TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

White Paper

Identity as a Service (IDaaS)

Table of contents

Introduction

Identity and Access Management (IAM) software has long played a key role in IT environments. Identification, authentication, and authorization ensure that users have the right access at the right time. But the role of Identity Management is changing. These changes are driven by growth in cloud services, new data regulations, increasing automation, and remote work. Below, we outline these trends.

📈 **Trend**	📊 **Consequence**
Organizations are transitioning to the cloud. Traditional infrastructure like Exchange, Active Directory, and local storage is being converted to Azure, O365, and Teams. HR systems and other business applications are usually the first systems to be migrated. Companies maintain their existing data centers only until the depreciation period has passed.	**On-premise IAM systems are being replaced with IDaaS (Identity as a Service) software.** Within a few years, most organizations will no longer have their own on-premise IT infrastructure. Cloud services will offer better uptime, lower costs, and seamless updates.
Data is becoming more valuable, but more regulated. Product, customer, and employee data are more valuable than ever before. Timely, complete, and correct access is essential. At the same time, strict laws and regulations (e.g., GDPR) force expensive, far-reaching changes. Organizations must prevent audits, negative publicity, fines, and breaches.	**Security and audit-compliance measures must be implemented at the lowest level – Identity.** Five years ago, semi-automated procedures and a few scripts were sufficient to comply. Shared accounts and passwords were still common. No longer. Management, boards of directors, and security officers are realizing the security and compliance benefits of professional IDaaS solutions.
Automation and efficiency are top priorities. But bottlenecks remain in the user lifecycle. Companies are rooting out inefficiencies and automating manual workflows wherever possible. But the smartest management teams have found an extra edge: streamlining the user account creation and access process.	**Complete IDaaS solutions now include user account provisioning.** In the past, HR submitted helpdesk tickets for new hires and IT created their accounts by hand. Today, IDaaS solutions automatically monitor HR data and propagate the necessary changes across all target systems. User accounts, email addresses, access rights, software licenses, and other resources are automatically provisioned without manual involvement.
Remote work has exploded the old network perimeters. Employees need access to their applications and data – at any time, with any device, and from any location. This creates both new risks and opportunities.	**Zero Trust Security models, anchored in Identity Management, are the future.** Access decisions are tightened and enforced at each step – seamlessly. The old threat of ‘perimeter breach’ is mitigated. Through IDaaS, all resources are provided securely and on time. Single sign-on (SSO) application access, paired with multi-factor authentication (MFA) is the first step.
Legacy “black box” IAM systems have become intolerable. Every year, traditional on-premise Identity Management software becomes harder and costlier to maintain. Few people in the organization understand them. Even fewer can manage them. Consultants are slow, scarce, and expensive.	**Organizations require expertly supported, actively developed IDaaS solutions.** Modern software allows quick adaptation to changes in the market and organization. Development teams are more responsive to customer feature requests. Expert support is provided in-house, with transparent and predictable cost structures.

With HelloID – Tools4ever's Identity as a Service (IDaaS) solution – we are ahead of these important developments. HelloID is a full-fledged native cloud application. It automates your organization's entire Identity lifecycle. Your users get easy and secure access to their IT services. You are relieved of the burden of maintaining costly local hardware, software, and storage infrastructure.

Installation and configuration are accomplished within a matter of hours. You decide who will manage the solution: Tools4ever, one of our trusted implementation partners, or your own organization.

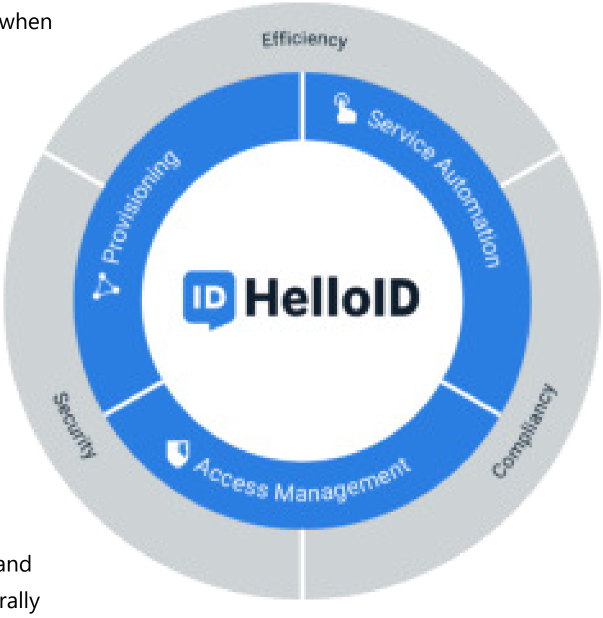
With HelloID, there is no trade-off between cost savings and security. In fact, IT auditors frequently praise our customers for their outstanding compliance evaluations. All HelloID tenants run in a maximum-security Azure environment, which is thoroughly checked by Deloitte Risk Services every six months. Security compliance is guaranteed.

