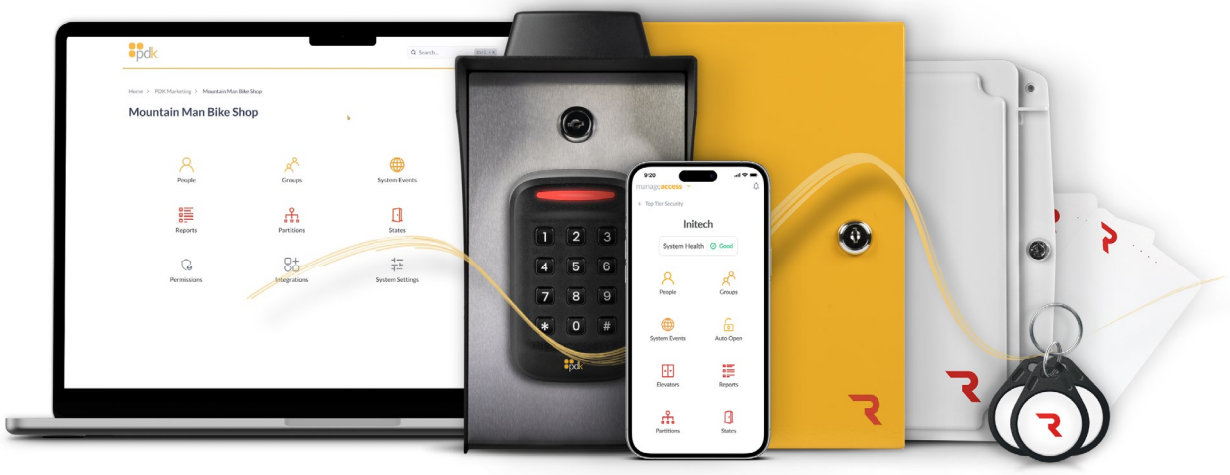
ProdataKey System Architecture



2026 Technical White Paper

Modern cloud-based access control platforms like PDK.io offer a robust foundation for secure physical access control infrastructure across enterprise, commercial, government, and residential markets.

This document was created for the thousands of security dealers across the world using PDK.io whom we are proud to have as partners. It is intended to communicate PDK.io system architecture from a security perspective and inform our customers how to best utilize features and protections PDK has provided to install secure and robust physical access control systems for their clients.

