Cloudera Data Engineering 1.5.5

Artifact access management

Date published: 2020-07-30
Date modified: 2025-11-08

https://docs.cloudera.com/

Legal Notice

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER’S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

Contents

Artifact access management

Learn about what artifact access management is and how to share artifacts between users or groups.

Important:

- Artifacts refer to jobs, resources, repositories, job runs, and sessions.
- Artifact access management is supported only for Cloudera Data Engineering service installation using Embedded Container Service.
- Artifact sharing is applicable only for users with VC User role. By default, users with DEAdmin, Service Admin, and VC Admin roles have full access to all the artifacts in the Virtual Cluster and the users with VC Viewer role have read-only access to all the artifacts in the Virtual Cluster.

By default, users can only manage the artifacts that are either created by them or if they are explicitly shared with them with full access by another user or group. Only users or groups with full access can share the artifacts with others. Users or members of a group with read-only access to the artifact cannot share or manage the artifact. You can share an artifact that you own with another user or group with either full access or read only access. Beside sessions which can only be shared during its creation, all other artifacts can be shared during their creation or later.

If the Restrict sharing by default option in Privacy Settings is not enabled for a Virtual Cluster, all the artifacts associated with that Virtual Cluster can be managed with full access by all users who have access to the Virtual Cluster. The users with Admin roles such as DEAdmin, Service Admin, and VC Admin have full access to the artifacts. The users with the VC Viewer role have view-only access to all the artifacts. The users with a VC User role can access all the artifacts that are created by any user in that Virtual Cluster after the Restrict sharing by default option is disabled.

Important: If you share a job or session with a user or group, first, make sure that you also share the associated resources and the repositories related to that job or session with them to ensure proper sharing and execution of the jobs and the sessions. If a job or session is shared with a user or a group, but the resources and repositories are not shared, the user or group cannot run the job or the session and any attempt to run the job or session will fail.

Limitations

- You can only share an artifact through the Cloudera Data Engineering API or CLI. You cannot share artifacts through the Cloudera Data Engineering UI.
- A user or a group who can access the Virtual Cluster can view the Spark History Server UI for all jobs in the virtual cluster.

Artifact sharing access levels

When sharing artifacts, in Cloudera Data Engineering, you can provide one of the following access levels to a user:

- **Full**: Provides complete access to manage a particular artifact. A user with full access can manage, kill, or delete an artifact.
- **View only**: Provides access to only view the artifact.

Important:

- An artifact owner who created it always has full access to the artifact. Any attempts to change the access to view only for the owner does not take effect. Cloudera does not recommend any actions to demote the access of an artifact owner.
- When you assign or unassign a role to a user or a group in a Service or a Virtual Cluster, it takes up to two minutes for the updated access to take effect. For example, if a user is assigned a VC User role to a Virtual Cluster, then the access to that Virtual Cluster is granted to that user within two minutes.

Role-based access for artifacts

Even though you are configuring the artifact access levels, implicit access to the artifacts is given to the users with higher roles. For example, DEAdmin gets full access to all the artifacts in the Cloudera Data Engineering environment, Service Admin gets full access to all the artifacts in that specific Service, and VC Admin gets full access to all the artifacts in that specific Virtual Cluster. The following tables outline the actions users with different roles can perform on artifacts in a Cloudera Data Engineering Virtual Cluster:

Table 1: Role based access

Role	Create	View	Update	Kill	Delete
DE Admin	Yes	Yes	Yes	Yes	Yes
Service Admin	Yes	Yes	Yes	Yes	Yes
VC Admin	Yes	Yes	Yes	Yes	Yes
VC User	Yes	Yes	Yes	Yes	Yes
VC Viewer	No	Yes	No	No	No

Table 2: Artifact sharing support for different users

Artifact name	DEAdmin	Service Admin	Service User	VC Admin	VC User	VC Viewer
Jobs	DEAdmin has full access to all the Jobs in all the Virtual Clusters and Services in a specific environment. DEAdmin can share or stop sharing a Job with a user or group whenever they want.	Service Admin has full access to all the Jobs in all the Virtual Clusters in a specific Cloudera Data Engineering Service. Service Admin can share or stop sharing a Job with a user or group whenever they want.	Service Users can share or stop sharing a Job only if they at least have a VC User role in the Virtual Cluster and they meet one of the following conditions: • They have full access to the Job. • They are the owner of the Job.	VC Admin has full access to all the Jobs in a specific Virtual Cluster. VC Admin can share or stop sharing a Job with a user or group whenever they want.	VC User can share or stop sharing a Job only if they have full access to the Job or are the owner of the Job.	View only

