TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

HelloID Security Whitepaper

ENHANCED SECURITY AND COMPLIANCEWITH SINGLE SIGN-ON

Index

Introduction

HelloID is a cloud-based Identity-as-a-Service (IDaaS) solution that provides Single Sign-On and Identity and Access Management (IAM) as part of its capabilities. Single Sign-On (SSO) ensures your employees" access to all their business applications and data via one portal, requiring only a single username and password. In addition, HelloID also contains service automation and provisioning modules. Development and integration of HelloID's access governance functionality is well underway.

With its enhanced Signle Sign-On functionality, HelloID supports all business applications—from online cloud to on-premise applications. Integrated MFA and HelloID's numerous, configurable access policies help secure and facilitate easy access for every implementation.

Security is the central theme when deploying Single Sign-On (SSO):

- SSO seamlessly blends protections directly into the overall login process to inherently combine intuitive use, security, and compliance assistance. Reducing credential requirements to just a single username and password simplifies access, fosters a more disciplined security culture, and supports compliance with new data and privacy laws.
- The SSO solution itself provides greater security through its protected 'single point of access", which is to say that the solution's own security must be a key consideration throughout research, implementation, and deployment.

This white paper examines these security topics within the cloud-based IDaaS solution, HelloID. Please read this document in conjunction with two other Tools4ever white papers:

- The HelloID white paper, which provides an introduction to the full HelloID functionality, characteristics and benefits.
- The Tools4ever Key Cloud Principles white paper, which explains our overall vision regarding the use of cloud technology for Identity and Access Management solutions.

In this white paper, we focus on the security principles as supported by and implemented in the HelloID solution itself. We address the following topics herein:

- How the HelloID solution enhances security and helps companies to become more compliant with data protection and privacy regulations.
- The architectural and design choices made to provide security throughout the complete HelloID solution—including automation, provisioning, MFA, and access governance functions.
- How the HelloID solution is independently tested against clear security requirements and relevant standards and how this is verified and certified.

1. HelloID solution overview

With over 20 years of experience in Identity Management solutions and over 10 million active users in the US, Netherlands, UK, Germany, and France, Tools4ever is an Identity Governance and Administration market leader. We serve a wide range of organizations across all industries that vary in size from 300 to over 200,000 user accounts. HelloID, developed initially as a cloud Single Sign-On platform, is one of our key solutions.

HelloID equips organizations with a fully cloud-based IDaaS solution that will "future-proof" your IT environment. This Tools4ever platform enables the transition from on-premise to an entirely cloud-based infrastructure. It supports a "cloud, unless" Identity Management strategy.

HelloID comprises three components:

1. Access Management: managing employee access to various applications.
2. Service Automation: enabling both employees to request and administrators to enforce
3. Provisioning: connecting source systems like HR and planning to resources in the network, enabling automation for onboarding, transferring, and offboarding user accounts.

HelloID's components provide organizations with a comprehensive foundation for securely managing user identities. Regardless of your existing environment, business processes, or other structures, HelloID helps any organization achieve a fully-fledged Identity Management solution. Rapid implementation and intuitive management controls facilitate HelloID's adoption and substantial impact throughout an organization's entire scope of operations—maximizing value and minimizing ROI timelines.

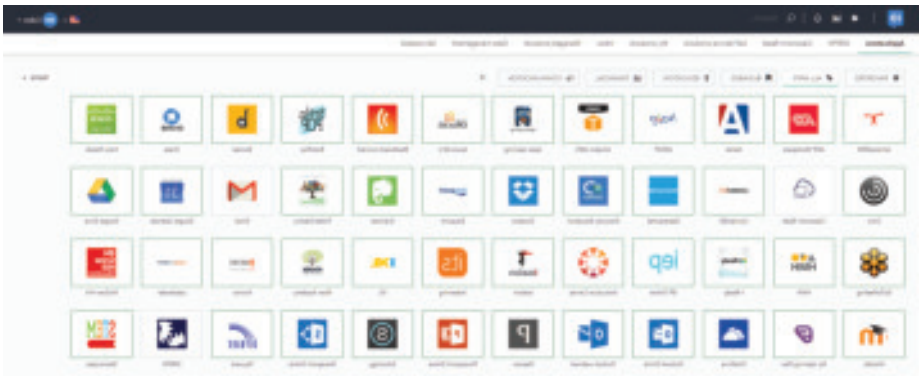
HelloID's short-term roadmap includes modules to fully automate role management in any organization, such as Access Governance. The functionality provided by these modules is already provided by Tools4ever's on-premise product portfolio (IAM and UMRA), which integrates seamlessly with HelloID.

1.1. HelloID Single Access Management

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

Authentication: The first step is the authentication of an end user, which takes place via a login prompt requiring a username and password. Optionally, a Multifactor Authentication (MFA) step may be added for additional verification. MFA requires completing at least one, further login prompt using a specific credential format (e.g. pin code, One-Time Password (OTP), token). Contextual information such as login time, login location, or browser type may also be used to verify access.

Dashboard: After successful authentication, the user is granted access to a dashboard of recognizable, cloud application icons. The available icons depend 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, presented in a simple, visually appealing layout within the portal or a mobile dashboard.



Single Sign-On (SSO): Depending on a given cloud application's authentication method, HelloID uses the relevant SSO protocol to automatically identify and authenticate end users "downstream" into that application. For applications that do not support any SSO protocol, HelloID uses a browser extension that provides a "catch-all", ensuring a consistent SSO experience for the end user. The plugin serves as a de facto password management solution. The passwords are stored centrally in HelloID.

Thanks to HelloID, the end user only logs in once to access all their assigned applications and resources through a clean dashboard—from any location, on any device.

