DATA SHEET

V-FRONT v8 ™

Comprehensive IAM & SSO Platform
On Premise Version Data-Sheet

The V-FRONT v8 solution is a robust IAM (Identity and Access Management) platform enhancing user authentication and access control across applications. It offers role-based access control (RBAC), single sign-on (SSO), and multi-factor authentication (MFA) with built-in two-factor authentication for accessing the MFA admin console. The platform integrates with LDAP, Active Directory, DBMS, and supports protocols like RADIUS, OpenID 2.0, and SAML 2.0. It supports cloud services (e.g., AWS, Azure, Google Cloud), virtualized environments, Office 365, and custom application systems both on-premises and in the cloud.

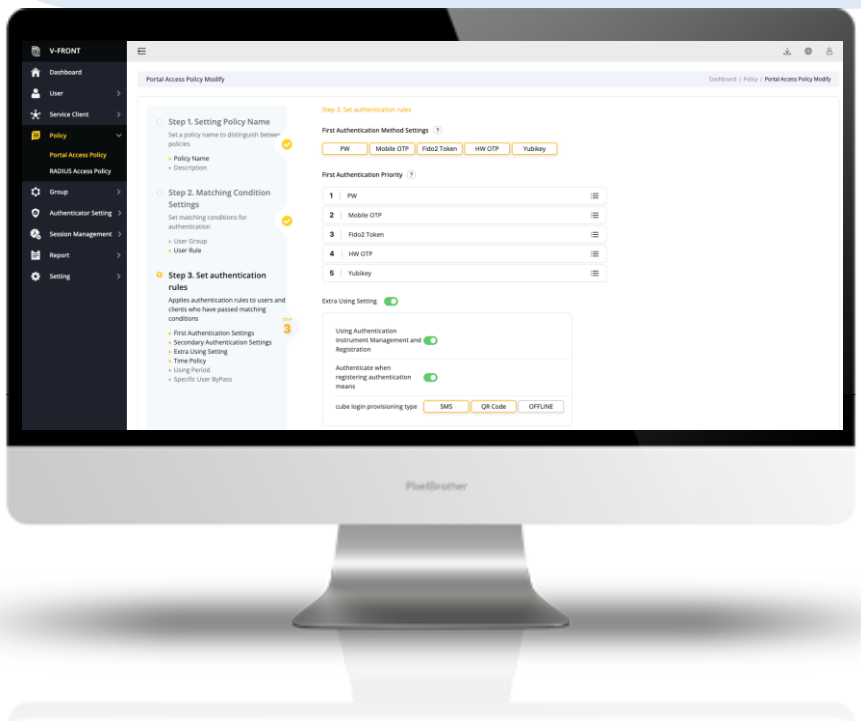
Additional features include:

•Automated auditing, access logs, and reports for security monitoring
•Remote disabling or wiping of soft tokens during incidents
•No credential retention in its database
•API support for customization and integration with third-party applications, such as reverse proxies and Privileged Identity Management (PIM) solutions
•Remote agent deployment capability for seamless management.

This integrated platform enhances security, user experience, and operational efficiency across diverse environments.

KEY FEATURES

- AAA Standard (RFC2865, 2866, 2868, 2869) RBAC support.
- Provide various protocols (RADIUS, FIDO2, OpenID 2.0, SAML)
- Mobile Application Support (iOS, Android, Multiple Organization on a Single Device)
- Supports for a Self-Service Portal for managing user accounts, access to applications, IDP-Initiated login, designation and management of second-factor authentication methods such as : Registering & De-Registering Mobile OTP, registering/deleting authentication tokens, changing/resetting passwords
- Configuration of login pages for application and security solutions according to security requirements with the ability to set authentication methods such as: Password, OTP, FIDO2 Token, Facial Recognition, YubiKey, QR, Push, etc.. For both primary and secondary authentication.
- Authorization upon authentication for OpenID and SAML clients
- Session Management Feature
- Support access control policies such as ACLs, policy-based ACLs and individual VLAN assignment for network access devices on user permission.
- Authentication Restriction/Block feature based on accumulated authentication fails.
- User authentication usage / re-authentication restriction depending on set usage period/time.
- Automatic account management based on long-term non-authentication user policies.
- Authentication logging functionality (ID, access time, auth request system IP, reason for authentication failure)
- Admin access to management pages and user group management based on administrator permissions.
- Self Service Portal activities and admin tasks & changes.
- Configuration functionality for external account management systems such as: DBMS, LDAP (AD), etc..
- Dashboard: User, System, Devices, etc.. Statistics. (Able to download authentication log Excel format)



Product Characteristics

1. Role-Based Access Control (RBAC)

RBAC grants permission/authentication to users based on assigned roles.

