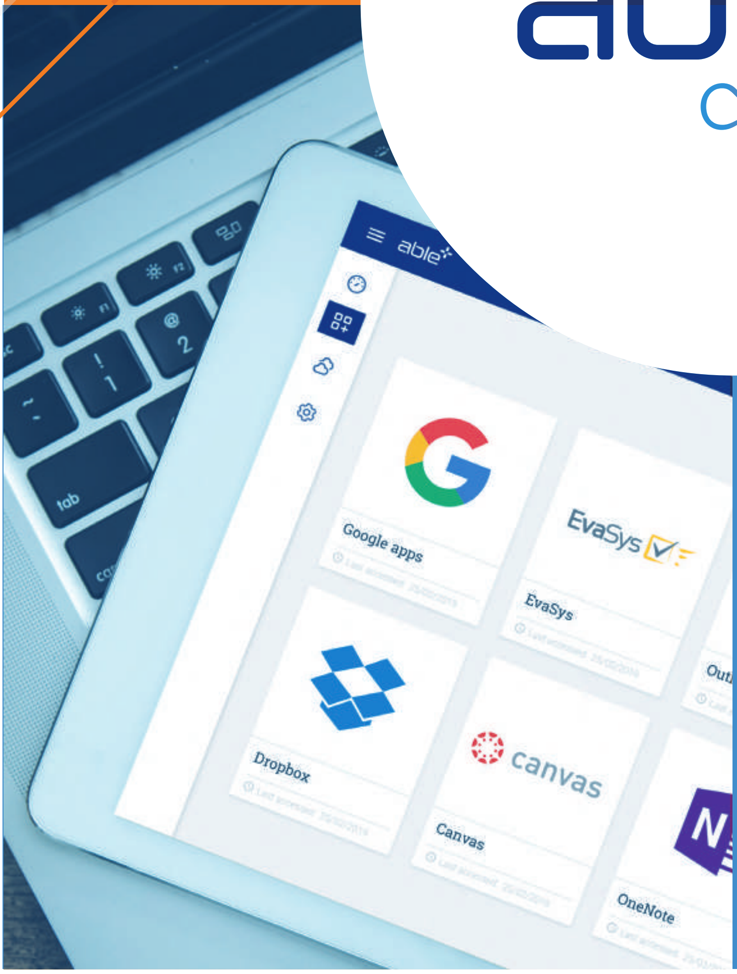
An introduction to
Able+ Cloud

new era.
TECHNOLOGY

able+
Cloud



Identity and Access
Management Solutions

new era TECHNOLOGY

About Us

New Era Technology specialises in developing and delivering business infrastructure SaaS platforms and solutions for organisations; primarily Access and Identity Management (IDaaS, IAM, IDAM).

As a Group, the Company employs over 800 staff, with an approximate turnover of £250m+; we offer highly innovative technological solutions that have positioned us as a global market leader in the educational software industry, with over 20 years' experience supporting complex projects in the UK, US, China, Australia and New Zealand. Our customer engagements and relationships are all long-standing and long-term.

IAM

Collaboration

Managed Services

Security

Cloud Solutions

Data Networking

The UK operation, based in Reading and Brighton, holds the sole responsibility, IP, development and support for the Group's software solutions including Able+ Cloud, our Identity and Access Management solution.

To remain at the forefront, current and competitive, innovation lies at the heart of our business strategy and the level of innovation is continuously contributing to the evolution of the digital ecosystem by providing efficient, agile process automation and security to the Identity Lifecycle.

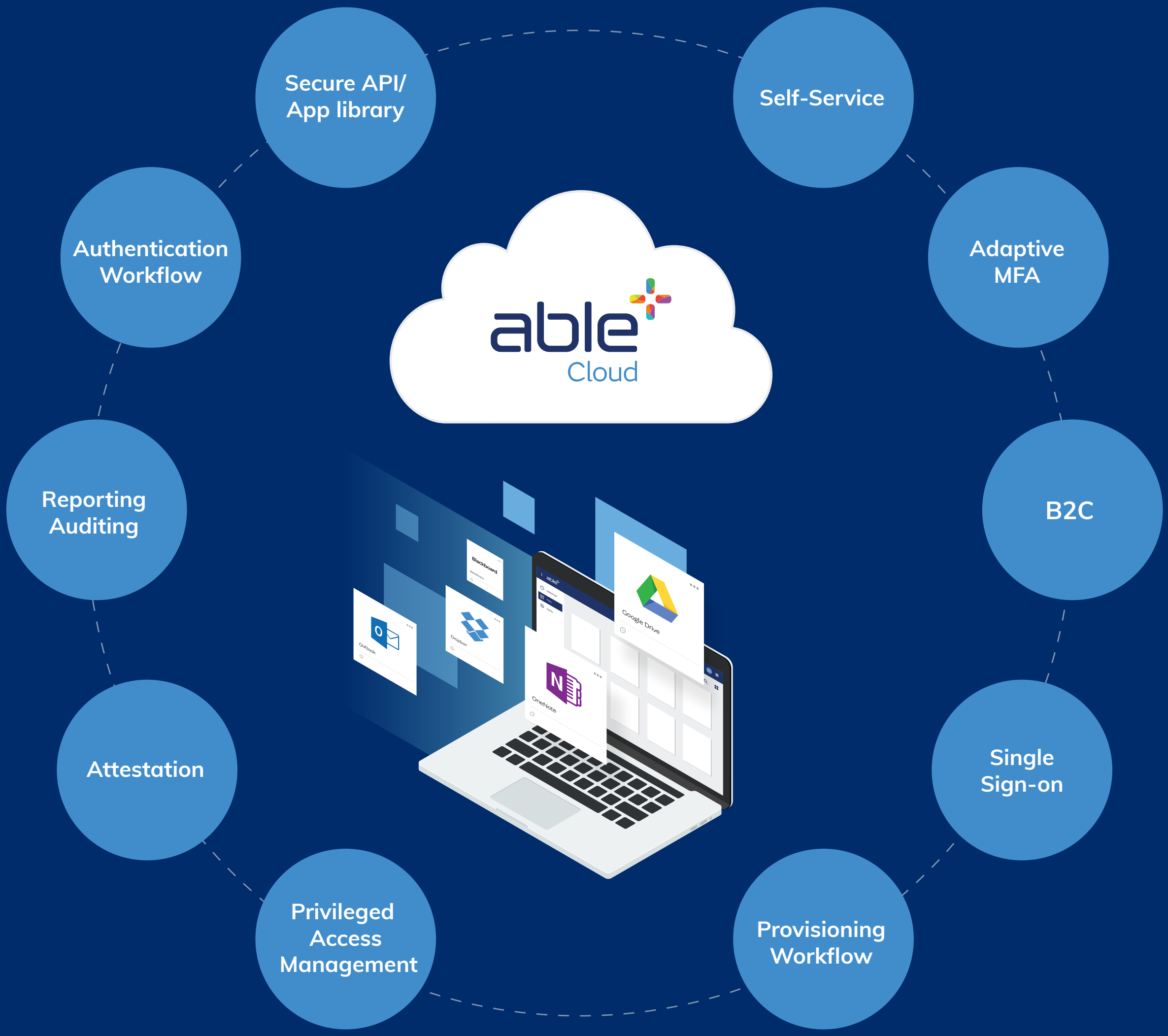
Further Information

Able+ Identity & Access Management and Education Division: **www.neweratech.co.uk**
Our Group: **www.neweratech.com**

An overview of the Able+ Cloud solution

Able+ is a highly advanced identity and access management solution (IAM) designed to support the complex and changing needs of modern user identities and multiple data source integration requirements in organisations.

