# Post-Install or Post-Upgrade Configurations Guide 2502

**Connected Worker Solutions** 



Copyright © 2012-2025, Innovapptive Inc. and/or its affiliates. All rights reserved

# Title and Copyright

**Copyright** and **Terms of Use** for the Post Install or Post Upgrade Configurations Guide for mAssetTag, mWorkOrder, mInventory, and all other solutions of *Connected Workforce Platform*<sup>TM</sup>.

The Post Install or Post Upgrade Configurations Guide for mAssetTag, mWorkOrder, mInventory and all other solutions of *Connected Workforce Platform*<sup>TM</sup>.

Product Version: 2502

Release Date: 11 March 2025

Published Date: 11 March 2025

**Document Version**: 1.0

Copyright © 2025, Innovapptive Inc. and/or its affiliates. All rights reserved.

Primary Author: Innovapptive Inc.

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

# Preface

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

### Audience

This guide is for technical configurators who do Post Install or Post Upgrade Configurations for mAssetTag, mWorkOrder, mInventory, mServiceOrder, mWorkList and all other solutions of *Connected Workforce Platform*<sup>TM</sup>.

### **Document Conventions**

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

#### Table 0-1 Conventions followed in the document

### **Related Products**

- Work Order Management
- Inventory and Warehouse Management
- Operator Rounds
- Inspections Checklist
- Fixed Asset Management
- Field Procurement
- Analytics and Dashboards

### **Contact Innovapptive**

For information on Innovapptive products, visit the Innovapptive's Support Portal at http:// helpdesk.innovapptive.com.

The updates to this document are published on this support portal. Check this website periodically for updated documentation.

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

# Contents

Title and Copyright	ii
Preface	iii
1. Post-Install or Post-Upgrade Configurations for Innovapptive Products	7
2. SAP BTP Configurations after Installing Innovapptive Products	8
3. Configure Authentications	
3.1. Configure HTTP/HTTPs Authentication	10
3.1.1. About SCPms	10
3.1.2. Create New Application using HTTP/HTTPs Authentication	11
3.2. Configure SAML Authentication	15
3.2.1. Establish trust between SAP BTP and ADFS	15
3.2.2. Add SAP BTP Metadata to ADFS	16
3.2.3. Add ADFS Metadata to SAP BTP	20
3.2.4. Add Roles to access SAP BTP Development and Operations Cockpit	
3.2.5. Configure Cloud Connector to accept SAML Assertion Token	
3.2.6. Create New Application using SAML Authentication	23
3.2.7. Define SAML SAP BTP Client Password Policy	26
3.3. Integrate SAP BTP with Azure AD	29
3.3.1. Configure and test Azure AD Single Sign-On	29
4. Configure Push Notifications for SAP BTP	30
4.1. Prerequisites for Push Notifications	
4.2. Configure SAP BTP for Push Notification	
4.2.1. Import SAP BTP Certificate to Gateway system	
4.2.2. Create RFC for Push Notification	35
4.2.3. Configure SAP BTP Applications for Push Notification	38
5. Manage Resource File in SAP BTP	42
5.1. Prepare and Update Resource File for SAP BTP	
5.2. Prepare and Update Resource File for SAP BTP (MWO 2009 SP03 and above releases)	49

5.3. Use Resource File in SAP BTP	55
5.3.1. Add back-end connection RACE URL and upload application help resour	ce55
5.3.2. Add backend connection for Dolphin Services Integration (mAssetTag only)	
5.3.3. Create Application and Upload Resource File	57
5.3.4. Defining Offline Settings for Applications	58
6. Configure Roles and Authorization for Products	63
6.1. Configure SAP security roles for application users	63
6.2. SAP Authorizations for mWorkOrder users	
6.2.1. Update Service authorization object for mWorkOrder	65
6.2.2. Transports for mWorkOrder roles	66
6.2.3. Import roles using Transports	67
6.3. SAP Authorizations for mInventory users	
6.3.1. Update Service authorization object for mInventory	71
6.3.2. Transports for minventory roles	72
6.3.3. Import roles using Transports	73
6.4. SAP Authorizations for mAssetTag users	75
6.4.1. Update Service authorization object for mAssetTag	78
6.5. SAP Authorizations for RACE Dynamic Forms users	80
6.5.1. Update Service authorization object for RACE Dynamic Forms	81
6.5.2. Transports for RACE Dynamic Forms roles	82
6.6. User roles for RACE	83

# 1. Post-Install or Post-Upgrade Configurations for Innovapptive Products

This guide contains instructions for post install or post upgrade configurations for SAP BTP environment. Depending on the platform you are on, choose your configuration path.

### Note:

If you are upgrading from previous versions of Innovapptive products, or if you have already installed one of the Innovapptive products, you would have done most of the configurations. Review all the configurations and do only those that are applicable for your environment.

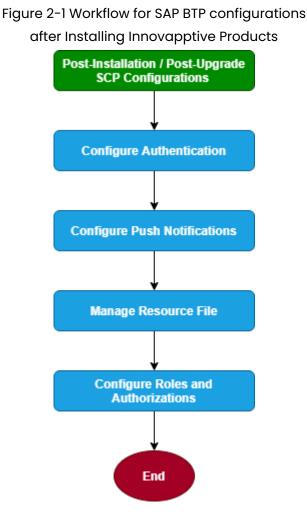
The instructions in the document help you do post-installation configurations for supported versions of the following Innovapptive products:

Table 1–1 Innovapptive Products Product mAssetTag mInventory mWorkOrder

RACE Dynamic Forms

# 2. SAP BTP Configurations after Installing Innovapptive Products

This section guides you with the required SAP BTP Configurations after installing Innovapptive Mobile Products.



Task	Reference to section
Configure authentication for mobile applica- tion	<ul> <li>Configure HTTP/HTTPs Authentication (on page 10)</li> <li>Configure SAML Authentication (on page 15)</li> <li>Integrate SAP BTP with Azure AD (on page 29)</li> </ul>
Configure SAP BTP for Push Notifications	Configure Push Notifications for SAP BTP <i>(on page 30)</i>
Prepare and update resource file	Manage Resource File in SAP BTP <i>(on page 42)</i>
Configure roles and authorizations	Configure Roles and Authorization for Prod- ucts <i>(on page 63)</i>

# 3. Configure Authentications

This section guides you how to set up various authentication mechanisms afterinstalling Innovapptive Mobile Products.

Choose the authentication from the options

- Configure HTTP/HTTPs Authentication (on page 10)
- Configure SAML Authentication (on page 15)
- Integrate SAP BTP with Azure AD (on page 29)

# 3.1. Configure HTTP/HTTPs Authentication

Configure Innovapptive products on SAP BTP Server and set up HTTP/HTTPs authentication mechanism to validate users. Also, validate users to backend servers using Principal Propagation.

Before you configure HTTP/HTTPs authentication, ensure you have:

- Access to SAP BTP as an Administrator
- Access to Cloud Controller as an Administrator
- Admin Roles to your S-User ID

### 3.1.1. About SCPms

Mobile Services Management Cockpit (SCPms) is used to manage and monitor mobile based applications, user registrations, and device connections.

On login, you can view mobile landscape information such as number of applications configured, users connected, and device registrations.

When you navigate to **Mobile Applications** menu you view **Application ID**, **Vendor**, **Number** of **Registrations**, and **Status**.

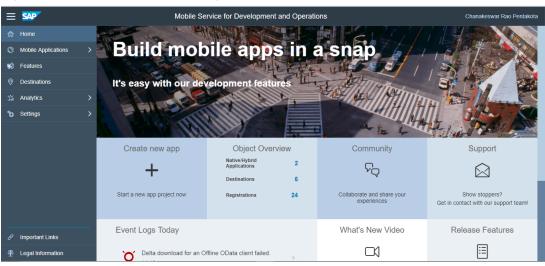


Figure 3-1 Mobile Services Management Cockpit

# 3.1.2. Create New Application using HTTP/HTTPs Authentication

To create new application using HTTP/HTTPs authentication, ensure you have an Application ID. To view the application ID, login to your **SAP BTP** instance and navigate to **Services**, **Development and Operations, Go to Service.** Enter the SAML **Username** and **Password** of the user, who has administrator authorization and click **Application**.

To create an application using HTTP/HTTPs authentication:

- 1. Expand Mobile Applications on the left navigation.
- 2. Click Native/Hybrid under Mobile Applications.
- 3. Click New.
- 4. Enter details such as **Application ID**.

Use the information in the table to add new application details for the product you purchased.

Product	App ID Name Type		Vendor	Security Con- figuration	
mAsset-	com.innovapptive-	Mobile Asset	Na-	Inno-	Basic
Tag	.massettag	Tag	tive	vapptive	
mlnven-	com.innovapptive.min-	Mobile Inven-	Na-	Inno-	Basic
tory	ventory	tory	tive	vapptive	

Product	App ID	Name	Туре	Vendor	Security Con- figuration
mService- Order	com.innovapptive.m- serviceorder	Mobile Service Order	Na- tive	Inno- vapptive	Basic
mShop	com.innovapptive- .mshop	Mobile Shop- ping Cart	Na- tive	Inno- vapptive	Basic
mWorklist	com.innovapptive.m- worklist	Mobile Worklist	Na- tive	Inno- vapptive	Basic
mWorkO- rder	com.innovapptive.m- workorder	Mobile Worko- rder	Na- tive	Inno- vapptive	Basic

- 5. Enter the following in the **New Application** window:
  - Config Templates: Select Native.
  - **ID**: Enter the ID of the product.
  - Name: Enter the name of the product.
  - **Description:** Enter the description of the product.
  - **Vendor**: Enter Innovapptive Inc.

#### Figure 3-2 Create New Application

$\equiv$	SAP		Mobile Service for Development and Operations s0015864207@internal innovapplive.com					
ක		Native/H	lybrid					
Ø		~	Native/Hybrid					
	Native/Hybrid			New App	lication			Q
	SAP Mobile Cards							
48	Features		Config Templates:	Native		~		î↓
0	Destinations		*ID:	scp.test.mwo			C+0530)	
35	Analytics		*Name:	scp.test.mwo				
°o	Settings		Description:					
			Vendor:	Innovapptive Inc.				
			vendor.	innovappiive inc.				
						Save	Cancel	
		s4h.mv		s4h.mwl.res	innov		-31 17:24	
e		s4h.mir		s4h.mim	innov		-31 16:04	
÷		s4h.mir	n.res	s4h.mim.res	innov	2018-08	-31 15:50	

6. Click **Save**.

Figure 3-3 Application Details

Ξ	SAP	Mobile Service for Development and Operations	s0015864207@internal.innovapptive.co
	Home	Native/Hybrid / scp.test.mwo	
	Mobile Applications	cost scp.test.mwo(scp.test.mwo)	
	Native/Hybrid	Delete Export Publish to Discovery Service Lock	
	SAP Mobile Cards	Delete Export Publish to Discovery Service LOCK	
48	Features		
	Destinations	Info APIs Application Links User Registrations Usage Analytics Blocked Users	
	Analytics >	Application Details  Assigned Features	+
°o	Settings >	ID: Name	State
		scp.test.mwo & Access Control	🗹 ок >
		Name:  Scp. test. mwo Client Policies	🗹 ок >
		Description: 40 Client Resources	🗹 ок >
		sample test % Connectivity Innovapotive Inc.	A Incomplete > Configuration
		<sup>b</sup> a Offine	🗹 ок >
		🖂 Push Notification	🗹 ок >
	Important Links		🗹 ок >
	Legal Information		

- 7. Click Connectivity in the Assigned Features section.
- 8. Click **Create** and enter these details.

Figure 3-4 Application Connectivity

≡	SAP		Mobile Service for Development and Operations s0015864207@internal.innovapptive.com								
命	Home		Native/Hybrid / so	cp.test.mwo	/ Connectivity						
٥	Mobile Applications	~	C () ]	nectivity							
	Native/Hybrid		Remove from A	onlication							
	SAP Mobile Cards		Remove non A	ppication							
<b>#</b> \$	Features										
0	Destinations	-	Configuration	Info							
35	Analytics	>								<b>(</b> +	↑Ļ
°¢	Settings	>	Name		Platform Destination Name	URL		Proxy Type	SSO Mechanism/Authenticatio n	Actions	
							No Destinations				
	Important Linka	-									
Ċ	Important Links										
Ŷ	Legal Information										

• **Back End URL**: This URL is from GW System along with Cloud Connector Virtual Host name. Refer the following table:

Product	OData URL
mAssetTag	http(s):// <gw_system_host>:<http(s)_port>/sap/opu/oda- ta/INVMAT/MASSETTAG_2_SRV/</http(s)_port></gw_system_host>
minventory	http(s):// <gw_system_host>:<http(s)_port>/sap/opu/oda- ta/INVMIM/MINVENTORY_2_SRV/</http(s)_port></gw_system_host>
mService- Order	http(s):// <gw_system_host>:<http(s)_port>/sap/opu/oda- ta/INVMSO/MSERVICEORDER_SRV/</http(s)_port></gw_system_host>
mShop	http(s):// <gw_system_host>:<http(s)_port>/sap/opu/oda- ta/INVMSC/MSHOP_SRV/</http(s)_port></gw_system_host>
mWorklist	http(s):// <gw_system_host>:<http(s)_port>/sap/opu/oda- ta/INVMWL/MWORKLIST_3_SRV/</http(s)_port></gw_system_host>
mWorkOrder	http(s):// <gw_system_host>:<http(s)_port>/sap/opu/oda- ta/INVMWO/MWORKORDER_SRV/</http(s)_port></gw_system_host>
RACE Dynam- ic Forms	http(s):// <gw_system_host>:<http(s)_port>/sap/opu/oda- ta/INVCEC/RACE_SRV/</http(s)_port></gw_system_host>

- Proxy Type: Enter Proxy Type as **On Premise**.
- **Maximum Connections**: Default is set to **100**. You may change it based on your requirement.
- Timeout (ms): Set the value to 180000.
- Rewrite Mode: Rewrite URL is set by default.
- SSO Mechanism: Click Add and select Principal Propagation.
- 9. Click Finish.
- 10. Ping the service to ensure it is working.
- 11. Click Security in Assigned Features section.
- 12. Select Security Configuration as **Basic**.

