KNIME Business Hub Release Notes

Table of Contents

This document is a collection of all the release notes and important bug fixes of the KNIME Business Hub released versions.

If you want to know more about how to install KNIME Business Hub in different environments and distributions refer to the following guides:

- KNIME Business Hub Installation Guide - Embedded Cluster
- KNIME Business Hub Installation Guide - Existing Cluster
- KNIME Business Hub Installation Guide - Existing OpenShift Cluster

To learn about administration topics refer to the following guides:

- KNIME Business Hub Admin Guide
- KNIME Business Hub Update Guide

If you are a KNIME Business Hub user you might be interested in knowing more about how to perform different actions, for example how to create deployments or manage secrets, refer to the following guides:

- KNIME Business Hub User Guide
- KNIME Secrets User Guide

Finally, have a look at all the different guides provided about various topics in the Hub section of the KNIME Documentation.

Changelog (KNIME Business Hub 1.14)

KNIME Business Hub 1.14.1

(released June 16, 2025)

Notable bug fixes

- Fixed a bug where job artifacts (e.g. swapped jobs) were not cleaned up correctly from the object store after deleting the job from Hub.
- Fixed a bug where loading a swapped jobs could lead to an incorrect job state.
- Fixed a bug where the name of an external group was returned in search instead of the displayName.

- It was not possible to upload files / write to spaces when using team scope deployments. This is now possible.

- Fixed a bug where, when opening the configuration dialog, advanced deployment settings (e.g. job lifecycle settings) where fetched from the execution context defaults, instead of from the already configured deployment.

- Notification emails now show team names when run in team scope execution, instead of team ID.

KNIME Business Hub 1.14.0

(released April 9, 2025)

Infrastructure changes

- Updated Kubernetes installer for **High Availability multi-node installations**.

  - Kubernetes version updated to 1.30

  - KOTS version updated to 1.123

  - Rook version updated to 1.16

  When upgrading an environment running an earlier version of Kubernetes and Rook, **some downtime is expected**. In this release, these components are updated sequentially across multiple minor versions. The Kubernetes installer upgrade process takes approximately four hours, so planning and scheduling should account for the expected downtime during this period.

- The "Select AWS ACM Certificate" KOTS configuration is **now deprecated** and will be removed in future versions.

- Updated `ingress-nginx` to 1.11.5 due to CVE-2025-1974 / CVE-2025-2787. When using an own ingress, make sure to update to a recent version that fixes this vulnerability.

Improvements

New features

- Team-scoped deployment execution: Deployments can now run within the scope of the team that created the deployment. This means that jobs started by a deployment can access team resources like secrets, components, workflows, and data files contained within the team's spaces. This is the default for newly created deployments. If needed,

you can still choose user-scoped execution for specific cases. (See documentation)

Further changes

- It is now possible to customize the "Download KNIME Analytics Platform" button to point to e.g. an internally hosted Analytics Platform download location. This setting is available in KOTS admin portal

- Microsoft interactive secrets now also support confidential apps

- Hub execution enabled for Tableau Reader (Labs) (requires KNIME Analytics Platform version 5.4.1 or newer as executor)

- Air gap bundles now come with KNIME Executor version 5.4.3

Notable bug fixes

- Job discard options for data app deployments are now hidden as discarding running data apps leads to undesired results.

- Workflow versions panel updated to fetch more than 10 versions.

- Fixed a bug where secrets created by team admins could not be fetched by the Secret Retriever node when using SCIM groups to sync KNIME Hub teams member/admin.

- Fixed a bug where execution context-level defaults were not updated correctly when creating/editing a deployment.

- Increased memory resources of the Fluent Bit sidecar that collects executor logs to avoid out-of-memory (OOM) issues in environments where Transparent Hugepages are enabled

New/improved Data Apps

- Improved and unified documentation of admin workflows

  ○ Unifying changes to admin workflows, including small bug fixes and improved error handling

- Executor Diagnostics data app (Link, [Documentation]): Additions to the Proxy Diagnostics Data App to additionally review nodes, extensions, conda environments, and linux packages on the executor the data app is executed on.

- Hub to Hub Migration data app (Link, Documentation): Migrate content from one Hub to another.

