

PUBLIC
SAP Service and Asset Manager
Document Version: 2511 – 2026-11-24

SAP Service and Asset Manager Configuration Guide

© 2026 SAP SE or an SAP affiliate company. All rights reserved.

Content

1 Features and Personas Configuration Matrix. 9

2 General Configurations. 77

2.1 Mobile Configuration Variant Tool Overview. 77

Variant Tool - Search Screen. 79

Configuring Variant General Settings. 80

Configuring Feature Toggles. 82

Configuring Mobile Application Parameters. 84

Configuring oMDO Filter Settings. 85

2.2 Configuring Personas and Features Overview. 87

Usage Types. 88

Configuring Personas. 89

Configuring Features. 93

Configuring Component Assignments. 101

2.3 Enabling and Disabling Features Per User Through SAP Authorization. 102

2.4 Configuring Notification Catalog Types. 106

2.5 Configuring Mobile User Attributes. 108

Recommended Configuration for Multiple Plants and Work Centers. 111

2.6 Removal of Dependent Objects Based on Lead Objects. 113

3 Persona Configurations. 116

3.1 Maintenance Technician Configuration. 116

Configuration Limitations - Maintenance Technician Persona. 118

Data Distribution Model Overview. 118

Mapping Work Orders to a STARTED Status - Overview. 134

Technical Objects Configuration. 135

OData Channel Integration Settings Procedures. 146

3.2 Field Logistics Configuration. 159

Assigning and Unassigning a Feature - Back End. 161

Enabling and Disabling a Feature - Back End. 162

Assigning and Unassigning an OMDO to a Feature - Back End. 163

Configuring Data Distribution - Back End. 165

Mobile Application Parameters - Back End. 169

3.3 Extended Warehouse Clerk Configuration. 170

Configuration Prerequisites and Limitations - Extended Warehouse Clerk. 171

General Feature Configuration - Extended Warehouse Clerk. 173

Mobile Application Parameters - Extended Warehouse Clerk. 174

oMDO Configuration - Extended Warehouse Clerk. . . . 175
3.4 Field Service Technician Configuration. . . . 176
Field Service Technician Configuration on a Customer Service Back End. . . . 177
Field Service Technician Configuration for SAP S/4HANA Service Order Scenario. . . . 205
3.5 Safety Technician Configuration. . . . 215
Configuration Prerequisites and Limitations - Safety Technician Persona. . . . 216
General Feature Configuration - Safety Technician Persona. . . . 218
Mobile Application Parameters - Safety Technician Persona. . . . 220
General oMDO Configuration - Safety Technician Persona. . . . 221
General Exchange Configuration - Safety Technician Persona. . . . 224
Work Order as a Dependency - Safety Technician Persona. . . . 225
Supported Usage Types - Safety Technician Persona. . . . 226
General User Parameters Configuration - Safety Technician Persona. . . . 227
3.6 Inventory Clerk Configuration. . . . 228
Configuration Prerequisites and Limitations - Inventory Clerk Persona. . . . 229
SAP Transactions Supported by Inventory Clerk 231
Application Features Assigned to Inventory Clerk 232
Configuring Data Distribution 236
Mobile Application Parameters 238
Configuring Printing 240

4 Feature Configurations. . . . 242
4.1 AI-Assisted Job Completion - Configuration. . . . 242
Configuring AI-Assisted Job Completion - BTP Mobile Services Connectivity. . . . 243
Configuring SAP Service and Asset Manager Security Settings to Access AI-Assisted Job Completion. . . . 245
Setting Up Roles and Role Collections for AI-Assisted Job Completion Users. . . . 248
Configuring AI-Assisted Job Completion - Back End - Enabling the Feature. . . . 249
4.2 ASPM and PdMS Configuration. . . . 250
Configuring Checklist Parameters. . . . 250
Setting Up an ASPM Connection to the ASPM System to Use Checklists. . . . 252
4.3 Assignment Management of Safety-Related Features. . . . 261
Configuring Assignment Type 1 (User Plant). . . . 263
Configuring Assignment Type 2 (User Work Center). . . . 266
Configuring Assignment Type 3 (User Planner Group). . . . 268
Configuring Assignment Type 4 (Partner Function). . . . 270
Configuring Assignment Type 5 (Selection Variant). . . . 276
Configuring Assignment Type 6 (Operational List + Selection Variant). . . . 281
4.4 Attachments - Abstract Document Management. . . . 287
Configuring Document Management. . . . 289
DMS Method. . . . 291
GOS Method. . . . 292

BDS Method. . . . 293
Other Method. . . . 294
SAM Document Data Filter. . . . 294
4.5 Auto-Resize Images with a Configured Maximum Size. . . . 302
4.6 Auto-Sync Configuration. . . . 303
Configuring Auto-Sync - Back End - Enabling the Feature. . . . 305
Configuring Auto-Sync - Back End - Mobile Application Parameters. . . . 305
Common Use Cases for Configuring Auto-Sync. . . . 309
4.7 Catalog Profiles Configuration. . . . 310
Configuring Catalog Profiles - Back End - Mobile Application Parameters. . . . 311
Configuring Catalog Profiles - Back End - OMDO Filters. . . . 313
4.8 CATS and PM Confirmation Time Entries Configuration. . . . 314
Allow Technician to Enter Time for Another Technician - Configuration. . . . 316
4.9 Clock In Clock Out Configuration. . . . 318
4.10 Confirmation Scenarios Configuration. . . . 319
Configuring Confirmation Scenarios - Back End - SAP GUI. . . . 321
Configuring Confirmation Scenarios - Back End - Mobile Application Parameters. . . . 326
Configuring Confirmation Scenarios - Back End - Enabling the Feature. . . . 328
4.11 Customer Service Notification Types Configuration. . . . 330
4.12 Customer Service Order Types Configuration. . . . 331
4.13 Digital Signature Overview. . . . 332
Enabling Digital Signature. . . . 333
Setting up the TOTP_2E Signature Strategy. . . . 335
Troubleshooting: Unable to Unregister the Device. . . . 339
4.14 Defense and Security Features Configuration. . . . 340
4.15 EAM Phase Model Configuration - Overview. . . . 341
Non-Phase Model Configuration. . . . 342
Phase Model Configuration. . . . 359
Phase Model + Non-Phase Model Configuration. . . . 381
4.16 EPD Visualization Configuration. . . . 403
4.17 Field Operations Worker Configuration. . . . 405
Differentiating a Base SAP Service and Asset Manager Work Order from a Field Operations Worker Order. . . . 406
4.18 FSM Crew Configuration. . . . 408
Configuring FSM Crew Integration - Back End - Enabling the Feature. . . . 409
Configuring FSM Crew Integration - Back End - oMDO. . . . 410
4.19 FSM Crowd Service Configuration. . . . 411
Configuring FSM Crowd Service - BTP Mobile Services Connectivity. . . . 413
Configuring FSM Crowd Service - Back End - Enabling the Feature. . . . 417
Configuring FSM Crowd Service - Back End - oMDO. . . . 418
4.20 FSM Smartforms Configuration for Maintenance Technician. . . . 420

4.21 Geospatial Service Definitions. . . . 421
ArcGIS. . . . 423
4.22 Guided Workflow Configuration. . . . 438
Creating a New Workflow - Back End. . . . 440
Creating a New Work Step - Back End. . . . 441
Modifying an Existing Workflow - Back End. . . . 442
Configuring Notifications with Workflows - Back End. . . . 443
4.23 Inbound Delivery Process Configuration (Extended Warehouse Clerk). . . . 445
4.24 Isolation Certificate Configuration. . . . 446
Configuring Isolation Cerificates - Back End - Enabling the Feature. . . . 448
4.25 Linear Asset Management Configuration. . . . 449
Disabling and Re-Enabling Linear Asset Management. . . . 450
Adding Linear Data for Characteristics. . . . 450
4.26 Local Object Mobile Status Configuration. . . . 451
4.27 Location Tracking Configuration. . . . 452
Configuring Location Tracking - Back End - Mobile Application Parameters. . . . 454
Accessing User Location Data - Back End - MAIF Administration Potral. . . . 455
4.28 Low Code No Code Support 458
Showing Customized Fields on the Detail Screen 459
Showing Customized Fields on the List Screen. . . . 460
Adding Customized Fields to the Search Criteria. . . . 462
4.29 Meter Management Configuration. . . . 463
Binding ISU Process Type to Work Order Type. . . . 464
Binding Meter Reading Notes Based on ISU Process Type. . . . 465
Meter Reading History Interval Definition. . . . 465
Binding Meter Reading Reasons Relevant for Technical Installation. . . . 466
4.30 Namespace Check Configuration. . . . 467
4.31 Push Notifications Configuration. . . . 468
Configuring the Push Infrastructure. . . . 470
Configuring the Push Scenarios. . . . 476
Activating the Push Processing. . . . 493
4.32 Online Search Configuration. . . . 515
Configuring Online Search - Back End - Enabling the Feature. . . . 516
Configuring Online Search - Work Orders and Notifications. . . . 517
4.33 Operational Item Configuration. . . . 521
4.34 Quality Management Configuration. . . . 523
Configuring Quality Management Notification Parameters. . . . 523
Configuring oData MDO Data Filters for Quality Management. . . . 525
Inspection Lots. . . . 527
EAM Checklist Overview. . . . 529
PM/EAM Checklists. . . . 535

4.35 Samsung Knox Capture Configuration. . . . 536
Configuring Samsung Knox Capture - Back End - Mobile Application Parameters. . . . 538
4.36 SAP Dynamic Forms Configuration for SAP Service and Asset Manager. . . . 540
Configuring SAP Dynamic Forms - Back End - Feature Configuration. . . . 542
Configuring SAP Dynamic Forms - Back End - Exchange Object. . . . 544
Identify Form Definitions for Client Download. . . . 546
Accessing Form Data from SAP Service and Asset Manager Metadata. . . . 547
4.37 Signature Control Configuration. . . . 549
4.38 Supervisor Mode Configuration. . . . 550
Work Order Operations State Machine for Maintenance Technician Persona. . . . 551
Work Order Assignment Type Configuration. . . . 552
Supervisor Roles and Team Assignment Type Configuration. . . . 553
Enabling the Supervisor Approval Process for Work Orders. . . . 555
Mobile Application Parameter Settings for the Supervisor Mode. . . . 556
Mobile Application Status Settings for the Supervisor Mode. . . . 559
Rejection Reason Configuration. . . . 559
4.39 Vehicle Stock Look Up Configuration. . . . 560
Configuring Vehicle Stock Look Up - Back End - Enabling the Feature. . . . 561
Configuring Vehicle Stock Look Up - Back End - OMDO Filters. . . . 562
4.40 Work Approval Configuration. . . . 563
Configuring Work Approvals - Back End - Mobile Application Parameters. . . . 564
4.41 Work Permit Configuration. . . . 565
Configuring Work Permits - Back End - Enabling the Feature. . . . 569
4.42 Work Permit Approvals Configuration. . . . 569
Configuring Work Permit Approvals - Back End - SAP GUI. . . . 571
Configuring Work Permit Approvals - Back End - Mobile Application Parameters. . . . 574
4.43 Work Order Operations Split Assignment for Maintenance Technician Persona. . . . 576
Split Assignment Status Flow . . . 576
4.44 Zebra Scanner Configuration. . . . 578
Configuring Zebra Scanner - Back End - Mobile Application Parameters. . . . 579

5 Performance Optimization. . . . 582
5.1 Delta Sync Optimization. . . . 582
Downloading Only Modified Entities. . . . 582
Upload Only Configuration. . . . 585
Lead Entity Based Flow Overview. . . . 588

6 Appendix. . . . 602
6.1 Supported SAP Transaction Codes for SAP Service and Asset Manager. . . . 602
6.2 User Parameter IDs. . . . 606
6.3 Mobile Application Integration Framework Configurations. . . . 607
Accessing the SAP Mobile Add-On for SAP Configuration Panel. . . . 608

Panels, Tabs, and Field Descriptions. 609
Shadow Table. 681
Configuring Confirmation Posting Dates - Overview. 684
Copying an Object to the Customer Namespace. 687

7 Troubleshooting. 690
7.1 SAP Gateway Client. 690
7.2 SAP Gateway Error Logs. 691
7.3 SAP Gateway Statistics. 692
7.4 SAP Gateway Tracing Tools. 692

Document History

Before you begin reading this guide, be sure that you have the latest version. Find the latest version at https://help.sap.com/docs/SAP_SERVICE_ASSET_MANAGER.

The following table provides an overview of the most important document changes.

Document Version	Date	Description of Changes
1.0	NOV 2025	Original release of the *SAP Service and Asset Manager Configuration* guide, version 2511.

1 Features and Personas Configuration Matrix

> **Note**
>
> - Use the filter below to hide/show any columns.
> - This table lists features specific to SAP Service and Asset Manager. For general MAIF configurations, refer to MAIF Configuration Guide.

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide

Defense and Security Features	DEFENSE_INTEGRATION	SAP Service and Asset Manager supports the following features for the Defense and Security industry:
		• Flight order
		• Support defense-related properties in Materials
		  • NATO Stock Number (NSN)
		  • Manufacturer Part Number (MPN)
		  • Long Manufacturer Part Number (LMPN)
		• Condition codes
		• Master and critical equipment
		• Additional defense and security fields on supply docs and material master
		• Support edge mobile services
			Maintenance Technician (Pro)	Maintenance Technician (Pro): **NO**	2410		Defense and Security Features Configuration [page 340]	Working with Defense and Security Features

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Metadata Upgrade Tool	-	The SAP Service and Asset Manager Metadata Upgrade Tool is a cross-platform Electron application for upgrading and merging **customized** SAP Service and Asset Manager metadata with new out-of-box releases, with a focus on usability, transparency, and control.	-	-	2210	-	-	SAP Service and Asset Manager Metadata Upgrade Tool

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Delta Sync Optimization - Upload Only	CA_UPLOAD_ONLY	With the **Upload Only** feature, you can improve efficiency and optimize delta synchronization. This allows users to upload recorded transactions independently, without triggering an immediate download of delta data. Users may choose to upload transactions immediately after: • Completing a job • Completing all jobs for the day • Finishing their shift • Completing their daily or weekly work cycle **Note** • Users can still initiate a full delta sync at any time to download the latest delta data. • Please note that the Upload Only feature has specific characteristics and limitations regarding how data is synced between the back end and the mobile device. Before enabling this feature, we recommend reviewing the current limitations [page 586].	Maintenance Technician (Standard) Maintenance Technician (Pro) Maintenance Technician (External) Inventory Clerk	Maintenance Technician (Standard): **NO** Maintenance Technician (Pro): **NO** Maintenance Technician (External): **NO** Inventory Clerk: **NO**	2505		Upload Only Configuration [page 585]	Using the Upload Only Feature

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Push Notifications	-	Push notifications enable SAP Service and Asset Manager to inform mobile users when relevant business object changes occur in the SAP back end system, such as newly assigned work orders or notifications.	Maintenance Technician (Standard) Maintenance Technician (Pro) Maintenance Technician (External) Field Service Technician (Standard) Field Service Technician (Pro) Field Service Technician (External) Inventory Clerk Safety Technician Extended Warehouse Clerk Field Logistics	Maintenance Technician (Standard): **NO** Maintenance Technician (Pro): **NO** Maintenance Technician (External): **NO** Field Service Technician (Standard): **NO** Field Service Technician (Pro): **NO** Field Service Technician (External): **NO** Inventory Clerk: **NO** Safety Technician: **NO** Extended Warehouse Clerk: **NO** Field Logistics: **NO**	1911	-	Push Notifications Configuration [page 468]	-

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Split Assignment	-	With split assignment, you can work on multiple work orders or tasks simultaneously within the SAP Service and Asset Manager app. You are not limited to just one assignment. This approach promotes efficient team collaboration, ensures tasks are completed quickly, and provides flexibility in managing workload distribution.	Maintenance Technician (Standard) Maintenance Technician (Pro)	Maintenance Technician (Standard): **NO** Maintenance Technician (Pro): **NO**	2511		Work Order Operations Split Assignment for Maintenance Technician Persona [page 576]	Split Assignment
Hierarchy Control	-	The hierarchical user interface control ensures a clear visual display of the selected nodes of parent and children when searching or navigating a node structure. When navigating this type of hierarchal node structures, users can tap on a parent node to expand and view their children, as well as to navigate up or down from that node location, opening or closing nodes as going through.	Maintenance Technician (Standard) Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro)	Maintenance Technician (Standard): **YES** Maintenance Technician (Pro): **YES** Field Service Technician (Standard) **YES** Field Service Technician (Pro): **YES**	4.0		Hierarchy Control	Hierarchy Control Overview

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
FSM SAP Cloud Integration	-	SAP Service and Asset Manager supports integration with **SAP S/4HANA** and **Field Service Management** for Plant Maintenance Orders using *SAP Cloud Integration (SCI)*, requiring specific configuration. This integration is beneficial for streamlining maintenance processes and enhancing operational efficiency.	Field Service Technician (Pro)	Field Service Technician (Pro): **NO**	2511		FSM SAP Cloud Integration [page 204]	-
Field Logistics features	-	The Field Logistics persona supports the following functions: • Managing logistics for stock, non-stock, and supplier items. • Receiving items at remote plants, including containers, delivery items, handling units, and package items. • Downloading voyages and set them to arrive. • Scanning QR-codes for containers, handling units, delivery items, and voyage numbers.	Field Logistics	-	2505		Field Logistics Configuration [page 159]	SAP Service and Asset Manager User Guide - Field Logistics Persona

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Confirmation Scenarios	PM_CONFIRMATION_SCENARIOS	When working with an Operation or Suboperation on a Work Order, SAP Service and Asset Manager supports the following confirmation scenarios to help technicians quickly apply confirmations via a dynamic QR code. Both scenarios require two users with devices to add the confirmation to the object. • *Verification*: In this confirmation scenario, a maintenance technician requests another maintenance technician who has appropriate authorization to review and confirm that a job has been correctly performed. • *Cooperation*: In this confirmation scenario, the main technician records the work performed by another technician in a supportive role using the QR code generated by that technician. **Note** Depending on your configuration, you can also print out static QR codes for technicians to scan.	Maintenance Technician (Pro)	Maintenance Technician (Pro): **NO**	2511		Confirmation Scenarios Configuration [page 319]	Working with Confirmation Scenarios

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Extended Warehouse Clerk features	EWM_CORE_DATA	The Extended Warehouse Clerk persona supports the following functions: • Managing and optimizing storage bins • Goods movements • Managing physical inventory • Planning and Monitoring goods movements and warehouse stocks • Warehouse Control • Inbound Delivery and Inbound Delivery Items	Extended Warehouse Clerk	-	2505	SAP S/4HANA 2022 FPS00	Extended Warehouse Clerk Configuration [page 170]	SAP Service and Asset Manager User Guide - Extended Warehouse Clerk

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Inbound Delivery Process (Extended Warehouse Clerk)	-	As an Extended Warehouse Clerk, you can search, fetch, and download Inbound Deliveries and Inbound Delivery Document Items, to view all the relevant delivery details and statuses, as well as to to manage and execute tasks accurately during the receiving process. Key features of the inbound delivery process include: • Change Inbound Delivery documents (with single edits or bulk edits) • Create Warehouse Tasks (both manual and auto-creation) • Pack Inbound Delivery Items (single and mixed Handling Units creation, auto packing) • Goods Receipt (single item and bulk items receiving) **Note** The Inbound Delivery feature differs for the Inventory Clerk and Extended Warehouse Clerk personas, since Inventory Clerk only supports Goods Receipt for Inbound Delivery.	Extended Warehouse Clerk	Extended Warehouse Clerk: **YES**	2511	SAP S/4HANA 2022 FPS00	Inbound Delivery Process Configuration (Extended Warehouse Clerk) [page 445]	Working with Inbound Deliveries

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Mobile Configuration Variant Tool	-	With the Mobile Configuration Variant Tool, you can create Configuration Variants and assign them to mobile application users in your organization. A Configuration Variant is a configuration object created based on an existing mobile application configuration. It contains a collection of override configuration changes that can be applied to an existing mobile application configuration at runtime. By creating and assigning Configuration Variants to users, you can quickly apply specific configuration scenarios to different Business Units within your organization, **without upgrading your application** or **creating a new instance** of your base mobile application configuration.	Maintenance Technician (Standard) Maintenance Technician (Pro) Maintenance Technician (External) Field Service Technician (Standard) Field Service Technician (Pro) Inventory Clerk Safety Technician	-	2.0		Mobile Configuration Variant Tool Overview [page 77]	-

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
FSM Crowd Service Integration	FSM_CROWD_INTEGRATION	If you are using SAP Field Service Management Crowd Workforce for external technicians, you can use SAP Service and Asset Manager to download Service Orders assigned to these external technicians via the FSM Planning and Dispatching Board. **Note** This feature is specifically created for external workers within your organization, and supported by the **External** Maintenance and Field Service Technician personas. For more information, see: • Mobile User Essential Authorizations • Configuring FSM Crowd Service - Back End - Enabling the Feature [page 417] • Maintenance Technician Persona Overview (Standard, Professional, External) • Field Service Technician Persona Overview (Standard, Professional, External)	Maintenance Technician (External) Field Service Technician (External)	Maintenance Technician (External): **YES** Field Service Technician (External): **YES**	2505		FSM Crowd Service Configuration [page 411]	-

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
FSM Crew Integration	FSM_CREW_MANAGEMENT	With the FSM Crew integration, technicians can perform the following activities, depending on their assigned role (Crew *Lead* or *Member*): • Access their crew members' assigned Service Orders, Items, Operations from the SAP Service and Asset Manager Homescreen. • Access information about their crews, crew schedule and crew members. • In the SAP Service and Asset Manager application, Crew Leads can update the Service Orders' status by changing the mobile status to *Start*, *Travel*, *On-site* or *Complete*. **Note** • The FSM Crew integration is **only** supported in the SAP S/4HANA Service scenario [page 205]. • For the Customer Service (CS) scenario [page 177], use the Crew Management [page 31] feature.	Field Service Technician (Standard) Field Service Technician (Pro)	Field Service Technician (Standard): **NO** Field Service Technician (Pro): **NO**	2505		FSM Crew Configuration [page 408]	Working with FSM Crew (S4)

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
AI-Assisted Job Completion	CA_AI_JOB_COMPLETION	Technicians can complete their job (Work Order, Service Order, Operation or Suboperation) with voice input using natural language and AI, instead of manually entering data required for the completion. The following fields support filling using AI: • Time • Expense • Milage • Note • Defect information **Note** • For Notifications, only the creation of the Notification Item and all its dependencies (such as Cause, Part, Damage, etc.) is supported. • This feature is in scope for the Maintenance Technician (Standard) persona. However, no applicable use case currently exists because this persona supports Notifications only and does not support Work Orders. As a result, the AI job completion flow is never triggered.	Maintenance Technician (Standard) Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro)	Maintenance Technician (Standard): **NO** Maintenance Technician (Pro): **NO** Field Service Technician (Standard): **NO** Field Service Technician (Pro): **NO**	2505		AI-Assisted Job Completion - Configuration [page 242]	Using AI to Complete Your Job

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Work Approval	-	A Work Approval is used to control the work execution. Work Approvals ask for measures to ensure a safe environment for working on a technical system. In doing so, approvals are used to define certain rules or requirements that must be followed.	Maintenance Technician (Pro) Safety Technician	Maintenance Technician (Pro): **YES** Safety Technician: **YES**	2305		Work Approval Configuration [page 563]	Work Approval Detail Screen

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
FSM Smartforms	-	SAP Service and Asset Manager supports FSM Smartforms that allow planning board administrators to efficiently gather technician activity information in an organized way. Planning board administrators can assign Smartform instances to activities and require technicians to fill out the Smartform instance before completing the activity. Smartform instances can be associated with the following objects: • Equipments • Functional Locations • Service Orders • Service Order Items **Note** • The FSM Smartforms feature can be used by both Customer Service [page 177] and SAP S/4HANA [page 205] back end systems. • FSM Smartforms can be configured for Maintenance Technician as well, and used in plant maintenance scenarios. In this case, FSM Smartforms will be attached to PM work order operations instead of CS and S/4 work orders. For more information, see FSM Smartforms Configuration	Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro)	Maintenance Technician (Pro): **YES** Field Service Technician (Standard): **YES** Field Service Technician (Pro): **YES**	2210		FSM Smartforms Configuration [page 195] FSM Smartforms Configuration for Maintenance Technician [page 420]	Smartforms Overview

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
		for Maintenance Technician [page 420].						
FSM Smartforms Template	-	Technicians can not only work with pre-attached Smartforms, but also add new ones to existing operations. They can create Smartforms from Templates and attach to the objects listed in Smartforms Overview. **Note** The FSM Smartform Template feature is: • Applicable for both Customer Service [page 177] and SAP S/4HANA [page 205] back end systems. • Part of Field Service Technician Scheduling [page 178], no additional configuration steps are required. • Supported by the Maintenance Technician (Pro) persona, if it already has Field Service Management integration configured [page 420].	Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro)	Maintenance Technician (Pro): **YES** Field Service Technician (Standard): **YES** Field Service Technician (Pro): **YES**	2505		FSM Smartforms Configuration (Customer Service Back End) [page 195] Configuring Persona (SAP S/4HANA Back End) [page 211] FSM Smartforms Configuration for Maintenance Technician [page 420]	Adding Smartforms to Objects

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Configurable Guided Workflow	CA_GUIDED_FLOW	Configurable guided workflow (CGW) defines the lifecycle of an object processed in your mobile app. Customers define a workflow for their specific persona and business needs. The mobile app then displays the custom workflow as a progress tracker.	Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro)	Maintenance Technician (Pro): **NO** Field Service Technician (Standard): **NO** Field Service Technician (Pro): **NO**	2410		Guided Workflow Configuration [page 438]	Using Guided Workflows
Attachments	CA_ATTACHMENT	Attachment support on business objects (DMS/BDS/GOS) **Note** Attachments for Inventory Clerk persona is supported from 2405.	Maintenance Technician (Standard) Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro) Inventory Clerk Safety Technician	Maintenance Technician (Standard): **YES** Maintenance Technician (Pro): **YES** Field Service Technician (Standard): **YES** Field Service Technician (Pro): **YES** Inventory Clerk: **YES** Safety Technician: **YES**	2110		Attachments - Abstract Document Management [page 287]	Working with Attachments - Maintenance Technician User Guide Working with Attachments - Field Service Technician User Guide Attaching Files - Inventory Clerk User Guide

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Auto-Sync	CA_AUTO_SYNC	Back end administrators can configure the app to auto-sync. Auto-syncs occur automatically, with no input needed from the app user.	Maintenance Technician (Standard) Maintenance Technician (Pro) Maintenance Technician (External) Field Service Technician (Standard) Field Service Technician (Pro) Inventory Clerk Extended Warehouse Clerk	Maintenance Technician (Standard): **NO** Maintenance Technician (Pro): **NO** Maintenance Technician (External): **NO** Field Service Technician (Standard): **NO** Field Service Technician (Pro): **NO** Inventory Clerk: **YES** Extended Warehouse Clerk: **YES**	2210		Auto-Sync Configuration [page 303]	Automatic Syncing - Maintenance Technician User Guide Automatic Syncing - Field Service Technician User Guide

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Bill of Materials	CA_BILL_OF_MATERIAL	Bill of Material for technical objects	Maintenance Technician (Pro) Field Service Technician (Pro)	Maintenance Technician (Pro): **NO** Field Service Technician (Pro): **YES**	2310		See *SAP Note* 3334014 for more information about *Support Material BOM using equipment or functional location construction type*.	Hierarchy Control Overview - Maintenance Technician User Guide Bill of Materials - Maintenance Technician User Guide

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Business Partners	CA_BUSINESS_PARTNER	Business partner details. Service orders, functional locations, and equipment can be linked to a business partner. Business partners are parties in which your company has a business interest. A business partner can be a customer, a prospect, a supplier, a competitor, or even an employee of your own company.	Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro) Safety Technician Extended Warehouse Clerk	Maintenance Technician (Pro): **NO** Field Service Technician (Standard): **YES** Field Service Technician (Pro): **YES** Safety Technician: **YES** Extended Warehouse Clerk: **YES**	2.0		Configuring the Creation of Technical Objects from a Template [page 137] Distribution by Work Order Header Business Partner [page 126] Distribution by Notification Header Level Business Partner [page 132]	Working with Business Partners - Maintenance Technician User Guide Working with Business Partners - Field Service Technician User Guide
Catalog Profile	-	By configuring catalog profiles, the user will be able to view safety-related catalogs, as well as other ones defined according to their preference.	Safety Technician	Safety Technician: **NO**	2410		Catalog Profiles Configuration [page 310]	-

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Classifications	CA_CLASSIFICATION	Classification and characteristics for technical objects. When you are managing a large number of objects, you can group these objects according to particular and logical features. The hierarchical structure of classifications enables you to find specific objects starting from one top object, moving to multiple, lower level objects.	Maintenance Technician (Pro) Field Service Technician (Pro)	Maintenance Technician (Pro): **YES** Field Service Technician (Pro): **YES**	2.0		Configuring the Creation of Technical Objects from a Template [page 137]	Working with Classifications - Maintenance Technician User Guide Classifications - Field Service Technician User Guide
Core Data	CA_CORE_DATA	Core data including org structure, such as Plant, Work Center etc.	Maintenance Technician (Standard) Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro) Inventory Clerk Safety Technician	Maintenance Technician (Standard): **YES** Maintenance Technician (Pro): **YES** Field Service Technician (Standard): **YES** Field Service Technician (Pro): **YES** Inventory Clerk: **YES** Safety Technician: **YES**				

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Creating Technical Objects	CA_CREATE_TECH_OBJECT	Create equipment and functional location.	Maintenance Technician (Pro) Field Service Technician (Pro)	Maintenance Technician (Pro): **YES** Field Service Technician (Pro): **YES**	2205		Creating a Technical Object Template Configuring the Creation of Technical Objects from a Template [page 137]	Working with Technical Objects - Maintenance Technician User Guide Technical Objects Detail Screen - Field Service Technician User Guide

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Crew Management	CA_CREW_MANAGEMENT	Crew Management is an optional component that allows supervisors and team leaders to manage their crew and vehicles with significantly lower cost and greater flexibility. **Note** • The Crew Management component is **only** supported in the Customer Service (CS) scenario [page 177]. • For the SAP S/4HANA Service scenario [page 205], use theFSM Crew Integration [page 20]. • For the Field Service Technician Standard and Pro personas, standard Crew Management is supported **only from 2505** version.	Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro)	Maintenance Technician (Pro): **NO** Field Service Technician (Standard): **NO** Field Service Technician (Pro): **NO**	2.0		Enabling and Disabling Features Per User Through SAP Authorization [page 102]	Crew Management Overview

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Digital Signature	CA_DIGITAL_SIGNATURE	Digital signature for S/4. This feature performs a verification of work by digitally signing the work, using a user name and password.	Maintenance Technician (Pro)	Maintenance Technician (Pro): **NO**	2105		Digital Signature Overview [page 332]	Adding a Signature - Maintenance Technician User Guide Adding a Signature - Field Service Technician User Guide
Samsung Knox Capture integration	-	On Samsung devices, users can scan QR codes by the Knox Capture integration, which will allow them to: • Scan a single QR code to navigate directly to an object's detail page. • Scan multiple QR codes at once to save/issue multiple objects. • Trigger the scanning function directly by pressing the **Active** or **XCover** keys on supported Samsung devices. **Note** This feature is a third-party integration by Samsung. For more information and the list of supported devices, refer to the official Samsung Knox documentation .	Maintenance Technician (Standard) Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro)	Maintenance Technician (Standard): **NO** Maintenance Technician (Pro): **NO** Field Service Technician (Standard): **NO** Field Service Technician (Pro): **NO**	2410		Samsung Knox Capture Configuration [page 536]	Using Samsung Knox Capture

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide

SAP Dynamic Forms	CA_DYNAMIC_FORMS	SAP Service and Asset Manager supports SAP Dynamic Forms, an SAP Business Technology Platform application that allows you to design, deploy, and use basic and complex forms. Key functionalities include:
		• Support to create and edit form instances associated with the following business objects:
		  • Work Orders
		  • Notifications
		  • Equipments
		  • Functional locations
		  • Work Permits
		  • Isolation Certificates and Other Certificates
		  • S/4 service system:
		  • Service Orders
		  • Service Items
		• Ability to create, edit and delete forms locally. While being offline, users can:
		  • Open, complete and submit locally created forms.
		  • Modify and save locally created and updated forms.
		  • Delete an unsynced form.
		• Support for syncing forms on SAP BTP.
			Maintenance Technician (Standard)
			Maintenance Technician (Pro)
			Field Service Technician (Standard)
			Field Service Technician (Pro)
			Safety Technician
				Maintenance Technician (Standard): **NO**
				Maintenance Technician (Pro): **NO**
				Field Service Technician (Standard): **NO**
				Field Service Technician (Pro): **NO**
				Safety Technician: **NO**
					2310		SAP Dynamic Forms Configuration for SAP Service and Asset Manager [page 540]	Working with Dynamic Forms

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Editable Data Table (EDT)	-	Editable Data Table is an extension, letting users to enter multiple records quickly in a table format. These tables have different types of cells that can include types of plain text, a switch, a picker or a signature control.	Maintenance Technician (Standard) Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro) Extended Warehouse Clerk	-	2310		Editable Data Table (EDT)	Working with Editable Data Tables (Maintenance Technician User Guide) Working with Editable Data Tables (Field Service Technician User Guide)

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Geographic Information System (GIS)	CA_GEOSPATIAL_INFO_SERVICE	GIS support for ESRI ArcGIS and GEF.	Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro) Safety Technician	Maintenance Technician (Pro): **YES** Field Service Technician (Standard): **YES** Field Service Technician (Pro): **YES** Safety Technician: **YES**	2010		Geospatial Service Definitions [page 421]	Maps Overview and Settings Options (Maintenance Technician User Guide) Maps Overview and Settings Options (Field Service Technician User Guide) Maps Overview and Settings Options (Safety Technician User Guide)

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Creating and Updating Geospatial Data	CA_GIS_ADD_EDIT	You can create and update geospatial data on the map.	Maintenance Technician (Standard) Maintenance Technician (Pro)	Maintenance Technician (Standard): **YES** Maintenance Technician (Pro): **YES**	3.0			Maps Overview and Settings Options (Maintenance Technician User Guide) Maps Overview and Settings Options (Field Service Technician User Guide)
Location Tracking	CA_LOCATION_UPDATE	This feature allows to track the Technicians' live location, so the Planner can identify the Technicians' proximity and provide options for the Scheduler to assign them urgent tasks or re-assign tasks to nearby Technicians.	Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro)	Maintenance Technician (Pro): **NO** Field Service Technician (Standard): **NO** Field Service Technician (Pro): **NO**	2205		Location Tracking Configuration [page 452]	Profile Settings Overview

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Notification History	CA_NO_HISTORY		Maintenance Technician (Standard) Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro) Safety Technician	Maintenance Technician (Standard): **YES** Maintenance Technician (Pro): **YES** Field Service Technician (Standard): **NO** Field Service Technician (Pro): **NO** Safety Technician: **YES**				
Online Search	CA_ONLINE_SEARCH	Users can search online for *Functional Locations* and *Equipments*, allowing them to view, filter and optionally download more objects to their mobile device, in addition to the ones already downloaded. This way users have more visibility of ongoing tasks, not limited to the ones available only offline. **Note** Online search for *Work Orders* and *Notifications* is supported from version 2410. See Online Search support for Work Orders and Notifications [page 38].	Maintenance Technician (Standard) Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro)	Maintenance Technician (Standard): **YES** Maintenance Technician (Pro): **YES** Field Service Technician (Standard): **YES** Field Service Technician (Pro): **YES**	2405		Online Search Configuration [page 515]	Using Online Search (Maintenance Technician User Guide) Using Online Search (Field Service Technician User Guide)

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Online Search support for Work Orders and Notifications	CA_ONLINE_SEARCH	As of version 2410, SAP Service and Asset Manager supports online search for *Work Orders* and *Notifications*. **Note** • Users can only *download* and *assign* Work Orders and Notifications. • For the Field Service Technician persona, this feature is supported on the Customer Service Back End system [page 177].	Maintenance Technician (Pro) Field Service Technician (Pro)	Maintenance Technician (Pro): **NO** Field Service Technician (Pro): **NO**	2410		Refer to *SAP note* 3480308/E. Configuring Online Search - Work Orders and Notifications [page 517]	Using Online Search (Maintenance Technician User Guide) Using Online Search (Field Service Technician User Guide)
PDF Service Report Generation	CA_SERVICE_REPORT	You can generate service reports in PDF format. You can then attach the PDF reports to service orders or share them through email.	Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro)	Maintenance Technician (Pro): **NO** Field Service Technician (Standard): **YES** Field Service Technician (Pro): **YES**	2205		Service Report Template Configuration [page 201]	Completing a Service Order

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Signature Capture	CA_SIGNATURE_CAPTURE	Signature (physical) capture as an image.	Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro)	Maintenance Technician (Pro): **NO** Field Service Technician (Standard): **YES** Field Service Technician (Pro): **YES**	2010		Signature Control Configuration [page 549]	Adding a Signature (Maintenance Technician User Guide) Adding a Signature (Field Service Technician User Guide)
Editing Technical Objects	CA_EDIT_TECH_OBJECT	Support for editing existing Functional Location and Equipment.	Maintenance Technician (Pro) Field Service Technician (Pro)	Maintenance Technician (Pro): **NO** Field Service Technician (Pro): **NO**	2410		Support for Editing Existing Technical Objects [page 142]	Equipment Overview Functional Location Overview

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Technical Objects	CA_TECH_OBJECT	Equipment and Functional Location Master Data. **Note** This feature controls if Functional Location and Equipment sections are visible in the mobile application.	Maintenance Technician (Standard) Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro) Safety Technician	Maintenance Technician (Standard): **YES** Maintenance Technician (Pro): **YES** Field Service Technician (Standard): **YES** Field Service Technician (Pro): **YES** Safety Technician: **YES**			Technical Objects Configuration [page 135]	Technical Objects Detail Screen Working with Technical Objects Equipment Overview Functional Location Overview
Work Order History	CA_WO_HISTORY		Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro)	Maintenance Technician (Pro): **YES** Field Service Technician (Standard): **NO** Field Service Technician (Pro): **NO**				

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Expense Reporting	CS_EXPENSE_REPORT	Service Technicians can record expenses for reporting.	Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro)	Maintenance Technician (Pro): **NO** Field Service Technician (Standard): **YES** Field Service Technician (Pro): **YES**	2205		Expense and Mileage Configuration [page 197]	Working with Expenses and Mileage
Mileage Reporting	CS_MILEAGE_REPORT	Service Technicians can record mileage for reporting.	Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro)	Maintenance Technician (Pro): **NO** Field Service Technician (Standard): **YES** Field Service Technician (Pro): **YES**	2205		Expense and Mileage Configuration [page 197]	Working with Expenses and Mileage
Service Notifications	CS_NOTIFICATION	As part of the Customer Service component, you can view, create and edit Service Notifications.	Field Service Technician (Standard) Field Service Technician (Pro)	Field Service Technician (Standard): **YES** Field Service Technician (Pro): **YES**	3.0		Customer Service Notification Types Configuration [page 330]	SAP Service and Asset Manager Overview Screen

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Service Orders	CS_SERVICE_ORDER	As part of the Customer Service component, you can view, create and edit Service Orders.	Field Service Technician (Standard) Field Service Technician (Pro)	Field Service Technician (Standard): **YES** Field Service Technician (Pro): **YES**	3.0		Customer Service Order Types Configuration [page 331]	SAP Service and Asset Manager Overview Screen
EAM Checklist	EAM_CHECKLIST	Checklists are needed in many EAM processes, especially inspections and maintenance. The EAM checklist feature allows association between a checklist and a work order or operation. This core feature is applicable for SAP S/4HANA back-end system.	Maintenance Technician (Pro)	Maintenance Technician (Pro): **NO**	2110		EAM Checklist Overview [page 529]	Using Inspection Checklists

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Emergency Work for Phase Model	EAM_EMERGENCY_WORK	This feature supports emergency work in the reactive maintenance phase model. It allows you to skip phases and issue a work order or notification when a technician is authorized to create these items.	Maintenance Technician (Standard) Maintenance Technician (Pro)	Maintenance Technician (Standard): **NO** Maintenance Technician (Pro): **NO**	2405		Emergency or Minor Work [page 378] (Phase Model Configuration) Emergency or Minor Work [page 400] (Phase Model + Non-Phase Model Configuration) SAP note 3489758 - *Enable S/4HANA EAM Emergency Work for Phase Model*	Emergency and Minor Work Notifications

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Event Prioritization for Notifications	EAM_EVENT_PRIORITY_MATRIX	Event priority matrix for non-phase model.	Maintenance Technician (Standard) Maintenance Technician (Pro)	Maintenance Technician (Standard): **NO** Maintenance Technician (Pro): **NO**	2210			
Minor Work for Phase Model	EAM_MINOR_WORK	This feature helps to skip phases and issue a work order or notification when a technician is authorized to create one.	Maintenance Technician (Standard) Maintenance Technician (Pro)	Maintenance Technician (Standard): **NO** Maintenance Technician (Pro): **NO**	2305			
Phase Control Codes	EAM_PHASE_CONTROL	Support phase contol codes for phase model orders and operations.	Maintenance Technician (Standard) Maintenance Technician (Pro)	Maintenance Technician (Standard): **NO** Maintenance Technician (Pro): **NO**	2305			-
Phase Model		Phase model process support. A phase-based maintenance process supports you in the maintenance of technical objects.	Maintenance Technician (Standard) Maintenance Technician (Pro)	Maintenance Technician (Standard): **NO** Maintenance Technician (Pro): **NO**	2110			-

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Product Model Viewer Integration	EPD_VISUALIZATION	Integrate with product model viewer for 3D AR visualization of assets.	Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro)	Maintenance Technician (Pro): **NO** Field Service Technician (Standard): **NO** Field Service Technician (Pro): **NO**	2305		EPD Visualization Configuration [page 403]	-
Field Operations Worker	FOW_ROUTE	Field Operations Worker capabilities, supporting technicians who perform asset inspections and checks with focus on measurement points and on smaller services and repairs. Use the Field Operations Worker (FOW) component to see the routes that you are assigned to.	Maintenance Technician (Pro)	Maintenance Technician (Pro): **NO**	2.0		Field Operations Worker Configuration [page 405]	Field Operations Worker Add-On Component

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
FSM Scheduler Integration	FSM_SCHED_INTEGRATION	Field Service Management planning board administrators can use geolocation information from the mobile app to enable scheduling and dispatching based on the location of the technician.	Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro)	Maintenance Technician (Pro): **NO** Field Service Technician (Standard): **NO** Field Service Technician (Pro): **NO**	2205		Field Service Management Scheduling - SAP Service and Asset Manager Integration [page 178] (FSM configuration on a customer service backend) Configuring Persona [page 211] (FSM configuration on an S/4 Field Service Management backend)	-

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
HR Timesheet	HR_TIME-SHEET	CATs time reporting functionalities. **Note** • If you are using CATS, the SAP HR module must be installed. • Maintenance Technician (Standard): Time can only be recorded against a Cost Center, WBS Element, or Network Activity. Work Orders are not supported. • Maintenance Technician (Professional): No such limitation; CATs timesheet entries can be made against Work Orders, Cost Centers, WBS Elements, and Network Activities.	Maintenance Technician (Standard) Maintenance Technician (Pro)	Maintenance Technician (Standard): **NO** Maintenance Technician (Pro): **NO**	1.0		CATS and PM Confirmation Time Entries Configuration [page 314]	Time Sheet Overview
ASPM Checklist	IAM_CHECK-LIST	Asset Strategy and Performance Management (ASPM) checklists are a type of assessment used for equipment. If an equipment has a mandatory checklist associated with it, when you click *End Work Order*, you are automatically taken to the *Checklist* screen to complete the checklist before you can fully complete your work order. A checklist can be composed of multiple choice questions or questions where you can enter free-form text.	Maintenance Technician (Pro)	Maintenance Technician (Pro): **NO**	4.0		Configuring Checklist Parameters [page 250]	Checklists
PdMS Indicators	IAM_INDICA-TORS	Use Predictive Maintenance and Service (PdMS) equipment indicators that allow you to identify the health status of your equipment.	Maintenance Technician (Pro)	Maintenance Technician (Pro): **NO**	3.0		-	PdMS Indicators

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Inventory Management Core Data	IM_CORE_DATA	-	Inventory Clerk	Inventory Clerk: **YES**	2110		Inventory Clerk Parameter Configuration [page 237]	Inventory Clerk Persona Overview
Meter Management	ISU_METER_MANAGEMENT	Meter Management capabilities allowing technicians to retrieve work orders assigned to them from the SAP system, and perform meter installation, meter removal or replacement, aperiodic readings, meter repair and plant maintenance. **Note** For the Field Service Technician persona, this feature is supported from version 2405.	Maintenance Technician (Pro) Field Service Technician (Pro)	Maintenance Technician (Pro): **YES** Field Service Technician (Pro): **YES**	2.0		Meter Management Configuration [page 463]	Meters Overview (Maintenance Technician user guide) Meters Overview (Field Service Technician user guide)
Goods Issue	MM_GOODS_ISSUE	Goods issue for inventory management. For more information, see Goods Issue.	Inventory Clerk	Inventory Clerk: **YES**	2110		-	Working with Goods Issues
Goods Receipt	MM_GOODS_RECEIPT	Goods receipt for inventory management. For more information, see Goods Receipt.	Inventory Clerk	Inventory Clerk: **YES**	2110		-	Working with Goods Receipts

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Material Master Data	MM_MATERIAL_DATA	You can enable the material data. The material master contains information on the materials that a company procures or produces, stores, and sells.	Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro) Inventory Clerk Extended Warehouse Clerk	Maintenance Technician (Pro): **YES** Field Service Technician (Standard): **YES** Field Service Technician (Pro): **YES** Inventory Clerk: **YES** Extended Warehouse Management: **YES**				
Physical Inventory	MM_PHYSICAL_INVENTORY	Physical Inventory capabilities for inventory management. For more information, see Physical Inventory.	Inventory Clerk	Inventory Clerk: **YES**	2205		Inventory Clerk Parameter Configuration [page 237]	Working with Physical Inventory
Production Order	MM_PRODUCTION_ORDER	Product orders for inventory management. For more information, see Inventory Clerk Persona Overview.	Inventory Clerk	Inventory Clerk: **YES**	2210			Inventory Clerk Persona Overview

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Purchase Requisition	MM_PURCHASE_REQUISITION	Purchase Requisition for inventory management. For more information, see Purchase Requisitions.	Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro) Inventory Clerk	Maintenance Technician (Pro): **YES** Field Service Technician (Standard): **YES** Field Service Technician (Pro): **YES** Inventory Clerk: **YES**	2305			Working with Purchase Requisition
Stock Lookup	MM_STOCK_LOOKUP	Stock Lookup by plant and storage location. For more information, see Stock Lookup.	Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro) Field Service Technician (External) Inventory Clerk	Maintenance Technician (Pro): **YES** Field Service Technician (Standard): **YES** Field Service Technician (Pro): **YES** Field Service Technician (External): **YES** Inventory Clerk: **YES**	2205		Vehicle Stock Look Up Configuration [page 560]	Working with Stock Lookup
Stock Transfer	MM_STOCK_TRANSFER	Stock Transfer for inventory management. For more information, see Stock Transfers.	Inventory Clerk	Inventory Clerk: **YES**	2110			

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Goods Issue for Planned Materials on Work Order	MM_TECHNICIAN_GOODS_ISSUE	For more information, see: • Inventory Clerk Persona Overview • Goods Issue	Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro)	Maintenance Technician (Pro): **YES** Field Service Technician (Standard): **YES** Field Service Technician (Pro): **YES**				Working with Goods Issues

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Vehicle Stock	MM_VEHICLE_STOCK	The Vehicle Stock component in SAP Service and Asset Manager offers inventory functionality to track stock items stored in vehicles, like work trucks or vans. Vehicle stock capabilities include: • Helping operators to manage stock items stored in vehicles for daily work. • Storage location assigned to the technician is displayed on the app. • Ability to transfer stock to and from the set storage location. • Look up stock for the set storage location. • Perform a physical inventory or cycle count for the set storage location. • Replenish stock through purchase requisitions. • Tracking tools and other items kept in the vehicles. **Note** From SAP Service and Asset Manager **2505 version**, the Vehicle Stock feture is supported by the Field Service Technician persona on the SAP S/4HANA back end system.	Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro) Field Service Technician (External)	Maintenance Technician (Pro): **NO** Field Service Technician (Standard): **YES** Field Service Technician (Pro): **YES** Field Service Technician (External): **YES**	2205		Vehicle Stock Look Up Configuration [page 560]	Working with Stock Lookup Working with Stock Transfers and Transfer Posting Adding Vehicles

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Equipment Assembly Information for Work Order	PM_ASSEMBLY	Plant Maintenance assemblies link spare parts to an equipment in a structured manner. These assemblies are not plant-specific and are not designed to be a complete material. Assemblies contain a bill of material (BOM).	Maintenance Technician (Pro)	Maintenance Technician (Pro): **YES**	2110		-	Work Order Detail Screen
Clock In / Clock Out	PM_CLOCK_IN_CLOCK_OUT	Clock In / Clock Out (CICO) capabalities enable multiple users to work on the same work order or operation. CICO also allows multiple work orders or operations that all belong to different users on a mobile device to exist in the Started state.	Maintenance Technician (Pro)	Maintenance Technician (Pro): **NO**	1911		Clock In Clock Out Configuration [page 318]	Working with Clock In Clock Out

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
PM Confirmations for Time Recording	PM_CONFIRMATION	PM confirmations on operations or work orders capture the time spent on the orders..	Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro)	Maintenance Technician (Pro): **YES** Field Service Technician (Standard): **YES** Field Service Technician (Pro): **YES**	2.0		CATS and PM Confirmation Time Entries Configuration [page 314] Configuring Confirmation Posting Dates - Overview [page 684]	Completing a PM Confirmation on a Maintenance Order (Maintenance Technician user guide) Completing a PM Confirmation on a Maintenance Order (Field Service Technician user guide)

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Equipment Install and Dismantle	PM_INSTALL_DISMANTLE	You can install or dismantle equipment under existing equipment. You can also install or dismantle equipment under existing functional locations.	Maintenance Technician (Pro)	Maintenance Technician (Pro): **YES**	4.0		Enabling and Disabling Features Per User Through SAP Authorization [page 102]	Equipment Overview Installing Equipment Dismantling Equipment

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Linear Asset Management	PM_LINEAR_ASSET_MANAGEMENT	Linear Asset Management (LAM) capabilities, enabling you to download the linear assets for your area of responsibility. Linear assets are technical systems with a linear infrastructure with conditions and properties that can vary from section to section (dynamic segmentation). You can see linear asset data associated with various objects such as work orders, operations, technical objects, and notifications. LAM enables you to create linear assets as technical objects (such as functional locations and equipment) and store linear data. You can carry out maintenance tasks for these technical objects, which result in notifications, work orders, and measurement documents. These tasks allow you to: • Monitor the condition of your linear assets. • Identify where there is any damage or defect using the start point, end point, and offset. • Manage all types of maintenance tasks such as planned, unplanned, and preventative.	Maintenance Technician (Pro)	Maintenance Technician (Pro): **NO**	2005		Linear Asset Management Configuration [page 449]	Linear Asset Management (LAM) Overview

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Measurement Readings	PM_MEASUREMENT	You can take measurement point readings at the work order header level across all operations for all equipment and functional locations.	Maintenance Technician (Standard) Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro)	Maintenance Technician (Standard): **YES** Maintenance Technician (Pro): **YES** Field Service Technician Technician (Standard): **NO** Field Service Technician Technician (Pro): **YES**	2005		Enabling and Disabling Features Per User Through SAP Authorization [page 102]	Measuring Points and Readings Overview (Maintenance Technician user guide) Measuring Points and Readings Overview (Field Service Technician user guide - Customer Service backend) Measuring Points and Readings Overview (Field

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
								Service Technician user guide - S/4 Field Service Management back-end)
PM Notifications	PM_NOTIFICATION	**Note** For the Safety Technician persona, notifications are supported from version 2305.	Maintenance Technician (Standard) Maintenance Technician (Pro) Safety Technician	Maintenance Technician (Standard): **YES** Maintenance Technician (Pro): **YES** Safety Technician: **YES**	1.0		-	Notifications Overview (Maintenance Technician user guide) Adding Notifications to Objects (Safety Technician user guide)

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Object Lists on Work Orders	PM_OBJECT_LIST	Object Lists support for work orders. A technical object serves a specific purpose or function, such as a piece of equipment. A technical object list is an object worklist that is configured to meet the specific requirements of the customer. An object worklist displays the most important pieces of information about the equipment and functional locations. An object worklist is associated with a work order.	Maintenance Technician (Pro)	Maintenance Technician (Pro): **YES**	2005		-	Using an Object List
Production, Resources and Tools	PM_PRT	Unlike fixed assets, production, resources, and tools (PRTs) are moveable (not stationary) operating resources that are required to perform an operation or suboperation. PRTs can be used repeatedly.	Maintenance Technician (Pro)	Maintenance Technician (Pro): **YES**	2.0		-	Managing PRTs

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Supervisor Mode	PM_SUPERVISOR_MODE	The supervisor role allows a team supervisor to: • Assign or reassign work orders using the mobile device. • Track the current work orders assigned to team members in order to monitor those work orders. • Use the back end to manage the members of the team. • Audit completed work orders to maintain a specific level of quality. • Approve workflows and reject work. **Note** In case of phase model is enabled, supervisor mode support is availabe from version 2305.	Maintenance Technician (Pro)	Maintenance Technician (Pro): **NO**	2105		Supervisor Mode Configuration [page 550]	-
PM Work Orders	PM_WORK_ORDER	PM Work Orders	Maintenance Technician (Pro)	Maintenance Technician (Pro): **YES**	-			
Calibration Orders and Inspection Lots	QM_CALIBRATION	The Quality Management (QM) component supports tasks associated with quality planning, quality inspection, and quality control. In addition, it controls the creation of quality certificates and manages problems with the help of quality notifications.	Maintenance Technician (Pro)	Maintenance Technician (Pro): **NO**	2010		Quality Management Configuration [page 523]	Working with Quality Management

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
S/4 Service Orders	S4_SERVICE_INTEGRATION	SAP S/4HANA Service integration for the Field Servcie Technician persona.	Field Service Technician (Standard)	Field Service Technician (Standard): **NO**	2305		Field Service Technician Configuration for SAP S/4HANA Service Order Scenario [page 205]	Service Order Detail Screen
General configuration of safety-related features	WCM_COMMON	For the Safety Technician persona in general as well as for a number of safety-related features to work, you must enable the *WCM_COMMON* feature. **Note** For the Maintenance Technician (Pro) persona, this feature is only available from 2410 version.	Maintenance Technician (Pro) Safety Technician	Maintenance Technician (Pro): **NO** Safety Technician: **YES**	2305		General Feature Configuration - Safety Technician Persona [page 218]	Safety Technician User Guide Working with Safety Technician Objects (Maintenance Technician User Guide)

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Isolation Certificate	WCM_SAFETY_CERTIFICATE	Isolation Certificates (also referred to as Safety Cerificates) are used to describe lockout and tagout procedures when controlling the physical blocking and tagging of affected technical objects. It contains the technical asset objects that are to be switched or controlled in the application and provides a detailed description of how the system is to be isolated. **Note** • For the Maintenance Technician (Pro) persona, this feature is only available from 2410 version. • The configuration of Assignment Management [page 261] affects the configurations of **WCM Work Order**, **Isolation Certificate** and **Work Permit**.	Maintenance Technician (Pro) Safety Technician	Maintenance Technician (Pro): **NO** Safety Technician: **YES**	2305		Isolation Certificate Configuration [page 446]	Isolation Certificate Detail Screen

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Other Certificate	WCM_SAFETY_CERTIFICATE	Other Certificate is used to describe lockout and tagout procedures when controlling the physical blocking and tagging of affected technical objects. Compared to Isolation Certificates, however, there is no action that can be done with Other Certificates, they are only displayed to check the status of the technical asset objects, and they can be attached to the work permits. **Note** • The configuration process for Other Cerificates is the same as for Isolation Certificates [page 446]. • For the Maintenance Technician (Pro) persona, this feature is only available from 2410 version.	Maintenance Technician (Pro) Safety Technician	Maintenance Technician (Pro): **NO** Safety Technician: **YES**	2305		Isolation Certificate Configuration [page 446]	Certificate Detail Screen

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Assignment Management of Safety-Related Features	-	Safety Technicians can see a filtered list of items on their mobile devices that are assigned to them. This applies to the following list screens: • Operational Items • Isolation Certificates • Other Cerificates • Work Permits • Work Orders (linked to the assigned objects) • Work Approvals (linked to the assigned objects) **Note** For the Maintenance Technician (Pro) persona, this feature is only available from 2410 version.	Maintenance Technician (Pro) Safety Technician	Maintenance Technician (Pro): **NO** Safety Technician: **YES**	2310		Assignment Management of Safety-Related Features [page 261]	Assignment Management - Filtering Your Assigned Objects

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Tagging and Untagging	-	For the Safety Technician persona, a key task is to orderly tag and subsequently untag technical objects, so that work and tests on Technical Objects can be performed safely by preventing accidental or unauthorized access to dangerous energy sources. Using SAP Service and Asset Manager, you can provide digital control of all the tagging and untagging procedures. **Note** • As of 2505 release, limited support is available for the temporary untagging phase. For more information, see Supported Usage Types - Safety Technician Persona [page 226]. • For more information about tagging and untagging, refer to Lockout/Tagout in *Work Clearance Management (PM-WCM)* documentation.	Maintenance Technician (Pro) Safety Technician	Maintenance Technician (Pro): **NO** Safety Technician: **YES**	2305		Operational Item Configuration [page 521]	Tagging and Untagging

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Operational Item	-	To ensure that safety measures for work are performed at the the operation level, Safety Technicians must perform isolation procedures for an Operational Item. The Operational Item is used to describe the operational processing of **lockout** and **tagout** procedures. This process consists of orderly tagging and subsequent untagging of technical objects, so that work and tests on technical objects can be performed safely. **Note** • For the Maintenance Technician (Pro) persona, this feature is only available from 2410 version. • For more information about recording lockout and tagout activity, refer to Lockout/Tagout section in *SAP ERP - Work Clearance Management (PM-WCM)* documentation.	Maintenance Technician (Pro) Safety Technician	Maintenance Technician (Pro): **NO** Safety Technician: **YES**	2305		Operational Item Configuration [page 521]	Operational Item Detail Screen Add New Operational Item on the Go to Isolation Cerificate

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
WCM Work Order	WCM_ORDER	Work Clearance order **Note** The configuration of Assignment Management [page 261] affects the configurations of **WCM Work Order**, **Isolation Cerificate** and **Work Permit**.	Maintenance Technician (Pro) Safety Technician	Maintenance Technician (Pro): **NO** Safety Technician: **YES**	2305		Work Order as a Dependency - Safety Technician Persona [page 225]	Work Order Detail Screen

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Work Permit	WCM_WORK_PERMIT	A (Work Clearance) Work Permit is approved by one or more Supervisors and is visible for the Safety Technician persona. After the Safety Technician persona has done his safety work by implementing and maintaining lockout and tagout procedures for energy source isolation, the Work Permit can be released, and the Maintenance Technician persona can do the work assigned to him. A (Work Clearance) Work Permit is approved by one or more Supervisors and is visible for the Safety Technician persona. After the Safety Technician persona has done his safety work by implementing and maintaining lockout and tagout procedures for energy source isolation, the Work Permit can be released, and the Maintenance Technician persona can do the work assigned to him. **Note** The configuration of Assignment Management [page 261] affects the configurations of **WCM Work Order**, **Safety Cerificate** and **Work Permit**. **Note** • For the Maintenance Technician (Pro) persona, this feature is only available from 2410 version.	Maintenance Technician (Pro) Safety Technician	Maintenance Technician (Pro): **NO** Safety Technician: **YES**	2305		Work Permit Configuration [page 565]	Work Permit Detail Screen

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
		• The configuration of Assignment Management [page 261] affects the configurations of **WCM Work Order**, **Isolation Certificate** and **Work Permit**.						
Work Permit Approval	-	Safety Technicians can issue approvals on the details screen of a selected Work Permit.	Maintenance Technician (Pro) Safety Technician	Maintenance Technician (Pro): **NO** Safety Technician: **NO**	2310		Work Permit Approvals Configuration [page 569]	Issuing Work Permit Approvals
Low Code No Code	-	The object detail screens in SAP Service and Asset Manager can be modified to include properties of the oData entity set that are not part of the detail screen out of the box.			2310			-

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Delta Sync Optimization - Downloading Only Modified Entities	-	As of SAP Service and Asset Manager version 2310, the application is activated for optimized delta synchronization by default. In this case, when the user initiates delta synchronization, an attempt is made to upload transactions, if any. An interactive call then identifies entities that need to be updated or have changed since the last synchronization. Only for these changed entities will delta synchronization be started, thus optimizing the duration of delta synchronization.	Maintenance Technician (Standard) Maintenance Technician (Pro) Maintenance Technician (External) Field Service Technician (Standard) Field Service Technician (Pro) Inventory Clerk Safety Technician Extended Warehouse Clerk Field Logistics	Maintenance Technician (Standard): **YES** Maintenance Technician (Pro): **YES** Maintenance Technician (External): **YES** Field Service Technician (Standard): **YES** Field Service Technician (Pro): **YES** Inventory Clerk: **YES** Safety Technician: **YES** Extended Warehouse Clerk: **YES** Field Logistics: **YES**	2310		Downloading Only Modified Entities [page 582]	Syncing to the SAP Back End

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Delta Sync Optimization - Lead Entity Based Flow	-	Lead entity based flow is a feature available for oMDOs and is enabled with exchange. Lead entity based flow performs an optimized delta key calculation, which reduces the delta sync duration.	Maintenance Technician (Standard) Maintenance Technician (Pro) Maintenance Technician (External) Field Service Technician (Standard) Field Service Technician (Pro) Field Service Technician (External) Inventory Clerk Safety Technician Extended Warehouse Clerk Field Logistics	Maintenance Technician (Standard): **NO** Maintenance Technician (Pro): **NO** Maintenance Technician (External): **NO** Field Service Technician (Standard): **NO** Field Service Technician (Pro): **NO** Field Service Technician (External): **NO** Inventory Clerk: **NO** Safety Technician: **NO** Extended Warehouse Clerk: **NO** Field Logistics: **NO**	2505		Lead Entity Based Flow Overview [page 588]	Syncing to the SAP Back End

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Shadow Table	-	Any custom configuration changes are stored in separate sets of tables, unlike standard configuration tables that use the MAIF framework. A custom application created using the configuration panel is marked as supporting shadow tables. **Note** This feature is part of the MAIF documentation. For more information about general MAIF configuration procedures, refer to the *MAIF Configuration Guide*.			2305		Shadow Table [page 681]	-
Removal of Dependent Objects Based on Lead Objects	-	SAP Service and Asset Manager downloads data to mobile by using distributon mode. One of the supported distributon modes is Dependency mode. When Dependency mode is activated for oMDO, objects get qualified by the lead object. With this new feature introduced, when the last lead object is removed from device, the associated dependent object will also be removed.			2310		Removal of Dependent Objects Based on Lead Objects [page 113]	-

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Support for LITE Version of Technical Objects	-	From SAP Service and Asset Manager 2310, LITE version of technical objects is activated as standard configuration (i.e., LITE version of oMDO exists as standard for Equipment and Functional Location objects). As a result, technical objects associated with work orders or notifications are downloaded with full-blown data and others have only minimum data (LITE version). When new jobs qualifiy with LITE version of technical object, the application automatically downloads the full-blown data for the respective technical object along with the workorder or notification download.			2310		Support for LITE Version of Technical Objects [page 143]	-
Namespace Check	-	SAP provides namespace check for a number of configuration areas. With SAP Service and Asset Manager 2210 or earlier versions, you can bypass namespace checks. Namespace bypass is not applicable to the Persona and Feature configuration, whereby a custom or partner namespace remains applicable in those areas and cannot be bypassed. **Note** As of SAP Service and Asset Manager 2305, this feature is no longer supported.					Namespace Check Configuration [page 467]	-

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Auto-Resize Images with a Configured Maximum Size	-	You can configure the maximum image size, which is allowed for uploading images from the application. Uploaded images exceeding the size limit will be resized automatically.			2310		Auto-Resize Images with a Configured Maximum Size [page 302]	-
Mobile Transaction History	-	With thisfeature, SAP introduces the possibility for users to record all successful *CREATE* and *UPDATE* transactions from the mobile device in to the */SYCLO/MBL02* table. This provides insight into which objects are either created or changed via the mobile application, by whom, and when the changes are made. **Note** This feature is part of the MAIF documentation. For more information about general MAIF configuration procedures, refer to the *MAIF Configuration Guide*.			2310		Mobile Transaction History [page 618]	-
Local Object Mobile Status	-	With this feature you can enable or disable the mobile client user to take a local object through its entire lifecycle even if the client is offline.			1911		Local Object Mobile Status Configuration [page 451]	-

Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Multi-User Support	-	Multiple users can use the client on the same device, capabilities such as adding a new user, switching across users, and searching from a list users are supported.			2110		Enabling Multi-User Support	Multi-User Overview (Maintenance Technician User Guide) Multi-User Overview (Field Service Technician User Guide)
Deep Link Support	-	Support of standard deep link URLs in SAP Service and Asset Manager to perform create, update, view operations.			2305		Customizing Deep Linking	-

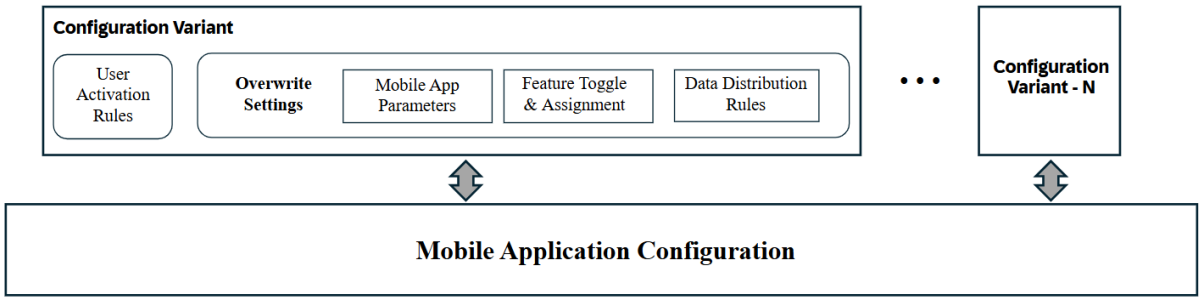
Feature name	Feature ID	Feature description	Personas supported	Enabled by default	Available from version	Minimum required SAP S/4HANA back end	Link to Configuration Guide	Link to User Guide
Zebra Scanner Integration	-	On Zebra devices, users can scan barcodes by using the Zebra Scanner integration, which will allow them to: • Scan a single barcode to navigate directly to an object's detail page. • Trigger the scanning function directly on Overview or List pages, by pressing the barcode scanner button on the device. **Note** This feature is a third-party integration by Zebra. For more information and the list of supported devices, refer to the official Zebra documentation and Zebra Products and Software Support .	Maintenance Technician (Standard) Maintenance Technician (Pro) Field Service Technician (Standard) Field Service Technician (Pro)	Maintenance Technician (Standard): **NO** Maintenance Technician (Pro): **NO** Field Service Technician (Standard): **NO** Field Service Technician (Pro): **NO**	2410		Zebra Scanner Configuration [page 578]	Using Zebra Scanner

2 General Configurations

2.1 Mobile Configuration Variant Tool Overview

With the Mobile Configuration Variant Tool, you can create Configuration Variants and assign them to mobile application users in your organization. A Configuration Variant is a configuration object created based on an existing mobile application configuration. It contains a collection of override configuration changes that can be applied to an existing mobile application configuration at runtime. By creating and assigning Configuration Variants to users, you can quickly apply specific configuration scenarios to different Business Units within your organization, **without upgrading your application** or **creating a new instance** of your base mobile application configuration.

- For a base mobile application, you can define **multiple** Configuration Variants.
- For a Configuration Variant, you can assign **multiple** users, by setting up User Activation Rules [page 81].
- A user can be assigned to **zero or one** Variant.
- Override configuration changes can be applied to:
  - Feature Toggles & Assignments [page 82]
  - Mobile Application Parameters [page 84]
  - Data Distribution Rules (oMDO Filters) [page 85]

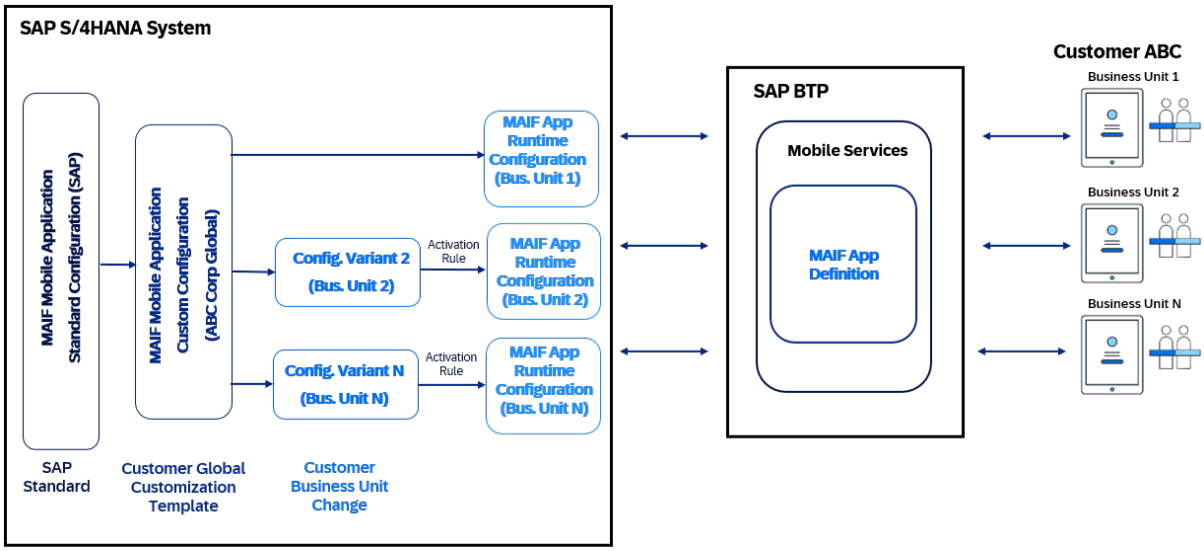


Configuration Variants in SAP Service and Asset Manager

The following image displays a high-level overview of how Configuration Variants work within the SAP Service and Asset Manager architecture.

> **Note**
>
> SAP Service and Asset Manager is a MAIF application.

MAIF Mobile Application with Configuration Variant



In this example **Customer ABC** has **three Business Units**:

1. The SAP Standard Configuration holds the BC set installed with your system. The BC set is used by all configurations and users for that system.
2. **Business Unit 1** uses the corporation's global custom configuration as is, **without** any Configuration Variant. Changes at this level are kept in a shadow table (see the Shadow Table [page 681] topic).
3. In the case of **Business Unit 2** and **Business Unit N**, **Configuration Variant 1** and **Configuration Variant N** are used to alter the corporation's global custom configuration according to their specific needs.
4. All Business Units remain on the same mobile application. If you want to upgrade the application later, you can do it simultaneously for all Business Units while retaining all Configuration Variants.

Supported Personas

This feature is applicable for the following personas:

Maintenance Technician (Standard)
Maintenance Technician (Pro)
Maintenance Technician (External)
Field Service Technician (Standard)
Field Service Technician (Pro)
Inventory Clerk
Safety Technician

Limitations

Currently, the Variant Tool has the following limitations:

- Configuration variant assignment to user is re-determined automatically every **720 hours** (30 days).
- You can change user variant assignment at any time by **either** of the following:
  - Manually assign the variant in *User Management* (see Administration - User Management in *MAIF Administrator Guide*).
  - In *SAP GUI*, run the program */MFND/CORE_USR_VARI_UPD_PROG*
- Currently the mobile parameter rule handler */MFND/CL_CORE_OM_DOF_LOOKUP_RU* does not support configuration variant. Assignment type changes in variant oMDO is not reflected in the output of */MFND/CL_CORE_OM_DOF_LOOKUP_RU*.
- Configuration variant is not yet available in the current support package for SAP Mobile Add-On for ERP and Mobile Add-On for SAP S/4HANA. Customers on SAP S/4HANA **1909** through **2023** should implement the latest TCI note in order to have access to the configuration variant support.
- There is no variant-specific OData model generation support due to potential performance issues.

Configuration

To access the Variant Tool, in *SAP GUI* enter the transaction code */MFND/CFG_VARIANT*. Then perform the following steps to create and configure a new Variant:

1. Create a new Variant on the Search Screen. [page 79]
2. Configure the Variant's general settings and User Activation Rules. [page 80]
3. Configure Feature Toggles and Assignments. [page 82]
4. Configure Mobile Application Parameters [page 84]
5. Configure oMDO Filter settings. [page 85]

Once you created and configured the Variant(s), proceed with the following steps in the Admin Portal:

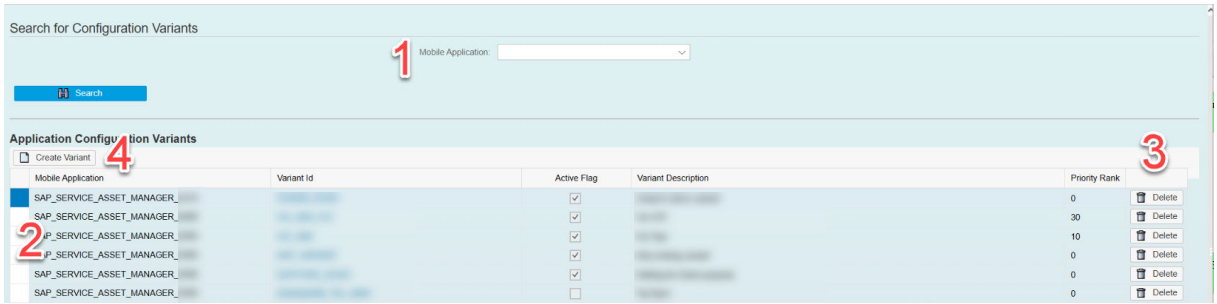
1. Assigning a User to a Variant Configuration

2.1.1 Variant Tool - Search Screen

Context

For detailed information about the Variant Tool, see Mobile Configuration Variant Tool Overview [page 77].

On the Variant Tool *Search Screen*, you can search and manage your existing Variants, as well as create new ones as follows:



Procedure

1. Filter and search your existing Variants by base *Mobile Application*.
2. You can access the Variants listed and see information about:
   - Base *Mobile Application*
   - *Variant Id*
   - If the *Active Flag* is checked

     > **Note**
     >
     > A Variant will **only** be used if it is set to *Active*.

   - *Priority Rank*
3. *Delete* any existing Variants.
4. Click *Create Variant* and fill in the following fields:
   1. Select a base *Mobile Application* with the correct version for the Variant.
   2. Enter a *Config Variant Id*.
   3. Enter a *Variant Description*.
   4. Click *Next*.

Next Steps

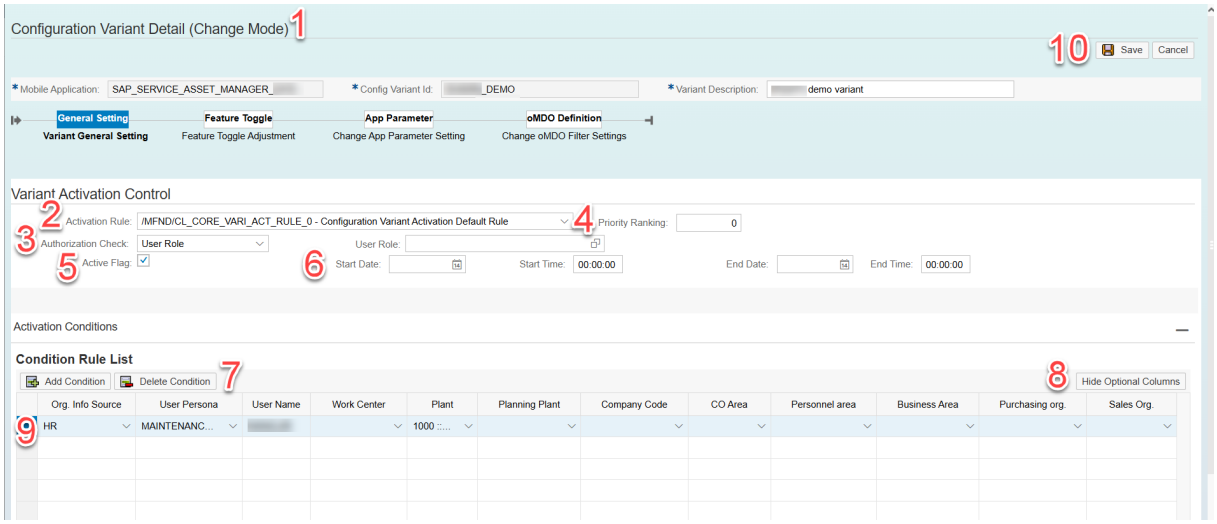
Continue with Configuring Variant General Settings [page 80].

2.1.2 Configuring Variant General Settings

Context

For detailed information about the Variant Tool, see Mobile Configuration Variant Tool Overview [page 77].

Under *General Settings*, you can configure the basic criteria to activate or deactivate the Variant, as well as define condition rules for users based on which they will be assigned to the Variant.



Procedure

1. Enter *Change mode*.
2. *Activation Rule*: You can use this field to determine, which Variant is relevant for user(s) at runtime. By default, there is one *Activation Rule* in the system you can use.
3. *Authorization Check*: As an additional check to the activation condition rules for users [page 81], you can set specific *User Roles* or *Authorization Profiles*; to make sure that users who meet the condition rules, but do not meet the required authorization, will be ignored for the Variant.
4. *Priority Ranking*: If a user meets the requirements for both activation condition rules [page 81] and Authorization Check [page 81] for **multiple** Variants, you can set a higher Priority Ranking number for the Variant you want to use.

   > ### Note
   >
   > By default, from the list of relevant Variants for a user, **alphabetically the first Variant** will be used.

5. *Active Flag*: Set to *Active* to enable the Variant.
6. *Start Date/Time* and *End Date/Time*: If set, the Variant will be enabled **only** within the specified time range.

   > ### Note
   >
   > If no time range is set, the Variant will be enabled immediately, without a time limit.

Condition Rule List

> ### Note
>
> You can create condition rules to define which user groups should be assigned to the Variant.

7. *Add* a new condition or *Delete* existing ones.
8. You can show/hide additional columns with conditions.
9. Define the following conditions according to your preference:

- *Org. Info Source*
- *User Persona*
- *User Name*
- *Work Center*
- *Plant*
- *Planning Plant*
- *Company Code*
- *Controlling Area*
- *Personnel Area*
- *Business Area*
- *Purchasing Org.*
- *Sales Org.*

> **Note**
>
> - If you create **multiple** condition rules, users who meet **at least one** of them will be assigned to the Variant (users do not need to meet all condition rules at once).
> - When creating a condition rule, all columns are optional to use.

10. *Save* your changes.

Next Steps

Continue with Configuring Feature Toggles [page 82].

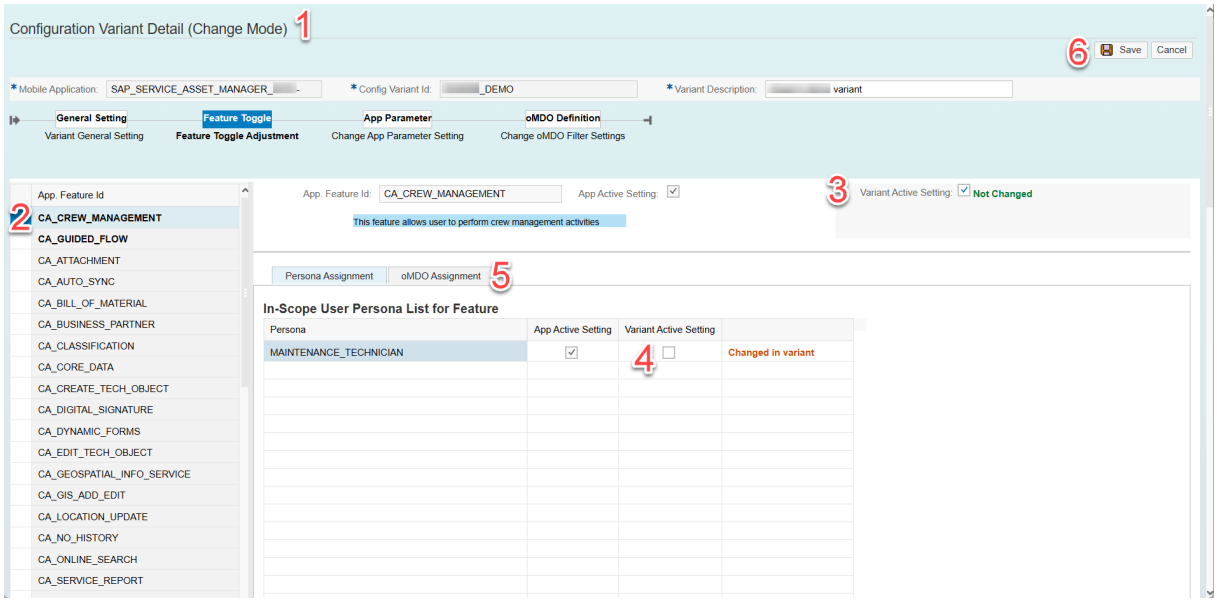
2.1.3 Configuring Feature Toggles

Context

For detailed information about the Variant Tool, see Mobile Configuration Variant Tool Overview [page 77].

Under *Feature Toggle*, you can override the base mobile application's feature settings. For each feature, you can change its assigned personas and oMDOs as follows:

> **Note**
>
> You can only change the settings of personas and oMDOs that are in-scope for the feature.



General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **Enabling and disabling features**: refer to Configuring Features in *MAIF Configuration Guide*.
- For more information about SAP Service and Asset Manager features, refer to Features and Personas Configuration Matrix [page 9].

Procedure

1. Enter *Change mode*.
2. Select a feature from the list of *App. Feature Id*.

   > ⓘ Note
   >
   > The features that have already been changed compared to the base mobile application configuration are highlighted.

3. You can see whether the feature is set to Active for the base mobile application, and override this setting for the Variant.
4. Under the *Persona Assignment* tab, you can activate or deactivate the feature for each persona(s).
5. Under the *oMDO Assignment* tab, you can activate or deactivate each oMDO filter(s) for the feature.

   > ⓘ Note
   >
   > For each setting, you can see whether it is *changed in the variant* or *not changed*.

6. *Save* your changes.

Next Steps

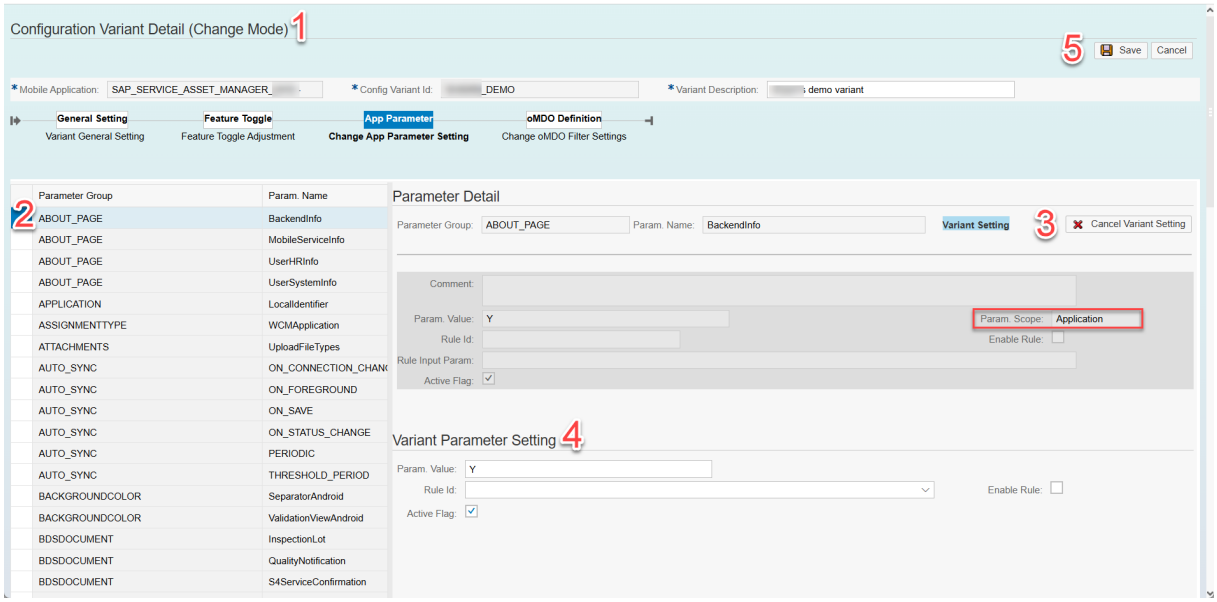
Continue with Configuring Mobile Application Parameters [page 84].

2.1.4 Configuring Mobile Application Parameters

Context

For detailed information about the Variant Tool, see Mobile Configuration Variant Tool Overview [page 77].

Under *App Parameter*, you can override the base mobile application's Application Parameters settings as follows:



General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **Mobile Application Parameters** configuration: refer to Parameters Tab in *MAIF Configuration Guide*.

Procedure

1. Enter *Change mode*.
2. Select a *Parameter* from the list.

> **Note**
>
> The Parameter(s) that have already been changed compared to the base mobile application configuration are highlighted.

3. If there is no Variant Setting for the Parameter, click *Create Variant Setting*.
4. Under *Variant Parameter Setting*, update the following according to your preference:

> **Note**
>
> You can only change Parameters for the Variant that have *Application* set as the *Parameter Scope* in the base mobile application configuration (see image above [page 84]). For more information, see Parameters Tab in *MAIF Configuration Guide*.

   - *Param. Value*
   - *Rule Id*
   - *Enable Rule*
   - *Active Flag*
5. *Save* your changes.

Next Steps

Continue with Configuring oMDO Filter Settings [page 85].

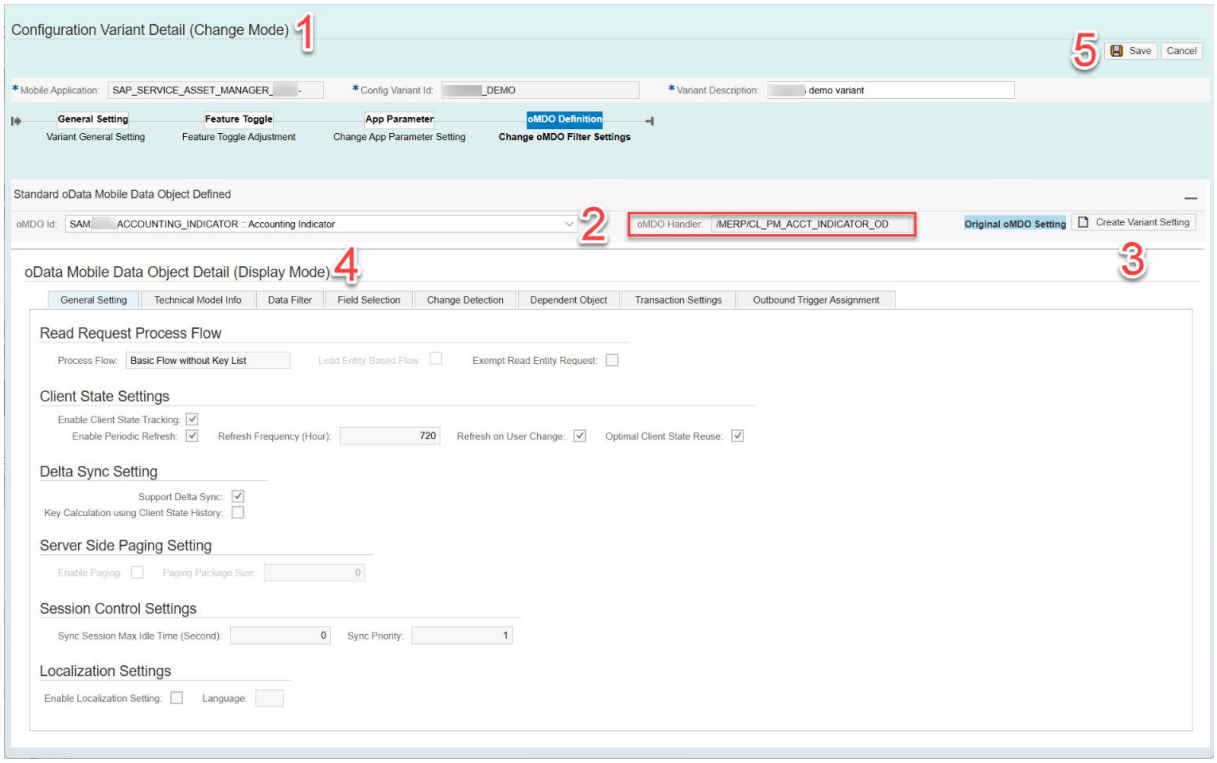
2.1.5 Configuring oMDO Filter Settings

Context

For detailed information about the Variant Tool, see Mobile Configuration Variant Tool Overview [page 77].

Under *oMDO Definition*, you can override the base mobile application's OData Mobile Data Object configuration as follows:

> **Note**
>
> - In this section you can change all oMDO-related data, **except the oMDO Handler** (see image below [page 86]).
> - All override changes recorded in the General Setting [page 80], Feature Toggle [page 82] and Mobile Application Parameter [page 84] sections are saved in separate tables for the Variant in the back end. However, override changes to oMDO objects are saved in the same table of the standard oMDO object.



General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **OMDO** and **OMDO filter** configuration: refer to OData Mobile Data Object Configuration and OData Mobile Data Object Configuration - Data Filter Tab in *MAIF Configuration Guide*.

Procedure

1. Enter *Change mode*.
2. Select an oMDO object from the drop-down list.

   > ⓘ Note
   >
   > If you have already created Variant Settings for any oMDO objects, they will be indicated with ** symbols at the top of the drop-down list.

3. Click *Create Variant Setting*.

   > ⓘ Note
   >
   > If you have already created a Variant Setting for the oMDO object, you can delete it by *Cancel Variant Setting*.

4. Make your changes to the oMDO object (for more information, refer to OData Mobile Data Object Configuration).

5. *Save* your changes.

Next Steps

Continue with Assigning a User to a Variant Configuration in the *MAIF Administrator Guide*.

2.2 Configuring Personas and Features Overview

Persona and feature assignments determine the data downloaded to the mobile client application.

The entity types below are introduced in SAP Service and Asset Manager to return persona- and feature-related configurations to the mobile client. The client logic looks at these entity types to check user personas assignment or assignments and to see if features are enabled. This is used in the mobile client application to determine which user interface elements should appear on certain screens and sections.

- **UserFeature:** In the /MERP/SAP_ONLINE_LOOKUP_EXT_XXXX service, this entity returns a list of features that are applicable based on user personas. With the support of UserFeature, enable parameters are no longer defined in AppParameters.
- **UserPersonas:** In the MERP/SAP_ONLINE_LOOKUP_EXT_XXXX service and /MERP/SAP_SRV_ASSET_MANAGER_XXXX service, this entity returns user persona assignment.
- **UserSyncGroupDetails:** In the /MERP/SAP_ONLINE_LOOKUP_EXT_XXXX service, this entity returns list of entity sets that are applicable based on user personas.

Previously, the application would download all data regardless of enabled or disabled features. This isn't optimal and can impact the performance of initial and delta syncs. Now, during the initial sync, the mobile client makes an online call to fetch the logged on user's persona assignment and entities needed to request in subsequent calls. The only data downloaded is data needed for the persona:

Stat...	Service Call Info	Method	Proc. Time	Appl. Time	Non-GW T...	Req. Size	Resp. Size	Form
■	/MERP/SAP_ASSET_MANAGER_2110/$batch	POST	4,739	2,040	0	4,910	37,213,4...	mixe
■	/MERP/SAP_ASSET_MANAGER_2110/$batch	POST	795	390	0	1,629	5,009,567	mixe
■	/MERP/SAP_ASSET_MANAGER_2110/$batch	POST	4,659	2,471	0	6,469	27,056,0...	mixe
■	/MERP/SAP_ASSET_MANAGER_2110/$batch	POST	1,980	961	0	16,681	4,332,311	mixe
■	/MERP/SAP_ASSET_MANAGER_2110/OpenSyncSession?SAPProd...	POST	66	34	0	0	520	json
■	/MERP/SAP_ASSET_MANAGER_2110/$metadata?sap-language=...	GET	290	2	0	0	1,045,062	xml
■	/MERP/SAP_ONLINE_LOOKUP_EXT_2110/UserSyncGroupDetails	GET	80	38	0	0	246,904	xml
■	/MERP/SAP_ONLINE_LOOKUP_EXT_2110/UserPersonas	GET	61	40	0	0	1,517	xml
■	/MERP/SAP_ONLINE_LOOKUP_EXT_2110/$metadata	GET	14	2	0	0	0	
■	/MERP/SAP_ONLINE_LOOKUP_EXT_2110/	GET	16	2	0	0	5,766	xml
■	/MERP/SAP_ONLINE_LOOKUP_EXT_2110/$metadata	GET	27	1	0	0	48,669	xml
■	/MERP/SAP_ONLINE_LOOKUP_EXT_2110/	GET	27	2	0	0	5,766	xml
■	/MERP/SAP_ONLINE_LOOKUP_EXT_2110/$metadata	GET	30	2	0	0	48,669	xml
■	/MERP/SAP_ONLINE_LOOKUP_EXT_2110/	GET	18	2	0	0	5,766	xml

Use the following topics to configure your personas and features in your mobile application:

- Configuring Personas [page 89]
- Configuring Features [page 93]

- Configuring Component Assignments [page 101]

2.2.1 Usage Types

Each persona is categorized by type of usage, either *Professional* or *Standard*. This determines the Full Use Equivalent (FUE) valuation according to the updated licensing model for SAP Service and Asset Manager.

Professional type of usage is one (1) FUE and Standard is one-half (1/2) FUE. In the base configuration, Maintenance Technician is defined as a professional user, and Field Service Technician and Inventory Clerk are defined as standard users. Customers can also define themselves as custom personas, which is considered a professional usage type.

> **Note**
>
> The usage type does not necessarily depend on the persona, but rather on the available feature sets. For example, a single FUE is the maximum value for any individual user that allows access to all available features, which means that the professional usage type is configured with more feature support than the standard usage type.
>
> The key difference is when a customer uses a standard Mobile Application Integration Framework (MAIF) app, such as SAP Service and Asset Manager, and only needs inventory or field service functionality. In this case, one (1) FUE could cover two users since those personas are standard with only one-half (1/2) FUE value.

The table below shows what type of usage can be configured for different types of application.

Application Type	Persona Type	Usage Type	Changeability
MAIF application	Maintenance Technician	Professional	No change allowed in customer system Changes allowed in SAP development system only
	Field Service Technician	Standard	
	Inventory Clerk	Standard	
	Custom	Professional	Change allowed in customer system. Custom persona can be created in customer namespace only.
Partner-defined MAIF application	Persona I	Professional	Can only be changed in partner development system
	Persona II	Standard	
	Persona III	Standard	
	Custom	Professional	Change allowed in customer system. Custom persona can be created in customer namespace only.

Application Type	Persona Type	Usage Type	Changeability
Custom-defined MAIF application	Custom	Professional	Change allowed in customer system. Custom persona can be created in customer namespace only.

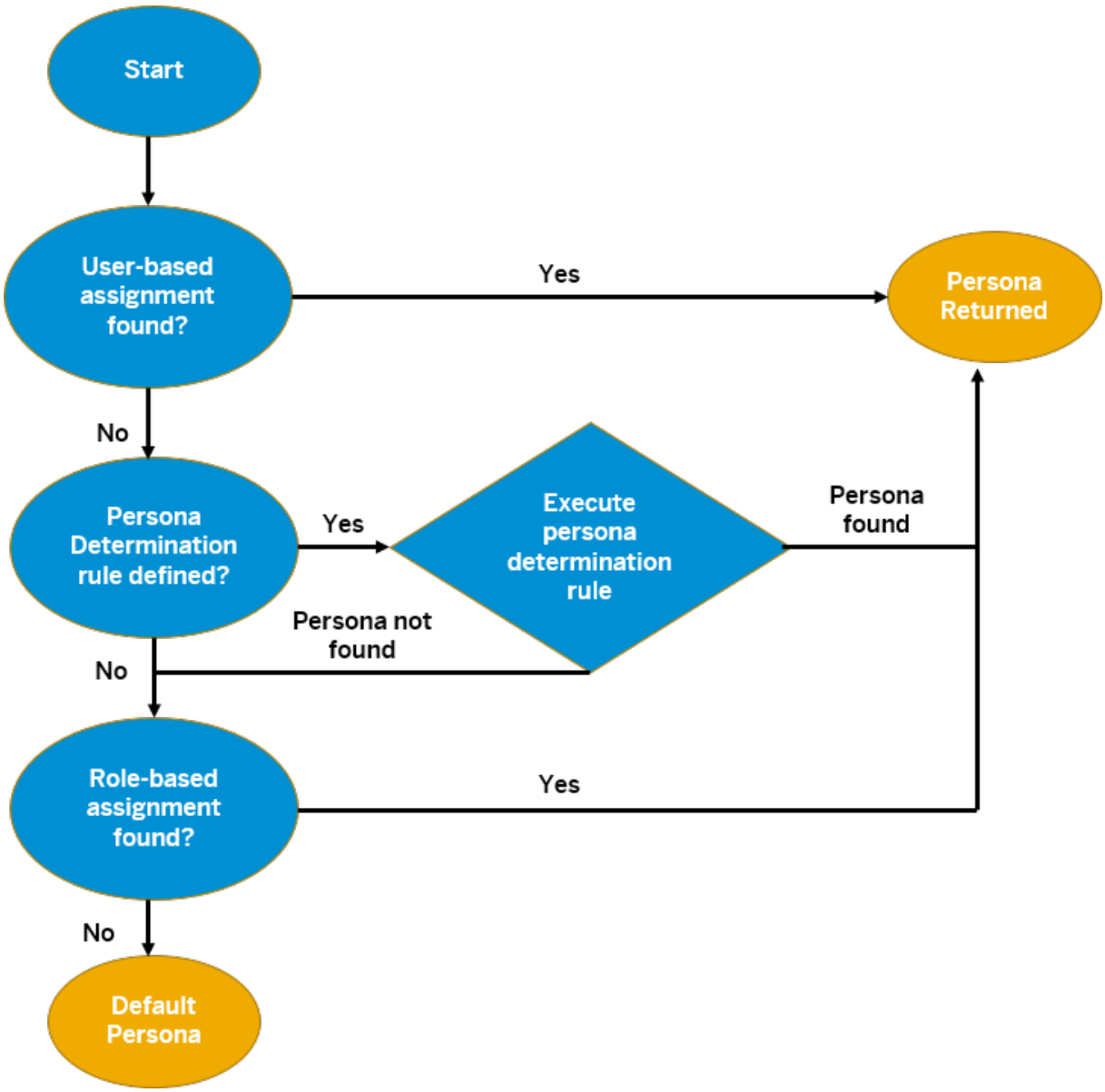
2.2.2 Configuring Personas

SAP Service and Asset Manager allows a single user to be assigned multiple personas, and the user may switch between them in the *Profile Settings* screen of the mobile application.

Context

> **Note**
>
> - From 2405 version upwards, you can pre-configure custom personas. However, this will not display the home page associated with it, instead you will receive a pop-up message that there is no home page for this persona.
> - For general information about SAP Service and Asset Manager personas, see Persona Overviews.

To access the default persona determination rule; in *SAP GUI*, navigate to */SYCLO/CL_CORE_PERSONA_RULE*. The system will determine the persona based on the following logic and sequence:



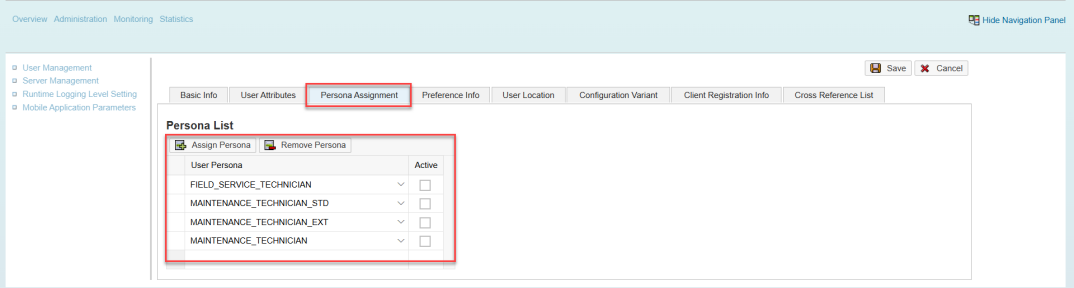
To assign persona(s) to a mobile user, and optionally create a custom persona, perform the following steps:

Procedure

1. Choose **one of the following ways** to assign a persona to a mobile user:
   a. **User-based assignment**:

      Users may be assigned to one or more personas in the *Admin Portal*, launched in *SAP GUI* with tcode `/n/syclo/admin`:

1. Navigate to *System Administration & Monitoring Portal* > *Administration* > *User Management*.
2. Search for and select a *Mobile User*, go to the *Persona Assignment* tab and enter *Change Mode*.
3. Assign or remove personas according to your preference.
4. This is first considered to determine a user's persona. If a persona is assigned here, you will not need to do further checks.



> **Note**
>
> - See the following topics and subtopics for detailed information, depending on your back end system:
>   - Enabling Mobile-Specific Authorization Checks *Mobile Add-On for SAP S/4HANA Security Guide topic and subtopics in the* .
>   - Topic and subtopics in the Enabling Mobile-Specific Authorization Checks topic and subtopics in the *Mobile Add-On for ERP Security Guide*.
> - For more information about the Admin Portal, refer to the MAIF Administrator Guide in *Mobile Application Integration Framework documentation*.

b. **Role-based assignment:**

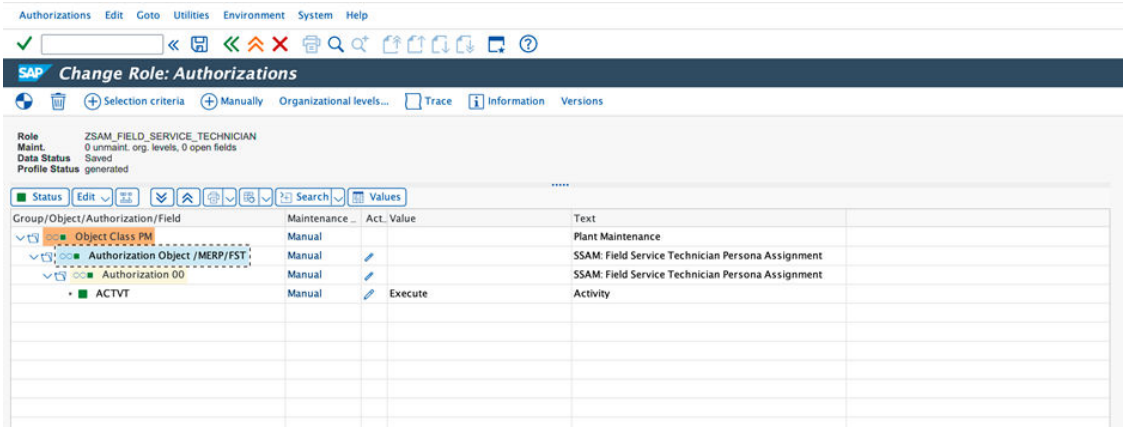
Each persona is associated with a pre-defined authorization object in SAP Service and Asset Manager. You can assign the pre-defined authorization objects to users as needed. The authorization objects are then used to determine the user persona.These are typically assigned to a role in *SAP GUI* via t-code PFCG. By default, the following standard authorization objects are delivered:

Persona Name	Authorization Object	Authorization Attribute	Value
FIELD_LOGISTICS_OPERATOR	/MERP/FLOG	ACTVT	16
FIELD_SERVICE_TECHNICIAN	/MERP/FST	ACTVT	16
FIELD_SERVICE_TECHNICIAN_PRO	/MERP/FSTP	ACTVT	16
FIELD_SERVICE_TECH_STD_EXT	/MERP/CST	ACTVT	16
INVENTORY_CLERK	/MERP/SIC	ACTVT	16
MAINTENANCE_TECHNICIAN	/MERP/SMT	ACTVT	16
MAINTENANCE_TECHNICIAN_EXT	/MERP/CST	ACTVT	16

Persona Name	Authorization Object	Authorization Attribute	Value
MAINTENANCE_TECHNI-CIAN_STD	/MERP/MTB	ACTVT	16
SAFETY_TECHNICIAN	/MERP/WCM	ACTVT	16
WAREHOUSE_CLERK	/MERP/EWM	ACTVT	16

> **Note**
>
> For more information, see Mobile User Essential Authorizations.

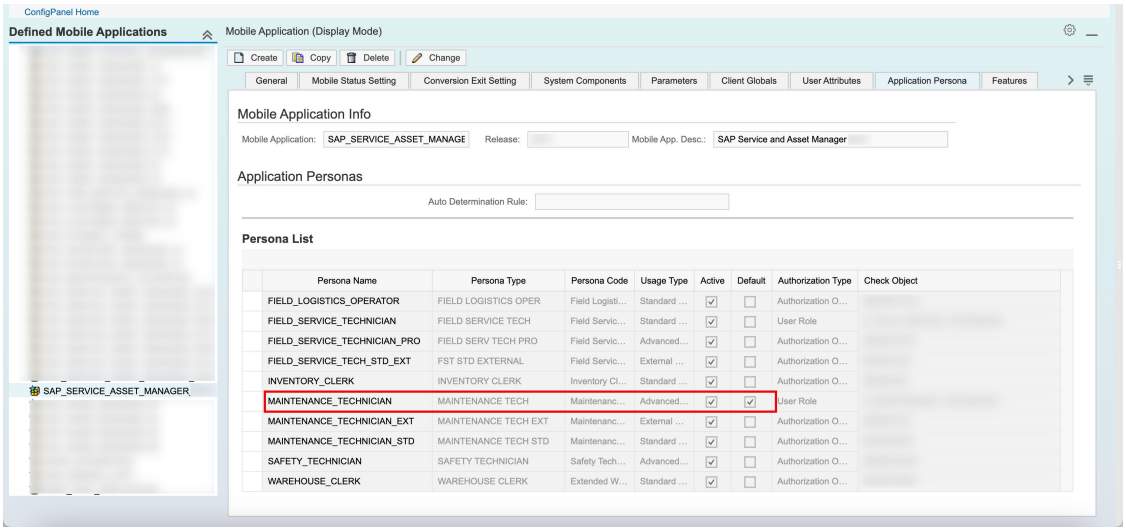
You need to create a custom role or roles and assigned authorization objects accordingly based on your own business and security needs.



c. **Default persona assignment:**

If none of the above options are found, the system will use the preconfigured default persona. The default persona is the *Maintenance Technician* in the standard delivery.

You can update the default persona based on your own business needs by selecting the default checkbox in the *Configuration Panel*:



2. Implement your own custom rule, if desired. Select your custom rule in the *Auto Determination Rule* field.
3. To pre-configure a custom persona, make the following changes to the metadata:
    - Create an item in the *SideMenuDrawer.page* with *_Name of OverviewCustom*
    - Set the *PageToOpen* property to point to a page (new or existing) that is to be the *Home* page for this persona.
      You can make other changes to the custom persona metadata, but these changes are mandatory.

2.2.3 Configuring Features

Customers can disable a feature if it is not relevant in their business scenarios, regardless of the personas used. Customers can also create features, not just enable or disable standard features.

Context

A new feature created by a customer can only be created in the customer namespace.

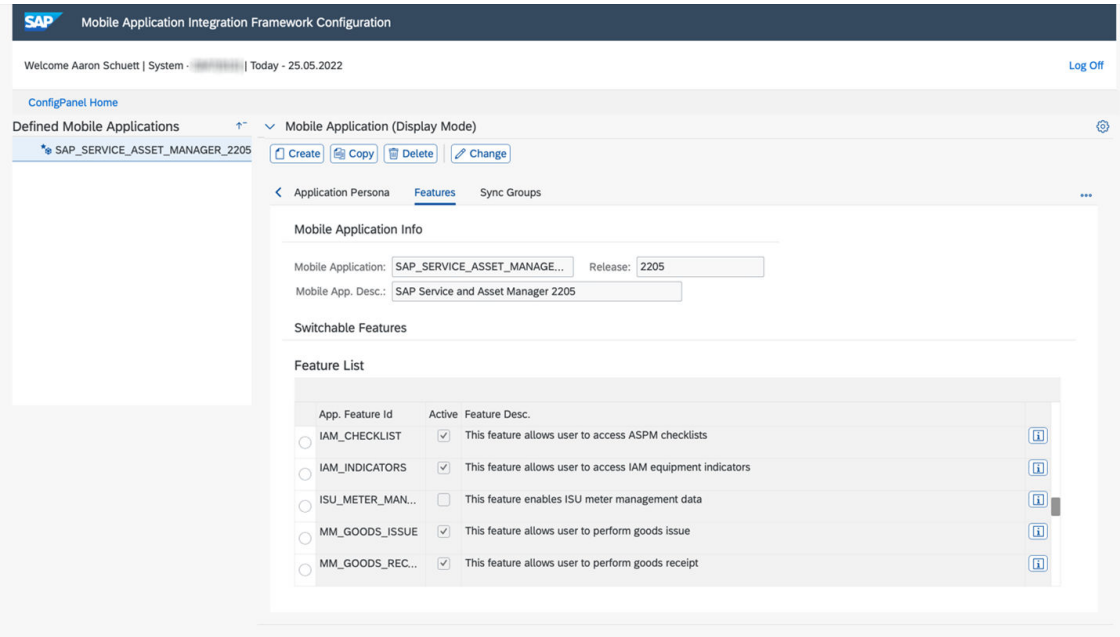
> ⓘ Note
>
> As of the SAP Service and Asset Manager 2205 release, enable and disable parameters are no longer available through the *Parameters* tab. You enable or disable all features through the *Features* tab. See the Configuring Features [page 93] procedure for details.

Procedure

1. Choose one of the following ways to proceed:
    a. **Application level**: Navigate to *Configuration Panel* > *Mobile Application Configuration hyperlink* > *Select Mobile Application (SAP_SERVICE_ASSET_MANAGER_<version>)* > *Features tab* from the home page.

    The list of features delivered in SAP Service and Asset Manager is displayed in the *Configuration Panel*. You may define new features in a customer namespace only.

    Each feature has an *Active* check mark that you can toggle. This acts as the master switch across the application.

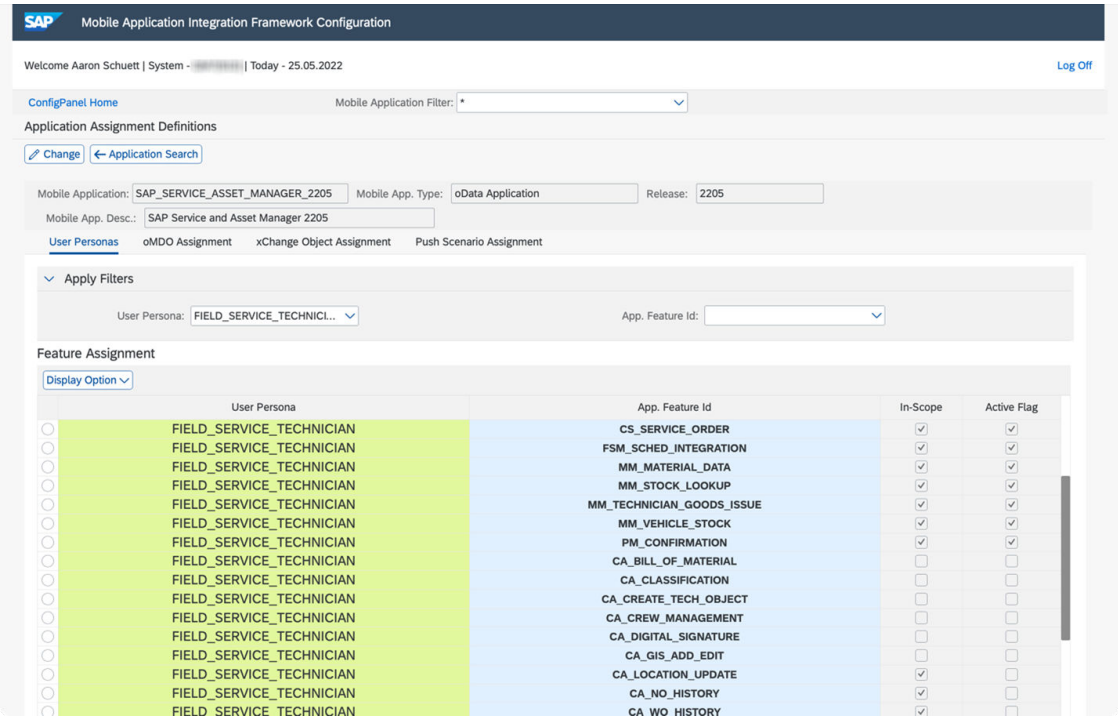


Note that enabling feature above does not check if system is qualified for the feature or not. If your system does not support ISU Meter Management, but you enable the ISU_METER_MANAGEMENT feature in the feature list, you could run into issues.

b. **Persona level**: Navigate to *Configuration Panel* > *Component Assignments hyperlink* > *Select Mobile Application (SAP_SERVICE_ASSET_MANAGER_<version>)* > *User Personas tab* from the home page.

   You can also toggle features related to a persona. Each persona is configured with a list of features supported in the standard delivery of SAP Service and Asset Manager.

   You can view a list of features by persona in the *Configuration Panel*. Each feature has an *In-Scope* checkbox, meaning that the feature is allowed for that persona. In-scope features are not editable in customer or QA environments. Only In-Scope items can be enabled or disabled using the *Active Flag* checkbox.



You can enable a feature for one persona, but disable the same feature for another persona. The list can be filtered using the *User Persona* or *Application Feature* Id drop-down list to find entries directly.

Note that if the feature is disabled at the application-main switch level, the feature is still considered disabled, regardless of the *Active Flag* status at the persona level.

2. Click the *Change* button. Enable or disable desired features.
3. *Save* your changes.

Results

Enabled features display in the *Component Assignment* > *Switchable Features* tab.

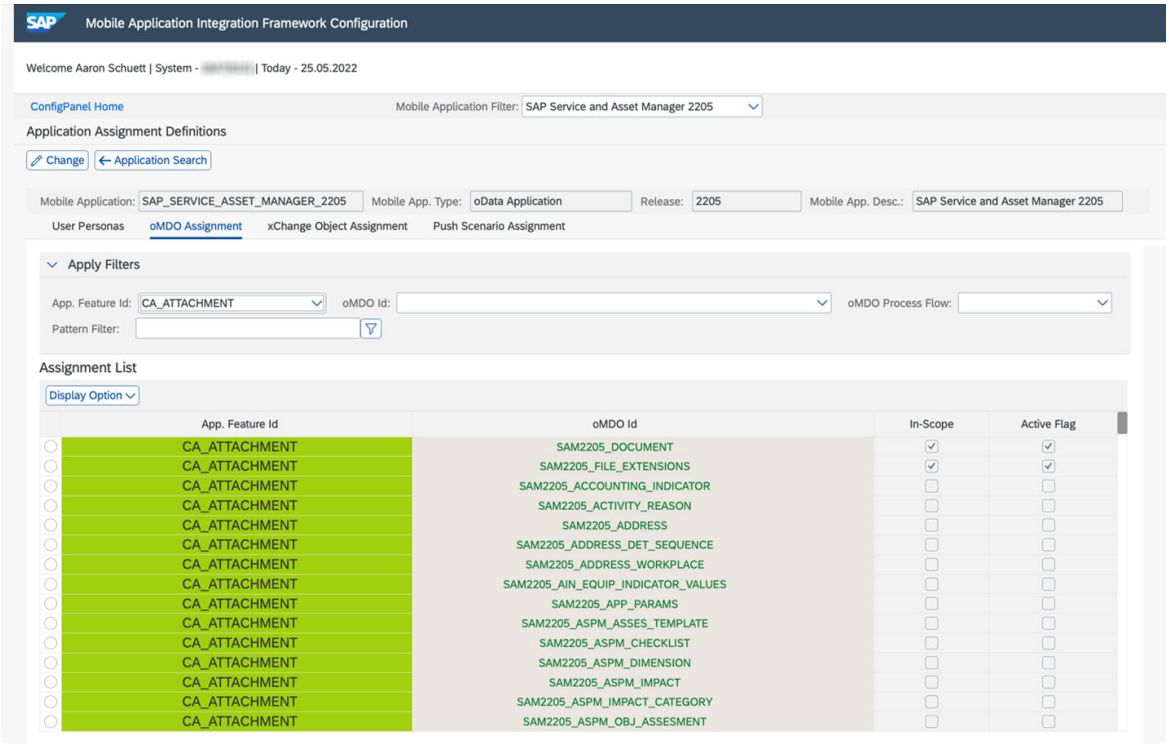
2.2.3.1 Performance Calibration

During mobile client synchronization, all active data objects are sent to the mobile user. For example, if data is being sent to the mobile user that the client application does not need, this can increase the synchronization time.

Disable the data objects that are not used in your workflow. Below are several ways to accomplish this.

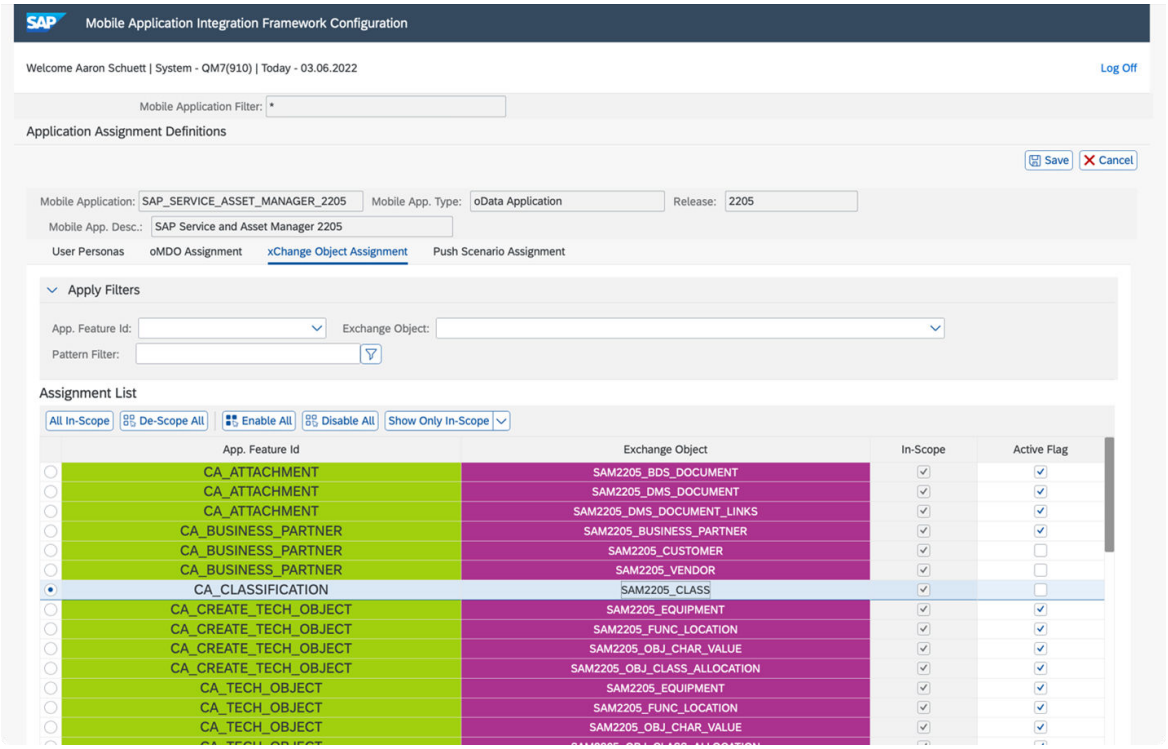
- **oMDO Assignment**: Navigate to *Configuration Panel* > *Component Assignments hyperlink* > *Select Mobile Application (SAP_SERVICE_ASSET_MANAGER_2205)* > *oMDO Assignment tab*.

Each feature is associated with one or more oData Mobile Data Object (oMDO) which provides business logic for a business object used in the mobile application and is mapped to OData requests for a business object on the backend.
You can view an oMDO list in the *Configuration Panel* and choose which entities are required and disable the others to avoid requesting unnecessary data during the mobile sync.

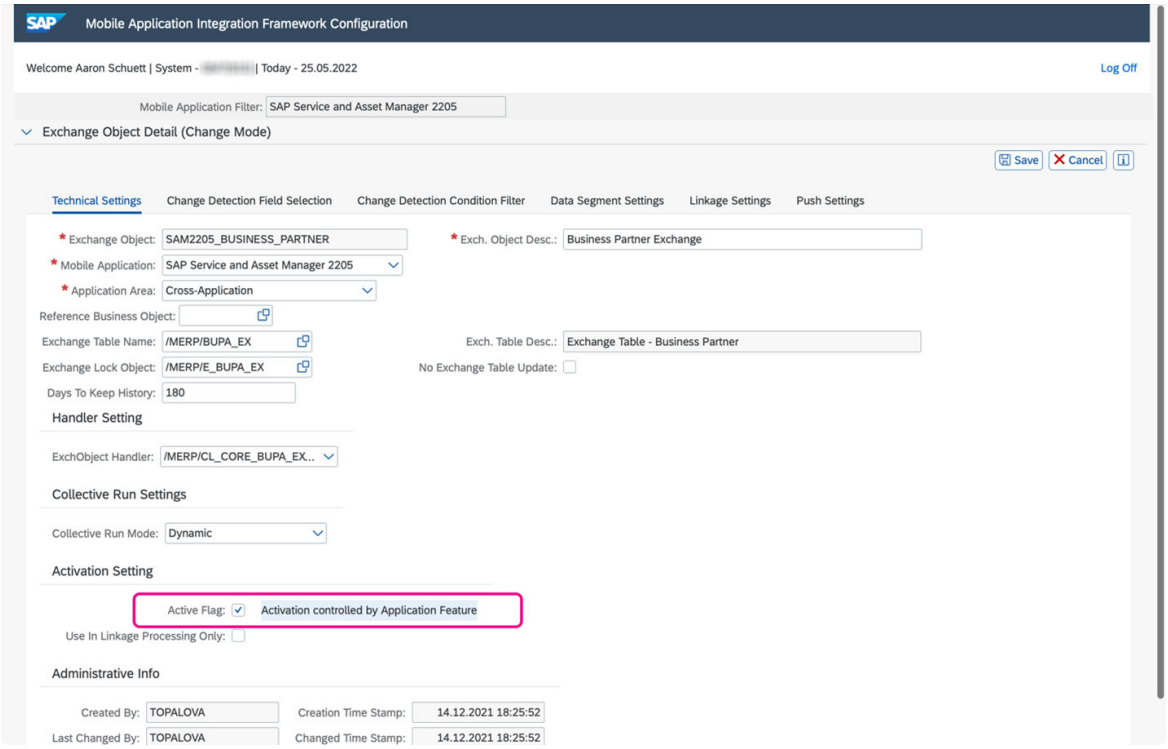


Like feature assignments, the *In-Scope* check mark indicates the data objects that are supported for each feature. Only In-Scope items can be enabled/disabled using the *Active Flag* check mark, and In-scope features are not editable in customer or QA systems.

- **Exchange Object Assignment:** Navigate to *Configuration Panel* > *Component Assignments hyperlink* > *Select Mobile Application (SAP_SERVICE_ASSET_MANAGER_2205)* > *xChange Object Assignment tab*.
Features can also be associated with an exchange object that combines technical objects, such as the exchange class handler, the exchange table and the lock object, with configuration rules.
You can view the list of exchange objects in the *Configuration Panel* and select the ones you need and disable the others.



You can also modify the active objects individually using the exchange object configuration. In this case, navigate to *Configuration Panel* > *Exchange Object Configuration hyperlink* > *Mobile Application Filter (SAP_SERVICE_ASSET_MANAGER_2205)* > *Exchange Object By Application Area* > *Technical Settings tab* >.



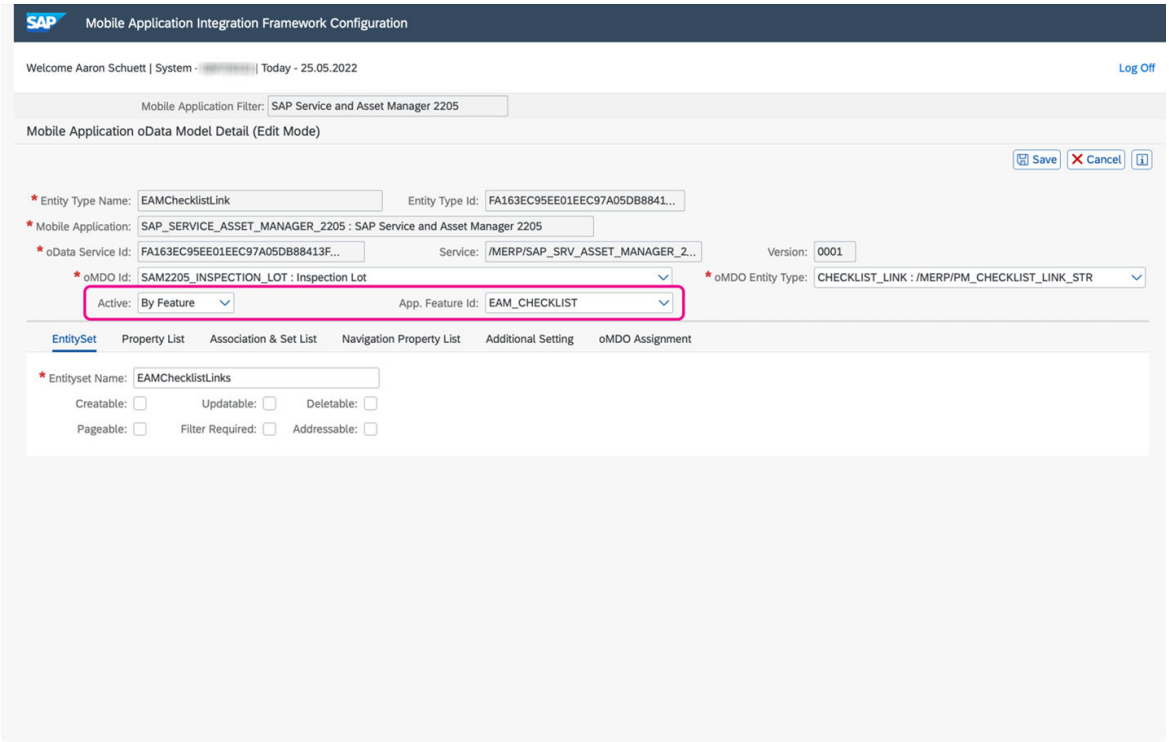
If the exchange object is assigned to a feature, the check mark *Activation controlled by Application Feature* will appear next to the *Active* check mark.

> **Note**
>
> This control is like a master switch; if activation is disabled here, it will be disabled in all places, regardless of the active flags set in the previously discussed methods. However, it is also important to note that if an object is active here but disabled by the other methods, the linked exchange will not be executed when changes are made to the object. This prevents unnecessary exchanges from being triggered if the feature is not applicable to customers.

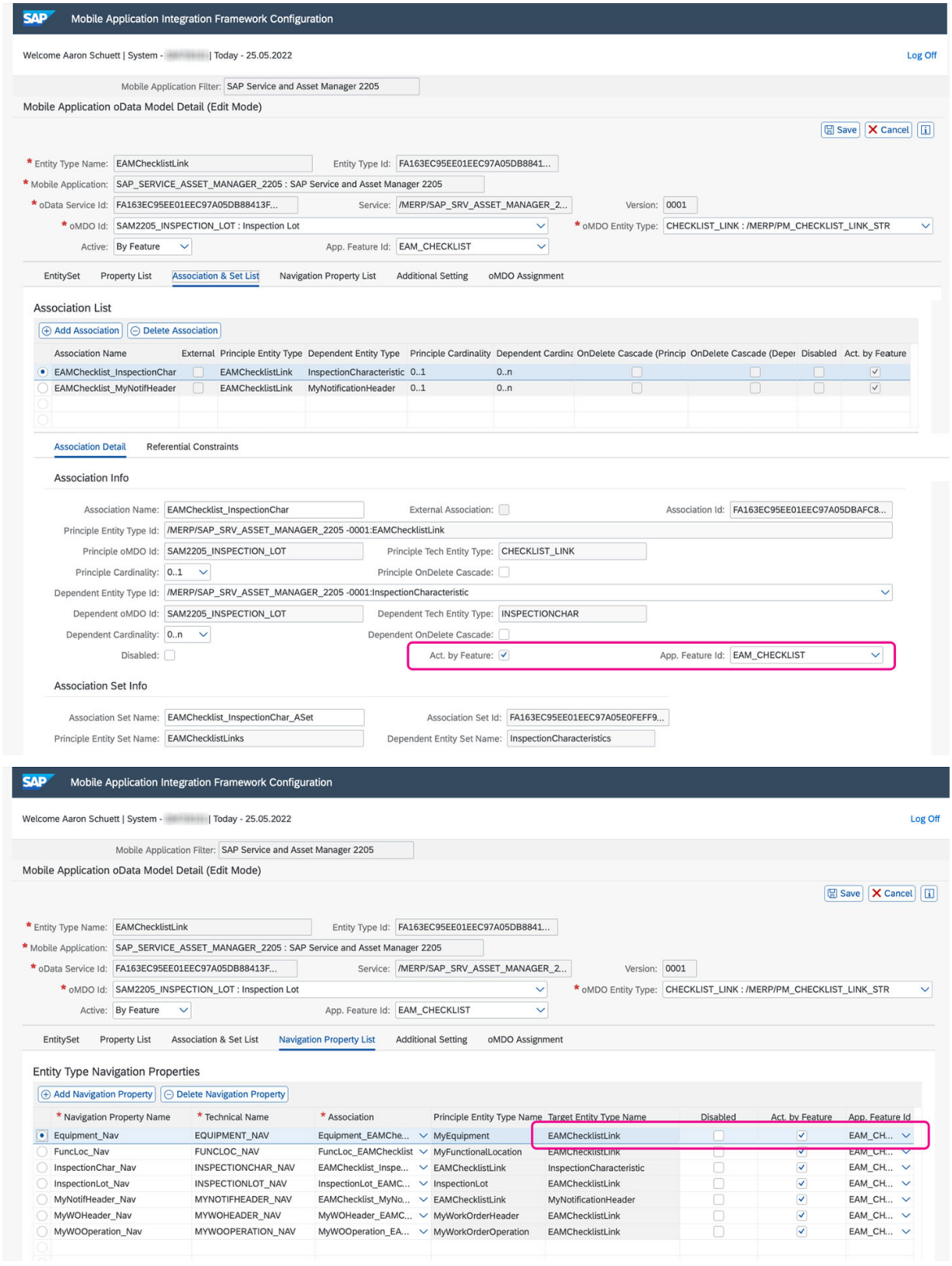
2.2.3.1.1 Activation by Feature

There are several entities in the Configuration Panel where it is possible to support activation by feature. This allows you to go down the hierarchy to manage entities, dependency objects, and more.

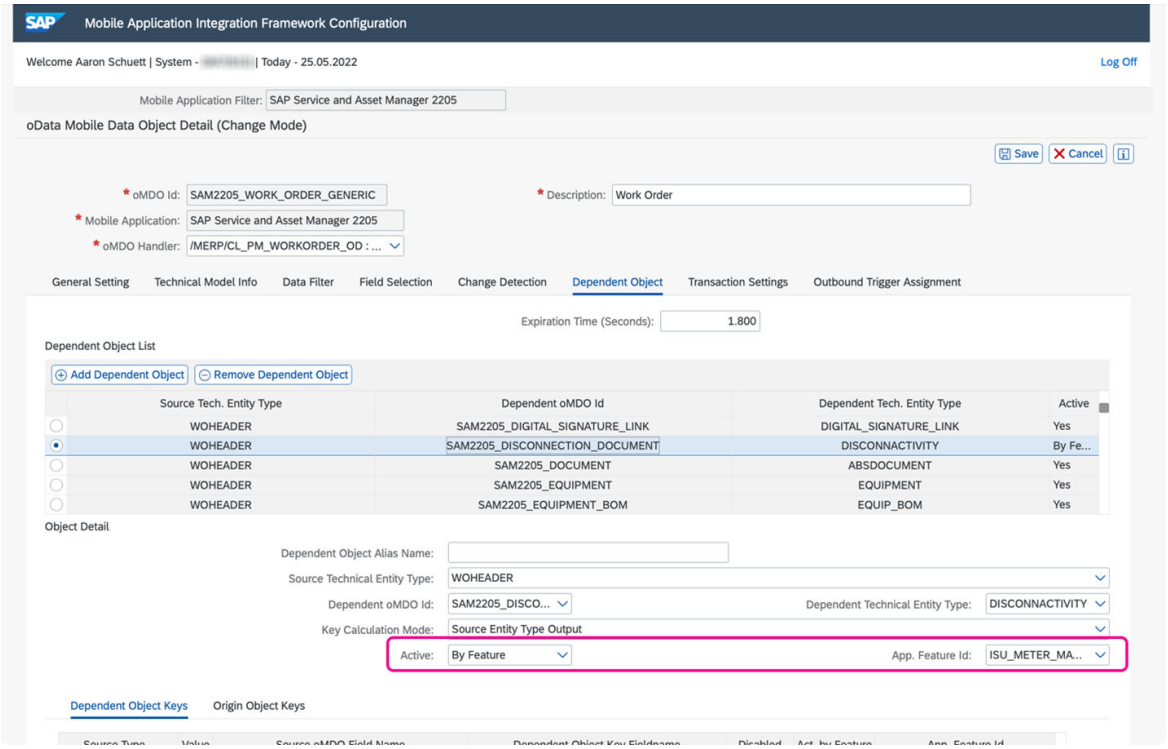
- **oData Model Entity Type:** You can specify a particular entity to be enabled only if the assigned feature is activated. In the example below, the EAMChecklistLink entity set is applicable to the Enterprise Asset Management (EAM) checklist functionality. Here only when EAM_CHECKLIST feature is enabled, EAMChecklistLink is available for the client.



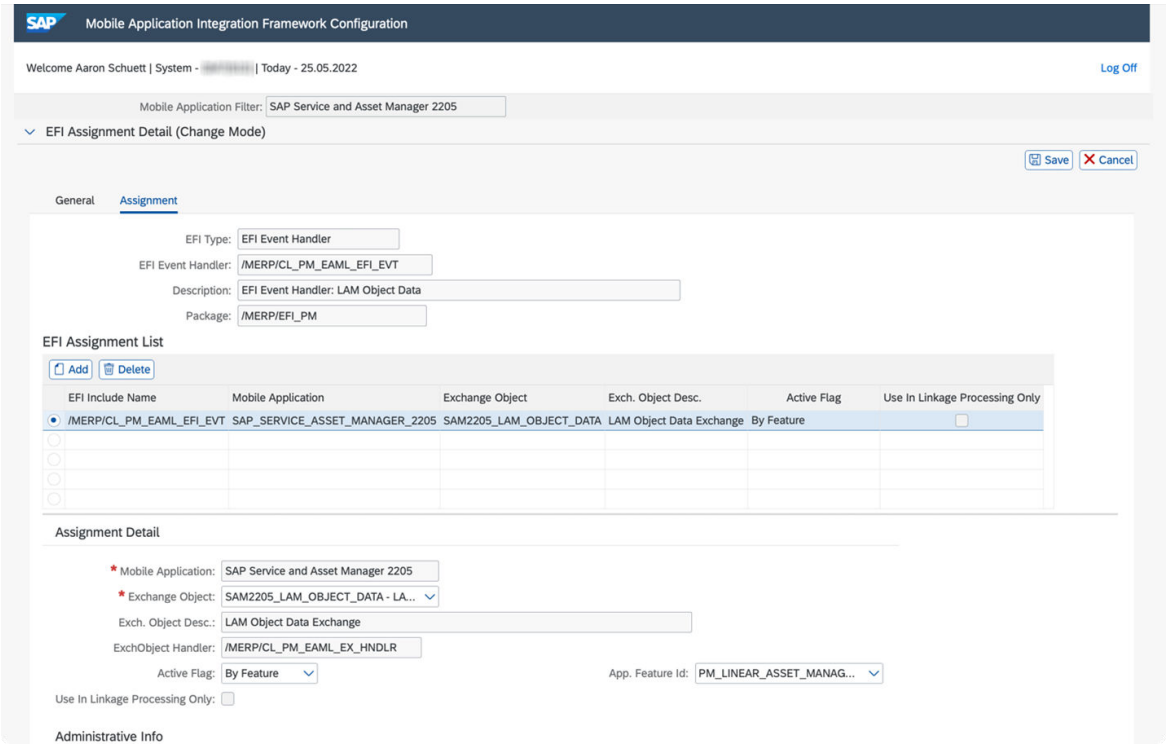
- **Association and navigation:** Like an entity type, association and navigation can be assigned to a feature. Only when the assigned feature is enabled does the association become visible to the mobile client. If the disabled flag is active, the entity will not be visible to the mobile client regardless of whether the feature is enabled or not.



- **Dependency Object:** If activation by feature is configured in a dependent object, and if the assigned feature is not enabled, dependency objects will not be generated in the dependency queue.



- **EFI configuration:** An Enhancement Framework Implementation (EFI) event handler can be assigned to a feature with active flag set to *By Feature*.



> **Note**
>
> We only support one feature assignment per object (such as entity type, association, navigation, EFI). You cannot assign multiple features to an object in the Configuration Panel.

2.2.4 Configuring Component Assignments

The *Component Assignment* page allows you to define what features are applicable for each persona.

Context

Using the *User Personas* tab, you can enable or disable features as desired. For example, *PM_CONFIRMATION* is enabled by default, and *HR_TIMESHEET* is disabled. If your site uses CATS, you can disable PM_CONFIRMATION and enable HR_TIMESHEET.

The *Switchable Features* tab allows you to configure OMDOs required for each feature. During initial and delta syncs, the client only downloads data from the assigned OMDOs. Activating specific OMDOs determines the entities and data that is downloaded to the mobile device.

Procedure

1. Navigate to *Component Assignments* from the home page. Select your application in the *Mobile Application Filter* dropdown. Click on your application hyperlink in the *Search Result* table.
2. Click the *Change* button. Enable or disable desired features using the *Active Flag* checkbox. *Save* your changes.
3. Select the *Switchable Features* tab.
4. Click the *Change* button. Enable or disable desired OMDOs using the *Active Flag* checkbox. *Save* your changes.

> **Note**
>
> Don't select OMDOs that belong to the online service (ex: */MERP/SAP_ONLINE_LOOKUP_EXT_<version>*). These online service entities might not exist in the base service (*/MERP/SAP_SRV_ASSET_MGR_<version>*).

> **Note**
>
> If you don't see an expected feature in the list, ensure it's enabled on the *Mobile Application Configuration* > *Features tab*. See the Configuring Features [page 93] procedure for more information.

Next Steps

After you've enabled or disabled a feature in the *Component Assignments* page, navigate to *Home* > *Mobile Application Configuration* > *Parameters tab*. Find the parameter group and parameter name and maintain the feature enablement accordingly.

2.3 Enabling and Disabling Features Per User Through SAP Authorization

Using parameter framework configuration, configure parameters to enable or disable various features per the authorization of the user in the back end.

Each mobile user is connected to a back end SAP user. The back-end SAP user can be assigned one or more roles. These roles grant their holders authorizations within the back end system. Through parameter configuration, SAP provides a standard rule handler that performs a TCode authorization. SAP also provides new globals that can turn on and off new features.

If a parameter is enabled to use a rule instead of a global, and the user role has an authorization to run a specific transaction code, then that specific feature is enabled for that SAP user. If the user has the authorization' for a specific transaction code, then the specific feature is disabled for that mobile user. Therefore, depending on the authorization of the SAP user, the feature now either works or does not work, displays, or does not display (depending on the feature function), rather than is turned on or off for all users.

Features Available Through SAP Authorization

The following features are available for you to enable or disable. Use the following subsection to learn how to use the ConfigPanel to enable or disable a feature based on the authorization of the user.

Component	Functionality	Category	TCODE	Back-End Parameter	Comments
SAP Service and Asset Manager	Create work order	Work Orders	IW31	Enable.WO.Create	Includes operations and suboperations
SAP Service and Asset Manager	Edit work order	Work Orders	IW32	Enable.WO.Edit	Includes operations and suboperations (except local)
SAP Service and Asset Manager	Create Notification	Notifications	IW26	Enable.NO.Create	Includes items, tasks, and activities

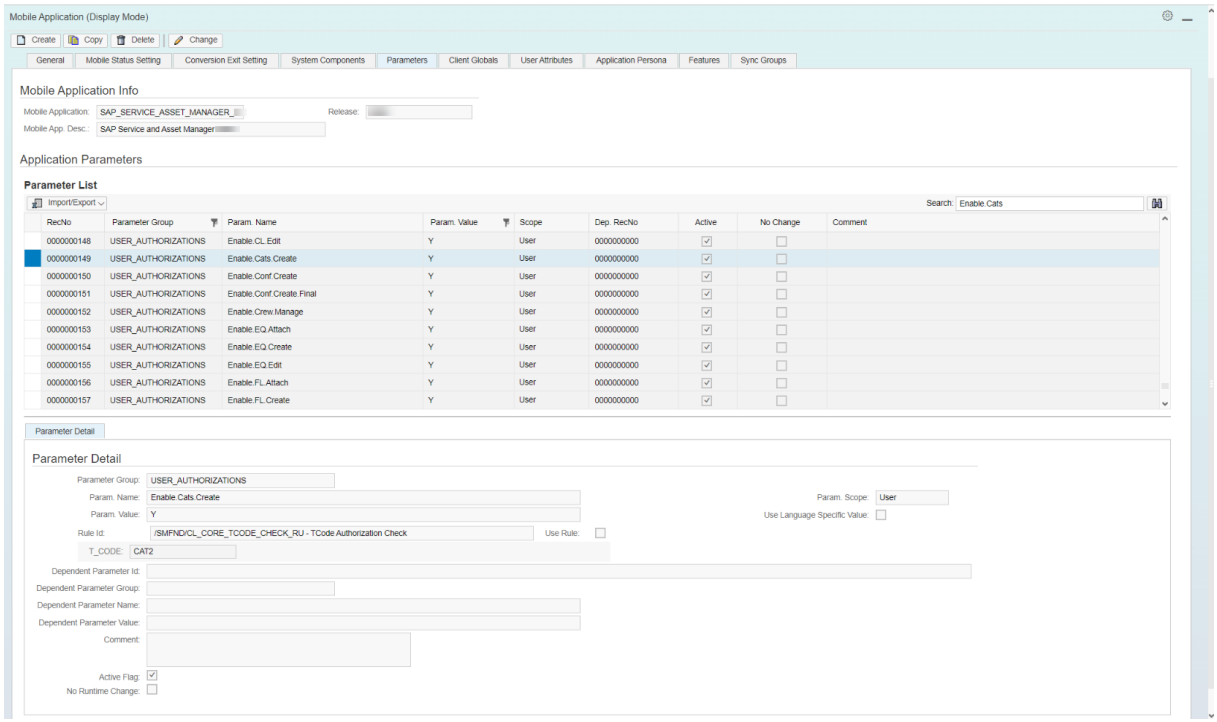
Component	Functionality	Category	TCODE	Back-End Parameter	Comments
SAP Service and Asset Manager	Edit Notification	Notifications	IW22	Enable.NO.Edit	Includes items, tasks, and activities (except local)
SAP Service and Asset Manager	Edit FLOC	Functional Location	IL02	Enable.FL.Edit	Includes adding characteristics (except local)
SAP Service and Asset Manager	Edit equip	Equipment	IE02	Enable.EQ.Edit	Includes adding characteristics, install, and dismantle (except local)
SAP Service and Asset Manager	Measurement readings	Measurement	IK11	Enable.MD.Create	
SAP Service and Asset Manager	Equip attachment upload	Attachments	N/A	Enable.EQ.Attach	See the *Generic Authorization Check* section in this topic
SAP Service and Asset Manager	FLOC attachment upload	Attachments	N/A	Enable.FL.Attach	See the *Generic Authorization Check* section in this topic
SAP Service and Asset Manager	Allow time recording	CATS	CAT2	Enable.Cats.Create	
SAP Service and Asset Manager	Allow confirmations	Confirmation	IW41	Enable.Conf.Create	
SAP Service and Asset Manager	Allow final confirmation	Confirmation	N/A	Enable.Conf.Create.Final	See the *Generic Authorization Check* section in this topic
SAP Service and Asset Manager	Issue and return parts	Materials	MIGO	Enable.Parts.Issue	
CUSTOMER SERVICE	Service notification create	Notifications	IW51	Enable.SNO.Create	
CUSTOMER SERVICE	Service notification edit	Notifications	IW52	Enable.SNO.Edit	Except local
ASSET CENTRAL	Add checklist	Checklist	N/A	Enable.CL.Create	See the *Generic Authorization Check* section in this topic
ASSET CENTRAL	Fill checklist	Checklist	N/A	Enable.CL.Edit	See the *Generic Authorization Check* section in this topic

Component	Functionality	Category	TCODE	Back-End Parameter	Comments
CREW	Manage crew	Crew	N/A	Enable.Crew.Manage	See the *Generic Authorization Check* section in this topic
SUPERVISOR	Enable the supervisor role	Supervisor		SupervisorRole	

How to Enable or Disable Features Per User Through Parameters

1. Using the ConfigPanel, navigate from the main screen to *Mobile Application Configuration* > *Parameters tab*. In the left column, *Defined Mobile Applications*, select your application.
   The *Parameter List* table populates with a list of all globals available for the application.
2. Perform a search for the parameter you want to enable or disable as a feature by user role by using the table in this topic to ensure that the parameter is available in the parameter framework for configuration. Search for your parameter in the *Parameter List* using the *Search* box. All user authorization parameters are found under the `<Parameter Group>` name of *USER_AUTHORIZATIONS*. Select your parameter and click the *Change* button.
3. The rule */SMFND/CL_CORE_TCODE_CHECK_RU - TCode Authorization Check* is already selected for you in the `<Rule ID>` field. When you check the `<Use Rule>` checkbox, the rule is active.
4. Change the `<Param. Scope>` dropdown selection from *Application* to *User*.
5. If needed, select the appropriate `<Dependent Parameter ID>` from the dropdown list.
6. Check the `<Active Flag>` checkbox to ensure that your new parameter is active for the user role. *Save* your changes.

See the following screenshot for an example of a configured user role parameter:



Generic Authorization Check

Use the rule */SMFND/CL_CORE_AUTH_CHECK_RU - TCode Authorization Check* to enable a more generic authorization check. This rule is used for the following parameters:

- Enable.EQ.Attach
- Enable.FL.Attach
- Enable.Conf.Create.Final
- Enable.Parts.Issue
- Enable.CL.Create
- Enable.CL.Edit
- Enable.Crew.Manage

To use the */SMFND/CL_CORE_AUTH_CHECK_RU - TCode Authorization Check*, do the following:

1. Create an authorization object. See Authorization Objects for more information.
2. Assign the authorization object to a role.
3. Assign the role to users who will be using the feature.
4. Configure the rule in the ConfigPanel to reference the new authorization object. For more information, see the AUTHORITY-CHECK topic.

2.4 Configuring Notification Catalog Types

Use parameters to configure the notification catalog types.

Context

Code groups that belong together in terms of content are grouped in catalogs. These catalogs are identified by the catalog type (a number or a letter). For example, in this way, you combine:

- All code groups for particular problems for a catalog type
- All code for causes for another catalog type and
- All code groups for activities for a further catalog type

Use the *CATALOGTYPE* parameter group and the following parameters within the group to configure your catalog types for notifications in SAP Service and Asset Manager:

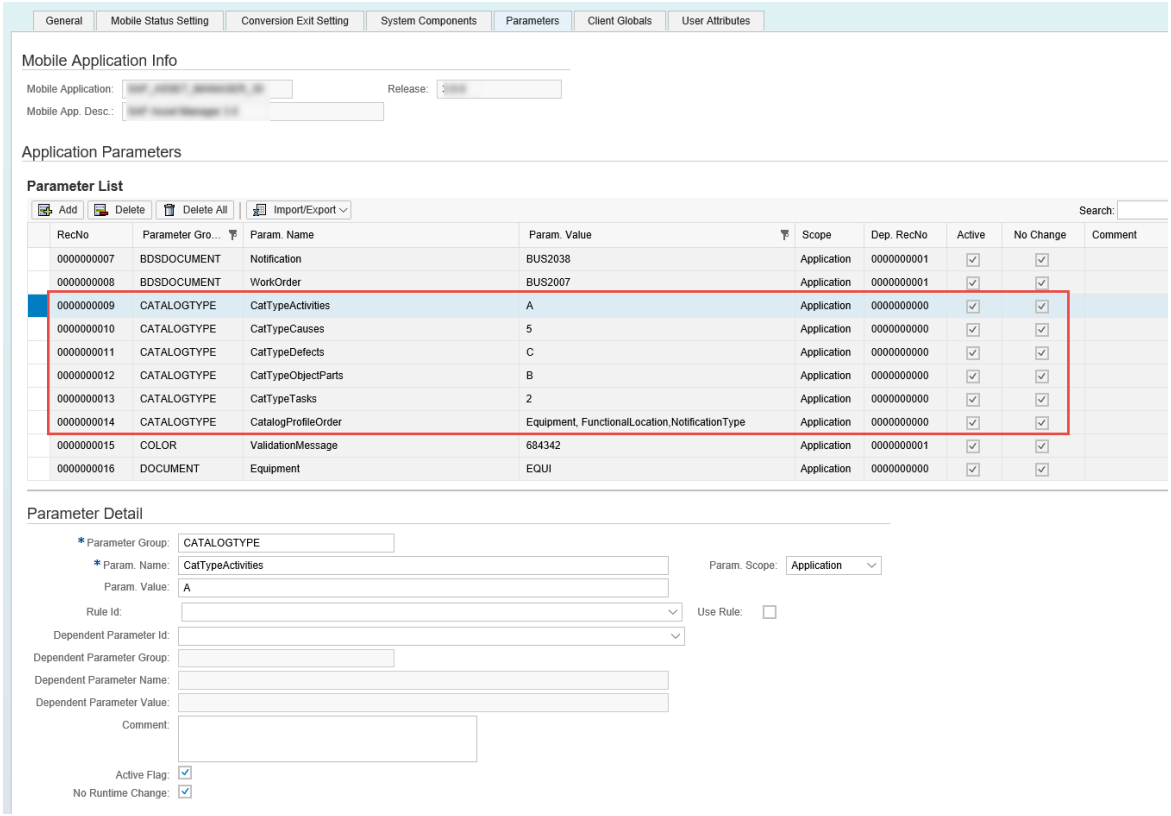
- **CatTypeActivities:** Default is *A*
- **CatTypeCauses:** Default is *5*
- **CatTypeDefects:** Default is *C*
- **CatTypeObjectParts:** Default is *B*
- **CatTypeTasks:** Default is *2*
- **CatalogProfileOrder:** Default is *Equipment, Functional Location, Notification Type*

The *CATALOGTYPE* parameters correspond to the rules found in the OData mobile data object *SAMXXXX_CATALOG_CODES*. You can add a new data filter rule to your customer namespace, or change the existing parameter-rule association to a new parameter-rule association.

Procedure

1. Using the ConfigPanel, navigate to *Mobile Application Configuration* > *Parameters tab*. In the left column, *Defined Mobile Applications*, select your application.

   The *Parameter List* populates with a list of all parameters available for the application.
2. The *CatType[xxx]* parameters are found in the *CATALOGTYPE* group. You can scroll down to find the parameter, or perform a search using the *Search* box. Highlight the parameter you want to configure and click the *Change* button.



3. Make your desired parameter association changes, or change the value of a parameter to *Z*, a custom activity catalog type.
4. Check the `<Active>` flag to ensure that the parameter is used by the mobile application. If desired, and if not already checked, check the `<No Runtime Change>` box to ensure that the value of the parameter is not overridden at runtime through synchronization processing.
5. *Save* your changes.
6. If you are creating a custom activity value type, navigate to *OData Mobile Data Object Configuration* > *Data Filter Tab* > *SAMXXXX_CATALOG_CODES* > *Operation - READ* > *Standard Filter* > *CATALOG_TYPE* .
7. Click the *Change* button. Add the new value. For information on working with rules, see Working with oData MDO Filter Rules [page 146].
8. *Save* your changes.

2.5 Configuring Mobile User Attributes

The *User Attributes* tab in the *Mobile Application Configuration* page of the ConfigPanel allows you to maintain multiple values for a selected attribute.

Context

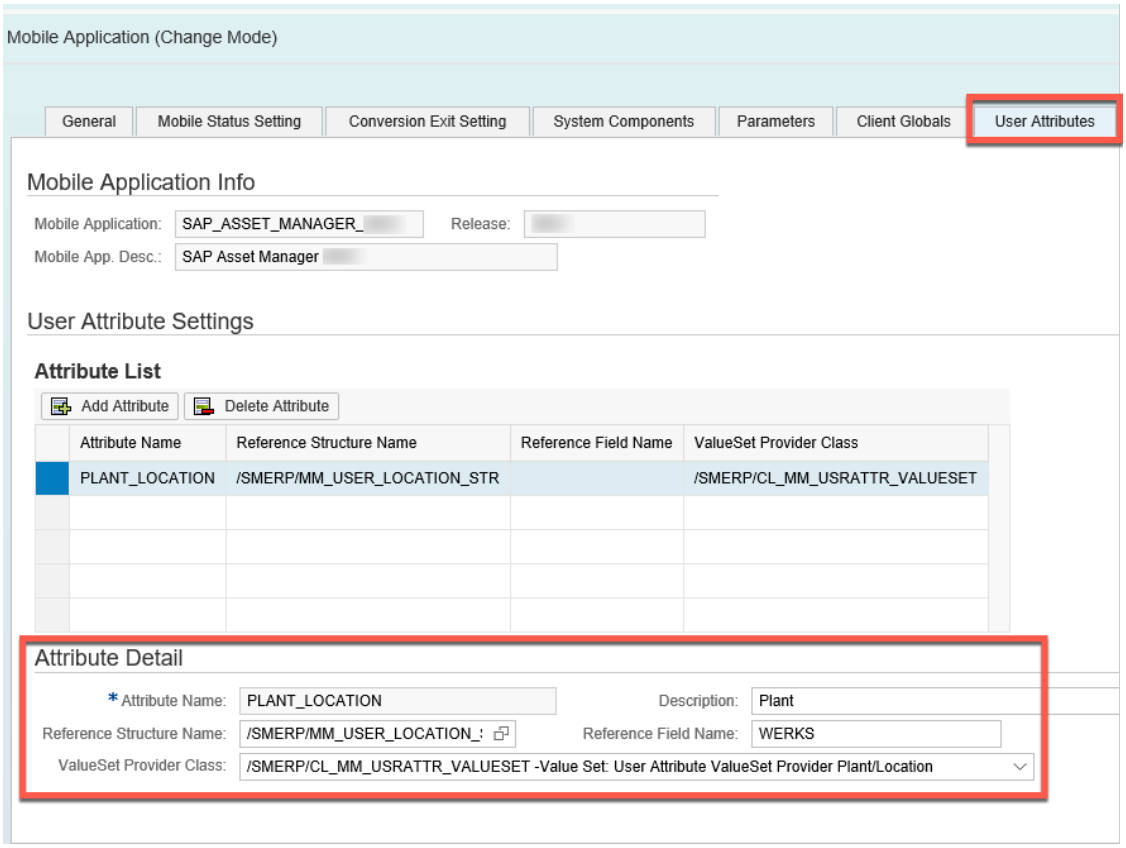
There are three core configuration steps to implement mobile user attributes:

1. Create the user attribute using the ConfigPanel [page 108]
2. Define and activate the new user attribute through the Admin Portal [page 109]
3. Define how to consume the data in the OMDO through the ConfigPanel [page 110]

> **Note**
>
> For more information about the ConfigPanel and Admin Portal, refer to the *Mobile Application Integration Framework documentation*:
>
> - MAIF Configuration Guide
> - MAIF Administrator Guide

Procedure

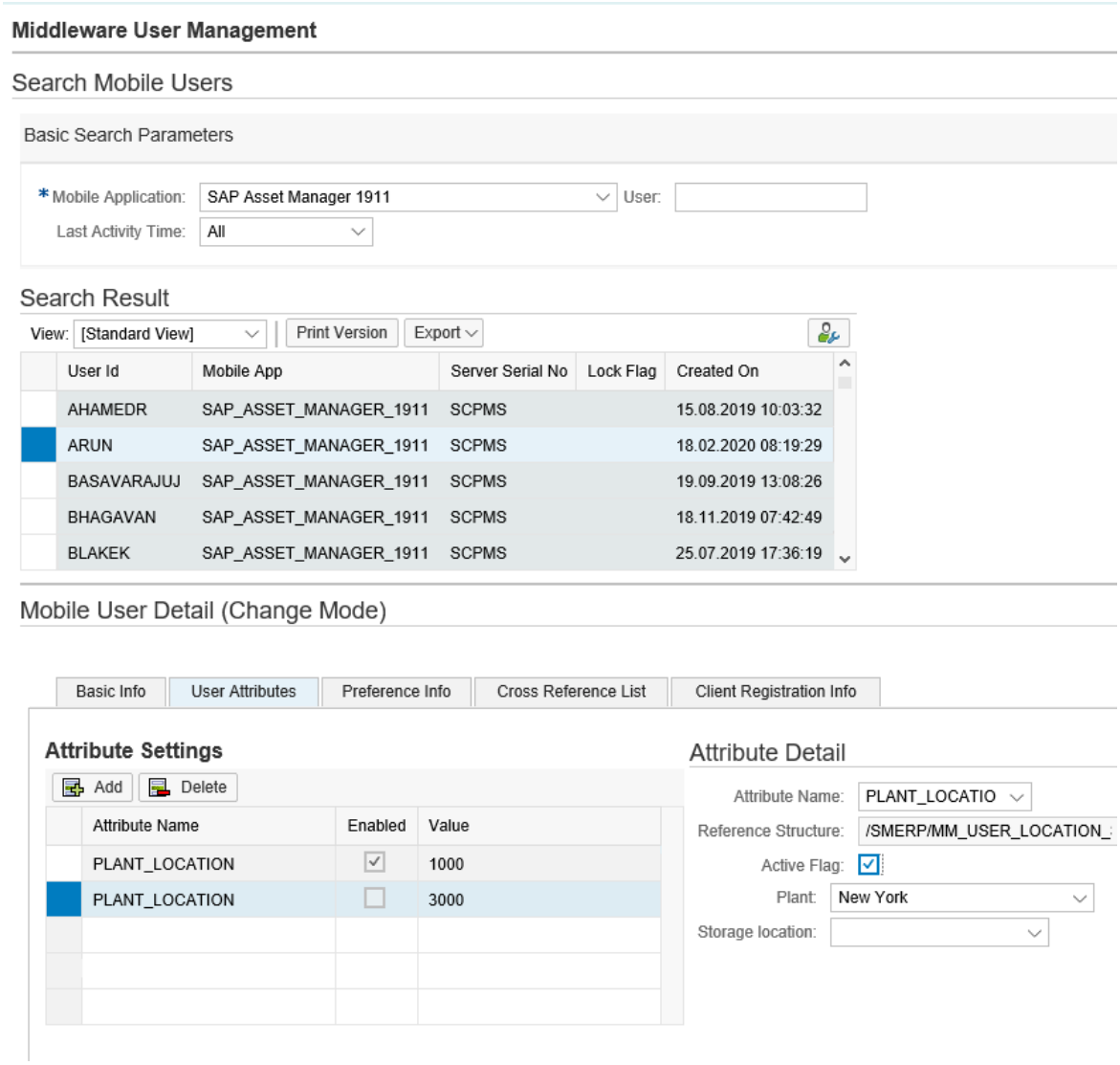
1. **Create the user attribute using the ConfigPanel:**
   a. From the home page of the ConfigPanel, navigate to *Mobile Application Settings* > *Mobile Application Configuration* and select the *User Attributes* tab.
   b. Click the *Change* button. Create your user attribute using the following fields. See the screenshot for an example:



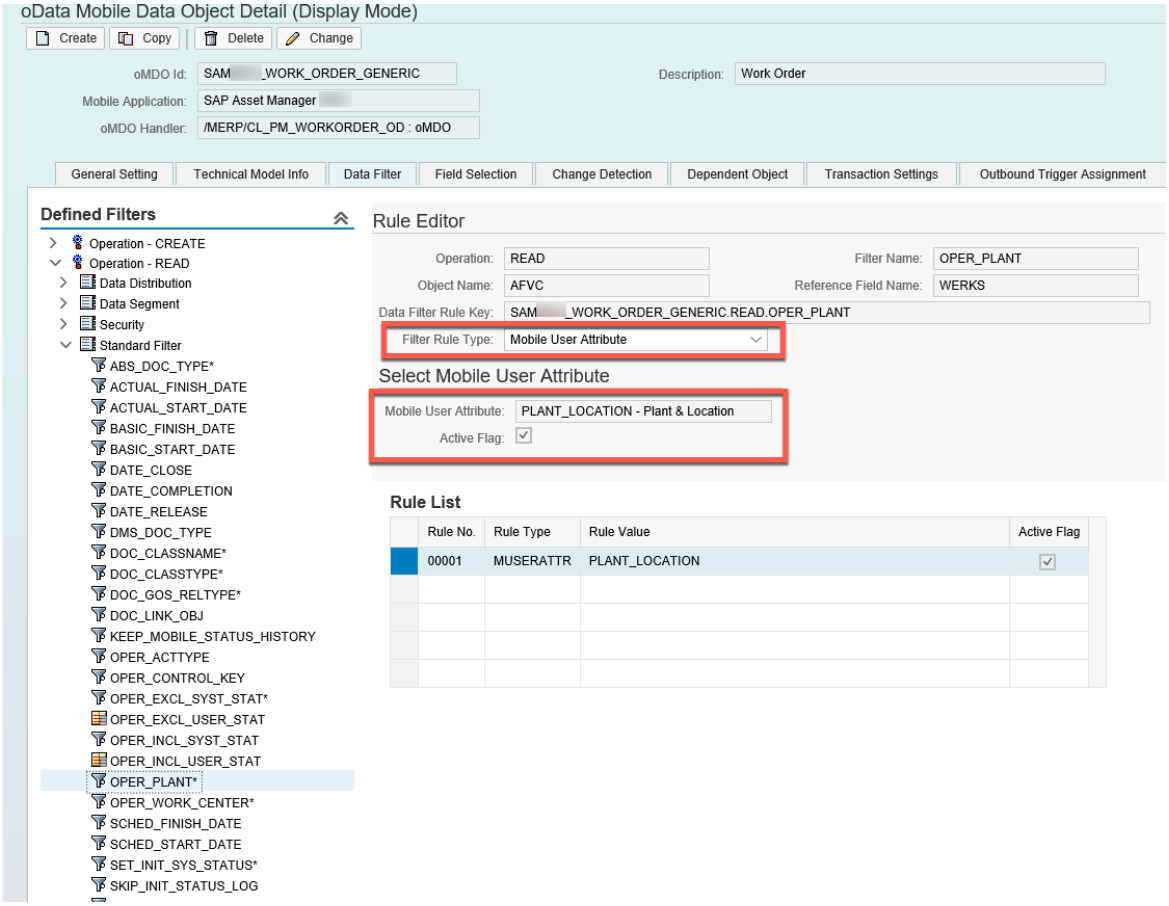
- `<Attribute Name>` and `<Description>`
- In the `<Reference Structure Name>` field, create or use an existing reference structure such as *PLANT* or *WORK CENTER*.
- The `<Reference Field Name>` is optional. Maintain if you are referring to a single field from the structure.
- Create a `<ValueSet Provider Class>` to populate possible values for your new user attribute. Use handler */SMERP/CL_MM_USRATTR_VALUESET* as a reference. Subclass from the base class */SMFND/CL_CORE_USRATTR_VS_BASE*.

c. Click *Save* to save your changes.

2. **Define and activate the new user attribute through the Admin Portal:**
   a. Access the Admin Portal from the *SAP GUI* using transaction code */n/SYCLO/ADMIN*.
   b. From the main page of the Admin Portal, navigate to *Administration* > *User Management* and select the *User Attributes* tab in the *Mobile User Detail* section of the screen.
   c. Select your desired mobile application from the dropdown. Search for available users connected to your selected application.
   d. Click the *User Attributes* tab. Then click the *Change* button.
   e. Click the *Add* button. Add the values created in *Step 1*. Repeat this step for all values you created. See the following screenshot for an example.



3. **Define how to consume the data in the OMDO through the ConfigPanel:**
   a. From the main page of the ConfigPanel, navigate to *OData Mobile Data Configuration* > *Data Filter tab*.
   b. Select the OMDO filter to which you're adding the new user attribute from the user attributes defined in the *Mobile Application Configuration* page in the ConfigPanel.
   c. Choose your filter from the *Defined Filters* list. Click *Change*.
   d. Assign your user attribute to the OMDO filter using a dynamic rule. The value is evaluated at runtime based on the runtime mobile user attribute of the user.
   e. Select *Mobile User Attribute* as the `<Filter Rule Type>`. See the following screenshot as an example.



2.5.1 Recommended Configuration for Multiple Plants and Work Centers

Altough SAP Service and Asset Manager technically supports comma-separated values for certain user parameters such as *WRK (Plant)*, *LAG (Storage Location)*, *AGR (Work Center)*, and *VAP (Main Work Center for maintenance tasks)*; this handler exists for backward compatibility and we **do not recommend** to use it for **multiple Plant**, **Storage Location**, or **Work Center** scenarios:

Persona	Feature Scenario
Maintenance Technician Field Service Technician	For the Vehicle Stock [page 560] feature, a *Plant* and *Storage Location* is used to identify the vehicle. Therefore, if you have multiple values, the feature **will not work**.
Maintenance Technician Field Service Technician	When adding a Part, the *Plant* and *Storage Location* are defaulted from *WRK* and *LAG* respectively; therefore, we **recommend to maintain only a single value in each**.

Persona	Feature Scenario
Inventory Clerk	The *Plant* is defaulted in all *ADD transactions* (adding items to Physical Inventory, Goods Receipt, etc); therefore, **only one Plant** is expected to be assigned to *WRK*. **Note** It is technically possible to use only the first *Plant* and *Storage Location* from a comma-separated *WRK*/*LAG* value. However, each time the value is needed, the client must execute additional rule logic, which increases loading time (for example, when refreshing pickers).
Maintenance Technician Inventory Clerk	All *Material*, *Batch*, *Valuation* and related pickers depend on the *Plant* value. Using comma-separated *Plants* triggers a chain of dependent updates and repeated rule execution, which negatively impacts performance. Therefore, we **do not recommend** using comma-separated values in *WRK* and *LAG*. Instead, use *ZWRK* and *ZLAG*, which **support multi-plant requirements** without affecting performance.

Summary of Recommended Configuration

Requirement	Parameter	Notes
Default Plant	*WRK* (standard parameter)	Must contain **one** Plant
Default Storage Location	*LAG* (standard parameter)	Must contain **one** Storage Location
Default Work Center	*AGR* and *VAP* (standard parameters)	Must contain **one** Work Center
Multi-Plant support	*ZWRK* (custom parameter)	Use OMDO filter logic for additional plants. For more information, see: • Working with oData MDO Filter Rules [page 146] • Configuring Mobile User Attributes [page 108]
Multi-Storage-Location support	*ZLAG* (custom parameter)	Avoid multi-value *LAG* for correctness and performance
Multi-Work-Center support	*ZAGR* and *ZVAP* (custom parameters)	*AGR* and *VAP* drives Assignment Types and OMDO filtering. For more information, see: • Work Order Assignment Type Options [page 150] • Work Order Distribution Rules [page 122]

> **Note**
>
> For more information, see:
>
> - User Parameter IDs [page 606]
> - Vehicle Stock Look Up Configuration [page 560]
> - Configuring Mobile User Attributes [page 108]
> - Configuration Prerequisites and Limitations - Inventory Clerk Persona [page 229]

2.6 Removal of Dependent Objects Based on Lead Objects

SAP Service and Asset Manager downloads data to mobile by using distributon mode. One of the supported distributon modes is Dependency mode. When Dependency mode is activated for oMDO, objects get qualified by the lead object. With this new feature introduced, when the last lead object is removed from device, the associated dependent object will also be removed.

Feature Description

See the following example and explanation for this feature:

Example: *Workorder 450000001* references *technical object 100000010* and the required dependency configurations are active in the mobile applicaton configuration.

- When the *workorder 450000001* qualifies for the mobile device, the workorder oMDO generates dependency queue to equipment oMDO. When the equipment oMDO performs key calculation, it qualifies the *technical object 100000010* for download.
- With this feature, when the life cycle of *workorder 450000001* is completed from the mobile device and the object gets removed from it, the *technical object 100000010* (which was downloaded as dependent object to *workorder 450000001*) will also be removed.

  > **Note**
  >
  > If the same dependent object is referenced by more than one lead objects (e.g., workorder and notification), the dependent object will be removed **only when the last lead object life cycle is completed and removed from mobile device**.

Supported Objects

Removal of dependent objects based on lead object removal is supported **only** for the following objects using standard handlers:

PM Objects in SAP Service and Asset Manager	Handlers
Notification	`/MERP/CL_PM_NOTIFICATION_OD`

PM Objects in SAP Service and Asset Manager	Handlers
Functional Location	`/MERP/CL_PM_FUNCLOC_OD`
Equipment	`/MERP/CL_PM_EQUIPMENT_OD`
Measuring Point	`/MERP/CL_PM_MEASURING_POINT_OD`
Measurement Document	`/MERP/CL_PM_MEASUREMENT_DOC_OD`

Standard Support for SAP Service and Asset Manager 2310

From SAP Service and Asset Manager 2310, all configurations required for this feature are available as standard, with the following exception:

- If the LITE version of oMDO is used for Equipment and/or Functional Location, the removal of dependent feature is deactivated. To switch it manually, refer to Support for LITE Version of Technical Objects [page 143].

If you want to use this feature on SAP Service and Asset Manager versions released **before 2310**, please consider the following:

- In addition to the existing standard configuration (and other notes it there are any), you must apply the following manual configuration changes:
  1. For configuration steps, see Section 3 (*High-Level Steps to Enable Support for SAP Service and Asset Manager 2305 or lower*) of the attached document in 3378889 SAP note.
  2. After the configuration changes are done, reset the application.

Design and Limitations

Please consider the following information and limitations regarding the feature:

- Any changes to the configuration and/or offline files require a reset and initial sync of the application.
- If entries in the user dependent list are modified or deleted manually, or other than the standard oMDO is used, the feature may not work as intended.
- This feature keeps track of objects that are downloaded **only via dependency queue**. If the same object has qualified via another distribution mode, this feature will not work.
- Changes of referenced dependent objects after the lead object was downloaded to the mobile device are treated as a new dependent object for the lead object.

> **Note**
>
> For example, the lead object references to dependent object "A" and it has already been downloaded to the mobile device. Then in the back end if the referenced dependent object is changed from "A" to "B", the delta sync will refresh the lead object with the newly referenced dependent object "B". However, the removal of dependent object "A" happens only on reset of mobile application. The removal of dependent object "B" happens when the lead object is removed from device.

- If the implementation involves client state keys and/or origin dependent keys format change (either through code and/or configuration), this feature may not work.
- Unless explicitly stated, no other objects support the dependency removal without a reset of the mobile application.
- With 2310, LITE version of oMDO is introduced for Equipment and Functional Location objects. While the regular oMDO for Equipment and Functional Location downloads the full-blown data for each qualified object that is associated with workorder or notification, the LITE version downloads only the minimum details of technical object (i.e., without any dependencies like documents, classification, characteristics, measuring points, measurement documents etc.).
    - As a result, when the LITE version of oMDO is active for Equipment and/or Functional Location as standard configuration for the mobile application or enabled via manual configuration, the removal of dependent object for Equipment and Functional Location will be deactivated.
        - If this feature was manually enabled for lower versions of SAP Service and Asset Manager and you want to deactivate it, refer to the 3368555 SAP note.
        - If you want to activate the removal of dependent object for Equipment and/or Functional Location, because the LITE version is not used in implementation, refer to Support for LITE Version of Technical Objects [page 143] to activate it.

3 Persona Configurations

3.1 Maintenance Technician Configuration

SAP Service and Asset Manager supports the following Maintenance Technician personas:

- **Maintenance Technician Professional**: Supports **all** Maintenance Technician features.
- **Maintenance Technician Standard**: Supports a reduced number of features compared to Professional persona.
- **Maintenance Technician External**:
  - Compared to Maintenance Technician Standard and Professional, it is a separate persona with limited functionality, created specifically for **external workers** within your organization.
  - You do not need to set up SAP User IDs for all your external workers.
  - This persona is required for the FSM Crowd Service Integration [page 411] (FSM Crowd users do not exist in the SAP back end system).
  - The Maintenance Technician **External** and Field Service Technician **External** personas **cannot** be used with other personas. Users may be assigned only one of these personas and must not be assigned any additional personas.

> **Note**
>
> - For more information about configuring features specific to the Maintenance Technician persona, see Features and Personas Configuration Matrix [page 9], where you can filter by the supported persona(s).
> - For more information about using Maintenance Technician features, see SAP Service and Asset Manager User Guide - Maintenance Persona.

General Configurations

Refer to the following documents for general Maintenance Technician configuration:

- Configuration Limitations - Maintenance Technician Persona [page 118]
- Configuring Personas [page 89]
- Mobile User Essential Authorizations
- Data Distribution Model Overview [page 118]
- Technical Objects Configuration [page 135]
- Enabling and Disabling Features Per User Through SAP Authorization [page 102]
- oData Channel Integration Settings Procedures [page 146]
- Mapping Work Orders to a STARTED Status - Overview [page 134]
- Configuring Mobile User Attributes [page 108]

- MAIF Configuration Guide - Application-agnostic configuration procedures and general information about configuring MAIF.
- Supported SAP Transaction Codes for SAP Service and Asset Manager [page 602]
- User Parameter IDs [page 606]

> **Note**
>
> Within data distribution models for a work order or notification, only work centers with cost center assignment types can be downloaded. For more information, refer to the Work Order Distribution Rules [page 122] and Notification Distribution Rules [page 129] topics.

FSM Integration Support Matrix

See the following table about the supported integration types for SAP Service and Asset Manager and Field Service Management:

Persona / Back End	Proaxia	CPI / SCI
Maintenance Technician [page 116]*	YES	YES
Field Service Technician with Customer Service [page 177]	YES	NO
Field Service Technician with SAP S/4HANA [page 205]	NO	YES

* Status changes are not propagated to Service Assignments for EAM phase model orders. The operation status is propagated to the *Activity* by the underlying integration.

> **Note**
>
> See the following documents for more information:
>
> - Integration of SAP Service and Asset Manager with Field Service Management Using the Proaxia Field Service Management Connector [page 180]
> - FSM SAP Cloud Integration [page 204]
> - EAM Phase Model Configuration - Overview [page 341]

3.1.1 Configuration Limitations - Maintenance Technician Persona

Limitations

Currently, the Maintenance Technician persona has the following limitations:

- In the case of configuring **multiple** *Plant*, *Storage Location* and *Work Center* parameters:
  - For the Vehicle Stock [page 560] feature, a *Plant* and *Storage Location* is used to identify the vehicle. Therefore, if you have multiple values, the feature **will not work**.
  - When adding a Part, the *Plant* and *Storage Location* are defaulted from *WRK* and *LAG* respectively; therefore, we **recommend to maintain only a single value in each**.
  - All *Material*, *Batch*, *Valuation* and related pickers depend on the *Plant* value. Using comma-separated *Plants* triggers a chain of dependent updates and repeated rule execution, which negatively impacts performance. Therefore, we **do not recommend** using comma-separated values in *WRK* and *LAG*. Instead, use *ZWRK* and *ZLAG*, which **support multi-plant requirements** without affecting performance.

> → Tip
>
> For more information, see Recommended Configuration for Multiple Plants and Work Centers [page 111].

- The Maintenance Technician **External** and Field Service Technician **External** personas **cannot** be used with other personas. Users may be assigned only one of these personas and must not be assigned any additional personas.

3.1.2 Data Distribution Model Overview

A data distribution model defines how and what back end data are downloaded to the mobile devices.

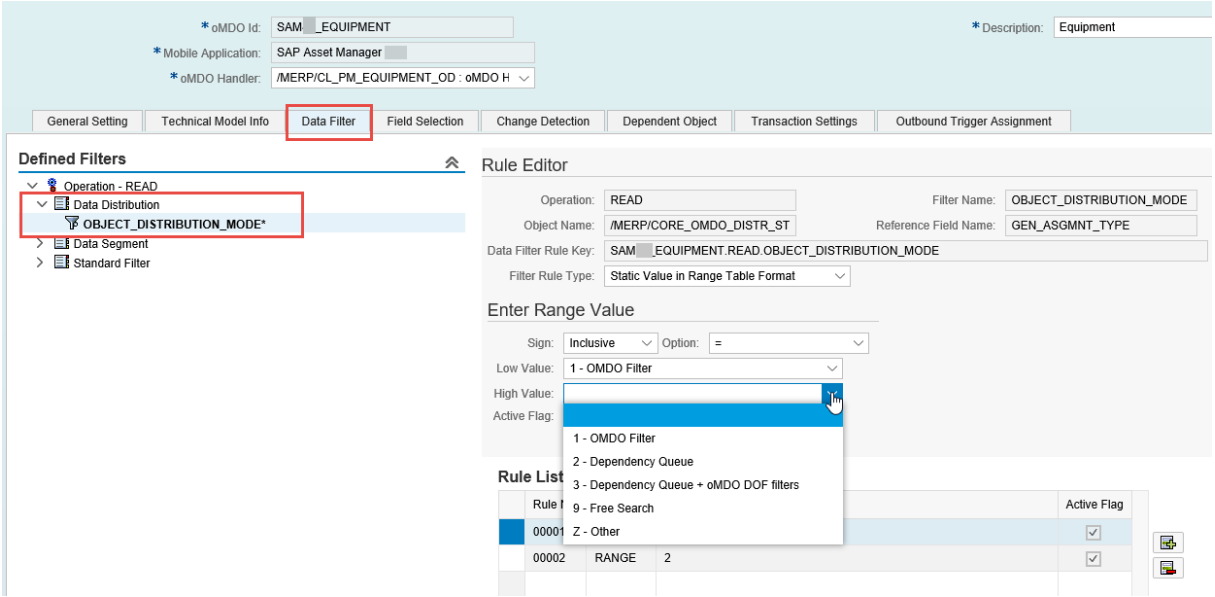
Data distribution models consider various factors when determining what backend data should be downloaded to the mobile client and to the mobile user. Some common criteria are:

- Relevant business processes and business rules
- User business roles in the organization
- Last mobile client synchronization time with the back-end system
- Backend data changes and the time of the changes
- Current state of data objects on the mobile device

For the initial synchronization from the mobile device to the back-end system, the first two bullet points are considered when determining what data should be downloaded to the mobile device and for the requesting user. For subsequent delta synchronizations from the mobile device to the back-end system, all bullet points are considered when determining what data should be downloaded to the mobile device for the requesting user.

The following data distribution models are supported for the SAP Service and Asset Manager application:

- **OMDO Filters**
  Object data collection entirely depends on *OMDO* filter conditions.
- **Dependency Queue**
  Object data collection entirely depends on Dependency Queue objects, and no filter conditions are applied for the fetch criteria.
- **Dependency Queue + OMDO DOF Filters**
  Object data collection is based on dependency queue objects, and the *OMDO DOF* filters are applied for the result set.
- **Other (Custom BAdI)**
  You can implement your own distribution logic using a BAdI.



By default, the SAP Service and Asset Manager application determines object data collection based on distribution model by using *OMDO* filters. In some cases, both *OMDO* filters and *Dependency Queue* are used depending on the business use case. You can choose the appropriate distribution model based on your specific business processes and requirements.

To change the data distribution model for a particular *OMDO* object, complete the steps below:

1. On the ConfigPanel home page, choose *OData Mobile Data Object Configuration*.
   Make sure you select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. From the *OData Mobile Data Object List* select the desired OMDO object, such as *SAMXXXX_EQUIPMENT*, and then click on the *Data Filter* tab.
3. Expand the *Defined Filters* list under *Operation - READ* > *Data Distribution* > *OBJECT_DISTRIBUTION_MODE*. Choose the *Change* button from the menu.
4. Set the distribution model.
5. Save your changes.

3.1.2.1 Data Distribution by Assignment Types

By default, the SAP Service and Asset Manager application determines the assignment of work orders and notifications using the personnel number assignment at header level. However, implementation environments in different industries or business types may use a different assignment model from the default to determine the proper technician assignment for work orders and notifications. The SAP Service and Asset Manager application supports several assignment models; you only need to change the assignment type configuration for the specific model.

See Business Object Distribution by Assignment Model [page 149] for more details about assignment model distribution, and how to change assignment type for both work order and notification.

3.1.2.2 Common Filters for SAP Service and Asset Manager

The filters listed in the following table are common to all SAP Service and Asset Manager distribution rules. See the specific rules for details on filter requirements for those rules.

Common Filters: Back End Data Filter Matrix

Common Filters: Back End Data Filter Matrix

Filter Name	Type	Value	Comments
WO_ASSIGNMENT_TYPE	Data Distribution, Mandatory	See specific rule for value	Defines which distribution model is used
COMP_CODE	Data Distribution, Optional	Any	Restricts work order distribution based on the maintenance plant company code on the work order.
CO_AREA	Data Distribution, Optional	Any	Restricts work order distribution based on work order maintenance plant controlling area.
DATE_CLOSE	Standard Filter, Optional	Any	Restricts work order distribution based on date range within which work order has been closed.
DATE_COMPLETION	Standard Filter, Optional	Any	Restricts work order distribution based on date range within which work order has been technically completed.
DATE_RELEASE	Standard Filter, Optional	Any	Restricts work order distribution based on date range within which work order has been released

Filter Name	Type	Value	Comments
ORDER_CATG	Data Distribution, Optional	See specific rule for value	Restricts work order distribution based on work order category. For maintenance orders, it should be value `30`.
ORDER_TYPE	Data Distribution, Optional	Any	Restricts work order distribution based on work order type.
ORDERID	Data Distribution, Optional	Any	Restricts work order distribution to a specific work order number.
OPER_ACTTYPE	Standard Filter, Optional	Any	Restricts work order distribution based on work order operation level activity type.
OPER_CONTROL_KEY	Standard Filter, Optional	Any	Restricts work order distribution based on the operation level control key on the work order.
OPER_EXCL_SYST_STAT	Standard Filter, Optional	Any	Restricts work order distribution by excluding work orders with operations that have a specified system status code.
OPER_EXCL_USER_STAT	Standard Filter, Optional	Any	Restricts work order distribution by excluding work orders with operations that have a specified user status code.
OPER_INCL_SYST_STAT	Standard Filter, Optional	Any	Restricts work order distribution by requiring work order operations with a specified system status code.
OPER_INCL_USER_STAT	Standard Filter, Optional	Any	Restricts work order distribution by requiring work order operations with a specified user status code.
OPER_PLANT	Standard Filter, Optional	Any	Restricts work order distribution based on the operation level plant of the work order.
PLANNER_GROUP	Data Distribution, Optional	Any	Restricts work order distribution based on the header planner group of the work order.
PLANNING_PLANT	Data Distribution, Optional	Any	Restricts work order distribution based on the work order header planning plant.
PLANT	Data Distribution, Optional	Any	Restricts work order distribution based on the header maintenance plant of the work order.
PM_PHASE	Data Distribution, Optional	Any	Restricts work order distribution based on the maintenance process phase of the work order.
WO_EXCL_SYST_STAT	Standard Filter, Optional	Any	Restricts work order distribution by excluding work orders header with a specified system status code.

Filter Name	Type	Value	Comments
WO_INCL_SYST_STAT	Standard Filter, Optional	Any	Restricts work order distribution by requiring a work order header with a specified system status code.
WO_EXCL_USER_STAT	Standard Filter, Optional	Any	Restricts work order distribution by excluding a work order header with a specified user status code.
WO_INCL_USER_STAT	Standard Filter, Optional	Any	Restricts work order distribution by requiring a work order header with a specified user status code.
MAIN_WORK_CENTER	Data Distribution, Optional	Any	Restricts work order distribution based on the work order header work center.
DOC_GOS_RELTYPE	Standard Filter, Optional	Data Segment, Optional	Determines whether the GOS attachment is supported based on a GOS relationship.
DMS_DOC_TYPE	Standard Filter, Optional	Data Segment, Optional	Determines whether the DMS attachment is supported based on the DMS document type.
DOC_LINK_OBJ	Standard Filter, Optional	Data Segment, Optional	Determines whether the DMS attachment is supported based on the linked SAP object.

3.1.2.3 Work Order Distribution Rules

The standard SAP Service and Asset Manager application work order distribution is controlled by the OMDO (OData mobile data object) **SAMXXXX_WORK_ORDER_GENERIC** *READ* operation. It supports several data distribution models for the work order.

You can choose the appropriate distribution model based on your specific business processes and requirements.

3.1.2.3.1 Distribution by Work Order Header Person Responsible

Requirements

The following are requirements before configuring the distribution model for Distribution by Work Order Header Person Responsible:

- Mobile user has an employee number (personnel number) assigned in SAP
- Employee number is assigned to the work order header as the person responsible
- Work order has been released

- Work order has not been marked for deletion

Back End Data Filter Matrix

Filter Name	Type	Value	Comments
WO_ASSIGNMENT_TYPE	Data Distribution Mandatory	1	Defines which distribution model is used
ORDER_CATG	Data Distribution Optional	30	Restricts work order distribution based on work order category. For maintenance orders, it should be value `30`.

3.1.2.3.2 Distribution by Work Order Operation Person Responsible

Requirements

The following are requirements before configuring the distribution model for Distribution by Work Order Header Person Responsible:

- Mobile user (i.e., the technician) must have an employee number (personnel number) assigned in SAP
- Employee number is assigned to the work order operation as the person responsible
- Work order is released
- Work order is not marked for deletion

Back End Data Filter Matrix

Filter Name	Type	Value	Comments
WO_ASSIGNMENT_TYPE	Data Distribution Mandatory	2	Defines which distribution model is used
ORDER_CATG	Data Distribution Optional	30	Restricts work order distribution based on work order category. For maintenance orders, value should be *30*.

3.1.2.3.3 Distribution by Work Order Suboperation Person Responsible

Requirements

The following are requirements before configuring the distribution model for Distribution by Work Order Suboperation Person Responsible:

- Mobile user (i.e., the technician) must have an employee number (personnel number) assigned in SAP
- Employee number is assigned to the work order suboperation as the person responsible
- Work order is released
- Work order is not marked for deletion

Back End Data Filter Matrix

Filter Name	Type	Value	Comments
WO_ASSIGNMENT_TYPE	Data Distribution Mandatory	3	Defines which distribution model is used
ORDER_CATG	Data Distribution Optional	30	Restricts work order distribution based on work order category. For maintenance orders, value should be *30*.

3.1.2.3.4 Distribution by Capacity Requirement Person Responsible

Requirements

The following are requirements before configuring the distribution model for Distribution by Capacity Requirement Person Responsible:

- Mobile user (i.e., the technician) must have an employee number (personnel number) assigned in SAP
- Employee number is assigned to the work order capacity requirement split records as the person responsible
- Work order is released
- Work order is not marked for deletion

Back End Data Filter Matrix

Filter Name	Type	Value	Comments
WO_ASSIGNMENT_TYPE	Data Distribution Mandatory	4	Defines which distribution model is used
ORDER_CATG	Data Distribution Optional	30	Restricts work order distribution based on work order category. For maintenance orders, value should be *30*.

3.1.2.3.5 Distribution by Work Order Header Planner Group

Requirements

The following are requirements before configuring the distribution model for Distribution by Work Order Header Planner Group:

- Mobile user (i.e., the technician) has been assigned to the planner group based on the business
- Employee number is not required
- Planner group associated with the mobile user is assigned to the work order header
- Work order is released
- Work order is not marked for deletion

Back End Data Filter Matrix

Filter Name	Type	Value	Comments
WO_ASSIGNMENT_TYPE	Data Distribution Mandatory	5	Defines which distribution model is used
ORDER_CATG	Data Distribution Optional	30	Restricts work order distribution based on work order category. For maintenance orders, value should be *30*.

3.1.2.3.6 Distribution by Work Order Operation Work Center

Requirements

The following are requirements before configuring the distribution model for Distribution by Work Order Operation Work Center:

- Mobile user (i.e., the technician) has been associated with a work center in business
- Employee number is not required
- Work center associated with the mobile user is assigned to work order operation
- Work order has been released
- Work order has not been marked for deletion

> **Note**
>
> Within data distribution models for a work order or notification, only work centers with cost center assignment types can be downloaded.

Back End Data Filter Matrix

Filter Name	Type	Value	Comments
WO_ASSIGNMENT_TYPE	Data Distribution Mandatory	6	Defines which distribution model is used
ORDER_CATG	Data Distribution Optional	30	Restricts work order distribution based on work order category. For maintenance orders, value should be *30*.

3.1.2.3.7 Distribution by Work Order Header Business Partner

Requirements

The following are requirements before configuring the distribution model for Distribution by Work Order Header Business Partner:

- Predefined partner function is used in work order for work assignment
- Employee number is not required

- By default, the SAP user ID for the mobile user is used for data distribution by partner function
- Work order is released
- Work order is not marked for deletion

Back End Data Filter Matrix

Filter Name	Type	Value	Comments
WO_ASSIGNMENT_TYPE	Data Distribution Mandatory	7	Defines which distribution model is used
ORDER_CATG	Data Distribution Optional	30	Restricts work order distribution based on work order category. For maintenance orders, value should be *30*.

3.1.2.3.8 Distribution by Work Order Header Work Center

Requirements

The following are requirements before configuring the distribution model for Distribution by Work Order Header Work Center:

- Mobile user (i.e., technician) has been associated with a work center based on the business
- Employee number is not required
- Work center associated with the mobile user is assigned to the work order header
- Work order is released
- Work order is not marked for deletion

> **Note**
>
> Within data distribution models for a work order or notification, only work centers with cost center assignment types can be downloaded.

Back End Data Filter Matrix

Filter Name	Type	Value	Comments
WO_ASSIGNMENT_TYPE	Data Distribution Mandatory	8	Defines which distribution model is used
ORDER_CATG	Data Distribution Optional	30	Restricts work order distribution based on work order category. For maintenance orders, value should be *30*.

3.1.2.3.9 Distribution through Multi Resource Scheduling Engine

Requirements

The following are requirements before configuring the distribution through **Multi Resource Scheduling (MRS) Engine**:

- MRS has been implemented in the SAP system, and is responsible to schedule and update work order capacity records with the assigned technician
- Employee number is required for the mobile user
- Work order is released
- Work order is not marked for deletion

> ⓘ Note
>
> For more information about Multi Resource Scheduling, refer to the official product pages:
>
> - SAP Multiresource Scheduling
> - SAP Multiresource Scheduling, Option for SAP S/4HANA

Back End Data Filter Matrix

Filter Name	Type	Value	Comments
WO_ASSIGNMENT_TYPE	Data Distribution Mandatory	A	Defines which distribution model is used. For more information, see Work Order Assignment Type Options [page 150].

Filter Name	Type	Value	Comments
ORDER_CATG	Data Distribution Optional	30	Restricts work order distribution based on work order category. For maintenance orders, value should be *30*.

3.1.2.3.10 Distribution by Free Search

Requirements

The following are requirements before configuring the distribution model for Distribution by Free Search:

- Free search criteria for the work order. Used for an OnDemand work order look-up scenario.
- Employee number is not required
- Work order is released
- Work order is not marked for deletion

Back End Data Filter Matrix

Filter Name	Type	Value	Comments
WO_ASSIGNMENT_TYPE	Data Distribution Mandatory	7	Defines which distribution model is used
ORDER_CATG	Data Distribution Optional	30	Restricts work order distribution based on work order category. For maintenance orders, value should be *30*.

3.1.2.4 Notification Distribution Rules

The OMDO (OData mobile data object) **SAMXXXX_NOTIF_ASSIGNMENT_TYPE** *READ* operation controls the standard SAP Service and Asset Manager application notification distribution. It supports several data distribution models for the notification.

You can choose the appropriate distribution model based on your specific business processes and requirements.

Notification requests are assigned to the technician directly or assigned through the work center, planner group, or related business partner of the technician. The SAP Service and Asset Manager application supports these different assignment types while downloading notifications associated with the technician.

Valid assignment types are:

- **1 - Header Level Person Responsible:** Assign this notification to the HR personnel number of the technician through the notification header *Partner* section.
- **2 - Notification Task Level Personnel Number:** Assign this notification to the HR personnel number of the technician through individual *Task Personnel Number* field.
- **3 - Header Level Planner Group:** Assign this notification to the planner group associated with the technician through the header level *Planner Group* field.
- **4 - Header Level Business Partner:** Assign this notification to the business partner associated with the technician through header level *Partner Function Maintenance*. The business partner can be anyone related to the notification partner function and associated with the technician, such as user responsible, sold-to-party, or other party. If there is no MAM configuration set up for the user, the default configuration uses *VU-User Responsible* as the default partner function and the technician *SAP User ID* as the partner number.
- **5 - Header Level Work Center:** Assign this notification to the work center associated with the technician through the header level *Work Center* field.
- **D - Dependency Queue:** Enables the dependency queue from the work order. When active, all notifications associated with a work order are downloaded, as well as qualifying data based on additional distribution rules that are set.

Customers can choose the appropriate distribution model based on their specific business processes and requirements.

3.1.2.4.1 Distribution by Notification Header Person Responsible

Requirements

The following are requirements before configuring the distribution model for Distribution by Notification header Person Responsible:

- Technician has an employee number (personnel number) assigned in SAP
- Employee number is assigned to the notification header partner overview as the person responsible
- Notification is not marked for deletion

Back End Data Filter Matrix

Filter Name	Type	Value	Comments
NOTIF_ASSIGNMENT_TYPE	Data Distribution Mandatory	1	Defines which distribution model is used

3.1.2.4.2 Distribution by Notification Task Level Person Responsible

Requirements

The following are requirements before configuring the distribution model for Distribution by Notification task level Personal Responsible:

- Technician has an employee number (personnel number) assigned in SAP
- Employee number is assigned to the notification task *Person Responsible* field
- Notification is not marked for deletion

Back End Data Filter Matrix

Filter Name	Type	Value	Comments
NOTIF_ASSIGNMENT_TYPE	Data Distribution Mandatory	2	Defines which distribution model is used

3.1.2.4.3 Distribution by Notification Header Level Planner Group

Requirements

The following are requirements before configuring the distribution model for Distribution by Notification header level Planner Group:

- Technician is assigned to the planner group based on the business
- Employee number is not required
- Planner group associated with the mobile user is assigned to the notification header

- Notification is not marked for deletion

Back End Data Filter Matrix

Filter Name	Type	Value	Comments
NOTIF_ASSIGNMENT_TYPE	Data Distribution Mandatory	3	Defines which distribution model is used

3.1.2.4.4 Distribution by Notification Header Level Business Partner

Requirements

The following are requirements before configuring the distribution model for Distribution by Notification header level Business Partner:

- Business partner is assigned to the notification header partner overview
- The SAP user ID of the mobile user is used for data distribution by partner function using *User Responsible*
- Employee number is not required
- Notification is not marked for deletion

Back End Data Filter Matrix

Filter Name	Type	Value	Comments
NOTIF_ASSIGNMENT_TYPE	Data Distribution Mandatory	4	Defines which distribution model is used

3.1.2.4.5 Distribution by Notification Header Level Work Center

Requirements

The following are requirements before configuring the distribution model for Distribution by Notification header level Work Center:

- Technician is associated with a work center in business
- Employee number is not required
- Work center associated with the mobile user is assigned to the notification header
- Notification is not marked for deletion

> **Note**
>
> Within data distribution models for a work order or notification, only work centers with cost center assignment types can be downloaded.

Back End Data Filter Matrix

Filter Name	Type	Value	Comments
NOTIF_ASSIGNMENT_TYPE	Data Distribution Mandatory	5	Defines which distribution model is used

3.1.2.4.6 Distribution by Free Search - Notifications

Requirements

The following are requirements before configuring the distribution model for Distribution by Free Search:

- Free search for notification used for an on-demand notification look-up scenario
- Employee number is not required
- Notification is not marked for deletion

Back End Data Filter Matrix

Filter Name	Type	Value	Comments
NOTIF_ASSIGNMENT_TYPE	Data Distribution Mandatory	9	Defines which distribution model is used

3.1.3 Mapping Work Orders to a STARTED Status - Overview

By default, the SAP Service and Asset Manager application maps the *STARTED* work order status on the client to the *REL* status in SAP Mobile Add-On.

In many implementations, a status of *MOBI* is used in SAP Mobile Add-On to indicate that the work order is started by a technician. The *MOBI* status cannot be modified on the back end.

You can map the mobile status to a different status within SAP Mobile Add-On by altering the mobile application configuration for SAP Service and Asset Manager and changing the system status technical code for the STARTED mobile status. After you change the system status technical code, updates to SAP Mobile Add-On made when a user starts a work order set the status in SAP Mobile Add-On to the MoBI status, matching the entered technical code.

The only modification to make is in the ConfigPanel, in the *Mobile Application Configuration* page, *Mobile Status Setting* tab. Change the mobile status for a started work order in the list of the mobile status options for SAP Service and Asset Manager, with the system status value of that same record altered to use the technical code of the desired status.

3.1.3.1 Changing the Mapping of a Mobile Status to STARTED

Prerequisites

Address the following before performing this procedure:

- Determine and note the technical code of the work order system status to which the mobile status STARTED will be mapped, as it is used in the procedure.
- The system status to which you are mapping the mobile status of STARTED in this procedure is configured as a work order status.
- The person performing this procedure has access to the ConfigPanel and permissions to change configuration settings of the elements within it.

Context

The following procedure describes the steps required to change a system status when a mobile STARTED status is mapped to it.

Procedure

1. Starting from the ConfigPanel home page, click the *Mobile Application Configuration* link. Then click the *Mobile Status Setting* tab.
2. Choose your desired mobile application from the list of *Defined Mobile Applications* in the left pane.

   The application level status settings display in the tab to the right. Information includes the *Mobile Status List*.
3. In the *Mobile Status List* table, find the *Object Type* of `<WORKORDER>` with a *Mobile Status* of `<STARTED>` and click the *Change* button.
4. Change the *System Status* value to the technical code of the system status to which the STARTED mobile status should be mapped. When done, click *Save*.

Results

After completion of the procedure, the STARTED mobile work order status is mapped to a different system status than the default REL status.

3.1.4 Technical Objects Configuration

Technical Objects are either Equipments or Functional Locations. In the *Config Panel*, you can configure the following related *App. Feature Ids*:

- *CA_TECH_OBJECT*: controls if Functional Locations and Equipments sections are visible in the mobile application.
- *CA_CREATE_TECH_OBJECT*: controls if the user is allowed to create a new Technical Object.
- *CA_EDIT_TECH_OBJECT*: controls if the user is allowed to edit Technical Objects, which are already downloaded to the mobile device.

> **Note**
>
> For more information about using Technical Objects, see:
>
> - Technical Objects Detail Screen
> - Working with Technical Objects
> - Equipment Overview
> - Functional Location Overview

Limitations

Notification and work order history for technical objects (Functional Locations and Equipment) are only downloaded if an order or notification is present on the device that has the technical object assigned. Therefore, technical objects downloaded by the 1-OMDO filter distribution mode don't have related orders or notifications downloaded. Only dependent technical objects have them.

Supported Personas

This feature is applicable for the following personas:

Maintenance Technician (Standard)
Maintenance Technician (Pro)
Field Service Technician (Standard)
Field Service Technician (Pro)
Safety Technician

Configuration

See the following configuration procedures for Technical Objects:

- Creating a Technical Object Template
- Configuring the Creation of Technical Objects from a Template [page 137]
  - App Customization with Additional Fields [page 138]
- Support for Editing Existing Technical Objects [page 142]
- Support for LITE Version of Technical Objects [page 143]

> **Note**
>
> From SAP Service and Asset Manager 2310, LITE version of Technical Objects is activated as standard configuration. As a result, Technical Objects associated with Work Orders or Notifications are downloaded with full-blown data and others have only minimum data (LITE version). If the LITE version of Technical Objects is not preferred for the implementation, you need to perform this configuration.

3.1.4.1 Configuring the Creation of Technical Objects from a Template

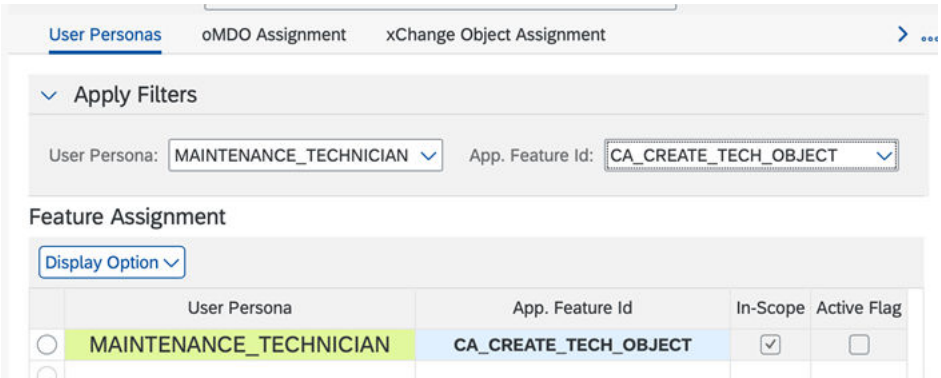
You can create Equipment and Functional Locations from the SAP Service and Asset Manager application in a similar way to executing transactions IE01 and IL01 from the SAP Service and Asset Manager GUI.

Context

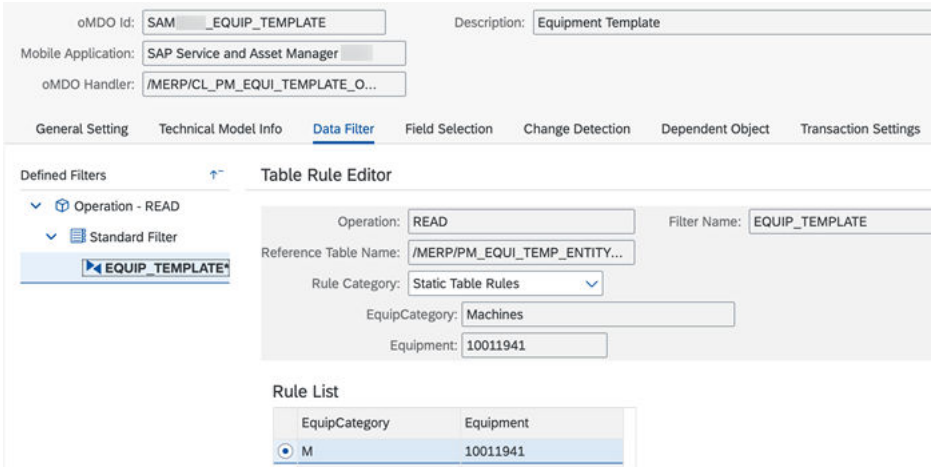
A template is required when you create equipment, but it's optional when you create a functional location. Any existing equipment or functional location can be used as a template. It's possible to copy the classifications, measuring points, business partners, documents, install location (equipment only), and notes from the template. The description, maintenance plant, start date, manufacturer, date of manufacturer, model number, serial number, and room are populated from the template object and you can overwrite them. It's possible to update equipment and functional location before syncing.

Procedure

1. To access the ConfigPanel using a direct transaction code shortcut, enter `/n/syclo/configpanel`.
2. Activate CA_CREATE_TECH_OBJECT for MAINTENANCE_TECHNICIAN Persona in the *Component Assignments*.

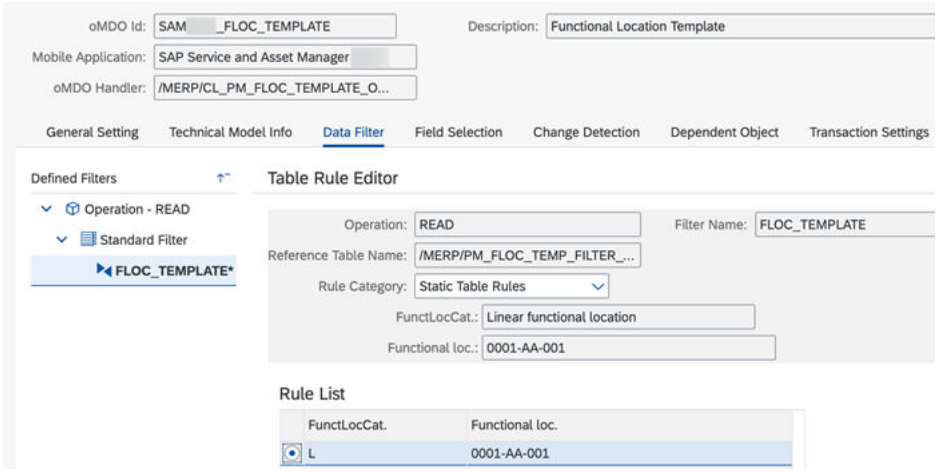


3. Add a rule to EQUIP_TEMPLATE filter in the SAM<version>_EQUIP_TEMPLATE oMDO in the oData Mobile Data Object Configuration.



The following step is optional:

4. Add a rule to FLOC_TEMPLATE filter in SAM<version>_FLOC_TEMPLATE oMDO in the oData Mobile Data Object Configuration.

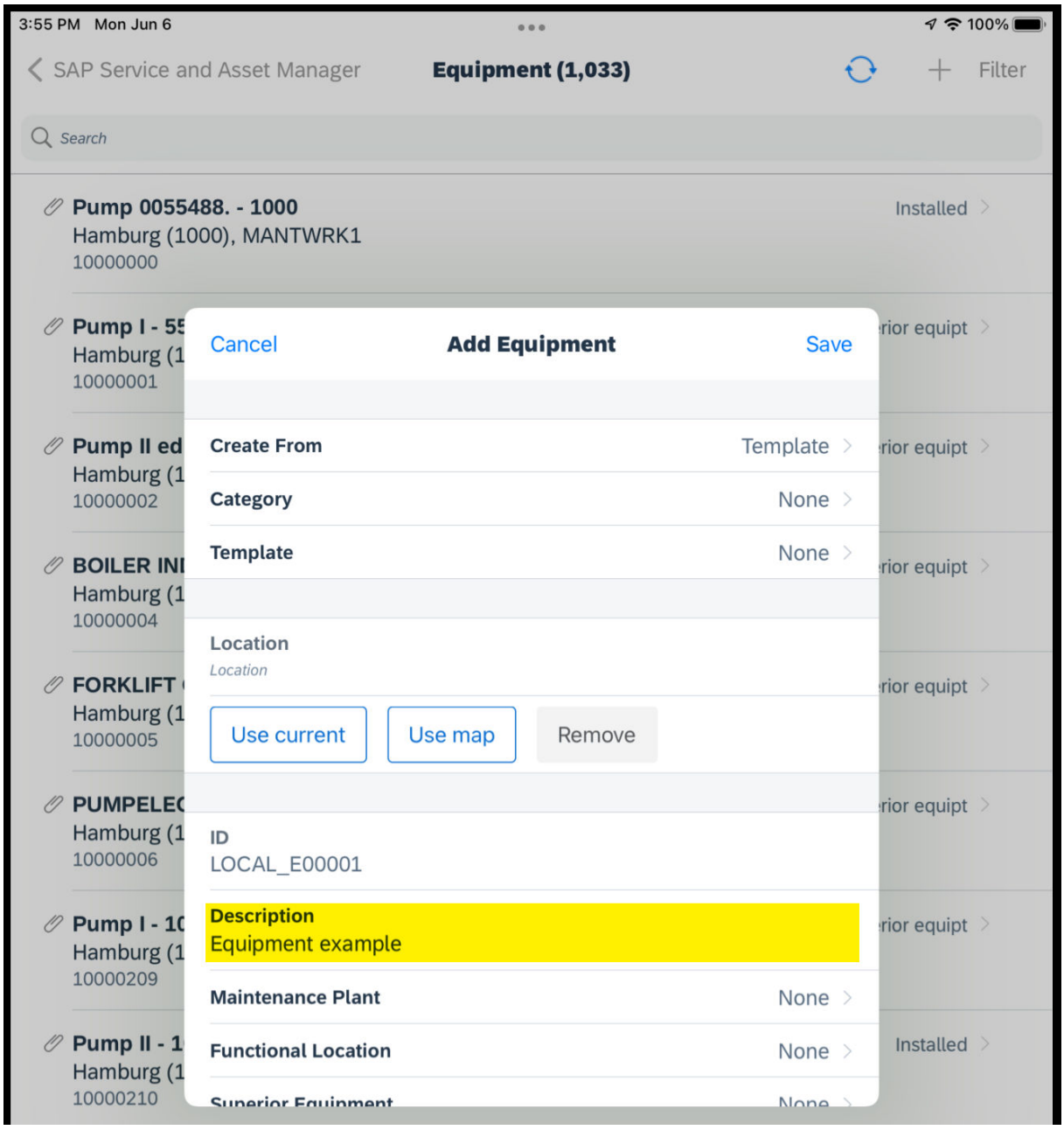


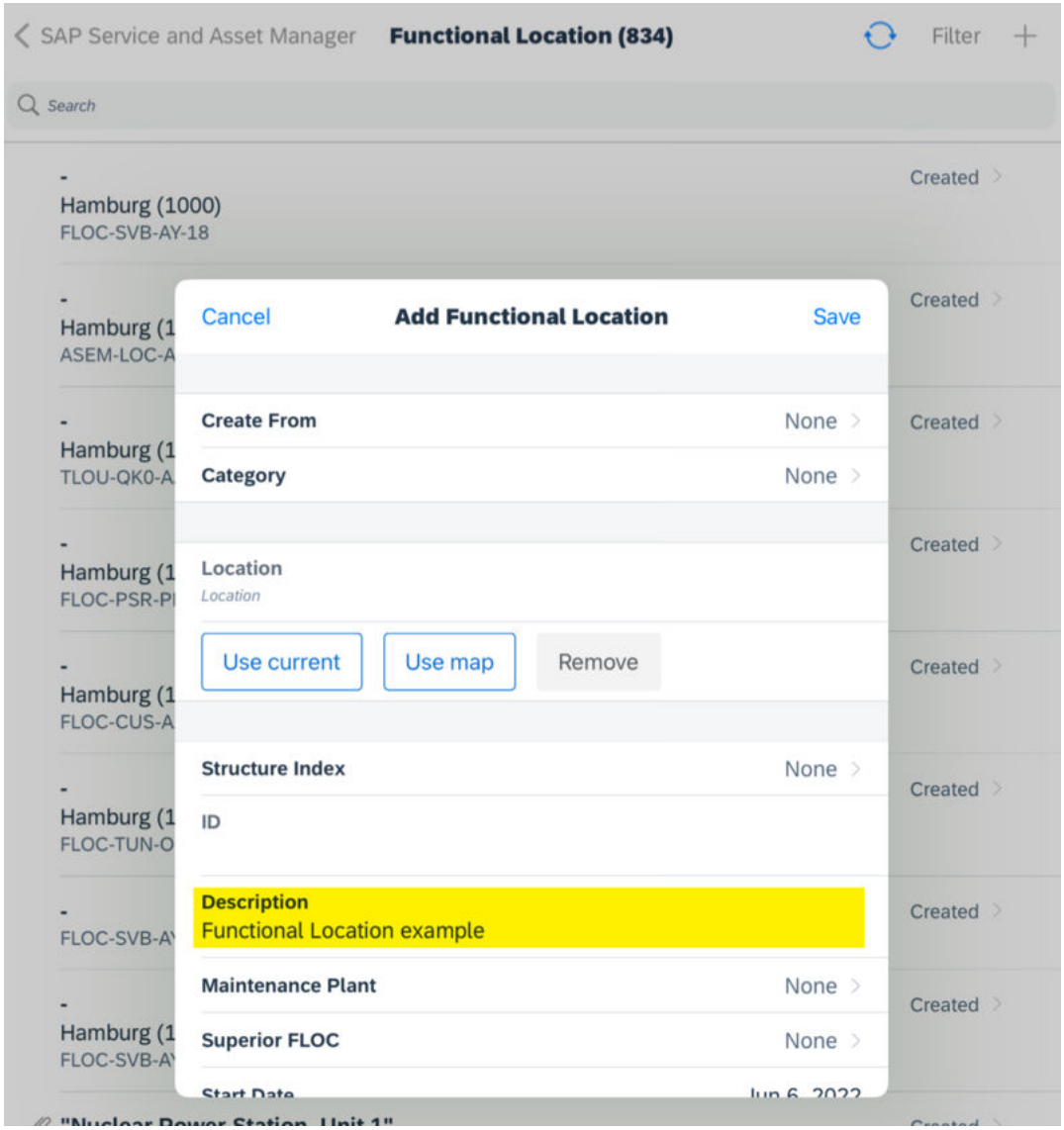
5. Save your changes.

3.1.4.1.1 App Customization with Additional Fields

The *PROPERTY_FLAG* filter in the technical objects, either *Equipment* or *Functional Location* oMDO contains the list of properties available to edit during the creation of a technical object. The properties, which are active

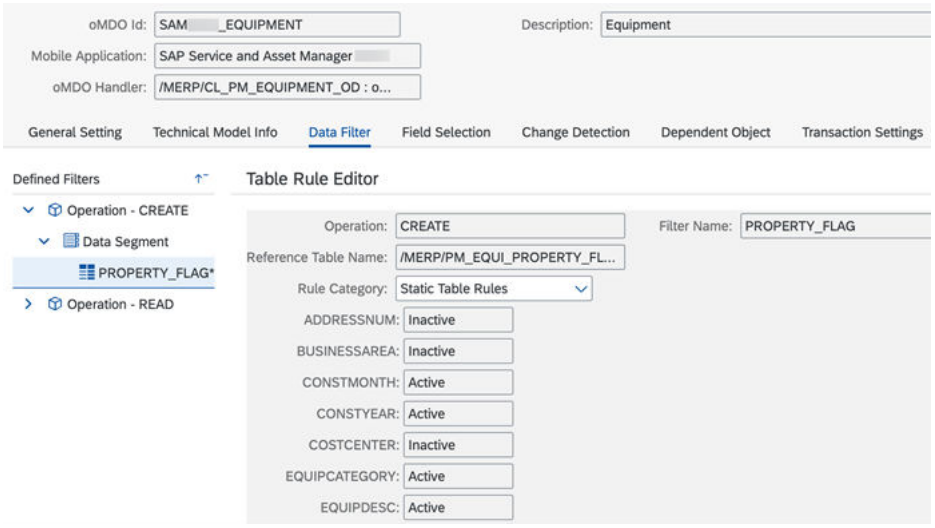
by default correspond to the default fields in the applications technical object create page. See the following examples:



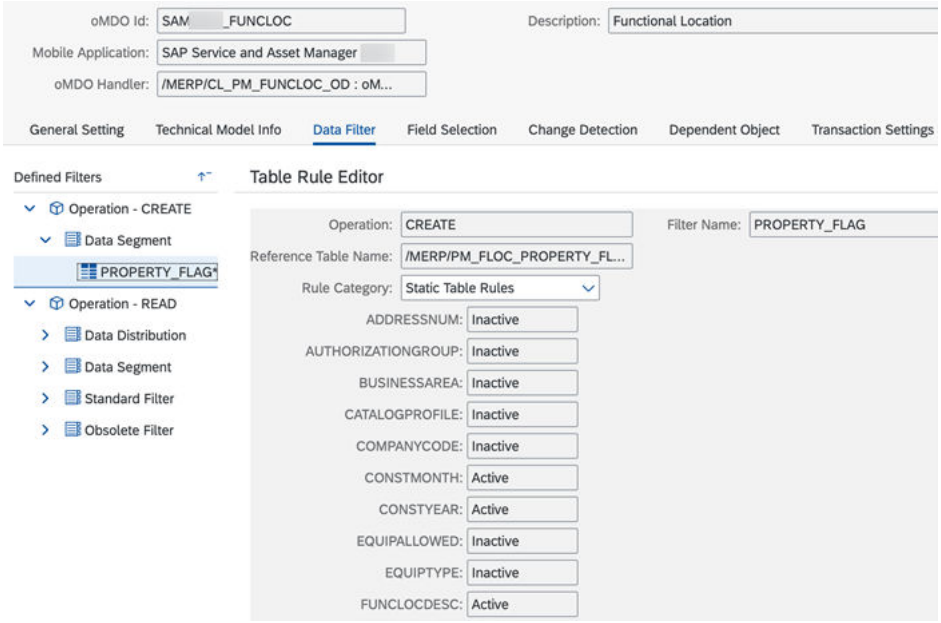


If a property is **inactive**, the value from the template or a previously created technical object is written to the newly created object. Updating the property to active in the filter does not change the create page of the application, a customization would be required in the application, too.

- *EQUIPDESC* corresponds to the *Description* field in the *Equipment* create page of the app.



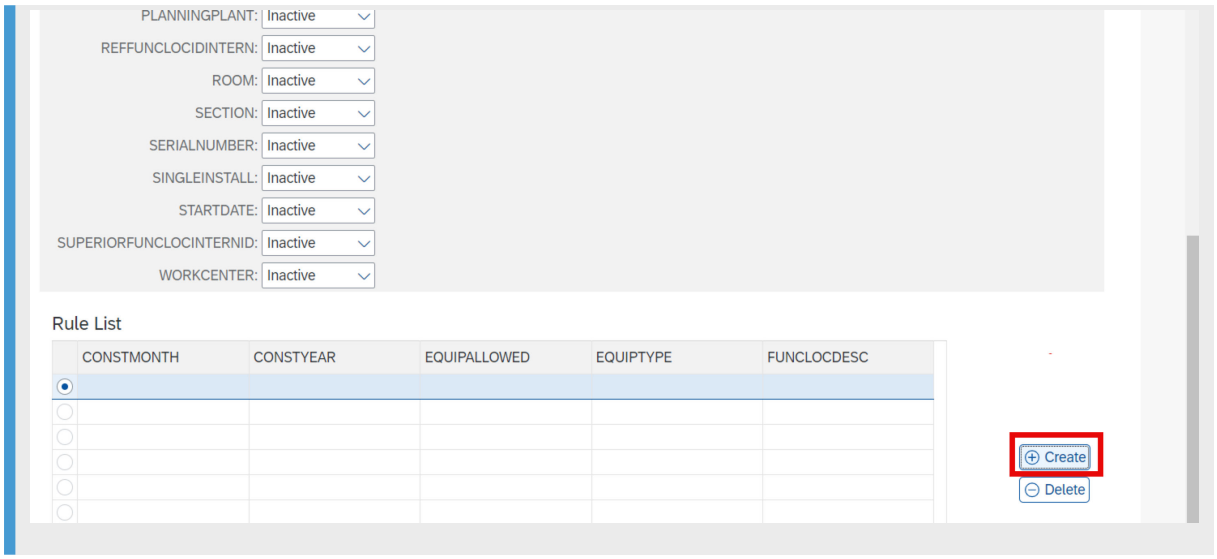
- *FUNCLOCDESC* corresponds to *Description* field in the *Functional Location* create page of the app.



Note

When clicking *Change*, the fields will still remain *inactive*. To edit the properties:

1. Click *Create* in the *Rule List* table below.
2. Edit the new rule with the properties according to your preference.



3.1.4.2 Support for Editing Existing Technical Objects

Context

For detailed information about Technical Objects, see the overview topic, Technical Objects Configuration [page 135].

From 2410 release, users can edit existing Equipments and Functional Locations downloaded to their mobile device, not only the ones they have created locally. Below procedure describes how to enable this feature.

Supported Personas

This feature is applicable for the following personas:

Maintenance Technician (Pro)
Field Service Technician (Pro)

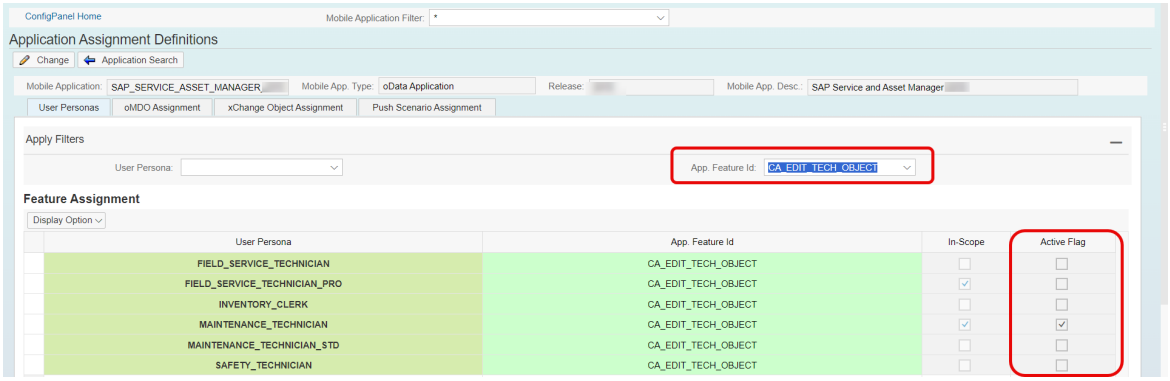
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **Enabling and disabling features**: refer to Configuring Features in *MAIF Configuration Guide*.

Procedure

1. On the Configuration Panel, go to *Component Assignments* and select your application from the list.
2. In the *App. Feature Id* dropdown, select *CA_EDIT_TECH_OBJECT*.
3. Enter *Change mode* and set the feature to *Active* for the personas you want to enable the feature.



4. Click *Save*.

3.1.4.3 Support for LITE Version of Technical Objects

From SAP Service and Asset Manager 2310, LITE version of technical objects is activated as standard configuration (i.e., LITE version of oMDO exists as standard for Equipment and Functional Location objects). As a result, technical objects associated with work orders or notifications are downloaded with full-blown data and others have only minimum data (LITE version). When new jobs qualifiy with LITE version of technical object, the application automatically downloads the full-blown data for the respective technical object along with the workorder or notification download.

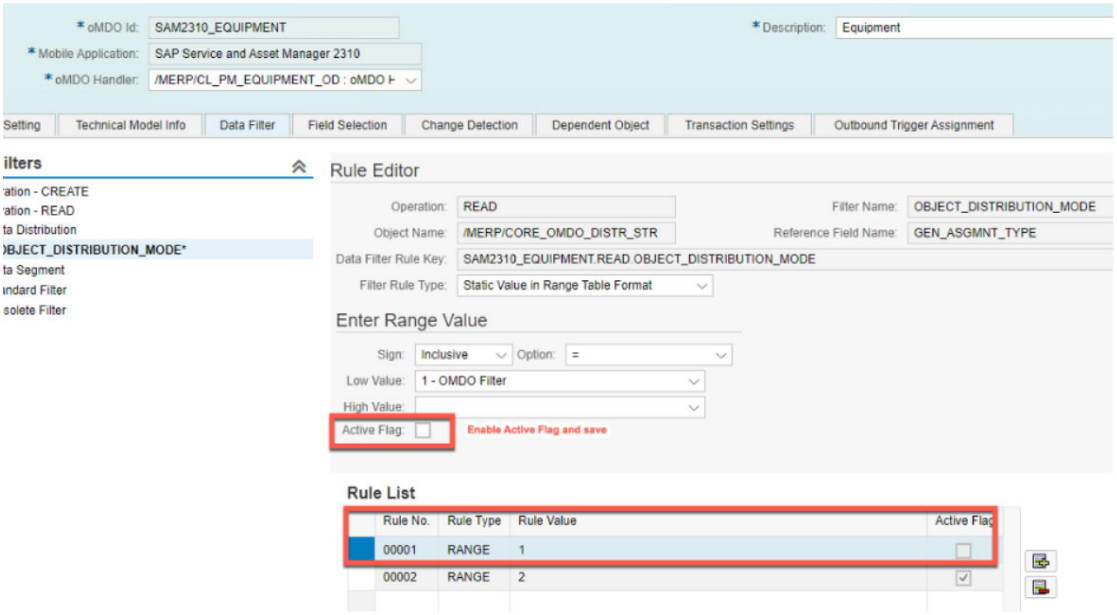
Context

If the LITE version of technical objects is not preferred for the implementation (i.e., implementation prefers full-blown data for all technical objects downloaded to the device), perform the following steps to switch:

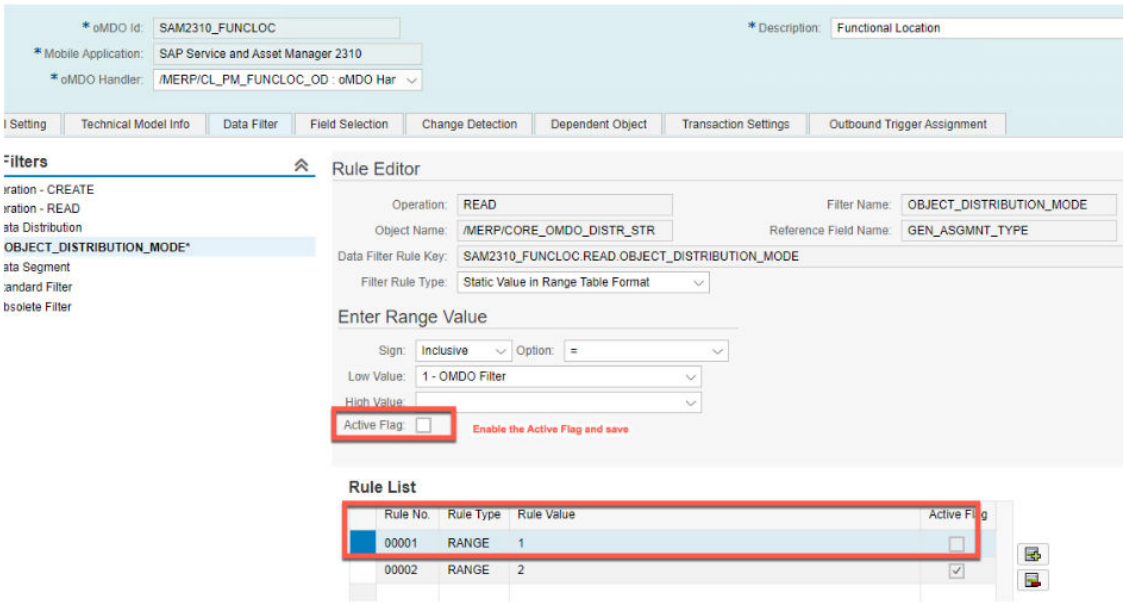
> **Note**
>
> Switching from LITE version to full-blown version is relevant only from 2310 version.

Procedure

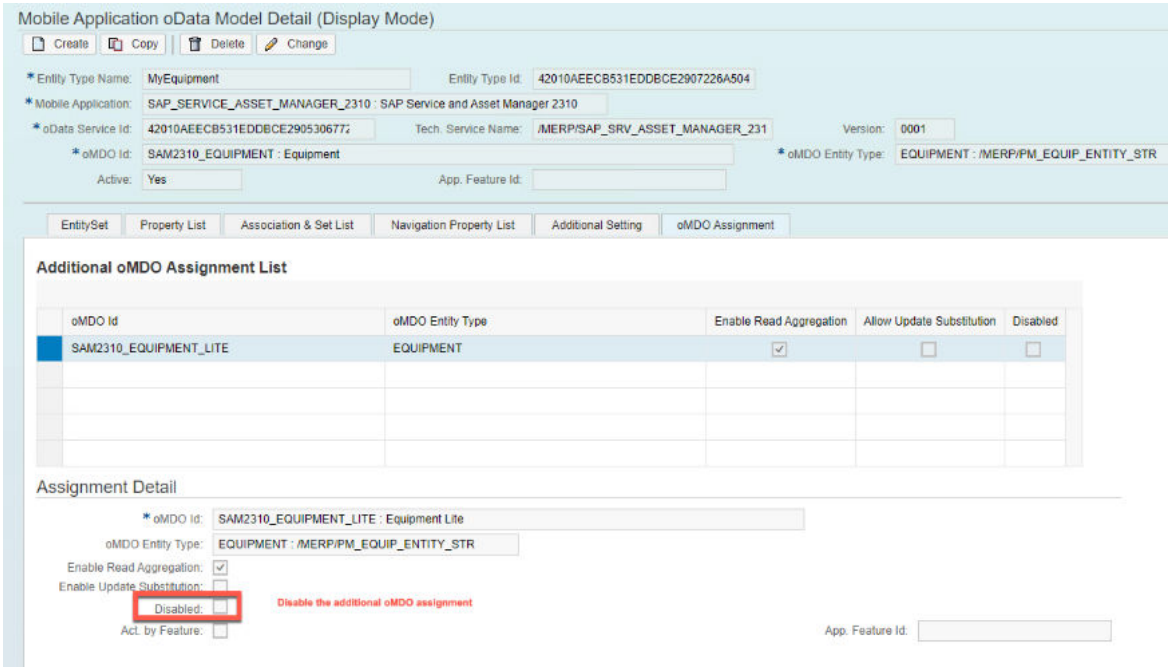
1. Disable additional oMDO assignment settings for the following oModels:
   - MyEquipment
   - MyEquipLongText
   - MyFunctionalLocation
   - MyFuncLocLongText
2. Enable oMDO data distribution filters for the following oMDOs:
   - *SAM2310_EQUIPMENT*



- *SAM2310_FUNCLOC*



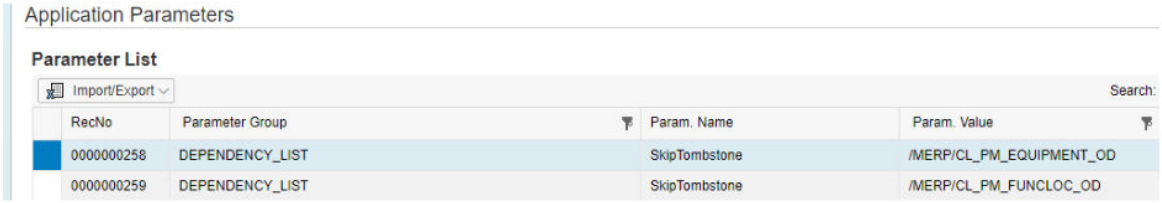
3. Disable the additional oMDO assignment for the *MyEquipment* entity type and click *Save*.



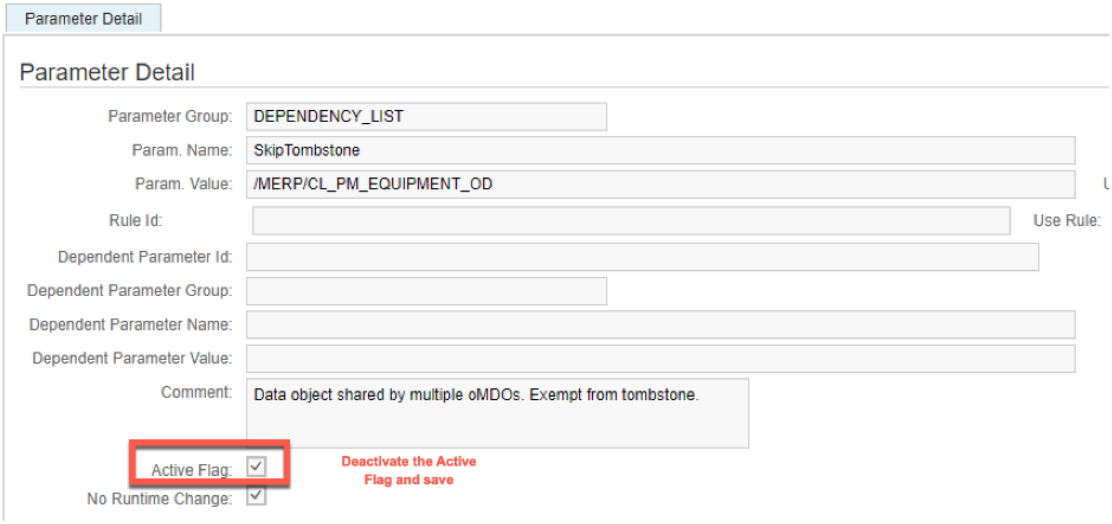
4. Repeat the previous step for all the entity types mentioned in Step 1 [page 143].

