

McKesson – Biologics Portal Okta Integration Design Document

**Version**: 1.1

**Last Updated**: Jun 09, 2022

Table of Contents

[1. Document Control 3](#_Toc104890590)

[1.1. Revision History 3](#_Toc104890591)

[1.2. Document References 3](#_Toc104890592)

[2. Introduction 4](#_Toc104890593)

[2.1. Purpose 4](#_Toc104890594)

[2.2. Intended Audience 4](#_Toc104890595)

[2.3. Scope 4](#_Toc104890596)

[2.4. Acronyms 5](#_Toc104890597)

[2.5. Application Overview 5](#_Toc104890598)

[3. Application Integration Requirements 7](#_Toc104890599)

[3.1. Functional Requirements 7](#_Toc104890600)

[3.2. Non-Functional Requirements 9](#_Toc104890601)

[4. Solution Overview – To Be State 12](#_Toc104890602)

[4.1. Business Goals and Objectives 12](#_Toc104890603)

[4.2. Assumptions 12](#_Toc104890604)

[4.3. Pre-Requisites 12](#_Toc104890605)

[4.4. Architecture 13](#_Toc104890606)

[4.5. Data Model 15](#_Toc104890607)

[4.6. Use Cases 15](#_Toc104890608)

[4.7. Security 30](#_Toc104890609)

[5. Configuration Details 32](#_Toc104890610)

[5.1. Okta Tenant Details 32](#_Toc104890611)

[5.2. Application Details 33](#_Toc104890612)

[6. Traceability 38](#_Toc104890613)

[7. Appendix 39](#_Toc104890614)

[7.1. Call Recordings 39](#_Toc104890615)

[7.2. Application Architecture 39](#_Toc104890616)

Table of Figures

[Figure 1: Application Architecture 13](#_Toc104891234)

[Figure 2: External user registration flow 17](#_Toc104891235)

[Figure 3: Internal user registration flow 18](#_Toc104891236)

[Figure 4 : External user authentication flow 20](#_Toc104891237)

[Figure 5 : Internal user authentication flow 21](#_Toc104891238)

[Figure 6 : External user authorization flow 23](#_Toc104891239)

[Figure 7 : Internal user authorization flow 24](#_Toc104891240)

[Figure 8 : External user forgot password flow 25](#_Toc104891241)

[Figure 9 : External user change password flow 26](#_Toc104891242)

# Document Control

## Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Author | Approver | Reason for version |
| 1.0 | 05-31-2022 | EY |  | First Draft |
| 1.1 | 09-06-2022 | EY |  | Minor updates based on team reviews |
| 1.2 |  |  |  |  |
| 1.3 |  |  |  |  |
| 1.4 |  |  |  |  |

## Document References

|  |  |  |
| --- | --- | --- |
| Ref # | Referenced Item | Source |
| 1 | McKesson SSO Integration Questionnaires\_BIOLOGICSPortal\_v1.1 | [McKesson SSO Integration Questionnaires\_BiologicsPortal\_v1.1.xlsx](https://mckessoncorp.sharepoint.com/:x:/r/sites/GRPMcKIAM-OktaIntegration/Shared%20Documents/Jira%20High%20Priority%20Tickets/03%2004%20IPSEN%20and%20Biologics/01%20Requirement%20Gathering/IPSEN%20and%20Biologics/McKesson%20SSO%20Integration%20Questionnaires_BiologicsPortal_v1.1.xlsx?d=w561835be048c4fe5bbc2b32ad9413072&csf=1&web=1&e=MybjoN) |
| 2 | Okta Documentation | <https://help.okta.com/> |

# Introduction

This document elaborates the requirements, design, and configurations of Okta solution for Biologics Portal.

## Purpose

The purpose of this document is to create technical representation of functional requirements and flow of information across all the solution components responsible for user authentication and authorization.

This document helps intended audience to understand the high-level design involved in meeting the authentication and authorization requirements for Biologics Portal. This document consists of technical specifications, design and architecture, integration approach, and serves as a reference in system testing for the deployment of IAM solution.

## Intended Audience

Following is the intended audience of the Biologics application integration document:

1. Project Manager, to define tasks for phases & milestones
2. Architects, to define the implementation strategy
3. Application Developers, to define any custom applications needed
4. Business Analysts, to define user experience
5. Application testers, to define test cases
6. EAM Team, to configure and review Okta tenants and configurations

## Scope

### In-Scope

The following items are in scope:

1. Requirements for Okta integration with Biologics Portal (Listed in section [3. Application Integration Requirements](#_Application_Integration_Requirement))
2. Okta solution overview
3. Okta tenant integration details
4. Application integration details

### Out-of-Scope

The following items are out of scope:

1. Migration of existing application users to Okta B2B
2. Managing internal users in Active Directory or Okta B2E
3. Internal user onboarding/offboarding processes
4. Application side development activities

## Acronyms

| Acronym | Full form |
| --- | --- |
| B2B | Business-to-business |
| B2E | Business-to-employee |
| EAM | Enterprise Access Management |
| IAM | Identity and Access Management |
| IDP | Identity Provider |
| MFA | Multi Factor Authentication |
| OAuth | Open Authorization |
| OIDC | OpenID Connect |
| PKCE | Proof Key for Code Exchange |
| SAML | Security Assertion Markup Language |
| SP | Service Provider |
| SSO | Single Sign On |
| SSPR | Self Service Password Reset |

## Application Overview

Biologics Commercial portal is built for drugs manufacturers from Biologics, who are McKesson clients.

The portal is accessed by external and internal users where external users are all Biologics clients and internal users are McKesson Employees.

1. External users have 3 different personas/roles in Biologics Portal:
2. Patients: Patients uses drugs manufactured by Biologics
3. Providers (physicians who track patients/progress, office staff, nursing staff).
4. Manufacturers (users who are drugs manufacturers or sales representatives, etc.)
5. Internal users perform administrative roles such as initiate external user registration, validate and activate their account, etc.

### Current State

Not Applicable.

Biologics portal is fresh built application.

# Application Integration Requirements

## Functional Requirements

Functional requirements define the software functionality to be implemented in order to support business processes.

