

Password Geneous

PASSWORD MANAGEMENT ACROSS ALL PLATFORMS

GENEOUS SOFTWARE provides Identity Management (IdM and IAM) solutions to increase enterprise security with enhanced access control and improved efficiency. Authentication, role and rule based access control (RBAC), database and directory integration and reduction in helpdesk calls are all provided with the implementation of GENEIOUS solutions.

The ability to implement the solutions quickly in order to provide a rapid return on investment (ROI) is a fundamental part of the GENEIOUS design. The scalability and ROI provided by Geneous solutions makes them ideal for enterprises from a few hundred employees to tens of thousands.

PASSWORD GENEIOUS allows you to manage user accounts on the following platforms

- AIX
- Tru64
- HP_UX
- Linux
- Sun Solaris
- OS/400
- OS/390
- Open VMS
- Windows 2000/2003 AD
- LDAP

Applications and Databases

- MS Exchange
- SQL Server
- Oracle
- Lotus Notes/Domino
- SAP/RS

Web Password Management Solution

PASSWORD GENEIOUS is a sophisticated multi platform tool providing transparent and secure distributed User Password Management and Synchronization. Users need only remember one 'Enterprise' password to access any number of computers.

Password synchronisation ensures that however a user changes their password at any managed platform or application, the new password is securely propagated to all the hosts to which the user has been authorized. A clear and easy to use interface simplifies the set-up and maintenance of the rules that allow

Account Geneous users to manage host resources and user access.

Because users do not need to remember more than one password at any time, they will not need to write them down, and **PASSWORD GENEIOUS** will encourage the use of non-trivial passwords, helping to reduce the risk of trial and error brute force security breaches.

May be implemented either 'stand alone' or together with **Account Geneous** for comprehensive management and efficiency.

Rule Base

PASSWORD GENEIOUS allows a sophisticated rule base to be created that provides complete control over password propagation. The rules apply user defined tests to match incoming password change notifications. When a match is found, the appropriate user-defined actions are applied. The actions specify the accounts on remote systems that need to be updated for the specified password change notification.

Full wildcard matching is supported against incoming password change notifications, as is matching against user names, node names, Windows local or global groups, OpenVMS UICs etc. You can also specify logically associated groups of hosts, which can be referenced by a mnemonic host group name. This host group name can be used in rules as part of either tests or actions.

Another important source for these rules is the Subscriber Database itself. If the customer decides to use subscribers, then each person (subscriber) can have the passwords synchronized between all of his assigned platform accounts.

continued overleaf



Password Geneous



Rule Base continued

The rules database can be exported and imported to allow backup, merging, copying and updating of the database. **PASSWORD GENEIOUS** offers a convenient GUI for editing and adding new rules according to the specific needs.

BENEFITS

- Consistent sign-on access is provided to multiple systems for users with a single password
- Simultaneously increasing security by mandating the use of stronger passwords and enforcing password change policies
- Nearly 80% of all security breaches are from current and former employees. With PGS users may be revoked, resumed and deleted from all platforms and applications immediately from a single point with optional post-processing
- Gartner and other consultants estimate that helpdesks spend more than 50% of their time at a cost of up to \$30 per reset with calls for forgotten passwords. Peak levels after holidays
- Reduces requirements for out-of-hours cover due to reduced calls
- Rapid ROI without the cost and effort of a single sign-on implementation

KEY FEATURES

- **PASSWORD GENEIOUS** intercepts passwords when they are changed
- In a Microsoft Active Directory (AD) or domain environment, this can be run on the domain controllers
- This new password is transmitted in an encrypted form to the **Password Controller/Propagator**, a module of the Account Geneous server
- The strong encryption used by all the PGS communications ensures that password secrecy is maintained as the changes are propagated
- The **Password Propagator** module of the Account Geneous server determines from the rules how to propagate the password change to target hosts for which the user has access
- LDAP support to synchronise to any LDAP Directory
- Full audit trail with centralised reporting
- Different User-IDs may be mapped together to ensure maximum benefit
- No code installed at the desktop
- APIs and user exits to integrate all applications
- Password Rule checking to ensure compliance with policies

OTHER AVAILABLE GENEIOUS MODULES

ACCOUNT GENEIOUS (AG)

May be implemented 'stand alone'. Web-based provisioning and management of user accounts across multi-platforms.

ACCOUNT GENEIOUS SINGLE SIGN-ON (SSO)

Single access to all the systems and applications of a user with a single user-id and password when implemented with Account Geneous.

PASSWORD GENEIOUS-RESET (PGR)

May be implemented 'stand alone'. User's self-reset of own password without helpdesk intervention

CONTACT & SUPPORT INFORMATION

GENEIOUS Software AG

Stenhaldestrasse 8
CH-8954 Genolève / Zürich
Switzerland

TEL +41 (0)1 747 82 60
FAX +41 (0)1 747 82 61
EMAIL office@geneious.com
support@geneious.com
INTERNET www.geneious.com

UK CONTACT INFORMATION

ProActiva Ltd

The Old Exchange, South Cadbury Way,
Somerset, BA22 7ET United Kingdom

TEL +44 (0)1962 843211
FAX +44 (0)1962 843212
EMAIL sales@geneious-software.co.uk
support@geneious-software.co.uk
INTERNET www.geneious-software.co.uk

WEB ARCHITECTURE



- 1 User enters his password through the machine-specific interface
- 2 The AG password integrator detects this password change and sends it to the AG Server
- 3 The AG password propagator reads the rules for propagation from the DB database (14) or its own reliable rules repository (16)
- 4 The AG Propagator sends the password changes to the target machines

