Post-Install or Post-Upgrade Configurations Guide 2505

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*TM.

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

Product Version: 2505

Release Date: 07 May 2025

Published Date: 07 May 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*TM.

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 | 22 |
| 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 reso | ource55 |
| 5.3.2. Add backend connection for Dolphin Services Integration (mAssetTag | 9 |
| only) | 56 |
| 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 | 63 |
| 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 | 69 |
| 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 | |
| 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 | Configure HTTP/HTTPs Authentication (on page 10) Configure SAML Authentication (on page 15) Integrate SAP BTP with Azure AD (on page 29) |
| 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> |

| Table 2-1 Tasks for SMP Configurations after Ir | nstalling Innovapptive Products |
|---|---------------------------------|
| | 1 |

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 | Туре | 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@mte | | | | | s0015864207@interna | Il innovapptive.com |
|----------|-----|---|---|-------------------|-------------------|------------|--------|---------------------|---------------------|
| ක | | | Native/ | Hybrid | | | | | |
| ٢ | | ~ | | Native/Hybrid | | | | | |
| | | | | | New Ap | pplication | | | |
| | | | | | | | | | 4 |
| 48 | | | | Config Templates: | Native | | ~ | _ | î↓ |
| 0 | | | | *ID: | scp.test.mwo | | | C+0530) | |
| 35 | | | | *Name: | scp.test.mwo | | | | |
| °0 | | | | Description: | | | | - 60 | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | Vendor: | Innovapptive Inc. | | | | |
| | | | | | | | Save | Cancel | |
| | | | | | | | | Guncer | |
| | | - | s4h.m | wt.res | s4h.mwi.res | innov | 2018-0 | 8-31 17:24 | |
| C | | | s4h.m | lim | s4h.mim | innov | 2018-0 | 8-31 16:04 | |
| Ŧ | | | s4h.m | im.res | s4h.mim.res | innov | 2018-0 | 8-31 15:50 | |

6. Click **Save**.

Figure 3-3 Application Details

| | SAP | Mobile Service for Development and Operations | s0015864207@internal.innovapptive.c |
|----|---------------------|--|-------------------------------------|
| | Home | Native/Hybrid / scp.test.mwo | |
| | Mobile Applications | ຽດງ scp.test.mwo(scp.test.mwo) | |
| | Native/Hybrid | Duble Evront Dubleh to Discovery Service Lock | |
| | SAP Mobile Cards | | |
| 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 | 🗹 ОК > |
| | | Description: | 🗹 ок > |
| | | sample test Vendor % Connectivity Innovantive Inn | Configuration |
| | | °₂ Offline | 🗹 ок > |
| | | 🖂 Push Notification | 🗹 ок > |
| | Important Links | Security | 🗹 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.c | | | | | ive.com | | |
|------------|---------------------|---|---|------------------------------|-----|-----------------|------------|-------------------------------------|--------------|----|
| 命 | Home | | Native/Hybrid / scp.test.mw | / Connectivity | | | | | | |
| 0 | Mobile Applications | ~ | ζόζ Connectivity | | | | | | | |
| | Native/Hybrid | | Remove from Application | | | | | | | |
| | SAP Mobile Cards | | remore non repression | | | | | | | |
| 9 8 | Features | | Continuation Info | | | | | | | |
| 0 | Destinations | - | | | | | | | | |
| 35 | Analytics | > | | | | | | | () + | ↑Ļ |
| ° | Settings | > | Name | Platform Destination Name | URL | | Proxy Type | SSO Mechanism/Authenticatio n | Actions | |
| | | | | | | No Destinations | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | - | | | | | | | | |
| e | Important Links | | | | | | | | | |
| ₫¢ | 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- | http(s):// <gw_system_host>:<http(s)_port>/sap/opu/oda-</http(s)_port></gw_system_host> |
| Order | ta/INVMSO/MSERVICEORDER_SRV/ |
| 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 BTP 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
- BTP 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 Trust Relationships | Display | | | | |
| Claims Provider Trusts | | | | | |
| Relying Party Trusts | HANA I | | | | |
| 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 BTP 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 | | | | | _ <u>5</u> × |
| (= =) 🖄 🖬 🔢 🖬 | | | | | |
| AD F5 2.0 | Relying Party Trusts | | | | Actions |
| E Service | Display Name | Enabled | Identifier | | Relying Party Trusts |
| Certificates | HCPTRIAL_\$0015864207 | Yes | https://hanatrial.ondemand.com/s00 | | Add Relying Party Trust |
| Claim Descriptions | | | | | View 🕨 |
| Claims Provider Trusts | | | | | New Window from Here |
| Relying Party Trusts | | | | | Refresh |
| Attribute Stores | | | | | P Help |
| | | | | | HCPTRIAL_50015864207 |
| | | | | | Update from Federation Metadata |
| | | | | | Edit Claim Rules |
| | | | | | Disable |
| | | | | | Properties |
| | | | | | 🔀 Delete |
| | | | | | 👔 Help |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | 1 | | |] | |

