COGNITUM Software

go:Identity

The Identity Management Appliance

User Management Out of the Box - Easy, Secure, and Effective

The Problem

A secure IT infrastructure is not possible without a system-wide authorization management

Identity and Access Management (IAM) solutions offer automated authorization management and a tight HR integration to keep employee and organizational data synchronized.

However, tight IT budgets often hinder organizations from implementing necessary IAM solutions. In doing so, they risk not meeting management, data protection and auditing requirements.

The Desire

Maximum ease of work and security within a short period of time

- Reduce the effort in administration of AD, Azure AD, LDAP, SharePoint, SAP, ERP, CRM, etc.
- Conduct regular recertifications for user and role authorisations (for auditors)
- Migrate applications into the cloud (Exchange/Lotus Notes to Office 365, SharePoint, etc.)
- Manage file share permissions and VPN access easily
- Move IT permission requests to a self-service web front end with subsequent approval workflows
- Relieve IT administration of mindless and error-prone tasks
- One single authentication for all user applications (SSO + Federation)
- Receive detailed reports on “Who has had/issued/withdrawn the authorisation when, from when, until when”
- Improve IT security

The Solution

A quickly deployable identity management solution

go:Identity is a complete, centralized, out-of-the-box identity management solution for all sizes of organizations.

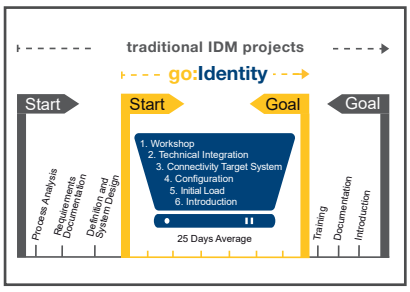
go:Identity will manage identities, roles and user accounts, including permissions in any target system.

go:Identity is productive in 25 project days on average for all projects. Various functionality like user provisioning and de-provisioning, user self-service and approval workflows are already integrated.

The Key Benefits

Simple, safe and effective...

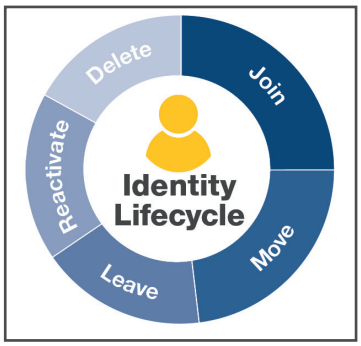
- Automation of many tasks and manual jobs
- Increase security
- Control over access and permissions
- Reliable data for reports
- Preserve data integrity
- Reduce the error rate
- Standardise data quality
- Appliance provides rapid deployment



... with low project risk

go:Identity‘s “out-of-the-box” approach significantly reduces project risk in our projects. Thanks to the built-in best practice, the processes and functions have already proven their suitability.

Core Features



User Life Cycle Management

go:Identity provides complete employee life cycle management. From the time an employee starts, moves laterally within the organization, or is terminated for any reason, changes are managed with workflow and tracked for compliance automatically.

Automated and manual features:

- Creation of identities - automatically from HR data or manually via the User Interface
- Modification of identity data - automatically through changed HR data or via the User Interface
- Deactivation of identities as well as the associated permissions - automatically on a set date
- Deletion of identities - automatically after a defined period if necessary

Automated HR Data Import

HR data should be complete, up to date and consistent across all systems to avoid security risks.

go:Identity offers an interface for importing HR data that will automatically update data on a regular basis:

- Creation of new identities
- Generation of unique user IDs and e-mail addresses
- Update existing identities
- Deactivate or delete employees who have left and are no longer recorded in the HR data or inactive employees

Administration of Other Identities

Contractors, temporary employees and technical identities for IT - external identities for short - often do not have a staff account and are generally not entered into the system through an HR data import.

go:Identity offers the ability to manually enter, maintain and delete external identities to enhance your security and compliance:

- created and secured by approval process
- provided with permissions through structured processes
- revoking permissions at the right time, per event or on a set date

User Self-Registration

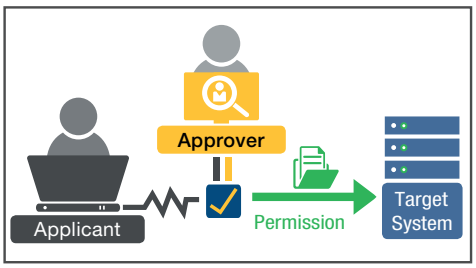
If management of any external identities (i.e. customers, partners, prospects, students, etc.) is needed, **go:Identity** offers an optional self-service interface. This also supports Consumer Identity and Access Management (CIAM) use cases for organizations who need to manage consumer identities. Optionally, this interface can be combined with web SSO for complete control access to all web applications for better online service in the organization.

Provisioning of User Accounts and Permissions

Manual provisioning of access rights to target systems often takes a lot of time, sometimes several days, and it is difficult to determine if the access has been granted.

go:Identity connects to a variety of common systems, such as Active Directory, LDAP, Lotus Notes, SAP, databases, mainframe, and many others, thus automating the management of accounts and permissions:

- Central management of user accounts, permissions and passwords
- Centrally controlled blocking and deletion of user accounts



Display and Analysis of permissions on fileshare folders

go:Identity shows all fileshare permissions of an identity or all access rights to a specific fileshare folder. For this purpose, the NTFS permissions are related to actual memberships in AD groups. This way, even unintentionally assigned permissions become visible.
All information can be found in a central place: in the central authorisation view of your identities. Dangerous exceptions can be unmasked, and more transparency and security can be brought into access management on file shares.