This completes SCP Development & Operations configurations for Basic Authentication.

# 3.2. Configure SAML Authentication

Configure Innovapptive products on SAP BTP Server and set up SAML Authentication mechanism to validate users. Also, validate users to backend servers using Principal Propagation.

Before you configure, ensure:

- Corporate ADFS is working and available outside Corporate Network for Authentication
- You have ADFS Server Metadata
- SCP access with Administrator Authorizations
- OpenSSL Certificates
- Cloud Connector Admin Portal Access

Following sections help you configure SAP BTP Mobile applications to be authenticated with Innovapptive products with your Corporate Active Directory Federation Services.

### 3.2.1. Establish trust between SAP BTP and ADFS

To establish trust between SAP BTP and ADFS:

- 1. Log in to SAP BTP.
- 2. Go to SAP BTP Account, Security, Trust.

# See that **Trust Management** and **Configuration Type** are set to **Default**, which works on **SAP S- User ID** or **SCN ID**.

- 3. Click Edit and make the following changes:
  - **Configuration Type**: Custom (Enables to Add Trust connection).
  - Local Provider Name: https://hanatrial.ondemand.com/s0015864207trial (should be generated automatically from SAP BTP. URL will be different for each instance based on its ID).
  - Signing Key: If the Signing Key is blank, click Generate Key Pair.
  - Signing Certificate: If the Signing Certificate is blank, click Generate Key Pair.
  - Principal Propagation Enabled.
  - Force Authentication: Disabled.
- 4. Click Get Metadata link and save it as a local file.

This allows you to add a new Trust Relaying Party in ADFS.

### 3.2.2. Add SAP BTP Metadata to ADFS

After you download Metadata file from SAP BTP, log in to ADFS 2.0 server and copy the Metadata file to Desktop.

To establish Mutual Trust between SAP BTP and ADFS:

- 1. Click Start, Administration Tools, AD FS 2.0 Management.
- 2. Expand View ADFS 2.0, Trust Relationships, right-click Relying Party.
- 3. Select Relying Party Trusts and select Add Relying Party Trust.

Figure 3-5 ADFS Relying Party Trusts

🃬 AD F5 2.0					
🏟 File Action View Wind	dow Help				
🗢 🔿 🔰 🖬 🚺					
AD FS 2.0	Relying Par				
E Service     Displa     Displa					
Claims Provider Trust	ts HANA 1				
Relying Party Trusts	114414.1				
Attribute Stores Add Relying Party Trust					
	View   New Window from Here				
	Refresh				
	Help				

- 4. Click Start.
- 5. Select Import data about the relying party from a file and click Browse.
- 6. Navigate to the file, which you copied and click Next.
- 7. Enter **Display name** and click **Next**.
- 8. Select Permit all users to access this relying party and then click Next.

All the SAML2 Metadata configurations that are imported into ADFS can be viewed in different tabs.

- 📬 Add Relying Party Trust Wizard X Ready to Add Trust Steps The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database. Welcome Select Data Source 4 > Encryption Signature Accepted Claims Organization Endpoints Notes Advanced Specify Display Name Specify the endpoints to use for SAML and WS-FederationPassive protocols. Choose Issuance Authorization Rules URL Index Binding Default Response URL Ready to Add Trust SAML Assertion Consumer Endpoints Finish https://authn.hanatrial.ondem... 0 POST Yes SAML Logout Endpoints https://authn.hanatrial.ondem... n/a Redirect No https://authn.hanatrial.ondem... n/a POST No Cancel < Previous Next > Help
- Figure 3-6 Relying Party Trust Wizard

#### 9. Click Next.

10. Click Close. The Claim Rule Editor window opens.

If you do not remove the check box active, you will continue further to post user creations.

- 11. After adding the SCP Metadata to ADFS, add Claim Rules to accept username and password and send the required assertion tokens after validations.
- 12. Go to ADFS Management Console, select **Relying Party Trusts** and select the entry. In this case, it is **SCPTRIAL\_SOOXXXXX**.
- 13. Click Edit Claim Rules.

💱 AD FS 2.0				
翰 File Action View Window Help				_ <b>5</b> ×
🗢 🔿 📩 📅 🔽 🖬				
AD FS 2.0	Relying Party Trusts			Actions
Service Endpoints	Display Name	Enabled	Identifier	 Relying Party Trusts 🔺
Certificates	HCPTRIAL_S0015864207	Yes	https://hanatrial.ondemand.com/s00	Add Relying Party Trust
Claim Descriptions				View 🕨
Claims Provider Trusts				New Window from Here
Relying Party Trusts Attribute Stores				Q Refresh
Attribute stores				I Help
				HCPTRIAL_S0015864207
				Update from Federation Metadata
				Edit Claim Rules
				Disable
				Properties
				🗙 Delete
				Palp

Figure 3-7 Edit Claim Rules

This Claim Rule instructs ADFS to issue the user's (Domain) logon name as the subject name identifier (Name ID) in the SAML Response sent back to SAP BTP.

- 14. Click Add Rule, select Send LDAP Attributes as Claims under Claim rule template and click Next.
  - Claim rule name: Issue SAMAccountName as Name ID.
  - Attribute store: Active Directory.
  - Mapping of LDAP attributes to outgoing claim types:
    - LDAP Attribute: SAM-Account-Name.
    - Outgoing Claim Type: Name ID.

#### Figure 3-8 Edit Rule

dit Ru	le - att		×
whicł issue		values of LDAP attributes as claims. Select an attribute store y how the attributes will map to the outgoing claim types tha	
att			
Rule	template: Send LDAP Attributes as	Claims	
Attrib	ute store:		
Activ	e Directory	<b>•</b>	
Марр	ing of LDAP attributes to outgoing	claim types:	
	LDAP Attribute	Outgoing Claim Type	
+	SAM-Account-Name	Name ID	-
*			-

- 15. Click **Finish**. Rule1 is now saved.
- 16. Click Add Rule. This Claim Rule instructs ADFS to issue the user's firstname, lastname, organizational ID, and employee ID as SAML Attributes (also known as "Claims") in the response. (Options Configurations per the requirement).
- 17. Under Claim rule template, select Send LDAP Attributes as Claims and click Next.

Figure 3-9	Select Rule	Template
------------	-------------	----------

Select Rule Templat	e
Steps	Select the template for the claim rule that you want to create from the following list. The description
🥥 Choose Rule Type	provides details about each claim rule template.
Configure Claim Rule	Claim rule template: Send LDAP Attributes as Claims

18. Claim rule name: Enter the Claim rule name as Send Given Name and enter the details

as shown below.

Figure 3-10 Configure R	ule
-------------------------	-----

<b>\$</b>	Add Transfo	rm Claim Rule Wizard
Configure Rule		
Steps Choose Rule Type Configure Claim Rule	also map an incoming claim va outgoing claim type and wheth Claim rule name: Send Given Name Rule template: Transform an Ir Incoming claim type: Incoming name ID format: Outgoing claim type: Outgoing name ID format: Outgoing name ID format: Outgoing name ID format: Outgoing name ID format: Outgoing claim type: Outgoing claim value: Outgoing claim value:	Given Name  Unspecified  Name ID  Common Name
		< Previous Finish Cancel

19. Click Finish.

### 3.2.3. Add ADFS Metadata to SAP BTP

To complete trust between SAP BTP and ADFS, you must also add ADFS metadata to SCP.

To add ADFS metadata to SAP BTP:

- 1. Generate metadata file from ADFS server, using the following URL: https:// ADFSServerHostname/federationmetadata/2007-06/federationmetadata.xml
- 2. Save the metadata file.



Use ID while generating metadata files.

- 3. Login to SAP BTP Account and navigate to **Security**, **Trust**, **Trusted Identity Provider**, **Add Trusted Identity Provider**.
- 4. Click **Browse** and select ADFS Metadata file.
- 5. Click **Save**.

# 3.2.4. Add Roles to access SAP BTP Development and Operations Cockpit

Once SAML is enabled, you cannot login with S-User ID. All services and applications are redirected to ADFS for SAML Authentication. Hence, roles added to SAP BTP Development and Operations help users from ADFS to login for administration or development tasks.

To add roles:

- 1. Navigate to SAP BTP, Services, Development & Operations, Configure Development & Operations Cockpit, In Application Permissions.
- 2. Click Edit.
- 3. Under Assign Role, select MobileServicesCockpitAdministrator.
- 4. Click Save.
- 5. Navigate to SAP BTP, Services, Development & Operations, Configure Development & Operations, Roles.

SAP BTP pre-defined roles are displayed on the right side of the window.

Figure 3-11 SAP BTP Roles

6. Select Administrator and click Add User under Individual Users.

# Note: If your user ID is username@domain.com, add only username. If it does not work, you must add full details username@domain.com.

#### SAP Cloud Platform Cockpil ሲ 🕲 🖬 🤣 ₿ De (∂ н.. US East (As.. ✓ / 品 Innovapptive. Newmont\_P... ✓ / ₩ Development & Operat Configure Develo ment & Operations Roles (All: 9) 🔎 Role ? 📑 New Role Name Туре Predefined Helpdock Administrat Predefined Predefined Administrator Predefined: Provisioned by the application idual Users Assign Unassign All Groups Assign Unassign Al User ID Actions Group Unassign ⑦ Useful Links 🖗 Legal Inf

Repeat the same process with other roles such as Developer, Helpdesk, Impersonator, and Notification User based on your access requirements for User IDs.

### 3.2.5. Configure Cloud Connector to accept SAML Assertion Token

As Innovapptive servers are set up at various environments, such as Public Cloud and Corporate Network, you use Cloud Connector to securely transmit data from different environments. It is required to establish trust between SAP BTP, Cloud Connector and SAP Gateway System which is on the Corporate Network.

Before configuring, ensure you have:

- Working Cloud Connector
- Certificates exchanged between Cloud Connector GW system
- Access Controls are defined, and resources are available to SAP BTP Server

To configure Cloud Connector to accept SAML Assertion Token:

- 1. Login to Cloud Connector and navigate to Account, Principal Prorogation.
- 2. Click Synchronize.

Trust between SAP BTP and ADFS is updated and Cloud Connector accesses the same details.

3. Configure Trust for **dispatcher** and **mobilejava**.

Once ADFS Server is listed, ensure it is operational as shown below.

Figure 3-12 Trust Configuration

Trust Configuration			6	/ 0
Name	Description	Туре	Trusted	Actions
accounts.sap.com	SAP ID Service	IDP	$\oslash$	R
http://adfs.innovapptive.com/adfs/services/trust		IDP	$\odot$	R
b70068d2c:jsy	jsy	HANA	$\otimes$	R
b70068d2c:yze	yze	HANA	$\otimes$	R
portal:nwc	nwc	JAVA	$\otimes$	R
services:dispatcher	dispatcher	JAVA	$\odot$	R
hanamobileprod:mobilejava	mobilejava	JAVA	$\odot$	E.

### 3.2.6. Create New Application using SAML Authentication

To create new application using SAML authentication, login to your SAP BTP instance and navigate to **Services**, **Development and Operations**, **Go to Service**. Enter the SAML **Username** and **Password** of the user, who has administrator authorization and click **Application**.

To create an application using SAML Authentication:

- 1. Expand Mobile Applications on the left navigation.
- 2. Click Native/Hybrid under Mobile Applications.
- 3. Click Create New Application.

Use the information in the table to add new application details for the product you purchased.

Product	App ID Name Type Vend		Vendor	Security Con- figuration	
mAsset-	com.innovapptive-	Mobile Asset	Na-	Inno-	Basic
Tag	.massettag	Tag	tive	vapptive	
mlnven-	com.innovapptive-	Mobile Inven-	Na-	Inno-	Basic
tory	.minventory	tory	tive	vapptive	

Product	App ID	Name	Туре	Vendor	Security Con- figuration
mSer- viceOrder	com.innovapptive.m- serviceorder	Mobile Service Order	Na- tive	Inno- vapptive	Basic
mShop	com.innovapptive- .mshop	Mobile Shop- ping Cart	Na- tive	Inno- vapptive	Basic
mWorklist	com.innovapptive.m- worklist	Mobile Worklist	Na- tive	Inno- vapptive	Basic
mWorkO- rder	com.innovapptive.m- workorder	Mobile Worko- rder	Na- tive	Inno- vapptive	Basic

4. Enter the following information in the **New Application** window:

- Config Templates: Select Native.
- **ID**: Enter the ID of the product.
- Name: Enter the name of the product.
- **Description:** Enter the description of the product.
- **Vendor**: Enter Innovapptive Inc.

#### Figure 3-13 Create New Application

$\equiv$	SAP			Mobile	Service	e for Development and	Operations	\$			s00158642	207@internal.inno	vapptive.com
â			Native/	Native/Hybrid									
٢		~		Native/Hybrid									
						New App	olication						q
48				Config Templates:	Native					~			î↓
0				*iD:	scp.tes	t.mwo						C+0530)	
35				*Name:	scp.tes	t.mwo							
°0				Description:									
												_	
				Vendor:	Innova	pptive Inc.							
										Save	Cancel		
											08-31 17:24		
		-											
e			s4h.m			s4h.mim		innov			08-31 16:04		
Ŧ			s4h.m	im.res		s4h.mim.res		innov		2018-	08-31 15:50		

- 5. Click **Save**.
- 6. Click **Connectivity** in the **Assigned Features** section.
- 7. Click **Create** and enter these details.