Artifact name	DEAdmin	Service Admin	Service User	VC Admin	VC User	VC Viewer
Job Runs	DEAdmin has full access to all the Job Runs in all the Virtual Clusters and Services in a specific environment.	Service Admin has full access to all the Job Runs in all the Virtual Clusters in a specific Cloudera Data Engineering Service.	Job Runs inherit the same access levels that of the Cloudera Data Engineering they are part of. Service Users must at least have a VC User role assigned in the Virtual Cluster to access or view a Job Run. Service Users can interact with a Job Run only if they have full access to that particular Job or if they created that Job Run. Otherwise, a Service User can only view the Job Run until they have access to the Job. If the access to the Job is removed, then the Service User cannot view the Job Runs that are created after the access is removed. They can only view the Job Runs that are created when they had access to that Job.	VC Admin has full access to all the Job Runs in a specific Virtual Cluster.	Job Runs inherit the same access levels that of the Cloudera Data Engineering Jobs they are part of. VC Users can view a Job Run only if it was created when they had access to that particular Job that the Job Run is part of. VC Users can view a Job Run if they have at least view-only access to the Job. However, they can interact (terminate or clone) with a Job Run only if they have full access to that Job Run. If the access to the Job is removed for the VC Users, then they cannot access or view the Job Runs that are created after the access is removed. They can only view the Job Runs that are created when they had access to that Job.	View only
Sessions	DEAdmin can view all the Sessions in all the Virtual Clusters and Services in a specific environment.	Service Admin can view all the Sessions in all the Virtual Clusters in a specific Cloudera Data Engineering Service.	A Service User must at least have a VC User role assigned in the Virtual Cluster to view the Sessions in that Virtual Cluster.	VC Admin can view all the Sessions in a specific Virtual Cluster.	VC Users can view a Session if they at least have view-only access to a specific Virtual Cluster.	View only
Repositories	DEAdmin has full access to all the Repositories in all the Virtual Clusters and Services in a specific environment. DEAdmin can share or stop sharing a Repository with a user or group whenever they want.	Service Admin has full access to all the Repositories in all the Virtual Clusters in a specificCloudera Data Engineering Service. Service Admin can share or stop sharing a Repository with a user or group whenever they want.	Service Users can share or stop sharing a Repository only if they at least have a VC User role in the Virtual Cluster and they meet one of the following conditions: • They have full access to the Repository. • They are the owner of the Repository.	VC Admin has full access to all the Repositories in a specific Virtual Cluster. VC Admin can share or stop sharing a Repository with a user or group whenever they want.	VC Users can share or stop sharing a Repository only if they have full access to the Repository or if they are the owner of the Repository.	View only

Artifact name	DEAdmin	Service Admin	Service User	VC Admin	VC User	VC Viewer
Resources	DEAdmin has full access to all the Resources in all the Virtual Clusters and Services in a specific environment. DEAdmin can share or stop sharing a Resource with a user or group whenever they want.	Service Admin has full access to all the Resources in all the Virtual Clusters in a specific Cloudera Data Engineering Service. Service Admin can share or stop sharing a Resource with a user or group whenever they want.	Service Users can share or stop sharing a Resource only if they at least have a VC User role in the Virtual Cluster and they meet one of the following conditions: • They have full access to the Resource. • They are the owner of the Resource.	VC Admin has full access to all the Resources in a specific Virtual Cluster. VC Admin can share or stop sharing a Resource with a user or group whenever they want.	VC Users can share or stop sharing a Resource only if they have full access to the Resource or if they are the owner of the Resource.	View only
Credentials	DEAdmin has full access to all the Credentials in all the Virtual Clusters and Services in a specific environment. DEAdmin can share or stop sharing a Credential with a user or group whenever they want.	Service Admin has full access to all the Credentials in all the Virtual Clusters in a specific Cloudera Data Engineering Service. Service Admin can share or stop sharing a Credential with a user or group whenever they want.	Service Users can share or stop sharing a Credential only if they at least have a VC User role in the Virtual Cluster and they meet one of the following conditions: • They have full access to the Credential. • They are the owner of the Credential.	VC Admin has full access to all the Credentials in a specific Virtual Cluster. VC Admin can share or stop sharing a Credential with a user or group whenever they want.	VC Users can share or stop sharing a Credential only if they have full access to the Credential or if they are the owner of the Credential.	View only