> ### Note
>
> If a similar configuration is enabled for other application versions, perform this step for those entity types as well.

5. In the respective mobile application parameter configuration, deactivate the following parameters:



- Deactivate the following parameter by unticking the *Active Flag* checkbox and save the changes. Repeat this step for all parameter values shown above.



6. When all changes are done, reset the mobile application and perform an initial sync.
7. Before productive migration, verify that all required data is downloaded and relevant functonalities work as intended.

3.1.5 OData Channel Integration Settings Procedures

3.1.5.1 Working with oData MDO Filter Rules

Filter rules specify a single field within the database tables from which data is retrieved. Filter rules also specify under which conditions records are included in the operation based on the value of the field.

Data filters are part of the configuration of an oMDO. If you make configuration changes to SAP Service and Asset Manager, you may need to adjust the rules for one or more of the oMDO filters.

Many of the filters in SAP Service and Asset Manager either do not contain active rules or contain rules that you can adjust. A filter only effects the synchronization behavior when it has one or more active rules.

The following procedure [page 146] instructs you on how to adjust a filter using the ConfigPanel.

3.1.5.1.1 Changing oData MDO Filter Rules

Many of the common configuration changes made for an SAP Service and Asset Manager implementation involve modifying or adding one or more filter rules in an oData MDO.

Context

In SAP S/4HANA, each user is assigned a role based profile with authorization permissions on viewable data and available activities. For example, a user working in one plant should not be able to view data for a different

plant. When business activities performed by a user are mobilized through the mobile application, the ability to extend the same restrictions to the mobile application is necessary. Data filter rules provide the function to restrict data access for mobile applications.

Use the following procedure to modify a data filter rule for an oMDO. The changes you make to the settings of a given rule vary depending on your mobile application implementation requirements. Subsequent procedures in the *Configuration Guide* refer to this procedure and provide detailed values and settings for filter rules involved in the specific change.

Procedure

1. Access the ConfigPanel. See Accessing the SAP Mobile Add-On for SAP Configuration Panel [page 608] for information.
2. From the ConfigPanel *Home* page, click the *oData Mobile Data Object Configuration* link.
3. At the top of the *oData Mobile Data Object Configuration* page display, in the *Mobile Application Filter* field, choose your mobile application from the dropdown menu. Choosing your mobile application is not a necessary step, but it eliminates objects that are not part of your mobile application from the object list.
4. Click the *Data Filter* tab.
5. Expand the *oData Mobile Data Object List* tree so you can see all of the oData mobile objects.
6. Select the oData mobile data object that requires filter modification from the list.

   The current rule filter settings are displayed in the *Rule Editor* section. All existing rules for the filter are displayed in the *Rule List* table.
7. To add a new rule, edit an existing rule, or delete a rule from the filter, click *Change*.

   Many of the fields in the rule editor become editable, and the buttons *Add Row* and *Delete Row* appear.
8. Set or modify any editable fields desired according to your mobile application needs. For a detailed description of all oData mobile data object fields, see the *OData Channel Integration Settings* topic and and the related subtopics in the section.
9. Set the *Active Flag* to `<True>` for each added or edited field before saving changes. Inactive filter rules have no effect on synchronization processing.
10. Click *Save* to apply your changes.

3.1.5.2 Work Order Distribution by Order Type Overview

In the default configuration of SAP Service and Asset Manager, work orders are distributed to technicians based on basic parameters. Your site may wish to distribute work orders to users based on the order type.

By default, all Plant Maintenance specific order types are included in the synchronization logic for the SAP Service and Asset Manager application.

In many environments, one or more order types are added to SAP Mobile Add-On specifically for work orders that are distributed to technicians. The added order types indicate that SAP Service and Asset Manager will

only download certain specified work orders. To support this distribution method, change the data filter rules of the OMDOs involved in work order synchronization. The OMDOs include:

- **SAMXXXX_ORDER_TYPE**
- **SAMXXXX_WORK_ORDER_GENERIC**

3.1.5.2.1 Configuring Work Order Distribution by Work Order Type

Creating rules based on work order types affects synchronization processing and work order downloads to the mobile devices of your users.

Prerequisites

Address the following before performing the procedure:

- The order types for work orders that are downloaded to technicians using the SAP Service and Asset Manager application are already determined.
- The person performing the procedure has access to the Config Panel and permissions to change settings.

Context

The following procedure modifies the synchronizing behavior of the SAP Service and Asset Manager application so only work orders with a given order type or types are downloaded to the client. In the procedure, you'll change the ORDER_TYPE filter in the OMDOs involved in work order synchronization. Specifically, you add rules to the filter in each OMDO to include only the desired work order types. You add a rule for each order type to include.

If you don't create a rule for a work order type, then those work order types are excluded from the work order download synchronization processing. If the work orders are excluded from the synchronization processing, then the work orders aren't present on the mobile clients of your users.

Procedure

1. From the Config Panel home page, click the *OData Mobile Data Object Configuration* link, then click the *Data Filter* tab. Be sure to have your desired mobile application chosen in the *Mobile Application Filter* field at the top of the page.
2. Expand the *OData Mobile Data Object by Mobile App* list on the left and click **SAMXXXX_ORDER_TYPE**.
3. Expand the *Standard Filter* in the *Defined Filters* pane, and click the *ORDER_TYPE* filter.
4. View the rule list for the filter, which is empty in the default configuration of SAP Service and Asset Manager. Click the *Change* button.

5. Create a rule for each order type included in the work order distribution to the SAP Service and Asset Manager technicians. The settings for the rule are as follows:
   - **DOF Rule Type:** Static Value in Range Format
   - **Sign:** Inclusive
   - **Option:** =
   - **Low Value:** The desired order type

   For more details on adding or editing filter rules, see Changing oData MDO Filter Rules [page 146].
6. *Save* your changes once you're finished.
7. Find and click the **SAMXXXX_WORK_ORDER_GENERIC** OData mobile data object on the list on the left.
8. Expand the *Operation - READ* > *Data Distribution* in the *Defined Filters* pane, and click the *ORDER_TYPE* filter.
9. View the rule list for the filter, which is empty in the default configuration of SAP Service and Asset Manager. Click the *Change* button.
10. Create a rule for each order type included in the work order distribution to the SAP Service and Asset Manager technicians, as you did with the previous OMDO filter. The settings for the rule are as follows:
    - **DOF Rule Type:** Static Value in Range Format
    - **Sign:** Inclusive
    - **Option:** =
    - **Low Value:** The desired order type
11. *Save* the changes.

Results

After you finish the procedure, work orders are downloaded by the SAP Service and Asset Manager application only if their work order type is set to a type for which a filter rule was created. Other work order types aren't retrieved by the application.

3.1.5.3 Business Object Distribution by Assignment Model

Business object distribution defines the data that needs to be downloaded to the mobile device based on the resource planning of technicians for different business objects, such as work order and notification. You can use this configuration to define which technicians has to complete which activities on the mobile device.

Implementation environments in different business industries or business types may use a different business object model from the default to determine the proper technician assignment for a business object such work order and notification.

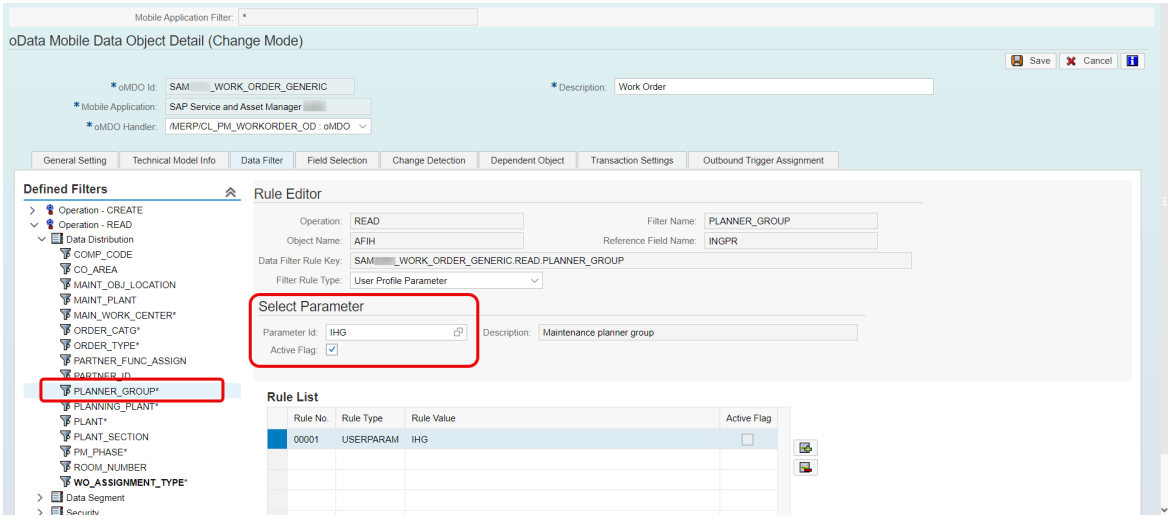
3.1.5.3.1 Work Order Assignment Type Options

By default, the SAP Service and Asset Manager application determines the assignment of a work order using the personnel number of the work order header. However, you can make minor configuration changes to support several work assignment models.

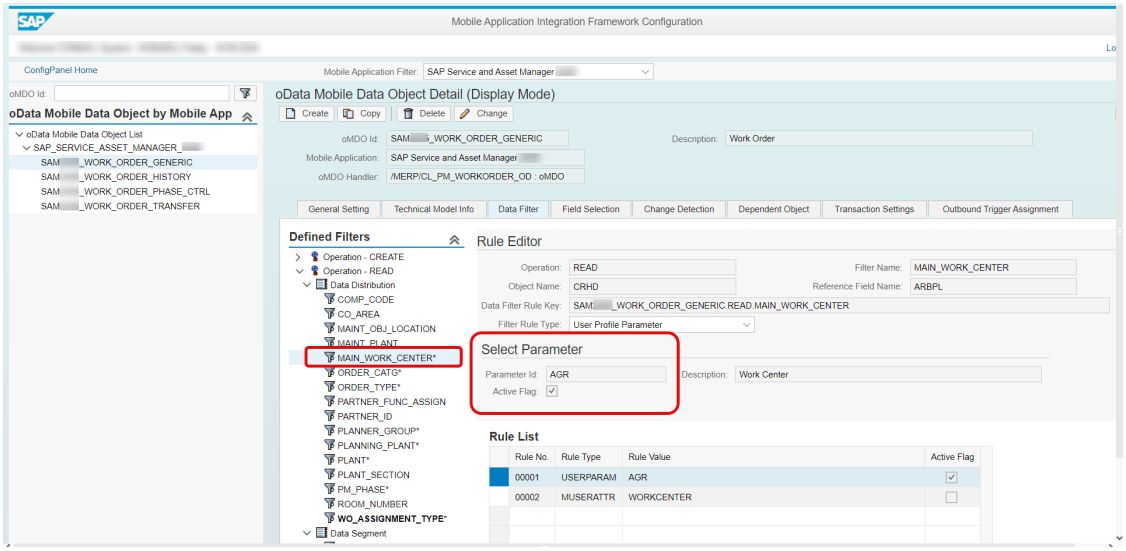
Supported configuration changes for assignment types

The following assignment types are supported with **minor** configuration changes:

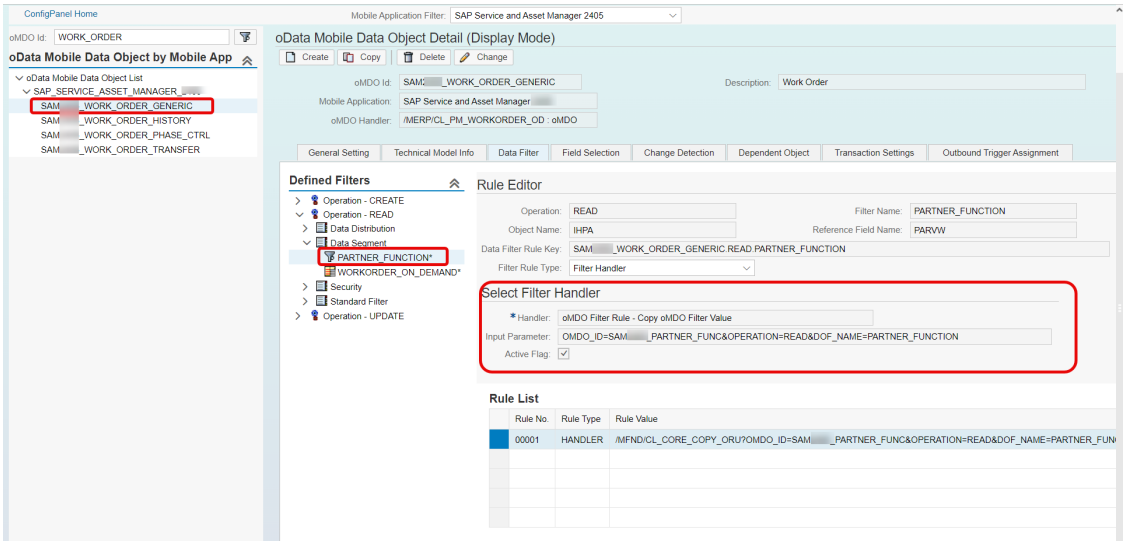
- **Assignment Type 1:** Header-level person responsible for the work order (default, no change required)
- **Assignment Type 2:** Operation-level personnel number of the work order
- **Assignment Type 3:** Sub-operation-level personnel number of the work order
- **Assignment Type 4:** Capacity requirement personnel assignment
- **Assignment Type 5*:** Header-level planner group. Prerequisites:
  - Mobile user must have the user parameter *IHG* set up in the user profile parameter (see screenshot about user parameters [page 152]).
  - You need to maintain the *PLANNER_GROUP* filter as shown in screenshot below:



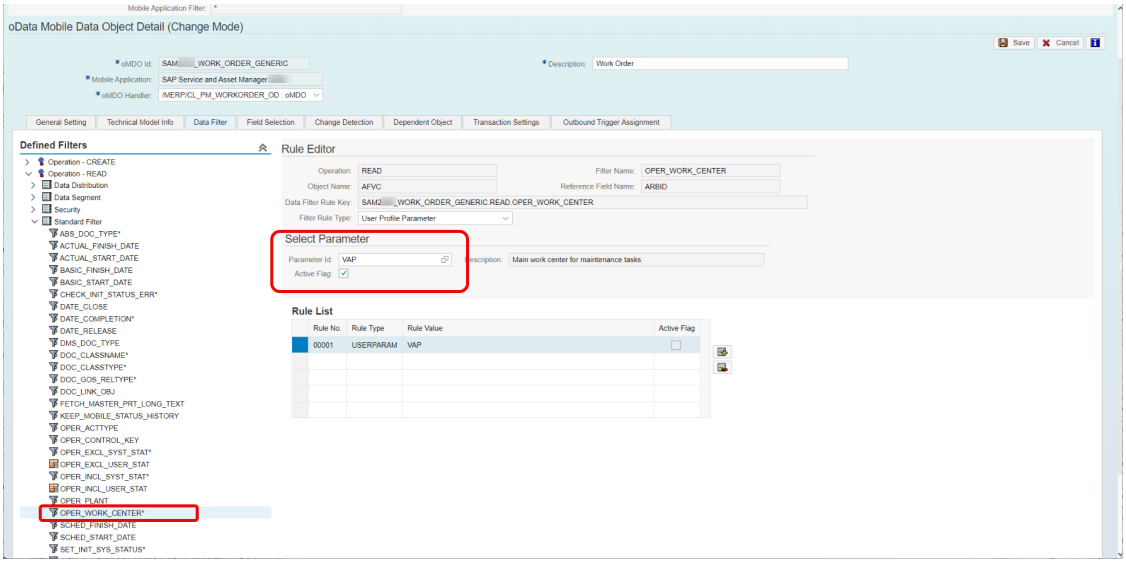
- **Assignment Type 6*:** Operation- or task-level work center. Prerequisites:
  - Mobile user must have the user parameter *AGR* set up in the user profile parameter (see screenshot about user parameters [page 152]).
  - You need to maintain the *MAIN_WORK_CENTER* filter as shown in screenshot below:



- **Assignment Type 7*:** Header-level business partner. Prerequisites:
  - Mobile user parameter needs to be set up (see screenshot about user parameters [page 152]).
  - In the work order *oData Mobile Data Object* configuration you need to define the partner function. Once the *SAM<version>_WORK_ORDER_GENERIC* filter is defined, assign a corresponding partner function for the work order object using the *PARTNER_FUNCTION* filter, as shown in screenshot below:



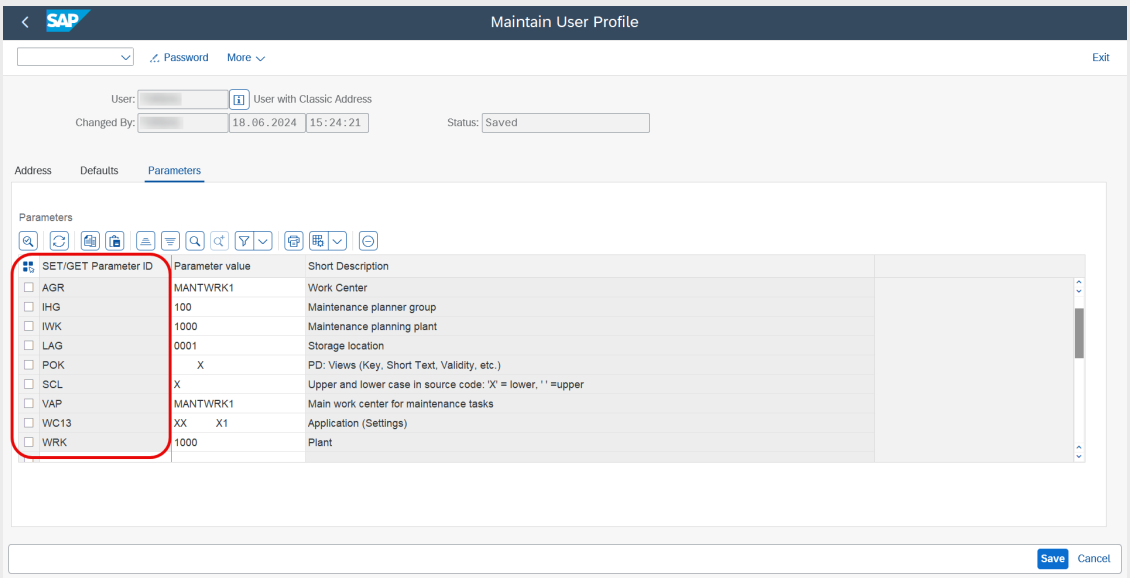
- **Assignment Type 8*:** Header-level of the work center. Prerequisites:
  - Mobile user must have the user parameter *VAP* set up in the user profile parameter (see screenshot about user parameters [page 152]).
  - You need to maintain the *OPER_WORK_CENTER* filter as shown in screenshot below:



- **Assignment Type A:** Multi resource scheduling (MRS). For more information, see Distribution through Multi Resource Scheduling Engine [page 128].
- **Assignment Type Z*:** Other (custom BAdI option)

Note

- ** These assignment types don't require a technician to have a personnel number.*
- The SAP HR module is needed for assignment types 1–4.
- For each assignment type you need to set up a specific user parameter. The user parameters you also need to maintain in *SAPGUI* > *Maintain User Profile* menu (see screenshot below).



- For some customers using Assignment Type 3 for work orders, viewing a list of suboperations is more important than viewing a list of operations. Work order headers are still visible. You can configure your preference using the ConfigPanel for SAP Service and Asset Manager.
- For assignment types 2 and 6, some customers prefer the ability to view all operations rather than all work orders. Work order headers are still visible. You can configure your preference using theConfigPanel for SAP Service and Asset Manager.

- Implementation environments in different business industries or business types may use a different business model from the default to determine the proper technician assignment for a work order.

Changing an assignment type used in a deployment

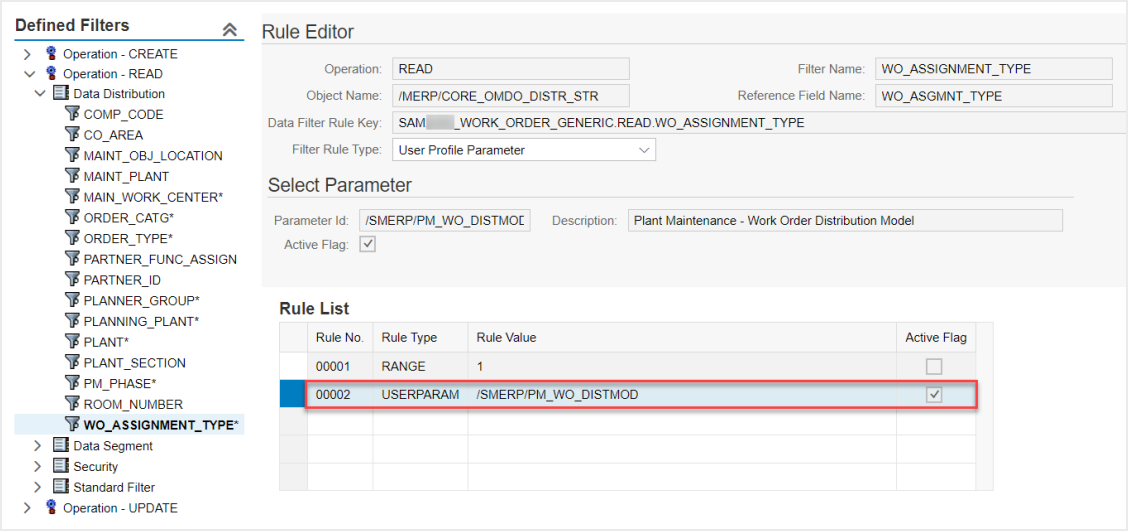
Perform the following steps to change the assignment type used in a deployment:

1. On the ConfigPanel home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. In the *OData Mobile Data Object List* select **SAMXXXX_WORK_ORDER_GENERIC**, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* > *Data Distribution* > and click *WO_ASSIGNMENT_TYPE*. Click the *Change* button.
4. Set *Low Value* with the desired assignment type as defined by the assignment type model.
5. *Save* your changes.

Note

Please note the following:

- If you are configuring an operation level assignment type, you must update the *OPER_EXCL_SYST_STAT* filter with the *I0009 - CNF:Confirmed* value. However, remove the value if you are configuring a header level assignment type.
- Under *Rule List*, you can set any number of Assignment Types for which the objects will be downloaded from the back end. However, on the client side **only one** of them will be considered by standard, namely the first one on top of the list, which has the Active Flag enabled (see image below). The business logic of this one Assignment Type will be applied to all downloaded objects.
  - Also note that in Supervisor Mode (supported Assignment Types: 6 and 8), you may not see the complete list of objects downloaded from the back end due to filtering. For more information, see Work Order Assignment Type Configuration [page 552].



3.1.5.3.2 Notification Assignment Options

By default, the SAP Service and Asset Manager application determines the assignment of a notification associated with the notification header. However, you can make minor configuration changes to support several other assignment models for the notification object.

The following assignment types are supported for the notification object:

> **Note**
>
> The SAP HR module is required for *Assignment Type 1* and *Assignment Type 2*.

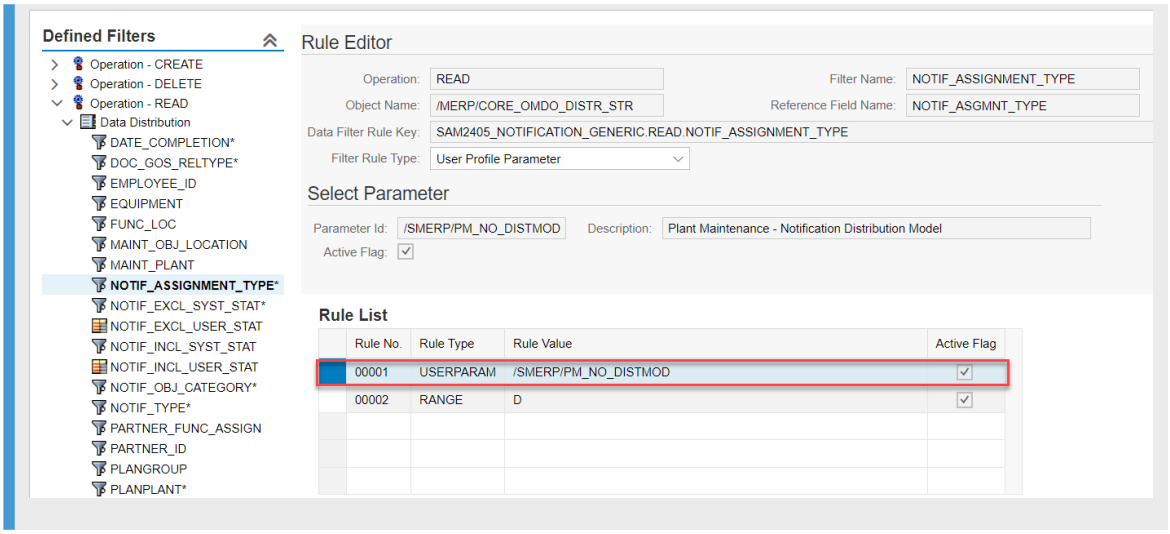
- **Assignment Type 1:** Header-level person responsible for the notification assignment (default, no change required)
- **Assignment Type 2:** Task-level personnel number of the notification assignment
- **Assignment Type 3:** Header-level planner group*
  Prerequisite: Mobile user has to have the user parameter *IHG* set up in the user profile parameter.
- **Assignment Type 4:** Header-level business partner*
- **Assignment Type 5:** Header-level of the work center*
  Prerequisite: Mobile user has to have the user parameter *AGR* set up in the user profile parameter.
- **Assignment Type D:** Dependent Queue
  By default, this assignment is based on the technician's notification assignment dependent collection*.
- **Assignment Type Z:** Other (custom BAdI option)*

** These assignment types don't require a technician to have a personnel number.*

Perform the following steps to change the assignment type used in a deployment:

1. On the ConfigPanel home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. In the *OData Mobile Data Object List* select **SAMXXXX_NOTIFICATION_GENERIC**, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* > *Data Distribution* and click *NOTIF_ASSIGNMENT_TYPE*. Click the *Change* button.
4. Set *Low Value* with the desired assignment type as defined by the assignment type model.
5. *Save* your changes.

   > **Note**
   >
   > Please note that under *Rule List*, you can set any number of Assignment Types for which the objects will be downloaded from the back end. However, on the client side **only one** of them will be considered by standard, namely the first one on top of the list, which has the Active Flag enabled (see image below). The business logic of this one Assignment Type will be applied to all downloaded objects.



3.1.5.4 Filtering Equipment Records by Equipment Status

A large set of records could affect performance on the SAP Asset Manager client. Therefore, you can employ more filtering based on the status of equipment.

By default, SAP Asset Manager filters records through a user-dependent rule based on the planning plant of the user.

To filter records on the status of equipment retrieved for the table stored on the SAP Asset Manager client, modify the **SAMXXXX_EQUIPMENT** OMDO. Specifically, in the following procedure, you will configure the *EQUI_INCL_SYS_STAT* filter with a rule that specifies which status or statuses to include. After you configure the rule, only the equipment records with the specified statuses are retrieved by the application for download to the clients.

A common equipment status is *INST*. However, the INST status is only one example of many options. You can configure other filters, either with this example, or in place of it.

For your given SAP Asset Manager implementation, thoroughly review the equipment data stored in the database before deciding which filter rules to configure. After your equipment review, create the appropriate filters within the **SAMXXXX_EQUIPMENT** OMDO.

3.1.5.4.1 Configuring an Equipment Status Filter for an Equipment Table

Prerequisites

Address the following items before performing the procedure:

- Know the status or statuses that you are filtering on for equipment synchronization, as they are used in the procedure

- Have access to the ConfigPanel and permissions to change configuration settings

Context

Use the following procedure to create a filter rule for the OMDO, **SAMXXXX_EQUIPMENT**. Specifically, you are adding a rule to the filter *EQUI_INCL_SYST_STAT*. After you add the filter rule, only the equipment records that match the ones configured in the rule are downloaded to the SAP Asset Manager client.

Procedure

1. Navigate to *ConfigPanel Home* > *OData Mobile Data Object Configuration*.
2. Select your application in the *Mobile Application Filter* field.

   Selecting an application filters the *OData Mobile Data Object by Mobile App* choices in the left panel with only OMDOs available in your application.
3. View the new OMDO copy by selecting it in the *OData Mobile Data Object by Mobile App list*.
4. Select the *Data Filter* tab.
5. In the *Defined Filters* list, click the *Operation - READ* > *Standard Filter* > *EQUI_INCL_USER_STAT* node.
6. Add a rule to the filter with the following configuration settings:
   - **Filter Rule Type:** Static Value in Range Format
   - **Sign:** Inclusive
   - **Option:** =
   - **Low Value:** Equipment status to filter on
   - **Active Flag:** Checked
7. Repeat the previous step to include additional statuses in the filter.
8. *Save* your changes.

Results

When you finish the procedure, the equipment records downloaded by the SAP Asset Manager application are filtered to only include records with the status or statuses configured in the filter rules.

Next Steps

You may need to filter equipment according to additional criteria. Test that the status filters created during this procedure are performing as expected before creating additional filters for the same data set. Regardless of additional changes, test the synchronization of the equipment data thoroughly after you modify the application.

3.1.5.5 Retrieving Additional Data for OData Mobile Data Objects

The default implementation of SAP Asset Manager includes the typical data values required by most users and at most implementation. However, it is a common requirement that additional values are retrieved and stored.

3.1.5.5.1 Adding New Retrievable Values for OData Mobile Data Objects

Prerequisites

Address the following before performing this procedure:

- Determine and note the field values as well as any table values you want to add, as well as which tables the desired fields reside in SAP Mobile Add-On
- You must have access to the ConfigPanel and permissions to change configuration settings within it

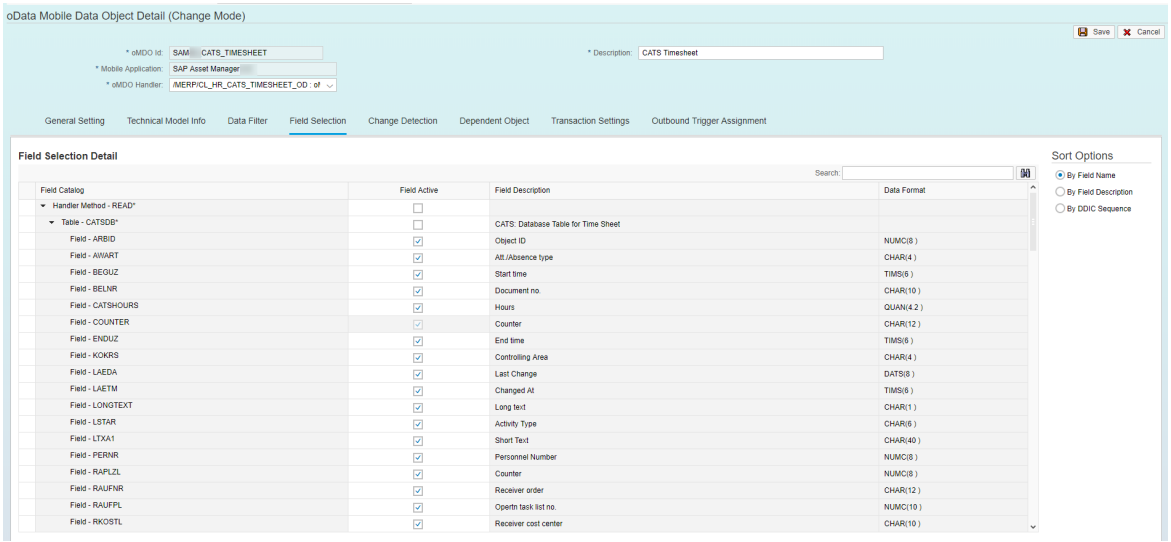
Context

Use the following procedure to add new fields to OData mobile data objects.

Procedure

1. Navigate to *ConfigPanel Home* > *OData Mobile Data Object Configuration*. Select the desired OMDO from the list on the left of the current configuration page.
2. Click the *Field Selection* tab, then click the *Change* button.

   The *Field Active* column is enabled.



3. In the *Field Selection Detail* pane, expand the *Handler Method* and the *Table* to search for the fields that you wish to activate. Fields that are already active are marked with a check in the checkbox.
4. Check the fields that you wish to activate and uncheck any active fields you wish to deactivate. *Save* your changes when finished.

Results

After completing the procedure, one or more new values are retrieved as part of the data for the object. The new values are displayed, edited, searched on, or used in other manners on the mobile client.

In the example screenshot in the procedure, the OData mobile data object used is **SAMXXXX_CATS_TIMESHEET**. To make other OMDO configuration changes to the object, navigate to the ConfigPanel home page, then click the *OData Model Configuration* link. On the left panel, find the corresponding *EntityType* to make any additional configuration changes. In this procedure example, the entity type is *CatsTimesheet*. See for more information.

3.1.5.6 Enabling or Disabling Follow-On Work Orders

Prerequisites

Ensure that business function *Enterprise Asset Management Part 7 (LOG_EAM_CI_7)* is activated in the back end. See Creating Follow-On Orders for more details.

Context

By default, follow-on Work Orders are enabled in a new installation. You can configure if a follow-on link exists or does not exist at the time of a new Work Order creation.

Procedure

1. Access the ConfigPanel through SAP Mobile Add-On.
2. Click the *OData Model Configuration* link from the home page of the ConfigPanel.
3. Select and expand the *OData Model Entity Type List* at the left of the pane. Select and expand your application from the list.
4. Select *MyWorkOrderHeader*. Navigate to the *Property List* tab and click the *Change* button.
   a. Delete the *ReferenceOrder* property by clicking the *Delete* button to disable.
   b. Enable the *ReferenceOrder* property by clicking the *Add Property* button and adding the following:
      - **Property Name:** ReferenceOrder

- **OMDO Field Name:** REFNR (select from a drop-down list)
- **Edm Type:** Edm.String (select from a drop-down list)
- **Max Length:** 12
- **Conversion Exit:** ALPHA

5. *Save* your changes.
6. Click the *OData Mobile Data Object Configuration* link from the home page of the ConfigPanel.
7. Choose your mobile application from the dropdown menu at the top of the *OData Mobile Data Object Configuration* page display, in the *Mobile Application Filter* field. Choosing your mobile application isn't a necessary step, but it eliminates objects that aren't part of your mobile application from the object list.
8. Click the *Field Selection* tab.
9. Expand the *OData Mobile Data Object List* tree so you can see all of the OData mobile objects.
10. Select *SAMXXXX_WORK_ORDER_GENERIC* from the list. Click the *Change* button.
11. Expand the *Table - AUFK* node, and then locate the *REFNR* field.
12. Enable or disable the field by selecting or deselecting the *Field Active* checkbox.
13. *Save* your changes.

3.2 Field Logistics Configuration

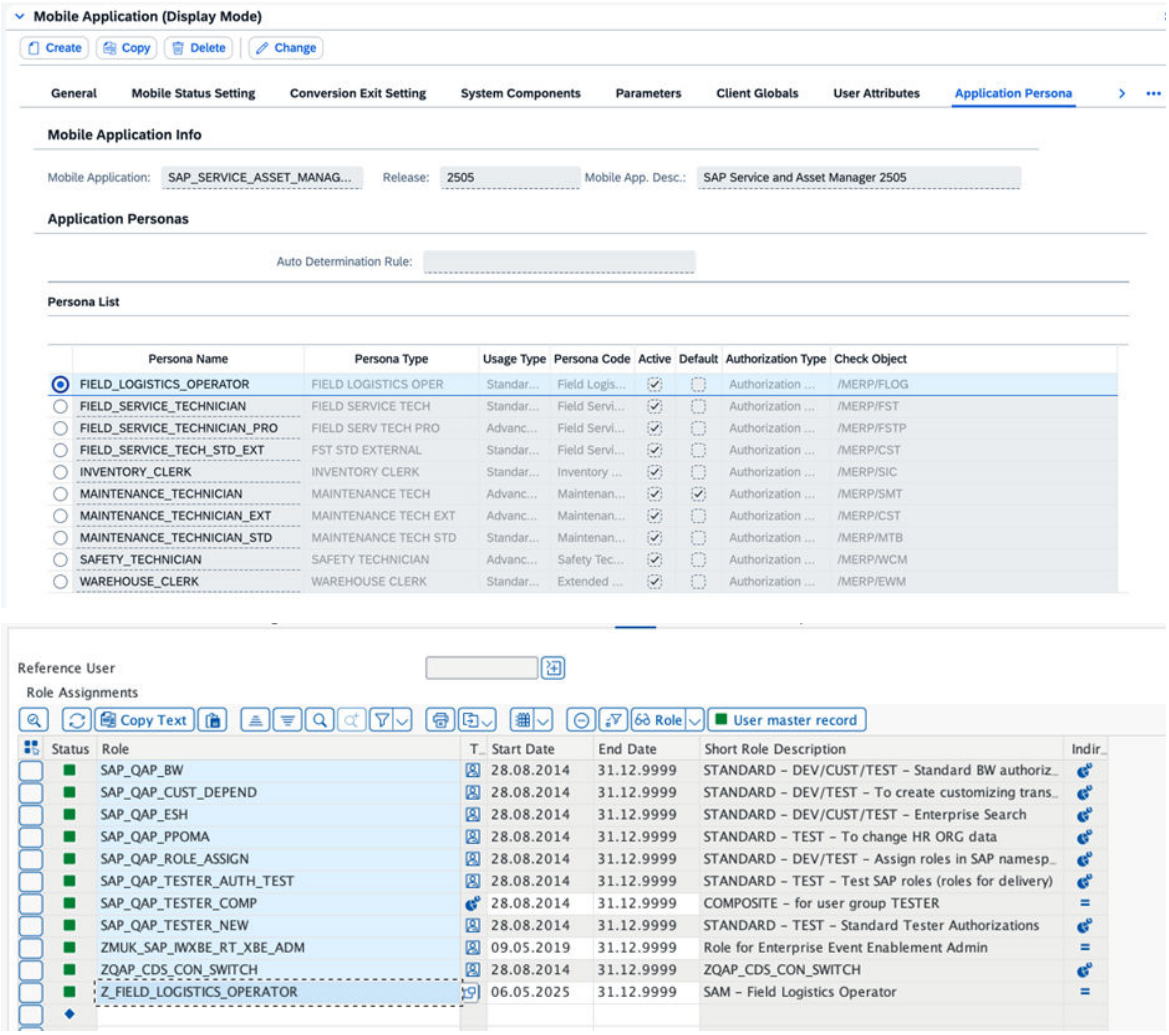
The *Field Logistics* persona allows you perform goods receiving for products, whether or not they have container assignments or handling units. This applies to both supplying (base) and offshore (remote) plants, with or without voyages. In this section of the guide, we cover the configuration options available for the *Field Logistics* persona.

> **Note**
>
> - For more information about using the *Field Logistics* features, see Field Logistics User Guide.
> - For general information about the *Field Logistics* persona, see Application Product Overview - Field Logistics Persona Overview.

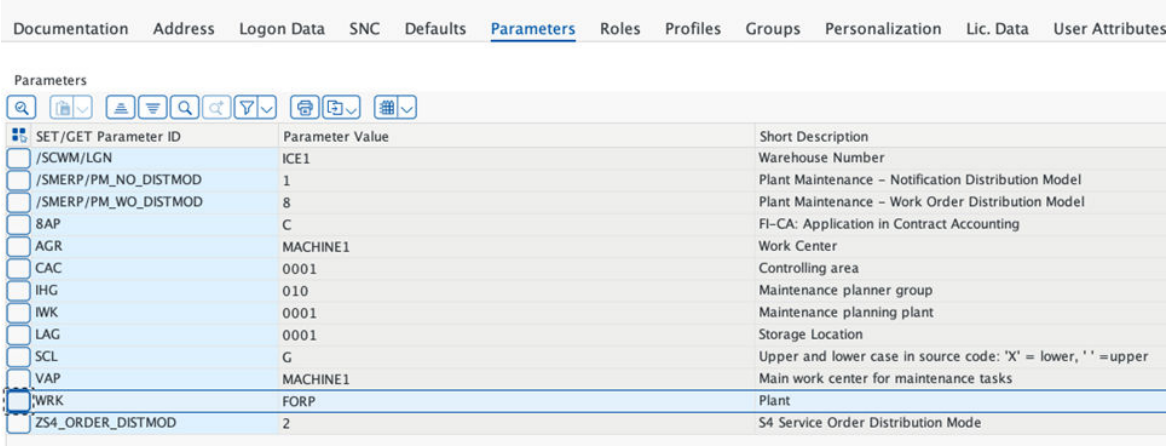
Prerequisites

Below are the prerequisites for implementing the *Field Logistics* persona.

1. Assign a user the *Field Logistics* persona. For more details, refer to the Configuring Personas [page 89] procedure in the SAP Service and Asset Manager configuration guide.
   - Create separate security roles for each persona. For instance, assign a role with the */MERP/FLOG* authorization object to the *Field Logistics* persona.



2. Assign the WRK (Plant) user parameter to a user.



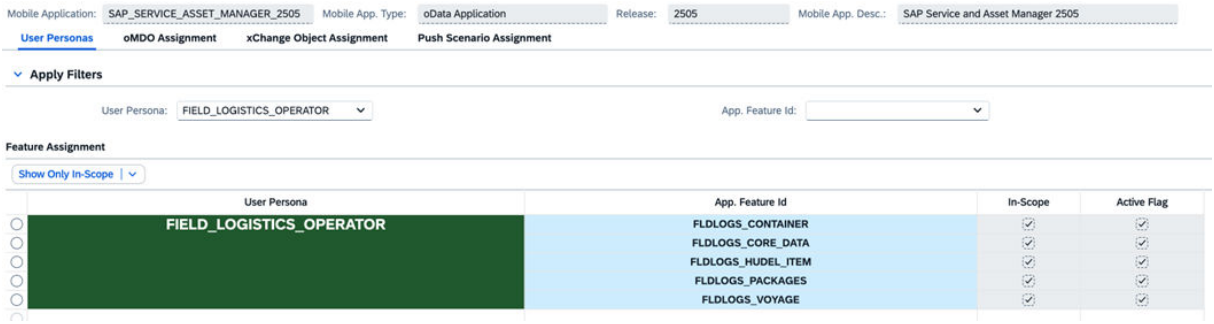
> ### Note
>
> Users must have the authority to create field logistics documents and post goods issues or receipts for deliveries.

Application Features Assigned to the Field Logistics Persona

The component assignment allows you configure features for a user persona.

You can assign new application features to a user persona or enable or disable features already assigned to them.

Below are the application features assigned to the *Field Logistics* persona.



> **Note**
>
> The *Field Logistics* persona has a separate data core.
>
> For more information on component assignments, refer to the Configuring Component Assignments [page 101] topic.

Configuration

Perform the following configuration step(s):

1. Assigning and Unassigning a Feature - Back End [page 161]
2. Enabling and Disabling a Feature - Back End [page 162]
3. Assigning and Unassigning an OMDO to a Feature - Back End [page 163]
4. Configuring Data Distribution - Back End [page 165]
5. Mobile Application Parameters - Back End [page 169]

3.2.1 Assigning and Unassigning a Feature - Back End

Context

OMDO groups are assigned to application features, which in turn are assigned to user personas. The following procedure explains how to generally assign an application feature.

General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **Enabling and disabling features**: refer to Configuring Features in *MAIF Configuration Guide*.
- **mobile application parameters** configuration: refer to Parameters Tab in *MAIF Configuration Guide*.
- **OMDO** and **OMDO filter** configuration: refer to OData Mobile Data Object Configuration and OData Mobile Data Object Configuration - Data Filter Tab in *MAIF Configuration Guide*.
- **Exchange** and **Exchange filters** configuration: refer to Exchange Object Configuration and Change Detection Condition Filter Tab in *MAIF Configuration Guide*.
- **Server parameters** configuration: refer to Administration - Server Management in *MAIF Administrator Guide*.
- **User attributes** configuration: refer to Sync Groups in *MAIF Configuration Guide*.
- **User parameters** configuratio:, refer to Administration - User Management in *MAIF Administrator Guide*.

Procedure

1. Log in to the configuration panel using `TCode /SYCLO/CONFIGPANEL`.
2. On the main page of the config panel, select *Component Assignment*.
3. Select the mobile app from the list and choose it.
4. Use the picker for user personas to select the *Field Logistics* persona.
5. Choose *Change* to edit the data.
6. To limit the features, select the *Show Only Enabled* feature assignment.
7. In the list of features assigned to the user persona, uncheck the active flag to disable the feature, or select a feature (for which In-Scope = True) to assign the feature to the user persona.

> ⓘ Note
>
> Assigning an application feature to a persona affects only that persona within the context.
>
> If an application feature isn't active, the ODMO and related entities won't load during synchronization. An ODMO can be assigned to multiple features. In this case, the ODMO is invoked even if just one of the features is assigned to a persona.

3.2.2 Enabling and Disabling a Feature - Back End

Context

Alternatively, you can disable the application features themselves. The following procedure explains how to enable or disable application features.

General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **Enabling and disabling features**: refer to Configuring Features in *MAIF Configuration Guide*.
- **mobile application parameters** configuration: refer to Parameters Tab in *MAIF Configuration Guide*.
- **OMDO** and **OMDO filter** configuration: refer to OData Mobile Data Object Configuration and OData Mobile Data Object Configuration - Data Filter Tab in *MAIF Configuration Guide*.
- **Exchange** and **Exchange filters** configuration: refer to Exchange Object Configuration and Change Detection Condition Filter Tab in *MAIF Configuration Guide*.
- **Server parameters** configuration: refer to Administration - Server Management in *MAIF Administrator Guide*.
- **User attributes** configuration: refer to Sync Groups in *MAIF Configuration Guide*.
- **User parameters** configuratio:, refer to Administration - User Management in *MAIF Administrator Guide*.

Procedure

1. On the main page of the config panel, select *Mobile Application Configuration*.
2. Select the mobile application from the list.
3. On the *Features* tab, choose *Change* to edit the data.
4. To modify the application feature, check the flag to activate it or uncheck the flag to disable it.

> **Note**
>
> When an application feature is disabled, it affects all application personas. Additionally, the OMDOs assigned to the feature aren't called anymore.

3.2.3 Assigning and Unassigning an OMDO to a Feature - Back End

Context

The OMDO group is assigned to an application feature, which is then assigned to user personas.

General Links

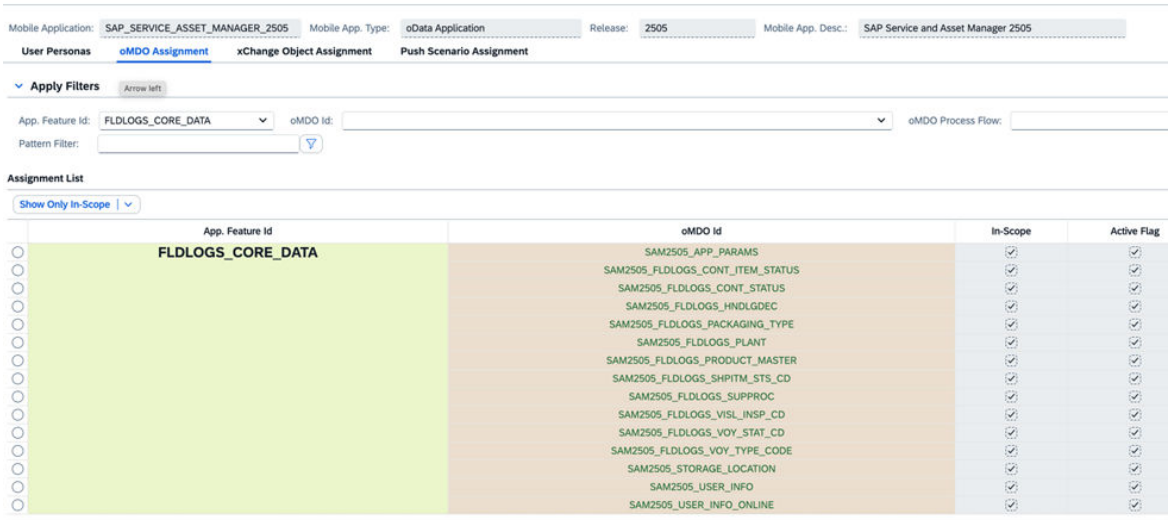
If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **Enabling and disabling features**: refer to Configuring Features in *MAIF Configuration Guide*.

- **mobile application parameters** configuration: refer to Parameters Tab in *MAIF Configuration Guide*.
- **OMDO** and **OMDO filter** configuration: refer to OData Mobile Data Object Configuration and OData Mobile Data Object Configuration - Data Filter Tab in *MAIF Configuration Guide*.
- **Exchange** and **Exchange filters** configuration: refer to Exchange Object Configuration and Change Detection Condition Filter Tab in *MAIF Configuration Guide*.
- **Server parameters** configuration: refer to Administration - Server Management in *MAIF Administrator Guide*.
- **User attributes** configuration: refer to Sync Groups in *MAIF Configuration Guide*.
- **User parameters** configuratio:, refer to Administration - User Management in *MAIF Administrator Guide*.

Procedure

1. Log in to the configuration panel using `TCode /SYCLO/CONFIGPANEL`.
2. On the main page of the config panel, select *Component Assignment*.
3. Select the mobile app from the list.
4. To edit the data, go to the *OMDO Assignment* tab and choose *Change*.
5. Use the picker to select a feature to limit the list to that feature.
6. Select *Display OptionsShow Only In-Scope*.
7. In the *OMDO* list, assign or unassign an OMDO by selecting the active checkbox.



3.2.4 Configuring Data Distribution - Back End

Context

With OMDO's data distribution rules, you identify:

- How data is uploaded
- Which data is uploaded to the mobile application.

SAP Service and Asset Manager supports various data distribution models:

- **OMDO Filters**: The collection of object data relies entirely on the conditions set by OMDO filters.
- **Dependency Queue**: The collection of object data depends solely on dependency queue objects, with no filter conditions applied to the fetch criteria.
- **Dependency Queue + OMDO DOF Filters**: The collection of object data depends on dependency queue objects, and OMDO DOF filters are applied to the result set.
- **Other (Custom) BAdIs**: You can implement your own distribution logic using BAdIs.
  For more details on data distribution, refer to the Data Distribution Model Overview topic.

General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **Enabling and disabling features**: refer to Configuring Features in *MAIF Configuration Guide*.
- **mobile application parameters** configuration: refer to Parameters Tab in *MAIF Configuration Guide*.
- **OMDO** and **OMDO filter** configuration: refer to OData Mobile Data Object Configuration and OData Mobile Data Object Configuration - Data Filter Tab in *MAIF Configuration Guide*.
- **Exchange** and **Exchange filters** configuration: refer to Exchange Object Configuration and Change Detection Condition Filter Tab in *MAIF Configuration Guide*.
- **Server parameters** configuration: refer to Administration - Server Management in *MAIF Administrator Guide*.
- **User attributes** configuration: refer to Sync Groups in *MAIF Configuration Guide*.
- **User parameters** configuratio:, refer to Administration - User Management in *MAIF Administrator Guide*.
  The table below summarizes the data distribution for OMDO within the Field Logistics persona.

> **Note**
>
> The table displays only transactional data. It doesn't include master or configuration OMDO data, such as material or plant information. The source OMDO for all entities is *SAM2505_ONDEMAND_OBJECT*, and the technical entity type is *ONDEMANDOBJECT*.

OMDO Name	Distribution Mode
SAM2505_FLDLOGS_VOYAGE	1-OMDO Filter and 2-Dependency Queue
SAM2505_FLDLOGS_CONTAINER	1-OMDO Filter and 2-Dependency Queue
SAM2505_ FLDLOGS_PACKAGE	1-OMDO Filter and 2-Dependency Queue
SAM2505_ FLDLOGS_HUDEL_ITEM	1-OMDO Filter and 2-Dependency Queue

> **Note**
>
> Currently, the SAP Service and Asset Manager app doesn't download *Received Containers*, *Packages*, *Container/Package Items*, *Handling Units*, or *Delivery Items*.

By default, SAP configures the master data entities, like handling decisions, statuses, and plants, to use the 1-OMDO filter distribution mode. This setup means that during synchronization, the data for these entities downloads based on the pre-defined filters in OMDO.
Below is a list of master data entities related to the Field Logistics persona:

OMDO Name	Description
SAM2505_FLDLOGS_CONT_ITEM_STATUS	Field Logistics Container Item Status
SAM2505_FLDLOGS_CONT_STATUS	Field Logistics Container Status
SAM2505_FLDLOGS_HNDLGDEC	Field Logistics Handling Decision
SAM2505_FLDLOGS_PACKAGING_TYPE	Field Logistics Packaging Type
SAM2505_FLDLOGS_PLANT	Field Logistics Plant
SAM2505_FLDLOGS_SHPITM_STS_CD	Field Logistics - Delivery Item/Handling Unit Status
SAM2505_FLDLOGS_SUPPROC	Field Logistics Supply Process
SAM2505_FLDLOGS_VISL_INSP_CD	Field Logistics Visual Inspection Code
SAM2505_FLDLOGS_VOY_STAT_CD	Field Logistics Voyage Status Code
SAM2505_FLDLOGS_VOY_TYPE_CODE	Field Logistics Voyage Type Code

By default, transactional data entities—such as voyages, containers, packages, and handling units/delivery items—use the 2-dependency queue distribution mode. This configuration means that data for these entities downloads based on the dependencies of other entities. For instance, when a voyage order downloads, the dependent containers, packages, handling units, and delivery items also download.

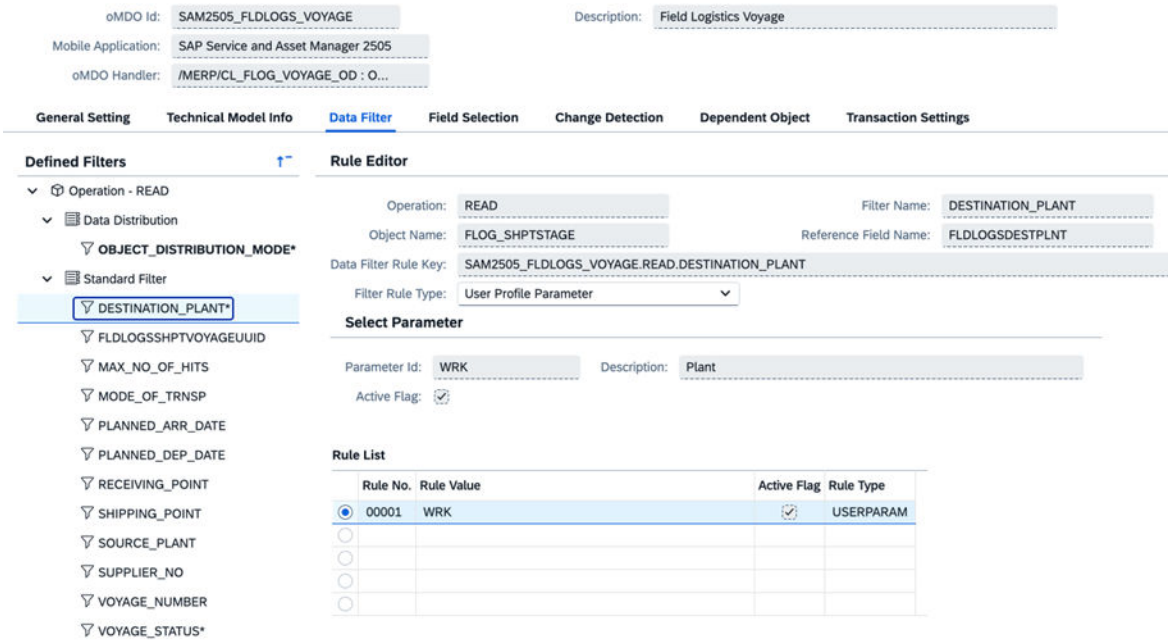
Below is a list of transactional data entities related to the Filed Logistics persona:

OMDO Name	Description
SAM2505_FLDLOGS_VOYAGE	Field Logistics Voyage
SAM2505_FLDLOGS_VOYAGE_LITE	Field Logistics Voyage Lite
SAM2505_FLDLOGS_CONTAINER	Field Logistics Container
SAM2505_FLDLOGS_PACKAGE	Field Logistics Package
SAM2505_FLDLOGS_HUDEL_ITEM	Field Logistics Handling Unit and Deliver Items

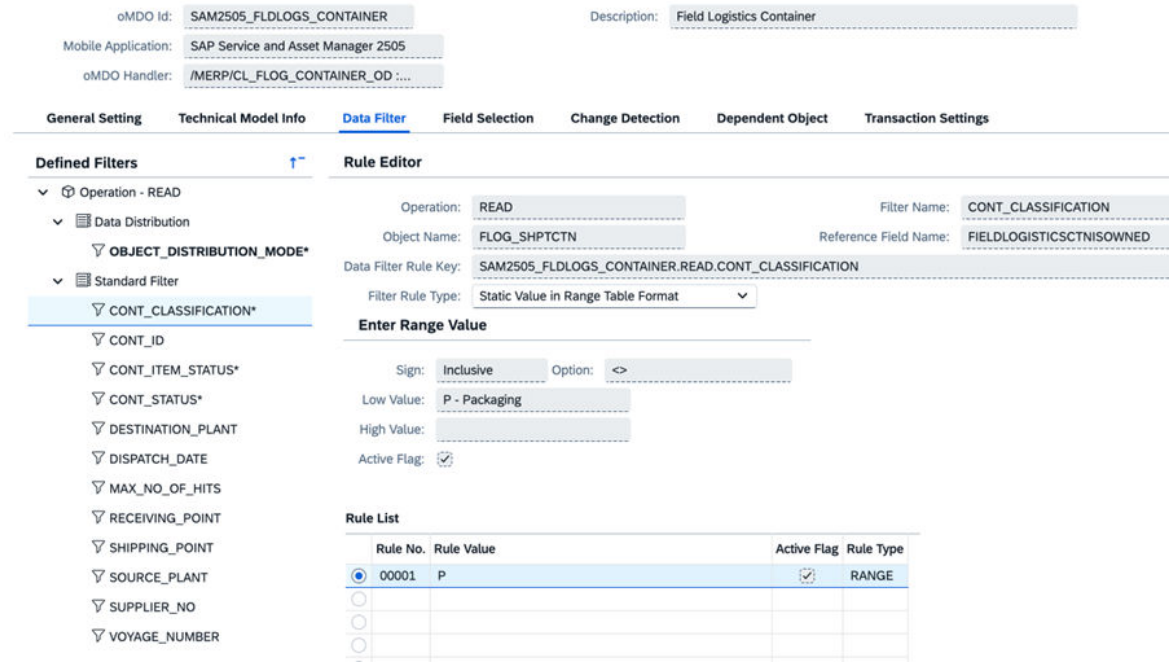
Voyage LITE: *SAM2505_FLDLOGS_VOYAGE_LITE*
This oMDO downloads only voyage header information during the initial sync. The data distribution uses the 1-OMDO filter distribution mode.
For online searches, the following OMDOs are used:

OMDO Name	Distribution Mode
SAM2505_FLDLOGS_VOYAGE_ONLINE	9 - Free Search
SAM2505_FLDLOGS_CONTAINER_ONLINE	9 - Free Search
SAM2505_ FLDLOGS_PACKAGE_ONLINE	9 - Free Search
SAM2505_ FLDLOGS_HUDEL_ITEM_ONLINE	9 - Free Search

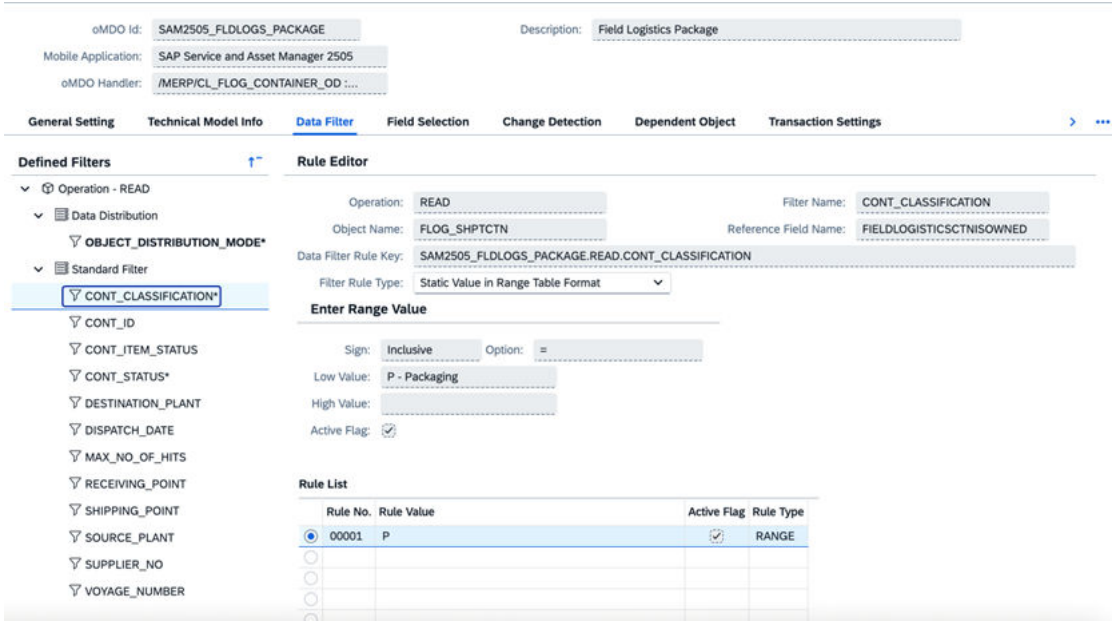
Configuring Filters
The following filters are available for configuration:
OMDO name: SAM2505_FLDLOGS_VOYAGE



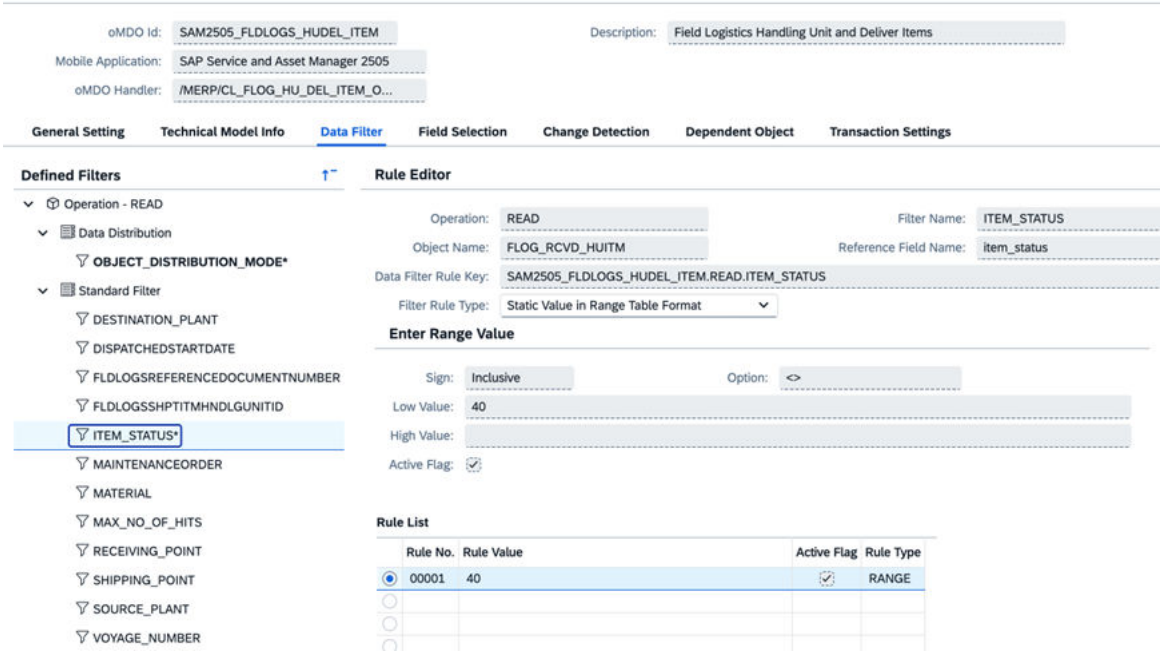
OMDO name: SAM2505_FLDLOGS_CONTAINER



OMDO name: SAM2505_FLDLOGS_PACKAGE



OMDO name: SAM2505_FLDLOGS_HUDEL_ITEM



To configure Exchange, use the following Exchange objects:

Exchange Object Name
SAM2505_FLDLOGS_VOYAGE
SAM2505_FLDLOGS_CONTAINER
SAM2505_FLDLOGS_PACKAGE
SAM2505_FLDLOGS_HUDEL

3.2.5 Mobile Application Parameters - Back End

Context

With the mobile app settings, you can control client-side runtime behavior.

For more details, check out the *Parameters Tab* section in the Mobile Application Configuration topic.

Below is a list of mobile app parameters specific to the Field Logistics persona:

Group	Name	Value	Scope	Description
FL	download.lite	Y	Application	During the fetch action, download only Voyages, Containers, Packages, Delivery Items, and Handling Units. Y - Yes N - No
FL	search.auto.navigate	Y	Application	Enable automatic navigation to the document details page when a search returns only one document

General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **Enabling and disabling features**: refer to Configuring Features in *MAIF Configuration Guide*.
- **mobile application parameters** configuration: refer to Parameters Tab in *MAIF Configuration Guide*.
- **OMDO** and **OMDO filter** configuration: refer to OData Mobile Data Object Configuration and OData Mobile Data Object Configuration - Data Filter Tab in *MAIF Configuration Guide*.
- **Exchange** and **Exchange filters** configuration: refer to Exchange Object Configuration and Change Detection Condition Filter Tab in *MAIF Configuration Guide*.
- **Server parameters** configuration: refer to Administration - Server Management in *MAIF Administrator Guide*.
- **User attributes** configuration: refer to Sync Groups in *MAIF Configuration Guide*.
- **User parameters** configuratio:, refer to Administration - User Management in *MAIF Administrator Guide*.

3.3 Extended Warehouse Clerk Configuration

In the SAP Service and Asset Manager mobile application, the Extended Warehouse Clerk persona is based on the Extended Warehouse Management (EWM) back end solution, supporting both the **Embedded** and **Decentralized** architectures.

See the following documents to configure the Extended Warehouse Clerk persona:

- Configuration Prerequisites and Limitations - Extended Warehouse Clerk [page 171]
- General Feature Configuration - Extended Warehouse Clerk [page 173]
- Mobile Application Parameters - Extended Warehouse Clerk [page 174]
- oMDO Configuration - Extended Warehouse Clerk [page 175]

- Configuring Personas [page 89]
- Supported SAP Transaction Codes for SAP Service and Asset Manager [page 602]

Key Feature Configurations

- Inbound Delivery Process Configuration (Extended Warehouse Clerk) [page 445]

Related Documents

- SAP Extended Warehouse Management (SAP EWM) product page
- Extended Warehouse Management User Guide
- Application Product Overview - Extended Warehouse Management Persona Overview .

3.3.1 Configuration Prerequisites and Limitations - Extended Warehouse Clerk

Prerequisites

- To use the Extended Warehouse Clerk persona in the SAP Service and Asset Manager mobile app, you need the Extended Warehouse Management back end solution installed and configured (with either of the supported EWM architectures [page 170]). For more information, refer to the SAP Extended Warehouse Management (SAP EWM) documentation.
- For all users, you need to maintain the */SCWM/LGN* User Parameter with the *Warehouse Number* that is also used in the EWM system. For more information, see User Parameter IDs [page 606].
- Refer to the *SAP Note* 3577734 for information on the prerequisites needed for making resource changes to persona.

OnDemand Flow

The Extended Warehouse Clerk persona has been refactored to use the new OnDemand flow to download, update, and remove its data on the device. To use this flow, your system must run a version of the Mobile Application Integration Framework (MAIF) that supports the new OnDemand flow (the OnDemand storage table and the related object distribution mode), and the following SAP Notes should be implemented:

SAP Note	Title
3802562	*Mobile Application Integration Framework – Consolidated OnDemand flow (MFND layer)*
3803244	*Update OnDemandObject handler to support operations to the OnDemand table*

SAP Note	Title
3803295	*SAP Service and Asset Manager – EWM – Refactor EWM Outbound Delivery oMDO handler to support new OnDemand flow*
3803296	*SAP Service and Asset Manager – EWM – Refactor EWM Warehouse Order oMDO handler to support new OnDemand flow*
3803487	*SAP Service and Asset Manager – EWM – Refactor EWM Handling Unit oMDO handler to support new OnDemand flow*
3803913	*SAP Service and Asset Manager – EWM – Refactor EWM Storage Bin oMDO handler to support new OnDemand flow*
3803914	*SAP Service and Asset Manager – EWM – Refactor EWM Pick HU oMDO handler to support new OnDemand flow*
3812161	*SAP Service and Asset Manager – EWM – Refactor EWM Resource oMDO handler to support new OnDemand flow*
3831027	*SAP Service and Asset Manager – EWM – Refactor EWM Inbound Delivery oMDO handler to support new OnDemand flow*
3831028	*SAP Service and Asset Manager – EWM – Refactor EWM Physical Inventory oMDO handler to support new OnDemand flow*
3832175	*SAP Service and Asset Manager – EWM – Refactor EWM Warehouse Task oMDO handler to support new OnDemand flow*

> **Note**
>
> These changes will be part of the **MFND** and **MERP 2702 TCIs**.

When your MAIF version supports the OnDemand flow and the SAP Notes listed above are implemented, the *Fetch and download* feature of SAP Service and Asset Manager uses *Object Distribution Mode 4* for the **source** (OnDemand) entities and *Object Distribution Mode 3* (or 2 in some cases) for the **dependent** entities. This combination ensures that both source and dependent entities are correctly downloaded, updated, and removed from the device.

Depending on new implementation or existing implementations, apply the following:

- **New implementations**:
  Implement all of the SAP Notes listed above, follow the manual instructions contained in each note, and import the configuration delta files delivered with the notes. No further configuration changes are required: the delivered standard configuration already enables the OnDemand flow.
- **Existing implementations with custom configuration**:
  If you have adapted the delivered configuration for these objects, be aware that the behavior of the EWM object handlers changes once the SAP Notes are implemented. Review the new standard settings - Object Distribution Mode 4 for the source entities and Object Distribution Mode 3 for the dependent entities - and consider adopting them so that your scenario benefits from the corrected download, update, and removal behavior.

Limitations

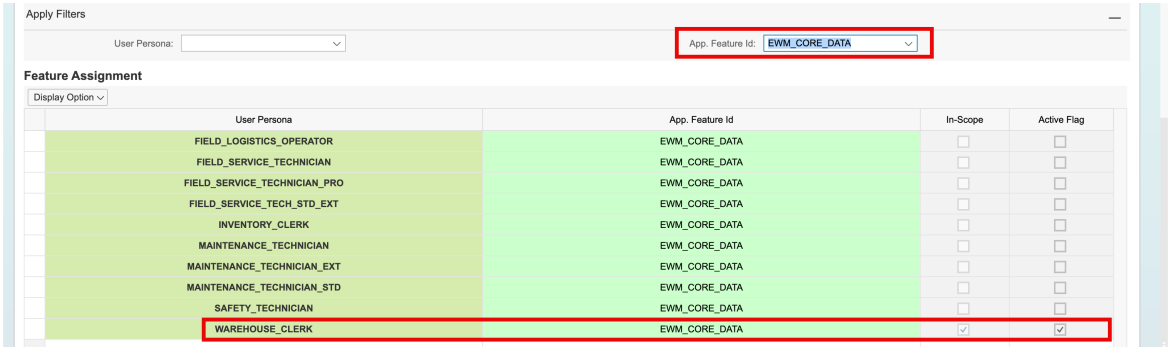
- If SAP Service and Asset Manager is connected to the **Decentralized EWM architecture**, the mobile app **will not support** any other personas.
- In the case of *Goods Receipt* for *Inbound Deliveries*, receiving a single item directly is not supported. You can only receive a single item by confirming the *Warehouse Task* of the corresponding *Item*.

3.3.2 General Feature Configuration - Extended Warehouse Clerk

For the Extended Warehouse Clerk persona to work, you must enable the *EWM_CORE_DATA* feature in the ConfigPanel.

Procedure

1. Go to *Component Assignments* and select your application from the list.
2. In the *App. Feature Id* dropdown, select *EWM_CORE_DATA*.
3. Enter *Change mode* and set the feature to *Active* for the Extended Warehouse Clerk persona.



4. *Save* your changes.

3.3.3 Mobile Application Parameters - Extended Warehouse Clerk

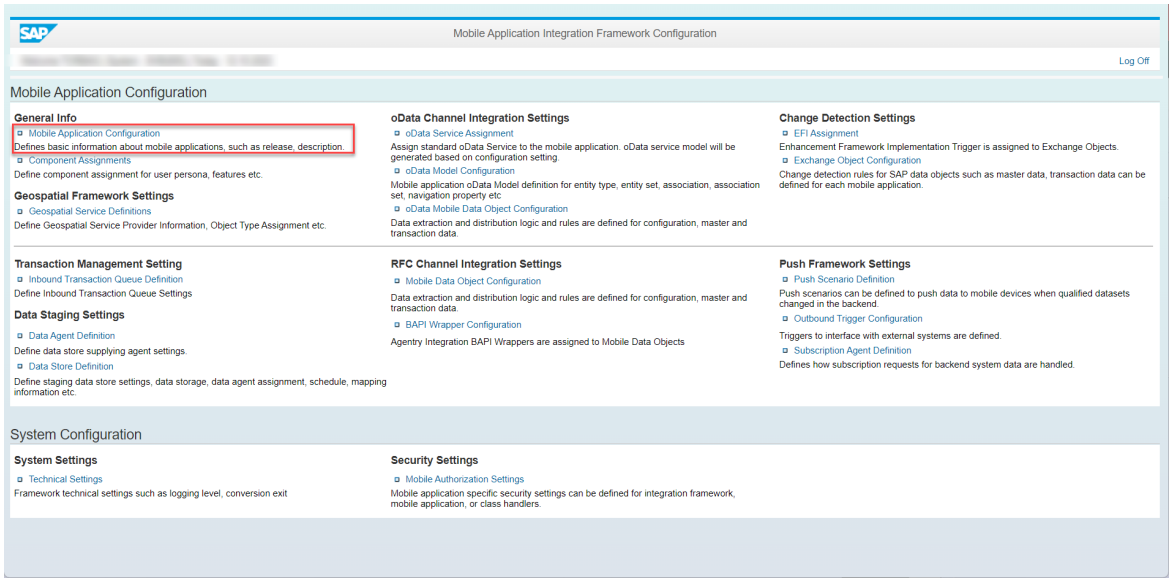
Context

For the Extended Warehouse Clerk persona, you can configure the following mobile app parameters:

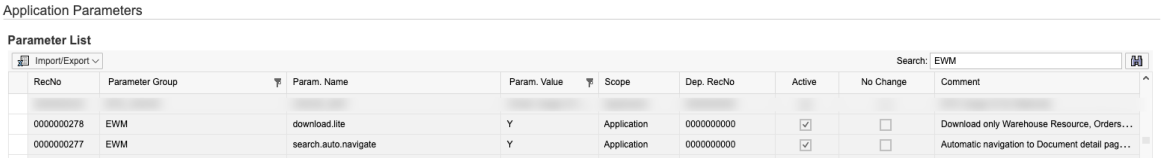
> **Note**
>
> For more information about **Mobile Application Parameters** configuration, refer to Parameters Tab in *MAIF Configuration Guide*.

Procedure

1. On the *Configuration Panel*, go to *Mobile Application Configuration*.



2. On the left, select your application from the list, and go to the *Parameters* tab.
3. Under *Parameter List*, you can search or filter the list of parameters related to the Extended Warehouse Clerk persona (filter the *Parameter Group* to *EWM*).



4. Configure the following Extended Warehouse Clerk-related parameters according to your preference:

   - `download.lite`: To optimize delta synchronization, only Warehouse Resources, Orders, Tasks, TaskSerialNumbers and WHPiCKHUs are downloaded during the fetch action (Inventory Management data will not be downloaded).

- `search.auto.navigate`: Enable automatic navigation to the document details page when a search returns only one document.

5. *Save* your changes.

3.3.4 oMDO Configuration - Extended Warehouse Clerk

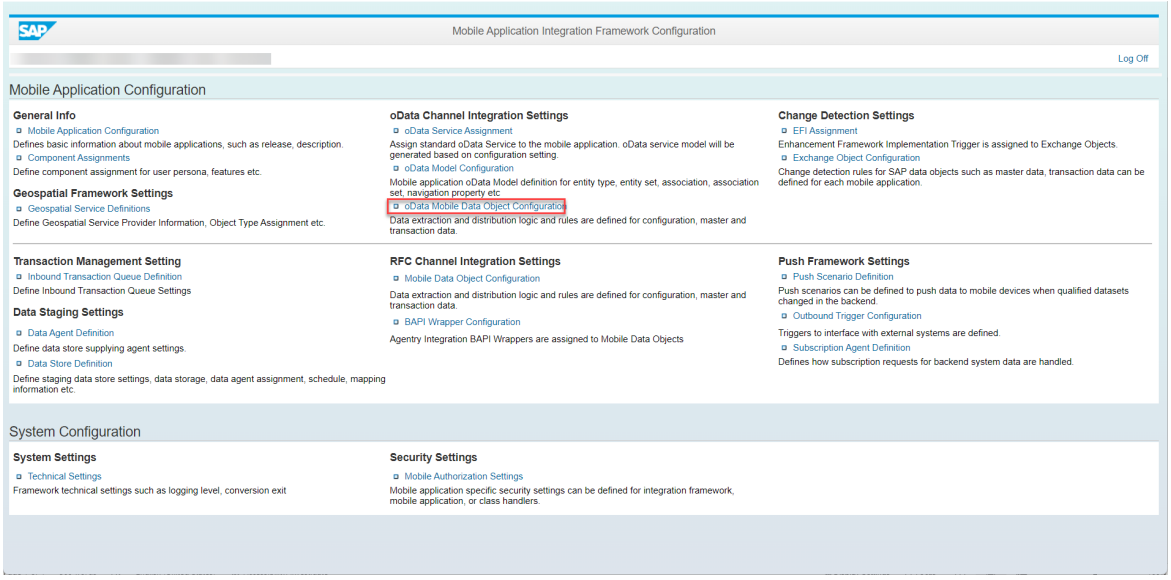
Context

To change the oMDO data filters for the Extended Warehouse Clerk persona, perform the following steps:

> **Note**
>
> For more information about **oMDO** and **oMDO filter** configuration, refer to OData Mobile Data Object Configuration and OData Mobile Data Object Configuration - Data Filter Tab in *MAIF Configuration Guide*.

Procedure

1. On the *Configuration Panel*, go to *oData Mobile Data Configuration*.



2. You can configure the following *oMDOs* under the *Data Filter* tab according to your preference:
   - *SAM<XXXX>_WAREHOUSE_INBOUND_DLV*
   - *SAM<XXXX>_WAREHOUSE_INBOUND_DLV_ONLINE*
3. *Save* your changes.

3.4 Field Service Technician Configuration

In this section of the guide, we cover general configuration procedures related to the Field Service Technician persona, arranged according to the relevant back end systems; **Customer Service [page 177]** and **SAP S/4HANA [page 205]** back end.

> **Note**
>
> For more information about the Field Service Technician persona, see Field Service Technician Persona Overview (Standard, Professional, External).

- SAP Service and Asset Manager supports the following Field Service Technician personas:
  - **Field Service Technician Standard**:
    - Supports a reduced number of Field Service Technician features.
  - **Field Service Technician Professional**:
    - The Field Service Technician **Professional** persona supports **all** Field Service Technician features on the **Customer Service back end** system and also Meter Management [page 463].
    - The Field Service Technician **Professional** persona on the SAP S/4HANA back end system is currently **not supported**.
  - **Field Service Technician External**:
    - Compared to Field Service Technician Standard and Professional, it is a separate persona with limited functionality, created specifically for **external workers** within your organization.
    - You do not need to set up SAP User IDs for all your external workers.
    - This persona is required for the FSM Crowd Service Integration [page 411] (FSM Crowd users do not exist in the SAP back end system).
    - The Maintenance Technician **External** and Field Service Technician **External** personas **cannot** be used with other personas. Users may be assigned only one of these personas and must not be assigned any additional personas.

FSM Integration Support Matrix

See the following table about the supported integration types for SAP Service and Asset Manager and Field Service Management:

Persona / Back End	Proaxia	CPI / SCI
Maintenance Technician [page 116]*	YES	YES
Field Service Technician with Customer Service [page 177]	YES	NO
Field Service Technician with SAP S/4HANA [page 205]	NO	YES

* Status changes are not propagated to Service Assignments for EAM phase model orders. The operation status is propagated to the *Activity* by the underlying integration.

> **Note**
>
> See the following documents for more information:
>
> - Integration of SAP Service and Asset Manager with Field Service Management Using the Proaxia Field Service Management Connector [page 180]
> - FSM SAP Cloud Integration [page 204]
> - EAM Phase Model Configuration - Overview [page 341]

3.4.1 Field Service Technician Configuration on a Customer Service Back End

The Field Service Management solution connects and enables operations while simplifying and automating processes, helping to accelerate execution, improve the productivity of service teams, and control costs.

Using the Field Service Management solution, field service leaders and managers can make decisions based on real-time insights, gain visibility of field service operations, and take advantage of analytical dashboards.

Field service technicians using the SAP Service and Asset Manager app get assignment information in advance, so they are better prepared. Flexible mobile tools, including guided procedures and checklists help solve issues on the first visit while reducing time spent on administrative tasks. While on-site, technicians can collect relevant information about the assignment, get customer signatures, and sync information and back office processes quickly.

3.4.1.1 Configuration Prerequisites and Limitations - Field Service Technician on Customer Service Back End

Prerequisites

- It is assumed that the Proaxia Field Service Management connector [page 180] is configured and set up to replicate the data between the SAP back end and the SAP Field Service Management system.
  SAP Service and Asset Manager integration with Field Service Management requires that the following scenarios are configured and enabled within the Proaxia Field Service Management connector:
  - **Employees:** Replicate employees (SAP HR Personnel numbers) from SAP ECC to Field Service Management as Persons. Use transaction *PA30* to configure *Infotype 0105/001* to map the user name to the user's personnel number replicated in Field Service Management.
  - **Materials:** Replicate *Materials* in the back end as *Items* to Field Service Management. Items are needed to create equipment.
  - **Equipment / Functional Locations:** Replicate *Equipment* and/or *Functional Location* to Field Service Management as *Equipment*. Equipment are technical objects assigned to service orders
  - **Customers:** Replicate *Customers* to Field Service Management as *Business Partners*. Business partners are assigned to service orders.

- **Business Partners (Optional):** Replicate *Business Partners* to Field Service Management if they're needed in the customer scenario as part of order processing.
- **Orders:** Replicate *Service Orders*, *Work Orders*, and *Operations* to Field Service Management.
- **Assignments (Field Service Management):** Replicate *Assignments* from the Field Service Management system to the back end.

- **Supported Smartforms fields**:
  - Not all fields within Smartforms [page 195] are supported in the same way. Smartforms must be preconfigured and customized by administrators before users can fill in all the fields.
  - For the complete list of Smartform elements available for use, refer to Template Elements section in the official *Field Service Management* documentation.

Limitations

Currently, the Field Service Technician persona (**Customer Service back end**) has the following limitations:

- In the case of configuring **multiple** *Plant*, *Storage Location* and *Work Center* parameters:
  - For the Vehicle Stock [page 560] feature, a *Plant* and *Storage Location* is used to identify the vehicle. Therefore, if you have multiple values, the feature **will not work**.
  - When adding a Part, the *Plant* and *Storage Location* are defaulted from *WRK* and *LAG* respectively; therefore, we **recommend to maintain only a single value in each**.

  > → Tip
  >
  > For more information, see Recommended Configuration for Multiple Plants and Work Centers [page 111].

- The Maintenance Technician **External** and Field Service Technician **External** personas **cannot** be used with other personas. Users may be assigned only one of these personas and must not be assigned any additional personas.
- See FSM Integration Support Matrix [page 176] for the supported integration types.

3.4.1.2 Field Service Management Scheduling - SAP Service and Asset Manager Integration

Field Service Management planning board administrators can use geolocation information from the mobile app to enable scheduling and dispatching based on the location of the technician.

Supported Scenarios

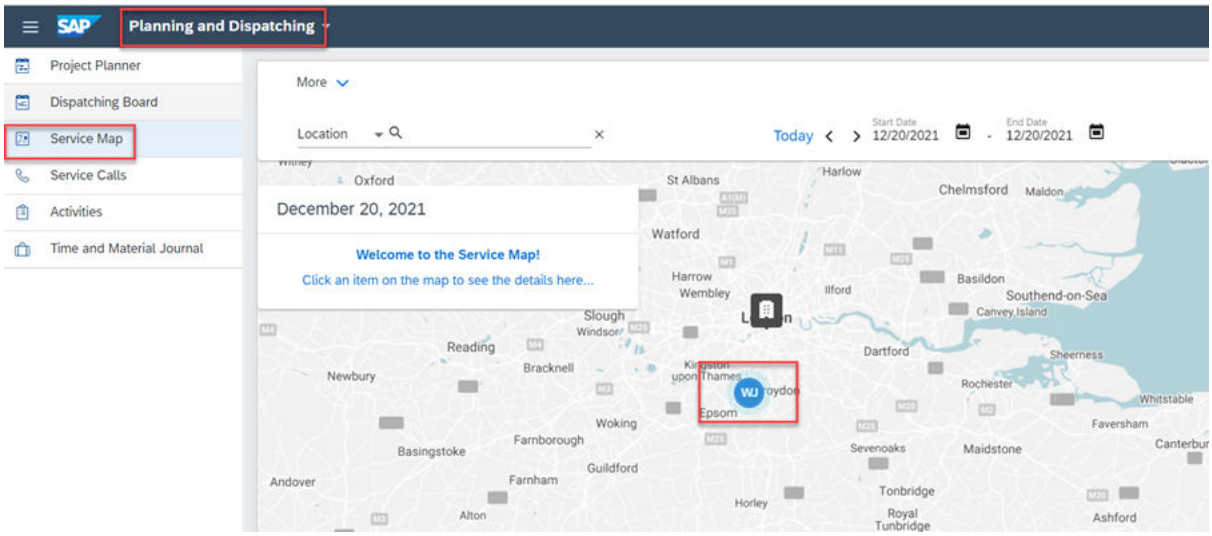
The following scenarios are supported for the integration of SAP Service and Asset Manager with Field Service Management Scheduling:

- Status updates: Status updates from SAP Service and Asset Manager are propagated to the Field Service Management Planning and Dispatching Tool. Since Field Service Management supports only activity level assignments, status transition is only supported for the *Assignment Type 2 – Operation Level Assignment to Personnel Number*. Only statuses assigned to the Field Service Management service workflow statuses are propagated to Field Service Management.
- Technician Location Tracking: The location of the technician captured from SAP Service and Asset Manager is updated to Field Service Management so that it can be viewed in the Field Service Management service map.
- Reject Operation: If a technician rejects an operation, the corresponding activity in Field Service Management is unassigned.
- Transfer Operation: If a technician transfers an operation from one technician to another, the corresponding activity in Field Service Management is reassigned from one technician to another.

Employee Location Update

- The employee location is captured in SAP Service and Asset Manager, and the location can be updated into Field Service Management.
- The mobile status changes from SAP Service and Asset Manager can be updated into the Field Service Management.

The location updates from the client can be viewed under the Field Service Management Map, *Planning and Dispatch* > *Service Map*.



> ### Note
>
> For more information about how to configure User Location Tracking, see Location Tracking Configuration [page 452].

3.4.1.2.1 Integration of SAP Service and Asset Manager with Field Service Management Using the Proaxia Field Service Management Connector

To execute the supported integration scenarios between SAP Service and Asset Manager and Field Service Management, SAP Service and Asset Manager integrates directly with Field Service Management using the Service and Data APIs provided by Field Service Management. However, the underlying objects that need to be updated (service orders (service calls in Field Service Management), operations (activities in Field Service Management), employees (persons in Field Service Management), are created by the Proaxia connector.

Therefore, you must implement the following prerequisites for the end-to-end scenarios to work:

- Proaxia prerequisites [page 177]
- Switching on Sending externalID from the Proaxia Field Service Management Connector to the Field Service Management Solution [page 180]
- Implement BADI Methods [page 181]

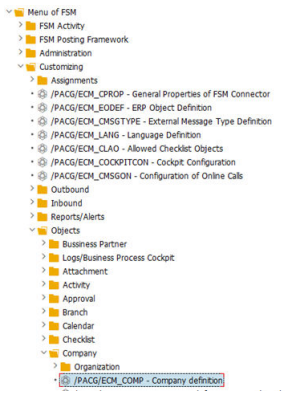
3.4.1.2.1.1 Switching on Sending externalID from the Proaxia Field Service Management Connector to the Field Service Management Solution

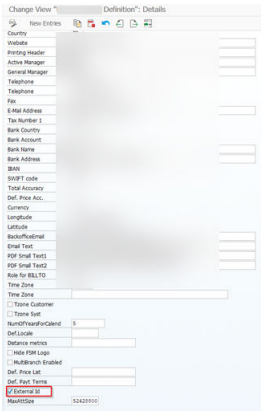
Context

> **Note**
>
> Perform these changes within the configuration of the Proaxia Field Service Management connector.

Procedure

Switch on the sending of the *externalId* from the Field Service Management connector to Field Service Management as shown in the following screenshots:





3.4.1.2.1.2 Implement BADI Methods

Context

Depending on the integration framework used, implement the */MERP/CA_FSM_CROSSREF_BADI* BADI. The methods in the BADI must return the cross-referencing information between the back end object ID and the Field Service Management object ID.

Procedure

1. Implement the local method to determine the company ID, required for the *GET_EMPLOYEE_IDS BADI* method.

```
METHOD get_compid.

    DATA: lv_string1    TYPE string,
          lv_string2    TYPE string,
          lv_account    TYPE string,
          lv_fsmaccount TYPE /pacg/ecm_cloudaccount,
          lv_fsmcompany TYPE /pacg/ecm_cloudid,
          lv_compid     TYPE /pacg/ecm_compid,
          ls_cacc       TYPE /pacg/ecm_cacc.

    lv_account = iv_account.

    SPLIT lv_account AT '&account=' INTO lv_string1 lv_string2.
    SPLIT lv_string2 AT '&company=' INTO lv_string1 lv_string2.

    lv_fsmaccount = lv_string1.
    lv_fsmcompany = lv_string2.


    ls_cacc = /pacg/ecm_cl_d_access=>get_cloudcomp_definition(
```

```
iv_cloudaccount = lv_fsmaccount
iv_cloudid      = lv_fsmcompany ).

rv_compid = ls_cacc-compid.

ENDMETHOD
```

2. Implement the method */MERP/IF_CA_FSM_CROSSREF_BADI~GET_EMPLOYEE_IDS*:

   This method is a prerequisite for saving geolocations captured from SAP Service and Asset Manager to the Field Service Management planning and scheduling board.

   The method must return the Field Service Management internal employee ID(s) (*Field* `id` of the Field Service Management *Person* entity) based on the personnel number(s) provided.

   Use the importing parameter *IO_ACI_SERVICE* to execute a service call to Field Service Management for retrieving the `id` based on the `code` in the following code example.

   > ### Note
   >
   > For simplicity, it is assumed that only a single personnel number is passed as a parameter. Adjust the code accordingly to handle multiple parameters. The following code is an example. You may need to make additional adjustments for your environment.

```
METHOD /merp/if_ca_fsm_crossref_badi~get_employee_ids.

    TYPES: BEGIN OF ty_error,
             error TYPE string,
           END OF ty_error.

    TYPES: BEGIN OF ty_fsmitem,
             id         TYPE string,
             externalid TYPE string,
             username   TYPE string,
           END OF ty_fsmitem.

    TYPES: BEGIN OF ty_persondata,
             person TYPE ty_fsmitem,
           END OF ty_persondata.

    DATA:
      lv_pernr_query TYPE string,
      ls_oblnk       TYPE /smfnd/sync_d_oblnk_h_upd_str,
      lv_id          TYPE /smfnd/sync_object_key_dte,
      lv_url         TYPE string,
      lv_char_code   TYPE n LENGTH 3,
      lt_persondata  TYPE STANDARD TABLE OF ty_persondata,
      ls_persondata  LIKE LINE OF lt_persondata,
      lt_error       TYPE STANDARD TABLE OF ty_error,
      ls_error       LIKE LINE OF lt_error,
      lv_status_code TYPE i,
      lv_reason      TYPE string,
      lv_result      TYPE string,
      lv_raw_data    TYPE xstring,
      lv_compid      TYPE /pacg/ecm_compid,
      lv_cloud_uname TYPE /pacg/ecm_cloud_uname,
      ls_pernr       LIKE LINE OF it_pernr.

    TYPES: BEGIN OF ty_personresp,
             data LIKE lt_persondata,
           END OF ty_personresp.

    DATA: ls_personresp TYPE ty_personresp.

    IF io_aci_service IS BOUND.
```

```
      IF it_pernr IS INITIAL.
        RETURN.
      ENDIF.

      lv_compid = get_compid( iv_account ).

      LOOP AT it_pernr INTO ls_pernr.

        CLEAR lv_pernr_query.

        IF ls_pernr-low IS NOT INITIAL.
          TRY.
              lv_cloud_uname = /pacg/
ecm_cl_x_util=>build_cloud_uname( iv_pernr       = ls_pernr-low
                                                                    iv_comp
id      = lv_compid ).
            CATCH /pacg/ecm_cx_main.
              "No FSM user exists
              CONTINUE.
          ENDTRY.
          CONCATENATE lv_pernr_query 'externalId="' ls_pernr-
low '"' INTO lv_pernr_query.
        ENDIF.

        IF lv_pernr_query IS NOT INITIAL.
          CONCATENATE '/api/data/v4/Person?
dtos=Person.24' '&query=' lv_pernr_query
                      '&fields=id,externalId,userName' iv_account INTO lv_url.

          CALL METHOD io_aci_service->call_service
            EXPORTING
              iv_request_uri    = lv_url
              iv_request_method = 'GET'
              it_headers        = it_headers
            IMPORTING
              ev_status_code    = lv_status_code
              ev_reason         = lv_reason
              ev_result         = lv_result
              ev_raw_data       = lv_raw_data.

          lv_char_code = lv_status_code.
          IF lv_char_code CP '4*'.
            ls_error-error = lv_result.
            APPEND ls_error TO lt_error.
          ELSE.
            /aci/
cl_util_json_handler=>deserialize(  EXPORTING json =  lv_result
                                                    CHANGING  data =  ls_pers
onresp  ).
            LOOP AT ls_personresp-data INTO ls_persondata.
              lv_id = ls_persondata-person-id.
              ls_oblnk-object_type  = 'EMPLOYEE'.
              ls_oblnk-object_key  = ls_pernr-low.
              ls_oblnk-ext_object_type  = 'PERSON'.
              ls_oblnk-ext_object_key  = lv_id.
              ls_oblnk-sys_comp = 'SAM_FSM'.
              ls_oblnk-mobile_app = iv_mapp.
              APPEND ls_oblnk TO et_oblnk.
              CLEAR ls_oblnk.
            ENDLOOP.
          ENDIF.
        ENDIF.
      ENDLOOP.
    ENDIF.
  ENDMETHOD.
```

3. Implement the method */MERP/IF_CA_FSM_CROSSREF_BADI~GET_ACTIVITY_ID*:

This method is a prerequisite for implementing the relevant status updates from SAP Service and Asset Manager to the Field Service Management planning and scheduling board. This method must return the Field Service Management internal activity ID (the `id` field of the Field Service Management *Activity* entity) based on the order and operation number provided.

Use the importing parameter *IO_ACI_SERVICE* to execute a service call to Field Service Management for retrieving the ID based on the code. See the following code example for more details.

> **Note**
>
> The following code is an example. You may need to make additional adjustments for your environment.

```
METHOD /merp/if_ca_fsm_crossref_badi~get_activity_id.

    TYPES: BEGIN OF ty_fsmitem,
             id         TYPE string,
             externalid TYPE string,
           END OF ty_fsmitem.

    TYPES: BEGIN OF ty_error,
             error TYPE string,
           END OF ty_error.

    TYPES: BEGIN OF ty_actdata,
             activity TYPE ty_fsmitem,
           END OF ty_actdata.

    DATA:
      lv_act_query   TYPE string,
      lv_id          TYPE /smfnd/sync_object_key_dte,
      lv_url         TYPE string,
      lv_char_code   TYPE n LENGTH 3,
      lt_actnr       TYPE STANDARD TABLE OF /pacg/ecm_actnr,
      lv_actnr       TYPE /pacg/ecm_actnr,
      lv_object_key  TYPE /smfnd/sync_object_key_dte,
      lt_error       TYPE STANDARD TABLE OF ty_error,
      ls_error       LIKE LINE OF lt_error,
      lt_actdata     TYPE STANDARD TABLE OF ty_actdata,
      ls_actdata     LIKE LINE OF lt_actdata,
      lv_status_code TYPE i,
      lv_reason      TYPE string,
      lv_result      TYPE string,
      lv_raw_data    TYPE xstring,
      lv_aufnr_len   TYPE i,
      lo_descr       TYPE REF TO cl_abap_elemdescr,
      ls_aufnr_dfies TYPE dfies.

    TYPES: BEGIN OF ty_actresp,
             data LIKE lt_actdata,
           END OF ty_actresp.

    DATA: ls_actresp TYPE ty_actresp.

    IF io_aci_service IS BOUND.
      IF iv_aufnr IS INITIAL OR iv_vornr IS INITIAL.
        RETURN.
      ENDIF.

      lv_object_key = iv_aufnr.
      lo_descr ?= cl_abap_elemdescr=>describe_by_data( iv_aufnr ).
      ls_aufnr_dfies = lo_descr->get_ddic_field( ).
      lv_aufnr_len = ls_aufnr_dfies-leng.
      lv_object_key+lv_aufnr_len = iv_vornr.

      "Get all activitties for order operation
```

```
      SELECT actnr INTO TABLE lt_actnr FROM /pacg/
ecm_acti WHERE aufnr = iv_aufnr AND vornr = iv_vornr.

      "Get the newest activity
      SORT lt_actnr DESCENDING.
      READ TABLE lt_actnr INTO lv_actnr INDEX 1.
      IF sy-subrc IS NOT INITIAL.
        RETURN.
      ENDIF.

      CONCATENATE lv_act_query 'externalId="' lv_actnr '"' INTO lv_act_query.

      IF lv_actnr IS NOT INITIAL.
        CONCATENATE '/api/data/v4/Activity?
dtos=Activity.39' '&query=' lv_act_query '&fields=id,externalId' iv_account IN
TO lv_url.

        CALL METHOD io_aci_service->call_service
          EXPORTING
            iv_request_uri    = lv_url
            iv_request_method = 'GET'
            it_headers        = it_headers
          IMPORTING
            ev_status_code    = lv_status_code
            ev_reason         = lv_reason
            ev_result         = lv_result
            ev_raw_data       = lv_raw_data.

        lv_char_code = lv_status_code.
        IF lv_char_code CP '4*'.
          ls_error-error = lv_result.
          APPEND ls_error TO lt_error.
        ELSE.
          /aci/
cl_util_json_handler=>deserialize(  EXPORTING json =  lv_result
                                                CHANGING  data =  ls_actres
p  ).
          LOOP AT ls_actresp-data INTO ls_actdata.
            lv_id = ls_actdata-activity-id.
            es_oblnk-object_type  = 'OPERATION'.
            es_oblnk-object_key  = lv_object_key.
            es_oblnk-ext_object_type  = 'ACTIVITY'.
            es_oblnk-ext_object_key  = lv_id.
            es_oblnk-sys_comp = 'SAM_FSM'.
            es_oblnk-mobile_app = iv_mapp.
      ev_id = ls_actdata-activity-id.
            EXIT.
          ENDLOOP.
        ENDIF.
      ENDIF.
    ENDIF.

  ENDMETHOD.
```

4. Implement the method */MERP/IF_CA_FSM_CROSSREF_BADI~GET_SERV_ASSIGN_ID*:

   This method is a prerequisite for implementing relevant status updates from SAP Service and Asset Manager to the Field Service Management planning and scheduling board. The method must return the Field Service Management internal activity ID (the `id` field of the Field Service Management *Activity* entry) based on the order and operation number provided.

   Use the *QUERY_FSM_SERVICEASSIGN* method from the */MERP/CL_CA_FSM_INTEGRATION* class to get this value based on the following code example.

> **Note**
>
> The following code is an example. You may need to make additional adjustments for your environment.

```
METHOD /merp/if_ca_fsm_crossref_badi~get_serv_assign_id.
    DATA lref_fsm_integration TYPE REF TO /merp/cl_ca_fsm_integration.

    TRY.
        " Create FSM object
        CREATE OBJECT lref_fsm_integration
          EXPORTING
            iv_mapp = iv_mapp.
      CATCH /merp/cx_core_exception_gen INTO DATA(lref_badi_exception).
        RETURN.
    ENDTRY.
    " Fetch Service Assignment from FSM if it exists
    lref_fsm_integration->query_fsm_serviceassign(
      EXPORTING
        iv_aufnr       = iv_aufnr
        iv_vornr       = iv_vornr
        iv_activity_id = iv_activity_id
      IMPORTING
        ev_id          = ev_id
        ev_activity_id = ev_activity_id
        es_oblnk       = es_oblnk
        ).
  ENDMETHOD.
```

5. Implement the */MERP/IF_CA_FSM_CROSSREF_BADI~GET_SERV_ASSIGN_STATUS_ID*:

   This method is a prerequisite for implementing relevant status updates from SAP Service and Asset Manager to the Field Service Management planning and scheduling board. The method must return the Field Service Management internal activity ID (the `id` field of the Field Service Management *Activity* entry) based on the order and operation number provided.

   Use the *QUERY_FSM_SERVICEASSIGNSTATUS* method from the */MERP/CL_CA_FSM_INTEGRATION* class to get this value based on the following code example.

   > **Note**
   >
   > The following code is an example. You may need to make additional adjustments for your environment.

```
METHOD /merp/if_ca_fsm_crossref_badi~get_serv_assign_status_id.
    DATA lref_fsm_integration TYPE REF TO /merp/cl_ca_fsm_integration.

    TRY.
        " Create FSM object
        CREATE OBJECT lref_fsm_integration
          EXPORTING
            iv_mapp = iv_mapp.
      CATCH /merp/cx_core_exception_gen INTO DATA(lref_badi_exception).
        RETURN.
    ENDTRY.

    lref_fsm_integration->query_fsm_serviceassignstatus(
        EXPORTING
          iv_aufnr       = iv_aufnr
          iv_vornr       = iv_vornr
          iv_activity_id = iv_activity_id
        IMPORTING
          ev_id          = ev_id
          es_oblnk       = es_oblnk
          ).
```

```
    ENDMETHOD.
```

6. Implement the BADI method *IS_VALID_ORDER_FOR_REPLICATION* from the BADI */MERP/CA_FSM_CROSSREF*.

   This method must return a *TRUE* (*X*) value if the supplied order ID or order type is valid for replication to Field Service Management. The status changes on the operation (activity in Field Service Management) are replicated to the Field Service Management Scheduling and Dispatching board only if a *TRUE* value is returned by the method.

   If this method isn't implemented, by default no replication of status occurs from SAP Service and Asset Manager to Field Service Management

7. Implement the *GET_ACTIVITY_ID_MULTI* method from BADI */MERP/CA_FSM_CROSSREF_BADI*.

   This method gets a set of identifiers in the *IT_ACTIVITIES* parameter. The ids will be in the format <OrderID>-<OperationNumber>. Split these identifiers to pass the orderID and the operation number to the */pacg/ecm_acti* table to retrieve the activity identifiers from the FSM. These activity identifiers should be used to query the code property of the activity DTO in the FSM. The logic for retrieving activity identifiers from the FSM will be similar to that used in the */MERP/IF_CA_FSM_CROSSREF_BADI~GET_ACTIVITY_ID* method.

> ### Note
>
> For efficiency, a single query string can contain multiple codes. Below is an example of what the query part will look like:
>
> /api/data/v4/Activity?dtos=Activity.43&query=code in (<actid1>,<actid2>...)
>
> If the query string is too long or contains too many activity IDs, the FSM will generate an error. In this case, the request will need to be sent in batches.

> ### Note
>
> For detailed code notes for implementing the logic in the *GET_ACTIVITY_ID_MULTI* method of BADI */MERP/CA_FSM_CROSSREF_BADI*, see Consulting Note for BADI Implementation with SAP Field Service Management Integration.

3.4.1.2.2 Configuring Connectivity between SAP Service and Asset Manager and Field Service Management

Context

The following configuration is needed to establish a connectivity between SAP Service and Asset Manager and Field Service Management. For information on announcing root certificate change, refer to Announcing Root Certificate Change.

Procedure

1. **Create a client in Field Service Management:**
   a. Log on to your Field Service Management administrative URL.
   b. Create a new client with the following parameters:
      - **Client Authentication Method:** CLIENT_SECRET
      - **User Groups:** Admin
   c. Save the *Client ID* and *Client Secret*.
2. **Configure STRUST in the back end:**
   a. Download the *ISRG Root X1* certificate. See the Announcing Root Certificate Change topic for more details.

      > **Note**
      >
      > The `.pem` file can be downloaded.

   b. Install the *ISRG Root X1* certificate against the *SSL Client (Anonymous)* in the Trust Manager.
3. **Create RFC destinations in the back end:**
   a. Create a destination for establishing the oAuth connection between the back end and Field Service Management with the following parameters:
      - **Name:** SAMXXXX_FSM_OAUTH
      - **Connection Type:** G (HTTP Connection to External Server)
      - **Technical Settings**
        - **Target Host:** auth.coresuite.com
        - **Path Prefix:** /api/oauth2/v1/token
      - **Logon and Security**
        1. Select *Basic Authentication*
        2. Under *User and Password* enter the client ID and client secret from *Step 1*.
        3. Under *Security Options* specify the following:
           - **SSL:** Active
           - **SSL Certificate:** ANONYM SSL Client (Anonymous)
   b. Create a destination for implementing the API calls to Field Service Management with the following parameters:
      - **Name:** SAMXXXX_FSM_API
      - **Connection Type:** G (HTTP Connection to External Server)
      - **Technical Settings**
        - **Target Host:** <cluster e.g. us/eu>.coresuite.com
      - **Logon and Security**
        1. Select *Do not use a user*.
        2. Under *Security Options*, specify the following:
           - **SSL:** Active
           - **SSL Certificate:** ANONYM SSL Client (Anonymous)

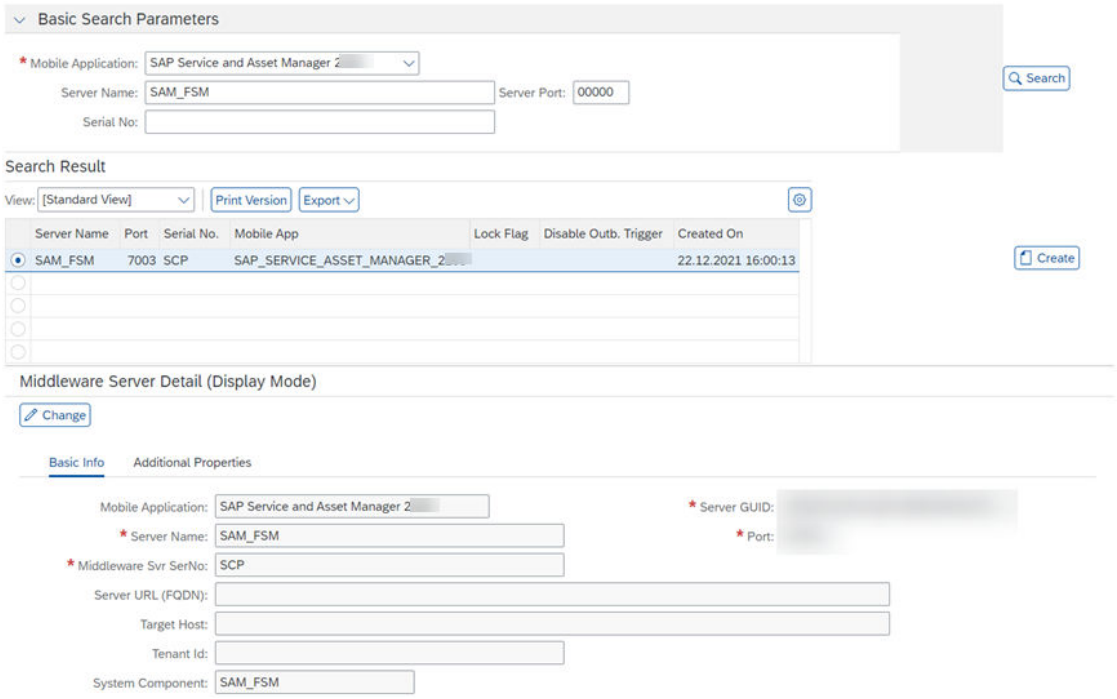
3.4.1.2.3 Configuring Server Parameters - Customer Service Back End

Context

> **Note**
>
> The parameters listed in this document are applicable for:
>
> - PM orders and CS orders on ECC and SAP S/4HANA back end systems
> - Field Service Technician and Maintenance Technician personas

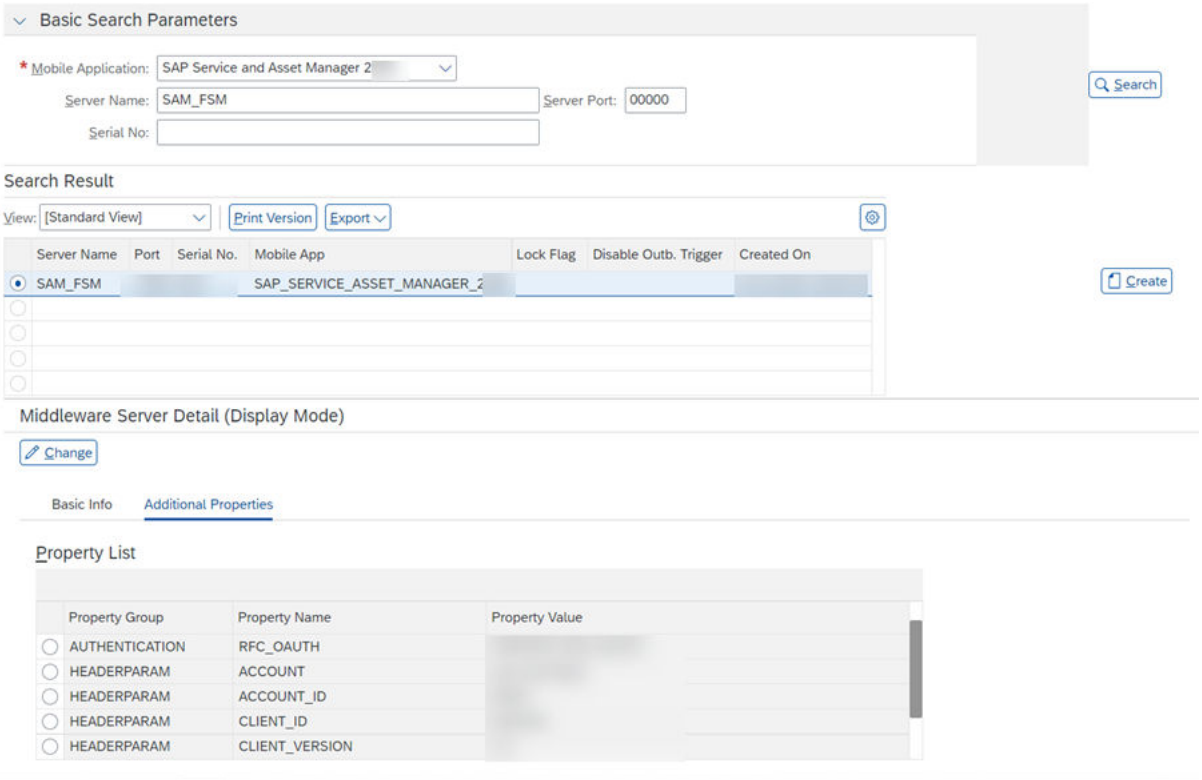
Procedure

1. Log on to the *Administration and Monitoring Portal* in the back end using transaction */SYCLO/ADMIN*. Under the *Administration* tab, select *Server Management*.
2. Create a new server with the name *SAM_FSM* for the application *SAP_SERVICE_ASSET_MANAGER_<version>*.



3. Under *Server Properties* maintain the following properties:

Property Group	Property Name	Property Value
AUTHENTICATION	RFC_OAUTH	Name of the RFC in *Step 3.1* of the Configuring Connectivity between SAP Service and Asset Manager and Field Service Management [page 187] procedure
AUTHENTICATION	RFC_API	Name of the RFC in *Step 3.2* of the Configuring Connectivity between SAP Service and Asset Manager and Field Service Management [page 187] procedure
HEADERPARAM	ACCOUNT	Field Service Management Account Name
HEADERPARAM	ACCOUNT_ID	Field Service Management Account ID
HEADERPARAM	COMPANY	Field Service Management Company Name
HEADERPARAM	COMPANY_ID	Field Service Management Company ID
HEADERPARAM	CLIENT_ID	Client ID to send to Field Service Management (e.g: SYSid.Client)
HEADERPARAM	CLIENT_VERSION	1.0



> **Note**
>
> The following additional server parameters can be defined if needed but they are **optional**. Their default values are also specified below. Changing these values may result in the need for customers to customize their back end integration code.

Property Group	Property Name	Property Value	Description
AUTHENTICATION	AUTH_TYPE	OAUTH	Authentication type used to communicate with Field Service Management – Default is OAUTH.
DTO	STATUSDEF	ServiceAssignmentStatus-Definition.9	Field Service Management Data Transfer Object (DTO) version. Can be changed if a newer version of a DTO is needed.
	ITEM	Item.23	
	EQUIPMENT	Equipment.23	
	BUSINESSPARTNER	BusinessPartner.23	
	ADDRESS	Address.21	
	PERSON	Person.24	
	SERVICEASSIGN	ServiceAssignment.28	
	SERVICECALL	ServiceCall.26	
	ACTIVITY	Activity.39	
	SERVICEASSIGNSTATUS	ServiceAssignmentStatus.15	
INTEGRATION	CREATEPERSON	admin	User for creating new objects in Field Service Management (related to SAP Service and Asset Manager only)
UI_URL_PATH	ADDRESS	/api/data/v4/Address	URI strings for the Field Service Management api call
	EQUIPMENT	/api/data/v4/Equipment	
	ITEM	/api/data/v4/Item	
	PERSON	/api/data/v4/Person	
	BUSINESSPARTNER	/api/data/v4/BusinessPartner	
	SERVICEASSIGN	/api/data/v4/ServiceAssignment	
	QUERY	/api/query/v1	
	SERVICEASSIGNSTATUS	/api/data/v4/ServiceAssignmentStatus	
	SERVICECALL	/api/data/v4/ServiceCall	
	SERVICEORDERCREATE	/service-management/api/v2/composite-tree/service-calls?autoCreateActivity=false	

Property Group	Property Name	Property Value	Description
	ACTIVITY	/api/data/v4/Activity	

4. *Save* your changes.

3.4.1.2.4 Configuring the Field Service Management Personas

Prerequisites

Ensure the *FIELD_SERVICE_TECHNICIAN* persona is added and activated in the Administration and Monitoring Portal.

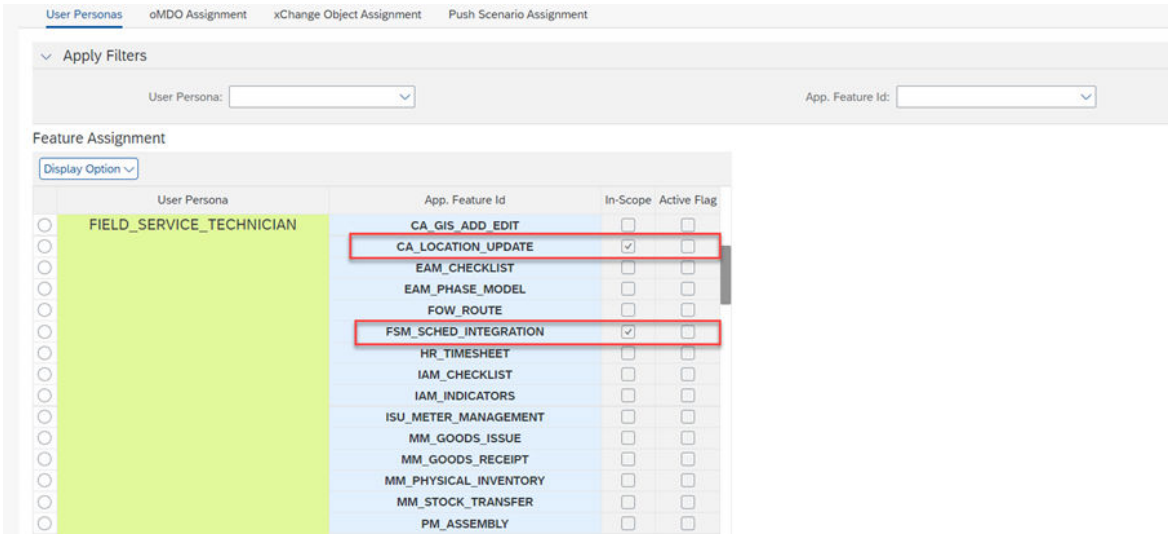
For detailed information about personas and how they work, see the Configuring Personas and Features Overview [page 87] topic and subtopics.

Context

Use the following procedure to enable the *FSM_SCHED_INTEGRATION* and *CA_LOCATION_UPDATE* features. They are disabled by default.

Procedure

1. From the ConfigPanel home screen, navigate to *Component Assignments* > *Select Mobile Application* > *User Personas tab*. You can then filter for only the *FIELD_SERVICE_TECHNICIAN* user persona, if desired.
2. Click the *Change* button.
3. Check the *Active Flag* for *CA_LOCATION_UPDATE* and *FSM_SCHED_INTEGRATION*.



4. *Save* your changes.

Next Steps

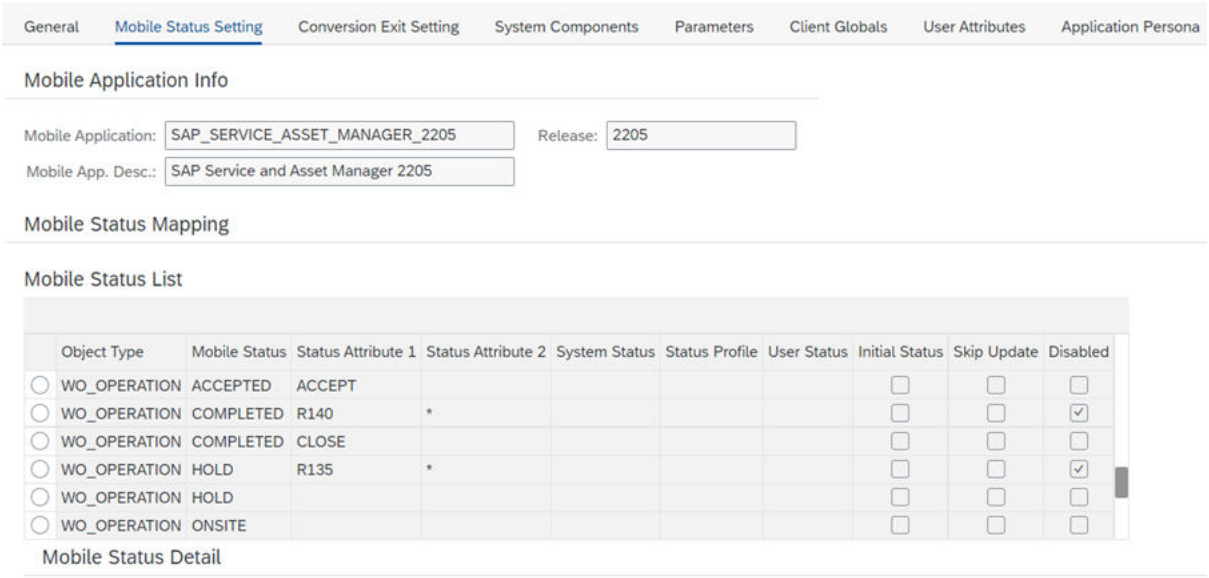
> **Note**
>
> For more information about how to configure User Location Tracking, see Location Tracking Configuration [page 452].

3.4.1.2.5 Status Configuration

The only assignment type supported for the Field Service Management solution is *Assignment Type 2*. Therefore, status changes are only supported at the operation level.

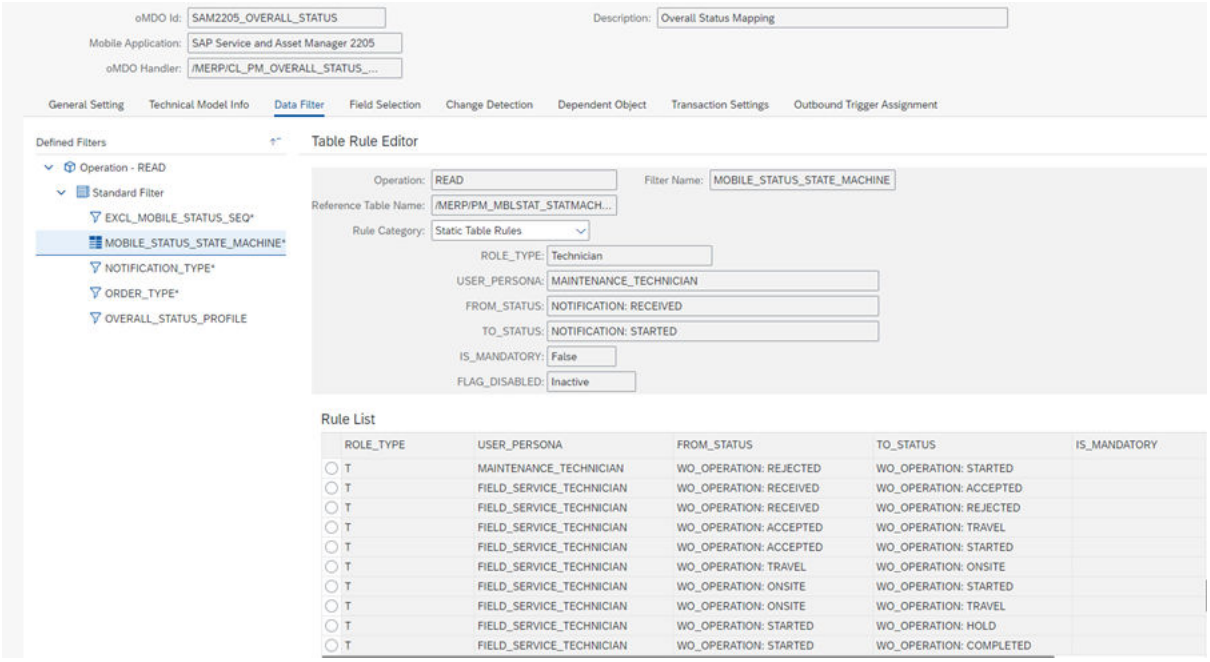
The following table shows the default SAP Service and Asset Manager statuses supported for the Field Service Technician persona as defined in the *Mobile Status Settings Configuration* on the ConfigPanel:

Object Type	Mobile Status	Initial Status (Y/N)	Status Attribute 1 (FSM status)
WO_OPERATION	RECEIVED	Y	new
WO_OPERATION	ACCEPTED		accept
WO_OPERATION	REJECTED		
WO_OPERATION	TRAVEL		travel
WO_OPERATION	ONSITE		
WO_OPERATION	STARTED		work
WO_OPERATION	HOLD		
WO_OPERATION	COMPLETED		close
WO_OPERATION	TRANSFER	No status update	



If any additional SAP Service and Asset Manager statuses are used or a custom service workflow is used in Field Service Management – the additional statuses can be configured in the *Mobile Application* > *Mobile Status Settings Configuration*. In this case, customization may be needed at the backend and/or MDK level depending on how the statuses need to be used.

The default status transitions are defined in the **SAMXXXX_OVERALL_STATUS** oMDO, *MOBILE_STATUS_STATE_MACHINE* filter. If additional status transitions are needed or existing ones need to be changed, then the filter values in this oMDO need to be changed. In this case, customization may be needed at the backend and/or MDK level depending on how the status transitions work.



3.4.1.3 FSM Smartforms Configuration

SAP Service and Asset Manager supports FSM Smartforms that allow planning board administrators to efficiently gather technician activity information in an organized way. Planning board administrators can assign Smartform instances to activities and require technicians to fill out the Smartform instance before completing the activity. Smartform instances can be associated with the following objects:

- Equipments
- Functional Locations
- Service Orders
- Service Order Items

> **Note**
>
> - For more information about using FSM Smartforms, see Smartforms Overview.
> - FSM Smartforms can be configured for Maintenance Technician as well, and used in plant maintenance scenarios. In this case, FSM Smartforms will be attached to PM work order operations instead of CS and S/4 work orders. For more information, see FSM Smartforms Configuration for Maintenance Technician [page 420].
> - The FSM Smartforms feature can be used by both Customer Service [page 177] and SAP S/4HANA [page 205] back end systems.
> - **Supported Smartforms fields**:
>   - Not all fields within Smartforms [page 195] are supported in the same way. Smartforms must be preconfigured and customized by administrators before users can fill in all the fields.
>   - For the complete list of Smartform elements available for use, refer to Template Elements section in the official *Field Service Management* documentation.

Supported Personas

This feature is applicable for the following personas:

Maintenance Technician (Pro)
Field Service Technician (Standard)
Field Service Technician (Pro)

Prerequisites

FSM Smartforms will be enabled to the persona if the feature flag of *FSM_SCHED_INTEGRATION* is turned on. To use and preconfigure the FSM Smartforms within SAP Service and Asset Manager, refer to:

- Field Service Management Scheduling - SAP Service and Asset Manager Integration [page 178]
- Configuring the Field Service Management Personas [page 192]

Configuration

Perform the following configuration step(s):

1. Configuring FSM Smartform DTO Versions [page 196]
2. Smartform Instance and Template oMDO filters [page 197]

3.4.1.3.1 Configuring FSM Smartform DTO Versions

MAIF has an oData Model that defines configurations and settings for sets of entities. Similarly, FSM has a data model for various entities, which are called DTOs. The DTOs have different versions as new features are developed for each DTO.

Context

Procedure

1. Log in to the *Administration and Monitoring Portal* in the backend (transaction code /SYCLO/ADMIN). On the *Administration* tab, select *Server Management*.
2. In the search parameters, enter:
   - Mobile Application = SAP Service and Asset Manager <VERSION>
   - Server Name = SAM_FSM
3. Select the appropriate entry in the search results and navigate to the *Additional Properties* tab in the *Middleware Server Detail* section.
4. Add the following properties in the *Property List*:

Property Group	Property Name	Property Value
HEADERPARAM	ATTACHMENT_DTO_VERSION	14
HEADERPARAM	INSTANCE_DTO_VERSION	19
HEADERPARAM	ITEMPLATE_DTO_VERSION	19

The DTO versions can be changed to a newer version if necessary. For more information on DTO versions, refer to the Field Service Management - Domain Model documentation.

5. Save your changes.

3.4.1.3.2 Smartform Instance and Template oMDO filters

Context

Technicians can not only work with pre-attached Smartforms, but also add new ones to existing operations. They can create Smartforms from Templates and attach to the objects listed in Smartforms Overview.

> **Note**
>
> The FSM Smartform Template feature is:
>
> - Applicable for both Customer Service [page 177] and SAP S/4HANA [page 205] back end systems.
> - Part of Field Service Technician Scheduling [page 178], no additional configuration steps are required.
> - Supported by the Maintenance Technician (Pro) persona, if it already has Field Service Management integration configured [page 420].

See the following oMDO filters for optional configuration of Smartforms instances and templates:

Procedure

1. Log in to the ConfigPanel in the back end (transaction code `/SYCLO/CONFIGPANEL`).
2. Navigate to *oData Mobile Data Object Configuration* > *SAP_SERVICE_ASSET_MANAGER_<VERSION>* > *SAM<VERSION>_FSM_FORM_INSTANCE*.
3. Navigate to the *Data Filter tab* > *Operation – READ* > *Standard Filter*.
4. The following filters should be noted:
   - *MAX_INSTANCES*: This filter controls the maximum number of instances that can be loaded during synchronization.
   - *GET_CLOSED*: If this filter is set to true, closed Smartform instances will also be loaded.
5. To configure *MAX_TEMPLATES*, which has the same functionality as *MAX_INSTANCES* but for Smartform instances, follow all previous steps but search for the *SAM<VERSION>_FSM_FORM_TEMPLATE* oMDO.

3.4.1.4 Expense and Mileage Configuration

SAP Service and Asset Manager supports expense and mileage entries for the Field Service Technician persona.

The configuration of separate *Activity Types* and *Work Center* combinations are required to be able to enter expenses and mileage using SAP Service and Asset Manager. Expenses and mileage are entered as *IW41* confirmations in the back end. Both planned and unplanned mileage recordings are supported. Since the Expense and Mileage entries are stored in the backend as confirmations, due to the limitation of the corresponding field in the backend, a single decimal place is supported for the Expense and Mileage values.

> **Note**
>
> Since the IW41 confirmation only supports time-related units of measurement (for example hours and minutes), dummy units of measurement are displayed on the screen to make it more user friendly. However, the confirmation is posted to the back end with the Unit of Measure `Minutes` by default.

> **Note**
>
> Expense and Mileage entries are stored in the back end as confirmations. Due to limitations of the corresponding field in the back end, a single decimal space is supported for expense and mileage values.

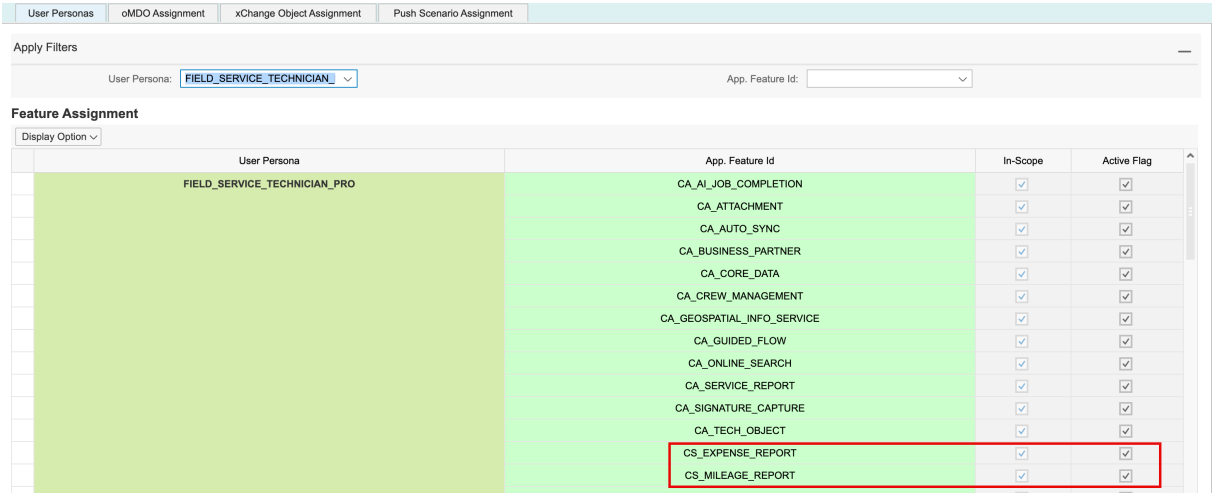
The parameters configured in the Configuring Mileage and Expense Parameters [page 198] procedure display as the *Activity Type* and *Work Center* fields in the app after you enter the order and operation number. If the *Work Center* parameter isn't defined, then this parameter is inherited from the operation. You can select a different *Activity Type* and *Work Center*, but it requires knowledge on the values that are selected to avoid errors when the data is posted to the back end.

3.4.1.4.1 Configuring Mileage and Expense Parameters

Prerequisites

Expense and mileage reporting is enabled on the mobile app when the following conditions are met:

- The user is assigned to the Field Service Technician persona.
- The *CS_EXPENSE_REPORT* and *CS_MILEAGE_REPORT* are enabled.



> **Note**
>
> You can enable the expense reporting and mileage reporting features for the Maintenance Technician persona.

Context

Use this procedure to configure the following parameters:

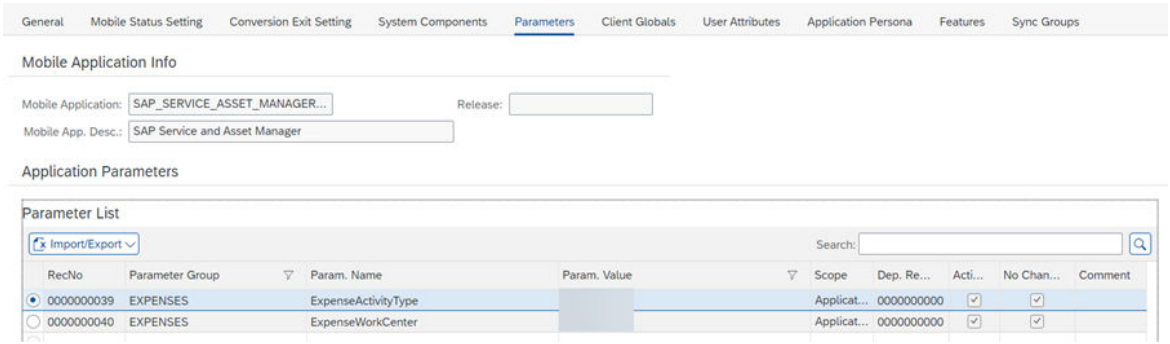
- *EXPENSES* group:
  - ExpenseActivityType: Activity type created for expenses. The defined value is the default displayed in the *Expense Type* field on the app.
  - ExpenseWorkCenter: The work center associated with the activity type defined for expenses.
- *MILEAGE* group:
  - MileageActivityType: Activity type created for mileage.
  - MileageWorkCenter: The work center associated with the activity type defined for mileage.
  - MileageUOM: The unit of measure (for example, miles or kilometers) displayed on the app.

Procedure

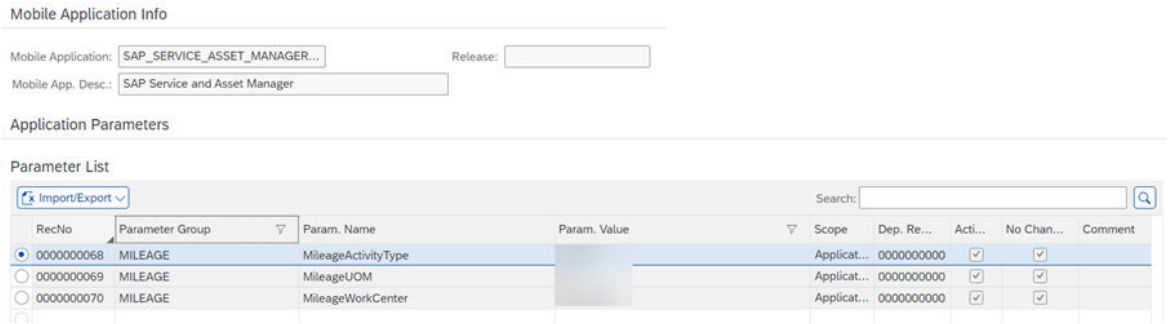
1. Using the ConfigPanel, navigate to *Mobile Application Configuration* > *Parameters tab*. In the left column, *Defined Mobile Applications*, select your application.

   The *Parameter List* populates with a list of all parameters available for the application.
2. The *ExpenseActivityType* and *ExpenseWorkCenter* parameters are found in the *EXPENSES* group. You can scroll down to find the parameter, or perform a search using the *Search* box. Highlight the desired parameter and click the *Change* button.
3. Configure the expense parameters as desired.

   > **Note**
   >
   > The UOM for expenses displayed on the SAP Service and Asset Manager screen is the currency field inherited from the order header.



4. The *MileageActivityType*, *MileageWorkCenter*, and *MileageUOM* parameters are found in the *MILEAGE* group. You can scroll down to find the parameter, or perform a search using the *Search* box.



5. Configure the mileage parameters as desired.
6. *Save* your changes.

3.4.1.4.2 Assignment Type for Planned Expenses and Mileage

When planned expenses and mileage are supported, certain assignment types are not impacted, while others must be addressed.

Since the planned expenses and mileage would involve adding additional operations, additional administrative steps or configuration may be needed to ensure that all operations, including expenses and mileage operations, are downloaded to SAP Service and Asset Manager.

Not Impacted Header Assignment Types

The following header assignment types are not impacted, because the entire order with all the operations is downloaded to the SAP Service and Asset Manager:

- Header Level Person Responsible
- Header Level Planner Group
- Header Level Business Partner
- Header Level Work Center

Assignment Types That Must Be Addressed

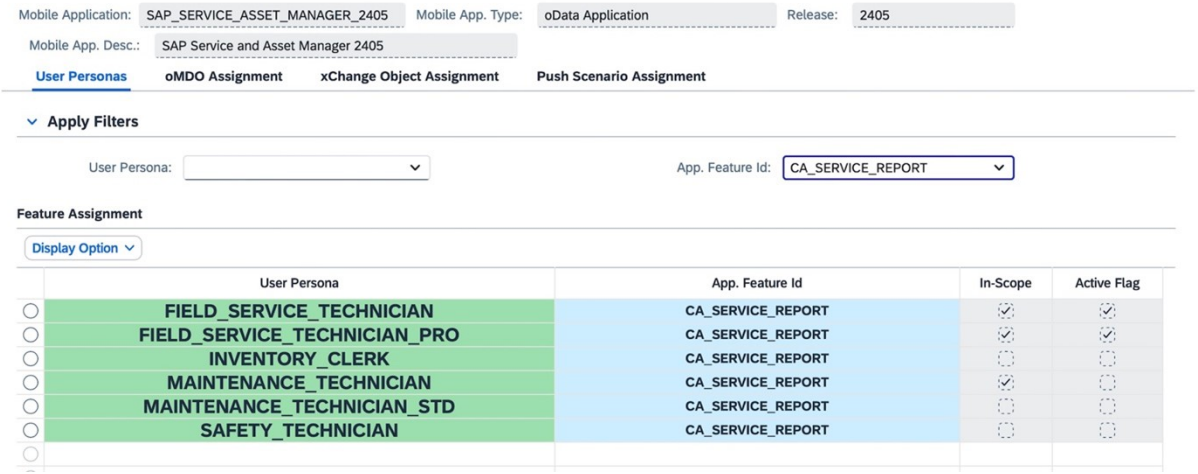
- **Operation Level Personnel Number**: To ensure that the planned expense and mileage operations are downloaded, ensure that each technician who works on the order is assigned to operations with expense and mileage activity types.
- **Sub-Operation Level Personnel Number**: To ensure that the planned expense and mileage operations are downloaded, ensure that each technician who works on the order is assigned to operations with expense and mileage activity types.

- **Capacity Requirements**: Planned operations with the expense and mileage activity types must be assigned to all technicians working on the order.
- **Operation Level Work Center**: If the customer has different work centers for mileage and expenses, a user attribute must be created to support multiple work center assignments. This user attribute must be assigned to the OPER_WORK_CENTER filter of the SAM2205_WORK_ORDER_GENERIC oMDO. Ensure that the expense and mileage work centers are also assigned to the technician via the User Administration section in the Administration and Monitoring Portal.

3.4.1.5 Service Report Template Configuration

SAP Service and Asset Manager supports service report template via the ReportTemplates entity set.

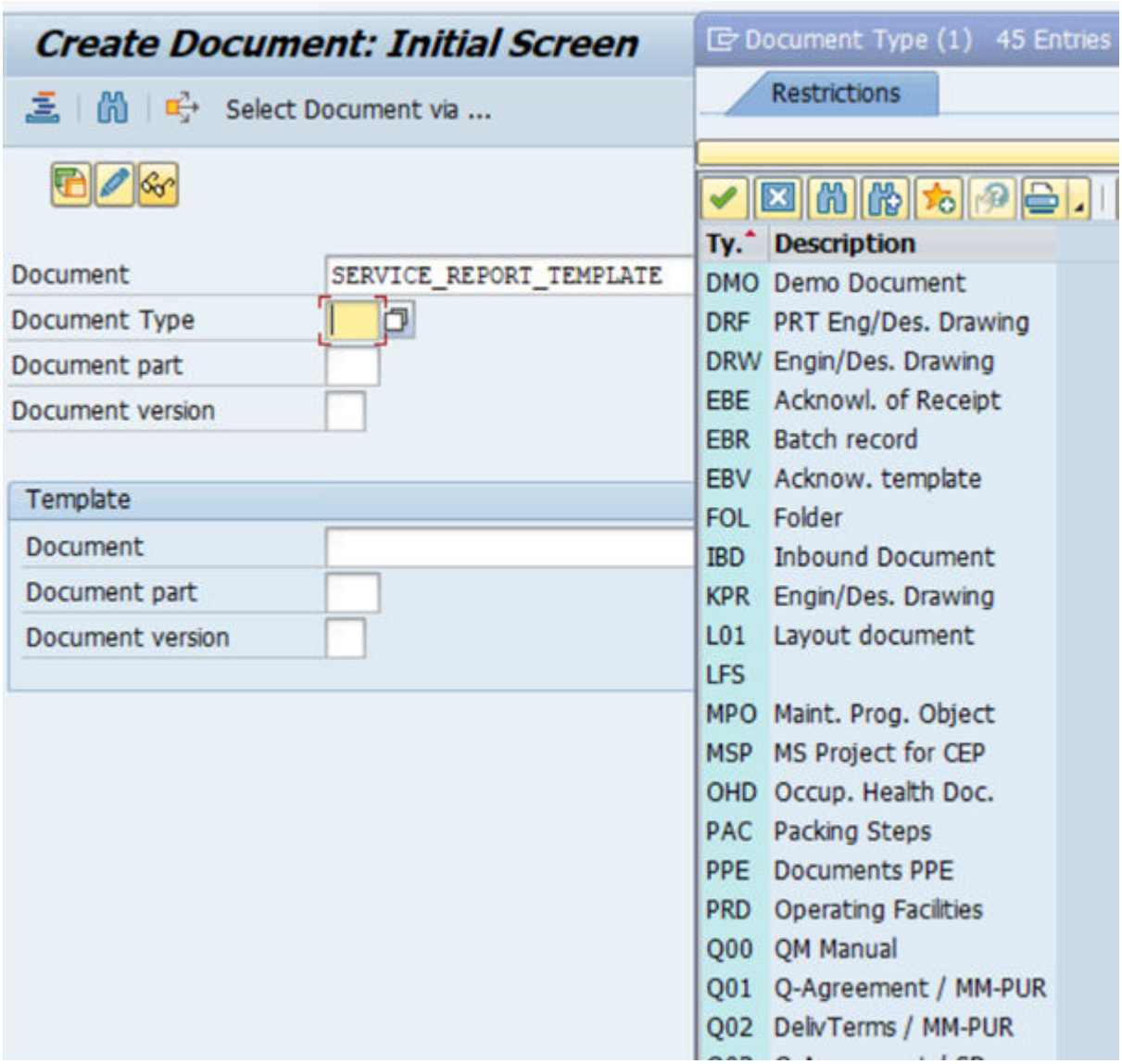
The functionality of the service report template is linked to the function CA_SERVICE_REPORT in SAP Service and Asset Manager. In the default configuration, the function CA_SERVICE_REPORT is only enabled for the Field Service Technician persona and Field Service Technician PRO persona but can also be enabled for the Maintenance Technician persona. This function is not applicable to the Inventory Technician persona and Maintenance Technician STD persona.



From the SAP backend perspective, service report template is configured as DMS document via t-code CV01N. Customer is required to configure report template in SAP backend prior to using Service Report functionality in SAP Service and Asset Manager.

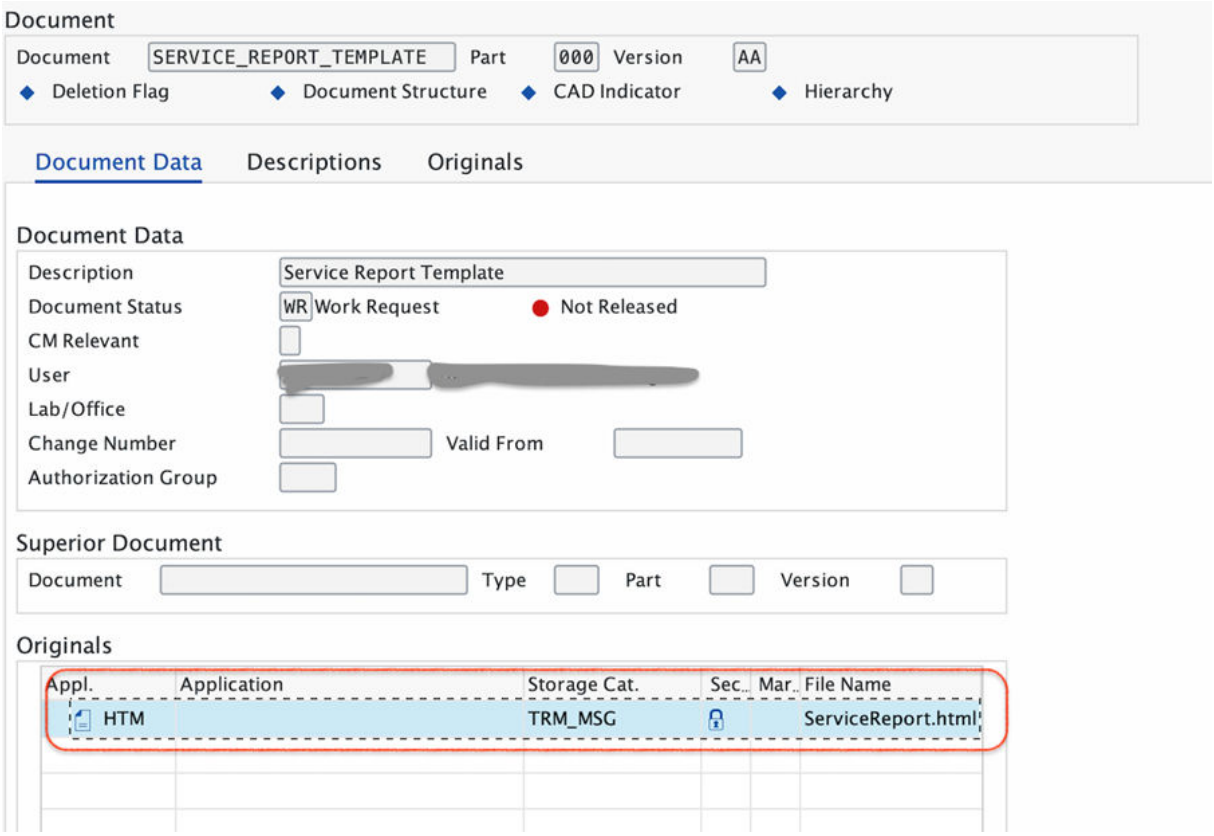
> **Note**
>
> SAP Service and Asset Manager does not provide any default service report template.

DMS documents support different document types, so the customer is able to use any type of document as long as it supports the HTML file.



Customer can create a service report template under any name using t-code CV01n. However, only the HTML file must be uploaded to the DMS document. The service report template is not linked to any business object.

> ⓘ Note
>
> Use this path to download the service report template: *SAPAssetManager.brandingsdk-2205.0.200-ms-06-27 2* > *Resources* > *ServiceReport.html*.



Once customer has created a service report DMS document in backend, they need to proceed to the Configuration Panel to configure appropriate filter or filters for service report template to be downloaded to SAP Service and Asset Manager.

> **Note**
>
> Without configuring oMDO filter in the Configuration Panel, no service report template would be downloaded.

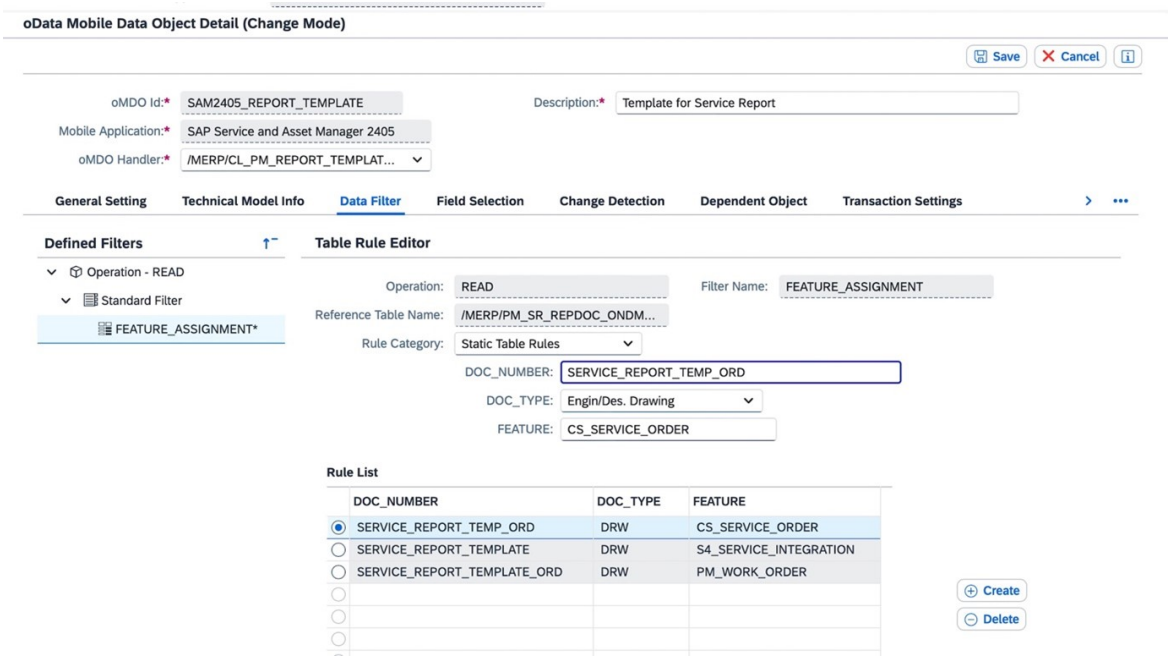
3.4.1.5.1 Configuring Service Report Template

Context

Procedure

1. Navigate to the Configuration Panel. In the Change Mode, open oData Mobile Data Object Configuration. Choose the SAM2405_REPORT_TEMPLATE oMDO configuration.
2. Navigate to *Data Filter* > *Standard filter*.
3. Expand *Standard Filter* > *FEATURE_ASSIGNMENT*.
4. Enter the name of the DMS document (as you created for the service report template using t-code CV01N) into the DOC_NUMBER filter, select the document type in the DOC_TYPE field and enter feature ID in the FEATURE field.

   Note that you can potentially configure different service report templates for PM order, S4 order and CS order (as shown below). Configure a filter with the same DOC_NUMBER and DOC_TYPE if the same report template is used for all types.



3.4.1.6 FSM SAP Cloud Integration

SAP Service and Asset Manager supports integration with **SAP S/4HANA** and **Field Service Management** for Plant Maintenance Orders using *SAP Cloud Integration (SCI)*, requiring specific configuration. This integration is beneficial for streamlining maintenance processes and enhancing operational efficiency.

To enable this feature in the SAP Service and Asset Manager, ensure that *SAP Cloud Integration* is configured for Plant Maintenance Orders. For detailed configuration procedure, refer to Configure Maintenance Order Integration.

By default, SAP Service and Asset Manager supports the **Proaxia** [page 180] integration for Plant Maintenance Orders. To switch to *SAP Cloud Integration*, add the specified parameter to the *SAM_FSM Server* configuration. This parameter is already defined as part of the FSM integration configuration. For more information, refer to Configuring Server Parameters – Customer Service Back End.

Required Server Parameter

To activate SAP Cloud Integration for Plant Maintenance Orders, configure the following:

Property Group: `INTEGRATION`

Property Name: `INTEGRATION_TYPE`

Property Value:

`SCI`

3.4.2 Field Service Technician Configuration for SAP S/4HANA Service Order Scenario

- Configuration Prerequisites and Limitations - Field Service Technician on SAP S/4HANA Back End [page 205]
- Configuring Connectivity between SSAM and FSM [page 206]
- Configuring Server Parameters - SAP S/4HANA Back End [page 208]
- Configuring Persona [page 211]
- Configuring Statuses [page 212]
- Auto Release of S4 Service Orders [page 213]
- Configure the Employee Responsible Application Parameter [page 214]
- Configuring Dynamic Predefined Text in the FSM Text Input Control [page 215]

3.4.2.1 Configuration Prerequisites and Limitations - Field Service Technician on SAP S/4HANA Back End

Prerequisites

- **Supported Smartforms fields**:
  - Not all fields within Smartforms [page 195] are supported in the same way. Smartforms must be preconfigured and customized by administrators before users can fill in all the fields.
  - For the complete list of Smartform elements available for use, refer to Template Elements section in the official *Field Service Management* documentation.

Limitations

Currently, the Field Service Technician persona (**SAP S/4HANA back end**) has the following limitations:

- In the case of configuring **multiple** *Plant*, *Storage Location* and *Work Center* parameters:
  - For the Vehicle Stock [page 560] feature, a *Plant* and *Storage Location* is used to identify the vehicle. Therefore, if you have multiple values, the feature **will not work**.
  - When adding a Part, the *Plant* and *Storage Location* are defaulted from *WRK* and *LAG* respectively; therefore, we **recommend to maintain only a single value in each**.

  > → Tip
  >
  > For more information, see Recommended Configuration for Multiple Plants and Work Centers [page 111].

- The Maintenance Technician **External** and Field Service Technician **External** personas **cannot** be used with other personas. Users may be assigned only one of these personas and must not be assigned any additional personas.
- The Field Service Technician **Professional** persona on the SAP S/4HANA back end system is currently **not supported**.
- See FSM Integration Support Matrix [page 176] for the supported integration types.

3.4.2.2 Configuring Connectivity between SSAM and FSM

Prerequisites

Ensure that a basic integration structure exists between the S/4 Service module in the S/4HANA backend and the FSM to enable data replication between the SAP backend and the FSM.

The following replication scenarios must already be active and implemented between the SAP ECC or S/4HANA backend and the FSM:

1. Status Updates: Status updates from SSAM will be transmitted to the FSM Planning and Dispatching Tooll. Since the FSM only supports Activity (Item) level assignment, status transitions are only supported for assigning a service item to a business partner. Only statuses mapped to FSM service workflow statuses will be transferred to the FSM.
2. Technician Location Tracking: The technician location obtained from SSAM will be updated in FSM so that it can be seen on the FSM Service Map.

   > ⓘ Note
   >
   > For more information about how to configure User Location Tracking, see Location Tracking Configuration [page 452].

3. FSM Smart Forms: FSM Smart Forms can be assigned to a service item, downloaded and completed in SSAM.

> **Note**
>
> Rejection and transfer of items is not supported in SSAM with FSM scheduling integration scenario.

For more information, refer to the Integration with SAP Field Service Management topics.

Context

Procedure

1. Create a client in SAP FSM
   - Log on to your FSM administrative URL
   - Create a new client with the following parameters:
     - Client Authentication Method = CLIENT_SECRET
     - User Groups = Admin
     - Save the Client Id and Client Secret
2. Configure STRUST in the SAP Backend
   - Download the ISRG Root X1 certificate. The .pem file can be downloaded.

   > **Note**
   >
   > For more information, refer to the Announcing Root Certificate Change topic.

   - Install the ISRG Root X1 certificate against SSL Client (Anonymous) in the Trust Manager
3. Create RFC Destinations in the SAP Backend
   1. Create a destination for establishing the oAuth connection between the SAP backend and FSM with the following parameters:
      - Name: <e.g. SSAMXXXX_FSM_OAUTH>
      - Connection Type: G (HTTP Connection to External Server)
        Under Technical Settings:
        - Target Host: auth.coresuite.com
        - Path Prefix: /api/oauth2/v1/token

        Under Logon & Security:
        - Select Basic Authentication
        - In the User and Password section, enter the client ID and client secret from step 1
        - In the Security Options section, specify the following:
          - SSL = Active
          - SSL Certificate = ANONYM SSL Client (Anonymous)
   2. Create a destination for implementing the API calls to FSM with the following parameters:

   - Name: <e.g. SSAMXXXX_FSM_API>

- Connection Type: G (HTTP Connection to External Server)
  Under Technical Settings:
  - Target Host: us.coresuite.com

  Under Logon & Security:
  - Select Do not use a user
  - In the Security Options section, specify the following:
    - SSL = Active
    - SSL Certificate = ANONYM SSL Client (Anonymous)

3.4.2.3 Configuring Server Parameters - SAP S/4HANA Back End

Context

For the Field Service Management integration you need to configure the *SAM_FSM* server with required connectivity parameters as described in the following procedures:

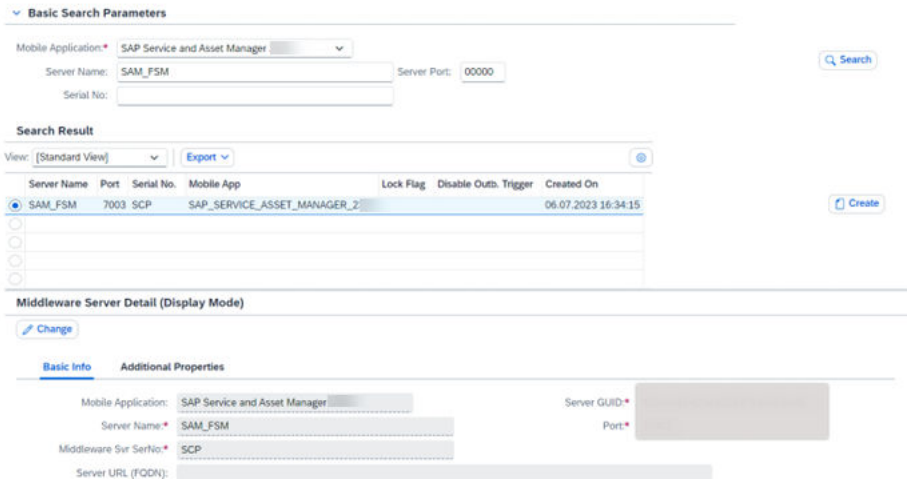
- Configure FSM General Connectivity [page 208]
- Configure FSM Smartform DTO Versions [page 210]

> ⓘ Note
>
> - MAIF has an oData Model that defines configurations and settings for sets of entities. Similarly, FSM has a data model for various entities, which are called DTOs. The DTOs have different versions as new features are developed for each DTO, and DTO versions can be changed to a newer version if necessary. For more information on DTO versions, refer to Field Service Management - Domain Model Overview.
> - The properties listed in this document are mostly specific to the SAP S/4HANA **Service Order** scenario.

Procedure

Configure FSM General Connectivity

1. Log in to the administration and monitoring portal in the backend (transaction /SYCLO/ADMIN). On the *Administration* tab, select *Server Management*.
2. Create a new server with the name *SAM_FSM* for the application *SAP_SERVICE_ASSET_MANAGER_<version>*.



3. On *Server Properties* tab, save the following properties:

Property Group	Property Name	Property Value
AUTHENTICATION	RFC_OAUTH_S4	<Name of the RFC in Step 3.a> RFC_OAUTH_S4: <e.g., SSAM2511_FSM_OAUTH>
AUTHENTICATION	RFC_API_S4	<Name of the RFC in Step 3.b> RFC_API_S4: <e.g., SSAM2511_FSM_API>
HEADERPARAM	ACCOUNT_S4	<FSM Account Name>
HEADERPARAM	ACCOUNT_ID_S4	<FSM Account Id>
HEADERPARAM	COMPANY_S4	<FSM Company Name>
HEADERPARAM	COMPANY_ID_S4	<FSM Company ID>
HEADERPARAM	CLIENT_ID	<Client ID to send to FSM. E.g SY-Sid.Client>
HEADERPARAM	CLIENT_VERSION	1.0

The following additional server parameters can be defined as needed, but they are not mandatory. Their default values are listed below. Changing these values may result in having to refine the backend integration code.

Property Group	Property Name	Property Value	Description
AUTHENTICATION	AUTH_TYPE	OAUTH	Authentication type used to communicate with FSM – Default OAUTH
DTO	STATUSDEF	ServiceAssignmentStatus-Definition.9	FSM Data Transfer Object (DTO) version. Can be changed if a newer version of a DTO is needed.
	ITEM	Item.23	
	EQUIPMENT	Equipment.23	
	BUSINESSPARTNER	BusinessPartner.23	

Property Group	Property Name	Property Value	Description
	ADDRESS	Address.21	
	PERSON	Person.24	
	SERVICEASSIGN	ServiceAssignment.28	
	SERVICECALL	ServiceCall.26	
	ACTIVITY	Activity.39	
	SERVICEASSIGNSTATUS	ServiceAssignmentStatus.15	
INTEGRATION	CREATEPERSON	admin	User to create new objects in FSM (applies to SSAM only)
UI_URL_PATH	ADDRESS	/api/data/v4/Address	URI strings for calling FSM api
	EQUIPMENT	/api/data/v4/Equipment	
	ITEM	/api/data/v4/Item	
	PERSON	/api/data/v4/Person	
	BUSINESSPARTNER	/api/data/v4/BusinessPartner	
	SERVICEASSIGN	/api/data/v4/ServiceAssignment	
	QUERY	/api/query/v1	
	SERVICEASSIGNSTATUS	/api/data/v4/ServiceAssignmentStatus	
	SERVICECALL	/api/data/v4/ServiceCall	
	SERVICEORDERCREATE	/service-management/api/v2/composite-tree/service-calls?autoCreateActivity=false	
	ACTIVITY	/api/data/v4/Activity	

Configure FSM Smartform DTO Versions

4. Log in to the *Administration and Monitoring Portal* in the backend (transaction code /SYCLO/ADMIN). On the *Administration* tab, select *Server Management*.
5. In the search parameters, enter:
   - Mobile Application = SAP Service and Asset Manager 2511
   - Server Name = SAM_FSM
6. Select the appropriate entry in the search results and navigate to the *Additional Properties* tab in the *Middleware Server Detail* section.
7. Add the following properties in the *Property List*:

Property Group	Property Name	Property Value
HEADERPARAM	ATTACHMENT_DTO_VERSION	14

Property Group	Property Name	Property Value
HEADERPARAM	INSTANCE_DTO_VERSION	19
HEADERPARAM	ITEMPLATE_DTO_VERSION	19

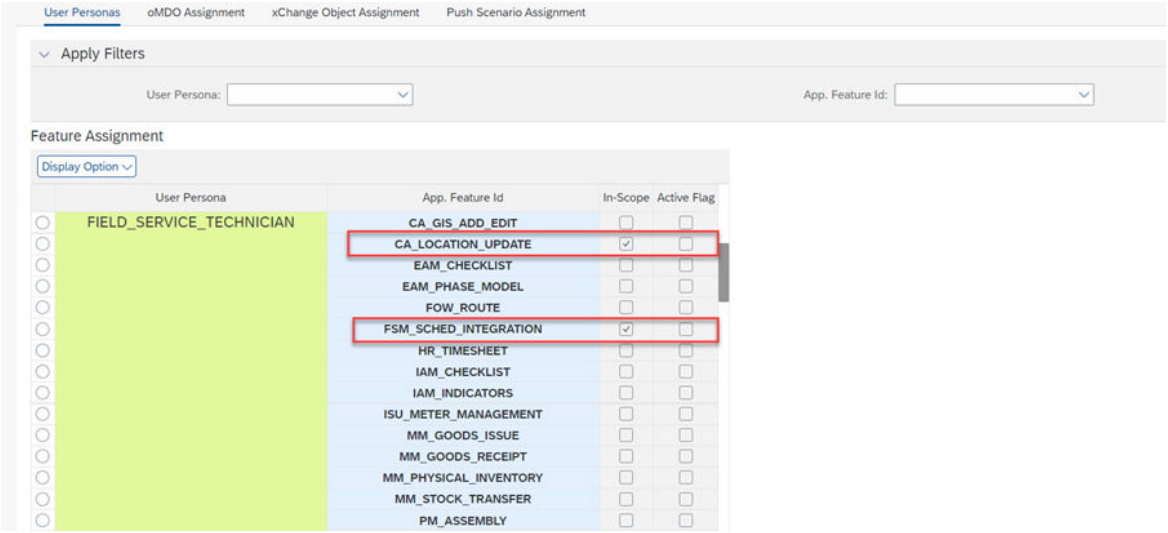
8. Save your changes.

3.4.2.4 Configuring Persona

Context

The following configurations are required to use the FSM scheduling integration scenarios in FSM:

1. You must add the FIELD_SERVICE_TECHNICIAN persona assigned to the user.
2. In the configuration panel, navigate to the component assignment for the mobile application and ensure that the FSM_SCHED_INTEGRATION and CA_LOCATION_UPDATE features are enabled, as they are disabled by default.



> **Note**
>
> For more information about configuring:
>
> - User Location Tracking, see Location Tracking Configuration [page 452].
> - FSM Crowd Service Integration, see FSM Crowd Service Configuration [page 411].

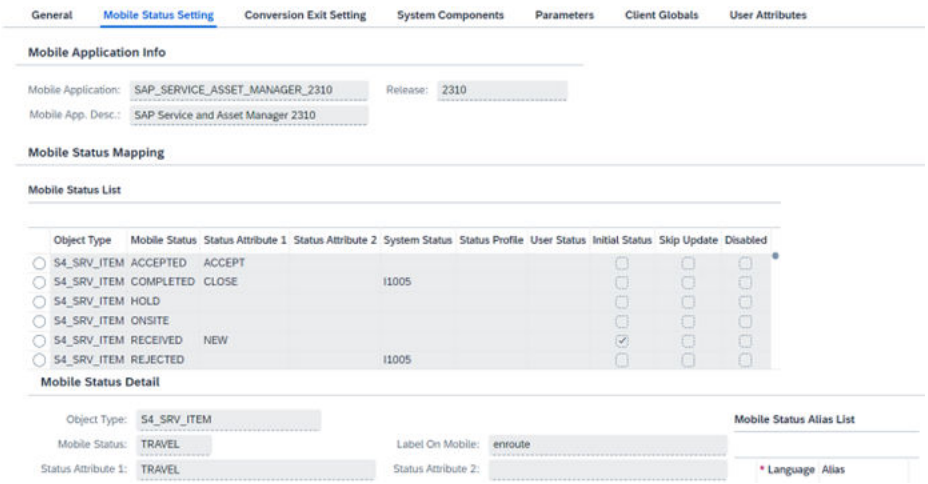
3.4.2.5 Configuring Statuses

Context

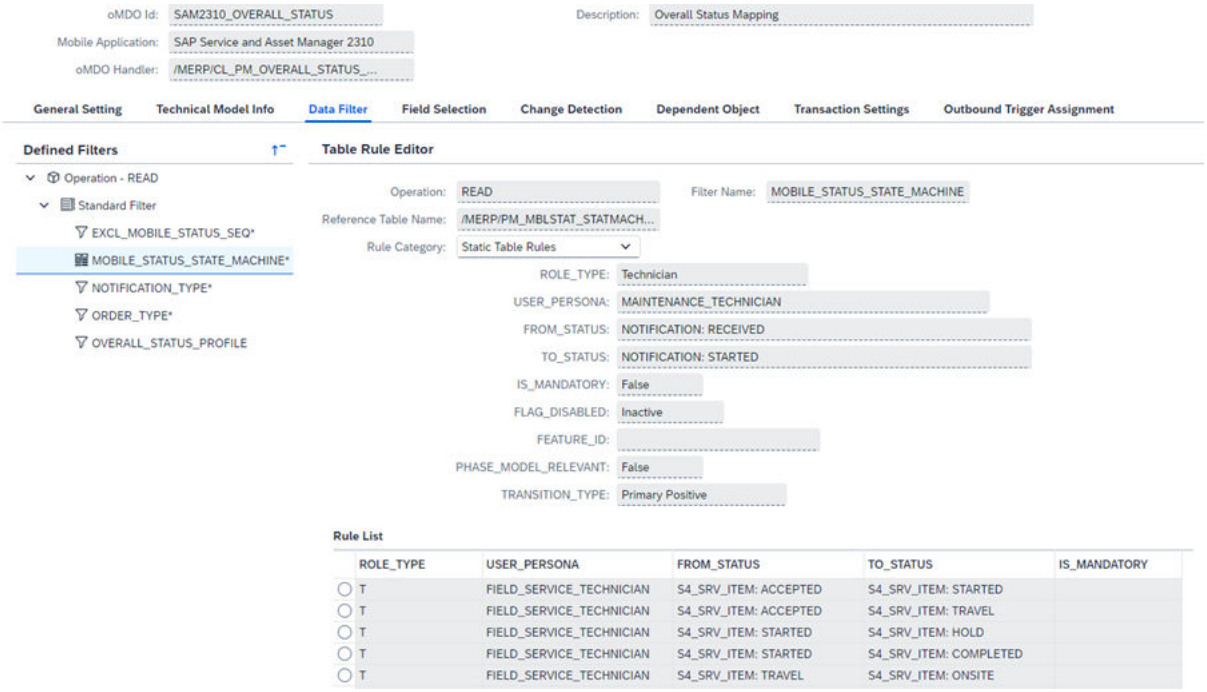
For the FSM scenario, only assignment type 2 is supported, and status changes are therefore only supported at the operation level. The default SSAM statuses supported for the Field Service Technician persona are defined in the *Mobile Application* > *Mobile Status Settings* configuration:

Object Type	Mobile Status	Initial Status (Y/N)	Status Attribute 1 (FSM status)
S4_SRV_ITEM	RECEIVED	Y	new
S4_SRV_ITEM	ACCEPTED		accept
S4_SRV_ITEM	TRAVEL		travel
S4_SRV_ITEM	ONSITE		
S4_SRV_ITEM	STARTED		work
S4_SRV_ITEM	HOLD		
S4_SRV_ITEM	COMPLETED		close
S4_SRV_ITEM	TRANSFER	No status update	

If any additional SSAM statuses are used or a custom service workflow is applied in the FSM then additional statuses can be configured in the *Mobile Application* > *Mobile Status Settings* configuration. In this case it may require customization at the back end and/or MDK level depending on how the statuses are to be used.



The default status transitions are defined in the oMDO SSAMXXXX_OVERALL_STATUS, filter MOBILE_STATUS_STATE_MACHINE. If additional status transitions are required or existing ones need to be modified, the filter values in this oMDO must be changed. This may require customization at the back end and/or MDK level depending on how the status transitions work.

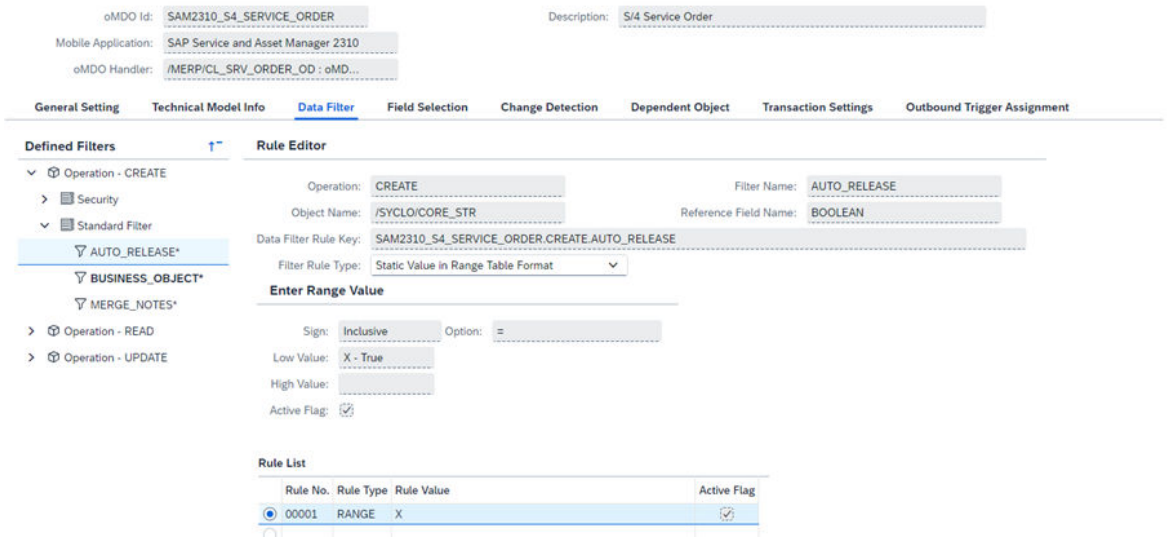


3.4.2.6 Auto Release of S4 Service Orders

When a service order is created in SSAM, you can configure that the service order is automatically released when it is published in SAP.

To set up automatic release of an order, you must perform the following configuration:

- Configure the AUTO_RELEASE filter for the CREATE operation in oMDO SAMXXXX_S4_SERVICE_ORDER - Filter I = 'X' must be active.



3.4.2.7 Configure the Employee Responsible Application Parameter

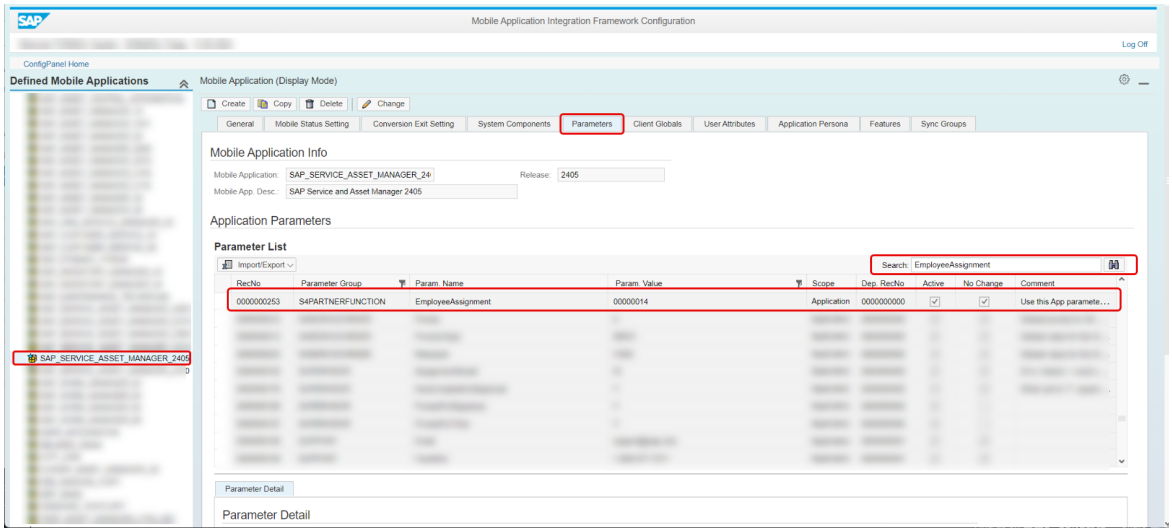
Context

When a user is creating a Service Order or Service Request, you can update the Application Parameter for the employee responsible field (partner function) so that the back-end will set the right partner function, based on your configuration. This Application Parameter will be also used by the client to send it to the back-end as a partner function value for transferring Service Orders and Service Requests.

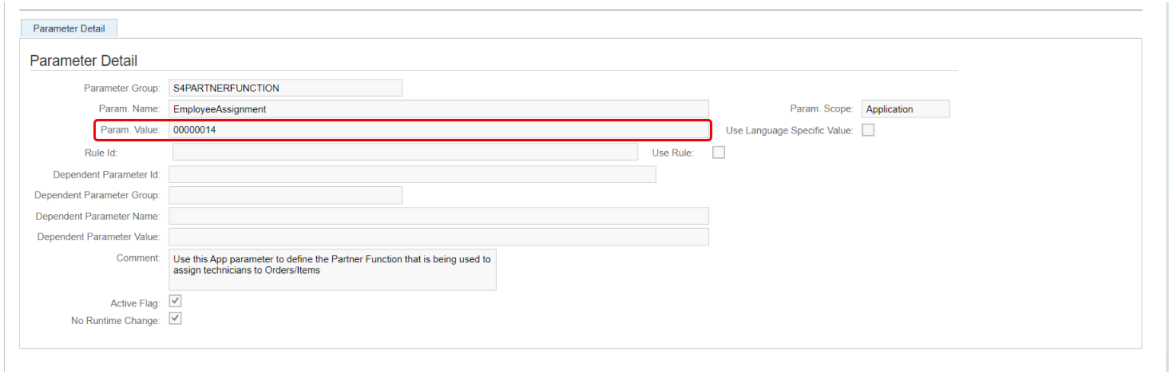
To update the parameter, perform the following steps:

Procedure

1. On the *Configuration Panel*, navigate to *Mobile Application Configuration*.
2. Select your application from the list, go to the *Parameters* tab, search for the parameter *EmployeeAssignment* and click on it.



3. Enter *Change mode*, and under *Parameter Detail*, set Parameter Value to *00000014*.
4. Click *Save*.



3.4.2.8 Configuring Dynamic Predefined Text in the FSM Text Input Control

In the text input control of the FSM smart form, dynamic texts in the @ref (<FSMentity.property>) format are supported. In such a case, a corresponding cross-reference to the FSM entity property must be supported within the MAIF framework so that the SAP Service and Asset Manager client can substitute the correct value from the corresponding MAIF entity.

These cross-reference values must be configured in SAM2405_FSM_FSM_FORM_TEXT_TEXT_CRREF OMDO, the READ filter is DYNAMIC_TEXT_CROSSREF.

The following fields must be specified:

- FSM Entity Property Name (such as, ServiceCall.externalId)
- SSAM Entity Property Name (such as, MyWorkOrderHeader.OrderId)
- SSAM Persona (such as, MAINTENANCE_TECHNICIAN)
- FeatureID (such as, PM_WORK_ORDER)

The default cross-reference values supported by SAP Service and Asset Manager are already configured in OMDO. You can add new entries for new or additional values that need to be supported.

> ⓘ Note
>
> Adding additional cross-reference values require adjustments to the SSAM MDK code.

3.5 Safety Technician Configuration

Once the Safety Technician persona is enabled for the user [page 89], you can refer to this section of the guide for additional configurations.

> ⓘ Note
>
> From **2410 onwards**, the configuration of Safety Technician features changes from persona-based feature enablement to feature checks. Meaning, only those features can be set to **Active**, which are already **In scope** for a given persona.

Key Feature Configurations

- Assignment Management of Safety-Related Features [page 261]
- Catalog Profiles Configuration [page 310]
- Isolation Certificate Configuration [page 446]
- Operational Item Configuration [page 521]
- Work Approval Configuration [page 563]

- Work Permit Configuration [page 565]
- Work Permit Approvals Configuration [page 569]

> **Note**
>
> For a comprehensive list of the latest features supported by the Safety Technician persona, see Features and Personas Configuration Matrix.

Related Documents

- Safety Technician Persona User Guide
- Work Clearance Management (PM-WCM) in *SAP ERP* documentation.
- Supported SAP Transaction Codes for SAP Service and Asset Manager [page 602].

3.5.1 Configuration Prerequisites and Limitations - Safety Technician Persona

Prerequisites

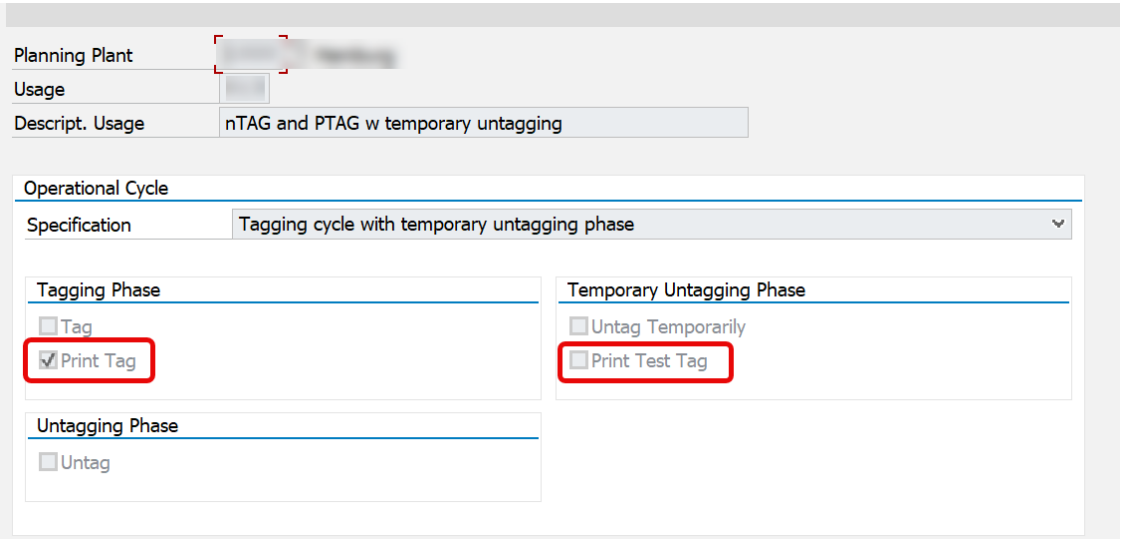
There are a few guidelines that must be applied to the SAP system for the user to be able to use the safety technician persona:

- The https://me.sap.com/notes/3262754 SAP note: On ECC, SMERP software component, Safety Technician persona is available **only on SP13 or higher**.
- The https://launchpad.support.sap.com/#/notes/2551483 SAP note: No transfer of lock number for item maintenance for API.
  Lock numbers are not transmitted during the maintenance of existing items in the work clearance document using the API used by the SAP Service and Asset Manager mobile application. This is necessary because safety technician persona can enter the physical lock number during the tagging process.
- The https://launchpad.support.sap.com/#/notes/3277604 SAP note: Data provision for Asset Management.
  Use BAdI/Exit to effectively delta-synchronize the WCM data for SAP Service and Asset Manager.
- The https://launchpad.support.sap.com/#/notes/2431765 SAP note: Processing the user status in the APIs for WCM objects.
  Use the WCM APIs to execute function codes (ACTION_EXECUTE suffix) to support setting or resetting the user status. User status can be entered in Mobile Status configuration at the Syclo Configpanel.

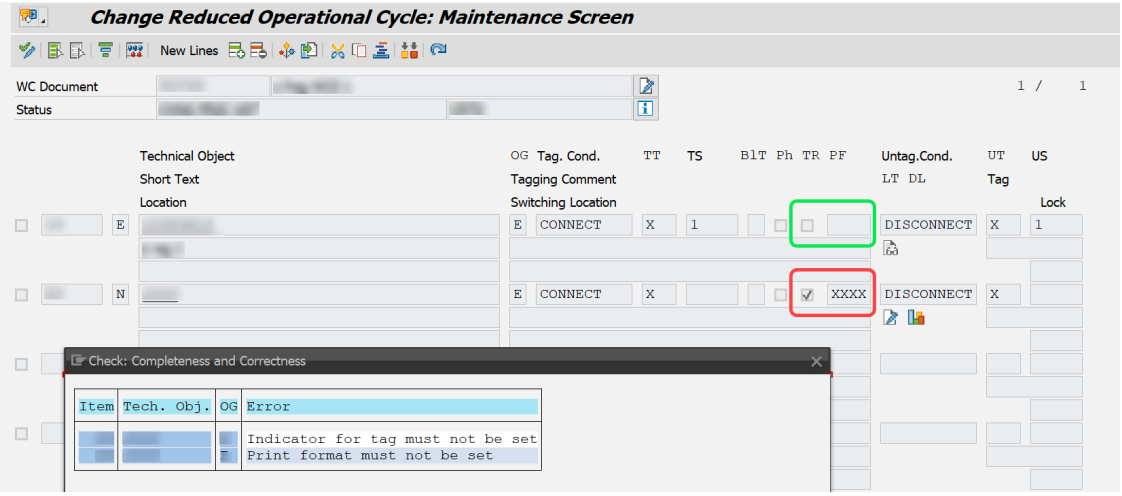
Limitations

Currently, the Safety Technician persona has the following limitations:

- For the Safety Technician persona, both standard and enhanced models are supported (see Architecture in *SAP ERP* documentation). However, Work Approval [page 563] is **only** available in the enhanced model.
- You can add Operation Items to an Isolation Certificate **only** if it's status is set to *Change* mode, by using the *Revoke Prepared* button. See Isolation Certificate Detail Screen for more information.
- When creating and configuring work orders as dependent objects [page 225], assignments at the operation level are **not** supported, only at work order header level.
- When creating and configuring usage types [page 226]:
  - The following Operational Cycle types are supported:
    - Tagging cycle **without** temporary untagging phase
    - Tagging cycle **with** temporary untagging phase (limited support from 2505 release)
    - No items
  - The following Operational Cycle types are **not** supported:
    - Test cycle
  - If the *Print Tag* checkbox is selected, the user will not be able to set the Isolation Certificate to prepared **in the mobile application**. However, the user will still be able to create the Operational Item.
  - If the *Print Tag* checkbox is selected **only**, and the *Print Test Tag* is **not**, then an error will occur while setting the status to prepared:



- If the *Print Tag* checkbox is selected, for **all** the Operational Items (added to the Isolation Certificate), the *TR* and *PF* fields **must be empty**. Otherwise, an error will occur while setting the status to prepared:



- Working with SAP Dynamic Forms [page 9]:
  - Safety Technicians can **create, edit and submit** Forms attached to Work Permits, Isolation Certificates and Other Certificates. However, Forms attached to other object types (e.g., Work Orders, Notifications) are **read-only**. Additionally:
    - Work Permits in *Closed* status are **read-only** as well.
    - Isolation Certificates and Other Certificates in *Closed* status **will not be downloaded** to the client by default.

3.5.2 General Feature Configuration - Safety Technician Persona

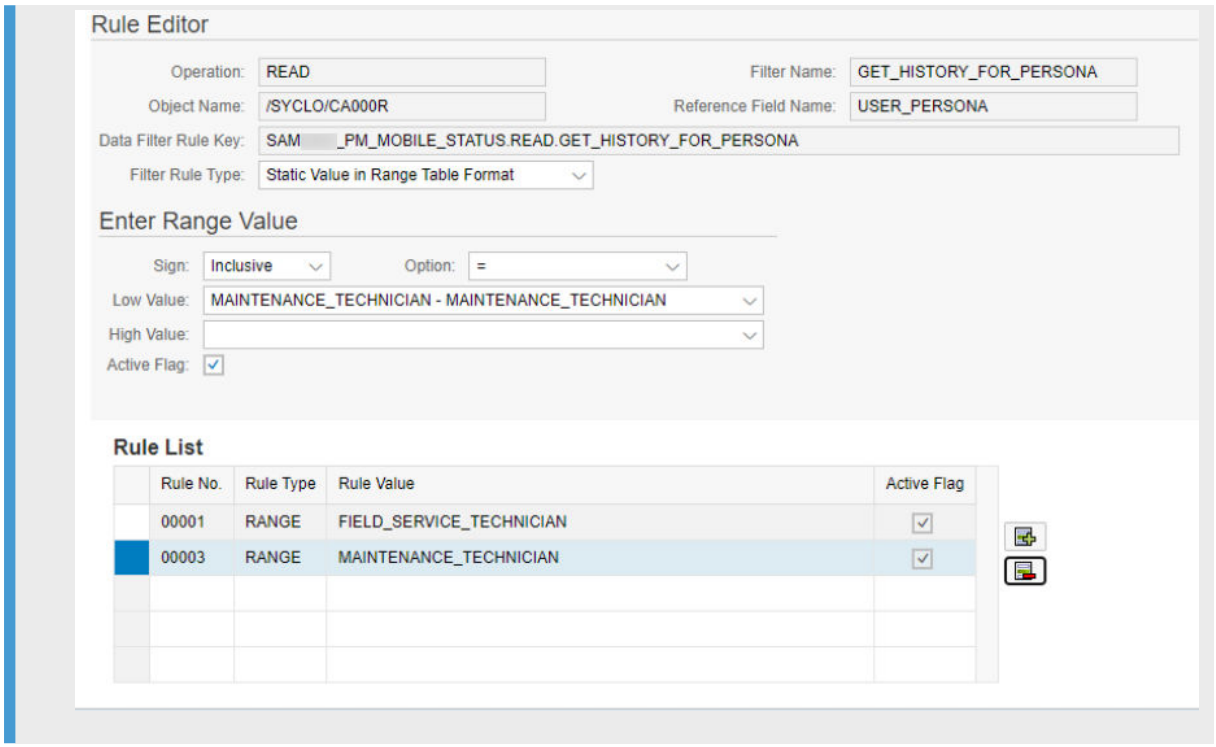
For the Safety Technician persona in general as well as for a number of safety-related features to work, you must enable the *WCM_COMMON* feature.

Supported Personas

This feature is applicable for the following personas:

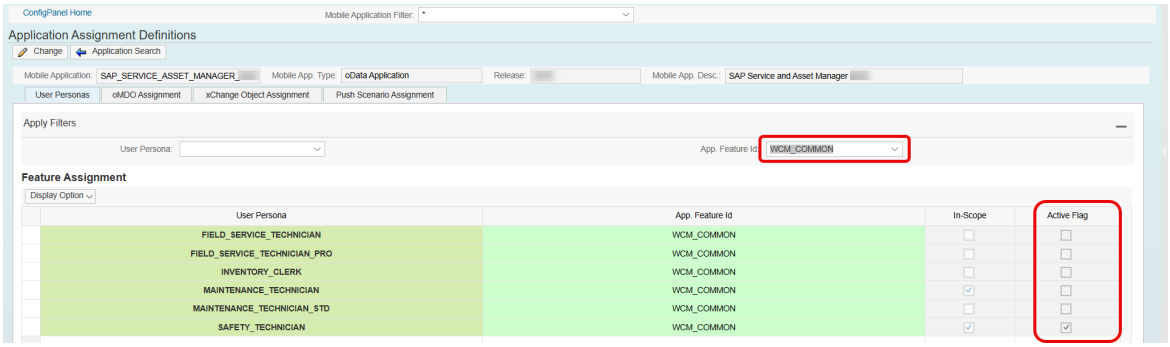
Maintenance Technician (Pro)
Safety Technician

> **Note**
>
> - For the Maintenance Technician (Pro) persona, this feature is only available from 2410 version.
> - If the user uses Safety Technician (WCM) features via the Maintenance Technician (Pro) persona, you need to add the persona to the data filter *SAMXXXX_PM_MOBILE_STATUS* > *GET_HISTORY_FOR_PERSONA*:



Procedure

1. On the Configuration Panel, go to *Component Assignments* and select your application from the list.
2. In the *App. Feature Id* dropdown, select *WCM_COMMON*.
3. Enter *Change mode* and set the feature to *Active* for relevant persona(s) [page 218].



4. Save your changes.

3.5.3 Mobile Application Parameters - Safety Technician Persona

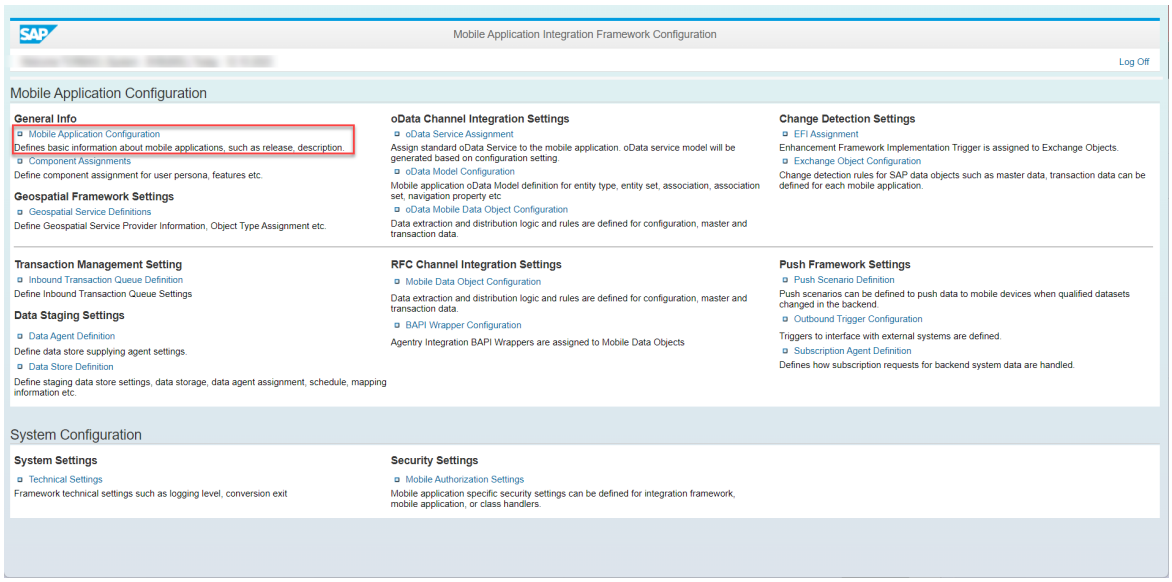
Context

For the Safety Technician persona, use the following mobile app settings to get some entities disappear and make the signature optional.

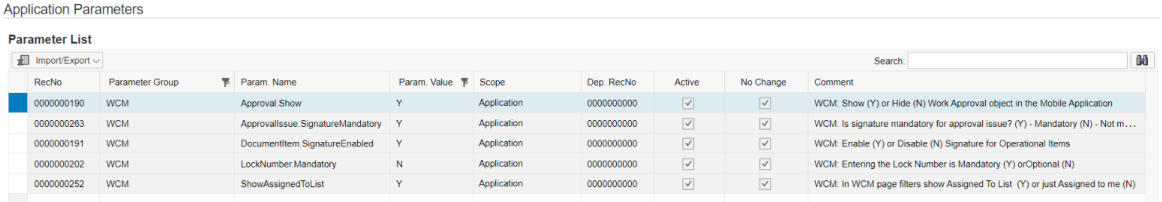
> **Note**
>
> For more information about **Mobile Application Parameters** configuration, refer to Parameters Tab in *MAIF Configuration Guide*.

Procedure

1. On the *Configuration Panel*, go to *Mobile Application Configuration*.



2. On the left, select your application from the list, and go to the *Parameters* tab.
3. Under *Parameter List*, you can search or filter the list of parameters related to the Safety Technician persona (filter the *Parameter Group* to *WCM*).



RecNo	Parameter Group	Param. Name	Param. Value	Scope	Dep. RecNo	Active	No Change	Comment
0000000190	WCM	Approval.Show	Y	Application	0000000000	☑	☑	WCM: Show (Y) or Hide (N) Work Approval object in the Mobile Application
0000000263	WCM	ApprovalIssue.SignatureMandatory	Y	Application	0000000000	☑	☑	WCM: Is signature mandatory for approval issue? (Y) - Mandatory (N) - Not m…
0000000191	WCM	DocumentItem.SignatureEnabled	Y	Application	0000000000	☑	☑	WCM: Enable (Y) or Disable (N) Signature for Operational Items
0000000202	WCM	LockNumber.Mandatory	N	Application	0000000000	☑	☑	WCM: Entering the Lock Number is Mandatory (Y) orOptional (N)
0000000252	WCM	ShowAssignedToList	Y	Application	0000000000	☑	☑	WCM: In WCM page filters show Assigned To List (Y) or just Assigned to me (N)

4. Configure the following Safety Technician-related parameters according to your preference:

- `Approval.Show`: Enables or disables the display of Work Approval objects.
- `ApprovalIssue.SignatureMandatory`: Enables or disables for Safety Technicians to confirm the Work Permit Approval by adding a signature. For more information, see Configuring Work Permit Approvals - Back End - SAP GUI [page 571].
- `DocumentItem.SignatureEnabled`: Enables or disables signature input during tagging or untagging of an operational item. When disabled, it also hides the signature panel.
- `LockNumber.Mandatory`: Users can set the Lock Number as mandatory or optional in the tagging process.
- `ShowAssignedToList`: Enables or disables for Safety Technicians to filter not just their assigned objects, but the assigned objects of other specific users as well. For more information, see Configuring the ShowAssignedToList parameter [page 274].
- `WCMCatalogProfileName`: By configuring catalog profiles, the user will be able to view safety-related catalogs, as well as other ones defined according to their preference. For more information, see Catalog Profiles Configuration [page 310].

3.5.4 General oMDO Configuration - Safety Technician Persona

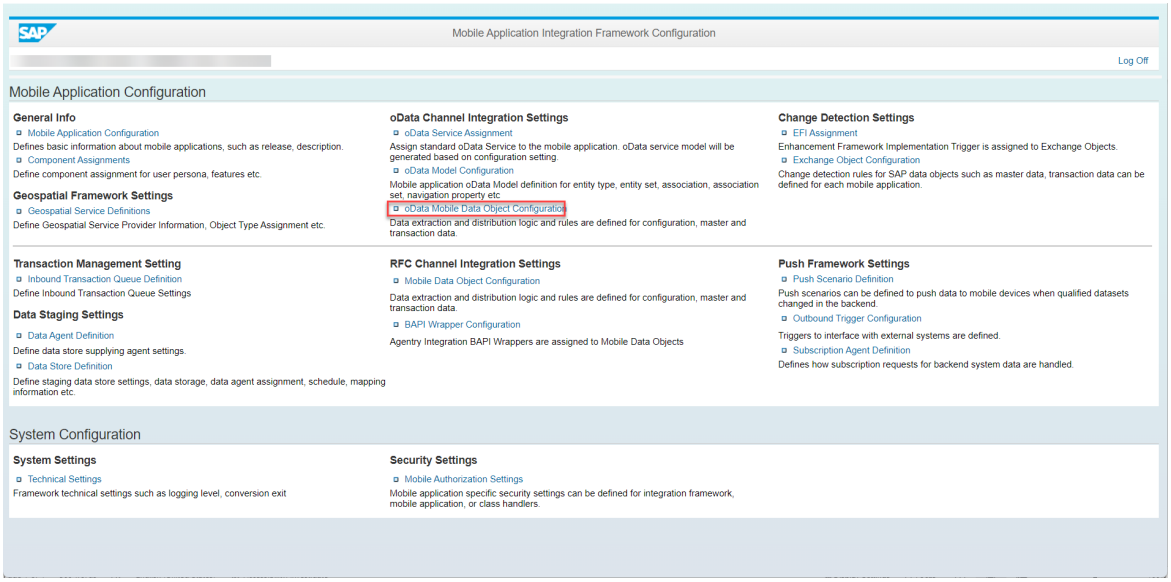
Context

To change the oMDO data filters for the Safety Technician Persona, perform the following steps:

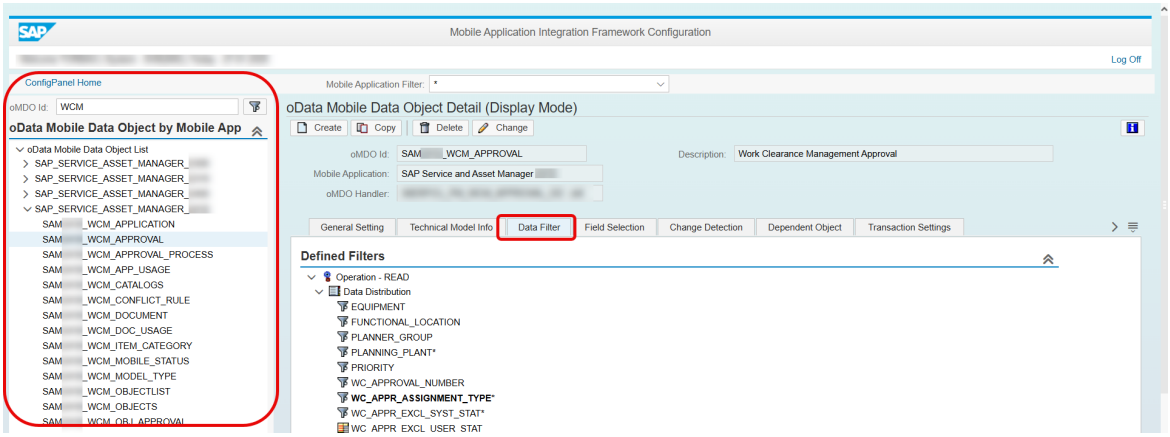
> **Note**
>
> For more information about **oMDO** and **oMDO filter** configuration, refer to OData Mobile Data Object Configuration and OData Mobile Data Object Configuration - Data Filter Tab in *MAIF Configuration Guide*.

Procedure

1. On the *Configuration Panel*, go to *oData Mobile Data Configuration*.



2. Select the required *oMDO* from the left and go to the *Data Filter* tab.



3. Enter *Change Mode* and add any Data Filter(s):

Assignment Types

The following Work Permit Assignment Types (same for Safety Certificates) are supported by the Safety Technician persona:

- 1: User Plant [page 263] (the user must add the *IWK* User Parameter)
- 2: User Work Center [page 266] (the user must add the AGR User Parameter)
- 3: User Planner Group [page 268] (the user must have the IHG User Parameter setup)
- 4: Partner Function [page 270]
- 5: Selection Variant [page 276]
- 6: Operational List + Selection Variant [page 281]
- D: Dependency queue
- Z: Other (implement BADI)

> ⚠ Caution
>
> Please note that in the case of Work Permit Configuration [page 565], the Assignment Type 6: Operational List + Selection Variant [page 281] is **not** relevant.

> ⓘ Note
>
> For more information about User Parameters, see:
>
> - User Parameter IDs [page 606]
> - Work Order Assignment Type Options [page 150]

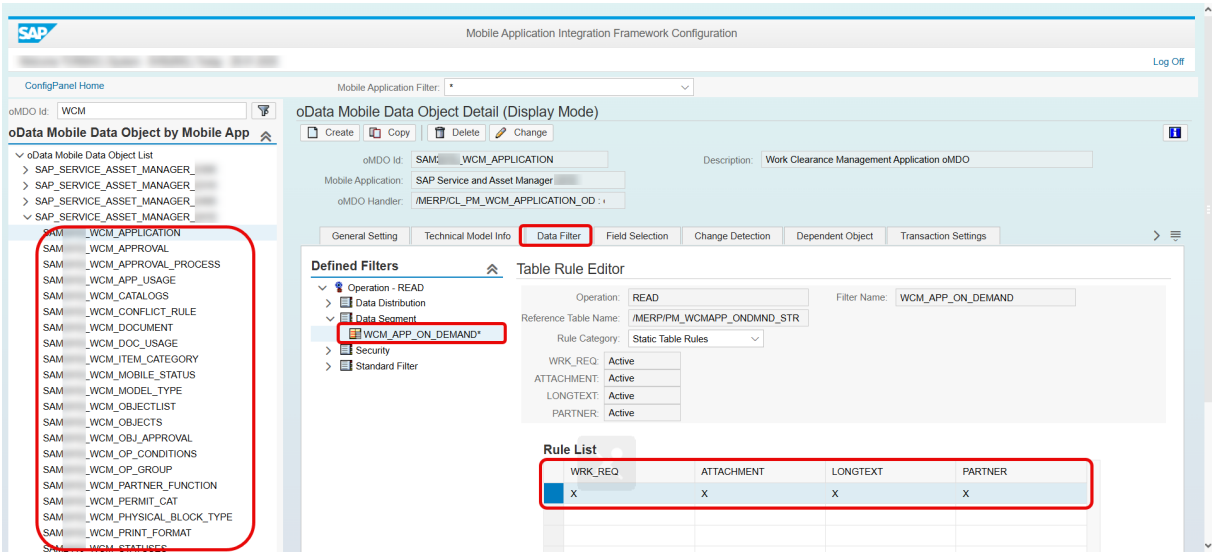
Next Steps

User Parameters Configuration

See General User Parameters Configuration - Safety Technician Persona [page 227].

On-demand structure configuration (optional)

As an optional custom configuration, you can enable or disable sampling of some entities if required:For example, you can disable `WCMApplicationLongtext`, `WCMApplicationAttachments` and other such entities.



1. In the *oData Mobile Data Configuration* menu, select your application on the left.
2. Select an oMDO, go to the *Data Filter* tab.
3. Under *Defined Filters*, go to *Data Segment* > *WCM_APP_ON_DEMAND*.
4. Depending on the oMDO, you can set to *Active* or *Inactive* the following entities:
   - `WCMApplication`
   - `WCMApplicationAttachments`
   - `WCMApplicationDocument`
   - `WCMApplicationLongtext`

- `WCMApplicationOrder`
- `WCMApplicationPartner`
- `WCMApplicationRequirement`

3.5.5 General Exchange Configuration - Safety Technician Persona

Context

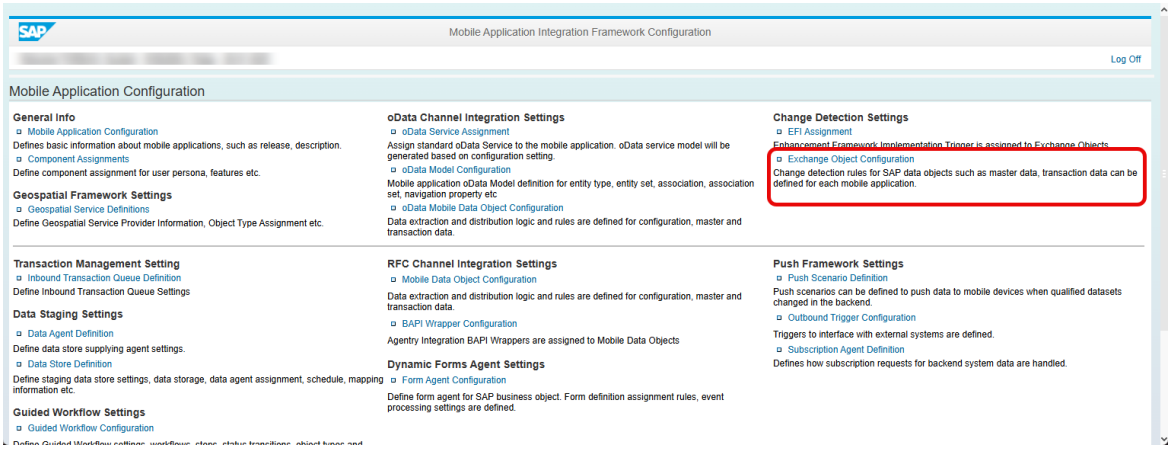
With the exchange framework, we also provide exchange detection. The exchange framework allows users to capture changes made in the backend to WCM objects. This is also highly customizable. You can choose which fields you want to check, and you can also enter data filters.

> **Note**
>
> For more information about **Exchange** and **Exchange filters** configuration, refer to Exchange Object Configuration and Change Detection Condition Filter Tab in *MAIF Configuration Guide*.

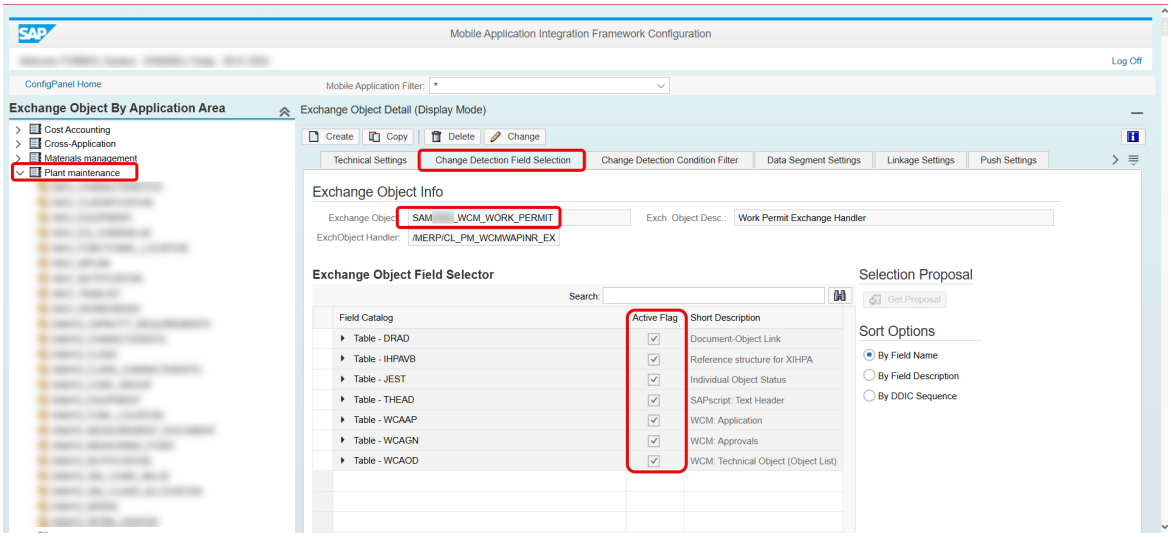
To access the Exchange field detection and select specific fields of the object, perform the following steps:

Procedure

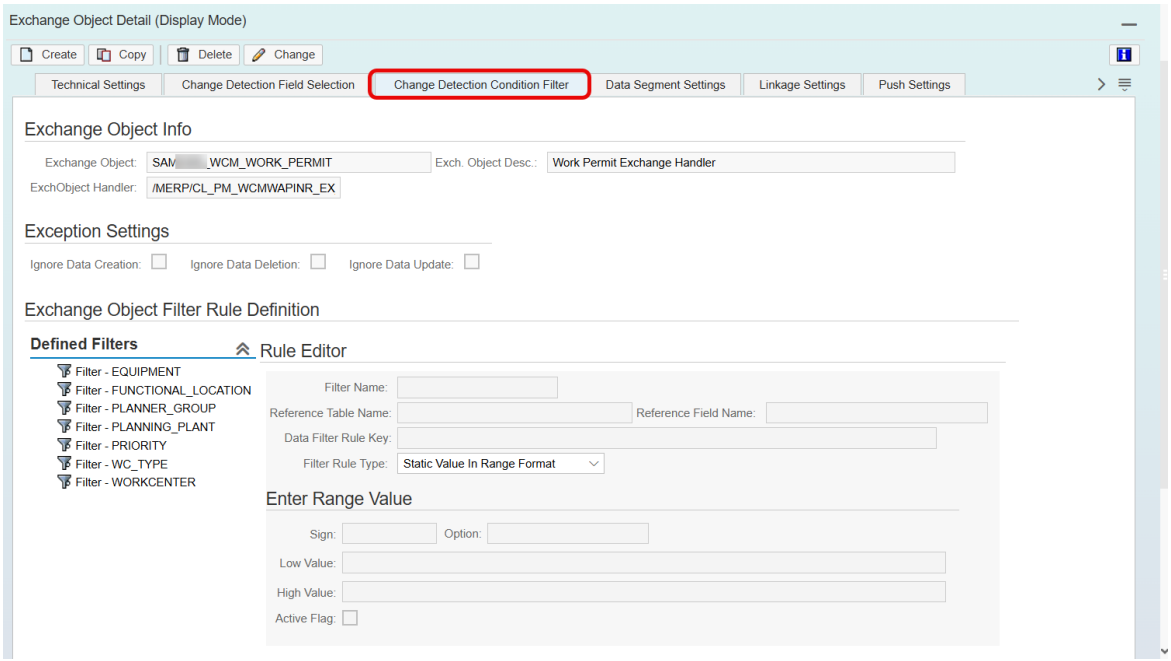
1. On the *Configuration Panel*, go to *Exchange Object Configuration*.



2. Go to *Plant Maintenance* and select any of the following objects related to the Safety Technician persona:
   - *SAM<VERSION>_WCM_APPROVAL*
   - *SAM<VERSION>_WCM_DOCUMENT*
   - *SAM<VERSION>_WCM_WORK_PERMIT*
3. Go to the *Change Detection Field Selection* tab, enter *Change Mode* and set *Exchange Object Fields* to *Active* according to your preference.



4. Optionally, under the *Change Detection Condition Filter* tab, you can also add Data Filters similar to oMDOs (see General oMDO Configuration - Safety Technician Persona [page 221]).



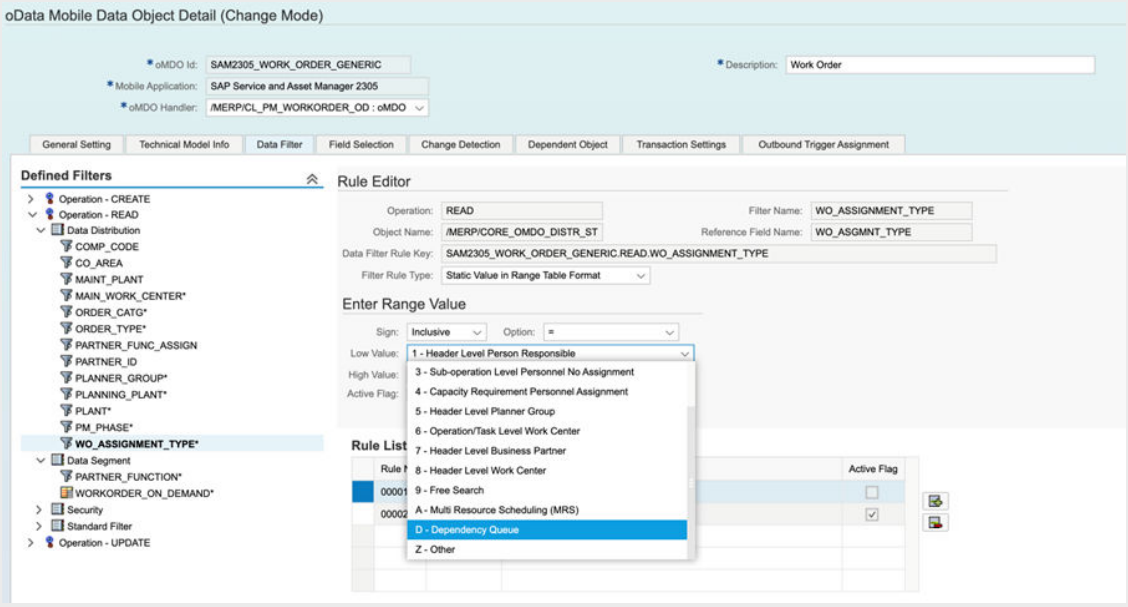
3.5.6 Work Order as a Dependency - Safety Technician Persona

For the safety technician persona, orders can be dependent objects. This means that if the persona is enabled, you have the ability to load work orders that are associated with the related work permits.

> **Note**
>
> In this release, only assignments at the work order header level are supported for the safety technician persona. Operation level assignments will be supported in a later version.

To enable this configuration:

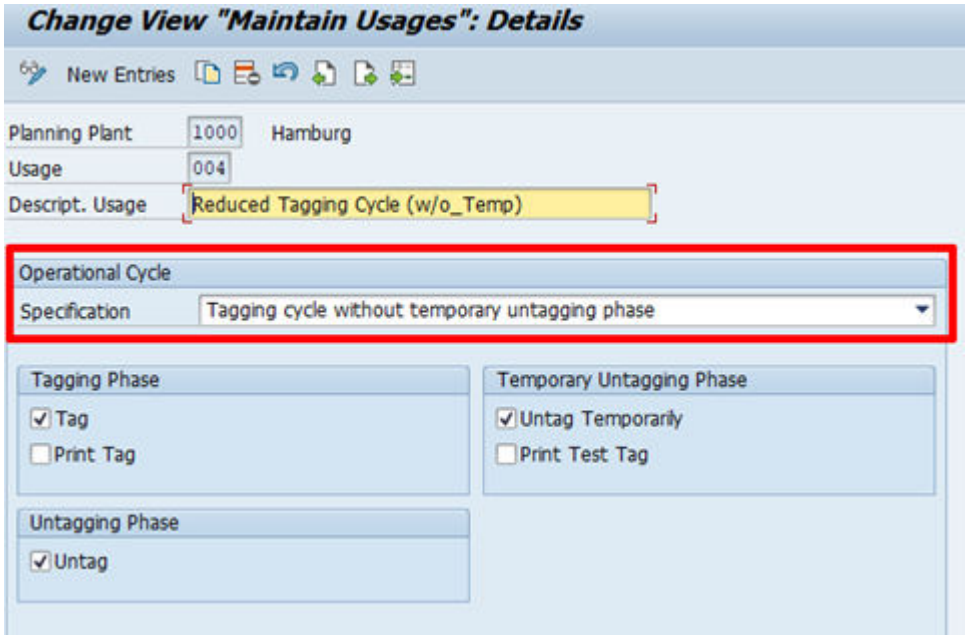
1. Navigate to the `Configuration panel`, select *oMDO* configuration, then select `SAM****_WORK_ORDER_GENERIC`
2. Navigate to *Data Filters* and add a *D Assignment Type* to the object.



3.5.7 Supported Usage Types - Safety Technician Persona

You can create and configure the usage types. There are several customization options, the most important of which is *Operation Cycle - Specification*.

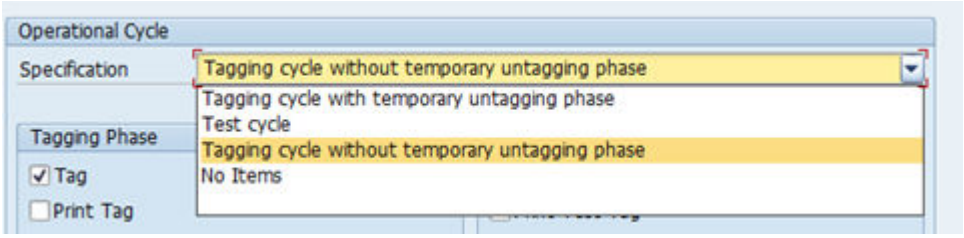
Currently the following types are supported:



- *Tagging cycle with temporary untagging phase*

  > **Note**
  >
  > Limited support from 2505 release. Currently you cannot set the status of the object to *Temporarily Untagged*; however, if it is set to *Temporarilyy Untagged* already, you can set it to *Tagged* or *Untagged*. For more information, see Tagging and Untagging.

- *Tagging cycle without temporary untagging phase*
- *No items*



3.5.8 General User Parameters Configuration - Safety Technician Persona

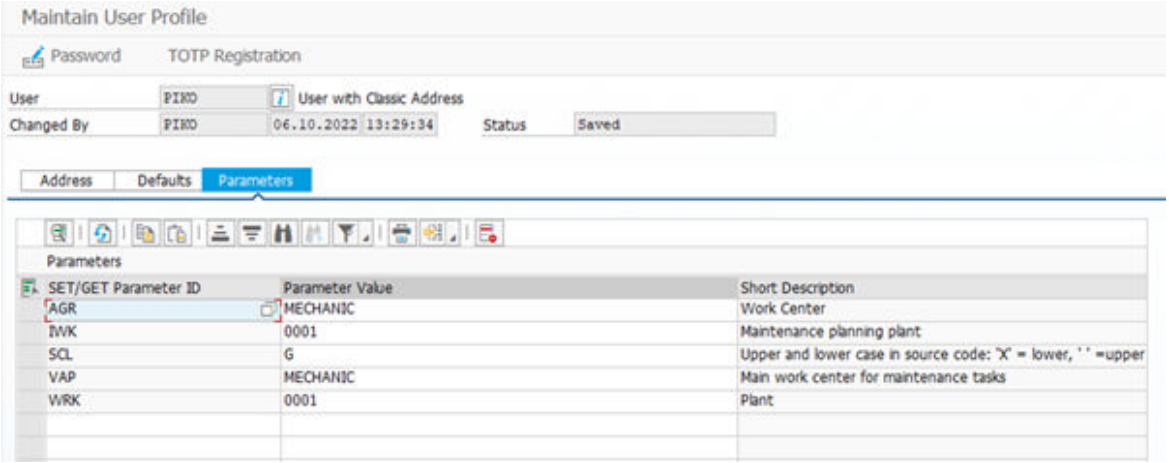
Context

To configure a user's *User Parameter ID* and *User Parameter Value* for the Safety Technician Persona, perform the following steps:

> **Note**
>
> For more information about **User Parameters** configuration: refer to Administration - User Management in *MAIF Administrator Guide*.

Procedure

1. On the *SAP GUI*, navigate to the *SU3* transaction and select the *Parameters* tab.
2. Add a *User Parameter ID* with the *Parameter Value*.



> ### Note
>
> - As of 2410 release, you can add **multiple** user parameter values.
> - For more information about User Parameters, see:
>   - User Parameter IDs [page 606]
>   - Work Order Assignment Type Options [page 150]

3. Save your changes.

3.6 Inventory Clerk Configuration

The Inventory Clerk persona allows a stockroom operator to receive, issue, or transfer stock (materials). The Inventory Clerk persona supports valuated, batch-managed materials, and serialized parts.

> ### Note
>
> For more information on the Inventory Clerk functionality, see Inventory Clerk Persona Overview.

In this section of the guide, we cover the configuration options available for the Inventory Clerk persona:

Related Information

Configuration Prerequisites and Limitations - Inventory Clerk Persona [page 229]
SAP Transactions Supported by Inventory Clerk [page 231]
Application Features Assigned to Inventory Clerk [page 232]
Assigning, Unassigning an Application Feature to a User Persona [page 233]
Enabling, Disabling an Application Feature [page 234]
Assigning, Unassigning an OMDO to a Feature [page 235]
Configuring Data Distribution [page 236]

Mobile Application Parameters [page 238]
Configuring Mobile Application Parameters [page 239]
Configuring Printing [page 240]

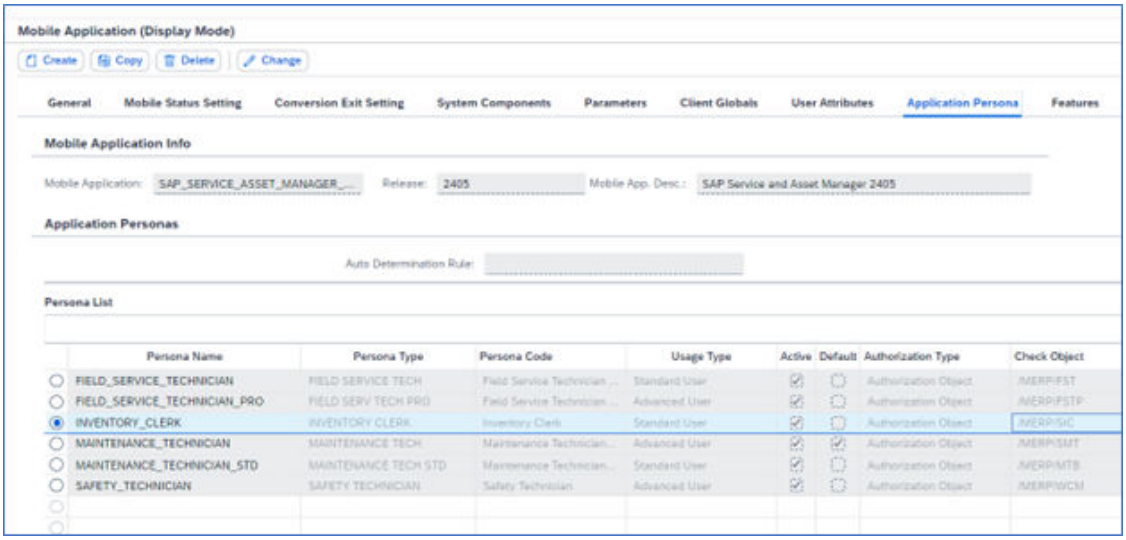
3.6.1 Configuration Prerequisites and Limitations - Inventory Clerk Persona

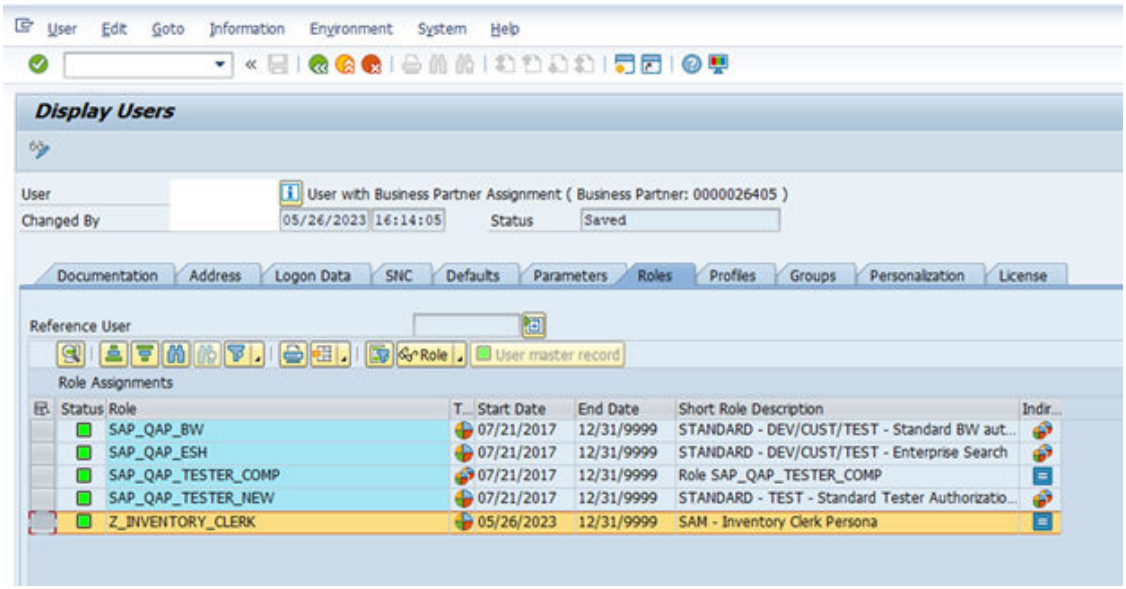
Prerequisites

Please find below the prerequisites for the implementation of the Inventory Clerk persona.

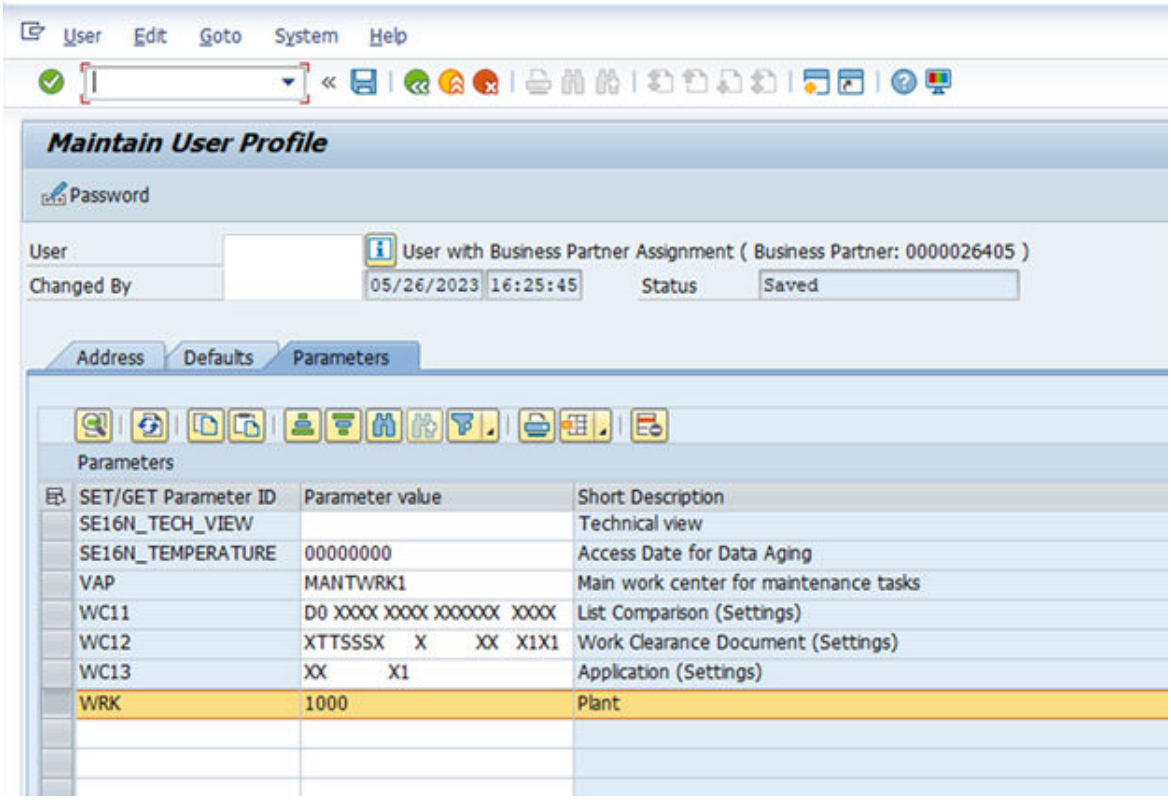
Procedure

1. Assign the Inventory Clerk persona to a user. For more information, see Configuring Personas [page 89].
    1. Create separate security roles for each persona. For example, a rule with the authorization object */MERP/SIC* for the Inventory Clerk persona. For more information, see Mobile User Essential Authorizations.





2. Assign the user parameter *WRK (Plant)* to the user.



> ⓘ Note
>
> The user must have authority to create a material document, post goods issue or receipt of deliveries, and create or count for physical inventory.

Limitations

Currently, the Inventory Clerk persona has the following limitations:

- A duplicate key error occurs when an Inventory Clerk discards a document, like a purchase order, and then tries to re-download it without syncing. In this situation, the app confirms the download, but the document will not appear under the expected filters, such as physical inventory or purchase orders.
  - This issue arises because the local OnDemand record remains until a sync is completed. This creates a conflict with the new download attempt.

  > → Tip
  >
  > Perform a sync before re-downloading discarded documents to avoid this issue.

- In the case of configuring (multiple) *Plant* and *Storage Location* parameters:
  - The *Plant* is defaulted in all *ADD transactions* (adding items to Physical Inventory, Goods Receipt, etc); therefore, **only one Plant** is expected to be assigned to *WRK*.

    > ⓘ Note
    >
    > It is technically possible to use only the first *Plant* and *Storage Location* from a comma-separated *WRK*/*LAG* value. However, each time the value is needed, the client must execute additional rule logic, which increases loading time (for example, when refreshing pickers).

  - All *Material*, *Batch*, *Valuation* and related pickers depend on the *Plant* value. Using comma-separated *Plants* triggers a chain of dependent updates and repeated rule execution, which negatively impacts performance. Therefore, we **do not recommend** using comma-separated values in *WRK* and *LAG*. Instead, use *ZWRK* and *ZLAG*, which **support multi-plant requirements** without affecting performance.

  > → Tip
  >
  > For more information, see Recommended Configuration for Multiple Plants and Work Centers [page 111].

3.6.2 SAP Transactions Supported by Inventory Clerk

The inventory clerk persona supports a subset of the functions offered by standard SAP transactions. The list of transactions below is for reference only.

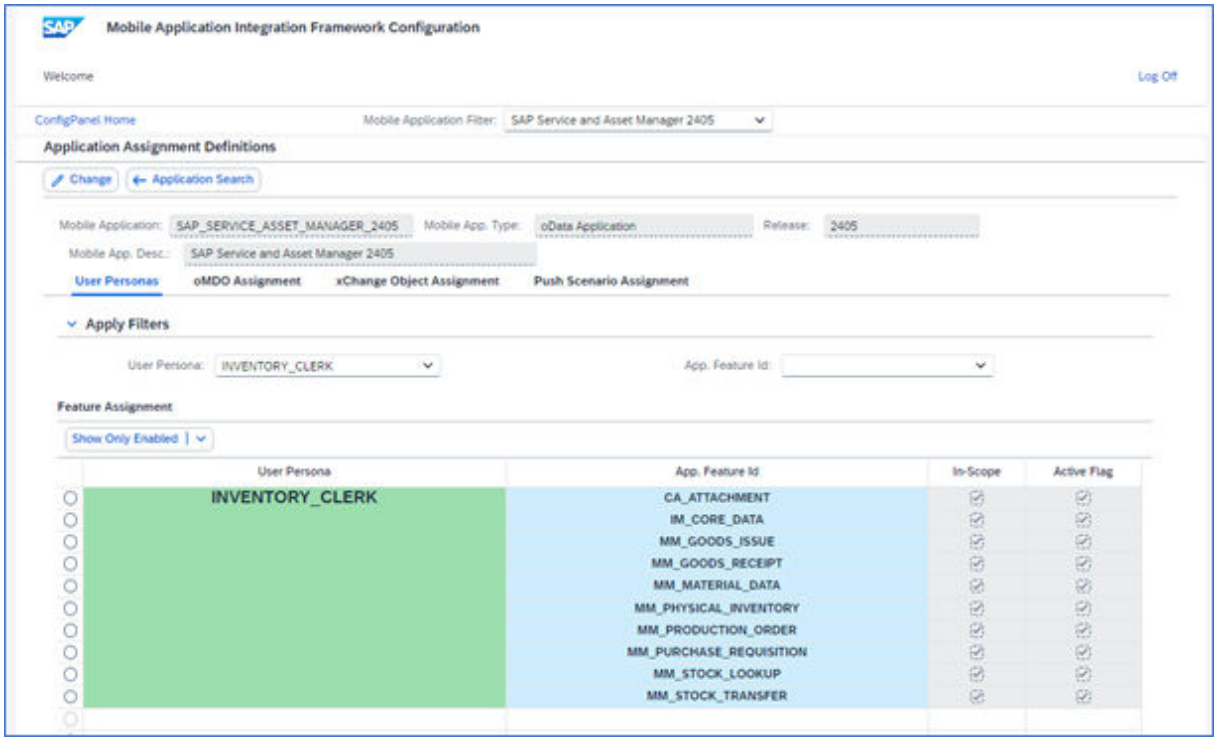
Transaction Codes	Description
MIGO	All the goods movements such as: • Goods receipt • Goods issues • Stock transfers • Transfer postings • Goods issues for scrap • Cancellation and reversals • Vendor returns
MIGO / MB1B	Transfer posting
MIGO / MB1A	Miscellaneous goods issue
MB23	Display reservation
VL02N and VL03N	Outbound delivery display and PGI
VL32N and VL33N	Inbound delivery display and PGR
CO03	Display production order
ME23N	Display purchase order Display stock transport order (STO)
MI01	Create physical inventory
MI03	Display physical inventory
MI04	Enter inventory count
MI05	Change inventory count
ME51	Create purchase requisition

3.6.3 Application Features Assigned to Inventory Clerk

The component assignment allows you to configure the features assigned to a user persona.

