CDP Private Cloud Data Services 1.5.0

CDP Private Cloud Data Services User Management

Date published: 2020-12-16
Date modified: 2023-01-25

https://docs.cloudera.com/

Legal Notice

© Cloudera Inc. 2025. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Unless otherwise noted, scripts and sample code are licensed under the Apache License, Version 2.0.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 (“ASLv2”), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

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.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

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

Managing user access and authorization..... 4

Access paths to CDP and its components..... 5

Onboarding users..... 6
Configuring identity providers..... 6
Configuring LDAP authentication for CDP Private Cloud..... 6
Updating an identity provider..... 8
Changing your Local Administrator password..... 9
Importing or uploading users..... 9
Synchronizing group membership..... 10

Understanding CDP Private Cloud user accounts..... 11
CDP account administrator..... 11
CDP user..... 11
CDP machine user..... 12

Working with machine users..... 12
Creating a machine user..... 12
Generating an API access key..... 13
Deleting a machine user..... 14

Understanding roles..... 14
Assigning account-level roles to users..... 16
Assigning resources to users..... 17

Enabling admin and user access to environments..... 18

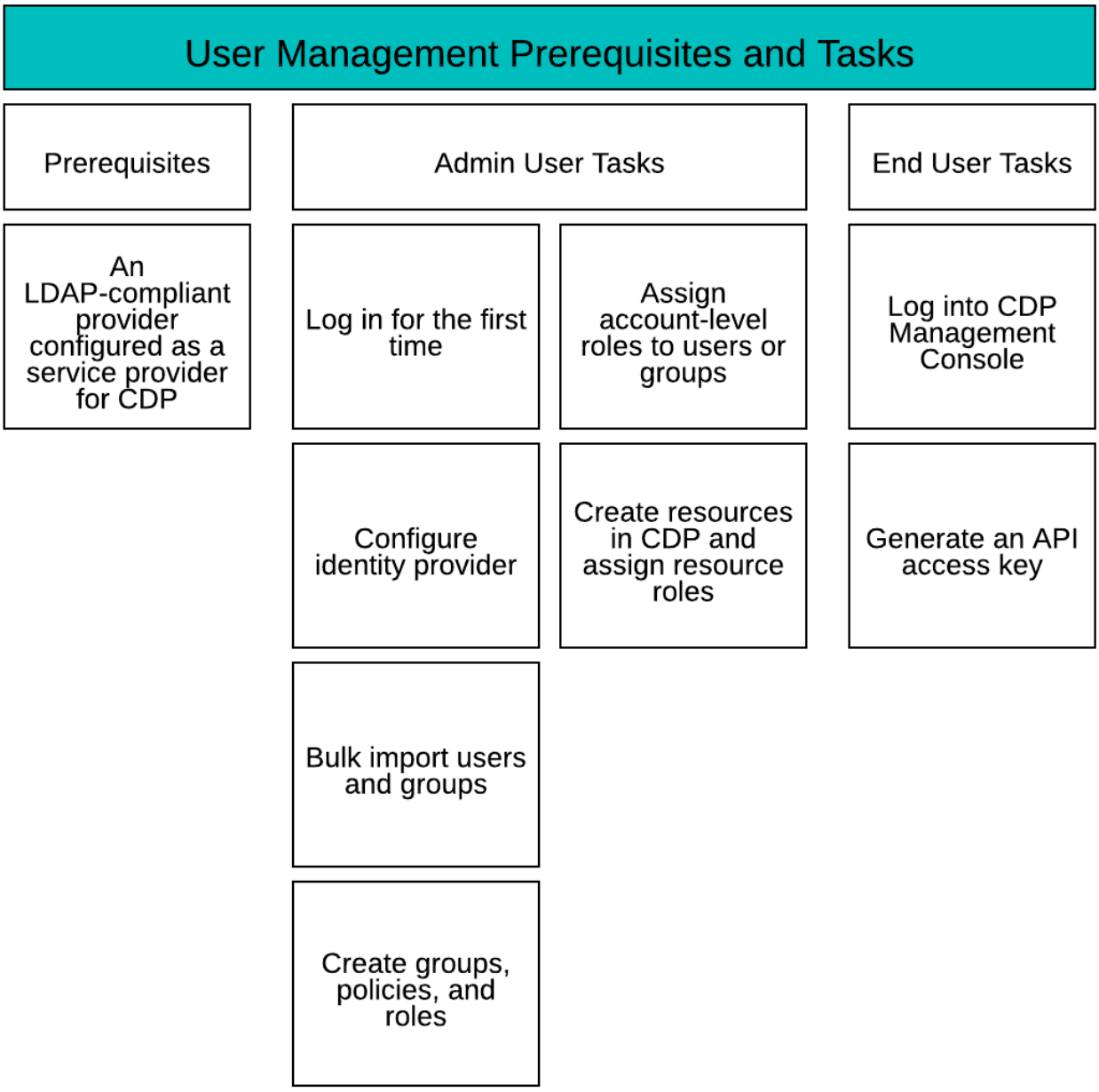
Understanding CDP groups..... 18
Creating a group..... 18
Adding or removing a user from a group..... 19
Assigning account roles to a group..... 20
Assigning resource roles to a group..... 21
Assigning a group membership administrator..... 22
Removing a group membership administrator..... 23
Updating a group..... 23
Removing account roles from a group..... 24
Deleting a group..... 25
Reserved group names..... 25

Managing user access and authorization

To provide access to resources such as environments and clusters, you must add users and assign roles and resources to them.

