v1.0 | 2017 10 17

White Paper HelloID

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

INDEX

SUMMARY

Your organization requires various applications to operate – some are managed internally, but an increasing number are cloud-based. It is critical that these applications and the data contained within are adequately protected, so that only your employees may access them and any risk regarding the misuse of business or customer information is mitigated. Aside from financial and reputation damages, the legislation and regulations concerned with securing data have become more and more strict.

However, you do not want excess security to hinder your employees' work. Repeated logins and having to remember numerous credentials for each application add layers of inefficiency. Instead, every organization benefits from one integrated and secure, web-based workplace in which they can seamlessly use both cloud-based apps and windows applications. Combining IT security with user-friendliness eliminates this undesirable tradeoff.

HelloID is a cloud-based, Identity and Access Management (IAM) solution that provides your employees access to all your business applications via one portal - requiring only one username and password. This portal grants them access to all the applications and data they need to do their work. With its enhanced Single Sign-On functionality, HelloID integrates all business applications - from online cloud apps to internally hosted web applications. This easy access is secured with configurable access policies, such as Two Factor Authentication, for additional security.

HelloID's access and data management tools provides you complete control over who has access to which applications and data, at what time and from which location or device. Through the Self-Service portal, employees can request access to the resources they require, but have not yet been given permissions for. Managers and "data owners" can grant this permission with one click. This not only increases the ease of use to employees and managers, but also reduces the IT department and helpdesk workload.

HelloID is a modern, cloud-based IAM solution. The installation is fast and easy, without requiring expensive specialists for management. With easy-to-use HelloID, your organization will be prepared for future application and data protection requirements.

INTRODUCTION

Identity and Access Management (IAM) is increasing in importance, particularly due to rapid changes in IT infrastructure and ever-evolving laws and regulations.

- Until recently, most organizations managed their local infrastructure, focusing on optimizing IT and business process efficiency. However, the explosive transition to cloud-based IT has disrupted these efforts. Many companies are preparing for this change by adopting a “cloud, unless” policy. Their current data centers are expected to remain in service through the depreciation period for a few more years before the whole infrastructure will be reviewed. Even traditional infrastructure components such as Citrix, Exchange, Active Directory (AD) and Local Storage will be reevaluated.

- Simultaneously the evolving laws and regulations regarding data security and privacy require action and policies. The US Health Insurance Portability and Accountability Act (HIPAA) , The Gramm-Leach-Bliley Act (GLBA) and Sarbanes-Oxley Act (SOX) are known data protection regulations in the United States. On May 18th, 2018, the EU’s General Data Protection Regulation (GDPR) will come into effect. These regulations carry significant operational impact for all organizations. The yellow cards from the audit reports require attention, and in many organizations, a security officer is appointed for all information security issues.

Using Identity and Access Management (IAM), organizations manage user account information and user access to their infrastructure, applications, and data. IAM provides streamlined hiring, promotion, and resign processes and role-based access to applications. Access is granted via a dashboard, and for optimal user experience, IAM also offers Single Sign-On, Self-Service, and workflow management functionality.

IAM plays a central role in the migration to cloud environment and adapting to new laws and regulations. A reliable and future-proof IAM solution makes access management not only more efficient, but should also help the organization regarding laws and regulations, support cloud applications and be available in the cloud itself. IAM is, therefore, a high-priority subject on the agenda for many boards of directors.

The traditional, larger IAM enterprise solutions are no longer suitable for most organizations. Those solutions are costly, not flexible and require specialized management staff. Cloud-based IAM solutions, on the other hand, are easy and quick to implement. They are simple to modify, maintain and keep in accordance with the latest security standards. The speed of implementation and adoption combined with the lack of required, specialized personnel translates to considerable up-front and long-term savings.

HelloID IDENTITY AND ACCESS MANAGEMENT AS A SERVICE

The HelloID platform by Tools4ever offers organizations the possibility to transition from on-premise to entirely cloud infrastructure, supporting a “cloud, unless” strategy regarding Identity Management. HelloID equips organizations with a full cloud-based IDaaS platform that will make them future proof.