Following table captures the functional requirement for Biologics Portal.

| Req ID | Grouping | Requirement | Description | Owner |
| --- | --- | --- | --- | --- |
| FR-01 | User Management | Internal user migration | Internal users will be preloaded into Okta B2B and added to internal group | * App Team - Will follow McKesson’s existing process to import data into Okta B2B tenant. |
| FR-02 | User Management | External user migration | As the Biologics portal is newly built application, there is no existing external user base. | * NA |
| FR-03 | User Management | External user deactivation/ deprovision | Deactivate the account in Okta post 90 days of inactivity | * App Team – Functionality handled by portal team leveraging Okta API |
| FR-04 | Authentication | OIDC Integration | Biologics portal will integrate with Okta B2B tenant using OIDC PKCE flow. | * App Team- To enable application to support OIDC PKCE integration. * App Team- To share application endpoints for integration and required claims information * EAM Team- To share Okta OIDC endpoints, client credentials to integrate with portal |
| FR-05 | Authentication | IDP Discovery | Okta B2B tenant will be configured for IDP discovery to identify internal users and redirect them to Okta B2E for internal user authentication and MFA. | * EAM Team - To configure routing rules in Okta for IDP discovery |
| FR-06 | Authentication | External user login | Externaluser authentication and MFA will be handled by Okta B2B | * App Team- To share application endpoints for integration and required information * EAM Team- Integrate Biologics with Okta B2B using OIDC PKCE flow and configure required claims. |
| FR-07 | Authentication | Internal user login | Internal user authentication and MFA will be handled through Okta B2E using IDP discovery. | * EAM Team- Integrate Okta B2B with Okta B2E |
| FR-08 | Authorization | External User authorization | External User authorization will be based on Role/Persona’s stored in portal’s config DB and OIDC claims received from Okta B2B | * App Team- To implement authorization policy on application side |
| FR-09 | Authorization | Internal user authorization | Internal user authorization will be based on pre-register details available in portal’s config DB and OIDC claims received from Okta B2B | * App Team- To implement authorization policy on application side |
| FR-10 | Authentication | Attribute Mappings | The user attributes that need to be passed to the application as claims along with token response from Okta  *Note: Awaiting confirmation on exact attribute list from application team* | * App Team- To provide the list of the attributes that need to be enabled/mapped. * EAM Team- Configure required OIDC claims in Okta |
| FR-11 | MFA | External users MFA | External users MFA will be handled by Okta B2B | * EAM Team- To configure required MFA authenticators in Portal's B2B Okta tenant for external users. ‘Email’ authenticator required |
| FR-12 | MFA | Internal user MFA | Internal users MFA will be handled by Okta B2E | * Internal user MFA will be followed as per McKesson internal user policy |
| FR-13 | Password Reset | External user change password | External User- Change Password is required for external users only. This functionality will be available in the user profile page inside Biologics Portal. | * App Team- Functionality handled by portal team leveraging Okta API. |
| FR-14 | Password Reset | Internal user change password | Internal User- Change password link will be disabled for internal users’ login into Biologics Portal. | * Not applicable |
| FR-15 | Password Reset | External user forgot password | External User- Forgot Password is required for external users only. This functionality will be available on the portal’s login page. | * App Team- Functionality handled by portal leveraging Okta API |
| FR-16 | Password Reset | Internal user forgot password | Internal User- If an internal user tries to access Forgot password link, they will be notified that password cannot be reset from here. | * App Team- To set user notification |
| FR-17 | User Management | Okta API | * Following Okta APIs are required- * getpasswordpolicy * getuser: /api/v1/users/${userId} * changepassword: /api/v1/users/${userId}/credentials/change\_password * resetpassword: /api/v1/users/${userId}/lifecycle/reset\_password * createuser: /api/v1/users * deactivateuser: /api/v1/users/{{userId}}/lifecycle/deactivate | * EAM Team- To provide API endpoint and API token to invoke Okta APIs |

## Non-Functional Requirements

Following table captures the non-functional requirement for Biologics Portal.

| Req ID | Grouping | Requirement | Description | Owner |
| --- | --- | --- | --- | --- |
| NFR-01 | Infrastructure | Infrastructure to host to-be solution | Biologics Portal: Hosted in Azure Cloud  Okta tenant: Vendor managed infrastructure | * NA |
| NFR-01 | Security | Secure protocols for user interfaces | Okta login page must transmit data through HTTPS. | * NA |
| NFR-02 | Security | Revoke access of disabled user. | The solution must revoke user access and disable the user in Okta B2E when the user is disabled in McKesson AD. | * EAM Team- Manage functionality with Okta B2E |
| NFR-03 | Security | Logging and Reporting | Okta administrators can login to Okta dashboard and access system logs and reports | * NA |
| NFR-04 | Accessibility | Portal accessibility over network | Portal should be accessible over internet as well as intranet. Since portal is accessed by both external and internal users. | * App Team- Managing internet facing application deployment in Azure cloud |
| NFR-05 | Compliance | Enable end user login through unique login IDs | The solution must be secured with individual, unique login IDs, to verify that an individual is authorized to access the system. | * App Team- Store unique userlogin for users during registration |
| NFR-06 | Segregation of Duties | Least privileged access | Okta should support role-based access control so that users are assigned the least privilege for Okta admin dashboard or APIs | * EAM Team- To assign administrative users with required Okta admin roles |
| NFR-07 | Segregation of Duties | Restrict access to global administrator role | Access to Okta system administrator role should be restricted based on principle of least privilege. | * EAM Team- To assign global admin role to limited and required users |
| NFR-08 | Performance | Okta tenant performance | Okta tenant performance is managed by Okta vendor | * NA |
| NFR-09 | Business Continuity | High Availability Requirements | Okta tenant high availability is managed by Okta vendor | * NA |
| NFR-10 | Business Continuity | Backup Requirements | Okta tenant backup requirement is managed by Okta vendor | * NA |
| NFR-11 | Business Continuity | Archiving Requirements | Okta system log archiving will be supported as per standard Okta specification. | * NA |

# Solution Overview – To Be State

## Business Goals and Objectives

Biologics portal will be integrated with Okta to provide users with self-registration, self-service features, login, and MFA functionality.