Shared Responsibility

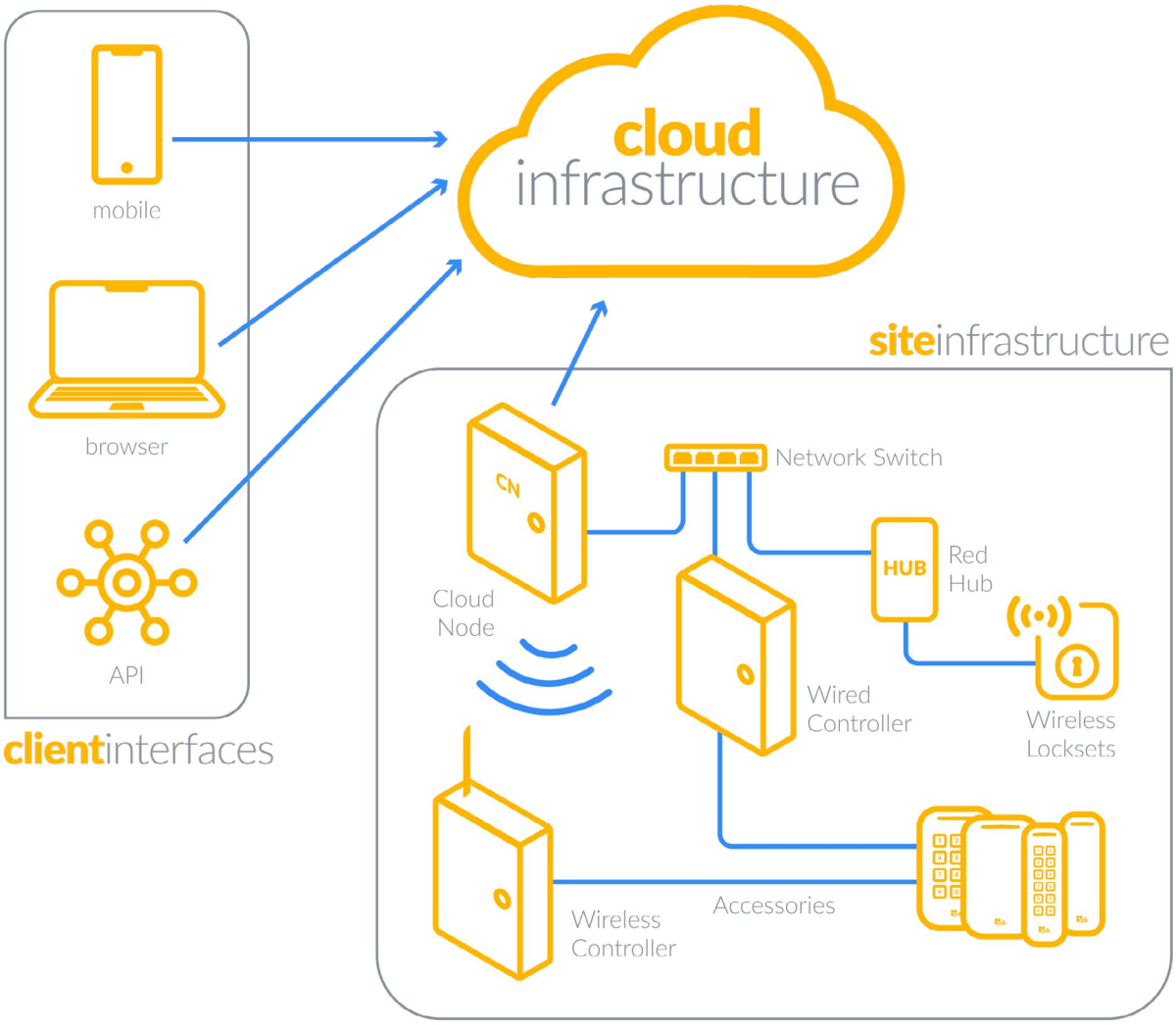
Choosing a cloud-based platform like PDK.io changes how physical security work is divided. As a Software as a Service (SaaS) solution, ProdataKey takes on infrastructure installers would otherwise own: servers, remote access, encryption, patching, and platform monitoring. But on-site responsibility remains. Security and reliability still depend on local decisions: hardware placement, network design and protection, the choice of locks, readers, and credentials, and how access is managed over time. This Shared Responsibility Model is broken down as follows:

	ProdataKey (PDK) Responsibility	Installer/Security Dealer Responsibility
Cloud & Infrastructure	SaaS infrastructure, multi-tenant logical isolation, data encryption at rest, automated cloud backups, SOC2 compliance & penetration testing.	Browser/device endpoint security, enforcing strict user access policies, preventing password reuse.
Network & Communications	Secure VPN tunnels, secure client interfaces, secure API/Webhook architecture.	Local network design, dedicated access control networks or VLAN segmentation, firewall configuration, QoS management.
On-Site Appliances	Secure operating system and application software, firmware image signing/verification.	Proper placement and physical security of enclosures, protecting accessory wiring from physical tampering.
Peripherals & Credentials	Manufacturing highly secure products.	Hardware selection matching the risk profile (choosing OSDP over Wiegand, choosing high-frequency/Red low-frequency.
Power & Continuity	Providing native battery charging circuits and offline local intelligence redundancy.	Selecting and installing backup batteries/UPS for controllers and network switches, choosing proper fail-safe vs. fail-secure locking hardware.
Lifecycle Management	Continuous vulnerability monitoring, developing and publishing timely software/firmware security patches.	Keeping on-site systems online, repairing local faults, coordinating operational downtime with the end-user.

