User Registration Multi-factor Authentication | Set up Instructions.

Last Updated: April 2024
Applicable Markets: **Global, including partners.**

Product Overview

What is Multi-Factor Authentication (MFA)?

Multi Factor Authentication, or MFA, is a security measure that requires users to provide two or more types of authentication factors to verify their identity. These factors can include something the user knows (like a password or PIN), something the user has (like a mobile device or smart card), and/or something the user is (like a fingerprint or facial recognition).

Why is activation necessary?

MFA is important because it adds an extra layer of security to the authentication process, making it more difficult for unauthorized individuals to access sensitive information or conduct fraudulent transactions. In other words, MFA helps to protect your Sabre credentials from cyber criminals.

There are two main App options presented:

- Okta Verify
- Other Authenticator ie. (Google Authenticator, Microsoft Authenticator, MobilePass+)

This document takes you through the activation process using the Okta Verify Authentication App. If you are using an alternative, the ‘in app’ process may look slightly different.

Step 1—Access the MFA Setup Page

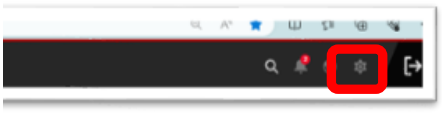
1

For newly registered EPRs or user's whose MFA has been reset by the Sabre helpdesk.

Upon annual password reset process the user will be prompted to configure their MFA settings.

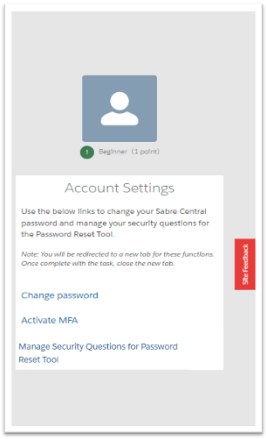
2

Existing EPRs can navigate to Sabre Central to configure their MFA settings.



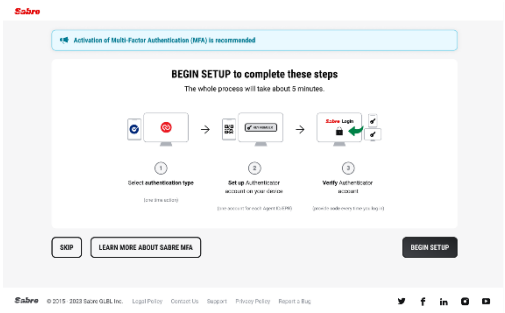
3

From the top-right corner, click **My Profile**.



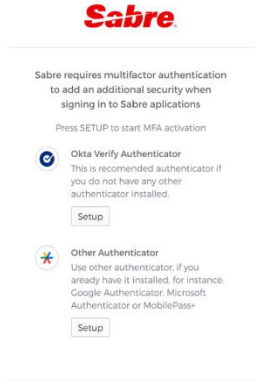
4

Select and click the **Activate MFA** link



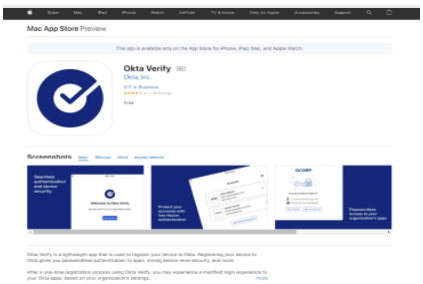
5

Select and click **Begin Setup**



6

Pick a Multi- Factor authentication option and click **Setup** below it.



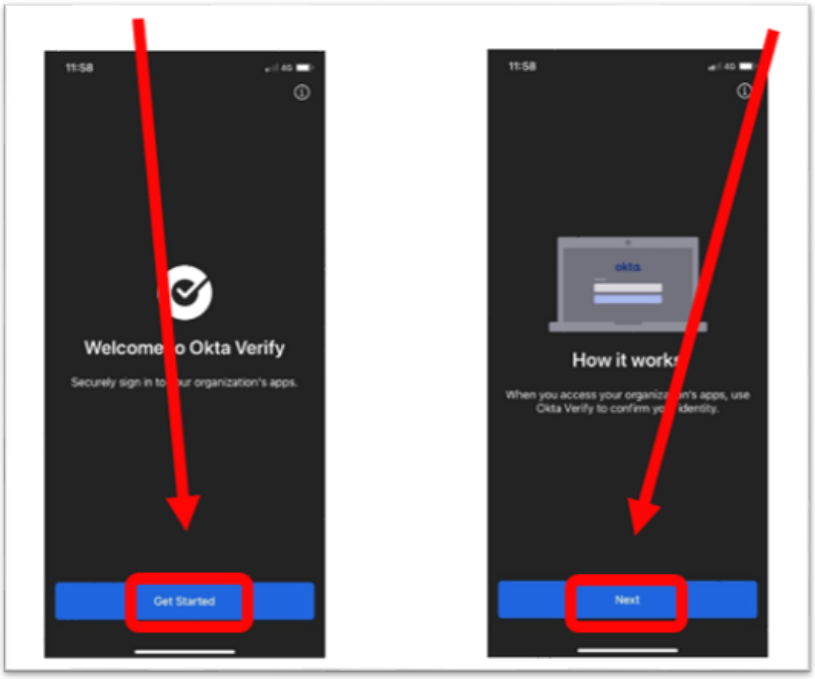
Select your device type (**iPhone** or **Android**) and then click **Next** to continue with device enrollment.

