Delivering a Business-to-Business IAM Project

An Auth0 Planning Guide to Business-to-Business Identity & Access Management

auth0-tfg-00001 version June 21, 2019

Introduction

This document provides planning guidance for integrating Auth0 within a Business-to-Business IAM style project, and is based on real world customer implementation experience. Customers implementing Auth0 for Business-to-Business IAM (a.k.a. B2B) focused projects, regardless of vertical or market, typically find they have a common set of goals and objectives they need to consider and plan for. This document distills our experience working with these customers in order to help you deliver your solution in the most effective manner. By following the advice provided, you are setting your project up for success.

Identifying your primary objectives early on will help your teams focus on the specifics important to building out your solution. For instance, if your primary objective is to avoid disruption for end-users and provide continuity of service, then you shouldn't adopt a "big-bang" approach when integrating with Auth0.

In our experience, customers who've established clear objectives and who have aligned those objectives to requirements early on have benefitted the most when it comes to integrating with Auth0. Whether working on a green-field project, or modernizing identity and access management across an established application suite, our customers have been most successful when they plan their project using a **phased** approach across multiple workstreams**.**

Customers who also adopt an iterative release style typically make better progress. For example, you may have three or four applications you wish to integrate and instead of tackling them all at once, consider treating your project as a series of iterations tackling one application at a time. This way your teams can benefit from experience, and can leverage this to help increase velocity with each iteration.

Whilst adopting an iterative release style will improve your time to market, if you do have multiple applications and you want Single Sign On (SSO) support then our Architecture guidance will help you understand what you need to consider.

There may also be other groups within your organization who've also been working with Auth0, and from whom you could gain first-hand experience too; it's not uncommon for our customers to have disparate departments within their organization who serve different user communities. The team at Auth0 may be able to assist you in identifying these, and doing so early will help you in structuring your work.

Phase 1

In almost all cases we've observed that our most successful customers adopt a multi-phase approach when it comes to project planning and execution. Phase 1 focuses on integrating your Application(s) with Auth0 to provide user Authentication, and is a pre-cursor to all other activities involving the use of Auth0. During Phase 1 you'll tackle the 10 key stages to Go-Live, across 3 key milestones, and by tackling the main risk items will address the most critical paths associated with integration.

Planning: Phase 1 – Application integration and User Authentication

Workstreams											
Architecture	Tenant Provision	Tenant Association	Custom Domains		SDLC Support						
Provisioning		Provision a new Organization	User Migration	Provisioning Organization users	User Invite						
Authentication		Universal Login	Username & 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				ï		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, Authz
Demonstration to stakeholders.

Milestone 3: Go-Live
Deployment to Production

As can be seen from the diagram above (click to navigate), at the end of Phase 1 you'll have working implementation that integrates with Auth0 to provide user Authentication across your application(s). This can be taken into production, or at the very least be provided as part of an early adopter or Beta program.

Phase 1 consists of a number of workstreams, with a number of topics in each. The workstreams, topics and the order in which you address each is important, so we recommend you follow the guidance prescribed. That's not to say you can't or shouldn't tackle work in parallel: Provisioning and Authentication, for example, could be tackled independently and at the same time, and these could both be tackled in parallel with your Branding efforts.

In most successful integration cases we've also found that different teams tackle different streams, and that this can provide significant benefit: your design and development team(s) would typically tackle implementation whilst at the same time your branding team would tackle Auth0 asset customization thus reducing overall time to market.

- Architecture is the first workstream you will cover, with Tenant Provision being the precursor topic to all others. Other topics to address at this stage include:
    - Custom Domains,
    - Tenant Association, and
    - Support for the Software Development Life Cycle (SDLC)
- Provisioning is the next workstream, and this can be done in parallel with Authentication. We've found that the most successful implementations address the following topics at this stage during Phase 1, however precisely what you tackle will depend on your specific requirements - i.e. you may not need User Migration for example, or you may already have an existing invite mechanism that can be leveraged :
    - Provisioning a new Organization,
    - User Migration,
    - Provisioning Organization Users, and/or
    - User Invite

The Auth0 Dashboard in conjunction with the Delegated Administration extension can be used out-of-box to provide for user deprovisioning (as well as provisioning). If you require more comprehensive deprovisioning functionality - say for compliance reasons - then refer to the Provisioning guidance provided in Phase 2.

