intercede

MyID MFA PSM

What's new in MyID MFA & PSM v5.5

MMC migration phase two, native policy management, and broader FIDO and OTP token support.

Web Management Portal: MMC Migration Phase Two

MyID® MFA & PSM 5.5 delivers the second phase of the programme to retire the legacy Microsoft Management Console snap-in. Application Management, Access Control Policies and Identity Provider configuration all move into the Web Management Portal, giving administrators a single, browser-based home for everyday tasks. With phase three on the roadmap, daily administration is faster, easier to delegate, and consistent across deployments.

Native Policy Mechanism Replaces Group Policy

MyID MFA & PSM 5.5 introduces a native policy mechanism inside the Web Management Portal, removing the dependence on Microsoft Group Policy for client configuration. Administrators define and distribute MyID MFA /PSM policies directly from the portal, simplifying deployment in mixed environments and reaching users on machines that sit outside an Active Directory domain.

OneSpan OTP Token Integration

MyID MFA 5.5 adds management for OneSpan one-time password tokens. DPX seed files import directly into MyID MFA, individual tokens are assigned to users through a new device assignment mechanism, and the resulting OTP codes work for both Identity Provider authentication and Windows Desktop logon. Organisations standardised on OneSpan can now bring their existing OTP estate under MyID MFA without changing hardware.

Auto-Locking With Device Bound FIDO Keys

The MyID Windows Desktop Agent now supports auto-locking, keeping a user's account unlocked only while their registered FIDO key remains inserted. Remove the key and the workstation locks immediately, giving security teams a stronger physical-presence control with no extra steps for the user.

For further information, please contact us to discuss your requirements.

Web: www.intercede.com
Email: info@intercede.com
or call: +44 (0) 1455 558111
+1 888 646 6943

intercede

MyID MFA PSM

Auto-Selecting a FIDO User at Logon

MyID MFA 5.5 also introduces automatic user selection. When a user inserts a registered FIDO key, the logon process starts automatically with the device and username pre-selected and ready to authenticate. Combined with auto-locking, the FIDO key becomes a true session anchor: insert to log in, remove to lock.

Support for IDEMIA One Key Bolt FIDO Tokens

The Windows Desktop Agent now supports the IDEMIA One Key Bolt FIDO token, expanding the range of certified, hardware-backed passkey devices that work with MyID MFA. Users get the same passwordless logon experience already available with other supported FIDO devices, with the choice of token left to the organisation.

Streamlined .NET Deployment

The .NET prerequisites for the Windows Desktop Agent, the Domain Controller Agent and the MyID Authentication Server are no longer bundled with the installation programs. Administrators download the latest packages directly from Microsoft, so systems pick up the newest security updates immediately rather than waiting for a bundled version to refresh.

Licensing Improvements

Licence administration has been refined in MyID MFA & PSM 5.5 to give administrators clearer visibility of consumed and available licences across the platform. The improvements simplify reporting, reduce the chance of mismatches during scaling, and make audits faster to complete.

For further information, please contact us to discuss your requirements.

Web: www.intercede.com
Email: info@intercede.com
or call: +44 (0) 1455 558111
+1 888 646 6943