hub URL

Current

User application password (No password needed if "Current")

Current

Password

Figure 13. Hub URL and user application password configuration.

# **Executor Diagnostics**

The Executor Diagnostics data app covers the following use cases:

- Verify capabilities: List extensions, nodes, conda environments, and Linux packages that are installed on the execution context the data app is running on.
- **Replicate conda environments**: Download the conda environment of the execution context to replicate it on another machine.
- **Troubleshoot network configuration**: Check the proxy settings in the execution context and verify if external URLs are reachable. If a URL is not reachable, receive hints regarding potential reasons.

- 1. Download the workflow
- 2. Navigate to the space on your Hub where you want to upload the workflow to
- 3. Use the upload button to upload the workflow (learn more)
- 4. Run the workflow to start an ad hoc execution (learn more)
  - Optional: Instead, deploy the workflow as a data app to persist any configuration and make it available to others by sharing the deployment (learn how).
- 5. Run the workflow

# Manage Existing Jobs

The Manage Existing Jobs data app covers the following use cases:

- **Inspect all existing jobs**: View and monitor all jobs that remain accessible in the executor's memory or object store.
- Jobs cleanup and storage optimization: Delete jobs to free up disc space in object store or memory in executors.

- 1. Download the workflow
- 2. Navigate to the space on your Hub where you want to upload the workflow to
- 3. Use the upload button to upload the workflow (learn more)
- 4. Run the workflow to start an ad hoc execution (learn more)
  - Optional: Instead, deploy the workflow as a data app to persist any configuration and make it available to others by sharing the deployment (learn how).
- 5. Optional: impersonate another user or configure another Hub in the configuration panel shown in Figure 14.
  - User application password: specify the user you want to impersonate.
    - "Current" (default) for the currently logged in user. The password is not needed.
    - Application password of the user you want to impersonate. This allows you to use permissions of another user.
  - Hub URL: specify the Hub you want the data app to refer to.
    - "Current" (default) for the Hub on which the execution takes place.
    - The URL of the other Hub you want to refer to.

Control the parametrization of the workflow execution.

Hub URL

Current

User application password (No password needed if "Current")

Current

Password

Figure 14. Hub URL and user application password configuration.

# Manage Workflow Versions

The Manage Workflow Version data app covers the following use cases:

- **Identify unused versions**: Detect workflow versions that are no longer in use in any deployment.
- Version cleanup: Delete outdated and unused workflow versions to free up disc space.

- 1. Download the workflow
- 2. Navigate to the space on your Hub where you want to upload the workflow to
- 3. Use the upload button to upload the workflow (learn more)
- 4. *Run* the workflow to start an ad hoc execution (learn more)
  - Optional: Instead, deploy the workflow as a data app to persist any configuration and make it available to others by sharing the deployment (learn how).
- 5. Optional: impersonate another user or configure another Hub in the configuration panel shown in Figure 15.
  - User application password: specify the user you want to impersonate.
    - "Current" (default) for the currently logged in user. The password is not needed.
    - Application password of the user you want to impersonate. This allows you to use permissions of another user.
  - $\,\circ\,$  Hub URL: specify the Hub you want the data app to refer to.
    - "Current" (default) for the Hub on which the execution takes place.
    - The URL of the other Hub you want to refer to.

Control the parametrization of the workflow execution.

Hub URL

Current

User application password (No password needed if "Current")

Current

Password

Figure 15. Hub URL and user application password configuration.





KNIME AG Talacker 50 8001 Zurich, Switzerland www.knime.com info@knime.com

The KNIME® trademark and logo and OPEN FOR INNOVATION® trademark are used by KNIME AG under license from KNIME GmbH, and are registered in the United States. KNIME® is also registered in Germany.