Post-Install or Post-Upgrade Configurations Guide 2009

Connected Worker Solutions

INNOVAPPTIVE

Title and Copyright

Copyright and **Terms of Use** for the Post Install or Post Upgrade Configurations Guide for mAssetTag, mWorkOrder, mInventory, mServiceOrder, mWorkList and all other solutions of *Connected Workforce Platform*^{TM} .

The Post Install or Post Upgrade Configurations Guide for mAssetTag, mWorkOrder, mInventory, mServiceOrder, mWorkList and all other solutions of *Connected Workforce Platform*^{TM}

Product Version: *2009 SP03*

Document Version: *1.0*

Published Date: *29 June 2021*

Revised Date: *29 June 2021*

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 placeholder variables for which you supply values.
`monospace`	Indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Related Products

- 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 both SCP and SMP environments. Depending on the platform you are on, choose your configuration path.

- If you are using SCP, check SCP Configurations after Installing Innovapptive Products *(on page 11)* for configuration instructions.
- If you are using SMP, check SMP Configurations after Installing Innovapptive Products *(on page 65)* for configuration instructions.

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 configurations after you install the following Innovapptive products:

Table 1-1 Innovapptive Products

Product	Version (Release/HF)
mServiceOrder	6.1.0
mShop	6.1.0
mWorklist	5.1.0
mWorkOrder	7.0.0
mWorkOrder	7.1.0
mAssetTag	7.2.0
mWorkOrder	7.2.0
mInventory	7.2.0
mAssetTag	7.3.0

Table 1-1 Innovapptive Products (continued)

Product	Version (Release/HF)
mWorkOrder	7.3.0
mInventory	7.3.0
mAssetTag	7.4.0
mInventory	7.4.0
mWorkOrder	7.4.0
mAssetTag	2003
mInventory	2003
mWorkOrder	2003
mAssetTag	2006
mInventory	2006
mAssetTag	2006
mInventory	2006
mWorkOrder	2006

2. SCP Configurations after Installing Innovapptive Products

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

Figure 2-1 Workflow for SCP configurations after Instllaing Innovapptive Products

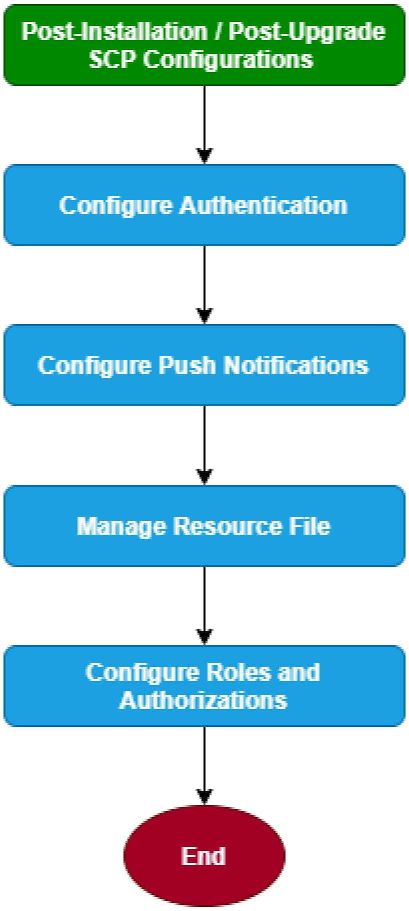

Post-Installation / Post-Upgrade SCP Configurations
Configure Authentication
Configure Push Notifications
Manage Resource File
Configure Roles and Authorizations
End

Table 2-1 Tasks for SMP Configurations after Instllaing Innovapptive Products

Task	Reference to section
Configure authentication for mobile application	• Configure HTTP/HTTPs Authentication *(on page 12)* • Configure SAML Authentication *(on page 16)* • Integrate SCP with Azure AD *(on page 31)*

Table 2-1 Tasks for SMP Configurations after Instllaing Innovapptive Products (continued)

Task	Reference to section
Configure SCP for Push Notifications	Configure Push Notifications for SCP *(on page 32)*
Prepare and update resource file	Manage Resource File in SCPms *(on page 44)*
Configure roles and authorizations	Configure Roles and Authorization for Products *(on page 141)*

2.1. Configure HTTP/HTTPs Authentication

Configure Innovapptive products on SCP 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 authenticatione, ensure you have:

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

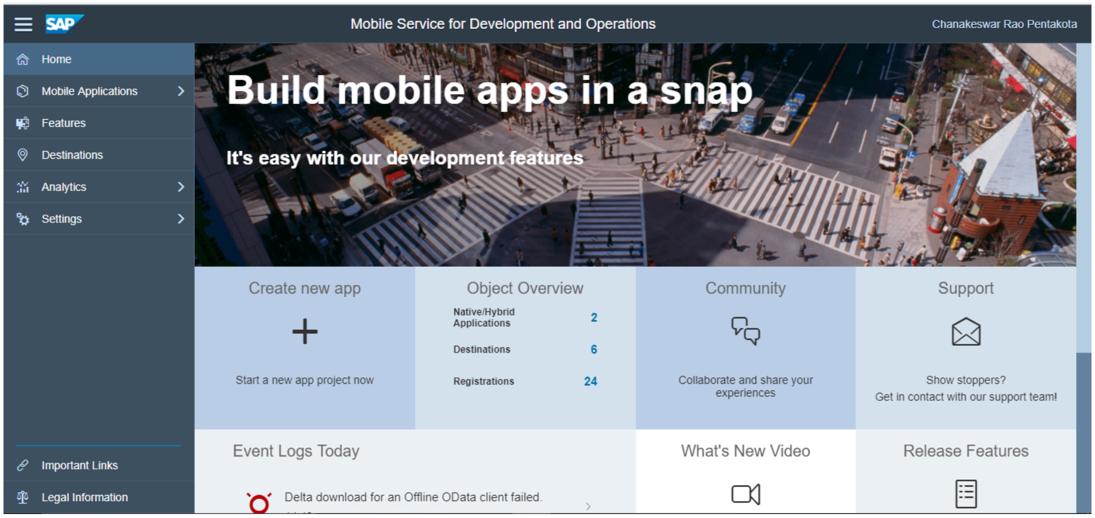
2.1.1. About SCPms

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 2-2 Mobile Services Management Cockpit


SAP
Mobile Service for Development and Operations
Chanakeswar Rao Pentakota
Home
Mobile Applications
Features
Destinations
Analytics
Settings
Important Links
Legal Information
Build mobile apps in a snap
It's easy with our development features
Create new app
Start a new app project now
Object Overview
Native/Hybrid Applications 2
Destinations 6
Registrations 24
Community
Collaborate and share your experiences
Support
Show stoppers?
Get in contact with our support team!
Event Logs Today
What's New Video
Release Features

Delta download for an Offline OData client failed.

2.1.2. 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 **SCP** 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:

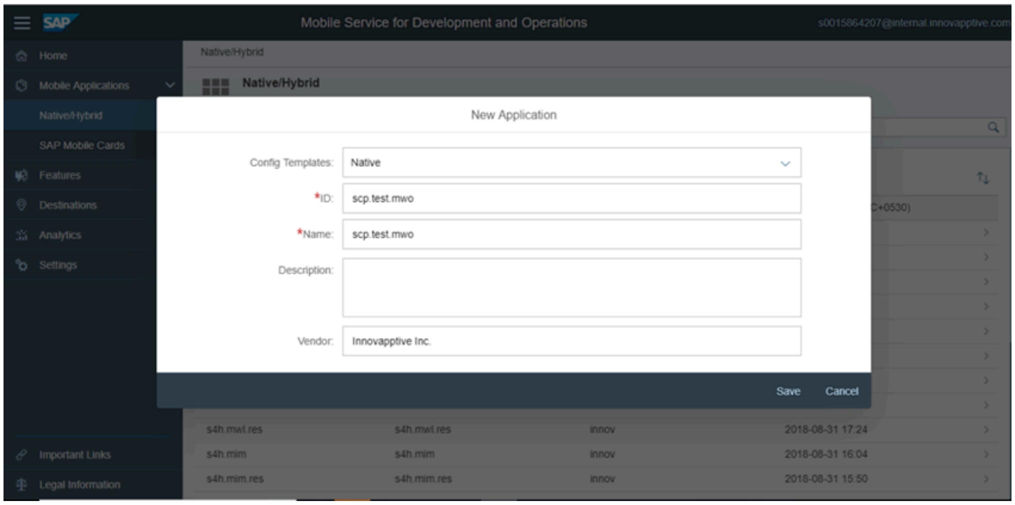
1. Expand **Mobile Applications** on the left navigation.
2. Click **Native/Hybrid** under Mobile Applications.
3. Click **New**.
4. Enter details such as **Application ID**.
   Use the information in the table to add new application details for the product you purchased.

Product	App ID	Name	Type	Vendor	Security Configuration
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

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 2-3 Create New Application



New Application

Config Templates: Native

*ID: scp.test.mwo

*Name: scp.test.mwo

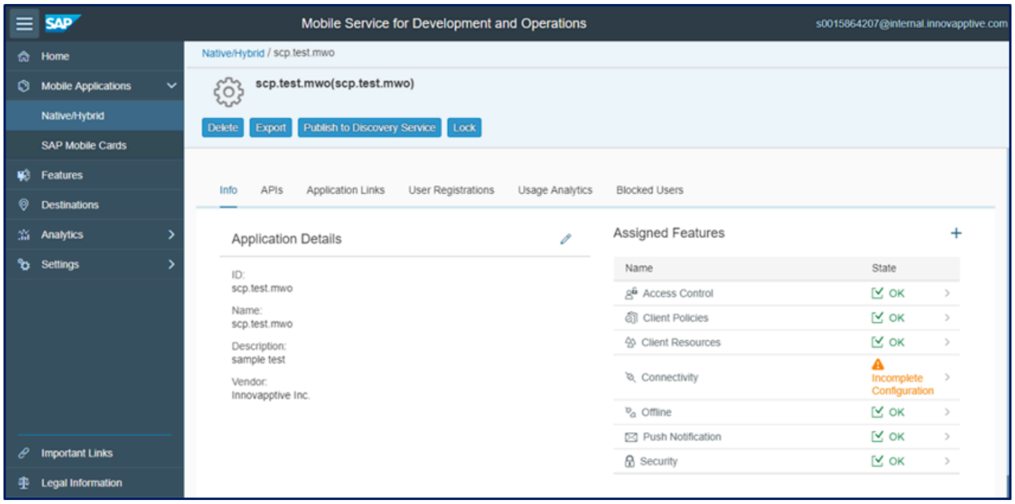
Description:

Vendor: Innovapptive Inc.

s4h.mwl.res	s4h.mwl.res	innov	2018-08-31 17:24
s4h.mim	s4h.mim	innov	2018-08-31 16:04
s4h.mim.res	s4h.mim.res	innov	2018-08-31 15:50

6. Click **Save**.

Figure 2-4 Application Details



Application Details

ID:
scp.test.mwo

Name:
scp.test.mwo

Description:
sample test

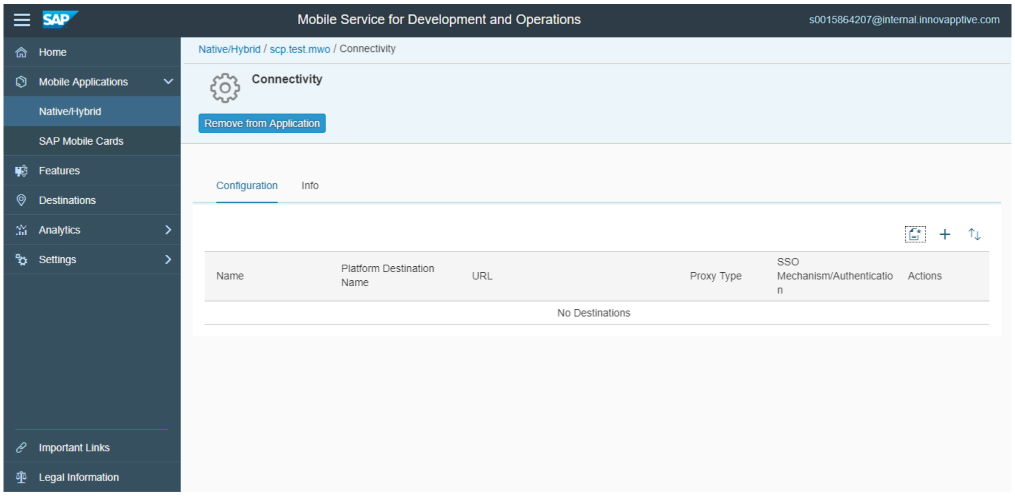
Vendor:
Innovapptive Inc.

Assigned Features

Name	State
Access Control	OK
Client Policies	OK
Client Resources	OK
Connectivity	Incomplete Configuration
Offline	OK
Push Notification	OK
Security	OK

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

Figure 2-5 Application Connectivity



Name	Platform Destination Name	URL	Proxy Type	SSO Mechanism/Authentication	Actions
		No Destinations			

- **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/
mServiceOrder	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 SCP Development & Operations configurations for Basic Authentication.

2.2. Configure SAML Authentication

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

Before you configure, ensure:

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

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

2.2.1. Establish trust between SCP and ADFS

To establish trust between SCP and ADFS:

1. Log in to SAP Cloud Platform (SCP).
2. Go to **SCP 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 SCP. 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.

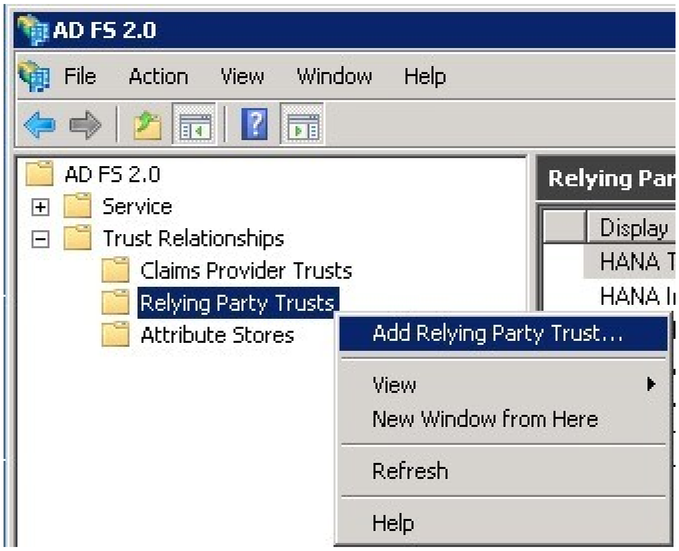
2.2.2. Add SCP Metadata to ADFS

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

To establish Mutual Trust between SCP 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**.

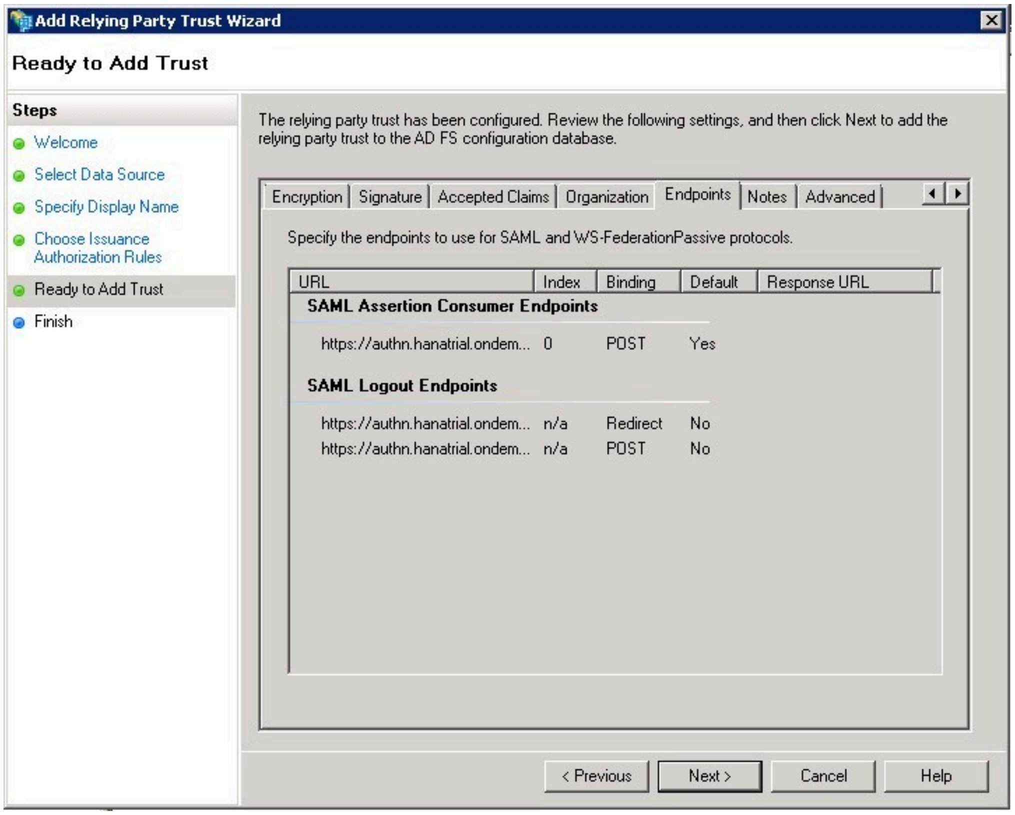
Figure 2-6 ADFS Relying Party Trusts



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 2-7 Relying Party Trust Wizard



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.

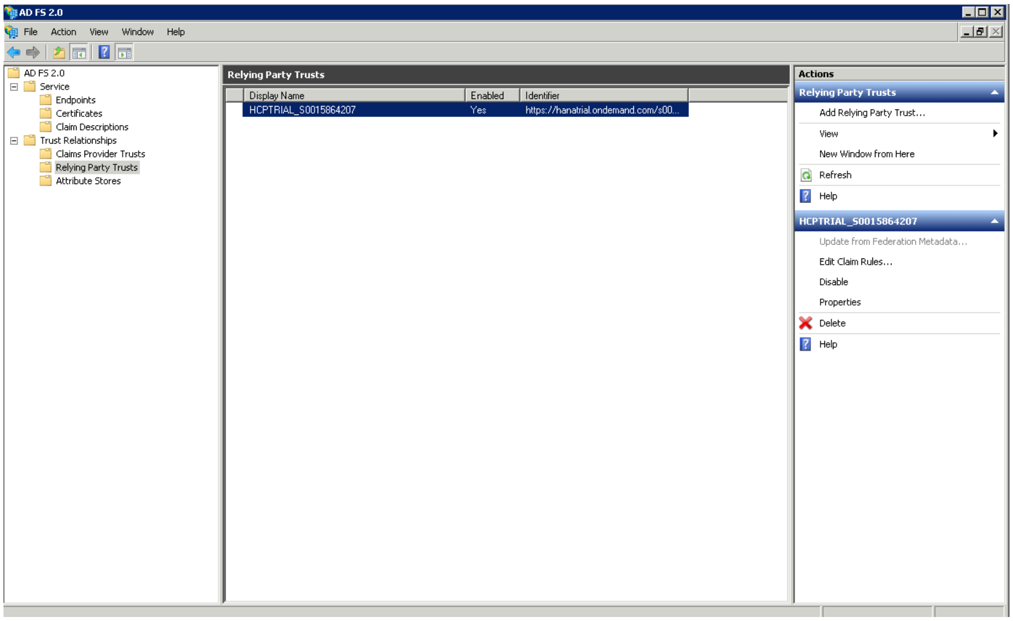
Specify the endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	Binding	Default	Response URL
SAML Assertion Consumer Endpoints				
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	

9. Click **Next.**
10. Click **Close**. The **Claim Rule Editor** window opens.

    If you do not remove the check box active, you will continue further to post user creations.
11. After adding the SCP Metadata to ADFS, add Claim Rules to accept username and password and send the required assertion tokens after validations.
12. Go to ADFS Management Console, select **Relying Party Trusts** and select the entry. In this case, it is **SCPTRIAL_S00XXXXX**.
13. Click **Edit Claim Rules**.

Figure 2-8 Edit Claim Rules

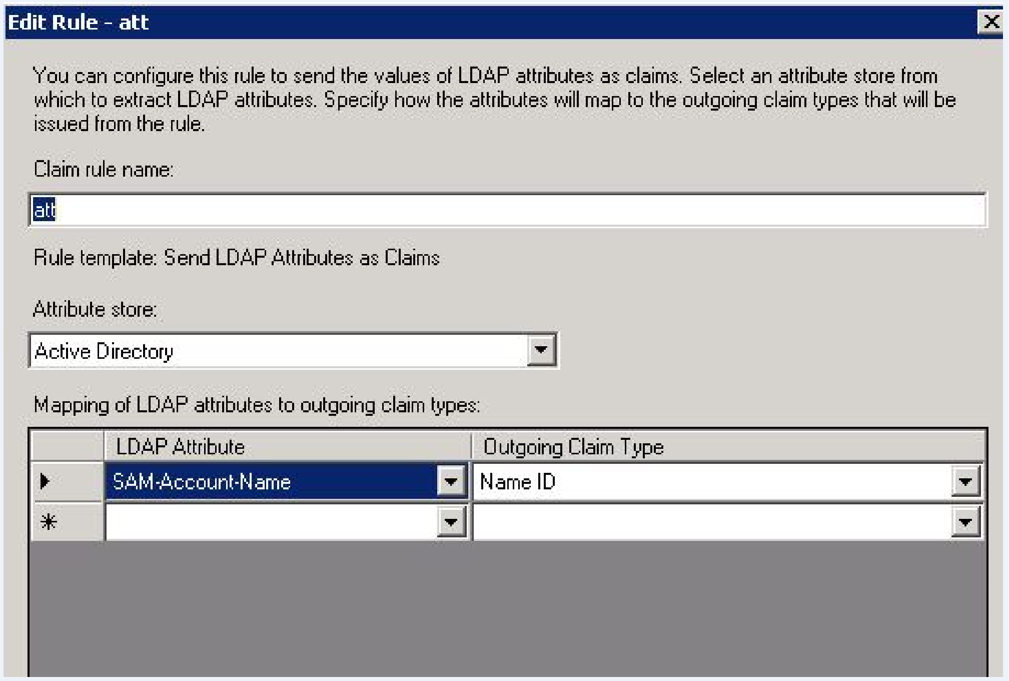


Display Name	Enabled	Identifier
HCPTRIAL_S0015864207	Yes	https://hanatrial.ondemand.com/s00...

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 SCP.

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 2-9 Edit Rule



Edit Rule - att

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

att

Rule template: Send LDAP Attributes as Claims

Attribute store:

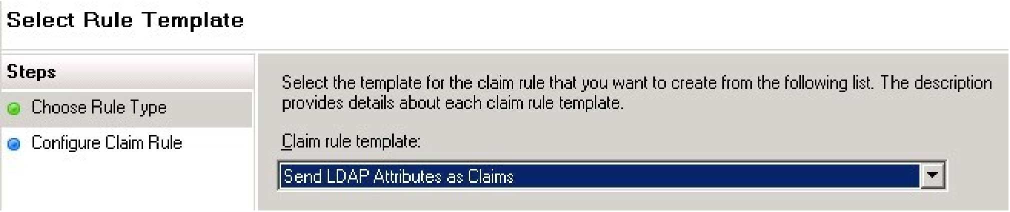
Active Directory

Mapping 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 2-10 Select Rule Template



Select Rule Template

Steps

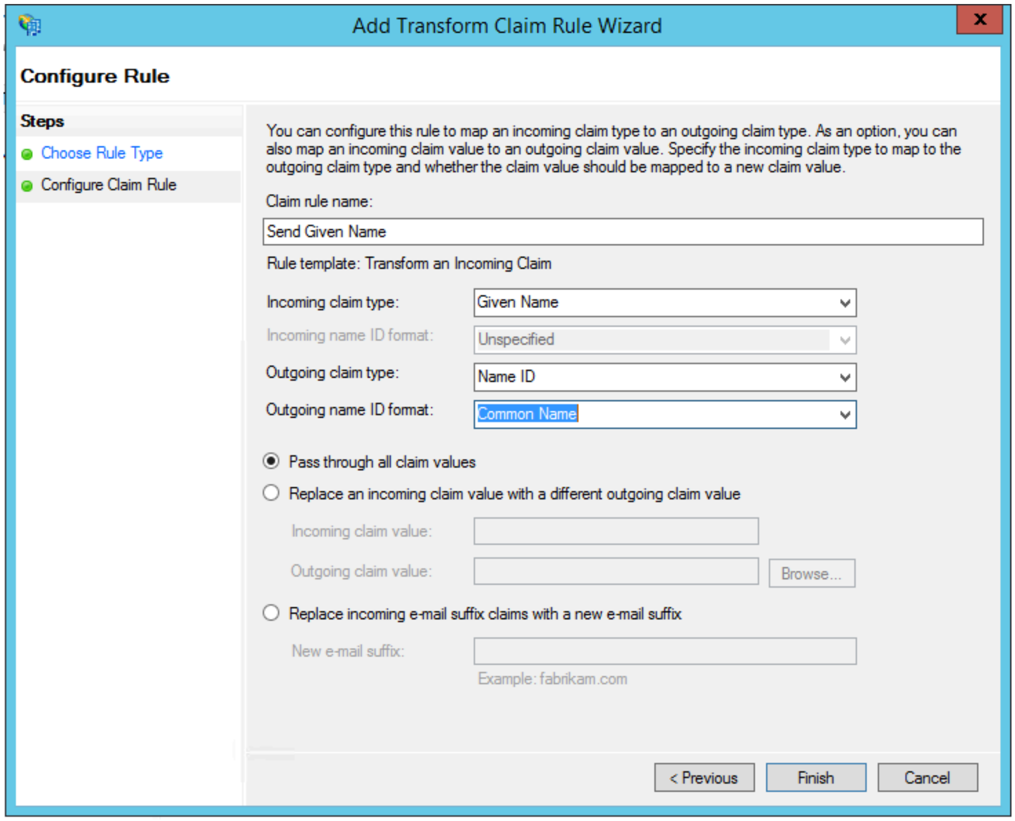
- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

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 2-11 Configure Rule



Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name: Send Given Name

Rule template: Transform an Incoming Claim

Incoming claim type: Given Name

Incoming name ID format: Unspecified

Outgoing claim type: Name ID

Outgoing name ID format: Common Name

● Pass through all claim values

○ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

○ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

19. Click **Finish**.

2.2.3. Add ADFS Metadata to SCP

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

To add ADFS metadata to SCP:

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 SCP Account and navigate to **Security**, **Trust**, **Trusted Identity Provider**, **Add Trusted Identity Provider**.
4. Click **Browse** and select ADFS Metadata file.
5. Click **Save**.