HelloID comprises three components:

1. **Access Management**, responsible for managing employee access to the various applications.
2. **Self Service and Workflow Management** enabling employees to request and administrators to enforce changes automatically to the network settings without contributing to the helpdesk’s workload.
3. **Data Management**, easily managing and securing employee access to files and other business data.

These combined components, further elaborated upon in the following pages, offer organizations the foundation to quickly and securely manage user identities. Taking the existing structures at the time of implementation as the starting point, it is possible to realize a full-fledged Identity Management solution with limited investment. Further, HelloID’s short-term roadmap includes additional cloud-based modules, including Provisioning and Self Service Password Reset. Currently, these modules are already available in Tools4ever’s on-premise product portfolio (UMRA and IAM), which integrates seamlessly with HelloID.

An essential condition for a cloud-based IAM platform is that the solution is safe and sufficiently secured, particularly as cloud security concerns have traditionally been the largest impediment to adoption. As the supplier of HelloID, Tools4ever can demonstrate this protection through periodic intrusion detection and penetration testing conducted by Deloitte Risk Services. Organizations using HelloID can demonstrate that Tools4ever takes sufficient measures, available for presentation to external and internal auditors.

ACCESS MANAGEMENT

With the rapid rise of cloud applications, more and more data is stored outside of the organization's network environment. This trend poses significant challenges for access management and security, as end users desire effortless access to IT resources. This access must be well-controlled and manageable to optimally secure data outside the corporate network, protecting your business data and assisting compliance measures aimed at the increasingly strict laws and regulations.

CENTRAL ACCESS MANAGEMENT

Without an Access Management solution, the security is decentralized and controlled remotely by the various cloud-application suppliers. To ensure data security and to comply with "strong authentication" requirements, these vendors develop their individual authentication processes, pushing login challenges onto to their customer organizations. Instead, organizations desire a consistent and uniform login process that they can easily control. For the end user, the numerous credentials contribute to login fatigue and create barriers to efficient execution of their duties. Furthermore, nobody wants to juggle multiple two-factor devices. It makes the login process unnecessarily complicated, requiring extra time and potentially compromising security.

USER EXPERIENCE

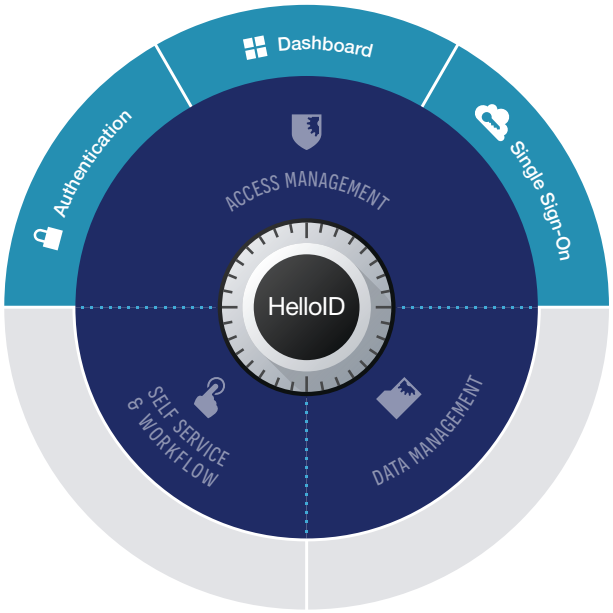
HelloID offers employees, partners and even customers easy and unified access to cloud applications. The end user is only responsible for remembering one web address instead of various URLs for each application. Also, the end user only needs to authenticate at the central directory, such as Active Directory, identifying themselves with their username and password. This verification can be expanded with a two-factor authentication step for additional security. After that, the end user no longer requires to log in to other cloud applications (SSO).

