iPermits Configuration Guide

Connected Worker Solutions

INNOVAPPTIVE

Title and Copyright

Copyright and **Terms of Use** page for **iPermits Configuration**.

Configuration Guide for **iPermits**, a *Connected Office Worker Solution*.

Release Version: *2609*

Release Date: *19 Oct 2026*

Published Date: *19 Oct 2026*

Document Version: *1.0*

Copyright © 2012-2026, Innovapptive Inc. and/or its affiliates. All rights reserved.

Primary Author: Innovapptive Inc.

Copyright Notices: Neither our Application nor any content may be copied without inclusion of all copyright notices and/or disclaimers provided therein. Any third party provider logos or marks provided through the Application shall remain owned by such third party provider as may be indicated in a notice contained in the Application or content and you shall not modify or remove any such notice. Neither we nor our suppliers or any third party providers grant any rights or license to any logos, marks, or copyrighted material other than as expressly set forth herein.

PDF technology powered by PDFTron Mobile SDK copyright © PDFTron™ Systems Inc., 2001-2019, and distributed by Innovapptive Inc under license. All rights reserved.

Preface

Understand audience, know related documents and products and conventions followed in this document.

Intended Audience

This user guide is for plant maintenance field service technicians in your organization. The user guide familiarizes operators or technicians with features and functionality of the Connected Back Office solution.

Document Conventions

Table 0-1 Conventions followed in the document

Convention	Meaning
boldface	Indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Indicates book titles, emphasis, or placeholder variables for which you supply values.
`monospace`	Indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter

Related Products & Solutions

- Work Order Management
- Inventory and Warehouse Management
- Analytics and Dashboards

Contact Innovapptive

For information on Innovapptive products, visit the Innovapptive's Support Portal at http://helpdesk.innovapptive.com. The updates to this document are published on this support portal. Check this website periodically for updated documentation.

For additional information about this document, send an email to documentation@innovapptive.com.

Contents

Title and Copyright....ii
Preface....iii
1. Introduction....6
1.1. About the Configuration Platform....6
1.2. What's New for Configuration....7
2. Log in to Application....8
2.1. Log in to Platform Application....8
2.2. Troubleshoot Login Issues....9
3. Navigate to the iPermits Configuration....10
3.1. Explore the Home Screen....10
3.2. Access Modules....11
3.3. Understand the Platform Layout....11
4. Customer Tenant Onboarding with Azure IDP....12
5. Authentication Identity Configuration....15
5.1. Federated SSO Login Flow....16
5.2. Token-Based App API Flow....18
5.3. Use the Token After Login....18
5.4. Refresh Token Handling....19
5.5. Alternatives for Users Table Synchronization....19
6. Manage Users & Roles....21
6.1. Add and Modify Users....21
6.2. Manage User Groups....24
6.3. Create Roles and Permissions....26
6.4. Bulk Upload Users....28
7. Maintain Master Data....30
7.1. Create a Plant....30
7.2. Create a Shift....32
7.3. Create a Location....32
7.4. Create an Asset....33
7.5. Create UOM....34
7.6. Create a Global Response Set....35
7.7. Bulk Upload Master Data....36
8. Configure iPermits Settings....37
8.1. Enable or Disable Modules....37

8.2. Configure Dashboard Availability (Mobile) 38
8.3. Configure Session Timeout 39
8.4. Configure Bottom Navigation (Mobile) 40
8.5. Configure AI 42
9. Integration Setup 44
9.1. Understand the Integration Workflow 44
9.2. Connect Work Order Data to iPermits 45
10. Design and Manage Permit Template 46
10.1. Create Permit Template 46
10.2. Configure Permit List View 50
11. Design and Manage JHA Template 52
11.1. Create JHA Template 52
11.2. Configure JHA List View 54
12. Design and Publish Forms 56
13. Customize Platform Settings 60
13.1. Manage Storage & Sync Settings 60
13.2. Define Mobile Data Sync Preferences 61
13.3. Apply Theme Configurations 64
14. Set Up Notifications 65

1. Introduction

The **iPermits Configuration Guide** is your blueprint for shaping how iPermits works in your organization.

This guide helps you transform the out-of-the-box system into a solution tailored to your business processes, plants, and teams.

Unlike installation or deployment activities that typically sit with IT, the configurations in this guide define how permits are structured, reviewed, approved, and enforced across your organization.

From defining Permit Types and safety rules, to configuring approval workflows, roles, Job Hazard Analysis (JHA), PPE validation, and notifications, every section of this guide is designed to help you align iPermits with the way your organization manages risk, compliance, and safe work execution.

With this guide, you will:

- **Establish the foundation** → onboard your tenant, configure authentication, and set up users and master data.
- **Control product behavior** → decide which modules are available, how Work Orders flow, and how AI, timers, and measuring points are applied.
- **Customize and optimize** → design forms, create RACE templates, define risk matrices, set notifications, and personalize platform settings.

1.1. About the Configuration Platform

The **iPermits Configuration Console** is the web-based admin layer that allows your organization to control how permits are created, reviewed, authorized, and tracked — without writing code.

From a single interface, functional administrators can define Permit Types, approval chains, safety validations, risk rules, and compliance controls, ensuring workers, supervisors, and auditors experience a consistent, safe, and policy-aligned permit process.

What you can do here:

- **Manage Permit Types**: Create and configure Hot Work, Cold Work, Confined Space, Electrical, and other permits.
- **Design Permit Forms**: Configure fields, sections, validations, and conditional logic.
- **Assign by Hierarchy**: Map permits and rules to plants.
- **Administer Access**: Manage users, roles, permissions, and governance policies.
- **Enable Notifications & Alerts**: Configure expiry reminders.
- **Maintain Audit & Compliance Records**: Ensure digital traceability for each action taken at permit level.

Who should use this

- **Functional Administrators / Doc Owners** — primary audience. They own templates, module controls, business rules, and access policies.
- **IT / Basis (as-needed support)** — assists when a configuration requires backend application (e.g., DB-stored flags), SSO/IDP wiring, or transport/security steps documented in the **Deployment & Setup Guide**.

> "
>
> If you execute work (create/complete WOs, inspections, timesheets), see the **User Guides**. If you shape how iMaintenance works, you're in the right place.
>
> "

1.2. What's New for Configuration

Review the iPermits capabilities introduced in release 2609

New Features and Enhancements in Release 2609

Table 1-1 New Features and Enhancements in Release 2609

Configurable Storage Location for Permit PDFs Choose whether Permit PDFs generated at permit surrender are synced to SAP ERP or kept only in Innovapptive storage (S3). The default is S3; Operation-level Permit PDFs always remain in S3.

2. Log in to Application

This Section guides users on how to securely access the platform using their credentials across web and mobile applications.

This chapter has the following topics:

- Log in to Platform Application *(on page 8)*
- Troubleshoot Login Issues *(on page 9)*

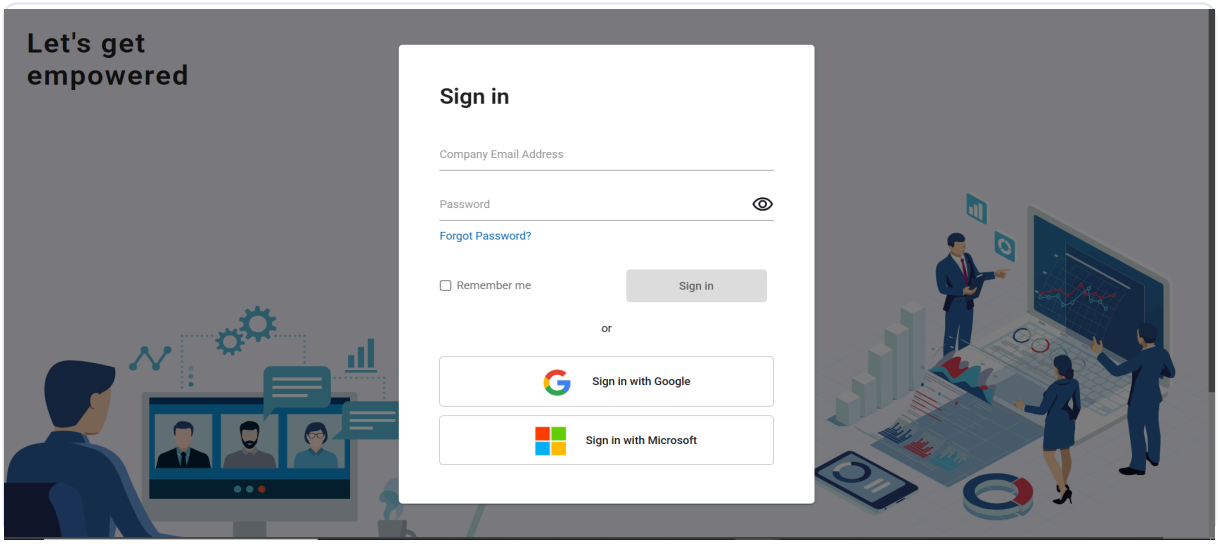
2.1. Log in to Platform Application

You can access the platform using multiple login methods based on your organization's configuration. This section explains how to sign in and access the iPermits Web Application.

Basic Authentication

Use your company registered email and password to log in.

1. Open the application.
2. Enter your **Email Address** and **Password**.
3. Click **Sign in**.
4. Select **Remember me** to save login credentials. (Optional)



Single Sign-On (SSO: Google or Microsoft)

You can also sign in using your **Google** or **Microsoft** account—whichever is enabled for your organization.

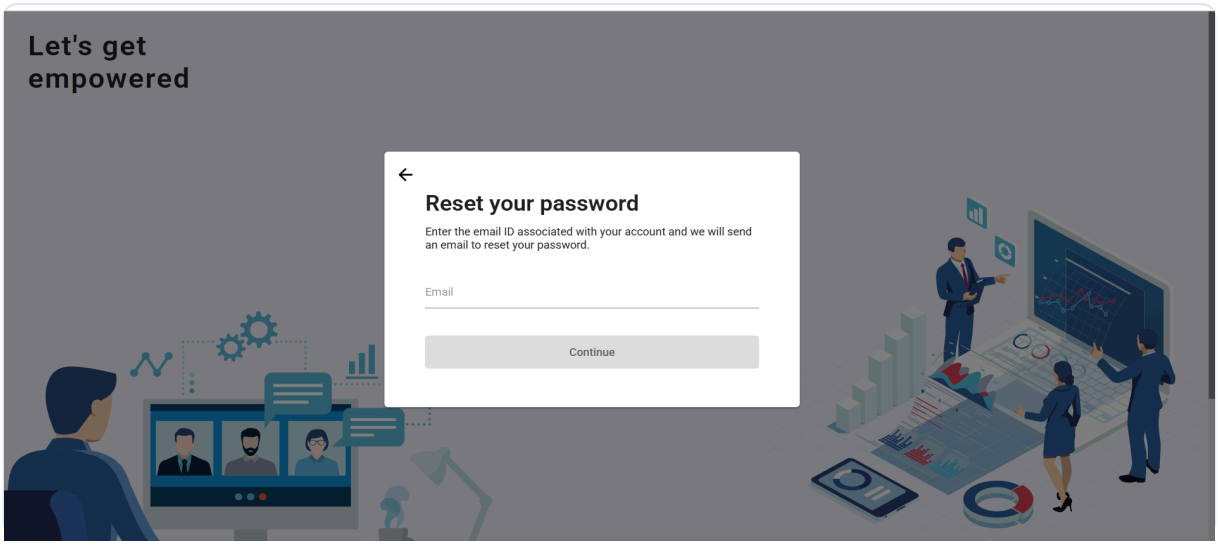
1. On the login screen, click **Sign in with Google** or **Sign in with Microsoft**.
2. Select or enter your account credentials.

> **Note:**
> If this is your first time, the same button completes your sign-up process. If your browser has saved Google or Microsoft accounts, they will appear automatically for quicker selection.

2.2. Troubleshoot Login Issues

If you forget your password:

1. Navigate to the **Sign in** page.
2. Click **Forgot Password?**
3. Enter your registered email and click **Continue**.



4. If two-factor authentication is enabled, verify using the code sent to your phone.
5. Follow the email link to set a new password.

3. Navigate to the iPermits Configuration

This section helps you get familiar with the layout of the platform and how to access various modules efficiently.

This chapter has the following topics:

- Explore the Home Screen *(on page 10)*
- Access Modules *(on page 11)*
- Understanding the Platform Layout *(on page 11)*

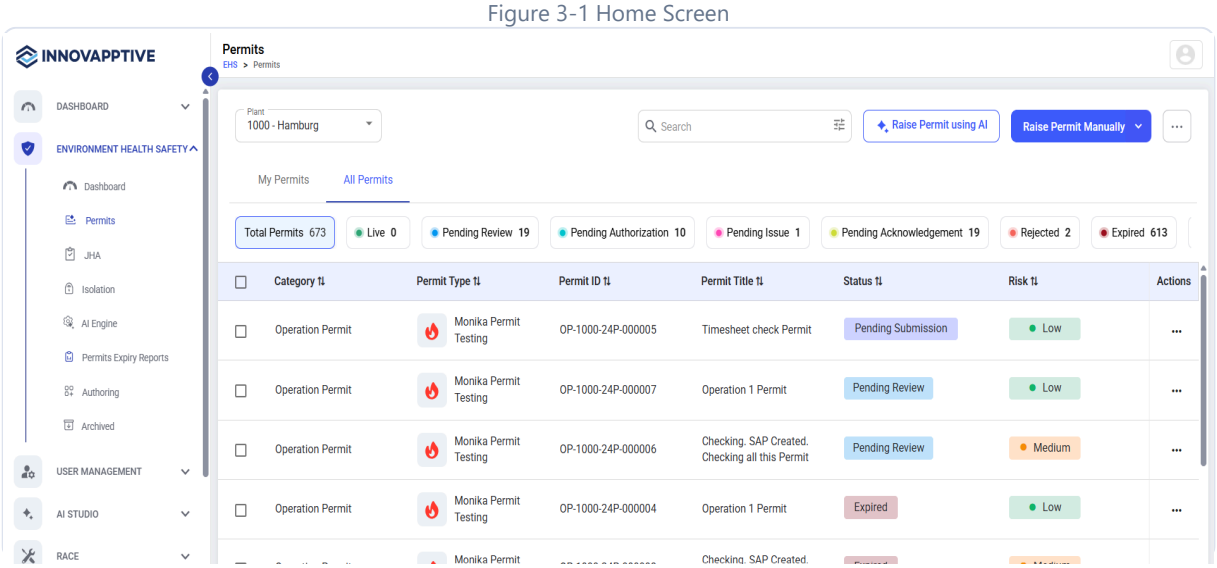
3.1. Explore the Home Screen

This section helps you get familiar with the layout of the platform and how to access various modules efficiently.

After logging in, you are directed to the **Home Screen**, which serves as the central hub for iPermits activity. From here, you can:

- View permit summaries and system insights.
- Track permit status across plants or areas
- Access dashboards and reports.
- Use the left-hand navigation panel to quickly open modules such as Permits, JHA, Authoring etc. under Environment Health Safety.

Figure 3-1 Home Screen



The layout is designed for **ease of use**, with consistent elements across modules for a smoother user experience.