Plus, we offer you a balanced growth path. HelloID doesn't force you into a 'big bang' adoption scenario with big risks and pressure. Instead, HelloID is split into modules. The roll-out takes place in stages. You are free to start with the module(s) of your choice. If necessary, active modules can be disabled without disturbing other modules.

HelloID has the following modules:

1. **Provisioning** automatically creates, manages, and deletes user accounts in any number of target systems, based on source information in your HR system. It automatically assigns rights, permissions, and other resources based on context. The blanket term we use is "entitlements." Whenever a user's context is changed, their entitlements are adjusted accordingly. For example, when someone leaves the organization, all of their entitlements are automatically revoked, including their accounts. This happens without manual intervention or helpdesk tickets.

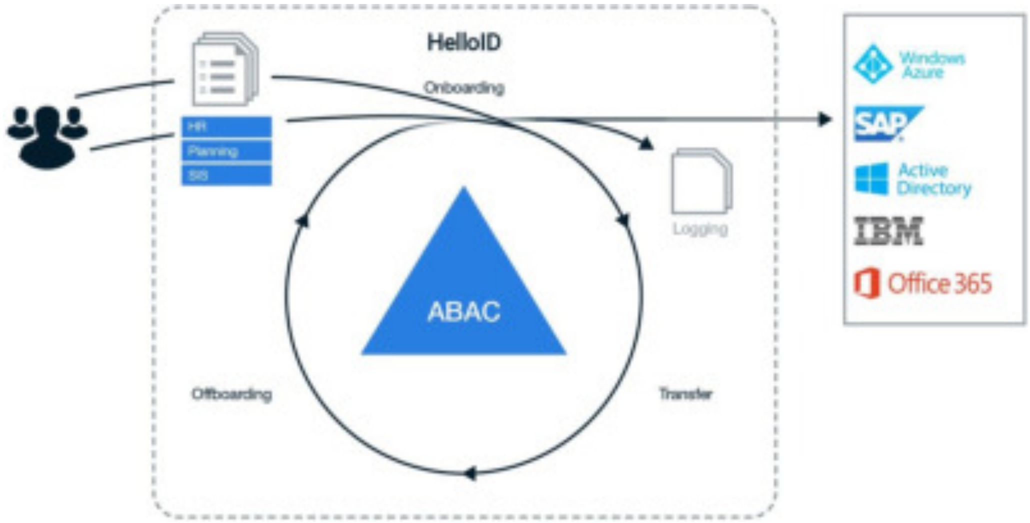
2. **Service Automation** seamlessly connects with Provisioning. Inevitably, there are one-off requests which can't be anticipated in Provisioning business rules. For example, a user temporarily needs a specific application or file share. Service Automation fills this gap. Employees and managers simply fill out a web form, and HelloID handles the rest. Full PowerShell support allows every task to be automated to the fullest possible extent. Changes are made directly in the network, without intervention by IT staff.



3. **Access Management** provides easy, secure access to applications and data. Users authenticate via the appropriate Identity Provider, generally paired with multi-factor authentication. Applications are then accessed via a user-friendly dashboard. Comprehensive single sign-on (SSO) protocol support means that almost any application can be accessed with a single click.

Provisioning

User accounts must be created, enabled, updated, and disabled on a regular basis. This may include multiple account types, including permanent and temporary employees, contractors, partners, and even customers. In addition to a 'main' directory account (typically Active Directory), each user needs accounts in other target systems. Entitlements, including rights, applications, and other resources must then be managed in all systems. HelloID Provisioning takes care of everything. It automates the entire inflow, throughflow and outflow process. This is called 'Identity Lifecycle Management'.



With HelloID, new employees receive their accounts, access rights, and other resources on day one. They hit the ground running. Then, routine work throughout the user lifecycle is minimized. Entitlements are automatically modified in response to context changes such as transfers, department changes, promotions, etc.

Is an employee leaving? HelloID can block the account immediately. Follow-up actions like deleting mailboxes and home directories can be scheduled for weeks or months in the future. You can even configure anticipatory actions, like reminding a manager to collect a departing employee's laptop. This automatic roll-back of entitlements creates immediate cost savings. Resource inventory is precisely tracked and expensive licenses are recycled instead of lost. Unused software subscriptions can be identified and canceled.