STAGES HelloID ACCESS MANAGEMENT

End users pass through three distinct stages of access management when interacting with HelloID's login process:

1. Authentication

The first step is the authentication of an end user, which takes place via a login prompt with username and password. Optionally, a two-factor authentication step can be added for additional verification.



2. Dashboard

After successful authentication, the user is granted access to a dashboard of recognizable, cloud application icons. The icons available are dependent on an individual user's resources and permissions, only displaying those for which access has been given. Each icon serves as the link to its respective cloud application, simply presented in a visually appealing layout within the portal or a mobile dashboard.

3. Single Sign-On (SSO)

Depending on the cloud application authentication protocol, HelloID uses the relevant SSO protocol to automatically identify and authenticate end users downstream into the cloud application. HelloID supports all popular SSO protocols (e.g. SAML, HTTP(S), OAuth). For applications that do not support any SSO protocol (correctly), HelloID uses a browser extension that allows a "catch-all," ensuring a consistent SSO experience for the end user.

Thanks to HelloID, the end user logs in once to access all their available applications through a clear dashboard – from any location, on any device. In the following pages, we will explain the three stages summarized above in greater detail.

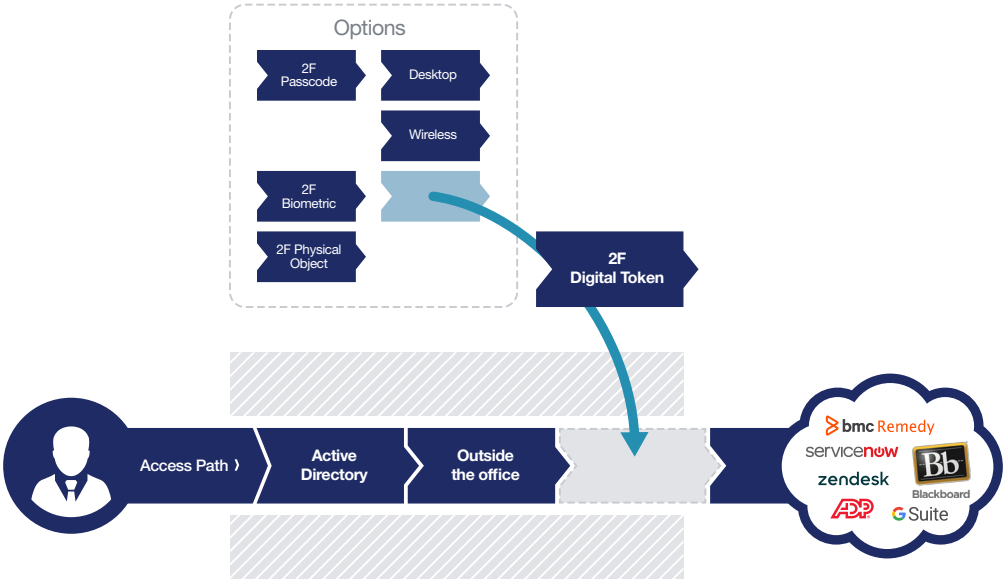
AUTHENTICATION

Logging onto HelloID will usually be achieved via the Active Directory. HelloID also supports other Identity Providers such as SAML, LDAP, and Azure, or you could alternatively use the login of the local HelloID directory. As an example, the local HelloID directory can be used to control access for the organization's clients or patients without creating these users in Active Directory or another Identity Provider. HelloID offers complete, highly cost-effective provisioning technology.

Subsequently, a second verification layer may be required to authenticate the user before granting access. This is a 2FA (Two-Factor Authentication) check. In addition to soft or hard tokens and SMS, different one time passwords (OTPs) are also supported as a 2FA option. Depending on the organization's need, HelloID offers a variety of integration options, including Radius Client Integration. Biometric options such as facial recognition are in development.

