WSO2CON2024

WSO2's IAM Vision: Identity-Led Digital Transformation

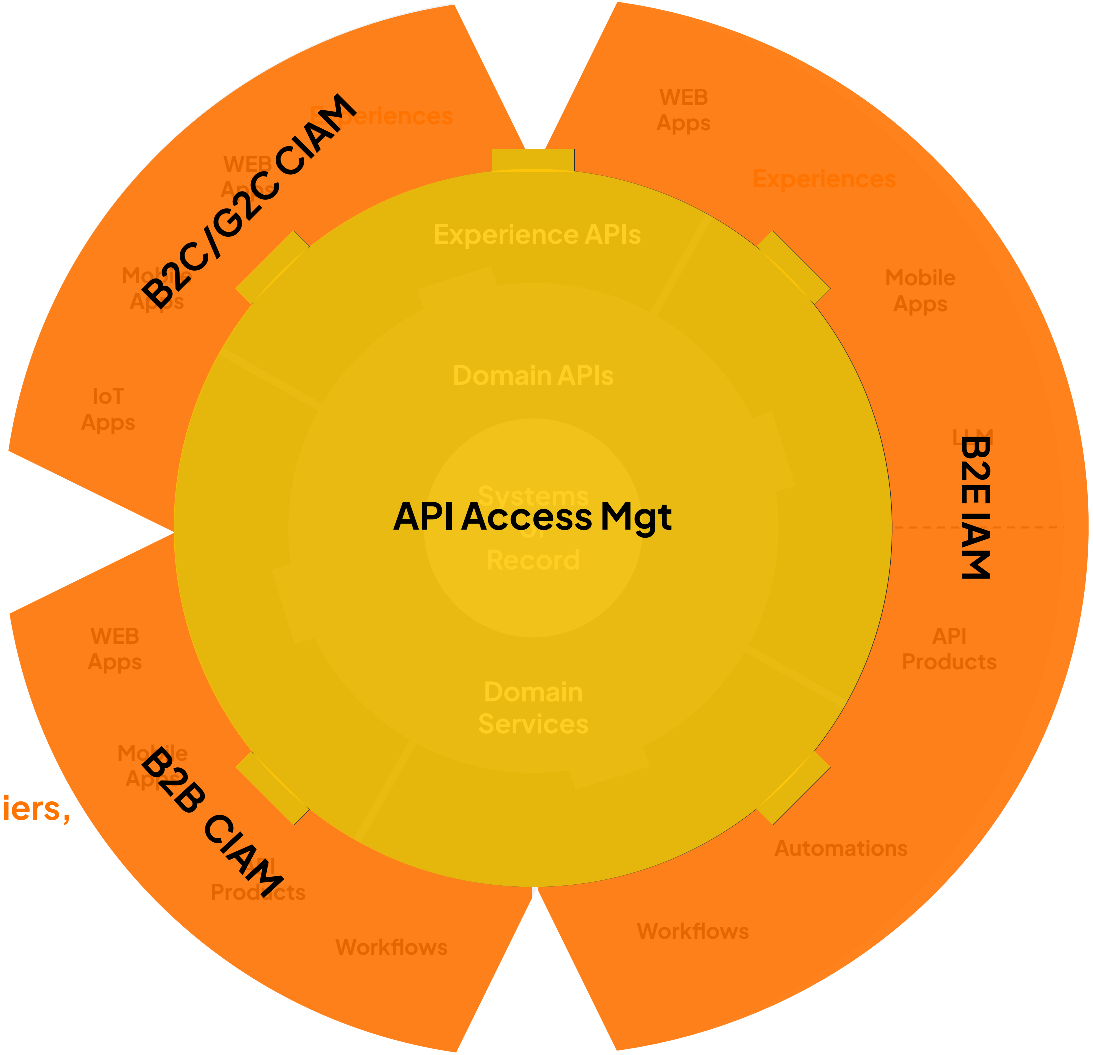
Geethika Cooray
Vice President & General Mgr - IAM
WSO2

Digital Transformation…

The shift to Identity– Led digital

External Digital Experiences for **Consumers/ Citizens**

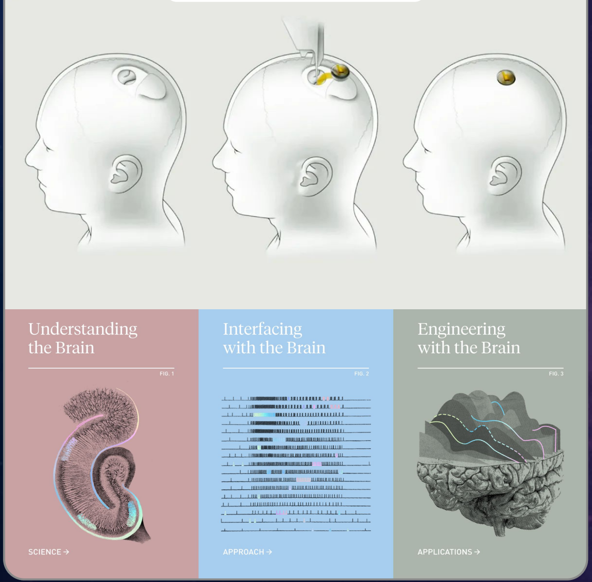
External Digital Experiences for **Enterprise Customers, Partners, Suppliers, API buyers**



Internal Digital Experiences for **Employees**

Need to reimagine Access Management…

Neuralink



Understanding the Brain

FIG. 1

SCIENCE →

Interfacing with the Brain

FIG. 2

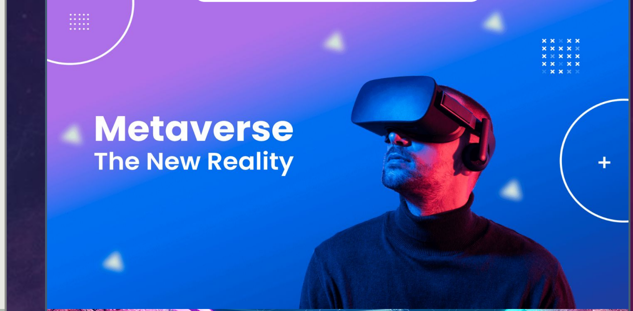
APPROACH →

Engineering with the Brain

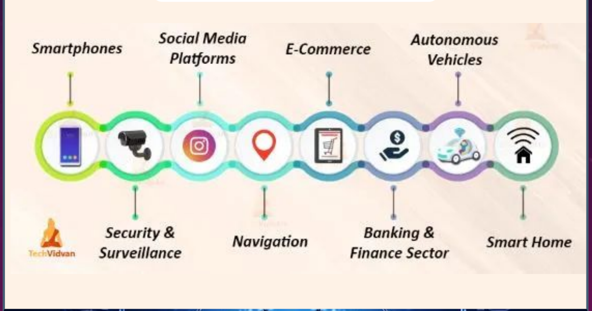
FIG. 3

APPLICATIONS →

Metaverse



AI



Smartphones

Social Media Platforms

E-Commerce

Autonomous Vehicles

Security & Surveillance

Navigation

Banking & Finance Sector

Smart Home

Identity-led Digital Transformation…

Benefits of Identity-led Digital Transformation

Access Management

Customer IAM

B2C/G2C

- Self-service and social-login
- Digital IDV, Progressive profiling, Consent Mgt,
- Passworless, Adaptive MFA
- Seamless Omni-Channel & personalized Experiences

