

Machine Learning

Personal and Team Accounts

Date published: 2020-07-16

Date modified: 2024-06-11

CLOUDERA

<https://docs.cloudera.com/>

Legal Notice

© Cloudera Inc. 2024. 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

User Roles.....	4
Business Users and CML.....	5
Managing your Personal Account.....	5
Creating a Team.....	6
Managing a Team Account.....	7

User Roles

Users in Cloudera Machine Learning are assigned one or more of the following roles.



Important: Cloudera Data Platform (CDP) Public Cloud allows customers to maintain full ownership and control of their data and workloads and is designed to operate in some of the most restricted public cloud environments. Since CDP Public Cloud runs in a customer's cloud account, Security and Compliance is a shared responsibility between Cloudera and its public cloud customers. User roles form the first layer of security for securing the ML workloads.

It is your responsibility to diligently allocate the permissions to the users. For more information, see *Cloudera's Shared Responsibility Model*.

There are two categories of roles: environment resource roles, which apply to a given CDP environment, and workspace resource roles, which apply to a single workspace. To use workspace resource roles, you may need to upgrade the workspace or create a new workspace.

If a user has more than one role, then the role with the highest level of permissions takes precedence. If a user is a member of a group, it may gain additional roles through that membership.

Environment resource roles

- **MLAdmin:** Grants a CDP user 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. They can also add the MLUser and MLBusinessUser roles to their assigned environment. This user also needs the account-level role of IAMViewer, in order to access the environment Manage Access page. To create or delete workspaces, this user also needs the EnvironmentAdmin role.
- **MLUser:** Grants a CDP user 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.
- **MLBusinessUser:** Grants permission to list Cloudera Machine Learning workspaces for a given CDP environment. MLBusinessUsers are able to only view applications deployed under the projects that they have been added to as a Business User.

Workspace resource roles

Workspace roles are for users who are granted access to just a single workspace.

- **MLWorkspaceAdmin:** Grants permission to manage all machine learning workloads and settings inside a specific workspace. To perform resource role assignment, the IAMViewer role is also needed. A user with this role can administer the workspace, but is not able to utilize CDP APIs that modify a workspace (for example, creating or upgrading workspaces).
- **MLWorkspaceBusinessUser:** Grants permission to view shared machine learning applications inside a specific workspace.
- **MLWorkspaceUser:** Grants permission to run machine learning workloads inside a specific workspace.

Using the workspace resource roles

A power user or account administrator must assign the first MLWorkspaceAdmin to a workspace. Subsequently, if the MLWorkspaceAdmin also has the IAMViewer role, they can assign resource roles to the workspace.

An MLAdmin (an environment resource role) is not automatically able assign workspace resource roles on the Manage access page. A role such as MLWorkspaceAdmin is needed to do this.

You can check the permissions for a given resource role by clicking the Information icon by each resource role shown in User Management, on the Resources tab for a user, or in a CDP user profile.



Note: Any user that lists users or assigns resource roles also needs the account-level role of IAMViewer.

Related Information

[Cloudera's Shared Responsibility Model](#)

Business Users and CML

A user is treated as a Business User inside of CML if they are granted the `MLBusinessUser` role on the Environment of the given ML Workspace. Inside of the Workspace, a Business User is able to access and view applications, but does not have privileges to access any other workloads in the Workspace.

Logging in as a Business User

When you log in as a Business User, the only page you see is the Applications page. The page shows any applications associated with any projects that you have been added to as a Collaborator, even though you do not have rights to access the other assets associated with those projects.

In order for applications to appear in your view, contact the Project Owner to add you as a Collaborator to the project. If you have not been added to any projects, or none of the projects that you have been added to have applications, the Applications page displays the message, You currently don't have any applications.

Managing your Personal Account

You can edit personal account settings such as email, SSH keys and Hadoop credentials.

About this task

You can also access your personal account settings by clicking Account settings in the upper right-hand corner drop-down menu. This option will always take you to your personal settings page, irrespective of the context you are currently in.

Procedure

1. Sign in to Cloudera Machine Learning.
2. From the upper right drop-down menu, switch context to your personal account.
3. Click Settings.

Profile

You can modify your name, email, and bio on this page.

Teams

This page lists the teams you are a part of and the role assigned to you for each team.

SSH Keys

Your public SSH key resides here. SSH keys provide a useful way to access to external resources such as databases or remote Git repositories. For instructions, see *SSH Keys*.

Related Information

[SSH Keys](#)

Creating a Team

Users who work together on more than one project and want to facilitate collaboration can create a Team. Teams enable you to efficiently manage the users assigned to projects.

About this task

Team projects are owned by the team, rather than an individual user. Team administrators can add or remove members at any time, assigning each member different permissions. A team cannot be deleted and atleast one member must be there on the team.

Site Administration

Overview Users **Teams** Usage Quotas Models Runtime Data Connections Security AMPs Learning Hub Settings Support

Create Team

* Name
data-scientist

Description
Group members of DL

Team Type
☐ Local ☒ Synced Team

Add Groups

Select Group Select Role Add

Viewer
Operator
Contributor
Admin

No data

Cancel Create Team

Procedure

1. In Site Administration Teams , select New Team.

2. Enter the name of the team.

3. Select Local or Synced Team.

CDP manages the member data of a Synced Team. The members and information about the members of a Local team is not managed by CDP.

4. If Synced Team is selected, under Add Groups, select a group name and the role for the group and click Add. You can add multiple groups and roles using the Add option.



Note: By default, each member will inherit the role of the groups they belong to. If a member belongs to multiple groups, their effective role in the team is the highest role assigned to the member (Viewer < Operator < Contributor < Admin).

5. Enter a Description, if needed.

6. Add or invite team members. Team members can have one of the following privilege levels:
 - Viewer - Read-only access to team projects. Cannot create new projects within the team but can be added to existing ones.
 - Operator - Read-only access to team projects. Additionally, Operators can start and stop existing jobs in the projects that they have access to.
 - Contributor - Write-level access to all team projects to all team projects with Team or Public visibility. Can create new projects within the team. They can also be added to existing team projects.
 - Admin - Has complete access to all team projects, can add new team members, and modify team account information. The creator of the team is assigned the Admin privilege, and can also assign other team members the Admin privilege. Each team must have at least one Admin user.
7. Select Create Team.
8. Select Sync Teams to update the teams with information in the CDP management console.

Managing a Team Account

Team administrators can modify account information, add or invite new team members, and view/edit privileges of existing members.

Procedure

1. From the upper right drop-down menu, switch context to the team account.
2. Click Settings to open up the Account Settings dashboard.
3. Modify any of the following settings:

Profile

Modify the team description on this page.

Members

You can add new team members on this page, and modify privilege levels for existing members.

SSH Keys

The team's public SSH key resides here. Team SSH keys provide a useful way to give an entire team access to external resources such as databases. For instructions, see *SSH Keys*. Generally, team SSH keys should not be used to authenticate against Git repositories. Use your personal key instead.

Related Information

[SSH Keys](#)