What is?

Authentication Management® validates people’s identities to protect their personal information.

Product components

Authentication Management® consists of three modules: Server®, SDK® and App®.

This product is the ideal complement for environments which already have a robust authentication process but may also need an additional emergency solution.

Modules and add-ons

Server® is a user authentication model. It is multi-factor and multi-platform, and the integration in the cloud is flexible and personalized.

SDK® is a module that integrates Authentication Management’s functions into any Android or iOS mobile application.

App® is a stand-alone ready-to-use mobile application that allows end-users to register their accounts and get a second-factor authentication code.

© 2022 VU Inc. All rights reserved.
Server
Authentication Management
Datasheet
v6.0.00

© 2022 VU Inc. All rights reserved.
**What is?**

*Authentication Management*® validates people’s identities to protect their personal information.

The *Server*® module is responsible for the multi-factor authentication process that unifies the user’s policies, passwords, and traceability. It provides a flexible scheme that is easy and customizable when implementing a second-factor system on the cloud through any device connected to the Internet.

*Authentication Management* is available in the following options:

**SaaS:** Cloud deployment option.

**On premises:** Option that allows the deployment of single tenant components on the client’s own servers.

**Logical functional diagram**

![Logical functional diagram](image-url)
The **Server** module is a solution that acts as an authentication node. Thanks to its wide integration capacity, it can be implemented through REST Web services in any environment or technological platform, regardless of the language employed. The communication between the presentation layers and the product server is carried out via an SSL/TLS connection.

**User interface options**

**Integration API**
Through this technology, you can add security tokens (OTP, HOTP, Sync, Push) to various environments such as VPN, Intranets, Applications, and Office 365. This is achieved by using the most recognized integration technologies and protocols on the market such as SAML2, OIDC, Radius, API, and App. Authentication Management simplifies the authentication processes through its Single Sign-on capabilities. Thus, it can also be integrated into the solution's administration Backoffice with Active Directory for both user management and access control.

**Functional scope**

**Use cases**

Authentication Management as an identity provider

- Authentication Management allows you to authenticate users to an application through the following interfaces:
  - SAML2
  - OIDC
  - Radius (through VPN)
  - WebServices REST

- Authentication Management can be integrated with Active Directory (through a VPN tunnel), allowing to:
  - Verify that the user is enabled in Active Directory to validate that it can be used.
  - Validate user passwords in Active Directory.
  - Use Active Directory users to gain access to the configuration portal (Backoffice), along with the ability to establish role equivalencies between both platforms.
  - Massive registration of users through CSV or synchronization with AD/LDAP.
  - Unsubscribe users in the following way:
    - Authentication Management checks whether the user exists in Active Directory to enable it and does not allow users that do not exist in Active Directory to register with Authentication Management.
    - If the password is locked in Active Directory, the user is considered locked for all operations.

- Authentication Management allows you to provide identities and two-factor authentication to any application that supports the interfaces mentioned before.
Single sign-on in Authentication Management

- Authentication Management simplifies authentication processes by recognizing active sessions to prevent users from having to authenticate to each application they wish to enter.

Authentication management as a two-factor authentication provider

- Allows using the following two-factor authentication methods:
  - TOTP: Time-based one-time password.
  - HOTP: HMAC-based one-time password.
  - SYNC: In-app notifications via the standalone app or the SDK. There is no cost to the customer, and it allows more than one device per user to be associated.
  - PUSH: The notifications are built into the mobile OS (enabled by using the SDK or standalone app). They are deployed through Firebase (for setup, it is required a client API-key).
- Each one of these methods of two-factor authentication can be sent to the end-user through the following channels:

<table>
<thead>
<tr>
<th>Method</th>
<th>SMS</th>
<th>E-mail</th>
<th>mobile OS</th>
<th>In-app (SDK)</th>
<th>App Authentication Management</th>
<th>2FA wallets*</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOTP</td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>HOTP</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>PUSH</td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>SYNC</td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>

* Google Authenticator, Microsoft Authenticator, etc.

- Per interface, the following channels are supported:

<table>
<thead>
<tr>
<th>Channel</th>
<th>WebServices</th>
<th>SAML2</th>
<th>OIDC</th>
<th>RADIUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>In-app (SDK)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>App Authentication Management</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>2FA wallets *</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

* Google Authenticator, Microsoft Authenticator, etc.
• It is possible to strengthen authentication processes by supporting one-time authentication factors (OTP). Authentication Management provides time-based (TOTP), and event based (HOTP) factors.
• Through the integration with FreeRadius, Authentication Management provides two-factor authentication options for VPN access.
• Allows registering the two-factor authentication through email.
• It allows sending the two-factor authentication through email, SMS, Push notifications to the mobile applications, and synchronization notifications through the Authentication Management SDK itself.
• Authentication Management can provide two-factor authentication capabilities to the existing users in the Active Directory instances.
• The registration and management of OTPs in mobile applications, whether native or hybrid, is allowed through an SDK.
• Allows assigning one or more two-factor authentication methods to each user.
• Authentication management allows using identity wallets such as Microsoft Authenticator or Google Authenticator. Additionally, including a service’s application.

