



The announce on release of Two-factor authentication.

April 14, 2020
Fleekdrive Co., Ltd.

Contents

1	Introduction	3
2	Changes from current specifications	4
3	The procedure to set up Two-factor authentication	6
3.1	Set the Two-factor authentication to "Use"	6
3.2	Login method after applying Two-factor authentication	7
3.3	In case of notify mobile phones by SMS	8
3.4	In case of notify by e-mail	9
3.5	Enroll device as trusted	10
4	Login method when authentication fails	11
4.1	Authenticate with Backup Code	11
4.2	Administrator resets settings	12
5	Notes	13

1 Introduction

This document provides information on "Two-factor authentication" to be released with the Major version upgrade (Ver3.0.0) of Fleekdrive on June 13, 2020.

In recent years, cases have frequently occurred where a third party illegally obtains a user ID or password and attempts to log in to a Web service.

Currently, Fleekdrive supports illegal login with various functions, such as a function to lock an account if you enter a wrong password multiple times and a function to restrict the IP address that can be connected.

However, security measures taken by the users themselves were not fully followed.

Therefore, in order to use Fleekdrive in a more secure environment, we will be released a new Two-factor authentication login method that notifies the authentication code by SMS and e-mail with the major version upgrade on June 13, 2020.

With the new authentication method, authentication is performed using two factors: a password (knowledge factor that only the user can know) and an authentication code (factor that is sent to the device or account owned by the user).

It is much more secure than the login method before.

Also, with the release of the above Two-factor authentication, the secret question / answer at the time of password reset will be abolished, and password reset will be possible only by inputting the user ID.

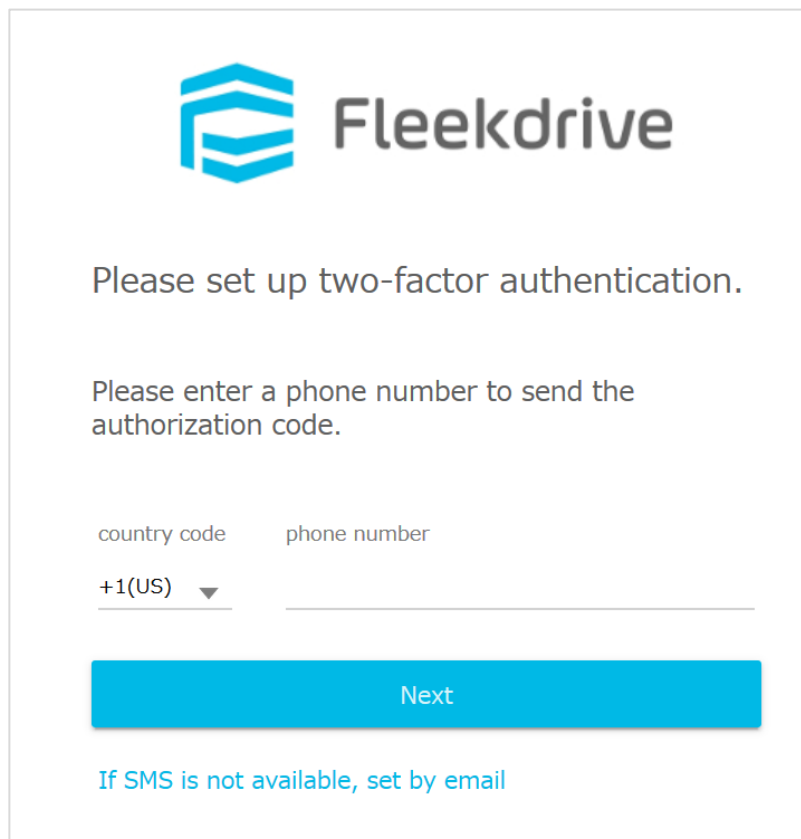
Therefore, we ask that you use Two-factor authentication as necessary to enhance security.