1.2. From on-premise SSO towards cloud-based SSO

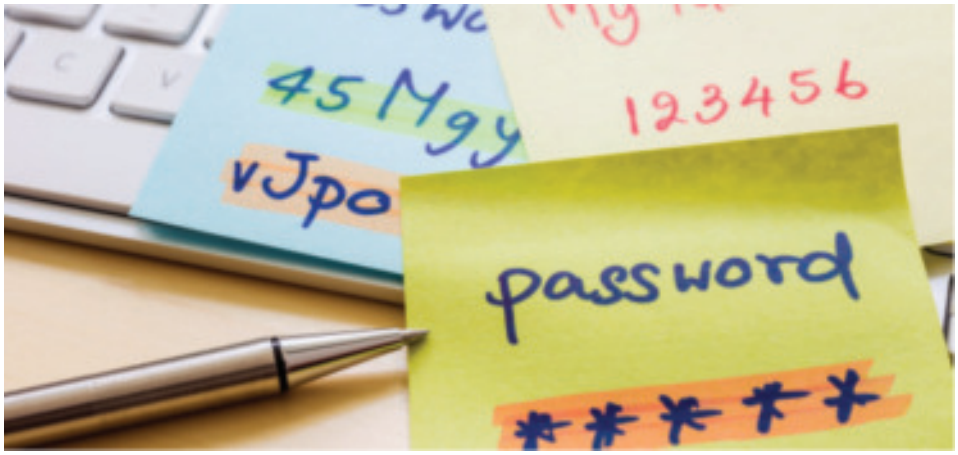
RightScale's 2018 cloud survey illustrated that 96% of companies already use the cloud today—92% of which already use public cloud infrastructure. On average, organizations use 4.8 different cloud offerings across the full range of private, hybrid, and public services. [1]

Tools4ever's customers have been rapidly migrating their IT landscapes to the cloud. The key driver behind cloud migrations has been the need for greater flexibility and adaptability. Additionally, cloud technologies provide organizations a cost-efficient method to focus on optimizing core business operations. As part of these widespread migration strategies, our customers also demand our Identity and Access Management solutions to be cloud-based. We are listening.

Given these demands and our firm belief in cloud technology, we started adapting our Identity Governance & Administration solutions from requiring on-premise implementations to being fully cloud-enabled. Our first implementation of a "cloud-only product", HelloID, is fully designed, developed, and tested for public cloud deployment—a milestone for Tools4ever.

2. HelloID supports privacy, security, & compliance assitance

Single Sign-On helps to mitigate the “password fatigue” and identity chaos that occur when users must remember an excessive number of passwords as part of their daily life. SSO requires users to remember only one username and password, logging in just once to access all their applications. This result also greatly assists IT administrators in spending more time on tasks that matter instead of handling helpdesk calls related to forgotten passwords.

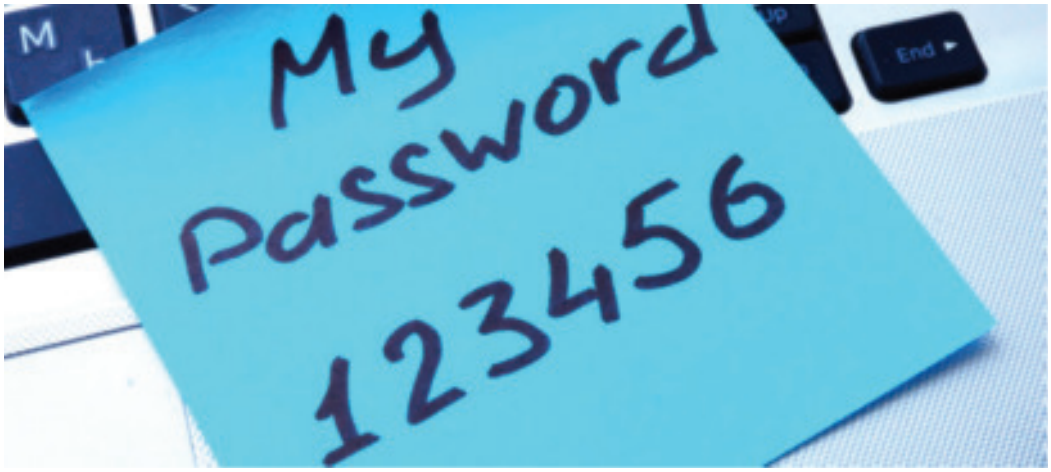


Unfortunately, this scenario may lead some to incorrectly regard SSO’s purpose as primarily focused on usability. Even worse, management might be concerned that the single set of credentials introduces a major risk. This mistakenly portrays SSO as merely a single gateway between the unauthorized users and full, unrestricted access to the organization’s applications and data.

In this chapter, we elaborate upon Tools4ever’s vision of SSO as an inherently strong foundation for providing secure access management at any organization. Consequently, the result similarly supports far better compliance with data protection and privacy laws.

2.1. SSO fosters the use of secure passwords

If users must remember multiple usernames and passwords, they immediately start to search for workarounds. Systems become unsecured with practices such as writing passwords down on sticky notes. Alternatively, people rely on simple and extremely vulnerable passwords. In 2018, “password”, “123456” and “qwerty” were still in the top-10 of the most common passwords. [2]

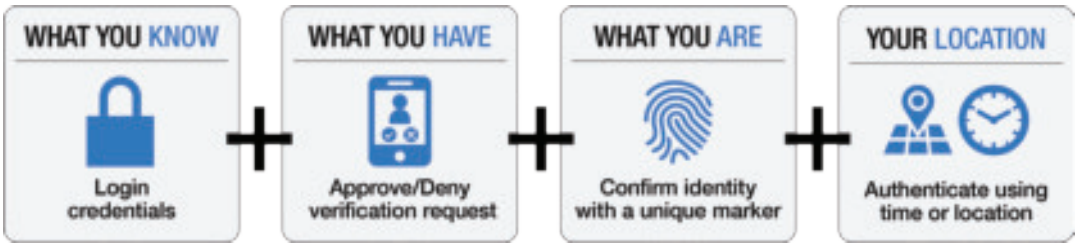


To mitigate this issue, Single Sign-On allows employees to eliminate their extensive set of credentials and remember only a single user name and password. Since only one password is used much less frequently, complex passwords and passphrases become significantly less problematic. This approach also helps organizations more easily enforce password change policies and integrates with password reset software to better facilitate periodic password changes.

