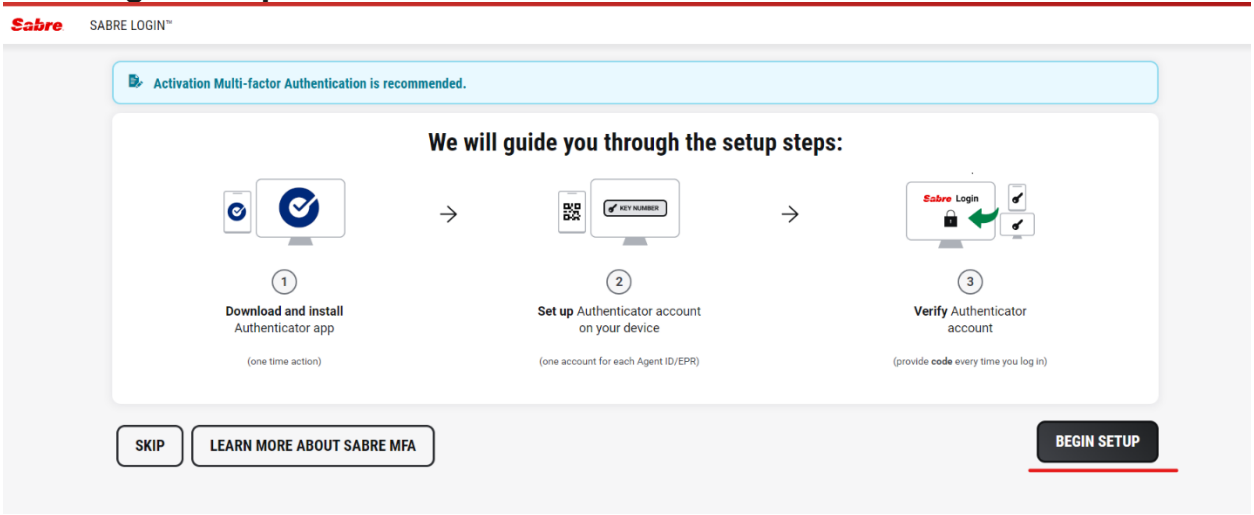
# Google Authenticator (MFA)

Google Authenticator is an app that provides a Time-based One-time Password (TOTP) as a second factor of authentication to users who sign in to environments where multifactor authentication (MFA) is required.

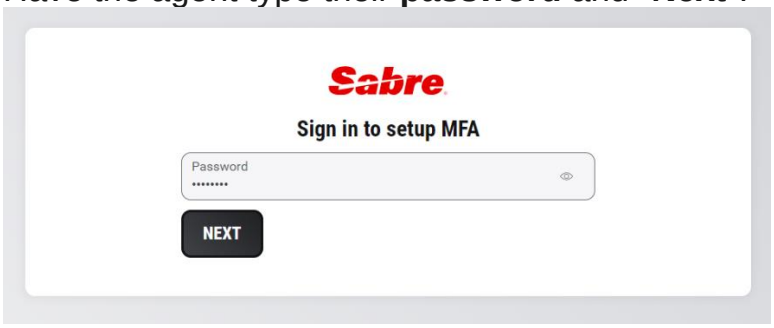
Admins add Google Authenticator to the list of accepted factors in Okta. Then, users who select it to authenticate are prompted to enter the time-based, six-digit code they see in the Google Authenticator app in Okta.

## End-user experience

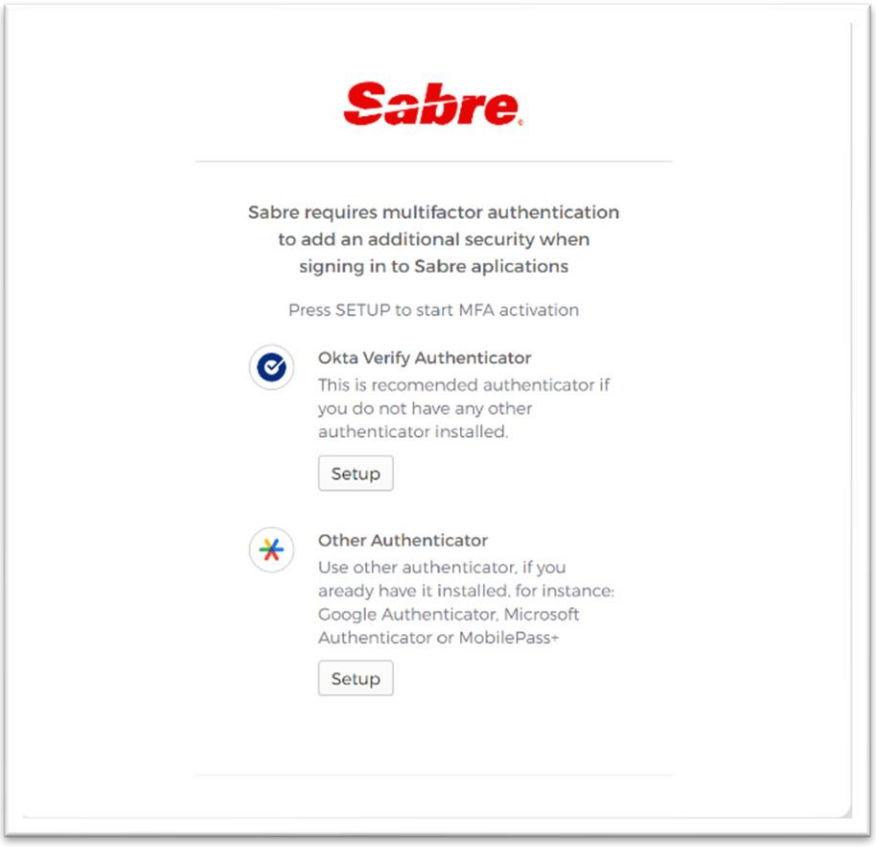
1. Go to the Apple App Store or the Google Play Store and install Google Authenticator on your device.
2. In the web browser on your computer: When signing in to Okta or accessing an Okta-protected resource, enter your credentials and then click **Begin Setup**