Changelog (KNIME Business Hub 1.13)

KNIME Business Hub 1.13.3

(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.

We recommend all users update to this version.

KNIME Business Hub 1.13.2

(released March 05, 2025)

Important bug fixes

- Basic account information such as team membership is not shown anymore to unauthenticated users
- Business Hub version number is not shown anymore to unauthenticated users
- Fixed a bug that affected the presentation of the application password creation menu
- Fixed a bug where jobs were marked as vanished in case a load error occurred
- Fixed an issue where data in catalog could end up in an inconsistent state following migrations from older versions
- Fixed an issue where deployments only showed default configuration values when editing a deployment
- SCIM: User provisioning uses partial instead of exact user matching

- Single pod Postgres clusters now default to failsafe mode to prevent any communication outages with the Kubernetes control plane from causing patroni to demote that pod from its leader status. This issue could, for example, show executed jobs in a *Running* state even though they have already *Completed*

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.

Additional changes

- Existing execution contexts are switched to set `defaultMaxScheduleFailures` to `unlimited`, effectively removing the disabling of deployments as a consequence of load errors. This migration is only applied to execution contexts where `defaultMaxScheduleFailures` is left at the default value of `3`.

KNIME Business Hub 1.13.1

(released January 24, 2025)

Important installation notes (please read carefully)

- In case you need to apply tolerations to kotsadm pods, KNIME Business Hub 1.13.1 requires an update of KOTS to version 1.123.0. Make sure to perform this update before updating Business Hub. In case you don't require such a setup, no KOTS update is needed.
  - To do so use the following command: `curl -sSL https://kurl.sh/knime-hub | sudo bash`.

New features

- KNIME Business Hub now supports using taints and tolerations to control which pods can be scheduled on specific nodes by allowing nodes to repel certain pods unless

those pods explicitly tolerate the taints. (See Documentation)

Important bug fixes

- Fixed a bug where executors configured to use a proxy could not communicate with Hub anymore

- Fixed a bug where a database migration could lead to incorrect data for the job instrumentation service

- Fixed a bug from the 1.13.0 release where clusters using an older version of kots would not be able to deploy namespace migration jobs

KNIME Business Hub 1.13.0

(released January 07, 2025)

Important installation notes (please read carefully)

- During update, all executors will be terminated. Due to this, any **running jobs will be cancelled and will not be retrievable.** In order to avoid data loss, please make sure that no jobs are running during the update (e.g. by stopping all execution contexts before performing the update).

- Customers managing their own CRDs need to update these **before** performing the Business Hub update.

- Keycloak is updated to a new version. In case you have changed the automatically assigned password for the Keycloak admin console, a new password will be assigned. You can retrieve this password as described here.

- If the cluster allows only specific domains, for the cluster to be able to pull Docker images, a new host `cr.fluentbit.io` needs to be added to the list of accessible hosts before updating.

- Airgapped bundles now come with KNIME Analytics Platform 5.3.3 as executor.

Infrastructure changes

- Keycloak has been updated to version 25

- Installing into existing clusters supports custom defined namespace names

- Namespaces consolidated in this version. With provided Istio instance new existing

cluster installs can use a single namespace

- Kubernetes version updated to 1.30 for embedded cluster installs

- Kots version updated to 1.121

- Postgres read replicas enabled to improve performance and resilience

Improvements

New features

- Validation service: Execution contexts can now be configured to require certain labels to be set when trying to execute a workflow or to create a deployment. If the workflow's version label does not match the executor's requirement, it is not accepted. (See Documentation)

- Private search: It is now possible to use Hub search to find items located in private spaces.

- Execution context log file download: Global admin users can download execution context's log files from the Hub UI. This feature works irrespective of current execution context status. I.e., it is also possible to retrieve log files from crashed executors, facilitating debugging.

- Global admin secrets: Global admin users can manage secrets on a Hub-wide level and share them with teams or individual users.

- Databricks secret: Added support for Databricks authentication methods, allowing easy and secure access to your Databricks workspace. (See Documentation)

- Salesforce secret: Added support for Salesforce authentication methods, allowing easy and secure access to your Salesforce data. (See Documentation)

- AI service:

  ○ Added the possibility to configure the disclaimer displayed by K-AI in scripting editors (e.g. Expression or Python Script) on the KOTS admin page.

