Workload Password Policies (Preview)

Date published: 2021-04-27
Date modified: 2021-09-14

Legal Notice

This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided ‘as is’ without warranty or support. Further, Cloudera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.

Contents

Revision history

2021-09-14	Added two new workload password policy parameters: *Minimum lifetime of password* and *Number of previous passwords that can't be reused*.
2021-08-26	Added a note.
2021-04-27	Initial draft
2021-05-25	Added Beta CDP CLI instructions.
2021-06-02	Added CDP web interface instructions.
2021-06-03	Removed related links to public CDP CLI docs.

About workload password policies

In order to bring your workload password complexity requirements in line with company policy, you can manage your FreeIPA password policies via CDP web interface and CDP CLI.

Password policies can be configured for length, complexity, expiration, and scope.

Note: Configuring password policies takes effect in all environments within a tenant, but applies to newly configured passwords only. As such, admins should advise users to reset their passwords to achieve compliance with their new password policy.

Warning: There is currently no stable notification system in place that would inform users that their password expired. When users SSH to a node and their password has expired, they may be prompted to reset their password in the SSH session. As resetting the password in the SSH session may only work for a short period, the users should instead set a new workload password using the Management Console in CDP. For instructions, see Setting the workload password.

Password policy types

There are two types of password policies:

- **Global policies** - Apply to all users including machine users
- **Machine user policies** - Apply to machine users only

You can set either or both policies. By default, global policies are applied to all users, including machine users. An optional override for configuring a different policy for machine users is available. For example, setting strict password expiration policies for machine users may not be desired, as password expiration in those accounts may cause upstream failures in the applications that use them.

Default password policy

If a password policy has not been set, the following default password policy is used:

- A minimum password length of 8 characters
- Must include at least 1 upper case character, lowercase character, number and special character.
- The password never expires
- All previous passwords can be reused
- The password can be changed at any time

Install Beta CDP CLI

If you would like to manage workload password policies via CDP CLI, you need to download and install Beta CDP CLI. If you would like to manage the policies using the CDP web interface, skip this step.

Prerequisites

Do not install both the regular and beta CLIs in the same Python environment, as they use the same entry points and will therefore conflict. Either use a separate virtual environment or uninstall the cdpcli first before installing cdpcli-beta.

Steps

1. Install Python if needed, as described in CDP CLI documentation for your platform. Do not install CDP CLI. Instead, proceed to step 2.
2. Run the following to install Beta CDP CLI:
   ```
   pip3 install cdpcli-beta
   ```
3. Configure access keys as described in Generating an API access key.
4. If you have previously installed Beta CDP CLI, you can update it to the latest version using:
   ```
   pip3 install cdpcli-beta --upgrade --user
   ```

Check your current password policy

You can check your current password policy from the **Workload Password Policies** page or using the `cdp iam get-account` CLI command.

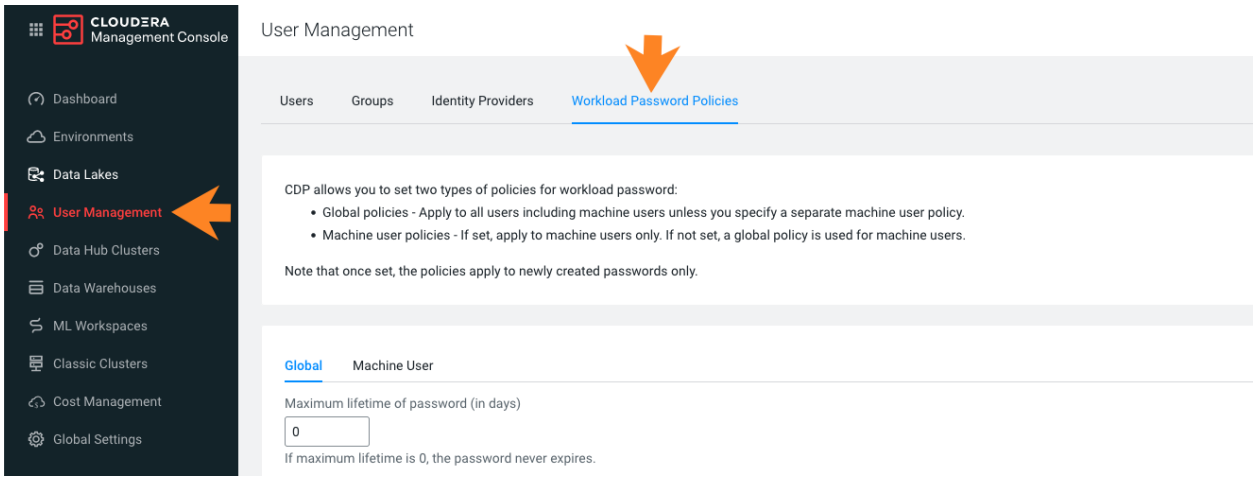
Required Role: PowerUser

Steps - CDP web interface

You can check the current password policy from the **Workload Password Policies** page. To access this page:

1. Log in to the CDP web interface.

2. Navigate to the **Management Console > User Management > Workload Password Policies**:



Steps- CDP CLI

Use the `cdp iam get-account` to obtain your current password policy.

