# Post-Install or Post-Upgrade Configurations Guide 2512

## Connected Worker Solutions

# 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*™.

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

**Product Version**: *2512*

**Release Date**: *09 January 2026*

**Published Date**: *09 January 2026*

**Document Version**: *1.0*



Primary Author: Innovapptive Inc.

# 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*™.

## Document Conventions

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

| Convention | Meaning |
|---|---|
| **boldface** | Indicates graphical user interface elements associated with an action, or terms defined in text or the glossary. |
| *italic* | Indicates book titles, emphasis, or 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. |

## 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

# 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.

Figure 2-1 Workflow for SAP BTP configurations after Installing Innovapptive Products

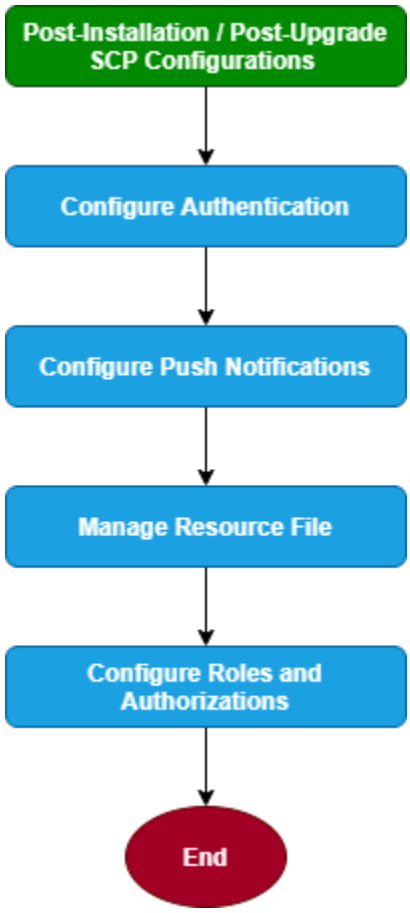


**Table 2-1 Tasks for SMP Configurations after Installing Innovapptive Products**

| Task | Reference to section |
|---|---|
| Configure authentication for mobile application | • Configure HTTP/HTTPs Authentication *(on page 10)*<br>• Configure SAML Authentication *(on page 15)*<br>• Integrate SAP BTP with Azure AD *(on page 29)* |
| Configure SAP BTP for Push Notifications | Configure Push Notifications for SAP BTP *(on page 30)* |
| Prepare and update resource file | Manage Resource File in SAP BTP *(on page 42)* |
| Configure roles and authorizations | Configure Roles and Authorization for Products *(on page 63)* |

# 3. Configure Authentications

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

Choose the authentication from the options



## 3.1. Configure HTTP/HTTPs Authentication

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

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

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

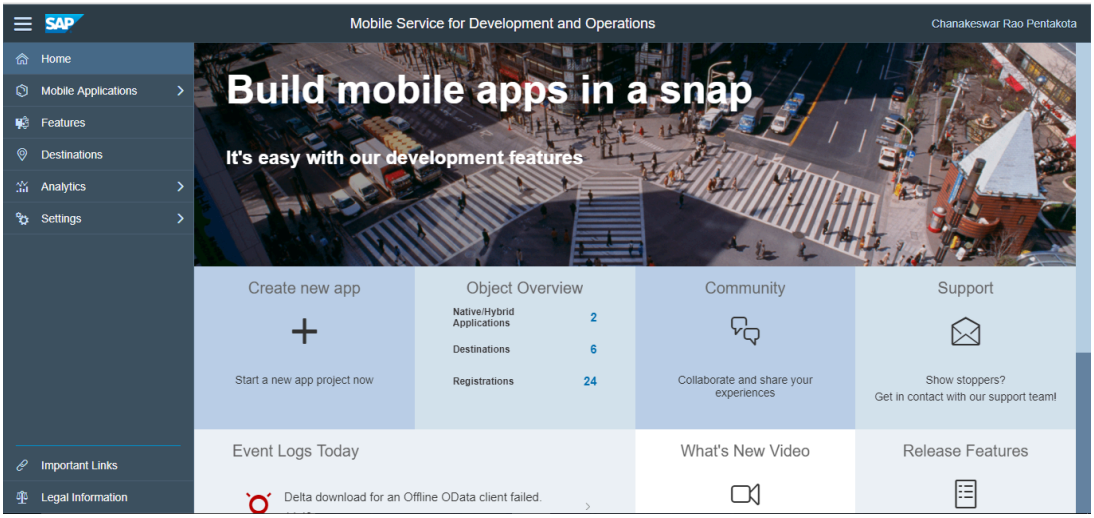
### 3.1.1. About SCPms

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

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

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

Figure 3-1 Mobile Services Management Cockpit




## 3.1.2. Create New Application using HTTP/HTTPs Authentication

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

To create an application using HTTP/HTTPs authentication:

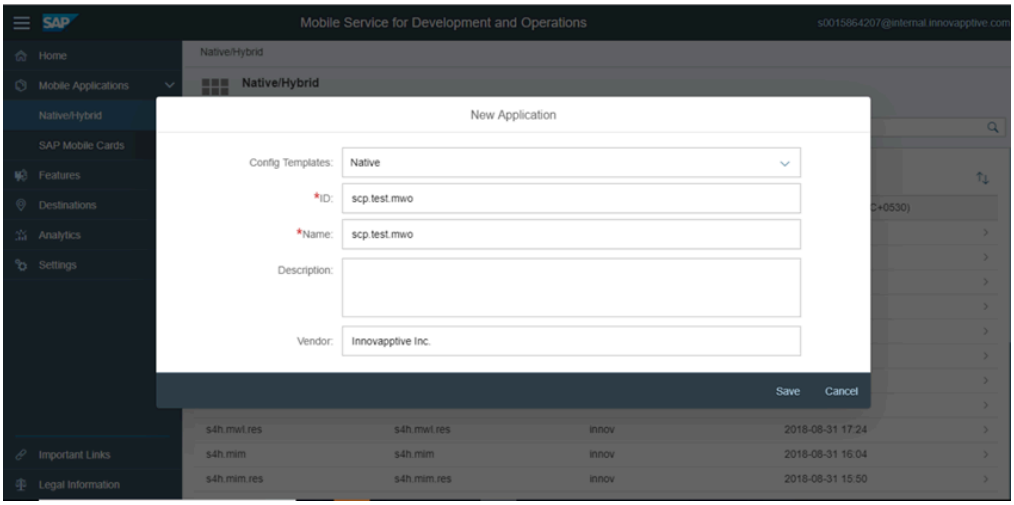
1. Expand **Mobile Applications** on the left navigation.
2. Click **Native/Hybrid** under Mobile Applications.
3. Click **New**.
4. Enter details such as **Application ID**.
   Use the information in the table to add new application details for the product you purchased.

| Product | App ID | Name | Type | Vendor | Security Configuration |
|---|---|---|---|---|---|
| mAsset-Tag | com.innovapptive-.massettag | Mobile Asset Tag | Native | Innovapptive | Basic |
| mInventory | com.innovapptive.minventory | Mobile Inventory | Native | Innovapptive | Basic |

| Product | App ID | Name | Type | Vendor | Security Configuration |
|---|---|---|---|---|---|
| mServiceOrder | com.innovapptive.mserviceorder | Mobile Service Order | Native | Innovapptive | Basic |
| mShop | com.innovapptive-.mshop | Mobile Shopping Cart | Native | Innovapptive | Basic |
| mWorklist | com.innovapptive.mworklist | Mobile Worklist | Native | Innovapptive | Basic |
| mWorkOrder | com.innovapptive.mworkorder | Mobile Workorder | Native | Innovapptive | Basic |

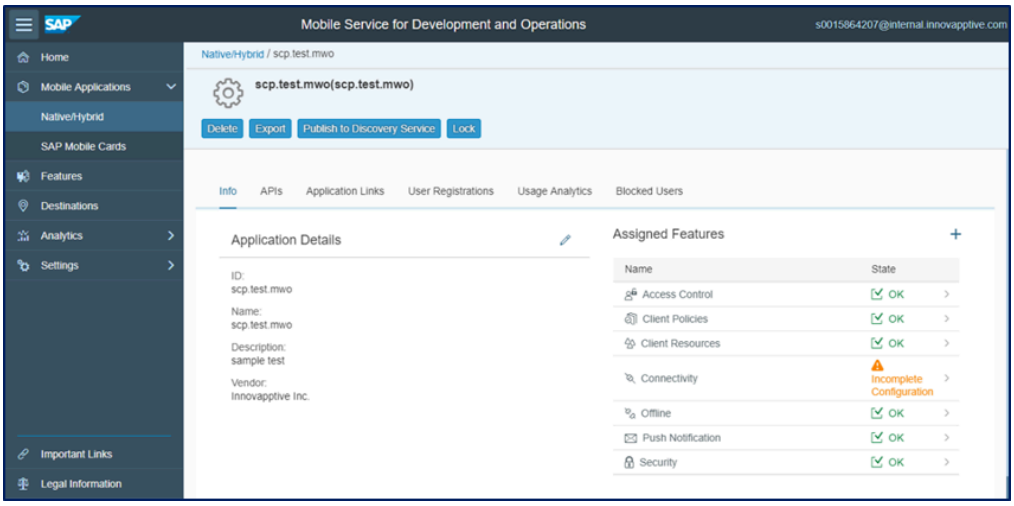
5. Enter the following in the **New Application** window:
    - **Config Templates**: Select **Native**.
    - **ID**: Enter the ID of the product.
    - **Name:** Enter the name of the product.
    - **Description:** Enter the description of the product.
    - **Vendor**: Enter Innovapptive Inc.

    Figure 3-2 Create New Application



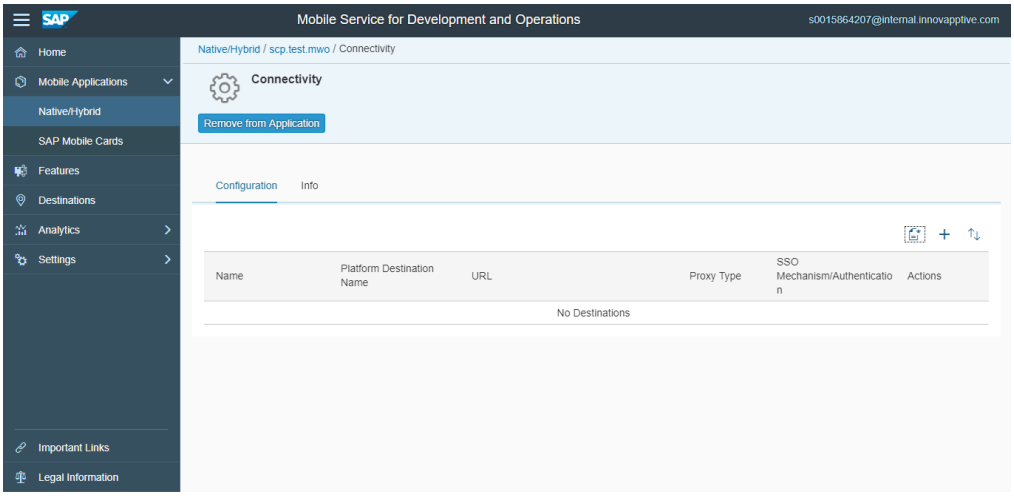

6. Click **Save**.

Figure 3-3 Application Details




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

Figure 3-4 Application Connectivity



- **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/odata/INVMAT/MASSETTAG_2_SRV/ |
| mInventory | http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/INVMIM/MINVENTORY_2_SRV/ |
| mService-Order | http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/INVMSO/MSERVICEORDER_SRV/ |
| mShop | http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/INVMSC/MSHOP_SRV/ |
| mWorklist | http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/INVMWL/MWORKLIST_3_SRV/ |
| mWorkOrder | http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/INVMWO/MWORKORDER_SRV/ |
| RACE Dynamic Forms | http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/INVCEC/RACE_SRV/ |

- 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.

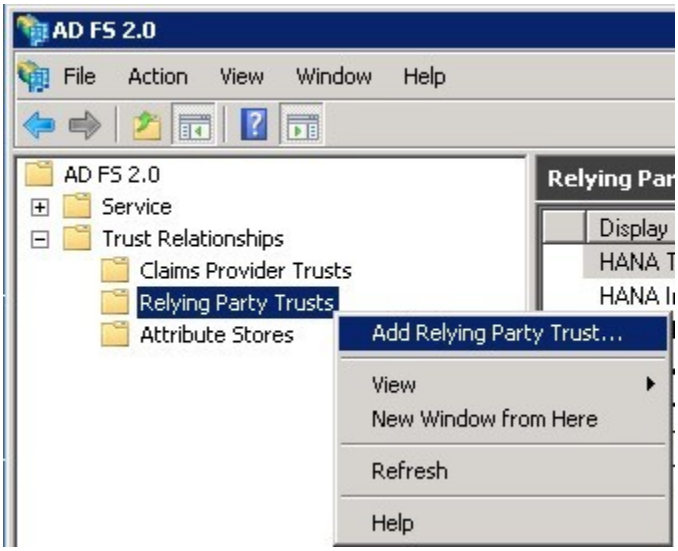
## 3.2.2. Add SAP BTP Metadata to ADFS

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:

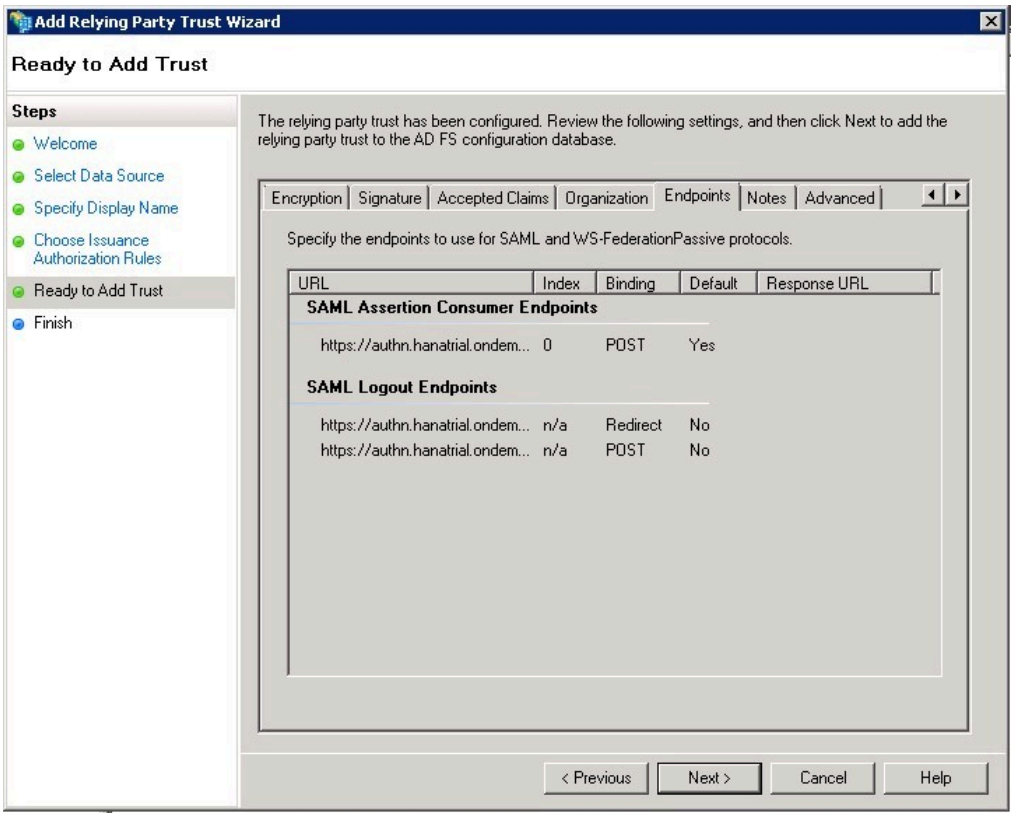
1. Click **Start, Administration Tools, AD FS 2.0 Management**.
2. Expand **View ADFS 2.0, Trust Relationships,** right-click **Relying Party**.
3. Select **Relying Party Trusts** and select **Add Relying Party Trust**.

