intercede

MyiD MFA

What's new in MyID MFA v5

MyID® MFA v5 brings enhanced security, flexibility and ease of integration, making it the simplest way for organisations to protect their applications, data and networks against cyber-attack with phishing-resistant authentication that's easy to deploy, manage and use.

FIDO Passkeys for the enterprise

Passkeys are based on the FIDO standard and enable cryptography-based phishing-resistant authentication. By combining high security with a passwordless user experience Passkeys are revolutionising the consumer authentication experience.

However, it has been difficult for enterprises to gain the benefits Passkey-based authentication brings, as by design they do not enable the level of management and integration enterprises require.

By bringing enterprise managed FIDO passkeys into the MyID MFA product, organisations can now easily FIDO-enable multiple applications and deploy passkeys to end users enhancing security and improving the user experience.

MyID MFA acts as both a FIDO authentication server and a passkey issuance solution. End users authenticate to MyID MFA with their passkey, and by support for standard federated identity protocols, MyID MFA provides authentication services to multiple applications including cloud, on-premise and Windows desktop logon.

There are two type of Passkeys, both of which are supported by MyID MFA, enabling customers to choose the best balance of security and costs that fits their particular needs.

Synchable Passkeys

Synchable Passkeys use an existing mobile phone to protect the private key used in the authentication process. Able to communicate over the FIDO protocol built into multiple devices and web browsers, the phone simply acts as the user's security token and the user accesses the protected private key via fingerprint, face ID or PIN, delivering secure, passwordless authentication with a simple user experience.

Synchable passkeys can be backed up and restored using the mobile operating system's built in mechanisms such as iCloud. This effectively deals with lost or replacements devices without having to reissue credentials.

Device Bound Passkeys

Device Bound Passkeys: for organisations wanting higher levels of security and control over where passkeys are, MyID MFA also support device-bound passkeys such as those stored on a USB authenticator like a YubiKey. Device-bound passkeys never leave the device, resulting in the highest levels of phishing resistance.

MyID MFA supports the innovative YubiKey Bio device, enabling users to replace a PIN with a simple match of a fingerprint, delivering a seamless authentication experience while maintaining the highest level of security.

Federation

Federation brings the ability to share identity and authentication information between systems in a managed way. By supporting standards-based protocols such as OpenID Connect and SAML, MyID MFA can easily add stronger authentication to a range of applications be they cloud based or on-premise.

By supporting the widest range of authentication options from OTP over SMS, through pass phrases, OTP generation via App, push-notifications and FIDP passkeys, organisations can introduce a single means of strong authentication to project multiple applications or mix and match technologies as best fits their security needs and deployment scenario.

Building Identity provider capabilities into the MyID MFA solution, not only supports federation, but also delivers a unified authentication experience across the entire application suite, including authentication to application, logging on to the Windows desktop, accessing the self-service portal and resetting credentials such as passwords. A simplified and consistent authentication process improves the user experience and reduces the likelihood of a call to the help desk.

ADFS replacement

Microsoft ADFS (Active Directory Federation Services) have been the mainstay of many organisations looking to add secure authentication to multiple applications in a Microsoft-centric environment. With the move to Microsoft Entra based solutions a number of organisations are finding themselves looking for an alternative that is simpler to deploy and provides support for both cloud and legacy on-premise applications as well as securing the Windows Desktop logon and Microsoft 365.

The federated identity provider (IDP) capabilities MyID MFA delivers, provide a modern and easy to alternative to ADFS. By supporting a wide range of authenticators, include FIDO passkeys, and standard protocols such as OpenID Connect and SAML, MyID MFA is a natural successor to ADFS.

Bring your own credentials

In addition to acting as an Identity provider, enabling third party applications to easily call into the strong authentication services delivered by MyID MFA, the solution enables federation with existing credentials and identity providers, including OATH compliant Google and Microsoft Authenticator apps. This allows users to use apps they are already familiar with and enables organisations to use credentials that are already deployed, reducing operational costs and speed to deployment.

If an organisation is already using a standards based IDP, them MyID MFA can federate to it, enabling an existing digital identity to be used to access MyID MFA protected application. This capability extends to being able to configure MyID MFA to support national government issued credentials that can then be used to securely access local resources protected by MyID MFA.

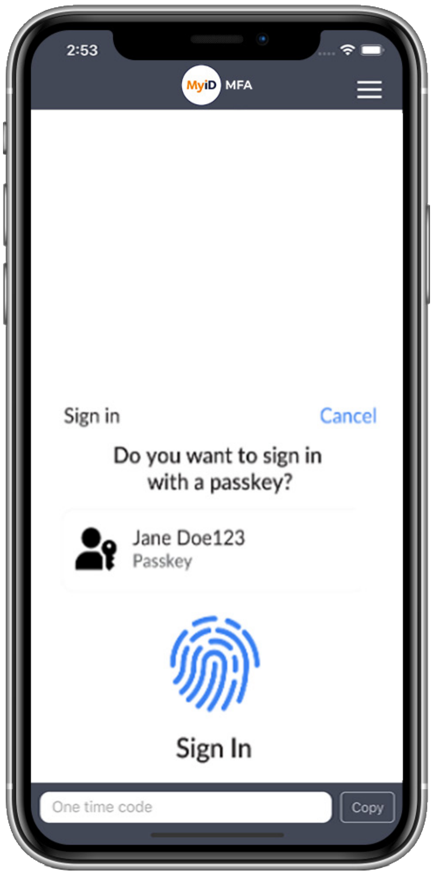
Enhanced Windows Desktop Agent

The MyID MFA Windows Desktop Agent already provides a secure passwordless experience for protecting Windows PCs and network access. With MyID MFA v5, adding support for federation, 3rd party authenticators and FIDO passkeys have all been included, meaning organisations have a wider choice than ever on how to protect the primary gateway to their data, networks and applications regardless of whether they are on Windows 11 or Windows 10 devices.

Authentication with 3rd party apps, external IDPs, a user's own phone with a phishing resistant passkey or a YubiKey device-bound Passkey with a biometrics are now all merely configuration options with the product, ensuring customers can achieve maximum security with minimal deployment effort and cost.

Inclusion in the MyID product family

MyID MFA was previously known as Authlogics MFA. Authlogics are now an Intercede Group company, and the product has been rebranded as part of the MyID family of credential management and strong authentication products. Customers now benefit from increased investment in the product roadmap and an expanded customer support and professional services team.



Do you want to sign in with a passkey?