Sign-in with multi-factor authentication

Multi-factor authentication can be performed at sign-in.

Multi-factor authentication protects accounts from unauthorized access and enhances security.

The multi-factor authentication method is as follows

Email Authentication	The tenant member's e-mail address (the one you set up when you invited them to the Service Management Portal) will be used to verify their identity with a one-time code received via e-mail.
Authentication App	The identity is verified with a time-based one-time code obtained from the authentication application.

NOTE

Multi-factor authentication can be configured from the Service Management Portal.

For details on how to set up multi-factor authentication on the Service Management Portal, please refer to the following.

⇒ Service Management Portal Manual > "Multi-factor Authentication Settings".

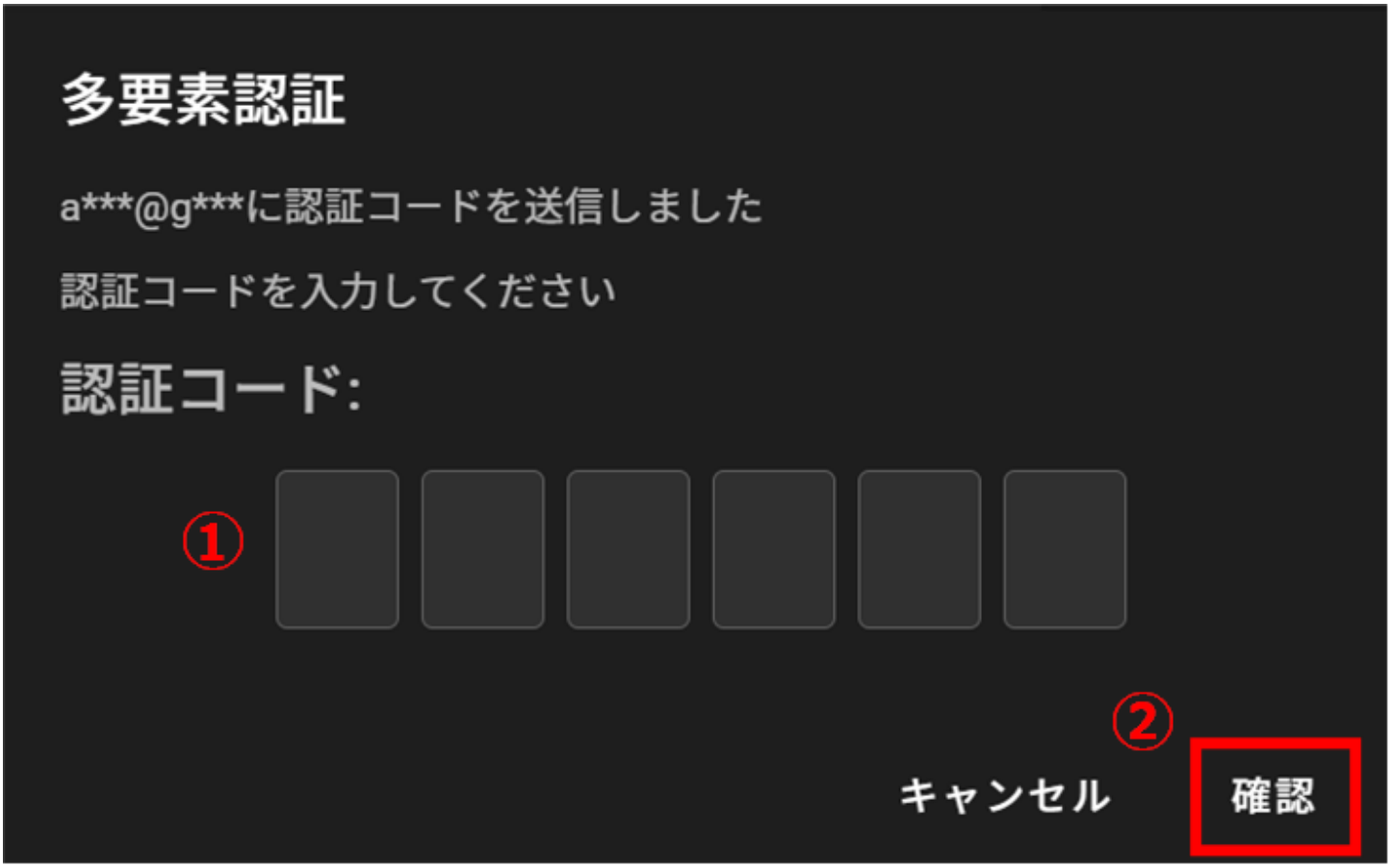
Sign in via email authentication

On the sign-in screen, enter your e-mail address and password, then click "Sign In" to display the multifactor authentication dialog box.