Figure 3-5 ADFS Relying Party Trusts



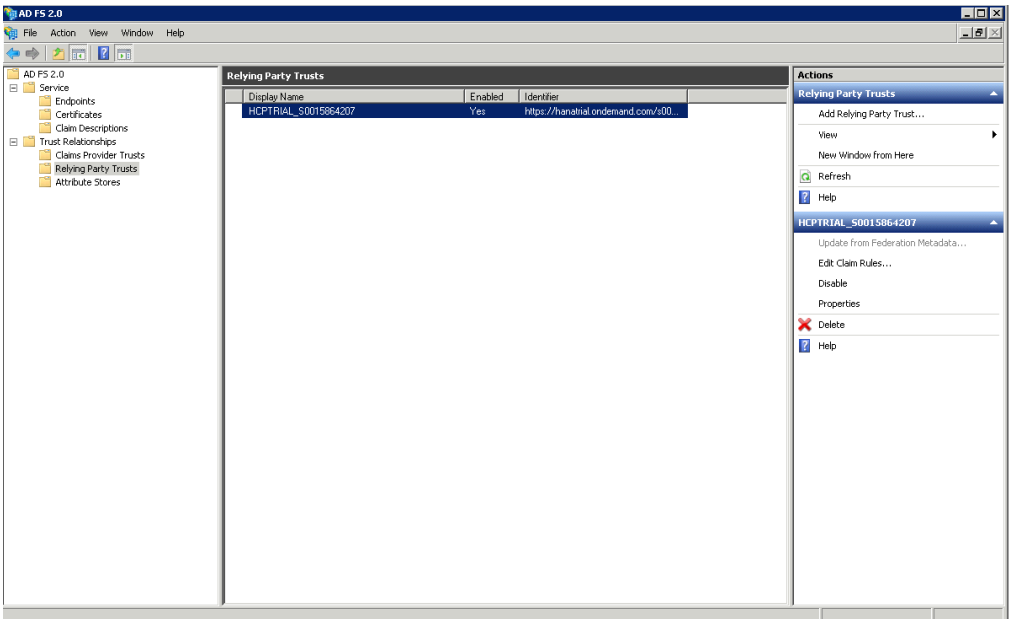

4. Click **Start**.
5. Select **Import data about the relying party from a file** and click **Browse.**
6. Navigate to the file, which you copied and click **Next.**
7. Enter **Display name** and click **Next**.
8. Select **Permit all users to access this relying party** and then click **Next**.
   All the SAML2 Metadata configurations that are imported into ADFS can be viewed in different tabs.

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_S00XXXXX**.
13. Click **Edit Claim Rules**.

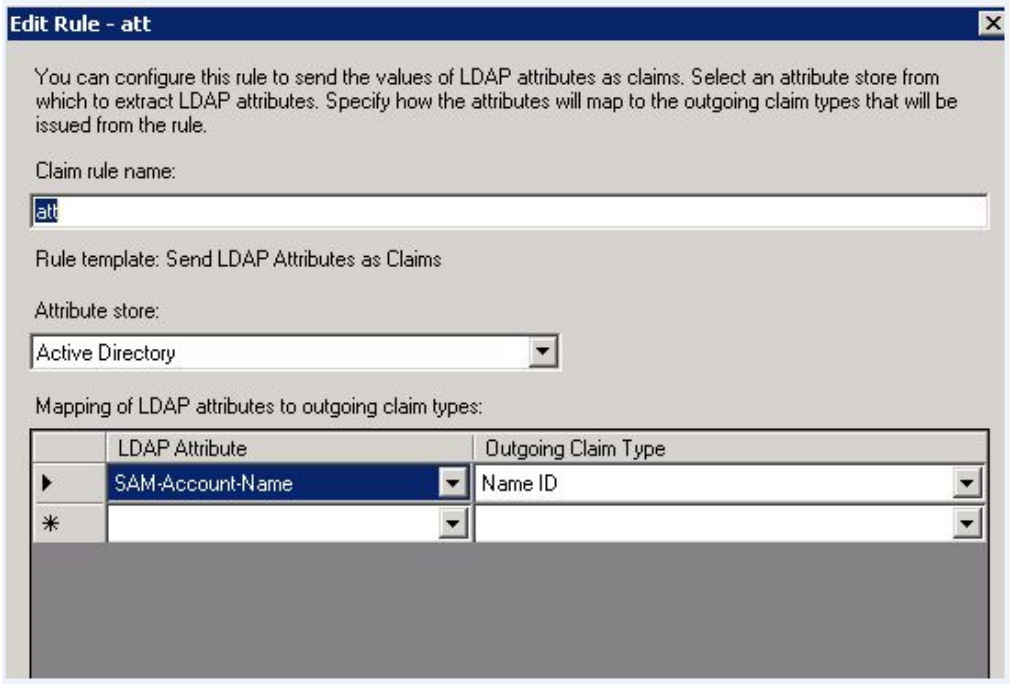
Figure 3-7 Edit Claim Rules




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.

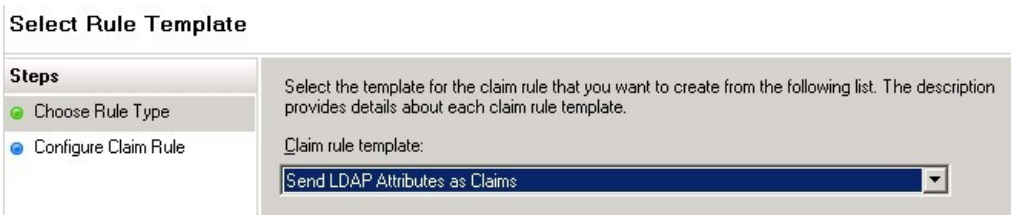
14. Click **Add Rule,** select **Send LDAP Attributes as Claims** under Claim rule template and click **Next**.
    - **Claim rule name**: Issue SAMAccountName as Name ID.
    - **Attribute store**: Active Directory.
    - **Mapping of LDAP attributes to outgoing claim types:**
        - **LDAP Attribute**: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

Figure 3-8 Edit Rule



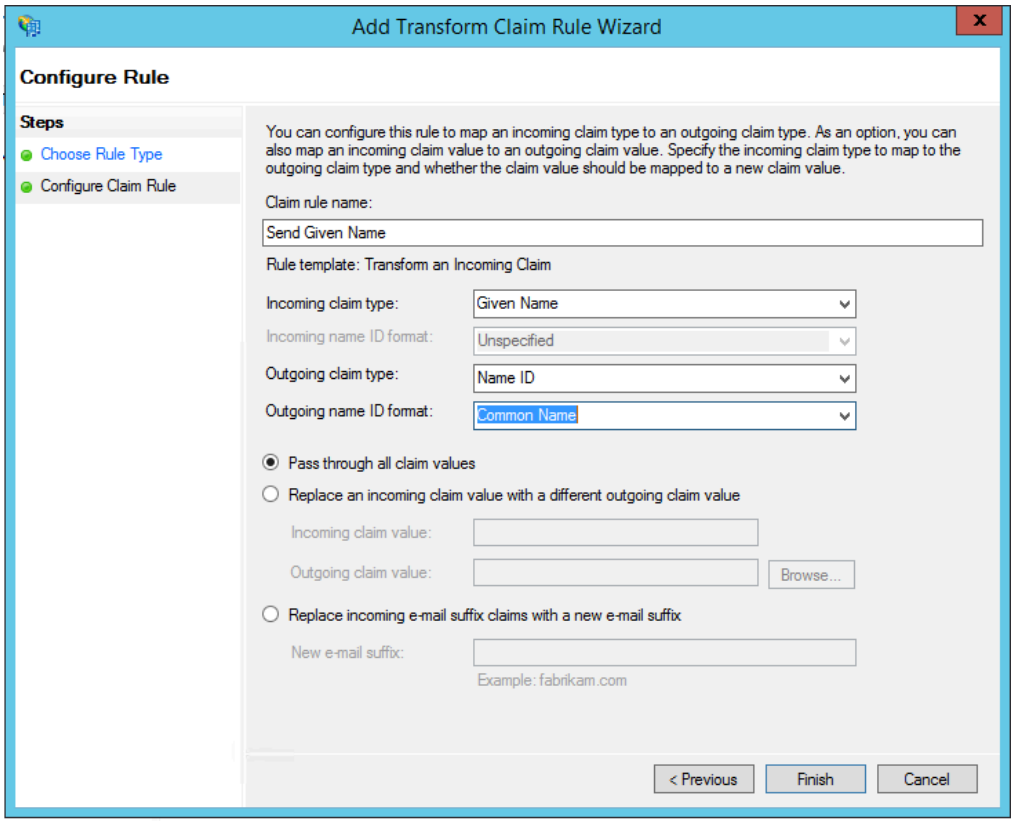

15. Click **Finish**. Rule1 is now saved.
16. Click **Add Rule**. This Claim Rule instructs ADFS to issue the **user's firstname**, **lastname**, **organizational ID**, and **employee ID** as **SAML Attributes** (also known as "Claims") in the response. (Options Configurations per the requirement).
17.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

Figure 3-9 Select Rule Template




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

Figure 3-10 Configure Rule




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.

> **Note:**
> 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.

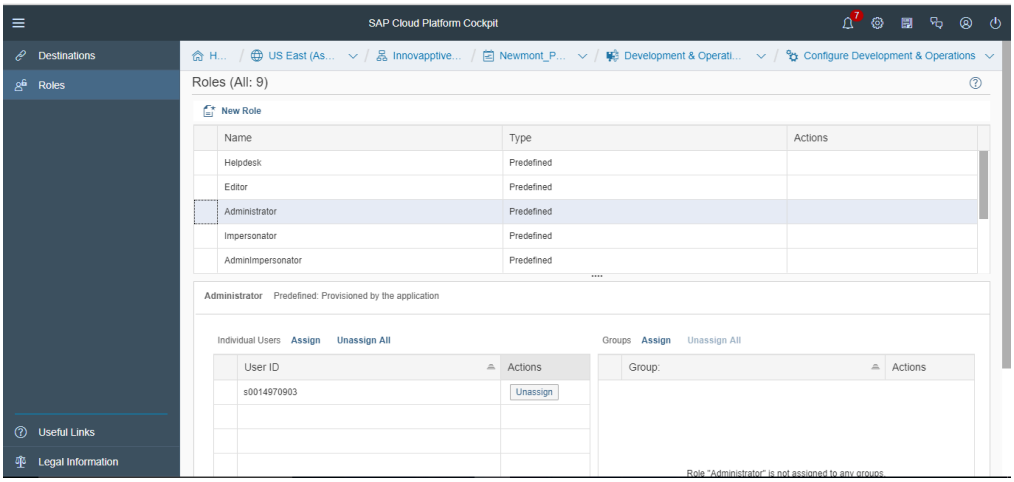
To add roles:

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.

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.

Figure 3-11 SAP BTP Roles




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.

