Authentication MANAGEMENT

VU

Datasheet

Versão 6.19

Março 2025
Link da última versão disponível

2025 VU Inc. Todos os direitos reservados.

O que é?

Authentication Management® é uma solução projetada para proteger as organizações contra roubo ou uso indevido de credenciais corporativas por meio de mecanismos Zero-Trust baseados em vários fatores de autenticação adaptáveis e sistemas biométricos de reconhecimento facial e de voz.

Oferece uma camada extra de segurança nos processos de autenticação, simplificando-os por meio de seus recursos de logon unificado (Single sign-on). Assim, também tem a possibilidade de integrae a ferramenta Active Directory tanto para o gerenciamento de usuários quanto para controle de acesso ao backoffice de administração próprio da solução.

Authentication Management permite incorporar a tecnologia da VU a qualquer recurso corporativo, incluindo VPNs, Intranets, aplicativos e Office 365, utilizando as integrações e protocolos mais reconhecidos do mercado, como SAML2, OIDC, Radius, API e App.

Benefícios

• **Segurança Zero-Trust** para ambiente cloud, híbrido ou on-premise. Por meio da autenticação multifator, é garantido que o legítimo proprietário das credenciais seja a entidade que está acessando o sistema.

• **Melhora a experiência nos processos de autenticação** graças à funcionalidade de Single sign-on. Em um único passo, é possível autenticar os usuários em diversos aplicativos e sistemas corporativos.

• **Oferecido na modalidade SaaS**, permite uma implantação e integração fácil e simples com um impacto mínimo na operação diária da organização.

• **Oferecido na modalidade de licenciamento de software (on-premises)**, permite a implantação dos componentes na infraestrutura do cliente.

• **Escalabilidade. Authentication Management** foi projetado para ser o blocoa partir do qual construir a estratégia de gerenciamento da identidade e acessos.

Solução modular

A VU oferece soluções modulares para oferecer aos clientes fácil integração, rapidez e flexibilidade. Authentication Management conta com 3 módulos: Server, SDK e App.

- **Server** é o módulo de autenticação do usuários. É multifator e multiplataforma, e possui integração flexível e personalizada na nuvem. No modo SaaS, são geradas instâncias personalizadas que se conectam à infraestrutura do cliente por meio de um agente.
- **SDK** é o módulo integrador das funcionalidades do Authentication Management para aplicativos móveis de Android e iOS.
- **App** é um aplicativo móvel standalone, pronto para usar, para registro e obtenção do segundo fator de autenticação pelos usuários finais.

2025 VU Inc. Todos os direitos reservados.

Escopo funcional

Autenticação de identidades

• O **Authentication Management** permite autenticar usuários em aplicativos usando as seguintes interfaces:
- SAML2
- OIDC – OpenID Connect
- Radius (através do agente)
- WebServices REST

• Integra-se com vários Active Directory (através de agente) permitindo:
- verificar se o usuário está habilitado no Active Directory para validar seu uso,
- validar as senhas dos usuários no Active Directory,
- usar os próprios usuários do Active Directory para obter acesso ao portal de configuração (backoffice).

• Permite fornecer identidades e segundo fator de autenticação para qualquer aplicativo compatível com as interfaces mencionadas anteriormente.

• Fornece identidades cujas informações podem estar em um Active Directory ou identidades nativas armazenadas diretamente na solução. Ou seja, a solução pode operar com ou sem Active Directory e ainda ter algumas identidades AD e outras identidades nativas.

Single sign-on

• **Authentication Management** simplifica os processos de autenticação reconhecendo sessões ativas para evitar que os usuários tenham que se autenticar em cada aplicativo que desejam acessar.

• Múltiplos fluxos de autenticação de usuários, com um ou dois fatores, configuráveis para cada aplicativo.

2025 VU Inc. Todos os direitos reservados.

Segundo fator de autenticação

Os fatores de autenticação de uso único (OTP) é possível fortalecer os processos de autenticação. Por exemplo, no caso do Secure VPN, **Authentication Management** fornece o segundo fator através da integração com um agente/FreeRadius.