2.2.4. Add Roles to access SCP 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 SCP Development and Operations help users from ADFS to login for administration or development tasks.

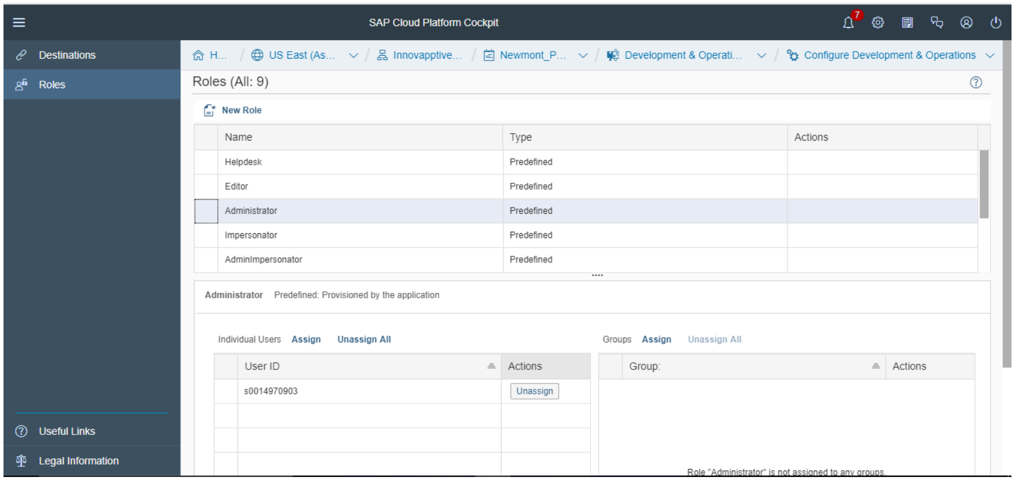
To add roles:

1. Navigate to **SCP, 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 **SCP, Services, Development & Operations, Configure Development & Operations, Roles**.
   SCP 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 2-12 SCP Roles


SAP Cloud Platform Cockpit
7
Destinations
Roles
Useful Links
Legal Information
H... / US East (As... / Innovapptive... / Newmont_P... / Development & Operati... / Configure Development & Operations
New Role
Assign
Unassign All
Unassign

Roles (All: 9)

Name	Type	Actions
Helpdesk	Predefined	
Editor	Predefined	
Administrator	Predefined	
Impersonator	Predefined	
AdminImpersonator	Predefined	

Administrator Predefined: Provisioned by the application

Individual Users

User ID	Actions
s0014970903	Unassign

Groups

Group:	Actions

Role "Administrator" is not assigned to any groups.

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

2.2.5. 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 SCP, Cloud Connector and SAP Gateway System which is on the Corporate Network.

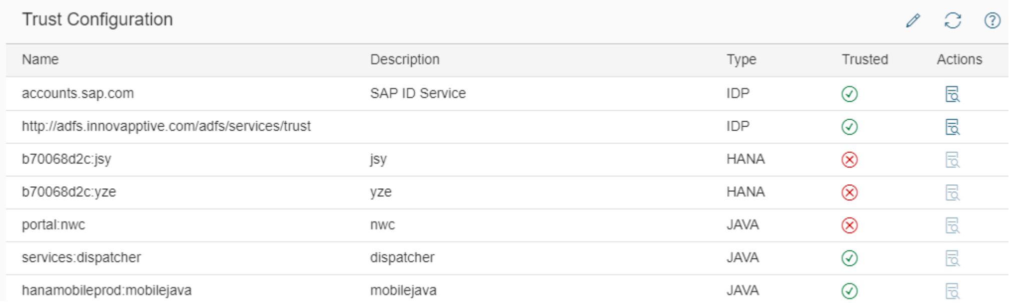
Before configuring, ensure you have:

- Working Cloud Connector
- Certificates exchanged between Cloud Connector GW system
- Access Controls are defined, and resources are available to SCP 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 SCP 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 2-13 Trust Configuration



Trust Configuration

Name	Description	Type	Trusted	Actions
accounts.sap.com	SAP ID Service	IDP	✓	
http://adfs.innovapptive.com/adfs/services/trust		IDP	✓	
b70068d2c:jsy	jsy	HANA	⊗	
b70068d2c:yze	yze	HANA	⊗	
portal:nwc	nwc	JAVA	⊗	
services:dispatcher	dispatcher	JAVA	✓	
hanamobileprod:mobilejava	mobilejava	JAVA	✓	

2.2.6. Create New Application using SAML Authentication

To create new application using SAML authentication, login to your SCP 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:

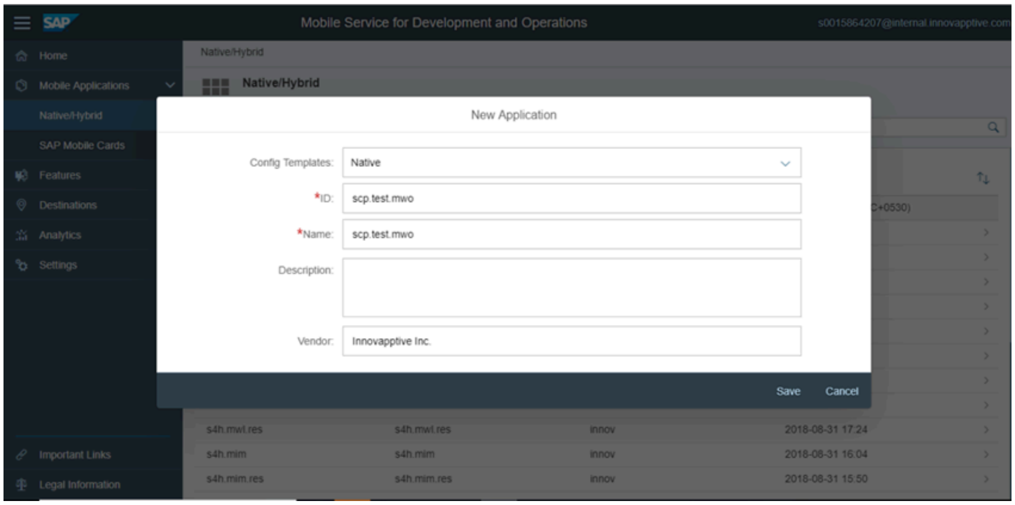
1. Expand Mobile Applications on the left navigation.
2. Click **Native/Hybird** under Mobile Applications.
3. Click **Create New Application**.
   Use the information in the table to add new application details for the product you purchased.

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 2-14 Create New Application



Config Templates: Native

*ID: scp.test.mwo

*Name: scp.test.mwo

Description:

