Predict | Protect | Prevent

ARCON|PAM

ARCON|PAM Features

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 a 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.

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

Organizations implement various systems and applications to support its internal & customer client needs & leverage on technology to offer efficient and cost effective services to its clients. This has led to substantial investments in data Centre and technology to manage several databases, operating systems, web servers, routers etc. The flavors include but not limited to Unix, Linux. The complexity of managing such large number of systems, with 24*7 support and limited resources requires the administrators to multitask and have access to almost all systems under their work domain. Further, various application coordinators have access to the systems with varied access entitlements to enable them to troubleshoot. The access to back end is also granted to certain end-users for the purpose of analytics, reporting etc.

IT infrastructure being a critical function of the organization should be up & running 24*7. This raises the need to implement a solution for accessing servers in a secure manner & log the activities in the data center. ARCON PAM helps to meet information technology challenges and offers a technologically advanced and a comprehensive **P**rivilege **A**ccess **M**anagement **S**olution, which besides ensuring adequate control on all the administrative privileges provides features for centralized administrative log management and password management.

2 Features

Below are the features provided by ARCON PAM.

Feature	Description
Password Management	• ARCON offers automated password management for range of devices viz.: UNIX, Linux, AIX, Win2K, Win2k3, Oracle, MS SQL, Services, dcom etc. and is one of the strongest module in the industry. • The password connectors available are both agent based and agent less. The agent less 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. Also the passwords can be sequentially changed for dependent systems and services. • The password communication between the ARCOS client and ARCOS server is in AES-256 encrypted form. • There is a password request mechanism for electronically releasing the password in case hard console access is required. • Password change Logs are produced which automatically verifies whether the passwords are changed or not. If some passwords are not synced, password manager runs again & changes the password • Support for Password management for service accounts while allowing to configure service to restart /update etc. (inbuilt feature) • All ARCON Data is completely encrypted using AES 256 bit encryption. ARCON passwords can also be provided in secured enveloped or encrypted soft files as a break glass measure. • Historic password can be restored for any account. • Critical feature when restoring old Virtual machines copies. • Facility to reset passwords using Super Administrator account. Critical feature while managing Unix based devices. • Auto discovery of accounts across Windows, Unix, Database (other products are limited to windows domain only)

Feature	Description
Password Vault	• The ARCOS 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 how frequently the password must be changed and the rules for the password content, such as: length, combination of different types of characters, password history, etc. ▪ The password configuration is parameterized 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.
Session Recordings/ Text Logs	• ARCOS is built for enterprise class environment and offers unlimited concurrent session recording without any agent on the target devices. • ARCOS Logs also provide complete meta-data of the windows sessions and command fired on CLI interfaces.

Feature	Description
Audit Trail/ Session Monitoring and Log Management	• Audit logs for administrative access have been an important issue for all IT Security and Governance experts, as it has been found to be extremely difficult to set triggers and to enable audit trails on the native systems due to various performance issues. This has been so far largely ignored. ARCON meets this challenge by capturing the logs at a central location. • The logs captured include commands fired on the SSH/telnet clients as well as actions performed on the MS SQL Enterprise Manager and Windows. • Further all actions performed by any application support engineer on the databases including queries etc. is also logged by the Server Manager (SM). • The logs captured include both command & video based session recordings. All the critical data including logs, passwords, credential stored on secured vault are AES-256 bit encrypted & are indelible in nature & are tamper proof. • ARCON captures comprehensive audit trails of any PIM initiated session of the target devices. • Staging Log Server is used to store visual logs before they are transferred to Database Server. Logs are compressed and stored on this server.
Access Control	• User Access Control is a security feature, which helps to prevent unauthorized changes to your computer. These changes can be initiated by applications, viruses or other users. • User Access Control module makes sure that these changes are made only with approval from the Administrator. • Administrators can enable the user logon period, disable the user logon, session lockout, endpoint based access, and to enable or disable the dual authorization factor for user(s).

Feature	Description
Onboarding	• Supports Windows, Azure, AWS Onboarding. • Auto provision and de-provision Users and Services. • Supports Privileged User Onboarding, Desktop User Onboarding and Device Onboarding. • Rule Based Automation • Windows: Auto provision and de-provision Users and Services i.e, Devices, and Users within the devices. • Azure: Auto provision and de-provision Users and Services. • Amazon Web Service (AWS): Auto provision and de-provision Users and Services, supports EC2 instance, linux machine, RDS, S3, and other native services. It supports auto scaling, user management, and Password Vaulting. • Offers Network Discovery through IP and Port Scanner, Active Directory Scan and SSH Key Scan.
SSO (Single Sign-On)	• ARCON offers most advanced single sign for almost all conventional IT Devices with more than 200+ plug-n-play connectors. • This covers a range of range of devices including Windows, Unix, Databases (Toad, SQL+, SQL Developer etc.), Network Devices, VMWare, HyperV, Peripheral devices consoles and Web Applications. • Strong feature on managing Network Devices (SSH/Telnet and GUI based). • Seamless support for Oracle Database over SSH. • Dedicated support for developing additional connectors. • ARCOS SSO is integrated with build in plugins for Multi Domain Authentication, RSA / Safenet / Vasco Tokens / Duo. • Inbuilt Mobile App Based Authentication, SMS Token based. (Part of single ARCON license)

