fálaina

THE NEXT GENERATION IDENTITY AND ACCESS GOVERNANCE PLATFORM

PRODUCT BRIEF

MULTI-FACTOR AUTHENTICATION (MFA)

Fálaina's Multi-factor Authentication (MFA) is an integrated MFA solution that helps to secure workforce and customer access to corporate network and applications. This includes ability to manage and provide secure access to non-employee, which includes contractor, supplier and vendor.

Fálaina's MFA is designed to secure the users (identity), their accounts and resources, while login or during other transactions. Fálaina MFA provides various authentication method that requires the user to provide two or more verification to gain access to a resource such as an application, online account, or a VPN, which decreases the likelihood of account takeover (ATO), phishing, key logger, credential stuffing, brute force attack and man-in-the-middle (MITM) attack. The objective is to secure, control, manage and monitor users access journey throughout.

Fálaina MFA support password-less authentication via out of band OTP, TOTP and Mobile Push. These MFA authentication is further strengthen using mobile phone PIN, biometric and face id authentication before MFA is approved.

Fálaina MFA implemented as native mobile applications and supports iOS and Android. Fálaina MFA support corporate branding activity like changing Fálaina Mobile Application's logo, name and background images to customer's branding guidelines to ensure seamless user experience.

Fálaina's MFA key capabilities includes:

- Multi-factor Authentication in Zero Trust Approach or Zero Trust Network Access (ZTNA) with Falaina Radius Server
- Integrated Multi-factor Authentication with Account Unlock and Password Reset
- Comprehensive Metric and Adaptive Multi-factor Authentication Policies
- Step-up Authentication with MFA for Privileged Access Management (PAM) and Web Single Sign-On (SSO)

Fálaina's MFA support cloud and on-premise deployment to meet customer preference and demand.

Multi-factor Authentication in Zero Trust Approach or Zero Trust Network Access (ZTNA) with Fálaina Radius Server

Fálaina's MFA or strong authentication, is a key component to achieving Zero Trust. It adds a layer of security to access a network or web application by requiring additional factors to prove the identity of users.

Fálaina's MFA takes a user-to-application approach rather than a network-centric approach to security. User, including non-employee access to corporate network. Fálaina Radius Server helps to secure employee and non-employee access with MFA authentication from VPN/NAC from self-service registration, workflow approval, authentication against Ms. Active Directory or Falaina IDP, then accessing the corporate network or applications. Conditional and Adaptive policies can be applied to different users group to provide flexible and secure access.

Integrated Multi-factor Authentication with Account Unlock and Password Reset

Fálaina's MFA differentiate itself from all other MFA technology by providing integrated account unlock and password reset. These integrated solution eliminates the need for enterprises to have multiple mobile applications, for MFA functionalities as well as for account unlock and password reset - this in turn provide better user experience and overall improve productivity.

Account unlock and password reset, integrated with MFA work seamlessly with Ms. Active Directory Server, LDAP Server, Azure, AWS and Google platform.

Comprehensive Metric and Adaptive Multi-factor Authentication Policies

Fálaina's support both metric and adaptive MFA policies to strengthen the authentication. Adaptive MFA policies applies knowledge, business rules or policies to user-based factors, such as device or location. For example, enterprise application knows that it is okay for a user to sign on from corporate network because it sees the user's location and can determine the risk of misuse or compromise. But an employee who accesses the same application from public network will trigger the system and be required to enter MFA credentials.

Metric based MFA policies are defined based on attribute value from information store including user store such as Ms. Active Directory or other information from Fálaina database.

In both scenario, risk-based authentication can be implemented based on what's being accessed and who's requesting access. In both cases, a username and password may suffice for the latter, but multi-factor authentication makes sense when there's a high-value asset or sensitive/privileged account at risk.

Fálaina provide configuration based wizard driven user interface to define rules and policies for both metric and adaptive policies. This make the implementation and deployment much more simpler and quicker.

Step-up Authentication with MFA for Privileged Access Management (PAM) and Web Single Sign-On (SSO)

Fálaina's MFA is fully integrated with other Fálaina products such as IGA, DAG and Web SSO. This allows stronger authentication to be implemented as password-less authentication or step-up authentication for the functionalities within the products. For example, using step-up authentication with MFA for privileged access to target systems based on specific asset or accounts; for approval or sign-off of access rights review or for web application single sign-on.

Fálaina MFA also support step-up authentication for third party PAM or SSO products.

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.

fálaina