



Technology whitepaper

IAM integration and automation with Able+

Abstract

An organisation's IAM solution is its "single source of truth" for identity. However, efficiently creating and managing these identities typically requires technical integration and automation between the IAM solution and other relevant systems. Unlike most IAM solutions, which require the use of software developers to perform this integration and automation, Able+ provides three unique capabilities that enable typical users to easily integrate and automate their organisation's IAM processes. This whitepaper discusses these capabilities and provides a worked example that illustrates their intuitiveness, power, and flexibility.

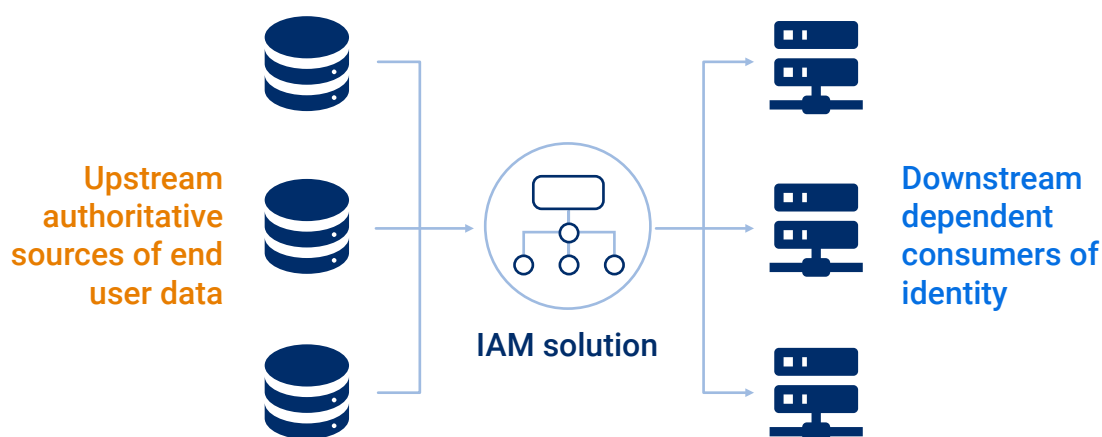
Document Date: December 2020

Author: Josh Howlett

Introduction

Every organisation needs an IAM solution that is its “single source of truth” for identity.

The authoritative sources of data used to construct these identities are typically Human Resources (HR), Customer Relationship Management (CRM), and other business systems ‘upstream’ of the IAM solution. The consumers of these identities are the services downstream of the IAM solution. These relationships are shown in the figure below.



Some of IAM’s key challenges are related to the management of the flows of this data:

- obtaining it in a variety of different formats from numerous upstream systems
- consolidating and normalising it so that it can be managed as one data-set; and
- making it available to downstream systems.

Issues can arise if these flows are poorly managed or executed, for example:

- delays in updates from upstream sources result in a new employee lacking the access they need to start work
- human error during a manual process leads to an ex-employee retaining access to sensitive information; or
- a rogue employee changes their entitlements and so acquires access to sensitive business information.

These issues often arise because systems are poorly integrated. As a result, additional business processes are needed; for example, a periodic creation and transfer of a CSV report from the CRM system to the IAM solution. These can create operational complexity and the scope for error, failure, and security vulnerabilities.

Some IAM solutions can address these issues by providing integration and automation capabilities. However, these almost always require IAM technical specialists, with the result that:

- costly consultants might be needed if technical specialists are not available within the organisation
- the business process owners must work with the technical specialists to explain their requirements and facilitate integration and testing; and
- the technical specialist might be the only person who can understand configuration.