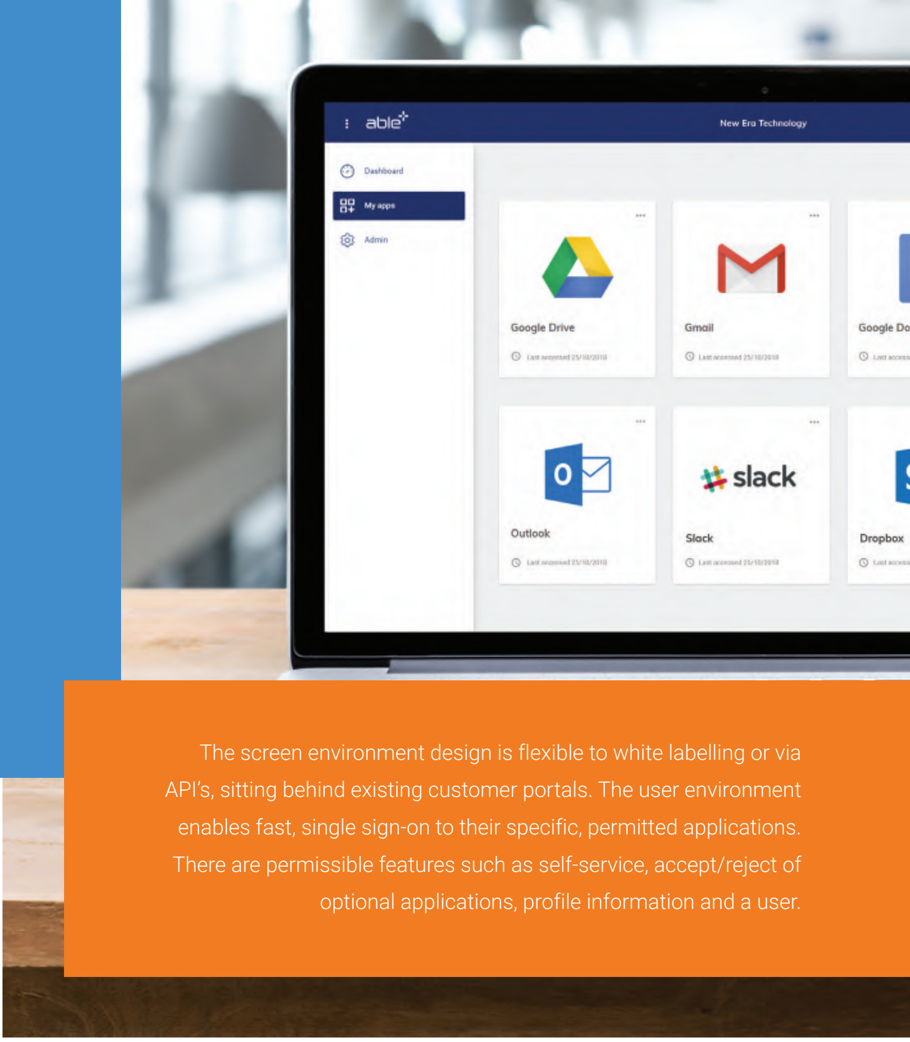
Any elements, services, functions of Able+ may be utilised where required to support a legacy or part IAM system or process. Able+ is designed to operate on the latest and evolving cloud providers' infrastructure; maximising advantage of the performance, compute, security and compliance standards and available services. All our services run on the latest version of the infrastructure and are monitored live 24/7 to guarantee the SLAs required and the security of the data and Able+ processes.



Able+ has been designed to incorporate the latest in modern identity concepts, whilst being able to cater for legacy systems and complex user requirements.

IAM solutions need to be flexible, responsive and cost-effective, whilst striking the right balance between agility and control.

Originally designed to handle the multi-location; multi-role changing complexities of the education market, Able+ was conceived with these capabilities at its core.



The screen environment design is flexible to white labelling or via API's, sitting behind existing customer portals. The user environment enables fast, single sign-on to their specific, permitted applications. There are permissible features such as self-service, accept/reject of optional applications, profile information and a user.

User Experience

Able+ has been designed with an intuitive end user experience as a priority. Hover-overs and additional information is displayed when required to enable all common tasks to be undertaken by a non-technical user requiring zero to minimal additional support. The same principle applies to managing the Able+ solution where workflows and actions, platform settings are for administrative level without the requirement for IT technical intervention.

Scalability and availability

As a SaaS solution designed to run on the latest cloud providers' infrastructure (such as Microsoft Azure or Amazon Web Services), Able+ can be scaled up or down to meet the demands of an organisation. This enables the solution to run at an optimal level for an organisation's specific needs, but also provides the on-demand changes to adapt to situations where the capacity fluctuates, for example due to seasonal, operational or unforeseen events and activities.

The SaaS delivery model includes service level agreements that guarantee the level of availability of the solution (typically 99.9%).

Underlying security & compliance

Able+ and our customers leverage the security strengths and development of its hosting providers, Microsoft and AWS. Data is hosted in the UK and/or Europe as specified by our customer. Data is encrypted at rest and password values are hashed. They are not released to any third-party; the federated identity is matched and monitored in session, real-time.

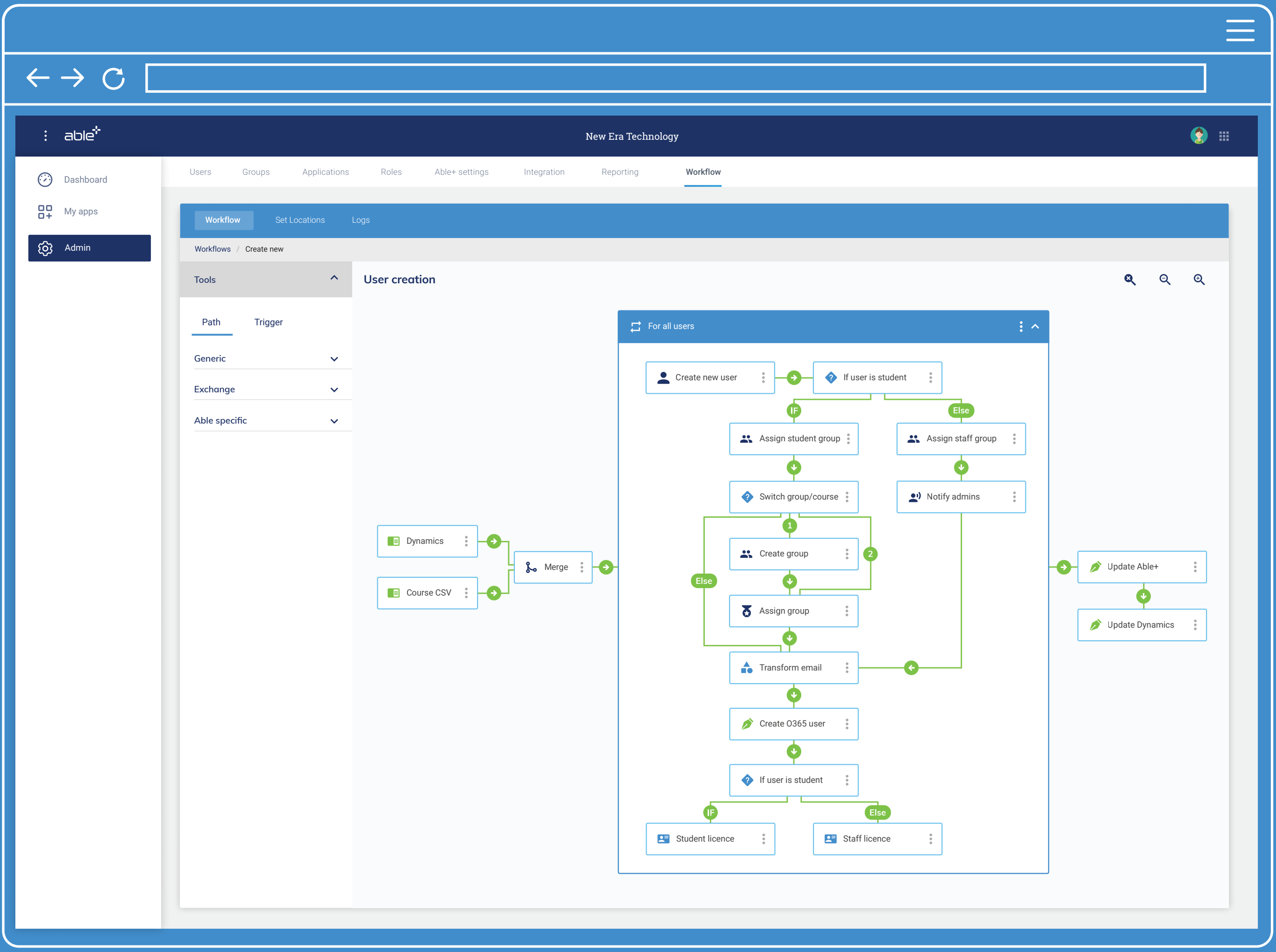
The data is/remains the property of our customer. Access and retrieval processes are agreed and organised as part of the project programme.

New Era and Able+ complies with all GDPR and other data legislation. Able+ is subject to regular penetration testing and other security evaluation as part of development and on-going security assessments.

Able+ delivers compliance adherence by mapping and reporting on the execution of security and compliance policies. Approvals are tracked when rights are modified, providing a clear trail for monitoring, reporting and auditing purposes.