You can assign new application features to a user persona or enable or disable an application feature already assigned to a user persona.

The following application features are assigned to the inventory clerk persona shown below.



> **Note**
>
> The inventory clerk persona has a separate data core.
>
> As of version 2405, attachment support has been added to the SAP Service and Asset Manager application.

For more information on the component assignments, refer to the Component Assignments [page 616] topic.

3.6.3.1 Assigning, Unassigning an Application Feature to a User Persona

Context

The OMDO group is assigned to an application feature. The application feature, on the other hand, is assigned to a user persona. The following procedure explains how to assign the application feature in general.

Procedure

1. Log in to the configuration panel using TCode `/SYCLO/CONFIGPANEL`
2. On the main page of the config panel, select *Component Assingment*
3. Select the mobile app from the list and click on it
4. Use the picker for user personas to select the inventory clerk persona
5. Click on the *Change* button to edit the data
6. To limit the features, select the *Show Only Enabled* feature assignment
7. In this list of features assigned to the user persona, you can uncheck the active flag to disable the feature, or select a feature (for which In-Scope = True) to assign the feature to the user persona.

> ⓘ Note
>
> Assigning an application feature to a persona affects only the persona in the context.
>
> If an application feature is not active, the ODMO (and related entities) will not be loaded during synchronization. An ODMO can be assigned to more than one feature, in which case OMDO will be invoked even if one of the features is assigned to a persona.

3.6.3.2 Enabling, Disabling an Application Feature

Context

Alternatively, you can also disable the application feature itself. The following procedure explains how to enable or disable an application feature.

Procedure

1. On the main page of the config panel, select *Mobile Application Configuration*
2. Select the mobile application from the list
3. Select the *Features* tab
4. Click on the *Change* button to edit the data
5. From this feature list, you can either:
   - Uncheck the active flag to disable the feature, or
   - Select the active flag to activate the application feature

> ⓘ Note
>
> When an application feature is disabled, all application personas are affected.

Also, the OMDO assigned to the feature will no longer be called.

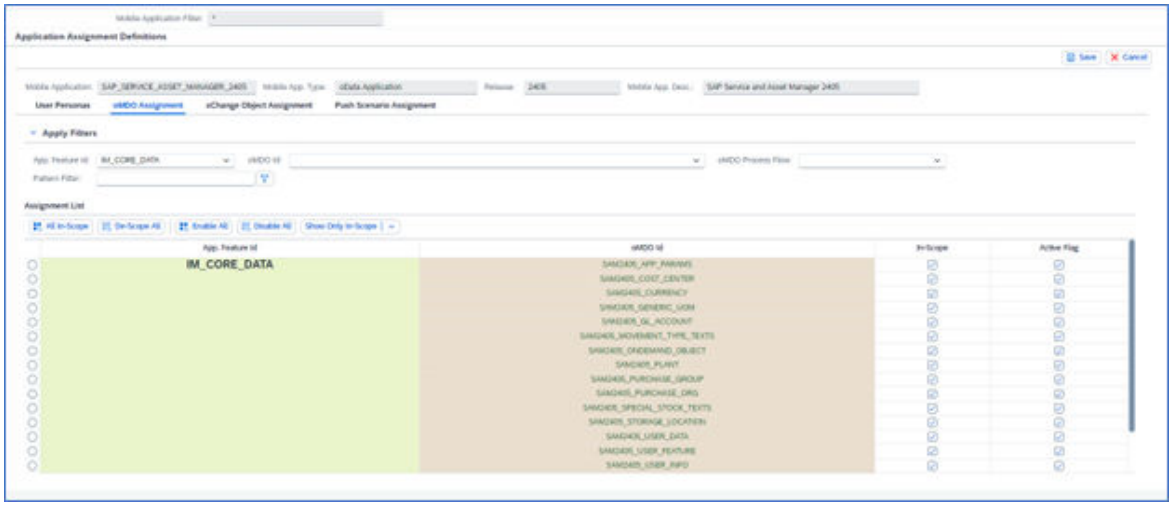
3.6.3.3 Assigning, Unassigning an OMDO to a Feature

Context

The OMDO group is assigned to an application feature. The application feature, in turn, is assigned to a user persona.

Procedure

1. Log in to the configuration panel using TCode `/SYCLO/CONFIGPANEL`
2. On the main page of the config panel, select *Component Assignment*
3. Select the mobile app from the list and click on it
4. Navigate to the *OMDO Assignment* tab
5. Click on the Change button to edit the data
6. Use the picker to select a feature to limit the list to that feature
7. Select *Display Options* > *Show Only In-Scope*
8. In the OMDO list, assign or unassign an OMDO by selecting the active checkbox.



3.6.4 Configuring Data Distribution

With OMDO's data distribution rules, you identify:

- How data is uploaded
- Which data is uploaded to the mobile application.

There are different data distribution models supported by SAP Service and Asset Manager:

- OMDO filters

In this case, the collection of object data depends entirely on the conditions of OMDO filters.

- Dependency Queue

In this case, the collection of object data depends entirely on dependency queue objects, and no filter conditions are applied to the fetch criteria.

- Dependency Queue + OMDO DOF Filters

In this case, the collection of object data depends on dependency queue objects, and the OMDO DOF filters are applied to the result set.

- Other (custom) BAdIs

You can implement your own distribution logic using BAdIs.

For more information on data distribution, see Data Distribution Model Overview [page 118].

The table below summarizes the data distribution for OMDO within the inventory clerk persona.

> **Note**
>
> The table shows only transactional data, not including master or configuration OMDO data such as material, plant, so on.
>
> The source OMDO for all the entities is SAM2405_ONDEMAND_OBJECT and the technical entity type is ONDEMANDOBJECT.

OMDO Name	Distribution Mode
SAM2405_MATERIAL_DOCUMENT	2-Dependency Queue
SAM2405_PURCHASE_ORDER	2-Dependency Queue
SAM2405_RESERVATION	2-Dependency Queue
SAM2405_PHYSICAL_INVENTORY	2-Dependency Queue
SAM2405_INBOUND_DELIVERY	2-Dependency Queue
SAM2405_OUTBOUND_DELIVERY	2-Dependency Queue
SAM2405_PRODUCTION_ORDER	2-Dependency Queue
SAM2405_PURCHASE_REQUISITION	1-OMDO Filter and 2-Dependency Queue

> ### Note
>
> Currently, canceled material documents are not downloaded to the mobile app. Therefore, duplicate cancelations are possible.

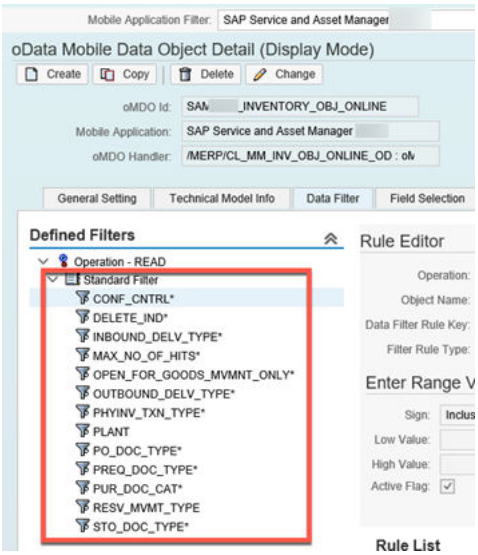
By default, the SAP configuration and master data entities (such as material, plant, and so on) are configured to use the 1-OMDO filter distribution mode. As a result, the data for these entities is downloaded based on the pre-defined filters in OMDO during synchronization.

By default, transactional data entities (such as purchase order, material documents) are configured to use the 2-dependency queue distribution mode. As a result, data for these entities is downloaded based on the dependency of the other entities. For example, when a purchase order is downloaded, the dependent material documents are also downloaded.

3.6.4.1 Inventory Clerk Parameter Configuration

You can search for inventory objects you want to process directly from your mobile device.

Based on the search criteria, the application will search for objects locally or in the backend (if enabled). Objects matching the oMDO filter values will be returned in the search results.



- CONF_CNTRL: Default value is blank and used in PO and STO search
- DELETE_IND: Default value is blank and used in PO, STO, RS, and PI search
- INBOUND_DELV_TYPE: Default value is ‘EL’ and used in IB search
- MAX_NO_OF_HITS: Default value is ‘1000’ and applied for each object search individually
- OPEN_FOR_GOODS_MVMNT_ONLY: Default value ‘X’ and applied for in each object search

  > ### Note
  >
  > This filter is cascaded and set to active for all inventory objects oMDO except the physical inventory.

- OUTBOUND_DELV_TYPE: Default value is ‘LF’ and used in OB search

- PHYINV_TXN_TYPE: Default values are ‘IB’ and ‘IN’. Used only in the physical inventory search.
- PLANT: Default value is none and used in each object search
- PO_DOC_TYPE: Default value is ‘NB’ and used in PO search
- PUR_DOC_CAT: Default value ‘F’ and used in PO search
- RESV_MVMT_TYPE: Default value is none and used in RS search
- STO_DOC_TYPE: Default value is ‘UB’ and used in STO search.

> **Note**
>
> OUTBOUND and INBOUND_DELIVERY prioritize the USER_LOCATION filter over all other filters. If you have multiple values, maintain the corresponding mobile user attribute, like USER_TRUNK. Comma-separated values in user parameters aren't supported for this purpose.

3.6.5 Mobile Application Parameters

With the mobile app settings, you can control client-side runtime behavior.

For more information, see the *Parameters Tab* section in the Mobile Application Configuration [page 611] topic.

The list of mobile app parameters specific to the inventory clerk persona is as follows:

Group	Name	Value	Scope	Description
INVENTORY	search.online	Y	Application	Y = Enable back end search from the overview page N = Disable back end search (for example, local search restriction)
INVENTORY	search.minimum.characters	5	Application	Minimum number of characters required to run a back end search
INVENTORY	search.auto.navigate	Y	Application	Allow automatic navigation to the document details page when returning a search (1 document only)
INVENTORY	Hide.PhysicalInventory.SummaryPage	Y	Application	Y = Hides the summary page during physical inventory creation N = Shows the summary page during physical inventory creation

Group	Name	Value	Scope	Description
INVENTORY	CheckToleranceLimit.PhysicalInventory	Y	Application	Y = Check physical inventory tolerance limit N = Do not check physical inventory tolerance limit
INVENTORY	ToleranceLimitPercent.PhysicalInventory	5	Application	Tolerance limit for physical inventory in %
INVENTORY	CheckStock.GoodsIssue	Y	Application	Y = Check stock level at the end of a goods issue N = Skip zero stock level check

3.6.5.1 Configuring Mobile Application Parameters

Context

Using the mobile app settings, an inventory clerk persona can automatically search for documents and enable or disable validation rules.

> **Note**
>
> The mobile app parameters for the inventory clerk persona have parameter group = INVENTORY.

Procedure

1. Log in to the configuration panel using TCode `/SYCLO/CONFIGPANEL`
2. From the main page of the configuration panel, go to the *Mobile Application Configuration* section
3. Select the version of the mobile application you want to configure
4. Go to *Parameters Tab*
5. Click the filter icon under *Parameter Group* > *User Defined Filters*
   - Set the parameter group filter = INVENTORY
6. Click on the *Change* button to edit the parameter
7. Edit the value of the parameter or select a rule
8. Click the *Save* button to commit the changes.

> **Note**
>
> You can create a complex rule where the value of a parameter can vary from user to user.

If you select a rule that is unique to a user, change the parameter scope to *User*.

3.6.6 Configuring Printing

With the SAP Service and Asset Manager app, the inventory clerk persona can print labels for the movement of goods using *SAP Output Control*.

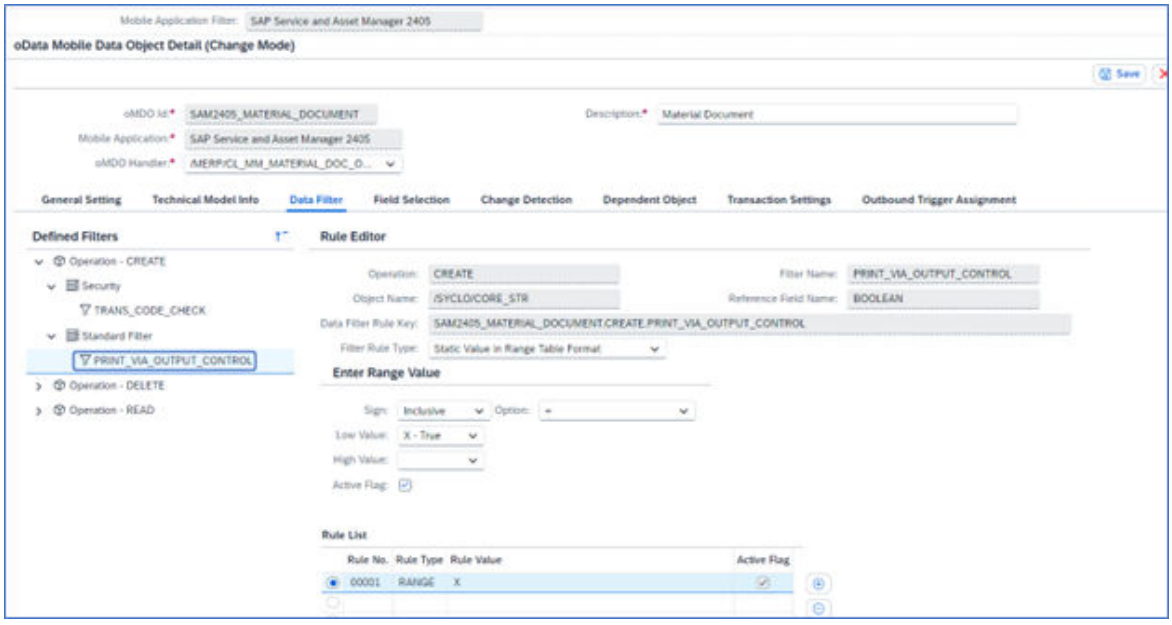
Context

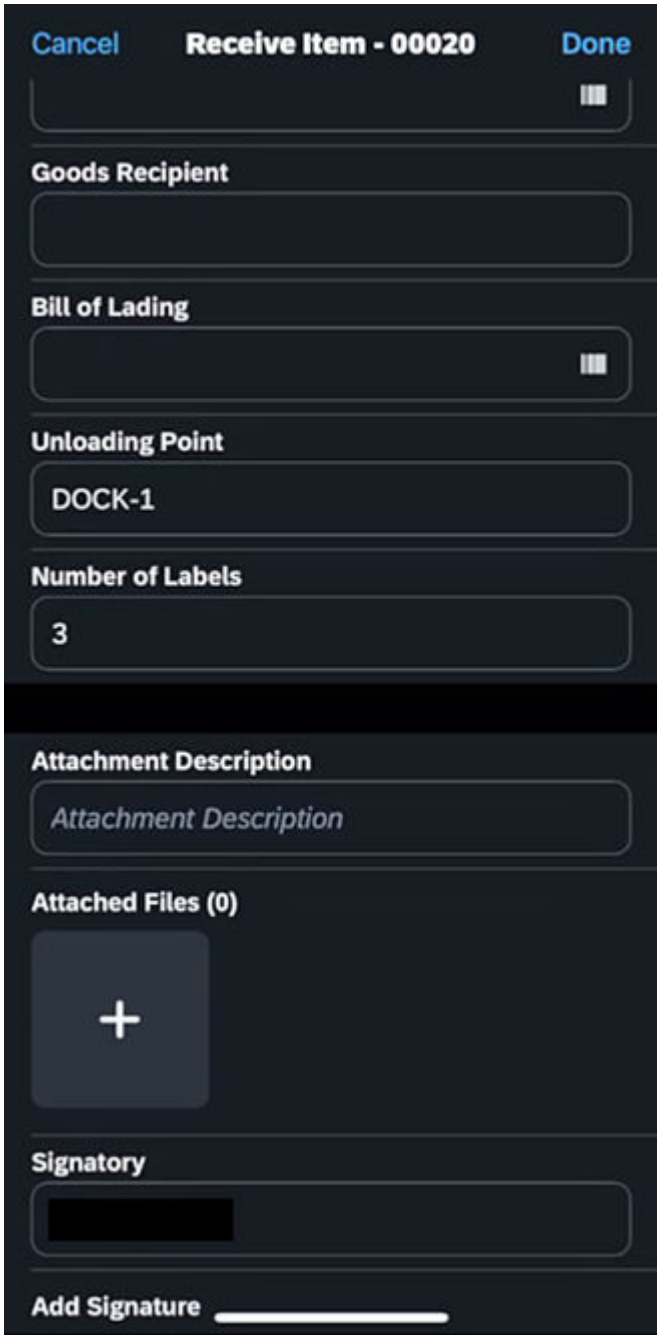
Print slips and goods movement labels are posted using the SAP Service and Asset Manager mobile app.

> **Note**
>
> Currently, printing via BRF+ configuration is not supported.

Procedure

1. Log in to the configuration panel using TCode `/SYCLO/CONFIGPANEL`
2. On the config panel home page, select *OData Mobile Data Object Configuration* > *SAM2405_MATERIAL_DOCUMENT*
3. Go to *Data Filter* > *Create Transaction* > *Standard Filter*
4. Configure the *PRINT_VIA_OUTPUT_CONTROL* filter. Add a filter rule
5. Enter the label number (individual slip) when entering data on goods movement in the mobile application.




Cancel
Receive Item - 00020
Done
Goods Recipient
Bill of Lading
Unloading Point
DOCK-1
Number of Labels
3
Attachment Description
Attachment Description
Attached Files (0)
Signatory
Add Signature

4 Feature Configurations

4.1 AI-Assisted Job Completion - Configuration

Technicians can complete their job (Work Order, Service Order, Operation or Suboperation) with voice input using natural language and AI, instead of manually entering data required for the completion. The following fields support filling using AI:

- Time
- Expense
- Milage
- Note
- Defect information

> **Note**
>
> For more information about using AI-assisted job completion, see Using AI to Complete Your Job.

Supported Personas

This feature is applicable for the following personas:

Maintenance Technician (Standard)
Maintenance Technician (Pro)
Field Service Technician (Standard)
Field Service Technician (Pro)

> **Note**
>
> This feature is in scope for the Maintenance Technician (Standard) persona. However, no applicable use case currently exists because this persona supports Notifications only and does not support Work Orders. As a result, the AI job completion flow is never triggered.

Limitations

For Notifications, only the creation of the Notification Item and all its dependencies (such as Cause, Part, Damage, etc.) is supported.

Prerequisites

- To use this AI feature, you must add the SAP Dynamic Forms service (Production or Preview) to the entitlements on the SAP BTP subaccount where your SAP Service and Asset Manager application is running. However, this prerequisite does not mean you have to use SAP Dynamic Forms actively. The SAP Dynamic Forms service acts as a proxy for the SAP AI service.
- As this is a premium AI feature for SAP Service and Asset Manager, you need an active subscription to this Cloud Service and SAP AI Units to use AI within the mobile application. For more information about the pricing of the *SAP Service and Asset Manager, mobile execution* AI feature, refer to the SAP Business AI Catalog in Discovery Center.

Configuration

Perform the following configuration step(s):

1. Configuring AI-Assisted Job Completion - BTP Mobile Services Connectivity [page 243]
2. Configuring SAP Service and Asset Manager Security Settings to Access AI-Assisted Job Completion [page 245]
3. Setting Up Roles and Role Collections for AI-Assisted Job Completion Users [page 248]
4. Configuring AI-Assisted Job Completion - Back End - Enabling the Feature [page 249]

4.1.1 Configuring AI-Assisted Job Completion - BTP Mobile Services Connectivity

Context

For detailed information about AI-assisted job completion, see the overview topic, AI-Assisted Job Completion - Configuration [page 242].

This procedure describes how to create the destination required for your mobile application in BTP Mobile Services.

General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- SAP Mobile Services product page

Procedure

1. Navigate to the app in BTP Mobile Services and select the *Connectivity* settings.

2. Click the + (*Add*) button, then *Create Destination*.
3. Fill in the fields as follows:
    1. *Name*: *AIProxyAPI*
    2. *Type*: *Internet Destination*
    3. *URL*: Enter the provider URL depending on your region. Currently the following regions are supported:

Region	Production Provider URL	Preview Provider URL
AP10	`https://ai-proxy.ap10.dynamicforms.cloud.sap`	`https://ai-proxy.ap10.preview.dynamicforms.cloud.sap`
AP11	`https://ai-proxy.ap11.dynamicforms.cloud.sap`	`https://ai-proxy.ap11.preview.dynamicforms.cloud.sap`
AP20	`https://ai-proxy.ap20.dynamicforms.cloud.sap`	`https://ai-proxy.ap20.preview.dynamicforms.cloud.sap`
EU10	`https://ai-proxy.eu10.dynamicforms.cloud.sap`	`https://ai-proxy.eu10.preview.dynamicforms.cloud.sap`
EU20	`https://ai-proxy.eu20.dynamicforms.cloud.sap`	`https://ai-proxy.eu20.preview.dynamicforms.cloud.sap`
EU30	`https://ai-proxy.eu30.dynamicforms.cloud.sap`	`https://ai-proxy.eu30.preview.dynamicforms.cloud.sap`
IN30	`https://ai-proxy.in30.dynamicforms.cloud.sap`	`https://ai-proxy.in30.preview.dynamicforms.cloud.sap`
JP10	`https://ai-proxy.jp10.dynamicforms.cloud.sap`	`https://ai-proxy.jp10.preview.dynamicforms.cloud.sap`
US10	`https://ai-proxy.us10.dynamicforms.cloud.sap`	`https://ai-proxy.us10.preview.dynamicforms.cloud.sap`
US21	`https://ai-proxy.us21.dynamicforms.cloud.sap`	`https://ai-proxy.us21.preview.dynamicforms.cloud.sap`
US30	`https://ai-proxy.us30.dynamicforms.cloud.sap`	`https://ai-proxy.us30.preview.dynamicforms.cloud.sap`

> **Note**
>
> Your SAP BTP subaccount must be in one of these regions to use the feature.

4. *SSO Mechanism*: *Forward Authentication*

Next Steps

Continue with Configuring SAP Service and Asset Manager Security Settings to Access AI-Assisted Job Completion [page 245].

4.1.2 Configuring SAP Service and Asset Manager Security Settings to Access AI-Assisted Job Completion

Prerequisites

Before performing the configuration steps in this document, make sure that you completed Configuring AI-Assisted Job Completion - BTP Mobile Services Connectivity [page 243].

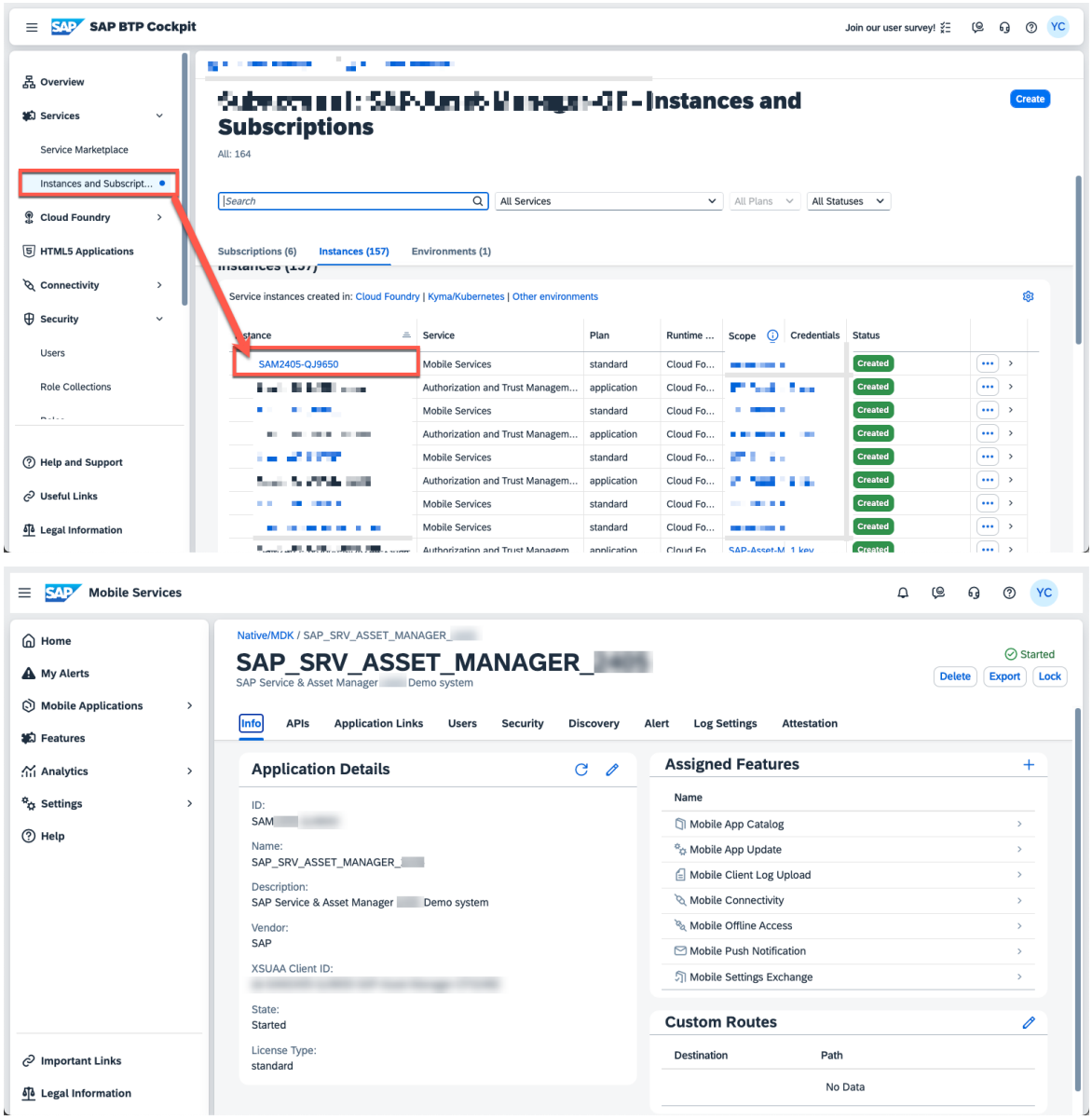
Context

For detailed information about AI-assisted job completion, see the overview topic, AI-Assisted Job Completion - Configuration [page 242].

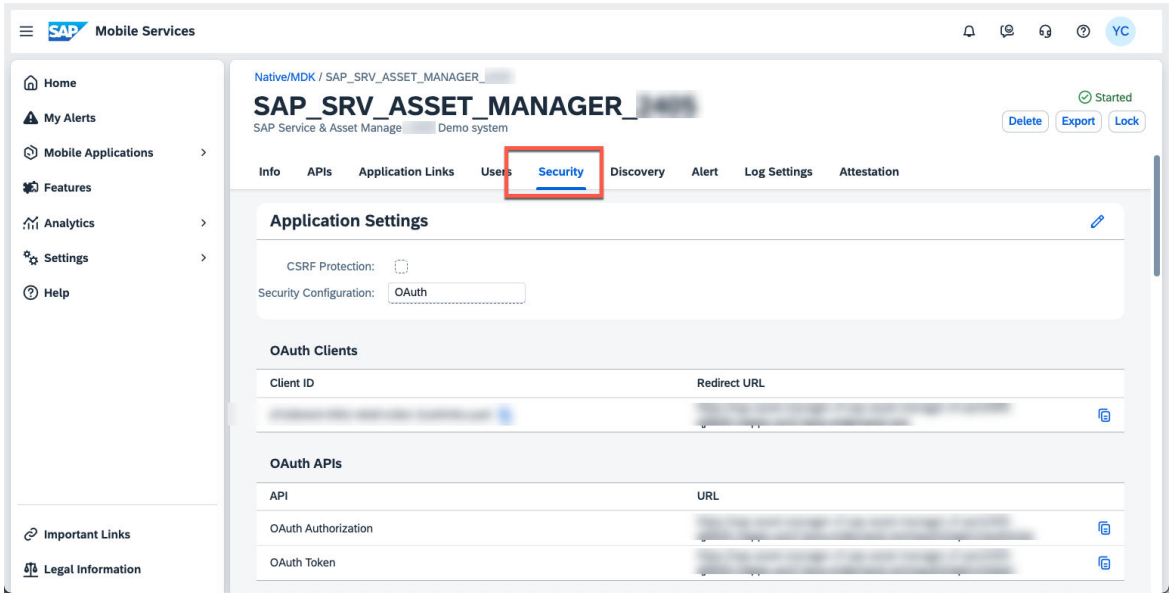
For this feature to work, SAP Service and Asset Manager must be installed and operated in the same SAP BTP subaccount as SAP Dynamic Forms. The security settings of the Mobile Services application (that connects the SAP On-Premise back end system to the SAP Service and Asset Manager mobile applications) must be configured to connect with SAP Dynamic Forms. Perform the following steps to configure the Mobile Services application:

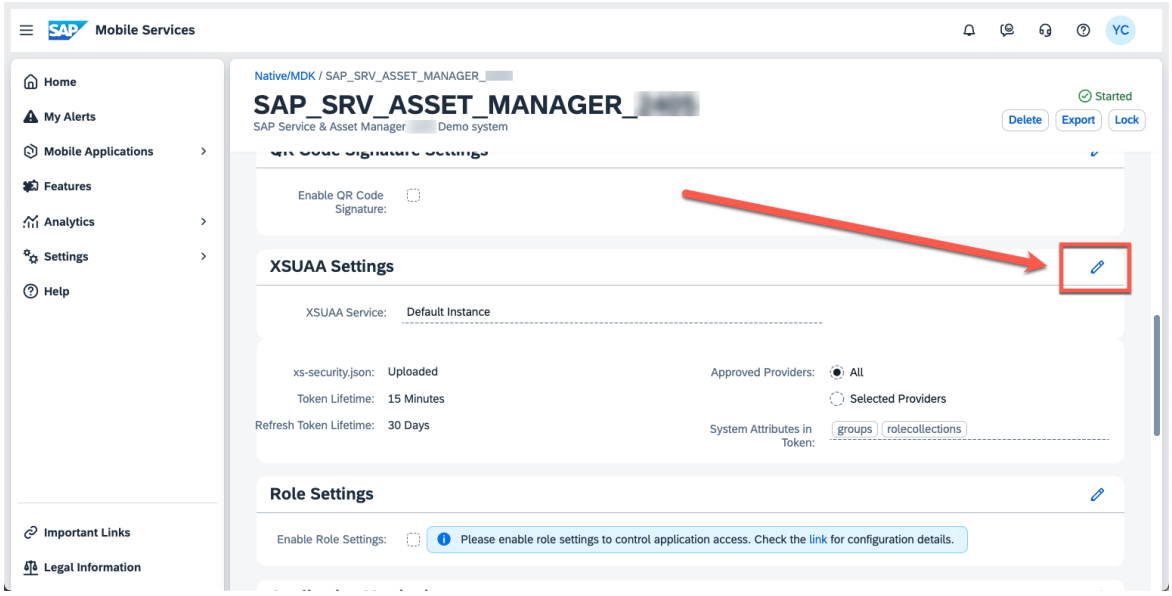
Procedure

1. In the SAP BTP subaccount, open the corresponding Mobile Services application that is associated with the SAP Service and Asset Manager instance that you want to connect with SAP Dynamic Forms.

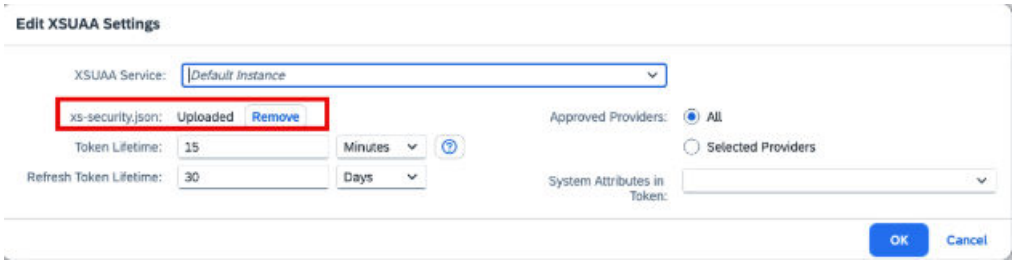


2. Go to the *Security* tab in the Mobile Service application definition, scroll down to *XSUAA Settings* and click the *Edit* icon.





3. Upload the `xs-security.json` file corresponding to your SAP BTP subaccount's region [page 244].



> **Note**
>
> - To retrieve the corresponding `xs-security.json` file, refer to the SAP Note 3455014: *SAP Dynamic Forms - SAP Service and Asset Manager Integration*.

- Please note that if you have downloaded the `xs-security.json` file **before the SAP Dynamic Forms release 2509**, you need to **download again** and upload to your SAP BTP subaccount's region. If you upload an earlier version of the `xs-security.json` file, the AI-assisted job completion feature **will not work**.

4. Click *Save*.

Next Steps

Continue with Setting Up Roles and Role Collections for AI-Assisted Job Completion Users [page 248].

4.1.3 Setting Up Roles and Role Collections for AI-Assisted Job Completion Users

Prerequisites

Before performing the configuration steps in this document, make sure that you completed Configuring SAP Service and Asset Manager Security Settings to Access AI-Assisted Job Completion [page 245].

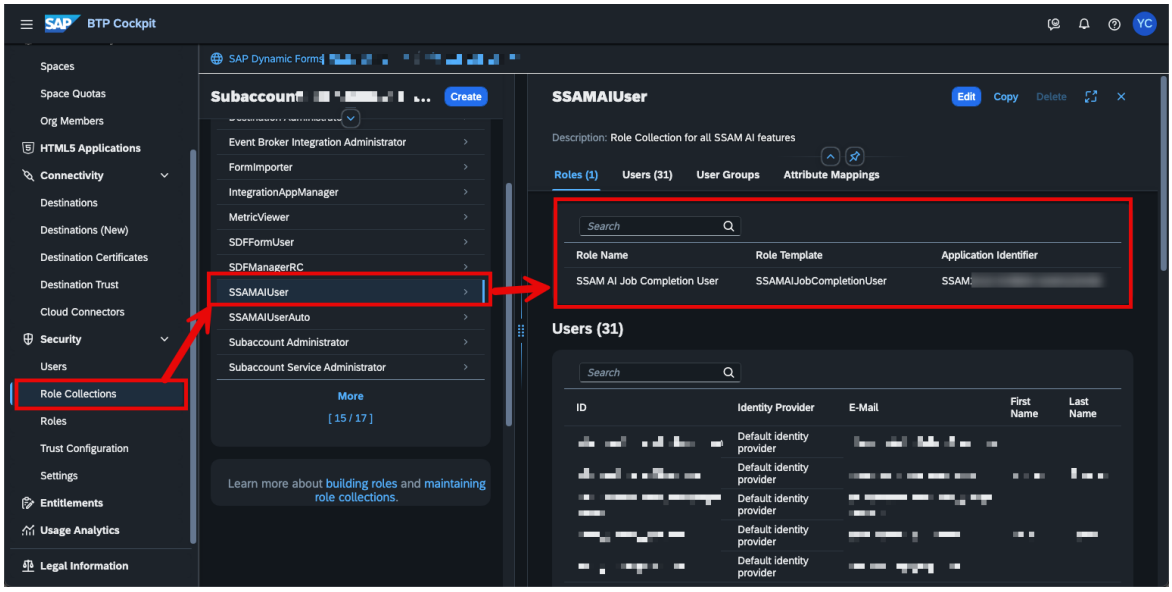
Context

Access control to the AI-assisted job completion feature provided by SAP Service and Asset Manager can be gated by Roles and Role Collections, which are native to the SAP BTP Cloud Foundry environment. Once you have uploaded the `xs-security.json` file [page 247] in the Mobile Service application *Security* settings, the *SSAMAIUser* Role Collection **will be provided by default**.

Procedure

1. In the SAP BTP subaccount, navigate to *Security* > *Role Collections*.
2. Select the Role Collection *SSAMAIUser*.

> **Note**
>
> This Role Collection includes **all the necessary Roles** for users to access the AI-assisted job completion feature.



3. Assign users to the Role Collection by either of the following ways:
   - Directly in the *Users* section of the Role Collection.
   - Via *User Groups* in the SAP BTP.
4. *Save* your changes.

Next Steps

Continue with Configuring AI-Assisted Job Completion - Back End - Enabling the Feature [page 249].

4.1.4 Configuring AI-Assisted Job Completion - Back End - Enabling the Feature

Prerequisites

Before performing the configuration steps in this document, make sure that you completed Setting Up Roles and Role Collections for AI-Assisted Job Completion Users [page 248].

Context

For detailed information about AI-assisted job completion, see the overview topic, AI-Assisted Job Completion - Configuration [page 242].

To enable this feature in the ConfigPanel, perform the steps below.

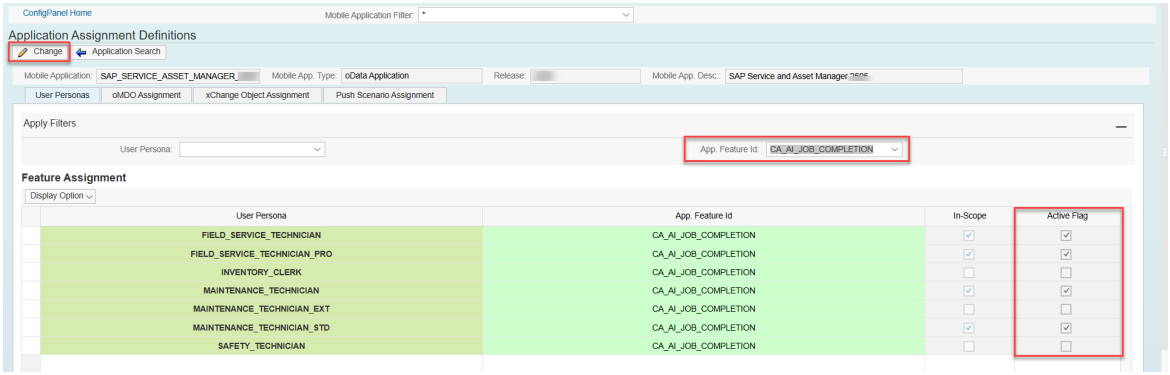
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **Enabling and disabling features**: refer to Configuring Features in *MAIF Configuration Guide*.

Procedure

1. In the *Config Panel*, go to *Component Assignments*.
2. Select the application with correct version from the list.
3. Select the *CA_AI_JOB_COMPLETION* as *App. Feature Id*, enter *Change Mode* and set the feature to *Active* for the relevant persona(s).



4. Save your changes.

4.2 ASPM and PdMS Configuration

4.2.1 Configuring Checklist Parameters

Use parameters to enable the checklist feature and configure other checklist options available.

Context

> **Note**
>
> As of the SAP Service and Asset Manager 2205 release, enable and disable parameters are no longer available through the *Parameters* tab. You enable or disable all features through the *Features* tab. See the Configuring Features [page 93] procedure for details.

The ASPM Checklist feature is called *IAM_CHECKLIST*. By default, the feature is not enabled.

To configure the checklist options for SAP Service and Asset Manager, use the *CHECKLISTS* parameter group and the following parameters within the group:

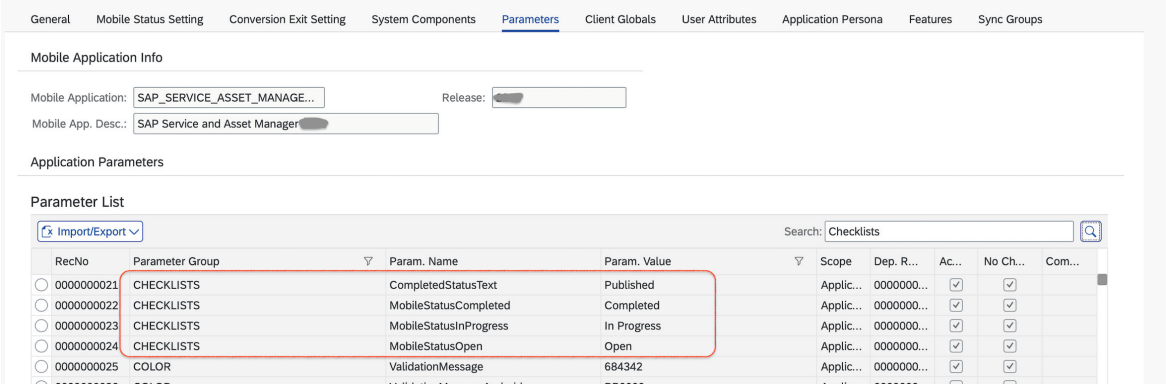
- **MobileStatusCompleted:** Default is *Completed*. Do not change this setting unless you are integrating SAP Service and Asset Manager with another product besides ASPM.
- **MobileStatusInProgress:** Default is *In Progress*
- **MobileStatusOpen:** Default is *Open*
- **CompletedStatusText:** Default is *Published*. This parameter is used to distinguish completed checklists that have been downloaded from the back end versus checklists that have been completed locally on the client but are not yet synced. The parameter is necessary to make logic decisions on the client as checklists that have been completed and synced to the back end are no longer allowed to be edited. Do not change this setting unless you are integrating SAP Service and Asset Manager with another product besides ASPM.

The *CHECKLISTS* parameters correspond to the rules found in the OData mobile data object *SAMXXXX_ASPM_CHECKLIST*. You can add a data filter rule to your customer namespace, or change the existing parameter-rule association to a new parameter-rule association.

Procedure

1. Using the ConfigPanel, navigate to *Mobile Application Configuration* > *Parameters tab*. In the left column, *Defined Mobile Applications*, select your application.

   The *Parameter List* populates with a list of all parameters available for the application.
2. You can scroll down to find the *CHECKLISTS* group parameters, listed in the *Context* section, or perform a search using the *Search* box. Highlight the parameter you want to configure and click the *Change* button.



3. Make your desired parameter association changes, or change the value of a parameter to *Z*, a custom activity catalog type.
4. Check the `<Active>` flag to ensure that the parameter is used by the mobile application. If desired, and if not already checked, check the `<No Runtime Change>` box to ensure that the value of the parameter is not overridden at runtime through synchronization processing.
5. *Save* your changes.

Results

You have enabled the checklist parameters in the ConfigPanel.

Next Steps

Continue to the following procedures to finish configuring the checklist feature for ASPM:

- Setting Up an ASPM Connection to the ASPM System to Use Checklists [page 252]
- Checking the Readiness of the ASPM System [page 255]
- Readiness Check for Authenticated GIS Maps [page 260]

4.2.2 Setting Up an ASPM Connection to the ASPM System to Use Checklists

The RFC destination is already created and connected to the ASPM out of box. However, an oAuth connection from the ASPM Cloud Foundry system to SAP Service and Asset Manager is required.

Prerequisites

Use the Integration of Asset Central Foundation with SAP EAM guide to establish an oAuth connection. Pay attention to the Server Management Properties topic.

Context

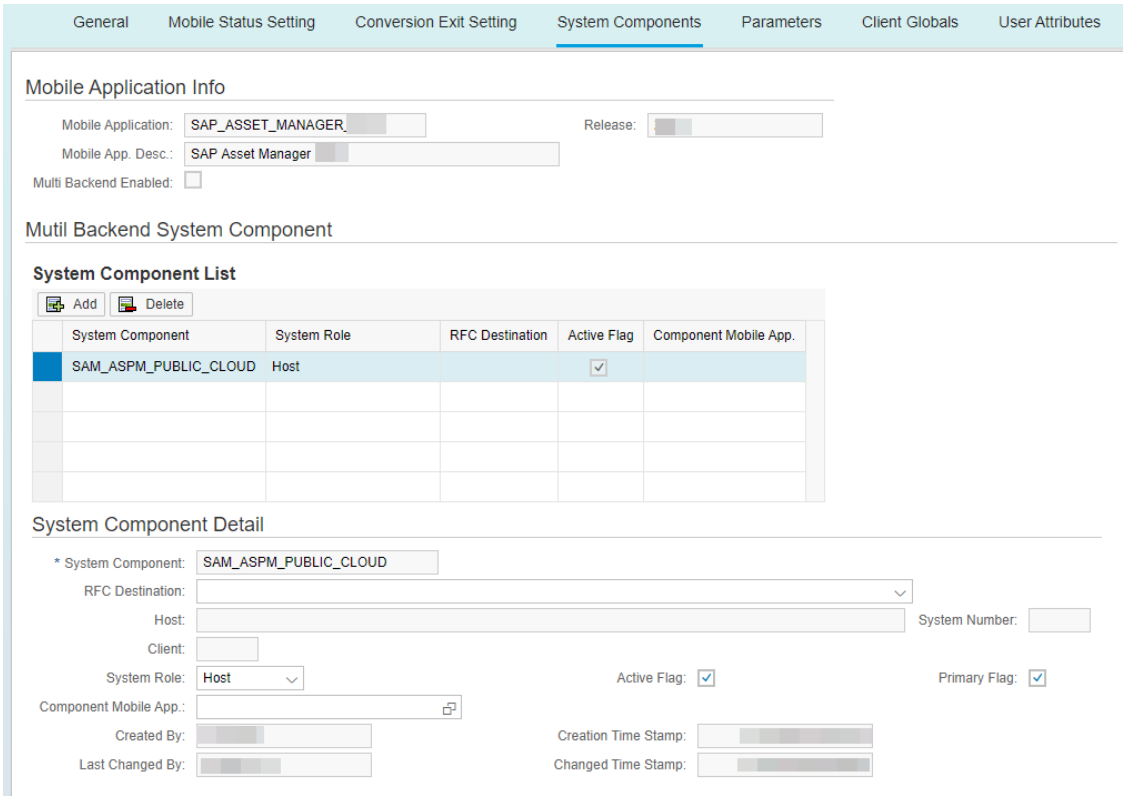
Use the following procedure to create and configure an oAuth connection from the ASPM Cloud Foundry system to SAP Service and Asset Manager.

Procedure

1. **Configure system component settings using the ConfigPanel:**
   a. From the home page of the ConfigPanel, select *Mobile Application Configuration*. Choose your application from the *Defined Mobile Applications* list. Then select the *System Components* tab.
   b. Click the *Change* pencil icon.

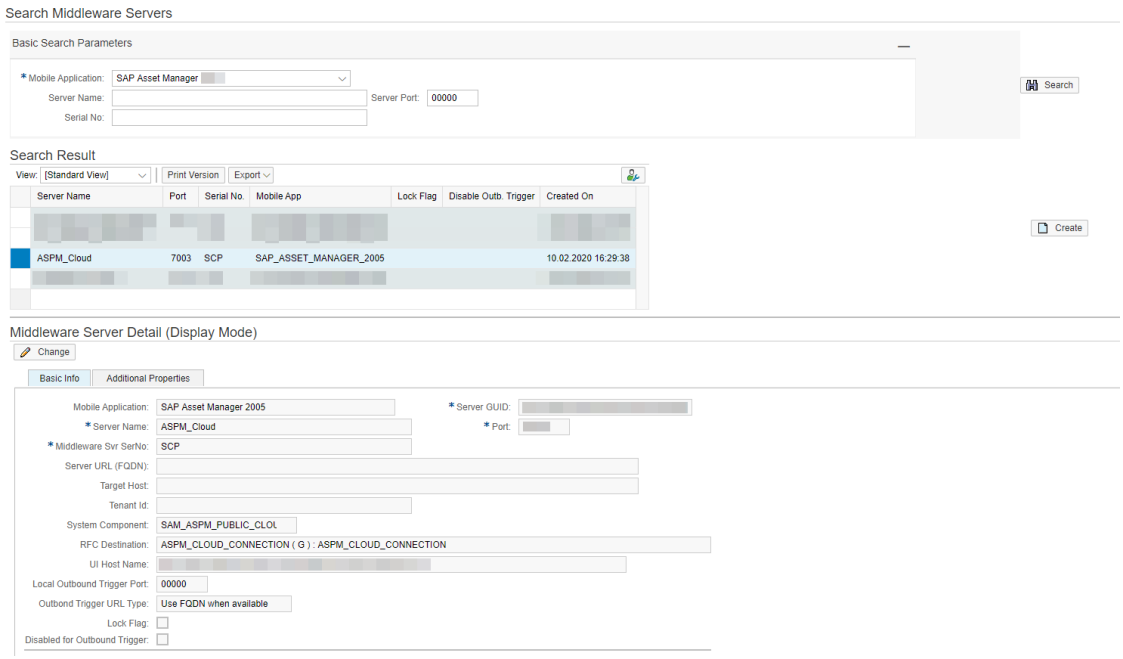
      The *System Components* page becomes editable.

c. Click the *Add* button in the *System Component List* to add a new component.
d. Create your new component using the following fields:
   - **System Component:** SAM_ASPM_PUBLIC_CLOUD
   - **Active Flag:** checked
   - **Primary Flag:** checked



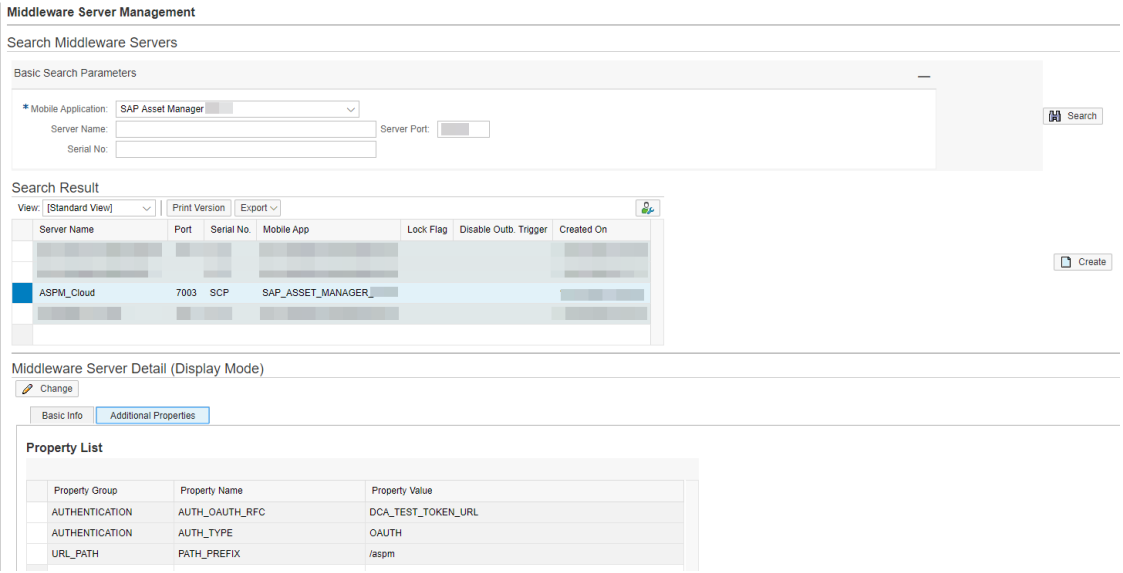
You've configured which system component you're connecting to the ASPM system.

2. Press the *Save* button. If necessary, move these changes to other systems in your landscape.
3. **Configure server component settings using the Admin Portal**
   a. Access the Admin Panel from the SAP GUI using transaction code */n/SYCLO/ADMIN*.
   b. From the main page of the Admin Portal, navigate to *Administration* > *Server Management*. In the *Search Middleware Servers* section, choose your application from the list in the `<Mobile Application>` field. Click *Search*.
   c. Click the *Create* button to add a new middleware server.
   d. In the *Middleware Server Detail* section, *Basic Info* tab, add the following fields:
      - **Server Name:** ASPM_CLOUD
      - **System Component:** SAM_ASPM_PUBIC_CLOUD
      - **RFC Destination:** [Select the ASPM RFC destination you previously created]



e. Select the *Additional Properties* tab. Add the following properties:

- Property Name: AUTH_OAUTH_RFC
  - Property Group: AUTHENTICATION
  - Property Value: [RFC destination created for oAuth token]
- Property Name: AUTH_TYPE
  - Property Group: AUTHENTICATION
  - Property Value: OAUTH
- Property Name: PATH_PREFIX
  - Property Group: URL_PATH
  - Property Value: [/ain or /aspm depended on Asset Central API version]



You've configured which ASPM system you're connecting to.

4. Click the *Save* button to save your new settings.

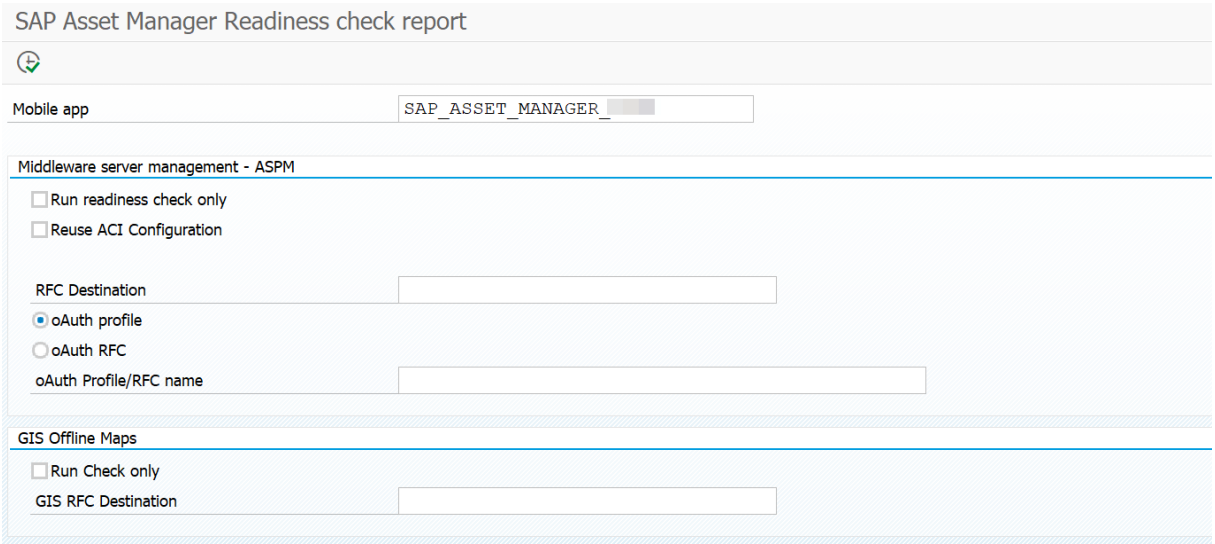
4.2.2.1 Checking the Readiness of the ASPM System

The ASPM readiness check program on the SAP GUI checks the readiness of the ASPM checklist feature.

> **Note**
>
> Before following the instructions in this topic, ensure that you've performed the Setting Up an ASPM Connection to the ASPM System to Use Checklists [page 252] procedure.

The readiness check program checks your set-up (performed in the Setting Up an ASPM Connection to the ASPM System to Use Checklists [page 252] procedure), such as the system component. If your configuration has an error, a red light displays on the output that isn't set up properly. The /syclo/admin set-up is also completed you've selected certain options listed in this topic.

Using the SAP GUI, execute the program */MERP/CORE_READINESS_CHK_PROG* to run the readiness check. The selections you make in this procedure are all found in the main *Middleware server management - ASPM* section. See the Readiness Check for Authenticated GIS Maps [page 260] procedure for details on the *GIS Offline Maps* section.

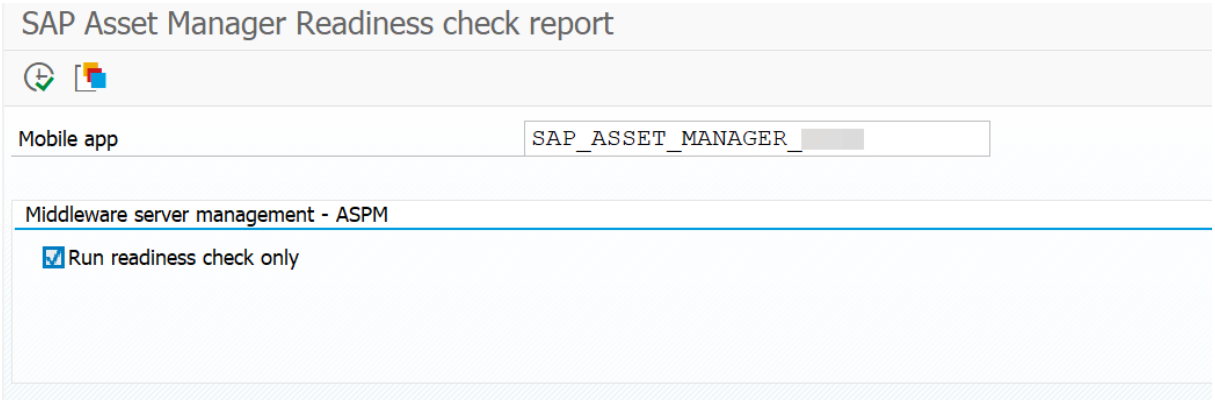


The readiness check program gives 3 options to check or complete the ASPM checklist for SAP Service and Asset Manager:

Run Readiness Check Only

This checkbox disables the rest of the inputs on the screen if checked. Choosing this option runs the program in check-only mode. No RFC destination or configuration is made. Select this option if you've performed all the steps in Setting Up an ASPM Connection to the ASPM System to Use Checklists [page 252]. Running the readiness check only confirms that no steps were missed. If there are errors in your set-up, a red light displays by the output. You can then use the transaction code for that output to fix the issue.

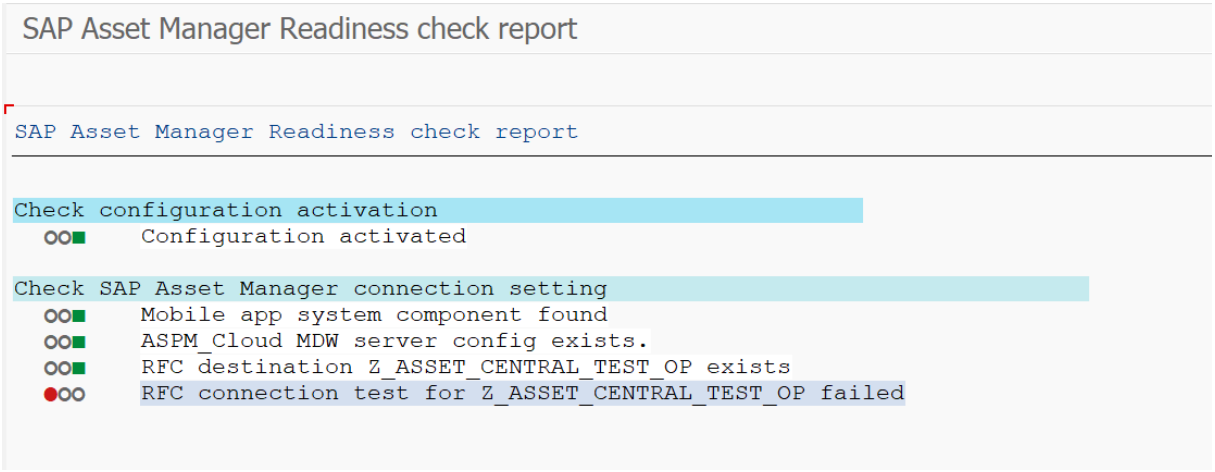
Input



Output

In the following sample screenshot, the red light result means that the RFC connection test used to set up the ASPM checklist feature has failed the connection test. To fix:

1. Enter transaction code *SM59* and test the connection.
2. If the connection fails, fix the issue by using a proxy. Make sure that configurations such as user credentials are correct.
3. Rerun the check program after fixing any issues to ensure a green light is displayed.

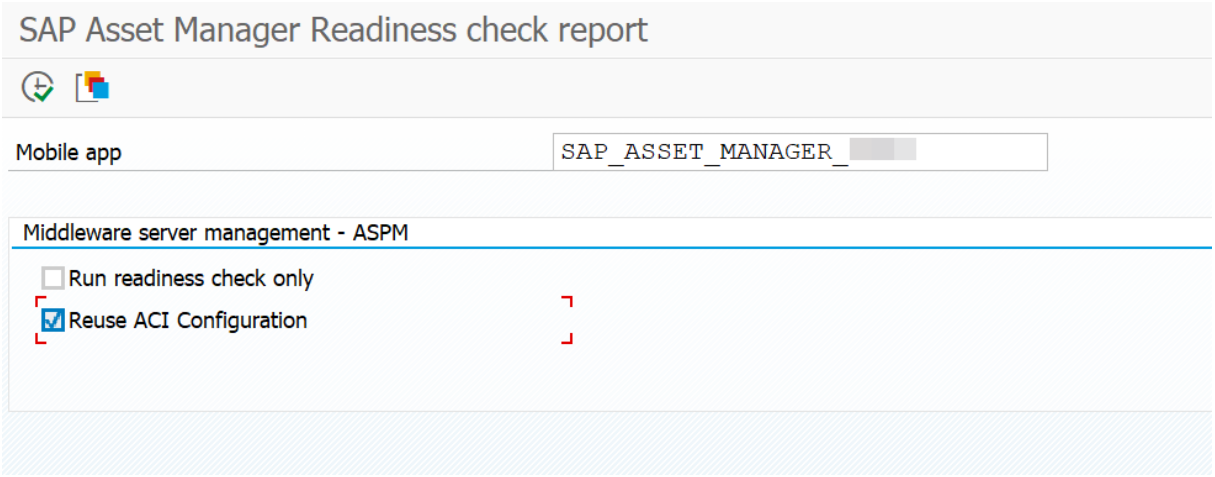


Reuse Asset Central Integration Configuration

Use this checkbox to reuse the ACI app if it exists. Selecting this option uses the same RFC destination and authentication properties to create a new server configuration.

Input

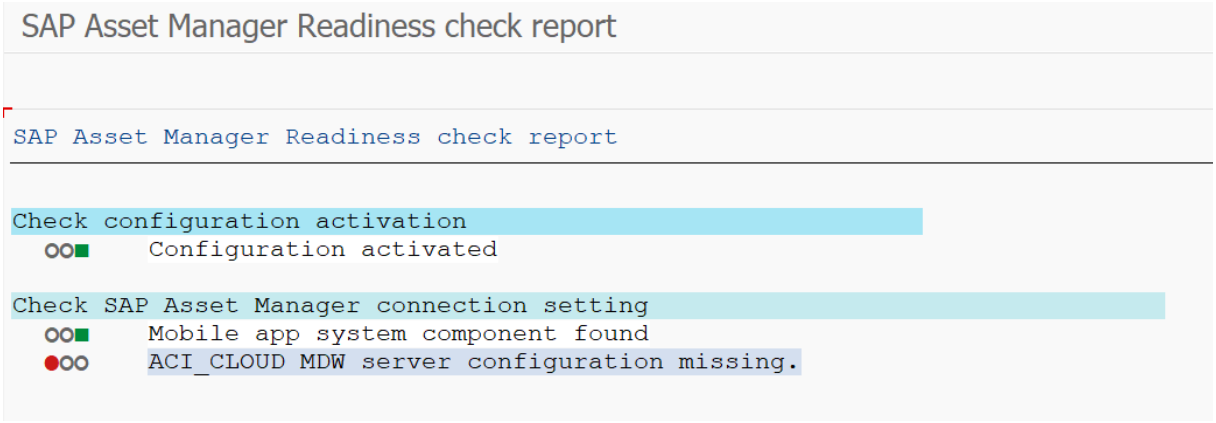
Use this option if *Step 3d* wasn't completed in the Setting Up an ASPM Connection to the ASPM System to Use Checklists [page 252] procedure and you want to result the RFC destination used for ACI configuration to complete the set-up .



Error Output Example

This option uses the ACI middleware configuration to create the ASPM_CLOUD server configuration for SAP Service and Asset Manager. If ACI configuration doesn't exist, use the *Input RFC Destination* option to create the configuration.

The red light shown in the following example screenshot shows the error thrown when there's no ACI configuration in the customer system to reuse. If a red light is displayed, complete the set-up, then run the check program in reuse mode to complete the ASPM checklist set.



Input RFC Destination

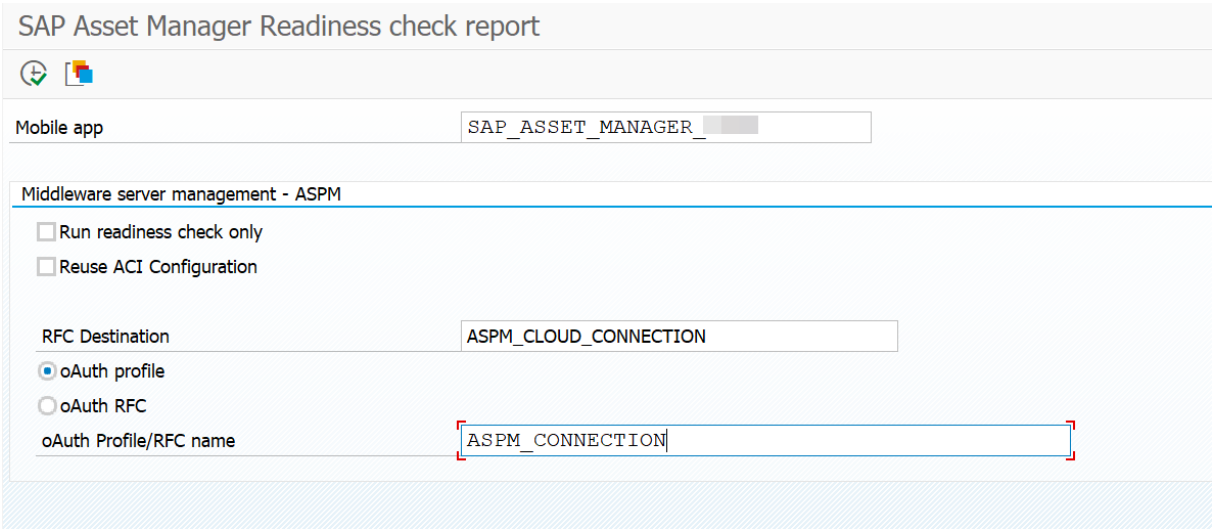
Create the RFC destination or middleware server configuration: Using the *RFC Destination* section, give an *RFC Destination*, select an *oAuth Method* and *oAuth Value*. An RFC destination and/or middleware server configuration is created if they don't already exist.

Use this option if *Step 3d* wasn't completed in the Setting Up an ASPM Connection to the ASPM System to Use Checklists [page 252] procedure and you want to complete the rest of the set-up-up, along with the RFC destination creation. Once the destination is created, or if the destination exists, but the ASPM feature set up in */SYCLO/ADMIN* doesn't exist, this program completes the set-up with the RFC destination.

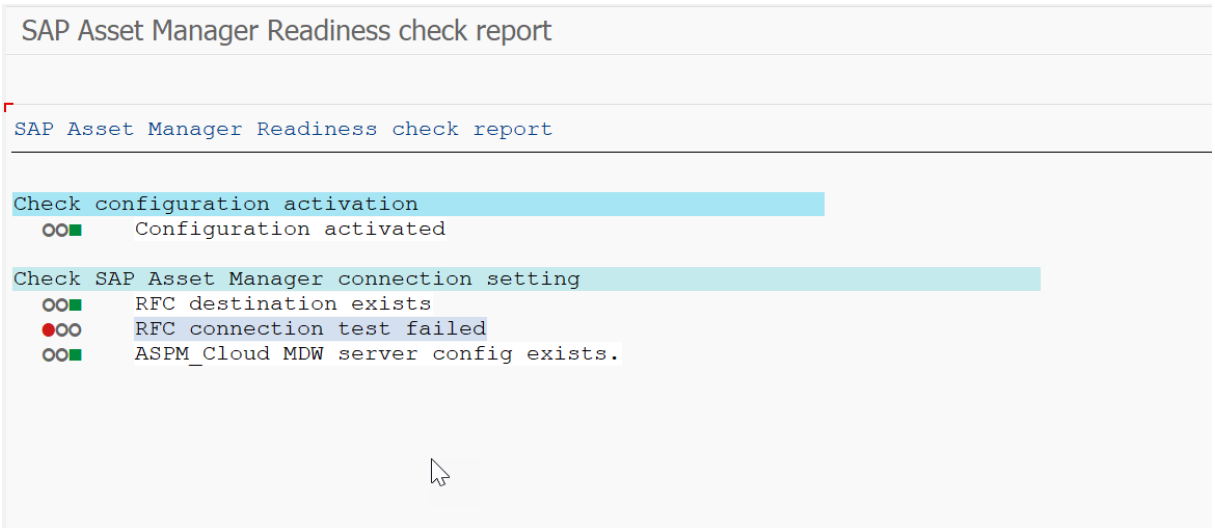
If the RFC destination and middleware configuration don't exist; the program redirects to the *RFC Destination Creation* screen. Once the RFC destination is ready, it creates a management entry for the middleware server in the configuration tables for SAP Service and Asset Manager.

> **Note**
>
> For SAP_BASIS release 752 and above, use the radio button *oAuth Profile* and property *AUTH_OAUTH_PROFILE*. For earlier versions, use the radio button *oAuth RFC* and property *AUTH_OAUTH_RFC*.

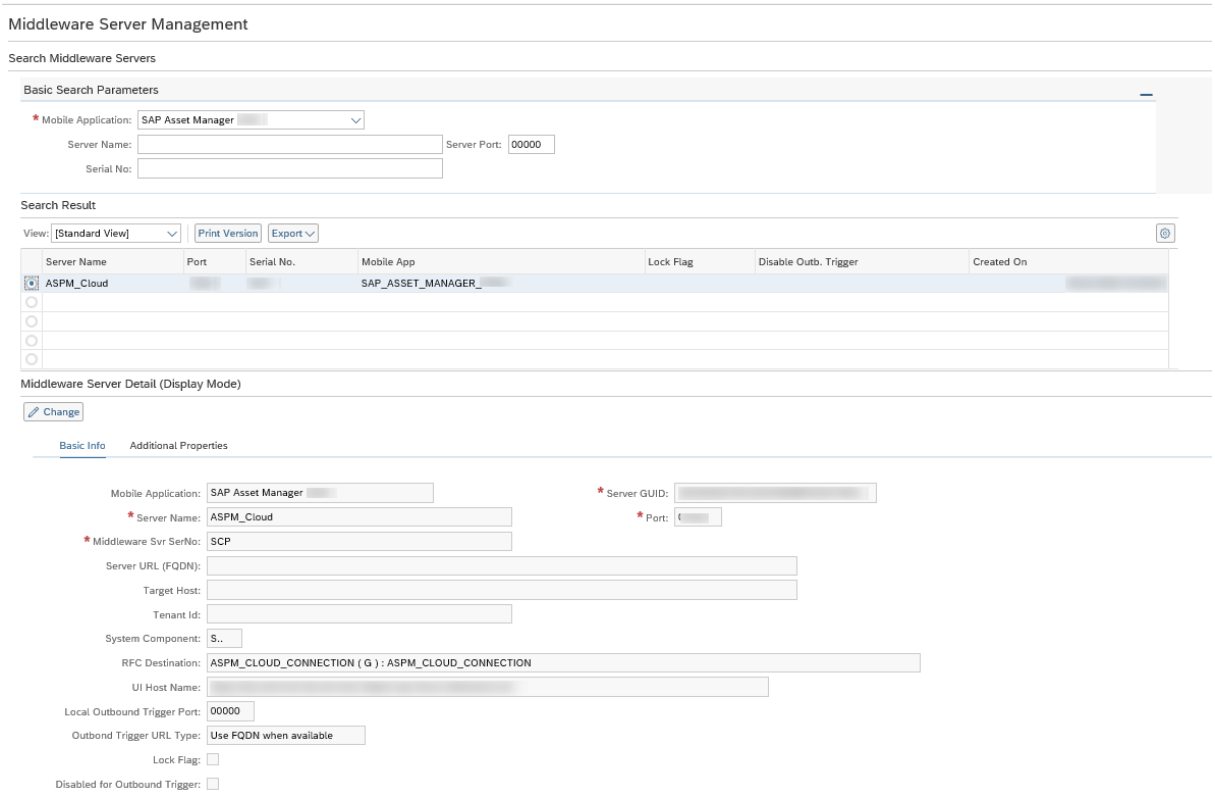
Input



Output



The */SYCLO/ADMIN* ConfigPanel entry the ASPM readiness check program checks or creates is shown in the following example:



Troubleshooting

If the output of the readiness check shows the RFC connection test failed, perform a manual test. Make sure to add a proxy and/or certificate to *STRUST* if needed.

You can manually change the middleware server configuration via */SYCLO/ADMIN*.

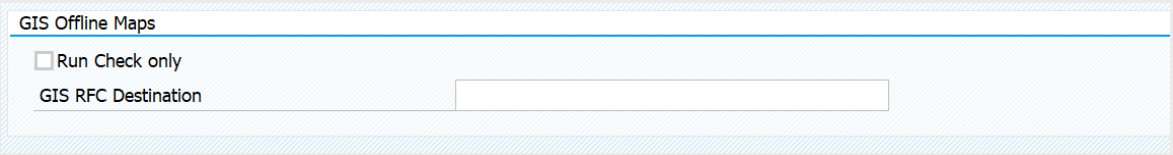
Next Steps

If you're using SAP Service and Asset Manager with authenticated GIS, continue to the Readiness Check for Authenticated GIS Maps [page 260] topic.

4.2.2.1.1 Readiness Check for Authenticated GIS Maps

Context

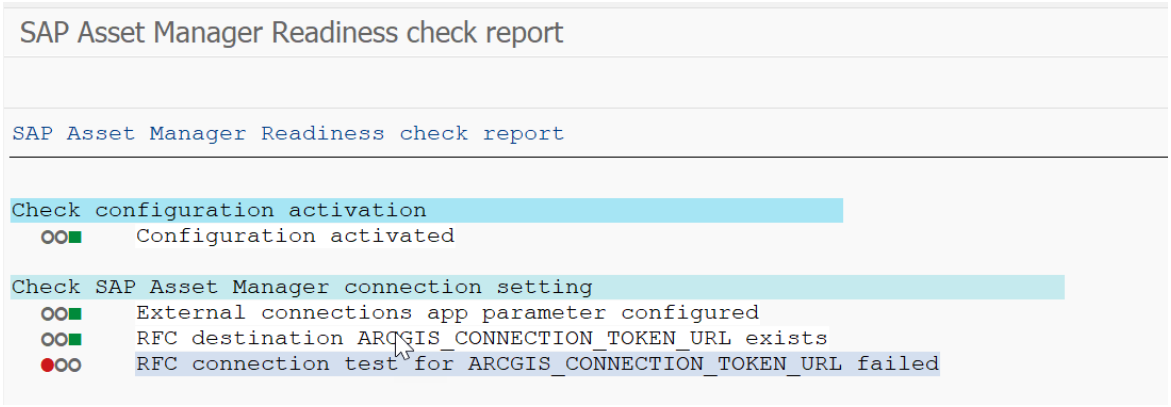
> **Note**
>
> Before performing this procedure, follow the appropriate ASPM readiness check. See the Checking the Readiness of the ASPM System [page 255] topic for details.



Procedure

1. **Run Readiness Check Only**

   Example of *Run Check only* output:

2. **Create the RFC Destination:** Creating the RFC destination stores the GIS server login credentials and adds them to the mobile application parameter.

Example of *GIS RFC Destination* and config parameter output:

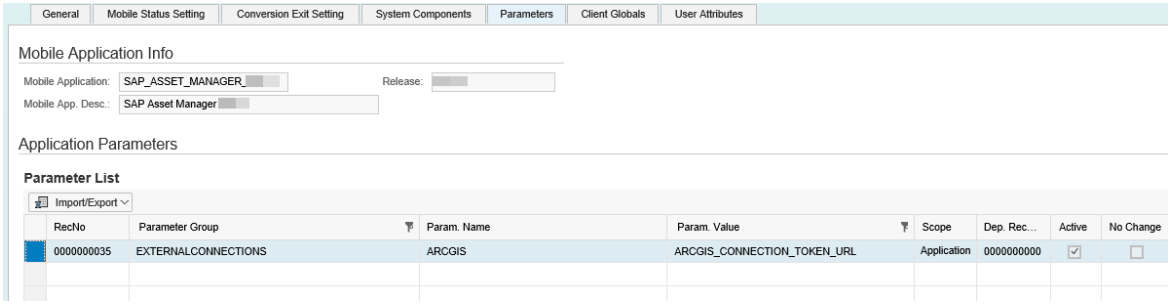
SAP Asset Manager Readiness check report

```
SAP Asset Manager Readiness check report

Check configuration activation
   OO■    Configuration activated

Check SAP Asset Manager connection setting
   ●OO    External connections app parameter not configured
   OO■    RFC destination ARCGIS_CONNECTION_TOKEN_URL exists
   ●OO    RFC connection test for ARCGIS_CONNECTION_TOKEN_URL failed
   ●OO    External connections app parameter cannot be configured without RFC
```

The */SYCLO/ADMIN* ConfigPanel entry the Authenticated GIS readiness check program checks or creates is shown in the following example:



4.3 Assignment Management of Safety-Related Features

Safety Technicians can see a filtered list of items on their mobile devices that are assigned to them. This applies to the following list screens:

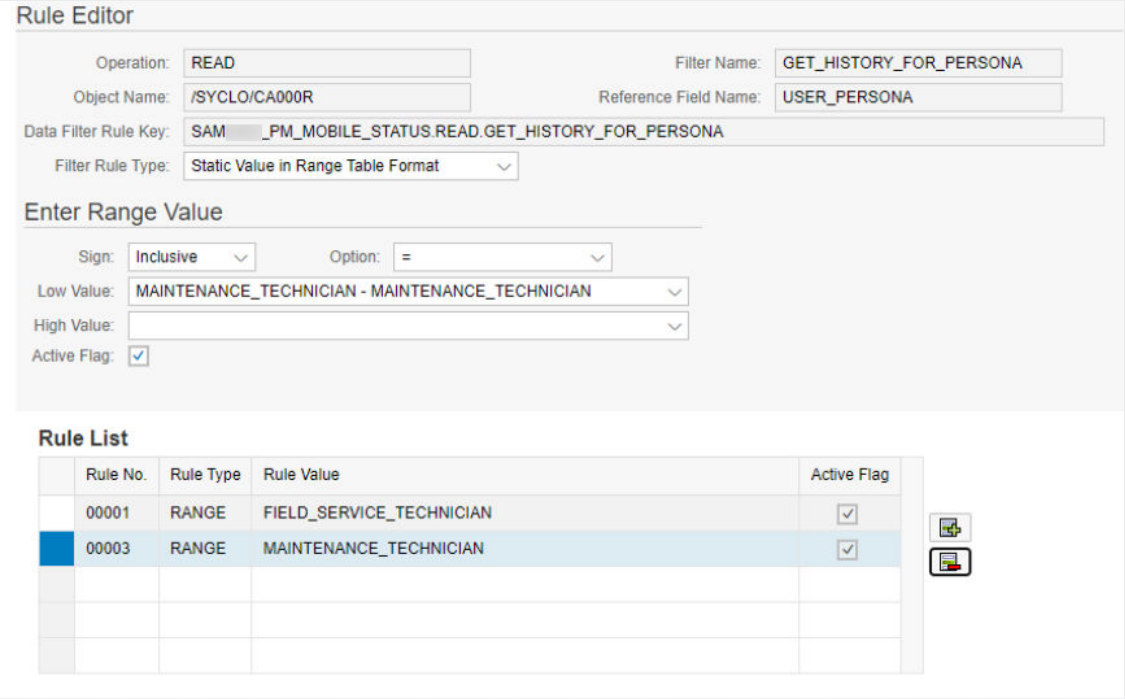
- Operational Items
- Isolation Certificates
- Other Cerificates
- Work Permits
- Work Orders (linked to the assigned objects)
- Work Approvals (linked to the assigned objects)

> **Note**
>
> - For more information about how to filter assigned objects, see Filtering Your Assigned Objects.
> - The procedures in this section are applicable to **safety-related** assignment configuration. For more information about assigning Work Orders, see Work Order Assignment Type Options [page 150].

Supported Personas

This feature is applicable for the following personas:

Maintenance Technician (Pro)
Safety Technician

> **Note**
>
> - For the Maintenance Technician (Pro) persona, this feature is only available from 2410 version.
> - If the user uses Safety Technician (WCM) features via the Maintenance Technician (Pro) persona, you need to add the persona to the data filter *SAMXXXX_PM_MOBILE_STATUS* > *GET_HISTORY_FOR_PERSONA*:
>
> 
>

Limitations

See Configuration Prerequisites and Limitations - Safety Technician Persona [page 216].

Configuration

Perform the following configuration steps to enable the *Assigned to me* filtering option for users by the following Assignment Types:

- Assignment Type 1: User Plant [page 263]

- Assignment Type 2: User Work Center [page 266]
- Assignment Type 3: User Planner Group [page 268]
- Assignment Type 4: Partner Function (Approval Roles + Partner Functions) [page 270]
- Assignment Type 5: Selection Variant [page 276]
- Assignment Type 6: Operational List (Operational list + Selection Variant) [page 281]

> **Note**
>
> *5 - Selection Variant* and *6 - Operational List (Operational list + Selection Variant)* are non-regular Assignment Types, dedicated to provide additional assignment functionalities. You can create selection variants, define filters for them, and assign the variant to users. Then the filters from the variant will be used during a sync. When only these assignment types are set up, regular oMDO filters are not taken into account during the sync.

4.3.1 Configuring Assignment Type 1 (User Plant)

Context

> **Note**
>
> This procedure is applicable to **safety-related** assignment configuration. For detailed information, see the overview topic, Assignment Management of Safety-Related Features [page 261].

To enable the Assigned to me filtering option for users by the *1 - User Plant* Assignment Type, perform the following steps:

General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **OMDO** and **OMDO filter** configuration:
  - General oMDO Configuration - Safety Technician Persona [page 221]
  - OData Mobile Data Object Configuration and OData Mobile Data Object Configuration - Data Filter Tab in *MAIF Configuration Guide*.
- **User Parameters** configuration: refer to Administration - User Management in *MAIF Administrator Guide*.

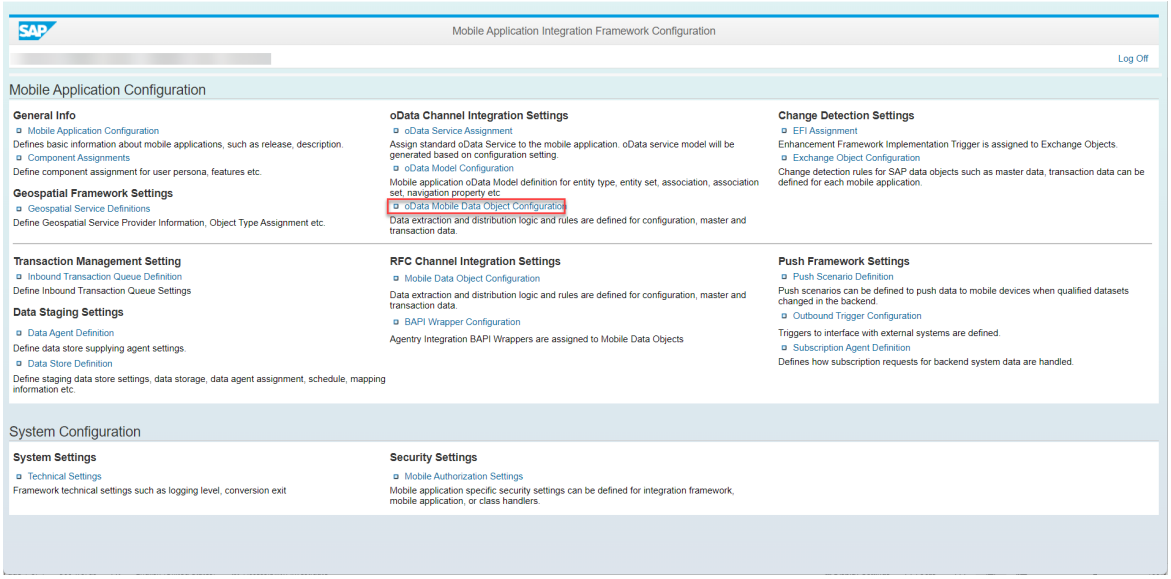
Procedure

User Parameter Configuration

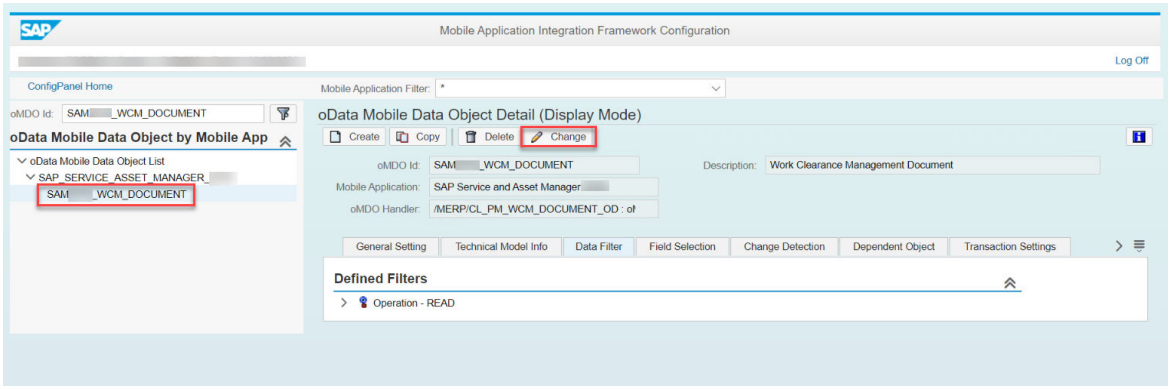
1. In *SAP GUI*, navigate to the *SU3* transaction and configure User Parameters. See General User Parameters Configuration - Safety Technician Persona [page 227].

oMDO Configuration

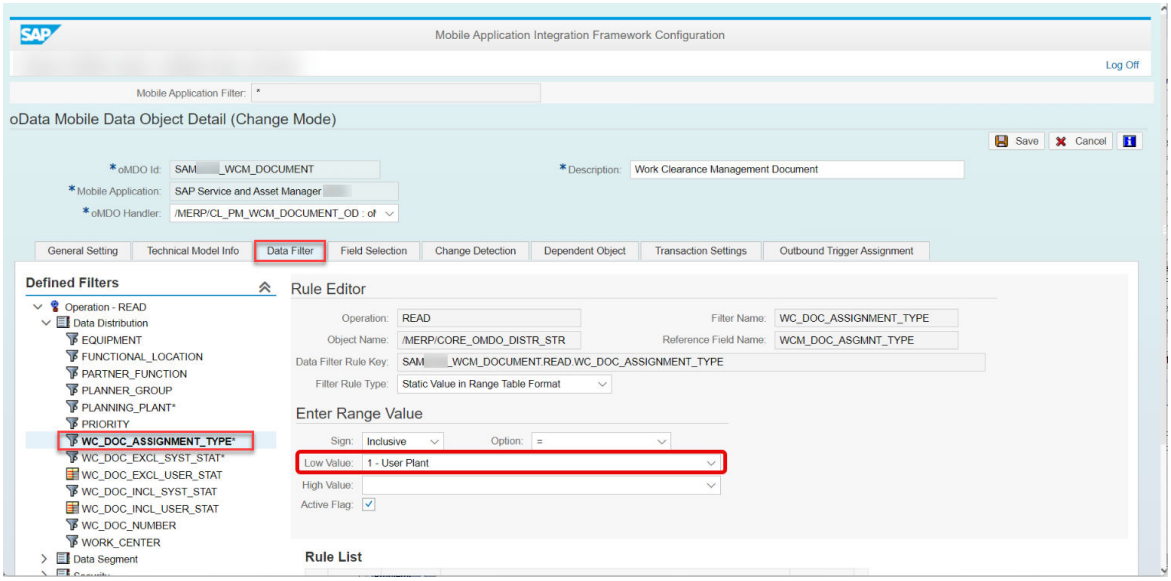
2. Under *oData Channel Integration Settings*, navigate to *oData Mobile Data Configuration*.



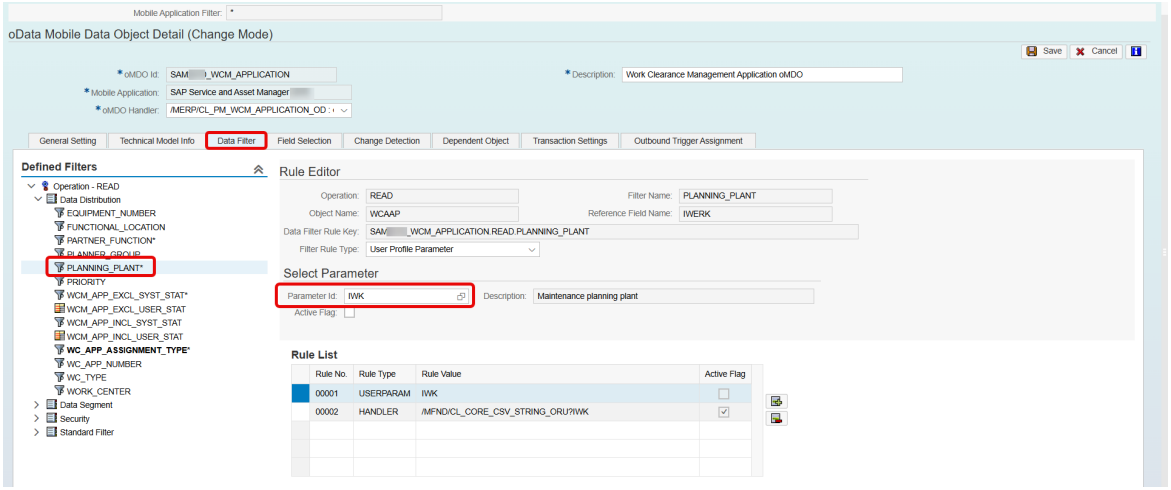
3. From the list of oMDOs, select the relevant object and click *Change*:
   - *SAMXXXX_WCM_DOCUMENT* for Isolation Cerificates [page 446] (also referred to as Safety Cerificates)
   - *SAMXXXX_WCM_APPLICATION* for Work Permits [page 565]



4. Under the *Data Filter* tab, select:
   - *WC_DOC_ASSIGNMENT_TYPE* for Isolation Cerificates [page 446]
   - *WC_APP_ASSIGNMENT_TYPE* for Work Permits [page 565]
5. From the *Low Value* drop-down list, choose *1 - User Plant* as assignment type.



6. Under the *Data Filter* tab, select *PLANNING_PLANT*, then select *IWK* (Maintenance planning plant) as *Parameter ID*.



> **Note**
>
> For more information, see User Parameter IDs [page 606].

7. Save your changes.

4.3.2 Configuring Assignment Type 2 (User Work Center)

Context

> **Note**
>
> This procedure is applicable to **safety-related** assignment configuration. For detailed information, see the overview topic, Assignment Management of Safety-Related Features [page 261].

To enable the Assigned to me filtering option for users by the *2 - User Work Center* Assignment Type, perform the following steps:

General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **OMDO** and **OMDO filter** configuration:
  - General oMDO Configuration - Safety Technician Persona [page 221]
  - OData Mobile Data Object Configuration and OData Mobile Data Object Configuration - Data Filter Tab in *MAIF Configuration Guide*.
- **User Parameters** configuration: refer to Administration - User Management in *MAIF Administrator Guide*.

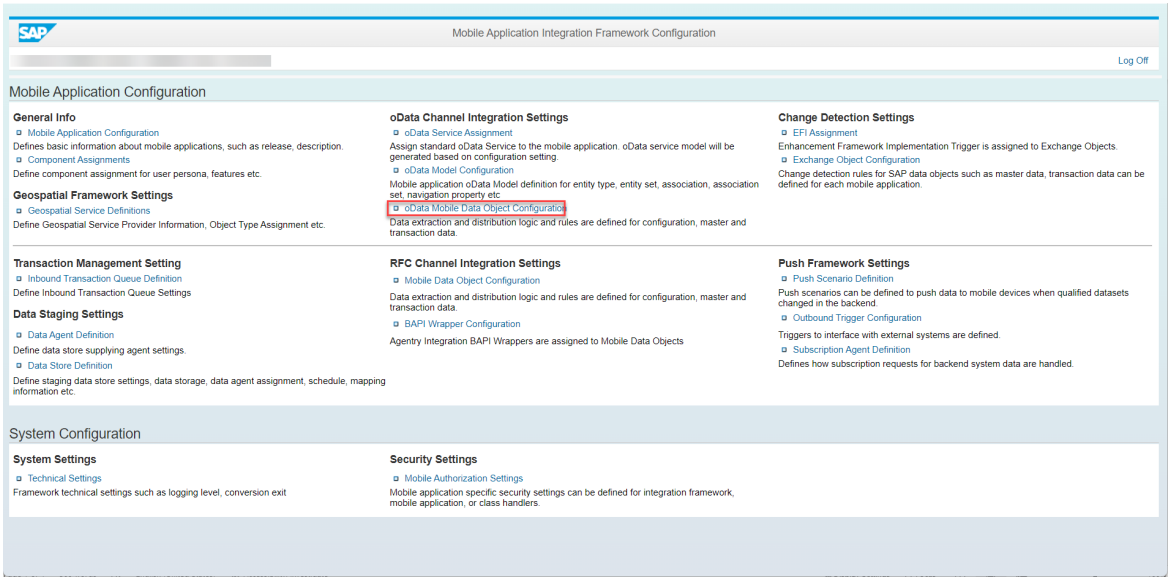
Procedure

User Parameter Configuration

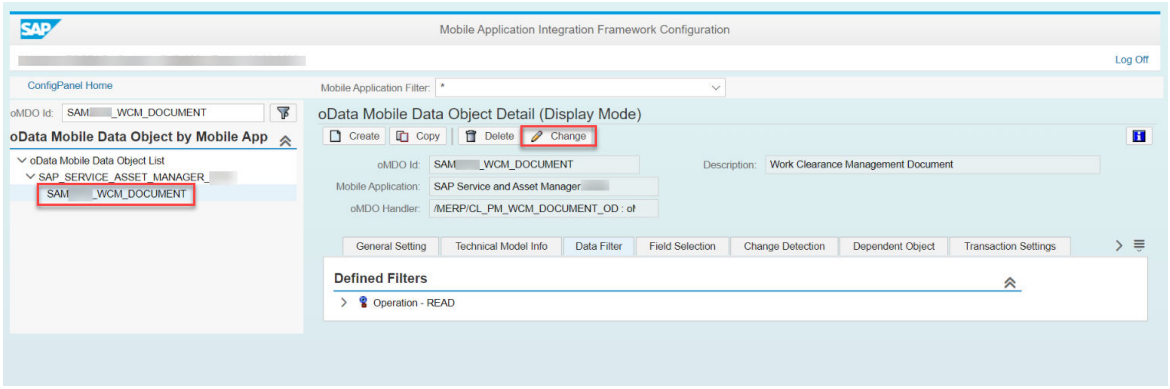
1. In *SAP GUI*, navigate to the *SU3* transaction and configure User Parameters. See General User Parameters Configuration - Safety Technician Persona [page 227].

oMDO Configuration

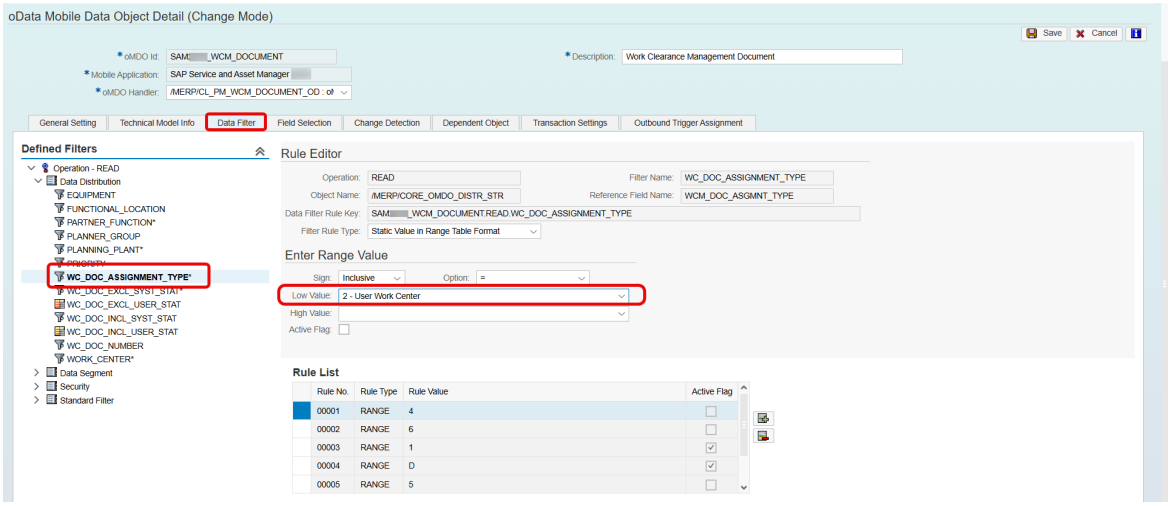
2. Under *oData Channel Integration Settings*, navigate to *oData Mobile Data Configuration.*



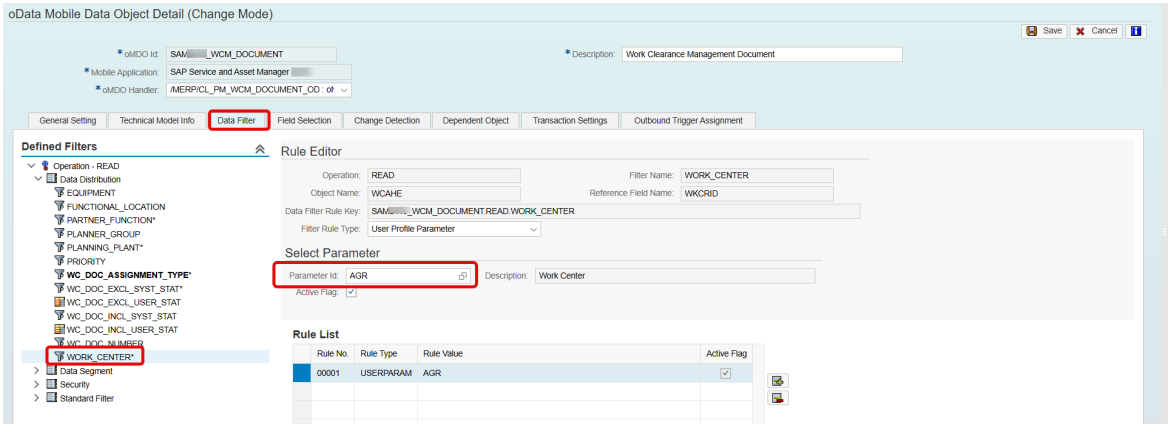
3. From the list of oMDOs, select the relevant object and click *Change*:
    - *SAMXXXX_WCM_DOCUMENT* for Isolation Cerificates [page 446] (also referred to as Safety Cerificates)
    - *SAMXXXX_WCM_APPLICATION* for Work Permits [page 565]



4. Under the *Data Filter* tab, select:
    - *WC_DOC_ASSIGNMENT_TYPE* for Isolation Cerificates [page 446]
    - *WC_APP_ASSIGNMENT_TYPE* for Work Permits [page 565]
5. From the *Low Value* drop-down list, choose *2 - User Work Center* as assignment type.



6. Under the *Data Filter* tab, select *WORK_CENTER*, then select *AGR* (Work center) as *Parameter ID*.



> **Note**
>
> For more information, see User Parameter IDs [page 606].

7. Save your changes.

4.3.3 Configuring Assignment Type 3 (User Planner Group)

Context

> **Note**
>
> This procedure is applicable to **safety-related** assignment configuration. For detailed information, see the overview topic, Assignment Management of Safety-Related Features [page 261].

To enable the Assigned to me filtering option for users by the *2 - User Planner Group* Assignment Type, perform the following steps:

General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **OMDO** and **OMDO filter** configuration:
  - General oMDO Configuration - Safety Technician Persona [page 221]
  - OData Mobile Data Object Configuration and OData Mobile Data Object Configuration - Data Filter Tab in *MAIF Configuration Guide*.
- **User Parameters** configuration: refer to Administration - User Management in *MAIF Administrator Guide*.

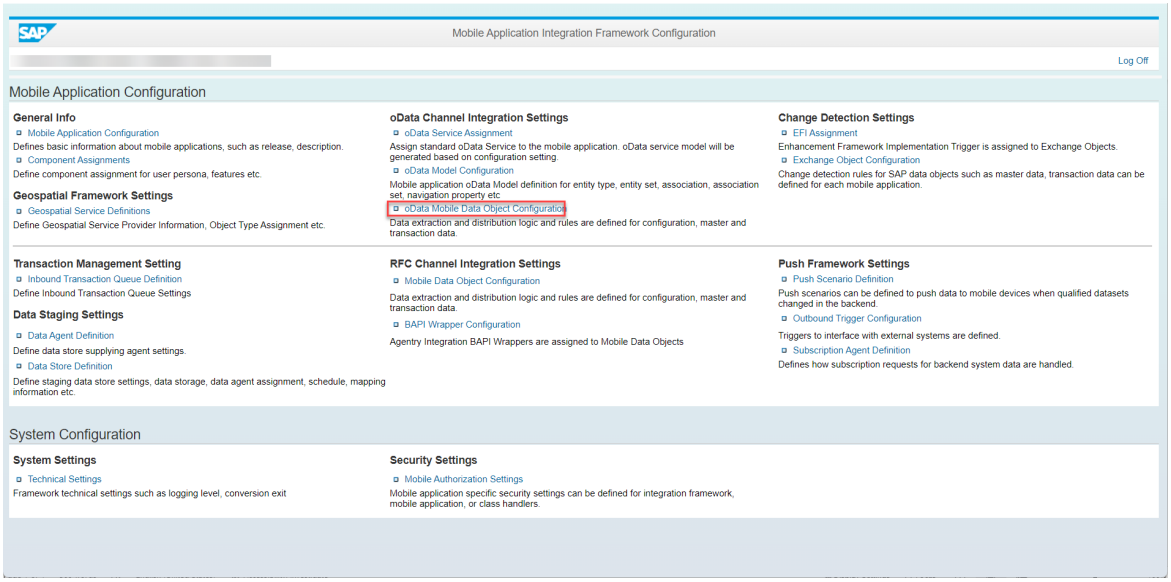
Procedure

User Parameter Configuration

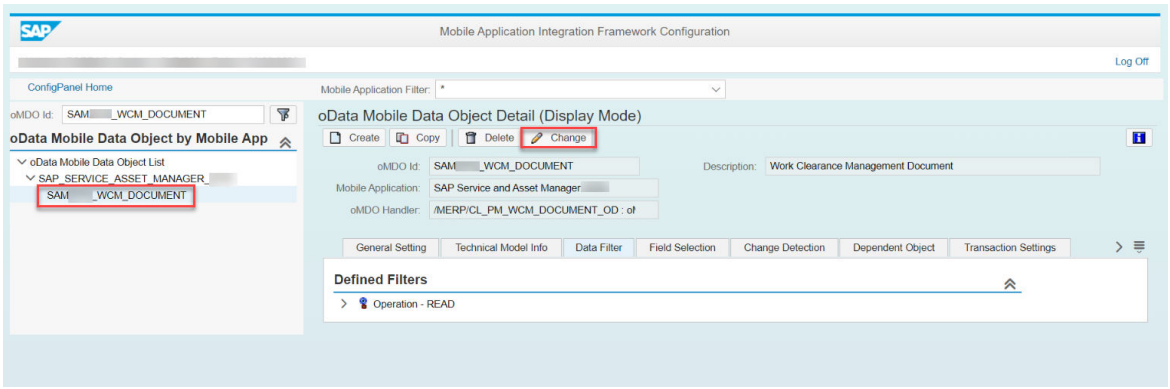
1. In *SAP GUI*, navigate to the *SU3* transaction and configure User Parameters. See General User Parameters Configuration - Safety Technician Persona [page 227].

oMDO Configuration

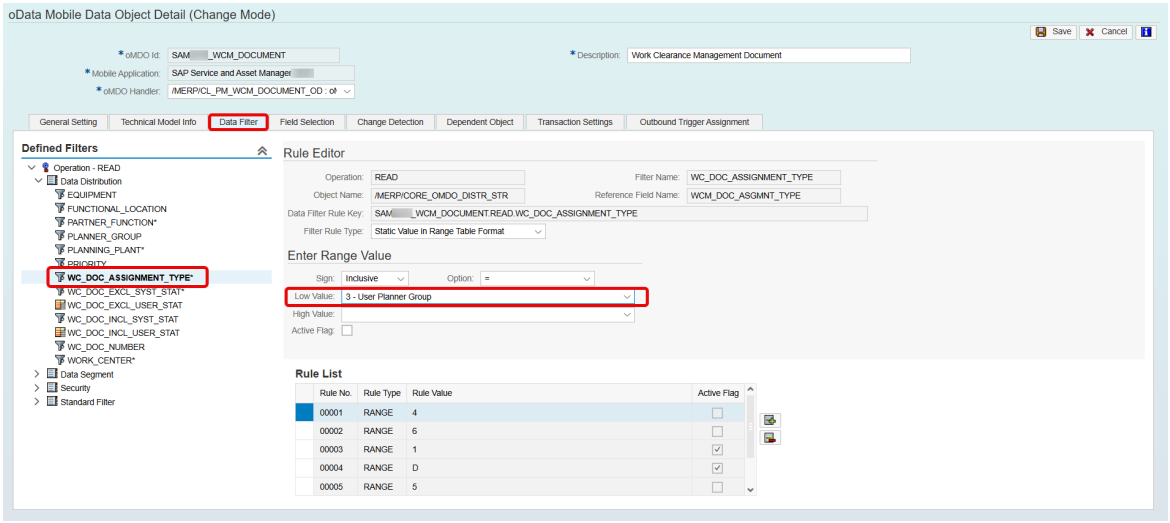
2. Under *oData Channel Integration Settings*, navigate to *oData Mobile Data Configuration.*



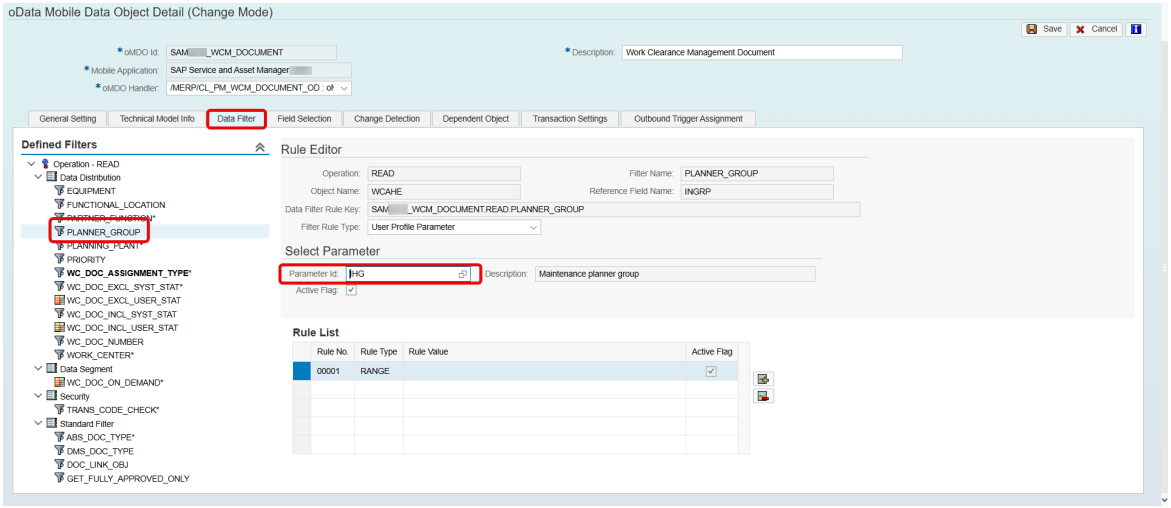
3. From the list of oMDOs, select the relevant object and click *Change*:
   - *SAMXXXX_WCM_DOCUMENT* for Isolation Cerificates [page 446] (also referred to as Safety Cerificates)
   - *SAMXXXX_WCM_APPLICATION* for Work Permits [page 565]



4. Under the *Data Filter* tab, select:
   - *WC_DOC_ASSIGNMENT_TYPE* for Isolation Cerificates [page 446]
   - *WC_APP_ASSIGNMENT_TYPE* for Work Permits [page 565]
5. From the *Low Value* drop-down list, choose *2 - User Planner Group* as assignment type.



6. Under the *Data Filter* tab, select *PLANNER_GROUP*, then select *IHG* (Maintenance planner group) as *Parameter ID*.



> **Note**
>
> For more information, see User Parameter IDs [page 606].

7. Save your changes.

4.3.4 Configuring Assignment Type 4 (Partner Function)

Context

> **Note**
>
> This procedure is applicable to **safety-related** assignment configuration. For detailed information, see the overview topic, Assignment Management of Safety-Related Features [page 261].

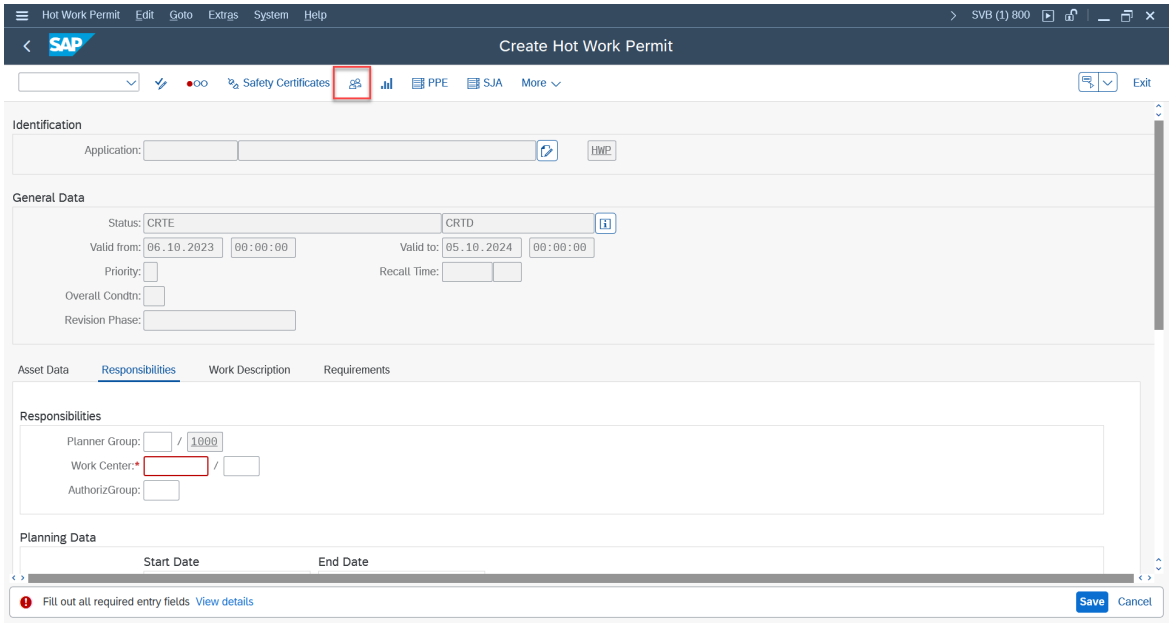
To enable the Assigned to me filtering option for users by the *4 - Partner Function (Approval Roles + Partner Functions* Assignment Type, perform the following steps:

> **Note**
>
> - This procedure applies to Work Permits (and related Work Orders, Work approvals) and Isolation Certificates (and related Operational Items).
> - Regarding the order of steps, it does not matter if you perform the SAP GUI or Configuration Panel changes first.
> - If you want to enable for Safety Technicians to filter for objects assigned to other users as well, perform the additional steps from Configuring the ShowAssignedToList parameter [page 274].

Procedure

SAP GUI changes

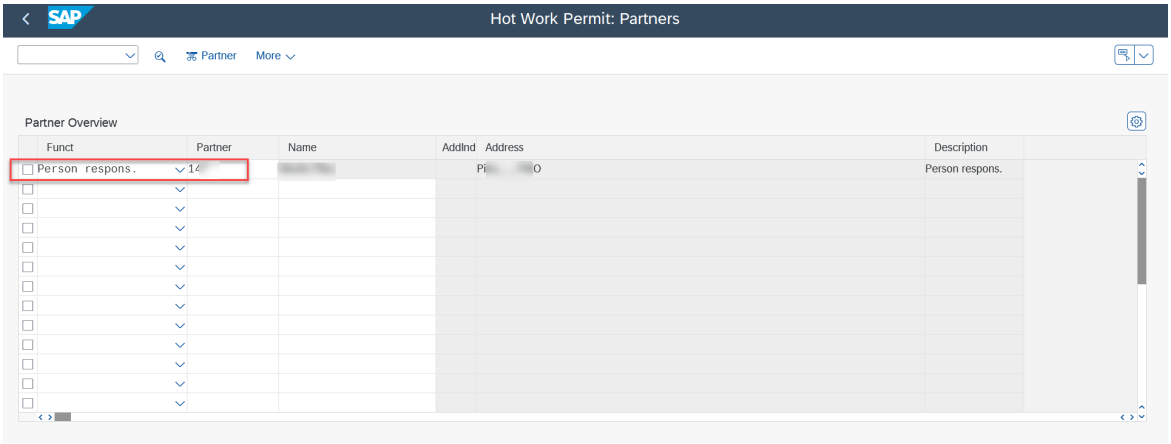
1. Create a new (or change existing) Work Permit or Safety Cerificate.
   - To create a new **Work Permit**, use the transaction code `WCTK`.
   - To create a new **Safety Cerificate**, use the transaction code `WCT6`.
2. After the Initial Screen, click the *Create Partner* icon at the top of the Create Work Permit / Safety Cerificate screen.



> **Note**
>
> To do that, first you have to fill in the *Work Center* field.

3. On the *Partners* screen, fill in partner data as follows:
   1. *Partner Function*: From the drop-down, select *Person Responsible*.
   2. *Partner*: Enter the Personal Number of the user, who you would like to assign to the Work Permit / Safety Cerificate.

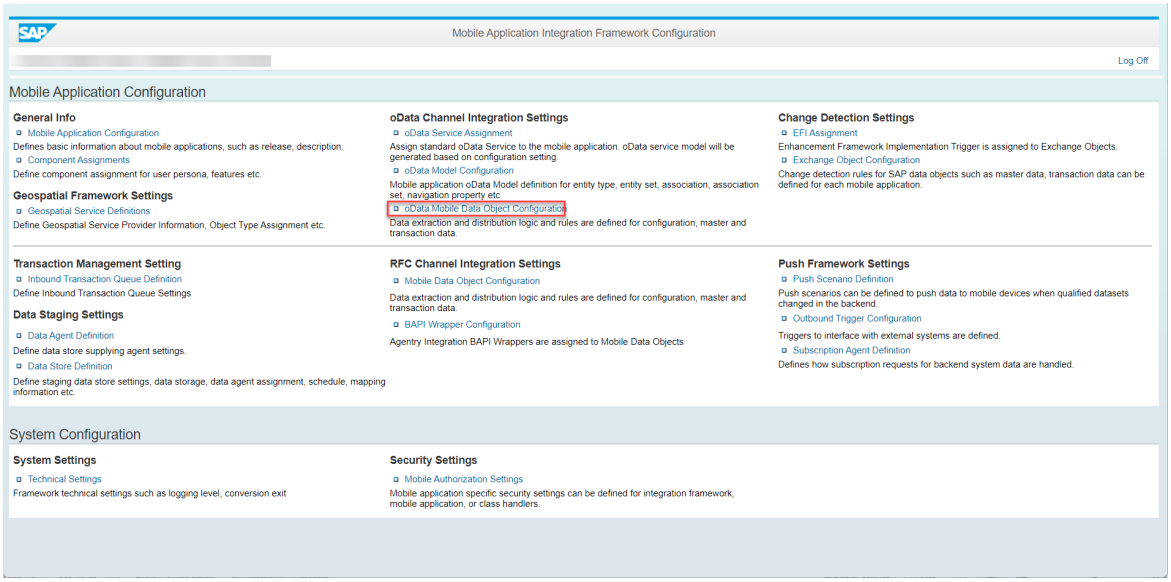
3. All other fields will be filled automatically.



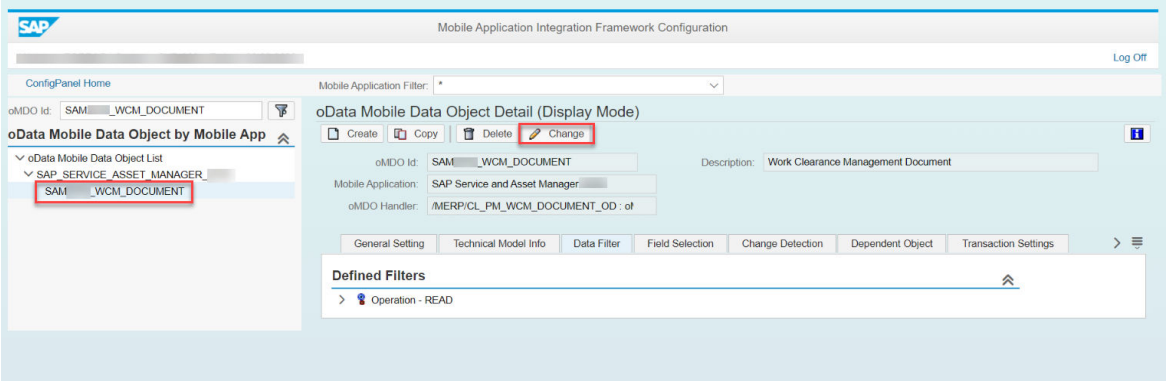
> **Note**
>
> - If the user does not have a Personal Number yet, you need to create it in the SAP HR Module.
> - By using *Person Responsible* as *Partner Function*, you can assign a specific SAP user to the Work Permit / Safety Cerificate.

oMDO Configuration

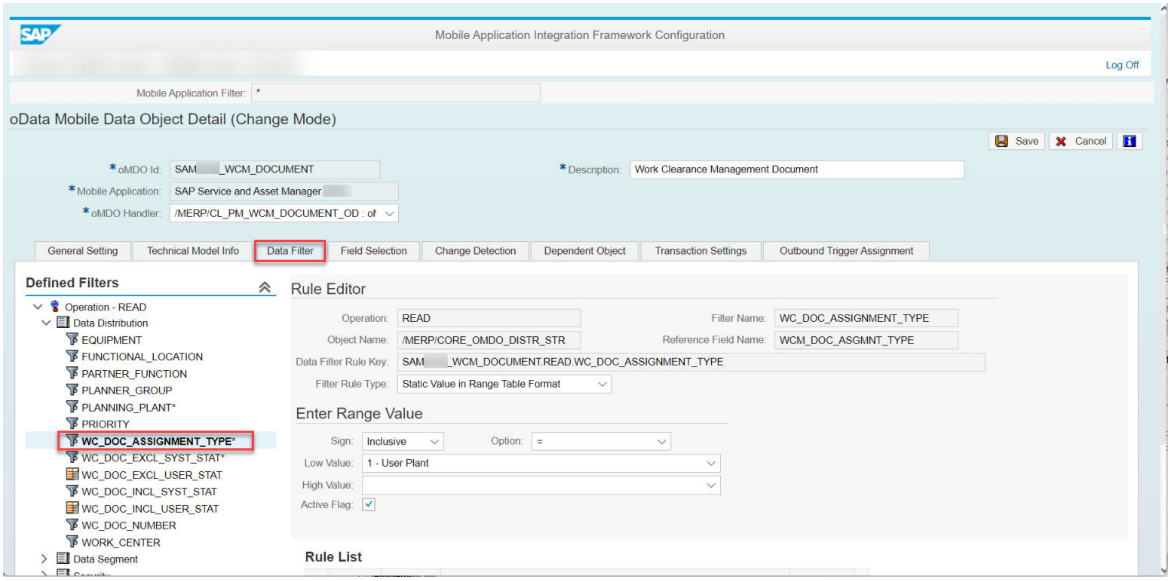
4. In the *SAP GUI*, navigate to the `/n/syclo/configpanel` transaction to open the Configuration Panel.
5. Under *oData Channel Integration Settings*, navigate to *oData Mobile Data Configuration*.



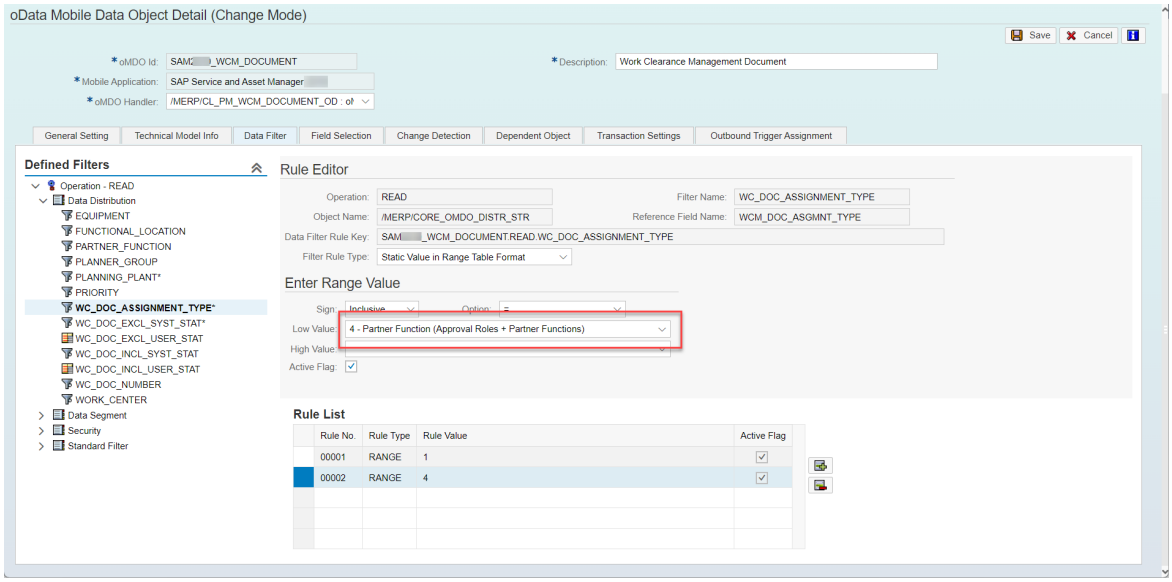
6. From the list of oMDOs, select the relevant object and click *Change*:
   - *SAMXXXX_WCM_DOCUMENT* for Isolation Cerificates [page 446] (also referred to as Safety Cerificates)
   - *SAMXXXX_WCM_APPLICATION* for Work Permits [page 565]



7. Under the *Data Filter* tab, select:
   - *WC_DOC_ASSIGNMENT_TYPE* for Isolation Cerificates [page 446]
   - *WC_APP_ASSIGNMENT_TYPE* for Work Permits [page 565]



8. From the Low Value drop-down list, choose *4 - Partner Function (Approval Roles + Partner Functions)* as assignment type.

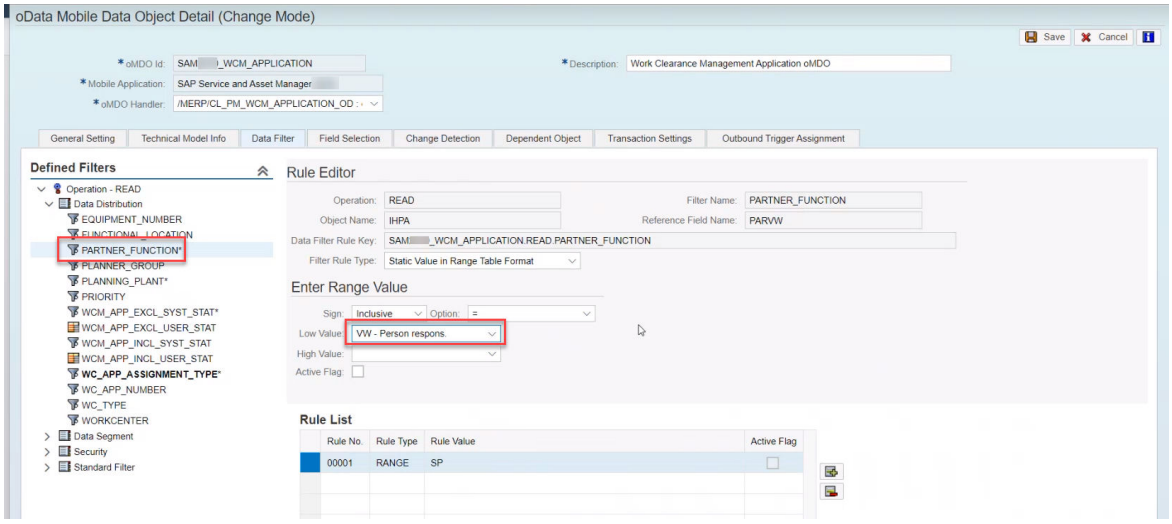


Note

Consider the following in the *Rule List* table, *Rule Value* column:

- If there is only one row with assignment type *4*, then only the objects assigned to the user will be downloaded to the client (*Assigned to me* button will not be displayed).
- If there are two rows with assignment types *1* and *4* (see the screenshot above), then all the objects will be donwloaded to the client and the user can filter them with the *Assigned to me* button.

9. Under the *Data Filter* tab, select *PARTNER_FUNCTION*, then *VW - Person responsible* from the Low Value drop-down list.



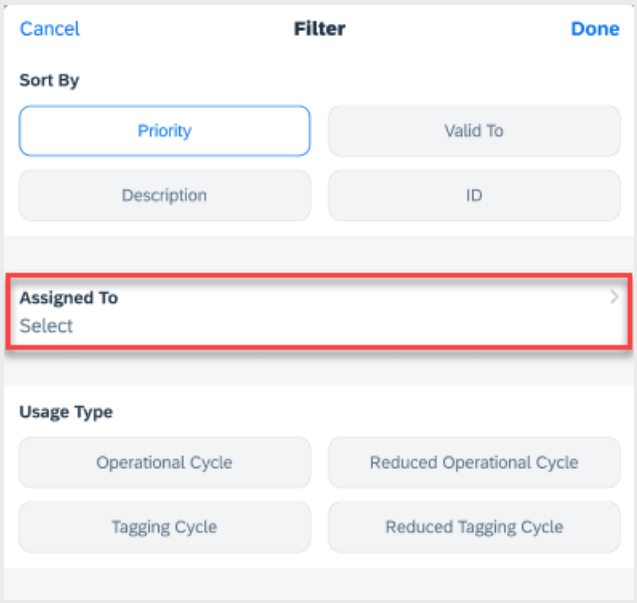
10. Click *Save* to exit Change Mode.

Configuring the ShowAssignedToList parameter

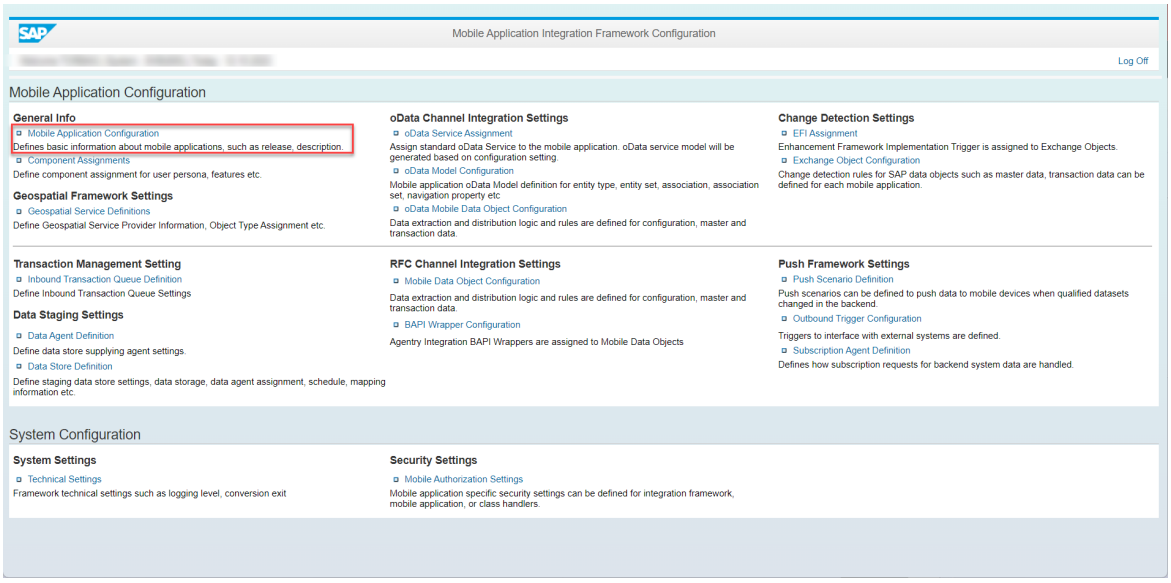
Note

The following steps are optional, perform them if you want to enable for Safety Technicians to filter not just their assigned objects, but the assigned objects of other specific users as well. This filtering option will be

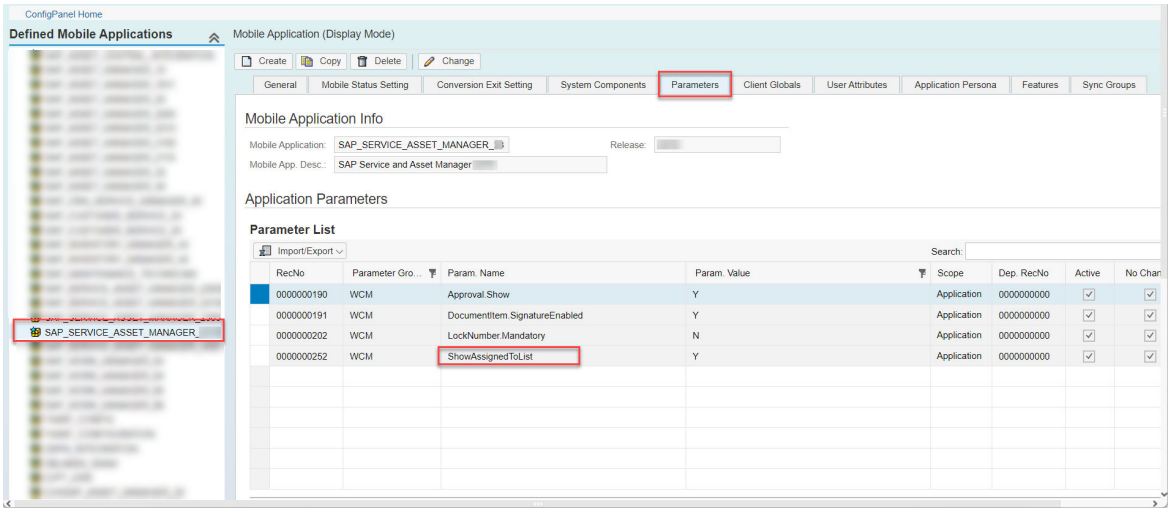
available in the *Filter* menu, from the *Assigned To* drop-down list. For more information, see Filtering Your Assigned Objects.



11. In the Configuration Panel, navigate to *Mobile Application Configuration*.



12. Select the application from the list, go to *Parameters* tab and click the *ShowAssignedToList* parameter.



13. Enter Change Mode and set the *Parameter Value* to *Y*.

> **Note**
>
> - If the *Parameter Value* is *Y*, the user will see the *Assigned To* filtering option (filtering for other users as well).
> - If the *Parameter Value* is *N*, the user will see the *Assigned To Me* filtering option (filtering only own assigned objects).

14. Click *Save* to exit Change Mode.

4.3.5 Configuring Assignment Type 5 (Selection Variant)

Context

> **Note**
>
> - This procedure is applicable to **safety-related** assignment configuration. For detailed information, see the overview topic, Assignment Management of Safety-Related Features [page 261].
> - *5 - Selection Variant* and *6 - Operational List (Operational list + Selection Variant)* are non-regular Assignment Types, dedicated to provide additional assignment functionalities. You can create selection variants, define filters for them, and assign the variant to users. Then the filters from the variant will be used during a sync. When only these assignment types are set up, regular oMDO filters are not taken into account during the sync.

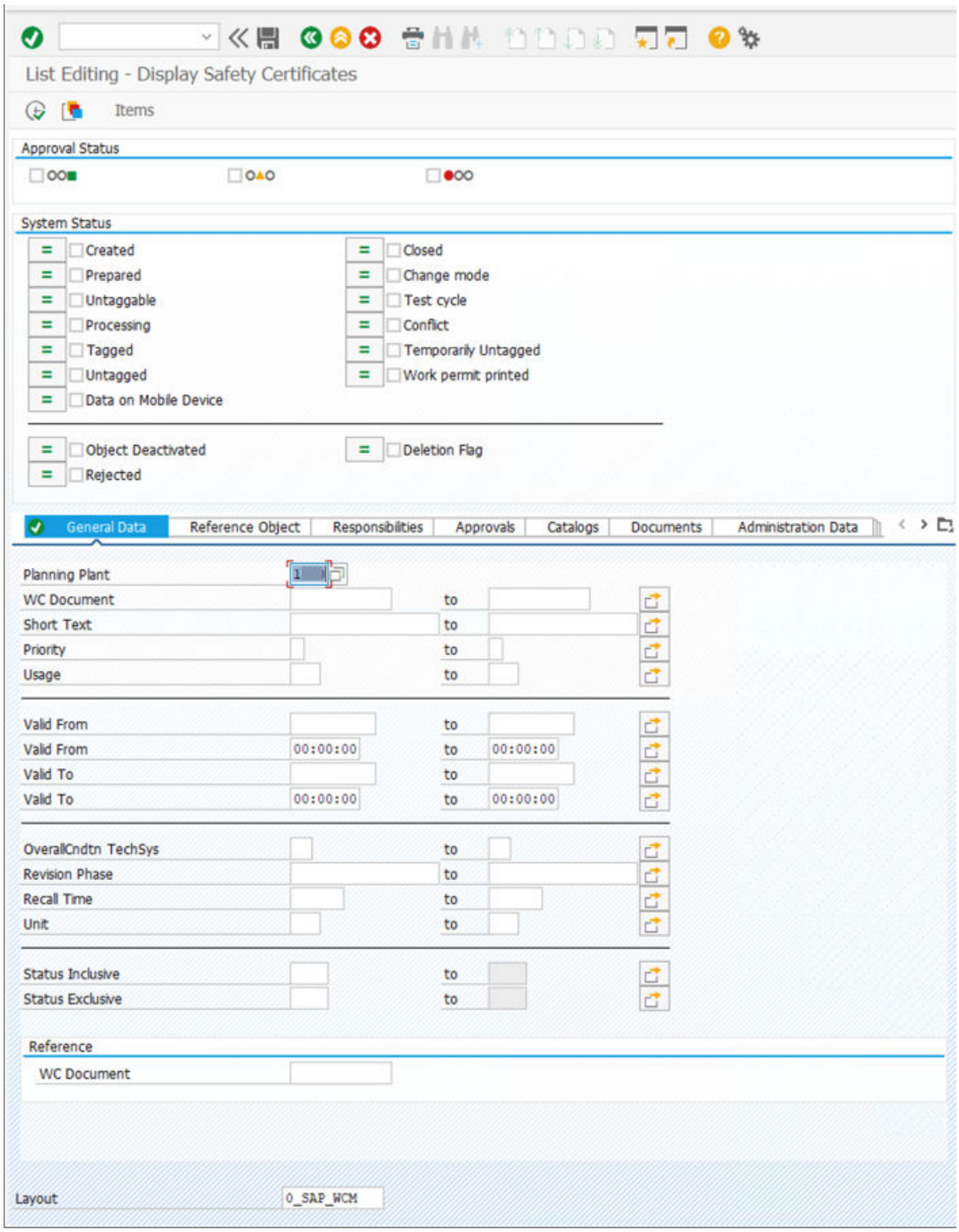
To enable the *Assigned to me* filtering option for users by the *5 - Selection Variant* Assignment Type, perform the following steps:

> **Note**
>
> Regarding the order of steps, it does not matter if you perform the SAP GUI or Configuration Panel changes first.

Procedure

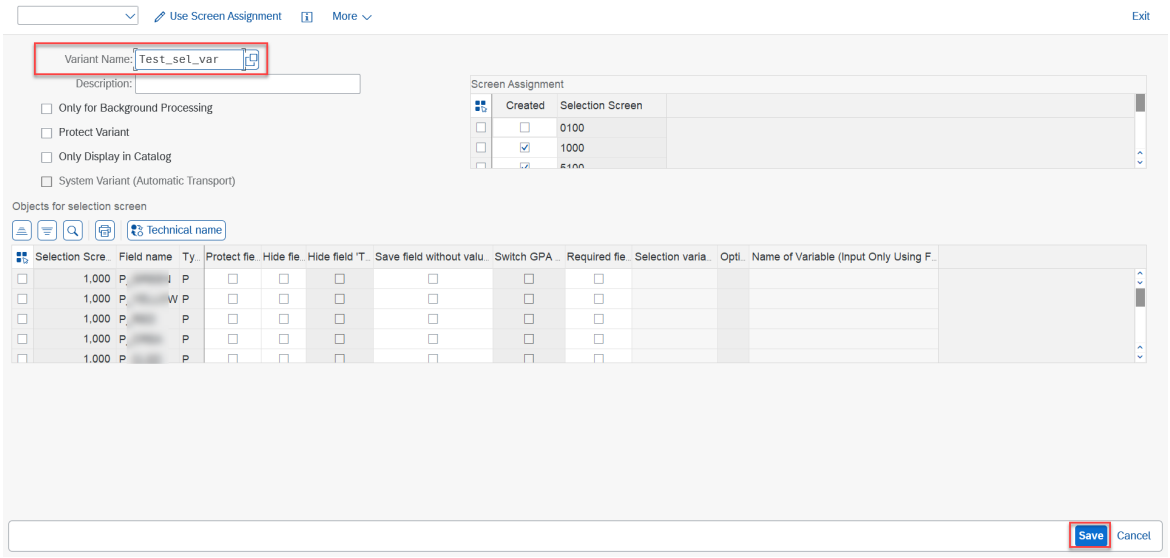
SAP GUI changes

1. To create the Selection Variant, use the `WCL4` transaction to open the *List Editing - Display Safety Cerificates* screen.

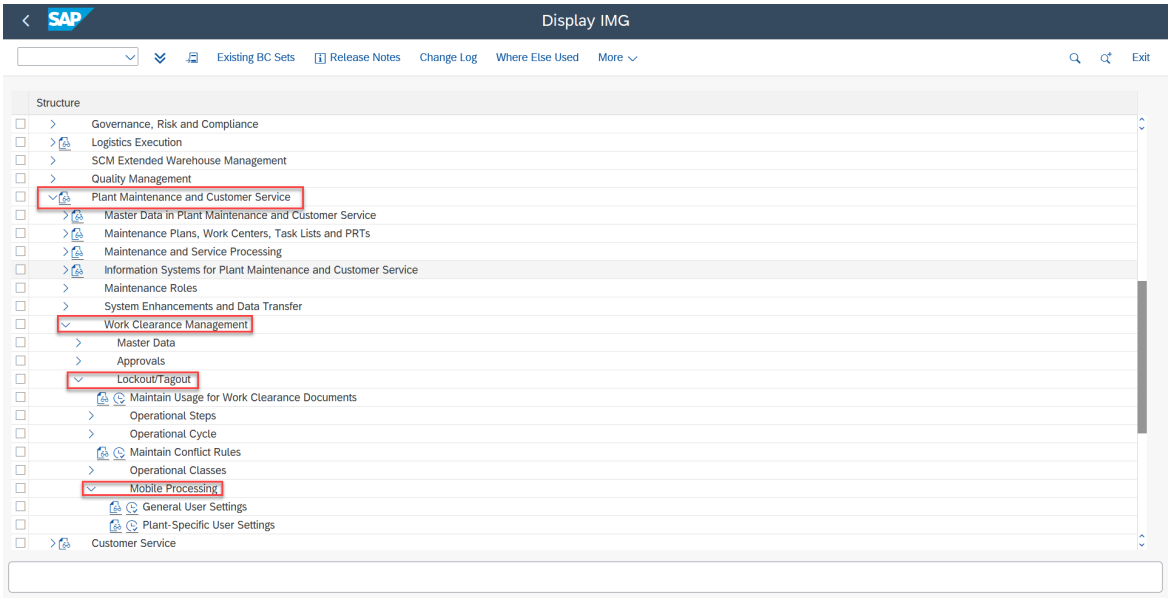


2. Select the filters you would like to use and click *Save*.

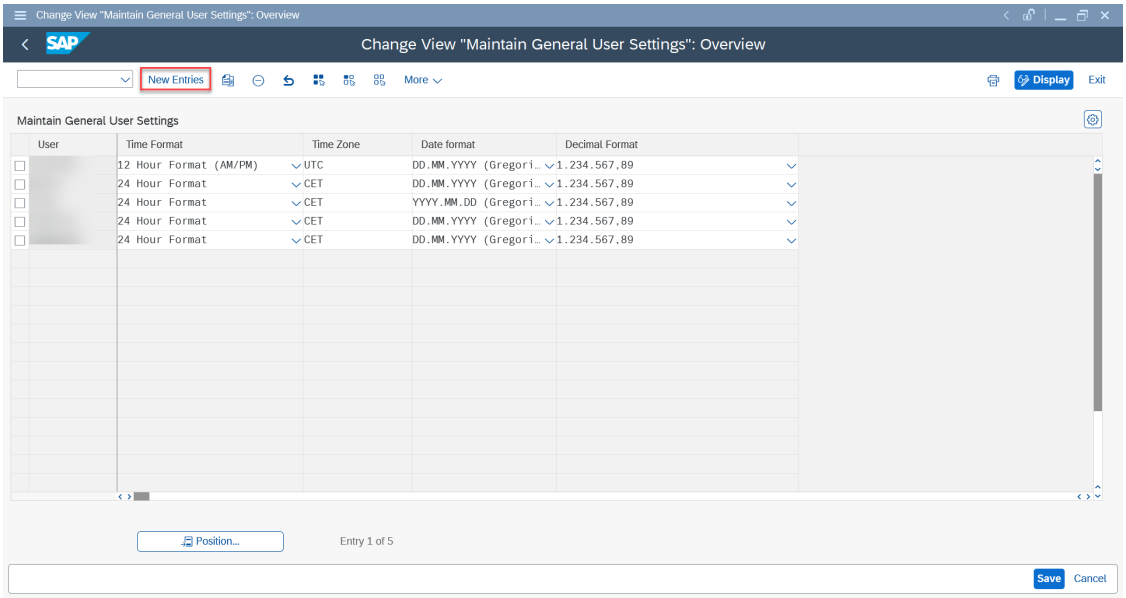
3. Enter a name for the Selection Variant and click *Save*.



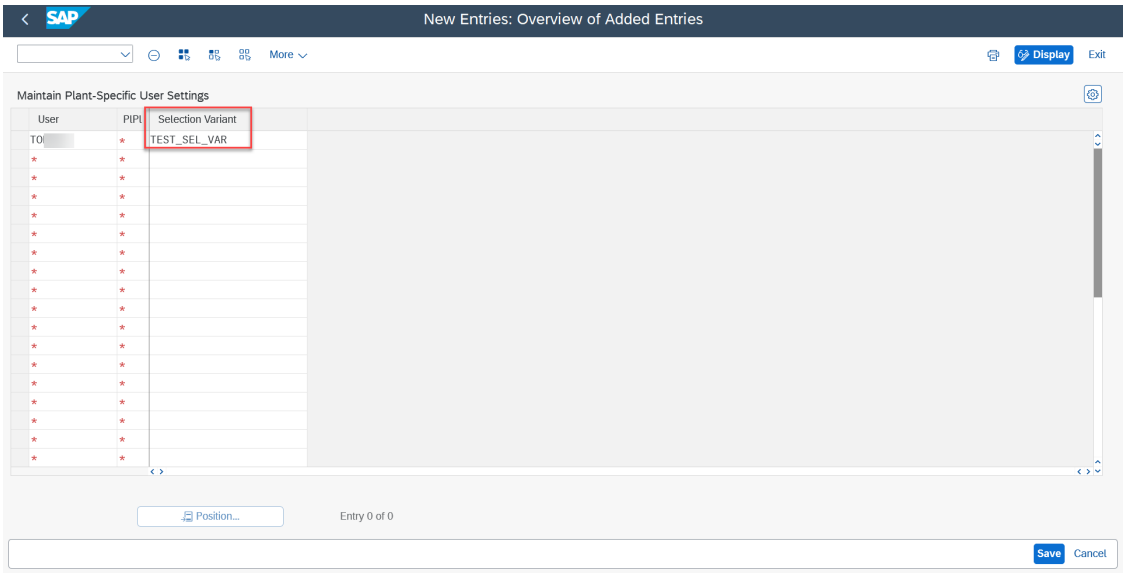
4. Go to the SPRO transaction and navigate to `Plant Maintenance and Customer Service` > `Work Clearance Management` > `Lockout/Tagout` > `Mobile Processing`.



1. Go to the `General User Settings` and add the user to the list.

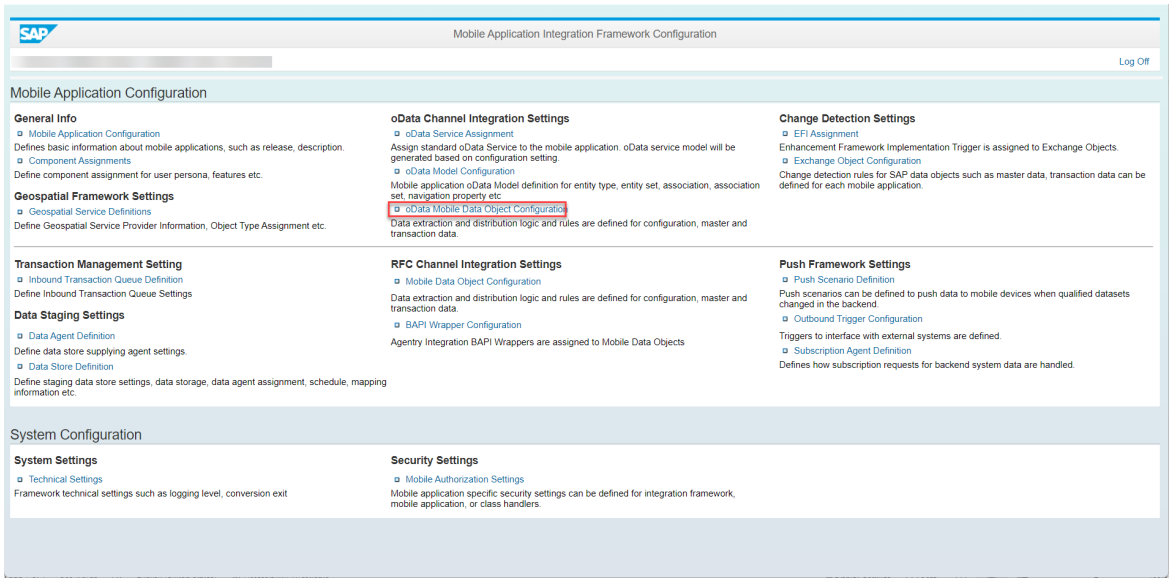


2. Go to the `Plant-Specific User Settings`, add the user to the list and assign the previously created Selection Variant to the user.

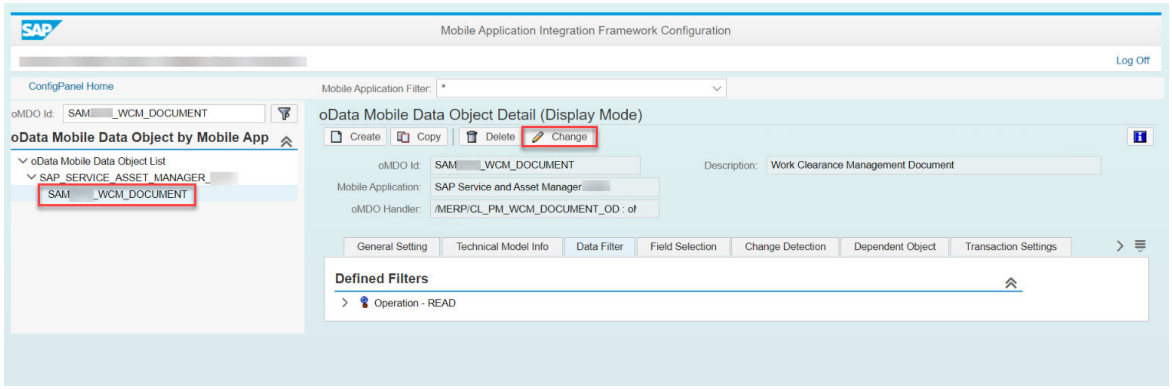


Configuration Panel - oMDO changes

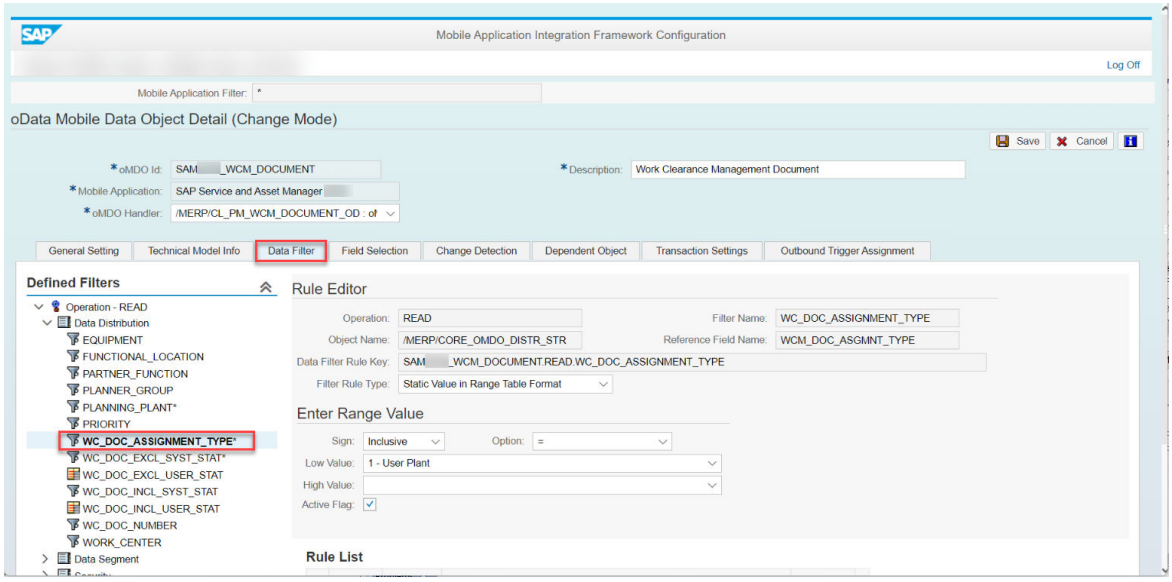
5. In the *SAP GUI*, navigate to the `/n/syclo/configpanel` transaction to open the configuration panel.
6. Under *oData Channel Integration Settings*, navigate to *oData Mobile Data Configuration.*



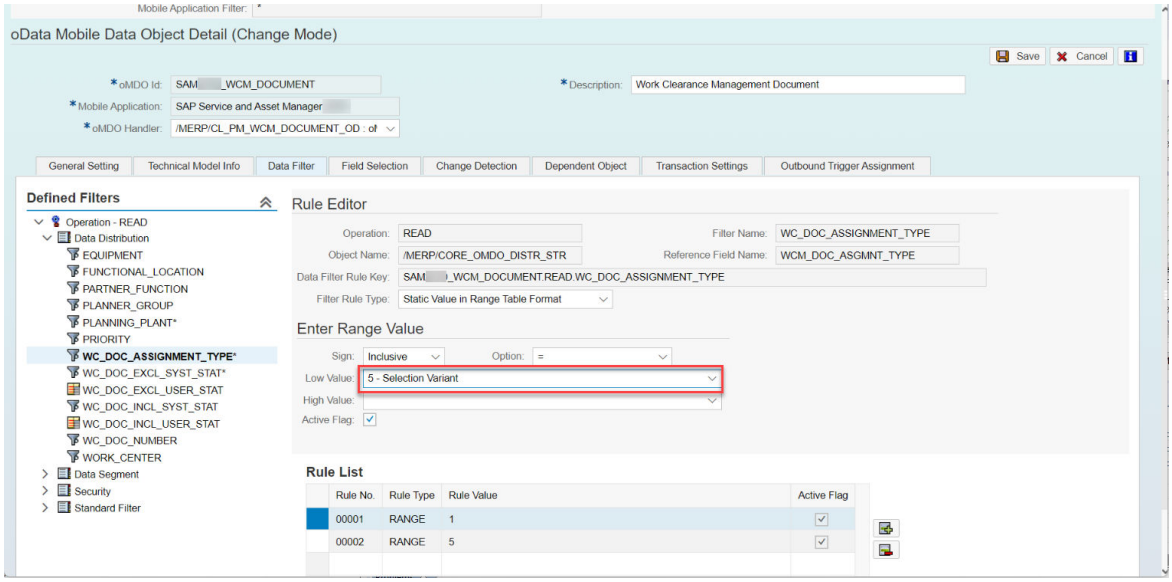
7. From the list of oMDOs, select *SAMXXXX_WCM_DOCUMENT* and click *Change*.



8. Under the *Data Filter* tab, select *WC_DOC_ASSIGNMENT_TYPE* from the list of filters.



9. From the Low Value drop-down list, choose *5 - Selection Variant* as assignment type.



> **Note**
>
> Consider the following in the *Rule List* table, *Rule Value* column:
>
> - If there is only one row with assignment type *5*, then only the objects assigned to the user will be downloaded to the client (*Assigned to me* button will not be displayed).
> - If there are two rows with assignment types *1* and *5* (see the screenshot above), then all the objects will be donwloaded to the client and the user can filter them with the *Assigned to me* button.

10. Click *Save* to exit Change Mode.

4.3.6 Configuring Assignment Type 6 (Operational List + Selection Variant)

Context

> **Note**
>
> - This procedure is applicable to **safety-related** assignment configuration. For detailed information, see the overview topic, Assignment Management of Safety-Related Features [page 261].
> - *5 - Selection Variant* and *6 - Operational List (Operational list + Selection Variant)* are non-regular Assignment Types, dedicated to provide additional assignment functionalities. You can create selection variants, define filters for them, and assign the variant to users. Then the filters from the variant will be used during a sync. When only these assignment types are set up, regular oMDO filters are not taken into account during the sync.

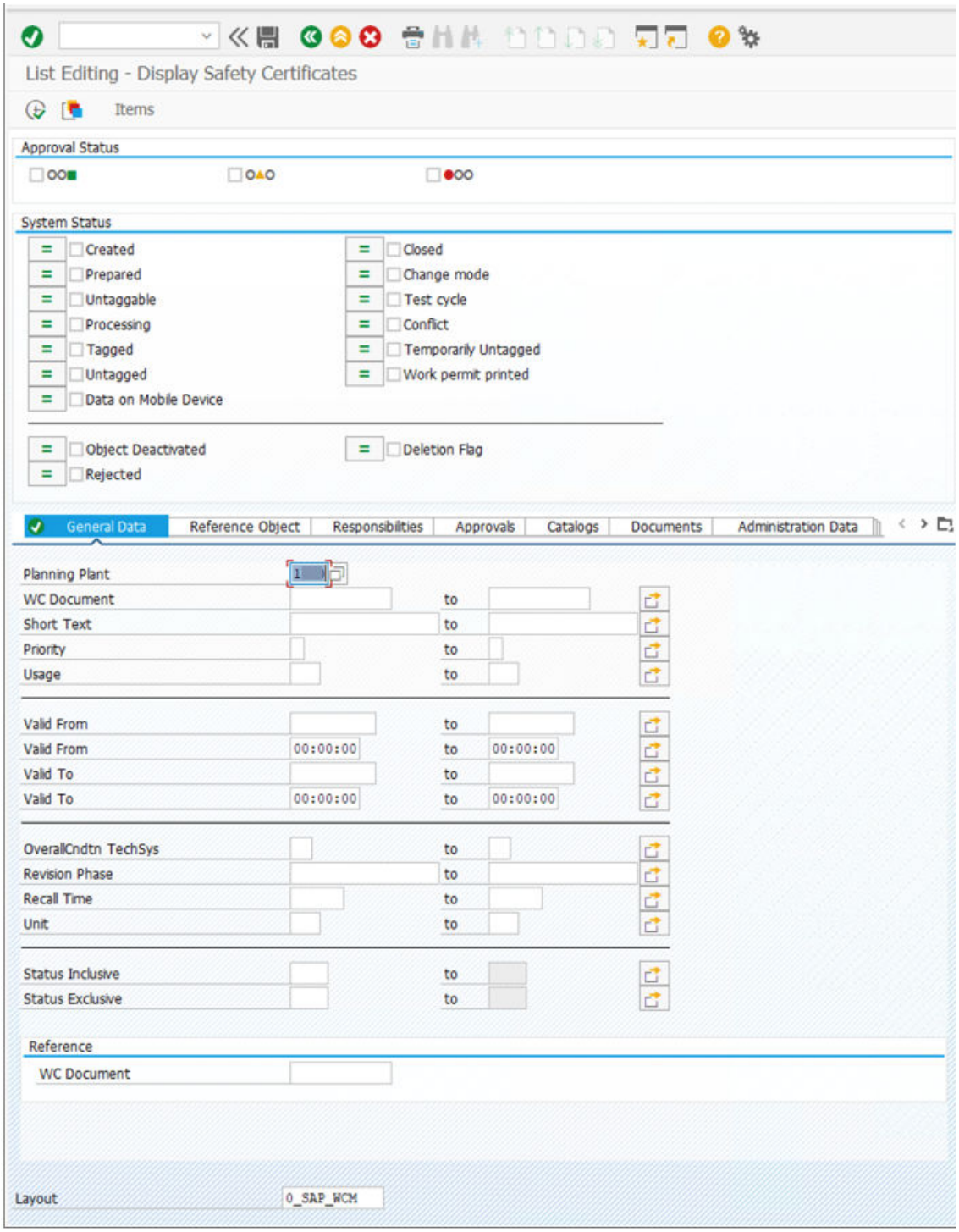
To enable the Assigned to me filtering option for users by the *6 - Operational List (Operational list + Selection Variant)* Assignment Type, perform the following steps:

> **Note**
>
> Regarding the order of steps, it does not matter if you perform the SAP GUI or Configuration Panel changes first.

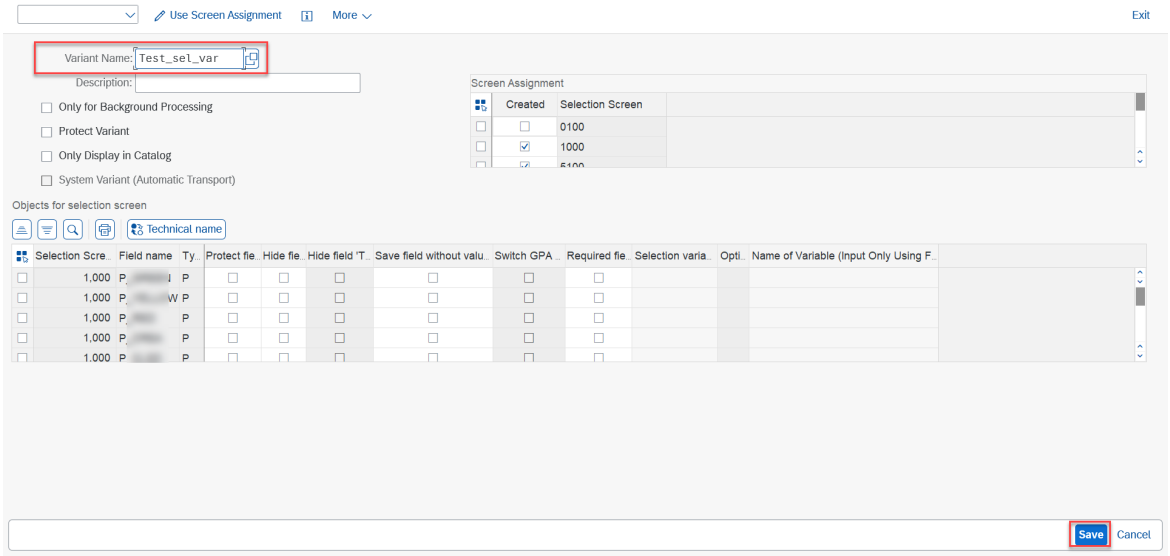
Procedure

SAP GUI changes

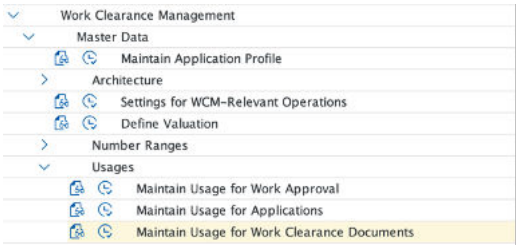
1. To create the Selection Variant, use the `WCL4` transaction to open the *List Editing - Display Safety Cerificates* screen.

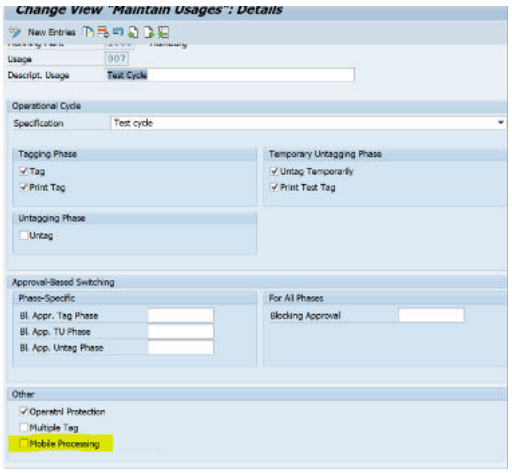


2. Select the filters you would like to use and click *Save*.
3. Enter a name for the Selection Variant and click *Save*.

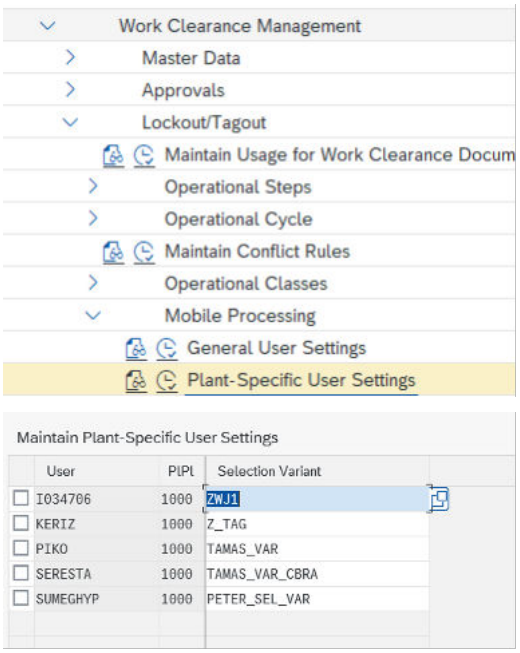


4. Enable Mobile Processing for the created Safety Certificate's Usage Type:
    - SPRO: Maintain Usage for Work Clearance Documents.

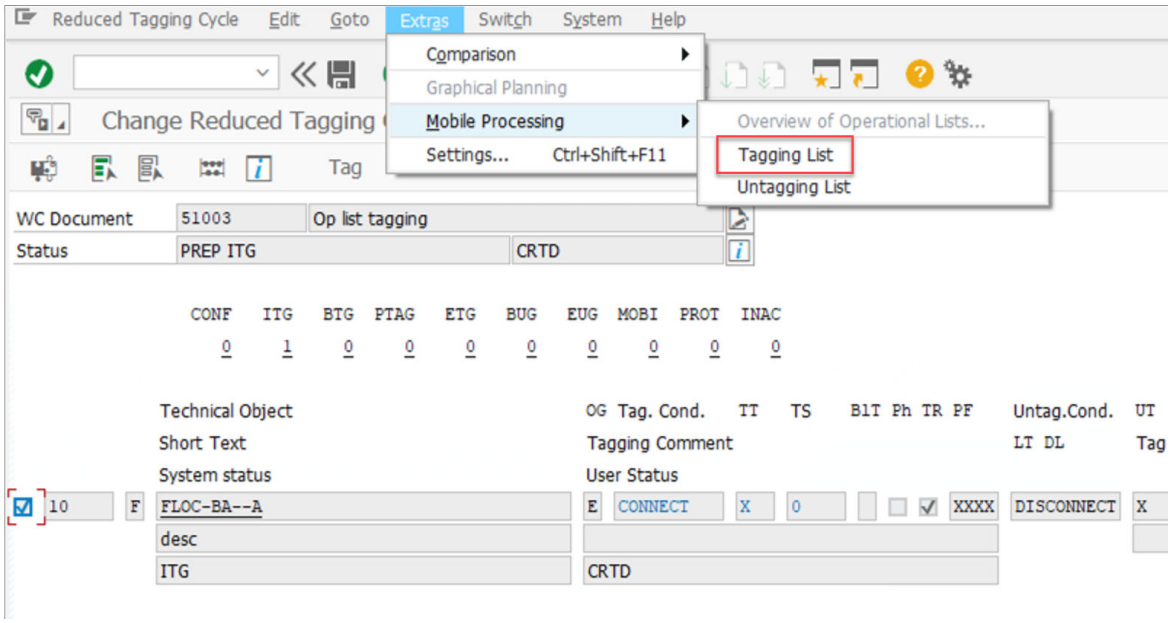




    - SPRO:
        - General User Settings: Add a test user
        - Plant Specific User Settings: Add the created variant.

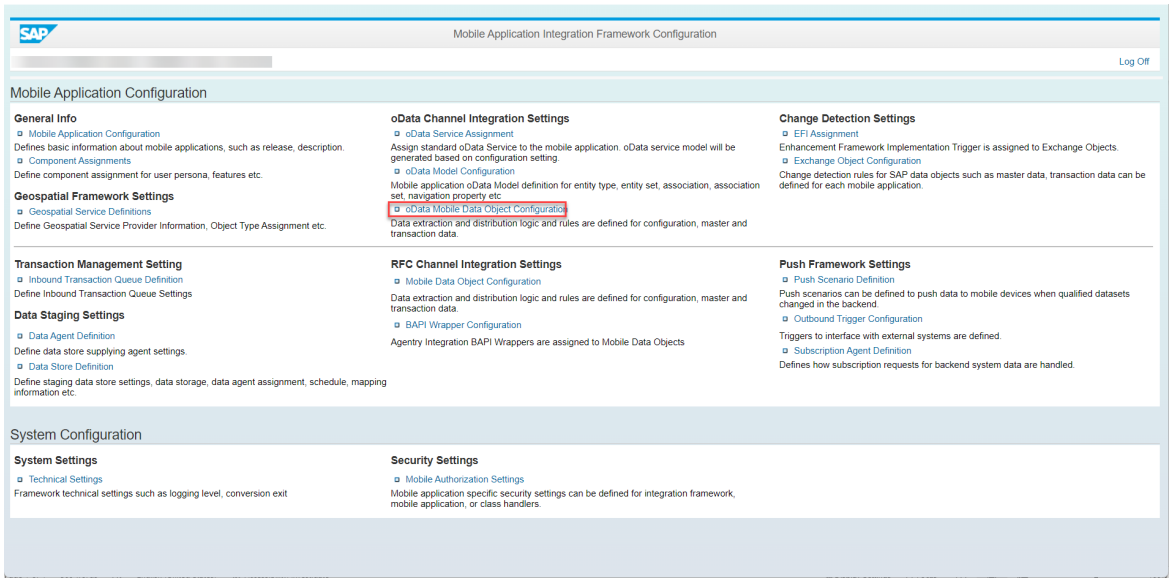


5. Add the Operational Item to the *Tagging List*.

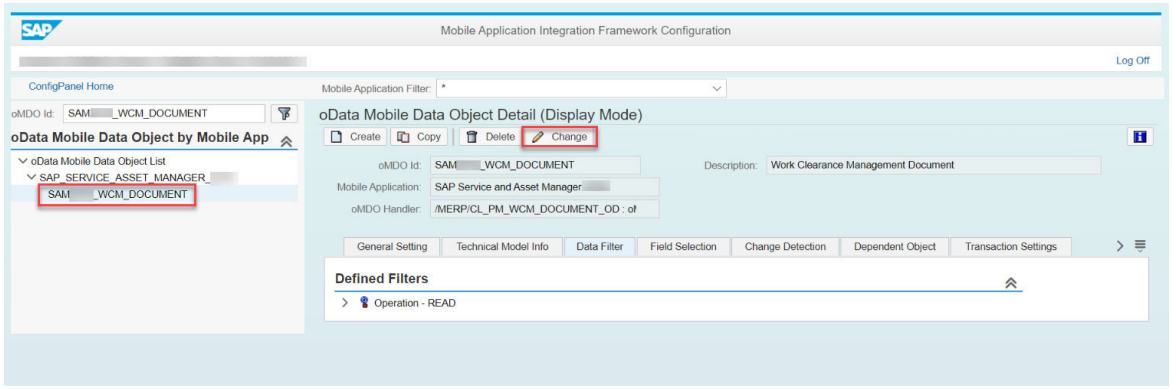


Configuration Panel - oMDO changes

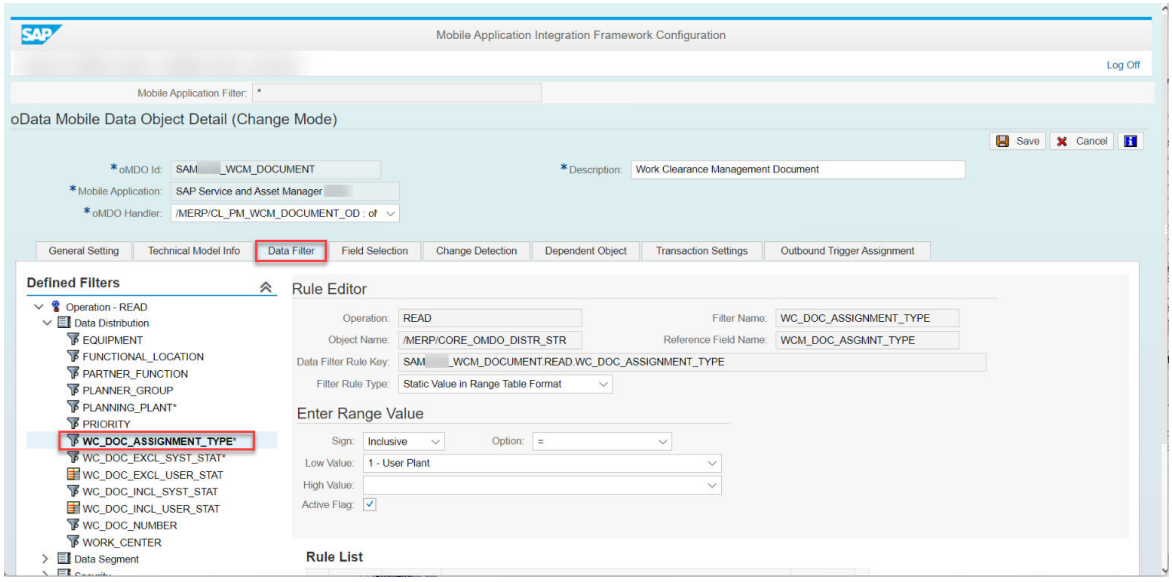
6. In the *SAP GUI*, navigate to the `/n/syclo/configpanel` transaction to open the configuration panel.
7. Under *oData Channel Integration Settings*, navigate to *oData Mobile Data Configuration.*



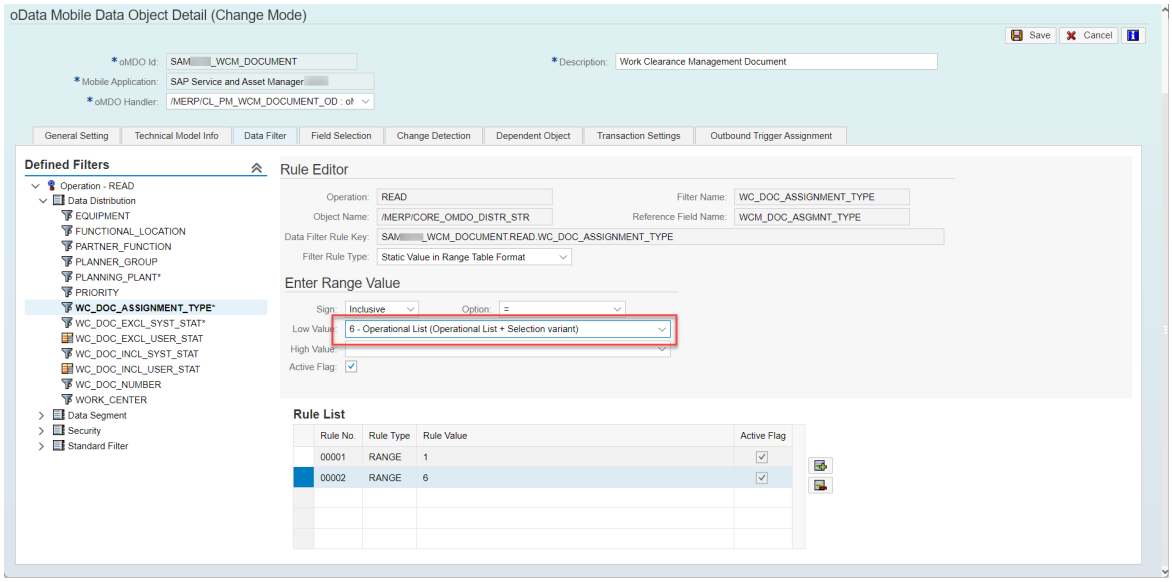
8. From the list of oMDOs, select *SAMXXXX_WCM_DOCUMENT* and click *Change*.



9. Under the *Data Filter* tab, select *WC_DOC_ASSIGNMENT_TYPE* from the list of filters.



10. From the Low Value drop-down list, choose *6 - Operational List (Operational list + Selection Variant)* as assignment type.



> **Note**
>
> Consider the following in the *Rule List* table, *Rule Value* column:
>
> - If there is only one row with assignment type *6*, then only the objects assigned to the user will be downloaded to the client (*Assigned to me* button will not be displayed).
> - If there are two rows with assignment types *1* and *6* (see the screenshot above), then all the objects will be donwloaded to the client and the user can filter them with the *Assigned to me* button.

11. Click *Save* to exit Change Mode.

4.4 Attachments - Abstract Document Management

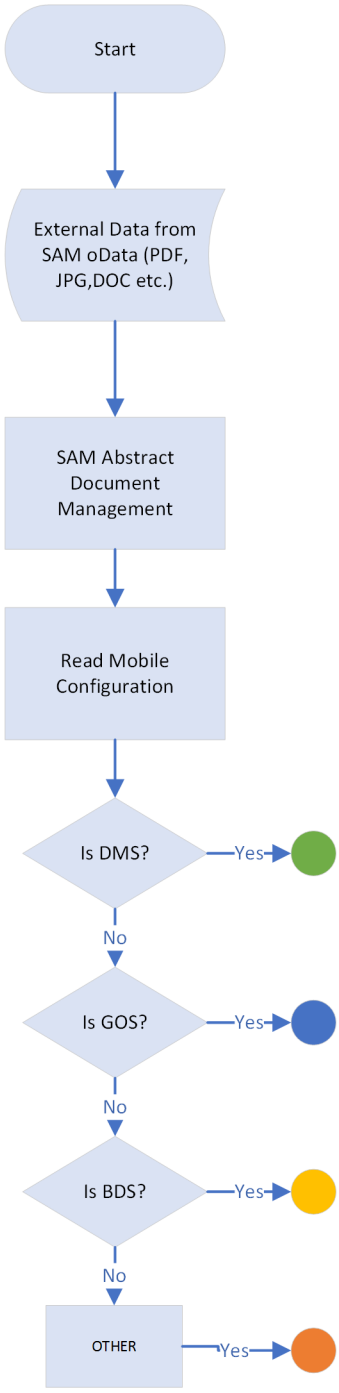
SAP Service and Asset Manager supports viewing of attachments, or documents, on the mobile device. You can also add an attachment to a local object.

Attachments include Microsoft Office documents, PDF files, and other commonly used business documents including videos, pictures, and audio files.

Abstract document management provides the option to create and read DMS, GOS, or BDS documents without configuration at the client application level.

Abstract Document Management Overview

Hover over the different types of abstract document in the flow chart to view the specific flow chart for the document type.



- DMS Method [page 291]
- DMS Method [page 291]
- BDS Method [page 293]
- Other Method [page 294]

4.4.1 Configuring Document Management

Abstract document management provides the option to create and read DMS, GOS, or BDS documents without configuration at the client application level.

Configuring Document Management in the ConfigPanel

Prerequisites

Address the following items before performing the procedure:

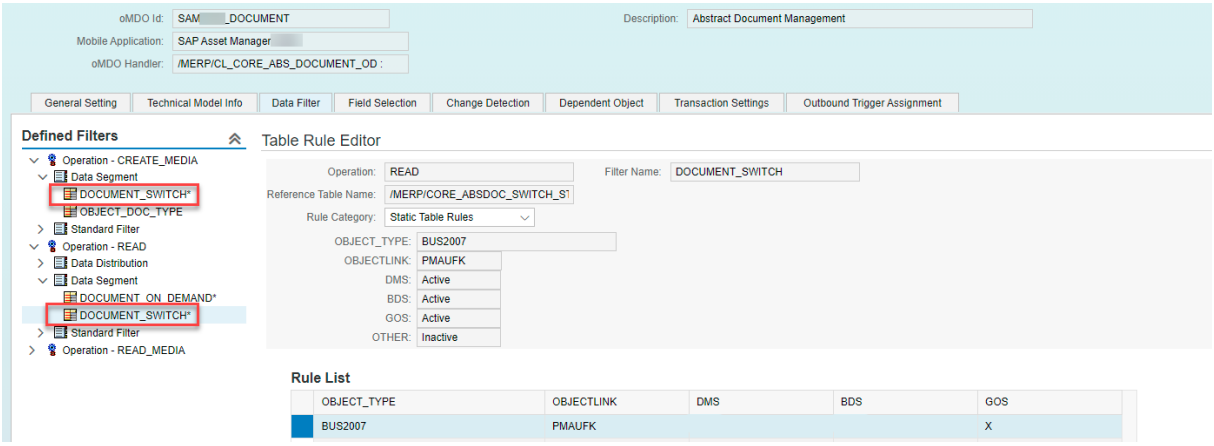
- Know the status or statuses that you're filtering on for equipment synchronization, as they're used in the procedure
- Ability to access to the ConfigPanel and permissions to change configuration settings

With a standard activation of a DMS or GOS document management solution, each document type has its own default content repository. Any application consuming document solutions like DMS or GOS follow the back-end configuration settings.

Select **SAMXXXX_DOCUMENT** from the *oData Mobile Data Object List* and navigate to the following locations:

- *Operation - CREATE_MEDIA* > *Data Segment* > *DOCUMENT_SWITCH*
- *Operation - READ* > *Data Segment* > *DOCUMENT_SWITCH*

Ensure the repository you're using is set to *Active*:



When you require SAP Service and Asset Manager to create content in a custom repository that is different than your back-end configuration, use the *OTHER* option. Implement the BADI *IF_CORE_OMDO_ABSDOC_BADI* > *CREATE_OTHER_DOCUMENT*. Your implementation must match with the ABS data model to work with standard SAP Service and Asset Manager metadata. See the Other Method [page 294] flow chart for more information.

Configuration Variations

Configuring the Document Solution to Work with a Third-Party Repository or Content Server

Beginning with the SAP Service and Asset Manager 2010 release, SAP Service and Asset Manager supports working with third-party repositories like Open Text or HTTP. Using third-party repositories leverages the back-end configuration for GOS, BDS, or DMS for work orders, notifications, equipment, and functional locations. See 2945017 to configure older application releases to work with third part repositories.

When using DMS, create custom storage category *ZEXT* to link to a third-party repository, such as an Open Text content server. See 2945017 for more information. Through this additional configuration, attachments uploaded from the application are stored in the third-party content server rather than the default content server.

See the following release notes for addition information on configuring abstract documents:

- 2457912: How to Create a Content Repository in OAC0
- 782614: Using an External Content Server in the BDS
- 530792: Storing Documents in Generic Object Services
- 2571570: Where are Documents Physically Stored with Business Communication Services
- 2945017: SAP Asset Manager ABS Enhancement

> ⓘ Note
>
> It isn't possible to integrate ABS documents with third-party repositories. Use this SAP note to deliver additional parameters such as storage category at an object level.

Document Management Configuration Examples

See the following examples of back-end configuration with a third-party content server:

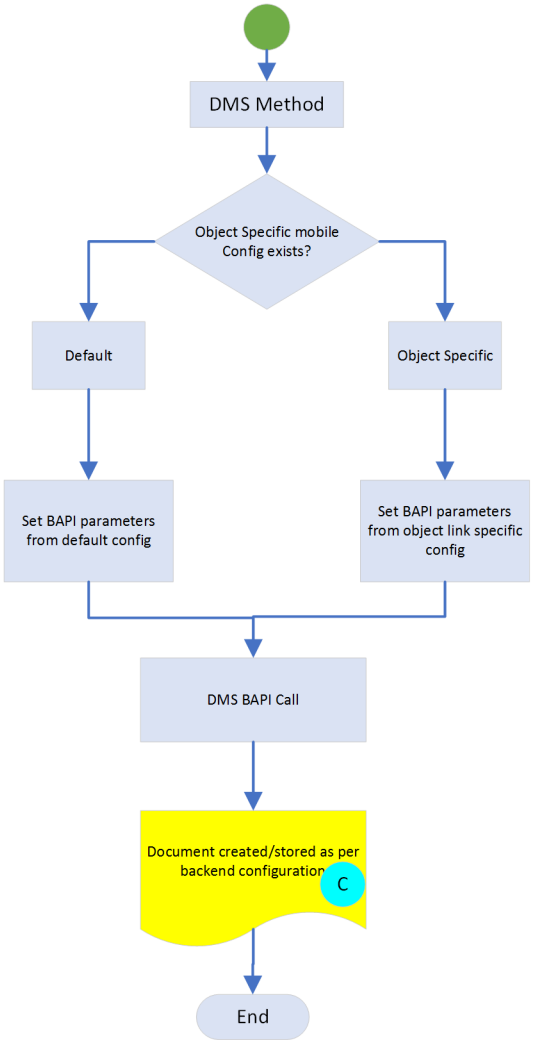
Example 1

Configure third-party repositories like Open Text to work with one of the available document solutions like BDS, DMS, or GOS using the ConfigPanel. Then apply SAP Note 2945017 and configure the desired document solution for work orders, equipment, and functional location objects.

Example 2

Integrate a third-party repository in more than one way with your back-end SAP system. If your implementation doesn't fit with DMS, BDS, or GOS, use the OTHER option in the ConfigPanel. Implement BADI */MERP/CORE_OMDO_ABSDOC_BADI* to align with the implementation.

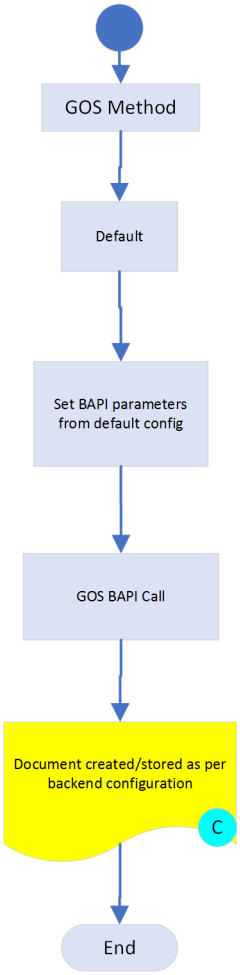
4.4.2 DMS Method



Mandatory - SAP backend configuration in working state

C **Optional – Customer specific customisation in backend for DMS, GOS or BDS to store documents in an external repository.**

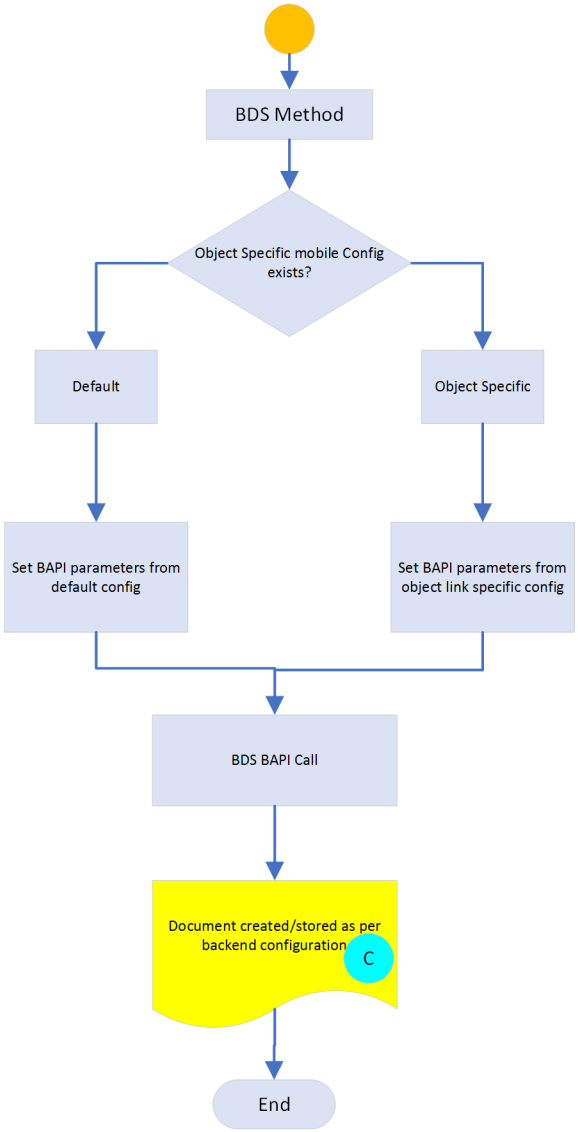
4.4.3 GOS Method



Mandatory - SAP backend configuration in working state

C **Optional – Customer specific customisation in backend for DMS, GOS or BDS to store documents in an external repository.**

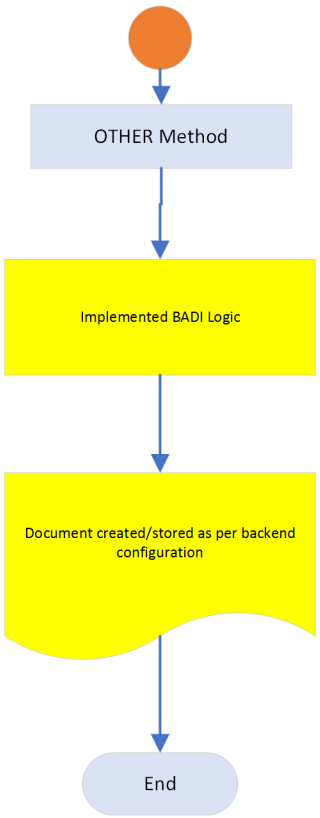
4.4.4 BDS Method



Mandatory - SAP backend configuration in working state

C **Optional – Customer specific customisation in backend for DMS, GOS or BDS to store documents in an external repository.**

4.4.5 Other Method



Mandatory - SAP backend configuration in working state

4.4.6 SAM Document Data Filter

When taking readings in the SAP Service and Asset Manager mobile app, you can attach documents related to S4 service orders, requests, confirmations, contracts, and related items. Activate S4 on the *SAMXXXX_DOCUMENT* data filter to attach documents to S4 objects.

> **Note**
>
> You only need the ENCODE_ASCII filter for the CREATE_MEDIA and UPDATE_MEDIA operations of the SAMXXXX_DOCUMENT oMDO if the SAP Gateway doesn't support unescaping URL encoding of request headers. If the Gateway does support it, deactivate the filter.

1. Select *SAMXXXX_DOCUMENT* in the *oData Mobile Data Object List* and navigate to the following:
   - *Operation* > *CREATE_MEDIA Data Segment DOCUMENT_SWITCH*

- *Operation* > *READ Data Segment DOCUMENT_SWITCH*

2. In the Rule List, activate the following objects:
   - BUS2000116: Service Order
   - BUS2000117: Service Confirmation
   - BUS2000223: Service Request
   - BUS2000112: Service Contract
   - BUS2000140: Service Product Item
   - BUS2000146: Service Mat. Item
   - BUS2000159: Service Expense Item
   - BUS2000142: ServMatConfirmItem
   - BUS2000143: ServProdConfirmItem
   - BUS2000158: SrvcExpenseConfItem
   - BUS2000137: Service Contr. Item

   > **Note**
   >
   > Ensure that both *BDS* and *GOS* are set to *Active*.

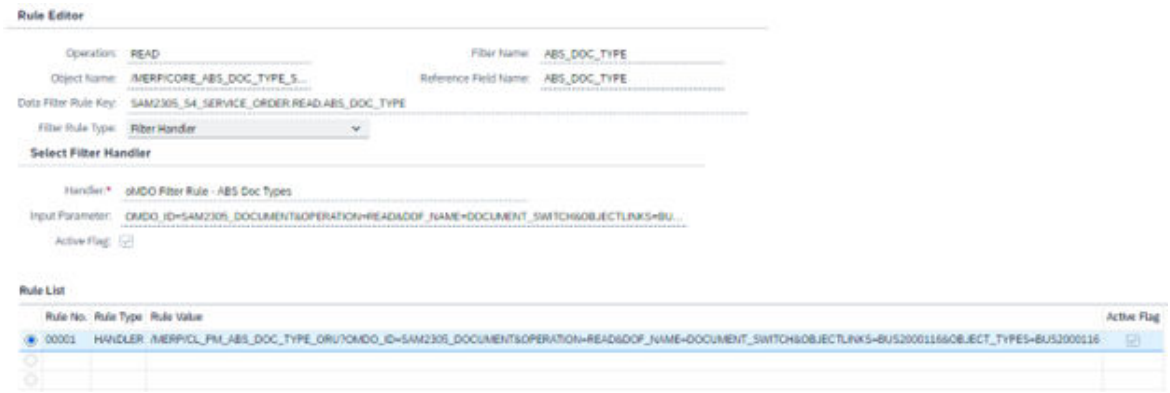
3. Navigate to *Operation* > *READ Standard Filter DOC_CLASSNAME*
4. Add a new line to the *Rule List* for each low value and enter the following range value:
   - *Sign*: Inclusive
   - *Option*: =
   - *Low Value*: BUS2000116
5. Activate the following objects:
   - BUS2000117
   - BUS2000223
   - BUS2000112
   - BUS2000140
   - BUS2000146
   - BUS2000159
   - BUS2000142
   - BUS2000143
   - BUS2000158
   - BUS2000137

4.4.6.1 S4 Service Order

Context

Procedure

1. Select *SAM2305_S4_SERVICE_ORDER* in the *oData Mobile Data Object* list and navigate to the *Data Filter* tab.
2. In the *Defined Filters* list, navigate to *Operation* > *READ Standard Filter ABS_DOC_TYPE*.
3. Set the filter handler *OMDO_ID=SAM2305_DOCUMENT&OPERATION=READ&DOF_NAME=DOCUMENT_SWITCH&OBJECTLINKS=BUS2000116&OBJECT_TYPES=BUS2000116* to *Active*.



4. Enable dependency between the S4 service order and the related document on the mobile device.
5. Navigate to the *Dependent Object* tab. Find the *S4SERVDOCUMENT* object in the *<Source Tech. Entity Type>* column. Scroll the page to find the *SAM2305_DOCUMENT* object. Ensure it is marked as *Active*.
6. Insert the two lines in the *Dependent Object Keys* tab:
    1. *Source oMDO Field Name:* OBJECT_KEY
       Dependent Object Key Fieldname: OBJECT_KEY
    2. *Source oMDO Field Name:* OBJTYPE_H
       Dependent Object Key Fieldname: OBJECTLINK
7. Insert the two lines in the *Origin Object Keys* tab:
    1. *Field name:* OBJECT_KEY
    2. *Field name:* DOC_OBJ_ID
8. Enable dependency between the S4 service order item and the related document on the mobile device.
9. Navigate to the *Dependent Object* tab. Find *S4SERVITEM* object in the *<Source Tech. Entity Type>* column. Scroll the page to find the *SAM2305_DOCUMENT* object. Ensure it is marked as *Active*.
10. Insert the two lines in the *Dependent Object Keys* tab:
    1. *Source oMDO Field Name:* ITEM_GUID_CHAR
       Dependent Object Key Fieldname: OBJECT_KEY
    2. *Source oMDO Field Name:* OBJTYPE_I
       Dependent Object Key Fieldname: OBJECTLINK
11. Insert the three lines in the *Origin Object Keys* tab:
    1. *Field name:* OBJTYPE_H
    2. *Field name:* OBJECT_ID
    3. *Field name:* NUMBER_INT

4.4.6.2 S4 Service Quotation

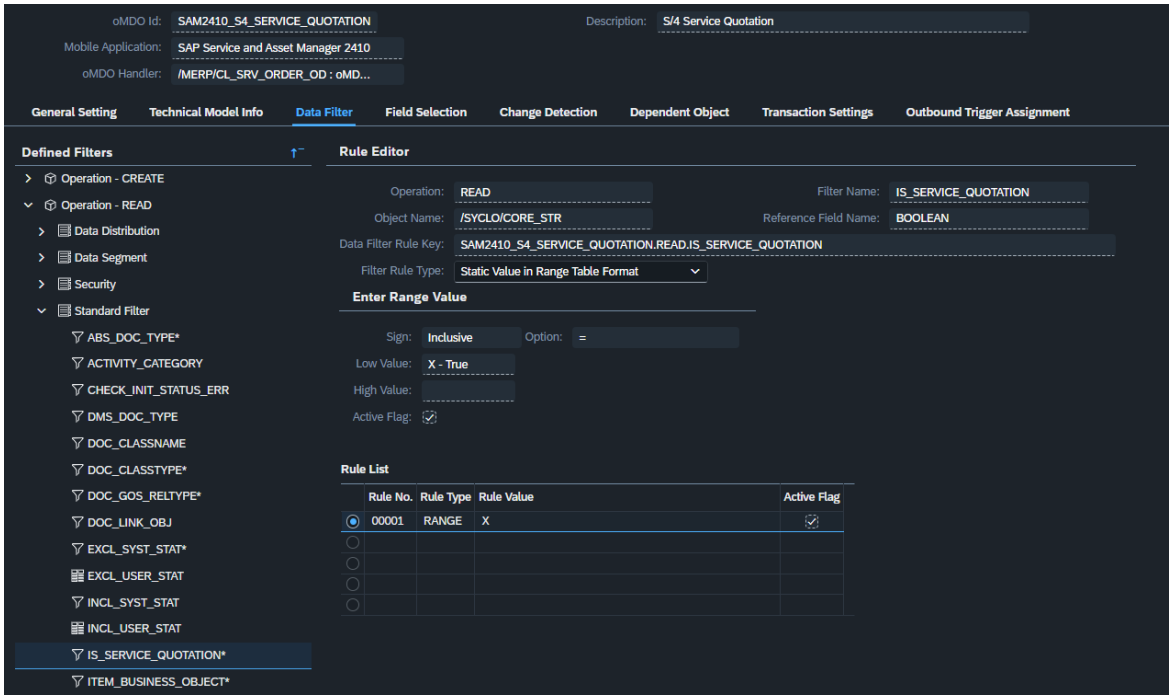
Context

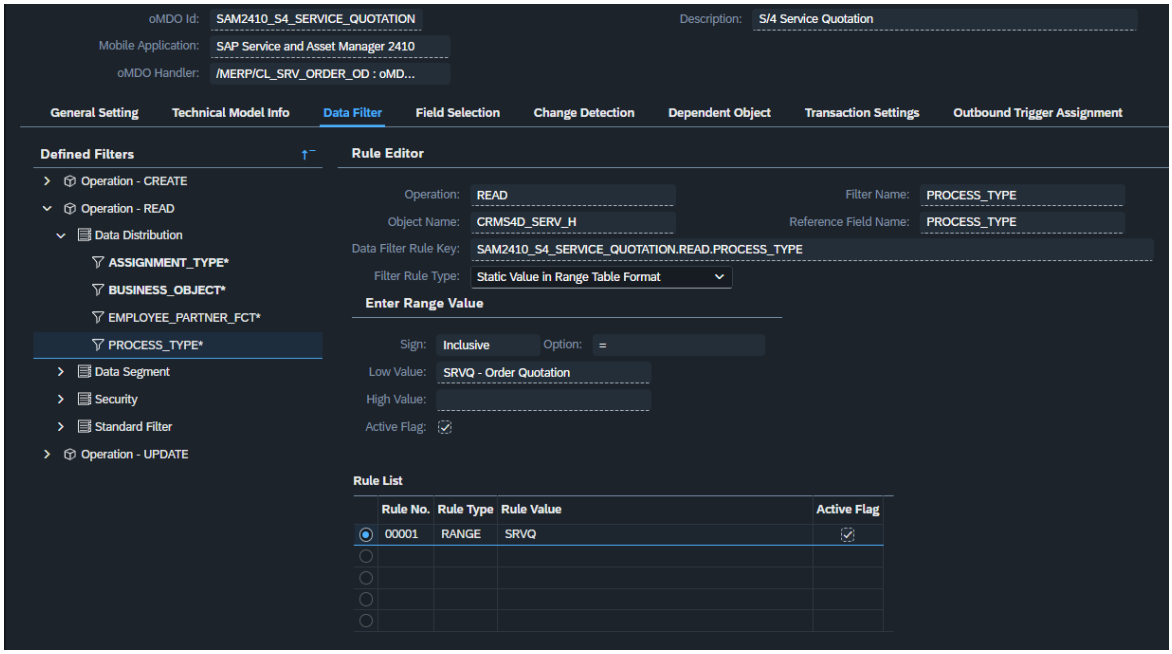
The *Service Quotation* feature has basically the same data filters as the *Service Order* feature. For more information on how to configure this feature, see the S4 Service Order [page 295] topic and the Confoguration Support for Service Quotation in SAP Service and Asset Manager 2410 note. For the back end suport for the configuration update, refer to the Support S4 Service Quotation note.

> **Note**
>
> The IS_SERVICE_QUOTATION data filter must always be true for S4_SERVICE_QUOTATION, but must not be true for S4_SERVICE_ORDER.

Procedure

1. Select SAM2410_S4_SERVICE_QUOTATION in the oData Mobile Data Object list and navigate to the Data Filter tab.
2. In the Defined Filters list, set the IS_SERVICE_QUOTATION filter handler to active.



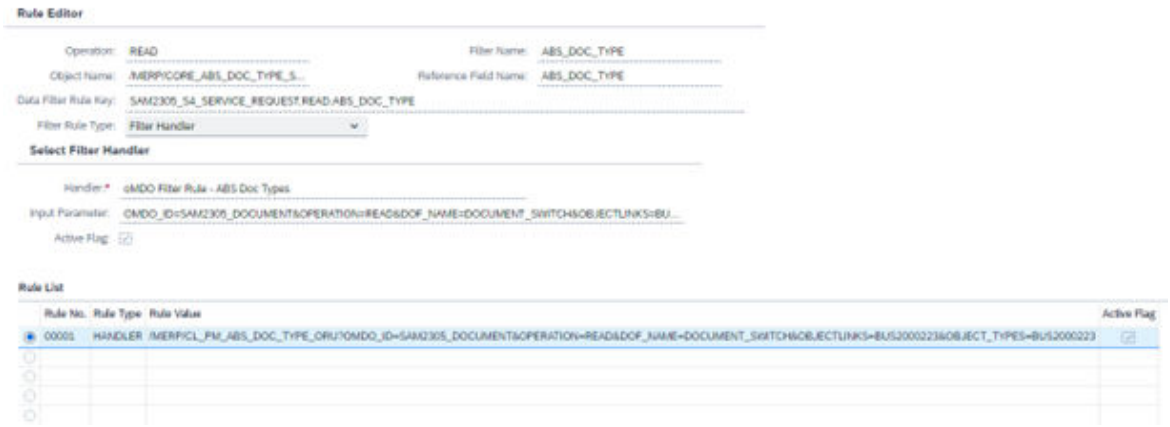


4.4.6.3 S4 Service Request

Context

Procedure

1. Select *SAM2305_S4_SERVICE_REQUEST* in the *oData Mobile Data Object* list and navigate to the *Data Filter* tab.
2. In the *Defined Filters* list, navigate to *Operation* > *READ Standard Filter ABS_DOC_TYPE*.
3. Set the filter handler *OMDO_ID=SAM2305_DOCUMENT&OPERATION=READ&DOF_NAME=DOCUMENT_SWITCH&OBJECTLINKS=BUS2000223&OBJECT_TYPES=BUS2000223* to *Active*.



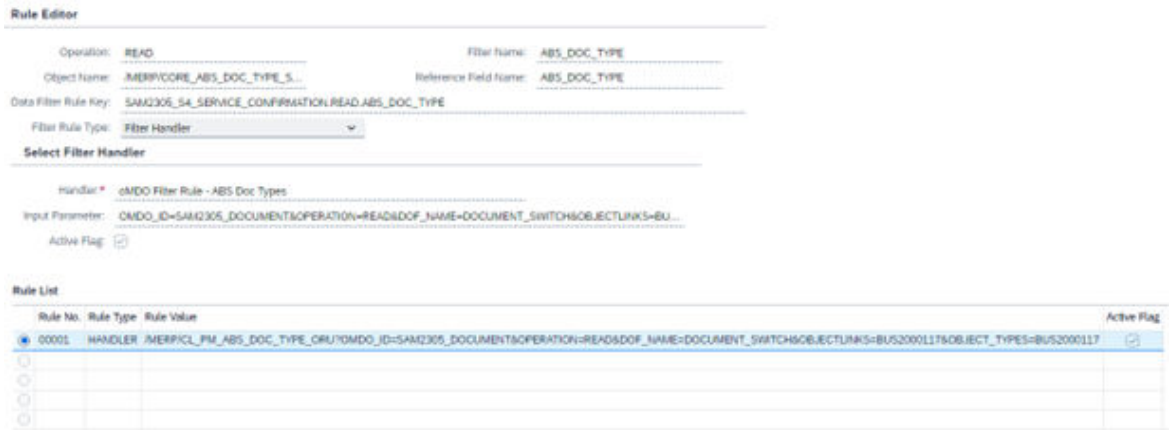
4. Enable dependency between the S4 service request and the related document on the mobile device.
5. Navigate to the *Dependent Object* tab. Find the *S4SERVDOCUMENT* object in the *<Source Tech. Entity Type>* column. Scroll the page to find the *SAM2305_DOCUMENT* object. Ensure it is marked as *Active*.
6. Insert the two lines in the *Dependent Object Keys* tab:
    1. *Source oMDO Field Name:* OBJECT_KEY
    Dependent Object Key Fieldname: OBJECT_KEY
    2. *Source oMDO Field Name:* OBJTYPE_H
    Dependent Object Key Fieldname: OBJECTLINK
7. Insert the two lines in the *Origin Object Keys* tab:
    1. *Field name:* OBJECT_KEY
    2. *Field name:* DOC_OBJ_ID

4.4.6.4 S4 Service Confirmation

Context

Procedure

1. Select *SAM2305_S4_SERVICE_CONFIRMATION* in the *oData Mobile Data Object* list and navigate to the *Data Filter* tab.
2. In the *Defined Filters* list, navigate to *Operation* > *READ Standard Filter ABS_DOC_TYPE*.
3. Set the filter handler *OMDO_ID=SAM2305_DOCUMENT&OPERATION=READ&DOF_NAME=DOCUMENT_SWITCH&OBJECTLINKS=BUS2000117&OBJECT_TYPES=BUS2000117* to *Active*.



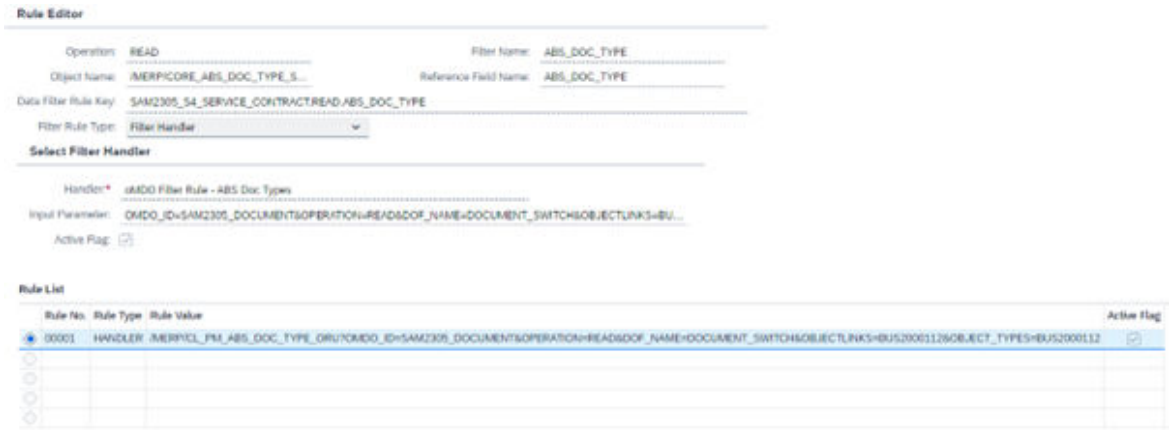
4. Enable dependency between the S4 service confirmation and the related document on the mobile device.
5. Navigate to the *Dependent Object* tab. Find the *S4SERVDOCUMENT* object in the *<Source Tech. Entity Type>* column. Scroll the page to find the *SAM2305_DOCUMENT* object. Ensure it is marked as *Active*.
6. Insert the two lines in the *Dependent Object Keys* tab:
    1. *Source oMDO Field Name:* OBJECT_KEY
       Dependent Object Key Fieldname: OBJECT_KEY
    2. *Source oMDO Field Name:* OBJTYPE_H
       Dependent Object Key Fieldname: OBJECTLINK
7. Insert the two lines in the *Origin Object Keys* tab:
    1. *Field name:* OBJECT_KEY
    2. *Field name:* DOC_OBJ_ID
8. Enable dependency between the S4 service confirmation item and the related document on the mobile device.
9. Navigate to the *Dependent Object* tab. Find *S4SERVITEM* object in the *<Source Tech. Entity Type>* column. Scroll the page to find the *SAM2305_DOCUMENT* object. Ensure it is marked as *Active*.
10. Insert the two lines in the *Dependent Object Keys* tab:
    1. *Source oMDO Field Name:* ITEM_GUID_CHAR
       Dependent Object Key Fieldname: OBJECT_KEY
    2. *Source oMDO Field Name:* OBJTYPE_I
       Dependent Object Key Fieldname: OBJECTLINK
11. Insert the three lines in the *Origin Object Keys* tab:
    1. *Field name:* OBJTYPE_H
    2. *Field name:* OBJECT_ID
    3. *Field name:* NUMBER_INT

4.4.6.5 S4 Service Contract

Context

Procedure

1. Select *SAM2305_S4_SERVICE_CONTRACT* in the *oData Mobile Data Object* list and navigate to the *Data Filter* tab.
2. In the *Defined Filters* list, navigate to *Operation* > *READ Standard Filter ABS_DOC_TYPE*.
3. Set the filter handler *OMDO_ID=SAM2305_DOCUMENT&OPERATION=READ&DOF_NAME=DOCUMENT_SWITCH&OBJECTLINKS=BUS2000112&OBJECT_TYPES=BUS2000112* to *Active*.



4. Enable dependency between the S4 service contract and the related document on the mobile device.
5. Navigate to the *Dependent Object* tab. Find the *S4SERVDOCUMENT* object in the *<Source Tech. Entity Type>* column. Scroll the page to find the *SAM2305_DOCUMENT* object. Ensure it is marked as *Active*.
6. Insert the two lines in the *Dependent Object Keys* tab:
    1. *Source oMDO Field Name:* OBJECT_KEY
       Dependent Object Key Fieldname: OBJECT_KEY
    2. *Source oMDO Field Name:* OBJTYPE_H
       Dependent Object Key Fieldname: OBJECTLINK
7. Insert the two lines in the *Origin Object Keys* tab:
    1. *Field name:* OBJECT_KEY
    2. *Field name:* DOC_OBJ_ID
8. Enable dependency between the S4 service contract item and the related document on the mobile device.
9. Navigate to the *Dependent Object* tab. Find *S4SERVITEM* object in the *<Source Tech. Entity Type>* column. Scroll the page to find the *SAM2305_DOCUMENT* object. Ensure it is marked as *Active*.

10. Insert the two lines in the *Dependent Object Keys* tab:
    1. *Source oMDO Field Name:* ITEM_GUID_CHAR
       Dependent Object Key Fieldname: OBJECT_KEY
    2. *Source oMDO Field Name:* OBJTYPE_I
       Dependent Object Key Fieldname: OBJECTLINK
11. Insert the three lines in the *Origin Object Keys* tab:
    1. *Field name:* OBJTYPE_H
    2. *Field name:* OBJECT_ID
    3. *Field name:* NUMBER_INT

4.5 Auto-Resize Images with a Configured Maximum Size

You can configure the maximum image size, which is allowed for uploading images from the application. Uploaded images exceeding the size limit will be resized automatically.

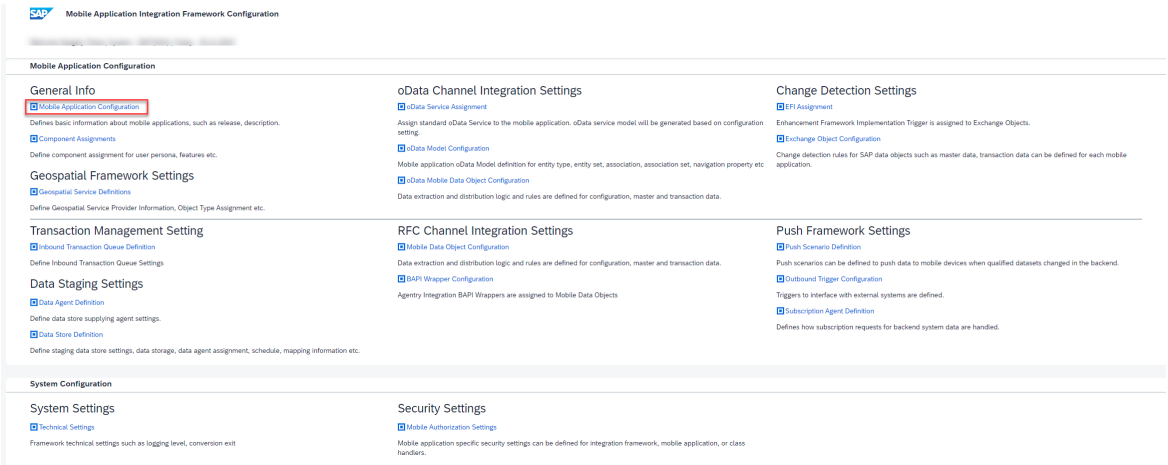
Context

> **Note**
>
> Decreased size of the images will be less, but not necessarily equal to the configured maximum size.

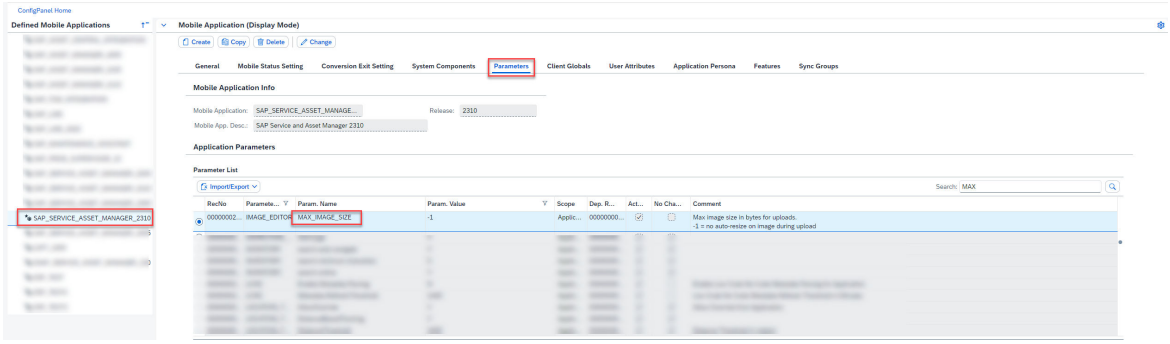
See configuration steps as follows:

Procedure

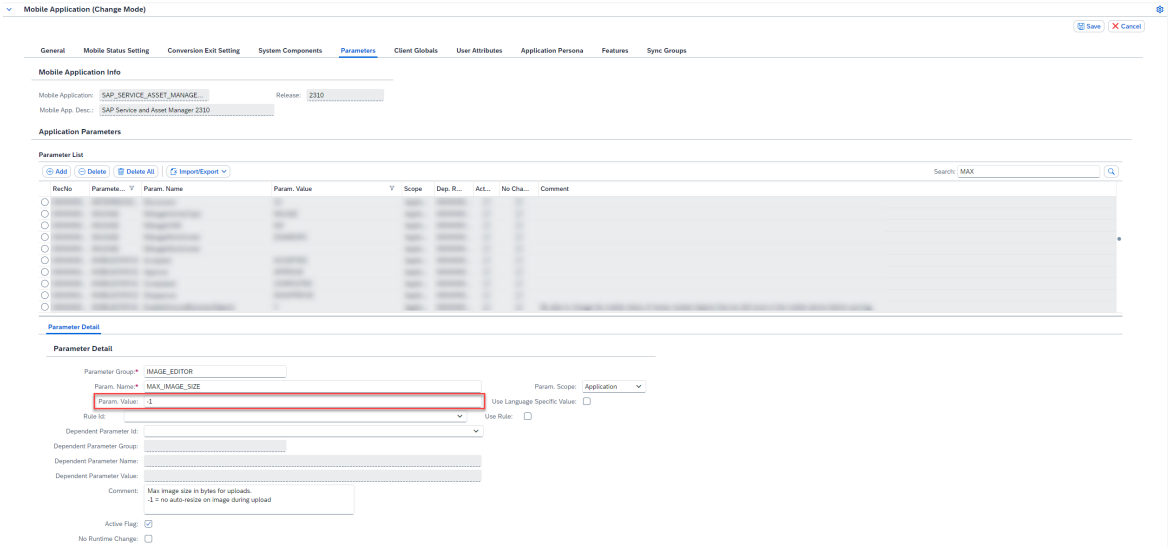
1. On the *Configuration Panel*, go to *Mobile Application Configuration*.



2. Select your mobile application, go to the *Parameters* tab and select the parameter *MAX_IMAGE_SIZE*.



3. Enter *Change mode* and in the *Parameter Details* section add your preferred maximum image size as the *Parameter Value*.



> **Note**
>
> - Add value number in **BYTES**.
> - The default value is **-1**, in this case the auto-resize feature is disabled.

4. Click *Save* to exit *Change mode*.

4.6 Auto-Sync Configuration

Back end administrators can configure the app to auto-sync. Auto-syncs occur automatically, with no input needed from the app user.

Auto-syncs can happen in the following ways, depending on the configuration:

- The app auto-syncs when network connectivity changes from offline to online. [page 306]
- The app auto-syncs when the status of an object (e.g. work order, operation, sub-operation, notification) has changed. [page 306]

- The app auto-syncs periodically when it is running in the foreground of the mobile device. [page 306]
- The app auto-syncs when the app is launched or is moved from the background to the foreground on the mobile device. [page 307]
- The app auto-syncs when a database save occurs in the app (e.g. applying and saving any changes to an object). [page 307]

> ⓘ Note
>
> - All these scenarios have a corresponding mobile application parameter. For more information about how these parameters relate and how to configure them, see Configuring Auto-Sync - Back End - Mobile Application Parameters [page 305].
>   - Currently, it is recommended to use only the *PERIODIC* parameter without combining it with other parameters.
> - For more information about using the Auto-Sync feature, see Automatic Syncing.

Supported Personas

This feature is applicable for the following personas:

Maintenance Technician (Standard)
Maintenance Technician (Pro)
Maintenance Technician (External)
Field Service Technician (Standard)
Field Service Technician (Pro)
Inventory Clerk
Extended Warehouse Clerk

Configuration

Perform the following configuration step(s):

1. Configuring Auto-Sync - Back End - Enabling the Feature [page 305]
2. Configuring Auto-Sync - Back End - Mobile Application Parameters [page 305]

> → Tip
>
> For best practices and examples on how to configure the Auto-Sync feature, see Common Use Cases for Configuring Auto-Sync [page 309].

4.6.1 Configuring Auto-Sync - Back End - Enabling the Feature

Context

For detailed information about Auto-Sync, see the overview topic, Auto-Sync Configuration [page 303].

The below procedure describes how to enable the feature in the Configuration Panel.

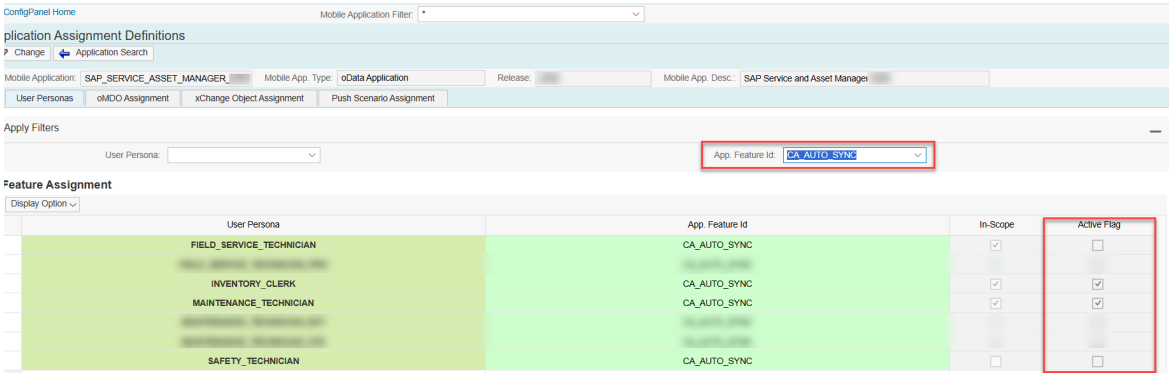
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **Enabling and disabling features**: refer to Configuring Features and Component Assignments in *MAIF Configuration Guide*.

Procedure

1. On the Configuration Panel, go to *Component Assignments* and select your application from the list.
2. In the *App. Feature Id* dropdown, select *CA_AUTO_SYNC*.
3. Enter *Change mode* and set the feature to *Active* for the persona(s) you want to enable it.



4.6.2 Configuring Auto-Sync - Back End - Mobile Application Parameters

Context

For detailed information about Auto-Sync, see the overview topic, Auto-Sync Configuration [page 303].

You can enable, disable, and customize the following Mobile Application Parameters to control how you use the Auto-Sync feature:

> **Note**
>
> - Currently, it is recommended to use only the *PERIODIC* parameter without combining it with other parameters.
> - If the TRESHOLD_PERIOD [page 308] parameter is enabled, the threshold time period will affect **all** parameters in the table.
> - The table below details the expected behavior of all parameters, depending on whether the TRESHOLD_PERIOD [page 308] is set or not set.

Auto-Sync Mobile Application Parameters

Mobile App Parameter	Description	TRESHOLD_PERIOD Set?	Expected Behavior	Parameter Value
PERIODIC	Enables or disables periodic auto-sync.You can set the number of minutes to wait after a completed sync, before starting the next one.	YES	Auto-sync will be performed periodically based on the number of minutes set as the *Parameter Value*. However, auto-sync will **only** be triggered when the time period set for TRESHOLD_PERIOD [page 308] has also elapsed.	• *0* - Disabled • **Number of minutes** - Enabled with an interval in minutes equal to the specified value.
		NO	Auto-sync will be performed periodically based on the number of minutes set as the *Parameter Value*. Sync will start immediately once the specified time period has elapsed.	
ON_CONNECTION_CHANGE	Enables or disables auto-sync on network connectivity changes (from offline to online).	YES	If the mobile device comes from offline to online, **and** the time period set for TRESHOLD_PERIOD [page 308] elapses, auto-sync will be performed.	• *Y* - Enabled • *N* - Disabled
		NO	When the mobile device comes from offline to online, auto-sync starts immediately.	
ON_STATUS_CHANGE	Enables or disables auto-sync on status changes of an object (e.g. work order, operation, sub-operation, notification etc).	YES	If there is a status change for an object, **and** the time period set for TRESHOLD_PERIOD [page 308] elapses, auto-sync will be performed.	• *Y* - Enabled • *N* - Disabled

Mobile App Parameter	Description	TRESHOLD_PERIOD Set?	Expected Behavior	Parameter Value
		NO	If there is a status change for an object, auto-sync starts immediately.	
ON_FOREGROUND	Enables or disables auto-sync when the app moves to the foreground on the mobile device.	YES	If the app moves to the foreground on the mobile device, **and** the time period set for TRESHOLD_PERIOD [page 308] elapses, auto-sync will be performed.	• *Y* - Enabled • *N* - Disabled
		NO	If the app moves to the foreground on the mobile device, auto-sync starts immediately.	
ON_SAVE	• Enables or disables auto-sync on a database save (e.g. saving any changes to an object). • Works **only** if the TRESHOLD_PERIOD [page 308] is enabled as well (set to more than zero). • Applicable only to Maintenance Technician and Field Service Technician personas.	YES	If there is a save to the database, **and** the time period set for TRESHOLD_PERIOD [page 308] elapses, auto-sync will be performed.	• *Y* - Enabled • *N* - Disabled
		NO	*ON_SAVE* parameter cannot be configured.	

Mobile App Parameter	Description	TRESHOLD_PERIOD Set?	Expected Behavior	Parameter Value
THRESHOLD_PERIOD	• You can set the number of minutes for the threshold period. During this period of time, **no auto-sync will be initiated** (even if during that time another parameter would trigger a sync). • The aim of the *THRESHOLD_PERIOD* parameter is to optimize performance, by avoiding too frequent auto-syncs, triggered by all the other parameters in this table. • The *THRESHOLD_PERIOD* parameter is a prerequisite for the ON_SAVE [page 307] parameter to work.	YES	• If any other parameters try to trigger an auto-sync during the threshold period, the auto-sync will **not start** until the threshold period has elapsed. • If no other parameters try to trigger an auto-sync during the threshold period, once the threshold period has elapsed, auto-sync **will not** be performed, and the threshold period will start again.	• *0* - Disabled • **Number of minutes** - Enabled with an interval in minutes equal to the specified value.
		NO	All other parameters (except ON_SAVE [page 307]) can trigger an auto-sync right away.	

→ Tip

- For best practices and examples on how to configure the Auto-Sync feature, see Common Use Cases for Configuring Auto-Sync [page 309].

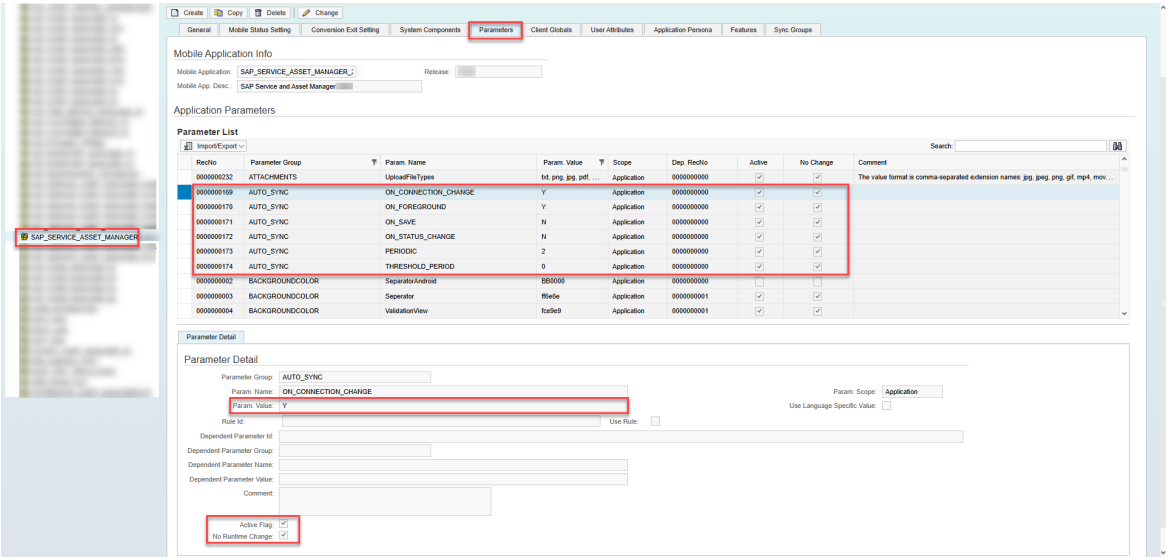
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **Mobile Application Parameters** configuration: refer to Parameters Tab in *MAIF Configuration Guide*.

Procedure

1. Ensure the *CA_AUTO_SYNC* feature is enabled for your persona(s). See Configuring Auto-Sync - Back End - Enabling the Feature [page 305].
2. Navigate to *Mobile Application Configuration* > *Parameters* tab.



3. Select your application from the list of *Defined Mobile Applications*
4. Configure one or more parameters in the *AUTO_SYNC Parameter Group* as desired. See the table above [page 306] for more information about parameters and how to configure them.
5. Check the *Active* flag to ensure that the parameter is used by the mobile application.
6. **OPTIONAL**: If not already checked, check the *No Runtime Change* box to ensure the value of the parameter will not be overridden at runtime through synchronization processing.
7. *Save* your changes.

4.6.3 Common Use Cases for Configuring Auto-Sync

This document describes examples and common scenarios for configuring the Auto-Sync feature to achieve optimal performance and efficiency when using the SAP Service and Asset Manager application.

> **Note**
>
> For detailed information about Auto-Sync, see the overview topic, Auto-Sync Configuration [page 303].

Periodic Sync - Recommended

The app auto-syncs periodically when it is running in the foreground of the mobile device. No other events will trigger auto-sync, which is currently the recommended scenario for optimal performance. You can set the time

period according to your preference. When configuring mobile application parameters for this use case, make sure **to enable only the Periodic [page 306]** parameter.

Auto-sync triggered by specific events

If you do not want to initiate auto-sync solely by a set time period, you can configure it to be triggered by specific events, for example in case of a status change of an object, or when the user makes any change to an object and saves the change to the back end (see Configuring Auto-Sync - Back End - Mobile Application Parameters [page 305]).

> **Note**
>
> In this case you must also enable the TRESHOLD_PERIOD [page 308] parameter for all other parameters.

4.7 Catalog Profiles Configuration

This document describes how to configure the Catalog Profiles feature for the Safety Technician persona.

By configuring catalog profiles, the user will be able to view safety-related catalogs, as well as other ones defined according to their preference.

> **Note**
>
> - For more information about using Catalogs, see Work Permit Detail Screen and Isolation Certificate Detail Screen in *Safety Technician User Guide*.
> - For more information about Catalogs configuration, see Configuring Notification Catalog Types [page 106].

Supported Personas

This feature is applicable for the following personas:

Safety Technician

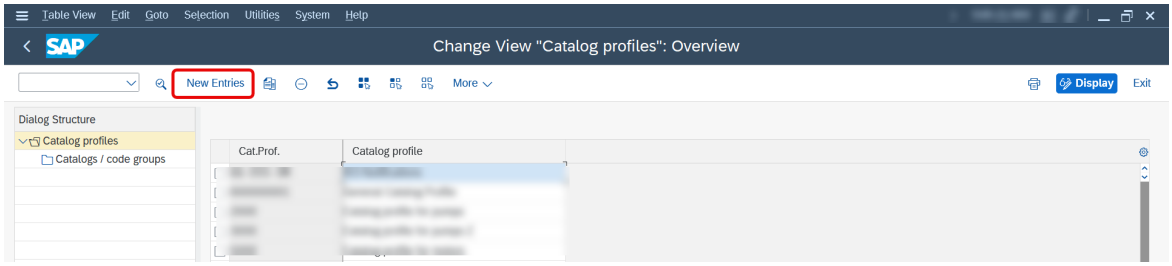
Limitations

See Configuration Prerequisites and Limitations - Safety Technician Persona [page 216].

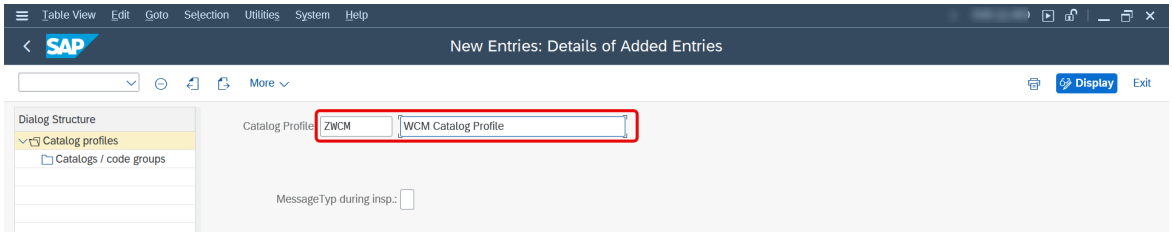
Prerequisites

Before proceeding with configuration steps below [page 311], you need to create a Catalog Profile by performing the following *SPRO* changes in *SAP GUI*:

1. In *SAP GUI* use the transaction code *SPRO* and go to *SAP Reference IMG* > *Logistics - General* > *Product Lifecycle Management (PLM)* > *Plant Maintenance and Customer Service* > *Work Clearance Management* > *Master Data* > *Catalogs* > *Define Catalog Profile*.
2. Click *New Entries*.



3. Enter a name and description of your choice for the Catalog Profile.



4. Click *Save*.

Configuration

Perform the following configuration step(s):

- Configuring Catalog Profiles - Back End - Mobile Application Parameters [page 311]
- Configuring Catalog Profiles - Back End - OMDO Filters [page 313]

4.7.1 Configuring Catalog Profiles - Back End - Mobile Application Parameters

Context

For detailed information about Catalog Profiles, see the overview topic, Catalog Profiles Configuration [page 310].

For the Catalog Profiles feature to work, perform the following Mobile Application Parameters configuration.