The entire login process is governed by easy-to-configure access policies available in the management portal. It is possible to set extended access rules based on - among other things – network, network type, location, time, device and application. HelloID's administrator determines who, and under what conditions, will gain access to the portal or the underlying applications. For example, it is possible to block access from an external network, tablet or smartphone as well as from abroad or at specific times, such as outside office hours.

The authentication process is automatically monitored, with reports readily available regarding who has started which applications, at what time and from which location. This not only provides a detailed picture of the authentication path but also shows failed login attempts and attempts made via suspicious IP addresses. This makes the authentication process transparent, verifiable and adjustable. Possible threats can be identified in good time to take countermeasures - something not only desirable, but required by the new laws and regulations.

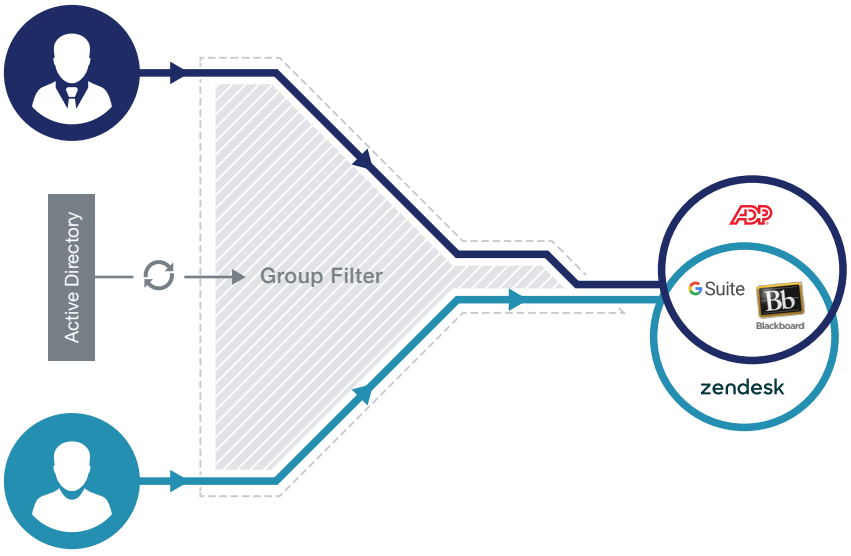


DASHBOARD

After successfully logging in, end users receive access to an online dashboard (or desktop), with the displayed icons allowing instant access to the linked cloud applications. What cloud applications are displayed depends on the role of the employee within the organization – only showing those to which they have been granted permissions. Employees can be linked to a particular group within HelloID based on their department, function, location, etc. Each group provides authorization for certain applications, easily facilitating administrators' control over who can access which cloud application.

For example, HelloID's integration with Active Directory makes it possible to place users in AD groups and synchronize with SSO groups, saving administrators a lot of work. For example, the membership of an AD group determines whether an employee is allowed to accesses a cloud application and/or requires 2FA - without any additional or manual administration actions in HelloID.

Further, the layout of the dashboard is fully customizable to the particular needs of the organization. In addition to a default layout, HelloID offers options for integrating custom stylesheets, CSS links, or other links. The end user API makes it easy to integrate the dashboard into social intranet applications like TripTic, Embrace , Google Sites or Sharepoint Online.

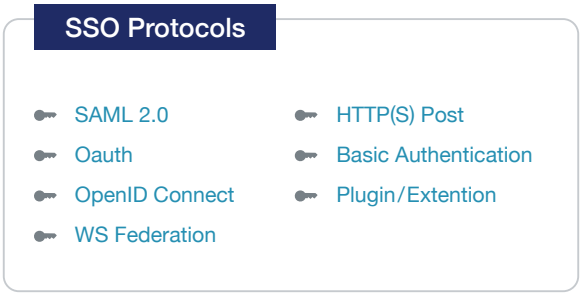


SINGLE SIGN-ON (SSO)

Once the user has authenticated to the HelloID dashboard, it is possible to automate downstream authentication to other applications. The HelloID dashboard provides the user with an overview of available cloud applications, while the central HelloID portal manages the authentication to applications. This eliminates the need for users to login each time for the specific applications. The HelloID portal remembers the user and verifies the user's identity automatically on the other system (automated login).