• **Back End URL**: This URL is from GW System along with Cloud Connector Virtual Host name. Refer the following table:

Product	OData URL
mAssetTag	http(s):// <gw_system_host>:<http(s)_port>/sap/opu/oda- ta/INVMAT/MASSETTAG_2_SRV/</http(s)_port></gw_system_host>
mInventory	http(s):// <gw_system_host>:<http(s)_port>/sap/opu/oda- ta/INVMIM/MINVENTORY_2_SRV/</http(s)_port></gw_system_host>
mService- Order	http(s):// <gw_system_host>:<http(s)_port>/sap/opu/oda- ta/INVMSO/MSERVICEORDER_SRV/</http(s)_port></gw_system_host>
mShop	http(s):// <gw_system_host>:<http(s)_port>/sap/opu/oda- ta/INVMSC/MSHOP_SRV/</http(s)_port></gw_system_host>
mWorklist	http(s):// <gw_system_host>:<http(s)_port>/sap/opu/oda- ta/INVMWL/MWORKLIST_3_SRV/</http(s)_port></gw_system_host>
mWorkOrder	http(s):// <gw_system_host>:<http(s)_port>/sap/opu/oda- ta/INVMWO/MWORKORDER_SRV/</http(s)_port></gw_system_host>
RACE Dynam- ic Forms	http(s):// <gw_system_host>:<http(s)_port>/sap/opu/oda- ta/INVCEC/RACE_SRV/</http(s)_port></gw_system_host>

- Proxy Type: Enter Proxy Type as On Premise.
- **Maximum Connections**: Default is set to **100**. You may change it based on your requirement.
- Timeout (ms): Set the value to 180000.
- **Rewrite Mode**: Rewrite URL is set by default.
- SSO Mechanism: Click Add and select Principal Propagation.
- 8. Click Finish.
- 9. Ping the service to ensure it is working.
- 10. Click Security in the Assigned Features section.
- 11. Select Security Configuration as **SAML**.

### Note:

You should have Users Mapping in GW system to have Principal Propagation working to Gateway System.

## 3.2.7. Define SAML SAP BTP Client Password Policy

Define the client password policy that is used to unlock the DataVault for the applications. Application developers must add code to the DataVault to enforce the client password policy. An administrator must enter the application password policy to unlock the DataVault during application initialization.

The client password policy applies only to the application password that unlocks the DataVault during application initialization; it affects neither SAP Cloud Platform mobile service for development and operations security profiles nor the back-end security systems with which it integrates. Password policies for back-end security systems are administered by your information technology departments using native security administration tools.

To define the Password policy:

- 1. In Mobile Service for Development and Operations cockpit, select **Mobile Applications >** Native/Hybrid.
- 2. Select an application, and then select Client Policies under Assigned Features.

≡	SAP	Mobile Service for Development and Operations		s0015864207@internal.innovapptive.com
ଜ	Home	Native/Hybrid / scp.mlm		
٥	Mobile Applications	scp.mim(scp.mim)		
	Native/Hybrid	Delete Export Publish to Discovery Service		
	SAP Content to Go	Delete Export Publish to Discovery Service		
<b>1</b> 8	Features			
	Destinations	Info APIs User Registrations Usage Analytics Blocked Users		
	Analytics >	Application Details	Assigned Features	+
°¢	Settings	ID:	Name	State
		scp.mim	음 <sup>6</sup> Access Control	🗹 ок >
		Name: scp.mim	ଶ୍ୱି) Client Policies	[⊻ ок →
		Description:	A Client Resources	≤ок >
		minventory	え Connectivity	г⊻ ок →
		Vendor:	°a Offline	[⊻ок >
			Push Notification	<b>⊠</b> ок >
	Important Linka		Security	🗹 ок >
	Important Links			
	Legal Information			

Figure 3-14 Application Details

3. Under **Passcode Policy**, select **Enable Passcode Policy** checkbox and enter these details.

≡	SAP	Mobile Service for Develo	opment and Operations	s0015864207@internal.innovapptive.co
৯	Home	Native/Hybrid / scp.mim / Client Policies		
٥	Mobile Applications	Client Policies		
	Native/Hybrid	Save Reset Remove from Application		
	SAP Content to Go	Заче понт Арлісакон		
40	Features			
0	Destinations	Configuration Info		
35	Analytics >	Passcode Policy	Log Policy	
°O	Settings >	Enable Passcode Policy:   Expiration Time Frame:	Enable Client Log Upload:  Database Upload Policy Enable Database Upload Policy: Usage Report Policy Enable Usage Report Policy s	
_	Important Linke	Feature Restriction Policies (8)		G
e t	Important Links			
- 19	Legal Information	Plugin	ID	Allowed Actions

Figure 3-15 Client Policies

The following table shows the description for the fields.

Property	De- fault	Description
Expira- tion Time Frame Days	0	The number of days a password remains valid. The default value, 0, means the password never expires.
Minimum Length	8	The minimum password length.
Retry Limit	10	The number of retries allowed when entering an incorrect password. After this number of retries, the client is locked out, the DataVault and all its contents are permanently deleted, the application is un- usable, and encrypted application data is inaccessible.

Property	De- fault	Description
Minimum Number of Unique Charac- ters	0	The minimum number of unique characters required in the pass- word.
Lock Timeout	300	The number of seconds the DataVault remains unlocked within an application, before the user re-enters his or her password to continue using the application (like the screen-saver feature).
Default Passcode Allowed	Dis- abled	If enabled, a default password is generated by the DataVault. This disables the password.
Finger Print Al- lowed	En- abled	If enabled, it allows the use of native biometric techniques to unlock the app.
Upper Case Charac- ter Re- quired	Dis- abled	If enabled, the password must include uppercase letters.
Lower Case Charac- ter Re- quired	Dis- abled	If enabled, the password must include lowercase letters.
Special Charac- ter Re- quired	Dis- abled	If enabled, the password must include special characters.
Digits Re- quired	Dis- abled	If enabled, the password must include digits.

### 4. Click **Save**.

# 3.3. Integrate SAP BTP with Azure AD

By integrating SAP BTP with Azure AD:

- You can control users' access to SAP BTP
- You can manage accounts using the Azure portal
- Users can login (Single Sign-On) to SAP BTP using their Azure AD accounts

For more information on SaaS app integration with Azure AD, see what is application access and single sign-on with Azure Active Directory.

To integrate SMP with Azure AD:

- Configure the SAP BTP application for Single Sign-On using Azure AD
- Configure assertion-based groups for Azure Active Directory Identity Provider

Azure AD users assigned to SAP Cloud Platform can single sign into the application using the Introduction to the Access Panel.

Before proceeding, ensure you have:

- Azure AD subscription
- SAP Cloud Platform Single Sign-On enabled subscription

### 3.3.1. Configure and test Azure AD Single Sign-On

Read these topics to learn how to configure and test Azure AD Single Sign-On with SAP BTP:

- 1. Add SAP Cloud Platform from the gallery
- 2. Configure Azure AD Single Sign-On
- 3. Configure SAP Cloud Platform Single Sign-On
- 4. Configure assertion-based groups: This is an optional step.
- 5. Create an Azure AD test user
- 6. Assign the Azure AD test user
- 7. Create SAP Cloud Platform test user
- 8. Test single sign-on

# 4. Configure Push Notifications for SAP BTP

Field workers gets an alert when an item to which he /she is tagged to is created or modified. However, if the app is not launched on the device, they do not receive these alerts. You must configure Push Notifications to send the alerts to the workers even when the app is not opened in the device.

This section helps you configure Push Notification for SAP BTP mobile services that you are using with Innovapptive iOS Certificates/ Android API Key / Windows SID. Check pre-requisites and limitations listed in the document carefully.

**Assumptions**: Your organization has discussed with Innovapptive about the Push Functionality requirement and are aware of the following details:

- You are aware of iOS, Android, and Windows Push Functionalities.
- You have discussed with Innovapptive team about Push Notification.
- You have collected the necessary Certificates/Key to configure Push Notification.
- You do not have your own Push Certificates/Keys for configurations.

The following topics help you configure push notifications with Innovapptive iOS Certificates/ Android API Key / Windows SID:

- Prerequisites for Push Notifications (on page 30)
- Configure SAP BTP for Push Notification (on page 31)
- Configure SAP BTP Applications for Push Notification (on page 38)

# 4.1. Prerequisites for Push Notifications

Based on your operating system, obtain the following:

#### System and Software

- Certificate and API key
- **iOS**: Obtain the Push Certificate.
- Android: Obtain the Google API Key & Sender ID.
  - Public Server Key: AlzaSyDURzJeh8FTBIJBDxwwRSZLfp755I7jTAw
  - Sender ID: 877276486448
- Windows: Obtain Package SID and Client Secret key.

#### Note:

For the certificates and keys, contact Innovapptive.

#### • Access

#### Note:

This section describes the process of configuring with Innovapptive Certificates/API Key. Any changes in the process must be discussed with Innovapptive team.

- SAP BTP Admin Access.
- Access to SAP Gateway System with Basis Roles.

**Dependency**: If your organization has Own Push Certificates (iOS) and Keys (Android/ Windows), inform Innovapptive because the Application release plan might have to be changed based on your organization's needs.

# 4.2. Configure SAP BTP for Push Notification

To configure SAP BTP for push notification:

- 1. Log in to SAP BTP Account.
- 2. Navigate to your **Sub Accounts**.

Sub Accounts depends on whether they are created for your account. You can directly create a Tenant in your main account. For example, {your\_company\_name} can be main account and it could have multiple sub accounts and the sub accounts can have a tenant. {your\_company\_name} can also directly have a tenant under it.

- 3. Click your **Tenant**.
- 4. Click Services.
- 5. Select Mobile option from All Categories list.

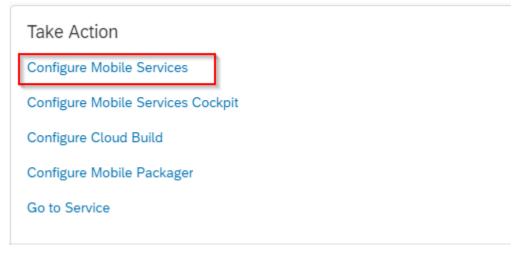
| 4 - Configure Push Notifications for SAP BTP

	HTML5 Applications			All Categories V Search
	HANA XS Applications	Analytics		All Categories Analytics
	Subscriptions	Predictive Service	SAP Smart Business Service	Data Management
¢	Services	Not enabled	Enabled Expose KPIs and OPIs as SAP Fiori	Data Privacy & Security
•	Solutions	data in your SAP HANA database.	applications without the need to write any code.	Developer Experience
۲	SAP HANA / SAP ASE 🗸 🗸			DevOps Document Management
	Database Systems	Data Management		Integration
	Databases & Schemas	📫 SAP ASE	📫 SAP HANA	Internet of Things
	Service Requests	Enabled	Enabled	Mobile

6. Select Mobile Services, users.

Mobile Services, consumers	Nobile Services, preview	Nobile Services, users
Enabled Build and run mobile apps for B2C use cases.	Failed Run integration and regression tests and explore new mobile features. NOT FOR PRODUCTIVE USE.	Enabled Build and run mobile apps for B2E and B2B use cases.

7. In the Service: Mobile Services, users – Overview screen, click Configure Mobile Services in the Take Action section.



- 8. Click Roles.
- 9. In the Service Configuration: Configure Mobile Services Roles screen, select Notification User in the New Role table.

10. Click Assign.

<i> </i>	📟 US East 🗸 / 品 Innovapptive Inc. 🗸 / 営 Innovappti	ve Inc. 🗸 / 📢 D
ුස් Roles	Roles (All: 10)	
	E New Role	
	Name	Туре
	Microservice	Predefined
	Security User	Predefined
	AccountDeveloper	Custom
	Notification User	Predefined
	Developer	Predefined
	Notification User Predefined: Provisioned by the application	101
	Individual Users Assign Unassign All	
	User ID	Actions

- 11. In the **Assign role "Notification User" to user popup**, enter the S-User ID that has administrator access to SCP.
- 12. Click Assign.

### 4.2.1. Import SAP BTP Certificate to Gateway system

Import SAP BTP certificate to Gateway system to establish mutual trust between SAP BTP and Netweaver Gateway.

