

企业级双因素认证（E2FA）专为大企业提供

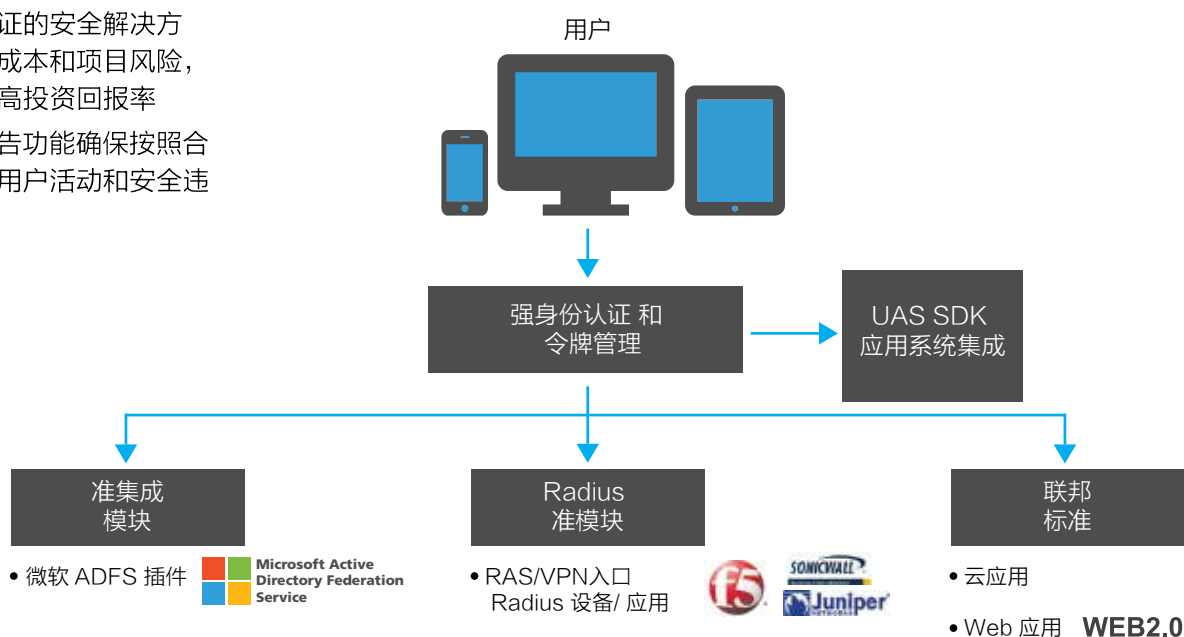
主要优点

- 通过AccessMatrix™ UAS灵活集成架构和细粒度安全策略可实现强 OTP 身份认证解决方案的快速部署
- 通过带外 OOB 身份认证增强安全性，以缓解钓鱼软件的攻击
- 利用 HSM 硬件提供预先的 OTP 生成和对比选项
- 通过部署已验证的安全解决方案，降低实施成本和项目风险，最大限度地提高投资回报率
- 强大的审计报告功能确保按照合规性要求报告用户活动和安全违规信息

企业应用系统的多因素OTP身份验证和令牌管理解决方案

为大企业应用系统和 Radius 设备提供统一的身份认证，使企业能够快速部署 OTP 令牌，满足强认证要求。带外 OOB 认证方式，支持各种短信网关、邮件网关，显著减少部署工作，提高访问企业资源的安全性。

UAS 提供一个统一的令牌管理功能，提供产品级灵活的强身份认证和授权机制；并基于 AccessMatrix 集成安全基础架构，UAS 为用户提供管理、认证、授权和审计（4A）服务，以满足安全和合规性的要求。



主流应用和网络设备的准集成

支持2FA的无缝集成:

- 企业应用和系统: Microsoft ADFS Plugin, Citrix, VMware 等。
- 网络设备: Juniper, F5, Checkpoint, Palo Alto, NetScaler, Huawei, SANGFOR, Cisco 等。
- 云/SaaS 应用: Google Apps, IdeaScale, Salesforce, WebEx, Zendesk 等。

灵活的集成选项

使用开放 API 和标准行业协议等多种集成方法

特点

- 灵活的 OTP 策略
- 审计跟踪
- 多种交付机制
- 灵活集成 SDK
- 内置 RADIUS 服务器
- 无缝集成

系统要求

- 服务器 OS: MS Windows Server 2012/ 2016 及 Red Hat Enterprise Linux 7
- 应用服务器: Oracle WebLogic, IBM WebSphere, Apache Tomcat 及 JBoss Web Server
- Java 运行环境: JRE 1.8 及 JRE 11 LTS
- 数据库支持: MS SQL Server、Oracle RDBMS 和 Oracle MySQL
- 外部用户存储: AD目录、LDAP v3 兼容目录 和 JDBC 兼容数据库
- FIPS 认证的 HSM

未来的令牌解决方案

- AccessMatrix™ UAS支持多品牌OTP令牌的嵌入式认证，包括 One-Span (Vasco)、Thales-Gemalto 和基于 OATH 的厂商（如 Google 认证软件令牌、OneSpan (Vasco)、V-key 和安讯奔YESsafe令牌）。
- 成熟的 E2FA 解决方案，可以减少集成的复杂性，缩短为安全敏感程序部署的时间，并确保安全的远程访问。

使用多因素认证来加强对用户身份的保护

支持基于 AccessMatrix™ UAS 统一身份认证体系的认证机制。如：数字证书、智能卡、生物识别等。其松耦合的特性使业务系统在更换认证方式时可通过 UAS 平台页面配置实现，无需对应用程序做大量改造。

使用可扩展的安全基础架构来提升程序的安全性

AccessMatrix 采用 JAVA 技术、开放的架构、灵活的框架和最新的技术构建而成，提供单点登录和访问控制服务，以满足客户目前和未来的需求。

灵活的管理和授权

- 已获得专利的 AccessMatrix 模块，采用动态分级授权的架构设计，允许企业为不同层级的安全管理员分发不同权限策略。使得企业在保证效率的前提下同样具有较高的权限控制。
- 针对外部用户/合作伙伴，系统允许其通过他们自己的安全管理员来管理 ID 和用户权限，减少企业对此类用户繁琐的处理过程，提高生产力。除此之外，AccessMatrix 进一步简化完善用户管理，通过与现有用户存储（如 LDAP 或 Microsoft AD 目录）集成来实现。

完整的令牌生命周期管理

集成型解决方案，提供管理整个令牌生命周期的功能：

- 核发、交付、启用、令牌丢失、不同步和逾时重置
- 定制化的用户界面，方便服务台工作人员使用令牌管理功能
- 详细的审计跟踪信息和灵活的报告
- 提供令牌管理的外部 API 接入能力

多认证和交易授权选项

- 一次性挑战密码
- 挑战应答 OTP
- 关键交易再认证
- 二层静态密码/ 组合认证
- 安全的场景认证