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 | | × |
|-----------------------------------|---|---|-------------------------|
| You c which issued Claim | can configure this rule to send the v n to extract LDAP attributes. Specif d from the rule. rule name: | values of LDAP attributes as claims. Select an attribute str y how the attributes will map to the outgoing claim types t | ore from hat will be |
| att | | | |
| Rule | template: Send LDAP Attributes as | Claims | |
| Attribu | ute store: | | |
| Activ | e Directory | • | |
| 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 |
|-------------------------|-----|
|-------------------------|-----|

| \$ | Add Transfo | rm Claim Rule Wizard | × |
|---|--|---|---|
| Configure Rule | | | |
| Configure Rule Steps Choose Rule Type Configure Claim Rule | You can configure this rule to r also map an incoming claim va outgoing claim type and wheth Claim rule name: Send Given Name Rule template: Transform an In Incoming claim type: Incoming name ID format: Outgoing claim type: Outgoing name ID format: • Pass through all claim value Replace an incoming claim Incoming claim value: Outgoing claim value: | nap an incoming claim type to an outgoing clai lue to an outgoing claim value. Specify the inc er the claim value should be mapped to a new incoming Claim Given Name Unspecified Name ID Common Name es value with a different outgoing claim value | m type. As an option, you can oming claim type to map to the claim value. |
| | New e-mail suffix: | Example: fabrikam.com | 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 SAP BTP.

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 Helpdori 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 | | | Ø | 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 | B |
| b70068d2c:yze | yze | HANA | \otimes | B |
| portal:nwc | nwc | JAVA | \otimes | B |
| services:dispatcher | dispatcher | JAVA | \odot | Ð |
| 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 | Туре | Vendor | Security Con- figuration |
|---------|-------------------|---------------|------|----------|-----------------------------|
| mAsset- | com.innovapptive- | Mobile Asset | Na- | Inno- | Basic |
| Tag | .massettag | Tag | tive | vapptive | |
| mInven- | 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 | d Operation | s | | s00158642 | 07@internal.innov | rapptive.com |
|----------|-----|---|---------|-------------------|---------|-----------------------|-------------|-------|-------|-------------|-------------------|--------------|
| â | | | Native/ | Hybrid | | | | | | | | |
| ٢ | | ~ | | Native/Hybrid | | | | | | | | |
| | | | | | | New Ap | plication | | | | | |
| | | | | | | | | | | | | |
| 48 | | | | Config Templates: | Native | | | | ~ | | | îĻ |
| 0 | | | | *iD: | scp.tes | t.mwo | | | | | C+0530) | |
| 35 | | | | *Name: | scp.tes | t.mwo | | | | | | |
| 80 | | | | Description: | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | Vendor: | Innova | pptive Inc. | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | Save | Cancel | | |
| | | | | | | s4h.mwl.res | | innov | | 08-31 17:24 | | |
| e | | | s4h.m | im | | s4h.mim | | innov | 2018- | 08-31 16:04 | | |
| ₽ | | | 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 Business Technology 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 |
|------------|---------------------|--|-----------------------------------|
| | Home | Native/Hybrid / scp.mim | |
| | Mobile Applications | ၄၀၃ scp.mim(scp.mim) | |
| | Native/Hybrid | Delete Evand Publish to Discovery Service | |
| | SAP Content to Go | | |
| Ķ ŝ | Features | | |
| | Destinations | Into APIs User Registrations Usage Analytics Blocked Users | |
| | Analytics > | Application Details Assigned Features | + |
| °œ | Settings > | ID: Name | State |
| | | scp.mim g ⁶ Access Control | ⊠ок > |
| | | Name: scp.mim ଚୌ Ctient Policies | ⊠ок → |
| | | Description: 2 Client Resources | С ок > |
| | | mInventory & Connectivity | Г ок > |
| | | Vendor: % Offline | С ок > |
| | | Push Notification | Г ок > |
| | Important Links | B Security | 🗹 ок > |
| | Legal Information | | |

Figure 3-14 Application Details

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

| | , | | | |
|----|---------------------|---|---------------------------------|--------------|
| ≡ | SAP | Mobile Service for Development and Opera | tions s0015864207@internal.inno | ovapptive.co |
| ଜ | Home | Native/Hybrid / scp.mim / Client Policies | | |
| ٩ | Mobile Applications | Client Policies | | |
| | Native/Hybrid | | | |
| | SAP Content to Go | Save Reset Remove from Application | | |
| 43 | Features | | | |
| 0 | Destinations | Configuration Info | | |
| 35 | Analytics | Passcode Policy | Log Policy | |
| ° | Settings | Enable Passcode Policy: Expiration Time Frame: Days Minimum Length: 8 | Enable Client Log Upload: | |
| | | Retry Limit: 10 | | |
| | | 0 | Usage Report Policy | |
| | | Lock Timeout: | Enable Usage Report Policy: | |
| | | 300 Seconds | | |
| | | Passcode Properties: | | |
| в | Important Links | Feature Restriction Policies (8) | | E. |
| ÷ | 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 contin- ue 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 Business Technology Platform can single sign into the application using the Introduction to the Access Panel.