Automatic provisioning offers powerful security benefits. Employees often gradually – and unintentionally – accumulate more and more access rights. There is often no structured process for reclaiming unused or expired rights. Former employees may even retain access to company accounts, creating massive breach risks. With HelloID, you can ensure that your users always have exactly the necessary rights – no more, and no less. Grace periods ensure smooth transitions.

Provisioning makes user account management easier, faster and more secure. Managing user accounts is no longer a manual, complex and time-consuming task for HR and IT. Employees immediately become more productive. Access bottlenecks become a thing of the past.

Attribute Based Access Control (ABAC)

HelloID Provisioning uses the Attribute Based Access Control methodology. ABAC provides a structured, gradual way of creating Business Rules. These drive the provisioning process.

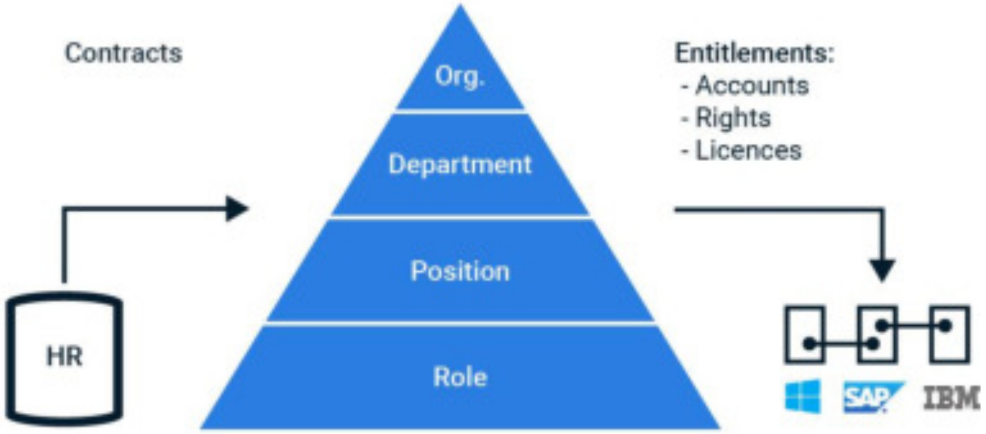
Using Business Rules, a 'matrix' is created. It cross-references context attributes vs. necessary entitlements. Attributes may include job roles, contracts, departments, or any other relevant factors. Each attribute is matched with its corresponding entitlements. Then, attributes are 'stacked' bottom-up to develop organizational job profiles.

The lion's share of this work can be done before Provisioning is rolled out. This immediately catapults the ABAC matrix to ~80% completion. The remaining 20% (detailed rules) are filled in over time. In this way, you can implement provisioning with a phased approach. You gradually transform your organization's current approach to full lifecycle automation – without planning every detail in advance.

The ABAC approach is a major improvement on traditional provisioning methodologies. For example, unstructured manual mapping is extremely complex and time consuming. On the other hand, the 'template user' approach – "Kim will do the same work as Wendy" – is too simple. ABAC threads the needle in a practical and simple way.

Formerly, ABAC was only available to large financial institutions and international corporations. But ABAC has become increasingly available in recent years due to new laws and regulations (e.g., GDPR, FISMA, HIPAA, SOX, NEN7510). It's now common practice, or even required, for healthcare institutions, medium-sized companies (300-5000 employees) and other commercial organizations.

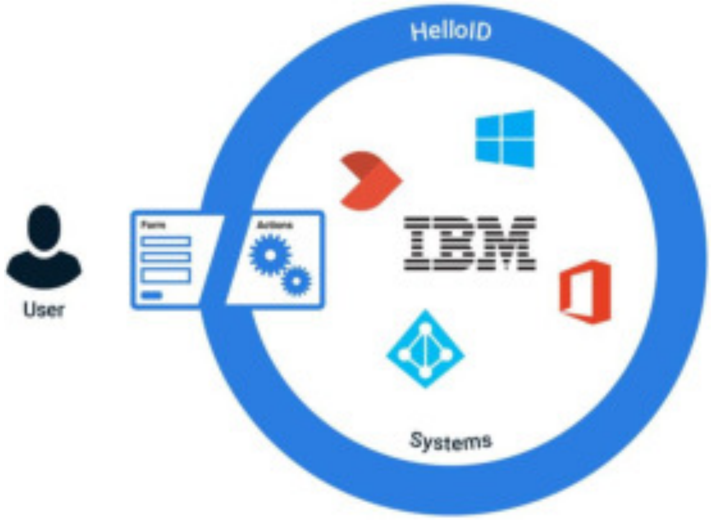
The diagram below provides a schematic overview of HelloID Business Rules. Context attributes determine which entitlements are needed at each level – organization, department, position, and individual job role.