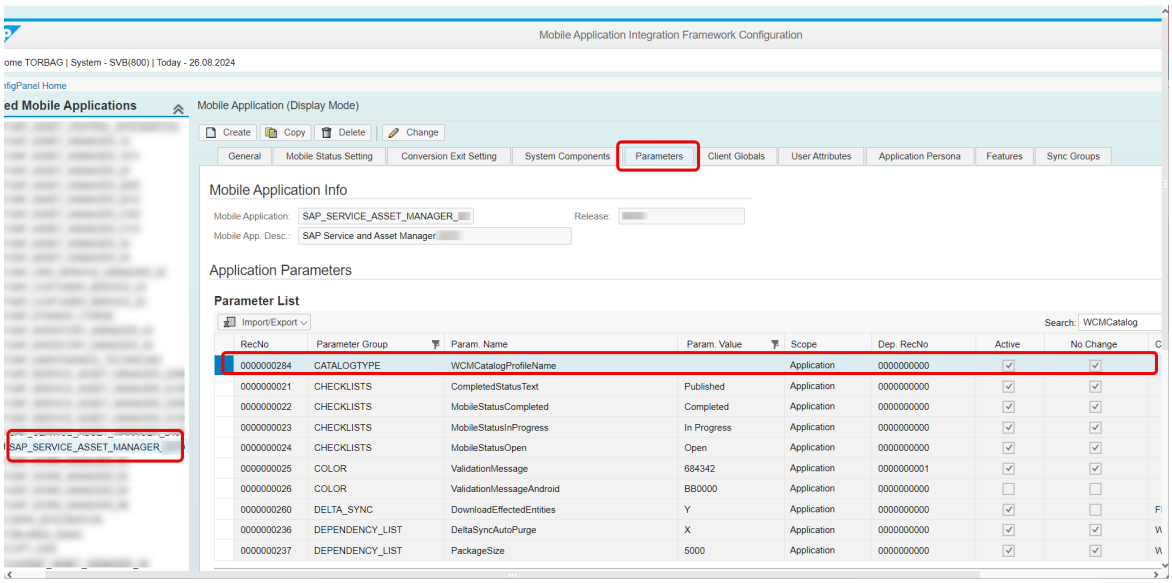
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

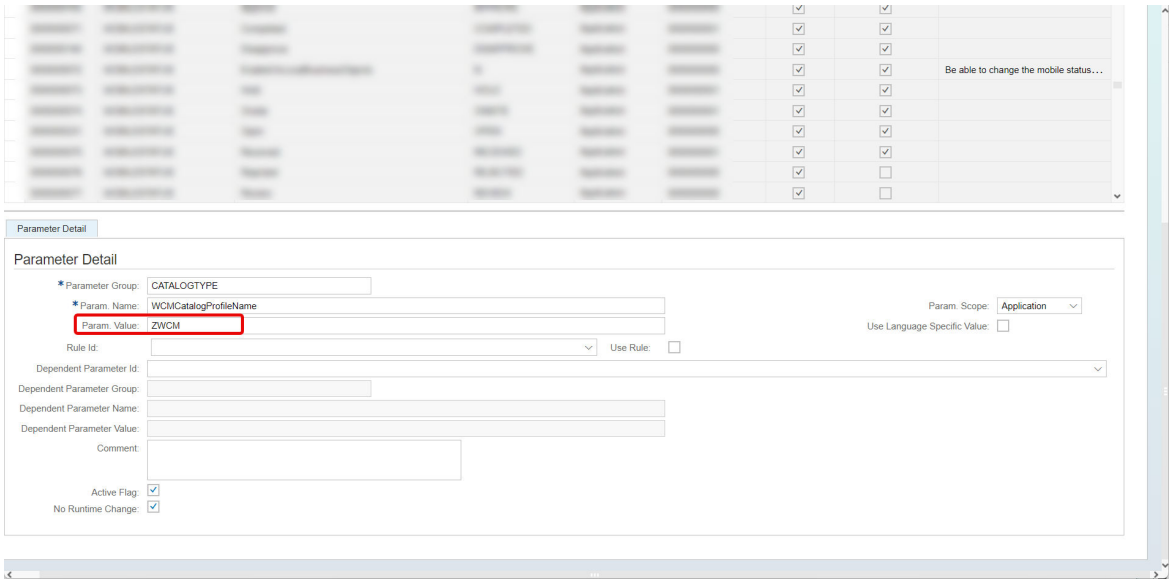
- **Mobile Application Parameters** configuration: refer to Parameters Tab in *MAIF Configuration Guide*.

Procedure

1. On the Configuration Panel, go to *Mobile Application Configuration*.
2. Select your application from the left, go to the *Parameters* tab and select the *WCMCatalogProfileName* Application Parameter.



3. Enter *Change Mode* and under *Parameter Detail*, add the *Parameter Value* that you have already created in SAP GUI [page 311].



4. Click *Save*.

4.7.2 Configuring Catalog Profiles - Back End - OMDO Filters

Context

For detailed information about Catalog Profiles, see the overview topic, Catalog Profiles Configuration [page 310].

For the Catalog Profiles feature to work, perform the following OMDO filters configuration.

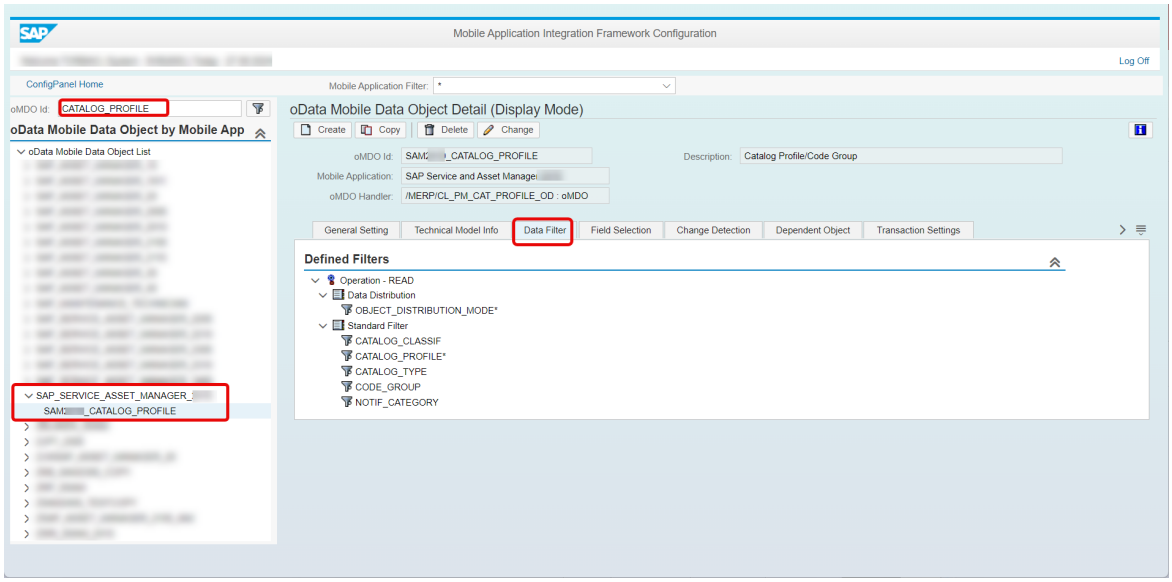
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

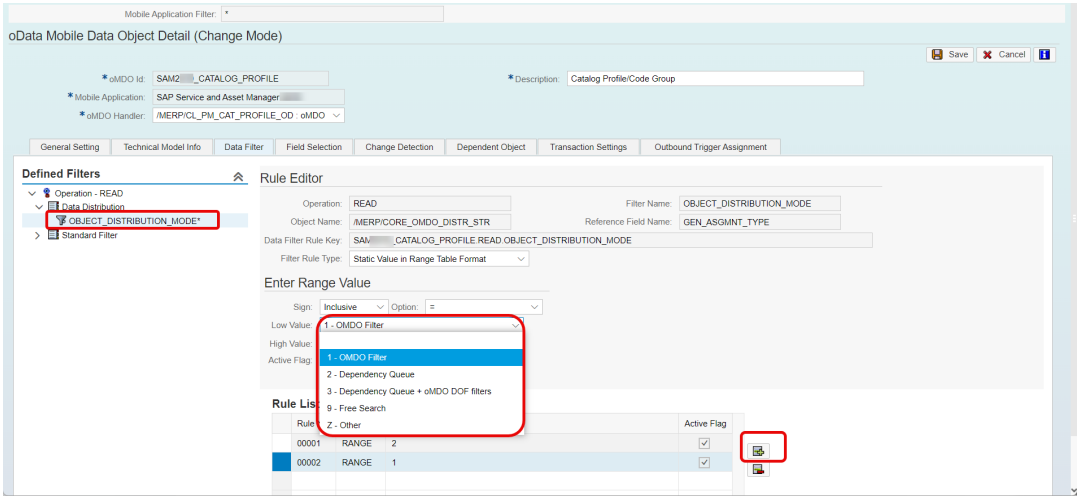
- **OMDO** and **OMDO filter** configuration: refer to OData Mobile Data Object Configuration and OData Mobile Data Object Configuration - Data Filter Tab in *MAIF Configuration Guide*.

Procedure

1. On the Configuration Panel, go to *oData Mobile Data Object Configuration*.
2. On the left, select the oMDO object *<MobileApp>_CATALOG_PROFILE* according to your mobile app version, go to the *Data Filter* tab and maintain the following filters:

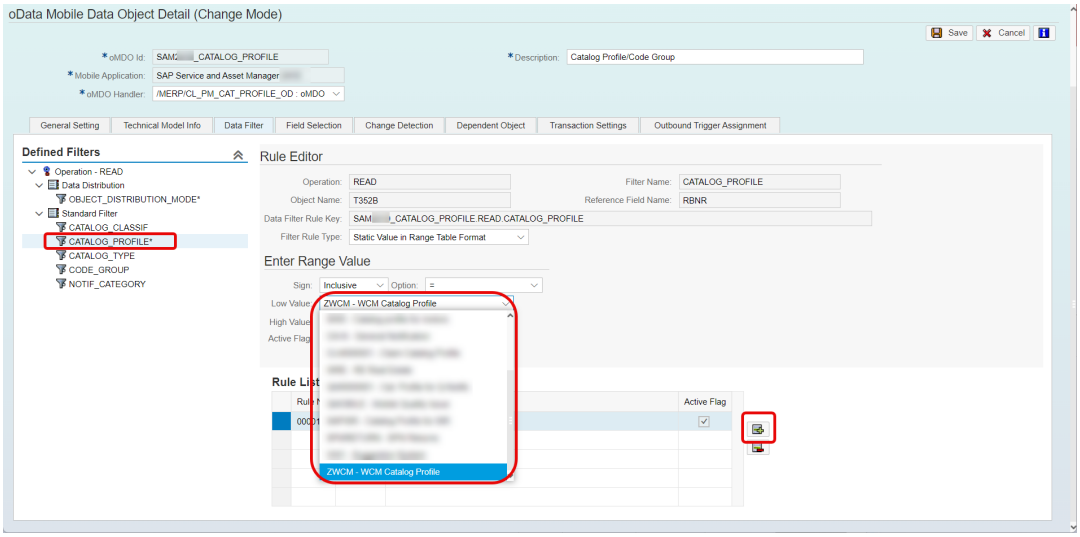


- Under *Data Distribution*, select the *OBJECT_DISTRIBUTION_MODE* filter.
  1. Enter *Change Mode*.
  2. Under *Rule List*, insert a new row and set the *Low Value* field to *1 - OMDO Filter*.



3. Click *Save*.

- Under *Standard Filter*, select the *CATALOG_PROFILE* filter.
  1. Enter *Change Mode*.
  2. Under *Rule List*, insert a new row and in the *Low Value* field select the Catalog Profile that you have already created in SAP GUI [page 311].



3. Click *Save*.

4.8 CATS and PM Confirmation Time Entries Configuration

Use parameters to configure CATS and PM confirmation minute interval values.

Prerequisites

If you're using CATS, the SAP HR module must be installed.

Context

The HR Timesheet feature is called *HR_TIMESHEET*. The PM Confirmation feature is called *PM_CONFIRMATION*. By default, the PM Confirmation feature is enabled. Note that only one feature should be enabled at any given time.

> **Note**
>
> As of the SAP Service and Asset Manager 2205 release, enable and disable parameters are no longer available through the *Parameters* tab. You enable or disable all features through the *Features* tab. See the Configuring Features [page 93] procedure for details.

Use the *CatsMinuteInterval* parameter when CATS is enabled and the *LaborTimeMinutesInterval* parameter when PM confirmations are enabled. The following procedure is the same for either parameter, even though this guide is using the *CATSMinuteInterval* parameter as an example.

When a mobile user manually logs their time, or their time is automatically logged for them through the use of the application, the time logged is rounded to the nearest interval configured. For example, you manually log an additional 12 minutes of work on a work order on a mobile device. Your *CATSMinuteInterval* parameter is set to *15*. Therefore, your additional time logged is automatically rounded up to 15 minutes. The time entry screens also have their duration control values limited to minute values matching the configured interval.

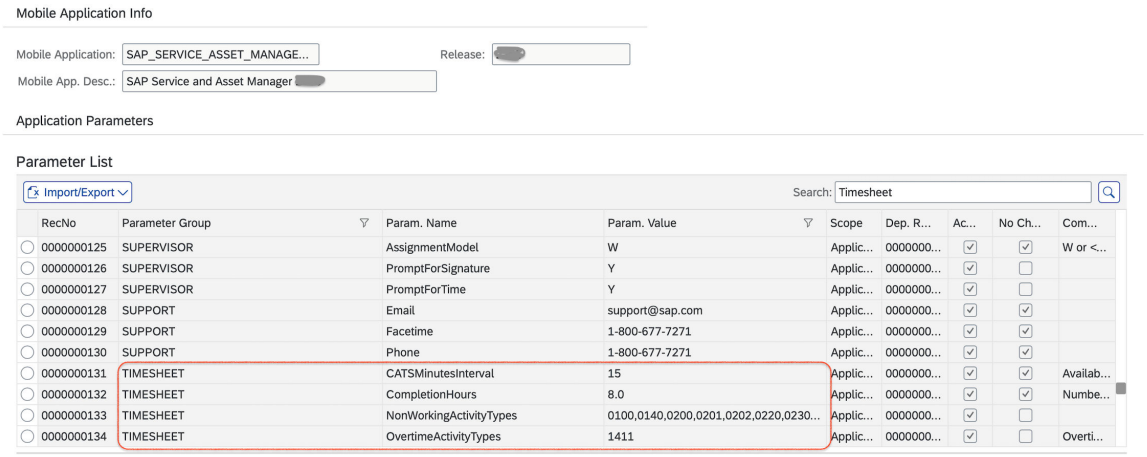
The default value for both parameters is *15*.

Procedure

1. Using the ConfigPanel, navigate to *Mobile Application Configuration* > *Parameters tab*. In the left column, *Defined Mobile Applications*, select your application.

   The *Parameter List* populates with a list of all parameters available for the application.
2. The *CATSMinuteInterval* parameter is found in the *TIMESHEET* group. You can scroll down to find the parameter, or perform a search using the *Search* box. Highlight the *CATSMinuteInterval* parameter and click the *Change* button.

   > **Note**
   >
   > You can find *LaborTimeMinutesInterval* parameter in the *PMCONFIRMATION* group.



3. You can change either the CATS or the PM confirmation labor time interval to the following values:
   - 1
   - 5
   - 10
   - 15
   - 30

   If you accidentally set the parameter to an interval value that isn't an allowed value, the parameter automatically defaults to a value of *15* on the client device.
4. Check the `<Active>` flag to ensure that the parameter is used by the mobile application. If desired, and if not already checked, check the `<No Runtime Change>` box to ensure that the value of the parameter isn't overridden at runtime through synchronization processing.
5. *Save* your changes.

4.8.1 Allow Technician to Enter Time for Another Technician - Configuration

Context

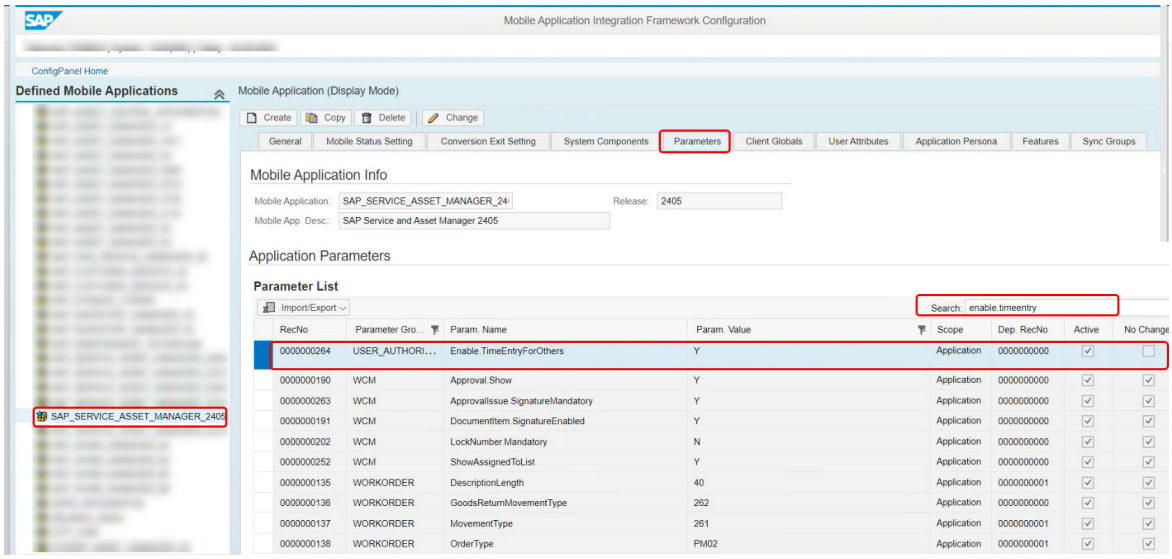
As an administrator you can enable for technicians to enter time on behalf of another user in the application. When enabled, the technician can enter time in:

- PM time confirmations
- CATs timesheet

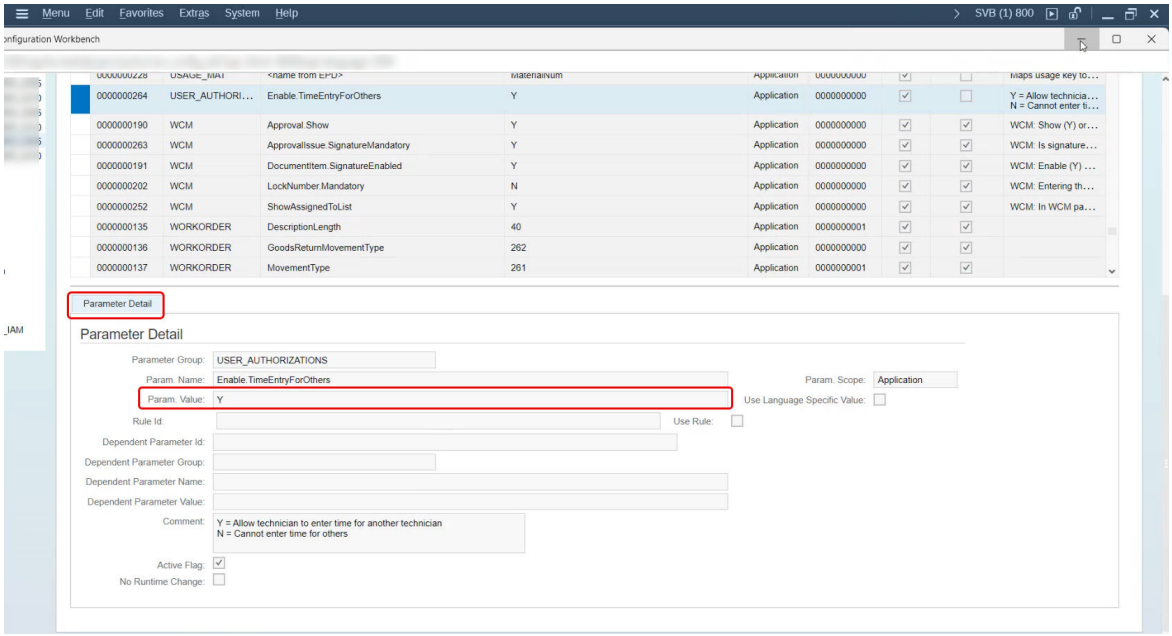
> **Note**
>
> - To be able to enter time for another user in the application, the user need to have a personnel number in the system.
> - This feature **will not work** if the Crew component is enabled (it can be considered as an alternative to the Crew component with easier configuration procedure).
> - For more information about how the feature works in the application, see Adding Time for Another Technician.

Procedure

1. In the *Configuration Panel*, navigate to *Mobile Application Configuration*.
2. Select the application, go to *Parameters* tab and search for the parameter *Enable.TimeEntryForOthers*.



3. Under the *Parameter Detail* tab, set the *Parameter Value* to *Y* (Yes).



4.9 Clock In Clock Out Configuration

The Clock In Clock Out (CICO) feature decouples time tracking from the mobile status of a work order or operation, allowing multiple users to start and log time against the same work order or operation simultaneously.

Overview

> **Note**
>
> As of the SAP Service and Asset Manager 2205 release, enable and disable parameters are no longer available through the *Parameters* tab. You enable or disable all features through the *Features* tab. See the Configuring Features [page 93] procedure for details.

The Clock In Clock Out feature is called *PM_CLOCK_IN_CLOCK_OUT* .

The CICO parameter in the ConfigPanel allows multiple users to work on the same work order or operation, where all users receive the work orders and operations to their devices. CICO allows multiple work orders and operations to be in the Started state that belong to different users. Mobile device users are able to see the CICO state of all work orders or operations on their device. Users can also filter their work order or operations lists based on clock in or clock out status.

If CICO is enabled in the ConfigPanel:

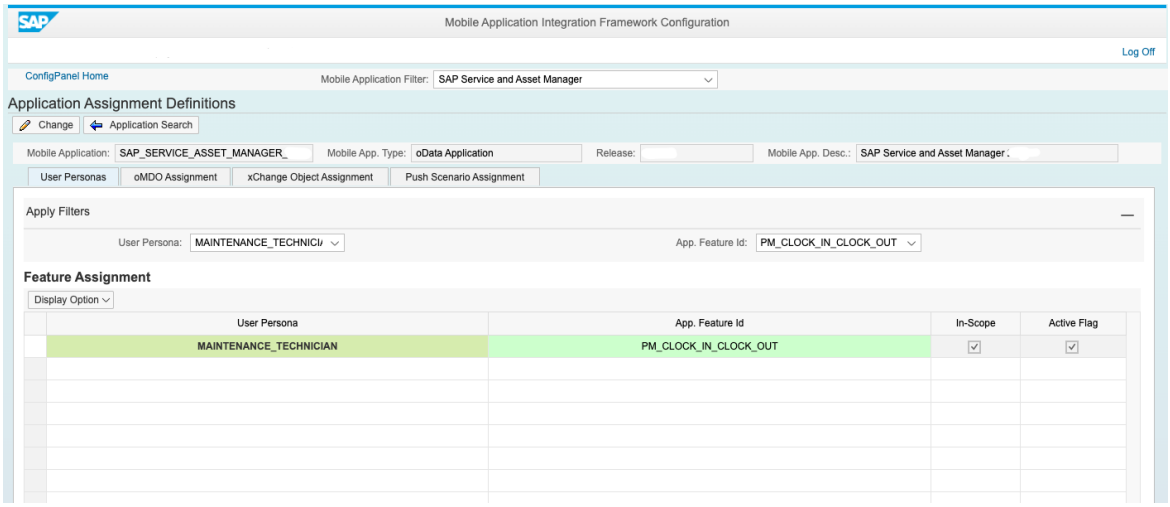
- Multiple people can work on the same work order or operation even if the work order or operation is already started by another user
- Users can clock in to any work order or operation on their device
- Users can only clock in to one work order or operation on their device at a time
- Users must clock out of the current work order or operation before clocking in to a different work order or operation
- All time recording (CATS and Confirmation) uses the clock in clock out period as the default duration in time entry screens
- When a user clocks in to a work order or operation:
  - The timestamp of the work order or operation is saved to a user-specific table that is persisted in the back end
  - The mobile status of the work order or operation is set to Started if it isn't already in a started state
- When a user clocks out of a work order or operation:
  - The work order or operation status is set to either Hold or Complete
  - If a work order or operation is set to Complete and Confirmations are used, the user can set it as the final confirmation

If CICO is disabled in the ConfigPanel:

- A user can start any work order or operation that is in a Hold, Received, or Local state
- A user can start only one work order or operation at a time
- The mobile status of a work order or operation is used to track time in either CATS or Confirmations

How to Set the CICO Parameter Using the Configuration Panel

1. Using the ConfigPanel, navigate to *Component Assignments*. Select your application in the *Mobile Application Filter*. Click the application link in the *Search Result* table.
   The *Application Assignment Definitions* page displays.
2. Click the *Change* button. Find the PM_CLOCK_IN_CLOCK_OUT feature ID in the MAINTENANCE_TECHNICIAN user persona part of the table. Enable or disable the feature using the *Active Flag* checkbox.



3. *Save* your changes.

4.10 Confirmation Scenarios Configuration

When working with an Operation or Suboperation on a Work Order, SAP Service and Asset Manager supports the following confirmation scenarios to help technicians quickly apply confirmations via a dynamic QR code. Both scenarios require two users with devices to add the confirmation to the object.

- *Verification*: In this confirmation scenario, a maintenance technician requests another maintenance technician who has appropriate authorization to review and confirm that a job has been correctly performed.
- *Cooperation*: In this confirmation scenario, the main technician records the work performed by another technician in a supportive role using the QR code generated by that technician.

> **Note**
>
> - Depending on your configuration, you can also print out static QR codes for technicians to scan.
> - For more information about using this feature, see Working with Confirmation Scenarios.
> - For more information about Confirmation Scenarios, refer to Maintenance Management in *SAP S/4HANA documentation*.

Supported Personas

This feature is applicable for the following personas:

Maintenance Technician (Pro)

Prerequisites

This feature is supported **only** on SAP S/4HANA back end system, **on-premise edition 2025**, **or higher**.

Configuration

Depending on the confirmation scenario, perform the following procedure(s):

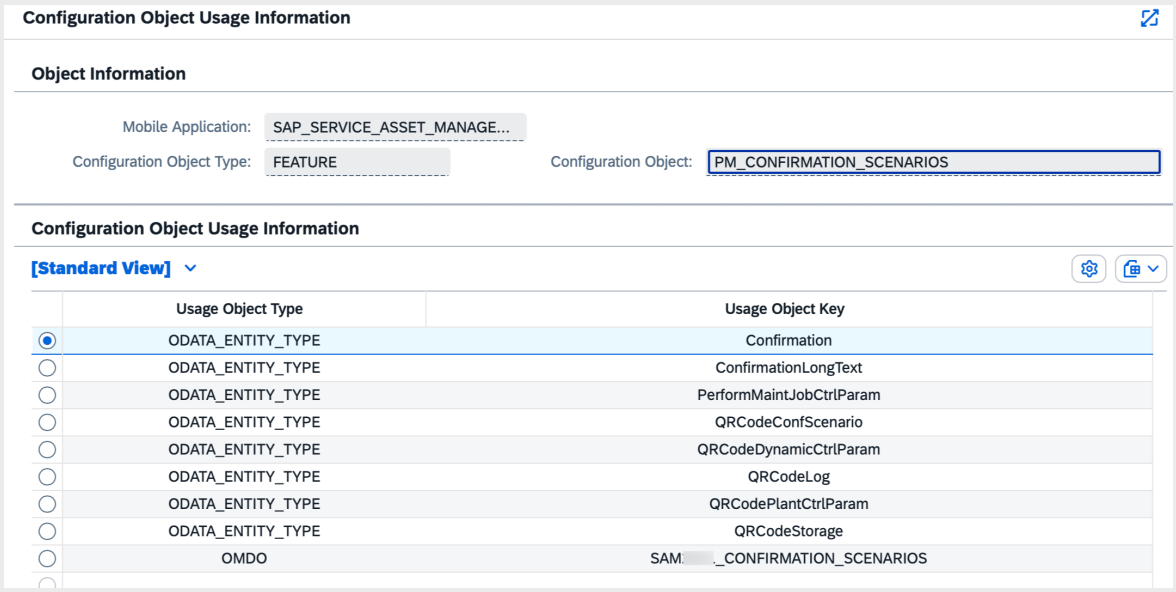
Verification High-Level Configuration Steps

1. Activate the *Verification* feature at the application level:
    1. Ensure the *Maintenance Job Verification* function is set to active in the *V_EAM_ACT_FUNC* table [page 321].
    2. Ensure the *EnableMaintJobVerification* mobile app parameter is set to active [page 327].
2. Configure the user authorization:
    1. Configure the *I_CONFSC* Authorization Object [page 323].
    2. Ensure the *Enable.Conf.Create.DoubleVerification* mobile app parameter is set to active [page 327].
3. Customize the QR code according to your preference [page 324].
4. Enable the feature in the ConfigPanel [page 328].

Cooperation High-Level Configuration Steps

1. Activate the *Cooperation* feature for *Planning Plant* and *Order Type* [page 322].
2. Configure the user authorization:
    1. Configure the *I_CONFSC* Authorization Object [page 323].
    2. Ensure the *Enable.Conf.Create.Cooperation* mobile app parameter is set to active [page 327].
3. Customize the QR code according to your preference [page 324].
4. Enable the feature in the ConfigPanel [page 328].

> **Note**
>
> Additionally, refer to the following object usage information for the Confirmation Scenarios feature:



4.10.1 Configuring Confirmation Scenarios - Back End - SAP GUI

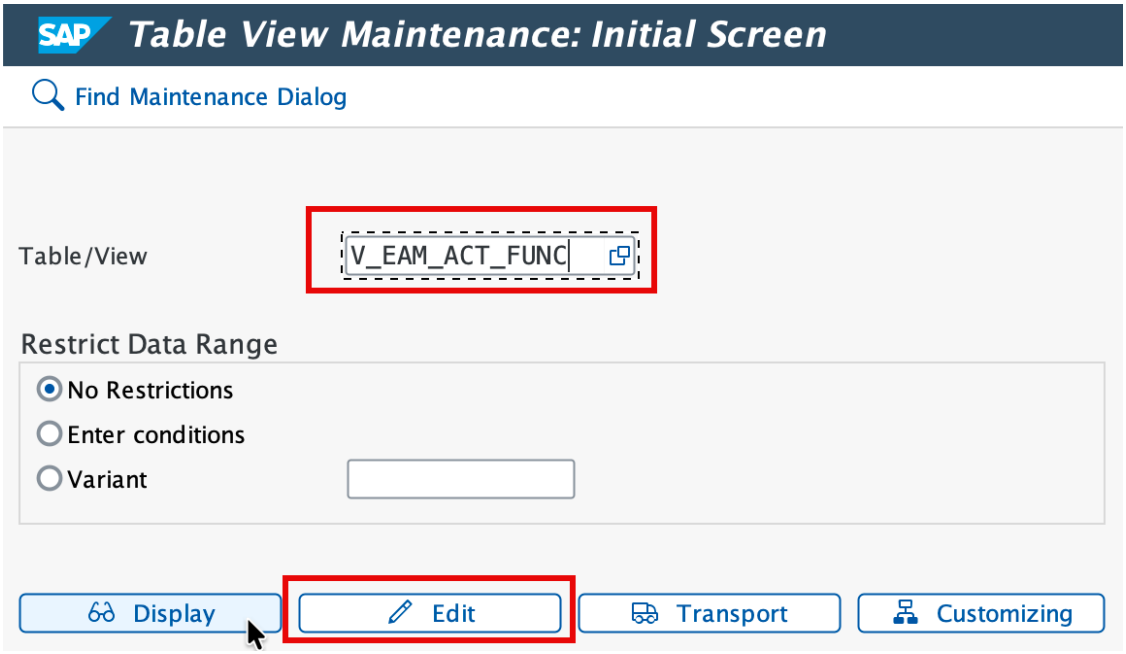
Context

For the **Verification** and/or **Cooperation** scenarios to work, perform the following configuration steps in *SAP GUI*:

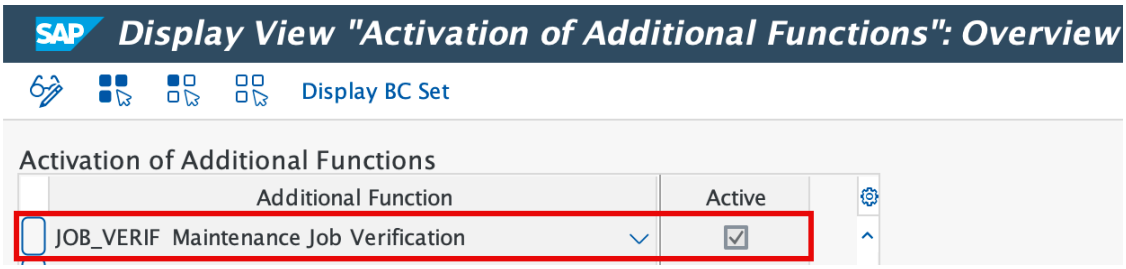
> **Note**
>
> For detailed information about Confirmation Scenarios and the high-level configuration process, see Confirmation Scenarios Configuration [page 319].

Procedure

1. Activate the *Maintenance Job Verification* Function (relevant for the *Verification* scenario):
    1. Enter the transaction code `SM30`.
    2. Enter the table name *V_EAM_ACT_FUNC* and click *Edit*.



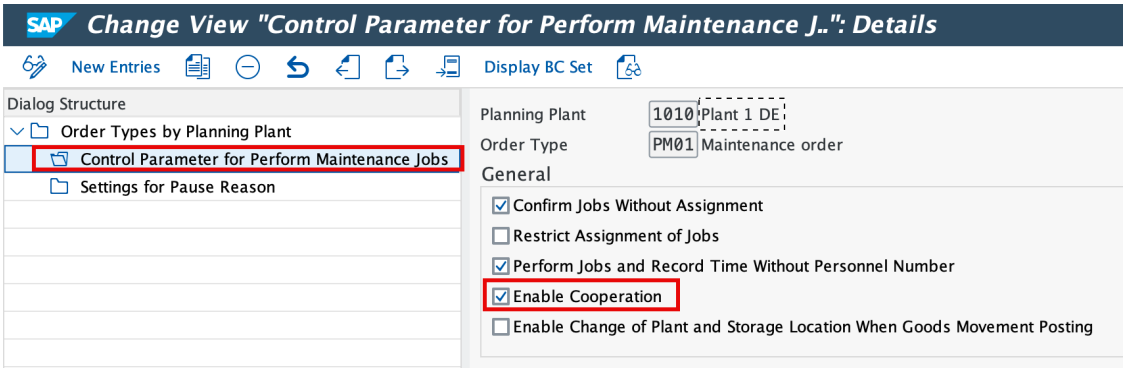
3. Make sure that the function *JOB_VERIF Maintenance Job Verification* is set to *Active*.



4. *Save* your changes.

- Now the *EnableMaintJobVerification* mobile app parameter can read from the *V_EAM_ACT_FUNC* table. See Configuring Confirmation Scenarios - Back End - Mobile Application Parameters [page 327].
- *Verification* is enabled at the **application level**.

2. Enable Cooperation for *Planning Plant* and *Order Type* (relevant for the *Cooperation* scenario):
    1. Enter the transaction code *SIMG* (Implementation Activities).
    2. Navigate to *SAP Customizing Implementation Guide* > *Plant Maintenance and Customer Service* > *Maintenance and Service Processing* > *Completion Confirmations* > *Define Control Parameters for Perform Maintenance Jobs*.
    3. Select an *Order Type by Planning Plant* of your choice from the list and click *Control Parameter for Perform Maintenance Jobs*.
    4. Ensure *Enable Cooperation* is checked.



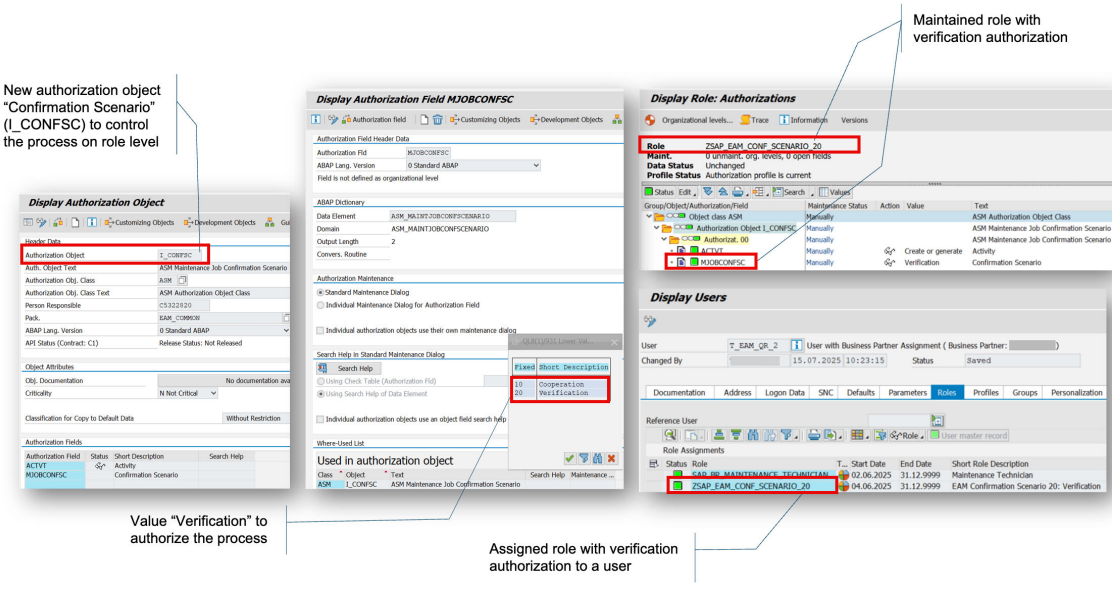
> **Note**
>
> *Cooperation* is enabled for a specific **Planning Plant and Order Type**.

5. *Save* your changes.

3. Configure the user autorization (relevant for both *Verification* and *Cooperation* scenarios):

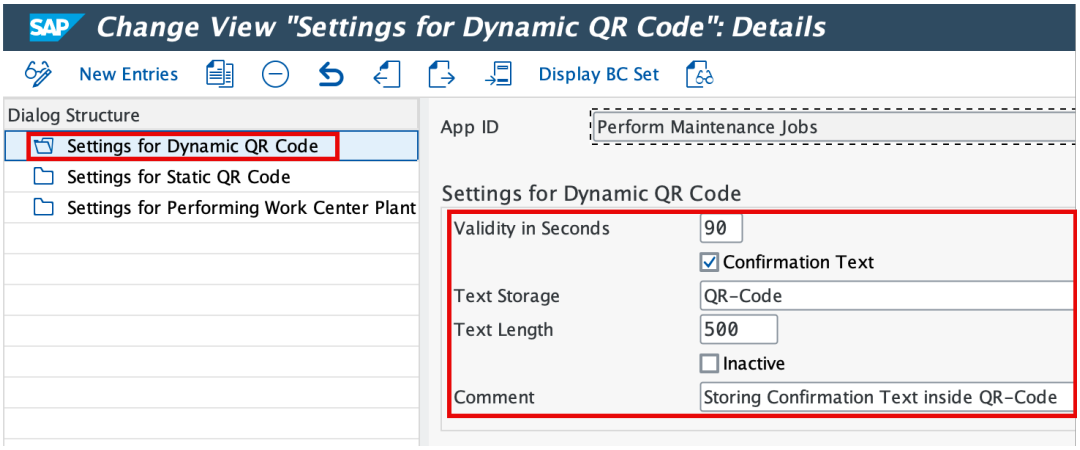
> **Note**
>
> For the Generate QR Code button in the side navigation bar to work, you need to configure the *I_CONFSC* Authorization Object that controls the process on the *Role* level. This is required for the Enable.Conf.Create.DoubleVerification [page 327] and Enable.Conf.Create.Cooperation [page 327] mobile app parameters.

1. Enter the transaction code **SU21** and display the authorization object *I_CONFSC*.
2. Use either *Cooperation* or *Verification* as value to authorize the process.
3. Enter the transaction code **PFCG** and create and maintain a *Role* with the *Cooperation* or *Verification* authorization.
4. Assign the *Role* to the user.
5. See the following image about the procedure, using *Verification* for the *Value*:

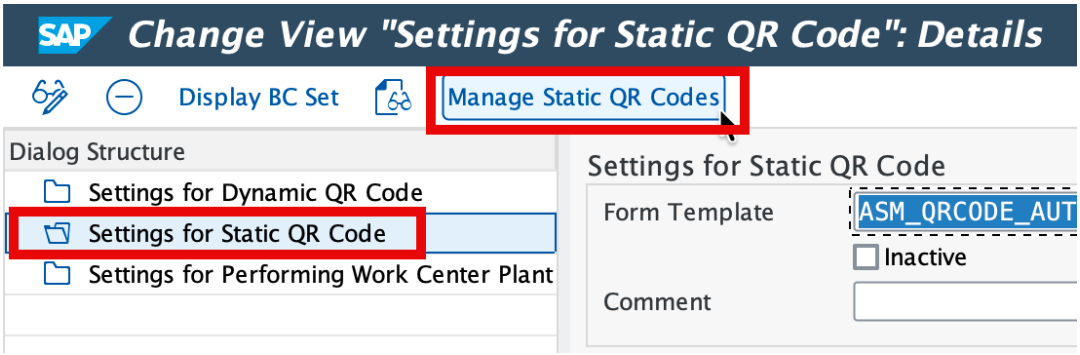


6. *Save* your changes.

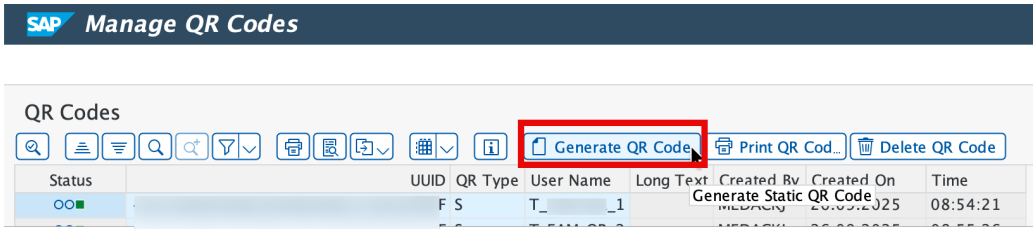
4. Customize the QR Code (relevant for both *Verification* and *Cooperation* scenarios):
    1. Enter the transaction code *SIMG* (Implementation Activities).
    2. Navigate to *SAP Customizing Implementation Guide* > *Plant Maintenance and Customer Service* > *Maintenance and Service Processing* > *Completion Confirmations* > *Define Control Parameters for QR Code Service*.
    3. Here you have the following configuration options for QR codes:
        - *Settings for Dynamic QR Code*: This QR code will be generated by the technician on their mobile device, from the side navigation bar.



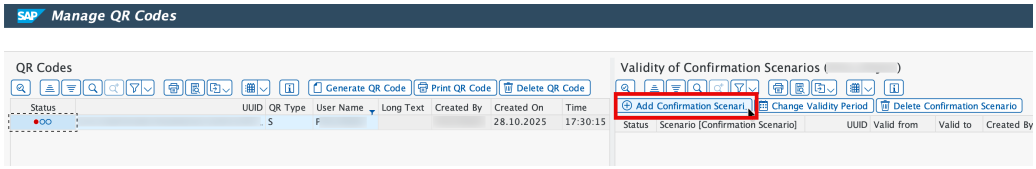
            - *Validity in Seconds*: You can specify the duration in seconds for which the generated dynamic QR code is valid.
            - *Confirmation Text*: If this flag is active, the Technician will have the option of providing a *Confirmation Text* during QR-Code generation.
        - *Settings for Static QR Code*: This QR code is generated from the back end and can be printed out.



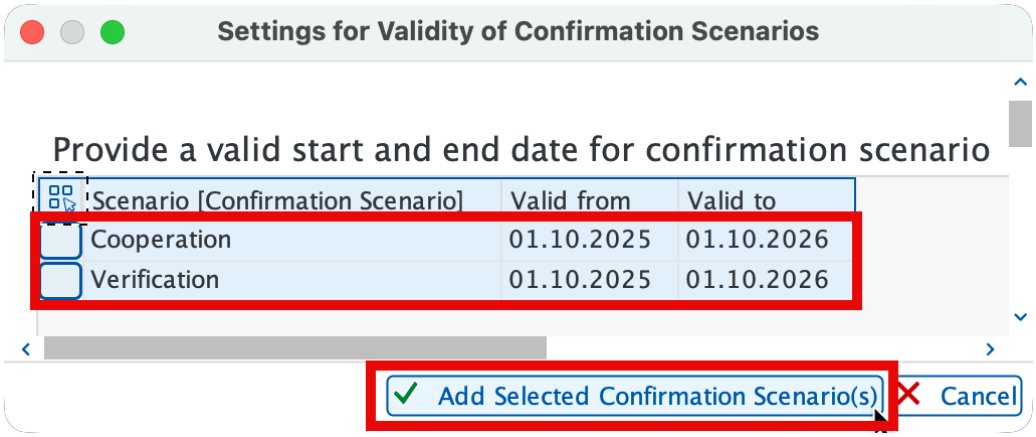
            1. Click *Manage Static QR Codes*.
            2. Click *Generate QR Code*.



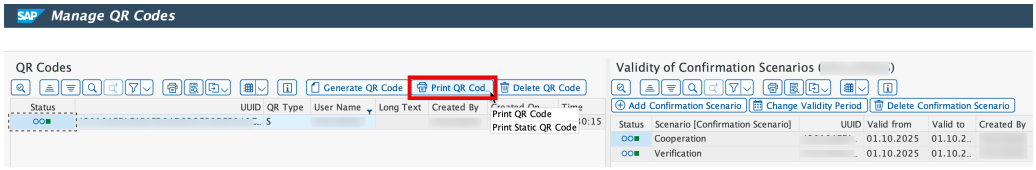
            3. Select a *User*.
            4. Click *Add Confirmation Scenario*.



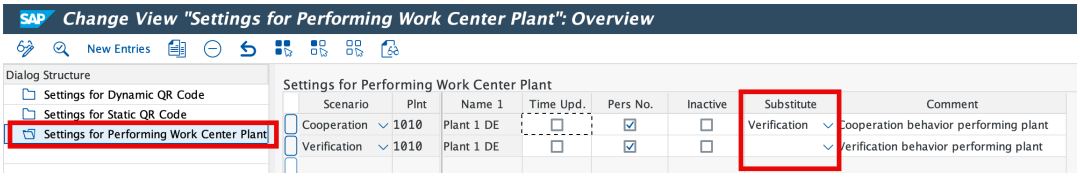
5. Select *Cooperation* and/or *Verification*, set the *Valid from* and *Valid to* dates, and click *Add Selected Confirmation Scenario(s)*.



6. Once added, you can *Print the QR Code*.



- *Settings for Performing Work Center Plant*: You can apply additional settings, according to your preference.



  - *Substitute* Scenario for QR Code Confirmation: Specifies the authorized substitute scenario for the selected confirmation scenario. The QR code that would be generated for the substitute scenario can be used for the selected confirmation scenario too.

    > **Note**
    >
    > For example if the user wants to record a *Cooperation*, but scans a QR code that is only valid for *Verification*, the confirmation will fail. However, if *Cooperation* is set as a *Substitute*, the confirmation will succeed.

Next Steps

Continue with Configuring Confirmation Scenarios - Back End - Mobile Application Parameters [page 326].

4.10.2 Configuring Confirmation Scenarios - Back End - Mobile Application Parameters

Prerequisites

See Configuring Confirmation Scenarios - Back End - SAP GUI [page 321].

Context

For the **Verification** and/or **Cooperation** scenarios to work, configure the *Mobile Application Parameters* in the **ConfigPanel** as follows.

> **Note**
>
> For detailed information about Confirmation Scenarios and the high-level configuration process, see Confirmation Scenarios Configuration [page 319].

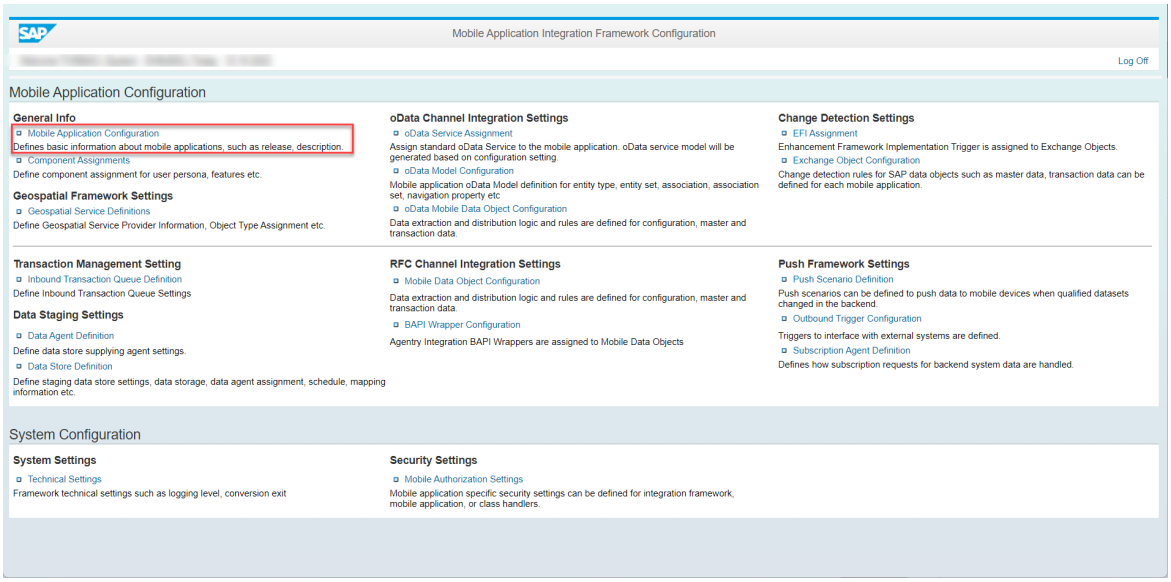
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **Mobile Application Parameters** configuration: refer to Parameters Tab in *MAIF Configuration Guide*.

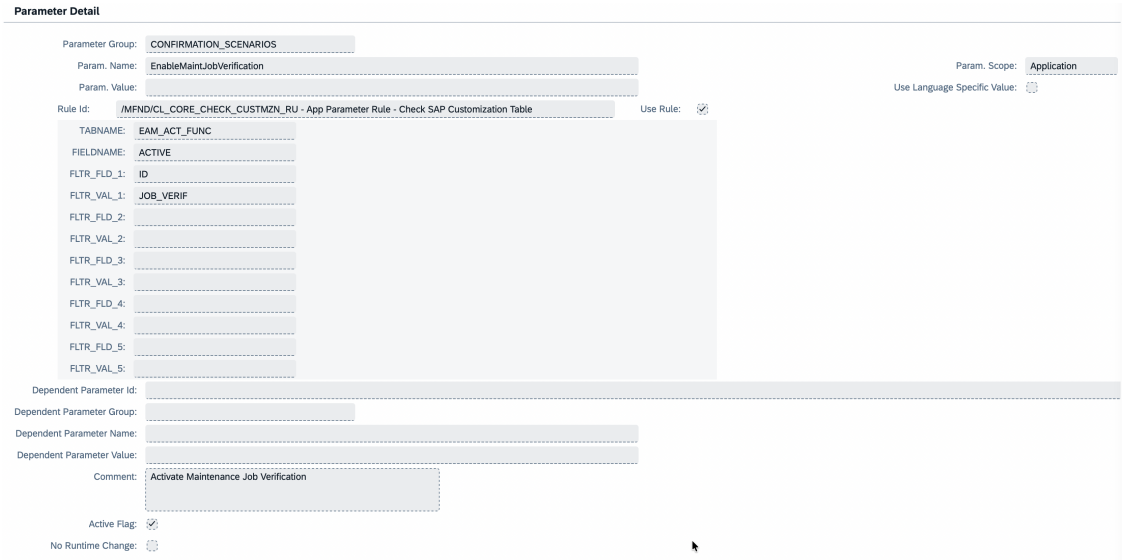
Procedure

1. Navigate to *Mobile Application Configuration*.

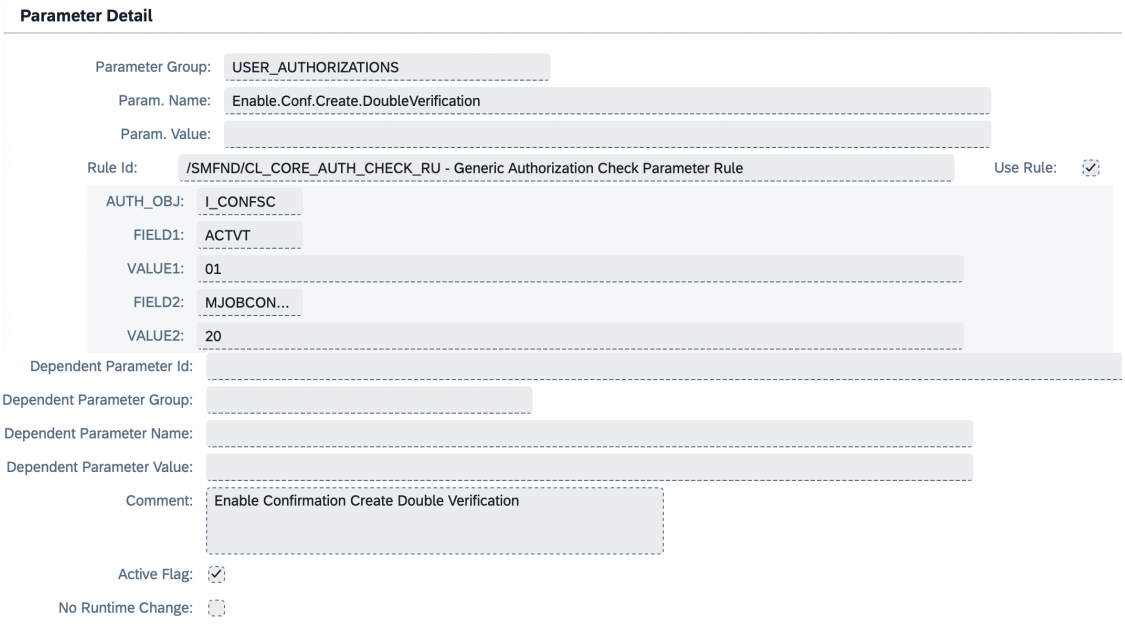


2. Select the application from the list and go to the *Parameters* tab.
3. Ensure the following parameters are configured:

   - *EnableMaintJobVerification* (for **Verification** scenario):
     - Ensure it is set to *Active*.
     - This parameter reads data from the table configured in Activating the Maintenance Job Verification Function [page 321].

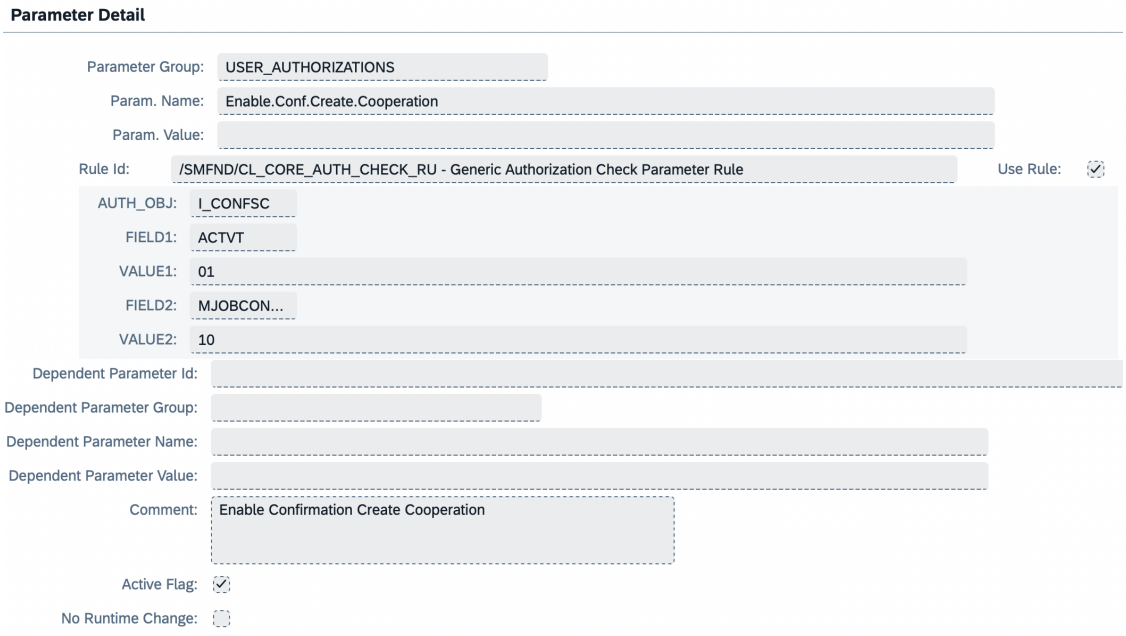


   - *Enable.Conf.Create.DoubleVerification* (for Verification):
     - Ensure it is set to *Active*.
     - For the QR code generation to work, this parameter is checking the *I_CONFSC* authorization object. See Configuring Confirmation Scenarios - Back End - SAP GUI [page 323].



   - *Enable.Conf.Create.Cooperation* (for Cooperation):
     - Ensure it is set to *Active*.

- For the QR code generation to work, this parameter is checking the *I_CONFSC* authorization object. See Configuring Confirmation Scenarios - Back End - SAP GUI [page 323].



Next Steps

Continue with Configuring Confirmation Scenarios - Back End - Enabling the Feature [page 328].

4.10.3 Configuring Confirmation Scenarios - Back End - Enabling the Feature

Prerequisites

See Configuring Confirmation Scenarios - Back End - Mobile Application Parameters [page 326].

Context

The below procedure describes how to enable the feature in the ConfigPanel by persona [page 329] or on the application level [page 329].

> **Note**
>
> For detailed information about Confirmation Scenarios and the high-level configuration process, see Confirmation Scenarios Configuration [page 319].

General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

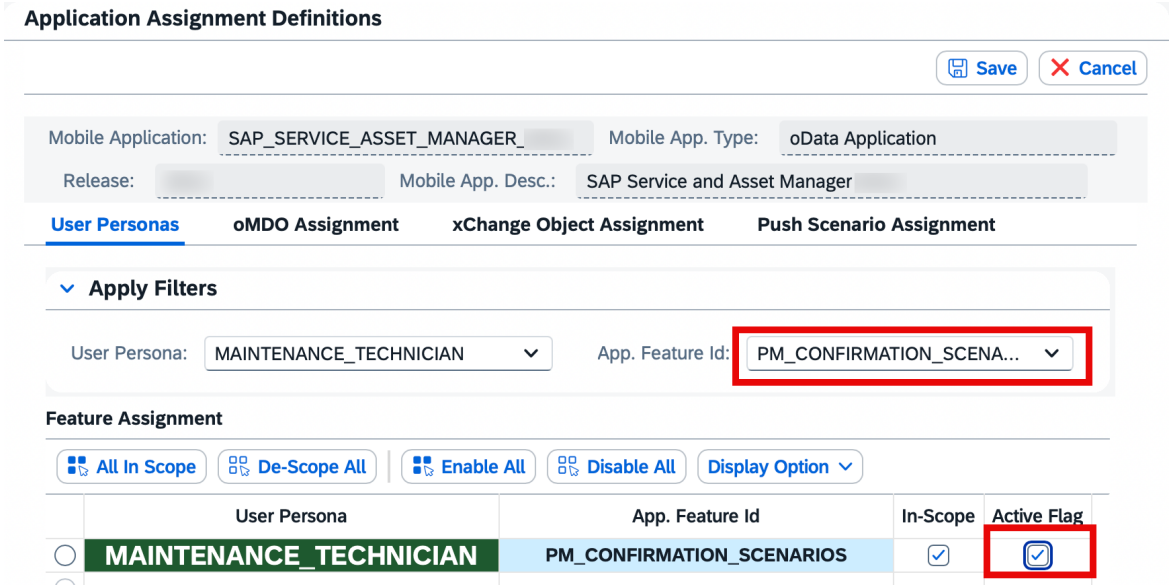
- **Enabling and disabling features**: refer to Configuring Features and Component Assignments in *MAIF Configuration Guide*.

Procedure

Enabling the Feature for Persona

To enable this feature for the supported personas [page 320], perfom the following:

1. Go to *Component Assignments* and select your application from the list.
2. In the *App. Feature Id* dropdown, select *PM_CONFIRMATION_SCENARIOS*.
3. Enter *Change mode* and set the feature to *Active* for the personas you want to enable it.

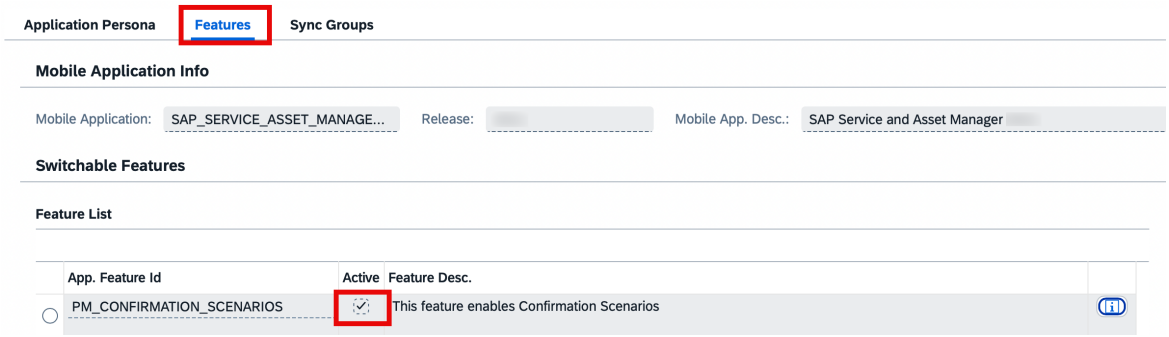


4. *Save* your changes.

Enabling the Feature on the Application Level

To enable this feature on the application level, perform the following:

5. In the ConfigPanel, go to *Mobile Application Configuration*.
6. Select your application from the left and go to the *Features* tab.
7. Enter *Change mode* and set the **PM_CONFIRMATION_SCENARIOS** feature to *Active*.



8. *Save* your changes.

4.11 Customer Service Notification Types Configuration

Prerequisites

Be sure that you have installed the Customer Service component. See the instructions in the Asset Manager Component Installation Guide for IOS for more information.

> **Note**
>
> Configuring Customer Service notification types is optional and is required only if the Customer Service component is enabled.

Procedure

1. Access the ConfigPanel through SAP Mobile Add-On.
2. From the ConfigPanel *Home* page, click the *OData Mobile Data Object Configuration* link.
3. At the top of the *OData Mobile Data Object Configuration* page display, in the *Mobile Application Filter* field, choose your mobile application from the dropdown menu. Choosing your mobile application is not a necessary step, but it eliminates objects that are not part of your mobile application from the object list.
4. Click the *Data Filter* tab.
5. Expand the *OData Mobile Data Object List* tree so you can see all of the OData mobile objects.
6. Select *SAMXXXX_NOTIFICATION_GENERIC* from the list. Then select *Data Filter tab* > *Operation - READ* > *Data Distribution* > *NOTIF_TYPE*

   The current rule filter settings are displayed in the *Rule Editor* section. All existing rules for the filter are displayed in the *Rule List* table.
7. To activate the Customer Service order type, click *Change*.

   Many of the fields in the rule editor become editable.
8. Set the *Active Flag* to *True* `<Rule Value>` */MERP/CL_PM_NOTIF_TYPE_ORU?CS*.

9. To apply your changes, click *Save*.

Results

The Customer Service notification type is activated in the ConfigPanel.

4.12 Customer Service Order Types Configuration

Prerequisites

Be sure that you have installed the Customer Service component. See the instructions in the Asset Manager Component Installation Guide for IOS for more information.

> **Note**
>
> Configuring Customer Service order types is optional and is required only if the Customer Service component is enabled.

Procedure

1. Access the ConfigPanel through SAP Mobile Add-On.
2. From the ConfigPanel *Home* page, click the *OData Mobile Data Object Configuration* link.
3. At the top of the *OData Mobile Data Object Configuration* page display, in the *Mobile Application Filter* field, choose your mobile application from the dropdown menu. Choosing your mobile application is not a necessary step, but it eliminates objects that are not part of your mobile application from the object list.
4. Click the *Data Filter* tab.
5. Expand the *OData Mobile Data Object List* tree so you can see all of the OData mobile objects.
6. Select *SAMXXXX_WORK_ORDER_GENERIC* from the list. Then select *Data Filter tab* > *Operation - READ* > *Data Distribution* > *ORDER_TYPE*

   The current rule filter settings are displayed in the *Rule Editor* section. All existing rules for the filter are displayed in the *Rule List* table.
7. To activate the Customer Service order type, click *Change*.

   Many of the fields in the rule editor become editable.
8. Set the *Active Flag* to *True* for the `<Rule Value>` */MERP/CL_PM_ORDER_TYPE_ORU?CS*.
9. To apply your changes, click *Save*.

Results

The Customer Service order type is activated in the ConfigPanel.

4.13 Digital Signature Overview

The digital signature feature performs a verification of work by digitally signing for the work using a user name and password. The digital signature framework is able to create digital signature verification by using a back-end user name and registered time-based one-time password, or TOTP. The TOTP is brought by the CL_TOTP object.

The digital signature UI5 reuse component provides an OData service that allows for direct online interaction by the client to register a digital signature completed work.

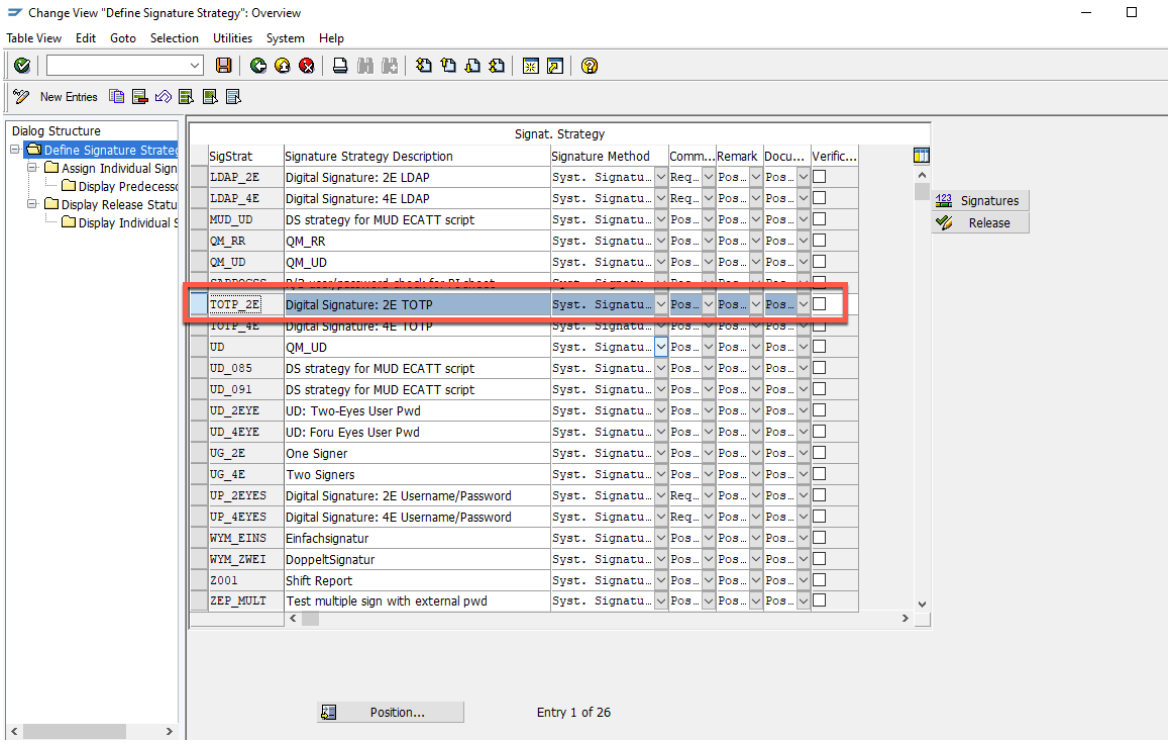
The Digital Signature feature is called *CA_DIGITAL_SIGNATURE*. By default, the feature is not enabled.

> **Note**
>
> As of the SAP Service and Asset Manager 2205 release, enable and disable parameters are no longer available through the *Parameters* tab. You enable or disable all features through the *Features* tab. See the Configuring Features [page 93] procedure for details.

For complete information on digital signature, see the Digital Signature guide, specifically the Implementation Guide for UI5 Reuse Component topic and subtopics.

Limitations

- SAP Service and Asset Manager digital signature relies on the CL_TOTP object interface.
- SAP Service and Asset Manager digital signature uses a connection to the UI5 Reuse component in digital signature. The UI5 Reuse component provides the ability to digitally sign different objects.
- Digital signature support from SAP Service and Asset Manager is only available on an SAP S/4HANA 2020 or later back end system. Digital signature is therefore available for SAP Service and Asset Manager 2105 or later releases installed on a SAP S/4HANA 2020 or later back end system.
- Digital signature is supported with any two-eyed (2E) strategy. Out of the box, the TOTP_2E strategy is used. TOTP_2E is the two-eyed principle of a technician signing the operation for their work. You can configure the 2E strategy by navigating to *OData Mobile Data Object Configuration* > *Data Filter*. Select the **SAMXXXX_DSIG_CONFIGURATION** OMDO with the filter *SIGNATURE_STRATEGY*.



4.13.1 Enabling Digital Signature

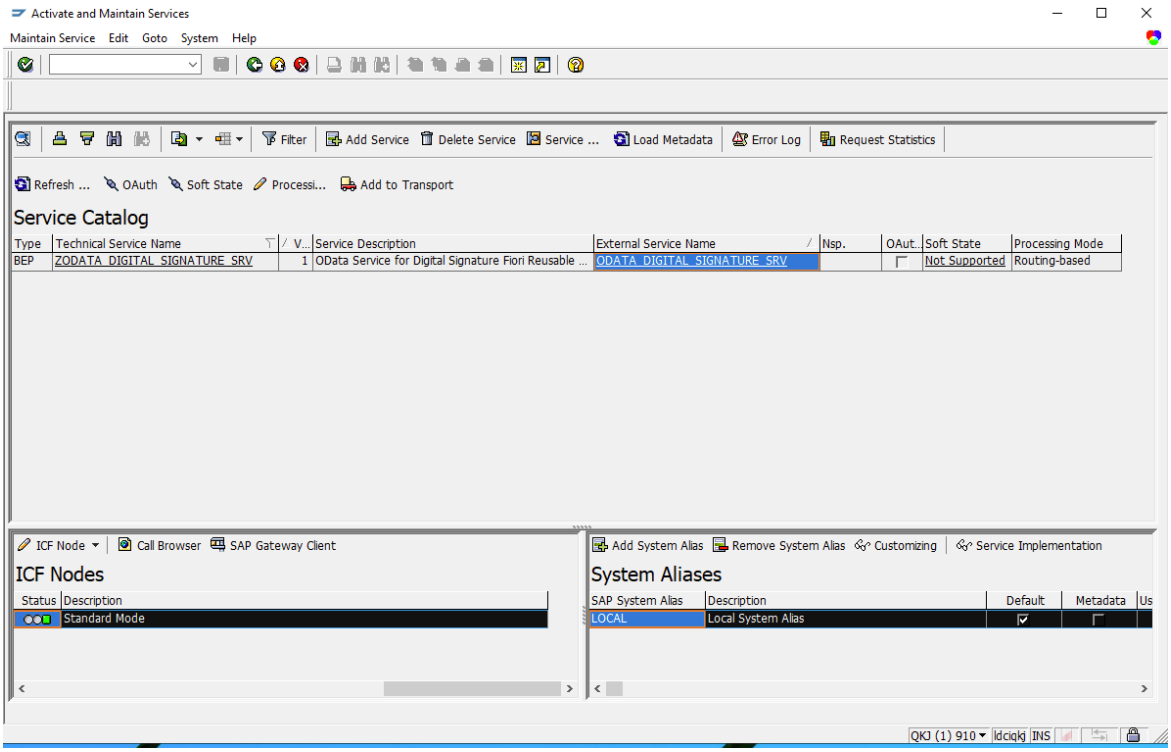
Prerequisites

Ensure you're following all points discussed in the *Limitations* section of the Digital Signature Overview [page 332] topic.

An authenticator application, such as Microsoft Authenticator, must be installed on the mobile device, in order to use the TOTP process.

Procedure

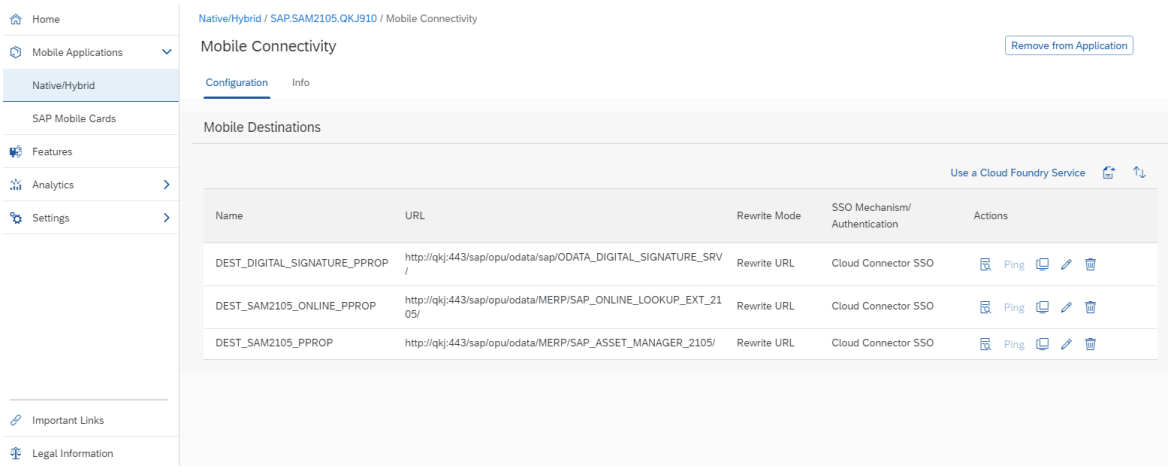
1. **Create a destination in SAP Business Technology Platform Mobile Services (SAP BTP services)**: Create a specific destination in SAP BTP services that points to the digital signature service.



The digital signature service must be exposed to the back-end gateway in transaction */n/IWFND/MAINT_SERVIVCE*. The external service name that must be exposed is *ODATA_DIGITAL_SIGNATURE_SRV*.

If a front-end service exists, expose the digital signature service in the same way you expose other services.

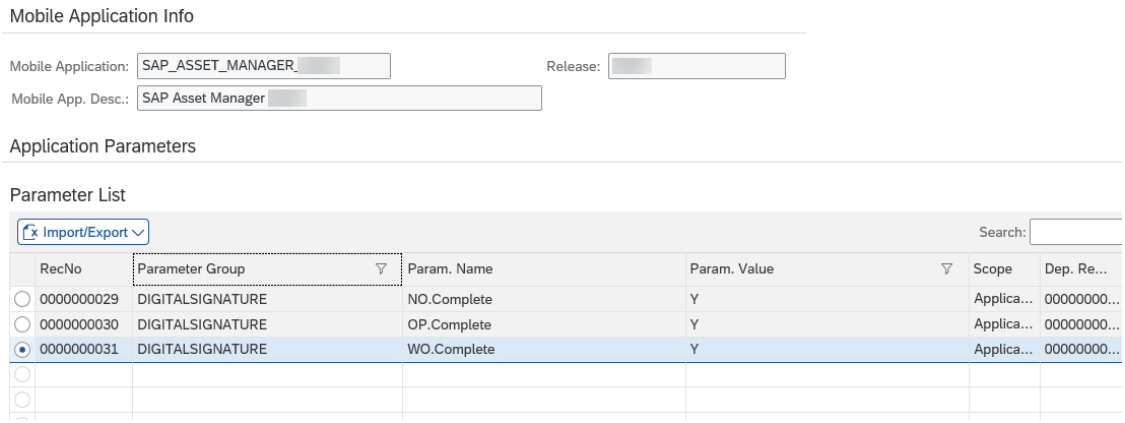
2. **Expose the service on SAP BTP services**: Create a mobile destination and attach it to the SAP Service and Asset Manager 2511 application. The destination name is *DEST_DIGITAL_SIGNATURE_PPROP* with the URL pointing to the back-end service for digital signature.



3. **Enable digital signature on the ConfigPanel:**

   a. Open the ConfigPanel and navigate to *Mobile Application Configuration* > *Parameters tab*. Select your application release.

   b. Enable the *DIGITAL SIGNATURE* parameters required for your site.



c. *Save* your changes.

4.13.2 Setting up the TOTP_2E Signature Strategy

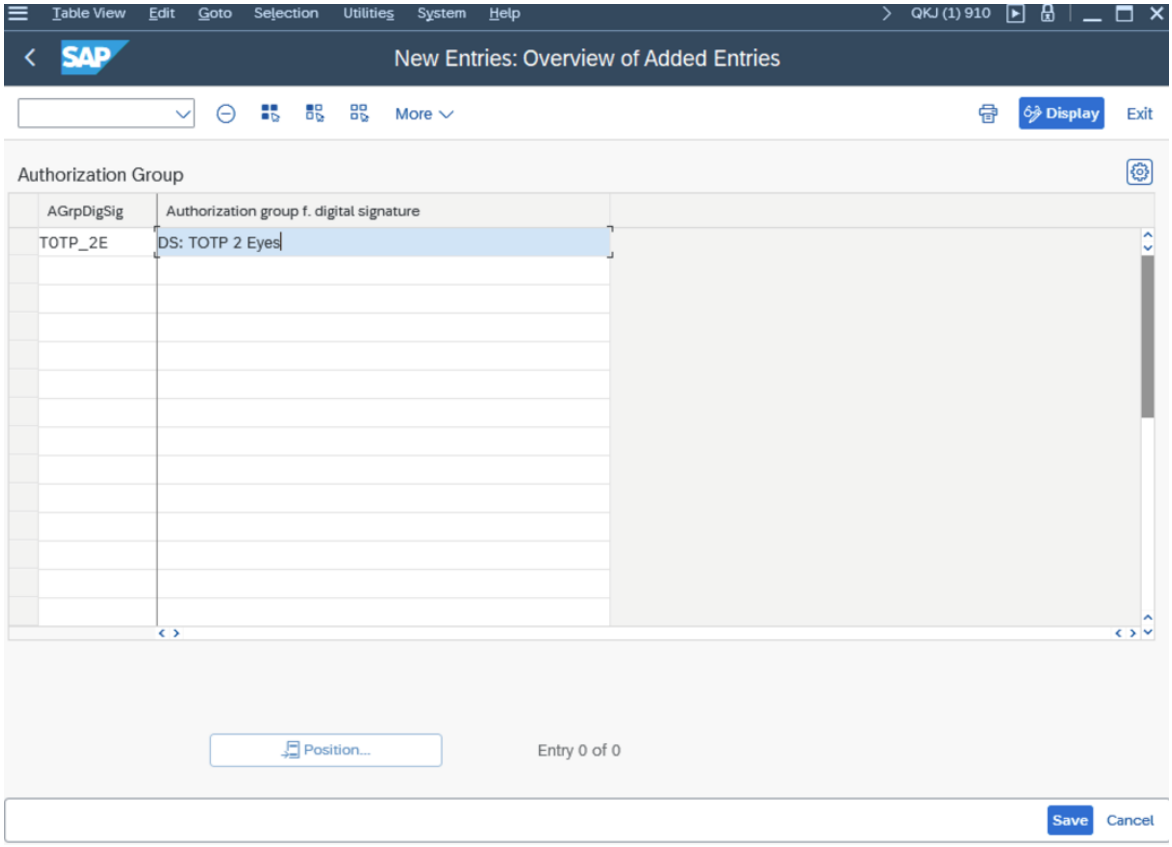
Context

In order for Digital Signature to work with SAP Service and Asset Manager, the digital signature strategy for two-eyed principle needs to be setup in the backend SAP S/4HANA system. This is required for technicians to successfully execute the signature, be it at operation or header level work order scenario.

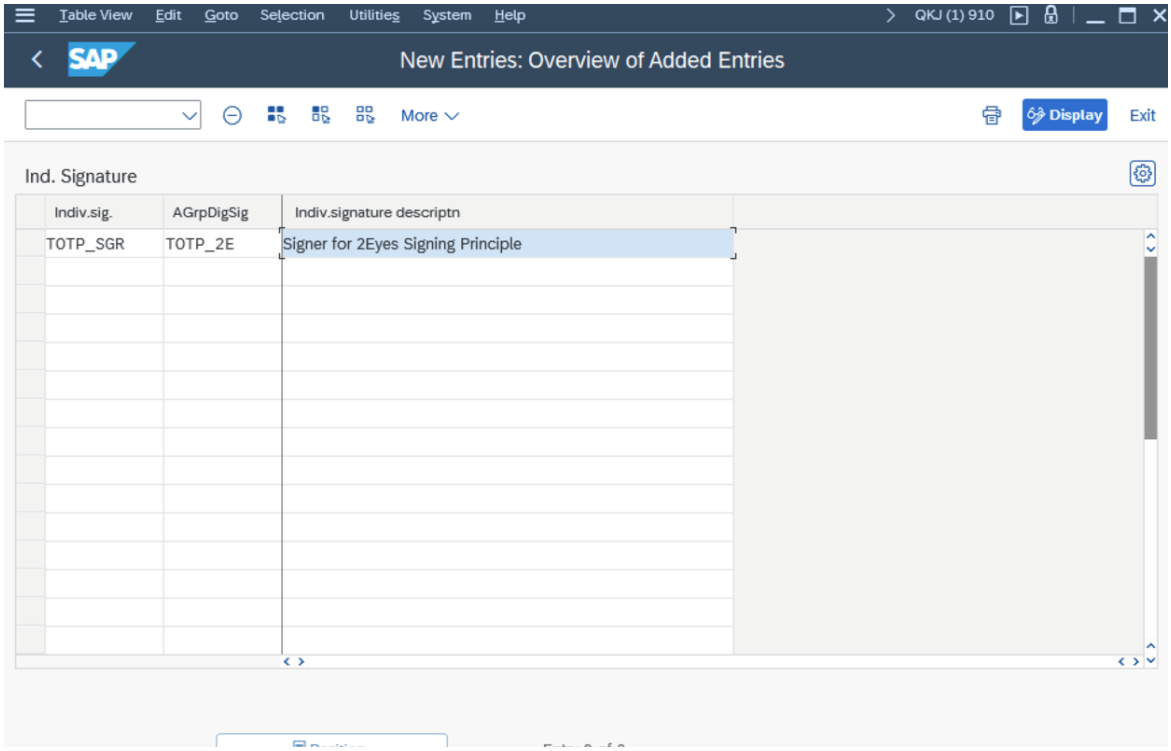
Perform the following steps to setup the TOTP_2E strategy so that the SAP Service and Asset Manager Client can properly react to digital signatures.

Procedure

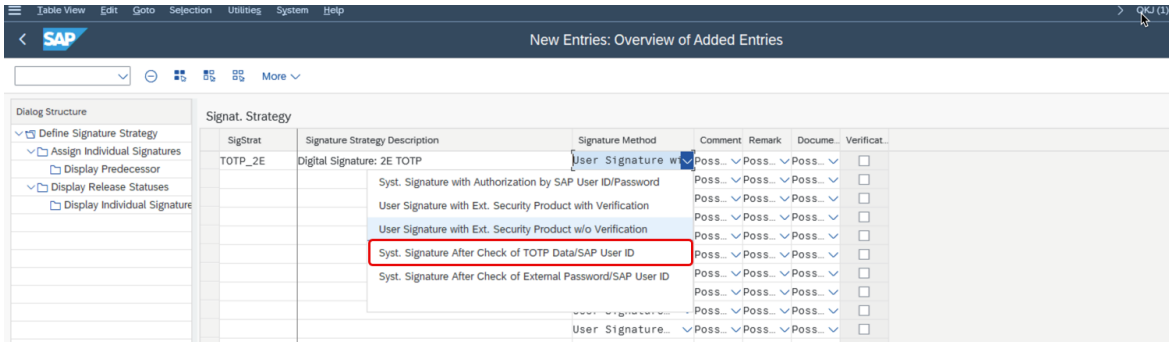
1. From the SAP Easy Access Menu, navigate to transaction *ELSIG01*. This is where you specify a new authorization group for your strategy. Click the *New Entries* button and specify the following *AGrpDigSig*: *TOTP_2E* with the description: *DS: TOTP 2 Eyes*. Then click *Save*.



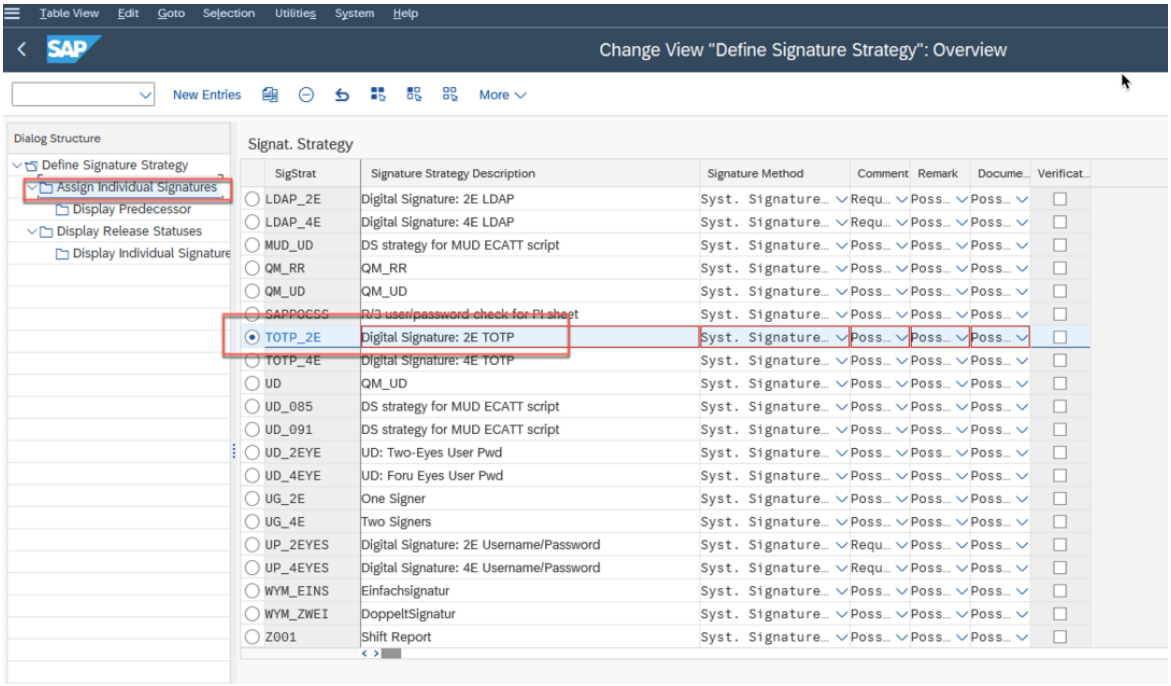
2. Navigate to transaction *ELSIG02* where you will specify the individual signature and bind it to the authorization group that was created in Step 1. Click the *New Entries* button and fill out the fields as follows: *Indiv. Sig*: *TOTP_SGR*, *AGrpDigSig*: *TOTP_2E*, description: *Signer for 2Eyes Signing Principle*. Click *Save*.



3. Navigate to transaction code *ELSIG00* to set up the new strategy with the individual signature created in Step 2.
    1. Click the *New Entries* button at the top of the screen and specify *SigStrat* as *TOTP_2E* and the dscription as: *Digital Signature: 2E TOTP*.
    2. Make sure that the following signature method is selected: *Syst. Signature After Check of TOTP Data/ SAP User ID*.
    3. Configure the *Comment*, *Remark* and *Document* according to your specifications (this configuration is customer-specific).
    4. Click *Save*.

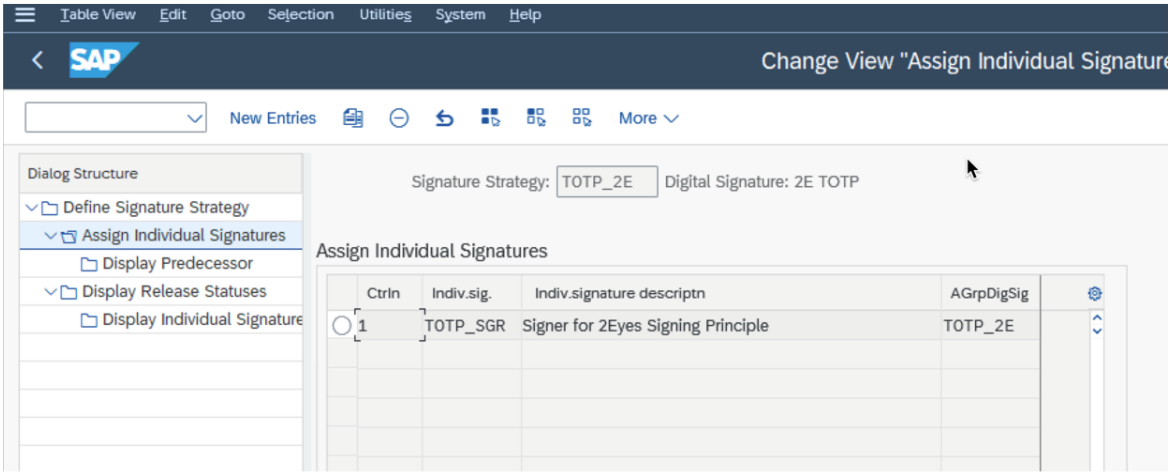


4. Go back to the overview where all of the strategies are listed in *ELSIG00* and select the newly created *TOTP_2E* strategy. In the *Dialog Structure* on the left, double click on *Assign Individual Signatures*.



5. Click the *New Entries* button and from the dropdown select the signer created above *TOTP_SGR*. Click *Save*.

> **Note**
>
> There are no predecessor or order of signatories because this strategy involves only the Technician signing their own work. SAP Service and Asset Manager **does not support** multiple signatory and signatory order from the mobile device.



Results

The TOTP_2E strategy is now correctly configured for SAP Service and Asset Manager and the digital signature will be able to use it to sign the work that the technician completes from the mobile client.

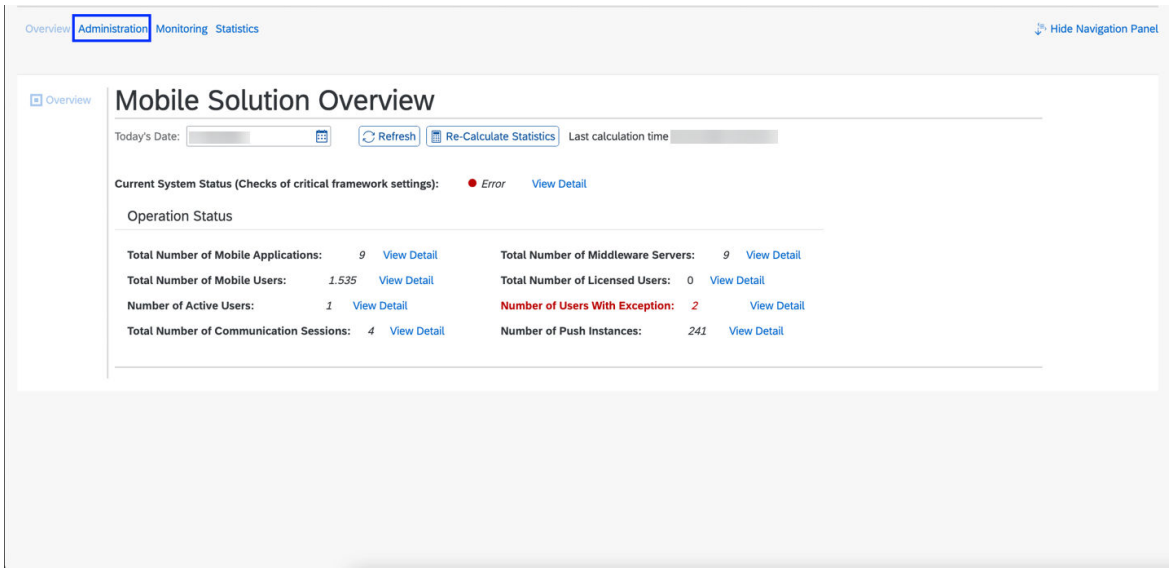
> **Note**
>
> For more information, see:
>
> - Digital Signature Overview [page 332]
> - Enabling Digital Signature [page 333]

4.13.3 Troubleshooting: Unable to Unregister the Device

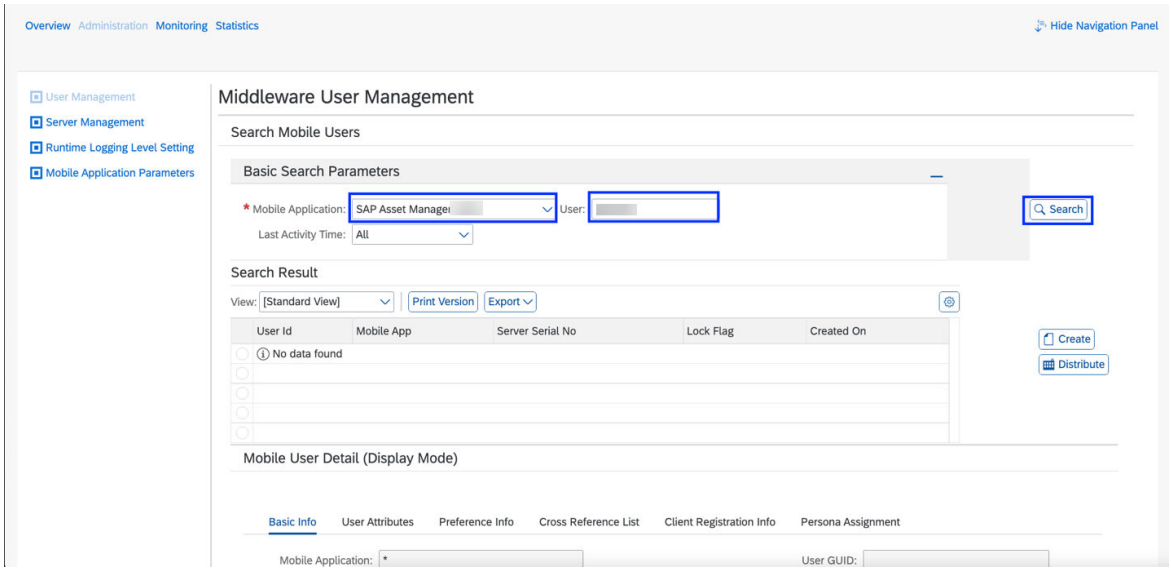
Procedure

1. Use transaction code *SU3* on the SAP GUI. Choose *TOTP Registration* from the menu options.

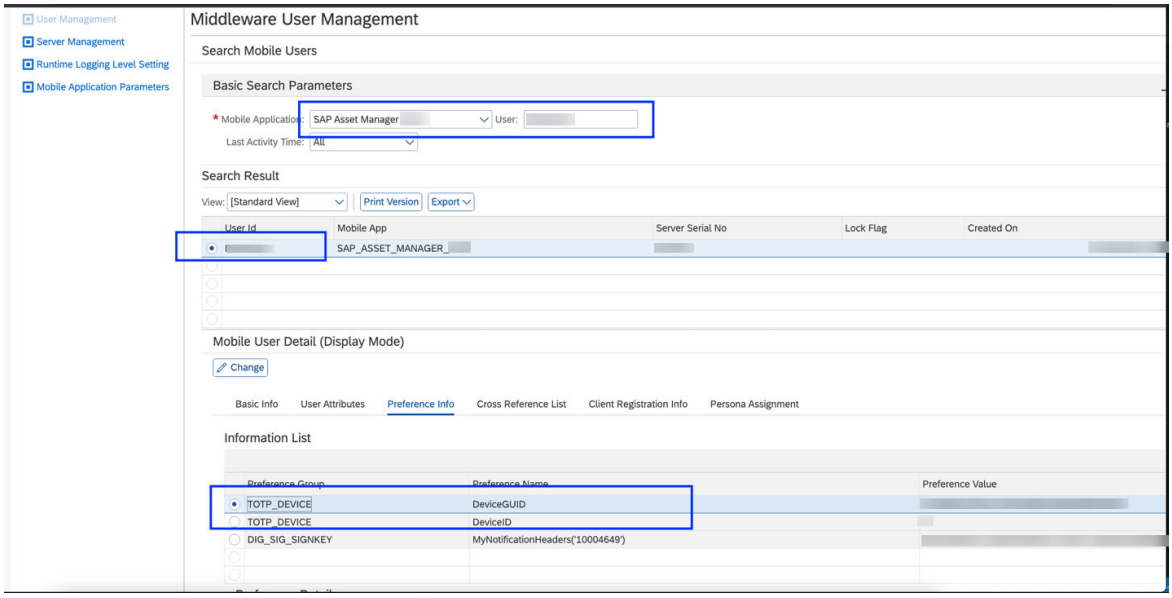
   The *Administration of TOTP Devices* window appears. The TOTP Devices table should contain a default entry. If the entry is missing, continue this procedure.
2. Open the Administration & Monitoring Portal through the transaction code */n/SYCLO/ADMIN*. Select the *Administration* tab.



3. Select the *User Management* tab. Provide the `<Mobile Application>` and `<User>` as search input. Click *Search*.



4. Select the appropriate entry from the *Search Result* section. Click the *Preference Info* tab.



5. Delete both *TOTP_DEVICE*-related entries.
6. Open your authenticator app. Delete the old token, then restart the registration process for the device.

4.14 Defense and Security Features Configuration

SAP Service and Asset Manager supports the following features for the Defense and Security industry:

- Flight order
- Support defense-related properties in Materials
  - NATO Stock Number (NSN)

    - Manufacturer Part Number (MPN)
    - Long Manufacturer Part Number (LMPN)
- Condition codes
- Master and critical equipment
- Additional defense and security fields on supply docs and material master
- Support edge mobile services

> **Note**
>
> - For more information about using Defense and Security features, see Working with Defense and Security Features.
> - For more information about the Defense Forces & Public Security (DFPS) component, refer to Defense Forces & Public Security in SAP S/4HANA documentation.

Supported Personas

This feature is applicable for the following personas:

Maintenance Technician (Pro)

Limitations

Please note that SAP Service and Asset Manager Defense and Security features are available only from SAP S/4HANA 2023 FPS3.

Configuration

To enable Defense integration, you need to activate the corresponding BC set for SAP Service and Asset Manager while performing MAIF installation steps:

1. Refer to Installing the MAIF document in *MAIF Installation Guide* for the complete set of installation steps and configuration.
2. When performing the step *Activate the relevant BC (Business Configuration) set for your application.* in Required Configuration - Enabling MAIF, make sure you activate BC Set for Defense: `MDFS_SAP_SRV_ASSET_MGR_2511_REF` (see Application BC Sets).

4.15 EAM Phase Model Configuration - Overview

The EAM Phase Model feature is called *EAM_PHASE_MODEL*.

> **Note**
>
> As of the SAP Service and Asset Manager 2205 release, enable and disable parameters are no longer available through the *Parameters* tab. You enable or disable all features through the *Features* tab. See the Configuring Features [page 93] procedure for details.

Follow one of the following configuration steps to configure the scenario according to the backend order type and notification type configuration, that is, whether the phase model has been enabled for all, some, or none at all.

> **Note**
>
> Notifications with a phase model and non-phase model notifications can be pulled together in SAP Service and Asset Manager, but in this case, only transitions for non-phase model notifications are supported on the device due to the limitations of the core feature.

1. Non-Phase Model Configuration
   If no phase model is active in the backend for any maintenance order types, configure SAP Service and Asset Manager for non-phase model orders by following the steps described in the Non-Phase Model Configuration [page 342] section and the related topics.
2. Phase Model Configuration
   If the backend system is configured so that all types of maintenance orders are enabled for the phase model, use the SAP Service and Asset Manager configuration steps described in the Phase Model Configuration [page 359] section and the related topics.
3. Phase Model + Non-Phase Model Configuration
   If you have multiple types of maintenance orders activated in your backend system for the phase model, and for some you use the traditional approach, follow the SAP Service and Asset Manager configuration steps described in the Phase Model + Non-Phase Model Configuration [page 381] section and the related topics.

4.15.1 Non-Phase Model Configuration

If no phase model is active in the backend for any maintenance order and notification types, configure SAP Service and Asset Manager for non-phase model orders by following the steps described in the topics within the Non-Phase Model Configuration [page 342] section.

> **Note**
>
> The following configuration will pull all non-phase model notifications. And the following status transitions will be available on the device for non-phase model notifications.
>
> *NOTIFICATION:RECEIVED* > *NOTIFICATION:STARTED*
>
> *NOTIFICATION:STARTED* > *NOTIFICATION:COMPLETED*

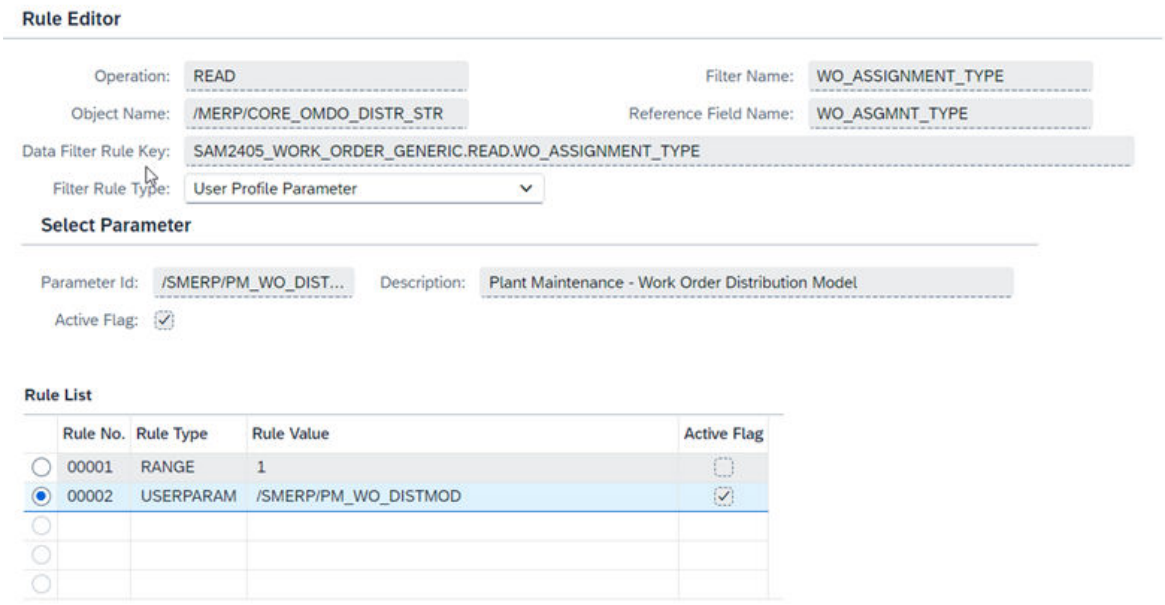
4.15.1.1 Work Order oMDO Configuration

Context

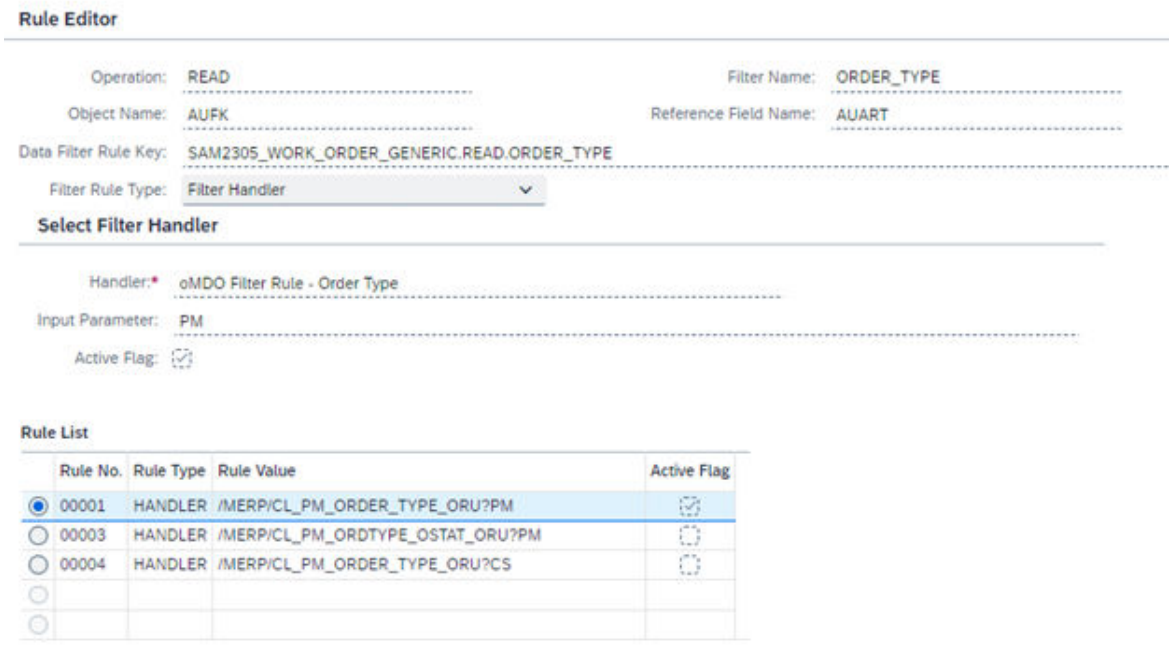
- On the *ConfigPanel* home page, select *OData Mobile Data Object Configuration*. Make sure you select the correct mobile application in the *Mobile Application Filter* field at the top of the page.
- From the *OData Mobile Data Object* list, select *SAMXXXX_WORK_ORDER_GENERIC*, and then select the *Data Filter* tab
- Expand the *Defined Filters* list as follows; *Operation - READ* > *Data Distribution* and select the filters shown in the screenshots below. Click the *Change* button.

Procedure

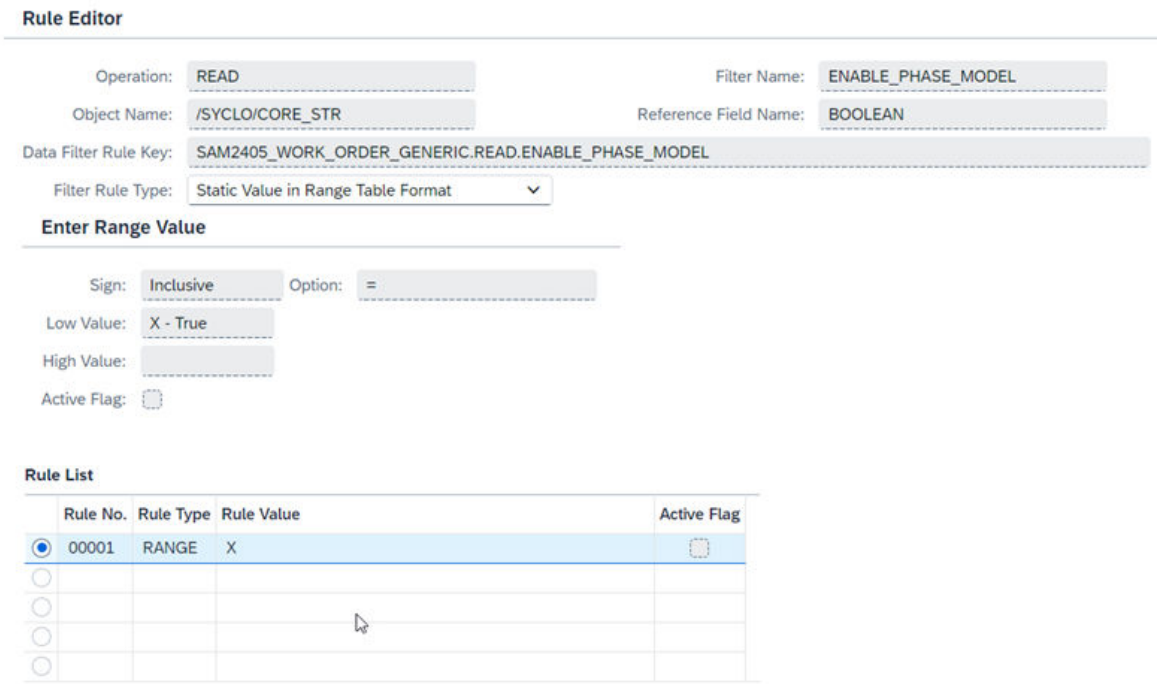
1. Maintain assignment type filter *WO_ASSIGNMENT_TYPE* with any of the static assignment types you need or with the custom parameter `/SMERP/PM_WO_DISTMOD`.



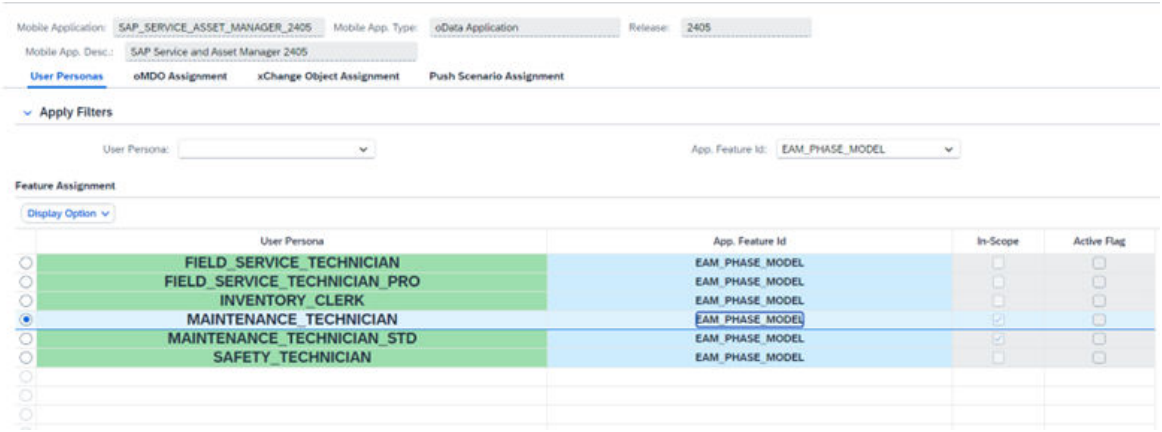
2. In the *ORDER_TYPE* filter, set the filter handler */MERP/CL_PM_ORDER_TYPE_ORU?PM* to the active state.



3. Disable the values of the *ENABLE_PHASE_MODEL* filter.

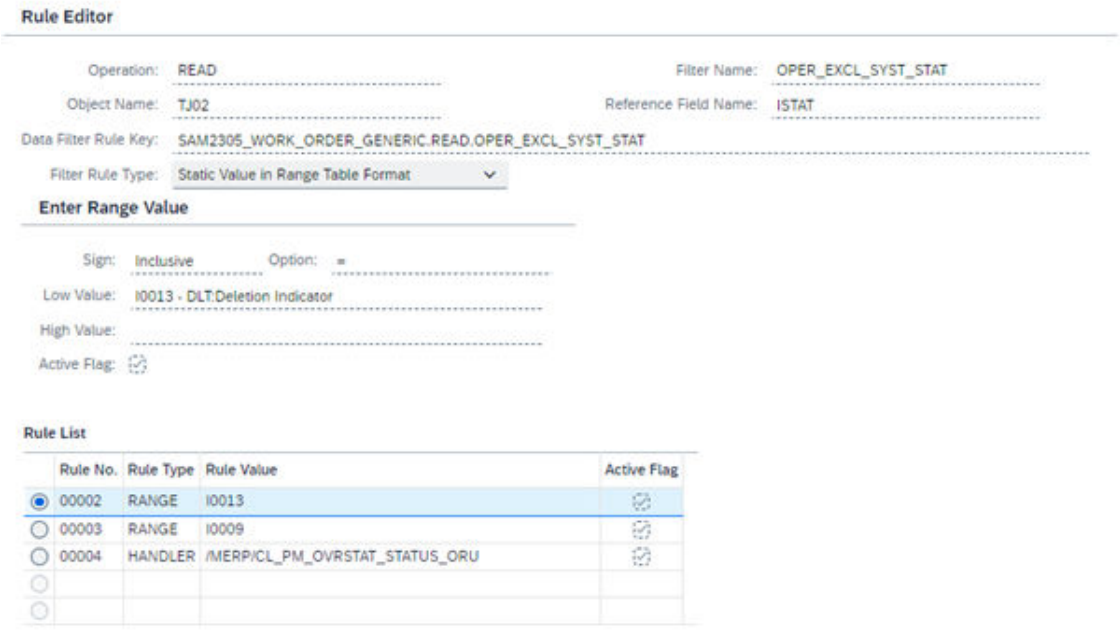


Deactivate the features in the *Component Assignments* section of the configuration for the Maintenance Technician persona.



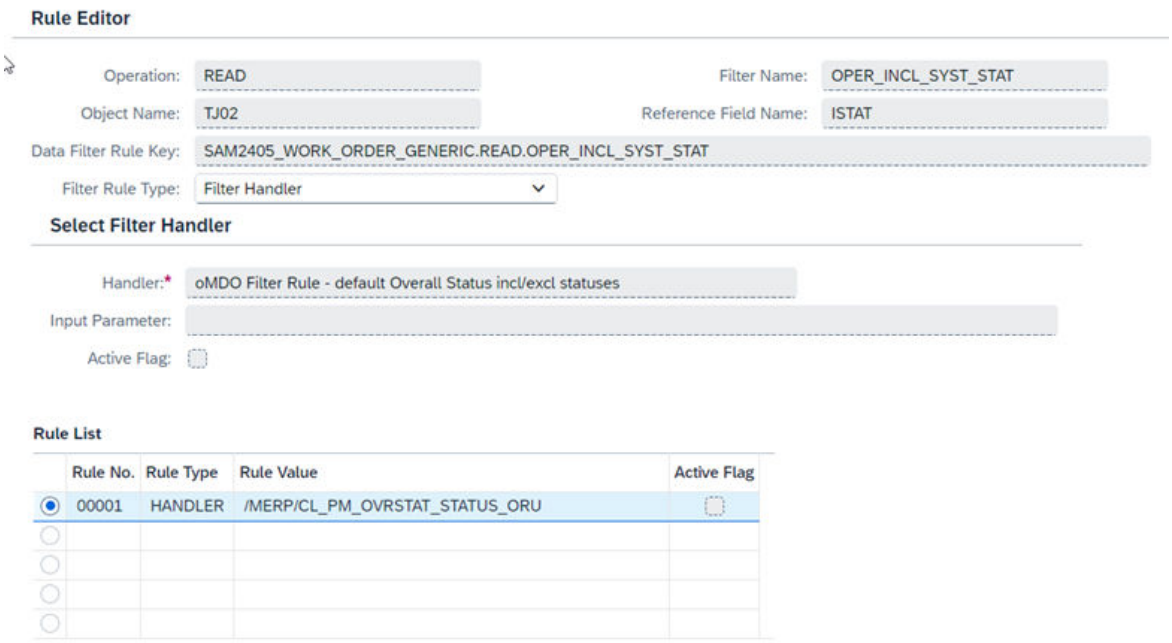
4. Make sure that filter handler */MERP/CL_PM_OVRSTAT_STATUS_ORU* is active in the *OPER_EXCL_SYST_STAT* filter.

> ### Note
>
> If the default statuses defined in filter handler don't fulfill your business scenario, you can manually add the system statuses individually to the filter.

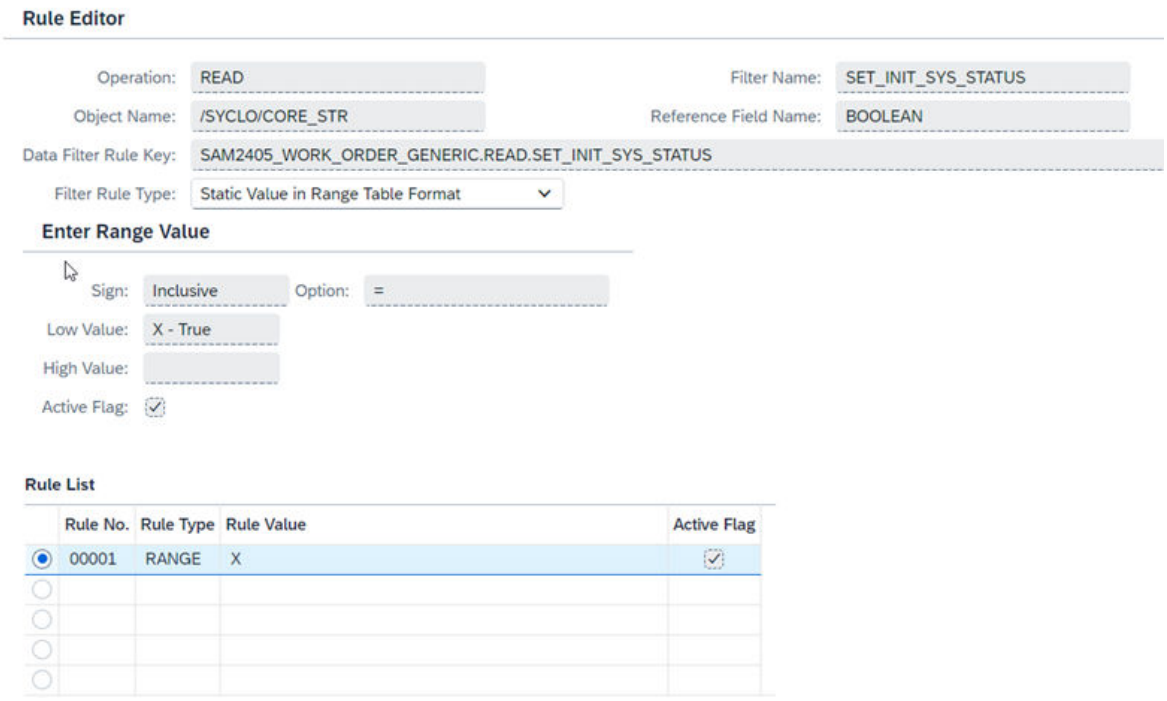


5. Disable the */MERP/CL_PM_OVRSTAT_STATUS_ORU* filter handler in *OPER_INCL_SYST_STAT* filter.

> ### Note
>
> If the default statuses defined in filter handler don't fulfill your business scenario, you can manually add the system statuses individually to the filter.

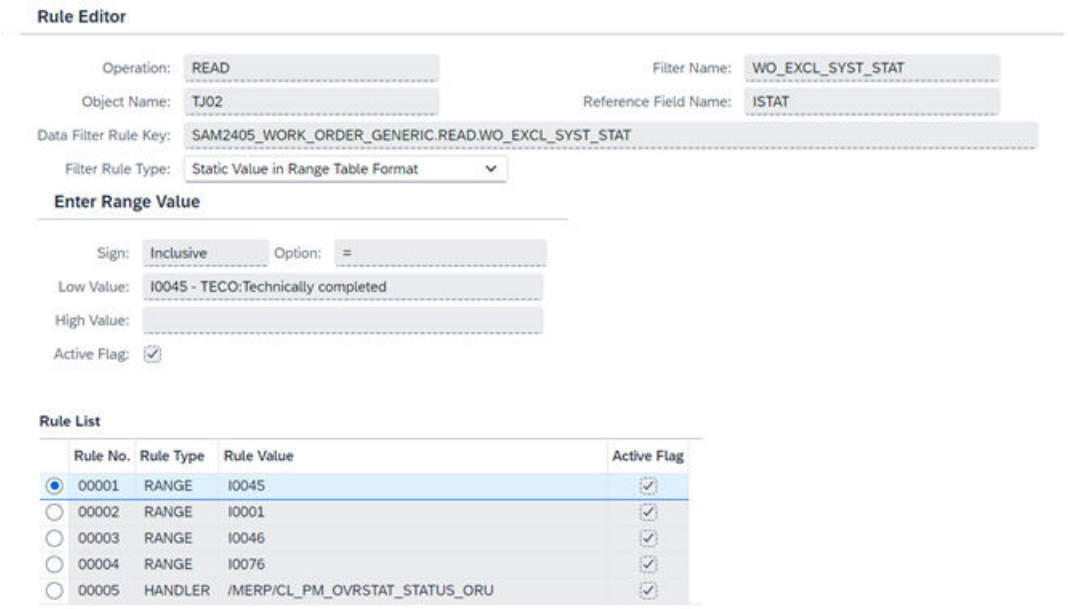


6. Set *SET_INIT_SYS_STATUS* filter to active. Initial mobile status will be determined for all orders.



7. Set the */MERP/CL_PM_OVRSTAT_STATUS_ORU* filter handler to active in the *WO_EXCL_SYST_STAT* filter.

   If the default statuses defined in filter handler don't fulfill your business scenario, you can manually add the system statuses individually to the filter.



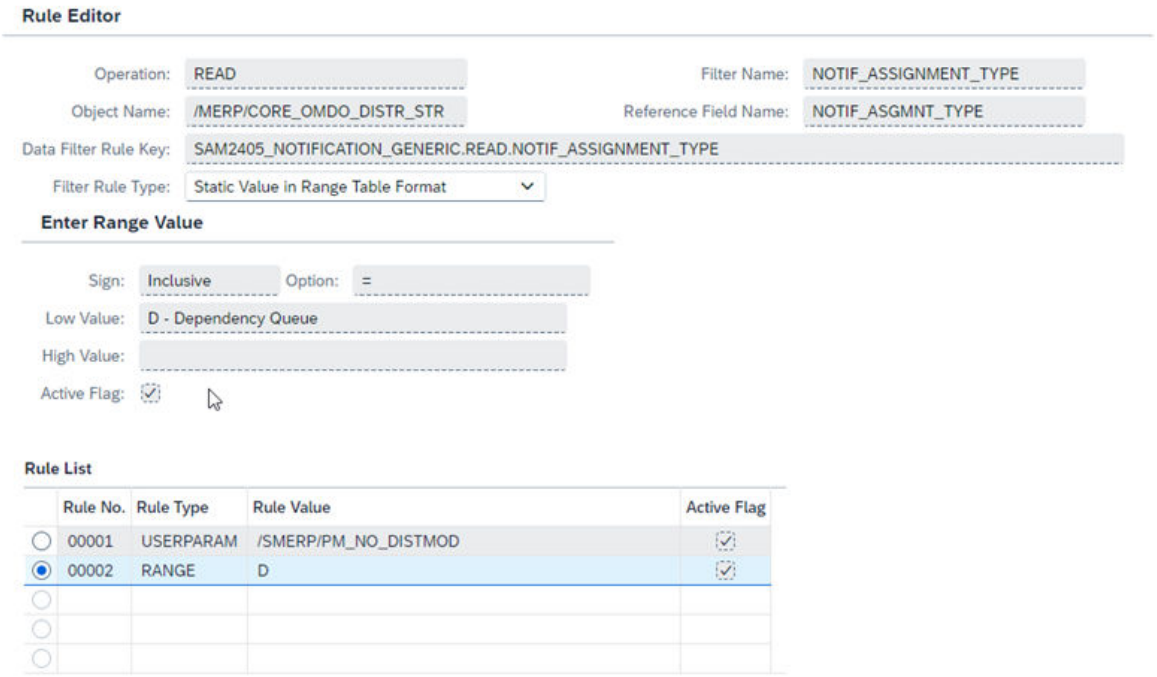
4.15.1.2 Notification Assignment Type Configuration

Configuring the Notification Assignment Type Filter

The following assignment types are supported:

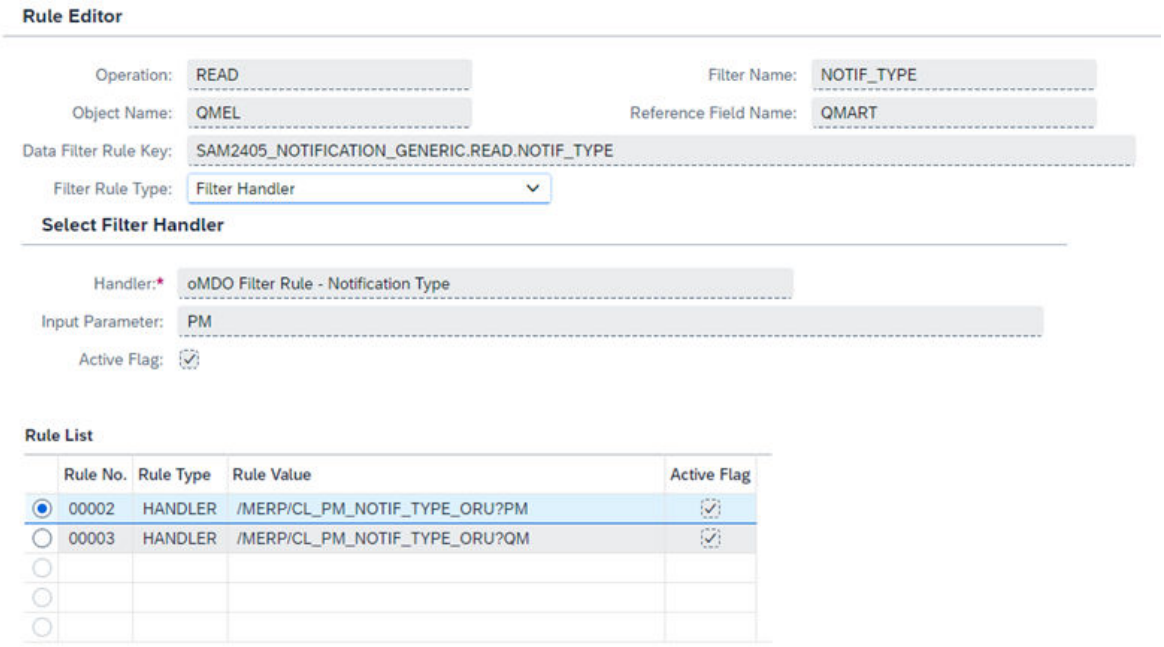
- 1: Header level person responsible
- 5: Header level work center
- D: Dependency queue

1. On the ConfigPanel home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. In the *OData Mobile Data Object List* select **SAMXXXX_NOTIFICATION_GENERIC**, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* *Data Distribution* and click *NOTIF_ASSIGNMENT_TYPE*. Click the *Change* button.
4. Set *Low Value* with the desired assignment type as defined by the assignment type model.
5. *Save* your changes.



Configuring the Notification Type Filter

1. On the ConfigPanel home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. In the *OData Mobile Data Object List* select **SAMXXXX_NOTIFICATION_GENERIC**, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* > *Data Distribution* > and click *NOTIF_TYPE*. Click the *Change* button.
4. Set the */MERP/CL_PM_NOTIF_TYPE_ORU?PM* and */MERP/CL_PM_NOTIF_TYPE_ORU?CS* filter handlers to *Active*. The notification types returned wil be non-phase model related.
5. *Save* your changes.

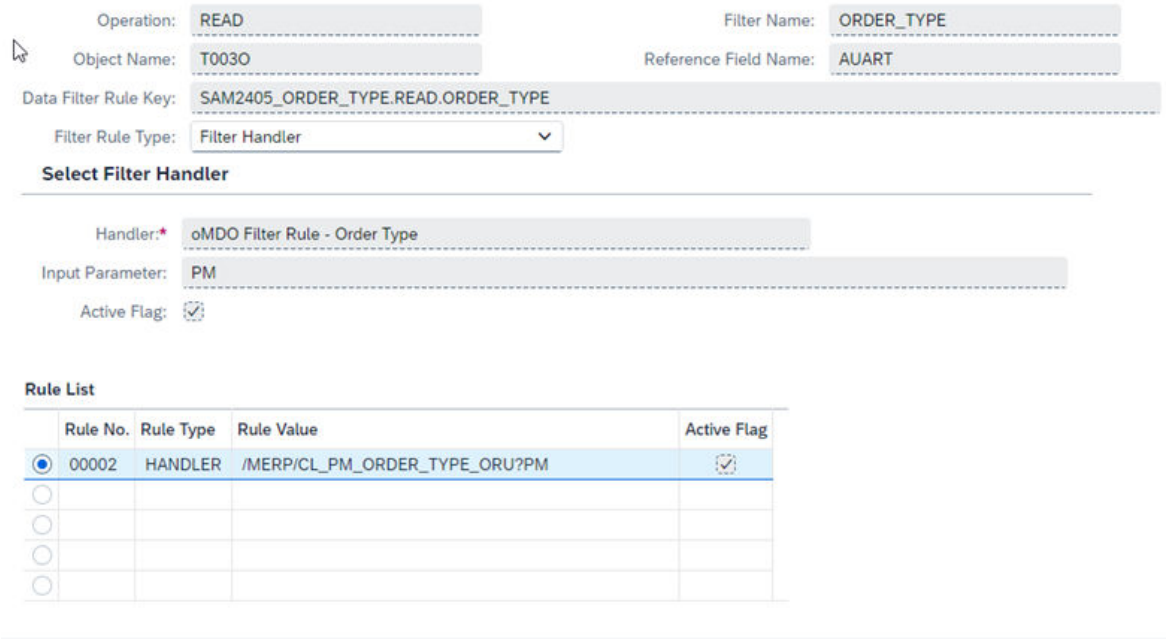


4.15.1.3 Order Type oMDO Configuration

Context

Procedure

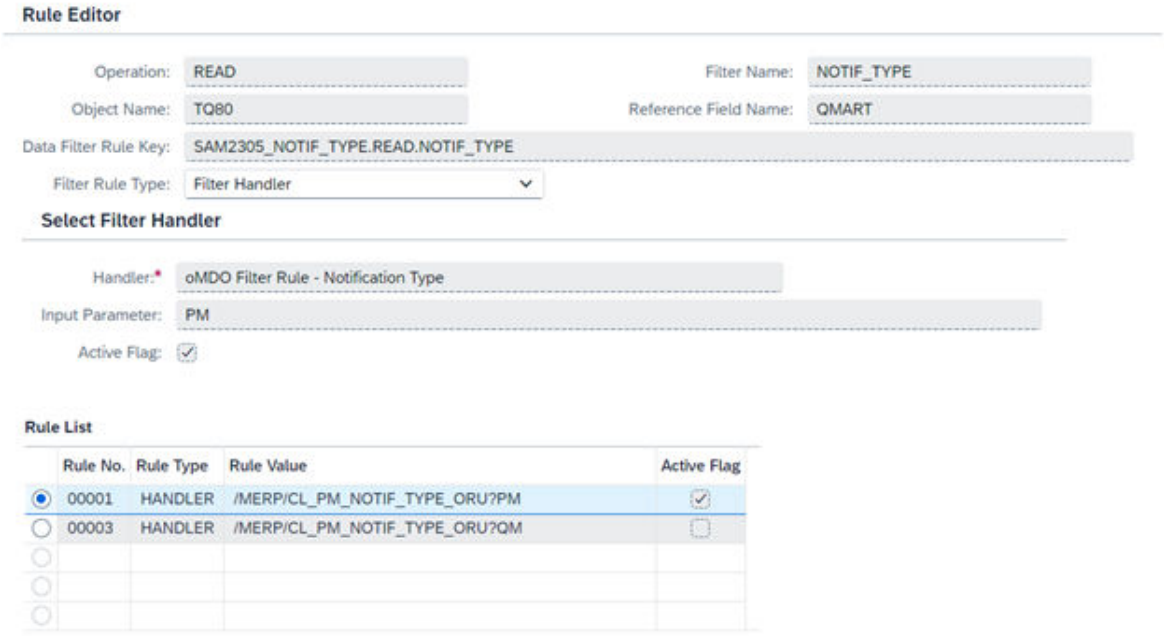
1. On the *ConfigPanel* home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. In the *OData Mobile Data Object* list select SAMXXXX_ORDER_TYPE, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* > *Standard Filter* and click *ORDER_TYPE*. Click the *Change* button.
4. Set the */MERP/CL_PM_ORDER_TYPE_ORU?PM* filter handler to active. All non-phase model relevant order types will be returned.
5. Save your changes.



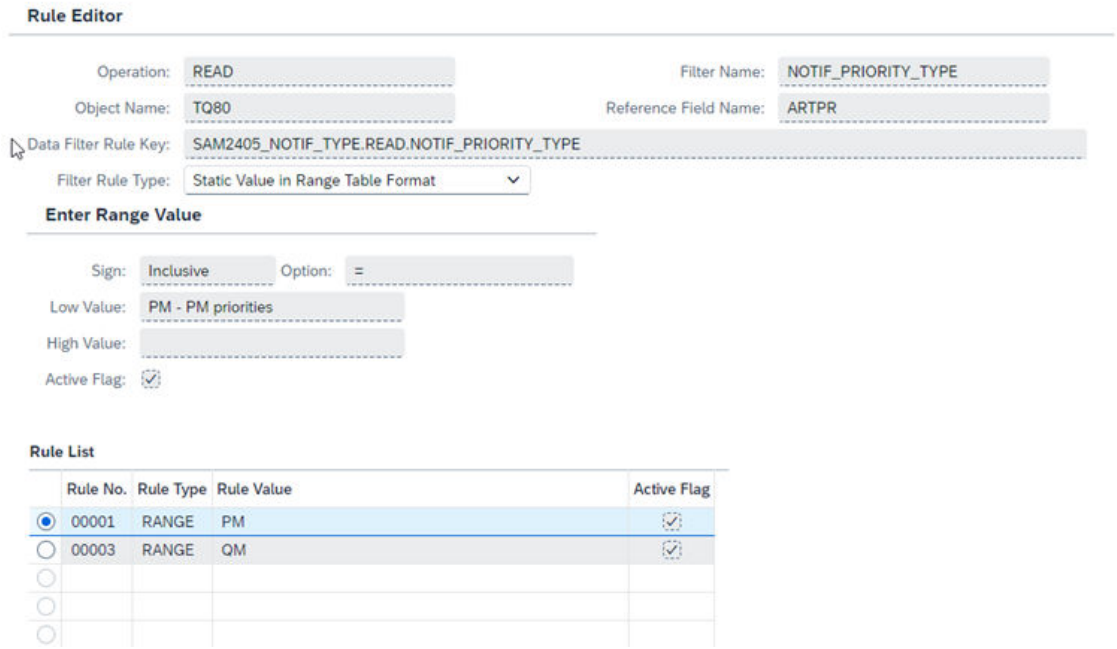
4.15.1.4 Notification Type oMDO Configuration

Procedure

1. On the *ConfigPanel* home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. In the *OData Mobile Data Object* list select SAMXXXX_NOTIF_TYPE, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* *Standard Filter* and click *NOTIF_TYPE*. Click the *Change* button.
4. Set the */MERP/CL_PM_NOTIF_TYPE_ORU?PM* and/or */MERP/CL_PM_NOTIF_TYPE_ORU?QM* and/or */MERP/CL_PM_NOTIF_TYPE_ORU?CS* filter handlers to active.



5. Configure additional priority type values if the notification uses a priority type other than PM in the *NOTIF_PRIORITY_TYPE* filter.



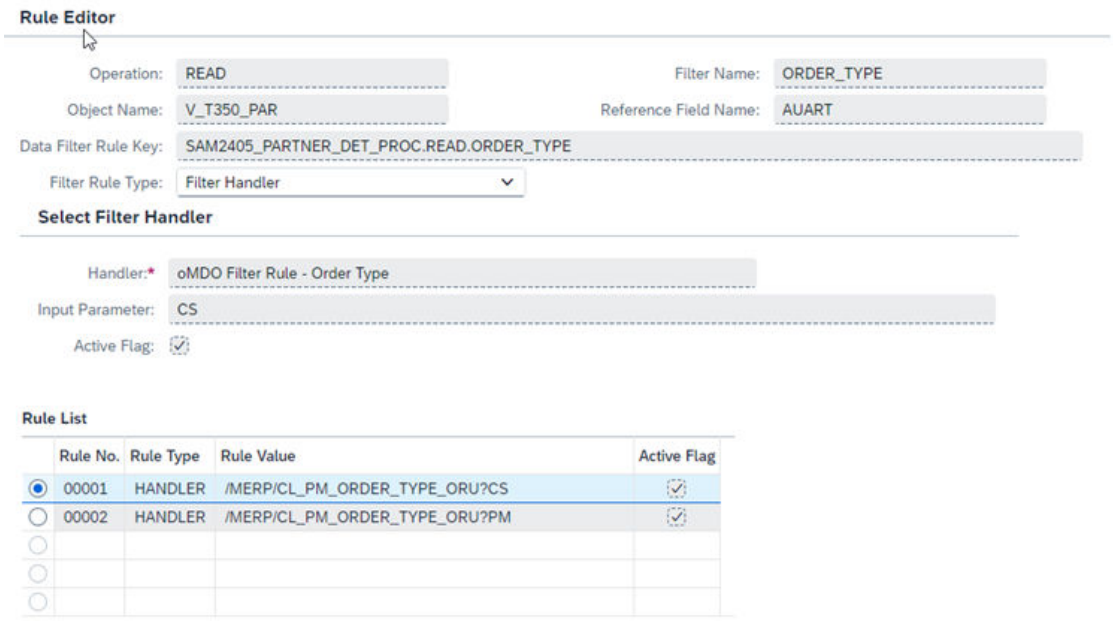
6. Save your changes.

4.15.1.5 Work Order Partner Determination Procedure oMDO Configuration

Context

Procedure

1. On the *ConfigPanel* home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. In the *OData Mobile Data Object* list select SAMXXXX_PARTNER_DET_PROC, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* > *Standard Filter* and click *ORDER_TYPE*. Click the *Change* button.
4. Set the */MERP/CL_PM_ORDER_TYPE_ORU?PM* and */MERP/CL_PM_ORDER_TYPE_ORU?CS* filter handlers to active.
5. Save your changes.

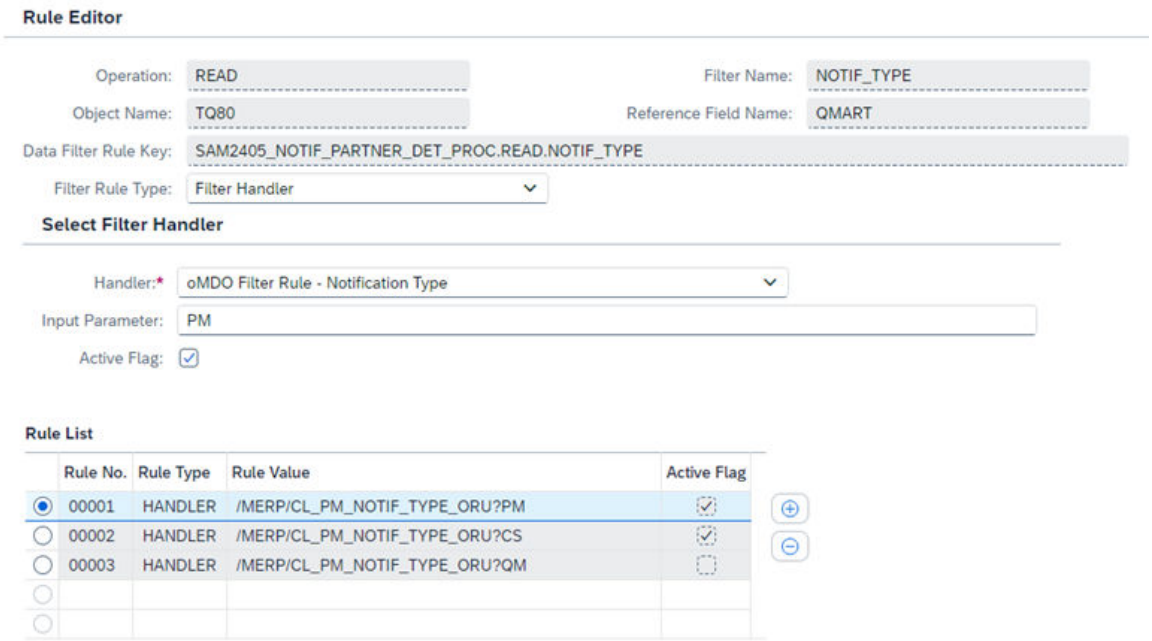


4.15.1.6 Notification Partner Determination oMDO Configuration

Context

Procedure

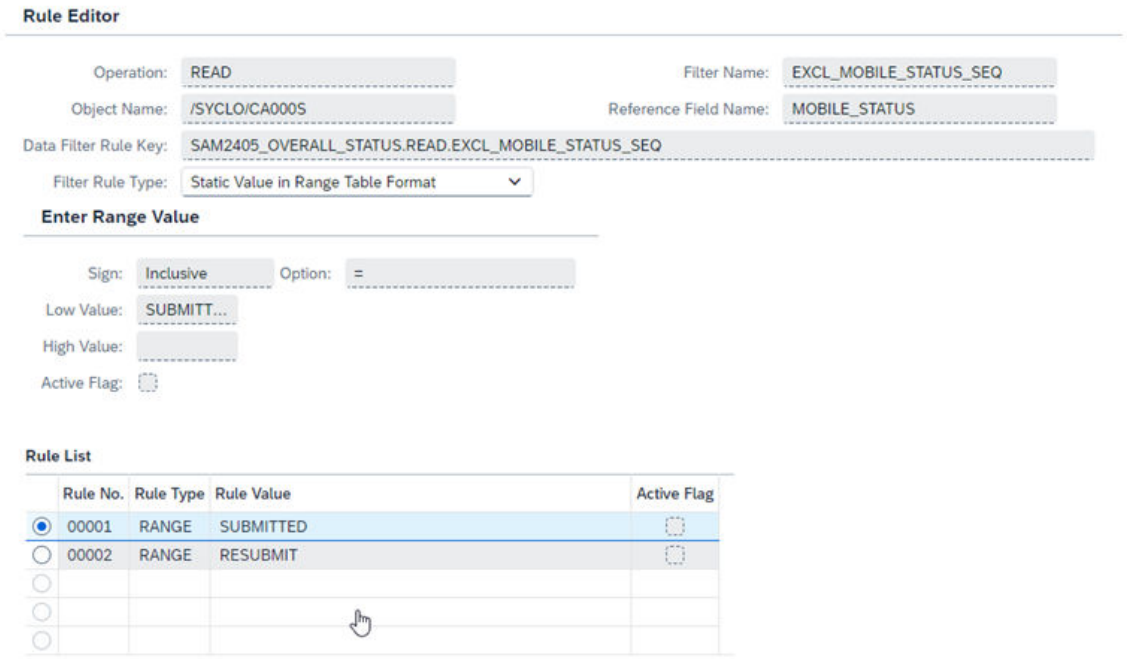
1. On the *ConfigPanel* home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. In the *OData Mobile Data Object* list select SAMXXXX_NOTIF_PARTNER_DET_PROC, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* > *Standard Filter* and click *NOTIF_TYPE*. Click the *Change* button.
4. Set the */MERP/CL_PM_NOTIF_TYPE_ORU?PM* and */MERP/CL_PM_NOTIF_TYPE_ORU?CS* filter handlers to active. If needed, set up other filter handlers according to your business requirements.
5. Save your changes.



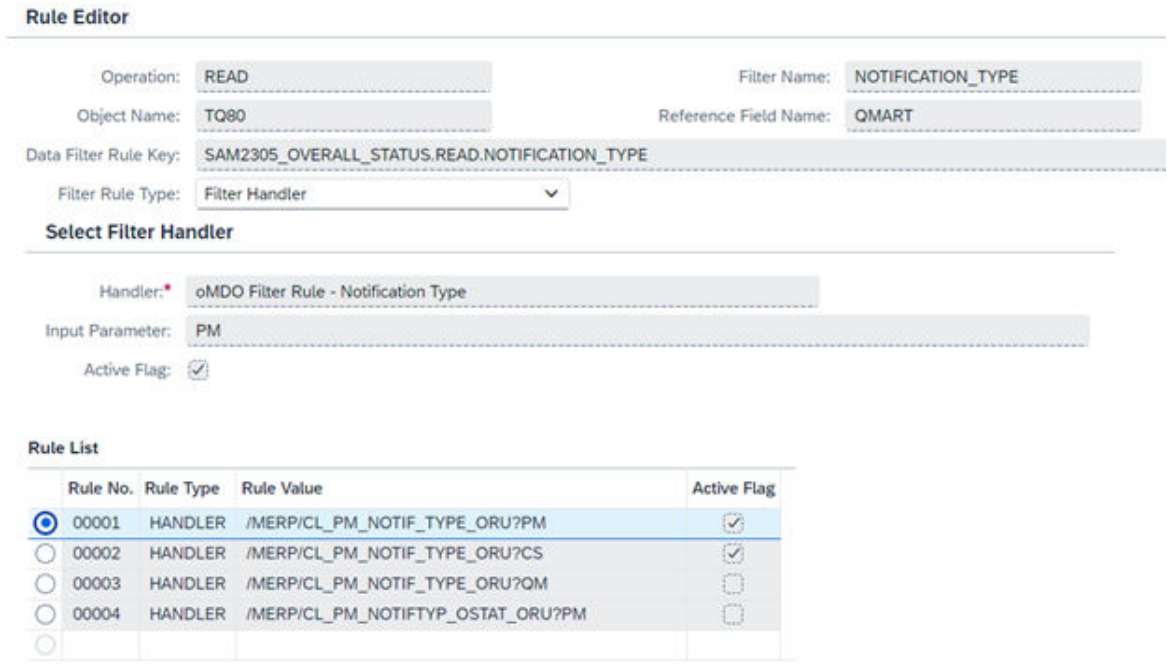
4.15.1.7 Overall Status oMDO Configuration

Procedure

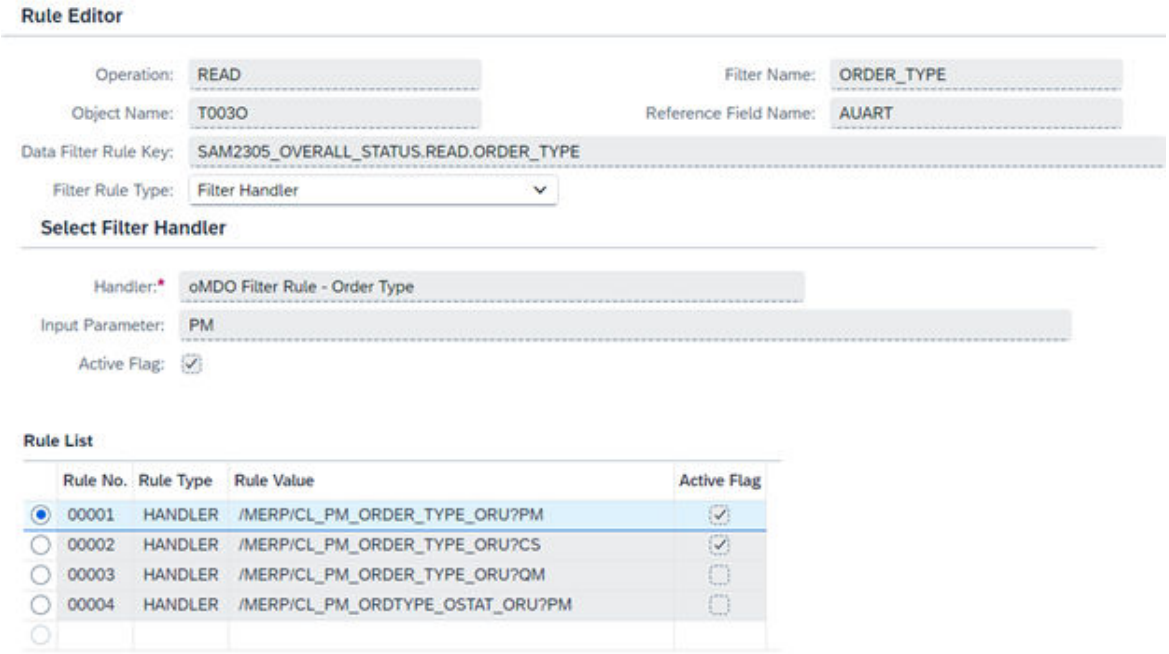
1. On the *ConfigPanel* home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. In the *OData Mobile Data Object* list select SAMXXXX_OVERALL_STATUS, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* *Standard Filter* and then click on the filters described in the steps below. Click the *Change* button.
4. Use *EXCL_MOBILE_STATUS_SEQ* filter to disable certain phase model status transitions on your mobile client. Disable if any filter specific to the phase model has been set.



5. *NOTIFICATION TYPE*: Set the */MERP/CL_PM_NOTIF_TYPE_ORU?PM* and/or */MERP/CL_PM_NOTIF_TYPE_ORU?CS* filter handlers to active.



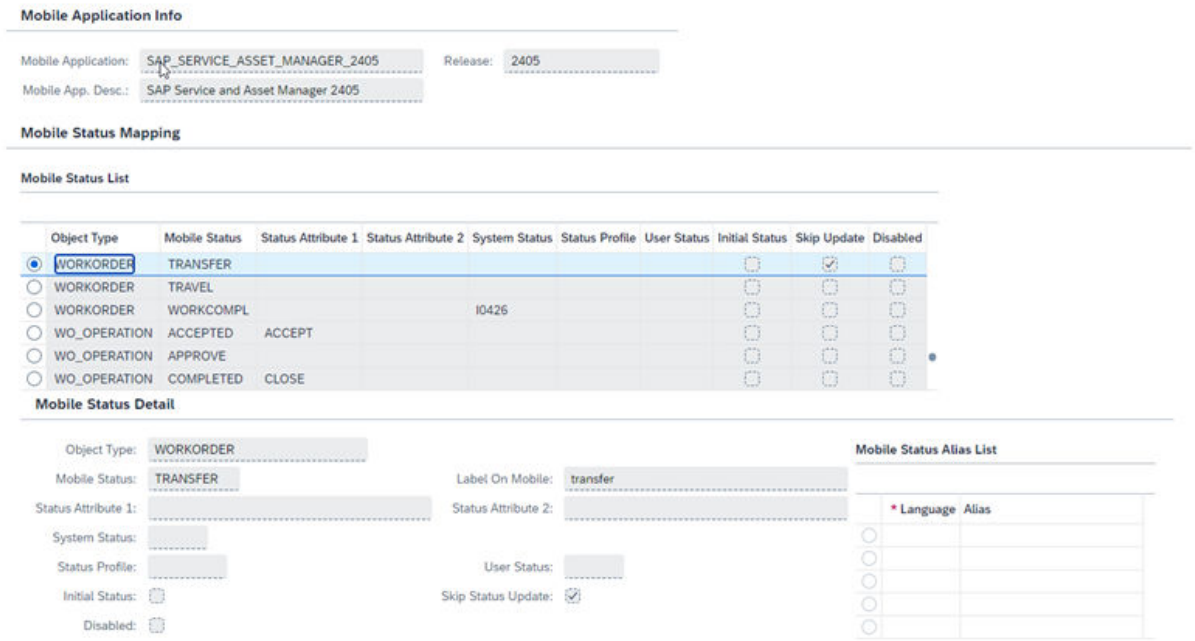
6. *ORDER_TYPE*: Set the */MERP/CL_PM_ORDER_TYPE_ORU?PM* and/or */MERP/CL_PM_ORDER_TYPE_ORU?CS* filter handlers to active.



4.15.1.8 Mobile Status Mapping Configuration

Mobile status mapping is still maintained in the configuration panel.

> **Note**
>
> In the out-of-the-box configuration, the statuses associated with the phase model will be active. They do not need to be disabled. Since the phase model feature is not active, these statuses and their associated transitions will not be available on the device.



The following mobile status display should be active for non-phase model orders and/or notifications. See the table below.

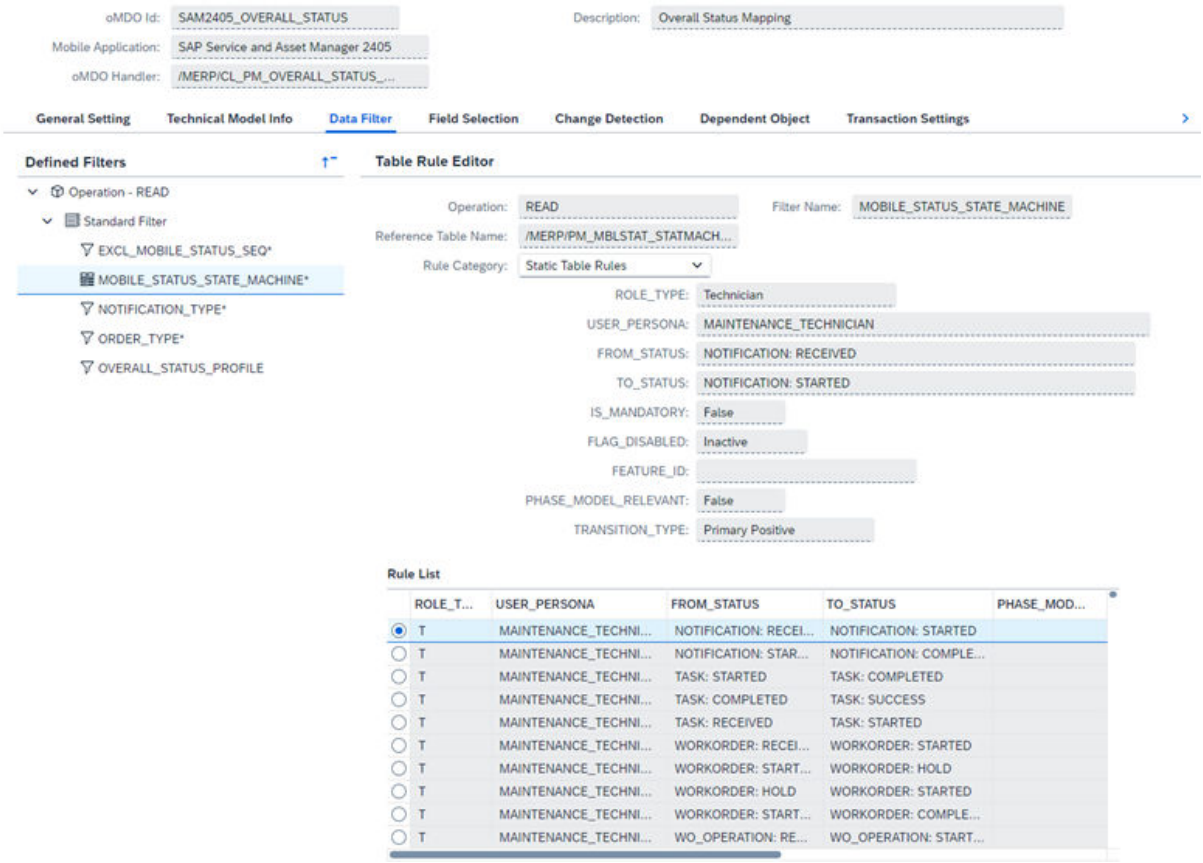
Mobile Status Mapping

Object Type	Mobile Status	Status Attribute 1	Status Attribute 2	System Status
NOTIFICATION	COMPLETED Status is used in both phase model ON and OFF scenarios			I0072
NOTIFICATION	POSTPONE			I0069
NOTIFICATION	RECEIVED			
NOTIFICATION	STARTED Status is used in both phase model ON and OFF scenarios			I0070
TASK	COMPLETED			I0156
TASK	RECEIVED			
TASK	STARTED			I0155

Object Type	Mobile Status	Status Attribute 1	Status Attribute 2	System Status
TASK	SUCCESS			I0157
WORKORDER	COMPLETED			I0045
WORKORDER	HOLD			
WORKORDER	RECEIVED			I0630
WORKORDER	REJECTED			
WORKORDER	REVIEW			
WORKORDER	STARTED			I0002
WORKORDER	TRANSFER			
WO_OPERATION	COMPLETED			
WO_OPERATION	HOLD			
WO_OPERATION	RECEIVED			
WO_OPERATION	REJECTED			
WO_OPERATION	REVIEW			
WO_OPERATION	STARTED			
WO_OPERATION	TRANSFER			

4.15.1.9 Mobile Status State Machine

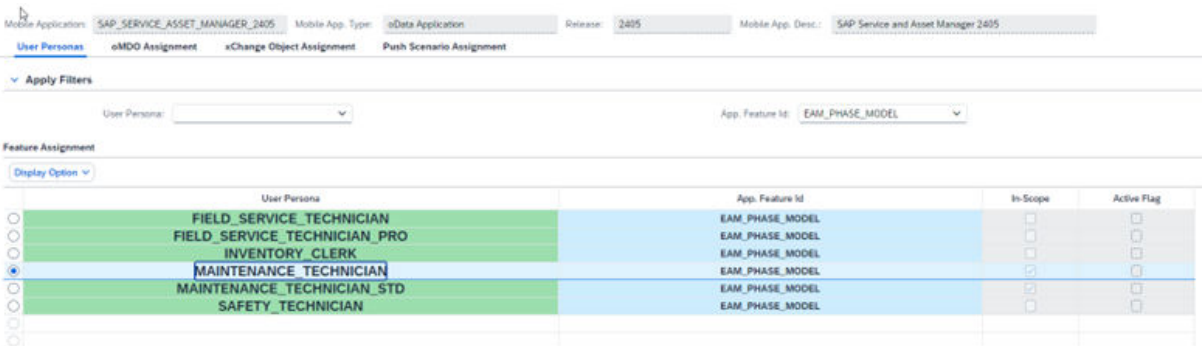
Mobile status state machine is added as filter in *Overall Status oMDO* (SAM2405_OVERALL_STATUS). This configuration allows us to configure all status transition on mobile client, given the mobile status is already maintained in the configuration of mobile status mapping.



> **Note**
>
> Transitions that are active in this state machine are available on the device. Even if transitions related to the phase model are still active; as the phase model function is not active, they will not be available on the device, so they can be left alone.

4.15.1.10 Persona and Feature Enablement

If the phase model is not active in the backend, make sure that the next persona and feature assignment for *EAM_PHASE_MODEL* is not active. By default, the next assignment is inactive.



4.15.2 Phase Model Configuration

If the backend system is set up so that all maintenance order types and notification types are enabled for the phase model, configure SAP Service and Asset Manager by following the steps described in the topics within the Phase Model Configuration [page 359] section.

> **Note**
>
> The following configuration will pull all phase model notifications. And the following status transitions will be available on the device for phase model notifications.
>
> *NOTIFICATION:ACTIONREQ* > *NOTIFICATION:SUBMITTED*

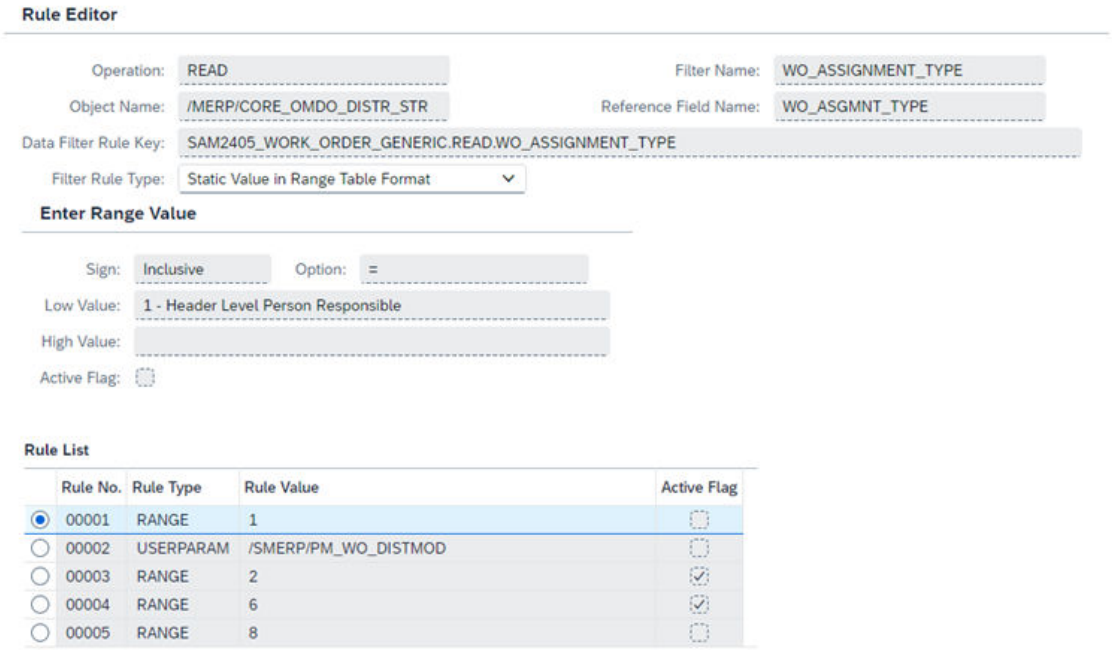
4.15.2.1 Work Order oMDO Configuration

Context

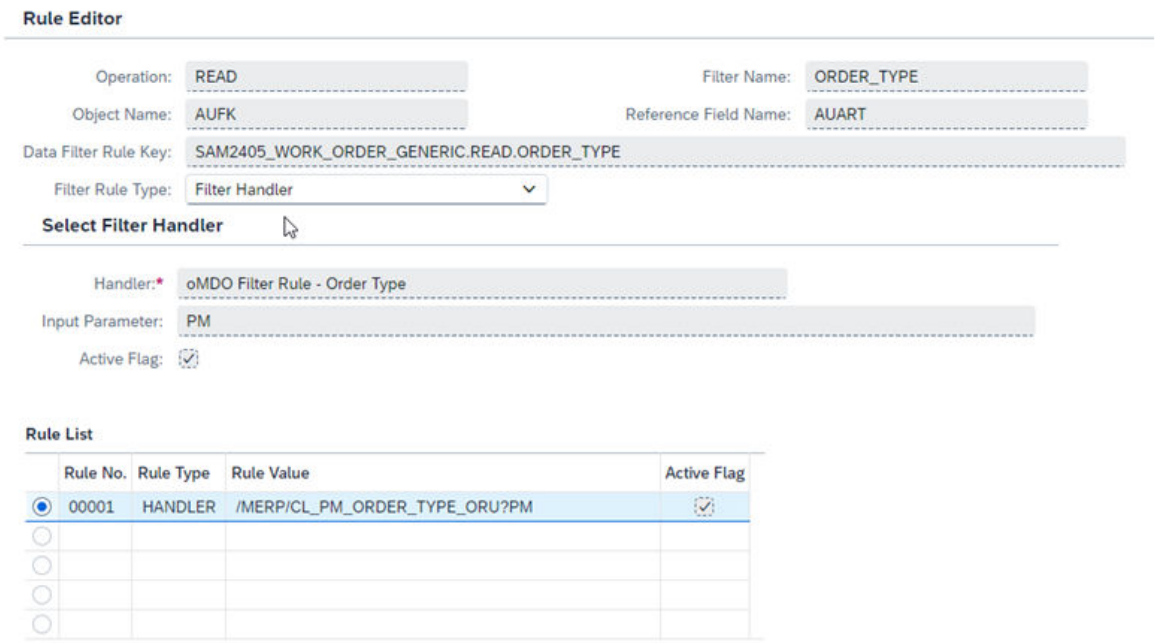
- On the *ConfigPanel* home page, select *OData Mobile Data Object Configuration*. Make sure you select the correct mobile application in the *Mobile Application Filter* field at the top of the page.
- From the *OData Mobile Data Object* list, select *SAMXXXX_WORK_ORDER_GENERIC*, and then select the *Data Filter* tab
- Expand the *Defined Filters* list as follows; *Operation - READ* > *Data Distribution* and select the filters shown in the screenshots below. Click the *Change* button.

Procedure

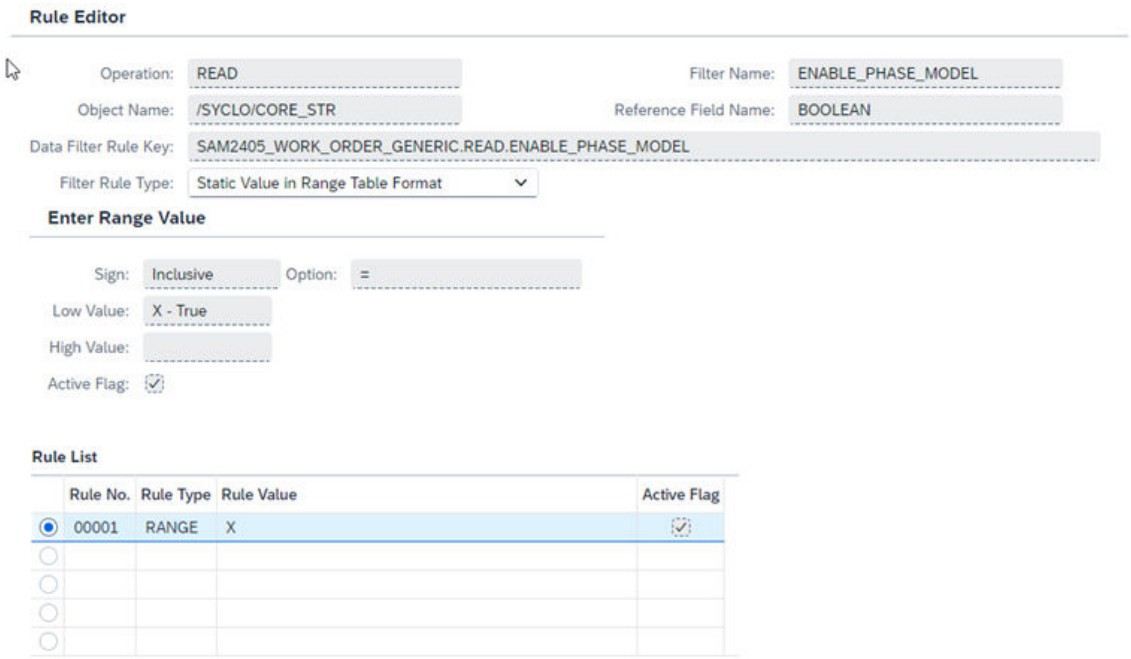
1. Maintain assignment type filter *WO_ASSIGNMENT_TYPE* with the following assignment types shown below.



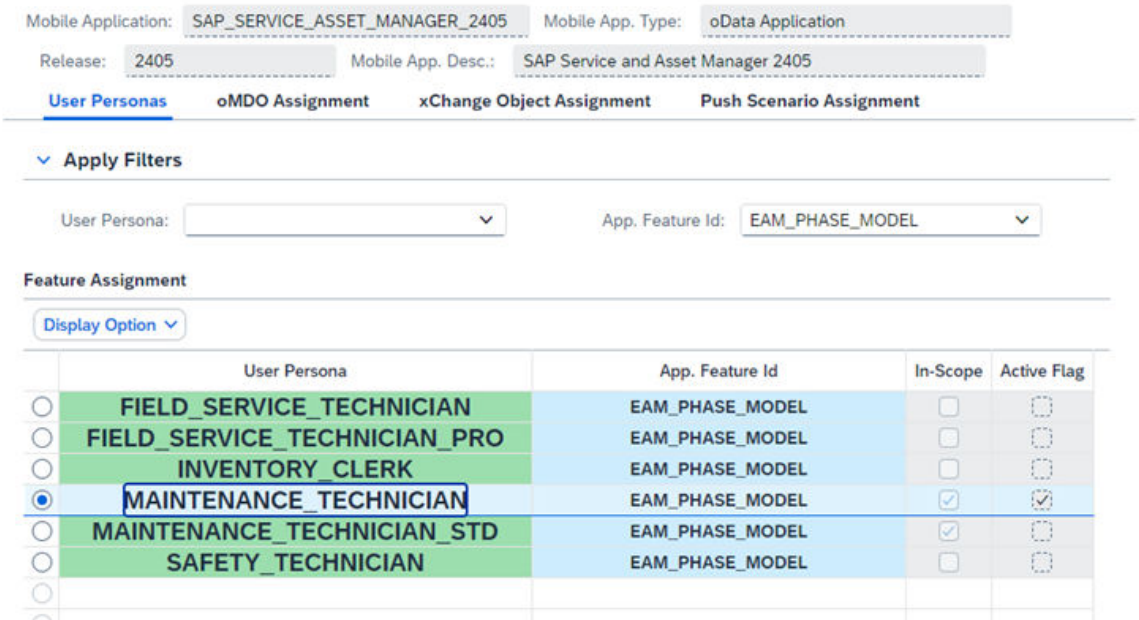
2. In the *ORDER_TYPE* filter, set the filter handler */MERP/CL_PM_ORDER_TYPE_ORU?PM* to the active state, which returns order types that have been assigned a common status profile and those that have not.



3. Set the *ENABLE_PHASE_MODEL* filter to active in the standard filter section.

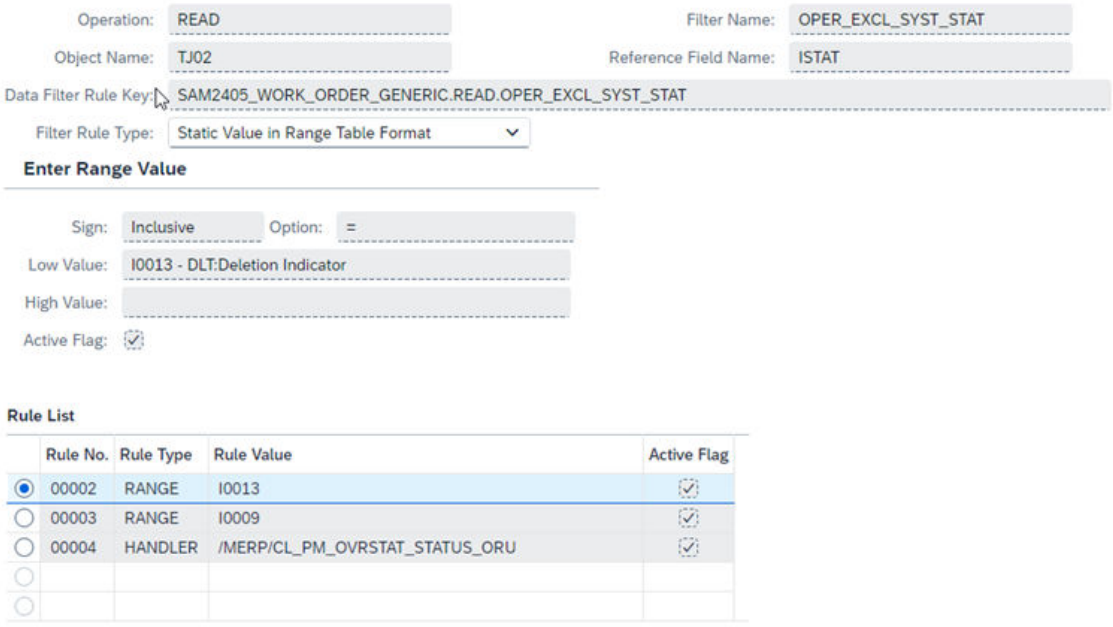


Activate the features in the *Component Assignments* section of the configuration for the Maintenance Technician persona.



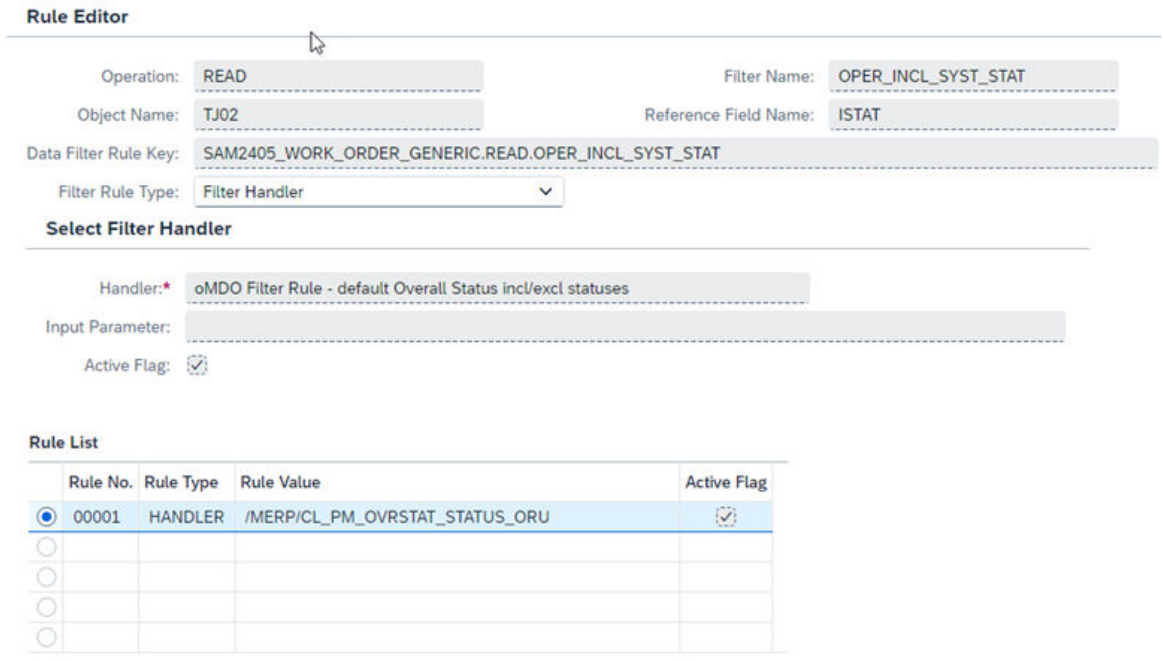
4. Make sure that filter handler */MERP/CL_PM_OVRSTAT_STATUS_ORU* is active, which by default enters the *IEAM5 (ORSC - Ready for Scheduling)* and *I0820 (JBFI - Job Finished)* system statuses into the *OPER_EXCL_SYST_STAT* filter.

> **Note**
>
> If the default statuses defined in filter handler don't fulfill your business scenario, you can manually add the system statuses individually to the filter.

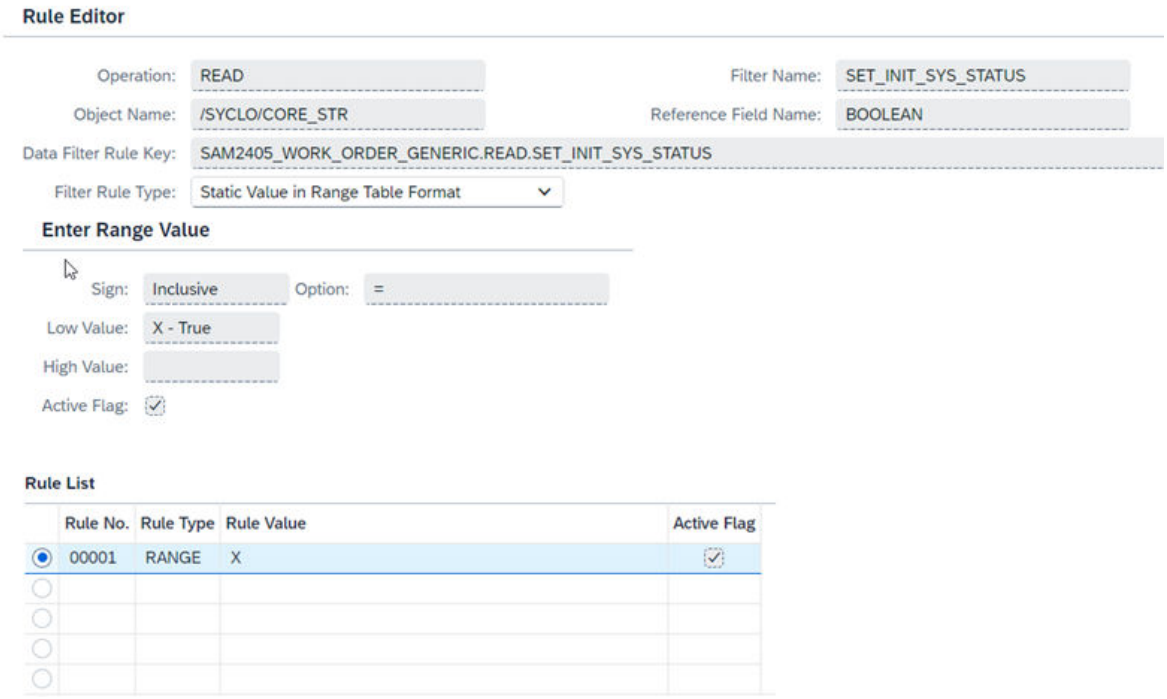


5. Make sure that the */MERP/CL_PM_OVRSTAT_STATUS_ORU* filter handler is active, which by default enters the *I0117 (DSPT - Scheduled)*, *I0809 (JIPR – Job In Process)*, and *I0010 (PCNF – Partially Confirmed)* system statuses into the *OPER_INCL_SYST_STAT* filter.

> ### Note
>
> If the default statuses defined in filter handler don't fulfill your business scenario, you can manually add the system statuses individually to the filter.

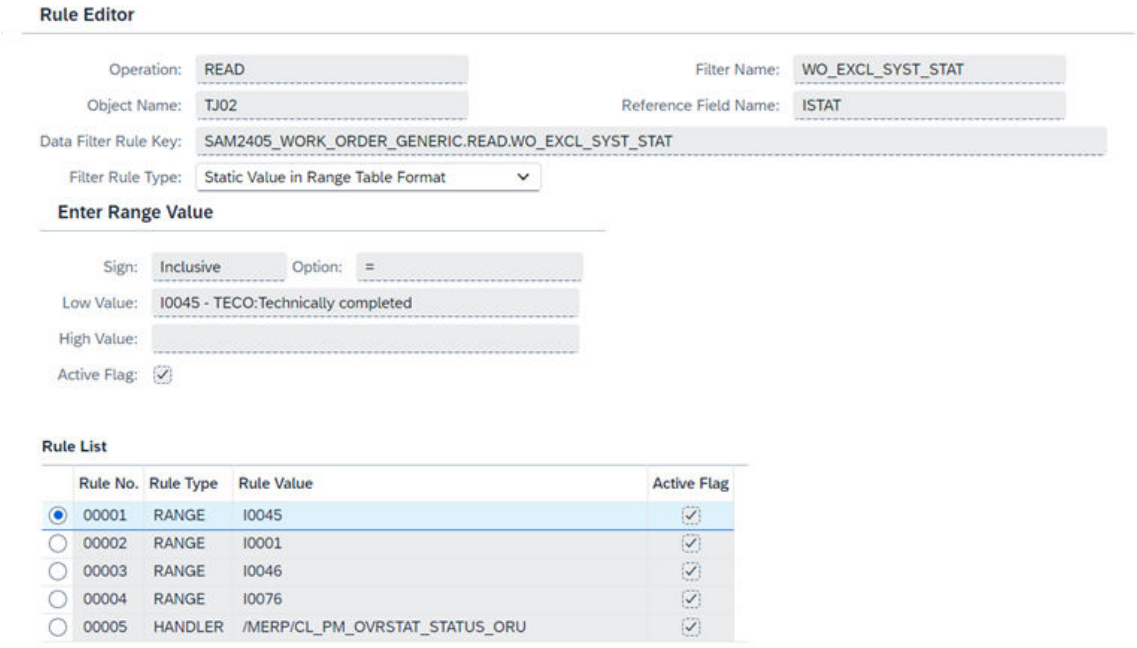


6. Set *SET_INIT_SYS_STATUS* filter to active. Initial mobile status will be determined for both overall status profile based orders and non-phase model related orders.



7. Set the */MERP/CL_PM_OVRSTAT_STATUS_ORU* filter handler to active, which by default enters the *IEAM6 (OMWC – Main Work Completed)* and *I0820 (JBFI – Job Finished)* system statuses into the *WO_EXCL_SYST_STAT* filter.

   If the default statuses defined in filter handler don't fulfill your business scenario, you can manually add the system statuses individually to the filter.



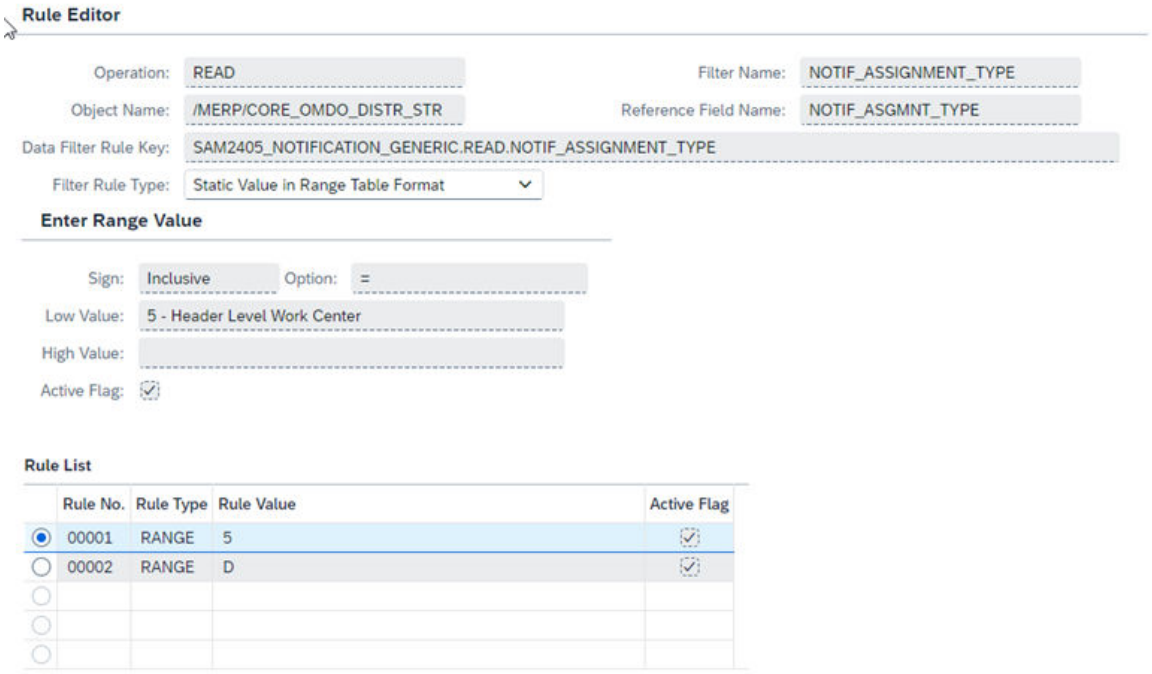
4.15.2.2 Notification Assignment Type Configuration

Configuring the Notification Assignment Type Filter

The following assignment types are supported:

- 1: Header level person responsible
- 5: Header level work center
- D: Dependency queue

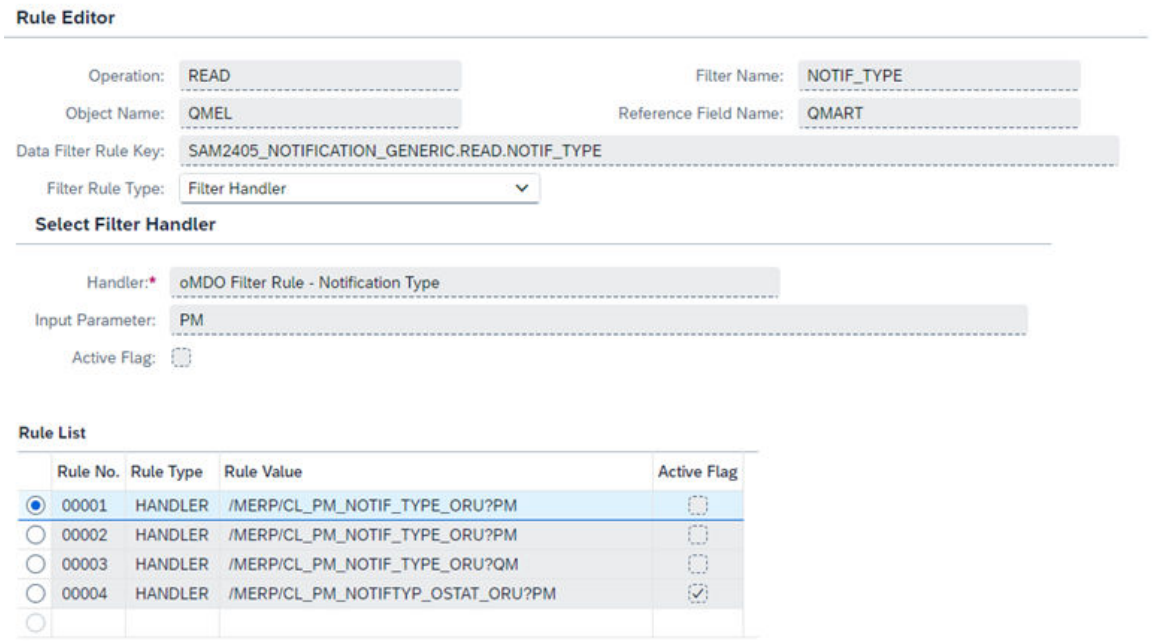
1. On the ConfigPanel home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. In the *OData Mobile Data Object List* select **SAMXXXX_NOTIFICATION_GENERIC**, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* *Data Distribution* and click *NOTIF_ASSIGNMENT_TYPE*. Click the *Change* button.
4. Set *Low Value* with the desired assignment type as defined by the assignment type model.
5. *Save* your changes.



Configuring the Notification Type Filter

1. On the ConfigPanel home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.

2. In the *OData Mobile Data Object List* select **SAMXXXX_NOTIFICATION_GENERIC**, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* > *Data Distribution* and click *NOTIF_TYPE*. Click the *Change* button.
4. Set the */MERP/CL_PM_NOTIFTYP_OSTAT_ORU?PM* filter handler to *Active*. This filter handler will return the notification types that have been assigned an overall status profile.
5. *Save* your changes.



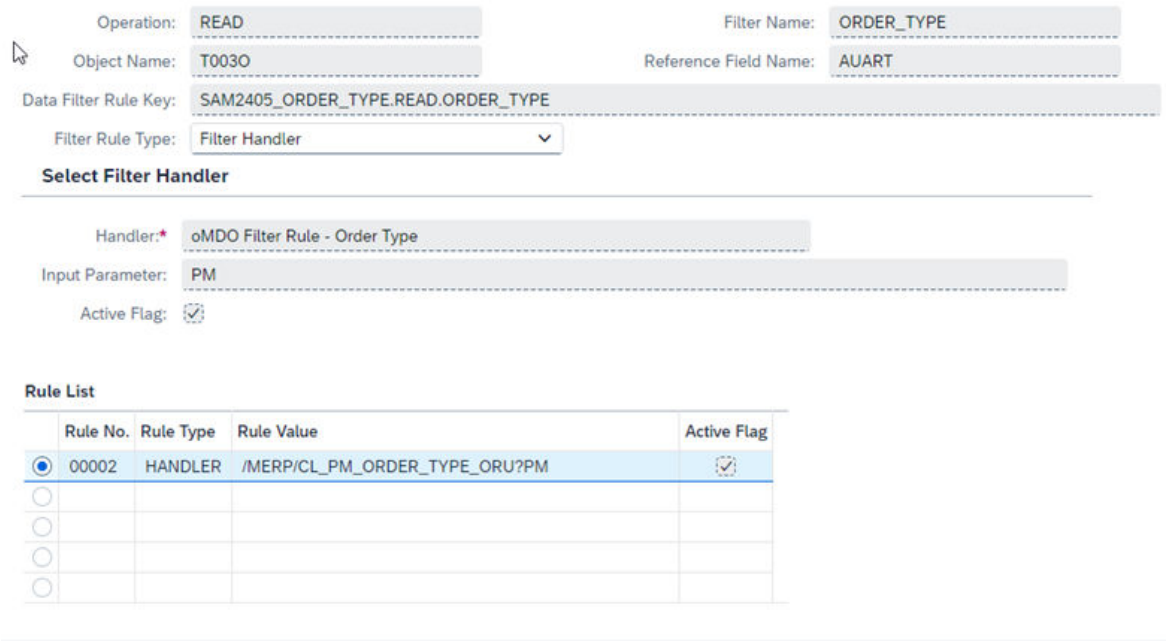
4.15.2.3 Order Type oMDO Configuration

Context

Procedure

1. On the *ConfigPanel* home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. In the *OData Mobile Data Object* list select SAMXXXX_ORDER_TYPE, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* > *Standard Filter* and click *ORDER_TYPE*. Click the *Change* button.

4. Set the */MERP/CL_PM_ORDER_TYPE_ORU?PM* filter handler to active, as it will return order types related to both phase and non-phase models.
5. Save your changes.



4.15.2.4 Notification Type Configuration (SPRO and oMDO Configuration)

This section describes the configuration required to ensure that notification types are fetched and displayed correctly in SAP Service and Asset Manager. The configuration includes both back end SPRO settings and the required OData Mobile Data Object (oMDO) configuration in the ConfigPanel.

Both backend SPRO configuration and MDO OData filtering must be aligned:

Area	Purpose
SPRO Notification Type Assignment	Ensures the notification type is valid and linked to the correct order type. Missing configuration prevents notifications from syncing to SSAM.
oMDO SAMXXXX_NOTIF_TYPE Filters	Ensures that only notification types with valid status profiles and priority categories are exposed to the mobile app.

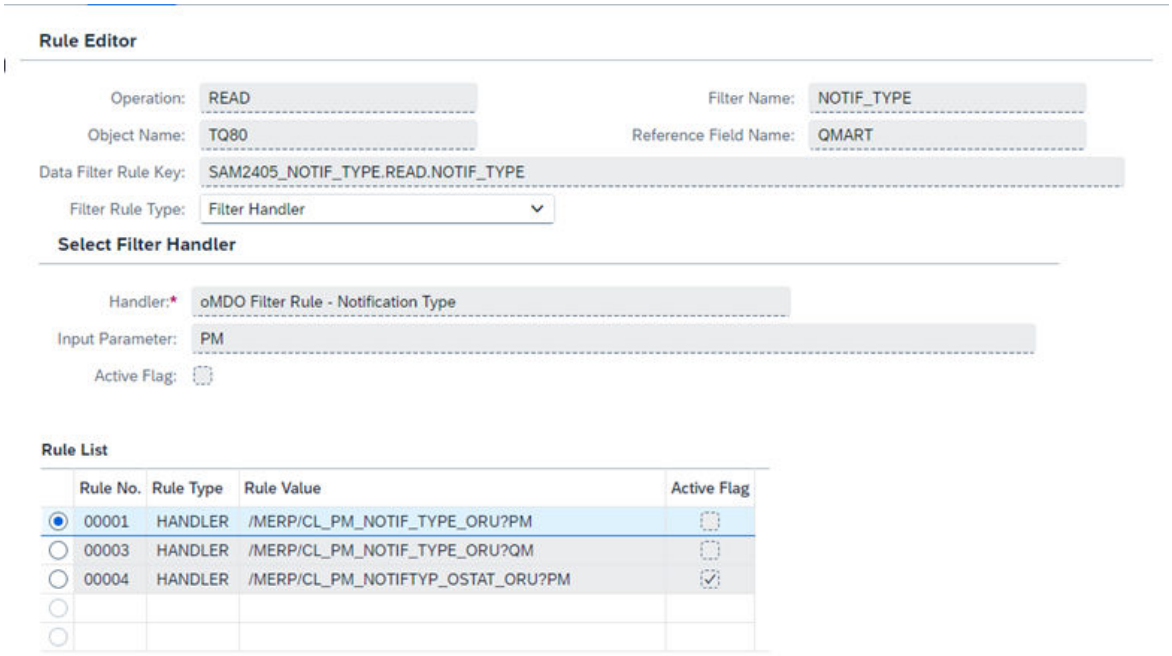
When both layers are configured properly, SSAM can successfully retrieve and display notifications of the desired notification types.

4.15.2.4.1 Notification Type oMDO Configuration

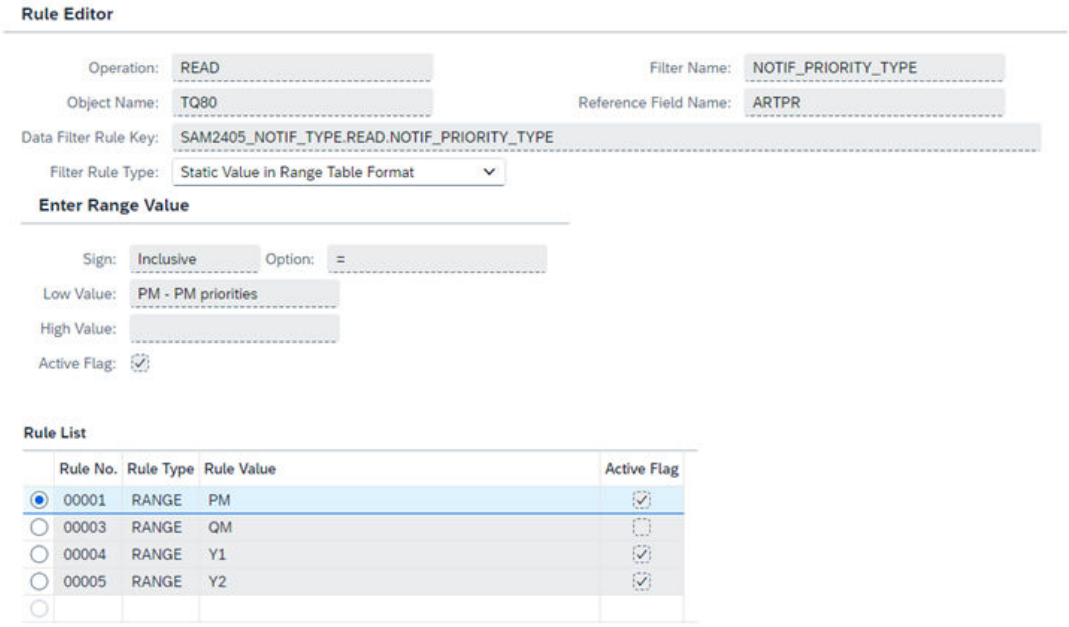
After you complete the back end customizing, configure the SAMXXXX_NOTIF_TYPE MDO so that SSAM retrieves the correct notification types based on filtering rules.

Procedure

1. On the *ConfigPanel* home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. In the *OData Mobile Data Object* list select SAMXXXX_NOTIF_TYPE, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* *Standard Filter* and click *NOTIF_TYPE*. Click the *Change* button.
4. Set the */MERP/CL_PM_NOTIFTYPE_OSTAT_ORU?PM* filter handler to active, which returns notification types that have been assigned an overall status profile



5. Configure additional priority type values if the notification uses a priority type other than PM in the *NOTIF_PRIORITY_TYPE* filter.



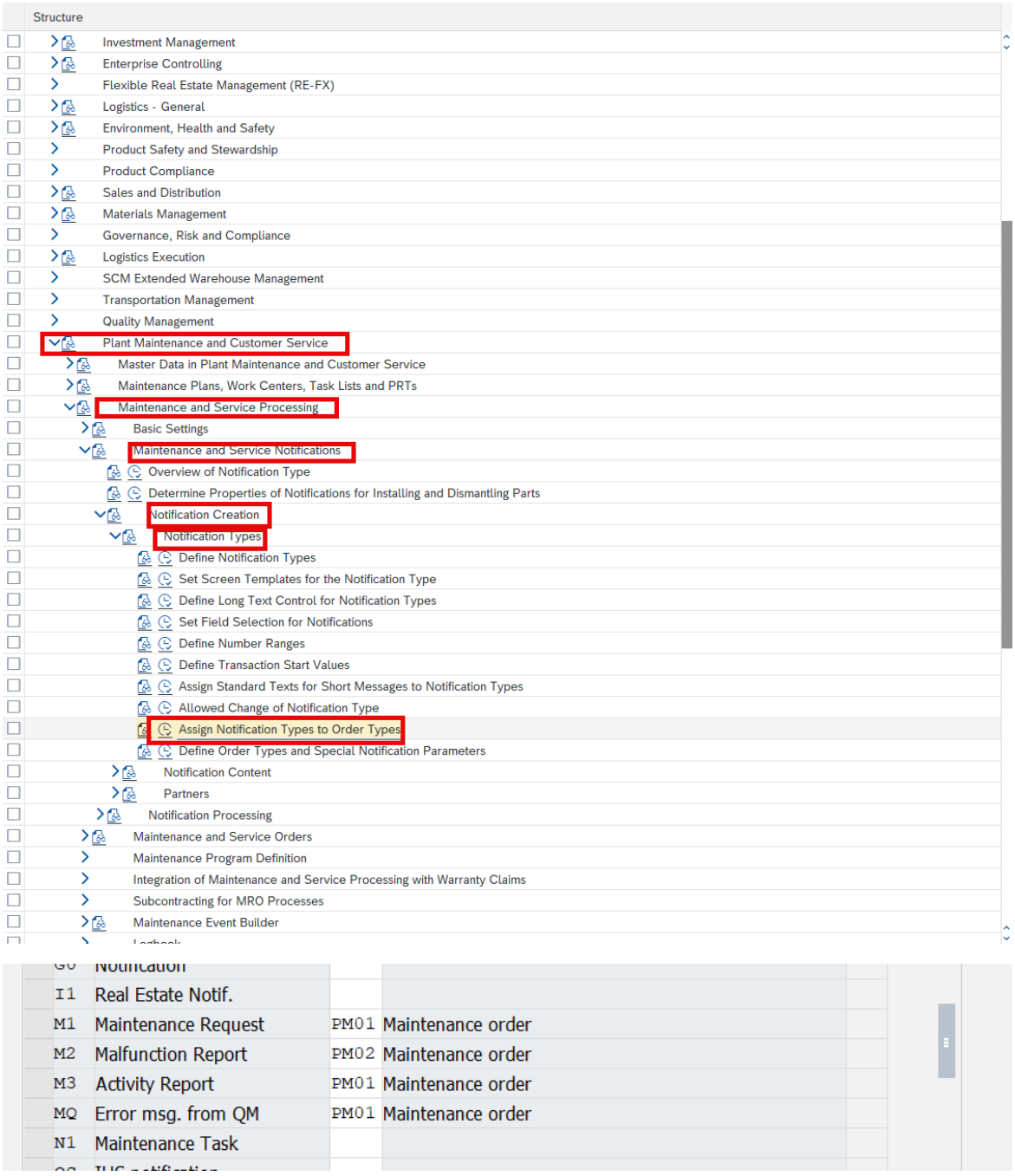
6. Save your changes.

4.15.2.4.2 Notification Type SPRO Back End Configuration

Before the oMDO layer can return notification types to SSAM correctly, ensure that notification types are assigned to the appropriate order types in the back end.

Procedure

1. Navigate to: *IMG* > *Plant Maintenance and Customer Service* > *Maintenance and Service Processing* > *Maintenance and Service Notifications* > *Notification Creation* > *Notification Types* > *Assign Notification Types to Order Types*
2. Locate the notification type you want to expose to SSAM (for example, M1 or M2).
3. Maintain the assignment to the appropriate order type according to your system design.



4. Save your configuration.

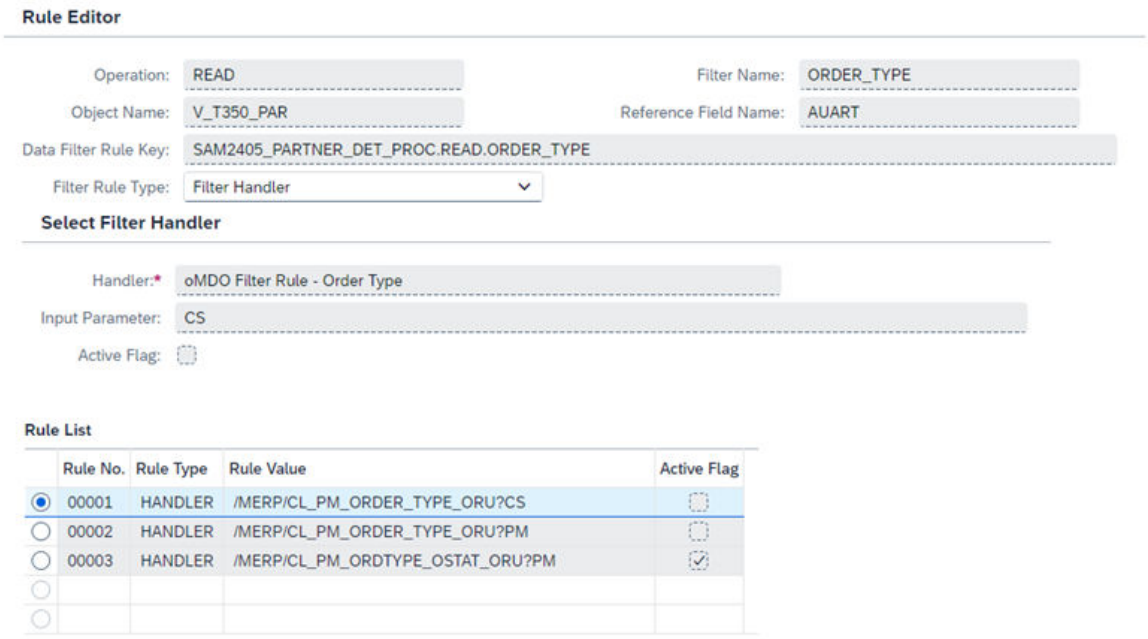
> **Note**
>
> If this assignment is missing, notifications created with unassigned notification types aren't fetched into SSAM. For example, if notification type M1 is expected to sync to SSAM but M1 isn't assigned to an order type, SSAM doesn't retrieve it.

4.15.2.5 Work Order Partner Determination Procedure oMDO Configuration

Context

Procedure

1. On the *ConfigPanel* home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. In the *OData Mobile Data Object* list select SAMXXXX_PARTNER_DET_PROC, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* *Standard Filter* and click *ORDER_TYPE*. Click the *Change* button.
4. Set the */MERP/CL_PM_ORDTYPE_OSTAT_ORU?PM* filter handler to active. It will receive all order types supported by the phase model.
5. Save your changes.

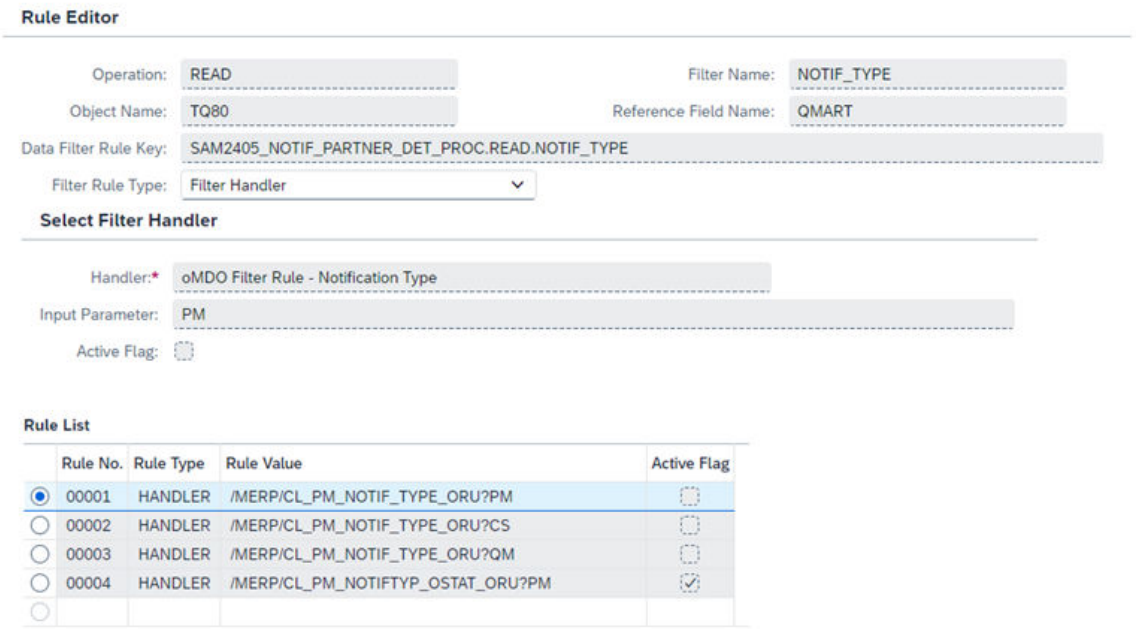


4.15.2.6 Notification Partner Determination oMDO Configuration

Context

Procedure

1. On the *ConfigPanel* home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. In the *OData Mobile Data Object* list select SAMXXXX_NOTIF_PARTNER_DET_PROC, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* *Standard Filter* and click *NOTIF_TYPE*. Click the *Change* button.
4. Set the */MERP/CL_PM_NOTIFTYPE_OSTAT_ORU?PM* filter handler to active. It will return all phase model enabled notification types.
5. Save your changes.

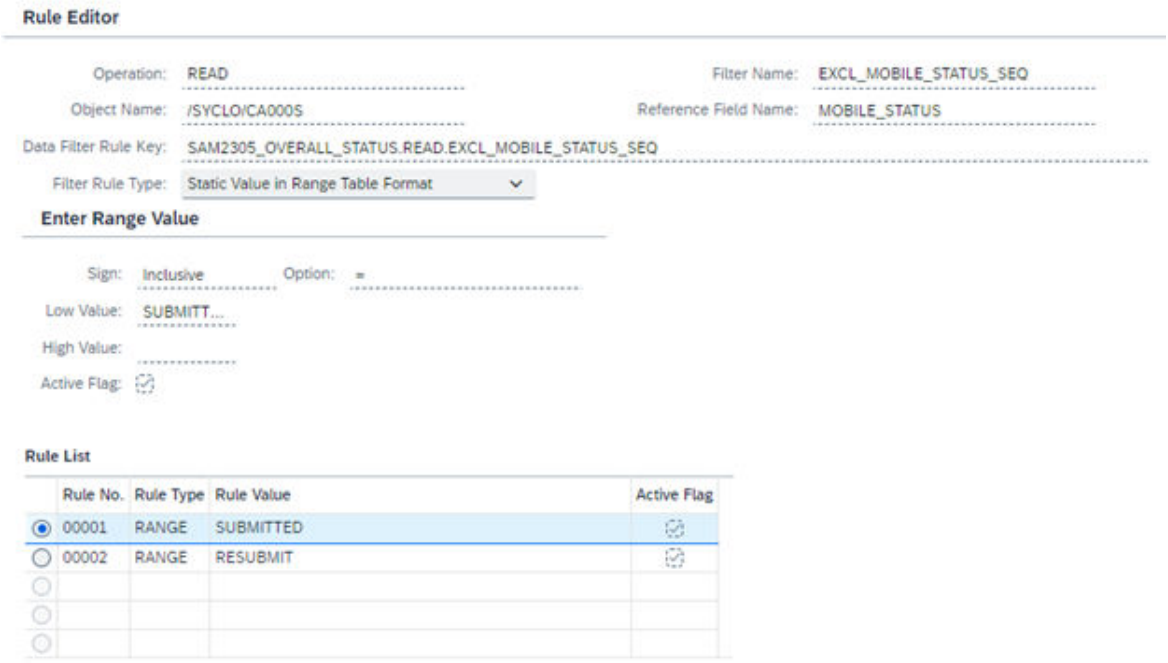


4.15.2.7 Overall Status oMDO Configuration

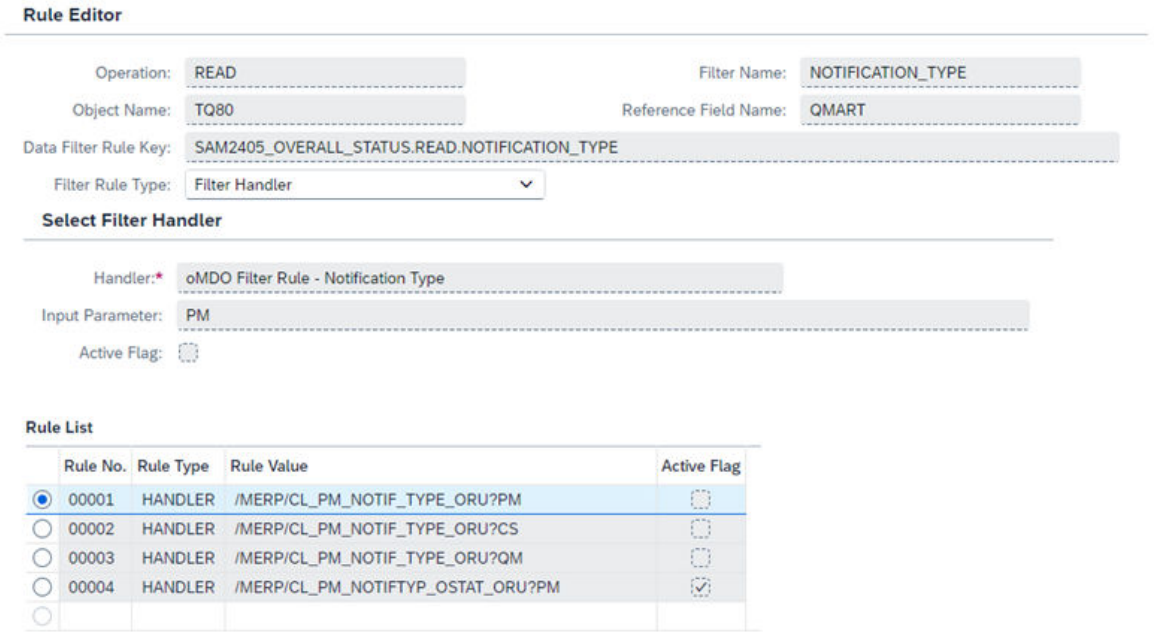
Procedure

1. On the *ConfigPanel* home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. In the *OData Mobile Data Object* list select SAMXXXX_OVERALL_STATUS, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* *Standard Filter* and then click on the filters described in the steps below. Click the *Change* button.
4. Use *EXCL_MOBILE_STATUS_SEQ* filter to disable certain phase model status transitions on your mobile client. Disable if any filter specific to the phase model has been set.

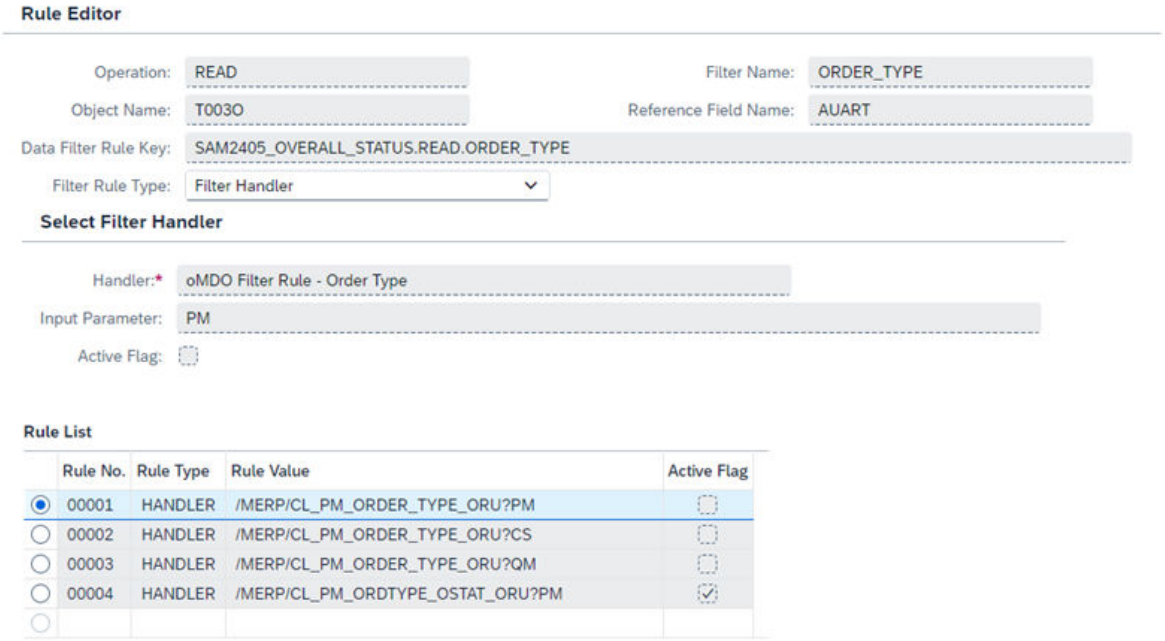
   The configuration of the phase model status transition allows SUBMITTED in ACTIONREQ, but this is not allowed in SAP Service and Asset Manager, so the following filter values must be active when the phase model is enabled.



5. *NOTIFICATION TYPE*: Set the */MERP/CL_PM_NOTIFTYPE_OSTAT_ORU?PM* filter handler to active.



6. *ORDER_TYPE*: Set the */MERP/CL_PM_ORDTYPE_OSTAT_ORU?PM* filter handler to active.

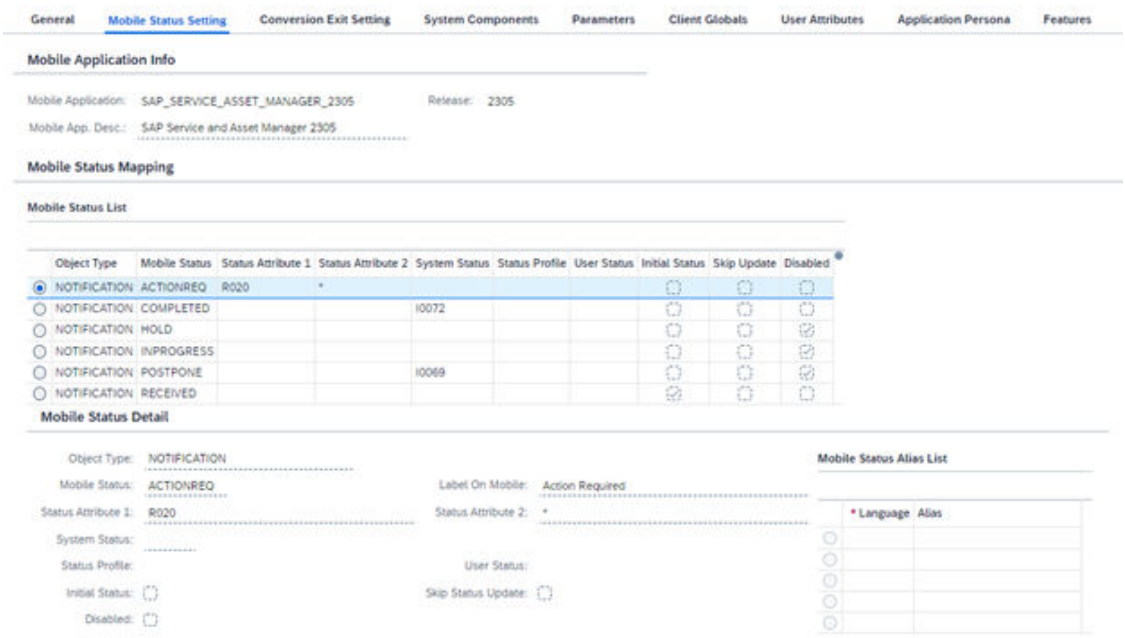


4.15.2.8 Mobile Status Mapping Configuration

The ConfigPanel shows you which PM mobile statuses are mapped to the phase model statuses.

1. From the main *ConfigPanel* page, click the *Mobile Application Configuration Mobile Status Setting* tab.

2. Select your application from the *Defined Mobile Applications* list.
3. Click the *Change* button to change the configuration.
   The *Status Attribute 1* and *Status Attribute 2* fields are used to map statuses as follows:
   - Status Attribute 1: Overall Status
   - Status Attribute 2: Overall Status Profile
     If an asterisk (*) is present, this indicates any overall status profile.



> ### Note
>
> If you enable the phase model, activate the following mobile statuses by setting the *Status Attribute 1* and *Status Attribute 2* fields as indicated in the table.

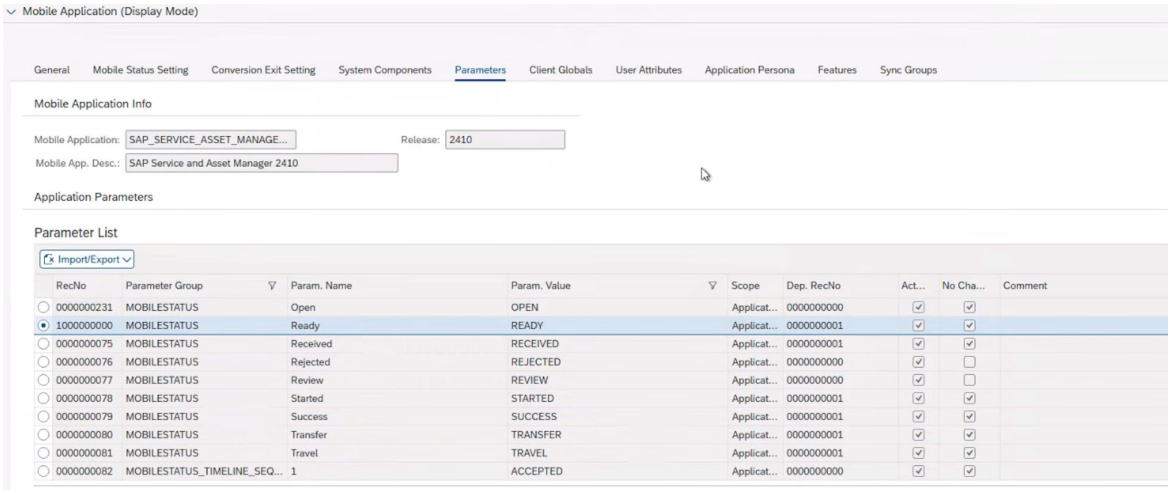
4. When the phase model is enabled, make sure the *Mobile Status Mapping* statuses listed below are enabled.

Mobile Status Mapping

Object Type	Mobile Status	Status Attribute 1	Status Attribute 2	System Status
NOTIFICATION	ACTIONREQ	R020	*	
NOTIFICATION	COMPLETED Status is used in both phase model ON and OFF scenarios			I0072
NOTIFICATION	RESUBMIT	R025	*	
NOTIFICATION	STARTED Status is used in both phase model ON and OFF scenarios			I0070

Object Type	Mobile Status	Status Attribute 1	Status Attribute 2	System Status
NOTIFICATION	SUBMITTED	R005	*	
NOTIFICATION	ORDASSN	R030	*	
NOTIFICATION	ACCEPTED	R010	*	
WORKORDER	COMPLETED	R075	*	
WORKORDER	DONE	R080	*	
WORKORDER	READY	R065	*	
WORKORDER	STARTED	R070	*	
WO_OPERATION	COMPLETED	R140	*	
WO_OPERATION	HOLD	R135	*	
WO_OPERATION	READY	R125	*	
WO_OPERATION	STARTED	R130	*	

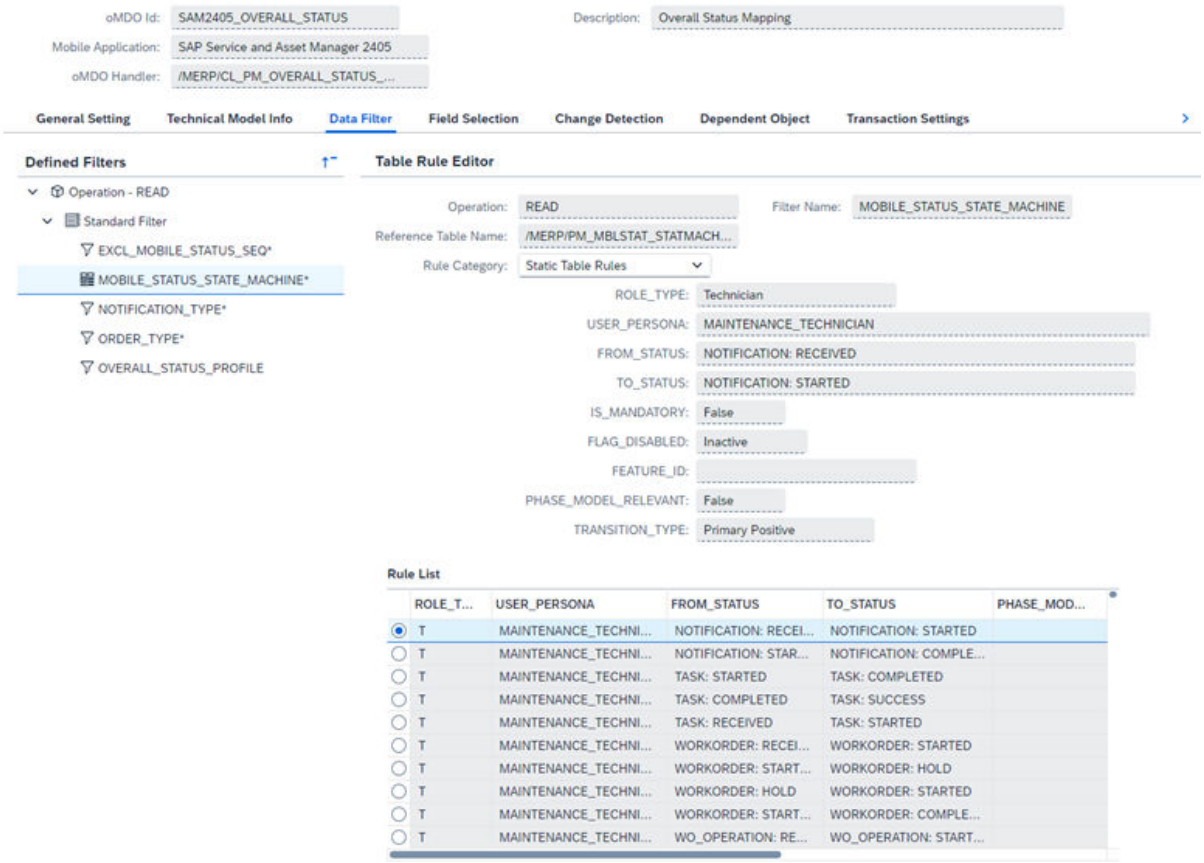
5. From the main *ConfigPanel* page, click the *Parameters* tab.
6. Select your application from the *Defined Mobile Applications* list.
7. Click the *Change* button to modify the configuration.
8. Add the *Ready* status as shown below:



9. Save all the changes you have made.

4.15.2.9 Mobile Status State Machine

The status transition of the phase model is supported in *IMG Plant Maintenance* and *Customer Service Maintenance Service Processing Fiori Apps* for Maintenance Processing Configure Overall Status Profiles.



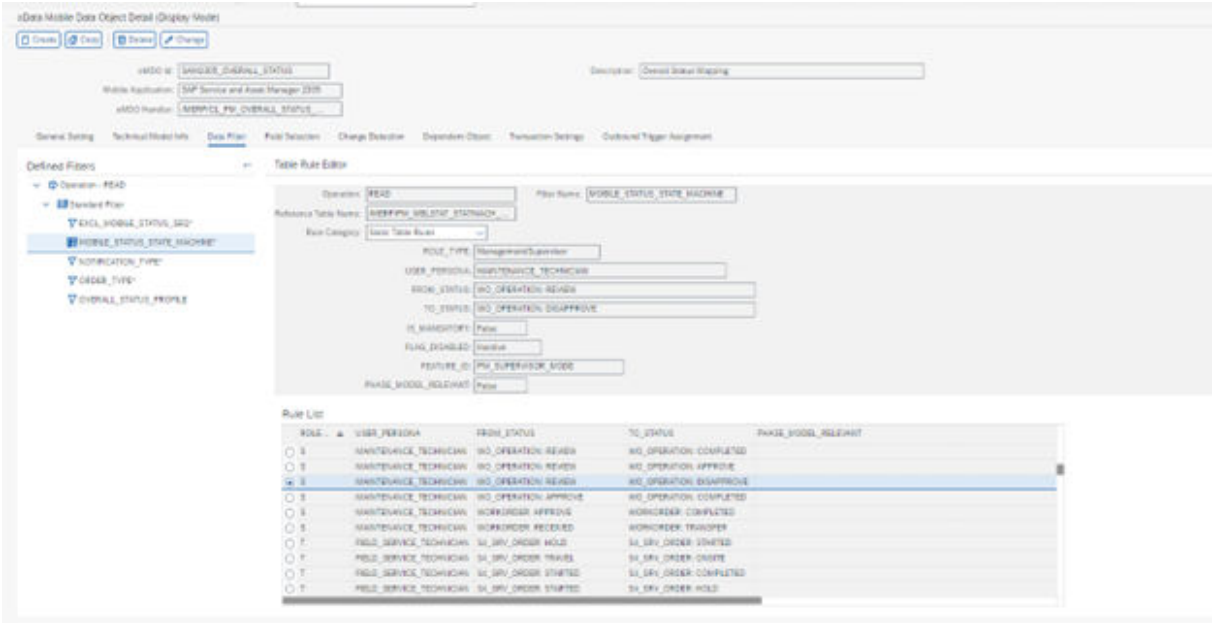
The status transition data is downloaded as a set of the *EAMOverallStatusSeqs* entities for the mobile client that defines the status transition on the device.

> **Note**
>
> As of SAP Service and Asset Manager release 2305, SAP adds new status transitions to the mobile state machine for the supervisor and technician roles in the *Maintenance Technician Persona*. The *ROLE_TYPE* property allows you to define a status transition record for the *Technician* or *Supervisor* role. Any supervisor-specific status records are only used if the *Supervisor* mode is enabled.
>
> If the phase model is enabled, this filter will be ignored.

Configure status transitions (such as add, delete, activate or deactivate) in the state machine for the corresponding phase model flag. The *MOBILE_STATUS_STATE_MACHINE* data filter is located in SAMXXXX_OVERALL_STATUS.

The status transitions corresponding to the phase model in the state machine are added based on the status profile of the phase model from the core configuration. The state machine is the driving factor and not the status transition in IMG (*IMG Plant Maintenance and Customer Service Maintenance Service Processing Fiori Apps for Maintenance Processing Configure Overall Status Profiles*) as of SSAM2305.

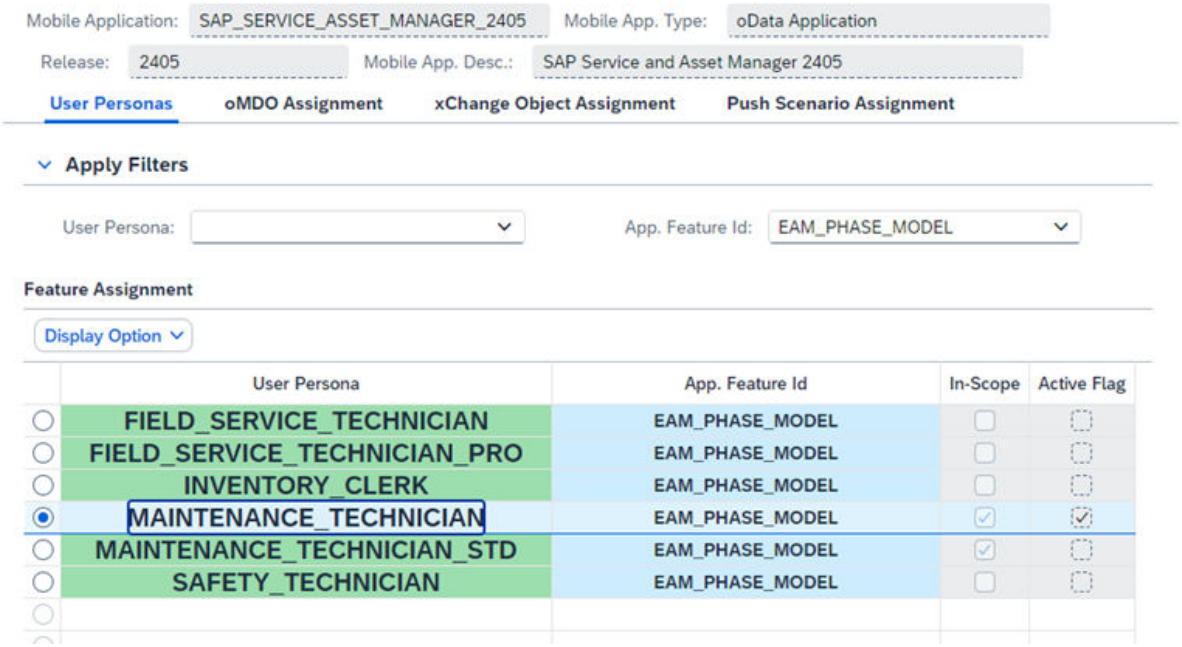
The *USER_PERSONA, FEATURE_ID* and *PHASE_MODEL_RELEVANT* new fields have been added to the state machine table to indicate transitions specific to persona, feature, and whether they apply to a phase model only. For example, the highlighted status transition in the screenshot below allows a supervisor with the *Maintenance Technician Persona* role to not approve a work order transaction in the review status for an order type without a phase model when the *PM_SUPERVISOR_PHASE* model feature is enabled.



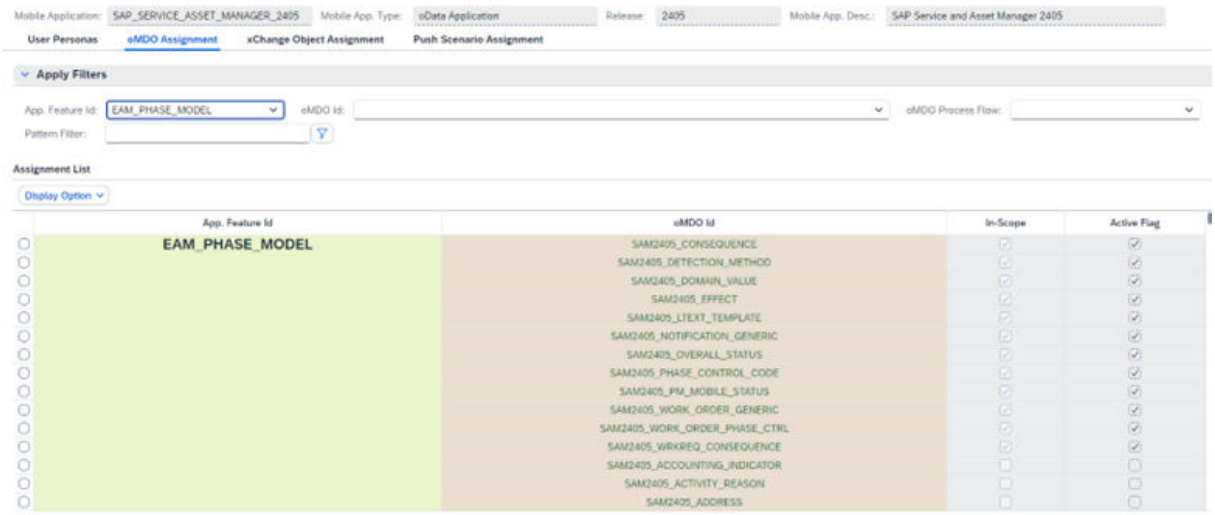
Make sure that all the state transitions marked *PHASE_MODEL_RELEVANT = X* are active when the phase model is enabled.

4.15.2.10 Persona and Feature Enablement

The EAM phase model is added as a persona or feature assignment. When the phase model is enabled, the following persona or feature assignments must be enabled. The following settings are disabled by default, as shown in the figure.



When the *EAM_PHASE_MODEL* feature is active, data related to the phase model, such as *WorkRequestConsequence* or *Effect*, is downloaded during synchronization.



When the phase model is disabled, the mobile phone status in SSAM 2110 behaves the same as in the previous versions. However, in SSAM 2110, a status state machine has been added. For the corresponding configuration, follow the instructions in the following Emergency or Minor Work [page 378] topic.

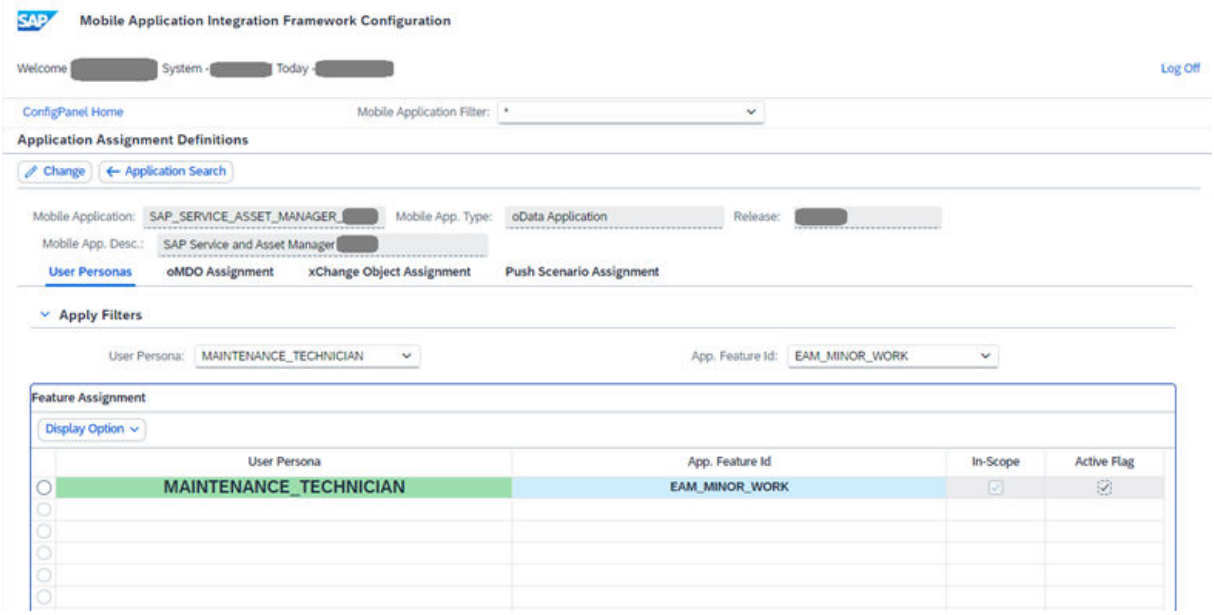
4.15.2.11 Emergency or Minor Work

This new feature is added to support emergency or minor work in the reactive maintenance phase model. It allows you to skip phases and issue a work order or notification when a technician is authorized to create these items.

> **Note**
>
> You can read and process notifications for both minor and emergency work. However, creating notifications is only supported for minor work.

