

CDP One

Accessing Clusters

Date published: 2022-06-03

Date modified: 2022-08-15

CLOUDEXERA

<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

About accessing clusters.....4

Setting a workload password..... 4

Using SSH to access gateway nodes.....6

Registering SSH keys..... 7

Creating an SSH key pair..... 9

About accessing clusters

You can use SSH to access a CDP One gateway node CLI (Command Line Interface), and you can access Hive or Impala via JDBC.

Accessing Hive and Impala via JDBC is described in the [Running SQL Queries](#) guide (see the links below).

Related Information

[Running Hive queries](#)

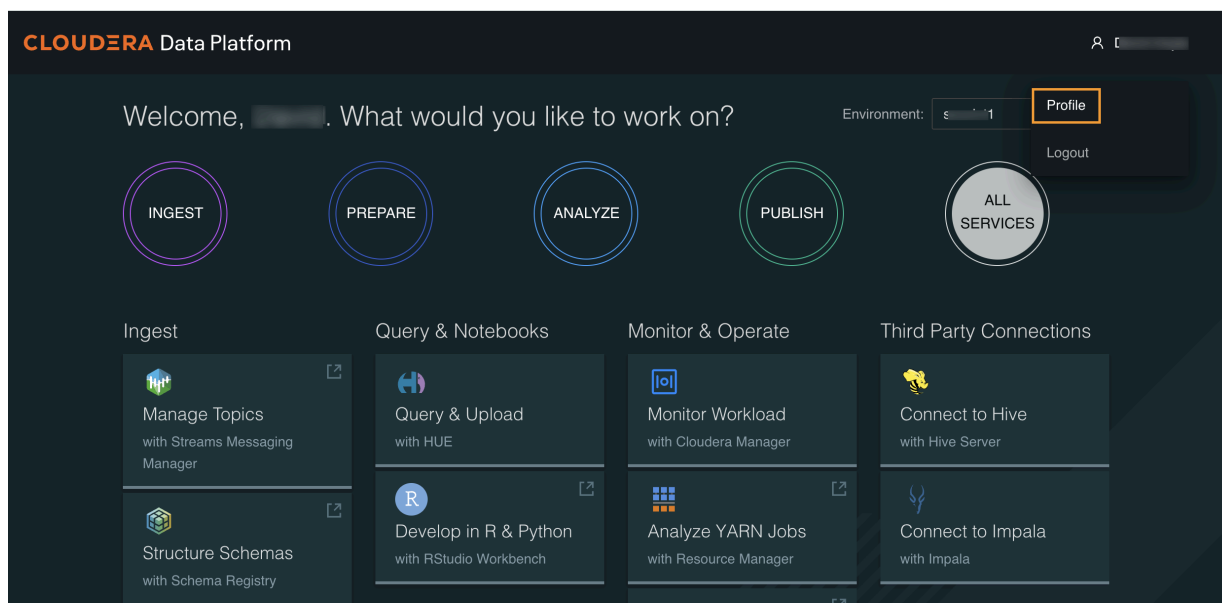
[Running Impala queries](#)

Setting a workload password

You can use your user profile page to set a workload password. Your workload password is used as the SSH password when accessing the gateway node CLI. You must perform a user sync after setting a workload password.

