Delivering a B2B IAM Project

An Auth0 planning guide to business-to-business identity and access management

auth0-tfg-00001 version March 7, 2024

Introduction

This document provides guidance for integrating Auth0 within a business-to-business (B2B) identity and access management (IAM) project.

Based on our experience working with customers who've implemented Auth0 for this type of project, we've developed a set of goals and milestones that will help you plan your solution efficiently and deliver it effectively.

Before you begin, consider the following items:

1. Identify your primary objectives and determine the requirements to achieve them.
2. Use a phased approach across multiple workstreams.
3. Adopt an iterative release process.

Identify your primary objectives

Determining the key goals of your project early on will help your teams focus on the specifics when building out your solution.

For example, if your primary objectives are to avoid disruption for end-users and provide continuity of service, then consider adopting an iterative release process instead of a "big-bang" approach when integrating with Auth0.

Use a phased approach

A phased approach across multiple workstreams will help your teams divide and conquer. Many implementation tasks can be completed in parallel, which will allow you to reach milestones faster and present your project to stakeholders sooner.

This is also a good time to check if other groups within your organization have been working with Auth0. There may be opportunities to share first-hand experience with the product, consolidate resources, and inform the structure of your implementation.

We may be able to help you identify these teams and provide guidance for collaboration.

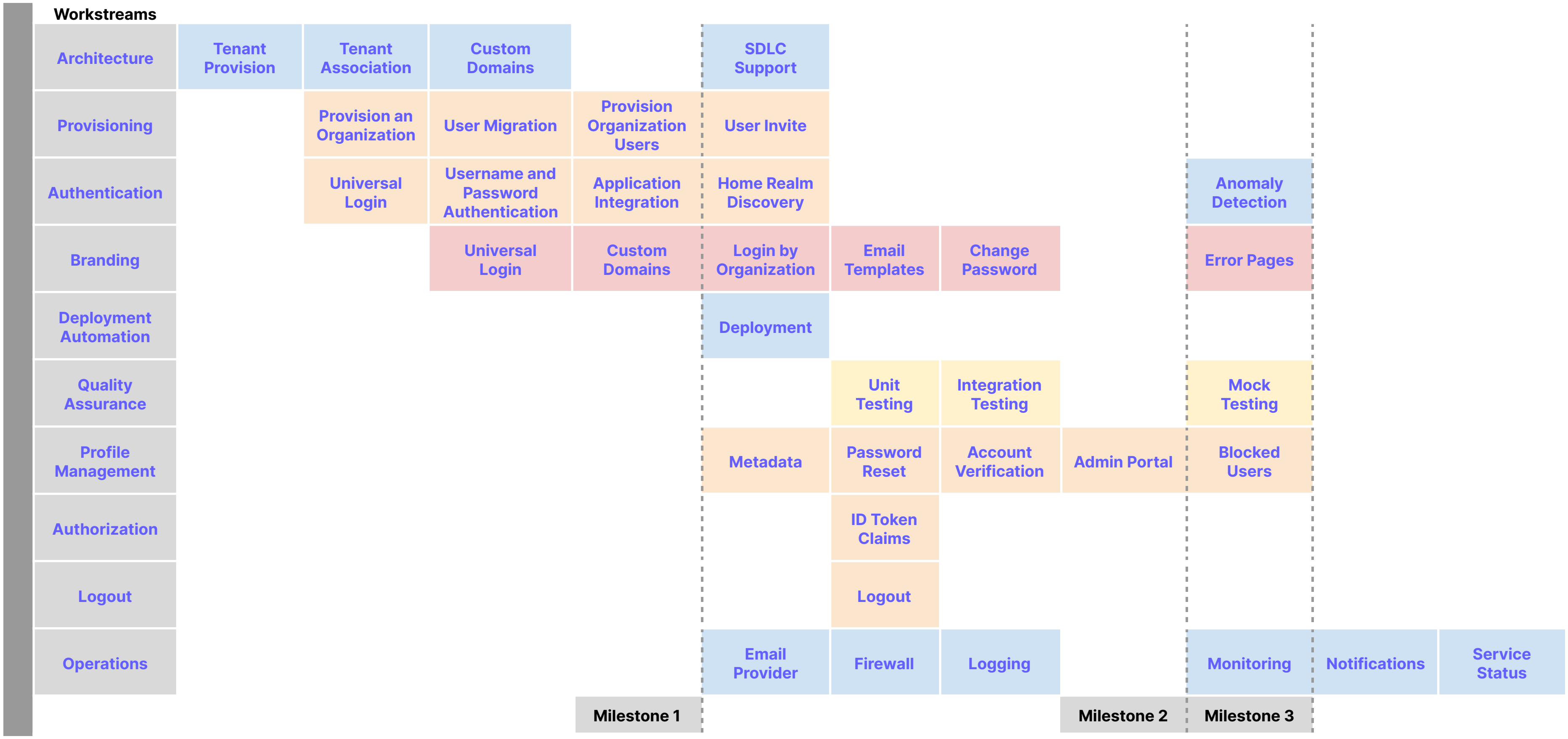
Adopt an iterative release process

Adopting an iterative release process will help your teams reduce cognitive overload and improve the velocity of development.

For example, if you have three or four applications you want to integrate with Auth0, consider working on one application at a time. This way, your teams can take what they learned from the previous iteration into the next one.

> If you have multiple applications and you want Single Sign-On (SSO) support, read Architecture to help you understand what you need to consider when using an iterative release process.

Phase 1: Application Integration and User Authentication



Workstreams											
Architecture	Tenant Provision	Tenant Association	Custom Domains		SDLC Support						
Provisioning		Provision an Organization	User Migration	Provision Organization Users	User Invite						
Authentication		Universal Login	Username and Password Authentication	Application Integration	Home Realm Discovery				Anomaly Detection		