Mobile applications in Authentication Management

• It allows users to receive two-factor authentication on the mobile app through the native SDK on iOS and Android and Hybrid (JavaScript). It can be integrated for both registrations and obtaining two-factor authentication.
• A ready-to-use standalone mobile app for end-user registration and obtaining two-factor authentication.
• The mobile apps allow the creation of multiple accounts, with their seeds, as well as the synchronization of clocks.

Messaging characteristics:

• Authentication management allows two types of notifications in mobile applications: SYNC and PUSH.
• SYNC: In-app notifications in the standalone app or via the SDK. There is no cost to the customer, and it allows more than one device per user to be associated.
• PUSH: Notifications built into the mobile operating system (enabled via the SDK or standalone app).
• E-mail is sent through the client’s SMTP server.
• SMS is sent through the Operator gateway.

Other Authentication Management characteristics:

• It allows massive registration of users and their contact channels for sending the two-factor authentication.
• Allows defining user and password creation policies.
• Allows defining user blocking policies.
• Supports hard-tokens integration (RFC 6238/4226).
• The communication between the presentation layers and the product server is carried out via an SSL/TLS connection.
• The methods available through the API allow:
  • Enabling and disabling users and types of authentication factors.
  • Validate credentials.
  • Removal of users and types of authentication factors from the platform.
  • Modification and assignment of a user password on the platform.
  • Addition of Access Control Service groups.
  • User creation, registration, validation, blocking, and unblocking.
  • Cancel the authentication factors assigned to users.
  • Provision of OTP codes assigned to the user in the mobile application.
  • End-user token validation.

Software as a Service features

Service degradation alerts
• The following anomalies will be monitored and alerted:
  • Response time
  • Error rates

High availability
• Azure Kubernetes Service manages the service within the Brazil (Sao Paulo) region.
• The recovery of the service in another region, in case of interruption of the service in Brazil (Sao Paulo), will be carried out within a maximum period of 30 minutes.

Backups
• Backups are performed incrementally several times an hour and under retention policies for all databases.
  • Backups are replicated in an alternate region to the production one.

Update
• VU will perform corrective and evolutionary updates based on availability and in hot-swapping mode from the pre-production environment exclusively.
  • Updates occur under incremental policies with rollback in the case of eventual failures.

Uptime
• 99% annual uptime outside the maintenance time window
  • 00:00 a 22:00, GMT-3
• 98% annual uptime inside the maintenance time window
  • 22:00 a 00:00, GMT-3
Infraestructure

There will be a maintenance window from 10:00 p.m. until 12:00 p.m., Argentine time. While from 00:00 to 22:00 there will be no maintenance activities. In the case of the maintenance window, the SLA will be 98% of the annual uptime, while in the production period the SLA will be 99% of the uptime.

Recovery time before service interruption

The service will be configured to sustain a 3-hour Recovery Time Objective and a 1-hour Recovery Point Objective.

Recovery time before service degradation

The infrastructure is built on elastic services, expanding its capabilities when the configured thresholds are exceeded, fixing any service degradation.

Instance adjustment is automatic and for this, a maximum time of 15 minutes is established.

On-premises features

Software requirements and compatibility

<table>
<thead>
<tr>
<th>Operative system</th>
<th>Database</th>
<th>App Server</th>
<th>Java</th>
<th>Devices compatibility (SDK)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centos/ Red Hat 7.9</td>
<td>PostgreSQL 9 or higher</td>
<td>Tomcat 9.x</td>
<td>1.8</td>
<td>iOS 11 or higher</td>
</tr>
<tr>
<td>Ubuntu 18.x or higher (*)</td>
<td>MS SQL 2019 or higher</td>
<td>Jboss 7.11</td>
<td></td>
<td>Android 5 or higher</td>
</tr>
<tr>
<td>(Preferably versions LTS: 18.04 y 20.04) (**)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Server 2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(*) Recommended

(**) It is recommended to use LTS (Long Term Support) versions. These versions are updated every 2 years.
## Hardware sizing guidelines*