Authentication Management possibilita o cadastramento do segundo fator de autenticação no aplicativo do cliente (SDK) através do envio de um cupom ou código QR por e-mail, SMS ou algum outro canal que o cliente possua. Por sua vez, permite-lhe inscrever-se na aplicação móvel TOTP, autenticações do tipo push e sync.

Tipos de fatores de autenticação

Authentication Management permite a configuração dos seguintes fatores de autenticação:

• **TOTP:** senha de uso único baseada no tempo.

• **HOTP:** senha de uso único baseada em eventos (contador HMAC).

• **SYNC:** notificações in-app no aplicativo autônomo ou por meio do SDK. Não tem custo para o cliente e permite associar mais de um dispositivo por usuário.

• **PUSH**: notificações integradas ao sistema operacional móvel (ativadas através do uso do SDK ou aplicativo standalone). É implementada por meio do Firebase (é necessária uma API key do cliente para sua configuração).

• **Magic Link**: permite autenticação por meio de um link enviado ao e-mail do usuário. Isso evita que o usuário precise gerenciar um maior número de senhas.

• **QR Code**: método de autenticação baseado em códigos QR. Está integrado ao App genérico VU, permitindo ao usuário utilizar dispositivos móveis para verificar sua identidade e autenticar transações, entre outras ações.

2025 VU Inc. Todos os direitos reservados.

Os fatores de autenticação podem ser enviados ao usuário final através dos seguintes canais:

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

* Google Authenticator, Microsoft Authenticator, entre outros.

Authentication Management suporta os seguintes canais por interface:

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

* Google Authenticator, Microsoft Authenticator, entre outros.

2025 VU Inc. Todos os direitos reservados.

Aplicativos móveis

Authentication Management permite que seus usuários recebam o segundo fator de autenticação no seu próprio aplicativo móvel através do SDK nativo em iOS e Android, bem como um híbrido (Javascript) que pode ser integrado tanto para registro quanto para obtenção do segundo fator de autenticação. Os aplicativos móveis permitem a criação de várias contas com suas sementes, bem como a sincronização de relógios.

Também está disponível nas lojas do Android e da Apple o aplicativo móvel standalone, pronto para uso, para o registro e obtenção do segundo fator de autenticação pelos usuários finais.

Características do sistema de mensagens

- **Authentication Management** permite dois tipos de notificações em aplicativos móveis: SYNC e PUSH.
  - **SYNC**: notificações in-app no aplicativo autônomo ou por meio do SDK. Não tem custo para o cliente e permite associar mais de um dispositivo por usuário.
  - **PUSH**: notificações integradas ao sistema operacional móvel (ativadas através do uso do SDK ou aplicativo standalone).
- Envio de e-mail através do próprio servidor SMTP do cliente.
- Envio de SMS.

Portal do usuário

O portal permite que os usuários realizem várias tarefas, incluindo:

- ver seus dados e as aplicações às quais têm acesso,
- acessar cada uma dessas aplicações sem a necessidade de reingressar credenciais (login único),
- solicitar acesso a aplicações,
- gerenciar dispositivos e sessões,
- ver sua atividade dentro do portal,
- alterar a senha,
- recuperar a senha no formulário de autenticação.

2025 VU Inc. Todos os direitos reservados.

O mesmo formulário de autenticação permite autenticar usuários nativos da solução e usuários autenticados em um Active Directory.

Se o usuário for administrador, um de seus aplicativos é o portal de administração, que pode ser acessado a partir do portal do usuário.

Portal de administração

O portal de administração permite:

- Configurar políticas de senha, visualizar e criar usuários (um por um ou em lotes), configurar aplicativos com seus fluxos de usuários e revisar os logs de execução.
- Sincronização de usuários de múltiplos AD (repositório centralizado).
- Registro em massa de usuários antivos através de arquivos CSV.
- Revisar as listas de usuários (tanto nativos como de AD), incluindo seus dados.
- Criar um usuário nativo inserindo seus dados.