Important:

- Airflow DAGs are not protected by Jobs API ACLs, so the above Job sharing limitation for the VC User does not apply to them. The Airflow UI provides full read access to all DAGs. To disable Airflow Jobs, see User Access Management Overview.
- A Session can be shared only during Session creation. The Session owner can only interact with it and no one else can interact with the Session or remove access to it.

Table 3: Artifact sharing support in Cloudera Data Engineering UI, CLI, and API

Artifact name	Cloudera Data Engineering UI	Cloudera Data Engineering CLI	Cloudera Data Engineering API
Jobs	Yes	Yes	Yes
Job Runs **Important:** Job Runs inherit the same level of access as the parent Jobs have at the moment of the Job Run creation.	No	No	No
Sessions	Yes	Yes	Yes
Repositories	Supported only in Cloudera Data Engineering 1.5.5 SP1 and higher versions, during Repository update.	Yes	Yes
Resources	Supported only in Cloudera Data Engineering 1.5.5 SP1 and higher versions, during Resource update.	Yes	Yes
Credentials	No	Yes	Yes

Sharing an artifact with a user or group

Learn about how to share an artifact with a user or a group.

Important:

- If a job is shared with a user or a group, they can only view the job runs for that job, which are created after the job is shared. The runs for a job that were executed before the job was shared will not be accessible by the user or the group.
- For each artifact, you can add up to 20 users and 20 groups for each access level. For example, a job can have up to 20 users and 20 groups with full access and 20 users and 20 groups with view only access for that job.
- Job runs cannot be shared independently with any user or group. Any user or group with access to the job only can access the job runs associated with that job from the time that job is shared with that user or group.
- A Cloudera Data Engineering session cannot be interacted by another VC User. Only a session owner who created the session can interact with it, but administrators or VC Users with whom the session is shared with full access level can manage or terminate it.
- The owner of the job can never be changed even if you share the job with another user or group with full access. The user or group can edit the job but cannot change the owner.

Prerequisites

- If you share a job or session with a user or a group, first, also share the associated resources and the repositories related to that job or session with them to ensure proper sharing and execution of the jobs and the sessions. If a job or session is shared with a user or a group, but the resources and repositories are not shared, the user or group cannot run the job or the session and any attempt to run the job or session will fail.
- When you want to share an artifact or stop sharing an artifact, you must provide the Workload User Name of the user in the Cloudera Data Engineering CLI or Cloudera Data Engineering API. To check your workload user name, go to Cloudera Management Console User Management Users , find the user name, and then find the Workload User Name.

Sharing an artifact while creating an artifact

For Cloudera Data Engineering UI

Note:

- From Cloudera Data Engineering 1.5.5 SP1 onward, you can share the artifacts using Cloudera Data Engineering UI while creating the artifacts.
- Sessions can be shared using Cloudera Data Engineering UI only while creating them. Jobs can be shared during job creation and later, only during job updates. Other artifacts, such as repositories, resources, and credentials can only be shared post-creation by updating them.

To share artifacts using Cloudera Data Engineering UI while creating them, see the following pages in Cloudera Data Engineering documentation:

- Jobs - Creating jobs in Cloudera Data Engineering
- Sessions - Creating Sessions in Cloudera Data Engineering

For Cloudera Data Engineering CLI

Run the following command to share an artifact with a user or group while creating an artifact:

```
./cde <***ARTIFACT_TYPE***> create -h
Usage:
  cde <***ARTIFACT_TYPE***> create [flags]
Flags:
      --acl-full-access-group stringArray      group with full access pe
rmission (can be repeated to add multiple groups)
      --acl-full-access-user stringArray       user with full access permi
ssion (can be repeated to add multiple users) (set '*' value for all VC
Users)
      --acl-view-only-group stringArray        group with view only permi
ssion (can be repeated to add multiple groups)
      --acl-view-only-user stringArray         user with view only permis
sion (can be repeated to add multiple users) (set '*' value for all VC U
sers)
```

The <****ARTIFACT_TYPE****> value can be a job, session, resource, repository, or credential. Only Artifact access management-specific flags are shown for clarity.