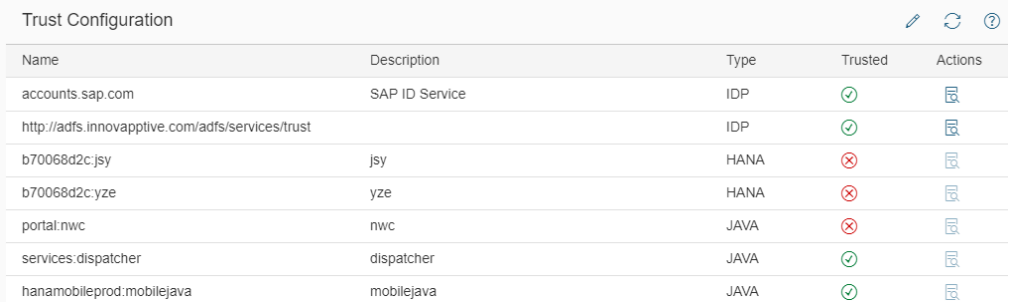
Before configuring, ensure you have:

- 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




## 3.2.6. Create New Application using SAML Authentication

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

To create an application using SAML Authentication:

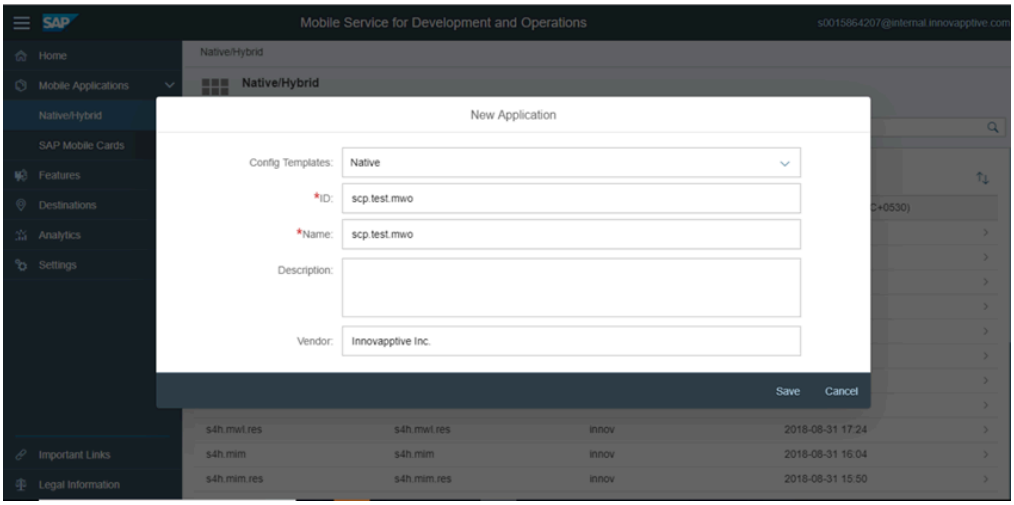
1. Expand Mobile Applications on the left navigation.
2. Click **Native/Hybrid** under Mobile Applications.
3. Click **Create New Application**.
   Use the information in the table to add new application details for the product you purchased.

| Product | App ID | Name | Type | Vendor | Security Configuration |
|---|---|---|---|---|---|
| mAssetTag | com.innovapptive.massettag | Mobile Asset Tag | Native | Innovapptive | Basic |
| mInventory | com.innovapptive.minventory | Mobile Inventory | Native | Innovapptive | Basic |

| Product | App ID | Name | Type | Vendor | Security Configuration |
|---|---|---|---|---|---|
| mServiceOrder | com.innovapptive.mserviceorder | Mobile Service Order | Native | Innovapptive | Basic |
| mShop | com.innovapptive-.mshop | Mobile Shopping Cart | Native | Innovapptive | Basic |
| mWorklist | com.innovapptive.mworklist | Mobile Worklist | Native | Innovapptive | Basic |
| mWorkOrder | com.innovapptive.mworkorder | Mobile Workorder | Native | Innovapptive | 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




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/odata/INVMAT/MASSETTAG_2_SRV/ |
| mInventory | http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/INVMIM/MINVENTORY_2_SRV/ |
| mService-Order | http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/INVMSO/MSERVICEORDER_SRV/ |
| mShop | http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/INVMSC/MSHOP_SRV/ |
| mWorklist | http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/INVMWL/MWORKLIST_3_SRV/ |
| mWorkOrder | http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/INVMWO/MWORKORDER_SRV/ |
| RACE Dynamic Forms | http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/INVCEC/RACE_SRV/ |

- **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

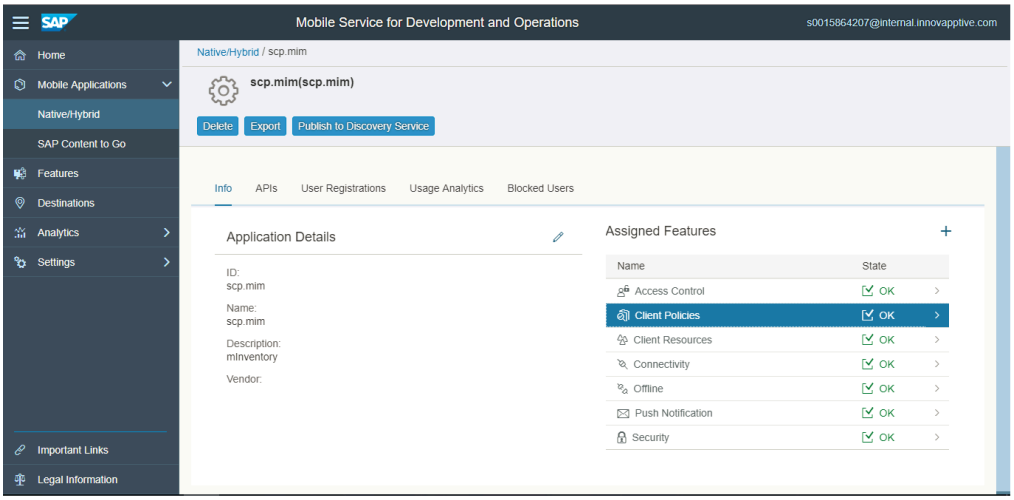
Define the client password policy that is used to unlock the DataVault for the applications. Application developers must add code to the DataVault to enforce the client password policy. An administrator must enter the application password policy to unlock the DataVault during application initialization.

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:

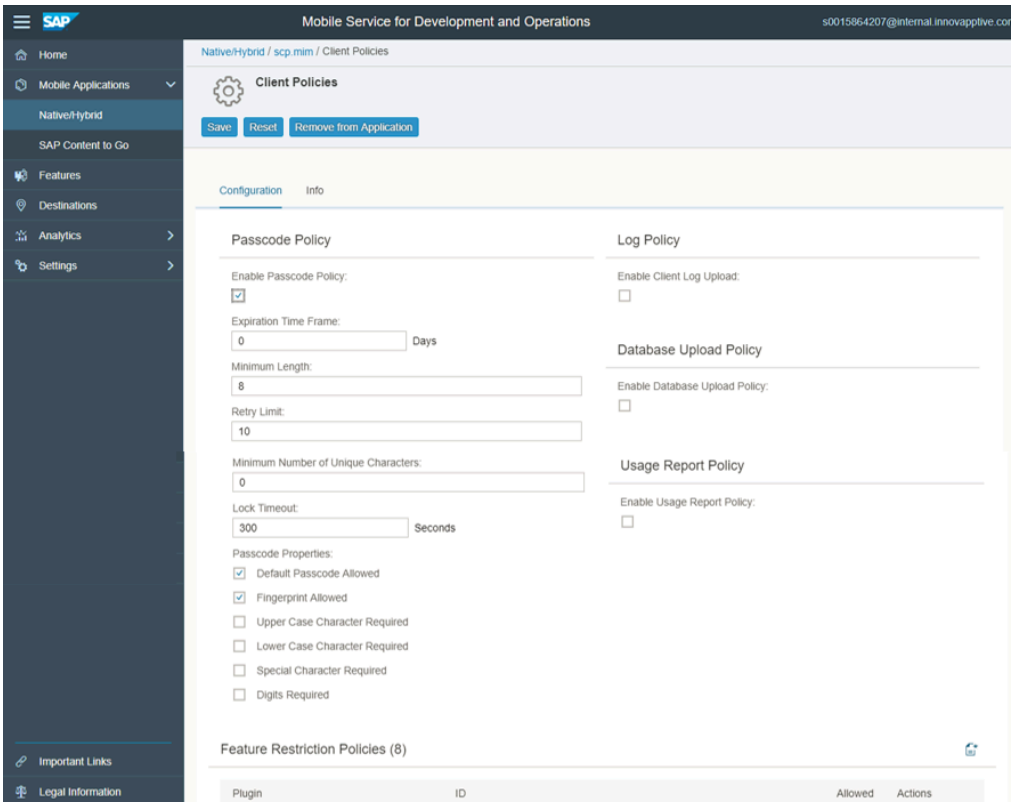
1. In Mobile Service for Development and Operations cockpit, select **Mobile Applications > Native/Hybrid.**
2. Select an application, and then select **Client Policies** under **Assigned Features**.

Figure 3-14 Application Details




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

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 | Default | Description |
|---|---|---|
| Minimum Number of Unique Characters | 0 | The minimum number of unique characters required in the password. |
| Lock Timeout | 300 | The number of seconds the DataVault remains unlocked within an application, before the user re-enters his or her password to continue using the application (like the screen-saver feature). |
| Default Passcode Allowed | Disabled | If enabled, a default password is generated by the DataVault. This disables the password. |
| Finger Print Allowed | Enabled | If enabled, it allows the use of native biometric techniques to unlock the app. |
| Upper Case Character Required | Disabled | If enabled, the password must include uppercase letters. |
| Lower Case Character Required | Disabled | If enabled, the password must include lowercase letters. |
| Special Character Required | Disabled | If enabled, the password must include special characters. |
| Digits Required | Disabled | 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:** AIzaSyDURzJeh8FTBIJBDxwwRSZLfp755l7jTAw
    - **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.

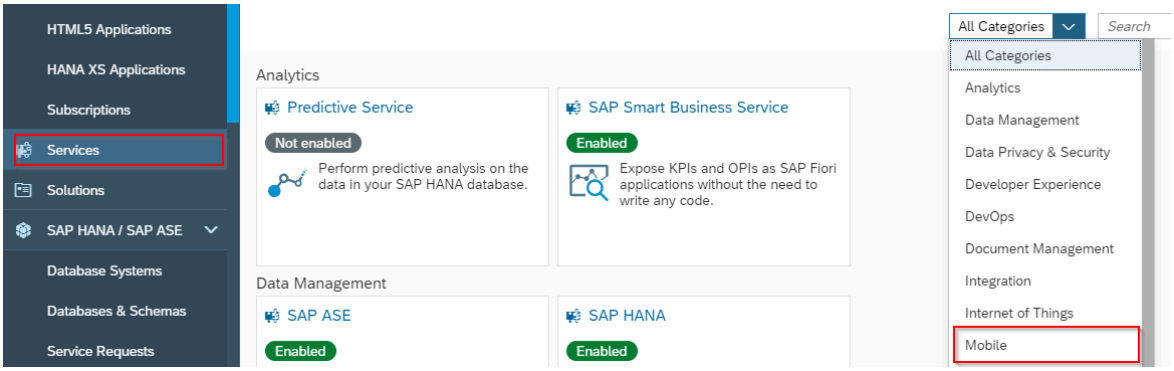
- SAP BTP Admin Access.
- Access to SAP Gateway System with Basis Roles.

**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.

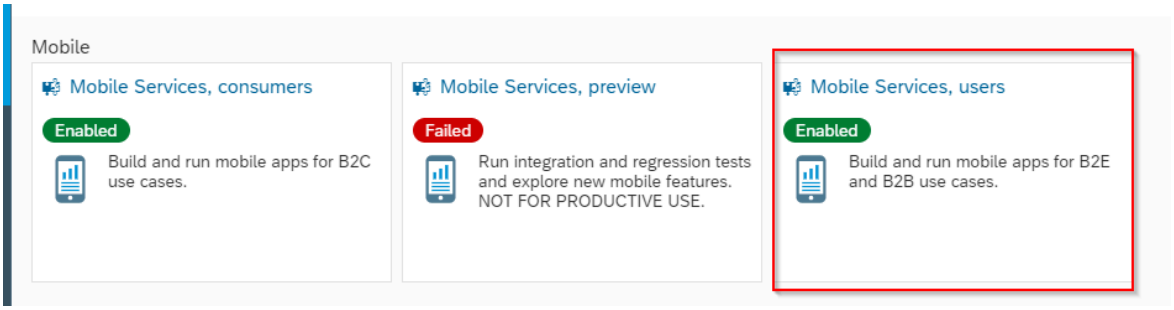
## 4.2. Configure SAP BTP for Push Notification

To configure SAP BTP for push notification:

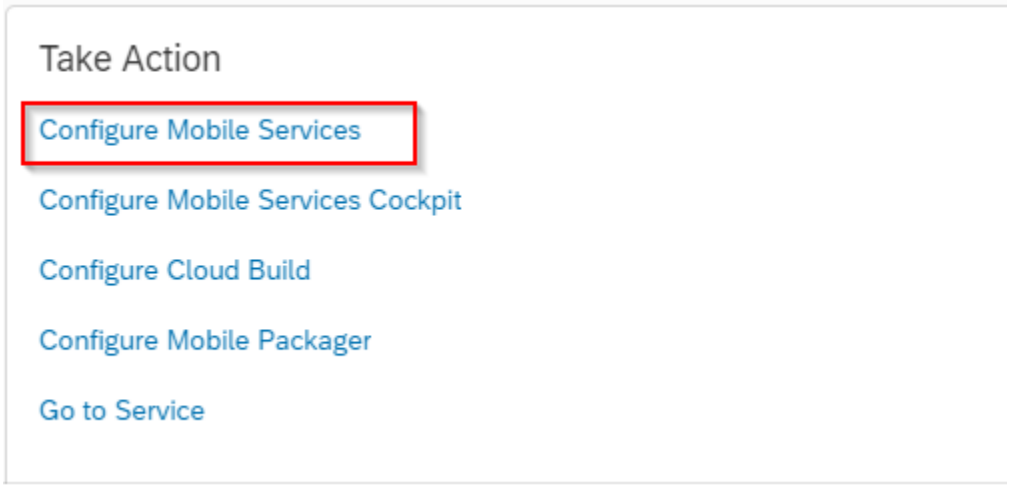
1. Log in to **SAP BTP Account**.
2. Navigate to your **Sub Accounts**.
   Sub Accounts depends on whether they are created for your account. You can directly create a Tenant in your main account. For example, {your_company_name} can be main account and it could have multiple sub accounts and the sub 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.