Branding			Universal Login	Custom Domains	Login by Organization	Email Templates	Change Password		Error Pages		
Deployment Automation					Deployment						
Quality Assurance						Unit Testing	Integration Testing		Mock Testing		
Profile Management					Metadata	Password Reset	Account Verification	Admin Portal	Blocked Users		
Authorization						ID Token Claims					
Logout						Logout					
Operations					Email Provider	Firewall	Logging		Monitoring	Notifications	Service Status
				Milestone 1				Milestone 2	Milestone 3		

Legend

Audience

- 🟥 Branding
- 🟧 Design & Development
- 🟦 Operations & Infrastructure
- 🟨 Testing

Milestones

Milestone 1	Authentication. Demonstration to stakeholders.
Milestone 2	Profiles, branding, authorization. Demonstration to stakeholders.
Milestone 3	Go-Live. Deployment to production.

Phase 1

The first phase focuses on integrating your application(s) with Auth0 to provide user authentication. You'll address the 10 key stages across three key milestones required to go live. Ultimately, you'll have a production-ready implementation that integrates with Auth0 to provide user authentication across your application(s).

The workstreams, the topics they address, and the order in which you complete them are important, so we recommend you follow the guidance as prescribed.

Some topics can be worked on by different teams in parallel, such as Provisioning, Authentication, and Branding. We've found that if you assign a topic to the team that has the most experience with it (such as your design team to Branding), you can accelerate implementation with minimal overlap.

Architecture

The Architecture workstream must consider how your application(s) fits in your organization, what the user base looks like, how to structure your Auth0 assets, and if there are opportunities for cross-integration.

Topics include:

- Tenant Provision
- Custom Domains
- Tenant Association
- Software Development Life Cycle (SDLC) Support

Provisioning

The Provisioning workstream must consider how users sign up with your application(s), which identity providers you will support, and how and what user data will be stored.

The **Provisioning** workstream can complete their work in parallel with the Authentication and Branding workstreams.

Topics include:

- Provision an Organization
- User Migration

- Provision Organization Users
- User Invite

> The Auth0 Dashboard (along with the Delegated Administration extension) can be used out-of-box to perform user provisioning and deprovisioning.
>
> If you require more comprehensive deprovisioning functionality (for example, compliance reasons) then refer to the Provisioning guidance provided in Phase 2.