To import SAP BTP certificate:

- 1. Go to **STRUST** transaction.
- 2. Navigate to Environment, SSL Client Identities.
- 3. Click on **Change** option and select New Entries --> create SSL identity with the following details:
  - a. Identity: SCPMS
  - b. Description: SAP Cloud Platform

Figure 4-1 SSL Client Identities

Display	View "SSL Client Identities of System": Ove	erview
🦻 🖪 🖪 I	B	
SSL Client Id	entities of System	
Identity	Description	<b></b>
ANONYM	SSL Client (Anonymous)	*
DFAULT	SSL Client (Standard)	<b>_</b>
SCPMS	SAP Cloud Platform	
WSSE	WSSE Web Service Security Test	44

- 4. Navigate to the **STRUST** screen.
- 5. Right-click on SSL Client SAP Cloud Platform and click Create.
- 6. On the **Create PSE** screen, the following details are retrieved from the source certificate:
  - a. Name
  - b. Org.
  - c. Comp./Org.
  - d. CA
  - e. Algorithm
  - f. Key Length

Figure 4-2 Create PSE

🔄 Create PSE	×
Name	NGT SSL client SAP Cloud Platform
Org. (Opt)	10020732638
Comp./Org.	SAP Web AS
Country	
CA	O=SAP Trust Community, C=DE
Algorithm	RSA with SHA-1 🔻
Key Length	1024 🔹

7. Import the SAP BTP certificate provided by Innovapptive under **SSL client SAP Cloud Platform**.

#### 8. Click Add to Certificate List.

9. Click **Save**.

Figure 4-3 Add SAP BTP certificate to list

Trust Manager: Change		
🦻 🕅		
System PSE     SNC SAPCryptolib	Subject	01-1031-335, 08-384, 0900 Pietronn, 00-10020732036, 00-384, 998- (Self-Signed)
SSL server Standard     SSL client SSL Client (Anonymo     SSL client SSL Client (Standar	Certificate List	Subject
SSL clent SAP Cloud Platform     SSL clent SAP Cloud Platform     SSL clent WSSE Web Service Se		
WS Security Standard     WS Security Other System Encry     WS Security WS Security Keys	P	
SMIME Standard     SF File     SSF Collaboration Integration	Verl. PSE	Password
SSF SAML2 Service Provider - E     SSF SAML2 Service Provider - S	Certificate	
<ul> <li>I SSF Logon Ticket</li> </ul>	Subject	CN=*.us1.hana.ondemand.com, OU=SAP Cloud Managed Services, O=SA
	Subject (Alt.)	dNSName=*.hana.ondemand.com, dNSName=us1.hana.ondemand.com, _
	Issuer	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US
	Serial Number (Hex.)	09:13:BD:22:5F:7D:88:DF:59:78:06:34:0B:74:B9:4F
	Serial Number (Dec.)	12065541701101858254166065755618326863
	Valid From	06.01.2019 00:00:00 to 01.02.2021 12:00:00
	Algorithm	RSA with SHA-256 Key Length 2048
	Check Sum (MD5)	02:ED:64:3C:DA:82:62:9D:34:3B:09:39:C1:6D:16:8D
	Checksum (SHA1)	8A:F7:15:33:7B:F1:E2:F7:56:59:89:8E:C9:05:15:57:F4:A1:BE:52
		Add to Certificate List
		Add Certificate to PSE

### 4.2.2. Create RFC for Push Notification

Following steps guide you to configure RFC to establish HTTP communication between SAP and external server.

- 1. Go to SM59 transaction and create a RFC of connection type G.
- 2. In the **RFC Destination** window, enter the following information:

#### Table 4-1 RFC Destination

Field	Description
RFC Destination	IWBEP_ODATA_OD_PUSH
Target Host	SAP BTP Host
Path Prefix	/notification

Field	Description
Service No	443

#### Figure 4-4 Create RFC

CFC Destinatio	n IWBEP_ODATA_OD_PUSH
onnection Test 😚	
Connection Type	IWBEP_ODATA_OD_PUSH       HTTP Connection to External Serv     Description
	TTP connection to SMP Dev for Push
Description 1 H	
Description 3	
Description 3	
Administration	Technical Settings Logon & Security Special Options
Target System Settin	05
E-	noble-
Target Host	
Target Host	noble-Intercontent .hana.ondemand.com
Target Host r Path Prefix	Notification
Target Host r Path Prefix /	Notification
Target Host Fr Path Prefix // HTTP Proxy Options Global Configuration	Notification
Target Host Fr Path Prefix // HTTP Proxy Options Global Configuration Proxy Host	Notification
Target Host Path Prefix P HTTP Proxy Options Global Configuration Proxy Host Proxy Service	noble-Internet .hana.ondemand.com

- 3. On the Logon & Security tab, choose Basic Authentication.
- 4. Enter **S-User** and **Password**.

5. In the **Security Options** section, select the SSL Certificate (SCPMS SAP Cloud Platform) created in Import SAP BTP Certificate to Gateway system *(on page 33)*.

RFC Destination IWBEP_ODATA_OD_PUSH	
Connection Test  ô	
RFC Destination     IWBEP_ODATA_OD_PUSH       Connection Type     G       HTTP Connection to External Serv     Description	
Description 1 HTTP connection to SMP Dev for Push Description 2 Description 3	
Administration       Technical Settings       Logon & Security       Special Options         Security Options       Status of Secure Protocol       SSL       Inactive       Active         SSL       Inactive       Active       SSL       Cert. List         Authorization for Destination	
	×

Figure 4-5 Select SSL Certificate

- 6. Click **Save**.
- 7. Click **Connection Test** to validate the configuration.

Figure 4-6 HTTP Connection to External Server

Connection Test HTTP Destination IWBEP_ODATA_OD_PUSH			
Destination IV	WBEP_ODATA_OD_PUSH		
Ту. Η	TTP Connection to External	Server	
Test Result	Response Header Fields	Response Body Response Text	
Detail	Value		
Status HTTP Respon	ise 405		
Status Text Method Not Allowed			
Duration Test Call	1140 ms		

## 4.2.3. Configure SAP BTP Applications for Push Notification

To configure SAP BTP applications for push notification:

- 1. Log in to SAP BTP Account.
- 2. Navigate to your **Sub Accounts**.

Sub Accounts depends on whether they are created for your account. You can directly create a Tenant in your main account. For example, {your\_company\_name} can be main account and it could have multiple sub accounts and the sub accounts.

- 3. Click your **Tenant**.
- 4. Click Services.
- 5. Select Mobile option from All Categories list.
- 6. Select Mobile Services, users.
- 7. In the Service: Mobile Services, users Overview screen, click Go to Service in the Take Action section.

Take Action
Configure Mobile Services
Configure Mobile Services Cockpit
Configure Cloud Build
Configure Mobile Packager
Go to Service

#### Note:

Depending on your environment, you could be asked for authentication.

- 8. Expand Mobile Applications and click Native/Hybrid button.
- 9. In the **Native/Hybrid** screen, click the Application ID for which you need Push Notification.

#### | 4 - Configure Push Notifications for SAP BTP

≡	SAP Cloud Platform M	Iobile Services		
命	Home	Native/Hybrid		
0	Mobile Applications 🛛 🗸	Native/Hybrid           All 4		
	Native/Hybrid	New Import		
	SAP Mobile Cards			
<b>P</b> Ş	Features	Name	Application ID	Vendor
0	Destinations	10 Terrip	And the second	innov
~~	A	top manage at	top manage an	innov
	Analytics >	10.040.40	1(2-1040.40)	
°¢	Settings >	10.510	10.510	

10. In the Application ID Details screen, click **Push Notification**.

ଜ	Home	Native/Hybrid /	
Ø	Mobile Applications 🔹 🗸		
	Native/Hybrid	Delete App Export App Lock App Publish to Discovery Service	
	SAP Mobile Cards	Info APIs Application Links User Registrations Usage Analytics Blocked Users Support Sessions	
<b>Ņ</b> Ŝ	Features	Application Details	+
0	Destinations	Name State	•
35	Analytics >	g <sup>6</sup> Access Control ☑ C	
°o	Settings	බ් Client Policies 🗹 c	ж >
- 22	Setungs 7	성 Client Resources [] C	ж >
		🗟 Connectivity 🗹 🖸	ж
		land a filine [✓ C	ж
		🖂 Push Notification 🗹 🖸	ж >
Ċ	Important Links	🔒 Security 🗹 🖸	ж >
Ф.	Legal Information		

11. Click the **Configuration** tab and do the following:

• **iOS Device:** Scroll to option Apple and change the **APNS Endpoint** from *None* to *Sandbox/Production* based on the certificate type. Upload Certificate and save the settings.

Apple	
APNS Endpoint:	
Production	~
Authentication:	
<ul> <li>Certificate</li> </ul>	
O Token-based	
*Certificate (P12):	
1986/00/00/00/00/00/00/00/00/00/00/00/00/00	Browse
*Password:	

• Android Device: To configure Android, enter the Server Key and Sender ID in the same screen.

Android			
Server Key:			
*Sender ID:			

• Windows Device: To configure Windows, enter the Package SID and Client Secret details in the same screen in WNS.

#### | 4 - Configure Push Notifications for SAP BTP

WNS			
Package SID:			
Client Secret:			

12. Click **Save**.

## 5. Manage Resource File in SAP BTP

Resource File in SAP BTP helps you centrally administer and manage common settings.

Resource file helps you do the following:

- Use a single file (or build) for all system landscapes (Dev, QA, and Production). Users then:
  - Do not have to manually maintain the settings/parameters on the Login screen.
  - Can select/switch the appropriate environment they want to access.
  - Avoid need for managing multiple files/builds.
  - Can rollout mobile app deployment, as the system parameters/settings details are automatically determined improving user experience, ease of use, and adoption.
  - Can maintain common settings/parameters information Security profile, and Connection details in the resources text file and administer centrally by the SAP BTP admin user.
- **Make branding changes**: Change background images, color, and theme based on your enterprise branding needs by changing the settings/parameters in the resources text file. This file is administered centrally by the SAP BTP admin user.

When this resource file is updated, the application connects to the mobile platform (SAP BTP) and registers the device with the available branding images of your organization. Once the registration is completed, the application fetches settings like Application ID, Security Profile, Port Numbers, HTTP/HTTPs connection details and multiple languages, which are supported by the applications.

#### Note:

The branding changes are not applicable to MWO 2009 SP03 version.

Learn how to manage the **resources file** using the SAP Business Technology Platform (SAP BTP):

- Prepare and update the resource file (All platforms-iOS, Android, and Windows).
- Configure resource file for SAP BTP (Cloud).

The following topics help you with resource file management:

- Prepare and Update Resource File for SAP BTP (on page 43)
- Prepare and Update Resource File for SAP BTP (MWO 2009 SP03 and above releases) (on page 49)
- Use Resource File in SAP BTP (on page 55)

## 5.1. Prepare and Update Resource File for SAP BTP

The **mWorkOrder** application resource file **resources\_mworkorder.zip** on Windows platform is used as an example to demonstrate the procedure. Do your branding changes in the zip file that is provided by Innovapptive initial deployment.

To prepare and update the resource file:

- 1. Download the **resources\_mworkorder\_zip** file to the local drive.
- 2. Extract the resource\_mmworkorder.zip file.

The following folder structure is displayed when you extract.

4	resource_mworkorder
۵	🃕 DEV
	🌗 ios

I

3. Navigate to the iOS folder. (Same file and settings are applicable for iOS, Android, and Windows).



4. Open the file **settings.json** in Notepad/Notepad++ (any standard text file editor) and make the changes to following properties as required.

As a best practice, create and maintain the backup of the original or modified file with a different name.

Prop- erty	Description
App-	Helps you identify the Innovapptive product name.
Name	

Prop- erty	Description
	<ul> <li>Conditions: Use uppercase alphabets.</li> <li>Possible Values: Based on the product, refer to the table below. For example, Mobile Work Order.</li> </ul>
Envi- ron- ment	Helps you identify the landscape that the mobile application is connected to. This value is displayed on the Login page of the mobile app. • <b>Conditions:</b> None • <b>Possible Values:</b> Development/Quality/Production.
Show- Demo- Button	<ul> <li>Set to True to display the Sample Data button on the application Login page that helps the user view the demo data. If this value is set to false, button is not displayed.</li> <li>Conditions: Use lowercase alphabets.</li> <li>Possible Values: true/false</li> </ul>
hcolor	<ul> <li>Custom header color for application. Provides the ability to customize the app screen elements, such as the header bar, to meet your corporate branding needs. Work with your appropriate branding team to identify the color that meets your enterprise palette.</li> <li><b>Tip:</b> Use the Google Hex color picker to identify the Hex color code value that needs to be set up. To find the hex color code, go to www.google.com and search for "hex color picker." Select the desired color and you will see the color code.</li> <li><b>Conditions:</b> Use the Hex color code value based on the color you would like to see on the mobile app screen elements.</li> <li><b>Possible Values:</b> As required. For example, #42c2f4</li> </ul>
Offline- Status- Color	<ul> <li>Configure the color of your choice for the status bar that is displayed on top of the screen when the device is not connected to the network.</li> <li><b>Tip:</b> Use the Google Hex color picker to identify the Hex color code value that needs to be set up. To find the hex color code, go to www.google.com and search for "hex color picker." Select the desired color and you will see the color code.</li> <li>For example, the parameter value could be configured as "OfflineStatusCol- or":"#DF264D" in the json file.</li> </ul>

Prop- erty	Description
isUn- regis- terRe- quired	Set the value as <b>False</b> to disable the unregister feature in application.
isEU- LARe- quired	Set the value as <b>False</b> to disable the EULA agreement screen in application.
Touchld	Set the value as <b>True</b> to enable the <b>Touch ID</b> feature in application.
App- Pass- Code	Set the value as <b>True</b> to enable the <b>App Passcode</b> feature in application.
Forgot- Pwd	Set the value as <b>True</b> to enable the <b>Forgot Password</b> feature in application.
Forgot- PwdLink	Set the value as <b>True</b> to display the website link to reset password.
Forgot- Pwd- Msg	Set the value as <b>True</b> to display the message to reset password.