Relatórios, dashboards e logs de auditoria

Relatórios e logs de auditoria são incluídos para controlar a operação do sistema. Além disso, existem APIs com informações para poder desenvolver dashboards..

Relatórios

• Acesso à solução.
• Criação, exclusão e modificação de usuários.
• Autenticações/acessos com falha.
• Redefinição e alterações de senhas.
• Número total de identidades.
• Identidades por seu status (ativo, inativo).
• Identidades por tipo (AD, soluções nativas).
• Tipo de MFA usado (SMS, e-mail, OTP).

2025 VU Inc. Todos os direitos reservados.

Dashboards (APIs)

- Número total de usuários.
- Quantidade de usuários por estado.
- Estado dos agentes.
- Número e porcentagem de MFA usado.
- Número de autenticações bem-sucedidas e com falha.
- Número de acessos com sucesso e com falha.
- Número e porcentagem de senhas redefinidas.
- Número de acesso a aplicações integradas.

Controle de acesso baseado em funções (RBAC)

O acesso aos aplicativos é feito com base nas funções do usuário. Cada aplicativo tem uma permissão de acesso que inclui o nome do aplicativo. Essa permissão pode ser incluída na definição de uma ou mais funções, para que os usuários com uma função apropriada possam entrar no aplicativo.

As funções de usuário podem ser associadas a grupos de AD. Assim, um membro de um grupo AD terá automaticamente todas as funções associadas a esse grupo. Essa associação é dinâmica, portanto, se o usuário sair do grupo, ele perderá suas funções. Além disso, se a associação de grupos e funções for alterada, os usuários poderão ganhar ou perder funções.

Controle de acesso baseado em atributos (ABAC)

O acesso aos aplicativos é baseado nos atributos do usuário. Durante o processo de login, incluindo SSO, se o usuário tiver fornecido uma senha correta e se o mecanismo de regras estiver ativo, as regras habilitadas devem ser validadas.

As regras do mecanismo serão configuradas para que retornem um dos dois códigos de ação possíveis: permitir ou negar acesso.

2025 VU Inc. Todos os direitos reservados.

Gerenciamento de autenticação multifator (MFA)

O sistema permite gerenciar a existência de múltiplos fatores de autenticação, tanto para aplicativos conectados com OIDC ou SAML quanto para clientes RADIUS.

No caso de aplicativos **OIDC ou SAML**, é possível configurar o processo de autenticação para cada aplicativo. O administrador pode escolher a política de autenticação, por exemplo: somente senha, somente TOTP, senha e TOTP, senha e segundo fator escolhido pelo usuário, entre outras variantes adicionais.

No caso de clientes **RADIUS**, é possível escolher o tipo de OTP de acordo com a função do usuário. Os usuários farão login com sua senha e o OTP configurado para suas funções. Também é possível dar acesso a um usuário que não esteja em nenhuma das funções configuradas para esse fim. Nesse caso, eles entrarão apenas com uma senha. Como os grupos de usuários AD podem ser vinculados a funções, esse recurso também pode funcionar com grupos AD.

Perfis de acesso

Os perfis de acesso permitem estabelecer políticas de autenticação e restrições de acesso para usuários e aplicações.

Cada usuário pode ter um ou mais perfis de acesso de acordo com suas funções, assim como as aplicações a que têm acesso. Portanto, é incorporado o conceito de perfil de acesso dinâmico, que calcula a combinação de perfis para permitir ou restringir o acesso dos usuários em cada caso, seja solicitando autenticação de duplo fator (2FA), reautenticação ou controle de acesso baseado em atributos.

Motor de regras

O motor de regras de Authentication Management é baseado na configuração de um conjunto de atributos para restringir o acesso aos usuários, que podem ser adaptados às necessidades de cada empresa ou organização.