Therefore, SSO often shepherds a change from vast collections of very weak passwords towards a single, strong, well-protected, and well-managed password. In the ideal scenario, strong username/password combinations for all applications are generated automatically in the backend per application. This way, the end users are only able to access the applications through the SSO portal.

2.2. SSO supports strong authentication

Single Sign-On allows companies to implement strong authentication with Multifactor Authentication (MFA). This enhances security by requiring users to enter a second code or credential to access the system or application. This additional credential may be delivered to the user via a dedicated client, SMS, or another method during a set window. While MFA provides greater security, end users will still seek workarounds unless the SSO solution eliminates any further need for additional credentials after login. HelloID supports MFA by default and is configurable according to the user, location, or time.



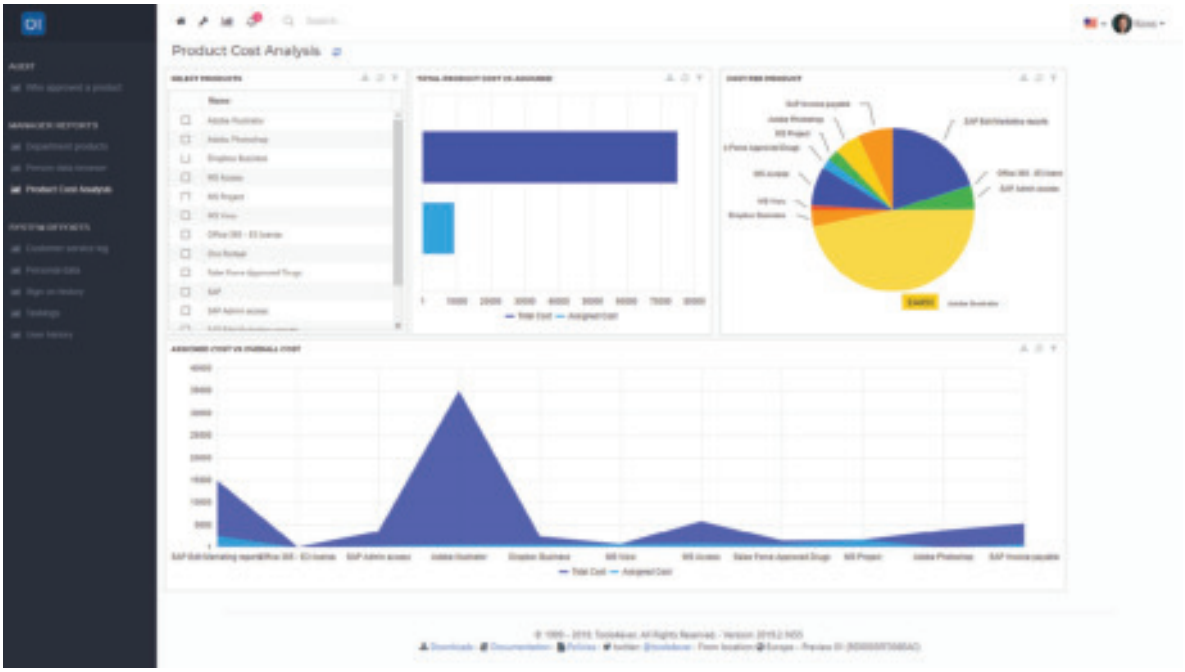
2.3. SSO facilitates the introduction of individual accounts

For compliance reasons—specifically regarding GDPR, HIPAA, SOX, and other regulations—organizations must document what each employee is doing on the company's network and prove that people may only access data relevant to their role. In many organizations, employees share generic accounts with other coworkers, meaning that they all log in with the same credentials to access systems and applications.

As it is impossible to determine which employee did what while logged in, organizations should eliminate shared accounts. However, eliminating these accounts forces employees to remember several new sets of credentials for each system or application. A Single Sign-On solution solves this issue and easily streamlines the change from shared accounts to individual and monitored accounts for everyone. With an SSO solution, each employee will be required to remember a single set of credentials whose value is unique to them. This allows the organization to eliminate shared accounts and become compliant with data protection and privacy laws without drastically disrupting business procedures.

2.4. HelloID supports easy audit trails

Complying with industry regulations requires a complete audit trail of all users. SSO solutions should automatically compile audit trails through their central database, logging all user activity along with an encrypted copy of every users" unique credential set. This database must also report exactly which user accounts have access to what applications along with the dates and times access occurs. Logged events include successful and failed logins, geographic location of the user devices used, password resets initiated, application access attempts, and access failures due to configured policies. The logs allow organizations to securely store this information for as long as regulations require and easily pull audit trails whenever necessary—even years after a given event.



4. HelloID solution security

As described in the previous chapter, HelloID's SSO functionality fosters the use of secure passwords and strong authentication while facilitating the use of individual accounts and compiling audit trails. Since SSO's 'single point of access" provides users with full access to the complete range of applications and data assigned to their role or job function, the solution demands an inherently strong and well-maintained architecture. In this chapter, we will summarize the fundamental principles we incorporated during development to ensure an optimally secured SSO solution.