Using the CDP Private Cloud Management Console, you can perform the following tasks:

- Onboarding users
  - Configuring identity providers
  - Importing or uploading users
- Managing users
  - Adding users
  - Creating machine users
  - Deleting machine users
  - Assigning roles to users
  - Assigning environments to users
  - Generating access keys to users
  - Removing roles assigned to users
  - Unassigning roles to users
  - Unassigning resources to users
- Managing groups
  - Adding groups
  - Assigning roles to groups
  - Adding users to groups
  - Assigning a group membership administrator
  - Unassigning roles to groups
  - Unassigning resources to groups



Access paths to CDP and its components

To access the various CDP components, you must understand the access paths unique to the entry points that are specific to users and situations.

The typical access entry methods and their details are as follows:

- LDAP access through Management Console - After configuration of LDAP authentication, users can make use of their credentials to access CDP services such as Machine Learning Workspaces and Virtual Data Warehouses. CDP Private Cloud supports both Microsoft Active Directory LDAP and Open LDAP for user authentication.
- SSO access through Management Console - After the initial identity provider configuration, users logged into the Management Console can automatically access services such as Machine Learning Workspaces through internal SSO.

- Machine user access - To get programmatic access to CDP and its services, you can create and use a machine user. The process to set up the machine user for access is as follows:
  - Create a machine user in the User Management section of Management Console.
  - Get access keys in the Management Console for this machine user.

Onboarding users

To enable users to work on the various CDP components and services, you can onboard them by using LDAP.

Configuring identity providers

You can onboard users by setting up identity federation with CDP.

If your organization uses an enterprise Identity Provider (IdP) that is compliant with Lightweight Directory Access Protocol (LDAP), you can set up identity federation with CDP. Identity federation allows users within your organization to log in to CDP through the authentication system in your organization without registering with Cloudera or creating a Cloudera account.

Configuring LDAP authentication for CDP Private Cloud

You can configure LDAP user authentication for CDP Private Cloud from the Administration page of the Management Console.

Before you begin

If you intend to use Hue as your SQL editor in CDW, you must use LDAP over SSL.

Procedure

1. Sign in to the CDP console.
2. Click Management Console.
3. On the Management Console home page, select Administration>Authentication.
4. Configure the following settings for LDAP authentication:

Property	Description	Sample values
LDAP URL	The LDAP server URL. The URL must be prefixed with ldap:// or ldaps://. The URL can optionally specify a custom port, for example: ldaps://ldap_server.example.com:1636.	ldap://<ldap-host>:389 or ldaps://<ldap-host>:636

CA Certificate for Secure LDAP	The X.509 PEM certificate to be used to access secure LDAP (URLs starting with ldaps://). Ensure that at least one valid certificate is provided. A typical CA certificate is structured as follows:
	`-----BEGIN CERTIFICATE-----`
	`...`
	`-----END CERTIFICATE-----`
		If you add or update CA certificates and you have deployed the Cloudera Data Warehouse (CDW) service in your ECS cluster, you must refresh the affected Database Catalogs and Virtual Warehouses from the CDW UI. Go to the CDW UI, click on the more vertical menu on the Database Catalog or Virtual Warehouse and click Refresh.

Property	Description	Sample values
LDAP Bind DN	The Distinguished Name of the user to bind to LDAP for user authentication search/bind and group lookup for role authorization.	Distinguished Name (DN) example: CN=cdh admin,OU=svcaccount,DC=example,DC=com FreeIPA example: uid=username,cn=users,cn=accounts,dc=example,dc=com
LDAP Bind Password	The bind user password.	
LDAP User Search Base	The distinguished name indicating the path within the directory information tree from which to begin user searches.	AD example: cn=users,dc=example,dc=com LDAP example: ou=people,dc=example,dc=com FreeIPA example: cn=accounts,dc=example,dc=com
LDAP User Search Filter	The search filter to use for finding users.	AD example: (sAMAccountName={0}) LDAP example: (uid={0}) Note that a custom attribute can also be used if the directory is configured differently for user names. The {0} expands the currently authenticating user's name entered in the login form for the query. FreeIPA example: (&(uid={0})(objectClass=person))
LDAP Group Search Base	The distinguished name indicating the path within the directory information tree to begin group searches from.	cn=accounts,dc=example,dc=com

LDAP Group Search Filter	The search filter to use for finding groups for authorization of authenticated users for their roles. You must configure this value such that only the groups associated with the user logging in are fetched from the IdP.
	There are two placeholders that can be used to match the groups of a user, {0) and {1}. {0} expands into the user DN and {1} expands into the username.
		For Active Directory and openLDAP compatible directories this will usually be (member={0}), where {0} will be replaced by DN string for a successfully authenticated user through the search/bind process. This requires configuration of the LDAP Bind User Distinguished Name field.
		AD example:
		`(member={0})`
		LDAP/FreeIPA example:
		`(&(member={0})(objectClass=posixgroup)(!(cn=admins)))`

Email Mapping Attribute	The LDAP attribute to be used for mapping the email in Identity Management. If no value is provided, mail is used as the default email mapping attribute. Email is a mandatory value in CDP. If no value is found for the email attribute, a value of {userame}@cdp.example is assumed for the user.	

5. Select Show Other Options and configure the following setting:

Property	Description	Sample values
Username Mapping Attribute	The LDAP attribute to be used for mapping the userId in Identity Management. **Important:** This property must be provided in order for job restore to work in CDE Virtual Clusters.	

