v1.03 | 2017 10 26

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

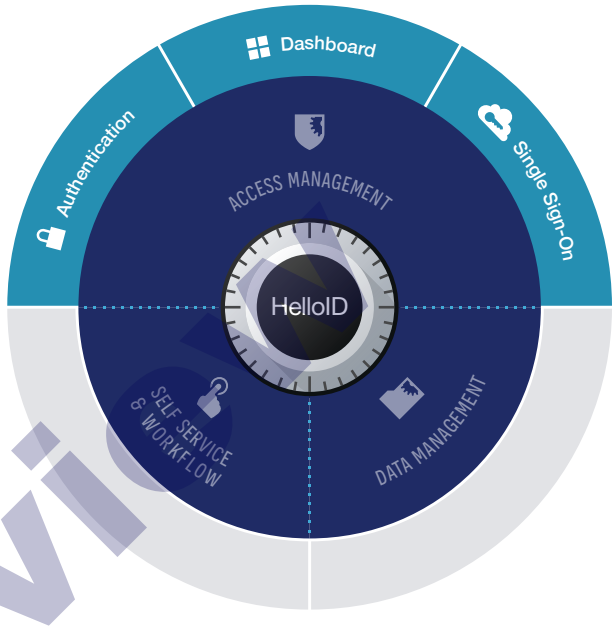
Without an Access Management solution, the security is decentralized and controlled remotely by the various cloud-application suppliers. To ensure data security and to comply with "strong authentication" requirements, these vendors develop their individual authentication processes, pushing login challenges 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 is no longer required 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.

This concludes the preview of this Tools4ever white paper. For the full version, please register for access to our white paper library at Tools4ever.com.

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