3.1. Security design, development, and deployment principles

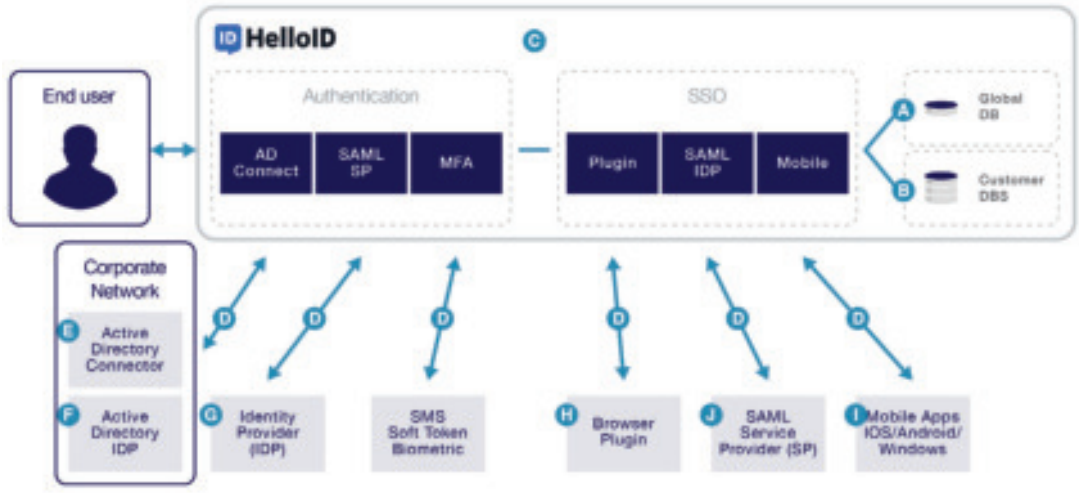
The way we design, develop, and maintain our solutions is based on a set of key principles described below. The 'security by Design Principles" as defined by OWASP forms our approach's foundation.

1	Minimize attack surface area	Our aim for secure development is to reduce the overall risk by reducing the so-called "attack surface area". Every feature added to an application adds a certain amount of risk to the overall application.
2	Establish secure defaults	By default, we deliver a maximally secure user experience. It is up to the application user—within his or her mandate—to reduce the default security configuration.
3	Principle of least privilege	Accounts, by default, have the minimal privileges required to perform the necessary business processes. This covers not just user rights, but also resource permissions like CPU limits, memory, and network and file system permissions.
4	Principle of defense in depth	Even when one control would be reasonable, we prefer more controls in order to approach risks in different fashions. This principle can make severe vulnerabilities extraordinarily difficult to exploit and, thus, less likely to occur.
5	Fail securely	An application may fail to process transactions for a variety of reasons. However, the result of such a failure determines whether an application is secure or not. All HelloID components are designed for a 'secure fail."
6	Do not trust services by default	Third-party partners will typically have different security policies and procedures than we do. Therefore, we do not implicitly trust externally-run systems and treat all external systems in a similar fashion.
7	Separation of duties	This is an essential fraud control part of the implemented solutions" process flows. For example, administrators should not typically be users of the application.
8	No security by obscurity	In our vision, the security of key systems should not just rely on hiding details. We consider this a weak security control.
9	We keep security simple	Our approach favors straightforward and simple code instead of overly complex approaches; no double negatives or complex architectures are used unless absolutely necessary.
10	Fix security issues correctly	Once a security issue has been identified, it is important to develop a test for it and to understand the root cause of the issue. When design patterns are used, it is likely that the security issue is widespread amongst all codebases, so developing the right fix without introducing regressions is essential.

3.2. HelloID solution platform

The HelloID architecture consists of several components. **Diagram 1** provides an overview of the most important components and their interaction. Whether information is in transit or is stored (temporarily), the information is always encrypted. The diagram shows what security mechanisms are applied per level. The degree of security differs per level and depends on the extent of impact, risk and technical applicability.

Diagram1: *HelloID architecture components and security mechanisms*



HelloID is hosted on Microsoft Azure cloud

HelloID is hosted on Microsoft Azure's cloud computing platform. Microsoft Azure, our cloud partner, is internationally recognized as a global Infrastructure-as-a-Service (IaaS) market leader and has deployed a cloud infrastructure that fully covers global and local demands. By leveraging their leading and well-structured topology of Geographies, Regions, and Availability Zones, we can guarantee our customers the highest levels of data resilience. Because Azure has data centers around the world, it is possible to place the customer's database in their desired region. Tools4ever has a long-standing Microsoft Gold Partnership and has built up specific security experience working with the Microsoft product suite.

Security is built into the Microsoft Cloud from the ground up, starting with the Security Development Lifecycle. This mandatory development process embeds security requirements into every phase of the development process. The Security Development Lifecycle ensures that the Microsoft Cloud is protected at the physical, network, host, application, and data layers so that their online services are resilient to attack. Continuous proactive monitoring, penetration testing, and the application of rigorous security guidelines and operational processes further increase the level of detection and protection throughout the Microsoft Cloud.

Database security in HelloID

The HelloID database contains global configuration settings and customer information (A). This information is encrypted using an RSA 1024-bit encryption key. The customer database (B) contains all of the customer-specific configurations and user data. All sensitive data is encrypted using an RSA 1024-bit encryption key. Each customer has its own separate database and encryption key.

The customer can configure exactly which user data is available for retrieval from other source systems and stored in the HelloID database. Administrators use the HelloID "attribute mapper" to configure which user attributes from the source system (Active Directory (AD) in this example) will be used in the HelloID database. Thus, if the first name of a user is stored in AD, the customer may choose whether this attribute will be made available in HelloID. This configurable mapping ensures that the HelloID database always remains fully compliant with the organization's privacy and security policy.

Internet communications

The HelloID webserver communicates with components over the internet using HTTPS (D). The level of encryption is TLS 1.2, AES with 256-bit encryption.