Procedure

1. On the CDP One console, move the pointer over the user icon at the top right of the page, then click Profile.



2. On your user profile page, click Set Workload Password.

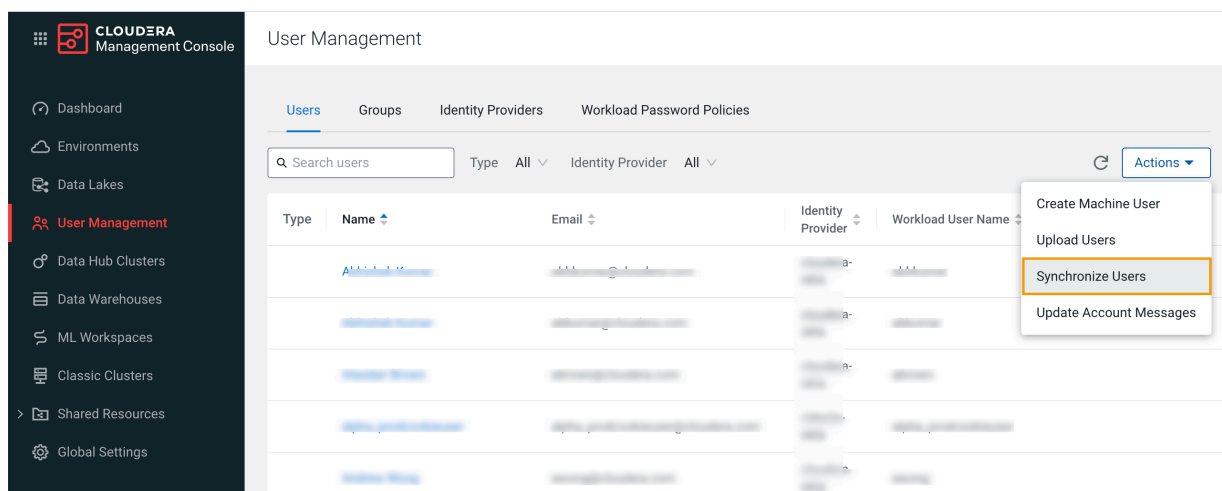
The screenshot shows the Cloudera Management Console interface. On the left is a dark sidebar with navigation links: Dashboard, Environments, Data Lakes, User Management (highlighted), Data Hub Clusters, Data Warehouses, ML Workspaces, Classic Clusters, Shared Resources, and Global Settings. The main content area is titled 'Users / [redacted]'. It displays a user profile with fields: Name, Email, Workload User Name, CRN, Tenant ID, Identity Provider, Last Interactive Login, Profile Management, Workload Password, and Azure Object ID. The 'Workload Password' field is highlighted with an orange box and contains the text 'Set Workload Password' followed by '(Workload password is currently not set)'. Below the profile is a tabbed interface with 'Access Keys' selected, showing 'No access keys found.' and a 'Generate Access Key' button.

3. On the Workload Password page, type in and confirm a workload password, then click Set Workload Password.

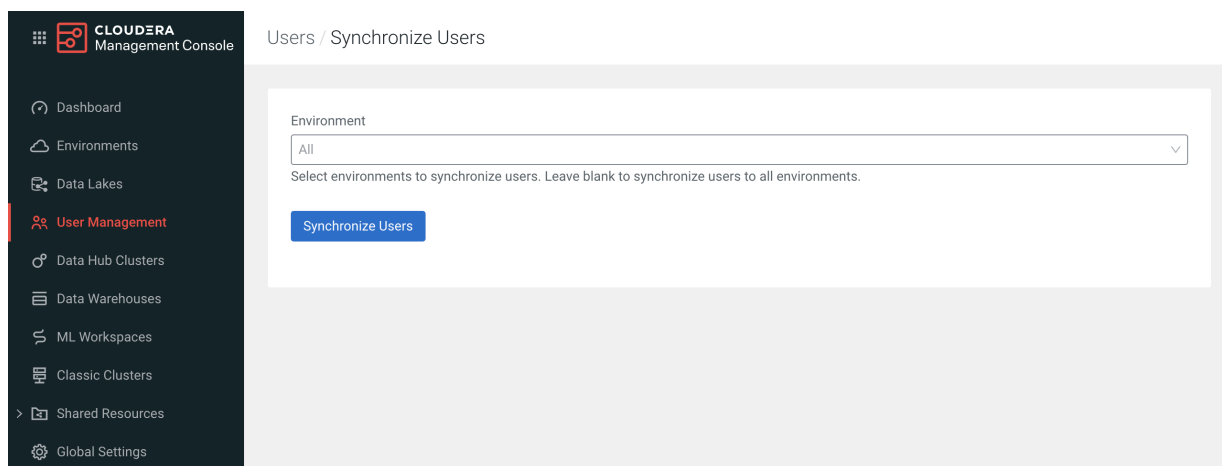
The password must be a minimum of eight characters, and must include at least one upper case character, one lowercase character, one number, and one special character. Supported special characters are "#", "&", "*", "\$", "%", "@", "^", ".", ":", "_", and "!".

