# Authentication

## MANAGEMENT

VU

## Datasheet

Version 6.19

**July 2025**
Link to the latest available version

# What Is?

**Authentication Management**® is a solution to protect organizations from theft or misuse of corporate credentials through Zero-Trust mechanisms based on multiple adaptive authentication factors and facial and voice recognition biometric systems.

It offers an extra layer of security in the authentication processes, while simplifying them through its single sign-on capabilities. In addition, it has the ability to integrate Active Directory both for user management and for access control to the solution's administration backoffice.

Authentication Management allows incorporating VU technology to any corporate resource, including VPNs, Intranets, applications and Office 365, using the most recognized protocols in the market, such as SAML2, OIDC, Radius, API and App.

# Benefits

• **Zero-Trust security** for cloud, hybrid or on-premises environments. Through multi-factor authentication, it is guaranteed that the legitimate owner of the credentials is the entity that is accessing the system.

• **It improves the experience in the authentication processes** thanks to the Single sign-on functionality. In a single step, it is possible to authenticate users in multiple applications and corporate systems.

• **Offered in SaaS mode**, it allows an easy and simple deployment and integration with a minimum impact on the daily operation of the organization.

• **Offered in on-premises mode**, it allows deploying the components in the client's infrastructure.

• **Scalability**. Authentication Management is conceived to be the key piece to build the identity and access management strategy.

# Modular Solution

VU offers modular solutions to give customers easy integration, speed and flexibility.
Authentication Management has three main modules: Server, SDK and App.

- **Server** is the user authentication module. It is multifactor and cross-platform, and has flexible and personalized integration in the cloud.
- **SDK** is the module that integrates Authentication Management functionalities into Android and iOS mobile applications.
- **App** is a standalone mobile application, "ready to use", for the enrollment and obtaining of the second factor of authentication by end users.

# Functional scope

## Identity Authentication

**Authentication Management** allows you to authenticate users to applications using the following interfaces:

- SAML2
- OIDC – OpenID Connect
- Radius (through agent)
- WebServices REST

• It integrates with multiple Active Directory (through agent) allowing:

- verify that the user is enabled in Active Directory in order to validate its use,
- validate user passwords in Active Directory,
- take the users from the Active Directory to obtain access to the administration portal (backoffice).

• It allows to provide identities and second authentication factor to any application compatible with the mentioned interfaces.

• The solution provides identities that can be stored in an Active Directory or directly in the solution, which means it can operate with or without an Active Directory. It also supports having some identities from AD and others as native identities.

## Single Sign-On

• **Authentication Management** simplifies authentication processes by recognizing active sessions so users don't have to authenticate to each application they want to log in to.

• The solution provides multiple user authentication flows, with one or two factors, configurable for each application.

# Two Factor Authentication (2FA)

One-time authentication factors (OTP) make it possible to strengthen authentication processes. For example, in the case of Secure VPN, **Authentication Management** provides the second factor through integration with an agent/FreeRadius.

**Authentication Management** enables the enrollment of the second factor of authentication in the client's application (SDK) by sending a coupon or QR code by email, SMS or some other channel that the client has. In turn, it allows the enrollment in the mobile application of TOTP, push and sync type authentications.

## Types of Authentication Factors

**Authentication Management** allows the configuration of the following authentication factors:

• **TOTP**: time-based one-time password.

• **HOTP**: event-based one-time password (HMAC counter).

• **SYNC**: in-app notifications in the standalone application or through the SDK. It has no cost for the client and allows the association of more than one device per user.

• **PUSH**: notifications integrated into the mobile operating system (enabled through the use of the SDK or standalone application). It is implemented through Firebase (a client API key is required for its configuration).

• **Magic Link**: enables authentication through a link sent to the user's email, avoiding the need for the user to manage additional passwords.

• **QR Code**: QR code-based authentication method. It is integrated with the generic VU App, allowing users to use mobile devices to verify their identity and authenticate transactions, among other actions.

Authentication factors can be sent to the end user through the following channels:

| | SMS | E-mail | Mobile OS | In-app (SDK) | App Authentication Management | 2FA Wallets* |
|---|---|---|---|---|---|---|
| TOTP | - | - | - | ✓ | ✓ | ✓ |
| HOTP | ✓ | ✓ | - | ✓ | ✓ | ✓ |
| PUSH | - | - | ✓ | - | ✓ | - |
| SYNC | - | - | - | ✓ | ✓ | - |
| Magic Link | - | ✓ | - | - | - | - |

* Google Authenticator, Microsoft Authenticator, among others.