Increased conversion & retention, loyalty & revenue

B2B

- Organization Mgt, Delegated Administration, user roles/entitlements
- Faster and easier customer/partner onboarding
- Friction-less and Improved end-user experience

Reduces overheads, increases time to market and revenue potential

Workforce IAM

B2E

- SSO, MFA, BYOID, Passkeys, etc.
- Reduced friction at login, resulting in improved security posture

Improves employee productivity and overall employee sentiment

API Access Mgt

APIs

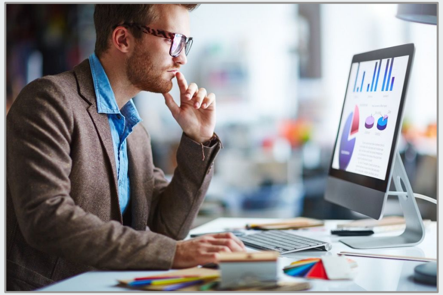
- OAuth 2.0/OIDC compliance
- Consent-, role- and context-based authorization

Improves overall security posture and reduces risk

All Users Deserve Seamless and Secure Digital Experiences

Identity and Access Management

is fundamental to ensuring a **secure**, **frictionless** experience for consumers, business partners or employees.



Multiple Deployment Options to Support Any IT Strategy

WSO2 Identity Server

The Leading Open Source IAM

WSO2 Identity Server is a powerful, modern identity and access management solution for your on-premises or cloud environment

ASGARDEO

Multi-tenant SaaS IAM

Asgardeo is a developer-focused, multi-tenant IDaaS solution that provides seamless, secure authentication and user management

WSO2 Private Identity Cloud

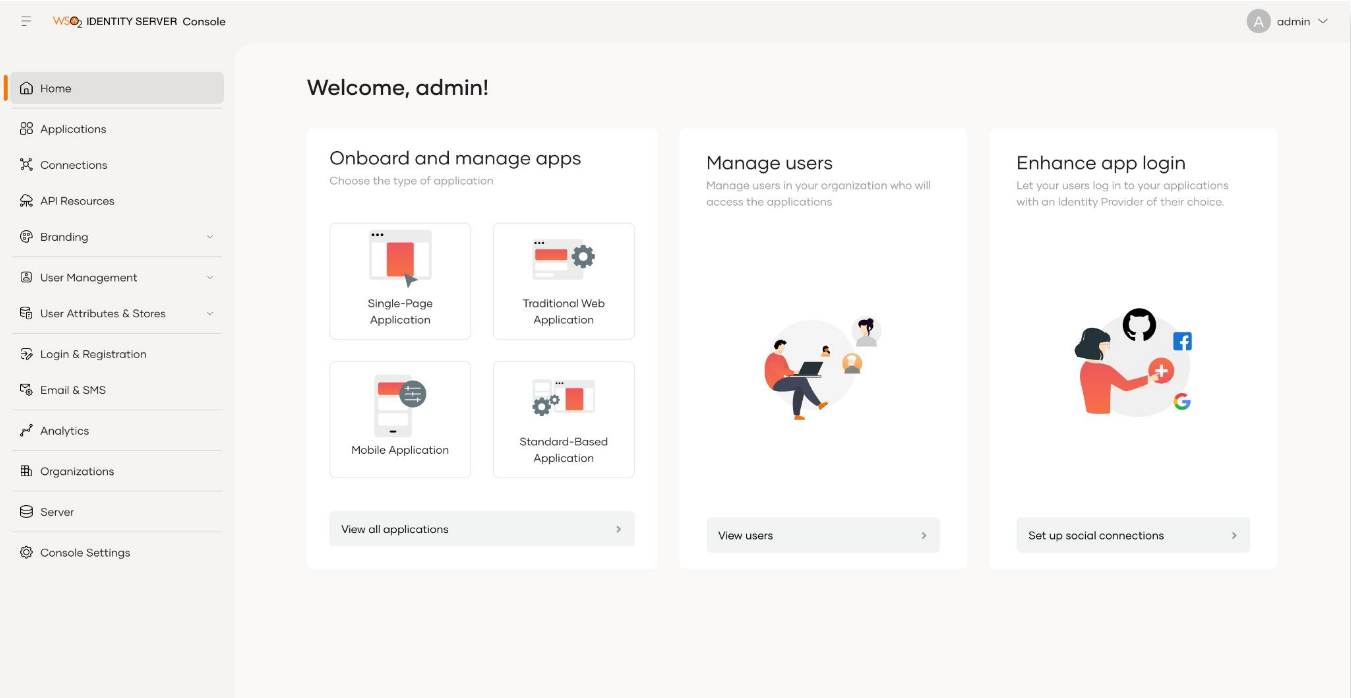
Single-tenant SaaS IAM

Private Identity Cloud is a single-tenant cloud identity solution, fully managed and maintained by WSO2

Latest improvements…

Optimized Developer Experience

Improved UI/UX



WSO2 IDENTITY SERVER Console

A admin

- Home
- Applications
- Connections
- API Resources
- Branding
- User Management
- User Attributes & Stores
- Login & Registration
- Email & SMS
- Analytics
- Organizations
- Server
- Console Settings

Welcome, admin!

Onboard and manage apps

Choose the type of application

- Single-Page Application
- Traditional Web Application
- Mobile Application
- Standard-Based Application

View all applications ›

Manage users

Manage users in your organization who will access the applications

View users ›

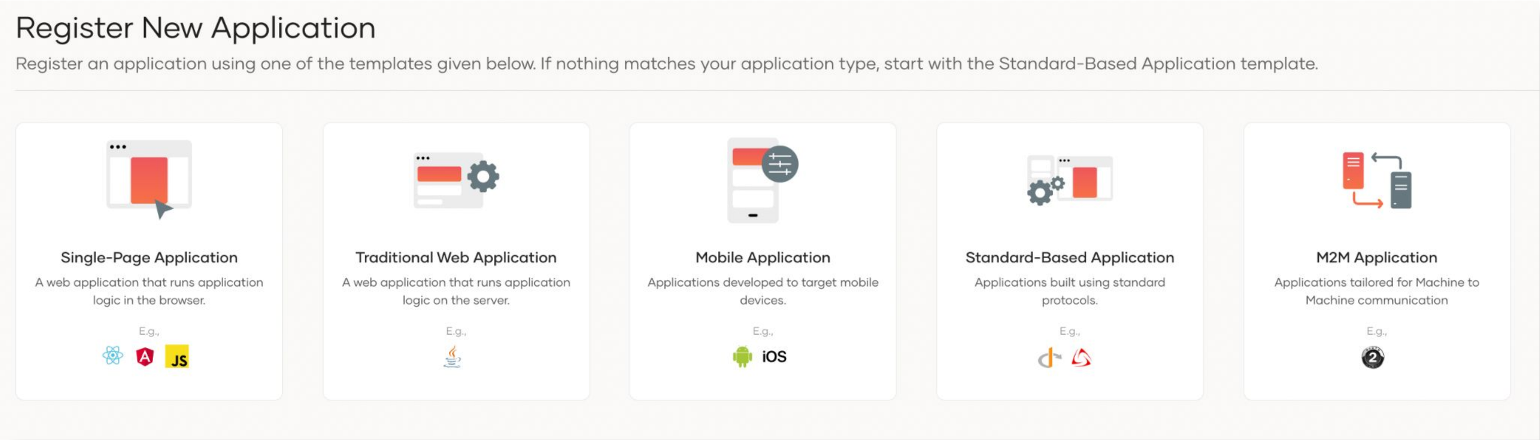
Enhance app login

Let your users log in to your applications with an Identity Provider of their choice.

