Skillmine
Technology • Consulting • Services

Skillmine Auth™

Windows MFA: Securing Remote & Field Teams

Industry Focus

Remote & Hybrid Workforces – Financial Services, Healthcare, IT, and other sectors where employees access Windows desktops, RDP sessions, or virtual machines remotely.

- Designed for sales, support, and field teams who frequently connect from untrusted networks.
  Critical for organizations that must protect sensitive data and
- comply with regulatory requirements such as ISO 27001 and PCI-DSS.

The Challenge

Remote and hybrid work introduces high-risk endpoints:

Employees logging in from **hotels, airports, or home networks** face increased threats of credential theft.

Field teams and support staff often access critical systems via **RDP or VDI,** making endpoints prime targets for attackers

Passwords alone cannot defend against **phishing, brute-force attacks, or stolen credentials,** leaving systems exposed.

Regulatory frameworks require **strong authentication at endpoints**, and failure can result in penalties, breaches, or operational loss.

Our Approach

Skillmine Auth Windows MFA enforces multi-factor authentication at the OS level to protect remote and hybrid workforce logins:

- Secures **local, RDP, and VDI logins,** blocking unauthorized access at the first point.
- Supports multiple authentication methods: **Push, TOTP, SMS, Email OTP, and hardware tokens,** ensuring flexibility and usability.
  Mobile-friendly MFA ensures **fast, seamless access** without slowing down productivity.
- Provides **audit-ready evidence** to support compliance.
-

Core Capabilities

- **Multi-Factor Authentication (MFA)** for Windows desktops, RDP, and VDI sessions
- Authentication methods: **Push, TOTP, SMS, Email OTP, hardware tokens,** etc.
- **Scalable** for hybrid IT environments (on-prem, remote, cloud-hosted)
- Minimal disruption to employee workflows while maintaining **OS-level security**

Impact and Results

Stronger Endpoint Security:
Blocks unauthorized access and prevents credential misuse.

Regulatory Compliance:
Supports ISO 27001, PCI-DSS, and other frameworks by enforcing strong authentication at endpoints.

Operational Efficiency:
Mobile-friendly MFA ensures fast logins for remote and field teams.

User-Friendly Experience:
Seamless authentication minimizes workflow disruption.

Enterprise-Ready:
Scalable across multiple endpoints, remote access points, and hybrid IT environments.

Real-World Examples

- **Sales Teams on the Road:** A regional sales executive logs in via RDP from a hotel Wi-Fi. Windows MFA ensures their credentials cannot be misused even if intercepted on an unsecured network.
- **Customer Support Teams Working Remotely:** Support agents accessing customer data remotely verify logins with MFA, reducing insider threats and credential misuse.
- **Field Engineers Accessing Critical Systems:** Engineers servicing remote sites log into servers via RDP. MFA ensures only authorized staff can reach these critical endpoints.
- **Hybrid Workforce Using Shared Devices:** In offices with shared machines, Windows MFA ensures that even if one user's password is compromised, the attacker cannot access the system without the second factor.
- **VDI Access in High-Security Industries:** Financial or healthcare organizations using virtual desktops enforce MFA at Windows login to safeguard sensitive data against breaches.

For more information
Contact: info@skill-mine.com
Visit us: skill-mine.com

Skillmine
Technology • Consulting • Services

Stay Connected