Before proceeding, ensure you have:

- Azure AD subscription
- Business Technology 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 |
| | Subscriptions | Predictive Service | SAP Smart Business Service | Data Management |
| I Ç | 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 |
| | 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 | | |
|--|--|--|
| 📫 Mobile Services, consumers | Nobile Services, preview | 📫 Mobile 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.

| | IN SEast 🗸 / 器 Innovapptive Inc. 🗸 / 営 Innovappti | ve Inc. 🗸 / 🎼 D |
|----------------------|--|-----------------|
| ු ^ණ 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 | nut. |
| | 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 BTP.
- 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: BTPMS
 - b. **Description**: Business Technology Platform

Figure 4-1 SSL Client Identities

| | Display V | iew "SSL Client Identities of System": Ove | erview |
|---|----------------|--|----------|
| 6 | » 🖪 🖪 🖥 | 1 | |
| | SSL Client Ide | ntities of System | |
| | Identity | Description | |
| | ANONYM | SSL Client (Anonymous) | * |
| | DFAULT | SSL Client (Standard) | _ |
| | SCPMS | SAP Cloud Platform | |
| | WSSE | WSSE Web Service Security Test | 44 |
| | | | |
| | | | |
| | | | |

- 4. Navigate to the **STRUST** screen.
- 5. Right-click on SSL Client Business Technology 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 | | X |
|--------------|-----------------------------------|---|
| Name | NGT SSL client SAP Cloud Platform | |
| Org. (Opt) | 10020732638 | |
| Comp./Org. | SAP Web AS | |
| Country | | |
| CA | O=SAP Trust Community, C=DE | 1 |
| 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 | | |
|--|----------------------|---|
| 1 the second sec | | |
| System PSE SNC SAPCryptolb | Subject | (Self-Signed) |
| SSL Server's Standard SSL server's Standard SSL client SSL Client (Anonymo SSL client SSL Client (Standar SSL client SAP Cloud Platform SSL client SAP Cloud Platform SSL client WSSE Web Service Se WS Security Standard WS Security Other System Encry | Certificate List | Subject |
| WS Security WS Security Keys SMIME Standard General Standard SF File SSF Collaboration Integration SSF SAML2 Service Provider - E SSF SAML2 Service Provider - S | Certificate | Password |
| Image: SSF Logon Ticket | 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 |
| | er qa | Add to Certificate List |

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

| RFC Destinatio | n IWBEP_ODATA_OD_PUSH |
|--|--|
| connection Test 😚 | |
| RFC Destination | IWBEP_ODATA_OD_PUSH G HTTP Connection to External Serv Description |
| Description 1 | TTP connection to SMD Day for Dush |
| Description 2 | |
| Description 2 | |
| Description 5 | |
| Administration | Tachalad Cattings |
| Auministration | Technical Security Special Options |
| Target System Settir | 105 |
| Target Host | mobile- |
| Path Prefix | /Notification |
| | |
| | |
| | |
| HTTP Proxy Options | |
| HTTP Proxy Options Global Configurati | on |
| HTTP Proxy Options Global Configurati Proxy Host | on |
| HTTP Proxy Options Global Configurati Proxy Host Proxy Service | on |
| HTTP Proxy Options Global Configurati Proxy Host Proxy Service Proxy User | on |
| HTTP Proxy Options Global Configurati Proxy Host Proxy Service Proxy User Proxy PW Status | ON Is initial |
| HTTP Proxy Options Global Configurati Proxy Host Proxy Service Proxy User Proxy PW Status Proxy Password | ON Is initial |

- 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 (BTPMS Business Technology Platform) created in Import SAP BTP Certificate to Gateway system *(on page 33)*.

| RFC Destination IWBEP_ODATA_OD_PUSH | |
|---|---|
| Connection Test 💖 | |
| 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 Certificate SCPMS SAP Cloud Platform Cert. List Authorization for Destination Inactive Inactive Inactive Inactive | • |
| | * |

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 | BEP_ODATA_OD_PUSH | I | |
| Ту. Η | TTP Connection to Exter | rnal Server | |
| Test Result R | esponse Header Fields | Response Body Response Text | |
| | | | |
| Detail | Value | | |
| Status HTTP Respon | se 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

| = | E SAP Cloud Platform Mobile Services | | | | |
|------------|--------------------------------------|-------------------------------|----------------|--------|--|
| 命 | Home | Native/Hybrid | | | |
| 0 | Mobile Applications 🔹 🗸 | Native/Hybrid All 4 | | | |
| | Native/Hybrid | New Import | | | |
| | SAP Mobile Cards | | | | |
| j ĝ | Features | Name | Application ID | Vendor | |
| 0 | Destinations | top theory | All Comp | innov | |
| ~~ | Analytics > | tig minip mi | to recept | innov | |
| | | 10.040.40 | 1(3-040.40) | | |
| ¢ | Settings | 10.50 | 10.510 | | |

