TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

EMPOWER BUSINESS ORGANIZATIONS THROUGH TECHNOLOGY

Enterprise Identity Management Solutions

23 Years

5 Million+ Active User Accounts

1,500+ Commercial Clients

About Tools4ever

Tools4ever centralizes your organization's identity data from cloud and network systems in order to automate time-intensive manual processes. Our solutions provide your IT staff with the tools they need to standardize user accounts and streamline secure application access through secure portals and intuitive interfaces Partnering with Tools4ever minimizes employee downtime, solidifies infrastructure, and optimizes processes.

Solutions Overview

As a global market leader in Identity and Access Governance, Tools4ever develops and delivers several software solutions and consultancy services. Our solution suite is designed to streamline and automate otherwise manual IT processes:

- Identity & Access Management
- Identity-as-a-Service & Single Sign-On
- User & Downstream Provisioning
- Role-Based Access Control
- Password Management & Reset
- Self-Service & Workflow Management

Trends and Concepts

Continual Cloud Transitions

In 2022, the question is not whether organizations will adopt cloud services, but how many are already in use. Cloud services have reached maturity and are used for mission critical IT services. Check out Tools4ever's "Key Cloud Principles" white paper for more info.

Provisioning

A new hire walks into work on their first day and starts with access to all their accounts; Tools4ever makes this a reality, not a daydream. Automations, email notifications, and data synchronization ensure employees have their resources promptly without consuming all of IT's bandwith.

Single Sign-On

Employees log in once to access all of their applications via a secure portal. A single set of credentials makes login-related employee downtime and poor password management legacy problems.

Onboarding

Getting first-time users up to speed is critical, but providing new employees with their accounts and credentials remains a massive risk in any organization. Secure account claiming portals remove these massive account and password vulnerabilities.

Self-Service ("Service Automation")

If resource requests require running around for approval signatures (in triplicate), your staff is wrapped up in restrictive red tape. Self-service allows users to route requests directly to resource owners or their manager for rapid response and automated fulfillment. Tools4ever's Self-Service functionality is named "Service Automation".

Authentication & MFA

When users log in to their accounts, they must authenticate their identity as a security measure—most often with usernames and passwords. Multifactor Authentication (MFA) provides an additional layer of security for any login process via "Push-to-Verify", One-Time Passwords, authenticator client apps, PIN codes, tokens, and more.

HelloID
Cloud. Identity. Access.

Cloud-based Identity and Access Management

HelloID is a modern and secure, cloud-based Identity and Access Management solution that provides your employees with a user-friendly dashboard containing all of their approved applications. Users only log in once to access their customized dashboard, which can be accessed from any device (e.g., desktop, smart phone, tablet, or web browser).

Highlights:
- Empowers users & increases IT resource adoption
- Connects to any app via Single Sign-On (SSO)
- Reduces management efforts for IT and managers
- Increases security via activity logs & configurable access policies
- Minimizes login-related employee downtime