As regras disponíveis para negação de acesso são:

- Endereços IP
- Dias da semana
- Intervalo de horas
- Países

As regras se aplicam por fuso horário, e pode ser configurada uma exceção para uma função específica. Por exemplo, para a função Administrador.

2025 VU Inc. Todos os direitos reservados.

Login sem senha: FIDO2

O FIDO2 é um padrão de autenticação global desenvolvido pela FIDO Alliance e baseado em criptografia de chave pública. O FIDO2 permite que os usuários usem seus próprios dispositivos (telefones, desktops, chaves de segurança USB, etc.) para realizar a autenticação de forma rápida e segura em vez de sua senha habitual.

Escopo do FIDO2 no Authentication Management:

- Configuração do fator FIDO2 e cadastro de autenticadores do portal de administração para usuários com função de Administrador.
- Cadastro de autoatendimento dos autenticadores de FIDO2 do portal do usuário.
- Possibilidade de usar um autenticador FIDO2 registrado como alternativa à senha no login do portal do usuário.
- Possibilidade de usar um autenticador FIDO2 registrado como alternativa à senha no módulo de Single Sign-On (SSO).

VU Access for Windows

O VU Access for Windows é um provedor de credenciais alternativo para o Microsoft Windows, que implementa o 2FA ao solicitar a entrada de um aplicativo móvel OTP (Microsoft Authenticator, VU App, entre outros) ao fazer login. Isso possibilita reforçar a segurança dos equipamentos pessoais e corporativos.

Na versão offline, os usuários não precisam estar conectados à Internet para se autenticar e fazer login no Windows. Esta versão permite que os usuários se registrem automaticamente por meio de um aplicativo instalado em seus PCs.

Características:

- Solicita nome de usuário, senha e OTP.
- Inclui aplicativo para configurar o TOTP no app móvel.
- Compatível com diferentes aplicativos mobile.
- Compatível com Windows 10 ou 11.
- Inclui o instalador do Windows.

Módulo Directory

O módulo Directory gerencia os dados (atributos) das identidades do Authentication Management, possibilitando o registro de múltiplos atributos do usuário no sistema.

A ativação deste módulo permite que os usuários armazenem e recuperem atributos personalizados. Na versão atual, os usuários nativos podem ser criados no Authentication Management com seus nomes pessoais.

2025 VU Inc. Todos os direitos reservados.

Integração com VU Identity Link

A integração com o VU Identity Link permite aos usuários autenticar sua identidade por meio de reconhecimento biométrico e verificação de documentos.

Isso garante que os usuários que estão tentando acessar o Authentication Management ou as aplicações gerenciadas pelo portal sejam realmente quem dizem ser. Além disso, essa integração ajuda a melhorar a qualidade dos dados, detectar ataques e proteger seu negócio.

Outras características

• Permite definir as políticas para criação de nomes de usuário e senhas:
  • Configurações de complexidade de senhas.
  • Histórico de senhas.
  • Lista de exclusão de senhas.

• Permite definir políticas de bloqueios automáticos de usuários.

• Permite definir políticas de desbloqueio automático de contraseñas y tokens de correio eletrônico e SMS após um número configurável de minutos.

• Suporta a integração com *hard tokens*.

• A comunicação entre as camadas de apresentação e o servidor do produto é feita por meio de uma conexão SSL/TLS.

• Os métodos disponíveis através da API permitem:
  • Habilitar e desabilitar usuários e tipos de fatores de autenticação.
  • Validar credenciais.
  • Remover usuários e tipos de fatores de autenticação da plataforma.
  • Modificar e atribuir a senha de um usuário na plataforma.
  • Adicionar grupos de Access Control Service.
  • Criar, registrar, validar, bloquear e desbloquear usuários.
  • Cancelar fatores de autenticação atribuídos aos usuários.
  • Fornecer códigos OTP atribuídos ao usuário no aplicativo móvel.
  • Validar o token de um usuário final.
  • Informar o estado de um usuário.

• Registro automático do fator OTP móvel para novos usuários do Active Directory ao registrá-los no Authentication Management.

