




## Case Study – Quorum Network Resources

### Creating a Better User Experience...

Our client who is within the Oil and Gas industry had several third-party Software as a Service (SaaS) applications which were used by the business for core operations...

This provided several challenges around users having separate logins that they were required to remember and many different interfaces making administration of identity time consuming and difficult.

Quorum implemented Azure Active Directory to provide a single directory for managing user Identity and Authentication.



*Azure Active Directory as a single system for identity and authentication created a better and safer user experience.*

## The Challenge

The client had several key line-of-business applications that were used by most of the staff. These were third party Software as a Services (SaaS) based apps such as Office 365, Mimecast and ServiceNow.

As the adoption of Cloud based applications grew within the company, the administrative overhead of managing Identity across each application became an increasing burden. Each application required different accounts and security options making it unnecessarily challenging for employees to manage.

The client wanted to consolidate all of their identification and authentication into one platform and add some additional security which was consistent across applications. The key goals for the client were:

- Have a single login for all applications and a single identity solution to manage;
- Additional security through a single Multi Factor Authentication solution.

## The Solution

Quorum was brought in to perform analysis on the current third-party SaaS applications currently being utilised by the business. The analysis allowed us to confirm that each of the applications being used were suitable to be used with a single Identify provider using SAML (Security Assertion Markup Language) and Oath2 (open standard for access delegation).

The client was already in the process of migrating to Office 365 so the obvious choice was Azure Active Directory as they had the necessary licencing and this would integrate into their current identify and authentication model.

Quorum implemented Azure Active Directory and setup each application to use Azure Active Directory as the central identity provider. In addition, Azure Multi Factor Authentication was setup as an additional level of security. Threat analytics built into the platform allows the client to reduce the risk of costly damage and get all the information they need in a succinct, real-time view.

All applications were available to access through a single portal, creating a more efficient and painless user experience.

## The Results

As a result of implementing Azure Active Directory the client now has a central place to monitor and manage identity and authentication for all line-of-business applications whether on-premises or a Cloud based SaaS application.

Users found it easier only having to remember the credentials of one account across all applications. This resulted in fewer helpdesk calls with forgotten passwords or account lockout issues.

Having a single identity solution also enables the business to report on usage and take advantage of the threat analysis and protection built into the platform. This allows the client to analyse and identify normal and suspicious user or device behaviour.