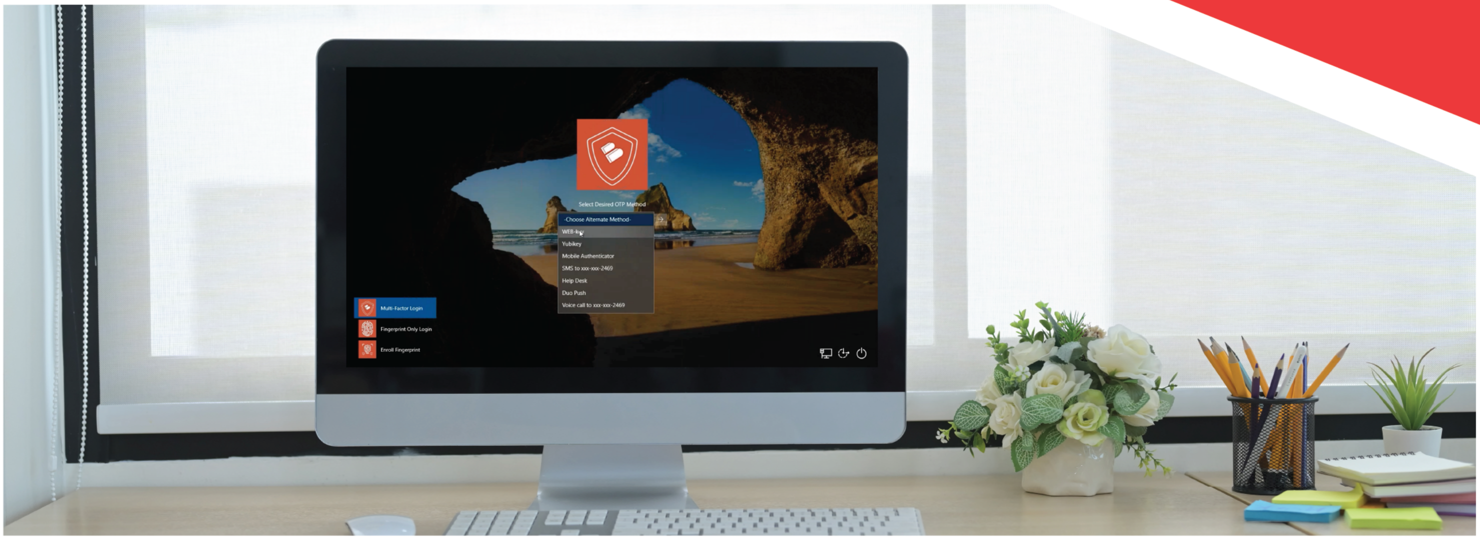
BIO-key®



Data Sheet

PortalGuard Desktop

PortalGuard is built with flexibility and user experience as a top priority – so you can configure it to meet your specific security requirements. As an optional client-side component, you can install the PortalGuard Desktop on your workstations or Windows-based servers.

PortalGuard Desktop can be used to secure logins from both the desktop and servers with flexible options for Multi-factor Authentication, Identity-Bound Biometrics, and Self-service Password Reset.

The latest update now allows organizations' Mac users to take full advantage of PortalGuard Desktop capabilities.

Features & Capabilities

Desktop Self-Service & Enrollment

PortalGuard Desktop integrates with Windows and MacOS to communicate with the PortalGuard server when it is available on the network.

- Allows Self-service Password Reset with multiple MFA options, including Identity-Bound Biometrics, hardware tokens, OTPs and more.
- Ease of use for employees to reset passwords directly from login screen.
- Reduces downtime for IT team by empowering the user with the tools to complete password recovery quickly and securely on their own.

Desktop Multi-factor Authentication

- MFA driven from central security policy.
- Flexibility for administrators to select and require specific security policies.
- Ability to enforce MFA for users and admins with access to remote desktops.
- Supports secure authentication for remote admins, local admins and remote users.

Support, Flexibility, and Security for All Users

Organizations of all sizes have segments of their user population on both Windows and Mac operating systems. PortalGuard Desktop provides true MFA capabilities for all logins across all workstations.

– 10+ options for MFA type provides unrivaled flexibility when implementing MFA in an enterprise.

– Works with both on-premises and cloud/IDaaS deployments of PortalGuard, while many alternatives are cloud-only Identity Providers.

– Offers unmatched security by enforcing MFA when unlocking the workstation, which also helps maintain productivity.

  - If a company requires users to fully log out of their desktop or workstation whenever they leave, this becomes a major issue for both security and productivity.

Technical Specifications

– Mac Support
  - MacOS versions 12.6 or later
  - Intel or M1/M2 chipsets

– Windows Support
  - Windows Server 2016 or later
  - Windows 10 or later (desktops and workstations)

– MFA types supported in this release:
  - MobileAuth v1 (Palm) and MobileAuth v2 (Face, Device Bio, Push Token)
  - Mobile App TOTP (e.g. Google Authenticator, Authy)
  - OTPs (Email, SMS, YubiKey)
  - Printed / Backup codes
  - Help Desk generated
  - HOTP tokens
  - Duo Push
  - FIDO2 tokens (Windows only / Mac in Q4 2023)
  - WEB-key / Fingerprint Biometrics

– The user must have previously enrolled the MFA options prior to logging into the device or workstation

Key Benefits

- Reduces helpdesk calls through self-service password reset capabilities
- Reduces user training through end-user familiarity, as PortalGuard Desktop has the same interface as with the browser.
- Supports offline use while still being able to take advantage of fingerprint authentication (on Windows) and Time-based OTP (TOTP) authenticator apps (Windows and MacOS).
- Multiple MFA options provide flexible, secure self-service password reset
- Supports all user populations with the capability to implement for both Mac and Windows users.