BIO-key PORTALGUARD A BIO-key Solution

PortalGuard Authentication Methods

Contents

Disclaimer

This list is meant to provide a brief overview of the available Authentication Methods for Self-Service and MFA throughout PortalGuard. This list is not a technical document and serves only as an introduction. For detailed technical questions or usage details regarding any feature, please contact PortalGuard technical support directly:

Email: techsupport@portalguard.com

Phone: +1 (603) 547-1200

BIO-key MobileAuth

BIO-key MobileAuth is an easy-to-use mobile app with no new hardware required and a fast QR code registration and enrollment process that can be completed in seconds. MobileAuth offers PalmPositive as an authentication method and form of Identity-Bound Biometrics which uses a simple palm scan to authenticate the individual.

As part of BIO-key's PortalGuard IDaaS platform, BIO-key MobileAuth supports its MFA and SingleSign-On (SSO) solutions to streamline logins while making them more secure.

BIO-key MobileAuth with PalmPositive is available for both iOS and Android and requires an active BIO-key PortalGuard IDaaS account.

WEB-key™

WEB-key is an enterprise-grade Identity-Bound Biometric platform from BIO-key. For fingerprint biometric authentication it has the highest independently tested and verified NIST benchmarks for fingerprint identification, speed and accuracy.

WEB-key authentication is integrated with PortalGuard for Self-Service Password Reset and Multi-Factor Authentication actions. This integration requires manual user enrollment, as well as the setup anduse of a separate WEB-key server for secure validation of the biometric data.

For capturing fingerprint scans, BIO-key offers a variety of Microsoft-qualified Windows Hello USB scanners that can be used out of the box with Windows Hello and Windows Hello for Business, or for use with BIO-key Identity and Access Management (IAM) solutions like PortalGuard, as one of many supported brands of scanners. Available fingerprint scanner models include:

- SidePass
- PIV-Pro
- EcoID II
- SideSwipe
- SideTouch
- Pocket10

FIDO2/WebAuthn Tokens

FIDO2 (AKA WebAuthn) differs from FIDO U2F in that it is designed for a ‘password-less’ approach to secure authentication. Functionally, FIDO2 tokens support the same usage as FIDO U2F, though utilizing a different industry standard and browser-based API. FIDO2 Tokens support one of two usage types: Click to Authenticate or On-Device Authentication.

Click to Authenticate requires a tap/click of the token while On-Device Authentication detects the FIDO2 request and automatically responds, allowing the authentication action to proceed.

FIDO U2F Security Key

FIDO U2F is a standard protocol jointly developed by Yubico and Google as an alternative form of 'token'-based Two-Factor Authentication. The use of FIDO U2F requires a supported Security Key as well as a supported browser.

FIDO U2F Security Keys do not require any additional software, drivers, or client-side installation for use, and act as a strong and secure second factor for authentication. Adoption and usage are straight forward: simply plug in the key to a USB port and tap the button to use.

Supported FIDO Security Keys

As mentioned above, FIDO Security Keys are hardware devices which support the FIDO2 and FIDO U2F standards. PortalGuard supports multiple brands including:

- **BIO-key FIDO-keys:** BIO-key's FIDO-key security keys are compatible with the FIDO U2F, FIDO2, and WebAuthN standards for easy and secure online authentication. These keys boast plug-and-play technology and are compatible with major platforms including Microsoft Windows, macOS, and Linux. All tokens store an infinite number of cryptographic keys and are high-quality, durable, and even waterproof. With FIDO-key, customers and organizations have a selection of cost-effective options for online authentication.

- YubikeyTM: YubiKey tokens are unique hardware devices that generate a One-Time Passcode – usually at the tap of a button. These devices emulate a keyboard and offer a simple, secure method for providing a second factor during authentication. Yubikey tokens do not have a power source, display, or moving parts. These tokens are extremely resistant to damage and have a long lifetime.

- RSA SecurIDTM: RSA SecurID Tokens come in many shapes and forms. Most display a one-time passcode directly on the device, which the user then enters when requested through a supported application. Support for RSA SecurID tokens is dependent upon the PortalGuard server being able to communicate directly with the RSA Authentication Manager Server(s). You must also be an active RSA Customer.

HMAC-Based OTP Token

HMAC-Based OTP Tokens (HOTP) utilize a static shared key and a counter to generate a valid One Time Passcode. This type of OTP Token requires a synchronization between the device and the PortalGuard server to ensure bidirectional validation.

