

PRIVILEGED ACCESS MANAGER (PAM)

Fálaina's Privilege Access Manager (PAM) is designed to secure the privileged users (identity) and accounts, while enabling practical session management from single, integrated portal. This portal enables single sign-on for all privileged account via centralised authentication typically Microsoft Active Directory Server or any LDAP server. The objective is to secure, control, manage and monitor privileged session to enterprise critical asset. PAM also keep your organization safe from accidental or deliberate misuse of privileged access.

Fálaina's PAM using the same universal connectors, access request and approval workflow and Fálaina Universal SSO Workspace² technology from Web Access Manager/SSO product.

Fálaina's PAM provides out of the box multi-factor authentication (MFA) and step-up authentication for privileged access to critical asset. One-time Password (OTP) and Captcha authentication can be configured as part of the access policies. Rest API provided for integration with third party MFA or Hardware Security Module (HSM) for FIPS requirement.

Fálaina's PAM support dual authentication which allows two person to login using their own credentials to centralised authentication server before any session to be initiated. Each of these login can be done remotely across different geographic locations.

Fálaina's PAM key capabilities includes:

- Privileged access request management and approval workflow
- Privileged session - RDP, SSH and application access
- Session recording and keystrokes logging
- Fálaina Universal SSO Workspace
- Real-time session monitoring and access termination

Fálaina's PAM simplifies privilege access management process to enhance organisations IT security and enables organisations to meet regulatory requirements, while practically enables users to perform their day to day privileged activities.



Privileged access request management and approval workflow

Fálaina's PAM leverage access request management integrated with workflow technology from ILM. Privileged users can request for access to any privileged account on any critical asset based on the policy and rules created. These rules could be limiting the requestor to request only accounts within the group or set of servers the requestor is allowed to see and request. Other rules include day and time of access, especially after office hours access or location of access.

Other critical policies include if concurrent session is allowed, if users requires 2FA or second authentications, configurable password options. The access to each of these privilege or shared accounts are based on the policies and integrated as part of the on-line access request form and approvals via workflow.

The approver allowed to approve, reject or override the request items such as limiting time or locations or even a set of accounts requested. Other features include pre-approved access by systems owner themselves without approval process, but the session will be monitored and recorded.

Privileged session - RDP, SSH and application access

Fálaina's PAM enables any session to be initiated with privileged access including Microsoft Remote Desktop (RDP), Unix Secure Shell (SSH), typical client/server and HTTP(S) based applications management tools. Client/server applications for privileged access includes Oracle PL/SQL Developer and Oracle Enterprise Manager for Oracle Database, Management Studio for Microsoft SQL Server and so on.

These session is initiated from Universal SSO Workspace² from any device or computers. Privileged session login doesn't require password to be shared with the requestor and this eliminates the need for password management. If organization requires password to be reset, then policies can be applied on how frequent these password reset should happen.

Session recording and keystrokes logging

Fálaina's PAM log user session with both video recording and keystroke logging for all privileged session. These videos and keystrokes are encrypted and securely stored in the PAM server. The video and keystroke can be viewed only by authorised personnel based on RBAC security policies, via the administration web interface.

Fálaina's PAM also provides flexibility to record or log only selected user sessions based on the policies. Policies include user account, time, grouping of servers and so on. For instance, a user session into Office 365 portal for email access not record but same user session for Office 365 administration will be video recorded and keystroke logged.

Integration with SIEM solution allows correlation of security events and further actions can be taken for auditing and investigation purpose.

Fálaina's PAM provides threat intelligence and if enterprises adopt this threat-aware privileged access model, integrated processes can be implemented to quickly remove privileged credentials associated with a particular attack or device.

Fálaina Universal SSO Workspace²

Fálaina's PAM Universal SSO Workspace² provides portal for users to access their privileged session securely from any web browsers from any device.

Users need to login to centralised authentication server typically Microsoft Active Directory Server or any LDAP server. Upon login, users can select the session and accounts available in their Universal SSO Workspace² by clicking the icons - eventually proving better user experience and improves productivity.

Real-time session monitoring and access termination

Fálaina's PAM provides real-time session monitoring and access termination. The session is made available for remote monitoring via video streaming and only viewing is allowed. The view, based on the authorisation able to terminate the session remotely.

This feature enables systems owner or security personnel to monitor vendor (for system administration/maintenance work) session remotely instead of physically present.

About Fálaina

Fálaina is a technology provider of Identity and Access Management solutions. Fálaina enables enterprises to have visibility and secure their infrastructures, applications and data for private and public cloud. Fálaina comprehensive solution addresses today's requirements of an enterprise for:

- Identity Governance and Administration (IGA)
- Data Access Governance (DAG)
- Access Management (AM)

It provides businesses with the relevant reporting and analytics to improve IT security, maintain compliance and eventually minimise business risk.

To learn how Fálaina can help your business, visit www.falainacloud.com, or email us at sales@falainacloud.com.