Prop- erty	Description
Lan- guages	<ul> <li>Languages that are configured in the settings.json file are displayed to the user as a drop-down menu for selection. Additional languages can be added provided the language is available in SAP and the nec- essarytranslations are maintained.</li> <li>Syntax:</li> </ul>
	<pre>{"id":<sequencenumber>,"key":"<saplanguagecode>","value": "<languagename>"}</languagename></saplanguagecode></sequencenumber></pre>
	<ul> <li>Conditions: Use the Hex color code value based on the color you would like to see on the mobile app screen elements.</li> <li>Possible Values: Languages supported by SAP. For example, {"id":1,"key":"E","value":"English"}</li> </ul>
	<b>Note:</b> For RACE Dynamic Forms, only English language is supported.
Time- out	<ul> <li>Description &amp; Use: The application idle Timeout (in minutes). This setting allows the administrator to specify the automatic time out when apps are left idle.</li> <li>Possible Values: As required. For example, D30.</li> </ul>

5. For each environment (Development, Quality, and Production), review and update the content block in entirety.

	Note:
	Values described in the following table are case sensitive and are
	recommended to be used in the same format as mentioned in the Description
	section. All the values are mandatory.
_	

Para- meter	Description		
Server	The DNS/HostName of the SAP BTP servers, which will be used for mobile ap- plication connection. For example: scp.innovapptive.com		

Para- meter	Description
Port	<ul> <li>The application establishes the communication to the server based on the port number.</li> <li>Possible Values: 443. For example, HTTPs (SAP BTP default HTTPs port 443 and custom ports for proxy)</li> </ul>
Appli- cationID	<ul> <li>ID configured in SAP BTP and the mobile application will use it to connect to server for the registration.</li> <li>Condition: Use the same application ID as defined in SAP BTP.</li> <li>Possible Values: Based on the product, refer to the table below. For example: com.innovapptive.mworkorder.</li> </ul>
Securi- tyType	<ul> <li>Used to identify the security type configured in SAP BTP server for the application. Security types are used based on authentication mechanism/login mechanism selected for the application.</li> <li>Condition: Use the same security profile name as defined in SAP BTP. For example, Basic Authentication (SSO2), SAML Authentication (SAML) and x509 authentication(x509) mechanisms.</li> </ul>
https	<ul> <li>Used to identify the protocol type. The default value should be set to false.</li> <li>Condition: Use lowercase alphabets.</li> <li>Possible Values: true/false.</li> </ul>
Whitelist [Appli- cation- ID]	All Innovapptive applications require connection settings for RACE services and may also require other connection settings. mWorkOrder application requires connection setting for RACE, EQUIPMENT, FUNCTIONALLOCATION, and ATTACHMENT. For Example, com.innovapptive- .race, mwo.equipment, mwo.funloc and mwo.attach.
Whitelist [Store- Name]	The name Offline stores for whitelist ApplicationIDs. RACE store is common for all Innovapptive applications. mWorkOrder application requires to configure for following StoreName – RACE, EQUIPMENT, FUNCTIONALLOCATION, and ATTACHMENT.

The following screenshot shows sample **settings** file with the configuration details.

6. **ApplicationID** and **AppName** depend on the app that you configure. Use the following table to configure:

Name	APP ID	AppName
Mobile Asset Tag	com.innovapptive.massettag	MASSETTAG
Mobile Inventory	com.innovapptive.minventory	MINVENTORY
Mobile Work Order	com.innovapptive.mworkorder	MWORKORDER
RACE Dynamic Forms	com.innovapptive.racedynamicforms	RACEDYNAMICFORMS

- 7. Save the **settings.json** file.
- 8. Update the image files.

Replace the **.png** image files with your brand images. Ensure that the file format, image size, quality, resolution, and so on match the default images that are being replaced.

- 9. Compress the following files with the updated files from Part 1 & 2 into a zip file with the name **resources\_ios.zip**. Ensure that the content and filenames match.
  - App\_BG\_iPad\_Landscape.png
  - App\_BG\_iPad\_Protrait.png
  - App\_BG\_iPhone.png
  - App\_Logo.png
  - settings.json

# 5.2. Prepare and Update Resource File for SAP BTP (MWO 2009 SP03 and above releases)

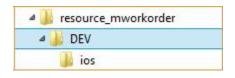
The **mWorkOrder** application resource file **resources\_mworkorder.zip** on Windows platform is used as an example to demonstrate the procedure. Do your branding changes in the zip file that is provided by Innovapptive initial deployment.

This procedure is applicable to releases MWO 2009 SP03 and above.

To prepare and update the resource file:

- 1. Download the **resources\_mworkorder\_zip** file to the local drive.
- 2. Extract the resource\_mmworkorder.zip file.

The following folder structure is displayed when you extract.



3. Navigate to the iOS folder. (Same file and settings are applicable for iOS, Android, and Windows).

4 🎉 resource_mworkorder	^					(100 million
Isource_mworkorder Isource_mworkorder Isource_mworkorder	20		1.3	3		wannen
∠ JEV		and a	2	2	Ŕ	4
		BG_iPad_La cape.png	App_BG_iPad_Pro trait.png	App_BG_iPhone. png	mWorkOrder App_Logo.png	settings.json

4. Open the file **settings.json** in Notepad/Notepad++ (any standard text file editor) and make the changes to following properties as required for MWO 2009 SP03.

As a best practice, create and maintain the backup of the original or modified file with a different name.

Prop- erty	Description
App-	Helps you identify the Innovapptive product name.
Name	<ul> <li>Conditions: Use uppercase alphabets.</li> </ul>
	<ul> <li>Possible Values: Based on the product, refer to the table below. For ex-</li> </ul>
	ample, <b>Mobile Work Order</b> .

Prop- erty	Description
Envi- ron- ment	Helps you identify the landscape that the mobile application is connected to. This value is displayed on the Login page of the mobile app. • <b>Conditions:</b> None • <b>Possible Values:</b> Development/Quality/Production.
hcolor	<ul> <li>Custom header color for application. Provides the ability to customize the app screen elements, such as the header bar, to meet your corporate branding needs. Work with your appropriate branding team to identify the color that meets your enterprise palette.</li> <li><b>Tip:</b> Use the Google Hex color picker to identify the Hex color code value that needs to be set up. To find the hex color code, go to www.google.com and search for "hex color picker." Select the desired color and you will see the color code.</li> <li><b>Conditions:</b> Use the Hex color code value based on the color you would like to see on the mobile app screen elements.</li> <li><b>Possible Values:</b> As required. For example, #42c2f4</li> </ul>
Cus- tomer- Name	Helps you identify the name of the customer. For example, Innovapptive.
Offline- Status- Color	<ul> <li>Configure the color of your choice for the status bar that is displayed on top of the screen when the device is not connected to the network.</li> <li><b>Tip:</b> Use the Google Hex color picker to identify the Hex color code value that needs to be set up. To find the hex color code, go to www.google.com and search for "hex color picker." Select the desired color and you will see the color code.</li> <li>For example, the parameter value could be configured as "OfflineStatusCol- or":"#DF264D" in the json file.</li> </ul>
isEU- LARe- quired	Set the value as <b>False</b> to disable the EULA agreement screen in application.
Online- Offline	Set the value as <b>True</b> to enable the <b>Online/Offline</b> feature in application.

Prop- erty	Description
UseDe- faultUrl	Set the value as <b>True</b> to use the default URL. The default URL is used for inter- net speed test. Android users connects to the Okla server and iOS users con- nects to the Apple sever to get the bandwidth value.
Forgot- Pwd	Set the value as <b>True</b> to enable the <b>Forgot Password</b> feature in application.
INVAM- Base- URL	Helps you to post the data in INVAM application. For example, http://in- vam-api.innovapptive.com:6001.
Ses- sion- Time- out	<ul> <li>Description &amp; Use: The user session idle timeout. This setting allows the administrator to inform the user whether the session should continue when the application left idle for some time. This configuration is applicable only for online.</li> <li>Possible Values: As required. For example, 4. Here, the value 4 represents 60 minutes (4 * 15 minutes = 60). For every 15 minutes the app notifies the user that the session is idle and after 60 minutes, it prompts the user whether to continue the session or not. When you choose to continue the session, it refreshes the application and asks you to enter the passcode.</li> </ul>
Forgot- Pwd- Msg	Set the value as <b>True</b> to display the message to reset password.
Store- Name	Helps you to identify the store name. • <b>Conditions:</b> None • <b>Possible Values:</b> WORKORDER
Store- Descrip- tion	Helps you to identify the description regarding the store name. • <b>Conditions:</b> None • <b>Possible Values:</b> General
Store- Index	Helps you to identify the index value of the store name and the order is in as- cending order. • <b>Conditions:</b> None • <b>Possible Values:</b> 1 or 2

Prop- erty	Description
Store- Type	Helps you to identify the type of the store. • <b>Conditions:</b> None • <b>Possible Values:</b> T
Lan- guages	<ul> <li>Languages that are configured in the settings.json file are displayed to the user as a drop-down menu for selection. Additional languages can be added provided the language is available in SAP and the nec- essarytranslations are maintained.</li> </ul>
	Syntax:
	<pre>{"id":<sequencenumber>,"key":"<saplanguagecode>","value": "<languagename>"}</languagename></saplanguagecode></sequencenumber></pre>
	<ul> <li>Conditions: Use the Hex color code value based on the color you would like to see on the mobile app screen elements.</li> <li>Possible Values: Languages supported by SAP. For example, {"id":1,"key":"E","value":"English"}</li> </ul>
	<b>Note:</b> For RACE Dynamic Forms, only English language is supported.
Time-	<ul> <li>Description &amp; Use: The application idle Timeout (in minutes). This set-</li> </ul>
out	ting allows the administrator to specify the automatic time out when apps are left idle.
	<ul> <li>Possible Values: As required. For example, D30.</li> </ul>

5. For each environment (Development, Quality, and Production), review and update the content block in entirety.

## Note:

Values described in the following table are case sensitive and are recommended to be used in the same format as mentioned in the Description section. All the values are mandatory.

Para- meter	Description
Server	The DNS/HostName of the SAP BTP servers, which will be used for mobile ap- plication connection. For example: scp.innovapptive.com
Port	<ul> <li>The application establishes the communication to the server based on the port number.</li> <li>Possible Values: 443. For example, HTTPs (SAP BTP default HTTPs port 443 and custom ports for proxy)</li> </ul>
Appli- cationID	<ul> <li>ID configured in SAP BTP and the mobile application will use it to connect to server for the registration.</li> <li>Condition: Use the same application ID as defined in SAP BTP.</li> <li>Possible Values: Based on the product, refer to the table below. For example: com.innovapptive.mworkorder.</li> </ul>
Securi- tyType	<ul> <li>Used to identify the security type configured in SAP BTP server for the application. Security types are used based on authentication mechanism/login mechanism selected for the application.</li> <li>Condition: Use the same security profile name as defined in SAP BTP. For example, Basic Authentication (SSO2), SAML Authentication (SAML) and x509 authentication(x509) mechanisms.</li> </ul>
https	<ul> <li>Used to identify the protocol type. The default value should be set to false.</li> <li>Condition: Use lowercase alphabets.</li> <li>Possible Values: true/false.</li> </ul>
Whitelist [Appli- cation- ID]	All Innovapptive applications require connection settings for RACE services and may also require other connection settings. mWorkOrder application requires connection setting for RACE, EQUIPMENT, FUNCTIONALLOCATION, and ATTACHMENT. For Example, com.innovapptive- .race, mwo.equipment, mwo.funloc and mwo.attach.

Para- meter	Description
[Store-	The name Offline stores for whitelist ApplicationIDs. RACE store is common for all Innovapptive applications.
Name]	mWorkOrder application requires to configure for following StoreName – RACE, EQUIPMENT, FUNCTIONALLOCATION, and ATTACHMENT.

The following screenshot shows sample **settings** file with the configuration details.



6. **ApplicationID** and **AppName** depend on the app that you configure. Use the following table to configure:

Name	APP ID	AppName
Mobile Asset Tag	com.innovapptive.massettag	MASSETTAG
Mobile Inventory	com.innovapptive.minventory	MINVENTORY
Mobile Service Order	com.innovapptive.mserviceorder	MSERVICEORDER
Mobile Shopping Cart	com.innovapptive.mshop	MSHOP
Mobile Worklist	com.innovapptive.mworklist	MWORKLIST
Mobile Work Order	com.innovapptive.mworkorder	MWORKORDER
RACE Dynamic Forms	com.innovapptive.racedynamicforms	RACEDYNAMICFORMS

#### 7. Save the **settings.json** file.

8. Compress the following files with the updated files from Part 1 & 2 into a zip file with the name **resources\_ios.zip**. Ensure that the content and filenames match.

- App\_BG\_iPad\_Landscape.png
- App\_BG\_iPad\_Protrait.png
- App\_BG\_iPhone.png
- App\_Logo.png
- settings.json

## 5.3. Use Resource File in SAP BTP

The following topics help you with uploading resource file in SAP BTP:

- Add back-end connection RACE URL and upload application help resource *(on page 55)*
- Add backend connection for Dolphin Services Integration (mAssetTag only) *(on page 56)*
- Create Application and Upload Resource File (on page 57)

# 5.3.1. Add back-end connection RACE URL and upload application help resource

To configure the RACE URL and Resource APPID on SAP BTP mobile services, get the admin authorization for SCP mobile service.

To add back end connection RACE URL and upload help resource file:

- 1. Log in to SAP BTP Account.
- 2. Click Services.
- 3. Click Mobile Services.
- 4. Click Go to Service.
- 5. Select Mobile Applications tab and click Native/Hybrid option
- 6. Select the application that you have configured.

For example, com.innovapptive.mworkorder and you will navigate to application setting page. You can configure the Assigned Features of the application.

- 7. Click the **Connectivity** option.
- 8. Select **Configuration** tab and click the **Create** option.
- 9. Enter the following:

• Mobile Destination: com.innovapptive.mworace

#### Note:

Mobile Destination name should be the same as used in the **settings.json** file.

• URL: http://Virtualhost:HTTP(s)/sap/opu/odata/INVCEC/RACE\_SRV/

#### Note:

RACE URL remains the same for all applications, such as mWorkOrder, mWorklist, mAssetTag, and mInventory.

 For com.innovapptive.mworkorder(mWorkOrder) application, multiple connection names are used for creating multiple offline stores in application.

- Mobile Destination name is mwo.funloc and URL is http://
   Virtualhost:HTTP(s)/sap/opu/odata/INVMWO/MWOFUNLOCATION\_SRV/
- Mobile Destination name is **mwo.equipment** and URL is http:// Virtualhost:HTTP(s)/sap/opu/odata/INVMWO/MWOEQUIPMENT\_SRV/
- Mobile Destination name is **mwo.attach** and URL is http://
- Virtualhost:HTTP(s)/sap/opu/odata/INVMWO/WOATTACHMENTS\_SRV/
- 10. Proxy Type: OnPremise (Cloud Connector) and click Next.
- 11. Select SSO Mechanism as Principal Propagation.
- 12. Click **Finish** and test the destination by a ping test.
- 13. Click the **Client Resources** tab.

a. Enter the Bundle Name and Version as **application\_help** and **1.0** respectively.

b. Browse and upload the resource file.

