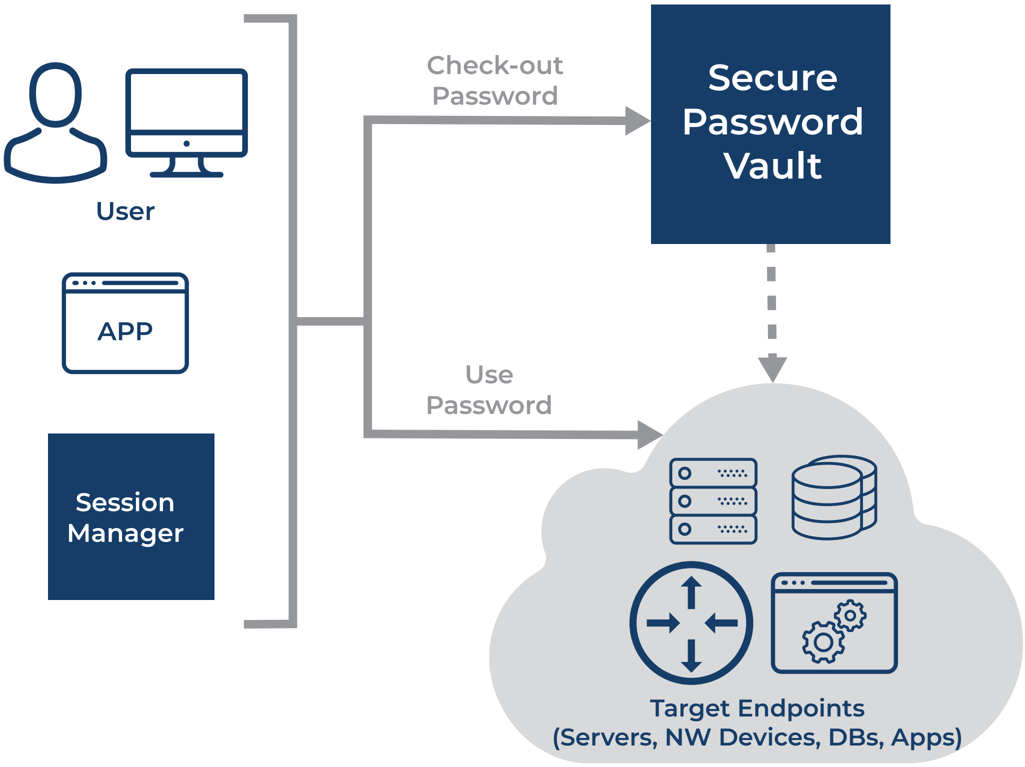
Dynamic Password Controller

Shared accounts are non-personal accounts. Local Administrative Accounts that provide administrative access to the local host, such as administrator for Windows servers, root for Unix servers, SYSDBA for oracle DBA, admin for Cisco devices, etc., often have the same password across an entire organization for ease of use, and the involved staff is aware of it.

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. These passwords can be compromised; this 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, or for an enterprise email account (hr@company.com, corpcom@company.com).

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 it is successful implemented, and any shared accounts are properly protected.

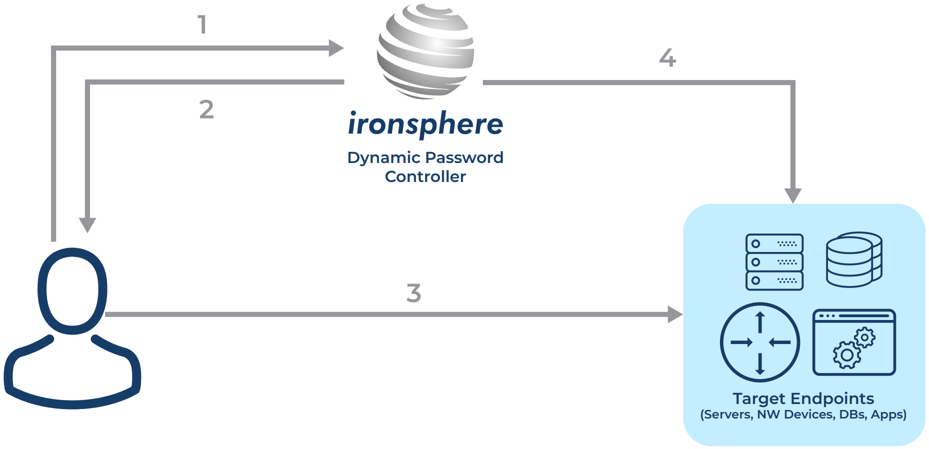


Ironsphere's Dynamic Password Controller is a secure password vault. It does not require an agent to be installed on the User PCs or target servers/applications.