Check the authentication code (6 digits) in the email with the subject line "Authentication Code".

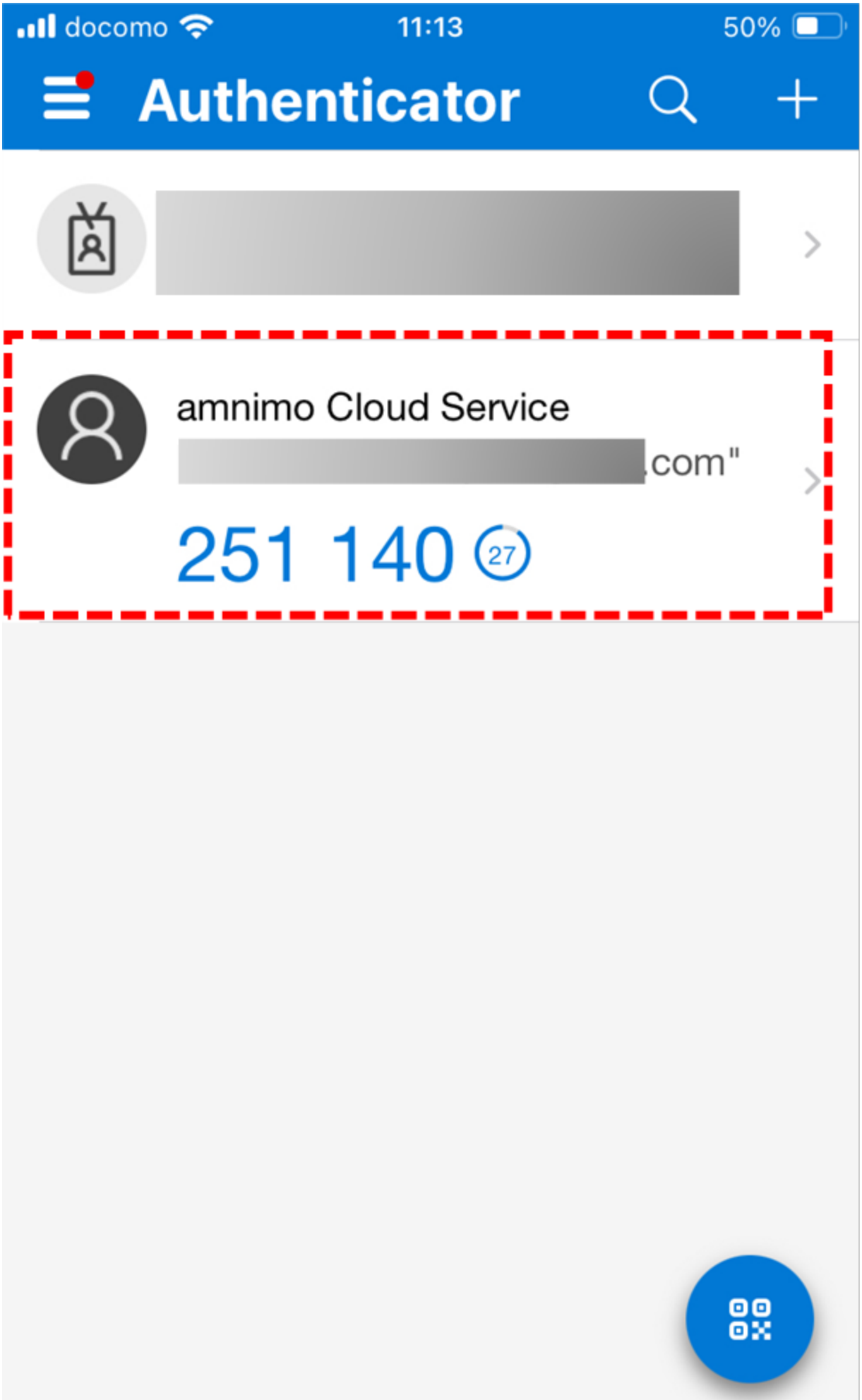


Enter the authentication code in half-width characters (①) and click [Confirm] (②) to complete sign-in.



Sign-in with Authentication App

On the sign-in screen, enter your e-mail address and password, then click "Sign In" to display the multifactor authentication dialog box.
Confirm the authentication code (6-digit number) displayed on the authentication application.


docomo
11:13
50%
Authenticator
amnimo Cloud Service
.com"
251 140
27

Enter the authentication code in half-width characters (①) and click [Confirm] (②) to complete sign-in.