# 5.3.2. Add backend connection for Dolphin Services Integration (mAssetTag only)

Applicable only for mAssetTag product when deploying the Dolphin Invoice module.

To add backend connection for Dolphin Services Integration:

1. Select the application that you have configured.

For example, com.innovapptive.mAssetTag and you will navigate to application setting page. You can configure the Assigned Features of the application

- 2. Click the **Connectivity** option.
- 3. Select the **Configuration** tab and click **Create**.
- 4. Enter the following details
  - Mobile Destination: com.innovapptive.dolphin.pts

## Note:

Connection name should be same as used in the **settings.json** file.

- URL: http://Virtualhost:HTTP(s)/sap/opu/odata/DOL/AP\_GW\_SRV
- Proxy Type: OnPremise (Cloud Connector) and click Next.
- Select SSO mechanism as **Principal Propagation**.
- 5. Click **Save** and ping test the destination.

## 5.3.3. Create Application and Upload Resource File

Upload the resource file that you created at Prepare and Update Resource File for SAP BTP (on page 43).

To create application and upload resource file:

- 1. Select the Native/Hybrid option in SCPms home page.
- 2. Click New and enter the following details:

Con- Native fig Templates

ID com.innovapptive.massettag.resources / com.innovapptive.minventory.resources / com.innovapptive.mserviceorder.resources / com.innovapptive-.mshop.resources / com.innovapptive.mworklist.resources / com.innovapptive-.mworkorder.resources / com.innovapptive.racedynamicforms

Name MWORKORDER/MWORKLIST/MINVENTORY/MASSETTAG/MFORM

Ven- Innovapptive Inc.

dor

```
De- (Optional as required)
scrip-
tion
```

- 3. Click Save.
- 4. In the Applications Configurations page, click the **Connectivity** tab and enter the URL http(s)://virutalhost:HTTP(s)port/sap/bc/ping
- 5. Click the Security tab and select Security Configuration as None.
- 6. Click Client Resources tab and click Upload Client Resource icon.
  - a. Enter the **Bundle Name** and **Version** as **resources\_ios** and **1.0** respectively.
  - b. Browse and upload the resource file.
- 7. Click Save.
- 8. Ping and test the service.

## 5.3.4. Defining Offline Settings for Applications

To define offline settings:

- 1. In Mobile Services cockpit, navigate to Mobile Applications, Native/Hybrid.
- 2. Select an application.
- 3. In the Info tab, select Offline in the Assigned Features section and click OK.
- 4. On the **Configuration** tab of **Offline** screen, click the *icon* next to Destination name to configure the settings manually.

You can also upload the Configuration (.ini) file using the **Upload** option. Copy this content to a text editor and save the file as fit.mwo.ini.



#### | 5 - Manage Resource File in SAP BTP

max\_delta\_resends=0 [defining\_query] name=MATNRCollection is\_shared\_data=N [defining\_query] name=MeasPointCollection is\_shared\_data=N [defining\_query] name=NotificationsCollection is\_shared\_data=N [defining\_query] name=WorkOrdersCollection is\_shared\_data=N [defining\_query] name=WOTaskListCollection is\_shared\_data=N [defining\_query] name=MaterialDocListCollection is\_shared\_data=N [endpoint] name=fit.mwo.equipment prepopulate\_offline\_db=N request\_format=application/json;q=1,application/atom+xml;q=0.5 delta\_request\_format=application/atom+xml batch\_all\_defining\_queries=N case\_sensitive\_offline\_db=N offline\_db\_collation=UTF8BIN local\_change\_expiry=0 content\_id\_header\_location=mime

#### | 5 - Manage Resource File in SAP BTP

json_datetimeoffset_in_utc=Y
max_delta_resends=0
[defining_query]
name=EquipmentListCollection
is_shared_data=N
[defining_query]
name=EQUNRCollection
is_shared_data=N
[defining_query]
name=HEQUICollection
is_shared_data=N
[endpoint]
name=fit.mwo.funloc
prepopulate_offline_db=N
request_format=application/json;q=1,application/atom+xml;q=0.5
delta_request_format=application/atom+xml
batch_all_defining_queries=N
case_sensitive_offline_db=N
offline_db_collation=UTF8BIN
local_change_expiry=0
content_id_header_location=mime
allow_omitting_max_length_facet=N
json_datetimeoffset_in_utc=Y
max_delta_resends=0
[defining_query]
name=FunctionalLocCollection
is_shared_data=N
[defining_query]
name=TPLNRCollection
is_shared_data=N

5. Specify the **Endpoint properties** and click **Next**.

- 6. Specify the Endpoint Customized Properties.
- 7. Click Next.
- 8. Enter the **Client Index** parameters.
- 9. Click Next.
- 10. Enter the defining request parameters like **Name**, **Refresh Interval**, **Delta Tracking** and **Token Lifetime** in the **Defining Requests** screen.

#### For mWorkOrder Service:

Mabile Application               Defining Requests               Left Offline Configuration               Left Offline               Left Offline <th>Home</th> <th>Networkshild</th> <th>ow</th> <th></th> <th></th> <th></th> <th></th> <th>_</th>	Home	Networkshild	ow					_
Nativerhytrid     Defining Requests     +       Name     Refresh Interval (min)     Deta Tracking     Token Lifetime (min)     Stare Data     Action       SAP Modele Cards     MartineCollection     Image: Stare Data     MartineCollection     Image: Stare Data     Action       Features     MathineCollection     Image: Stare Data     Image: Stare Data     Image: Stare Data     Image: Stare Data       Destinations     Image: Stare Data     Image: Stare Data     Image: Stare Data     Image: Stare Data       Analydick     Image: Stare Data     Image: Stare Data     Image: Stare Data     Image: Stare Data       Store Data     Image: Stare Data     Image: Stare Data     Image: Stare Data     Image: Stare Data       Store Data     Image: Stare Data     Image: Stare Data     Image: Stare Data     Image: Stare Data       Store Data     Image: Stare Data     Image: Stare Data     Image: Stare Data     Image: Stare Data       Store Data     Image: Stare Data     Image: Stare Data     Image: Stare Data     Image: Stare Data       Store Data     Image: Stare Data     Image: Stare Data     Image: Stare Data     Image: Stare Data       Store Data     Image: Stare Data     Image: Stare Data     Image: Stare Data     Image: Stare Data       Store Data     Image: Stare Data     Image: Stare Data		4		Edit Offline (	Configuration			
Name     Refresh Interval (min)     Deta Tracking     Token Lifetime (min)     Share Data     Action       SAP Model Curds     MatTiN&Collection     Image: Curds     I	Mobile Applications 🗸	Defining Requests					+	
SAP Mobile Cards     MTNRCollection     Image Point Callection     Image Point Callection       Features     Notifications Collection     Image Point Callection     Image Point Callection       Destinations     Notifications Collection     Image Point Callection     Image Point Callection       Analysics     Vorko/Orders/Callection     Image Point Callection     Image Point Callection       Storings     Vorko/Orders/Callection     Image Point Callection     Image Point Callection	Native/Hybrid			Delta Tracking	Token Lifetime (min)	Share Data		
Destrutions     NotificationsCollection     Image: Collection     Image: Collection       Analysics     WorkOrdersCollection     Image: Collection     Image: Collection       Settings     WOTaskLisCollection     Image: Collection     Image: Collection	SAP Mobile Cards							
Analytics >> WorkScillection Control C	Features	MeasPointCollection					<b></b>	
Analysics         Work/Order=Collection         Image: Collection         <	Destinations	NotificationsCollection					÷.	
Settings	Analytics	WorkOrdersCollection		~			÷	
		WOTaskListCollection		~			÷	
MaterialDocListCollectik V		MaterialDocListCollect	ix .	×			8	
	Important Links					Pre	evious Next Cancel	

#### For Equipment:

Ξ	E SAP Cloud P	latform Mot	vile Services						VALLAKAS
ଜ			<b></b>		Edit Offline Con	figuration			
¢		~ (							
			Defining Requests				Share Data	+ Action	
			EquipmentListCollection	Refresh Interval (min)	Delta Tracking	Token Lifetime (min)	Share Data	action	
R		- 1	EQUNRCollection						
Ø		- 1	HEQUICollection						
		<u> </u>							Q / 1 🛓
		· >							
~		-							
		. 1							
		. 1							
		. 1							
		. 1							
		. 1							
		- 1							
ø							Previous	Next Cancel	
Ŧ									

#### For Functional Location:

Home	Networkshild	Sull					
			Edit Offline 0	Configuration			
Mobile Applications 🗸 🗸	Defining Requests					+	
Native/Hybrid	Name	Refresh Interval (min)	Delta Tracking	Token Lifetime (min)	Share Data	Action	
SAP Mobile Cards	FunctionalLocCollection			loken Electrice (min)		1 IIIIIIII	
Features	TPLNRCollection					- -	
Destinations							
Analytics							
settings							
, ooungo , ,							
Important Links					Pre	vious Next Cancel	

- 11. Click Next.
- 12. Enter request groups on the **Defining Request Groups** screen.
- 13. Click Finish.

# 6. Configure Roles and Authorization for Products

Configure roles and provide authorizations to do tasks using Innovapptive products.

The following topics help you configure roles and authorizations for innovapptive products:

- Configure SAP security roles for application users (on page 63)
- SAP Authorizations for mWorkOrder users (on page 63)
- SAP Authorizations for mInventory users (on page 69)
- SAP Authorizations for mAssetTag users (on page 75)
- User roles for RACE (on page 83)

## 6.1. Configure SAP security roles for application users

Configure security authorizations for application users and RACE Administrators.

Innovapptive applications are pre-packaged with roles for application users and RACE Administrators. Import the roles to the ECC and NetWeaver Gateway development/sandbox system using the Transports.

Assign the roles to users after importing transports. Contact the Project Manager for list of users that require the access.

#### Note:

If the transports are not imported, create users using your standard process based on the transaction and access requirements noted for each role.

Users must have a common SAP User ID setup in NetWeaver Gateway system and the backend ERP system.

## 6.2. SAP Authorizations for mWorkOrder users

Application user requires access to the following transaction codes or relevant custom transaction codes and appropriate authorizations objects to use the mWorkOrder application.

Use **SU01** transaction to assign Innovapptive pre-packaged role or enterprise relevant roles to the application user.

#### Note:

On the non-development systems (Quality, Pre-Production and Production systems), the application user needs the same access.

Role Name	Description	Transactions	Authoriza- tion Objects
ZINV_MWO_ECC	Innovapptive mWork-	IW21, IW22, IW23,IW31,	S_RFC, S_RFCACL
END_USER_R2208	Order - End User -	IW32, IW33, IW34,	
	ECC Authorizations -	IW39, IW41, IW42,	
	Release 2208	IW43, IW45, IW51,	
		IW52, IL01, IL02, IL03,	
		IE01, IE02, IE03, IK01,	
		IK02, IK03, IK11, IK13,	
		IK33, IQS1, IQS2, IQS3,	
		QA03, QA11, QA32,	
		QE03, QE11, CV03N,	
		IP03, IP10, CS02, CS03,	
		CAT2, CAT3, CATS	
		APPR_LITE	
ZINV_MWO_ECC	Innovapptive mWork-		S_RFC and S_RFCACL
RACE_ADM_R2208	Order - RACE Admin -		
	ECC Authorizations –		
	Release 2208		

#### Table 6-1 Roles for ECC System

#### Table 6-2 Roles for NetWeaver Gateway System

Role Name	Description	Authorizations
ZINV_MWO_NWG_END USER_R2208	Innovapptive mWorkOrder - End User - Gateway Autho- rizations - Release 2208	S_RFC, S_RFCACL, S_SERVICE, S_TABU_DIS, S_USER_GRP
ZINV_MWO_NWG_RACE_AD- M_R2208	Innovapptive mWorkOrder - RACE Admin - Gateway Au- thorizations - Release 2208	S_RFC, S_RFCACL, S_SERVICE, S_TABU_DIS, S_USER_GRP, / INVCEC/RA

Generate the role and use it or copy the role to appropriate enterprise naming convention, generate, and use.

## 6.2.1. Update Service authorization object for mWorkOrder

S\_SERVICE authorization object with customer system generated service value.