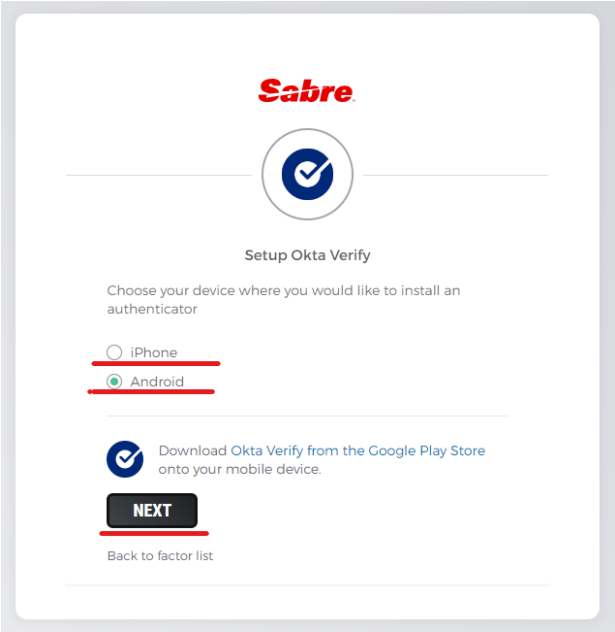

3. Have the agent type their **password** and "**Next**".



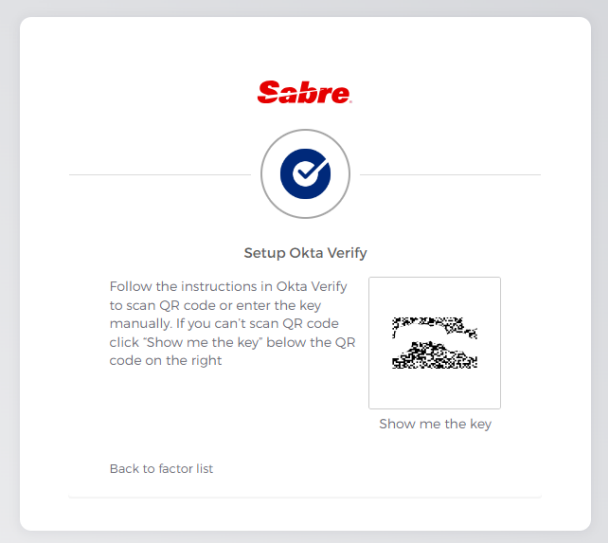
4. On the **Setup security authenticators** page, select **Other Authenticators** and click **Set up**.




5. Select your device type, and then click **Next**.



5. Perform the QR code scanning steps that apply to you:




## If your device can scan QR codes:

a. Don't click **Next** in the browser yet; instead, on your mobile device, launch Google Authenticator.
b. In Google Authenticator, tap the + sign.
c. Tap **Scan a QR code** and then point your camera at the QR code displayed in the browser on your computer. Your device camera scans the QR code automatically.
d. In the web browser on your computer, click **Next**.
e. In the **Enter Code** field, enter the setup key shown in Google Authenticator on your mobile device.
f. Click **Verify**.

## If your device can't scan QR codes:

a. Don't click **Next** in the browser yet.
b. In the web browser on your computer, click **Show me the key**.
c. In the field above the **Next** button, make a note of the string of numbers and letters.
d. On your mobile device, launch Google Authenticator.
e. Tap the **+** sign.
f. Tap **Enter a setup key manually**.

g. In the **Account** field, enter your Sabre EPR.
h. In the **Key** field, enter the string of numbers and letters that you made a note of earlier – ***Show me the key***.
i. Tap **Add**. The message **Secret saved** appears.
j. In the web browser on your computer, click **Next**.
k. In the **Enter Code** field, enter the setup key shown in Google Authenticator on your mobile device.
l. Click **Verify**.

# Important considerations

- The time on the end user's device might not be the same as the time on the clock in the Google Authenticator app. The Google Authenticator app allows a time difference on the end-user device of up to two minutes earlier or later than the time in the Google Authenticator app.
- After five unsuccessful authentication attempts, regardless of the time between the attempts, the user account is locked and the admin must reset it.