Before proceeding further, ensure Okta Verify is installed on your mobile which can be downloaded from the Apple App Store or Google Play Store

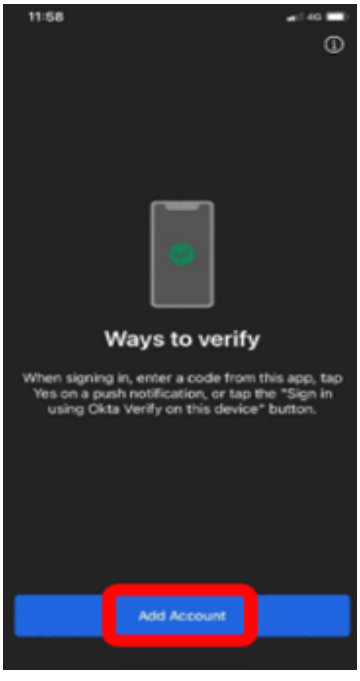
Step 2 —Enroll your device with Okta Verify

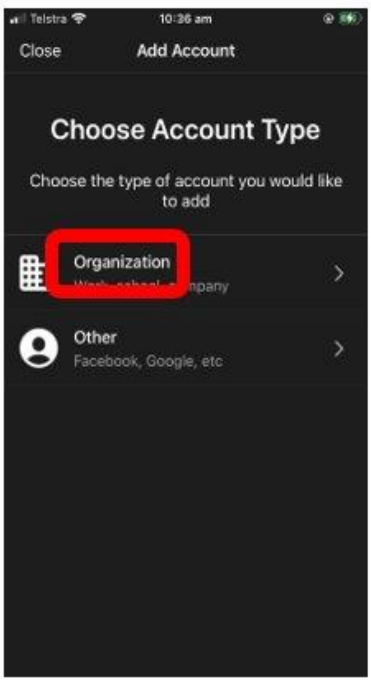
IMPORTANT: The below instructions are illustrated using an iPhone running iOS. The instructions may vary for an Android device.

1. On your mobile device, launch the **Okta Verify** app.
2. If you are setting up the Okta Verify app for the first time on your mobile device, you will receive a Welcome to Okta Verify screen.
3. Tap **Get Started** and **Next**.