To update service values under S\_SERVCE:

#### 1. Go to SE16/SE16N or SE11 and open the table USOBHASH.

2. Enter this information:

#### Table 6-3 S\_SERVICE values

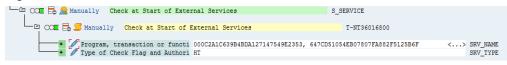
Test Status Type	HT (Hash Value for TADIR Object)
Object Type	IWSG (Gateway Service group metadata)
	<b>IWSV</b> (Gateway Business Suite Enable- ment – Service)
Object Name	/INVMWO/MWORKORDER_SRV*,
	/INVCEC/RACE_SRV*,
	/INVMWO/MWOFUNLOCATION_SRV*,
	/INVMWO/MWOEQUIPMENT_SRV*,
	/INVMWO/WOATTACHMENTS_SRV*
	/INVMWO/MWOOPERATORROUND_SRV*

Figure 6-1 USOBHASH table

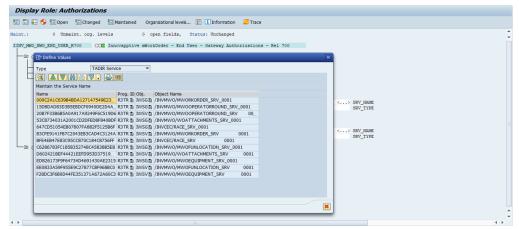
	<b>F</b>	1	el :			<b>F</b> 1 <b>F</b> 1
Name	Test	PgID	Obj.	Object Name	Type of External Service	External Service
BFE4EB47E83C95CC870C1B4C8756FF	HT	R3TR	IWSV	/INVCEC/RACE_SRV 0001		
647CD51054EB07807FA882F5125B6F	HT	R3TR	IWSG	/INVCEC/RACE_SRV_0001		
F28DC3F6B0D44FE351371A672A60C3	HT	R3TR	IWSV	/INVMWO/MWOEQUIPMENT_SRV 0001		
ED826173F9F64734D4691430AE2315	HT	R3TR	IWSG	/INVMWO/MWOEQUIPMENT_SRV_0001		
EE0833A59F955E9C27877CBF968BC0	HT	R3TR	IWSV	/INVMWO/MWOFUNLOCATION_SRV 0001		
C6286783FC1B5B35274BC45838B5E8	HT	<b>R3TR</b>	IWSG	/INVMWO/MWOFUNLOCATION_SRV_0001		
20B7F33B6B5A0A917A9249F6C519D6	HT	R3TR	IWSV	/INVMWO/MWOOPERATORROUND_SRV 0001		
15D8DAD83D3B5EBDCF0940DE2D4A34	HT	R3TR	IWSG	/INVMWO/MWOOPERATORROUND_SRV_0001		
B3CFE9141FB7C2043EB3CAD4C3124A	HT	R3TR	IWSV	/INVMWO/MWORKORDER_SRV 0001		
000C2A1C639B4BDA127147549E2353	HT	R3TR	IWSG	/INVMWO/MWORKORDER_SRV_0001		
D602421BEF44421EEFD953D37519DA	HT	R3TR	IWSV	/INVMWO/WOATTACHMENTS_SRV 0001		
53C8734031A2001CD2DFED8F840BDF	HT	R3TR	IWSG	/INVMWO/WOATTACHMENTS_SRV_0001		

3. Pick the names of the hashed services (the 30-character length alpha numerical name) and use them under S\_SERVICE - SRV\_NAME.

#### Figure 6-2 Hashed Service Name



#### Figure 6-3 Display Role Authorization



## 6.2.2. Transports for mWorkOrder roles

Import the transports into SAP ECC and GW with dependency and sequence as shown in the following tables. See Import roles using Transports *(on page 67)* to understand how to import transports.

#### Table 6-4 SAP ECC Transports

Transport	Description	Dependency
ERDK912282	Innov ECC R 2208 Mworkorder Application End User Roles	None

#### Table 6-5 SAP GW Transports

Transport	Description	Dependency
NGTK909710	Innov Gateway R 2208 mworkorder Application End user Roles	None

## 6.2.3. Import roles using Transports

To import roles using Transports into ECC and GW development/sandbox system:

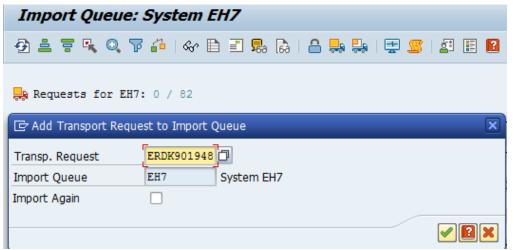
- 1. Extract the zip or .rar files that you received from Innovapptive and save the files to your local machine.
- 2. Extract and upload/copy the files to the SAP ECC & GW System Directories.
  - a. Extract the zip files and copy all co-files (files starting with 'K902\*') from software deployment package to the USR/SAP/TRANS/COFILES path on SAP ECC & GW system.
  - b. Extract the zip files and copy all the data files R902\* provided in the software deployment package to the specified path on the SAP ECC &GW system USR/ SAP/TRANS/DATA.
- 3. Log in to the SAP GW & ECC System (based on the transport being imported).
- 4. Navigate to the transaction code STMS\_Import.
- 5. Navigate to Extras, Other Requests, Add.

#### Figure 6-4 Import Queue

🔄 Queue Edit Goto Request	Extras Environment System <u>H</u> elp	_
🖉 🔽 🔻 🗧	Legend Ctrl+Shift+F4 Personal Settings Ctrl+Shift+F12	📮 🖻   😰 🖳
Import Queue: System El	Other Requests	Add
多 흔 후 및 Q 下 👍 । 삶 🗎	Activate Inactive Requests	Find in Other Groups
	Delete Imported Requests	F
Requests for EBS: 0 / 1		-

6. Enter the transport number in the **Transp. Request** field and confirm by pressing the **ENTER** key (or click the green-colored icon) to attach transports to the import queue.

Figure 6-5 Add Transport Request to Import Queue



- 7. Click **Yes** to proceed to the next step.
- 8. Select the transport request that needs to be imported.
- 9. Click the **Truck** icon (highlighted by red in the screenshot).

Figure 6-6 Truck icon

5							
Impor	Import Queue: System EH7						
2) 🚢 🐨 🧏 🔍 🔽 🖆 🕼 🔚 🔜 🔜 🔚 🔛 🔛 💷 💷 💷							
	sts for EH7: ( st ERDK901948	) / 1		01.08.2016 14:	27:35		
Number	Request	RC	Owner	Short Text	St		
83	ERDK901948	۵	E5000103		Т <u>к</u>		

- 10. Enter the target client number in Target Client field.
- 11. Select Leave Transport Request in Queue for Later Import and Ignore Invalid Component Version check boxes.
- 12. Click Yes in the confirmation screen.

#### Note:

If you face any issues/errors while importing the Transports, send the log files with screenshots and details of the error to your Innovapptive SAP Basis team contact assigned to your project.

## 6.3. SAP Authorizations for mInventory users

Application user requires access to the following transaction codes or relevant custom transaction codes and appropriate authorizations objects to use the mInventory application.

Use **SU01** transaction to assign Innovapptive pre-packaged role or enterprise relevant roles to the application user.

## Note:

On the non-development systems (Quality, Pre-Production and Production systems), the application user needs the same access.

#### Table 6-6 Roles for ECC System

Role Name	Description	Transactions	Authoriza- tion Objects
ZINV_MIM_ECC END_USER_R2009	mInventory - End User - ECC Authoriza- tions - Release 2009	MMBE, LX02, MIGO, MB1C, MB1A, HUMO, LT12, VL06O, VL02N, LT03, VL06I, HUIMV03, HUINV05, MI04, MI07, LI11N, LI20, LT10 & MB1B, ML81N, MI09	S_RFC, S_RFCACL
ZINV_MIM_ECC RACE_ADM_R2009	mInventory - RACE Admin - ECC Autho- rizations - Release 2009		S_RFC, S_RFCACL

#### Table 6-7 Roles for NetWeaver Gateway System

Role Name	Description	Authorizations
ZINV_MIM_NWG_END USER_R2009	mInventory - End User - Gateway Authorizations - Re- lease 2009	S_RFC, S_RFCACL, S_SERVICE, S_USER_GRP & S_TABU_DIS
ZINV_MIM_NWG_RACE_AD- M_R2009	mInventory - RACE Admin - Gateway Authorizations – Re- lease 2009	S_RFC, S_RFCACL, S_SERVICE, S_TABU_DIS, S_USER_GRP, / INVCEC/RA

#### Table 6-8 Roles for RLM System

Role Name	Description	Transactions	Authorizations
ZINV_MIM_RLM END_USER_R2009	mInventory - End User - RLM Authoriza- tions - Release 2009	/NSCWM/PRDI,O3O PACK01,O3O PACK03,O3O_PACK05	S_RFC, S_RFCACL
ZINV_MIM_RLM RACE_ADM_R2009	mInventory - RACE Admin - RLM Autho- rizations - Release 2009		S_RFC, S_RFCACL

#### Table 6-9 Roles for EWM Authorizations

Role Name	Description	Transactions	Authorizations
ZINV_MIM_EWM END_USER_R2009	mInventory - End User - EWM Autho-	/SCWM/MATI	S_RFC, S_RFCACL
	rizations - Release	/SCWM/TODLV_I	
	2009	/SCWM/PRDI	
		/scwm/mon	
		/SCWM/TODLV_M	
		/SCWM/TODLV_O	
		/SCWM/PRDO	
		SMQ1	
		SMQ2	
		/scwm/idn	
		/SCWM/TODLV_T	
		/SCWM/PRFIXBIN	
		/SCWM/PRBIN	
		/SCWM/TO_CONF	

Role Name	Description	Transactions	Authorizations		
		/SCWM/PACK			
		/SCWM/LOAD			
		/scwm/unload			
		/scwm/adhu			
		/SCWM/PI_PROCESS			
ZINV_MIM_EWM RACE_ADM_R2009	mInventory - RACE Admin - EWM Autho- rizations - Release 2009		S_RFC, S_RFCACL		

Table 6-9 Roles for EWM Authorizations	(continued)
--	-------------

Generate the role and use it or copy the role to appropriate enterprise naming convention, generate, and use.

## 6.3.1. Update Service authorization object for mInventory

Update the system specific S\_SERVICE authorization object with customer system generated service value.

To update service values under S\_SERVCE:

#### 1. Go to **SE16/SE16N** or **SE11** and open the table **USOBHASH**.

2. Enter this information:

#### Table 6-10 S\_SERVICE values

Test Status Type	HT (Hash Value for TADIR Object)
Object Type	IWSG (Gateway Service group metadata)
	<b>IWSV</b> (Gateway Business Suite Enable- ment – Service)
Object Name	/INVMIM/MINVENTORY_ <b>2</b> _SRV*,

/INVCEC/RACE\_SRV\*,

Figure 6-7 USOBHASH table

 Table: USOBHASH Displayed Fields: 6 of 7 Fixed Columns: [2] List Width 0250						
NAME	TYPE	PGMID	OBJECT	OBJ_NAME	SERVICE_TYPE	
E72B118C808CE6DBD3F1443CD8275A 0D617E64EC8B9891CE615BF4F640E5 647CD51054EB07807FA882F5125B6F BFE4EB47E83C95CC870C1B4C8756FF	HT HT	R3TR R3TR R3TR R3TR	IWSG IWSV IWSG IWSV	/INVMIM/MINVENTORY_2_SRV_0001 /INVMIM/MINVENTORY_2_SRV 0001 /INVCEC/RACE_SRV_0001 /INVCEC/RACE_SRV 0001		

3. Pick the names of the hashed services (the 30-character length alpha numerical name) and use them under S\_SERVICE - SRV\_NAME.

#### Figure 6-8 Hashed Service Name

COE 🔁 🧟 Manually Check at Start of External Services	S_SERVICE	
COE 🗟 写 Manually Check at Start of External Services	T-NT36016900	
<ul> <li>Program, transaction or functi 647CD51054EB07807FA882F5125B6F, BFE4E</li> <li>Type of Check Flag and Authori HT</li> </ul>		SRV_NAME SRV_TYPE

#### Figure 6-9 Change Role Authorization

C Authorizations	<u>E</u> dit <u>G</u> oto Utilit	tie <u>s</u> En <u>v</u> ironment S	zstem <u>H</u> elp					
0	▼ « 🔚 ]		61000					
Change Ro	ole: Authorizatio	ons						
12 12 🛃 😏	📅 🗟 Selection criteria	a 🖶 Manually 🛅 O	pen ! 🔃 Change	ed 🛅 Maintained	Organizational leve	els 匪 🚺 Information	🖵 Trace	
Maint.:	0 Unmaint. org. ]	levels 0	open fields,	Status: Unchange	ed			
ZINV_MIM_NWG_F	RACE_ADM_R50 O	C Innovapptive mIr	ventory - RAC	E Admin - Gateway	Authorizations	- Rel 5.0		
- COE Ma	anually Cross-appl	lication Authorizati	on Objects		AAAB			
	E B & Manually E B & Manually E B & Manually	Authorization Check Authorization Check	for RFC Acce for RFC User	ss (e.g. Trusted Sys	stem) S_RF	fC FCACL		
		Check at Start of H	xternal Servi	ces	S_SE	IRVICE		
	🖻 Define Values		_					
1	Type	TADIR Service					<> SRV_NAME	
				Technical Name Full A	Authorization		SRV_TYPE	
	Maintain the Service							
	Name			ct Name				
	E72B118C808CE6DB	D3F1443CD827R3TR	IWSG /INV	MIM/MINVENTORY_2_	SRV_0001		A	
	0D617E64EC8B9891	CE615BF4F640E5 R3TR	IWSV /INV	MIM/MINVENTORY_2_	SRV 0001		<b>T</b>	
	647CD51054EB0780	7FA882F5125B6F R3TR	IWSGE /INV	CEC/RACE_SRV_0001				
		870C1B4C8756FF R3TR			0001			
		R3TR						
		R3TR					44	
	_	R3TR						
		R3TR						
		R3TR						
		R3TR						
		R3TR						
		R3TR	 8 8					
		R3TR	ē ē					
		R3TR	8 8				A	
+ >		0270	<b>3</b> ', <b>3</b> ',				T	

## 6.3.2. Transports for mInventory roles

Import the transports into SAP ECC and GW with dependency and sequence as shown in the following tables. See Import roles using Transports *(on page 67)* to understand how to import transports.

#### Table 6-11 SAP ECC Transports

Transport	Description	Dependency
ERDK912041	INNOV ECC R 2206 Minventory Application End User Roles	None

#### Table 6-12 SAP GW Transports

Transport	Description Dependency	
NGTK909543	Innov Gateway R 2206 Min- ventory Application End User Roles	None

#### Table 6-13 SAP RLM Transports

Transport	Description	Dependency
ЕС7К900231	INNOV:RLM: R 2206 mInvento- ry Application End User Roles	None

#### Table 6-14 SAP EWM Transports

Transport	Description Dependency	
H18K900227	INNOV:EWM: R 2206 mInven- tory Application End User Roles	None

## 6.3.3. Import roles using Transports

To import roles using Transports into ECC and GW development/sandbox system:

- 1. Extract the zip or .rar files that you received from Innovapptive and save the files to your local machine.
- 2. Extract and upload/copy the files to the SAP ECC & GW System Directories.
  - a. Extract the zip files and copy all co-files (files starting with 'K902\*') from software deployment package to the USR/SAP/TRANS/COFILES path on SAP ECC & GW system.
  - b. Extract the zip files and copy all the data files R902\* provided in the software deployment package to the specified path on the SAP ECC &GW system USR/ SAP/TRANS/DATA.

