Kron TECHNOLOGIES

DATASHEET

# Kron PAM Password Vault

Eliminate Your Risk with Shared Account Password Management

## There are always **non-personal** accounts within organizations that have administrative access to localhosts and resources, such as administrator for Windows servers, root for Linux/Unix servers, SYSDBA for oracle DBA, admin for Cisco devices, etc.

Most of the time, the passwords for such local accounts cannot be managed by a central directory server (Active Directory, LDAP) because they are local (designed to be local) on the host. When these **passwords** are compromised it represents a **critical threat** for the enterprise.

Shared accounts are not limited to local administrative accounts and there are many shared accounts within an enterprise infrastructure for different user groups, such as for a group of engineers in a specific region, for an enterprise email account (hr@company.com, info@company.com) or social media accounts of the organization.

Usually, the enterprise's **security policy** requires employees to change the local account password regularly, to use strong passwords, not to share with colleagues, but it is often impossible to ensure that this is successfully implemented, and any shared accounts are properly protected. With the Kron PAM **Password Vault** you can easily eliminate the security risks associate with shared accounts.

## Manage Your Passwords in a Central and Secure Vault

The **Password Vault** removes the vulnerability of a privileged shared account by limiting the lifetime of its password, by **verifying** and accounting for users and by preserving **passwords** in a secure password vault, without having to install an agent to be installed on users' PCs or target servers/ applications.

## The Password Vault can manage accounts on the following platforms;

**Operating Systems:** Windows, macOS, Linux and Unix.
**Databases:** All well-known databases including Oracle, PostgreSQL, MySQL, MSSQL, Cassandra, SAP Sybase, SAP HANA and Teradata.
**Devices and Appliances** with CLI interface that provide password change commands including console access.
**Applications:** All web-based applications such as SAP, Office 365, Google, AWS, Salesforce, Github, JIRA etc.
**Social Media:** Facebook, Twitter, LinkedIn, YouTube and other social media applications. Directory Services with LDAP interface.

## How The Password Vault Works?

### As a Centralized Password Vault

The Kron PAM Password Vault keeps all passwords in a secure, centralized vault, in fully encrypted form and assigns strong and unique passwords to your target hosts, as well as automating randomization of your passwords.

The Password Vault's discovery engine can discover Windows local and domain accounts, including service accounts, network devices, virtual platforms and Linux servers.

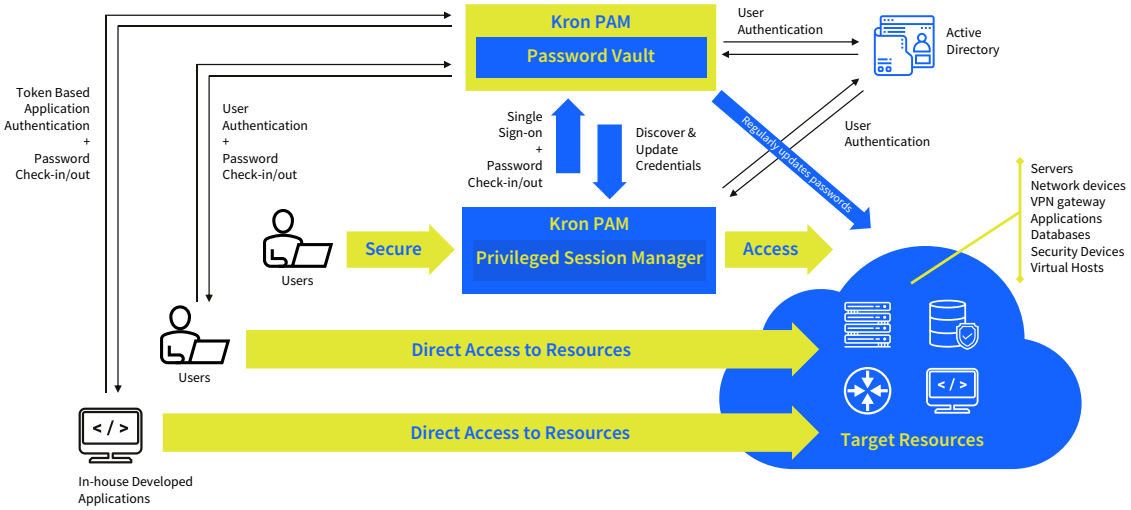
?

**Step 1**
The User logs in to the Kron PAM Password Vault with his/her own username and selects the target host he/she wants to connect to.

**Step 2**
The Kron PAM Password Vault releases the target host's password to the User. This password is a One-Time Password (OTP) and is valid for a limited time (e.g., 1 hour). Kron PAM ensures logging of the entire check-out activity.

**Step 3**
The User connects directly to the target host and logs in with the password he/she just received. Kron PAM is not in the middle.

**Step 4**
At the end of the allotted time (e.g., 1 hour), the Kron PAM Password Vault connects to the target host and changes the password. So, once again, the password is unknown.




## As An Application-To-Application Password Manager

Application accounts are used to access databases, connect network devices or other applications, and run batch jobs or scripts. The passwords for these accounts are often embedded and stored in unencrypted text files, DBs or in source code. Most of the time, these passwords are not changed regularly and can easily be found by people who have access to the server that application runs on, which constitutes a security vulnerability.

The Kron PAM AAPM enables enterprises to remove these static passwords stored in applications and keep them in the secure Password Vault. Kron PAM provides a token-based authentication for 3rd party applications while accessing the password vault. This authentication process verifies the application identity and gives secure access to the password associated with that identity.

### Step 1
The Application asks Kron PAM AAPM for the password (of a target host) via secure API.

### Step 2
After Kron PAM successfully authenticates the Application, it delivers the target host's password to the Application via API. This password is a One-Time Password (OTP) and is valid for a limited time (e.g., 1 hour).

### Step 3
The Application directly connects to the target host and logs in with the password it just received. Kron PAM is not in the middle.

### Step 4
At the end of the allotted time (e.g., 1 hour), the Kron PAM Password Vault connects to the target host and changes the password. So, once again, the password is unknown.

## Feature & Benefits

Ensures the real user of the local account is indisputable.

The Kron PAM Password Vault logs which real user checked out the OTP (One -Time Password), along with the beginning and end times.

Ensures strong **passwords** are used for local and service accounts by having the Single Connect Password Vault generate them.

Keep all services and client applications passwords **up-to-date** by having the Kron PAM Password Vault update them.

Eliminates the use of **non-expiry** passwords.The Kron PAM Password Vault changes the password after every use – One-Time Password

The passwords are not shared among employees. The password is valid for a limited time and even if an employee shares it, he/she is still accountable because Kron PAM Password Vault **indisputably** logs which real user checked out the One-Time Password.

The passwords are stored securely. You never know how and where **employees** store passwords (sometimes in a text file, sometimes in the cloud), but the Kron PAM Password Vault stores the passwords securely in a vault.

Auto lock user accounts when employees terminate employment (integration with enterprise **Active** Directory or LDAP is required).

**Auto** enable new user accounts with privileges when new employees start working (integration with enterprise Active Directory or **LDAP** is required).

The password of the critical systems can be split into pieces by the **Password Vault** so that a connection to that system can be authorized by the participation of all users – **Split** Password

One or two-level **managerial approval** processes can be applied for password check-out – Managerial Approval.

The password **reservation** feature allows users to reserve the password for future usage.

The secure vault also stores and manages sensitive information such as **private** passwords, documents, and digital identities (SSH keys, certificates and digital assets).