TOOLS4EVER

7 steps to a successful IAM implementation

Table of contents

Introduction

HelloID is an IAM solution with which you can fully automate identity and access management. The platform supports the entire 'identity lifecycle', from the onboarding of new employees to the automatic adjustment of rights when someone takes on a different role, and the closing of an account when someone leaves the organisation. The application and approval of (temporary) software licenses, and support processes such as name changes and password resets, can also be fully automated.

This means that the implementation of an IAM project requires a lot of attention. The platform will need to be connected to, among others, source systems, target systems, Identity Providers and management systems. Therefore, the implementation and migration of an IAM system must be carefully planned and executed. Tools4ever offers an extensive blueprint for this. In this whitepaper, we provide a brief summary with the most important steps and points of attention.

Step 1: Projectteam

It is important to realise that prior to the implementation project, a preparatory phase has usually already been completed within the client organisation. Generally speaking, the stakeholders will have been identified, the main requirements and wishes have been established, the choice of supplier has been made based on these, and if desired, a business case has been prepared. Following the proverbial 'go' from management, the implementation project then starts in order to actually implement and migrate the selected solution.

As the first step of the HelloID implementation project, we refine the standard blueprint into a concrete project implementation plan and form the project team. As a project manager, you will want to give the key stakeholders an active role in the project execution, for example as a member of the project team:

- Involving an HR specialist is very important because the HR system manages and provides the source data for the creation of accounts and the associated rights. It is crucial that these data are accurate and consistent at all times.
- The system or application administrators of the 'receiving' systems must be directly involved to ensure that these connections function properly.
- For a security and privacy specialist, the IAM system plays a key role in the organisation's access and information security.
- In order to ensure a seamless adoption of the new solution, it is wise to involve the Helpdesk and representatives of the end-users early on in the process.
- This is also the right time to involve the new HelloID application administrator in the implementation and to build up as much knowledge as possible about the new application.

Preferably have the involved employees follow HelloID trainings before the project starts. HelloID is designed in such a way that the IT team of the client organisation – or their service provider – can do as much themselves as they want. For this purpose, the platform has powerful and user-friendly configuration options. HelloID offers several free trainings, following which you can start working independently:

- An administrator training where you learn how to optimally manage HelloID following the handover (1 day).
- An implementation training that is considerably more substantive and technical, teaching you how to implement HelloID independently in a network environment (2 days).

On the Tools4ever side, the project is supervised by a business consultant and a technical consultant. The business consultant is the contact person during the entire implementation. The technical consultant takes the lead on the technical side.

Step 2: Intake

It is important to first map out the existing identity and access processes. This concerns the onboarding, transitioning and offboarding processes, but also other processes for, for example, name changes in accounts, user requests for additional applications and password resets. We inventory the various systems used for these processes through an intake session, where both the business consultant and the technical consultant are present. We also discuss the requirements and wishes related to the IAM functionality. The goal is to clarify the current pain points in the area of user, authorisation and access management, so that we know which HelloID modules offer a solution for the challenges your organisation faces, and how we can deploy these solutions to address those challenges.

HelloID biedt de volgende modules:

- Provisioning
- Service Automation
- Access Management

A key component of the HelloID solution is the Role Based Access Control feature. Through an authorisation matrix with business rules, the platform determines for each user which user rights they receive, based on their role(s) within the organisation. If an organisation does not have such an authorisation matrix in place, we look at how we can export the current setup from the HRM system to use as a basis. After that, we plan a role mining session in which we map out the various roles and rights groups both top-down and bottom-up. Our business consultants have extensive experience in this area and through a clear, defined consultancy trajectory they assist you in quickly establishing a baseline authorisation matrix through role mining. If desired, more extensive role mining can become part of the agreed project scope.

To learn more about role mining, you can read this blog:

https://www.tools4ever.nl/blog/2022/slimme-rol-mining-de-booster-voor-role-based-access-control/

During the intake session, we compile a list of action items and refine the project plan. The intake documents are discussed and shared with the client, so that they can carry out the necessary internal preparations.

## Step 3: Drafting design and test plans

Using the information from the intake, we then design the new process flows for the account lifecycle processes and other account-related service processes. We establish, for instance, how and when an account is created for new employees, as well as the timing for sending a notification with login details to the supervisor. This design also details which modules, and which specific functions within those, are used and which data must be exchanged with other systems.

The design that is created is discussed in a meeting. At the same time, based on the design, we also develop a test plan with corresponding acceptance criteria. This allows us to evaluate the results post implementation and to determine whether the implementation has been carried out according to the agreed guidelines. Once both the design and test plan are approved, we proceed with the technical implementation of the chosen HelloID modules.