Vendor: Innovapptive Inc.

```
s4h.mwl.res    s4h.mwl.res    innov    2018-08-31 17:24
s4h.mim        s4h.mim        innov    2018-08-31 16:04
s4h.mim.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/odata/INVMAT/MASSETTAG_2_SRV/
mInventory	http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/INVMIM/MINVENTORY_2_SRV/
mServiceOrder	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.

2.2.7. Define SAML SCP Client Password Policy

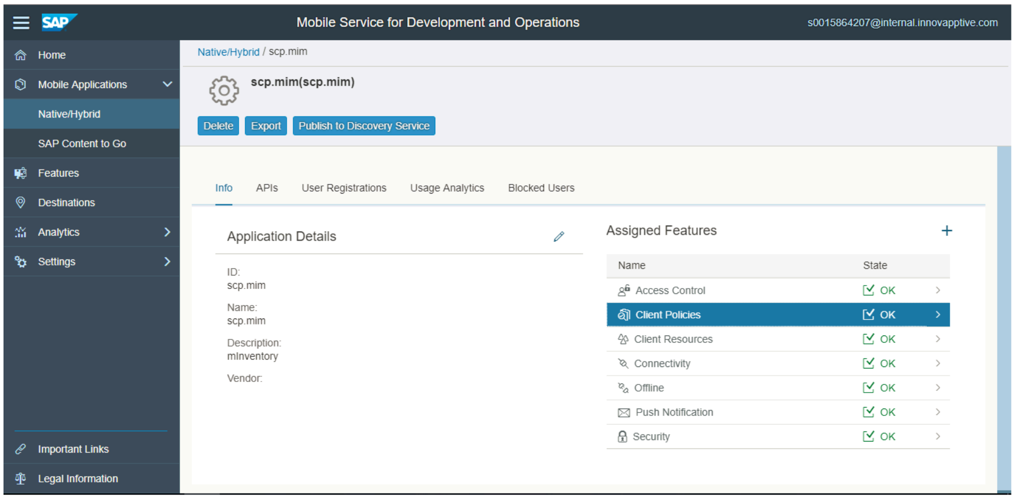
Define the client password policy that is used to unlock the DataVault for the applications. Application developers must add code to the DataVault to enforce the client password policy. An administrator must enter the application password policy to unlock the DataVault during application initialization.

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

To define the Password policy:

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

Figure 2-15 Application Details



Application Details

ID:
scp.mim

Name:
scp.mim

Description:
mInventory

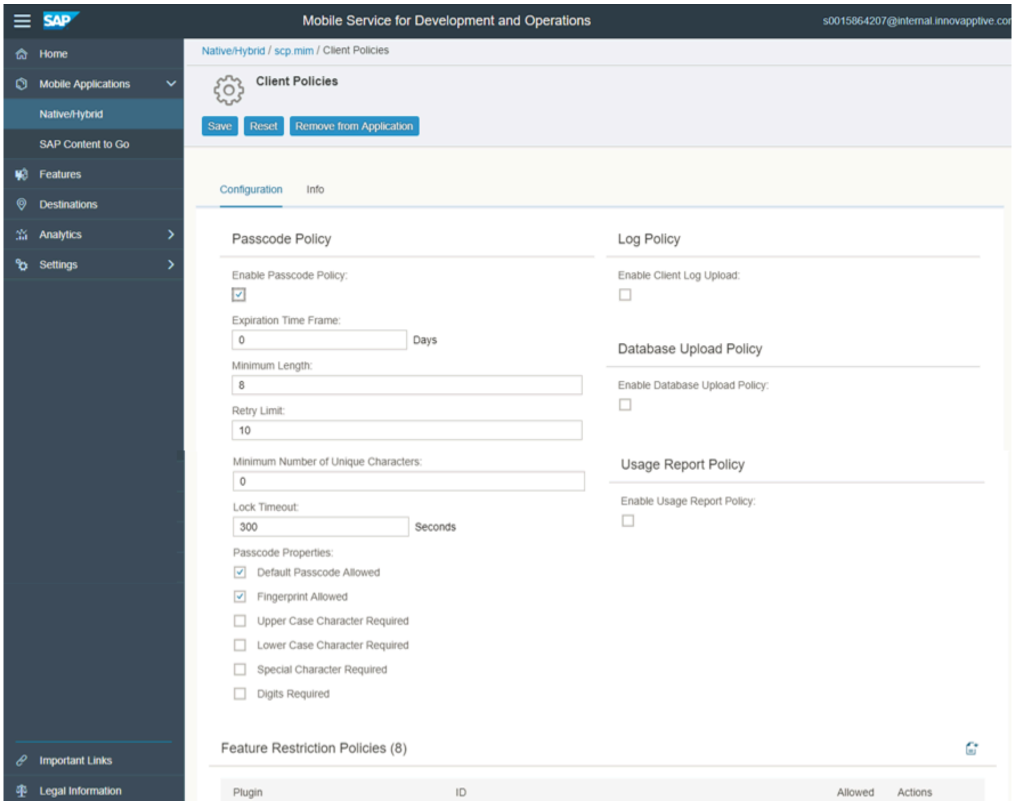
Vendor:

Assigned Features

Name	State
Access Control	OK
Client Policies	OK
Client Resources	OK
Connectivity	OK
Offline	OK
Push Notification	OK
Security	OK

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

Figure 2-16 Client Policies



Passcode Policy

Enable Passcode Policy: ☑

Expiration Time Frame: 0 Days

Minimum Length: 8

Retry Limit: 10

Minimum Number of Unique Characters: 0

Lock Timeout: 300 Seconds

Passcode Properties:

- ☑ Default Passcode Allowed
- ☑ Fingerprint Allowed
- □ Upper Case Character Required
- □ Lower Case Character Required
- □ Special Character Required
- □ Digits Required

Log Policy

Enable Client Log Upload: □

Database Upload Policy

Enable Database Upload Policy: □

Usage Report Policy

Enable Usage Report Policy: □

Feature Restriction Policies (8)

Plugin	ID	Allowed	Actions

The following table shows the description for the fields.

Property	Default	Description
Expiration 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 unusable, 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.

Property	Default	Description
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**.

2.3. Integrate SCP with Azure AD

By integrating SCP with Azure AD:

- You can control users’ access to SCP
- You can manage accounts using the Azure portal
- Users can login (Single Sign-On) to SCP 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 SCP application for Single Sign-On using Azure AD
- Configure assertion-based groups for Azure Active Directory Identity Provider

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

Before proceeding, ensure you have:

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

2.3.1. Configure and test Azure AD Single Sign-On

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

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

2.4. Configure Push Notifications for SCP

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 Cloud Platform (SCP) 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 33)*
- Configure SCP for Push Notification *(on page 33)*
- Configure SCP Applications for Push Notification *(on page 40)*

2.4.1. 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.

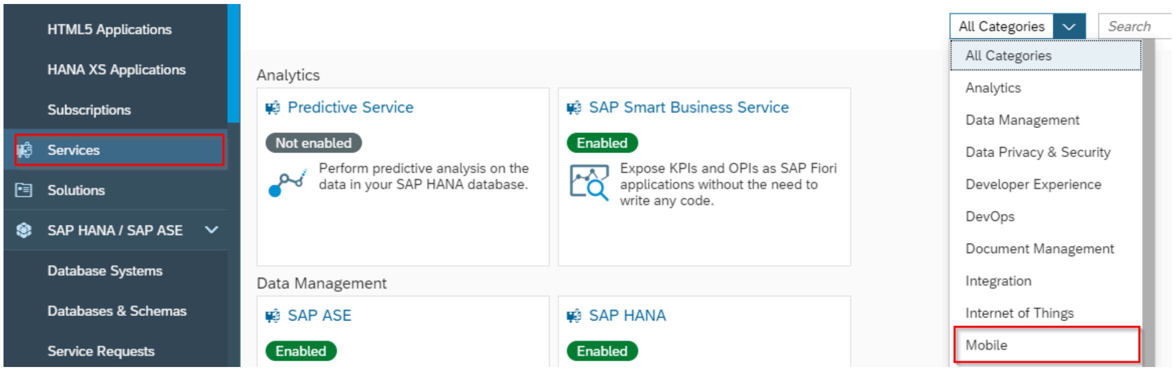
- SAP Cloud Platform (SCP) Admin Access.
- Access to SAP Gateway System with Basis Roles.

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.

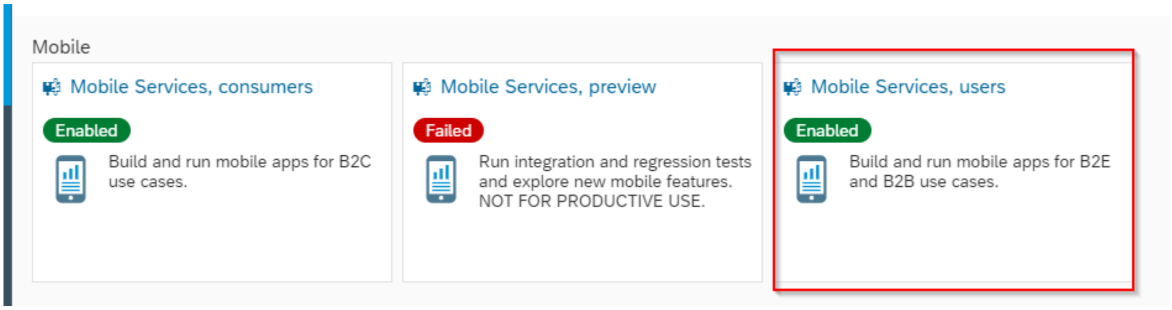
2.4.2. Configure SCP for Push Notification

To configure SCP for push notification:

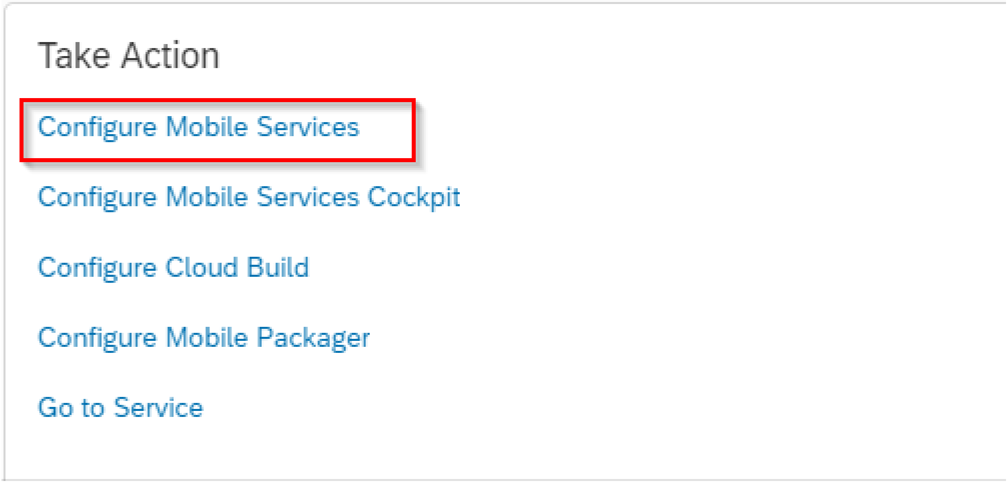
1. Log in to **SCP Account**.
2. Navigate to your **Sub Accounts**.
   Sub Accounts depends on whether they are created for your account. You can directly create a Tenant in your main account. For example, {your_company_name} can be main account and it could have multiple sub accounts and the sub accounts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


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



Take Action

Configure Mobile Services

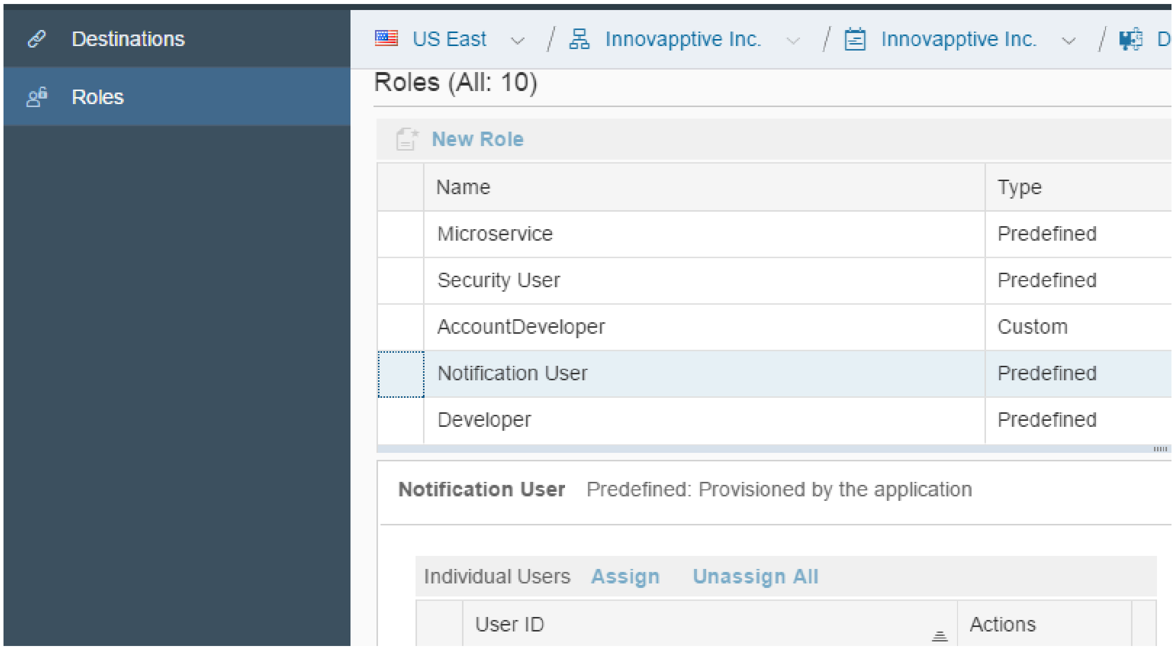
Configure Mobile Services Cockpit

Configure Cloud Build

Configure Mobile Packager

Go to Service

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



Roles (All: 10)

New Role

Name	Type
Microservice	Predefined
Security User	Predefined
AccountDeveloper	Custom
Notification User	Predefined
Developer	Predefined

Notification User Predefined: Provisioned by the application

Individual Users Assign Unassign All

User ID	Actions

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

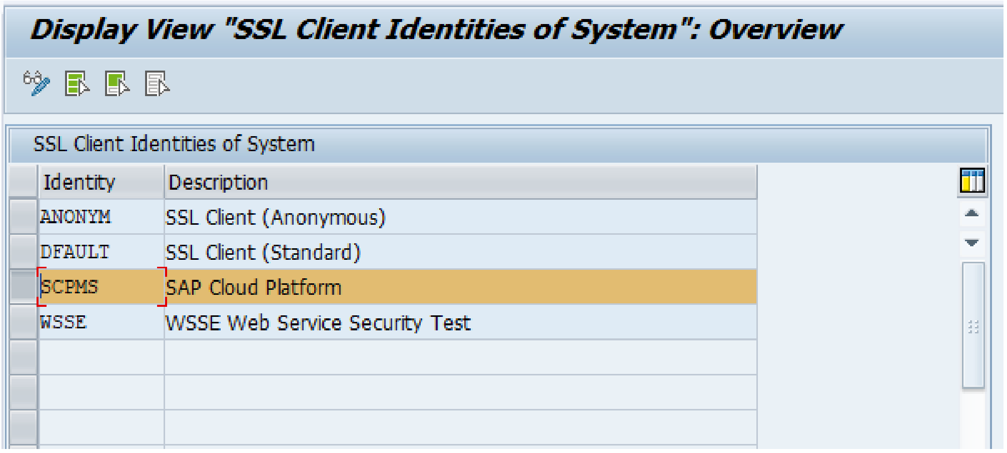
2.4.2.1. Import SCP Certificate to Gateway system

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

To import SCP certificate:

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

Figure 2-17 SSL Client Identities



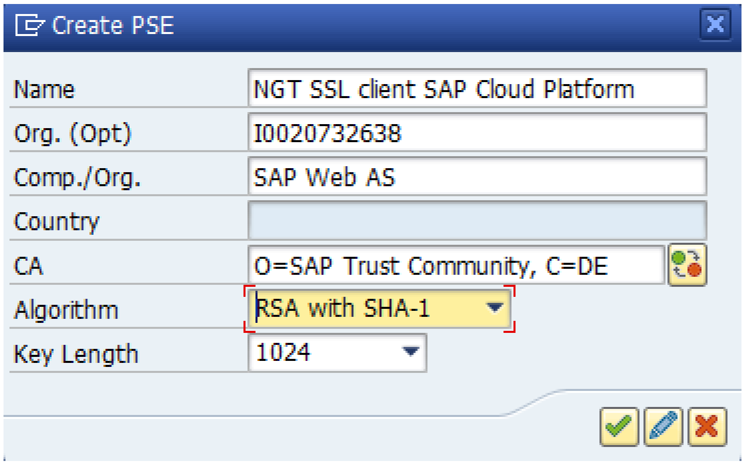
Display View "SSL Client Identities of System": Overview

SSL Client Identities of System

Identity	Description
ANONYM	SSL Client (Anonymous)
DFAULT	SSL Client (Standard)
SCPMS	SAP Cloud Platform
WSSE	WSSE Web Service Security Test

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

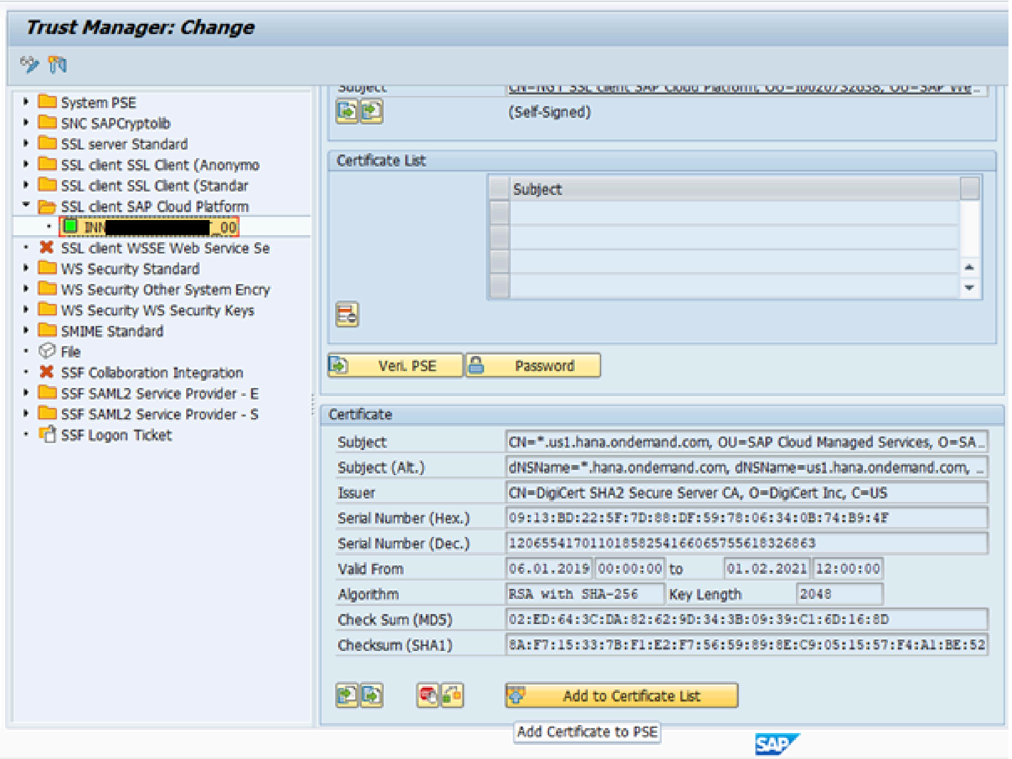
Figure 2-18 Create PSE



Name	NGT SSL client SAP Cloud Platform
Org. (Opt)	I0020732638
Comp./Org.	SAP Web AS
Country	
CA	O=SAP Trust Community, C=DE
Algorithm	RSA with SHA-1
Key Length	1024

7. Import the SCP certificate provided by Innovapptive under **SSL client SAP Cloud Platform**.
8. Click Add to Certificate List.
9. Click **Save**.

Figure 2-19 Add SCP certificate to list


Trust Manager: Change
System PSE
SNC SAPCryptolib
SSL server Standard
SSL client SSL Client (Anonymo
SSL client SSL Client (Standar
SSL client SAP Cloud Platform
INN[redacted]_00
SSL client WSSE Web Service Se
WS Security Standard
WS Security Other System Encry
WS Security WS Security Keys
SMIME Standard
File
SSF Collaboration Integration
SSF SAML2 Service Provider - E
SSF SAML2 Service Provider - S
SSF Logon Ticket
(Self-Signed)
Certificate List
Subject
Veri. PSE
Password
Add to Certificate List
Add Certificate to PSE

Certificate

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

2.4.2.2. Create RFC for Push Notification

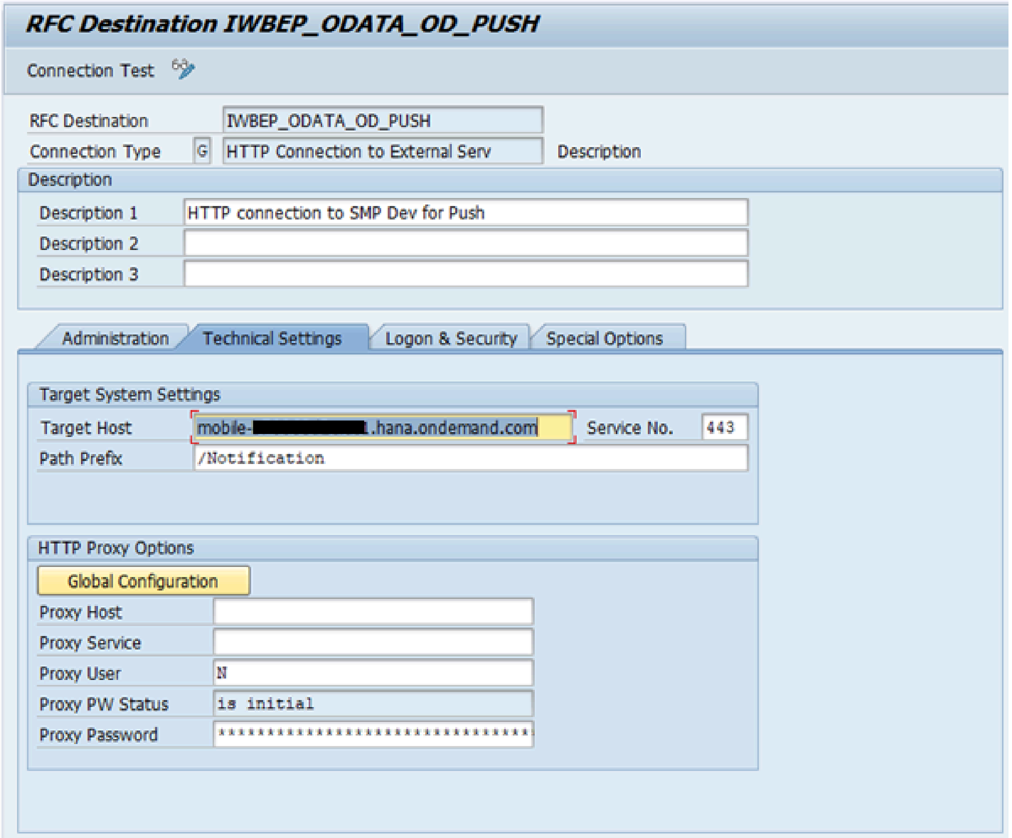
Following steps guide you to configure RFC to establish HTTP communication between SAP and external server.

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

Table 2-7 RFC Destination

Field	Description
RFC Destination	IWBEP_ODATA_OD_PUSH
Target Host	SCP Host
Path Prefix	/notification
Service No	443

Figure 2-20 Create RFC



RFC Destination IWBEP_ODATA_OD_PUSH

RFC Destination: IWBEP_ODATA_OD_PUSH
Connection Type: G HTTP Connection to External Serv
Description

Description
Description 1: HTTP connection to SMP Dev for Push
Description 2:
Description 3:

Target System Settings
Target Host: mobile-[redacted].hana.ondemand.com
Service No.: 443
Path Prefix: /Notification

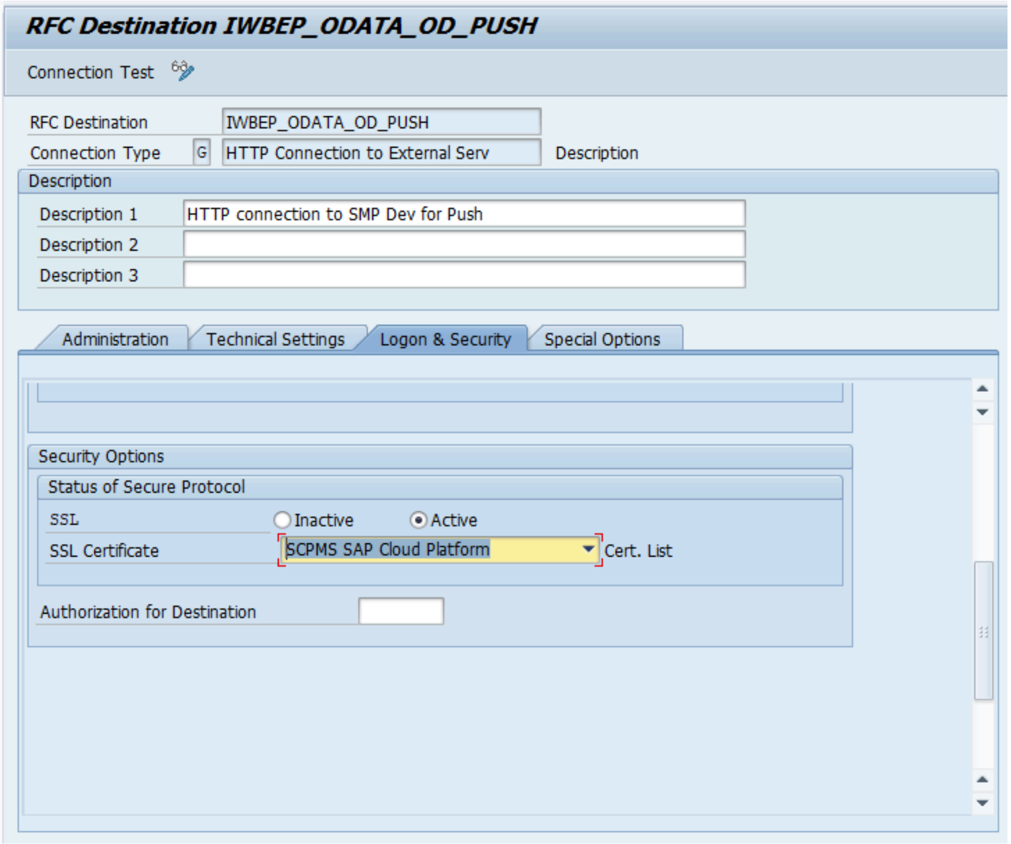
HTTP Proxy Options

Proxy Host:
Proxy Service:
Proxy User: N
Proxy PW Status: is initial
Proxy Password: ********************************

3. On the **Logon & Security** tab, choose **Basic Authentication**.

4. Enter **S-User** and **Password**.
5. In the **Security Options** section, select the SSL Certificate (SCPMS SAP Cloud Platform) created in Import SCP Certificate to Gateway system *(on page 35)*.

Figure 2-21 Select SSL Certificate



RFC Destination IWBEP_ODATA_OD_PUSH

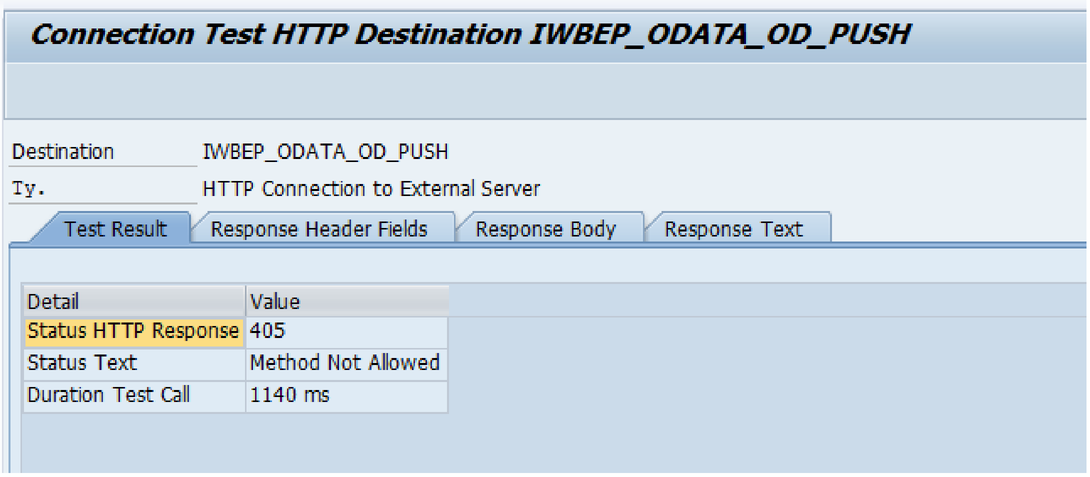
RFC Destination: IWBEP_ODATA_OD_PUSH
Connection Type: G HTTP Connection to External Serv

Description 1: HTTP connection to SMP Dev for Push
Description 2:
Description 3:

Security Options
Status of Secure Protocol
SSL: ○ Inactive ● Active
SSL Certificate: SCPMS SAP Cloud Platform
Authorization for Destination:

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

Figure 2-22 HTTP Connection to External Server



Connection Test HTTP Destination IWBEP_ODATA_OD_PUSH

Destination IWBEP_ODATA_OD_PUSH

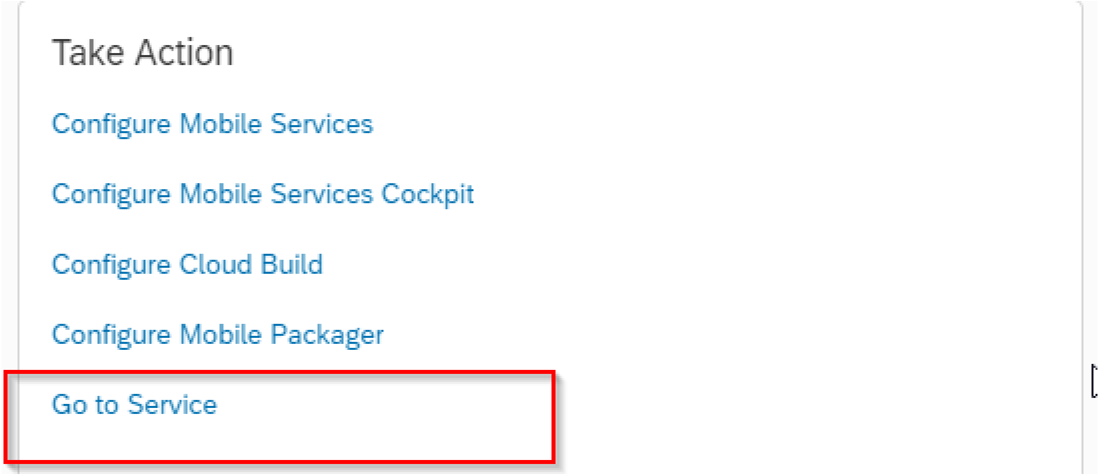
Ty. HTTP Connection to External Server

Detail	Value
Status HTTP Response	405
Status Text	Method Not Allowed
Duration Test Call	1140 ms

2.4.2.3. Configure SCP Applications for Push Notification

To configure SCP applications for push notification:

1. Log in to **SCP 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

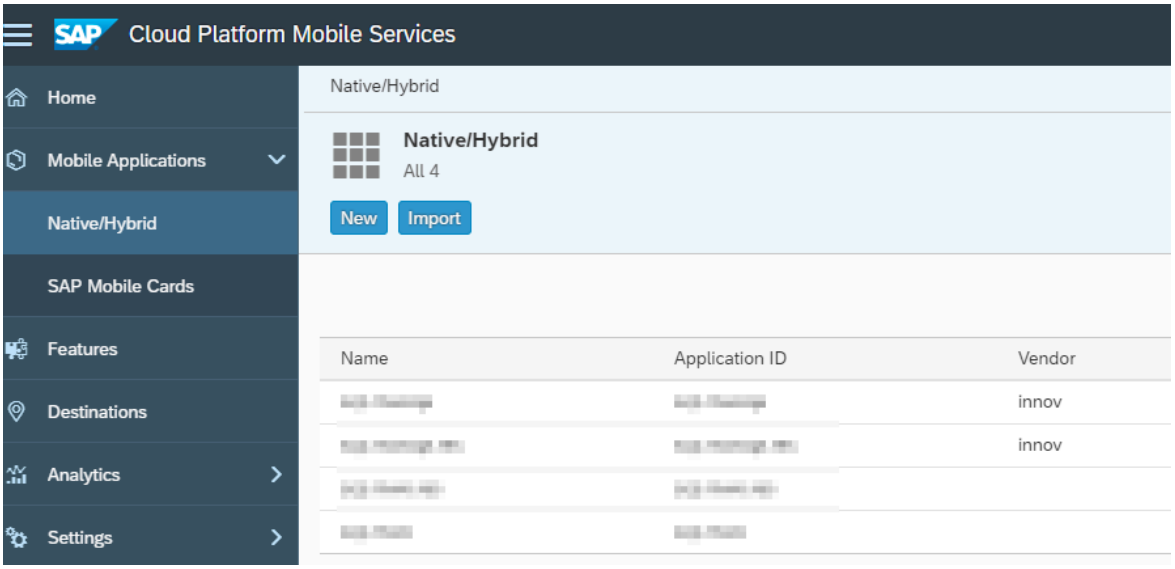
Configure Cloud Build

Configure Mobile Packager

Go to Service

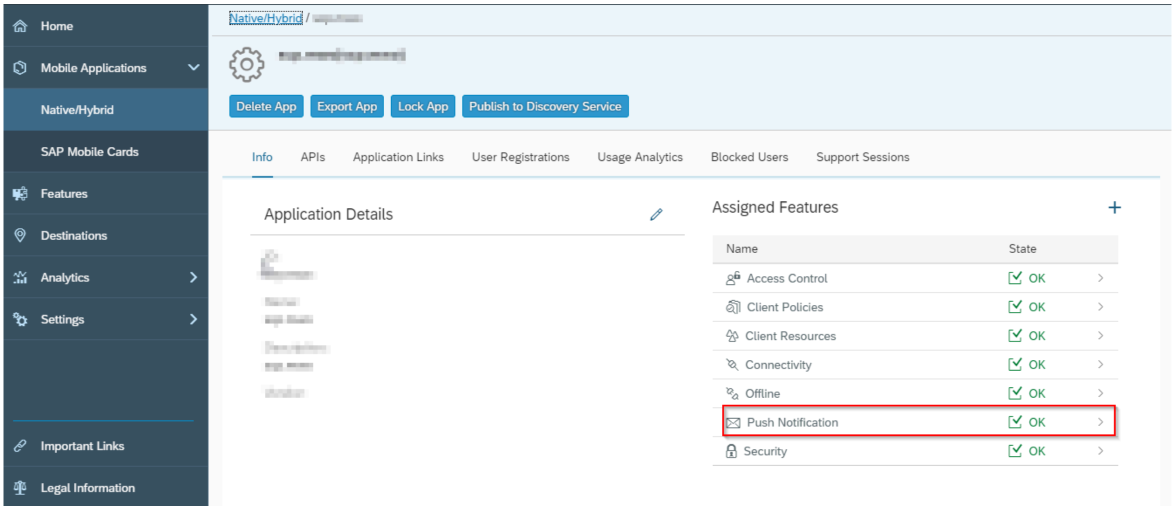
> **Note:**
> Depending on your environment, you could be asked for authentication.

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



Name	Application ID	Vendor
[redacted]	[redacted]	innov
[redacted]	[redacted]	innov
[redacted]	[redacted]	
[redacted]	[redacted]	

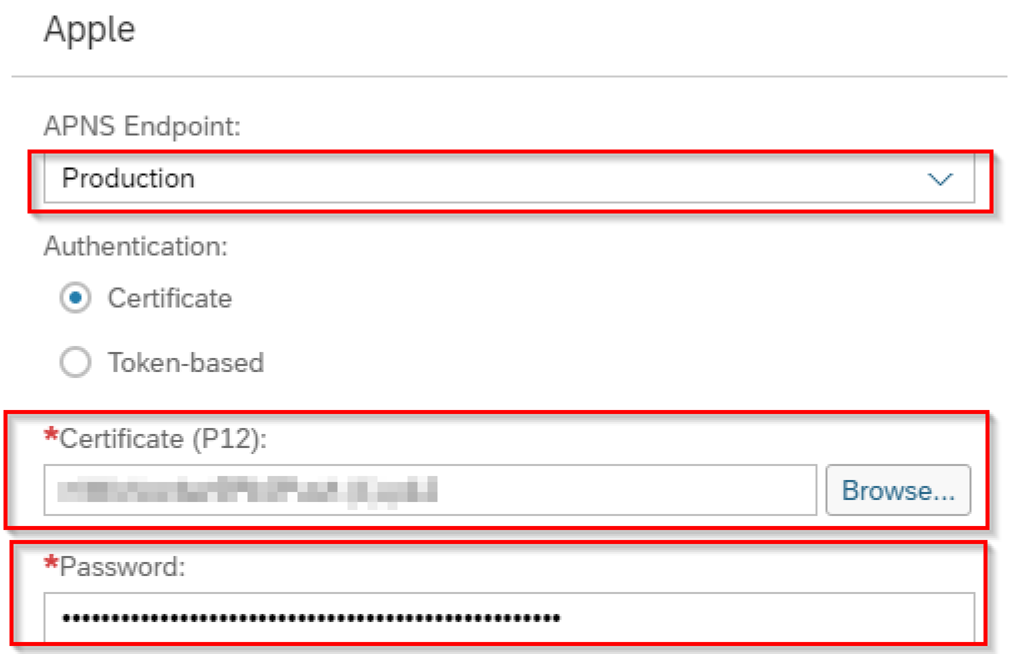
10. In the Application ID Details screen, click **Push Notification**.



Name	State
Access Control	OK
Client Policies	OK
Client Resources	OK
Connectivity	OK
Offline	OK
Push Notification	OK
Security	OK

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:

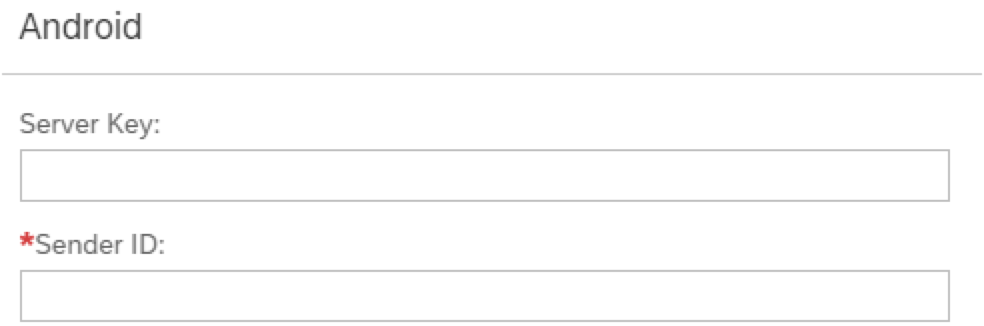
● Certificate

○ Token-based

*Certificate (P12): [redacted]

*Password: ••

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

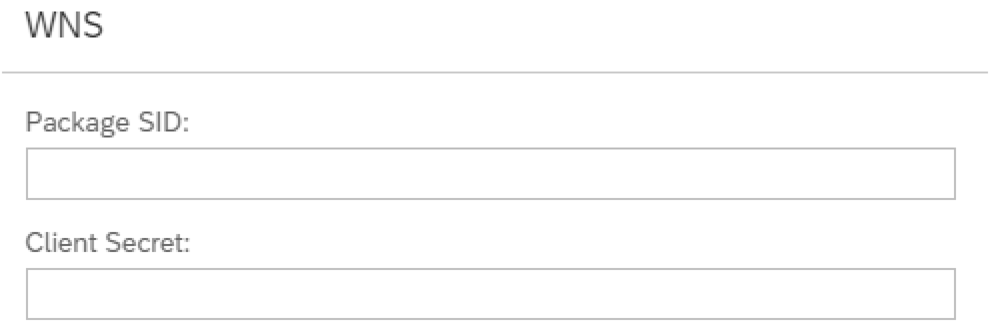


Android

Server Key:

*Sender ID:

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


WNS

Package SID:

Client Secret:

12. Click **Save**.

2.5. Manage Resource File in SCPms

Resource File in SCP 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 SCPms 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 SCPms admin user.

When this resource file is updated, the application connects to the mobile platform (SCPms) 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 Cloud Platform Mobile Services (SCPms):

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

The following topics help you with resource file management:

- Prepare and Update Resource File for SCPms *(on page 45)*
- Use Resource File in SCP *(on page 56)*
- Use Resource File in SMP *(on page 135)*

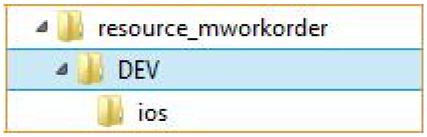
2.5.1. Prepare and Update Resource File for SCPms

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.

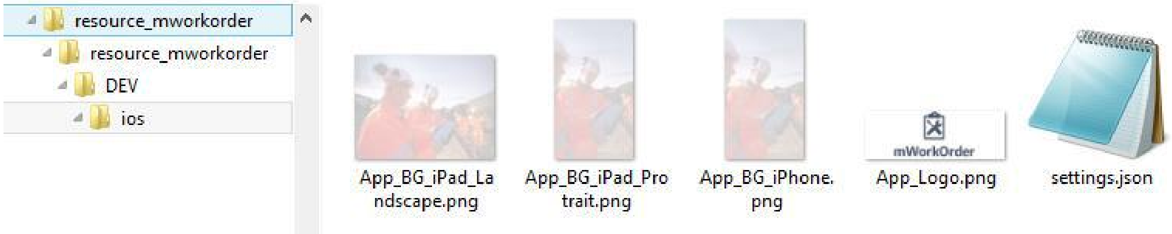
To prepare and update the resource file:

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. • **Conditions:** Use uppercase alphabets. • **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. • **Conditions:** None • **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. • **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 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

Property	Description
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. • **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 "OfflineStatusColor":"#DF264D" in the json file.
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. **Syntax:** `{"id":<SequenceNumber>,"key":"<SAPLanguageCode>","value":"<LanguageName>"}` • **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.
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. • **Possible Values:** As required. For example, D30.

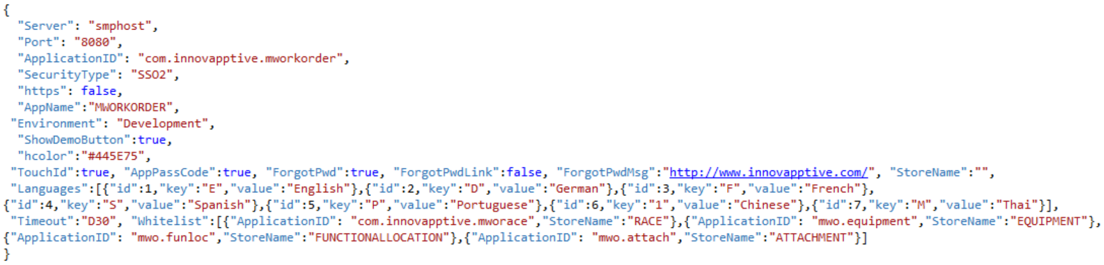
5. For each environment (Development, Quality, and Production), review and update the content block in entirety.

> **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 SCPms 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. • **Possible Values:** 443. For example, HTTPs (SCPms default HTTPs port 443 and custom ports for proxy)
Application-ID	• ID configured in SCPms and the mobile application will use it to connect to server for the registration. • **Condition:** Use the same application ID as defined in SCPms. • **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 SCPms 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 SCPms. 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 [Application-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 [StoreName]	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": "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.racedynamic-forms	RACEDYNAMICFOR-MS

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

2.5.2. Prepare and Update Resource File for SCPms (MWO 2009 SP03 and above releases)

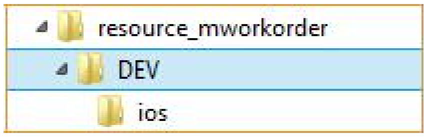
The **mWorkOrder** application resource file **resources_mworkorder.zip** on Windows platform is used as an example to demonstrate the procedure. Do your branding changes in the zip file that is provided by Innovapptive initial deployment.

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

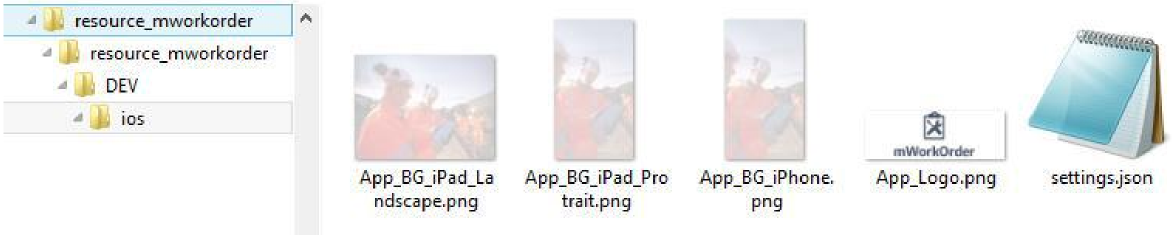
To prepare and update the resource file:

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. • **Conditions:** Use uppercase alphabets. • **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. • **Conditions:** None • **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. **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
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. • **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 "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. • **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. • **Conditions:** None • **Possible Values:** WORKORDER
StoreDescription	Helps you to identify the description regarding the store name. • **Conditions:** None • **Possible Values:** General
StoreIndex	Helps you to identify the index value of the store name and the order is in ascending order. • **Conditions:** None • **Possible Values:**1 or 2

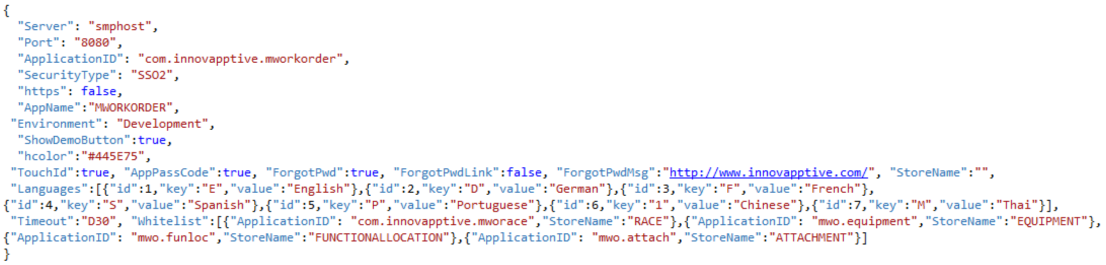
Property	Description
StoreType	Helps you to identify the type of the store. • **Conditions:** None • **Possible Values:** T
Languages	• Languages that are configured in the **settings.json** file are displayed to the user as a drop-down menu for selection. Additional languages can be added provided the language is available in SAP and the necessarytranslations are maintained. **Syntax:** `{"id":<SequenceNumber>,"key":"<SAPLanguageCode>","value":"<LanguageName>"}` • **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.
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. • **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 SCPms 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. • **Possible Values:** 443. For example, HTTPs (SCPms default HTTPs port 443 and custom ports for proxy)
Application-ID	• ID configured in SCPms and the mobile application will use it to connect to server for the registration. • **Condition:** Use the same application ID as defined in SCPms. • **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 SCPms 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 SCPms. 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 [Application-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 [StoreName]	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": "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.racedynamic-forms	RACEDYNAMICFOR-MS

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

2.5.3. Use Resource File in SCP

The following topics help you with uploading resource file in SCP:

- Add back-end connection RACE URL and upload application help resource *(on page 57)*
- Add backend connection for Dolphin Services Integration (mAssetTag only) *(on page 58)*
- Create Application and Upload Resource File *(on page 59)*

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

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

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

1. Log in to **SCP 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.

2.5.3.2. 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.

2.5.3.3. Create Application and Upload Resource File

Upload the resource file that you created at Prepare and Update Resource File for SCPms *(on page 45)*.

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.
Description	(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.

2.5.3.4. 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
```

