Solution Brief

Dynamic Password Controller for Applications

Ironsphere
A Krontech Company

Introduction

Ironsphere provides centralized and unified management of privileged accounts. Accounts are stored securely and encrypted in a digital vault, and passwords are auto changed (rotated) regularly.

Some applications use privileged credentials to access other servers, systems, or databases to perform their tasks. Those privileged credentials are embedded in the script itself, or stored in configuration files or application databases, exposed and easily stolen by people who gain access to those scripts and applications.

Ironsphere's digital vault provides capabilities for scripts and applications, making those credentials invisible to users.

Typically there are two broad categories of applications of interest; custom applications, ranging from utility scripts to full-fledged in-house built solutions, where the customer has control over the contents of the applications; and commercial off-the-shelf applications, which may offer limited interfaces for password management and/or integrations.

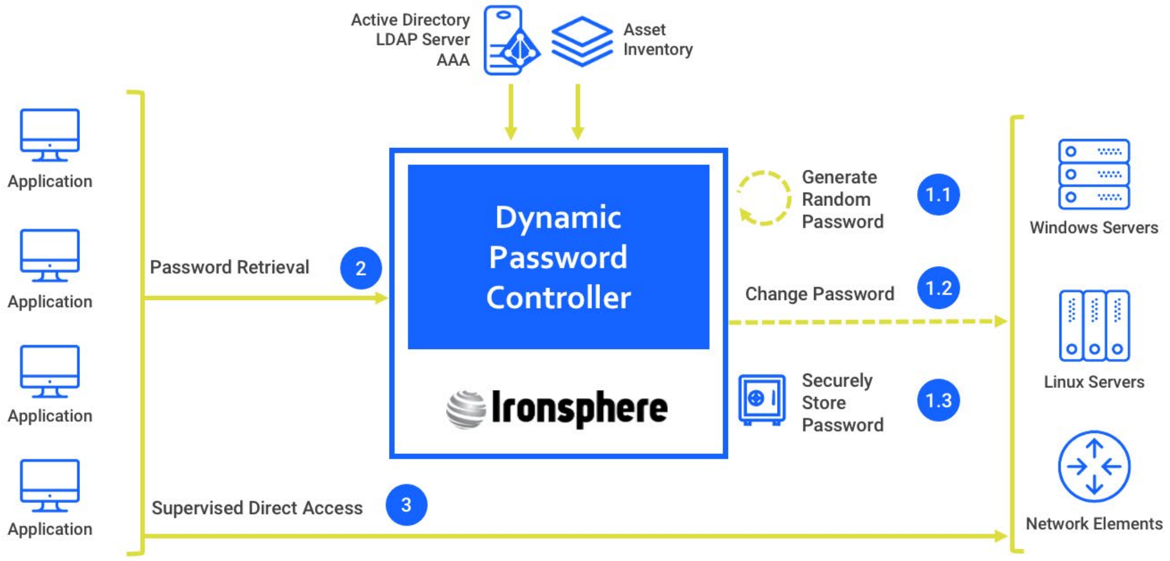

Figure 1 — Password Retrieval & Target Access with Dynamic Password Controller

Custom Applications

When an application needs privileged credentials to perform its operations, it retrieves them from Ironsphere's digital vault on-demand, and uses them without storing. Before an application retrieves the credentials from Ironsphere's vault, there are four available options to meet the required level of trust:

1 – Basic Authentication (IP)

2 – Basic + PIN Authentication

3 – Basic + PIN + Path

4 – Basic + PIN + Path + Hash

1 – Password Retrieval for Applications (Basic Security Level)

The Basic security level in password retrieval by an application ensures that the request comes to Ironsphere from the allowed source IP address. The application sends the password retrieval request with a specified token. If the application IP matches the predefined IP in Ironsphere, the password is shared in response to the request. The application can now access the device and execute essential operations using the shared password.

Update password periodically: Predefined passwords in the Dynamic Password Controller can be updated periodically.

Send password retrieval request: The application sends an API request to fetch the target device password.

Check application IP: At the Basic security level, Ironsphere checks the IP of the server the application request originates from. If it does not match the predefined IP, the password is not shared.