3.2. Access Modules

Modules represent different functional areas of the platform (e.g.,Forms, RACE, Settings, Master Data etc.).

To access a module:

1. Use the **left navigation pane** to browse through available modules.
2. Click a module name (e.g., **Environment Health Safety**) to open it.
3. If the module contains sub-sections, they expand below the selected module .

   Some modules may only appear based on your **role and access permissions**.

   Tip: If the navigation panel is collapsed, hover over icons to view full module names.

3.3. Understand the Platform Layout

The platform interface is made up of the following key areas:

Area	Description
Header Bar	Located at the top, it includes user profile options, notifications, and product/version details.
Navigation Panel (Left Sidebar)	Lets you access different modules, features, and configuration options.
Main Workspace	The center of the screen where dashboards, forms, reports, and module content are displayed.
Filters and Actions (Top of Workspace)	Contextual filters, search bars, and action buttons are available based on the module in use.

The interface is consistent across modules to make navigation intuitive and user-friendly.

4. Customer Tenant Onboarding with Azure IDP

This section provides step-by-step instructions to configure a customer's Azure Active Directory (Azure AD) for federated Single Sign-On (SSO) with Innovapptive mobile applications. It applies to IT administrators and implementation engineers performing customer onboarding.

Follow the below steps to register tenant specific CWP enterprise application in the Azure portal:

1. Access the Azure portal using the following URL https://portal.azure.com/ and, use required tenant credentials to login into the Azure portal.
2. Post login, click the **View** button.
3. Click the **App registrations** on the left-side menu.
4. Click the **New Registration** button and provide the required information to register tenant specific CWP enterprise application.
    a. Name (Name of the CWP enterprise application).
    b. Supported account types (It is self-explanatory. Select it based on the client's requirement. For now, go with a single tenant).
    c. Redirect URI (Mention here the Tenant Specific URL that the user must be redirected to post successful login with Azure IDP).
    d. Click the **Register** button.
    e. For iPermit Product the redirect URI should be added as Web based application.

> **Note:**
>
> - The CWP application URL follows the format: <customername><tenanttype>.innovapptive.com. For example, if the customer name is Google, the URLs will be:
> - Dev: googledev.innovapptive.com
> - QA: googleqa.innovapptive.com
> - Prod: google.innovapptive.com
> - Both QA and Prod environments share the same domain format.

5. Click the **Authentication** on the left-side menu to select the token authorization endpoint flow.
6. Select **Access tokens** checkbox and click the **Save** button.

7. Click the **API Permissions** from the left-side menu.
    a. Click the **Add a permission** button. You must see Request API Permissions on the right side.
    b. Click the **Microsoft Graph**.
    c. Click the **Delegated permissions**.
    d. Search and select email, offline_access, openid, chat, apple maps, and profile permissions one by one.
    e. Click the Add permissions button.
    f. Click the **Grant admin consent** button.
    g. Select Microsoft APIs and click on Microsoft Graph (Refer Below)
    h. Add 7 user delegation permissions and 1 application permission (Refer below)
    Optional: sharepoint permissions need to be added if we want to integrate sharepoint.

> **Note:**
>
> In Azure App Registrations, there are two types of API permissions: **Delegated** and **Application**. **Delegated permissions** are used when an app acts on behalf of a signed-in user, meaning the app's access is limited to the user's permissions and requires user login. These are ideal for interactive apps like web or mobile applications. **Application permissions**, on the other hand, allow the app to run independently of a user and access APIs with its own identity, typically used by background services or daemons. Application permissions usually require admin consent and provide broader access at the tenant level.

Claim Value	Permission	Type	Permission Status
offline_access	Maintain access to data you have given it access to	Delegated	Default
AccessReview.Read-.All	Read all access reviews	Application	Default
Files.Read.All	Read all files that user can access	Delegated	Sharepoint
User.Read.All	Read all users' full profiles	Delegated	Default
Files.Read.All	Read files in all site collections	Application	Sharepoint
Sites.Read.All	Read items in all site collections	Delegated	Sharepoint
Sites.Read.All	Read items in all site collections	Application	Sharepoint
Files.Read	Read user files	Delegated	Sharepoint
User.Read	Sign in and read user profile	Delegated	Default
openid	Sign users in	Delegated	Default
profile	View users' basic profile	Delegated	Default
email	View users' email address	Delegated	Default

8. The following steps are useful in SAP OData endpoint authentication using SSO (SAML 2.0 Bearer Assertion Flow for OAuth 2.0).
    a. Click the **Certificates and secrets** from the side menu. You must see the Certificates and secrets screen.
    b. In the **Client secrets** tab, click the **New client secret** button. Provide description, expiration days and then click the **Add** button.
    c. Copy the generated secret value using the **Copy** icon and save it in a text file, to use at the time of tenant onboarding from the CWP web application. In case of secret expiration, follow the above step to generate a new secret and update in tenant onboarding.
    d. Click **Expose an API** from the side menu and then click the **Add a scope** button. You'll be asked to set the Application ID URI for the enterprise application registration. Accept the proposed default value by clicking the **Save and continue** button.
    e. Provide the required details and click the **Add scope** button.
    f. Copy the created scope by using the Copy icon and save it in a text file (or) Come back to Expose an API side menu for scope (View => App registrations => Application Name => Expose an API), to use at the time of tenant onboarding.

9. Click **Overview** from the side menu. Copy the Application (client) ID, Directory (tenant) ID and Application ID URI of the newly registered CWP enterprise application and save it in a text file (or) Come back to Overview side menu for client, tenant ids and application id URI (View => App registrations => Application Name), to use at the time of tenant onboarding.

10. If the user is not added into AAD Enterprise applications please follow the below steps to add the user into a particular application.
    a. Go to the e-application and look for the application that you created.
    b. Open the application and select users / groups and add the user if he is not added already to the application.

> **Note:**
> If the user is already added to the application, **don't follow the 9th step.**

Table 4-1 From CWPEnterpriseApp

Tenant ID	f8e6xxx-xxxx-xxxx-xxx-bxxxxxx
Client ID	50xxxxxxx-xxxxxx2ad-xxxxxx
Application ID URI	api://50bfxxxxxxxx-42ad-xxxxxx
Client secret	hyxxQ~wXXXXXXXac0bntd4xxxxxx
Scope	api://50xxxxxxx-42ad-xxxxx/netweavexxxx

> **Note:**
> Above is the base format of the Azure Enterprise app details.

5. Authentication Identity Configuration

This section explains how Innovapptive's mobile applications handle user authentication in a multi-tenant deployment environment. The authentication framework is based on federated Single Sign-On (SSO) and secure token-based session management.

It covers how users authenticate using enterprise-managed identity providers (such as Azure AD, Google, or Okta), how access and refresh tokens are managed, and how user data is synchronized with backend systems. This information is relevant for developers, implementers, and security teams configuring the authentication layer in customer deployments.

Component Overview

The authentication flow involves multiple systems working together to validate user identity, issue secure tokens, and enable access to backend services. The table below summarizes the core components involved:

Component	Description
Innovapptive DB	Stores tenant-specific configuration such as Tenant ID, SSO method (e.g., Azure, Google), Client ID, and Client Secret.
Tenant ID	A unique identifier assigned to each customer environment.
SSO Method	Specifies the identity provider (e.g., Cognito, Azure AD, Google, Okta) used for user authentication.
Client ID & Secret	Credentials associated with the Innovapptive application registered in the tenant's SSO provider.
Mobile App	The application being used — such as mWorkOrder, mRounds, or mTag — initiates the authentication request.
Auth Server	Innovapptive's authentication microservice, deployed in the tenant's cloud, is responsible for token issuance and user validation.
Users Table	Managed by the Auth Server. Stores user records, including internal User ID, SSO identifier, and SSO-issued refresh tokens.
SSO Server	The tenant-managed identity provider is responsible for authenticating users and issuing authorization codes and refresh tokens.
Mongo User Directory	MongoDB Realm directory is used to authorize users for offline data sync and database access.

5.1. Federated SSO Login Flow

Innovapptive's mobile apps authenticate users using federated SSO, integrating with tenant-managed identity providers like Azure AD, Google, or Okta.

The following flow explains the complete authentication sequence—from mobile app launch to user provisioning—highlighting how the app, backend services, SSO server, and user management databases interact at each step.

1. The mobile app fetches the SSO method and Client ID for the tenant from the Innovapptive DB.
2. Based on the SSO type, the app displays a single sign-in button, such as Sign in with Google or Sign in with Okta.
3. When the user taps the button, an in-app browser opens and redirects them to the SSO login or consent screen.
4. Upon successful authentication, the SSO server redirects the user to Innovapptive's landing URL with a one-time authorization code.
5. The app sends this code—along with the tenant ID—to the Auth Backend.
6. The backend sends a grant request to the SSO server using:
    - Authorization code
    - Client ID
    - Client Secret
7. The SSO server responds with an access token and a refresh token.

8. Using the access token, the Auth Backend fetches the user's profile details from the SSO server.

9. The backend then:
    - Stores the user details and SSO refresh token in the Users Table
    - Creates a Mongo Realm user with a unique password

10. The backend returns the following credentials to the mobile app:
    - Realm username and password
    - Basic Auth JWT token (used for secure API and DB sync)

Figure 5-1 Federated SSO Login Flow – From Mobile App to SSO and Backend Sync

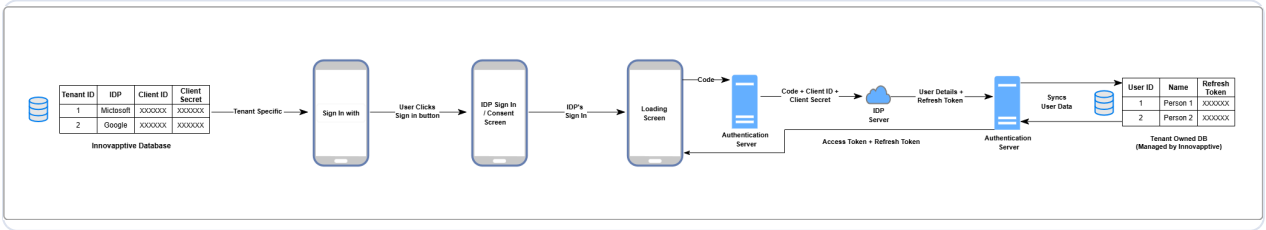
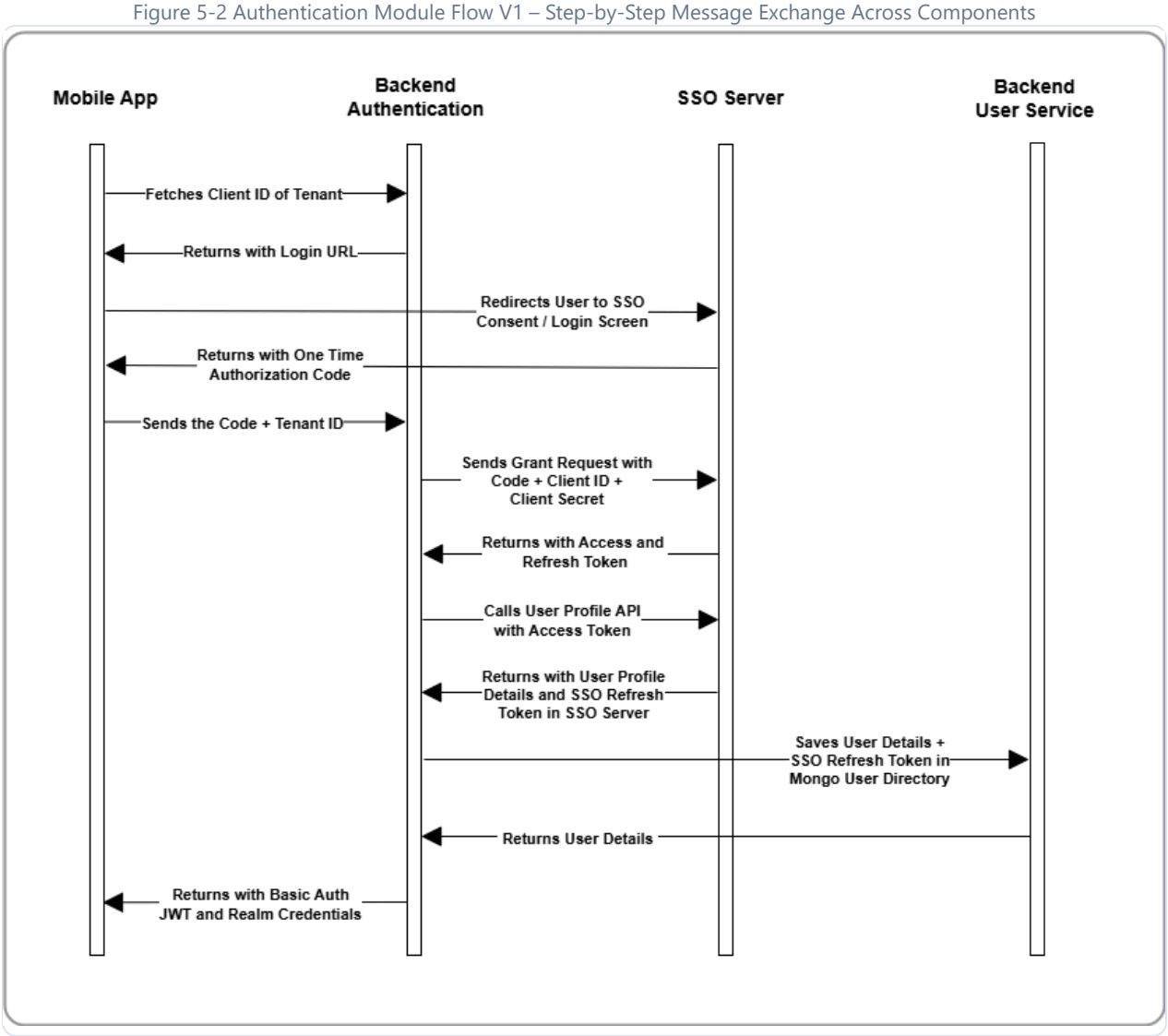


Figure 5-2 Authentication Module Flow V1 – Step-by-Step Message Exchange Across Components



Reference: https://excalidraw.com/#json=Uc84zojdzuFrFQB_0mr-5,UHk6cX3C_yJpW-dDgC4nPw

5.2. Token-Based App API Flow

After the user is authenticated via SSO, the mobile app uses access and refresh tokens issued by the Auth Server to interact securely with backend services. This section explains how these tokens are generated, validated, and refreshed across service calls.

This flow assumes that the mobile app interacts with one or more backend services behind a common authentication layer.

What Happens at Login

1. Once the user logs in, the Auth Server generates both an access token and a refresh token, which are stored in the Users Table and also sent to the mobile app.
2. Both tokens are formatted as JWTs (JSON Web Tokens).
3. The access token is short-lived (default: 15 minutes, configurable).
4. The refresh token has a longer lifespan (default: 30 days, configurable).
5. Tokens are signed using asymmetric encryption:
    - The Auth Server holds the Private Key used to sign tokens.
    - All other backend services use the Public Key to verify access tokens.