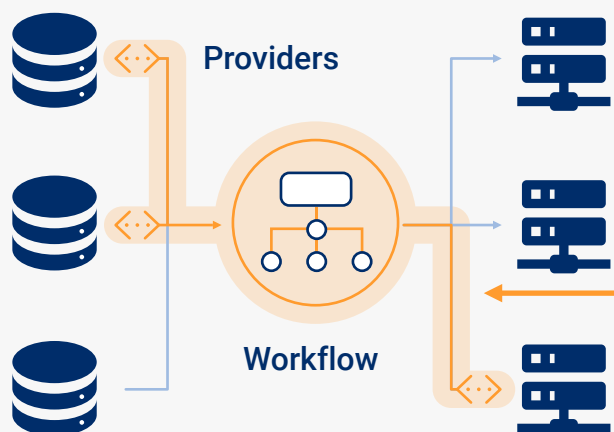


Tools for automation and integration in Able+

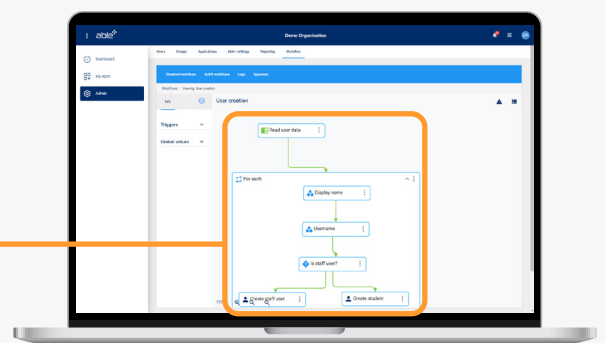
Able+ solves these problems with three key capabilities:

- its **workflows**, which act on flows of data from upstream to downstream systems
- its **workflow designer**, which is a visual editor for creating and managing workflows; and
- its **providers**, which connect Able+ to upstream and downstream systems.

These are illustrated in the figure below.



Workflow Designer



Workflows

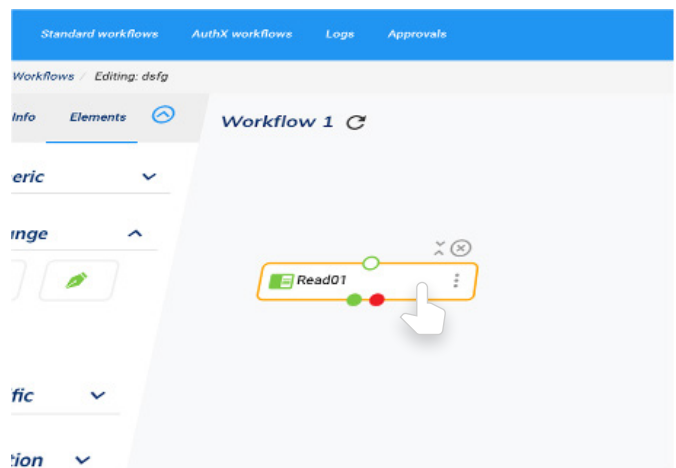
A workflow is simply a sequence of actions, defined by the user, that automates IAM administration. They are a powerful tool, that can address almost any IAM need, but common scenarios include:

- identity provisioning and deprovisioning triggered by changes to the HR system with changes synced to on-premise and cloud-based systems
- ensuring that users' access entitlements are consistent with their role; and
- creating users' display names, usernames, and email addresses according to the organisation's preferences.

Workflows can be triggered manually; or automatically by internal or external events; or according a defined schedule. They can be cloned to ease the creation of multiple similar workflows; executed as a 'dry run' for testing; and their management delegated and permissioned.

Workflow designer

The workflow designer is an intuitive “drag and drop” interface for users working with workflows. The elements used to define the business logic within a workflow can be placed onto a canvas, and their behaviour and interactions controlled through a purely “point and click” configuration. As a result, the user does not need any programming experience.



Providers

Finally, Able+ includes the providers needed to define workflows connecting common upstream or downstream systems, such as Microsoft Active Directory. These will be sufficient for most organisations. However, it is also straightforward to create custom providers – for example, for legacy or inhouse systems – using the product's API. This requires software development, but it is a one-time investment: once implemented, users can integrate it seamlessly within their workflows using the visual editor.