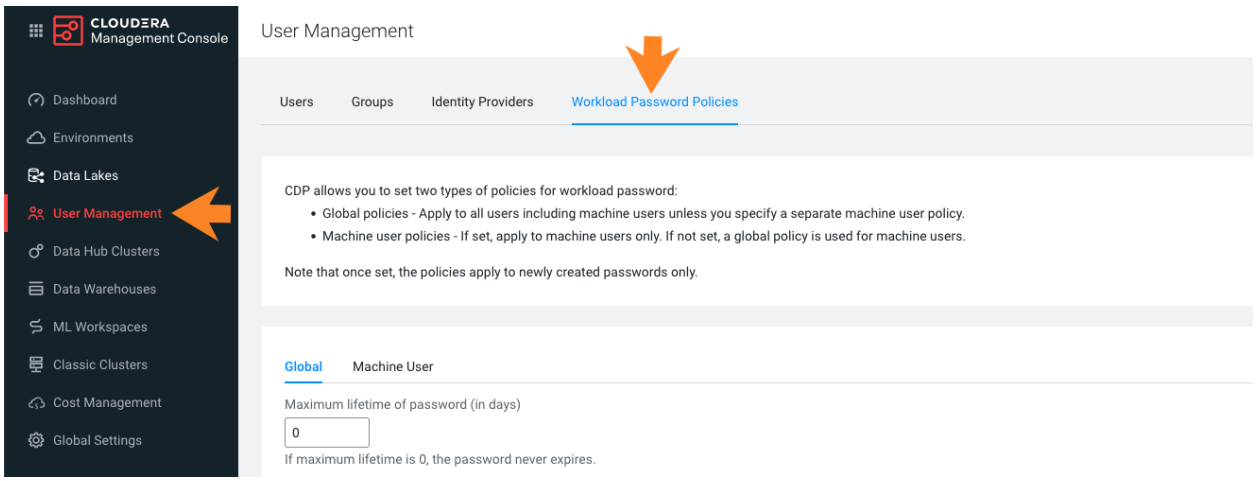
Set a password policy

You can set password policies from the **Workload Password Policies** page or using the via CDP CLI using the `cdp iam set-workload-password-policy` command.

Required Role: PowerUser

Steps - CDP web interface

3. Log in to the CDP web interface.
4. Navigate to the **Management Console > User Management > Workload Password Policies**:



5. In the **Global** tab, specify a policy that applies to all CDP users and machine users. The following options are available:

UI option	Description
Minimum lifetime of password (in days)	Once set, the password must remain the same for this period of time. **Note:** If a user forgets their password, they will be unable to reset it until the minimum period has passed. Even a *PowerUser* or an account administrator will be unable to reset the password in this case.
Maximum lifetime of password (in days)	Allows you to specify password expiration period in days.
Minimum password length	Allows you to specify minimum password length, must be between 6 and 256 characters.
Number of previous passwords that can't be reused	If set to 0, all previous passwords can be reused. Any number larger than 0 indicates the number of most recent passwords that can't be reused. The maximum allowed value for this parameter is 20, so you can prevent users from reusing up to 20 recent passwords. **Note:** Password history information is only recorded when password history size is set to a value other than zero. This means that when the password history size is initially set from zero to non-zero, the previous passwords that were set (while the password history size was as at 0) are not considered when the password history check is done.
Must include uppercase characters	When checked, at least one uppercase character is required
Must include lowercase characters	When checked, at least one lowercase character is required
Must include numbers	When checked, at least one number is required
Must include symbols	When checked, at least one special character is required

6. Click **Update**.
7. By default, global policies are applied to machine users. If you would like to set a different policy for machine users:
    a. Navigate to the **Machine User** tab.

b. Uncheck **Inherit from global policy.**
c. Set a desired policy (the available options are the same as for global policy).
d. Click **Update**.

Steps- CDP CLI
The following example creates a global policy:

```
cdp iam set-workload-password-policy --global-password-policy
minPasswordLength=8,mustIncludeUpperCaseCharacters=true,mustInclude
LowerCaseCharacters=true,mustIncludeNumbers=true,mustIncludeSymbols
=false
```

The following example creates a machine user policy. This overrides the global policy for machine users:

```
cdp iam set-workload-password-policy
--machine-users-password-policy
minPasswordLength=8,mustIncludeUpperCaseCharacters=true,mustInclude
LowerCaseCharacters=true,mustIncludeNumbers=true,mustIncludeSymbols
=true
```

The following password complexity requirements can be set as part of your policy:
Note: The `set-workload-password-policy` command currently does not support partial updates. No parameters are explicitly required, but if you do not specify a parameter, that parameter's value may revert to its default value, “false”, or “0”. As a workaround, when using this command, make sure to specify all parameters.