• Notificações relacionadas à criação/recuperação de senhas podem incluir dados personalizados do usuário armazenados no módulo Directory.

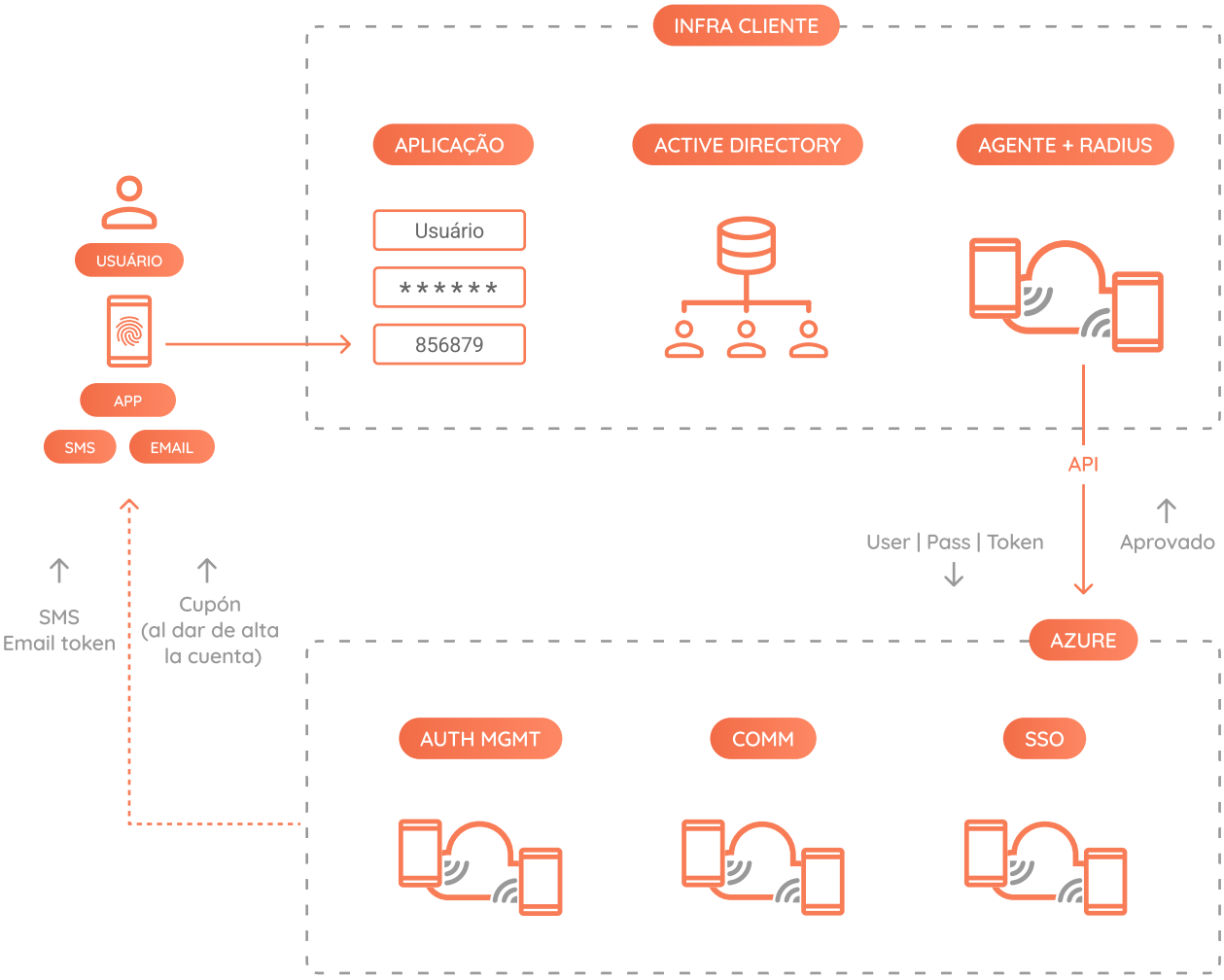
2025 VU Inc. Todos os direitos reservados.