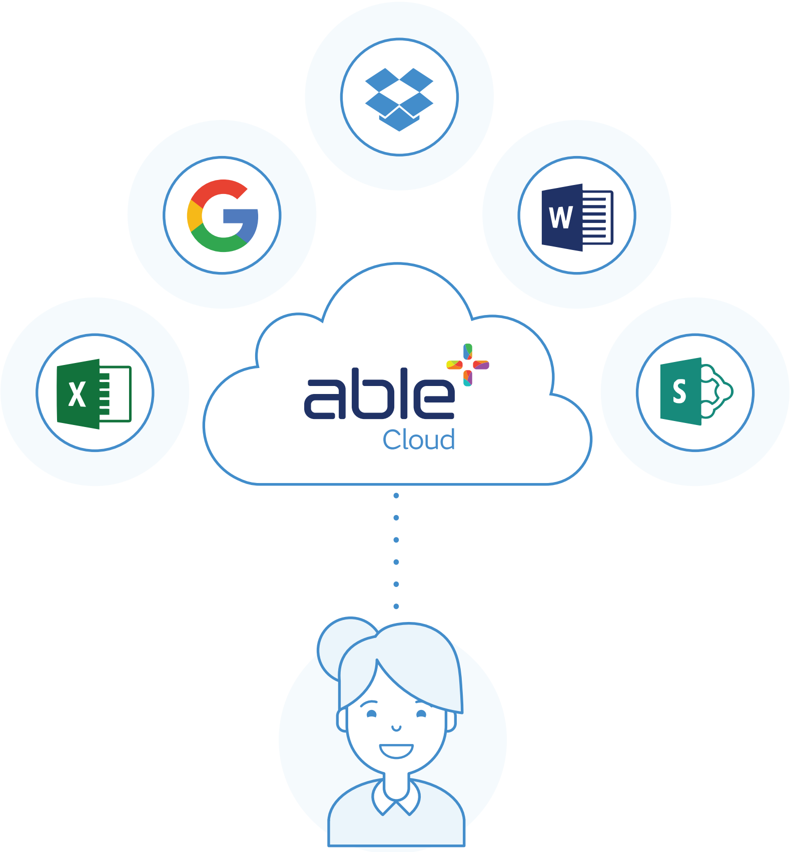
Configuration – Automating processes with consistent policies & procedures through Workflows

A key pillar of the Able+ solution approach is that the it will adapt to the way an organisation wants to work rather than an organisation needing to change their business processes to adapt to an inflexible product or technical methodology.
To this end, the solution is built on configurable micro-services that are defined by easy to select options to suit each customer. One of the most innovative features of this lies in the Able+ workflows module, used to create and configure workflows via an intuitive user interface. This minimises the need for any additional development required to fulfil a customer's unique requirements. The workflow management is placed at the administrative level so does not require any technical knowledge or certificated, complex training. We believe this is one of our unique differentiators in the IAM space. Multiple 'providers' can be included within a single workflow (both to read data and be written to) so the workflows can be completely customised to adapt to an organisation's external systems. The relevant workflows can be configured both to run automatically and/or to be triggered manually.



Application management – Single Sign-On and API Security

Able+ Cloud provides a simple to manage application access with one single identity. Using the MDX engine, Able+ can bring together identities from Management Information Systems (MIS), AD's and Apps into one single identity. This ensures users only need to enter their credentials once, to access all their apps.



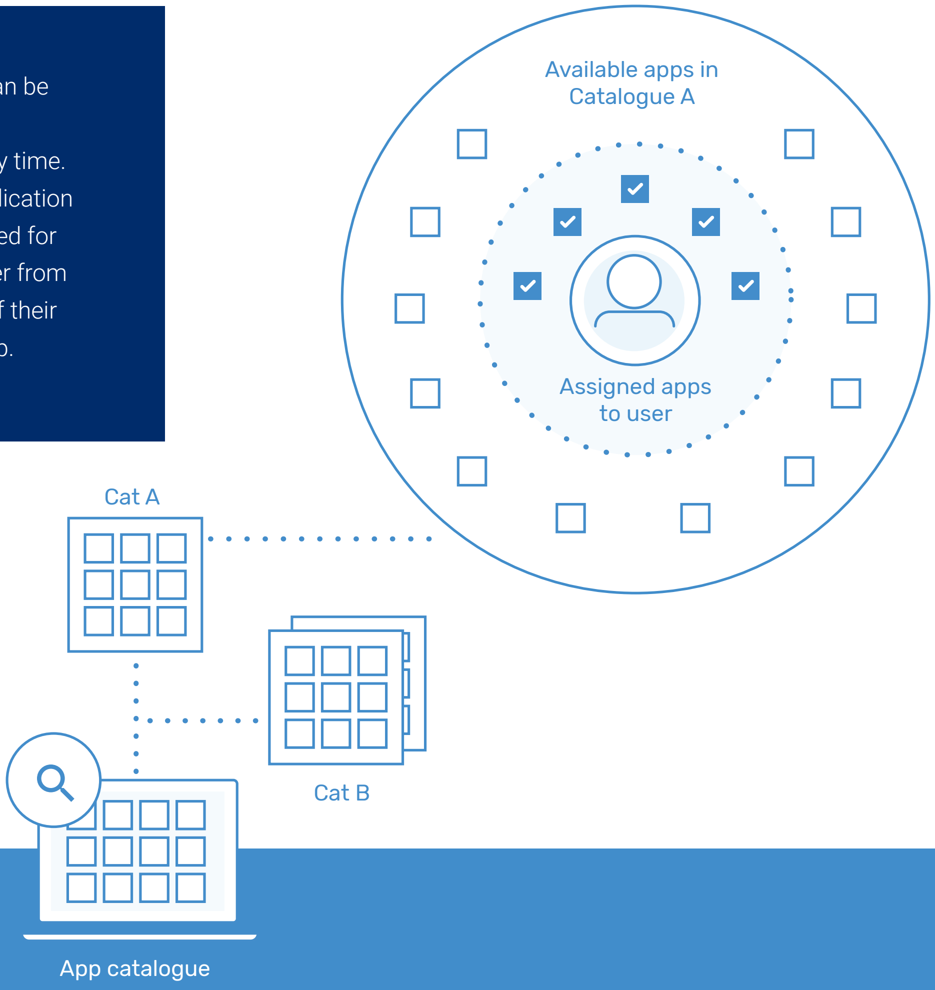
Serving either as the identity provider (IDP), or IDP manager (where other directory or directories remain in operation), users provisioned into Able+ are authorised and authenticated through SAML protocols and OAuth workflows enabling access to federated service providers.

Able+ supports on premises, hybrid and cloud applications and as a technology neutral developer, we effectively manage API integration irrespective of vendor or environment.