2 Changes from current specifications

1. At Login

In the current specification, only login authentication was performed with a user ID and password. For organizations that have set "Use" for Two-factor authentication, the following screen will be displayed when logging in for the first time after changing the settings, and you will be required to set Two-factor authentication.

Figure 2-1



The screenshot shows the Fleekdrive logo at the top left. Below it, the text reads "Please set up two-factor authentication." followed by "Please enter a phone number to send the authorization code." There are two input fields: "country code" with a dropdown menu showing "+1(US)" and a small downward arrow, and "phone number" with an empty text box. Below these fields is a large blue button labeled "Next". At the bottom, there is a link that says "If SMS is not available, set by email".

2. At reset the password

With the current specifications, if you forget your password, you can enter your secret question and answer, and if the combination matches, you can reset the password yourself.

Figure 2-2 Current password reset screen

Fleekdrive
Password Reset

New password

Confirm Password

--secret question--

answer

Degree of safety of the password: _____

OK CANCEL

After the release on April 25, 2020, the password can be reset only by entering the user ID.

Figure 2-3 Password reset screen after major version upgrade

Fleekdrive
Password Reset

forgot your password?
You can reset your password by entering your user ID.

User ID

SEND CANCEL

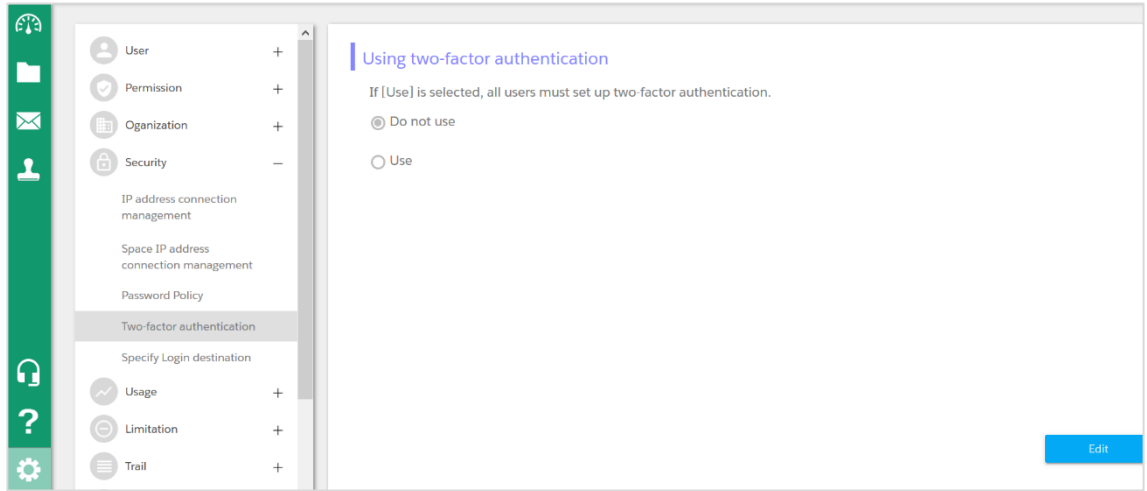
See the next chapter for the actual setting procedure when using Two-factor authentication.

3 The procedure to set up Two-factor authentication

3.1 Set the Two-factor authentication to "Use"

Open Settings> Security> Two-factor authentication.

