

Multi-Factor Authentication (MFA) Troubleshooting Guide

Zurich Access Portal

This guide is to help users resolve common issues when signing in with Multifactor Authentication (MFA) using **SMS, Email, Phone Call, Okta Verify, or Google Authenticator**.

1. Common Issues & Fixes

"I'm not receiving my MFA code"

- Check the internet or mobile signal.
- Ensure the device is not in Airplane Mode or Do Not Disturb.
- Confirm the registered phone number or email address is correct.
- Wait 30 seconds and select **'Resend code'**.

"My code isn't working"

- Codes expire quickly - request a new one.
- Ensure the most recent code is being entered.
- Avoid copying extra spaces when pasting.

"I changed my phone or number"

- Users can remove and re-install the authentication type in their security setting

"I'm locked out"

- After several failed attempts an account will be temporarily locked.
- Please try again after the indicated time has elapsed
- Contact Support if it remains locked (See How to contact Support in section 7)

2. SMS Authentication

"Not receiving SMS codes"

- Check mobile signal.
- Restart phone.
- Ensure the phone can receive SMS (some work phones block short codes like one time passcodes (OTP)).
- Remove SMS blockers or spam filters.
- If abroad, ensure roaming is enabled.

"My code has arrived late"

- Network congestion can delay SMS.
- Request a new code only after 30 seconds to avoid confusion.

3. Email Authentication

"I haven't received the email code"

- Check Spam, Junk, Clutter, or other folders.
- Ensure mailbox isn't full.
- Confirm the correct email account is being checked.
- Please add Zurich to your 'safe senders' list to help ensure MFA codes and account-related emails are delivered successfully. If you're not sure how to do this, please speak to your IT representative or support provider.

"My email Code isn't working"

- Codes can expire - request a new one.
- Make sure it's the latest email code that is being used.

4. Phone Call Authentication

"I've not received a call"

- Ensure the phone is not on **Do Not Disturb**, **Airplane Mode** or **Silence Unknown Callers**.
- Check mobile signal.
- Confirm the number is correct.
- If using a work phone, ensure automated calls are not blocked.

"The call drops immediately before I can get the code"

- Restart the phone.
- Disable call blocking apps.
- Try switching to Wi-Fi calling if mobile signal is weak.

5. Okta Verify

"My push notification hasn't arrived"

- Ensure the phone has internet access (Wi-Fi or mobile data).
- Check that notifications for **Okta Verify** are enabled:
 - iPhone: Settings → Notifications → Okta Verify → Allow
 - Android: Settings → Apps → Okta Verify → Notifications
- Ensure the app is running in the background.
- Disable battery-saving modes that restrict background activity.

"The app shows 'Device not registered' "

- This usually happens after:
 - A phone reset
 - A new phone
 - Reinstalling the app
- Re-enrol Okta Verify

"The QR code won't scan"

- Clean the camera lens.
- Increase screen brightness on the computer.
- Ensure the QR code is not partially cut off.

6. Google Authenticator

'Code not accepted'

- Time-based codes require the phone's clock to be accurate.
- Enable Automatic Date & Time on the phone.
- Ensure it's the correct account if there are multiple entries.

Lost or changed phone

- Google Authenticator codes cannot be transferred automatically unless the built-in transfer tool is used.
- Contact Support to reset MFA.

App not generating codes

- Restart the phone.
- Ensure the app is updated.
- Ensure there is internet signal
- Check that the time sync is correct.

7. How to contact ZAP Support

When contacting support users will need to provide the following information:

- Full name
 - Username or email
 - Which MFA method is being used
 - What error message came up
 - Whether the phone, number, or email has been changed recently
-
- Email **ZAPSupport@uk.zurich.com**
 - Call **0800 141 2002 (option 4)**

8. Best Practices for Smooth MFA Use

- Phones should be kept charged and accessible.
- Ensure contact details in the portal are always up to date.
- Enable backup MFA methods (e.g. Email + Google Authenticator).
- Avoid deleting Okta Verify or Google Authenticator unless instructed.