3.3. Authentication elements

Authenticating an end user is the first step of a secure login process, facilitated by following the elements described in this section.

Active Directory (AD) authentication

HelloID can use various sources to authenticate users, such as Active Directory. The Active Directory Connector (E) installed on the organization's network facilitates this method for AD. The connector does not synchronize credentials to the HelloID portal; it only authenticates users against Active Directory on a per-use basis. The Active Directory connector uses HTTPS and authenticates to the portal using a shared secret.

The Active Directory Identity Provider (F) is used to authenticate users from inside the corporate network, allowing the users to log in without providing their credentials (Integrated Windows Authentication). If the user is logged in to Active Directory, they will automatically be logged in to HelloID as well.

Authentication via an external Identity Provider

HelloId also supports other Identity Providers (IdP), such as OpenID Connect, Google, SalesForce, Azure, SAML, and LDAP. Alternatively, you can use the login of the local HelloID directory.

For example, it is possible to interact with a SAML-capable, external Identity Provider to authenticate users. This method does not require any form of credential synchronization. HelloID does not store the credentials used to log into the identity provider. Authentication is purely based on SAML standards and HelloID redirects to the IdP portal for authentication and identification purposes. An organization's system administrator manages the certificate used to set up the connection between the IdP and HelloID, and stores that certificate in the organization's database. Please refer to "4.1 SAML – Identity Provider (IdP)" for a detailed description of a SAML connection with an external IdP.

Multifactor Authentication (MFA) as additional verification layers

Subsequently, a second verification layer may be required to authenticate the user before granting access. In addition to soft or hard tokens and SMS, different One-Time Passwords (OTPs) and clients are also supported as MFA options. Depending on your organization's needs, HelloID offers a variety of integration options, including RADIUS Client Integration.

Configurable access policies

Access policies govern the entire login process, with easy, intuitive configuration provided via HelloID's management portal. It is possible to configure extended access rules based on—among others—network type, location, time, device, or application. The organization's HelloID administrator determines who will gain access to the portal or its underlying applications according to what conditions. For example, it is possible to block access based on different criteria:

- Access can be denied from external networks. Geographic restrictions can be set to prevent access from certain locations of countries—including ranges of IP addresses. This feature increases security for companies that do not need access to the portal from the specified countries.
- Time restrictions can be configured—i.e. groups of users can have their access restricted based on the time of day, day of the week, or specific dates.
- Access can be denied based on the device (e.g. tablets or smartphones) or browsers used.

3.4. Portal and Single Sign-On elements

Users are redirected to their personal portal after logging in, where they can open their applications with a single click and without additional login steps. The following elements support this process.

Logging in to applications

To enable automated SSO for the various applications, HelloID supports all existing SSO protocols—such as SAML, HTTP(S) Post, OpenID Connect, OAuth, or Basic Authentication. Even for legacy applications, or if a vendor does not support any SSO protocol, HelloID still provides SSO via a browser extension that enables a “catch-all”. This guarantees SSO access for all applications.

While the HelloID portal saves the connection 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, preventing malicious intruders from easily accessing them. The user can terminate the session without having to sign in again, quickly closing the applications and minimizing the risks of improper use. The organization fully controls who can access which applications.

Browser plugins and mobile apps

HelloID does not store credentials nor any other personal information locally within a browser plugin H. For every new application session, a request is made to the HelloID portal to verify if the user is still logged in and to request the credential details for their chosen application.

HelloID has an app available for every mobile platform (e.g. smartphones and tablets I) to interact with the HelloID portal for primary authentication and for SSO purposes on mobile websites. End users are required to identify themselves once in a configurable timeframe. The timeframe can be set from 0 days to permanent; standard is every 30 days. The IdP credentials are stored in runtime memory, never on the device. For credential management, HelloID uses the same mechanism as for plugins (see H , above). There is no local storage or caching of application credentials.

3.5. Logging and reporting

HelloID logs all important events. These events include successful and failed logins, user location, the devices used, password resets initiated, application access attempts, and access failures due to access policy. These events may be used to create detailed security reports. These reports may be used to identify possible threats and/or provide an audit trail. Reports may be created for the following scenarios (among others):

- Multiple login failures for specific accounts.
- Attempted access when access policies apply.
- Failed Multifactor Authentication (MFA)
- Application access for a specific account.

The logged information may be retrieved using an API for processing by business intelligence tools like PowerBI. HelloID also provides a dashboard, which presents real-time information about these events. Based on this information, access policies may be configured to prevent certain events from happening. For instance, if the information reveals a user is accessing a specific application from a mobile device, and this is against company policy, an administrator may disallow such.