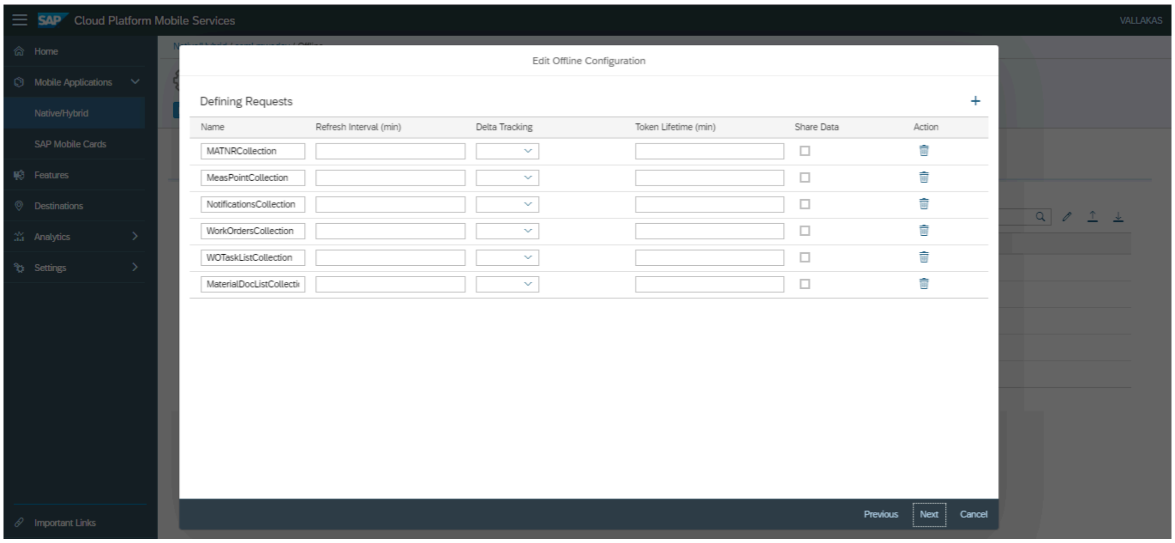
```
prepopulate_offline_db=N
request_format=application/json;q=1,application/atom+xml;q=0.5
delta_request_format=application/atom+xml
batch_all_defining_queries=N
case_sensitive_offline_db=N
offline_db_collation=UTF8BIN
local_change_expiry=0
content_id_header_location=mime
allow_omitting_max_length_facet=N
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:

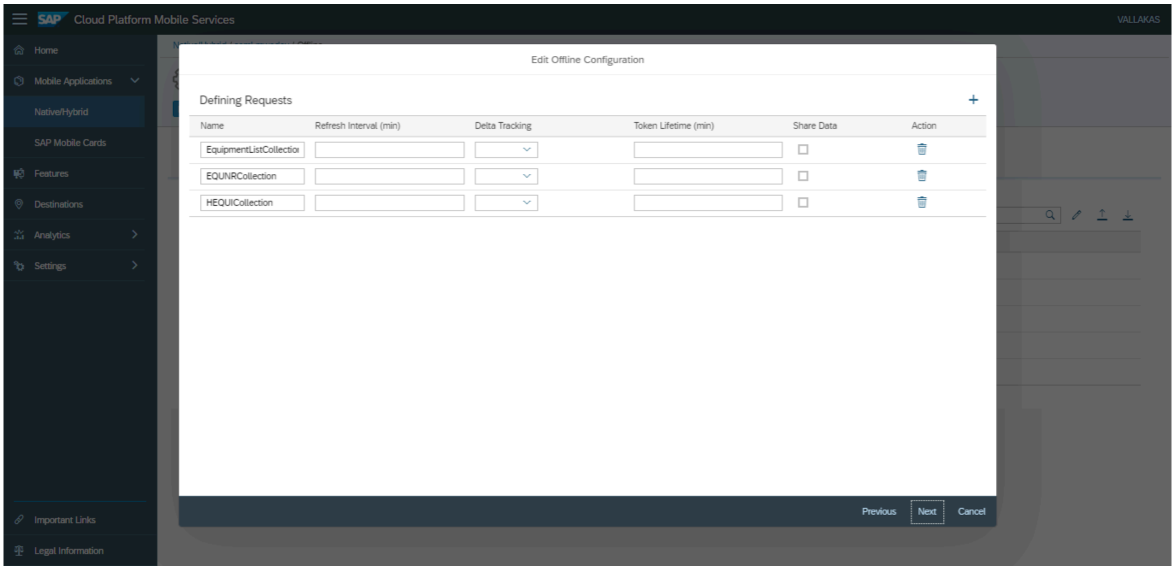


Edit Offline Configuration

Defining Requests

Name	Refresh Interval (min)	Delta Tracking	Token Lifetime (min)	Share Data	Action
MATNRCollection				□	
MeasPointCollection				□	
NotificationsCollection				□	
WorkOrdersCollection				□	
WOTaskListCollection				□	
MaterialDocListCollecti				□	

For Equipment:

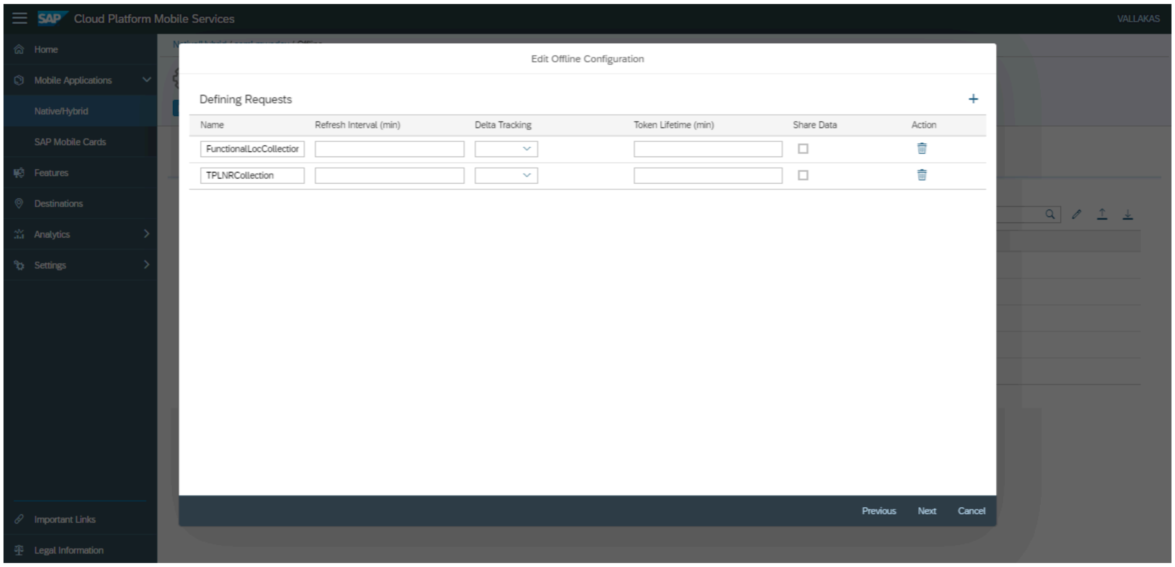


Edit Offline Configuration

Defining Requests

Name	Refresh Interval (min)	Delta Tracking	Token Lifetime (min)	Share Data	Action
EquipmentListCollectio				□	
EQUNRCollection				□	
HEQUICollection				□	

For Functional Location:



Edit Offline Configuration

Defining Requests

Name	Refresh Interval (min)	Delta Tracking	Token Lifetime (min)	Share Data	Action
FunctionalLocCollectior				□	
TPLNRCollection				□	

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

3. SMP Configurations after Installing Innovapptive Products

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

Figure 3-1 Workflow for SMP configurations after Instllaing Innovapptive Products

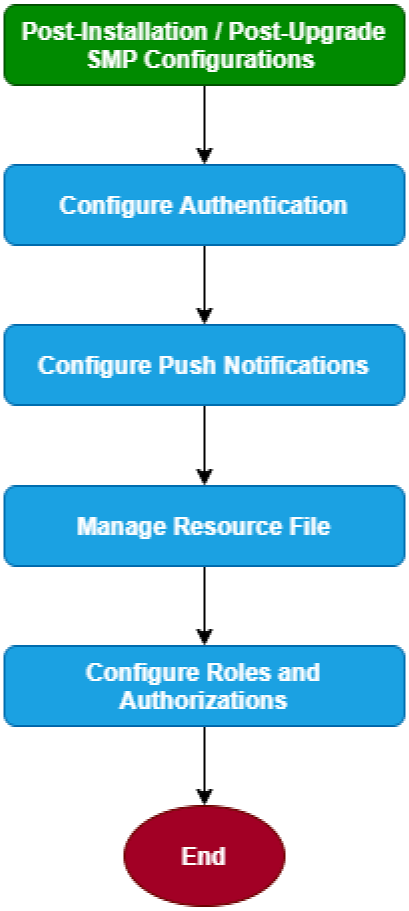

Post-Installation / Post-Upgrade SMP Configurations
Configure Authentication
Configure Push Notifications
Manage Resource File
Configure Roles and Authorizations
End

Table 3-1 Tasks for SMP Configurations after Instllaing Innovapptive Products

Task	Reference to section
Configure Authentication	• Authenticate users using HTTP Authentication *(on page 70)* • Authenticate users using HTTPs Authentication *(on page 74)* • Authenticate users using LDAP Server *(on page 85)* • Authenticate users using SAML Authentication *(on page 95)* • Authenticate users using X.509 Authentication *(on page 102)* • Integrate SMP with Azure AD *(on page 109)*
Configure Push Notifications	Configure Push Notifications for SMP *(on page 115)*
Prepare and update resource file	Manage Resource File in SMP *(on page 122)*
Configure roles and authorizations	Configure Roles and Authorization for Products *(on page 141)*

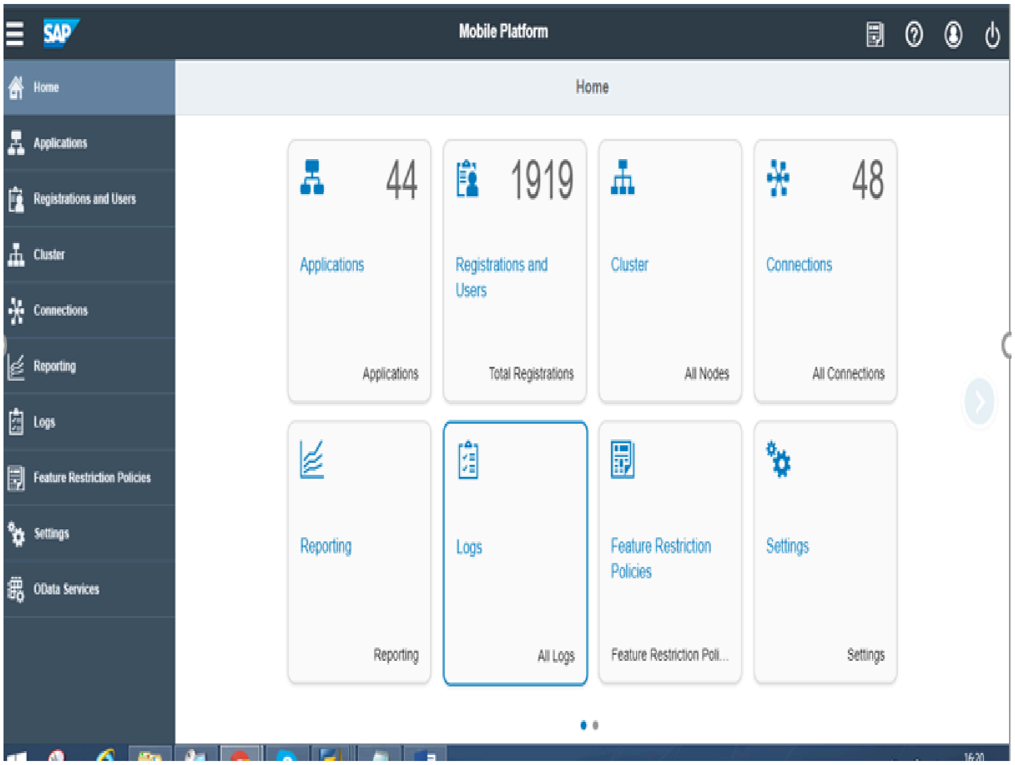
3.1. Access SMP Management Cockpit

Use SMP Management Cockpit to deploy, manage, and monitor SMP-based applications, user registrations, and device connections.

To access SMP Management Cockpit:

1. Access the URL: https://<SMPServerAddress>:8083/Admin
   Example: https://innosmpdev:8083/Admin
2. Enter your credentials.
   You can view mobile landscape information, such as number of applications configured, users connected, and device registrations.

Figure 3-2 SMP Management Cockpit



3.2. Define Application Authentication

Define authentication for your applications that are being deployed on SMP.

You can authenticate Clients, Administrators, and back-end systems using these authentication types:

- **Anonymous Access:** Applications that do not require authentication can use anonymous access. Users can access such applications without entering credentials.
- **Basic Authentication:** Basic authentication requires a valid username and password. The basic authentication mechanism relies on the standard Authorization: basic (base64 encoded username:password) HTTP header. Because the username:password can be decoded from the request, basic authentication should only be used over HTTPS.

  SAP Mobile Platform basic authentication uses the following authentication providers:

  - HTTP/HTTPS Authentication
  - System Login (Admin Only)
  - Directory Service (LDAP/AD)
- **X.509 Certificate Authentication:** X.509 is a client-certificate authentication that requires an HTTPS connection to SMP Server, which can authenticate users based on their personal X.509 certificates.
- **Token-Based Authentication:** Token-based authentication uses the value of the opaque field in HTTP headers or cookies to authenticate users.
- **Single Sign-On:** Single sign-on (SSO) is token-based authentication in which an SSO token is passed in an HTTP header or cookie.

3.2.1. Worksheet for SMP Configuration

Take a printout of the following worksheet and gather the details of SMP server and related information that is required for configuring authentications.

Table 3-2 Worksheet for SMP Configuration

Question	Comment
What is the Type of Architecture (HUB or Embedded)	
Prerequisites on Hardware and Software Components/OS	
Admin Access for Basis Consultant with Create and change access.	
SMP Server OS Details	
SMP Dev Server IP Address	
SMP Dev Server Host Name	

Table 3-2 Worksheet for SMP Configuration (continued)

Question	Comment
SMP Dev Server OS Version	
SMP Dev Server CPU	
SMP Dev Server Memory	
SMP Dev Installation Path	
SMP Server Access Details	
Admin Access URL	
Admin User Name	
SMP Server Version including PLs	
Do you have Admin Access to SMP Dev Server	
SMP Server DB Details	
Default DB vs 3rd Party DB	
If, 3rd Party DB	
DB Host Name	
DB IP Address	
DB Port	
DB Name	
DB Login ID	
Driver Path If Any	
SMP Server Ports	
HTTP Port	
HTTPs Port	
HTTPs Mutual Port	
HTTPs Admin Port	
GW Server Details	

Table 3-2 Worksheet for SMP Configuration (continued)

Question	Comment
GW Server Host Name	
HTTP Port	
HTTPs Port	
UI5 URL	
Product UI5 URL	
RACE UI5 URL	
Authentication Type	
Basic SSO2 Authentication	
oData Ping URL from GW System	
Firewall Request, If any,	
SMP to GW	
GW to SMP	
Any knows Firewall Restrictions?	
Wifi Access	
Can the Users access SMP Server within Corporate Network without VPN Settings?	
Any special request which is necessary before testing the apps?	
Proxy	
Push Notification	
Username / Password	

3.3. Authenticate users using HTTP Authentication

Configure Innovapptive products on SMP Server and set up HTTP communication between SMP and Gateway System.

Create and configure security profiles to control how the server authenticates users and manage request-response transactions with the back end. You can use the same Security Profile to authenticate users for multiple applications if the applications point to the same Gateway system.

Note:
Innovapptive recommends that you use HTTP for internal communication within VPN Networks and for POC testing scenarios.

Before proceeding, ensure you have:

- Access to SAP Mobile Platform as an Administrator
- Access to SAP Gateway System
- Access to SMP system as an administrator
- List of Gateway documents that need to be checked

3.3.1. Create security profile for HTTP Authentication

Create security profile for HTTP/HTTPS Authentication with SSO tokens using HTTP communication port.

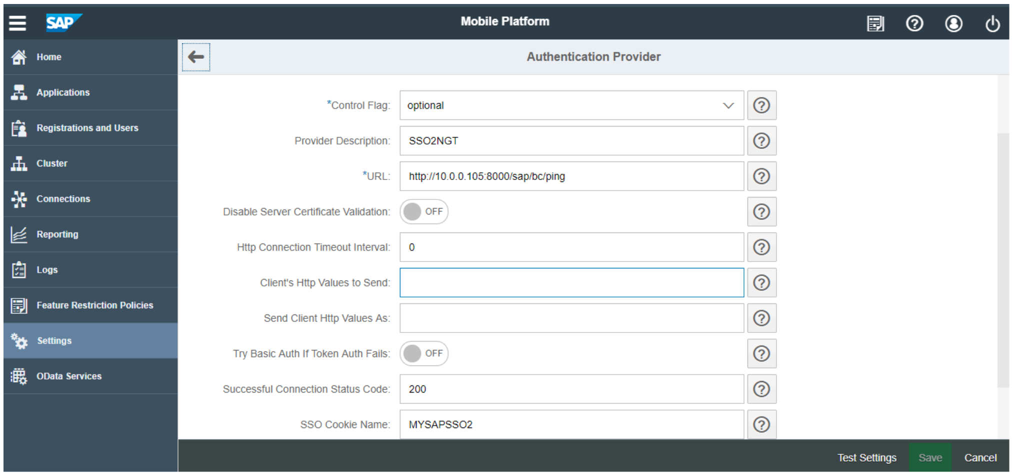
To create security profile for HTTP Authentication:

1. Login to SMP Admin Cockpit and go to **Settings**, **Security Profiles**.
2. Click **New**.
3. Enter the **Security Profile Name**, for example, SSO2NGT.
4. Click **Add**.
5. Select **HTTP/HTTPs Authentication** in the **Authentication Provider** drop-down and enter details such as **Control Flag**, **Gateway Server Ping URL** and **SSO2 Cookie Name**. Get the Gateway Server Ping URL and ensure the URL prompts for **Username** and **Password**. Test the URL on a Browser.

   URL format: http://GatewayHost:HTTP_Port/sap/bc/ping

In our case, the URL from GW System is: http://ngwt.innovapptive.com:8000/sap/bc/ping and **SSO2 Cookie Name**: MYSAPSSO2.

Figure 3-3 Security profile for HTTP Authentication



*Control Flag: optional

Provider Description: SSO2NGT

*URL: http://10.0.0.105:8000/sap/bc/ping

Disable Server Certificate Validation: OFF

Http Connection Timeout Interval: 0

Client's Http Values to Send:

Send Client Http Values As:

Try Basic Auth If Token Auth Fails: OFF

Successful Connection Status Code: 200

SSO Cookie Name: MYSAPSSO2

6. Click **Test Settings**.
7. Click **Save**.

3.3.2. Create an Application using HTTPs Authentication

To create a new application using HTTPs authentication:

1. Log in to **SMP Admin Cockpit**.
2. Under **Application**, click **New**.

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

APP ID	Name	Vendor	Type	Service Name
com.innovapptive.massettag	Mobile Asset Tag	Innovapptive	Native	/INVMAT/MASSETTAG_2_SRV/
com.innovapptive.minventory	Mobile Inventory	Innovapptive	Native	/INVMIM/MINVENTORY_2_SRV/
com.innovapptive.mserviceorder	Mobile Service Order	Innovapptive	Native	/INVMSO/MSERVICEORDER_2_SRV/

APP ID	Name	Vendor	Type	Service Name
com.innovapptive.mshop	Mobile Shopping Cart	Innovapptive	Native	/INVMSC/MSHOP_SRV/
com.innovapptive.mworklist	Mobile Universal Approvals	Innovapptive	Native	/INVMWL/MWORKLIST_3_SRV/
com.innovapptive.mworkorder	Mobile WorkOrder	Innovapptive	Native	/INVMWO/MWORKORDER_SRV/
com.innovapptive.racedynamicforms	RACE Dynamic Forms	Innovapptive	Native	/INVCEC/RACE_SRV/

3. Enter the following details in the **Create Application** window
   - **Application ID**: Enter the ID of the product.
   - **Version**: Enter the application version.
   - **Name**: Enter the name of the product.
   - **Type**: Select **Native**.
   - **Description**: Enter the description of the product.
   - **Vendor**: Enter Innovapptive Inc.
4. Click **Save**.
5. On the **Back End** tab, enter the primary connection details such as back-end URL and maximum number of connections.

   Endpoint:

   https://innovapptive.gw.server:8001/sap/opu/odata/iwfnd/rmtsampleflight/

   The following table lists the backend URLs for Innovapptive products.

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/
mServiceOrder	http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/INVMSO/MSERVICEORDER_SRV/

Product	OData URL
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/

6. On the **Authentication** tab, select the Security Profile.
7. Click **Save**.
8. Select the Application from **Applications** menu and click **Ping**.

3.4. Authenticate users using HTTPs Authentication

Set up HTTPs communication between SMP and Gateway System.

To set up Basic Authentication with HTTPs communication channel, establish trust between SMP and Gateway servers by importing Root Certificates.

Before proceeding, ensure you have:

- Access to SAP Mobile Platform as an Administrator
- Access to SAP Gateway System with Basis Authorizations
- Access to SMP system as an administrator
- List of Gateway documents that need to be checked

3.4.1. Establish trust between SMP and Gateway

To establish trust between SMP and Gateway servers using HTTPs communication channel, do the following:

1. Export Gateway Certificate *(on page 75)*
2. Import Gateway Certificate to SMP Server *(on page 75)*
3. Generate Root Certificate for HTTPs Authentication using OpenSSL *(on page 76)*
4. Import OpenSSL Certificate to SMP Certificate *(on page 78)*
5. Import Technical Certificate to Local SMP Certificate *(on page 78)*
6. Import Root and Intermediate Certificate to Shared KeyStore Entries *(on page 79)*
7. Import the SMP Root CA to Gateway System *(on page 79)*

3.4.1.1. Export Gateway Certificate

To export the Gateway Certificate:

1. Login to **SAP Gateway Sandbox** system.
2. Navigate to **T-Code STRUST.**
3. Open the **SSL server Standard** and the component under the server.

Figure 3-4 SSL server Standard

4. Click **Edit** and double-click **Own Certificate—Subject**.
5. Export the certificate into **.cer** or **.crt** format.

Figure 3-5 Export Gateway Certificate

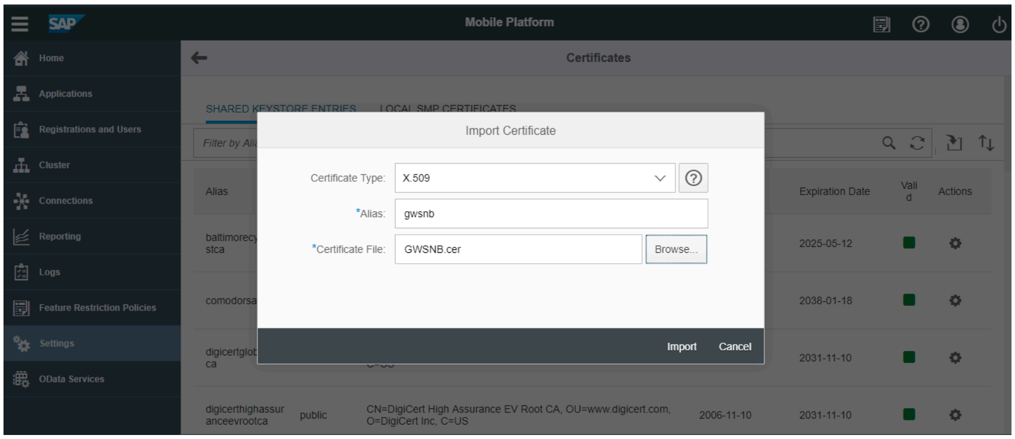
3.4.1.2. Import Gateway Certificate to SMP Server

To import Gateway Certificate to SMP:

1. Copy the Gateway certificate to SMP server.
2. Login to **SMP Admin Console**.
3. Navigate to **Settings and Certificates.**
4. Under **Shared Key Store**, click **Import** and browse the certificate.

5. Enter the **certificate alias** and click **Import.**

Figure 3-6 Import Gateway Certificate



Import Certificate

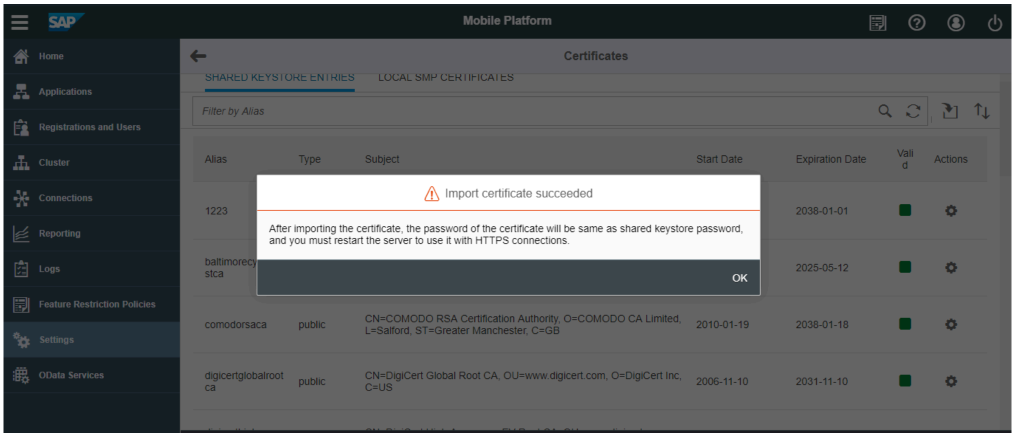
Certificate Type: X.509

*Alias: gwsnb

*Certificate File: GWSNB.cer

6. Click **OK.**

Figure 3-7 Import Certificate Success



Import certificate succeeded

After importing the certificate, the password of the certificate will be same as shared keystore password, and you must restart the server to use it with HTTPS connections.

3.4.1.3. Generate Root Certificate for HTTPs Authentication using OpenSSL

SMP default certificates do not work for HTTPs connections. You can use **OpenSSL** to generate **RootCA** and corresponding technical certificates for mutual setup or use Internal PKI Server for generating certificates.

Use this Root Certificate for the child/signed certificates to be recognized by the server/client. You need CA Server and Mobile Device Management for certificate distribution. Before proceeding, ensure you have:

- OpenSSL Software installed. You can use the link to download: https://www.openssl.org/.
- These details to generate Certificate for SMP Server
  - Country Name—Country where you have the SMP Server
  - State or Province Name
  - Locality Name
  - Organization Unit
  - Organization Unit Name
  - Common Name
  - Email ID – Optional
- SMP Keystore password

Assumptions

- You have discussed with Innovapptive and your organization about the HTTPs setup and certificate replacements. You have a backup of the entire SMP Software including certificates. You are aware of OpenSSL standards.
- Your organization has decided to use OpenSSL certificates instead of your Organizations PKI & RootCA.

If your organization has an internal PKI System, use it to generate the certificates signed by your Organization RootCA.

To create RootCA for SMP using **OpenSSL**:

1. Open **Command Prompt** and navigate to OpenSSL-Win64\bin.
2. Run these commands:
   a. openssl genrsa -des3 -out RootCertificate.key 2048

      Note:
      Your password should be same as SMP Keystore Password.

   b. openssl req -new -x509 -days 9999 -key RootCertificate.key -out RootCertificate.crt
   c. openssl genrsa -des3 -out smp.key 2048
   d. openssl req -new -key smp.key -out smp.csr
   e. Openssl x509 -req -days 365 -in smp.csr -CA RootCertificate.crt -CAkey RootCertificate.key-set_serial 01 -out smp.crt
   f. openssl pkcs12 -export -clcerts -in smp.crt -inkey smp.key -out smp.p12

3.4.1.4. Import OpenSSL Certificate to SMP Certificate

Import a **Root Certificate** and **Technical Certificate** to the SMP Key store. The certificates are generated from the Innovapptive Internal CA Server.

To import, log in to the **SMP Sandbox Admin URL**: https://hostname:8083/Admin/

3.4.1.5. Import Technical Certificate to Local SMP Certificate

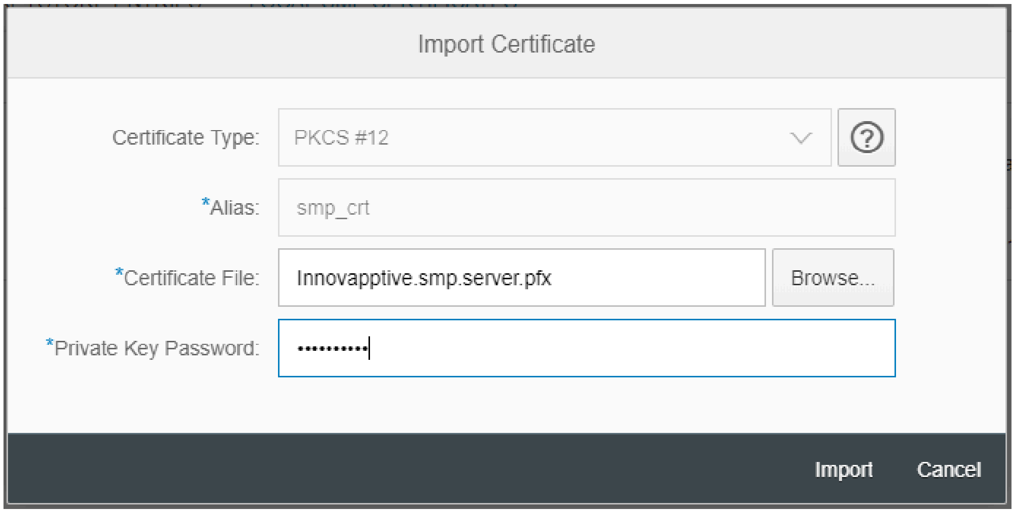
This is a local certificate and valid only on the local system. This is used as an authentication parameter for mutual trust between SMP and GW.

To import technical certificate to the local SMP certificate:

1. Go to **Settings, Certificates, Local SMP Certificate.**
2. Click **Browse.**
3. Select the certificate and enter the password.
4. Click **Import.**

> **Note:**
> The related Root Certificate should be imported on the Shared KeyStore.

Figure 3-8 Import Technical Certificate to Local SMP Certificate



Import Certificate

Certificate Type: PKCS #12

*Alias: smp_crt

*Certificate File: Innovapptive.smp.server.pfx

*Private Key Password: ••••••••••

5. Click **OK** in the **Import Success!** pop-up screen.
6. Repeat the same step in the **Shared KeyStore Entries** screen with alias as **smp_crt**.

3.4.1.6. Import Root and Intermediate Certificate to Shared KeyStore Entries

This certificate establishes a mutual connection with SMP and backend system. The same certificate is imported into the Gateway Sandbox.

To import root and intermediate certificate to Shared KeyStore Entries:

1. Click **Settings, Certificates, Shared SMP Certificate.**
2. Click **Browse.**
3. Select the Certificate: **RootCertificate.crt** and enter the alias name as **RootCAOpenSSL.**
4. Click **Import.**
5. Click **OK** in the **Import Success!** window.

   Now, you have imported four certificates into the SMP Sandbox:

   - RootCA
   - Intermediate CA.
   - SMP HOST Certificate.
   - SAP Gateway Certificate.

> **Note:**
> Any changes in the Certificate and SMP requires a restart to take effect. Restart the SMP Server.

3.4.1.7. Import the SMP Root CA to Gateway System

Import SAMA Internal Root CA **RootCA.cer** into the Gateway Sandbox to complete the mutual trust setup.

To import SMP Root CA to Gateway System:

1. Logon to SAP Gateway Sandbox system.
2. Go to **T-Code STRUST, SSL server Standard** and the component under it.
3. Click **Edit** and then click **Import Certificate**.
4. Browse the certificate **RootCA.cer** and then click **OK**.
5. Click **Add to Certificate List** and the certificate should be visible in the Certificate list.

> **Note:**
> Repeat the same steps for all three certificates:

- RootCA.
- Intermediate CA.
- SMP Host Certificate.

Figure 3-9 Import SMP Root CA to Gateway System

6. Click **Save** and then exit the **Tcode.**

   You can set up the Security profile for authentication mechanisms such as:

   - Basic HTTPs Login.
   - Basic SSO2 HTTPs Login.
   - LDAP Authentication.
   - SAML Authentication.
   - X509 Certificate based Authentication.

3.4.2. Create security profile for HTTPs Authentication

Create security profile for Basic HTTPs Authentication with SSO2 Tokens.

To create security profile for HTTPs Authentication:

1. Login to SMP Admin Cockpit and navigate to **Settings**, **Security Profiles**.
2. Click **New**.
3. Enter the **Security Profile Name**, for example, **HTTPs**.
4. Clear the **Check Impersonation** check box.
5. Click **Add**.
6. Select **HTTP/HTTPs Authentication** in the **Authentication Provider** drop-down and enter this information:

Field	Value
Control Flag	Optional
URL	https://innovapptive.gw.server:8001/sap/bc/ping
HTTP Connection Timeout Interval	60000
Client’s HTTP Values to Send	Authorization

Field	Value
Send Client HTTP Values as	header:Authorization
Successful Connection Status Code	200

7. Click **Test Settings**.
8. Click **Save**.

3.4.3. Create an Application using HTTPs Authentication

To create a new application using HTTPs authentication:

1. Log in to **SMP Admin Cockpit**.
2. Under **Application**, click **New**.

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

APP ID	Name	Vendor	Type	Service Name
com.innovapptive.massettag	Mobile Asset Tag	Innovapptive	Native	/INVMAT/MASSETTAG_2_SRV/
com.innovapptive.minventory	Mobile Inventory	Innovapptive	Native	/INVMIM/MINVENTORY_2_SRV/
com.innovapptive.mserviceorder	Mobile Service Order	Innovapptive	Native	/INVMSO/MSERVICEORDER_SRV/
com.innovapptive.mshop	Mobile Shopping Cart	Innovapptive	Native	/INVMSC/MSHOP_SRV/
com.innovapptive.mworklist	Mobile Universal Approvals	Innovapptive	Native	/INVMWL/MWORKLIST_3_SRV/

APP ID	Name	Vendor	Type	Service Name
com.innovapptive.mworkorder	Mobile WorkOrder	Innovapptive	Native	/INVMWO/MWORKORDER_SRV
com.innovapptive.racedynamicforms	RACE Dynamic Forms	Innovapptive	Native	/INVCEC/RACE_SRV/

3. Enter the following details in the **Create Application** window
   - **Application ID**: Enter the ID of the product.
   - **Version**: Enter the application version.
   - **Name**: Enter the name of the product.
   - **Type**: Select **Native**.
   - **Description**: Enter the description of the product.
   - **Vendor**: Enter Innovapptive Inc.
4. Click **Save**.
5. On the **Back End** tab, enter the primary connection details such as back-end URL and maximum number of connections.

   Endpoint:

   https://innovapptive.gw.server:8001/sap/opu/odata/iwfnd/rmtsampleflight/

   The following table lists the backend URLs for Innovapptive products.

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/
mServiceOrder	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/

Product	OData URL
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/

6. On the **Authentication** tab, select the Security Profile.
7. Click **Save**.
8. Select the Application from **Applications** menu and click **Ping**.

3.4.4. Test HTTPs authentication using REST client

To test HTTPs Registration on the Rest Client:

1. Access the **Advanced REST Client** extension on Chrome browser.
2. Enter this information:

Registration URL with HTTPs Port	https://innovapptive.smp.server:8091/odata/applications/latest/com.innovapptive.flight/Connections
Headers	-
X-SMP-APPCID	-
Content-Type	application/xml
Payload	<?xml version="1.0" encoding="utf-8"?> <entry xmlns="http://www.w3.org/2005/Atom" xmlns:m="http://schemas.microsoft.com/ado/2007/08/dataservices/metadata" xmlns:d="http://schemas.microsoft.com/ado/2007/08/dataservices"> <content type="application/xml"> <m:properties> <d:DeviceType>iPhone</d:DeviceType> </m:properties>