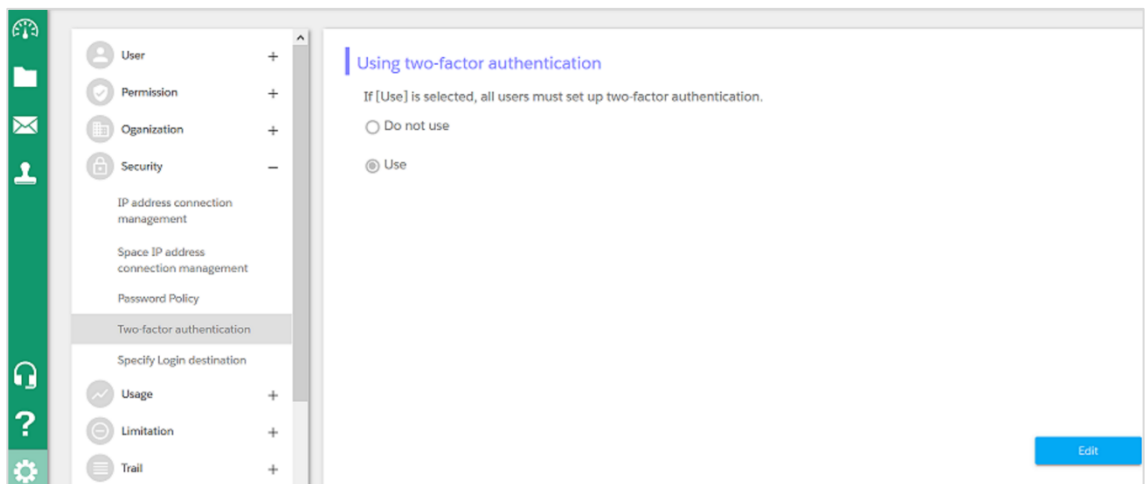
Figure 3-1



By default, two-step authentication is set to [Do not use], so click [Edit] at the bottom right of the screen, change use Two-factor authentication to [Use], and click [OK] button.

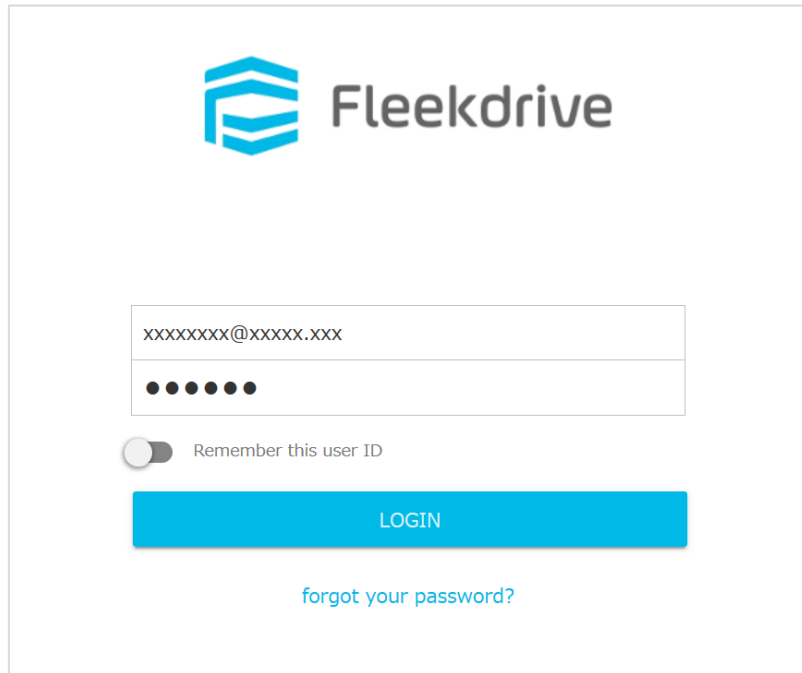
* Applies to all users.

Figure 3-2



3.2 Login method after applying Two-factor authentication
Enter your user ID and password and log in to Fleekdrive.

Figure 3-3



The image shows the Fleekdrive login interface. At the top left is the Fleekdrive logo, a blue stylized 'F' icon. To its right is the text 'Fleekdrive'. Below the logo is a login form with two input fields: the first contains a placeholder email address 'xxxxxxx@xxxxx.xxx' and the second contains six black dots representing a password. Below the password field is a toggle switch labeled 'Remember this user ID', which is currently turned off. A large blue button labeled 'LOGIN' is centered below the form. Below the button is a blue link that says 'forgot your password?'.