Distribuição

O **Authentication Management** pode ser adquirido como licenciamento de software (on-premises) ou como software como serviço (SaaS).

Software como Serviço (SaaS)

Sua arquitetura cloud com um portal de administração multitenant e multicliente, permite o gerenciamento privado por diferentes negócios ou clientes internos. Ela está otimizada para Microsoft Azure, integrado com Azure DevOps, Azure Vault e Azure Monitor usando instâncias Dockerizadas.



2025 VU Inc. Todos os direitos reservados.

Agente: requisitos de software e hardware

O Agente é utilizado para conectar a infraestrutura do cliente (AD, terminador VPN) com a implantação na nuvem do Authentication Management. Ele é instalado em uma máquina virtual com sistema operacional Linux e tecnologia de contêineres Docker.

É um requisito que nessa máquina virtual o agente possa se comunicar com o AD e o servidor VPN em relação ao agente.

Componente de infraestrutura	Requisitos (*)	Entrega
Agente	Máquina Virtual Linux 2 core 4 GB de RAM 20 GB de espaço em disco Docker (versão 3.x)	Imagens Docker

(*) Para alta disponibilidade do agente, serão necessárias 2 máquinas virtuais e um balanceador de carga.

Monitoramento e alarmes

Todos os componentes são monitorados usando Azure Monitor, Azure Log Analytics e Azure Application Insights para manter as métricas de performance para cada componente envolvido e um rastreamento de logs para auditoria e troubleshooting tanto da infraestrutura como das instâncias do Authentication Management.

Alta disponibilidade

O serviço é gerenciado por Azure Kubernetes Service, com replicação em 3 áreas na região West Europe (Netherlands). A recuperação do serviço em outra região (em caso de interrupção do serviço na West Europe (Netherlands) será executada no prazo máximo de 30 minutos.

2025 VU Inc. Todos os direitos reservados.

Backups

Para todos os bancos de dados, os backups são realizados várias vezes por hora de forma incremental e sob políticas de retenção. Os backups são replicados em uma região alternativa à produtiva.

Atualização

A VU realizará atualizações corretivas e evolutivas de acordo com a disponibilidade e em modo hot-swapping do ambiente de pré-produção exclusivamente. As atualizações acontecem sob políticas incrementais com *rollback* em caso de eventuais falhas.

Uptime

- 99% de tempo de atividade anual fora do horário de manutenção: 00:00 às 22:00, GMT-3.
- 98% de tempo de atividade anual dentro do horário de manutenção: 22:00 às 00:00, GMT-3.

Haverá um portão de manutenção das 22h00 às 12h00, horário argentino, enquanto das 12h00 às 22h00 não serão realizadas atividades de manutenção. No caso da janela de manutenção, o SLA será de 98% de uptime anual, enquanto o período de produção ou SLA será de 99% de uptime.

Tempo de recuperação diante da descontinuação do serviço

O serviço será configurado para oferecer um Recovery Time Objective de 3 horas e Recovery Point Objective de 1 hora.