Step 4: Technical implementation

During the technical implementation, our implementation consultant ensures that the agreed design and prerequisites are implemented in the utilised platform modules. The time required for implementation primarily depends on the size of the organisation, the number of connected systems, and the complexity of the authorisation matrix and the associated management processes. HelloID is developed as a Software-as-a-Service and, thanks to the large set of APIs and powerful configuration capabilities, the implementation takes little time. Generally, one implementation consultant needs 4 to 6 days to implement the full installation and configuration. Because this often requires certain details to be worked out and agreed upon within the organisation, the usual duration is typically a few weeks.
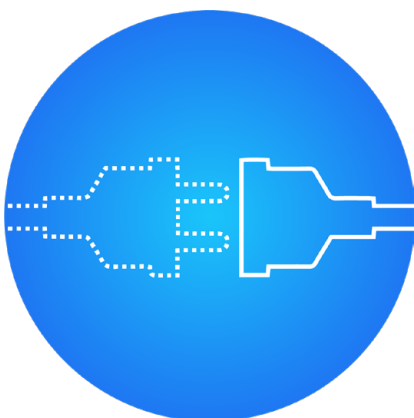
To ensure a successful implementation, it is crucial that existing accounts in target systems are unambiguously correlated with individuals in the source system. This prevents HelloID from creating redundant accounts or leaving an account needlessly active if someone subsequently leaves the organisation. To this end, within HelloID we use what are known as correlation values, a unique key to relate individuals in a source system to accounts in target systems. The unique employee number is often suitable for this, but an email address is also an option. After configuring this correlation in HelloID, the customer receives a full report, including any missing correlations that still need to be added. The implementation consultant discusses this report with the customer.

To learn more about account correlation, read this blog: *https://www.tools4ever.nl/blog/2023/correlatie-van-bestaande-accounts/*

Step 5: Test and acceptance

Once the technical implementation is completed, the test and acceptance phase can begin. In this phase, we perform a trial run of the test plan that was established during the design phase. For the onboarding, transitioning and offboarding processes of the organisation, we use static test data and dummy accounts. This allows us to correct any potential errors in the implementation without impacting the organisation and its users. Only after successfully completing the acceptance tests will we proceed to the subsequent step of using client-specific production data.

Step 6: Onboarding and handover

Once the test plan has been successfully completed, we transition from static test data to production data, using a phased approach to minimise the risk of errors. We start by onboarding a few employees. Once these workflows are successfully completed, we proceed by onboarding an entire department. After that, we gradually roll out the new IAM solution across the entire organisation.

Step 7: Support

Following handover, we hold a closing meeting to assess whether the implementation has been completed according to the guidelines. Afterwards, the client can independently work with the IAM solution. We offer HelloID as a Software-as-a-Service that is centrally managed with automatic updates. Thanks to the available trainings, extensive documentation at docs.helloid.com and release notes and webinars, the organisation's own IT team or their service provider can easily manage and modify the platform operationally. And if the client encounters any issues or change requests for which they would like assistance, the Tools4ever support team is always there to help.

Points of attention and tips

Monitor the release planning of other systems

In many organisations, the IAM platform is truly the hub of the IT network, connected to almost all systems. That means it is important to stay alert to planned changes in those connected systems so that you are always informed, understand the impact, and if necessary, can adjust the connection between HelloID and the system in time.

Establish guidelines

Confirm internal agreements and guidelines in writing. For example: "What should an email address look like?" This might seem like a simple task, but it can entail quite a bit of complexity. For instance, the employer may wish to work based on birth name, but the employee may prefer to use their married name. And what do you do if the email address is already assigned to someone with a matching name? This occurs more often than you might think. What agreements do you put in place to respond to these types of situations within your organisation?

Ensure that the organisation is well documented

For a smooth introduction of Role Based Access Control, it is tremendously helpful if the existing organisation of departments, functions and roles is stable and well documented. It is preferable to invest in this prior to the IAM implementation project.

Carefully plan the implementation period

Depending on the industry, you may encounter different peak periods, such as during an audit, the financial year-end closing or the migration of another IT system. IAM is a critical and central system, and its implementation will require considerable attention. We recommend trying to avoid scheduling the IAM implementation during such a peak period.

Advice on your IAM implementation and migration project?

Contact us for a no-obligation consultation.

TOOLS4EVER

Address	102-103 Church Street, GL20 5AB, Tewkesbury, UK
General	+44 (0)1684 274 845
Support	+44 (0)1684 270 822
Information	uksales@tools4ever.com
Sales	uksales@tools4ever.com
Support	uksupport@tools4ever.com