Reporting and Auditing

go:Identity provides the data necessary for detailed reporting. Additionally, custom report templates can be configured.

The audit data in **go:Identity** allows users to quickly access the necessary information to manage compliance and governance across identities. The audit data can answer the following questions amongst others:

- Which permissions does the employee have and when did he receive or lose them?
- Who approved what when?
- Which identity data has been changed?

Workflow Portal for Processes and Recertifications

The approval processes in go:Identity are configured and updated in the workflow portal. This portal also provides the ability to manage and update workflow throughout the go:Identity solution. In this interface, the attestation process allows business owners to manage recertification of employees.

Periodic confirmation of employee access can be initiated from the workflow portal. This regular certification ensures that only identified and confirmed users gain or lose access to systems.

Overview of the function processes:

- Approval processes for roles
- Processing of external identities
- Cyclical confirmation of identities, roles and organization units within defined periods of time

Regulatory Compliance

Identity data is becoming more strictly regulated (e.g. GDPR, HIPAA and SOX, etc.), and it is important to adhere to guidelines as they continue to evolve. In addition, organizations are more educated and sensitive to what data is provided and how it is used.

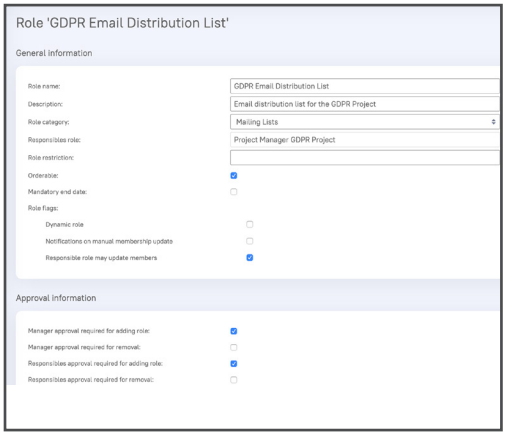
go:Identity supports the current guideline requirements and will continue to maintain those and modify them as necessary.

Admin User Interface for Editing Roles

In go:Identity, roles are the central tool for managing and assigning permissions. Depending on your objectives, your admin can establish various roles via the admin user interface.

Here the role can either end in a real permission on a target system or lead to a grouping of identities. The admin user interface enables you to manage roles and dynamically manage the approval processes and notifications for each role:

- Role name, categorization and description
- Is the role available and is a term limit specified?
- Is a manager approval required?
- Does another group or person have to approve?
- Who is the role owner? Does he/she have to approve?
- Who should receive notification of the result at the end of an approval process?



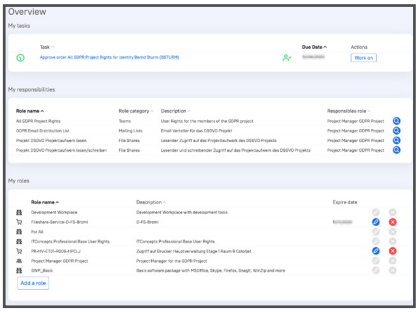
Roles can easily be assigned and managed by business owners or system owners, taking the burden off IT and placing it on the business users in the organization who are responsible for access to their owned data.

Central Dashboard for Employees

In the employee portal dashboard, employees can review roles and entitlements and request further permissions directly. This provides improved efficiency and allows employees direct access to request what they need to do their job. The associated approval process is automated, which gives the requester the visibility they need throughout the process and improves the operational efficiency of the IT organization.

Additional self-service features:

- Change and reset passwords
- Maintain delegations
- Review and edit own data



Organizational Units and Management

go:Identity offers a module for managing hierarchical organizational units and responsible people, or managers. These organizational units also offer the option to assign standard permissions that can be inherited within the organizational tree.

Technical Details

User Interface

- Browser-based interface allowing simple use from “anywhere”
- Multilingualism (DE, EN, FR, + other languages as required)
- Adaptable design (adaptation to your existing CI)

Connection of target systems

- Connection of legacy systems, e.g. Microsoft Active Directory, Azure AD, Exchange, SharePoint, SAP, LDAP
- Other modules available for connection, e.g.:
  - Notes
  - Database Applications, e.g. Oracle, MSSQL, MySQL und PostgreSQL
  - Linux und Unix
  - and many more
- Customer-specific or other systems can be integrated via the flexible connector framework

Specifications

- The solution is provided as a virtual machine (VM)
- Preconfigured system - no complicated installations necessary
- Predefined workflows and approval processes - use of practically tested processes from the very start, adjustments are possible
- Integration and commissioning in your environment
- No subscription commitment – annual termination possible

go:Identity

The standardised user management “out-of-the-box“

- ✓ **go:fast** – Improved Productivity
- ✓ **go:cost-effective** – Cost Savings
- ✓ **go:secure** – Audit-Friendly and Transparent
- ✓ **go:easy** – Control of Permission Allocation

COGNITUM Software

go:Identity

COGNITUM Software combines long-term Identity and Access Governance expertise for the development of standard software.

Identity & Access Governance is a key component in building a secure IT infrastructure. With our comprehensive practical experience in consulting, implementation and our expertise in identity and access governance solutions, we have developed our software that is deployable rapidly and cost effective - for any business, regardless of industry and size. COGNITUM Software emerged from ITConcepts group, a leading, global IT service provider and agnostic system integrator.

COGNITUM Software Team GmbH
Leitschweg 2c, 38448 Wolfsburg, Germany • Phone: +49 5361 8349527 • Email: info@cognitum-software.com • Web: www.cognitum-software.com