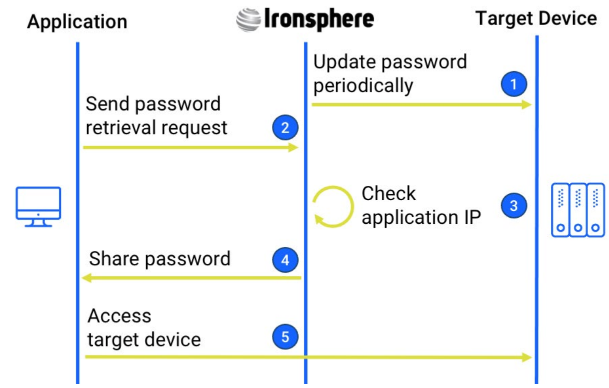

Figure 2 — Password Retrieval for Applications, Basic Security Level

Share password: If the security conditions are satisfied, Ironsphere shares the password with the application in response to the API request.

Access target device: The application can access the target device after getting the password from the Dynamic Password Controller.

2 – Password Retrieval for Applications (Basic + PIN Security Level)

The Basic + PIN security level in password retrieval by an application ensures that the request comes to Ironsphere from the allowed source IP address. The application sends the password retrieval request with a specified token. If the application IP matches the predefined IP in Ironsphere, a PIN code is shared with the application using a predefined port on the application server. The application sends the retrieval request again. After the PIN is checked, the password is shared in response to the request. The application can now access the device and execute essential operations using the shared password.

Update password periodically: Predefined passwords in the Dynamic Password Controller can be updated periodically.

Send password retrieval request: The application sends an API request to fetch the target device password.

Check application IP: At the Basic security level, Ironsphere checks the IP of the server the application request originates from. If it does not match the predefined IP, the password is not shared.

Send an access PIN to a predefined port: Ironsphere sends a PIN code to the predefined port of the server where the application runs.

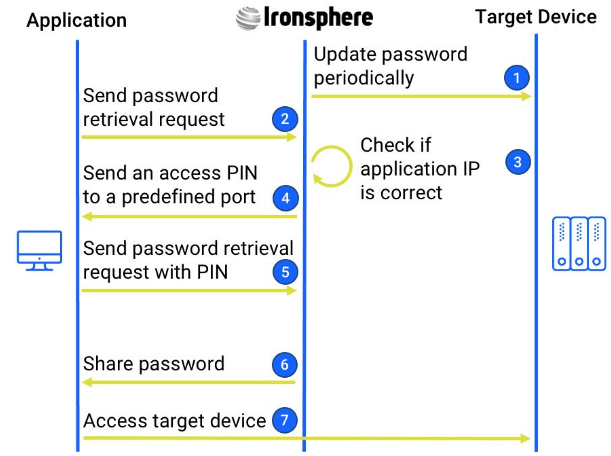
Application
Ironsphere
Target Device
Update password periodically 1
Send password retrieval request 2
Check if application IP is correct 3
Send an access PIN to a predefined port 4
Send password retrieval request with PIN 5
Share password 6
Access target device 7

Figure 3 — Password Retrieval for Applications, Basic + PIN Security Level

Send password retrieval request with PIN: The application sends a retrieval request with the PIN code received from Ironsphere.

Share password: If the security conditions are satisfied, Ironsphere shares the password with the application in response to the API request.

Access target device: The application can access the target device after getting the password from the Dynamic Password Controller.

3 – Password Retrieval for Applications (Basic+PIN+Path Security Level)

The Basic + PIN + Path security level in password retrieval by an application ensures that the request comes to Ironsphere from the right IP, enhancing the security level with a PIN code and application path control. The application sends the password retrieval request with a specified token. If the application IP matches the predefined IP in Ironsphere, a PIN code is shared with the application using a predefined port on the application server. The application sends the retrieval request again. After the PIN is checked, Ironsphere connects to the application server and checks if the actual application path matches the predefined application path. If these checks are successful, the password is shared in response to the request. The application can now access the device and execute essential operations using the shared password.