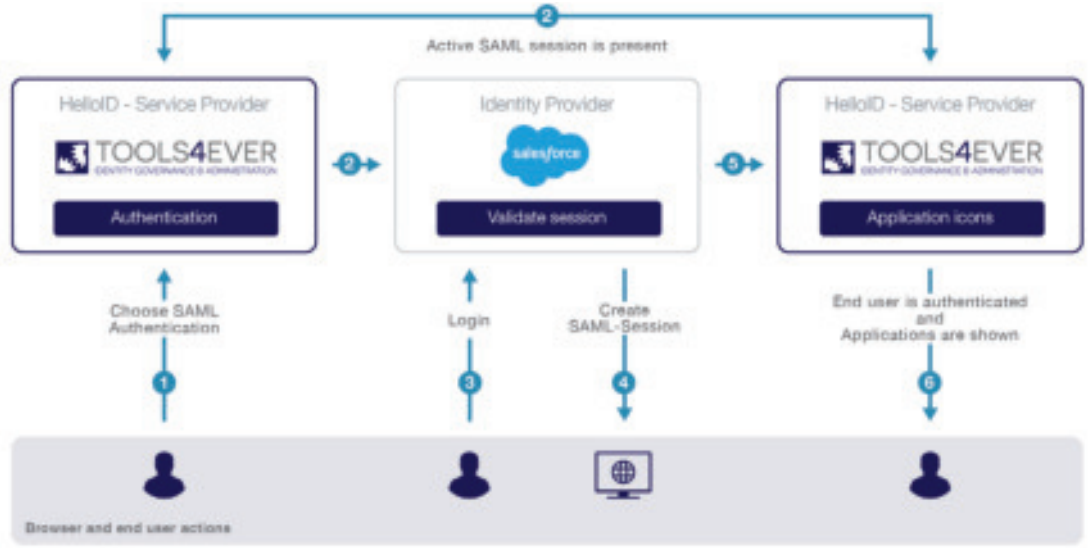
5. Examples of HelloID scenarios

4.1. SAML - Identity Provider (IdP) to HelloID (as Service Provider)

SAML provides the mechanisms to identify an end user using another, trusted 3rd party (the IdP). Common IdPs are Salesforce, Google, and Amazon, but other 3rd parties can easily serve as a trusted IdP. HelloID may be configured to trust any IdP via the SAML 2.0 protocol. Certificates can be exchanged and set by system administrators in the HelloID portal. The certificate information is stored in the customer database, as illustrated in Diagram 2.

Diagram 2: *SAML—Identity Provider (IdP) to HelloID (SP)*

Step 1	The user browses to the HelloID portal using HTTPS. Each client will receive their own unique domain/URL. The first step is authentication of the end user. Multiple authentication methods are available for configuration. The diagram below explains the IdP SAML setup.
Step 2	If no valid SAML session is detected, the user is redirected to the Identity Provider and the user is asked to identify themselves (Step 3). If a valid SAML session is detected, proceed to Step 5.
Step 3	The user logs in to the Identity Provider. HelloID fully trusts the authentication provided by this IdP (as configured in HelloID).
Step 4	After successful identification, a SAML session is created by the IdP and passed to HelloID for Step 6.
Step 5	If a valid session is available, the end user is redirected to the HelloID portal and all the applications that the user may access.
Step 6	The user is redirected to the HelloID portal and is logged in.

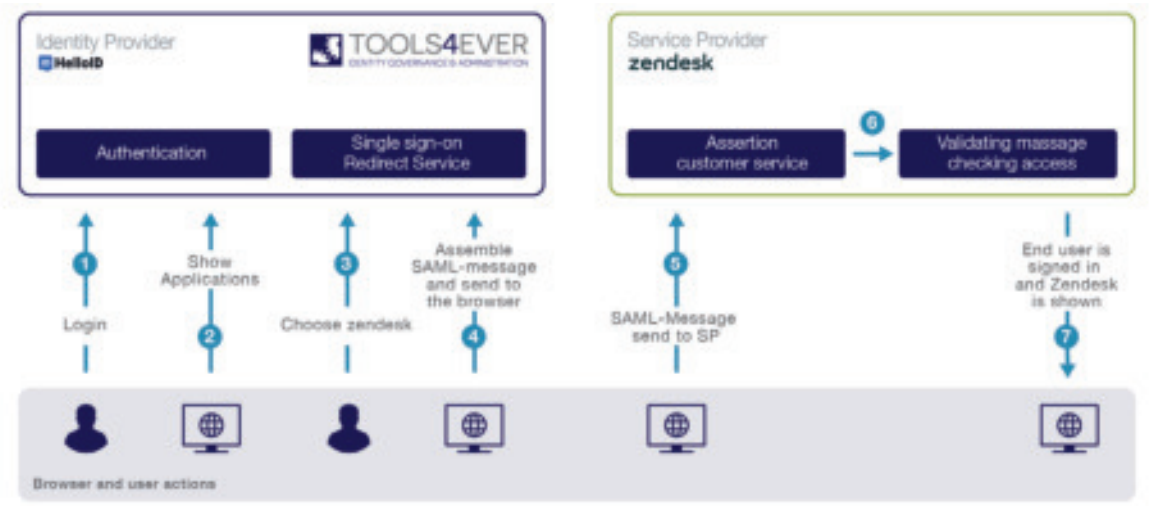


4.2 SAML—HelloID (as IdP) to Service Provider (SP)

The most common and accepted SSO mechanism for web-based applications is SAML 2.0. The protocol is widely adopted and implemented by many different software companies. HelloID can serve as a trusted IdP party for a SAML-enabled application (the SP's 'service"). If successfully authenticated through the HelloID portal, clicking on any application icon on the dashboard will create a SAML-session with the SP to automatically sign in to and access the resource. Please see Diagram 3.

Diagram 3: *SAML—HelloID (as IdP) to Service Provider (SP)*

Step 1	The user browses to the HelloID portal via HTTPS. Each client will receive their own unique domain/URL. The first step is authentication of the end user. The authentication method can vary and is not determined by the portal's SSO protocol. For example, an end user can use Active Directory Connector for authentication and then use SAML to access applications via SSO.
Step 2	HelloID displays the user's dashboard containing all the applications that the user may access.
Step 3	The user chooses the service provider (in this case, Zendesk)
Step 4	HelloID creates a SAML session with/within the browser. The SP determines the most effective session type. This can be a browser memory session or a session stored in a cookie.
Step 5	The browser is instructed to redirect to the service provider.
Step 6	The SAML message signature is validated by Zendesk.
Step 7	The SAML message signature is validated by Zendesk.