Minor Work Notification

Feature: *EAM_MINOR_WORK*

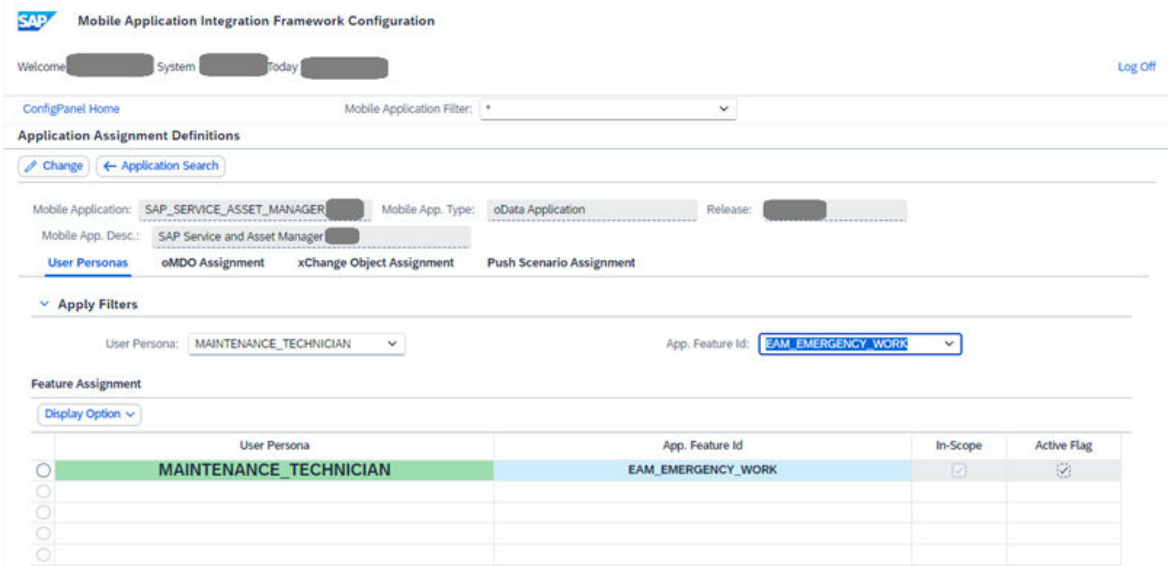


- The *EAM_MINOR_WORK* and *EAM_EMERGENCY_WORK* features are created and assigned to the *NotificationProcessingContext* entity linked to the *NotifProcessingContext* property in the *MyNotificationHeaders* entity.
- The user must have authority (the *I_EXCP_MN* object: *Exception Process* > *Maintenance Notification*) to be able to create a notification with an exception process.

> **Note**
>
> The EAM_MINOR_WORK feature depends on EAM_PHASE_MODEL. Therefore, EAM_PHASE_MODEL must be active for the EAM_MINOR_WORK feature to work.

Emergency Work Notification

Feature: *EAM_EMERGENCY_WORK*



- The *OrderProcessingContext* property in the *MyWorkOrderHeader* entity drives the emergency WO creation/release.

- The user must have authority (the *I_EXCP_MN* object: *Exception Process* > *Maintenance Notification* and *I_EXCP_MO*: *Exception Process* > *Maintenance Order*) to be able to create an emergency work notification and related work order with an exception process.

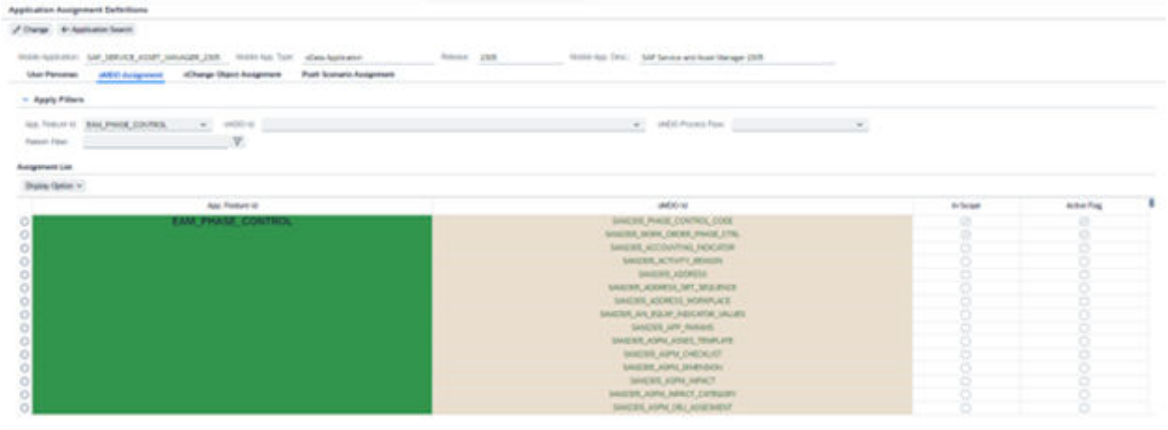
> **Note**
>
> The EAM_EMERGENCY_WORK feature depends on EAM_PHASE_MODEL. Therefore, EAM_PHASE_MODEL must be active for the EAM_EMERGENCY_WORK feature to work.

4.15.2.12 EAM Phase Control Code

The process control code can limit a certain process state change based on the system state. It can also be applied to the execution phase, which prevents the user from moving the order or operation from one sub-phase to another.

As for 2410 release:

- IMG backend configuration path is the following: *IMG* > *Logistics* > *General* > *Product Lifecycle Management (PLM)* > *Plant Maintenance and Customer Service* > *Maintenance and Service Processing* > *Fiori Apps for Maintenance Processing* > *General Settings* > *Define Phase Control Code for Maintenance Orders*
- The new feature *EAM_PHASE_CONTROL* is created to enable the EAM phase control code. To block the transition of an order or operation from one phase to another when the phase model feature is enabled. If the EAM_PHASE_CONTROL feature is active, the following entities are enabled.
  - PhaseControl
  - PhaseControlCode
  - PhaseControlKey
  - PhaseControlSystemMobileStatusMap
  - PhaseControlSystemStatus
  - WorkOrderOperationPhaseControl
  - WorkOrderPhaseControl
- This feature is active right out of the box. To disable it, refer to the feature configuration.



> **Note**
>
> For this feature to work, the *EAM_PHASE_MODEL* feature must be active in the SSAM application configuration.

> **Note**
>
> This feature is available for the S4CORE 106 and subsequent versions.

4.15.3 Phase Model + Non-Phase Model Configuration

If your backend system has several types of maintenance orders activated for the phase model, and some use the traditional approach, use the SSAM configuration described in the following Phase Model + Non-Phase Model Configuration [page 381] section.

> **Note**
>
> This configuration is possible for SSAM 2305 and subsequent versions. The WO assignment types are limited to 2 and 6, that is, only at the operational level, due to the restriction imposed on the basic feature of the phase model.

The following configuration will pull both phase model and non-phase model notifications. However, only non-phase model notifications can be processed on the device due to the core phase model notification feature. And the following status transitions will be available on the device for non-phase model notifications.

NOTIFICATION:RECEIVED > *NOTIFICATION:STARTED*

NOTIFICATION:STARTED > *NOTIFICATION:COMPLETED*

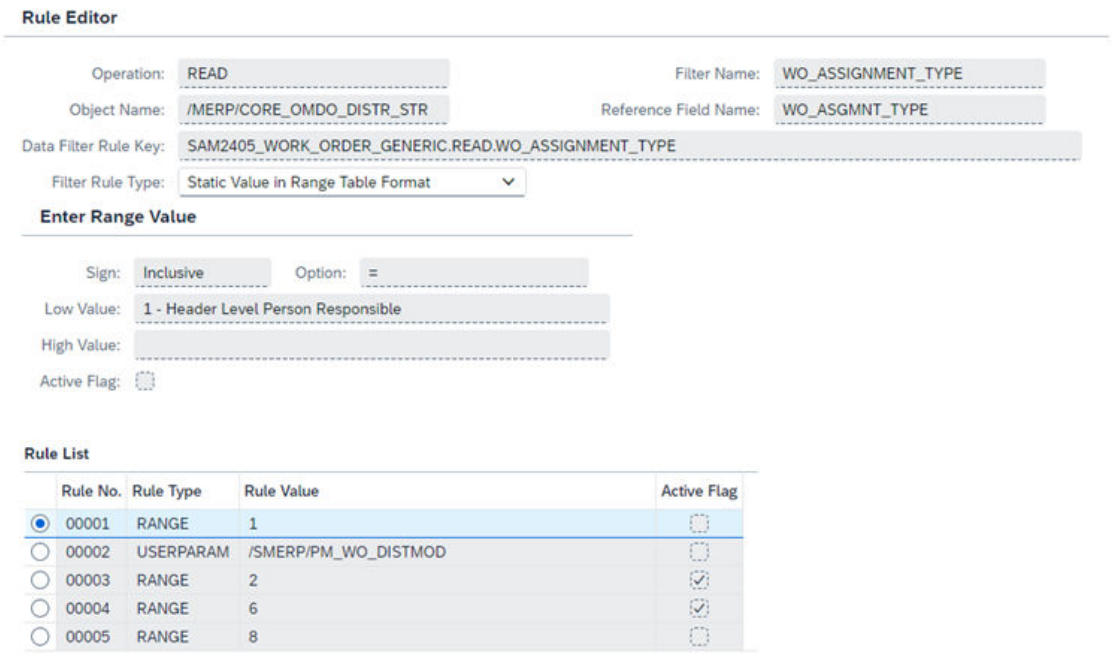
4.15.3.1 Work Order oMDO Configuration

Context

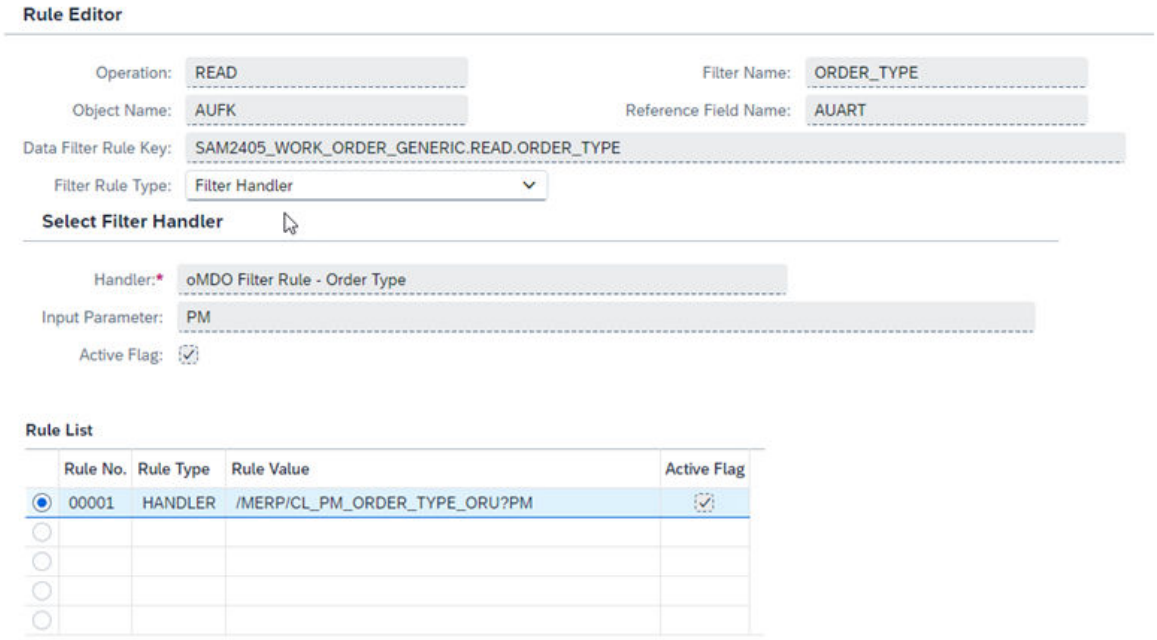
- On the *ConfigPanel* home page, select *OData Mobile Data Object Configuration*. Make sure you select the correct mobile application in the *Mobile Application Filter* field at the top of the page.
- From the *OData Mobile Data Object* list, select *SAMXXXX_WORK_ORDER_GENERIC*, and then select the *Data Filter* tab
- Expand the *Defined Filters* list as follows; *Operation - READ* > *Data Distribution* and select the filters shown in the screenshots below. Click the *Change* button.

Procedure

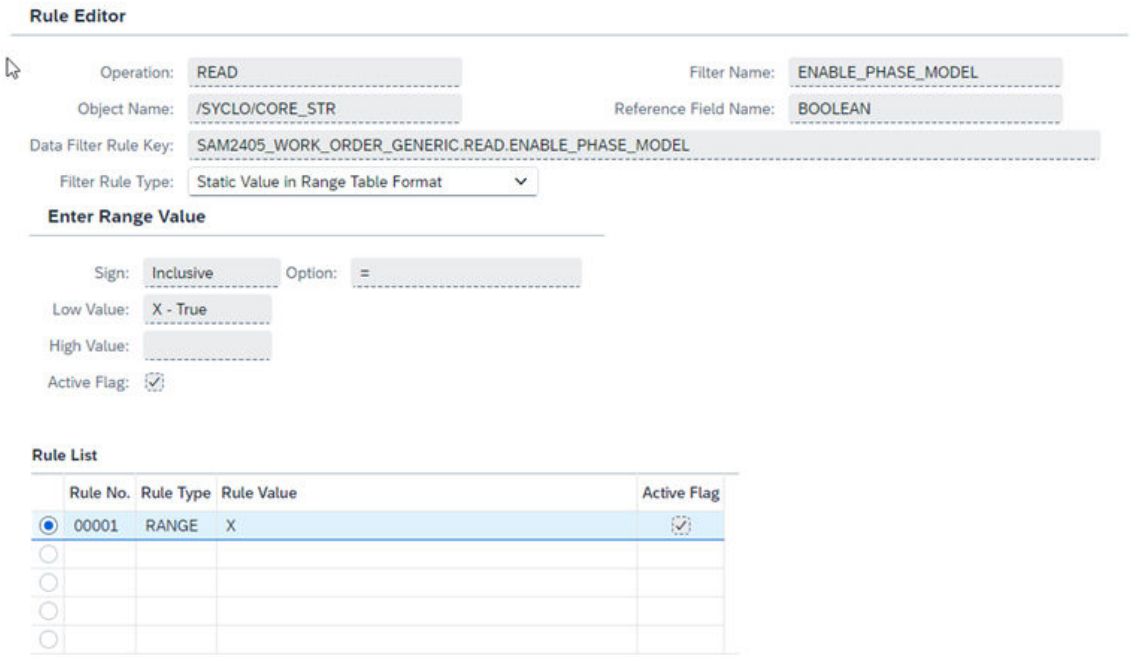
1. Maintain assignment type filter *WO_ASSIGNMENT_TYPE* with the following assignment types shown below.



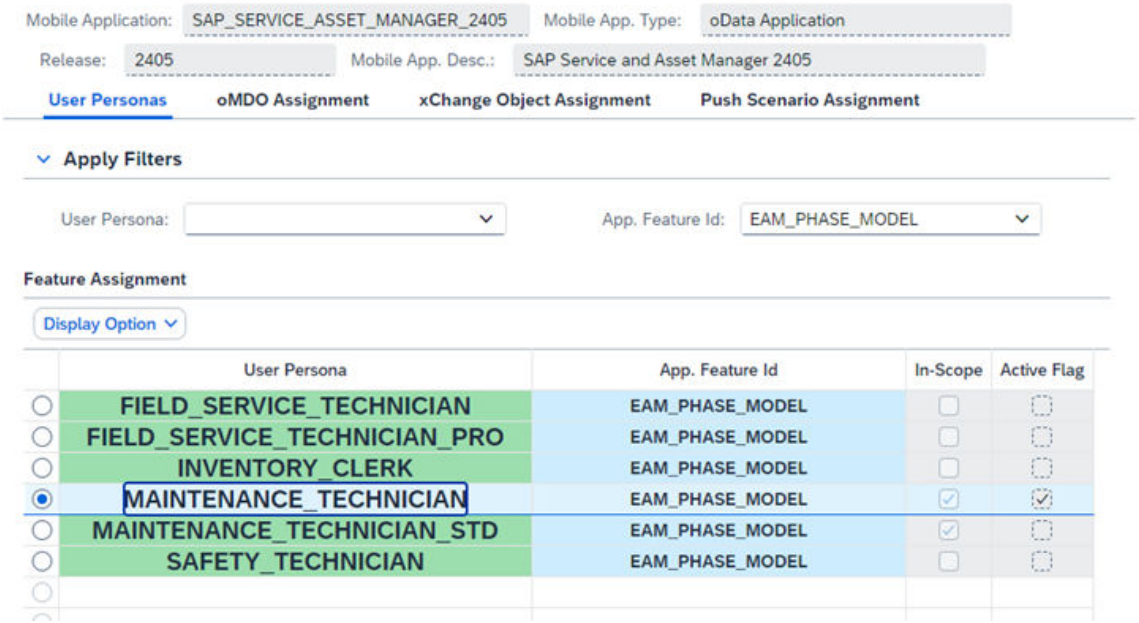
2. In the *ORDER_TYPE* filter, set the filter handler */MERP/CL_PM_ORDER_TYPE_ORU?PM* to the active state, which returns order types that have been assigned a common status profile and those that have not.



3. Set the *ENABLE_PHASE_MODEL* filter to active in the standard filter section.

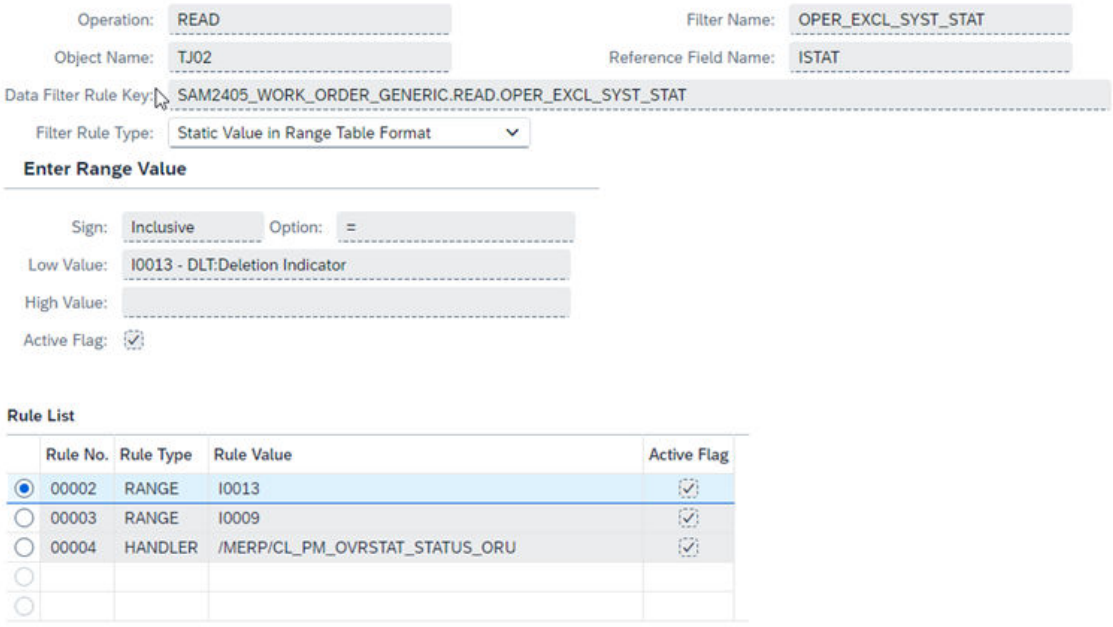


Activate the features in the *Component Assignments* section of the configuration for the Maintenance Technician persona.



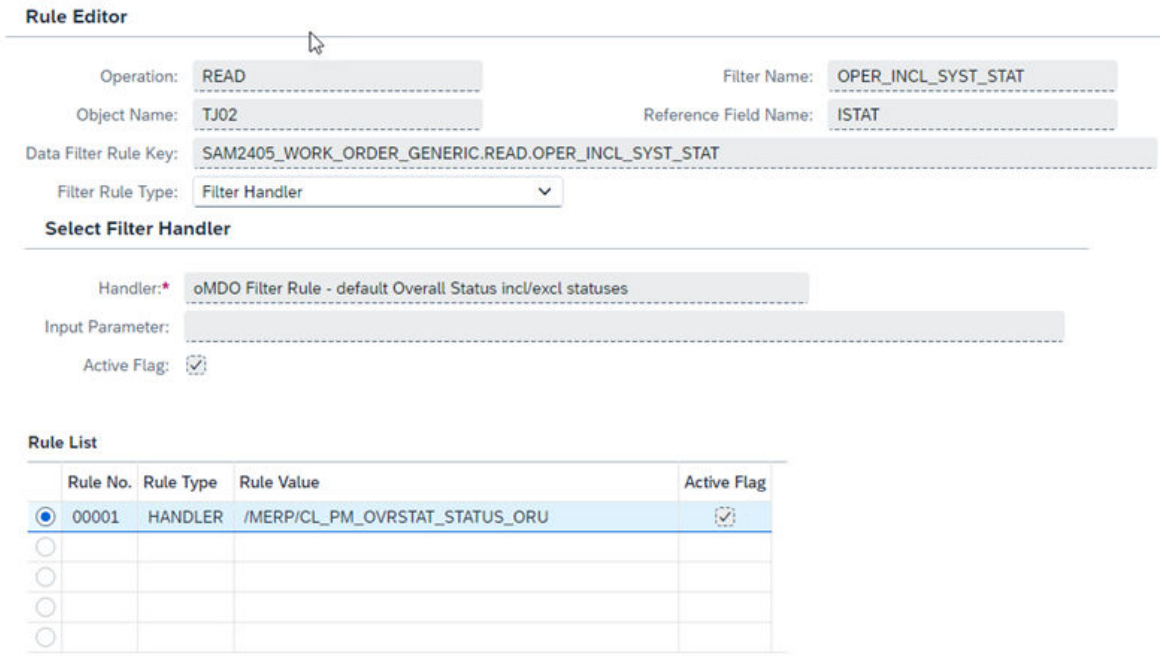
4. Make sure that filter handler */MERP/CL_PM_OVRSTAT_STATUS_ORU* is active, which by default enters the *IEAM5 (ORSC - Ready for Scheduling)* and *I0820 (JBFI - Job Finished)* system statuses into the *OPER_EXCL_SYST_STAT* filter.

> **Note**
>
> If the default statuses defined in filter handler don't fulfill your business scenario, you can manually add the system statuses individually to the filter.

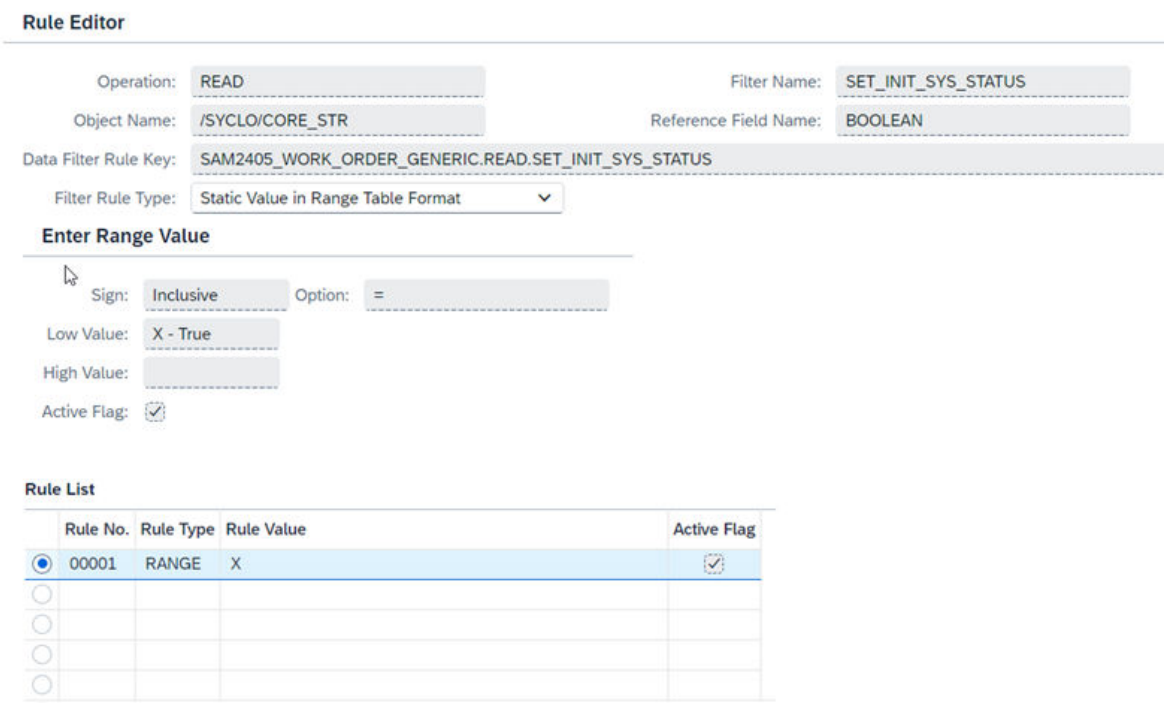


5. Make sure that the */MERP/CL_PM_OVRSTAT_STATUS_ORU* filter handler is active, which by default enters the *I0117 (DSPT - Scheduled), I0809 (JIPR – Job In Process)*, and *I0010 (PCNF – Partially Confirmed)* system statuses into the *OPER_INCL_SYST_STAT* filter.

> **Note**
>
> If the default statuses defined in filter handler don't fulfill your business scenario, you can manually add the system statuses individually to the filter.

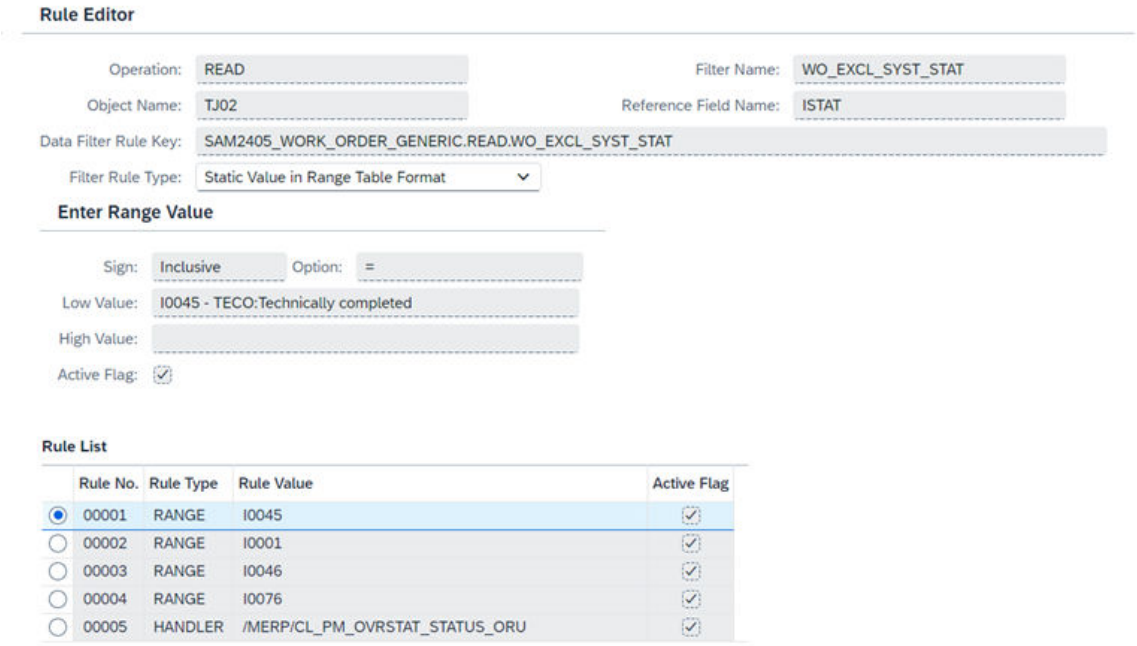


6. Set *SET_INIT_SYS_STATUS* filter to active. Initial mobile status will be determined for both overall status profile based orders and non-phase model related orders.



7. Set the */MERP/CL_PM_OVRSTAT_STATUS_ORU* filter handler to active, which by default enters the *IEAM6 (OMWC – Main Work Completed)* and *I0820 (JBFI – Job Finished)* system statuses into the *WO_EXCL_SYST_STAT* filter.

   If the default statuses defined in filter handler don't fulfill your business scenario, you can manually add the system statuses individually to the filter.



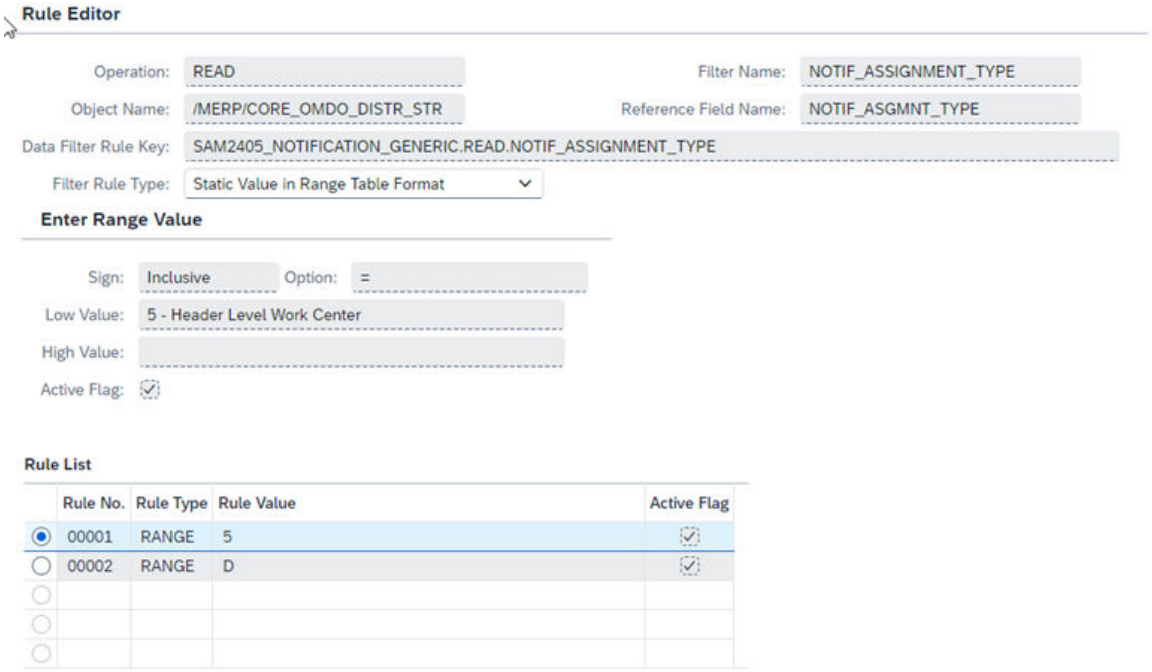
4.15.3.2 Notification Assignment Type Configuration

Configuring the Notification Assignment Type Filter

The following assignment types are supported:

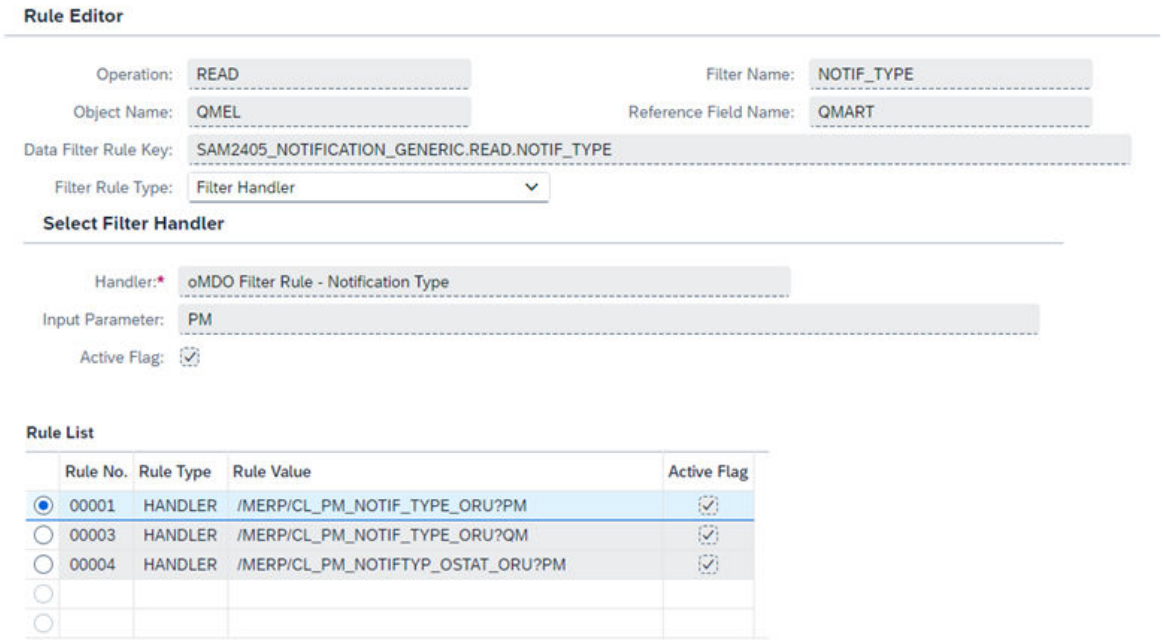
- 1: Header level person responsible
- 5: Header level work center
- D: Dependency queue

1. On the ConfigPanel home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. In the *OData Mobile Data Object List* select **SAMXXXX_NOTIFICATION_GENERIC**, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* > *Data Distribution* > and click *NOTIF_ASSIGNMENT_TYPE*. Click the *Change* button.
4. Set *Low Value* with the desired assignment type as defined by the assignment type model.
5. *Save* your changes.



Configuring the Notification Type Filter

1. On the ConfigPanel home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. In the *OData Mobile Data Object List* select **SAMXXXX_NOTIFICATION_GENERIC**, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* > *Data Distribution* > and click *NOTIF_TYPE*. Click the *Change* button.
4. Set the */MERP/CL_PM_NOTIFTYP_OSTAT_ORU?PM* filter handler to *Active*. This filter handler will return the notification types that have been assigned an overall status profile.
5. Set the */MERP/CL_PM_NOTIF_TYPE_ORU?PM* and/or */MERP/CL_PM_NOTIF_TYPE_ORU?QM* filter handlers to *Active*. The notification types returned will be non-phase model related.
6. *Save* your changes.

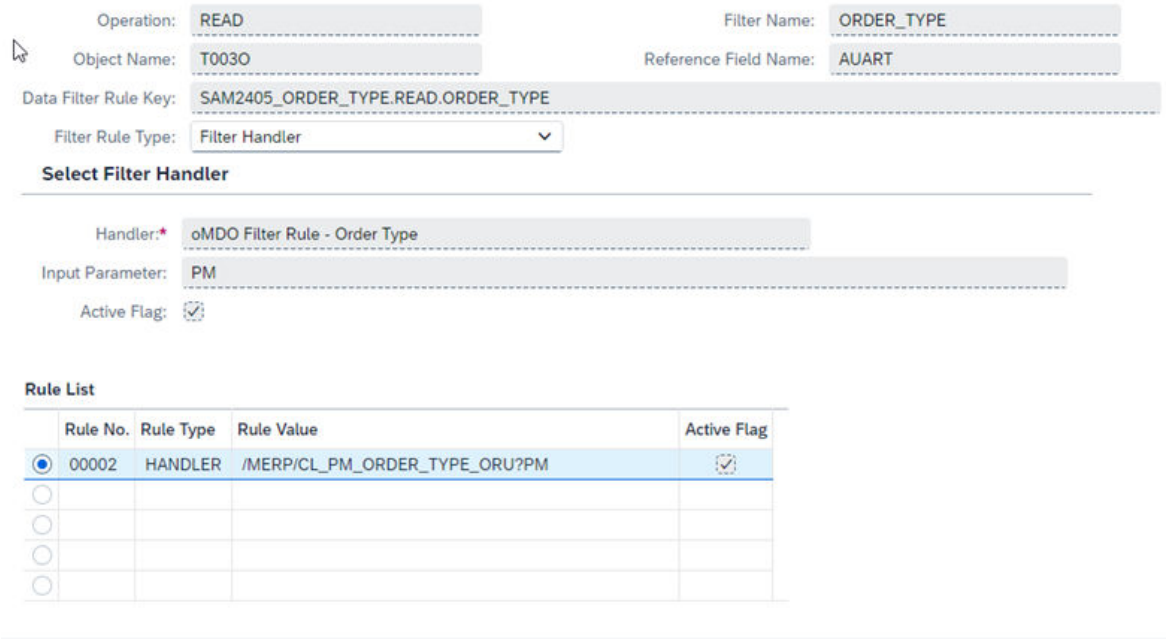


4.15.3.3 Order Type oMDO Configuration

Context

Procedure

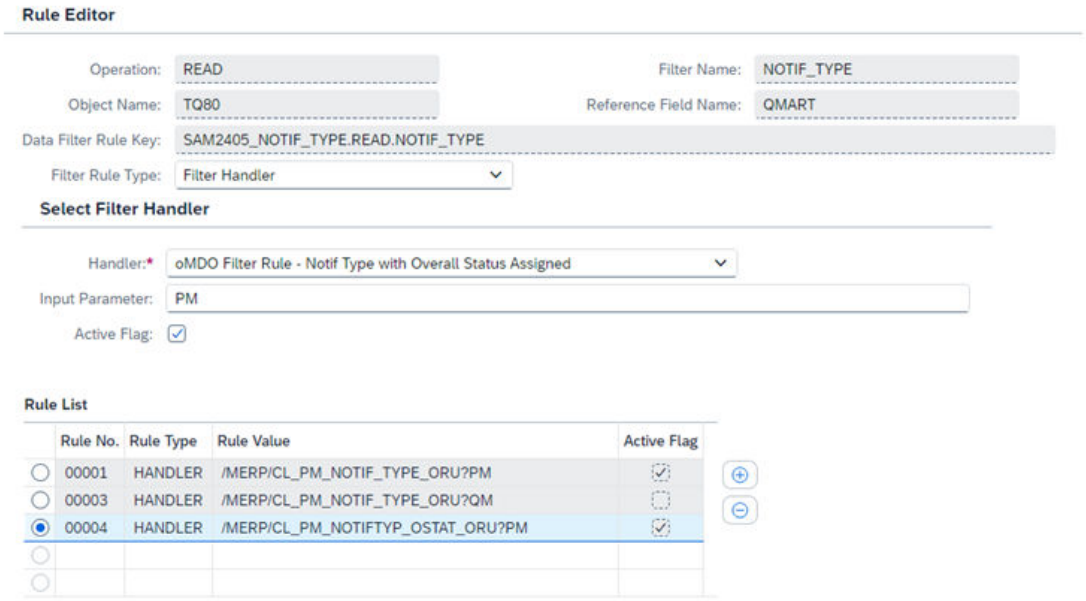
1. On the *ConfigPanel* home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. In the *OData Mobile Data Object* list select SAMXXXX_ORDER_TYPE, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* > *Standard Filter* and click *ORDER_TYPE*. Click the *Change* button.
4. Set the */MERP/CL_PM_ORDER_TYPE_ORU?PM* filter handler to active, as it will return order types related to both phase and non-phase models.
5. Save your changes.



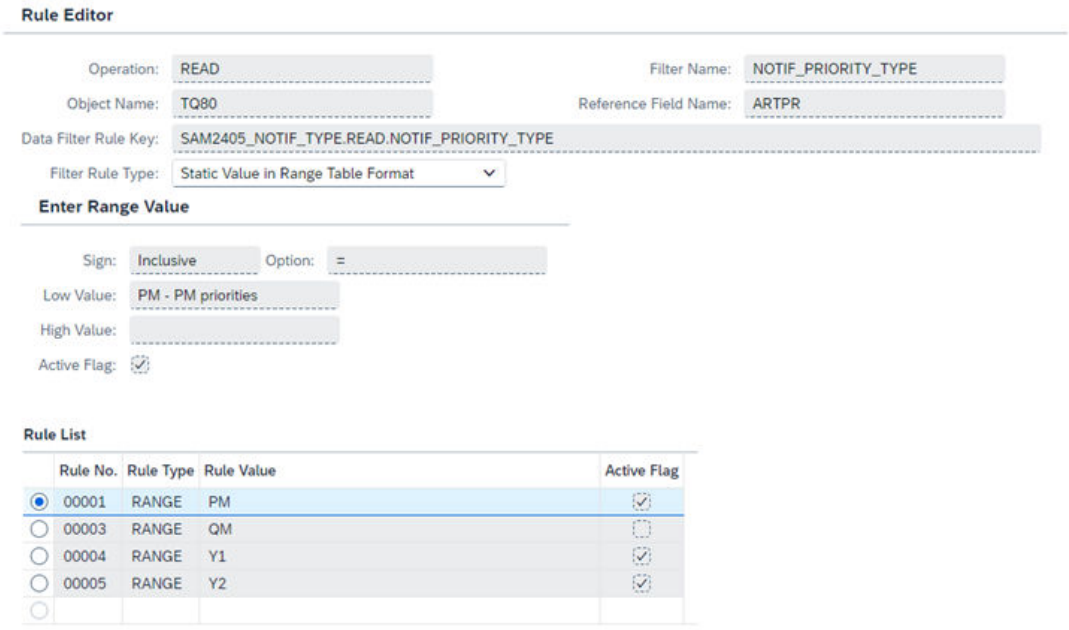
4.15.3.4 Notification Type oMDO Configuration

Procedure

1. On the *ConfigPanel* home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. In the *OData Mobile Data Object* list select SAMXXXX_NOTIF_TYPE, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* *Standard Filter* and click *NOTIF_TYPE*. Click the *Change* button.
4. Set the */MERP/CL_PM_NOTIF_TYPE_ORU?PM* and/or */MERP/CL_PM_NOTIFTYPE_OSTAT_ORU?PM* filter handlers to active, which returns notification types that have been assigned an overall status profile, along with others



5. Configure additional priority type values if the notification uses a priority type other than PM in the *NOTIF_PRIORITY_TYPE* filter.



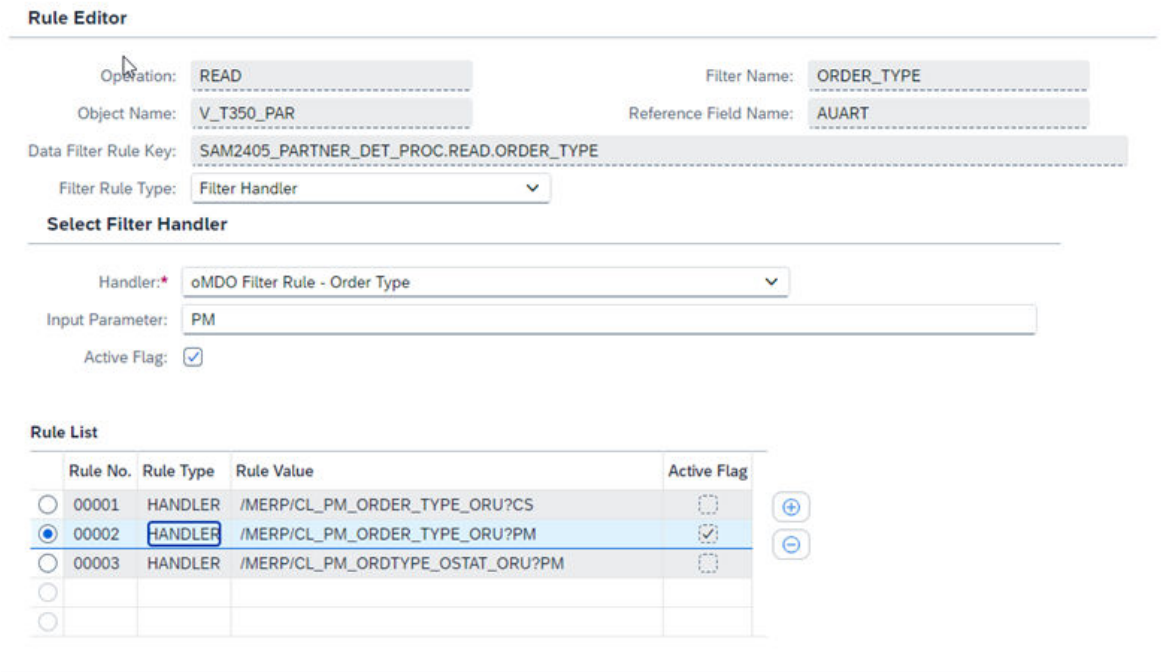
6. Save your changes.

4.15.3.5 Work Order Partner Determination Procedure oMDO Configuration

Context

Procedure

1. On the *ConfigPanel* home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. In the *OData Mobile Data Object* list select SAMXXXX_PARTNER_DET_PROC, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* > *Standard Filter* and click *ORDER_TYPE*. Click the *Change* button.
4. Set the */MERP/CL_PM_ORDER_TYPE_ORU?PM* filter handler to active. It will receive all order types supported by the phase model.
5. Save your changes.

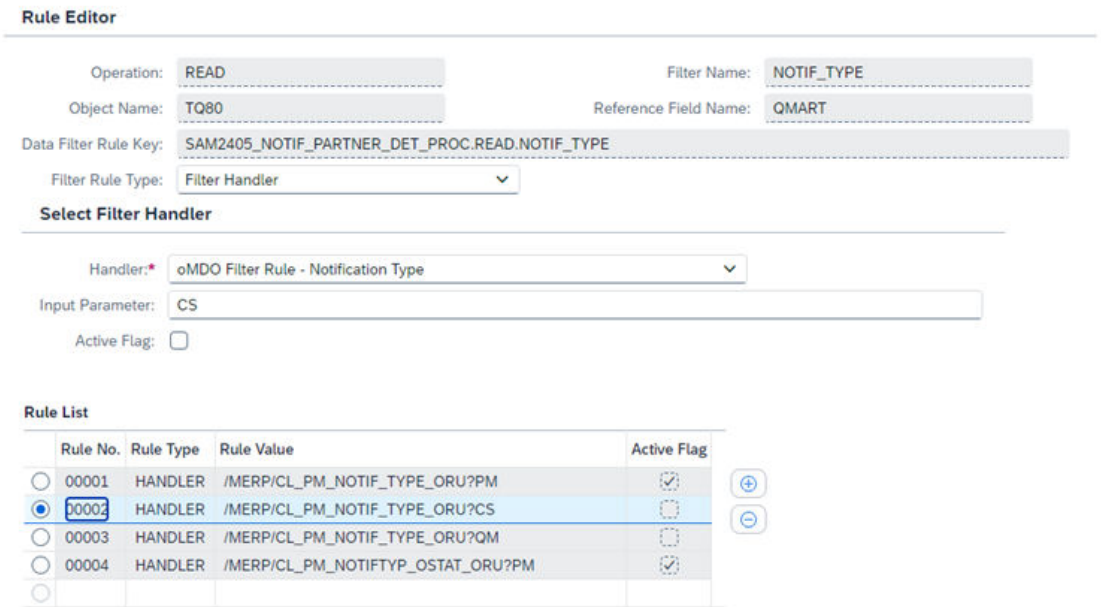


4.15.3.6 Notification Partner Determination oMDO Configuration

Context

Procedure

1. On the *ConfigPanel* home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. In the *OData Mobile Data Object* list select SAMXXXX_NOTIF_PARTNER_DET_PROC, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* *Standard Filter* and click *NOTIF_TYPE*. Click the *Change* button.
4. Set the */MERP/CL_PM_NOTIF_TYPE_ORU?PM* and */MERP/CL_PM_NOTIFTYPE_OSTAT_ORU?PM* filter handlers to active. It will return all types of notifications, both those included in the phase model and those not included in the phase model.
5. Save your changes.

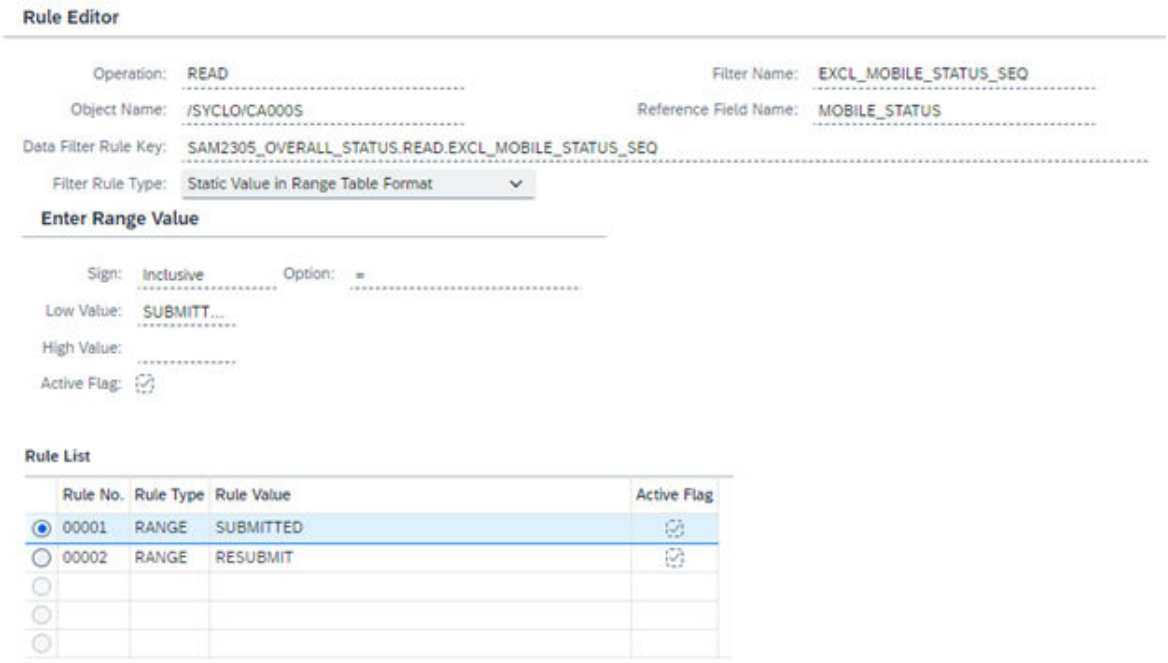


4.15.3.7 Overall Status oMDO Configuration

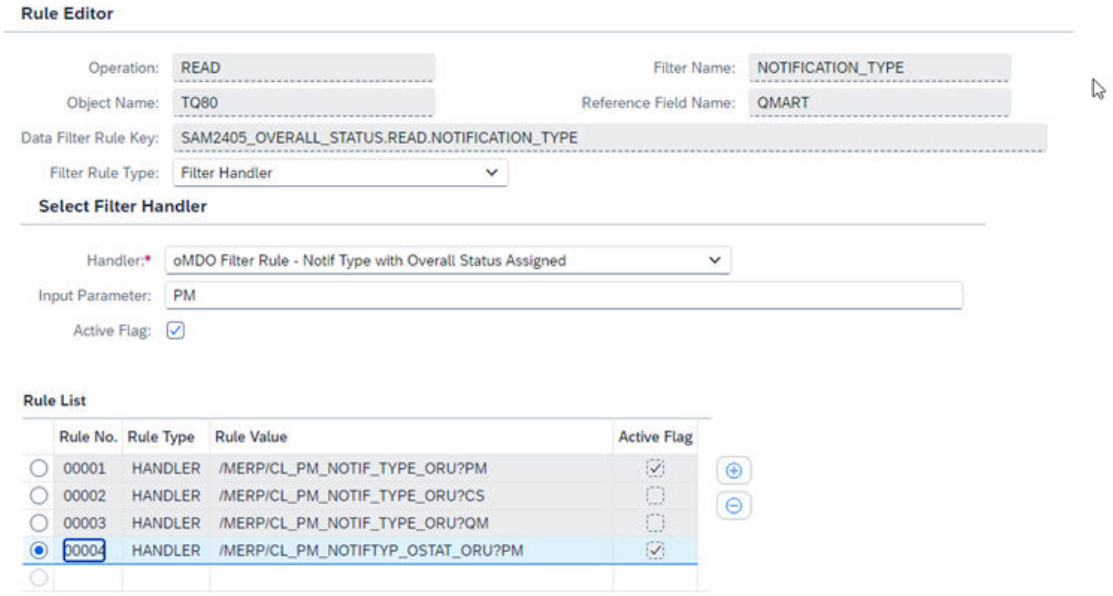
Procedure

1. On the *ConfigPanel* home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. In the *OData Mobile Data Object* list select SAMXXXX_OVERALL_STATUS, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* *Standard Filter* and then click on the filters described in the steps below. Click the *Change* button.
4. Use *EXCL_MOBILE_STATUS_SEQ* filter to disable certain phase model status transitions on your mobile client.

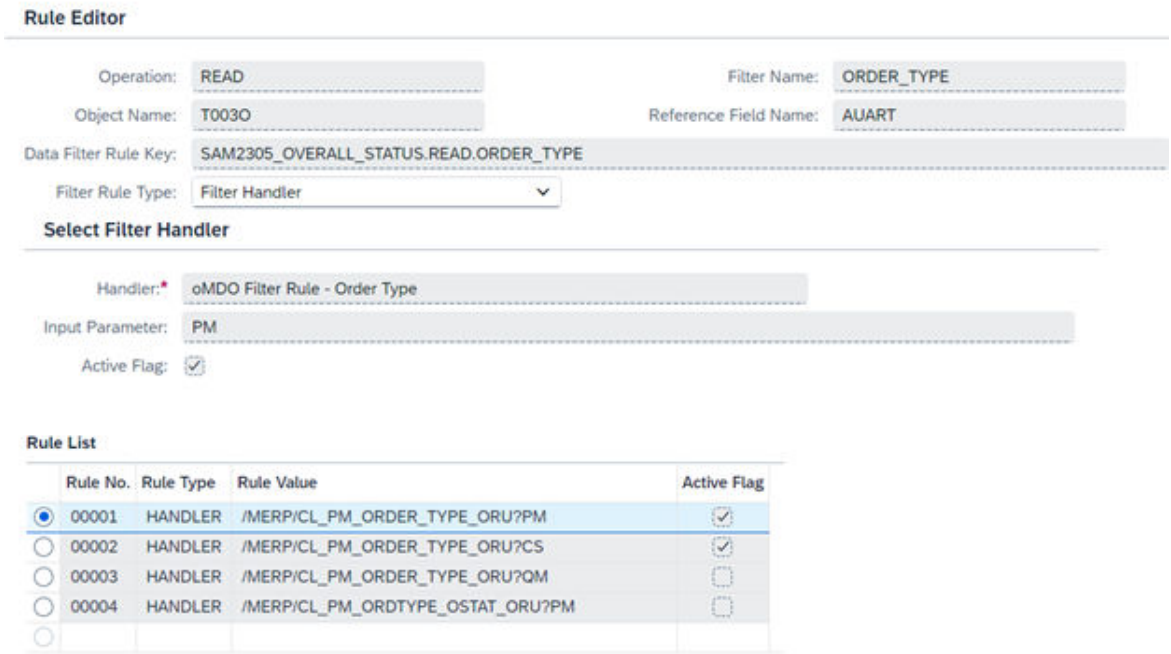
   The configuration of the phase model status transition allows SUBMITTED in ACTIONREQ, but this is not allowed in SAP Service and Asset Manager, so the following filter values must be active when the phase model is enabled.



5. *NOTIFICATION TYPE*: Set the */MERP/CL_PM_NOTIF_TYPE_ORU?PM* and/or */MERP/CL_PM_NOTIFTYPE_OSTAT_ORU?PM* filter handlers to active.

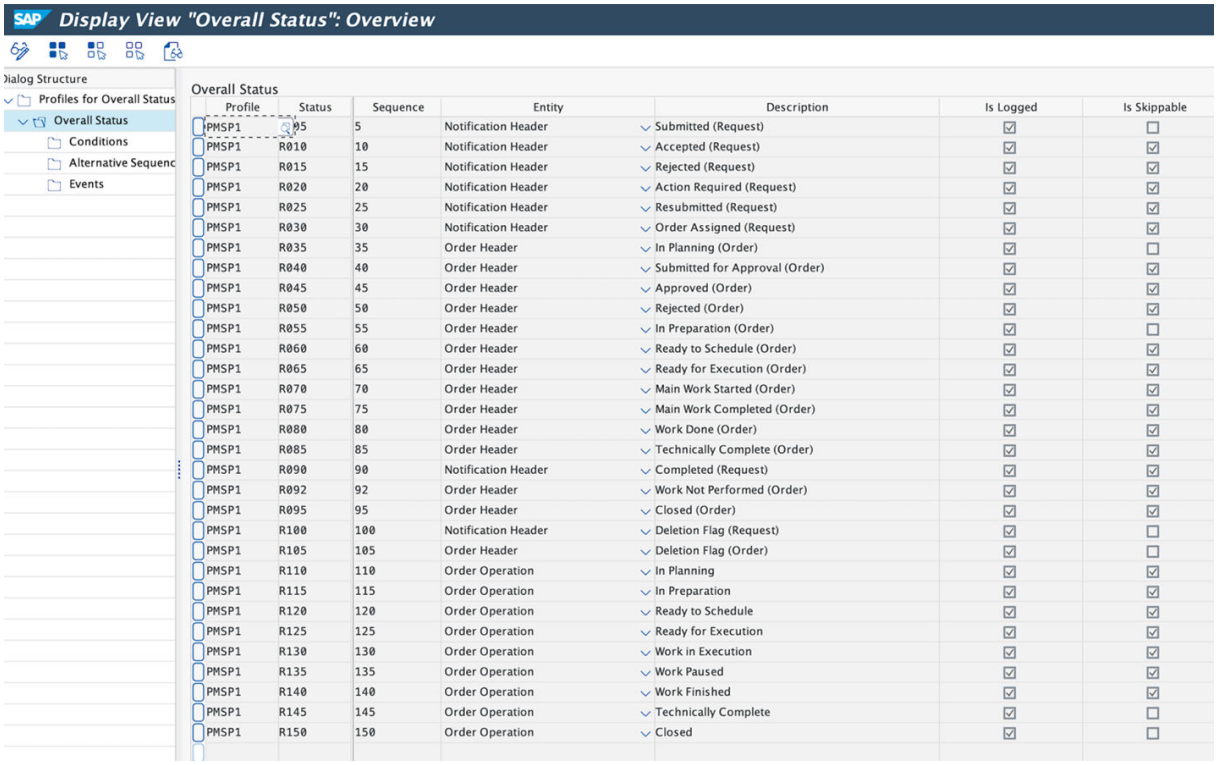


6. *ORDER_TYPE*: Set the */MERP/CL_PM_ORDER_TYPE_ORU?PM* and/or */MERP/CL_PM_ORDER_TYPE_ORU?CS* filter handlers to active.



4.15.3.8 Mobile Status State Machine

The status transition of the phase model is supported in *IMG Plant Maintenance* and *Customer Service Maintenance Service Processing Fiori Apps* for Maintenance Processing Configure Overall Status Profiles.



Profile	Status	Sequence	Entity	Description	Is Logged	Is Skippable
PMSP1	R005	5	Notification Header	Submitted (Request)	☑	☐
PMSP1	R010	10	Notification Header	Accepted (Request)	☑	☑
PMSP1	R015	15	Notification Header	Rejected (Request)	☑	☑
PMSP1	R020	20	Notification Header	Action Required (Request)	☑	☑
PMSP1	R025	25	Notification Header	Resubmitted (Request)	☑	☑
PMSP1	R030	30	Notification Header	Order Assigned (Request)	☑	☑
PMSP1	R035	35	Order Header	In Planning (Order)	☑	☐
PMSP1	R040	40	Order Header	Submitted for Approval (Order)	☑	☑
PMSP1	R045	45	Order Header	Approved (Order)	☑	☑
PMSP1	R050	50	Order Header	Rejected (Order)	☑	☑
PMSP1	R055	55	Order Header	In Preparation (Order)	☑	☐
PMSP1	R060	60	Order Header	Ready to Schedule (Order)	☑	☑
PMSP1	R065	65	Order Header	Ready for Execution (Order)	☑	☑
PMSP1	R070	70	Order Header	Main Work Started (Order)	☑	☑
PMSP1	R075	75	Order Header	Main Work Completed (Order)	☑	☑
PMSP1	R080	80	Order Header	Work Done (Order)	☑	☑
PMSP1	R085	85	Order Header	Technically Complete (Order)	☑	☑
PMSP1	R090	90	Notification Header	Completed (Request)	☑	☑
PMSP1	R092	92	Order Header	Work Not Performed (Order)	☑	☑
PMSP1	R095	95	Order Header	Closed (Order)	☑	☑
PMSP1	R100	100	Notification Header	Deletion Flag (Request)	☑	☐
PMSP1	R105	105	Order Header	Deletion Flag (Order)	☑	☐
PMSP1	R110	110	Order Operation	In Planning	☑	☑
PMSP1	R115	115	Order Operation	In Preparation	☑	☑
PMSP1	R120	120	Order Operation	Ready to Schedule	☑	☑
PMSP1	R125	125	Order Operation	Ready for Execution	☑	☑
PMSP1	R130	130	Order Operation	Work in Execution	☑	☑
PMSP1	R135	135	Order Operation	Work Paused	☑	☑
PMSP1	R140	140	Order Operation	Work Finished	☑	☑
PMSP1	R145	145	Order Operation	Technically Complete	☑	☐
PMSP1	R150	150	Order Operation	Closed	☑	☐

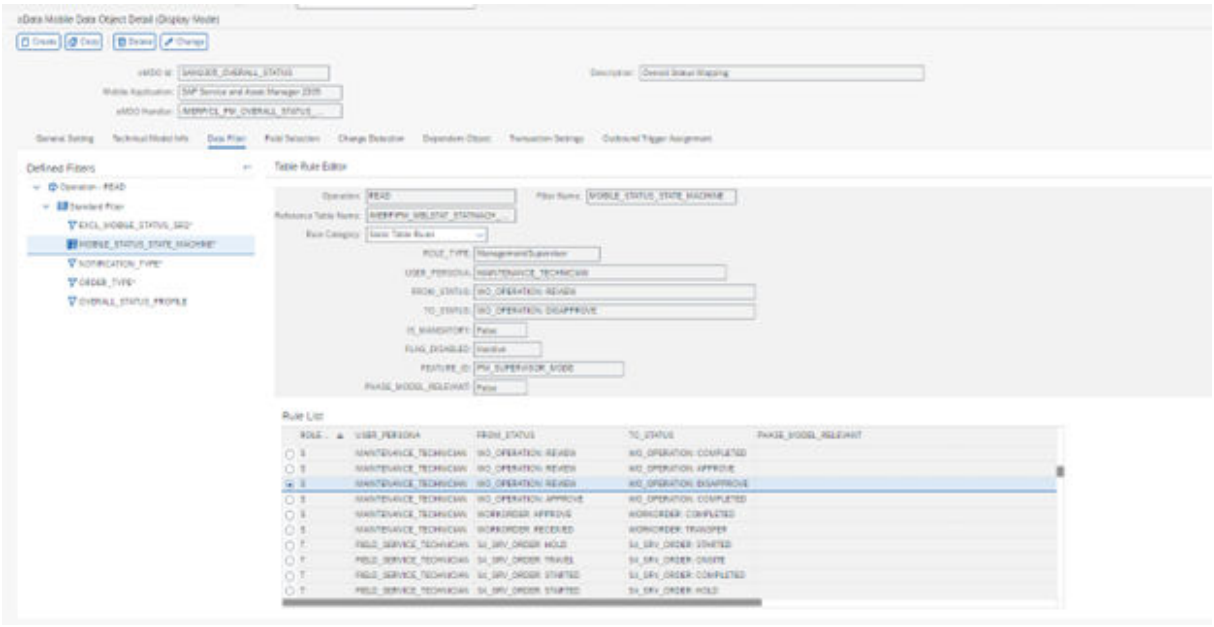
The status transition data is downloaded as a set of the *EAMOverallStatusSeqs* entities for the mobile client that defines the status transition on the device.

> **Note**
>
> As of SAP Service and Asset Manager release 2305, SAP adds new status transitions to the mobile state machine for the supervisor and technician roles in the *Maintenance Technician Persona*. The *ROLE_TYPE* property allows you to define a status transition record for the *Technician* or *Supervisor* role. Any supervisor-specific status records are only used if the *Supervisor* mode is enabled.
>
> If the phase model is enabled, this filter will be ignored.

Configure status transitions (such as add, delete, activate or deactivate) in the state machine for the corresponding phase model flag. The *MOBILE_STATUS_STATE_MACHINE* data filter is located in SAMXXXX_OVERALL_STATUS.

The status transitions corresponding to the phase model in the state machine are added based on the status profile of the phase model from the core configuration. The state machine is the driving factor and not the status transition in IMG (*IMG Plant Maintenance and Customer Service Maintenance Service Processing Fiori Apps for Maintenance Processing Configure Overall Status Profiles*) as of SSAM2305.

The *USER_PERSONA, FEATURE_ID* and *PHASE_MODEL_RELEVANT* new fields have been added to the state machine table to indicate transitions specific to persona, feature, and whether they apply to a phase model only. For example, the highlighted status transition in the screenshot below allows a supervisor with the *Maintenance Technician Persona* role to not approve a work order transaction in the review status for an order type without a phase model when the *PM_SUPERVISOR_PHASE* model feature is enabled.



Make sure that all the state transitions marked *PHASE_MODEL_RELEVANT = X* are active when the phase model is enabled. For the *Phase + Non-Phase model*, check that all state transitions associated with *phase model = X* are enabled and active. Check also the non-phase model transitions and set them inactive according to your business requirements.

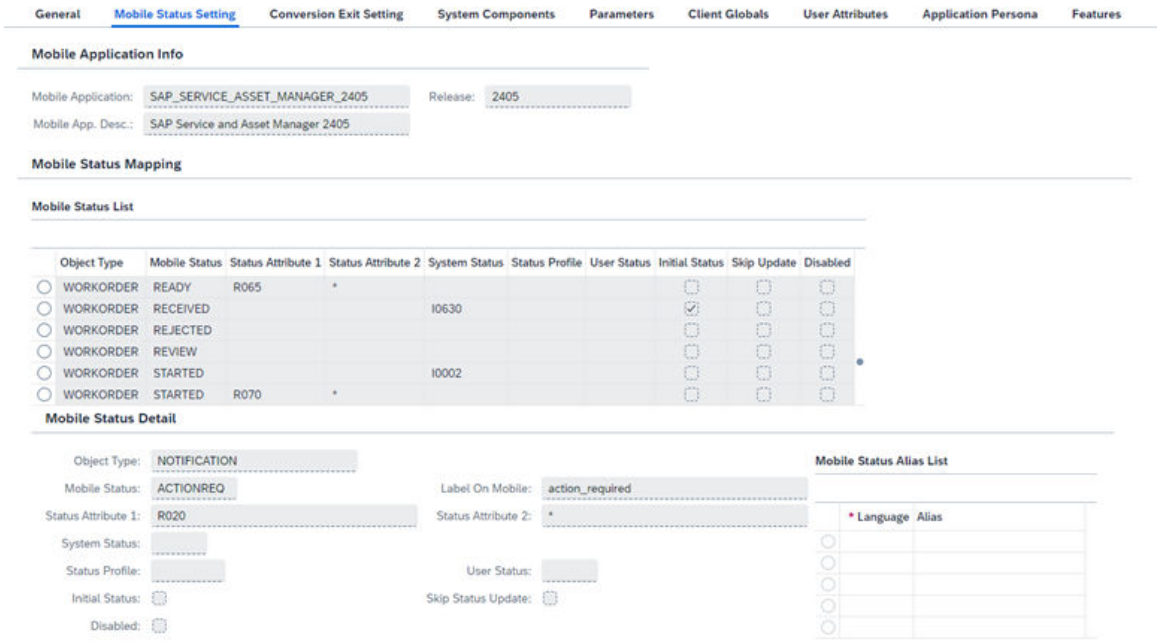
4.15.3.9 Mobile Status Mapping Configuration

The ConfigPanel shows you which PM mobile statuses are mapped to the phase model statuses.

From the main *ConfigPanel* page, click the *Mobile Application Configuration Mobile Status Setting* tab. Select your application from the *Defined Mobile Applications* list. Click the *Change* button to change the configuration.

The *Status Attribute 1* and *Status Attribute 2* fields are used to map statuses as follows:

- Status Attribute 1: Overall Status
- Status Attribute 2: Overall Status Profile
  If an asterisk (*) is present, this indicates any overall status profile.



Note

If you enable the phase model, activate the following mobile statuses by setting the *Status Attribute 1* and *Status Attribute 2* fields as indicated in the table. In an out-of-the-box installation, these statuses are active but the phase model is disabled by default.

Make sure that the following statuses are active when working with the *Phase + Non-Phase model*.

Mobile Status Mapping Configuration (specific to the phase model)

Object Type	Mobile Status	Status Attribute 1	Status Attribute 2	System Status
NOTIFICATION	ACTIONREQ	R020	*	
NOTIFICATION	COMPLETED Status is used in both phase model ON and OFF scenarios			I0072
NOTIFICATION	STARTED	R025	*	I0070
NOTIFICATION	STARTED Status is used in both phase model ON and OFF scenarios			I0070
NOTIFICATION	SUBMITTED	R005	*	
WORKORDER	COMPLETED	R075	*	
WORKORDER	DONE	R080	*	
WORKORDER	READY	R065	*	

Object Type	Mobile Status	Status Attribute 1	Status Attribute 2	System Status
WORKORDER	STARTED	R070	*	
WO_OPERATION	COMPLETED	R140	*	
WO_OPERATION	HOLD	R135	*	
WO_OPERATION	READY	R125	*	
WO_OPERATION	STARTED	R130	*	

Make sure that the following statuses are active when working with the Non-Phase model.

Mobile Status Mapping Configuration (specific to the non-phase model)

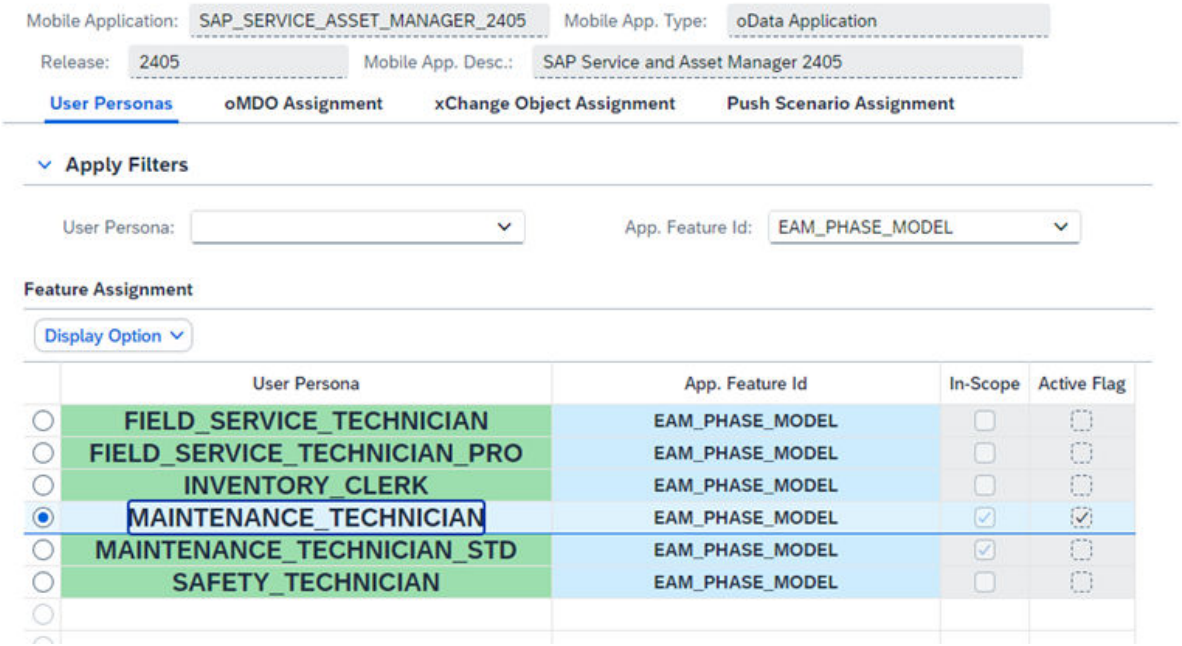
Object Type	Mobile Status	Status Attribute 1	Status Attribute 2	System Status
NOTIFICATION	COMPLETED Status is used in both phase model ON and OFF scenarios			I0072
NOTIFICATION	POSTPONE			I0069
NOTIFICATION	RECEIVED			
NOTIFICATION	STARTED Status is used in both phase model ON and OFF scenarios			I0070
TASK	COMPLETED			I0156
TASK	RECEIVED			
TASK	STARTED			I0155
TASK	SUCCESS			I0157
WORKORDER	COMPLETED			I0045
WORKORDER	RECEIVED			I0630
WORKORDER	REJECTED			
WORKORDER	HOLD			
WORKORDER	REVIEW			
WORKORDER	STARTED			I0002
WORKORDER	TRANSFER			
WO_OPERATION	COMPLETED			
WO_OPERATION	HOLD			
WO_OPERATION	RECEIVED			
WO_OPERATION	REJECTED			
WO_OPERATION	REVIEW			

Object Type	Mobile Status	Status Attribute 1	Status Attribute 2	System Status
WO_OPERATION	STARTED			
WO_OPERATION	TRANSFER			

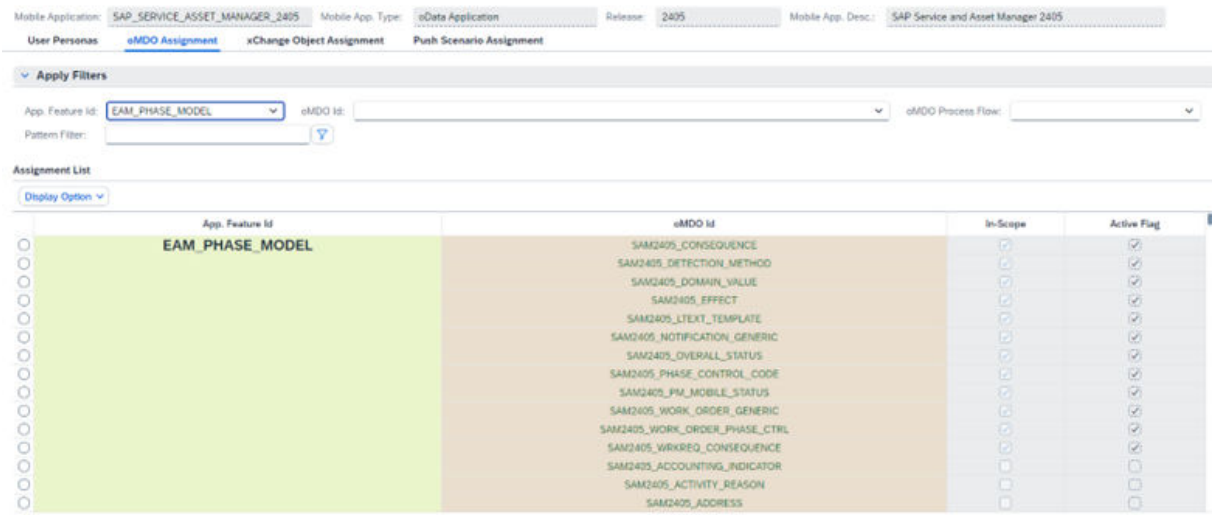
Save all the changes you have made.

4.15.3.10 Persona and Feature Enablement

The EAM phase model is added as a persona or feature assignment. When the phase model is enabled, the following persona or feature assignments must be enabled. The following settings are disabled by default, as shown in the figure.



When the *EAM_PHASE_MODEL* feature is active, data related to the phase model, such as *WorkRequestConsequence* or *Effect*, is downloaded during synchronization.



When the phase model is disabled, the mobile phone status in SSAM 2110 behaves the same as in the previous versions. However, in SSAM 2110, a status state machine has been added. For the corresponding configuration, follow the instructions in the following Emergency or Minor Work [page 378] topic.

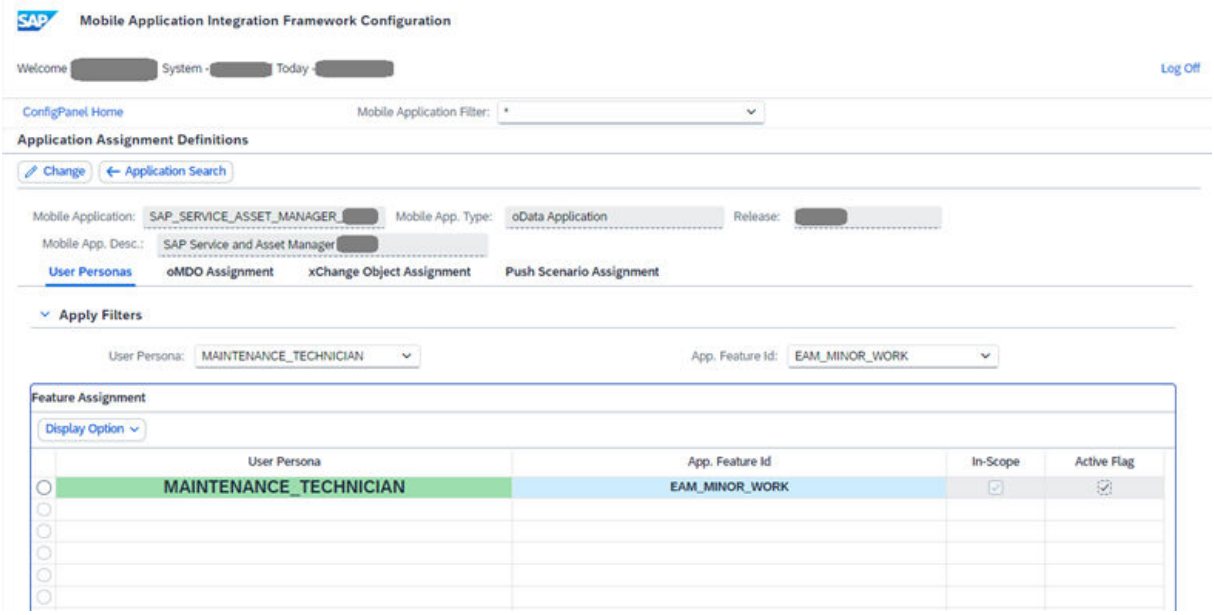
4.15.3.11 Emergency or Minor Work

This new feature is added to support emergency or minor work in the reactive maintenance phase model. It allows you to skip phases and issue a work order or notification when a technician is authorized to create these items.

> **Note**
>
> You can read and process notifications for both minor and emergency work. However, creating notifications is only supported for minor work.

Minor Work Notification

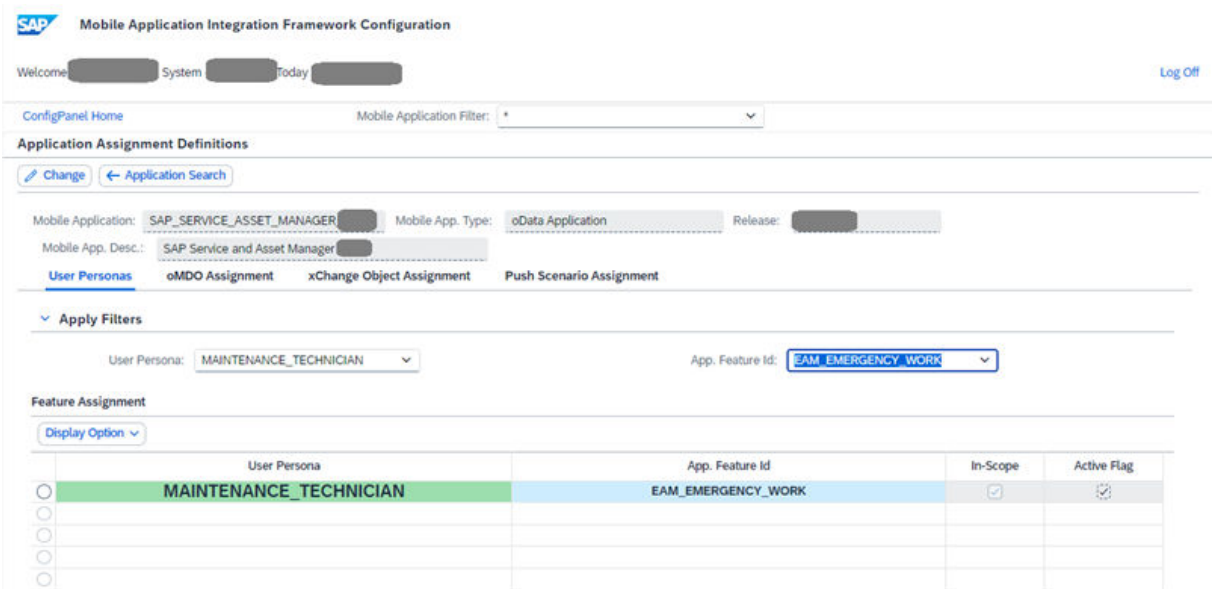
Feature: *EAM_MINOR_WORK*



- The *EAM_MINOR_WORK* and *EAM_EMERGENCY_WORK* features are created and assigned to the *NotificationProcessingContext* entity linked to the *NotifProcessingContext* property in the *MyNotificationHeaders* entity.
- The user must have authority (the *I_EXCP_MN* object: *Exception Process* > *Maintenance Notification*) to be able to create a notification with an exception process.

> **Note**
>
> The EAM_MINOR_WORK feature depends on EAM_PHASE_MODEL. Therefore, EAM_PHASE_MODEL must be active for the EAM_MINOR_WORK feature to work.

Emergency Work Notification
Feature: *EAM_EMERGENCY_WORK*



- The *OrderProcessingContext* property in the *MyWorkOrderHeader* entity drives the emergency WO creation/release.
- The user must have authority (the *I_EXCP_MN* object: *Exception Process* > *Maintenance Notification* and *I_EXCP_MO*: *Exception Process* > *Maintenance Order*) to be able to create an emergency work notification and related work order with an exception process.

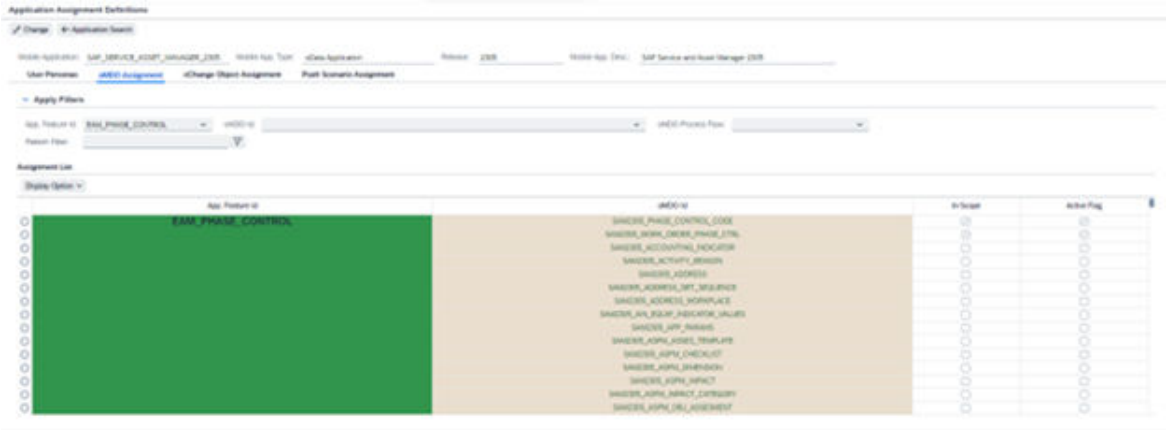
> **Note**
>
> The EAM_EMERGENCY_WORK feature depends on EAM_PHASE_MODEL. Therefore, EAM_PHASE_MODEL must be active for the EAM_EMERGENCY_WORK feature to work.

4.15.3.12 EAM Phase Control Code

The process control code can limit a certain process state change based on the system state. It can also be applied to the execution phase, which prevents the user from moving the order or operation from one sub-phase to another.

As for 2410 release:

- IMG backend configuration path is the following: *IMG* > *Logistics* > *General* > *Product Lifecycle Management (PLM)* > *Plant Maintenance and Customer Service* > *Maintenance and Service Processing* > *Fiori Apps for Maintenance Processing* > *General Settings* > *Define Phase Control Code for Maintenance Orders*
- The new feature *EAM_PHASE_CONTROL* is created to enable the EAM phase control code. To block the transition of an order or operation from one phase to another when the phase model feature is enabled. If the EAM_PHASE_CONTROL feature is active, the following entities are enabled.
  - PhaseControl
  - PhaseControlCode
  - PhaseControlKey
  - PhaseControlSystemMobileStatusMap
  - PhaseControlSystemStatus
  - WorkOrderOperationPhaseControl
  - WorkOrderPhaseControl
- This feature is active right out of the box. To disable it, refer to the feature configuration.



> **Note**
>
> For this feature to work, the *EAM_PHASE_MODEL* feature must be active in the SSAM application configuration.

> **Note**
>
> This feature is available for the S4CORE 106 and subsequent versions.

4.16 EPD Visualization Configuration

Prerequisites

1. Customize the EPD tenant. For more information, refer to the SAP Product Model View - Administration Guide guide.
2. Install and configure PMV. For more information, refer to the SAP Product Model Viewer overview.
3. Create SSAM sub-account and customize the mobile services application.
4. Create a visualization destination within the SAP Service and Asset Manager app. For more information, refer to the Configure the Mobile Application chapter of the *SAP Product Model Viewer Administration Guide*.

> **Note**
>
> For EPD visualization integration with the SAP Service and Asset Manager app to work properly, both the EPD and SAP Service and Asset Manager tenants must be set up in the same SAP BTP region.
>
> To preconfigure the SAP Product Model Viewer (PMV), refer to the Overview chapter of the *SAP Product Model Viewer Administration Guide*.

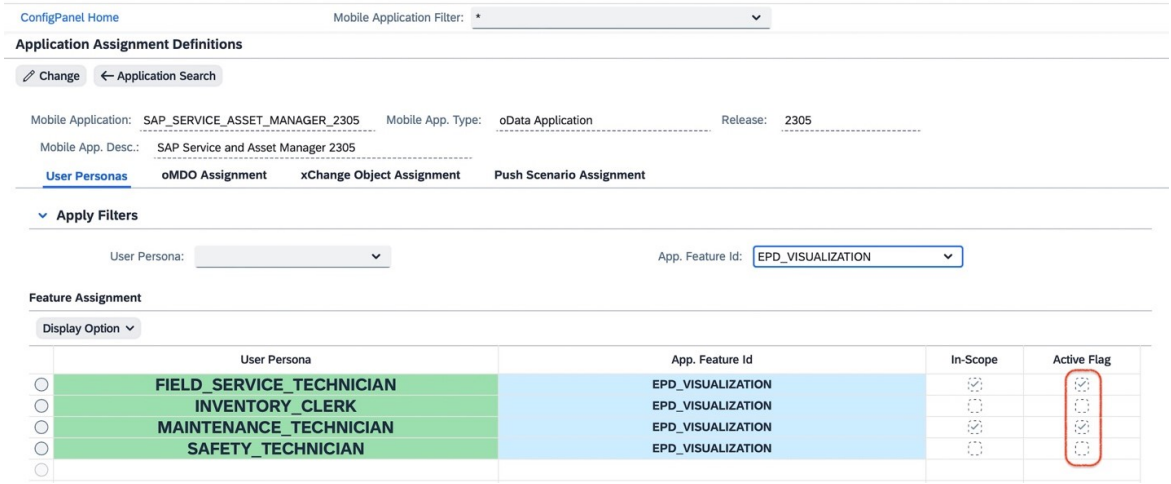
Context

EPD visualization in the SAP Service and Asset Manager is available by enabling the feature in the configuration panel. The feature is only available for the Maintenance Technician and Field Service Technician personas.

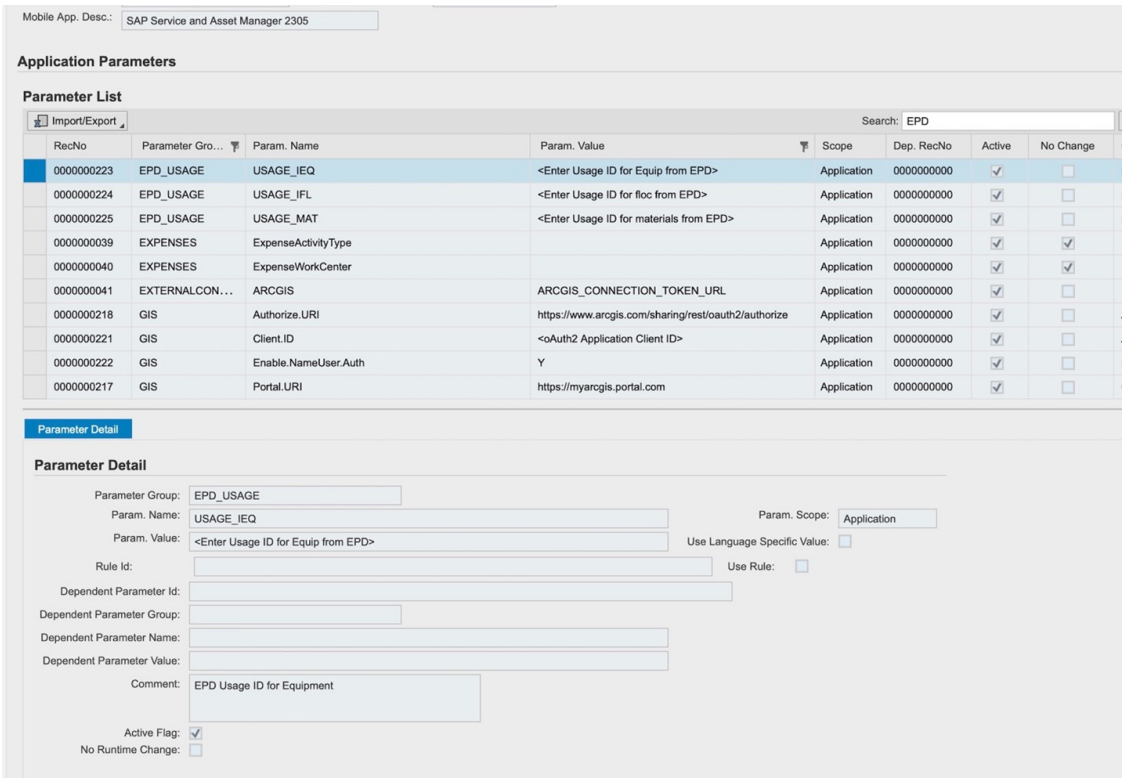
Procedure

1. To enable or disable the feature, check or uncheck the *Active Flag* box and save.

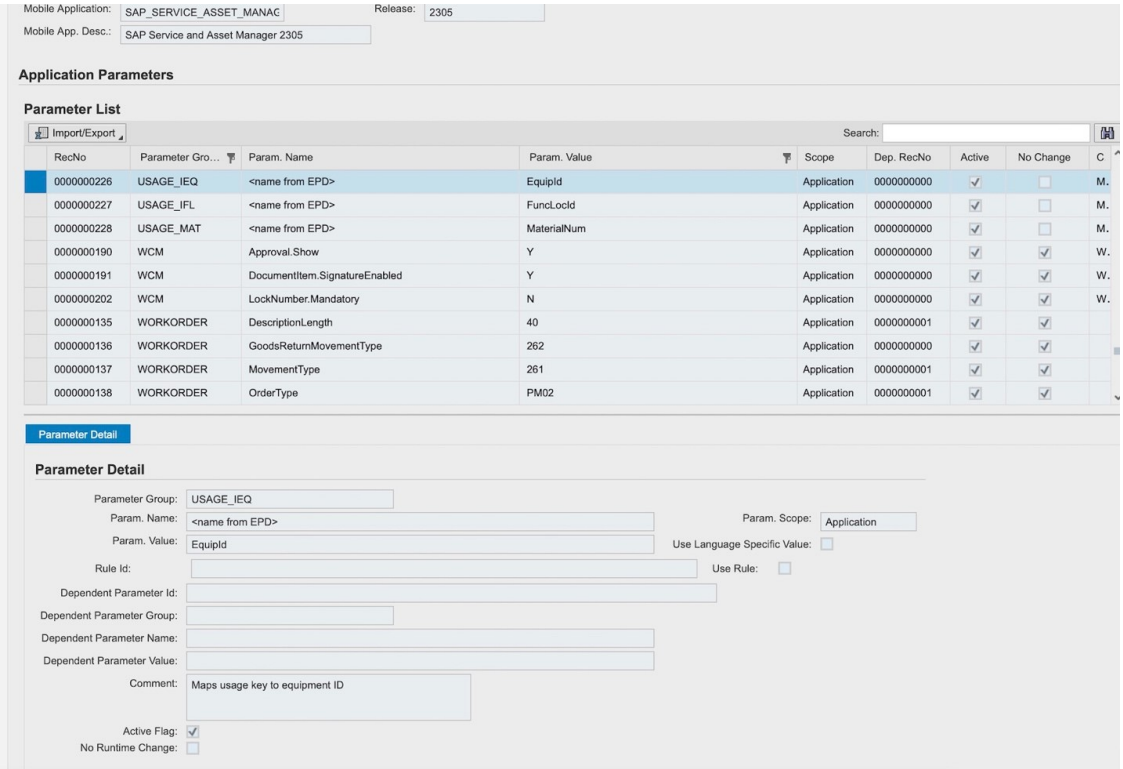
> **Note**
>
> By default, this feature is enabled in *Configuration Panel* > *Component Assignment* > *<Select Mobile Application>* > *User Personas tab*.



2. To use EPD visualization in the SAP Service and Asset Manager app,maintain the application parameters in the ConfigPanel. Navigate to *Application Configuration* > *<select Mobile Application>* > *Parameters tab* .
3. Depending on which object is configured in the EPD, choose an option:
    - **To maintain usage ID:** *Param. Value:* Usage ID for equipment/functional location/material from EPD (example values: *As-Maintained*/*As-Installed*/*As-Designed*)



    - To maintain key usage for objects:
        - **Param. Name:** Usage key from the EPD customization (ex: *Equipment_ID*/*FuncLocID*/*Material*)
        - **Param. Value:** Key field of the object or entity type. Note that *EquipID*, *FuncLocId*, and *MaterialNum* are configured by default.



4.17 Field Operations Worker Configuration

SAP Service and Asset Manager for Field Operations Worker uses the digital core with SAP S/4HANA for task driven activities and rounds. It supports workers who perform asset inspections and checks with focus on measurement points and on smaller services and repairs.

Field Operations Worker, or FOW, is an add-on component to SAP Service and Asset Manager. If you don't see FOW features while using the SAP Service and Asset Manager application, or in the ConfigPanel, your site hasn't installed the component.

Field Operations Worker adds the following functionality to the core SAP Service and Asset Manager application:

- **View routes data:** A route is comparable to a work order in the base SAP Service and Asset Manager application.
- **View stops data:** A stop in Field Operations Worker is comparable to an operation in the base SAP Service and Asset Manager application. A route is composed of one or more stops.
- **View asset information:** An asset in Field Operations Worker is comparable to a piece of equipment in the base SAP Service and Asset Manager application. Assets are located at an FOW stop.
- Use field data capture to take readings on measurement points. Measurement points are located on assets or a set of assets at a route stop.

4.17.1 Differentiating a Base SAP Service and Asset Manager Work Order from a Field Operations Worker Order

Creating rules based on order types affects synchronization processing and order downloads to the mobile devices of your users who use the Field Operations Worker component.

Prerequisites

Address the following before performing the procedure:

- The order types for work orders that are downloaded to technicians using the Field Operations Worker component are already determined.
- The person performing the procedure has access to the Config Panel and permissions to change settings.

Context

> **Note**
>
> Field Operations Worker orders are a subset of the base SAP Service and Asset Manager application work orders.

The following procedure modifies the synchronizing behavior of the SAP Service and Asset Manager application, along with the Field Operations Worker component. After you complete the procedure, only orders with a given order type of *PM02* are downloaded to the FOW component. In the procedure, you change the *ORDER_TYPE* filter in the OMDOs involved in order synchronization. Specifically, you add a rule to the filter in the **SAMXXXX_ROUTE** OMDO to include only the desired order type.

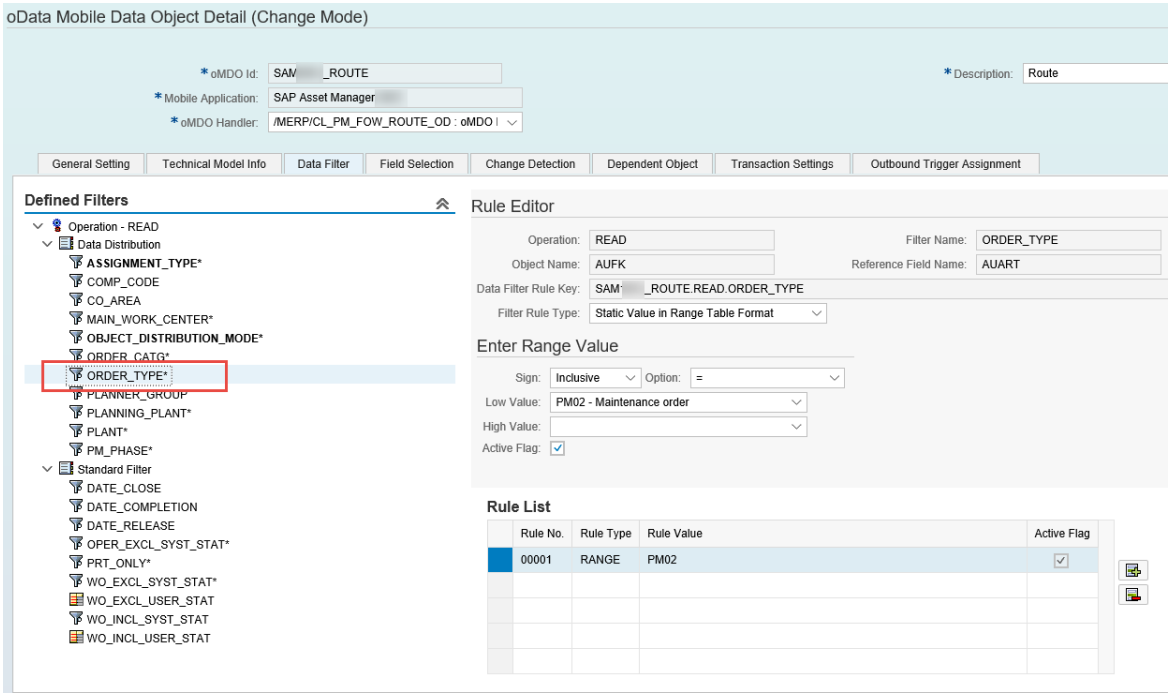
If you don't create a rule for the *PM02* order type, then that order type is excluded from work order download synchronization processing. If the FOW orders are excluded from synchronization processing, then the orders aren't present on the mobile clients of your users.

Procedure

1. Click the *OData Mobile Data Object Configuration* link, then click the *Data Filter* tab from the main ConfigPanel page. Be sure to have your desired mobile application chosen in the *Mobile Application Filter* field at the top of the page.

   Selecting an application filters the *OData Mobile Data Object by Mobile App* choices in the left panel with only OMDOs available in your application.
2. Expand the *OData Mobile Data Object by Mobile App* list on the left and click **SAMXXXX_ROUTE**.
3. Select the *Data Filter* tab.

4. Click the *Operation - READ* > *Data Distribution* > *ORDER_TYPE* node in the *Defined Filters* list.
5. Create a rule using the following parameters if the rule doesn't already exist:
   - **DOF Rule Type:** Static Value in Range Format
   - **Sign:** Inclusive
   - **Option:** =
   - **Low Value:** PM02 - Maintenance order
   - Ensure the *Active Flag* box is checked



6. Influence Field Operations Worker orders using the following filters found in *Operation - READ* > *Standard Filter* if needed:
   - WO_EXCL_SYST_STAT
   - WO_EXCL_USER_STAT
   - WO_INCL_SYST_STAT
   - WO_INCL_USER_STAT
7. *Save* your changes.

Results

After you finish the procedure, both Field Operations Worker orders and base SAP Service and Asset Manager work orders are downloaded by the SAP Service and Asset Manager application.

4.18 FSM Crew Configuration

With the FSM Crew integration, technicians can perform the following activities, depending on their assigned role (Crew *Lead* or *Member*):

- Access their crew members' assigned Service Orders, Items, Operations from the SAP Service and Asset Manager Homescreen.
- Access information about their crews, crew schedule and crew members.
- In the SAP Service and Asset Manager application, Crew Leads can update the Service Orders' status by changing the mobile status to *Start*, *Travel*, *On-site* or *Complete*.

> ⓘ Note
>
> For more information about using the FSM Crew Integration, see Working with FSM Crew (S4).

Supported Personas

This feature is applicable for the following personas:

Field Service Technician (Standard)
Field Service Technician (Pro)

Limitations

The FSM Crew integration is **only** supported in the SAP S/4HANA Service scenario [page 205].

> ⓘ Note
>
> For the Customer Service (CS) scenario [page 177], use the Crew Management [page 31] feature.

Configuration

Perform the following configuration step(s):

1. Configuring FSM Crew Integration - Back End - Enabling the Feature [page 409]
2. Configuring FSM Crew Integration - Back End - oMDO [page 410]

4.18.1 Configuring FSM Crew Integration - Back End - Enabling the Feature

Context

For detailed information about the FSM Crew Integration, see the overview topic, FSM Crew Configuration [page 408].

The below procedure describes how to enable the feature in the Configuration Panel.

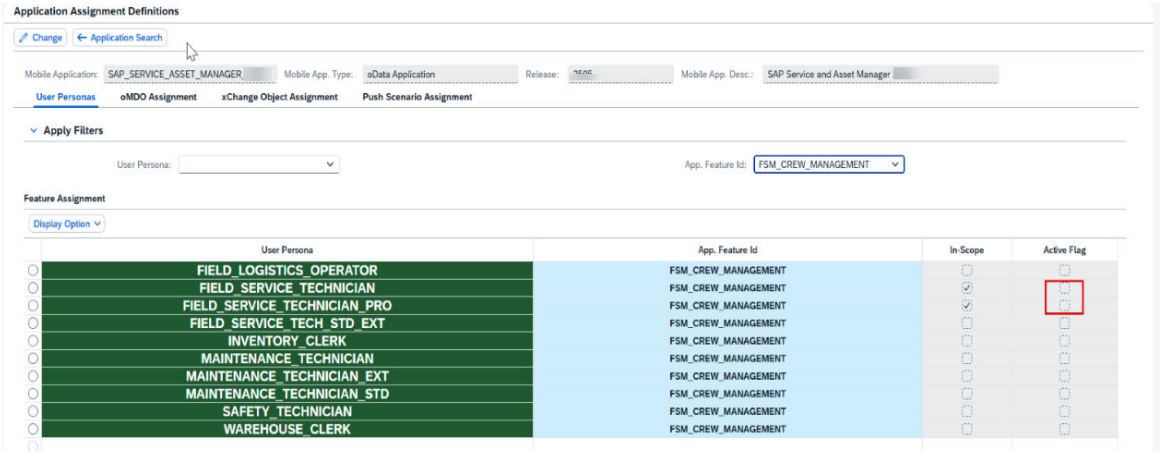
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **Enabling and disabling features**: refer to Configuring Features in *MAIF Configuration Guide*.

Procedure

1. In the *Config Panel*, go to *Component Assignments*.
2. Select the application with correct version from the list.
3. Select the *FSM_CREW_MANAGEMENT* as *App. Feature Id*, enter *Change Mode* and set the feature to *Active* for the relevant persona(s).



4. Save your changes.

4.18.2 Configuring FSM Crew Integration - Back End - oMDO

Context

For detailed information about the FSM Crew Integration, see the overview topic, FSM Crew Configuration [page 408].

For the FSM Crew Integration to work, configure oMDO filters as described in the procedure below.

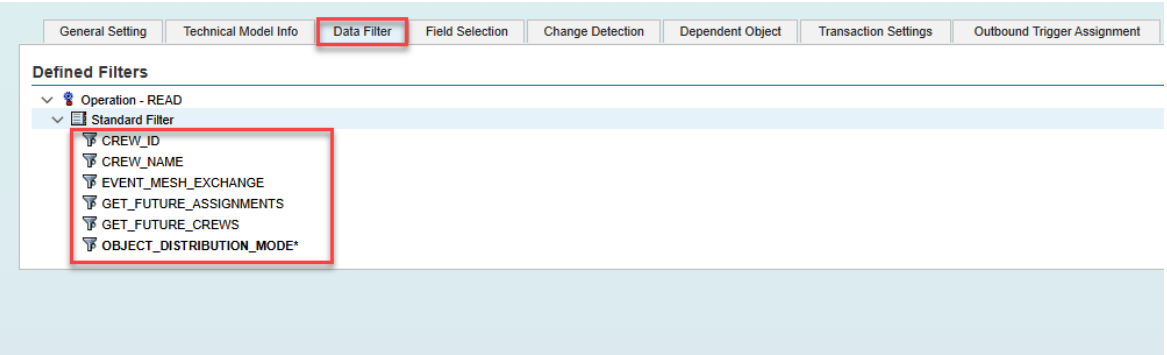
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **OMDO** and **OMDO filter** configuration: refer to OData Mobile Data Object Configuration and OData Mobile Data Object Configuration - Data Filter Tab in *MAIF Configuration Guide*.

Procedure

1. In the *Config Panel*, go to *oData Mobile Data Object Configuration*.
2. On the left, select the oMDO *SAMXXXX_S4_SRV_FSM_CREW* with the correct version and go to the *Data Filter* tab.
3. Enter *Change Mode* and configure the following data filters:



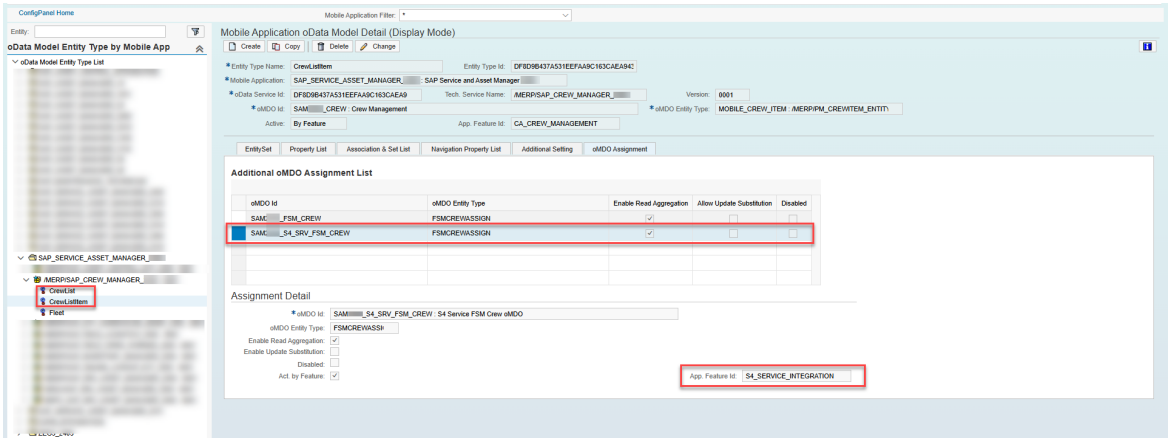
- *OBJECT_DISTRIBUTION_MODE*:
  - The default value for this filter is *1 – oMDO Filter*. Currently **only this value is supported**.
  - This filter ensures that the Crew data is downloaded based on the filter values specified in the oMDO.
- *GET_FUTURE_ASSIGNMENTS*:
  - If this filter is configured to *True*, Crew assignments with start dates in the future (i.e., after the current date) will **also be downloaded**.
- *GET_FUTURE_CREWS*:
  - If this filter is configured *True*, Crews with start dates in the future (i.e., after the current date) will **also be downloaded**.
- *EVENT_MESH_EXCHANGE*:

- The default value for this filter is *False*.
- For this configuration, there will be a call to Field Service Management at every sync to determine if there is any change to the **Crew** and/or **Crew Assignments**. If the filter is configured to *True*, the changes to the Crew will be captured in the MAIF exchange tables and calls will be made to Field Service Management **only** to download the delta records when changes are captured in the exchange tables. The pre-requisite to set this filter to *True* is that the Event Mesh Framework must be set up and configured.

  > **Note**
  >
  > In SAP Service and Asset Manager **2505** version, Crew Exchange via the Event Mesh is **not supported**.

- *CREW_ID* and *CREW_NAME*: These can be configured with specific Crew IDs and/or Crew Names.

4. *Save* your changes.
5. In the *Config Panel*, go to *oData Model Configuration*.
6. On the left, select your application with the correct version and make sure that for both the *CrewList* and *CrewListItem* oData entities, the *SAMXXXX_S4_SRV_FSM_CREW* oMDO **is enabled** by the feature *S4_SERVICE_INTEGRATION*.



4.19 FSM Crowd Service Configuration

With SAP Field Service Management Crowd Workforce, you can find additional technician manpower in real-time using the SAP Field Service Management Crowd Marketplace.

If you are using SAP Field Service Management Crowd Workforce for external technicians, you can use SAP Service and Asset Manager to download Service Orders assigned to these external technicians via the FSM Planning and Dispatching Board.

> **Note**
>
> - In this scenario, neither the external crowd user nor the Customer Identity provider will exist in the SAP back end system.
> - For more information about FSM Crowd Workforce, refer to Field Service Management - Crowd Workforce in *SAP Field Service Management documentation*.

Supported Personas

This feature is applicable for the following persona(s):

Maintenance Technician (External)
Field Service Technician (External)

> **Note**
>
> This feature is specifically created for external workers within your organization, and supported by the **External** Maintenance and Field Service Technician personas. For more information, see:
>
> - Mobile User Essential Authorizations
> - Configuring FSM Crowd Service - Back End - Enabling the Feature [page 417]
> - Maintenance Technician Persona Overview (Standard, Professional, External)
> - Field Service Technician Persona Overview (Standard, Professional, External)

Limitations

- In the SAP Service and Asset Manager application, external technicians can **only read** objects and **cannot edit or delete** them through the standard application UI. To **add, edit, or update** the status of Work Orders and Operations, they must use a **Dynamic Form or a FSM Smartform**.

  > **Note**
  >
  > For more information about SAP Dynamic Forms and FSM Smartforms, refer to the SAP Dynamic Forms documentation and Smartforms Overview.

- The Maintenance Technician **External** and Field Service Technician **External** personas **cannot** be used with other personas. Users may be assigned only one of these personas and must not be assigned any additional personas.
- Features that can be enabled by *User Authorization Parameters* are **not supported**, except the *Enable.FSMSmartform.Edit* app parameter. This parameter determines whether external technicians can edit FSM Smartforms on the mobile client. For more information, see Enabling and Disabling Features Per User Through SAP Authorization [page 102].
- The *PM_CONFIRMATION* feature is **not supported**.
  - **Maintenance Technician (External):** Users can only post their time by the *HR_TIMESHEET* feature (see CATS and PM Confirmation Time Entries Configuration [page 314]).
  - **Field Service Technician (External):** Users will not be able to post their time; neither *S4_SERVICE_CONFIRMATION* nor *HR_TIMESHEET* is available.
- For the Field Service Technician (External) persona, FSM Crowd Service Integration is supported **only** in the CS (Customer Service) back end [page 177].

Prerequisites

The following prerequisite configurations must be in place before SAP Service and Asset Manager can be configured to work with FSM Crowd users:

- The Crowd Workforce functionality must be configured and working in FSM. Refer to Crowd Workforce in *SAP Field Service Management documentation*.
- The Integration between S/4HANA Service and SAP FSM must be configured. Refer to Integration with SAP Field Service Management in *SAP S/4HANA documentation*.
- This scenario assumes that the FSM Crowd technicians are not provisioned into the Customer Identity provider. Therefore, the crowd technicians need to be provisioned into SAP IAS. Follow the *Field Service Management documentation* for provisioning users from FSM to SAP IAS.

> **Note**
>
> A trust connection needs to be established between the BTP subaccount and SAP IAS. For more information, refer to Trust and Federation with Identity Providers in *SAP Business Technology Platform documentation*.

Configuration

Perform the following configuration steps:

1. Configuring FSM Crowd Service - BTP Mobile Services Connectivity [page 413]
2. Configuring FSM Crowd Service - Back End - Enabling the Feature [page 417]
3. Configuring FSM Crowd Service - Back End - oMDO [page 418]

4.19.1 Configuring FSM Crowd Service - BTP Mobile Services Connectivity

Context

For detailed information about FSM Crowd Service, see the overview topic, FSM Crowd Service Configuration [page 411].

When an FSM Crowd user connects from SAP Service and Asset Manager to BTP Mobile Services, they will authenticate against BTP Mobile Services using their email and password that has been provisioned from SAP FSM into SAP IAS. However, since the Crowd user does not exist in the SAP back end, the user cannot be propagated to the back end using the Principal Propagation set up. Follow the steps below for establishing connectivity between the BTP Mobile Services and the SAP back end system.

General Links

If necessary, see the following links for additional information for the required steps included in this procedure:

- SAP Mobile Services product page
- Cloud Connector in *SAP BTP Connectivity* documentation

Procedure

1. Create a **Technical User** in the SAP back end system. This user must have:
   - *User Type* set to '*S*' (*Service*).
     - A user of the type *Service* is a dialog user that is available to an anonymous, larger group of users.
     - During logon, the system does not check for expired and initial passwords. Only the user administrator can change the password.
     - Multiple logons are allowed.
   - All the authorizations for a SAP Service and Asset Manager mobile user as specified in the SAP Service and Asset Manager Security Guide.

     > **Note**
     >
     > Since the Technical User is being used by the SAP Service and Asset Manager mobile user, necessary authorizations are required for the user to:
     > - Download master and transactional data needed on the device.
     > - Upload updates from the SAP Service and Asset Manager application.

   - The authorization object */MERP/CST* assigned (either via custom role or authorization object directly).

     > **Note**
     >
     > Authorization Object */MERP/CST* is associated with the Maintenance Technician (External) and Field Service Technician (External) personas in the *ConfigPanel* > *Mobile Application Configuration* > *Select Mobile App* > *Application Persona* tab (see Enabling the Feature [page 417]).

   - The necessary *SU3* user parameters for downloading the relevant data to SAP Service and Asset Manager (e.g. Maintenance Plant, WorkCenter, etc.). For more information, see User Parameter IDs [page 606].

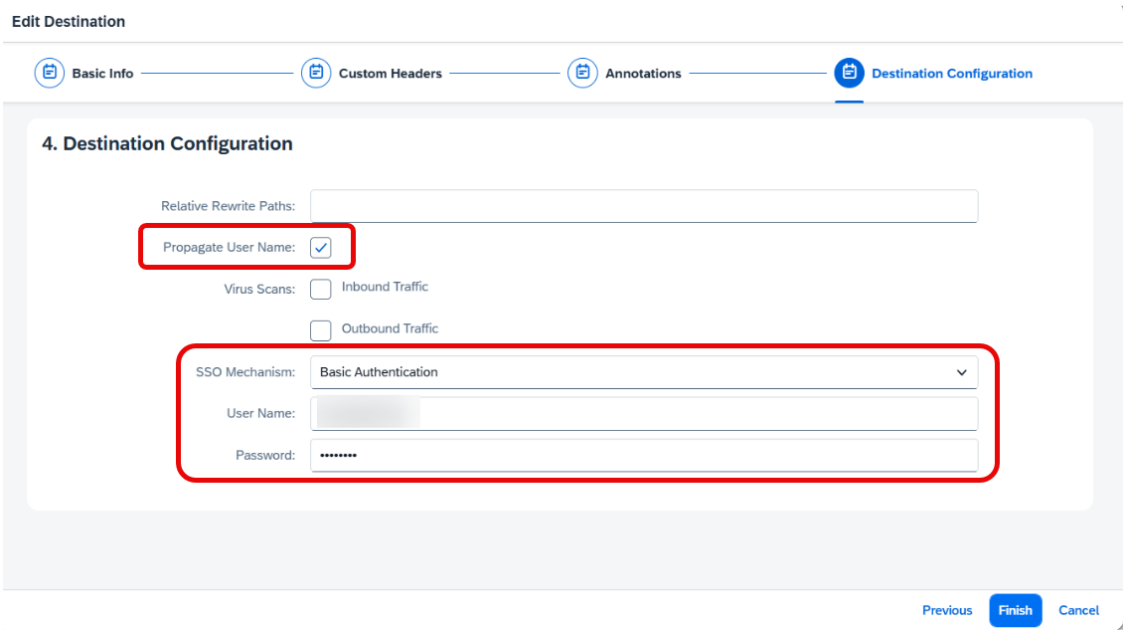
   > **Note**
   >
   > All the transactions in the back end will be logged against this Technical User.

2. Configure your existing Cloud Connector to propagate a Technical User to the SAP back end. Refer to the SAP Cloud Connector documentation for steps to perform this activity.
3. Create a mobile application in SAP BTP using the *App Create* program. For detailed information, follow the steps in Create an SAP Mobile Services App for the SAP Service and Asset Manager Mobile App.

> **Note**
>
> For more information, see Using the SAP Business Technology Platform Mobile Services App Creator to Create an Application.

4. Once the application is created in BTP Mobile Services, you must apply the following changes to the mobile destinations:

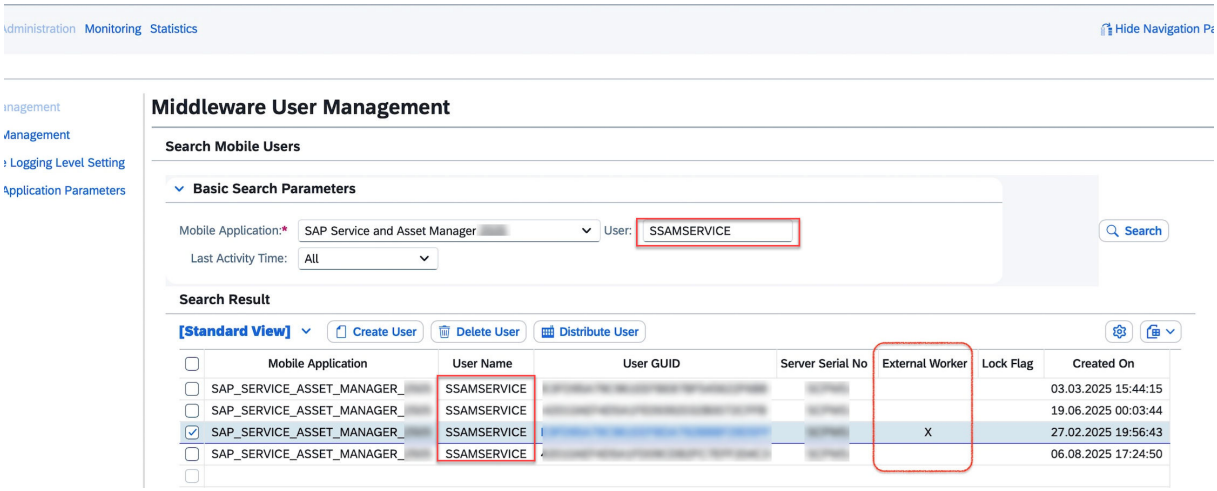
    1. Navigate to the app in BTP Mobile Services and select the *Connectivity* settings.
    2. Make the following changes to **both** the Online and Offline destinations under the *Destination Configuration* section:
        1. Make sure that the *Propagate User Name* checkbox is checked.
        2. Change the *SSO Mechanism* to *Basic Authentication* and update the *Technical Username* and *Password* fields.



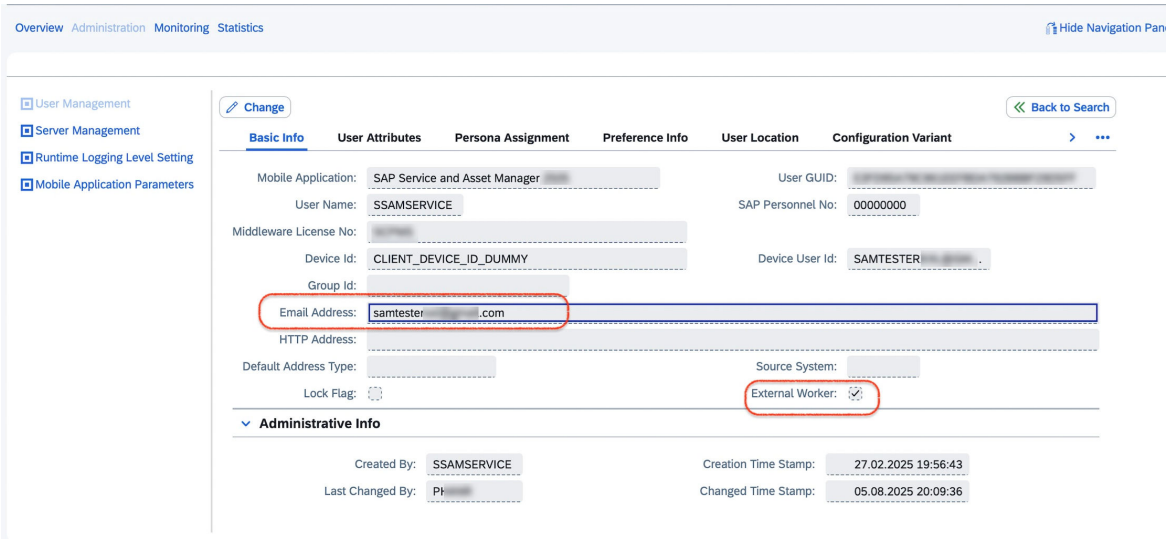
> **Note**
>
> - If you have multiple partner companies that require different data sets, then you need to perform the steps above for **each** partner company.
> - If you want to utilize both Maintenance Technician and Field Service Technician External personas in your environment, for **each** persona you need to create:
>   - Separate **SAP BTP apps**.
>   - Separate **Technical Users** in the back end.
> - It is recommended to use role-based authorization in Persona configuration (instead of authorization object-based as in standard configuration) and create different custom role - one for each external persona and assign the role to the corresponding Technical User (see Mobile User Essential Authorizations).

Results

In the SAP Service and Asset Manager application, external workers will log in using their email address; however, when connecting to the SAP back end, they will be connected using the Technical User configured above [page 414]. In the Admin Portal, you can access these users as follows:



- If multiple external workers are configured in FSM, you will see multiple user records for a single Technical User, each associated with different email addresses.
- From these records, the email addresses configured in FSM as **crowd resources**, will have the *External Worker* flag checked automatically:



> **Note**
>
> From 2505 version, in *Admin Portal* > *Administration* > *User Management*, the *External Worker* flag is available to identify external workers in your organization.

Next Steps

Continue with Configuring FSM Crowd Service - Back End - Enabling the Feature [page 417].

4.19.2 Configuring FSM Crowd Service - Back End - Enabling the Feature

Context

For detailed information about FSM Crowd Service, see the overview topic, FSM Crowd Service Configuration [page 411].

The below procedure describes how to enable the *FSM_CROWD_INTEGRATION* feature and the *MAINTENANCE_TECHNICIAN_EXT*, *FIELD_SERVICE_TECH_STD_EXT* personas in the ConfigPanel.

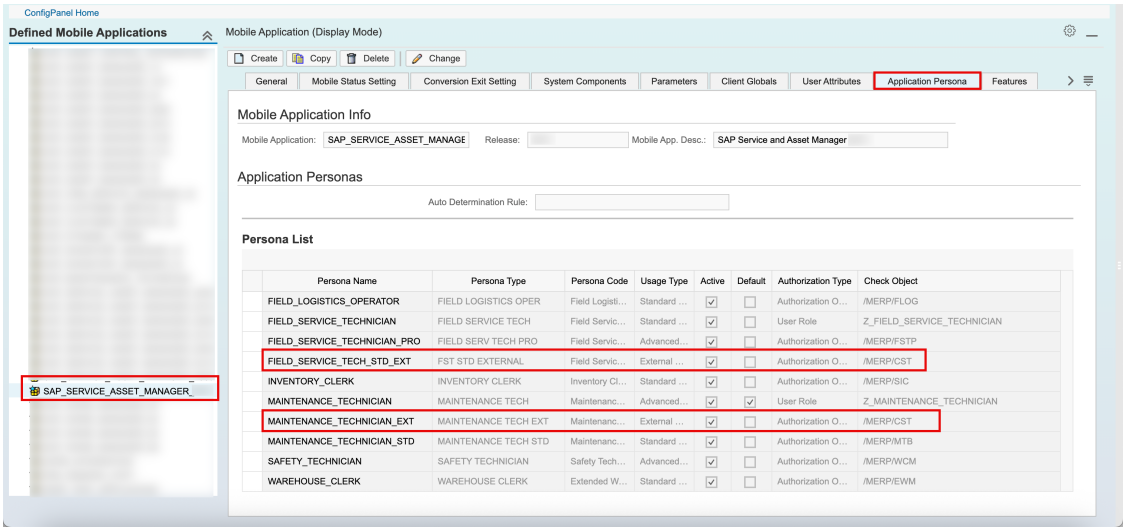
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **Enabling and disabling features**: refer to Configuring Features [page 93].

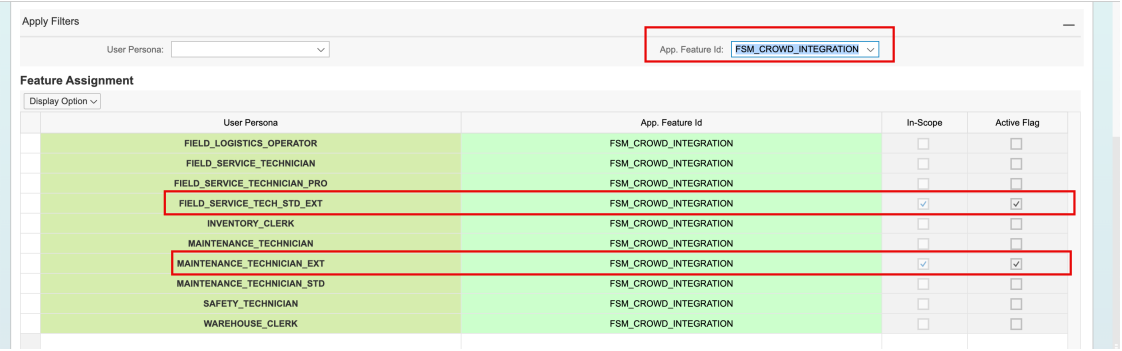
Procedure

1. Perform the baseline configuration for SAP Service and Asset Manager and FSM integration as described in Field Service Technician Configuration on a Customer Service Back End [page 177].
2. External personas (*MAINTENANCE_TECHNICIAN_EXT*, *FIELD_SERVICE_TECH_STD_EXT*) have been created for the Crowd Technician. Make sure that at least one of these personas is active for the relevant Mobile Application version of SAP Service and Asset Manager:
    1. On the *Config Panel*, go to *Mobile Application Configuration*.
    2. Select the application with correct version from the left and go to the *Application Persona* tab.
    3. Enter *Change Mode* and set the *MAINTENANCE_TECHNICIAN_EXT* and/or *FIELD_SERVICE_TECH_STD_EXT* personas to *Active*.



> **Note**
>
> By default, these personas will be active. However, if they are not, you must activate them.

3. Assign the authorization object */MERP/CST* to the Technical User(s) you have already created in Configuring FSM Crowd Service - BTP Mobile Services Connectivity [page 413].
4. Make sure that the *FSM_CROWD_INTEGRATION* feature is active for the *MAINTENANCE_TECHNICIAN_EXT* and/or *FIELD_SERVICE_TECH_STD_EXT* personas:
    1. On the *Config Panel*, go to *Component Assignments*.
    2. Select the application with correct version from the list.
    3. Select the *FSM_CROWD_INTEGRATION* as *App. Feature Id*, enter *Change Mode* and set the feature to *Active* for the *MAINTENANCE_TECHNICIAN_EXT* and/or *FIELD_SERVICE_TECH_STD_EXT* personas.



> **Note**
>
> By default, this feature will be active for the *MAINTENANCE_TECHNICIAN_EXT* and *FIELD_SERVICE_TECH_STD_EXT* personas. However, if it is not, you must activate it.

Next Steps

Continue with Configuring FSM Crowd Service - Back End - oMDO [page 418].

4.19.3 Configuring FSM Crowd Service - Back End - oMDO

Context

For detailed information about FSM Crowd Service, see the overview topic, FSM Crowd Service Configuration [page 411].

For the FSM Crowd Service feature to work, perform the following OMDO filters configuration.

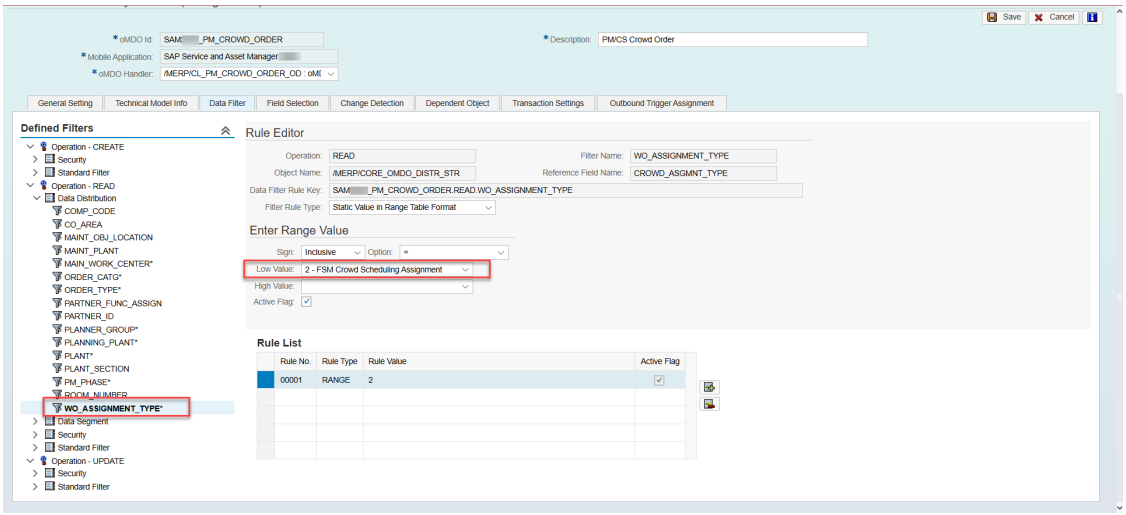
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **oMDO** and **oMDO filter** configuration: refer to OData Mobile Data Object Configuration and OData Mobile Data Object Configuration - Data Filter Tab in *MAIF Configuration Guide*.

Procedure

1. On the *Config Panel*, go to *oData Mobile Data Object Configuration*.
2. On the left, select either of the following oMDOs with the correct version and go to the *Data Filter* tab:
   - *SAM<VERSION>_PM_CROWD_ORDER* - Maintenance Technician (External) persona
   - *SAM<VERSION>_S4_CROWD_ORDER* - Field Service Technician (External) persona
3. Enter *Change Mode* and configure the following data filters:
   1. *ASSIGNMENT_TYPE*: set the data filter to *2 - FSM Crowd Scheduling Assignment*.



   2. Configure any other filters provided within the oMDO as per your business requirements.

4.20 FSM Smartforms Configuration for Maintenance Technician

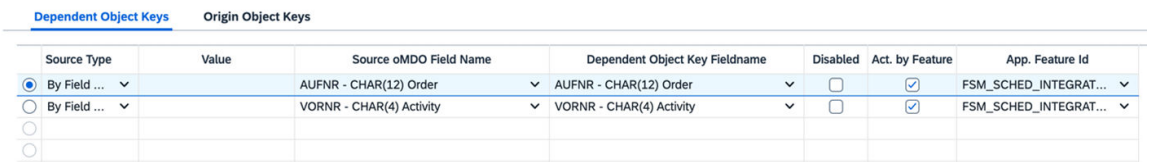
FSM Smartforms can be used in plant maintenance scenarios with SAP Service and Asset Manager. In this case, FSM Smartforms will be attached to PM work order operations instead of CS and S/4 work orders.

Context

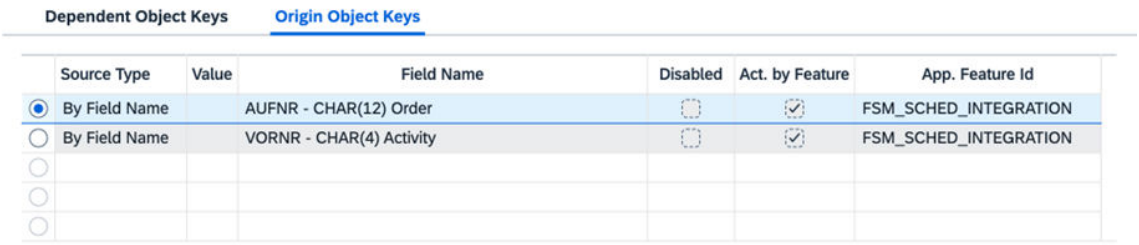
You must perform the prerequisite configuration steps to integrate the SAP backend with Field Service Management Scheduling. For more information, see the SAP Service and Asset Manager Integration with Field Service Management Scheduling [page 178] documentation, but ignore the Configuring the Field Service Management Personas section.

Procedure

1. On the ConfigPanel main screen, click *Component Assignments* > *SAP_SERVICE_ASSET_MANAGER_XXXX* > *User Personas*. If desired, you can filter only the *MAINTENANCE_TECHNICIAN* user persona.
2. Click *Change*.
3. Check the *Active Flag* for *FSM_SCHED_INTEGRATION*.
4. Click *Save*.
5. Navigate to the ConfigPanel main screen.
6. Navigate to *oData Mobile Data Object Configuration* > *SAP_SERVICE_ASSET_MANAGER_XXXX* > *SAMXXXX_WORK_ORDER_GENERIC* > *Dependent Object*.
7. Click *Change* and *Add Dependent Object*.
8. In the *Object Detail* section, enter the following:
   - Source Technical Entity Type = WOOPERATION
   - Dependent oMDO Id = SAMXXXX_FSM_FORM_INSTANCE
   - Dependent Technical Entity Type = FSMFORMINSTANCE
   - Key Calculation Mode = Source Entity Type Output + Target Entity Type Client State
   - Act. by Feature = checked
   - App. Feature Id = FSM_SCHED_INTEGRATION
9. In the *Dependent Object Keys* section, enter the information as shown below.



10. In the *Origin Object Keys* section, enter the information as shown below.



11. Click *Save*.
12. From the Administrator Portal, assign the MAINTENANCE_TECHNICIAN persona to the appropriate users.

4.21 Geospatial Service Definitions

Geospatial Services provide the technology to create, analyze, maintain and distribute geospatial data and information.

In SAP Service and Asset Manager you can use either GIS (Geographic Information System) or GEF (Geographical Enablement Framework).

> **Note**
>
> - You **cannot** use both services at the same time in SAP Service and Asset Manager.
> - Esri base maps are the only base maps supported for the app.

Any procedures in this section describe configuration procedures of Geospatial Services specific to the SAP Service and Asset Manager application. For application-agnostic procedures, see the following documents in the *MAIF Configuration Guide*:

- Geospatial Service Definitions - GEF
- Geospatial Service Definitions - GIS

> **Note**
>
> When you work as the Maintenance Technician persona, work orders, equipment, and functional locations with geocoded addresses (`/MFND/GISGEOCODE`) don't appear on the map.
>
> To resolve this issue, you need:
>
> - BAS/Visual Studio Code with SAM MDK Project
> - `patch` command (available on BAS and macOS by default) via terminal or other patching utility
>
> Before you begin, read the guidelines on how to apply the patch and review the appendix section if you receive any errors.
>
> 1. Download the attached file `3629554.patch`.
> 2. Save the patch file to a known location.

3. Run the following command in the base metadata folder:

```
patch -p1 <
          /path/to/3629554.patch
```

4. Validate that four files changed and no hunk failures occurred.
5. Republish the application.

Geographic Information System (GIS)

A geographic information system (GIS) integrates hardware, software, and data for capturing, managing, analyzing, and displaying all forms of geographically referenced information.

Your mobile application has custom map controls with GIS functionality implemented using MAIF / Mobile Development Kit and Open UI extensions. The SAP Service and Asset Manager application is delivered with predefined globals that are Esri-specific, however, you can point to any GIS vendor you choose.

> ⓘ Note
>
> See Geographic Information System (GIS) [page 425].

Geographic Enablement Framework (GEF)

Geographical Enablement Framework (GEF) works as the foundation to extend business data with geometric attributes for MAIF / SAP S/4HANA. GEF is integrated directly into your system.

As a framework leveraging the spatial capabilities inherent on the MAIF / SAP S/4HANA platform, it enables organizations to develop geospatially enriched business data, and make them accessible from within your mobile application.

Your mobile application uses the geometries (points, lines, and polygons) from the GEF geotables stored in MAIF / SAP S/4HANA for the geo-enabled objects in the application. The application also uses the business layers, including the symbology, from GEF. Users can view and work with base maps and feature layers on the device.

> ⓘ Note
>
> See Geographical Enablement Framework (GEF) [page 433].

User Authorization through ArcGIS

As of version 2405, SAP Service and Asset Manager supports individual user authentication using named user authentication with the ArcGIS Identity.

ArcGIS services and resources are secured using token-based authentication. You can implement user authentication workflows in your application to obtain an access token and make secure requests.

User authentication is a set of authentication workflows that allow users with an ArcGIS account to sign in to the application and access ArcGIS content, services, and resources. The typical authentication protocol used is OAuth 2.0. When you signs into the application with your ArcGIS account, an access token is generated that authorizes the application to access services and content on your behalf. The resources and functionality available depend on the user type, roles, and privileges of the user's ArcGIS account.

> **Note**
>
> See ArcGIS [page 423].

4.21.1 ArcGIS

ArcGIS is Esri's comprehensive geospatial platform. ArcGIS services and resources are secured using token-based authentication. You can implement user authentication workflows in your application to obtain an access token and make secure requests.

User authentication is a set of authentication workflows that allow users with an ArcGIS account to sign in to the application and access ArcGIS content, services, and resources. The typical authentication protocol used is OAuth 2.0. When you signs into the application with your ArcGIS account, an access token is generated that authorizes the application to access services and content on your behalf. The resources and functionality available depend on the user type, roles, and privileges of the user's ArcGIS account.

OAuth 2.0 is a methodology that is recommended for authorizing ArcGIS users from the application. The ArcGIS platform follows the OAuth 2.0 protocols to authenticate the user, and a token is provided to the application. This token is used in subsequent requests to secure resources.

Depending on the request, in the OAuth 2.0 workflow, when an access token is issued to a user, an update token is issued along with it. The access token has a short lifetime and expires soon. The application can use the refresh token to obtain a new access token without asking for the your credentials.

Before configuring your ArcGIS functionality, be sure to activate the following features:

- CA_GEOSPATIAL_INFO_SERVICE

For detailed information on activating a feature, see the topic and subtopics.

Follow the steps required to implement ArcGIS Identity with your application using OAuth 2.0 authentication using the ArcGIS - Implementing User Authentication [page 423] procedure.

4.21.1.1 ArcGIS - Implementing User Authentication

Context

Implementing user authentication in ArcGIS requires three main steps. The first is to register the client application with ArcGIS. Then you'll perform a multi-step process to set up and configure the OAuth workflow.

Procedure

1. **Register the client application with ArcGIS:** In the OAuth flow, it is important the the application is registered with ArcGIS. Registration prevents malicious applications from stealing user data. OAuth 2.0 APIs will only redirect you to a registered URL to prevent redirection attacks where an authorization or access token can be intercepted by an attacker.
   a. Add the application as a portal item.
   b. Register the portal item, the application, as an application by providing a redirect URI.
   c. Obtain and note the app ID and app secret.
2. **Authenticate the user (new user or user with an invalid update token):** This step gets an authorization code from ArcGIS
   a. Send a request to the OAuth2 authorization endpoint in ArcGIS.

   Source Code

   ```
   client_id = <app ID of the client app registered with ArcGIS>
   &redirect_uri = <redirect URI specified when registering the client app
   with ArcGIS>
   &response_type = code
   ```

   Note

   If the App ID is invalid or the Redirect URI is not specified in ArcGIS for the registered application (App ID), ArcGIS will not return an authorization code.

   If AGO, send an OAuth request to https://www.arcgis.com/sharing/rest/oauth2/authorize .

   For examples, refer to https://developers.arcgis.com/rest/users-groups-and-items/authorize/ , follow the Explicit Grant workflow.

   b. At the ArcGIS prompt, log in as either an embedded or corporate user.

   If the login is successful, the authorization code is sent back to the redirect URI in the request.
3. **Obtain an access token and a refresh token:** You'll need the authorization code you got in the previous step. Send a request to the OAuth2 token endpoint.

   Source Code

   ```
   client_id = <app ID of the client app registered with ArcGIS>
   &redirect_uri = <redirect URI specified while registering client app with
   ArcGIS>
   &code = <authorization code from the previous step>
   &grant_type = authorization_code
   ```

   Note

   If the App ID is invalid or the Redirect URI is not specified in ArcGIS for the registered application (App ID), ArcGIS will not return an authorization code.

   If AGO, send an OAuth request to https://www.arcgis.com/sharing/rest/oauth2/token/ .

   A successful response will be sent back to the redirect URI in the request. The response will include an access token and a refresh token.

For examples, refer to https://developers.arcgis.com/rest/users-groups-and-items/token.htm .

4. **Use the access token:** The access token is needed to use and update your protected ArcGIS resource. The access token has a short lifespan. You can use a refresh token to obtain a new access token. This method means the user does not have to provide ArcGIS login credentials. Use the substeps to make one of the following choices:

   - Obtain a new access token by using the refresh token
   - Obtain a new refresh token by exchanging an existing refresh token

   a. Obtain a new access token by using the refresh token. Send a request to the OAuth2 token endpoint.

   ```
   client_id = <app ID of the client app registered with ArcGIS>
   &refresh_token = <refresh token from the previous step>
   &grant_type = refresh_token
   ```

   b. Obtain a new refresh token by exchanging an existing refresh token. Send a request to the OAuth2 token endpoint.

   ```
   client_id = <app ID of the client app registered with ArcGIS>
   &redirect_uri = <redirect URI specified while registering client app with
   ArcGIS>
   &refresh_token = <refresh token from the previous step>
   &grant_type = exchange_refresh_token
   ```

> ### Note
>
> For examples, refer to https://developers.arcgis.com/rest/users-groups-and-items/token/ .

4.21.1.2 Geographic Information System (GIS)

A geographic information system (GIS) integrates hardware, software, and data for capturing, managing, analyzing, and displaying all forms of geographically referenced information.

Your mobile application has custom map controls with GIS functionality implemented using MAIF / Mobile Development Kit and Open UI extensions. The SAP Service and Asset Manager application supports ESRI GIS out of the box and, as such, is delivered with predefined globals that are Esri-specific.

Before configuring your GIS functionality, be sure to activate the following features:

- CA_GEOSPATIAL_INFO_SERVICE
- CA_GIS_ADD_EDIT

For detailed information on activating a feature, see the topic and subtopics.

For information about configuring GEF, see the subtopics located in the Geographical Enablement Framework (GEF) [page 433] topic.

4.21.1.2.1 Configuring Your Map Settings

Some GIS settings are standard in your MAIF / SAP S/4HANA application.

You can change any of the settings described in this topic to configure the application for your site.

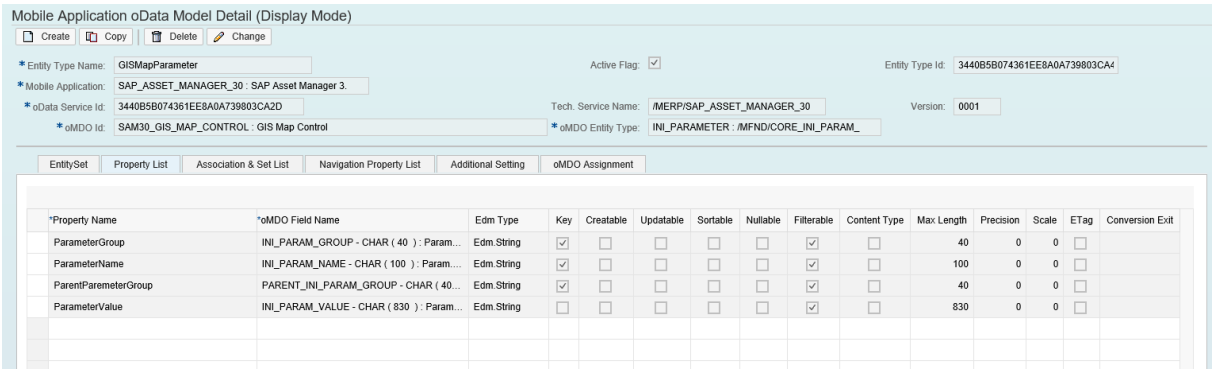
> **Note**
>
> You can also change the map setting metadata through the Mobile Development Kit. Note that if there are metadata differences, Mobile Development Kit changes override ConfigPanel changes.

OData Model Configuration - Property List Tab

In the ConfigPanel, the *GISMapParameter* entity type contains the following properties:

- ParameterGroup
- ParameterName
- ParentParameterGroup
- ParameterValue

Use the fields in the following section to properly categorize these parameters.



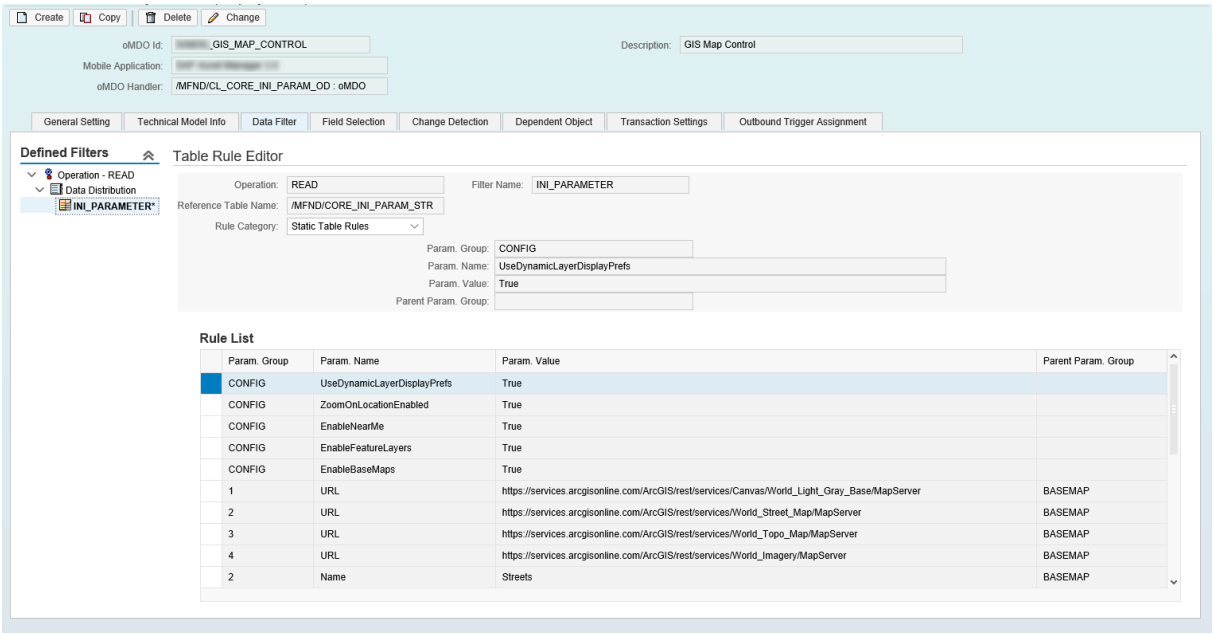
OData Mobile Data Object Configuration - Data Filter Tab

From the ConfigPanel Home page, navigate to *OData Mobile Data Object Configuration* > *Data Filter Tab* > *<APP_VERSION>_GIS_MAP_CONTROL* > *Operation - READ* > *Data Distribution*. Click the *Change* button.

The following parameters are standard:

- **CONFIG:** Parameter Group
- **BASEMAP:** Parent Parameter Group
- **FEATURELAYER:** Parent Parameter Group

See the following for an example screenshot of the parameters in the ConfigPanel in the *Data Filter* tab, and a table representing how to configure the parameters in the tab.



Parameter Group	Parameter Name	Parameter Value	Parent Parameter Group	Description
1	URL	<https://>	BASEMAP	Basemap URL
2	Name	Text value	BASEMAP	Basemap display name
1	Filename	<filename.tpk>	BASEMAP	Offline filename for basemap
1	Name	Text value	FEATURELAYER	Display name of feature layer
1	URL	<https://>	FEATURELAYER	Feature layer URL
1	Properties	**Example** { "ID": "{objectid}", "Title": "{metamorphic_facies}", "HeadlineText": "{geomodifications}", "Subhead": "{comments}" }	FEATURELAYER	Feature layer properties/ attributes to display in object cell. Map properties to `ObjectCell`fields
1	Actions	[]	FEATURELAYER	Array of actions to run for this feature layer.

Parameter Group	Parameter Name	Parameter Value	Parent Parameter Group	Description
CONFIG	`EsriClientID`	<Enter Esri License Key>		Esri runtime license string. **Note** For more information about how to get license to ESRI ClientID, see ArcGIS Developers documentation.
CONFIG	`EsriAPIKey`	<Enter ESRI API Key>		**Note** You can find your ESRI API Key on the dashboard in your ArcGIS developer account. For more information and API Key description, see ArcGIS Developers documentation.
CONFIG	`UseDynamicLayerDisplayPrefs`	TRUE/FALSE		Use layer visibility setting from each dynamic layer (business layer) as default.
CONFIG	`ZoomOnLocationEnabled`	TRUE/FALSE		Set to true if the map must zoom to current location when location is toggled on.
CONFIG	`EnableNearMe`	TRUE/FALSE		Enable near me feature
CONFIG	`EnableFeatureLayers`	TRUE/FALSE		Enable display of feature layers.
CONFIG	`EnableBaseMaps`	TRUE/FALSE		Enable display and switching of basemaps.
CONFIG	`EnableDynamicLayers`	TRUE/FALSE		Enable display of dynamic layers (business layers)

Parameter Group	Parameter Name	Parameter Value	Parent Parameter Group	Description
CONFIG	`EnableCurrentLocation`	TRUE/FALSE		Enable display of current location.
CONFIG	`DefaultNearMeRadius`	<number>		Default value of near me radius if Near Me feature is enabled in EnableNearMe parameter.
CONFIG	`DefaultNearMeUnits`	Mi/KM		Default value of near me radius unit if Near Me feature is enabled in EnableNearMe parameter.
CONFIG	`RoutingURL`	The following is an example of a URL put into your server ID: `https://utility.arcgis.com/usrsvcs/servers/<ID of server>/rest/services/World/Route/NAServer/Route_World`		Routing URL to be set if Field Operations Worker component (FOW) is enabled.
CONFIG	`GefUIProfileId`	<profile ID value as set in GEF config>		GEF profile id
CONFIG	`EnableGef`	TRUE/FALSE		Enable GEF as map data provider.

4.21.1.2.2 Configuring Your GIS Mapping Table

Use the /SMFND/GIS_OIDMAP_UPLOAD_PROG program to upload object values to the /SMFND/OID01_GS mapping table.

- **SPATIAL_OBJECTID:** Esri field

  > **Note**
  >
  > You can maintain either the SPATIAL_OBJECTID field or the SPATIAL_GUID field, or both. However, it is recommended that you maintain the SPATIAL_OBJECTID field.

- **SPATIAL_GUID:** Esri field
- **OBJKEY:** SAP key (for example, FLOC or EQ, depending on OBTYP)
- **OBJECT_GROUP / OBJECT_GROUP1:** SAP fields that allow for extra attributes or segregation

4.21.1.2.3 Supporting Authenticated GIS Services

You can view token-based authenticated basemaps and feature layers on the mobile client. Use the ConfigPanel to configure the client ID and client secret strings.

The mobile client retrieves the tokens. The client ID and client secret are supplied to the client so each client can generate their tokens for accessing authenticated services.

If your organization wishes to access Esri application-level authenticated GIS services, configure your application as shown in the following procedure.

You can also configure a proxy through Esri. Authenticated basemaps and feature layers are requested through a local proxy. The proxy manages the generation and use of tokens based on the client ID and client secret. For more information on configuring a proxy, see the Esri documentation, Working with Proxy Services .

To turn on GIS authenticated services in the ConfigPanel, add the following rule:

1. From the ConfigPanel *Home* page, navigate to *OData Mobile Data Configuration* > *OData Mobile Data Object List* > *Data Filter Tab* > *<Mobile Application>* > *<Mobile Application>_GIS_MAP_CONTROL* > *Operation - READ* > *Data Distribution* > *INI_PARAMETER*.
2. Click the *Change* button. In the *Rule List* section, click the *Add* button to add a new rule. The rule gives you the freedom to retrieve your client credentials in a manner appropriate for your organization:
   - **Parameter Group:** `AUTHENTICATION`
   - **Parameter Name:** `ConfigRule`
   - **Parameter Value:** `/<Mobile Application>/Rules/Path/To/A/Rule.js`
     The specified rule must return a json object in the form of the following example. Be sure to replace the text in the sample code with your actual client ID and client secret (`"YourClientId"` and `"YourClientSecret"`):

     Sample Code

     ```
     {
         "ClientId": "YourClientId",
         "ClientSecret": "YourClientSecret"
     }
     ```

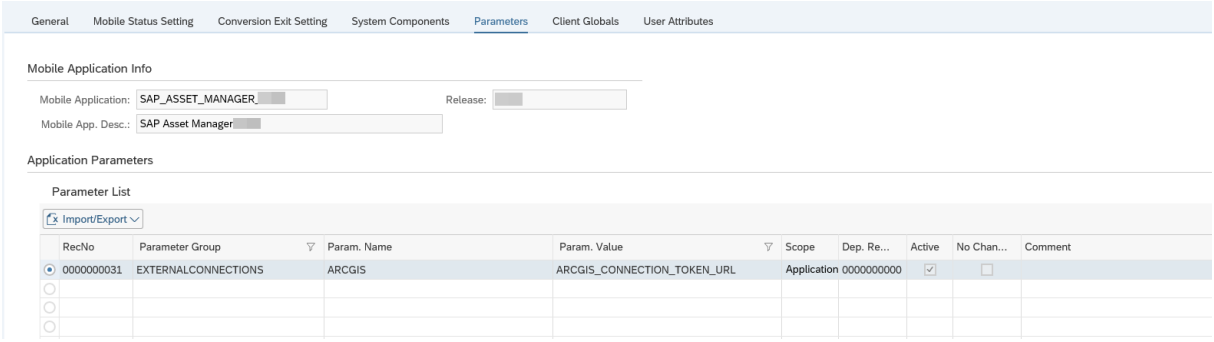
4.21.1.2.4 Creating and Configuring an RFC Destination for Offline Maps

Establish an oAuth connection using a secure TokenID to request offline maps information from the ArcGIS server.

Context

The oAuth 2.0 client ID and secret for your connection are stored in the RFC destination. Maintain the RFC destination in the app parameters in the ConfigPanel.

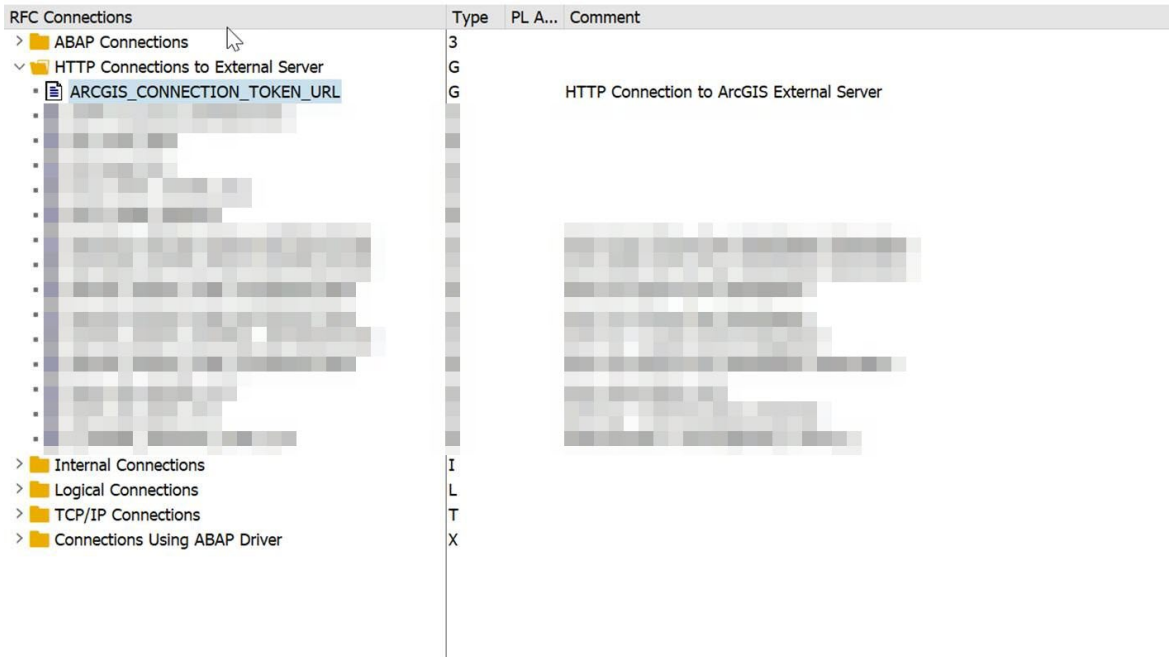
See the following screenshot for the parameter that is included in your mobile application:



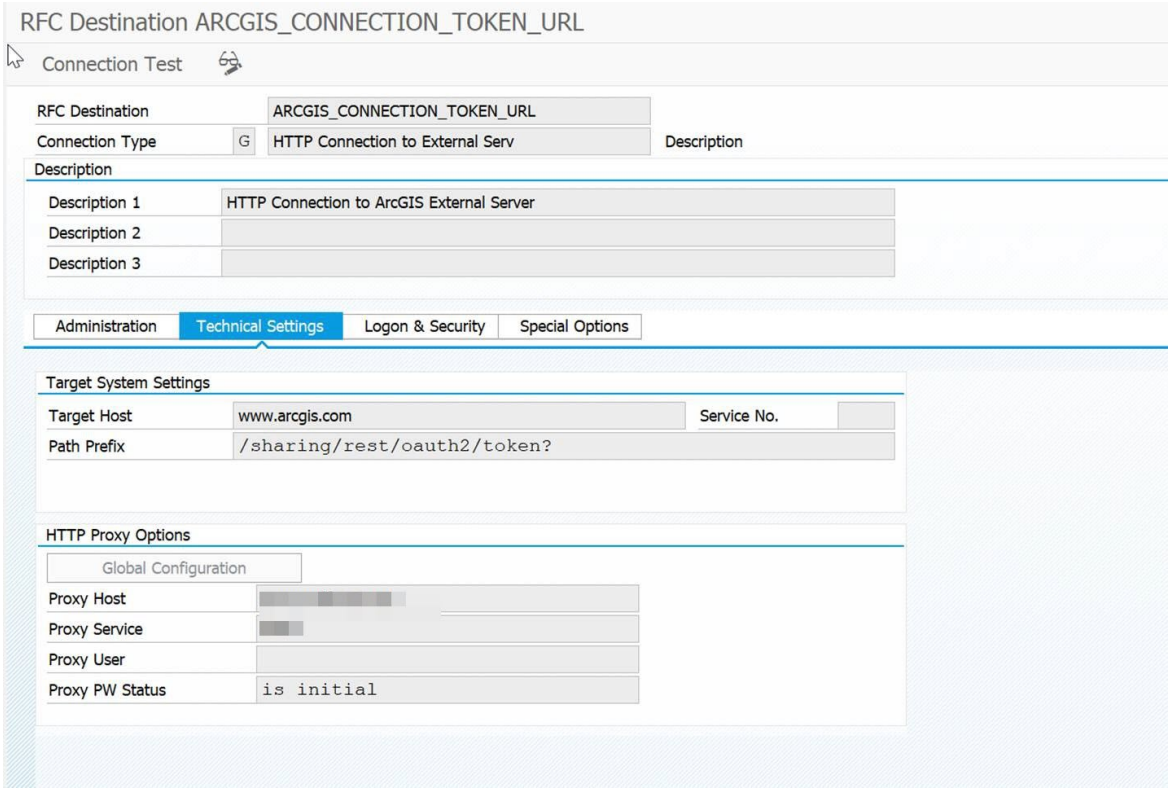
The *OauthTokens* entity set is provided out of the box to use for the RFC destination set in the *Parameters* tab. Use the following procedure to create the *ARCGIS_CONNECTION_TOKEN_URL* RFC destination in your backend system:

Procedure

1. Using the SAP GUI enter transaction *SM59* and enter *ARCGIS_CONNECTION_TOKEN_URL*, the new RFC destination.



2. From the *Technical Settings* tab of your new RFC connection, set the *Target Host* to match the ArcGIS server URL. Find the information for the `Target Host` field in the `Service Host` field on the *General Data* tab of the *Geospatial Service Definitions* page in the ConfigPortal. Set the *Path Prefix* to `/sharing/rest/oauth2/token?`.
3. If necessary, configure the proxy that you're using to allow your back end systems to connect to the internet.



4. Click the *Logon & Security* tab. Under *Logon Procedure*, select *Basic Authentication*. In the *User Name* field, enter the client ID. In the *Password* field, enter the client secret.
5. In the *Security Options* section of the *Logon & Security* tab, ensure that the SSL is set to *Active*.
6. Select your SSL certificate from the *SSL Certificates* list.
7. *Save* the connection and perform a connection test.

   If the connection is configured correctly, a 200 HTTP response is returned.
8. Import the SSL certificate and ensure its active using transaction code *STRUST*.

4.21.1.2.4.1 Configuring Offline GIS Metadata

Create a new rule in the SAP Service and Asset Manager metadata to retrieve a valid authentication token for authenticated resources within the map control.

Context

To create a new rule for offline GIS, see the existing rule found in the metadata file of your application at `/<MobileApplicationName>/Rules/Extensions/TokenRequest.js`. The rule found there uses an online oData request to get the token from the back-end server. This rule is the recommended way to retrieve a token from the Esri oAuth service.

Procedure

1. Navigate to the metadata of your project using your preferred text editor or the SAP Business Application Studio and create a new rule.
2. Save the rule you created.
3. Open the `.page` file that contains your map control using your preferred text editor.
4. Navigate to the *Controls* section and locate the control for the map. The map control has the following specific properties:
   - *Type* of *Control.Type.Extension*
   - *Module* of *Extension-MapFramework*
5. Add a *TokenAuthentication* object within the *ExtensionProperties* object of the control. Add an *Action* property of a rule to retrieve a valid authentication token as shown in the following example:

   Sample Code

   ```
   {
            "_Type":"Control.Type.Extension",
            "Module": "extension-MapFramework",
            "Control":"MapExtensionWithContext",
            "Class":"MapExtensionWithContext",
            "_Name":"MapExtensionControl",
            "ExtensionProperties": {
                 …
                   "TokenAuthentication": {
                                  "Action": "/path/to/rule/that/returns/a/
   token"
                   },
                 …
            }
       }
   ```

6. Save the page and update your application with the new metadata.

Results

The new metadata allows token authentication on your ArcGIS map when required.

4.21.1.3 Geographical Enablement Framework (GEF)

Geographical Enablement Framework (GEF) works as the foundation to extend business data with geometric attributes for MAIF / SAP S/4HANA. GEF is integrated directly into your system.

As a framework leveraging the spatial capabilities inherent on the MAIF / SAP S/4HANA platform, it enables organizations to develop geospatially enriched business data, and make them accessible from within your mobile application.

Your mobile application uses the geometries (points, lines, and polygons) from the GEF geotables stored in MAIF / SAP S/4HANA for the geo-enabled objects in the application. The application also uses the business

layers, including the symbology, from GEF. Users can view and work with base maps and feature layers on the device.

> **Note**
>
> Esri base maps are the only base maps supported for the app.

Before configuring your GEF functionality, be sure to activate the following features:

- CA_GEOSPATIAL_INFO_SERVICE

For detailed information on activating a feature, see the topic and subtopics.

For detailed information about GEF, including installation and implementation procedures, see the Geographical Enablement Framework documentation.

For information about configuring GIS, see the subtopics located in the Geographic Information System (GIS) [page 425] topic.

4.21.1.3.1 Disabling GIS

Your application utilizes GIS by default. When implementing GEF, ensure that GIS is disabled in the ConfigPanel.

1. From the ConfigPanel home page, navigate to *Geospatial Service Definitions*. Select your application release using the *Mobile Application Filter*. Expand the *Geospatial Mobile Services by App* tree in the left panel.
2. Uncheck the *Active* boxes from the following services:
   - *<APPXX>_GIS_QUERY_EQUIPMENT*
   - *<APPXX>_GIS_QUERY_FLOC*
   - *<APPXX>_GIS_QUERY_NOTIFICATION*
   - *<APPXX>_GIS_QUERY_WORKORDER*

4.21.1.3.2 Configuring Your Map Settings - GEF

Some GEF settings are standard with your initial application.

You can change any of the settings described in this topic to configure the application for your site.

> **Note**
>
> You can also change the map setting metadata through the SAP Business Application Studio. Note that if there are metadata differences, SAP Business Application Studio changes override ConfigPanel changes.

Before enabling GEF, deactivate GIS if you previously had it activated. See the Disabling GIS [page 434] topic for more information.

Geospatial Service Definitions - General Data Tab

1. From the ConfigPanel home page, navigate to *Geospatial Service Definitions*. Select your application release using the *Mobile Application Filter*. Expand the *Geospatial Mobile Services by App* tree in the left panel.
2. Check the *Active* boxes from the following services:
   - *<APPXX>_GEF_QUERY_EQUIPMENT*
   - *<APPXX>_GEF_QUERY_FLOC*
   - *<APPXX>_GEF_QUERY_NOTIFICATION*
   - *<APPXX>_GEF_QUERY_WORKORDER*

   > **Note**
   >
   > If you are using custom GEF services, enable those rather than the standard GEF services.
3. *Save* your changes.

Geospatial Service Definitions - Parameters Tab

If you've mapped a custom business object to a GEF scenario using *SPRO* in the SAP GUI, you must also map the connection in the Config Panel.

1. From the Config Panel home screen, navigate to *Geospatial Service Definitions* > *Parameter Settings tab*. Select your application release, then select the GEF service you've customized in the *Geospatial Services by Mobile App* list.
2. Click the *Change* button.
3. In the *Operation Parameter Settings* section, navigate to *Parameters for Service Operation* > *Provider Operation - QUERY* > *Standard Parameter* > *Parameter - EAM Scenario*.
4. In the *Value Setting* section, change the *Parameter Value* to your custom business object.
5. *Save* your changes.

OData Mobile Data Object Configuration - Data Filter Tab

1. From the ConfigPanel Home page, navigate to *OData Mobile Data Object Configuration* > *Data Filter Tab* > *<SAMXX>_GIS_OBJECT_DATA* > *Operation - READ* > *Standard Filter* > *GEOSERVICE_ID*. Click the *Change* button.
   Ensure that any GIS objects are inactive. Ensure that the following objects are active:
   - *<APPXX>_GEF_QUERY_EQUIPMENT*
   - *<APPXX>_GEF_QUERY_FLOC*
   - *<APPXX>_GEF_QUERY_NOTIFICATION*
   - *<APPXX>_GEF_QUERY_WORKORDER*

> ⓘ Note
>
> If you have any custom OMDOs for GEF, enable those. If you have any custom OMDOs for GEF, enable those, rather than the standard GEF OMDOs.

2. While still on the *Data Filter* tab with the *<SAMXX>_GIS_OBJECT_DATA* selected, navigate to *Operation - READ* > *Data Distribution* > *GIS_ASSIGNMENT_TYPE*.
   Ensure the *Range Value* is set to *2 - GEF Integration*.
3. By default, all basemaps are maintained. GEF uses information coming from MAIF / SAP S/4HANA GEF APIs. When you activate GEF, all GIS configuration is invalid. Configure the following parameters for GEF:
   While still on the *Data Filter* tab, navigate to *<SAMXX>_GIS_MAP_CONTROL* > *Operation - READ* > *Data Distribution* > *INI_PARAMETER*.
   Ensure that the following parameters found in the *CONFIG* parameter group are configured for GEF:
   - **GefUIProfileID**: Standard configuration is *EAMALL*. If you've customized this in the SAP GUI, select your customization.
   - **EnableGef**: Set to *True*

Save your changes.

4.21.1.3.3 Configuring Pagination

You can configure the number of business objects with geometry information displayed per page.

Procedure

1. Navigate to `metadata/definitions/Pages/Extensions/Map.page`.
2. Change `100` to the number of business objects displayed per page as shown in the following example:

> {·} Sample Code
>
> ```
>    "Controls": [
>                "ExtensionProperties": {
>                "ItemsPerPage": 100,
> ```

4.21.1.3.4 Enabling GEF Create and Update

Your application supports GEF geometry download as well as GEF create and update.

Context

- **Create:** Supports the ability to create GEF point, line, and polygon directly from the map and from the MAIF `/MERP/CL_CORE_GIS_GEOSERV_GEF` object handler.
- **Update:** Supports the ability to update GEF point, line, and polygon directly from the map and from the MAIF `/MERP/CL_CORE_GIS_GEOSERV_GEF` object handler.

> **Note**
>
> The update feature supports the ability to update a time-sensitive GEF coordinate. Currently, the create feature does not support time-sensitive geometry.

Procedure

1. In the ConfigPanel, navigate to the *OData Mobile Data Object Configuration* section and find OMDO **<APPXX>_GIS_OBJECT_DATA**. Click the *Data Filter* tab.
2. Click the *Change* button.
3. Expand the *Defined Filters* list to show and change the following ▶ ▶ ▶.
   a. ▶ *Operation - CREATE* ▶ *Standard Filter* ▶ *GEOSERVICE_ID** ▶. Perform the following actions:
      - Uncheck the *Active* flag for all GIS rules.
      - Check the *Active* flag for all GEF rules.
   b. ▶ *Operation - READ* ▶ *Standard Filter* ▶ *GEOSERVICE_ID** ▶. Perform the following actions:
      - Uncheck the *Active* flag for all GIS rules.
      - Check the *Active* flag for all GEF rules.
   c. ▶ *Operation - UPDATE* ▶ *Standard Filter* ▶ *GEOSERVICE_ID** ▶. Perform the following actions:
      - Uncheck the *Active* flag for all GIS rules.
      - Check the *Active* flag for all GEF rules.
4. Staying in the oMDO, navigate to ▶ *Operation - READ* ▶ *Data Distribution* ▶ *GIS_ASSIGNMENT_TYPE** ▶. Select *2 - GEF Integration* and be sure the *Active* flag is checked.
5. Move to the **<APPXX>_GIS_MAP_CONTROL** oMDO and navigate to ▶ *Operation - READ* ▶ *Data Distribution* ▶ *INI_PARAMTER** ▶. Check the *Active* flag for the *EnableGef* parameter found in the *CONFIG* parameter group.
6. From the ConfigPanel home page, navigate to *Geospatial Service Definitions*. Select your application release using the *Mobile Application Filter*. Expand the *Geospatial Mobile Services by App* tree in the left panel. Ensure that the following services are active in the *General* tab:

- **<APPXX>_GEF_ADD_EQUIPMENT**
- **<APPXX>_GEF_ADD_FLOC**
- **<APPXX>_GEF_ADD_NOTIFICATION**
- **<APPXX>_GEF_ADD_WORKORDER**
- **<APPXX>_GEF_UPDATE_EQUIPMENT**
- **<APPXX>_GEF_UPDATE_FLOC**
- **<APPXX>_GEF_UPDATE_NOTIFICATION**
- **<APPXX>_GEF_UPDATE_WORKORDER**

7. *Save* your changes.

4.22 Guided Workflow Configuration

Configurable guided workflow (CGW) defines the lifecycle of an object processed in your mobile app. Customers define a workflow for their specific persona and business needs. The mobile app then displays the custom workflow as a progress tracker.

Using the guided workflow configuration method means you no longer need to change the configuration in the Status machine filter values (oMDO *SAM<XXXX>_OVERALL_STATUS*) or make code updates through the MDK to handle updates on the mobile device.

Administrators plug in customizations through the ConfigPanel, where they can see the process flow defined with easy to follow steps. The steps, in turn, have the status definitions defined for the selected object. The steps are reusable. Once you define a step, you can reuse it in multiple workflows.

A configurable guided workflow is available for the following object types:

- WORKORDER (included as part of the standard delivery)
- WO_OPERATION (included as part of the standard delivery)
- S4_SERVICE_ORDER
- S4_SERVICE_ITEM
- NOTIFICATION

Note that only one feature can be assigned to a guided workflow at the header level.

If no workflow is defined for an object, the object defaults back to the regular mobile status flow defined in the status machine filter *MOBILE_STATUS_STATE_MACHINE* in the oMDO *<APPXXXX>_OVERALL_STATUS*.

> **Note**
>
> For more information about using the guided workflow in the mobile app, see the Using Guided Workflows topic.

Supported Personas

This feature is applicable for the following personas:

- Maintenance Technician (Pro)
- Field Service Technician (Standard)
- Field Service Technician (Pro)

Limitations

The following object types are not supported in a standard delivery of a MAIF application:

- TASK
- S4_SRV_CONF_ITEM
- S4_SRV_CONF
- S4_SERV_REQUEST
- WCMDOCHEADER
- WCMDOCITEM
- WCMDOCUMENT

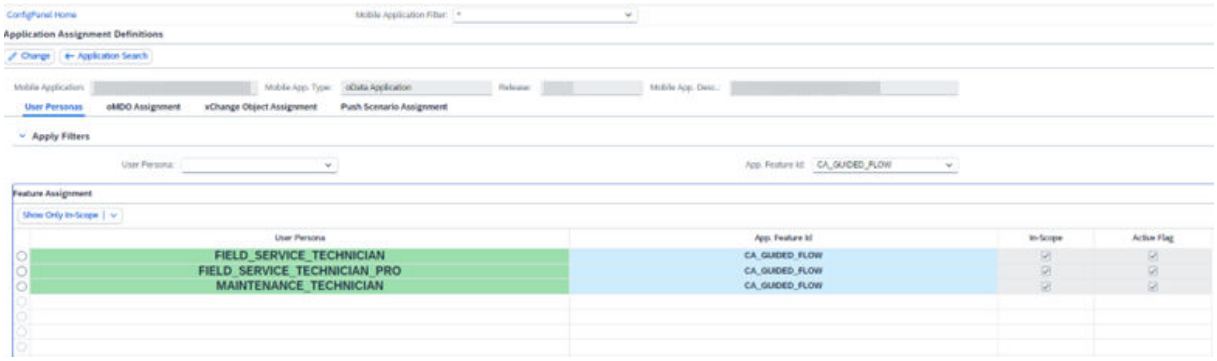
> **Note**
>
> These object types are handled separately on the back end client. Therefore, these objects need custom client enhancement to support them, along with custom object types and workflow configuration. The process to create these custom enhancements and configurations are outside the scope of this manual.

An upgrade from a lower version of SAP Service and Asset Manager to 2410 requires additional efforts from the customer to reconfigure the customizations done to the old status machine. These customizations are maintained in the filter *MOBILE_STATUS_STATE_MACHINE* in the *SAMXXXX_OVERALL_STATUS* oMDO.

Note that only one workflow can be designated as the default for a given object type, persona, role, and feature combination. If multiple flows are designed for an object, the flow that is marked as default is used.

Prerequisites

If you're planning on modifying existing guided workflows or adding new workflows to your mobile application, be sure to activate the *CA_GUIDED_FLOW* feature and assign it to the desired personas. See Configuring Features in *MAIF Configuration Guide* for detailed information.



Configuration

See the following procedures to configure guided workflows:

- Creating a New Workflow - Back End [page 440]
- Creating a New Work Step - Back End [page 441]
- Modifying an Existing Workflow - Back End [page 442]
- Configuring Notifications with Workflows - Back End [page 443]

4.22.1 Creating a New Workflow - Back End

Context

For detailed information about guided workflow, see the overview topic, Guided Workflow Configuration [page 438].

A configurable guided workflow is available for the following object types:

- WORKORDER
- WO_OPERATION
- S4_SERVICE_ORDER
- S4_SERVICE_ITEM
- NOTIFICATION

Note that only one feature can be assigned to a guided workflow at the header level.

General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **Enabling and disabling features**: refer to Configuring Features in *MAIF Configuration Guide*.
- **Mobile Application Parameters** configuration: refer to Parameters Tab in *MAIF Configuration Guide*.
- **OMDO** and **OMDO filter** configuration: refer to OData Mobile Data Object Configuration and OData Mobile Data Object Configuration - Data Filter Tab in *MAIF Configuration Guide*.
- **Exchange** and **Exchange filters** configuration: refer to Exchange Object Configuration and Change Detection Condition Filter Tab in *MAIF Configuration Guide*.
- **Server parameters** configuration: refer to Administration - Server Management in *MAIF Administrator Guide*.
- **User attributes** configuration: refer to Sync Groups in *MAIF Configuration Guide*.
- **User parameters** configuration:, refer to Administration - User Management in *MAIF Administrator Guide*.

Procedure

1. On the ConfigPanel Home page, select *Guided Workflow Configuration*. Make sure to select your desired mobile application in the *Mobile Application* field and your desired object type in the *Object Type* field at the top of the page.
2. Click the *Create Flow* button.

   A Guided Flow Detail screen appears, with all fields empty except for the Mobile App and Object Type fields.
3. Type in desired field names or use the dropdown buttons where available to select choices for all fields. See the Guided Workflow Configuration [page 649] topic in the *Panels, Tabs, and Field Descriptions* chapter for detailed explanations of all fields.
4. Use the + button to add steps to your workflow. See the Creating a New Work Step - Back End [page 441] for more details.
5. Be sure to check the *Default* box if you would like your newly created workflow to be the default.
6. *Save* your changes.

4.22.2 Creating a New Work Step - Back End

Guided workflows consist of a series of steps. Each step contains a list of transactions a user can perform within the given step.

Context

For detailed information about the guided workflow, see the overview topic, Guided Workflow Configuration [page 438].

Guided workflow steps use the statuses defined against the objects at the mobile application level.

Steps are defined for an object type. Each step contains a list of status transactions a mobile user can perform within the given step. Note that each step must contain at least one status transition.

When adding a status transition to a step, define the transition type and assign a feature ID to the status transition. If a status transition has a feature ID assigned, it is only available on the mobile device if the feature is enabled.

When creating a new work step for a guided workflow, keep the following requirements in mind:

- Every step must have at least one status transition
- The *FROM* status can never be empty
- The *TO* status can be empty, which indicates a final status in a guided workflow

General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **Enabling and disabling features**: refer to Configuring Features in *MAIF Configuration Guide*.

- **Mobile Application Parameters** configuration: refer to Parameters Tab in *MAIF Configuration Guide*.
- **OMDO** and **OMDO filter** configuration: refer to OData Mobile Data Object Configuration and OData Mobile Data Object Configuration - Data Filter Tab in *MAIF Configuration Guide*.
- **Exchange** and **Exchange filters** configuration: refer to Exchange Object Configuration and Change Detection Condition Filter Tab in *MAIF Configuration Guide*.
- **Server parameters** configuration: refer to Administration - Server Management in *MAIF Administrator Guide*.
- **User attributes** configuration: refer to Sync Groups in *MAIF Configuration Guide*.
- **User parameters** configuratio:, refer to Administration - User Management in *MAIF Administrator Guide*.

Procedure

1. On the ConfigPanel Home page, select *Guided Workflow Configuration*. Make sure to select your desired mobile application in the *Mobile Application* field and your desired object type in the *Object Type* field at the top of the page.
2. Either create a new workflow or modify an existing workflow:
   - Modifying an Existing Workflow - Back End [page 442]
   - Creating a New Workflow - Back End [page 440]

4.22.3 Modifying an Existing Workflow - Back End

Context

For detailed information about the guided workflow, see the overview topic, Guided Workflow Configuration [page 438].

A configurable guided workflow is available for the following object types:

- WORKORDER (included in the standard delivery)
- WO_OPERATION (included in the standard delivery)
- S4_SERVICE_ORDER
- S4_SERVICE_ITEM
- NOTIFICATION

Note that only one feature can be assigned to a guided workflow at the header level.

> → Tip
>
> If you want to modify a standard delivery flow included with your installation, we recommend using the *Copy* button to copy the existing flow into a custom flow. Then, you can deactivate the standard flow if it's no longer needed.

General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **Enabling and disabling features**: refer to Configuring Features in *MAIF Configuration Guide*.
- **Mobile Application Parameters** configuration: refer to Parameters Tab in *MAIF Configuration Guide*.
- **OMDO** and **OMDO filter** configuration: refer to OData Mobile Data Object Configuration and OData Mobile Data Object Configuration - Data Filter Tab in *MAIF Configuration Guide*.
- **Exchange** and **Exchange filters** configuration: refer to Exchange Object Configuration and Change Detection Condition Filter Tab in *MAIF Configuration Guide*.

Procedure

1. On the ConfigPanel Home page, select *Guided Workflow Configuration*. Make sure to select your desired mobile application in the *Mobile Application* field and your desired object type in the *Object Type* field at the top of the page.
2. Highlight the row of the workflow you want to copy. Click the *Copy Flow* button.

   The Guided Flow Detail screen opens and the copied workflow is ready for modifications.
3. Change the *Flow ID* name, which is the original flow name with *_CPY* appended to the end. Select field values for all desired fields.
4. Use the + and - buttons to the side of the *Steps* table to add new steps or delete existing steps. See the Creating a New Work Step - Back End [page 441] procedure for more details.
5. Be sure to check the *Default* box if you would like your newly created workflow to be the default.
6. *Save* your changes.

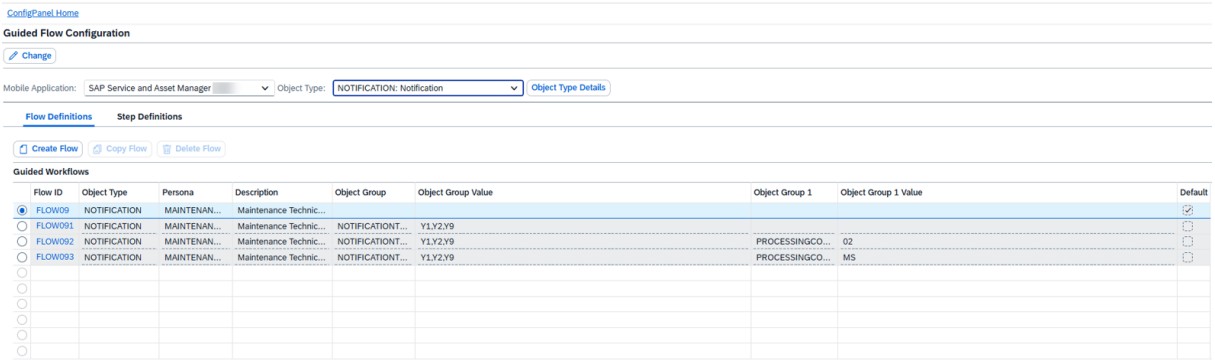
4.22.4 Configuring Notifications with Workflows - Back End

As of SAP Service and Asset Manager 2505 version, Notifications/Maintenance Requests are supported with Configurable Guided Flows.

Context

For detailed information about the guided workflow, see the overview topic, Guided Workflow Configuration [page 438].

The following Guided Flows are part of standard delivery:



- *FLOW09*: Default flow for notifications handling the non-phase notifications.
- *FLOW091*: Flow for phase model notifications.
- *FLOW092*: Phase model notification flow for processing context 02 (i.e., minor work notifications).
- *FLOW093*: Phase model notification flow for processing context MS (i.e., minor work with screening notifications).

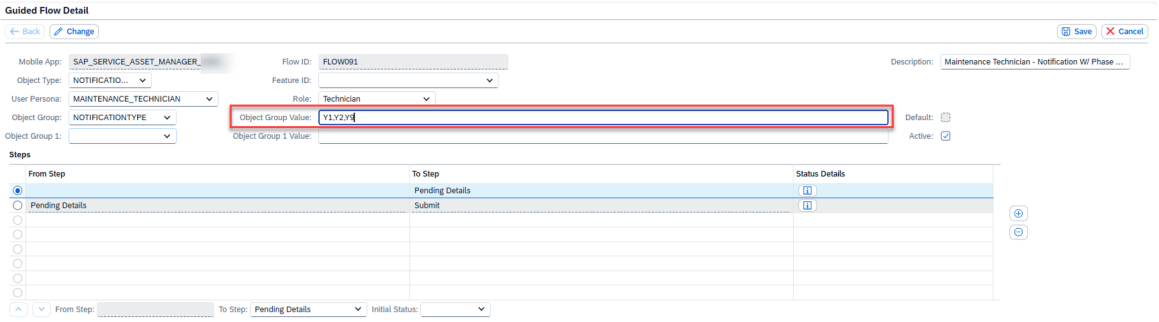
If phase model notifications are processed on the device, customization is required.. You need to update the *Object Group Value* (*Y1,Y2,Y9*) for the flows *FLOW091*, *FLOW092*, and *FLOW093* based on the notification type(s) the core configuration supports. If more than one notification types are supported with phase model, you need to maintain the comma-separated values.

To update the *Object Group Value*, perform the following steps:

> **Note**
>
> It is recommended to copy the standard delivered flow, make your changes, then deactivate the original flow.

Procedure

1. Click *Change* to enter change mode.
2. Click on the flow you want to change.
3. Add/remove the Notification types from the *Object Group Value* field.



4. *Save* your changes,

> Note
>
> - *FLOW091*, *FLOW092*, *FLOW093* have the notification types separated by comma in the *Object Group Value* field. You can change these to support the notification types which are activated with phase model.
> - *MS* (Minor work with screening) is a new notification processing context supported in **S/4 OP2023 SP03** and onwards.
> - For more information about Phase Model, see EAM Phase Model Configuration - Overview [page 341].

4.23 Inbound Delivery Process Configuration (Extended Warehouse Clerk)

As an Extended Warehouse Clerk, you can search, fetch, and download Inbound Deliveries and Inbound Delivery Document Items, to view all the relevant delivery details and statuses, as well as to to manage and execute tasks accurately during the receiving process. Key features of the inbound delivery process include:

- Change Inbound Delivery documents (with single edits or bulk edits)
- Create Warehouse Tasks (both manual and auto-creation)
- Pack Inbound Delivery Items (single and mixed Handling Units creation, auto packing)
- Goods Receipt (single item and bulk items receiving)

> Note
>
> - For more information about using the Inbound Delivery feature, see Working with Inbound Deliveries.
> - The Inbound Delivery feature differs for the Inventory Clerk and Extended Warehouse Clerk personas, since Inventory Clerk only supports Goods Receipt for Inbound Delivery.

Supported Personas

This feature is applicable for the following personas:

Extended Warehouse Clerk

Limitations

In the case of *Goods Receipt* for *Inbound Deliveries*, receiving a single item directly is not supported. You can only receive a single item by confirming the *Warehouse Task* of the corresponding *Item*.

Prerequisites

The *EWM_CORE_DATA* feature must be enabled (see General Feature Configuration - Extended Warehouse Clerk [page 173]). For additional prerequisites, see Configuration Prerequisites and Limitations - Extended Warehouse Clerk [page 171].

Configuration

Perform the following configuration step(s):

1. Mobile Application Parameters - Extended Warehouse Clerk [page 174]
2. oMDO Configuration - Extended Warehouse Clerk [page 175]

4.24 Isolation Certificate Configuration

Isolation Certificates (also referred to as Safety Cerificates) are used to describe lockout and tagout procedures when controlling the physical blocking and tagging of affected technical objects. It contains the technical asset objects that are to be switched or controlled in the application and provides a detailed description of how the system is to be isolated.

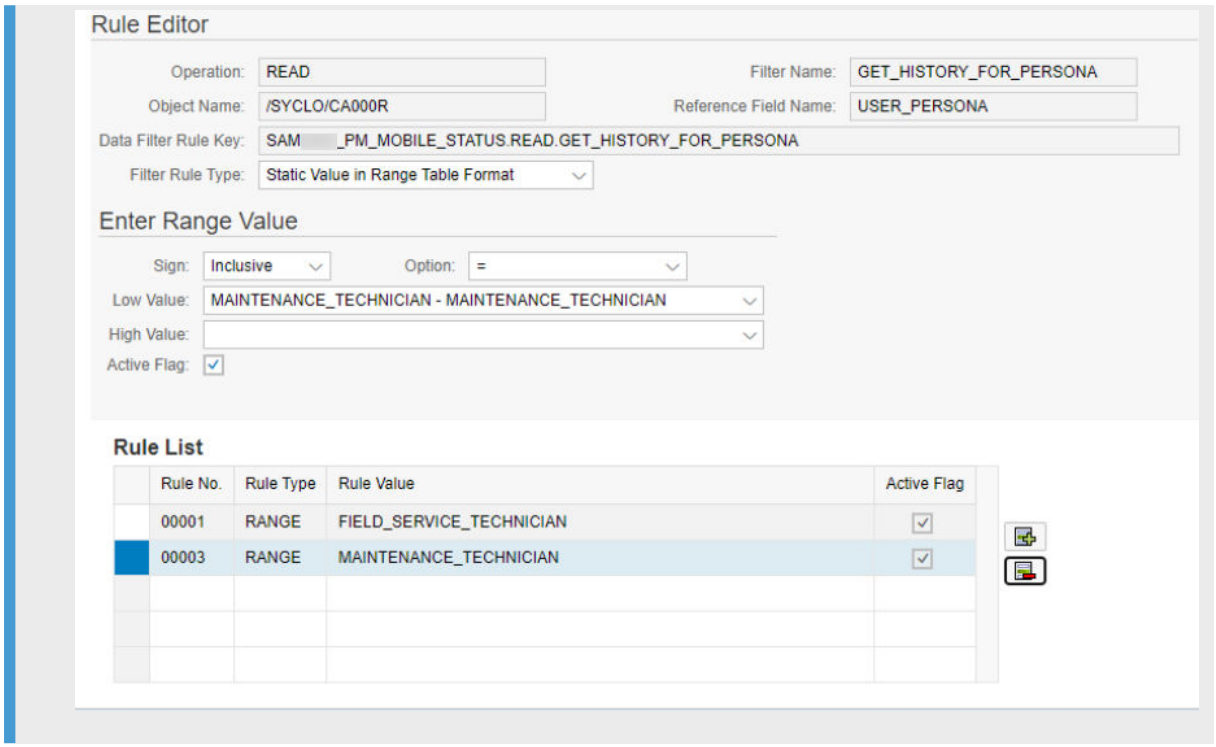
> **Note**
>
> - For more information about using Isolation Certificates, see Isolation Certificate Detail Screen.
> - The configuration of Assignment Management [page 261] affects the configurations of **WCM Work Order**, **Isolation Certificate** and **Work Permit**.

Supported Personas

This feature is applicable for the following personas:

Maintenance Technician (Pro)
Safety Technician

> **Note**
>
> - For the Maintenance Technician (Pro) persona, this feature is only available from 2410 version.
> - If the user uses Safety Technician (WCM) features via the Maintenance Technician (Pro) persona, you need to add the persona to the data filter *SAMXXXX_PM_MOBILE_STATUS* > *GET_HISTORY_FOR_PERSONA*:



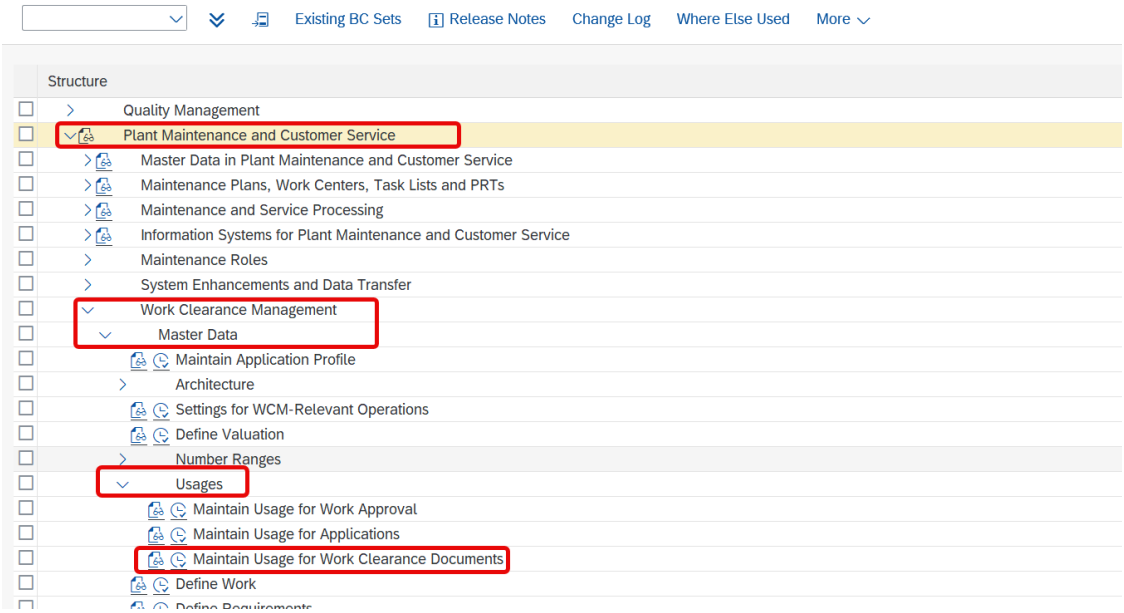
Limitations

For current limitations of Isolation Cerificates, see Configuration Prerequisites and Limitations - Safety Technician Persona [page 217].

Prerequisites

Before going through the configuration steps below [page 448], you need to make sure the following prerequisites are met:

- The *WCM_COMMON* feature is enabled. See General Feature Configuration - Safety Technician Persona [page 218].
- Perform the following *SPRO* changes:
  1. In *SAP GUI* use the transaction code *SPRO* and click *SAP Reference IMG*.
  2. Navigate to *Plaint Maintenance and Customer Service* > *Work Clearance Management* > *Master Data* > *Usages* > *Maintain Usage for Work Clearance Documents*.



3. Create and configure the usage types according to your preference. See Supported Usage Types - Safety Technician Persona [page 226].

Configuration

Perform the following configuration step(s):

1. Configuring Isolation Cerificates - Back End - Enabling the Feature [page 448]
2. Configure oMDO data filters as described in General oMDO Configuration - Safety Technician Persona [page 221].
3. Configure Exchange Objects as described in General Exchange Configuration - Safety Technician Persona [page 224].
4. Configure User Parameters as described in General User Parameters Configuration - Safety Technician Persona [page 227].

4.24.1 Configuring Isolation Cerificates - Back End - Enabling the Feature

Context

For detailed information about Isolation Cerificates, see the overview topic, Isolation Certificate Configuration [page 446].

The below procedure describes how to enable the feature in the Configuration Panel.

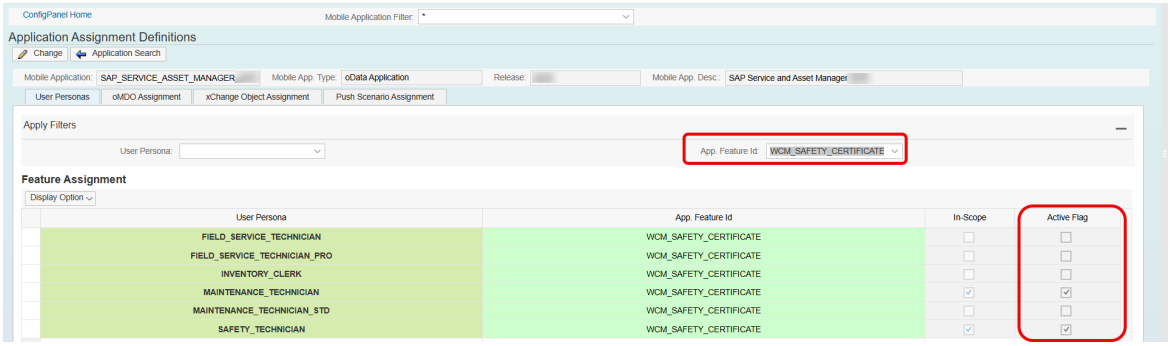
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **Enabling and disabling features**: refer to Configuring Features in *MAIF Configuration Guide*.

Procedure

1. On the Configuration Panel, go to *Component Assignments* and select your application from the list.
2. In the *App. Feature Id* dropdown, select *WCM_SAFETY_CERIFICATE*.
3. Enter *Change mode* and set the feature to *Active* for the personas [page 446] you want to enable it.



4. Save your changes.

4.25 Linear Asset Management Configuration

Linear assets are technical systems with a linear infrastructure whose condition and properties can vary from section to section (dynamic segmentation). You can see linear asset data associated with various objects such as work orders, operations, technical objects, and notifications.

In addition to the basic SAP Service and Asset Manager configuration, there are a few considerations when configuring SAP Service and Asset Manager with Linear Asset Management (LAM).

Configuration items include:

- Disabling and re-enabling LAM
- Enabling technical objects work list feature
- Adding the LAM equipment type filter
- Adding linear data for statistics

Each of these configuration items is described in the sections that follow.

> **Note**
>
> Before configuring LAM on your system, see 2900476 so that the LAM exchange works properly.

4.25.1 Disabling and Re-Enabling Linear Asset Management

Linear Asset Management (LAM) is especially designed to meet the requirements of linear asset maintenance. A linear asset is a special type of asset that has an associated length dimension. This dimension is represented through starting and ending points or by specifying the asset length. For the mobile device, the linear asset management functionality enables the field technician to work on orders and notifications that have linear equipment and functional locations. Field personnel can create work orders, notifications, time confirmations, and material confirmations for the linear assets.

From the mobile device, you can view linear data for the following:

- Work orders
- Operations
- Notifications
- Items
- Equipment
- Functional locations
- Confirmations
- Measuring points
- Measurement documents

You can create or edit linear data on characteristic values.

The Linear Asset Management feature is called *PM_LINEAR_ASSET_MANAGEMENT*. By default, the feature is not enabled.

> **Note**
>
> As of the SAP Service and Asset Manager 2205 release, enable and disable parameters are no longer available through the *Parameters* tab. You enable or disable all features through the *Features* tab. See the Configuring Features [page 93] procedure for details.

Use the following OMDOs to configure your LAM feature:

- LAM_OBJECT_DATA
- LAM_OFFSET_TYPE
- LINEAR_REFERENCE_PATTERN

For general information on configuring OMDOS, see the *OData Channel Integration Settings Procedures* topics found in the *Mobile Add-On Configuration Configuration Panel Common Procedures* chapter of this guide.

4.25.2 Adding Linear Data for Characteristics

The functionality of adding or editing linear data for characteristics defines segments of a linear asset where a specific attribute, or characteristic value, is valid. A segment is defined by start point, end point, length, and unit of measurement (linear data).

Relevant OMDO: **SAMXXXX_LAM_CHAR_VALUE**.

> **Note**
>
> - Linear data for characteristics works only for characteristics that are marked as relevant for linear asset management.
> - To use linear data for characteristics, create a special *Organizational Area* and assign it to the relevant classes and characteristics.
> - It's possible to assign several characteristic values in different segments of a linear asset. Therefore, set the value assignment to *multiple values* when the characteristics are created.

4.26 Local Object Mobile Status Configuration

The EnableOnLocalBusinessObjects parameter found in the MOBILESTATUS group enables or disables a mobile client user to take a local object through its entire lifecycle even if the client is offline.

Context

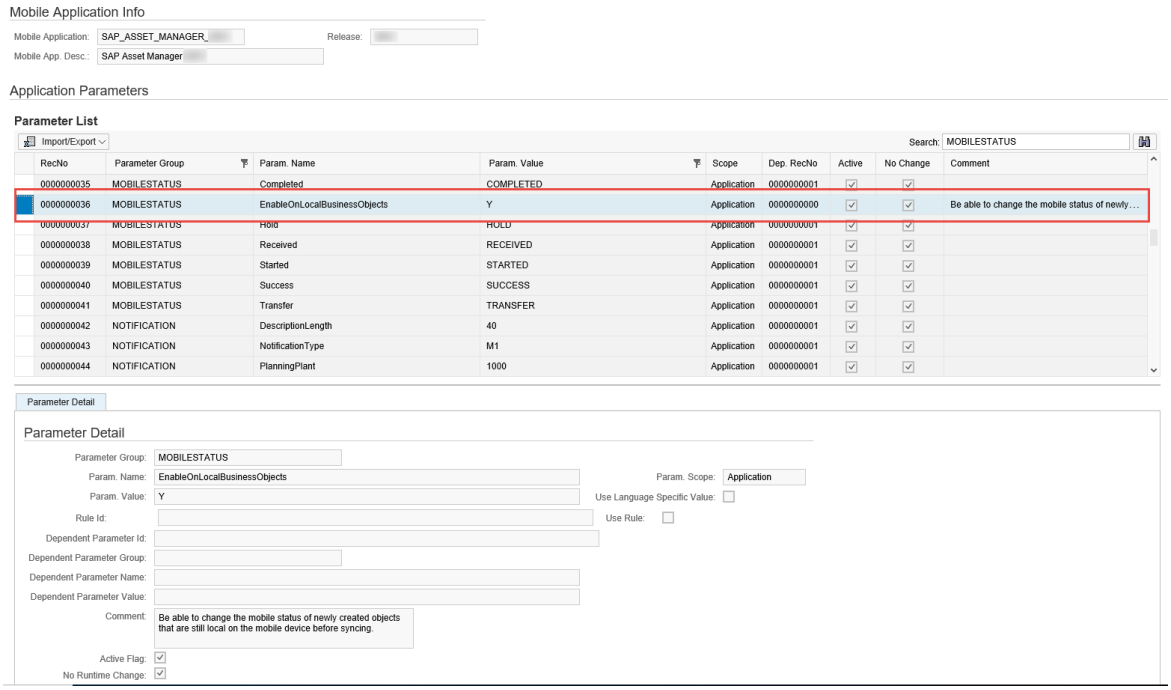
If you enable the *EnableOnLocalBusinessObjects* parameter, SAP Service and Asset Manager allows mobile status update changes for the following:

- Work Order - Assignment level 1
- Operation - Assignment level 2
- Suboperation - Assignment level 3
- Notification
- Notification task
- Notification item task

Procedure

1. Navigate to *Mobile Application Configuration* > *Parameters tab* using the ConfigPanel. Select your application in the left column, *Defined Mobile Applications*.

   The *Parameter List* populates with a list of all parameters available for the application.
2. Find the *EnableOnLocalBusinessObjects* parameter in the *MOBILESTATUS* group. Scroll down to find the parameter, or perform a search using the *Search* box. Highlight the parameter you want to configure and click the *Change* button.



3. Enable or disable the parameter using the following strings: *Y*, *Yes*, *T*, or *True* are used to enable the parameter. *N*, *No*, *F*, or *False* are used to disable the parameter.
4. Check the `<Active>` flag to ensure that the parameter is used by the mobile application. Check the `<No Runtime Change>` box to ensure that the value of the parameter isn't overridden at runtime through synchronization processing if desired and if not already checked.
5. *Save* your changes.

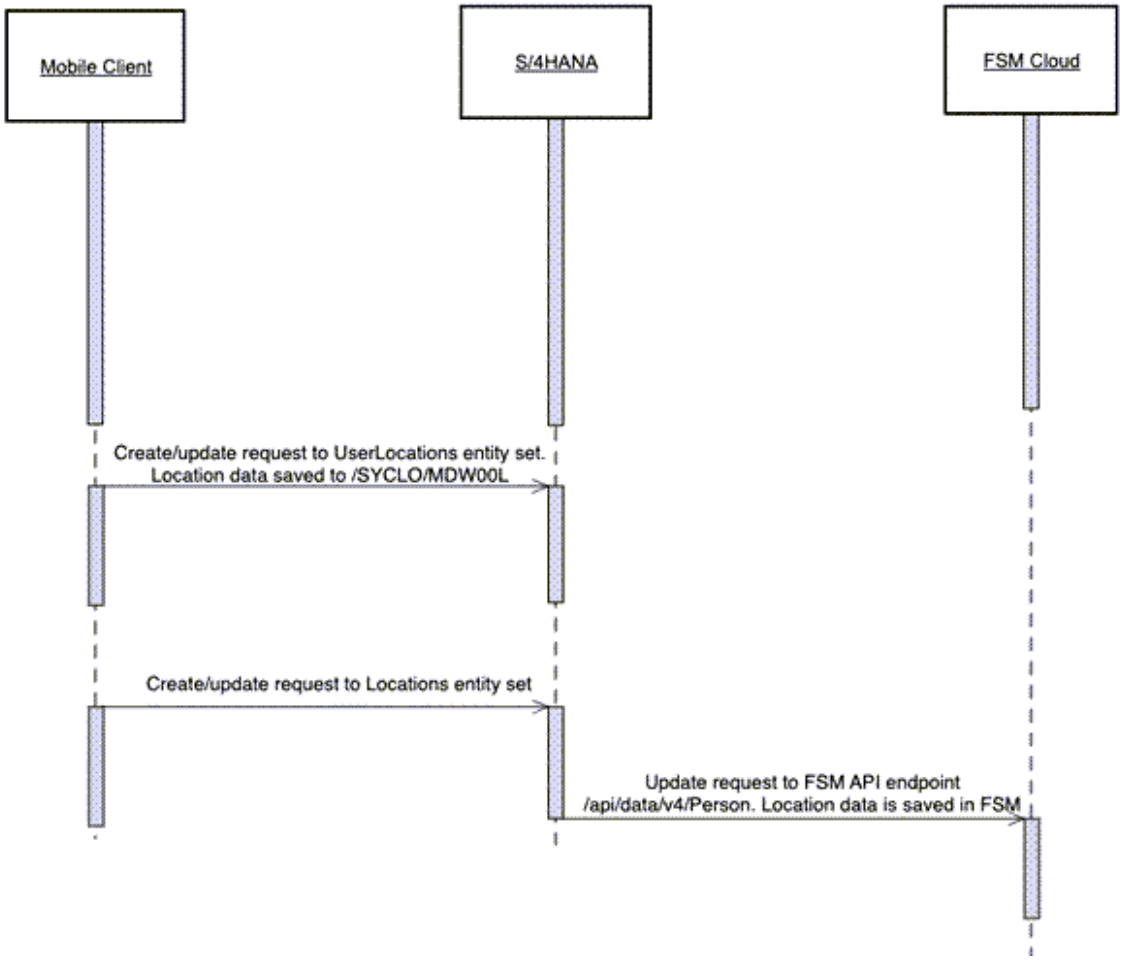
4.27 Location Tracking Configuration

This feature allows to track the Technicians' live location, so the Planner can identify the Technicians' proximity and provide options for the Scheduler to assign them urgent tasks or re-assign tasks to nearby Technicians.

To track and access the user's location from the mobile device, perform the configuration steps below [page 454].

> **Note**
>
> The location information can only be sent if the user allows the application to access the location in the application settings. For more information, see Profile Settings Overview.

High-Level Process Map



When the Technician is online, using the SAP Service and Asset Manager mobile application, the location data (Latitude and Longitude co-ordinates) is synchronized automatically to the SAP S/4HANAback end and stored in MAIF user location data table. Also, if the FSM integration feature [page 454] is active then the Technician's location captured from SSAM will be updated to FSM so that it can be viewed in the FSM Service Map.

> **Note**
>
> For more information, refer to Service Map in *SAP Field Service Management* documentation.

Supported Personas

This feature is applicable for the following personas:

Maintenance Technician (Pro)
Field Service Technician (Standard)
Field Service Technician (Pro)

> **Note**
>
> This feature is supported by both Customer Service and S/4HANA back end systems.

Prerequisites

Depending on you want to enable the FSM Integration feature on a Customer Service or S/4HANA back end system, refer to:

- Field Service Technician Configuration on a Customer Service Back End [page 177]
- Field Service Technician Configuration for SAP S/4HANA Service Order Scenario [page 205]

Configuration

Perform the following steps to configure Location Tracking and access User Location Data:

1. Configuring Location Tracking - Back End - Mobile Application Parameters [page 454]
2. Accessing User Location Data - Back End - MAIF Administration Potral [page 455]

4.27.1 Configuring Location Tracking - Back End - Mobile Application Parameters

Context

For detailed information about Location Tracking, see the overview topic, Location Tracking Configuration [page 452].

The below procedure describes how to enable the *AllowOverride* Application Parameter, so users' will be able to toggle the Location Tracking feature in the Profile settings menu of the application.

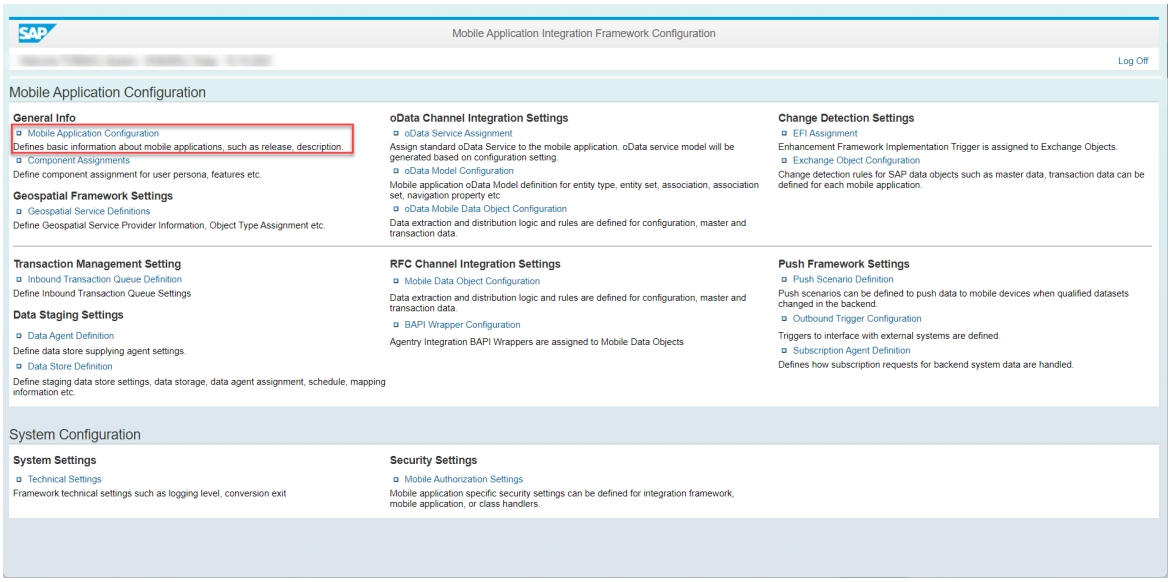
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

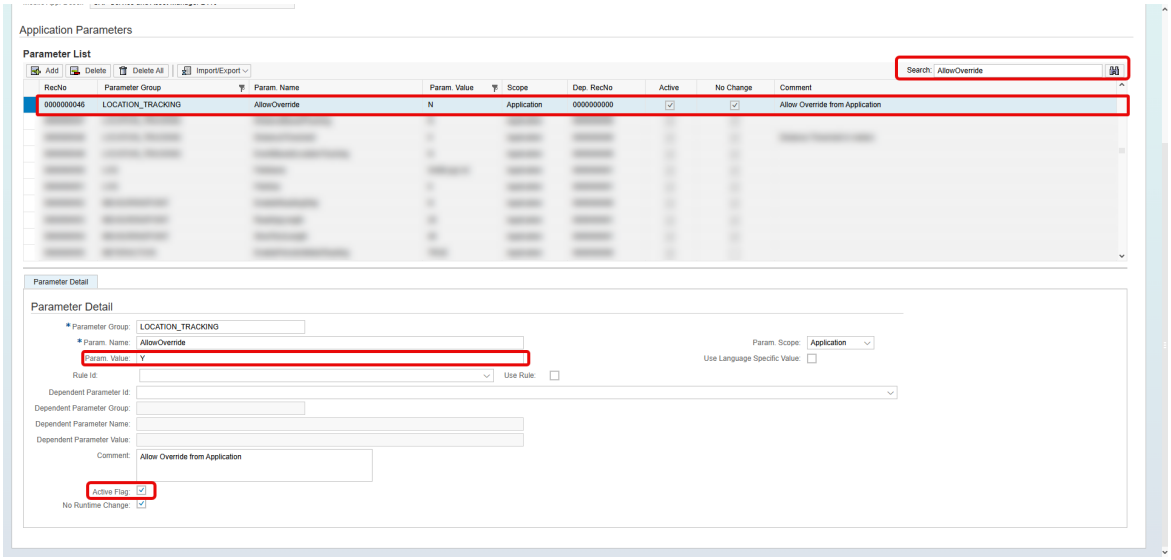
- **Mobile Application Parameters** configuration: refer to Parameters Tab in *MAIF Configuration Guide*.

Procedure

1. On the *Configuration Panel*, go to *Mobile Application Configuration*.



2. On the left, select your application from the list, and go to the *Parameters* tab.
3. Search for the *AllowOverride* parameter, enter *Change Mode*, set the *Parameter Value* to *YES* and check the *Active Flag* checkbox.



4.27.2 Accessing User Location Data - Back End - MAIF Administration Potral

Context

For detailed information about Location Tracking, see the overview topic, Location Tracking Configuration [page 452].

This guide describes for Planners and Administrators how to access Technicians' location data from the SAP back end, using the MAIF Administration Portal.

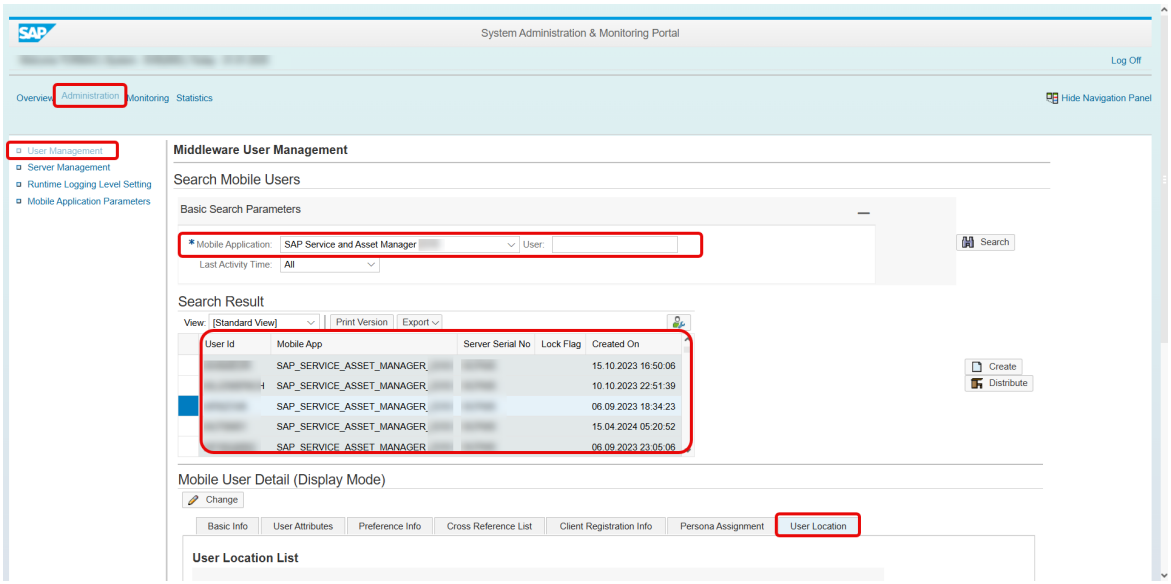
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

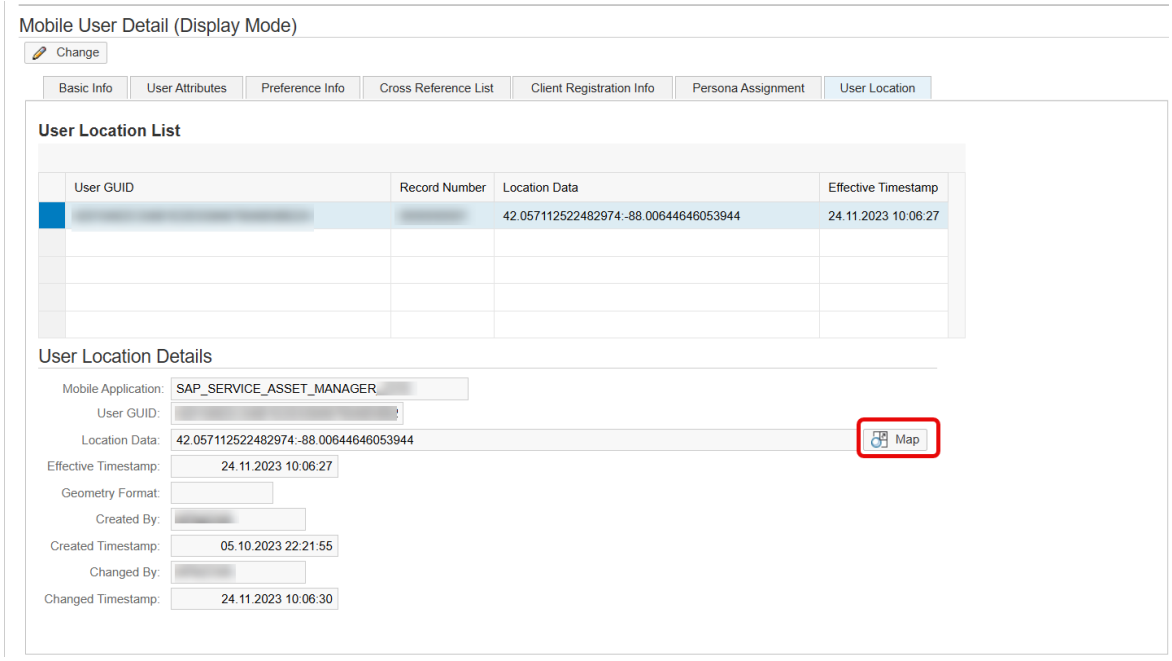
- **User Location**: refer to Administration - User Management in *MAIF Administrator Guide*.

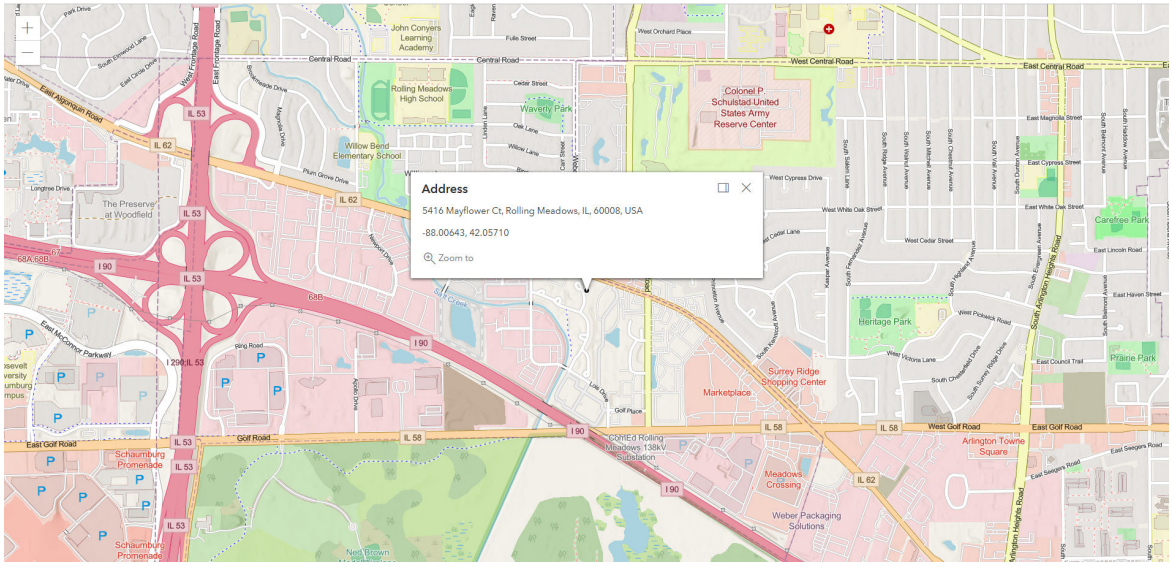
Procedure

1. To access User Location Data stored in MAIF user table (`/SYCLO/MDW00L`), open the *MAIF Administration & Monitoring Portal*. To do so, in *SAP GUI* enter the transaction code `/SYCLO/ADMIN`.
2. Go to *Administration* > *User Management*.
3. Select your *Mobile Application*, search and select the *User*, then go to *User Location*.



4. Under *User Location Details*, you can directly open the *Map* to display the selected User's location.





5. If FSM Integration is active [page 454], then the location data is synchronized to FSM Service Map as well, using the `/api/data/v4/Person` data API.

> **Note**
>
> For more information, see:
>
> - Service Map in *SAP Field Service Management* documentation
> - Configuring Server Parameters - Customer Service Back End [page 191]
> - Configuring Server Parameters - S/4 Back End [page 210]

4.28 Low Code No Code Support

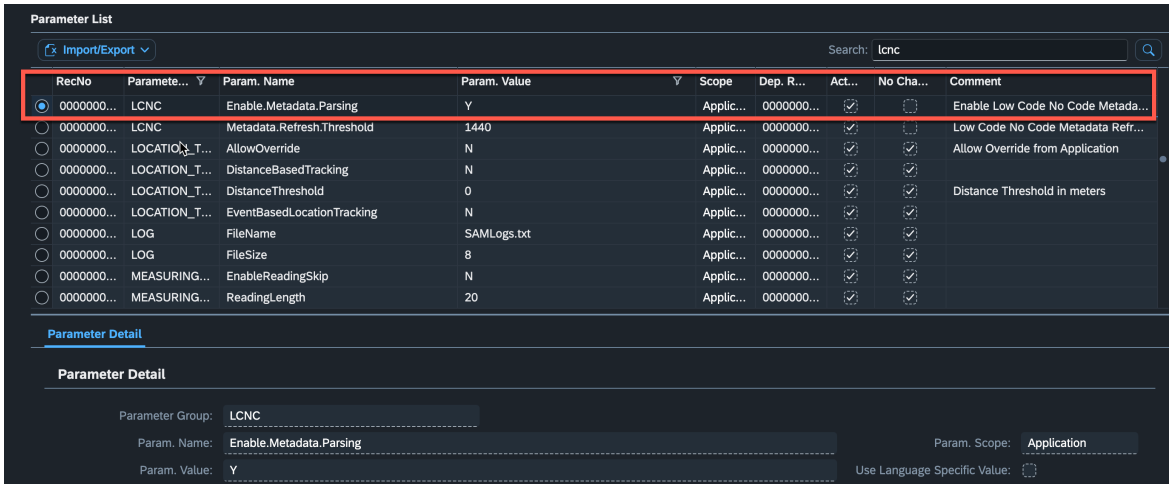
Context

The object detail screens in SAP Service and Asset Manager can be modified to include properties of the oData entity set that are not part of the detail screen out of the box. To do this, simply change the back end configuration and then synchronize with the mobile client.

Procedure

1. Log on to the SAP system and execute the transaction code /SYCLO/CONFIGPANEL.
2. Log on to the configuration panel.
3. Navigate to the main page of the configuration panel. Under *Mobile Application Configuration* > *SAP_SERVICE_ASSET_MANAGER_XXXX* > *Parameters* in the configuration panel, ensure that the parameter value is *Y* and is active.

> **Note**
>
> The LCNC feature does not support any translations or text formatting depending on the locale and region of the device.



> **Note**
>
> For further steps on how to set up custom fields on the detail object screen, see the following Showing Customized Fields on the Detail Screen [page 459], Showing Customized Fields on the List Screen [page 460] and Adding Customized Fields to the Search Criteria [page 462] topics.

4.28.1 Showing Customized Fields on the Detail Screen

In SAP Service and Asset Manager, the detail view screens can be modified to include properties of the oData entity set that are not part of the table out of the box. The new properties will be added to the table description field, each in a new line.

Context

To add a new property, change the back end configuration and then synchronize with the mobile client.

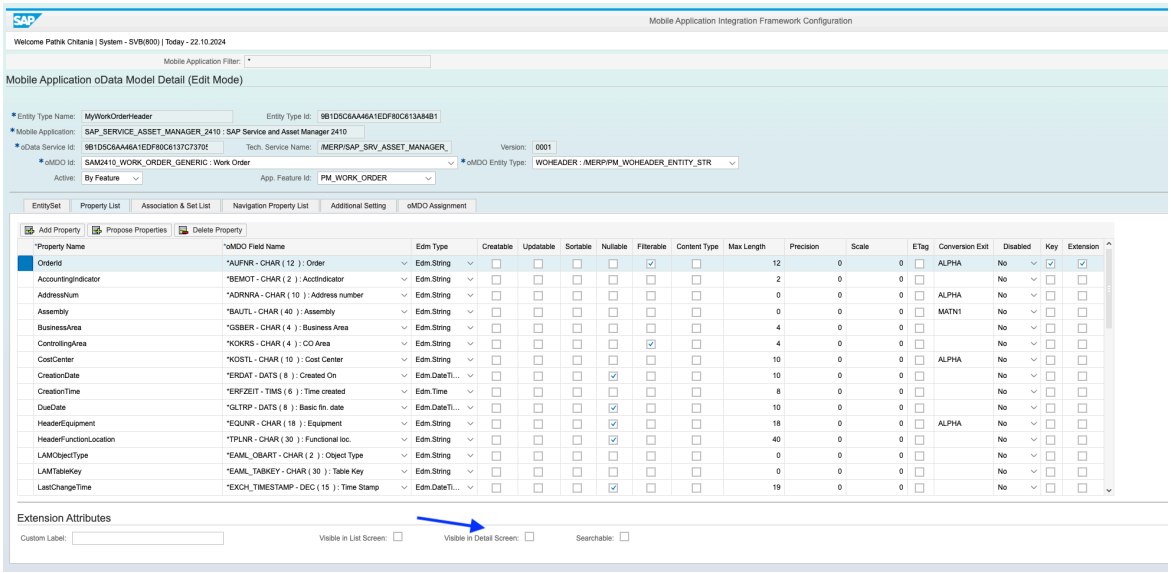
Procedure

1. Log on to the SAP system and execute the transaction code /SYCLO/CONFIGPANEL.
2. Log on to the Configuration Panel.
3. Navigate to *oData Model Configuration*.
4. Open *SAP_SERVICE_ASSET_MANAGER_XXXX* and find the entity you want to change on the mobile client.
5. Navigate to the *Property List* tab and select the new oData entity set property that should appear on the object detail screen.

   > **Note**
   >
   > Custom Z properties are also supported.

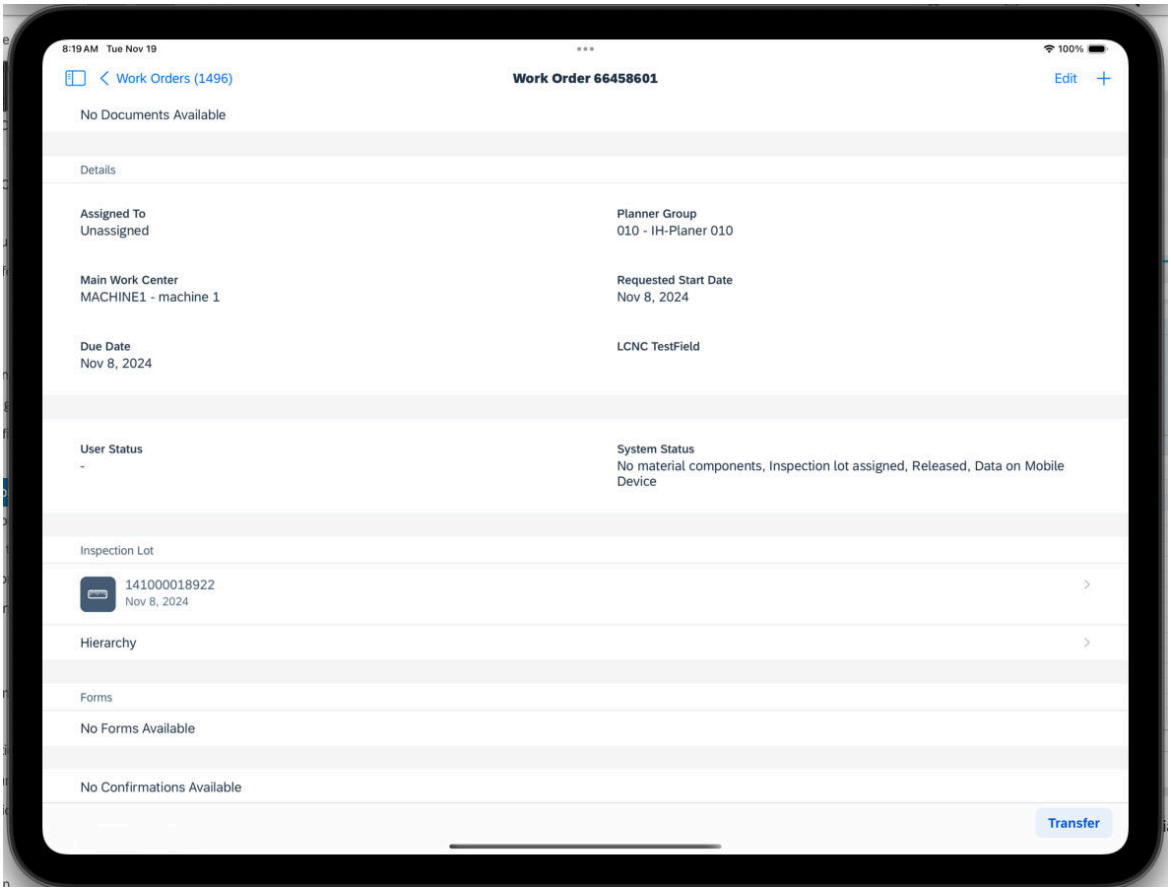
6. Click the *Extension* check box.

   The *Extension Attributes* section appears.



7. Enter the label to be used on the mobile client for this property if necessary. If this value is empty, the default data item field label associated with the oMDO entity type structure component will be used.

8. Click the *Visible in Detail Screen* check box.
9. Save changes and select a customization request if necessary.
10. Synchronize from a mobile device.
11. The property will now appear on the list screen of the corresponding object.



4.28.2 Showing Customized Fields on the List Screen

In SAP Service and Asset Manager, the list view screens can be modified to include properties of the oData entity set that are not part of the table out of the box. The new properties will be added to the table description field, each in a new line.

Context

To add a new property, change the backend configuration and then synchronize with the mobile client.

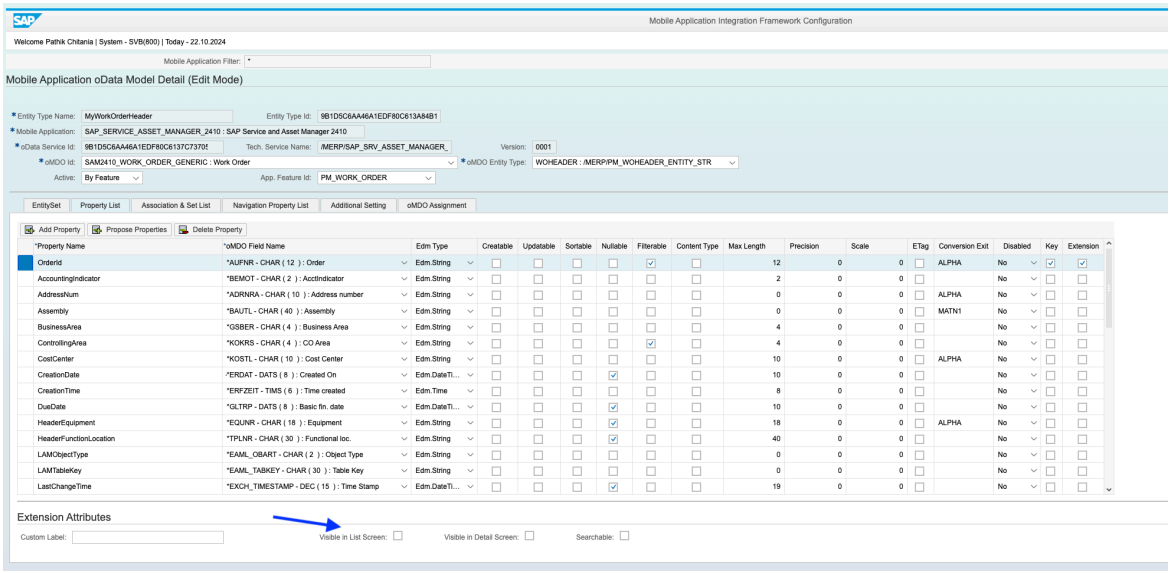
Procedure

1. Log on to the SAP system and execute the transaction code /SYCLO/CONFIGPANEL.
2. Log on to the Configuration Panel.
3. Navigate to *oData Model Configuration*.
4. Open *SAP_SERVICE_ASSET_MANAGER_XXXX* and find the entity you want to change on the mobile client.
5. Navigate to the *Property List* tab and select the new oData entity set property that should appear on the object detail screen.

> **Note**
>
> Custom Z properties are also supported.

