intercede

MyID Authenticate

— DATA SHEET

MyID Authenticate

Phishing-Resistant, Passwordless, Directory Independent



MyID® Authenticate, version 2026.1 brings multi-factor and passwordless sign-in to Windows desktops, cloud services and on-premise applications. User accounts can be onboarded through Active Directory or other data source, with their information held within a dedicated MyID Authenticate database. Phishing resistant credentials are supported as MyID Authenticate acts as both a FIDO server and a passkey issuer.

Key features

Authentication methods

- Synced & device-bound passkeys
- YubiKey & OneSpan Digipass
- Grid Pattern, 4x4 up to 6x6
- One Time Code by SMS or email
- Mobile Push with biometrics

Passwordless Windows

- Agent for Windows Client
- Passwordless login via Client vault
- Supported online and offline logon
- Locks when the key is removed
- User auto selected on FIDO key insertion

Phishing resistance

- Passkeys work only from registered device
- Private keys never leave the device
- Credentials cannot be copied or shared.
- Authentication is tied to a trusted device.

Integration & federation

- NPS and RADIUS
- SAML 2.0 & OpenID Connect
- SCIM user provisioning
- Web services API
- VPN integration via standard industry protocols

Enrolment & administration

- Self service, up to 10 devices
- Operators issue grids & tokens
- Browser-based administration
- Light and dark modes

Deployment & availability

- Windows Server 2022 and 2025
- SQL Server or PostgreSQL
- Simple guided deployment
- Load balancer can optionally front authentication servers
- Event codes to the Event Log

HIGHLIGHTS

A standalone FIDO server

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

Directory Independent

Accounts and attributes arrive through SCIM, so identities can come from whichever database you choose.

Works offline

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

A modern ADFS alternative

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

Administer from a browser

Every administrative task runs in the Web Management Portal, on a desktop or a tablet.

Scripted deployment

PowerShell installs the server interactively or from a script, against SQL Server or PostgreSQL.

RELATED DOCUMENTS

The MyID Authenticate Server Installation and Configuration Guide, Web Management Portal User Guide, Self Service Portal User Guide and Windows Desktop Agent Integration Guide are available from Intercede support.

Product Version: MyID Authenticate 2026.1

Book your MyID Authenticate Demo now

www.intercede.com | info@intercede.com
+44 (0) 1455 558111 | +1 888 646 6943

© 2026 Intercede Group plc

Technical specifications



MyID Authenticate

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 2022 Windows Server 2025
Authentication Server	MyID Authentication Server
Web Management Portal	Browser-based administration and policy management
Directory Service	None required, SCIM provisioning
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 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
Database	SQL server or PostgreSQL

CLIENT REQUIREMENTS

COMPONENT	REQUIREMENT
Desktop Operating Systems	Windows 10, Windows 11
Client Software	MyID Windows Desktop Agent
Browser Support	Edge, Chrome, Firefox, Safari
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	Directory Independent (SCIM)
Deployment Models	On-Premise, Cloud, 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

Product Version: MyID Authenticate 2026.1

© 2026 Intercede Group plc

www.intercede.com | info@intercede.com
+44 (0) 1455 558111 | +1 888 646 6943