Service Automation

The Provisioning process automates nearly all user-related IT changes. However, there are always exceptions. Many business functions depend on data and decisions which aren't recorded in the company's HR source system. Think of an employee who temporarily fills in for an absent colleague, or an employee who collaborates with another department. In these cases, employees will need temporary entitlements. Perhaps rights in SAP, a cloud application, a project license, membership on a distribution list, or membership in a Microsoft Teams site.

Most companies handle these changes through the IT service desk or Functional Management (FM). But this is expensive and time-consuming. Service Automation automates these changes. Using simple web forms called "delegated forms," employees without IT knowledge or domain admin rights can safely make changes to the network. This happens via a delegated shell, in which the HelloID engine executes pre-defined tasks. These tasks are always executed in the same way, with a full audit log.



With HelloID Service Automation:

- Trusted users can make pre-defined changes in the network, in a safe and controlled way. The helpdesk is liberated.
- Changes happen immediately, because there is no ticket queue involved.
- Managers have immediate insight into their employees' resources, including licenses and costs. Direct changes can be made as needed.
- Time limits prevent unwanted accumulation of rights and licenses.
- The organization projects a modern and professional image, particularly to new employees.
- ITSM platforms such as Servicenow and TOPdesk are seamlessly integrated. This increases end user acceptance by reducing the number of separate portals which employees must learn to use.

Service Automation can be implemented step-by-step. In each step, eligible delegated tasks are pushed 'downward'. Thus, users at every level of the organization are maximally empowered. Each request and approval decision happens at the lowest possible level.

Delegation to the service desk

The first step is delegating tasks from system specialists down to service desk staff. This immediately provides the biggest possible efficiency win. Non- or semi-technical service desk staff take over tasks which were previously only possible for system specialists[1]. The key is that no admin rights are required. Delegated forms ensure that only specifically allowed tasks are available. For example, a delegated form could reset Active Directory passwords, assign group memberships, or execute any custom PowerShell task in the network. No IT or application knowledge is required and every change is recorded in detailed logs.

Delegation to managers

The second step is further delegate the forms developed in step (1). This time, eligible forms are delegated from the service desk down to managers. This is a simple step, because at this point the forms have already been created. This is the step in which more employees come into direct contact with HelloID. Managers now have immediate insight into what entitlements their employees have. They can make immediate changes without involving IT staff. Cumbersome ticket processes are fully eliminated.

Delegation to end users

The final step is delegating eligible forms from managers down to end users themselves. An important prerequisite for this step is integrating existing self-service portals, such as TOPdesk or AFAS. End users are empowered to directly request resources necessary for their jobs, such as specific software applications. When a user submits a request through a form, their manager is notified and can approve or deny the request. This check is much easier for a user’s direct manager or license manager than for an IT employee. This is the benefit of the downward-delegation model. After approval, the Service Automation module automatically delivers the product if it is a digital item. If the product is a physical item, the necessary notifications are dispatched.

[1] Such as second-line and/or third-line system administrators or functional application administrators

Access Management

HelloID's Access Management module offers your employees, partners, and customers simple and uniform access to cloud applications. Authentication takes place via a username/password combination and two-factor (2FA) method of your choice.

Users can access the HelloID application dashboard from their laptop, tablet or smartphone. Cloud applications are listed as simple and recognizable tiles, which are launched with a single mouse click. Single Sign-On (SSO) automatically logs the user into the launched applications, with no additional login screen required.

Access Management is a three-step process:

1. The user proves that they are the person they claim to be (**Authentication**);
2. The user gets an overview of the applications they have access to (**Dashboard**);
3. The user launches an application directly, without having to log in again (**Single Sign-On**).