Think of it this way: PDK is responsible for the security of the platform, while the Installer/Security Dealer is responsible for the security in the deployment. This shared responsibility model allows for greater focus on physical security by domain-specific professionals and the leveraging of efficiencies at scale.

PDK.io Platform Architecture

At the foundation of PDK access control is the PDK.io platform, which consists of client interfaces, cloud infrastructure, and site infrastructure.



PDK is responsible for the operation of the components within this architecture that are produced by PDK, according to its specifications. Products offered by ProdataKey and from third parties offer varying levels of security and reliability, both in their design and their configuration. It is the responsibility of each installer to understand the features and configurations of each component and the effect each component selection and configuration choice will have on the security, reliability, and capability of the installed system.

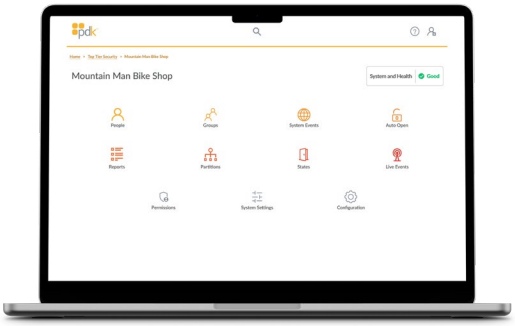
The following sections cover the security features of each component in a PDK.io physical access control installation.

Client Interfaces

Client interfaces are generally of three types: web application access, mobile device applications, and programmatic API access. Each has its own security features and considerations.

Web Application Access via Browser

Browser access to the PDK.io web application is protected with TLS 1.2 and TLS 1.3 using modern, forward-secret AES-GCM cipher suites. Legacy protocols (TLS 1.0/1.1 and SSL) are disabled. Our public endpoints carry an "A" rating from Qualys SSL Labs. Authentication for PDK.io is handled by a dedicated identity service, separate from the application and system-management APIs. It implements the OpenID Connect standard and issues signed, asymmetrically-verified tokens. The token signature algorithm is fixed by the platform, and tokens are validated on every request.



Access tokens used by a browser accessing the PDK.io web application are short-lived, limiting the window in which a token is useful if exposed. Tokens are also scoped to a specific customer system, so a token issued for one system cannot be used to act on another.

Multi-factor authentication is supported for all account holders and is required for privileged administrative roles, who must enroll a second factor before they can perform management operations. The platform supports multiple second-factor methods, including time-based one-time passwords, hardware security keys, and SMS-based verification.

Authentication and other sensitive endpoints are protected by brute-force and rate-limiting controls. Interactive sessions use signed, server-side session storage with bounded lifetimes; an extended "remember me" lifetime is available at the user's choice. Sessions are transmitted only over TLS.

Like all web applications, PDK access control is subject to the same browser-based security risks. Though not a complete list, common methods are:

- Outdated or Insecure Browsers
- Inadequate Protection of Login Credentials
- Reuse of Passwords
- Use of Insecure Browser Add-Ons
- Leaving PDK.io Sessions Logged in and Unattended

The security of the web browser and devices used to access PDK.io is a responsibility of every user of the PDK.io web application.

Mobile Device Applications (Android and iOS)

ProdataKey offers the PDK Access app through the Google Play Store and the Apple App Store and is subject to their quality and security standards. Within the PDK Access app, communication with the PDK.io cloud platform is secured using session management and TLS. Digital Credentials are securely delivered through these mechanisms after the mobile app user has been securely authenticated.