6. Select **Mobile Services, users**.

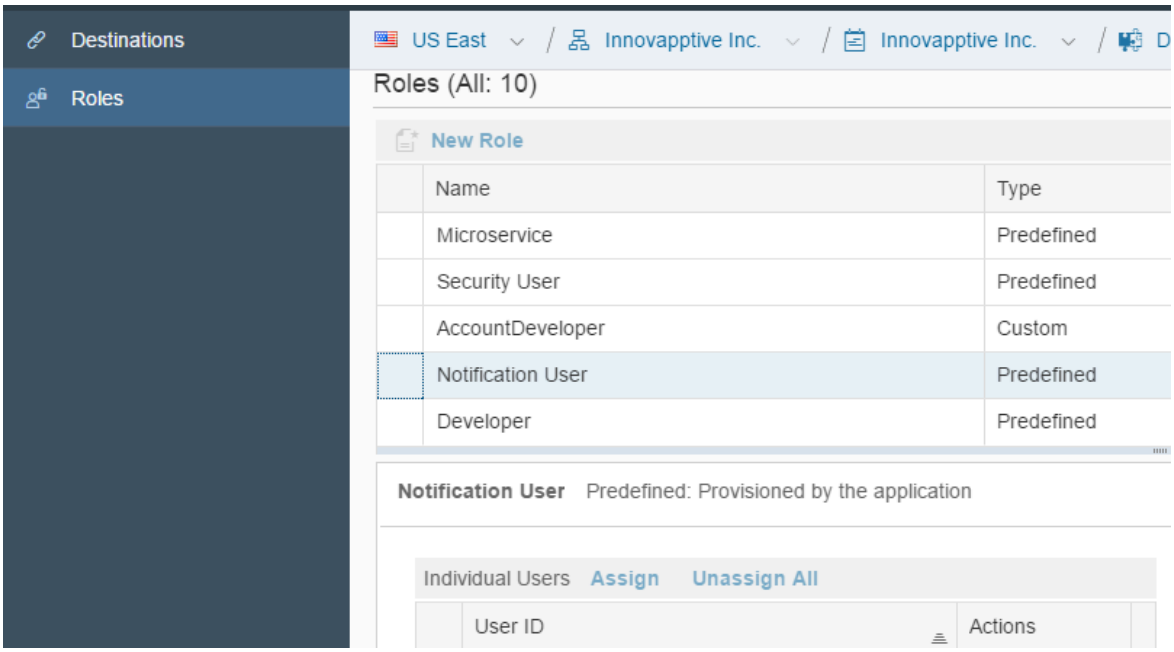



7. In the **Service: Mobile Services, users – Overview** screen, click **Configure Mobile Services** in the **Take Action** section.




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

10. Click **Assign**.




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

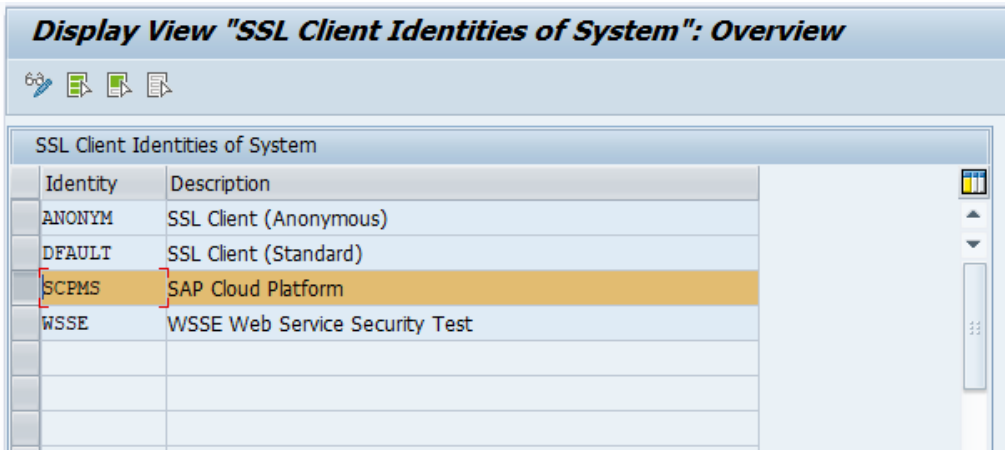
## 4.2.1. Import SAP BTP Certificate to Gateway system

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

To import SAP BTP certificate:

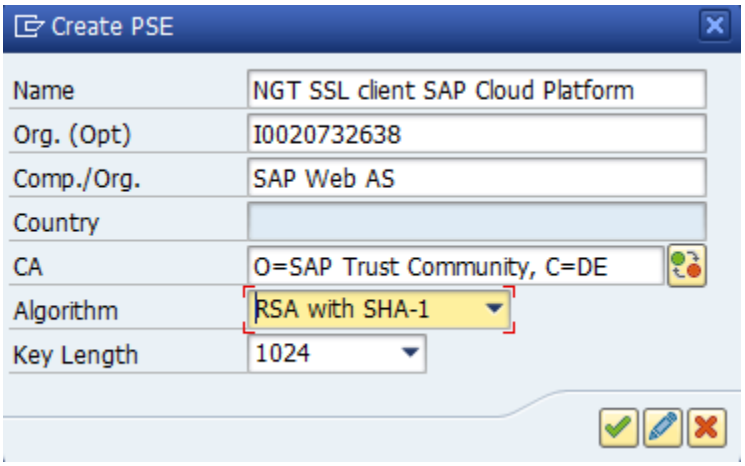
1. Go to **STRUST** transaction.
2. Navigate to **Environment**, **SSL Client Identities**.
3. Click on **Change** option and select New Entries --> create SSL identity with the following details:
    a. **Identity**: BTPMS
    b. **Description**: Business Technology Platform

Figure 4-1 SSL Client Identities



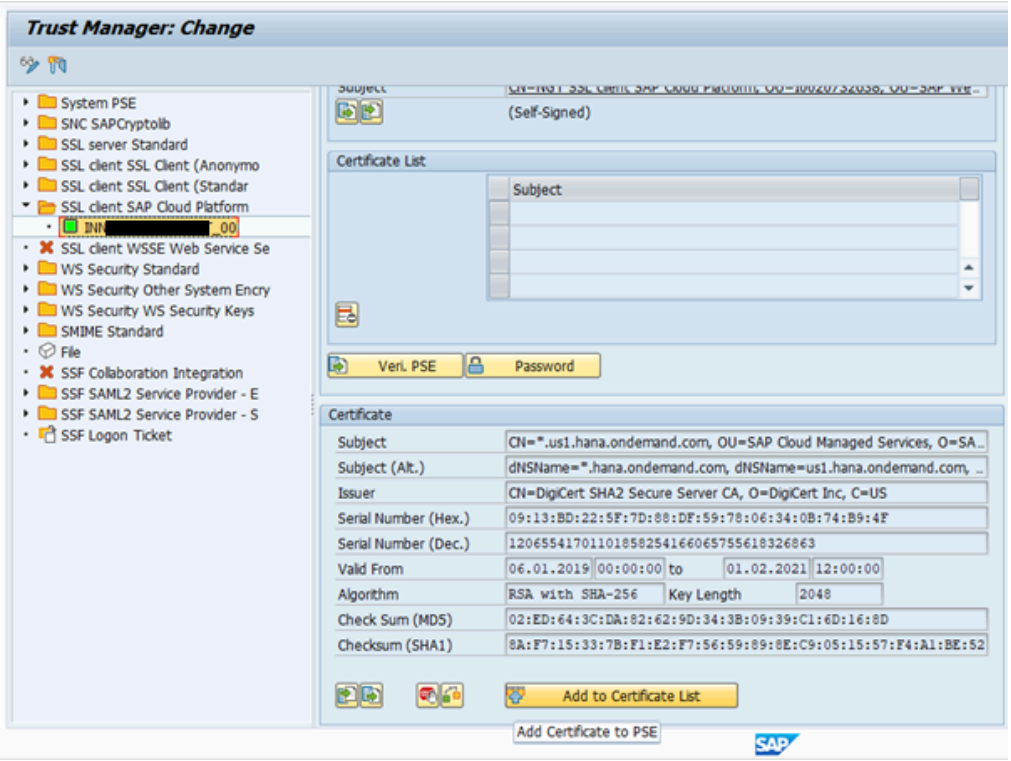

4. Navigate to the **STRUST** screen.
5. Right-click on **SSL Client Business Technology Platform** and click **Create**.
6. On the **Create PSE** screen, the following details are retrieved from the source certificate:
    a. Name
    b. Org.
    c. Comp./Org.
    d. CA
    e. Algorithm
    f. Key Length

Figure 4-2 Create PSE



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




## 4.2.2. Create RFC for Push Notification

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

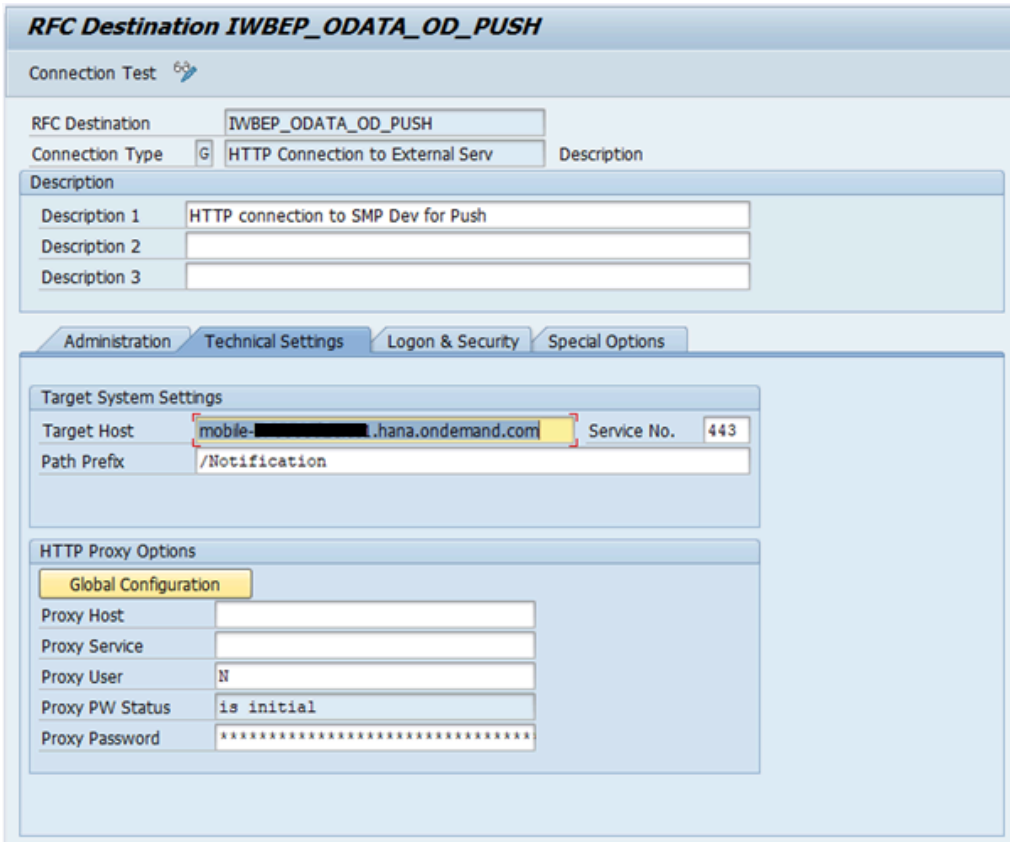
1. Go to **SM59** transaction and create a RFC of connection type G.
2. In the **RFC Destination** window, enter the following information:

**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 |

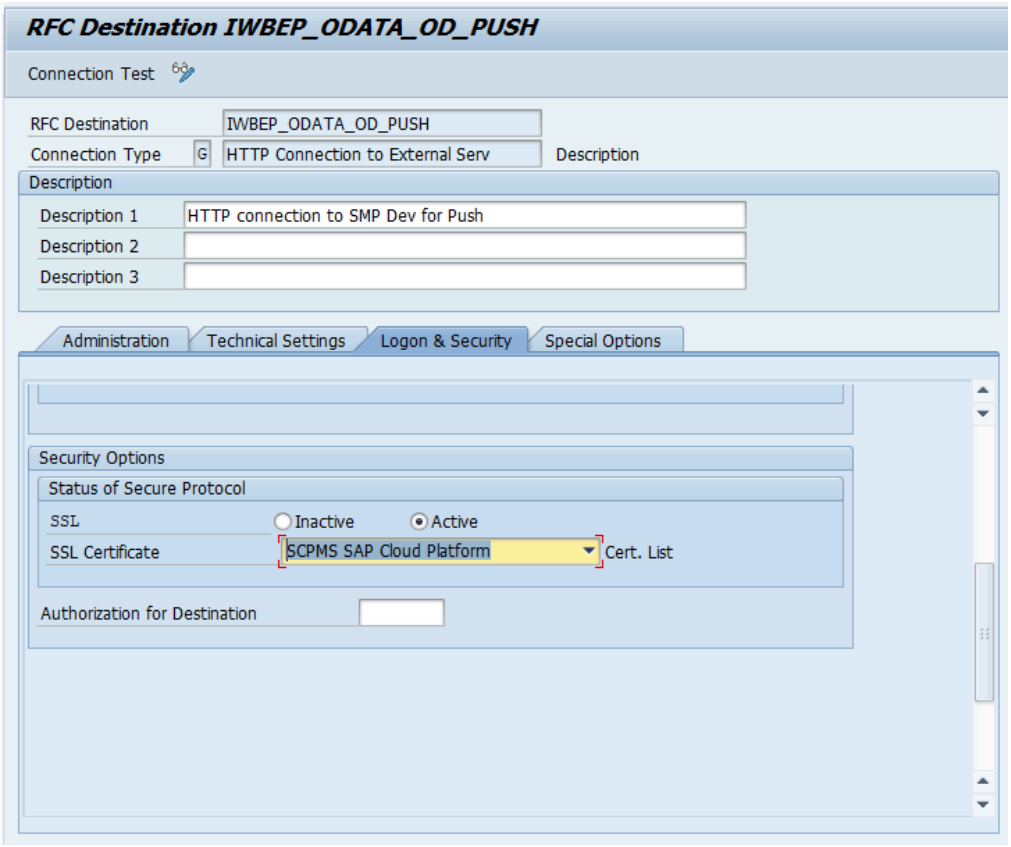
Figure 4-4 Create RFC




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

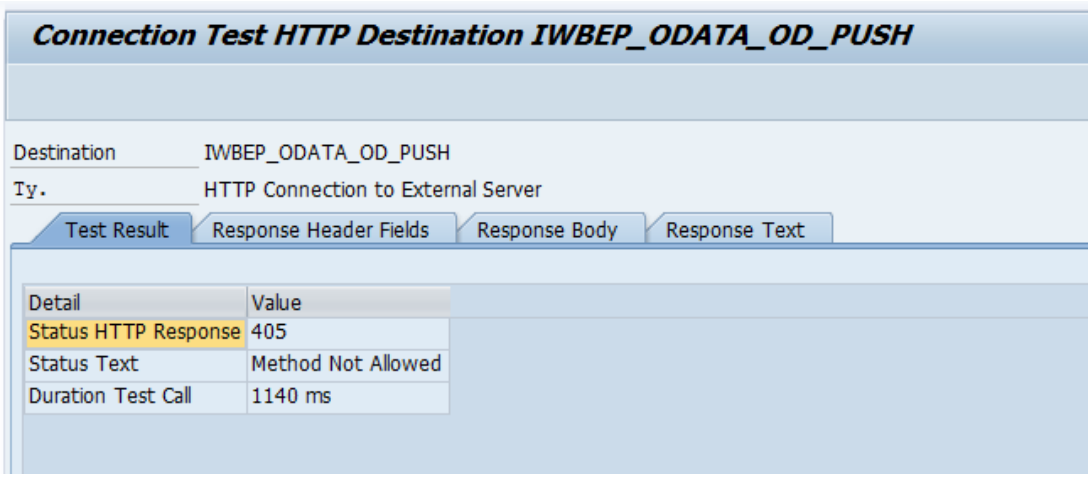
5. In the **Security Options** section, select the SSL Certificate (BTPMS Business Technology Platform) created in Import SAP BTP Certificate to Gateway system *(on page 33)*.