## Assumptions

There are several assumptions made in this design. If these are not accurate or misrepresented, there may be impact to the overall Okta Integration.

|  |  |  |
| --- | --- | --- |
| **No.** | **Assumption** | **Description** |
| 1 | Application will be made OIDC compliant to integrate with Okta | Application does not support federation by default. The application team will develop a custom code to make the application OIDC compliant. |
| 2 | User Migration | Application team will migrate internal users (as explained in Requirements section 3.1 [Functionaol Requirement](#_Functional_Requirements) before integrating the application with Okta. |
| 3 | Internal Users login and MFA policy | Login journey and MFA policies for Internal users accessing this application will be as per existing B2E standards and configurations and no changes to existing B2E setup will be made as part of this integration. |
| 4 | User notification templates customization | Template customization will be done as per Okta out of box capabilities. |

## Pre-Requisites

### Okta Tenant

New Okta tenants will be procured to integrate with Biologics portal’s different environment.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Apps Environment | Dev | QA | UAT | Prod |
| Okta B2B Tenant | UAT/Preview Tenant | UAT/Preview Tenant | UAT/Preview Tenant | Prod Tenant |
| Okta B2B Tenant URL | [mckb2bbiologics-qa.oktapreview.com](https://urldefense.com/v3/__http:/mckb2bbiologics-qa.oktapreview.com__;!!KMayzP4JbQ!cVHtDRMaRsaIF66ms_wpsRVL4AW32YeiaUVnPE5MNUKDtNP_QNwgQ4Gg7cKn2C8t8xxn5A-afwibO-pZYoaFhA$) | [mckb2bbiologics-qa.oktapreview.com](https://urldefense.com/v3/__http:/mckb2bbiologics-qa.oktapreview.com__;!!KMayzP4JbQ!cVHtDRMaRsaIF66ms_wpsRVL4AW32YeiaUVnPE5MNUKDtNP_QNwgQ4Gg7cKn2C8t8xxn5A-afwibO-pZYoaFhA$) | [mckb2bbiologics-qa.oktapreview.com](https://urldefense.com/v3/__http:/mckb2bbiologics-qa.oktapreview.com__;!!KMayzP4JbQ!cVHtDRMaRsaIF66ms_wpsRVL4AW32YeiaUVnPE5MNUKDtNP_QNwgQ4Gg7cKn2C8t8xxn5A-afwibO-pZYoaFhA$) | [mckb2bbiologics.okta.com](https://urldefense.com/v3/__http:/mckb2bbiologics.okta.com__;!!KMayzP4JbQ!cVHtDRMaRsaIF66ms_wpsRVL4AW32YeiaUVnPE5MNUKDtNP_QNwgQ4Gg7cKn2C8t8xxn5A-afwibO-oUn2lF7w$) |

### Application-level changes

Biologics Portal does not support federation integration by default. Hence, application team has developed a custom code to enable the application to be OIDC Compliant.

The custom code has been deployed in Development environment and application team will progress these changes to higher environments i.e., QA, UAT and Prod, once tested successfully in Development environment.

### User Migration to Okta

External users: NA (All new users)

Internal users: Application team will follow McKesson process to import authorized internal user’s details into Okta B2B tenant.

## Architecture

### Application Architecture

Biologics portal will be integrated with Okta for user authentication and authorization.

|  |  |
| --- | --- |
| App Feature | Details |
| App Name | Biologics Commercial Portal |
| Hosted Environment | Azure Kubernetes Service |
| Built Language | ReactJS |
| Application Access | External users & Internal users |
| Accessibility | Internet |

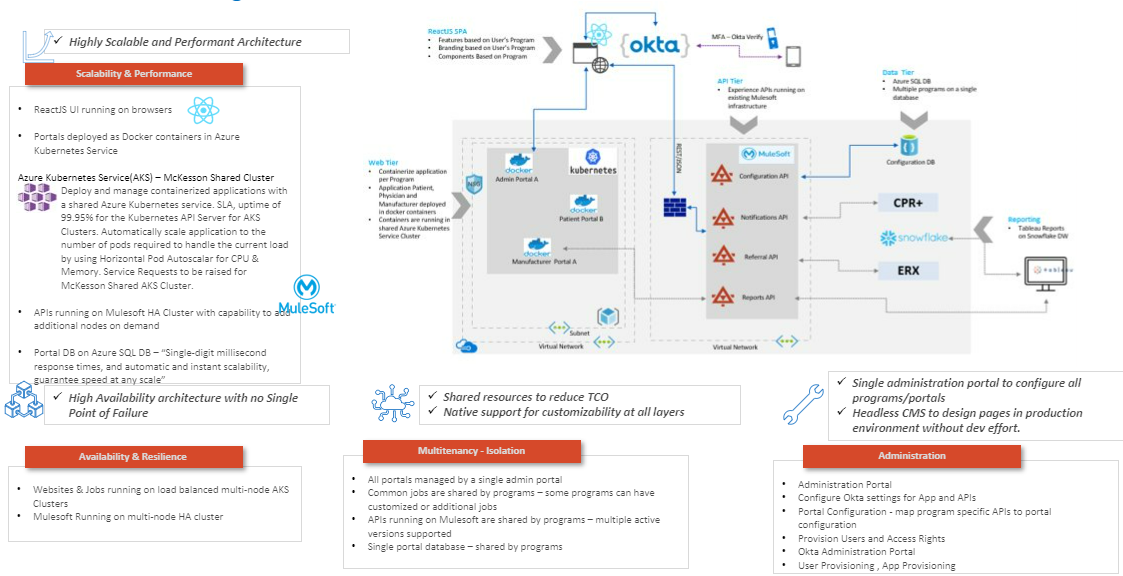


Figure 1: Application Architecture

*Note: This architecture diagram is provided by application team for reference.*

### Okta Solution Architecture

#### System Components

Below table captures description of different components and actors of IAM logical view.

|  |  |  |
| --- | --- | --- |
| **Sl. No.** | **Component** | **Description** |
| 1 | Users | Biologics portal is accessed by external and internal users |
| 2 | Biologics Portal | Biologics Commercial Portal is web application built for drug manufactures who are clients of McKesson |
| 3 | Okta B2B Tenant | New Okta tenant will be procured to integrate with Biologics Portal |
| 4 | Okta B2E Tenant | Existing Okta B2E tenant will be integrated with Okta B2B for internal user authentication |
| 5 | McKesson AD | McKesson’s internal users are stored in McKesson AD. Okta B2E integrated with McKesson AD for internal user authentication. |

#### Logical View



Figure 2 : Logical View for Biologics Portal

#### Process Flows

|  |  |
| --- | --- |
| **Steps#** | **Description** |
| 1 | User will try to access portal URL in browser through internet. |
| 2 | Portal is ReactJS based application and will be integrated with Okta using OIDC PKCE integration flow. Portal will send authentication request to Okta OIDC endpoint. |
| 3 | User will be prompted to enter user login details on Okta login page. |
| 4 | Routing rules will be configured on Okta for IDP discovery |
| * 1. Based on routing rule, internal users will be redirected to Okta B2E for authentication |
| * 1. External users will be authenticated locally with Okta B2B directory |
| 5 | Users will be prompted to enter login password. |
| * 1. Okta B2E will validate internal user login credential and applicable MFA. |
| * 1. Okta B2B will validate external user login credential and applicable MFA. |
| 6 | In case of internal user, Okta B2E will send authentication response to Okta B2E through SAML assertion. Okta B2B will validate SAML assertion with pre-loaded internal users accounts. |
| 7 | Okta B2B will generates access token, ID token and refresh token and will send them to portal. |
| 8 | Portal will authorize user based on OIDC claims and user details available in portal’s config DB and user will get access to portal dashboard. |