Set up social connections ›

Optimized Developer Experience

Out-of-the-box Application Templates



Register New Application

Register an application using one of the templates given below. If nothing matches your application type, start with the Standard-Based Application template.

Single-Page Application

A web application that runs application logic in the browser.

E.g.,

Traditional Web Application

A web application that runs application logic on the server.

E.g.,

Mobile Application

Applications developed to target mobile devices.

E.g.,

Standard-Based Application

Applications built using standard protocols.

E.g.,

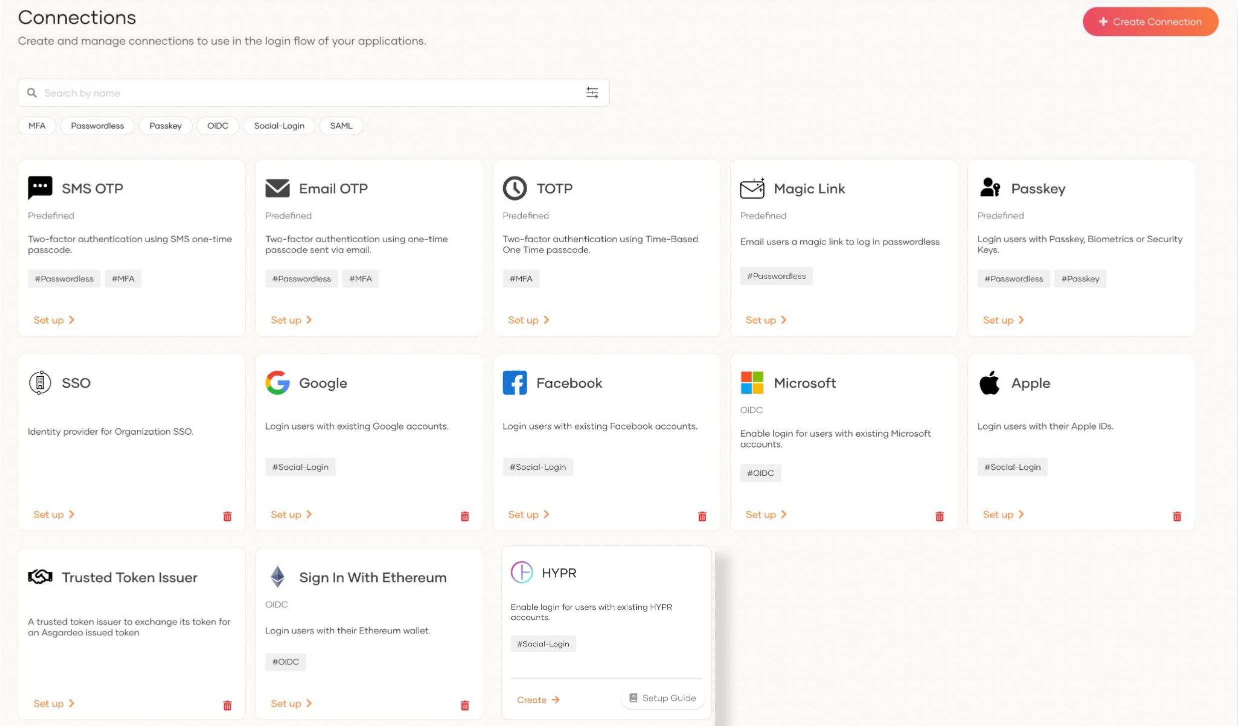
M2M Application

Applications tailored for Machine to Machine communication

E.g.,

Optimized Developer Experience

More authentication methods to choose from



Connections

Create and manage connections to use in the login flow of your applications.

SMS OTP
Predefined
Two-factor authentication using SMS one-time passcode.
#Passwordless #MFA
Set up >

Email OTP
Predefined
Two-factor authentication using one-time passcode sent via email.
#Passwordless #MFA
Set up >

TOTP
Predefined
Two-factor authentication using Time-Based One Time passcode.
#MFA
Set up >

Magic Link
Predefined
Email users a magic link to log in passwordless
#Passwordless
Set up >

Passkey
Predefined
Login users with Passkey, Biometrics or Security Keys.
#Passwordless #Passkey
Set up >

SSO
Identity provider for Organization SSO.
Set up >

Google
Login users with existing Google accounts.
#Social-Login
Set up >

Facebook
Login users with existing Facebook accounts.
#Social-Login
Set up >

Microsoft
OIDC
Enable login for users with existing Microsoft accounts.
#OIDC
Set up >

Apple
Login users with their Apple IDs.
#Social-Login
Set up >

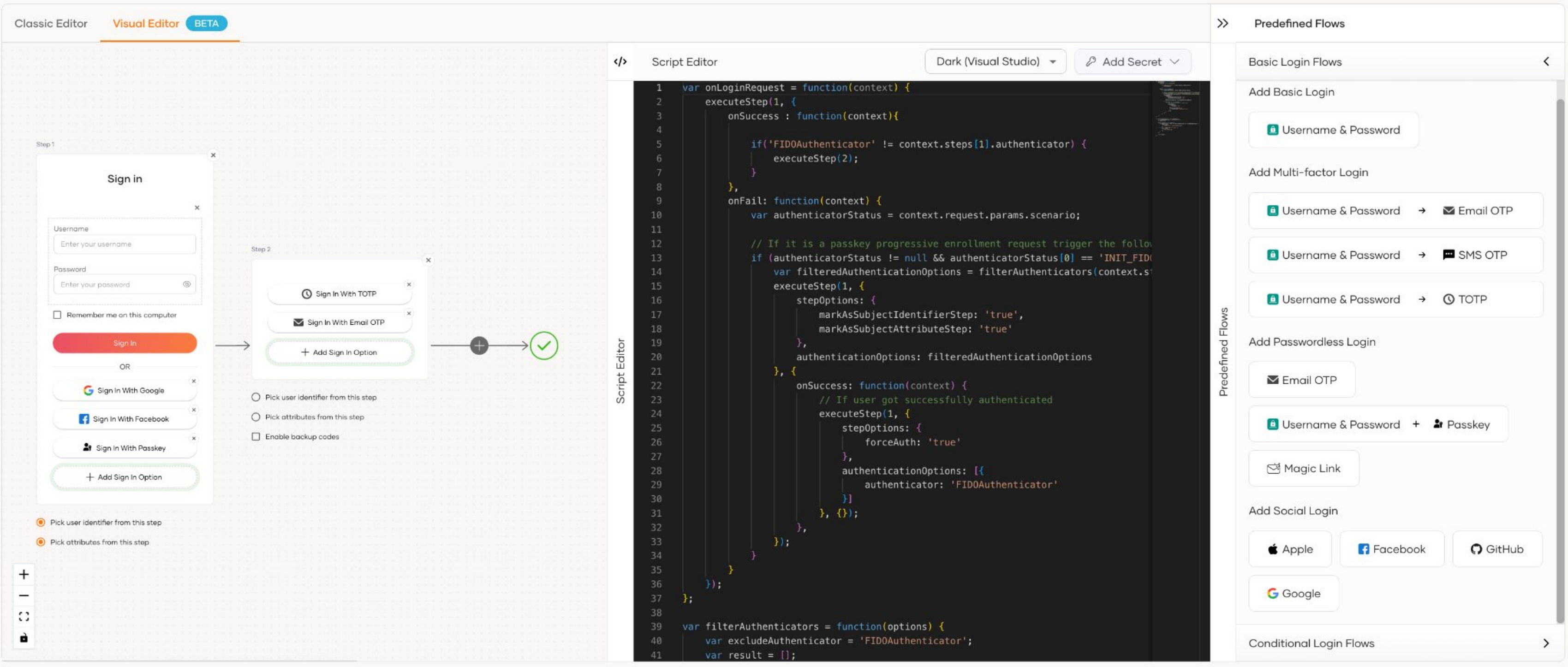
Trusted Token Issuer
A trusted token issuer to exchange its token for an Asgardeo issued token
Set up >