6. Click the *Extension* check box.

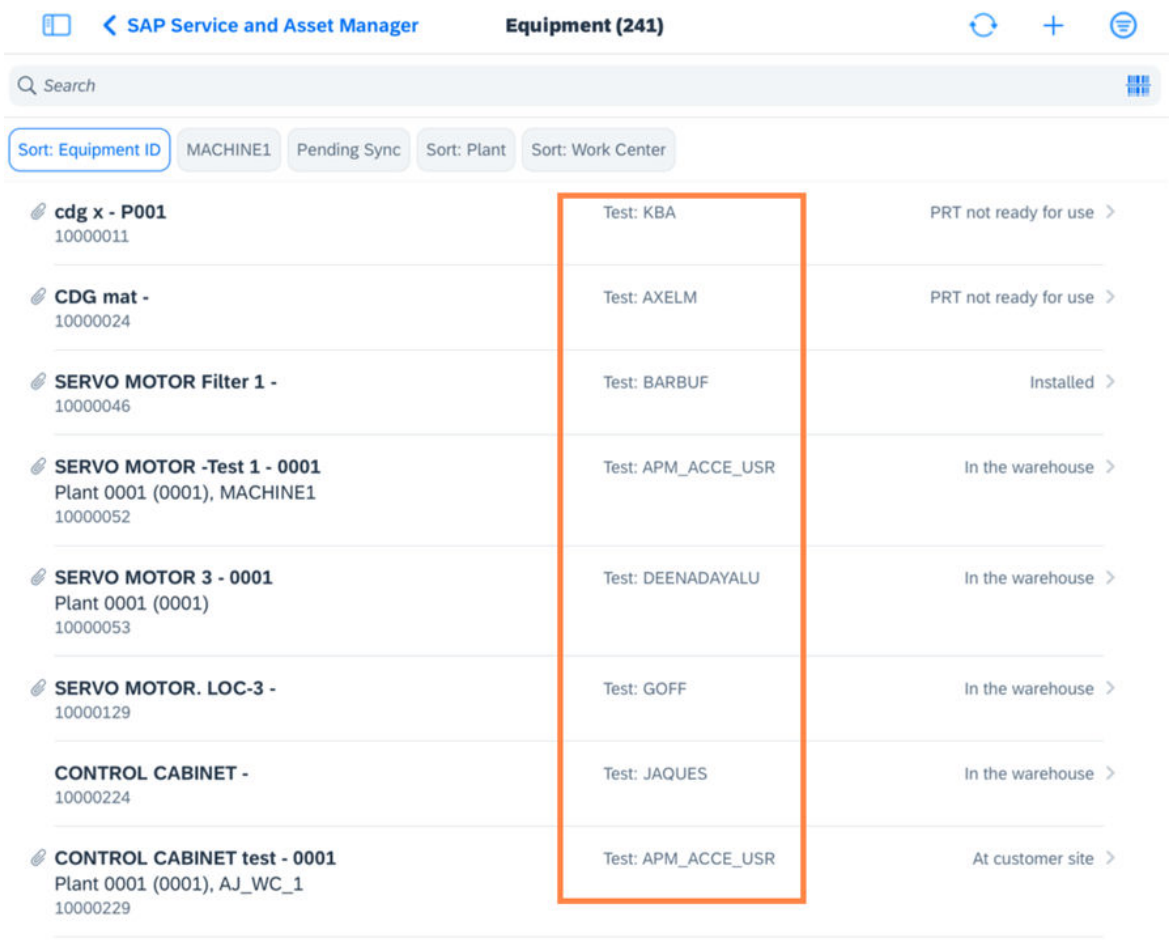
   The *Extension Attributes* section appears.



7. Enter the label to be used on the mobile client for this property if necessary. If this value is empty, the default data item field label associated with the oMDO entity type structure component will be used.
8. Click the *Visible in List Screen* check box.
9. Save changes and select a customization request if necessary.
10. Synchronize from a mobile device.
11. The property will now appear on the list screen of the corresponding object.

    See the table description fields that are highlighted on the image.

> **Note**
>
> Only three lines are supported in the description. New properties will be applied in alphabetical order. Displaying custom properties on the list and detail pages is supported.



4.28.3 Adding Customized Fields to the Search Criteria

Context

The object detail screens in SAP Service and Asset Manager can be modified to include properties of the oData entity set that are not part of the detail screen out of the box. To do this, simply change the backend configuration and then synchronize with the mobile client.

Procedure

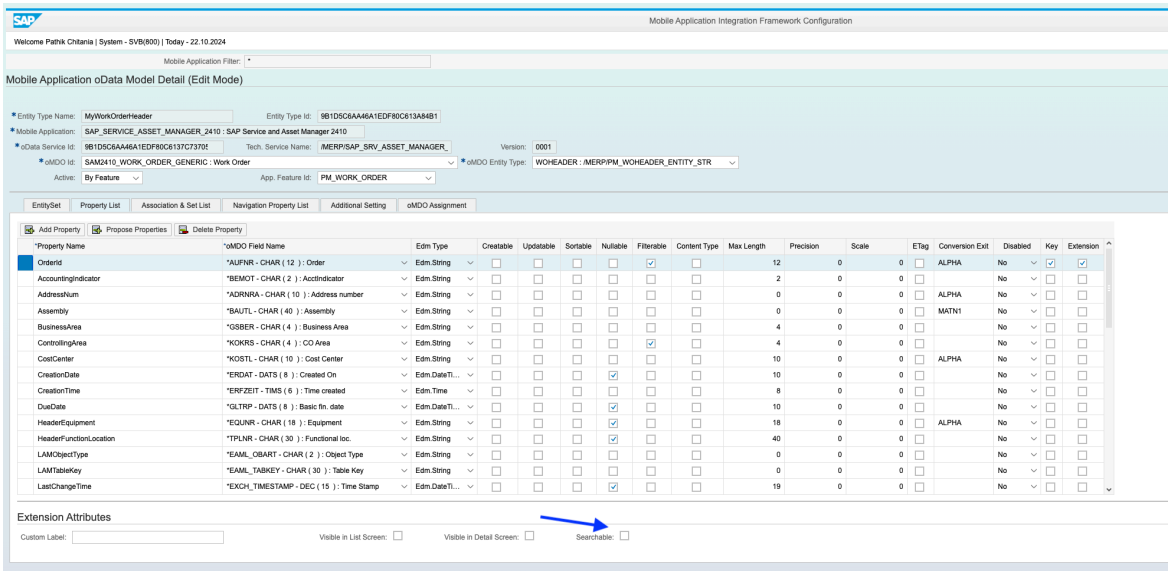
1. Navigate to *oData Model Configuration*.
2. Open *SAP_SERVICE_ASSET_MANAGER_XXXX* and find the entity you want to change on the mobile client.

3. Navigate to the *Property List* tab and select the new oData entity set property that should appear on the object detail screen.

> **Note**
>
> Custom Z properties are also supported. You can enable a searchable field for any property. The value of this property will be used when searching the list page.

4. Click the *Extension* check box.

   The *Extension Attributes* section appears.



5. Enter the label to be used on the mobile client for this property if necessary. If this value is empty, the default data item field label associated with the oMDO entity type structure component will be used.
6. Click the *Searchable* check box.
7. Save changes and select a customization request if necessary.
8. Synchronize from a mobile device.

4.29 Meter Management Configuration

The Meter Management component is delivered out of the box with predefined settings, which you can change according to your back-end system setup. The following settings, however, have to be set:

- Binding Industry Solutions & Utilities (ISU) process type to work order type
- Setting the optimal meter reading history
- Binding meter reading reason relevant for technical installation
- Binding meter reading notes based on the ISU process type

4.29.1 Binding ISU Process Type to Work Order Type

Binding the ISU process type to the work order type provides the SAP Service and Asset Manager application the correct representation of what process type is being conducted with the different work order types. This binding is located in the **SAMXXXX_ORDER_ISULINK** OMDO, under the *Read* filter. You can update these filters according to your business process.

All assignment types are supported for the Meter Management component.

The following filters represent binding criteria for different process types. By default, the ISU process types are bound to order types as follows:

Filter Name	Type	Value	Comments
ORDTYPE_DISCONNECT	Standard Filter Mandatory	DC01 RC01	Used for the disconnect process
ORDTYPE_INSTALL	Standard Filter Mandatory	SM01	Used for the installation process
ORDTYPE_READING	Standard Filter Mandatory	MR01	Used for the meter reading process
ORDTYPE_REMOVE	Standard Filter Mandatory	CU01	Used for the remove process
ORDTYPE_REPAIR	Standard Filter Mandatory	SM02	Used for the repair process
ORDTYPE_REPLACE	Standard Filter Mandatory	RP01	Used for the replace process

To change the default binding for a particular process, complete the steps below:

1. On the ConfigPanel home page, choose *OData Mobile Data Object Configuration*.
   Make sure that you select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. From the *OData Mobile Data Object List* select desired OMDO object, such as **SAMXXXX_ORDER_ISULINK**, and then click the *Data Filter* tab.
3. Expand the *Defined Filters* list under the *READ* operation with the standard filter. Select the filter that you want to update from the list of available filters as listed in the table in this topic. Choose the *Change* button from the menu.
4. Set the order type for the desired process type you have selected.
5. Save your changes.

4.29.2 Binding Meter Reading Notes Based on ISU Process Type

The back end ISU system configuration specifies which meter reading notes are relevant for the major ISU process types. This configuration has to be replicated in the OData Mobile Data Object **SAMXXXX_METER_READING_NOTE** under the *READ* operation with the standard filters, so that the SAP Service and Asset Manager application reflects the proper meter reading notes for a specific process type. The default configuration lists the meter reading notes relevant for the ISU process. However, you can change it if you have different requirements in your back end configuration.

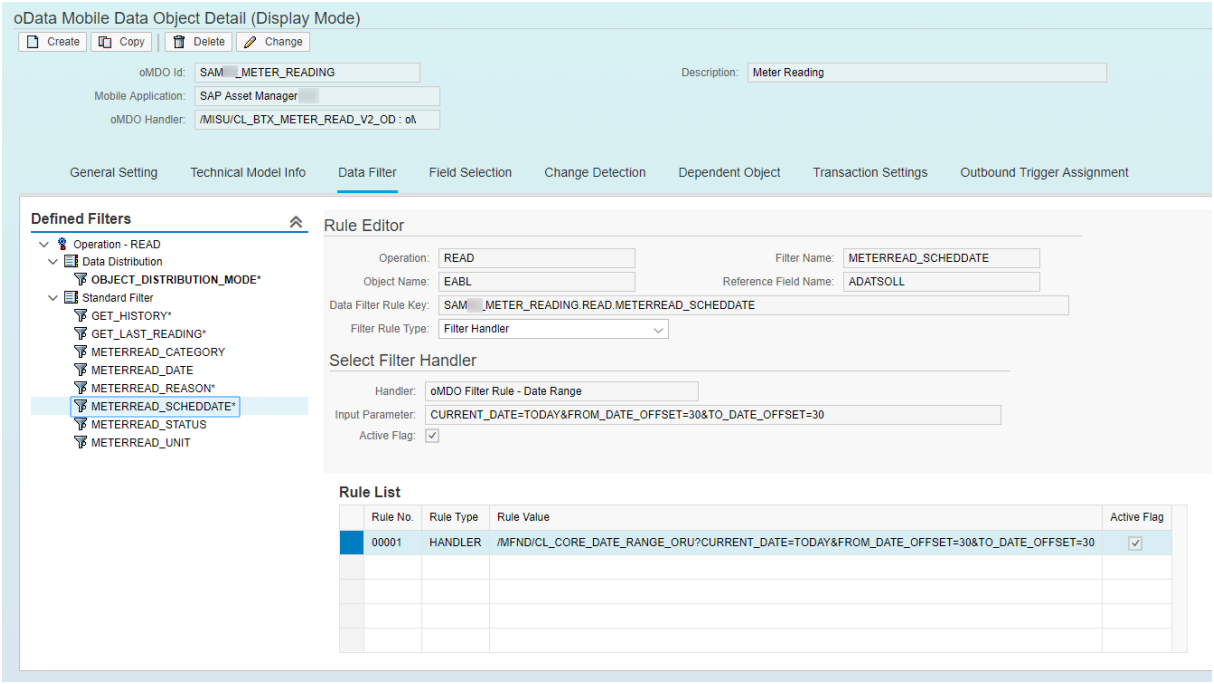
Filter Name	Type	Value	Comments
DISCONNECT_NOTE_REMOVE	Standard Filter, Mandatory	01 04 05	Used for the disconnect notes for the remove process
METERREAD_NOTE _INSTALL	Standard Filter, Mandatory	01 04	Used for the meter reading notes for the installation process
METERREAD_NOTE _REMOVE	Standard Filter, Mandatory	04 05	Used for the meter reading notes for the remove process

To change the default binding for a particular process, complete the following steps:

1. On the ConfigPanel home page, choose *OData Mobile Data Object Configuration*.
   Make sure you select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. From the *OData Mobile Data Object List* select desired OMDO object, such as **SAMXXXX_METER_READING_NOTE**, and then click on the *Data Filter* tab.
3. Expand the *Defined Filters* list under the *READ* operation with the standard filter. Select the filter that you want to update from the list of available filters as listed above. Choose the *Change* button from the menu.
4. Set the meter reading note for the desired ISU process type you have selected.
5. *Save* your changes.

4.29.3 Meter Reading History Interval Definition

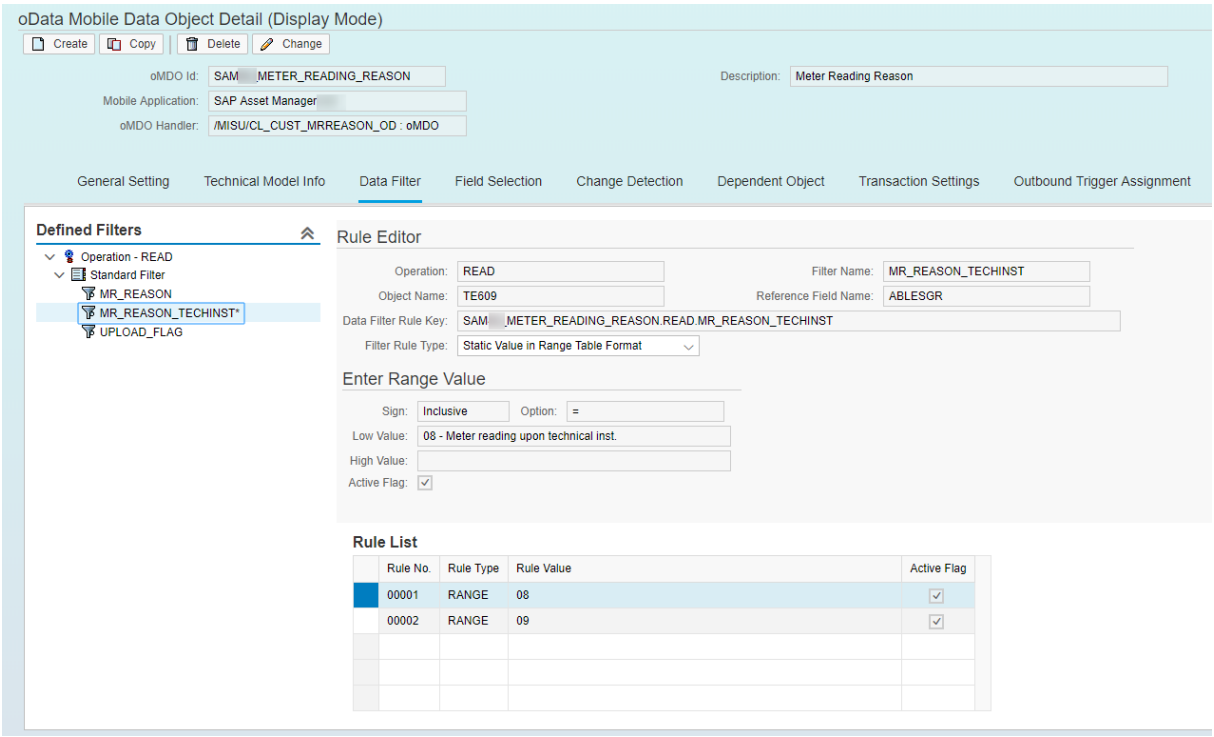
The default setting for meter reading history is to include all meter readings from the past 30 days till the current day. If you have a different requirement, you can change it from the OData Mobile Data Object **SAMXXXX_METER_READING** under the READ operation with the standard filter *METERREAD_SCHEDDATE* as shown in the following example.



4.29.4 Binding Meter Reading Reasons Relevant for Technical Installation

The back end ISU system configuration specifies explicitly which meter reading reasons are relevant for technical installation. These are the only reasons displayed on the SAP Service and Asset Manager application when completing a meter reading during the technical installation process. Set this binding in the OData Mobile Data Object **SAMXXXX_METER_READING_REASON** under the *READ* operation with the standard filter *MR_REASON_TECHINST*.

The default configuration contains meter reading reasons *08* and *09* as required for technical installation. If you have different requirements for your back end configuration, you can change these defaults.



4.30 Namespace Check Configuration

SAP provides namespace check for the following configuration areas:

- oMDO class
- oData Model Entity Type Name
- Entity Set Name
- Entity Type Property Name
- Association Name
- Association Set Name
- Navigation Property Name
- Navigation Property Technical Name
- User Attribute

This works so that only Y or Z namespace can be used in the user SAP system while only the partner namespace is allowed in the partner system.

With SAP Service and Asset Manager 2210 or earlier versions, you can bypass namespace checks by setting the *NO_NAMESPACE_CHECK* runtime parameter to X. Namespace bypass is not applicable to the Persona and Feature configuration, whereby a custom or partner namespace remains applicable in those areas and cannot be bypassed.

> **Note**
>
> As of SAP Service and Asset Manager 2305, you can no longer use the runtime parameter to bypass namespace check. A custom or partner namespace is enforced in the above mentioned

configuration areas. For more information on how to set the runtime parameter, see the https://launchpad.support.sap.com/#/notes/2713969 SAP note.

4.31 Push Notifications Configuration

Push notifications enable SAP Service and Asset Manager to inform mobile users when relevant business object changes occur in the SAP back end system, such as newly assigned work orders or notifications.

- Timely communication is essential for technicians and field personnel working with SAP Service and Asset Manager. Push notifications keep you informed about updates that require attention without the need to continuously synchronize the application or manually check for new assignments.
- SAP Service and Asset Manager uses the Mobile Application Integration Framework (MAIF) together with SAP Business Technology Platform Mobile Services to deliver push notifications to registered mobile devices using platform-specific notification services, such as Apple Push Notification Service (APNS) and Firebase Cloud Messaging (FCM).
- When you receive a push notification, you can open SAP Service and Asset Manager and perform a synchronization to download the latest information associated with the business object that triggered the notification.

The end-to-end push notification process consists of the following steps:

1. A business event triggered by a business object change sends a push notification from the SAP back end system to SAP Business Technology Platform Mobile Services. The push notification contains information such as the SAP Business Technology Platform Mobile Services application ID, business object type, object key, recipient user ID, and push message payload.
2. SAP Business Technology Platform Mobile Services receives the push notification and forwards it to the mobile device using Apple Push Notification Service (APNS) or Firebase Cloud Messaging (FCM).
3. SAP Service and Asset Manager receives the push notification.
4. You acknowledge the notification and perform an on-demand synchronization to download the latest data.

Supported Personas

This feature is applicable for the following personas:

Maintenance Technician (Standard)
Maintenance Technician (Pro)
Maintenance Technician (External)
Field Service Technician (Standard)
Field Service Technician (Pro)
Field Service Technician (External)
Inventory Clerk
Safety Technician
Extended Warehouse Clerk
Field Logistics

Prerequisites

Before you configure push notifications, ensure the following:

- SAP Service and Asset Manager is installed and configured.
- SAP Business Technology Platform Mobile Services is available.
- MAIF is installed and configured.
- APNS or FCM is available for the target platform.
- The SAP Service and Asset Manager application is deployed to SAP Business Technology Platform Mobile Services.

Configuration

Perform the following configuration procedures:

1. Configure Push Infrastructure:
   - Configuring SAP Business Technology Platform Mobile Services Push Notification Service (Cloud Foundry) [page 470]
   - Configuring SAP Business Technology Platform Mobile Services Push Notification Service (Neo) [page 471]
   - Configuring MAIF Push Notifications for Cloud Foundry [page 472]
   - Configuring MAIF Push Notifications for Neo [page 474]
2. Configure Push Scenarios:
   - Understanding Push Scenarios [page 476]
   - Creating and Configuring a Custom Push Scenario [page 480]
   - Configuring Push Notification Recipients [page 484]
   - Configuring Push for Work Order Assignment Type 1 [page 489]
   - Configuring Push for Work Order Assignment Type 2 [page 490]
   - Configuring Push for Notification Assignment Types 1 - 5 [page 491]
3. Activate Push Processing:
   - Setting Up the Outbound Trigger for Your Push Configuration [page 493]
   - Activating Default Push Services on the Neo Platform [page 496]
   - Activating Default Push Services on the Cloud Foundry Platform [page 504]
   - Configuring Push for the Android Platform [page 511]

Result

After you complete the configuration, SAP Service and Asset Manager can receive push notifications generated by business object changes in the SAP back end system. SAP Business Technology Platform Mobile Services delivers notifications to registered devices using APNS or FCM. You can synchronize the application to retrieve the latest business data.

4.31.1 Configuring the Push Infrastructure

4.31.1.1 Configuring SAP Business Technology Platform Mobile Services Push Notification Service (Cloud Foundry)

Configure SAP Business Technology Platform Mobile Services to support push notification processing in a Cloud Foundry environment. This procedure describes how to enable the **Mobile Push Notification** feature, create a service key, and obtain the API information required for SAP Service and Asset Manager push notification configuration.

Prerequisites

Before you begin, ensure the following:

- SAP Business Technology Platform Mobile Services is available.
- An SAP Service and Asset Manager mobile application exists in SAP Business Technology Platform Mobile Services.

Context

To enable push notification delivery in a Cloud Foundry environment, configure SAP Business Technology Platform Mobile Services for SAP Service and Asset Manager. This configuration provides the Push API URL and API Key required for subsequent back end and MAIF push notification configuration.

Procedure

1. Enable the **Mobile Push Notification** feature:
   - Open the SAP Service and Asset Manager Native / Hybrid application in SAP Business Technology Platform Mobile Services.
   - Open the **Info** tab.
   - Verify that the **Mobile Push Notification** feature is assigned.
   - If the feature is not assigned, add it.
2. Configure the feature.

   Maintain the following value:

Setting	Value
Predefined Global Push Configuration	SAP Service and Asset Manager

3. Create a service key with the following settings:

Setting	Value
Alias	SAPServiceandAssetManagerPushService
Assign Roles	Push_single, Push_all, Push_multiple, Register_onbehalf, PushRegistrations_read

4. Record the following information for later configuration:
   - Push API Key
   - Push API URL

   The URL format is: `https://<host_name>/<push_service_identifier>`.

Results

SAP Business Technology Platform Mobile Services is configured for push notification processing in the Cloud Foundry environment.

4.31.1.2 Configuring SAP Business Technology Platform Mobile Services Push Notification Service (Neo)

Configure SAP Business Technology Platform Mobile Services to support push notification processing in a Neo environment. This procedure describes how to enable the **Push Notification** feature and obtain the **Enhanced Push API** information required for SAP Service and Asset Manager push notification configuration.

Prerequisites

Before you begin, ensure the following:

- SAP Business Technology Platform Mobile Services is available.
- An SAP Service and Asset Manager mobile application exists in SAP Business Technology Platform Mobile Services.

Context

To enable push notification delivery in a Neo environment, configure SAP Business Technology Platform Mobile Services for SAP Service and Asset Manager. This configuration provides the **Enhanced Push API URL** required for subsequent back end and MAIF push notification configuration.

Procedure

1. To enable the **Push Notification** feature:
   - Open the mobile application in SAP Business Technology Platform Mobile Services.
   - Open the **Info** tab.
   - Verify that the **Push Notification** feature is assigned.
   - If necessary, add the feature.
2. Configure the feature with the following settings:

Setting	Value
Predefined Global Push Configuration	SAP Service and Asset Manager

3. To identify the **Enhanced Push API URL**:
   - Open the APIs tab.
   - Locate the **Enhanced Push API URL**.
     The URL format is:
     `https://<host_name>/restnotification`

Results

SAP Business Technology Platform Mobile Services is configured for push notification processing in the Neo environment.

4.31.1.3 Configuring MAIF Push Notifications for Cloud Foundry

Configure the Mobile Application Integration Framework (MAIF) to communicate with SAP Business Technology Platform Mobile Services in a Cloud Foundry environment. This procedure describes how to maintain outbound trigger settings, create the required RFC destination, configure the MAIF middleware server, and verify mobile user registration information.

Prerequisites

Complete the following:

- Configuring SAP Business Technology Platform Mobile Services Push Notification Service (Cloud Foundry)

Context

To enable push notification processing in a Cloud Foundry environment, configure MAIF to communicate with SAP Business Technology Platform Mobile Services. This configuration includes outbound trigger settings, RFC destination configuration, middleware server maintenance, and mobile user registration verification.

Procedure

1. Update outbound trigger configuration:

   Use transaction `/SYCLO/CONFIGPANEL` to update the following:

   - SSAMNNNN_WORKORDER_TRIGGER_SCPMS
   - SSAMNNNN_NOTIFICATION_TRIGGER_SCPMS

   Configure these attributes:

Attribute	Value
CLOUD_FOUNDRY	True
SCPMS_WITH_SAP_USER_ID	According to BTP identity provider configuration

2. Define RFC destination:

   Use transaction `SM59` to create RFC destination `SSAMNNNN_BTPMS_PUSH_NOTIF`.

   Configure the destination using the **Push API URL** from SAP Business Technology Platform Mobile Services.

   1. Technical Settings
      Configure the HTTP connection as follows:
      - **Target Host**: Host name from the Push API URL
      - **Service No.**: 443
      - **Path Prefix**:

      ```
      /<Push URL GUID>/mobileservices/push/v1/backend/applications/<App ID>/
      notifications/users
      ``
      ```

      Where:
      - **<Push URL GUID>** is the GUID segment of the Push API URL.
      - **<App ID>** is the application ID configured for the mobile application in SAP Business Technology Platform Mobile Services.

      For example:

      ```
      /1/backend/applications/<App Id>/notifications/users
      ```

      In this example, **SAM2511.SVB800** is the application ID maintained in SAP Business Technology Platform Mobile Services.
   2. Logon & Security

Configure the following settings on the **Logon & Security** tab:

- **Logon Procedure**: Basic Authentication
- **User**: Mobile Push Notification Alias
- **Password**: Mobile Push Notification API Key
- **SSL Secure Protocol**: Active
- **SSL Certificate List**: Ensure that the SSL certificate list contains the SAP Business Technology Platform certificate chain and is active.

For additional information about **Push Notification Alias** and **API Key** values, see Configuring SAP Business Technology Platform Mobile Services Push Notification Service (Cloud Foundry) [page 470].

3. Define MAIF middleware server:

   Use `/SYCLO/ADMIN` and navigate to *Administration* > *Server Management*.

   Create a middleware server with these attributes:

Attribute	
Server Name	BTP_MOBILE_SERVICES
Middleware Server ID	BTP
RFC Destination	SSAMNNNN_BTPMS_PUSH_NOTIF

   Maintain the following property:

Property Group	Property
PUSH	X-API-Key

   Enter the API Key obtained from SAP Business Technology Platform Mobile Services.

4. Verify a mobile user registration:

   Verify the CPms User ID in *Administration* > *User Management* > *Client Registration Info*.

Results

MAIF can communicate with SAP Business Technology Platform Mobile Services in a Cloud Foundry environment and submit push notifications for delivery.

4.31.1.4 Configuring MAIF Push Notifications for Neo

Configure the Mobile Application Integration Framework (MAIF) to communicate with SAP Business Technology Platform Mobile Services in a Neo environment. This procedure describes how to create the

required RFC destination, maintain outbound trigger settings, and verify mobile user registration information required for push notification delivery.

Prerequisites

Complete the following:

- Configure SAP Business Technology Platform Mobile Services Push Notification Service (Neo).

Context

To enable push notification processing in a Neo environment, configure MAIF to communicate with SAP Business Technology Platform Mobile Services. This configuration includes RFC destination configuration, outbound trigger settings, and mobile user registration verification required to send push notification requests from the SAP back end system to SAP Business Technology Platform Mobile Services.

Procedure

1. Define RFC destination:
   - Use transaction `SM59`.
   - Create `SSAMNNNN_BTPMS_PUSH_NOTIF`.
   - Configure the destination using the **Enhanced Push API URL**.
2. Update outbound trigger configuration:
   - Use `/SYCLO/CONFIGPANEL`.
   - Update the following:
     - `SSAMNNNN_WORKORDER_TRIGGER_BTPMS`
     - `SSAMNNNN_NOTIFICATION_TRIGGER_BTPMS`
   - Configure the attributes:

Attribute	Value
HTTP RFC Destination	SSAMNNNN_BTPMS_PUSH_NOTIF
CLOUD_FOUNDRY	False
BTPMS_WITH_SAP_USER_ID	According to BTP identity provider configuration

3. Verify a mobile user registration:
   - Use `/SYCLO/ADMIN`.
   - Go to *Administration* > *User Management*.
   - Verify CPms User ID values.

Results

MAIF can communicate with SAP Business Technology Platform Mobile Services in a Neo environment and submit push notifications for delivery.

4.31.2 Configuring the Push Scenarios

4.31.2.1 Understanding Push Scenarios

Push scenarios define the complete conditions for delivering push notifications to mobile users of SAP Service and Asset Manager.

A push scenario controls the following:

- When a push notification is triggered
- What business data is associated with the notification
- Which mobile users receive the notification
- How the notification is delivered to mobile devices

Push scenarios are configured in the ConfigPanel under *Push Framework Settings* > *Push Scenario Definition*.

> **Note**
>
> Before notifications can be delivered, activate a push scenario and link it to a source object, distribution rules, and at least one outbound trigger.

Supported Personas

This feature is applicable for the following personas:

Prerequisites

Before you configure push scenarios, ensure that the push notification infrastructure is configured in SAP Business Technology Platform Mobile Services and in the SAP back end system.

Push Scenario Components

The SAP Service and Asset Manager push architecture consists of the following components:

- **xChange Objects**

The **xChange** framework detects changes to business objects in the SAP back end system and determines whether push processing should be initiated.

Push-relevant changes are defined in the **Push Settings** tab of an **xChange Object** configuration. You can configure change detection conditions so that push processing is triggered only when specific criteria are met. For example, you can restrict push processing to a specific work order type or priority.

> Example
>
> `SAMnnnn_WORK_ORDER_PUSH`

> Note
>
> Configure an **xChange Object** as **Push Relevant** in the **Push Settings** tab before you select it as a **Source Object** in a **Push Scenario Definition**.

- **OData Mobile Data Objects (OMDOs)**
  OData Mobile Data Objects (OMDOs) define the mobile data payload and determine how business data is structured and made available to the mobile application.
  In push processing, **Push OMDOs** determine which mobile users qualify to receive a push notification.
  Two OMDO types are commonly used in push processing:
  - **Data Synchronization OMDOs**: Distribute business object data during application synchronization. These **OMDOs** reference a **Lead xChange Object** that identifies changed records for delta synchronization. This allows only changed records to be sent to the device instead of the full data set during each synchronization.

    > Example
    >
    > `<APPXX>_WORK_ORDER_GENERIC`

  - **Push OMDOs**: Used during push processing. They are assigned to a push scenario as the **Distribution Object** and determine which mobile users qualify to receive the notification. Recipient selection is typically based on the **Assignment Type** filter defined in the **Push OMDO** configuration. In most cases, a **Push OMDO** assignment type filter aligns with the assignment type filter of the corresponding **Data Sync OMDO**.

    > Example
    >
    > `<APPXX>_WORK_ORDER_PUSH`

Push Scenario Definition – The Orchestrator

The **Push Scenario Definition** is the central configuration that connects **xChange Object**, **OMDO**, and **Outbound Trigger**.

Configure the **Push Scenario Definition** in the ConfigPanel under *Push Framework Settings* > *Push Scenario Definition*.

The most important settings include the following:

- The **General Data** tab
  It contains the primary push configuration:

1. **Source Type** defines what triggers the push. When the xChange Object option is used, push processing starts when the configured source object detects qualifying data changes.
2. **Source Object** and **Source Handler** identify the xChange Object and its handler class that provide change events for the push scenario.
3. **Distribution Type** defines the distribution criteria and the recipients targeted through the configured **Push OMDO**.
4. The scenario must be activated before notifications can be generated.

- The **Outbound Trigger** tab
  One or more outbound triggers can be assigned to a push scenario. Assigned outbound triggers are invoked at the end of push processing according to the configured execution sequence. Each assigned trigger must be enabled by selecting the **Enable Outbound Trigger** checkbox.

Outbound Triggers — Delivering to BTP Mobile Services

An **Outbound Trigger** is a handler-based function that runs an action after push processing is complete.

In SAP Service and Asset Manager, outbound triggers act as the bridge between the SAP back end system and SAP Business Technology Platform Mobile Services.

Configure outbound triggers in the ConfigPanel under *Push Framework Settings* > *Outbound Trigger Configuration*.

The configuration requires the following:

- An **HTTP RFC Destination** pointing to the SAP BTP Mobile Services push API endpoint
- The correct **Mobile Services Application ID**
- The **CLOUD_FOUNDRY** parameter set to **True** for Cloud Foundry deployments.

SCPMS_WITH_SAP_USER_ID Parameter

Some SAP BTP environments allow users to sign in to Mobile Services using the same user ID used for SAP back end authentication. In these environments, enable the **SCPMS_WITH_SAP_USER_ID** parameter. For example, this may be required when SAP Business Technology Platform Mobile Services and the SAP back end system share the same **Identity Authentication Services (IAS)** trust configuration.

SAP Business Technology Platform Mobile Services — Final Delivery

SAP Business Technology Platform Mobile Services is the cloud component that receives the push notification payload from the SAP back end system and routes it to the user's device.

Its responsibilities include the following:

- Receiving the HTTP push request from the SAP back end outbound trigger
- Looking up the registered device token for the user
- Forwarding the notification payload to **Apple Push Notification Service (APNS)** or **Firebase Cloud Messaging (FCM)**
- Delivering the notification to the SAP Service and Asset Manager application.

To support push notifications, configure the following prerequisites in SAP Business Technology Platform Mobile Services:

- The **Mobile Push Notification** feature is assigned to the mobile application definition (`SAP_SERVICE_AND_ASSET_MANAGER_NNNN_OAUTH`).
- A push API connection is created.
- The following roles are assigned:
  - `Push_single`
  - `Push_all`
  - `Push_multiple`
  - `Register_onbehalf`
  - `pushRegistrations_read`
- APNS certificates are configured for iOS devices.
- FCM configuration is maintained for Android devices.

End-to-End Push Flow

The following sequence illustrates how the components interact during push notification processing:

1. A change occurs to a business object in the SAP back end system.
2. The **xChange** framework detects the change and evaluates the configured push-relevant conditions.
3. The **Push Scenario Definition** determines whether the change qualifies for push processing.
4. The **Push OMDO** determines which mobile users are eligible to receive the notification.
5. The assigned **Outbound Trigger** sends the push notification request to SAP Business Technology Platform Mobile Services.
6. SAP Business Technology Platform Mobile Services identifies the recipient's registered mobile device.
7. SAP Business Technology Platform Mobile Services forwards the notification through **Apple Push Notification Service (APNS)** or **Firebase Cloud Messaging (FCM)**.
8. The mobile device receives the notification.
9. The user opens SAP Service and Asset Manager and synchronizes the application to retrieve the latest business data.



4.31.2.2 Creating and Configuring a Custom Push Scenario

A custom push scenario defines how SAP Service and Asset Manager detects business object changes, determines push recipients, and delivers push notifications to mobile users.

Prerequisites

Before you begin, ensure the following:

- A **custom xChange** handler is developed, if required.
- A **custom Push OMDO** handler is developed, if required.
- The **Mobile Push Notification** feature is enabled on your SAP Business Technology Platform Mobile Services application definition (`SAP_SERVICE_AND_ASSET_MANAGER_NNNN_OAUTH`).
- A push **API HTTP** connection is configured in SAP Business Technology Platform Mobile Services with the following roles:
  - `Push_single`
  - `push_all`
  - `push_multiple`
  - `register_onbehalf`
  - `pushRegistrations_read`
- An **HTTP RFC** destination from the SAP back end system to the SAP Business Technology Platform Mobile Services push API endpoint is created.
- An **APNS certificate (iOS)** or **FCM server key/sender ID (Android)** is configured in the mobile application definition in SAP Business Technology Platform Mobile Services.

Access ConfigPanel using transaction `/n/SYCLO/CONFIGPANEL`.

Context

A custom push scenario consists of the following phases:

1. Configure the **custom xChange Object** (optional).
2. Verify **EFI** assignment.
3. Configure the **Push OMDO** (optional).
4. Configure the outbound trigger.
5. Create and configure the **Push Scenario Definition**.

You must complete each phase before proceeding to the next phase.

Phase 1.1: Configure the Custom xChange Object (Optional)

> ⓘ Note
>
> Perform this phase only when using a **custom xChange** handler.

The **xChange** object is the source of change detection and must be marked as **Push Relevant** before you can select it as a source object in a **Push Scenario Definition**.

Exchange table update is not required for **Push xChange**.

1. In ConfigPanel, navigate to MAIF *Configuration* *Exchange Object Configuration*.
2. Set the **Mobile Application Filter** to the target application.
3. Select an existing exchange object and select **Copy**. Rename the new object using a **Z** or **Y** namespace. Alternatively, create a new exchange object when extending a custom business object.
4. On the **Technical Settings** tab, configure the following options:
   - Set the **Exchange Handler Class**. Use a subclass of `/SYCLO/CL_CORE_EX_HANDLER_BASE` or an appropriate standard handler.
   - Set the **Exchange Table** reference.
   - Select the **No Exchange Table Update** checkbox.
5. On the **Change Detection Field Selection** tab, select the SAP object fields that trigger change detection when modified.
6. On the **Change Detection Condition Filter** tab, define filter conditions that determine whether a change is relevant for push processing.
7. On the **Push Settings** tab, select the **Push Relevant** checkbox.

   > **Note**
   >
   > This setting is mandatory. Without it, the exchange object does not appear in the **Source Object** list of the **Push Scenario Definition**.

8. Save the configuration.

Phase 1.2: Verify EFI Assignment

> **Note**
>
> The **xChange Object** must be active in **EFI assignments** so that it is triggered when business objects change in the back end system.

1. In ConfigPanel, navigate to MAIF *Configuration* *EFI Assignment*.
2. Locate the **EFI Include** or **Enhancement Implementation** associated with the business object, for example `/MERP/EFI_PM`.
3. Verify that the **xChange Object** configured in Phase 1 is assigned.
4. Verify that the **Active** flag is selected.
5. Save the configuration.

Phase 2: Configure the Push OMDO (Optional)

> **Note**
>
> Perform this phase only when using a **custom Push OMDO** handler.
>
> The **Push OMDO** defines push object filters and typically determines push recipients through the `ASSIGNMENT_TYPE` data filter.

To configure the **Push OMDO**, follow these steps:

1. In ConfigPanel, navigate to OData Mobile Data Object Configuration.
2. Set the **Mobile Application Filter** to the target application.
3. Copy an existing **Push OMDO**, such as `_WORK_ORDER_PUSH`, and rename it using a **Z** or **Y** namespace.
4. On the **General Settings** tab, complete the following:
   - Verify that the **OMDO Handler Class** is appropriate for the object type.
   - Disable**Client State Tracking**.
   - Disable **Periodic Refresh**.
   - Disable **Delta Sync**.
   - Select **Exempt Read Entity Request**.
5. On the **Data Filter** tab, complete the following:
   - Add an `ASSIGNMENT_TYPE` filter value.
   - Add any additional filters required by the scenario.
6. Save the configuration.

Phase 3: Configure the Outbound Trigger

The outbound trigger calls SAP Business Technology Platform Mobile Services through HTTP after push processing is completed.

1. In ConfigPanel, navigate to *Push Framework Settings* > *Outbound Trigger Configuration*.
2. Set the **Mobile Application Filter** to the target application.
3. Reuse an existing outbound trigger, such as one of the following:
   - `SAMnnnn_WORKORDER_TRIGGER_SCPMS`
   - `SAMnnnn_NOTIFICATION_TRIGGER_SCPMS`

   Alternatively, create a new outbound trigger using a **Z** or **Y** namespace.
4. On the **General Data** tab, maintain the following settings:

Attribute	Value / Notes
Outbound Trigger ID	`ZSAMnnnn_CUSTOM_TRIGGER_SCPMS`
Outbound Trigger Handler	`/MFND/CL_CORE_OTRIG_CPMS_PUSH`
Outbound Trigger Type	HTTP based trigger
RFC Destination	Your HTTP RFC destination pointing to the SAP Business Technology Platform Mobile Services push API endpoint
Cloud Platform Mobile Application ID	Application ID configured in BTP
Allow Retry	Checked
Maximum Number of Retries	10
Active Flag	Checked

5. On the **Parameters** tab, maintain the following settings:

Attribute	Value / Notes
CLOUD_FOUNDRY	True (required for Cloud Foundry deployments)

Attribute	Value / Notes
SCPMS_WITH_SAP_USER_ID	True if an SAP user ID is used to authenticate in BTP; False if a custom IdP is in use

6. Save the configuration.

Phase 4: Create and Configure the Push Scenario Definition

This phase binds the **xChange Object**, **Push OMDO**, and **Outbound Trigger**.

1. In ConfigPanel, go to *Push Framework Settings* > *Push Scenario Definition*.
2. Set the **Mobile Application Filter** to the target application.
3. Select **New**.

General Data Tab

Maintain the following values:

Field	Value / Notes
Scenario ID	Your unique **Z/Y** namespace ID, max 40 characters. Must match the `SCENARIO_ID` data filter set in your push OMDO (Phase 2).
Mobile Application	Your target mobile application name
Description	Free-text description of the scenario
Source Type	`xChange Object` — push fires when qualifying data changes are detected
Source Object	Select the xChange Object configured in Phase 1 (only appears here if it was marked Push Relevant in Phase 1), or standard xChange Object for push
Source Handler	Handler class associated with the selected xChange Object
Distribution Type	`OData Mobile Data Object`
Distribution Object	Select the push OMDO created in Phase 2, or standard push OMDO
Subscriber Type	All mobile users
Validity	Duration in hours for which a generated push instance remains valid
Priority	Processing priority; higher value = processed first
Disable Owner Originated Push	Check this if the user who made the object change should not receive the notification
Active	Must be checked to enable the scenario

Event Setting Tab

Configure the following settings:

- Select **Disable Background Event Trigger**.
- Select **Enable qRFC Processing**.
- Enter a queue name, for example: `SAMnnn_EM_&OBJKEY&`.

- Select a qRFC rule, for example: `/SYCLO/CL_CORE_QRFC_ROUTINE`.
- Under **Runtime Parameters**, configure the following options:
  - Select **Allow Instance Merge**.
  - Select **Exclude Status SRV_COMP**.
  - Set **Maximum Select Delay** to **1**.
  - Set **Select Retry** to **10**.

Outbound Trigger Tab

To configure the outbound trigger, complete the following steps:

1. Select **Use Single Instance Processing**.
2. Select **Add** and assign the outbound trigger configured in Phase 3.
3. Select the assigned outbound trigger.
4. Select **Enable Outbound Trigger**.

   > ⓘ Note
   >
   > Assigning an outbound trigger without enabling it has no effect.

   Subscription Settings Tab
   Leave **Allow Subscription** unselected for standard OData-based SAP Service and Asset Manager applications.
5. Save the **Push Scenario Definition**.

Results

The custom push scenario is configured and activated. The configured xChange Object detects qualifying business object changes, the Push OMDO determines eligible recipients, and the outbound trigger sends push notification requests to SAP Business Technology Platform Mobile Services.

4.31.2.3 Configuring Push Notification Recipients

Recipient determination is a two-stage SAP process that identifies who receives push notifications and how those notifications reach their devices. Push notification recipients are determined by the **Push OMDO distribution rules and assignment types** in the SAP back end system. The notification reaches the device based on the user identity mapping between the SAP back end system and SAP Business Technology Platform Mobile Services.

Use recipient determination to ensure push notifications are correctly configured and delivered to the right mobile users.

Supported Personas

This feature is applicable for the following personas:

Prerequisites

Before you configure push notification recipients, ensure that push notifications are configured in the SAP back end system and SAP Business Technology Platform Mobile Services.

Configuration

Stage 1 — OMDO-Driven Recipient Determination (SAP Back End)

The Role of the Push OMDO

The **Push OMDO** (for example, `_WORK_ORDER_PUSH` or `_NOTIFICATION_PUSH`) is the primary component that determines recipients.

When a push instance is created, triggered by the **xChange Object** detecting a qualifying back end change, the push process agent reads the **Push OMDO** to:

- Resolve the list of eligible recipients for the changed object
- Determine the data payload to include in the push.

The OMDO uses its own handler logic to query back end tables, such as work order assignment data or notification responsible person data, and returns a list of SAP user IDs that should receive the notification.

The implementation logic is in the following method of the Push OMDO class:

`/SYCLO/IF_CORE_PUSH_SERV~DETERMINE_PUSH_RECIPIENTS`.

The push scenario's **Distribution Object** field identifies the **Push OMDO**.

Assignment Types and Distribution Rules

The assignment type is the core rule that governs how the back end system maps a business object, such as a work order or PM notification, to a specific mobile user.

The assignment type is configured on the **data synchronization OMDO** (for example, `<SAMXXXX>_WORK_ORDER_GENERIC`) using the `WO_ASSIGNMENT_TYPE` filter.

The **Push OMDO** typically carries the same assignment type filter to ensure consistency.

The distribution rules of the **Push OMDO** must match the distribution rules in the corresponding **data synchronization OMDO**.

Subscriber Type

The **Subscriber Type** setting in the **General Data** tab of the **Push Scenario Definition** defines the pool of users that the push processing engine searches when resolving recipients.

It does not define routing logic itself, but acts as a filter on which users are considered as potential recipients before the distribution rule is applied.

The **Subscriber Type** corresponds to the mobile user population within MAIF, for example, all registered mobile users for a specific mobile application. This ensures that push notifications are sent only to active mobile users and not to SAP users who do not use the mobile application.

Disable Owner Originated Push

When you select **Disable Owner Originated Push** in the **General Data** tab of the **Push Scenario Definition**, the user who made the object change is excluded from the recipient list.

This is useful when a planner or dispatcher updates a work order and should not receive the notification intended for the assigned technician.

Stage 2 — User Identity Mapping

Once the back end system resolves a list of SAP user IDs as recipients, the Outbound Trigger translates those SAP user IDs into **SAP Business Technology Platform Mobile Services user identities** so that the correct registered device receives the notification.

The identity model of the SAP Business Technology Platform Mobile Services subaccount determines how this mapping is performed.

The Push Notification Payload

The push notification sent from the SAP back end system to SAP Business Technology Platform Mobile Services contains the following information:

- **SAP Business Technology Platform Mobile Services Application ID**, which identifies the target mobile application
- **SAP business object type and object key**, for example a work order number
- **Push recipient user ID**
- **Push message payload**, including notification title and body.

The push recipient user ID is the critical field. SAP Business Technology Platform Mobile Services uses this value to look up the user registration list and locate the device token (APNS or FCM) used for notification delivery.

If the user ID sent by the SAP back end system does not match the user ID stored in SAP Business Technology Platform Mobile Services, no device is found and no notification is delivered.

SAP User ID and BTP User ID

SAP Service and Asset Manager supports two identity models controlled by the `SCPMS_WITH_SAP_USER_ID` parameter in the **Outbound Trigger** configuration.

Scenario	Parameter Value	Behavior
SAP back end user ID = BTP user ID (same identity store)	True	The back end system sends the SAP user ID as the recipient identifier. SAP Business Technology Platform Mobile Services resolves the device using the same ID.
SAP back end user ID ≠ BTP user ID (separate identity providers)	False	The back end system uses the BTP-side user ID. You must maintain this value as the CPms User ID in the MAIF mobile user record.

SCPMS_WITH_SAP_USER_ID = True

Use this setting when users log on to both the SAP back end system and SAP Business Technology Platform Mobile Services using the same identity.

Examples include the following:

- SAP ID Service (S-users or P-users) used as the identity provider for both systems.
- A single corporate identity provider trusted by both systems and using the same username attribute.

SCPMS_WITH_SAP_USER_ID = False

Use this setting when the SAP Business Technology Platform Mobile Services identity differs from the SAP back end user ID.

Examples include the following:

- Azure AD
- Okta
- Principal propagation scenarios with custom SAML attribute mapping.

The CPms User ID

The **CPms User ID** (**Cloud Platform Mobile Services User ID**) is the BTP-side identity stored in the MAIF mobile user record.

It represents the user identifier that SAP Business Technology Platform Mobile Services recognizes for push notification delivery. It corresponds to the identity the mobile application uses when registering its device token.

Locating the CPms User ID

To locate the **CPms User ID**, follow these steps:

1. Open transaction `/SYCLO/ADMIN`.
2. Navigate to *Administration* > *User Management*.
3. Search for the mobile user.
4. Open the user record.
5. Navigate to the **Client Registration Info** tab.

The CPms User ID field displays the SAP Business Technology Platform Mobile Services user identity stored for that user.

Maintaining the CPms User ID

The **CPms User ID** is populated automatically during the user's initial synchronization.

When the mobile application first connects to the back end system and registers, MAIF captures the authenticated SAP Business Technology Platform Mobile Services identity and stores it in this field.

If the field is empty or incorrect, for example after an identity provider migration, you must update it manually in `/SYCLO/ADMIN`.

Relationship to SAP Business Technology Platform Mobile Services User Registrations

SAP Business Technology Platform Mobile Services maintains a user registration list for each mobile application. The registration list contains user IDs and their associated device tokens.

When the back end system sends a push notification with a recipient user ID, SAP Business Technology Platform Mobile Services looks up that user ID in the registration list and sends the notification to the registered device or devices.

The **CPms User ID** must exactly match the user identifier stored in the SAP Business Technology Platform Mobile Services registration list.

Validation Steps — Verifying Recipient Mapping

If push notifications are delivered to the wrong user or are not delivered at all, complete the following steps:

1. Verify that the assignment type filter on the data synchronization **OMDO** and the **Push OMDO** match.
2. Verify the back end master data. For assignment types 1 and 2, confirm that the responsible person on the work order header or operation has a personnel number linked to an SAP user.
3. Verify that the mobile user exists in `/SYCLO/ADMIN → User Management`. A user is created only after an initial synchronization.
4. Check the CPms User ID in `/SYCLO/ADMIN → User → Client Registration Info`. If `SCPMS_WITH_SAP_USER_ID = False`, the CPms User ID must contain the correct SAP BTP user identity.
5. Verify the user registration in SAP Business Technology Platform Mobile Services *Push Registrations*. Confirm that the stored user ID matches one of the following conditions:
   - The CPms User ID when `SCPMS_WITH_SAP_USER_ID = False`.
   - The SAP user ID when `SCPMS_WITH_SAP_USER_ID = True`.

Result

Push notification recipients are determined through Push OMDO distribution rules and assignment types in the SAP back end system. Recipients are mapped to registered devices through user identity mapping between the SAP back end system and SAP Business Technology Platform Mobile Services.

4.31.2.4 Configuring Push for Work Order Assignment Type 1

Configure event-based push notifications for work orders assigned using **Assignment Type 1 (header-level person responsible)**. You can configure push for only one work order assignment type at a time.

Context

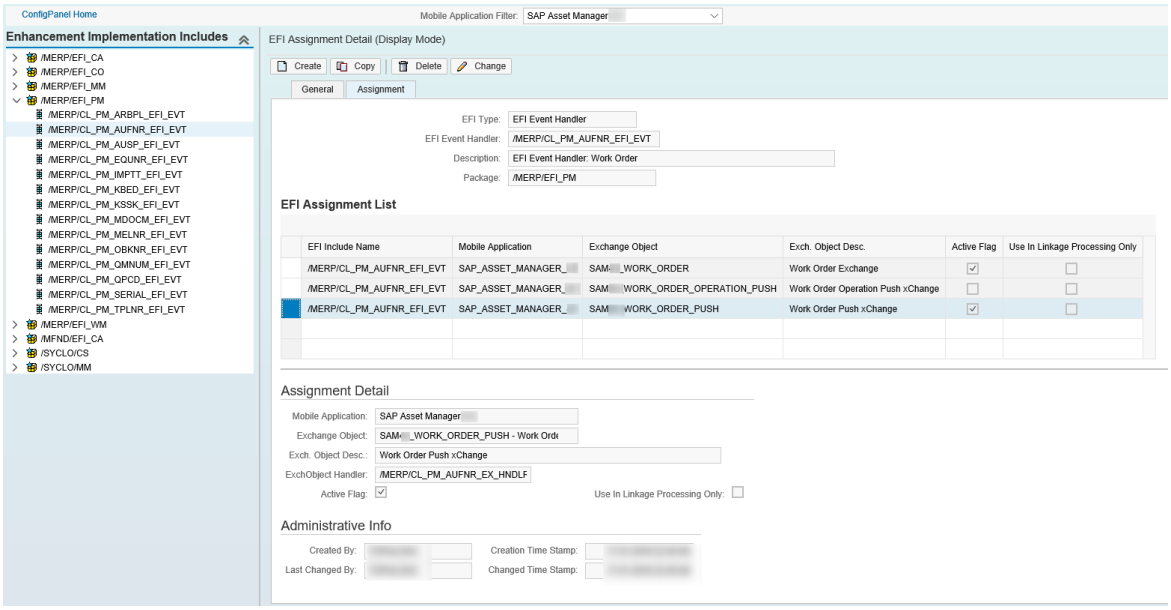
By default, work order push is enabled for the assignment type configured for the work order OMDO. To specify a push assignment type different from the assignment type used by the work order data distribution, manually assign the *WO_ASSIGNMENT_TYPE* filter for your data distribution model.

This procedure describes the configuration for **Assignment Type 1 (header-level person responsible for the work order)**.

Procedure

1. In the ConfigPanel, navigate to the *OData Mobile Data Object Configuration* section and find OMDO **<APPXX>_WORK_ORDER_GENERIC**.
2. On the *Data Filter* tab, ensure the filter *WO_ASSIGNMENT_TYPE* is set to *1*.
3. Return to the ConfigPanel home page and select *Push Scenario Definition*.
4. Ensure that your mobile application is selected in the *Mobile Application Filter*.
5. On the *General Data* tab, ensure the *Active* checkbox is selected for the **<APPXX>_EMERGENCY_WORKORDER_PUSH** scenario.
6. Make sure the configuration in the *Source Setting* and *Distribution Setting* sections are correct.

   By default, the `<Source Object>` for the work order push is the exchange object **<APPXX>_WORK_ORDER_PUSH** with the `<Distribution Object>` **<APPXX>_WORKORDER_PUSH**.
7. Return to the ConfigPanel home page and navigate to the *EFI Assignment* section.
8. In the *Enhancement Implementation Includes* list, select *⏵ /MERP/EFI_PM ⏵ /MERP/CL_PM_AUFNR_EFI_EVT ⏹*.
9. Select the *Assignment* tab.
10. Ensure the *Active* checkbox is selected for the exchange object **<APPXX>_WORK_ORDER_PUSH**.



11. *Save* your changes.

4.31.2.5 Configuring Push for Work Order Assignment Type 2

Configure event-based push notifications for work orders assigned using **Assignment Type 2 (operation-level personnel number)**. You can configure push for only one work order assignment type at a time.

Context

By default, work order push is enabled for the assignment type configured for the work order OMDO. To specify a push assignment type different from the assignment type used by the work order data distribution, manually assign the *WO_ASSIGNMENT_TYPE* filter for your data distribution model.

This procedure describes the configuration for **Assignment Type 2 (operation-level personnel number of the work order)**.

Procedure

1. In the ConfigPanel, navigate to the *OData Mobile Data Object Configuration* section and find OMDO **<APPXX>_WORK_ORDER_GENERIC**. Ensure the filter *WO_ASSIGNMENT_TYPE* is set to *2* on the *Data Filter* tab.
2. Return to the *Home* page of the ConfigPanel. Click the *Push Scenario Definition* link. Ensure that your mobileapplication is selected in the *Mobile Application Filter*.
3. Ensure the *Active* flag for the <APPXX>_EMERGENCY_WORKORDER_OPER_PUSH scenario on the *General Data* tab is checked.

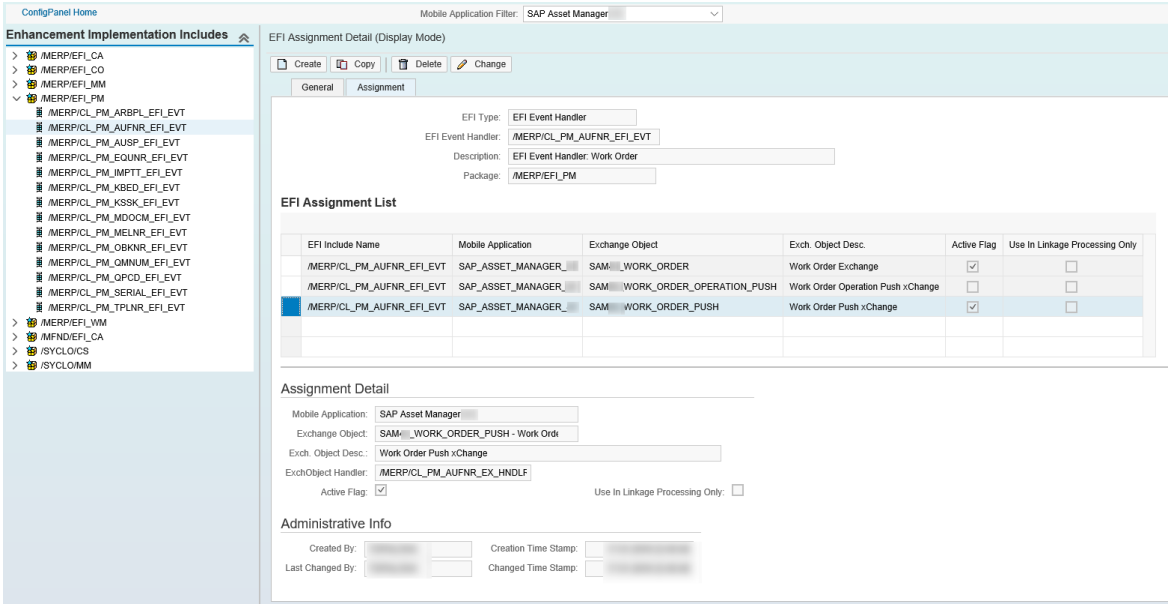
> **Note**
>
> You can have both work order and notification pushes marked as *Active* because they are separate objects.

4. Make sure the configuration in the *Source Setting* and *Distribution Setting* sections are correct.

   By default, the `<Source Object>` for the work order operation push is the exchange object **<APPXX>_WORK_ORDER_OPERATION_PUSH** with the `<Distribution Object>` **<APPXX>_WORKORDER_PUSH**.

5. Return to the ConfigPanel Home page, then navigate to the *EFI Assignment* section. In the *Enhancement Implementation Includes* list, select */MERP/EFI_PM* > */MERP/CL_PM_AUFNR_EFI_EVT*.

6. Click the *Assignment* tab. Ensure the *Active* checkbox is checked for the exchange object **<APPXX>_WORK_ORDER_OPERATION_PUSH**.



7. *Save* your changes.

4.31.2.6 Configuring Push for Notification Assignment Types 1 - 5

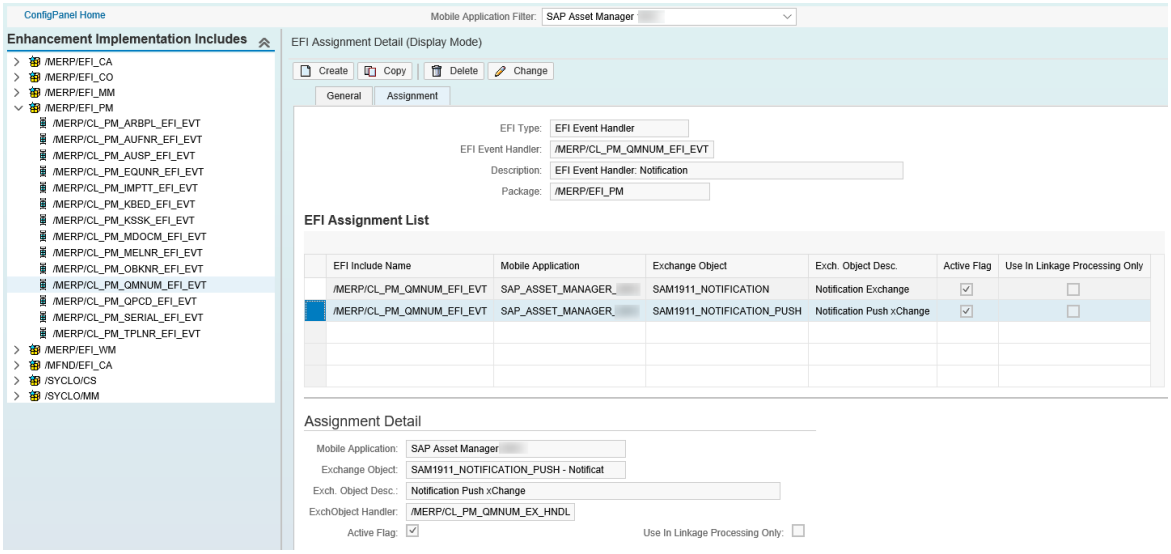
Context

Event-based push is supported for notification assignment types 1 through 5. You can only configure push for one notification assignment type at a time.

By default, notification push is enabled for whichever assignment type your notification OMDO is set to. You can manually assign the *NOTIF_ASSIGNMENT_TYPE* filter for your data distribution model to *1*, *2*, *3*, *4* or *5* to set a push assignment type different to the assignment type of the notification data distribution.

Procedure

1. In the ConfigPanel, navigate to the *OData Mobile Data Object Configuration* section and find OMDO **<APPXX>_NOTIFICATION_GENERIC**. Ensure the filter *NOTIF_ASSIGNMENT_TYPE* is set to the assignment type of your choice (*1* - *5*) on the *Data Filter* tab.
2. Return to the *Home* page of the ConfigPanel. Click the *Push Scenario Definition* link. Ensure that your mobile application is selected in the *Mobile Application Filter*.
3. Ensure the *Active* flag for the **<APPXX>_EMERGENCY_NOTIFICATION_PUSH** scenario on the *General Data* tab is checked. Note that you can have both work order and notification pushes marked as Active because they are separate objects.
4. Make sure the configuration in the *Source Setting* and *Distribution Setting* sections are correct. By default, the `<Source Object>` for the notification push is the exchange object **<APPXX>_NOTIFICATION_PUSH** with the `<Distribution Object>` **<APPXX>_NOTIFICATION_PUSH**.
5. Return to the ConfigPanel Home page, then navigate to the *EFI Assignment* section. In the *Enhancement Implementation Includes* list, select */MERP/EFI_PM* > */MERP/CL_PM_QMNUM_EFI_EVT*.
6. Click the *Assignment* tab. Ensure the *Active* checkbox is checked for the exchange object **<APPXX>_NOTIFICATION_PUSH**.



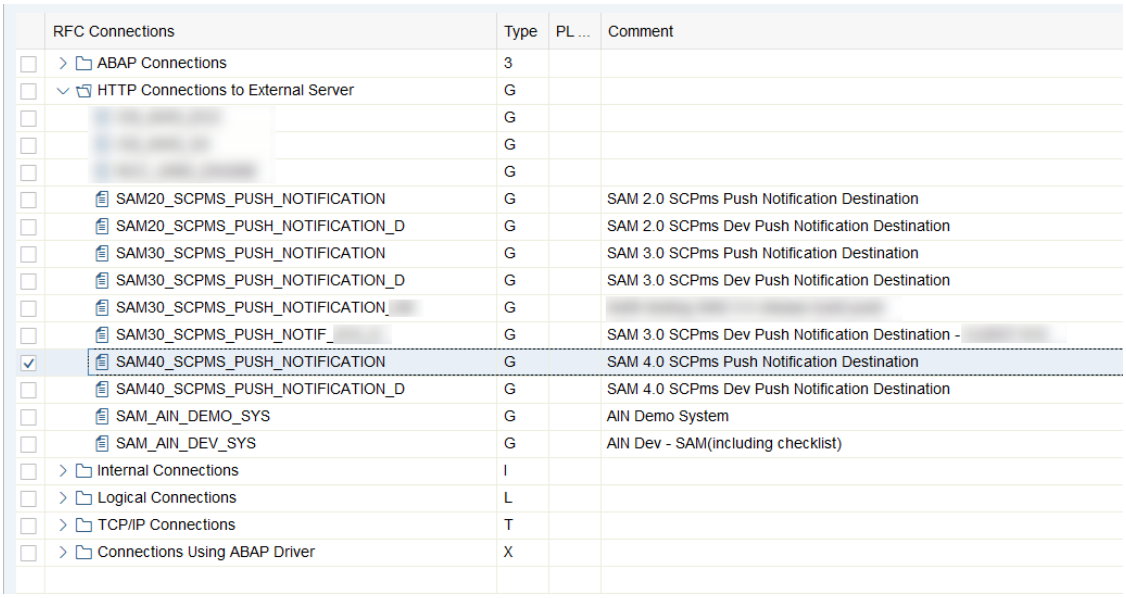
7. *Save* your changes.

4.31.3 Activating the Push Processing

4.31.3.1 Setting Up the Outbound Trigger for Your Push Configuration

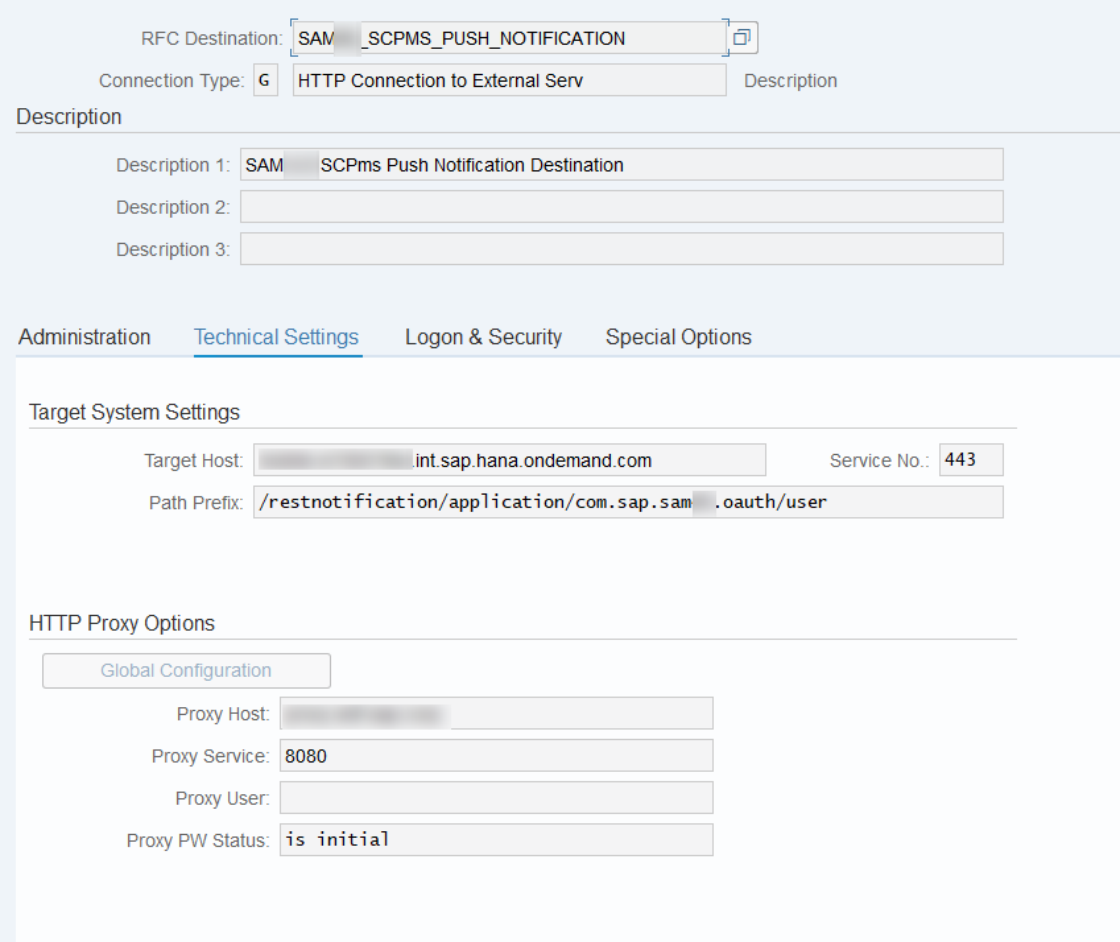
Procedure

1. From the ConfigPanel *Home* page, navigate to the *Outbound Trigger Configuration* section and select your desired mobile application from the *Mobile Application Filter* dropdown menu at the top of the page.
2. From the *Outbound Triggers by Mobile App* list, select the outbound trigger **SAMXXXX_WORKORDER_TRIGGER_SCPMS**. Make sure that the `<Cloud Platform Mobile App ID>` matches your mobile services application ID from SAP Business Technology Platform Mobile Services. By default, the application ID is set to *com.sap.<appXX>.oauth.prod*.
3. Set up the RFC destination **<APPXX>_SCPMS_PUSH_NOTIFICATION** pointing to the mobile services host name using the SAP GUI:
   a. In the SAP GUI, using transaction *SM59*, add the following new RFC destination: **<APPXX>_SCPMS_PUSH_NOTIFICATION** of type *G (HTTP Connection to External Serv)*



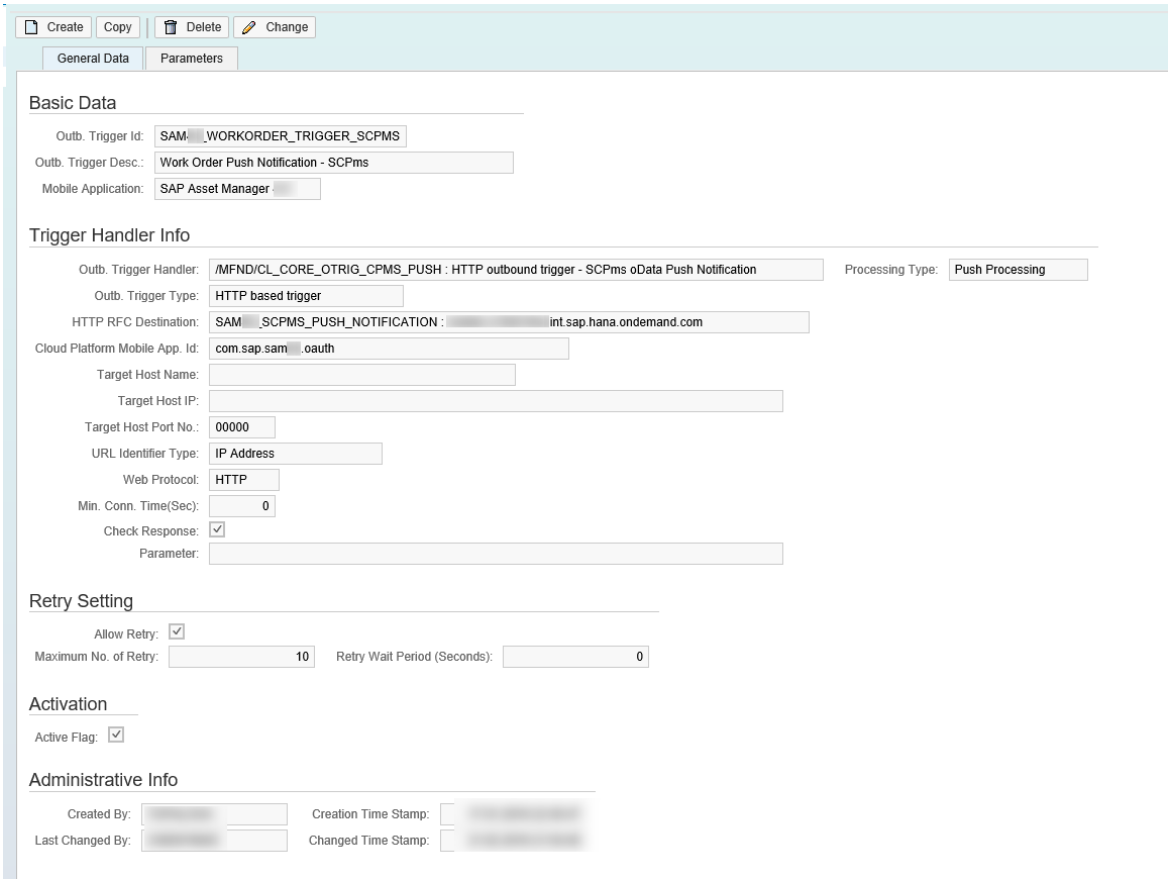
   b. On the *Technical Settings* tab of the new connection, set the *Target Host* to match the push API of the SAP Business Technology Platform Mobile Services. Use service number *443*, which is the port number of the HTTPS connections.

> **Note**
>
> If necessary, configure the proxy that you are using to allow your back-end systems to connect to the Internet.



c. On the *Logon & Security* tab, under the *Logon Procedure*, select *Basic Authentication*. Enter the user name and password of the service user. Assign the *Notification User* role to this service user in the SAP Business Technology Platform Mobile Services configuration to ensure that the user is allowed to utilize the push notification service.
d. In the *Security Options* section of the *Logon & Security* tab, ensure that the *SSL* is set to *Active*.
e. In the *Security Options* section, ensure that the *SSL Certificate List* contains the SAP Business Technology Platform certificate chain. You can check the certificate chain at the SSL client certificate list with the *STRUST* transaction. Display the SAP Business Technology Platform Mobile Services certificate chain in any web browser by opening the SAP Business Technology Platform Mobile Services cockpit and checking the security settings.
f. Save the connection and perform a connection test. If the configuration is completed properly, a 200 HTTP response is returned.
g. In the *Technical Settings* tab, add the rest of the path for the PUSH API in *Path Prefix* to allow the POST operation to work properly.

4. In the ConfigPanel, return to the *Outbound Trigger Configuration* panel, *General Data* tab, if you are not already there. Check the outbound trigger configuration to ensure that the previously established *HTTP RFC Destination* is set as the RFC destination to the proper mobile application. This configuration ensures that push notifications reach the right mobile application user.



5. On the *Parameters* tab, set parameter *SCPMS_WITH_SAP_USER_ID* to *True* if the SAP Business Technology Platform user store is the same as the back end user store, that is, if you use the same mobile user for both SAP Business Technology Platform logon and back end logon. If the user store is not identical, set the parameter to *False* and update the mobile user setting as explained in the next step.
6. If parameter *SCPMS_WITH_SAP_USER_ID* is set to *False*, maintain the user mapping under *User Management* using the Admin portal in the SAP GUI:

> ### Note
>
> On the first delta sync, the mobile client automatically performs substeps *a* - *d* for you. If desired, you can still perform these substeps to verify that the push registration process has completed successfully.

   a. Using the SAP GUI, launch the Admin portal with transaction code */n/SYCLO/ADMIN*. On the Admin portal home page, select *Administration* > *User Management*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page. Choose *Search* to list all users for that application.
   b. Select *User ID* under *Search Result*, and click the *Client Registration Info* tab under the *Mobile User Detail* section. Choose *Change* from the menu bar.
   c. Enter the matching *CPms User Id* (using upper case) for the back end user name listed under this tab.
   d. *Save* your changes.
7. Return to the *Home* page of the ConfigPanel. Select the *Push Scenario Definition* page. Under *Push Scenarios by Mobile App* list, select the desired push scenario definition. Click the *Outbound Trigger* tab and ensure that the proper outbound trigger is assigned and active for the push scenario.

8. *Save* your changes.

4.31.3.2 Activating Default Push Services on the Neo Platform

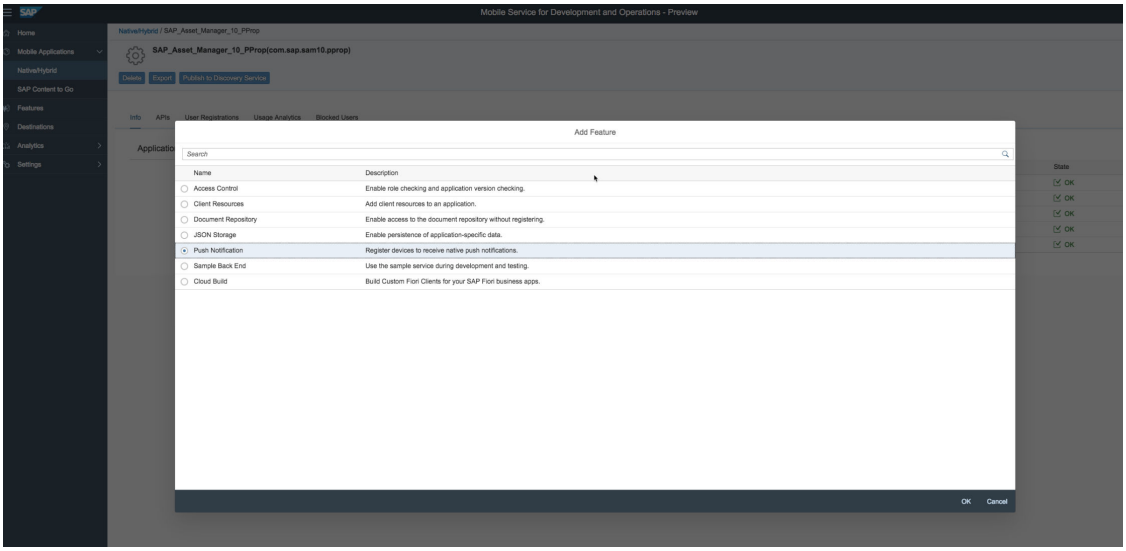
Prerequisites

> → Remember
>
> SAP Business Technology Platform, Neo environment will sunset as described in SAP Note 3351844. For more information about how to migrate the SAP Service and Asset Manager application, see Migrating From Neo to Cloud Foundry Environment.

- If you're not using MAIF , ensure you've installed either SAP Mobile Add-On ECC or SAP Mobile Add-On for SAP S/4HANA. See the following installation guides on the following portal pages for version information:
  - SAP S/4HANA Mobile Add-On
  - SAP Mobile Add-On ECC

Procedure

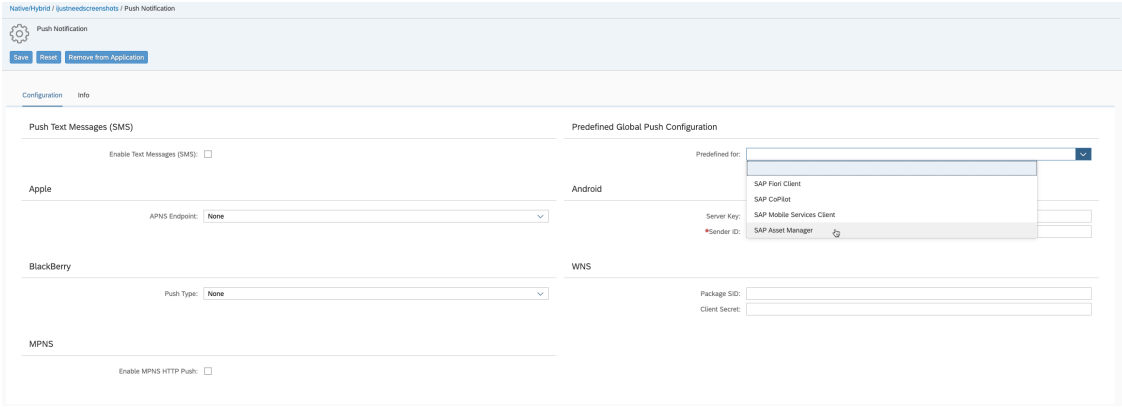
1. **Configure the SAP Business Technology Platform Mobile Services push API:**
   a. Enable the *Push Notification* feature in SAP BTP services:



   b. Navigate to the *Push Notification* in the mobile app and create a new HTTP connection to your external server named *Assigned Features*:



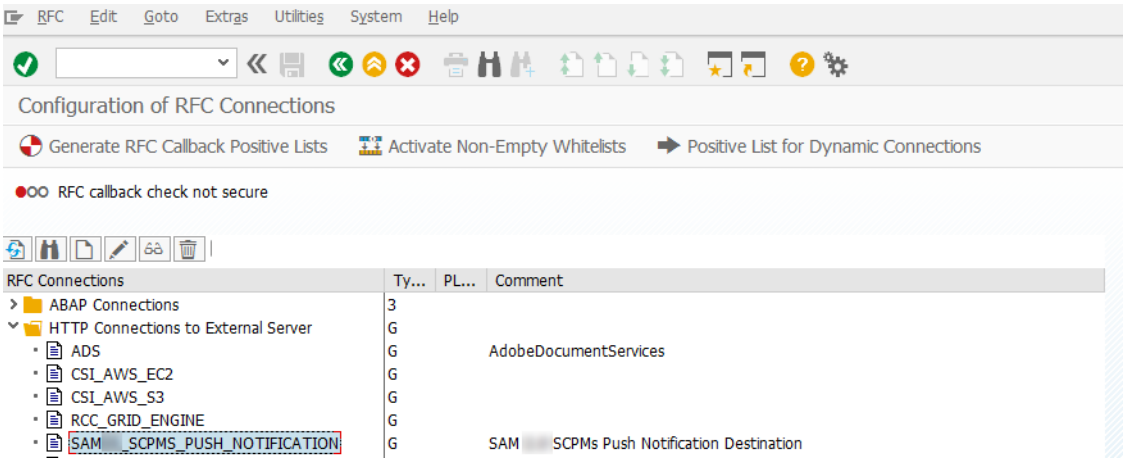
c. If you are using a custom deployment of your mobile application, upload the corresponding APNs certificates here. If you are using the default application provided by the Apple App or the Google Play store, select *Predefined for <Mobile Application Name>* in the *Predefined Global Push Configuration* section.



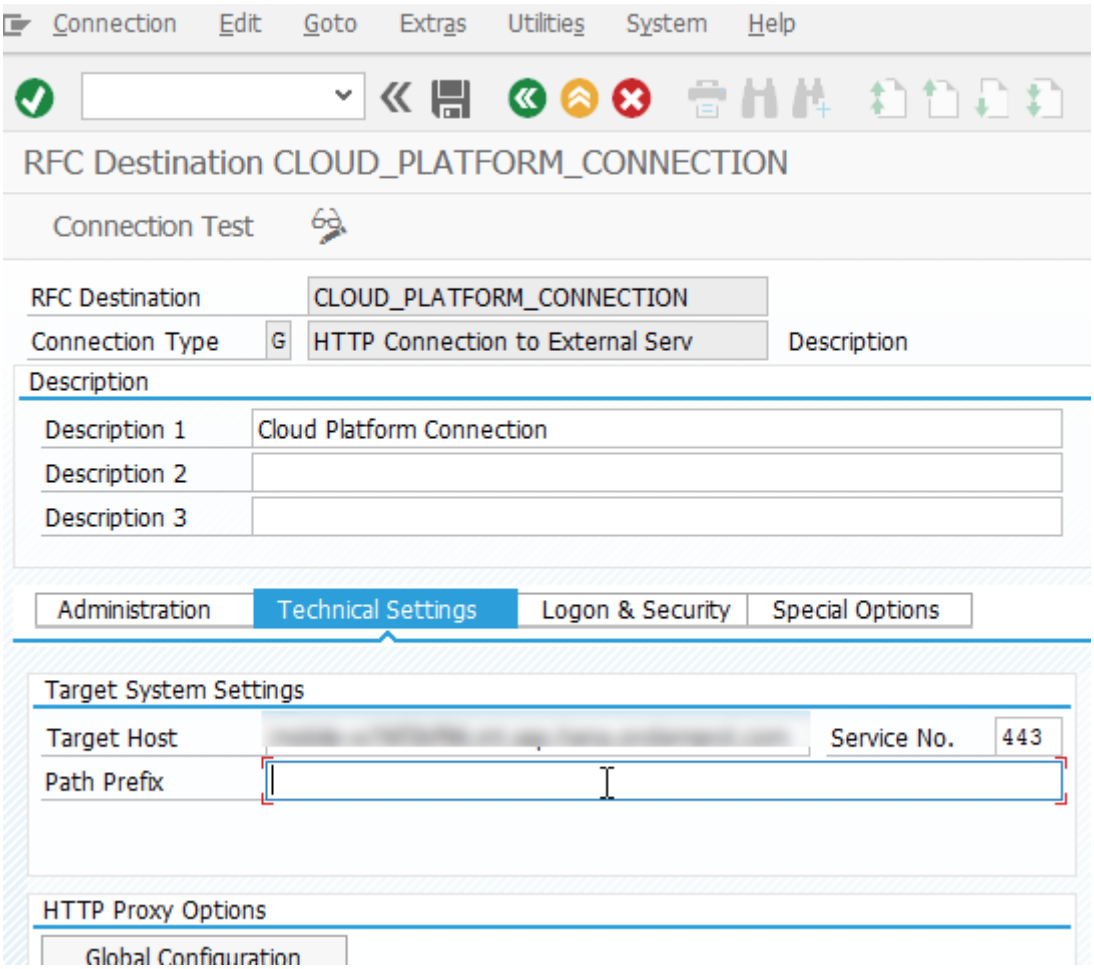
The SAP Business Technology Platform Mobile Services is configured for push.

2. **Configure the back-end system to utilize the SAP BTP services push APIs:**

a. Using the SAP GUI, run transaction *SM59*. Create a new HTTP connection with the name *<APPXX>_SCPMS_PUSH_NOTIFICATION*.



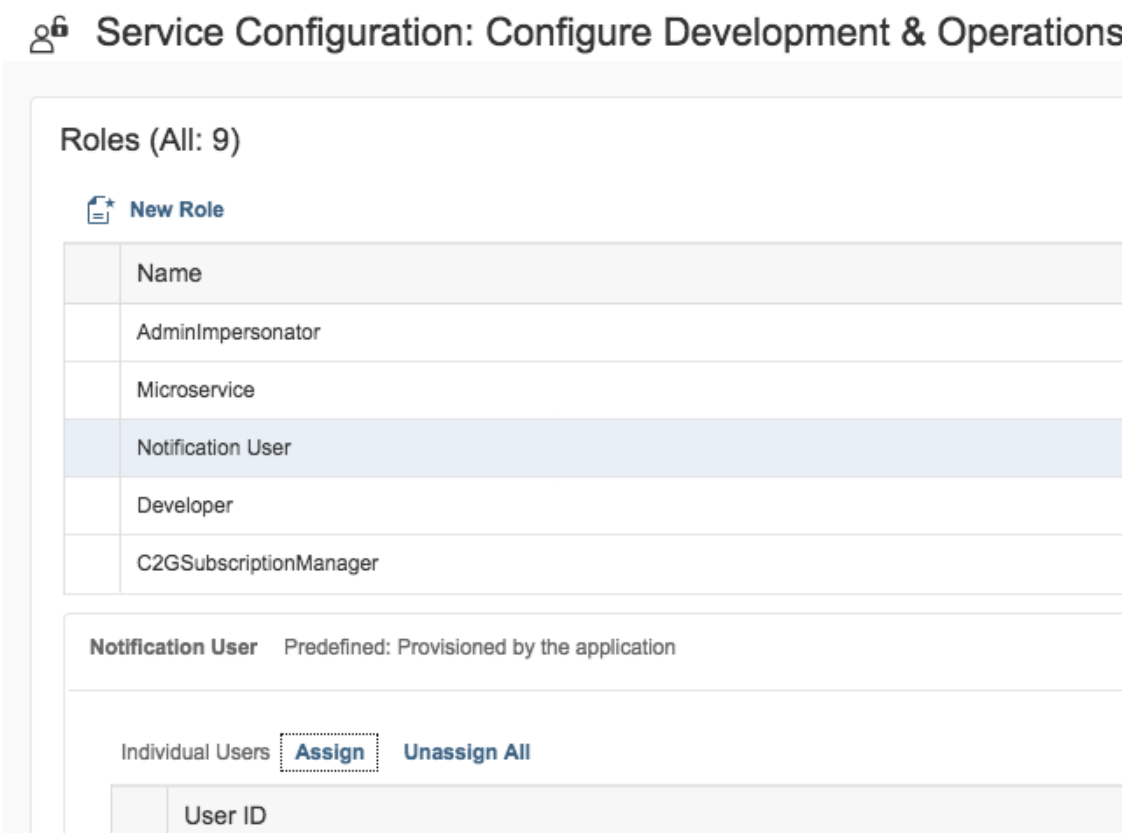
b. In the *Technical Settings* tab of the new connection, set the *Target Host* to match the push API of the SAP BTP services, using *443* (the port number for HTTPS connections).



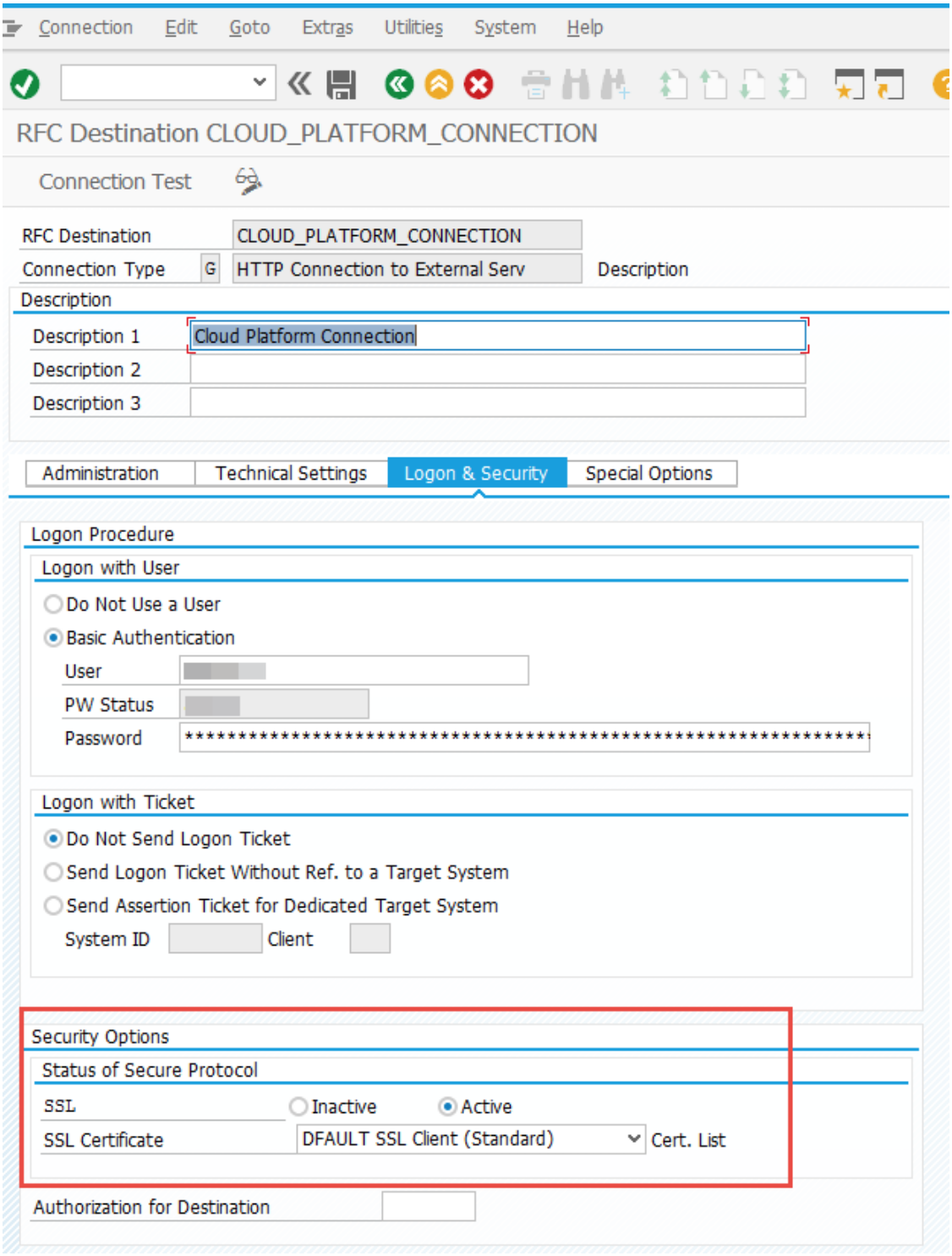
> **Note**
>
> If necessary, configure the proxy you are using to allow your back end to connect to the outside internet.

c. Click the *Logon & Security* tab. Under the *Logon Procedure*, select *Basic Authentication*. Enter the user name and password of a service user.

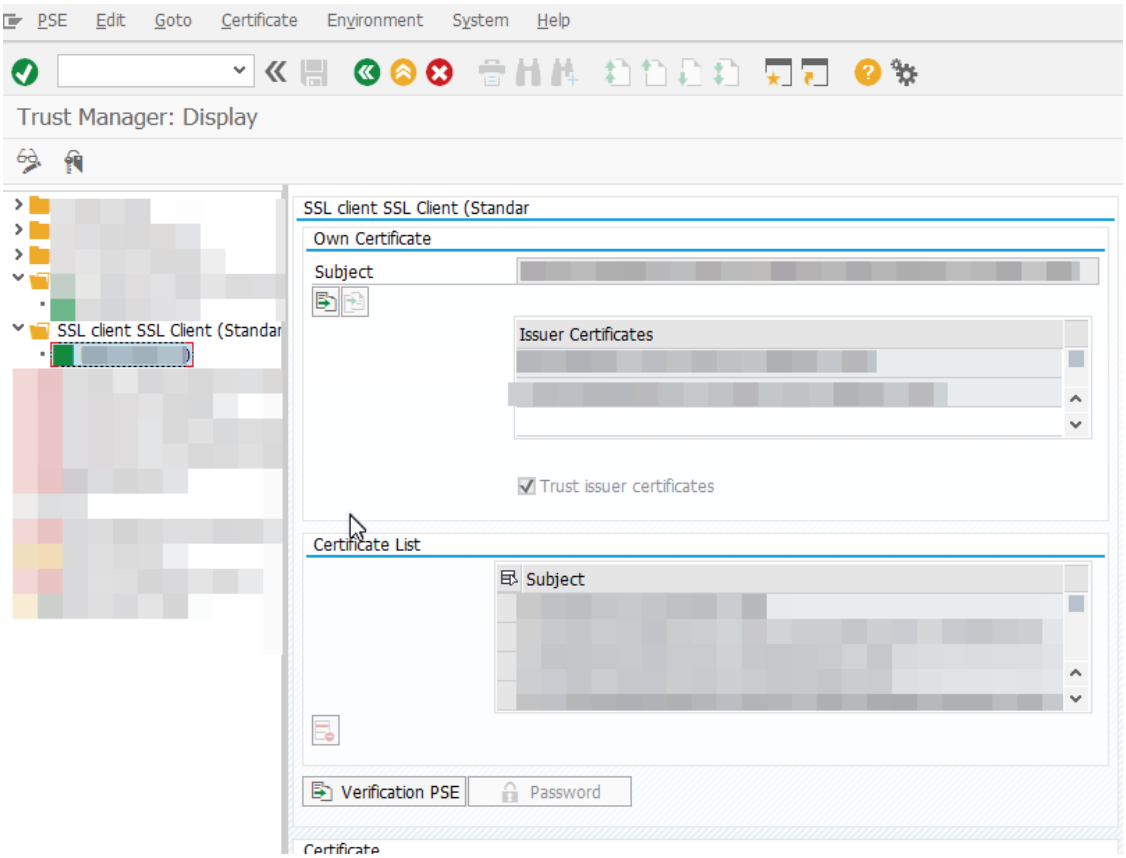
d. In SAP Business Technology Platform, ensure your service user has the role of *Notification User* assigned to them to ensure that the user is allowed to utilize the SAP BTP services API. The service user must be a member of the SAP Business Technology Platform account.



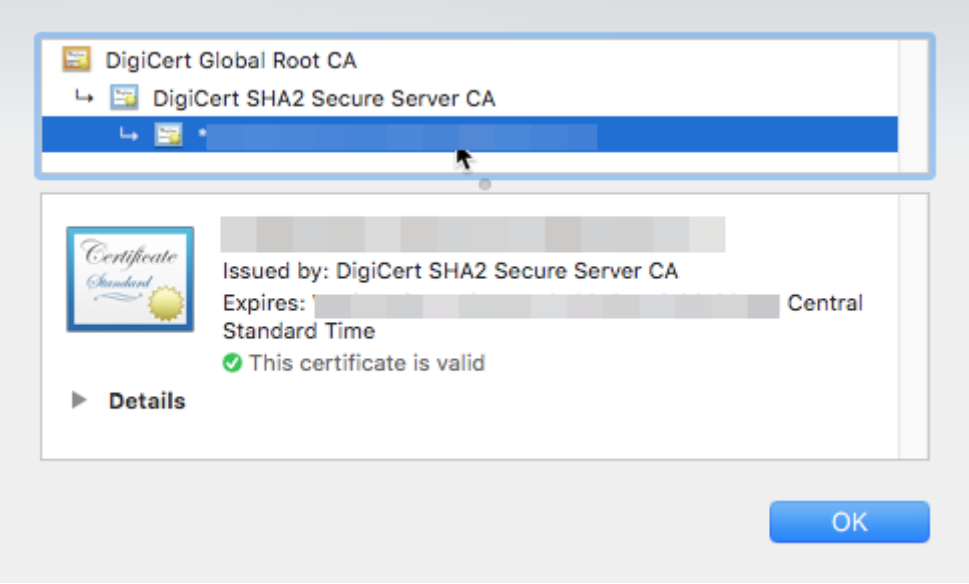
e. In the *Security Options* section of the *Logon & Security* tab, ensure that the `<SSL Secure Protocol>` is set to *Active*.
f. Remaining in the *Security Options* section, ensure that the *SSL Certificate List* used contains the SAP Business Technology Platform certificate chain and is active.



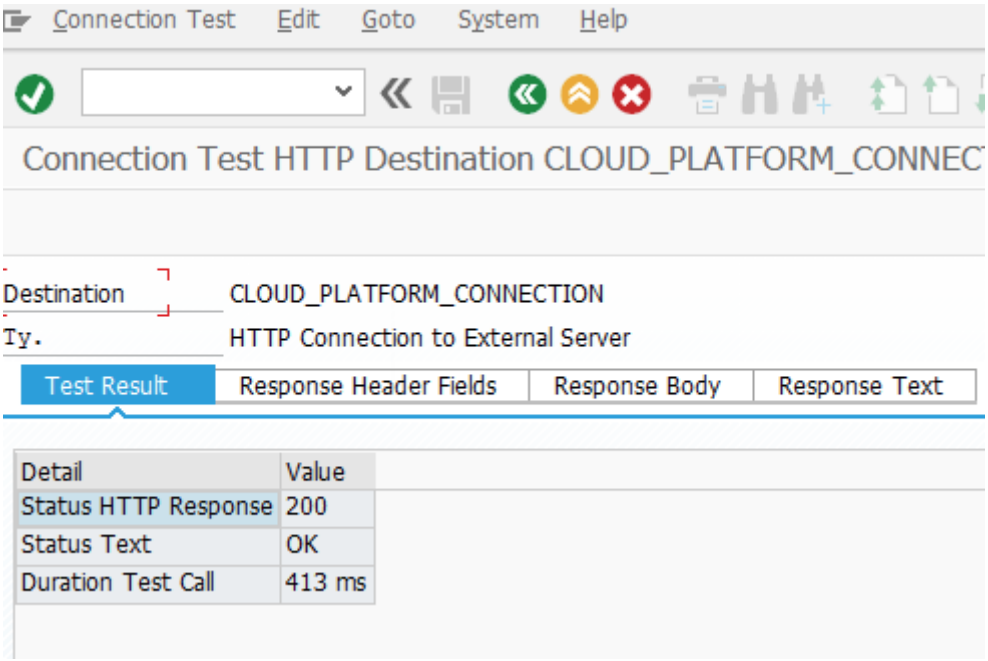
Check the certificate list of the SSL client by using the *STRUST* transaction. Check the matching trust list and ensure that the SAP BTP services certificate chains are in it.



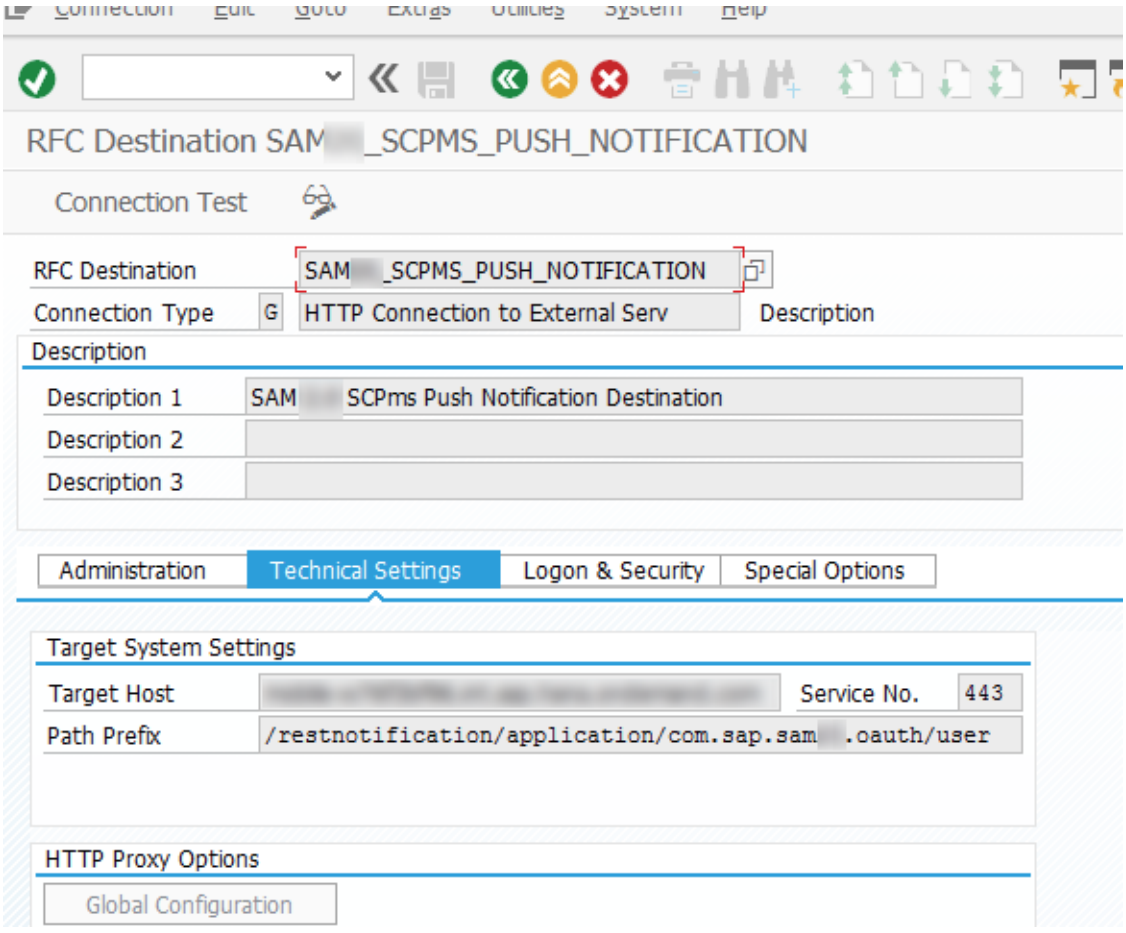
View the SAP BTP services certificate chain in any web browser by opening up the SAP BTP services cockpit and checking the security settings.



g. Save the connection and perform a connection test. If the configuration is completed properly, a 200 HTTP response is returned.

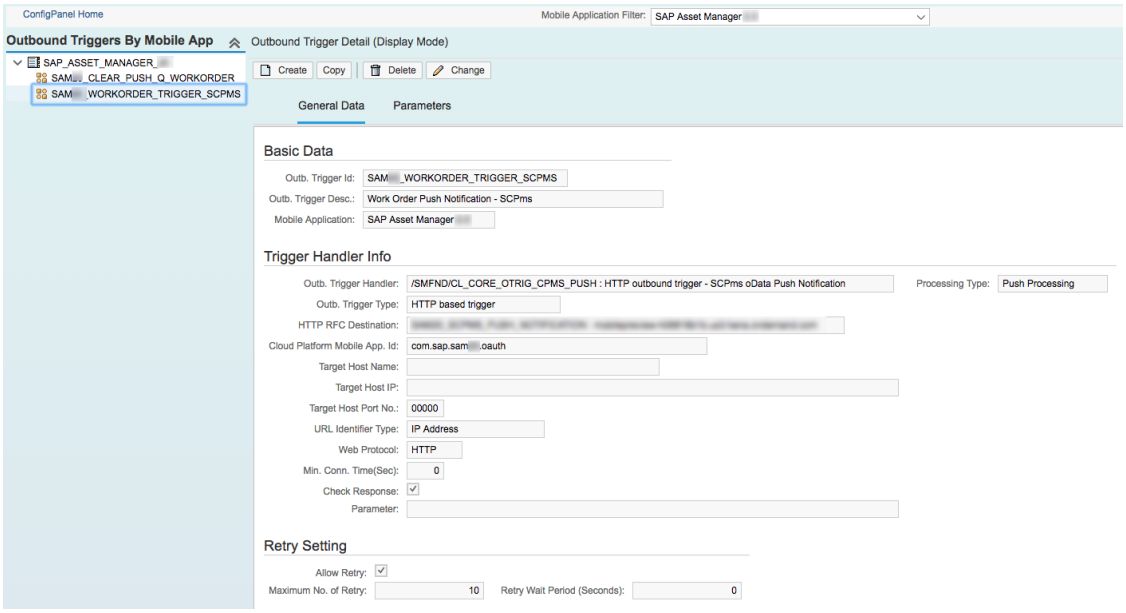


h. If the previous step correctly returned a status of *200*, add the rest of the path for the API to allow the POST to work properly.

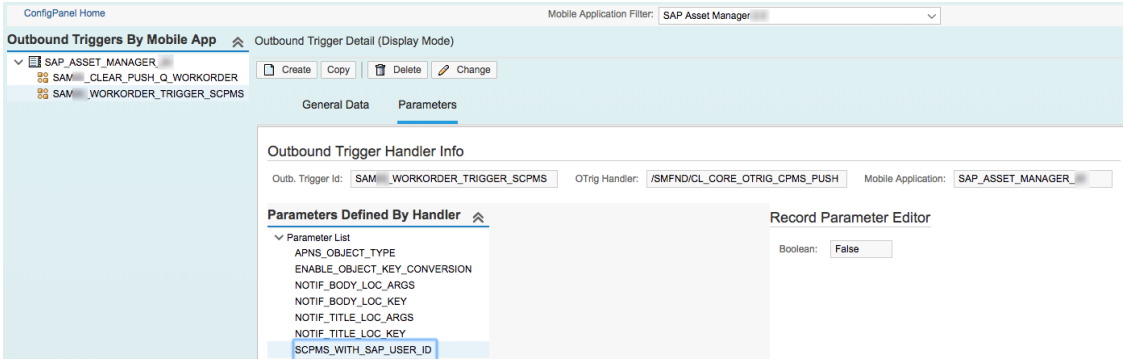


The back-end system can now send push notifications.

3. **Configure the back end to enable push from the SAP Service and Asset Manager application:**
   a. Using the ConfigPanel, navigate to the *Outbound Trigger Configuration* panel, *General Data* tab. Check the outbound triggers to ensure that the previously established *HTTP RFC Destination* is set as the RFC destination to the APPID that provides the push notifications to the mobile devices.



   b. Click the *Parameters* tab. If your user store on the back end and user store on the SAP Business Technology Platform are identical, set the *SCPMS_WITH_SAP_USER_ID* parameter value to *True*. If the user stores are not identical, set the parameter to *False*.



   c. Return to the ConfigPanel home screen and click the *Push Scenario Definition* link. Navigate to the *Outbound Trigger* tab. Find and highlight the push on the list of *Push Scenarios by Mobile App* and ensure that the outbound trigger is active.

Results

Push services are activated for your mobile application. Thoroughly test the push functionality before deploying to the client devices.

4.31.3.3 Activating Default Push Services on the Cloud Foundry Platform

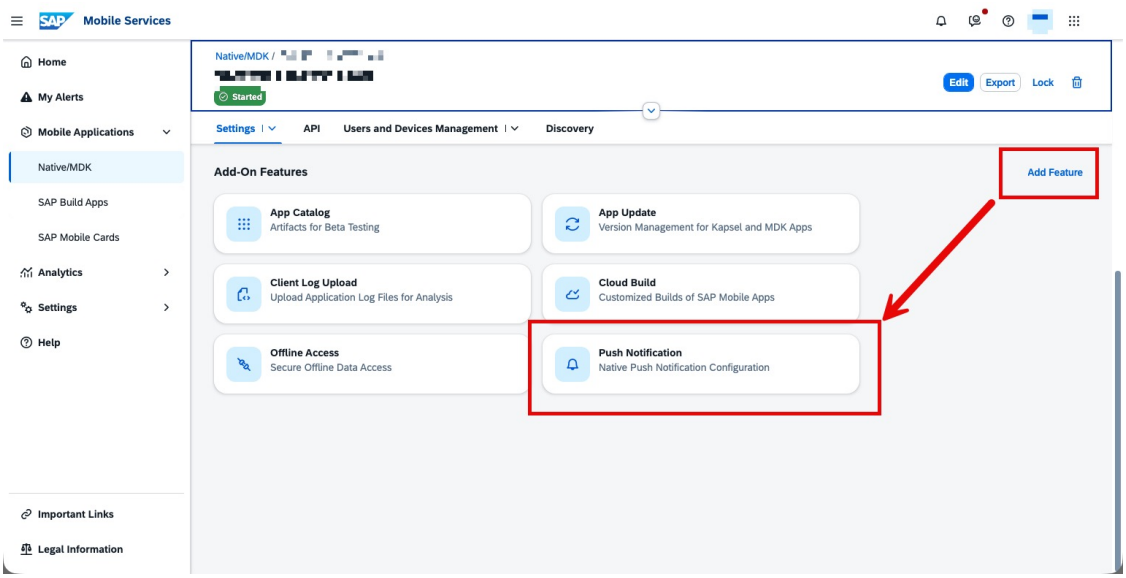
Configure BTP Mobile Services and the SAP back end system to enable push notification delivery in a Cloud Foundry environment. This procedure describes how to activate push services, configure connectivity, maintain middleware server settings, and enable outbound push processing for SAP Service and Asset Manager.

Prerequisites

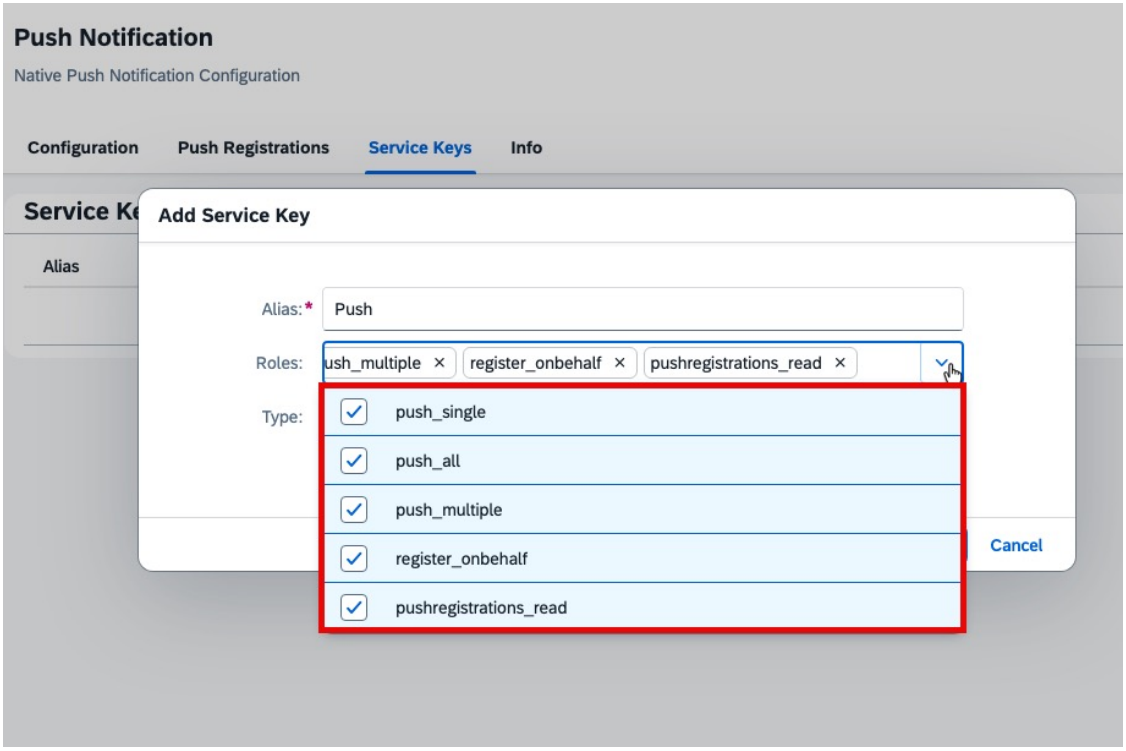
- If you're not using Mobile Application Integration Framework delivered as a part of SAP S/4HANA 1909 or newer, install either SAP Mobile Add-On ECC or SAP Mobile Add-On for SAP S/4HANA. See the following installation guides on the following portal pages for version information:
  - SAP S/4HANA Mobile Add-On
  - SAP Mobile Add-On ECC

Procedure

1. **Enable the Push Notification feature in SAP Business Technology Platform Mobile Services:**
   a. Ensure that the *Push Notification* feature is enabled for SAP BTP services.



   b. Open the mobile application's *Add-On Features* section and verify that the *Push Notification* feature is assigned.
   c. If the feature is not assigned, enable it. For more information, see Configuring Assigned Features.
   d. Navigate to the *Service Keys* section and create a service key with all of the push notification roles.

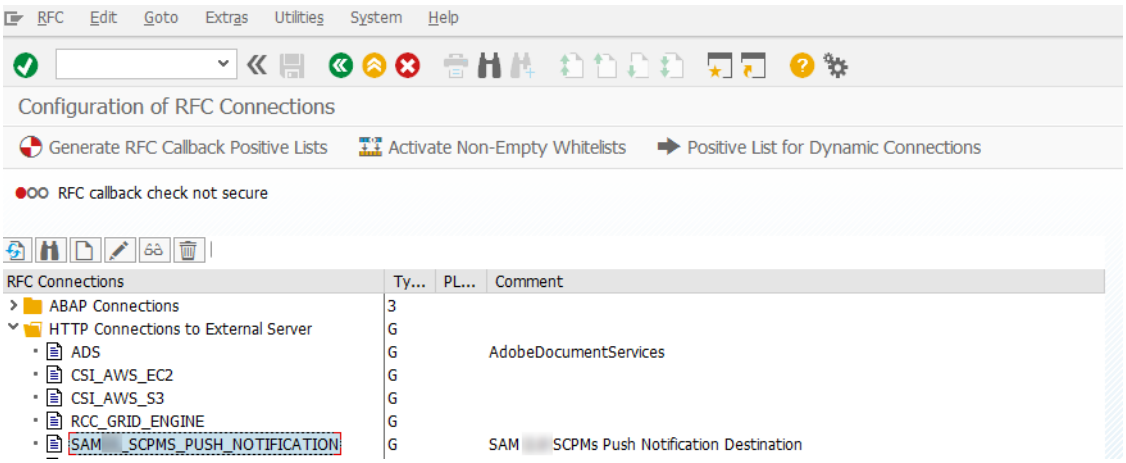


e. Record the generated **Alias** and **API Key** for later use in the back end configuration.

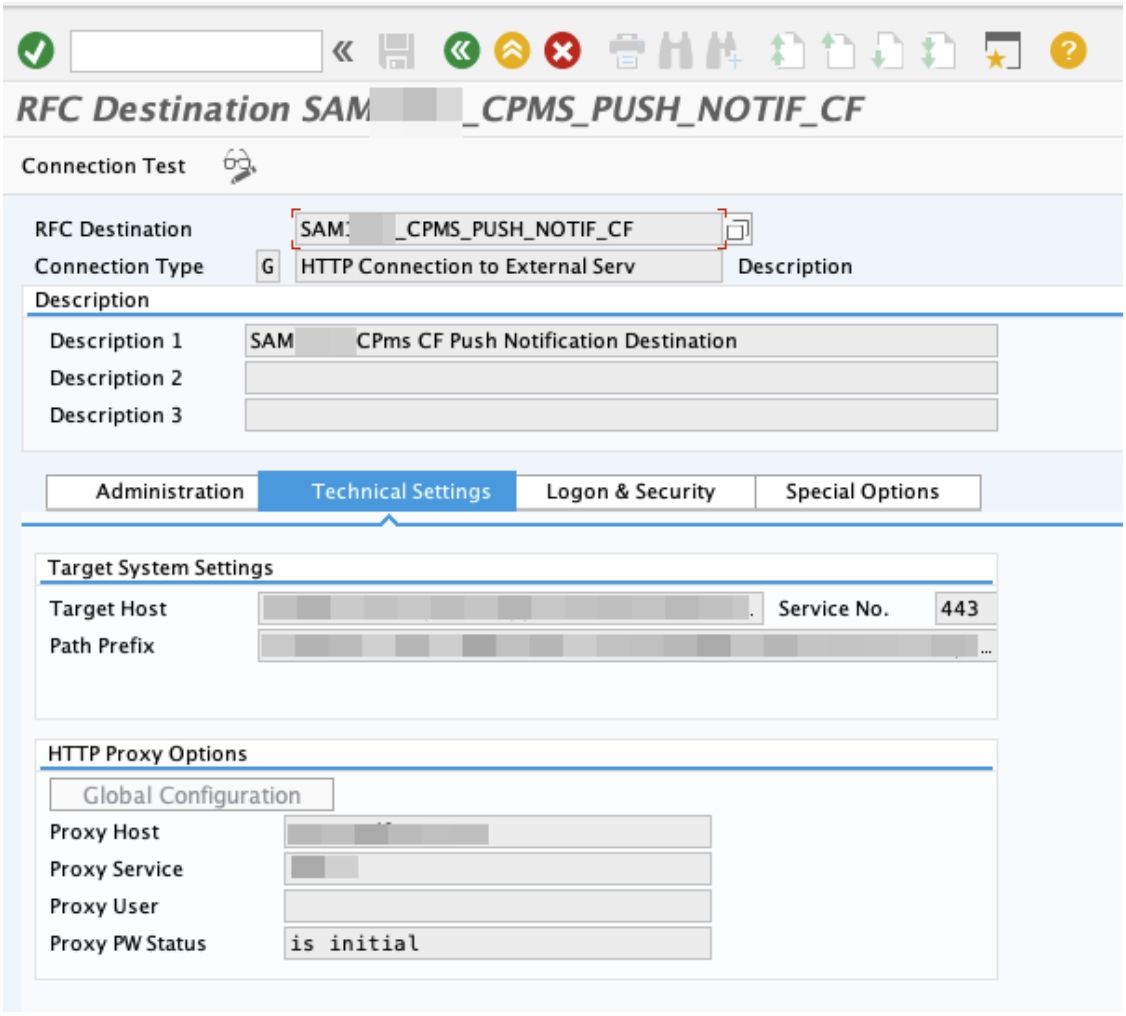
SAP Business Technology Platform Mobile Services is configured for push notification processing.

2. **Configure the back end system to utilize the BTP Mobile Services push APIs:**

   a. Using the SAP GUI, run transaction *SM59*. Create a new HTTP connection with the name *<APPXX>_SCPMS_PUSH_NOTIFICATION*.

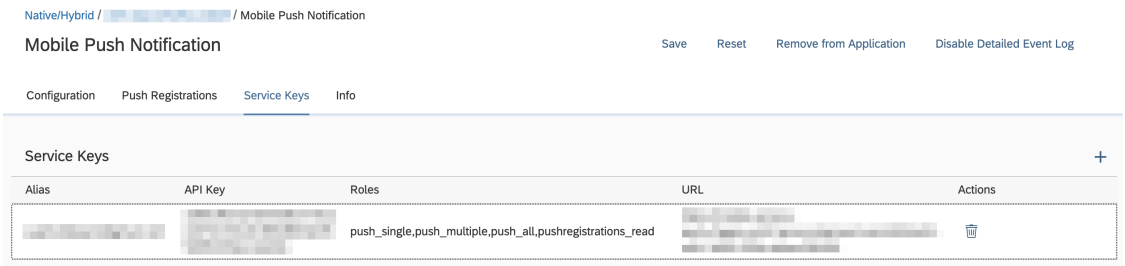


   b. In the *Technical Settings* and tab of the new connection, set the *Target Host* to match the push API of the SAP BTP services, using *443* (the port number for HTTPS connections). Ensure the *Path Prefix* equals `/<Push URL GUID>/mobileservices/push/v1/backend/applications/<App ID>/notifications/users`



> **Note**
>
> If necessary, configure the proxy you are using to allow your back end to connect to the outside internet.

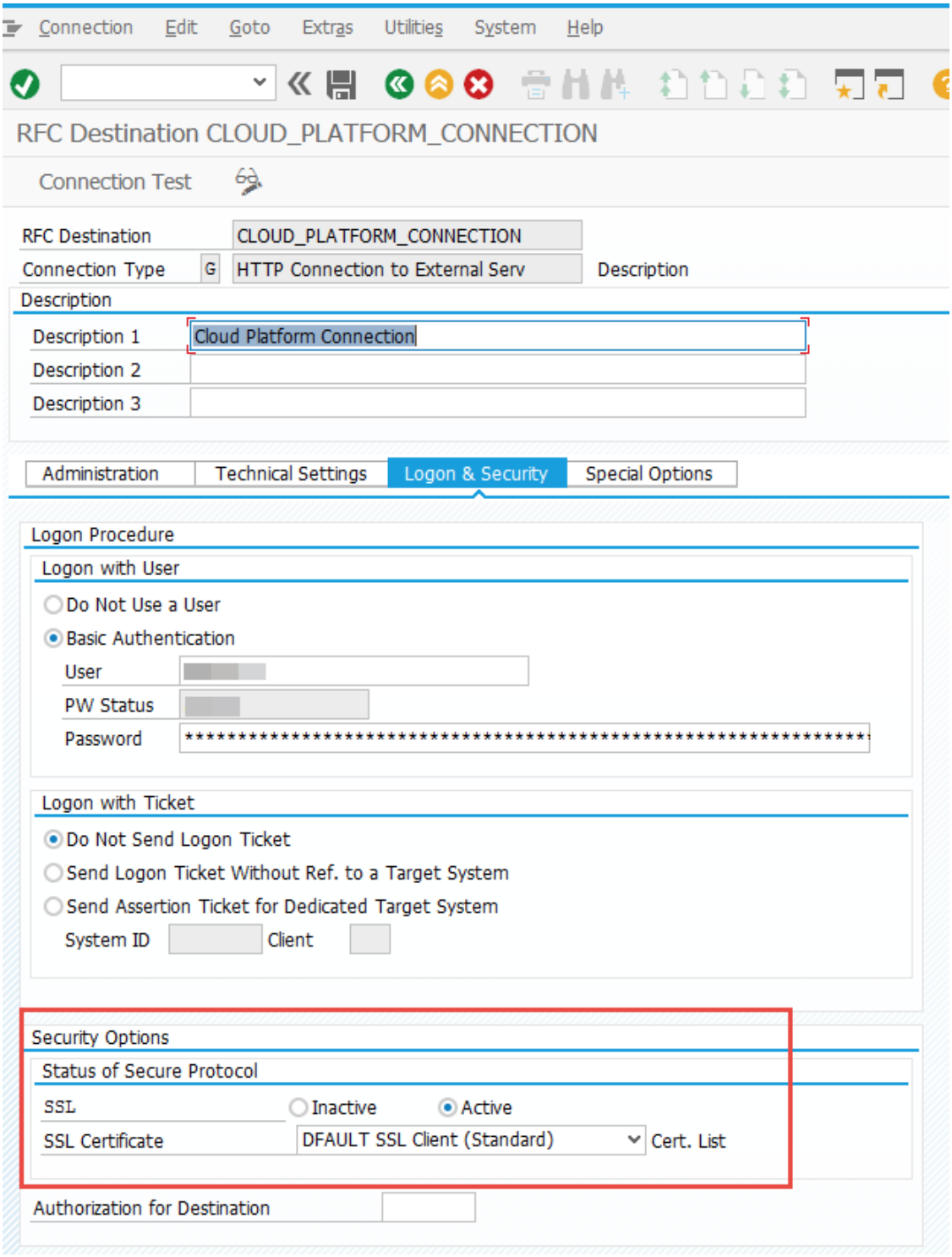
c. Ensure that you have saved the *API Key* for the *Service Key Alias* created in step 1e. This *API Key* is required for the *RFC Destination* configuration.



d. Click the *Logon & Security* tab. Under the *Logon Procedure*, select *Basic Authentication*. Enter the *Mobile Push Notification Alias* as the user name and the *Mobile Push Notification API Key* as the password.

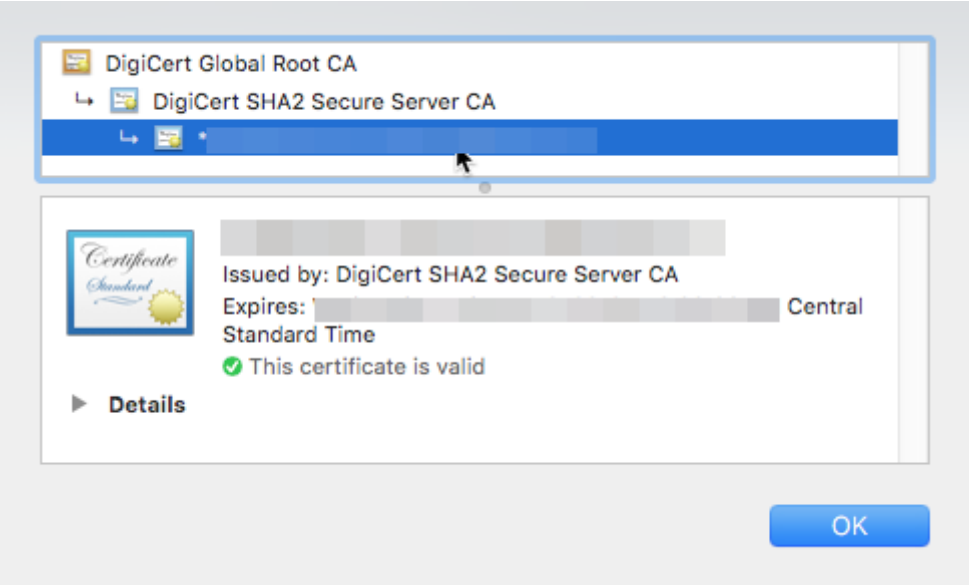
e. In the *Security Options* section of the *Logon & Security* tab, ensure that the `<SSL Secure Protocol>` is set to *Active*.

f. Remaining in the *Security Options* section, ensure that the *SSL Certificate List* used contains the SAP Business Technology Platform certificate chain and is active.

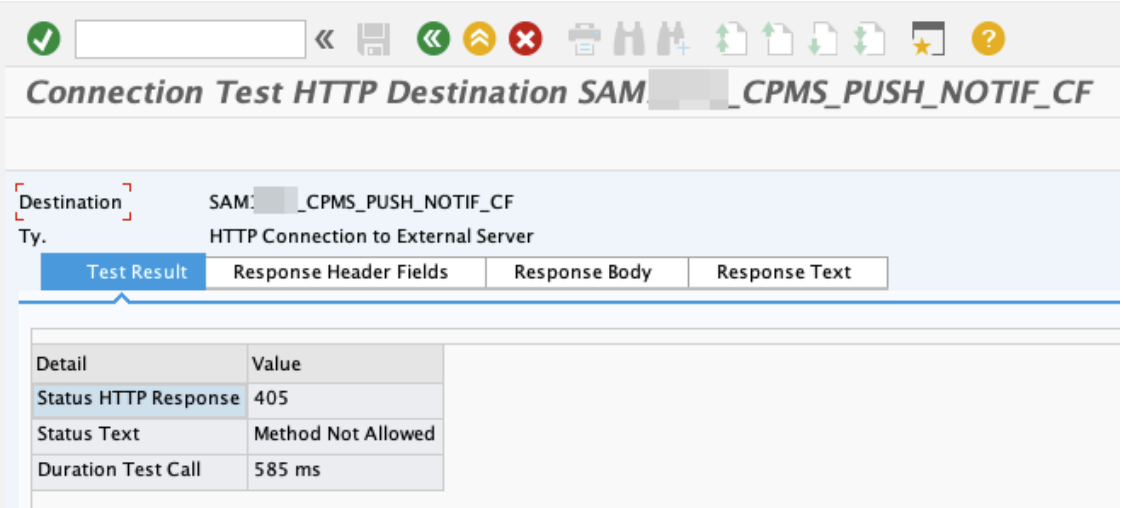


Check the certificate list of the SSL client by using the *STRUST* transaction. Check the matching trust list and ensure that the SAP BTP services certificate chains are in it.

View the SAP BTP services certificate chain is trusted by the SAP back end system. Use transaction **STRUST** to ensure that the SSL client trust list contains the required SAP BTP certificates. The certificate chain should match the certificates documented in the 3566727 SAP note. You can also review the certificate chain through the SAP BTP services cockpit using your browser's security certificate viewer.

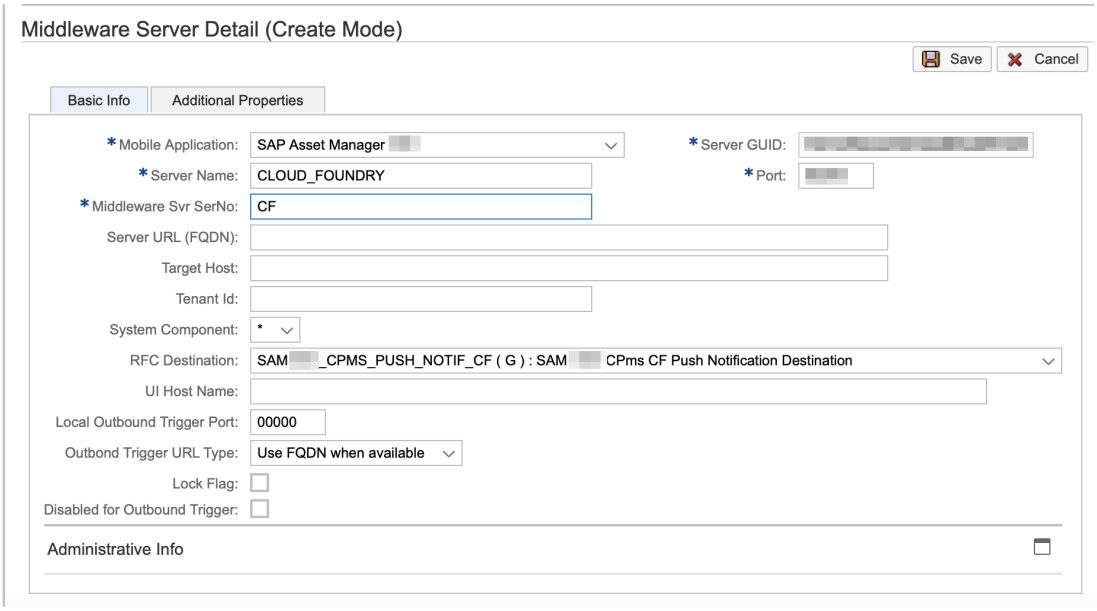


g. Save the connection and perform a connection test. If the configuration is completed properly, a 405 code is returned.



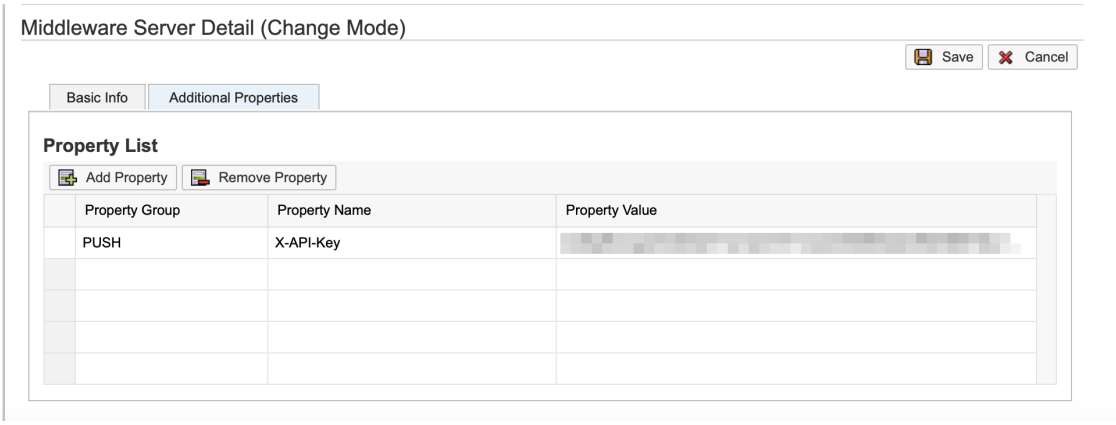
h. In the SAP GUI, open the Administration Panel using transaction */n/syclo/admin*.

i. Navigate to *Administration* > *Server Management*. Create a new middleware server, specifying the RFC destination you just created.



j. On the additional properties tab, create a new property with the following attributes:

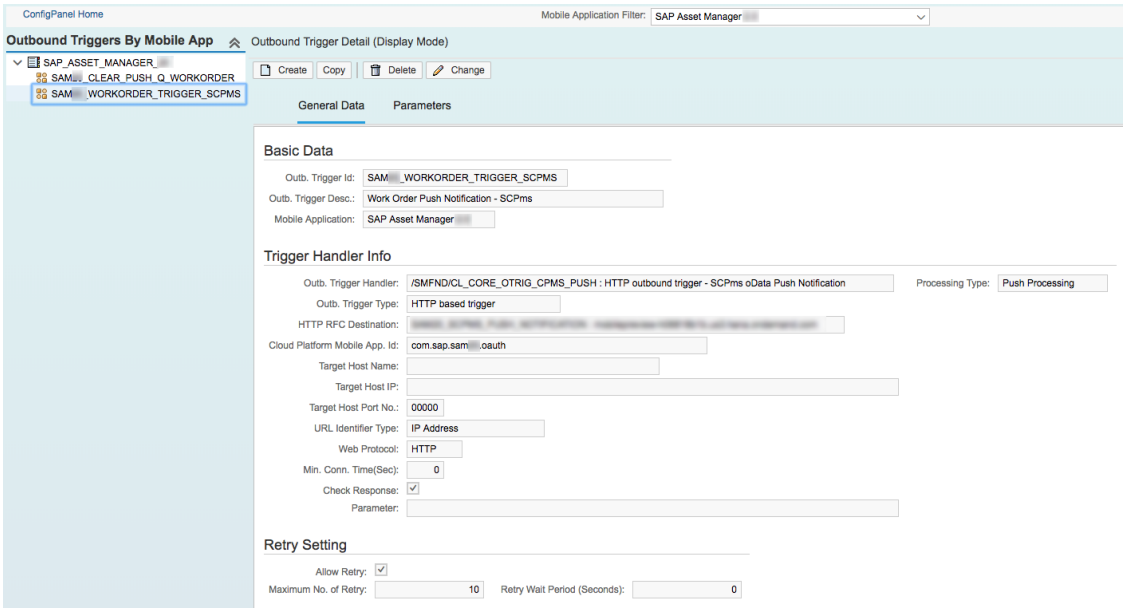
- Property Group: PUSH
- Property Name: X-API-Key
- Property Value: Mobile push API key from SAP BTP services



The back end system can now send push notifications.

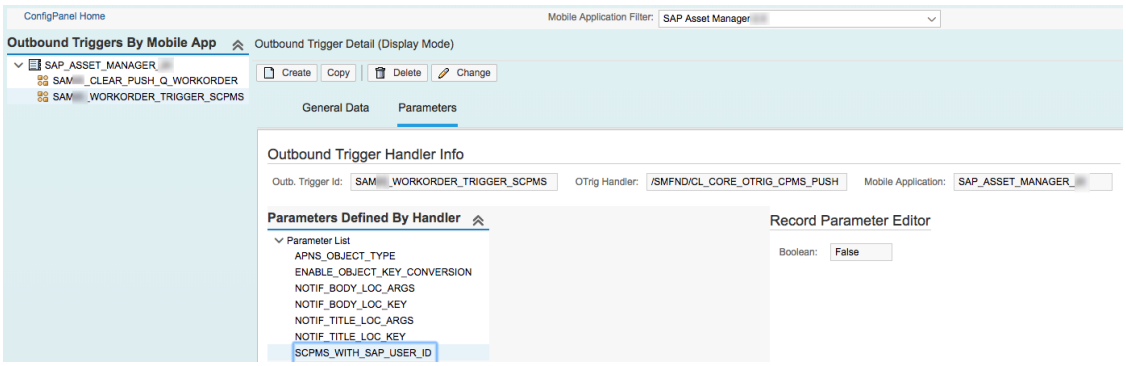
3. **Configure the back end to enable push from your mobile application:**

a. Using the ConfigPanel, navigate to the *Outbound Trigger Configuration* panel, *General Data* tab. Check the outbound triggers to ensure that the previously established *HTTP RFC Destination* is set as the RFC destination to the APPID that provides the push notifications to the mobile devices.



b. Click the *Parameters* tab. If your user store on the back end and user store on the SAP Business Technology Platform are identical, set the *SCPMS_WITH_SAP_USER_ID* parameter value to *True*. If the user stores are not identical, set the parameter to *False*.

> **Note**
>
> For the default Cloud Foundry environment deployments, BTP Mobile Services uses the user email address as the unique identifier for push notification processing.



c. Return to the ConfigPanel home screen and click the *Push Scenario Definition* link. Navigate to the *Outbound Trigger* tab. Find and highlight the push on the list of *Push Scenarios by Mobile App* and ensure that the outbound trigger is active.

Results

Push services are activated for your mobile application. Thoroughly test the push functionality before deploying to the client devices.

4.31.3.4 Configuring Push for the Android Platform

Configure Firebase Cloud Messaging (FCM) to enable push notifications for SAP Service and Asset Manager Android clients. This procedure describes how to create an FCM project, register an Android application, configure the client, and enable Android push notifications in SAP BTP Mobile Services.

Context

Firebase Cloud Messaging (FCM) is a cross-platform cloud solution for messages and notifications for Android, iOS, and web applications.

> **Note**
>
> If you use the SAP Service and Asset Manager Android client downloaded from the Google Play Store, no additional Firebase Cloud Messaging (FCM) configuration is required.
>
> If you use a branded or custom SAP Service and Asset Manager Android client that isn't downloaded from the Google Play Store, you must configure your own Firebase Cloud Messaging (FCM) project and integrate it into the client you build.
>
> For more information, see Enable Push Notifications in Your Branded MDK Client.

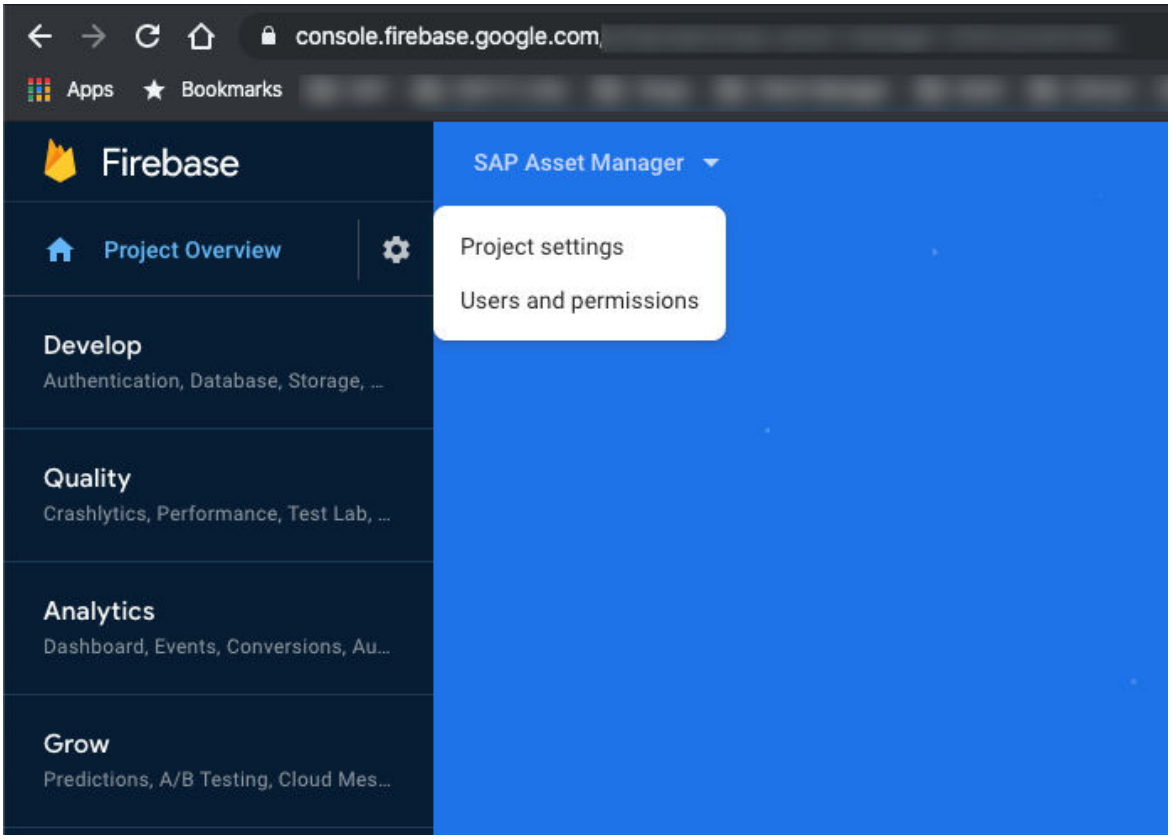
To enable push notification for your mobile application using the Android platform, use the following procedure:

Procedure

1. Create a free Firebase account. See the main Firebase page to set up a new account, or connect an existing account.

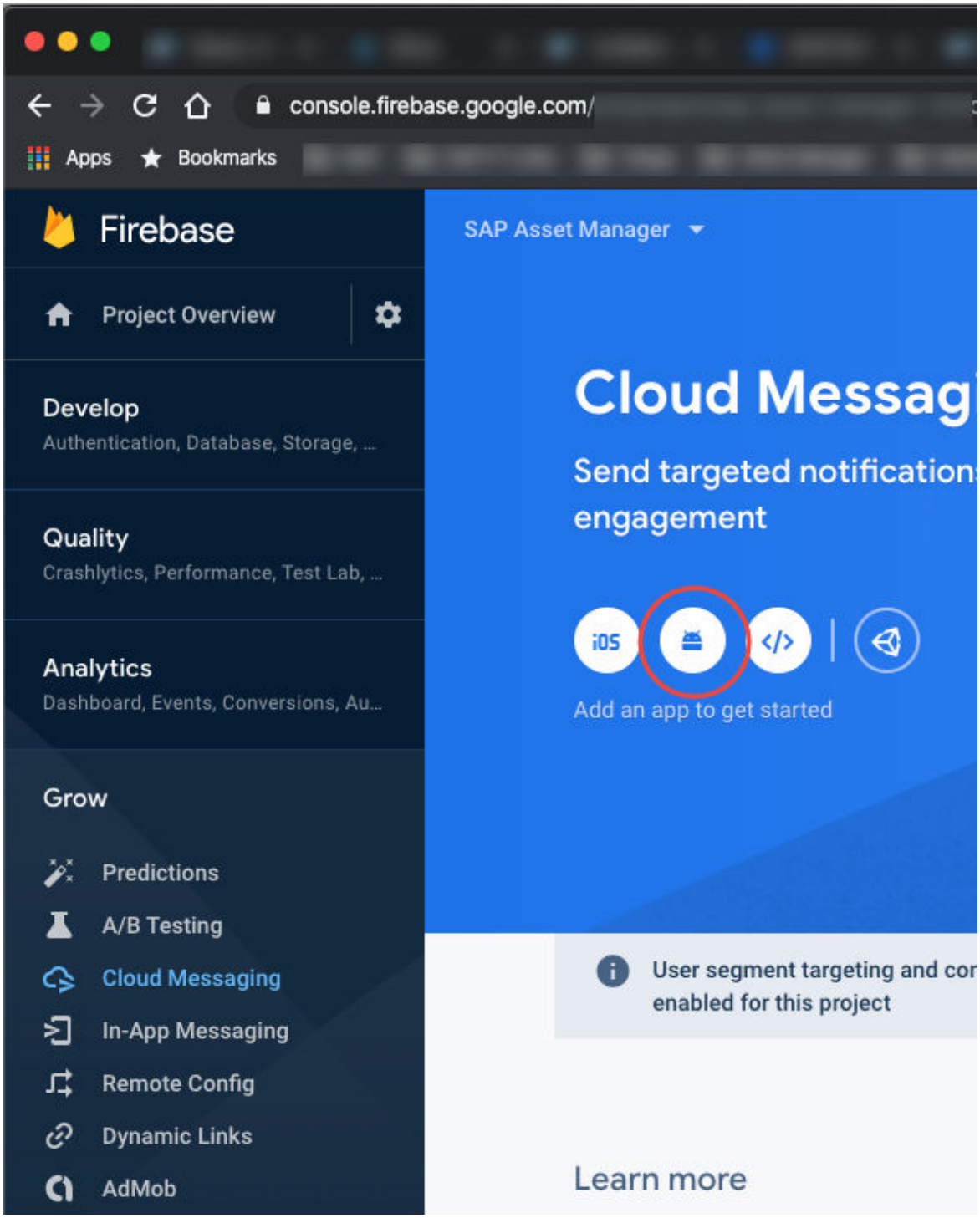
   > **Note**
   >
   > Documentation on Firebase is found on the Firebase Documentation page.

2. Add a new project, or use an already-existing project.
3. Click the gear icon and select the *Project Settings* menu option. Click the *Cloud Messaging* tab.



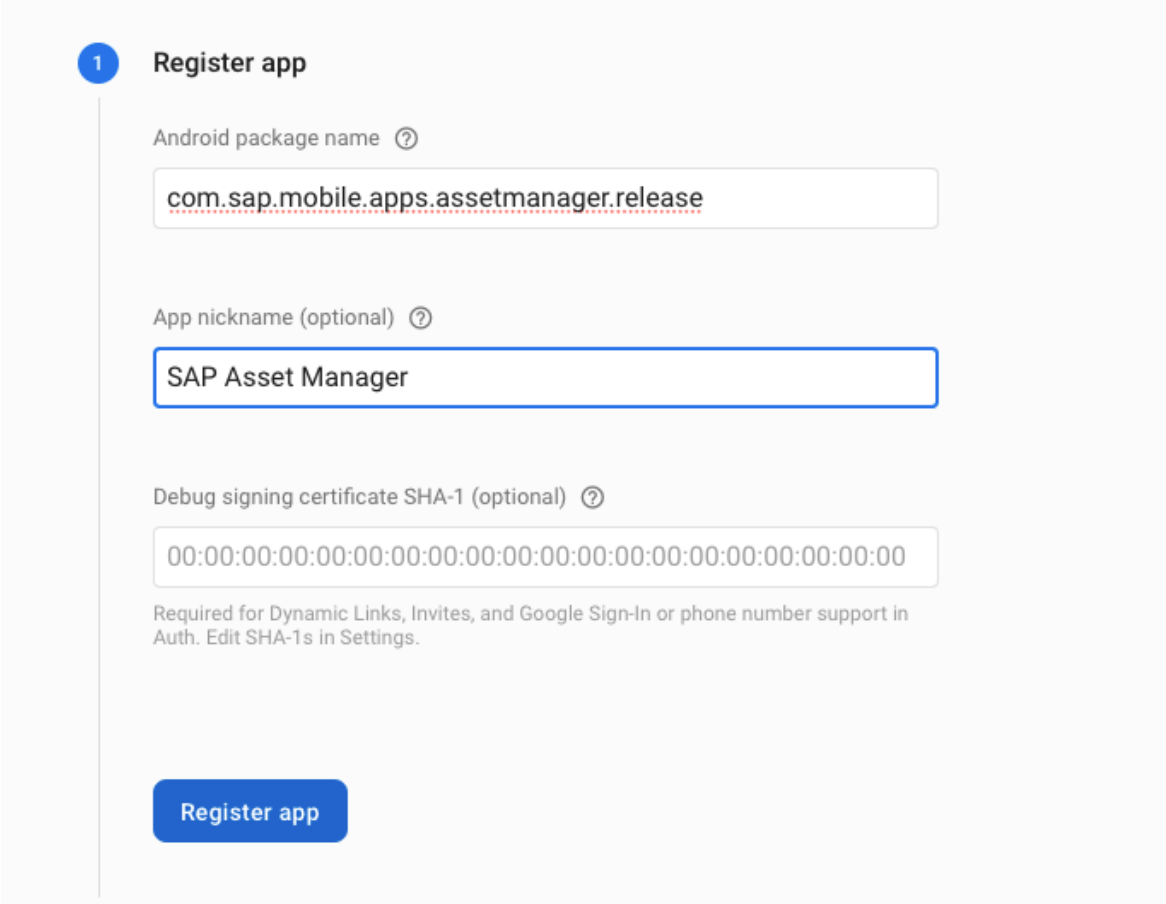
4. Copy and paste the information in the *Server Key* field to use in a later step.
5. Navigate to *Grow* > *Cloud Messaging* using the sidebar.
6. Click the Android icon to add a new Android app.

   The *Add Firebase to your Android app* window appears.



7. Add your package name to the *Android package name* field in *Step 1*. Ensure that the package name matches the *BundleID* found in the `<APPNAME>.mdkproject/MDKProject.json` file. When done, click *Register app*.

   Your app is registered and you're moved to *Step 2 - Download config file*.



8. Click the *Download google-services.json* button located in *Step 2 - Download config file*.

   The `google-services.json` file is downloaded to your computer.
9. Navigate to `<APPNAME>.mdkproject/App_Resources/Android`. Paste the `google-services.json` file you downloaded in the previous step to this location.
10. Build the mobile client. Use the instructions found in Building and Branding the SAP Service and Asset Manager Application Client as a guide.
11. Copy and paste the server key you saved in *Step 4* inside your SAP BTP services push notification configuration in the *Android* section.

    For instructions on how to enable Android push notifications in SAP BTP services, see the Android Push Notifications procedure.

    For detailed information on configuring push for your application and platform, see the following procedure, specifically the screenshot in *Step 1d*.

    - Activating Default Push Services on the Neo Platform [page 496]
    - Activating Default Push Services on the Cloud Foundry Platform [page 504]

Next Steps

Continue to the procedure Setting Up the Outbound Trigger for Your Push Configuration [page 493].

4.32 Online Search Configuration

Users can search online for *Functional Locations* and *Equipments*, allowing them to view, filter and optionally download more objects to their mobile device, in addition to the ones already downloaded. This way users have more visibility of ongoing tasks, not limited to the ones available only offline.

> **Note**
>
> - As of version 2410, SAP Service and Asset Manager supports online search for *Work Orders* and *Notifications*.
> - For more information about how to use the feature, see Maintenance Technician User Guide - Using Online Search.

Supported Personas

This feature is applicable for the following personas:

Maintenance Technician (Standard)
Maintenance Technician (Pro)
Field Service Technician (Standard)
Field Service Technician (Pro)

Limitations

The following limitations apply **only** to Online Search for **Work Orders and Notifications**:

- Users can only *download* and *assign* Work Orders and Notifications.
- For the Field Service Technician persona, this feature is supported on the Customer Service Back End system [page 177].

Configuration

Perform the following configuration step(s):

1. Configuring Online Search - Back End - Enabling the Feature [page 516]
2. To configure Online Search for *Work Orders* and *Notifications*, see Configuring Online Search - Work Orders and Notifications [page 517].

4.32.1 Configuring Online Search - Back End - Enabling the Feature

Context

The below procedure describes how to enable the feature for the selected persona(s).

> **Note**
>
> For detailed information about Online Search, see the overview topic, Online Search Configuration [page 515].

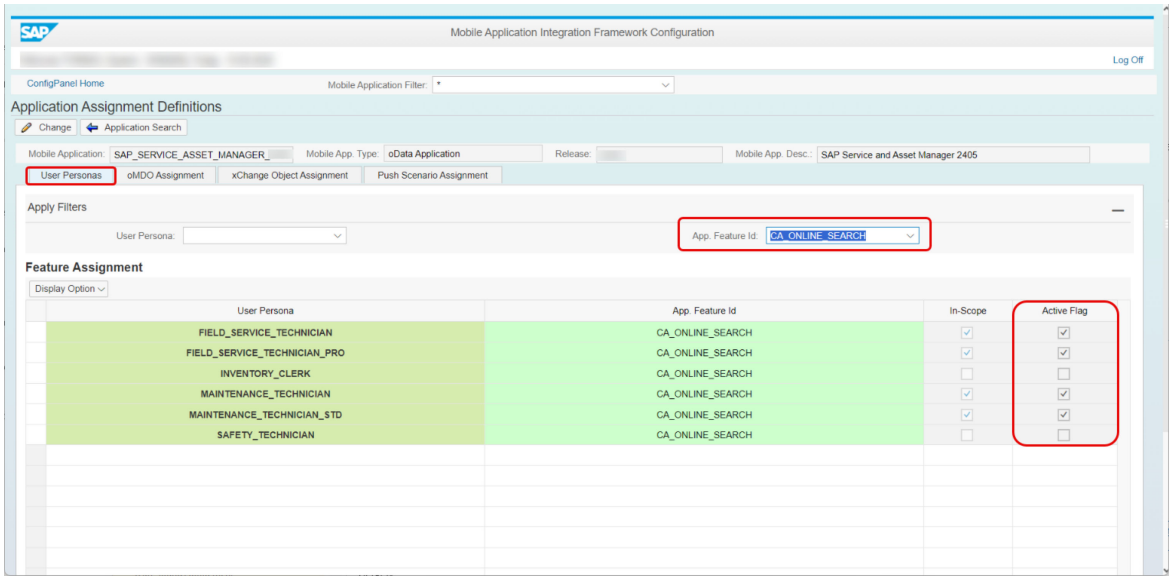
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **Enabling and disabling features**: refer to Configuring Features and Component Assignments in *MAIF Configuration Guide*.

Procedure

1. On the ConfigPanel, navigate to *Component Assignments*, and select the relevant mobile application from the list.
2. Under the *User Personas* tab, select *CA_ONLINE_SEARCH* as the *Application Feature ID*.
3. Enter *Change* mode and tick the *Active Flag* checkbox for the persona(s) you want to enable the feature.



4. *Save* your changes.

4.32.2 Configuring Online Search - Work Orders and Notifications

Context

As of version 2410, SAP Service and Asset Manager supports online search for *Work Orders* and *Notifications*.

> Note
>
> - Users can only *download* and *assign* Work Orders and Notifications.
> - For the Field Service Technician persona, this feature is supported on the Customer Service Back End system [page 177].
> - For detailed information about Online Search, see the overview topic, Online Search Configuration [page 515].

Supported Personas

Online Search for **Work Orders and Notifications** is applicable for the following personas:

Maintenance Technician (Pro)
Field Service Technician (Pro)

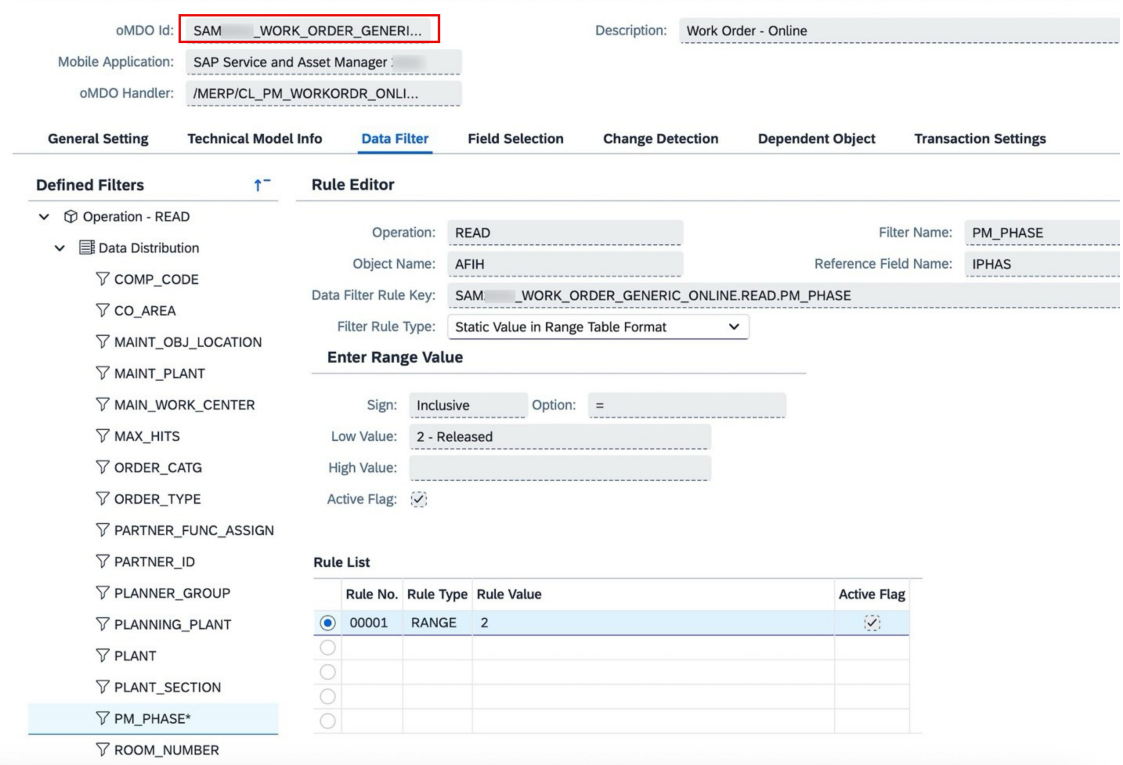
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

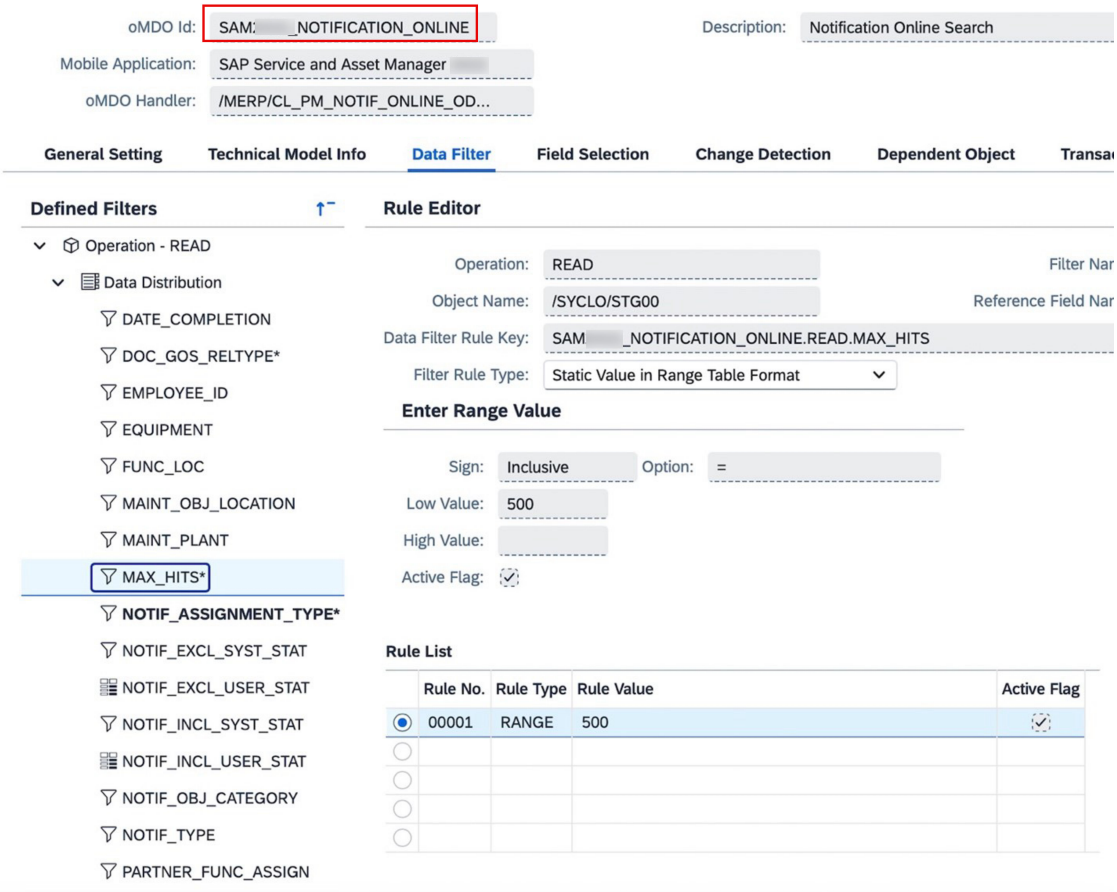
- **OMDO** and **OMDO filter** configuration: refer to OData Mobile Data Object Configuration and OData Mobile Data Object Configuration - Data Filter Tab in *MAIF Configuration Guide*.

Procedure

1. On the ConfigPanel, go to *oData Mobile Data Object Configuration*. Work Orders and Notifications are supported by the following oMDO configurations:
    - *Work Order*: *SAMXXXX_WORK_ORDER_GENERIC_ONLINE*
        - By default, only *Released* Work Orders are returned. See the following image:

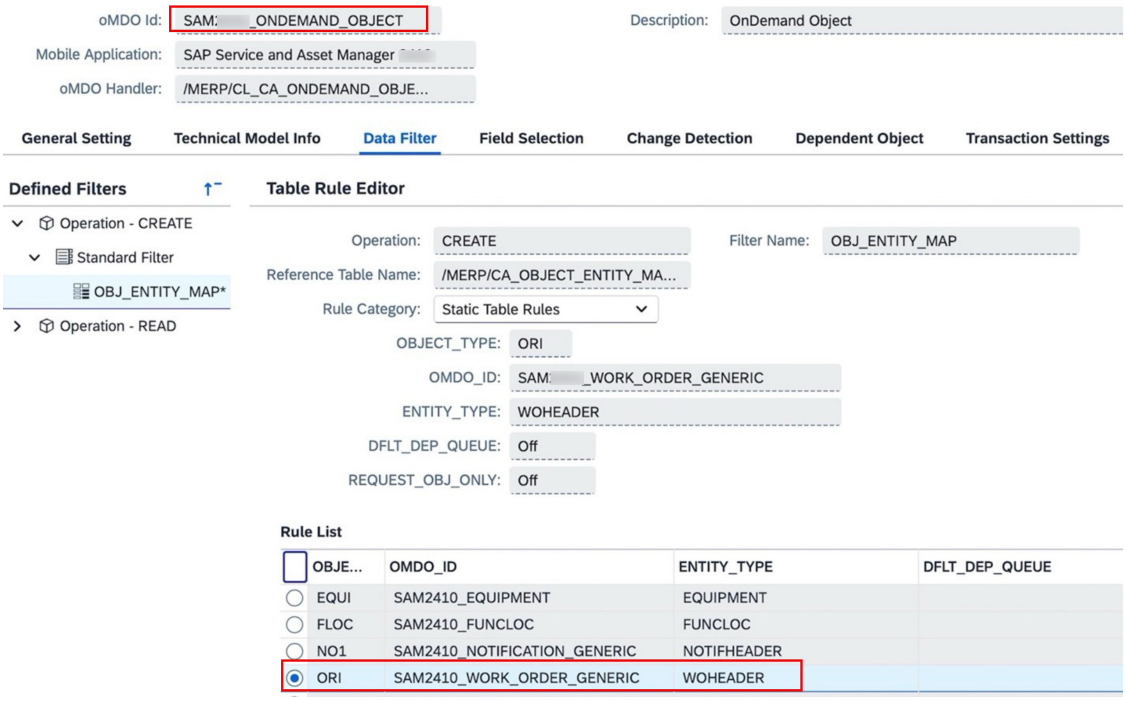


- *Notification*: *SAMXXXX_NOTIFICATION_ONLINE*
  - *MAX_HITS* filter value = *500* by default (to avoid returning too much search criteria data). See the following image:



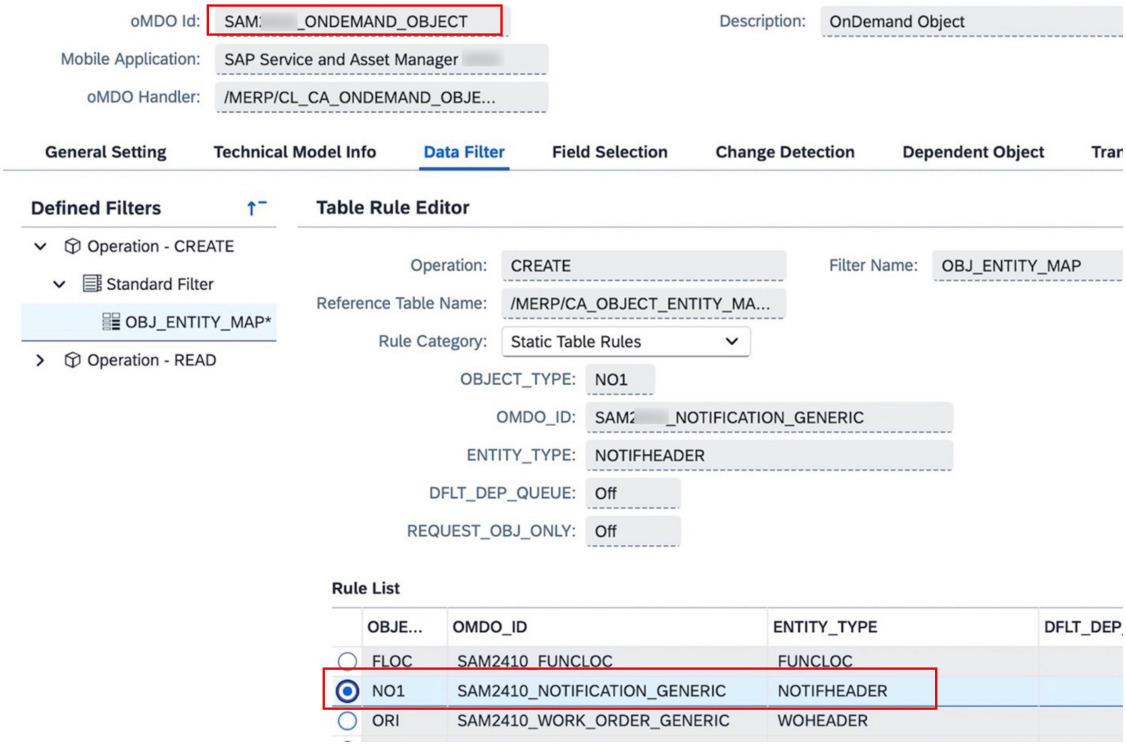
2. When using the SAP Service and Asset Manager mobile client, according to the search criteria, only the header data is returned to the client. However, the user can choose to download the object offline so that the full object details are downloaded to the device after delta synchronization.
3. The following on-demand configurations for Notifications and Work Orders are added to support the on-demand download scenario if users choose to download an object to the offline database:

- *Work Order*:



> **Note**
>
> For Work Orders, the SAP Service and Asset Manager client will also **assign the selected order(s) to the user**.

- *Notification*:



> **Note**
>
> - The distribution criteria configured in the oMDO configurations (*SAMXXXX_NOTIFICATION_GENERIC* and *SAMXXXX_WORK_ORDER_GENERIC*) apply for **on-demand downloads**.
> - If a user decides to download an order that is not in their work center (that is, it does not match the filter criteria in *SAMXXXX_WORK_ORDER_ORDER_GENERIC* oMDO), even if the order is assigned to the user, it will not be downloaded to the device after synchronization.

4.33 Operational Item Configuration

To ensure that safety measures for work are performed at the the operation level, Safety Technicians must perform isolation procedures for an Operational Item. The Operational Item is used to describe the operational processing of **lockout** and **tagout** procedures. This process consists of orderly tagging and subsequent untagging of technical objects, so that work and tests on technical objects can be performed safely.

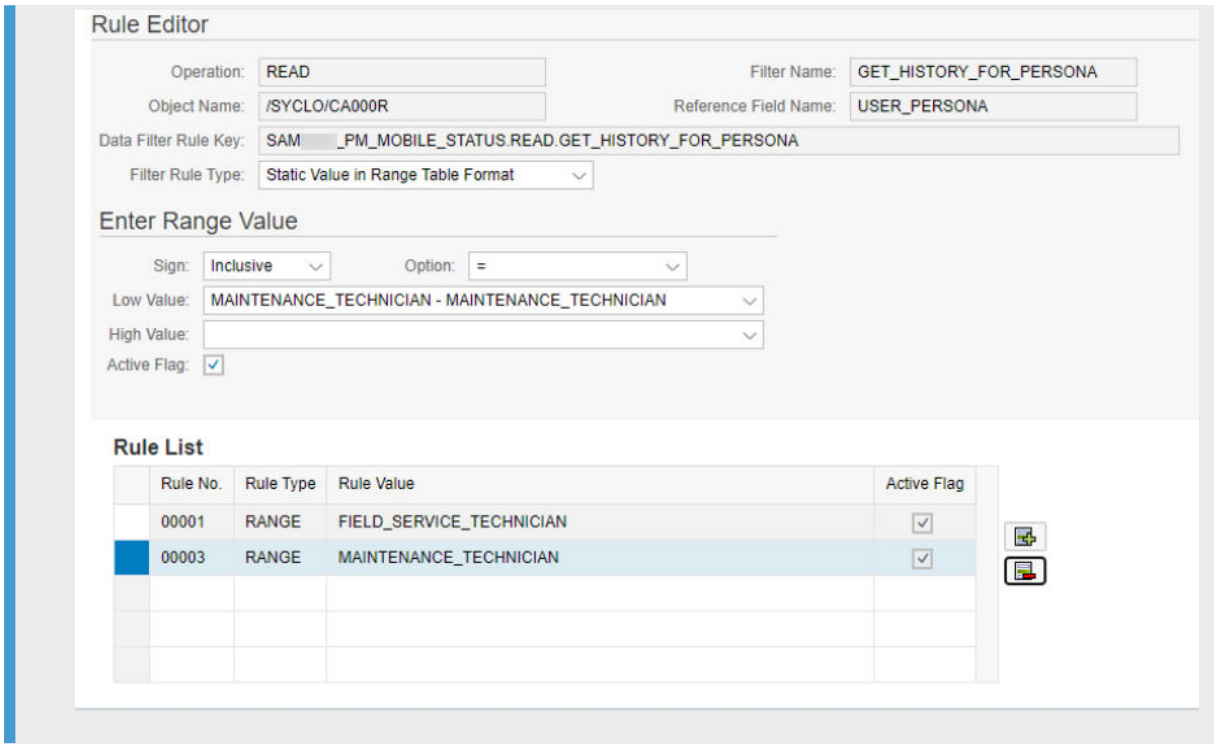
> **Note**
>
> - For more information about using Operational Items, see Operational Item Detail Screen.
> - For more information about recording lockout and tagout activity, refer to Lockout/Tagout section in *SAP ERP - Work Clearance Management (PM-WCM)* documentation.

Supported Personas

This feature is applicable for the following personas:

Maintenance Technician (Pro)
Safety Technician

> **Note**
>
> - For the Maintenance Technician (Pro) persona, this feature is only available from 2410 version.
> - If the user uses Safety Technician (WCM) features via the Maintenance Technician (Pro) persona, you need to add the persona to the data filter *SAMXXXX_PM_MOBILE_STATUS* > *GET_HISTORY_FOR_PERSONA*:



Limitations

See Configuration Prerequisites and Limitations - Safety Technician Persona [page 217].

Prerequisites

Before proceeding with configuration steps below [page 522], make sure the following prerequisite steps are complete:

1. The *WCM_COMMON* feature must be enabled. See General Feature Configuration - Safety Technician Persona [page 218].
2. The *WCM_SAFETY_CERIFICATE* feature must be enabled. See Configuring Isolation Cerificates - Back End - Enabling the Feature [page 448].

Configuration

Perform the following configuration procedure(s):

1. Configure Exchange objects as described in General Exchange Configuration - Safety Technician Persona [page 224].

2. According to your preference, enable or disable the *DocumentItem.SignatureEnabled* mobile application parameter (signature input during tagging or untagging of an operational item). See Mobile Application Parameters - Safety Technician Persona [page 221].

4.34 Quality Management Configuration

The Quality Management application component supports tasks associated with quality planning, quality inspection, and quality control. In addition, it controls the creation of quality certificates and manages problems with the help of quality notifications.

Quality Management (QM) notifications are integrated with SAP Service and Asset Manager as follows:

- Display QM type notifications on the mobile device
- Create QM notifications at the inspection lot level
- Create QM notification items to record defects noted in inspections
- Maintain the association of notifications and notification items with the characteristics

> **Note**
>
> Before configuring QM, you must install the QM component. See the Quality Management chapter in the *SAP Asset Manager Component Installation Guide* for the installation procedure.

Quality Management is disabled on an out-of-the-box new SAP Service and Asset Manager installation. Use the following topics and procedures found in this chapter to enable Quality Management.

4.34.1 Configuring Quality Management Notification Parameters

Context

Code groups that belong together in terms of content are grouped in catalogs. These catalogs are identified by the catalog type (a number or a letter). For example, in this way, you combine:

Use the following parameter groups and associated parameters to configure Quality Management in SAP Service and Asset Manager:

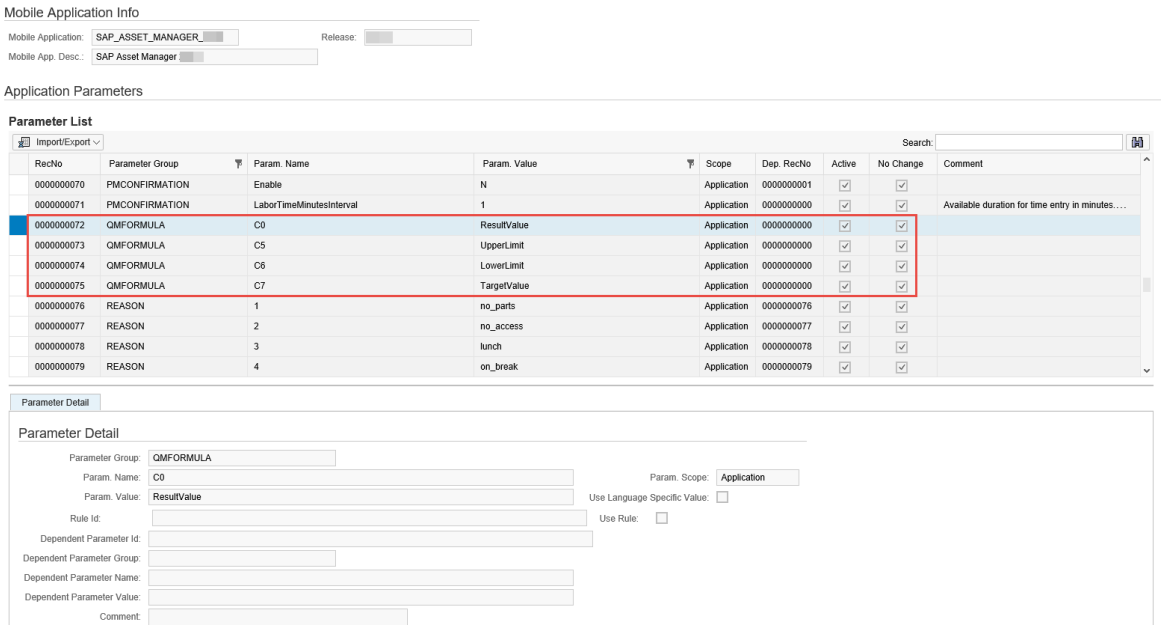
- **QMFORMULA:** Inspection lots can contain points or characteristics. You can use the following formula parameters to determine the characteristic value:
  - **C0:** Arithmetic mean of measured values for characteristic. Standard parameter.
  - **C5:** Upper limit of tolerance range
  - **C6:** Lower limit of tolerance range

    - **C7:** Target value of characteristic
- **CATALOGTYPE:** Sets a usage decision on inspection lots on the client. Standard is *3*
- **DOCUMENT:** Standard is *QMQMEL*
- **INSPECTION_LOT:** Controls if the user of the application can set a decision to complete an inspection lot. When you set an inspection lot to complete, defects are also automatically completed. Standard is *N*.

Procedure

1. Using the ConfigPanel, navigate to *Mobile Application Configuration* > *Parameters tab*. In the left column, *Defined Mobile Applications*, select your application.

   The *Parameter List* populates with a list of all parameters available for the application.
2. Type your desired parameter group into the *Search* box, or scroll to find your parameter. Highlight the parameter you want to configure and click the *Change* button. The following example uses the parameter group *QMFORMULA*.



3. Make your desired parameter association changes.
4. Check the `<Active>` flag to ensure that the parameter is used by the mobile application. If desired, and if not already checked, check the `<No Runtime Change>` box to ensure that the value of the parameter isn't overridden at runtime through synchronization processing.
5. *Save* your changes.

Results

Your Quality Management parameters are configured and enabled.

Next Steps

Complete all other topics and procedures in the Quality Management Configuration [page 523] to fully configure and enable the Quality Management feature.

4.34.2 Configuring oData MDO Data Filters for Quality Management

For general information and a procedure on changing OMDO data filters, see the following topics:

- Working with oData MDO Filter Rules [page 146]
- Changing oData MDO Filter Rules [page 146]

To fully enable Quality Management, ensure that the following data filters and data filter rules are configured properly and active:

SAMXXXX_CATALOG_CODES

Select **SAMXXXX_CATALOG_CODES** from the *oData Mobile Data Object List* and navigate to *Operation - READ* > *Standard Filter* > *CATALOG_TYPE*. Ensure the following rules in the `<Rule Value>` field are set to *Active*:

- 8 - Activities (QM)
- 9 - Defect Types
- D - Coding

SAMXXXX_DOCUMENT

When you enable QM on the **SAMXXXX_DOCUMENT** data filter, you enable the ability to attach documents to an inspection. When mobile client users take a reading on the SAP Service and Asset Manager application, they can attach documents that relate to the inspection on work orders, equipment, functional locations, or notifications.

Select **SAMXXXX_DOCUMENT** from the *oData Mobile Data Object List* and navigate to the following locations:

- *Operation - CREATE_MEDIA* > *Data Segment* > *DOCUMENT_SWITCH*
- *Operation - READ* > *Data Segment* > *DOCUMENT_SWITCH*

Set the following objects in the *Rule List* to *Active*:

- QMQEL: QM notification
- QMTBLOC: Inspection method

Ensure that both *BDS* and *GOS* are set to *Active*.

Navigate to *Operation - READ* > *Standard Filter* > *DOC_LINK_OBJ* > and ensure the following are set to *Active*:

- QMTBDOC: Inspection method attachment
- QMQMEL: QM notification attachment

SAMXXXX_INSPECTION_LOT

Set the dependency to get inspection lots based on work orders related to the inspection assigned to the mobile client user as follows:

Select **SAMXXXX_INSPECTION_LOT** from the *oData Mobile Data Object List* and navigate to *Operation - READ* > *Data Distribution* > *OBJECT_DISTRIBUTION_MODE* >. Ensure that `<Range Value>` *2 - Dependency Queue* is set to *Active*.

Navigate to the *Dependent Object* tab. Ensure that `<Source Tech Entity Type>` *INSPECTIONLOT* is connected to `<Dependent oMDO ID>` **SAMXXXX_NOTIFICATION_GENERIC** and is set to *Active*. When a mobile client user fetches the inspection lots, the related defects, created as QM notifications, are fetched as well.

Ensure that `<Source Tech Entity Type>` *INSPECTIONCHAR* is connected to `<Dependent oMDO ID>` **SAMXXXX_INSPECTION_HISTORY** and is set to *Active*. The fetched inspection history is based on the inspection characteristics available.

SAMXXXX_NOTIFICATION_GENERIC

Select **SAMXXXX_NOTIFICATION_GENERIC** from the *oData Mobile Data Object List* and navigate to *Operation - READ* > *Data Distribution* > *NOTIF_ASSIGNMENT_TYPE* >. Ensure that `<Range Value>` *D* is active.

Navigate to *Operation - READ* > *Data Distribution* > *NOTIF_TYPE* >. Ensure that `<Input Parameter>` *QM* is active.

SAMXXXX_NOTIF_PARTNER_DET_PROC

Enabling QM in the **SAMXXXX_NOTIF_PARTNER_DET_PROC** object means that selecting a business partner is mandatory when a user creates a QM notification.

Select **SAMXXXX_NOTIF_PARTNER_DET_PROC** from the *oData Mobile Data Object List* and navigate to *Operation - READ* > *Standard Filter* > *NOTIF_TYPE* >. Ensure that `<Input Parameter>` *QM* is active.

SAMXXXX_NOTIF_TYPE

Select **SAMXXXX_NOTIF_TYPE** from the *oData Mobile Data Object List* and navigate to *Operation - READ* > *Standard Filter*. Ensure that Quality Management is enabled in the following locations:

- **NOTIF_CATEGORY:** Ensure that `<Range Value>` *02 - Quality Notification* is active.
- **NOTIF_PRIORITY_TYPE:** Ensure that `<Range Value>` *QM - QM Priorities* is active.
- **NOTIF_TYPE:** Ensure that `<Input Parameter>` *QM* is active.

SAMXXXX_PRIORITY

Select **SAMXXXX_PRIORITY** from the *oData Mobile Data Object List* and navigate to *Operation - READ* > *Standard Filter* > *PRIORITY_TYPE*. Ensure that `<Rule Value>` *QM* is active.

SAMXXXX_WORK_ORDER_GENERIC

Enable the dependency between a work order and a related inspection lot on the mobile device:

Navigate to the *Dependent Object* tab. Find the *WOHEADER* objects in the `<Source Tech. Entity Type>` column. Scroll to find the **SAMXXXX_INSPECTION_LOT** object. Ensure it is marked as *Active*.

4.34.3 Inspection Lots

Quality Management enables you to ensure the quality of your products, processes, and services right from the start. It helps you to plan, execute, and monitor different types of quality inspections, for example, in procurement, production, or sales scenarios. Inspection plans help you to define how a quality inspection of one or several materials is to take place. For reuse purposes, you can integrate master data in your inspection plans. If defects occur, efficient nonconformance management features help you to report and process these defects to eliminate them and prevent them from recurring. By gaining better insights into your quality-related data, you can improve your processes and products and thereby achieve your corporate quality goals. For more information, refer to the Quality Management documentation.

Some basic configurations used in SSAM can be found at:

1. Catalogs used in the quality inspection characteristics are defined on the *IMG* > *Quality Management* > *Quality Planning* > *Basic Data* > *Catalog* > *Edit Catalogs* section
   - T-code: QS41 (edit catalog: 3 for usage decisions and 1 for characteristic attributes)
     QS51 (edit selected set)
   - Catalog/selected set data is used in SSAM for qualitative inspection characteristics as well as in the valuation of inspection points
2. Maintain master inspection characteristics (MIC):

- T-code: QS21 (create MIC)
- Information about the master inspection characteristics (MIC) is displayed in SSAM when you navigate to *More Informationon* on the *Record Results* screen displaying the inspection characteristics. This is only displayed if the inspection characteristics refer to the master inspection characteristics in the inspection plan

3. Maintenance of inspection types is defined on the *IMG* > *Quality Management* > *Quality Inspection* > *Inspection Lot Creation* > *Maintain Inspection Types* section
   - The selected set of UDs maintained here is used in SSAM to valuate inspection points and make decisions about their use
   - The notification type maintained here is used to create defects on rejected inspection characteristics when recording results

Following are the IMG paths for the QM calibration core configuration:

- *IMG* > *Quality Management* > *Quality Planning* > *Basic Data*
- *IMG* > *Quality Management* > *Quality Inspection* > *Inspection Lot Creation*
- *IMG* > *Quality Management* > *Quality Inspection* > *Inspection Lot Completion*
- *IMG* > *Plant Maintenance and Customer Service* > *Maintenance and Service Processing* > *Maintenance and Service Orders*

With that, here are the transactions used in the corre configuration of the general task list:

QCC0	QM IMG
IA05/06/07	Create/Change/Display General Task list
IP41/42	Create/Change Maintenance Plan
IP10	Manual Scheduling of Maintenance Plan
IP30	Background Scheduling of Maintenance Plan
QA03	Display Inspection Lot
QA11	Manual Usage Decision for Inspection Lot
QE51N	Record Results Mass
QE01	Record Results for Inspection Lot
CT04	Create/Change/Display Characteristics (otherwise known as class characteristics can be used to define master inspection characteristics and/or measuring points)
QS21/22/24	Create/Change/Display Master Inspection Characteristics
QA01/02/03	Create/Change/Display Inspection Lot
QA31/32/33	Create/Change/Display Results Data for Inspection Lot

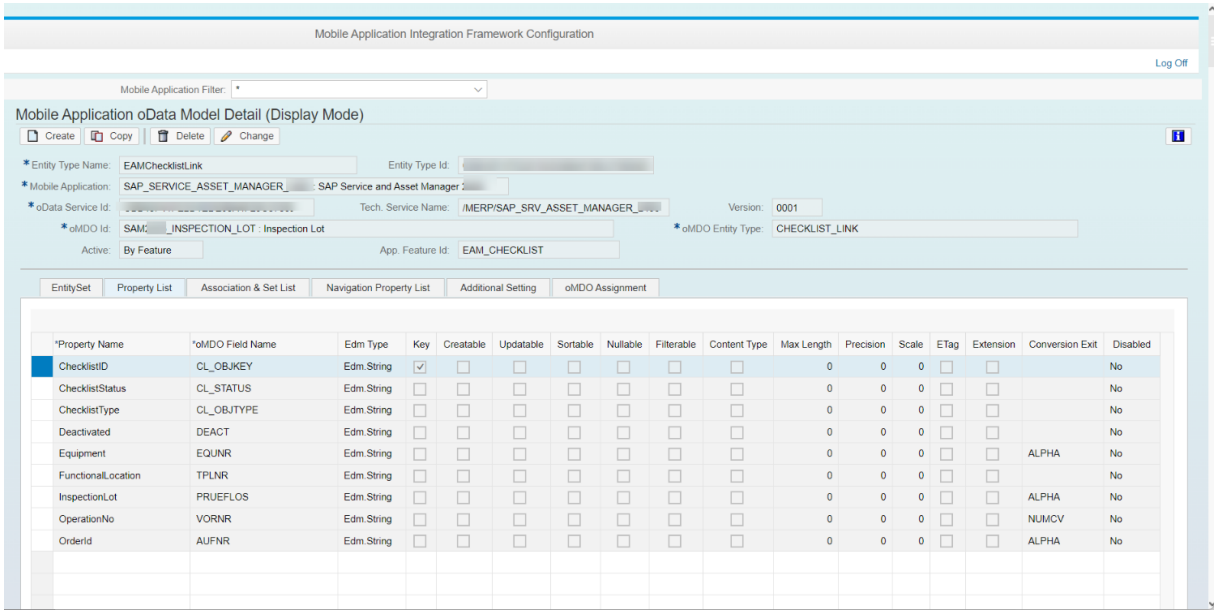
4.34.4 EAM Checklist Overview

EAM processes need checklists for actions such as inspections and maintenance. SAP Service and Asset Manager uses EAM checklists with work orders and operations.

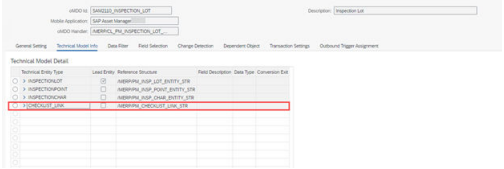
> **Note**
>
> This core feature is only available on an SAP S/4HANA 2021 or later back end system. This feature is therefore available for SAP Service and Asset Manager 2110 or later releases installed on an SAP S/4HANA or later back end system.

Find the EAM checklist feature in the OMDO handler */MERP/CL_PM_INSPECTION_LOT_OD*, as an existing entity. Features of inspection lot are reused to implement the EAM checklist functionality, along with a new entity, *EAMChecklistLink*. Access the OMDO handler through transaction *SE24* on your back end system.

You can view the new entity in the ConfigPanel by navigating to *oData Model Configuration* > *Mobile App SAP_SERVICE_ASSET_MANAGER_<version>* > */MERP/SAP_SRV_ASSET_MGR_<version>* > *EAMChecklistLink*.



The *INSPECTION_LOT* OMDO is updated to add a technical entry for checklists. Navigate to *oData Mobile Data Object Configuration* > *Technical Model Info tab* > *<version>_INSPECTION_LOT*. Be sure to choose your application release version using the *Mobile Application Filter*.



Use the following procedures to configure the EAM checklist feature:

- Enabling or Disabling the EAM Checklist [page 530]

- Enabling or Disabling Manual Defect Recording [page 531]

4.34.4.1 Enabling or Disabling the EAM Checklist

Context

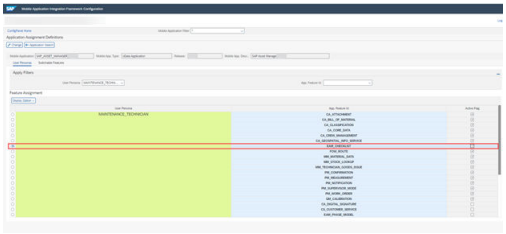
The EAM Checklist feature is called *EAM_CHECKLIST*. By default, the feature is not enabled.

> **Note**
>
> As of the SAP Service and Asset Manager 2205 release, enable and disable parameters are no longer available through the *Parameters* tab. You enable or disable all features through the *Features* tab. See the Configuring Features [page 93] procedure for details.

Procedure

1. Navigate to *Component Assignments*. Select your application in the *Mobile Application Filter*. Click the application link in the *Search Result* table.

   The *Application Assignment Definitions* page displays.
2. Click the *Change* button. Find the *EAM_CHECKLIST* feature ID in the *MAINTENANCE_TECHNICIAN* user persona part of the table. Enable or disable the feature using the *Active Flag* checkbox.

   
3. *Save* your changes.

   If you've enabled the checklist feature, the inspection results display on a mobile device on the *Checklists* detail screen. Validation of all inspections results is done per limits set during configuration of inspection characteristics in the inspection plan. Once results on the mobile device are synced to the back end, the results and usage decision are updated. The EAM checklist is marked as complete on the mobile device.
4. Enable the dependency between a work order and a related inspection lot on the mobile device. Navigate to *SAM<version>_WORK_ORDER_GENERIC oMDO*.
5. Select the *Dependent Object* tab. Find the *WOHEADER* objects in the *<Source Tech. Entity Type>* column.
6. Find the *SAM<version>_INSPECTION_LOT* object. Enable the feature using the *Active* checkbox.

4.34.4.2 Enabling or Disabling Manual Defect Recording

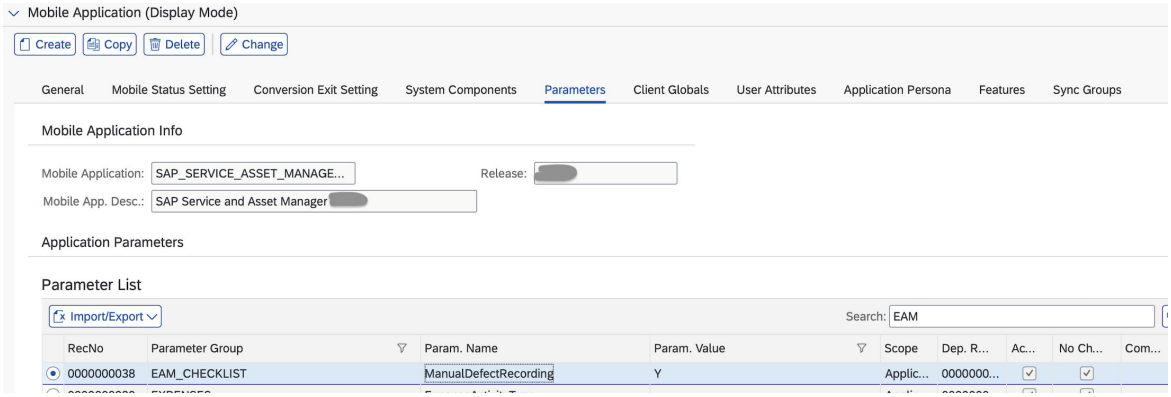
Context

The functionality for creating defects manually for a rejected inspection task result from the mobile device is enabled through the *Parameters* tab. The EAM checklist feature is enabled by default.

Procedure

1. Using the ConfigPanel, navigate to *Mobile Application Configuration* > *Parameters tab*. In the left column, *Defined Mobile Applications*, select your application.

   The *Parameter List* populates with a list of all parameters available for the application.
2. The EAM checklist parameters are found in the *EAM_CHECKLIST* group. You can scroll down to find the parameter, or perform a search using the *Search* box. Highlight the *ManualDefectRecording* parameter and click the *Change* button.



   The parameters found in the *EAM_CHECKLIST* group work alongside the order type configuration to automatically create the defects upon results recording. When the parameter is enabled, the *Record Defct* button on a rejected inspection characteristic is availabe on the app. A technician can add defect details. The app creates a notification on the back end when the mobile device is synced for the default EAM defect notification type assigned to that order type.
3. Make your desired parameter association changes. Enable the parameter as follows:

   - **Y:** Select if work order types are not set up with automatic defect recording
   - **N:** Select if you've configured work order types set up with automatic defect recording
4. Check the `<Active>` flag to ensure that the parameter is used by the mobile application. If desired, and if not already checked, check the `<No Runtime Change>` box to ensure that the value of the parameter is not overridden at runtime through synchronization processing.
5. *Save* your changes.

4.34.4.3 EAM Checklist Attachments

When enabling EAM on the SAM2305_DOCUMENT data filter, you can attach documents to inspection lots. And when taking readings in the SAP Service and Asset Manager mobile app, you can attach documents related to the inspection lots.

1. Select *SAM2305_DOCUMENT* in the *oData Mobile Data Object List* and navigate to the following:
   - *Operation* > *CREATE_MEDIA Data Segment DOCUMENT_SWITCH*
   - *Operation* > *READ Data Segment DOCUMENT_SWITCH*
2. Add new lines to the *Rule List* for *BDS* and *GOS*:
   - *OBJECT_TYPE*: BUS2045
   - *OBJECTLINK*: BUS2045

   > **Note**
   >
   > Ensure that both *BDS* and *GOS* are set to *Active*.
3. Add new lines to the *Rule List* for *DMS*:
   - *OBJECT_TYPE*: BUS2045
   - *OBJECTLINK*: QALS

   > **Note**
   >
   > Ensure that both *DMS* is set to *Active*.
4. Navigate to *Operation* > *READ Standard Filter DOC_LINK_OBJ*
5. Add a new line to the *Rule List* and enter the following range value:
   - *Sign*: Inclusive
   - *Option*: =
   - *Low Value*: QALS
6. Enable the active flag
7. Navigate to *Operation* > *READ Standard Filter CLASSNAME*
8. Add a new line to the *Rule List* and enter the following range value:
   - *Sign*: Inclusive
   - *Option*: =
   - *Low Value*: BUS2045
9. Enable the active flag.

4.34.4.3.1 SAM 2511 Inspection Lot

In SAP Service and Asset Manager, inspection lots often include related documents, such as attachments, URLs, or long-text information that technicians need to access while performing inspections on mobile devices.

Context

By default, SAM doesn't automatically synchronize all document-related metadata for inspection lots. To ensure that mobile users can view associated documents and long texts, administrators must configure the Inspection Lot mobile data object to retrieve and link these document records. This configuration enables the application to read and display attachments, URLs, and inspection characteristic long texts directly on the mobile device.

Procedure

1. Select *SAM<version>_INSPECTION_LOT* in the *oData Mobile Data Object List* and navigate to the *Data Filter* tab.
2. In the *Defined Filters* list, navigate to *Operation* > *READ Standard Filter ABS_DOC_TYPE*
3. Set filter handler *OMDO_ID=SAM<version>_DOCUMENT&OPERATION=READ&DOF_NAME=DOCUMENT_SWITCH&OBJECTLINKS=BUS2045,QALS&OBJECT_TYPES=BUS2045* to *Active*.

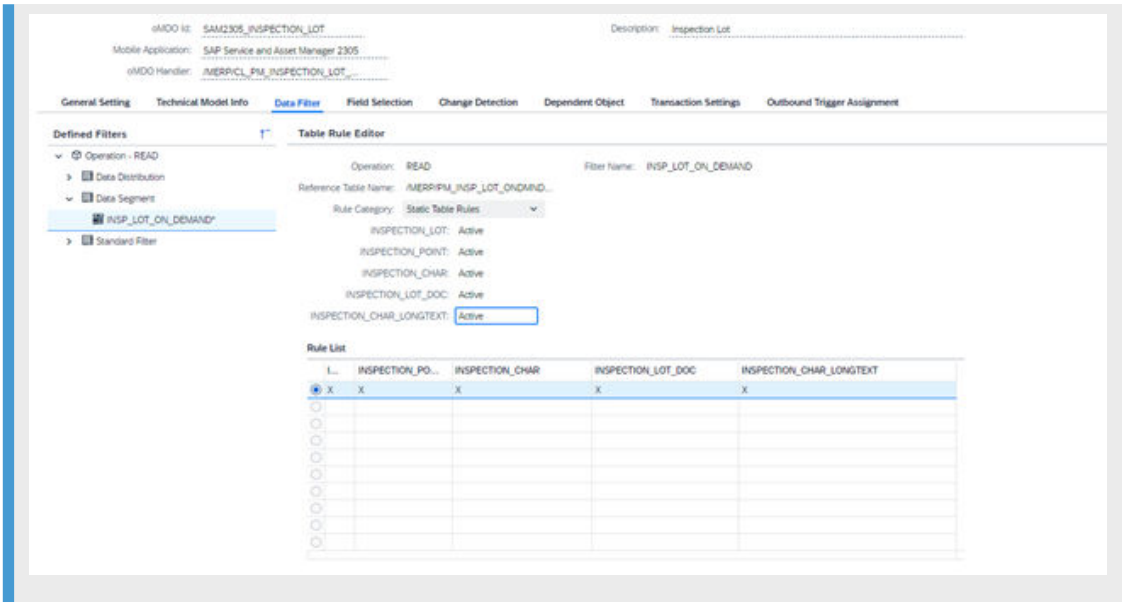


4. Navigate to *Operation* > *READ Standard Filter DOC_CLASSNAME*
5. Add a new line to the *Rule List* and enter the following range value:
   - *Sign*: Inclusive
   - *Option*: =
   - *Low Value*: BUS2045
6. Enable the active flag
7. Navigate to *Operation* > *READ Standard Filter DOC_CLASSTYPE*
8. Add a new line to the *Rule List* and enter the following range value:

- *Sign*: Inclusive
- *Option*: =
- *Low Value*: *BO* > *Business Object Repository* object

9. Enable the active flag
10. Navigate to *Operation* > *READ Standard Filter DOC_GOS_RELTYPE*
11. Add a new line to the *Rule List* and enter the following range value:
    - *Sign*: Inclusive
    - *Option*: =
    - *Low Value*: *ATTA* > *Has the Attachment*
12. Enable the active flag
13. Add a new line to the *Rule List* and enter the following range value:
    - *Sign*: Inclusive
    - *Option*: =
    - *Low Value*: *URL* > *Has Internet Link*
14. Enable the active flag
15. Enable dependency between the inspection lot and the related document on the mobile device
16. Navigate to the *Dependent Object* tab. Find *INSPECTIONLOTDOC* objects in the *<Source Tech. Entity Type>* column. Scroll the page to find the *SAM<version>_DOCUMENT* object. Ensure it is marked as *Active*.
17. Insert new lines in the *Dependent Object Keys* tab:
    1. *Source oMDO Field Name:* OBJECT_KEY
       Dependent Object Key Fieldname: OBJECT_KEY
18. Insert new lines in the *Origin Object Keys* tab:
    1. *Field name:* OBJECT_KEY
    2. *Field name:* DOC_OBJ_ID

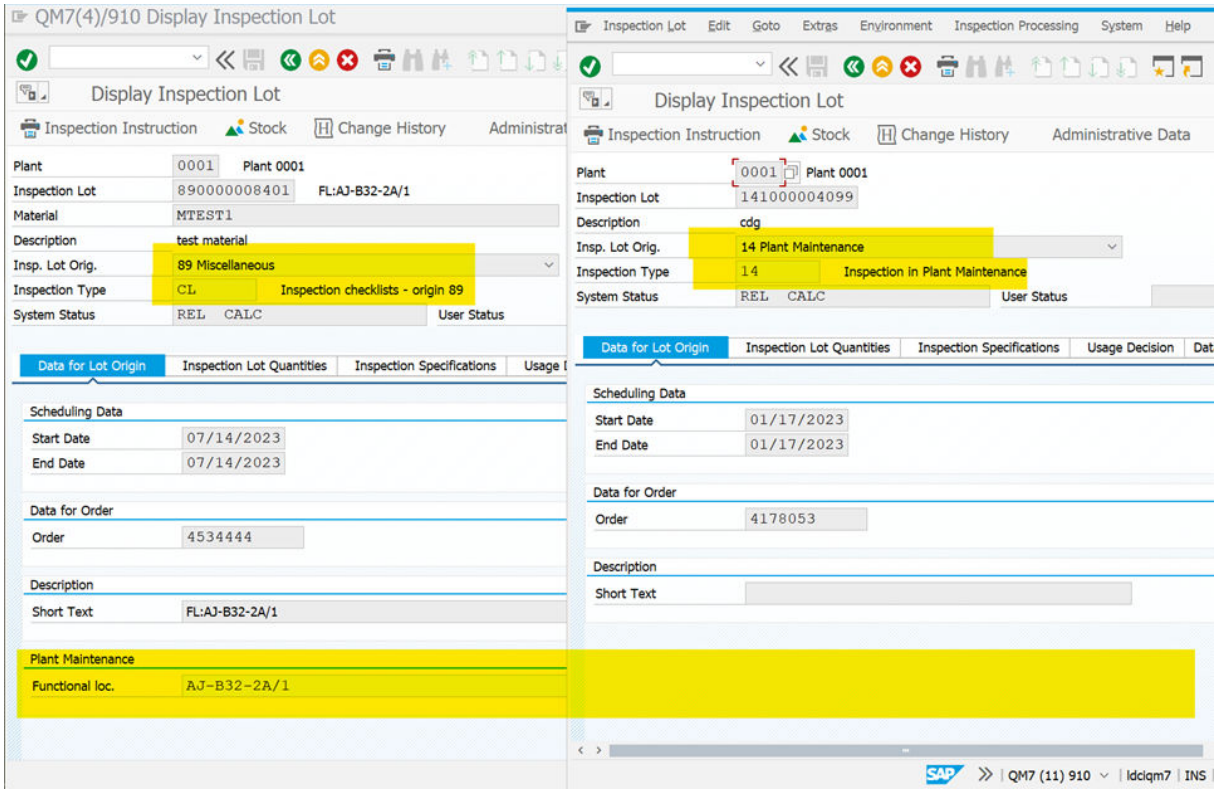
> **Note**
>
> As of 2305 version, the SAP Service and Asset Manager introduces an additional feature concerning long texts for master inspection characteristics: a new *MasterInspectionCharLongText* entity is created as an *InspectionLot* sub-entity. Set the flag to *Insp_Lot_On_Demand* to enable reading the long text of the main inspection characteristic. By default, it is active.



4.34.5 PM/EAM Checklists

You can use checklists to inspect and check assets. They are legally binding documents.

With the inspection checklist process configured in your system, you will minimize the effort to maintain and operate your master data. For more information, refer to the Maintenance Management documentation.



SAP Service and Asset Manager and core S4 uses the QM inspeciton lot framework for the EAM checklsists.

The inspection lot display transaction (t-code QA03) shows PM details, such as equipment or Floc, on the *Data for Lot Origin* tab of a lot. The checklist is created for the technical object. QM calibration lots are not created because they contain inspection points related to the technical object being inspected.

The basic configurations and operations listed above are also used for EAM checklists.

In addition, these T-codes (in the table) are used to process and configure EAM checklists.

T-Codes	Descrcription
QP01/02/03	EAM checklists: Create/Modify/Display Inspection Plans
IP01/02/03	QM Calibration Lots: Create/Modify/Display Maintenance Plans
IK01/02/03	Create/Change/Display Measuring Points
IK11/12/13	Create/Change/Display Measurement Document
IW91	Checklists: Result Overview
IW92	Checklists: Generation
IW93	Checklists: Collective Usage Decision
IW97	Checklists: Simulate Inspection Lots
IW98	Checklists: Classification Characteristics
IW99	Checklists: Types

4.35 Samsung Knox Capture Configuration

On Samsung devices, users can scan QR codes by the Knox Capture integration, which will allow them to:

- Scan a single QR code to navigate directly to an object's detail page.
- Scan multiple QR codes at once to save/issue multiple objects.
- Trigger the scanning function directly by pressing the **Active** or **XCover** keys on supported Samsung devices.

> ⓘ Note
>
> - For more information about using Samsung Knox Capture, refer to Using Samsung Knox Capture.
> - The **SAP Scanner Framework** allows metadata to manipulate different scanners using the same APIs. For more information, see SAP Scanner Framework.
> - This feature is a third-party integration by Samsung. For more information and the list of supported devices, refer to the official Samsung Knox documentation .

Supported Personas

This feature is applicable for the following personas:

Maintenance Technician (Standard)
Maintenance Technician (Pro)
Field Service Technician (Standard)
Field Service Technician (Pro)

Prerequisites

Before proceeding with SAP Service and Asset Manager back end configuration step below [page 538], you need to perform either of the following Knox configurations:

- Manual configuration (applicable only for a small group of users) [page 537]
- Mass deployment for a fleet of devices via EMM-based deployment [page 538]
- Share configuration via QR code, NFC or email [page 538]

Manual configuration

Perform the following steps as the IT Admin, before sharing the configuration via EMM-based deployment [page 538] or QR code [page 538].

1. Install and configure Samsung Knox Capture application on the mobile device:
    1. Download Samsung Knox Capture from the Google Play Store.
    2. Open the app and agree to the Privacy Policy.
    3. Select *Knox Capture* as scan engine.
    4. On the *Knox Capture* main menu, tap the three dots in the header and tap *License*.
        1. Enter your Knox Capture license key.

        > **Note**
        >
        > - Without a license, the number of free scans is limited.
        > - You can get your Knox Capture license from Samsung (refer to Manage licenses in official Samsung Knox documentation).

    5. Go back to the main menu and tap *Create profile*.
        1. Enter a name for the profile (e.g. SSAM).
        2. Select SAP Service and Asset Manager from the list of applications, tap *Create profile* and select all from the list of activities.
    6. In the profile you created, tap *Select app packages* to configure the intent output.
        1. Select SAP Service and Asset Manager from the list of applications and go back.
    7. Tap *Action* to configure the intent action.
        1. Enter `com.samsung.knoxcapture.intent.action.RECEIVER` as Action and tap *Save*.

        > **Note**
        >
        > Make sure you enter the Action correctly as it is key for SAP Service and Asset Manager to receive scan data from Knox Capture.

8. Go back to the main menu and tap the three dots in the header and tap *Camera scan triggers*.
    1. Enable the *Start scan from business app* option.
2. Depending on the Samsung device, you can configure the hardware key to trigger the scanning as follows:
    1. Go to the *Device Settings*.
    2. Search for and open the settings of either **XCover** button (on a phone) or **Active** button (on a tablet).
    3. Set SAP Service and Asset Manager as the application to use with the **XCover** / **Active** button.

Mass deployment through an EMM

As an IT admin, you can deploy Knox Capture with a custom scanning configuration across a fleet of devices, using EMM-based deployment.

1. Perform all the steps described in above section, Manual configuration. [page 537]
2. Export the configuration as a text file, as described in Exporting a configuration .
3. Perform all the steps described in the section Deploying through an EMM .

Sharing configuration via QR code, NFC or email

As an IT admin, you can also share the configuration via a QR code, NFC or email.

1. Perform all the steps described in above section, Manual configuration. [page 537]
2. Export the configuration either as an email, nearby share or QR code, as described in Exporting a configuration .
3. On the receiving devices, import the configuration file or scan the QR code as described in Sharing and importing configurations .

Back End Configuration

Perform the following configuration step(s):

- Configuring Samsung Knox Capture - Back End - Mobile Application Parameters [page 538]

4.35.1 Configuring Samsung Knox Capture - Back End - Mobile Application Parameters

Context

For detailed information about Samsung Knox Capture and prerequisite steps to perform in the Knox application, see the overview topic, Samsung Knox Capture Configuration [page 536].

The following procedure describes how to configure Mobile Application Parameters for the Samsung Knox Capture feature in the Configuration Panel.

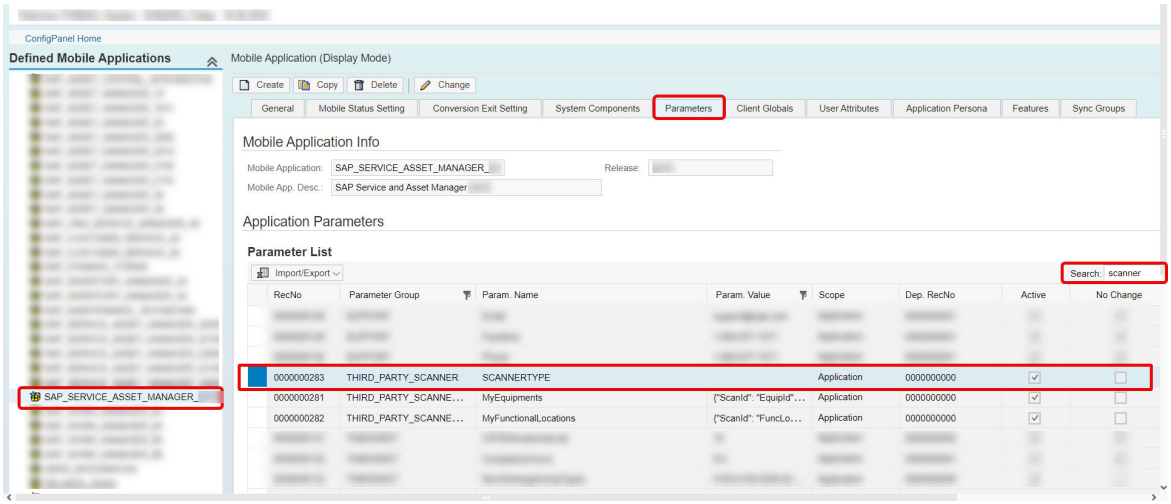
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

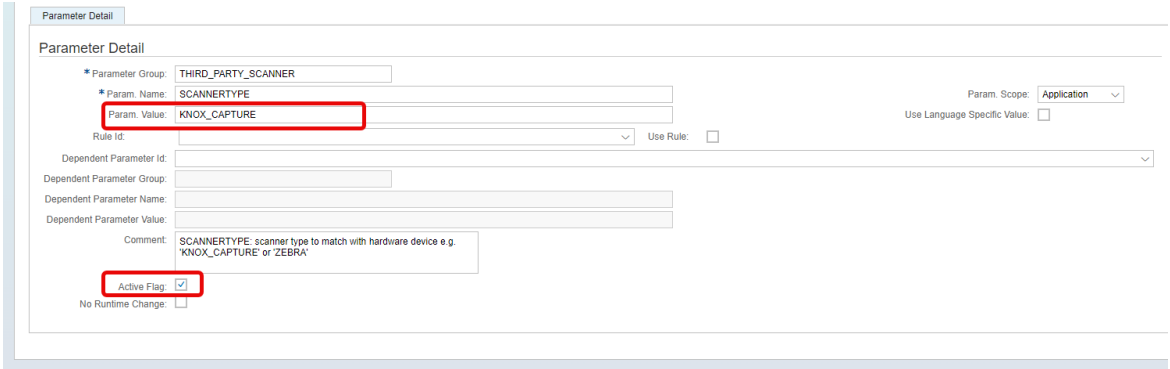
- **Mobile Application Parameters** configuration: refer to Parameters Tab in *MAIF Configuration Guide*.

Procedure

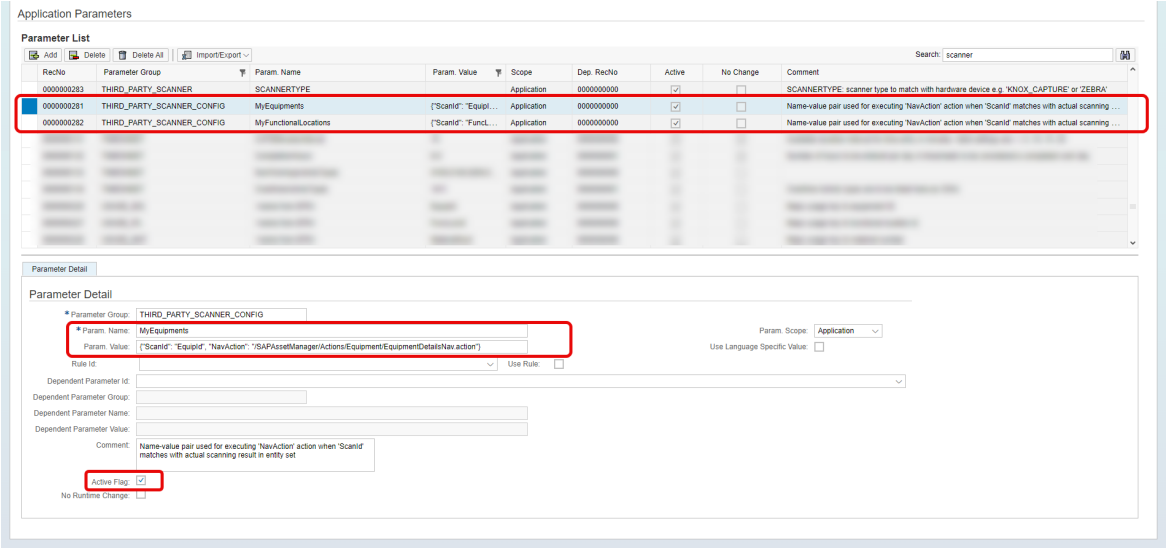
1. On the Configuration Panel, go to *Mobile Application Configuration*.
2. Select your application from the left, go to the *Parameters* tab and select the *SCANNERTYPE* Application Parameter.



3. Enter *Change* mode, add *KNOX_CAPTURE* as *Parameter Value*, set the parameter to *Active* and click *Save*.



4. In case of single scanning, you can configure additional parameters to quickly navigate the user to an object within the application, when scanning a QR code. See below example:



1. Enter *Change* mode and add a new row under *Parameter List*.
2. Under *Parameter Detail*, add *THIRD_PARTY_SCANNER_CONIG* as the *Parameter Group*.
3. Add the *Parameter Name* according to the object type you want the user to navigate to (e.g. 'MyEquipments', 'MyFunctionalLocations').
4. Add the *Parameter Value* according to the object type you want the user to navigate to (e.g. `{"ScanId": "EquipId", "NavAction": "/SAPAssetManager/Actions/Equipment/EquipmentDetailsNav.action"}`).
5. Set the parameter to *Active* and click *Save*.

> **Note**
>
> You can configure these parameters for any Overview or List pages in the application. However, please note the following:
>
> - Multiple objects may have the same ID (also different object types).
> - If you configure multiple parameters for multiple object types, the order of parameters matter in the Parameter List.
> - When the user scans a QR code, the application will navigate to the object, which has the first match with the scanned ID.

4.36 SAP Dynamic Forms Configuration for SAP Service and Asset Manager

SAP Service and Asset Manager supports SAP Dynamic Forms, an SAP Business Technology Platform application that allows you to design, deploy, and use basic and complex forms. Key functionalities include:

- Support to create and edit form instances associated with the following business objects:
  - Work Orders
  - Notifications

    - Equipments
    - Functional locations
    - Work Permits
    - Isolation Certificates and Other Certificates
    - S/4 service system:
        - Service Orders
        - Service Items
- Ability to create, edit and delete forms locally. While being offline, users can:
    - Open, complete and submit locally created forms.
    - Modify and save locally created and updated forms.
    - Delete an unsynced form.
- Support for syncing forms on SAP BTP.

> **Note**
>
> For more information about:
>
> - The product, see SAP Dynamic Forms product page.
> - Using SAP Dynamic Forms, see Working with Dynamic Forms.
> - Installing and configuring SAP Dynamic Forms, see SAP Dynamic Forms Installation Guide and SAP Dynamic Forms Configuration Guide in *SAP Dynamic Forms documentation*.
> - Mobile Application Integration Framework configuration for SAP Dynamic Forms, see Dynamic Forms Agent Settings in *MAIF Configuration Guide*.

Supported Personas

This feature is applicable for the following personas:

Maintenance Technician (Standard)
Maintenance Technician (Pro)
Field Service Technician (Standard)
Field Service Technician (Pro)
Safety Technician

> **Note**
>
> For the Safety Technician persona, SAP Dynamic Forms is available from **2511** version.

Limitations

Please note the following limitations for specific persona(s):

- **Safety Tehnician**:
  - Safety Technicians can **create, edit and submit** Forms attached to Work Permits, Isolation Certificates and Other Certificates. However, Forms attached to other object types (e.g., Work Orders, Notifications) are **read-only**. Additionally:
    - Work Permits in *Closed* status are **read-only** as well.
    - Isolation Certificates and Other Certificates in *Closed* status **will not be downloaded** to the client by default.

Configuration

By default, SAP Dynamic Forms is disabled for all mobile application versions. To enable and configure the feature, perform the following steps:

1. Configuring SAP Dynamic Forms - Back End - Feature Configuration [page 542]
2. Configuring SAP Dynamic Forms - Back End - Exchange Object [page 544]

Additional Configuration Options

- Identify Form Definitions for Client Download [page 546]: If there is **at least one** Form Instance downloaded to the SAP Service and Asset Manager client, it will download the corresponding Form Definition. However, by default the client **will not download** any other Form Definitions and you need to identify additional Form Definitions to download to the client.
- Access Form Data from SAP Service and Asset Manager Metadata [page 547] to create customized forms.

4.36.1 Configuring SAP Dynamic Forms - Back End - Feature Configuration

Context

For detailed information about SAP Dynamic Forms, see the overview topic, SAP Dynamic Forms Configuration for SAP Service and Asset Manager [page 540].

The following procedure describes how to enable the SAP Dynamic Forms feature in the Configuration Panel.

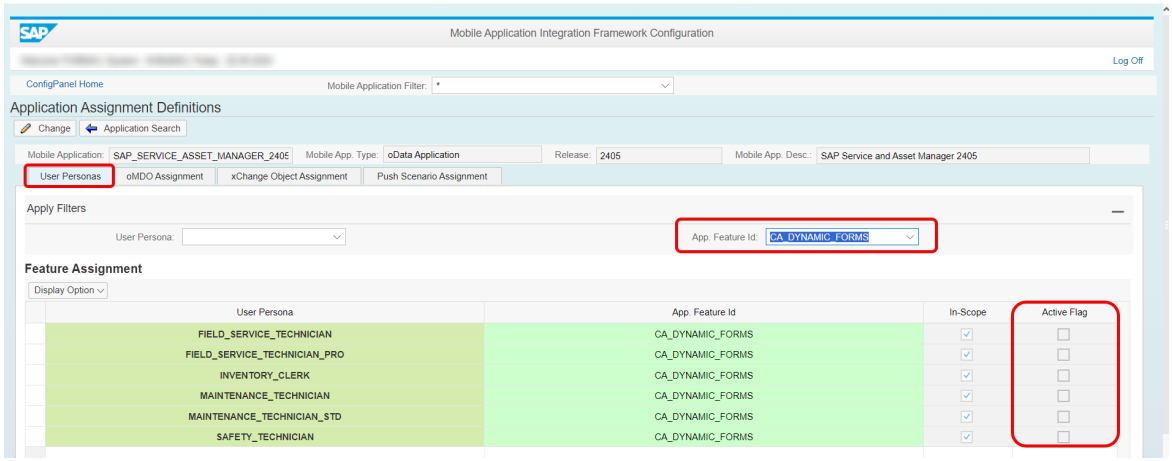
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

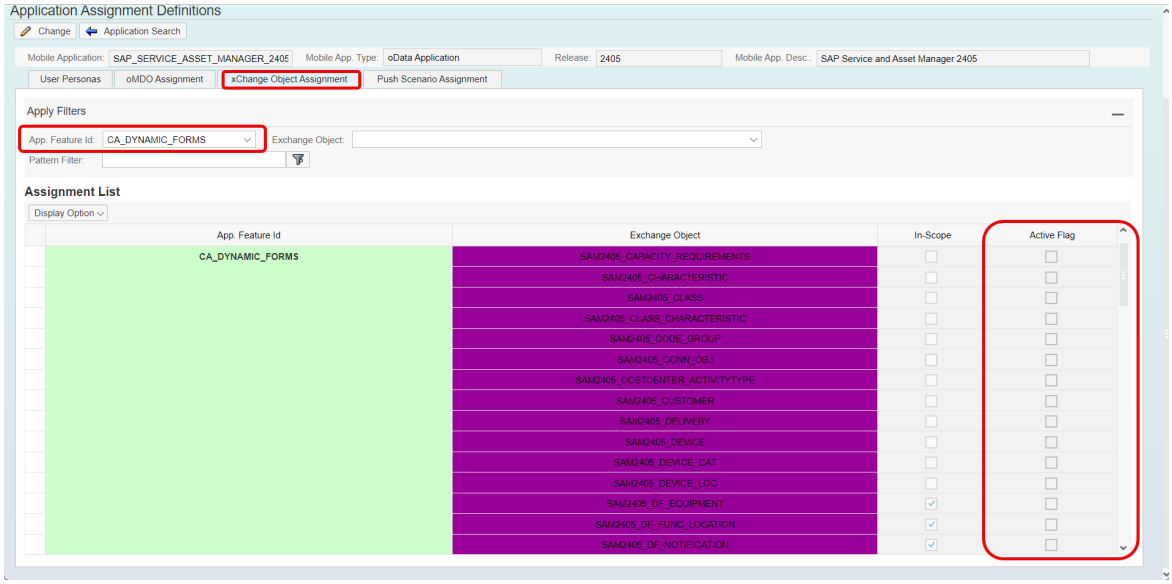
- **Enabling and disabling features**: refer to Configuring Features in *MAIF Configuration Guide*.

Procedure

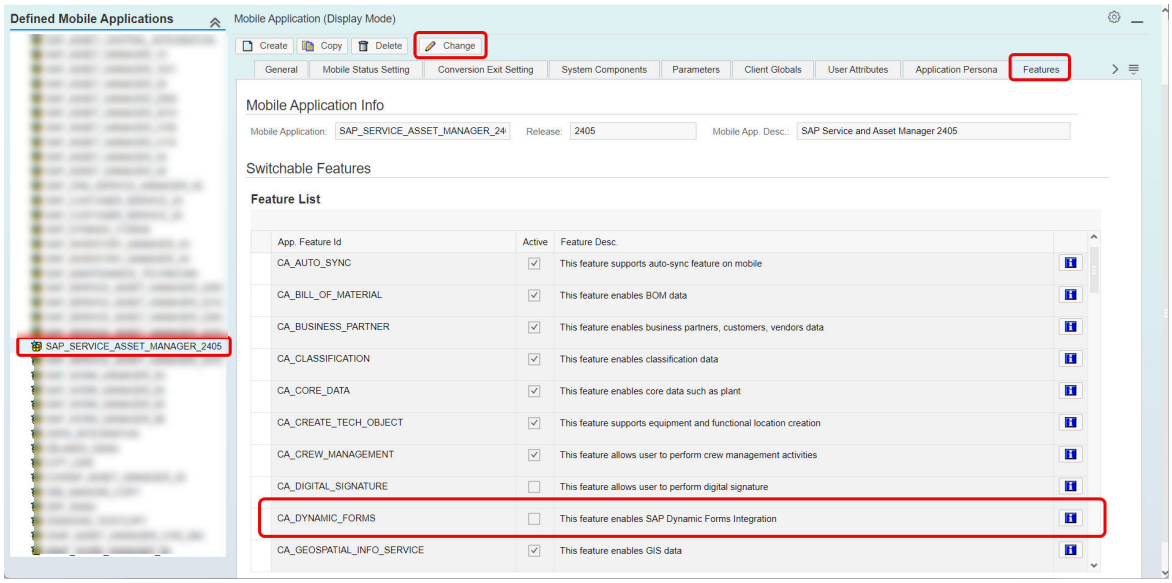
1. Log in to *SAP GUI* and execute transaction `/SYCLO/CONFIGPANEL` to open to the *Config Panel*.
2. Navigate to *Component Assignments* > *SAP_SERVICE_ASSET_MANAGER_XXXX*.
3. Under the *User Personas* tab, filter by the *CA_DYNAMIC_FORMS* App. feature Id.



4. Enter change mode and check the *Active* flag for the dynamic forms relevant personas.
5. Go to the *xChange Object Assignment* tab.
6. Filter by the *CA_DYNAMIC_FORMS* app and enable the exchange objects for any corresponding SAP objects that are relevant for using forms.



7. Click *Save*.
8. Go back to the *Config Panel* home page and navigate to *Mobile Application Configuration* > *SAP_SERVICE_ASSET_MANAGER_XXXX* > *Features*.



9. Enter change mode, find the *CA_DYNAMIC_FORMS* feature ID and activate it.
10. Click *Save*.

Results

SAP Dynamic Forms is now enabled to use with SAP Service and Asset Manager. Continue the configuration process with Configuring SAP Dynamic Forms - Back End - Exchange Object [page 544].

4.36.2 Configuring SAP Dynamic Forms - Back End - Exchange Object

Context

For detailed information about SAP Dynamic Forms, see the overview topic, SAP Dynamic Forms Configuration for SAP Service and Asset Manager [page 540].

SAP Dynamic Forms uses the exchange process during automatic form creation. The exchange determines whether a creation or change to an SAP business object has met the conditions for forms creation. To change these conditions according to your business needs, perform the following steps.

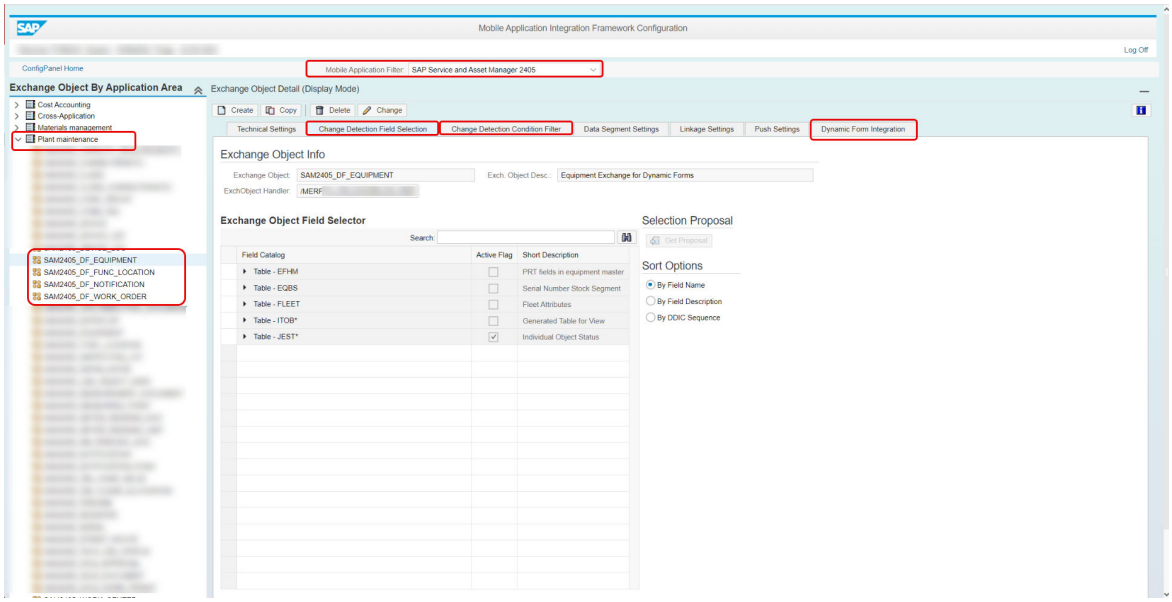
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

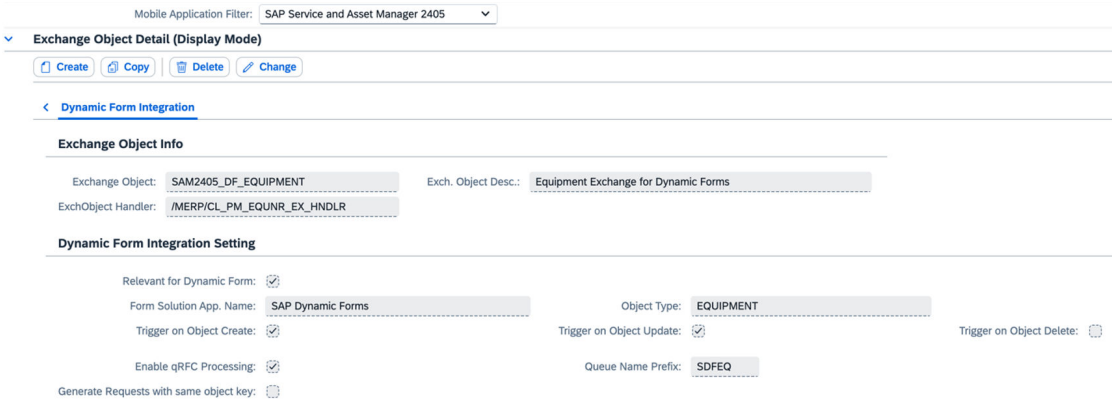
- **Exchange** and **Exchange filters** configuration: refer to Exchange Object Configuration and Change Detection Condition Filter Tab in *MAIF Configuration Guide*.

Procedure

1. Go to the *Config Panel* home page and navigate to *Exchange Object Configuration*.
2. Filter the exchange objects by your mobile application version.
3. Under Plant maintenance, click on one of the exchange objects that matches the following pattern: *SAMXXXX_DF_** (e.g., SAM2405_DF_EQUIPMENT)



4. Check the following tabs and configurations:
   - *• Change Detection Field Selection*: This configuration restricts change detection based on the selected fields of the data tables. For more information, refer to Exchange Object - Change Detection Field Selection.
   - *Change Detection Condition Filter*: This configuration restricts change detection based on data content. For more information, refer to Exchange Object - Change Detection Condition Filter
   - *Dynamic Forms Integration*



   - *Relevant for Dynamic Forms*: Marks the corresponding exchange object as Dynamic Forms-relevant. This means that any qualifying change detected by this exchange object will be sent to the Dynamic Forms agent for form definition determination.
   - *Form Solution App. Name*: The application name of the forms solution.

- *Object Type*: Links a Dynamic Forms agent to this exchange object by identifying the agent's object type.
- *Trigger on Object **: Restricts form definition determination by the corresponding actions.
- *qRFC Processing*: Enabling qRFC processing allows automatic form instance creation and attachment to the SAP object in the background (assuming a successful form definition determination).
- *Generate Requests with same object key*: When this is enabled, multiple qualifying changes to the same SAP object will trigger multiple form definition determination requests.

Results

After you finish the steps above, continue the configuration process with MAIF Configuration Guide - Dynamic Forms Agent Settings.

4.36.3 Identify Form Definitions for Client Download

This document describes the MAIF configuration steps to identify which Form Definitions to download to the SAP Service and Asset Manager client.

Context

If there is **at least one** Form Instance downloaded to the SAP Service and Asset Manager client, it will download the corresponding Form Definition. However, by default the client **will not download** any other Form Definitions.

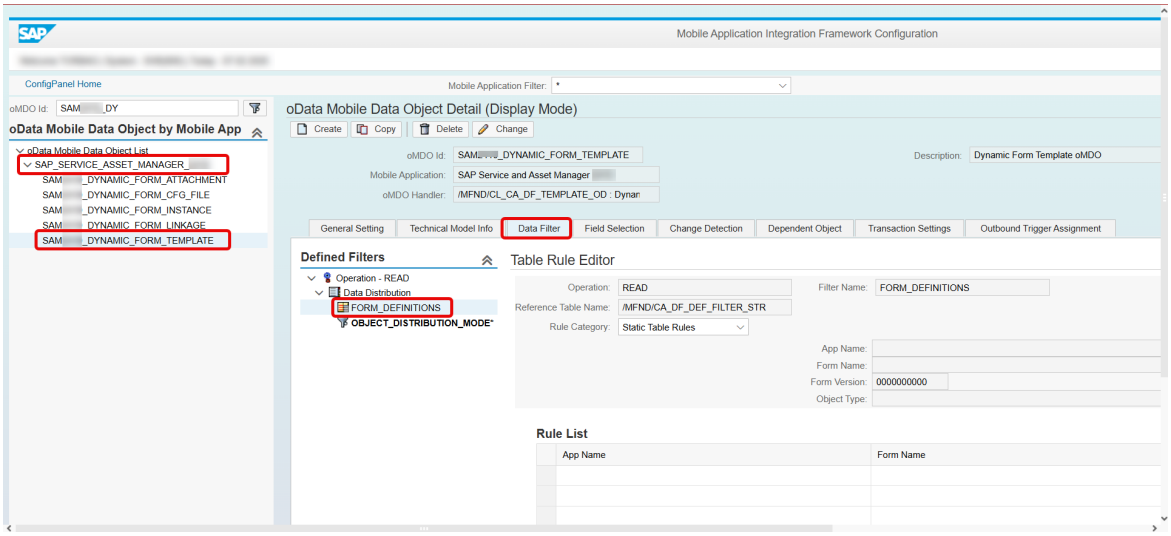
Follow the steps below to identify additional Form Definitions to download to the client. These definitions will be available for Form Instance creation on the client.