## Data Model

Below user attributes will be captured in Okta B2B for user authentication and authorization.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sl. No.** | **Attribute name used in Portal** | **Type** | **Attribute name in Okta** | **Description** |
| 1 | User Login | String | User Login |  |
| 2 | First Name | String |  |  |
| 3 | Last Name | String |  |  |
| 4 | Email | String |  |  |
| 5 | Mobile Number | String |  |  |

## Use Cases

### User Registration

#### UC01- External User registration

|  |  |
| --- | --- |
| Use Case ID: | UC01 |
| **Use Case Name:** | External User Registration to Biologics Portal |
| **Description:** | External user account creation in Okta and Config DB via Biologics Portal registration feature |
| **Primary Actor(s):** | External User |
| **Secondary Actor(s):** | Internal User (Portal Admin) |
| **Trigger:** | Portal admin initiates new user registration process |
| **Preconditions:** | 1. Internal user acting as admin should be available in Okta and able to login to Biologics portal 2. Admin should have required external user account details to initiate registration process 3. Biologics Portal has configured required API endpoint and API token to invoke Okta createuser API |
| **Process Flow:** | 1. Admin will initiate external user registration on portal using user’s details (such as first name, last name, email, mobile number, and other required details) and send invitation code to external user. This will create record in portal’s config DB. 2. Email and text message will be delivered to user with 6-digit code along with registration URL. 3. User will access registration URL and enters 6-digit code, verification done by Portal itself. Few details filled by admin cannot be edited by users such as userlogin/email. 4. User can add required details, password, consent and submit the registration form. 5. Portal will create user profile in portal's config DB as well as in Okta domain. 6. Additionally, Portal will trigger an email to admin and admin can see all the registered user who are not activated. 7. Admin will validate the user details as per persona/role and authorize/activate. 8. Once activated, user gets welcome email with login link to portal. |
| **Post Conditions:** | 1. External user account is created in Portal’s config DB. 2. External user account is created in Okta B2B directory. |
| **Exception to the Flow** | 1. If user enters incorrect 6-digit verification code- Portal notify user with appropriate message. 2. If user enters userlogin not unique in config DB- Portal notify user with appropriate message. 3. If user enters userlogin in email format with domain @mckesson.com- Portal notify user with appropriate message. 4. If user access Okta’s email verification link post expiry- |



Figure 3: External user registration flow

#### UC02- Internal User Registration

|  |  |
| --- | --- |
| Use Case ID: | UC02 |
| **Use Case Name:** | Internal User Registration to Biologics Portal |
| **Description:** | Internal user account creation in Config DB Biologics Portal registration feature |
| **Primary Actor(s):** | Internal User |
| **Secondary Actor(s):** | Internal User (Portal Admin) |
| **Trigger:** | Portal admin initiates new user registration process |
| **Preconditions:** | 1. Internal user acting as admin should be available in Okta and able to login to Biologics portal 2. Admin should have required internal user account details to initiate registration process 3. Biologics Portal has configured required API endpoint and API token to invoke Okta createuser API |
| **Process Flow:** | 1. Admin will initiate internal user registration on portal from admin module using user’s details (such as first name, last name, email, mobile number, and other required details) and send invitation code to internal user. These details will be stored in the portal's config DB.  2. Email and text message will be delivered to the user with 6-digit code along with registration URL  3. User will access registration URL and enters 6-digit code, verification done by Portal itself. Few details filled in by admin cannot be edited by users such as userlogin/email.  4. User can add more details, consent, and submit the registration form. At this stage portal will not call Okta APIs to create user since internal users are already available in Okta B2E.  5. Portal will create user profile in portal's config DB.  6. Additionally, portal will trigger an email to admin and admin can see all the registered users who are not activated.  7. Admin will validate the user as per role and authorize/activate.  8. Once activated, the user gets a welcome page and login link to portal. |
| **Post Conditions:** | 1. Internal user account is created in Portal’s config DB. |
| **Exception to the Flow** | 1. If user enters incorrect 6-digit verification code- Portal notify user with appropriate message. 2. If user enters userlogin not unique in config DB- Portal notify user with appropriate message. 3. If user enters userlogin in email format with different domain than @mckesson.com- Portal notify user with appropriate message. |



Figure 4: Internal user registration flow

### Groups Assignment

Internal and external users should be grouped in Okta B2B with proper naming convention.

#### UC03- External user group assignment

|  |  |
| --- | --- |
| Use Case ID: | UC03 |
| **Use Case Name:** | User group assignment |
| **Description:** | User group assignment is required for external users |
| **Primary Actor(s):** | External User |
| **Secondary Actor(s):** | NA |
| **Trigger:** | 1. External user account is created in Okta B2B |
| **Preconditions:** | 1. Okta group is created for external users in Okta B2B |
| **Process Flow:** | 1. User account is created in Okta B2B using Okta API 2. Biologics portal will call another Okta API to assign user into external user Biologics group |
| **Post Conditions:** | 1. External user assigned to external Biologics group 2. Okta B2B can send group claim in OIDC token to Biologics portal |
| **Exception to the Flow** | NA |

#### UC04- Internal user group assignment

|  |  |
| --- | --- |
| Use Case ID: | UC04 |
| **Use Case Name:** | User group assignment |
| **Description:** | User group assignment is required for internal users |
| **Primary Actor(s):** | Internal User |
| **Secondary Actor(s):** | NA |
| **Trigger:** | 1. Internal user account is created in Okta B2B |
| **Preconditions:** | 1. Okta group is created for internal users in Okta B2B |
| **Process Flow:** | 1. User basic details are loaded into in Okta B2B through Org2Org connect 2. Okta B2B has configured group assignment for users coming from Okta B2E IDP |
| **Post Conditions:** | 1. Internal user assigned to internal Biologics group 2. Okta B2B can send group claim in OIDC token to Biologics portal |
| **Exception to the Flow** | NA |

### User Authentication

Biologics commercial portal is being used by internal and external users.