Summary

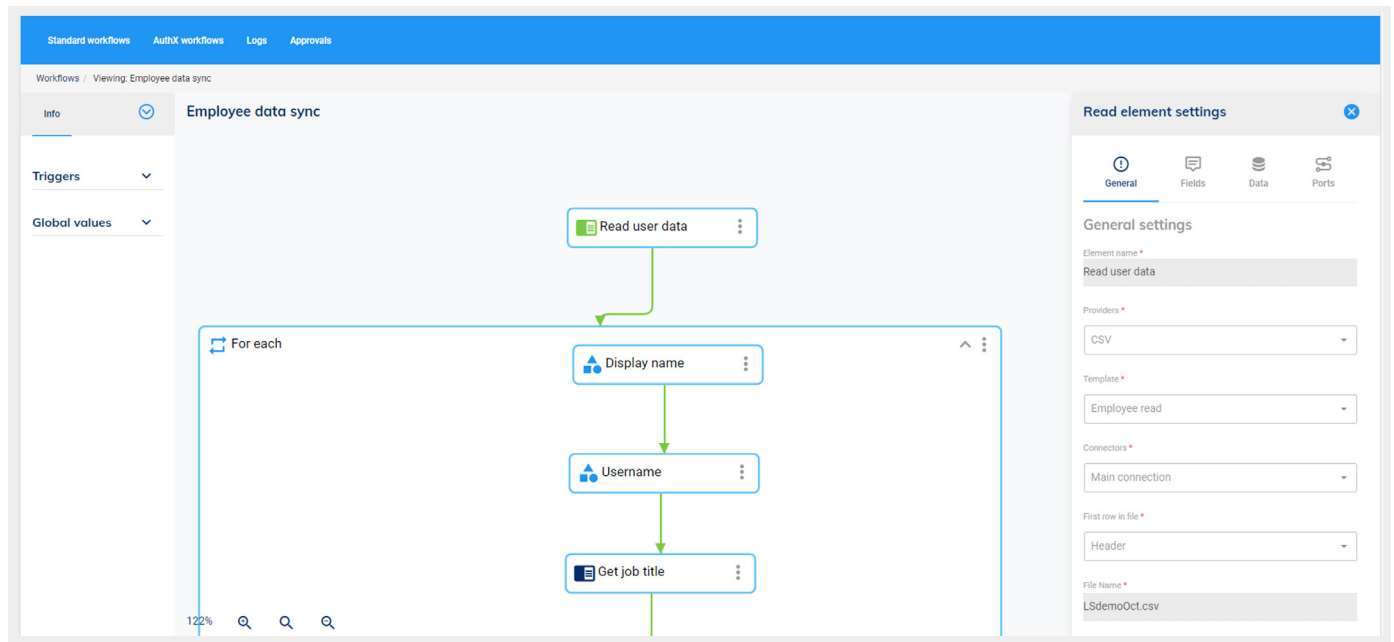
Together, these capabilities mean that

- typical users, such as administrative staff, can create and manage workflow, avoiding the use of technical specialists
- business process owners – who might be the user noted above – can take ownership of their workflows and make them available to others to inspect and modify; and
- the solution is flexible and extensible, so that it adapts to the organisation's business processes rather than dictate them.

An onboarding workflow

In this section we examine an onboarding workflow. This is a simplistic example, but it helps to illustrate the key concepts.

The screenshot below shows the first part of the workflow



The workflow starts with the element named 'Read user data'. This is a read element which, as can be seen within its configuration pane, uses the 'CSV' provider. The element is configured to read the CSV data using the 'Employee read' template. This defines a schema mapping the values of each CSV position (e.g., the first position) to an internal field ('Employee number'). This leads to a For each loop, which proceeds to iterate over each row within the CSV file as it performs the following actions.

The next two elements are transformation elements that construct the display name and username attributes using the fields extracted from CSV. The screenshot below shows the transformation configuration of the 'Display name' element, whose value is created by concatenating the forename field, a space, and the surname field.

The screenshot shows the 'Transform element settings' pane for the 'Display name' element. The 'Transform' tab is active, showing a formula builder. The instruction 'Create a transform formula by adding 1 or more fields' is displayed. The formula is constructed as follows: 'Input field' (dropdown) followed by 'Entire field' (dropdown), then a plus sign, then 'Space' (dropdown), then another plus sign, and finally 'Other field' (dropdown) followed by 'Family name' (dropdown) and 'Entire field' (dropdown).