- Authentication comes next and can be done in parallel with Provisioning. Topics to address at this point will include:
    - Universal Login
    - Username and Password Authentication,
    - Application Integration,
    - Home Realm Discovery, and
    - Anomaly Detection

- Branding can be done in parallel with Provisioning & Authentication, and with most customers would typically be handled by their branding team. Topics to address here include:
    - Universal Login page customization,
    - Naming for your Custom Domain,
    - Login by Organization,
    - Change Password page customization,
    - Error Page customization, and
    - Email Template customization (though we recommend you follow Operations guidance before doing so).

By this point you will have completed major work required to integrate an application, will have addressed the most significant risk items, and will also be able to provide demonstrable functionality to stakeholders too. From here on in you'll be working towards production Go-Live. As you progress through the remaining workstreams and topics you can start to align your Auth0 tenants with your SDLC, and you'll be steadily and progressively reducing risk as you go. You'll also have the opportunity to demonstrate further functionality to stakeholders, which will also help you to garner feedback from the rest of the business:

- Deployment Automation. Up 'till now you'll most likely have been working with the one Auth0 development Tenant created as part of Provisioning. Auth0 tooling to automate deployment of assets will now allow you to utilize additional tenant provision in preparation for your testing effort and also your production release - providing you with stable environment(s) which can be used for both demonstration and evaluation.

- Quality Assurance mechanisms should now be employed to ensure any breakages due to defects or changes are detected early, and this is where Auth0 tenant provision for QA will be utilized. Topics to address here include:
    - Unit testing,
    - Mock testing and
    - Integration testing

- Profile Management will address the most common cases for the changes users will want to make to their profile. We've found the most successful implementations address the following topics at this point during Phase 1, however precisely what you tackle will depend on your specific requirements (i.e. you won't need to provide for metadata management if you're not utilizing user metadata):
    - Metadata management,
    - Password Reset,
    - Account Verification,
    - Admin Portal, and
    - Blocked Users

- Authorization, at this stage, is for customers who have specific access control requirements, and the focus for Phase 1 will be centered on how custom ID Token Claims can be leveraged to support this.

- Logout comes next on the agenda. Eventually users will want to log out of your system and you'll need to decide exactly what this looks like. Auth0 supports several variations when it comes to user logout giving you flexibility to choose what works best for your implementation.
- Operations can be addressed in parallel, though we do recommend you setup your email provider early on, as this will enable you to minimize disruption moving forward as well as allow you to quality test specific functionality not possible with out-of-box email provision. Topics to cover here will include:
    - Email Provider Setup,
    - Monitoring,
    - Logging,
    - Firewall configuration, and
    - Notifications

Congratulations! Reaching this point you have integrated with Auth0 to provide user Authentication and are ready for Go-Live. If you've not already done so, you can align your Auth0 production tenant via deployment automation and run any final QA in preparation for production release. As you move forward you'll want to keep a watch for Notifications from Auth0, which may contain important information that could impact your tenant(s) and/or project(s) going forward.