  ○ Added the possibility to configure the retention period of the AI history via the KOTS admin page. Note: The default is set to 180 days.

  ○ It is now possible to configure whether K-AI should include public workflows and components in its answers. In order to include them, K-AI uses their name and description which means that those are shared with the GenAI provider.

Further changes

- Improved workflow and job states: Ensures that users can, at any time, find out the

precise status of a job. (See Documentation)

- Select executor images via dropdown

  ◦ Global admin can add new images to dropdown selection using this data app (See Documentation)

- Improved handling of configuration nodes for ad-hoc execution and deployments

  ◦ Added support for more configuration nodes to be used while creating jobs or deployments

- Easier period input for advanced deployment and execution context settings

- Control executor heap requirements from UI

  ◦ Needed if memory intensive processes run alongside the executor container, e.g. Python

- Enable iframe embedding for shared data apps. (See Documentation)

- Performance improvements when uploading items to Hub, including parallel upload of multiple items

- Added the ability to upload workflows and files from the Hub UI

- Added live update of content on the secrets pages (e.g. no refresh needed after adding a new secret)

- Listing jobs via /jobs endpoint does not return configuration and/or input/output data anymore. In case this information is needed, the job needs to be queried directly via /jobs/jobId. This change reduces load caused by large job listings.

- Team members can now retrieve information on other team members' jobs via the instrumentation endpoint (was: users could only see their own jobs)

  ◦ This is now in line with visibility of existing jobs

- SCIM functionality is now also available for Business Hub Standard Edition licenses

  ◦ This facilitates sharing deployments with externally managed groups of consumers

- Increased default job swap retries to "unlimited" (i.e. jobs stuck from swapping will eventually be swapped)

  ◦ New defaults only apply to newly created execution contexts and deployments. Please update existing execution contexts / deployments if needed.

- Increased default schedule load attempts until schedule is disabled to "unlimited" (i.e. schedules will not be disabled anymore if the job fails loading x times in a row)

  ◦ New defaults only apply to newly created execution contexts. Please update existing execution contexts if needed.

Notable bug fixes

- In embedded cluster installs, garbage collection was not disabled by default for the embedded image registry

- Jobs created by a now deleted user were not discarded

- Executor IPs were also shown to non-admin users

- Updated execution context settings were only shown after page refresh

New/improved Data Apps

- Version label/validation service admin workflows

- Manage List of Executor Images (new) (Link)

   - Allows to manipulate the dropdown list when configuring an execution context.

- Proxy Diagnostics (new) (Link)

   - Investigate the current proxy related settings on either a local AP or remote executor to help debug proxy/networking issues. Check the reachability of a URL directly in a data app, i.e. check if a URL is reachable from an execution context.

- Admin Dashboard (new) (Link)

   - Gain insight about the usage of the current Hub usage, e.g. how many users, items, execution contexts each team has.

- Customization Profile Application (improved) (Link)

   - Manage customization profiles with a better UI and e.g. edit settings directly in the data app.

- Monitor User Usage (improved) (Link)

   - Monitor the sessions users have on the KNIME Business Hub to identify e.g. inactive users and times of high load.

- Delete Old Item Versions (improved) (Link)

   - Data app to free disk space by deleting workflow versions that are older than a certain date and not involved in any deployments.

- Executor Image Builder (improved) (Link)

   - Build executor images now directly from dockerfiles, add proxies, and updated the python support.

- Published data apps adapted to new job states in 1.13.0:

   - Manage All Existing Jobs (Link)

- ◦ Workflow Jobs Monitoring ([Link](#))

Changelog (KNIME Business Hub 1.12)

KNIME Business Hub 1.12.4

(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 1.12.3

(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 1.12.2

(released November 26, 2024)

Important changes (please read carefully)

- KNIME Business Hub 1.12.2 addresses default memory requests across multiple services. This helps lowering the minimum hardware requirements, so that Business Hub can again be deployed on machines with only 32GB of memory (while allowing an executor with at most 12GB RAM). Customers with larger machines do not need to go to this version.

