TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

HelloID – IDaaS Solution

Access Management Key Focus: Easy end-user access for all online resources

Securely access all of your cloud applications from anywhere in the world with a single login. HelloID supports all common SSO protocols. Apply additional security measures with multi-factor authentication and access policies.

Key Features: Single Portal, One Log-In, Chromebook Integration, Custom Branding and Layout, AD User and Group Synchronization, Managed and Personal Applications Tab.

Service Automation Key Focus: Self-service actions.

HelloID's Service Automation module catapults the end user into a self-service enabled world. Utilizing the "Shifting Left" concept, IT can provide a state-of-the-art delegation, workflow management, and real-time status request reporting solution to an organization. This allows IT to focus on big-picture tasks.

Key Features: Self-Service Request for Local Resources, Service Desk for Delegated Interaction (Delete/Add User), Customizable Web Forms, Dynamic Workflow & Approval Processes, Reporting & Resource Tracking

Stakeholder Departments: IT, HR, Student Information, Curriculum

Project Implementation: A dedicated consultant will create a custom instance of HelloID. The initial training session will consist of configurations of IdP and a settings overview. Documentation delivery and direction on application set-up is also included. Additional resources and follow-up meetings are set to assist in ensuring rollout and adoption are a success. Expect about two hours of consultancy before allocating in-house hours toward configuration and customization.

PRODUCT SUITE

IAM – Identity & Access Management

Key Focus: Eliminates Manual Account Processes

IAM stores source data in its Vault, which is then used to create and manage the complete lifecycle of a user account within an organization. Processes such as account creation are automated for multiple applications without IT intervention.

Manual processes, like audits of accounts, are also eliminated with IAM. HR and SIS systems are the source of truth to provision and deprovision accounts to ensure which accounts remain active. IAM also has the capability to export reports of this behavior on scheduled intervals if requested.

Key Feature: Easy-Access Web Portal, Access Governance Model

Stakeholder Departments: IT, HR, Student Information

Project Implementation: Intake begins with client deliverables relating to server requirements and source data. The first phase of the implementation includes incorporating source data to the IAM vault and linking source systems to downstream targets (i.e. AD / G Suite / Office 365). A dedicated consultant then commences training on the IAM portal feature set, Access Governance (AG) model, and reports. AG modeling is built out based on roles and finally, user provisioning is turned on. A more detailed timeline can be found in your project quote, however, expect about 6 weeks for implementation. The initial phases will require the most time for both parties to initiate processes, thereafter, expect up to 1-2 hour per day in direct correspondence with the designated consultant.

SSRPM - Self Service Password Management

Key Product Focus: Easy end-user password reset

Empowers the end-user with the ability to change their own password from their desktop, Chromebook, or other device.

Key features: Chromebook Kiosk App, Web Interface, Custom Branding and Layout.

Most utilized module: Account Claiming

Account Claiming removes the gap from transferring accounts and credentials to new users. Once an account is created, staff can be directed to a portal or receive an email to “claim” their account for the first time, with or without being on-premise, and without the need for ever knowing their initial password. The new user enters in some identifiable credentials about his/herself for authentication purposes. The account is then activated and the user is then given their username and can reset their password. Additionally, the new staff member can enroll in the password management solution during the claiming process. Future instances of password resets are now managed by end users and without the assistance of IT

Stakeholder Departments: IT, HR

Project Implementation: A dedicated consultant will help install this on-premise solution. Options for deployment to the end-user can include your Windows log-in screen, Chromebook kiosk app, and web interface. Google reset links can be redirected to SSRPM’s web interface. Additional training includes an overview of most utilized settings or customization options to cater to your specific environment. Expect about one hour of implementation and consultancy before allocating in-house hours for configuration and password customization.

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

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

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