Authentication

The Authentication workstream must consider how users will prove their identity, how you'll balance user experience and security, and what levels of additional authentication are necessary (such as Multi-factor authentication or Step-up authentication).

The **Authentication** workstream can complete their work in parallel with the Provisioning and Branding workstreams.

Topics include:

- Universal Login
- Username and Password Authentication
- Application Integration
- Home Realm Discovery
- Anomaly Detection

Branding

The Branding workstream must consider how to customize the look and feel of Auth0 to align with your organization's requirements and provide a consistent user experience to instill trust in your brand.

The **Branding** workstream can complete their work in parallel with the Provisioning and Authentication workstreams.

Topics include:

- Universal Login Customization
- Custom Domain
- Login by Organization

- Change Password Customization
- Error Page Customization
- Email Template Customization (read Operations guidance before doing so)

Deployment Automation

The Deployment Automation workstream must consider how to manage the development and release cycle for Auth0 assets, ensure a dynamic development environment, and guarantee a stable production environment.

Topics include:

- SDLC Support
- Tenant-Specific Variables

Quality Assurance

The Quality Assurance workstream must consider how to detect breakages in your Auth0 integration and mitigate the resulting impact on users.

Topics include:

- Unit Testing
- Mock Testing
- Integration Testing

Profile Management

The Profile Management workstream must consider how to manage user profile data, user account verification and recovery, and user account restriction.

Topics include:

- Metadata Management
- Password Reset
- Account Verification
- Admin Portal
- Blocked Users

Authorization

The Authorization workstream must consider how and what user data is passed between the authorization server and the application(s).

Topics include:

- ID Token Claims

Logout

The Logout workstream must consider how users terminate their application, Auth0, and identity provider sessions.

Topics include:

- Session Layers
- Session Lifetime Limits
- Log Users Out of Applications
- Log Users Out of Identity Providers

Operations

The Operations workstream must consider how to send emails and notifications to users, monitor Auth0 user activity, and process Auth0 log data.

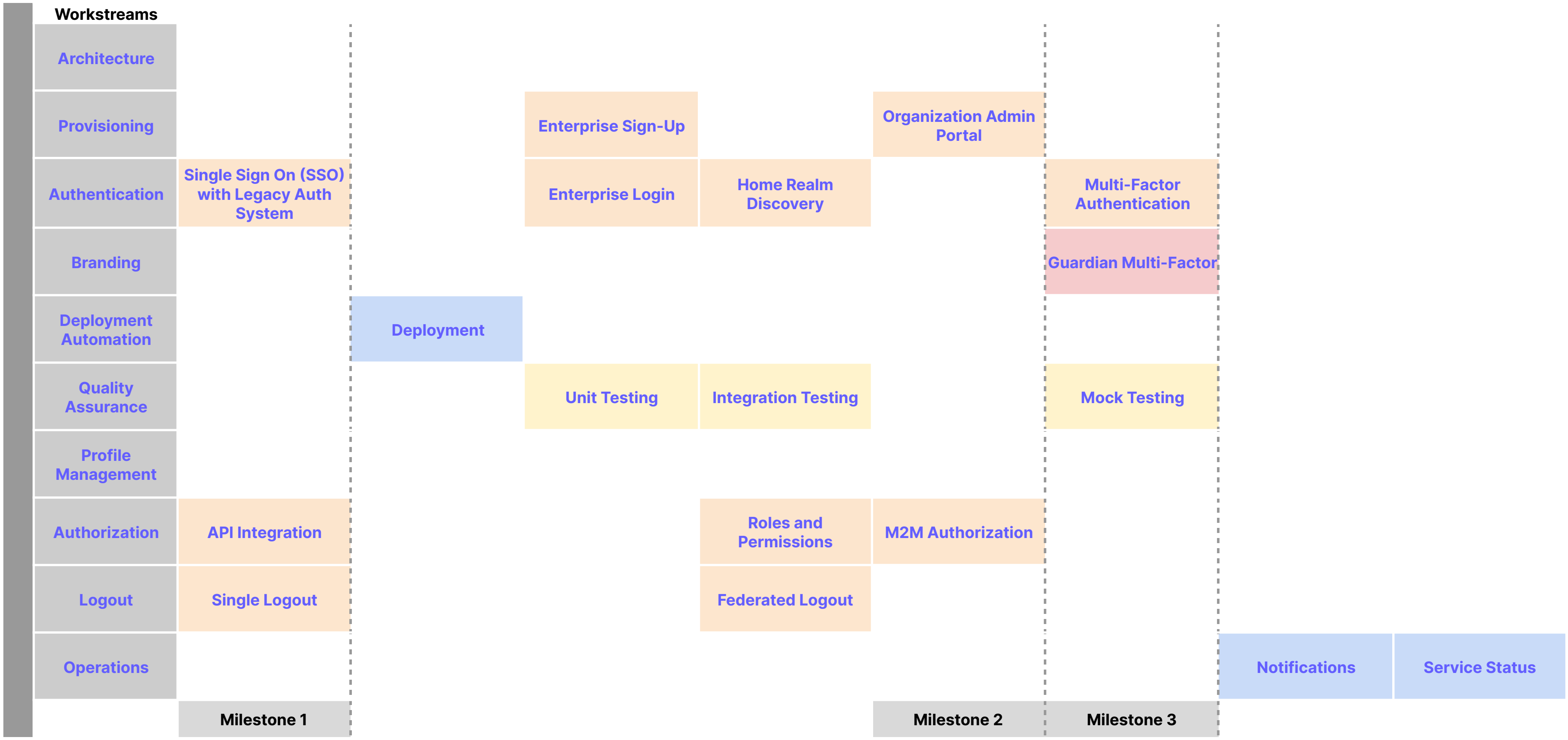
Topics include:

- Email Provider Setup
- Monitoring
- Logging
- Firewall Configuration
- Notifications

Next steps

At this point, you've integrated your application(s) with Auth0, configured user authentication, and are ready for production.

Phase 2: API Authorization, Advanced Authentication, Provisioning, and Profile Management



Workstreams								
Architecture								
Provisioning			Enterprise Sign-Up		Organization Admin Portal			
Authentication	Single Sign On (SSO) with Legacy Auth System		Enterprise Login	Home Realm Discovery		Multi-Factor Authentication		
Branding						Guardian Multi-Factor		
Deployment Automation		Deployment						
Quality Assurance			Unit Testing	Integration Testing		Mock Testing		
Profile Management								
Authorization	API Integration			Roles and Permissions	M2M Authorization			
Logout	Single Logout			Federated Logout				
Operations							Notifications	Service Status
	Milestone 1				Milestone 2	Milestone 3		

Legend

Audience

🟥	Branding
🟧	Design & Development
🟦	Operations & Infrastructure
🟨	Testing

Milestones

Milestone 1	API integration. Demonstration to stakeholders, deployment to production.
Milestone 2	Advanced features. Demonstration to stakeholders, deployment to production.
Milestone 3	Go-Live. Deployment to production.

Phase 2

The second phase focuses on integrating your API(s) with Auth0 to provide authorization functionality and configuring enterprise federations.

Additionally, the Authentication, Deployment Automation, Provisioning, and Logout workstreams will address topics that allow for advanced functionality.

The workstreams, the topics they address, and the order in which you complete them are important, so we recommend you follow the guidance as prescribed.

Authorization

The Authorization workstream must consider how your API(s) will be integrated with Auth0 and how access management will be handled (policy and method).

The **Authorization** workstream can complete their work in parallel with the Authentication and Deployment Automation workstreams.

Topics include:

- API Integration
- Roles and Permissions
- M2M Authorization

Authentication

The Authentication workstream must consider how users log in to your applications and if there are areas for improvement.

The **Authentication** workstream can complete their work in parallel with the Authorization and Deployment Automation workstreams.