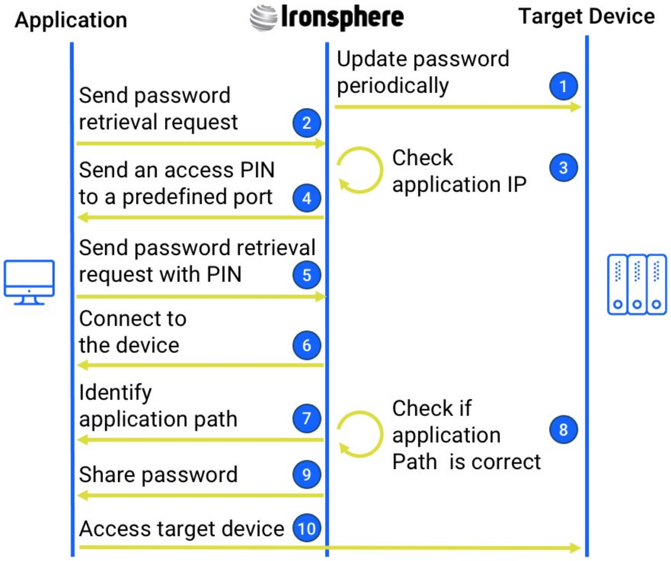
Application
Ironsphere
Target Device
Update password periodically 1
Send password retrieval request 2
Check application IP 3
Send an access PIN to a predefined port 4
Send password retrieval request with PIN 5
Connect to the device 6
Identify application path 7
Check if application Path is correct 8
Share password 9
Access target device 10

Figure 4 — Password Retrieval for Applications, Basic+PIN+Path Security Level

Update password periodically: Predefined passwords in the Dynamic Password Controller can be updated periodically.

Send password retrieval request: The application sends an API request to fetch the target device password.

Check application IP: At the Basic security level, Ironsphere checks the IP of the server the application request originates from. If it does not match the predefined IP, the password is not shared.

Send an access PIN to a predefined port: Ironsphere sends a PIN code to the predefined port of the server where the application runs.

Send password retrieval request with PIN: The application sends a retrieval request with the PIN code received from Ironsphere.

Connect to the device: Ironsphere connects to the device where the application runs.

Identify application path: Ironsphere detects the application path.

Check if application path is correct: The application path is cross-checked with the predefined values in Ironsphere. If they do not match, the password is not shared.

Share password: If the security conditions are satisfied, Ironsphere shares the password with the application in response to the API request.

Access target device: The application can access the target device after getting the password from the Dynamic Password Controller.

4 – Password Retrieval for Applications (Basic+PIN+Path+Hash)

The Basic + PIN + Path + Hash security level in password retrieval by an application ensures that the request comes to Ironsphere from the right IP, enhancing the security with a PIN code, application path and hash control. The application sends the password retrieval request with a specified token. If the application IP matches the predefined IP in Ironsphere, a PIN code is shared with the application using a predefined port on the application server. The application sends the retrieval request again. After the PIN is checked, Ironsphere connects to the application server and checks if the application path and hash match the predefined values. If these checks are successful, the password is shared in response to the request. The application can now access the device and execute essential operations using the shared password.

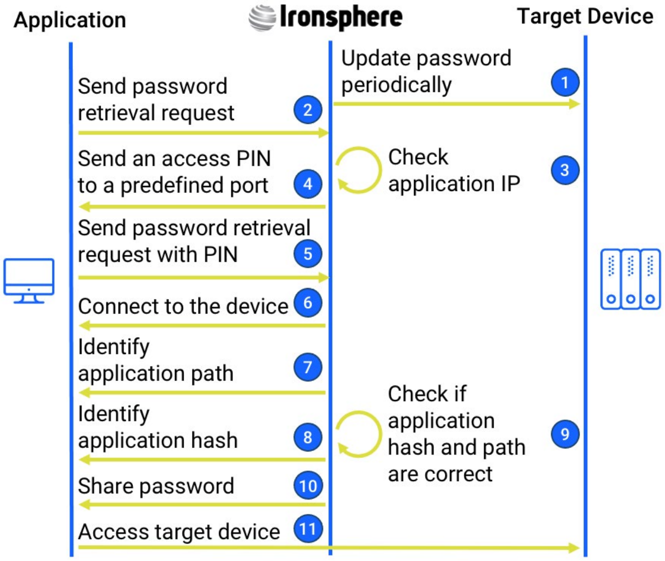
Application
Ironsphere
Target Device
Update password periodically 1
Send password retrieval request 2
Send an access PIN to a predefined port 4
Check application IP 3
Send password retrieval request with PIN 5
Connect to the device 6
Identify application path 7
Identify application hash 8
Check if application hash and path are correct 9
Share password 10
Access target device 11