Note: If the username and email attributes on the LDAP server contain spaces, Management Console includes the spaces when copying the corresponding attribute information.

6. If required, select Show Other Options and configure the following additional settings:

Property	Description	Sample values
LDAP User Bind Property	The property of the LDAP user object to use when binding to verify the password.	This value should always be set to dn.
Groupname Mapping Attribute	The LDAP attribute to be used for mapping the groupId in Identity Management.	
Group DN Property	The property of user object to use in {{dn}} interpolation of groupSearchFilter.	This value should always be set to dn.
First Name Mapping Attribute	The LDAP attribute to be used for mapping the first name attribute in Identity Management.	
Last Name Mapping Attribute	The LDAP attribute to be used for mapping the last name attribute in Identity Management.	

Note: If the username and email attributes on the LDAP server contain spaces, Management Console includes the spaces when copying the corresponding attribute information.

7. Click Test Connection to verify whether the LDAP information you have provided is valid.

   Management Console attempts a connection with the LDAP source based on the information provided, and returns a confirmation message if the connection is successful.
8. Click Save. The LDAP users are listed on the User Management page.

Updating an identity provider

You can update the access keys and roles associated with a CDP identity provider. To update an identity provider in CDP, you must be a CDP account administrator or have the PowerUser role.

Procedure

1. Sign in to the CDP console.
2. Click Management Console.
3. In the side navigation panel, click User Management.
4. Click the user name you want to update.
5. Click the Roles tab.

   Alternatively, you can click the Actions button and select Update Roles.
6. Choose the checkbox next to the roles you want to add for the user or unclick the checkbox next to roles you want to remove for the user.
7. Click Update.
8. If you choose to use a Bind DN, enter the appropriate information in the LDAP Bind DN and LDAP Bind Password fields.

9. If you want to specify LDAP attribute for mapping the email in Identity Management, enter it in the Email Mapping Attribute field.

   If you do not enter an email, the default is mail.
10. If you are using a non-standard attribute, click Show Other Options.
    a) Enter DN in the LDAP User Bind Property field.
    b) Enter the LDAP attribute for mapping the group ID in Identify Management in the Groupname Mapping Attribute field.
    c) Enter the property of the user object in the Group DN Property field.
    d) Enter the first and last name of the attribute in the First Name Mapping Attribute and Last Name Mapping Attribute fields.

       These attributes are optional.
11. Click Save.
12. Verify the updates and click OK.

    CDP updates the information for the CDP identity provider.

Changing your Local Administrator password

Management Console uses a default password for your Local Administrator account. After you access Management Console for the first time you should change your Local Administrator password for security reasons.

About this task

Procedure

1. Sign in to the CDP console.
2. Click Management Console.
3. On the Management Console home page, select Administration>Authentication.
4. Click Change Password then enter and confirm your new password.
5. Click Change to save your changes.

Importing or uploading users

You can bulk import users to CDP Private Cloud and assign them access rights and roles. Importing users in bulk allows admins to prepare the system for the desired level of access before users log in to CDP Private Cloud.

Procedure

1. Sign in to the CDP console.
2. Click Management Console.
3. Click User Management in the left navigation panel.

   The Users page displays the list of all CDP users.
4. Click Actions.
5. From the dropdown list that appears, click Upload Users.

   The Upload Users page appears.
6. Select an identity provider from the dropdown list.
7. Select an option for adding user details:
   - File Upload - If you want to upload a CSV or a JSON file with the details of the users that you like to add.
   - Direct Input - Enter the user details in the format specified. Make sure you add the header row as specified in the sample.

8. Click Next.
9. In the Preview Users screen that appears, verify if all the details are uploaded or added accurately.
10. Click Upload.

Synchronizing group membership

CDP can synchronize the user's group membership provided by your enterprise Identity Provider (IdP) with the user's group membership in CDP.

When a user initially logs in to CDP through the identity management system in your organization, CDP creates a CDP user account for the user. However, without being assigned CDP roles, the user cannot perform tasks in CDP. Cloudera recommends that you create CDP groups with assigned roles and add users to the groups so that the users can take on the roles assigned to the groups.

When you create an identity provider, you can select the Sync Groups on Login option to enable CDP to synchronize the user group membership. By default, the Sync Groups on Login option is disabled. Clear the option selection if you do not want CDP to synchronize the user group membership.

Group names must be alphanumeric, may include '-' and '_', and be fewer than 32 characters long. Additionally, names can only start with an alphabet or an underscore.

Sync Groups on Login enabled

When the Sync Groups on Login option is enabled, CDP synchronizes a user's group in the following manner:

- The group membership that your enterprise IdP specifies for a user overrides the group membership set up in CDP. Each time a user logs in, CDP updates the user's group membership based on the groups that your enterprise IdP specifies for the user.
- If the group exists in CDP, CDP adds the user to the group. The user takes on all the roles associated with the group.
- If the group does not exist in CDP, CDP creates the group and adds the user to the group. However, no roles are assigned to the new group, so a member of the new group does not take on roles from the group.
- If the user is a member of a group in CDP that is not included in the list provided by your enterprise IdP, CDP removes the user from the group.
- If the list of groups from your enterprise IdP is empty, CDP removes the user from all groups in CDP. After login, the user will not be a member of any CDP group and will not have roles from any group.

To ensure that users can perform tasks in CDP, Cloudera recommends that you set up the groups in CDP with appropriate roles before you assign them to users.

Important: CDP Private Cloud currently *does not support* synchronization of user groups for CDW workloads.