Tempo de recuperação diante da degradação do serviço

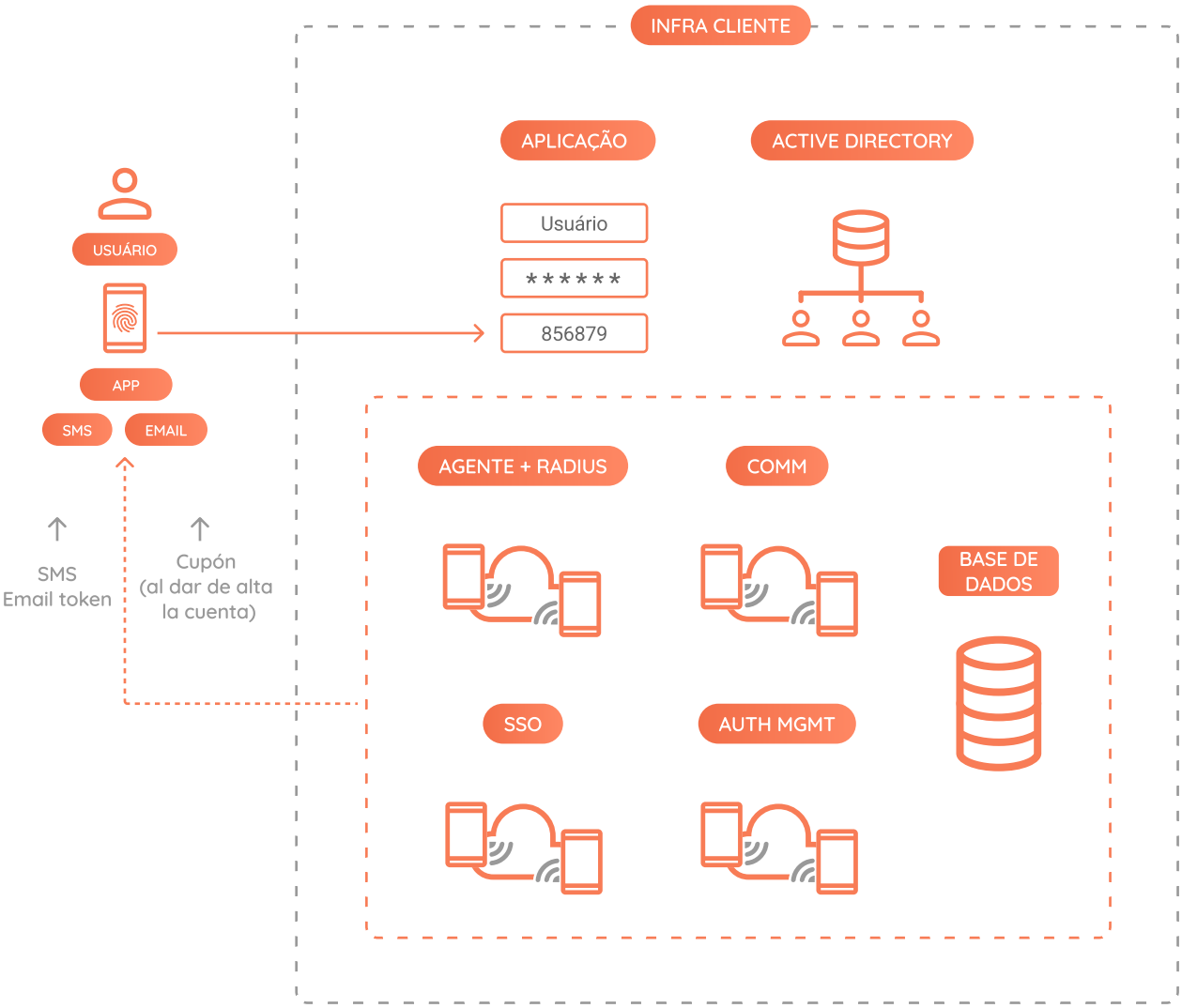
A infraestrutura é montada sobre serviços elásticos, estendendo suas capacidades desta quando os limites configurados são ultrapassados, resolvendo a possível degradação do serviço.

O processo de ajuste das instâncias é automático e para isso é estabelecido em tempos máximos de 15 minutos.

2025 VU Inc. Todos os direitos reservados.

Licenciamento de software (on-premises)

Authentication Management on-premises permite implementar os componentes single tenant nos próprios servidores do cliente.



2025 VU Inc. Todos os direitos reservados.

Requisitos de hardware e software

A solução Authentication Management é composta por 4 componentes, que são implantados em uma arquitetura de microserviços executando no Docker ou Kubernetes.

Esses serviços são:

- Servidor de autenticação.
- Módulo single sign-on (IdP).
- Servidor de comunicações.
- Agente.