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

| 命 | Home | | Native/Hybrid | | | | | | | |
|----------|---------------------|---|-----------------------|-----------------|----------------------|-----------------|-------------------|------------------|---------------|---|
| ٥ | Mobile Applications | ~ | <u>نې</u> | men (| | | | | | |
| | Native/Hybrid | | Delete App Export App | p Lock App | Publish to Discovery | Service | | | | |
| | SAP Mobile Cards | | Info APIs App | olication Links | User Registrations | Usage Analytics | Blocked Users | Support Sessions | | |
| Щŝ | Features | | Application Date | aile | | R | Assigned Fea | tures | | + |
| 0 | Destinations | | Application Deta | aits | | 0 | Nama | | State | |
| | Analytics | > | <u>É.</u> | | | | All Access Co | ntrol | State ⊡ OK | > |
| 0 | 6 -11-1- | 、 | No. 14 | | | | ିଶ୍ୱି Client Poli | cies | [⊻ ок | > |
| Ŷ | Settings | ' | and they | | | | 🕸 Client Res | ources | 🗹 ОК | > |
| | | | and water | | | | े Connectivi | ty | 🗹 ок | > |
| | | | Ventor | | | | තු Offline | | 🗹 ОК | > |
| _ | | _ | | | | | 🖂 Push Notif | ication | [⊻ ок | > |
| Ð | Important Links | | | | | | 🔒 Security | | [⊻ ок | > |
| ą | 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: | |
| Certificate | |
| O Token-based | |
| *Certificate (P12): | |
| 1980/00/00/00/00/00/00/00/00/00/00/00/00/0 | 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 | |
|---|---------------------|--|
| 4 | 🍶 dev | |
| 1 | 퉬 ios | |

L

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- Name | Helps you identify the Innovapptive product name. |

| Prop- erty | Description |
|------------------------------|--|
| | Conditions: Use uppercase alphabets. Possible Values: Based on the product, refer to the table below. For example, Mobile Work Order. |
| 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. • Conditions: None • Possible Values: Development/Quality/Production. |
| Show- Demo- Button | 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. Conditions: Use lowercase alphabets. Possible Values: true/false |
| hcolor | Custom header color for application. Provides the ability to customize the app screen elements, such as the header bar, to meet your cor- porate branding needs. Work with your appropriate branding team to identify the color that meets your enterprise palette. |
| | Tip: 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. |
| | Conditions: Use the Hex color code value based on the color you would like to see on the mobile app screen elements. Possible Values: As required. For example, #42c2f4 |
| Offline- Status- Color | 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. Tip: 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. For example, the parameter value could be configured as "OfflineStatusCol- or":"#DF264D" in the json file. |

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

| Prop- erty | Description |
|----------------|--|
| Lan- guages | 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. |
| | <pre>{"id":<sequencenumber>,"key":"<saplanguagecode>","value": "<languagename>"}</languagename></saplanguagecode></sequencenumber></pre> |
| | Conditions: Use the Hex color code value based on the color you would like to see on the mobile app screen elements. Possible Values: Languages supported by SAP. For example, {"id":1,"key":"E","value":"English"} |
| | Note: For RACE Dynamic Forms, only English language is supported. |
| Time- out | Description & Use: The application idle Timeout (in minutes). This setting allows the administrator to specify the automatic time out when apps are left idle. Possible Values: As required. For example, D30. |

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 | The application establishes the communication to the server based on the port number. Possible Values: 443. For example, HTTPs (SAP BTP default HTTPs port 443 and custom ports for proxy) |
| Appli- cationID | ID configured in SAP BTP and the mobile application will use it to connect to server for the registration. Condition: Use the same application ID as defined in SAP BTP. Possible Values: Based on the product, refer to the table below. For example: com.innovapptive.mworkorder. |
| Securi- tyType | 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. 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. |
| https | Used to identify the protocol type. The default value should be set to false. Condition: Use lowercase alphabets. Possible Values: true/false. |
| 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.

{
 "Server": "smphost",
 "Port": "8680",
 "ApplicationID": "com.innovapptive.mworkorder",
 "SecurityType": "SSO2",
 "https:/false,
 "ApplicationID": "Com.innovapptive.mworkorder",
 "SecurityType": "SSO2",
 "https:/false,
 "Appliame": "MoNKORDER",
 "Environment": "Development",
 "ShouDemoButton":true,
 "hoclor":#445E75",
 "ToucLid":true, "AppPassCode":true, "ForgotPwdLink":false, "ForgotPwdMsg":"<u>http://www.innovapptive.com</u>/", "StoreName":"",
 "Languages:[{['dd':1, "key":"E", "value":"ForgotPwdLink":false, "ForgotPwdMsg":"<u>http://www.innovapptive.com</u>/", "StoreName":"",
 "Languages:[{['dd':1, "key":"E", "value":"English"},['id':2, "key":"D", 'value":"German"},[''dd':2, "key":"T", "value":"Ferench"},
 "'inouClid":"Soainsh"},[''dd':5, "key":"Portuguese"],{['dd':3, "key":"N", "value":"Thai"}],
 "''inouClid":"Twoi.funloc", "StoreName":"FUNCTIONALLOCATION"}, ("ApplicationID": "mwo.funloc", "StoreName":"EQUIPMENT"]]

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).

