Predict | Protect | Prevent

ARCON|PAM

Password Management Offerings

arcon

Table of Contents

Disclaimer

The handbook of ARCON PAM solution is being published to guide stakeholders and users. If any of the statements in this document are at variance or inconsistent it shall be brought to the notice of ARCON through the support team. Wherever appropriate, references have been made to facilitate better understanding of the PAM solution. ARCON team has made every effort to ensure that the information contained in it was correct at the time of publishing.
Nothing in this document constitutes a guarantee, warranty, or license, expressed or implied. ARCON disclaims all liability for all such guarantees, warranties, and licenses, including but not limited to: Fitness for a particular purpose; merchantability; non-infringement of intellectual property or other rights of any third party or of ARCON; indemnity; and all others. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technologies discussed herein, and is advised to seek the advice of competent legal counsel, without obligation of ARCON.

Trademarks
Other product and corporate names may be trademarks of other companies and are used only for explanation and to the owners' benefit, without intent to infringe.

Sales Contact
You can directly contact us with sales related topics at the email address <sales@arconnet.com>, or leave us your contact information and we will call you back.

1 Overview

Password management a large number of passwords and account information. They store the login information of the various accounts and automatically enter them into the forms. This helps in the prevention of hacker attacks like keystroke logging and it prevents the need to remember multiple passwords.

Password managers enable the use of strong and unique passwords for each online account and provide an efficient way to manage all the passwords. The login information is encrypted and stored in either the local memory of the user's system or in cloud storage. Portable password manager applications installed in mobile devices can also be used as a way to manage and remember passwords anywhere and use them on shared systems.

Password managers usually incorporate some additional features like automatic form filling and password generation. The automatic form filling feature fills in the login information for a particular URL whenever it loads, and thus reduces manual errors and protects systems from hacker attacks such as keylogging. As password managers can identify the right URL for a particular login ID and password pair automatically, they are capable of protecting credentials from phishing sites. The automatic password generation feature available in certain password managers helps to create strong, unique and random passwords for each account.

1.1 Why ARCON PAM Password Management?

Mismanagement of Privileged Users and their passwords is a major cause of security breaches and one of the top reasons for passwords unavailability that leads to a long recovery process from IT failures. Password Management helps a user store and organize passwords. Password Manager offers a readily configurable password policy profiler and a password generator, where the passwords generated are unique from each other. The passwords generated are fired on the end devices including dependencies if any, such as services, task, scripts etc. The password vault is an electronic vault, which stores the privileged passwords in a highly secured manner. The vault is AES-256 bit encrypted, which is further wrapped with a proprietary encryption algorithm. The electronic vault requires the authorization of users for secured printing.

The password vault secures all the passwords with its proprietary encryption methodology. Further, it provides dynamic password generation facility, which incorporates the following:

- The Vault can enforce a password policy to avoid usage of passwords that can be easily guessed.
- The password policy defines rules for the password content such as the length, combination of different types of characters, and password history.
- The password configuration includes parameters such that the user can select the appropriate parameters based on the IT Security Policy of your organization.
- Further password management module enables Administrator to perform bulk password changes on scheduled intervals.

The password management module also offers the following:

- Automated password change for various systems viz Unix, Linux, Solaris, AIX, Win2K3, Win2K8, Oracle, MS SQL, Services, DCOM etc.
- The password connectors available are both agent-based and agentless. The agentless connectors offer scalability and the agent-based connectors offer control on the password management activity and better error trapping.
- There are features to set password dependencies for all the systems and services which ensure that passwords on multiple systems can be common and changed at the same time. In addition, the passwords can be sequentially changed for dependent systems and services.
- The password communication between the ARCON PAM Client and Server is in encrypted form.
- There is a password request mechanism for electronically releasing the password in case hard console access is required.

2 How Does it work?

2.1 Central Password Change

WinVaulting Service is deployed on the Centralized server that needs to run as Domain Operator as a logon user or if installed on AD Server has to be installed using Domain Operator rights and do not require the service to run as logon user.