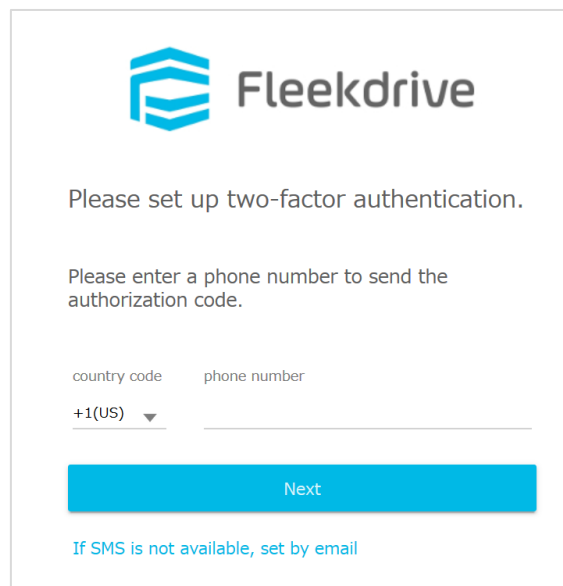
It will be asked to set up Two-factor authentication, so select the destination to send the verification code.

In case of notify mobile phones by SMS→エラー! 参照元が見つかりません。

In case of notify by e-mail→エラー! 参照元が見つかりません。

*SMS has priority.

Figure 3-4

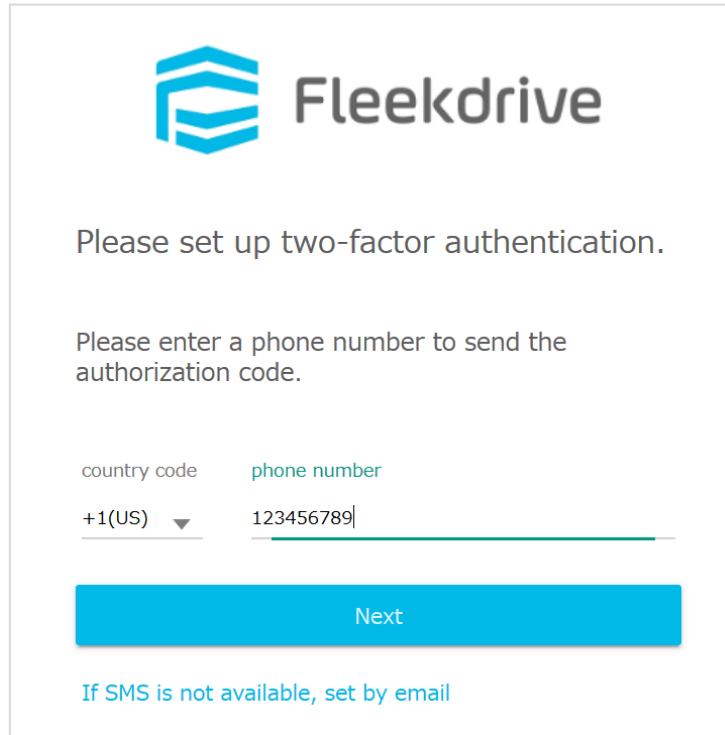


The image shows the Fleekdrive two-factor authentication setup screen. At the top left is the Fleekdrive logo, a blue stylized 'F' icon. To its right is the text 'Fleekdrive'. Below the logo is the text 'Please set up two-factor authentication.' followed by 'Please enter a phone number to send the authorization code.' Below this text are two input fields: 'country code' and 'phone number'. The 'country code' field has a dropdown menu with '+1(US)' selected. Below the input fields is a large blue button labeled 'Next'. Below the button is a blue link that says 'If SMS is not available, set by email'.

