Solution Brief

Dynamic Password Controller for Human Users

Ironsphere
A Krontech Company

Introduction

Ironsphere provides a centralized password management service that allows users to access privileged accounts. Privileged accounts should be available through a system that can be accessed securely by authorized technical staff. Ironsphere's Dynamic Password Controller (DPC) enables users with different access levels and fully manages and maintains privileged accounts, recording privileged users' access and activities indisputably in readable and searchable logs. In this way, DPC prevents the use of privileged accounts without tracking and accountability.

The Dynamic Password Controller enforces user compliance with certain standards and account access procedures, as part of a complete privileged account management strategy.

For details on the use of privileged accounts in Infrastructure Systems and Applications, please refer to the Ironsphere "Dynamic Password Controller" Solution Brief.

- The Dynamic Password Controller generates new passwords periodically and changes these passwords by connecting to devices. Changed passwords are checked and stored securely.
- Users connect to the Dynamic Password Controller to access privileged accounts and get updated account passwords. They can access the system with their individual account credentials.
- Access to devices is indirectly blocked, as users have no direct access to the privileged account passwords managed by the Dynamic Password Controller.

In line with a zero-trust/zero-knowledge policy, the user is only required to know their individual access credentials to Ironsphere.

Beyond that point, access to privileged accounts is entirely managed by the Dynamic Password Controller and, depending on the importance/critical nature of the privileged account, and/or the necessary level of security, the DPC allows for multiple approaches to accommodate different business use cases.

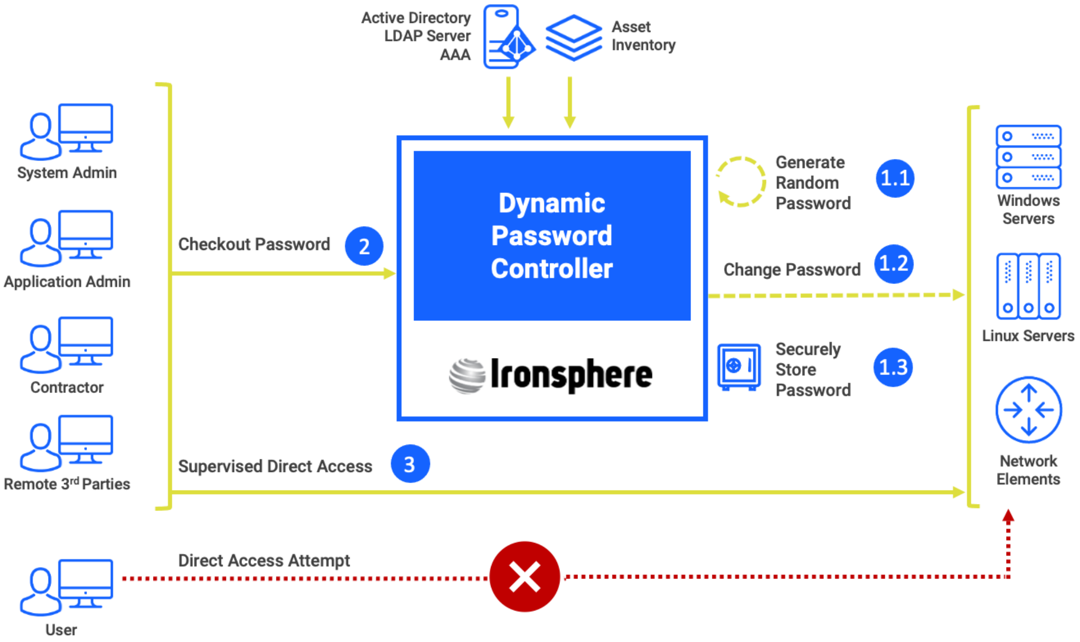

Figure 1 — Dynamic Password Controller

Password Check Out

Users need to check out the password from the DPC to connect to a device.