| resource_mworkorder Je resource_mworkorder DEV | ^ | 1 | 10 | 1.2 | | ounnume. |
|--|---|-------------------------------|------------------------------|-----------------------|--------------|---------------|
| a 🕌 ios | | 1 25 | C CA | | mWorkOrder | 4 |
| | | App_BG_iPad_La ndscape.png | App_BG_iPad_Pro trait.png | App_BG_iPhone. png | 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 |
|---------------|--|
| Арр- | Helps you identify the Innovapptive product name. |
| Name | Conditions: Use uppercase alphabets. |
| | Possible Values: Based on the product, refer to the table below. For ex- |
| | ample, Mobile Work Order . |

| 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. • Conditions: None |
| hcolor | 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. Tip: 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. Conditions: Use the Hex color code value based on the color you would like to see on the mobile app screen elements. Possible Values: As required. For example, #42c2f4 |
| Cus- tomer- Name | Helps you identify the name of the customer. For example, Innovapptive. |
| Offline- Status- Color | 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. Tip: 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. For example, the parameter value could be configured as "OfflineStatusCol- or": "#DF264D" in the json file. |
| isEU- LARe- quired | Set the value as False to disable the EULA agreement screen in application. |
| Online- Offline | Set the value as True to enable the Online/Offline feature in application. |

| Prop- erty | Description |
|-------------------------------|--|
| UseDe- faultUrl | Set the value as True 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 True to enable the Forgot Password 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 | Description & 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. 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. |
| Forgot- Pwd- Msg | Set the value as True to display the message to reset password. |
| Store- Name | Helps you to identify the store name. • Conditions: None • Possible Values: WORKORDER |
| Store- Descrip- tion | Helps you to identify the description regarding the store name. • Conditions: None • Possible Values: General |
| Store- Index | Helps you to identify the index value of the store name and the order is in as- cending order. • Conditions: None • Possible Values: 1 or 2 |

| Prop- erty | Description | |
|----------------|--|--|
| Store- | Helps you to identify the type of the store. | |
| Туре | Conditions: None | |
| | • Possible Values: T | |
| Lan- guages | 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. | |
| | Syntax: | |
| | <pre>{"id":<sequencenumber>,"key":"<saplanguagecode>","value": "<languagename>"}</languagename></saplanguagecode></sequencenumber></pre> | |
| | Conditions: Use the Hex color code value based on the color you would like to see on the mobile app screen elements. Possible Values: Languages supported by SAP. For example, {"id":1,"key":"E","value":"English"} | |
| | Note: For RACE Dynamic Forms, only English language is supported. | |
| Time- out | Description & Use: The application idle Timeout (in minutes). This setting allows the administrator to specify the automatic time out when apps are left idle. Possible Values: As required. For example, D30. | |

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.

| Description |
|---|
| The DNS/HostName of the SAP BTP servers, which will be used for mobile ap- plication connection. For example: scp.innovapptive.com |
| The application establishes the communication to the server based on the port number. Possible Values: 443. For example, HTTPs (SAP BTP default HTTPs port 443 and custom ports for proxy) |
| ID configured in SAP BTP and the mobile application will use it to connect to server for the registration. Condition: Use the same application ID as defined in SAP BTP. Possible Values: Based on the product, refer to the table below. For example: com.innovapptive.mworkorder. |
| 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. 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. |
| Used to identify the protocol type. The default value should be set to false. Condition: Use lowercase alphabets. Possible Values: true/false. |
| 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 |
|-------------------------------|--|
| 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 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 BTP 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 |
| <pre>request_format=application/json;q=1,application/atom+xml;q=0.5</pre> |
| 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:

| \equiv | SAP Cloud Pl | | | | | | | | |
|----------|--------------|----------|---------------------------|------------------------|-------------------------|----------------------|------------|-------------|--|
| ଜ | | | | N86 | Edit Offline Configurat | tion | | | |
| ٢ | | ~ 4 | | | | | | | |
| | | | Defining Requests | | | | | + | |
| | | | MATNRCollection | Refresh Interval (min) | Delta Tracking | Token Lifetime (min) | Share Data | Action | |
| 69 | | | MeasPointCollection | | | | | <u></u> | |
| 0 | | | NotificationsCollection | | | | | - - | |
| 35 | | > | WorkOrdersCollection | | | |] | ÷. | |
| 95 | | <u> </u> | WOTaskListCollection | | · · · | | | ÷. | |
| ~ | | _ | MaterialDocListCollection | | · · · | | | ŧ. | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| Ø | | | | | | | Previous | Next Cancel | |
| | | | | | | | | | |

For Equipment:

| Ξ | | | | | | | | | | |
|-----|------------------|-----|------|-------------------------|------------------------|-----------------------|----------------------|------------|-------------|---|
| ଜ | | | N | | W1 | Edit Offline Configur | ation | | | |
| ¢ | | s 🗸 | Nov. | | | 6 | | | | |
| | | | Ľ. | Defining Requests | | | | | + | |
| | SAP Mobile Cards | | | Name | Refresh Interval (min) | Delta Tracking | Token Lifetime (min) | Share Data | Action | |
| | | | | EquipmentListCollection | | | | | | |
| | | | | EQUNRCollection | | ~ | | | | |
| 0 | | | | HEQUICollection | | · · | | | | Ļ |
| 223 | | > | | | | | | | | |
| 30 | | > | | | | | | | | |
| - | | · · | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| 0 | | | | | | | | Previous | Next Cancel | |
| 嚾 | | | | | | | | | | |

