



SMBsecure™ For Windows Server

ENFORCED TWO-FACTOR AUTHENTICATION FOR ANY:
DOMAIN | LOCAL | THIRD-PARTY ACCOUNT ON WINDOWS SERVER

Overview of Service

Windows Servers are highly vulnerable to Brute Force, RDP and Account attack.

SMBsecure™ for Windows Server simplifies multi-factor authentication (MFA) implementation on Windows Servers. It provides easy setup, strong login verification through 2FA codes, and support for local, remote, online, and offline logins. The solution improves Server security and compliance with reporting and auditing capabilities.

HOW IT WORKS

SMBsecure™ for Server enforces multi-factor authentication (MFA) to add a critical layer of protection to Windows Server security beyond passwords. It requires both credentials and a time-sensitive code from an authenticator app for authorised users to access the server.

Hardening Access to Servers is now a Critical Control!

SIMPLE SETUP

The solution is designed to be easy to set up and use, simplifying the process of implementing 2FA for Windows Server logons.

ZERO-TRUST USER VERIFICATION

MFA adds an additional layer of security to the login process by requiring users to provide a second form of authentication, typically a code generated by an authenticator app, in addition to their password alone.

MFA & PASSWORD POLICY FOR NON-DOMAIN SERVERS

Maybe you are already using MFA for domain-accounts synced to M365, but what about all those local accounts **NOT synced with M365?! This yields very high risks for exploit and server compromise. SMBsecure™** can selectively implement MFA for all or local accounts only. It can also enforce a password policy to reform authentication posture on non-domain servers, including password length, strength, complexity and account lock-out.

SECURE LOCAL AND REMOTE LOGONS

The MFA implementation works for both local and remote logons, ensuring that users go through the MFA process regardless of their location.

OFFLINE AND ONLINE ACCESS

The MFA codes can be used for both online and offline logins, providing flexibility and security even when the server is not connected to the internet. Administrators can also use an offline Recovery Code, if needed!

SUPPORT FOR AUTHENTICATOR APPS

The solution supports multiple authenticator apps, such as Google Authenticator and Microsoft Authenticator, allowing users to choose their preferred app for generating 2FA codes. No MFA fatigue here!

CENTRALLY AUDIT, REVIEW & REPORT MFA

Easily assess (in real-time) the use & status of **SMBsecure™** MFA across ALL User Accounts on computers (including blind spot local accounts) to report and prove **SMBsecure™** managed 2FA is used as a vital authentication control for Governance, Risk & Compliance (GRC).