Feature	Description
EPM (Endpoint Privilege Management) - Separate license required.	• Introduced to elevate or restrict an application or process for an User based on his role or preference. • The Users or Groups assigned to the Elevated or Restricted Profile, are those Users who have been onboarded in ARCON PAM. • Supported in both Ubuntu and Windows platform. • EPM is designed to detect and prevent known cyber threats using fixed techniques, protection methodologies. • Specific Processes are either elevated or restricted for users based on their job role or their requirements. EPM will allow certain processes to be executed under elevated privileges and restrict certain process that should be restricted for the particular end user. Administrators can define policies to limit the access levels according to their requirements thus limiting the scope of any unsafe activities that could become a potential threat.
AD Bridging - Separate license required.	• Active Directory Bridging is an application that configures bridging between various operating machines (Unix, Linux) and Windows Active Directory server. • Leverage existing Active Directory deployments to centrally manage disparate workstations and users. • Achieves SSO for any Enterprise application which supports Kerberos or LDAP, including SSH, Apache, Oracle, and MySql.
Multi-tab	• Enable users to access multiple PAM services in a single window. • Supported for SSH and RDP service types. • Makes it easier for the user to toggle between services and control all user sessions centrally from a single window.

Feature	Description
Desk Insight - Separate license required.	• ARCON PAM Desk Insight is a specialized plugin based module available with ARCON PAM Privileged Identity Management Suite for remote desktop management. • Administrators can establish a remote connection within an enterprise network to any client machine. • Client users can allow administrators to trouble shoot the machine in a controlled environment. • ARCON PAM Desk Insigh toffers features like Desktop Account Password Change, Remote Elevation and Dekstop Discovery.
SSH Key Management	• SSH Key Management feature enables SSH Linux services to be managed by SSH Key. The single sign on and key rotation for SSH Linux services will be managed by SSH Key. • SSH keys shall be vaulted in ARCON PAM as of password. Key rotation is similar concept to password change process in ARCON PAM. • SSH Key rotation logs can be generated and users can also request for SSH keys of services.

Feature	Description
Multi-factor Authentication	• A dual authentication process is used in ARCON PAM wherein the user is authorized twice in ARCON PAM, after which the user can get access to the application, making it more secure. • Static passwords for authentication has quite a few security drawbacks such as passwords can be guessed, forgotten, written down and stolen, eavesdropped or deliberately being told to other people. A better, more secure way of authentication is called "dual-factor" based on one time passwords. • Listed below are the types of OTPs used in ARCON PAM ▪ **Mobile OTP:** Mobile one time password (OTP) configuration is one of the dual factor authentication. It is used by mobile users by implementing the application on mobile, inorder to securely login into ARCON PAM. The users will have to download and install **ARCON Authenticator** App from **Google Play Store** to the mobile device to configure mobile OTP dual factor authentication. ▪ **SMS OTP:** SMS OTP as dual factor authentication means that during login the user has to provide two secure information such as his password and one time password he receives as SMS on his mobile phone. SMS OTP is one of the methods, wherein ARCON PAM user's receives OTP on registered mobile number. ▪ **Biometric Device**: Biometric Device Configuration is a dual factor authentication supported by ARCON PAM. It is performed by using biometric data (fingerprint) of the user. ARCON PAM acts as a strategic entry and identity management system for managing several system based user. It supports leading biometric devices such as 3M Cogent, Morpho, and Precission.

Feature	Description
	▪ **Hardware Token:** A Hardware token is a security token which may be a physical device that an authorized User of computer services is given, to ease authentication. It may be a small hardware device that the owner carries to authorize access to a network service. In ARCON PAM, RADIUS servers are used for authentication of a RSA portal. RADIUS is a protocol similar to LDAP, DCPIP, and RDP protocol. Similarly, RADIUS is a kind of protocol that helps to communicate with another server. ▪ **Email OTP:** A dual factor authentication means that during login the user has to provide two secure information such as his password and one time password he receives on the registered email address. Email OTP is one of the methods, wherein ARCON PAM users receive OTP on registered email address. ▪ **Voice Biometric:** Voice Bio-metric Authentication is a type of Dual Factor Authentication which uses Web Service for authenticating user before logging into Client Manager. The predefined web service authentication is configured, which will authenticate the user through their voice and decide whether to allow the user to login or not. ▪ **TOTP:** Time-based One-time Passwords Authentication is a robust multi-factor authentication where the login tokens are formed by mixing a secret key with the current time interval to generate the OTP. There are various applications on which TOTP can be received. Users can choose the **authentications** from Google Authenticator, Microsoft Authenticator, Symantec VIP Authenticator, etc.
Passwordless Authentication	• **Passwordless authentication** frees the users from remembering long passwords while logging into their systems. • Users are validated against the domain. • It also supports all the Multifactor Authentications mentioned aboved.