**Authentication Management** supports the following interface channels:

| | WebServices REST | SAML2 | OIDC | RADIUS |
|---|---|---|---|---|
| E-mail | ✓ | ✓ | ✓ | ✓ |
| SMS | ✓ | ✓ | ✓ | ✓ |
| In-app (SDK) | ✓ | ✓ | ✓ | ✓ |
| App Authentication Management | ✓ | ✓ | ✓ | ✓ |
| 2FA wallets* | ✓ | ✓ | ✓ | ✓ |

* Google Authenticator, Microsoft Authenticator, among others.

## Mobile Apps

**Authentication Management** allows users to receive the second factor of authentication in their own mobile application through the native SDK on iOS and Android, as well as hybrid (Javascript), which can be integrated both for enrollment and for obtaining the second factor of authentication. Mobile apps make it possible to create multiple accounts with the seeds, as well as synchronize clocks.

The standalone mobile application is available on the Android and Apple stores, ready to use for enrollment and obtaining the second factor of authentication by end-users.

### Messaging features

- **Authentication Management** allows two types of notifications in mobile applications: SYNC and PUSH.
  - **SYNC**: in-app notifications in the standalone app or through the SDK. It has no cost for the client and allows more than one device to be associated per user.
  - **PUSH**: notifications integrated into the mobile operating system (enabled through the use of the SDK or standalone application).
- Sending email through the client's own SMTP server.
- SMS sending.

## User Portal

The portal allows users to perform various tasks, including:

- see their data and the apps they have access to,
- enter each of these applications without having to re-enter credentials (single sign-on),
- request access to applications,
- manage devices and sessions,
- consult their activity within the portal,
- change password,
- recover the password in the authentication form.

The same authentication form allows authenticating native users of the solution and authenticated users in an Active Directory.

If the user is an administrator, one of their applications is the administration portal, which they can access from the user portal.

## Administration Portal

The administration portal allows:

- Configure password policies, view and create users (one by one or in batches), configure applications with their user flows, and review execution logs.
- Synchronization of users from multiple AD (centralized repository).
- The massive attachment of native users through .CSV files.
- Review lists of users (both native and AD) including their data.
- Create a native user by entering their data.

## Reports, Dashboards and Audit Logs

Reports and audit logs are included to control the operation of the system. In addition, there are APIs with information to develop dashboards.

### Reports

- Total number of users.
- Users by their status (enabled, disabled, active, inactive).
- Users by type (native and Active Directory).
- Creation/Deletion/Modification of users.
- Reset and password changes.
- Type of MFA used (SMS, email, OTP).
- Failed and successful authentications/accesses.

### Dashboards (APIs)

- Total number of users.
- Users by their status.
- State of the agents.
- Number and percentage of MFA used.
- Number of successful and failed authentications.
- Number of successful and failed accesses.
- Number and percentage of passwords reset.
- Access number to integrated applications.

## Role-Based Access Control (RBAC)

The access to applications is based on the user's roles. Each application has an access permission that includes the application's name. This permission can be included in the definition of one or more roles, so that users with the appropriate role(s) can access the application.

User roles can be associated with AD groups. Therefore, a member of an AD group will automatically have all the roles associated with that group. This association is dynamic, so if the user leaves the group, the user loses the roles. Also, if the association of groups and roles is changed, users may gain or lose roles.

## Attribute-Based Access Control (ABAC)

Access to applications is based on user attributes. During the login process, including SSO, if the user has provided a correct password and the rule engine is active, enabled rules will be validated.

The rule engine will be configured to return one of two possible action codes: allow or deny access.

## MFA Management

The system allows managing the existence of multiple authentication factors, both for applications connected with OIDC or SAML and for RADIUS clients.

In the case of **OIDC or SAML** applications, it is possible to configure the authentication process for each application. The administrator can choose the authentication policy, for example: password only, TOTP only, password and TOTP, password and second factor chosen by the user, among others.

In the case of **RADIUS** clients, it is possible to choose the OTP type according to the user's roles. Users will login with their password and the OTP configured for their roles. It is also possible to give ac cess to users who are not in any of the identified roles configured for this purpose. In that case, they will enter only with a password. Since user AD groups can be linked to roles, this feature can also work with AD groups.