Phase 2

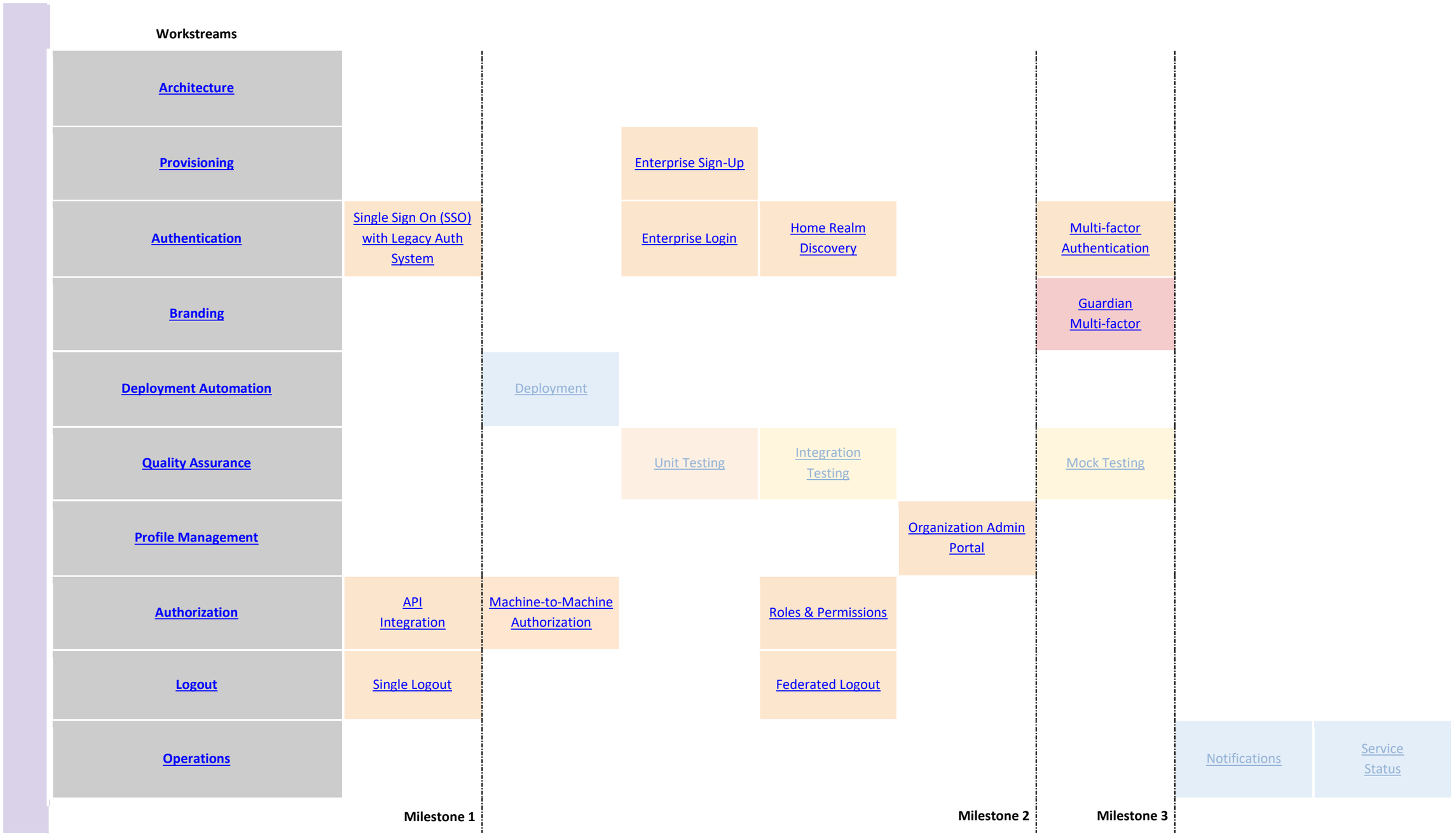
Phase 2 builds on the work conducted as part of Phase 1, and will primarily focus on integrating your API(s) with the Authorization capabilities provided by Auth0 and setting up enterprise federation; completing Phase 1 is a pre-cursor to Phase 2.

In Phase 2 you'll also address additional aspects of Authentication, Provisioning and Profile Management. Having completed Phase 1 activities as prescribed, Auth0 capabilities allow you to incorporate elements of advanced functionality in these areas, to provide enhanced capability in short order.