Figure 4-5 Select SSL Certificate




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

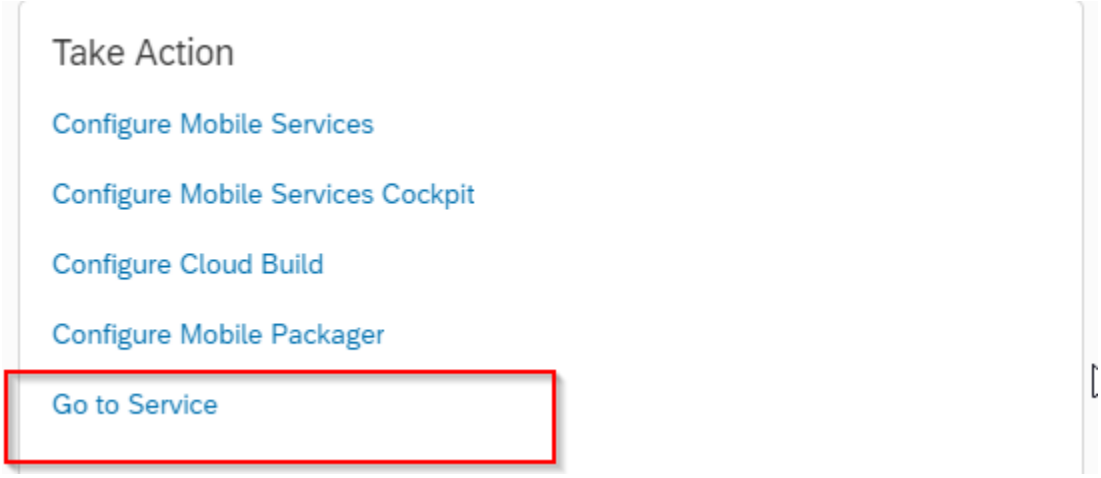
Figure 4-6 HTTP Connection to External Server



## 4.2.3. Configure SAP BTP Applications for Push Notification

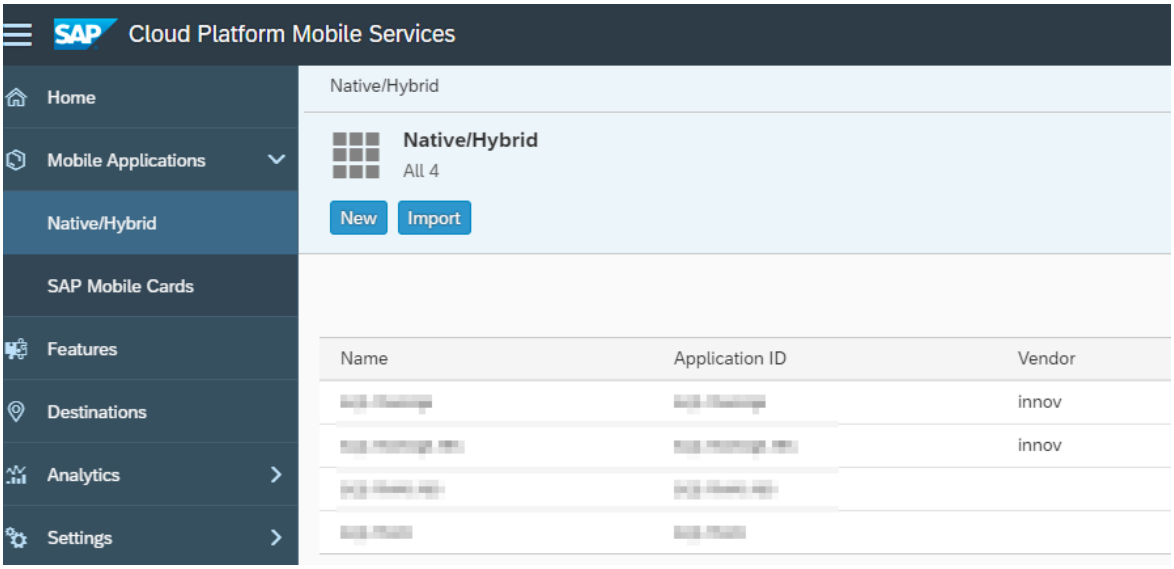
To configure SAP BTP applications for push notification:

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.

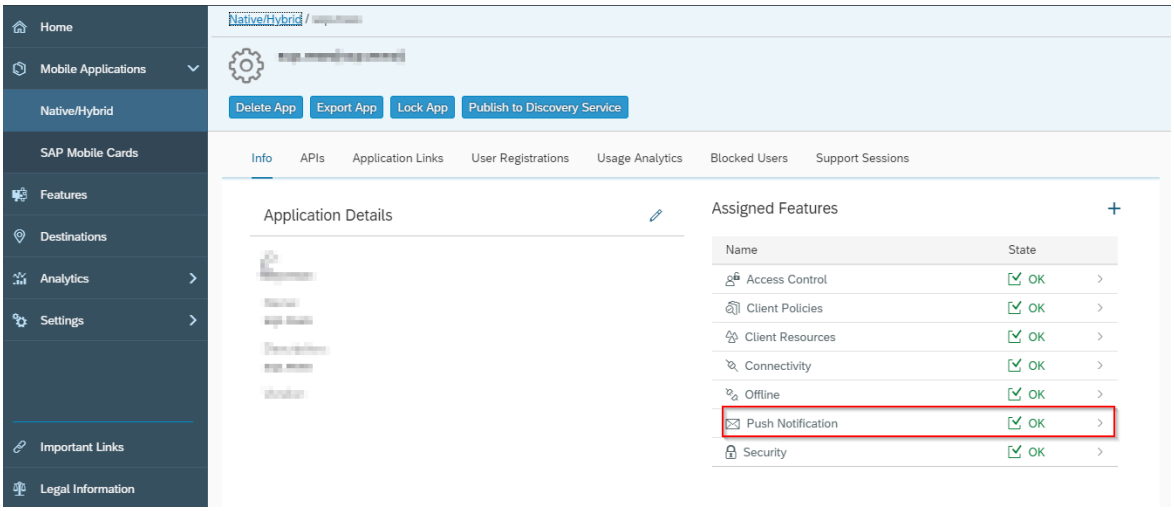



> **Note:**
> Depending on your environment, you could be asked for authentication.

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.

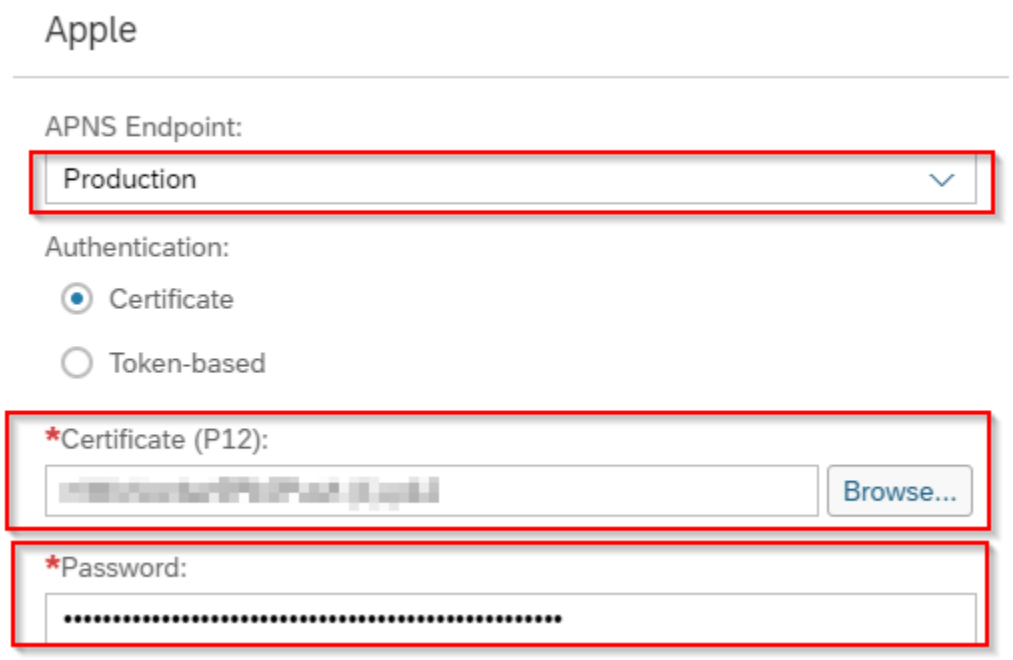



10. In the Application ID Details screen, click **Push Notification**.

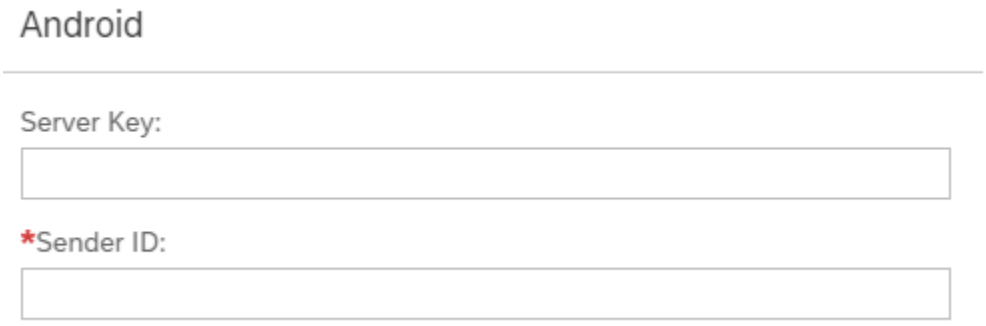



11. Click the **Configuration** tab and do the following:

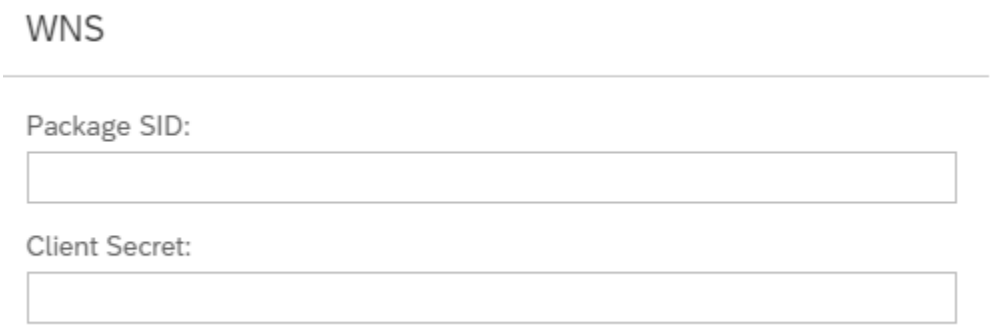
- **iOS Device:** Scroll to option Apple and change the **APNS Endpoint** from *None* to *Sandbox/Production* based on the certificate type. Upload Certificate and save the settings.




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




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




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).