Examples

The following examples are for jobs. But the same flags apply to sessions, resources, repositories, or credentials.

```
# create a job and give access to all users
./cde job create --name job-1 --acl-full-access-user '*'

# create a job and give full access to only a specific group
./cde job create --name job-1 --acl-full-access-group 'qe_group'
# create a job with a complex combination of acl rules
./cde job create --name job-1 --acl-full-access-user cdpuser1 --acl-full
-access-user cdpuser2 --acl-view-only-group 'qe-group' -acl-full-access-
group 'dev-group'
```

For Cloudera Data Engineering API

- Run the following JSON payload to provide full access for an artifact to a user while creating the artifact:

```
curl -X POST \
<jobs_api_url>/<***ARTIFACT_TYPE***> \
-H "Authorization: Bearer ${CDE_TOKEN}" \
-H "Content-Type: application/json" \
-d'{
"name": "<***ARTIFACT_NAME***>",
"acls": {
 "full_access": {
  "users": [<users>]
 }
}

}'
```

  The <****ARTIFACT_TYPE****> value can be job, resource, repository, or credential and the <****ARTIFACT_NAME****> value is the name of the artifact.
- Run the following JSON payload to provide full access for an artifact to a group while creating the artifact:

```
curl -X POST \
<jobs_api_url>/<***ARTIFACT_TYPE***> \
-H "Authorization: Bearer ${CDE_TOKEN}" \
-H "Content-Type: application/json" \
-d '{
"name": "<***ARTIFACT_TYPE***>",
"acls": {
 "full_access": {
  "groups": [<groups>]
 }
}
}'
```

The <****ARTIFACT_TYPE****> value can be job, resource, repository, or credential and the <****ARTIFACT_NAME****> value is the name of the artifact.

- Run the following JSON payload to provide view-only access for an artifact to a user while creating the artifact:

```
curl -X POST \
<jobs_api_url>/<***ARTIFACT_TYPE***> \
-H "Authorization: Bearer ${CDE_TOKEN}" \
-H "Content-Type: application/json" \
-d '{
"name": "<***ARTIFACT_NAME***>",
"acls": {
 "view_only": {
  "users": [<users>]
 }
}

}'
```

The <****ARTIFACT_TYPE****> value can be job, resource, repository, or credential and the <****ARTIFACT_NAME****> value is the name of the artifact.

- Run the following JSON payload to provide view-only access for an artifact to a group while creating the artifact:

```
curl -X POST \
<jobs_api_url>/<***ARTIFACT_TYPE***> \
-H "Authorization: Bearer ${CDE_TOKEN}" \
-H "Content-Type: application/json" \
-d '{
"name": "<***ARTIFACT_NAME***>",
"acls": {
 "view_only": {
  "groups": [<groups>]
 }
}

}'
```

The <****ARTIFACT_TYPE****> value can be job, resource, repository, or credential and the <****ARTIFACT_NAME****> value is the name of the artifact.

Examples

- This examples show creating a job and giving access to all users.

```
# create a job and give access to all users
curl -X POST \
https://qnrjlcs6.cde-fllv7d7m.apps.apps.shared-rke-dev-01.kcloud.clou
dera.com/dex/api/v1/jobs \
-H "Authorization: Bearer ${CDE_TOKEN}" \
-H "Content-Type: application/json" \
-d'{
"name": "job-1",
"spark": {
  "className": "org.apache.spark.examples.SparkPi",
 "file": "local:///opt/spark/examples/jars/spark-examples.jar"
},
"type": "spark",
"acls": {
  "full_access": {
      "users": ["*"]
  }
}

}'
```

- This example shows creating a job and giving full access to only a specific group.

```
# create a job and give full access to only a specific group
curl -X POST \
https://qnrjlcs6.cde-fllv7d7m.apps.apps.shared-rke-dev-01.kcloud.clouder
a.com/dex/api/v1/jobs \
-H "Authorization: Bearer ${CDE_TOKEN}" \
-H "Content-Type: application/json" \
-d'{
"name": "job-1",
"spark": {
  "className": "org.apache.spark.examples.SparkPi",
 "file": "local:///opt/spark/examples/jars/spark-examples.jar"
},
"type": "spark",
"acls": {
  "full_access": {
      "groups": ["cdpcp"]
  }
}

}'
```