— Requisitos de hardware

A máquina virtual mínima deve ser:

vCPU	Memória (Gb)	Armazenamento do sistema (Gb)
2	8	60

Com base nisso, é possível dimensionar verticalmente, adicionando mais CPUs e memória, ou horizontalmente (recomendado) adicionando réplicas. Para esse último cenário, é recomendável a implementação com Kubernetes. Um balanceador de carga deve ser fornecido.

Com o nó base, é possível gerenciar até 8 transações por segundo.

Usuários (referência)	Transações por segundo	Node / VM				DB	
		Cores	RAM	Réplicas	Armazenamento do sistema	Armazenamento mensal	Armazenamento anual
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

2025 VU Inc. Todos os direitos reservados.

— Requisitos de software

Como toda a aplicação é baseada em arquitetura de contêineres, são necessários apenas o sistema operacional e as ferramentas do Docker.

Sistema Operacional	Ferramentas de contêineres	Banco de dados
Linux Centos / Ubuntu / Red Hat	Esquema 1: Docker Engine (v. 19+) (*) com Docker Compose (v. 3+) (*) Esquema 2: Kubernetes (v. 1.24+)	SQL Server 2019 Outros esquemas de bancos de dados: consultar

* A VU fornecerá suporte para a instalação e configuração do Docker e Docker Compose.

— Alta disponibilidade

- No esquema Docker + Docker Compose: duplicar a quantidade de máquinas virtuais.
- Nas implementações com Kubernetes: trabalhar com n+1 nós ou conforme a política do cliente.
- Banco de dados em esquema de alta disponibilidade com redundância (ativo - ativo ou ativo - passivo).

— Componentes do cliente

A VU oferece um SDK que pode ser integrado em aplicativos móveis Android e iOS e que permite a geração do TOTP.

Sistema Operacional	Tecnologia	Entrega
Android	Java	SDK + Exemplo
iOS	Swift	SDK + Exemplo
Híbrido	Javascript	SDK + Exemplo

2025 VU Inc. Todos os direitos reservados.

Fim do suporte estendido (EOS) e fim de vida (EOL)

	Suporte completo	Manutenção	Apenas suporte	Sem suporte
Novas funcionalidades podem ser esperadas	✓	No	No	No
Correção de erros	✓	✓	No	No
Atendimento ao cliente	✓	✓	✓	No
Anos desde a data de lançamento	2	3	4	-

Versão	Data de lançamento	Última entrega ao cliente	Novas funcionalidades até	Correções até	Último dia de suporte (LDOS)	Sem suporte desde
6.x	1/4/2022	1/4/2025	1/4/2025	1/4/2026	1/4/2027	2/4/2027

Contato

Se você precisar de mais informações ou quiser agendar uma demonstração desta solução, escreva para: sales@vusecurity.com

Outros produtos da VU

Fraud & AML | Fraud Analysis | Device Finger Print

Onboarding Management | ID | Face | Voice | Touch

CIAM

2025 VU Inc. Todos os direitos reservados.

Sobre a VU

A VU é uma empresa global de cibersegurança, especializada em proteção da identidade e prevenção de fraude, que desenvolve soluções modulares, fáceis de integrar e adaptáveis tanto à esfera corporativa quanto governamental.

Para isso, utiliza tecnologias inovadoras baseadas na combinação de controles tradicionais de cibersegurança, biometria, geolocalização, inteligência artificial, machine learning, reconhecimento de documentação e análise do comportamento do usuário.

Mais de 350 milhões de pessoas em todo o mundo e mais de 130 clientes em 30 países da América Latina, Europa e Estados Unidos utilizam a tecnologia VU para digitalizar seus negócios e aumentar o nível de operações, reduzindo os riscos de ataques e perda de informações.

Suas alianças estratégicas com a Microsoft, Telefónica, IBM, BGH, Intel, Cisco e Accenture, entre outras empresas, ajudam a VU a cumprir sua missão: criar experiências seguras e sem atritos que melhorem a qualidade de vida de cidadãos e organizações.

vusecurity.com

2025 VU Inc. Todos os direitos reservados.