For Functional Location:

| E SAP Cloud Platform Mobi | le Services | | | | | | VALLAKAS |
|---------------------------|-------------------------|------------------------|----------------|----------------------|------------|------------------|----------|
| ☆ Home | | 000 | Edit Offline C | onfiguration | | | |
| Mobile Applications ~ | | | | | | | |
| Native/Hybrid | Defining Requests | | | | | + | |
| SAP Mobile Cards | FunctionalLocCollection | Refresh Interval (min) | | loken Litetime (min) | Share Data | Action | |
| 📢 Features | TPLNRCollection | | | | | | |
| Ø Destinations | | | | | | | |
| 💥 Analytics > | | | | | | | |
| Settings > | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| Important Links | | | | | Prev | ious Next Cancel | |
| 파 Legal Information | | | | | | | |

- 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 END_USER_R2208 | Innovapptive mWork- Order - End User - ECC Authorizations - Release 2208 | IW21, IW22, IW23,IW31, IW32, IW33, IW34, IW39, IW41, IW42, 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 | S_RFC, S_RFCACL |
| ZINV_MWO_ECC RACE_ADM_R2208 | Innovapptive mWork- Order - RACE Admin - ECC Authorizations - Release 2208 | | S_RFC and S_RFCACL |

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) | | |
| | IWSV (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

| Name | Tort | Dath | Obi | Object Name | Type of External Service | External Convice |
|--------------------------------|------|------|------|-----------------------------------|--------------------------|------------------|
| | LIT. | FUID | DUGU | | Type of Excental Service | Excernal Service |
| BFE4EB4/E83C95CC8/0C1B4C8/56FF | ні | R31R | 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 | R3TR | 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

| 년 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 6-5 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

| U | | | | | | | | | |
|-------------------|---|-------|----------|-----------------|------------|--|--|--|--|
| Impor | Import Queue: System EH7 | | | | | | | | |
| Ø = 1 | ④ ≛ 〒 ┖ Q 〒 ♣ ☆ ≞ ≡ 県 ╠ 읍 븢 🥵 🕾 💷 🖾 🗄 🛛 | | | | | | | | |
| 属 Reques 🖓 Reques | sts for EH7: (st ERDK901948 |) / 1 | | 01.08.2016 14:2 | 27:35 | | | | |
| Number | Request | RC | Owner | Short Text | St | | | | |
| 83 | ERDK901948 | ۵ | E5000103 | | Т <u>і</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

| Description | Transactions | Authoriza- tion Objects |
|-----------------------|--|--|
| mInventory - End | MB1A, MB1B, MB1C, | S_RFC, S_RFCACL |
| User - ECC Authoriza- | ME29N, ME51N, ME52N, | |
| tions - Release 2212 | ME53N, ME21N, ME22N, | |
| | ME23N, VT03N, MM03, | |
| | VT02N, VT01N, VL02N, | |
| | VT01N, MM02, MIGO, | |
| | MI01, MI02, MI03, MI07, | |
| | LI01N, LI02N, LI03N, LT31, | |
| | MI04, LI11N, HUINV02, | |
| | MI09, MMBE, LX02, | |
| | LX03, LT03, LT12, LT0F, | |
| | LT04 | |
| | Description mInventory - End User - ECC Authoriza- tions - Release 2212 | DescriptionTransactionsmInventory - EndMB1A, MB1B, MB1C,User - ECC Authoriza-ME29N, ME51N, ME52N,tions - Release 2212ME53N, ME21N, ME22N,ME23N, VT03N, MM03,VT02N, VT01N, VL02N,VT01N, MM02, MIGO,MI01, MI02, MI03, MI07,LI01N, LI02N, LI03N, LT31,MI04, LI11N, HUINV02,MI09, MMBE, LX02,LX03, LT03, LT12, LT0F,LT04LT04 |

Table 6-7 Roles for NetWeaver Gateway System

| Role Name | Description | Authorizations |
|------------------|------------------------------|-----------------------------|
| ZINV_MIM_NWG_END | mInventory - End User - | S_RFC, S_RFCACL, S_SERVICE, |
| USER_R2212 | Gateway Authorizations - Re- | S_USER_GRP & S_TABU_DIS |
| | lease 2212 | |

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) |
| | IWSV (Gateway Business Suite Enable- ment – Service) |
| Object Name | /INVMIM/MINVENTORY_ 2 _SRV*, |