The PDK Access app is designed and maintained with security as a core requirement. Users may introduce vulnerabilities by not:

- Securing their device via passwords and Touch or Face ID
- Operating the app on an insecure network
- Use of outdated operating systems and insufficient patching

Programmatic API Access

Approved third parties may request API client credentials that allow them to interact with the platform programmatically using ProdataKey's REST API, WebSocket service, webhook service, and mobile SDKs. These developer tools are documented at https://developer.pdk.io.

Supported authentication strategies include the authorization code flow (with optional PKCE support) and the client credentials flow, both of which adhere to OAuth 2.0 standards. With the authorization code flow, an application can interact only with systems that the authenticated user is authorized to access. With the client credentials flow, an application can interact only with systems that the API client service user is authorized to access.

Webhook subscriptions require secure URLs (HTTPS) for the notification target. API users may also supply a secret that is used to generate a SHA-1 HMAC from the response body. This HMAC is then included in a response header, which can be used to verify the authenticity of each webhook notification.

Security of Each Platform Component

Delivering a secure access control system for customers requires a disciplined application of security strategies and principles across different layers and security domains. Security for some elements falls within the responsibility of ProdataKey, while others fall upon their respective manufacturers and the skill of the installer.

Cloud Layer

PDK.io's cloud layer is hosted in secure data centers (Google and AWS) governed by industry-leading physical security protocols and procedures trusted by thousands of private and public companies worldwide [1][2]. PDK's cloud infrastructure runs in a private, segmented network. Inbound access is restricted by firewall to a single hardened HTTPS entry point, which terminates TLS; backend services and data stores are not directly accessible from the public internet.

PDK.io provides a multi-tenant platform utilizing application-level access controls to keep dealer and end-customer data logically isolated. These controls are enforced at both the API layer and in back-office services that perform synchronization, backup, and reporting, each of which operates on a single customer system at a time. Customer data stored in our cloud is encrypted at rest, and customer systems are backed up regularly and automatically. Access to data-storage systems is restricted to ProdataKey personnel on a least-privilege basis, and that access is audited regularly and adjusted as roles change.

Because PDK.io infrastructure is maintained by ProdataKey and monitored by its employees, users of PDK.io benefit from managed hosting and ongoing security maintenance.

Regular Penetration Testing

As part of our SOC2 compliance, ProdataKey undergoes regular penetration tests by a well-established third-party contractor. ProdataKey's engineering staff evaluates all findings and prioritizes remediation based on risk, with retesting as appropriate.

Site Infrastructure

Use of PDK.io for physical access requires access control hardware and network devices produced by ProdataKey to be utilized on-site. When installing such systems, careful consideration must be taken to ensure physical, network, and accessory security are properly matched and designed to work together for the desired security profile. Securing the on-premises appliance and the local network it connects to is a shared responsibility: PDK secures the cloud platform and its connection; the installer is responsible for the site network and the physical security of the appliance.

Physical Security

Cloud Nodes are an on-site gateway for controllers and wireless hubs to connect to the cloud. They are shipped in lockable metal cans, which are designed to resist tampering in typical office environments. When installing, select a location where unauthorized access or tampering is unlikely, such as a locked IT or mechanical room. Installation into vulnerable environments may require further physical security measures to be taken. Cloud Nodes are not designed for outdoor installations. Door controllers, similar to Cloud Nodes, are shipped in lockable metal cans, and similar considerations must be taken to guard against tampering.

Never install door controllers or Cloud Nodes on the unsecured side of an entry. Physical access to these enclosures generally means physical access to the doors they control — and attackers will take the easiest path available.

For a secure installation, credential readers with appropriate security features for that site must be selected. Rugged readers are an excellent choice where durability against physical attack is required, and OSDP-connected readers should be used where a threat of digital attack exists.

Door position sensors (DPS), request to exit (REX) devices, and lock actuation devices (maglocks, door strikes, etc.) are simple electromechanical devices most often controlled by simple electronic circuits. For an installation to be considered secure, all wiring from accessories to door controllers must be physically protected from tampering.