```
</content>

</entry>
```

Figure 3-10 Advanced REST Client

3. Click **Send**.
4. Enter SMP **Username** and **Password** and click **Log In.**

   If the authentication is successful, **201 Created Response** appears.

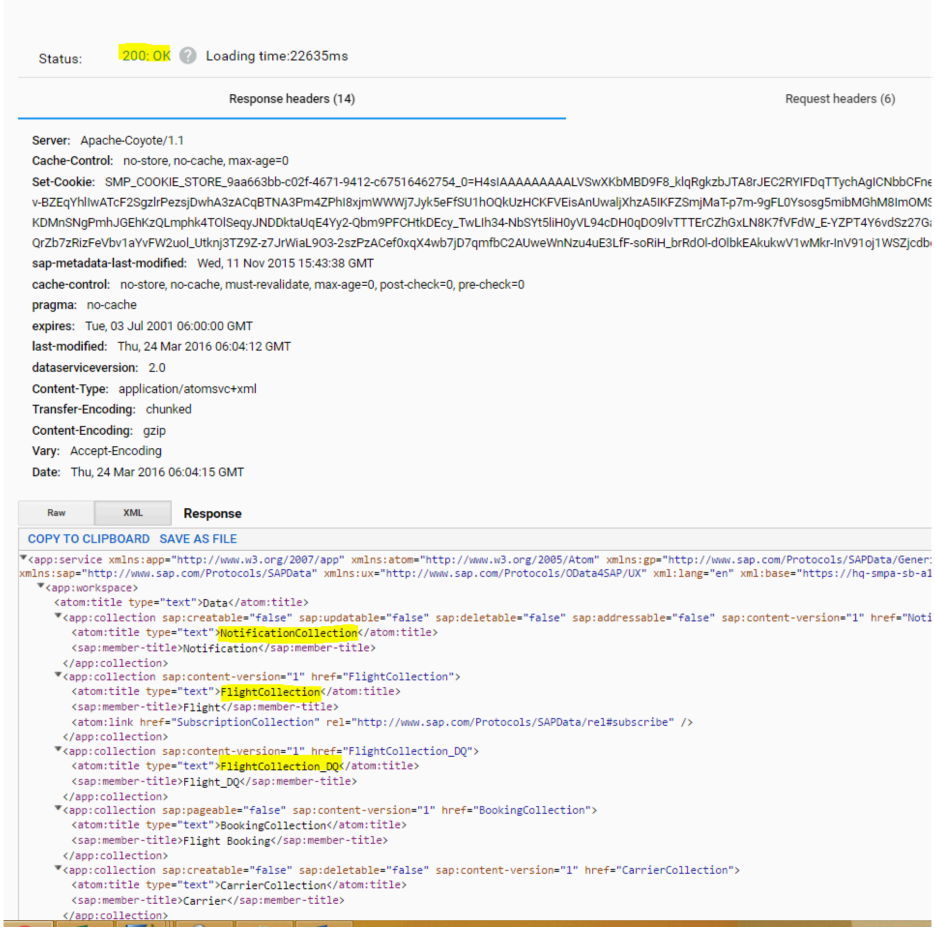
   Figure 3-11 Authentication successful screen

   You can also verify the registration in SMP using Registrations and Users menu.
5. Read Data (GET Query) from the Gateway system:

a. Copy the X-SMP-APP CID generated during the registration.
b. Enter the APP CID on **Headers** tab in the REST client.
c. Click **Send**.

The response 200 OK and data as shown in the screenshot, is displayed.

Figure 3-12 Response 200 OK screen



Status: 200: OK Loading time:22635ms

```
Server: Apache-Coyote/1.1
Cache-Control: no-store, no-cache, max-age=0
Set-Cookie: SMP_COOKIE_STORE_9aa663bb-c02f-4671-9412-c67516462754_0=H4sIAAAAAAAAALVSwXKbMBD9F8_klqRgkzbJTA8rJEC2RYIFDqTTychAgICNbbCFne
v-BZEqYhlIwATcF2SgzlrPezsjDwhA3zACqBTNA3Pm4ZPhI8xjmWWWj7Jyk5eFfSU1hOQkUzHCKFVEisAnUwaljXhzA5IKFZSmjMaT-p7m-9gFL0Ysosg5mibMGhM8ImOMS
KDMnSNgPmhJGEhKzQLmphk4TOlSeqyJNDDktaUqE4Yy2-Qbm9PFCHtkDEcy_TwLIh34-NbSYt5liH0yVL94cDH0qDO9lvTTTErCZhGxLN8K7fVFdW_E-YZPT4Y6vdSz27G
QrZb7zRizFeVbv1aYvFW2uol_Utknj3TZ9Z-z7JrWiaL9O3-2szPzACef0xqX4wb7jD7qmfbC2AUweWnNzu4uE3LfF-soRiH_brRdOl-dOlbkEAkukwV1wMkr-InV91oj1WSZjcdb
sap-metadata-last-modified: Wed, 11 Nov 2015 15:43:38 GMT
cache-control: no-store, no-cache, must-revalidate, max-age=0, post-check=0, pre-check=0
pragma: no-cache
expires: Tue, 03 Jul 2001 06:00:00 GMT
last-modified: Thu, 24 Mar 2016 06:04:12 GMT
dataserviceversion: 2.0
Content-Type: application/atomsvc+xml
Transfer-Encoding: chunked
Content-Encoding: gzip
Vary: Accept-Encoding
Date: Thu, 24 Mar 2016 06:04:15 GMT
```

```
<app:service xmlns:app="http://www.w3.org/2007/app" xmlns:atom="http://www.w3.org/2005/Atom" xmlns:gp="http://www.sap.com/Protocols/SAPData/Gener
xmlns:sap="http://www.sap.com/Protocols/SAPData" xmlns:ux="http://www.sap.com/Protocols/OData4SAP/UX" xml:lang="en" xml:base="https://hq-smpa-sb-a1
  <app:workspace>
    <atom:title type="text">Data</atom:title>
    <app:collection sap:creatable="false" sap:updatable="false" sap:deletable="false" sap:addressable="false" sap:content-version="1" href="Noti
      <atom:title type="text">NotificationCollection</atom:title>
      <sap:member-title>Notification</sap:member-title>
    </app:collection>
    <app:collection sap:content-version="1" href="FlightCollection">
      <atom:title type="text">FlightCollection</atom:title>
      <sap:member-title>Flight</sap:member-title>
      <atom:link href="SubscriptionCollection" rel="http://www.sap.com/Protocols/SAPData/rel#subscribe" />
    </app:collection>
    <app:collection sap:content-version="1" href="FlightCollection_DQ">
      <atom:title type="text">FlightCollection_DQ</atom:title>
      <sap:member-title>Flight_DQ</sap:member-title>
    </app:collection>
    <app:collection sap:pageable="false" sap:content-version="1" href="BookingCollection">
      <atom:title type="text">BookingCollection</atom:title>
      <sap:member-title>Flight Booking</sap:member-title>
    </app:collection>
    <app:collection sap:creatable="false" sap:deletable="false" sap:content-version="1" href="CarrierCollection">
      <atom:title type="text">CarrierCollection</atom:title>
      <sap:member-title>Carrier</sap:member-title>
    </app:collection>
```

3.5. Authenticate users using LDAP Server

Authenticate an end user using LDAP Authentication and manage communication between SMP and Gateway system using HTTPs ports.

Before proceeding, ensure you have:

- Access to SAP Mobile Platform as an Administrator (SMP Admin Cockpit)
- Access to SAP Gateway System with Basis roles
- GW Basis roles
- Access to SMP system as an administrator

- List of Gateway documents that need to be checked
- Completed SAP Gateway pre-installation configuration
- Completed SAP ECC and Gateway Add On installation
- Completed configurations as described in Authenticate users using HTTPs Authentication *(on page)*

3.5.1. LDAP Authentication with SSO2 Generator

From **SMP 3 server Service Pack 8** onwards, SMP uses SAP logon tickets to authenticate a user to a backend system. Also called as SAPSSO2 or MYSAPSSO2 cookies, SAP logon tickets are generated by SMP for an authenticated user and attached to requests going to backend system.

The authentication provider, SAPSSO2 Generator is used only in combination with other providers such as HTTP/HTTPs Authentication, LDAP, and SAML.

As there is no user mapping in SMP, the username authenticated in SMP must also exist in the backend system. User is authenticated using LDAP server and then the user details are posted to SAP backend using SSO2 Generator. To do this, a keypair is required to sign SAP logon tickets.

Note:

This key must be a **Digital Signature Algorithm** (DSA) key as **RSA is NOT supported**.

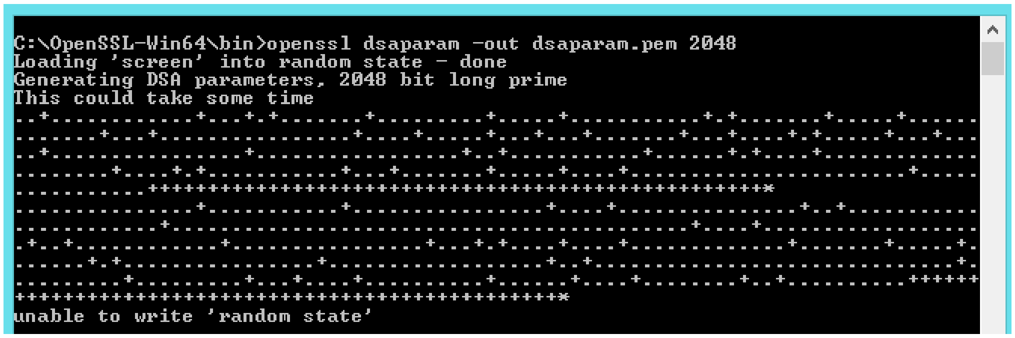
Use OpenSSL to create a self-signed certificate.

3.5.1.1. Generate certificate for SSO2 Generator (DSA)

To generate certificate for SSO2 Generator DSA:

1. In command prompt, execute **openssl dsaparam -out dsaparam.pem 2048.**

   Figure 3-13 DSA Parameter Command

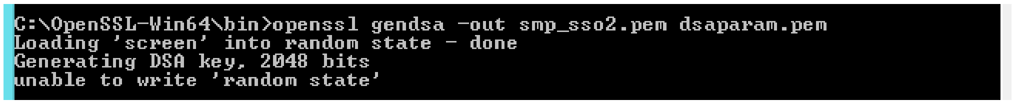
   

   ```
   C:\OpenSSL-Win64\bin>openssl dsaparam -out dsaparam.pem 2048
   Loading 'screen' into random state - done
   Generating DSA parameters, 2048 bit long prime
   This could take some time
   ..+............+...+.+.......+.........+.....+...........+.+.......+.....+......
   .......+...+................+....+.....+...+...+.......+...+....+.+.....+...+...
   ..+................+.................+..+...........+......+.+....+.............
   ........+....+.+...........+...+.......+.....+....+.......................+.....
   ...........+++++++++++++++++++++++++++++++++++++++++++++++++++*
   ...............+...........+................+....+...............+..+...........
   ............+...........................................+....+..................
   .+..+............+................+...+.+....+....+.............+.......+.....+.
   ......+.+................+..................+..+..............................+.
   .........+.........+...+....+..........+......+....+........+..+..........++++++
   +++++++++++++++++++++++++++++++++++++++++++++*
   unable to write 'random state'
   ```

2. Create a new DSA key based on the parameters:

   openssl gendsa -out smp_sso2.pem dsaparam.pem

   Figure 3-14 Create DSA Key

   ```
   C:\OpenSSL-Win64\bin>openssl gendsa -out smp_sso2.pem dsaparam.pem
   Loading 'screen' into random state - done
   Generating DSA key, 2048 bits
   unable to write 'random state'
   ```

3. Create a self-signed certificate. The common name should match with the SID of your system, for example, SMP.

   openssl req -days 730 -x509 -new -key smp_sso2.pem -out smp_sso2.cer

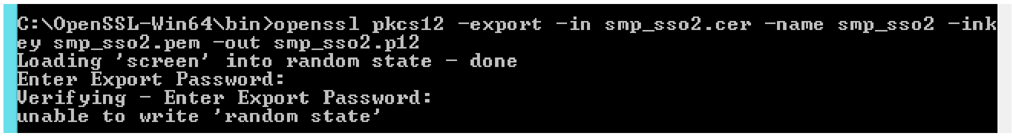
   Figure 3-15 SSO2 - Self-signed Certificate

   The output shown here is the certificate (public part), which you import later in your backend system.

Note:
As the Issue SID for SAPSSO2 Generator accepts only three characters with capital letters, use SMP for testing.

4. Create a keypair (PKCS12 keystore) and import this keypair into SMP keystore. (Define a password for this keystore). The attribute name defines the alias of the keypair inside this keystore.
   openssl pkcs12 -export -in smp_sso2.cer -name smp_sso2 -inkey smp_sso2.pem -out smp_sso2.p12

Figure 3-16 PKCS12 keypair command