- This example shows creating a job with a complex combination of access sharing rules.

```
# create a job with a complex combination of access sharing rules
curl -X POST \
https://qnrjlcs6.cde-fllv7d7m.apps.apps.shared-rke-dev-01.kcloud.cloude
ra.com/dex/api/v1/jobs \
-H "Authorization: Bearer ${CDE_TOKEN}" \
-H "Content-Type: application/json" \
-d'{
"name": "job-1",
"spark": {
  "className": "org.apache.spark.examples.SparkPi",
 "file": "local:///opt/spark/examples/jars/spark-examples.jar"
},
"type": "spark",
"acls": {
  "full_access": {
   "users": ["cdpuser1"]
  },
  "view_only": {
   "users": ["cdpuser2"],
   "groups": ["cdpcp", "hivetest"]
}
}

}'
```

Updating artifact sharing after creating an artifact

For Cloudera Data Engineering UI

Note:

- From Cloudera Data Engineering 1.5.5 SP1 onward, you can share the artifacts using Cloudera Data Engineering UI.
- You can share sessions only while creating them. You canot share sessions while updating them.

To share jobs while updating them, perform the following steps:

1. In the Cloudera console, click the Data Engineering tile. The Cloudera Data Engineering Home page displays.
2. In the left navigation menu, click Jobs. The Jobs page is displayed.
3. Select the job that you want to share and click on the Sharing tab.
4. In the Sharing Settings section, click Add User or Group. The Add User or Group pop-up appears.
5. In the Search for a User or a Group field, type the user or group name and select the required user or group from the list.
6. Select Full or Read Only depending on the access you want to provide from the Access Level drop-down list.
7. Click Add.

To share repositories while updating them, perform the following steps:

1. In the Cloudera console, click the Data Engineering tile. The Cloudera Data Engineering Home page displays.
2. In the left navigation menu, click Repositories. The Repositories page is displayed.
3. Select the repository that you want to share and click on the Sharing tab.
4. In the Sharing Settings section, click Add User or Group. The Add User or Group popup appears.
5. In the Search for a User or a Group field, type the user or group name and select the required user or group from the list.
6. Select Full or Read Only depending on the access you want to provide from the Access Level drop-down list.
7. Click Add.

To share resources while updating them, perform the following steps:

1. In the Cloudera console, click the Data Engineering tile. The Cloudera Data Engineering Home page displays.
2. In the left navigation menu, click Resources. The Resources page is displayed.
3. Select the resource that you want to share and click on the Sharing tab.
4. In the Sharing Settings section, click Add User or Group. The Add User or Group popup appears.
5. In the Search for a User or a Group field, type the user or group name and select the required user or group from the list.
6. Select Full or Read Only depending on the access you want to provide from the Access Level drop-down list.
7. Click Add.

For Cloudera Data Engineering CLI

Run the following command to share an artifact with a user or group after creating an artifact:

```
./cde <***ARTIFACT_TYPE***> update -h
Usage:
  cde <***ARTIFACT_TYPE***> update [flags]
Flags:
      --add-acl-full-access-group stringArray      add group with full a
ccess permission (can be repeated to add multiple groups)
      --add-acl-full-access-user stringArray       add user with full acce
ss permission (can be repeated to add multiple users) (set '*' value for
 all VC Users)
      --add-acl-view-only-group stringArray        add group with view on
ly permission (can be repeated to add multiple groups)
      --add-acl-view-only-user stringArray         add user with view onl
y permission (can be repeated to add multiple users) (set '*' value for
all VC Users)
```

The <***ARTIFACT_TYPE***> value can be job, resource, repository, or credential. Only Artifact access management specific flags are shown for clarity.