> ⓘ Note
>
> For more information about configuring SAP Dynamic Forms for SAP Service and Asset Manager, refer to SAP Dynamic Forms Configuration for SAP Service and Asset Manager in *SAP Service and Asset Manager Configuration Guide*.

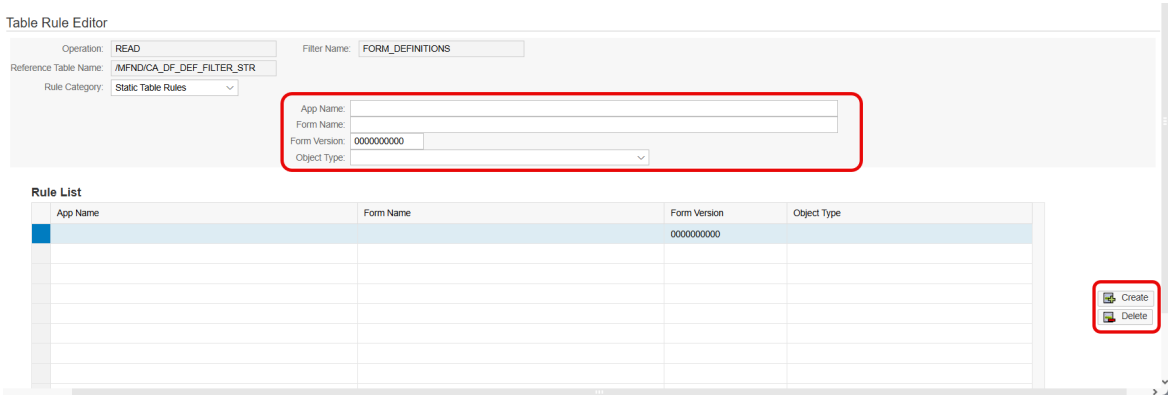
Procedure

1. In *SAP GUI*, execute the transaction code `/SYCLO/CONFIGPANEL`
2. Go to *oData Mobile Data Object Configuration*.
3. Select your application from the left, then the *SAMXXXX_DYNAMIC_FORM_TEMPLATE* oMDO.

4. Go to the *Data Filter* tab and select *FORM_DEFINITIONS*.



5. Enter *Change Mode* and add the Form Definition(s):
   - *App Name*
   - *Form Name*
   - *Form Version*
   - *Object Type* (for which the Form is relevant)



6. *Save* your changes.

4.36.4 Accessing Form Data from SAP Service and Asset Manager Metadata

In the metadata of SAP Service and Asset Manager, you can access and modify form data sent from SAP Dynamic Forms to the SAP Service and Asset Manager application. This enables you to create customized forms and assign them to SAP business objects used by the application.

SAP Service and Asset Manager provides an extension point [page 548] that allows you to intercept, inspect, and modify form data when a user *saves*, *completes*, or *reopens* a form. You can use this extension point to execute custom logic on the submitted data before it is stored.

> **Note**
>
> This customization requires modifying SAP Service and Asset Manager metadata source code. For accessing SAP Service and Asset Manager data within a form definition at design time, refer to Accessing SAP Service and Asset Manager Data Using Services and Actions in *SAP Dynamic Forms documentation*.

Procedure

1. Edit the file `/SAPAssetManager/Rules/Forms/SDF/SubmissionHandler.js`
   - This extension point is the submission handler rule file in the SAP Service and Asset Manager.
   - SAP Dynamic Forms calls this handler each time the user triggers a *save*, *complete*, or *reopen* action on a form instance within the SAP Service and Asset Manager application.
   - The handler receives the form data as submitted by the user. You can process this data and then return one of the following status values to control what happens next:

Return Value	Behavior
PROCESS_STATUS.OK	Continue saving the form data as normal. No modification.
PROCESS_STATUS.STOP	Do not save the form data, the submission is discarded.
PROCESS_STATUS.REPLACE_DATA	Save the form data, but use the supplied data property instead of the data that came from the form.

2. Create a form with the modified attributes. See Form Creation in *Form Builder Developer's Guide*.
3. Publish the form. See Publishing in *Form Builder Developer's Guide*.
4. Assign the form to an SAP business object. See Form Explorer User Guide.

Usa Cases

See the following customization examples:

- Scan submitted form values and trigger existing SAP Service and Asset Manager actions accordingly (for example, creating measurement documents or follow-on notifications and work orders).
- Run a GPS query at form save time and add location data to the form submission.
- Validate form data and prevent saving if specific conditions are not met.
- Replace the submitted form data with a modified version before it is stored.

Additional Links

See the following links for additional information and instructions regarding this topic:

- **SAP Service and Asset Manager documentation**:
  - SAP Dynamic Forms Configuration for SAP Service and Asset Manager
  - Metadata and customization:
    - Building and Branding the SAP Service and Asset Manager Application Client
    - Customizing Metadata Using the Mobile Development Kit
- **SAP Dynamic Forms documentation**:
  - Accessing SAP Service and Asset Manager Data Using Services and Actions
  - SAP Dynamic Forms product page

4.37 Signature Control Configuration

Use parameters to configure signature control.

Context

Use the *SIGN_CAPTURE* parameter group and the following parameters within the group to configure signature control for SAP Service and Asset Manager:

- OP.Complete: Enable for operations
- SubOp.Complete: Enable for suboperations
- WO.Complete: Enable for work orders

> ⚠ Restriction
>
> The digital signature feature is available in SAP S/4HANA 2020 and above releases. The digital signature feature is not available for SAP ERP systems or SAP S/4HANA systems lower than 2020.

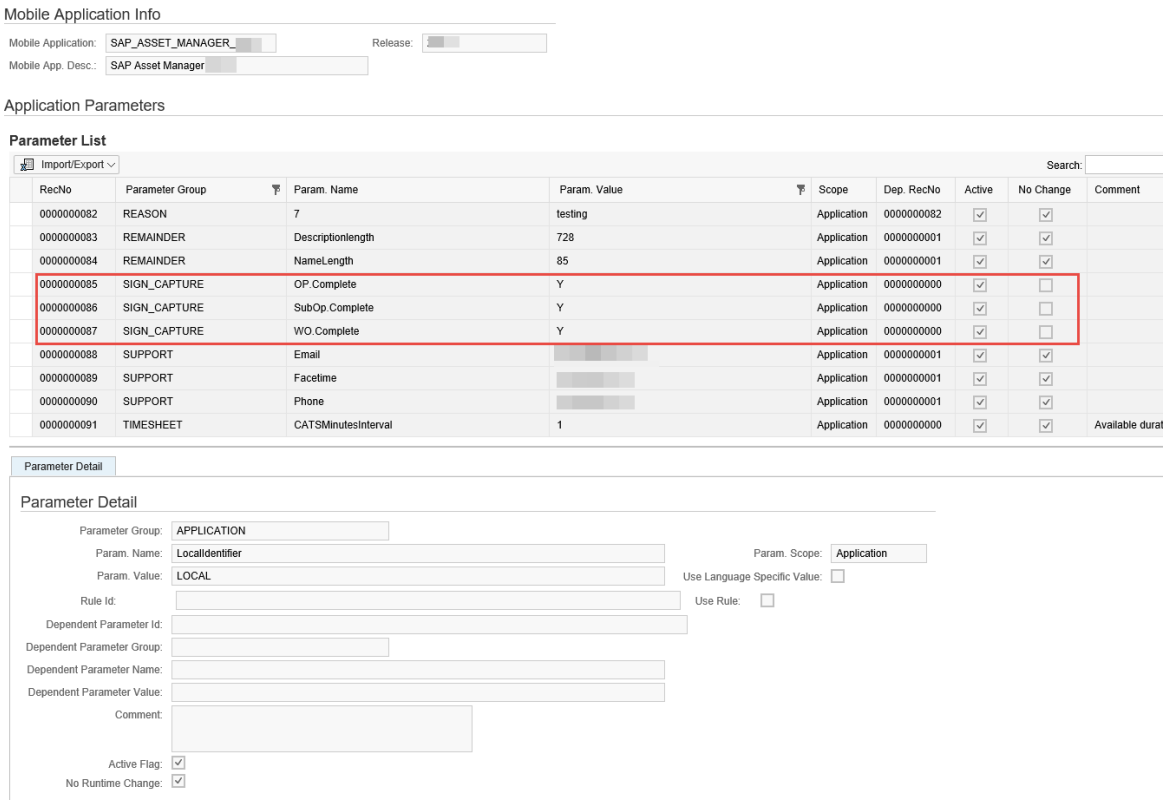
By default, the signature control feature is not enabled. To enable signature control:

Procedure

1. Using the ConfigPanel, navigate to *Mobile Application Configuration* > *Parameters tab*. In the left column, *Defined Mobile Applications*, select your application.

   The *Parameter List* populates with a list of all parameters available for the application.

2. The signature control parameters are found in the *SIGN_CAPTURE* group. You can scroll down to find the parameter, or perform a search using the *Search* box. Highlight the parameter you want to configure and click the *Change* button.



3. Make your desired parameter association changes. Enable the parameter as follows:

   - **Y:** Control is displayed on the client and is required before completing the object
   - **N:** Control is not displayed on the client (enabled by default)
   - **O:** Control is displayed on the client and is an optional step to complete the object

> ### Note
>
> If the parameters have no *Parameter Value* assigned, signature control does not display on the client.

4. Check the `<Active>` flag to ensure that the parameter is used by the mobile application. If desired, and if not already checked, check the `<No Runtime Change>` box to ensure that the value of the parameter is not overridden at runtime through synchronization processing.
5. *Save* your changes.

4.38 Supervisor Mode Configuration

Use the following procedures to configure the supervisor mode:

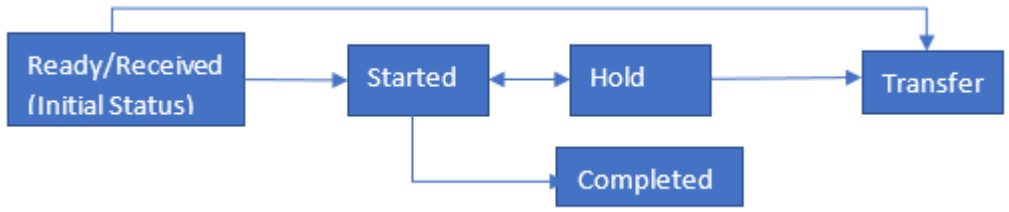
- Work Order Assignment Type Configuration [page 552]

- Supervisor Roles and Team Assignment Type Configuration [page 553]
- Enabling the Supervisor Approval Process for Work Orders [page 555]
- Mobile Application Parameter Settings for the Supervisor Mode [page 556]
- Mobile Application Status Settings for the Supervisor Mode [page 559]
- Rejection Reason Configuration [page 559]

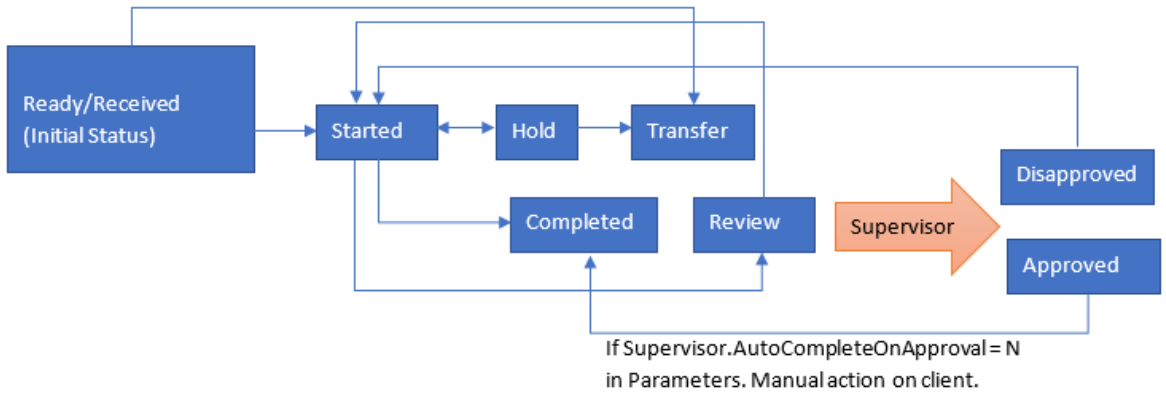
4.38.1 Work Order Operations State Machine for Maintenance Technician Persona

Technician Role:

- Supervisor Feature PM_SUPERVISOR_MODE Inactive



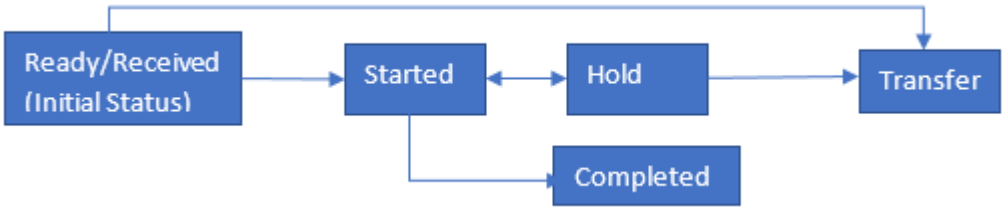
- Supervisor Feature PM_SUPERVISOR_MODE Active



> **Note**
>
> The supervisor approves or disapproves the operation once the technician puts it in review. This process is covered under the supervisor role.

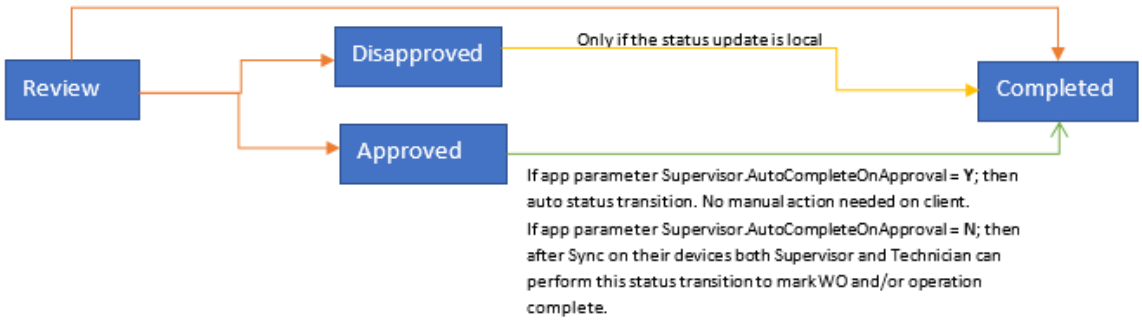
Supervisor Role:

- Supervisor Feature PM_SUPERVISOR_MODE Inactive



> **Note**
>
> As a supervisor, when you're logged in, you have access to these status transitions. This access remains available even if the PM_SUPERVISOR_MODE feature is inactive. However, it's unlikely that the supervisor configuration and authorizations in the backend would exist without the PM_SUPERVISOR_MODE feature being active.

- Supervisor Feature PM_SUPERVISOR_MODE Active



4.38.2 Work Order Assignment Type Configuration

Context

The following assignment types are supported when using the Supervisor mode:

- **Supported work order assignment types for the technician**
  - 1 - Header level person responsible
  - 2 - Operation/Task level personnel number
  - 6 - Operation/Task level work center
  - 8 - Header level work center
- **Supported work order assignment types for the supervisor**
  - 6 - Operation/Task level work center

- 8 - Header level work center

Configure the assignment types for the work order OData MDO as follows:

> **Note**
>
> One of the assignment types must be configured for the technician, while the other assignment type must be configured for the supervisor based on the supported work assignment types. Only the same level of assignment types is supported. In this, you can configure either header level assignments or operation level assignments, and not both.

Procedure

1. On the ConfigPanel home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. In the *OData Mobile Data Object List* select **SAMXXXX_WORK_ORDER_GENERIC**, and then the *Data Filter* tab.
3. Expand the *Defined Filters* list as follows; *Operation - READ* > *Data Distribution* > and click *WO_ASSIGNMENT_TYPE*. Click the *Change* button.
4. Set *Low Value* with the desired assignment type as defined by the assignment type model.
5. *Save* your changes.

> **Note**
>
> If you're configuring an operation level assignment type, you must update the *OPER_EXCL_SYST_STAT* filter with the *I0009 - CNF: Confirmed* value. However, remove the value if you're configuring a header level assignment type.

4.38.3 Supervisor Roles and Team Assignment Type Configuration

Configure the data filters to define the Supervisor role and Team Assignment types for the OMDO. Your specific configuration is based on how the supervisor team is maintained in the back end.

For detailed instructions on how to work with data filters, see the Working with oData MDO Filter Rules [page 146] and Changing oData MDO Filter Rules [page 146] topics.

You're configuring the data filters found in the **SAMXXXX_USER_ROLE** OMDO.

In addition to configuring the data filters found in the **SAMXXXX_USER_ROLE** OMDO, you must manually maintain the team assignments for each user in the Mobile Administration and Monitoring Portal. Information on configuring user parameters is found at the following locations:

- **Mobile Add-On for SAP S/4HANA Security Guide**
  - Defining an Additional User Role Required for a Mobile Application User

    - Defining an Additional User Role Required for an OData Mobile Object Handler
- **SAP Mobile Add-On Security Guide**
    - Defining an Additional User Role Required for a Mobile Application User
    - Defining an Additional User Role Required for an OData Mobile Object Handler

ASSIGNMENT_TYPE Data Filter

The following team assignment types are supported for downloading the supervisor team:

- **1 - Work Center Assignment:** Use when the team (technicians and supervisors) is maintained in the back end through the Work Center Maintenance transaction (CR02/CR03)
- **2 - Organizational Structure Assignment:** Use when the team is maintained in the back end through the Org. Structure Assignment (PPOMA transaction).
- **3 - User Attribute Assignment:** Use when the team isn't maintained in the back end through either the Work Center Maintenance or the Org. Structure Assignment transactions. Additional configuration and manual team assignments are needed.
- **4 - Custom Assignment:** Use by the customer to define custom logic for downloading the teams. Customer logic is implemented in the BADI method `/MERP/CA_OMDO_USER_ROLE_BADI - GET_ASSIGNMENT_OTHERS`.

POSITION_ROLE_TYPE Data Filter

The position role type filter defines the Position Org ID for the supervisor, and is maintained as part of the team configuration in the back end. The definition is needed to identify the mobile user with the Supervisor role. It's also needed for Team Assignment types 1 and 2.

WORKCENTER_ROLE_TYPE Data Filter

The work center role type filter is used for Team Assignment type 3. When using Team Assignment type 3, create a new filter rule with the following properties:

- Rule Type: Non-Static Table Rules
- Non-Static Table Rules: Mobile User Attribute
- User Attribute: WORKCENTER_ROLETYPE
- Active: Checked

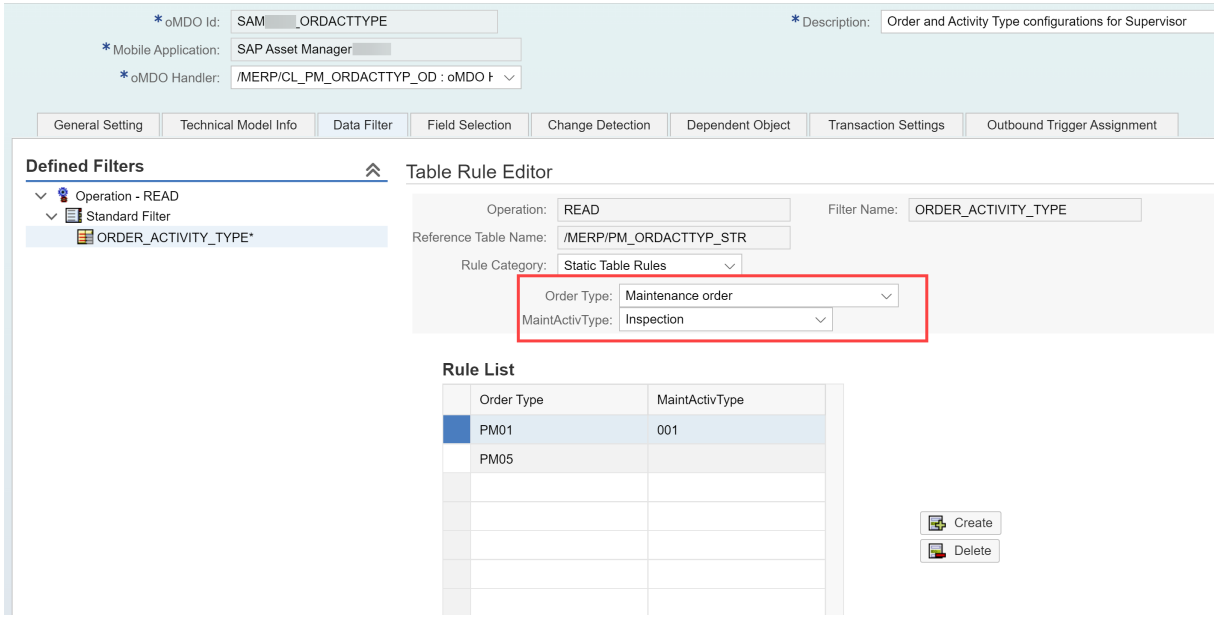
4.38.4 Enabling the Supervisor Approval Process for Work Orders

Configure the data filters to define the Supervisor role and Team Assignment types for the OMDO. Your specific configuration is based on how the supervisor team is maintained in the back end.

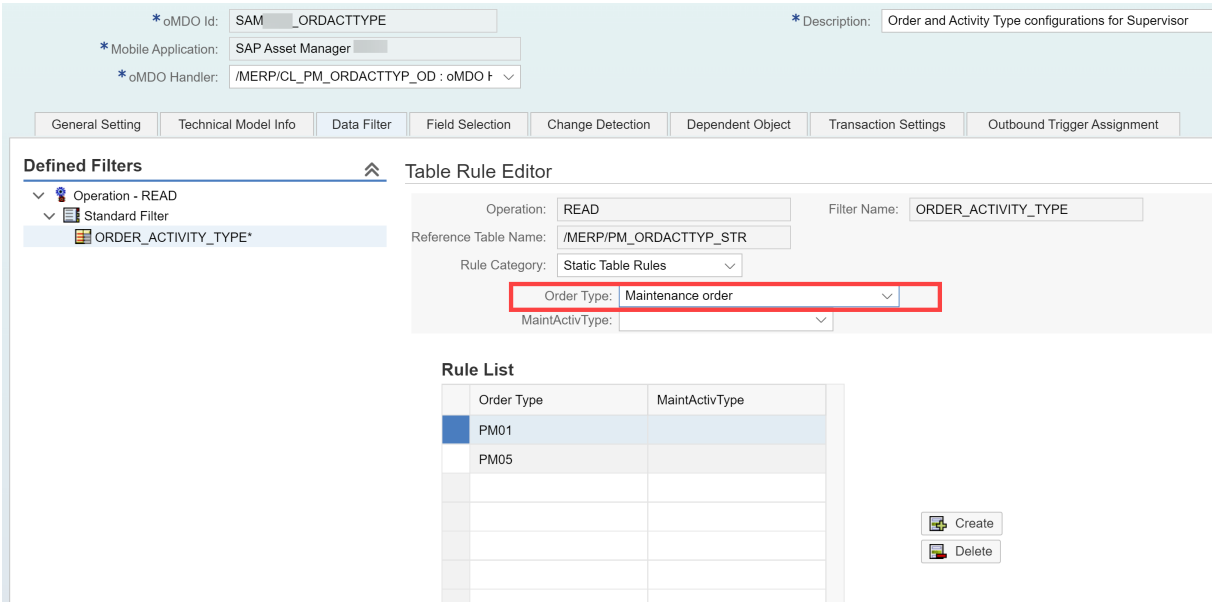
For detailed instructions on how to work with data filters, see the Working with oData MDO Filter Rules [page 146] and Changing oData MDO Filter Rules [page 146] topics.

You're configuring the *ORDER_ACTIVITY_TYPE* data filter found in the **SAMXXXX_ORDACTTYPE** OMDO.

If `<Order Type>` and `<MaintActiv Type>` fields are specified, the supervisor approval functionality is enabled for the combination:



If only `<Order Type>` is specified, the supervisor approval functionality is enabled for all orders of that type:



4.38.5 Mobile Application Parameter Settings for the Supervisor Mode

Context

> **Note**
>
> As of the SAP Service and Asset Manager 2205 release, enable and disable parameters are no longer available through the *Parameters* tab. You enable or disable all features through the *Features* tab. See the Configuring Features [page 93] procedure for details.

> **Note**
>
> As of the SAP Service and Asset Manager 2305 release, SAP introduces a new parameter for the supervisor that allows you to enable auto completion on approval. See the configuration procedure below.

The Supervisor feature is called *PM_SUPERVISOR_MODE*. By default, the feature is not enabled.

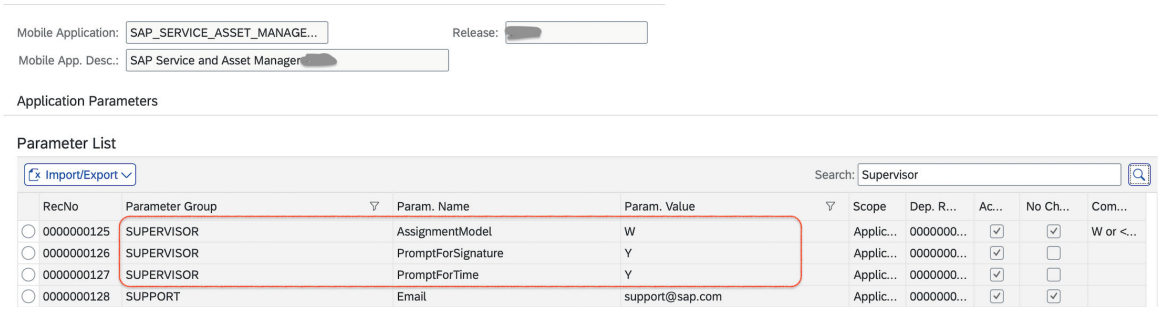
To configure the supervisor options for SAP Service and Asset Manager, use the *SUPERVISOR* parameter group and the following parameters within the group:

Procedure

1. Using the ConfigPanel, navigate to *Mobile Application Configuration* > *Parameters tab*. In the left column, *Defined Mobile Applications*, select your application.

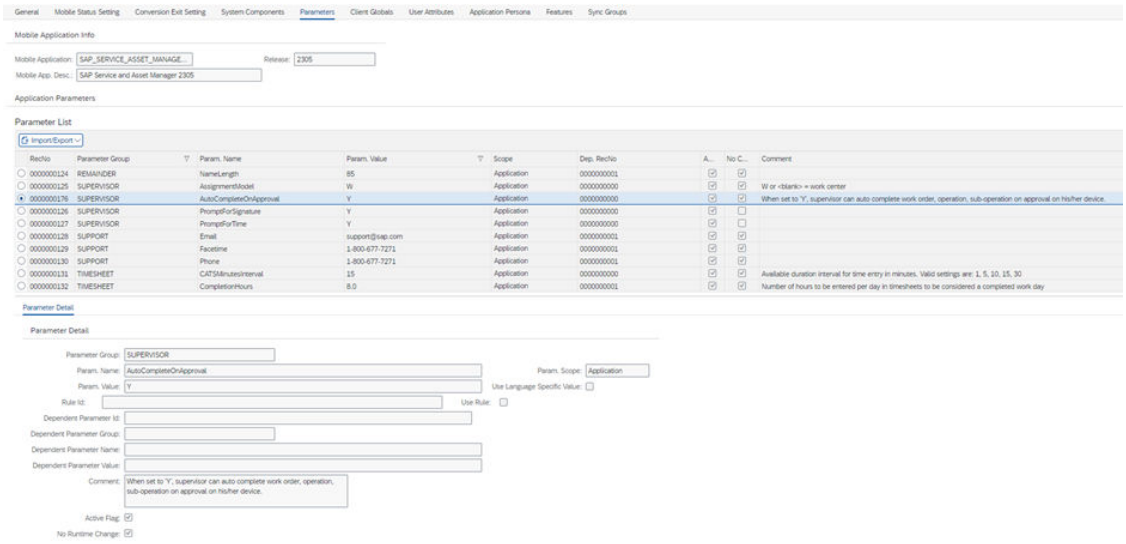
   The *Parameter List* populates with a list of all parameters for the application.

2. The supervisor parameters are found in the *SUPERVISOR* group. You can scroll down to find the parameter, or perform a search using the *Search* box. Highlight the parameter you want to configure and click the *Change* button.



3. Make desired parameter changes as follows:
   a. **AssignmentModel:** Set according to how your team is maintained and based on your team assignment type configuration:
      - For team assignment types *1* or *3*, set the value to *W* or *<blank>*.
      - For team assignment type *2*, set the value to *O*.
   b. **PromptForSignature:** Set the parameter to *Y* if signature capability is needed for supervisor approval.
   c. **PromptForTime:** Set the parameter to *Y* if time capture is needed when the supervisor is executing the approval process.
   d. **AutoCompleteOnArppoval**:

- If set to *Y*, the supervisor can automatically complete a work order, operation, or sub-operation after approval on his device.
- If set to *N*, the supervisor can only set the work order, operation, or sub-operation to the *Approved* status.
  After synchronization on their devices, both the assigned technician and supervisor can set the status to *Completed* by manually changing the status on the device.



4. Locate the parameter group *USER_AUTHORIZATIONS*. The parameter *SupervisorRole* is optional and is blank by default. You can configure it in one of the following ways:

> **Note**
>
> If the *Parameter Value* field and the *Rule ID* fields are blank, and if no data filter rule is created, the authorization model is not used. The *UserRoles* entity set is then used to determine the authorization role.

   - Set the *Parameter Value* field:
     - <blank>: The parameter is ignored
     - Y: Supervisor. If set, the current user has the role of Supervisor and the UserRoles entity set is ignored.
     - N: Technician. If set, the current user has the role of Technician and the UserRoles entity set is ignored.
   - Use the authorization check rule */SMFND/CL_CORE_AUTH_CHECK_RU* and corresponding authorization object to check if the user is a supervisor. If the parameter is enabled, it determines if the logged-in user is a supervisor or not in the application. Be sure to check the *Use Rule* box if you're using an authorization check rule.
   - Use the position org ID defined in the *POSITION_ROLE_TYPE* data filter rule in the **SAMXXXX_USER_ROLE** OMDO. By default, the data filter rule is blank. See Supervisor Roles and Team Assignment Type Configuration [page 553] for information on creating a position role type data filter rule.
5. *Save* your changes.
6. Use the SAP GUI transaction *SU3* to assign parameters depending on assignment types:
   a. **VAP:** Main work center for maintenance tasks. Assign the work center of the user to this parameter when using team assignment type *1* or *3*.
   b. **/MERP/SUPVR_ORGID:** Configure this parameter when using team assignment *2* as follows:
      - For a supervisor, configure with the org ID of the supervisor.
      - For a technician, configure with the org ID of the supervisor, which typically is the same as the org ID of the technician.

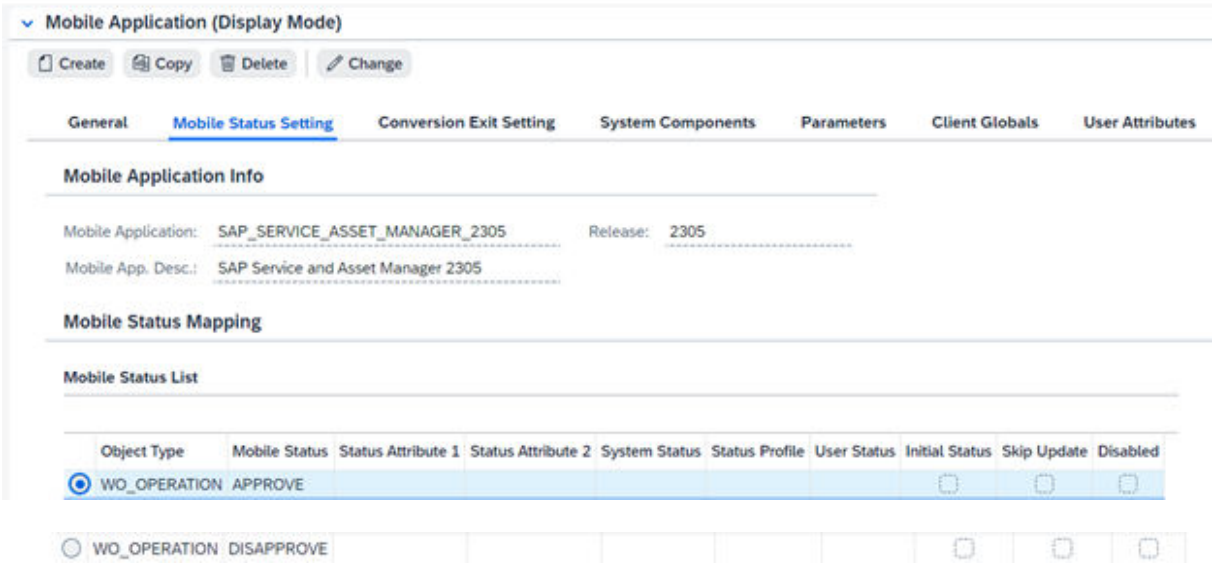
4.38.6 Mobile Application Status Settings for the Supervisor Mode

> **Note**
>
> By default status settings for the supervisor mode aren't mapped to any back-end user or system status. For an example of how to configure a mapping status, see the Changing the Mapping of a Mobile Status to STARTED [page 134] procedure.

The following statuses to support the supervisor functionality are available at the work order and operation levels, depending on your configuration of the work order assignment type:

- **REVIEW:** Set by the technician after they've completed their work. The supervisor is then required to review the work.
- **APPROVE** and **DISAPPROVE**

  > **Note**
  >
  > **ACCEPTED** and **REJECTED:** Set by the field service technician if he is rejecting the work done on the work order or operation.



When a supervisor approves a work order or an operation, the status moves to COMPLETED.

4.38.7 Rejection Reason Configuration

The supervisor can reject an order or operation as part of the review process. If an order or operation is rejected, the supervisor must specify a rejection reason.

Configure the rejection reasons in the **SAM2205_REJECTION_REASON** OMDO, using the *REJECTION_REASON* data filter.

For information on how to work with data filters, see the Changing oData MDO Filter Rules [page 146] topic.

4.39 Vehicle Stock Look Up Configuration

The Vehicle Stock component in SAP Service and Asset Manager offers inventory functionality to track stock items stored in vehicles, like work trucks or vans. Vehicle stock capabilities include:

- Helping operators to manage stock items stored in vehicles for daily work.
- Storage location assigned to the technician is displayed on the app.
- Ability to transfer stock to and from the set storage location.
- Look up stock for the set storage location.
- Perform a physical inventory or cycle count for the set storage location.
- Replenish stock through purchase requisitions.
- Tracking tools and other items kept in the vehicles.

> **Note**
>
> - For more information about how to use this feature, see Working with Stock Look Up.
> - From SAP Service and Asset Manager **2505 version**, the Vehicle Stock feture is supported by the Field Service Technician persona on the SAP S/4HANA back end system.

Supported Personas

In the system, the *MM_VEHICLE_STOCK* feature is relevant for the following personas:

Maintenance Technician (Pro)
Field Service Technician (Standard)
Field Service Technician (Pro)
Field Service Technician (External)

In the system, the *MM_STOCK_LOOKUP* feature is relevant for the following personas:

Maintenance Technician (Pro)
Field Service Technician (Standard)
Field Service Technician (Pro)
Field Service Technician (External)
Inventory Clerk

Prerequisites

You need to maintain the *WRK/LAG* and/or *USER_TRUNK* user parameter values.

Limitations

In the case of configuring (multiple) *Plant* and *Storage Location* parameters:

- For the Vehicle Stock [page 560] feature, a *Plant* and *Storage Location* is used to identify the vehicle. Therefore, if you have multiple values, the feature **will not work**.

> → Tip
>
> For more information, see Recommended Configuration for Multiple Plants and Work Centers [page 111].

Configuration

Perform the following configuration step(s):

1. Configuring Vehicle Stock Look Up - Back End - Enabling the Feature [page 561]
2. Configuring Vehicle Stock Look Up - Back End - OMDO Filters [page 562]

4.39.1 Configuring Vehicle Stock Look Up - Back End - Enabling the Feature

Context

For general information about configuring Vehicle Stock Look Up, see the Vehicle Stock Look Up Configuration overview topic.

The below procedure describes how to enable the feature in the Configuration Panel.

General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- Mobile user attributes configuration: refer to the Configuring Mobile User Attributes topic in the Configuration guide.
- User management configuration: refer to the Administration - User Management topic in the Add-On Administrator guide.
- **Enabling and disabling features**: refer to Configuring Features in *MAIF Configuration Guide*.
- **Mobile Application Parameters** configuration: refer to Parameters Tab in *MAIF Configuration Guide*.

Procedure

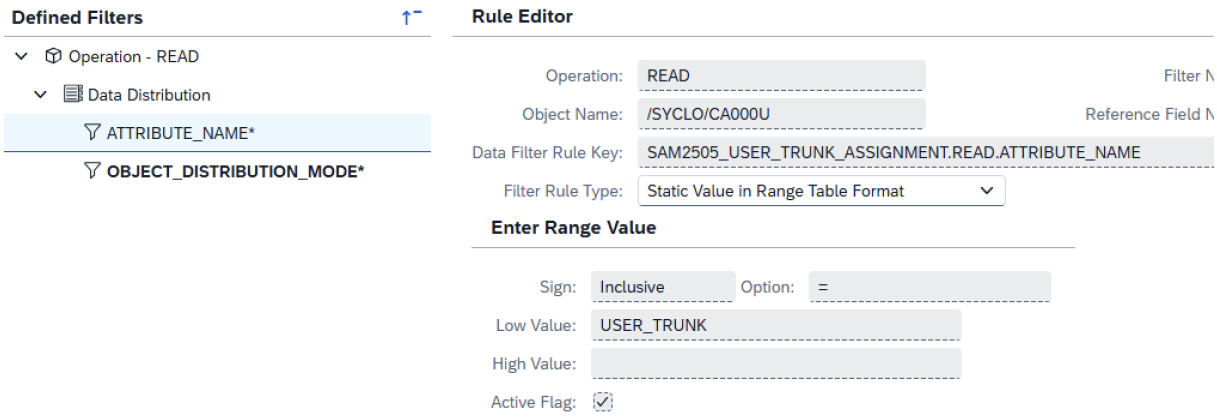
1. On the Configuration Panel, go to **Component Assignments** and select your application from the list.
2. In the **App. Feature Id** drop-down, select **Stock Look Up**.
3. Enter **Change mode** and set the feature to **Active** for the persona(s) you want to enable it.

4.39.2 Configuring Vehicle Stock Look Up - Back End - OMDO Filters

Context

For general information about configuring Vehicle Stock Look Up, see the Vehicle Stock Look Up Configuration overview topic.

The oMDO -> SAMXXX_USER_TRUNK_ASSIGNMENT feature, with MERP/CL_MM_USER_TRUNK_OD as its handler, downloads values for mobile user attributes configured in the filter. There are two filters for the oMDO, pre-configured in the BC set, as shown in the image.



General Links

Configuring the mobile user attribute value is a generic process applicable to several oMDOs. Follow the instructions in the configuration guide to set up the mobile user attribute value:

- **Mobile user attributes configuration**: refer to the Configuring Mobile User Attributes topic in the Configuration guide.
- **User management** configuration: refer to the Administration - User Management topic in the Add-On Administrator guide.

4.40 Work Approval Configuration

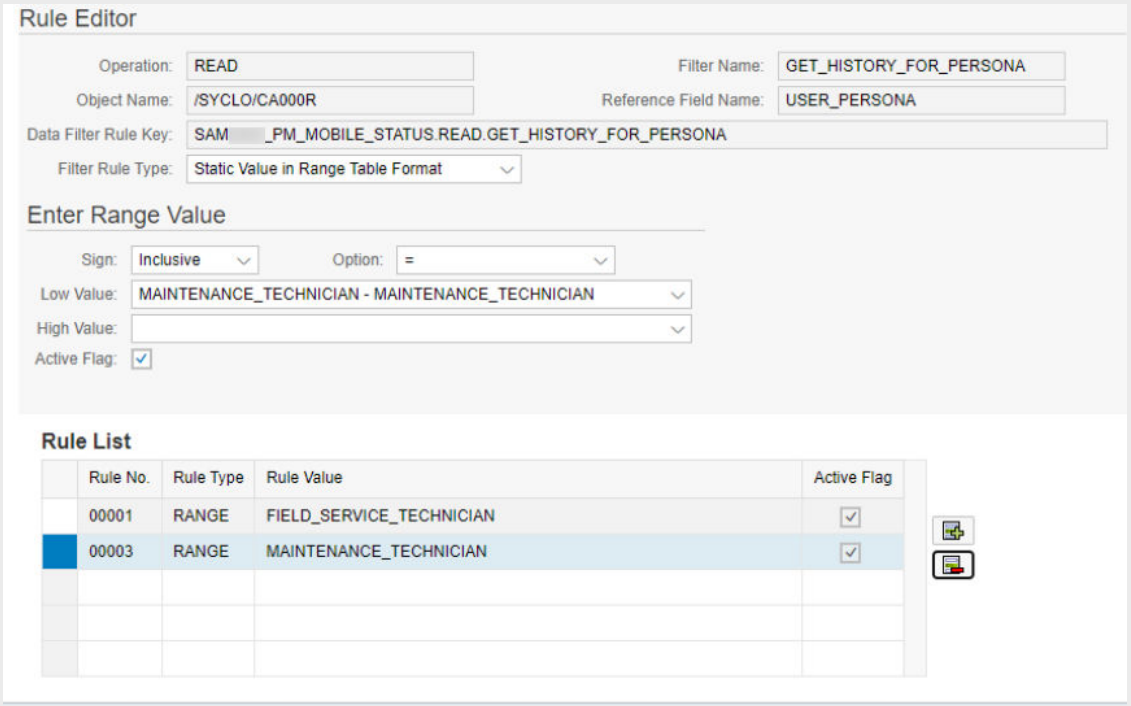
A Work Approval is used to control the work execution. Work Approvals ask for measures to ensure a safe environment for working on a technical system. In doing so, approvals are used to define certain rules or requirements that must be followed.

> **Note**
>
> - For more information about using Work Approvals, see Work Approval Detail Screen.
> - Please note that Work Approvals are enabled by default, if you have already configured Work Permits [page 565]. The configuration steps below [page 564] only apply in case you want to **hide** Work Approvals for the Technician.

Supported Personas

This feature is applicable for the following personas:

Maintenance Technician (Pro)
Safety Technician

> **Note**
>
> - For the Maintenance Technician (Pro) persona, this feature is only available from 2410 version.
> - If the user uses Safety Technician (WCM) features via the Maintenance Technician (Pro) persona, you need to add the persona to the data filter *SAMXXXX_PM_MOBILE_STATUS* > *GET_HISTORY_FOR_PERSONA*:
>
> 
>

Limitations

Work Approval is **only** available in the **enhanced** model structure.

> ⓘ Note
>
> For more information about standard and enhanced models, refer to Work Clearance Management (PM-WCM) in *SAP ERP* documentation.

Prerequisites

Work Approvals are available only, if you have previously configured Work Permits [page 565].

Configuration

Perform the following configuration to **hide/show** Work Approvals for the Technician:

1. Configuring Work Approvals - Back End - Mobile Application Parameters [page 564]

4.40.1 Configuring Work Approvals - Back End - Mobile Application Parameters

Context

For detailed information about Work Approvals, see the overview topic, Work Approval Configuration [page 563].

The below procedure describes how to hide or display Work Approvals for Technicians by configuring the Mobile Application Parameters in the Configuration Panel.

> ⓘ Note
>
> Work Approvals will be **displayed by default**, once the Work Permit feature is configured [page 565].

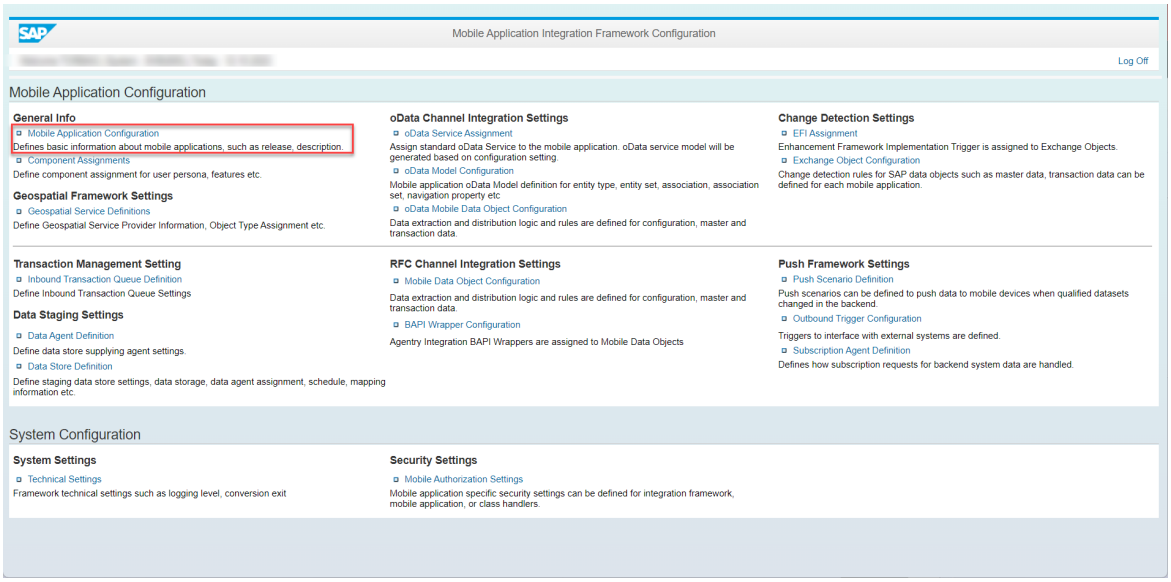
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

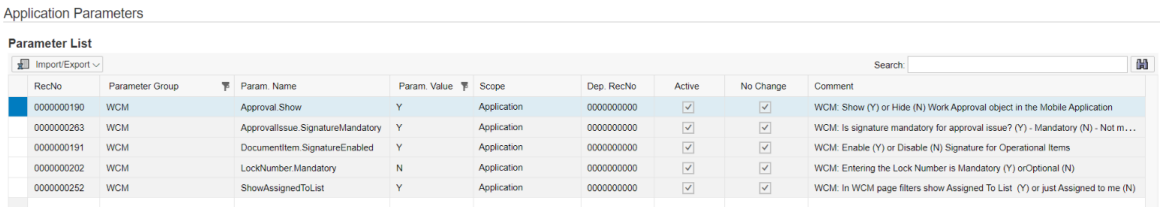
- **Mobile Application Parameters** configuration: refer to Parameters Tab in *MAIF Configuration Guide*.

Procedure

1. On the *Configuration Panel*, go to *Mobile Application Configuration*.



2. On the left, select your application from the list, and go to the *Parameters* tab.
3. Under *Parameter List*, you can search or filter the list of parameters related to the Safety Technician persona (filter the *Parameter Group* to *WCM*).



4. Enter *Change Mode* and disable or enable the `Approval.Show` parameter, depending on you want to hide or display Work Approvals in the application.

> **Note**
>
> For more information about Mobile Application Parameters relevant for the Safety Technician persona, see Mobile Application Parameters - Safety Technician Persona [page 220].

5. Save your changes.

4.41 Work Permit Configuration

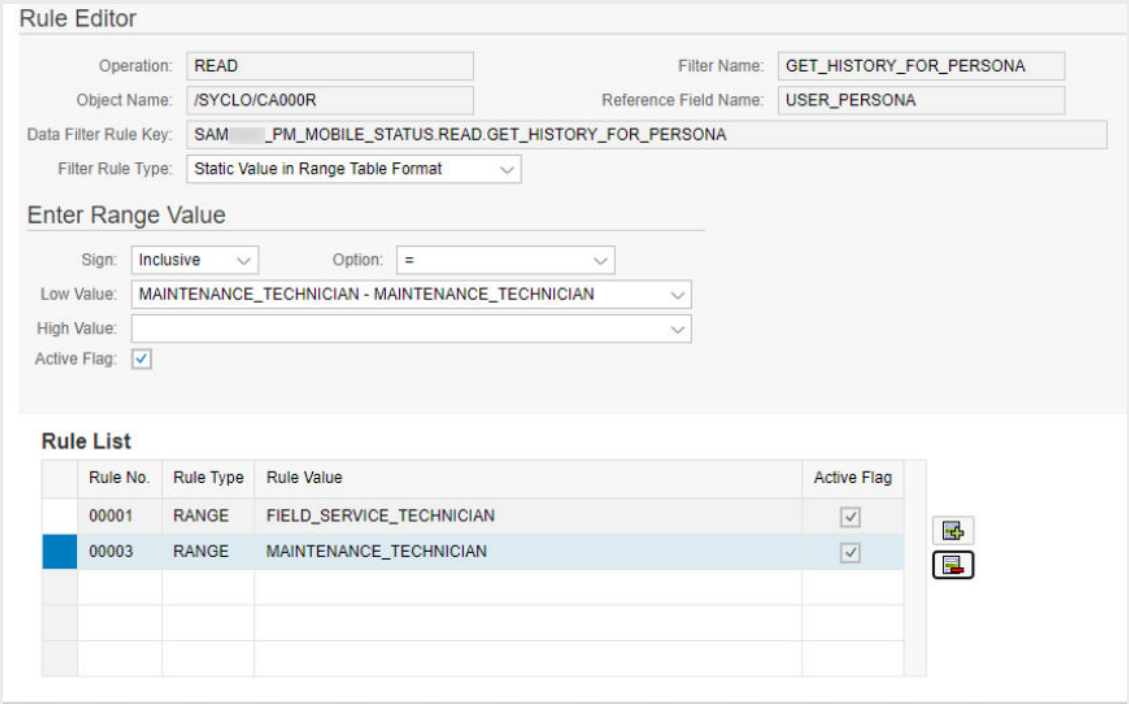
A (Work Clearance) Work Permit is approved by one or more Supervisors and is visible for the Safety Technician persona. After the Safety Technician persona has done his safety work by implementing and maintaining lockout and tagout procedures for energy source isolation, the Work Permit can be released, and the Maintenance Technician persona can do the work assigned to him.

> **Note**
>
> - For more information about how to use Work Permits, see Work Permit Detail Screen.
> - For more information about how to configure and issue Work Permit Approvals, see Work Permit Approvals Configuration [page 569] and Issuing Work Permit Approvals.
> - The configuration of Assignment Management [page 261] affects the configurations of **WCM Work Order**, **Isolation Certificate** and **Work Permit**.

Supported Personas

This feature is applicable for the following personas:

Maintenance Technician (Pro)
Safety Technician

> **Note**
>
> - For the Maintenance Technician (Pro) persona, this feature is only available from 2410 version.
> - If the user uses Safety Technician (WCM) features via the Maintenance Technician (Pro) persona, you need to add the persona to the data filter *SAMXXXX_PM_MOBILE_STATUS* > *GET_HISTORY_FOR_PERSONA*:
>
> 
>

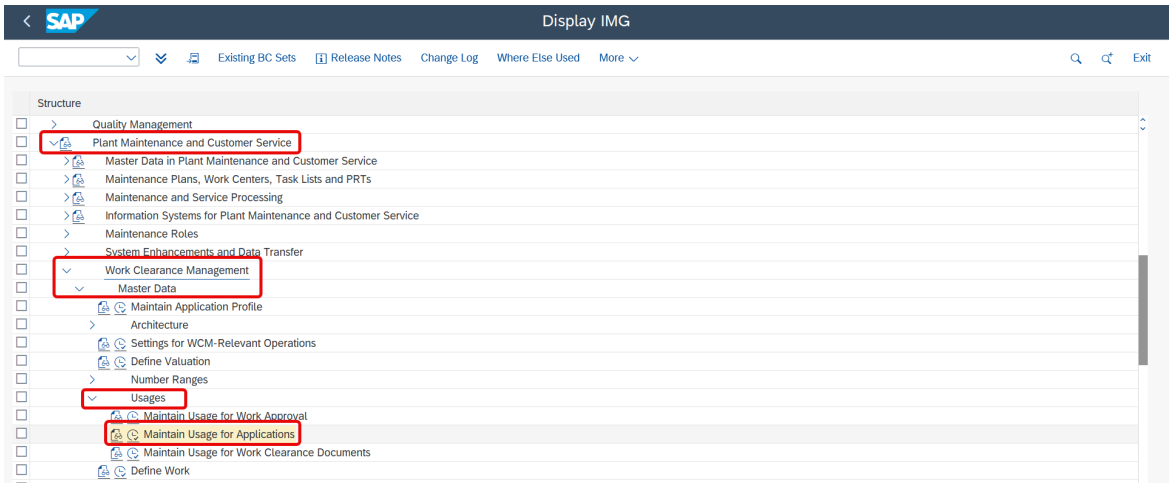
Limitations

See Configuration Prerequisites and Limitations - Safety Technician Persona [page 216].

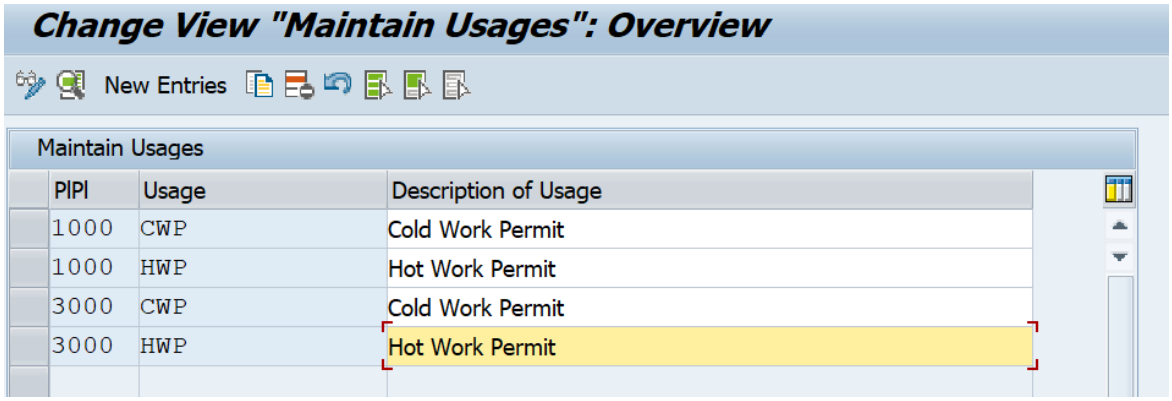
Prerequisites

Before going through the configuration steps below [page 568], you need to perform the the following **SPRO** changes:

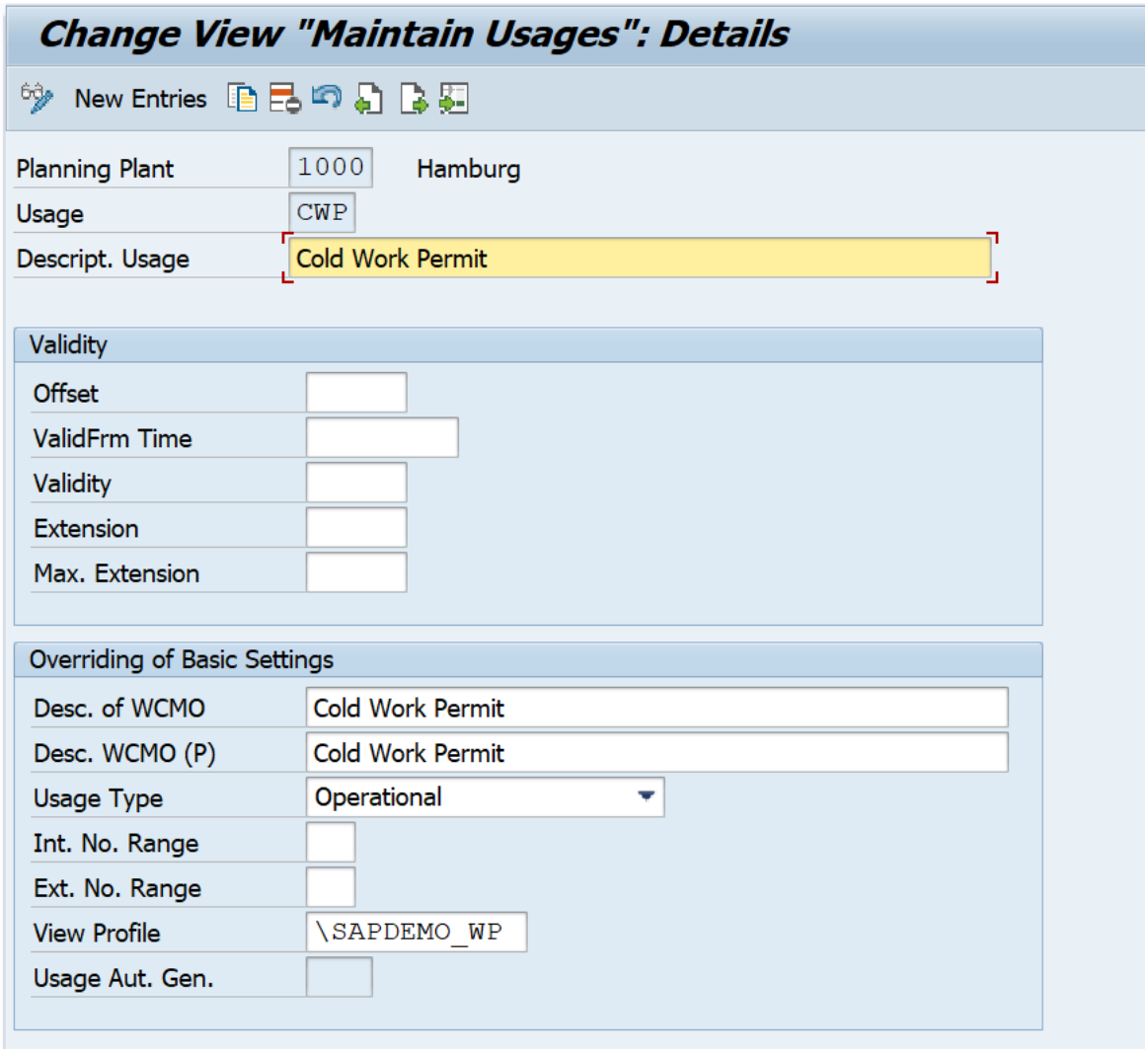
1. In *SAP GUI* use the transaction code *SPRO* and click *SAP Reference IMG*.
2. Navigate to *Plaint Maintenance and Customer Service* > *Work Clearance Management* > *Master Data* > *Usages* > *Maintain Usage for Applications* .



3. Select a *Planning Plant* from the list.



4. Maintain the Usage Type details according to your preference.



> **Note**
>
> For more information about Usage Types for Isolation Safety Certificates, see Supported Usage Types - Safety Technician Persona [page 226].

Configuration

Perform the following configuration procedure(s):

1. Configuring Work Permits - Back End - Enabling the Feature [page 569]
2. Configure Mobile Application Parameters as described in Mobile Application Parameters - Safety Technician Persona [page 220].
3. Configure oMDO filters as described in General oMDO Configuration - Safety Technician Persona [page 221].
4. Configure Exchange objects as described in General Exchange Configuration - Safety Technician Persona [page 224].

5. Configure User Parameters as described in General User Parameters Configuration - Safety Technician Persona [page 227].

4.41.1 Configuring Work Permits - Back End - Enabling the Feature

Context

For detailed information about Work Permits, see the overview topic, Work Permit Configuration [page 565].

The below procedure describes how to enable the feature in the Configuration Panel.

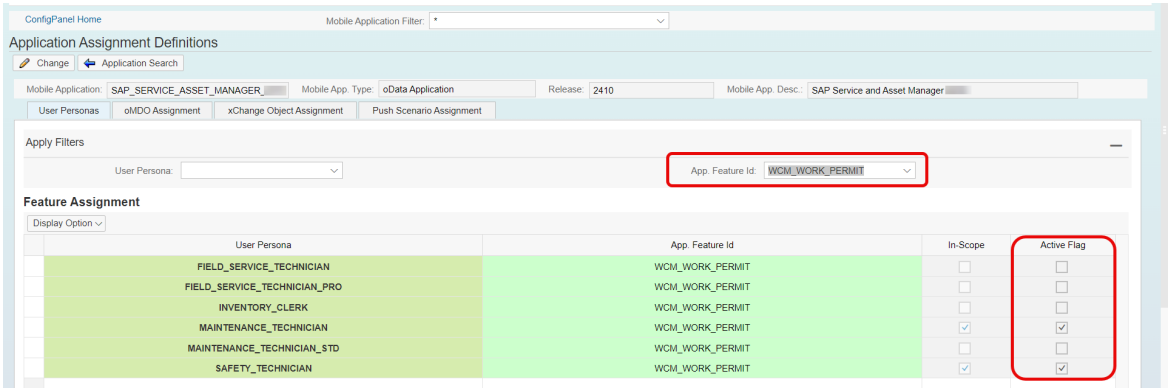
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **Enabling and disabling features**: refer to Configuring Features and Component Assignments in *MAIF Configuration Guide*.

Procedure

1. On the Configuration Panel, go to *Component Assignments* and select your application from the list.
2. In the *App. Feature Id* dropdown, select *WCM_WORK_PERMIT*.
3. Enter *Change mode* and set the feature to *Active* for the personas you want to enable it.



4.42 Work Permit Approvals Configuration

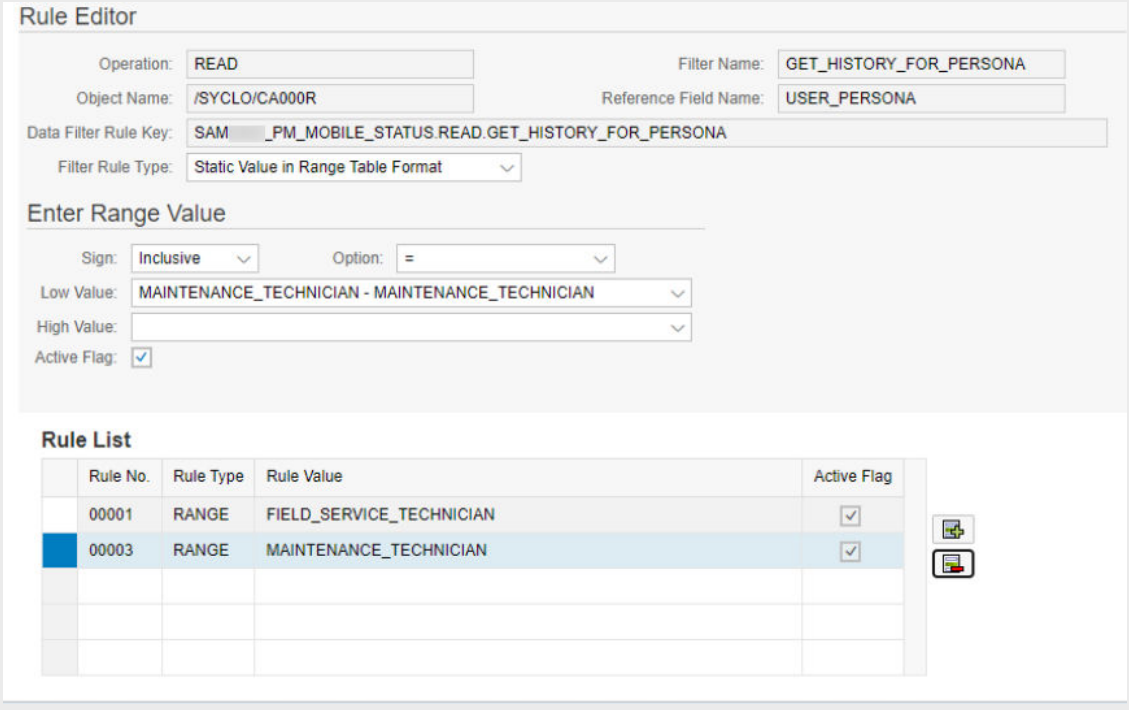
Safety Technicians can issue approvals on the details screen of a selected Work Permit.

> **Note**
>
> For more information about using the Work Permit Approvals feature, see:
>
> - Issuing Work Permit Approvals (Safety Technician User Guide)
> - Working with Safety Technician Objects (Maintenance Technician User Guide)

Supported Personas

This feature is applicable for the following personas:

Maintenance Technician (Pro)
Safety Technician

> **Note**
>
> - For the Maintenance Technician (Pro) persona, this feature is only available from 2410 version.
> - If the user uses Safety Technician (WCM) features via the Maintenance Technician (Pro) persona, you need to add the persona to the data filter *SAMXXXX_PM_MOBILE_STATUS* > *GET_HISTORY_FOR_PERSONA*:
>
> 
>

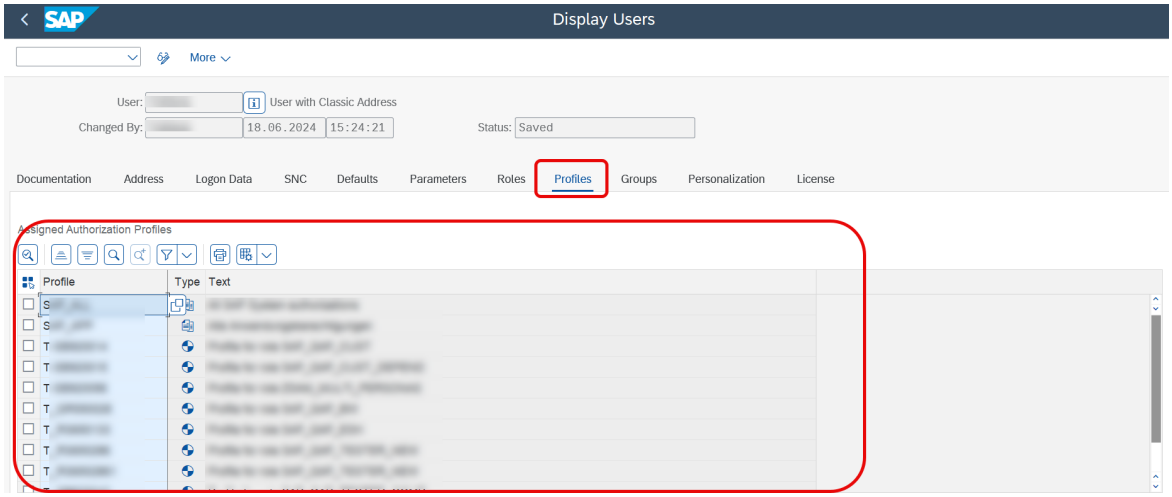
Limitations

See Configuration Prerequisites and Limitations - Safety Technician Persona [page 216].

Prerequisites

Before performing configuration steps described in Configuring Work Permit Approvals - Back End - SAP GUI [page 571], you need to identify, which of the user's profile contains the object *I_SOGEN*. To do that, perform the following:

1. In *SAP GUI*, go to transaction code `SU01`.
2. Enter the *USER* and click *Display*.
3. Under the *Profiles* tab, go through the profiles, and note the one for later use that contains the *I_SOGEN* object.



Configuration

Perform the following configuration step(s):

1. Configuring Work Permit Approvals - Back End - SAP GUI [page 571]
2. Configuring Work Permit Approvals - Back End - Mobile Application Parameters [page 574]: This is an **optional** configuration, if you want to enable for the Safety Technician to confirm the Work Permit Approval by adding a signature.

4.42.1 Configuring Work Permit Approvals - Back End - SAP GUI

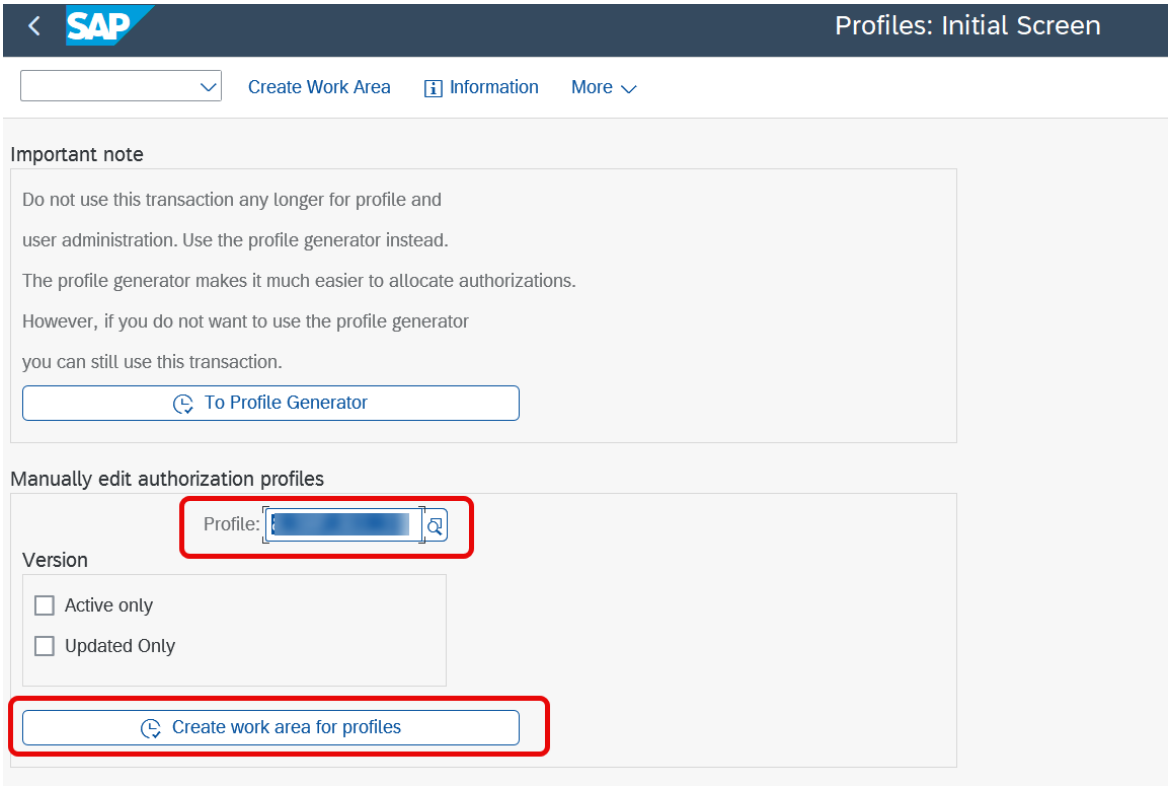
Context

For detailed information about Work Permit Approvals, see the overview topic, Work Permit Approvals Configuration [page 569].

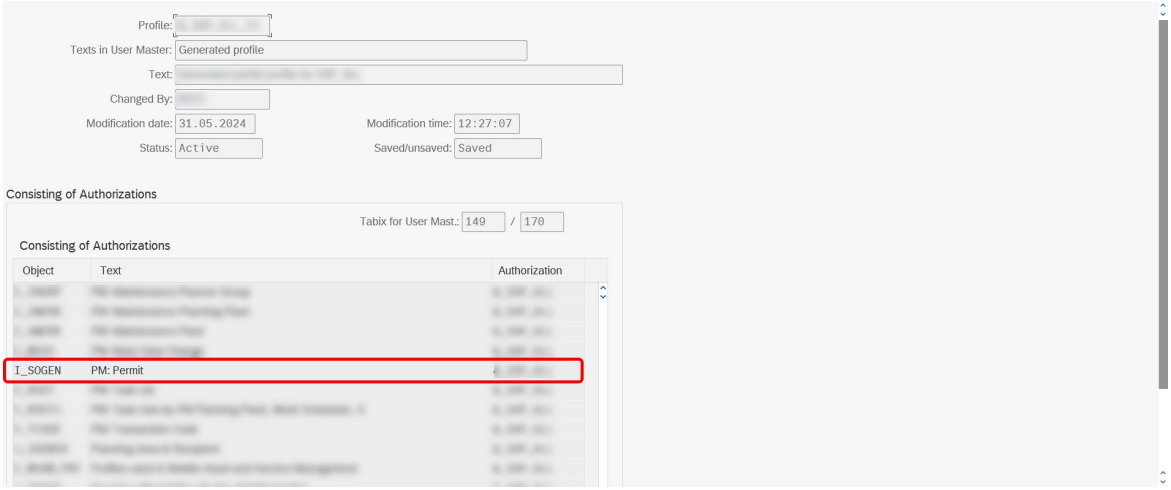
The following procedure describes how to configure the *I_SOGEN* object for users in *SAP GUI*, so that they will have the right authorization to issue Work Permit Approvals.

Procedure

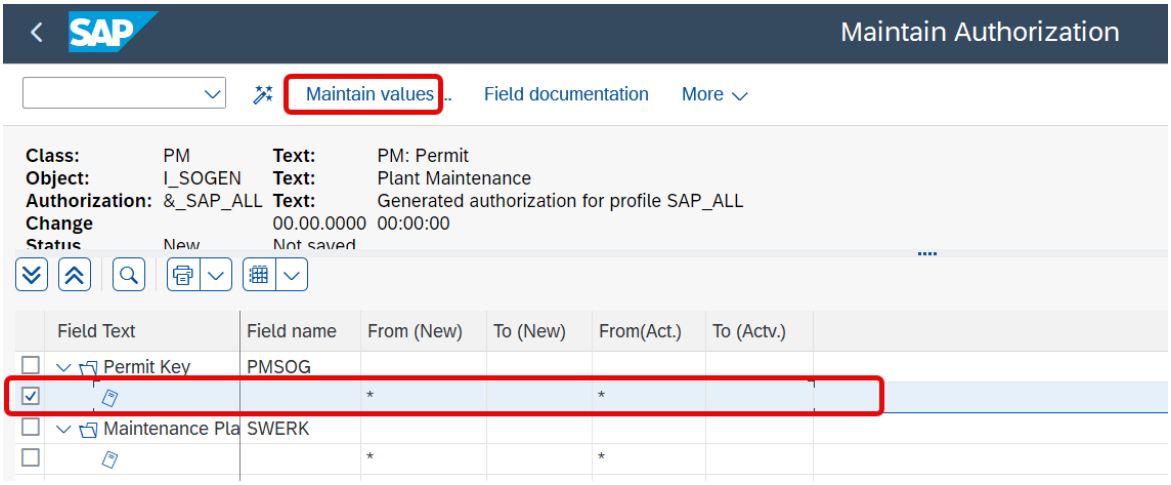
1. In the *SAP GUI*, navigate to the `SU02` transaction.
2. Enter the *Profile* that you have already noted in Prerequisites [page 571] section and click *Create work area for profiles*.



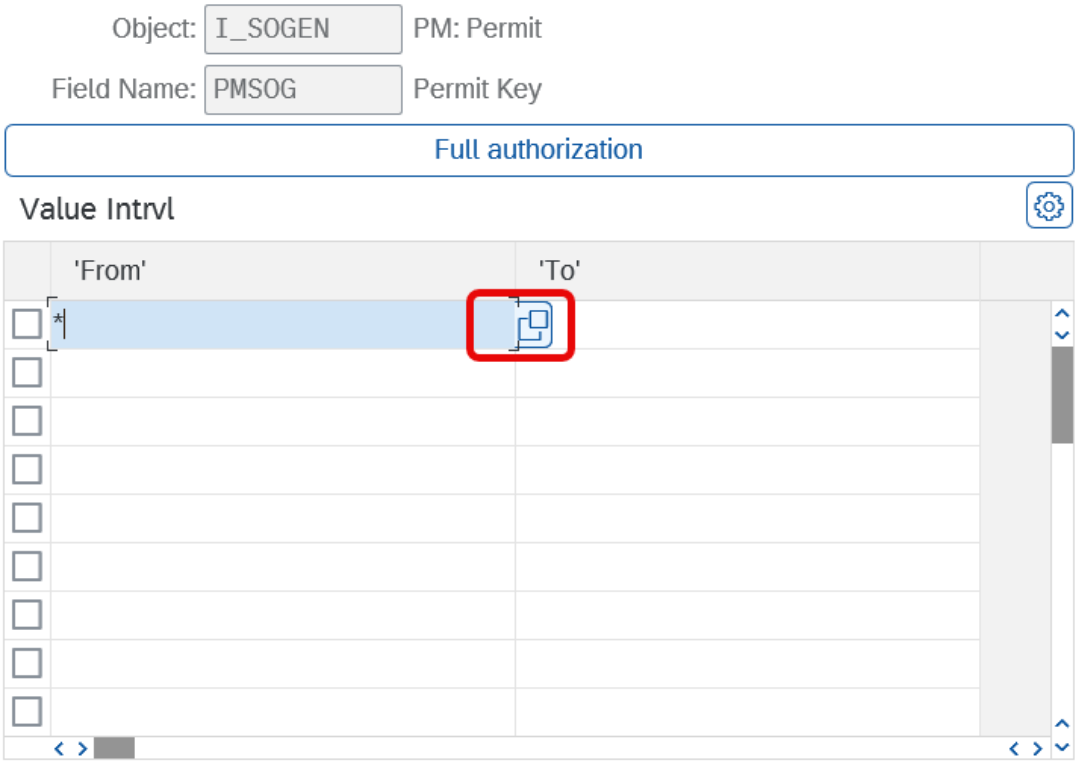
3. Click *Edit Profile* and open *I_SOGEN* from the list of objects.



4. In the *Maintain Authorization* window, select the row below *PMSOG* and click *Maintain values*.



1. In the *Field Values* window, you can choose from the list of available *Permit Keys*, based on which the user will have the correct authorization to issue Work Permit Approvals. Add the **same** value to both *From* and *To* columns.



5. Similar to the previous step, select the row below *SWERK*, click *Maintain values*, and add the *From* and *To* values for the *Maintenance Plant*.

> ⚠ Caution
>
> When maintaining values for both *PMSOG* and *SWERK*, please be aware that:
>
> - You need to add the **same** value to *From* and *To* columns.

- These fields are free text fields. If you enter values manually, make sure to enter them correctly since they will not be validated.

6. Save your changes.
7. Once configured, we recommend to doublecheck in the user's profile (as described in Prerequisites [page 571] section), whether the correct values will show up after saving your changes.

4.42.2 Configuring Work Permit Approvals - Back End - Mobile Application Parameters

Context

For detailed information about Work Permit Approvals, see the overview topic, Work Permit Approvals Configuration [page 569].

The following is an **optional** configuration in case you want to enable for Safety Technicians to confirm the Work Permit Approval by adding a signature.

> **Note**
>
> For more information about how to use this feature, see Issuing Work Permit Approvals.

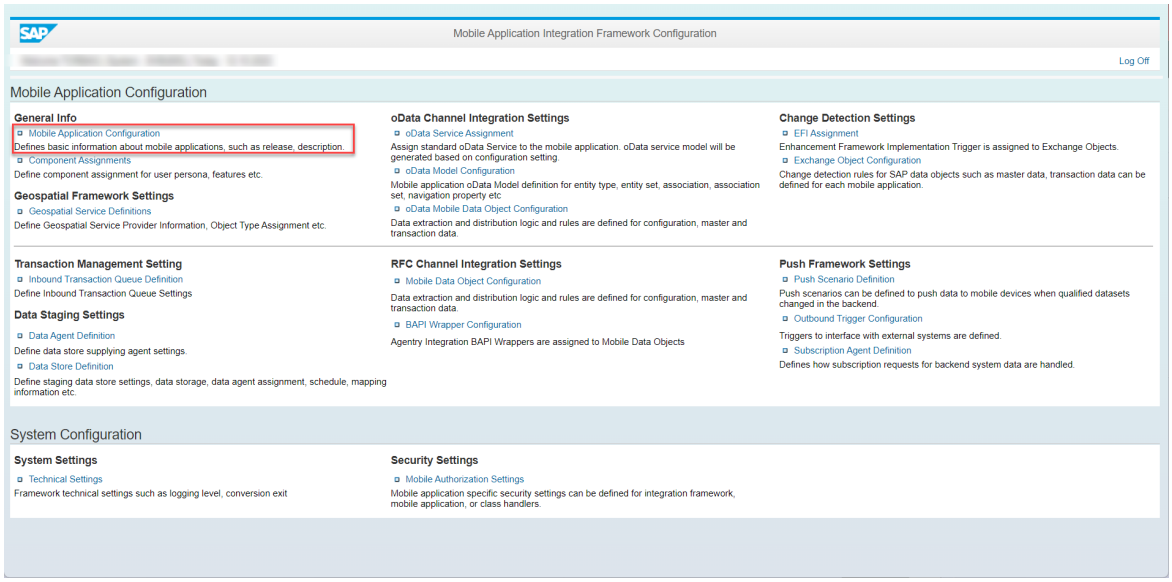
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

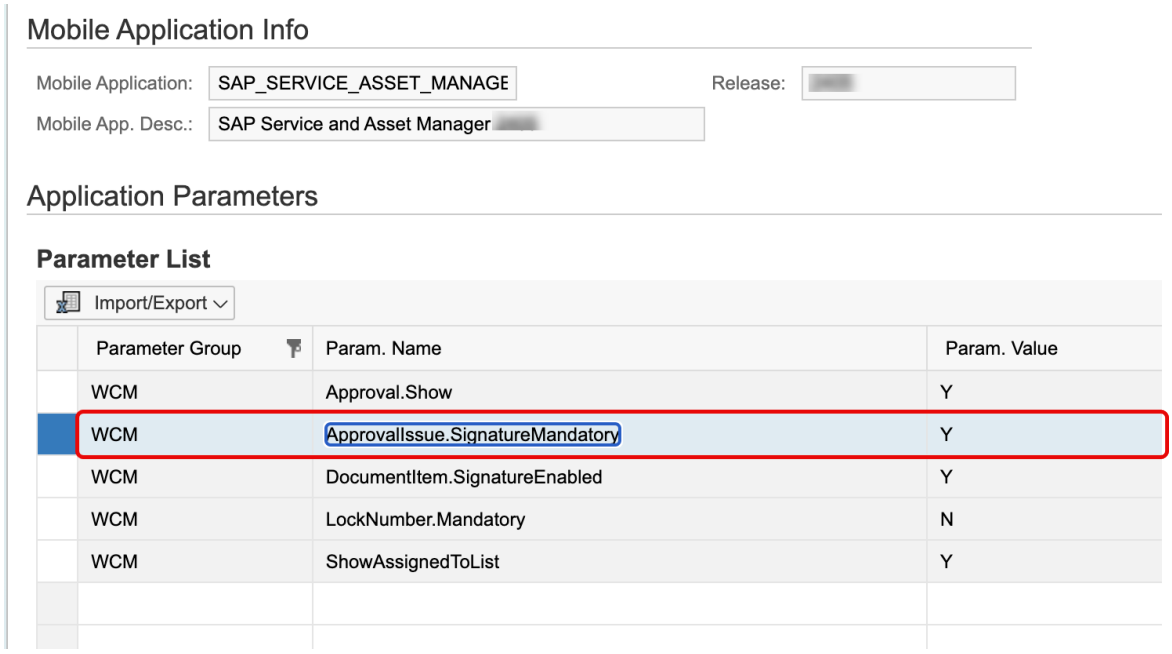
- **Mobile Application Parameters** configuration: refer to Parameters Tab in *MAIF Configuration Guide*.

Procedure

1. In the *SAP GUI*, navigate to the `/n/syclo/configpanel` transaction to open the Configuration Panel.
2. Under *General Info*, navigate to *Mobile Application Configuration*.



3. Select the application from the list, go to the *Parameters* tab and select the *ApprovalIssue.SignatureMandatory* parameter.
4. Enter *Change mode* and set the Parameter Value to **Y**.



> ### Note
>
> If you set the Parameter Value to **N**, the default process will not change and Safety Technicians will not be able to add signatures to the approval.

5. Save your changes.

4.43 Work Order Operations Split Assignment for Maintenance Technician Persona

With split assignment, you can work on multiple work orders or tasks simultaneously within the SAP Service and Asset Manager app. You are not limited to just one assignment. This approach promotes efficient team collaboration, ensures tasks are completed quickly, and provides flexibility in managing workload distribution.

> ⓘ Note
>
> - For more information on handling split assignment work tasks, see the Split Assignment topic in the SAP Service and Asset Manager user guide.
> - For more information on issuing operations with split possibilities, see Creating Employee Requirements Records (Splits) documentation.

Supported Personas

This feature is applicable for the following personas:

Maintenance Technician (Standard)
Maintenance Technician (Pro)

Configuration

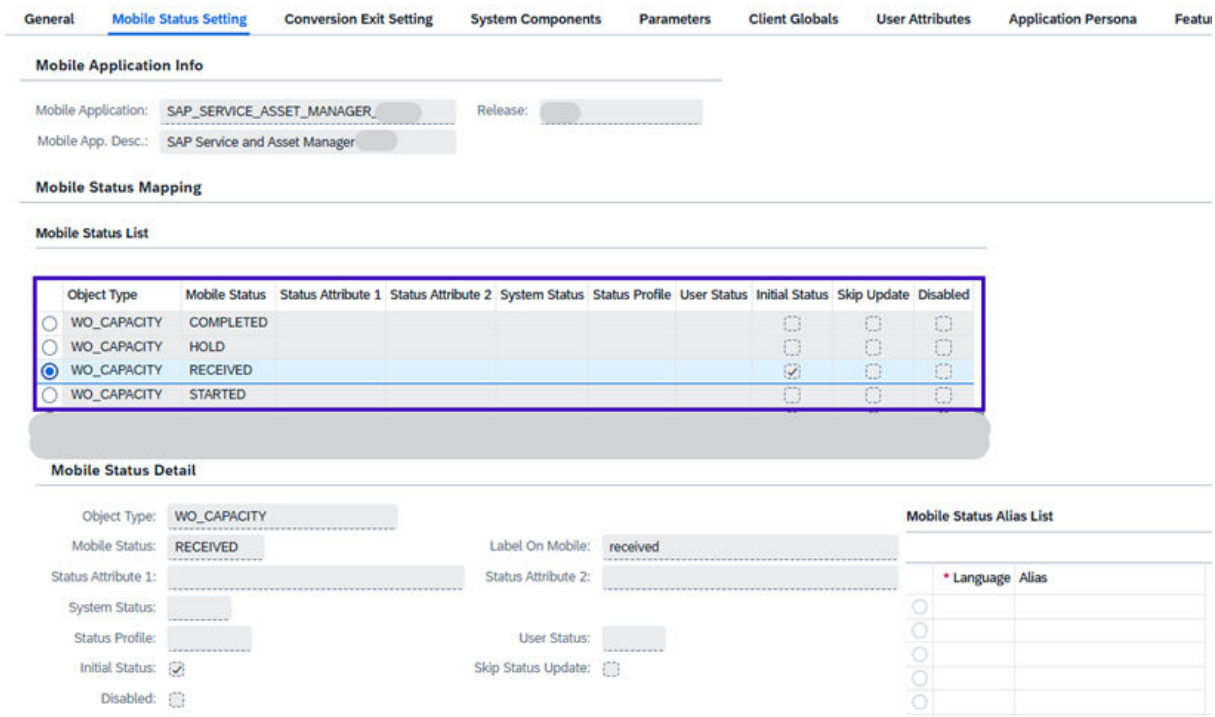
Perform the following configuration procedure(s):

Split Assignment Status Flow [page 576]

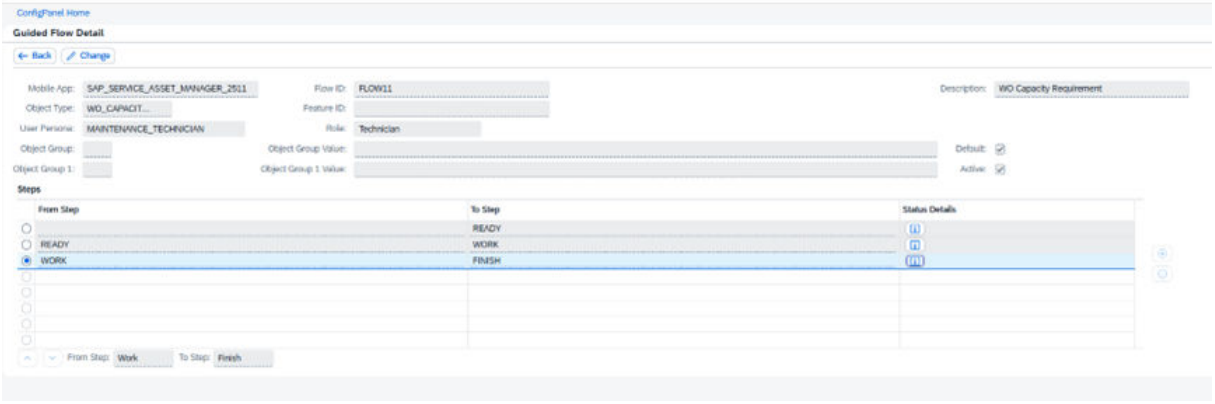
4.43.1 Split Assignment Status Flow

SAP Service and Asset Manager introduces several statuses for WO_CAPACITY in Mobile Status Settings at the application level. You can see these statuses in the screenshot below.

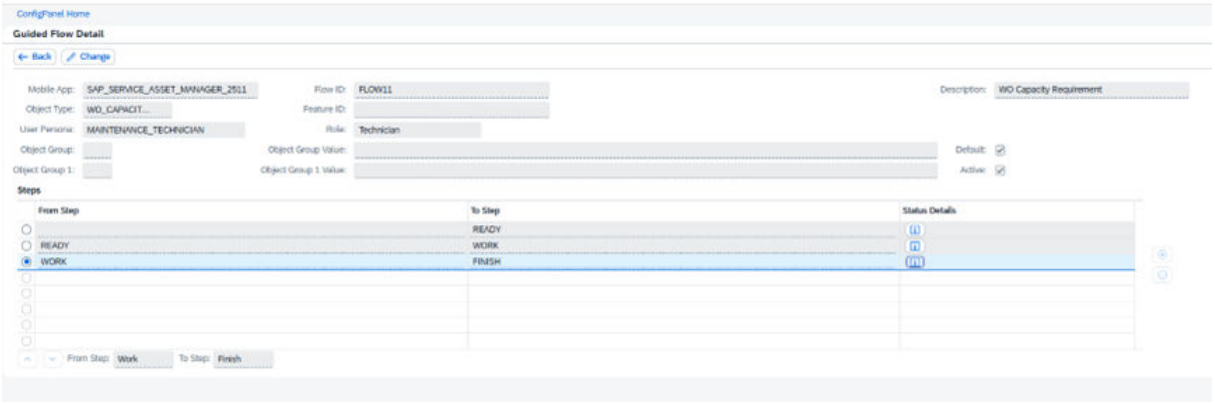
> ⓘ Note
>
> These statuses are specific to mobile use only.



Follow the configurable guided flow FLOW11, which is delivered in SSAM2511 for WO_CAPACITY:



The diagram below illustrates the flow of the technician role status.



> **Note**
>
> As of 2511 release, FLOW111 is added using the same steps as described above for the *Supervisor* role.

4.44 Zebra Scanner Configuration

On Zebra devices, users can scan barcodes by using the Zebra Scanner integration, which will allow them to:

- Scan a single barcode to navigate directly to an object's detail page.
- Trigger the scanning function directly on Overview or List pages, by pressing the barcode scanner button on the device.

> **Note**
>
> - For more information about how to use this feature, refer to Using Zebra Scanner.
> - The **SAP Scanner Framework** allows metadata to manipulate different scanners using the same APIs. For more information, see SAP Scanner Framework.
> - This feature is a third-party integration by Zebra. For more information and the list of supported devices, refer to the official Zebra documentation and Zebra Products and Software Support .

Supported Personas

This feature is applicable for the following personas:

Maintenance Technician (Standard)
Maintenance Technician (Pro)
Field Service Technician (Standard)
Field Service Technician (Pro)

Prerequisites

Before proceeding with SAP Service and Asset Manager configuration, you need to perform the following steps:

1. On the Zebra device, open the *DataWedge* application.
2. In the *Profile* menu, create a new profile and enter a name for it (e.g. SSAM).
3. Go to the *Profile* you just created.
4. Go to the *Applications* menu, select SAP Service and Asset Manager as application, and select all activities from the list.
5. Go to *Intent Output*, enable it, tap *Intent action* and enter `com.zebra.android.intent.action.SCAN` as intent action name.

> **Note**
>
> Make sure you enter the action name correctly as it is key for SAP Service and Asset Manager to receive scan data from Zebra Scanner.

6. Under *Intent Output*, tap *Intent delivery* and select *Broadcast intent*.

Configuration

Perform the following configuration procedure(s):

- Configuring Zebra Scanner - Back End - Mobile Application Parameters [page 579]

4.44.1 Configuring Zebra Scanner - Back End - Mobile Application Parameters

Context

For configuration prerequisites and detailed information about Zebra Scanner, see the overview topic, Zebra Scanner Configuration [page 578].

The following procedure describes how to configure Mobile Application Parameters for the Zebra Scanner feature in the Configuration Panel.

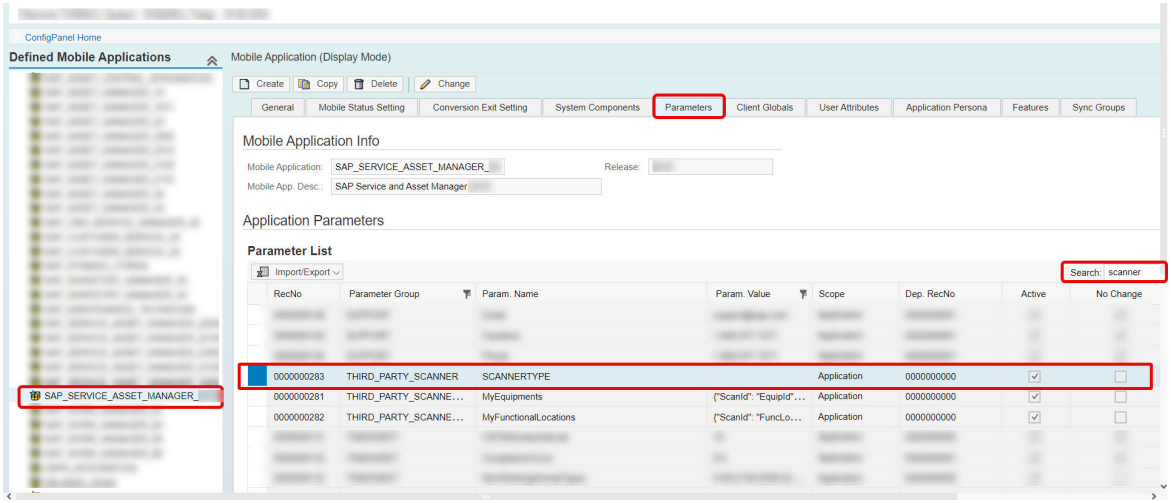
General Links

If necessary, see the following link(s) for additional information and instructions for the required steps included in this procedure:

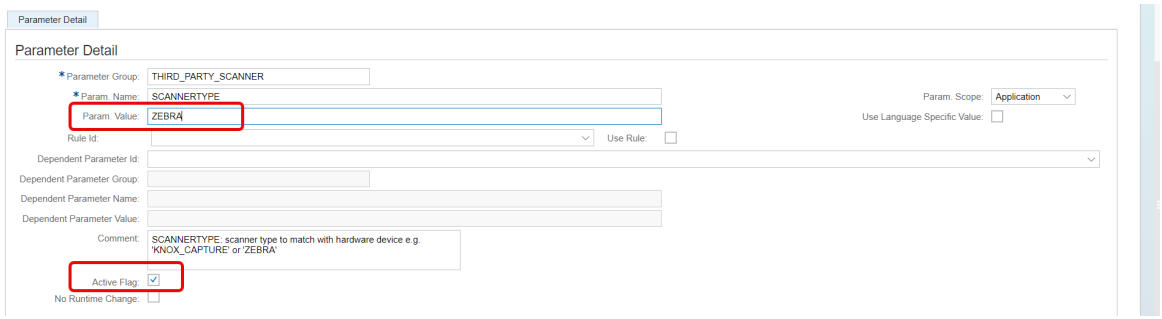
- **Mobile Application Parameters** configuration: refer to Parameters Tab in *MAIF Configuration Guide*.

Procedure

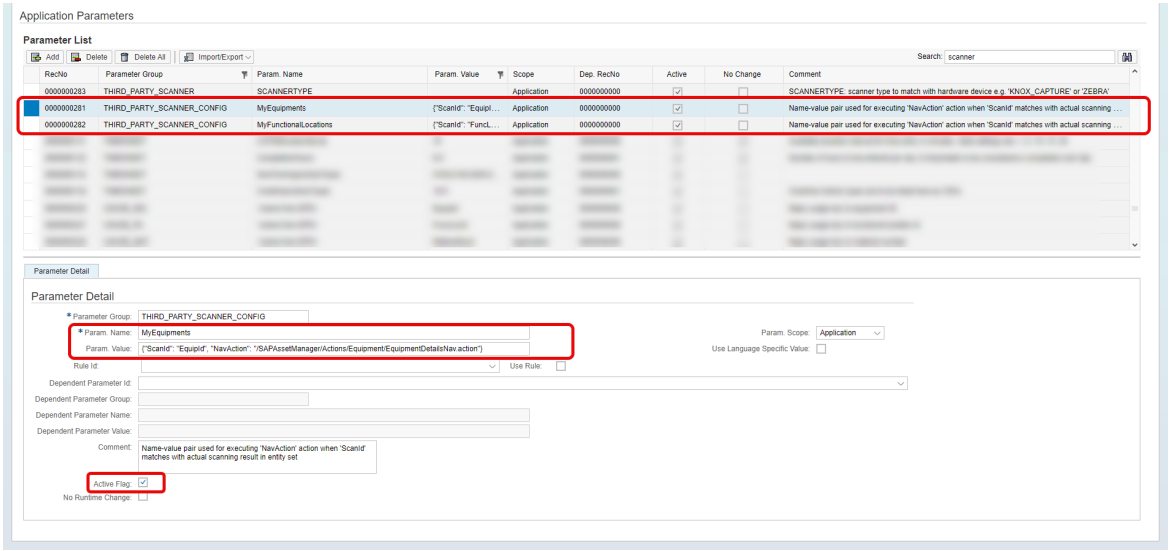
1. On the Configuration Panel, go to *Mobile Application Configuration*.
2. Select your application from the left, go to the *Parameters* tab and select the *SCANNERTYPE* Application Parameter.



3. Enter *Change* mode, add *ZEBRA* as *Parameter Value*, set the parameter to *Active* and click *Save*.



4. You can configure additional parameters to quickly navigate the user to an object within the application, when scanning a barcode. See below example:



1. Enter *Change* mode and add a new row under *Parameter List*.
2. Under *Parameter Detail*, add *THIRD_PARTY_SCANNER_CONIG* as the *Parameter Group*.
3. Add the *Parameter Name* according to the object type you want the user to navigate to (e.g. 'MyEquipments', 'MyFunctionalLocations').

4. Add the *Parameter Value* according to the object type you want the user to navigate to (e.g. `{"ScanId": "EquipId", "NavAction": "/SAPAssetManager/Actions/Equipment/EquipmentDetailsNav.action"}`).
5. Set the parameter to *Active* and click *Save*.

> **Note**
>
> You can configure these parameters for any Overview or List pages in the application. However, please note the following:
>
> - Multiple objects may have the same ID (also different object types).
> - If you configure multiple parameters for multiple object types, the order of parameters matter in the Parameter List.
> - When the user scans a QR code, the application will navigate to the object, which has the first match with the scanned ID.

5 Performance Optimization

5.1 Delta Sync Optimization

The SAP Service and Asset Manager application performs two types of synchronization:

- **Initial synchronization**: Performed either when the user logs in to the application for the first time or after the application is reset. Any subsequent synchronization performed after a successful initial synchronization and before the app is reset is a delta synchronization.
- **Delta synchronization**:
  - Uploads any pending transactions created locally on the mobile device to the back end system.
  - Downloads delta data from the back end system to the mobile device for entities that are new or have changed since the last synchronization.

See the following configuration options to optimize delta synchronization:

- Performing a delta sync with a list of modified entities. See Downloading Only Modified Entities [page 582].
- Performing periodic syncs. See Configuring Auto-Sync - Back End - Mobile Application Parameters [page 306].
- Lead Entity Based Flow configuration. See Lead Entity Based Flow Overview [page 588].
- Performing only uploads. See Upload Only Configuration [page 585].

5.1.1 Downloading Only Modified Entities

As of SAP Service and Asset Manager version 2310, the application is activated for optimized delta synchronization by default. In this case, when the user initiates delta synchronization, an attempt is made to upload transactions, if any. An interactive call then identifies entities that need to be updated or have changed since the last synchronization. Only for these changed entities will delta synchronization be started, thus optimizing the duration of delta synchronization.

Since the last synchronization completed, entities are qualified for delta synchronization as follows:

- An entity that has a new dependent queue.
- An entity that has a triggered exchange.
- An entity whose configuration includes delta key calculation on every delta synchronization.
- An entity for which Periodic sync [page 306] is enabled and expired.
- Entities that are marked as dependent for **any** of the qualified entities mentioned above, or
- Entities that are active by feature or persona for the respective user.

Optimized delta synchronization will be equivalent to normal delta synchronization if:

- The application cannot detect the completion time of the user's last synchronization.

- The application's *DownloadEffectedEntities* parameter is set to *N* (off).
- The application initiated synchronization due to a user change. For example, **User A** logged out and **User B** logged in, which initiated synchronization.

Supported Personas

This feature is applicable for the following personas:

Maintenance Technician (Standard)
Maintenance Technician (Pro)
Maintenance Technician (External)
Field Service Technician (Standard)
Field Service Technician (Pro)
Inventory Clerk
Safety Technician
Extended Warehouse Clerk
Field Logistics

Configuration

Perform the following configuration step(s):

1. Configuring Entities to Download - Back End - Mobile Application Parameters [page 583]

5.1.1.1 Configuring Entities to Download - Back End - Mobile Application Parameters

Context

For detailed information about Downloading Only Modified Entities, see the overview topic, Downloading Only Modified Entities [page 582].

The below procedure describes how to qualify entities for delta synchronization [page 582], by enabling the *DownloadEffectedEntities* mobile application parameter.

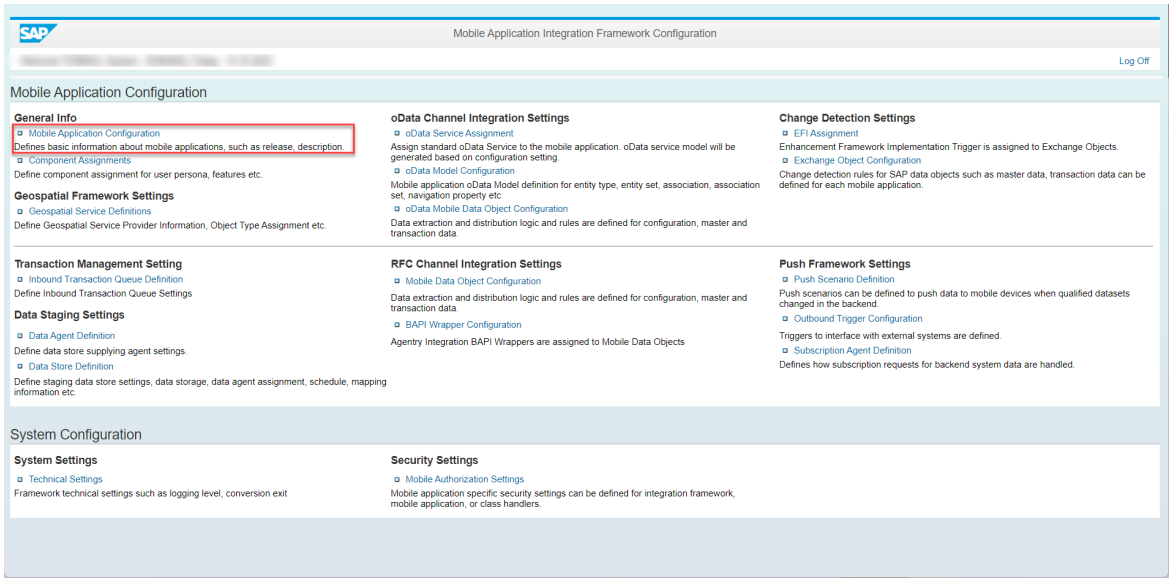
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

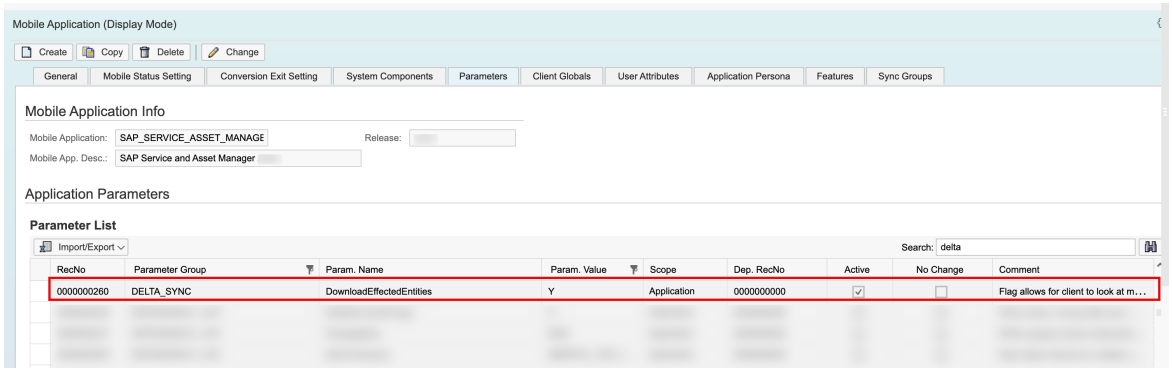
- **Mobile Application Parameters** configuration: refer to Parameters Tab in *MAIF Configuration Guide*.

Procedure

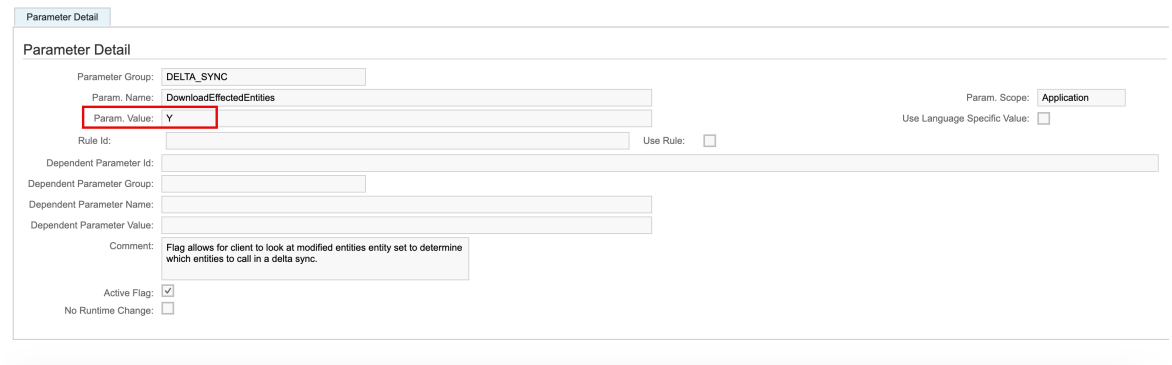
1. On the ConfigPanel, go to *Mobile Application Configuration*.



2. On the left, select your application from the list, and go to the *Parameters* tab.
3. Under *Parameter List*, in the *DELTA_SYNC Parameter Group*, select the *DownloadEffectedEntities* parameter.



4. Enter *Change Mode* and set the *Parameter Value* to *Y* or *N* to enable or disable for the client to look at modified entities and identify them to download during delta sync.



5. Save your changes.

5.1.2 Upload Only Configuration

Overview

SAP Service and Asset Manager mobile users follow a workflow defined in the back end system, which requires downloading all necessary data at the beginning of their shift (either daily or weekly) to perform their assigned jobs or tasks. During the shift, users record transactions related to completed jobs. As an offline application, SAP Service and Asset Manager must be synchronized with the back end system to **upload recorded transactions** and **download any new or updated data** (see delta synchronization [page 582]). These two actions are coupled, and occur when the user taps the *Sync* button. However, in many scenarios users may not need to download new or updated data throughout the day, they only need to post their recorded transactions.

With the **Upload Only** feature, you can improve efficiency and optimize delta synchronization. This allows users to upload recorded transactions independently, without triggering an immediate download of delta data. Users may choose to upload transactions immediately after:

- Completing a job
- Completing all jobs for the day
- Finishing their shift
- Completing their daily or weekly work cycle

> **Note**
>
> - Users can still initiate a full delta sync at any time to download the latest delta data.
> - Please note that the Upload Only feature has specific characteristics and limitations regarding how data is synced between the back end and the mobile device. Before enabling this feature, we recommend reviewing the current limitations [page 586].
> - For more information about using the Upload Only feature, see Using the Upload Only Feature.

Supported Personas

This feature is applicable for the following personas:

Maintenance Technician (Standard)
Maintenance Technician (Pro)
Maintenance Technician (External)
Inventory Clerk

Limitations

The Upload Only feature currently has the following limitations:

- The **Upload Only** and **Inbound Transaction Queue** features are mutually exclusive; you can use one or the other.

  > ⓘ Note
  >
  > For more information about Inbound Transaction Queue, refer to MAIF documentation:
  > - Inbound Transaction Management
  > - Inbound Transaction Queue Definition Settings

- After performing an upload only action, all the local transactions created or updated on the device will be out of sync with the actual object created or updated in the back end system, until a sync (i.e. download action) is performed.

  > ⚠ Caution
  >
  > Please note that any additional updates to the object (or creating or updating its sub-objects) may result in data conflicts between the mobile device and the back end system, during subsequent uploads.

- Local **Work Orders** will be removed after the upload only action, except when the *AUTO_RELEASE* is enabled.

Configuration

Perform the following configuration step(s):

- Configuring Upload Only - Back End - Enabling the Feature [page 586]

5.1.2.1 Configuring Upload Only - Back End - Enabling the Feature

Context

For detailed information about the Upload Only feature, see the overview topic, Upload Only Configuration [page 585].

To enable this feature in the ConfigPanel, perform the steps below.

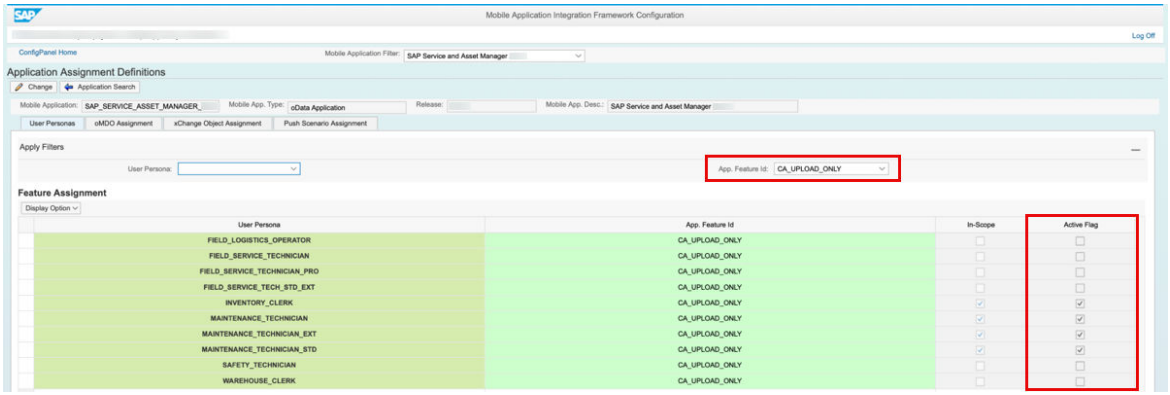
General Links

If necessary, see the following links for additional information and instructions for the required steps included in this procedure:

- **Enabling and disabling features**: refer to Configuring Features in *MAIF Configuration Guide*.

Procedure

1. In the ConfigPanel, go to *Component Assignments*.
2. Select the application with correct version from the list.
3. Select the *CA_UPLOAD_ONLY* as *App. Feature Id*, enter *Change Mode* and set the feature to *Active* for the relevant persona(s).



4. Save your changes.

5.1.2.2 Use Cases for the Upload Only Feature

The following scenarios show how the Upload Only feature works:

> ⓘ Note
>
> For detailed information about the Upload Only feature, see the overview topic, Upload Only Configuration [page 585].

Scenario A

The user has downloaded the data scheduled for the day and is guided along a route to travel to each location to perform tasks associated with specific Work Orders. Upon arriving at each location, the user performs the task, uploads the data from the device, and then moves on to the next location. See detailed steps below:

1. The user arrives at a location where they are about to perform a task associated with a Work Order.

2. Finds the appropriate Work Order and starts the Work Order.
3. Navigates to the related Operation and the Equipment and performs the required repairs to the Equipment.
4. Records the Readings for all the Measuring Points on the Equipment.
5. Confirms the repair through the Operation and enters the time.
6. Completes the Work Order.
7. Performs an upload.
8. Moves on to the next location to perform the next job associated with another Work Order.

Scenario B

The user has downloaded the data scheduled for the day and will be **offline** to perform all the tasks associated with specific Work Orders. At the end of the day when the user arrives at a location **with connectivity**, they upload the data from the device before the end of their shift. See detailed steps below:

1. The user arrives at a location without connectivity, where a list of Equipment objects are to be inspected for regular maintenance.
2. Finds the appropriate Work Order and starts the Work Order.
3. Navigates to Record Points for all Equipment associated with the Work Order.
4. Filters the list of points by each Equipment and records the Readings.
5. Creates various Notifications for any Defects found while recording the Readings.
6. Completes the Work Order.
7. Continues to perform the same for each location.
8. At the end of the day, the user arrives at location with connectivity and performs an upload for all the transactions.

5.1.3 Lead Entity Based Flow Overview

For oData Mobile Data Objects (oMDOs) that need a key list, MAIF supports Standard Flow using Key List as a default configuration option. For oMDOs that need a key list, you can optionally activate and configure the the Lead Based Entity Flow feature.

General Overview

Lead entity based flow is a feature available for oMDOs and is enabled with exchange. Lead entity based flow performs an optimized delta key calculation, which reduces the delta sync duration. When the lead entity based flow is active for an object, the business object's key list is managed through the Lead Entity key list only. Client states are persisted in the database for the lead and child entities. Additionally, the detail client state holds the key's qualified data source (distribution mode 1 or 2, etc.). In subsequent delta syncs, new keys, delta keys, accumulation, and tombstones are also managed based on the lead entity key list only, including for all child entities.

The lead entity based flow feature is a standard feature for functional locations, equipment, and material oMDOs.

MAIF supports the following flow types:

- Basic Flow without Key List
- Standard Flow with Key List

The lead entity based flow feature is a variant of the Standard Flow with Key List.

The following table shows the standard SAP-delivered handlers for the lead entity based flow:

oMDO	SAP-Delivered Handler	Support	
		Standard Flow	Lead Flow
SAMXX_FUNCLOC_OD SAMXX_FUNCLOC_OD_LITE	/MERP/CL_PM_FUN-CLOC1_OD	X	X
SAMXX_EQUIPMENT_OD SAMXX_EQUIP-MENT_OD_LITE	/MERP/CL_PM_EQUIP-MENT1_OD	X	X
SAMXX_MATERIAL_OD	/MERP/CL_PM_MATE-RIAL1_OD	X	X

Functionally, there is no difference between the standard flow with key list with or without the lead entity based flow. For example, data downloaded to the device using either configuration option should be the same. However, the performance of an oMDO enabled with lead entity based flow is optimized and expected to consume less time, due to the way the delta is calculated. As there are multiple factors which can influence the delta calculation duration, it is not possible to quantify the improved runtime.

Switching between Standard Flow with Key List and without Lead Entity Based Flow

It is possible to switch between Standard Flow with Key List with and without Lead Entity Based Flow by activating or deactivating the *Lead Entity Based Flow* option in the oMDO general settings. See *Step 1* in the Configuring the Lead Entity Based Flow [page 591] procedure for detailed information.

Standard SAP-delivered handlers, as shown in the above table, are backwards compatible (they support both flows without the need to change the handler).

> **Note**
>
> If mobile users have synced using either active configuration, they must reset the mobile app on their device after each configuration switch.

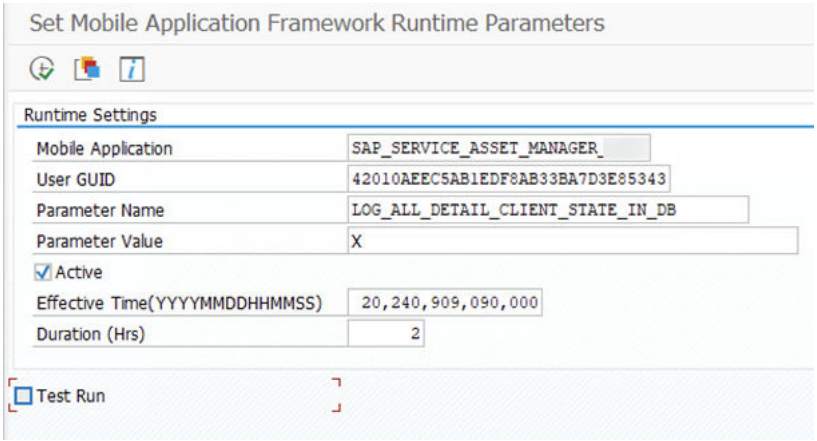
Advantages of Lead Entity Based Flow

- A valid keylist is calculated during the initial sync. In subsequent delta syncs, the valid keylist is not calculated, but rather adjusted based on the exchange keylist.
- You can accumulate keys for the selected distribution mode through a config filter.
- The detail client state table provides insight of the keys' qualified source.

- With the data in the detail client state table, accumulation based on distribution mode is possible. This avoids generic key accumulation from all sources and redundant dependent keys from either the distribution key list and/or the target client state.
- Subsequent delta syncs process only the delta and not the complete distribution keylist.
- Based on the exchange keylist, the business object handler determines the deletion keylist. This avoids looping through the valid distribution keylist and delta keylist to determine the deletion keylist. Therefore, the overall execution time of the oMDO is optimized.
- Data from the detailed client state is useful for troubleshooting.

Design Constraints for Lead Entity Based Flow

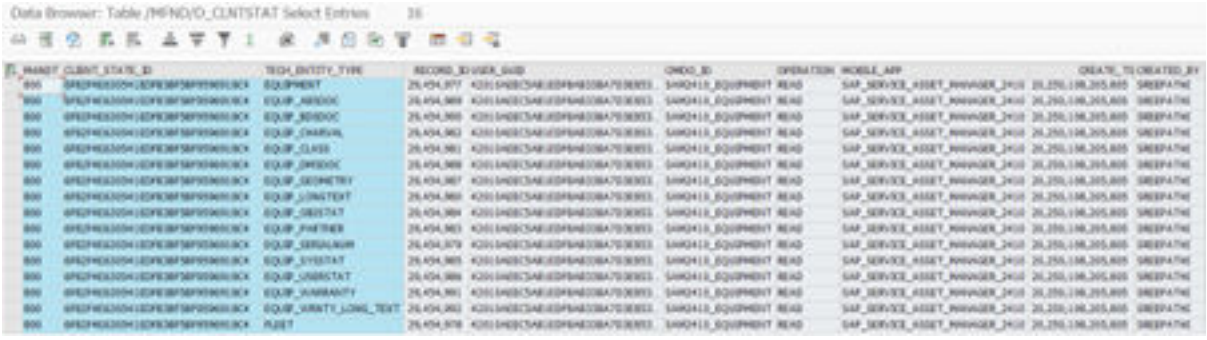
- The oMDO with the exchange enabled is expected to show performance improvement
- The switch of oMDO configuration from Lead Entity Based Flow to Standard Flow with Key List and/or a change of the oMDO filter value requires a reset of the app
- If the handler does not define the lead entity but it is active in the oMDO configuration, sync should raise an error
- For a lower version of a system that doesn't support the batch at once feature in gateway, the lead entity and child entity calls are designed to be handled in a different session. To support it, the delta and tombstone key list for all entities (lead and child) are persisted in a detailed client state table. For a higher version of the system, which does support the batch at once feature, it is optional and can be turned on by setting the runtime parameters as follows:
  - **Report Program:** /SYCLO/CORE_RUNTIME_PARAM_PROG
  - **Transaction:**SE38 or SA38
  - **Authorization:** OBJECT *S_MI_CCMS* ID *ACTVT* FIELD *06*
  - **Execution Type:** Foreground
  - **Runtime values for report**



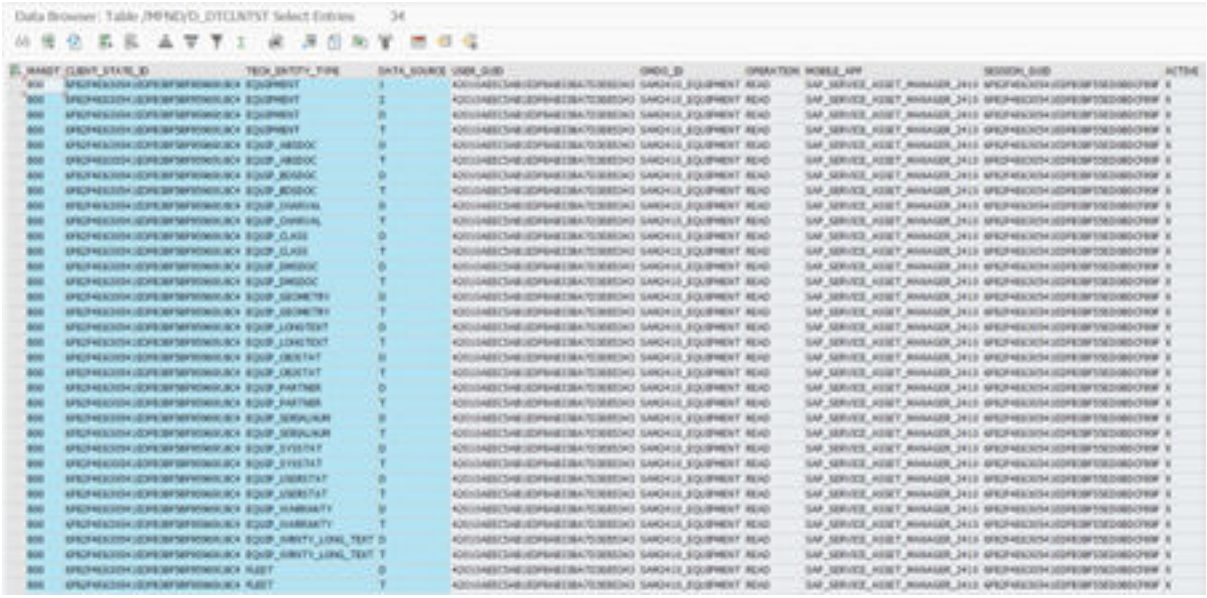
Database Tables for Lead Entity Based Flow

- **/MFND/D_CLNTSTAT:** Consolidated client state for lead and child entities

- **/MFND/D_DTCLNTST:** Detailed client state for lead entity. Based on the system level or runtime, it optionally holds the delta and tombstone key list for all entities handled by the OMDO.



Standard Client State Table



Detailed Client State Table

5.1.3.1 Configuring the Lead Entity Based Flow

For oData Mobile Data Objects (oMDOs) that need a key list, MAIF supports Standard Flow using Key List as a default configuration option. For oMDOs that need a key list, you can optionally activate and configure the the Lead Based Entity Flow feature.

Prerequisites

See the *Design Constraints* section of the Lead Entity Based Flow Overview [page 588] topic for important considerations before implementing this feature.

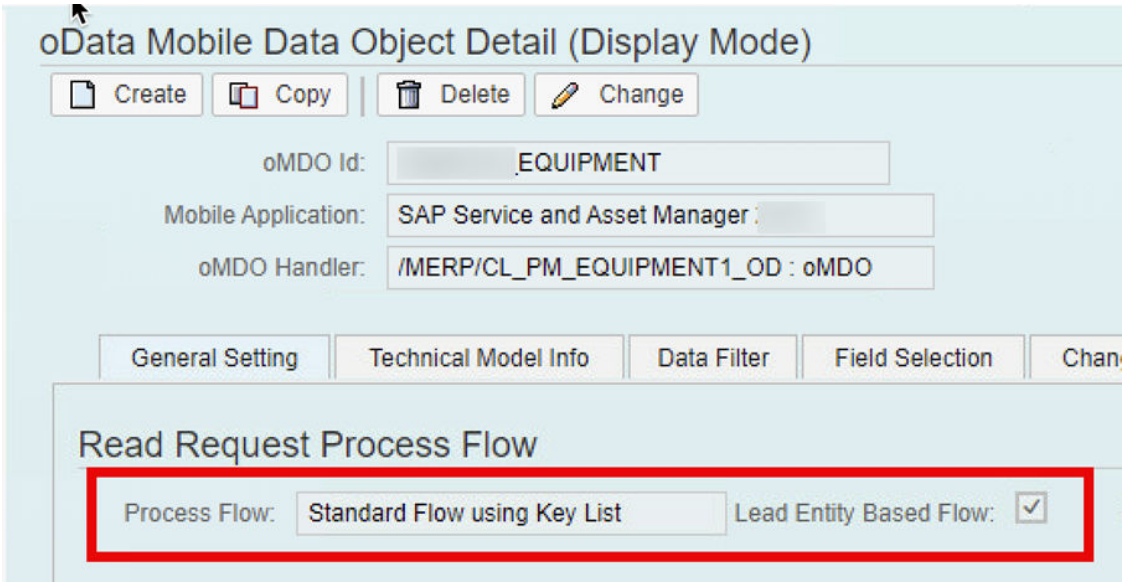
Context

See the Lead Entity Based Flow Overview [page 588] topic for detailed information about the lead entity based flow feature, advantages of implementation, and design constraints of the feature.

Procedure

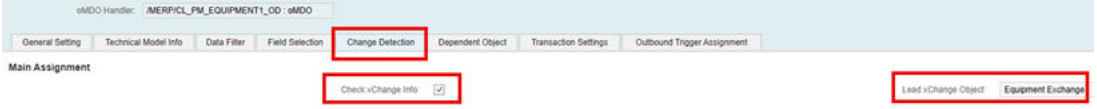
1. **Configuration through the ConfigPanel:**
   a. On the ConfigPanel Home page, select *oData Mobile Data Object Configuration*.
   b. Select your application in the *Mobile Application Filter*. Then select your oMDO in the *oData Mobile Data Object List*.
   c. Click the *Change* button and check the *Lead Entity Based Flow* box.

> **Note**
>
> Remember that the lead entity based flow feature is available for functional location, equipment, and material oMDOs only.



After you *Save* your changes, the oMDO settings that are not relevant for lead entity based flow are hidden.

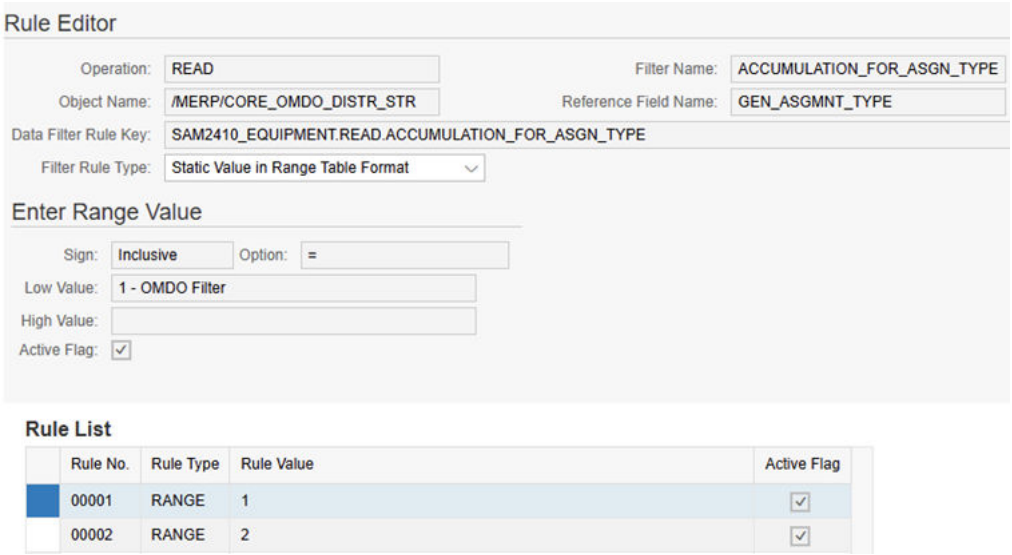
   d. Click the *Change Detection* tab on the *oData Mobile Data Object Configuration* page. Ensure that the business object is supporting change detection through the exchange configuration.



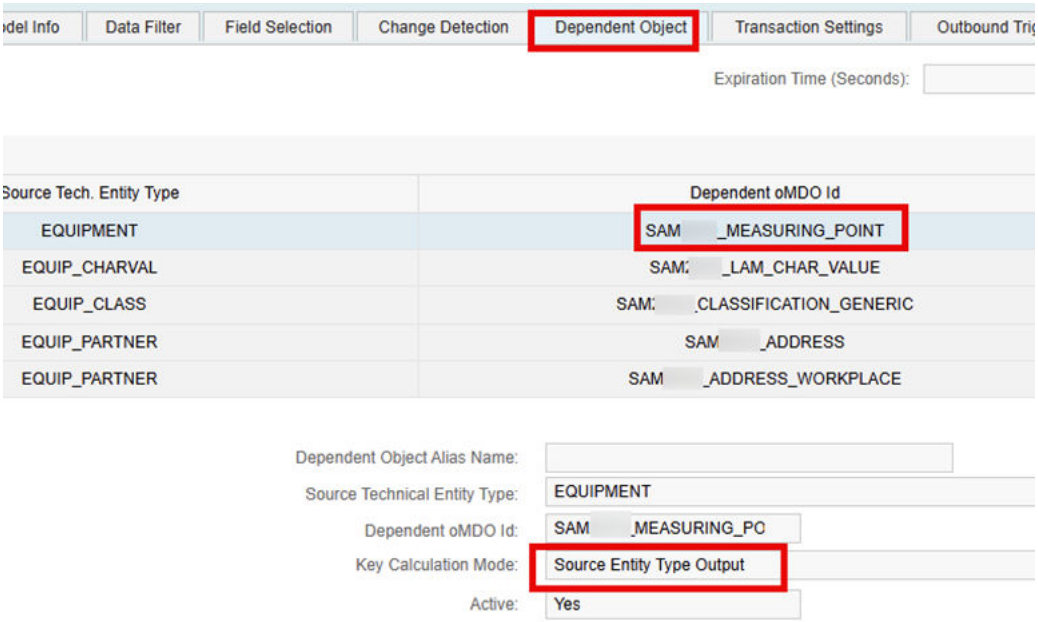
   e. While your app is still selected in the *Mobile Application Filter*, and you are on the *oData Mobile Data Object Configuration* page, click the *Data Filter* tab. Select the object you're configuring from the list. Ensure that the oMDO object has the *ACCUMULATION_FOR_ASGN_TYPE* filter defined and that it is maintained with values in sync with the *OBJECT_DISTRIBUTION_MODE* filter.

During an initial sync, the object distribution keys are collected from various sources. During a delta sync, keys are accumulated only for the filter values specified in the filter *ACCUMULATION_FOR_ASGN_TYPE*. For unspecified accumulation assignment type, the subseequent delta sync qualifies the respective keys for deletion.

> **Note**
>
> All other filters in the respective oMDO are treated the same in both flows and should be configured as needed for the implementation.

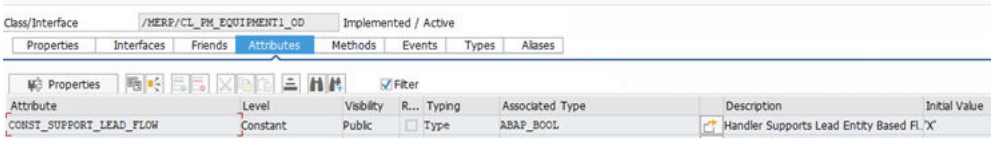


f. While still on the *oData Mobile Data Object Configuration* page, click the *Dependent Object* tab. Ensure that any oMDO that generates a dependent queue to the oMDO that supports the lead based entity flow feature, uses the dependency key calculation mode as the *Source Entity Type Output*.

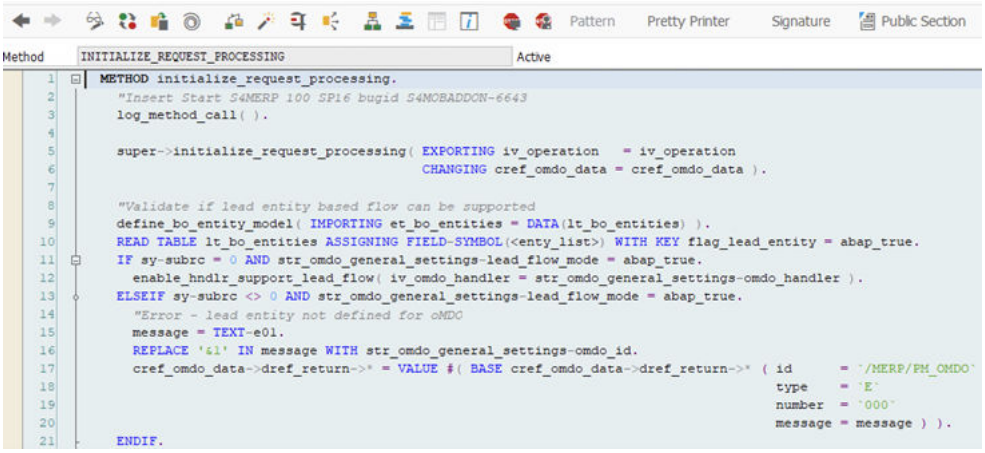


> ### Note
>
> For reference, use one of the standard delivered handlers:
>
> - /MERP/CL_PM_FUNCLOC1_OD
> - /MERP/CL_PM_EQUIPMENT1_OD
> - /MERP/CL_PM_MATERIAL1_OD

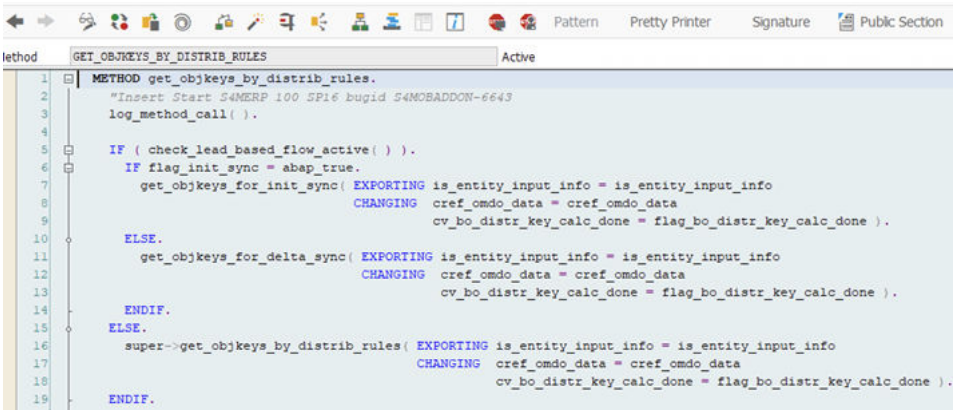
2. **Configuration through the SAP GUI:**
   a. The respective handler must define the constant attribute *CONST_SUPPORT_LEAD_FLOW* of type *ABAP_BOOL*, with a default value of *X*.



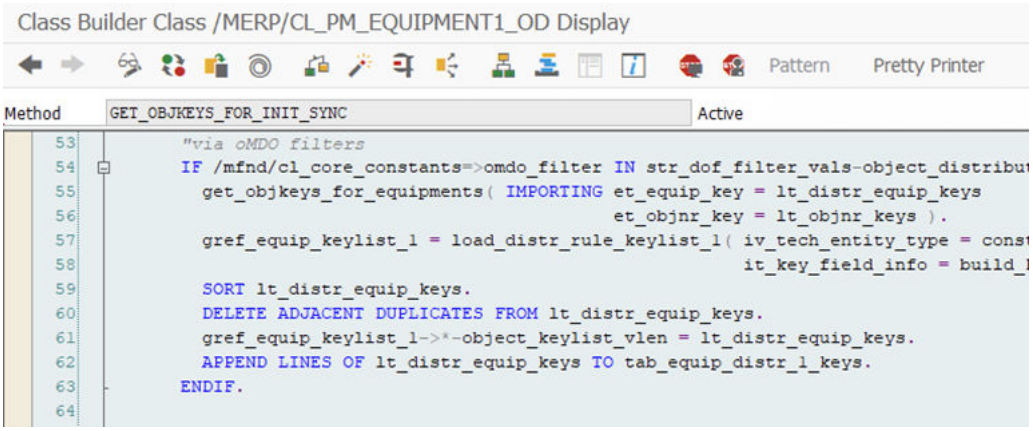
   b. Redefine the method *INITIALIZE_REQUEST_PROCESSING* to achieve the following:
      - Validate if the lead entity is defined in the buisness object model
      - Check if the oMDO configuration is enabled and the Lead Entity Based Flow is active
      - Call the *ENABLE_HNDLR_SUPPORT_LEAD_FLOW* method to set the lead flow active



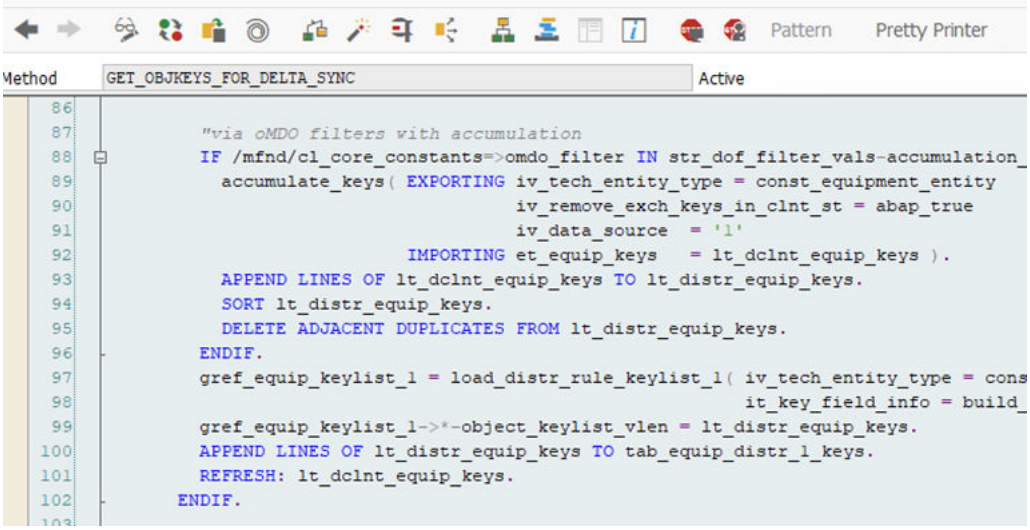
   c. Redefine the method *GET_OBJKEYS_BY_DISTRIB_RULES* to achieve the following:
      - Validate if lead entity based flow can be supported by calling the *CHECK_LEAD_BASED_FLOW_ACTIVE* method. If supported, implement separate methods for both the initial sync and the delta sync.
      - If not enabled, invoke the *GET_OBJKEYS_BY_DISTRIB_RULES* method to support both initial and delta sync. This ensures backwards compatibility and avoids a configuration of the handler in reselection.



d. Update the keys qualfied via individual distribution mode to the base handler's internal table *LOAD_DISTR_RULE_KEYLIST_X* (where *X* represents the distribution mode) in the initial sync implementation of the handler. For example, keys qualified via the *1* distrubution mode are saved in *LOAD_DISTR_RULE_KEYLIST_1*.

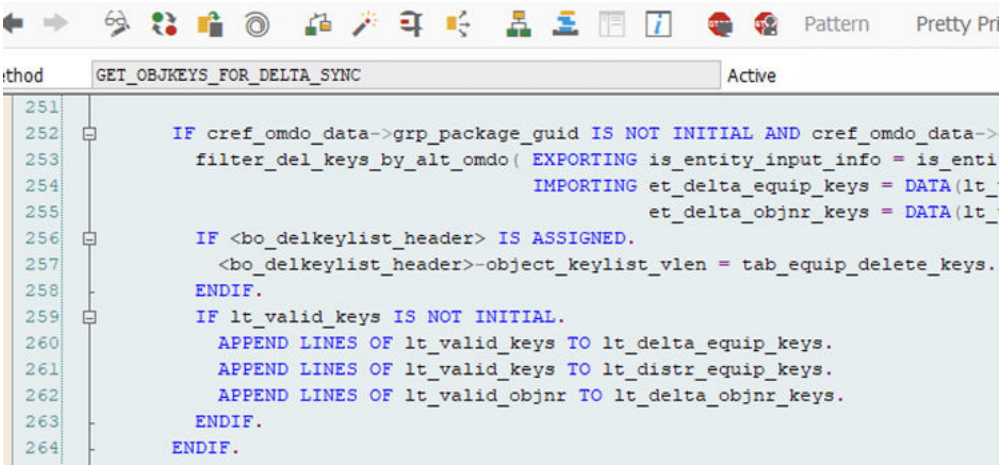


e. Ensure the following delta sync implementaion scenarios are configured properly for your application:
   - New keys that become valid from multiple sources souch as *1*, *2*, *3*, *9*, or *Z*
   - Accumulation of existing keys based on the filter value *ACCUMULATION_FOR_ASGN_TYPE*
   - Existing keys that require refresh due to exchange
   - Existing keys that require tombstone generation

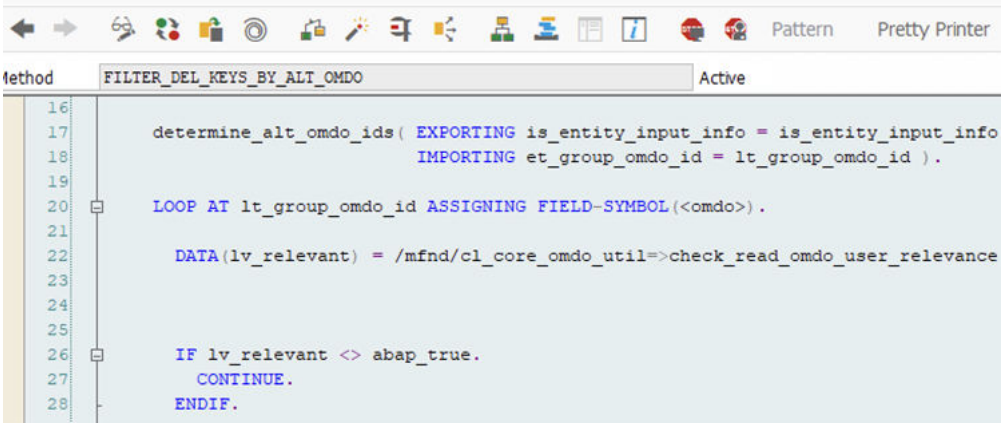



```
"via oMDO filters with accumulation
IF /mfnd/cl_core_constants=>omdo_filter IN str_dof_filter_vals-accumulation_
  accumulate_keys( EXPORTING iv_tech_entity_type = const_equipment_entity
                             iv_remove_exch_keys_in_clnt_st = abap_true
                             iv_data_source  = '1'
                   IMPORTING et_equip_keys   = lt_dclnt_equip_keys ).
  APPEND LINES OF lt_dclnt_equip_keys TO lt_distr_equip_keys.
  SORT lt_distr_equip_keys.
  DELETE ADJACENT DUPLICATES FROM lt_distr_equip_keys.
ENDIF.
gref_equip_keylist_1 = load_distr_rule_keylist_1( iv_tech_entity_type = cons
                                                  it_key_field_info = build_
gref_equip_keylist_1->*-object_keylist_vlen = lt_distr_equip_keys.
APPEND LINES OF lt_distr_equip_keys TO tab_equip_distr_1_keys.
REFRESH: lt_dclnt_equip_keys.
ENDIF.
```

f. If the entity type has multiple oMDO assignments, initial and delta sync key calculation must filter the delete keys based on other oMDO's delta key list. The method *DETERMINE_ALT_OMDO_IDS* returns a list of oMDOs valid for entity type, excluding the current oMDO.




```
IF cref_omdo_data->grp_package_guid IS NOT INITIAL AND cref_omdo_data->
  filter_del_keys_by_alt_omdo( EXPORTING is_entity_input_info = is_enti
                               IMPORTING et_delta_equip_keys = DATA(lt_
                                         et_delta_objnr_keys = DATA(lt_
  IF <bo_delkeylist_header> IS ASSIGNED.
    <bo_delkeylist_header>-object_keylist_vlen = tab_equip_delete_keys.
  ENDIF.
  IF lt_valid_keys IS NOT INITIAL.
    APPEND LINES OF lt_valid_keys TO lt_delta_equip_keys.
    APPEND LINES OF lt_valid_keys TO lt_distr_equip_keys.
    APPEND LINES OF lt_valid_objnr TO lt_delta_objnr_keys.
  ENDIF.
ENDIF.
```




```
determine_alt_omdo_ids( EXPORTING is_entity_input_info = is_entity_input_info
                        IMPORTING et_group_omdo_id = lt_group_omdo_id ).

LOOP AT lt_group_omdo_id ASSIGNING FIELD-SYMBOL(<omdo>).

  DATA(lv_relevant) = /mfnd/cl_core_omdo_util=>check_read_omdo_user_relevance



  IF lv_relevant <> abap_true.
    CONTINUE.
  ENDIF.
```

g. For initial and delta sync, the key calculation of the child entity must be based on the lead entity key list.

```
GET_OBJKEYS_FOR_DELTA_SYNC                                    Active
    SORT: lt_delta_equip_keys, lt_delta_objnr_keys.
    DELETE ADJACENT DUPLICATES FROM lt_delta_equip_keys.
    DELETE ADJACENT DUPLICATES FROM lt_delta_objnr_keys.
    get_objkeys_for_child_entities( EXPORTING is_entity_input_info = is_entity_input_info
                                              it_equip_keys  = lt_delta_equip_keys
                                              it_objnr_keys  = lt_delta_objnr_keys
                                    CHANGING  cref_omdo_data = cref_omdo_data ).
```

Child entity key calculation must set the distribution key list and delete key list based on the lead entity key list for distribution and delete, respectively.

```
GET_OBJKEYS_FOR_CHILD_ENTITIES                                Active
  IF ls_equip_on_demand-classification = 'X'.
    get_objkeys_for_equip_classes( EXPORTING it_equip_key     = it_equip_keys
                                   IMPORTING et_objclass_key  = DATA(lt_equipclass_key) ).
    SORT lt_equipclass_key.
    DELETE ADJACENT DUPLICATES FROM lt_equipclass_key COMPARING ALL FIELDS.
    lref_class_delta_keylist->*-object_keylist_vlen = lt_equipclass_key.
    IF ( flag_init_sync = abap_true AND cref_omdo_data->flag_user_switch = abap_true )
      OR flag_init_sync = abap_false.
      determine_obsolete_keys( EXPORTING iv_tech_entity_type = const_equip_class_entity
                                         is_entity_input_info = is_entity_input_info
                                         it_equi_objnr_exch_keys = lt_equi_objnr_keys
                                         it_delta_keylist = lref_class_delta_keylist
                               CHANGING  ct_distr_keylist = lref_class_distr_keylist
                                         ct_del_keylist = lref_class_del_keylist ).
    ELSEIF flag_init_sync = abap_true.
      lref_class_distr_keylist->*-object_keylist_vlen = lref_class_delta_keylist->*-object_keylist_vlen.
    ENDIF.
  ENDIF.
```

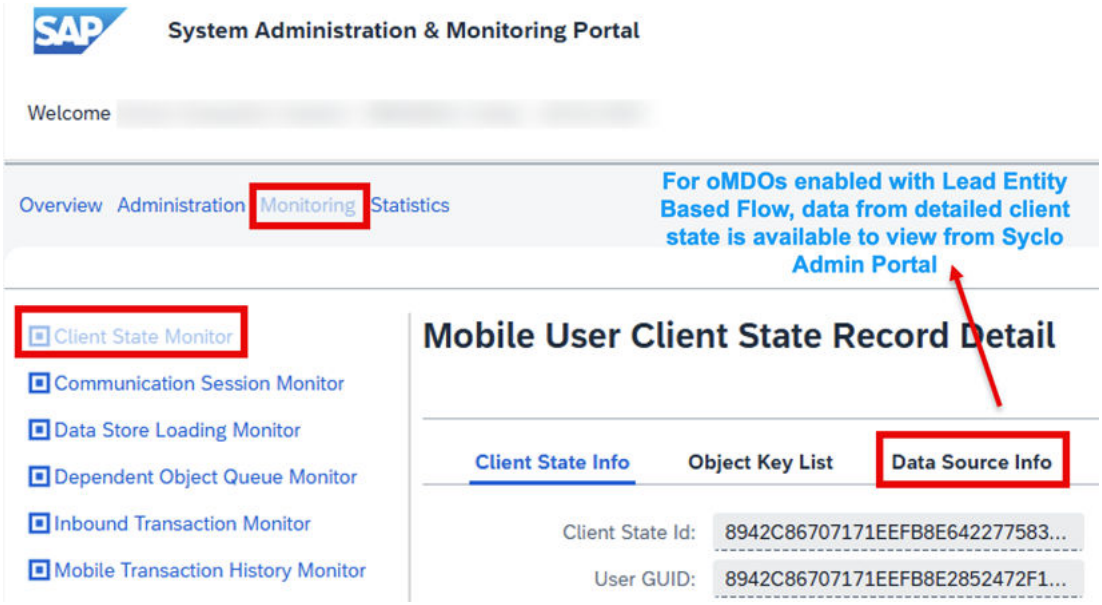
For cases where the child entity keys become invalid due to a deletion flag set or they are deleted from the back end but the lead object is stil valid, obsolete keys should be determined in the BO handler and set for deletion. For example, equipment EQ1 is valid and has a classification of CL1. During the lifetime, CL1 is removed and introduced with CL2. In such cases, CL1 should be set for deletion and CL2 details should be set as a delta for EQ1.

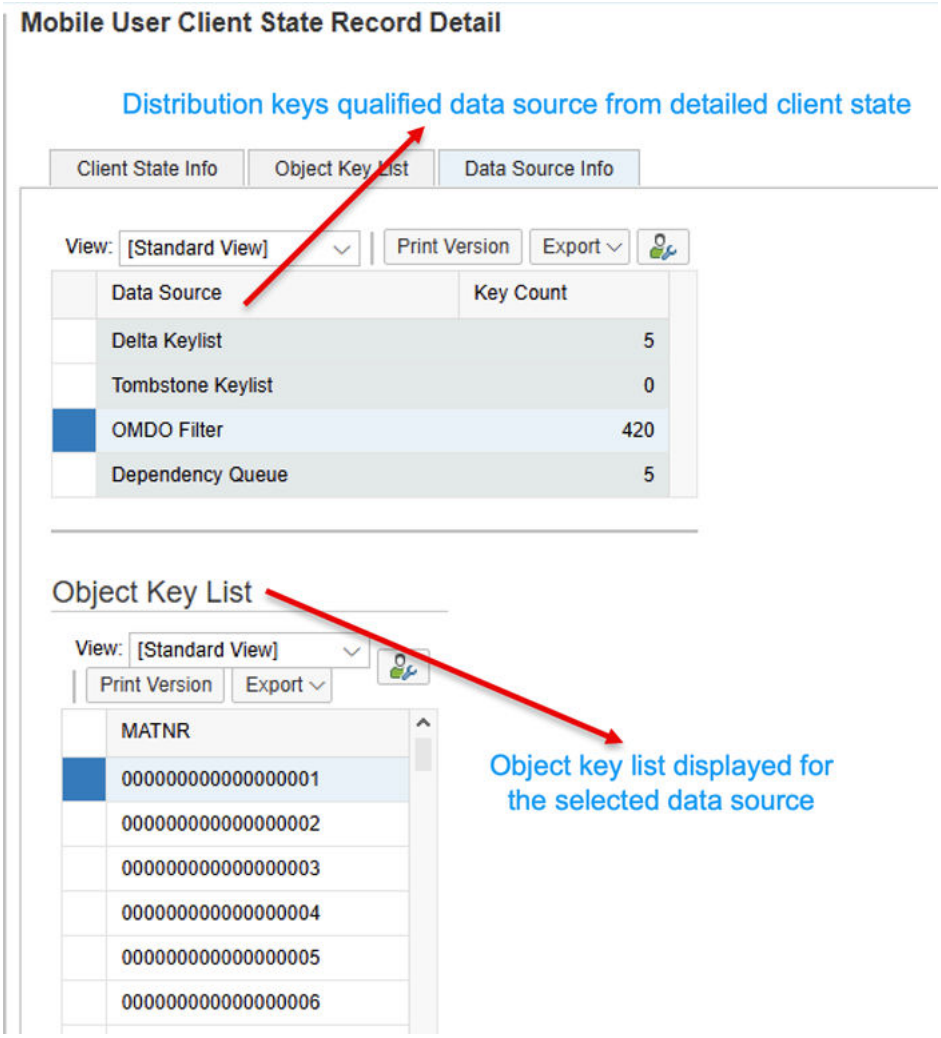
```
DETERMINE_OBSOLETE_KEYS                                       Active
    WHEN const_equip_class_entity.
      lt_distr_class = ct_distr_keylist->*-object_keylist_vlen.
      SORT lt_distr_class BY equnr.
      LOOP AT it_equi_objnr_exch_keys ASSIGNING <chg_equip>.
        READ TABLE lt_distr_class TRANSPORTING NO FIELDS "#EC PREF_LINE_EX
          WITH KEY equnr = <chg_equip>-equnr BINARY SEARCH.
        IF sy-subrc = 0.
          lv_index = sy-tabix.
        ENDIF.
        LOOP AT lt_distr_class ASSIGNING FIELD-SYMBOL(<exch_class>) FROM lv_index.
          IF <exch_class>-equnr <> <chg_equip>-equnr.
            EXIT.
          ENDIF.
          CONCATENATE <exch_class>-objek <exch_class>-equnr <exch_class>-mafid <exch_class>-klart <exc
          lv_object_key = shift_right( lv_object_key ).
          READ TABLE it_delta_keylist->*-object_keylist_vlen TRANSPORTING NO FIELDS "#EC PREF_LINE_EX
            WITH KEY table_line = lv_object_key BINARY SEARCH.
          IF sy-subrc <> 0.
            APPEND INITIAL LINE TO ct_del_keylist->*-object_keylist_vlen ASSIGNING FIELD-SYMBOL(<del_
            <del_class_key> = lv_object_key.
            DELETE ct_distr_keylist->*-object_keylist_vlen WHERE table_line = lv_object_key.
          ENDIF.
        ENDLOOP.
      ENDLOOP.
```

3. **Configuration through the Admin Portal:** For oMDOs enabled with the Lead Entity Based Flow feature, detailed client states are available, in addition to client states.
   a. Enter transaction code */SYCLO/ADMIN* in the SAP GUI.
   The Administration Portal appears in your browser.

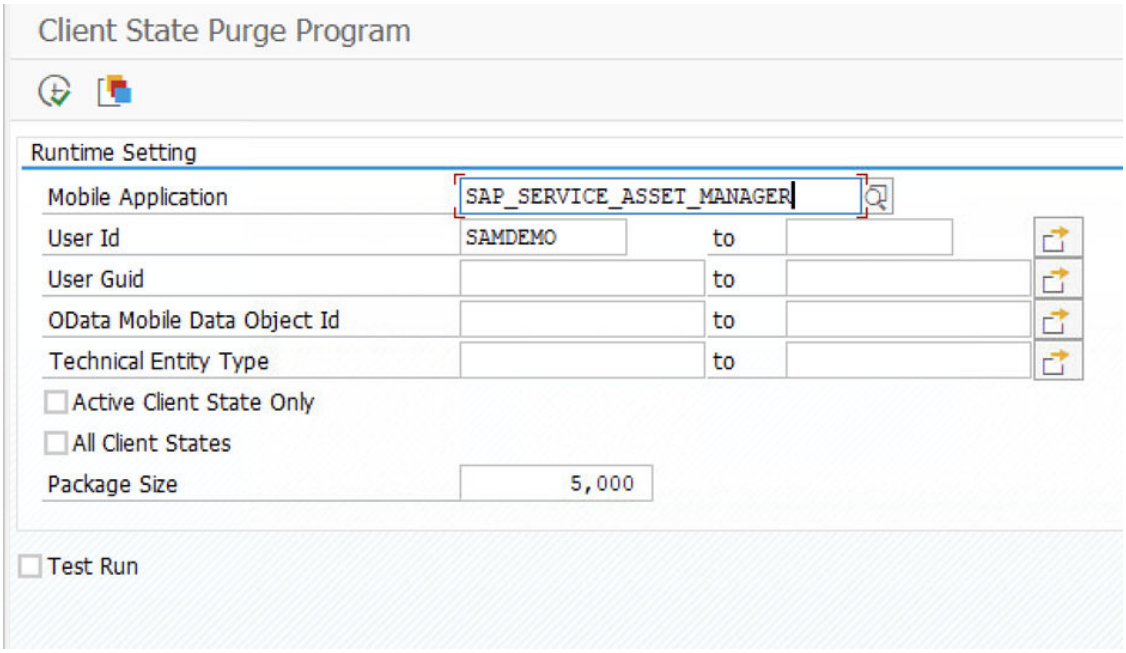
b. Navigate to the *Monitoring* page, then click *Client State Monitor*.

c. Click the *Data Source Info* tab.



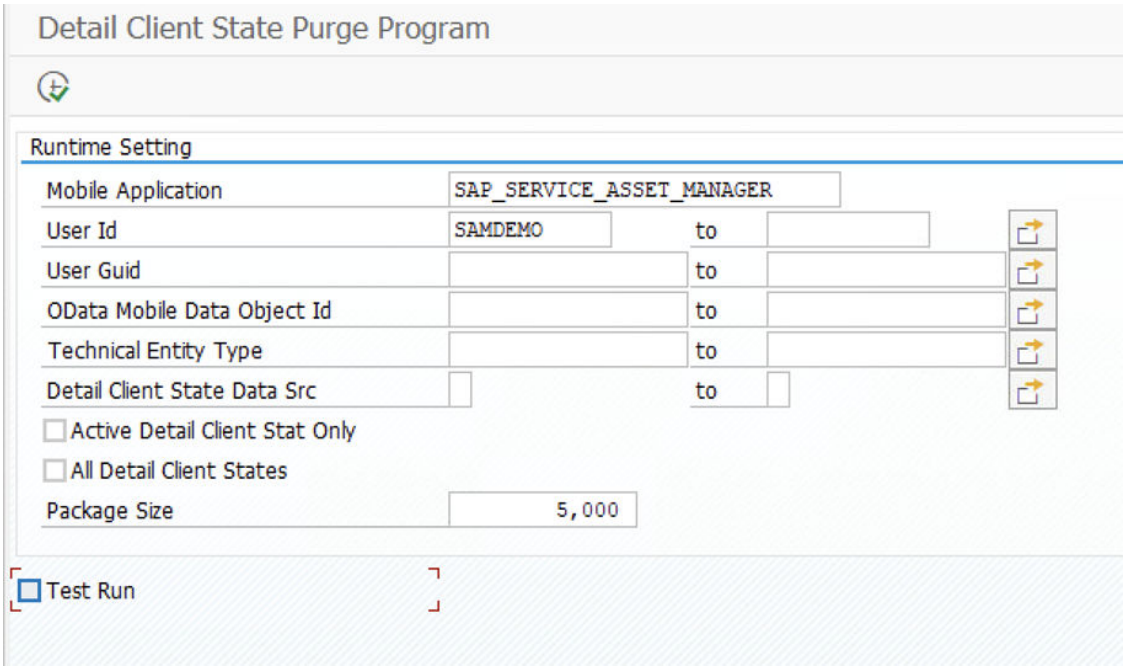


4. **Configuring Purge Reports**: See the chapter in the *Administration Guide* for instructions on how to access reports, as well as general information about all available reports.
    a. **Client State Purge Report:** If the implementation uses Standard Flow using Key List, standard client states are generated and consumed by the application. Standard client states are saved in the */MFND/D_CLNTSTAT* database table. For optimum system performance, configure the purge job as follows:
        - **Report Program:** /MFND/CORE_CLNT_ST_PURGE_PROG
        - **Authorizations:**
            - **OBJECT:** /SMFND/A01
            - **ID:** /SMFND/APP
            - **FIELD:** <MOBILE_APP>
            - **ID:** ACTVT
            - **FIELD:** 06
        - **Execution Type:** Background (JOB)
        - Runtime values for report



b. **Detailed Client State Purge Report:** If your implementation uses Lead Entity Based Flow, detailed client states are generated and consumed by the application. Detailed client states are saved in the */MFND/D_DTCLNTST* database table. For optimum system performance, configure the purge job as follows:

- **Report Program:** /MFND/CORE_DTL_CLNT_ST_PURGE
- **Authorizations:**
  - **OBJECT:** /SMFND/A01
  - **ID:** /SMFND/APP
  - **FIELD:** <MOBILE_APP>
  - **ID:** ACTVT
  - **FIELD:** 06
- **Execution Type:** Background (JOB)
- Runtime values for report



Next Steps

If your mobile users have synced using a previous configuration, they must reset their mobile app on their device.

6 Appendix

6.1 Supported SAP Transaction Codes for SAP Service and Asset Manager

SAP Service and Asset Manager uses the SAP back end and specific SAP ERP transaction codes to help configure the application.

Transaction Codes	Definition	Persona
IW21	Create notifications	Maintenance Technician
IW22	Edit notifications	Maintenance Technician
IW23	Display notifications	Maintenance Technician
IW31	Create work orders	Maintenance Technician
IW32	Edit work orders	Maintenance Technician
IW33	Display work orders	Maintenance Technician
IW51	Create service notification	Maintenance Technician
IW52	Change service notification	Maintenance Technician
IW53	Display service notification	Maintenance Technician
CAT2	Record time entries	Maintenance Technician
IE03	Display equipment BOM	Maintenance Technician
IE13	Display functional location BOM	Maintenance Technician
IL03	Display functional location	Maintenance Technician
MM03	Display material	Maintenance Technician
IK13	Display measurement document	Maintenance Technician
IK12	Change measurement document	Maintenance Technician
IK11	Create measurement document	Maintenance Technician
IW41	Create PM confirmation	Maintenance Technician
MIGO	Goods issue for work orders	Maintenance Technician

Transaction Codes	Definition	Persona
CV01N	Create DMS document	Maintenance Technician
CV03N	Display DMS document	Maintenance Technician
OAOR	Manage BDS document	Maintenance Technician
ES55	Create connection object (technical master data for meter transactions)	Maintenance Technician
ES56	Change connection object (technical master data for meter transactions)	Maintenance Technician
ES57	Display connection object (technical master data for meter transactions)	Maintenance Technician
ES60	Create premise (technical master data for meter transactions)	Maintenance Technician
ES61	Change premise (technical master data for meter transactions)	Maintenance Technician
ES62	Display premise (technical master data for meter transactions)	Maintenance Technician
ES30	Create installation (technical master data for meter transactions)	Maintenance Technician
ES31	Change installation (technical master data for meter transactions)	Maintenance Technician
ES62	Display installation (technical master data for meter transactions)	Maintenance Technician
ES65	Create device location (technical master data for meter transactions)	Maintenance Technician
ES66	Change device location (technical master data for meter transactions)	Maintenance Technician
ES67	Display device location (technical master data for meter transactions)	Maintenance Technician
EG04	Create register group (device management for meter transactions)	Maintenance Technician
EG05	Change register group (device management for meter transactions)	Maintenance Technician
EG06	Display register group (device management for meter transactions)	Maintenance Technician
EG01	Create device category (device management for meter transactions)	Maintenance Technician
EG02	Change device category (device management for meter transactions)	Maintenance Technician
EG03	Display device category (device management for meter transactions)	Maintenance Technician

Transaction Codes	Definition	Persona
IQ01	Create meter (device management for meter transactions)	Maintenance Technician
IQ02	Change meter (device management for meter transactions)	Maintenance Technician
IQ03	Display meter (device management for meter transactions)	Maintenance Technician
EG31	Full installation (device management for meter transactions)	Maintenance Technician
EG33	Technical installation (device management for meter transactions)	Maintenance Technician
EG32	Full removal (device management for meter transactions)	Maintenance Technician
EG36	Technical removal (device management for meter transactions)	Maintenance Technician
EG30	Full replacement (device management for meter transactions)	Maintenance Technician
EL40	Change street route (device management for meter transactions)	Maintenance Technician
EL41	Display street route (device management for meter transactions)	Maintenance Technician
EL42	Display meter reading units (device management for meter transactions)	Maintenance Technician
EL01	Individual meter reading order create (device management for meter transactions)	Maintenance Technician
EL06	Mass meter reading order creation (device management for meter transactions)	Maintenance Technician
EC85	Create disconnection document (disconnection/reconnection)	Maintenance Technician
EC86	Change disconnection document (disconnection/reconnection)	Maintenance Technician
QA03	Display inspection lot/EAM checklist	Maintenance Technician
QA11	Usage decision recording for inspection lot/EAM checklist	Maintenance Technician
QE01	Results recording for inspection lot/EAM checklist	Maintenance Technician
QE03	Display results for inspection lot/EAM checklist	Maintenance Technician
QE51N	Inspection lots/EAM checklist (results recording)	Maintenance Technician
QE11	Results recording for inspection points for QM inspection lots	Maintenance Technician

Transaction Codes	Definition	Persona
QE72	Tabular results recording for inspection lots/EAM checklist	Maintenance Technician
QF31	Defects recording for characteristics	Maintenance Technician
QS24	Display master inspection characteristics	Maintenance Technician
IE01	Create equipment	Maintenance Technician Field Service Technician
IE02	Change equipment	Maintenance Technician Field Service Technician
IL01	Create functional location	Maintenance Technician Field Service Technician
IL02	Change functional location	Maintenance Technician Field Service Technician
WCT8	Display operational work clearance document (safety certificate)	Safety Technician
WCT7	Change operational work clearance document (safety certificate)	Safety Technician
WCTM	Display work clearance application (work permit)	Safety Technician
WCTL	Change work clearance application (work permit)	Safety Technician
MIGO	All the goods movements such as: • Goods receipt • Goods issues • Stock transfers • Transfer postings • Goods issues for scrap • Cancellation and reversals • Vendor returns	Inventory Clerk
MIGO / MB1B	Transfer posting	Inventory Clerk
MIGO / MB1A	Miscellaneous goods issue	Inventory Clerk
MB23	Display reservation	Inventory Clerk
VL02N and VL03N	Outbound delivery display and PGI	Inventory Clerk
VL32N and VL33N	Inbound delivery display and PGR	Inventory Clerk
CO03	Display production order	Inventory Clerk

Transaction Codes	Definition	Persona
ME23N	Display purchase order Display stock transport order (STO)	Inventory Clerk
MI01	Create physical inventory	Inventory Clerk
MI03	Display physical inventory	Inventory Clerk
MI04	Enter inventory count	Inventory Clerk
MI05	Change inventory count	Inventory Clerk
ME51	Create purchase requisition	Inventory Clerk
/SCWM/MON	Warehouse Management Monitor	Extended Warehouse Clerk
/SCWM/PRDI	Maintain Inbound Delivery	Extended Warehouse Clerk

6.2 User Parameter IDs

User Parameter IDs are used to filter data that mobile users download when they perform a sync. By setting the Parameter IDs for users, you can define which assignment types technicians will receive and which activities they have to complete on their mobile devices. To update these IDs in your user profile, perform the following steps:

1. Use the transaction code *SU3* on the SAP GUI.
2. Select the *Parameters* tab.
3. In the list of parameters you can add a new row or modify/delete existing ones.

> **Note**
>
> - To display other users' Parameter IDs, use the transaction code *SU01D* on the SAP GUI.
> - You need authorization to edit the list of User Parameter IDs for other users.
> - User Parameter IDs are updated **only** in case of initial sync, not delta sync.

List of User Parameter IDs

The following table lists all User Parameter ID values available in SAP Service and Asset Manager:

User Parameter ID	Description
AGR	Work center
SWK	Maintenance plant

User Parameter ID	Description
VAP	Main work center for maintenance tasks
WRK	Plant
IWK	Maintenance planning plant
CAC	Controlling area
IHG	Maintenance planner group
KOS	Cost Center
LAG	Storage location
PBR	Personnel Area
RVK	Reference sales organization

> **Note**
>
> For more information about which assignment types require User Parameter IDs, see:
>
> - Work Order Assignment Type Options [page 150]
> - Notification Assignment Options [page 154]

6.3 Mobile Application Integration Framework Configurations

> **Note**
>
> - This section includes feature configurations that you need to perform in the Mobile Application Integration Framework (MAIF), but are specific to SAP Service and Asset Manager. Therefore, these documents are only a subset of MAIF configuration procedures. For the complete documentation, refer to *MAIF Configuration Guide*.
> - Please note that all Mobile Application Integration Framework documentation in this section will be removed from *SAP Service and Asset Manager Configuration Guide* and you will be able to find all such content on the Mobile Application Integration Framework (MAIF), Private Cloud help portal page.

6.3.1 Accessing the SAP Mobile Add-On for SAP Configuration Panel

Context

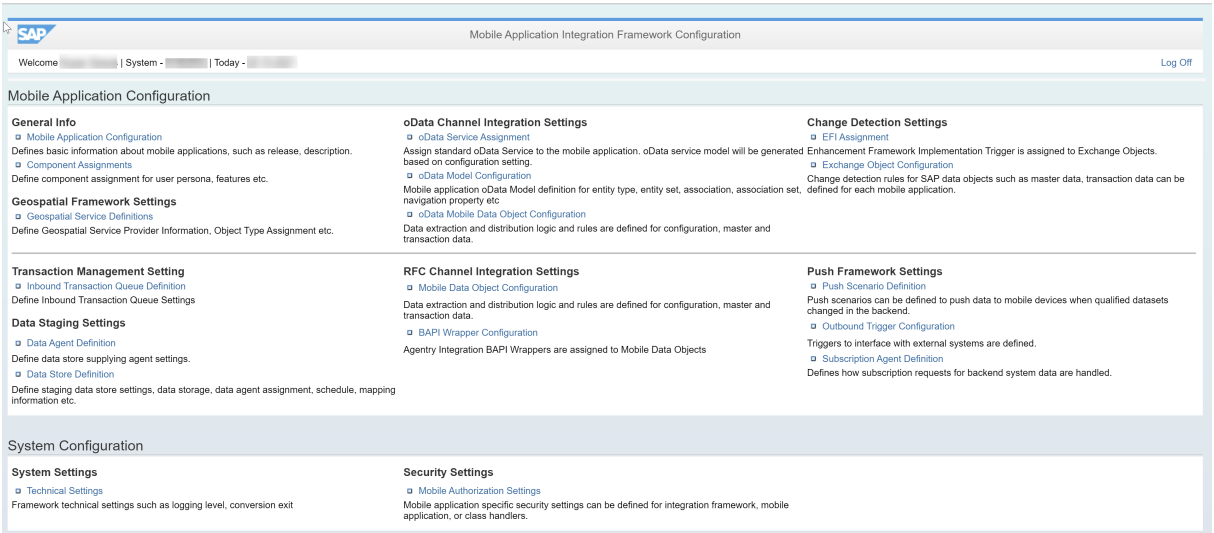
You can access the Configuration Panel either through SAP Customizing or using a transaction code directly. First, log into your back-end system, and then you can choose from the following two options:

Procedure

1. To access the ConfigPanel through *Customizing*, enter the transaction *spro* to open the *Customizing: Execute Project* screen. Select the *SAP Reference IMG* tab. Using the *SAP Customizing Implementation Guide* list, select *Agentry SAP Framework Configuration* > *System Settings* > *Define Mobile Applications*.
2. To access the ConfigPanel using a direct transaction code shortcut, enter */n/syclo/configpanel*.

Results

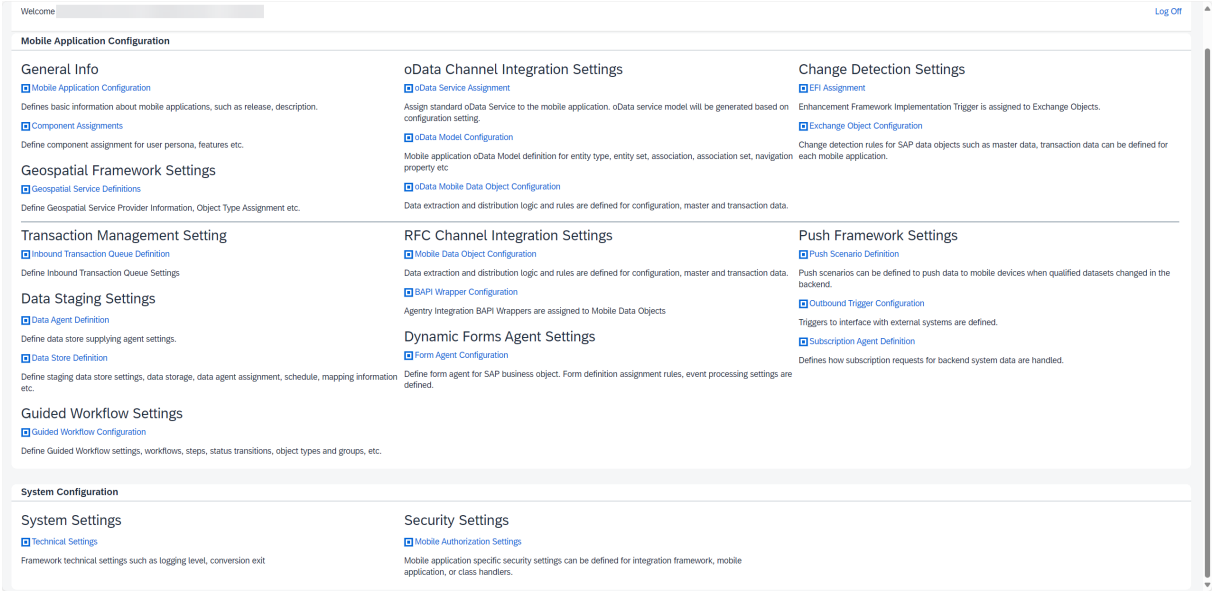
The *Mobile Application Integration Framework* home page is displayed in a browser.



6.3.2 Panels, Tabs, and Field Descriptions

Perform configuration activities for your app through the ConfigPanel.

Customization changes you make via the ConfigPanel can significantly impact the behavior of your app. Always follow SAP best practices, make changes and test them in the development and quality control systems before you transport the changes into your production landscape.



- General Info Settings [page 611]
- Geospatial Service Definitions - GIS [page 618]
- OData Channel Integration Settings [page 625]
- Change Detection Settings [page 642]
-
-
- Guided Workflow Configuration [page 649]
- RFC Channel Integration Settings [page 652]
- SAP Dynamic Forms Agent Settings [page 662]
- Push Framework Settings [page 669]
- Technical Settings [page 678]
- Mobile Authorization Settings [page 680]

6.3.2.1 Standard Operations in the Configuration Panel

While configuration for each mobile application is unique, certain toolbar functions in the Configuration Panel are common and are available for all applications.

Mobile Application Filter

If more than one mobile application is available in the same system, you can use the filter function to only view items for a specific application. Find the filter option on any page where multiple applications are displayed.

To filter by application, click the arrow to the right of the *Defined Mobile Applications* field, and select the appropriate mobile application. To remove the selection and view all items for all mobile applications in the system, click in the field again and select the asterisk (*) symbol.

Creating, Copying, Deleting, and Changing Items

The following standard actions are available to configure different components and items within your mobile application setup:

- **Create:** Creates a new item. All modifiable fields are empty.
- **Copy:** Copies the item that was highlighted and creates a new item. All modifiable fields are filled in with the information from the existing item and are available for changes before saving.
- **Delete:** Deletes the highlighted item.
- **Change:** Allows you to change the highlighted item in the modifiable fields.

Saving or Canceling Changes for an Item

Once you click the *Create*, *Copy*, or *Change* button, the *Save* and *Cancel* buttons are displayed. After you change the configuration of the item, click *Save* to save the changes or *Cancel* to discard the changes.

> ⓘ Note
>
> If the *Save* and *Cancel* buttons are active, the *Home* link for the ConfigPanel is not available. Either save your changes or cancel out of the changes to return to the main Configuration Panel page

Message List

Certain actions can generate system messages. These messages can be error messages or informational messages. If you perform an action that prompts a system message, a message bar appears above the main panel with a brief description of the message.

Click the *Show List* button to display the detailed view of the message list.

6.3.2.2 General Info Settings

The following areas are used in configuring general information for the application:

- Mobile Application Configuration [page 611]
- Component Assignments [page 616]
- Mobile Transaction History [page 618]

6.3.2.2.1 Mobile Application Configuration

The Mobile Application Configuration page allows you to configure general settings for the entire mobile application.

The page contains the following tabs:

- General
- Mobile Status Setting
- Conversion Exit Setting (not used in SAP Service and Asset Manager)
- System Components (not used in SAP Service and Asset Manager)
- Parameters
- Client Globals (not used in SAP Service and Asset Manager)
- User Attributes (not used in SAP Service and Asset Manager)
  Application Persona
- Features

General Tab

Create or change basic information about a mobile application through this tab.

- **Basic Data section:** Enter the name of the mobile application in the `<Mobile Application>` field, which is limited to 40 characters. Select the type of application in the `<Type>` field. Note that for SAP Service and Asset Manager, the type is `<oData Applications>`. Enter a brief, easy to understand description in the `<Description>` field, limited to 60 characters. Type in the release number of the application in the `<Release>` field.
- **User Management Setting:** When the `<Disable Automatic User Creation>` box is checked, a new user GUID is not automatically created when a new mobile client is detected in the system. Manually create and maintain mobile users through the Administration portal.
- **Server Management Setting:** When the `<Disable Automatic Server Registration>` box is checked, a new server GUID is not automatically created when a new server is detected in the system. You must manually create and maintain servers through the Administration portal.

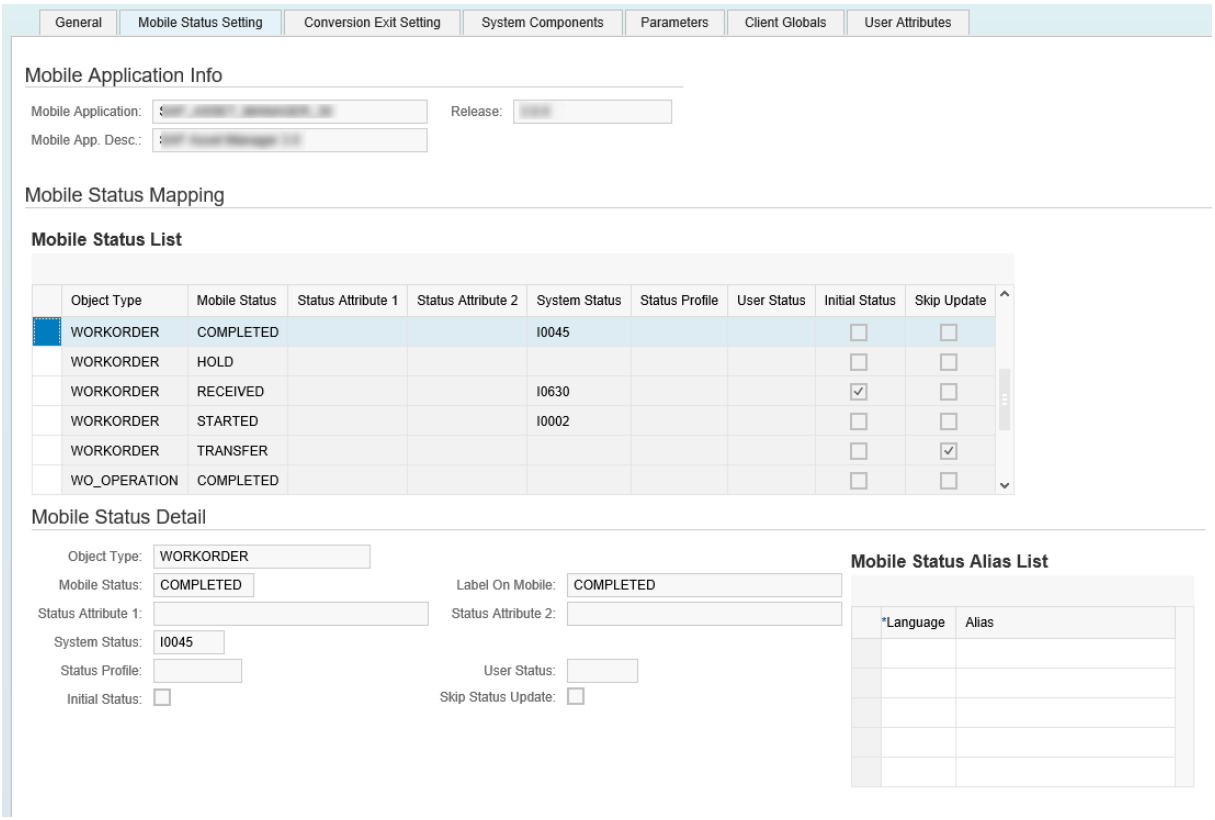
- **Life-cycle management:** When the <Application Blocked> box is checked, the mobile application is disabled. The mobile user can no longer connect to the back-end system for the mobile application, and the xChange process is also disabled. The <Effective Date> and <Time> fields flag when the change takes effect.
- **xChange Setting:** When the <Disable Change Detection> box is checked, the change detection process, or xchange process, for the application is completely disabled.
- **Inbound Transaction Management:** Not used in the SAP Service and Asset Manager application.
- **Multi Backend Setting:** When checked, enables a specific mobile application to connect to multiple SAP systems, consisting of one host server and one or more satellite servers.
- **System Role:** Dropdown menu where you can select either *Host* or *Satellite*.
  A *Host* system is the connection between SAP and the application in the SAP Business Technology Platform. The host server provides the logic to the application and functions as the bridge to the satellite server or servers. There can only be one host server per system.
  Satellite servers communicate with SAP through the host server. To complete multi backend configuration, configure the host and back-end servers using the *System Components* tab. See that section for more details.

Mobile Status Setting Tab

Use the Mobile Status Setting tab to map the available mobile statuses that an oData mobile data object (OMDO) supports on the client side. If a user status also exists for the same object type, you can link it to the mobile status and the system status through this tab.

- **Mobile Application Info:** The <Mobile Application> field is read only and is the name of the mobile application. The <Mobile Application Description> is read only and is a brief description of the mobile application. The <Release> field is read only and is the release number of the application.
- **Mobile Status Mapping:** Use the <Add Status> and <Delete Status> buttons to create and delete mobile status mappings. Fill out the <Object Type> with the specific object in the mobile application, for example, <Notification>. The <Mobile Status> is the status defined by the mobile application. The <Label on Mobile> is not used. The <User Status> is an SAP status code as defined in SAP. Note that the status codes are language independent codes.
  If the <Initial Status> checkbox is selected, the mobile status is displayed by default when you download the object to the mobile device. To skip a specific mobile status update from a mobile device, use the <Skip Update> checkbox corresponding to the mobile status object.
  Use the *Mobile Status Alias List* table to define language-specific mobile status aliases.

In the following example screen, the highlighted row in the mapping table indicates that if a user sets a work order to completed, the application sets the work order system status to I0045 in SAP.



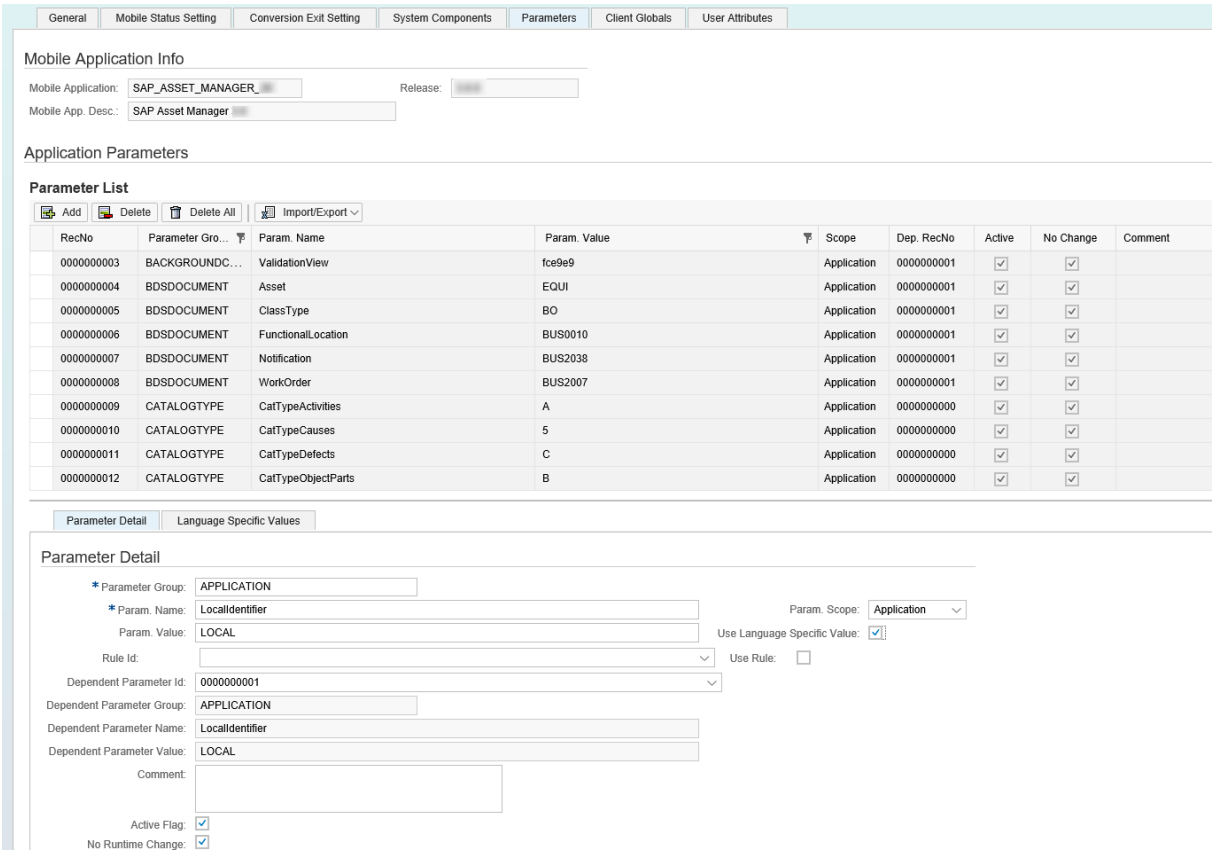
If there is no system status or user status, the mobile status only affects the mobile device and does not affect the backend SAP system.

If there is a user status specified but no status profile when the mobile user sets the mobile status, the app sets that user status for the object, disregarding the status profile of that object.

If there is a user status and status profile specified when the mobile user sets the mobile status, the app sets that user status if the object uses that status profile.

Parameters Tab

The *Parameters* tab defines system parameters.



- **Mobile Application Info:** The `<Mobile Application>` field is read only and is the name of the mobile application. The `<Mobile Application Description>` is read only and is a brief description of the mobile application. The `<Release>` field is read only and is the release number of the application.
- **Application Parameters:** Use the `<Add>` and `<Delete>` buttons to create and delete parameters.
- **Parameter Detail:** The `<Parameter Group>` is the group to which the parameter belongs. Groups are how you organize parameters. References to a parameter include both the group name and the parameter name. The `<Parameter Name>` is the unique name of the parameter.
  The `<Parameter Value>` is the currently configured value of the parameter. References to the parameter return the configured value. Use the `<Language Specific Value>` checkbox to select which parameters you wish to be language dependent. The checkbox and the corresponding *Language Specific Values* tab are only active after you have clicked the *Change* button. Note that the language available in the *Language Specific Values tab*, *Value List* table, depends on the language you are using to log into the mobile client. You must manually maintain each parameter that you wish to control for a language specific value separately.
  Set the `<Parameter Scope>` to one of the following options:
  - Mobile Application: Value for all users of the application
  - Mobile User: Value you can override for individual users. To override a parameter value of a user, see the Administration & Monitoring Portal on parameters

> ### Note
>
> For information on setting user parameters, see the following security guides, depending on your back end system:
>
> - Mobile Add-On for ERP Security Guide

- Mobile Add-On for S/4HANA Security Guide

The <Rule ID> field contains the rule used at runtime. If you check the <Use Rule> box, the rule in the <Rule ID> field is active.
Check the <Active Flag> box to ensure that the parameter is used by the mobile application. Inactive parameters are not used by the application. When you check the <No Runtime Change> box, you cannot override the value of the parameter. The configured value is always the value. If the box is not checked, the parameter values can be overridden at runtime through synchronization processing.

Application Persona Tab

The persona selected determines the data that is downloaded to the mobile client.

Mobile Application Info

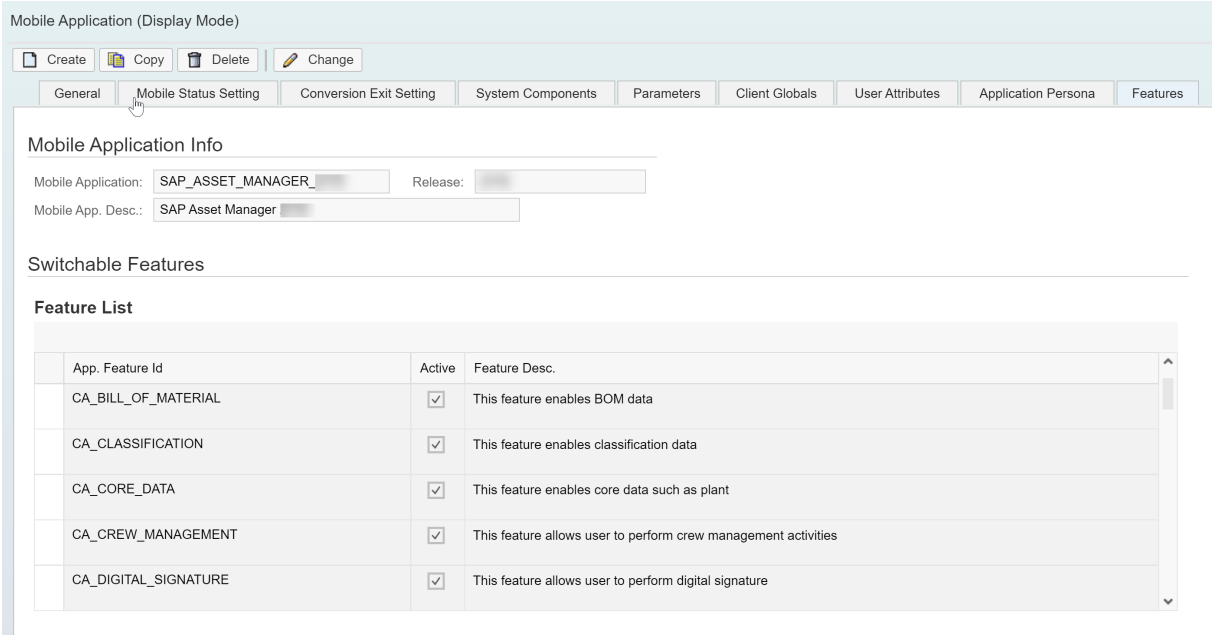
Read-only information about the application.

Application Personas

- Auto Determination Rule:
- Persona List: The following personas are standard in an SAP Service and Asset Manager installation:
  - MAINTENANCE_TECHNICIAN (default)
  - INVENTORY_CLERK

Features Tab

Switchable features allow you to configure various components into features. Feature assignment determines the data that is downloaded to the mobile client.



Mobile Application Info

Read-only information about the application.

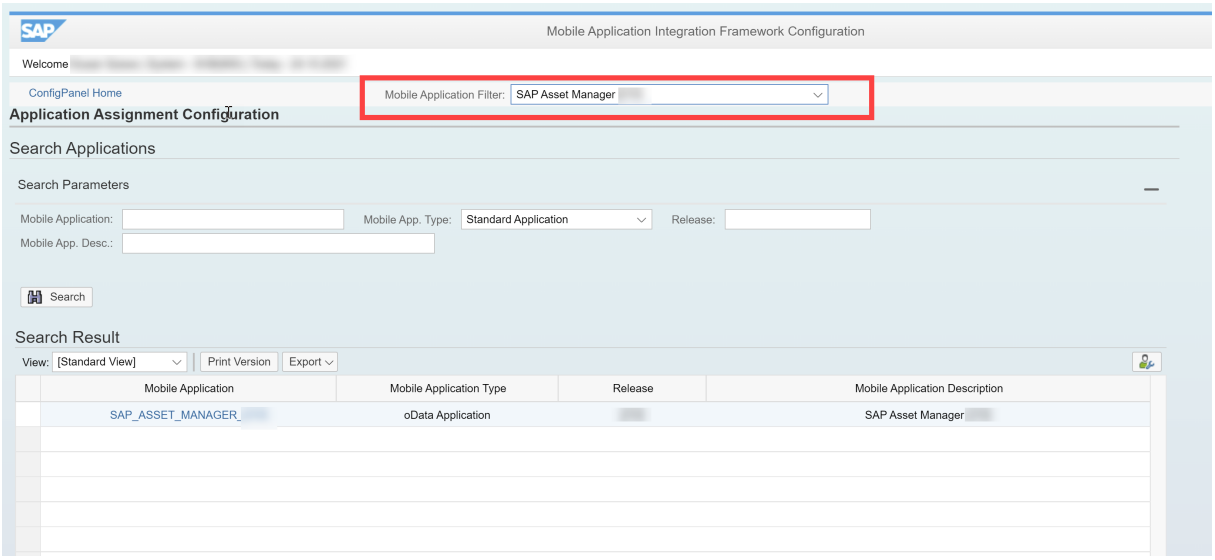
Switchable Features

Check or uncheck a feature from the feature list to enable or disable it.

6.3.2.2.2 Component Assignments

The *Component Assignments* page allows you to configure persona and feature assignments.

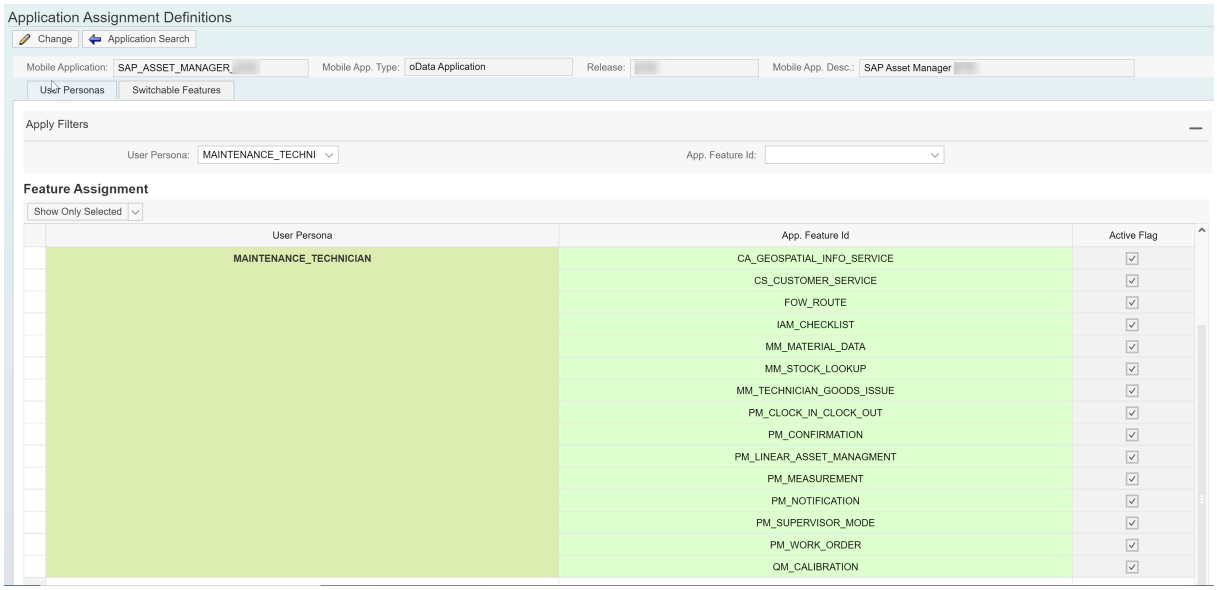
Use the *Mobile Application Filter* field to select your application. Then, click the application hyperlink in the *Search Results* table.



User Personas Tab

Use the *Apply Filters* section to filter for a specific persona or specific features. In the following example, we've filtered for all features that belong to the *MAINTENANCE_TECHNICIAN* persona.

The *Feature Assignment* section shows you the filtered results. Use the drop-down menu to further filter your selections. For example, we've chosen to display only active, or selected features for the maintenance technician persona.



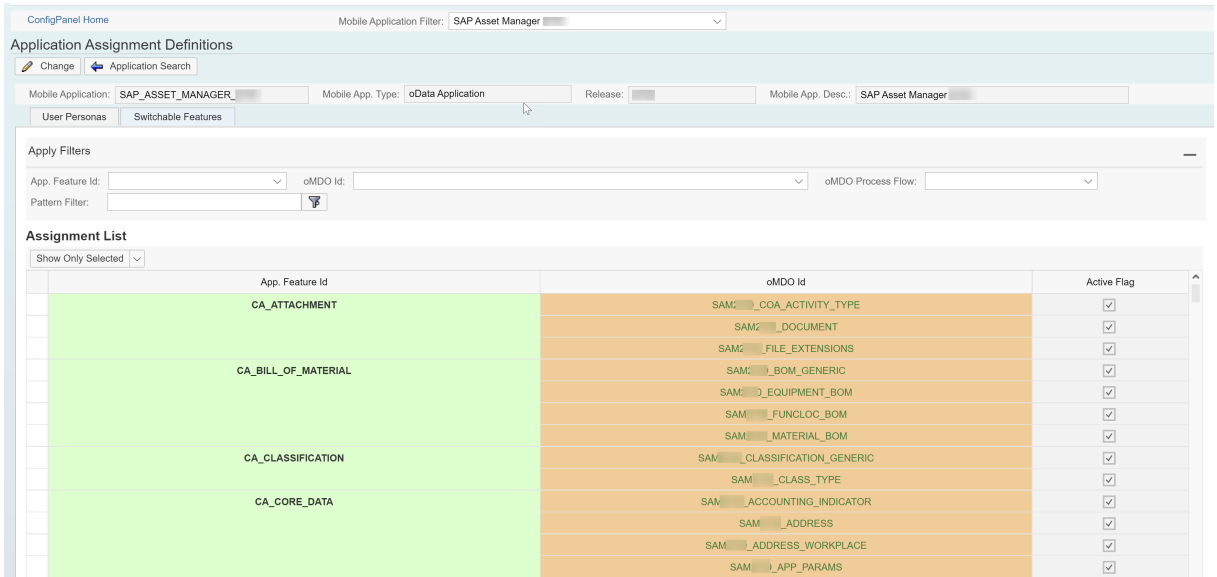
Switchable Features Tab

The *Switchable Features* tab allows you to configure OMDOs required for each feature. During initial and delta syncs, the mobile client only downloads data from the assigned OMDOs.

Use the *Apply Filters* section to filter for a specific OMDO or feature ID.

The *Assignment List* section shows you which OMDOs are assigned and active (or not active) with a feature.

> ### Note
>
> Don't select OMDOs that belong to the online service (ex: */MERP/SAP_ONLINE_LOOKUP_EXT_<version>*). These online service entities might not exist in the base service (*/MERP/SAP_SRV_ASSET_MGR_<XXXX>_REF*).



6.3.2.2.3 Mobile Transaction History

With the *Mobile Transaction History* feature, SAP introduces the possibility for users to record all successful *CREATE* and *UPDATE* transactions from the mobile device in to the */SYCLO/MBL02* table. This provides insight into which objects are either created or changed via the mobile application, by whom, and when the changes are made.

To enable mobile transaction history logging for your mobile app, use one of the following options:

1. On the Mobile Application Configuration page (transaction `/n/SYCLO/CONFIGPANEL`), select the *Enable Mobile Transaction History* check box.
2. Run the program `/SYCLO/CORE_RUNTIME_PARAM_PROG`, select your mobile application and the parameter *ENABLE_MTRAN_HIST*.

> **Note**
>
> If you specify a user ID, only transactions for that user will be logged. Otherwise, the runtime parameter will be applied to all users using the application.

To view and search mobile transaction history in the Syclo admin panel (transaction `/n/SYCLO/ADMIN`) through the *Mobile Transaction History Monitor* application:

- Open the transaction, click the *Monitoring* tab and select *Mobile Transaction History Monitor*
- Select a mobile application and view the mobile transaction history for this application.

> **Note**
>
> Use the *oMDO Id* and *Technical Entity Type* filters to filter by object type, and the *Object Key* filter to display individual objects.

> **Note**
>
> To remove records from the *Mobile Transaction History* table, you can use the `/SYCLO/CORE_MTRAHIS_PURGE_PROG` report.

6.3.2.3 Geospatial Service Definitions - GIS

A geographic information system (GIS) integrates hardware, software, and data for capturing, managing, analyzing, and displaying all forms of geographically referenced information.

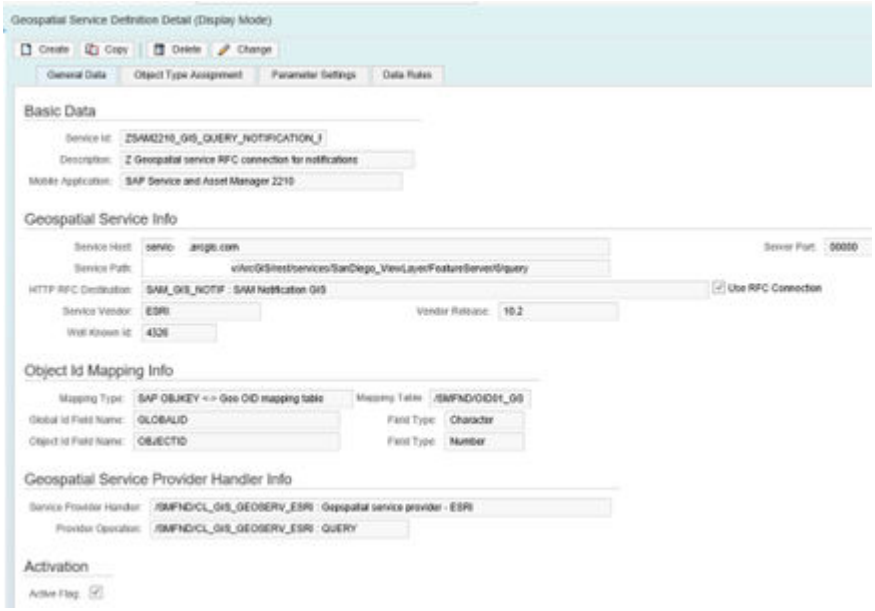
> **Note**
>
> GIS is enabled by default. See the Geospatial Service Definitions - GEF [page 623] topic if you are using GEF (SAP Geographical Enablement Framework).

Geospatial data plays an important part in the daily operations of many organizations. By adding geospatial data to the technical data of an asset, you get a full picture of that asset.

The *Geospatial Service Definitions* page contains the following tabs:

- General Data
- Object Type Assignment
- Parameter Settings
- Data Rules

General Data Tab



General Data tab:

Basic Data

- **Service ID:** Required field. Name of the geospatial service ID, limited to 40 characters, with namespace protection. Use the Y or Z namespace.
- **Description:** Description of the geospatial service
- **Mobile Application:** Mobile application of the geospatial service. Every geospatial service is assigned to a specific mobile application.

Geospatial Service Info

- **Service Host:** Host name of the geospatial service provider

  > **Note**
  >
  > The information in this field is used in the `Target Host` field in the Creating and Configuring an RFC Destination for Offline Maps [page 430] procedure.

- **Server Port:** Port number of the geospatial service provider
- **Service Path:** End-point URL of the geospatial service (it is unique for each technical object)

- **HTTP RFC Destination:** RFC destination pointing to the GIS. By using the RFC destination, you can support various logon authentication methods of the geospatial service. If you use an RFC destination, service host, port, and path are not required.
- **Use RFC Destination:** Indicator that you must use an RFC destination to connect to GIS
- **Service Vendor:** Vendor name of the GIS provider.SAP uses Esri for its out of the box installation of the SAP Service and Asset Manager application.
- **Vendor Release** Version information of the GIS provider. The Esri version for SAP Service and Asset Manager is *ArcGIS iOS SDK 200.5.1* for iOS and *ArcGIS Runtime SDK for Android 200.3.0* for Android.
- **Well Known ID:** Well-known ID of the coordinate system

Object ID Mapping Info

- **Mapping Type:** Defines how the SAP object ID is mapped to the object ID in the geospatial service provider database. Select from the following:
  - **No mapping:** SAP object ID is the same as the object ID in the GIS provider database
  - **SAP OBJKEY <-> GEO OID-mapping table:** Mapping is stored in a mapping table
  - **Lookup Routing:** Use a lookup ABAP object-oriented class to determine the mapping dynamically. The ABAP object-oriented lookup class must implement the `/SMFND/IF_GIS_OID_MAPPING` interface.
- **Mapping Table:** SAP mapping table name, if used. The standard `/SMFND/OID01_GS` mapping table is the default. The standard `/SMFND/GIS_OIDMAP_UPLOAD_PROG` program is provided to load the table with a text file
- **Object ID Lookup Routine:** OID lookup routine name, if used. Used in conjunction with the *Lookup Routing* mapping type
- **Global ID Field Name:** Name of the Global ID field in the GIS provider database, if relevant. For example, in the Esri database, the global field name is *GLOBALID*
- **Object ID Field Name:** Name of the `<Object ID>` field in the GIS provider database, if relevant. For example, in the Esri database, the field name is *OBJECTID*
- **Field Type** Use the dropdown to select the type of field for both the `<Global ID>` and the `<Object ID>`
- **Service Provider Handler:** ABAP object-oriented class that handles integration to the GIS provider
- **Provider Operation:** ABAP OO class operation that handles integration to the GIS service provider.

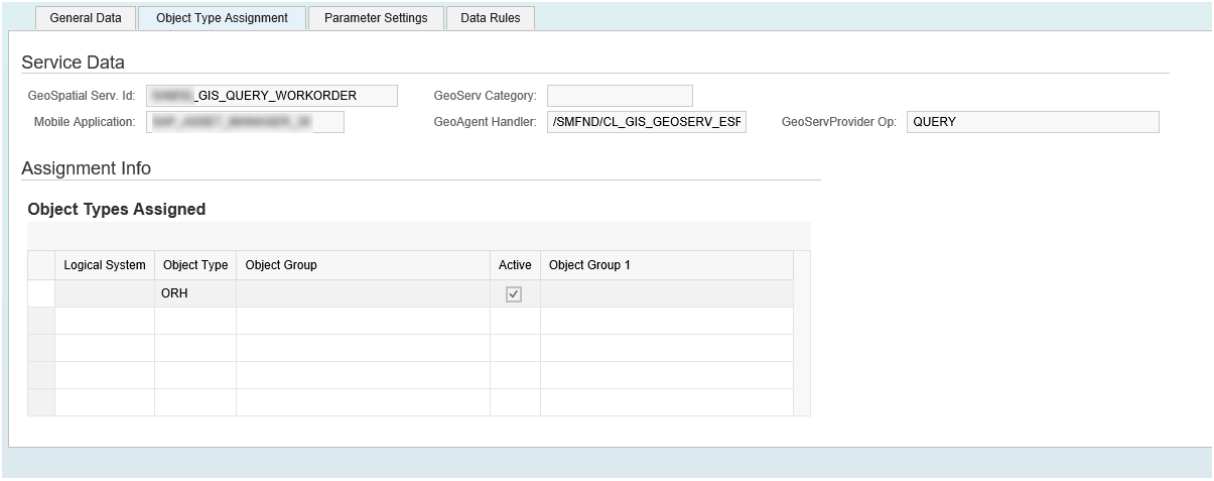
Activation

- **Active Flag** Check the checkbox to activate the GIS query service

Object Type Assignment Tab

Use the *Object Type Assignment* tab to define what type of SAP objects are assigned to the geospatial service. You can define different geospatial services for different SAP object types.

For example, you can map equipment with polygon geospatial data to one geospatial feature layer. You can then map equipment with point geospatial data to a different geospatial feature layer.

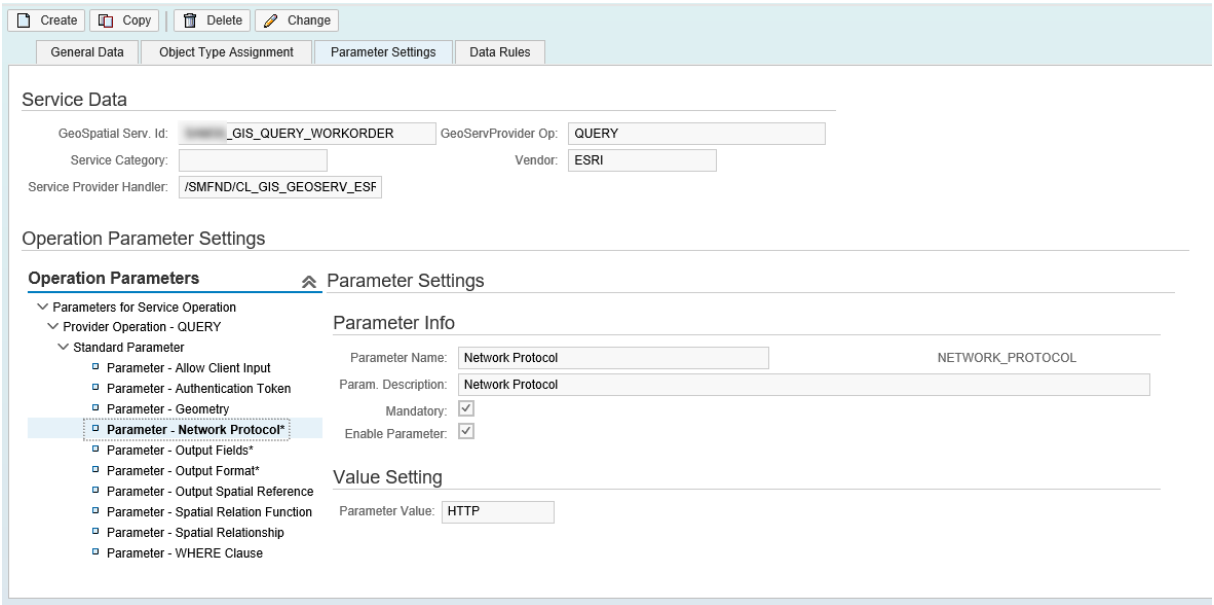


Assignment Info

- **Logical System:** Logical system of the SAP object. A logical system is required to properly identify the SAP object if the mobile add-on aggregates data from different back-end systems.
- **Object Type:** Type of the object as it is identified in the mobile add-on. For example, the standard object type *IEQ* is used to identify the *Equipment* object.
- **Object Group:** Optional setting used to further group the objects in the same object type.
- **Active:** When the *Active* checkbox is marked, the assignment is active.
- **Object Group 1:** Optional setting used to further group objects of the same object type and object group.

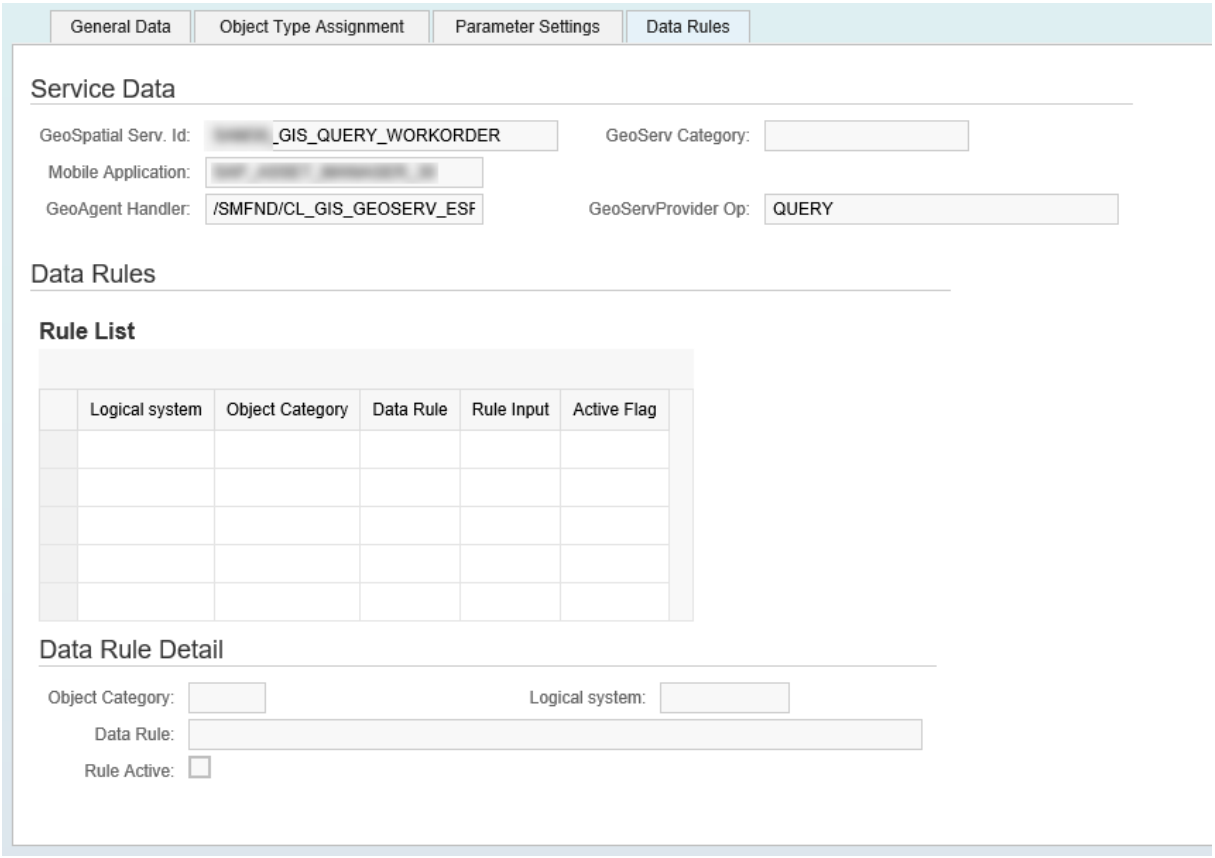
Parameter Settings Tab

Use the *Parameter Settings* tab to define parameter settings for the service provider handler. The service provider handler can declare the list of parameters that might require input. If parameters are declared, they are displayed on this tab, and you can enter values for them.



Data Rules Tab

Use the *Data Rules* tab to define data rules. A data rule is used to transform input data to the service provider handler, before calling the geospatial service. For example, to dynamically assign values of object type, object group, and object group 1 to input data, use a data rule. Using a data rule influences which geospatial service is assigned to an input object.



Data Rule Detail

- **Object Category:** Type of the object as it is identified in the mobile add-on. For example, you can use the standard object type *IEQ* to identify the *Equipment* object.
- **Logical System:** Logical system of the SAP object. If the mobile add-on aggregates data from different back-end systems, the logical system is required to identify the object.
- **Data Rule:** Data rules are ABAP OO classes that implement the `/SMFND/IF_GIS_DATA_RULE` interface.
- **Rule Active:** If the checkbox is checked, the rule is active.

6.3.2.4 Geospatial Service Definitions - GEF

The SAP Geographical Enablement Framework (GEF) enables the augmentation of business data with spatial attributes for SAP S/4HANA applications. The framework allows SAP data to be used in GIS-based geo-processing operations.

> **Note**
>
> GIS is enabled by default. See the topic if you're using GIS (Geographical Information System).

GEF reduces, and in some cases, eliminates the need for complex synchronization between SAP and GIS systems. Business data can be combined with engineering data in a single map view independent of the user working with SAP tools or GIS tools, decreasing TCO, increasing the value of business data, and simplifying user interaction.

The framework provides an embeddable map-based UI for SAP S/4HANA applications to quickly geo-enable their business objects and support geospatial processes. It also exposes the geometries and attributes of geo-enabled SAP business objects as feature classes to be consumed via standard GIS tools.

The *Geospatial Service Definitions* page contains the following tabs:

- General Data
- Object Type Assignment
- Parameter Settings
- Data Rules

General Data Tab

As GEF is integrated directly to SAP S/4HANA systems, there's no need to call REST APIs outside of SAP S/4HANA. All information and coordinates are already stored as part of the system.

General Data tab:

Basic Data

- **Service ID:** Required field. Name of the geospatial service ID, limited to 40 characters, with namespace protection. Use the Y or Z namespace.
- **Description:** Description of the geospatial service
- **Mobile Application:** Mobile application of the geospatial service. Every geospatial service is assigned to a specific mobile application.

Geospatial Service Info

- **Service Host:** Automatically set to *NO_HOST_NAME*
- **Server Port:** Port number of the geospatial service provider
- **Service Path:** Automatically set to *NO_SERVICE_PATH*
- **HTTP RFC Destination:** RFC destination pointing to the GIS. By using the RFC destination, you can support various logon authentication methods of the geospatial service. If you use an RFC destination, service host, port, and path are not required.

- **Use RFC Destination:** Indicator that you must use an RFC destination to connect to GIS
- **Service Vendor:** Vendor name of the GIS provider. For GEF, automatically set to SAP.
- **Vendor Release** Not required for GEF
- **Well Known ID:** Not required for GEF

Object ID Mapping Info

- **Mapping Type:** Automatically set to *No Mapping*. Objects are directly integrated to GEF.
- **Global ID Field Name:** Not used for GEF
- **Object ID Field Name:** Automatically set to *GEF_OBJECTID*. Only used for visibility into which field is used.
- **Field Type** Use the dropdown to select the type of field for both the `<Global ID>` and the `<Object ID>`
- **Service Provider Handler:** Automatically populated with `/MERP/CL_CORE_GIS_GEOSERV_GEF`

  > **Note**
  >
  > Custom handlers are supported.

- **Provider Operation:** Automatically populated with `/MERP/CL_CORE_GIS_GEOSERV_GEF`

Activation

- **Active Flag** Check the checkbox to activate the GEF query service

Object Type Assignment Tab

Use the *Object Type Assignment* tab to define what type of SAP objects are assigned to the geospatial service. You can define different geospatial services for different SAP object types.

For example, you can map equipment with polygon geospatial data to one geospatial feature layer. You can then map equipment with point geospatial data to a different geospatial feature layer.

Assignment Info

- **Logical System:** Logical system of the SAP object. A logical system is required to properly identify the SAP object if the mobile add-on aggregates data from different back-end systems. You can configure the following fields on the
- **Object Type:** Type of the object as it is identified in the mobile add-on. For example, the standard object type *IEQ* is used to identify the *Equipment* object.
- **Object Group:** Optional setting used to further group the objects in the same object type.
- **Active:** When the *Active* checkbox is marked, the assignment is active.
- **Object Group 1:** Optional setting used to further group objects of the same object type and object group.

Parameter Settings Tab

Use the *Parameter Settings* tab to define parameter settings for the service provider handler. The service provider handler can declare the list of parameters that might require input. If parameters are declared, they're displayed on this tab, and you can enter values for them.

There are two standard parameters: EAM Scenario and Output Format

The *EAM Scenario* parameter data mines the GEF scenario object. For each scenario, there's a corresponding business object:

EAM Scenario ID	GEF Business Object ID
EAM Equipment EAMS_EQUI	EAMEQUI
EAM Functional Location EAMS_FLOC	EAMFLOC
EAM Maintenance Notification EAMS_NOTIF	EAMNTF
EAM Maintenance Order EAMS_ORDER	EAMORD

You can assign different business objects for your system needs.

Output Format: The only supported parameter value is JSON.

Data Rules Tab

The *Data Rules* tab isn't used in GEF configuration.

6.3.2.5 OData Channel Integration Settings

6.3.2.5.1 OData Service Assignment

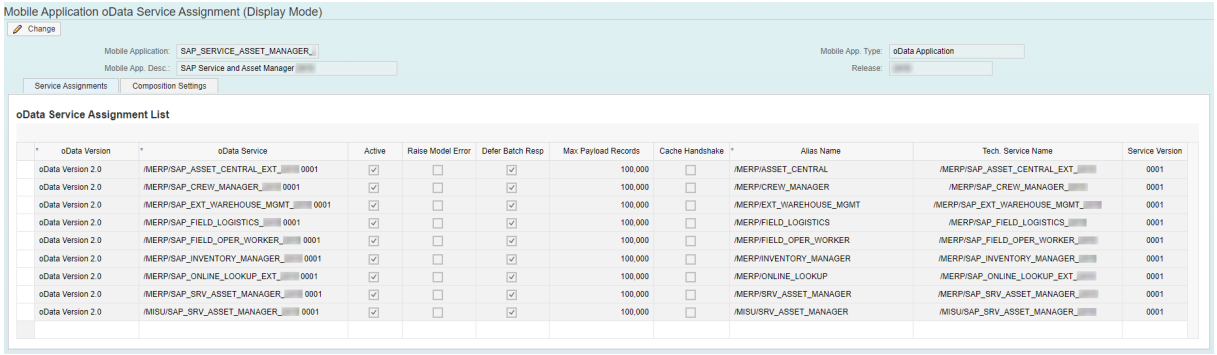
Gateway OData services implemented using the Mobile Integration Framework for SAP are different from the typical Gateway OData services.

The following requirements must be met for the Gateway OData services:

- Define the Gateway OData technical model using the generic model provider class of the Mobile Integration Framework `/MFND/CL_CORE_ODATA_V2_MPC`. You can maintain the OData technical model with transaction `/IWBEP/REG_MODEL`.
- Define the Gateway OData technical service using the generic data provider class of the Mobile Integration Framework `/MFND/CL_CORE_ODATA_V2_DPC`. You can maintain the OData technical service with transaction `/IWBEP/REG_SERVICE`.
- Assign the Gateway OData technical service to a mobile application by choosing the *OData Service Assignment* in the ConfigPanel.
- Do not define the Gateway OData technical model using the Gateway Service Builder. The model is determined and generated dynamically by the generic model provider class `/MFND/CL_CORE_ODATA_V2_MPC` based on the model configuration settings defined in the ConfigPanel.
- The generic data provider class `/MFND/CL_CORE_ODATA_V2_DPC` doesn't provide the required business logic for the Gateway OData technical service. Business logic is provided by OMDOs. Assign every OData

business request to the service to an OMDO. The assigned OMDO performs the necessary business logic for the business request.

Service Assignments



You can define the following settings for the OData service assignment:

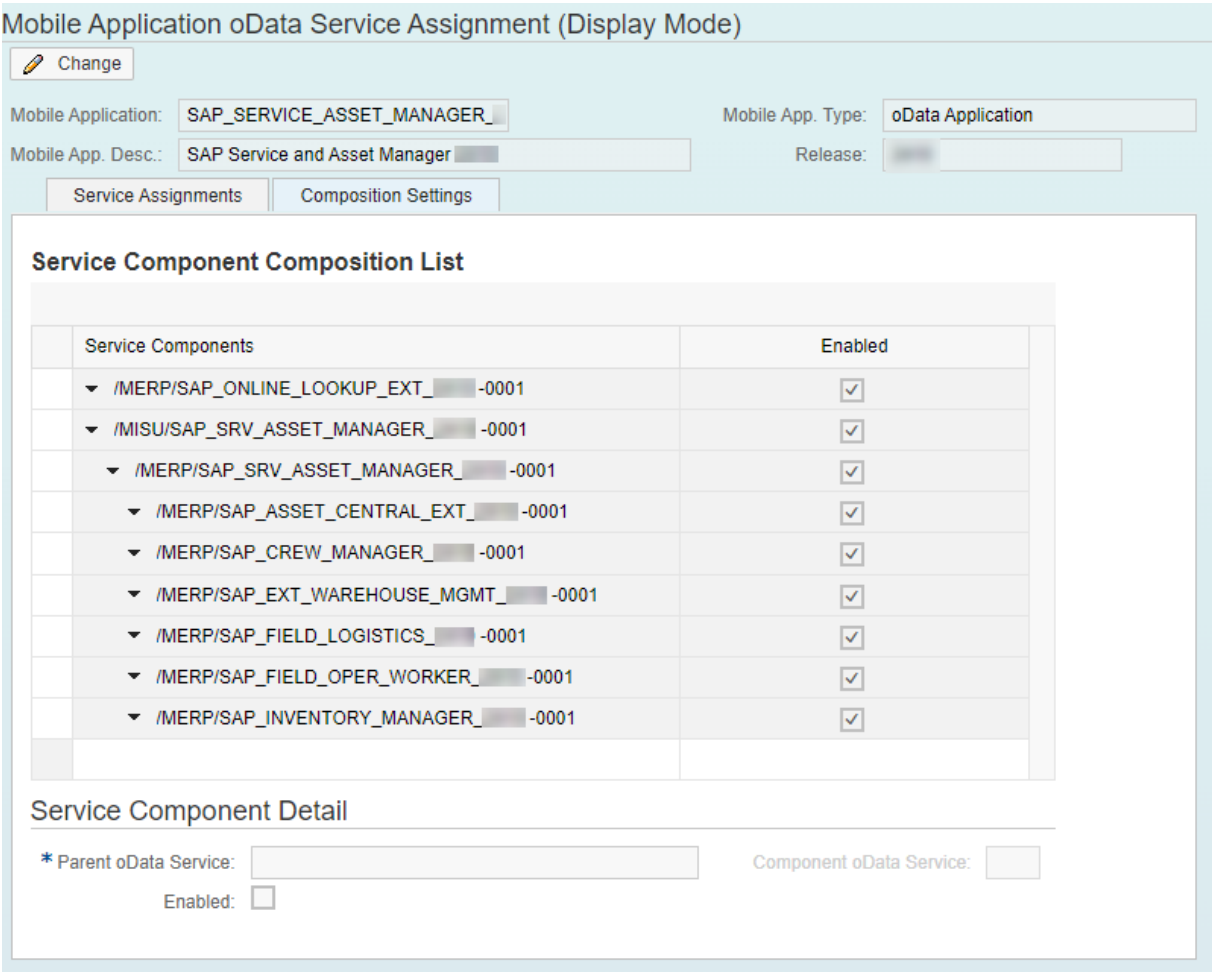
- **OData Version:** OData version 2.0 is supported.
- **OData Service:** The Gateway OData technical service that is assigned to the mobile application. You can only assign a single mobile application to a Gateway OData technical service. Assignment to multiple mobile applications is not supported.
- **Active:** If the *Active* checkbox is checked, both the OData model and OData service are supported. If the checkbox is not checked, no OData model is generated for the service, and the data request to the service is not supported.
- **Defer Batch Response:** This setting is only relevant if you have an SAP S/4HANA back-end system. If the checkbox is checked, the Gateway runtime deferred batch response is enabled, which can improve performance during read request processing.
- **Max Payload Records:** Maximum number of records in the response payload to a read request. In case the read request is a batch request with multiple read requests, this setting defines the total number of records allowed in the overall payload, which is the aggregation of individual read request responses.
- **Cache Handshake:** When checked, the Gateway runtime metadata cache handshake is enabled for the service.
- **Technical Service Name:** Read-only information. Gateway OData technical service name.
- **Service Version:** Read-only information. Gateway OData technical service version.

Composition Settings

With service component composition, you can compose a complex service using component services.

In the following example, service `/MERP/SAP_SRV_ASSET_MANAGER_1911 version 0001` is composed of service `/MERP/SAP_ASSET_CENTRAL_EXT_1911 version 0001`, service `/MERP/SAP_CREW_MANAGER_1911 version 0001`, and service `/MERP/SAP_FIELD_OPER_WORKER_1911 version 0001`.

The entity model for service `/MERP/SAP_SRV_ASSET_MANAGER_1911 version 0001` includes the entity model from `/MERP/SAP_CREW_MANAGER_1911 version 0001` and the other two entity models listed. The entity model for service `/MERP/SAP_CREW_MANAGER_1911 version 0001` only contains its own entities.



To define a component composition, define the following:

- **Parent OData Service and Version:** Parent OData service. Entity model of a child OData service is included in the parent entity model. Association and navigation properties can be defined between parent service and component service.
- **Component OData Service and Version:** Child OData service
- **Enabled:** If the checkbox is not checked, the entity model of the component service is not included in the entity model of the parent service.

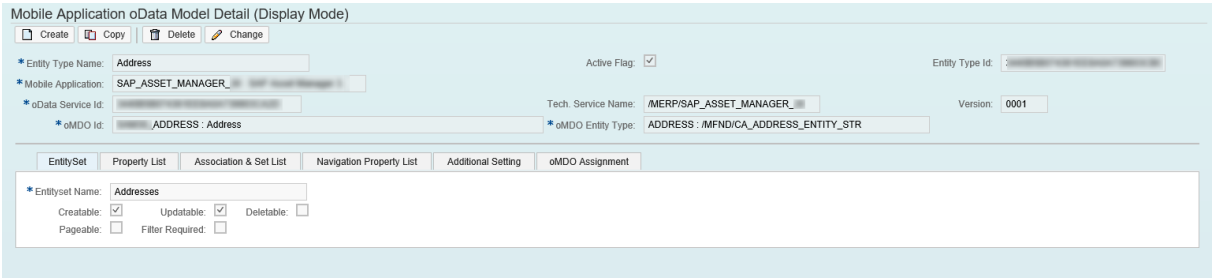
6.3.2.5.2 OData Model Configuration

OData service implemented using the Mobile Application Integration Framework does not use the Gateway Service Builder to define the OData model. Define the OData model using the OData Model configuration tool in the ConfigPanel. The runtime OData model is generated dynamically based on the configuration settings. The OData model configuration is mobile application-specific. You cannot share OData models across mobile applications.

Define the OData model configuration settings through the following screens:

Entity Set Tab

Entity configuration defines the OData entity type. Entity set configuration defines the OData entity set. In an OData model configuration, each entity type is limited to one entity set. Reuse of entity types by multiple entity sets or by different OData services is not supported.



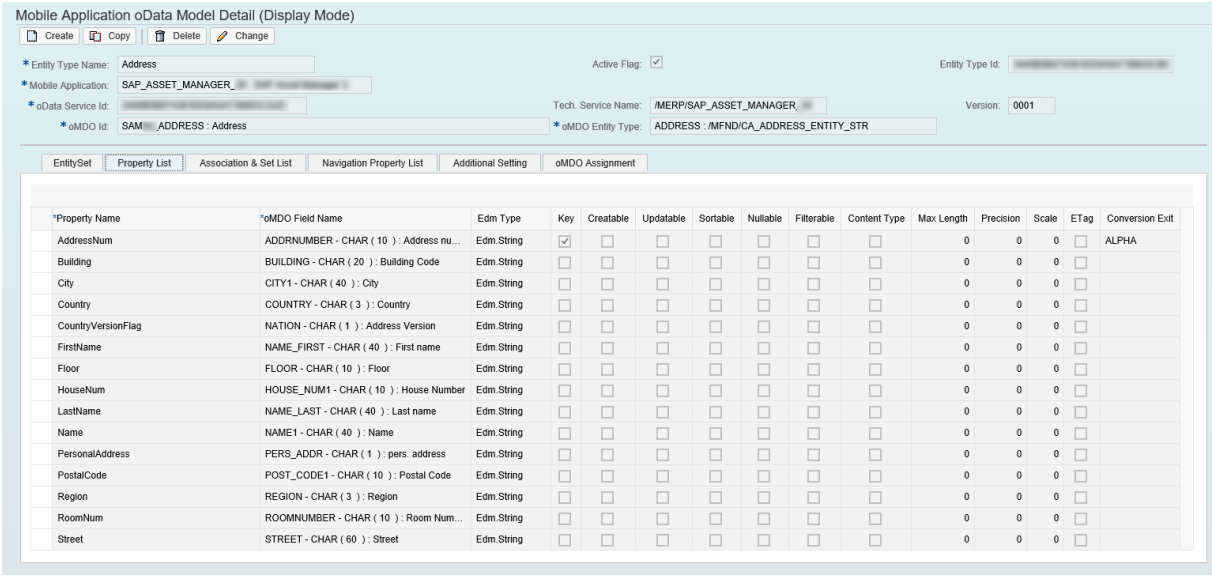
The following attributes are available for the *Entity Type* definition:

- **Entity Type Name:** Case-sensitive name of the entity type. The name must be unique within the OData service.
- **Active Flag:** If unchecked, the entity type is not included in the generated OData model
- **Entity Type ID:** Internal ID generated by the system to identify the entity type
- **Mobile Application:** Mobile application for the entity type. The OData model configuration is defined for individual mobile applications. You can reuse the entity type name in different mobile applications.
- **Internal OData Service ID:** Internal OData service ID that identifies the OData service for which the entity type is defined
- **Service:** Gateway technical service name of the OData service. Information is read-only.
- **Version:** Gateway technical service version. Information is read-only.
- **OMDO ID:** OMDO that provides business logic for the entity type and its entity set
- **OMDO Entity Type:** Technical entity type of the OMDO that is mapped to the OData entity type. Data for the OData entity type is supplied by the OMDO entity type.