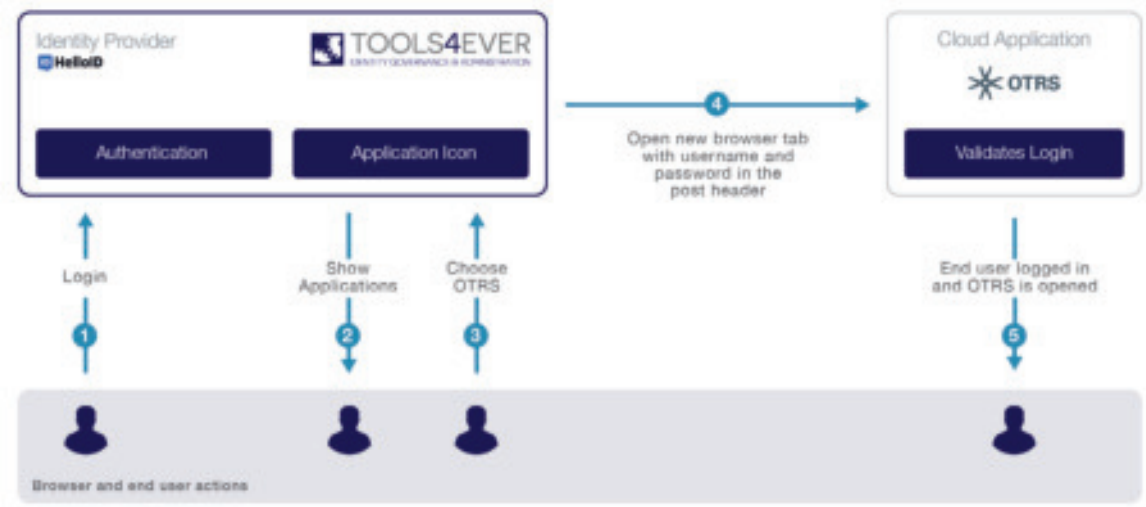
4.3. Form POST scenario

The form POST SSO mechanism relies on putting the username and password in the HTTP POST header sent to the web-based application. This mechanism is also used if a user accesses the given application via the normally-provided website login page (alternatively, user access may be restricted exclusively via the HelloID portal). The login page posts the credentials in the header (client side). The application (server-side) then reads these credentials, verifies them, and authenticates the user.

HelloID can leverage this mechanism to provide SSO capabilities for applications that do not support modern SSO protocols. The end user will experience the same effect as with SAML: a transparent login not requiring any additional user interaction. HelloID supports both HTTP and HTTPS. Tools4ever strongly recommends the latter for its substantial security increase via encryption, whereas the former exchanges credentials in clear, unencrypted text (see Diagram 4).

Diagram 4: *Form POST scenario*

Step 1	The user browses to the HelloID portal over HTTPS. Each client will receive their own unique domain/ URL. The first step is authentication of the end user.
Step 2	HelloID displays the user's dashboard containing all the applications that the user may access.
Step 3	The user chooses the application.
Step 4	The user is redirected to the application with the form POST mechanism containing their credentials.



6. HelloID verification and certification

The deployment of a secure, cloud-based SSO solution starts with the right principles, technologies, and partners—as addressed in the previous chapters. In addition, we also want to provide our customers with as much continual verification and certification as possible that HelloID is independently tested against clear security requirements and complies with relevant standards. Verification and certification are, therefore, important elements of the Tools4ever cloud security policy.

Deloitte Security Scan

At Tools4ever, we consider proactive and frequent testing of our security solutions a cornerstone of our success. Since we develop advanced Identity & Access Management solutions, we have a large number of security experts within our own ranks. They are not only active in developing our security solutions and products; we also run an in-house program in which HelloID is tested on potential security flaws by our own experts on a regular basis.

However, in-house testing is only our first line of prevention. We also have HelloID externally tested twice a year by the top-class, ethical hackers of Deloitte. By selecting Deloitte for this, we have opted for the guaranteed, independent and highly qualified expertise of the market leader in information security. Gartner positioned Deloitte first in global Security Consulting Services for the sixth consecutive year in its July 2018 report titled “Market Share: Security Consulting Services, Worldwide, 2017”. [3]

These external tests keep us sharp, prevent the occurrence of blind spots and provide us with an extra pair of eyes.

The test consists of a large number of attempts by professional, ethical hackers to attack the HelloID solution. These ethical hackers have been trained to look at IT systems from the point of view of an experienced cybercriminal to recognize vulnerabilities that others might overlook. For example, they utilize NCSC ICT-B v2 guidelines and the OWASP Top 10 Application Security Risks of 2013 and 2017.

The tests cover the full range of potential vulnerabilities: from system reports providing too many details to the presence of cross-site scripting (XSS) vulnerabilities. Besides the well-known black box tests, the testers go further and execute “grey box tests”. A “grey box test” looks for security weaknesses in specific parts of HelloID using inside information about the design and operation of the software. Finally, we look at the possibilities for authorized users within the system. Do they have “unintended” possibilities that go beyond what is necessary for their role? This is critical because fraud and cybercrime have been determined to take place most often from within organizations.

Certification

A crucial element in cloud services is compliance with international standards because of their global reach. This element ensures both the correct integration with IT systems in other domains as well as the adoption of the latest security, privacy, and availability developments.

Tools4ever has an active compliance and certification policy. A recent example is our HelloID OpenID certification. This certification confirms the high quality of the OpenID Connect implementation as part of our HelloID Identity-as-a-Service solution, further reinforcing our customers" confidence in the quality of our services.

Our cloud IaaS provider, Microsoft Azure, maintains the most extensive compliance portfolio in the industry both in terms of breadth (total number of offerings), as well as depth (number of customer-facing services) [4]. Compliance covers major, globally applicable standards and certifications. Microsoft's regulatory compliance covers major, globally applicable standards and certifications. In addition, Microsoft complies with both industry-specific and region/country-specific standards and certifications.