Examples

The following examples are for jobs. But the same flags apply to jobs, resources, repositories, or credentials.

```
# Add * to give access to everybody
./cde job update --name job-1 --add-acl-full-access-user '*' --vcluster-
endpoint https://7jn5szdr.cde-tz8dl6vr.apps.host-1.dex-ecs.kcloud.cloude
ra.com/dex/api/v1 --user cdpuser4

# add cdpuser5 to view-only, cdpuser6 to full-access, remove wildcard from
 full-access

./cde job update --name job-1 --add-acl-view-only-user 'cdpuser5' --add-
acl-full-access-user 'cdpuser6' --remove-acl-full-access-user '*'
```

For Cloudera Data Engineering API

Important: Passing the artifact sharing configuration overrides the existing configuration for the artifacts. So, to add additional users to an access level, you must pass the full list that includes the existing users and the new users you want to add. To get the existing users list, see Viewing artifact sharing information.

- Run the following JSON payload to provide full access for an artifact to a user:

  ```
  curl -X PATCH \
  <jobs_api_url>/<***ARTIFACT_TYPE***>/<***ARTIFACT_NAME***> \
  -H "Authorization: Bearer ${CDE_TOKEN}" \
  -H "Content-Type: application/json" \
  -d '{
  "acls": {
   "full_access": {
    "users": [<users>]
   }
  }

  }'
  ```

  The <****ARTIFACT_TYPE****> value can be jobs, resource, repository, or credential and the <****ARTIFACT_NAME****> value is the name of the artifact.
- Run the following JSON payload to provide full access for an artifact to a group:

  ```
  curl -X PATCH \
  <jobs_api_url>/<***ARTIFACT_TYPE***>/<***ARTIFACT_NAME***> \
  -H "Authorization: Bearer ${CDE_TOKEN}" \
  -H "Content-Type: application/json" \
  -d '{
  "acls": {
   "full_access": {
    "groups": [<groups>]
   }
  }

  }'
  ```

  The <****ARTIFACT_TYPE****> value can be jobs, resource, repository, or credential and the <****ARTIFACT_NAME****> value is the name of the artifact.
- Run the following JSON payload to provide view-only access for an artifact to a user:

  ```
  curl -X PATCH \
  <jobs_api_url>/<***ARTIFACT_TYPE***>/<***ARTIFACT_NAME***> \
  -H "Authorization: Bearer ${CDE_TOKEN}" \
  ```

```
-H "Content-Type: application/json" \
-d '{
"acls": {
 "view_only": {
  "users": [<users>]
 }
}

}'
```

The <****ARTIFACT_TYPE****> value can be jobs, resource, repository, or credential and the <****ARTIFACT_NAME****> value is the name of the artifact.

- Run the following JSON payload to provide view-only access for an artifact to a group:

```
curl -X PATCH \
<jobs_api_url>/<***ARTIFACT_TYPE***>/<***ARTIFACT_NAME***> \
-H "Authorization: Bearer ${CDE_TOKEN}" \
-H "Content-Type: application/json" \
-d '{
"acls": {
 "view_only": {
  "groups": [<groups>]
 }
}

}'
```

The <****ARTIFACT_TYPE****> value can be jobs, resource, repository, or credential and the <****ARTIFACT_NAME****> value is the name of the artifact.

Examples

- This example shows providing full access to all users.

```
# Add * to give access to everybody
curl -X PATCH \
https://qnrjlcs6.cde-fllv7d7m.apps.apps.shared-rke-dev-01.kcloud.cloudera.com/dex/api/v1/jobs/job-1 \
-H "Authorization: Bearer ${CDE_TOKEN}" \
-H "Content-Type: application/json" \
-d '{
 "acls": {
      "full_access": {
          "users": ["*"]
      }
}
}'
```

- This example shows adding cdpuser1 to view-only access, cdpuser2 to full-access, and removing the wildcard from full-access replacing the existing artifact sharing.

```
# add cdpuser1 to view-only, cdpuser2 to full-access, and remove wildcard from full-access (replaces the existing artifact sharing)
curl -X PATCH \
https://qnrjlcs6.cde-fllv7d7m.apps.apps.shared-rke-dev-01.kcloud.cloudera.com/dex/api/v1/jobs/job-1 \
-H "Authorization: Bearer ${CDE_TOKEN}" \
-H "Content-Type: application/json" \
-d '{
 "acls": {
      "full_access": {
          "users": ["cdpuser2"]
      },
  "view_only": {
   "users": ["cdpuser1"]
  }
}
}'
```