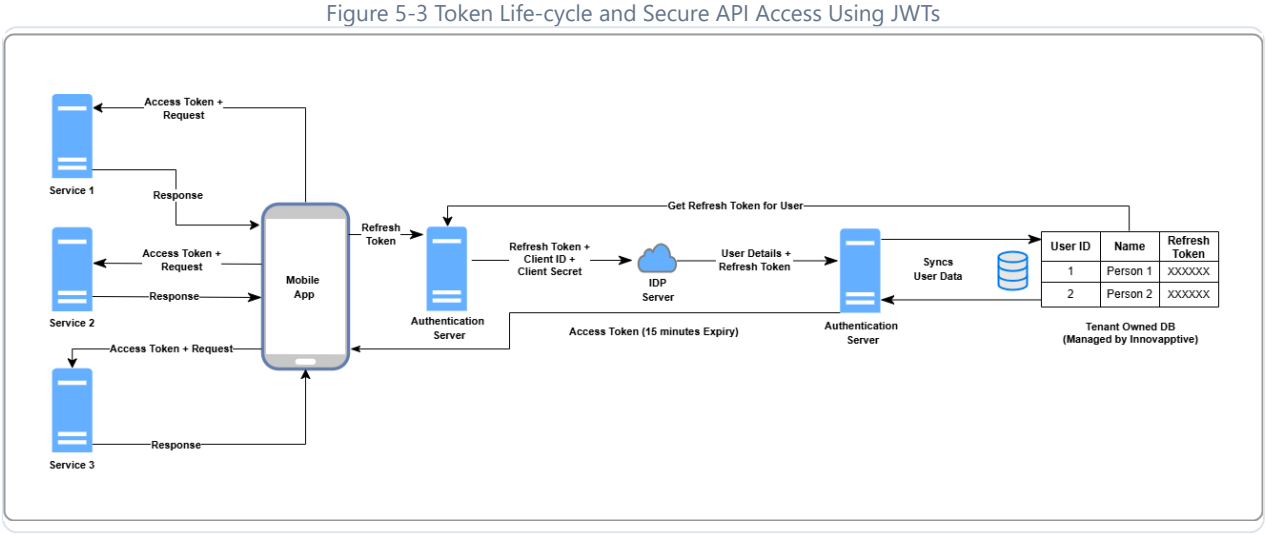
5.3. Use the Token After Login

1. Every backend service is protected by a common middleware that validates the incoming access token using the Public Key.
2. For user-related data:
    - Services may perform read-only access to the Users Table directly for performance.
    - Alternatively, they can proxy the request via the Auth Server if direct access is restricted or decoupled.
3. If the access token has expired (after 15 minutes), the API call will fail with an authentication error.
4. When this happens, the app uses the refresh token to request a new access token from the Auth Server.

5.4. Refresh Token Handling

1. During the refresh call, the app also submits the SSO-issued refresh token to the Auth Server.
2. The Auth Server verifies the user's presence and active status in the tenant's SSO system.
3. If valid, it issues a new access token back to the app.
4. If the user no longer exists in the SSO system or is marked inactive:
    - The Auth Server deletes the corresponding user entry from the Users Table.
    - The app is instructed to log the user out immediately.

Figure 5-3 Token Life-cycle and Secure API Access Using JWTs



5.5. Alternatives for Users Table Synchronization

If the Users Table cannot always be reliably synchronized with the tenant's SSO server, alternative mechanisms may be considered to maintain alignment between user records and identity provider data.

There are two commonly adopted patterns for maintaining sync between the SSO system and the Users Table:

Scheduled Sync Pipeline

Establish a synchronization pipeline that pulls user data from the SSO server and updates the Users Table.

- This can be either a manual process (e.g., initiated by admin tools) or an automated one.
- For automated sync, the cadence (hourly, daily, etc.) must be defined based on acceptable staleness and load tolerance.
- This method is relatively straightforward but introduces a time gap between SSO changes and backend updates.

Event-Driven Pub/Sub Model

Adopt a publish/subscribe architecture, where the SSO server emits events (e.g., user created, updated, deactivated) to an exposed API endpoint on Innovapptive's side.

- These events are then used to update or delete user entries in the Users Table in near real-time.
- This approach ensures better consistency and reacts instantly to user state changes.
- However, it depends heavily on:
  - The SSO provider's eventing capabilities
  - Proper initial sync to align existing records

Reference: JSON Web Tokens with Public Key Signatures – Miguel Grinberg

6. Manage Users & Roles

This section explains how administrators can onboard users, assign appropriate roles and permissions, and organize users into groups to control access and responsibilities across the platform

The **User Management** module allows administrators to onboard users, define roles, manage access levels, and organize users into groups. It ensures users only see and interact with modules relevant to their responsibilities.

This chapter has the following topics:

- Add and Modify Users *(on page 21)*
- Create Roles and Permissions *(on page 26)*
- Manage User Groups *(on page 24)*

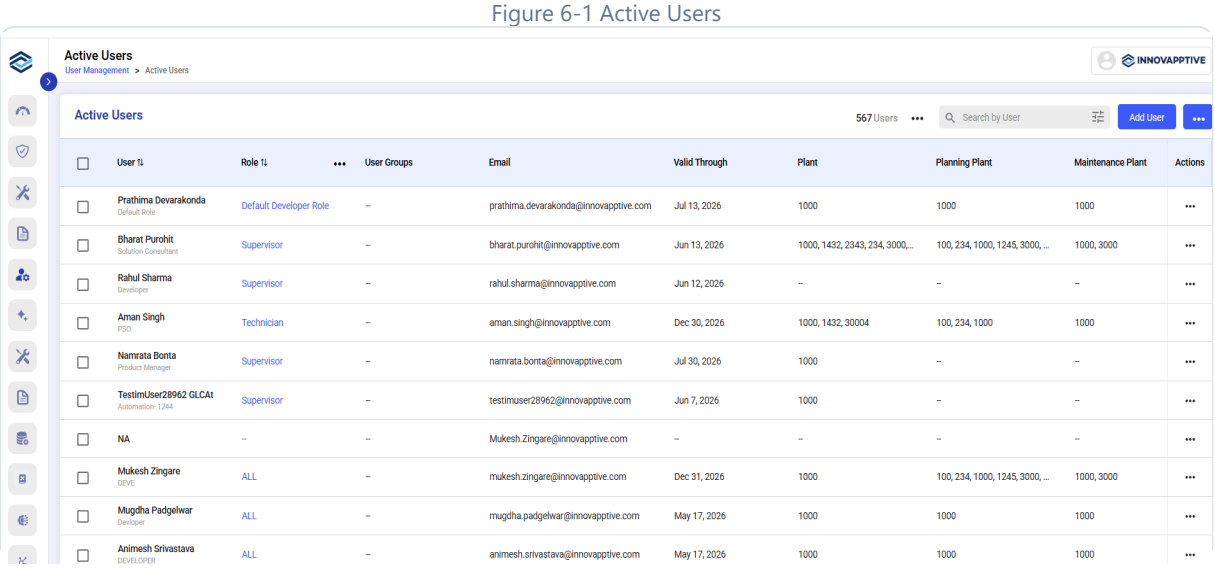
6.1. Add and Modify Users

Administrators can create users manually or in bulk, assign them roles, link them to plants, and control their access period.

To create a user manually:

1. Navigate to **User Management** > **Active Users**.

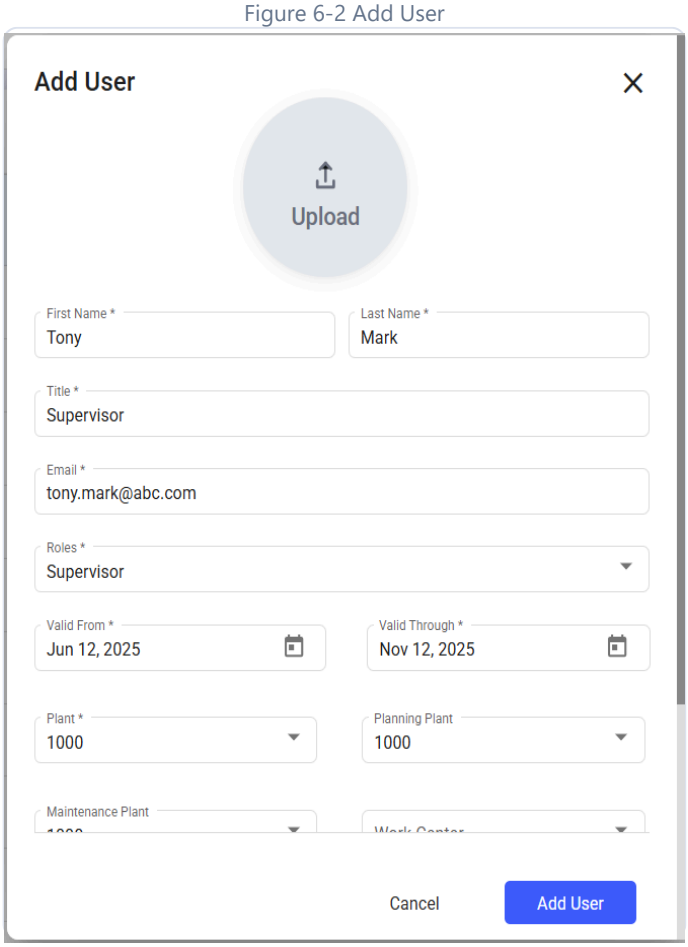
Figure 6-1 Active Users



2. Click **Add User** > **Create Manually**.

3. In the **Add User** window, fill in the following fields:
    - First/Last Name, Title, Email
    - Role, Validity Dates
    - Plant, Planning Plant, Maintenance Plant
    - Work Center, Reporting To, Reportees
    - User Group, Data Entry Profile, Shift

Figure 6-2 Add User



4. Click **Add User**.

The user will appear under the *Active Users* tab.

Use **Upload Excel** for bulk creation.

Download the user list via **More** icon > **Download Users List**.

To modify or deactivate a user:

- Click **More** icon > **Edit** to update details.
- Click **Deactivate** to disable access. Deactivated users are listed under *Inactive Users*.

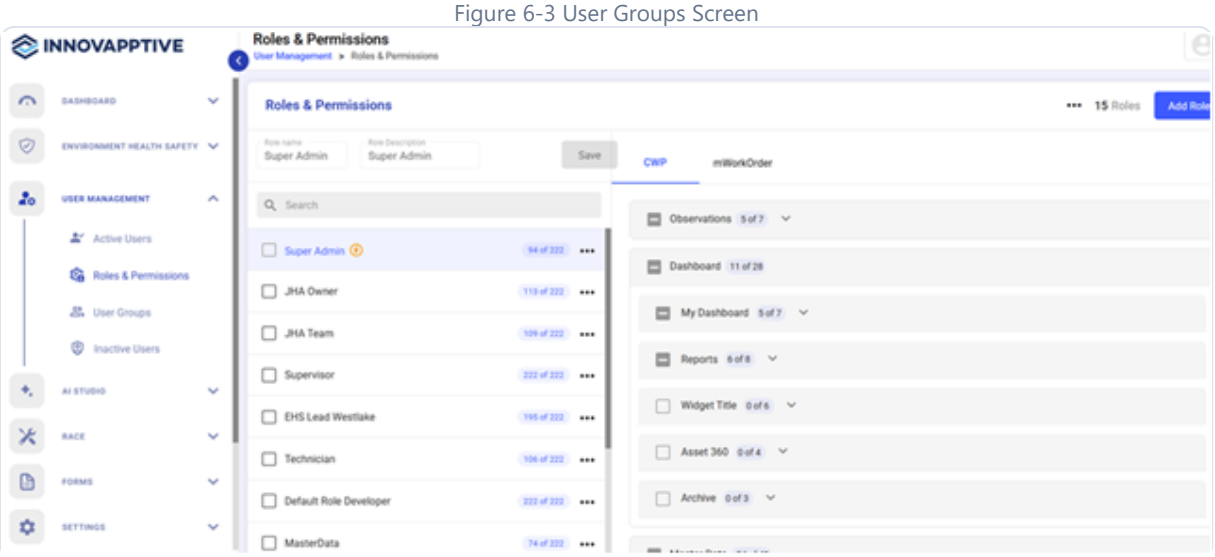
6.2. Manage User Groups

User Groups simplify access control by grouping users with similar responsibilities. This allows admins to assign permissions at the group level instead of individually.

To create a user group:

1. Navigate to **User Management** > **User Groups**.

Figure 6-3 User Groups Screen



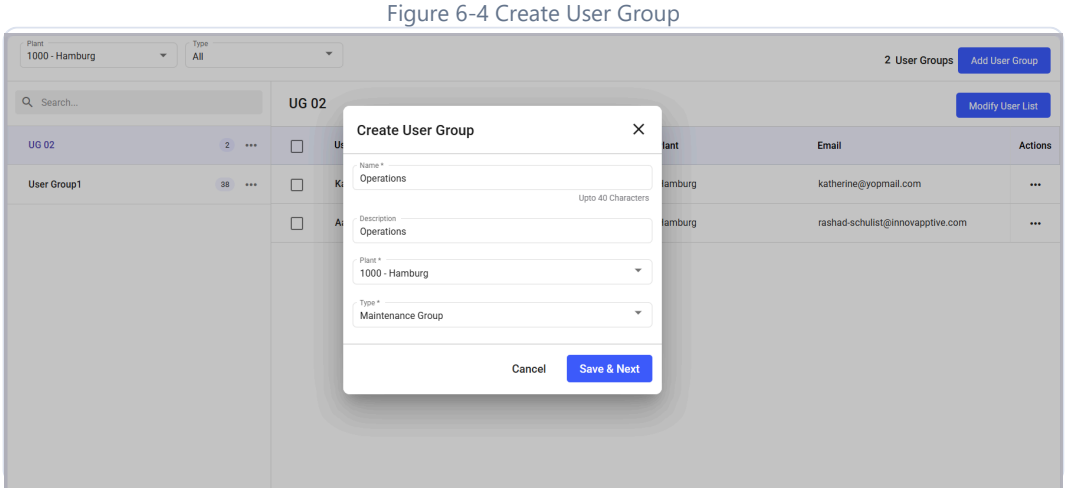
2. Click **Add User Group**.