Figure 5 — Password Retrieval for Applications, Basic+PIN+Path+Hash Security Level

Update password periodically: Predefined passwords in the Dynamic Password Controller can be updated periodically.

Send password retrieval request: The application sends an API request to fetch the target device password.

Check application IP: At the Basic security level, Ironsphere checks the IP of the server the application request originates from. If it does not match the predefined IP, the password is not shared.

Send an access PIN to a predefined port: Ironsphere sends a PIN code to the predefined port of the server where the application runs.

Send password retrieval request with PIN: The application sends a retrieval request with the PIN code received from Ironsphere.

Connect to the device: Ironsphere connects to the device where the application runs.

Identify application path: Ironsphere detects the application path.

Identify application hash: Ironsphere detects the application hash.

Check if application hash and path are correct: The application path and hash data is cross-checked with the predefined values in Ironsphere. If they do not match, the password is not shared.

Share password: If the security conditions are satisfied, Ironsphere shares the password with the application in response to the API request.

Access target device: The application can access the target device after getting the password from the Dynamic Password Controller.

Commercial Off-the-Shelf Applications

The Password Injection feature of the Dynamic Password Controller enables the implementation of periodic password change schemes for applications that do not offer native integrations for password management. Unchanged, static passwords used for service accounts have a very high risk of exposure. Password injection mitigates this risk by changing passwords periodically and eliminating any human interaction from the password management process. Ironsphere will periodically connect to the instance/ device running the application/service and update the password. The Dynamic Password Controller makes enforcing complex password rules and periodic password changes sustainable and secure.

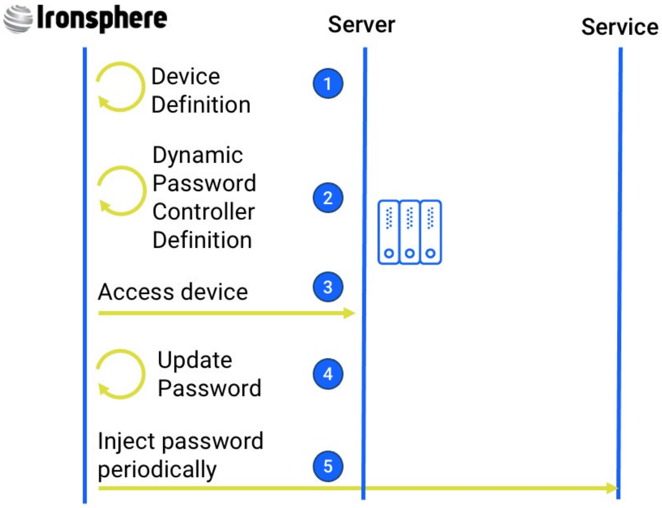

Figure 6 — Password Injection

Device definition: The device where the application or service runs, is defined in Ironsphere.

Dynamic Password Controller definition: The password definitions are made.

Access device: Ironsphere accesses the device where the password should be injected.

Update password: Ironsphere updates password periodically.

Inject password periodically: Ironsphere injects the password periodically.

Conclusion

Ironsphere provides centralized and unified management of privileged accounts. The Dynamic Password Controller enables password rotation of privileged accounts in the technology infrastructure, securely storing them in an encrypted vault, and auto changing and generating random strong passwords at regular intervals.

Applications can retrieve these passwords and access target servers. Different levels of security mechanisms can be applied while retrieving these passwords, without exposing them to human resources. When an application attempts to retrieve a password from the Ironsphere digital vault, the required level of security must be met, such as IP Address, PIN, hash, and path validations. Ironsphere also injects passwords to services, to assure there is no human involvement in the password rotation process.

Ironsphere
A Krontech Company