The screenshot shows the 'Users / [redacted] / Workload Password' page. It features two input fields: '* Password' and '* Confirm Password'. Below these fields is a blue informational box with a key icon and text: 'If you use keytabs, you need to regenerate them after changing your workload password. You can do this from your user profile > Actions > Get Keytab.' At the bottom is a blue button labeled 'Set Workload Password'.

- Click User Management, then select Actions > Synchronize Users.



- On the Synchronize Users page, all environments are selected by default. You can synchronize users in all environments, or select a specific environment. Click Synchronize Users to synchronize users in the specified environments.



Using SSH to access gateway nodes

You can use SSH to connect to CDP One gateway nodes. This enables you to access the command line utilities of the analytic components in your CDP cluster and perform client tasks, such as querying Hive or Impala remotely from the command line. You use the Secure Shell (SSH) protocol to connect to a node from a terminal utility. Using SSH, you log into the node using a key pair for authentication instead of a user name and password.

Before you begin

- Set a workload password. See [Setting a workload password](#) on page 4.
- Register your SSH key pair for authentication. See [Registering SSH keys](#) on page 7.

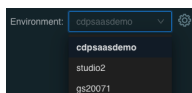


Note: You can only SSH into gateway nodes.

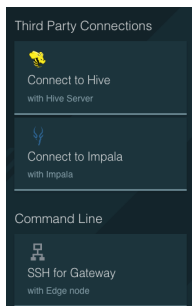
Procedure

- Log into CDP One.

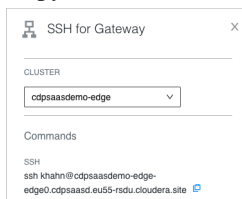
2. In the Environment drop-down list, accept the default environment or select another environment.



3. Click All Services.
4. Under Command Line in the UI, click SSH for Gateway.



5. Copy the SSH command.



6. Open a terminal, and paste the command.

```
$ ssh myname@cdpsaasdemo-edge-edge0.cdpsaasd.eu55-rsdu.cloudera.site
```

7. At the password prompt, enter your workload password.
The connection to the gateway succeeds. The output looks something like this:

```
Last login: Mon Jun 27 21:12:10 2022 from 10.19.9.93
```

```

  _ _ _ _ _
 / _ _ _ _ \
( _ _ _ _ )
 \ _ _ _ _ /
  _ _ _ _ _
  =====

```

Related Information

[Setting a workload password](#)

[Registering SSH keys](#)

Registering SSH keys

You learn how to register an existing Secure Shell (SSH) key pair. Registering the key pair of a user allows the user to access the cluster from the command line. RSA or ED25519 keys are supported.

Before you begin

You must have one of the following roles to complete this task:

- EnvironmentAdmin
- DataSteward
- PowerUser

Procedure

1. Go to the root directory on your computer.
For example, on Linux enter the change directory command:

```
$ cd
```

2. List hidden directories and files and look for the .ssh directory.
For example, on Linux enter the following command:

```
$ ls -ailg
```

3. If you find an .ssh directory, list the files in it.

```
$ cd .ssh  
$ ls
```

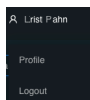
Output might include a private and public key pair, such as the following pair:

```
id_rsa  
id_rsa.pub
```