The Dynamic Password Controller supports:

- Operating Systems: Windows, Linux and Unix.
- Databases: All well-known databases including Oracle, PostgreSQL, MySQL, MSSQL.
- Devices and Appliances with CLI interface Applications that provide password change API.
- Directory Services with LDAP interface.

How the Dynamic Password Controller (DPC) Works



Step 1: The User logs in to Ironsphere's Dynamic Password Controller with his/her own username and selects the target host he/she wants to connect to.

Step 2: The Ironsphere Dynamic Password Controller 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).

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

Step 4: At the end of allotted time (e.g. 1 hour), the Ironsphere Dynamic Password Controller connects to the target host and changes the password. So, once again, the password is unknown.

Features & Benefits

» Makes sure the real user of the local account is indisputable. Ironsphere logs which real user checked out the OTP (One-Time Password), along with the beginning and end times.

» Makes sure strong passwords are used for local accounts by having Ironsphere generate them.

» Eliminates usage of non-expiry passwords. Ironsphere changes the password after every use - One-Time Password.

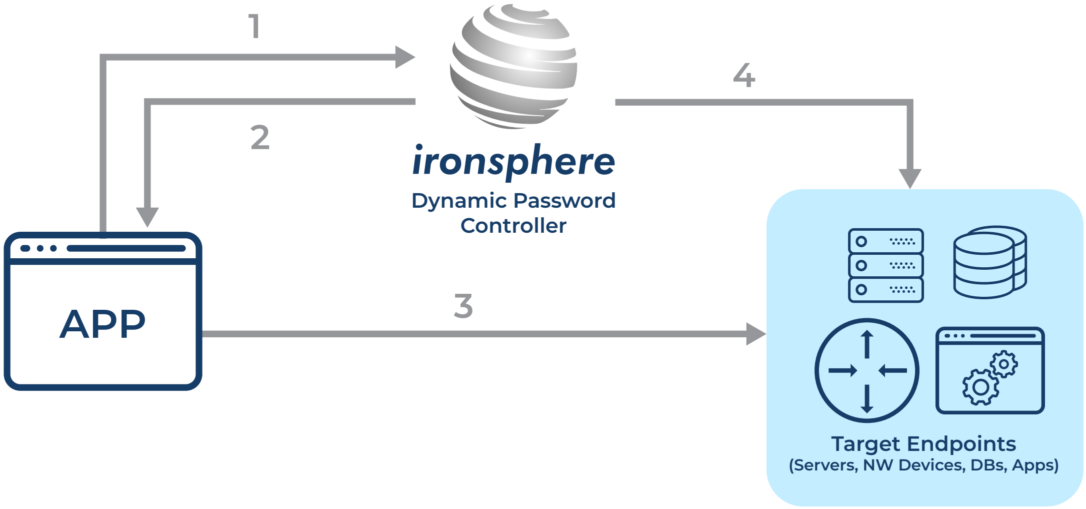
» The passwords are not shared among employees. The password is valid for a limited time and even if an employee shares it, he is still accountable because Ironsphere indisputably logs which real user checked out the One-Time Password.

» The passwords are stored securely. You never know how and where employees store the passwords (sometimes in a text file, sometimes in the cloud), but Ironsphere stores the passwords securely, in a vault.

» Auto lock user account when an employee terminates employment (integration with enterprise Active Directory or LDAP is required).

How Application to Application Dynamic Password Controller (AADPC) Works

Application accounts are used to access databases, connect network devices or other applications, run batch jobs or scripts. The passwords for these accounts are often embedded and stored in unencrypted text files, DB 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.



Step 1: The Application asks the Ironsphere Dynamic Password Controller for the password (of a target host) via API.

Step 2: After Ironsphere 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. Ironsphere is not in the middle.

Step 4: At the end of allotted time (e.g. 1 hour), the Ironsphere Dynamic Password Manager connects to the target host and changes the password. So, once again, the password is unknown.

Features & Benefits

- Makes sure the real user of the local account is indisputable. Ironsphere logs which real user checked out the OTP (One-Time Password), along with the beginning and end times.
- Makes sure strong passwords are used for local accounts by having Ironsphere generate them.
- Eliminates usage of non-expiry passwords. Ironsphere 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 is still accountable because Ironsphere indisputably logs which real user checked out the One-Time Password.
- The passwords are stored securely. You never know how and where employees store the passwords (sometimes in a text file, sometimes in the cloud), but Ironsphere stores the passwords securely, in a vault.
- Auto lock user account when an employee terminates employment (integration with enterprise Active Directory or LDAP is required).