



MyID® PSM enables organisations to enforce modern NIST 800-63B compliant password policies. Existing and new passwords within Active Directory are validated against the extensive MyID Password Breach Database.

Continued compliance: The MyID PSM Domain Controller Agent validates password changes in real time. Scheduled scans re-check existing passwords against new breaches. Breached, shared and dormant accounts are then automatically remediated.

Key features

Breach detection

- Checks the Breach Database
- Over 11 billion breached credentials
- Only a partial hash is sent
- Full offline set on request
- Stems catch similar passwords

NIST-aligned policy

- Defaults meet NIST 800-63B
- Minimums per character class
- User names excluded from passwords
- Passphrases skip complexity
- Longer passwords live longer

Remediation & alerting

- Force a change, or disable
- Exclude service accounts
- Alerts to admins & managers
- Administrators get summaries
- Password Security dashboard

Real time & retrospective

- Agent intercepts every change
- Non-compliant ones rejected
- Scheduled scans of hashes
- Run Now starts in 15 minutes
- Fail-safe denies a password change if a domain controller is offline

Domain Controller Agent

- Runs on writeable controllers
- No direct internet by default
- Talks to the server on 14443
- Failover with proxy support
- Keeps the Vault in step

Deployment & availability

- Windows Server 2019 to 2025
- Active Directory, no changes
- Load balancer can optionally front authentication servers
- Event codes to the Event Log
- Policy from the portal

HIGHLIGHTS

Over 11 billion breached credentials

And counting, stored in our Password Breach Database and continually updated.

Works fully offline

A full offline copy is available, so sites with no internet can disable cloud lookups.

NIST 800-63B by default

Default policy meets NIST SP 800-63B, with a live compliance breakdown in the portal.

Stops shared passwords

A password already used by another account in the domain is rejected outright.

Catches disguised passwords

Heuristics revert substitutions such as @ to a, and stemming catches variants.

Memorable security phrases

Automatically generates memorable security phrases for users, these are breach and blacklist checked.

RELATED DOCUMENTS

The Password Security Management Quick Start Guide and the Domain Controller Agent guide are available from Intercede support.

Product Version: MyID PSM v5.5



Technical specifications

SERVER REQUIREMENTS

COMPONENT	REQUIREMENT
Authentication Server	MyID Authentication Server
Operating System	Windows Server 2019 Windows Server 2022 Windows Server 2025
Directory Service	Microsoft Active Directory
Domain Controller Agent	Required on Every Writable Domain Controller
Administration Interface	Web Management Portal
Alerting Services	Email Notification Services
Password Database	Cloud or Offline Deployment Options

CLIENT REQUIREMENTS

COMPONENT	REQUIREMENT
Desktop Operating Systems	Windows 10, Windows 11
Client Software	MyID Windows Desktop Agent
Browser Support	Modern Web Browser
Active Directory Account	Required
Self-Service Password Reset	Supported
Self-Service Account Unlock	Supported
Email Recovery Services	Supported
SMS Recovery Services	Supported

SUPPORT ENVIRONMENTS

ENVIRONMENT	SUPPORTED PLATFORMS
Desktop Operating Systems	Windows 10, Windows 11
Server Operating Systems	Windows Server 2019, 2022, 2025
Directory Services	Microsoft Active Directory
Deployment Model	On-Premise
Management Interface	Web Management Portal
Password Databases	Cloud, Offline Full, Offline Minimal
Integration Interfaces	REST API, Web Services API

PASSWORD SECURITY CAPABILITIES

CAPABILITY	DESCRIPTION
Breached Password Detection	Validates Against Compromised Credential Database
Password Stemming	Detects Common Password Variations
Heuristic Analysis	Identifies Weak Password Patterns
Shared Password Discovery	Detects Password Reuse Across Accounts
Dormant Account Analysis	Identifies Inactive Accounts
Policy Enforcement	Real-Time Validation During Password Changes
Compliance Monitoring	Continuous Assessment and Reporting

COMPLIANCE AND STANDARDS

AREA	STANDARD
Password Management	NIST SP 800-63B
Directory Enforcement	Active Directory Native Integration
Security Monitoring	Compromised Password Detection
Compliance Reporting	ISO 27001 Reporting Support GDPR Reporting Support Cyber Essentials Plus Reporting Support
Audit Controls	Full Audit Trail
Integration Standards	REST API Web Services API

Product Version: MyID PSM v5.5