Sync Groups on Login disabled

When the Sync Groups on Login option is disabled, CDP does not synchronize the user's group membership in CDP with the user's group membership provided by the IdP. After login, a user's group membership in CDP is determined by the CDP groups assigned to the user in CDP. The groups assigned to the user in your enterprise IdP are ignored.

Sync Membership option for a newly created group

Additionally, once you have synced your IdP and you create a new group in CDP, you have an option called Sync Membership that determines whether group membership is synced to IdP when a user logs in. By default, Sync Membership is enabled when Sync Groups on Login is enabled.

The following table describes how the global Sync Groups on Login and the per-group Sync Membership options can be used:

	IdP Sync Groups on Login on	IdP Sync Groups on Login off
Group Sync Membership on	Group membership for the specific group is reflected in IdP.	Group membership for the specific group is not reflected in IdP.
Group Sync Membership off	Group membership for the specific group is not reflected in IdP.	Group membership for the specific group is not reflected in IdP.

In other words, if Sync Groups on Login is off at the IdP level, then no groups are getting synced regardless of what the setting for Sync Membership is. But if Sync Groups on Login is turned on at the IDP level, then you have the option to override it for certain groups that you explicitly leave off.

Understanding CDP Private Cloud user accounts

User accounts identify the users who can access services, applications, and components in the Cloudera Data Platform.

Roles assigned to a user account determine the actions that the user can perform in CDP.

There are three types of user accounts in CDP Private Cloud:

- CDP Account administrator
- CDP user
- CDP machine user

CDP account administrator

CDP designates a default user account as a CDP account administrator during the initial setup.

A CDP account administrator has administrator privileges in CDP. The CDP account administrator user account cannot be managed within CDP. The default username and password for CDP account administrator is admin/admin. You should consider changing the default password for security purposes. You must contact Cloudera support to add or remove an account administrator from your CDP account.

As an account administrator, you have all the privileges in CDP and can perform any task in CDP. You can set up users and assign roles, services, and environments to users in CDP according to the tasks that they need to perform. You can set up another user as a CDP administrator by assigning the PowerUser role to the user. However, you cannot set up another user as a CDP account administrator.

CDP user

To perform tasks using CDP and its services, you must be a CDP user with the required roles and resources assigned.

CDP allows users within your organization to log in to CDP through the authentication system in your organization without registering with Cloudera or creating a Cloudera account. During the initial process of configuring the environment, the account administrator must set up identity federation and thus automatically add users.

When a CDP user who is not an account administrator logs in to CDP for the first time, the user has limited privileges. A CDP administrator must assign the appropriate roles to the user after the initial user login.

The CDP account administrator can revoke permissions for a CDP user account. When you revoke permissions for a user, ensure that you remove all the roles that grant the permissions that you want to revoke.

To revoke all permissions granted to a user, complete the following steps:

- Remove all roles assigned to the user.
- Delete any access key created for the user.

A user who has a valid account in CDP but is not assigned any role can perform a limited number of tasks. A user who logs in to the CDP console without an assigned role or environment can perform only the following task:

- View the CDP documentation.

CDP machine user

A machine user account provides programmatic access to CDP. Create a machine user account if you have an application that needs to access the CDP services with Management Console APIs.

You can define the machine user account in your application to create and manage clusters and run jobs in CDP using the CLI or API commands.

You can create and manage a machine user account within CDP. You must assign an API access key to a machine user account to enable it to access the CDP service. You must assign roles to a machine user account to authorize it to perform tasks in CDP.

A machine user account does not have an associated Cloudera user account. You cannot use a machine user to log in to the CDP console.

Machine users created in the control plane are not automatically created in the customer LDAP. Therefore you cannot use machine users to access data in the base cluster.

Use the following guidelines when you manage user accounts in CDP:

- When you create a machine user account, you assign roles and environments to the machine user account in the same way that you assign roles and environments to other user accounts.
- When you revoke permissions for a machine user, ensure that you remove all the roles that grant the permissions that you want to revoke. To revoke all permissions granted to a machine user account, complete the following steps:
  - Remove all roles assigned to the machine user.
  - Delete any access key created for the machine user.
- You can delete a machine user account in CDP. You can delete the machine user account on the CDP console.

Working with machine users

For programmatic access to CDP Private Cloud, you must create a machine user. After creating the user, you must also generate an API access key.

Creating a machine user

You must create a machine user for programmatic access to CDP Private Cloud.

Steps

Management Console UI

1. Sign in to the CDP console.
2. Click Management Console.
3. Select User Management > Users.
4. From the Actions menu, select Create Machine User.
5. Provide a name and click Create.

CLI

1. Use the following command to create the machine user:

```
cdp iam create-machine-user  \
--machine-user-name MACHINE_USER_NAME
```

2. Generate an API access key for your machine user by using the following command:

```
cdp iam create-machine-user-access-key \
    --machine-user-name MACHINE_USER_NAME
```

What to do next: You must generate an access key for the machine user.

Generating an API access key

A CDP user account (a user or a machine user) must have API access credentials to access CDP services.

About this task

When you use this method to generate an access key and then manually configure the access key in the ~/.cdp/credentials, the access credentials are permanent until they are removed from the ~/.cdp/credentials file. If you prefer that the API access key is shorter-lived, refer to the topic Logging into the CDP CLI/SDK, which describes a method of logging into the CLI/SDK through any SAML-compliant identity provider.

Required roles: Users who have the IAMUser role can generate an access key from their own account page. As a CDP Private Cloud administrator or PowerUser, you can generate an access key for a user account that does not have the IAMUser role.