- This examples shows combining user and groups.

```
# combine user and groups
curl -X PATCH \
https://qnrjlcs6.cde-fllv7d7m.apps.apps.shared-rke-dev-01.kcloud.cloud
era.com/dex/api/v1/jobs/job-1 \
-H "Authorization: Bearer ${CDE_TOKEN}" \
-H "Content-Type: application/json" \
-d '{
 "acls": {
      "full_access": {
          "groups": ["hivetest"]
      },
  "view_only": {
   "users": ["cdpuser1"]
  }
}
}'
```

Stop sharing an artifact with a user or group

Learn about how to stop sharing an artifact with a user or group.

Prerequisites

- When you want to share an artifact or stop sharing an artifact, you must provide the Workload User Name of the user in the Cloudera Data Engineering CLI or Cloudera Data Engineering API. To check your workload user name, go to Cloudera Management Console User Management Users , find the user name, and then find the Workload User Name.

For Cloudera Data Engineering UI

Note: From Cloudera Data Engineering 1.5.5 SP1 onward, you can stop sharing the artifacts using Cloudera Data Engineering UI.

To stop sharing jobs with a user or group, perform the following steps:

1. In the Cloudera console, click the Data Engineering tile. The Cloudera Data Engineering Home page displays.
2. In the left navigation menu, click Jobs. The Jobs page is displayed.
3. Select the job that you want to stop sharing and click on the Sharing tab.
4. In the Users and Groups table, click the 🗑 icon under the Actions column for the user or group that you want to stop sharing the job.
5. In the Remove Assignment pop-up, click Remove.

To stop sharing repositories with a user or group, perform the following steps:

1. In the Cloudera console, click the Data Engineering tile. The Cloudera Data Engineering Home page displays.
2. In the left navigation menu, click Repositories. The Repositories page is displayed.
3. Select the repository that you want to stop sharing and click on the Sharing tab.
4. In the Users and Groups table, click the 🗑 icon under the Actions column for the user or group that you want to stop sharing the repository.
5. In the Remove Assignment pop-up, click Remove.

To stop sharing resources with a user or group, perform the following steps:

1. In the Cloudera console, click the Data Engineering tile. The Cloudera Data Engineering Home page displays.
2. In the left navigation menu, click Resources. The Resources page is displayed.
3. Select the resource that you want to stop sharing and click on the Sharing tab.
4. In the Users and Groups table, click the 🗑 icon under the Actions column for the user or group that you want to stop sharing the resource.
5. In the Remove Assignment pop-up, click Remove.

For Cloudera Data Engineering CLI

Run the following command to stop sharing an artifact with a user or group:

```
./cde <***ARTIFACT_TYPE***> update -h
Usage:
  cde <***ARTIFACT_TYPE***> update [flags]
Flags:
      --remove-acl-full-access-group stringArray   remove group with full
 access permission (can be repeated to remove multiple groups)
      --remove-acl-full-access-user stringArray    remove user with full
 access permission (can be repeated to remove multiple users) (set '*' v
alue for all VC Users)
      --remove-acl-view-only-group stringArray     remove group with view
 only permission (can be repeated to remove multiple groups)
      --remove-acl-view-only-user stringArray      remove user with vie
w only permission (can be repeated to remove multiple users) (set '*' va
lue for all VC Users)
```

The <****ARTIFACT_TYPE****> value can be job, session, resource, repository, or credential. Only Artifact access management specific flags are shown for clarity.

Examples

The following examples are for jobs. But the same flags apply to sessions, resources, repositories, or credentials.

```
# remove cdpuser5 from view-only, cdpuser6 from full-access
./cde job update --name job-1 --remove-acl-view-only-user 'cdpuser5' --r
emove-acl-full-access-user 'cdpuser6'

# combine user and groups. Add cdpuser5 and qe-group group
./cde job update --name job-1 --add-acl-view-only-user 'cdpuser5' --add-a
cl-full-access-group 'qe-group'
```

For Cloudera Data Engineering API

Important: Passing the artifact sharing configuration overrides the existing configuration for the artifacts. So, to remove users to an access level, you must get the full list of existing users and pass the payload by removing the required users only. To get the existing users list, see Viewing artifact sharing information.