- This release introduces the ability to configure hardware resource requests for the additional services in the KOTS admin console. At the same time, default memory requests have been reduced for these services:

- Search-sync service: 2560MB → 1024MB

- Artemis: 2048MB → 1024MB

- Elasticsearch: 2048MB → 1024MB

- Memory requests for istio-proxy sidecar containers have been reduced from 128MB to 64MB per container

- This setting will only be applied after relevant pods have been restarted via `kubectl rollout restart deployment -n hub`. Doing so is not strictly necessary, but will save around 2.5GB of memory combined

KNIME Business Hub 1.12.1

(released September 11, 2024)

Important changes (please read carefully)

This release fixes wrong default values for CPU requests for various services. These values were introduced in KNIME Business Hub 1.12.0, and led to resource issues on smaller clusters.

For instance, the default memory requests for core services have been raised to 24GB, leaving only 8GB for an executor on a 32GB machine. This will be made configurable in an upcoming release in order to allow increasing execution resources again.

KNIME Business Hub 1.12.0

(released September 9, 2024)

Important installation notes

During the update executors of the Hub will restart. Some downtime in execution is expected.

Important changes (please read carefully)

- The Secret Store feature is now also available for Business Hub Basic Edition licenses (See documentation)

Improvements

- Scalability options for selected Hub services: IT now has the flexibility to configure resource usage and set limits for scaling with parameters such as minimum/maximum replicas, target CPU utilization, and memory resources for various Hub services like Account, Catalog, Execution Rest Interface, Search, and Websocket Proxy (See documentation)

- New monitoring dashboards: Administrators now have access to metrics from Kubernetes, KNIME Business Hub services, and tools like Keycloak and Minio to understand KNIME Business Hub operations better and troubleshoot performance issues more effectively (See documentation)

- Trigger deployments: Workflows can now be executed by events that occur across multiple teams and spaces, including those in newly created spaces. Global administrators can even set workflows to execute based on events across all spaces in the organization. This update is particularly helpful to administrators who want to deploy team or organization-wide governance workflows (See documentation)

Important bug fixes

- To avoid missing image problems coming up in airgapped installations. Garbage collection in the internal image registry shipped with Hub is now disabled by default.

Changelog (KNIME Business Hub 1.11)

KNIME Business Hub 1.11.4

(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 1.11.3

(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 1.11.2

(released August 21, 2024)

Important installation notes

- Updates from the Business Hub 1.11.x version are **highly recommended**, as critical issues were fixed in this release.

Important bug fixes

- Fixed an issue in SCIM integration where percentage-encoding did not allow upper- and lowercase characters in SCIM endpoints
- Fixed a bug where "number of executors" setting didn't work for shared execution

contexts through the Business Hub UI

- Fixed an issue where refreshing a Box/Generic/Google OAuth2 Interactive secret via the Secret Store consume endpoint failed on the second refresh
- Fixed an issue where Keyclaok didn't start up properly in some cases after a restart
- Fixed an issue in Secret Store where Google Sheets (read-only) scope group contained invalid scopes

Infrastructure update

- Security update: KNIME Business Hub does no longer utilize role bindings to default service accounts

KNIME Business Hub 1.11.1

(released August 9, 2024)

Important installation notes

- Updates from the Business Hub 1.11.0 version are **highly recommended**, as critical issues were fixed in this release.
- **Important** If an external loadbalancer is deployed for handling TLS, and the coreDNS configuration update is disabled, the checkbox Istio Oudbound Traffic Redirect has to be disabled as well. Otherwise, internal calls to the hub URL will skip the Loadbalancer and TLS is not handled.

Important bug fix

- Fixed the issue where in Business Hub 1.11.0 discarding and swapping jobs from running executors were not happening automatically. This would result in jobs piling up on the executor causing critical problems.

KNIME Business Hub 1.11.0

(released July 24, 2024)

Important installation notes

Important: If an external Loadbalancer is deployed for handling TLS, and the CoreDNS configuration update is disabled, the checkbox "Istio Outbound Traffic Redirect" has to be disabled as well on the KOTS Admin Console. Otherwise, internal calls to the Hub URL will skip the Loadbalancer and TLS is not handled.

Notice that due to the Postgres database update ~10 minutes downtime is expected.