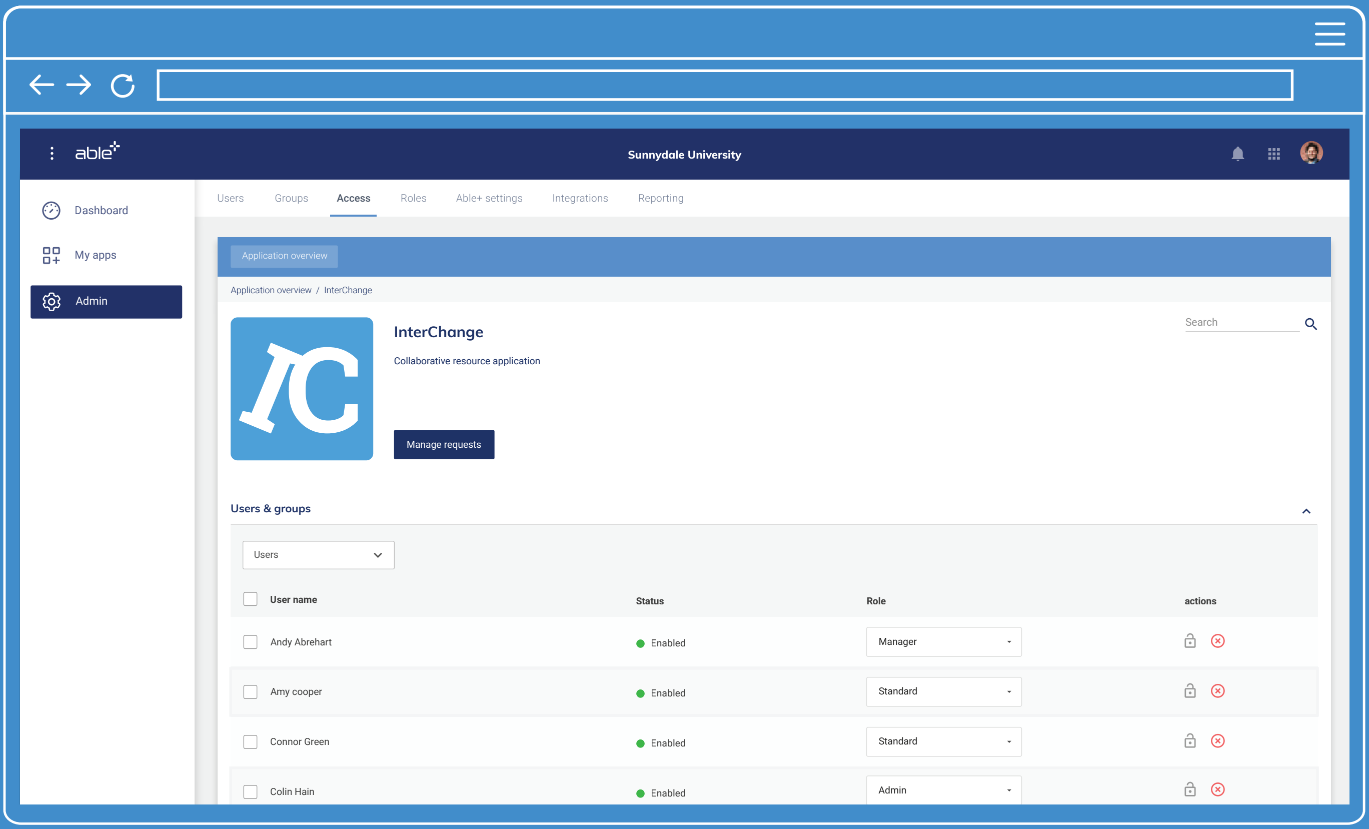
Application access

Application access is managed through the Able+ intuitive user interface. Access to applications can be granted to users, groups and/or roles and can be viewed and managed with either an application focus or a users'/group/role focus. Applications can be enabled (by which immediate access is given) or made available (whereby the applications can be added by users from the app catalogue).

Access to applications can be removed from users/groups/roles at any time. Where necessary, an application can be completely disabled for a user, preventing the user from accessing it regardless of their role or group membership.



The Single Sign-On capability provides secure application access and grants relevant access with the ability to control and manage license allocation. This is a crucial process in the efficient on/off boarding of employees, contractors, partners and visitors for example.



Application overview / InterChange

InterChange

Collaborative resource application

Users & groups

Users

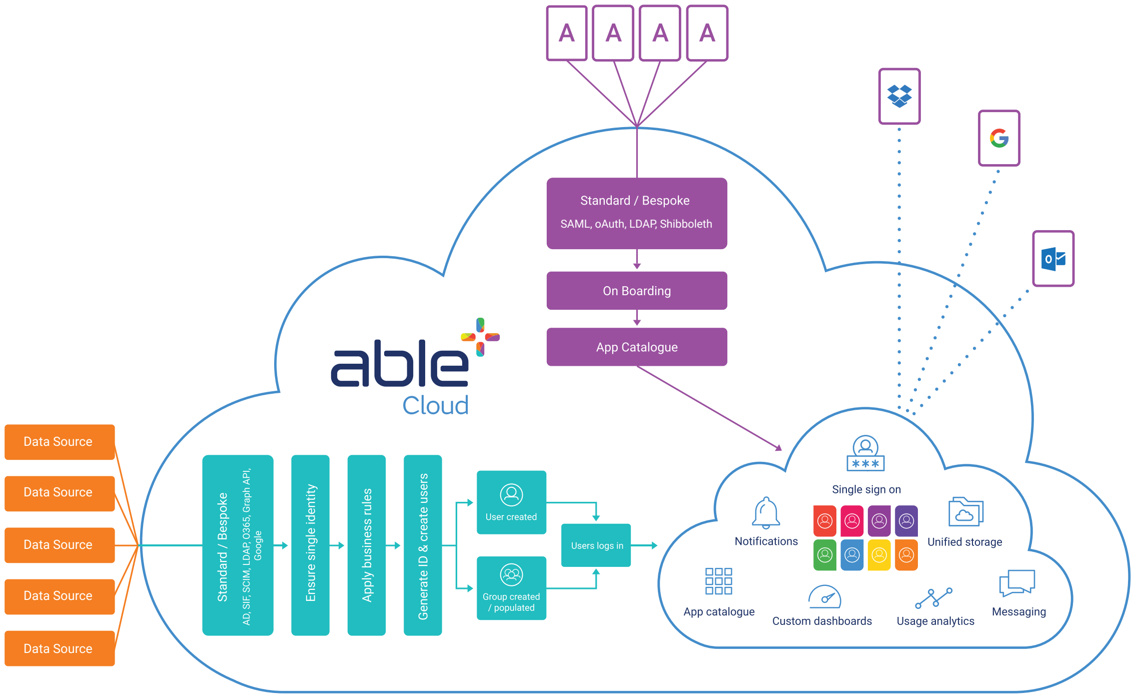
□ User name	Status	Role	actions
□ Andy Abrehart	● Enabled	Manager	
□ Amy cooper	● Enabled	Standard	
□ Connor Green	● Enabled	Standard	
□ Colin Hain	● Enabled	Admin	

Able+ Multi-data exchange (MDX)

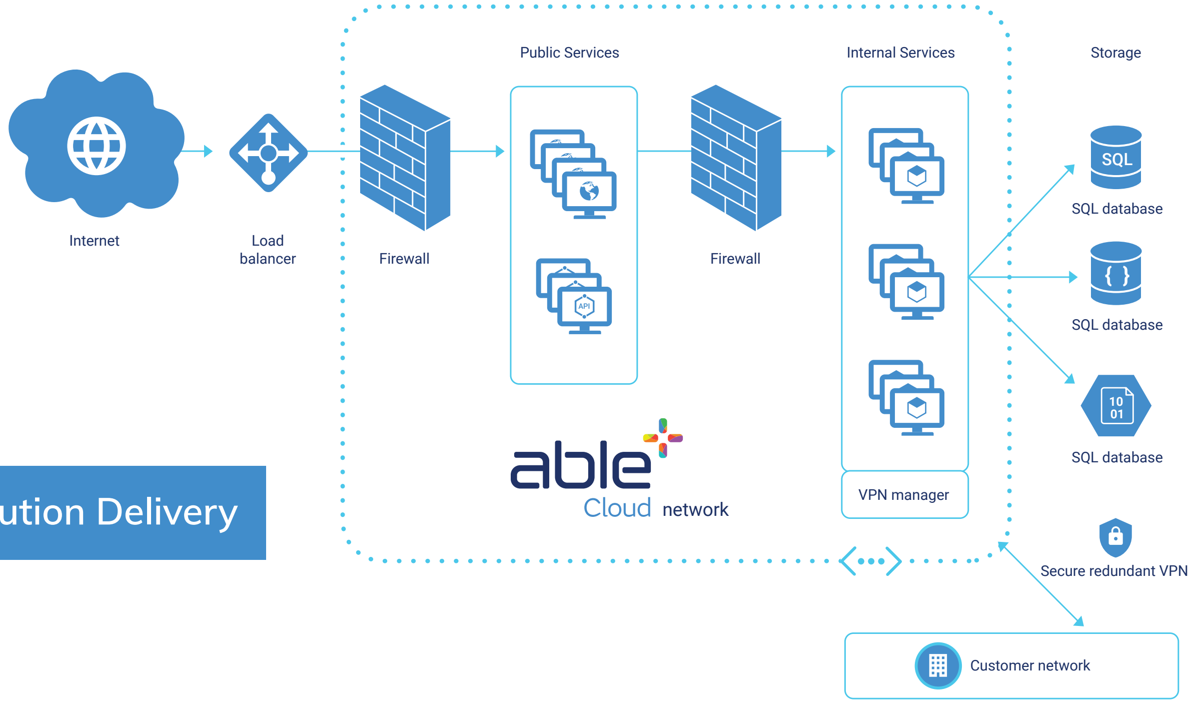
The MDX engine is the data processing engine within the Able+ platform. It manages data complexity and business rules as well as providing a single identity and unique user record. Able+ enables the synchronisation of users and groups with multiple directories, such as Active Directory, LDAP, GSuite and Office 365. Data is managed from multiple sources, then synchronised real-time or at your chosen frequency.

The MDX can be configured to call/send and process information from bespoke and/or legacy systems where required. This is particularly useful for organisations looking to run parallel systems as they migrate to the latest technologies.

The MDX can operate as the source of truth or mediate between multiple data systems.