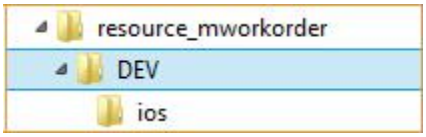
The following topics help you with resource file management:

# 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.




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.

| Property | Description |
|---|---|
| AppName | Helps you identify the Innovapptive product name. |

| Property | Description |
|---|---|
| | ◦ **Conditions:** Use uppercase alphabets.<br>◦ **Possible Values:** Based on the product, refer to the table below. For example, **Mobile Work Order**. |
| Environment | Helps you identify the landscape that the mobile application is connected to. This value is displayed on the Login page of the mobile app.<br>◦ **Conditions:** None<br>◦ **Possible Values:** Development/Quality/Production. |
| ShowDemoButton | ◦ 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.<br>◦ **Conditions:** Use lowercase alphabets.<br>◦ **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 corporate branding needs. Work with your appropriate branding team to identify the color that meets your enterprise palette.<br>**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.<br>◦ **Conditions:** Use the Hex color code value based on the color you would like to see on the mobile app screen elements.<br>◦ **Possible Values:** As required. For example, #42c2f4 |
| OfflineStatusColor | ◦ 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.<br>◦ **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.<br>For example, the parameter value could be configured as "OfflineStatusColor":"#DF264D" in the json file. |

| Property | Description |
|---|---|
| isUnregisterRequired | Set the value as **False** to disable the unregister feature in application. |
| isEULARequired | 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. |
| AppPassCode | Set the value as **True** to enable the **App Passcode** feature in application. |
| ForgotPwd | Set the value as **True** to enable the **Forgot Password** feature in application. |
| ForgotPwdLink | Set the value as **True** to display the website link to reset password. |
| ForgotPwdMsg | Set the value as **True** to display the message to reset password. |

| Property | Description |
|---|---|
| Languages | ◦ 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 necessarytranslations are maintained.<br><br>**Syntax:**<br>`{"id":<SequenceNumber>,"key":"<SAPLanguageCode>","value":"<LanguageName>"}`<br>◦ **Conditions:** Use the Hex color code value based on the color you would like to see on the mobile app screen elements.<br>◦ **Possible Values:** Languages supported by SAP. For example, {"id":1,"key":"E","value":"English"}<br><br>**Note:**<br>For RACE Dynamic Forms, only English language is supported. |
| Timeout | ◦ **Description & Use:** The application idle Timeout (in minutes). This setting allows the administrator to specify the automatic time out when apps are left idle.<br>◦ **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.

| Parameter | Description |
|---|---|
| Server | The DNS/HostName of the SAP BTP servers, which will be used for mobile application connection. For example: scp.innovapptive.com |

| Parameter | Description |
|---|---|
| Port | ◦ The application establishes the communication to the server based on the port number.<br>◦ **Possible Values:** 443. For example, HTTPs (SAP BTP default HTTPs port 443 and custom ports for proxy) |
| ApplicationID | ◦ ID configured in SAP BTP and the mobile application will use it to connect to server for the registration.<br>◦ **Condition:** Use the same application ID as defined in SAP BTP.<br>◦ **Possible Values:** Based on the product, refer to the table below. For example: com.innovapptive.mworkorder. |
| SecurityType | ◦ 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.<br>◦ **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**.<br>◦ **Condition:** Use lowercase alphabets.<br>◦ **Possible Values:** true/false. |
| Whitelist [Application-ID] | All Innovapptive applications require connection settings for RACE services and may also require other connection settings.<br>mWorkOrder application requires connection setting for RACE, EQUIPMENT, FUNCTIONALLOCATION, and ATTACHMENT. For Example, com.innovapptive-.race, mwo.equipment, mwo.funloc and mwo.attach. |
| Whitelist [StoreName] | The name Offline stores for whitelist ApplicationIDs. RACE store is common for all Innovapptive applications.<br>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": "8080",
  "ApplicationID": "com.innovapptive.mworkorder",
  "SecurityType": "SSO2",
  "https": false,
  "AppName":"MWORKORDER",
 "Environment": "Development",
  "ShowDemoButton":true,
  "hcolor":"#445E75",
 "TouchId":true, "AppPassCode":true, "ForgotPwd":true, "ForgotPwdLink":false, "ForgotPwdMsg":"http://www.innovapptive.com/", "StoreName":"",
 "Languages":[{"id":1,"key":"E","value":"English"},{"id":2,"key":"D","value":"German"},{"id":3,"key":"F","value":"French"},
{"id":4,"key":"S","value":"Spanish"},{"id":5,"key":"P","value":"Portuguese"},{"id":6,"key":"1","value":"Chinese"},{"id":7,"key":"M","value":"Thai"}],
 "Timeout":"D30", "Whitelist":[{"ApplicationID": "com.innovapptive.mworace","StoreName":"RACE"},{"ApplicationID": "mwo.equipment","StoreName":"EQUIPMENT"},
{"ApplicationID": "mwo.funloc","StoreName":"FUNCTIONALLOCATION"},{"ApplicationID": "mwo.attach","StoreName":"ATTACHMENT"}]
}
```


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

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

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

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

9. Compress the following files with the updated files from Part 1 & 2 into a zip file with the name **resources_ios.zip**. Ensure that the content and filenames match.
   - App_BG_iPad_Landscape.png
   - App_BG_iPad_Protrait.png
   - App_BG_iPhone.png
   - App_Logo.png
   - settings.json

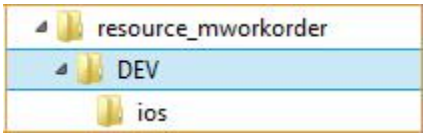
# 5.2. Prepare and Update Resource File for SAP BTP (MWO 2009 SP03 and above releases)

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

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

To prepare and update the resource file:

1. Download the **resources_mworkorder_zip** file to the local drive.
2. Extract the **resource_mmworkorder.zip** file.
   The following folder structure is displayed when you extract.




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


4. 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.

| Property | Description |
|---|---|
| AppName | Helps you identify the Innovapptive product name.<br>◦ **Conditions:** Use uppercase alphabets.<br>◦ **Possible Values:** Based on the product, refer to the table below. For example, **Mobile Work Order**. |

| Property | Description |
|---|---|
| Environment | Helps you identify the landscape that the mobile application is connected to. This value is displayed on the Login page of the mobile app.<br>◦ **Conditions:** None<br>◦ **Possible Values:** Development/Quality/Production. |
| 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.<br>**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.<br>◦ **Conditions:** Use the Hex color code value based on the color you would like to see on the mobile app screen elements.<br>◦ **Possible Values:** As required. For example, #42c2f4 |
| CustomerName | Helps you identify the name of the customer. For example, Innovapptive. |
| OfflineStatusColor | ◦ 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.<br>◦ **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.<br>For example, the parameter value could be configured as "OfflineStatusColor":"#DF264D" in the json file. |
| isEULARequired | Set the value as **False** to disable the EULA agreement screen in application. |
| OnlineOffline | Set the value as **True** to enable the **Online/Offline** feature in application. |

| Property | Description |
|---|---|
| UseDefaultUrl | Set the value as **True** to use the default URL. The default URL is used for internet speed test. Android users connects to the Okla server and iOS users connects to the Apple sever to get the bandwidth value. |
| ForgotPwd | Set the value as **True** to enable the **Forgot Password** feature in application. |
| INVAMBaseURL | Helps you to post the data in INVAM application. For example, http://invam-api.innovapptive.com:6001. |
| SessionTimeout | ◦ **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.<br>◦ **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. |
| ForgotPwdMsg | Set the value as **True** to display the message to reset password. |
| StoreName | Helps you to identify the store name.<br>◦ **Conditions:** None<br>◦ **Possible Values:** WORKORDER |
| StoreDescription | Helps you to identify the description regarding the store name.<br>◦ **Conditions:** None<br>◦ **Possible Values:** General |
| StoreIndex | Helps you to identify the index value of the store name and the order is in ascending order.<br>◦ **Conditions:** None<br>◦ **Possible Values:**1 or 2 |

| Property | Description |
|---|---|
| Store-Type | Helps you to identify the type of the store.<br>◦ **Conditions:** None<br>◦ **Possible Values:** T |
| Languages | ◦ 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 necessarytranslations are maintained.<br><br>**Syntax:**<br>`{"id":<SequenceNumber>,"key":"<SAPLanguageCode>","value":"<LanguageName>"}`<br>◦ **Conditions:** Use the Hex color code value based on the color you would like to see on the mobile app screen elements.<br>◦ **Possible Values:** Languages supported by SAP. For example, {"id":1,"key":"E","value":"English"}<br><br>**Note:**<br>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.<br>◦ **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.

| Parameter | Description |
|---|---|
| Server | The DNS/HostName of the SAP BTP servers, which will be used for mobile application connection. For example: scp.innovapptive.com |
| Port | ◦ The application establishes the communication to the server based on the port number.<br>◦ **Possible Values:** 443. For example, HTTPs (SAP BTP default HTTPs port 443 and custom ports for proxy) |
| ApplicationID | ◦ ID configured in SAP BTP and the mobile application will use it to connect to server for the registration.<br>◦ **Condition:** Use the same application ID as defined in SAP BTP.<br>◦ **Possible Values:** Based on the product, refer to the table below. For example: com.innovapptive.mworkorder. |
| SecurityType | ◦ 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.<br>◦ **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**.<br>◦ **Condition:** Use lowercase alphabets.<br>◦ **Possible Values:** true/false. |
| Whitelist [Application-ID] | All Innovapptive applications require connection settings for RACE services and may also require other connection settings.<br>mWorkOrder application requires connection setting for RACE, EQUIPMENT, FUNCTIONALLOCATION, and ATTACHMENT. For Example, com.innovapptive-.race, mwo.equipment, mwo.funloc and mwo.attach. |

| Parameter | Description |
|---|---|
| Whitelist [StoreName] | The name Offline stores for whitelist ApplicationIDs. RACE store is common for all Innovapptive applications.<br><br>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": "8080",
  "ApplicationID": "com.innovapptive.mworkorder",
  "SecurityType": "SSO2",
  "https": false,
  "AppName":"MWORKORDER",
 "Environment": "Development",
  "ShowDemoButton":true,
  "hcolor":"#445E75",
 "TouchId":true, "AppPassCode":true, "ForgotPwd":true, "ForgotPwdLink":false, "ForgotPwdMsg":"http://www.innovapptive.com/", "StoreName":"",
 "Languages":[{"id":1,"key":"E","value":"English"},{"id":2,"key":"D","value":"German"},{"id":3,"key":"F","value":"French"},
{"id":4,"key":"S","value":"Spanish"},{"id":5,"key":"P","value":"Portuguese"},{"id":6,"key":"1","value":"Chinese"},{"id":7,"key":"M","value":"Thai"}],
 "Timeout":"D30", "Whitelist":[{"ApplicationID": "com.innovapptive.mworace","StoreName":"RACE"},{"ApplicationID": "mwo.equipment","StoreName":"EQUIPMENT"},
{"ApplicationID": "mwo.funloc","StoreName":"FUNCTIONALLOCATION"},{"ApplicationID": "mwo.attach","StoreName":"ATTACHMENT"}]
}
```


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:

| | |
|---|---|
| Config Templates | Native |
| 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 |
| Vendor | Innovapptive Inc. |

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

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.

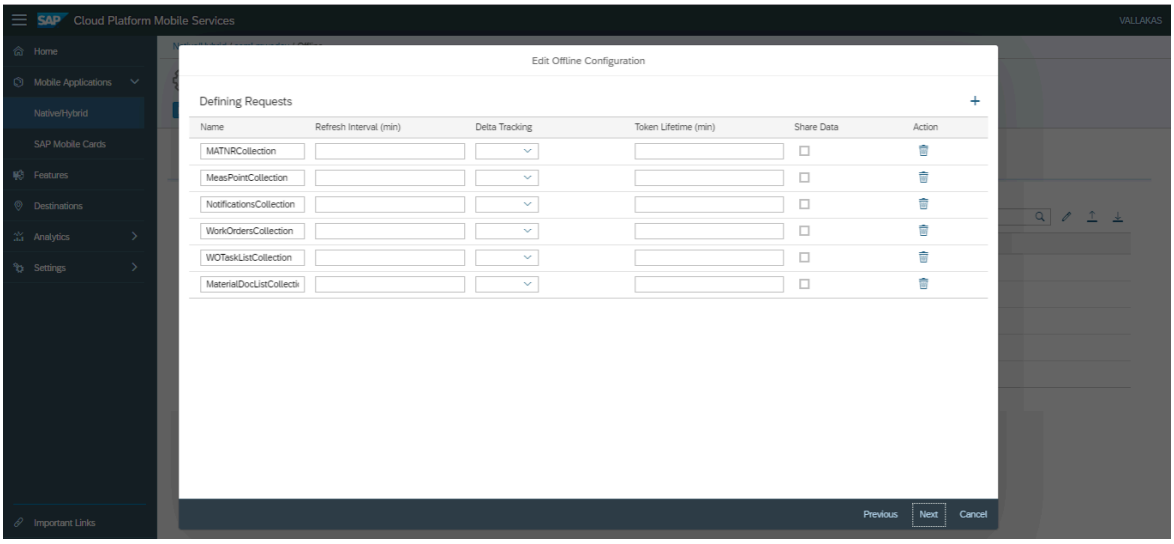
```
[endpoint]

name=fit.mwo

prepopulate_offline_db=N

request_format=application/json;q=1,application/atom+xml;q=0.5

delta_request_format=application/atom+xml

batch_all_defining_queries=N

case_sensitive_offline_db=N

offline_db_collation=UTF8BIN

local_change_expiry=0

content_id_header_location=mime

allow_omitting_max_length_facet=N
```

```
json_datetimeoffset_in_utc=Y

max_delta_resends=0


[defining_query]

name=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
```

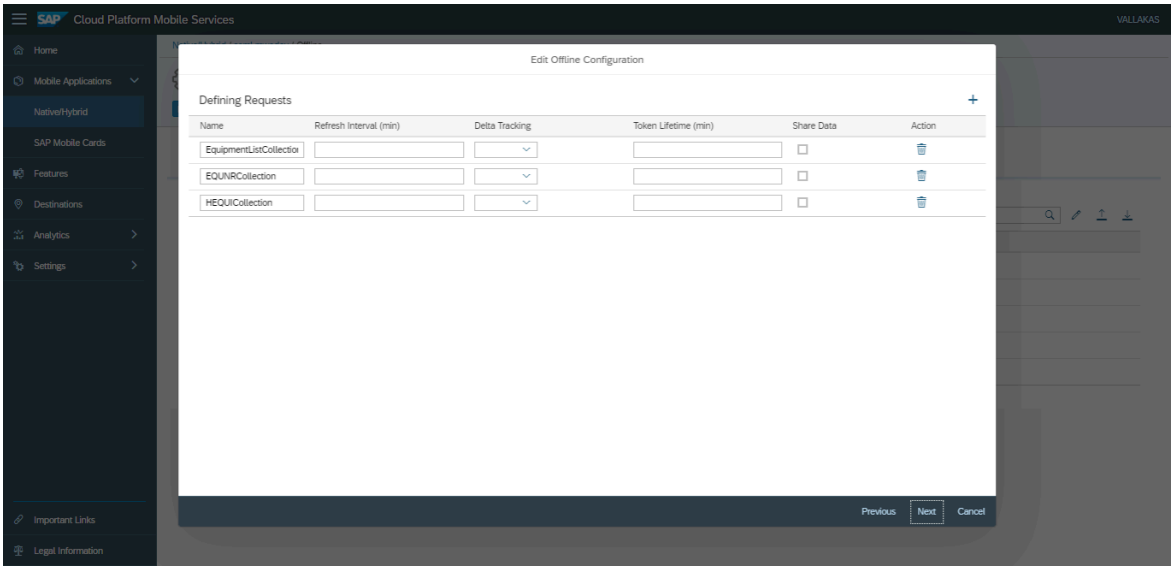
```
allow_omitting_max_length_facet=N

json_datetimeoffset_in_utc=Y

max_delta_resends=0


[defining_query]

name=EquipmentListCollection

is_shared_data=N


[defining_query]

name=EQUNRCollection

is_shared_data=N


[defining_query]

name=HEQUICollection

is_shared_data=N


[endpoint]

name=fit.mwo.funloc

prepopulate_offline_db=N

request_format=application/json;q=1,application/atom+xml;q=0.5

delta_request_format=application/atom+xml

batch_all_defining_queries=N

case_sensitive_offline_db=N

offline_db_collation=UTF8BIN

local_change_expiry=0

content_id_header_location=mime

allow_omitting_max_length_facet=N

json_datetimeoffset_in_utc=Y

max_delta_resends=0


[defining_query]

name=FunctionalLocCollection

is_shared_data=N


[defining_query]

name=TPLNRCollection

is_shared_data=N
```

