

Technology, Security and Compliance



What is iTrent Shield MFA?

Using your own Identify Provider (IDP), such as Azure Active Directory (AD), is the best approach for securing access to SaaS solutions like iTrent. If you don't have an IDP, or not all of your employees use an IDP, iTrent Shield MFA can help.

iTrent Shield MFA adds extra, essential security for your users by requiring an additional verification check on login ('two-factor authentication'). As well as a username and password, users must enter a six-digit code sent to their phone to validate who they are. This helps to protect against attacks where a user's password is guessed or obtained through a phishing e-mail.

Integration with Azure AD

iTrent Shield MFA allows your users with an Azure AD account to login to iTrent with their normal corporate username and password, and users without an Azure AD account to login with a standalone iTrent username and password.

How does iTrent Shield MFA work?

The solution is designed to be fully self-service and requires no additional administration. Only one setting needs to be changed on the iTrent user records to enable iTrent Shield MFA. This can be done on a person by person basis or in bulk via a data conversion.

Availability

The Microsoft platform provides 99.9% availability. This is coupled with a cross-region, resilient web service to provide high-availability.

All other user administration is then as normal. Users register themselves via the normal iTrent login page by creating a password and linking their authentication app. Any authenticator app can be used, such as Microsoft Authenticator or Google Authenticator.

Technical architecture

The solution is built on the Microsoft Azure AD B2C platform. Users are redirected to this platform for authentication, and if successful, automatically logged into iTrent. The SAML, which stands for Security Assertion Markup Language, is the protocol used for authentication between this platform and iTrent. The platform has been designed to look identical to iTrent, so the user experience is seamless to a normal iTrent login.

Data protection

Limited personal data is stored in the solution, consisting of first name, last name, IP addresses and password (in an encrypted form). The Azure platform is located in the Azure Europe region. There is no option for UK hosting at present.



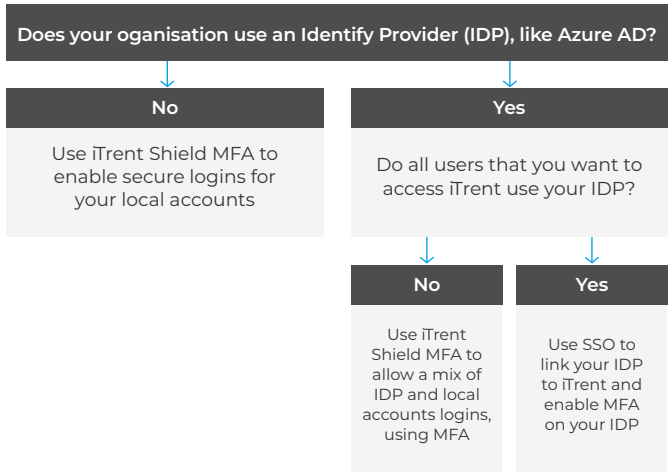
Security

The solution benefits from the high levels of security inherent with using the Azure platform, such as physical security of the Microsoft data centres and patch management processes. Within the platform itself, users are required to create passwords with a minimum length of eight characters and include three of lowercase, uppercase, numbers and symbols.

The solution also benefits from Azure’s Smart Lockout features. This uses many factors to determine when an account should be locked out, including the IP address of the user and the passwords entered.

This secures the platform against credential-based attacks, while reducing unnecessary account lockouts. All communication with the platform over the internet is encrypted.





The solution is manually penetration tested on an annual basis by CREST certified testers.



If you’re interested in this solution, please contact your Customer Relationship Manager for more information.

+44 (0) 115 945 6000
info@mhrglobal.com
mhrglobal.com

You can also keep up to date with all our latest news through our social media channels:

-  twitter.com/mhr_solutions
-  linkedin.com/company/mhr_solutions
-  youtube.com/MHR_solutions
-  facebook.com/MHRsolutions

