Windows MFA: Unlock Secure Access with Skillmine AUTH

Industry Focus

Healthcare → Secures shared clinical terminals and aligns with HIPAA compliance.

BFSI → Protects branch desktops and remote systems, ensuring RBI and GDPR audit-readiness.

Manufacturing & Industrial → Safeguards shared workstations on factory floors without requiring full AD integration.

Remote & Hybrid Workforces → Defends RDP and VDI logins for field teams on untrusted networks.

VDI & Thin Client Environments → Maintains strict access controls in cloud and hybrid setups.

The Challenge

With **80% of breaches tied to stolen or weak credentials,** Windows desktops, laptops, and servers have become **prime attack targets.**

- Passwords alone cannot prevent unauthorized access.
- Shared terminals increase the risk of insider misuse and credential sharing.
- Remote access via RDP or VDI makes systems vulnerable to theft on untrusted networks.

Our Approach

Skillmine AUTH introduces **MFA directly at the Windows login screen—covering local, RDP, and VDI logins.**

- Every user must verify identity with **multiple authentication factors.**
- Attacks are blocked **before applications or data are reached.**
- Delivers **seamless login experience** with minimal user disruption.

Core Capabilities

Native Windows Login Protection
MFA for local, RDP, and VDI logins.

Directory Integration (AD/LDAP)
Centralized user and policy management.

Flexible MFA Channels
Email OTP, SMS, WhatsApp, Push, TOTP,
Backup Codes, Face/Pattern, etc.

Comprehensive Audit Logs
Records every login and MFA check to support
RBI, ISO 27001, HIPAA, and GDPR compliance.

Impact and Results

99%+ Attack Reduction

Stops credential-based threats even with compromised passwords.

Regulatory Compliance

Meets mandates from RBI, HIPAA, GDPR, ISO, and cyber insurers.

Zero-Trust Alignment

Every login becomes a verified act of identity.

Operational Efficiency

·Smooth user switching and MFA with minimal workflow disruption.

Audit-Ready Evidence

Rich metadata captured for investigations and reporting.

Real-World Examples

- **Factory Floor Terminals** → MFA secures shared workstations, ensuring safety and compliance.

- **Sales & Support Teams** → Protects RDP sessions against stolen credentials, even on unsecured Wi-Fi.

- **Clinics & Branches** → Prevents unauthorized access to sensitive systems on shared devices.

- **Cyber Insurance** → Lowers premiums by meeting insurer MFA mandates. **Virtual Desktops** → Ensures stolen tokens can't be reused to hijack VDI
- sessions.

Stay Connected