Feature	Description
Smart Session Monitoring	• Monitor User activities on Server. • Monitors Servers for Windows RDP and Connectors service type. • Monitor activities such as creation, modification and deletion of files. • Capture function keys and mouse clicks on Server. • For Connectors service type, only mouse click User activity is monitored.
Real Time Session Monitoring	• Used to monitor live feed of a session. • The session can be quickly freezed, unfreezed or logout the session to minimize any potential damage. • It increases the control over user's activity.
Workflow Management	• Workflow Management makes an administrators life easy by streamlining the internal processeses by establishing a predefined hierarchy of Admins. ARCON PAM Workflows can be set for both users and admins activities. • Users can raise a service, passwords, and ticket requests with a description of their task and the approvers can approve/reject requests. Admins activities such as creation/deletion/modification on users/services/user groups/service groups automatically go into the workflow(if configured) when that action is performed. • All the transactions performed by users and admins are captured in the workflow tracker thereby which making individuals accountable for their actions.
Password Reconciliation	• Password Reconciliation is a process used to analyze failed scheduled passwords and auto heal them on both ARCON PAM and target server. • The reconciliation process compares the entries in ARCON PAM repository and the target system repository, determining the difference between the two repositories. • It determines the difference between the two repositories, and applies the latest changes on the servers. • All the status of success and failure are updated in Service Reconcile Status Report. This automated process helps enhancing the best privileged accounts practices offered by ARCON PAM.

Feature	Description
My Vault	• My Vault is a steadfast vaulting mechanism where users can upload/download/share their files/ secrets(PINs, Application Password, Service Password, and SSH Keys) in a secured and encrypted manner. • Users can share (documents, spreadsheets, images, certificates, SSH Keys, video, and/or audio files) with other ARCON PAM users without sending them through email or printing it out. • Admins can also set Password Policy for all the secrets. For enhanced protection we can secure secrets through ARCON Password Envelope Management (APEM) utility.
Staging Server Video Archival	• Used to store visual logs • Visual logs are compressed and stored on Staging server. This will help to reduce the bandwidth consumption and processing power at application and database server.
Realtime Data Synchronization and Near Zero Downtime - Separate license required.	• Supports continuous harmonization of the data when the Primary Node is down. • ARCOSDataSync service will synchronize the data from Secondary Node to Primary Node and Users will be able to see their activities log from Primary Node.
Knight Analytics	• ARCON PAM introduces Knight Analytics tool that continuously checks different user behaviors, learns from them, and predicts threats in advance. • It uses data mining, statistics, modeling, machine learning, predictive analytics, and AI for training the dataset, anomaly detection, and to make predictions about the existing and future threats. • The graphical user interface/intuitive dashboard displays critical issues from a list of riskiest users down to the raw events. It displays the most important security issues with respect to users, sessions, commands, processes that one should be aware of so that one can make better-informed business decisions. • Alerts are received based on the risky enetities, the one with the greatest potential risk level /risk score.

Feature	Description
Spection	• ARCON PAM Spection is used for reporting and data analysis, and is considered a core component of business intelligence. ARCON PAM Spection is a dynamic report builder that allows searching as well as filtering capabilities to derive a detailed compilation of all activities. It also provides entity wise views, so you can see the activities performed from a command level, session level, process level, user level, service level or even a group level view. It allows the user to select exactly what details (column) to add in your report. • Dynamic graphs help in visualizing large volumes of data in a coherent way for all the reports in Spection. • Video logs are captured for session, processes, and command fired by the Users. • Supports smart session monitoring which monitors and highlights all the users activities. • All the reports present in the Spection can be scheduled.
Two Level Data Encryption - HSM Integration	• Encrypt passwords of users and services. • The password is encrypted once with an ARCON PAM Key and then again encrypted with User defined key and store the passwords for enhanced security. • User Defined Key can be stored on the HSM device.
Integration with OKTA via SAML	• Okta is a cloud-based identity management provider that can be integrated with ARCON PAM SAML 2.0 API to allow users to log into ARCON PAM using their Single Sign-On (SSO) credentials. • Security Assertion Markup Language 2.0 (SAML) is an open standard for exchanging identity and security information with applications and service providers. • ARCON PAM's support for SAML enables you to sign in using your corporate directory credentials, such as your user name and password from Azure Active Directory. With SAML, you can use single sign-on (SSO) to sign in to all of your ARCON PAM applications by using a single set of credentials. • ARCON PAM will enable SAML for a domain. Any user who uses that domain will be forced to login via their enterprise identity provider. For existing ARCON PAM users, their ARCON PAM password will be no longer used.