Central Password Change mechanism will only work in case of the target windows device is part of Domain or LDAP (AD) User. Schedule password change service (which is in PAM Server Zone) will send the request to WinVaulting service to perform the password change activity. (**Annexure 1 for Ports prerequisites)**

Incase of password change via. Gateway is enabled for the service in the configuration of the service then the Schedule password change service (which is in PAM Server Zone) will create a secure tunnel to target WinVaulting service on the centralized server device send the request to WinVaulting service to perform the password change activity. **(Annexure 1.1 for Ports prerequisites)**

2.2 Windows Servers in Domain Password Change for local users (Agentless)

Windows servers in Workgroup or non Domain, password change services will not require any agent like WinVaulting service to perform the password change activity. windows services in ARCON PAM will have to be configured with <WAL> tag in description 4 in addition to the existing configured tags. Workgroup Administrator User with Operator privilege's service should be added in PAM and the service needs to be marked as an administrator for password change in global configuration.

Schedule password change service (which is in PAM Server Zone) will connect to the target device to perform the activity. **(Annexure 2 for Ports prerequisites)**

Incase of password change via. Gateway is enabled for the service in the configuration of the service then the Schedule password change service (which is in PAM Server Zone) will create a secure tunnel to target device to perform the activity. **(Annexure 2.1 for Ports prerequisites)**

2.3 Windows Servers in Domain Password Change for LDAP / AD Account (Agentless)

Windows Servers in Domain Password Change for LDAP / AD account will not require any agent like WinVaulting service to perform the password change activity. windows services in ARCON PAM will have to be configure with <WAL> tag in description 4 in addition to the existing configured tags. Domain User with Operator privilege's service should be added in PAM and the service needs to be marked as an administrator for password change in global configuration.

Schedule password change service (which is in PAM Server Zone) will connect to the target device to perform the activity. **(Annexure 3 for Ports prerequisites)**

Incase of password change via. Gateway is enabled for the service in the configuration of the service then the Schedule password change service (which is in PAM Server Zone) will create a secure tunnel to target device to perform the activity. **(Annexure 3.1 for Ports prerequisites)**

2.4 Windows Servers in Workgroup Password Change for local users (Agentless)

Windows servers in Workgroup or non Domain, password change services will not require any agent like WinVaulting service to perform the password change activity. windows services in ARCON PAM will have to be configure with <WAL> tag in description 4 in addition to the existing configured tags.

Schedule password change service (which is in PAM Server Zone) will connect to the target device to perform the activity. **(Annexure 4 for Ports prerequisites)**

Incase of password change via. Gateway is enabled for the service in the configuration of the service then the Schedule password change service (which is in PAM Server Zone) will create a secure tunnel to target device to perform the activity. **(Annexure 4.1 for Ports prerequisites)**

2.5 Linux | Unix | Network / Security Devices local users Password Change (Agentless)

Password change services will not require any agent like WinVaulting service to perform the password change activity.

Schedule password change service (which is in PAM Server Zone) will connect to the target device to perform the activity. **(Annexure 5 for Ports prerequisites)**

Incase of password change via. Gateway is enabled for the service in the configuration of the service then the Schedule password change service (which is in PAM Server Zone) will create a secure tunnel to target device to perform the activity. **(Annexure 5.1 for Ports prerequisites)**

2.6 Service Account password change

Service Accounts password change can be done on the basis of the feasibility.

⚠ *Service Accounts are to be handled carefully, ARCON will not be responsible for any 3rd party application impact due the password change.*

Alternate practice recommended in such cases, if the application does not allow to change the password is to keep the password in split custody.

2.6.1 Windows AD or OS dependence Service Accounts

WinVaulting Service is deployed on the target server which has to be installed with full privileges.