## Access Profiles

Access profiles allow establishing authentication policies and access restrictions for users and applications.

Each user can have one or more access profiles depending on their roles, as well as the applications they access. Therefore, the concept of dynamic access profile is incorporated, which calculates the combination of profiles to allow or restrict user access in each case, whether requesting two-factor authentication (2FA), reauthentication or attribute-based access control.

## Rule Engine

Authentication Management's rule engine is based on the configuration of a set of attributes for access restriction to users, which can be adapted to the needs of each company or organization.

The rules available for access denial are:

- IP addresses
- Days of the week
- Time interval
- Countries

The rules apply per time zone, and an exception can be configured for a specific role, such as the Administrator role.

## Passwordless Login: FIDO2

FIDO2 is a global authentication standard developed by FIDO Alliance and based on public key cryptography.

FIDO2 allows users to use their own devices (phones, desktop computers, USB security keys, etc.) for quick and secure authentication instead of their usual password.

Scope of FIDO2 in Authentication Management:

- Configuration of the FIDO2 factor and registration of authenticators from the administration portal for users with the role of Administrators.
- Self-service registration of FIDO2 authenticators from the user portal.
- Possibility of using a registered FIDO2 authenticator as an alternative to the password in the user portal login.
- Option to use a registered FIDO2 authenticator as an alternative to the password in the Single Sign-On (SSO) module.

## Directory Module

The Directory module manages the data (attributes) of the Authentication Management identities, which enables the registration of multiple user attributes in the system.

By enabling this module, it is possible to store and retrieve custom user attributes. In the current version native users can be created in Authentication Management with their personal names.

## Integration with VU Identity Link

Integration with VU Identity Link allows users to authenticate their identity through biometric recognition and document verification.

This ensures that users who are trying to log into Authentication Managementor applications managed by the portal are really who they say they are. Additionally, this integration helps improve data quality, detect attacks, and protect your business.

## Other Features

- Allows the definition of user name and password creation policies:
  - Password complexity settings.
  - Password history.
  - Password exclusion list.

- Allows defining policies for automatic user blocking.

- Allows the definition of policies for automatic unlocking of passwords and OTP.

- Supports integration with hard tokens.

- Communication between the presentation layers and the product server is over an SSL/TLS connection.

- The methods available through the API allow:
  - Enable and disable users and types of authentication factors.
  - Validate credentials.
  - Remove users and types of authentication factors from the platform.
  - Modify and assign a user's password on the platform.
  - Add Access Control Service groups.
  - Create, register, validate, block and unblock users.
  - Unsubscribe authentication factors assigned to users.
  - Provide OTP codes assigned to the user in the mobile application.
  - Validate an end user's token.
  - Report the status of a user.

- Automatic registration of the mobile OTP factor to new Active Directory users when registering them in Authentication Management.