Administrators have full access to enroll or re-synchronize these tokens via the PortalGuard Help Desk Console.

Push

Push is an 'out-of-band' second factor tied to a mobile device. This second factor allows end-users to confirm or deny an authentication request by interacting with their mobile device in real-time. No codes need to be remembered – just tap yes or no on the screen.

Mobile Authenticator

PortalGuard supports the use of multiple Mobile Authenticator Applications. These applications generate a Time-Based One-Time Passcode (TOTP), which can subsequently be utilized during various Self-Service Password Reset and Multi-Factor Authentication (MFA) Actions throughout PortalGuard.

The Mobile Authenticator Application requires a one-time enrollment to synchronize the authenticator application and the PortalGuard website. From there, the device can generate a valid TOTP even if it is not connected to the network.

Supported Mobile Authenticator Apps include but are not limited to:

- Google Authenticator
- Microsoft Authenticator
- Authy
- Duo

SMS

The SMS delivery method (often referred to simply as 'phone') involves sending an SMS text message to an enrolled mobile phone number. This SMS text message contains a One-Time Passcode (OTP) to validate the user to the PortalGuard System for a specific action. Administrators have full control over the length, character set, and validity of OTPs utilized by this option. These settings are shared by the 'Email' OTP type as well.

SMS functionality requires integration with a third party SMS provider system.

The following providers are supported in PortalGuard to send SMS messages for MFA:

- Clickatell
- Esendex
- MessageMedia
- Regroup
- SMSMatrix
- Twilio
- Plivo

Email

The Email Delivery method involves sending an email to an enrolled email address. This email contains an OTP to validate the user to the PortalGuard system for a specific action. Administrators have full control over the length, character set, and validity of OTPs utilized by this option. These settings are shared by the 'SMS' OTP type as well

Help Desk

This option allows end-users to receive an OTP generated by the PortalGuard Help Desk Console. End-users must be instructed (via end-user training and/or the PortalGuard User Interface) on how to contact the Help Desk team. Once contacted, the Help Desk team can utilize the PortalGuard Help Desk console to generate a code to provide the user.

Help Desk OTPs always utilize numeric characters, but the length is configurable on the administrative side.

Grid Authentication

Grid Authentication utilizes a third-party JavaScript implementation to allow for the tracing of a pattern as a second factor. This pattern is traced on a dotted grid and can be either visible or hidden as defined by the user.

This second factor will be familiar to any user who has utilized a pattern to unlock their mobile device, as it looks and feels the same. This type is especially handy for mobile-heavy environments, though it can be utilized in a full desktop environment as well.

Voice Biometrics

Voice Biometrics supports the delivery of a One-Time Passcode (OTP). A traditional call is made to the user's enrolled phone number via a third party messaging provider. The third party messaging provider takes the full text of the message set by the PortalGuard admin and converts it to a Text-to-Speech audio format, which is then read back to the end-user when they answer the call for verification.

This functionality is very helpful as it supports both landline phones as well as cell phones.

The following providers are supported in PortalGuard to send Voice Biometric messages for MFA:

- Esendex
- MessageMedia
- Regroup
- SMSMatrix
- Twilio

Printed

Printed OTPs are randomly generated on demand by the user through the Account Management page. These codes can be used any time the user fails to receive a real-time OTP (e.g. via SMS, Email, or through a Mobile Authenticator) or is otherwise unable authenticate for a specific Self-Service or MFA action.

Each of these Printed OTPs is usable only once and is specifically tied to the user account used to generate the batch.

The length and number of Printed OTPs is configurable on the administrative side, but only numeric characters are used for this OTP option.

Challenge Answers

Challenge Answers are the standard, go-to approach to user verification. Users provide answers to previously enrolled questions. This enrollment is completed by either an admin or the user during the first-time logging into the system.

Challenge Answers take two forms:

Mandatory

Mandatory challenge answers are stricter. The admin determines how many mandatory questions are required and the user must answer all questions.

During a Self-Service Password Reset or Knowledge Based Authentication (KBA) action, the user is required to answer a[redacted]mandatory challenge questions to complete the action.

Optional

Optional challenge answers allow the user to choose from a series of questions and only provide answers to a sub-set.

For example, when a user enrolls optional challenge answers, the user is required to set up five answers to questions chosen by said user. During a Self-Service Password Reset or KBA action, the user is required to choose any three of thosefive enrolled questions and provide valid answers.

This option provides flexibility if certain answers change or are simplyforgotten.