Finally, don't overlook methods of entry that bypass electronic control entirely — mechanical keys, unsecured doors, or windows can provide an easy path around the system.

Network Security and Reliability

As an IP-based access control system, having a reliable on-site Ethernet network properly architected, managed, and sized for the environment is paramount. PDK recommends physical access control to be installed on a fully dedicated and physically isolated Ethernet network. This isolation provides a high degree of reliability. Where this is not possible, digital network separation (such as VLANs with proper segmentation plus ACLs) may be an acceptable substitute where a trained networking expert can ensure a network topography for isolation, performance, and remote serviceability.

Any network infrastructure utilized for access control traffic must provide adequate quality of service, and congestion must not result in any meaningful delay of packets. Proper use of Class of Service (CoS) features can help to ensure reliable delivery of access control communication. Use of unmanaged switches or Ethernet hubs is discouraged as they cannot enforce quality of service and cannot be managed, configured, or restarted remotely when troubleshooting issues or network optimizations are required.

ProdataKey devices also depend on the site network for an accurate, secure time source and reliable, conflict-free IP address assignment.

Cloud Node

The Cloud Node is a security-hardened, embedded Linux-based appliance with minimal service exposure to the network to which it is attached. ProdataKey regularly reviews security announcements related to third-party open source software utilized on this device and takes action to address vulnerabilities that affect the device.

For simplicity of installation and management, Cloud Nodes are the only devices on the access control network that require access outside of the local intranet. All traffic to and from the PDK cloud is encapsulated in VPN tunnels and routed via the Cloud Node. Traffic between the site and the cloud is encrypted in transit using TLS, and VPN client network traffic is isolated from one another to prevent packets from being routed between sites. This network-level separation complements the application-level controls that keep dealer and end-customer data logically isolated — providing tenant separation in multiple layers.

Cloud Node (cont.)

When powered, a Cloud Node will acquire an IP address and the current time from authoritative sources. It then makes an outbound socket connection to cloudlink.pdk.io on port 443 (PDK's VPN).

Cloud Nodes run an OpenSSH server and listen on Port 22 to provide software maintenance from PDK's cloud or interaction for remote troubleshooting related to a support incident. For maximum security, this server operates with less secure "password authentication" disabled and only accepts modern MACS and ciphers. Additional details on which external services and ports the Cloud Node uses can be found in our documentation here. Upon installation, specific firewall rules may need to be configured to ensure reliable operation.

Lastly, Cloud Nodes offer a layer of offline redundancy by holding a copy of access decision-related information for the site. Should the Internet connection to the cloud be broken, Cloud Nodes continue managing secure access on site and execute any user-defined rules not dependent on cloud communication. Rules that produce notifications or emails will resume once Internet connectivity is restored.

WiMAC™ Wireless Communication

If equipped, Cloud Nodes directly communicate with edge devices via PDK's secure Zigbee-based WiMAC wireless network utilizing AES-128 encryption. For a more secure installation, PDK recommends setting a unique PAN id when WiMAC is used.

wimac™

Intranet Communication

Cloud Nodes communicate on the local intranet to Ethernet-connected Red™ edge devices via a secure TLS 1.3 connection using AES-256 encryption. These devices rely on a "Trust-on-First-Use" model for initial authentication at install time, and afterward rely upon connection locking for mutual authentication of the Cloud Node and edge device. Prior generations of PDK Controllers (end of sale in 2021) use add-on modules (Lantronix) for Ethernet communication (SIO, EIO, etc.), which do not support authentication or encrypted communication. Organizations still using legacy devices can improve their security profile by upgrading legacy controllers to PDK's current line of Red controllers.

Door Controller Security

Red controllers and wireless locks sold by ProdataKey feature "Controller Continuity" and contain a local database enabling local intelligent access control decisions at the door. Local decisions enable continued operation even without wired or wireless network communication.