Custom object element settings

General Filters Fields Data Ports

Filters

Job Code

Filter type *

Dynamic

Filter *

Job Code

Operator *

Is found in

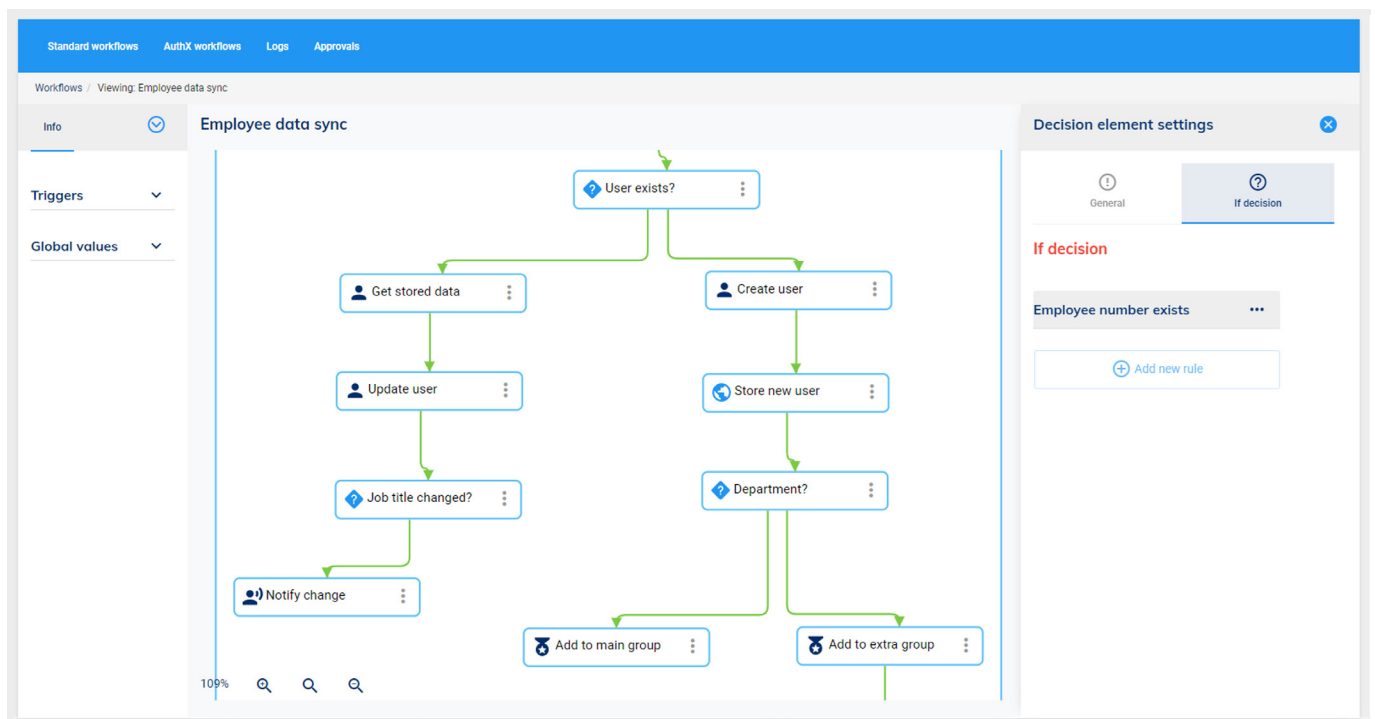
Data source *

Username: Post ID

+ Add new filter

The fourth element is a custom object element. These elements perform actions on objects that hold data within custom tables that are managed within Able+ (rather than accessed externally). As shown in the screenshot below, this element is configured to filter a table of job codes using the job code field (obtained from the CSV file) for the associated job title.

Having determined the display name, username, and job title for the user, the workflow proceeds towards either creating or updating the user account, depending on whether it already exists, as shown in the screenshot below.



Decision element settings

General If decision

If decision

Employee number exists ...

+ Add new rule

The 'User exists?' test is performed using a simple 'if' decision element, as shows in the screenshot below. It simply checks to see if the employee number field exists within Able+.