As with Phase 1, Phase 2 consists of a number of workstreams with a number of topics in each as illustrated in the diagram below (click to navigate). The workstreams, topics and the order in which you address each is important, so we recommend you follow the guidance prescribed. That's not to say you can't or shouldn't tackle work in parallel: Authorization and advanced Authentication, for example, could be tackled independently and at the same time, and these could both be tackled in parallel with your Branding or advanced Profile Management efforts.

The nature of Phase 2 means that work is less prescribed than in Phase 1. Unconnected topics such as API Integration and Enterprise Login can be tackled independently – or not at all. However, some of these do still have dependent relationships – Federated Logout for instance is something we would recommend only if you are considering any of the Enterprise connection flows.

Planning: Phase 2 – API Authorization and advanced Authentication, Provisioning and Profile Management



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

Utilizing continuous integration established in Phase 1 (as part of Deployment Automation), Phase 2 work can be taken into production in an accelerated fashion - or at the very least be provided as part of an early adopter or Beta program.

In a fashion similar to Phase 1, the majority of successful integration cases in Phase 2 have found significant benefit from having different teams tackle different streams: your design and development team(s) would typically tackle implementation whilst at the same time your branding team would tackle Auth0 asset customization thus reducing overall time to market.

- Authorization is the first workstream you'll cover, with API Integration being the focus topic on the agenda. Auth0 supports the OAuth 2.0 protocol, the industry-standard for authorization, as a first class citizen and using the capabilities provided you can implement secure access to any Application Program Interfaces you supply. Topics include:
    - API Integration,
    - Machine-to-Machine Authorization, and
    - Roles & Permissions
- Extending Authentication comes next, and can be done in parallel with both Authorization and Deployment Automation to provide advanced functionality to your Phase 1 implementation. Topics to address at this point may include:
    - SSO with the Legacy Auth System,
    - Enterprise Login,
    - Home Realm Discovery – consider whether you need to make changes once you add enterprise connections, and
    - Multi-factor authentication - an industry recommendation in many cases
- Deployment Automation setup in Phase 1 can be used to automate deployment of assets, allowing you to utilize SDLC supporting tenant provision in preparation for your testing effort and also your production release - providing you with stable environment(s) which can also be used for both demonstration and evaluation.
- Quality Assurance mechanisms employed in Phase 1 can be used to ensure any breakages due to defects or changes are detected early, and this is where Auth0 tenant provision for QA will be utilized. Topics to address here include:
    - Unit testing,
    - Mock testing and
    - Integration testing
- Provisioning is the next workstream, and this can be done in parallel. During Phase 2, the only provisioning topic is related to Enterprise connections; however, precisely what you tackle will depend on your specific requirements - i.e. if you do not need Enterprise connections, you will have no need to implement that workflow:
    - Enterprise Sign Up

- Profile Management will address advanced use cases for changes to a user's profile. We've found the most successful implementations address the following topic at this point during Phase 2, however precisely what you tackle will depend on your specific requirements (i.e. you may skip this workstream in this phase if you are not providing a user administration interface to admins of your customers' organization):
    - Organization Admin Portal
- Branding for MFA can be done in parallel with other work items, and with most customers would typically be handled by their branding team - though if you have no plans to support multi-factor authentication then there's no need to engage in Guardian multi-factor branding activities. However, as multi-factor is an industry recommendation in many cases, adding your brand is a recommended best practice at this time.
- With Logout we are adding some of the more complex options:
    - Single Logout
    - Federated Logout

Congratulations! Reaching this point you have integrated with Auth0 to provide API Authorization as well as advanced user Authentication, and are ready for Go-Live deployment to production (if you've not already done so via continuous integration). If you need to, now is the time to align your Auth0 production tenant via deployment automation, run any final QA in preparation for production release, and re-run your production check. As you move forward you'll want to keep a watch for Notifications from Auth0, which may contain important information that could impact your tenant(s) and/or project(s) going forward.