Topics include:

- SSO with the Legacy Auth System
- Enterprise Login
- Home Realm Discovery
- Multi-Factor Authentication

Deployment Automation

The Deployment Automation workstream must consider how to integrate Auth0 with your continuous integration/continuous deployment (CI/CD) pipeline.

The **Deployment Automation** workstream can complete their work in parallel with the Authorization and Authentication workstreams.

Topics include:

- Deploy CLI Tool
- Auth0 Terraform Provider

Quality Assurance

The Quality Assurance workstream must consider how to detect breakages in your Auth0 integration and how to mitigate the resulting impact on users.

Topics include:

- Unit Testing
- Mock Testing
- Integration Testing

Provisioning

The Provisioning workstream must consider how Enterprise connections will be supported.

Topics include:

- Organization Admin Portal
- Enterprise Sign-Up

Branding

The Branding workstream must consider how to customize the look and feel of Auth0 to align with your organization's requirements and provide a consistent user experience to instill trust in your brand.

Topics include:

- Customize Multi-Factor Authentication Pages
- Auth0 Guardian

Logout

The Logout workstream must consider how users terminate their application, Auth0, and identity provider sessions.

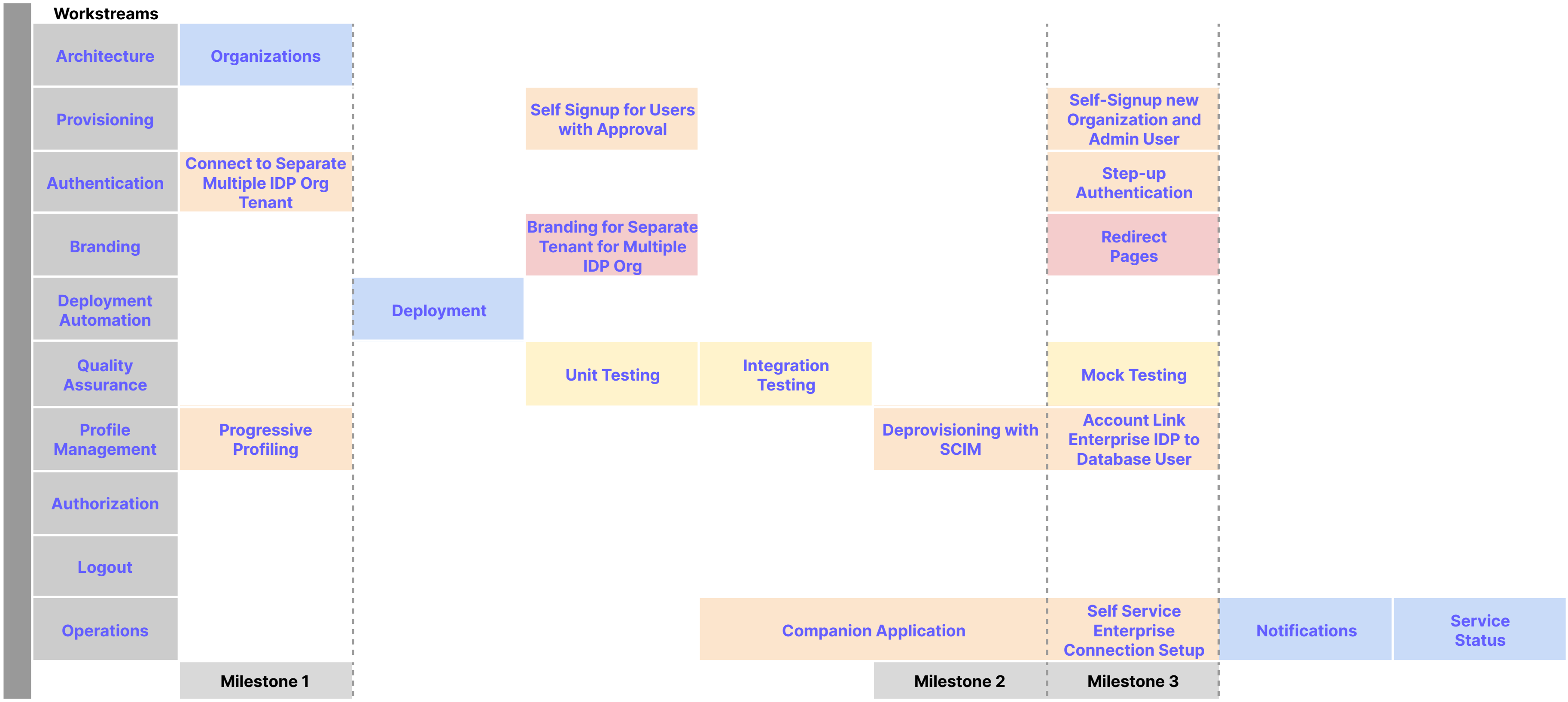
Topics include:

- Single Logout
- Federated Logout

Next steps

At this point, you've integrated your API(s) with Auth0, configured API authorization policies, and introduced advanced functionality in several workstreams.

Phase 3: Extended Use Cases for Authentication, Profile Management, and Operations



Workstreams								
Architecture	Organizations							
Provisioning			Self Signup for Users with Approval			Self-Signup new Organization and Admin User		
Authentication	Connect to Separate Multiple IDP Org Tenant					Step-up Authentication		
Branding			Branding for Separate Tenant for Multiple IDP Org			Redirect Pages		
Deployment Automation		Deployment						
Quality Assurance			Unit Testing	Integration Testing		Mock Testing		
Profile Management	Progressive Profiling				Deprovisioning with SCIM	Account Link Enterprise IDP to Database User		
Authorization								
Logout								
Operations				Companion Application		Self Service Enterprise Connection Setup	Notifications	Service Status
	Milestone 1				Milestone 2	Milestone 3		

Legend

Audience

- 🟥 Branding
- 🟧 Design & Development
- 🟦 Operations & Infrastructure
- 🟨 Testing

Milestones

Milestone 1	Extended use cases. Demonstration to stakeholders, deployment to production.
Milestone 2	Specialized customization. Demonstration to stakeholders, deployment to production.
Milestone 3	Go-Live. Deployment to production.

Phase 3

The third phase focuses on addressing complex use cases, including support for multiple IdPs and specialized customization.

Additionally, the Authentication, Profile Management, Branding, Provisioning, and Operations workstreams will address topics that allow for advanced functionality.

The workstreams, the topics they address, and the order in which you complete them are important, so we recommend you follow the guidance as prescribed.

Architecture

The Architecture workstream must consider how to manage tenant provisioning for complex organizations.

Topics include:

- Organizations

Authentication

The Authentication workstream must consider how to support multiple IdPs and handle use cases that require additional user verification.

Topics include:

- Connect to Separate Multiple IDP Org Tenant
- Step-up Authentication

Profile Management

The Profile Management workstream must consider how to enrich user profile data, manage user deprovisioning, and link user profiles.

Topics include:

- Progressive Profiling
- Deprovisioning with SCIM
- Account Link Enterprise IDP to Database User

Branding

The Branding workstream must consider how to manage the look and feel when supporting multiple organizations and ensure a consistent user experience across all user journeys.

Topics include:

- Branding for Separate Tenant for Multiple IDP Org
- Redirect Pages

Provisioning

The Provisioning workstream must consider how to manage complex provisioning use cases for multi-tenant applications.

Topics include:

- Just-In-Time Membership for Organizations
- Provisioning Organizations

Operations

The Operations workstream must consider how to manage multiple organizations and if the development of a companion application is necessary.

A companion application provides the ability for your organization's internal members (such as a customer support team) to perform actions on behalf of your users. If you'd like more information, ask your Technical Account Manager (TAM) for details.

Topics include:

- Organization Admin Portal

Conclusion

Thank you for taking the time to read this guide on integrating Auth0 within a business-to-business (B2B) identity and access management (IAM) project.

This guide is occasionally updated based on our continuing experiences with customers, and we recommend you check with our scenario guidance as you progress.

If you require more detailed information regarding certain functionality or would like to discuss a specific use case, please contact our Professional Services team.