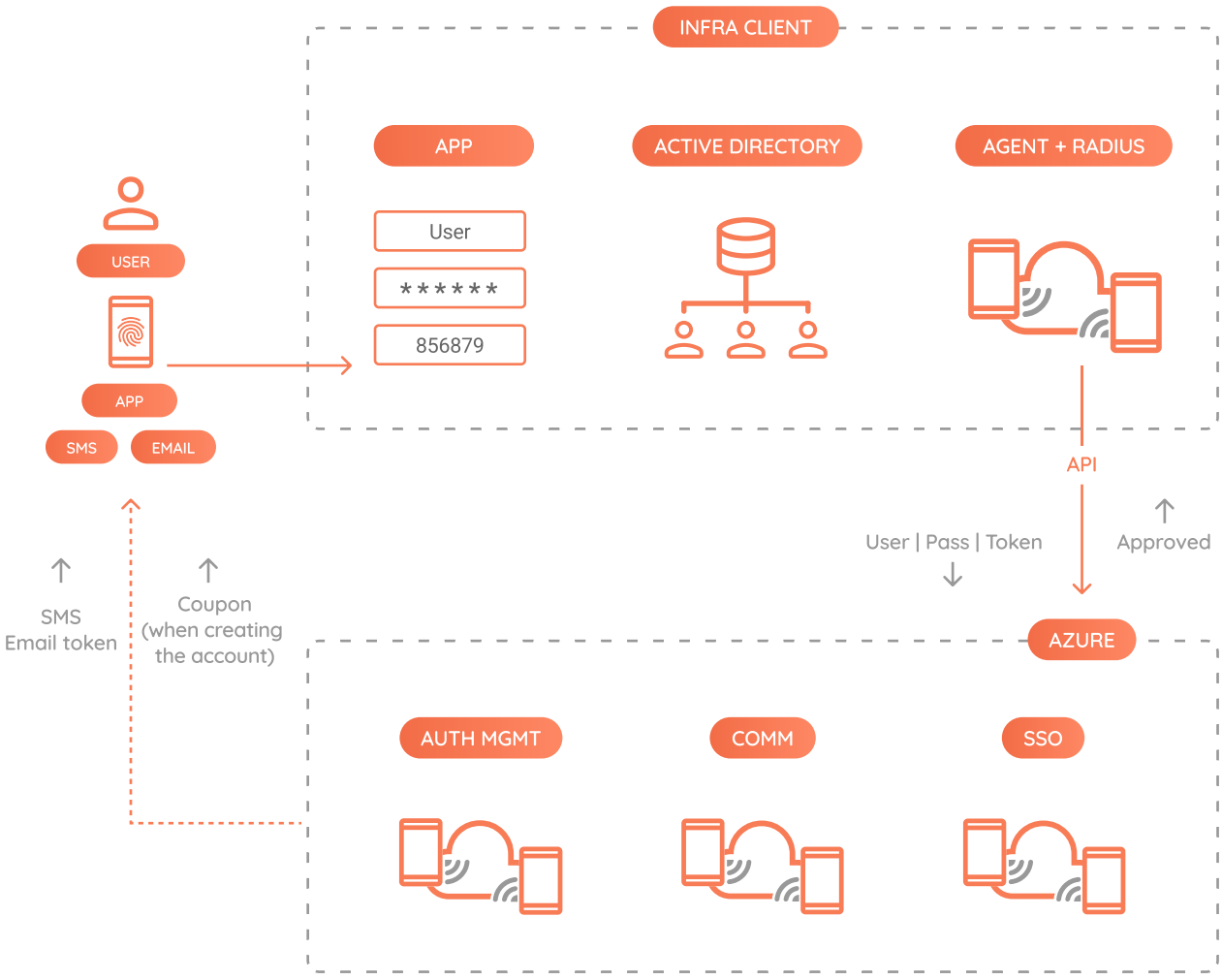
- Notifications related to password creation/recovery can include personalized user data stored in the Directory module.

# Distribution

**Authentication Management** can be purchased as software licensing (on-premises) or Software as a Service (SaaS).

## Software as a Service (SaaS)

**Its cloud architecture**, with a multi-tenant and multi-client administration portal, allows private management by different businesses or internal clients. It is optimized for Microsoft Azure and integrated with Azure DevOps, Azure Vault, and Azure Monitor using dockerized instances.



### Agent: Software and Hardware Requirements

It is used to connect the client infrastructure (AD, VPN terminator) with the cloud deployment of Authentication Management. It is installed in a virtual machine with a Linux operating system and Docker container technology.

It is a requirement that in said virtual machine the agent can communicate with the AD and the VPN server against the agent.

| Infrastructure component | Requirement (*) | Delivery |
|---|---|---|
| Agent | Linux VM<br>2 cores<br>4 GB RAM<br>20 GB disk<br>Docker Tool (version 3.x) | Docker images |

(*) For high availability of the agent, you will need to have 2 virtual machines and a load balancer.

### Monitoring and Alarms

All components are monitored using Azure Monitor, Azure Log Analytics and Azure Application Insights in order to maintain performance metrics for each component involved and a log trace for auditing and troubleshooting both the infrastructure and the Authentication Management instances.

### High Availability

The service is managed by Azure Kubernetes Service, with replication in 3 zones within the Brazil South or Europe region. Service recovery in another region, in case of disruption, will be executed within a maximum of 30 minutes.

### Backups

For all databases, backups are performed several times per hour on an incremental basis and under retention policies. The backups are replicated in a different region than the productive one.

### Update

VU will perform corrective and evolutionary updates according to availability and in hot-swapping mode from the pre-production environment exclusively. The updates happen under incremental policies with rollback in the event of failures.

### Uptime

- 99% annual uptime outside the maintenance window: 00:00 to 22:00, GMT-3.
- 98% annual uptime within the maintenance window: 22:00 to 00:00, GMT-3.

