

# GENEOUS SOFTWARE

# ACCOUNT GENEIOUS

IDENTITY MANAGEMENT ACROSS ALL PLATFORMS



## SOFTWARE PRODUCT DESCRIPTION – ACCOUNT GENEIOUS WEB 10.2

### IDENTITY MANAGEMENT

An Identity Management solution, **ACCOUNT GENEIOUS** manages the user's life-cycle management through the organization over time. It provides AAA (Authentication, Authorization and Audit), role engineering capabilities (RBAC model) and workflow automation for provisioning and deprovisioning tasks. Additional modules from **GENEOUS SOFTWARE** are available and include Password Synchronization Module and Self Service Module which includes password reset and file management capabilities.

### IDENTITY REPOSITORIES

**ACCOUNT GENEIOUS** system implements a virtual directory technology thus being able to integrate and aggregate data from a large variety of identity repositories (LDAP based directories or RDBMS systems). Existing Human Resources repositories can also be connected and integrated into the **ACCOUNT GENEIOUS** virtual directory system. The virtual directory system from **ACCOUNT GENEIOUS** can be used as a SoR (Source of Records) for other applications used in the organization. The synchronization/reconciliation processes between all the identity repositories can be configured by defining flexible rules.

### AGENTS

The management of the target platforms is realised through agents. Agents are designed to be flexible, extendable, fault tolerant and extremely secure applications. Usually an agent manages the users accounts and the users groups for a specific platform, but it can be easily extended for managing other entities that the customer needs (Identifiers on OpenVMS system for example). There are also some universal agents for managing LDAP structures or RDBMS proprietary tables.

### FEATURES

#### Java and Web

**ACCOUNT GENEIOUS** is built with portability in mind, thus the Java/J2EE solution ensures wide platform options for installing the server. The GUI, being web based, offers a consistent look over platforms and browsers (e.g. Internet Explorer and Mozilla, with JavaScript, popups and cookies enabled).

#### Flexible GUI

Its appearance uses CSS (style sheets) which can be customized as required. **ACCOUNT GENEIOUS** supports alternate language resource files, thus the help files and all the texts in the program can be changed with one click (other localization can be done at any time). All the tables from within the program, including the reports, can be exported to spreadsheet (CSV), PDF or other file formats.

#### Easy Setup

**ACCOUNT GENEIOUS** components have installation kits which reduce the installation effort to a minimum, making the **ACCOUNT GENEIOUS** a true 'out of the box' solution. However the product is highly configurable for each customer's specific needs. The XML configuration files describe all the items processed through the system (number of fields, characteristics, format, validators, restrictions, interdependencies, placement, GUI editors etc.). Access to each item and then to each resource field can be refined to none / read / readwrite and the user can later select among the permitted set of fields the ones which should appear and in which order they appear in the lists or dialogs.

#### Multiple Modes of Operation

The interface allows configurable multi-mode access, with different looks and functionalities for system administrators, configurators, normal users, helpdesk users, self service and any user-defined combination of actions and views.



## Scalability

The system is scalable and new modules can be added at any time including new platforms or new features (like single sign-on, password synchronization etc) Integrating a new agent can be

## USER PROVISIONING

### Coherent View

All the platforms supported by the product are integrated into a coherent and convenient interface, allowing users to add new platforms with minimal effort or training for the **ACCOUNT GENEIOUS** user.

### Multi-platform operations

This design also allows actions that span accounts of multiple platform types. To ease the user experience many help functions are directly available from the interface. For example the user can update a few fields identically to a group of accounts, reset passwords, create similar accounts on multiple platforms at once, create a number of accounts at once (called bulk creation), save filled items or lists and restore them for further use etc. Based on the data in the subscriber and application database, the multiple bulk-account creation feature can gather all the necessary information and present it pre-completed to the **ACCOUNT GENEIOUS** -user who can then

as simple as editing the new XML configuration files if the data structures and schemas for a new directory or database are different from the default ones. Full documentation for the API is available for customers wanting to develop their own modules or agents.



create all the necessary accounts with one click.

### Templates

Templates are a very useful tool for creating similar class users, for instance for handling standard values for privileges that are common across multiple job functions and locations. The templates defined as 'system' are shared between all the **ACCOUNT GENEIOUS** administrators and locations, so they can be used throughout the whole company. The accounts can be modified while applying the templates.

### Scripts

User-written scripts (platform specific) which are run before and after the actions are processed can perform site- or agent-specific tasks. For example, they can generate e-mail notifications, move user files, create extra links and more. The scripts can be marked as optional or mandatory - when an error will stop the further continuation of the action.

## SECURITY

### SSL Connections

The link between browser and **ACCOUNT GENEIOUS** system uses HTTPS (SSL security implemented by the web server). The links between the **ACCOUNT GENEIOUS** components use RMI-SSL (based on the configurable JSSE Java Secure Sockets Extension, SSL using AES as default). The certificates which can be used between all these endpoints are implemented by the SSL communication components, therefore they are configurable on site according to user requirements (using JSSE support and Java Cryptography Architecture).

### Encrypted Data

If the system is set to manage and hold internal authentication then all the password related data (including account passwords, secret questions, password propagation queue etc.) is stored encrypted using the server key, thus only the person administering the database system (where **ACCOUNT GENEIOUS** stores its data) can see the hashes/encrypted data. The storage, therefore, relies on the security of the underlying database.