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

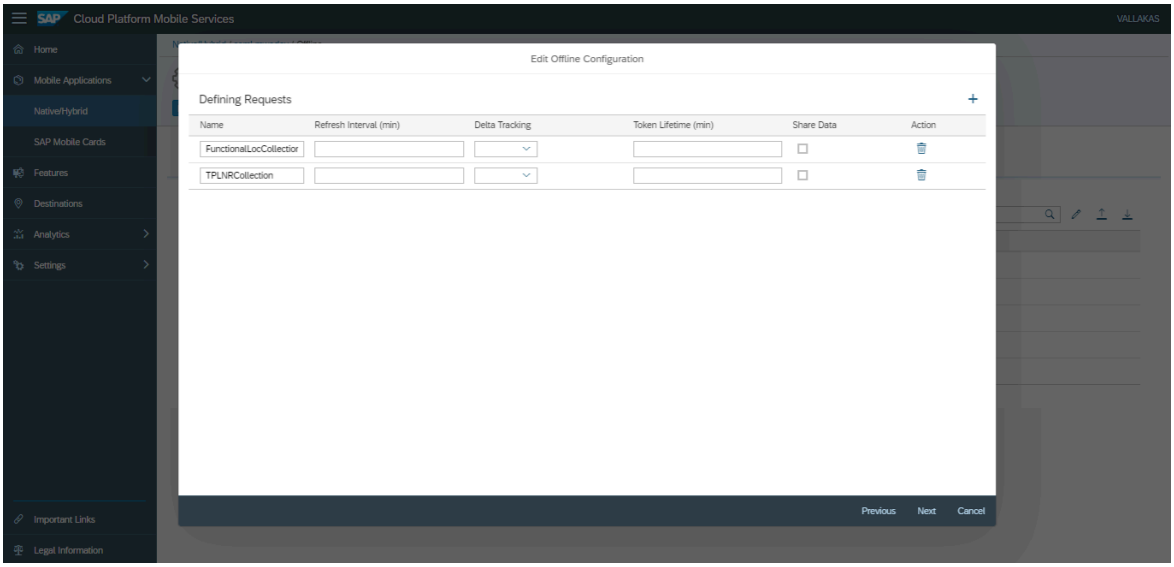
**For mWorkOrder Service:**




**For Equipment:**




**For Functional Location:**




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:



## 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.

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

| Role Name | Description | Transactions | Authorization 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 6-2 Roles for NetWeaver Gateway System**

| Role Name | Description | Authorizations |
|---|---|---|
| ZINV_MWO_NWG_END_-USER_R2208 | Innovapptive mWorkOrder - End User - Gateway Authorizations - 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 Authorizations – 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)<br>**IWSV** (Gateway Business Suite Enablement – Service) |
| Object Name | /INVMWO/MWORKORDER_SRV*,<br>/INVCEC/RACE_SRV*,<br>/INVMWO/MWOFUNLOCATION_SRV*,<br>/INVMWO/MWOEQUIPMENT_SRV*,<br>/INVMWO/WOATTACHMENTS_SRV*<br>/INVMWO/MWOOPERATORROUND_SRV* |

Figure 6-1 USOBHASH table

| Name | Test | PgID | Obj. | Object Name | Type of External Service | External Service |
|---|---|---|---|---|---|---|
| BFE4EB47E83C95CC870C1B4C8756FF | HT | R3TR | IWSV | /INVCEC/RACE_SRV 0001 | | |
| 647CD51054EB07807FA882F5125B6F | HT | R3TR | IWSG | /INVCEC/RACE_SRV_0001 | | |
| F28DC3F6B0D44FE351371A672A60C3 | HT | R3TR | IWSV | /INVMWO/MWOEQUIPMENT_SRV 0001 | | |
| ED826173F9F64734D4691430AE2315 | HT | R3TR | IWSG | /INVMWO/MWOEQUIPMENT_SRV_0001 | | |
| EE0833A59F955E9C27877CBF968BC0 | HT | R3TR | IWSV | /INVMWO/MWOFUNLOCATION_SRV 0001 | | |
| C6286783FC1B5B35274BC45838B5E8 | HT | 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

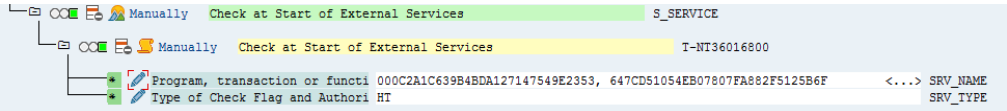
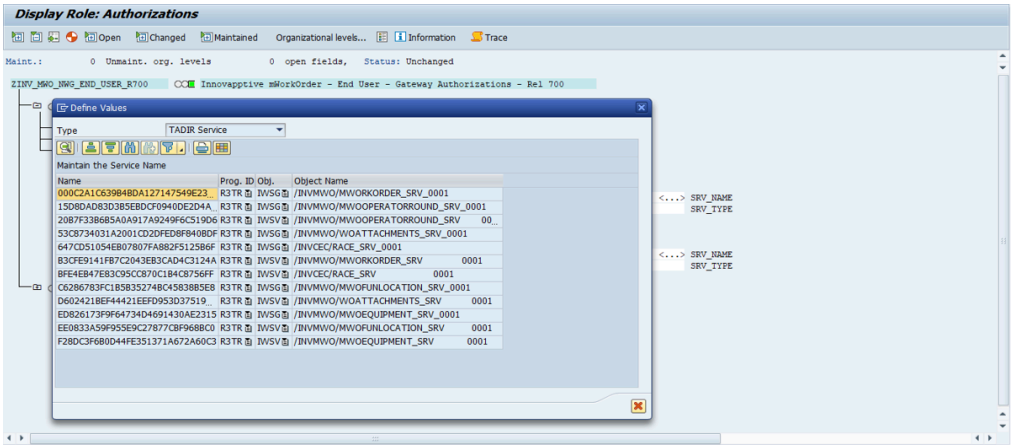



Figure 6-3 Display Role Authorization




## 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**

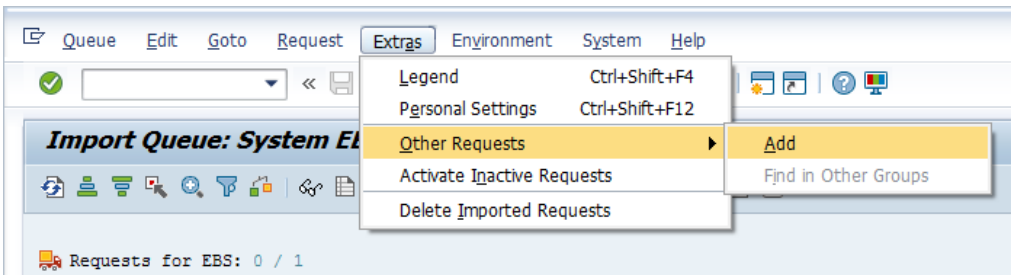
| Transport | Description | Dependency |
|---|---|---|
| NGTK909710 | Innov Gateway R 2208 mworkorder Application End user Roles | None |

## 6.2.3. Import roles using Transports

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

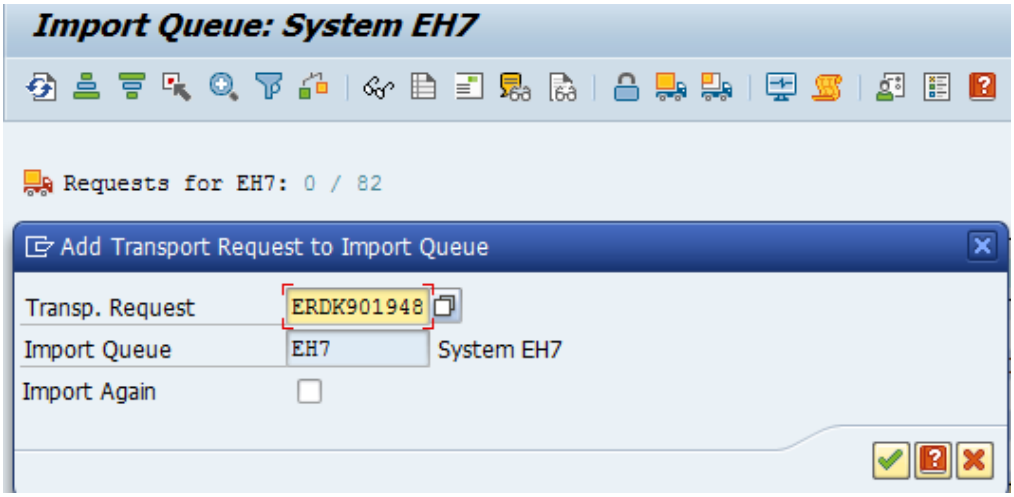
1. Extract the zip or .rar files that you received from Innovapptive and save the files to your local machine.
2. Extract and upload/copy the files to the SAP ECC & GW System Directories.
    a. Extract the zip files and copy all co-files (files starting with 'K902*') from software deployment package 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



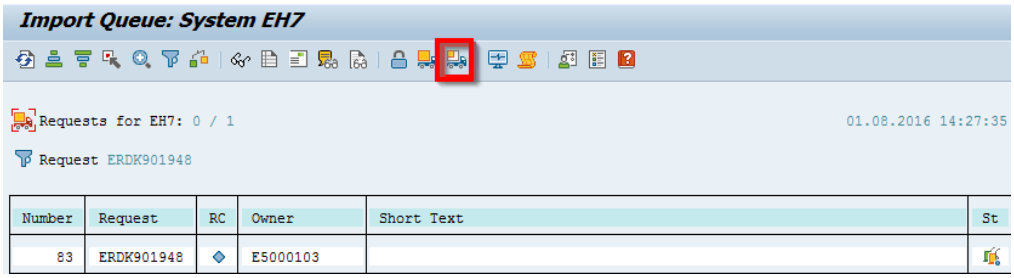
6. Enter the transport number in the **Transp. Request** field and confirm by pressing the **ENTER** key (or click the green-colored icon) to attach transports to the import queue.

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




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

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

## 6.3. SAP Authorizations for mInventory users

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

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

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

**Table 6-6 Roles for ECC System**

| Role Name | Description | Transactions | Authorization Objects |
|---|---|---|---|
| ZINV_MIM_ECC_-END_USER_R2212 | mInventory - End User - ECC Authorizations - Release 2212 | MB1A, MB1B, MB1C, ME29N, ME51N, ME52N, 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 | S_RFC, S_RFCACL |

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

| Role Name | Description | Authorizations |
|---|---|---|
| ZINV_MIM_NWG_END_-USER_R2212 | mInventory - End User - Gateway Authorizations - Release 2212 | S_RFC, S_RFCACL, S_SERVICE, S_USER_GRP & S_TABU_DIS |

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

| Role Name | Description | Transactions | Authorizations |
|---|---|---|---|
| ZINV_MIM_RLM_-END_USER_R2009 | mInventory - End User - RLM Authorizations - Release 2009 | /NSCWM/PRDI,O3O_-PACK01,O3O_-PACK03,O3O_PACK05 | S_RFC, S_RFCACL |
| ZINV_MIM_RLM_-RACE_ADM_R2009 | mInventory - RACE Admin - RLM Authorizations – 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 Authorizations - Release 2009 | /SCWM/MAT1<br>/SCWM/TODLV_I<br>/SCWM/PRDI<br>/SCWM/MON<br>/SCWM/TODLV_M<br>/SCWM/TODLV_O<br>/SCWM/PRDO<br>SMQ1<br>SMQ2<br>/SCWM/IDN<br>/SCWM/TODLV_T<br>/SCWM/PRFIXBIN<br>/SCWM/PRBIN<br>/SCWM/TO_CONF | S_RFC, S_RFCACL |

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

| Role Name | Description | Transactions | Authorizations |
|---|---|---|---|
| | | /SCWM/PACK<br>/SCWM/LOAD<br>/SCWM/UNLOAD<br>/SCWM/ADHU<br>/SCWM/PI_PROCESS | |
| ZINV_MIM_EWM_-RACE_ADM_R2009 | mInventory - RACE Admin - EWM Authorizations – Release 2009 | | S_RFC, S_RFCACL |

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:

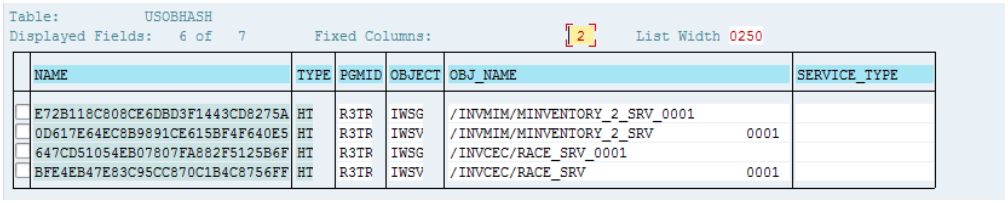
1. Go to **SE16/SE16N** or **SE11** and open the table **USOBHASH**.
2. Enter this information:

**Table 6-10 S_SERVICE values**

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

| | |
|---|---|
| | /INVCEC/RACE_SRV*, |

Figure 6-7 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.