To generate an API access key using the CLI, refer to the following commands on the IAM documentation page:

- create-user-access-key: for generating access key for users
- create-machine-user-access-key: for generating access key for machine users

To generate an API access key using the Management Console:

Procedure

1. Sign in to the CDP console.
2. Click on your user name in the bottom left corner and then select Profile.
3. On the user profile page that appears, click Generate Access Key.
4. On the **Generate Access Key** pop-up window, click Generate Access Key.

   CDP creates the key and displays the information on the screen.
5. Copy the access key and private key to a text file and send it to the CDP user who requires it.

   The private key is a very long string of characters. Make sure that you copy the full string. You can optionally download the credentials file containing the access key information by clicking Download Credentials File.

   Note: The CDP console displays the API access key immediately after you create it. You must copy or download the access key ID and private key information when it is displayed. Do not exit the console without copying the private key. After you exit the console, there is no other way to view or copy the private key.
6. Click Close to exit the access key window.

Results

Once you have generated the access key, you can configure CDP CLI, SDK, or other utilities that require it.

Deleting a machine user

Deleting a machine user also removes the resources associated with the user.

Steps

Management Console UI

1. Sign in to the CDP console.
2. From the CDP home page, click Management Console.
3. Click User Management.

   The Users page displays the list of all the available CDP users.
4. Search for the machine user that you want to delete and click the vertical ellipsis (three dots) against that user.
5. Click Delete Machine User and then OK on the confirmation screen.

CLI

Use the following command to delete the machine user:

```
cdp iam delete-machine-user \
--machine-user-name <value>
```

Note: For a detailed description of the command properties, use cdp --help:

```
cdp iam delete-machine-user --help
```

Understanding roles

To access resources and perform tasks in CDP, each user requires permissions. As a CDP administrator, you can assign a role to a user to give the user permission to perform the tasks.

A policy defines the permissions associated with a role. It consists of policy statements that grant permissions to resources. The policies attached to a role determine the operations that the role allows the user to perform. When users attempt to perform operations that are not permitted in their assigned role, they get a permission denied error message.

CDP provides the following types of roles:

- Account-level roles: These are global roles not associated with any specific resource. CDP has certain predefined account-level roles that you can assign to users.
- Resource roles: These are resource-specific roles that provide permissions to perform tasks on a specific resource, such as a CDW virtual warehouse.

The scope of predefined roles and resource roles can vary. For example, a role might grant view access only to CML clusters but not CDW clusters. You might need to assign multiple roles to ensure that a user can perform all the required tasks in CDP.

Account-level roles

An account-level role grants permissions to perform tasks in CDP that are not associated with a specific resource. You explicitly assign a role to a user account.

The predefined account-level roles available in CDP that you can assign to CDP users, machine users, and groups are as follows:

Table 1: CDP roles

CDP role	Description
PowerUser	Grants permission to perform all tasks on all resources. **Note:** Only a CDP account administrator or a user with the PowerUser role can create environments or assign roles to a user. Only a CDP account administrator or a user with the PowerUser or EnvironmentAdmin resource role can download and update the Kubernetes configuration file, and view the compute cluster information.
IamUser	Grants permission to create access keys for the user, view assigned roles, and view all users in the account.
IamViewer	Grants permission to view assigned roles and view all users in the account.
EnvironmentAdmin	Grants a CDP user all the rights to an environment and a data lake. The EnvironmentAdmin role is assigned the Limited Cluster Administrator role in Cloudera Manager. Environment Admins can manage the cluster lifecycle, change configurations, and manage parcels.
EnvironmentUser	Grants a CDP user the ability to view data lakes and set the password for the environment. The EnvironmentUser role is assigned the Read-Only role in Cloudera Manager.

Note:

Only a CDP account administrator or a user with the PowerUser role can create environments, create and manage data lakes, and assign roles to a user.

Resource roles

A resource role grants permission to access and perform tasks using specific resources.

When you assign a resource role, you must specify the resource on which to grant the resource role permissions. For example, you can assign a user a resource role that grants permission on a virtual warehouse. The user assigned the resource role can access and perform tasks on only the resources associated with the virtual warehouse.

The resource role determines the tasks that the user can perform using the resources associated with the role. For example, the MLUser resource role assigned to a user allows the user to view the Cloudera Machine Learning workspaces provisioned within an environment.

You cannot modify the pre-defined resource roles or the policies associated with the pre-defined resource roles.

The pre-defined resource roles available in CDP that you can assign to CDP users, machine users, and groups are as follows:

- ### Table 2: Resource roles

Resource role	Description
DWAdmin	Grants a CDP user/group the ability to activate/terminate or launch/stop/update services in Virtual Warehouses.
DWUser	Grants a CDP user/group the ability to view and use Cloudera Data Warehouse clusters within a given CDP environment.
MLAdmin	Grants a CDP user/group the ability to create and delete Cloudera Machine Learning workspaces within a given CDP environment. MLAdmins also have Administrator level access to all the workspaces provisioned within this environment. They can run workloads, monitor, and manage all user activity on these workspaces.

Resource role	Description
MLUser	Grants a CDP user/group the ability to view Cloudera Machine Learning workspaces provisioned within a given CDP environment. MLUsers will also be able to run workloads on all the workspaces provisioned within this environment.
DEAdmin	Grants a CDP user/group the permissions to create, delete, and administer Data Engineering services for a given CDP environment.
DEUser	Grants a CDP user/group the permissions to list and use Data Engineering services for a given CDP environment.