Access Management & Authentication:
- SSO connects to any app
- Customized dashboard
- Multifactor Authentication (MFA)
- Create Active Directory users
- Available as an Identity Provider (IdP)
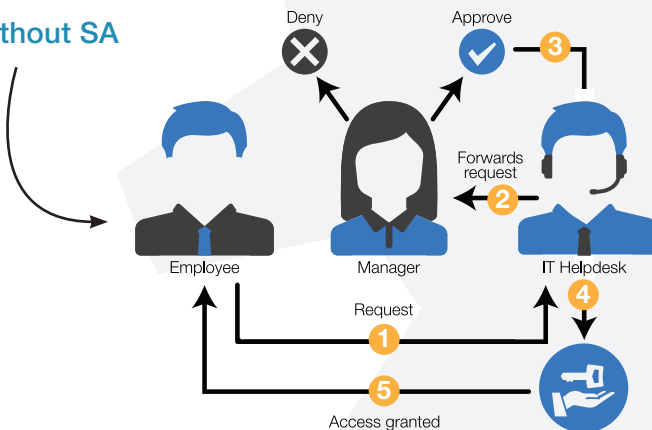- Deloitte Security Testing
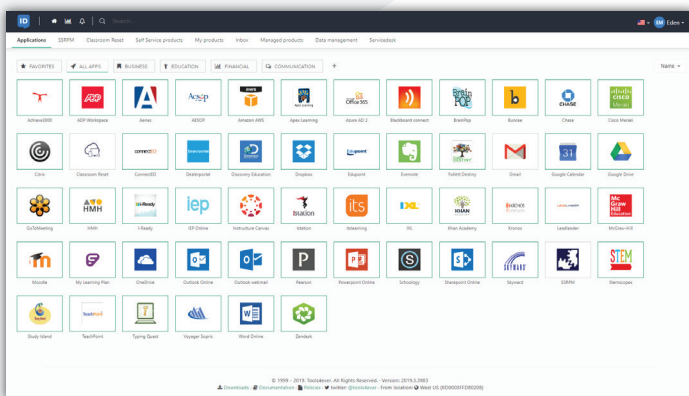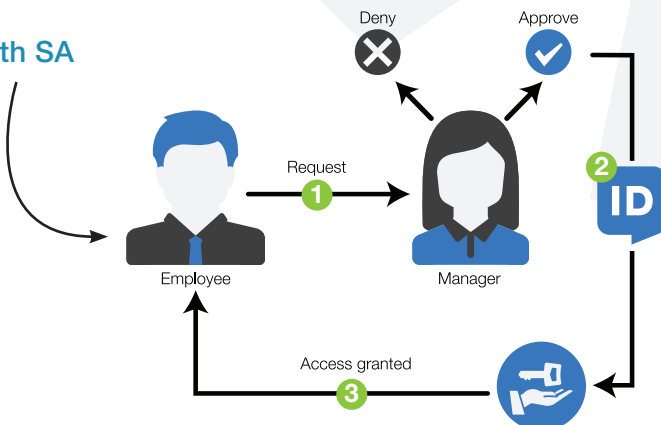
Service Automation

- Publish & manage an IT product catalog with self-service capabilities
- Assign data owners to manage relevant folders (e.g., IT, managers, team leads)
- Data owners can create groups, their associated folders, and set Access Control Lists (ACLs)
- Request, monitor, and approve access to any resource (e.g., applications, file shares, hardware, physical items)
- Automated request fulfillment without IT intervention
- See which users are active

Empowering users with Service Automation (SA)

Without SA

Deny | Approve | 3

Forwards request 2

Employee | Manager | IT Helpdesk

Request 1 | 4

5

Access granted

With SA

Deny | Approve

Request 1 | 2 ID

Employee | Manager

Access granted 3

IAM
Identity,Integrated

Identity and Access Manager (IAM)

On-premise Identity and Access Management

IAM centralizes user identity data through your entire environment, connecting your HR System to Active Directory user accounts. IAM connects further downstream to additional systems and resources as well, automating data transfer and enforcing role-based access controls throughout.
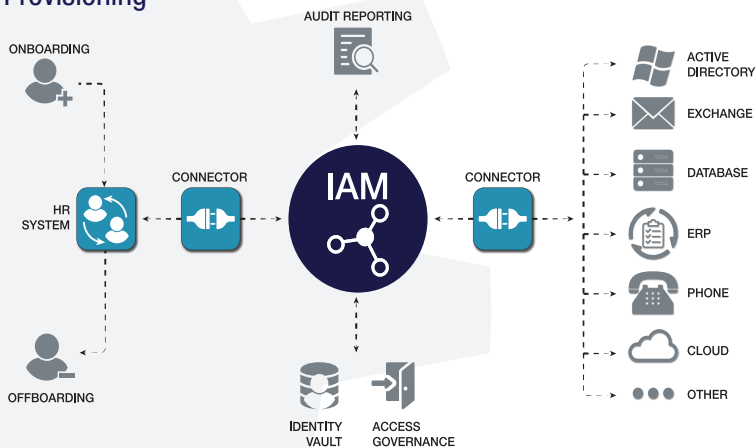
User Provisioning: Automated user and group provisioning facilitate faster onboarding for new hires. Provision Active Directory, Exchange, NTFS, and more downstream systems and resources.

