Automate & Transform Processes

Information Bundle

Identity Experts

www.identityexperts.co.uk
info@identityexperts.co.uk

Joiners Movers Leavers (JML)

Identity Experts

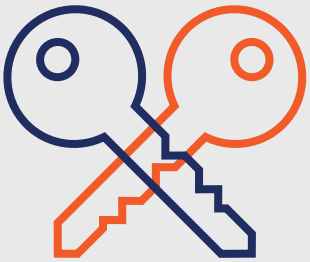
As people move throughout an organisation – as new hires, former employees and recipients of a promotion – their access must be made adjusted appropriately.

Slicker Onboarding

Employees can hit the ground running with autonomous processes managing the setup of new joiners within the organisation.

Efficient Termination of Rights

When a working relationship ends, ensure sensitive data is secure by automatically revoking access rights on a leaver's last day.



No More Permission-Amassing

Automatically change permissions to match an employee's changing job role as they move throughout the organisation, safeguarding confidential information in the process.

Self-Service

Gift users with the autonomy to manage their passwords and request access, freeing up the IT department to spend their time on more cost-sensitive tasks.

Reporting

Understand who has access to data, and who has accessed it in the past, for a top-down view of the organisation's security.

Recover Costs

Are all your user licences accounted for? With former employees still active, organisations can rack up huge costs in unused licences.

Access Reviews

Administrators can maintain confidence in the new Joiners-Movers-Leavers process with regular prompts to review permissions.

Did You Know?

Former employees retaining access to sensitive information opens organisations up to scrutiny under GDPR if personal data is available.

PRESTON'S COLLEGE

"It's vital that when learners start their courses with us, we can give them immediate access to the resources they need to study and succeed. Similarly, when a learner completes their course, or enrols again, their access to resources is changed accordingly."

Rick Giagnacovo, Preston's College

Single Sign-On (SSO)

Identity Experts

Single sign-on makes passwords a thing of the past, allowing access through one secure set of credentials.

Cloud Applications

Through proxies, single sign-on puts every on-premise app at your employees' fingertips.

Conditional Access

Machine learning detects suspicious behaviour, applying risk-based conditional access to minimise security risks. Users can also be restricted by location and device for additional control.

Reporting

Monitor the who, where and when of individual user access to information, all in real time.

Passwordless Working

Automatically change permissions to match an employee's changing job role as they move throughout the organisation, safeguarding confidential information in the process.

Multi-Factor Authentication

Administrators can maintain confidence in the new Joiners-Movers-Leavers process with regular prompts to review permissions.

Data Protection

Secure your data ready for a fresh start, with access automatically revoked on a leaver's last day.

Facts

In 2017, '123456', 'Password' and '12345678' topped Time magazine's list of the year's worst passwords.

How Does It Work?

Under the old working practices a user would have to login to each application, a repetitive, error prone and tedious process. With single sign on the user now only has to login once a day, first thing in the morning.

Access Governance

Access governance ensures that end users only have the necessary permissions available to them, reducing major role-based security risks.

Reporting

Understand who has access to data, and who has accessed it in the past, for a top-down view of the organisation's security.

Choose Between RBAC and ABAC

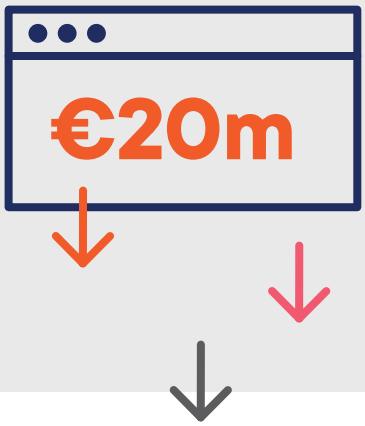
As job roles differ between organisations, so too does granting access. Organisations can choose to assign access based on an individual's Role (RBAC) or Attributes (ABAC).

Attestation Campaigns

Employees can request access to a resource for a limited amount of time, allowing for autonomy, swifter workflows and security.

Did You Know?

Companies who fail to report a data breach within 72 hours of discovery are liable to be fined up to €20million or 4% of their previous year's turnover under new GDPR guidelines.



Harris Federation

"Joiners and movers now get access to the correct resources immediately, ensuring they are productive straight away, whereas leavers are immediately denied access, helping to maintain security across our systems."

Andy Meighen,
Harris Federation

GDPR Compliance

Under the EU's new guidelines, ensuring that only the right people can access employees' personal data is crucial to compliance.

Financial Savings on Unused Licences

Are all your user licences accounted for? With former employees still active, organisations can rack up huge costs in unused licences.

How it Works

An employee moving departments from HR to Marketing would take their accesses with them and then be able to view their new manager's salary. With Access Governance this permission would be automatically revoked on the change of role.

Identity Experts