Assigning account-level roles to users

Assign account-level roles to a CDP user to manage the tasks that the user can perform in CDP. You can assign multiple roles to users or machine users to provide them with the permissions they need to perform their required tasks.

Steps

Management Console UI

1. Sign in to the CDP console.
2. Click Management Console.
3. Click User Management.

   The Users page displays the list of all CDP users.
4. Click the name of the user to whom you want to assign a role.

   The user details page displays information about the user.
5. Click the Roles tab.
6. Click Update Roles.
7. On the Update Roles window, select the roles you want to assign to the user.

   To remove a role from the user account, clear the selected role.
8. Click Update.

   The roles that you select displays in the list of roles assigned to the user.

   To remove a role from a user account, click check box next to the assigned role that you want to remove. Click Update to confirm that you want to revoke the role permissions.

CLI

You can use the following command to assign a role to a user or a machine user:

```
cdp iam assign-user-role \
--user-name <value> \
--role <value>
```

To remove a role from a user or a machine user:

```
cdp iam unassign-user-role \
--user-name <value> \
--role <value>
```

To get a list of the roles assigned to a group:

```
cdp iam list-user-assigned-roles \
```

```
--user-name <value>
```

```
cdp iam list-machine-user-assigned-roles \
--machine-user-name <value>
```

Assigning resources to users

Assign a user or a machine user a resource role on the scope of a CDP environment to grant the user access to the resources they need to perform their required tasks.

Steps

Management Console UI

1. Sign in to the CDP console.
2. Click Management Console.
3. Click Environments.
4. In the list of environments that appear, select your environment by clicking on it.

   The Environment Clusters page appears.
5. Click Actions.
6. Click Manage Access in the dropdown list.
7. In the Access tab, enter the name of the user in the Select group or user text box.

   The Update Resource Roles window appears.
8. Select the required resource role.
9. Click Update Roles.

CLI

You can use the following command to assign a resource role to a user or a machine user:

```
cdp iam assign-user-resource-role \
--user-name <value> \
--resource-role-crn <value> \
--resource-crn <value>
```

```
cdp iam assign-machine-user-resource-role \
--machine-user-name <value> \
--resource-role-crn <value> \
--resource-crn <value>
```

Note: The resource-role-crn parameter requires the CRN of the resource role you want to assign to the user. The resource-crn parameter requires the CRN of the resource on which you want to grant the resource role permissions.

To remove a resource role from a user or a machine user:

```
cdp iam unassign-user-resource-role \
--user-name <value> \
--resource-role-crn <value> \
--resource-crn <value>
```

```
cdp iam unassign-machine-user-resource-role \
--machine-user-name <value> \
--resource-role-crn <value> \
--resource-crn <value>
```

To get a list of the resource roles assigned to a user or a machine user:

```
cdp iam list-user-assigned-resource-role \
--user-name <value>
```

```
cdp iam list-machine-user-assigned-resource-role \
--machine-user-name <value>
```

Enabling admin and user access to environments

A user with PowerUser role enables admin and user access to environments in a CDP Private Cloud deployment.

1. A CDP user with PowerUser role creates an environment.
2. The PowerUser assigns the EnvironmentAdmin role to the intended user. For instructions, refer to Assigning account-level roles to users on page 16.
3. Additional admin resource roles enumerated in Understanding roles on page 14 should be assigned if admin access to specific CDP services is needed. For example, for admin access to the Data Warehouse service, assign DWAdmin role. For instructions, refer to Assigning resources to users on page 17.
4. The PowerUser assigns the EnvironmentUser to the intended users. For instructions, refer to Assigning account-level roles to users on page 16.
5. Additional user resource roles enumerated in Understanding roles on page 14 should be assigned if admin access to specific CDP services is needed. For example, for user access to the Data Warehouse service, assign DWUser role. For instructions, refer to Assigning resources to users on page 17.

Understanding CDP groups

A CDP group is a collection of user accounts that have the same roles and resource roles. A group can include CDP user accounts and machine user accounts. A group cannot include other groups. All users in a group inherit the roles and resource roles assigned to the group.

As a CDP administrator, you can create a group and manage the group membership. You can also manage the roles and resources assigned to the group. If you are not a CDP administrator, you can add users to and remove users from a group if you have the PowerUser role.

When you create a group, you do not automatically become a member of the group. To become a member of the group, you must add your user account to the group.

You can use groups to manage user access more efficiently. If multiple users require the same roles, you can create a group, add the user accounts to the group, and assign the required roles to the group. All user accounts in the group are assigned the roles assigned to the group.

Note: You cannot delete a group that already has members, roles, or resource roles assigned. You must first remove all the assignments for the group and only then delete it.

Creating a group

You can create CDP groups based on the tasks performed by CDP users in your organization.

Before you begin: To create a CDP group and to manage the users, roles, and resources in the group, you must have the PowerUser role.

Steps

Management Console UI

1. Sign in to the CDP console.
2. From the CDP home page, click Management Console.
3. In the User Management section of the side navigation panel, click Groups.The Groups page displays the list of all CDP groups.
4. Click Create Group.
5. On the Create Group window, enter the name of the group to create.

   Note: You must consider the following when naming a group:

   - The group name must be unique and not contain any of the reserved group names.
   - The group name can be up to 64 characters and can include only alphanumeric characters, hyphens (-), and underscores (_). The first character in the name must be an alphabetic character or underscore.
   - The group name is not case sensitive. For example, the group name AAa is equivalent to the group name aaa.
   - Depending on your IdP setup in CDP, you may be able to manipulate the Sync Membership option. To learn more about this option, refer to Synchronizing group membership.
6. Click Create. CDP creates the group and adds it to the list of groups on the particular page.

