

# GENEOUS SOFTWARE

# ACCOUNT GENEIOUS

IDENTITY MANAGEMENT ACROSS ALL PLATFORMS



## SOFTWARE PRODUKT BESCHREIBUNG – ACCOUNT GENEIOUS WEB 10.2

### BENUTZERKONTENVERWALTUNG

Eine Benutzerkontenverwaltungs-Lösung: **ACCOUNT GENEIOUS** verwaltet die Benutzer-Identitäten unternehmensweit mit Zugriff auf die entsprechenden Datenquellen. Es beinhaltet Zugriffe auf Benutzer-Datenbanken, Benutzer-Authentisierung, rollenbasierte Zugriffe, automatischer Arbeitsfluss, und als eine Hauptaufgabe Bereitstellung von Benutzerkonten über verschiedene Betriebssysteme hinweg. Zusätzliche Module von **GENEOUS** Software stehen ebenfalls zur Verfügung, d.h. **Passwort Synchronisation** and **Passwort-Reset Plus**.

### BENUTZERDATENBANKEN

Das **ACCOUNT GENEIOUS** System implementiert eine „Virtual Directory Technology“ und ist aus diesem Grunde in der Lage eine Vielzahl von Benutzerdatenbanken zu integrieren und gesamthaft zu verwalten (LDAP basierend oder RDBMS-Systeme). Bestehende Personal-Datenbanken können ebenfalls angeschlossen und in das **ACCOUNT GENEIOUS** Virtual Directory System integriert werden. Das **ACCOUNT GENEIOUS** Virtuelle Directory kann als Quelle von Informationen für andere Applikationen, die in der Gesellschaft eingesetzt werden, dienen. Die Synchronisations- und Abstimmungs-Prozesse zwischen allen Benutzerdatenbanken können mit flexiblen Regeln definiert und konfiguriert werden.

### AGENTEN

Von der Basis her sind alle Konnektoren zu den Plattformen und Applikationen agentenbasierend. Einige Agenten können jedoch auf der **ACCOUNT GENEIOUS** -Maschine (oder andere) installiert werden (JDBC für Datenbanken, LDAP, etc) Dazu braucht es höchstens kleinere Skripte um sie auf der Zielmaschine zu installieren/hinterlegen. Den Zustand der Agenten kann jederzeit im Agentenfenster eingesehen werden. Das API für die Agenten (RMI, JDBC) wird zur Zeit noch erweitert um den Kunden die eigene Agenten entwickeln wollen, die entsprechende SDK zu liefern. Neue LDAP-Agenten werden jedoch nicht benötigt. Durch das Editieren der XML Konfigurationsdatei sollten die LDAP-Strukturen ohne Schwierigkeiten übernommen werden.

### HAUPTMERKMALE

#### JAWA UND WEB

**ACCOUNT GENEIOUS** wurde mit dem Gedanken von Portabilität erstellt, deshalb garantiert die Java/J2EE Lösung vielseitige Möglichkeiten um den **ACCOUNT GENEIOUS** Server zu installieren. Der Web-basierte GUI bietet eine konstante Einheit auf den verschiedenen Betriebssystemen und den Browsern, wie z. B. Internet Explorer und Mozilla, mit aktivierten Java Skripten, „poppers“ und Cookies.

#### FLEXIBLER BENUTZEROBERFLÄCHE

Sein Erscheinungsbild benutzt „CSS style sheets“ das kundenspezifisch angepasst werden kann. **ACCOUNT GENEIOUS** unterstützt „Alternate Language Resource Files“ somit können die Help-Dokumente and alle Texte im Programm mit einem einzigen Klick

geändert werden (ein anderer Standort kann jederzeit zugeordnet werden.). Alle programmspezifischen Tabellen, inbegriffen Rapporte, können auf „Spreadsheets“ (CSV), PDF und andere Tabellenformate exportiert werden.

#### LEICHTE INSTALLATION

Die **ACCOUNT GENEIOUS** komponenten haben Installationswerkzeuge die den Installationsaufwand auf ein minimum reduzieren und somit **ACCOUNT GENEIOUS** zu einer fast „out of the box“ Lösung machen. Das Produkt ist jedoch äusserst leicht konfigurierbar um den einzelnen Bedürfnissen eines Kunden gerecht zu werden. Die XML Konfigurationsdokumente erklären alle Punkte die das System verarbeitet, Anzahl Felder,



Charakteristika, Formate, „validators“, Restriktionen, Abhängigkeiten, Platzhalter, GUI-Editoren, etc. Zugriffe auf jeden einzelnen Punkt und weiter auf jedes Quellfeld kann als kein / lesen / lesen,schreiben definiert werden. Somit kann später der **ACCOUNT GENEIOUS**-Benutzer selektiv die zur Verfügung stehenden Felder auswählen und auch die Reihenfolge bestimmen in der sie erscheinen sollen.