- **Policy Based Authentication:** Policy based authentication control is enable through policies that include various conditions and rules.
- **Authentication Allocation Using Group Management:** Manage large-scale user permissions through policies associated with group the users belong to.

2. Access Management

Provides robust access management features.

- **Single-Sign On (SSO):** Improves user experience and strengthens security by allowing access to multiple applications and services with a single authentication.
- **Multi-Factor Authentication (MFA):** SW/HW OTP, SMS, Email, Mobile App (IOS & Android), Hard Token, etc.. Strengthens security measure through variety of authentication tokens.
- **Access Policy:** Access setting access policies to permit access only under specific conditions. Various conditions such as time, location and device can be configured. Can enable "block account access that exceed certain number of failed auth".
- **Session Management:** Manage user sessions and supports automatic logout for inactive sessions / session re-authentication by setting session expiration and maintenance times..

3. Identity Federation

Support integration with various external directory services.

- **LDAP:** Allow leveraging existing user database within the organization by integration with external directory services via LDAP.
- **Active Directory (AD):** Supports integration with Microsoft Active Directory, enabling management of permission based on AD user and group information.
- **DBMS:** Can handle user authentication by integrating with various DBMS platforms.

4. Authenticator (Password-less)

Supports password-less authentication to enhance user experience and strengthen security

- **Mobile Push, QR, OTP:** Mobile Push notification, QR, one-time password(OTP).
- **YubiKey (FIDO2, OTP), YubiKey Bio:** Supports FIDO2 and OTP using YubiKey as as biometric authentication.
- **Face-Key (FIDO2 with Face):** Supports FIDO2 facial recognition authentication.
- **Facial Authentication:** User authentication via Facial Recognition.
- **H/W OTP Token:** Supports Hardware-Based OTP tokens for one-time password.
- **Finger-OTP:** Supports authentication combining fingerprint recognition and OTP.

5. Protocol Support

Supports Various Authentication Protocols to Facilitate Integration With Application and Security Solutions.

- **RADIUS:** Support network access control via the RADUYS protocol, enabling integration with various network devices.
- **OpenID 2.0:** Supports the OpenID 2.0 protocol, allowing integration with external authentication services.
- **SAML 2.0:** Supports SAML 2.0 protocol, providing SSO and federation capabilities.

6. Self-Service Portal:

Provides self service portal where users can manage authentication methods and application access permission.

