You Asked, We Listened:

Latest Updates to the PortalGuard Platform

June 2022 Masterclass

BIO-key®

Authentication Enhancements

BIO-key®

Proximity cards for easy login

More choices and flexibility to give your users without sacrificing security.

- Support for passwordless, single-factor, and multi-factor authentication

- Used for browser & desktop logins and self-service password reset

- Requires BIO-key WEB-key

BIO-key®

Geolocation improvement for contextual authentication

Using context to apply the appropriate authentication.

- Uses combination of network, IP address/network, date/time, and geolocation

- IPv6-based geolocation now supported

Additional authentication enhancements

Enhanced security for Linux/Unix

- New Pluggable Authentication Module (PAM) for enforcing MFA

- Utilizes the back end PortalGuard 2FA API

- Supports most authentication methods

Improved password management

- Password expiration time is more granular

- Desktop login via RDP does not require re-entering the password a second time

- Reports related to password reset have been improved.

BIO-key®

Improving endpoint security

PortalGuard Desktop secures endpoints with strong MFA.

- New mode to allow MFA from UAC authentication prompt

- Remote desktop credential passthrough supported for locked workstations

- Auto-fill last logged-in username on Windows login page

- Fixes, improvements, and cosmetic updates to enhance user experience

- Offline mode configured to improve security when workstations are not connected to corporate network for extended periods
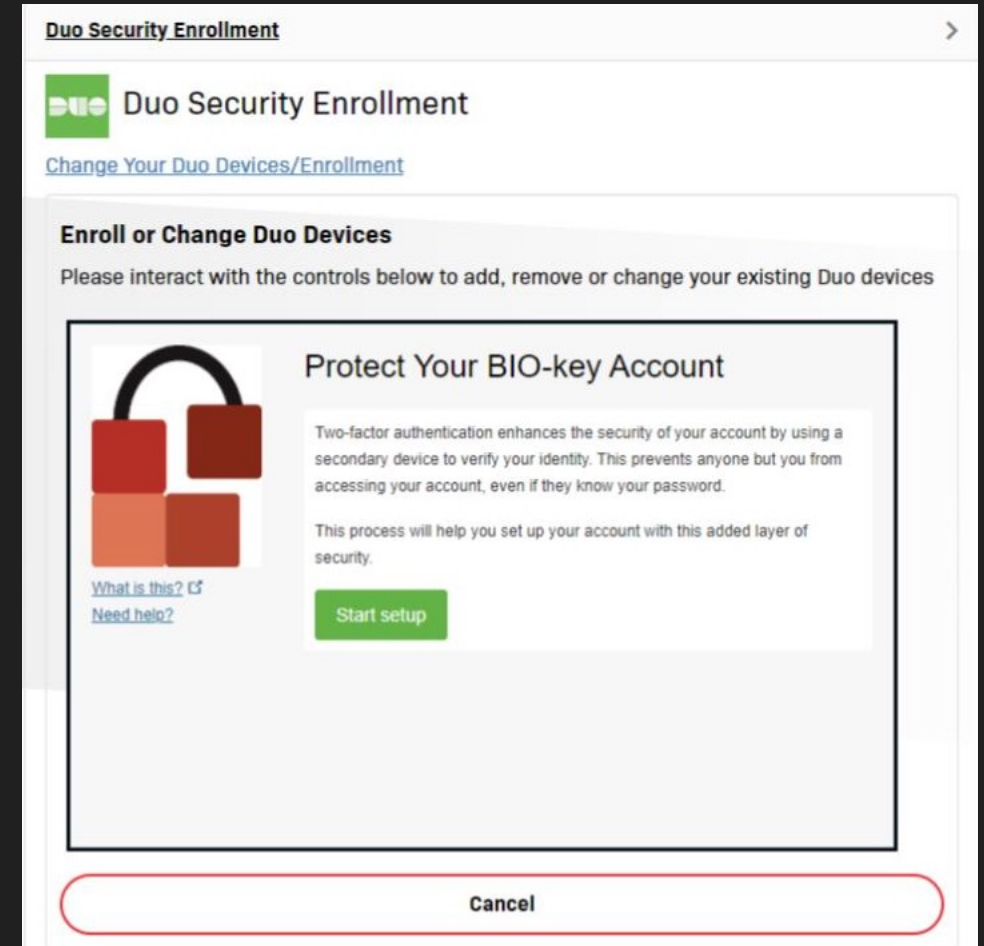
BIO-key®

Stronger Integration

Tailored authentication to improve DUO experience

- Improves DUO usability

- Can "force" specific actions:

    - DUO enrollment during PortalGuard login process

    - Create DUO bypass codes (printed)

- Use PortalGuard Account Management page to complete DUO enrollment

- DUO prompts for MFA

- PortalGuard provides wider range of SSO

BIO-key®

IDaaS Exclusive Improvements

IDaaS remote access enhancement

- RADIUS authentication support for PortalGuard IDaaS

- Enhances VDI support (specific environments)