3.3 In case of notify mobile phones by SMS

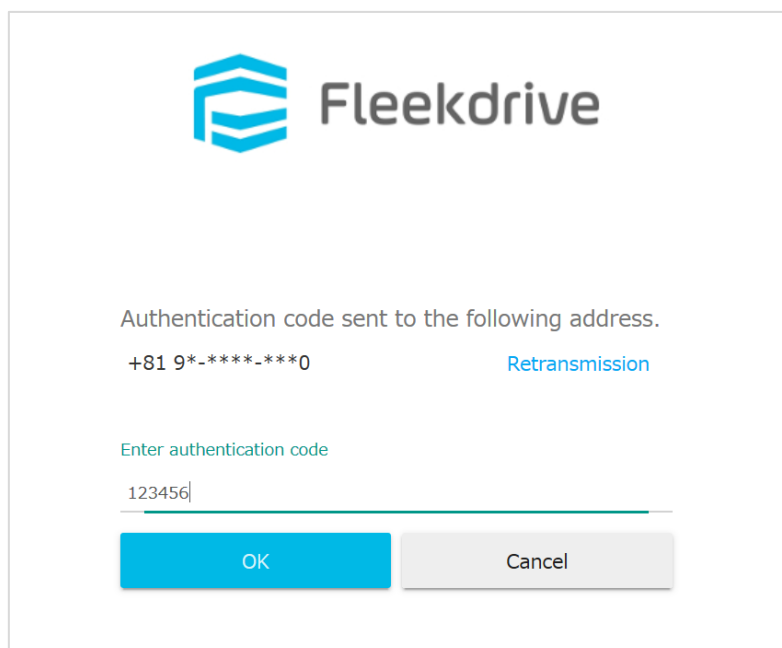
Enter the phone number of the notification destination and click [Next]. The authentication code will be issued and enter the authentication code notified by SMS and click [OK].

Figure 3-5



The screenshot shows the Fleekdrive logo at the top left. Below it, the text reads: "Please set up two-factor authentication." followed by "Please enter a phone number to send the authorization code." There are two input fields: "country code" with a dropdown menu showing "+1(US)" and "phone number" with the text "123456789" entered. A blue "Next" button is positioned below the fields. At the bottom, there is a link that says "If SMS is not available, set by email".

Figure 3-6



The screenshot shows the Fleekdrive logo at the top left. Below it, the text reads: "Authentication code sent to the following address." followed by the phone number "+81 9*-****-***0" and a blue link labeled "Retransmission". Below this, there is a prompt "Enter authentication code" and an input field containing "123456". At the bottom, there are two buttons: a blue "OK" button and a grey "Cancel" button.

3.4 In case of notify by e-mail

Click [Set by e-mail when SMS is not available], and then click [Next].

An authentication code will be issued to the e-mail address registered in Fleekdrive, so enter the notified authentication code.