Sign In With Ethereum
OIDC
Login users with their Ethereum wallet.
#OIDC
Set up >

HYPR
Enable login for users with existing HYPR accounts.
#Social-Login
Create → Setup Guide

Optimized Developer Experience

Low-code/No-code visual editor - Preview users’ login experience



Step 1:

□ Remember me on this computer

● Pick user identifier from this step

● Pick attributes from this step

Step 2:

○ Pick user identifier from this step

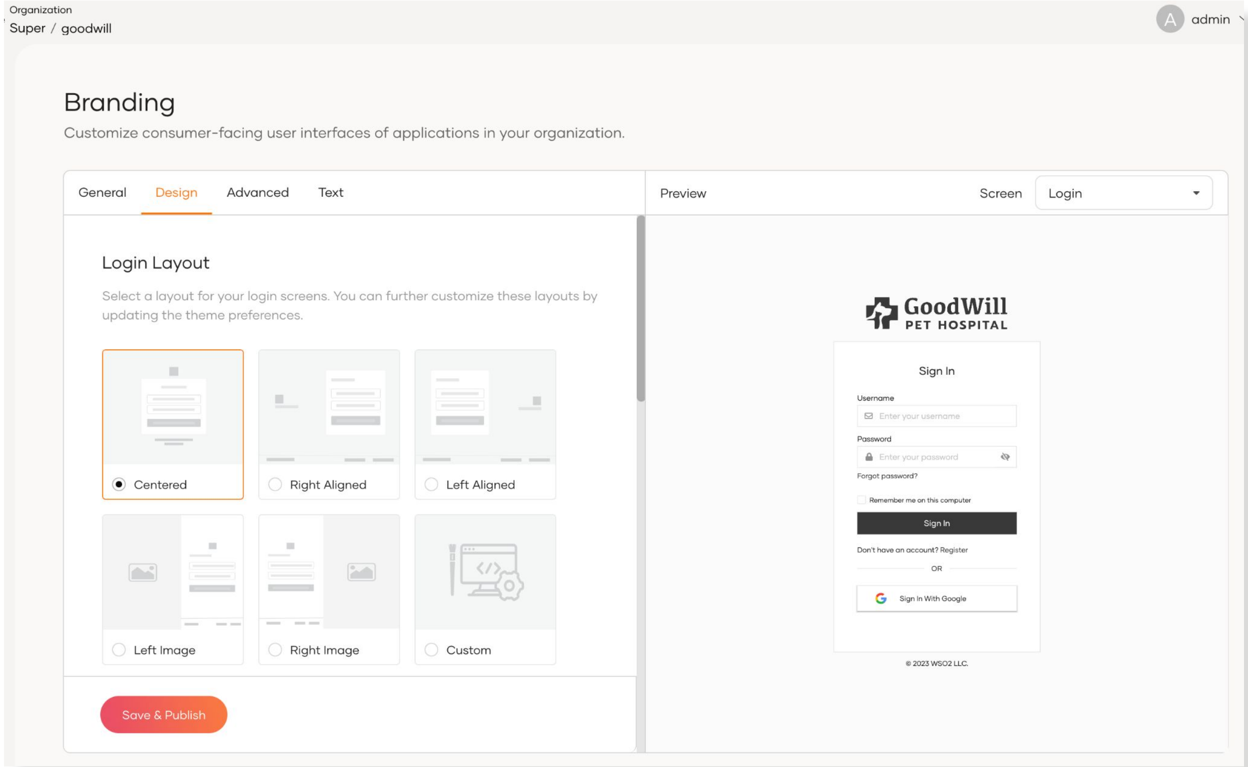
○ Pick attributes from this step

□ Enable backup codes

```
var onLoginRequest = function(context) {
    executeStep(1, {
        onSuccess : function(context){

            if('FIDOAuthenticator' != context.steps[1].authenticator) {
                executeStep(2);
            }
        },
        onFail: function(context) {
            var authenticatorStatus = context.request.params.scenario;

            // If it is a passkey progressive enrollment request trigger the follo
            if (authenticatorStatus != null && authenticatorStatus[0] == 'INIT_FID
                var filteredAuthenticationOptions = filterAuthenticators(context.s
                executeStep(1, {
                    stepOptions: {
                        markAsSubjectIdentifierStep: 'true',
                        markAsSubjectAttributeStep: 'true'
                    },
                    authenticationOptions: filteredAuthenticationOptions
                }, {
                    onSuccess: function(context) {
                        // If user got successfully authenticated
                        executeStep(1, {
                            stepOptions: {
                                forceAuth: 'true'
                            },
                            authenticationOptions: [{
                                authenticator: 'FIDOAuthenticator'
                            }]
                        }, {});
                    },
                });
            }
        }
    });
};

var filterAuthenticators = function(options) {
    var excludeAuthenticator = 'FIDOAuthenticator';
    var result = [];
```

Optimized Developer Experience

Simplified Branding experience



Organization

Super / goodwill

A admin

Branding

Customize consumer-facing user interfaces of applications in your organization.

General | Design | Advanced | Text

Login Layout

Select a layout for your login screens. You can further customize these layouts by updating the theme preferences.

● Centered

○ Right Aligned

○ Left Aligned

○ Left Image

○ Right Image

○ Custom

Save & Publish

Preview

Screen: Login

GoodWill PET HOSPITAL

Sign In

Username: Enter your username

Password: Enter your password

Forgot password?