Schedule password change service (which is in PAM Server Zone) will connect to the target device to perform the activity. **(Annexure 6 for Ports prerequisites)**

Incase of password change via. Gateway is enabled for the service in the configuration of the service then the Schedule password change service (which is in PAM Server Zone) will create a secure tunnel to target device to perform the activity. **(Annexure 6.1 for Ports prerequisites)**

3 Annexure

Annexure		Source	Destination	Port	Protocol	Description
1	Centralized Password Change	Schedule Password change Service	WinVaulting Service (Run As Domain Operator Privilidges)	45045	Custom	ARCOS Central Password Change Service
		WinVaulting Service (Run As Domain Operator Privilidges)	Windows Servers(added in Domain)	88	Kerberos	User and Computer Authentication, Forest Level Trusts
				135	RPC – Cert	RPC
				53	DNS	User and Computer Authentication, Name Resolution, Trusts
			LDAP	389	LDAP	LDAP Port
1.1	Centralized Password Change via. Secure Gateway	Schedule Password change Service	Secure Gateway	22	SSH	Secure Gateway
		Secure Gateway	WinVaulting Service (Run As Domain Operator Privilidges)	45045	Custom	ARCOS Central Password Change Service
		WinVaulting Service (Run As Domain Operator Privilidges)	Windows Servers(added in Domain)	88	Kerberos	User and Computer Authentication, Forest Level Trusts
				135	RPC – Cert	RPC
				53	DNS	User and Computer Authentication, Name Resolution, Trusts
			LDAP	389	LDAP	LDAP Port
2	Windows Domain Account	Schedule Password change Service	Windows Servers(added in Domain)	139, 445	NetBIOS Services	Name Resolution Service

				88	Kerberos	User and Computer Authentication, Forest Level Trusts
				53	DNS	User and Computer Authentication, Name Resolution, Trusts
2.1	Windows Domain Account	Schedule Password change Service	Secure Gateway	22	SSH	Secure Gateway
		Secure Gateway	Windows Servers(added in Domain)	139, 445	NetBIOS Services	Name Resolution Service
				88	Kerberos	User and Computer Authentication, Forest Level Trusts
				53	DNS	User and Computer Authentication, Name Resolution, Trusts
3	Windows Domain Account via LDAP (AD)	Schedule Password change Service	Windows Servers(added in Domain)	139, 445	NetBIOS Service	Datagram Services (Browsing)
				88	Kerberos	User and Computer Authentication, Forest Level Trusts
				53	DNS	User and Computer Authentication, Name Resolution, Trusts
			LDAP	389	LDAP	LDAP Port
3.1	Windows Domain Account via LDAP (AD)	Schedule Password change Service	Secure Gateway	22	SSH	Secure Gateway
		Secure Gateway	Windows Servers(added in Domain)	139, 445	NetBIOS Service	Datagram Services (Browsing)
				88	Kerberos	User and Computer Authentication, Forest Level Trusts
				53	DNS	User and Computer Authentication, Name Resolution, Trusts

			LDAP	389	LDAP	LDAP Port
4	Windows Local Acount	Schedule Password change Service	Windows Servers(added in Workgroup)	139, 445	NetBIOS Services	Session Service (net use)
4.1	Windows Local Acount	Schedule Password change Service	Secure Gateway	22	SSH	Secure Gateway
		Secure Gateway	Windows Servers(added in Workgroup)	139, 445	NetBIOS Services	Session Service (net use)
5	Linux/ Unix/ Network Devices	Schedule Password change Service	Target Devices	22, 23	SSH/ Telnet	SSH or Telnet Port
5.1	Linux/ Unix/ Network Devices	Schedule Password change Service	Secure Gateway	22	SSH	Secure Gateway
		Secure Gateway	Target Devices	22, 23	SSH/ Telnet	SSH or Telnet Port
6	Windows Services / COM Plus	Schedule Password change Service	Windows Servers	135, 445	NetBIOS Services	Session Service (net use)
	Windows Schedule Task, IIS APP Pools	Schedule Password change Service	Windows Servers	135, 445, 45045	NetBIOS Services, Custom	Session Service (net use)
6.1	Windows Services / COM Plus	Schedule Password change Service	Secure Gateway	22	SSH	Secure Gateway
		Secure Gateway	Windows Servers	135, 445	NetBIOS Services	Session Service (net use)
	Windows Schedule Task, IIS APP Pools	Schedule Password change Service	Secure Gateway	22	SSH	Secure Gateway

		Secure Gateway	Windows Servers	135, 445, 45045	NetBIOS Services, Custom	Session Service (net use)

Privileged Access Management Suite