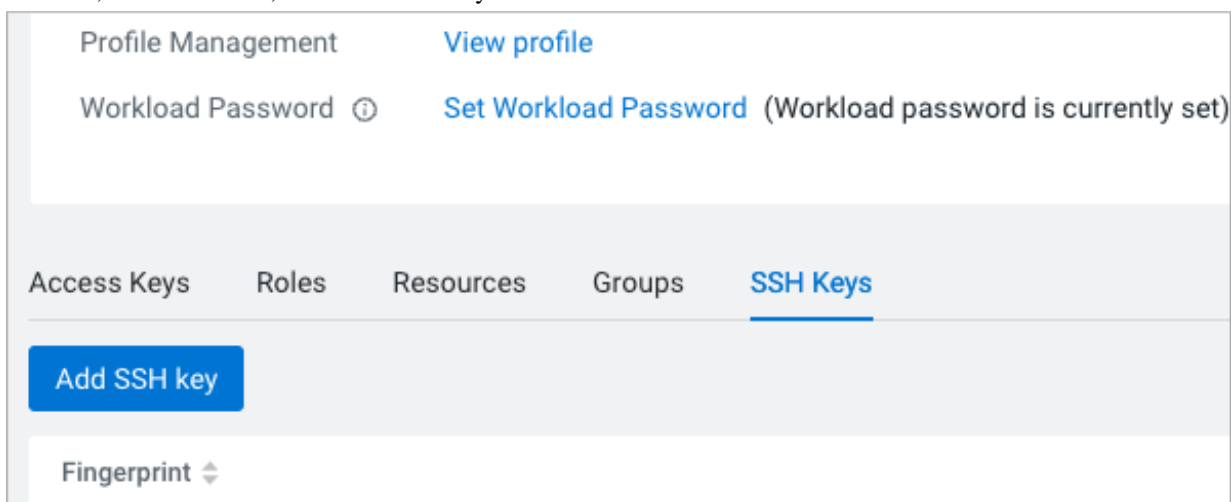
4. If you do not find a .ssh directory, skip the next step, and perform steps in the next topic, “Creating a new key pair”.
5. Copy your SSH public key to the clipboard.
For example, on Linux, enter the following command:

```
pbcopy < ~/.ssh/id_rsa.pub
```

6. In CDP One, click Profile.



7. In Users, on the SSH tab, click Add SSH key.



8. In Add SSH Public Key, click the SSH public key text box, and paste the contents of your clipboard.

Add SSH Public Key

Description

* SSH Public Key

ssh-rsa
AAAAOQABAAACAOC1SSxUv8OdaU/jRFK/o6R6iqAzmwsXN9LxatPniXFXWzwtG
r1A6xig7vUND/cYiEfexVK1xB5p3Xhm3RGiZzIN7thdXuc5i0Y5gXDgOZsyCU0BnbjKWaRseug4m592P+
D34R0lrKHlWmfNw4t3GYhGiCfSSSLMCA3873NSG4D/iaAcMhkeci1YhT1TgSltFkQz5mFmQuk7aa
srUD1ot0JyAhes3av9RkdaHzwE6pAzGzZ0mN94Cy1STc0P59COaYq9Clr88aPoi6JfGFrYC1WNX7p4wl2
HpWKSwwwJP8jEmtgFh0H6wk7GPmnDSSSL7MCA3873NSG4D/iaAcMhkeci1YhT1TgSltFkQz5mFmQuk7aa
YRfo1hiS+0U3SuXkEb2NGU2vdLkSDMOFagmphRFTImvem7PZok3uZPRD0ySQgSrZ+AqHIGUHuiUYTM
R2C3Mhkeci1YhT1TgSltFkQz5mFmQuk7aaYRfo1hiS+0U3SuXkEb2NGU2vdLkSDMOFagmphRFTImvem7PZok3uZPRD0ySQgSrZ+AqHIGUHuiUYTM
5mvJbWGjzNVnoSWkOGYCB12Y8KFtprV7GrVm118LWtEJEipHR8D5BBTp85l1Y6kion5mkFqexti5fpW
wODUtEGluO+Y4VNHrcGbZ0+EQijGcmAr8B4ukDjQkTyfYYIxU3at4hX1lfUTzp1cucb1smdCBYJw==
mulehoofs@gmail.com

Once the SSH key is added, the environment will need to be synced before it can be used for SSH access.

CancelSave

9. Click Save.
10. Synchronize users to the environment.

Creating an SSH key pair

Before you begin

OpenSSH is installed on your machine.

You checked for a pre-existing key pair as described in "Registering SSH keys" above, and found none.

Procedure

1. Open a terminal window, and on the command line, type the key generation command: `ssh-keygen`

```
$ ssh-keygen
```

2. Accept the default location for the keys `~/.ssh` (recommended) and file name `id_rsa` or specify another location and name.
3. At the passphrase prompt, create a password for the key pair.
4. Follow steps in "Registering SSH keys" above to register the keys in CDP.