#### UC05- External User Authentication

|  |  |
| --- | --- |
| Use Case ID: | UC05 |
| **Use Case Name:** | External User Authentication |
| **Description:** | External user account authentication to Biologics Portal |
| **Primary Actor(s):** | External User |
| **Secondary Actor(s):** | NA |
| **Trigger:** | External user attempt to access Biologics portal login URL |
| **Preconditions:** | 1. Biologics portal is integrated with Okta B2B for user authentication 2. External user login credential is available in Okta B2B |
| **Process Flow:** | 1. User will try to access portal URL in browser through internet 2. Portal is a ReactJS based application and will be integrated with Okta using OIDC PKCE integration flow. Portal will send authentication request to Okta OIDC endpoint. 3. Users will be prompted to enter user login details on Okta login page. Okta B2B authenticates user login credential and MFA. 4. Okta B2B will generate access token, ID token and refresh token and will send them to portal. 5. Portal will authorize user based on OIDC claims and user details available in portal’s config DB and user will get access to portal dashboard. |
| **Post Conditions:** | 1. External user gets access to portal features according to his role/persona |
| **Exception to the Flow** | 1. If user enters userlogin in email format with @mckesson.com domain- Okta B2B treat them as internal user and redirect to Okta B2E for authentication. 2. If user enters incorrect login credential- Okta B2B notify user with appropriate message. |



Figure 5 : External user authentication flow

#### UC06- Internal User Authentication

|  |  |
| --- | --- |
| Use Case ID: | UC06 |
| **Use Case Name:** | Internal User Authentication |
| **Description:** | Internal user account authentication to Biologics Portal |
| **Primary Actor(s):** | Internal User |
| **Secondary Actor(s):** | NA |
| **Trigger:** | Internal user attempt to access Biologics portal login URL |
| **Preconditions:** | 1. Biologics portal is integrated with Okta B2B for user authentication 2. Okta B2B is integrated with Okta B2E using Org2Org connector 3. Internal user login credential is available in Okta B2E 4. Internal user basic details are pre-loaded into Okta B2B |
| **Process Flow:** | 1. Internal users will try to access portal URL in browser through internet/intranet. 2. Portal is a ReactJS based application and will be integrated with Okta using OIDC PKCE integration flow. Portal will send authentication request to Okta OIDC endpoint. 3. Users will be prompted to enter their registered email address on Okta login page. 4. Routing rules will be configured on Okta for IDP discovery. Based on routing rules, internal users will be redirected to Okta B2E for authentication. 5. Users will be prompted to enter login credential. Okta B2E will validate internal user login credentials and applicable MFA. 6. Okta B2E will send authentication response to Okta B2B through SAML assertion. Okta B2B will validate SAML assertion with pre-loaded internal users accounts. 7. Okta B2B will generate access token, ID token and refresh token and will send them to portal. 8. Portal will authorize user based on OIDC claims and user details available in portal’s config DB and user will get access to portal dashboard. |
| **Post Conditions:** | 1. Internal user gets access to portal features according to his details stored in config DB |
| **Exception to the Flow** | 1. If user enters incorrect login credential- Okta B2E notify user with appropriate message. 2. If user enters userlogin in email format with domain another than @mckesson.com domain- Okta B2B treat them as external user. |



Figure 6 : Internal user authentication flow

### User Authorization

Biologics portal will handle user authorization based on user details stored in portal’s config DB and OIDC claims received from Okta B2B.

#### UC07- External User Authorization

Portal will have user’s details in config DB through registration process. It will authorize users based on their persona.

External users have 3 different personas stored in portal’s config DB:

1. Patients
2. Providers (physicians who track patients/progress, office staff, nursing staff).
3. Manufacturers (user who are drugs manufacturers or sales representative, etc.)

Additionally, portal will check claims received from Okta B2B. Portal will fetch userlogin from OIDC claim and put it as actor ID in config DB for further login validation.

|  |  |  |
| --- | --- | --- |
| Sl. No. | Okta OIDC Claims | Description |
| 1 | FirstName | First name of user in Okta B2B |
| 2 | Last Name | Last name of user in Okta B2B |
| 3 | Email | Email of user in Okta B2B |

*Note: Awaiting application team’s response for exact claims requirement*

|  |  |
| --- | --- |
| Use Case ID: | UC07 |
| **Use Case Name:** | External User Authorization |
| **Description:** | External user account authorization to Biologics Portal |
| **Primary Actor(s):** | External User |
| **Secondary Actor(s):** | NA |
| **Trigger:** | External user attempt to access Biologics portal login URL |
| **Preconditions:** | 1. User authentication flow is completed and Okta B2B has responded with token to Biologics portal 2. External user details are pre-registered in portal’s config DB |
| **Process Flow:** | 1. External user will access Portal URL, authentication completed 2. Okta B2B will responses with access token, ID token and Refresh token 3. Portal will fetch OIDC claims from the received token 4. Portal will fetch user details from config DB and update/map userlogin with actor ID in user table 5. Portal executes authorization policy based on user’s details fetched from config DB 6. Portal will give access to the user as per the Role/Persona |
| **Post Conditions:** | 1. External user gets access to portal |
| **Exception to the Flow** | 1. If user details not available in config DB- Portal notify for authorization error. |



Figure 7 : External user authorization flow

#### UC08- Internal User Authorization

Portal will have user’s details in config DB through registration process to authorize user access.

Additionally, portal will fetch userlogin from OIDC claim and put it as actor ID in config DB for further login validation.

|  |  |  |
| --- | --- | --- |
| **Sl. No.** | **Okta OIDC Claims** | **Description** |
| 1 | First name | First name of user in Okta B2B |
| 2 | Last Name | Last name of user in Okta B2B |
| 3 | Email | Email of user in Okta B2B |

*Note: Awaiting application team’s response for exact claims requirement*

|  |  |
| --- | --- |
| Use Case ID: | UC08 |
| **Use Case Name:** | Internal User Authorization |
| **Description:** | Internal user account authorization to Biologics Portal |
| **Primary Actor(s):** | Internal User |
| **Secondary Actor(s):** | NA |
| **Trigger:** | Internal user attempt to access Biologics portal login URL |
| **Preconditions:** | 1. User authentication flow is completed and Okta B2B has responded with token to Biologics portal 2. Internal user details are pre-registered in portal’s config DB |
| **Process Flow:** | 1. Internal user will access Portal URL 2. Okta B2B will responses with access token, ID token and Refresh token 3. Portal will fetch OIDC claims from the received token 4. Portal will fetch user details from config DB and update/map userlogin with actor ID in user table 5. Portal executes authorization policy based on user’s details fetched from config DB 6. Portal will give access to the user |
| **Post Conditions:** | 1. Internal user gets access to portal |
| **Exception to the Flow** | 1. If user details not available in config DB- Portal notify for authorization error. |



