

About Mavericks Identity Orchestrator™

Identity Orchestrator™ is a lightweight service deployed in the cloud or on-premises to orchestrate distributed identity systems. Identity Orchestrator™ connects to any identity system, transparently migrates users and credentials, replicates and synchronizes policies and configurations, and abstracts authentication and session management. Use Identity Orchestrator to integrate applications with any identity system without rewrites and with no impact on the user experience.

Problems Identity Orchestrator™ solves

Fragmentation caused by manually creating and maintaining multiple identity systems in a hybrid, multi-cloud enterprise.

Inconsistency of identities, policies, and configurations that occur as identity systems proliferate.

Lock-in that results from tightly integrating applications with legacy identity systems, and especially the complexity, added time, and manual efforts of migration to modern identity systems.

High costs that are inherent to keeping the lights on fragile deployments of legacy identity systems.

What you get

Break Lock-in: A lightweight software solution that breaks lock-in caused by heavyweight legacy identity systems.

Distributed Identity Management: Connected, distributed identity systems are cheaper to run and easier to maintain.

Dead Simple Integration: Integrate legacy applications with modernized identity systems, make apps standards-based, MFA and passwordless enabled, and zero-trust ready with no rewrites.

Features

Connects Distributed Identity Systems

Identity Orchestrator uses pre-built, Zero Code connectors to integrate with the proprietary APIs typical of legacy identity systems and to connect with modern cloud identity systems using standards such as OAuth, OpenID Connect, SCIM, and SAML as well as each cloud's native APIs.

Orchestrates Distributed Identity Management

Identity Orchestrator uses Workflows and Actions to orchestrate the complex flows of a distributed identity system using simple, declarative configuration.

Features continued...

Migrates Identity Data

Identity Orchestrator takes a unique network-based approach to incrementally migrate users and credentials from legacy identity systems such as Broadcom (CA) SiteMinder and Oracle Access Manager. Data flows in real-time to avoid the pitfalls of waterfall-style bulk migrations.

Replicates Identity Data

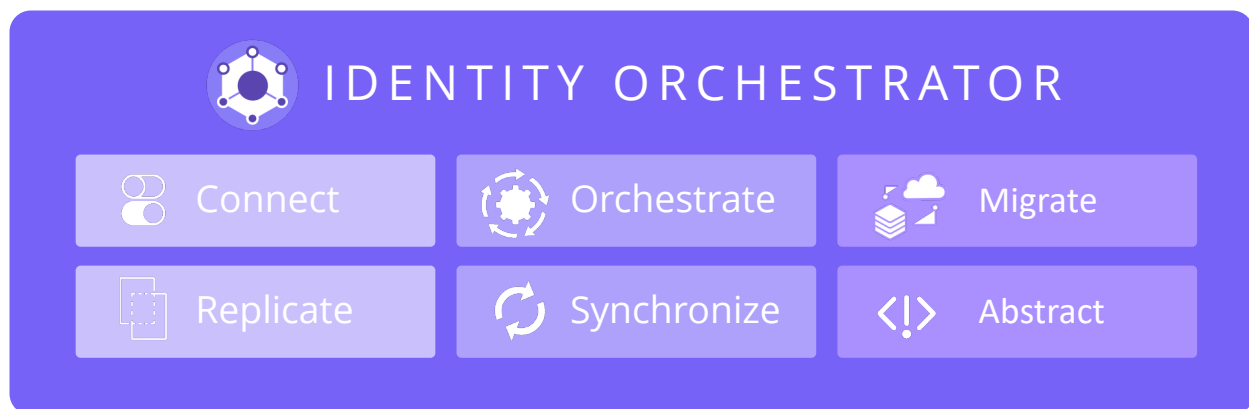
Identity Orchestrator automatically replicates identities, policies, and configurations from old to new, simplifying management and ensuring that each of your distributed identity systems has a common baseline of identity data.

Synchronizes Identity Data

Identity Orchestrator automatically keeps identity data in-sync across your distributed identity infrastructure, making sure changes are reflected in all of your source and target identity systems.

Abstracts Authentication and Session

Identity Orchestrator abstracts how different identity systems perform authentication and represent user sessions to apps, making it possible to create a proprietary session cookie from a standards-based session token without changing the user login experience.



Benefits

More Effective Identity

Resolve fragmentation across distributed and proliferated identity systems, increasing and giving you confidence that access controls, security, and compliance are accurately enforced.

Agile Identity Infrastructure

Increase choice and agility by integrating apps with your identity fabric, allowing you to transition apps across clouds and identity systems without rewrites and breaking the lock-in of centralized legacy identity systems.

Benefits continued...

Improve Security

Add important security capabilities like MFA, passwordless, and threat intelligence to apps without rewriting them.

Reduce Identity Management Costs

Retire expensive, outdated identity products, add automation and spend less on human resources performing manual tasks, and onboard new cloud identity services quickly and efficiently.

Migrate Faster

Reduce migration project timelines by 85%, avoid expensive application rewrites, and save millions of dollars in hard costs.

Single Pane of Glass

Identity Orchestrator gives unprecedented visibility into your distributed identity infrastructure so that you can have more control.

Zero Touch Deployment

Identity Orchestrator employs a Zero Touch, Zero Code, Zero Trust deployment model, adding critical new capabilities to distributed identity infrastructure with no impact on existing identity systems or applications.

How Identity Orchestrator™ works

- Deploy Identity Orchestrator™ onto your network.
- Connect identity systems to Identity Orchestrator™ using Zero Code connectors.
- Route identity system traffic through Identity Orchestrator™.
- Configure Workflows and automatically migrate identities, policies, and configurations, move authentication from proprietary and legacy to standards-based, and abstract sessions.
- Add Zero Touch integrations with 3rd party authorization engines, threat intelligence providers, and multi-factor authentication.

```
workflows:
- name: OAM Migration to Okta=
- name: SiteMinder to Okta Migration
  endpoint: /migrate-sm-okta
  actions:
  - connector: siteminder
    method: login
  - connector: have-i-been-pwned
    method: checkPassword
  onSuccess:
    operator: background
    actions:
    - connector: sm-ldap
      method: getprofile
    - connector: employee-database
      method: getprofile
    - connector: okta
      method: getprofile
  onFail:
    actions:
    - connector: okta
      method: createuser
- name: SiteMinder Session Abstraction
  endpoint: /abstract-session-sm
  actions:
  - connector: okta-sm
    method: login
  - connector: policy-extender
    method: authorize
  - connector: siteminder
    method: emulate
```

Workflows orchestrate the complex integrations of distributed identity systems