Figure 3-7

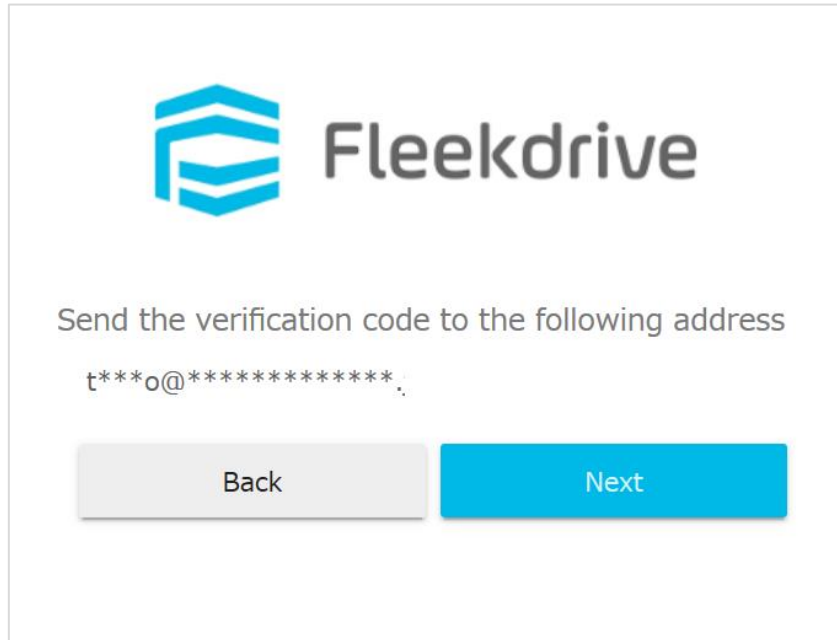
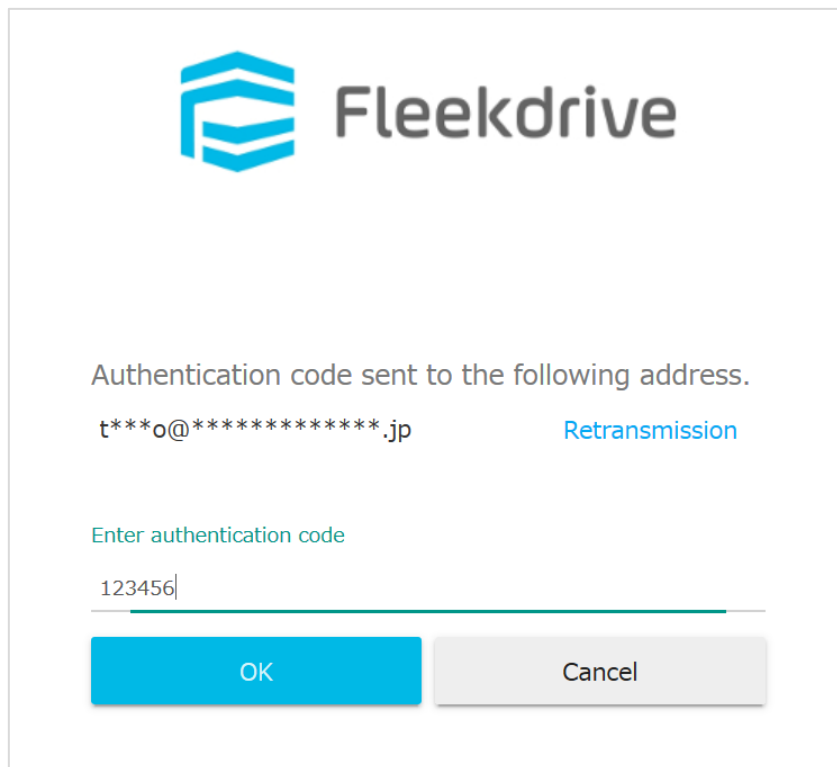


Figure 3-8



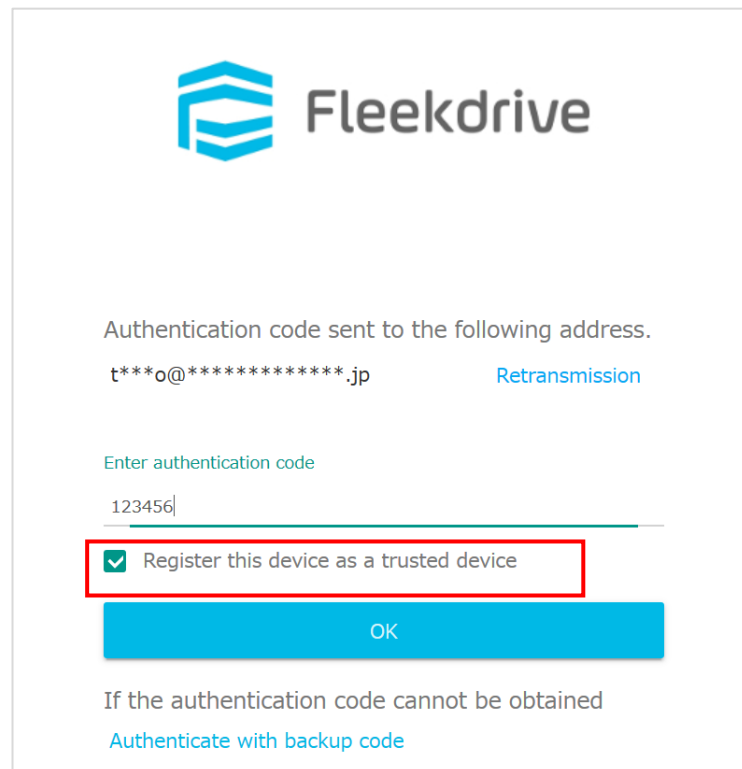
The validity period of the authentication code is 3 minutes after issuance. Resubmit if expired. Please note that if you enter the authentication code more than once, the lock will be activated. The number of maximum invalid login attempts and lockout effective period is based on the password policy.