Figure 8 : Internal user authorization flow

### UC09- Forgot Password

|  |  |
| --- | --- |
| Use Case ID: | UC09 |
| **Use Case Name:** | Forgot Password |
| **Description:** | Self service password reset or forgot password feature in Biologics Portal |
| **Primary Actor(s):** | External User |
| **Secondary Actor(s):** | NA |
| **Trigger:** | External user attempt to forgot password link on Biologics portal login page |
| **Preconditions:** | 1. Biologics Portal has configured required API endpoint and API token to invoke Okta resetpassword API 2. User is registered to access Biologics portal |
| **Process Flow:** | 1. Users can find Forgot password link on portal’s login page. 2. Users will be prompted to enter userlogin on forgot password page. 3. Portal will verify if the entered user login is for an external user. 4. Portal will use Okta API to send password reset email to user to registered email address. 5. Users follows password reset link in email notification and must verify with registered security questions to reset the password. |
| **Post Conditions:** | 1. External user password is reset, and he/she can login to Biologics portal with new password |
| **Exception to the Flow** | 1. If entered user login is not present in config DB or Okta B2B- Portal notify user with appropriate message. 2. If entered user login ha domain @mckesson.com - portal will notify user that their password cannot be reset from here. 3. If entered new password does not match with defined password policy- Portal notify user with appropriate message |



Figure 9 : External user forgot password flow

### UC10- Change password

|  |  |
| --- | --- |
| Use Case ID: | UC10 |
| **Use Case Name:** | Change Password |
| **Description:** | Change password feature in user profile page of Biologics Portal |
| **Primary Actor(s):** | External User |
| **Secondary Actor(s):** | NA |
| **Trigger:** | External user attempt to change/update existing password in user profile page inside Biologics portal |
| **Preconditions:** | 1. Biologics Portal has configured required API endpoint and API token to invoke Okta change password API 2. User is registered to access Biologics portal |
| **Process Flow:** | 1. Users can find change password link on user profile page post login to portal. 2. This link is visible to external users and disabled for internal users. 3. Users will be prompted to enter old password and new password. 4. Portal will use Okta APIs to validate old password, validate password policy and set new password for users. |
| **Post Conditions:** | 1. External user password is changed, and he/she can login to Biologics portal with new password |
| **Exception to the Flow** | 1. If logged in user is internal user, he/she will not find change password link in user profile. 2. If entered old password does not match with registered password in Okta B2B- Portal notify user with appropriate message 3. If entered new password does not match with defined password policy- Portal notify user with appropriate message |



Figure 10 : External user change password flow

### Multifactor Authentication

Multifactor authentication (MFA) provides a mechanism to protect applications by requiring additional information when logging into the application that cannot be stolen in the same way that a password can.

Okta’s MFA implementation complements login and password with a 2nd factor. The setup comprises of:

1. Selection of additional factors, such as Okta Verify Token, Okta Verify Push, SMS, Voice Call, FIDO, or third-party integrations
2. Setup of end-user multifactor enrollment policies

|  |  |  |  |
| --- | --- | --- | --- |
| Sl. No. | User Type | Okta Tenant | MFA Authenticators |
| 1 | Internal User | Okta B2E | Mckesson Policy |
| 2 | External User | Okta B2B | Email |

*Note: Awaiting confirmation from app team on require MFA authenticators for external users.*

#### UC11- External User MFA

|  |  |
| --- | --- |
| Use Case ID: | UC11 |
| **Use Case Name:** | External user MFA |
| **Description:** | Okta B2B will prompt MFA to external user during login to Biologics Portal |
| **Primary Actor(s):** | External User |
| **Secondary Actor(s):** | NA |
| **Trigger:** | External user login to Biologics portal using userlogin and password |
| **Preconditions:** | 1. Okta B2B has enabled required MFA authenticators 2. User is enrolled for MFA 3. User authenticated using userlogin and password |
| **Process Flow:** | 1. Post successful user authenticatation using userlogin and password, Okta B2B prompts for MFA 2. User will get MFA prompt with his/her enrolled MFA authenticators 3. User selects any one authenticator and proceed with verification. 4. Post verification, Okta B2B sends access token to Biologics Portal. |
| **Post Conditions:** | 1. Authentication response is passed to Biologics portal and Biologics portal can act on authorization of user. |
| **Exception to the Flow** | 1. If logged in user is not enrolled for MFA- external user will get option to enroll for MFA authenticator enabled for Biologics portal 2. If logged in user is unable to verify with enrolled MFA authenticators- they have to contact helpdesk for restting enrolled MFA authenticators. |



Figure 11 : External user MFA flow

#### UC12- Internal User MFA

|  |  |
| --- | --- |
| Use Case ID: | UC12 |
| **Use Case Name:** | Internal user MFA |
| **Description:** | Okta B2B will prompt MFA to Internal user during login to Biologics Portal |
| **Primary Actor(s):** | Internal User |
| **Secondary Actor(s):** | NA |
| **Trigger:** | Internal user login to Biologics portal using userlogin and password |
| **Preconditions:** | 1. Okta B2E has enabled required MFA authenticators 2. User is enrolled for MFA 3. User authenticated using userlogin and password |
| **Process Flow:** | 1. Post successful user authenticatation using userlogin and password, Okta B2E prompts for MFA 2. User will get MFA prompt with his/her enrolled MFA authenticators 3. User selects any one authenticator and proceed with verification. 4. Post verification, Okta B2E sends SAML response to Okta B2B. |
| **Post Conditions:** | 1. Okta B2B receives SAML response from Okta B2E and act upon user authentication step. |
| **Exception to the Flow** | 1. If logged in user is not enrolled for MFA- external user will get option to enroll for MFA authenticator enabled for Biologics portal 2. If logged in user is unable to verify with enrolled MFA authenticators- they have to contact helpdesk for restting enrolled MFA authenticators. |



Figure 12 : Internal user MFA

## Security

### End-User Communication

The email communication sent by Okta as part of self-service flows can be branded and customized for the application. The communication will follow a consistent template across all applications.

The following email templates are required to be branded:

1. User Creation
2. User activation
3. Account Password Reset
4. Password Reset by Admin
5. Account Lockout Self-Service
6. MFA Enrolment Success
7. MFA Reset

*Please note: Listed templates are indicative and application team will be sharing required templates to configure at Okta end.*

### User Sessions

There will be three types of session generated for user and stored in browser.