There will be a maintenance window from 01:00 to 03:00 UTC. Outside of these hours, maintenance activities will not be carried out. In the case of the maintenance window, the SLA will be 98% annual uptime, while in the production period the SLA is 99% uptime.

### Recovery Time Before Service Discontinuation

The service will be configured to maintain a three-hour Recovery Time Objective and a one-hour Recovery Point Objective.

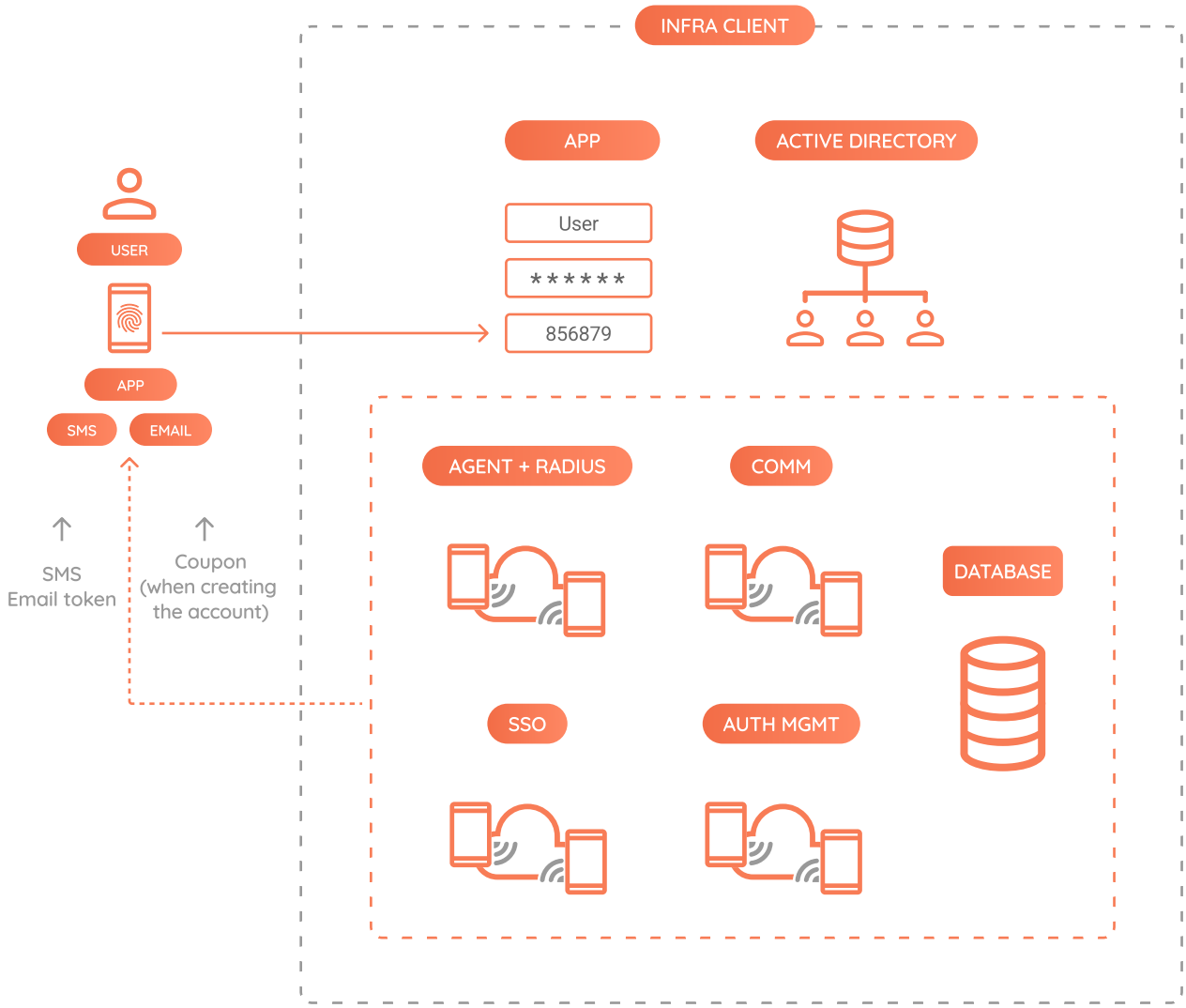
### Recovery Time Before Service Degradation

The infrastructure is deployed on elastic services, extending its capabilities when configured thresholds are exceeded, resolving eventual service degradation.