Run the following JSON payload to stop sharing an artifact with a user or a group:

```
curl -X PATCH \
<jobs_api_url>/<***ARTIFACT_TYPE***>/<***ARTIFACT_NAME***> \
-H "Authorization: Bearer ${CDE_TOKEN}" \
-H "Content-Type: application/json" \
-d '{
 "acls": {
      "full_access": {
          "users": []
      },
  "view_only": {
   "users": []
  }
}
}'
```

The <***ARTIFACT_TYPE***> value can be jobs, resource, repository, or credential and the <***ARTIFACT_NAME***> value is the name of the artifact.

Example

This exmaple shows removing cdpuser1 from view-only access and cdpuser2 from full-access.

```
# remove cdpuser1 from view-only and cdpuser2 from full-access
curl -X PATCH \
https://qnrjlcs6.cde-fllv7d7m.apps.apps.shared-rke-dev-01.kcloud.cloudera
.com/dex/api/v1/jobs/job-1 \
-H "Authorization: Bearer ${CDE_TOKEN}" \
-H "Content-Type: application/json" \
-d '{
 "acls": {
      "full_access": {
          "users": []
      },
  "view_only": {
   "users": []
  }
}
}'
```

Viewing artifact sharing information

Learn about how to check with which users or groups an artifact is shared with.

Jobs

You can check with which users or groups a specific Job is shared with.

1. In the Cloudera console, click the Data Engineering tile. The Cloudera Data Engineering Home page displays.
2. Click Jobs.
3. Click the Job for which you want to see the sharing information.
4. Click Sharing. You can see the details of the user or group with whom the Job is shared with and the type of access provided.

Job runs

You can check with which users or groups a specific Job Run is shared with.

1. In the Cloudera console, click the Data Engineering tile. The Cloudera Data Engineering Home page displays.
2. Click Job Runs.
3. Click the job run for which you want to see the sharing information.
4. Click Sharing. You can see the details of the user or group with whom the job run is shared with and the type of access provided.

Sessions

You can check with which users or groups a specific Session is shared with.

1. In the Cloudera console, click the Data Engineering tile. The Cloudera Data Engineering Home page displays.

2. Click Sessions.
3. Click the session for which you want to see the sharing information.
4. Click Sharing. You can see the details of the user or group with whom the session is shared with and the type of access provided.

Viewing artifact sharing information through Cloudera Data Engineering CLI

Run the following command to see the information about the users or the groups with whom the artifact is shared with:

```
./cde <***ARTIFACT_TYPE***> describe  --name <***ARTIFACT_NAME***>
```

Where, <***ARTIFACT_TYPE***> is job, job run, session, repository, or resource and <***ARTIFACT_NAME***> is the name of the artifact.

For example: The following example is for jobs.

```
./cde job describe  --name cli-sample
{
  "name": "cli-sample",
  "type": "spark",
  ...
  ...
  "acls": {
    "full_access": {
      "users": [
        "fullaccess1",
        "fullaccess2"
      ],
      "groups": [
        "group2"
      ]
    },
    "view_only": {
      "users": [
        "cdpuser2",
        "cdpuser3"
      ],
      "groups": [
        "group1"
      ]
    }
  },
  "aclsInfo": {
    "accessLevel": "FULL_ACCESS",
    "grantedAt": "2025-04-09T04:54:07.953974557Z"
  }
}
```

Viewing artifact sharing information through Cloudera Data Engineering API

Run the following JSON payload to view the the information about the users or the groups with whom the artifact is shared with in the endpoint:

```
curl -X GET \
<jobs_api_url>/jobs/<***JOB_NAME***> \
-H "Authorization: Bearer ${CDE_TOKEN}" \
-H "accept: application/json"
```

For example,

```
curl -X GET \
https://qnrjlcs6.cde-fllv7d7m.apps.apps.shared-rke-dev-01.kcloud.cloudera.
com/dex/api/v1/jobs/job-1 \
-H "Authorization: Bearer ${CDE_TOKEN}" \
-H "Content-Type: application/json"

{
       "name": "job-1",
       "type": "spark",
        ...
       "acls": {
             "full_access": {
                    "users": ["user1", "user2"],
                    "groups": ["group1", "group2"]
             },
             "view_only": {
                   "users": ["user3"],
                   "groups": ["group3"]
             }
}
```