The Controller Continuity database uses AES-128 encryption with a unique key per controller, designed to protect credentials and other sensitive information from retrieval, including against reverse-engineering attempts. PDK's door controller design incorporates a secure execution environment with firmware image signing and verification on every update.

Accessory Security

Readers

Of all components in a physical access control system (PACS), readers are, with few exceptions, installed in the least secure locations. Reader model selection is therefore one of the most important decisions made when designing any PACS. For the utmost security, no readers sold by ProdataKey contain access-decision logic.

ProdataKey sells a variety of low-cost to premium readers, each with its own set of security features. Readers that use Wiegand as a wire protocol do not utilize encryption or authentication and rely heavily on installer skill to minimize the likelihood of physical exploitation. In general, Wiegand should not be used where a high level of security is needed. OSDP-connected readers are a more secure option and provide encrypted secure channel communication, protecting against wiretapping that could reveal credential numbers.

It is the responsibility of every installer to understand the security technology offered in readers, PDK-branded or otherwise, and the features, protocols, and technologies provided.

Locking Devices

Locking devices must be carefully chosen to ensure they meet life safety, fire, and building code requirements. Free egress must be assured, and any delayed egress systems must be used only where permitted by code. Magnetic locks have special considerations for life safety and require a full egress package. Fail-safe versus fail-secure decisions must be driven by code compliance, not convenience. Installers must know exactly which doors will fail-safe versus fail-secure when all primary, secondary, and tertiary power sources have been exhausted.

ProdataKey is not responsible for the correct installation of any lock or access control product—this responsibility falls on the installer.

Credential Security

Low Frequency (125kHz Prox) Credentials

Prox credentials, a decades-old staple of the RFID-based access control market, offer minimal security and can be easily copied, emulated with readily available “flippers”, or read from a distance. While their low cost and high availability make them a common choice, they should not be used in applications where their drawbacks present a security risk.

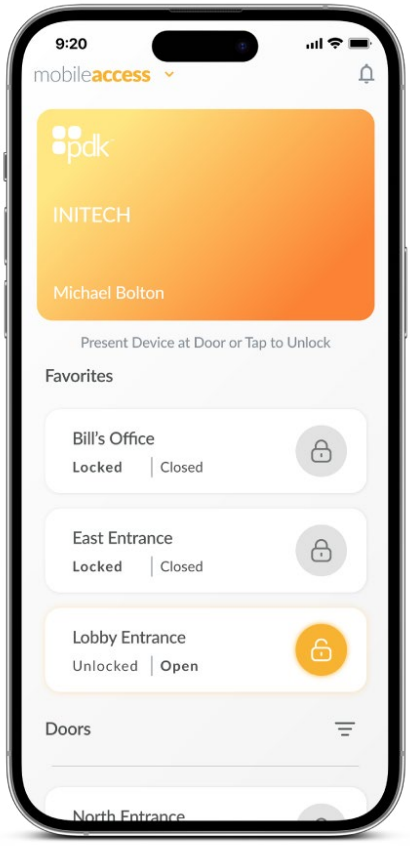
High Frequency (13.56MHz) Credentials

A more modern and superior option than low-frequency credentials, high-frequency credentials come in a variety of technologies, offering security profiles ranging from those equal to low-frequency credentials to the highly secure DESFire EV3, which supports LEAF credentials. Equally important to selecting the right credentialing technology is ensuring that the reader enforces their security features. Readers that ignore the secure badge ID on the credential, and instead read a credential’s serial number or UID, do not provide security greater than a low-frequency card.

Red Readers sold by ProdataKey provide a high-security solution and only read the secure badge ID of Red Credentials, designed to resist cloning, skimming, or relay attacks. For these reasons, ProdataKey always recommends Red Credentials and Red Readers.

