

Virtual Token & Authenticator App FAQ's

What is a Virtual Token App?

A virtual token app provides secure multi-factor authentication (MFA) for accessing business banking and other sensitive systems. Common solutions include Duo Mobile, Authy, and Symantec VIP.

Why do I need a Virtual Token or Authenticator App?

Many financial institutions and online platforms require an extra layer of security to protect sensitive information. These apps add a second factor beyond your password, reducing the risk of unauthorized access. They generate time-sensitive codes that verify your identity during login.

Which apps are supported?

- Duo Mobile: Enterprise-grade security with push notifications and TOTP codes.
- Authy: User-friendly with multi-device sync and encrypted backups.
- Symantec VIP: Strong compliance features and risk-based authentication for large organizations.

How do I install and register?

1. Download the app from your device's app store.
2. Follow your organization's enrollment instructions.
3. Scan the provided QR code or use the activation link.

Can I use my personal mobile device?

- Yes. If a business mobile device isn't available, it's perfectly fine to use your personal device. This is standard practice in business banking and widely adopted across the industry.
- Your device will only store authentication tokens, not sensitive banking data.
- The app uses very little space and does not store login credentials.

Is this method secure?

Yes. Authenticator apps are considered more secure than SMS or email verification because codes are generated locally on your device and are harder to intercept.

Best Practices

- Enable biometric authentication for added security.
- Keep your app updated.
- Do not share your device or authentication codes.

Troubleshooting

- Lost device? Contact your administrator immediately.
- App errors? Reinstall the app or check your internet connection.

Security Reminder

Virtual token apps are critical for safeguarding your business accounts. Using personal devices is secure when combined with strong passwords and MFA.