Phase 3

Phase 3 builds on the work conducted as part of Phase 2, and primarily deals with the more complex organizations that have more than one IDP for the individual organization. It also introduces some more specialized use cases – utilizing both standard out-of-box functionality, as well as specialized customization built using Auth0 out-of-box features. Phase 3 primarily focus on use cases which, though more specialized, we nevertheless see occur on a relatively frequent basis. Completing Phase 1 is a pre-cursor to Phase 3, though Phase 2 need not necessarily be a phase on which Phase 3 is predicated.

Utilizing Continuous Integration established in Phase 1 (as part of Deployment Automation), Phase 3 work can be taken into production in an accelerated fashion similar to Phase 2 - or at the very least be provided as part of an early adopter or Beta program. The diagram below (click to navigate) describes each of the Phase 3 workstreams with a number of topics in each.

In Phase 3, as in Phase 1 and Phase 2, there are a number of workstreams with a number of topics in each. The workstreams, topics and the order in which you address each is important, so we recommend you follow the guidance prescribed. That's not to say you can't or shouldn't tackle work in parallel: Progressive Profiling, for example, could be tackled independently and at the same time as Step-up Authentication.

Of all the phases, Phase 3 is the least prescribed: there are a variety of unconnected work stream topics which can be tackled independently – or not at all.

Planning: Phase 3 – Extended use cases for Authentication, Profile Management and Operations support

Workstreams								
Architecture	Separate Tenant for Multiple IDP Org							
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 Page	
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 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

Again, as with Phase 1 and Phase 2, in the majority of successful integration cases we've found that different teams tackle different streams, and that this can provide significant benefit: your design and development team(s) would typically tackle implementation whilst at the same time your branding team would tackle Auth0 asset customization thus reducing overall time to market.

- With Phase 3 and the complex organizations that have multiple IDP's, we need to discuss the concept of creating a separate Auth0 tenant for these organizations in Separate Tenant for Multiple IDP Org.
- In the Authentication workstream, we tackle the following items:
    - Connect to Separate Multiple IDP Org Tenant, and
    - Step-up Authentication
- In Profile Management, topics such as Progressive Profiling enable a rich user experience, whilst at the same time reducing user frustration by removing the need for extensive registration forms. Here are the topics we will address in profile management:
    - Progressive Profiling,
    - Deprovisioning with SCIM, and
    - Account Link Enterprise IDP to Database User
- Branding in phase 3 will cover customization of branding for specific organizations that have their own tenant and branding redirect pages:
    - Branding for Separate Tenant for Multiple IDP Org, and
    - Redirect Pages
- In Provisioning we start to look at some of the more complex provisioning for multi-tenant applications such as:
    - Self Signup for Users with Approval, and
    - Self-Signup new Organization and Admin User
- Providing a Companion Application (via specialized customization) can, in many cases, be a good secure alternative for use cases involving Impersonation – i.e. in cases where your support team(s) need to perform actions on behalf of a customer as part of your Operations infrastructure. You may also want to build out a Self Service Enterprise Connection Setup application for organizations to self-administer their own connection to their IDP.

Congratulations! Reaching this point you have integrated with Auth0 to support extended use cases and are ready for Go-Live deployment to production (if you've not already done so via continuous integration). If you need to, now is the time to align your Auth0 production tenant via deployment automation, run any final QA in preparation for production release, and re-run your production check. As you move forward you'll want to keep a watch for Notifications from Auth0, which may contain important information that could impact your tenant(s) and/or project(s) going forward.

The guidance provided describes our recommended strategy for integrating Auth0 in a B2B IAM project The guidance provided will be updated from time to time, and we recommend you check with our scenario guidance as you progress. If you require more detailed guidance regarding specific functionality and/or specific use case scenarios then we recommend you engage with the Professional Services team here at Auth0.

As some of this guidance is still being written, we have some more detailed documentation for B2B Multiple Organization Architecture (Multitenancy) that you can use to help decide how to approach the topics that address applications that are tailored to each organization they serve.