



**Identity Experts**  
performanta

# Consolidate & Manage Accounts

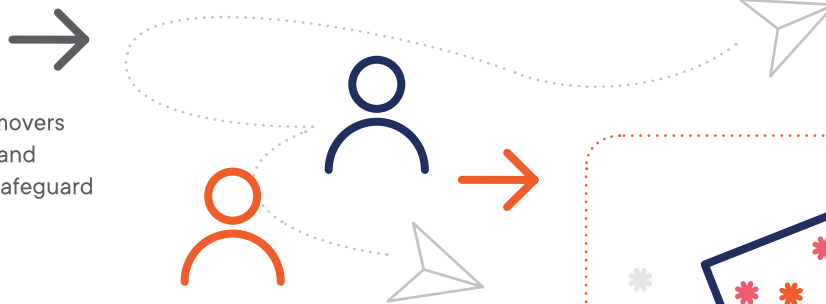
Information Bundle



Identity and access management refers to the framework put in place which provides the individuals in an organisation appropriate access to resources.

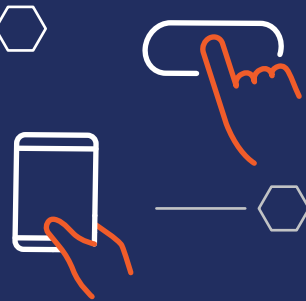
## JML

Keep up with joiners, leavers and movers within the organisation, changing and revoking access automatically to safeguard sensitive information.



### Self-Service

- ✓ Gift users with the autonomy to manage their passwords and request access to sensitive information.
- ✓ Save on support costs by freeing your IT department from trivial tasks.



### Single sign-on

The days of passwords scribbled on post-it notes are over: with single sign-on (SSO), users can use one identity to manage different access permissions.



## 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.



## Facts

A survey into IT managers' confidence around protecting their organisations showed that 42% of respondents admitted their uncertainty to prevent breaches caused by accidental or purposeful staff actions.



## Fresh start

Prevent duplicating pre-existing identities and unwittingly giving new starters years of amassed permissions.



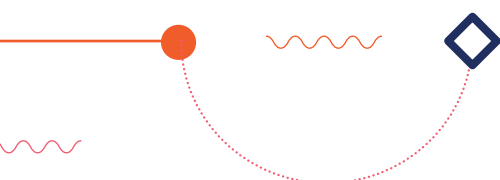
"We've got 15,000 students live at any one time, so to manually manage on-boarding and de-provisioning is a very onerous task for the IT team. Now, we have the automated management of staff and student account provisioning."

**Steve Parry,**  
Newham College

## How Can IAM Help You?

Before IAM was implemented, a new employee would have to wait for up to one day for their system accesses to be manually provisioned, causing frustration and wasting productive time.

With IAM, accounts, permissions and passwords were ready for them when they walked in the front door.





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



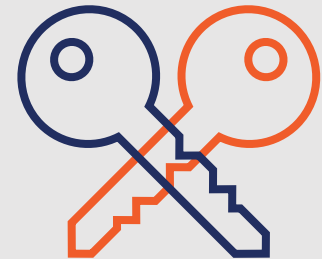
## Slicker Onboarding

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.



"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 enrolls again, their access to resources is changed accordingly."

Rick Giagnacovo, Preston's College



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.

## GET IN TOUCH

Contact our identity experts to find out how we can help you;  
email [enquiries@performanta.com](mailto:enquiries@performanta.com)

[www.performanta.com](http://www.performanta.com)