### Authentication

The authentication in **ACCOUNT GENEIOUS** is through username and password. In order to check the username and password the **ACCOUNT GENEIOUS** Server can use different authentication connectors.

The default is set to the **ACCOUNT GENEIOUS** Server internal users repository. Additional connectors can extend this authentication by checking the username/password in other available Subscriber connectors eg. directories, databases etc. Administrators of other **GENEIOUS** products (Password Synchronisation, Password Reset) use the same authentication schema. The changes on the target machines are made by the agents which have to run under a privileged account whose rights will allow them to perform the necessary user administration actions.

### Roles Based Authorization

Authorization of access to the system data is regulated by different mechanisms on a low level (data structures) and a high level (user security profiles). The fields that the system can access are set in the XML configuration files - which can be modified and reloaded dynamically. Users' access to items and item fields is defined by the user's attributed security profile. When creating a security profile one can select from the defined fields the ones its users will be allowed to access. Any updates are applied immediately to the affected users. Through the fine-grained security profile attributed to a user, any action, be it modify, create or delete, can be selected and refined down to the access to a single field (dependencies are also handled).



When the user gets more than one profile assigned, the evaluation of the rules is performed sequentially, in order to determine whether the user is denied or allowed.

With specially designated profiles, accounts too sensitive to be allowed handling (application accounts or groups, administrators) are denied access via **ACCOUNT GENEIOUS** - thus the **ACCOUNT GENEIOUS** tool will refuse to perform any actions affecting those marked entities. Profiles can be disabled thus removing access rights from a whole class if necessary.

### Roles Split in Domains

**ACCOUNT GENEIOUS** uses the concept of 'domains' to organize the access to different resources. To each domain is attributed a set of agents (and accounts or subscribers). By giving appropriate rights into a domain each security profile can refine what that user is able to do in a certain set of systems/applications (a domain).



### AUDIT TRAIL AND ARCHIVING

The agents will record locally startup/shutdown times and major communication errors, but the main storage for auditing data is the audit database. This database stores all the actions that involve the **ACCOUNT GENEIOUS** system, including all the configuration changes and the automated actions (for example, generated by password synchronization) **ACCOUNT GENEIOUS** stores an agent entry, an account, a group, a subscriber, a domain, an agent cluster, a profile, an action, ie. any object handled

### REPORTS

#### Covering all data

The report manager represents a separate module responsible for gathering data from all the possible sources in the system (live data from agents, archived entries, subscriber information, task queues etc). Field level filtering is provided for all the data sources involved, using flexible links and regular expressions.

#### Create new reports with ease

The reports are user configurable, thus new ones can be written any time to accommodate new logical rules and new tasks. For example, an appropriately built report can compare the pool of accounts to a set of rules (or reference account). If automation is not needed, manual reports can show changes in the subscriber database or assigned accounts and propose

### Configurable Data Validation

Each field of the user entered data is validated according to appropriate (and configurable) rules. Data validation can be performed between fields. Fields can be dynamically constructed and regular expressions can be used for special format specifications.

### Notifications

The actions of the system are then performed synchronously, so the result is immediately available to the **ACCOUNT GENEIOUS** administrator (or later in the audit logs). The password synchronization and the workflow modules offer the option to check the status of ongoing tasks from the queue. For security reasons the audit and queue checking rights will be attributed only to the designated administrators (with their security profile).

### Clusters

The **ACCOUNT GENEIOUS** system uses the agents clusters. This basically makes it possible for all the actions performed on one of the members to be done on all the members.

by the **ACCOUNT GENEIOUS** system. The item structures are documented and each field is available for archiving. All the three phases of an action and their corresponding data are stored (data before the change, data as requested, and result of data). The only exception is that the passwords are never saved in the archive, for security reasons. Any item can be traced with precision through its history, and if needed, restored at any time, reversing previous action.

the necessary actions for fixing any discrepancies.

### Defaults provided

**ACCOUNT GENEIOUS** provides by default some reports, like 'Account never used' (no logins), 'Expired accounts', 'Locked/disabled accounts', 'Accounts with no password', 'Accounts without link to subscriber' (orphans), 'Subscribers without platform accounts' (automatic assignment at system installation or de-assignment on system removal), 'Duplicate home directories'.

### Other options

Supplementarily, as long as the audit is in a database, any standard database reporting procedures can be used.





## WORKFLOW

An automated report or the subscriber database agent (with installed trigger procedures) can notify the system of changes. The workflow module will then take over the generated tasks and perform them. This module can automatically generate access-provisioning requests based on new hires, department/job title changes, and terminations. Even in the case when the automated subscriber or accounts connection is utilised, the system preserves its normal (user-driven) functionality, both from the subscriber database and

from the GUI. **GENEOUS** is currently developing a more complex workflow module, based on the web services technology. This will make it BPEL compliant, and all the functionality of this design (approvers and security administrators, responsibilities matrix, automatic provisioning or adjusting, special alarms and notifications for each stage, delays estimations, commentaries) will be within the reach of the **ACCOUNT GENEOUS** users.

## CONTACT AND SUPPORT INFORMATION

### GENEOUS SOFTWARE AG

Welbrüging 42  
8954 Geroldswil | Zurich  
Switzerland

Tel. +41 (0)44 747 52 60  
Fax +41 (0)44 747 52 61

Email : [office@geneous.com](mailto:office@geneous.com)  
Support : [support@geneous.com](mailto:support@geneous.com)  
Website : <http://www.geneous.com>