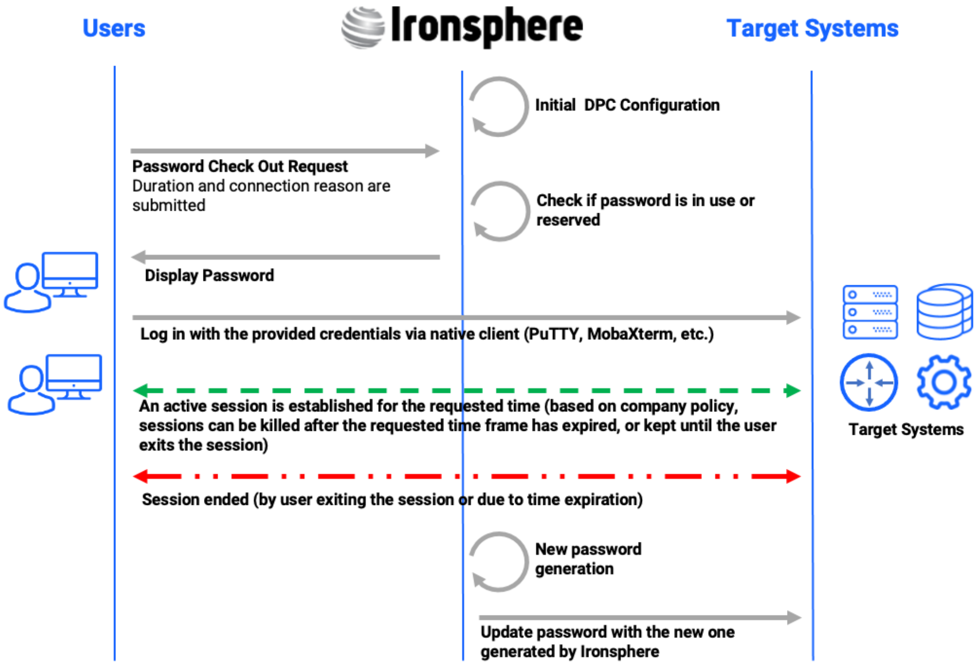
Users
Ironsphere
Target Systems
Initial DPC Configuration
Password Check Out Request
Duration and connection reason are submitted
Check if password is in use or reserved
Display Password
Log in with the provided credentials via native client (PuTTY, MobaXterm, etc.)
An active session is established for the requested time (based on company policy, sessions can be killed after the requested time frame has expired, or kept until the user exits the session)
Target Systems
Session ended (by user exiting the session or due to time expiration)
New password generation
Update password with the new one generated by Ironsphere

Figure 2 — Password Check Out

Password Check Out Request: The user sends a password check out request by providing information on why, and for how long they need the password.

Check Password Use Status: Ironsphere checks if the password is in use or reserved for the requested time frame, and will allow only one user to use the password at a time. If the password is in use or is reserved, Ironsphere will not release the password to the requester.

Display Password: If the password is not reserved or in use, Ironsphere shows the password to the user who requested it.

Log in to Target System: The user can use the provided password to connect to the target system via any native client.

Session Established: An active session is established between the user and Ironsphere. Since the connection is made via native client while using the password to connect directly to the device, Ironsphere cannot log the session itself, but the password checkout logs are recorded by Ironsphere.

Session Ended: When the password reservation or checkout time has expired, the ongoing session can be kept up until the user leaves, or it can be terminated by Ironsphere. An Ironsphere admin can configure these parameters based on company policies. If the user terminates the session before the allocated time runs out, they can reset the password manually from Ironsphere to release it for checkout.

New Password Generation: Upon timeout, Ironsphere generates a new password.

Update Password: Ironsphere logs in to the device and updates the password, after the reservation timeout or check out.

Password Reservation

Users can request a reservation for a password checkout. This feature is mainly used for maintenance activities and when there is a specific timeslot during which the user needs to access the device. Because the DPC is designed to prevent simultaneous usage of the credentials (username/password), if a user reserves the password for a specific time frame, another user cannot check it out during that time frame. Only one user can use the password at a time.