CLI

You can use the following command to create a group:

```
cdp iam create-group \
--group-name <value>
```

Adding or removing a user from a group

You can add a CDP user or a machine user account to a group. You cannot add a group to another group. You can remove a CDP user or a machine user account from a group.

All members of the group inherit the roles and resources assigned to the group.

Note: To add a user or remove a user from a group, you must have the PowerUser or the IamGroupAdmin resource role.

Steps

Management Console UI

1. Sign in to the CDP console.
2. From the CDP home page, click Management Console.
3. In the User Management section of the side navigation panel, click Groups.
4. Click the name of the group to which you want to add a user.

   The details page displays information about the group.
5. Click the Members tab.
6. Add or remove users according to your requirements.

   Adding a user to a group:

   - If the group does not have members, click Add Member. Select the name of the user that you want to add to the group.
   - If the group already has a list of members, click in the Add Member dropdown box. Select the name of the user that you want to add to the group.

   Removing a user from a group:

   - **a.** Click Remove from Group next to the user that you want to remove.
     b. Click OK to confirm that you want to remove the user from the group.

CLI

You can use the following command to add a user to a group:

```
cdp iam add-user-to-group \
--group-name <value> \
--user-id <value>
```

Note: The user-id parameter requires the CRN of the CDP user or machine user.

To remove a user from a group:

```
cdp iam remove-user-from-group \
--group-name <value> \
--user-id <value>
```

To add a machine user to a group:

```
cdp iam add-machine-user-to-group \
--group-name <value> \
--user-id <value>
```

To remove a machine user from a group:

```
cdp iam list-groups-for-machine-user \
--machine-user-name <value>
```

To get a list of the users in a group:

```
cdp iam remove-machine-user-from-group \
--group-name <value> \
--machine-user-name <value>
```

```
cdp iam list-group-members \
--group-name <value>
```

To get the list of groups that a user or machine user is a member of:

```
cdp iam list-groups-for-user \
--user-id <value>
```

```
cdp iam list-groups-for-machine-user \
--machine-user-name <value>
```

Assigning account roles to a group

When you assign a role to a group, the role is also assigned to all user and machine user accounts in the group.

Steps

Management Console UI

1. Sign in to the CDP console.
2. From the CDP home page, click Management Console.
3. In the User Management section of the side navigation panel, click Groups.

   The Groups page displays the list of the available CDP groups.

4. Click the name of the group to which you want to assign a role.

   The details page displays information about the group.
5. Click the Roles tab.
6. Click Update Roles.
7. On the Update Roles window, select the roles you want to assign to the group.
8. To view the permissions that the role grants to the group, click Policies. To remove a role from the group, clear the selected role.
9. Click Update.

   The roles that you select displays in the list of group roles.

   To remove a role from a group, click Unassign Role next to the role that you want to remove. Click OK to confirm that you want to remove the role permissions from the group.

CLI

You can use the following command to assign a role to a group:

```
cdp iam assign-group-role \
--group-name <value> \
--role <value>
```

To get a list of the roles assigned to a group:

```
cdp iam list-group-assigned-roles \
--group-name <value>
```

Assigning resource roles to a group

When you assign a resource role to a group, the resource role is also assigned to all user and machine user accounts in the group.

Steps

Management Console UI

1. Sign in to the CDP console.
2. From the CDP home page, click Management Console.
3. Click Environments.
4. In the list of environments, select your environment by clicking on it.

   The details page for the selected environment appears.
5. Click Actions.
6. Click Manage Access in the dropdown list.
7. In the Access tab, enter the name of the group in the Select group or user text box.

   The Update Resource Roles window appears.
8. Select the required resource role such as EnvironmentAdmin or EnvironmentUser.
9. Click Update Roles.

CLI

You can use the following command to assign a resource role to a group:

```
cdp iam assign-group-resource-role \
--group-name <value> \
--resource-role-crn <value> \
--resource-crn <value>
```

To remove a resource role from a group:

```
cdp iam unassign-group-resource-role \
--group-name <value> \
--resource-role-crn <value> \
--resource-crn <value>
```

- The resource-role-crn parameter requires the CRN of the resource role you want to assign to the group.
- The resource-crn parameter requires the CRN of the resource on which you want to grant the resource role permissions.

To get a list of the resource roles assigned to a group:

```
cdp iam list-group-assigned-resource-role \
--group-name <value>
```

Assigning a group membership administrator

As a CDP administrator, you can create a CDP group and manage the users, roles, and resources assigned to the group. You can also assign other users and groups the IamGroupAdmin role to allow them to manage the users in the group.

Note: The IamGroupAdmin role grants a user or group the permission to add users to or remove users from a group. The role does not grant permission to manage roles and resources for the group.

Steps

Management Console UI

1. Sign in to the Cloudera CDP console.
2. From the CDP home page, click Management Console.
3. In the User Management section of the side navigation panel, click Groups.

   The Groups page displays the list of the available CDP groups.
4. Click the name of the group to which you want to assign a group membership administrator.

   The details page displays information about the particular group.
5. Click the Admins tab.
6. Click in the Select group or user dropdown box.

   CDP displays the list of groups and users to which you can give group membership administrator permissions.
7. Select the name of a group or user.