To enable automated Single Sign-On (SSO) for the various applications, HelloID supports all existing SSO protocols such as SAML, HTTP(S) Post, OpenID connect, Oauth, WS Federation, Basic Authentication. Even with legacy applications or if a vendor does not support any SSO protocol (correctly), HelloID still provides SSO for user convenience via a browser extension that enables a 'catch-all.' This guarantees SSO access for all end users.

While the HelloID portal saves the link between the HelloID identity and the various applications, authentication to the portal and authentication to the various applications are separated for security purposes. This means the tokens are retrieved only during an access request, rather than stored somewhere a malicious intruder could easily access them should they gain entry. The user can terminate the session without having to sign-in again, quickly closing the applications and minimizing the risks of improper use. As stated earlier, the organization is in control over who can access which applications.



RADIUS – HARDWARE AND SOFTWARE TOKENS

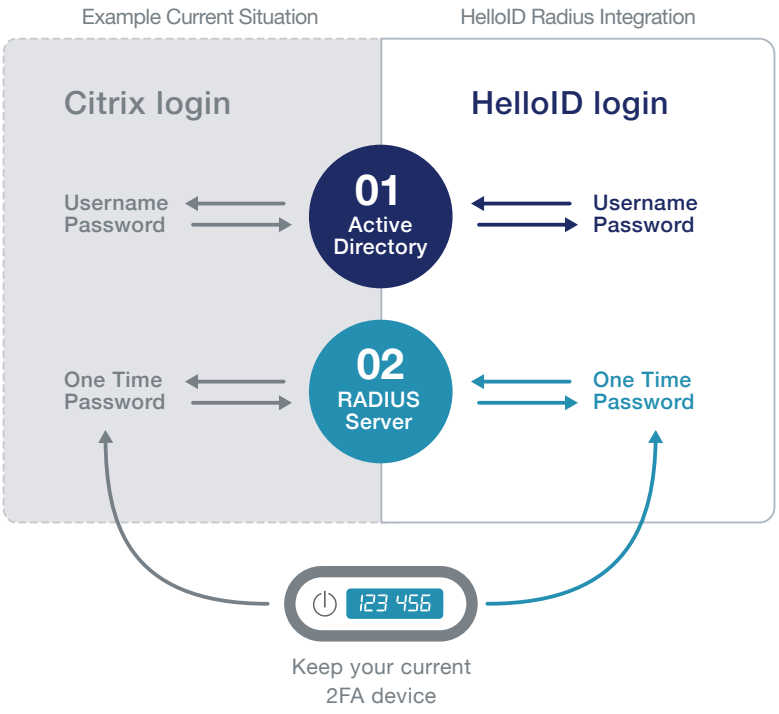
RADIUS (Remote Authentication Dial-In User Service) is the industry standard for integration between hardware and software tokens. HelloID offers RADIUS integration to enable organizations to continue using already purchased tokens and 2FA provided by existing vendors. HelloID's RADIUS integration provides savings by ensuring previous investments in 2FA are maintained and employees do not have to learn how to use new 2FA.

RADIUS is utilized when employees log into the corporate network from home or remote location with hardware and software tokens via Remote, VPN or RDP access. End users are often already familiar with these types of tokens. Especially in these situations, access to HelloID and the data must be made safe by requiring strong user authentication – which in many cases is already mandated by law or regulation.

The RADIUS authentication process in HelloID proceeds in two steps:

1. Once a user requests access, HelloID first carries out the initial authentication.

2. Second, the integrated HelloID-RADIUS client sends an access request to the RADIUS server. The RADIUS server then executes various controls set by the organization. Once the request is approved, a one-time token needs to be provided. If this is correct, the user receives access to the portal.