#### **VIelfÄLTIGE HANDHABUNGSARTEN**

Die Schnittstelle erlaubt konfigurierbare Handhabungsarten mit unterschiedlichen Erscheinungsbildern und Funktionalitäten für System Administratoren, normale Anwender, Helpdesk Mitarbeiter und jegliche Art von selbstdefinierten

Kombinationen von Aktionen und Aussehen.

#### **SKALABILITÄT**

Das System ist skalierbar und neue Module können jederzeit hinzugefügt werden. Inbegriffen sind neue Plattformen oder neue Merkmale wie Passwort Synchronisation, Passwort Reset Plus. Die Integration eines neuen Agenten kann so einfach wie das editieren eines neuen XML Konfigurationdokumentes sein falls die Datenstrukturen und Schemas für das neue Verzeichnis oder Datenbanken unterschiedlich von den Standards sind. Eine komplette Dokumentation des API steht für Kunden zur Verfügung, die ihre eigenen Module oder Agenten entwickeln wollen.

### **BENUTZER-PROVISIONIERUNG**

#### **KLARE, VERSTÄNDLICHE ANSICHT**

Alle Plattformen die durch das Produkt unterstützt werden, sind in einer klar, verständlichen Schnittstelle integriert. Dies erlaubt den **ACCOUNT GENEIOUS** - Benutzern leicht und mit minimalem Aufwand oder Training, neue Plattformen hinzuzufügen.

#### **MULTI-PLATTFORM AKTIONEN**

Die Architektur erlaubt ebenfalls Aktionen/Kreationen die Konten auf verschiedenen Betriebssystemen betreffen. Um dem Benutzer behilflich zu sein, werden viele Helpdesk-Funktionen direkt über die Schnittstelle abgerufen. Der Benutzer kann mehrere identische Felder einer Gruppe von Konten zuordnen, Passworte neu setzen, eine Anzahl Konten auf einmal kreieren (Bulk) Abspeichern von gesetzten Felder für späteres Wiedereinsetzen. Auf der Basis der Daten in der Subscriber- oder Applikationsdatenbank kann die Multiple-Konto-Kreation (Bulk) alle Informationen zusammenfassen und sie dem Benutzer vordefiniert präsentieren, der alsdann die entsprechenden Konten mit einem Klick kreieren kann.

#### **TEMPLATES**

Templates sind äusserst wertvolle Werkzeuge um gleichwertige Benutzer anzulegen. Dies ist vor allem nützlich beim Zuordnen von Standardwerten für Privilegien die gleich sind für viele Arbeitsfunktionen und Standorte. Die Templates die als „System“ bezeichnet werden, sind von allen **ACCOUNT GENEIOUS** - Benutzern und in der ganzen Betriebsumgebung einsetzbar. Konten können auch durch den Einsatz von Templates geändert werden.

#### **SKRIPTE**

Benutzerdefinierte Skripte (Plattform spezifisch) die vor und nachdem eine Aktion abgewickelt ist, ablaufen, können lokale oder agentenspezifische Aufgaben durchführen. Sie können zum Beispiel email Benachrichtigungen ausführen, Benutzerakten verschieben, spezielle Verbindungen kreieren, and vieles mehr. Die Skripte können optional oder als obligatorisch bezeichnet werden – wenn ein Fehler die Weiterführung der Aktion stoppen wird!!

### **SICHERHEIT**

#### **SSL VERBINDUNGEN**

Die Verbindung Browser und **ACCOUNT GENEIOUS** - System benutzt HTTPS (SSL Sicherheit vom Web-Server verwirklicht). Die Verbindung zwischen den **ACCOUNT GENEIOUS** -Komponenten benutzt RMI-SSL (basiert auf der konfigurierbaren JSSE Java Secure Sockets Extension, SSL AES als Standard eingesetzt). Die Zertifikate die zwischen all diesen Endpunkten eingesetzt werden können, werden durch die SSL Kommunikations-Komponenten bewerkstelligt. Dies bedeutet, dass sie vor Ort vom Benutzer gemäss seinen Bedürfnissen konfiguriert werden können (Benutzung von JSSE-Unterstützung und Java Verschlüsselungs-Architektur).