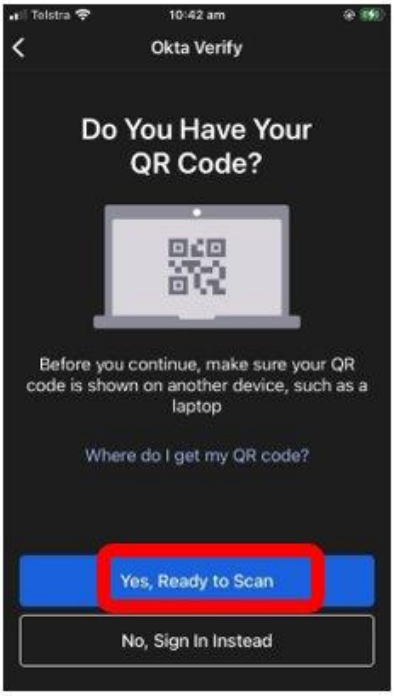


4. Tap **Add Account**.
5. On the **Choose Account Type** screen, **tap Organization**.

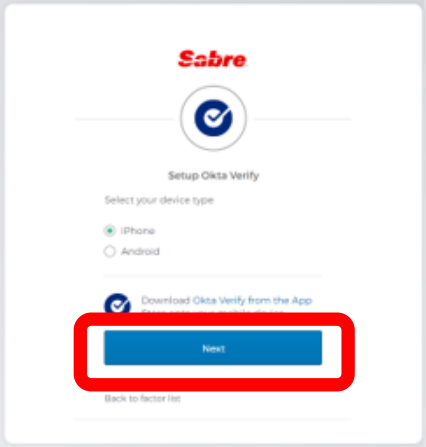




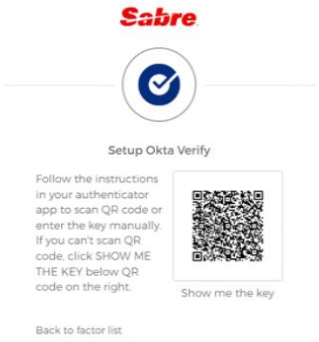
6. Tap Scan a **QR Code**. Note: You may be prompted to allow Camera access to the app. **Tap OK**.



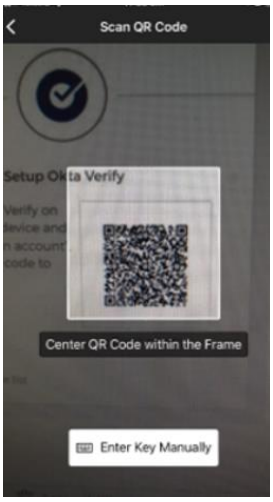
Step 3 —Activate your MFA



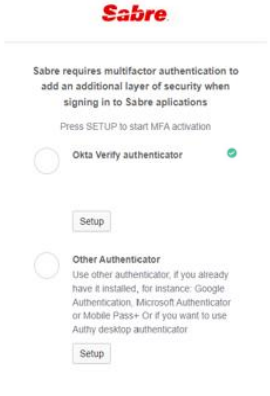
1 After OKTA Verify installation on your mobile click **Next** to continue with device enrollment



2 The **Scan barcode** screen appears.



3 Point the camera to the barcode on your computer screen. The camera detects and reads the barcode automatically and your device is enrolled.



4 Upon successful enrollment, **Setup Okta Verify** page will show a green check.

Frequently Asked Questions (FAQs)

Q: What is Multi-Factor Authentication (MFA)?
A: Multi-Factor Authentication is a security practice that requires more than one method of authentication, using independent categories of credentials to verify a user's identity. For example, you may log in to a system using your password ("what you know") and then verifying a separate six-digit number that is sent to your phone ("what you have"). By combining "what you know" and "what you have" verification, the hackers will have a harder time breaking into systems as they may not have both your password and your phone.

When you log in to an account or application, you're asked for a password so you can prove you are who you say you are. You may then be asked for a second factor.

Q: What is the benefit of using MFA?
A: MFA is an effective way to provide enhanced security. Traditional usernames and passwords can be stolen, and they've become increasingly more vulnerable to malicious activity, and cyber-attacks like phishing or brute force attacks. MFA creates multiple layers of security to help increase the confidence that the user requesting access is who they claim to be.

Q: How can I start using Multi-Factor Authentication (MFA) for my employees?
A: Employees will need to individually turn on MFA through their User Profile at Sabre Central. Use the steps described in this document to enable authentication through Okta Verify or another Authenticator.

Q: What if I am having issues downloading the Okta Verify app?
A: The Okta Verify app is available from the Google Play or App Store in all countries free of charge. You may, however, need a registered email address and password for the respective app store of your choice. If you are unsure of your Apple ID or password (for the App Store), please refer to support.apple.com and follow Apple's instructions. If you are unsure of your Google account password (for the Google Play store), this should be the same as you use to log in to other Google services. If you are unsure, please refer to accounts.google.com and follow Google's instructions.

Q: Is there a way to opt-out of Multifactor Authentication since I do not always have my phone handy?
A: Multi Factor Authentication is mandatory to help protect your account. If you have not set up Multi-factor Authentication, you will not able to access Sabre applications.

Q: Do I have to pay to download/use Okta Verify or another authenticator?
A: Okta Verify and Google Authenticator, Microsoft Authenticator are free to download from the Apple and Google play stores. All apps are free to use and do not have in-app purchases. Please ensure you read the application you are downloading carefully to ensure you are downloading the correct app.
Apple IOS users

You may be prompted to add a payment method to the Apple App store so that you can make purchases in the future and use subscriptions like iCloud+ Apple Music etc. Please refer to https://support.apple.com for further information.

Android users

You may be prompted to add a payment method to the Google Play store to assist with app purchases. You can simply elect to set this up later to proceed to download okta verify or google authenticator. Please refer to https://support.google.com/ for further information.

Q: What does it mean if my account is locked?
A: If we see suspicious activity on your account, like repeated failed attempts to sign-in, then we will lock your account. Reach out to our support team to help unlock your account.