Feature	Description
Auto Healing	• Auto healing is the process of automatically changing password of services using privilege accounts in case of password failure. • All the privilege accounts need to be on-boarded in ARCON for Auto-healing, On-boarding is the process of creating a service of the privileged user in ARCON. • During SPC password change process and manually Password change process, if the password fails for services, ▪ ARCON will automatically log in to server for which the password has failed through privilege account which is configured and change the password of the actual Service • Password failure and auto-heal process log can be viewed in password change history logs.
Integration with Bots	• Robotic Process Automation (RPA) is the process of automating mundane tasks with ease, efficiency and accuracy. ARCON PAM users can integrate with various automation solution.

Feature	Description
Remote Assist - Separate license required.	• ARCON PAM Remote Assist is a new remote desktop management tool available with ARCON PAM Privileged Identity Management Suite. • With Remote Assist IT process management is simplified and allows administrator to remotely stream the content of an end-user. • ARCON PAM Remote Assist manages all remote assistance provided between the PAM team (host) and the Service requestor even over the internet. • ARCON PAM Web Portal acts as a point of contact for identifying users with specific requirement for remote assistance. Remote assist includes a report that displays the record of each and every remote assistance provided. • Remote Assist login access is provided only to authorized ARCON PAM users. The target users will have to install Remote Assist application on to their respective systems. • Once installed, the target users can request for remote assistance from an authorized ARCON PAM user. • Client users can allow administrators to trouble shoot the machine in a controlled environment. • ARCON's File transfer provides a secure communication channel from one computer system to another, integrated inside the Remote Assist application. • Desk Insight functionality is enhanced to Arcon Remote Assist, where the connections can be established both over the intranet and the internet. • Process Elevation enables end-users to elevate admins' rights, privileges, change passwords, and access related tasks for any process, in a controlled environment. • The Activities can be overviewed through the Reporting feature.

Feature	Description
Automatic Failover Manager - Separate license required.	• Automatic Fail over Manager describes the automatic vault fail over Manager, It is programmed to automatically operate in case of failure of ARCON PAM Database Server. • ARCON PAM uses the MS SQL log shipping technology to automate the backup and restore process in case of ARCON PAM Database failures.All the transactions in the primary Database server in DC is copied and stored in the DR environment. • ARCON PAM automatic fail over manager will connect to the SQL cluster IP of the DC and will perform a DB check, if unsuccessful it will continue to check for the predefined interval. • After the per-defined unsuccessful attempts, ARCON PAM Automatic Vault Fail over manager will connect to DR database server and bring the ARCON PAM DR Database in Read/Write mode and bring the ARCON PAM Database Server up and running.
Auto-discovery	• Discovery processes are designed to be used when a resource is being deployed for the first time. It provides a means to load account information into ARCON PAM quickly • or example, the discovery process does not add entries to ARCON PAM nor can you run workflows before or after discovery. However, the discovery processes allows you to determine more quickly whether the users are present or are to be added in ARCON PAM. • ARCON PAM determines whether an input account matches (or correlates with) an existing user. If it does, the discovery process uses the account to discover other users on the same server. • Users Auto – Discovery is used to automatically discover all the users on all the target servers (server level users only) such as Linux, Windows, and Database.

Feature	Description
Application Gateway Server - Separate license required.	• ARCON PAM introduces AGW an intermediary gateway to a remote network through which connection can be made to another host. It would ensure a more security as the local infrastructure won't be exposed to the internet. • Application Gateway server is a fortified sever that is placed in a very secure zone which can be accessed by users in a less secured zone. AGW ensures to have a very comprehensive and secured work zone and shall be used only for administrative tasks. • It applies a control on the remote access as it ensures a connection in to the AGW and then into other network connections. AGW can slow down the progress of an attack as it protects confidentiality, integrity and availability of a network.
Command Profiler	• Command Profiler is used to restrict or elevate processes or commands. You can assign commands with **Critical With Approval** property, wherein an email notification will be sent to the Approver for approval. • Once approved, the command will be allowed for execution. This feature is used by Administrator who is responsible for keeping a track of unwanted or critical commands or processes that should/should not be executed by the user on the server. Multiple profiles can be created for each service type. • Also new processes or commands can be added to the existing set of processes and commands. In addition, you can modify and delete a command profiler.

Privileged Access Management Suite