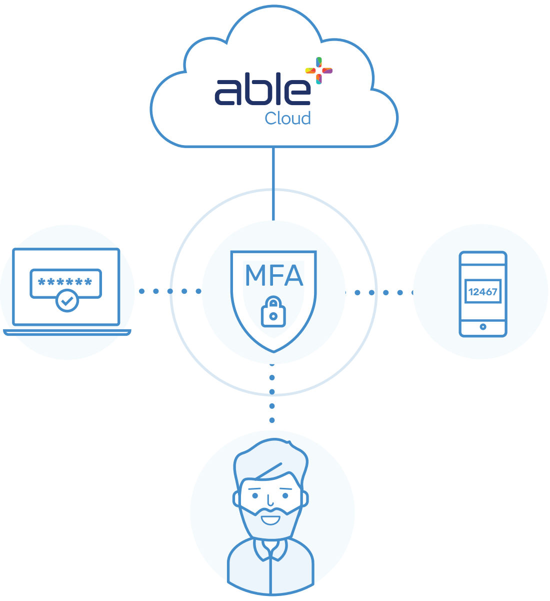
Solution Delivery

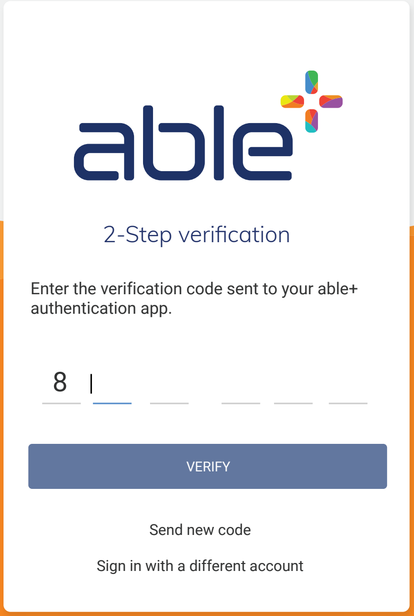


Adaptive Multi Factor Authentication

In many situations, additional levels of authentication are required – either to control access completely or to make certain applications, resources or actions more secure.

Able+ can provide blanket, location specific or time specific calls for additional authentication for all users, or users with certain roles (including as part of role-based access control).





able+

2-Step verification

Enter the verification code sent to your able+ authentication app.

8

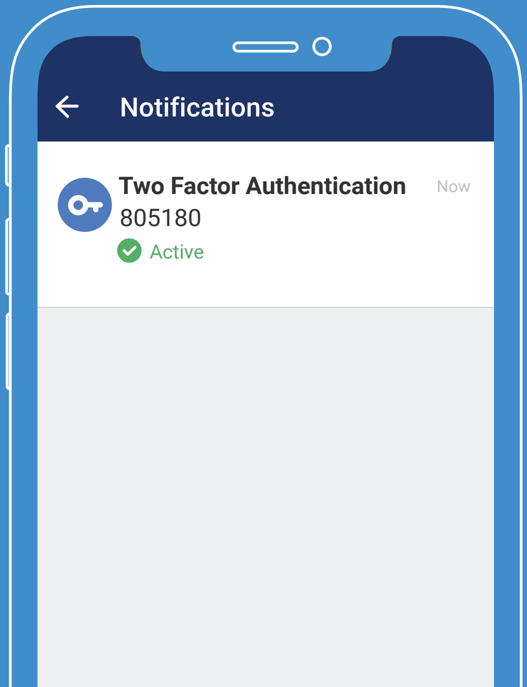
VERIFY

Send new code

Sign in with a different account

Where this level of restriction is not required (or indeed as a further level to initial authentication restrictions), additional authentication can be requested to control access to specific applications and/or resources. Users with administrative privileges can be required to perform further authentication when performing specified actions. Again, these restrictions can be applied in all cases or be dependent on location and/or time.

In addition to authentication via username/password, one-time codes sent via SMS or to an authorisation app are supported as standard. Other authentication methods can be implemented upon request.

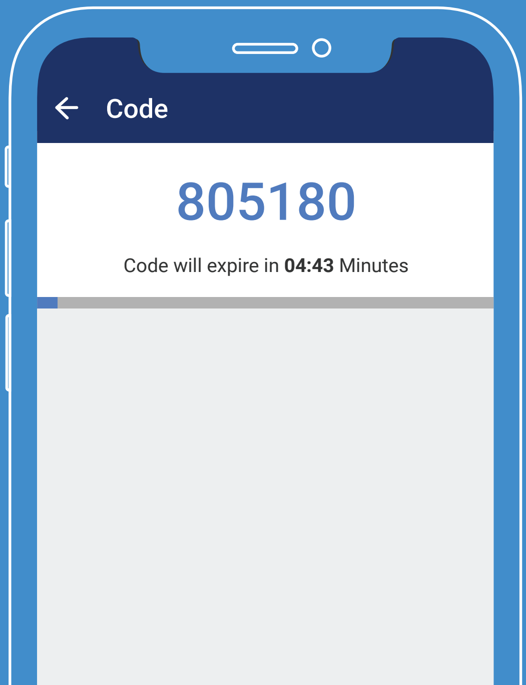


Notifications

Two Factor Authentication Now

805180

Active



Code

805180

Code will expire in **04:43** Minutes

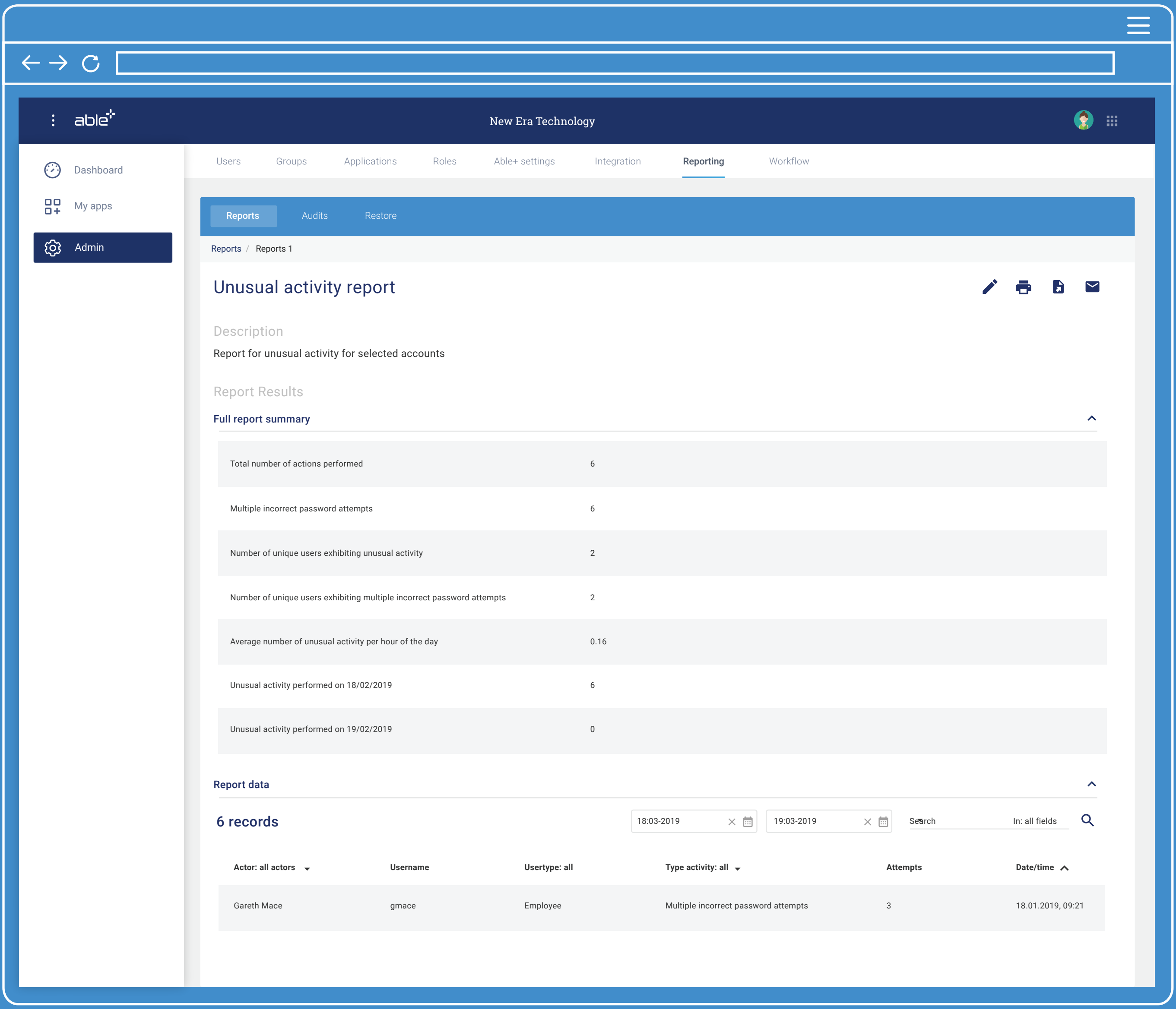
Unusual activity

Activity deemed 'unusual' is configured on a per-organisation basis.
Unusual activity reporting is available as standard and workflows can be created to manage system responses to such activity; this can include a variety of responses such as suspension of accounts, alerting of specified persons and requests for additional authentication.