□ Remember me on this computer

Sign In

Don't have an account? Register

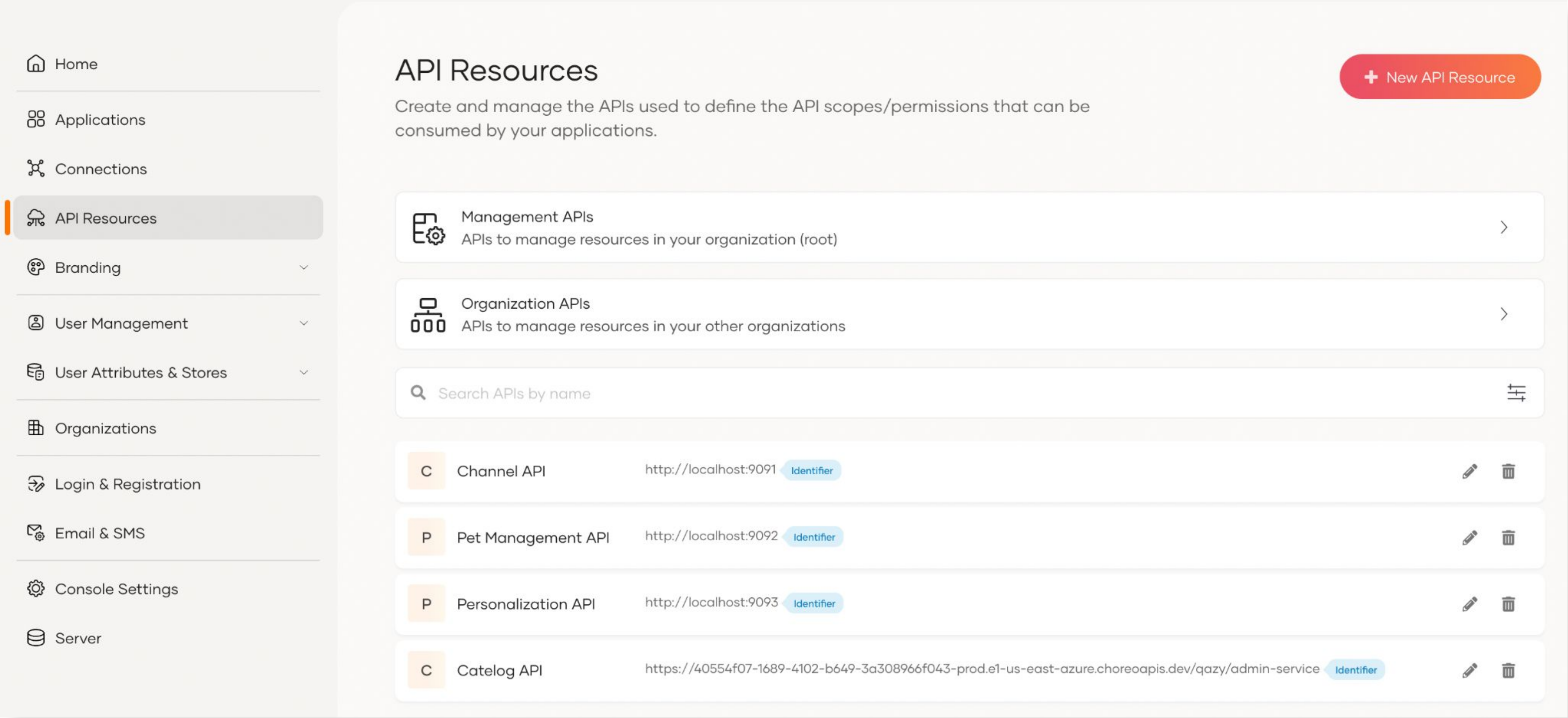
OR

Sign In With Google

© 2023 WSO2 LLC.

Optimized Developer Experience

Optimized API Authorization for Organizations through native scopes



API Resources

Create and manage the APIs used to define the API scopes/permissions that can be consumed by your applications.

Management APIs
APIs to manage resources in your organization (root)

Organization APIs
APIs to manage resources in your other organizations

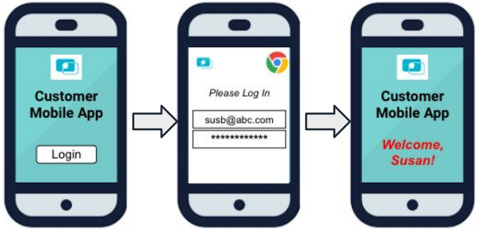
C	Channel API	http://localhost:9091	Identifier
P	Pet Management API	http://localhost:9092	Identifier
P	Personalization API	http://localhost:9093	Identifier
C	Catelog API	https://40554f07-1689-4102-b649-3a308966f043-prod.e1-us-east-azure.choreoapis.dev/qazy/admin-service	Identifier

Optimized Developer Experience

API for In-App Authentication

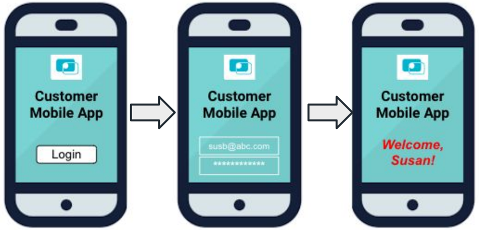
OLD USER EXPERIENCE

An external browser window is required to handle logging into the app



NEW USER EXPERIENCE

User never leaves the native application while logging in



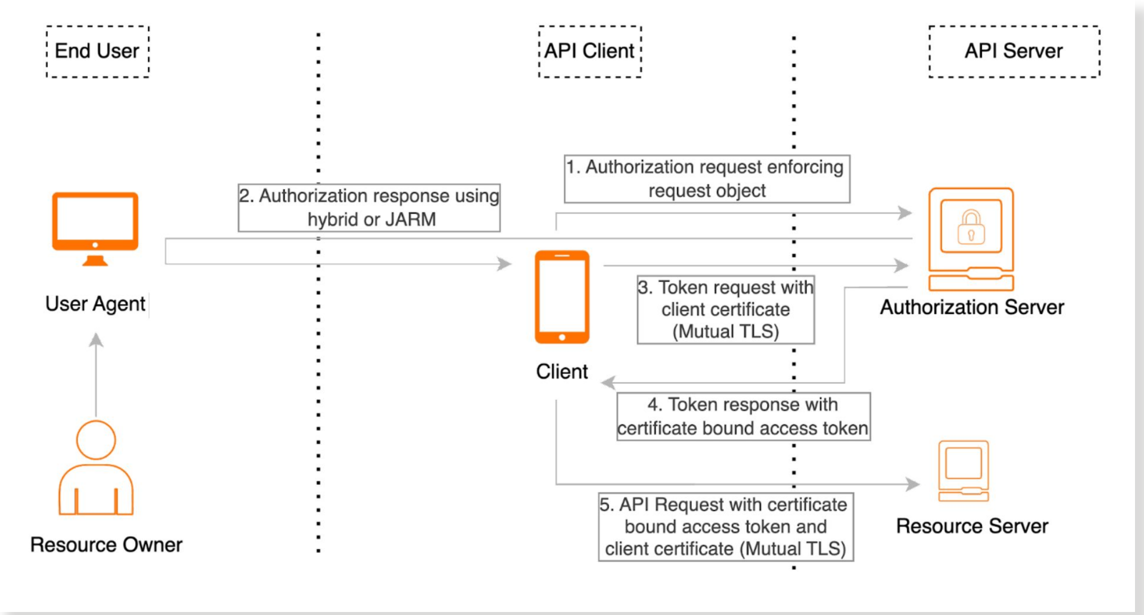
- Orchestrate authentication conditionally without changing the application logic
- Use OAuth 2.0/OpenID Connect flows without the need of a browser support
- Guarantees the identity and proof of possession of the client and the API only communicates with legitimate client apps

B2B CIAM capabilities

- Configure login experiences per organization.
- Including branding per organization.
- Maintain organization hierarchy.
- Delegated Administration.

