intercede

MyID CMS

What's New in MyID CMS v12.18

New Features

Fingerprint Enrollment for FIDO Security Keys

MyID now supports fingerprint enrollment directly at the point of Passkey registration, streamlining the onboarding process for biometric security keys.

Using fingerprint authentication offers a faster, more convenient sign in experience for users, while still retaining the option to use the device PIN whenever it is required.

The functionality is compatible with a range of FIDO-compliant devices equipped with integrated fingerprint sensors, including the YubiKey Bio Multi-Protocol Edition, YubiKey Bio FIDO Edition, OneSpan DigiPass FX1 Bio, and SafeNet eToken Fusion Bio.

New Device Integrations

MyID now supports Swissbit devices, for organisations who need PKI, passkeys and PACS to manage multiple credentials, on a single device.

- **Swissbit**
  - iShield Key 2 FIDO2
  - iShield Key 2 Pro
  - iShield Key 2 Pro FIPS
  - iShield Key 2 Pro Mifare
- **OneSpan**
  - Digipass FX7
  - Digipass FX1 Bio
- **IDEMIA**
  - ID-One Key Bolt
- **Thales**
  - Safenet eToken Fusion NFC PIV
  - Safenet eToken Fusion BIO

Enhanced Credential Lifecycle Controls

MyID CMS provides robust capabilities for initiating actions based on credential lifecycle events. For example, when a credential is cancelled, the system can enforce immediate or scheduled actions on different certificate types, as well as send notifications to external systems. It also manages the disposal status of cancelled devices to determine whether they can be reused, ensuring their final recorded state is accurate—for instance, confirming whether a device was returned, destroyed, or placed back into inventory for future use.

Cancellation reasons and disposal statuses in MyID can now be specified for each credential profile, delivering clearer context and more

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 CMS

What's New in MyID CMS v12.18

accurate reporting. This enhancement ensures organisations can streamline processes with confidence, using device specific options that support smoother workflows and more reliable operational insights.

This targeted approach prevents incorrect selections during the credential lifecycle, while also delivering measurable improvements to auditing accuracy and overall inventory control.

Improved Role Management

Role Based Access Control is used extensively in credential management, to determine available credentials to end users, access to features such as self-service and management capabilities for CMS Operators, Administrators and API access for systems integration.

The configuration and management of roles has been overhauled, modernizing the feature and introducing a range of new capabilities. This includes:

- A simpler web based configuration user interface for roles
- Ability to control access to advanced API operations
- Additional reporting of role configurations
- Easier assignment of operations to multiple roles

Additional workflows that have been modernised and are now available within the MyID Operator Client include editing and importing groups, certificate authorities, system status report, and device import.

Simplified server communications for DMZ deployments

MyID can now use secure HTTPS and OAuth authentication for communication between web and application servers, replacing the legacy NTLM and Windows COM+ dependencies previously required in split-tier deployments. This updated approach eliminates the need for shared Windows domain accounts, additional firewall ports, and proxy installer packages on web servers.

The result is a simpler, more flexible architecture that supports load-balanced web servers and DMZ configurations, while aligning with contemporary security standards. All inter-server traffic is encrypted end-to-end, improving both security posture and compatibility with modern infrastructure, including cloud and hybrid environments.

Integration Updates

MyID CMS now supports the Idemia MSO 1300 Series fingerprint readers for biometric verification, catering to both operator-led and self-service workflows. These devices can be used across a range of key CMS processes, including Reset Card PIN, PIV Card activation, and user authentication for PIV re-enrollment.

The series comprises two models to suit varying deployment requirements: the MSO 1300 E4, a compact fingerprint reader designed for space-conscious environments, and the MSO 1350 E4, which features an integrated smart card reader for enhanced functionality.

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