Able+ defines 'unusual activity' at an organisation level in areas including a combination of one or more of the following: number of incorrect attempts at credential entry; privileged access; time of day of activity; location (geolocation or IP address) of activity – both on a whitelist/blacklist basis and on a change of usual behaviour basis; unfamiliar device.

Where activity is found that corresponds to unusual activity as defined by the organisation, then a workflow will be triggered. The workflow(s) can include reporting, blocking of access, approval process and additional authentication.
Different workflows can be triggered depending on the type of user or the nature of the unusual activity.

Reports of unusual activity can be generated and distributed to the appropriate individuals both as the activity registers on the system and according to a defined schedule.



Unusual activity report

Description

Report for unusual activity for selected accounts

Report Results

Full report summary

Total number of actions performed	6
Multiple incorrect password attempts	6
Number of unique users exhibiting unusual activity	2
Number of unique users exhibiting multiple incorrect password attempts	2
Average number of unusual activity per hour of the day	0.16
Unusual activity performed on 18/02/2019	6
Unusual activity performed on 19/02/2019	0

Report data

6 records

18:03-2019 19:03-2019 Search In: all fields

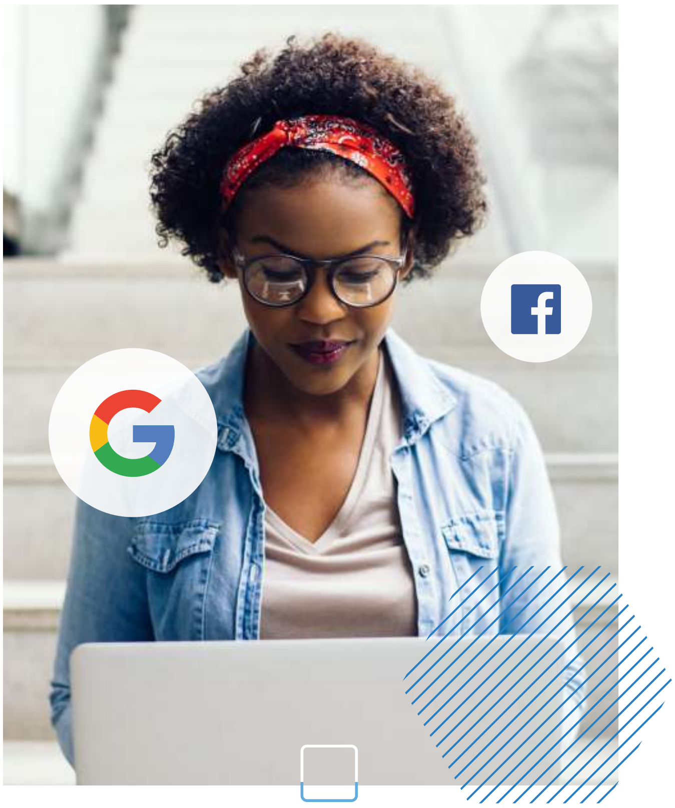
Actor: all actors	Username	Usertype: all	Type activity: all	Attempts	Date/time
Gareth Mace	gmace	Employee	Multiple incorrect password attempts	3	18.01.2019, 09:21

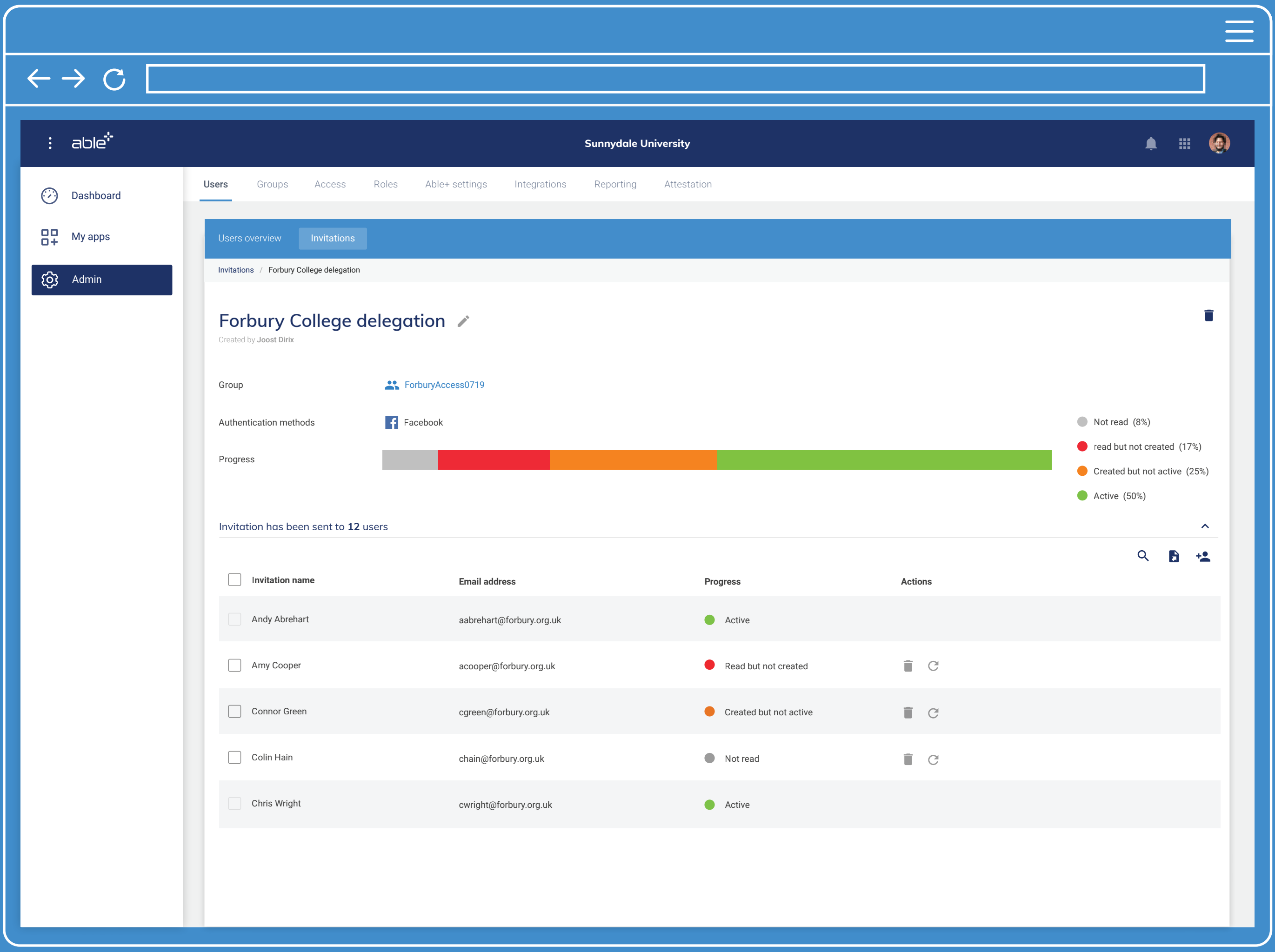
Business-to-Customer/Business authentication (B2x)

Able+ supports a range of B2x authentication scenarios. Where desired, organisations can allow their users to authenticate via third parties such as Google, Facebook and LinkedIn. The exact third parties available are controlled at an organisation level to ensure compliance with individual customers' policies.

Where an organisation wishes to grant access to their system by external users without creating 'standard' internal accounts for them, email invitations and portal links can be created to allow those users to 'sign up' to create accounts via the allowed third-party authentication methods.

Access to resources and/or applications is controlled for users authenticated and/or created by these methods in the same way as standard users. All activity by such accounts is tracked and audited in a similar way to activities performed other users of the system.





