intercede

MyID MFA PSM

What's new in MyID MFA & PSM v5.3

Security Phrases:
Security phrases replace passwords with long, random, memorable phrases offering enhanced protection. Their length and randomness increase entropy, preventing guessing or cracking, while memorability reduces insecure password storage. When enabled, users authenticate with security phrases instead of passwords. Phrases are server-generated, with users able to regenerate new ones themselves using the Self Service Portal or the Windows Desktop Agent.

4x4 and 5x5 Pattern Grids:
Grid patterns now support 4×4 and 5×5 dimensions. The 5×5 grid is recommended for optimal security; while 6×6 and 8×8 grids are larger, they support only numeric characters.

a	d	x	m	c
8	2	9	t	b
k	e	s	5	7
6	3	4	f	n
u	h	w	r	v

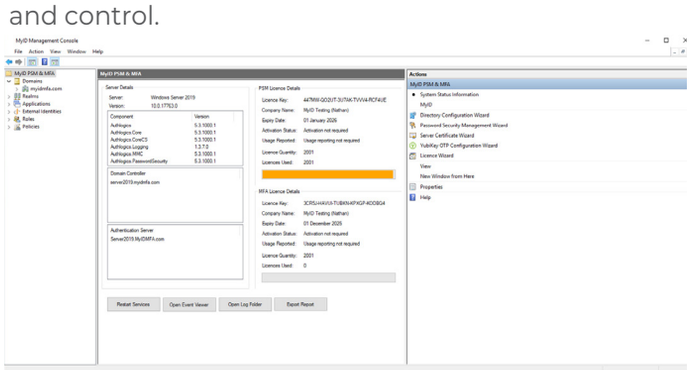
You can now specify which grid sizes are allowed rather than setting a minimum size. New installations of MyID MFA 5.3 and above default to 5×5 grids. Upgrades may allow 6×6 and 8×8 grids based on your previous configuration.

For enhanced security, 4×4 and 5×5 grids use both numbers and letters. Confusingly similar characters (like 1/i, 0/o) and characters with descenders (like y, p) are excluded for clarity.

Windows Server 2025 Support
MyID MFA and PSM now support Windows Server 2025 for the following additional features:

- Domain controllers.
- The MyID ADFS Agent.
- The MyID Exchange Agent.
- External Identities.

New System Dashboard
A new System Dashboard provides a real-time system snapshot directly within Microsoft Management Console (MMC) for improved visibility and control.



Swissbit and Onespan FIDO Integration
The Windows Desktop Agent now supports specific FIDO tokens from Swissbit and OneSpan in addition to YubiKey devices. The following keys are now supported:

- Swissbit iShield Key 2 Pro Mifare USB-C
- Onespan Digipass FX7

Windows for ARM64 Support
MyID MFA and PSM 5.3 now supports Windows for ARM64.

Change Password Link
Browser notifications for compromised passwords now include a direct link to the password change page for that site, when available. If the specific change-password page is unknown, the link redirects to the website's homepage where the compromised password was used.

Windows Desktop Agent Technology Restriction
MyID Windows Desktop Agent now defaults to restricting access to the authentication technology specified in the Authentication Provider UI GPO setting only. To permit users to use any configured authentication technology, enable the Allow Any Authentication Type GPO setting. This option is disabled by default for enhanced security.