#### **VERSCHLÜSSELTE DATEN**

Falls das System darauf eingestellt ist eine interne Authentisierung zu verwalten, so werden alle Passwort relative Daten (inbegriffen Konten Passworte, geheime

Fragen, Passwort Propagation Queue etc) verschlüsselt aufbewahrt unter Nutzung des Server Schlüssels. Dies bewirkt, dass nur die Person die die Datenbank verwaltet auf der **ACCOUNT GENEIOUS** seine Daten lagert, die „hashes/verschlüsselte“ Daten sehen kann. Die Lagerung unterliegt deshalb der Sicherheit der dafür eingesetzten Datenbank.

#### **AUTORISIERUNG**

Die Autorisierung im **ACCOUNT GENEIOUS** ist durch Benutzername und Passwort. Um den Benutzernamen und Passwort zu kontrollieren kann der **ACCOUNT GENEIOUS** -Server verschiedene Autorisierungs-Konnektoren einsetzen. Die Basis-einstellung führt zum internen **ACCOUNT GENEIOUS**-Server Aufbewahrungsort. Zusätzliche Konnektoren können diese Autorisierung der Benutzernamen/ Passworte erweitern auf weitere /andere zur Verfügung stehende Verzeichnisse, Datenbanken, etc. Administratoren von



anderen Geneous Produkten wie Passwort Synchronisation, Passwort Reset Plus, benutzen dasselbe Autorisierungs-Schema. Die Änderungen auf der Zielmaschine werden durch den Agenten vollzogen, der mit privilegierten Rechten die Möglichkeit hat, die Aktionen des Administrators auszuführen.

### ROLLENBASIERDEN AUTORISIERUNG

Zugriff-Autorisierung auf System Daten wird durch verschiedene Mechanismen reguliert, d. h. auf einer tieferen Ebene für Datenstrukturen, und einer höheren Ebene für die Sicherheitsprofile. Die Felder auf die das System zugreifen kann sind im XML Konfigurationsfile festgelegt, welches entsprechend modifiziert und dynamisch wieder geladen werden kann. Benutzer's Zugriff zu den Konten und entsprechenden Feldern wird durch die dem Benutzer zugewiesenen Sicherheitsprofile definiert. Bei der Kreierung von Sicherheitsprofilen kann von den zur Verfügung stehenden Feldern diejenigen ausgewählt werden auf die der Benutzer zugreifen kann. Jegliche „updates“ wirken sich sofort auf die entsprechenden Benutzer aus. Durch die filigrane Abstimmung der dem Benutzer zugewiesenen Sicherheitsprofile, jegliche Ausführung wie Änderung, Kreierung oder Löschung kann ausgewählt werden, kann auch der Zugriff bis auf die Feldebene bestimmt werden. (Abhängigkeiten werden ebenfalls gehandhabt). Wenn dem Benutzer mehr als ein Profil zugesprochen wird, werden die Regeln sequential abgespielt, um festzulegen ob der Benutzer Zugriffe bekommt oder abgelehnt wird. Profile können gesperrt werden und somit eine ganze Gruppe die Zutrittsrechte entziehen.

### ROLLENAUFTEILUNG IN DOMÄNEN

**ACCOUNT GNEOUS** das Konzept der Domänen um die Zugriffe auf verschiedene Datenquellen zu organisieren. Jeder Domäne wird eine Anzahl Agenten zugeordnet (plus Konten und Subscribers). Indem man gewisse Rechte auf die Domäne gibt, kann ein jedes Sicherheitsprofil granular abgestimmt werden zu was ein entsprechender Benutzer in den Systemen / Applikationen berechtigt ist.

### KONFIGURIERBARE DATENGÜLTIGKEIT

Ein jedes mit Daten eingegebene Feld wird auf seine Gültigkeit geprüft gemäss den gültigen und entsprechend konfigurierbaren Regeln. Die Datengültigkeit kann zwischen den verschiedenen Felder vorgenommen werden. Felder können dynamisch aufgebaut werden und reguläre Ausdrücke können für spezielle Formatspezifikationen angewandt werden.

### BENACHRICHTIGUNG

Die Handlungen des Systems werden alsdann synchron ausgeführt, womit die Resultate sofort dem **ACCOUNT GNEOUS** - Administrator zur Verfügung stehen (oder später im Auditlog). Die Passwort-Synchronisations und Workflow-Module bieten die Option die aktuellen Aufgaben in einer „Schlange“ zu verifizieren. Aus Gründen der Sicherheit werden die Verifizierrechte nur entsprechenden Administratoren zugesprochen (über deren Sicherheitsprofile)

### CLUSTER

Das **ACCOUNT GNEOUS** System kennt das Clustering von Agenten. Dies gibt die Möglichkeit, dass Aktionen auf einem Agenten, zusätzlich auf allen zugehörigen Agenten ausgeführt werden.

