1KOSMOS

Truly know who's behind the device.

# The Future of Shared Workstation Security: 12 Authentication Strategies for 2025

## How to Secure, Streamline, and Future-Proof Shared Workstation Access

As organizations move into 2025, securing shared workstations requires innovative authentication methods that balance security, usability, and compliance. Here are 12 critical factors to consider when upgrading authentication for shared work environments:

### 1 Passwords Are Dead—Go Passwordless

Passwords create security risks in shared workstations. Adopting **passwordless authentication** eliminates phishing threats, prevents credential sharing, and simplifies access.

### 2 Multi-User Authentication on a Single Device

In shared environments, requiring individual security keys inflates costs. **Choose authentication solutions that allow multiple users to securely log in using a shared device—like the 1Kosmos 1Key.**

### 3 Mobile Devices Aren't Always an Option

Many environments **prohibit mobile devices** in secure or high-traffic areas. Ensure your authentication solution **doesn't require a phone for MFA** and works in restricted environments.

### 4 Biometrics: The Future of Workstation Security

Fingerprint authentication **ensures fast, secure access** without passwords or PINs. **Biometric authentication eliminates credential theft** and unauthorized sharing while maintaining compliance with privacy regulations.

## 5 Minimize Downtime with Fast Login and Logout

In high-turnover environments like call centers or medical offices, **delays in authentication slow productivity**. Biometric login enables employees to **instantly access** and exit workstations securely.

## 6 Compliance-Ready Authentication for Regulated Industries

Shared workstations in **healthcare, finance, and government require strict authentication controls**. Ensure solutions meet **GDPR, HIPAA, and PCI-DSS compliance** and providefull audit trails to support compliance audits.

## 7 Reduce IT Workload with Seamless Integration

Your authentication system should **work with existing infrastructure** (Windows, macOS, Entra ID, cloud apps, etc.) and support **FIDO2 passwordless authentication standards** to minimize IT overhead and close security loopholes.

## 8 Improve Security While Lowering Costs

Managing passwords, access cards, and key fobs can get **expensive**. A **shared biometric security key** reduces hardware costs, minimizes lost devices, and eliminates password resets.

## 9 Address Insider Threats with Strong Identity Proofing

Shared workstations pose **a high risk for insider attacks**. Ensure your authentication process **verifies the true identity of users** before granting access to sensitive systems.

## 10 Enable Zero Trust Access at Shared Workstations

Zero Trust security requires **continuous and convenient identity verification**. Deploy **passwordless MFA** that monitors risky behaviors and enables frictionless step up authentication to ensure every session is, **secured to legitimate, authorized users.**

## 11 Modernize Security for Shared Access

Traditional MFA (like SMS or OTPs) **is vulnerable to SIM swaps, man in the middle attacks**, push bombing and more. A **modern authentication method**, such as using verified biometrics or FIDO2 security keys, prevents credential theft and compromised accounts.

## 12 Future-Proof Your Authentication Strategy

As cyber threats evolve, **invest in authentication solutions** that are scalable, flexible, and **adaptable to emerging security challenges**—ensuring long-term protection.

# Ready to Secure Your Shared Workstations?

**1Kosmos 1Key** offers **passwordless biometric authentication** designed for **multi-user shared workstations**—eliminating passwords, reducing risks, and increasing efficiency.

- **FIDO2-compliant biometric security**
- **Works without mobile devices**
- **Supports unlimited users per workstation**
- **Seamlessly integrates with existing infrastructure**

Learn More at 1Kosmos.com

1KOSMOS