3. In the **Create User Group** window, fill in the following details:

   - Name, Description, Plant
   - Type: Planner Group or Maintenance Group

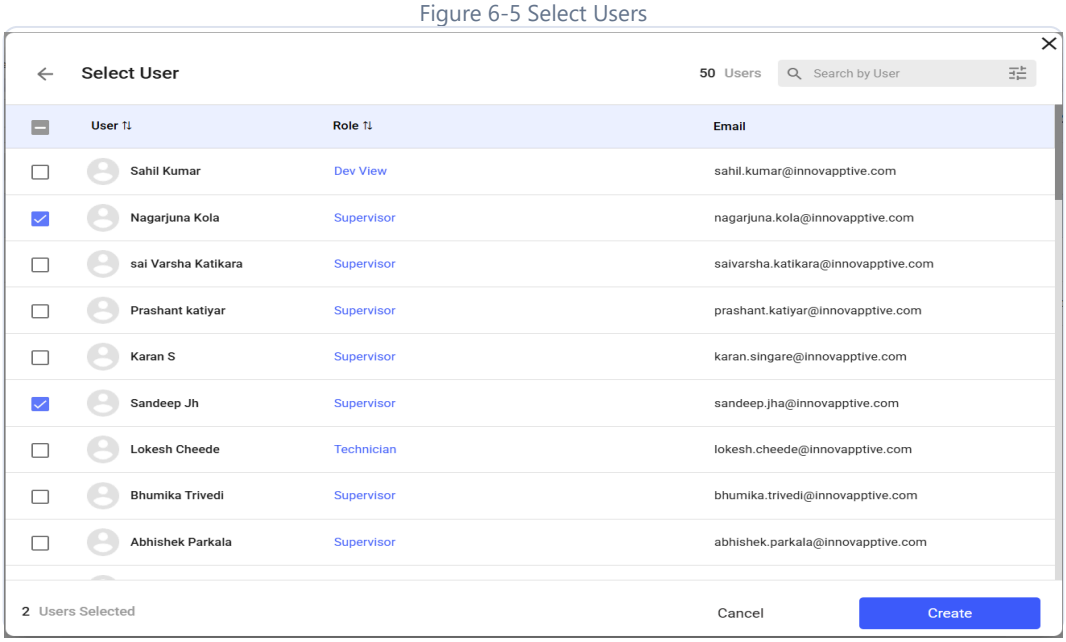
4. Click **Save & Next**.

Figure 6-4 Create User Group



5. In the **Select User** window, select users and click **Create**.

Figure 6-5 Select Users



To modify user groups:

- Use **More** icon > **Edit**, **Copy**, or **Delete**.
- To change members:
  - Select the group > click **Modify User List**.
  - Deselect or remove users as needed.
  - Save your changes.

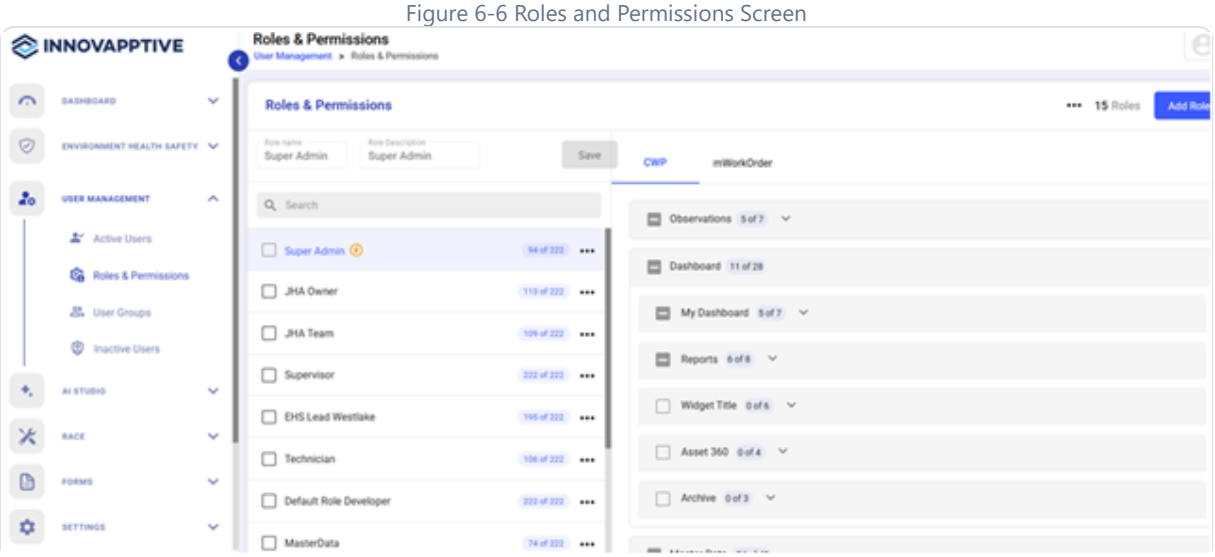
6.3. Create Roles and Permissions

Roles control which iPermits modules, permit actions, and safety features a user can access. Each role defines what a user can view, create, review, approve, issue, or manage within the iPermits system. Roles are typically aligned with permit personas such as Permit Requestor, Reviewer, Authorizer, Issuer, Safety Officer, and Administrator.

To create a role and assign permissions:

1. Navigate to **User Management** > **Roles and Permissions**.

Figure 6-6 Roles and Permissions Screen



2. Click **Add Role**.

3. Fill in **Role Name** and **Role Description**.

4. Click **Save**.

5. Select the new role.
6. Choose the modules that are required for the role or persona on the right-side.
7. Click **Save**.

Use **More** icon > **Copy** to clone existing roles.

Use **More** icon > **Delete** to delete the role.

Note:

- The Super Admin role cannot be edited or deleted. It can only be copied.
- You cannot delete a role that is currently assigned to users. Unassign users first, then delete the role.
- You cannot delete roles that are assigned to users or edit the Super Admin role.
- • Assign permissions carefully to ensure segregation of duties — for example, the same user should not both issue and authorize permits unless required by policy.

Best Practice for iPermits Role Design

Align roles with permit responsibilities:

- **Permit Requestor** - Create and submit permits.
- **Permit Reviewer** - Review risk, JHA, and safety controls.
- **Permit Authorizer** - Approve permits based on authority.
- **Permit Issuer** - Issue permits and validate site readiness.
- **Permit Holder** - Execute work under approved permits.
- **Safety / EHS Admin** - oversee safety rules and compliance.
- **System Admin** - manage configuration and access.

6.4. Bulk Upload Users

Administrators can streamline user creation by uploading multiple user records at once using an Excel template. This method is ideal for onboarding large teams efficiently.

Note:
The Work Center field is optional during bulk user creation.

To bulk upload users:

1. Expand the **User Management** and select **Active Users**.
2. Click the More icon on the top right corner and select **Download Template**.
3. Fill out the Excel sheet.
4. Click **Add User** > **Upload Excel**.
5. Select the excel and upload the file.

7. Maintain Master Data

This section explains how to set up and manage the core reference data required to configure iPermits, ensuring consistent behavior across permits, workflows, safety rules, and reports across plants and teams.

The **Master Data** module holds the foundational elements of your system—plants, locations, shifts, assets, units of measurement, and response sets. Proper configuration ensures consistency across forms, workflows, and analytics.

This chapter has the following topics:

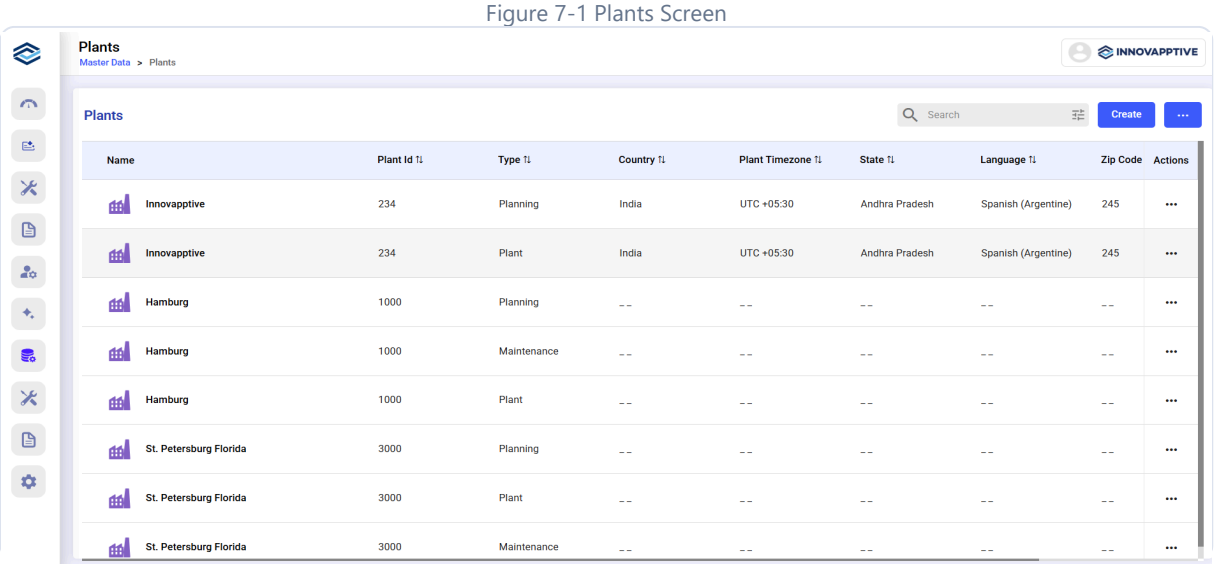
- Create a Plant *(on page 30)*
- Create a Shift *(on page 32)*
- Create a Location *(on page 32)*
- Create an Asset *(on page 33)*
- Create UOM *(on page 34)*
- Create a Global Response Set *(on page 35)*
- Bulk Upload Master Data *(on page 36)*

7.1. Create a Plant

To create a plant:

1. Navigate to **Master Data** > **Plants**.

Figure 7-1 Plants Screen



2. Click **Create New**.

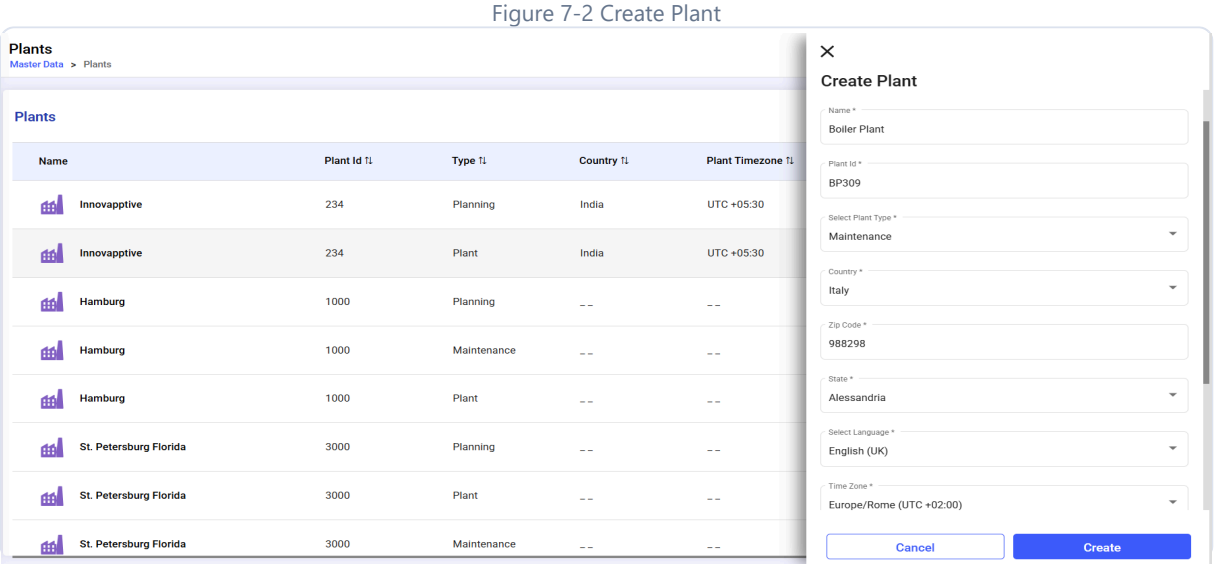
3. In the **Create Plant** window, fill in the following fields:
   - Name, Plant ID, Plant Type, Country, Zip Code, State, Time Zone, and Shifts.
   - Enable **Shift Handover Report** toggle if needed.

> **Note:**
> If the Plant ID already exists, an error message “Plant ID <> already exists” is displayed. Use another ID.

4. Under the **Additional Details** section, add custom Labels & Fields.

5. Click **Create**.

Figure 7-2 Create Plant



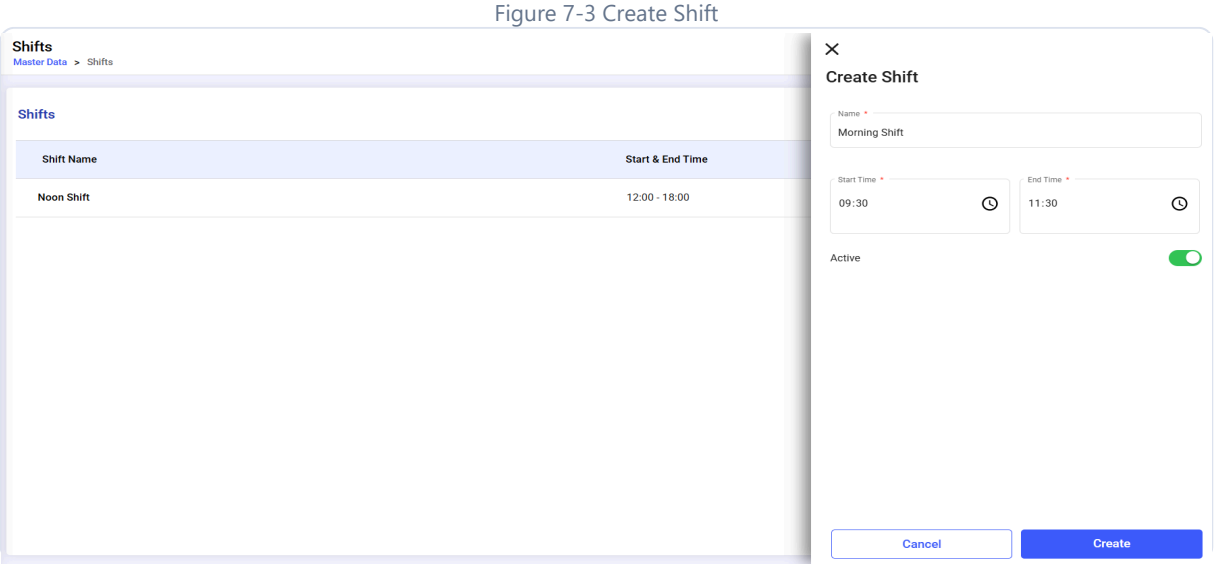
Use **More** icon to **Copy**, **Edit**, or **Delete**.

7.2. Create a Shift

To create a shift:

1. Navigate to **Master Data** > **Shifts**.
2. Click **Create New**.
3. In the **Create Shift** window, fill in the following details:
    - Name, Plant, Start Time, End Time.
    - Set **Active** toggle to make the shift active.
4. Click **Create**.