Self-Service: Request, monitor, approve, and automatically fulfill resource authorizations without requiring IT intervention.

Helpdesk Delegation: User account management requests can be delegated to less technical IT staff without also having to grant them advanced admin rights and privileges.

Access Governance: Ensures that all users maintain the correct and compliant authorizations via role-based access controls.

IAM Provisioning

ONBOARDING

AUDIT REPORTING

HR SYSTEM

CONNECTOR

IAM

CONNECTOR

OFFBOARDING

IDENTITY VAULT

ACCESS GOVERNANCE

ACTIVE DIRECTORY

EXCHANGE

DATABASE

ERP

PHONE

CLOUD

OTHER

SSRPM
Passwords Made Easy

Self-Service Reset Password Manager SSRPM

Provide 24/7 password reset capability for users to manage credentials or basic Active Directory information. Predefined challenge questions remove the need for IT intervention.

Account Claiming ensures that first-time users receive their newly created accounts and credentials via a secure portal during their onboarding rather than relying on risky emails, notes, or intermediaries.

Multifactor Authentication (MFA/2FA) provides a second level of login security; includes "Push-to-Verify", One-Time Passwords, authenticator client apps, PIN codes, tokens, and more.
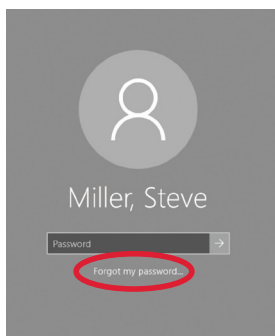
Active Directory Self-Service allows users to edit basic AD data to ensure their information is always up-to-date (e.g., name or address changes).

Helpdesk ID Verification provides IT with restricted visibility of credentials, allowing them to authenticate the caller without compromising security (e.g., "What is the fourth character of your mother's name?")

Password Synchronization Manager (PSM) Synchronize credentials across numerous systems and resources, such as Office365 and Google (G-Suite), to simplify access.
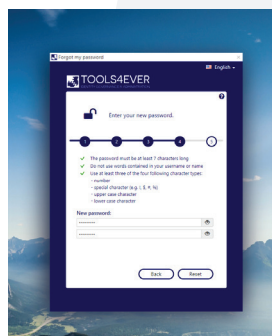
Password reset in three easy steps

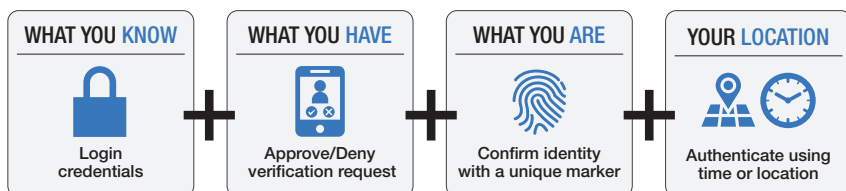| Click the "Forgot My Password" button	Answer a number of security questions	Enter and confirm the new password

MFA

Balance between access & security

A combination of criteria need to be met in order for the user to gain access to resources

HOW DOES IT WORK?

WHAT YOU KNOW	WHAT YOU HAVE	WHAT YOU ARE	YOUR LOCATION
Login credentials	Approve/Deny verification request	Confirm identity with a unique marker	Authenticate using time or location

55% of U.S. adults can **correctly define** two-step verification[1]

Username
****
Log In

59% of people **reuse** the same or similar passwords for **multiple accounts**[2]

92% of organizations unknowingly have credentials for sale on the **Dark Web**[3]

Receiving a secondary code by text or email blocked[4]:

100% of automated bot attacks

96% of bulk phishing attacks

76% of direct targeted attacks

80% of hacking-related **breaches are a result of** weak, default, or stolen passwords[5]

Sources: Tech Beacon[1], LastPass[2], McAfee[3], Nextweb/Google[4], Enterprise/Verizon[5]

CASE STUDY
Tronox
Stamford, CT

TRONOX

- ✓ 3,000 Employees
- ✓ Facilities on 4 Continents

⚙️ Challenge

Mergers and acquisitions created highly complex IT environments requiring too much management.

