AIRLOCK®

SECURE ACCESS HUB

FACTSHEET

Access for all users. Frictionless.

Airlock IAM

www.airlock.com

Airlock IAM is typically combined with Airlock Gateway, a component to protect web application and APIs (WAAP), in the Airlock Secure Access Hub. Airlock IAM's role is to manage and authenticate users and to forward the relevant identity information to the desired application in an appropriate form.

Customer IAM (cIAM)

Airlock IAM manages users who want to access applications, APIs, and microservices from the outside and is scalable for high numbers of users. Moreover, the cIAM solution offers a seamless user experience with optimized and integrated user interfaces for onboarding and self-services. The handling of social identities (BYOI) and high flexibility in the authentication process are key advantages of Airlock IAM.

Strong authentication with a broad range of factors

To prevent the login process from suffering the weaknesses of a single authentication factor, strong authentication is typically used with a second factor (also known as 2FA or MFA). Airlock offers fully integrated, modern, and highly user-friendly strong authentication with Airlock 2FA. This makes passwordless access easy and secure to configure.

Airlock IAM supports a wide range of other authentication factors, which can be combined flexibly. For instance: FIDO2/WebAuthn, mTAN (SMS), email OTP, OATH, matrix cards, client certificates, OneSpan Cronto, and Digipass OTP. Besides authentication factors, administration functions as well as self-services for end users are also available.

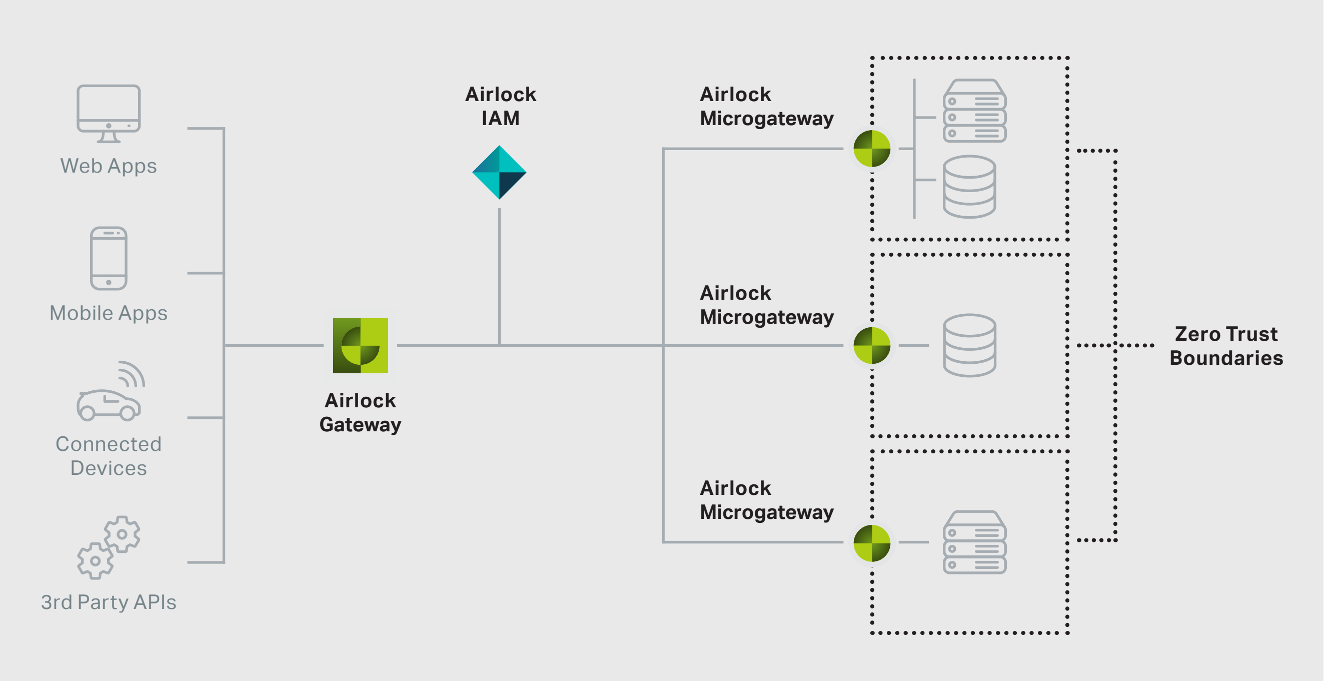
Adaptive authentication

Airlock IAM dynamically controls user access in various ways, offering the ideal balance between security and user-friendliness for all needs. In particular, the current access situation – e.g. from the workplace, home or on the move – and the user history can be taken into account. Included among the supported concepts are:

- **Continuous adaptive trust (CAT) in combination with Airlock Gateway**
- **RBAC/ABAC (role/attribute-based access control)**
- **Risk-based authentication**
- **Re-authentication and time-out functions for individual roles**
- **Implementation of complex access policies with rules and logical operators**

Single sign-on (SSO)

The Secure Access Hub decouples authentication from applications and therefore acts as a smart identity switch. Depending on the access target, the identity of the authenticated user can be represented differently. This enables transparent single sign-on which combines high security with high user acceptance.



docker kubernetes aws Google Cloud Azure OPENSHIFT

Airlock IAM supports various SSO and federation standards such as OpenID Connect, OAuth 2, SAML 2.0, and Kerberos. It is also able to propagate authentication information to target applications in simple HTTP headers, cookies or as part of the URL. Plug-ins can easily be written for integration in legacy systems.

Social registration and BYOI

Users want to register and log in quickly and conveniently. Reusing existing identities reduces the number of required passwords. When users provide their identities for access from outside, this is called “Bring Your Own Identity” (BYOI). Alternatives to handling a jumble of passwords include standards such as OAuth 2.0 and OpenID Connect 1.0. These allow the reuse of user identities and provide the user with control over their usage. If you prefer not to rely completely on an external identity provider (e.g. Facebook), Airlock IAM can augment these identities with a second factor to enable strong authentication.

Comprehensive user self-services

Setting up user accounts and login processes can result in lots of questions on the part of users. Targeted user guidance with an optimized user experience is therefore extremely important to prevent the helpdesk from being overwhelmed with support requests. Airlock IAM offers a wide range of optimized and integrated workflows for login, onboarding, and other self-services. These include kiosk and portal functions for managing one's own data, independent registration, as well as the administration of corresponding accounts and authentication factors.

Deployment

- **Docker image**
- **Self-contained application for Linux**

Functions

- **User authentication**
  - Password
  - Passwordless
  - Airlock 2FA (push, QR code, OTP, HW token)
  - FIDO / WebAuthn / Passkeys
  - OATH OTP, MTAN (SMS), email OTP
  - OneSpan Cronto and Digipass OTP
  - X.509 client certificates
  - Adaptive and risk-based
  - Workflow-based
  - "Remember Me" feature
  - RADIUS server
- **Request authentication**
  - Authentication of REST calls
  - JWT, OAuth, Basic Auth, client certificates, Kerberos, SSO tickets
- **User directories: Databases, LDAP, MSAD**
- **User, token and role management incl. helpdesk tool**
- **User self-services**
  - Password reset
  - Registration and management of authentication factors (in particular 2nd factors)
  - Management of sessions and logged-in browsers/devices
  - Kiosk and portal functions for own user data
  - Various other self-services
- **Additional functions:**
  - Single sign-on (SSO): OIDC, OAuth, SAML, cookies, HTTP headers, SSO tickets, JWT
  - REST APIs for all components (Loginapp, Adminapp, transaction approval)
  - Identity provider for OIDC, OAuth, SAML
  - Service provider for OIDC, OAuth, SAML
  - Social login and social registration
  - Multi-tenant capable
  - Highly scalable
  - Banking-level security
  - Individually extensible
- **Adminapp**
  - User management
  - Management and assignment of authentication tokens
  - Management of administrators and technical clients
  - Configuration management and configuration editor
  - Creation of authentication or self-service flows without programming
  - Flexible workflows with large library of integrated steps (no code)
  - Expansion with custom steps (low code)
  - Incremental changes with real-time feedback
  - Visualization of complex processes as a flow chart
  - Log viewer
  - Maintenance messages