1. **Okta Session:** Okta is also acting as IDP for Biologics portal. Okta will generate cookies-based session to store user information to track and facilitate interactions between the user and the Okta tenant. The IdP session is active until the user signs out from Okta or when the session expires, based on the session policies.
2. **Application session:** The application session is created by the portal after the user is authenticated. This session uses cookies to store user app-specific information to track and facilitate interactions between the user and the app.

The following session times provide an additional security measure when using the Okta solution:

|  |  |  |
| --- | --- | --- |
| **Lifetime** | **Details** | **Configuration** |
| Okta session  lifetime | This is determined by Okta sign-on policy and dictates whether a user should be prompted to sign-in when trying to access Okta-protected applications or resources. | Okta Standard- 2 hours or customizable as per the app requirements. |
| OAuth token  lifetime | Access token lifetime and refresh token lifetime is determined by access policy on authorization server and dictates whether a user should be prompted to sign-in when trying to validate and use Okta-generated tokens | ID token value is 60 min. Access token standard is 5 min to 24 hours and preference is to keep them short lived. Refresh token can be set to at least 10 minutes to unlimited. Standard practice is number of days but varies by industry |
| MFA factor lifetime | MFA factor lifetime is determined by Okta sign-on policy and dictates whether a user should be prompted to validate their MFA again if their MFA session has expired | Okta Standard or customizable as per the app requirements. |

### Logging and Reporting

Portal will use Okta system log API /api/v1/logs to fetch user activity logs and capture in portal’s log table.

Administrators can view and analyze statistics related to authentication requests. Following reports will be available for analysis.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Component Name** | **Log Name** | **Enabled in Production** | **Retention (In days/size)** | **To be sent for archival(Y/N)** | **Duration** |
| Okta B2B | System logs | Y | 90 days |  |  |

# Configuration Details

## Okta Tenant Details

The below tables assumed Okta behaves as IDP and Application as SP. In case, this is reversed, configurations should be revered.

| Identity Provider Federation | Description | QA | Prod |
| --- | --- | --- | --- |
| *SAML Integration* | | | |
| Display Name |  |  |  |
| Entity ID / Connection ID: | *Unique identifier of Identity provider (Okta)* |  |  |
| Protocol supported |  |  |  |
| Single Sign On (SSO) Endpoint URL |  |  |  |
| Single Logout (SLO) Endpoint URL |  |  |  |
| Federation Metadata | *An XML document describes a SAML deployment (EntityID, End point URLs, and cryptographic certificates) of Identity provider (Okta)* |  |  |
| Signing Algorithm | *Cryptographic algorithm used to digitally sign the SAML assertion* |  |  |
| X509 Certificate used to sign SAML assertion | *Save it a .cer file to import into your system* |  |  |
| *OIDC/OAuth 2.0 Integration* | | | |
| Display Name |  |  |  |
| Token Endpoint Base URL | *Base URL of identity provider (Okta)* | <https://biologics-portal-manufacturer-ui.dev.aks.west.us.mckesson.com/>login/callback |  |
| Protocol supported | *OIDC* |  |  |
| *Open ID Connect Metadata Endpoint* | *Web address of a document (JSON) that describes a OIDC deployment details of identity provider (Okta)* |  |  |
| *OAuth Token Endpoint* | *Web address where client (application) sends a request to exchange authorization code with an access token and ID token* |  |  |
| OAuth Token Revocation Endpoint | *Web address where client (application) sends a request to revoke an obtained access token or ID token* |  |  |
| JWKS Endpoint Path for id\_token | *Web address that contains a set of public keys that are used by identity provider (Okta) to digitally sign the OIDC tokens* |  |  |

## Application Details

### Application Generic Information

| Application General Information | Description | Responses |
| --- | --- | --- |
| Application Name | *Name of the application* | Biologics Commercial Portal |
| Application Description |  | Application is built for Drugs manufacturer- client of McKesson apart from Ipsen-clients of McKesson |
| Business Owner | *Name, LDAP ID, Email, Phone, Title* |  |
| Application Owner(s) | *Name, LDAP ID, Email, Phone, Title* | Brandon Tom |
| Vendor Contact (if applicable) | *Name, LDAP ID, Email, Phone, Title* |  |
| Business Unit | *Name of business unit or department function* | Bio\_Pharmacy\_DevOps |
| Data classification | *Select one classification level from below options:*  *Restricted*  *Confidential*  *Internal use*  *Public* |  |
| Types of users accessing Application | *Select one or multiple options from below:* | Internal users,  External users have 3 different persona-  a. Patients b. Providers (physicians who track patients/progress, office staff, nursing staff).  c. manufacturer (user who are drugs manufacturer or sales representative, etc.) |
| Type of Network  (Network from which application is accessed) | *Select one option from below:*  *Internal*  *External*  *Both internal and external* | Internet |
| Application hosting infrastructure | *Select one option from below:*  *On-premises –Datacenter*  *Cloud*  *SaaS* | Azure Cloud, accessible over internet |
| Estimated number of application Internal users | *Select one option from below:*  *100*  *100-999*  *1000-9999*  *10000+* | Internal user <100 |
| Estimated number of application External users | *Select one option from below:*  *100*  *100-999*  *1000-9999*  *10000+* | External user <2000 |
| Application platform | *Select one or multiple options from below:*  *Web-based*  *Desktop application*  *Mobile application* | Web-based |
| Lifecycle of application | *Select one or multiple options from below:*  *Dev* *QA* *Prod* | Dev, QA, Prod |
| Application Compliance category | *Select one option from below:*  *SOX Compliant*  *PCI*  *PII* *Contains sensitive data* *None* | PII |
| If SurePass MFA enabled for this application? | *Select one option from below:*  *Yes*  *No* | NO |
| Requested start date of application's QA environment integration with Okta QA |  | Application team need to confirm |
| Requested start date of application's Prod environment integration with Okta Production |  | 3 |
| Does the application has privileged access?  (ex: Accessed by admins) | *Select one option from below:*  *Yes*  *No* | Yes |
| Basic Test Case | *Specify URL used by end users, user ids, expected page. These details will be used for testing integration.* | NA |

