CaseWare

Two-Factor Authentication

FAQS

TWO-FACTOR AUTHENTICATION - FAQS

PURPOSE

This document is intended to aid in troubleshooting the most common issues users may experience when using or configuring two-factor authentication (2FA).

BEST PRACTICES

We recommend the following to ensure users with two-factor authentication can maintain access to Cloud:

- Ensure that your organization has **at least two** staff members with the Admin role before enabling two-factor authentication. Only staff members with the Admin role can disable two-factor authentication. Granting this role to two users ensures that at least one account will always be able to access Cloud. For instructions, see Assign security roles.

- Upon enabling 2FA, all users should generate backup codes. Backup codes enable users to log in if they cannot access their mobile phones, or if an administrator is unavailable to disable two-factor authentication for them. Backup codes are single-use, and must be generated while users have access to their account. For instructions, see Generate backup codes.

- **NOTE:** When users are entering their mobile number to enable 2FA, our SMS provider requires that phone numbers be in the international format of E.164, which includes the country code.

  In addition, note that if a user's mobile phone number has an area or mobile code that begins with a "0", the "0" must be omitted when they enter their mobile phone number to enable 2FA. If the "0" is not omitted, our SMS provider will be unable to send the 2FA verification code.

  For examples of correctly formatted phone numbers in the E.164 format, see the table below.

Mobile Number	Country Code	Country	E.164 Format
+4407111222333	44	GB	+447111222333

Administrators can help users who are experiencing trouble with their 2FA by referencing this help topic below: As an administrator, how can I help users who cannot receive their verification code and cannot log in?

FAQS

Q: Why haven't I received my verification code?

If you haven't received your verification code, check the following:

1. Ensure you have accurately entered your phone number with the correct area code.
2. Ensure the number you have entered is a **mobile** phone number. Our text message provider can only send messages to valid mobile phone numbers.
3. Ensure that the number you have entered is not a VOIP number. VOIP numbers may experience issues receiving verification codes. We recommend using your mobile phone when you configure 2FA.
4. Confirm whether your mobile network provider is experiencing issues. Ask a friend or co-worker to call or text you.

   If you cannot receive their call or text message, your provider may be experiencing issues.

   If you are able to receive other calls and texts, but cannot receive your verification code, your provider may be blocking our messages as spam. In order to fix this issue, you must set up your phone to accept all messages. You can work with your provider to find the appropriate settings. You can also perform an internet search for "<your provider> blocking sms" to determine what steps to take.

   Examples:
   - Sprint
   - TMobile

Q: Why does it take so long to receive my verification code?

Delivery delays can be caused by unreliable service. Mobile network providers may create a queue of text messages and delay delivery until service is reliable. This may cause a delay of several minutes to obtain a text message.

Note: Verification codes are valid for 3 minutes. If you do not receive a message within 3 minutes, you will have to repeat the login process. If you regularly experience delivery delays, we recommend you generate backup codes and keep them in a safe location. Backup codes are single-use codes that you can use to login when having issues with 2FA. For instructions, see Generate backup codes.

Q: How can I maintain access to my account if my mobile network provider is down?

When you are logged into CaseWare Cloud, generate a backup code. Backup codes enable you to log in if you cannot access your mobile phone, or if an administrator is unavailable to disable two-factor authentication for you. Backup codes are single-use, and must be generated while you have access to your account. For instructions, see Generate backup codes.

Q: As an administrator, how can I help users who cannot receive their verification code and cannot log in?

If users are experiencing issues receiving their verification code and have not generated or cannot access a backup code, administrators can temporarily or permanently disable 2FA for their account. For instructions, see Disable two-factor authentication for a specific user.

When the user logs in to their account, they can re-enable 2FA and enter a new phone number, if necessary. Users can update their mobile number by following the help section: Enable two-factor authentication for your own account.

They can also generate a backup code for their account. Backup codes enable users to log in if they cannot access their mobile phones, or if an administrator is unavailable to disable two-factor authentication for them. Backup codes are single-use, and must be generated while users have access to their account. For instructions, see Generate backup codes.

Q: As an administrator I am also experiencing issues with my 2FA and cannot login. How can I regain access to my account and help others within my firm who also have 2FA issues?

1. Do you have backup codes generated? If so, please use your backup codes to sign-in. If not, please proceed to the next step.
2. Are there any other administrators who can still login? If so, please have this user disable your 2FA. If not, please proceed onto the next step.
3. Contact your distributor’s customer support team and be prepared to provide the following information:

   a. Your firm's URL.
   b. The name and email of the administrator who requires site access.
   c. The administrator's mobile number and network provider
   d. Confirmation from the firm representative that the firm agrees to disable 2FA for the specified admin user.
4. See the below help topic on how to help others within your organization: As an administrator, how can I help users who cannot receive their verification code and cannot log in?

Q: I have deactivated and then reactivated a user with 2FA configured for their account. Why can this user log in without entering a 2FA verification code?

Users whose accounts are deactivated and reactivated are not required to enter a 2FA verification code under the following circumstances:

- The firm admin or user has configured 2FA for their account to require sign in with 2FA every 30 days. The user was deactivated and reactivated during the 30 day window and they will not be required to sign in with 2FA until 30 days after their last 2FA sign-in.
- The firm admin has disabled 2FA for the user's account. 2FA can be re-enabled from the user's account settings.

Q: Why are the same users consistently experiencing 2FA issues?

This may indicate that the user's mobile network is having issues. Ask the user to check if their mobile network provider is blocking incoming SMS verification codes. See step 4 in Why haven't I received my verification code?

If multiple users are affected, check if the affected users are all using the same mobile network provider.

Q: As an administrator, when I enable 2FA across my site for all Staff, and then disable it, why are my Staff still required to use 2FA to login?

If you enable then disable 2FA across your entire firm, existing user accounts will still be set to use 2FA. If users do not want to use 2FA for their account, they can manually disable it in their account settings. For instructions, see Disable two-factor authentication for a specific user.

Q: I configured 2FA to require sign-in every 30 days. Why am I being asked to sign in with 2FA within that time period?

We use cookies to store which device the user uses to login with 2FA. If you delete cookies or use a new device to log in, the 30 day counter is reset, and you are required to sign in with 2FA again.

Q: I have followed all troubleshooting steps but I'm still experiencing 2FA issues. What can I do?

If you are still experiencing issues, you can contact technical support. Be prepared to provide the following information:

1. How many users are affected? If multiple users are affected, are they using different mobile network providers?
2. Which country is the affected user located in?
3. Has the user experienced this issue multiple times?
4. Has the user changed their phone number recently?
5. Is the user receiving text messages and phone calls from friends or co-workers?
6. If the user requests multiple verification codes, does the user eventually receive at least one of the messages?
7. Has the user ever successfully received a verification code since enabling 2FA?
8. Has the user's 2FA configuration been permanently disabled by an admin?
9. What was the date and time when the errors occurred? Are text messages not delivered at specific times of day, such as high traffic times at the start of the work day?
10. Is 2FA setup for the entire firm?
11. What is the user's mobile number?
12. What is the user's mobile network provider?
13. What approximate time did the user notice that they were not receiving 2FA verification codes?