Improvements

- KNIME Business Hub now provides a GenAI Gateway that allows IT to centrally configure which GenAI providers and nodes can be accessed and used by team members
- Workflows and components now come with rich descriptions
- Personal credentials are now available to logged-in read-only users
- Admins of KNIME Business Hub can assign memory limits to Teams

Infrastructure updates

- Postgres database has been updated to version 16
- Artemis has been updated to version 2.35.0
- Quarkus has been updated to version 3.8 LTS

Important bug fixes

- Fixed an issue where members of a Team could see the delete button for Deployments even if they didn't have the permission to delete them
- Fixed an issue where deployment of Kots failed when there was no TLS certificate defined
- Security context fixes
- Various small bug fixes

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)

> **i** **Important note:** Updates from Business Hub 1.10.x versions are **highly** recommended, as critical issues were fixed in this release.

Important bug fixes

- 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/2024-06/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/-/~aRbyzgd02lbkB60j/most-recent/

- Docs: https://docs.knime.com/2024-06/business_hub_admin_guide/index.html#scim-users-teams-data-appliation

> ℹ️ 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.

Bug fixes

- 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://kurl.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. Additionally, make sure that the DNS entry of the Websocket URL (`ws.<base-url>`) is set up correctly. You can find the Websocket URL in the KOTS Admin Console under *URLs > Websocket URL*.

- 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-metadate-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. Refer to the steps here to retrieve the credentials.

> ℹ️ KNIME Business Hub 1.9.0 includes the Docker executor image: `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)

> **ℹ** KNIME Business Hub 1.8.0 includes the Docker executor image: `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)

- 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 bug fixes

- **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 bug fixes

- **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 bug fix

- **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 bug fixes

- 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 bug fixes

- 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 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:
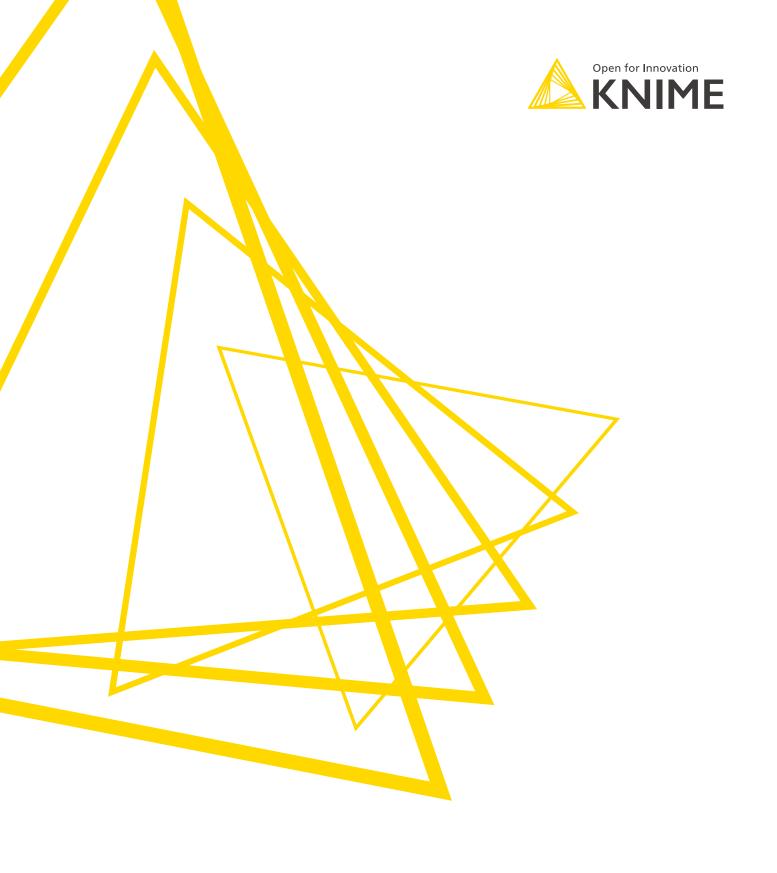
- ◦ First, check for updates in KOTS Admin Console.

- ◦ 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/2024-06/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/2024-06/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

Bug fixes

- Removed the unused ipv6 listener in the Business User Portal container, that could cause crashes in some environments