- Supports PAP, CHAP and MSCHAPv2 RADIUS protocols

Supported Multi-factor Authentication Methods

- BIO-key MobileAuth
- SMS
- Duo Push
- TOTP
- HOTP
- Printed
- Email
- Help Desk OTPs
- RSA SecurID

AttributeSync for IDaaS

Automatic syncing of user attributes between IDaaS cloud directory and on-premises LDAP/Active Directory

- Includes standard & custom fields

- One-way sync from on-premises to IDaaS Cloud Directory

- Occurs on a scheduled basis (e.g., every 15 minutes)

- Important for identity claims for SSO and group membership

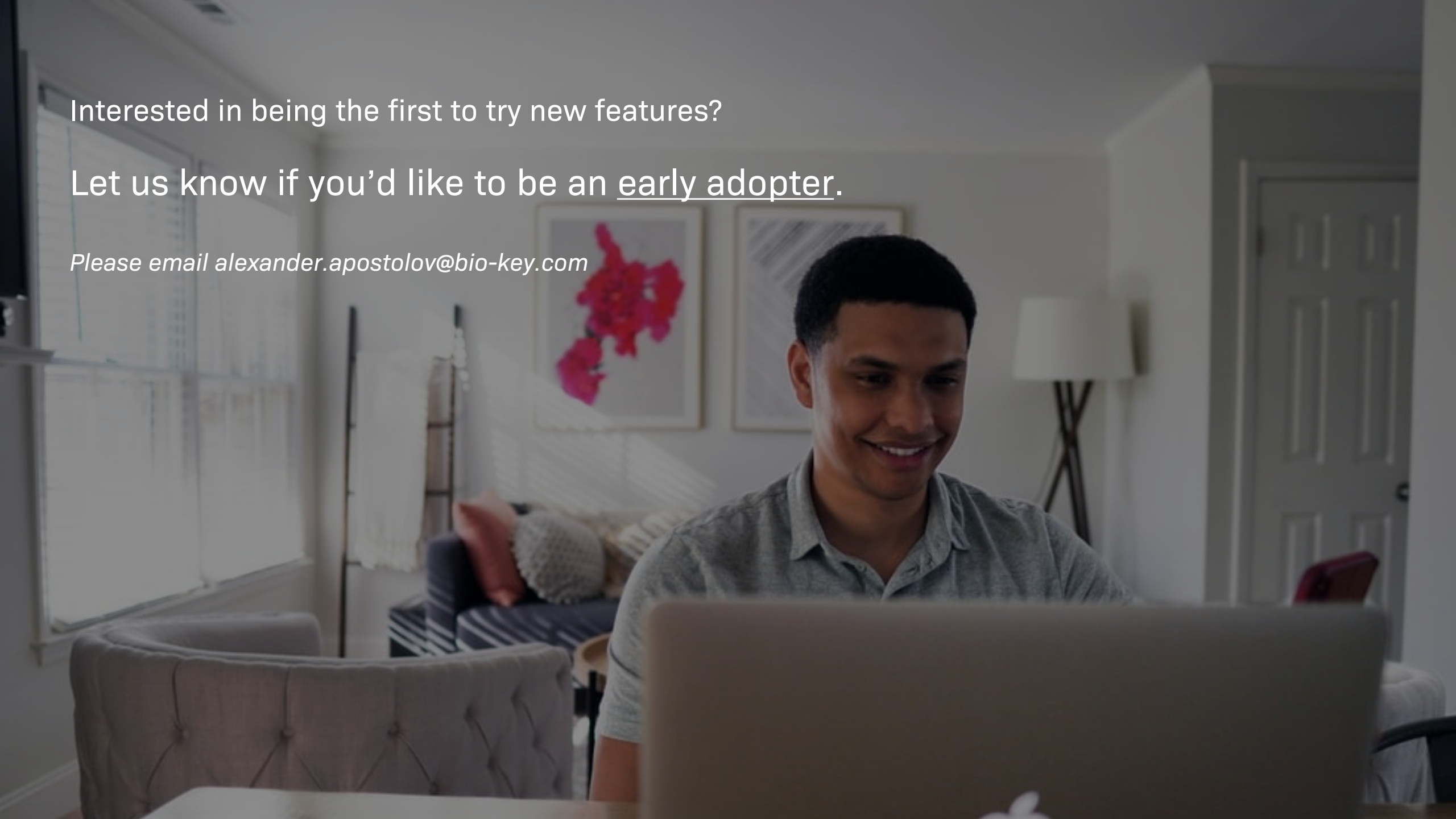BIO-key®

Let your brand shine with a vanity URL

IDaaS instances will use your own DNS domain
(e.g., *login.**acme.com***) instead of the default DNS
domain of ***onbio-key.com***.

Interested in being the first to try new features?

Let us know if you'd like to be an <u>early adopter</u>.

Please email alexander.apostolov@bio-key.com

Next steps

Subscribe to the Customer Blog:

https://customer.bio-key.com/blog

Book an Executive Business Review call to assess your own use of BIO-key.

Alexander.apostolov@BIO-key.com

Questions?

Please use the Questions panel to ask your questions now.

BIO-key®

Thank You

www.BIO-key.com