<table>
<thead>
<tr>
<th>Number of users</th>
<th>Parent instance</th>
<th>Secondary instance</th>
<th>Transactions per second</th>
<th>Required storage capacity</th>
<th>LOG storage</th>
<th>Onboarding storage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Processor</td>
<td>Memory</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 a 10.000</td>
<td>8 processing threads</td>
<td>6 GB RAM</td>
<td>8 processing threads</td>
<td>6 GB RAM</td>
<td>16</td>
<td>120 GB - HD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>178 GB - HD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>120 GB - HD</td>
</tr>
<tr>
<td>10.000 a 50.000</td>
<td>16 processing threads</td>
<td>8 GB RAM</td>
<td>16 processing threads</td>
<td>8 GB RAM</td>
<td>32</td>
<td>240 GB - HD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>980 GB - HD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>240 GB - HD</td>
</tr>
<tr>
<td>50.000 a 100.000</td>
<td>32 processing threads</td>
<td>16 GB RAM</td>
<td>32 processing threads</td>
<td>16 GB RAM</td>
<td>64</td>
<td>480 GB - HD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4,4 TB - HD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>480 GB - HD</td>
</tr>
<tr>
<td>100.000 a 250.000</td>
<td>64 processing threads</td>
<td>32 GB RAM</td>
<td>64 processing threads</td>
<td>32 GB RAM</td>
<td>128</td>
<td>960 GB - HD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6,3 TB - HD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>960 GB - HD</td>
</tr>
<tr>
<td>250.000 a 1.000.000</td>
<td>128 processing threads</td>
<td>64 GB RAM</td>
<td>128 processing threads</td>
<td>64 GB RAM</td>
<td>256</td>
<td>2 TB - HD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>24 TB - HD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2 TB - HD</td>
</tr>
</tbody>
</table>

* The calculations and estimates contemplate the functioning on high availability.

## Technical information

The SDK can be integrated in:

<table>
<thead>
<tr>
<th>Technology</th>
<th>Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android Java</td>
<td>SDK + Reference project</td>
</tr>
<tr>
<td>iOS</td>
<td>SDK + Reference project</td>
</tr>
<tr>
<td>Web</td>
<td>SDK + Reference project</td>
</tr>
<tr>
<td>Hybrid Cordova y Ionic</td>
<td>SDK + Reference project</td>
</tr>
<tr>
<td>Javascript</td>
<td>SDK + Reference project</td>
</tr>
<tr>
<td>Javascript (Swift y Java)</td>
<td>SDK + Reference project</td>
</tr>
</tbody>
</table>
## Integrations
- API REST
- Radius
- Syslog
- Nagios
- SAML2
- OIDC
- WebServices REST

## Access management
- Active Directory
- LDAP

## Log and data management
- PowerBI
- Kibana

## Mobile compatibility
- iOS
- Android

---

### Authentication Management Server v6.x has these milestones that define its life cycle:

<table>
<thead>
<tr>
<th></th>
<th>Release:</th>
<th>New features until:</th>
<th>Fixes until:</th>
<th>Last day of support:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>April 1st, 2022</td>
<td>April 1st, 2024</td>
<td>April 1st, 2025</td>
<td>April 1st, 2026</td>
</tr>
</tbody>
</table>

---

### Outstanding use cases

- User access and personal data management.
- Secure VPN: secure access to virtual private networks.
- Virtual token: OTP management.
Other VU modules and products that improve Server performance

Our products offer a 360° experience for both users and organizations. Each solution provides an additional layer of protection to their security strategy.

Onboarding Management Modules
• ID
• Face
• Voice
• Touch

VU Fraud Analysis

For more information or to request a demo, contact us by mail at: sales@vusecurity.com
VU SDK
Authentication Management
Datasheet
Android v2.0 / Cordova v1.0 / IOS v2.5
What is?

It is the component that integrates the Authentication Management’s functions into any Android or iOS mobile application, providing a robust two-factor authentication process to register, generate, and validate end-users identities.

This product is the ideal complement for environments that already have a robust authentication process but may also need an additional emergency solution.

SDK

Authentication Management® provides multi-factor identity authentication processes, including OTPs (One-time Passwords), which send end-users an identity verification code through different channels so they can log into the administrator’s app or web. Mobile Tokens® is the most widely used authentication channel as they provide flexibility and convenience to end-users and are more effective and cheaper for administrators.

Mobile Tokens are among the solutions VU Security offers to its clients to provide their users with an OTP verification code. This product is available for both Android and iOS.

Probably our customers have Mobile applications for their users, so VU Security offers the possibility of integrating App® (Mobile Tokens) and SDK®, which contains all the necessary methods to integrate the OTP functionality:

• Code triggering mechanisms
• Time synchronization between client and server
• OTP generation
• OTP management
The main goal of this module is to make it easy for developers to integrate App® into the administrator’s mobile application. It is for this reason that only the features listed above are included in the module. Screens and menus are not part of it, allowing the administrators to customize their application's user experience and preserve the security and integrity of their products.

Also, all the data stored in App & Cloud Server® is delivered to be persisted by the administrators in the way they want.

To make the integration easier, the SDK® module contains examples of all its features. Mobile Tokens® are integrated into the administrators’ applications through the following SDK:

- Android
- iOS
- Cordova

For more information or to request a demo, contact us by mail at: sales@vusecurity.com
What is?

App® is a stand-alone, ready-to-use, mobile application that allows end-users to register their accounts and get a second-factor authentication code.

Mobile Tokens® guarantees continuity in the security strategy established by your company, granting a temporary or permanent authentication system to deal with risks due to loss, theft, or inaccessibility to the method chosen by the use.

Downloads

Download App® from the official stores only:

• Android
• iOS

For more information or to request a demo, contact us by email at: corporate@vusecurity.com