Authentication Management
Datasheet
Version 6.5.0
What is? 02

Benefits 02

Modular solution 02

Functional scope 03
  - Identity authentication 03
  - Single sign-on 03
  - Two Factor Authentication (2FA) 04
  - Mobile apps 06
  - Self-service portal 06
  - Administration portal 07
  - Reports, dashboards and audit logs 07
  - Role Based Access Control (RBAC) 08
  - MFA management 08
  - Other features 09

Distribución 10
  - Software as a Service (SaaS) 10
  - Software licensing (on-premises) 12

Other VU products 14

Support 15

Contact 15
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-premise 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 and identity federation. 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.

• 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 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 configuration portal (backoffice).

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

- It provides identities whose information can be in an Active Directory or native identities stored directly in the solution. This means that the solution can operate with or without an Active Directory and even have some AD identities and some 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.

- Multiple user authentication flows, with one or two factors, configurable for each application.
Two Factor Authentication (2FA)

One-time authentication factors (OTP) allow robust authentication processes. Authentication Management provides second factor options to VPN access through integration with FreeRadius.

It makes it possible to enroll the second authentication factor through email, as well as SMS, push notifications to mobile applications and SYNC notifications through the Authentication Management SDK itself.

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

<table>
<thead>
<tr>
<th></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, among others.

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

<table>
<thead>
<tr>
<th></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, 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.

It is a standalone mobile application, ready to use, for the enrollment and obtaining of 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.

Self-service portal

Users have access to a self-service portal. This portal allows them to see their data, the applications they have access to, access one of those applications without the need to re-enter credentials (single sign-on), change the password from the portal or 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 self-service portal.

**Administration portal**

The administration portal allows the configuration of password policies, view and create users (one by one or in batches), configure applications with their user flows, and review the execution logs.

- Synchronization of users from multiple AD (centralized repository).
- Massive registration of native users through .CSV files.
- Review lists of users (both native and AD) including their data.
- Create a native user through data entry.

**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**

- Access to the solution.
- Creation, elimination and modification of users.
- Failed authentications/accesses.
- Reset and password changes.
- Total number of identities.
- Identities by status (active, inactive).
- Identities by type (AD, native solutions).
- Type of MFA used (SMS, email, OTP).
Dashboards

- Total number of identities.
- State of the agents.
- Percentage of identities with MFA.
- Number of authentications.
- Number of failed authentications.
- Number and percentage of reset passwords.

Role Based Access Control (RBAC)

- **Access to applications is based on user roles.** Each app has an access permission that includes the name of the app. This permission can be included in the definition of one or more roles, so that users with an appropriate role can enter the application.

- **User roles can be associated with AD groups.** Thus, 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 can gain or lose roles.

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 AD group. Users will login with their password and the OTP configured for their AD group. It is also possible to give access to users who are not in any of the AD groups configured for this purpose. In that case, they will enter only with a password.
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.
Distribution

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

**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.

**Server components**

- Guaranteed uptime.
- Hosting in world-class services.
- Isolated data for each client.

**Client components**

- Optional.
- Native iOS or Android SDK.
- Javascript SDK.
- Standalone application.

**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. It is possible to measure indicators such as number of nodes, CPU usage in NODES, disk usage, number of pods per component, number of http codes other than 200, use of each database, number of http requests and errors per tenant, number of erroneous password and OTP validations per unit of time, among others. Automated alerts can be established on all these indicators.
Service degradation alerts

The following anomalies will be monitored:
• response times,
• error rates.

High availability

• The service is managed by Azure Kubernetes Service.
• With replication in 3 zones within the Brazil South region.
• The recovery of the service in another region, in case of interruption of the service in Brazil South, will be carried out within a maximum period 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

• Corrective and evolutionary updates will be made according to availability and in hot-swapping mode from the pre-production environment exclusively.
• Updates are made under incremental policies with rollback in case of possible failures.

Uptime

• 99% annual uptime outside the maintenance time slot.
  • 00:00 to 22:00, GMT-3.

• 98% annual uptime within the maintenance time slot.
  • 22:00 to 0:00, GMT-3.

Infrastructure

There will be a maintenance window from 10:00 p.m. to 12:00 p.m. Argentine time, while from 12:00 a.m. to 10:00 p.m. no maintenance activities will be carried out. In the case of the maintenance window, the SLA will be 98% of annual uptime, and in the production period, the SLA is 99% of uptime.
Recovery time before service discontinuation

The service will be configured to support a Recovery Time Objective of three hours and a Recovery Point Objective of one hour.

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.

![Diagram]

**Server components**
- Identity server.
- Integration with authentication protocols.
- Messaging server.

**Client components**
- Optional.
- Native iOS or Android SDK.
- Javascript SDK.
- Standalone application.
Hardware and software requirements

Software requirements and compatibility

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Database</th>
<th>App Server</th>
<th>Java</th>
<th>Device compatibility (SDK)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centos/Redhat 7.9 (*)</td>
<td>PostgreSQL version 9 or higher</td>
<td>Tomcat 9.31 or higher (*)</td>
<td>11+</td>
<td>iOS 11 or higher</td>
</tr>
<tr>
<td>Ubuntu LTS (*)</td>
<td>MS SQL 2019 or higher (*) (**)</td>
<td>Jboss 7.11 or higher</td>
<td></td>
<td>Android 5 or higher</td>
</tr>
<tr>
<td>Windows Server 2019</td>
<td>MySQL</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Recommended.
** Provided in the installation packages.

Server components

<table>
<thead>
<tr>
<th>Users</th>
<th>transactions per second</th>
<th>Cores</th>
<th>RAM</th>
<th>Storage</th>
<th>Estimated monthly storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>250.000</td>
<td>8</td>
<td>2</td>
<td>4</td>
<td>60 GB</td>
<td>25 GB</td>
</tr>
<tr>
<td>500.000</td>
<td>16</td>
<td>4</td>
<td>8</td>
<td>120 GB</td>
<td>50 GB</td>
</tr>
<tr>
<td>1.000.000</td>
<td>32</td>
<td>8</td>
<td>16</td>
<td>240 GB</td>
<td>100 GB</td>
</tr>
<tr>
<td>2.000.000</td>
<td>64</td>
<td>16</td>
<td>32</td>
<td>480 GB</td>
<td>200 GB</td>
</tr>
<tr>
<td>+2.000.000</td>
<td>Consult</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* The calculations are estimated according to usual instances of the product. For high availability configurations, it is suggested to use instances with the same characteristics as those presented.
Client components

<table>
<thead>
<tr>
<th>Technology</th>
<th>Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>Java</td>
</tr>
<tr>
<td>iOS</td>
<td>Swift</td>
</tr>
<tr>
<td>Hybrid</td>
<td>Javascript</td>
</tr>
</tbody>
</table>

Other VU products

Onboarding Management
- ID
- Face
- Voice
- Touch

Fraud & AML
- Fraud Analysis
- Device Fingerprint

CIAM
Support

VU will provide **level 3 support**.

Support includes a set of technologies and rights to help the customer maximize the investment made in VU licenses.

Contact

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