Figure 6-8 Hashed Service Name

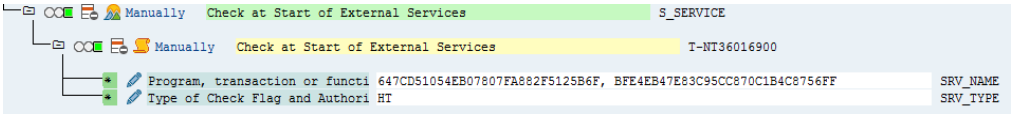
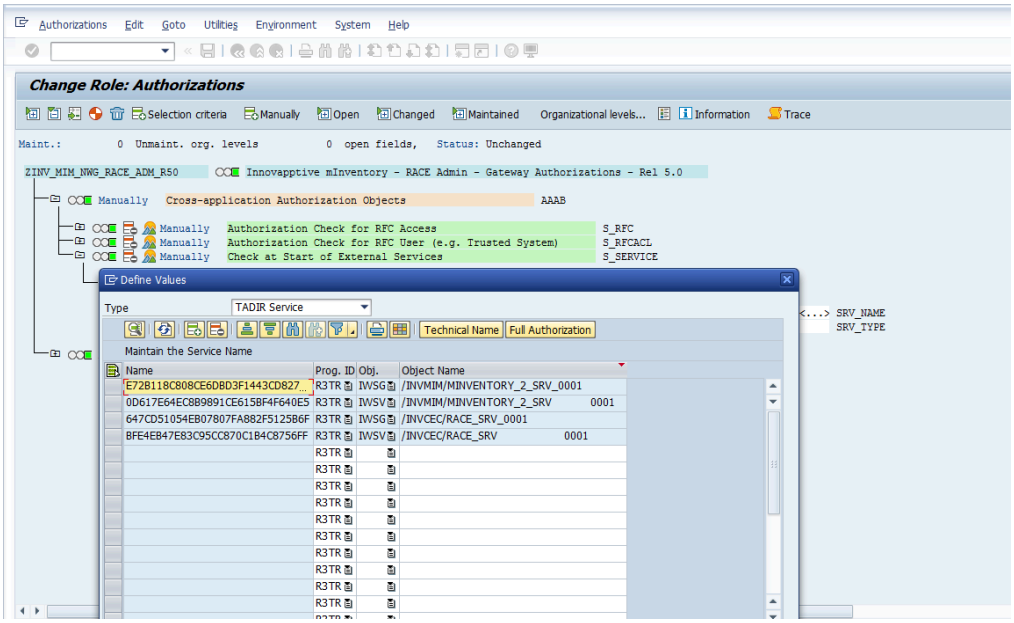



Figure 6-9 Change Role Authorization




## 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 Minventory Application End User Roles | None |

**Table 6-13 SAP RLM Transports**

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

**Table 6-14 SAP EWM Transports**

| Transport | Description | Dependency |
|---|---|---|
| H18K900227 | INNOV:EWM: R 2206 mInventory Application End User Roles | None |

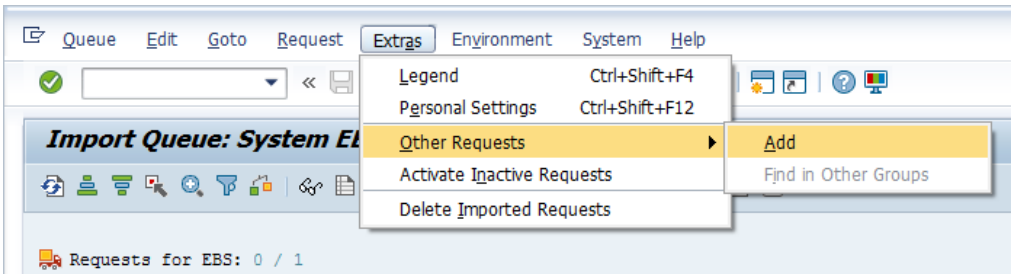
## 6.3.3. Import roles using Transports

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.

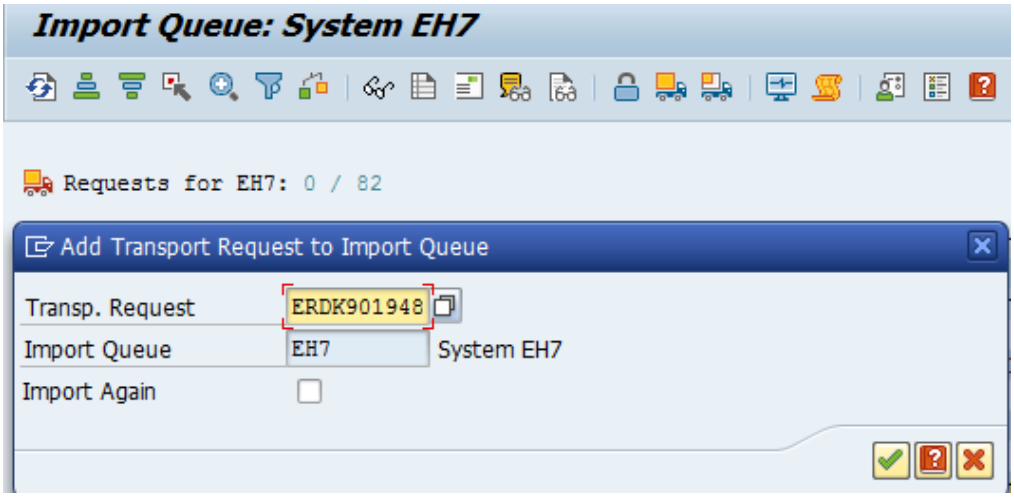
3. Log in to the SAP GW & ECC System (based on the transport being imported).
4. Navigate to the transaction code **STMS_Import**.
5. Navigate to **Extras**, **Other Requests**, **Add**.

Figure 6-10 Import Queue



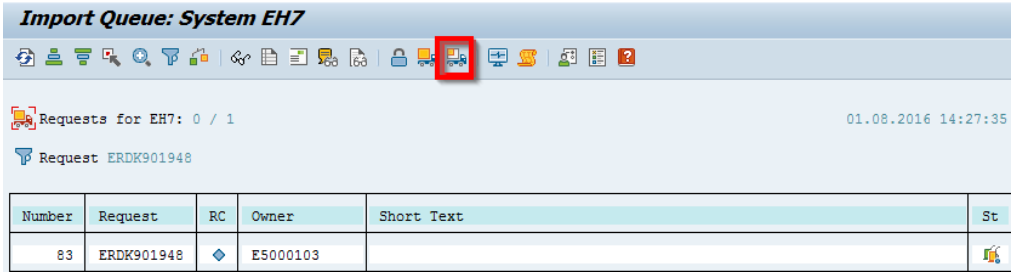

6. Enter the transport number in the **Transp. Request** field and confirm by pressing the **ENTER** key (or click the green-colored icon) to attach transports to the import queue.

Figure 6-11 Add Transport Request to Import Queue




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




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.

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

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

**Table 6-16 mAssetTag ECC Authorizations**

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

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

| User | Authorization Object | Authorizations |
|---|---|---|
| | S_RFCACL | • ACTVT = 16<br>• RFC_EQUSER = Y |

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

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

**Table 6-17 mAssetTag NetWeaver Gateway Authorizations (continued)**

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

**Table 6-17 mAssetTag NetWeaver Gateway Authorizations (continued)**

| User | Authorization Object | Authorizations |
|---|---|---|
| | S_RFCACL | • ACTVT = 16<br>• RFC_EQUSER = Y |

## 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)<br>**IWSV** (Gateway Business Suite Enablement – Service) |
| Object Name | /INVCEC/* and /INVMAT/* |

Figure 6-13 USOBHASH table

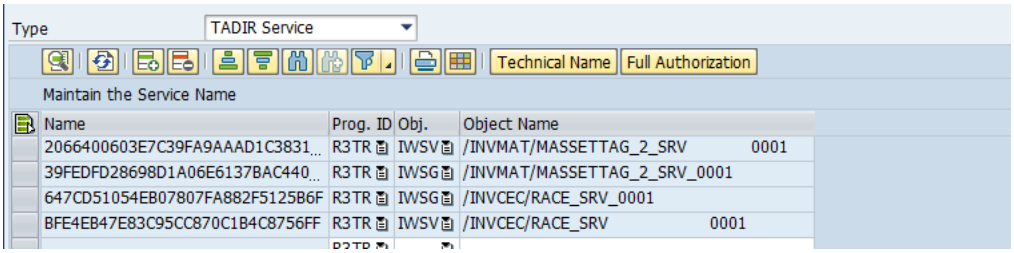
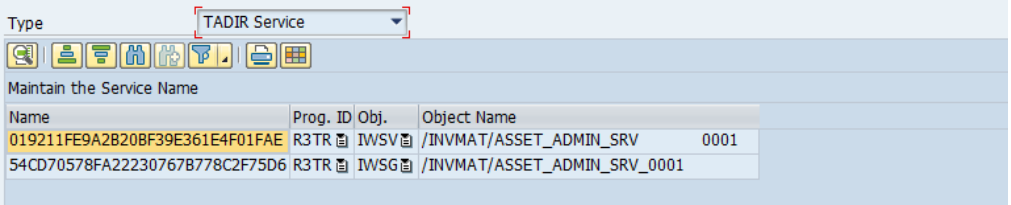
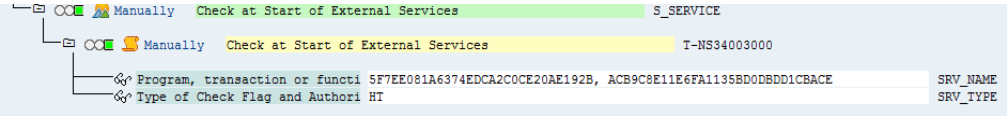


Figure 6-14 USOBHASH table



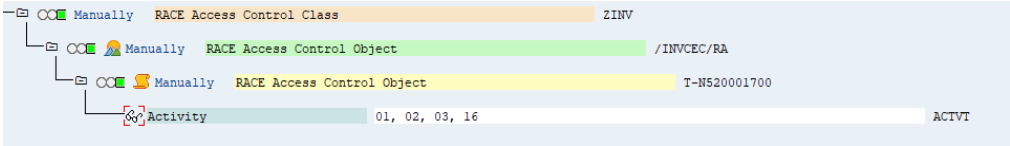

3. Pick the names of the hashed services (the 30-character length alpha numerical name) and use them under S_SERVICE - SRV_NAME.

Figure 6-15 Hashed Service Name




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

Figure 6-16 Hashed Service Name




## 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 | Authorization Objects |
|---|---|---|---|
| ZINV_RDF_ECC_-END_USER_R2203 | Innovapptive RACE Dynamic Forms - End User - ECC Authorizations - Release 2203 | /INVMGO/DOCFORM | S_RFC, S_RFCACL |
| ZINV_RDF_ECC_-RACE_ADM_R2203 | RACE Dynamic Forms - RACE Admin - ECC Authorizations – Release 2203 | | S_RFC and S_RFCACL |

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

| Role Name | Description | Authorizations |
|---|---|---|
| ZINV_RDF_NWG_END_-USER_R2203 | RACE Dynamic Forms - End User - Gateway Authorizations – Release 2203 | S_RFC, S_RFCACL, S_SERVICE, S_USER_GRP |
| ZINV_RDF_NWG_RACE_ADM_R2203 | RACE Dynamic Forms - RACE Admin - Gateway Authorizations – 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.

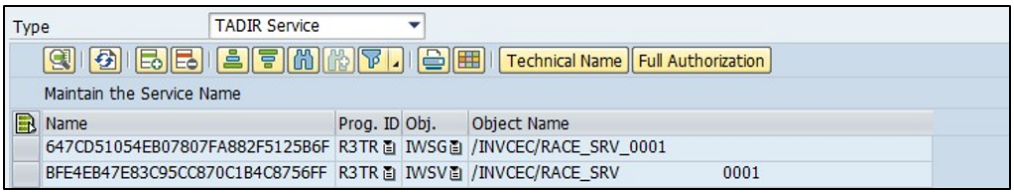
To update service values under S_SERVCE:

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*, |

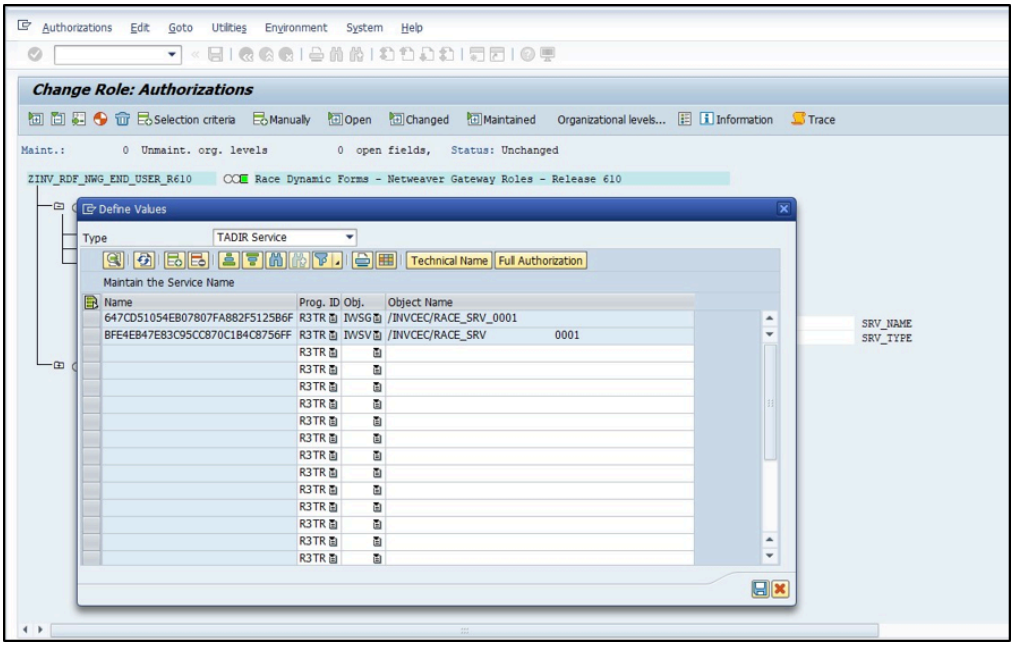
Figure 6-17 USOBHASH table




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


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 Application End User Roles | None |

**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 features |