## AUDITING UND ARCHIV

Die Agenten werden lokal Start- und Abbruchzeiten sowie wichtige Kommunikationsfehler aufzeichnen. Die hauptsächlichste Lagerung von Daten findet jedoch in der Audit-Datenbank statt. Diese Datenbank lagert alle Daten in „Relation“ mit dem **ACCOUNT GNEOUS** System. Inbegriffen sind alle Konfigurationswechsel und die automatischen Aktionen z.B. durch eine Passwort synchronisation ausgeführt. **ACCOUNT GNEOUS** lagert einen Eintrag in einem Agenten, Cluster, Profile, Aktionen, d.h. jedes Objekt das durch das Geneous System gehandhabt wird. Die Kontenstrukturen werden dokumentiert und jedes Feld steht für die Lagerung zur Verfügung. Alle drei Phasen einer Aktion mit den entsprechenden Daten werden gelagert, d.h. Daten vor dem Wechsel, Daten gemäss Eingabe und erzielt Resultat. Die einzige Ausnahme ist, dass aus Sicherheitüberlegungen die Passworte nie im Archiv gelagert werden. Ein jedes Konto kann mit äusserster Präzision durch seine ganze Geschichte verfolgt werden, und falls notwendig, wieder reaktiviert werden indem vorangegangene Aktionen rückgängig gemacht werden.

## RAPPORTE

### REPORTMANAGER ENTHÄLT ALLE DATEN

Der Rapportmanager ist ein separates Modul mit der Aufgabe alle möglichen Daten des Systems zusammenzuführen (aktuelle Daten von den Agenten, archivierte Daten, Subscriber Informationen,

Aufgabenlisten, etc.) Eine Filtrierung bis auf die Ebene eines jeden einzelnen Feldes ist möglich, indem flexible „links“ und normale Ausdrücke angewandt werden.



## EINFACHE RAPPORTKREATIONEN

Die Rapporte werden vom Benutzer konfiguriert, somit können neue Rapporte zu jeder Zeit geschrieben werden um neue Regeln und Aufgaben zu definieren. Als Beispiel könnte ein Rapport Vergleiche, Abstimmungen zwischen verschiedenen Konten aufzeigen. Falls keine automatisierten Aktionen vorgesehen sind, könnte ein manueller Rapport Änderungen in der Subscriber DB oder zugeordneten Konten aufzeigen und entsprechende Aktionen vorschlagen und die Differenzen ausgleichen.

## STANDARD-RAPPORTE

**ACCOUNT GENEIOUS** stellt einige Rapporte als

Basisinformation zur Verfügung, wie Konten die nie benutzt wurden (keine logins), abgelaufene Konten, geschlossene/gesperrte Konten, Konten ohne Passwort, Konten ohne Verbindung/Zugehörigkeit zu einem Subscriber. Subscribers ohne dazugehörige Konten (automatische Zuordnung bei Systeminstallation oder Deinstallation beim removal des Systemes) Doppelte Homedirectories.

## ANDERE OPTIONEN

So lange dass der Audit in einer Datenbank ist, kann jede mögliche standard Rapportprozedur angewandt werden.

## WORKFLOW

Ein automatischer Rapport oder der Agent der Subscriber Datenbank (mit installierten trigger prozeduren) kann das System über Änderungen informieren. Das Workflowmodul wird dann die erwogenen Aufgaben übernehmen und ausführen. Dieses Modul kann automatisch Zugriffsberechtigungsanfragen auf der Basis von neuen Anstellungen, Abteilungs-/Arbeits-/Funktionsänderungen, sowie Beendigung von Arbeitsverhältnissen generieren. Selbst wenn die automatische Subscriber oder Konten-Funktion benutzt wird, bleibt die benutzerabhängige

Funktionalität bestehen und dies von der Subscriber Seite wie auch von der des GUI aus. **GENEIOUS** ist daran ein komplexeres Workflowmodul auf der Basis der Webservicetechnologie zu erstellen Dies macht es BPEL kompatibel, und alle Funktionalitäten dieses Produktes (approvers and Sicherheits Managers, Verantwortlichkeitsmatrix, automatisches Provisioning oder Richtigstellung, spezielle Alarme oder Benachrichtigungen auf allen Stufen, Verspätungen, Kommentare) werden in reichbarer Nähe des **ACCOUNT GENEIOUS** -Benutzers sein.

## KONTAKT UND SUPPORT

### GENEIOUS SOFTWARE AG

Welbrügg 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>