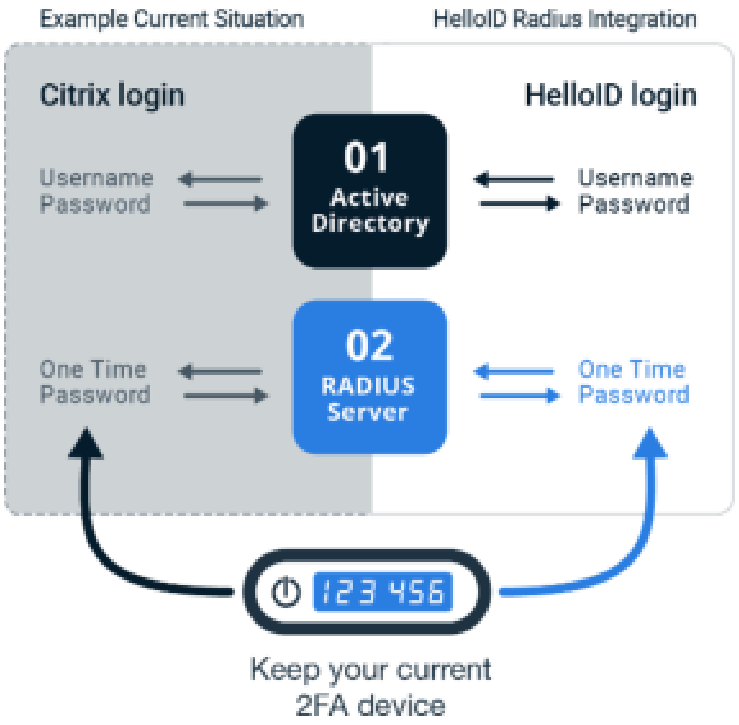
These three steps are explained below.

Authentication

Most often, Active Directory is used to authenticate users into HelloID. But, other Identity Providers such as Azure AD, Google G Suite, and Salesforce are also supported.

Local accounts, not tied to any Identity Provider, can also be created. This is a useful way to grant access to customers, partners, patients, or other guests of the organization. Local users can log into HelloID and access resources without having an account in the organization's directory system.

HelloID offers comprehensive 2FA technology and is very cost competitive (e.g., compared to Azure P1). Supported factors include push-to-verify, hard tokens and security keys, email, text message, and traditional one-time passwords (OTPs). A variety of other integration options are also possible, including Radius integration.



Dashboard

After logging in, end users are sent to the application dashboard. Graphic tiles provide one-click access to your organization's cloud applications.

HelloID group memberships determine which applications are available. Employees are added to groups based on department, position, location, etc. Then, applications are authorized on a group basis. This gives you an organized way of controlling who gets access to which cloud applications. Group membership can even be used to control whether a certain application requires an additional layer of 2FA.

To make access control even easier, group memberships can be directly synchronized from Active Directory or other directory systems. This saves administrators a lot of work. For example, an AD group can be mapped directly onto a HelloID group.

The dashboard's look and layout can be customized according to the specific needs of your organization. The default layout can be modified via custom style sheets, CSS coupling, or links. The end user API makes it easy to integrate the dashboard into social intranet applications such as TripTic, Embrace, a&m impact, Workplace365, Motivo, Google Sites or SharePoint Online.

Single Sign-On (SSO)

After the user is authenticated, it's possible to automate authentication to other applications via Single Sign-On (SSO). HelloID stores the user's credentials for each application and automatically forwards them via the appropriate SSO protocol when the user launches an application. The user doesn't need to log in again, unless additional requirements have been set (e.g., a second 2FA layer).

HelloID supports all standard SSO protocols, including: OpenID Connect, SAML, WS-Federation, HTTP(S) Post, and Basic Authentication, etc. A browser plugin covers edge cases for applications which don't support a standard protocol.

About Tools4ever

Tools4ever is a Dutch software company. We develop innovative and standardized Identity as a Service (IDaaS) solutions. Today's IDaaS solutions are complex, which is why we have dedicated ourselves to developing and delivering IDaaS solutions that are easy to implement and manage. From 2013 to 2020, we invested as much as possible to achieve this objective. HelloID is built from scratch using state-of-the-art software techniques. The first release of HelloID was received with great enthusiasm in early 2020. HelloID is a beautiful product that makes our users happy. We feel obliged to provide excellent service for a fair remuneration, and to continue to invest in the further development of HelloID.

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

Tools4ever New York

Address	300 Merrick Road, Suite 310 Lynbrook NY 11563 USA
General	+1 866 482 4414
Support	+1 516 482 7525
Fax	+1 516 825 3018
Information	nainfo@tools4ever.com
Sales	nasales@tools4ever.com
Support	support@tools4ever.com

Tools4ever Washington

Address	11515 Canyon Road E Puyallup WA 98373 USA
General	+1 888 770 4242
Support	+1 253 770 4823
Fax	+1 253 435 4966
Information	nwsales@tools4ever.com
Sales	nwsales@tools4ever.com
Support	nwsupport@tools4ever.com