Support for Financial-Grade APIs (FAPI)

FAPI first-class compliance to FAPI 1.0 and security for high-value APIs.with OAuth 2.0



End User
API Client
API Server
1. Authorization request enforcing request object
2. Authorization response using hybrid or JARM
User Agent
Client
Authorization Server
3. Token request with client certificate (Mutual TLS)
4. Token response with certificate bound access token
5. API Request with certificate bound access token and client certificate (Mutual TLS)
Resource Server
Resource Owner

- Facilitates enforcing FAPI at client registration, user authorization flows, and token issuance flows for third party clients.
- Supports OAuth 2.0 Pushed Authorization Requests
- Supports Financial-grade API: JWT Secured Authorization Response Mode for OAuth 2.0 (JARM)

Supporting Post Quantum Safe Cryptography

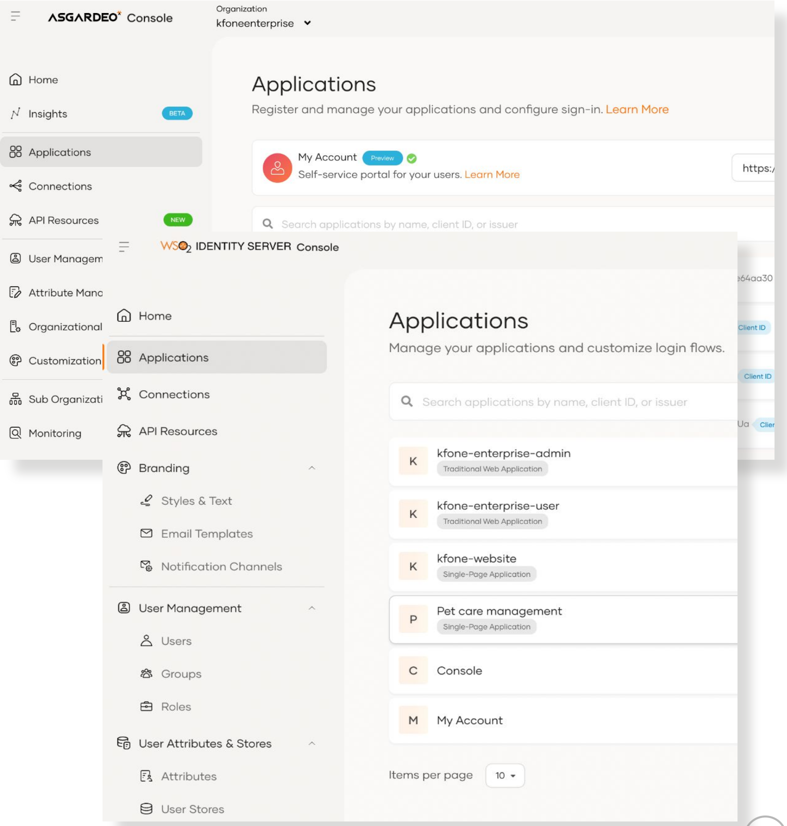
- Post-quantum secure mode can be enabled in IS 7.0 with a few steps

- Post-quantum secure mode will provide support for PQS TLS in inbound communications, more secure internal encryption and hashing.

Feature drop...

Unified IAM experience across all WSO2 IAM products

- A single open source code base across self-hosted, SaaS or private cloud
- Feature parity and consistent experience
  - Developer experience
  - User experience
  - SDKs, templates, and docs
- Supports customers wherever they are in their journey to cloud with common experience
  - Simplifies transition from software to cloud



Applications

Register and manage your applications and configure sign-in. Learn More

My Account

Self-service portal for your users. Learn More

Search applications by name, client ID, or issuer

Applications

Manage your applications and customize login flows.

Search applications by name, client ID, or issuer

kfone-enterprise-admin
Traditional Web Application

kfone-enterprise-user
Traditional Web Application

kfone-website
Single-Page Application

Pet care management
Single-Page Application

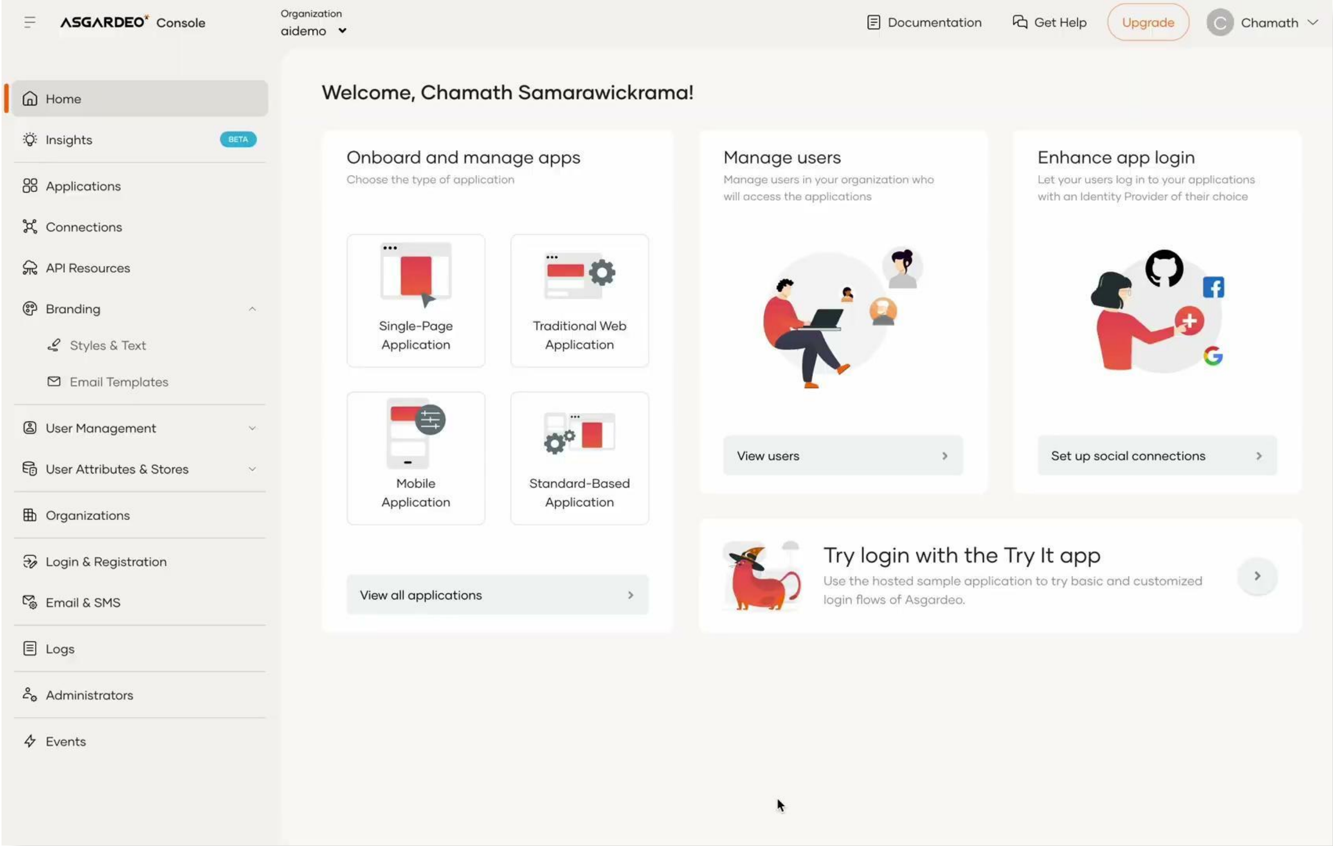
Console

My Account

Items per page 10

AI-assisted features

AI assisted branding



ASGARDEO Console

Organization
aidemo

Documentation
Get Help
Upgrade
Chamath

Home
Insights BETA
Applications
Connections
API Resources
Branding
Styles & Text
Email Templates
User Management
User Attributes & Stores
Organizations
Login & Registration
Email & SMS
Logs
Administrators
Events

Welcome, Chamath Samarawickrama!

