

MyID MFA

| Phishing-Resistant Authentication & Passwordless Windows



MyID® MFA adds multi-factor authentication and passwordless logon to Windows desktops, cloud services and on-premise applications. No additional database is required as MyID MFA stores user data in the existing Active Directory, with no schema extensions. It is a FIDO accredited server issuing and authenticating Phishing resistant credentials to security keys and mobile devices.

Key features

Authentication methods

- Grid Pattern, 4x4 up to 8x8
- One Time Code by SMS or email
- Mobile Push with biometrics
- YubiKey & OneSpan Digipass
- Synced & device-bound passkeys

Phishing resistance

- FIDO2 passkeys resist phishing
- Device-bound keys stay put
- Push carries no secret
- Throttling limits push fatigue
- Access control via group

Enrolment & administration

- Self service, up to 10 devices
- Password reset & unlock
- Operators issue grids & tokens
- Portal dashboards & reports
- Administrator & Auditor roles

Passwordless Windows

- Agent for Windows and Server
- Vault returns the AD password
- 32-byte managed password
- Supported both online and offline logon
- Locks when the key is removed
- User auto selected on FIDO key insertion

Integration & federation

- NPS and Free RADIUS
- SAML 2.0 & OpenID Connect
- Federation with Microsoft 365
- Web Services API
- VPN integration via standard industry protocols

Deployment & availability

- Windows Server 2019 to 2025
- Agents run active-active
- Load balancer can optionally front authentication servers
- Multi-tenant for providers
- Event codes to the Event Log

HIGHLIGHTS

A standalone FIDO server

Both a FIDO authentication server and a passkey issuer, with self-service enrolment.

Fully passwordless Windows

The MyID MFA Credential Provider enables users to authenticate Windows desktop using their FIDO credential directly, without the user entering a separate password.

Works offline

The desktop agent authenticates from an encrypted cache when no server answers.

A modern ADFS alternative

One identity provider covers cloud apps, on-premise apps and the Windows desktop.

No schema extensions

Users and settings are stored within existing Active Directory fields.

Push without shared secrets

No code or secret passes through Apple or Google, and push failure is handled.

RELATED DOCUMENTS

The Authentication Server Installation and Configuration Guide and the Windows Desktop Agent guide are available from Intercede support.

Product Version: MyID MFA v5.5

Technical specifications



SUPPORTED AUTHENTICATION METHODS

AUTHENTICATION METHOD	SUPPORTED
FIDO2 Security Keys	Yes
Device-Bound Passkeys	Yes
Synced Passkeys	Yes
Mobile Push	Yes
OATH TOTP	Yes
Pattern Grid	Yes
OneSpan OTP Tokens	Yes

SERVER REQUIREMENTS

COMPONENT	REQUIREMENT
Server Operating System	Windows Server 2019 Windows Server 2022 Windows Server 2025
Authentication Server	MyID Authentication Server
Web Management Portal	Browser-based administration and policy management
Directory Service	Microsoft Active Directory
Identity Federation	Microsoft Entra ID, Microsoft 365 and SAML 2.0 Identity Providers
Authentication Methods	FIDO2 Passkeys, Security Keys, Mobile Push, OATH TOTP, Pattern Grid and OTP Tokens
Policy Engine	Native web-based policy distribution and management
Audit & Reporting	Centralized authentication, enrollment and administration auditing
High Availability	Supports enterprise deployment architectures
Network Connectivity	Required for online authentication, federation and administration services
Offline Authentication Support	Windows client authentication remains available during loss of connectivity
Browser Requirement	Modern browser required for administration portal access

CLIENT REQUIREMENTS

COMPONENT	REQUIREMENT
Desktop Operating Systems	Windows 10, Windows 11
Client Software	MyID Windows Desktop Agent
Browser Support	Modern Web Browser
Authentication Devices	FIDO2 Keys, Passkeys, OTP Tokens
Offline Authentication	Supported
Self-Service Enrollment	Supported
Self-Service Recovery	Supported

SUPPORTED ENVIRONMENTS

ENVIRONMENT	SUPPORTED PLATFORMS
Server Authentication	Windows Server Platforms
Identity Providers	Microsoft Entra ID, Microsoft 365, SAML 2.0 Providers
Directory Services	Microsoft Active Directory
Deployment Models	On-Premises, Hybrid
Administration	Web Management Portal

SECURITY FEATURES

CAPABILITY	DESCRIPTION
Phishing Resistance	FIDO2 and WebAuthn Based Authentication
Replay Protection	Prevents Credential Replay Attacks
MitM Protection	Protection Against Adversary-in-the-Middle Attacks
Push Protection	Push Fatigue Mitigation Controls
Passwordless Access	FIDO2-Based Authentication
Offline Security	Secure Authentication Without Network Access

COMPLIANCE AND STANDARDS

AREA	STANDARD
Passwordless Authentication	FIDO2
Web Authentication	WebAuthn
Identity Federation	SAML 2.0
Authentication Assurance	NIST SP 800-63B AAL2 NIST SP 800-63B AAL3
Regulatory Alignment	NIS2 Phishing-Resistant MFA Requirements