🚩 Result

HelloID ensures easy management and harmonic integration throughout Tronox's IT environment.

🔑 Rick Davies, IT Lead at Tronox, explained, "IT optimization is a lengthy process… However, an important step is the introduction of self-service and service automation. We want employees to be able to access applications quickly and easily without intervention from the helpdesk.

"TOPdesk is our central system... We have rolled out all modules of this solution worldwide. HelloID is a certified TOPdesk partner, which guarantees good integration. As a next step, we also want to automate the inflow, interval flow, and outflow of employees — including automated onboarding and offboarding." With the built-in Role Based Access Control and Access Governance functionality, HelloID also plays a key role in these plans. "The powerful combination of HelloID Service Automation and TOPdesk provides highly simplified management processes and a stronger focus on innovation."

Service automation is an important development at Tronox to free IT staff for IT innovation projects. Davies elaborated, "Because we need less IT capacity for operational activities, the IT department can fully focus on innovation… We are also actively working on our ISO 27001 certification, and the extensive reporting functions in HelloID support our IT government plans."

Coordinated Health
Parts of PA, FL & NJ

✓ 1,300 Employees

✓ 20 Hospital and Healthcare Facilities

⚙ Challenge

Decentralized operations made user account and password management a nightmare.

🚩 Result

IAM automated account management; SSRPM and PSM allowed users to manage passwords.

🚀 IT staff were spending a lot of time manually managing access and completing password reset requests. Coordinated Health (CH) sought password management products for the challenge of synchronizing a user's password change from Active Directory to the Sophos Safeguard server. Users couldn't log in to their workstation and were prompted for their old password, as CH had Sophos Safeguard encryption at all of their end points.

Paul DeVries, System Administrator, stated, "Doing business with Tools4ever has been a very satisfying experience from the initial sales presentation to the project design and implementation." When name changes come via their Human Resource Information System (HRIS), IAM automatically schedules the update, notifies the user, and performs all necessary changes to the account.

CH wanted all solutions in place within 90 days of purchase. Tools4ever spent time qualifying requirements and scoping the project in detail in order to plan and schedule the project efficiently and met the deadline with ease. DeVries concluded, "I am impressed by the level of support we have received from Tools4ever. We have not had to deal with any real problems… and the Tools4ever support was outstanding."

Maas & Waal Care Group (zMW)
Land van Maas en Wall, Netherlands

✓ 800 Employees

✓ 5 Locations operating 24/7

⚙ Challenge

Access management for nearly 50 apps and systems was far too difficult.

🚩 Result

HelloID and SSRPM streamline access and drastically reduce helpdesk demand.

🚀 Maas & Waal Care Group (zMW) provides a complete package of healthcare services. Marco Peters, zMW's IT Coordinator, summed his department's duties, "IT management is responsible for… infrastructure, 45 applications, VOIP systems, Wi-Fi and… optical fiber connections. We are also responsible for healthcare [automation]." Maas & Waal's IT administrators often chose between dedicating efforts towards password resets or managing the technology environment.

"Unfortunately… a password ticket was sometimes only picked up after a few days," Marco Peters continued. Now, employees logged into HelloID using their Active Directory credentials can immediately and securely access applications such as YouForce, Planywhere, Outlook webmail, Qic, Sharepoint and UKON.

"Password management has been a problem for years. The challenge was to convince management to invest in a solution... I finally [started] the pilot with Tools4ever, after which [everyone] immediately saw the benefits. I should have done this much sooner… the organization wanted to keep this solution immediately."

Now, administrators focus on projects and night-time reset calls have been eliminated. Password-related tickets have plummeted to only 2 per week. Response time has similarly plummeted from up to 5 days to instantaneous.

Additional Information

Set up your staff for success via HelloID's seamless, secure access for all user identities.

For 23 years, Tools4ever has helped organizations of all industries and sizes by optimizing our partners' processes, user account management, and security. From automatically creating new user accounts to ensuring employees securely log into resources, Tools4ever is committed to leveraging your IT resources into impactful, reliable solutions.

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION