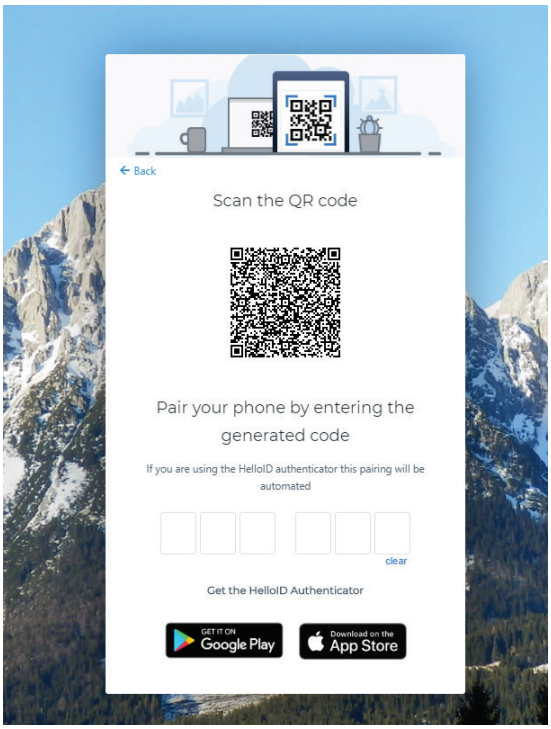
PRODUCT FLYER

HELLOID ACCESS MANAGEMENT

- Do your employees waste a lot of time logging into IT services?
- Do they regularly forget their password and get locked out?
- Is your helpdesk being burdened by a large number of outstanding password reset tickets?

✓ **These problems can be solved with HelloID!**



Nowadays, people have a more user-friendly IT environment at home than at the office. They have easy access to their applications from anywhere on any device. With HelloID Access Management, Tools4ever brings the same ease-of-use to the business world. With a user-friendly dashboard via HelloID, employees can access all their cloud applications with a single click from anywhere on any device. As a cloud-based Identity-as-a-Service (IDaaS) solution, HelloID requires minimal investment and implementation effort.

HelloID: safe, efficient and easy

Accessing all necessary applications can be done quickly using one portal, one username, and one password. Employees no longer need to remember different usernames and passwords or reenter them when switching applications. Single Sign-On (SSO) makes work much more pleasant and efficient while reducing downtime. The IT department also sees the benefit of significantly fewer password reset requests. HelloID Access Management also offers self-service password reset just in case an employee forgets their credentials.

As all users log into one portal to access their IT resources, HelloID also provides greater control over access rights. Multifactor Authentication (MFA) may also be required for advanced authentication security. HelloID recognizes login data (e.g., location and time), and may be configured to implement additional authentication measures accordingly.

HelloID also tracks who uses which applications, at what time, and from what location to provide detailed activity logs. These audit trails and reports may be pulled at any time to demonstrate compliance with laws and regulations (e.g., HIPAA, SOX, ISO 27001, GDPR/AVG).

IT innovation

HelloID Access Management offers employees, partners, and (in some instances) customers uniform and straightforward access to cloud applications. Typically, users log into HelloID via Active Directory. HelloID may be used as an Identity or Service Provider, supporting Azure, LDAP, and all standard SSO protocols (e.g., SAML and OpenID). Users log into HelloID with username and password credentials by default. If desired, cards with a QR code can simplify the login process for students or other specific user groups. After scanning a QR code, HelloID automatically identifies the user and ensures correct access to applications and data.

One digital workplace

HelloID Access Management is seamlessly integrated into the portals of leading intranet and IT management solutions. To this end, Tools4ever actively collaborates with suppliers like TOPdesk, AFAS, SharePoint, and others. Integrating the intranet with the Access Management functionality creates a single digital portal for employees. After logging into the intranet, users have access to a personal portal with information, communication tools, and, via the HelloID dashboard, their own applications and data folders which can be opened with one click, as we are used to at home.

Multifactor Authentication (MFA)

In some cases, you don't want users to log in with only a username and password but have additional verifications for added security. HelloID Access Management offers various MFA (FIDO, push to verify, SMS, email, etc.) methods for free, but also integrates seamlessly with the free Authenticator apps from Microsoft and Google. In addition, already availabe MFA methods and tokens can be used. If various applications (such as AFAS Insite and Nedap ONS) force different MFA methods, you can easily bring this back to one with HelloID. Based on the department, place, time and device, it is possible to set access rules for the portal or specific applications so that you can choose the correct level of authentication for each scenario.

Regulatory compliance

The increasingly strict laws and regulations in the field of audits and security require that use of and access to cloud application is tracked and transparent. HelloID Access Management automatically monitors the authentication process. Reports always provide insight into who has accessed which applications, at what time, and from which location. This provides not only a detailed picture of the authentication process but also shows login attempts from suspicious IP addresses. Potential threats can be identified in time to take countermeasures. This makes the authentication process transparent, verifiable, and adaptable.

Streamlined authentication methods

More and more, individual applications and services are enforcing stricter security through their own, unique authentication processes. However, without a central hub, this effectively doubles both login effort and cost—especially if each provider enforces their own MFA method your organization now has to support.

By contrast, once a user is logged into the HelloID dashboard, SSO protocols ensure automatic authentication into individual resources. For additional security, MFA can be enforced at the application level for resources storing sensitive data. HelloID provides streamlined authentication for all users by eliminating the repetitive and complicated logins each services or app requires otherwise.

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

New York
300 Merrick Road, Suite 310
Lynbrook, NY 11563
(866) 482-4414
nainfo@tools4ever

Washington
11515 Canyon Road E
Puyallup, WA 98373
(888) 770-4242
nwinfo@tools4ever