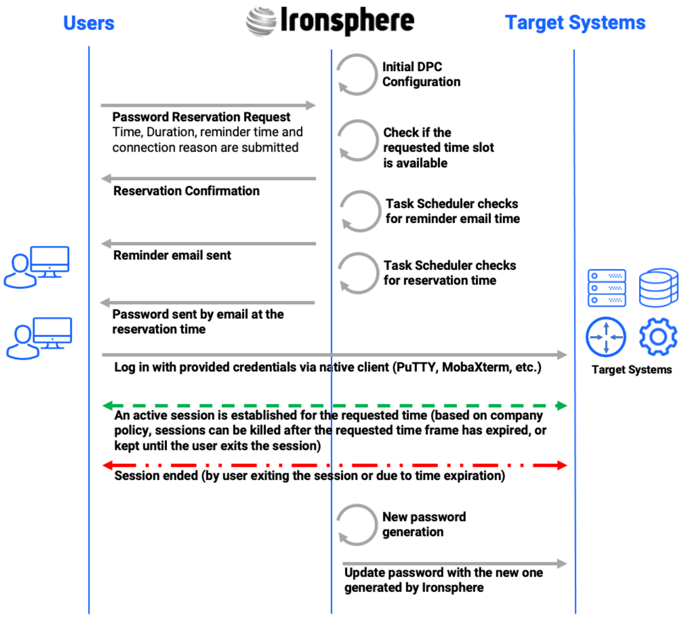
Users
Ironsphere
Target Systems
Initial DPC Configuration
Password Reservation Request
Time, Duration, reminder time and connection reason are submitted
Check if the requested time slot is available
Reservation Confirmation
Task Scheduler checks for reminder email time
Reminder email sent
Task Scheduler checks for reservation time
Password sent by email at the reservation time
Target Systems
Log in with provided credentials via native client (PuTTY, MobaXterm, etc.)
An active session is established for the requested time (based on company policy, sessions can be killed after the requested time frame has expired, or kept until the user exits the session)
Session ended (by user exiting the session or due to time expiration)
New password generation
Update password with the new one generated by Ironsphere

Figure 3 — Password Reservation

Password Reservation Request: The user sends a password reservation request by providing information on when, why, and for how long they need the password. If the reservation request is accepted, Ironsphere sends a reminder email for the upcoming timeslot, by default, 15 minutes before the password email is sent. This can be configured by the user.

Check Time Frame for Other Reservations: Ironsphere checks if there is an existing reservation for the requested time frame, and will allow only one user to use the password at a time. If there is a conflicting reservation for the requested timeslot, Ironsphere will not release the password to the requester.

Reservation Confirmation: If the requested timeslot is available, Ironsphere reserves it for the requester.

Task Scheduler Checks Reminder Email Time: The Task Scheduler runs frequent checks on when the email reminder must be sent.

Reminder Email Sent: When the time comes, Ironsphere sends the reminder email to the user.

Task Scheduler Checks Reservation Time: The Task Scheduler runs frequent checks on when the reservation time starts.

Password Sent by Email: When the time comes, Ironsphere sends out the password via email. The user can also go and check out the password directly from the Ironsphere Web GUI. No other user can check out or make a reservation for this reserved time frame.

Log in to Target System: After receiving the password, the user can use it with any native client to connect to the target system.

Session Established: An active session is established between the user and Ironsphere. Since the connection is made via native client while using the password to connect directly to the device, Ironsphere cannot log the session itself, but the password checkout logs are recorded by Ironsphere.

Session Ended: When the password reservation or checkout time has expired, the ongoing session can be kept up until the user leaves, or it can be terminated by Ironsphere. An Ironsphere admin can configure these parameters based on company policies. If the user terminates the session before the allocated time runs out, they can reset the password manually from Ironsphere to release it for checkout.

New Password Generation: Upon timeout, Ironsphere generates a new password.

Update Password: Ironsphere logs in to the device and updates the password, after the reservation timeout or check out.

Managerial Approval for Password Check Out

Admins can create a managerial approval policy for password check out. In the example below, SAPM admin users manage requests from users who need approval to check out the password.