SELF-SERVICE & WORKFLOW

These days, it has become standard practice for an organization to provide all kinds of services to their employees via portals. Where you previously received your payslip via (e)mail, you can now view them online in the eHRM portal. The same principle applies to self-service portals for facility management, planning, and other business processes – and with HelloID, it is now available for requesting SSO resources and applications.

Across all of IT, more and more services are offered via self-service. Instead of calling or sending an email, a request is entered into TOPdesk, ServiceNow, Zendesk or another IT portal. In many cases, further processing is still a manual task requiring a ticket at the IT helpdesk for someone to execute.

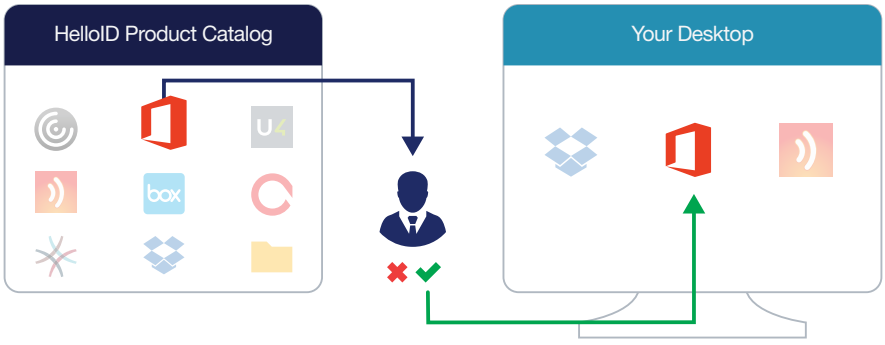
The next step in an organization's technological maturity is automating these tasks. HelloID's Self-Service functionality provides this automation easing the helpdesk's workload, making facilitation simple and improving organization-wide efficiency and turnaround. For example, HelloID makes possible Self-Service and service automation within TOPdesk, Zendesk and ServiceNow because these and most other portals are web-based, integration is quick and straightforward.

HelloID makes it possible to assemble a product catalog of applications and resources to make available to the organization. The management of this product catalog is very straightforward, and the attractive user interface ensures wide acceptance among users. The product catalog is built and maintained by automated rules within HelloID. These rules assure that changes to the infrastructure are processed automatically.

For example, a newly created network share will automatically appear in the product catalog where, based on the network settings, employees will immediately see who has access to that share. Employees can apply for access, and the managers responsible for the employee or the share can approve requests. HelloID offers additional controls, such as email approval or temporary approval, to prevent a user's accumulation of access permissions that threatens compliance and Segregation of Duty (SoD) principles.

Several PowerShell commands are available within HelloID for interfacing with the network. In addition to the standard set included, commands are customizable and additional can be added by the IT department or an implementation consultant. HelloID includes the GUI necessary for executing the PowerShell commands.

In this way, employees and managers can quickly and easily request or manage access permissions without the intervention of the IT department. The manager has direct insight into which employees are active in a department and which licenses, applications, shares and more are in use. All changes are conducted and recorded uniformly. HelloID's Self-Service capabilities sharply reduce the workload on the helpdesk department and enhances the IT department's professional image.



DATA MANAGEMENT

One of the most time-consuming tasks for the help desk is managing access to folders and shares. To collaborate efficiently, employees need to be able to share files. To grant an employee access to certain folders and shares, a helpdesk employee must perform a series of manual tasks on the file system and Active Directory. Manual methods always carry the risk of mistakes – such as naming errors, employees who are never denied access, necessary AD groups that are not created.

HelloID Data Management fully automates this process. A project manager, department manager or assistant can independently manage access to folders and shares as a “data owner” without the intervention of the help desk. Other employees can send access requests directly to the data owner. HelloID automatically creates groups, grants employees access to the right groups, creates folders, creates Access Control Lists (ACL’s) in directories, and all other necessary actions for “data owners” to create and manage shares.