CLI option	Type	Description	Default value
`minPasswordLifetimeDays`	`integer`	Minimum period in days during which password cannot be changed once it is set **Note:** If a user forgets their password, they will be unable to reset it until the minimum period has passed. Even a *PowerUser* or an account administrator will be unable to reset the password in this case.	0
`maxPasswordLifetimeDays`	`integer`	Expiration period in days	0
`minPasswordLength`	`integer`	Minimum password length; must be between 6 and 256 characters.	8

`passwordHistorySize`	`integer`	Number of previous passwords that can't be reused. 0 indicates that all previous passwords can be reused. Any number above 0 indicates the number of most recent passwords that can't be reused. The maximum allowed value for this parameter is 20, so you can prevent users from reusing up to 20 recent passwords. **Note:** Password history information is only recorded when password history size is set to a value other than zero. This means that when the password history size is initially set from zero to non-zero, the previous passwords that were set (while the password history size was as at 0) are not considered when the password history check is done.	0
`mustIncludeUpperCaseCharacters`	`true|false`	At least one uppercase character is required	true
`mustIncludeLowerCaseCharacters`	`true|false`	At least one lowercase character is required	true
`mustIncludeNumbers`	`true|false`	At least one number is required	true
`mustIncludeSymbols`	`true|false`	At least one special character is required	true

Reset password policies

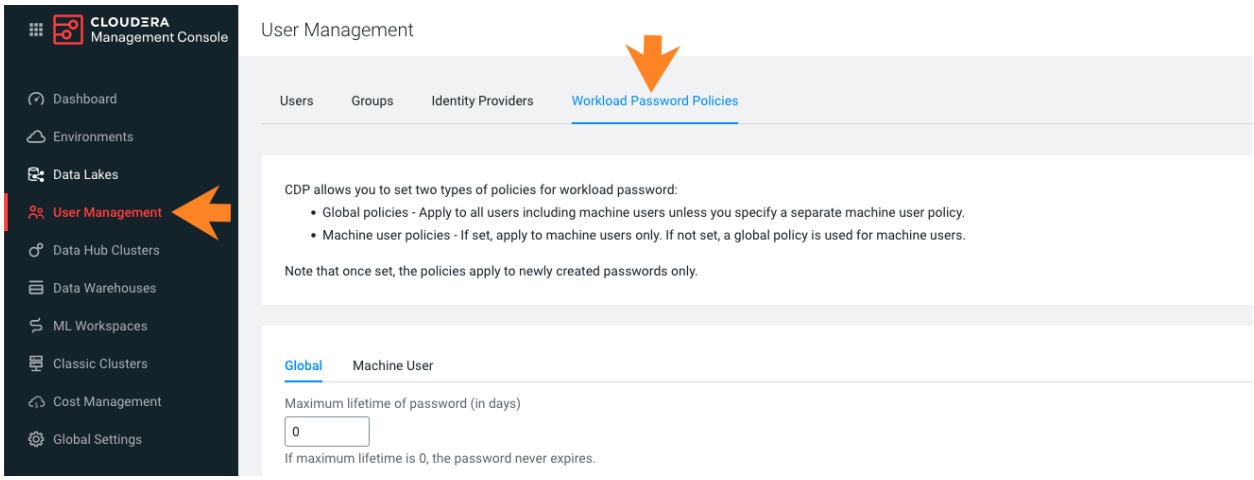
You can reset password policies via CDP CLI using the `cdp iam unset-workload-password-policy` command. As a result, default password policies will be reinstated.

A global password policy is always present for an account. When the global password policy is unset, the policy will revert to the documented defaults. A machine user password policy may or may not be present in the account. When the machine user policy is not set for the account, the global password policy will be enforced for machine users.

Required Role: PowerUser

Steps - CDP web interface

1. Log in to the CDP web interface.
2. Navigate to the **Management Console > User Management > Workload Password Policies**:



3. Navigate to the **Machine User** tab and make sure that **Inherit from global policy** is checked.
   Note: If this option remains unchecked, machine user policies will not be reset.
4. Click on **Reset to default values**.
5. Click **OK** to confirm.

Steps- CDP CLI

Use the following commands to reset password policies:

```
cdp iam unset-workload-password-policy --unset-global-password-policy

cdp iam unset-workload-password-policy --unset-machine-users-password-policy
```