Figure 7-3 Create Shift

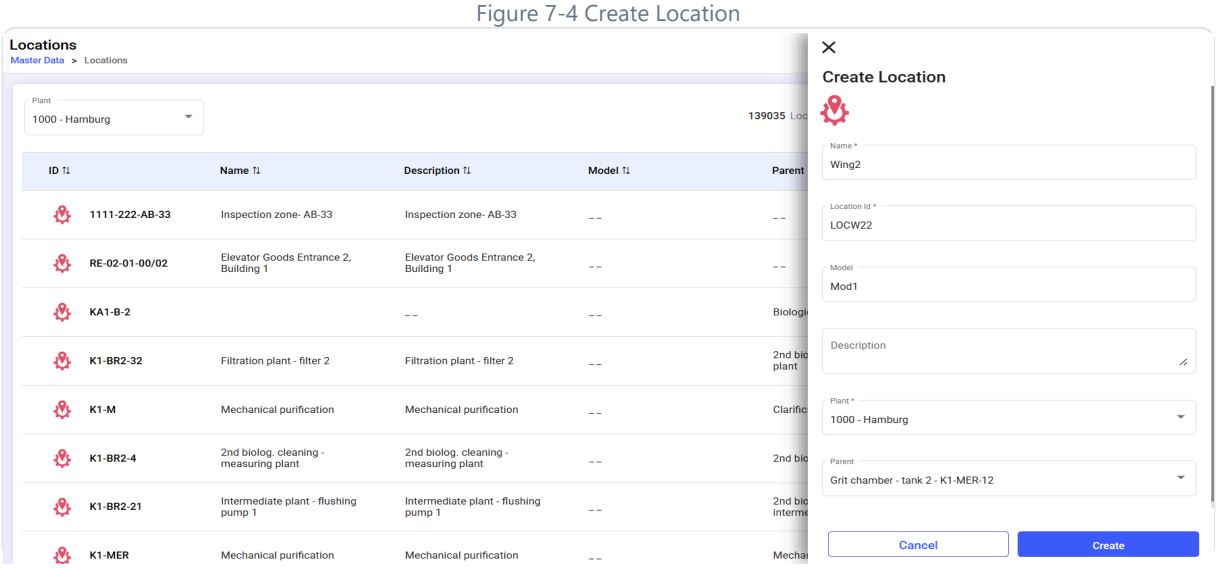


7.3. Create a Location

To create a location:

1. Navigate to **Master Data** > **Locations**.
2. Click **Create New** > **Create Manually**.
3. In the **Create Location** window, fill in the details, such as Name, Location ID, Model, Description, Plant, and Parent.
4. Click **Create**.

Figure 7-4 Create Location

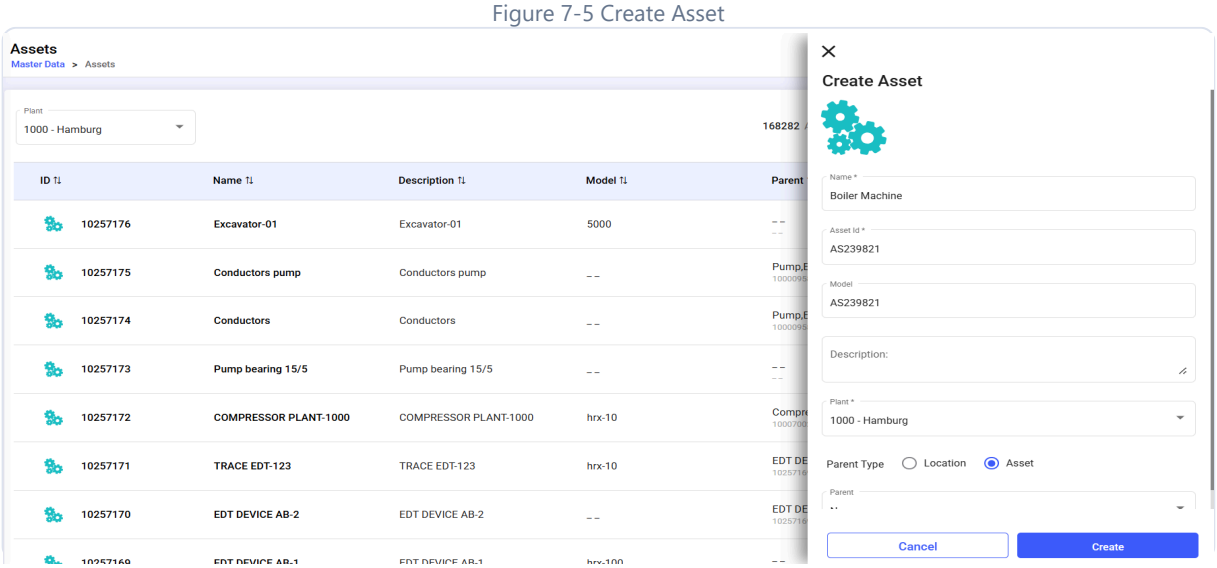


7.4. Create an Asset

To create an asset:

1. Navigate to **Master Data** > **Assets**.
2. Click **Create New** > **Create Manually**.
3. In the **Create Assets** screen, fill in the fields, such as Name, Asset ID, Model, Description, Plant, Parent Type/ Name.
4. Click **Create**.

Figure 7-5 Create Asset

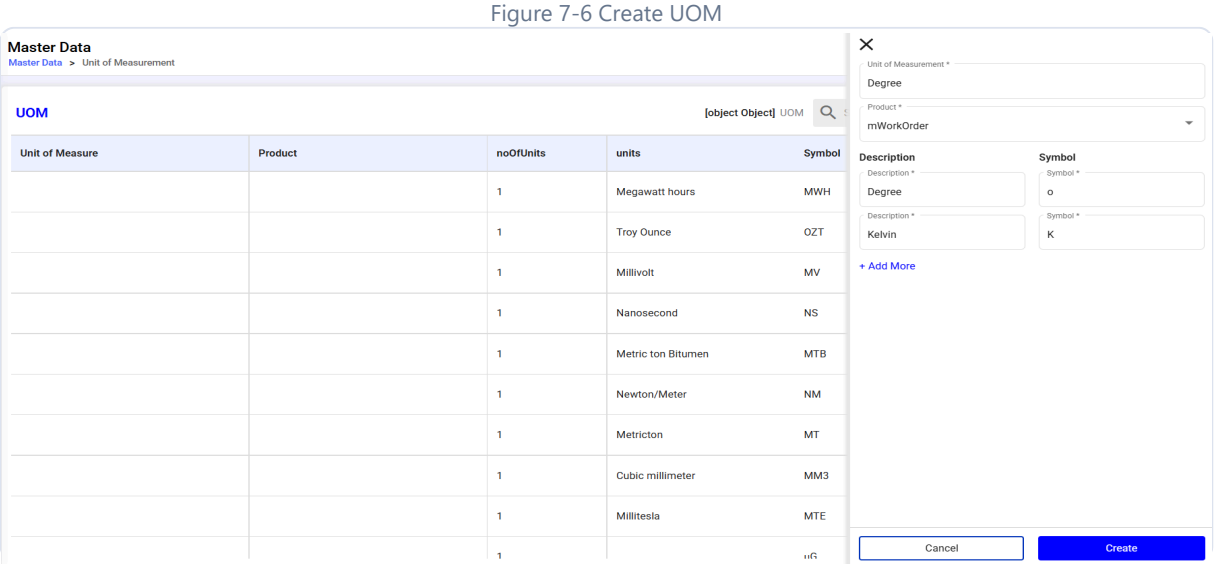


7.5. Create UOM

To create a UOM:

1. Navigate to **Master Data** > **Unit of Measurement**.
2. Click **Create New** > **Create Manually**.
3. In the **Create Unit** window, fill in the following fields:
    - Measurement Type, Description, Symbol.
    - Add more entries as needed.
4. Click **Create**.

Figure 7-6 Create UOM

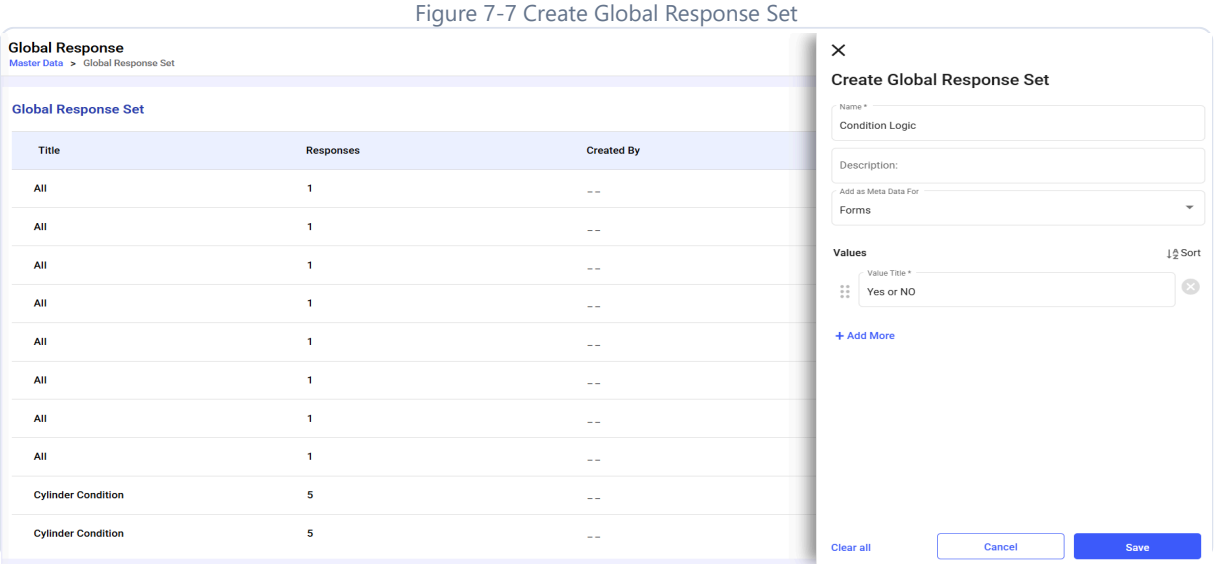


7.6. Create a Global Response Set

To create a global response set:

1. Go to **Master Data** > **Global Response Set**.
2. Click **Create New** > **Create Manually**.
3. In the **Create Global Response Set** window, fill in the following fields:
    - Name, Description, and Metadata Type.
    - Add response values.
4. Click **Save**.

Figure 7-7 Create Global Response Set



7.7. Bulk Upload Master Data

Bulk upload reduces manual effort for setting up master data.

To bulk upload master data:

1. Navigate to the respective module (Locations, Assets, UOM, or Response Sets).
2. Click the More icon on top right corner and select **Download Template**.
3. Open the downloaded Excel template and fill in the required data.
4. Click **Create** > **Upload Excel**.
5. Select the Excel file and upload it.

8. Configure iPermits Settings

The **Core Settings** in iPermits define how key features behave across your organization. These settings control fundamental aspects of daily use, such as mobile bottom navigation, dashboard availability, and AI-powered capabilities.

Although these options are stored at the database level, they directly influence how requesters, reviewers, authorizers, and issuers experience iPermits on both web and mobile. Functional teams should review these configurations to ensure they align with site workflows and safety processes, while IT teams may assist in applying and validating the changes.

By configuring these core settings, you can tailor iPermits to match your organization's operational needs, improve usability, and enforce consistent user experiences across roles and plants.

Note:

To modify the configurations, use the below collection in the database. Tap on the collection to view the list of configurations, each identified by its respective "**type**".

Collection Name: Configuration

8.1. Enable or Disable Modules

The Bottom Navigation, Dashboard Availability modules can be enabled or disabled at the **tenant** level. These settings determine whether the modules are visible and accessible across the web and mobile applications.

- Use the **tenantLevel flag** to turn a module on or off globally for all plants.

1. **tenantLevel Flag**
    - - **Purpose**: Controls module access at the **Tenant** level.
    - **Options**:
        - true: Enables the configured iPermits feature (for example, AI Agents) for all plants under the tenant.
        - false: Disables the configured iPermits feature globally across all plants.
        - **Default Value**: true

2. ◦ Set as true if you want all plants to access the EHS Module.
   ◦ Set as false to completely disable the EHS Module across the tenant.

```
Sample Configuration
Sample Configuration

  "_id": {
    "$oid": "6811d64e10cbda7d4d979883"
  },
  "type": "issueConfig", //Type would change for WorkOrder and Timesheet modules
  "config": {
    "tenantLevel": true,

  }
```

Note:
When a module is disabled, both their creation and any related features will be hidden and inaccessible across the Mobile and Web applications.

8.2. Configure Dashboard Availability (Mobile)

This configuration controls whether the Dashboard feature is available in iPermits Mobile application. While the feature enablement is configured at the plant level, dashboard visibility and content are governed by user roles/personas, ensuring users only see dashboards relevant to their responsibilities.

These configurations allow you to:

- Enable or disable access to Permit Overview Dashboards and custom dashboards.
- Control whether dashboard entry points are visible in the UI .
- Ensure dashboards are available only to permitted roles/personas.

```
Sample Configuration
  {
  "_id": {
    "$oid": "695bb3abe6af25cdab2ccdab"
  },
  "type": "permitFeatureFlags,
  "config": {,
    "dashboard": true
  },
  "plant": {
    "$oid": "681a06b3aab43f5e132ff5c3"
  }
```

Configure Session Timeout

Session timeout settings define how long a session remains active during inactivity.

- Session timeout can be configured at Tenant Level or Plant level.
- Default Session Timeout is at tenant level and set for 30 mins.
- All sessions login and logouts are captured in DB for audit purposes.
- The highlighted DB values should be used to manage Session timeout.
    - Session Timeout can be Enabled or Disabled by setting True or False.
    - Duration can be set in Million Seconds. Ex 30 mins/ 1800000 Ms


```
{
  "_id": {
    "$oid": "6788b5dec3ca9a2f538dbc1c"
  },
  "type": "sessionTimeout",
  "plant": {
    "$oid": "681a06b3aab43f5e132ff5c3"
  },
  "config": {
    "enabled": true,
    "duration": 1800000
  }
}
```


Table 8-1 Default Settings

Setting	Default Value	Description
dashboard	TRUE	Dashboard is visible in the application

8.3. Configure Session Timeout

User Session timeout settings define how long a session remains active during inactivity. .

- Session timeout can be configured at Tenant Level or Plant level.
- Default Session Timeout is at tenant level and set for 30 mins.
- All sessions login and logouts are captured in DB for audit purposes.
- The highlighted DB values should be used to manage Session timeout.

- Session Timeout can be Enabled or Disabled by setting True or False.
- Duration can be set in Million Seconds. Ex 30 mins/ 1800000 Ms.


```
  "_id": {
    "$oid": "6788b5dec3ca9a2f538dbc1c"
  },
  "type": "sessionTimeout",
  "plant": {
    "$oid": "681a06b3aab43f5e132ff5c3"
  },
```

```
  "config": {
    "enabled": true,
    "duration": 1800000
  }
```


TA warning message is displayed when the session times out and is redirected to the login screen.

8.4. Configure Bottom Navigation (Mobile)

The Bottom Navigation configuration controls which tabs are visible in the iPermits mobile application for each persona. This allows administrators navigation based on user roles and responsibilities.

These configurations allow you to:

- Define persona-based navigation menus.
- Control access to the tabs.
- Simplify navigation for approval-focused roles.

These configurations ensure a smooth, predictable user experience while aligning iMaintenance with your organization's compliance and collaboration needs.