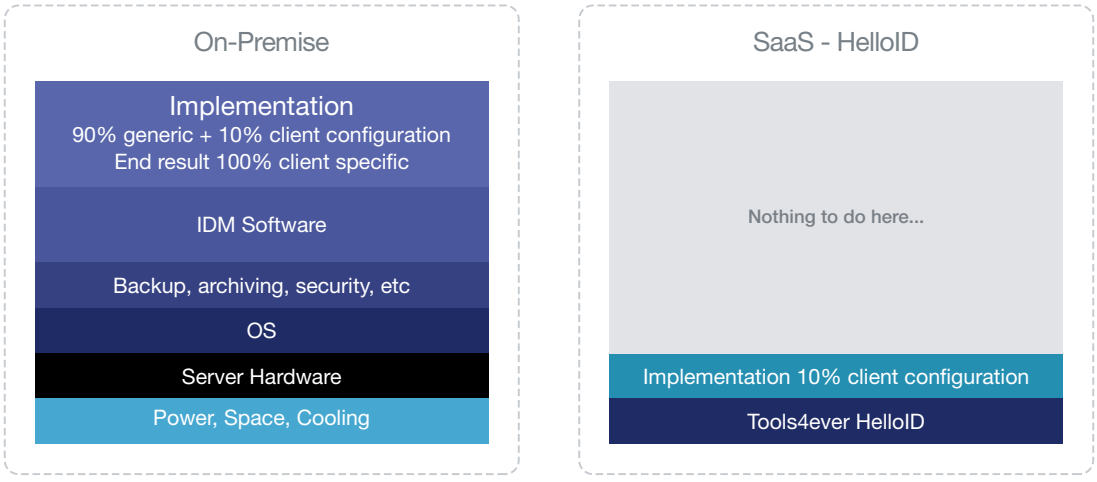
TOOLS4EVER

IAM IN THE CLOUD

Organizations increasingly benefit from the cloud services such as Identity as a Service (IDaaS). The choice to utilize an IDaaS such as HelloID gives an organization greater flexibility than traditional, on-premises offerings. The Identity and Access management (IAM) tools offered within HelloID integrate seamlessly across your organization's network to provide access and security to all of your cloud-based resources.

An organization implementing IDaaS no longer needs to invest in its own infrastructure: hardware, storage, security and identity management software. Following the implementation, easy configuration, administration and ongoing maintenance directly lead to savings by removing the need for specialized personnel. When the organization is responsible for providing local resources, server space, experts, version management and updates, IDaaS becomes a very clear answer.

HelloID's IDaaS implementation takes a mere matter of hours, requiring only the installation of a lightweight agent. Tools4ever automatically provides updates incorporating the latest functionality by using a worldwide-shared configuration that automatically updates. A general rule of thumb is that 90% of an implementation is standard, with only the other 10% being customer specific. This all-embracing standardization ensures that the organization is only responsible for the simple management of the 10% of HelloID comprising customer-specific settings. The lower costs and minimal administration do not arrive at the expense of control and security. On the contrary, Tools4evers IDaaS runs on a highly secured Azure environment, which Deloitte Risks Services thoroughly tests every 6 months. This ensures compliance with the most strict security requirements.



ABOUT TOOLS4EVER

Tools4ever is one of the largest vendors in Identity Governance & Administration with more than 5 million managed user accounts. Since 1999 Tools4ever has developed and delivered several software solutions and consulting services, such as Identity & Access Manager (IAM) and HelloID (IDaaS).

Tools4ever has many integrations and strategic partnerships with software vendors. This software is used by these vendors and vice versa. For example, Tools4ever works with software from TOPdesk and TOPdesk works with our software.

Tools4ever's Identity Governance & Administration solutions are installed in organizations from various sectors ranging in size from 300 to over 200,000 user accounts.

TOOLS4EVER

IDENTITY GOVERNANCE & ADMINISTRATION

TOOLS4EVER NEW YORK

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

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