Bluetooth (BLE) Credentials

PDK Bluetooth credentials conform to the LEAF standard, which uses an AES-256 symmetric key to establish a secure connection between the PDK Access mobile app and Red mobile-capable readers. The encryption algorithm enforces mutual authentication between the credential and the reader, and enables secure transmission of the badge ID. These steps are designed to make Bluetooth credentials resistant to sniffing and cloning.



PDK Access Mobile Button Credentials

PDK Access Mobile Button credentials use a secure JWT to identify and ensure the credential is issued by PDK. This token is protected at rest using the mobile device's native Secure Enclave (iOS) or Secure Element (Android). This uses hardware-backed security designed to ensure the encryption keys are bound to the specific device and resist extraction. This makes it extremely difficult for attackers to decrypt the token, even if they manage to copy the device's physical storage. Access requests are transmitted to the PDK cloud over modern HTTPS encryption and security standards, designed to protect the credential throughout transmission.

Electrical Power Sources

Electronic physical access control systems require a reliable power source to fulfill their function. Unreliable power undermines the installation's security and reliability.

Most installations achieve high reliability through a two- or three-layered approach:

- Reliable primary (grid) connection
- A standby generator and automatic transfer switch (ATS) (three-layer only)
- Access control specific battery failover

Many PDK.io on-site appliances (Cloud Nodes and controllers) are equipped with native backup battery support. Failure to utilize this capability or provide an external battery backup solution (such as a UPS) usually means door access is interrupted when power is lost and may increase the risk of unauthorized access to the facility.

Network switches for the access control network should also be under battery backup, especially when Power over Ethernet (PoE) devices are used.

Updatability

The security profile of any system inevitably degrades over time as new vulnerabilities appear. Because of this, robust and rapid updatability is important to mitigate and correct issues before they can be exploited. Software and firmware running on PDK.io's on-site appliances and accessories have been designed from the ground up to be remotely upgradable. ProdataKey's engineering staff regularly releases security updates to connected systems.

As security professionals, installers should accommodate updates, account for them in their systems management, and ensure that on-site systems are always healthy and online. Upgrades to software and firmware often entail restarting network services or rebooting embedded devices. These operations sometimes result in a brief downtime.

ProdataKey regularly publishes release notes and notices of upcoming updates to assist installers in their communication with end users.

Responsible Access Control Usage

To ensure secure operation, PDK.io users are responsible for following access control best practices:

Ensure every individual with access has a personal profile with accurate information. Do not allow for the sharing of credentials, PINs, or the duplication or emulation of credentials. Reclaim physical credentials upon revocation.

Utilize integrations such as Entra, Google Workspace, and similar systems to automate access provisioning and deprovisioning.

Configure alerts (door force, door prop, duress PIN, etc) on abnormalities and ensure those receiving these alerts are properly trained.

Regularly search event reports to spot abnormal or unexpected behaviors.

Assign access by role/group, not one-off per person, so policy is auditable and consistent.

Periodically audit (quarterly or semi-annually) all credential holders and their access rights to ensure compliance with best practices.

Do not grant access to any individual or group that extends beyond their role's responsibilities (principle of least privilege).

Utilize time-based schedules, like business hours, after-hours restrictions, and holiday calendars. Most people don't need 24/7 access.

References

1. Google Security Overview
2. AWS Security Overview

Notice

This document is provided for informational purposes only and reflects ProdataKey's (PDKs) current product offerings, which are subject to change without notice. The information contained herein does not constitute a commitment, representation, or warranty of any kind — express, implied, or statutory — by PDK, its customers, or its suppliers, and shall not be construed as creating any obligation or assurance on the part of any party.

PDK products and services are provided "as is," without warranties of merchantability, fitness for a particular purpose, or any similar guarantees. Each reader is solely responsible for independently evaluating any claims made in this document and assessing their applicability to specific installation environments. Users of PDK.io bear ultimate responsibility for the security profile of any installation they design, configure, or deploy.

Copyright © 2026 PDK. All rights reserved. No part of this document may be reproduced or distributed without prior written permission from PDK.