If the employee number exists, the workflow branches to the 'Get stored data' user element. This identifies the user data associated with the user's employee number, whose record is then updated by the following 'Update user' user element. A second 'if' decision element is used to determine if the user's job title has changed; if it has, a notification is issued to another user. The configuration for each step is shown in the sequence below.

User element settings

General Fields Ports

General settings

Element name *

Get stored data

Action *

Get user

Identify user by workflow field *

Employee number

Compare with Able+ field *

id

Filter users

User element settings

General Fields Ports

General settings

Element name *

Update user

Action *

Update

Identify user by workflow field *

person.username

Compare with Able+ field *

person.username

Period type *

Immediately

Decision element settings

General If decision

If decision

new different from old ...

+ Add new rule

Communication element settings

General Data Message Ports

General settings

Element name *

Notify change

Communication type *

☐ Email ☒ Internal

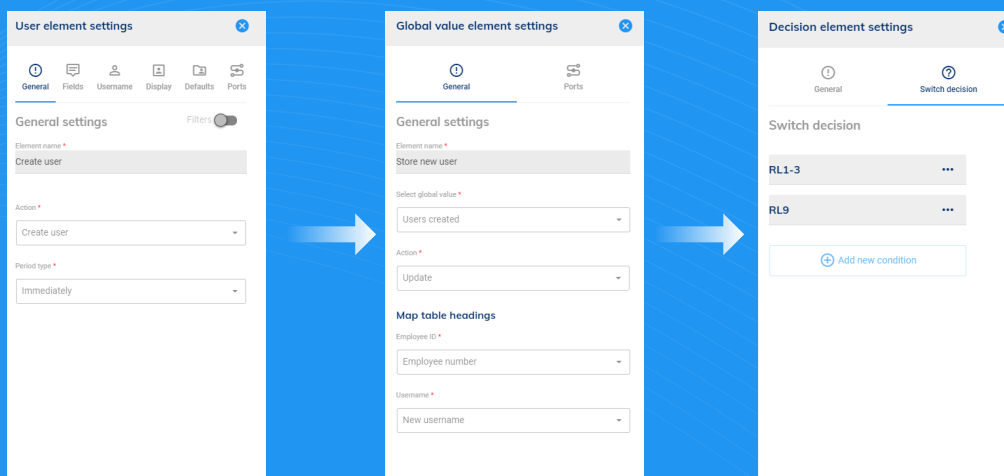
Recipient *

Named users

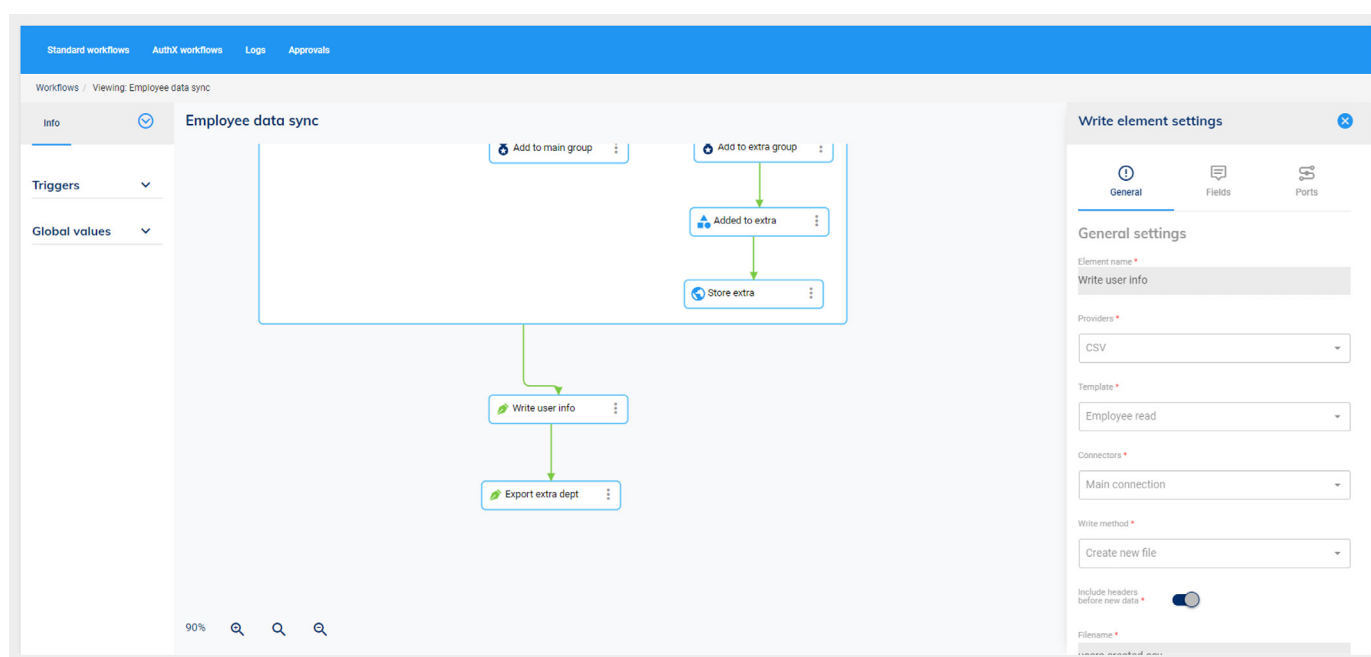
Recipients *

Angela Nightingale