Invitations / Forbury College delegation

Forbury College delegation

Created by **Joost Dirix**

Group	ForburyAccess0719
Authentication methods	Facebook
Progress	

- ● Not read (8%)
- ● read but not created (17%)
- ● Created but not active (25%)
- ● Active (50%)

Invitation has been sent to **12** users

□ Invitation name	Email address	Progress	Actions
□ Andy Abrehart	aabrehart@forbury.org.uk	● Active	
□ Amy Cooper	acooper@forbury.org.uk	● Read but not created	
□ Connor Green	cgreen@forbury.org.uk	● Created but not active	
□ Colin Hain	chain@forbury.org.uk	● Not read	
□ Chris Wright	cwright@forbury.org.uk	● Active	

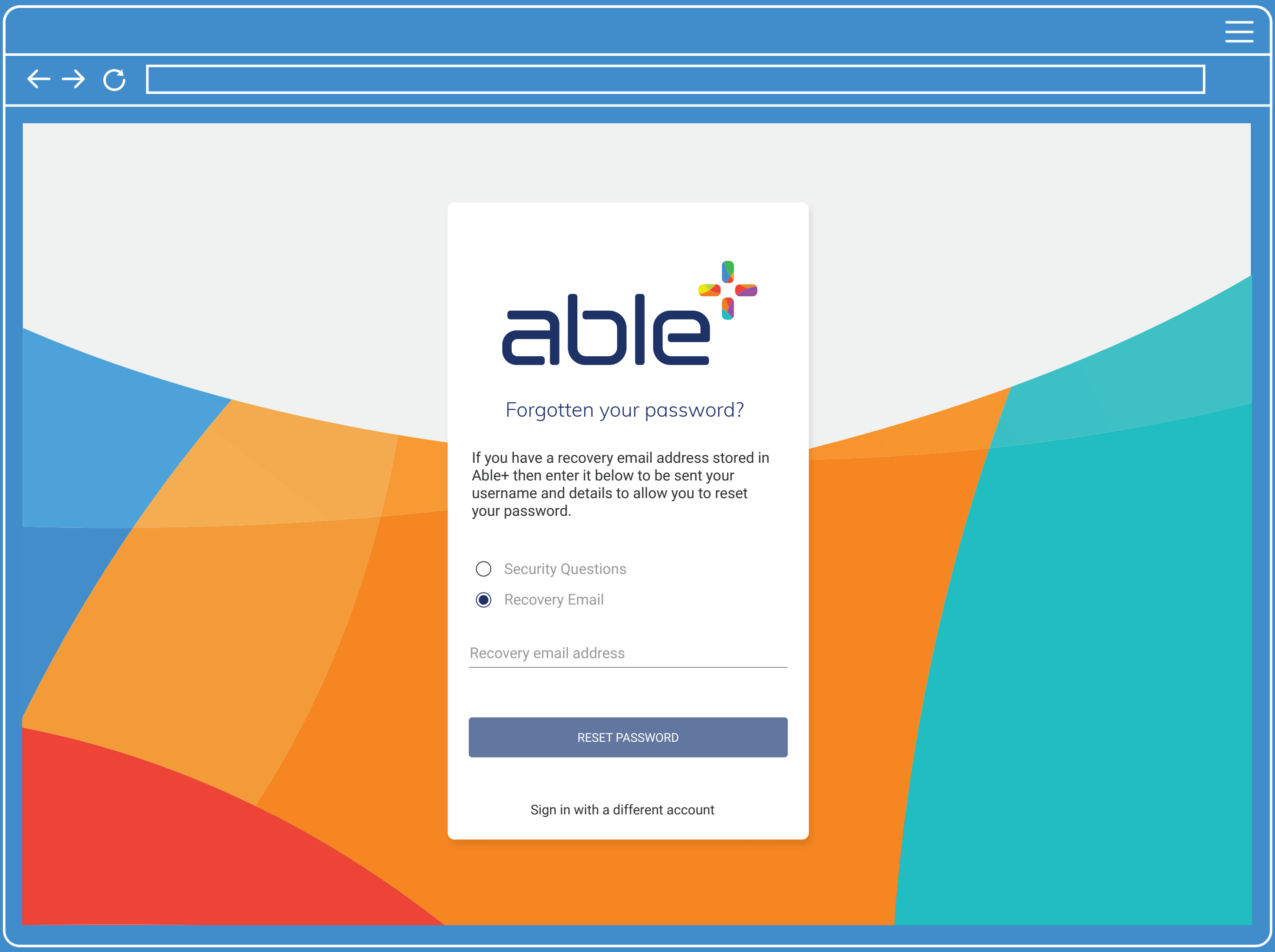
Self-service facilities

Forgetting passwords and log-in details is a common experience and a cliché yet still frustrates user experience and impacts productivity. Rectification requires high support levels, usually technical specialists, so the associated cost and time implications are high. Business systems have typically lagged user-friendly and efficient password reset functions available by the majority of on-line B2C retails service providers. Further pressure on legacy processes and systems has been applied by cloud migration and cloud adoption adding to log-in requirements across multiple environments.

Able+ offers a range of latest options, applied to individual, role, or group that can engage security questions, SMS, requirement to generate longer, higher-entropy passwords to enable your community to reset their password and gain secure, rapid access according to your security policies. Productivity and user experience are heightened with significant decreases of support activity to no technical involvement.

Where required, Able+ can be configured to enable users to manage their own accounts. Password resets, requests to access applications and/or resource and group membership requests can all be actioned by individual users. Depending on the user and/or request, these can be fulfilled by the system immediately or only after approval.

Available self-service facilities and approval workflows are configured to meet each specific organisation's needs.



Forgotten your password?

If you have a recovery email address stored in Able+ then enter it below to be sent your username and details to allow you to reset your password.

○ Security Questions

● Recovery Email

Recovery email address

Attestation

The Able+ attestation functionality will manage the workflow of recertification by both resource owners and line managers to remove identities from roles, remove roles from access and role removal.

Where a user has been given permission to perform edits on the information presented to them as part of the attestation process, then they will see action buttons next to the relevant information. Where relevant, it will be possible to make changes to the information both individually and in bulk.

A reason for making the change can be required from the user.

All certifications are audited and can be viewed per attestation workflow, interrogated across multiple workflows and exported for additional analysis.

The schedule by which archiving of records is managed and whether deletion is required, is set for each organisation. Archiving can also be carried out manually by a user with the relevant permissions.

Removal of access groups

The Able+ attestation functionality will manage the workflow of recertification by both resource owners and line managers to remove identities from roles, remove roles from access and role removal.

Where a user has been given permission to perform edits on the information presented to them as part of the attestation process, then they will see action buttons next to the relevant information. Where relevant, it will be possible to make changes to the information both individually and in bulk.

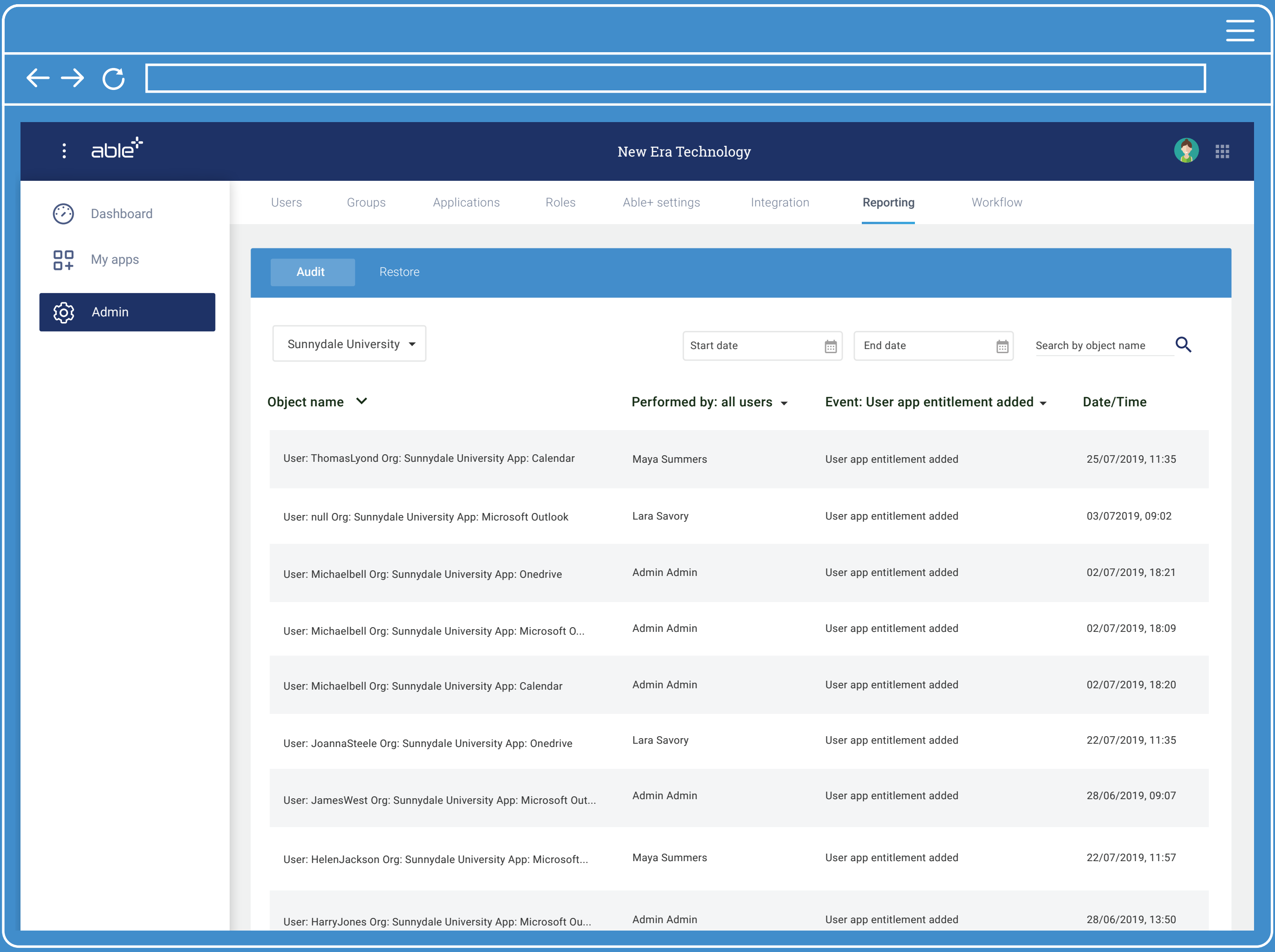
A reason for making the change can be required from the user.