3.5 Enroll device as trusted

By registering your device as a trusted device, you can skip Two-factor authentication when logging in.

Check "Register this device as a trusted device" when logging in for the second time.

Figure 3-9



The screenshot shows the Fleekdrive login interface. At the top is the Fleekdrive logo. Below it, a message states: "Authentication code sent to the following address." followed by a masked email address "t***o@*****.jp" and a "Retransmission" link. A text input field is labeled "Enter authentication code" and contains "123456". Below the input field is a checkbox labeled "Register this device as a trusted device", which is checked and highlighted with a red rectangular border. Below the checkbox is a blue "OK" button. At the bottom, there is a link: "If the authentication code cannot be obtained" followed by "Authenticate with backup code".

If you register as a trusted device, you can check it from [My Information].

If you remove a trusted device, you will be asked for an authorization code again.

4 Login method when authentication fails

4.1 Authenticate with Backup Code

If the authentication fails, you can also authenticate using the authentication code confirmed in advance from [My Information].

The backup code changes automatically once you use it.

Figure 4-1

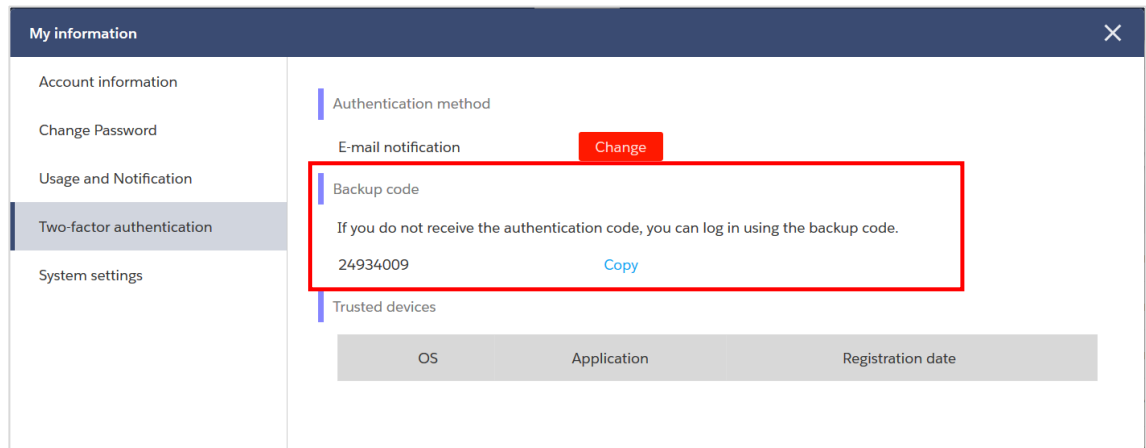
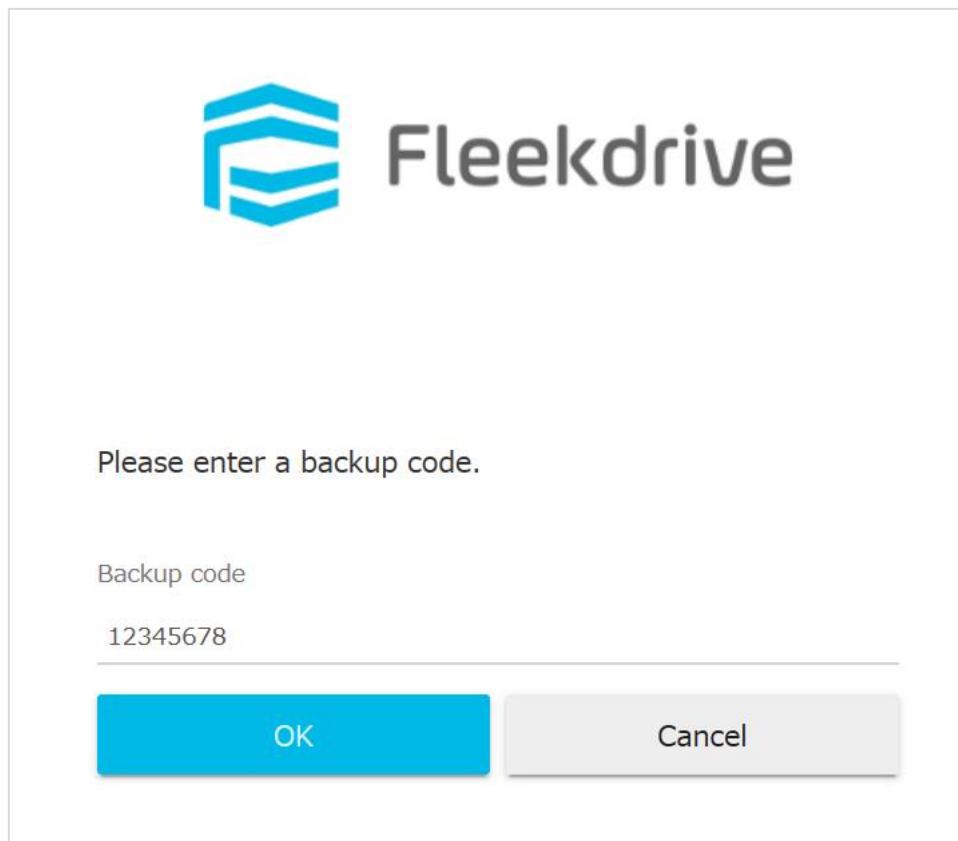