If the user does not exist, the workflow branches to the 'Create user' and 'Store user' user elements, which create and update the user account, respectively, as shown in the sequence below. Another 'if' decision is then used to determine, depending on the user's department code, whether to add the user to the main or extra groups.

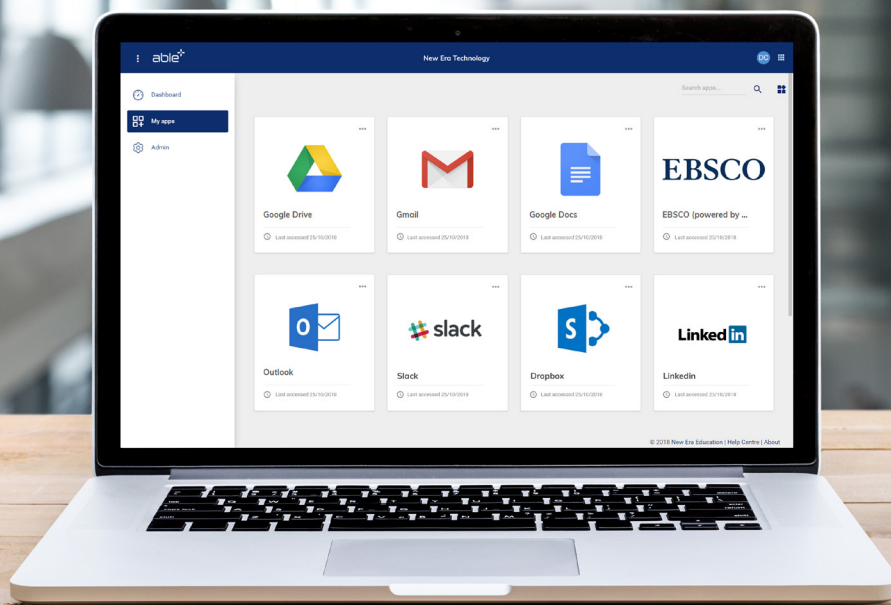


The workflow concludes after the For each loop has processed the final CSV row. The user information is saved externally to a CSV file using the 'Write user info' write element. As before, the position of the fields within each row specified by the 'Employee read' template. This configuration is shown in the screenshot below.



Conclusion

In this whitepaper we've seen how workflows facilitate the seamless automation and transfer of data between systems. These workflows connect to systems using providers, which provide a standard interface between external sources and consumers of identity. The workflow designer is an intuitive to use tool enabling typical users to easily design and manage their workflows. By empowering business owners, Able+ removes the dependence on technical specialists, increasing transparency and efficiency. The combination of these capabilities enables Able+ to easily integrate and automate any organisation's IAM processes.



03334 559424

info@neweratech.co.uk • neweratech.co.uk