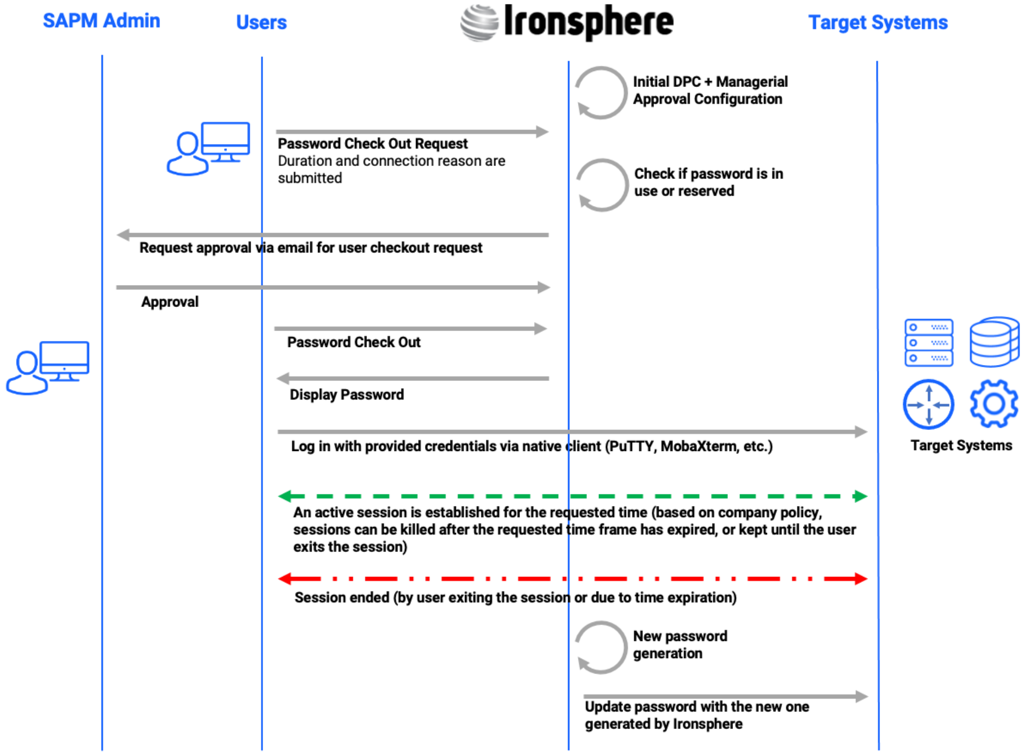
SAPM Admin
Users
Ironsphere
Target Systems
Initial DPC + Managerial Approval Configuration
Password Check Out Request
Duration and connection reason are submitted
Check if password is in use or reserved
Request approval via email for user checkout request
Approval
Password Check Out
Display Password
Target Systems
Log in with provided credentials via native client (PuTTY, MobaXterm, etc.)
An active session is established for the requested time (based on company policy, sessions can be killed after the requested time frame has expired, or kept until the user exits the session)
Session ended (by user exiting the session or due to time expiration)
New password generation
Update password with the new one generated by Ironsphere

Figure 4 — Managerial Approval for Password Check Out

Password Check Out Request: The user sends a password check out request by providing information on why, and for how long they need the password.

Check Password Use Status: Ironsphere checks if the password is in use or reserved for the requested time frame, and will allow only one user to use the password at a time. If the password is in use or is reserved, Ironsphere will not release the password to the requester.

Approval Request: Ironsphere sends an email to the designated SAPM Admin. A check out approval request does not create a reservation; therefore, during the approval process, the password is not reserved and can be checked out by another user. If another user checks out the password during the approval process, the SAPM Admin cannot approve the request until the other user terminates their session.

Approval: The SAPM Admin can approve or reject a request. If the SAPM Admin approves the request, the checkout process continues.

Password Check Out: The user checks out the password after the request is approved.

Display Password: If the password is not reserved or in use, Ironsphere shows the password to the user who requested it.

Log in to Target System: The user can use the provided password to connect to the target system via any native client.

Session Established: An active session is established between the user and Ironsphere.

Since the connection is made via native client while using the password to connect directly to the device, Ironsphere cannot log the session itself, but the password checkout logs are recorded by Ironsphere.

Session Ended: When the password reservation or checkout time has expired, the ongoing session can be kept up until the user leaves, or it can be terminated by Ironsphere. An Ironsphere admin can configure these parameters based on company policies. If the user terminates the session before the allocated time runs out, they can reset the password manually from Ironsphere to release it for checkout.

New Password Generation: Upon timeout, Ironsphere generates a new password.

Update Password: Ironsphere logs in to the device and updates the password, after the reservation timeout or check out.

Password Split

Admins may want to increase the security level by pairing users and splitting the password between them. This mostly occurs when companies want to control third-party user access by shadowing them. In such cases, Ironsphere can split the password into two pieces and give them to two separate users. By doing so, these two users are forced to log in together, merging their password pieces to make it whole. This is also applicable to a new user who needs to be overseen by experienced users.