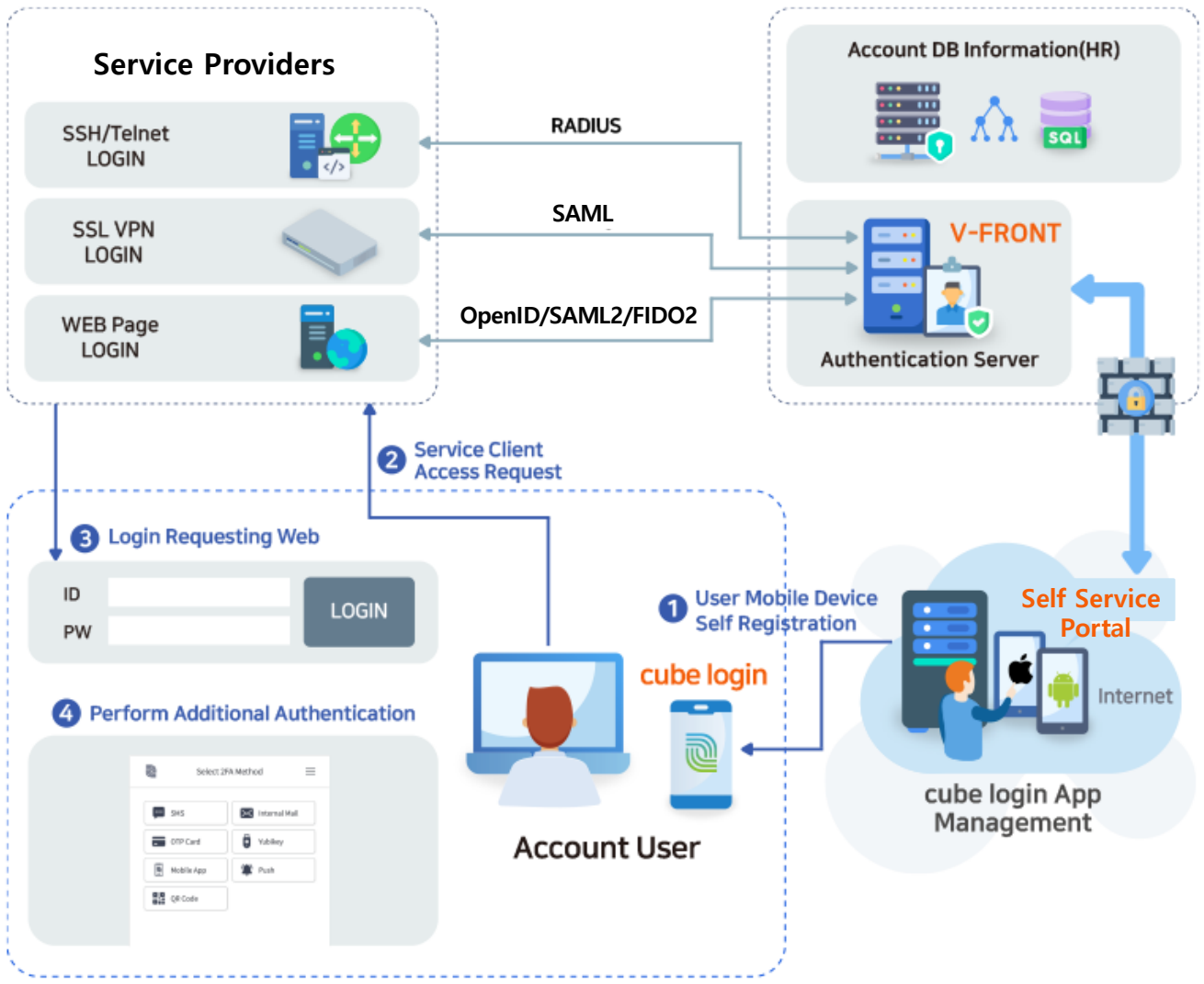
- **Authenticator Management:** Users can register new authentication methods or modify and delete existing ones, through the self-service portal.
- **Application Access:** User can manage access permission to application and services assigned to them.

DATA SHEET

V-FRONT v8 ™

Comprehensive IAM Platform
On Promise Version Data-Sheet

Product Compenets



V-FRONT v8 (AuthServer)

- Policy Based Integrated Auth Module(OpenID, SAML2, FIDO2, RADIUS protocol-based SMS, Email, HW OTP, Yubikey, Finger OTP, Mobile OTP, PUSH, QR Code, FIDO2 Token, etc.. Authentication token support)
- Management console module, API module, Notification module, Logging module

Self Service Portal(User management environment)

- User account password management
- Device registration and management of OTP card, Yubikey, Finger OTP, FIDO2 Token registration.
- Access application management and IDP-Initiated login.

cube login (Smart phone personal OTP App)

- Time-based OTP generation
- Push authentication feature support
- QR Code authentication feature support
- Android / IOS Application Support

Product Spec

Spec	OS	Dependency Package	Dependency H/W Spec	Recommended Browser
• V-FRONT Server • Self Service Portal Server	Linux Rocky 8 and above	OpenJDK 17.0.1 and above Openssl 1.1.1u Spring Boot 3.2.5 PostgreSQL	CPU : Quad Core 3.1Ghz (4 Core x 1 CPU) Memory : 16GB and above HDD : 500GB	• Chrome(V-FRONT Server) • Safari, Chrome, Edge
Mobile Application (Android)	Android 5.0 and above	-	-	-
Mobile Application (iOS)	iOS 13.0 and above	-	-	-

AirCUVE Inc.

http://www.aircuve.com

AirCUVE Inc.
Suite 606, GangseohankangXI Tower B, Yangchean-ro 401, Ganseo-gu, Seoul, Korea 07528

Inquiry: +82 10-5061-3227 | HQ: 02-3663-3181 FAX: 02-6968-5622 | e-mail: davlet@aircuve.com