### Application Federation Information

|  |  |  |  |
| --- | --- | --- | --- |
| **Service Provider details** | **Description** | **Responses** | |
| QA | Prod |
| *SAML Based Integration* | | | |
| Do you know if the application supports - SP Initiated as well as IdP Initiated federation? | *If both modes are supported, SP initiated is preferred as IdP initiated will not provide deep linking.* | NA | NA |
| Do you have SP Metadata file or URL? | *If yes, please attach it as a link here* | NA | NA |
| Entity ID / Connection ID: | *Provide a user-friendly name to identify service provider.*  *Example: Foobar.com* | NA | NA |
| ACS (Assertion Consumer Service) Endpoint URL |  | NA | NA |
| Do you want assertion to be signed? | *Yes/No*  *Recommended (Standard): Yes* | NA | NA |
| Do you want to send signed authentication request? | *Yes/No*  *If Yes, SP’s signing certificate is required, either through Metadata or separately.*  *Signing Algorithm supported: SHA256withRSA* | NA | NA |
| Does the application support Single Log Out (SLO)? If yes, please provide SLO endpoint URL. | *If after logout, application wants to send user to specific URL, please provide that URL.* | NA | NA |
| Requested claims / SAML Attributes | *Available claims: email, UPN, first name, last name* | NA | NA |
| Name pattern groups used by this application for authorization. | *This will return all user groups starting with this pattern.* | NA | NA |
| Does application has privileged access (accessed by admins)? If yes, then provide group information that admins are part of. | *Select one option from below:*  *Yes*  *No* | NA | NA |
| Do you want Okta to restrict users based on membership to groups used by this application? | *Only those users who belong to specified groups will be authorized.* | Yes | Yes |
| Name Id format | Select one option from below:  *Unspecified*  *Email address*  *Transient*  *Persistent* | NA | NA |
| What is the Assertion Attribute name in the authentication response that identifies the user ID? | Select one option from below:  *LDAP ID*  *email address* | NA | NA |
| Require SAML Token Encryption: | *Select one option from below:*  *Yes, No* | NA | NA |
| Secure Hash Algorithm: | *Only SHA256 is supported.*  *SHA1 is not supported.* | NA | NA |
| Assertion validity period: Before and After | *Defaults: Before = 5 minutes and After = 5 minutes* | NA | NA |
| *OIDC/OAuth2.0 Based Integration* | | | |
| Client Name | *Unique Name for application in Okta* | TBD | Biologics Portal |
| Redirect URI | *Application URL which receives the authorization code once user is authenticated* | Dev <https://biologics-portal-manufacturer-ui.dev.aks.west.us.mckesson.com/>login/callbackQA:  <https://biologics-portal-manufacturer-qa-ui.dev.aks.west.us.mckesson.com/> login/callback  UAT:  <https://biologics-portal-manufacturer-uat-ui.dev.aks.west.us.mckesson.com/>login/callback | Not yet provided |
| What OAuth grant type is supported by the application? | *Select one option from below:*  *Authorization Code*  *Authorization Code with PKCE*  *Implicit Grant*  *Client Credentials*  *Password Grant* | OIDC | OIDC |
| Does application support refresh token? | *Refresh token - used by clients to exchange refresh token for an access token* | Yes | Yes |
| Name pattern groups used by this application for authorization. |  |  |  |
| If application has privileged access (accessed by admins), then provide group information that admins are part of. | *Select one option from below:*  *Yes*  *No* | Yes | Yes |
| Do you want Okta to restrict users based on membership to groups used by this application? | *Only those users who belong to specified groups will be authenticated.* | Yes | Yes |
| Application Username format: | *Select one option from below:*  *LDAP ID*  *Email address* | Internal user- Email address  External user- userlogin/Email address | Internal user- Email address  External user- userlogin/Email address |
| Attributes to include in ID token | *List down the attributes that will be required by application (ex: first name, last name, mail etc.)* | TBC | TBC |

# Traceability

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Use Case** | **Description** |
|  | UC01 |  |
|  | UC02 |  |
|  | UC03 |  |
|  | UC04 |  |
|  | UC05 |  |
|  | UC06 |  |
|  | UC07 |  |
|  | UC08 |  |
|  | UC09 |  |
|  | UC10 |  |
|  | UC11 |  |
|  | UC12 |  |

# Appendix

## Call Recordings

[Walkthrough1 - JIRA-Biologics Portal and Biologics-20220505\_153430-Meeting Recording.mp4](https://mckessoncorp.sharepoint.com/:v:/r/sites/GRPMcKIAM-OktaIntegration/Shared%20Documents/Jira%20High%20Priority%20Tickets/IPSEN%20and%20Biologics/01%20Requirement%20Gathering/Recordings/Walkthrough1%20-%20JIRA-New%20IPSEN%20Portal%20and%20Biologics-20220505_153430-Meeting%20Recording.mp4?csf=1&web=1&e=OS9set)

[Technical Session1 - JIRA-Biologics Portal and Biologics-20220506\_203240-Meeting Recording.mp4](https://mckessoncorp.sharepoint.com/:v:/r/sites/GRPMcKIAM-OktaIntegration/Shared%20Documents/Jira%20High%20Priority%20Tickets/IPSEN%20and%20Biologics/01%20Requirement%20Gathering/Recordings/Technical%20Session1%20-%20JIRA-New%20IPSEN%20Portal%20and%20Biologics-20220506_203240-Meeting%20Recording.mp4?csf=1&web=1&e=VDzhDh)

[Walkthrough 2 - JIRA-Biologics Portal and Biologics-20220512-Meeting Recording.mp4](https://mckessoncorp.sharepoint.com/:v:/r/sites/GRPMcKIAM-OktaIntegration/Shared%20Documents/Jira%20High%20Priority%20Tickets/IPSEN%20and%20Biologics/01%20Requirement%20Gathering/Recordings/Walkthrough%202%20-%20JIRA-New%20IPSEN%20Portal%20and%20Biologics-20220512-Meeting%20Recording.mp4?csf=1&web=1&e=LISWvr)

## Application Architecture

[Architecture-Biologics-Ipsen.pptx](https://mckessoncorp.sharepoint.com/:p:/r/sites/GRPMcKIAM-OktaIntegration/Shared%20Documents/Jira%20High%20Priority%20Tickets/03%2004%20IPSEN%20and%20Biologics/01%20Requirement%20Gathering/Architecture-Biologics-Ipsen.pptx?d=w213f1b5deb984d0789a36ddddb5b9122&csf=1&web=1&e=3mtrEK)

[Ipsen & Biologics Portal\_Requirements & Additional Questionnaires.xlsx](https://mckessoncorp.sharepoint.com/:x:/r/sites/GRPMcKIAM-OktaIntegration/Shared%20Documents/Jira%20High%20Priority%20Tickets/03%2004%20IPSEN%20and%20Biologics/01%20Requirement%20Gathering/IPSEN%20and%20Biologics/Ipsen%20%26%20Biologics%20Portal_Requirements%20%26%20Additional%20Questionnaires.xlsx?d=wdac830f4bad245bc9b059760be0f2176&csf=1&web=1&e=C5A8sT)