- 3. Log in to the SAP GW & ECC System (based on the transport being imported).
- 4. Navigate to the transaction code **STMS\_Import**.
- 5. Navigate to Extras, Other Requests, Add.

Figure 6-10 Import Queue

도 Queue <u>E</u> dit <u>G</u> oto <u>R</u> equest	Extras Environment System Help	_
🖉 🔽 🗸 🦷	Legend Ctrl+Shift+F4	
	Personal Settings Ctrl+Shift+F12	
Import Queue: System El	Other Requests	<u>A</u> dd
🗿 🛓 🐺 🔍 🖓 🖆   🗞 🗎	Activate Inactive Requests	Find in Other Groups
Delete Imported Requests		
Requests for EBS: 0 / 1		_

6. Enter the transport number in the **Transp. Request** field and confirm by pressing the **ENTER** key (or click the green-colored icon) to attach transports to the import queue.

Figure 6-11 Add Transport Request to Import Queue

Import Queue:	System EH7
🔁 🚢 🗮 🔍 🤊	। 🕼 🖹 📰 🞭 🗞 । 合 🛼 🚑 । 🚍 🖾 🖺 🛽
Requests for EH7	': 0 / 82
🖻 Add Transport Requ	est to Import Queue
Transp. Request	ERDK901948
Import Queue	EH7 System EH7
Import Again	

- 7. Click **Yes** to proceed to the next step.
- 8. Select the transport request that needs to be imported.
- 9. Click the **Truck** icon (highlighted by red in the screenshot).

#### Figure 6-12 Truck icon

0					
Impor	Import Queue: System EH7				
<u> 9</u> = 1	r 🔍 🔍 🖓 i	<mark>1</mark> 0   6	êr 🗎 📰 晃 🕅		
	sts for EH7: ( st ERDK901948			01.08.2016 14:	27:35
Number	Request	RC	Owner	Short Text	St
83	ERDK901948	۵	E5000103		TÍ.

- 10. Enter the target client number in Target Client field.
- 11. Select Leave Transport Request in Queue for Later Import and Ignore Invalid Component Version check boxes.
- 12. Click **Yes** in the confirmation screen.

#### Note:

If you face any issues/errors while importing the Transports, send the log files with screenshots and details of the error to your Innovapptive SAP Basis team contact assigned to your project.

## 6.4. SAP Authorizations for mAssetTag users

Application user requires access to the following transaction codes or relevant custom transaction codes and appropriate authorizations objects to use the mAssetTag application.

Use **SU01** transaction to assign Innovapptive pre-packaged role or enterprise relevant roles to the application user.

#### Note:

On the non-development systems (Quality, Pre-Production and Production systems), the application user needs the same access.

Module	T-code
Display Asset	AS02, AS03
Add Asset	/INVMAT/COCKPIT
Goods Receiving	MIGO

#### Table 6-15 SAP Transaction Codes for mAssetTag

Table 6-16 mAssetTag ECC Authorizations

User	Authorization Object	Authorizations
	S_RFC	<ul> <li>ACTVT = 16</li> <li>RFC_TYPE = FUGR, FUNC</li> <li>RFC_NAME = /INVMAT/*, /INVCEC/*, / INV*</li> </ul>
mAssetTag End User	S_TABU_DIS	• ACTVT = 03 • DICBERCLS = IW*
	S_RFCACL	• ACTVT = 16 • RFC_EQUSER = Y
	S_RFC	<ul> <li>ACTVT = 16</li> <li>RFC_TYPE = FUGR, FUNC</li> <li>RFC_NAME = /INVMAT/*, /INVCEC/*, / INV*</li> </ul>
Asset Admin User	S_TABU_DIS	• ACTVT = 03 • DICBERCLS = IW*
	S_RFCACL	• ACTVT = 16 • RFC_EQUSER = Y
RACE Admin User	S_RFC	<ul> <li>ACTVT = 16</li> <li>RFC_TYPE = FUGR, FUNC</li> <li>RFC_NAME = /INVMAT/*, /INVCEC/*, / INV*</li> </ul>

User	Authorization Object	Authorizations
	S_RFCACL	• ACTVT = 16 • RFC_EQUSER = Y

#### Table 6-16 mAssetTag ECC Authorizations (continued)

#### Table 6-17 mAssetTag NetWeaver Gateway Authorizations

User	Authorization Object	Authorizations
	S_RFC	<ul> <li>ACTVT = 16</li> <li>RFC_TYPE = FUGR, FUNC</li> <li>RFC_NAME = /INVMAT/*, /INVCEC/*, / INV*, /IWBEP/*, ALFA*, ARFC*, BAPT*, EBNU*, MEWF, MEWQ, RHW1, SCVU, STXD, SWRR</li> </ul>
mAssetTag End User	S_TABU_DIS	• ACTVT = 03 • DICBERCLS = IW*
	S_USER_GRP	• ACTVT = 03 • CLASS = *
	S_RFCACL	• ACTVT = 16 • RFC_EQUSER = Y
Asset Admin User	S_RFC	<ul> <li>ACTVT = 16</li> <li>RFC_TYPE = FUGR, FUNC</li> <li>RFC_NAME = /INVMAT/*, /INVCEC/*, / INV*, /IWBEP/*, ALFA*, ARFC*, BAPT*, EBNU*, MEWF, MEWQ, RHW1, SCVU, STXD, SWRR</li> </ul>

User	Authorization Object	Authorizations
	S_TABU_DIS	• ACTVT = 03 • DICBERCLS = IW*
	S_USER_GRP	• ACTVT = 03 • CLASS = *
	S_RFCACL	• ACTVT = 16 • RFC_EQUSER = Y
	S_USER_GRP	• ACTVT = 03 • CLASS = *
RACE Admin User	S_RFC	<ul> <li>ACTVT = 16</li> <li>RFC_TYPE = FUGR, FUNC</li> <li>RFC_NAME = /INVMAT/*, /INVCEC/*, /IW-BEP/*, ALFA*, ARFC*, BAPT*, EBNU*, MEWF, MEWQ, RHW1, SCVU, STXD, SWRR</li> </ul>
	S_TABU_DIS	• ACTVT = 03 • DICBERCLS = IW*
	S_RFCACL	• ACTVT = 16 • RFC_EQUSER = Y

Table 6-17 mAssetTag NetWeaver Gateway Authorizations (continued)

## 6.4.1. Update Service authorization object for mAssetTag

Update the system specific S\_SERVICE authorization object with customer system generated service value.

To update service values under S\_SERVCE:

## 1. Go to **SE16/SE16N** or **SE11** and open the table **USOBHASH**.

2. Enter this information:

#### Table 6-18 S\_SERVICE values

Test Status Type	HT (Hash Value for TADIR Object)
Object Type	IWSG (Gateway Service group metadata)
	<b>IWSV</b> (Gateway Business Suite Enable- ment – Service)
Object Name	/INVCEC/* and /INVMAT/*

#### Figure 6-13 USOBHASH table

Тур	e TADIR Service		•		
	🕄 🔁 🗄 🔁 🛗 🛗 🎲 🏹 🖕 🌐 🖽 🛛 Technical Name Full Authorization				
	Maintain the Service Name				
	Name	Prog. ID	Obj.	Object Name	
	2066400603E7C39FA9AAAD1C3831	R3TR 🖹	IWSV 🖹	/INVMAT/MASSETTAG_2_SRV 0001	
	39FEDFD28698D1A06E6137BAC440	R3TR 🖹	IWSG 🖺	/INVMAT/MASSETTAG_2_SRV_0001	
	647CD51054EB07807FA882F5125B6F	R3TR 🗎	IWSG 🖹	/INVCEC/RACE_SRV_0001	
	BFE4EB47E83C95CC870C1B4C8756FF	R3TR 🖹	IWSV 🖹	/INVCEC/RACE_SRV 0001	
		DOTD Ph	<b>7</b> 1		

#### Figure 6-14 USOBHASH table



3. Pick the names of the hashed services (the 30-character length alpha numerical name) and use them under S\_SERVICE - SRV\_NAME.



4. Authorization Object: /INVCEC/RA with the authorization: ACTVT = 01, 02, 03, 16

#### Figure 6-16 Hashed Service Name

0	
COM Manually RACE Access Control Class	ZINV
🗆 🖂 🖓 Manually RACE Access Control Object	/INVCEC/RA
COE COE Manually RACE Access Control Object	T-N520001700
Activity 01, 02	, 03, 16 ACTVT

## 6.5. SAP Authorizations for RACE Dynamic Forms users

Application user requires access to the following transaction codes or relevant custom transaction codes and appropriate authorizations objects to use the RACE Dynamic Forms application.

Use **SU01** transaction to assign Innovapptive pre-packaged role or enterprise relevant roles to the application user.

Note:

On the non-development systems (Quality, Pre-Production and Production systems), the application user needs the same access.

#### Table 6-19 Roles for ECC System

Role Name	Description	Transactions	Authoriza- tion Objects
ZINV_RDF_ECC END_USER_R2203	Innovapptive RACE Dynamic Forms - End	/INVMGO/DOCFORM	S_RFC, S_RFCACL
	User - ECC Authoriza- tions - Release 2203		

Role Name	Description	Transactions	Authoriza- tion Objects
ZINV_RDF_ECC RACE_ADM_R2203	RACE Dynamic Forms - RACE Admin - ECC Authorizations - Re- lease 2203		S_RFC and S_RFCACL

#### Table 6-19 Roles for ECC System (continued)

#### Table 6-20 Roles for NetWeaver Gateway System

Role Name	Description	Authorizations
ZINV_RDF_NWG_END USER_R2203	RACE Dynamic Forms - End User - Gateway Authoriza- tions - Release 2203	S_RFC, S_RFCACL, S_SERVICE, S_USER_GRP
ZINV_RDF_NWG_RACE_AD- M_R2203	RACE Dynamic Forms - RACE Admin - Gateway Authoriza- tions - Release 2203	S_RFC, S_RFCACL, S_SERVICE, S_TABU_DIS, S_USER_GRP, / INVCEC/RA

Generate the role and use it or copy the role to appropriate enterprise naming convention, generate, and use.

## 6.5.1. Update Service authorization object for RACE Dynamic Forms

Update the system specific S\_SERVICE authorization object with customer system generated service value.

To update service values under S\_SERVCE:

#### 1. Go to **SE16/SE16N** or **SE11** and open the table **USOBHASH**.

2. Enter this information:

#### Table 6-21 S\_SERVICE values

Test Status Type	HT (Hash Value for TADIR Object)
Object Type	IWSG (Gateway Service group metadata)
Object Name	/INVCEC/RACE_SRV*,

Figure 6-17 USOBHASH table

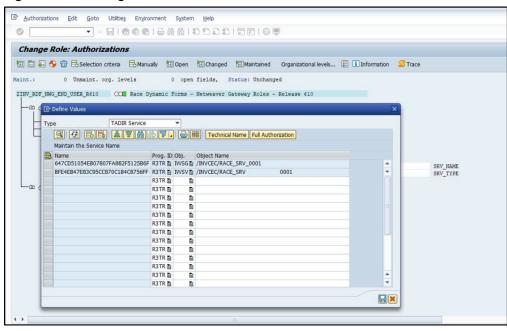
Тур	e TADIR Service		•		
	🕄 🚱 😓 🔁 🖍 🟠 🔽 📄 🌐 🖽 Technical Name Full Authorization				
	Maintain the Service Name				
	Name	Prog. ID	Obj.	Object Name	
	647CD51054EB07807FA882F5125B6F	R3TR 🖹	IWSG 🖹	/INVCEC/RACE_SRV_0001	
	BFE4EB47E83C95CC870C1B4C8756FF	R3TR 🖹	IWSV 🖹	/INVCEC/RACE_SRV 0001	

3. Pick the names of the hashed services (the 30-character length alpha numerical name) and use them under S\_SERVICE - SRV\_NAME.

Figure 6-18 Hashed Service Name

Check at Start of Exte	rnal Services	S_SERVICE	
🗆 🖂 🔁 🚾 Manually 🛛 Check at Start of 🔅	External Services	T-NT36023100	
🔸 🖉 Program, transaction or functi	647CD51054EB07807FA882F5125B6F,	BFE4EB47E83C95CC870C1B4C8756FF	SRV_NAME
<ul> <li>* 🖉 Type of Check Flag and Authori</li> </ul>	HT		SRV_TYPE

#### Figure 6-19 Change Role Authorization



## 6.5.2. Transports for RACE Dynamic Forms roles

Import the transports into SAP ECC and GW with dependency and sequence as shown in the following tables. See Import roles using Transports *(on page 67)* to understand how to import transports.

#### Table 6-22 SAP ECC Transports

Transport	Description	Dependency
ERDK911856	INNOV:ECC: R 2203 RACE DF	None
	Application End User Roles	

#### Table 6-23 SAP GW Transports

Transport	Description	Dependency
NGTK909453	INNOV:GW: R 2203 RACE DF Application End User Role	None

## 6.6. User roles for RACE

Following set of user roles are available for RACE application

#### Table 6-24 RACE User Roles

Role	Description	Access
ZINV_RACE_ADMIN_ACCESS	RACE Admin Access Role	RACE Administration
ZINV_RACE_DISPLAY_ACCESS	RACE Display Access Role	View only access to RACE configuration
ZINV_RACE_FULL_ACCESS	RACE Full Access Role	Complete access to RACE (Super)
ZINV_RACE_LIMITED_ACCESS	RACE Limited Access Role	Limited access to RACE fea- tures