7. Conclusion

In this white paper, we discussed the security aspects of the HelloID solution's Single Sign-On capabilities. The paper addresses HelloID's security from two different viewpoints:

- SSO seamlessly blends protections directly into the overall login process to inherently combine intuitive use, security, and compliance assistance. Reducing credential requirements to just a single username and password simplifies access, fosters a more disciplined security culture, and supports compliance with new data and privacy laws.
- The SSO solution itself provides greater security through its protected 'single point of access", which is to say that the solution's own security must be a key consideration throughout research, implementation and deployment.

HelloID SSO facilitates usability, security and compliance

HelloID SSO prevents the use of multiple passwords and the corresponding occurrence of "password fatigue" and identity chaos. The use of a single set of credentials fosters successful adoption of strict password change policies and secure password storage practices throughout an organization. HelloID's configurable access policies make deployment of MFA or other authentication restrictions substantially easier. Since users" individual access to applications becomes much more managed—and manageable—organizations can smoothly migrate from shared to individual accounts. Consequently, organizational compliance with the latest privacy and data security regulations is both simplified and better enforces, while all activities are logged for later inspection, reporting, and audit trails.

Security and integrity of the HelloID solution

Since SSO's 'single point of access" provides users with full access to the complete range of applications and data assigned to their role or job function, the solution demands an inherently strong and well-maintained architecture. Using a clear set of security design, development, and deployment principles, the HelloID solution maximally leverages the security features of Microsoft Azure's Infrastructure-as-a-Service (IaaS). The platform itself supports extensive logging and reporting functions.

Only the necessary data is stored in the encrypted (RSA-1024 bit) HelloID database itself. Using the HelloID "attribute mapper", the customer is in full control over which data is stored in the HelloID database. This helps ensure compliance with your organization's privacy and security policies. As much as possible, data is real-time verified in the connected source systems.

HelloID can be integrated with your organization's Active Directory. It also supports leading Identity Providers such as Google, SalesForce, Azure, SAML, and LDAP. Alternatively, HelloID's local directory is available as an IdP. For application access, HelloID supports all existing SSO protocols, such as SAML, HTTP(S) Post, OpenID Connect, OAuth, or Basic Authentication. For applications that do not support any SSO protocol, HelloID provides SSO via a browser extension that enables a "catch-all". In addition, Multifactor Authentication is available as a second verification layer with additional and extensive, configurable access policies.

HelloID verification and certification

Finally, we want to provide our customers with as much continual verification and certification as possible that HelloID is independently tested against clear security requirements and complies with relevant standards. "Our comprehensive certification program covers regular, in-house testing as well as external verification twice per year by the top-class, ethical hackers of Deloitte—the worldwide market leader in information security."

8. About Tools4ever

Tools4ever has offered a wide range of enterprise security-related solutions since 1999, specializing in Identity Management. Within the Identity Management portfolio, and in addition to user provisioning, Tools4ever offers a broad selection of password management products. HelloID is the most prominent product in this range. Other products within this suite are password synchronization between Active Directory, Mainframe, AS/400, Unix, Lotus Notes, SAP, etc. (Password Synchronization Manager - PSM); password complexity within Active Directory (Password Complexity Manager – PCM); and self-service password reset (Self-Service Reset Password Manager - SSRPM).

Thousands of clients around the world place their trust daily in the correct operation of Tools4ever software. For Tools4ever, the reliability and certification of its software is of utmost importance. Tools4ever has partnerships with the organizations that integrate with our software, including Microsoft, SAP, Citrix, IBM, Novell, and IGEL Technology. All relevant Tools4ever products are certified by Microsoft and Citrix.

Tools4ever has signed a contract with Deloitte Risk Services to uphold the highest security standards. Deloitte Risk Services periodically test HelloID for potential security issues.

9. Cited works

1	RightScale. 2018 State of the Cloud Report: Data to Navigate Your Multi-Cloud Strategy. RightScale. https://www.suse.com/media/report/rightscale_2018_state_of_the_cloud_report.pdf
2	SplashData. “Top 50 Worst Passwords of 2018.” TeamsID. https://www.teamsid.com/100-worst-passwords-top-50/.
3	Deloitte. “Deloitte positioned first by Gartner in market share for Security Consulting Services worldwide for sixth consecutive year.” 5 Oct. 2018. Deloitte. https://www2.deloitte.com/fi/fi/pages/risk/articles/ranked-one-gartner-security-consulting-services.html
4	Microsoft. “Overview of Microsoft Azure compliance.” 17 Jan. 2020. TechNet. https://gallery.technet.microsoft.com/Overview-of-Azure-c1be3942

Contact us

There are a lot of disruptions and responsibilities on a typical CTO's plate. Tools4ever offers a suite of solutions that can alleviate any potential pain point a CTO may have, removing concerns on possible back-end infrastructure issues, or other problems that can arise in daily operations. With Tools4ever, CTOs are finally able to focus on the priorities that matter.

If you would like more information on the subject of IDM solutions or to set up a consultative discussion with Tools4ever regarding steps to improve your organization's IT administration, please contact one of our North American offices (listed below).

For more reading on Tools4ever's IDM solutions and consultative expertise, please visit: tools4ever.com/resources/ or tools4ever.com/references/

Tools4ever's complete range of IDM solutions includes:

- ✓ Identity and Access Manager (IAM)
- ✓ HelloID (Cloud-Based IDaaS & SSO)
- ✓ Self-Service Reset Password Manager (SSRPM)
- ✓ Enterprise Resource Authorization Manager (ERAM)

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

TOOLS4EVER NEW YORK

Address 300 Merrick Road, Suite 310
Lynbrook NY 11563
USA

Phone 1-866-482-4414
Website tools4ever.com

Info nainfo@tools4ever.com
Sales nasales@tools4ever.com

TOOLS4EVER WASHINGTON

Address 11515 Canyon Road E
Puyallup WA 98373
USA

Phone 1-888-770-4242
Website tools4ever.com

Info nwsales@tools4ever.com
Sales nwsales@tools4ever.com