The process of adjusting the instances is automatic and for this purpose it is established in maximum times of 15 minutes.

# Software Licensing (On-Premises)

**Authentication Management on-premises** allows the deployment of single tenant components on the client's own servers.



## Hardware and Software Requirements

Authentication Management consists of 4 components, which are deployed in a microservices architecture that runs on top of Docker or Kubernetes.

These services are:

- Authentication server.
- Single sign-on (IdP) module.
- Communication server.
- Agent.

### — Hardware Requirements

The minimum virtual machine should be:

| vCPU | Memory (Gb) | System Storage (Gb) |
|---|---|---|
| 2 | 8 | 60 |

Based on this, it will be possible to scale both vertically by adding more CPU and memory, or horizontally (recommended) by adding replicas. For the latter scenario, it is recommended to deploy with Kubernetes. A load balancer must be provided.

With the base node, it can handle up to 8 transactions per second.

| Users (reference) | Transactions per second | Node / VM | | | | DB | |
|---|---|---|---|---|---|---|---|
| | | Cores | RAM | Replicas | System storage | Monthly storage | Annual storage |
| 250.000 | 8 | 2 | 8 | 1 | 60 GB | 25 GB | 300 GB |
| 500.000 | 16 | 2 | 8 | 2 | 120 GB | 50 GB | 600 GB |
| 1.000.000 | 32 | 2 | 8 | 4 | 240 GB | 100 GB | 1.2 TB |
| 2.000.000 | 64 | 2 | 8 | 8 | 480 GB | 200 GB | 2.4 TB |

## — Software Requirements

Since the entire application is containerized, only the operating system and Docker tools are required.

| Operating System | Container Tools | Database |
|---|---|---|
| Linux<br>Centos / Ubuntu / Red Hat | Esquema 1:<br>Docker Engine (v. 19+) (*)<br>con Docker Compose (v. 3+) (*)<br><br>Esquema 2:<br>Kubernetes (v. 1.24+) | SQL Server 2019<br><br>For other database schemas, please inquire |

* VU will support installation and configuration of Docker and Docker Compose.

## — High Availability

- For Docker + Docker Compose setup: double the number of virtual machines.
- For Kubernetes deployments: work with n+1 nodes or follow the client's policy.
- Database set up with high availability and redundancy (active-active or active-passive).

## — Client Components

VU offers an SDK that can be integrated into Android and iOS mobile applications and that allows the generation of the TOTP.

| Operating System | Technology | Delivery |
|---|---|---|
| Android | Java | SDK + Example |
| iOS | Swift | SDK + Example |
| Híbrido | Javascript | SDK + Example |

# End of Extended Support (EOS) and End of Life (EOL)

| | Full Support | Sustained | Support Only | Non-supported |
|---|---|---|---|---|
| New features might be expected | ✓ | No | No | No |
| Bug fixes | ✓ | ✓ | No | No |
| Customer support | ✓ | ✓ | ✓ | No |
| *Years since release date* | 2 | 3 | 4 | - |

| Version | Release date | Last customer ship | New features until | Fixes until | Last Day of Support (LDOS) | Non-supported since |
|---|---|---|---|---|---|---|
| 6.x | 4/1/2022 | 4/1/2025 | 4/1/2025 | 4/1/2026 | 4/1/2027 | 4/2/2027 |

# Contact

If you need more information or want to schedule a demo of this solution, please write to us at: sales@vusecurity.com

# Other VU Products

Fraud & AML | Fraud Analysis | Device Finger Print

Onboarding Management | ID | Face | Voice | Touch

CIAM

## About VU

VU is a global cybersecurity company, specializing in identity protection and fraud prevention. It develops modular solutions, easy to integrate and adaptable to both corporate and government environments.

To achieve this, VU uses innovative technologies based on the combination of traditional cybersecurity controls, biometrics, geolocation, artificial intelligence, machine learning, document recognition and user behavior analysis.

More than 350 million people around the world and 130 clients in 30 countries in Latin America, Europe and the United States use VU technology to digitize their businesses and increase the level of operations, reducing the risks of attacks and loss of information.

Its strategic alliances with Microsoft, Telefónica, IBM, BGH, Intel, Cisco and Accenture, among other companies, help VU fulfill its mission: build secure and frictionless experiences that improve the quality of life of citizens and organizations.

vusecurity.com