Sample Configuration{


```
  "_id": {
    "$oid": "68a2f38824677585ffab4b0f"
  },
  "type": "permitNavigation",
  "config": {
    "personaNavigation": {
      "Requester": [
        "Home",
        "Permits",
        "JHA",
        "Work Orders",
        "Issues",
        "Alerts",
        "More"
      ],
      "Default Developer Role": [
        "Home",
        "Permits",
        "JHA",
        "Work Orders",
        "Issues",
        "Alerts",
        "More"
      ],
      "Reviewer": [
        "Home",
        "Permits",
        "Work Orders",
        "JHA",
        "Issues",
        "Alerts",
        "More"
      ],
      "Authorizer": [
        "Home",
        "Permits",
        "More"
      ],
      "Issuer": [
        "Home",
        "Permits",
        "More"
      ],
      "Supervisor": [
        "Home",
        "Work Orders",
        "Issues",
        "Alerts",
        "More"
      ],
      "Permit": [
        "Home",
        "Permits",
        "JHA",
        "Work Orders",
        "More"
      ]
    }
  },
  "status": 1,
  "plant": {
    "$oid": "682319d8c23c1557532a3944"
  }
```


}

Table 8-2 Default Settings

Setting	Default Value	Description
personaNavigation.Requester	As configured	Bottom navigation tabs visible for the Requester persona
personaNavigation.Default Developer Role	As configured	Bottom navigation tabs visible for the Default Developer Role persona
personaNavigation.Reviewer	As configured	Bottom navigation tabs visible for the Reviewer persona
personaNavigation.Authorizer	As configured	Bottom navigation tabs visible for the Authorizer persona
personaNavigation.Issuer	As configured	Bottom navigation tabs visible for the Issuer persona
personaNavigation.Supervisor	As configured	Bottom navigation tabs visible for the Supervisor persona
personaNavigation.Permit	As configured	Bottom navigation tabs visible for the Permit persona

8.5. Configure AI

The AI configuration controls the availability of AI-powered features in iPermits at the plant level. Administrators can selectively enable or disable individual AI agents based on rollout strategy and readiness.

Table 8-3 Default Settings

Setting	Default Value	Description
aiPPE	TRUE	AI-based PPE recommendations
aiPermitRecommendation	TRUE	AI suggestions for permit setup

Sample Configuration

```
{
  "_id": {
    "$oid": "68c011ca76dee942e5397e11"
  },
  "plant": {
    "$oid": "682319d8c23c1557532a3944"
  },
  "type": "aiPermit",
  "config": {
    "aiPPE": true,
    "aiPermitRecommendation": true
  }
}
```

Note:

- AI configurations are stored in the database and can be customized per tenant or plant.
- Ensure consistent settings across modules and levels to avoid unexpected behavior in AI feature availability.

9. Integration Setup

This section explains how to integrate Work Order data or other source systems into iPermits to enable permit creation and ensure permits are aligned with operational work planning and execution.

In **iPermits**, external system integration focuses on ensuring the **availability of Work Order data**, which is a mandatory prerequisite for Permit creation. Permit workflows are designed to be initiated against a valid Work Order. As a result, tenants must ensure that **Work Order data is available and synchronized** in the platform database before users can create and execute permits.

Rather than treating "ERP integration" as a generic setup requirement, iPermits requires integration of Work Order data, regardless of the source system. This ensures that permit workflows remain tightly coupled with operational work planning and execution.

Work Order data can be sourced from:

- **ERP systems** (for example, SAP), or
- A **Transactional Data Repository** integrated with the Innovapptive platform.

Business Impact

- Ensures permits are always raised against valid, traceable work orders.
- Maintains alignment between safety workflows and operational execution.
- Prevents orphan permits and improves auditability and compliance.
- Enables consistent permit workflows across web and mobile applications.

9.1. Understand the Integration Workflow

Integration Manager supports three types of data synchronization:

Type	Description
Inbound Integration	Imports master data (plants, locations, assets) from ERP to the Innovapptive platform. Usually done during tenant on-boarding.
Outbound Integration	Pushes transactional data (e.g., issues, work orders) from the platform to ERP.
Delta Sync	Periodically syncs offline transactions by detecting and posting new/updated records once connectivity is restored. Runs via a scheduled cron job (every 2–4 hours).

This ensures that permit data, isolation status, and safety records remain consistent across both web and mobile experiences.

9.2. Connect Work Order Data to iPermits

CConnecting Work Order data is a one-time integration setup during tenant onboarding or platform configuration.

Once Work Order data is available:

- Users can select valid Work Orders while creating permits.
- Permit workflows (approval, execution, closure) function as designed.
- Permit records remain contextually linked to operational activities.

10. Design and Manage Permit Template

This section explains how administrators can create and manage permit templates to standardize permit structure, validations, and compliance across plants.

Permit Templates define the structure, sections, and mandatory fields used to create permits in iPermits. Admins configure permit templates to align with plant-specific safety procedures and compliance requirements, ensuring consistent permit creation, validation, and execution across web and mobile applications.

This section has the following topics:

- Create Permit Template *(on page 46)*
- Configure Permit List View *(on page 50)*

10.1. Create Permit Template

Configure and define the permit template with sections and required fields based on specific business use cases and plant requirements.

Create Permit Template – Manually

To create a permit template:

1. Expand the **EHS** module and click **Authoring**.

   The **Permits** tab is displayed with a list of permit templates.

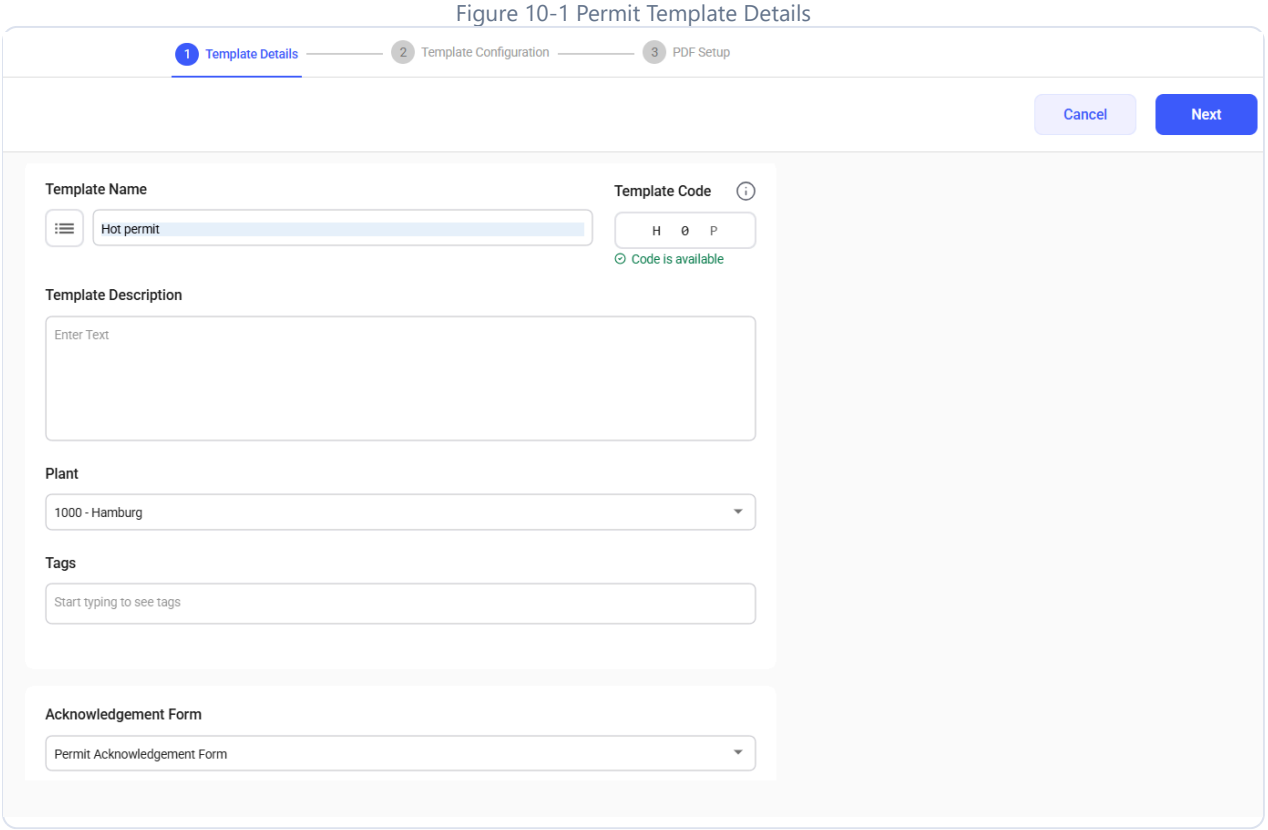
2. Click the **Create Manually** button on top right.

3. In the Template Details screen, provide the following information:

Field	Description
Template Name	◦ Click the Hamburger icon to select the Permit Type (For example, Hot Work, Mechanical, Work on Height, Confined Space, Radiation, Lifting, Electrical, and so on). ◦ Select an appropriate icon to visually represent the permit type (for example, a red flame icon for Hot Work permits and a confined space icon for Confined Space permits). ◦ Enter a unique name in the text box for the permit template (e.g., Mechanical Work Permit).
Template Code	Provide the required template code with 2 characters (letters/numbers).
Template Description	Describe the purpose of the template.
Plant	Select the applicable plant.
Tags	Add tags to categorize the template.
Acknowledgement Form	Select the required form applicable to the selected plant.
Additional Forms	Select the required additional forms.

4. Click **Next**.

Figure 10-1 Permit Template Details



5. In the Template Configuration screen:

   a. Add Sections within each page.

> **Note:**
> Default sections with fields are auto populated to help you get started. You can modify them or add new sections as required.

   b. Insert Fields (Questions) into sections.

   c. Select Response Type (Text, Number, Slider, Multiple Choice, etc.).

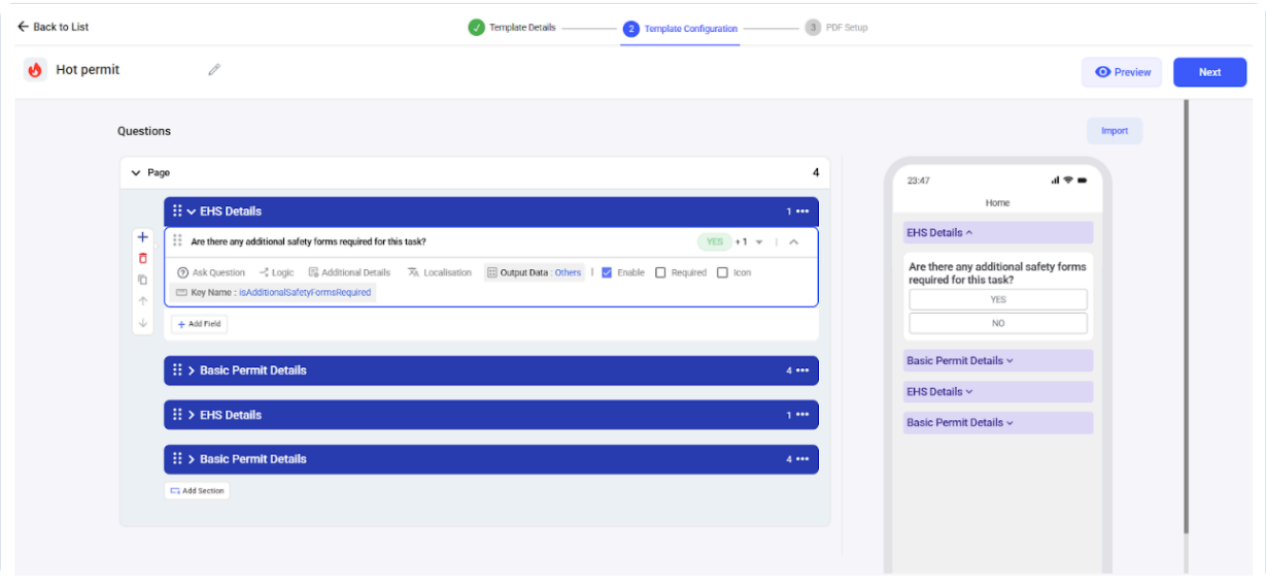
Response Type	Description	Supported Properties
Text	Free text input (e.g., title, descriptions).	Add Logic, Default Value, Additional Details, Localization, Enable, Required, Type
Number	Numeric values field	Add Logic, Default Value, Additional Details, Localization, Enable, Required, Unit, History, Range, Formula, and Unit of Measurement (UoM)
Date & Time	Calendar input for date & time values.	Additional Details, Localization, Enable, Required, Date & Time Format
Search Text	Searchable text field for selecting values from Dropdown.	Add Logic, Input Data, Localization, Enable, Required
Attachments	Uploads documents or files (PDFs, DOCs, Voice, Image, etc.).	Additional Details, Localization, Enable, Required, Attachment Details
Multiple choice	Allows to select one or more options from a predefined list.	Add Logic, Additional Details

   d. Add required properties.

Property/Attribute	Description
Ask Question	Allows you to add sub questions based on the condition.
Logic	Enables conditional rules for a field (show/hide Field/Section, Raise Issue, Mandatory field/ Section etc.) based on field values.
Default Value	Pre-fills the field with a value when the form loads in mobile application.
Format	Allows you to display the text in short text or paragraph.
Additional Details	Allows you to define character limit or extra metadata for users.

6. You can reuse sections and questions from existing Published or Draft permit templates to avoid rework and maintain consistency.
    - Click **Import** and select the permit template required from the list.
    - Click **Use** to import the selected content into the current permit template.
7. Click **Preview** to see how the template appears in both web and tab applications.
8. Click **Next**.

Figure 10-2 Permit Template Configuration



9. In the **PDF Setup** screen, click **Publish**.

> **Note:**
> You can configure the PDF on the left side pane to customize what information should appear in the PDF such as Logo, Header, Footer, Body Content, etc.

10.2. Configure Permit List View

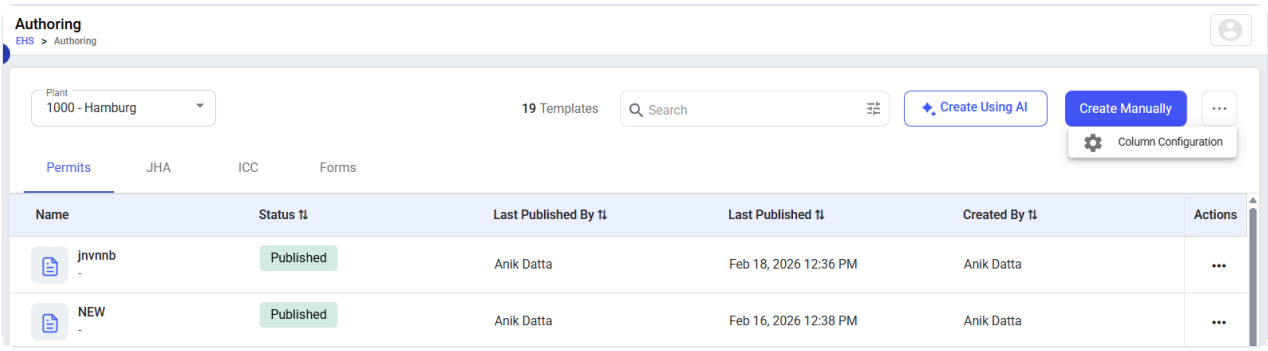
You can personalize the Permit list view by choosing which columns are visible, helping you focus on the information that matters most to you.