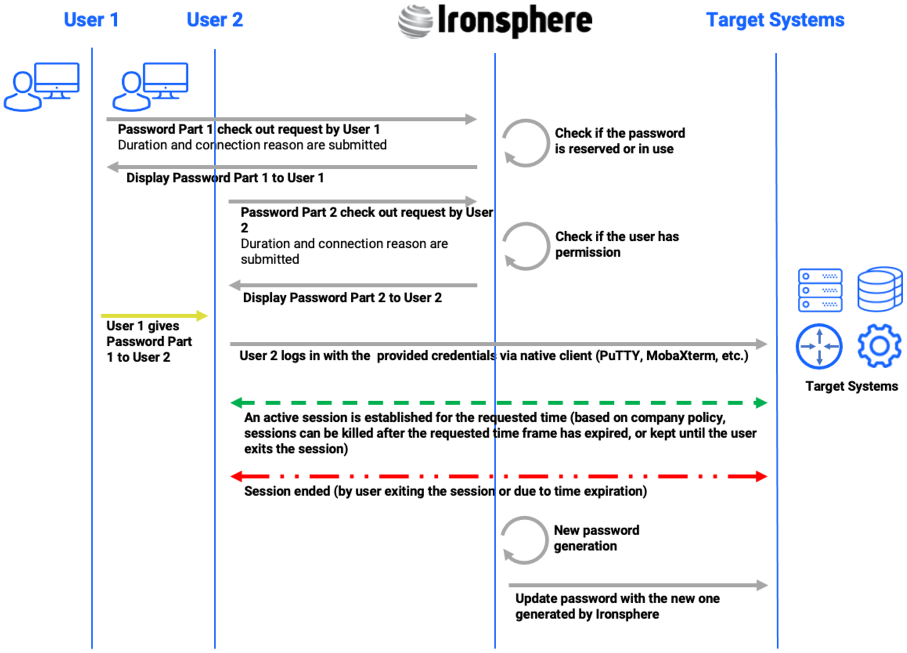
User 1
User 2
Ironsphere
Target Systems
Password Part 1 check out request by User 1
Duration and connection reason are submitted
Check if the password is reserved or in use
Display Password Part 1 to User 1
Password Part 2 check out request by User 2
Duration and connection reason are submitted
Check if the user has permission
Display Password Part 2 to User 2
User 1 gives Password Part 1 to User 2
User 2 logs in with the provided credentials via native client (PuTTY, MobaXterm, etc.)
Target Systems
An active session is established for the requested time (based on company policy, sessions can be killed after the requested time frame has expired, or kept until the user exits the session)
Session ended (by user exiting the session or due to time expiration)
New password generation
Update password with the new one generated by Ironsphere

Figure 5 — Password Split

Password Part 1 Check Out Request: User 1 submits a password check out request by providing information on why, and for how long the password is needed.

Check Password Use Status: Ironsphere checks if the password is in use or reserved for the requested time frame, and will allow only one user to use the password at a time. If the password is in use or is reserved, Ironsphere will not release the password to the requester.

Display Password: If the password is not reserved or in use, Ironsphere shows the 1st part of the password to User 1.

Password Part 2 Check Out Request: User 2 submits a password check out request by providing information on why, and how long the password is needed.

Check Password Use Status: Ironsphere checks if the full password is in use, other than by User 1.

Display Password: If the password is not reserved or in use, Ironsphere shows the 2nd part of the password to User 2.

Password Exchange by Users: The split password parts need to be merged to connect to the target system. In this example, User 1 gives their part to User 2.

Log in to Target System: User 2 merges the password parts and connects to the target system via a native client.

Session Established: An active session is established between the user and Ironsphere. Since the connection is made via native client while using the password to connect directly to the device, Ironsphere cannot log the session itself, but the password checkout logs are recorded by Ironsphere.

Session Ended: When the password checkout time has expired, the ongoing session can be kept until the user leaves, or it can be terminated by Ironsphere. An Ironsphere admin can configure these parameters based on company policies. If the user terminates the session before the allocated time runs out, they can reset the password manually from Ironsphere to release it for checkout.

New Password Generation: Upon timeout, Ironsphere generates a new password.

Update Password: Ironsphere logs in to the device and updates the password, after the reservation time out.

Conclusion

Password management for several accounts on its own is a cumbersome task. Adding security, compliance, and audit requirements on top of that makes it virtually impossible to manage without a specialized system. The Ironsphere Dynamic Password Controller eases our lives immensely, with more than a few benefits:

- Makes sure the real user of the local account is indisputable. Ironsphere logs which real user checked out the password, along with the session beginning and end times.
- Makes sure strong passwords are used for privileged accounts by having Ironsphere generate them.
- Eliminates the use of non-expiry passwords. Ironsphere changes the password after every use.
- 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 Ironsphere indisputably logs which real users checked out the password.
- The passwords are stored securely. You never know how and where employees store the passwords, but Ironsphere stores the passwords securely in its Dynamic Password Controller.

Ironsphere
A Krontech Company