The following attributes are available for the *Entity Set* definition:

- **EntitySet Name:** Case-sensitive name of the entity set. Must be unique within the OData service.
- **Creatable:** If checked, creation (POST) request for the entity set is supported
- **Updatable:** If checked, update (PUT / PATCH / MERGE) request for the entity set is supported
- **Deletable:** If checked, deletion (DELETE) request for the entity set is supported
- **Pageable:** If checked, paging is allowed for the entity set read request
- **Filter Required:** Not applicable for SAP Service and Asset Manager

Property List



*Property Name	*oMDO Field Name	Edm Type	Key	Creatable	Updatable	Sortable	Nullable	Filterable	Content Type	Max Length	Precision	Scale	ETag	Conversion Exit
AddressNum	ADDRNUMBER - CHAR (10) : Address nu...	Edm.String	☑	☐	☐	☐	☐	☐	☐	0	0	0	☐	ALPHA
Building	BUILDING - CHAR (20) : Building Code	Edm.String	☐	☐	☐	☐	☐	☐	☐	0	0	0	☐	
City	CITY1 - CHAR (40) : City	Edm.String	☐	☐	☐	☐	☐	☐	☐	0	0	0	☐	
Country	COUNTRY - CHAR (3) : Country	Edm.String	☐	☐	☐	☐	☐	☐	☐	0	0	0	☐	
CountryVersionFlag	NATION - CHAR (1) : Address Version	Edm.String	☐	☐	☐	☐	☐	☐	☐	0	0	0	☐	
FirstName	NAME_FIRST - CHAR (40) : First name	Edm.String	☐	☐	☐	☐	☐	☐	☐	0	0	0	☐	
Floor	FLOOR - CHAR (10) : Floor	Edm.String	☐	☐	☐	☐	☐	☐	☐	0	0	0	☐	
HouseNum	HOUSE_NUM1 - CHAR (10) : House Number	Edm.String	☐	☐	☐	☐	☐	☐	☐	0	0	0	☐	
LastName	NAME_LAST - CHAR (40) : Last name	Edm.String	☐	☐	☐	☐	☐	☐	☐	0	0	0	☐	
Name	NAME1 - CHAR (40) : Name	Edm.String	☐	☐	☐	☐	☐	☐	☐	0	0	0	☐	
PersonalAddress	PERS_ADDR - CHAR (1) : pers. address	Edm.String	☐	☐	☐	☐	☐	☐	☐	0	0	0	☐	
PostalCode	POST_CODE1 - CHAR (10) : Postal Code	Edm.String	☐	☐	☐	☐	☐	☐	☐	0	0	0	☐	
Region	REGION - CHAR (3) : Region	Edm.String	☐	☐	☐	☐	☐	☐	☐	0	0	0	☐	
RoomNum	ROOMNUMBER - CHAR (10) : Room Num...	Edm.String	☐	☐	☐	☐	☐	☐	☐	0	0	0	☐	
Street	STREET - CHAR (60) : Street	Edm.String	☐	☐	☐	☐	☐	☐	☐	0	0	0	☐	

You can configure the following on the *Property List* tab:

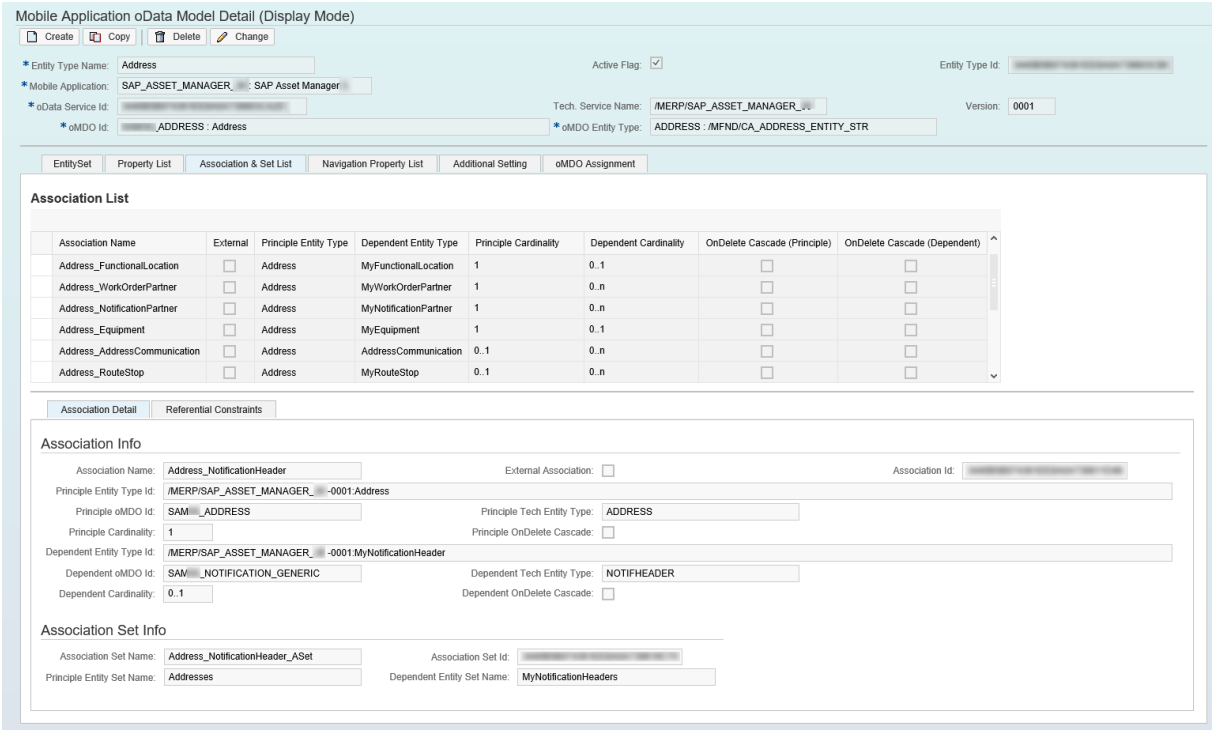
- **Property Name:** Case-sensitive name of the property
- **OMDO Field Name:** Field name of the OMDO technical entity type mapped to the property. The value of the property is supplied in the `<OMDO Entity Type>` field.
- **EDM Type:** Standard EDM type for the property
- **Key Indicator:** If checked, the property is the key property of the entity type
- **Creatable:** Not applicable for SAP Service and Asset Manager
- **Updatable:** Not applicable for SAP Service and Asset Manager
- **Sortable:** If checked, the property can be used for sorting
- **Nullable:** If checked, the property can have NULL value
- **Filterable:** If checked, the property can be used for filtering
- **Content Type:** If checked, the property value can represent content type
- **Max Length:** Maximum allowed length of the property value
- **Precision:** Decimal precision of the property, if relevant
- **Scale:** Decimal scale of the property, if relevant
- **ETag:** If checked, the property serves as the `<ETag>` field. You can set only one field as an `<ETag>` field in an entity type.
- **Conversion Exit:** Conversion exit for the property

Association & Set List Tab

An association defines the relationship between two entity types, with one entity type as the principle entity type, and the other as the dependent entity type. An association set defines the relationship between the two entity sets of the respective entity types in the association. In an OData model configuration, associations and

association sets are child objects of an entity type, and each association can have only one association set defined.

When you define an OData model to use with OData offline SDK client application, you also define referential constraints for the association. Only key fields of the principle entity type can be used in referential constraints.



You can configure the following in the *Association Info* section:

- **Association Name:** Case-sensitive name of the association
- **External Association:** By default, the parent entity type of the association is the principle entity type. However, if the *External Association* flag is checked, the parent entity type of the association is the dependent entity type. An external association is commonly used when defining associations between entity types across component services.
- **Association ID:** A read-only internal GUID generated by the system that identifies the association
- **Principle Entity Type ID:** Lead entity type of the association
- **Principle OMDO ID:** Read-only OMDO ID to which the principle entity type is mapped to
- **Principle Tech Entity Type:** Read-only technical entity type of the OMDO ID to which the principle entity type is mapped to
- **Principle Cardinality:** Cardinality of the lead entity type
- **OnDelete Cascade (Principle):** If checked, the dependent entity type and entity set are automatically deleted when the principle entity type and entity set are deleted
- **Dependent Entity Type ID:** For standard associations, the dependent entity type can be any entity type belonging to the same OData service or child component service
- **Dependent OMDO ID:** Read-only OMDO ID to which the dependent entity type is mapped to
- **Dependent Tech Entity Type:** Read-only technical entity type of the OMDO ID to which the dependent entity type is mapped to
- **Dependent Cardinality:** Cardinality of the dependent entity type

- **Dependent OnDelete Cascade:** If checked, the principle entity type and entity set are automatically deleted when the dependent entity type and entity set are deleted

You can configure the following in the *Association Set Info* section:

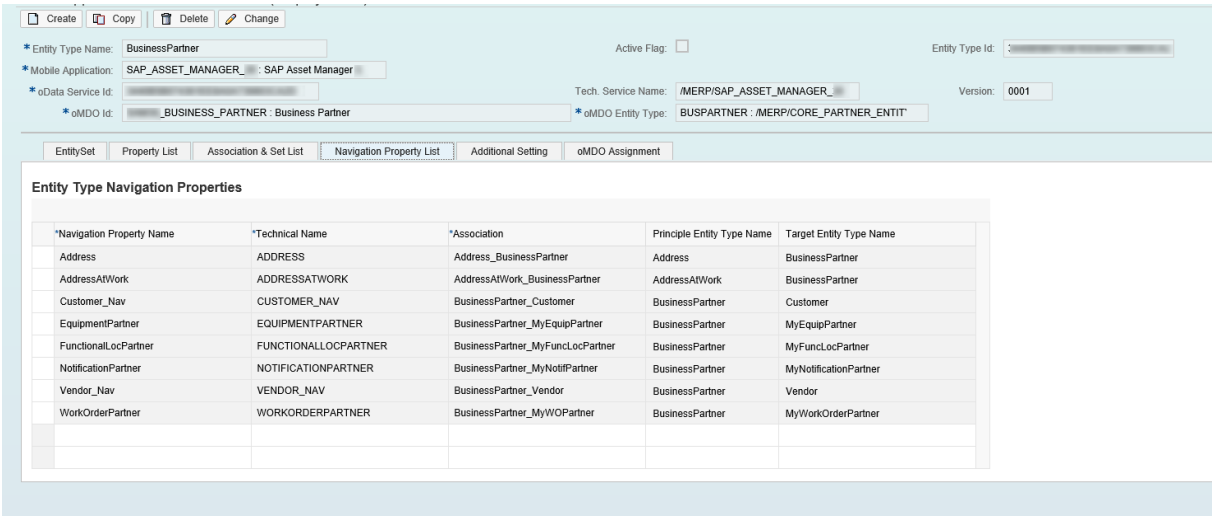
- **Association Set Name:** Case-sensitive name of the association set
- **Association Set ID:** Read-only internal GUID generated by the system that identifies the association set
- **Principle Entity Set Name:** Read-only entity set name of the principle entity type. Each entity type in the OData model configuration can only have one entity set.
- **Dependent Entity Set Name:** Read-only entity set name of the dependent entity type. Each entity type in the OData model configuration can only have one entity set

You can configure the following in the *Referential Constraints* section (not pictured in detail in the example screenshot):

- **Principle Entity Type:** Read-only principle entity type of the association
- **Principle Property:** Principle property of the referential constraint. The principle property is the key field of the principle entity type.
- **Dependent Entity Type:** Read-only dependent entity type of the association
- **Dependent Property:** Dependent property of the referential constraint. The dependent property can be any field of the dependent entity type that has a foreign key relationship with the principle property.

Navigation Property List Tab

A navigation property represents a link from the parent entity type to a related entity types.

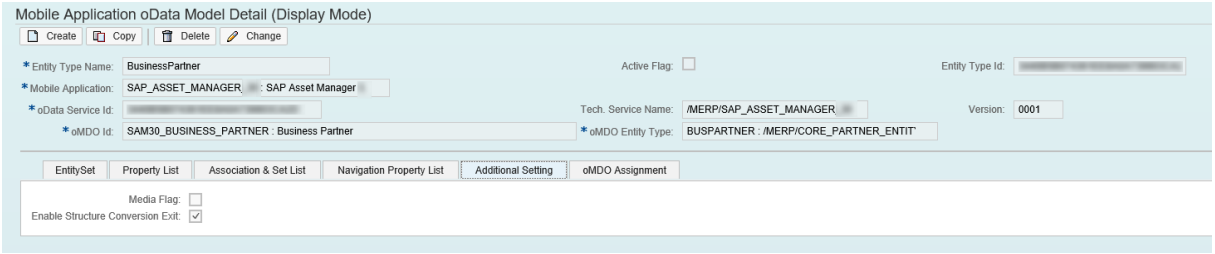


You can define the following attributes for a navigation property in the *Entity Type Navigation Properties* table:

- **Navigation Property Name:**
- **Technical Name:** Case-sensitive name of the Internal technical name of the navigation property. The technical name is not case-sensitive.
- **Association:** Association for the navigation property. The navigation represents the link between the principle entity type and the dependent entity type.

- **Principle Entity Type Name:** Read-only principle entity type name of the association used by the navigation property
- **Dependent Entity Type Name:** Read-only dependent entity type name of the association used by the navigation property

Additional Setting Tab



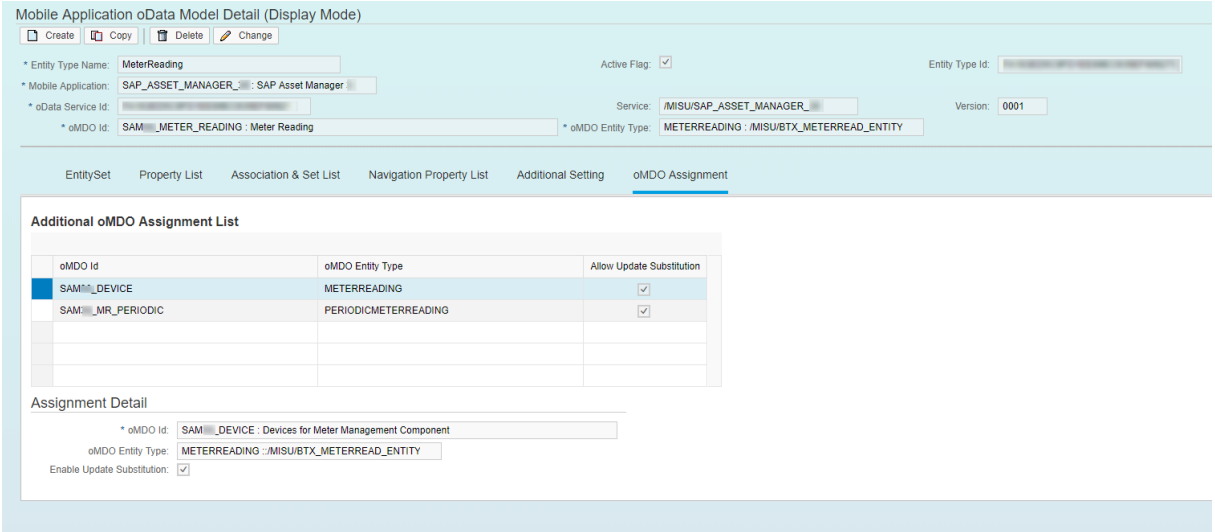
You can define the following additional settings for the OData model:

- **Media Flag:** If checked, the entity type is a media entity type
- **Enable Structure Conversion Exit:** If checked, the gateway automatically performs conversion exits for the entity type at runtime for both the request payload and the response payload

OMDO Assignment Tab

The *OMDO Assignment* tab only supports substitution configuration scenarios.

Use the following screenshot as an example. When a user posts a meter reading from their client, by default the reading is posted to the default OMDO, which here is *SAM<XX>_METER_READING*. However, if the user is reading a periodic meter, the reading is posted to the *SAM<XX>_MR_PERIODIC* OMDO, which is substituted for the default OMDO through the use of custom headers.

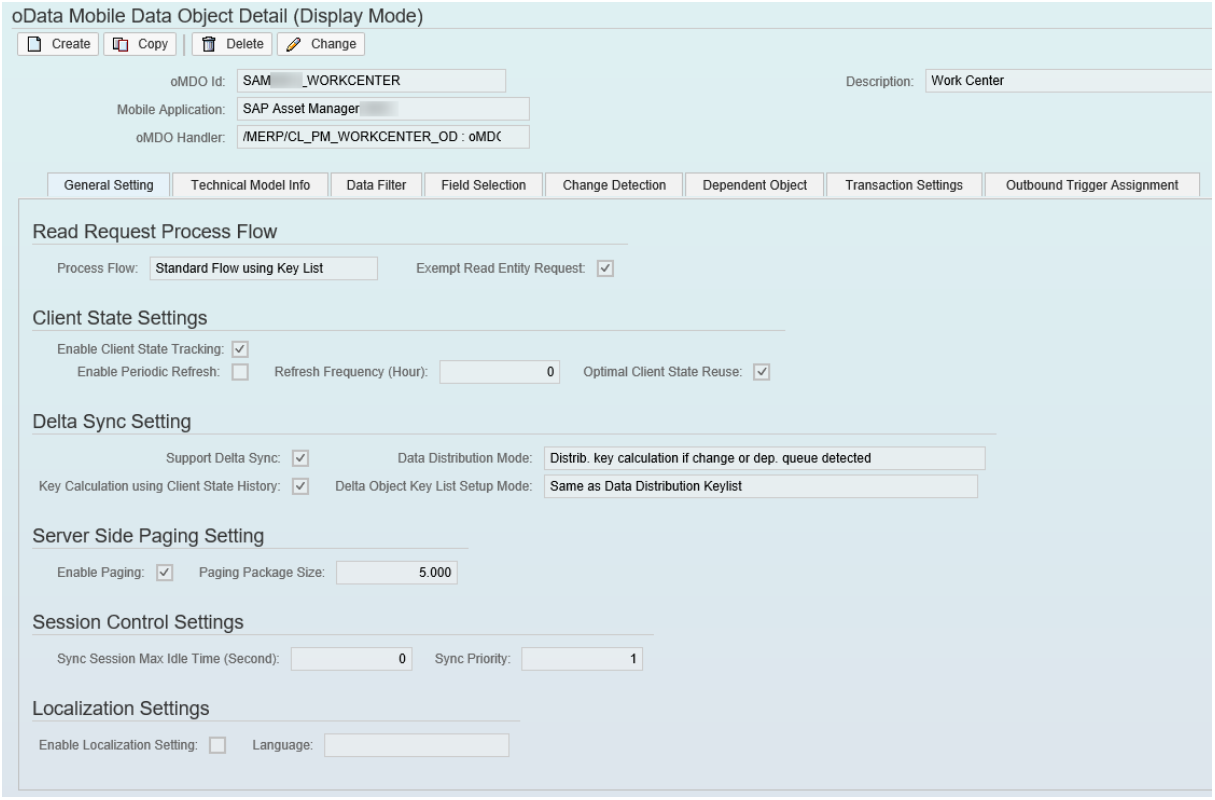


6.3.2.5.3 OData Mobile Data Object Configuration

An OData mobile data object (also known as OMDO) provides business logic for a business object used in an OData-based mobile application. An OMDO provides both technical implementation and configuration support for the represented business object, including all aspects of related operations such as object creation, update, deletion, or read and downloading. The OMDO also supports configuration such as data distribution rules for data download.

OData requests for a business object are mapped to an OMDO object. The OMDO handler then processes the requests for the OMDO object. For read requests, the OMDO handler considers and enforces the data distribution rules and other configuration settings, and determines the proper output response. For create, update, and delete requests, the OMDO handler creates or updates the SAP BusinessObjects in the back-end system as requested in the OData requests, and provides the relevant response.

General Setting Tab



You can set the following attributes on the *General Setting* tab:

- **OMDO ID:** ID of OData Mobile Data Object; limited to 40 characters. The OMDO ID must be unique in an SAP client, across all mobile applications, as namespace restriction is enforced. A customer-defined OMDO ID must use the Y or Z namespace.
- **Description:** Short description of the OMDO, limited to 60 characters
- **Mobile Application:** Mobile application of the OMDO. An OMDO always belongs to a single mobile application.

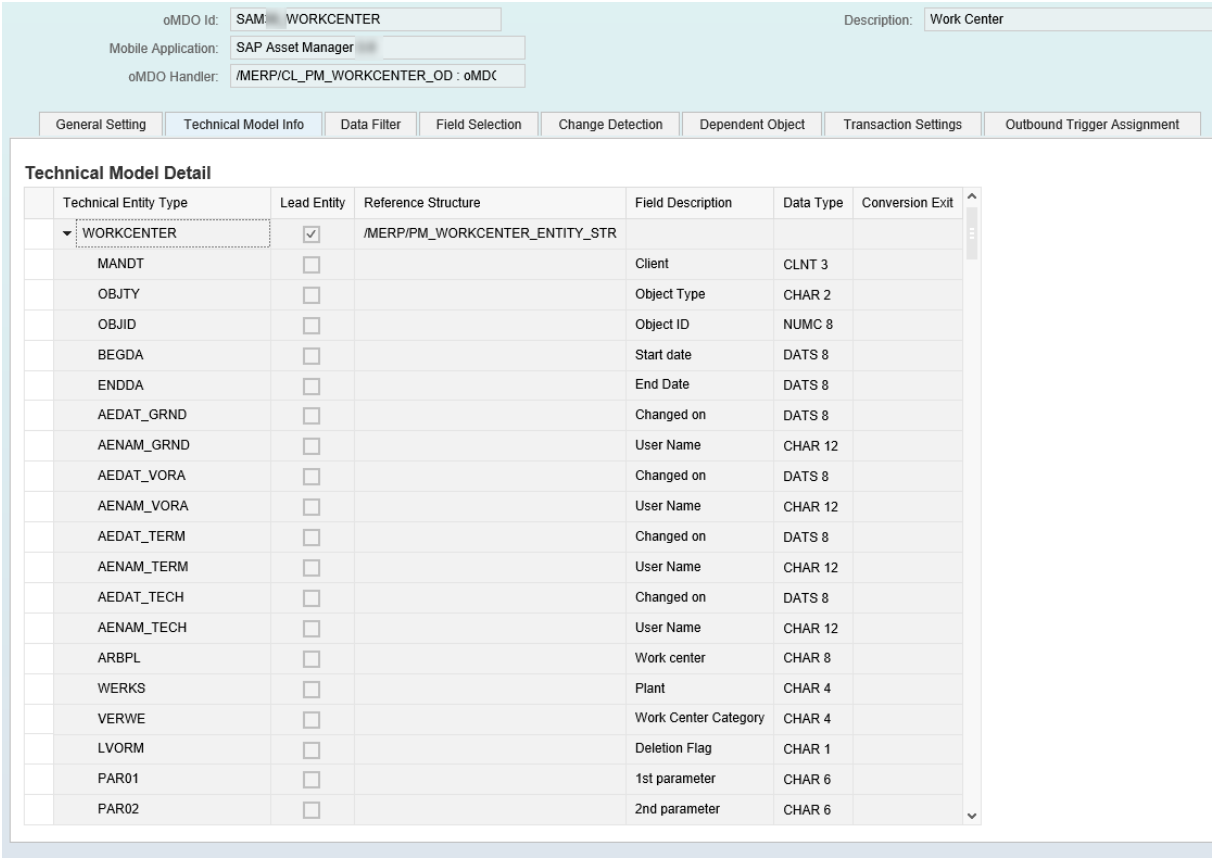
- **OMDO Handler:** An ABAP OO class that provides the technical implementation for the OMDO object. The OMDO handler must be a subclass of `/MFND/CL_CORE_OMDO_HNDLER_BASE`. You can reuse an OMDO handler to provide technical implementation for multiple OMDO objects.
- **Process Flow:** Determines how the OMDO handler processes OData entity set read requests. Based on the process flow setting, different OMDO handler methods are invoked at runtime. The OMDO handler determines which process flow it supports.
  - **Standard Flow using Key List:** Typically used by the OMDO handler to support complex SAP BusinessObjects with multiple entity types, complex relationships between entity types and data distribution rules, and with change detection support. Examples of SAP BusinessObjects that use the standard flow include transaction data objects such as work orders or notifications; and leading data objects such as equipment or functional locations.
  - **Basic Flow without Key List:** Typically used by the OMDO handler to support simple SAP BusinessObjects with a single entity type and no change detection support. Examples of SAP BusinessObjects that use the basic flow without key list include customizing data, such as plant or order type. OMDO handlers that only support basic flow are typically subclasses from `/MFND/CL_CORE_OMDO_BASIC_HNDLR`.
- **Exempt Read Entity Request:** If checked, the entity read request is handled by the *READ_ENTITY_REQUEST_PROC* method. The method supports on-demand entity read requests without interference with client state tracking for entity set read requests.
- **Enable Client State Tracking:** If checked, the client state records are maintained for each entity set read request. Client state tracking enablement is required for other features such as key list calculation using client state history, periodic refresh support, and optimized client state reuse.
  - **Client State:** Captures the list of calculated object keys that are sent to the mobile client for the entity set read requests, the data distribution rules used for the calculation, and the time of the calculation. By enabling client state management, the system has a record of the objects distributed to the mobile client. Enabling client state management also allows the system to calculate the list of objects to be removed from mobile client via tombstones.
    At runtime, the client state info generated during client synchronization can be displayed using the client state monitor through the Administration & Monitoring Portal.
- **Enable Periodic Refresh:** If checked, every entity set delta sync read request is checked if it qualifies for periodic refresh. A periodic refresh means that if time between an entity set initial sync or last period refresh read request and current read request has exceeded the defined frequency, all objects from the client are removed and a new object key list is calculated based on the current data distribution rules.
- **Refresh Frequency (Hour):** Defines the periodic frequency refresh in number of hours
- **Optimal Client State Reuse:** If checked, the system tries to reuse previous client state records whenever possible instead of generating new client state records. Reuse of previous client state records can improve runtime performance. Whether a client state record can be reused depends on the object key list and data distribution rules. If both items remain unchanged compared to the previous client state, the client state record can be reused.
- **Support Delta Sync:** If checked, a delta token is generated and returned in response to the entity set read request
- **Key Calculation using Client State History:** This setting is effective only if client state tracking is enabled. If checked, the object key list is taken from current data distribution calculation, and the list is compared against the object key list from the previous client state. Also, objects that should be removed from the client are automatically identified, and downloaded to the client again.
- **Data Distribution Mode:** Controls when data distribution key calculation is performed for delta sync entity set read requests. It's only relevant if OMDO handler supports the *Standard Flow using Key List* process flow. There's overhead associated with data distribution key calculation. You can reduce the number of

key calculations during sync to improve performance. However, the potential performance gain has to be measured against the correctness of the response. If the object key list from data distribution changes frequently, skipping the calculation can lead to incorrect results.

  - **Always perform distribution key calculation:** Perform the data distribution key calculation for every read request
  - **Distribution key calculation if change or dependent queue detected:** Perform data distribution key calculation only if there's data change detected in the back-end system, or if there are new dependent queue entries inserted
  - **No distribution key calculation. Delta calculation only:** Always skip data distribution key calculation in delta sync
- **Delta Object Key List Set up Mode:** Used in standard flow to determine how the delta object key list is initialized. The delta object key list determines the list of objects that are included in the delta sync response.
  - **Same as Data Distribution Key List:** Default delta sync object key list is the same as the data distribution key list. If change detection is supported by the OMDO, we recommend using this setting. Remove objects that do not have changes since the last delta sync from the delta object key list to prevent unnecessary download and to improve performance.
  - **Difference of Current and Last Data Distribution Key List:** The current data distribution key list is compared to the object key list from the last client state. The only objects that are not included in the last client state object list are included in the delta sync object key list. If no change detection is supported by the OMDO, we recommend using this setting.
- **Enable Paging:** If checked, server-side paging is activated. When paging is active, response from the OMDO to the OData request is limited to the specified paging package size. If the number of records in the response exceeds the paging package size, the response is divided into separate pages. The *$skiptoken* identifies the next page that is generated and included in the response to the client. The client then sends a follow-up request with the skip token to retrieve the next page. This process continues until the client retrieves all pages.
- **Paging Package Size:** Maximum number of records that can be included in a page for the response of the OMDO. For read requests in a batch, the maximum payload records number defined for the OData service assignment is also considered. If the overall number of records in the batch response has reached the maximum payload records number, the number of records in the individual request response can be less than the paging package size specified.
- **Sync Session Max Idle Time (Second):** Estimated maximum duration of a sync session for a single OMDO. For requests belonging to the same OMDO, the response can be calculated beforehand for all requests once and then reused. When the requests are received separately, as long as the requests are received within the defined sync time duration, the response calculated beforehand can be used, instead of calculating it again. Calculating a response beforehand can improve performance. If the sync session max idle time is set to *0*, each request triggers the calculation for the response.
- **Sync Priority:** Represents the processing sequence for read requests in a batch, where *0* has the first priority sequence. For OMDO objects with the same sync priority, OData read requests for these OMDO objects are processed based on the sequence in the batch.
- **Enable Localization Setting:** When checked, brings data associated with the OMDO fetch translated to the language specified in the `<Language>` field irrespective of what logon language is used for the connection. All other OMDOs that don't have *Enable Localization Setting* enabled use the logon language.
- **Language:** Used when the `<Enable Localization Setting>` box is checked. Select your desired language from the dropdown list.

Technical Model Info Tab

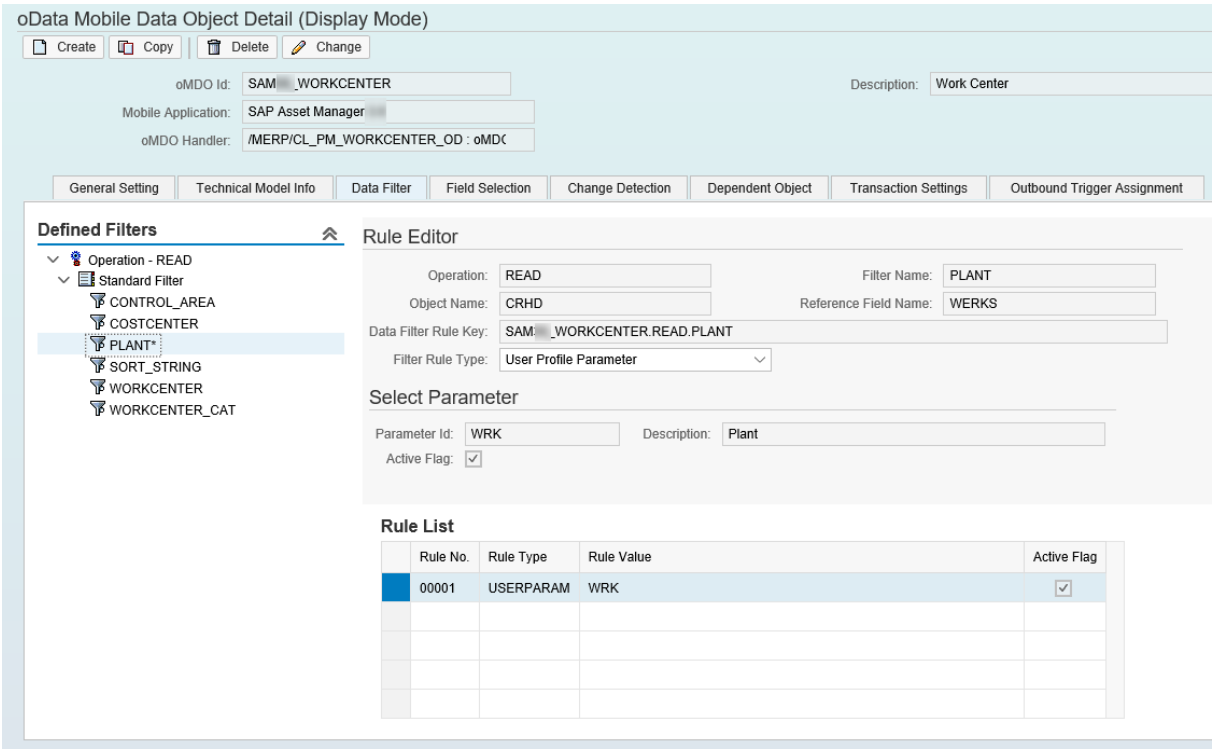
The *Technical Model Info* tab is a display only tab. This tab displays the technical entity model supported by the OMDO handler.



- **Technical Entity Type:** Technical entity type that the OMDO handler supports
- **Lead Entity:** Indicates whether a technical entity is the lead entity type supported by the OMDO handler. The lead entity type represents the header record of a business object. An OMDO operates on a business object level. For an OMDO CREATE operation, a create request (POST request) for the lead entity type is required. If the lead entity already exists, a CREATE request (POST request) for nonlead entity types are considered as OMDO UPDATE operations.
- **Reference Structure:** Data dictionary structure of the technical entity type
- **Field Name:** Field name from the data dictionary structure
- **Field Description:** Field description
- **Data Type:** Field data type
- **Conversion Exit:** Assigned conversion exit for the field

Data Filter Tab

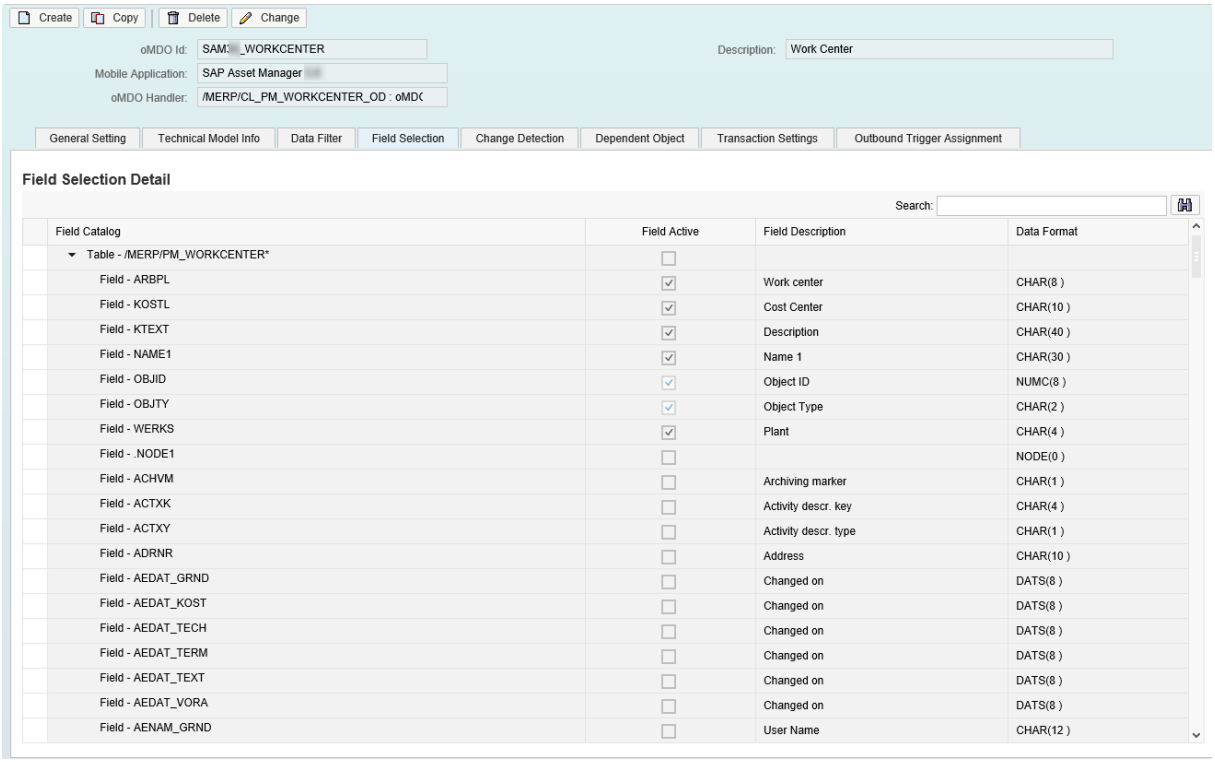
An OMDO handler can declare data filters and parameters supported by its CRUD (CREATE / READ / UPDATE / DELETE) operations. These filters are displayed on the *Data Filter* tab.



- **Defined Filters:** The *Defined Filters* navigation area displays the list of supported filters for the OMDO, grouped by operation and filter group. There are two types of filters available, though both types may not be available for every OMDO:
  - **Standard Filter:** A standard filter is a single field filter that references a table or structure field that is displayed in the `<Object Name>` field and the `<Reference Field Name>` field
  - **Table Filter:** A table filter is a structured filter that references a table or structure that is displayed in the `<Object Name>` field.
- **Rule Editor:** Details for a filter are displayed in this section when you select a filter from the *Defined Filters* section.
- **Filter Rule Type:** You can select one of the four types of rules to define:
  - **Static Value in Range Table Format:** Static rule, with the rule value defined at design time in the configuration
  - **User Profile Parameter:** Dynamic rule, with the rule value evaluated at runtime based on the runtime profile parameter value of the user. You can display and maintain the user profile parameter value with the transaction code *SU3*.
  - **Mobile User Attribute:** Dynamic rule, with the rule value evaluated at runtime based on the runtime mobile user attribute of the user. You can display and maintain the mobile user attribute in the Administration & Monitoring Portal, which you can access with the transaction */SYCLO/ADMIN*. Then select *Administration* > *User Management*.
  - **Filter Handler:** Dynamic rule, with the rule value evaluated at runtime by a filter handler. A filter handler is an ABAP subclass of `/MFND/CL_CORE_OMDO_RULE_BASE`.

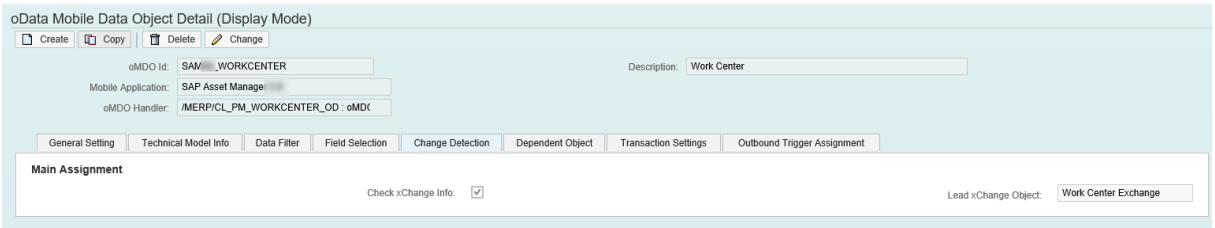
Field Selection Tab

An OMDO handler can declare field catalogs supported for the READ operation. If there is a READ operation, by default, all of the fields from the database tables related to the OMDO object are selected. Using the field catalog, customers can control which fields are selected, and improve performance, as typically a mobile application doesn't require all of the fields.



Change Detection Tab

You can enable change detection for the OMDO using the *Change Detection* tab.



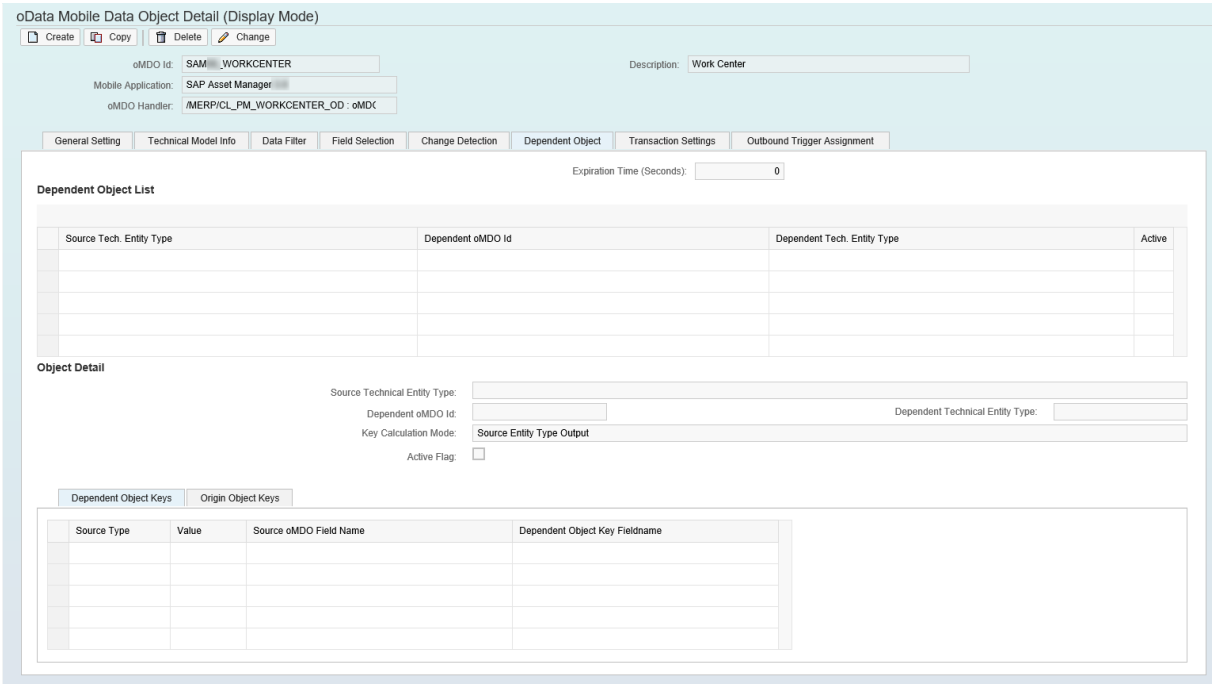
- **Check xChange Info:** Applies to standard flow processing only. If checked, change detection info is checked to determine the delta sync object key list.
- **Lead xChange Object:** xChange object that supplies the change detection information for the OMDO. Information from the xChange table of the xChange object is read and used for the calculation of the delta sync object key list.

Dependent Object Tab

Define settings related to dependent objects on the *Dependent Objects* tab.

In some business cases, the read request sequence for the OMDOs or SAP BusinessObjects is important, since the data distribution object key list of a subsequent OMDO depends on the results or outputs of the precedent OMDOs. The subsequent OMDO is treated as a dependent object of the precedent OMDO. The leading OMDO is the source OMDO, as the output of the lead OMDO supplies information for the dependent OMDO. Dependent object key information generated by the leading OMDO is stored in the dependent object queue, and is used by the dependent OMDO during its read request processing.

For example, SAP Service and Asset Manager downloads detailed information for equipment and functional locations used in work orders assigned to a technician. To fulfill this requirement, read requests for work order assignments occur first, and equipment and functional locations are set up as dependent objects for the work order OMDO.



You can define the following settings for a dependent object of the current OMDO:

- **Source Technical Entity Type:** Source OMDO technical entity type that contains information required by the dependent object
- **Dependent OMDO ID:** ID of the dependent OMDO
- **Dependent Technical Entity Type:** Receiving technical entity type of the dependent OMDO, for which information from the source technical entity type is transferred
- **Key Calculation Mode:** Select the way the keys are passed to the OMDO. Key calculation is a dependent object concept; how you set up your dependent object is based on your source object.
  - Source Entity Output: Input for the dependent key. Keys are calculated based on the source entity type output.
  - Source Entity Type Distribution Key List: Dependent Object Key construction comes from the distribution key list of the source entity type. Using this option always collects all the valid keys from the source entity type.

- Source Entity Type Output + Target Entity Type Client State: Similar to Source Entity Output plus the previous client state of the target entity type. Here, what is being created for dependent object collection is a combined collection of the source entity type output and the target entity type client state records from the previous sync.

- **Active Flag:** Enable or disable a dependent object definition

You can define the following settings for the mapping info of dependent object keys in the *Dependent Object Keys* tab:

- **Source Type:** Use option *By Field Name* if the information comes from a field of the source technical entity type. Use option *By Value* if a constant value is used.
- **Source Value:** Constant value for a dependent object key field. This field is only relevant if the source type is set to *By Value*.
- **Source OMDO Field Name:** Name of the source technical entity type field that supplies value for the dependent object key. This field is only relevant if the source type is set to *By Field Name*.
- **Dependent Object Key Field Name:** Field name of the dependent technical entity type that receives the value from the source technical entity type field

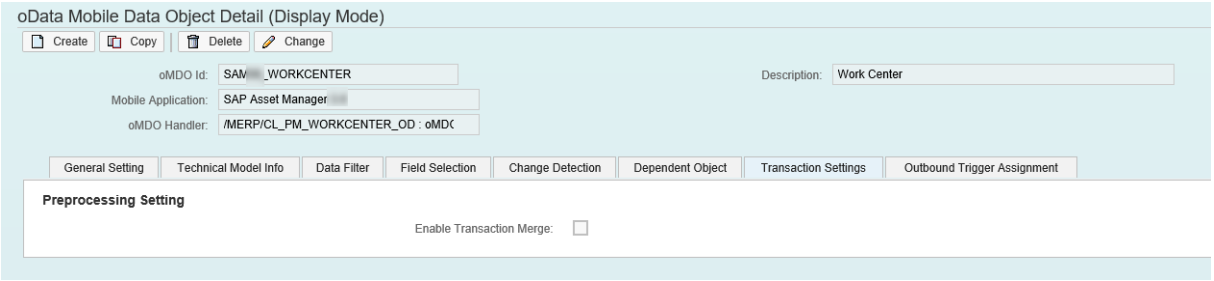
You can define the following settings for the mapping info of origin object keys in the *Origin Object Keys* tab (not shown in detail in the example screenshot). The origin object key identifies the source OMDO object that has generated the dependent object key.

- **Source Type:** Use option *By Field Name* if the information comes from a field of the source technical entity type. Use option *By Value* if a constant value is used.
- **Source Value:** Constant value for an origin object key field. This field is only relevant if the source type is set to *By Value*.
- **Source OMDO Field Name:** Name of the source technical entity type field that supplies value for the origin object key. This field is only relevant if the source type is set to *By Field Name*.

You can display the dependent object queues generated during client synchronization at runtime using the *Dependent Queue Monitor* on the Administration & Monitoring Portal.

Transaction Settings Tab

You can define settings related to transactions (CUD requests) on the *Transaction Settings* tab.



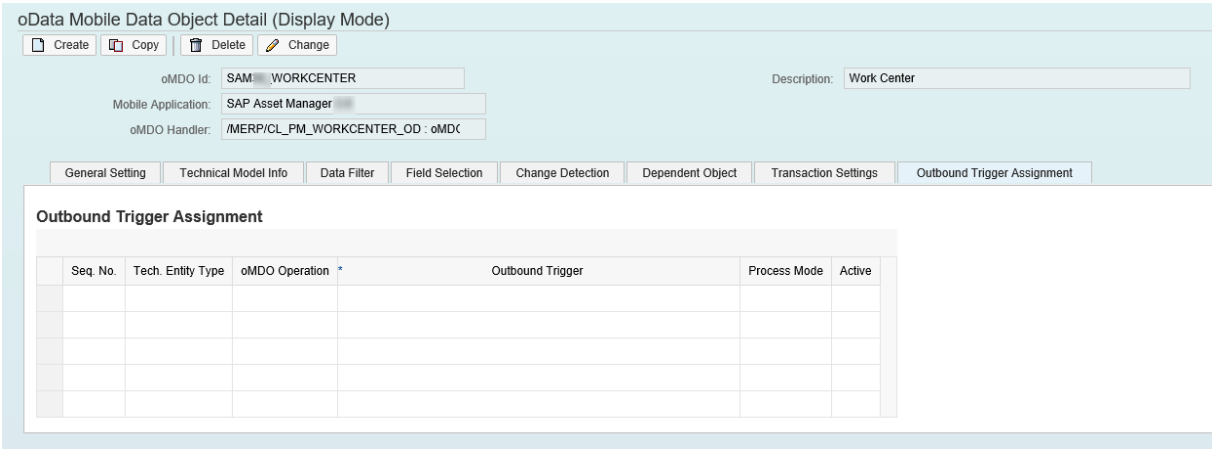
- **Enable Transaction Merge:** If checked, transaction requests for the same object that are received in the same changeset are merged. Therefore, the number of requests processed by the OMDO handler is reduced. The sequence of the transaction requests in the changeset is respected, with the attribute value of the last transaction request as the final value for the attribute.

For example, for *Object 123* the requests are as follows:

Requests in Changeset	Requests Processed by OMDO
Request #1 CREATE 123 Request #2 UPDATE 123 Request #3 DELETE 123	None
Request #1 CREATE 123 Request #2 UPDATE 123 Request #3 UPDATE 123	Request #1 CREATE 123 (attribute values from Request #2 and Request #3 are merged into Request #1)
Request #1 UPDATE 123 Request #2 UPDATE 123	Request #1 UPDATE 123 (attribute values from Request #3 merged into Request #1)

Outbound Trigger Assignment

An outbound trigger performs a function that is implemented by the outbound trigger handler. Outbound triggers can be assigned to an OMDO. The assigned outbound triggers are invoked after OMDO processing has been completed, based on the sequence of the assignment.



You can set the following attributes when assigning an outbound trigger to an OMDO:

- **Technical Entity Type:** Optional. If defined, the outbound trigger is invoked only if the specified technical entity type was processed by the OMDO.
- **OMDO Operation:** Optional. If defined, the outbound trigger is invoked only if the specified OMDO operation is processed.
- **Outbound Trigger ID:** Assigned outbound trigger ID
- **Process Mode:** Only the *Always Run* mode is supported
- **Active:** Enable or disable an outbound trigger

6.3.2.6 Change Detection Settings

Change detection settings are used to define and configure how the mobile application, such as SAP Service and Asset Manager, communicates with SAP and the object tables contained within SAP

The following areas are used to configure backend change detection:

- **Exchange Object Configuration:** Change detection rules for SAP data objects, such as leading data and transaction data, defined for each mobile application
- **EFI Assignment:** Enhancement framework implementation trigger assigned to exchange objects

> ⓘ Note
>
> Create tables and objects in SAP and the Mobile Development Kit before you can create or configure information in the ConfigPanel.

6.3.2.6.1 EFI Assignment

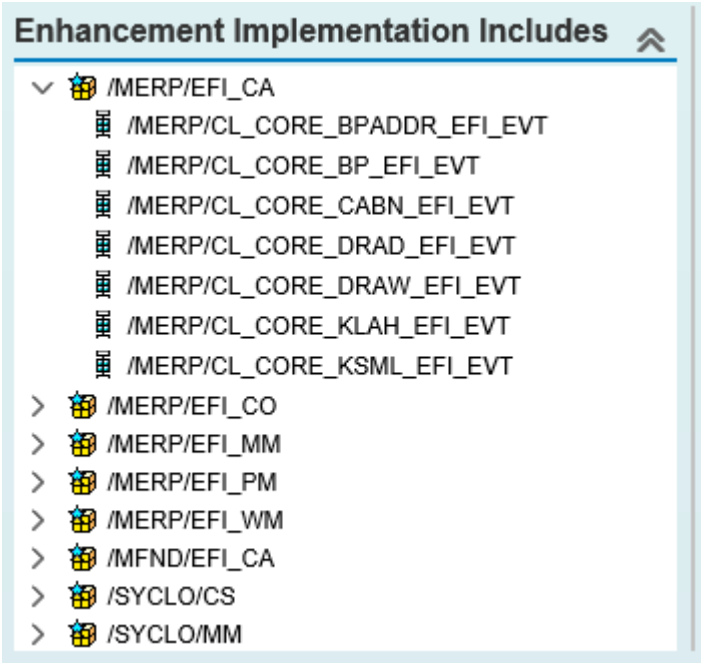
Enhancement Framework Implementation (EFI) source code plug-ins are implemented by the SAP Mobile Add-On for each business object where you configure change detection.

The source code plug-in is provided as an ABAP include file. Each exchange object is assigned to a plug-in to handle the actual change detection process. EFIs are typically available across multiple mobile applications running on the same system.

EFIs collect before and after images of data in an SAP object that was created, modified, or deleted. The EFI then hands those images to the exchange object, which continues with the data processing. Therefore, link the EFIs to their corresponding exchange objects.

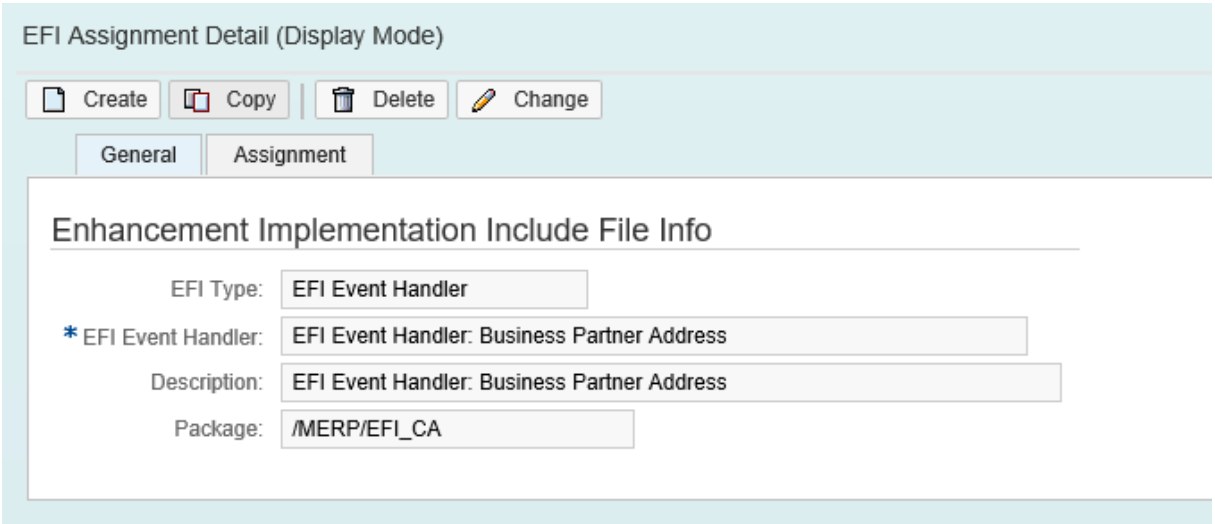
Enhancement Implementation Includes Section

The Enhancement Implementation Includes section is a tree of the include file list in the package. To expand the list, click the arrow to the right of the first item.



General Tab

Use the *General* tab to view and modify the general settings for chosen EFI file.

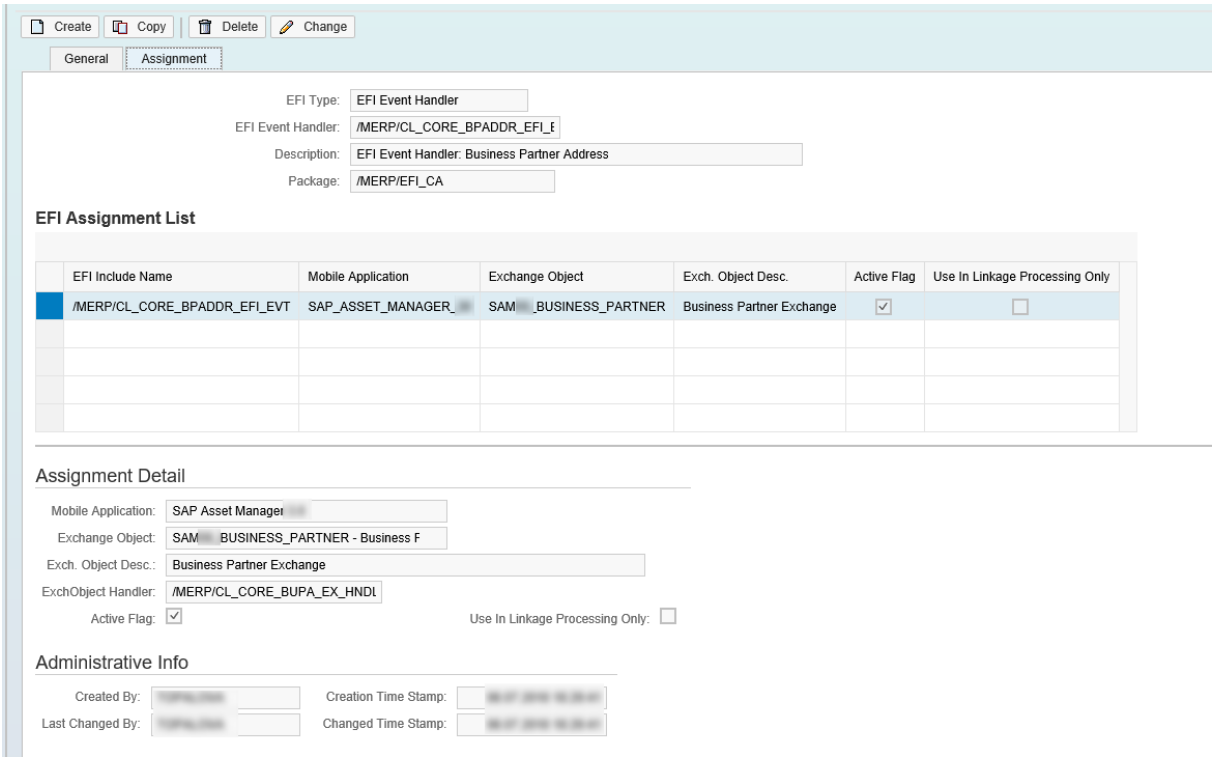


- **EFI Type:** Select one of two options; *Standard EFI Include* or *EFI Event Handler*. Choosing Standard EFI Include is the traditional way to implement EFI and configure the EFI assignments. Selecting EFI Event Handler implements EFI using an ABAP class-based approach.
  When you use a class-based approach, EFI implementation is developed as a subclass of `/SMFND/CL_CORE_EFI_EVENT_BASE`. Available EFI event handler classes are displayed in the dropdown field. The EFI class-based approach provides a more robust functionality and is recommended for a new EFI implementation.

- **EFI Include Name:** File name of the source code plug-in
- **Description:** Short description of the EFI. The description field is automatically populated when you select the EFI include name and is read only.
- **Package:** Package where the EFI is located. The package field is automatically populated when you select the EFI include name and is read only.

Assignment Tab

Use the *Assignment* tab to modify the EFI assignments.



- **EFI Information fields:** The EFI information fields at the top of the *Assignment* tab, like `<EFI Type>` and `<EFI Event Handler>`, are taken from information in the *General* tab and are read only.
- **EFI Assignment List:** Table that displays the plug-ins that are assigned to a specific include file. All column information is replicated in the *Assignment Detail* section directly below the table.
- **Mobile Application:** Read-only name of the specific mobile application
- **Exchange Object:** Name of the exchange object to which the EFI include file is assigned
- **Exchange Object Description:** Read-only description of the exchange object
- **Exchange Object Handler:** Read-only name of the class handler from the repository responsible for updating the exchange table
- **Active Flag:** When checked, the exchange object is in an active state. If unchecked, the EFI isn't linked to the assigned OMDO.
- **Use in Linkage Processing Only:** When checked, the xChange object is only allowed during linkage processing. If not checked, the original EFI is triggered during xChange processing.

6.3.2.6.2 Exchange Object Configuration

The exchange object defines what in the exchange table is updated in the exchange persistent layer, what class handler is called to update the exchange table, and what fields are related to the change detection.

Use the Configuration Panel to specify which changes are relevant to the mobile application and what conditions to satisfy for so that an update action is triggered. The *Exchange Object Configuration* panel has the following tabs:

- Technical Settings
- Change Detection Field Selection
- Change Detection Condition Filter
- Data Segment Settings
- Linkage Settings
- Push Settings

Technical Settings Tab

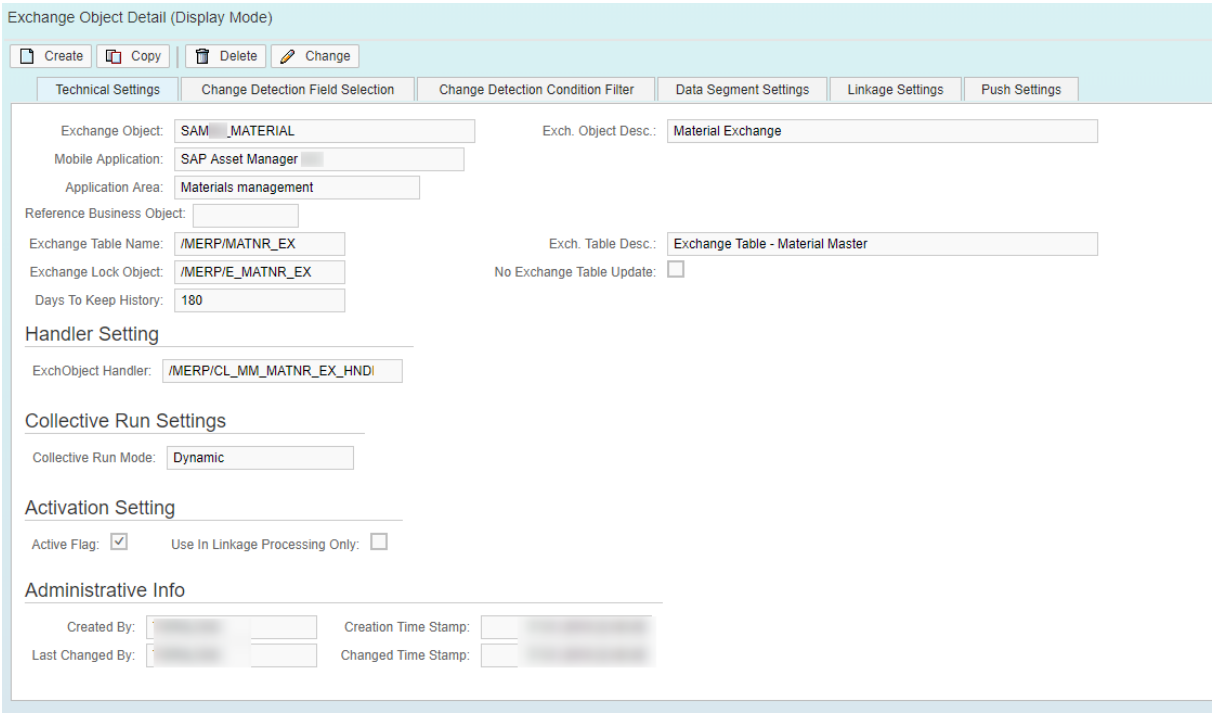
Use the Technical Settings tab to configure basic settings for an exchange object.

Use the `<Exchange Object>` field for the ID of the exchange object, limited to 40 characters. Type in a description in the `<Exchange Object Description>` field, limited to 60 characters. The `<Mobile Application>` field contains a dropdown where you can select your mobile application. The `<Application Area>` classifies the exchange object based on standard SAP application areas using a dropdown selection field.

The `<Reference Business Object>` is the standard SAP business object. The `<Exchange Table Name>` is the name of the table stored in SAP that contains the technical data. The `<Exchange Table Description>` is a brief description of the exchange table. The `<Exchange Lock Object>` field is used when updating the exchange table. Type in how many days you want to keep historical data in the `<Days to Keep History>` field. Check the `<No Exchange Table Update>` checkbox to not write the record to the exchange table in SAP when the record is changed.

- **Handler Setting:** Type in the name of the class handler from the repository that is responsible for updating the exchange table in the `<Exchange Object Handler>` field.
- **Collective Run Settings:** Define the condition where xChange processing is executed asynchronously as a V3 run by selecting one of the following mode options:
  - Dynamic: The collective run mode is determined at runtime by the xChange handler method `DETERMINE_EXEC_MODE`
  - Not Allowed: Not allowed to switch to collective run mode
  - Activated: Always execute asynchronously in V3 collective run mode
  - By User Parameter ID: Switch to V3 collective run mode for runtime user with the specified user parameter value set in the user profile
- **Activation Setting:** Check the `<Active Flag>` checkbox to ensure that the exchange object is in an active state. If unchecked, the exchange object performs no actions. When the `<Use in Linkage Processing Only>` checkbox is checked, the xChange object is only allowed during linkage processing and not if the original EFI was triggered during the xChange process.

The following screenshot shows an exchange process enabled for *MATERIAL*. Any changes for the MATERIAL leading data are recorded in the exchange table and are transmitted to the client during the next transmit.



Change Detection Field Selection Tab

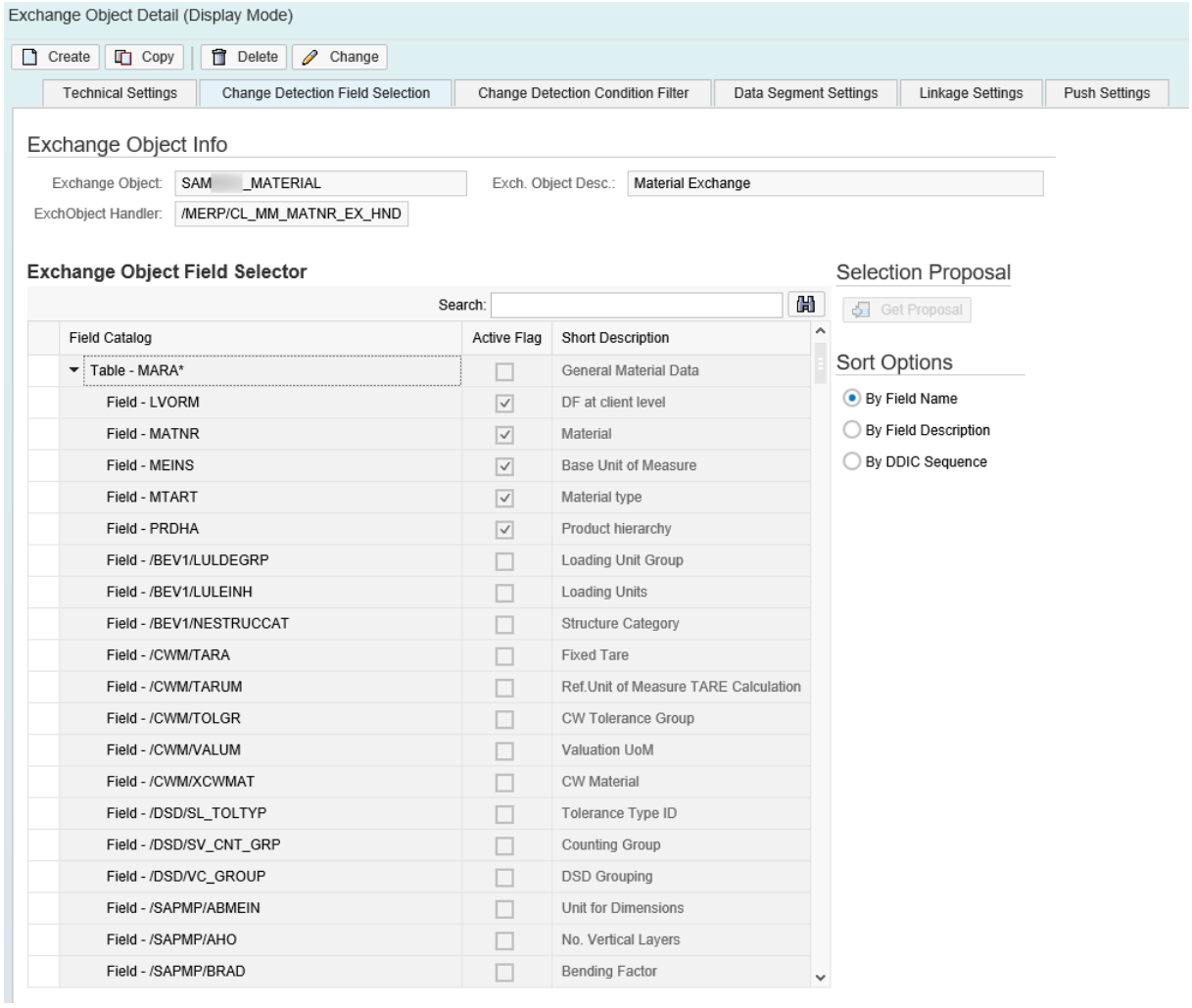
The Change Detection Field Selection tab lets you optimize the change detection process for a mobile application. If a value change is detected for any fields within the group, the object identifier is written to the exchange table, indicating that a change was made. If the `<Active Flag>` is not checked for a field, any value changes made to that field are not detected and recorded to SAP during the exchange process. By default, all fields are initially checked.

The *Exchange Object by Application* tree lists all application areas and the exchange objects linked to each application area. Expand the tree by clicking on the arrows to the right of the application area to display the exchange objects associated with it.

- **Exchange Object Info:** The `<Exchange Object>` field is read only and is the ID of the exchange object. The `<Exchange Object Description>` is read only and is a brief description of the exchange object. The `<Exchange Object Handler>` field is read only and is the name of the class handler from the repository that is responsible for updating the exchange table.
- **Exchange Object Field Selector:** The `<Field Catalog>` column is comprised of non-editable rows of all fields that are detected by the class handler when changes are made. These fields are grouped by the technical table name of the SAP business object.
  When the `<Active Flag>` checkbox is checked, either the table or a field within the table is active. Any value change to the selected field is detected by the class handler. Note that if you check the Active Flag checkbox on a table row, it selects all the rows within the table.
  The `<Short Description>` is a read only field that contains a brief description of the table or of a field withint the table.

- **Selection Proposal:** In a typical mobile application installation, you do not want to have all fields marked as active for change detection. Rather, only the fields that are active on the odata mobile data object that are brought down to the mobile device will also be active in the exchange object. Based on odata mobile data object usage in the application, the selection proposal examines the active flags that are checked for an exchange object's table fields and provides recommendations to the administrator on which fields should be checked or unchecked.

See the following screenshot for an example of the enabled exchange object *MATERIAL*, where the properties of the object are captured and recorded in the exchange table. The properties that trigger the exchange are defined on this *Change Detection Condition Filter* tab, as seen in the checked `<Active Flags>`:

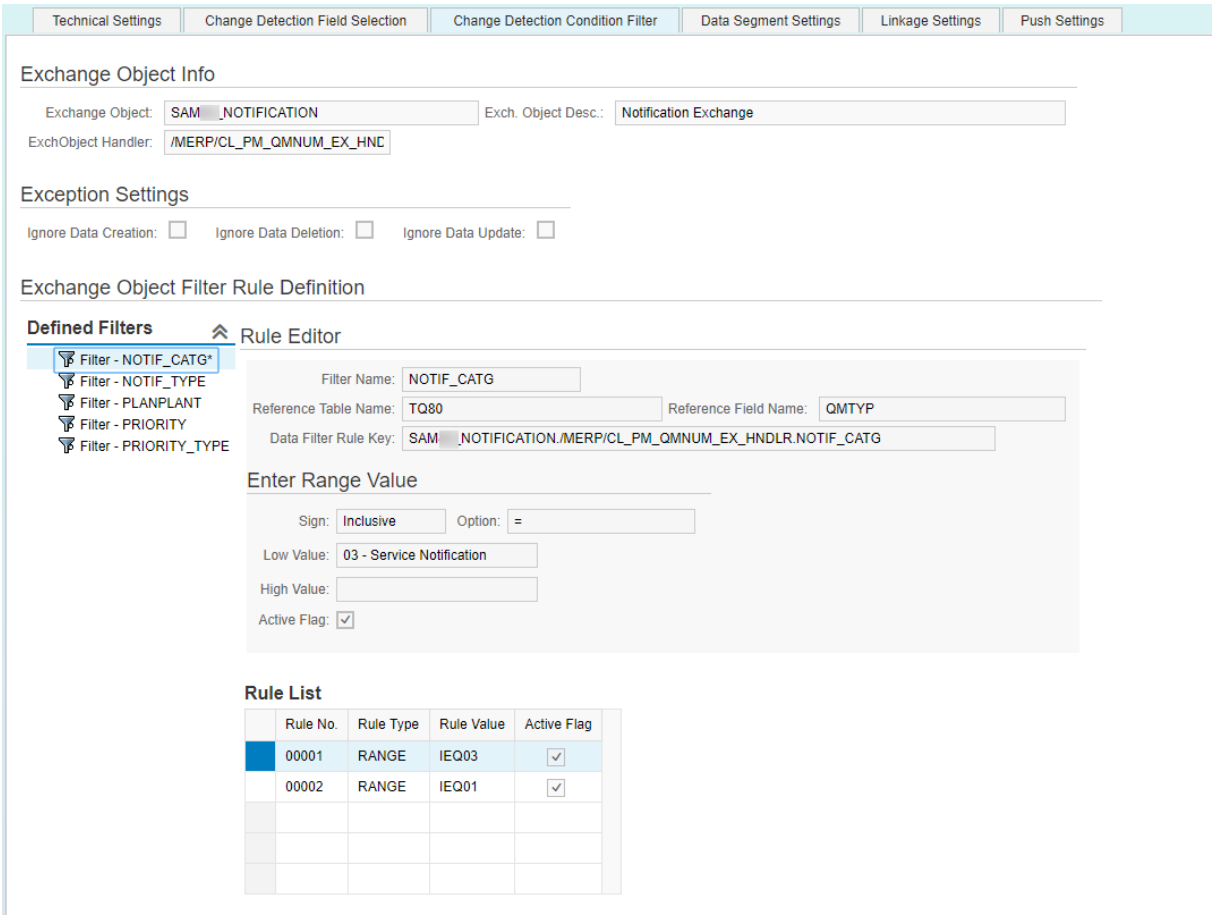


Change Detection Condition Filter Tab

The Change Detection Condition Filter tab lets you restrict change detection based on data content. For exchange handlers to support this feature, define data filter conditions for which the underlying SAP business object must qualify before the change detection process is triggered. The condition is defined at the table field level and is in the SAP range table format.

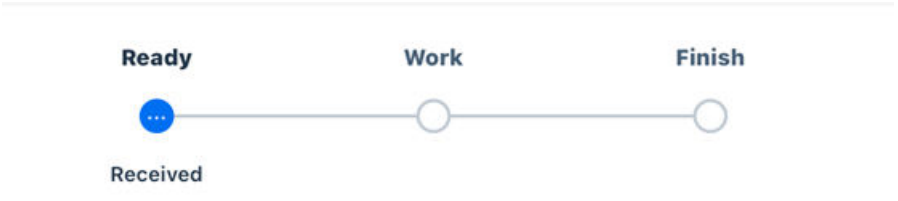
- **Exchange Object Info:** The `<Exchange Object>` field is read only and is the ID of the exchange object. The `<Exchange Object Description>` is read only and is a brief description of the exchange object. The `<Exchange Object Handler>` field is read only and is the name of the class handler from the repository that is responsible for updating the exchange table.
- **Exception Settings:** When the `<Ignore Data Creation>` checkbox is checked, newly created records and data are not processed to the exchange table. When the `<Ignore Data Deletion>` checkbox is checked, deleted records and data are not processed to the exchange table. When the `<Ignore Data Update>` checkbox is checked, updated records and data are not processed to the exchange table.
- **Defined Filters:** Lists all the data filters supported by the class handlers.
- **Rule Editor:** The `<Filter Name>` is read only and is the name of the filter as defined by the class handler developer in the class handler method. The `<Reference Table Name>` is read only and is the technical name of the SAP database table field where the filter is applied as defined by the class handler developer. The `<Reference Field Name>` is read only and is the technical name of the SAP database table field where the filter is applied as defined by the class handler developer. The `<Data Filter Rule Key>` is an internal technical key used by the framework at runtime.
  Use the values in the *Enter Range Value* section to set the range. The `<Sign>` field is the value for the SAP range table column SIGN. The `<Option>` field is the value for the SAP range table column OPTION. The `<Low Value>` field is the value for the SAP range table column LOW. The `<High Value>` field is the value for the SAP range table column HIGH. When the `<Active Flag>` checkbox is checked, the rule is active. The *Rule List* is a table that displays a list of rules that are defined using the values in the *Rule Editor* and the *Range Value* sections.

The following screen shows that any exchange detected for the exchange object *NOTIFICATION* will be considered only if the notification is maintained in one of the roles defined in the *NOTIF_CATG* criteria.



6.3.2.7 Guided Workflow Configuration

Configurable guided workflow (CGW) defines the lifecycle of an object processed in your mobile app. Customers define a workflow for their specific persona and business needs. The mobile app then displays the custom workflow as a progress tracker.



For example, guided workflow configuration can create a progress tracker for a work order that looks one way for a supervisor and a different way for a safety technician.

Administrators plug in customizations through the ConfigPanel, where they can see the process flow defined with easy to follow steps. The steps, in turn, have the status definitions defined for the selected object. The steps are reusable. Once you define a step, you can reuse it in multiple workflows.

Using the guided workflow configuration method means you no longer need to change the configuration in the Status machine filter values (oMDO *SAM<XXXX>_OVERALL_STATUS*) or make code updates through the MDK to handle updates on the mobile device.

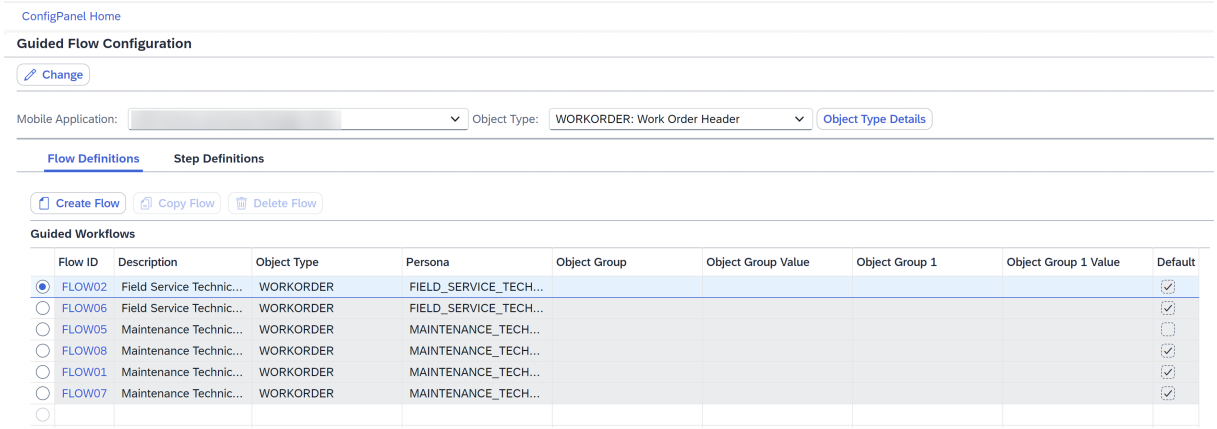
The following tabs make up the guided workflow configuration panel:

- **Flow Definition:**
- **Step Definitions**

See the Guided Workflow Configuration [page 438] chapter and associated topics for detailed procedures on how to modify existing workflows and steps, or how to create a new workflow.

Flow Definitions Tab

A list of all available flows is found on the *Flow Definitions* tab.

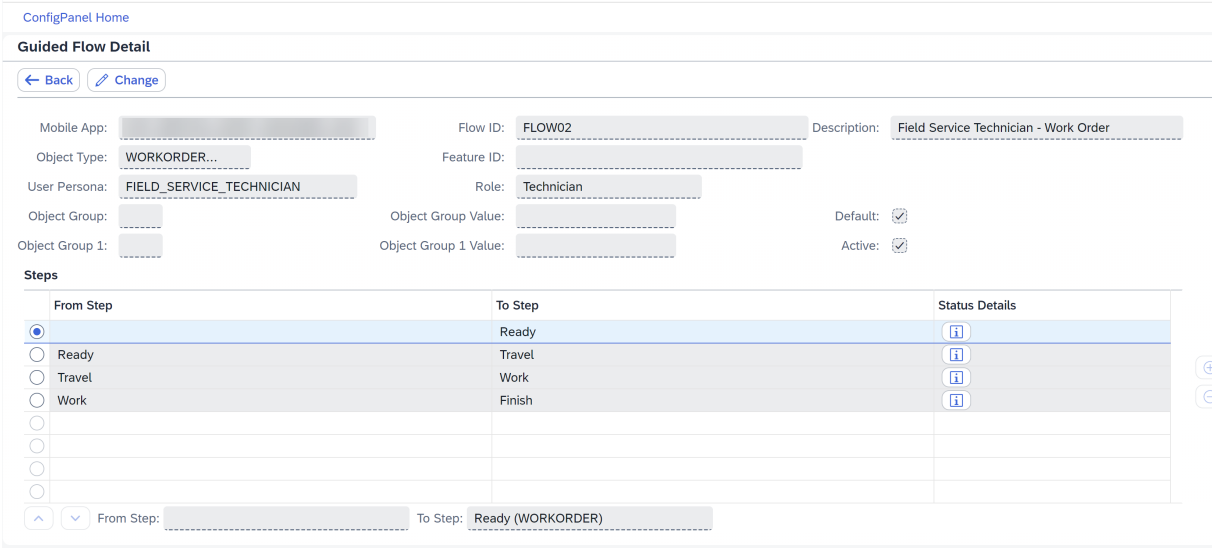


- **Mobile Application field:** A dropdown list of all available applications where guided workflow configuration is available
- **Create Flow button:**
- **Copy Flow button:**
- **Delete Flow button:**
- **Object Type field:** An object type represents a business object you are defining a workflow for (ex: maintenance order). Object types are tied to an entity type in the oData model. Object types can use object groups to further differentiate between business objects.

  > **Note**
  >
  > Define an object group by specifying a property in the model that will be used to distinguish between objects.

- **Guided Workflows section:** Displays a table of all available workflows for the mobile application and object type selection. Click on any *Flow ID* link to open the Guided Flow Detail screen. See the *Guided Flow Detail Screen* subsection in this topic for more details.

Guided Flow Detail Screen



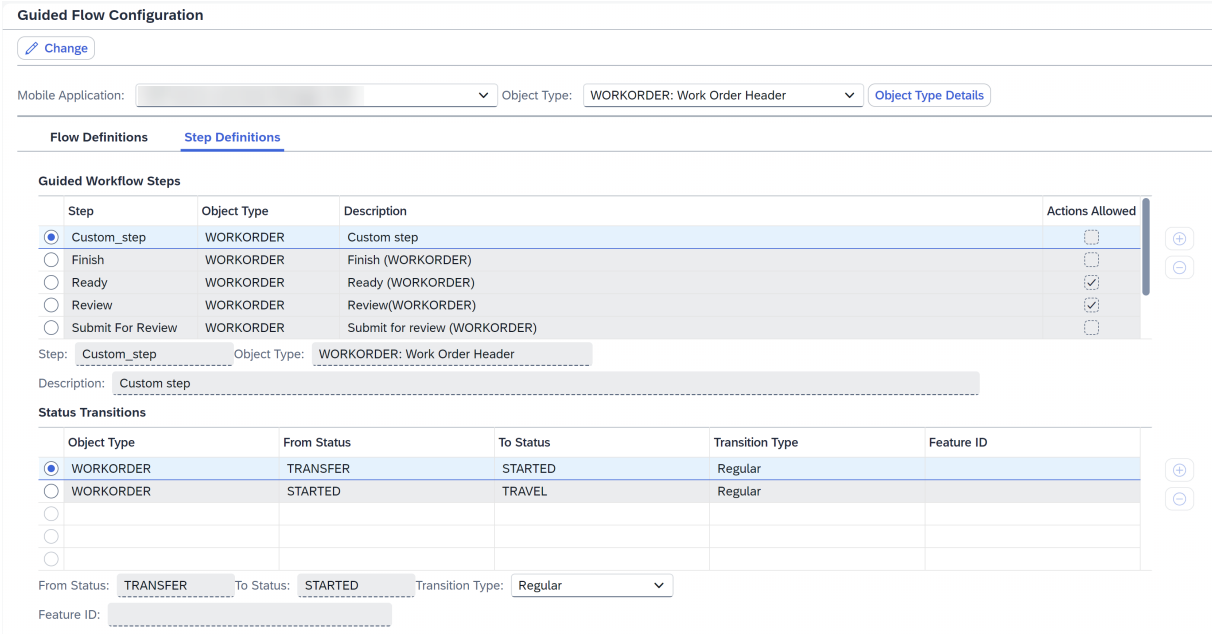
- **Flow ID:** Identifier for the flow. You can name it whatever you'd like. For example, *MT01*.
- **Description:** Human-readable description of the flow. For example, *Maintenance Technician - Basic Work Order*.
- **Object Type:** The object type the flow is designed for. For example, *WORKORDER*.
- **Feature ID:** Assign the flow to a feature. The flow will only be active if the feature is enabled. If the Feature ID field is blank, the flow is available regardless of feature enablement. For example, *PM_SUPERVISOR_MODE* flows can only be assigned to one feature.
- **User Persona:** Assign a user persona to a flow. The flow is only available to users assigned to the persona. If left blank, the flow is available for all app personas. For example, *MAINTENANCE_TECHNICIAN*.
- **Role:** Designate whether the flow applies to the technician or the supervisor role.
- **Object Group:** Choose an object group to further differentiate between object types. For example, *ORDER_TYPE*.
- **Object Group Value:** Provide a value for the selected object group. For example, *PM01*.
- **Object Group 1:** Choose a second object group to further differentiate between object types. For example, *Priority*.
- **Object Group 2:** Provide a value for the selected second object group. For example, to define a flow for High Priority PM01 type maintenance orders, you can maintain the following values in the flow header:
  - Object Group = ORDER_TYPE
  - Object Group Value = PM01
  - Object Group 1 = Priority
  - Object Group 1 Value = 2
- **Default:** Use the Default flag to designate a default row. For example, you've got multiple flows defined for the same object type, persona, role, and feature, and the same object group criteria is met. You can then use the Default flag to designate which flow will be used.

Step Definitions Tab

Guided workflows consist of a series of steps. Steps use the statuses defined against the objects at the mobile application level.

Steps are defined for an object type. Each step contains a list of status transactions a mobile user can perform within the given step. Note that each step must contain at least one status transition.

When adding a status transition to a step, define the transition type and assign a feature ID to the status transition. If a status transition has a feature ID assigned, it is only available on the mobile device if the feature is enabled.



6.3.2.8 RFC Channel Integration Settings

RFC, or Remote Function Call, enables you to call and execute predefined functions in a remote system or in the same system. RFCs manage the communication process, parameter transfer, and error handling.

6.3.2.8.1 Mobile Data Object Configuration Settings

A mobile data object, or MDO, represents a mobile semantic view of data and activity combination for an SAP business object.

Mobile data objects are data repositories in the namespace that can get, create, update, and delete information in SAP. They encapsulate the business logic of mobile applications by defining transactions, data structures, and business rules.

The following are the types of MDOs available for your MAIF app:

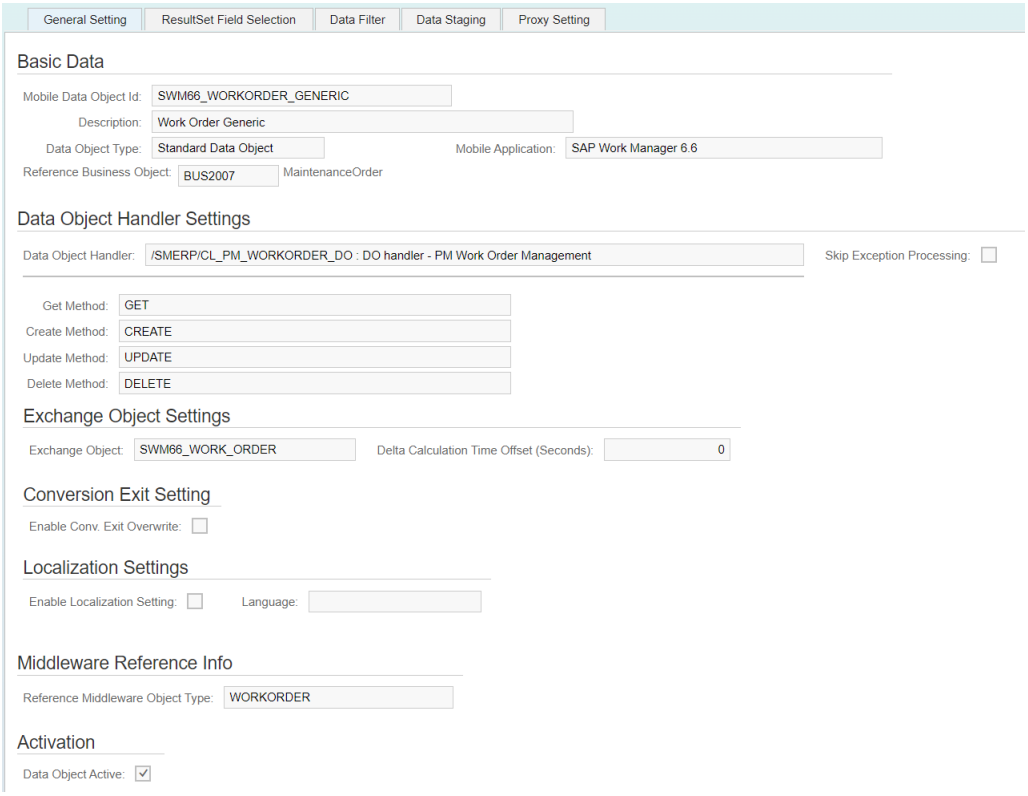
- **Data Table (DT):** A simple representation of SAP BusinessObjects KEY and VALUE.
- **Complex Table (CT):** A two-dimensional representation of a business object with a single table of multiple columns.
- **Standard Data Object (DO):** A multi-dimensional representation of a business object with multiple tables representing different subsets of the business object.
- Workflow Object (WF)
- Composite MDO (CM)

> ⚠ Caution
>
> Only administrators or mobile application developers should create, copy, or change mobile data objects.

Use the ConfigPanel to modify MDO properties such as object type, class handlers, data filters, and other settings. For example, instead of modifying BAPIs to change what information is retrieved from SAP and pushed out to mobile devices, administrators use the ConfigPanel to modify MDOs and set up data filter rules.

General Setting Tab

Use the *General Setting* tab to modify the general settings for a chosen mobile data object.



- **Basic Data:** The Basic Data section provides general information about the specific mobile data object. The basic data information is used in tabs of the Mobile Data Object screen.

- **Mobile Data Object ID:** Required field. Enter the name of the MDO, limited to 40 characters
- **Description:** Required field. Enter a brief, easy to understand description of the MDO, limited to 60 characters
- **Data Object Type:** A dropdown list of the three MDO types:
  - **Data Table:** A simple representation of the SAP BusinessObjects KEY and VALUE
  - **Complex Table:** A two-dimensional representation of the business object with a single table of multiple columns
  - **Standard Data Object:** A multi-dimensional representation of a complete business object. It can have multiple tables representing different subsets of the SAP BusinessObjects.
- **Mobile Application:** Name of the mobile application. Choose the mobile application from the dropdown list.
- **Reference Business Object:** SAP business object for which the MDO is being created.

- **Data Object Handler Settings:** Use the Data Object Handler Settings section to configure the methods of the MDO.
  - **Data Object Handler:** Name of the ABAP OO class handler from the class repository of SAP. The ABAP OO class handler is developed by the application developer with predefined business logic and scope to perform fetch, create, delete, or update activities for an SAP business object.
  - **Get Method:** Method defined in the class handler that fetches data for the underlying SAP business object (optional)
  - **Create Method:** Method defined in the class handler that creates data for the underlying SAP business object (optional)
  - **Update Method:** Method defined in the class handler that updates data for the underlying SAP business object (optional)
  - **Delete Method:** Method defined in the class handler that deletes data for the underlying SAP business object (optional)
  - **Skip Exception Processing:** When checked, the exception processing step is not invoked if an exception occurs during MDO handling
- **Exchange Object Settings:** Allows you to associate the MDO with an exchange object. Configure the exchange object using the *Exchange Object Configuration* screen in the ConfigPanel.
  - **Exchange Object:** Name of the exchange object as defined in the SAP mobile exchange persistent layer. Specify an exchange object from the dropdown menu if the selected class handler uses the mobile exchange persistent layer to determine data exchanges to the mobile application.
  - **Enable Conv. Exit Overwrite:** When checked, you can define specific internal and external conversion settings in the *Technical Settings* screen of the ConfigPanel.
- **Localization Settings:** When you enable localization in the MDO configuration, you can assign a localization language to an MDO, which is used for language related distribution. For example, a complex table MDO with localization language enabled returns language relevant descriptions in the specified localization language instead of the user logon language.
  - **Enable Localization Setting:** Check to allow localization
  - **Language:** Assign the localization language to the MDO
- **Middleware Reference Info:** If the middleware is specified, the MDO performs the standard exchange process as well as a lookup in the client object register table to determine what information the client contains. If data was removed from the client that still exists in the SAP table, the data is readded to the client during the transmit.
  - **Reference Middleware Object Type:** Middleware objects are set through the Administration portal (optional)

- **Activation:** Use the checkbox to enable or disable an MDO in the application without deleting the MDO.
  - **Data Object Active:** When checked, the MDO is in an active state. If unchecked, the MDO performs no actions

ResultSet Field Selection Tab

When you enable a field selector function for a class handler, you can then select fields for the GET method to populate. The class handler is mobile application neutral. It supplies more data than the mobile application needs. Therefore, to preserve system performance, customize field usage settings to only retrieve required data for the mobile application. The ability to customize prevents the need to develop a new class handler for each mobile application.

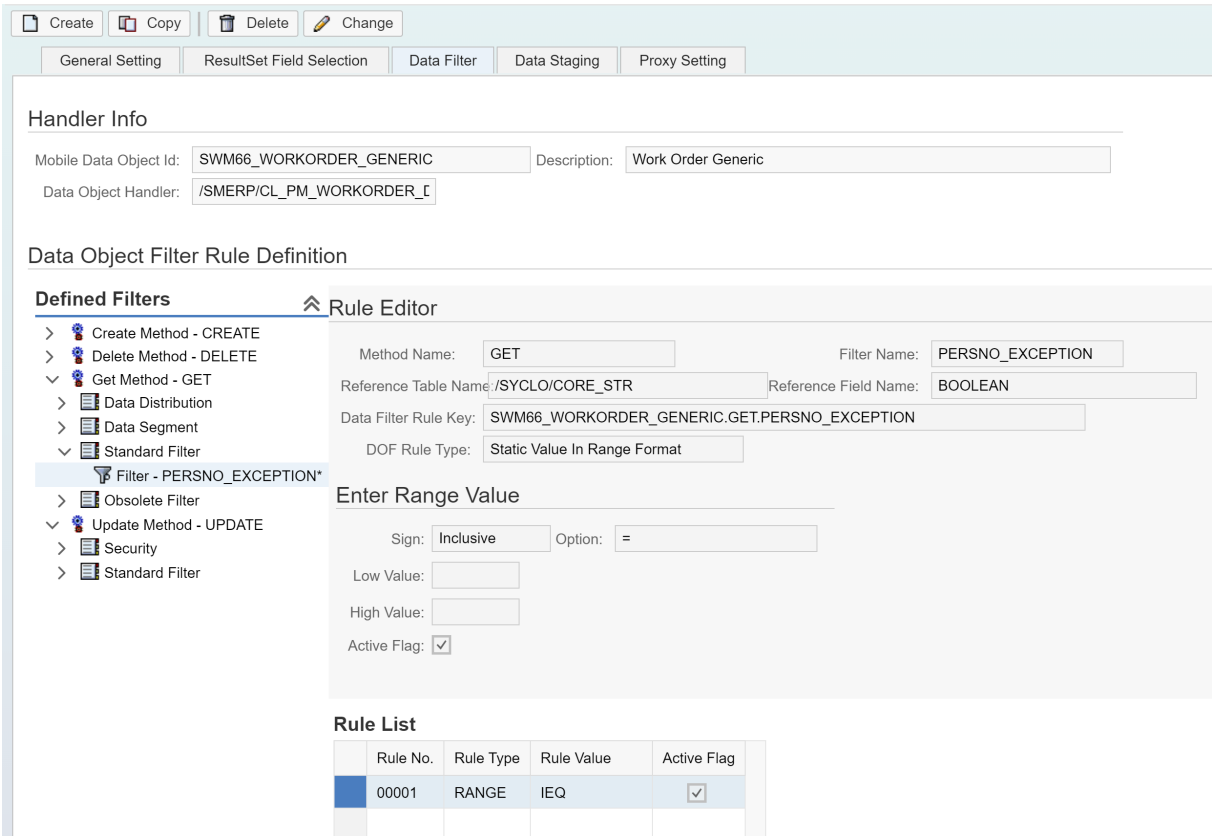


- **Handler Info fields:**
  - **Mobile Data Object ID:** Name of the MDO
  - **Description:** Description of the mobile data object, limited to 60 characters. Required field.
  - **Data Object Handler:** Name of the ABAP OO class handler from the class repository of SAP. The ABAP OO class handler is developed by the application developer with predefined business logic and scope to perform fetch, create, delete, or update activities for an SAP business object.
  - **Get Method:** Name of the GET method set in the *General Setting* tab.
- **Field Selection Detail fields:**
  - **Field Catalog column:** Lists all the fields that can be returned by the class handler method, grouped in the order of the name of the class handler method, SAP table name, and field name. To display all information in this column, click the arrows to the left of a name to expand the row.
  - **Field Active column:** When checked, the data for the selected field is returned by the class handler method
  - **Field Description column:** Description of the specific field in the SAP table
  - **Data Format column:** How data is presented
  - **Sort Options:** When a large amount of information is presented, use the sort options to find the information required easily. When you select a different radio button, the rows collapse. Expand them again to display the new field sorting.

Data Filter Tab

When a data filter function is enabled for a class handler, the option exists to define various types of filter rules to control what data a user can view on the mobile application based on the business process of the customer. In an SAP environment, each user is assigned a role-based profile with authorization restrictions for what data is viewed and which activities performed.

For example, a user who works for a specific plant should not be able to view data for another plant. Data filter rules allow you to restrict data access for mobile applications. Data filters can be user-dependent or applied to the entire mobile application.



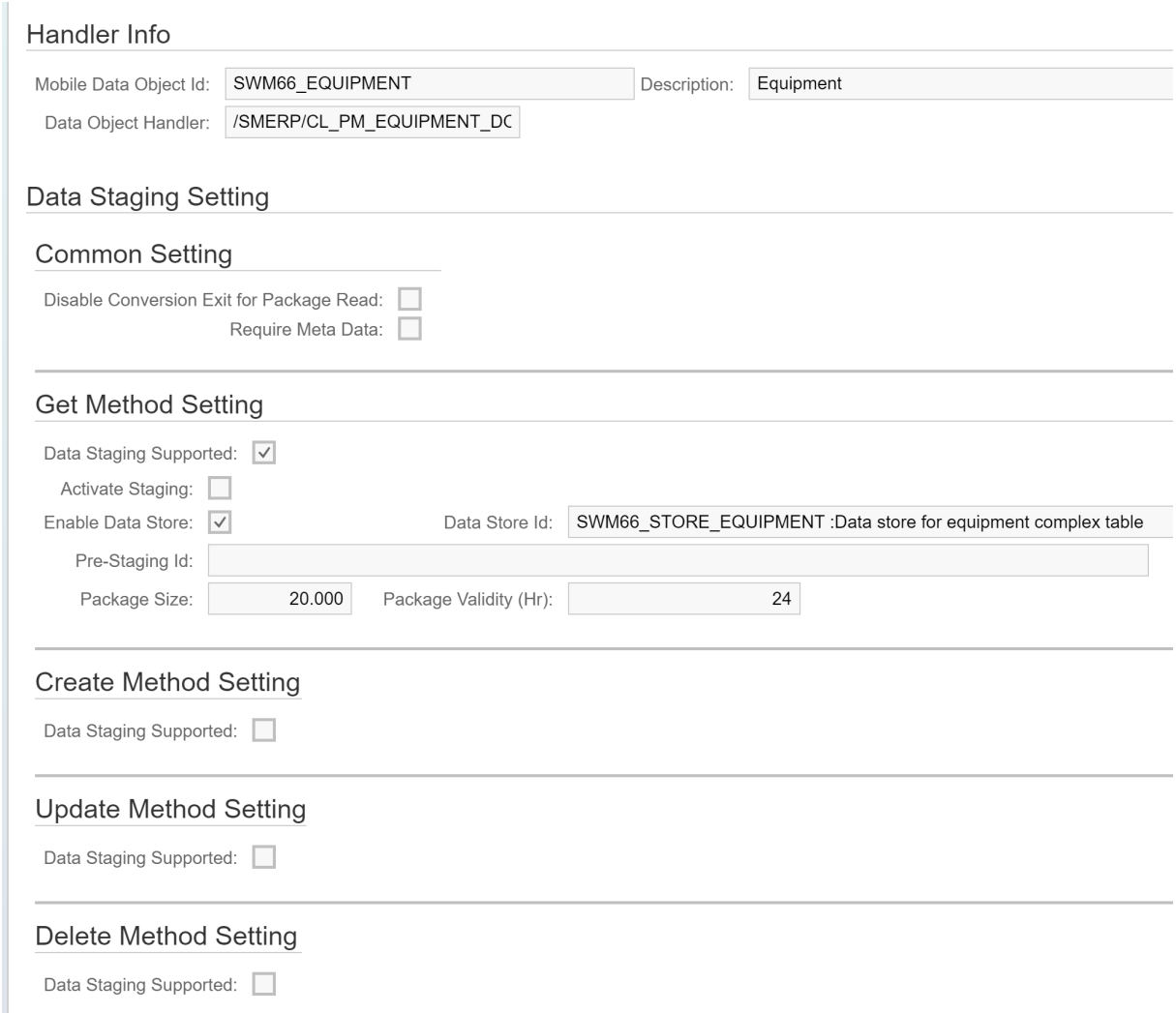
- **Handler Info fields:**
  - **Mobile Data Object ID:** Name of the MDO
  - **Description:** Description of the mobile data object, limited to 60 characters. Required field.
  - **Data Object Handler:** Name of the ABAP OO class handler from the class repository of SAP. The ABAP OO class handler is developed by the application developer with predefined business logic and scope to perform fetch, create, delete, or update activities for an SAP business object.
- **Defined Filters list:**
  The Defined Filters tree lists all data filters supported by the class handlers defined in the *Data Object Handler Settings* field in the *General Setting* tab. To expand the tree, click the arrows to the left of the class handler methods to display the filters associated with the methods.
- **Rule Editor fields:**
  - **Method Name:** Name of the class handler method where the data filter is defined. The data filter function is only supported for the GET method
  - **Filter Name:** Name of the filter as defined in the class handler method. The filter name is defined by the class handler developer and is not editable.
  - **Reference Table Name:** Technical name of the SAP database table where this filter is applied. The reference table name is defined by the class handler developer and is not editable.
  - **Reference Field Name:** Technical name of the SAP database table field where this filter is applied. The reference field name is defined by the class handler developer and is not editable.
  - **Data Filter Rule Key:** Internal technical key used by the framework at runtime
  - **DOF Rule Type:** Type of rule

  Each rule set has different settings options:
  - **User Profile Parameter rule**

        - **Parameter ID:** Memory parameter ID as defined in SAP and specified in the user profile. Click the icon to the right of the field box to perform a search on all available parameter IDs.
        - **Description:** Description of the memory parameter ID. The description field is not editable and is automatically filled in when the parameter ID is selected.
        - **Active Flag:** When checked, the rule is active
    - **Static Value in Range Format rule**
        - *Sign*, *Option*, *Low Value*, and *High Value* are the values for the applicable columns in the *SAP Range Table*.
    - **Syclo Filter Class Handler rule**
        - **Syclo Data Filter Handler:** Name of the handler class as defined in the system
        - **Parameter:** Additional processing information that is passed to the class handler. The parameters are entered as free text, and the syntax of the parameter stream is defined by the developer.
        - **Active Flag:** When checked, the rule is active
    - **Runtime Session Data rule**
        - **Runtime Session Data Name:** Session ID within the specified group
        - **Runtime Session Data Group:** Name of the session group
        - **Active Flag:** When checked, the rule is active
- **Rule List table:** The Rule List table displays a list of rules that have been defined
    - **Rule No.:** Number of the rule that is defined, in chronological order
    - **Rule Type:** Rule type, automatically assigned by the rule type selected in the *DOF Rule Type* field
    - **Rule Value:** Internal rule value saved by SAP

Data Staging Tab

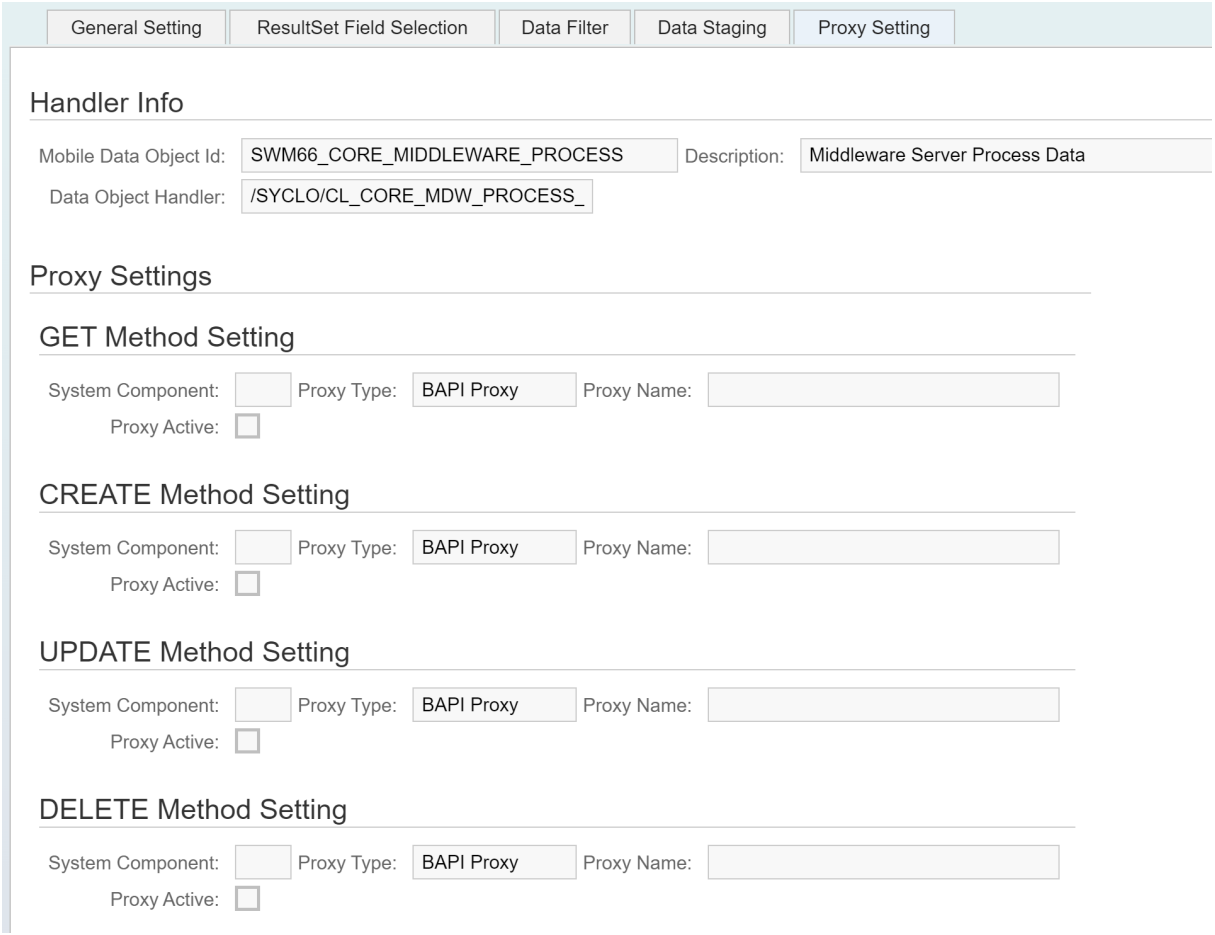
If an application processes a large amount of objects, data staging of the objects can assist with processing times. If an object is configured for data staging, the data within the object is stored as a package and is split into packets. The data can contain metadata and tagging for easy life-cycle management and data lookup. Standard APIs are provided for package management.



- **Handler Info fields:**
  - **Mobile Data Object ID:** Name of the MDO
  - **Description:** Description of the mobile data object, limited to 60 characters. Required field.
  - **Data Object Handler:** Name of the ABAP OO class handler from the class repository of SAP. The ABAP OO class handler is developed by the application developer with predefined business logic and scope to perform fetch, create, delete, or update activities for an SAP business object.
- **Data Staging Setting fields:**
  Get, **Create**, **Update**, and **Delete Method Setting:** When a checkbox is marked for a specific method, data staging is active for that method

Proxy Setting Tab

Use the *Proxy Setting* tab to define any proxy settings.



- **Handler Info fields:**
  - **Mobile Data Object ID:** Name of the MDO
  - **Description:** Description of the mobile data object, limited to 60 characters. Required field.
  - **Data Object Handler:** Name of the ABAP OO class handler from the class repository of SAP. The ABAP OO class handler is developed by the application developer with predefined business logic and scope to perform fetch, create, delete, or update activities for an SAP business object.
- **Proxy Settings fields:** The following fields are available for each of the methods:
  - **System Component:** Identifies the remote system
  - **Proxy Type:** BAPI Proxy is the only supported proxy type
  - **Proxy Name:** BAPI name of the remote system
  - **Proxy Active:** When checked, proxy settings are active for the specific method

6.3.2.8.2 BAPI Wrapper Configuration Settings

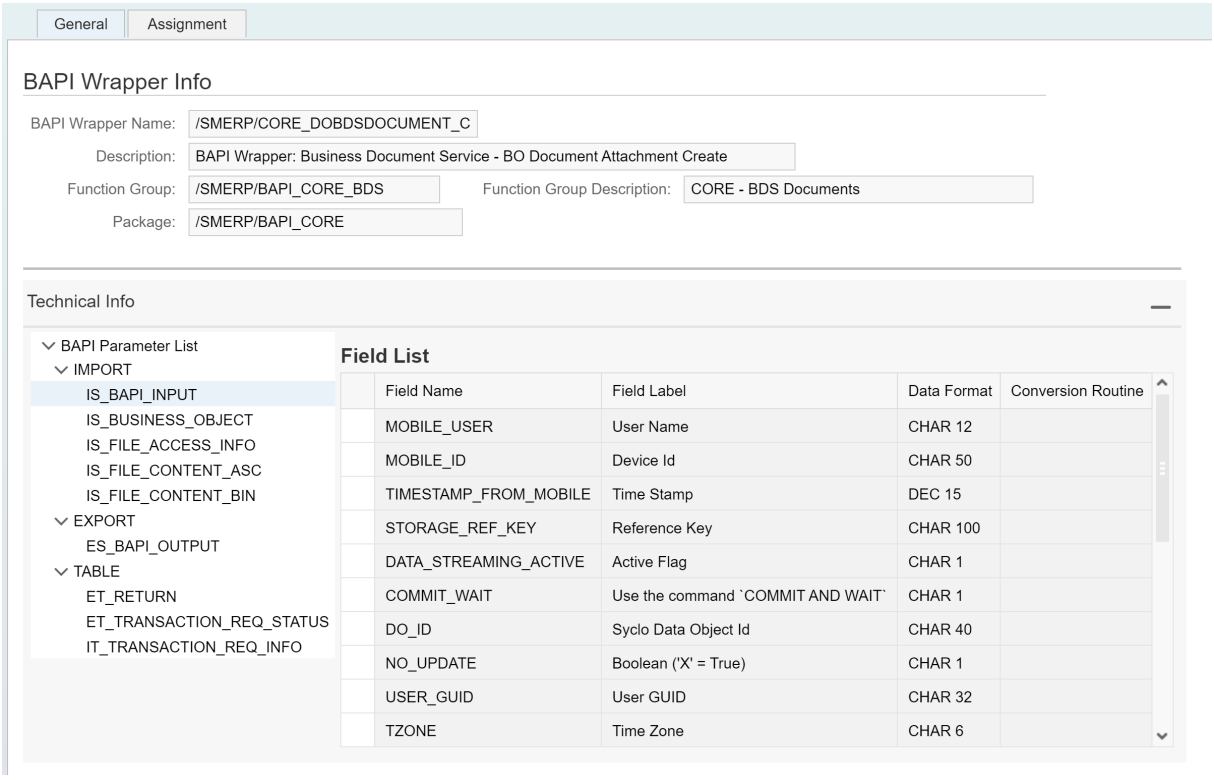
A BAPI wrapper is created by the application developer to expose SAP data and business logic to the mobile application. By design, the BAPI wrapper does not contain any business logic. Each BAPI wrapper is assigned to a specific method type (GET, CREATE, UPDATE, or DELETE) of an MDO to perform the required business logic. By decoupling the business logic from the BAPI wrapper, it is possible to switch MDOs without affecting the underlying mobile application definition.

The *BAPI wrapper Configuration* screen contains the following tabs:

- General
- Assignment

General Tab

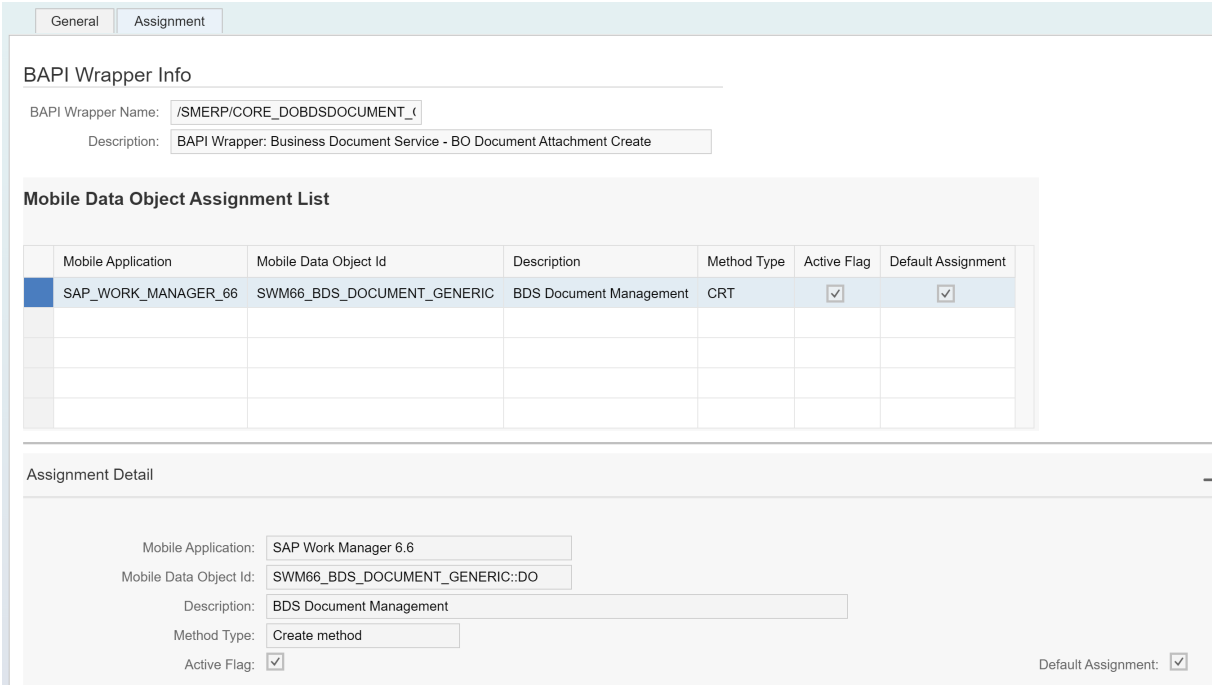
Use the *General* tab to modify general settings for a selected BAPI wrapper.



- **BAPI Wrapper Info fields:**
  - **BAPI Wrapper Name:** Technical name of the Remote Function Call (RFC) function module defined in the system
  - **Description:** Description of the BAPI wrapper, limited to 60 characters (required)
  - **Function Group:** Function group to which the BAPI belongs
  - **Function Group Description:** Description of the function group, limited to 60 characters
  - **Package:** SAP group to which the function group and the BAPI wrapper both belong
- **Technical Info:** The Technical Info, or BAPI wrapper list, provides an expandable tree of the available BAPI wrapper function groups and the BAPI wrapper names associated with each function group. Use the arrows to the left of the function name to display all BAPI wrapper names under the function group.

Assignment Tab

Use the Assignment tab to hook up BAPI wrapper assignments to mobile data objects. In this tab, you can change the assignment of a BAPI wrapper to specific mobile data objects, assign a new mobile data object to the BAPI wrapper, or delete a mobile data object assignment from the BAPI wrapper.



- **BAPI Wrapper Info fields:**
  - **BAPI Wrapper Name:** Technical name of the Remote Function Call (RFC) function module defined in the system
  - **Description:** Description of the BAPI wrapper, limited to 60 characters (required)
- **Mobile Data Object Assignment List:**
  - **Mobile Data Object Assignment table:** Table that displays which mobile data objects are assigned to each BAPI wrapper. All column information is replicated in the *Assignment Detail* section below the table.
    To highlight an individual row, click the gray square to the left of the *Mobile Application* column in that row.
- **Assignment Detail fields:** Information in these fields changes depending on which row you highlight in the *Mobile Data Object Assignment List* table
  - **Mobile Application:** The specific mobile application and its release number. This field is noneditable
  - **Mobile Data Object ID:** The name of the mobile data object in a dropdown field
  - **Description:** A brief, easy to understand description of the mobile data object, limited to 60 characters. This field is noneditable
  - **Method Type:** Mobile data object method (*GET*, *CREATE*, *UPDATE*, or *DELETE*) that is assigned to the BAPI wrapper
  - **Active Flag:** When checked, the mobile data object is in an active state. If unchecked, the mobile data object performs no actions

- **Default Assignment:** When checked, the specific mobile data object assigned to that BAPI wrapper is primary. If no mobile data object ID is specified in the standard BAPI wrapper input parameter `<IS_BAPI_INPUT-DO_ID>`, then the primary mobile data object is used during runtime.
  It is possible to assign multiple MDOs to the same BAPI in a single mobile application.
  To override the default MDO assignment at runtime and to specify the desired MDO, define the `<DO_ID>` field in `<IS_BAPI_INPUT>`.

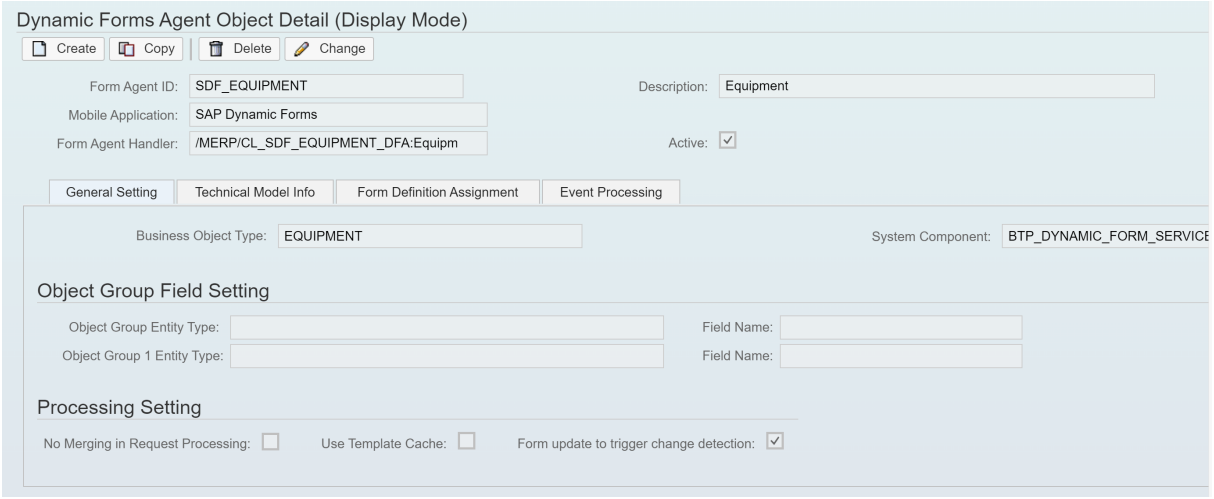
6.3.2.9 SAP Dynamic Forms Agent Settings

An agent is responsible for a single SAP buisness object type and handles all relevant form operations.

The following fields are at the top of each tab of the SAP Dynamic Forms Agent Settings page:

- **Form Agent ID:** Unique identifier for the customizing object
- **Form Agent Handler:** ABAP class that contains the agent's object-specific implementations

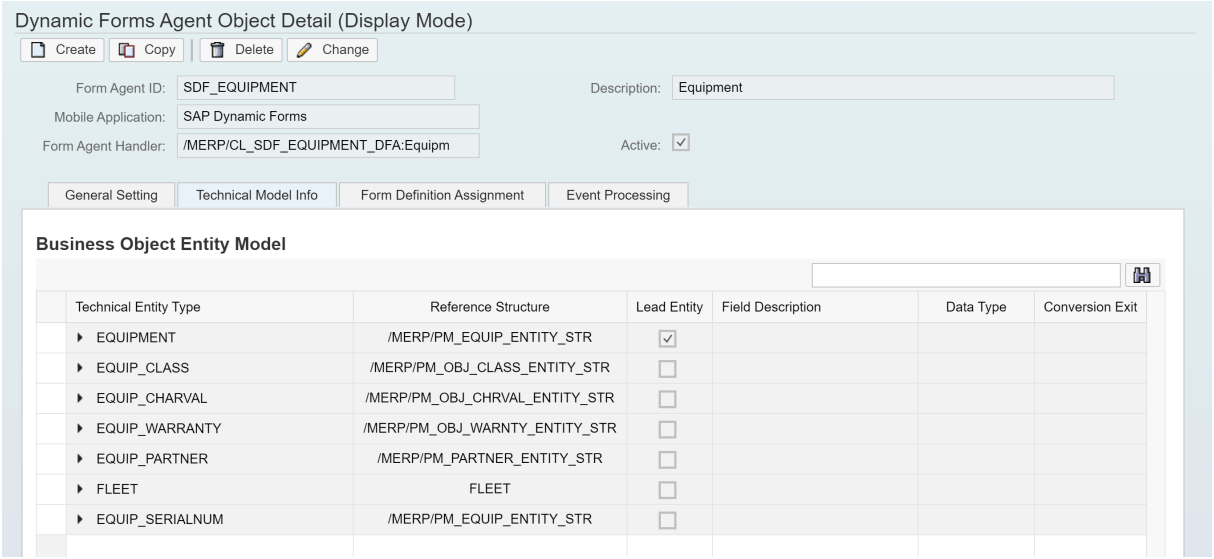
General Setting Tab



- **Business Object Type:** The SAP object for which the agent is responsible. Value is defined in the form agent handler.
- **System Component:** Defines the mobile application system component that contains all the SAP BTP SAP Dynamic Forms service connection details.
- **Object Group Field Setting:** Object groups are an optional way to subdivide an SAP business object by a certain entity type and field.
- **Processing Setting:**
  - **No Merging in Request Processing:** Enable this setting if requests for the same form instance and request type should be executed separately.
  - **Use Template Cache:** A periodically updated cache stores the form definitions and its categories. Enable this setting if the cache should be used to search for form definitions. If the setting is disabled, API calls are used instead.

- **Form Update to Trigger Change Detection:** Any changes to form instances update the exchange table for the SAP objects associated with the form.

Technical Model Info Tab



The *Technical Model Info* tab displays the technical entity model of the dynamic forms agent. These entity types and data are available to be used during the form definition assignment and event processing.

Form Definition Assignment Tab

Form definition assignment configuration determines the behavior of the automatic form definition determination. There are multiple configuration options and enhancement points available.

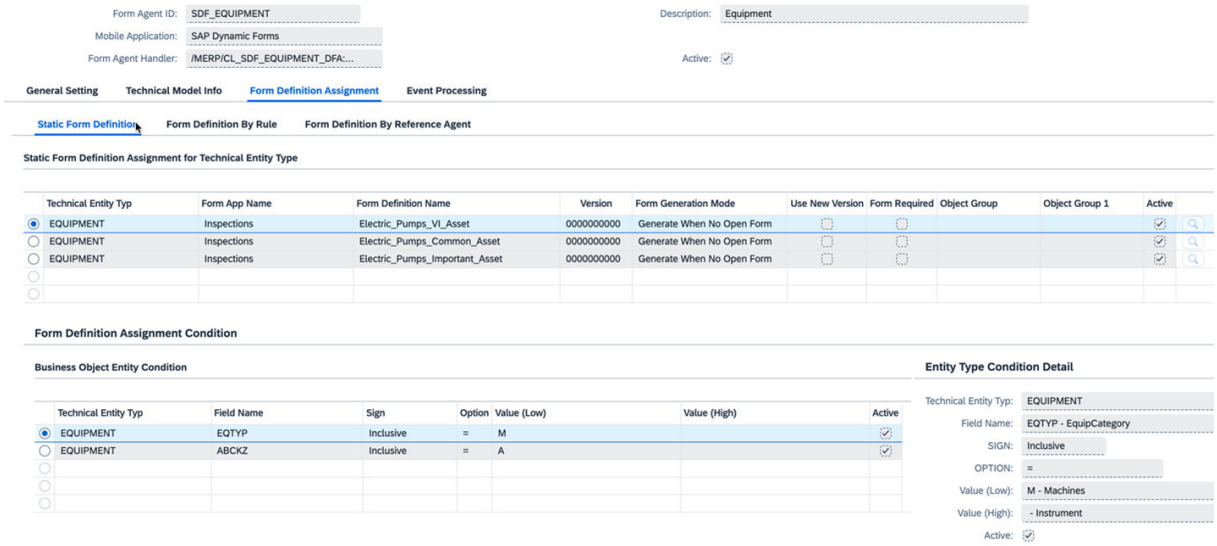
- **Technical Entity Type:** Determines which entity of the object type to assign the form to
- **Form Generation Mode**
  - **Always Generate New Form:** If a list of form definitions has met all the requirements for form creation, a form instance is always created (even if an existing instance of the form is already created and assigned to the object).
  - **Generate When No Open Form:** Before creating a form instance, checks if the object has an instance of the same form definition that is in an opened status (*New*, *In Process*, or *Reopened*). If there is, a new form instance is not created.
  - **Single Form Allowed:** Only a single instance of a form definition can be assigned to the same SAP object at a time. The status of the existing form instance is not checked in this scenario.
- **Use New Version:** Enabling this means the automatic form definition determination logic always uses the newest form definition version
- **Form Required:** Marks each created form instance as mandatory. A mandatory form instance means the form instance must be in a completed status before the SAP object can also be completed. Example: Form Instance A must be completed before the associated work order operation can be confirmed.

- **Object Group / Object Group 1:** Enter a value in one or both fields that corresponds to the entity type and field defined in the *General Settings* tab. At runtime, the entity type and field defined in General Settings are used to look up the object data and compare its value to the value defined in these configuration fields.
- **Business Object Entity Condition:** Use these settings to define conditions the SAP object must meet before triggering the automatic form definition determination flow. These conditions involve defining range tables for the SAP object's entity types and its fields. The range tables are used at runtime to compare against the SAP object.

The following assignment types can be used in automatic form definition determination:

- Static form definition
- Form definition by rule
- Form definition by reference agent

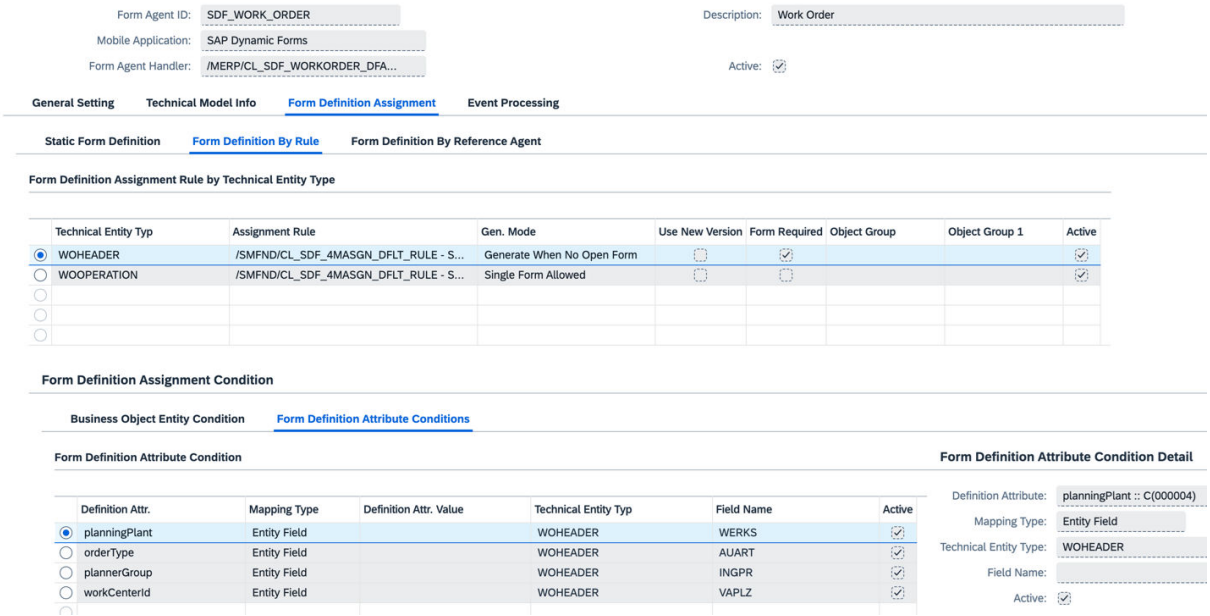
Assignment Type - Static Form Definition



Statically define specific form definitions that should be assigned to the SAP object. Use the *Form App Name*, *Form Definition Name*, and *Version* columns to define the form definition.

The magnifying glass icon can be used for form definition search help.

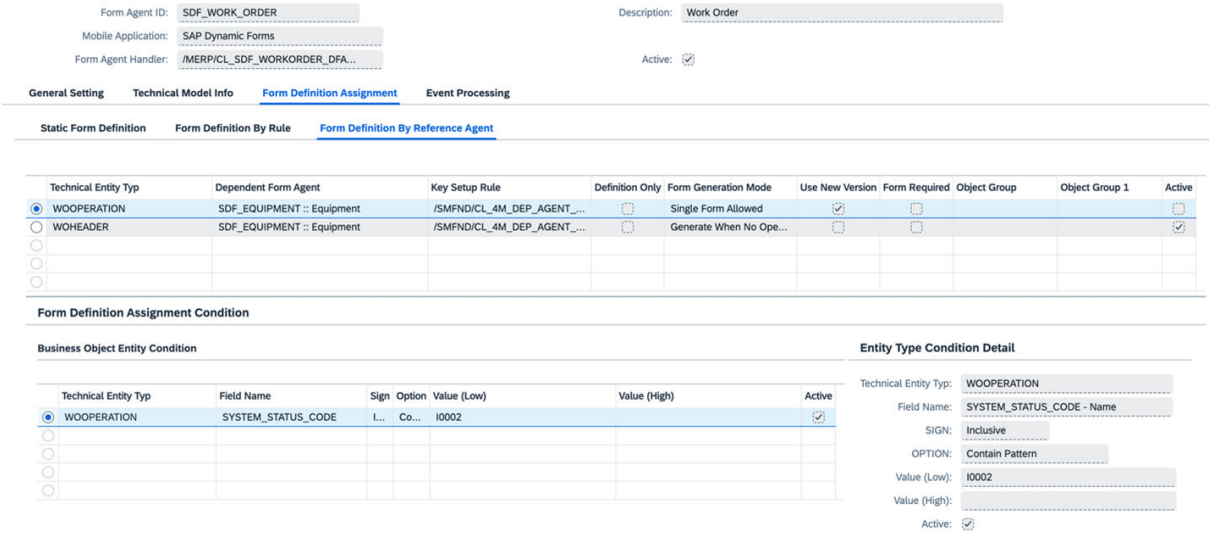
Assignment Type - Form Definition by Rule



Dynamically decide form definitions to create based on the runtime data of the SAP object.

- **Form Definition Attribute Conditions:** Define mappings of the technical entity type fields to *Form Definition Categories*. At runtime, the technical entity type data is compared against the values defined in the Form Categories Fiori app.
  - **Definition Attribute:** The category from the Form Categories Fiori app that should be considered when attribute matching.
  - **Mapping Type**
    - **Entity Field:** Compare the definition attribute to the technical entity type field
    - **Constant Value:** Compare the definition attribute to the value in the Definition Attribute Value field
  - **Definition Attribute Value:** a static value that is used to compare against the definition attribute when the mapping type is *Constant Value*
  - **Technical Entity Type:** The technical entity type that is relvant to this mapping configuration
  - **Field Name:** The field name of the corresponding technical entity type that is used during the runtime data comparision
- **Assignment Rule:** The selected ABAP class used to decide which SAP object entity key(s) should be assigned to a new form instance(s). The default class assigns new form instances to the key(s) defined in the technical entity type column.

Assignment Type - Form Definition by Reference Agent



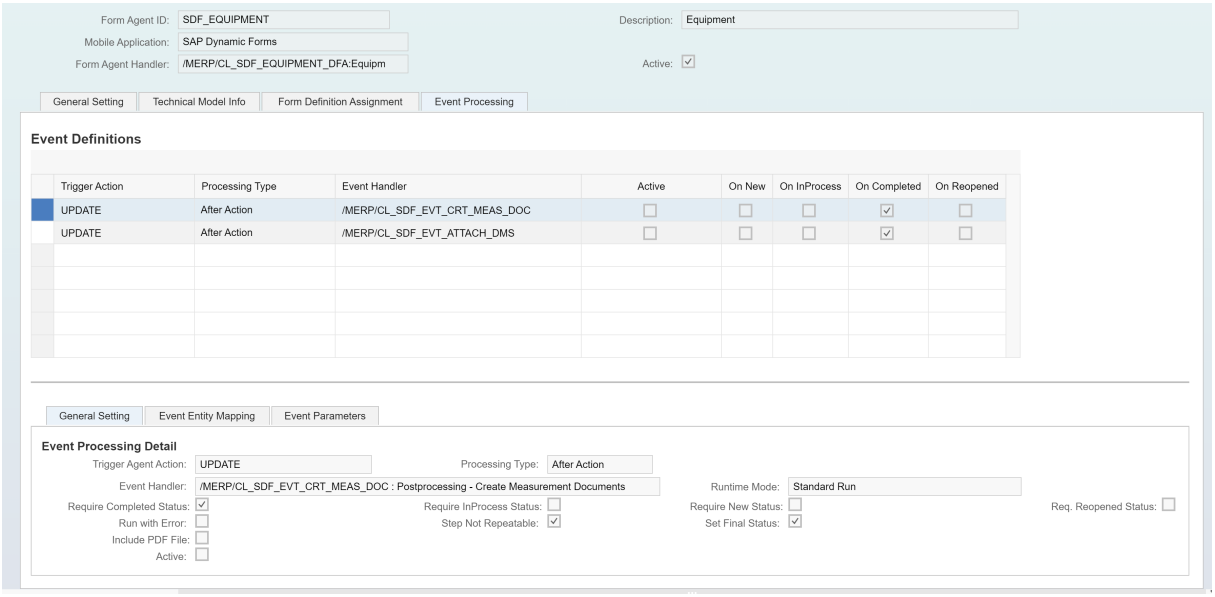
Defer the decision of which form definitions to create to the dependent agent. The parent agent passes the reference key to the child agent, where the child agent runs its own form definition assignment rules. A form instance created by the child agent is linked to both the parent and child objects.

- **Dependent Form Agent:** The agent used to run its own form definition assignment rules based on the configuration of the agent
- **Key Setup Rule:** Using the technical entity type data, this handler determines the object key to be used in the dependent form agent.
- **Header Entity Only:** If set to true, only create and assign the form instance to the header entity type.

Event Processing Tab

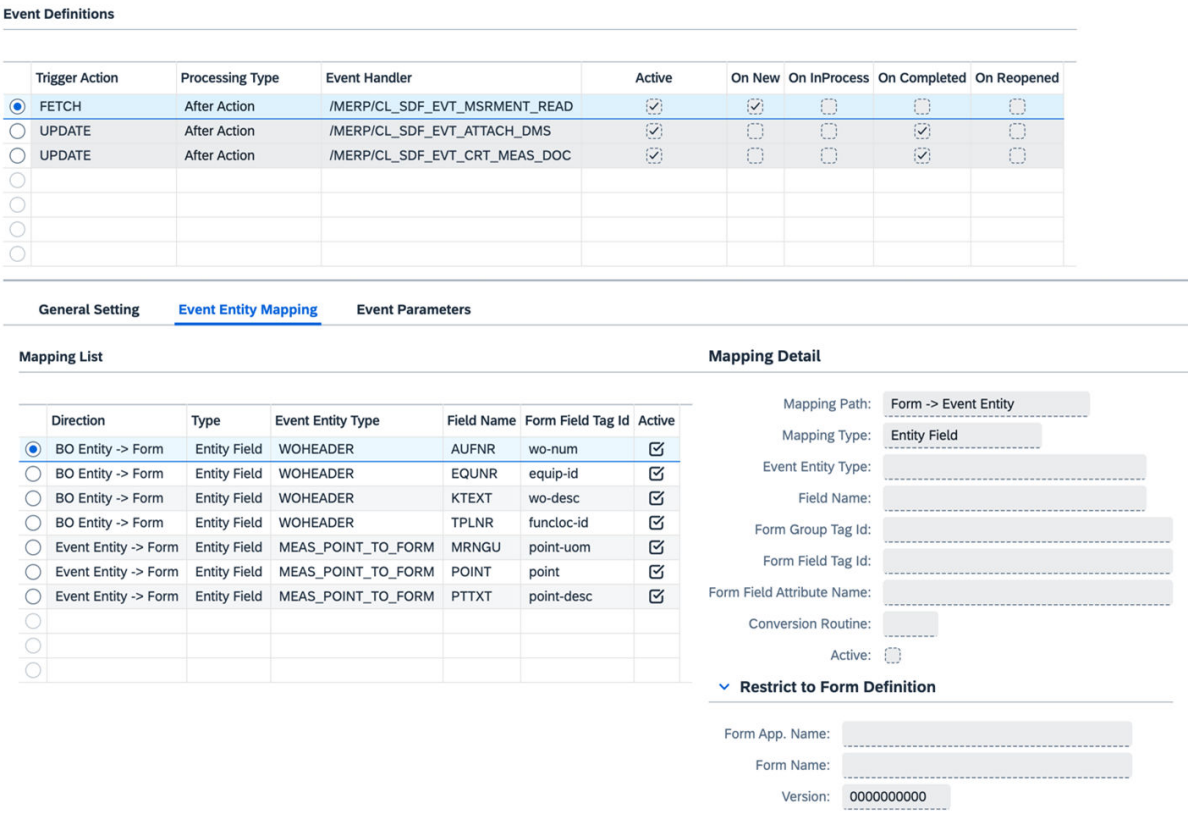
Events can be triggered throughout the lifecycle of a form to insert data into the form, and/or extract data out of the form to create or change SAP data. Event processing configuration allows you to define the event handlers that will run the logic, as well as define the conditions when the event should occur.

General Setting Subtab



- **Trigger Agent Action:** Action on which the event should be triggered
- **Processing Type:** Defines whether the event should trigger before or after the action
- **Event Handler:** The ABAP class that runs the logic of the event
- **Runtime Mode:** Determines how the event will run and what happens when events occur:
  - **Standard Run:** The event executes synchonously
  - **Error Handling with Transaction Queue:** If an error is encountered during the event, an entry is checked into the inbound transaction queue
  - **Always via the Transaction Queue:** Always check the event into the inbound transaction queue instead of running the event synchronously when an event should be triggered
- **Require* Status:** The form instance must be in this status for the event to be triggered
- **Run with Error:** If false, and an error occurs while processing an event, an error is thrown. Only applies to the *Standard Run* runtime mode.
- **Step Not Repeatable:** The same event cannot be run for the same form instance more than once
- **Set Final Status:** After the event is run successfully, the form instance is set to the *Final* status. Forms in the Final status are not editable. Therefore, the status is unmodifiable, and events cannot be run on them.
- **Include PDF File:** A PDF file of the form instance is generated automatically and can be referenced by the event handler.

Event Entity Mapping Subtab

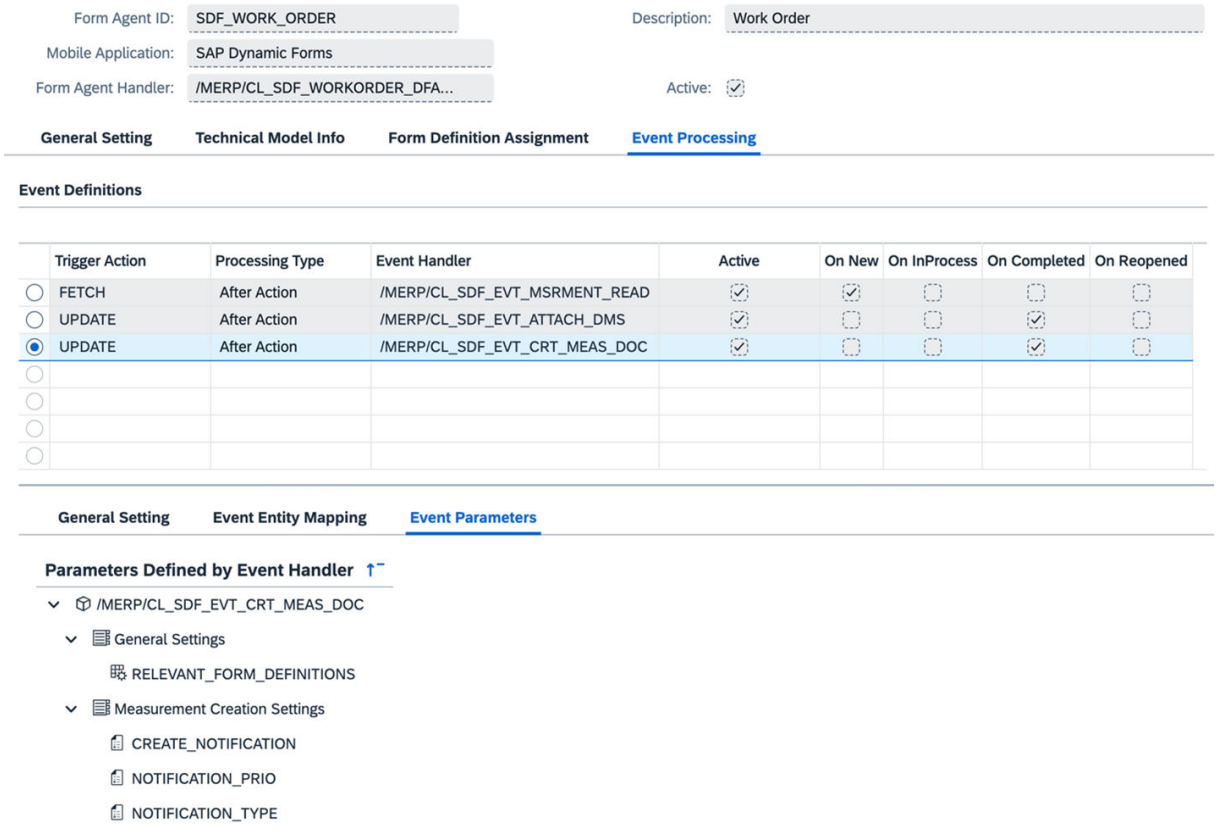


Map entity fields to form XML tags. The configuration can then be used in the event handler to easily input data into the form, or extract data out of the form.

- **Mapping Type Path:**
  - **Form - Event Entity:** Data input into the form is extracted and placed into the event entity field
  - **BO Entity - Form:** Input SAP object data into the form from the dynamic form's agent technial entity model
  - **Event Entity - Form:** Event handlers can define their own entity structures. This path takes the event entity data and inputs it into the form.
- **Mapping Type:** Map the form XML tag to either an entity field or a constant value
- **Event Entity Type:** The SAP entity that is relevant for this mapping
- **Field Name:** The field name of the corresponding entity type
- **Form Group Tag ID:** SAP Dynamic Forms supports the repeating grid control. Each row of that grid control has an identical XML tag. Define the group tag here.
- **Form Field Tag ID:** The form XML tag relevant to the data
- **Form Field Attribute Name:** An attribute of a form XML tag that can be referenced by putting the attribute name
- **Conversion Routine: Define the standard SAP conversion routine that should be executed on the data**
- **Restrict to Form Definition: Restrict this mapping configuration to a particular form app name and/or form name and/or form version**

Event Parameters Subtab

Event handlers can define parameters for users to define settings at the configuration level. Define the values for those parameters using the *Event Processing tab* > *Event Parameters subtab*.



The following standard event handlers are available:

- **/MERP/CL_SDF_EVT_MSRMENT_READ:** Preprocess the form with measuring point, class, characteristic, and/or characteristic value data
- **/MERP/CL_SDF_EVT_ATTACH_DMS:**Generates a PDF file of the form instance and attaches it to the corresponding object as a DMS document. The *Include PDF File* should be marked as true.
- **/MERP/CL_SDF_EVT_CRT_MEAS_DOC:** Created measurement documents from the measurement readings taken on a form

6.3.2.10 Push Framework Settings

6.3.2.10.1 Push Scenario Definition

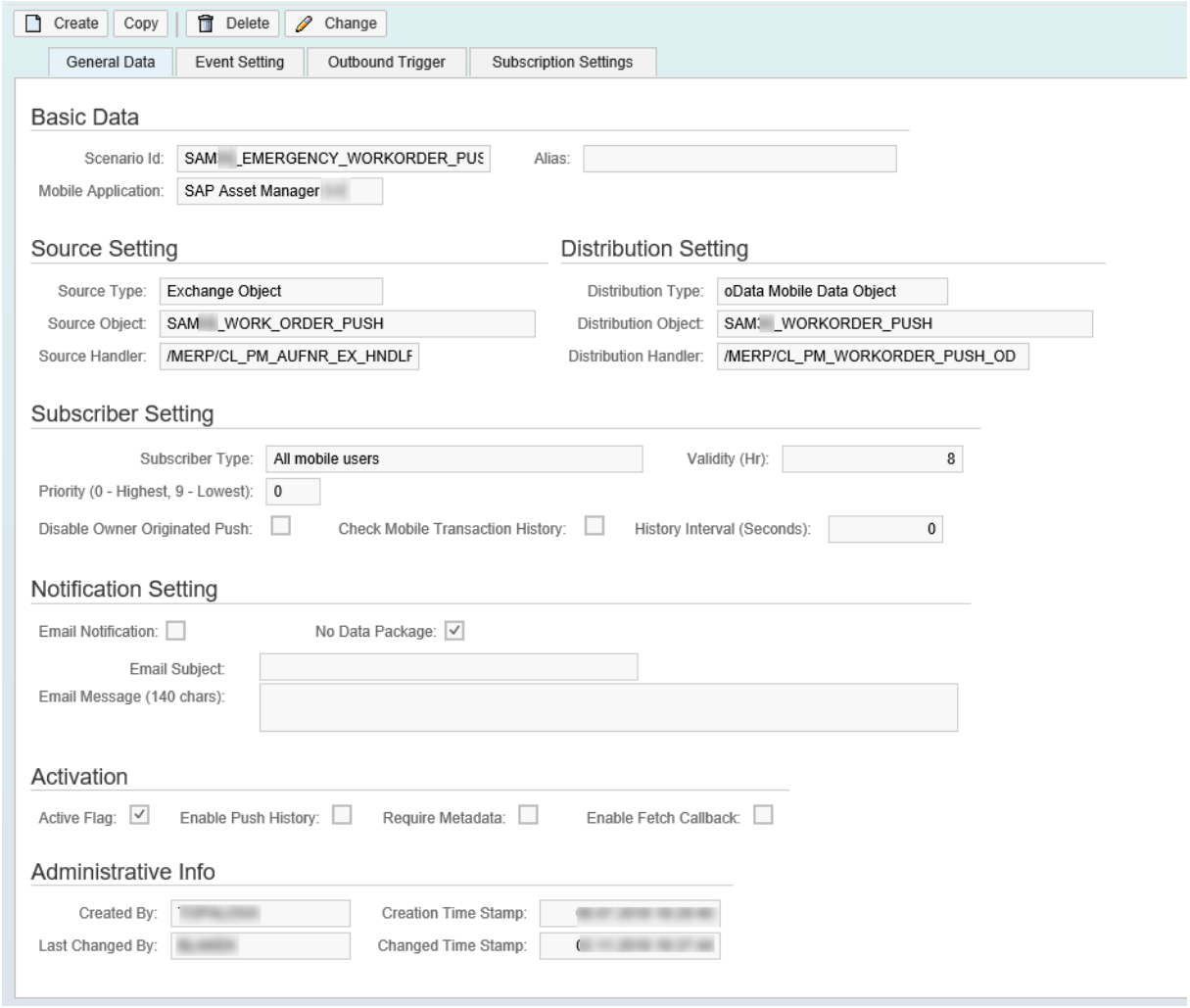
Push scenarios define the trigger conditions, type of data, the mobile users receiving the data, and the users for the data.

A mobile client typically synchronizes with the SAP system by initiating a synchronization request to download the latest application data from the SAP system. Some mobile applications require the SAP system to send application data or push notifications to the client when certain trigger conditions are met. If these trigger conditions are not present, the mobile client does not initiate the synchronization request.

You define trigger conditions through the creation of push scenario definitions. Use the tabs found in the *Push Scenario Definition* page to configure a push scenario. The *Push Scenario Definition* page contains the following tabs:

- General Data
- Event Setting
- Outbound Trigger
- Subscription Settings

General Data Tab



You can define the following attributes in the *General Data* tab:

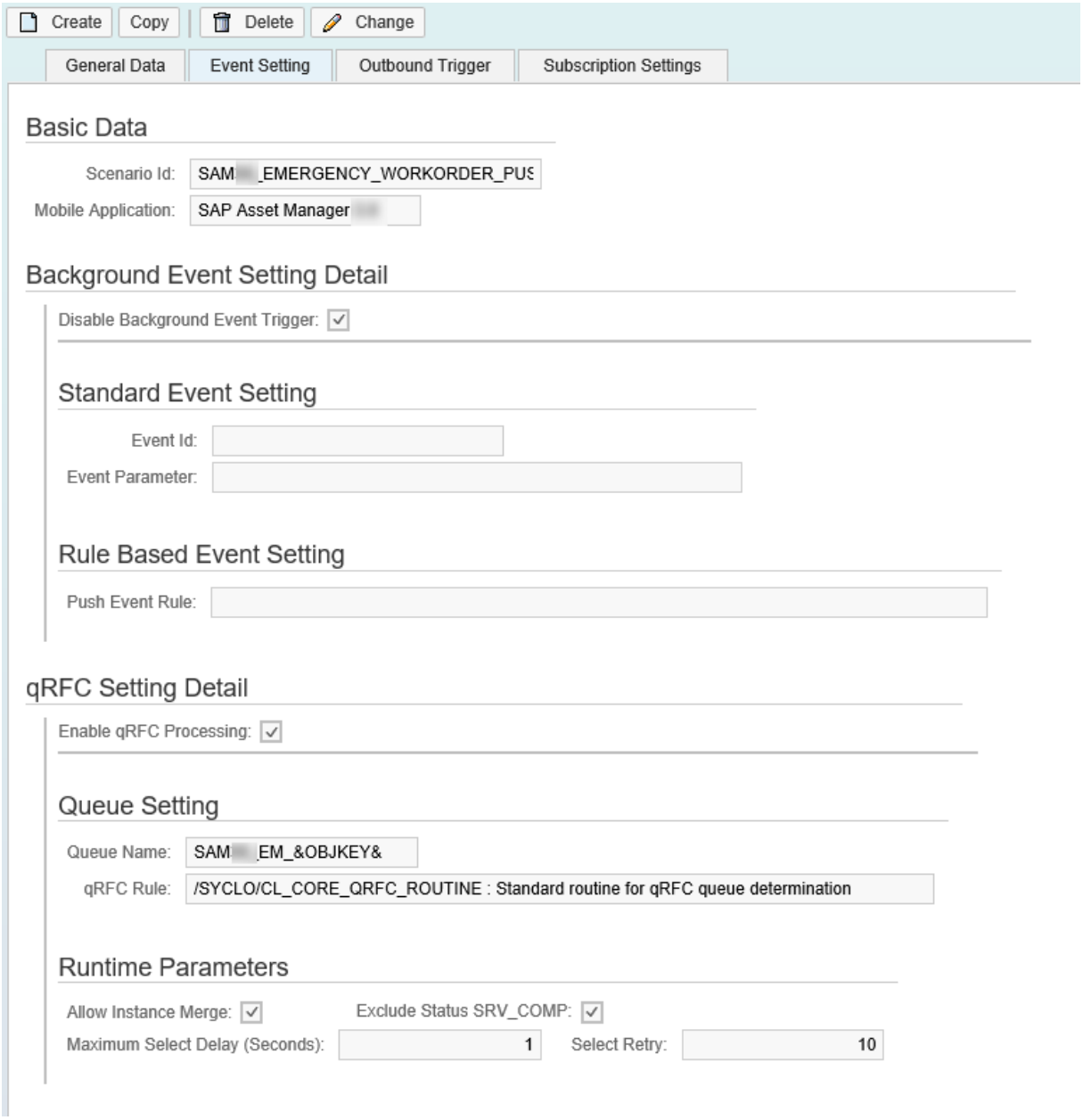
- **Basic Data section:** Enter the ID of the push scenario in the required `<Scenario ID>` field, which is limited to 40 characters with namespace protection. Use either a *Y* or a *Z* namespace. Ensure that the ID is unique in the SAP system. Enter the name of the mobile application in the `<Mobile Application>` field, limited to 40 characters. Give an optional `<Alias>` to the push scenario. Multiple push scenarios can share the same alias, to allow central processing on the client side.
- **Source Setting section:** The `<Source Type>` defines how to trigger the push scenario. Two options are supported:
  - xChange Object: The push scenario is triggered when qualifying data is changed in the SAP system and change conditions defined in the xChange object are detected.
  - Client on Demand Request: The push scenario is triggered based on a request from the mobile client. No data change in the SAP system is required. The client on demand request is not available for OData based mobile applications.

  The `<Source Object>` applies to the source type of the xChange object. The xChange object determines the data change trigger for the push scenario. The `<Source Handler>` is the xChange handler assigned to your selected xChange object.

- **Distribution Setting section:** The `<Distribution Type>` defines what application data is sent and how recipients are determined. Two options are supported:
  - Mobile Data Object: Not supported for the SAP Service and Asset Manager application
  - OData Mobile Data Object: Use *OData Mobile Data Object* for the SAP Service and Asset Manager application. The assigned OMDO determines the recipients for the push notification.

  When you select *OData Mobile Data Object* as a Distribution Type, assign an OMDO configuration object to the OMDO in the `<Distribution Object>` field. The `<Distribution Handler>` is the OMDO handler associated with the assigned OMDO configuration object.
- **Subscriber Setting section:** The `<Subscriber Type>` determines the user pool. The user pool is used to determine who receives the push notification. Enter the amount of time the push instance generated for the push scenario is valid, in hours, in the `<Validity>` field. The `<Priority>` is the processing priority of the push instance. A push instance with a higher priority is processed first.
  When the *Disable Owner Originated Push* checkbox is checked, the user who made the change to the SAP data is excluded from the push recipient list triggered by the data change. When the *Check Mobile Transaction History* checkbox is checked, the SAP system only sends a push to the user if the user has previously downloaded the same SAP object and the object is still valid. This setting is commonly used for pushing time sensitive data such as workflow tasks to users.
  Enter the `<History Interval>`, in seconds, to determine whether the object received by the user through a previous push is still valid. No push is sent to a user who has expired push data. The *History Interval* setting is linked to the *Check Mobile Transaction History* setting.
- **Notification Setting section:** When the *Email Notification* checkbox is checked, an email notification is generated to push recipients during push processing. The email address used is based on information defined in SAP user data or mobile user leading data defined in the Administration & Monitoring Portal. If email notification is enabled, type a subject in the `<Email Subject>` field. If email notification is enabled, type your e-mail in the `<Email Message>` field.
  When the *No Data Package* checkbox is checked, no data payload is generated by push processing. Check this box to generate only push notifications. OData-based mobile applications such as SAP Service and Asset Manager only support push notifications without data payloads. Traditional, Agentry-based, mobile applications can support a data payload during push processing.
- **Activation section:** If the *Active Flag* checkbox is checked, the push is active. If the *Enable Push History* checkbox is checked, information about push recipients and data object keys are recorded in the push history table. If the *Require Metadata* checkbox is checked, technical data for the push data payload is generated. If the *Enable Fetch Callback* checkbox is checked, the mobile client retrieves data about the pushed SAP object using a regular sync request instead of precalculating the push data payload during push processing. Enabling push callback can ensure the client always receives up-to-date SAP data when receiving a push.

Event Setting Tab

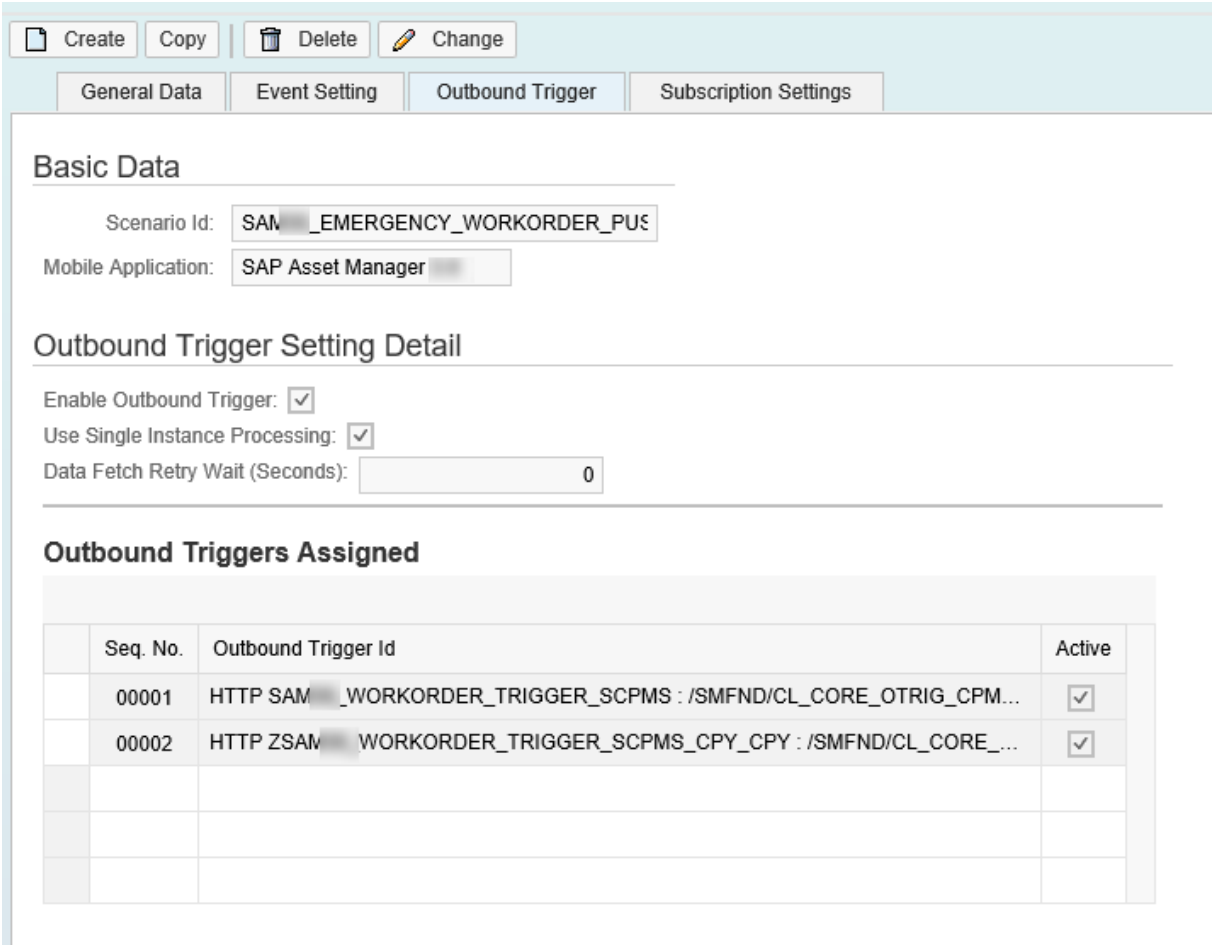


You can define the following attributes in the *Event Setting* tab:

- **Background Event Setting Detail setting:** If the *Disable Background Event Trigger* checkbox is *not* checked, a background event is raised during push processing.
- **Standard Event Setting:** The `<Event ID>` is the background event ID that is raised. The `<Event Parameter>` is the background event parameter.
- **Rule Based Event Setting:** The `<Push Event Rule>` is a routine that generates a dynamically formatted event ID and parameter based on supported runtime variables.
- **qRFC Setting Detail:** If the *Enable qRFC Processing* checkbox is checked, push processing is handled in the background as a qRFC call.

- **Queue Setting:** Enter the qRFC queue name used for push processing in the `<Queue Name>` field. The `<qRFC Rule>` is the routine that can generate a dynamically formatted qRFC queue name based on supported runtime variables.
- **Runtime Parameters:** If the *Allow Instance Merge* checkbox is checked, the creation of a new push instance cancels existing push instances for the same SAP object key that are not completed. If the *Exclude Status SRV_COMP:* checkbox is checked, push instances with a status of SRV_COMP are not reprocessed. If it is not checked, push instances with a status of SRV_COMP are reprocessed.
  Type in the time delay before processing a push sequence in the `<Maximum Select Delay>` field. The maximum select delay is used in qRFC push processing. Use this setting if there could be a time delay in the push instance registry table database update. The delay could allow the push registry data to fully update before the push processing starts.
  Type in the number of times the push processor should try to read push instance information from the push registry if the read failed into the `<Select Retry>` field.

Outbound Trigger Tab

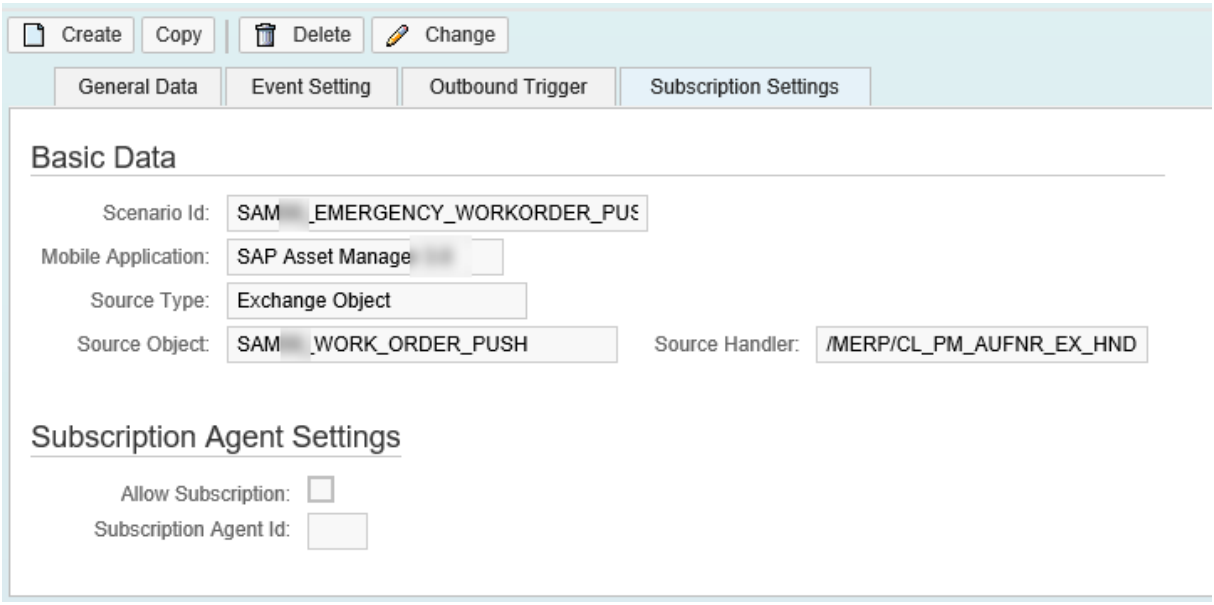


Outbound triggers handle interfacing with external systems. You can assign multiple outbound triggers to a push scenario. Assigned outbound triggers are invoked at the end of push processing, based on the assigned sequence.

Check the *Enable Outbound Trigger* checkbox to activate the selected outbound trigger.

Subscription Settings Tab

To allow an on-demand subscription based push request from the mobile client, define the subscription setting in the *Subscription Settings* tab. Subscriptions allow the mobile client to trigger a push process instead of a traditional trigger by the back end SAP system update. OData based mobile applications do not support subscription-based on-demand push configuration.



- **Allow Subscription:** Check to enable subscription-based push processing for the push scenario
- **Subscription Agent ID:** Displays the subscription agent assigned to handle the subscription request

6.3.2.10.2 Outbound Trigger Configuration

Outbound triggers allow a mobile application to interface with external systems such as the SAP Business Technology Platform.

You can integrate outbound triggers into one of the following mobile application processes:

- Push processing
- OData mobile data object processing

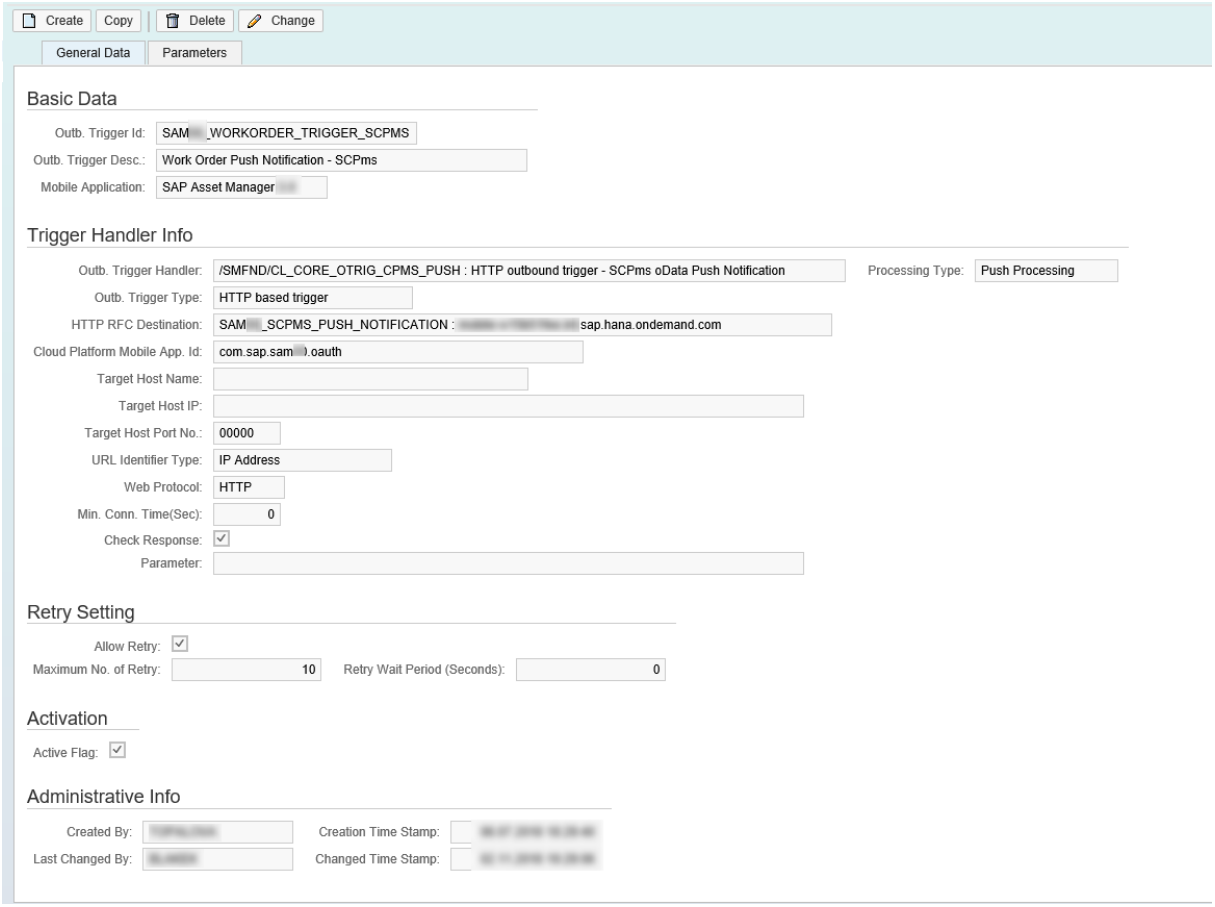
An outbound trigger can support only one of the two available processes. The process is determined by the outbound trigger handler. An outbound trigger handler can support any of the interface technologies, such as HTTP triggers, file triggers, and web service triggers.

The *Outbound Trigger* page contains the following tabs:

- General Data

- Parameters

General Data Tab



You can define the following attributes in the *General Data* tab:

Basic Data

- **Outbound Trigger ID:** Required field. Unique ID of the outbound trigger in the Y or Z namespace, limited to 40 characters.
- **Outbound Trigger Description:** Short description of the outbound trigger
- **Mobile Application:** Select your mobile application. The outbound trigger configuration detail is defined for the individual mobile application.

Trigger Handler Info

- **Outbound Trigger Handler:** ABAP OO class that provides the technical implementation for the outbound trigger. The outbound trigger handler must be a subclass of `/SYCLO/CL_CORE_XXX` You can reuse an outbound trigger handler to provide technical implementation for multiple outbound triggers.
- **Processing Type:**
- **Outbound Trigger Type:** Selection depends on the implementation of the outbound trigger handler

- **HTTP RFC Destination:** Only used when *HTTP-based trigger* is selected as the outbound trigger type. The HTTP RFC destination establishes a connection for the outbound trigger
- **Cloud Platform Mobile App ID:** used to interface with SAP Business Technology Platform Mobile Services. The ID identifies the mobile application ID that was set up in SAP BTP services.
- **Target Host Name:** Host name the outbound trigger is connecting to
- **Target Host IP:** IP address of the host to which the outbound trigger is connecting to
- **Target Host Port Number:** Port number of the host to which the outbound trigger is connecting to
- **URL Identifier Type:** Defines the information to use by the outbound trigger to make the connection
- **Web Protocol:** HTTP or HTTPS
- **Minimum Connection Time (Seconds):** Wait time before checking the response to an outbound trigger request from the remote system
- **Check Response:** If checked, a check response to an outbound trigger HTTP request is active
- **Parameter:** General purpose parameter that provides input information to the outbound trigger handler
- The following fields are only visible after other fields are selected:
  - Logical File Name: Used by outbound trigger type *File Based Trigger*
  - RFC Destination: Used by outbound trigger type *Remote Function Call*
  - RFC User ID: Used by outbound trigger type *RFC User ID*. User ID to make the RFC call.

Retry Setting

- **Allow Retry:** If checked, the outbound trigger is allowed to rerun
- **Maximum Number of Retry:** Set the maximum number of times the outbound trigger can rerun
- **Retry Wait Period (Seconds):** Set the minimum wait time between output trigger retries

Activation

If the *Active Flag* checkbox is not checked, the outbound trigger is not enabled.

Parameters Tab

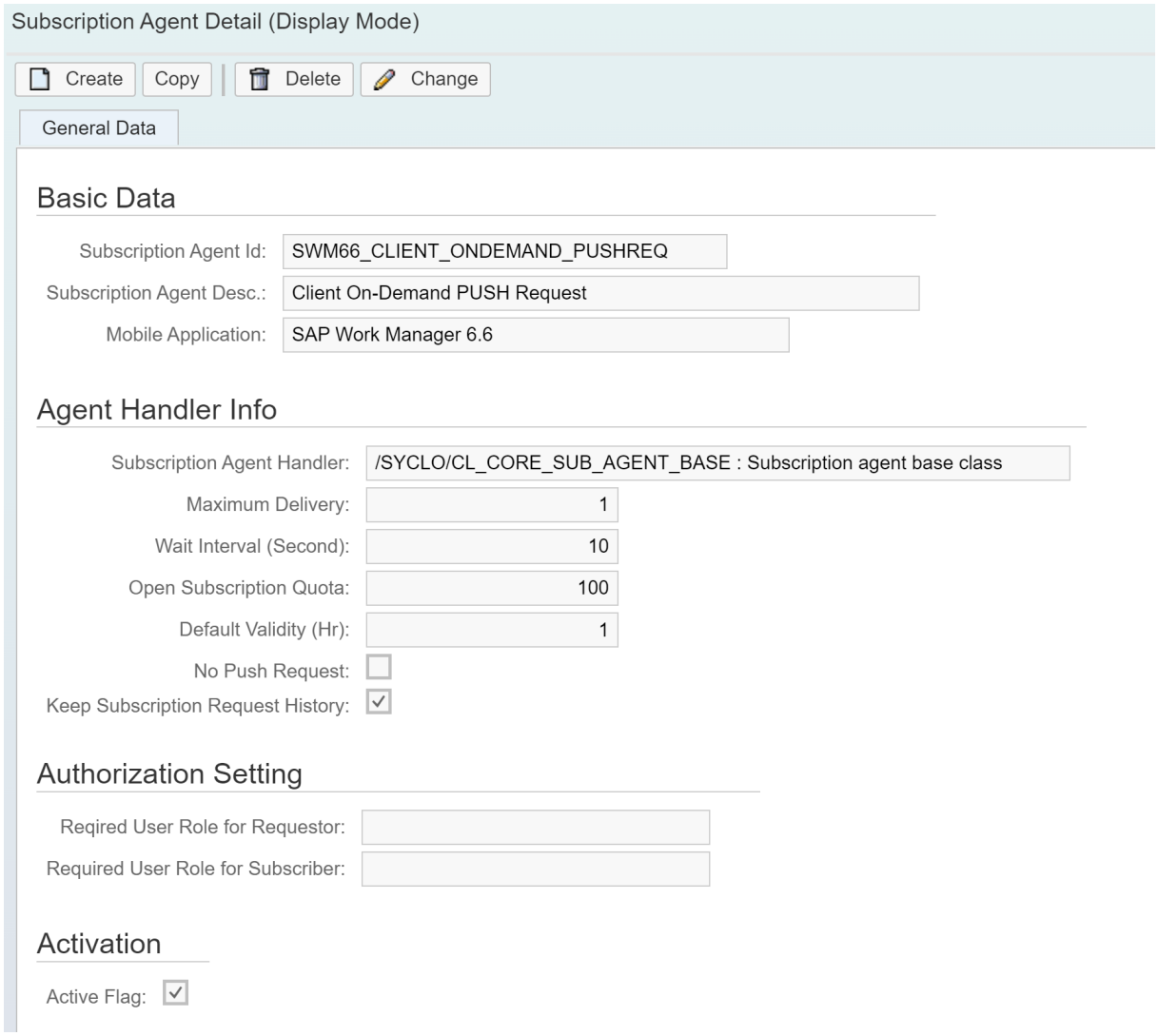
An outbound trigger handler can declare special purpose parameters. If parameters are declared, they are displayed in the *Parameters* tab. You can declare any number of parameters. A parameter can be a single field parameter or a structured record.



6.3.2.10.3 Subscription Agent Definition

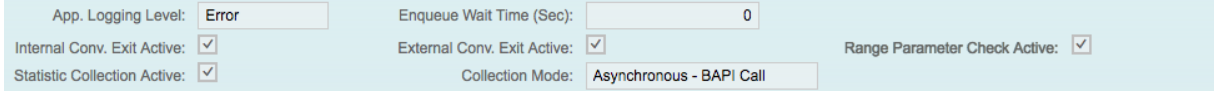
Subscription Agent Definitions allow you to define how subscription requests for back-end system data are handled.

On Demand subscriptions allow you to define push options. For instance, some accounts, or activities have attachments, which are not automatically pushed down. If subscribed, however, a sales manager can get those attachments on demand, based on the settings configured in the subscription agent.



6.3.2.11 Technical Settings

Technical settings affect all components of the framework.

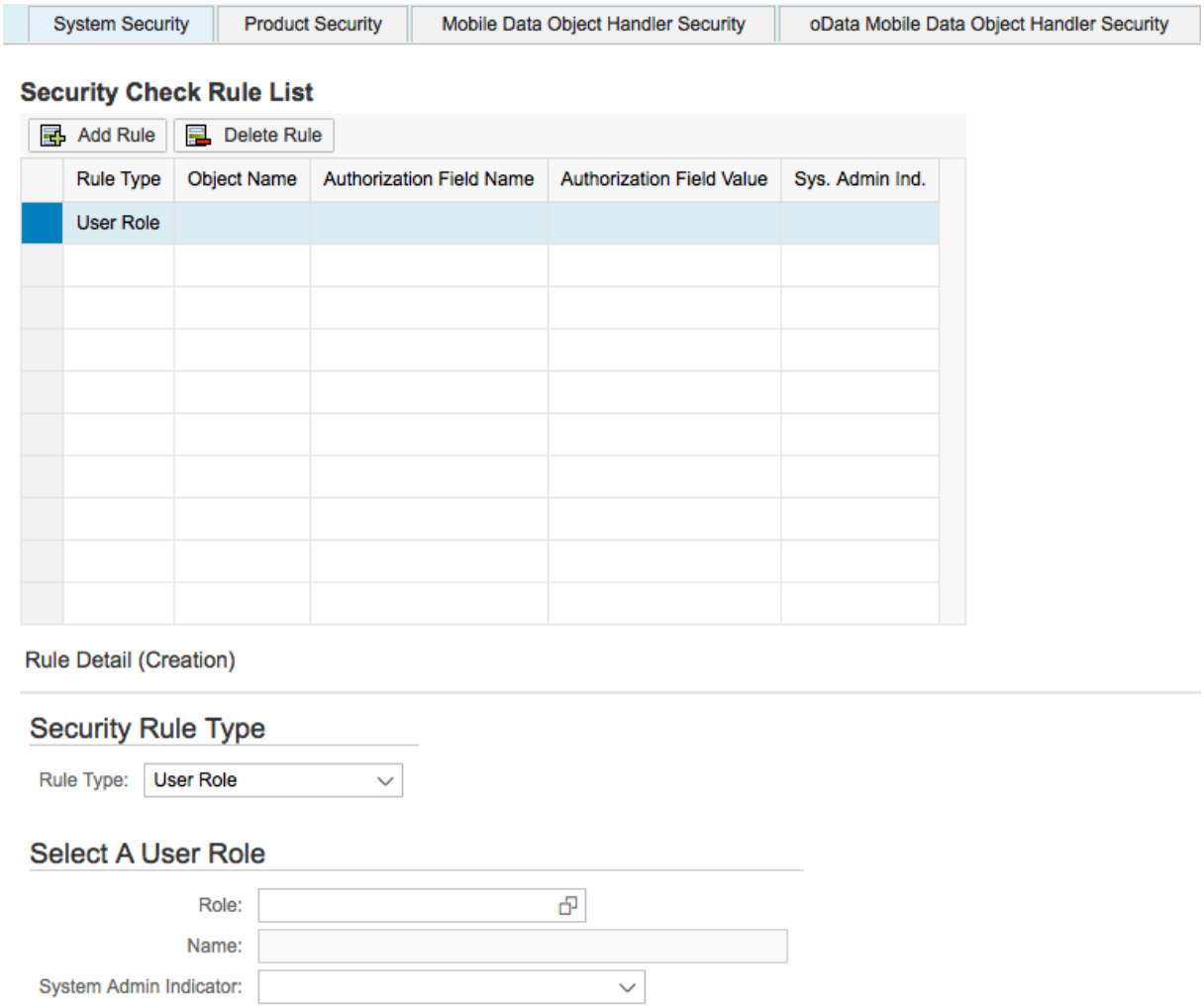


The following fields make up the Technical Settings page:

- **Application Logging Level:** Defines the logging level for all framework components. Logging entries are recorded in the SAP application log database under the object `/syclo/`. The logging levels are:
  - No logging
  - Abort
  - Error
  - Warning
  - Info
  - Debug
  - Trace
- **Enqueue Wait Time (Sec):** The Enqueue Wait Time parameter controls the number of seconds the underlying component should continue to try to access a locked SAP object in intervals of 1 second during an update by a mobile device. The update process aborts if accessing the locked object is still unsuccessful after the wait time.
- **Internal Conversion Exit Active:** When checked, the framework runtime data manager performs a standard SAP external-to-internal format conversion exit for all inbound BAPI parameters. The option is enabled by default. An application developer should only change this setting as it has a direct impact to the SAP Service and Asset Manager application.
- **External Conversion Exit Active:** When enabled, the framework runtime data manager performs standard SAP internal-to-external format conversion exit for all outbound BAPI parameters. This option is enabled by default. An application developer should only change this setting as it has a direct impact to the SAP Service and Asset Manager application.
- **Range Parameter Check Active:** When enabled, the framework runtime data manager performs checks on all SAP range parameters of inbound BAPI parameters. The SAP range parameter has the structure of SIGN, OPTION, LOW and HIGH. If SIGN and OPTION are not specified, a check routine sets SIGN to I and OTPION to EQ. This option is enabled by default. An application developer should only change this setting as it has a direct impact to the SAP Service and Asset Manager application.
- **Collection Mode:** Collection mode determines how system statistic records are written to the database. Two modes are supported currently: Synchronously and Asynchronously. When you select Synchronously, the statistics record is written to the database in real-time during BAPI calls. However, selecting this option incurs a performance penalty. Selecting Asynchronously means that statistics are collected in-memory and written asynchronously to the database at the end of the BAPI call.
- **Statistic Collection Active:** When enabled, the framework records all runtime statistics associated with the BAPI calls between the middleware server and SAP. This collection provides data for the KPI statistics collections found in the Administration portal. An application developer should only change this setting as it has a direct impact to the SAP Service and Asset Manager application.
- **Created By, Creation Time Stamp, Last Changed By, Changed Time Stamp:** The user ID and time stamps are automatically logged when a record is created or changed.

6.3.2.12 Mobile Authorization Settings

You can define security rule settings for the Mobile Integration Framework for SAP and mobile applications as well.



All security checks are carried out by the Mobile Integration Framework at runtime, with checks performed at the following levels:

- *System*
  Application independent. Applies to all components built on the Mobile Integration Framework.
- *Product*
  Security at the mobile application and product level
- *Mobile Data Object Handler*
  Specific to a Mobile Data Object class handler
- *OData Mobile Data Object Handler*
  Specific to an OData Mobile Data Object class handler

The following types of security rules can be defined:

- *User Role*
  Rules based on predefined user roles

- *Authorization Profile*
  Rules based on predefined authorization profiles.
- *Authorization Object*
  Rules based on predefined authorization objects.

Special Security Role with System Indicator

You can define special security rules using user roles. These security rules can be assigned with system indicators. These special security rules with system indicators are used to limit access to the ConfigPanel and Administration & Monitoring tools. The following system indicators are available:

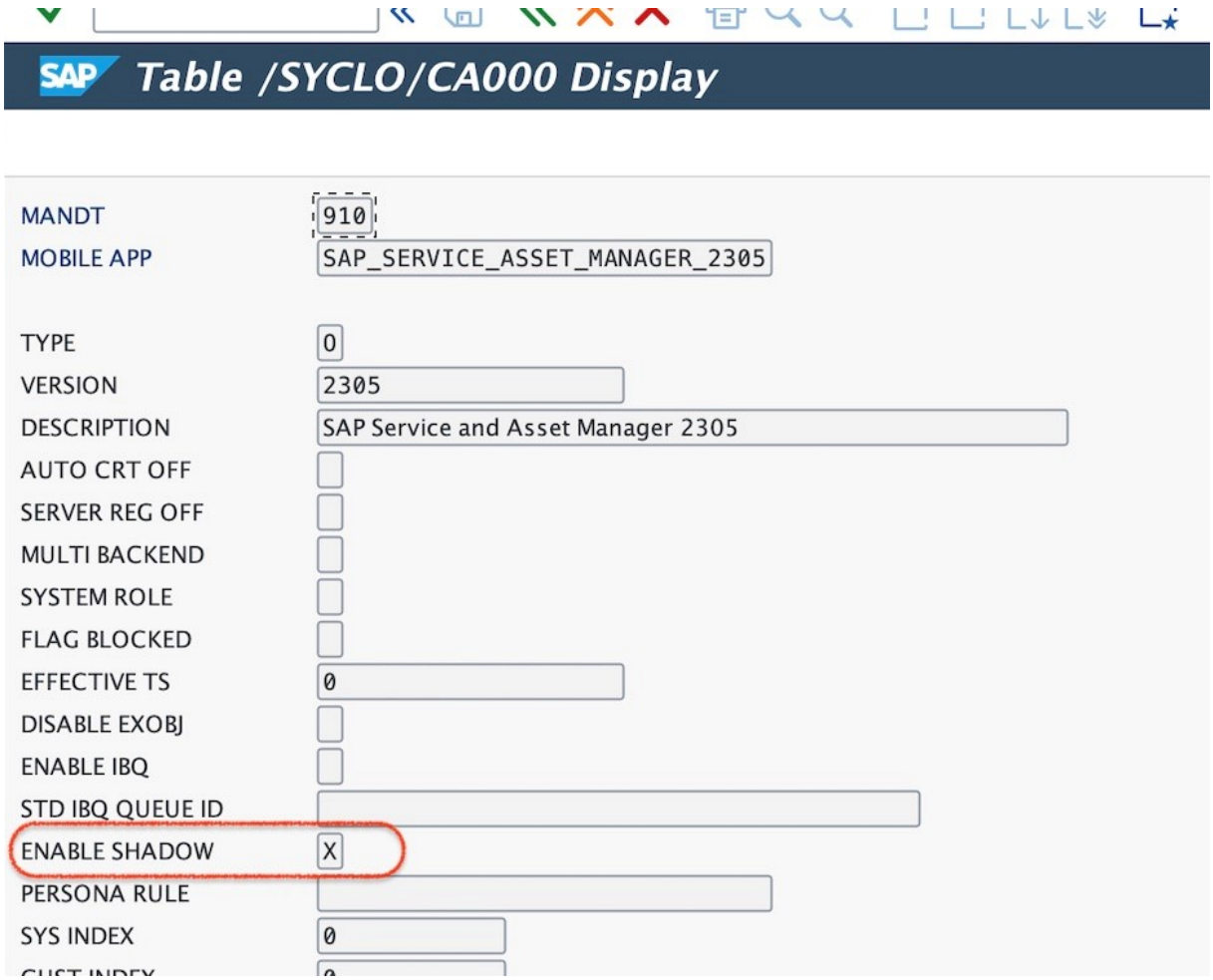
- *System Administrator*
  If security rules are defined, only users with the required user role can have full access to the Administration & Monitoring tool.
- *System Administration – View Only*
  If security rules are defined, only users with the required user role can have read access to the Administration & Monitoring tool.
- *System Configurator*
  If security rules are defined, only users with the required user role can have full access to the ConfigPanel.
- *System Configuration – View Only*
  If security rules are defined, only users with the required user role can have read access to the ConfigPanel.

6.3.3 Shadow Table

Any custom configuration changes are stored in separate sets of tables, unlike standard configuration tables that use the MAIF framework. A custom application created using the configuration panel is marked as supporting shadow tables.

> **Note**
>
> Shadow table support is only available for OData applications.

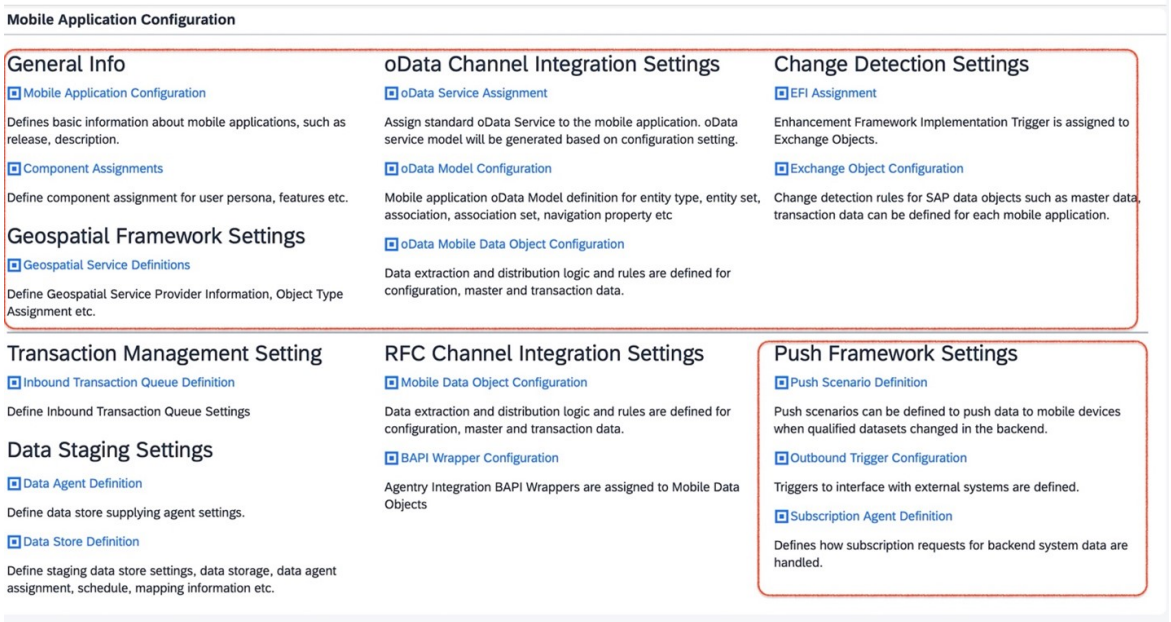
The *Enable Shadow* checkbox in the mobile application tables (/SYCLO/CA000 and /SYCLO/YCA000) is introduced to determine whether or not the application has enabled shadow table support:



If the application is enabled in shadow table mode, all user configuration changes will be saved in the shadow tables.

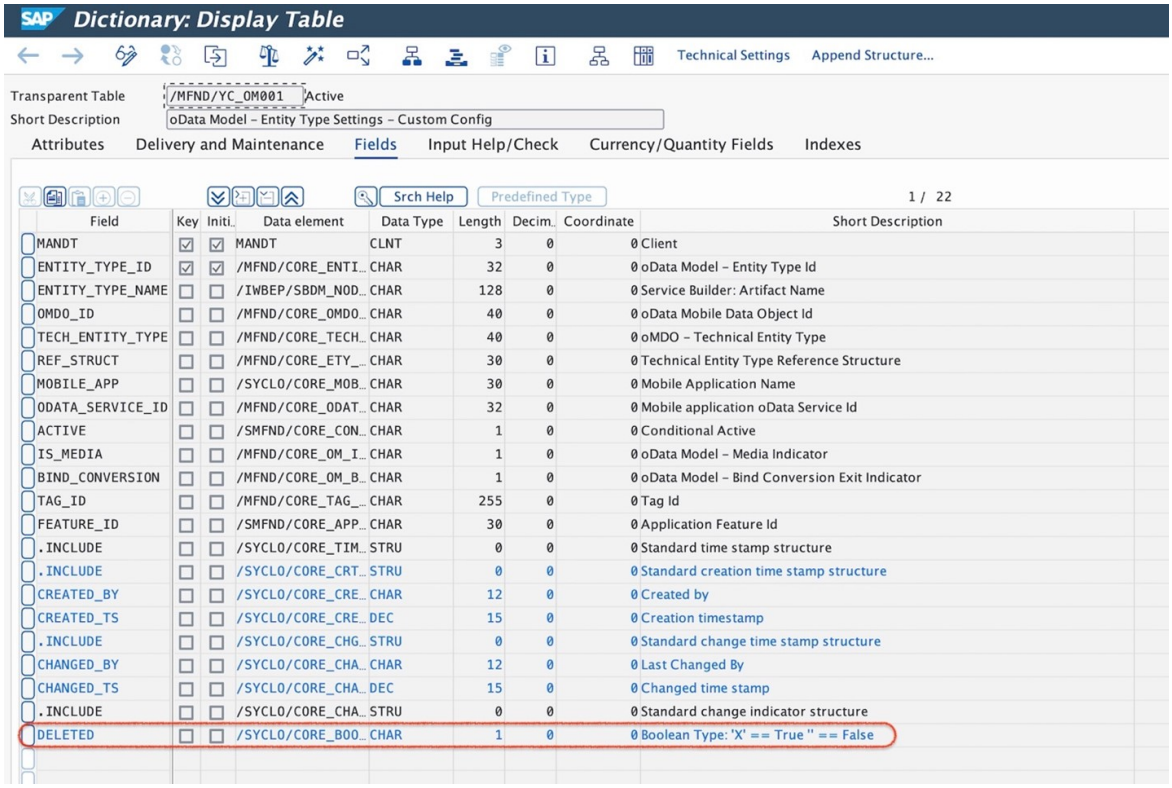
The following configuration fields from the configuration panel can be supported by shadow tables:

- Mobile Application Configuration
- Component Assignments
- Geospatial Service Definitions
- oData Service Assignment
- oData Model Configuration
- oData Mobile Data Object Configuration
- EFI Assignment
- Exchange Object Configuration
- Push Scenario Definition
- Outbound Trigger Configuration
- Subscription Agent Definition



A shadow table has the same name as a standard configuration table, with an extra *Y* in the table name. For example, the standard configuration table for an entity type is /MFND/C_OM001. The corresponding shadow table is /MFND/YC_OM001.

The shadow table has all the fields as in the standard configuration table, with an extra *DELETED* field used to indicate whether or not the standard configuration has been deleted. The configuration panel procedures combine the standard and custom configurations and return a consolidated result for display.



Field	Key	Initi.	Data element	Data Type	Length	Decim.	Coordinate	Short Description
MANDT	☑	☑	MANDT	CLNT	3	0	0	Client
ENTITY_TYPE_ID	☑	☑	/MFND/CORE_ENTI...	CHAR	32	0	0	oData Model – Entity Type Id
ENTITY_TYPE_NAME	☐	☐	/IWBEP/SBDM_NOD...	CHAR	128	0	0	Service Builder: Artifact Name
OMDO_ID	☐	☐	/MFND/CORE_OMDO...	CHAR	40	0	0	oData Mobile Data Object Id
TECH_ENTITY_TYPE	☐	☐	/MFND/CORE_TECH...	CHAR	40	0	0	oMDO – Technical Entity Type
REF_STRUCT	☐	☐	/MFND/CORE_ETY_...	CHAR	30	0	0	Technical Entity Type Reference Structure
MOBILE_APP	☐	☐	/SYCLO/CORE_MOB...	CHAR	30	0	0	Mobile Application Name
ODATA_SERVICE_ID	☐	☐	/MFND/CORE_ODAT...	CHAR	32	0	0	Mobile application oData Service Id
ACTIVE	☐	☐	/SMFND/CORE_CON...	CHAR	1	0	0	Conditional Active
IS_MEDIA	☐	☐	/MFND/CORE_OM_I...	CHAR	1	0	0	oData Model – Media Indicator
BIND_CONVERSION	☐	☐	/MFND/CORE_OM_B...	CHAR	1	0	0	oData Model – Bind Conversion Exit Indicator
TAG_ID	☐	☐	/MFND/CORE_TAG_...	CHAR	255	0	0	Tag Id
FEATURE_ID	☐	☐	/SMFND/CORE_APP...	CHAR	30	0	0	Application Feature Id
.INCLUDE	☐	☐	/SYCLO/CORE_TIM...	STRU	0	0	0	Standard time stamp structure
.INCLUDE	☐	☐	/SYCLO/CORE_CRT...	STRU	0	0	0	Standard creation time stamp structure
CREATED_BY	☐	☐	/SYCLO/CORE_CRE...	CHAR	12	0	0	Created by
CREATED_TS	☐	☐	/SYCLO/CORE_CRE...	DEC	15	0	0	Creation timestamp
.INCLUDE	☐	☐	/SYCLO/CORE_CHG...	STRU	0	0	0	Standard change time stamp structure
CHANGED_BY	☐	☐	/SYCLO/CORE_CHA...	CHAR	12	0	0	Last Changed By
CHANGED_TS	☐	☐	/SYCLO/CORE_CHA...	DEC	15	0	0	Changed time stamp
.INCLUDE	☐	☐	/SYCLO/CORE_CHA...	STRU	0	0	0	Standard change indicator structure
DELETED	☐	☐	/SYCLO/CORE_BOO...	CHAR	1	0	0	Boolean Type: 'X' == True '' == False

With shadow table support, customers can upgrade their mobile application versions without affecting previously created custom configurations. The migration tool has been enhanced to support migration of shadow table data.

6.3.4 Configuring Confirmation Posting Dates - Overview

Configure confirmation posting dates through the PM_CONFIRMATION OMDO. However, you can only enable one filter at a time. The USE_USER_TIME_ZONE filter is used for time zone conversion when the SAP system and mobile users are in different time zones, while the POSTING_DATE filter overrides the confirmation posting date as system date and requires the PostingDateFromUserOverride parameter to be enabled.

You can use either the *USE_USER_TIME_ZONE* or the *POSTING_DATE* filter, found in the **<MOBILE APP>_PM_CONFIRMATION** OMDO, to configure confirmation posting dates. Note that you can enable only one filter at a time. If both filters are enabled, you'll get an error.

USE_USER_TIME_ZONE Filter

See the Configuring Confirmation Posting Date Using the USE_USER_TIME_ZONE Filter [page 685] procedure for detailed instructions.

When the SAP system and mobile users are in different time zones, use the *USE_USER_TIME_ZONE* filter to perform the time zone conversion. When the filter is active, the application uses the time zone of the mobile user in the back end system to convert the actual start date / time. It also converts the finish date / time received from the mobile client. The system time zone is the default setting. The User Time Zone filter is a back end only configuration.

> **Note**
>
> To use the time zone handling functionality in confirmation, the SAP system must be customised with a time zone. If the SAP system time zone isn't maintained and the *USE_USER_TIME_ZONE* filter is active in the **<MOBILE_APP>_PM_CONFIRMATION** OMDO, posting of confirmation from the mobile application raises an error.

POSTING_DATE Filter

See the Configuring Confirmation Posting Date Using the POSTING_DATE Filter [page 686] procedure for detailed instructions.

The *POSTING_DATE* filter overrides the confirmation posting date as system date. The default option uses the posting date from the mobile device. If you use the *POSTING_DATE* filter, you must also enable the *PostingDateFromUserOverride* parameter. The Posting Date filter is a combination of front end and back end configuration.

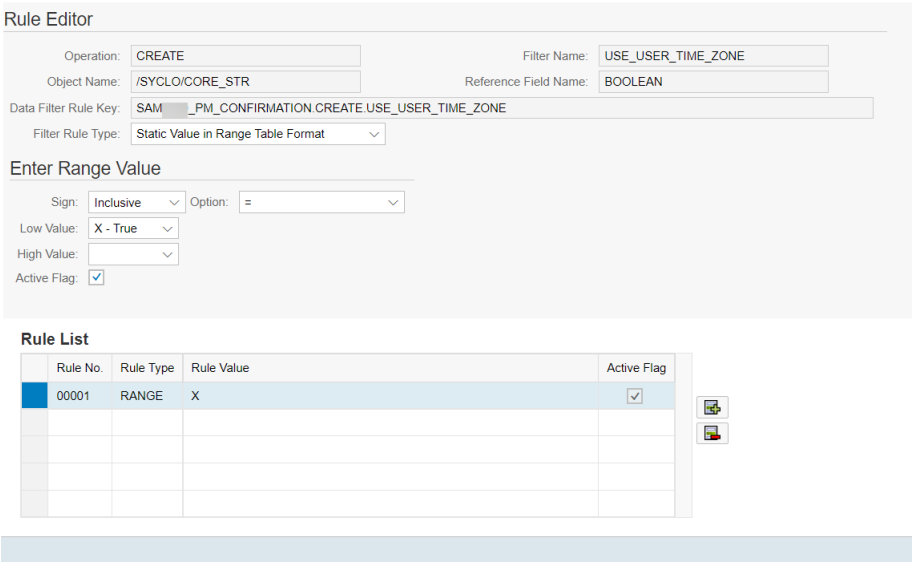
6.3.4.1 Configuring Confirmation Posting Date Using the USE_USER_TIME_ZONE Filter

Context

Use the following procedure if you're configuring the confirmation posting date using the *USE_USER_TIME_ZONE* filter.

Procedure

1. On the ConfigPanel Home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. Click on *oData Channel Integration Settings* > *oData Mobile Data Object Configuration*.
3. In the *OData Mobile Data Object List* select **<MOBILE_APPLICATION>_PM_CONFIRMATION**, and then the *Data Filter* tab.
4. Expand the *Defined Filters* list as follows: *Operation - CREATE* > *Standard Filter* > *USE_USER_TIME_ZONE*. Click the *Change* button.
5. Select the existing rule. Ensure the `<Low Value>` field is set to *X - True* and is enabled:



6. *Save* your changes.

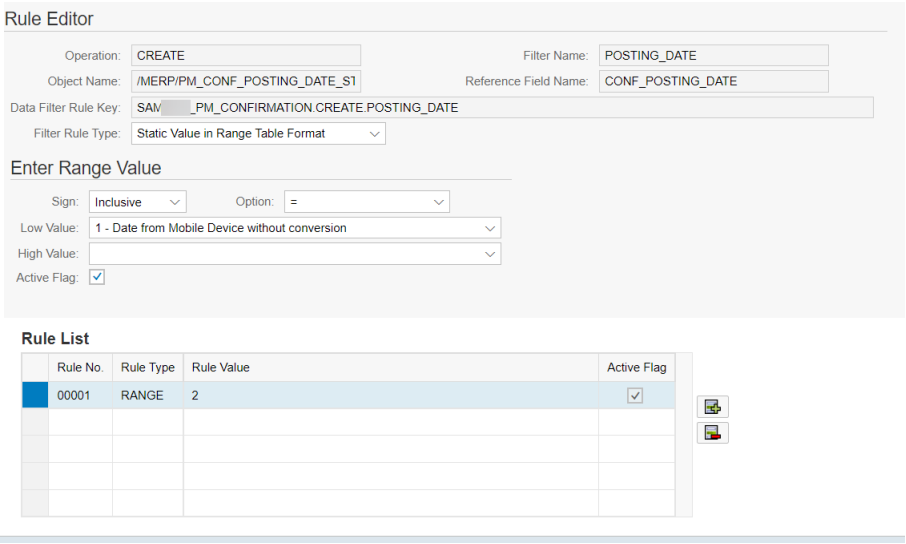
6.3.4.2 Configuring Confirmation Posting Date Using the POSTING_DATE Filter

Context

Use the following procedure if you're configuring the confirmation posting date using the *POSTING_DATE* filter.

Procedure

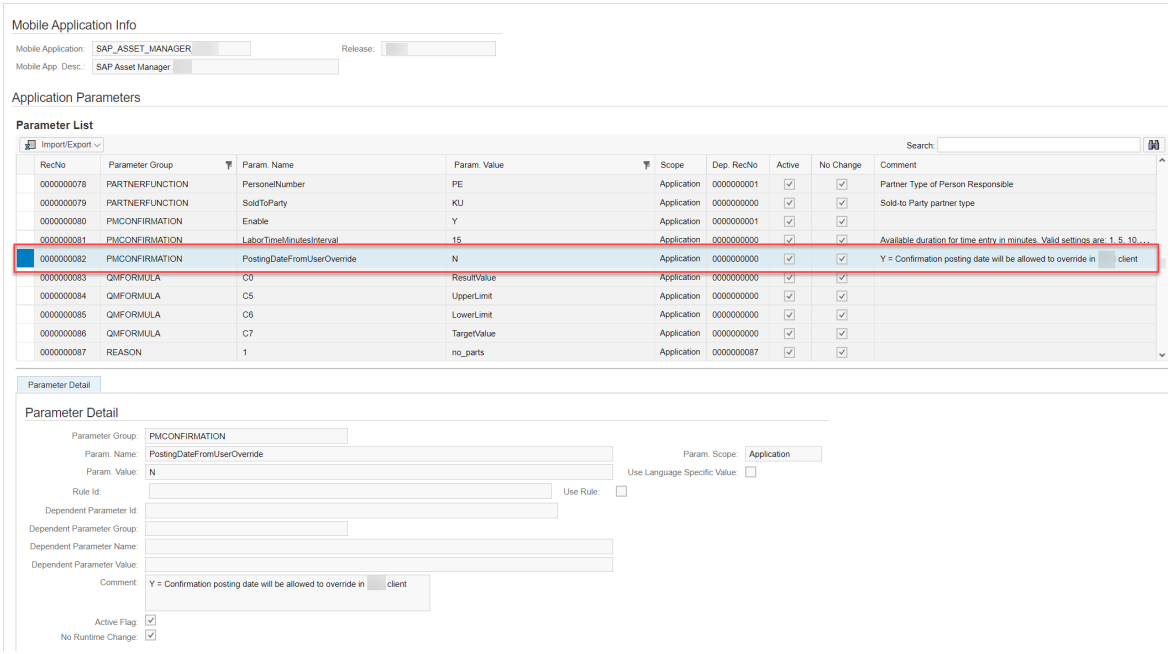
1. On the ConfigPanel Home page, select *OData Mobile Data Object Configuration*. Make sure to select your desired mobile application in the *Mobile Application Filter* field at the top of the page.
2. Click on *oData Channel Integration Settings* > *oData Mobile Data Object Configuration*.
3. In the *OData Mobile Data Object List* select **<MOBILE_APPLICATION>_PM_CONFIRMATION**, and then the *Data Filter* tab.
4. Expand the *Defined Filters* list as follows: *Operation - CREATE* > *Standard Filter* > *POSTING_DATE*. Click the *Change* button.
5. Select the existing rule. Ensure the `<Low Value>` field is set to *1* and is enabled:
   - **Default:** 1 - Date from Mobile Device without conversion
   - 2 - User Time Zone Date (at the time of BAPI execution)
   - 3 - System Time Zone Date (at the time of BAPI execution)



6. *Save* your changes.
7. Return to the *Home* page. Navigate to *Mobile Application Configuration* > *Parameters tab*. In the left column, *Defined Mobile Applications*, select your application.

   The *Parameter List* populates with a list of all parameters available for the application.

8. Click the *Change* button.
9. Find and highlight the *PostingDateFromUserOverride* parameter, located in the *PMCONFIRMATION* parameter group. Set the parameter to one of the following:
    - **N:** (Default). If set to N, the confirmation posting date is automatically taken from the time zone set on the mobile client.
    - **Y:** If set to Y, the mobile client user can manually enter a date on the Confirmation screen in the app.



10. Check the `<Active>` flag to ensure that the parameter is used by the mobile application. If desired, and if not already checked, check the `<No Runtime Change>` box to ensure that the value of the parameter isn't overridden at runtime through synchronization processing.
11. *Save* your changes.

6.3.5 Copying an Object to the Customer Namespace

When you modify either an oData mobile data object or an exchange object, first make a copy of the object and place it in the customer namespace.

Context

The following procedure provides information on making a copy of an oData mobile data object (OMDO) or exchange object within MAIF / SAP Mobile Add-On. In any of the procedures provided in this guide where an OMDO or an exchange object is copied, refer to this procedure for instructions. When you copy either an OMDO or an exchange object, you can roll back any changes you make to the application if necessary without changing the original objects.

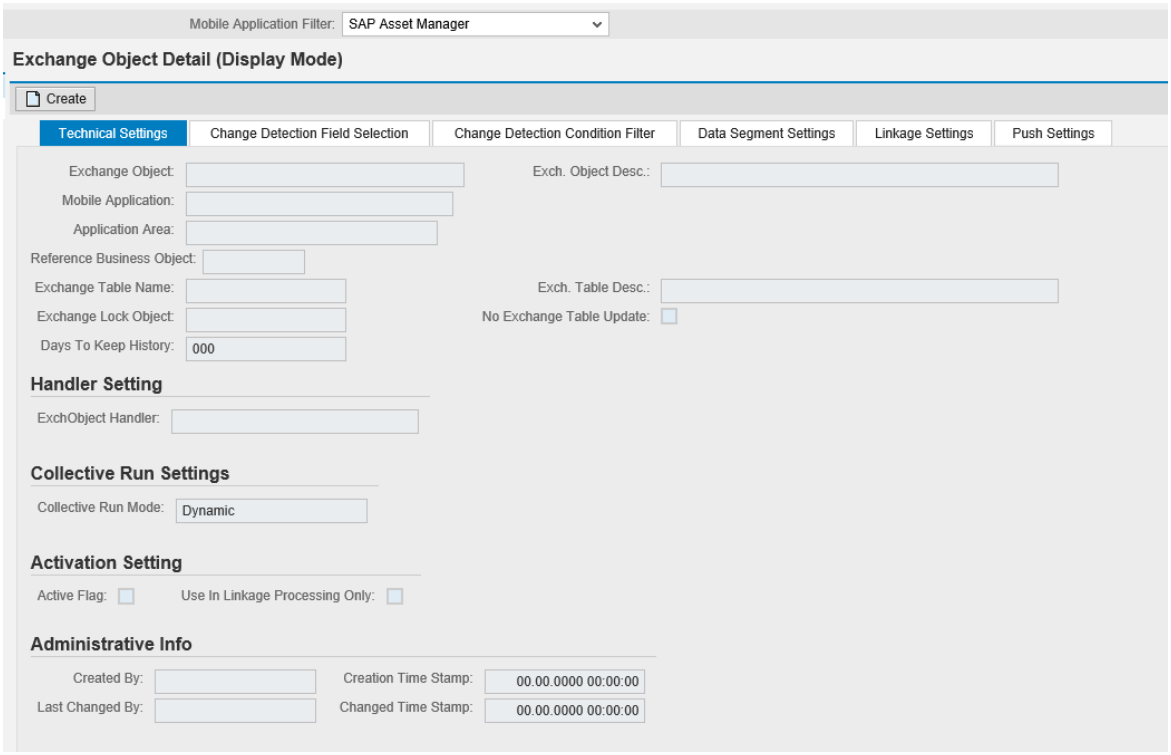
Once you copy an OMDO and modify the object, you may adjust the oData model definition to reference the new OMDO. Similarly, when you copy and modify an exchange object, you may need to change the EFI trigger assignment to the new exchange object. These procedures are covered separately.

Procedure

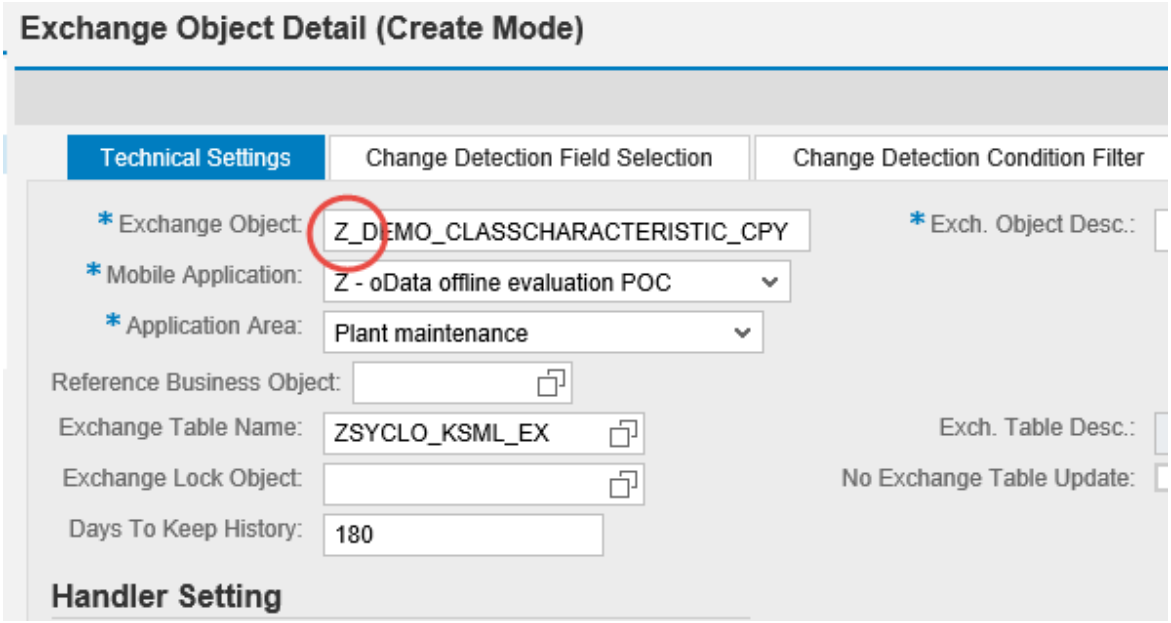
1. Log into the ConfigPanel.
2. Click either *Exchange Object Configuration* or *oData Mobile Data Object Configuration* from the home page.

   The Object Detail panel opens.

> ### Note
>
> Figures shown in this procedure are taken from the Exchange Object configuration page. Screens may look different when configuring an oData mobile data object. For either, the ability to copy is provided.



3. Select the object to copy from the list of OMDOs or exchange objects and click *Copy*.
4. In the main object `<ID>` field, add a `<Z>` to the beginning of the object name.



5. Click *Save* to save the object copy.

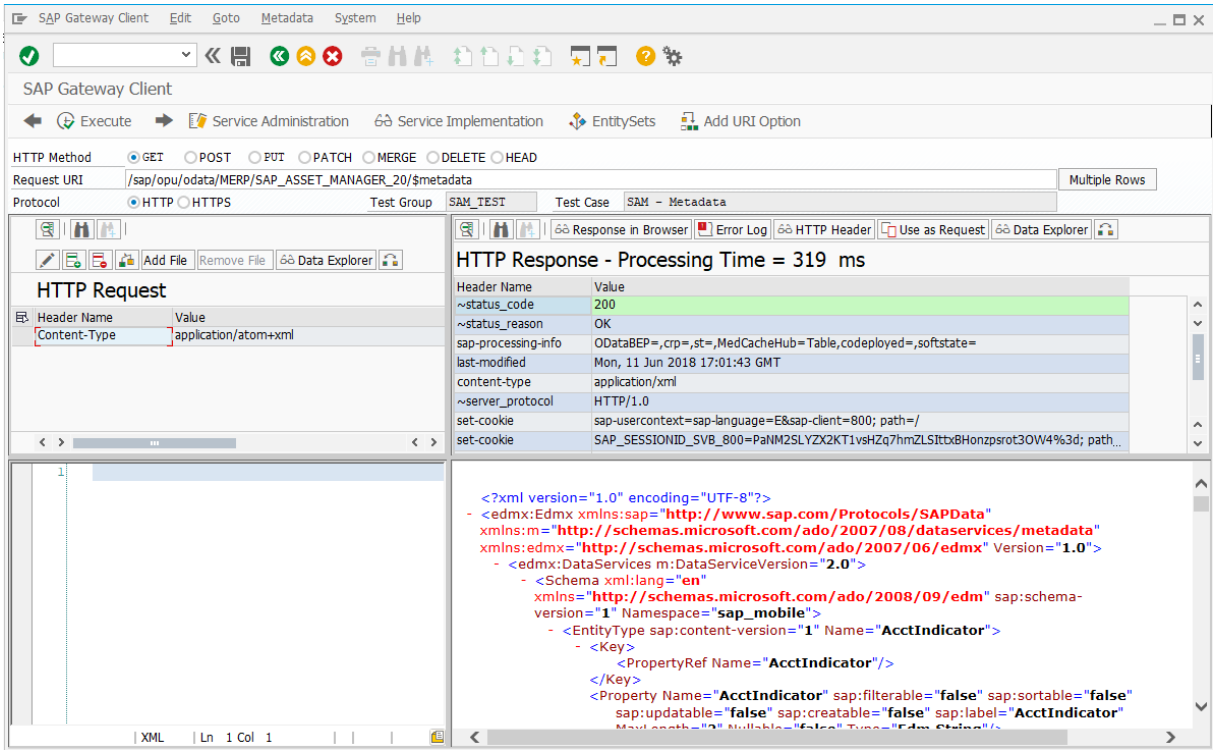
   A copy of the original object is created in the customer namespace. Now you can modify the object, with the original object as a back-up for rollback purposes, if necessary.

7 Troubleshooting

This section describes the various troubleshooting activities that you can perform in error situations, or the app users can perform on a regular basis to ensure the smooth running of the mobile application. It is also explains how to monitor the different components of SAP Gateway, how to use the logs, and how to carry out maintenance activities.

7.1 SAP Gateway Client

You can use the SAP Gateway Client (transaction code: */IWFND/GW_CLIENT*) to test your OData service provider without an OData consumer, such as the SAP Service and Asset Manager mobile client. This tool is especially useful to test your OData service from the back end to identify service-related issues before a service is used by the mobile application.



For more information about how to work with the SAP Gateway Client, see SAP Gateway Client in the SAP Gateway Technical Operations Guide.

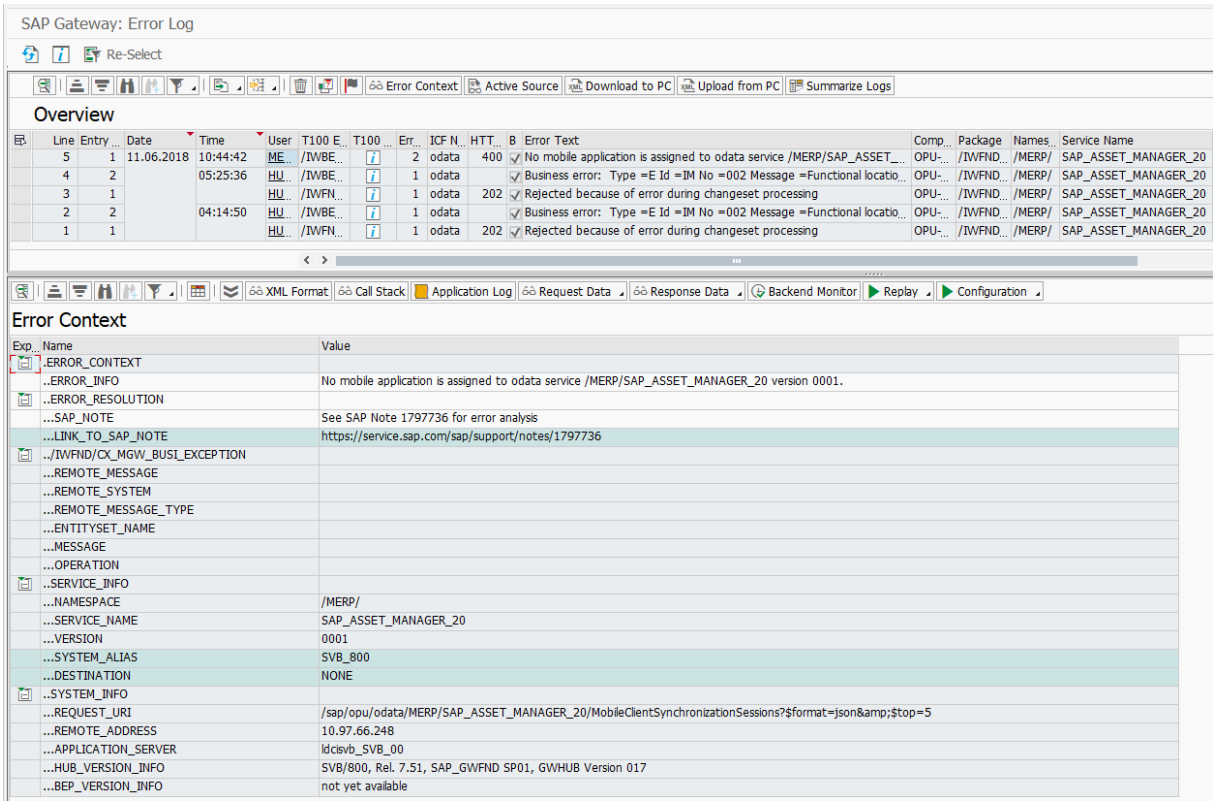
7.2 SAP Gateway Error Logs

Error logs provide detailed context information about errors that have occurred at runtime, enabling you to perform root cause analysis, as well as reproducing and correcting errors.

You can launch the error log with transaction */IWFND/ERROR_LOG* in Gateway Hub systems. Launch the error log with transaction */IWBEP/ERROR_LOG* in your back-end system.

The SAP Gateway error logs reveal basic details about errors and show errors from all users for a given client. Business logic errors are often displayed in this error log due to improper business logic. Other errors displayed include the HTTP code to indicate the type of error.

Note that based on the security level setting, advanced details or the replay function may be hidden or disabled. Note also that these error logs will not show generic authorization errors if users fail to properly authenticate.



You can navigate to different sections from the *Error Context* area as shown above. Choose *Replay* to reproduce and correct errors. Choose from the following two replay options:

- SAP Gateway Client
- Web Browser

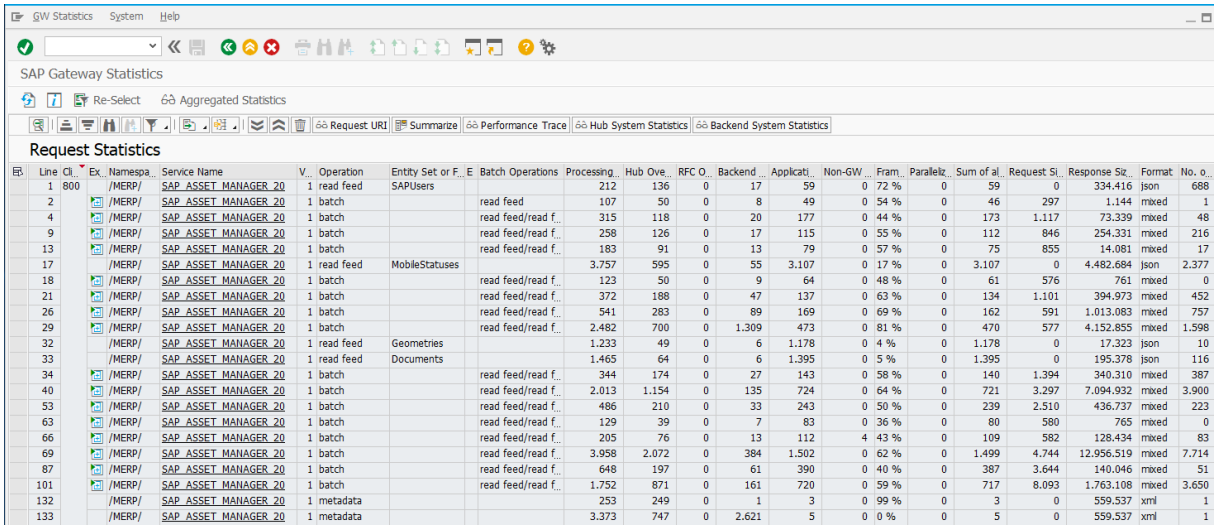
Use option *SAP Gateway Client* to reproduce runtime situations that led to a particular error without accessing the application from the actual mobile client, and to simulate a service at runtime to identify and resolve potential issues.

For more information about how to configure the error log, see Configuration Settings for the Error Log in the *SAP Gateway Technical Operations Guide*.

In addition, use the *Application Log Viewer* to display more technical error details by using transaction */IWFND/APPS_LOG*.

7.3 SAP Gateway Statistics

You can use the SAP Gateway Statistics (transaction code: */IWFND/STATS*) to display the request statistics and aggregated statistics. Each successful OData request has an entry in the statistics records, which is kept for 7 days by default, however, you can extend the period to 30 days. Request statistics can be aggregated, in which case they are kept for 90 days by default, however, you can extend the period to 365 days.



Line	Cli..	Ex..	Namespa..	Service Name	V..	Operation	Entity Set or F..	E	Batch Operations	Processing..	Hub Ove..	RFC O..	Backend ..	Applicati..	Non-GW ..	Fram..	Parallelz..	Sum of al..	Request Si..	Response Siz..	Format	No. o..
1	800		/MERP/	SAP_ASSET_MANAGER_20	1	read feed	SAPUsers			212	136	0	17	59	0	72 %	0	59	0	334.416	json	688
2			/MERP/	SAP_ASSET_MANAGER_20	1	batch			read feed	107	50	0	8	49	0	54 %	0	46	297	1.144	mixed	1
4			/MERP/	SAP_ASSET_MANAGER_20	1	batch			read feed/read f..	315	118	0	20	177	0	44 %	0	173	1.117	73.339	mixed	48
9			/MERP/	SAP_ASSET_MANAGER_20	1	batch			read feed/read f..	258	126	0	17	115	0	55 %	0	112	846	254.331	mixed	216
13			/MERP/	SAP_ASSET_MANAGER_20	1	batch			read feed/read f..	183	91	0	13	79	0	57 %	0	75	855	14.081	mixed	17
17			/MERP/	SAP_ASSET_MANAGER_20	1	read feed	MobileStatuses			3.757	595	0	55	3.107	0	17 %	0	3.107	0	4.482.684	json	2.377
18			/MERP/	SAP_ASSET_MANAGER_20	1	batch			read feed/read f..	123	50	0	9	64	0	48 %	0	61	576	761	mixed	0
21			/MERP/	SAP_ASSET_MANAGER_20	1	batch			read feed/read f..	372	188	0	47	137	0	63 %	0	134	1.101	394.973	mixed	452
26			/MERP/	SAP_ASSET_MANAGER_20	1	batch			read feed/read f..	541	283	0	89	169	0	69 %	0	162	591	1.013.083	mixed	757
29			/MERP/	SAP_ASSET_MANAGER_20	1	batch			read feed/read f..	2.482	700	0	1.309	473	0	81 %	0	470	577	4.152.855	mixed	1.598
32			/MERP/	SAP_ASSET_MANAGER_20	1	read feed	Geometries			1.233	49	0	6	1.178	0	4 %	0	1.178	0	17.323	json	10
33			/MERP/	SAP_ASSET_MANAGER_20	1	read feed	Documents			1.465	64	0	6	1.395	0	5 %	0	1.395	0	195.378	json	116
34			/MERP/	SAP_ASSET_MANAGER_20	1	batch			read feed/read f..	344	174	0	27	143	0	58 %	0	140	1.394	340.310	mixed	387
40			/MERP/	SAP_ASSET_MANAGER_20	1	batch			read feed/read f..	2.013	1.154	0	135	724	0	64 %	0	721	3.297	7.094.932	mixed	3.900
53			/MERP/	SAP_ASSET_MANAGER_20	1	batch			read feed/read f..	486	210	0	33	243	0	50 %	0	239	2.510	436.737	mixed	223
63			/MERP/	SAP_ASSET_MANAGER_20	1	batch			read feed/read f..	129	39	0	7	83	0	36 %	0	80	580	765	mixed	0
66			/MERP/	SAP_ASSET_MANAGER_20	1	batch			read feed/read f..	205	76	0	13	112	4	43 %	0	109	582	128.434	mixed	83
69			/MERP/	SAP_ASSET_MANAGER_20	1	batch			read feed/read f..	3.958	2.072	0	384	1.502	0	62 %	0	1.499	4.744	12.956.519	mixed	7.714
87			/MERP/	SAP_ASSET_MANAGER_20	1	batch			read feed/read f..	648	197	0	61	390	0	40 %	0	387	3.644	140.046	mixed	51
101			/MERP/	SAP_ASSET_MANAGER_20	1	batch			read feed/read f..	1.752	871	0	161	720	0	59 %	0	717	8.093	1.763.108	mixed	3.650
132			/MERP/	SAP_ASSET_MANAGER_20	1	metadata				253	249	0	1	3	0	99 %	0	3	0	559.537	xml	1
133			/MERP/	SAP_ASSET_MANAGER_20	1	metadata				3.373	747	0	2.621	5	0	0 %	0	5	0	559.537	xml	1

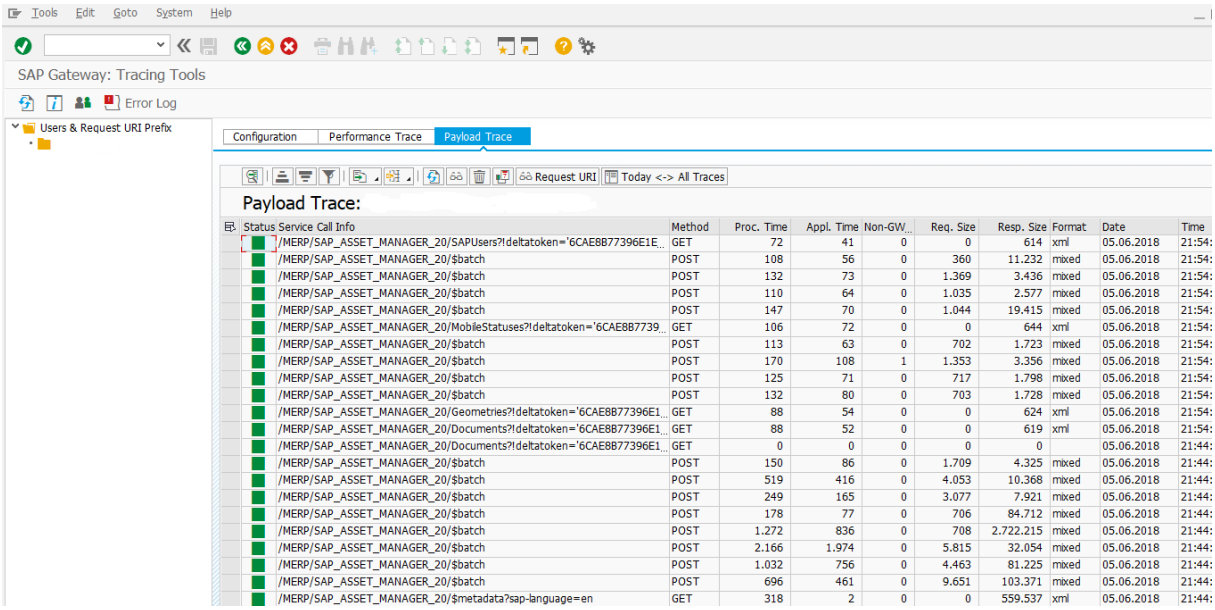
SAP Gateway Statistics aggregates the entries by various entities, for example, client, namespace, service name and version. With the */IWFND/STATS* transaction you can verify details, such as processing time, response size by entity, and other statistics about the complete request.

7.4 SAP Gateway Tracing Tools

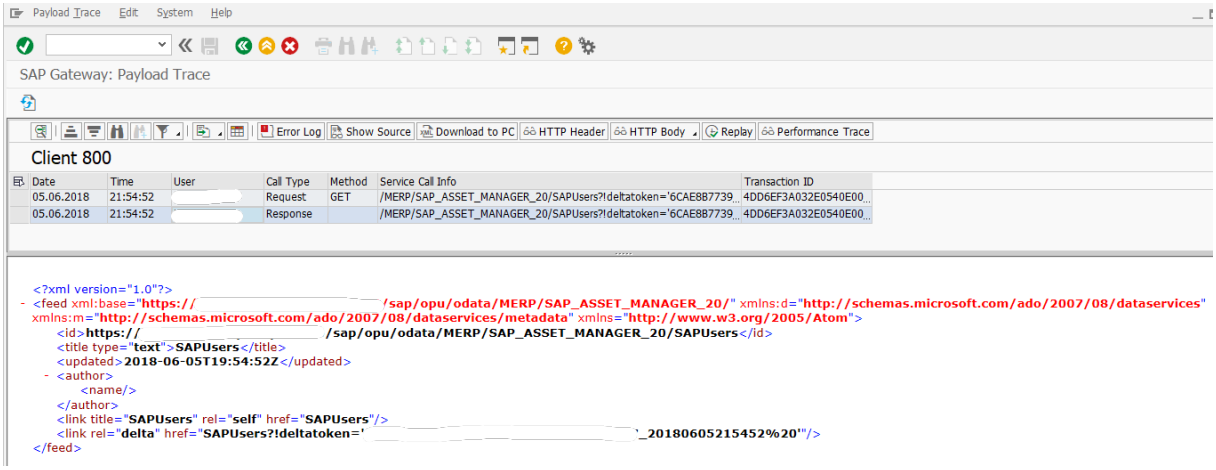
The SAP Gateway provides tracing tools (transaction code: `/IWFND/TRACES`) to trace on a particular user for both performance and payload.

Performance trace enables you to monitor performance at service call level for both the SAP Business Suite and the SAP Gateway. Payload trace enables you to monitor the service calls with request and response data, and to replay and simulate the service calls without accessing the application from the mobile client.

Traces display detailed request and response data coming into the SAP Gateway. Traces are active for only a short time, and are purged on a regular basis.



With this tool, you can verify the exact content of the request header and body that is sent from the mobile device, and also check the response from the SAP Gateway.



Note

For information about how to configure and activate the **Payload Trace** tool, refer to Tracing Tools: Configuration in the *SAP Gateway documentation*.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon  : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

© 2026 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see https://www.sap.com/about/legal/trademark.html for additional trademark information and notices.