



Secure Password Management for the Cross-Platform Enterprise

Change All Domain Passwords and Update Configurations Everywhere Credentials are Referenced, Including Services, Tasks, and Objects.

KEY FEATURES

ENUMERATE ACCOUNTS

Enumerate and view every location in the network where every account is used, including services, tasks, SQL accounts, components, and web sites.

RANDOMIZE PASSWORDS

Generate unique, frequently updated passwords for firecall accounts on every system throughout the network.

PASSWORD RECOVERY

Retrieve current passwords on demand through a secure, delegated, and audited web interface.

PASSWORD AUTO-ROLL

Re-randomize passwords after the temporary usage period expires.

ENCRYPTED DATABASE

Store passwords in an AES-256 bit encrypted database with optional hardware-based encryption at FIPS 140-2 levels 2 and 3.

CROSS-PLATFORM SUPPORT

Supports Windows, Linux, and UNIX systems; SQL Server, MySQL, and Oracle accounts; and Cisco IOS devices.

ZERO-TOUCH INSTALL

Operates without deploying or maintaining agents on remote systems.

DELEGATED USERS

Delegates which users can access and utilize stored passwords.

EXTENSIVE LOGGING

Provide password histories to security auditors to verify that all accounts are regularly updated and that IT has control over every system.

In most large enterprises, domain credentials are stored and used with a variety of applications and operating system objects such as services, scheduled tasks, COM+/DCOM objects, SQL accounts, and network devices. When changing the credentials of a domain account or local account, all of these applications and objects that reference existing credentials must also be changed. Otherwise, the account will be locked out, as applications persist in using obsolete credentials too many times. Simply avoiding updates to domain accounts invites the danger that a common local password can be decrypted and used to gain peer-level access throughout the network.

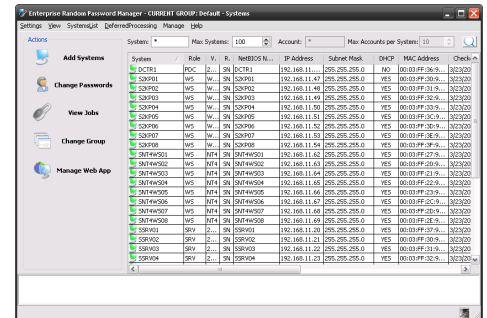
Enterprise Random Password Manager identifies and enumerates every location in the enterprise where every account is used. It then propagates the password change throughout the network to ensure uninterrupted access to resources, while maintaining password security. With Enterprise Random Password Manager, domain accounts can be changed on a regular basis, and users can be assured that the changes are reflected in all applications and objects that reference the account, every time.

RANDOMIZING PASSWORDS

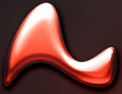
Enterprise Random Password Manager creates unique, cryptographically complex passwords for each account in the enterprise in one operation, all from a single console. Built-in common account passwords and guest account passwords can be scheduled for regular updates, even if the accounts have been renamed. Issuing unique credentials for each account mitigates the threat of peer-to-peer network access.

RECOVERING PASSWORDS

To ensure that administrator or root account passwords are readily available for system administration tasks, Enterprise Random Password Manager provides a delegated web interface to retrieve current passwords. The



Conduct all password management operations throughout the enterprise from one console.



KEY BENEFITS

PRODUCTIVITY

Reduces account lockouts following credentials changes by auto discovering all subsystems where an account is being used.

COMPLIANCE

Helps achieve successful security compliance audits by regularly updating local and domain passwords, and logging all changes.

SECURITY

Strengthens security by generating cryptographically complex passwords unique to each system, mitigating the threat of one decrypted local password leading to unrestricted network access.

MANAGEMENT

Provides comprehensive password management that could not be as reliably accomplished with scripts or manual processes.

passwords are secured in an encrypted database that can be accessed from any web enabled device. The web console integrates with SQL Server to allow administrator delegation over which accounts and systems a user can access. Passwords are issued on a temporary basis and automatically re-randomized after check-in. A complete audit trail of all password operations is maintained.

MAINTAINING COMPLIANCE

Government regulations such as HIPAA, Sarbanes-Oxley, and PCI call for frequent changes to administrator and root account passwords to prevent unauthorized personnel from being able to access critical systems. Enterprise Random Password Manager helps large enterprises accomplish this mandate by tracking where credentials are used and scheduling regular password changes that comprehensively impact every system, application, and object affected by the change. All password operations — including changes, recoveries, and check-ins — are logged and can be sorted, filtered, and provided to security auditors.

AVOIDING SCRIPTS

Enterprise Random Password Manager lets administrators accomplish what could not be done manually. Scripts cannot comprehensively update every place in the enterprise that is impacted by account changes, and they are difficult to document, support, and maintain.

ENSURING SECURITY

Credentials that are stored with Enterprise Random Password Manager are secured via AES-256 bit encryption of data in the database and transmitted with SSL encryption to the browser during password recovery. The product also provides hardware-level encryption when used with any PKCS #11 hardware device.

SUPPORTING MULTIPLE PLATFORMS

Enterprise Random Password Manager randomizes and recovers passwords on Windows NT, 2000, XP, Server 2003, Vista, and Server 2008. It also handles Linux, UNIX, and variations of UNIX, including HP-UX, AIX, Solaris, OS/390, and AS400. Randomization of Microsoft SQL Server, MySQL, and Oracle database accounts and Cisco IOS devices is also supported.

“Enterprise Random Password Manager randomizes passwords and updates an account’s password everywhere the account is used across an entire enterprise network.”

PETER VARHOL

Redmond Magazine

Executive Editor – Reviews