Figure 4-2

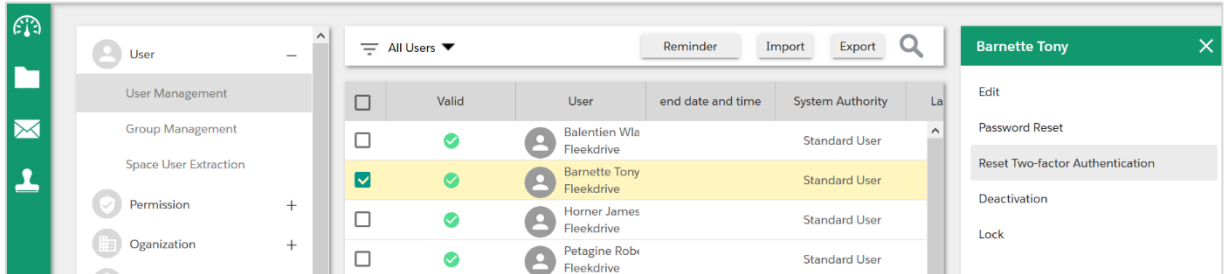


4.2 Administrator resets settings

In Fleekdrive Settings> User Management> User Management, select the user whose settings you want to reset and click [Reset Two-factor authentication] to reset.

For reset users, set the Two-factor authentication from the beginning.

Figure 4-3



5 Notes

- Two-factor authentication is setting for the entire environment. Therefore, it is not possible to set whether or not to use Two-factor authentication for each user.
- Applies to logins from Fleekdrive and Fleekdrive Mobile.
It does not apply to organizations that use single sign-on, use from Salesforce, or log in with the API.
- Once the Two-factor authentication is set to [Use] and then changed to [Do not use], all saved settings will be deleted. After that, if you change it to [Use] again, all users will need to set again.