   The name of the group or user you select displays in the list of group membership administrators.

CLI

You can assign the IamGroupAdmin resource role to users and groups to allow them to manage the users in a specified group.

You can use the following command to assign the IamGroupAdmin role to a user:

```
cdp iam assign-user-resource-role \
--user <value> \
--resource-role-crn <value> \
--resource-crn <value>
```

- The user parameter requires the CRN of the user to whom you want to assign the IamGroupAdmin resource role.
- The resource-role-crn parameter requires the CRN of the IamGroupAdmin role.
- The resource-crn parameter requires the CRN of the group on which the user will have administrator permission.

To assign the IamGroupAdmin role to a group:

```
cdp iam assign-group-resource-role \
--group-name <value>e \
--resource-role-crn <value> \
--resource-crn <value>
```

- The group-name parameter requires the name of the group to which you want to assign the resource role.
- The resource-role-crn parameter requires the CRN of the IamGroupAdmin role.
- The resource-crn parameter requires the CRN of the group on which the group specified in the group-name parameter will have administrator permission.

  For example, to assign the IamGroupAdmin to GroupABC so that GroupABC can manage the users in GroupXYZ, run a command similar to the following command:

  ```
  cdp iam assign-group-resource-role \
  --group-name groupABC \
  --resource-role-crn crn:cdp:iam:us-west-1:cdp:resourceRole:IamGroupAdmin \
  --resource-crn crn:cdp:iam:us-west-1:4e9d74e5-1cad-47d8-b645-7ccf9edbb73
  d:group:GroupXYZ/54218ac1-187b-40f7-aadb-5ghm96c35xy4
  ```
- To assign the users in a group to be the administrators of their own group, set the values of the group-name parameter and the resource-crn parameter to refer to the same group.

Removing a group membership administrator

If required, you can remove a particular user or group as the administrator of a group.

About this task

To remove a group membership administrator, you must have the PowerUser role.

Procedure

1. Sign in to the Cloudera CDP console.
2. From the CDP home page, click Management Console.
3. In the User Management section of the side navigation panel, click Groups.

   The Groups page displays the list of the available CDP groups.
4. Click the name of the group for which you want to remove a group membership administrator.

   The details page displays information about the particular group.
5. Click the Admins tab.
6. Click Remove Admin next to the user or group that you want to remove as the group administrator.
7. Click OK to confirm that you want to remove the selected user or group as the administrator.

Updating a group

Depending on your IdP setup in CDP, you can enable or disable the Sync Membership option for a group.

Before you begin

To manage CDP groups, you must have the PowerUser role.

Steps

Management Console UI

1. Sign in to the CDP console.

2. From the CDP home page, click Management Console.
3. In the User Management section of the side navigation panel, click Groups.

   The Groups page displays the list of the available CDP groups.
4. From the context menu to the right of the desired group, click Update Group.
5. Select or deselect the Sync Membership checkbox.
6. Click Update.

CLI

Depending on your requirement can use either of the following parameters with the cdp iam update-group command to update a group:

```
cdp iam update-group \
--group-name<value> \
--sync-membership-on-user-login
```

OR

```
cdp iam update-group \
--group-name <value> \
--no-sync-membership-on-user-login
```

Removing account roles from a group

When you unassign a role from a group, the role is also unassigned from all user and machine user accounts in the group.

Steps

Management Console UI

1. Sign in to the CDP console.
2. From the CDP home page, click Management Console.
3. In the User Management section of the side navigation panel, click Groups.

   The Groups page displays the list of all CDP groups.
4. Click the name of the group from which you want to remove the account role.

   The details page displays information about the group.
5. Click the Roles tab.
6. From the context menu to the right of a role, click Unassign role.
7. Click OK to confirm that you want to remove the role permissions from the group.

CLI

To remove a role from a group:

```
cdp iam unassign-group-role \
--group-name <value> \
--role <value>
```

The role parameter requires the CRN of the CDP role.

To get a list of the roles assigned to a group:

```
cdp iam list-group-assigned-roles \
--group-name <value>
```

Deleting a group

You can delete a CDP group if you have the PowerUser role.

Steps

Management Console UI

1. Sign in to the CDP console.
2. From the CDP home page, click Management Console.
3. In the User Management section of the side navigation panel, click Groups.
4. From the context menu to the right of the desired group, click Delete Group.
5. Click OK to confirm removal.

   CDP removes the group and from the list on the Groups page.

CLI

Use the following command to delete a CDP group:

```
cdp iam delete-group \
--group-name <value>
```

Reserved group names

There are certain group names that are reserved and therefore cannot be used in CDP. This applies to groups synchronized from your identity provider as well as groups created directly from CDP.

If you attempt to synchronize or register a group with a reserved name, you will get an error including the following message:

```
Invalid group name
Name cannot be a reserved group name
```

To avoid problems, review the following list and avoid synchronising or creating groups with the following names.

The following group names are reserved:

- accumulo
- admins
- atlas
- cruisecontrol
- dpprofiler
- druid
- editors
- flink
- flume
- h2o
- hbase
- hdfs
- hive
- httpfs
- hue
- impala
- ipausers
- kafka

- keytrustee
- kms
- knox
- kudu
- livy
- mapred
- nifi
- nifiregistry
- oozie
- phoenix
- ranger
- rangerraz
- schemaregistry
- sentry
- solr
- spark
- sqoop
- sqoop2
- streamsmsgmgr
- streamsrepmgr
- tez
- trust admins
- yarn
- yarn-ats
- zeppelin
- zookeeper