To configure the view:

1. Navigate to **EHS** → **Authoring** from the left navigation panel.
2. Go to the **Permit** tab.
3. Click the **More** options (⋯) icon next to Create Manually.

4. Select **Column Configuration**.

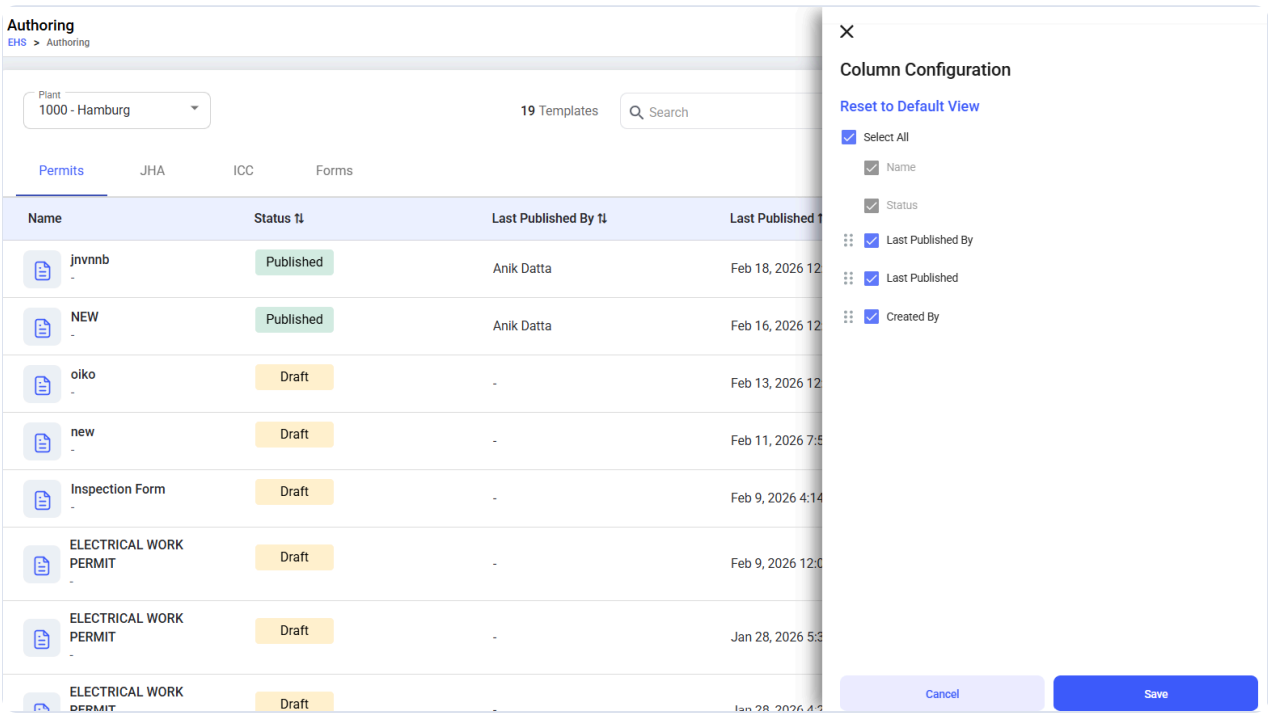
Configure Permit List



5. Select or clear the columns you want to display (for example, Name, Status, Last Published By, Last Published, Created By).

6. Click **Save** to apply the changes.

Column Configuration



11. Design and Manage JHA Template

This section explains how administrators can create and manage JHA templates to standardize JHA structure, validations, and compliance across plants.

The JHA Template Creation process allows admins to define the structure, fields, and sections used to capture job steps, hazards, control measures, and risk assessments. These templates standardize how JHAs are created and executed across the plants.

This section has the following topics:

- Create JHA Template *(on page 52)*
- Configure Permit Template List *(on page 54)*

11.1. Create JHA Template

This section explains how to create and configure a Job Hazard Analysis (JHA) template in iPermits, including defining job steps, hazards, control measures, and PDF output.

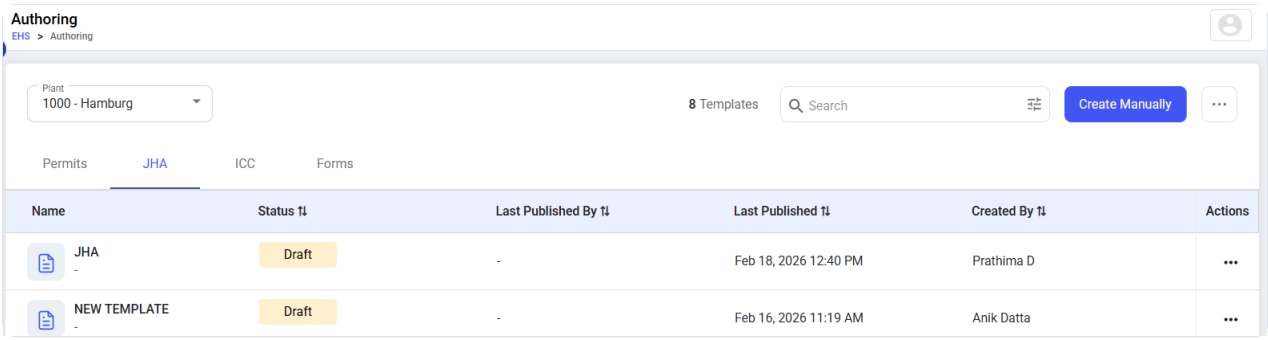
Create JHA Template:

1. Expand the **EHS module** and click **Authoring**.
2. Go to the **JHA tab**.

   The JHA tab is displayed with a list of JHA templates.

3. Click the **Create Manually** button at the top right.

Create JHA Template

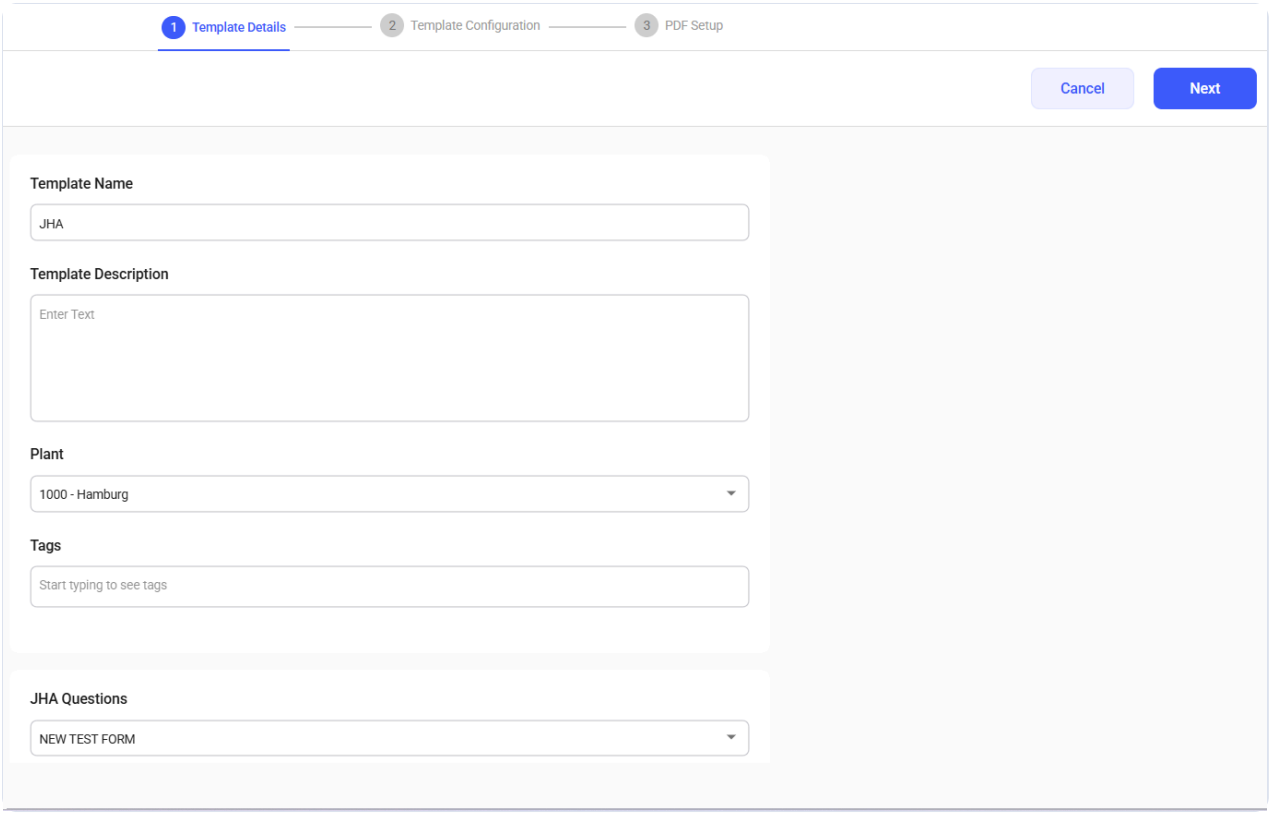


4. In the Template Details screen, provide the following information:

Field	Description
Template Name	Enter a unique name for the JHA template
Template Description	Describe the purpose of the JHA template.
Plant	Select the applicable plant.
Tags	Add tags to categorize the JHA template for easy search and filtering.
JHA Questions	Select or configure the standard JHA questions to be included in this template.
Additional Forms	Select any additional forms (for example, inspection or acknowledgement forms) that must be completed along with the JHA.

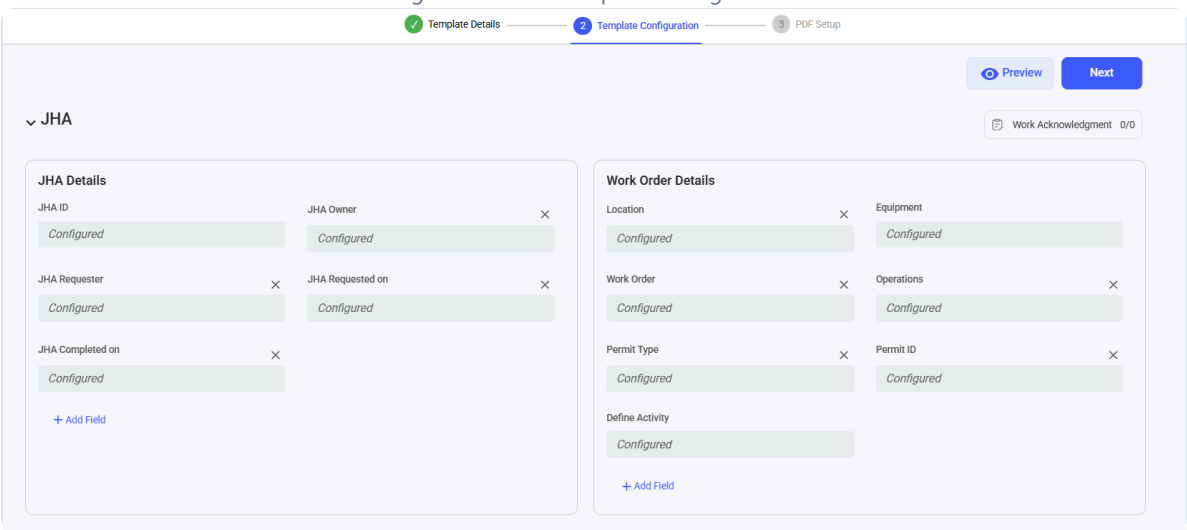
5. Click **Next**.

Figure 11-1 JHA Template Details



6. In the Template Configuration screen:
    a. Define the job steps in the JHA table.
    b. Configure sections such as Potential Hazards, Control Measures, and Risk Assessment.
    c. Add fields (questions) within each section as required.
    d. Select appropriate response types (Text, Number, Multiple Choice, Pick List, etc.).
    e. (Optional) Configure Equipment, Training, and Inspection sections to capture surrounding or related risks.
    f. (Optional) Configure Attachments and Notes for each step to allow field users to add photos and observations.
    g. Click **Preview** to see how the JHA template appears in both web and mobile applications.
    h. Click **Next**.

Figure 11-2 JHA Template Configuration



    i. In the PDF Setup screen, configure the PDF layout as required.
    j. Click **Publish**.

> **Note:**
> You can configure the PDF from the left pane to control what information appears in the exported document, such as Logo, QR code, Header, Footer, and Body Content.

11.2. Configure JHA List View

You can configure the columns displayed in the JHA list view to suit your preference.

To configure the view:

1. Navigate to **EHS** → **Authoring** from the left navigation panel.
2. Go to the **JHA** tab.
3. Click the **More** options (⋯) icon next to Create Manually.

4. Select **Column Configuration**.

5. Select or clear the columns you want to display (for example, Name, Status, Last Published By, Last Published, Created By).

6. Click **Save** to apply the changes.

   You can click Reset to Default View at any time to restore the default column layout.

12. Design and Publish Forms

This section explains how to create and manage configurable Forms that can be embedded into permits and JHAs to enforce safety and compliance before work begins.

Forms are configurable, reusable checklists (acknowledgements and inspection forms) that can be embedded into permits and JHAs to enforce mandatory safety and compliance checks before work proceeds. Administrators can create Forms either manually or using AI by converting existing documents into digital forms. Once published, Forms can be attached to relevant workflows to ensure consistent data capture, validation, and audit readiness across plants.

To create a form:

1. Expand the **EHS module** and click **Authoring**.
2. Go to the **Forms** tab.

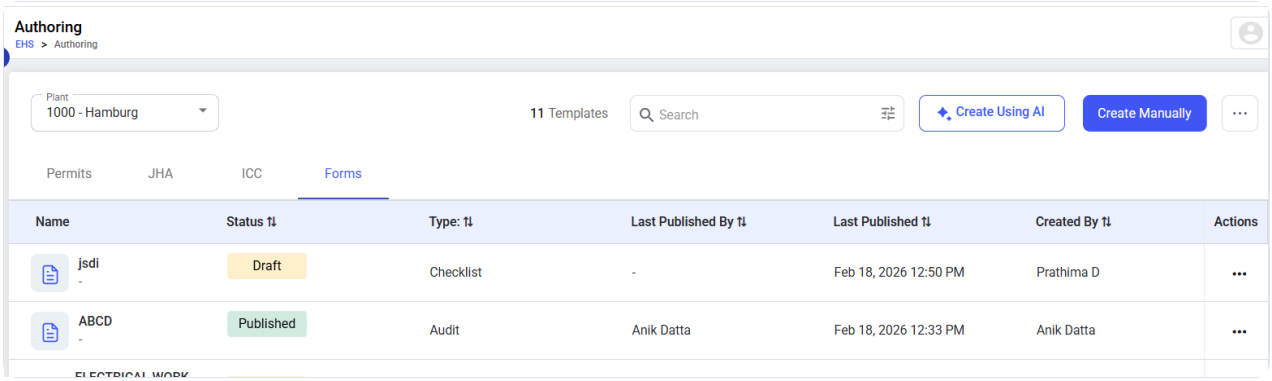
   The Forms tab is displayed with a list of Form templates

3. Click the **Create Manually** button at the top right (or click Create Using AI, if you want to generate a Form from an existing document).
4. Create **Form Template Manually**.
5. In the Template Details screen, provide the following information:

Field	Description
Template Name	Enter a unique name for the Form template
Template Description	Describe the purpose of the Form template.
Plant	Select the applicable plant.
Type	Select the Form type (for example, Acknowledgement, Audit, Checklist, JHA Questions, Atmospheric Logs, Zero Energy Test).