/INVCEC/RACE_SRV*,

Figure 6-7 USOBHASH table

| Ta Di | ib Is | le: USOBHASH played Fields: 6 of 7 | Fi | ked Col | lumns: | [2] List Width 0250 | |
|----------|----------|--|----------------------|--------------------------------------|------------------------------|--|--------------|
| | | NAME | TYPE | PGMID | OBJECT | OBJ_NAME | SERVICE_TYPE |
| | | E72B118C808CE6DBD3F1443CD8275A 0D617E64EC8B9891CE615BF4F640E5 647CD51054EB07807FA882F5125B6F BFE4EB47E83C95CC870C1B4C8756FF | HT HT HT HT | R3TR 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

| - | | | | | | | | | | | | |
|-------|------|--------|-----------|---------|----------|-----------|-----------------|-------------------|----------|------------------|---------|----------|
| - 🗆 🔾 | | 🖌 👧 Ma | nually | Check a | t Start | of Exte | rnal Services | | S | SERVICE | | |
| | | | - | | | | | | | - | | |
| | | | . | | | - | | | | | | |
| | - 00 | 🗕 Eð 🎍 | 🔰 Manuall | .y Che | ck at S | tart of : | External Servic | es | | T-NT36016900 | | |
| | | | | | | | | | | | | |
| | | -* 🧷 | Program. | transa | ction of | r functi | 647CD51054EB07 | 807FA882F5125B6F. | BFE4EB47 | 7E83C95CC870C1B4 | C8756FF | SRV NAME |
| | | _ | | (Th 1) | | 3 | | , | | | | |
| | | * 🖌 | Type or | Cneck r | lag and | Authori | HI | | | | | SRV_ITPE |
| | | | | | | | | | | | | |

Figure 6-9 Change Role Authorization

| C Authorizatio | ns <u>E</u> dit <u>G</u> oto Utilitie <u>s</u> En <u>v</u> ironmen | nt S <u>y</u> stem <u>H</u> elp | | |
|----------------|--|---|--------------------------------------|----------|
| Ø | | | | |
| | | | | |
| Change k | ole: Authorizations | | | |
| 12 12 🗧 | 🗑 📅 🗟 Selection criteria 🛛 🗟 Manually | Open Changed Maintained Organization | nal levels 🔢 🚺 Information 🛛 🗐 Trace | |
| Maint.: | 0 Unmaint. org. levels | 0 open fields, Status: Unchanged | | |
| ZINV_MIM_NWG | _RACE_ADM_R50 COE Innovapptiv | ve mInventory - RACE Admin - Gateway Authorizat | ions - Rel 5.0 | |
| | Manually Cross-application Author | rization Objects AAAB | | |
| | 🕮 🔁 👧 Manually 🛛 Authorization | Check for RFC Access | S_RFC | |
| | 💴 🔁 👧 Manually 🛛 Authorization | Check for RFC User (e.g. Trusted System) | S_RFCACL | |
| | OE 🔁 🎊 Manually Check at Start | t of External Services | S_SERVICE | |
| | C Define Values | | × | |
| | Type TADIR Service | • | | CDU NAME |
| | | 🕆 🏹 🔎 🌐 Technical Name 🛛 Full Authorization | | SRV_TYPE |
| | Maintain the Service Name | | | |
| 004 | R Name | Prog. ID Obi. Object Name | · | |
| | E72B118C808CE6DBD3F1443CD827 | R3TR I IWSG /INVMIM/MINVENTORY_2_SRV_0001 | A | |
| | 0D617E64EC8B9891CE615BF4F640E5 | R3TR IWSV /INVMIM/MINVENTORY_2_SRV 0 | 001 👻 | |
| | 647CD51054EB07807FA882F5125B6F | R3TR I IWSG /INVCEC/RACE_SRV_0001 | | |
| | BFE4EB47E83C95CC870C1B4C8756FF | R3TR I IWSV /INVCEC/RACE_SRV 0001 | | |
| | | R3TR 🗂 🗂 | | |
| | | R3TR 🖞 🖏 | 33 | |
| | | R3TR 🖹 💼 | | |
| | | R3TR 🖹 🗎 | | |
| | | R3TR 🖞 📓 | | |
| | | R3TR 🖬 🔳 | | |
| | | R3TR 🖹 🗎 | | |
| | | R3TR | | |
| | | | | |
| 4 > | | KJIKE E | | |

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 |
|------------|---|------------|
| ERDK912508 | INNOV ECC R 2212 Minventory Application End User Roles | None |

Table 6-12 SAP GW Transports

| Transport | Description | Dependency |
|------------|--|------------|
| NGTK909863 | Innov Gateway R 2212 Min- ventory Application End User Roles | None |

Table 6-13 SAP RLM Transports

| Transport | Description | Dependency | |
|------------|--|------------|--|
| EC7K900231 | INNOV:RLM: R 2206 mInvento- ry Application End User Roles | None | |

