Identity Security

wallix Sovereign Identity Access

Unify, Secure and Simplify Workforce Access to Applications

Securing access across cloud, on-premises, and hybrid environments requires more than strong authentication. Organisations must protect access without adding friction or complexity, **while retaining control over their identities, authentication infrastructure, and sensitive data.** This makes digital sovereignty, where and how identity services are operated, and who organisations depend on, an essential part of a resilient security strategy. **Sovereign Identity Access** simplifies secure access to corporate resources, helping organisations strengthen security, reduce friction, preserve **digital sovereignty**, and keep users productive wherever they work.

Features & Capabilities

User Provisioning & Lifecycle Management

- User onboarding and access management across the employee lifecycle.
- SCIM-based automated provisioning and deprovisioning.
- Delegated administration with centralised control.
- Self-service access to available applications.
- Monitoring and reporting for compliance and investigations.

Multi-Factor Authentication (MFA)+

- Protect against credential theft with MFA.
- Enable phishing-resistant authentication.
- Define authentication requirements for each use case and application.
- Extend MFA to privileged access through WALLIX Access Manager and PAM.

Identity Federation

- Federate identities across cloud and on-premises environments.
- Centralise application access via SAML and OpenID Connect.
- Integrate with Entra ID, Active Directory, LDAP, and Google Workspace for sovereign and phased modernisation.

Single Sign-On (SSO)

- Use one set of credentials for centralised access.
- Securely access applications on-site or in the cloud.
- Connect to pre-integrated, legacy, SaaS, and custom applications.
- Federate identities across on-premises and cloud directories.

wallix

Technical Characteristics

> **Silent Authentication:**
- Integrated Windows authentication (Kerberos)
- X509 authentication

> **Other authentication methods:**
- Password (Active Directory, LDAP, WALLIX Sovereign Identity Access)

> **Multi-Factor Authentication Methods (MFA):**
- Phishing-resistant: FIDO2/WebAuthn passkeys, U2F/FIDO2 security keys, X.509 certificates
- Additional methods: WALLIX Authenticator (TOTP + push), third-party TOTP, OTP by email/SMS

> **Single Sign-On for Applications:**
- SAML, OpenID Connect, OAuth2.0

> **Other supported protocols:**
- LDAP & RADIUS through connectors

> **Native Integration of Directories:**
- Active Directory, LDAP, Microsoft Entra ID, Google Workspace Directory

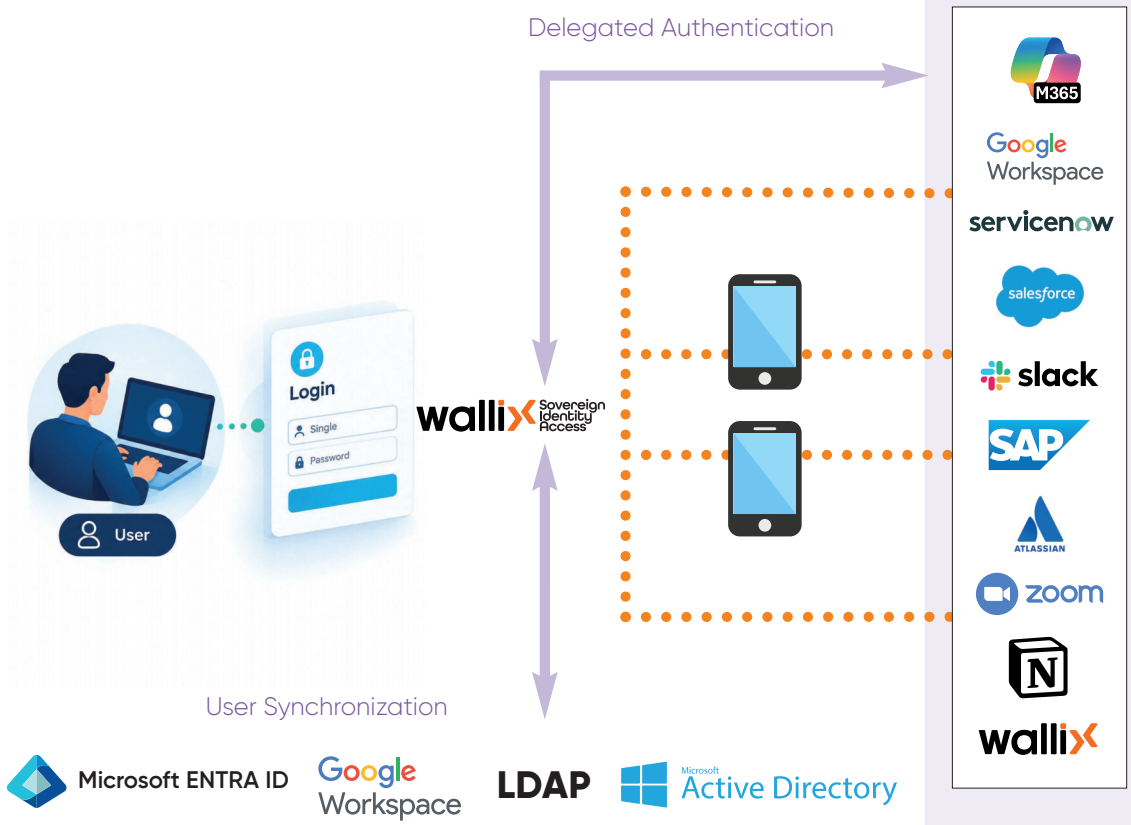
> **Self-Service Portal for Users:**
- MFA method enrolment
- Self-service password reset (SSPR), also available for Active Directory

> **Applications**
- Pre-integrated models: WALLIX PAM, Office 365, Google Workspace, Salesforce, Dropbox, WordPress...
- Generic models compatible with all industry-standard applications

> **Traceability:**
- Complete logging and auditability of access and authorisations

> **Extension:**
- APIs and scripts for integrating the platform with customer environments

How it Works



Choose Your deployment

SaaS	On-Premises
Rapid deployment and automatic updates	Complete control of identity data and authentication
Reduced infrastructure and operational overhead	Air-gapped & disconnected environments
Secure identity services for distributed users and cloud applications	Customer-controlled infrastructure and data
Hosted in France, independent of third-party infrastructure	Operated entirely within your infrastructure

About WALLIX

WALLIX protects identities and access to IT infrastructure, applications, and data. Specialising in Privileged Access Management, WALLIX solutions ensure compliance with the latest IT security standards and protect against cyberattacks, data theft and leaks resulting from stolen credentials and elevated privileges.