Onboard and manage apps
Choose the type of application

Single-Page Application
Traditional Web Application
Mobile Application
Standard-Based Application

View all applications

Manage users
Manage users in your organization who will access the applications

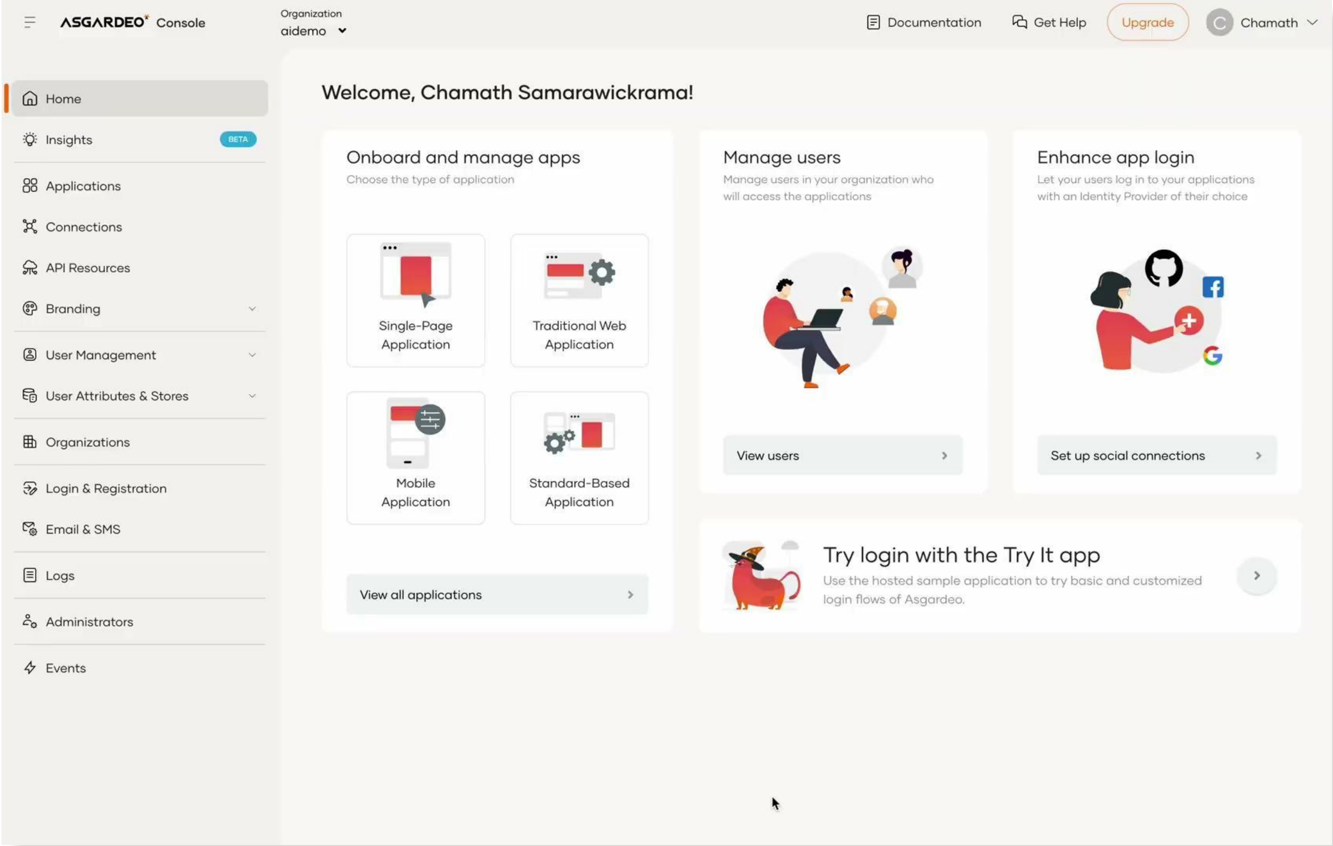
View users

Enhance app login
Let your users log in to your applications with an Identity Provider of their choice

Set up social connections

Try login with the Try It app
Use the hosted sample application to try basic and customized login flows of Asgardeo.

AI assisted login flow generator



ASGARDEO Console

Organization
aidemo

Documentation
Get Help
Upgrade
Chamath

- Home
- Insights BETA
- Applications
- Connections
- API Resources
- Branding
- User Management
- User Attributes & Stores
- Organizations
- Login & Registration
- Email & SMS
- Logs
- Administrators
- Events

Welcome, Chamath Samarawickrama!

Onboard and manage apps

Choose the type of application

Single-Page Application

Traditional Web Application

Mobile Application

Standard-Based Application

View all applications

Manage users

Manage users in your organization who will access the applications

View users

Enhance app login

Let your users log in to your applications with an Identity Provider of their choice

Set up social connections

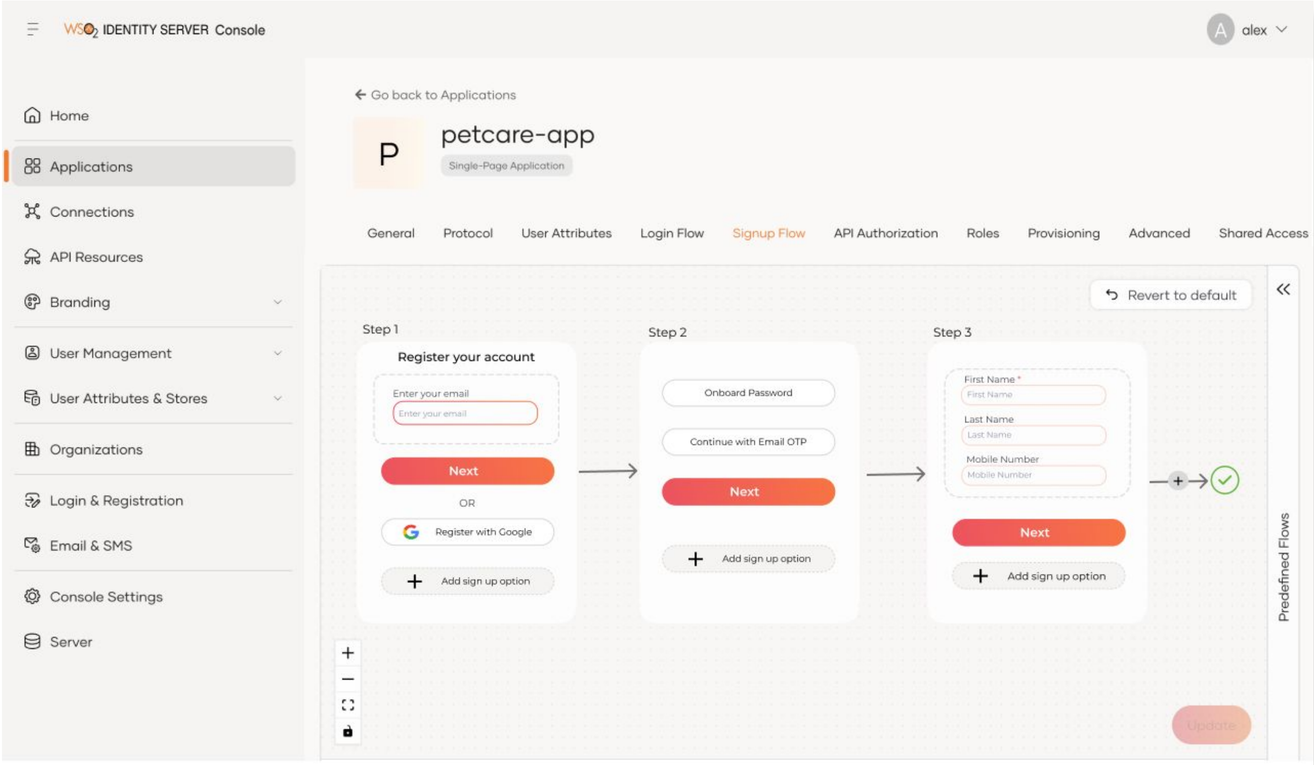
Try login with the Try It app

Use the hosted sample application to try basic and customized login flows of Asgardeo.