Table 6-14 SAP EWM Transports

| Transport | Description | Dependency |
|------------|---|------------|
| Н18К900227 | 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

| - | | | |
|---|----------------------------|------------------|----------------------|
| 匠 Queue <u>E</u> dit <u>G</u> oto <u>R</u> equest | Extras Environment Sys | tem <u>H</u> elp | |
| 🖉 🔻 🚽 | Legend Ct | rl+Shift+F4 | I 🔽 🛛 I 🕜 🖳 |
| | 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 | | | |
|--------------------------|---|--|--|
| 🔁 🚢 🐺 🔍 🎙 | 7 🖆 🛷 🗎 📰 🞭 🍖 🖴 🛼 😓 🚍 🖾 🖾 🔝 🔝 | | |
| Requests for EH7 | 7: 0 / 82 | | |
| 🔄 Add Transport Requ | 🔄 Add Transport Request 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

| - | - | | | | |
|--------------------------------------|---|----|----------|------------|-----|
| Impo | Import Queue: System EH7 | | | | |
| 2) 🚢 🔻 🤍 🖓 🏭 I 🗞 🗎 🗐 😓 🔒 🔐 🖽 🖽 🖽 🖬 🛍 | | | | | |
| 🔛 Reque | Requests for EH7: 0 / 1 01.08.2016 14:27:35 | | | | |
| Number | Request | RC | Owner | Short Text | St |
| 83 | ERDK901948 | | 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 |
|-----------------------|----------------------|--|
| mAssetTag End User | S_RFC | ACTVT = 16 RFC_TYPE = FUGR, FUNC RFC_NAME = /INVMAT/*, /INVCEC/*, / INV* |
| | S_TABU_DIS | • ACTVT = 03 • DICBERCLS = IW* |
| | S_RFCACL | • ACTVT = 16 • RFC_EQUSER = Y |
| Asset Admin User | S_RFC | ACTVT = 16 RFC_TYPE = FUGR, FUNC RFC_NAME = /INVMAT/*, /INVCEC/*, / INV* |
| | S_TABU_DIS | • ACTVT = 03 • DICBERCLS = IW* |
| | S_RFCACL | • ACTVT = 16 • RFC_EQUSER = Y |
| RACE Admin User | S_RFC | ACTVT = 16 RFC_TYPE = FUGR, FUNC RFC_NAME = /INVMAT/*, /INVCEC/*, / INV* |

| 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 | ACTVT = 16 RFC_TYPE = FUGR, FUNC RFC_NAME = /INVMAT/*, /INVCEC/*, / INV*, /IWBEP/*, ALFA*, ARFC*, BAPT*, EBNU*, MEWF, MEWQ, RHW1, SCVU, STXD, SWRR |
| 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 | ACTVT = 16 RFC_TYPE = FUGR, FUNC RFC_NAME = /INVMAT/*, /INVCEC/*, / INV*, /IWBEP/*, ALFA*, ARFC*, BAPT*, EBNU*, MEWF, MEWQ, RHW1, SCVU, STXD, SWRR |

| 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 | ACTVT = 16 RFC_TYPE = FUGR, FUNC RFC_NAME = /INVMAT/*, /INVCEC/*, /IW-BEP/*, ALFA*, ARFC*, BAPT*, EBNU*, MEWF, MEWQ, RHW1, SCVU, STXD, SWRR |
| | 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) |
| | IWSV (Gateway Business Suite Enable- ment – Service) |
| Object Name | /INVCEC/* and /INVMAT/* |

Figure 6-13 USOBHASH table

| | Тур | e TADIR Service | | • | | |
|---|-----|---|----------|------------|------------------------------|--|
| | | 역 🚱 트등 트랑 흐 루 🛗 🖄 🔽 🔎 🖽 Technical Name Full Authorization | | | | |
| | | Maintain the Service Name | | | | |
| | | Name | Prog. ID | Obj. | Object Name | |
| I | | 2066400603E7C39FA9AAAD1C3831 | R3TR 🗎 | IWSV 🖹 | /INVMAT/MASSETTAG_2_SRV 0001 | |
| I | | 39FEDFD28698D1A06E6137BAC440 | R3TR 🖹 | IWSG 🖹 | /INVMAT/MASSETTAG_2_SRV_0001 | |
| I | | 647CD51054EB07807FA882F5125B6F | R3TR 🖹 | IWSG 🖹 | /INVCEC/RACE_SRV_0001 | |
| | | BFE4EB47E83C95CC870C1B4C8756FF | R3TR 🖹 | IWSV ∎ | /INVCEC/RACE_SRV 0001 | |
| L | | | DOLD PL | 7 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 | | | |
|--|----------------|--------------|-------|
| COE Manually RACE Access Control Class | | ZINV | |
| COE 🔏 Manually RACE Access Control Ob | ject | /INVCEC/RA | |
| COE SManually RACE Access Contro | 1 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 User - ECC Authoriza- tions - Release 2203 | /INVMGO/DOCFORM | S_RFC, S_RFCACL |

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

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

| ſ | Тур | 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

| 🖵 🖓 COE 🔁 👧 Manually Check at Start of Exter | nal Services | S_SERVICE | |
|--|---------------------------------------|--------------------------------|----------------------|
| Check at Start of H | External Services | T-NT36023100 | |
| Program, transaction or functi Program, transaction or functi Type of Check Flag and Authori | 647CD51054EB07807FA882F5125B6F, HT | BFE4EB47E83C95CC870C1B4C8756FF | SRV_NAME 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 |