6. Click **Next**.

Figure 12-1 Create Forms Manually



7. In the Template Configuration screen:
    - Define the Form structure using Pages and Sections.
    - Add fields (questions) within each section as required.
    - Select appropriate response types (Text, Number, Yes/No, Pick List, Date, etc.).
    - Mark fields as Required, if mandatory completion is needed.
    - (Optional) Configure conditional logic to show or hide fields based on responses.
    - (Optional) Configure Default Values, formatting, and localization for fields.

    Each **Response Type** defines the field or input format used across the platform's authoring and execution modules

Response Type	Description	Supported Properties
Text	Free text input (e.g., title, descriptions).	Add Logic, Default Value, Additional Details, Localization, Enable, Required, Type
Number	Numeric values field	Add Logic, Default Value, Additional Details, Localization, Enable, Required, Unit, History, Range, Formula, and Unit of Measurement (UoM)
Date & Time	Calendar input for date & time values.	Additional Details, Localization, Enable, Required, Date & Time Format
Signature	Captures digital signatures from users.	Additional Details, Localization, Enable, Required
Hyperlink	Clickable link to web or document resources.	Additional Details, Localization, Enable, Required, Add Link
Add Photo	Upload images for visual evidence.	Additional Details, Localization, Enable, Required

Field Logic and Settings

- Set conditional logic (for example, show or hide fields or sections based on user responses), as described in the table below.
- Mark fields as Required, enable History, or apply Localization on business and compliance needs.

Response Type Properties

Add Logic	Enables conditional rules for a field (show/hide Field/Section, Raise Issue, Mandatory field/Section etc.) based on field values.
Default Value	Pre-fills the field with a value when the form loads in mobile application.
Additional Details	Allows admin to define character limit or extra metadata for users.
Localization	Allows admin to translate field labels into multiple languages.
Enable	Toggles whether the field is active and visible in the consumption.
Required	Marks the field as mandatory for submission.

8. Use **Preview** to see how the form appears in the mobile app.
9. Click **Next**.
10. In the PDF Setup screen, configure the PDF layout as required (Logo, QR code, footer text, body content visibility).
11. Click **Publish**.

13. Customize Platform Settings

This section explains how administrators can configure platform-wide settings that control mobile app behavior, appearance, and data synchronization to optimize user experience and performance.

The **Settings** module provides administrators with the tools to manage platform-wide preferences that directly affect the iMaintenance mobile application. These settings include storage behavior, theme configurations, and sync options that enhance user experience and app performance.

This chapter has the following topics:

- Manage Storage & Sync Settings *(on page 60)*
- Apply Theme Configurations *(on page 64)*
- Define Mobile Data Sync Preferences *(on page 61)*

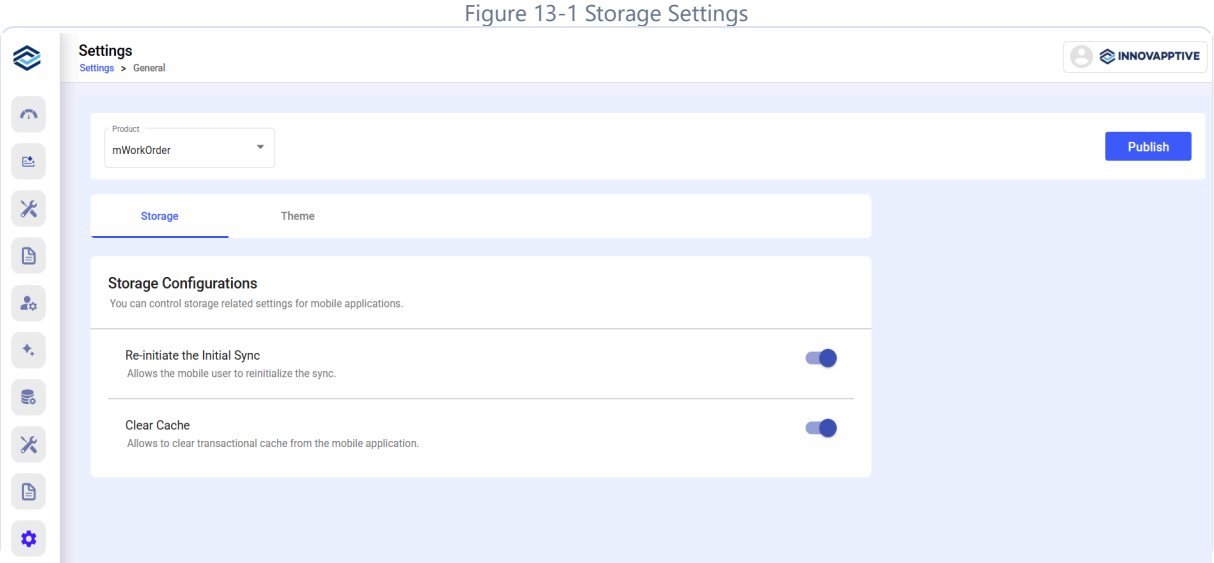
13.1. Manage Storage & Sync Settings

The **Storage** tab under **General** Settings allows admins to control how the mobile app handles data, including cache management and full sync initiation.

To manage storage and sync settings:

1. Navigate to **Settings** and click the **Storage** tab.
2. Select the **Product** (e.g., iMaintenance).
3. Enable or disable the storage related settings and click **Publish**.

Figure 13-1 Storage Settings



It has two primary options:

Setting	Description
Re-initiate Initial Sync	Enables mobile users to trigger a full sync with backend systems, useful when resolving sync issues or applying new configurations.
Clear Cache	Adds a "Clear Cache" button in the mobile app, allowing users to delete local data (junk/temporary files) to improve performance.

Once enabled and published the settings, they are applied to the selected product (e.g., iMaintenance) within the mobile application.

13.2. Define Mobile Data Sync Preferences

This feature lets you optimize how data is synchronized to mobile devices—minimizing sync times and improving app performance. Preferences can be set at **tenant**, **plant**, and **role** levels.

To define mobile data sync preferences:

1. Expand **Settings** and click **Mobile Data Preferences**.

2. Select the **Product** (e.g., iMaintenance).

The screen appears with two tabs:

Tab	Purpose
Global Data	Define default data fields for each plant (e.g., Maintenance Plant, Planning Plant)
Transactional Data	Define sync filters for Work Orders and Issues based on user roles

In this screen, you can,

- Rename or remove fields
- Add new fields
- Reorder fields
- Configure sync durations per role

Example: Supervisors may sync 7 days of data, while Technicians sync 3.

Figure 13-2 Global Data

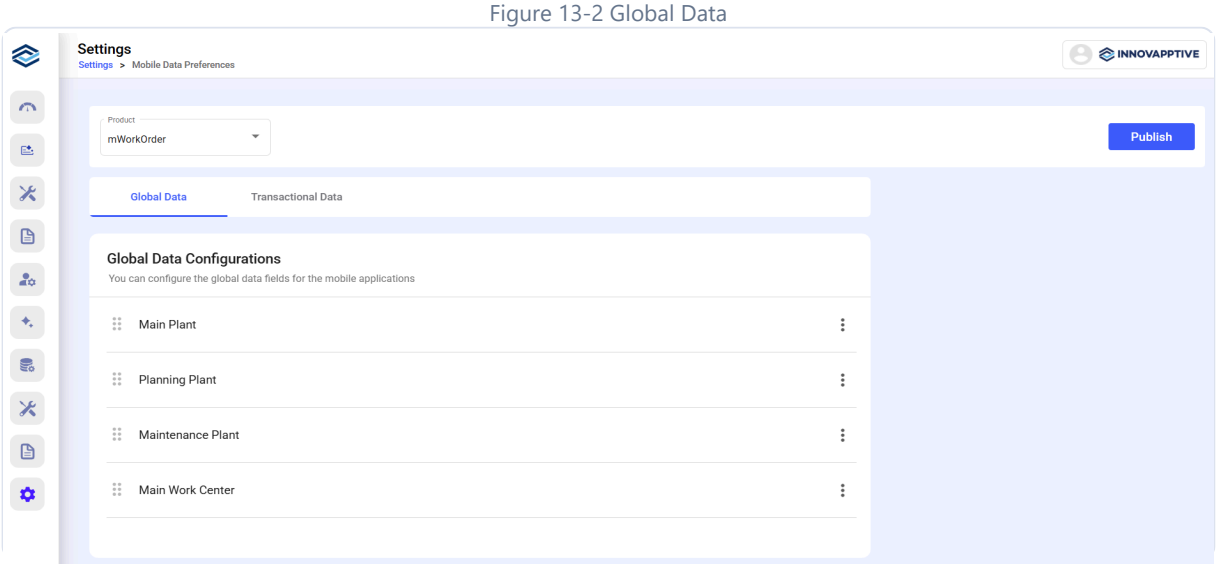
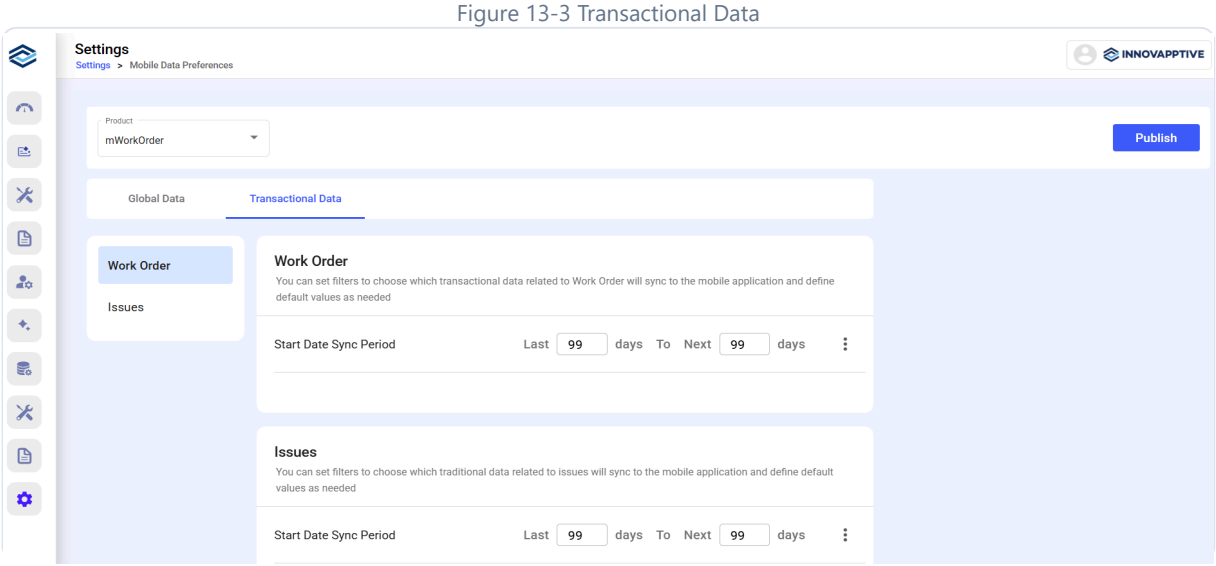


Figure 13-3 Transactional Data



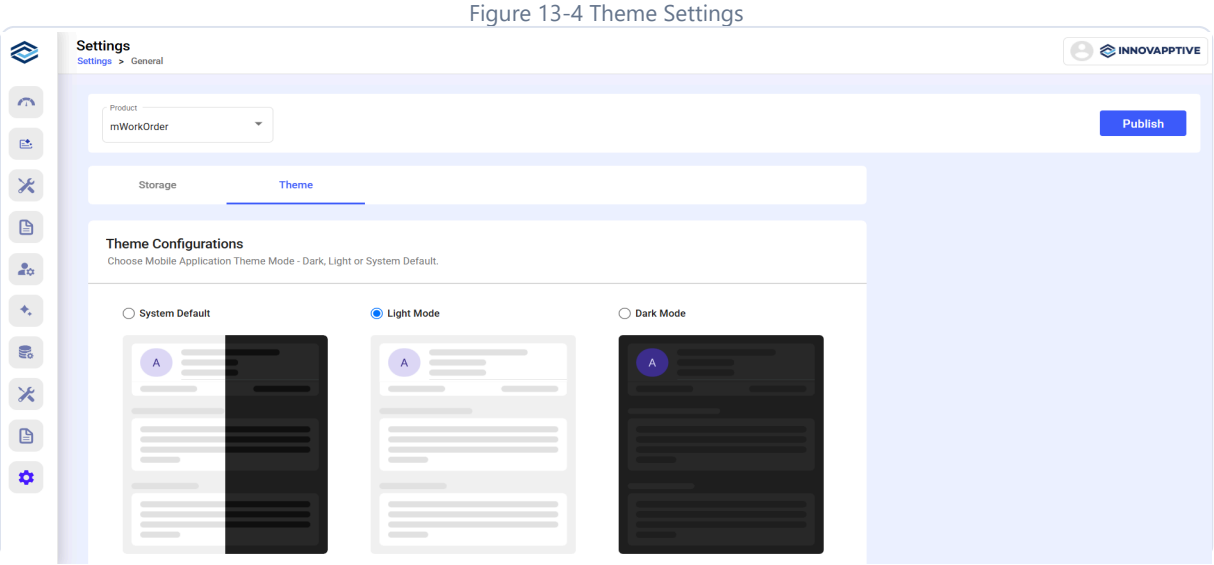
13.3. Apply Theme Configurations

Admins can customize the **visual appearance** of the iMaintenance mobile app using predefined themes to match user environments or company branding.

To apply theme configurations:

1. Navigate to **Settings** and click the **Theme** tab.
2. Select the **Product** (e.g., iMaintenance).
3. Choose a theme and click **Publish**.

Figure 13-4 Theme Settings



You can choose from the following mobile theme modes:

Mode	Description
System Default	Uses the theme based on the user's device setting (light/dark mode)
Light Mode	Clean, bright interface with dark text—ideal for daylight use
Dark Mode	Low-light UI for night shifts or dim environments (e.g., mining, manufacturing)

Theme preferences apply globally for that product once published.

14. Set Up Notifications

The Notification Engine gives administrators control over system-generated alerts, helping teams stay informed about workflow events without being overwhelmed. It's integrated with the iPermit mobile app, enabling flexible communication across devices.

Understand the Notification System

The notification system is built to support automated communication based on user actions and workflow milestones. It uses third-party services for email delivery and is governed by built-in templates and logic.

Key components:

Component	Description
Recipients	Defines who gets notified (e.g., reviewers, authorizers, technicians etc.)
Timing	When notifications are triggered (e.g., assignment, completion)
Content	Predefined messages that communicate what happened
Type	The nature of the event (e.g., permit raised, permit closed etc.)

These controls ensure that users receive timely alerts relevant to their role—improving visibility without unnecessary noise.