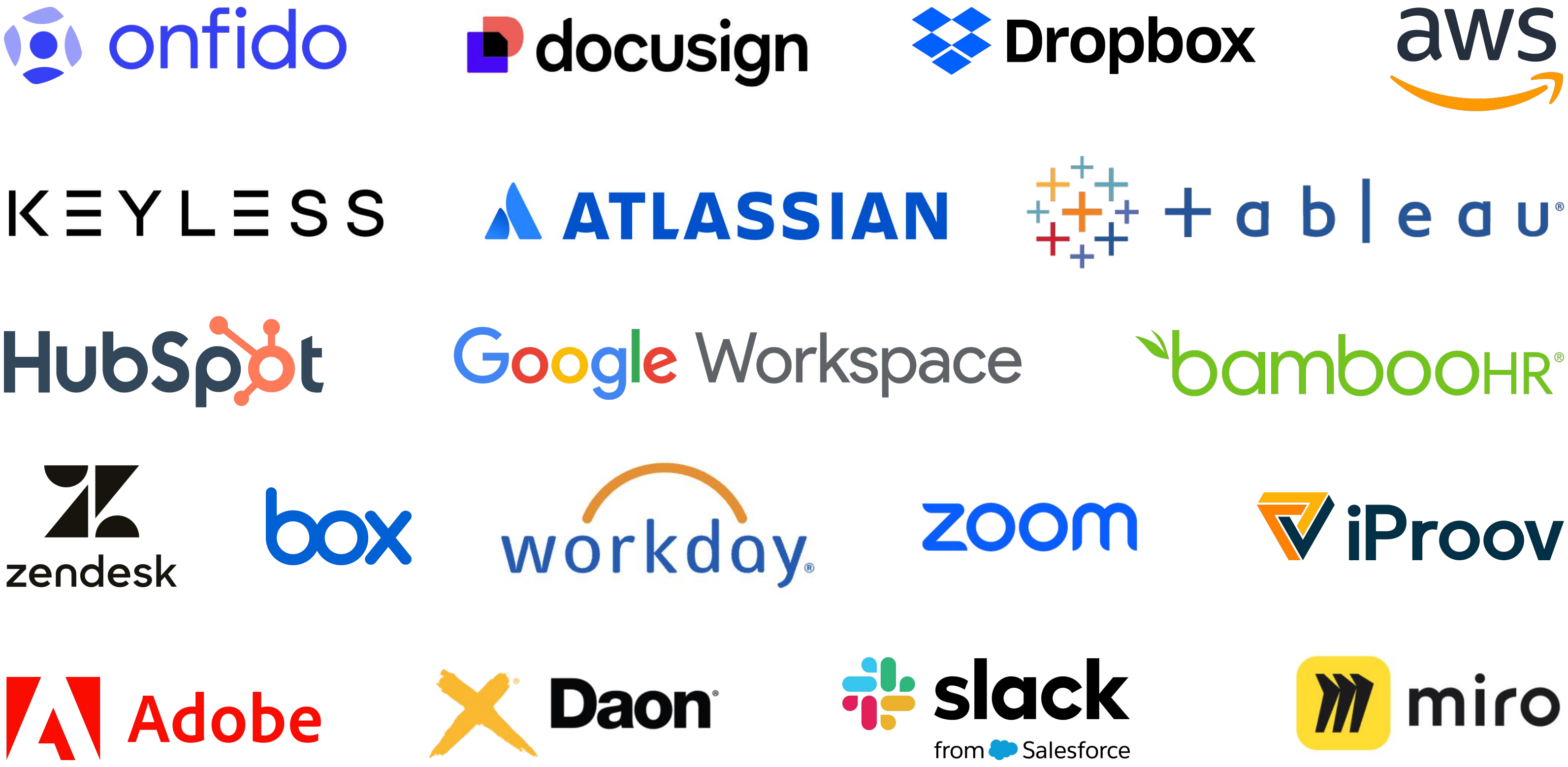
High-level Roadmap

Registration Orchestration

Low-code/No-code visual editor - Preview users’ registration experience



3rd Party Integrations



FAPI 2.0 – Securing high-value APIs

OAuth 2.0
Rich Authorization
Requests
(RAR)

Grant Management

DPoP

Consent Everywhere!

For First-party apps

- Focussed on
  - ⦿ Terms of Services
  - ⦿ Privacy policy and Cookie policy
- Enhanced by
  - ⦿ OAuth 2.0 - Scopes
  - ⦿ OAuth 2.0 - RAR

For 3rd party apps

- Focussed on
  - ⦿ Coarse-grained Authz
  - ⦿ Fine-grained Authz
  - ⦿ User-managed consent
- Enhanced by
  - ⦿ Grant Management

Self service across the above

Platform & architectural improvements

Eventing & Extension Support

Improving operational efficiency of the identity platform

Java 21 support

Upgrade vs Migration

TRACK

Identity & Access Management

Organization Management: The Revolution in B2B CIAM

Johann Nallathamby
Director - Solutions Architecture
WSO2

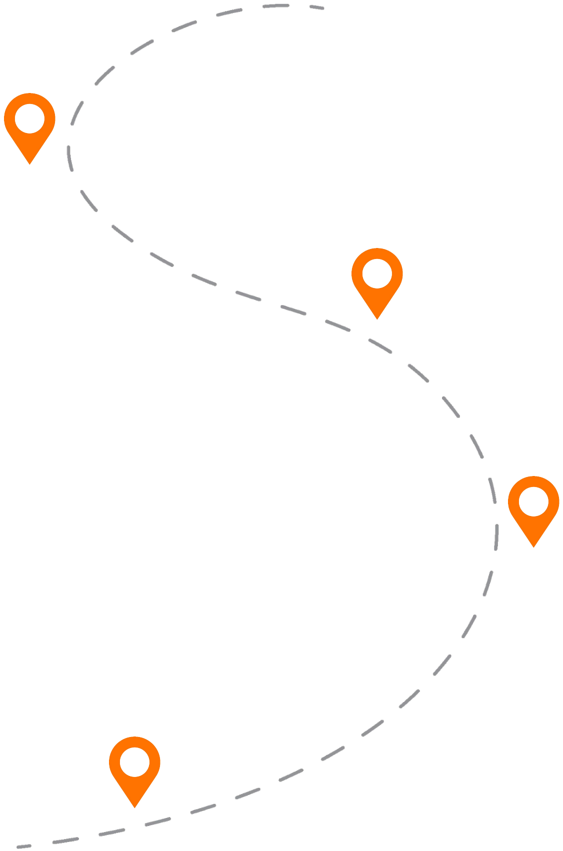
TRACK

Digitization Strategy

Unlocking the Identity: Embracing CIAM 2.0 for a Competitive Advantage

Omindu Rathnaweera
Associate Director/Architect
WSO2

IAM is a journey…



Question Time!

Let’s Connect!

Thank You!