All certifications are audited and can be viewed per attestation workflow, interrogated across multiple workflows and exported for additional analysis.

The schedule by which archiving of records is managed and whether deletion is required, is set for each organisation. Archiving can also be carried out manually by a user with the relevant permissions.

Auditing and Reporting

All events within Able+ are logged for auditing purposes. The audit logs can be interrogated dynamically with a focus on user/group, event or time. Reports can be generated (and distributed where required) to meet the customer's needs.
Able+ offers the option to interrogate all the audit actions of the platform through REST oData endpoints. All the events that involve identities (e.g. data exchange, workflow executions, attribute changes) are audited within the platform and this information is accessible both within the platform and /or through the APIs.



Object name	Performed by: all users	Event: User app entitlement added	Date/Time
User: ThomasLyond Org: Sunnydale University App: Calendar	Maya Summers	User app entitlement added	25/07/2019, 11:35
User: null Org: Sunnydale University App: Microsoft Outlook	Lara Savory	User app entitlement added	03/072019, 09:02
User: Michaelbell Org: Sunnydale University App: Onedrive	Admin Admin	User app entitlement added	02/07/2019, 18:21
User: Michaelbell Org: Sunnydale University App: Microsoft O...	Admin Admin	User app entitlement added	02/07/2019, 18:09
User: Michaelbell Org: Sunnydale University App: Calendar	Admin Admin	User app entitlement added	02/07/2019, 18:20
User: JoannaSteele Org: Sunnydale University App: Onedrive	Lara Savory	User app entitlement added	22/07/2019, 11:35
User: JamesWest Org: Sunnydale University App: Microsoft Out...	Admin Admin	User app entitlement added	28/06/2019, 09:07
User: HelenJackson Org: Sunnydale University App: Microsoft...	Maya Summers	User app entitlement added	22/07/2019, 11:57
User: HarryJones Org: Sunnydale University App: Microsoft Ou...	Admin Admin	User app entitlement added	28/06/2019, 13:50

Privileged access management (PAM)

Able+ supports just-in-time privileged access management to ensure the security of sensitive administrative actions both within the system and – where required – in third party systems. Privileged access management can also be used to restrict access to sensitive resources in third party systems. All privileged access activity is audited and reported on as required by the organisation.

Summary of why organisations choose to deploy Able+ Cloud

Cost control/ROI

- Reduce administration, technical and support costs
- Reduce license costs through efficient applications management
- Reduce costs by replacing legacy IAM systems and/or components
- Fixed pricing allows for flexible user numbers avoiding bill shock
- No additional costs for added users or role type: organisational license, not cost per user: fair usage
- Reduce costs of security breaches, risk and damages
- Reduce compliance reporting and audit costs
- No 3rd party, partner engagement with added service costs or need to buy add-on services or systems

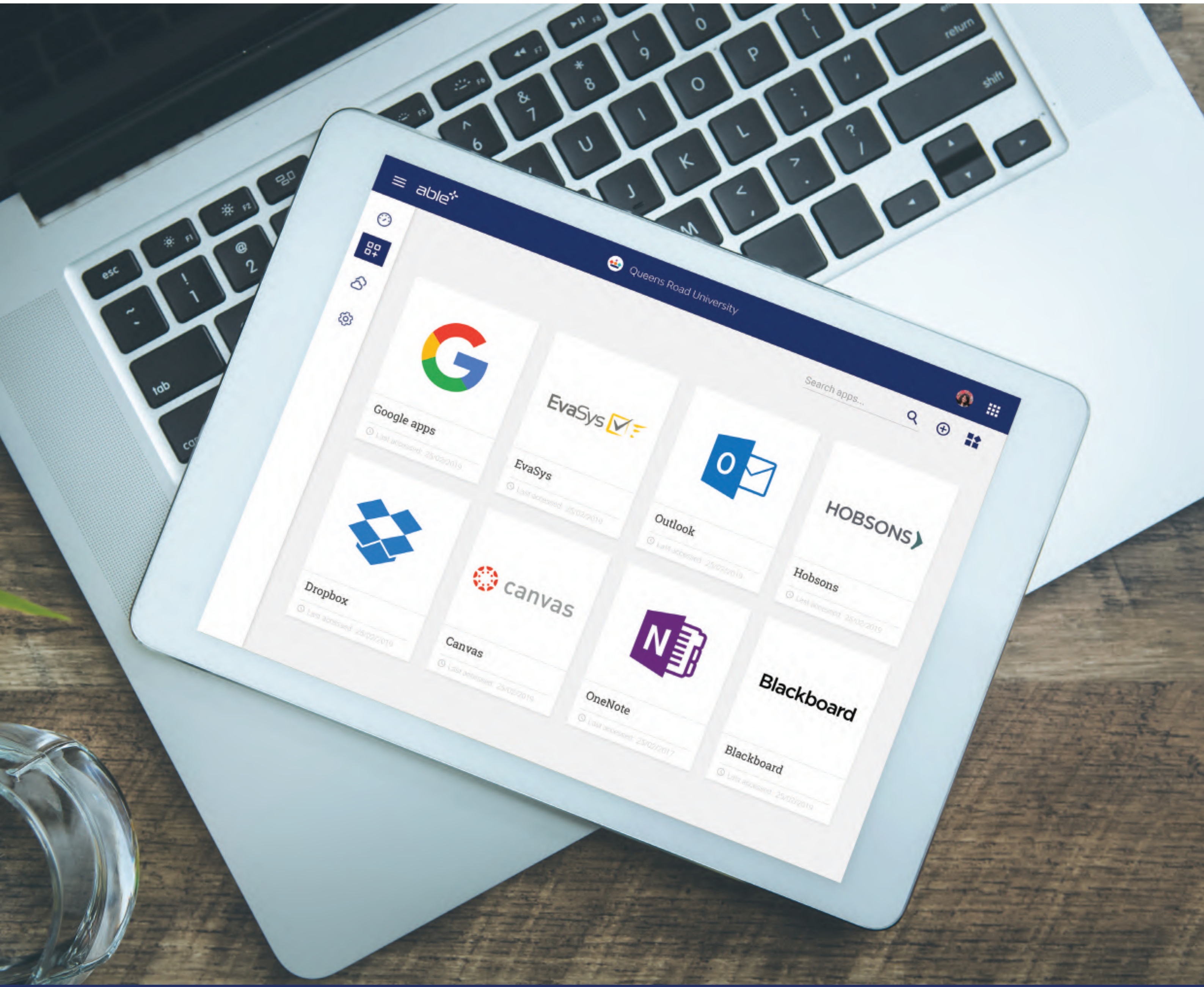
Operational

- Automated, reduced on-boarding/off-boarding processing times
- Federated identity management – enhanced security with SFA, MFA, PAM
- On prem/hybrid and SaaS environments: vendor and technology neutral
- Granular role management to fit the organisational/role structures and policies
- B2C - visitor, guest management with specific limited app access and time controls
- Reduced helpdesk and related log-in calls and queries; self-service password facility
- Faster log-in and access to apps, automated password management
- User ease of use and access to apps and content
- Increased user productivity
- Increased user, administration, management and technical team satisfaction
- Efficient license allocation and management
- Automation of manual processes
- Effective management by exception
- Direct solution developer relationship, no 3rd party complexity, opaque accountability

Functionality

- SAML/SAML2/Shibboleth/oAuth/Bespoke requirements
- CSV
- SaaS always on service
- On premises, hybrid, cloud integration
- High security level Identity management and authentication
- Adaptive AI Multi-Factor Authentication
- Privileged Access Management
- Single Sign-On (SSO)
- B2C services
- Password self-service reset
- Consolidate and manage app and content access
- Deploy to reduce sign-on systems
- Migrate existing legacy in-house related components: as the identity provider (IDP) or IDP manager (where other directory or directories remain in operation)
- Source of truth or effective source of truth mediation and management
- API Security
- Administrator centric management and workflow creation and management

able Cloud



For more information on all our products and services please get in touch or visit our website

01273 201 700
info@neweratech.co.uk • neweratech.co.uk

new era. TECHNOLOGY