```
C:\OpenSSL-Win64\bin>openssl pkcs12 -export -in smp_sso2.cer -name smp_sso2 -ink
ey smp_sso2.pem -out smp_sso2.p12
Loading 'screen' into random state - done
Enter Export Password:
Verifying - Enter Export Password:
unable to write 'random state'
```

3.5.1.2. Import ‘smp_sso2.p12’ certificate to SMP

To import the “smp_sso2_p12” certificate to SMP:

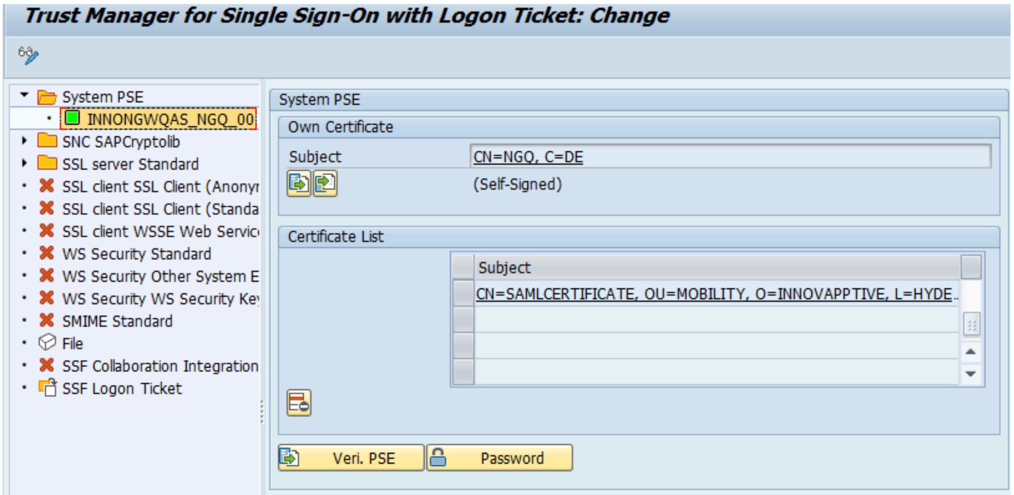
1. Go to **Settings, Certificates.**
2. Click **Import** and add the **smp_sso2.p12.**
3. Click **OK.**
4. Restart the SMP Server.

3.5.2. Import DSA certificate to GW Sandbox

To import the the smp.ss2.cer into the Gateway (GW) Sandbox system:

1. Navigate to **TCode: STRUSTSSO2** and import the certificate to System PSE.
2. Click **Add to Certificate List**.

Figure 3-17 Import Certificate


Trust Manager for Single Sign-On with Logon Ticket: Change
System PSE
INNONGWQAS_NGQ_00
SNC SAPCryptolib
SSL server Standard
SSL client SSL Client (Anonyı
SSL client SSL Client (Standa
SSL client WSSE Web Servic
WS Security Standard
WS Security Other System E
WS Security WS Security Ke
SMIME Standard
File
SSF Collaboration Integration
SSF Logon Ticket
System PSE
Own Certificate
Certificate List
Veri. PSE
Password

Subject: CN=NGQ, C=DE

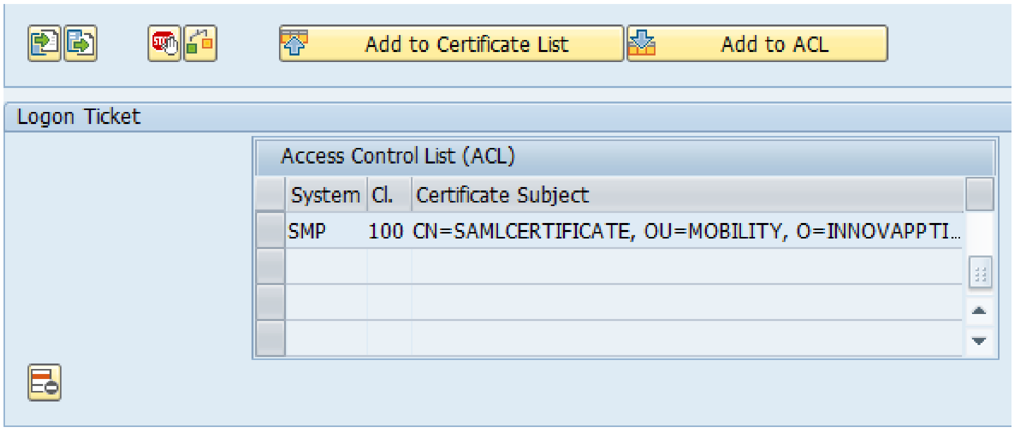
(Self-Signed)

Subject
CN=SAMLCERTIFICATE, OU=MOBILITY, O=INNOVAPPTIVE, L=HYDE..

3. Click **Add to ACL** and enter the details.

Note:
You will use the same details in the SMP Configurations.

Figure 3-18 Import Certificate 2



System	Cl.	Certificate Subject
SMP	100	CN=SAMLCERTIFICATE, OU=MOBILITY, O=INNOVAPPTI...

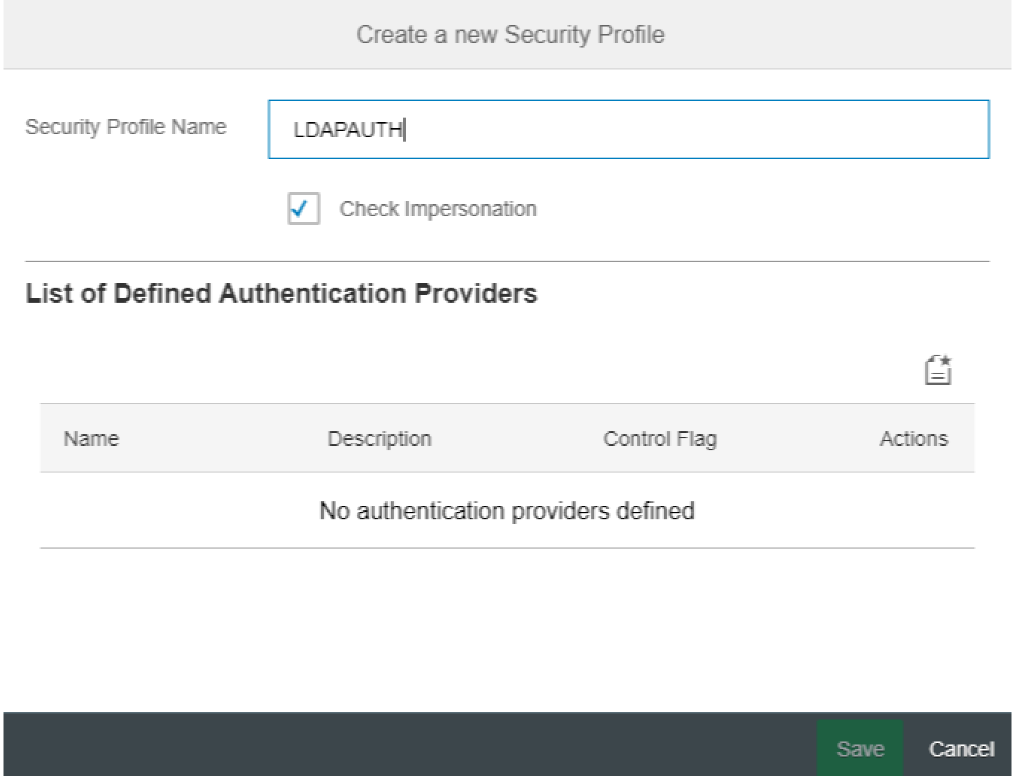
4. Click **Save**.

3.5.3. Create security profile for LDAP Authentication

To create a security profile for LDAP Authentication:

1. Log in to SMP Admin Cockpit.
2. Navigate to **Settings Tab, Security Profiles** and click **New**.
3. Enter the **Security Profile Name**, for example, **LDAPAUTH.**

Figure 3-19 LDAP Security Profile



Create a new Security Profile

Security Profile Name: LDAPAUTH

☑ Check Impersonation

List of Defined Authentication Providers

Name	Description	Control Flag	Actions
No authentication providers defined			

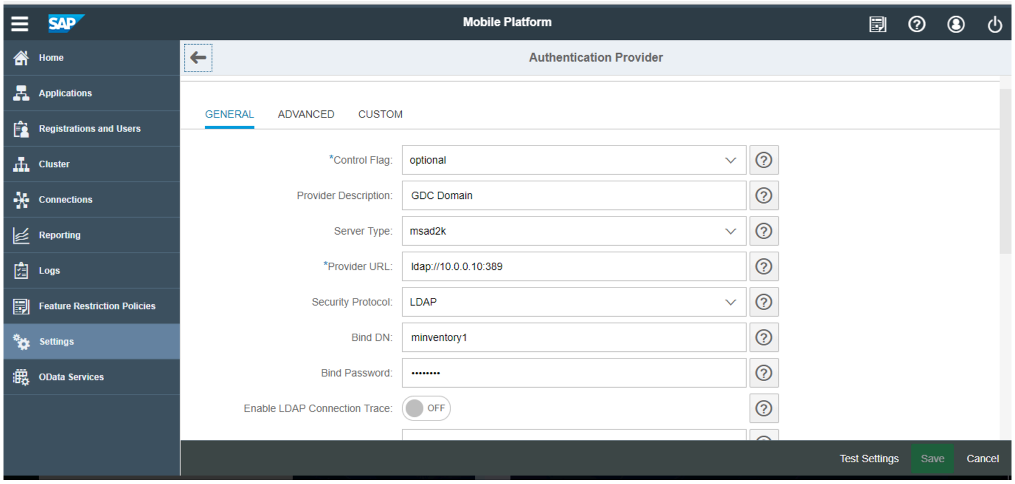
4. Click **Add** and select Directory Service (LDAP/AD) and enter the following details.

Property	Description
Server Type	Type of LDAP server.
LDAP URL	URL to connect to the LDAP server.
Security Protocol	Protocol to use when connecting to the LDAP server.
Bind DN	User Distinguished Name (DN) to bind when building the initial LDAP connection. This user needs read permissions on all user records.
Bind Password	Password for Bind DN to authenticate users.

Property	Description
Authentication Filter	Filter to find the username.
Role Search Base	Search to retrieve lists of roles. If this is not configured, the Default Search Base is used.
Role Filter	The role search filter, when combined with the role search base and role scope, displays the complete list of roles within LDAP server.
Default Search Base	LDAP search base that is used if no other search base is defined for authentication, roles, attribution, and self-registration.

5. Click **Save**.
6. Add the **LDAP Configurations,** as shown below.

Figure 3-20 LDAP Configurations



*Control Flag: optional

Provider Description: GDC Domain

Server Type: msad2k

*Provider URL: ldap://10.0.0.10:389

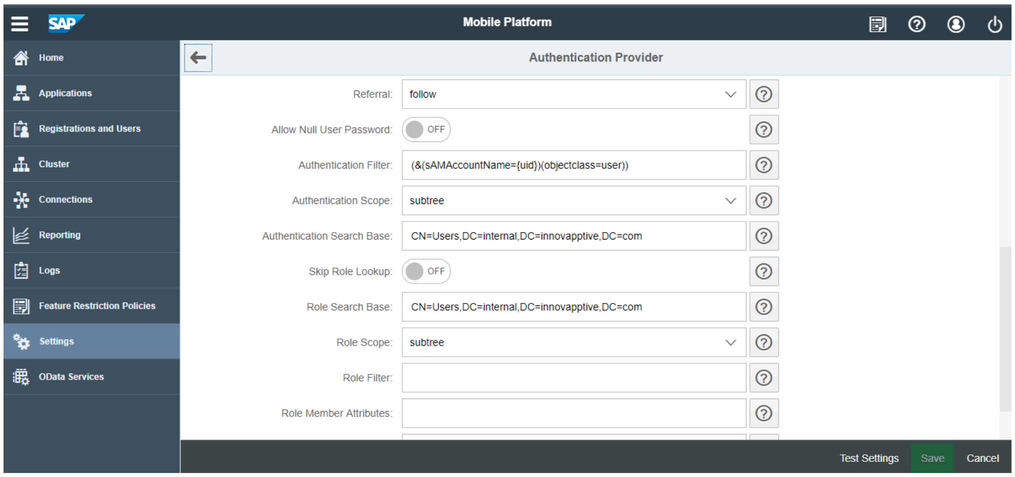
Security Protocol: LDAP

Bind DN: minventory1

Bind Password: ••••••••

Enable LDAP Connection Trace: OFF

Figure 3-21 LDAP Configuurations



Referral: follow

Allow Null User Password: OFF

Authentication Filter: (&(sAMAccountName={uid})(objectclass=user))

Authentication Scope: subtree

Authentication Search Base: CN=Users,DC=internal,DC=innovapptive,DC=com

Skip Role Lookup: OFF

Role Search Base: CN=Users,DC=internal,DC=innovapptive,DC=com

Role Scope: subtree

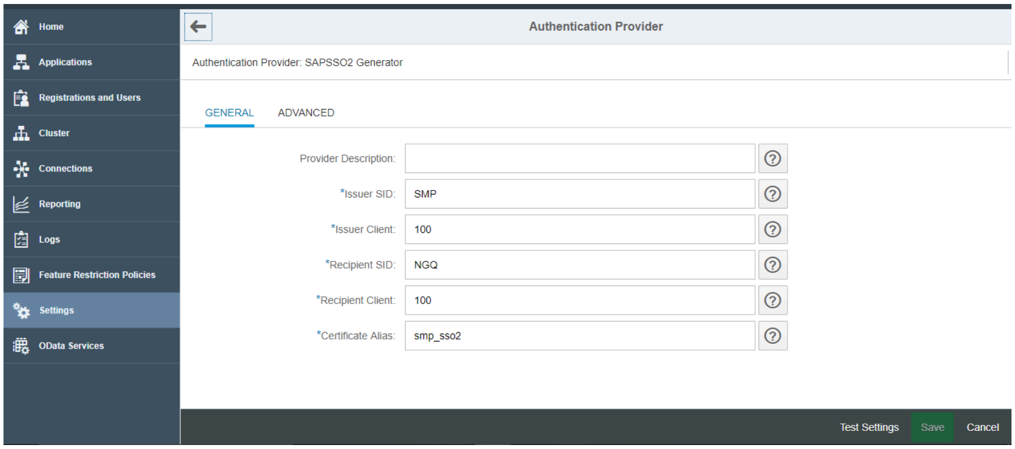
Role Filter:

Role Member Attributes:

7. Click **Save**.
8. Click **ADD** and select **Authentication Provider** as SAPSSO2 Generator.

9. Add **SSO2 Generator** details, as shown below.

Figure 3-22 SSO2 Generator details



Authentication Provider: SAPSSO2 Generator

Provider Description:

*Issuer SID: SMP

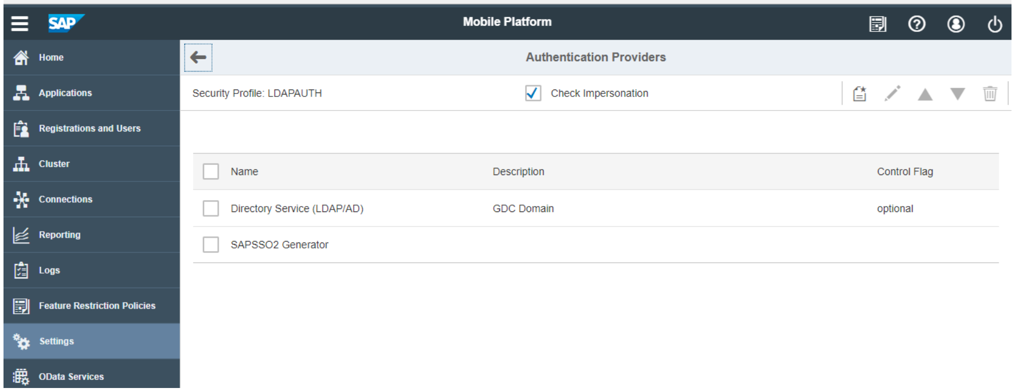
*Issuer Client: 100

*Recipient SID: NGQ

*Recipient Client: 100

*Certificate Alias: smp_sso2

Figure 3-23 SSO2 Generator details



Security Profile: LDAPAUTH ☑ Check Impersonation

Name	Description	Control Flag
□ Directory Service (LDAP/AD)	GDC Domain	optional
□ SAPSSO2 Generator		

10. Click **Save**.

3.5.4. Create an Application using LDAP Authentication

Learn how to create an Application using LDAP Authentication

To create an application using LDAP authentication:

1. Log in to the SMP Admin cockpit.
2. Under **Application**, click **New.**
3. Enter the following details in the **Create Application** window
    - **Application ID**: Enter the ID of the product.
    - **Version**: Enter the application version.
    - **Name**: Enter the name of the product.
    - **Type**: Select **Native**.
    - **Description**: Enter the description of the product.
    - **Vendor**: Enter Innovapptive Inc.
4. Click **Save**.
5. On the **Back End** tab, enter the primary connection details such as back-end URL and maximum number of connections.

   The following table lists the product Endpoints for Innovapptive products.

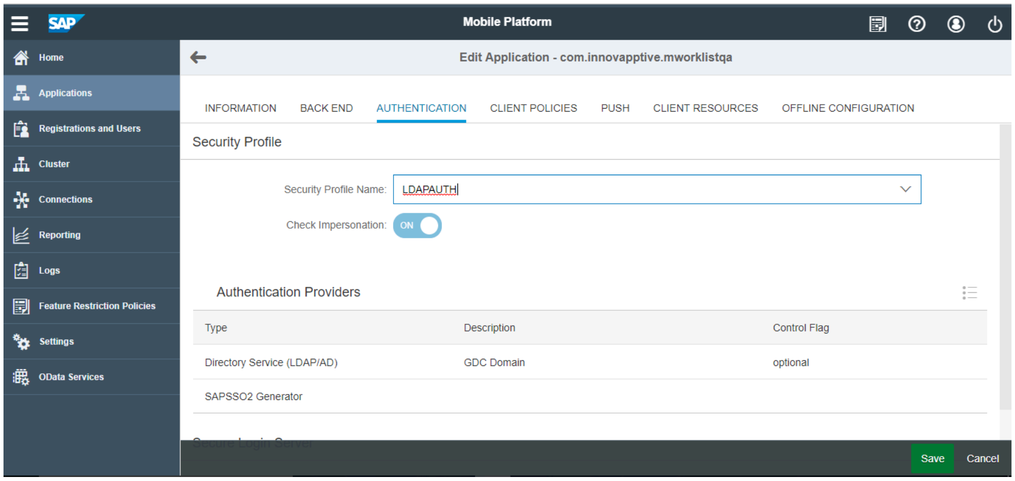
Product	OData URL
mAssetTag	http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/INVMAT/MASSETTAG_2_SRV/
mInventory	http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/INVMIM/MINVENTORY_2_SRV/
mServiceOrder	http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/INVMSO/MSERVICEORDER_SRV/
mShop	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/

6. Select SSO mechanism SSO2.

7. On the **Authentication** tab, select the Security Profile.

   Enable the **Check Impersonation** option.

   Figure 3-24 Security Profile for LDAP application



Security Profile

Security Profile Name: LDAPAUTH

Check Impersonation: ON

Authentication Providers

Type	Description	Control Flag
Directory Service (LDAP/AD)	GDC Domain	optional
SAPSSO2 Generator		

8. Click **Save**.

3.5.5. Test LDAP authentication using REST client

Use the General Registration process and GET data as shown below.

Figure 3-25 Advanced REST Client

3.6. Authenticate users using SAML Authentication

Authenticate an end user using SAML/ADFS Server and manage communication between SMP and Gateway system using HTTPs ports.

Create Security Profiles for SAML Authentication and SSO2 Generator for Backend Authentication and configure the Application IDs for connections.

Before proceeding, ensure you have:

- Access to SAP Mobile Platform as an Administrator (SMP Admin Cockpit)
- Access to SAP Gateway System with Basis roles
- GW Basis roles
- SAML Server Access/AD Resource
- Access to SMP system as an administrator

- ADFS Admin
- List of Gateway documents that need to be checked
- Completed configuration as described in Authenticate users using HTTPs Authentication *(on page 74)*.
- **Metadata Federation file** from the ADFS Admin

3.6.1. Establish trust between SMP and ADFS Server

To establish trust between SMP and Gateway servers exchange Metadata files between the systems.

1. Configure SAML with SMP *(on page 96)*
2. Import ADFS metadata file to SMP *(on page 96)*
3. Generate metadata file from SMP Server *(on page 97)*
4. Import SMP metadata file to ADFS Server *(on page 98)*

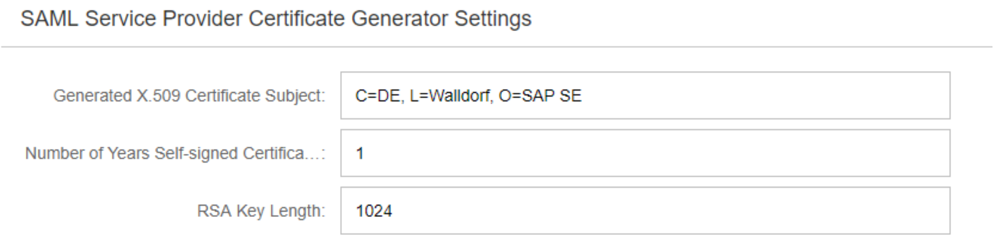
3.6.1.1. Configure SAML with SMP

To configure SAML with SMP server:

1. Log in to SMP Admin Cockpit and go to **Settings, System, SAML Service Provider Certificate Generator Settings.**
2. Enter the Certificate path of SMP Server.

Note:
It is recommended to use SMP Server details.

Figure 3-26 SAML Service Provider Certificate Generator Settings



SAML Service Provider Certificate Generator Settings

Generated X.509 Certificate Subject:	C=DE, L=Walldorf, O=SAP SE
Number of Years Self-signed Certifica...:	1
RSA Key Length:	1024

3. Click **Save**.

3.6.1.2. Import ADFS metadata file to SMP

To configure the trust between SMP Server and ADFS:

1. Log in to SMP Admin Cockpit and go to **Settings, SAML, Trusted Identity Provider**.
2. Click **New.**
3. Click **Browse** and select the **ADFS Metadata** file.
4. Ensure **Signature Algorithm** field is set as **SHA-256**.
5. Click **OK**.

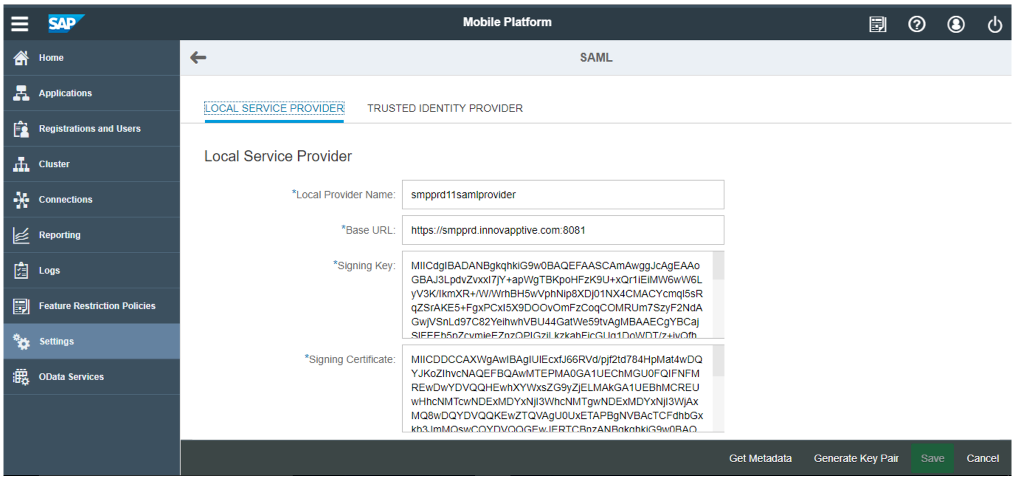
3.6.1.3. Generate metadata file from SMP Server

To generate metadata file from the SMP server and import it into ADFS Trusted Relying party:

1. Log in to **Admin Cockpit** and go to **Settings, SAML, Local Service Provider.**
2. Enter this information:
   - **Local Provider Name**
   - **Base URL**: This should be the server URL with HTTPs and port details.
   - **Signing Key:** Do not enter any value.
   - **Signing Certificate**: Do not enter any value.
3. Click **Generate Key Pair**.

   The **Signing Key** and **Signing Certificate** fields are populated based on **SAML Service Provider Certificate Generator Settings**.

Figure 3-27 Local Service Provider - SAML



Local Service Provider

*Local Provider Name: smpprd11samlprovider

*Base URL: https://smpprd.innovapptive.com:8081

*Signing Key:

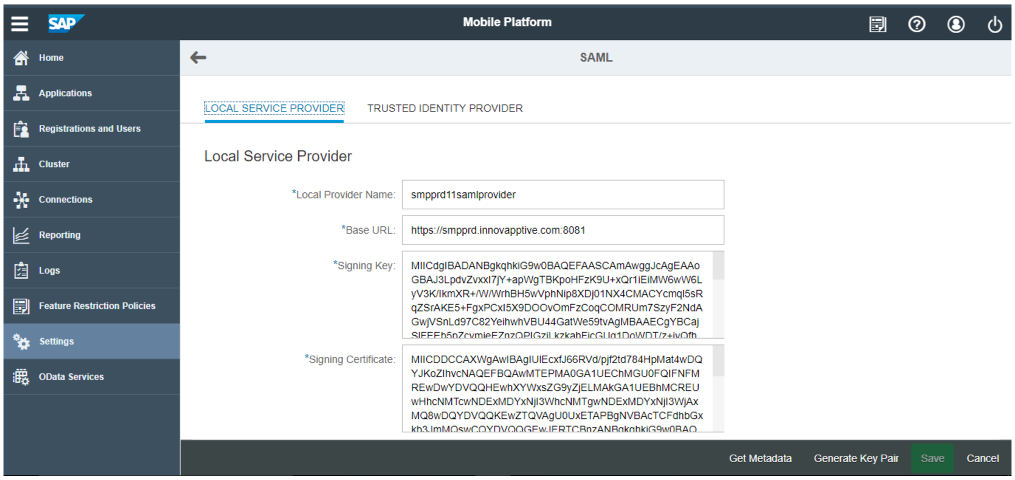
```
MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAo
GBAJ3LpdvZvxxI7jY+apWgTBKpoHFzK9U+xQr1iEiMW6wW6L
yV3K/IkmXR+/W/WrhBH5wVphNip8XDj01NX4CMACYcmqI5sR
qZSrAKE5+FgxPCxI5X9DOOvOmFzCoqCOMRUm7SzyF2NdA
GwjVSnLd97C82YeihwhVBU44GatWe59tvAgMBAAECgYBCaj
SIEEFb5nZcvmieFZnzQPIGziLkzkahFicGUg1DoWDT/z+ivOfh
```

*Signing Certificate:

```
MIICDDCCAXWgAwIBAgIUIEcxfJ66RVd/pjf2td784HpMat4wDQ
YJKoZIhvcNAQEFBQAwMTEPMA0GA1UEChMGU0FQIFNFM
REwDwYDVQQHEwhXYWxsZG9yZjELMAkGA1UEBhMCREU
wHhcNMTcwNDExMDYxNjI3WhcNMTgwNDExMDYxNjI3WjAx
MQ8wDQYDVQQKEwZTQVAgU0UxETAPBgNVBAcTCFdhbGx
kb3JmMQswCQYDVQQGEwJERTCBnzANBgkqhkiG9w0BAQ
```

Your-Dispatcher settings are shown as:

Figure 3-28 Your-Dispatcher settings



Local Service Provider

*Local Provider Name: smpprd11samlprovider

*Base URL: https://smpprd.innovapptive.com:8081

*Signing Key:

```
MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAo
GBAJ3LpdvZvxxI7jY+apWgTBKpoHFzK9U+xQr1iEiMW6wW6L
yV3K/IkmXR+/W/WrhBH5wVphNip8XDj01NX4CMACYcmql5sR
qZSrAKE5+FgxPCxI5X9DOOvOmFzCoqCOMRUm7SzyF2NdA
GwjVSnLd97C82YeihwhVBU44GatWe59tvAgMBAAECgYBCaj
SIFEEb5nZcvmieFZnzQPIGziLkzkabFicGUq1DoWDT/z+ivQfh
```

*Signing Certificate:

```
MIICDDCCAXWgAwIBAgIUIEcxfJ66RVd/pjf2td784HpMat4wDQ
YJKoZIhvcNAQEFBQAwMTEPMA0GA1UEChMGU0FQIFNFM
REwDwYDVQQHEwhXYWxsZG9yZjELMAkGA1UEBhMCREU
wHhcNMTcwNDExMDYxNjI3WhcNMTgwNDExMDYxNjI3WjAx
MQ8wDQYDVQQKEwZTQVAgU0UxETAPBgNVBAcTCFdhbGx
kb3JmMQswCQYDVQQGEwJERTCBnzANBgkqhkiG9w0BAQ
```

4. Click **Get Metadata** and save the file.

   Share this metadata file to ADFS Admin.

3.6.1.4. Import SMP metadata file to ADFS Server

To configure ADFS System to trust SMP Server:

1. Open **Server Manager Console.**
2. Go to **Tools, AD FS Management** to open the **AD FS Management Console**.
3. In the **AD FS Management Console**, go to **AD FS, Trust Relationships**.
4. Right-click **Relying Party Trust** and select **Add Relying Party Trust**.
5. Click **Next**.
6. On the **Select Data Source** screen:
   - Select **Import data** about the relying party from a file.
   - Click **Browse** to select the **smp-metadata.xml** file.
   - Click **Next.**
7. On the **Specify Display Name** screen, enter a name for the relying party trust.
8. Click **Next**

   Display Name should be same as **Local Provider Name** in ADFS.
9. On the **Configure Multi-Factor Authentication Now?** screen, select **I do not want to configure authentication settings for the relying party trust at this time**.
10. Click **Next**.

11. On the **Choose Issuance Authorization Rules** screen, select **Permit all users to access the relying party.**
12. On the **Ready to Add Trust** screen, review the information in the tabs.
13. Click **Next.**
14. Clear the **Open the Edit Claim Rules** checkbox.
15. Click **Close.**
16. Open the **AD FS Management Console**.
17. Right-click the **Created Trust** (here called SMPDEV) and select **Edit Claim Rules**.
18. In the **Issuance Transform** tab, click **Add Rules**.
19. In the **Choose Rule Type**, select **Send LDAP Attributes as Claims preferable**.
20. Create a rule to get the **Given Name Attribute** for an authenticated Active Directory User.
21. Create another rule to transform the **Given Name Attribute** as an identity claim to be used by the Service Provider.
22. Click **OK**.

3.6.2. Create security profile for SAML Authentication

To create a security profile for SAML Authentication:

1. Login to SMP Admin Cockpit and go to **Settings**, **Security Profiles**.
2. Click **New**.
3. Enter the **Security Profile Name**, for example, **SAMLSSO**.
4. Click **Add** and select SAML2 as **Authentication Provider**.
5. Enter the **Identity Provider Name** as the **Trust Identity Provider Name** maintained in SAML.
6. Click **Save**.
7. Click **ADD** and select authentication provider SAPSSO2 Generator.
   For SSO2 generator setup, see Authenticate users using LDAP Server *(on page 85)*.
8. Click **Save**.

3.6.3. Create an Application using SAML Authentication

To create an application using SAML authenticaton:

1. Log in to the SMP Admin cockpit.
2. Under **Application**, click **New.**
3. Enter the following details in the **Create Application** window
    - **Application ID**: Enter the ID of the product.
    - **Version**: Enter the application version.
    - **Name**: Enter the name of the product.
    - **Type**: Select **Native**.
    - **Description**: Enter the description of the product.
    - **Vendor**: Enter Innovapptive Inc.
4. Click **Save**.
5. On the **Back End** tab, enter the primary connection details such as back-end URL and maximum number of connections.

    The following table lists the product Endpoints for Innovapptive products.

Product	OData URL
mAssetTag	http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/IN-VMAT/MASSETTAG_2_SRV/
mInventory	http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/IN-VMIM/MINVENTORY_2_SRV/
mService-Order	http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/IN-VMSO/MSERVICEORDER_SRV/
mShop	http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/IN-VMSC/MSHOP_SRV/
mWorklist	http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/IN-VMWL/MWORKLIST_3_SRV/
mWorkOrder	http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/IN-VMWO/MWORKORDER_SRV/
RACE Dynamic Forms	http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/IN-VCEC/RACE_SRV/

6. Select SSO mechanism SSO2.
7. On the **Authentication** tab, select the Security Profile.
    Enable the **Check Impersonation** option.
8. Click **Save**.

3.6.4. Define SMP SAML Client Password Policy

The application developer must have added enforcement code to the application DataVault to enforce the password policy. The administrator enters the application password policy that is used to unlock the DataVault during application initialization.

The client password policy applies only to the application password that is used to unlock the DataVault during application initialization; it has nothing to do with SAP Mobile Platform security profiles or the back-end security systems with which they integrate. Password policies for back-end security systems are administered by customer information technology departments using their native security administration tools.

To define the SMP SAML password policy:

1. Login to SMP Management Cockpit and select **Applications**.
2. For an application, select **Settings, Configure, CLIENT POLICIES**.
3. Select **Enable Passcode Policy.**
4. Enter this information:

Property	Default	Description
Expiration Days	0	Number of days a password is valid before it expires.
Minimum Length	8	Minimum password length required.
Retry Limit	10	Number of attempts allowed when entering an incorrect password. After this number of attempts, the client is locked out, and the DataVault and all its contents are permanently deleted, the application is permanently unusable, and its encrypted data is inaccessible.
Minimum Unique Characters	0	Minimum number of unique characters required in the password.

Property	Default	Description
Lock Timeout	300	Number of seconds the DataVault remains unlocked within the application, while the application remains inactive.
Default Passcode Allowed	Disabled	Indicates whether a default password can be generated by the DataVault; from the user's point of view this policy turns off the password.
Has Digits	Disabled	Indicates whether the password must include digits.
Has Lower	Disabled	Indicates whether the password must include lower case letters.
Has Upper	Disabled	Indicates whether the password must include upper case letters.
Has Special	Disabled	Indicates whether the password must include special characters.
Fingerprint Allowed	Disabled	Indicates whether you can unlock the application with a fingerprint.

5. Click **Save.**

3.7. Authenticate users using X.509 Authentication

Authenticate an end user using X.509 Server and manage communication between SMP and Gateway system using HTTPs ports.

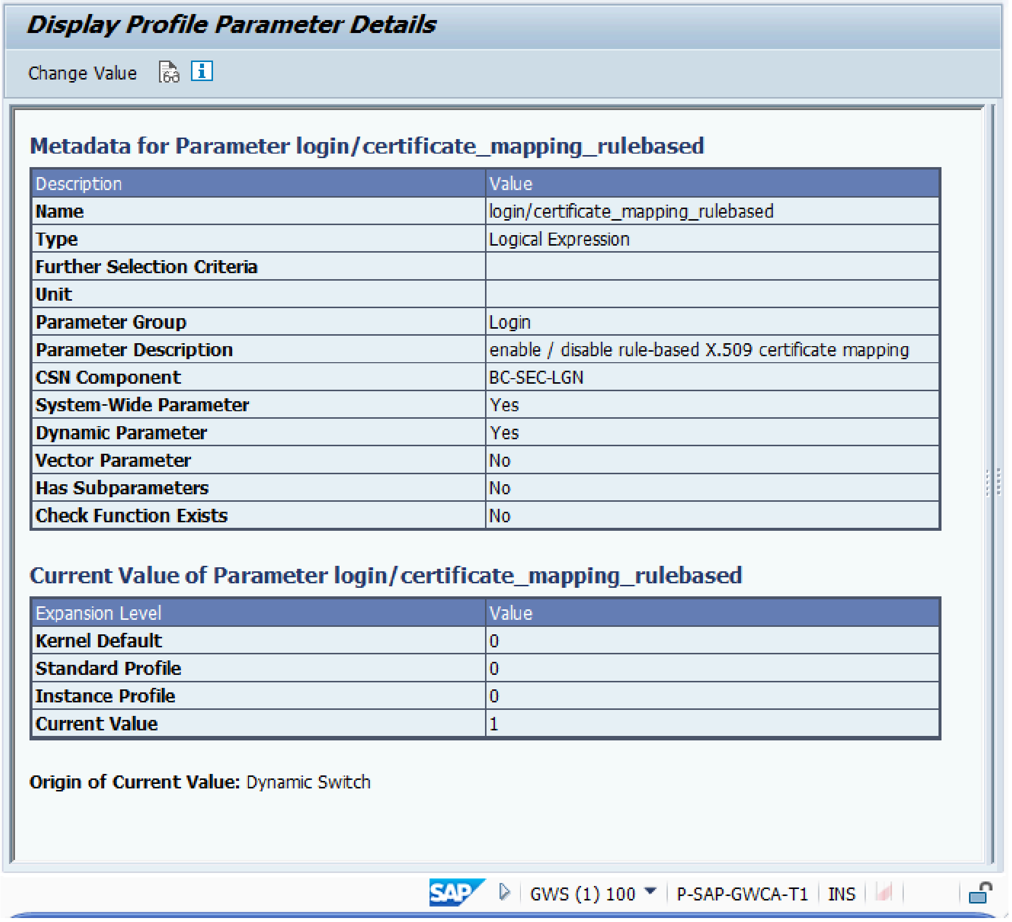
Rule-based certificate mapping (transaction CERTRULE) enables mapping of users from parts of the subject or the subject alternative name of an X.509 certificate for a given issuer to the user ID or alias of a user master record. With a few rules, you can enable logon with X.509 certificates for all users. The tool also enables you to load an X.509 certificate and check if a rule applies to the certificate and if the certificate maps to a user. For individual users that do not map to the rules you create, you can create exceptions.

Ensure you have,

- Access to SAP Mobile Platform as an Administrator (SMP Admin Cockpit)
- Access to SAP Gateway System
- GW Basis roles
- List of Gateway documents that need to be checked
- Completed configuration as described in Authenticate users using HTTPs Authentication *(on page 74)*
- Authorization objects:
  - CC control center: System administration (S_RZL_ADM)
    - Activity 03 grants display authorizations.
    - Activity 01 grants change authorizations.
- User Master Maintenance: User Groups (S_USER_GRP)
  - Activity 03 grants display authorizations.
  - Activity 02 grants change authorizations.
  - Class: Enter the names of user groups for which the administrator can maintain explicit mappings.
- Enabled the login/certificate_ mapping_ rulebased profile parameter

- ◦ Go to RZ11 or RZ10.
- ◦ Maintain the profile parameter **login/certificate_mapping_rulebased** value to 1.
- ◦ Save the settings and close.

Figure 3-29 Rule Based Profile Parameter



Display Profile Parameter Details

Metadata for Parameter login/certificate_mapping_rulebased

Description	Value
Name	login/certificate_mapping_rulebased
Type	Logical Expression
Further Selection Criteria	
Unit	
Parameter Group	Login
Parameter Description	enable / disable rule-based X.509 certificate mapping
CSN Component	BC-SEC-LGN
System-Wide Parameter	Yes
Dynamic Parameter	Yes
Vector Parameter	No
Has Subparameters	No
Check Function Exists	No

Current Value of Parameter login/certificate_mapping_rulebased

Expansion Level	Value
Kernel Default	0
Standard Profile	0
Instance Profile	0
Current Value	1

Origin of Current Value: Dynamic Switch

- Alias for the SAP User Name (Required for Innovapptive, as Certificate does not have SAP User Name)

Note: Once enabled, rule-based mapping replaces manual mapping in the table USREXTID. If you use the table USREXTID for certificate mapping, use transaction CERTRULE_MIG to create a set of rules based on your current entries.

3.7.1. Generate certificates for X509 Authentication

Learn how to generate User Certificate and Technical Certificate and sign it by the Root Certificate.

Same commands are used for both Technical Certificate and User Certificate. You may use the User name of Gateway System while generating the user certificate.

Technical Certificate is used for communication between SMP Server and Gateway Server. This should have the password same as **SMP Keystore**.

To generate the certificates:

1. Open **Command Prompt** and navigate to OpenSSL-Win64\bin.
2. Run these commands:
    a. Openssl genrsa -des3 -out 4374446.key 2048.
    b. openssl req -new -key 4374446.key -out 4374446.csr
    c. openssl x509 -req -days 365 -in 4374446.csr -CA RootCertificate.crt -CAkey RootCertificate.key -set_serial 01 -out 4374446.crt
    d. openssl pkcs12 -export -clcerts -in 4374446.crt -inkey 4374446.key -out 4374446.p12

   Total Certificates generated for X509:

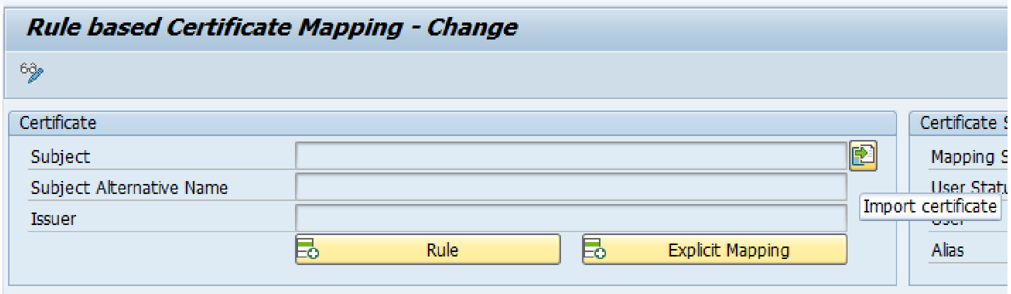
    - Technical Certificate (Preferred to be a Basis User ID from Gateway).
    - User Certificate (Based on the number of users, you have to generate X number of certificates to be distributed to them. Ensure there are no manual errors).

3.7.2. Import a Certificate to Create Rule

To import a certificate to create a rule:

1. Navigate to T-Code **CERTRULE**.
2. Ensure that you are in the Edit Mode.
3. Click **Import Certificate.**

   Figure 3-30 Import Certificate



4. Select the certificate, which is generated from Innovapptive PKI Service.
5. Click **Allow** on the GUI Security.

6. Click **Rule.**
7. Make the following changes (as in below image):

   Figure 3-31 Create Rule

8. Click **Generate** and click **OK** and Save your settings.

   The Mapping Status and User Status must be as:

   Figure 3-32 Certificate Status

   This completes Certificate Rule Mapping for One OU Structure. All the users with this OU can login with this Certificate. Ensure the Alias Perquisite is maintained for all the users.

3.7.3. Test the Certificate on a Browser

Test the URL from the Gateway Sandbox to ensure the certificate is working.

To test the certificate on a browser:

1. Install the Certificate in your browser and open the URL in Chrome Browser and then press <Enter>.
   innovapptive.gw.server https://innovapptive.gw.server:8001/sap/opu/odata/iwfnd/rmtsampleflight/

   The User Certificate that is installed on system pops-up.
2. Click **OK.**
3. Click **Advanced**, and click **Proceed to innovapptive.gw.server unsafe).**

   > **Note:**
   > Ignore the certificate error, as the certificate is not a signed certified.

   The data from oData Service is shown:

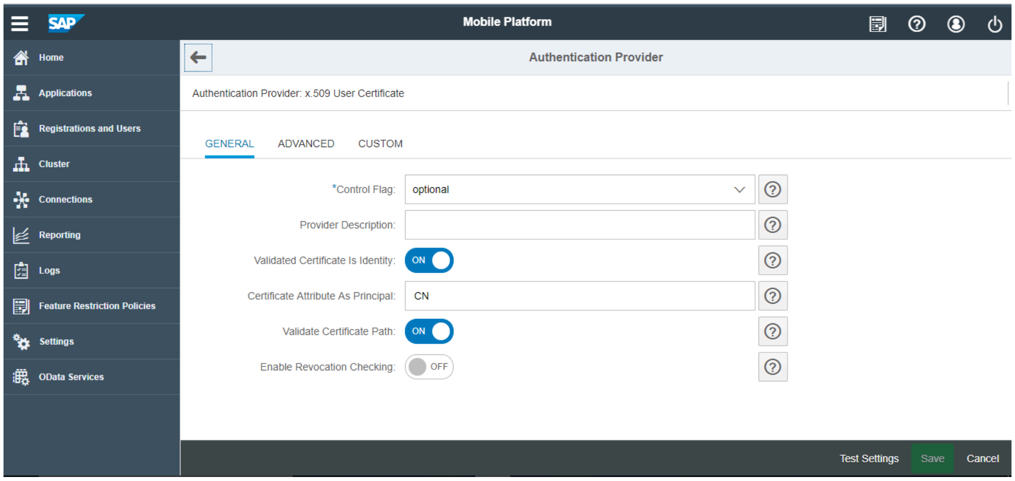
   Figure 3-33 X509 Certificate Testing

3.7.4. Create Security Profile for X509-Based Authentication

To create security profile for X509-based authentication:

1. Log in to SMP Admin cockpit.
2. Go to **Settings, Security Profiles.**
3. Click **New.**
4. Enter the **Security Profile Name**, for example, **X509 Rule Based**.
5. Click **Add**.
6. Select Authentication Provider as **x.509 User Certificate** and enter the following details.

Figure 3-34 x.509 Security Profile



Authentication Provider: x.509 User Certificate

*Control Flag: optional

Provider Description:

Validated Certificate Is Identity: ON

Certificate Attribute As Principal: CN

Validate Certificate Path: ON

Enable Revocation Checking: OFF

7. Click **Save**.

3.7.5. Create an Application using X509-Based Authentication

To create an application using X509-Based authentication:

1. Log in to the SMP Admin cockpit.
2. Under **Application**, click **New.**
3. Enter the details in the **New Application** window and click **Save**.
4. On the **Back End** tab, enter the primary connection details such as back-end URL and maximum number of connections.

   The following table lists the product Endpoints for Innovapptive products.

Product	OData URL
mAssetTag	http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/IN-VMAT/MASSETTAG_2_SRV/
mInventory	http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/IN-VMIM/MINVENTORY_2_SRV/

Product	OData URL
mService-Order	http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/IN-VMSO/MSERVICEORDER_SRV/
mShop	http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/IN-VMSC/MSHOP_SRV/
mWorklist	http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/IN-VMWL/MWORKLIST_3_SRV/
mWorkOrder	http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/IN-VMWO/MWORKORDER_SRV/
RACE Dynamic Forms	http(s)://<gw_system_host>:<http(s)_port>/sap/opu/odata/IN-VCEC/RACE_SRV/

Note:
A general Certificate is required to make a backend connection, once the user is authenticated. This is referred as a technical certificate.

5. On the **Authentication** tab, select the Security Profile (X509 Rule Based).
6. Click **Save**.

3.7.6. Test X509 authentication using RESTClient

To test X509 authentication using REST client:

1. Open the **RESTClient**.
2. Enter these details:

URL	https://innovapptive.smp.server:8092/odata/applications/latest/com.x509.test/Connections
X-SMP-AP-PCID	
Content-Type	application/xml

Payload	<?xml version="1.0" encoding="utf-8"?> <entry xmlns="http://www.w3.org/2005/Atom" xmlns:m="http://schemas.microsoft.com/ado/2007/08/dataservices/metadata" xmlns:d="http://schemas.microsoft.com/ado/2007/08/dataservices"> <content type="application/xml"> <m:properties> <d:DeviceType>iPhone</d:DeviceType> </m:properties> </content> </entry>

3. Click **Send.**

Figure 3-35 X509 test using RESTClient

4. Click **OK**.

The user gets registered successfully with Alias Name on SMP Server with the following message as shown in the below screenshot.

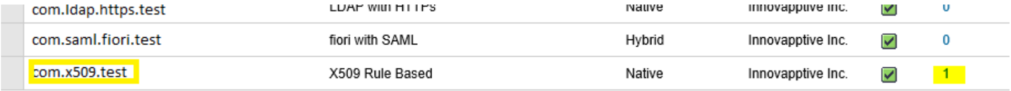
Figure 3-36 X509 RESTClient Response

5. Copy the **X-SMP-APPCID** and paste the value in box to perform the **Get operations** as shown below.

Figure 3-37 x509 X-SMP-APPCID Get Operation

User registration is shown in SMP.

Figure 3-38 x509 User Registration in SMP



com.ldap.https.test	LDAP with HTTPS	Native	Innovapptive Inc.	☑	0
com.saml.fiori.test	fiori with SAML	Hybrid	Innovapptive Inc.	☑	0
com.x509.test	X509 Rule Based	Native	Innovapptive Inc.	☑	1

3.8. Integrate SMP with Azure AD

By integrating SMP with Azure AD:

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

To integrate SMP with Azure AD:

- Create Non-Gallery Application in Microsoft Azure.
- Configure the application for Single Sign-On.
- Download the SAML Signing Certificate and import to SMP.
- Test application registration using Microsoft Azure AD.

3.8.1. Create Non-Gallery Application in Microsoft Azure

To create a Non-Gallery Application in Azure AD:

1. Login to Microsoft Azure AD cockpit.
   Access this URL: https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview
2. Select the **Azure Active Directory**, **Enterprise Applications**, **All Applications**.
3. Click **New Application**.
4. Select **Non-gallery Application** option.
5. Enter application name mwosaml.

Figure 3-39 Azure Non-gallery Application

3.8.2. Configure Application for Single Sign-on

To configure the application for Single Sign-on:

1. Click on the Application and navigate to the application property page.
2. Select **Single Sign** options on the left pane.
3. Under **Single Sign-on Mode,** select **SAML-based Sign-on** from the drop-down.
4. Enter this information:

   a. **Identifier**: mwosaml
   b. **Reply URL:** https://workordersmp.innovapptive.com:8081/saml/sso

      Here, **mwosaml** is non-gallery application name created in Microsoft Azure and **workordersmp.innovapptive.com** is the host name of SMP.

      By using Reply URL, Microsoft Azure sends a reply to SMP after the user authentication.

5. In the **SAML Signing Certificate** section, click **Metadata XML** and save the metadata file.

3.8.3. Import metadata file to SMP

To import metadata file to SMP:

1. Log in to SMP Admin cockpit.
2. Navigate to **Settings**, **SAML**.
3. Select **TRUSTED IDENTITY PROVIDER.**
4. Click **New**.
5. Click **Browse** to select the metadata file.
6. Click **OK**.

3.8.4. Configure Resource Application ID in SMP

To create the resource application ID in SMP:

1. Log in to SMP Admin cockpit.
2. Click on the **Application**.
3. On the **Edit Application** screen, under **INFORMATION** tab, enter this information:
   - **Application ID**: mwo.saml.res.
   - **Name**: mwo.saml.res.
4. On the **Backend** tab, enter this information:
   - **Back-End URL**: http://ngwq.innovapptive.com:8000/sap/bc/ping.
   - **Allow Anonymous Access**: Select the check box to enable it.
5. On the **Authentication** tab, enter NoAuth in the **Security Profile Name** field.
6. On the **Client Resources** tab:
   a. **Upload Client Resource:** Click **Browse** to select and upload the resources file with **Bundle Name** as **Resources_ios**.

3.8.5. Configure the Security Profile in SMP

To configure the security profile in SMP:

1. Click **Settings** in SMP cockpit.
2. Go to **Settings, Security Profiles.**
3. Click **New.**
4. Enter the **Security Profile Name**, for example, **SAMLSSO2Generator**.
5. Select **SAML2** and **SAPSSO2 Generator** as authentication providers.
6. Configure the Authentication Provider **SAML2** by using **Identity Provider Name.**
7. Click **Test Settings**.
8. Click **Save**.
9. Click **OK**.

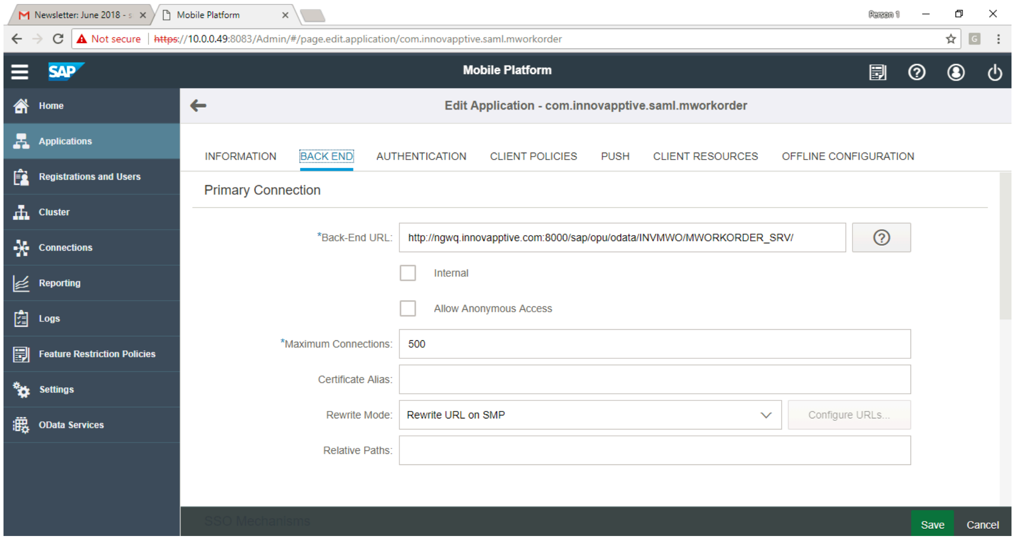
   To configure the Authentication Provider **SAPSSO2 Generator**, see LDAP Authentication with SSO2 Generator *(on page 86)* .

3.8.6. Configure Main Application ID in SMP

To configure Main Application ID in SMP:

1. Log in to SMP Admin cockpit.
2. Click on the **Application**.
3. On the **Edit Application** screen, under **Information** tab, enter **com.innovapptive.saml.mworkorder** in the **Application ID** field .
4. Under **Authentication** tab, enter **SAMLSSO2Generator** in the **Security Profile Name** field.
5. Under **Back End** tab, create two backend connections **com.innovapptive.saml.mworkorder** and **com.innovapptive.mworace** using SSO Mechanisms as SSO2.

Figure 3-40 SMP Application Back End tab



https://10.0.0.49:8083/Admin/#/page.edit.application/com.innovapptive.saml.mworkorder

Edit Application - com.innovapptive.saml.mworkorder

Primary Connection

*Back-End URL: http://ngwq.innovapptive.com:8000/sap/opu/odata/INVMWO/MWORKORDER_SRV/

□ Internal

□ Allow Anonymous Access

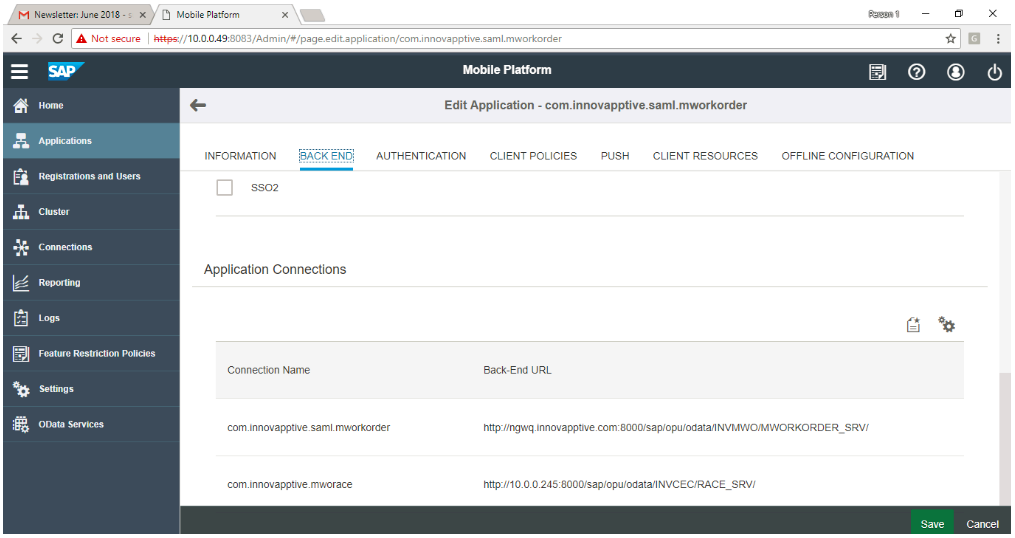
*Maximum Connections: 500

Certificate Alias:

Rewrite Mode: Rewrite URL on SMP

Relative Paths:

Figure 3-41 SMP Application Back End tab



https://10.0.0.49:8083/Admin/#/page.edit.application/com.innovapptive.saml.mworkorder

Edit Application - com.innovapptive.saml.mworkorder

□ SSO2

Application Connections

Connection Name	Back-End URL
com.innovapptive.saml.mworkorder	http://ngwq.innovapptive.com:8000/sap/opu/odata/INVMWO/MWORKORDER_SRV/
com.innovapptive.mworace	http://10.0.0.245:8000/sap/opu/odata/INVCEC/RACE_SRV/

3.8.7. Test Application registration using Azure AD

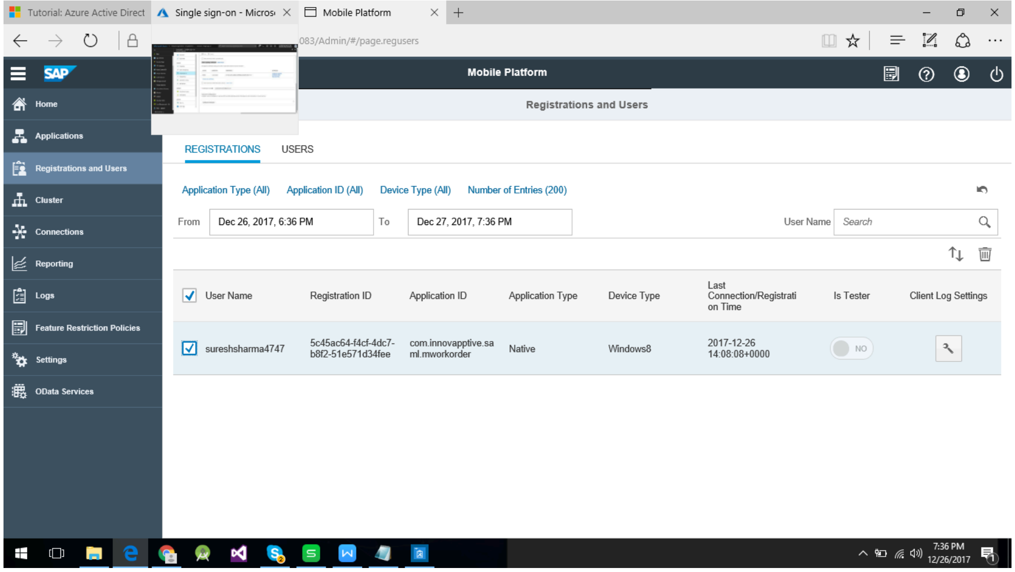
To test the application registration using Azure AD user:

1. Open the application and enter **Host**, **Port**, and **Resource App Id**.
2. Click **SAVE SETTINGS.**
3. On the **Login** screen, Enter **User Name** and **Password**.
4. Click **Login**.

   The **AZURE AD** page for login appears.
5. Enter **Username** and **Password** on **AZURE AD** login page.
6. Click **Sign In** to register the application with SMP.

   You can see the successful registration of Application with AZURE AD user.

Figure 3-42 Application registration with AZURE AD



From Dec 26, 2017, 6:36 PM To Dec 27, 2017, 7:36 PM

User Name Search

☑	User Name	Registration ID	Application ID	Application Type	Device Type	Last Connection/Registration Time	Is Tester	Client Log Settings
☑	sureshsharma4747	5c45ac64-f4cf-4dc7-b8f2-51e571d34fee	com.innovapptive.saml.mworkorder	Native	Windows8	2017-12-26 14:08:08+0000	NO	

3.8.8. Troubleshooting

If the application does not navigate to ADFS page, refer to the URL and enable **Under the Intranet** section, uncheck the **Windows Authentication** option, and select **Form Authentication**.

URL:

https://blogs.msdn.microsoft.com/josrod/2014/10/15/enabled-forms-based-authentication-in-adfs-3-0/

3.9. Configure Push Notifications for SMP

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 chapter helps you configure Push Notification for either SAP Mobile Platform (SMP) 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 115)*
- Create Push User in SMP Server *(on page 116)*
- Add Push User to the Application *(on page 117)*
- Create RFC for Push Notification *(on page 118)*
- Configure Push Notification in SMP Server *(on page 120)*

3.9.1. 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**
    - For SMP Server APNS, open Google Push Notification and Windows Push Notification Ports for communication.

Device	Communication	Port
iOS	gateway.push.apple.com	2195
iOS	feedback.push.apple.com	2196
Android	andoird.goolge.com	5228, 5229, 5230
Windows	TCP Port	443

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

- SAP Mobile Platform (SMP) 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.

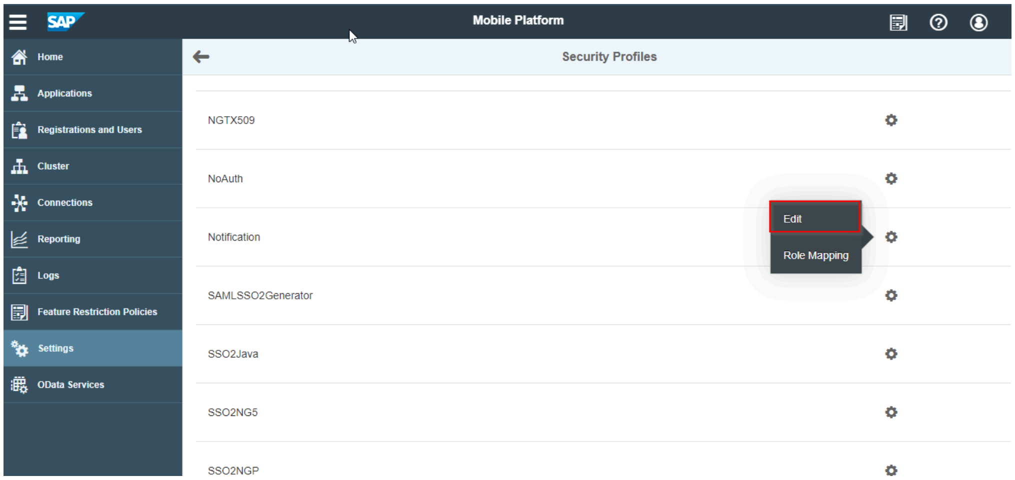
3.9.2. Create Push User in SMP Server

Create an ID to communicate between SMP Server and GW system.

To create a User ID to authenticate for the Push Notification:

1. Log in to **SMP Admin URL**
2. Navigate to **Settings** and select **Security Profiles**.
3. In the **Security Profiles** screen, click the settings icon next to **Notification**.
4. Click **Edit**.

Figure 3-43 Edit option for creating push user



5. Click the Create icon in the Authentication Providers screen.
6. In the Add Authentication Provider screen:

    a. Select System Login (Admin Only) for Authentication Provider field.

    b. In the General section:
    - Select **Control Flag** as optional.
    - Enter *Push User* in the **Provider Description** field.
    - Enter both **Username** and **Password** as *smppushuser*.
    - Enter **Notification User** in the Roles field.
7. Click **Save**.

    Push User is created.

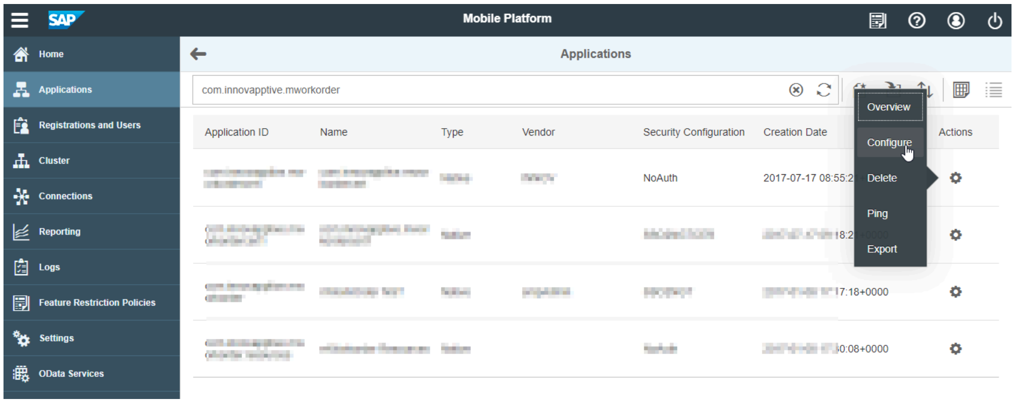
3.9.2.1. Add Push User to the Application

Add the user that you have created to the application where you want to enable push notifications.

To add push user to the application:

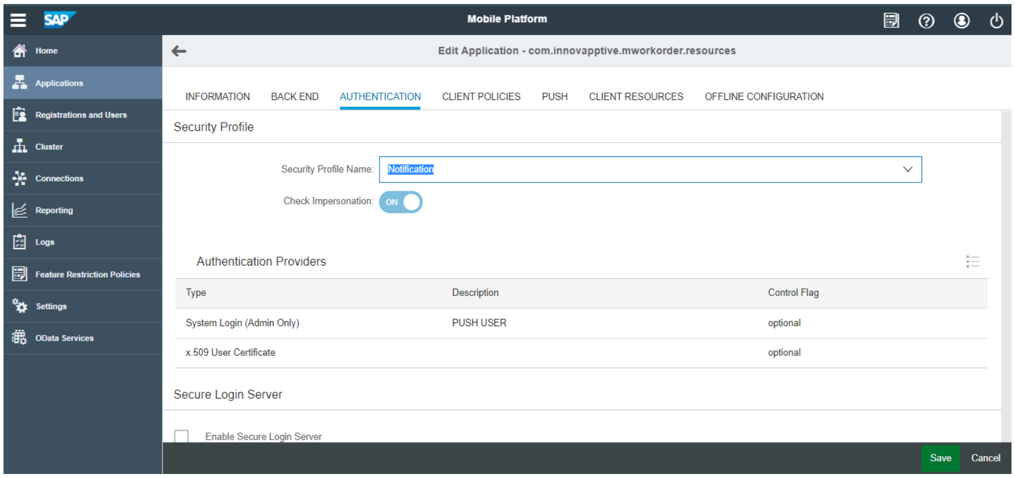
1. Click **Application** on the left navigation.
2. Click the **Setting** icon next to the application.
3. Click **Configure**.

Figure 3-44 Add push user to application



4. Click the Authentication tab.
5. Select **Notification** form the options for the **Security Profile Name** field.

Figure 3-45 Add push user to application



Security Profile Name: Notification

Check Impersonation: ON

Type	Description	Control Flag
System Login (Admin Only)	PUSH USER	optional
x.509 User Certificate		optional

□ Enable Secure Login Server

6. Click **Save**.

   System Login (Admin Only) profile is added.

3.9.2.2. Create RFC for Push Notification

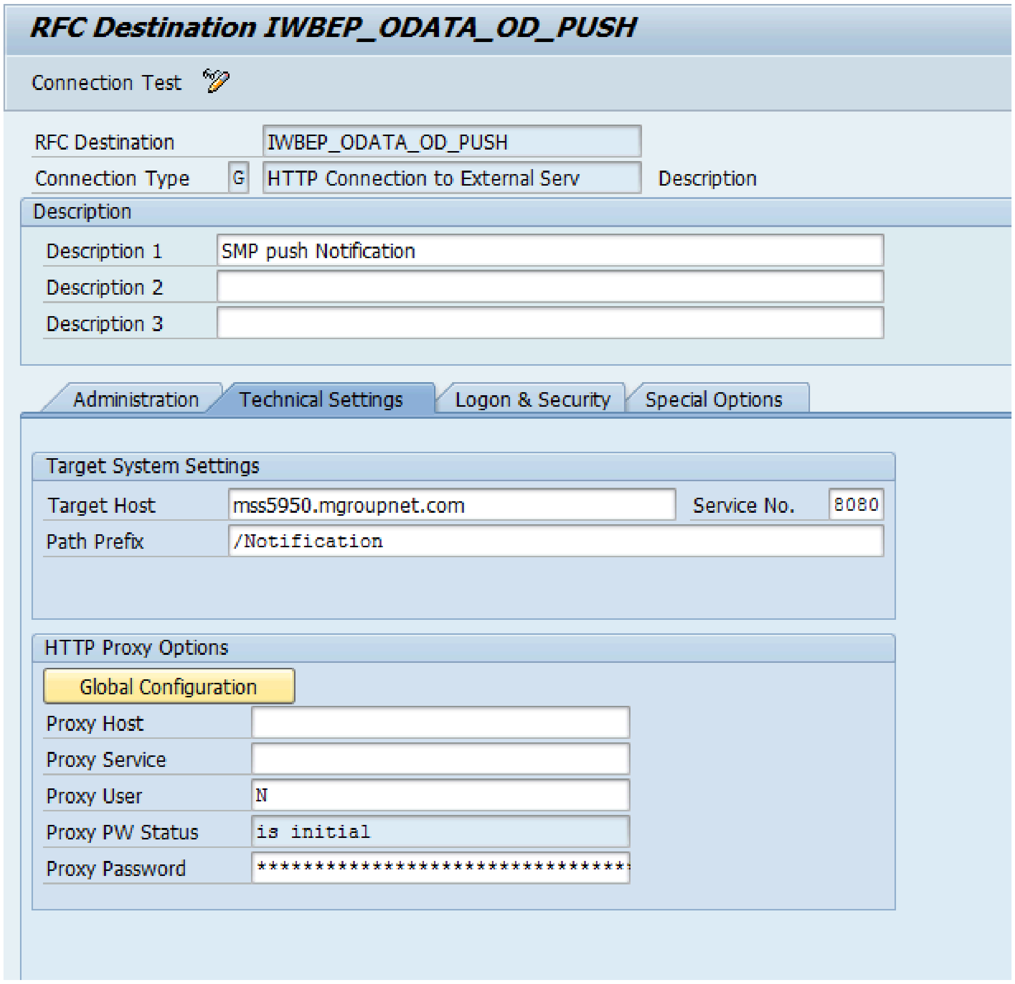
To establish RFC communication between Gateway Server and SMP Mobile Services:

1. Go to **SM59**.
2. Enter **RFC Destination**: *IWBEP_ODATA_OD_PUSH*.
3. Enter **Description**: *Notification to SMP Server*.
4. Enter the following information:
    - **Target Host**: SMP Hostname.
    - **Port**: HTTP Port (8080).

Note:

- Check your port number in **T-Code SMICM**, **Services**.
- For SCP configurations, GW system should be allowed to communicate to SCP via HTTP/HTTPs Port for Push Notification.

Figure 3-46 Create RFC



RFC Destination IWBEP_ODATA_OD_PUSH

Connection Test

RFC Destination: IWBEP_ODATA_OD_PUSH
Connection Type: G HTTP Connection to External Serv
Description

Description
Description 1: SMP push Notification
Description 2:
Description 3:

Target System Settings
Target Host: mss5950.mgroupnet.com
Service No.: 8080
Path Prefix: /Notification

HTTP Proxy Options

Proxy Host:
Proxy Service:
Proxy User: N
Proxy PW Status: is initial
Proxy Password: ********************************

5. In **Logon & Security** tab, choose **Basic Authentication**.
6. Enter **User: smppushuser; Password: smppushuser**.
7. Save your settings

> **Note:**
> Ignore the above procedure if done already while doing Gateway Configuration.

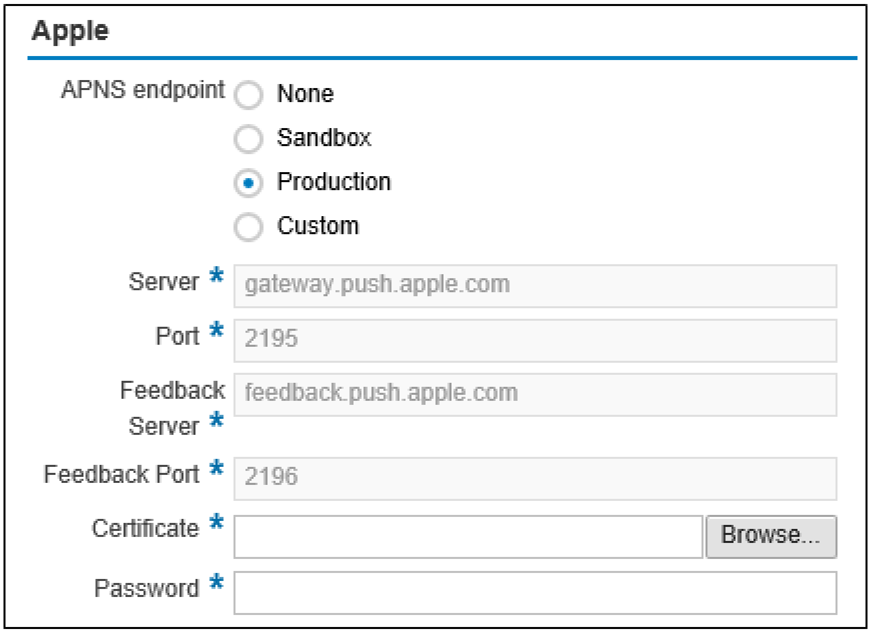
3.9.2.3. Configure Push Notification in SMP Server

To configure push notification in SMP server:

1. Log in to SMP Server Admin Portal.
   For example, https://smp.hostname.com:8083/Admin.
2. Open the Application for which you need to configure Push Notification.
   For example, **com.innovapptive.massettag**.
3. Navigate to **Push** tab and the enter the following details as shown in the following image.

- iOS Devices: Import Innovapptive Push Certificate.

Figure 3-47 Configure Push Notificationf for iOS



Apple

APNS endpoint ○ None
○ Sandbox
● Production
○ Custom

Server * gateway.push.apple.com

Port * 2195

Feedback Server * feedback.push.apple.com

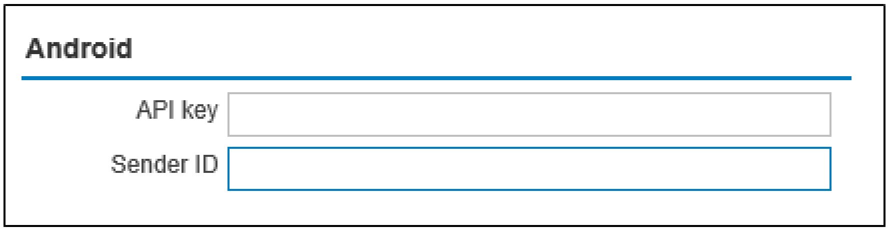
Feedback Port * 2196

Certificate *

Password *

- Android

Figure 3-48 Configure Push Notificationf for Android



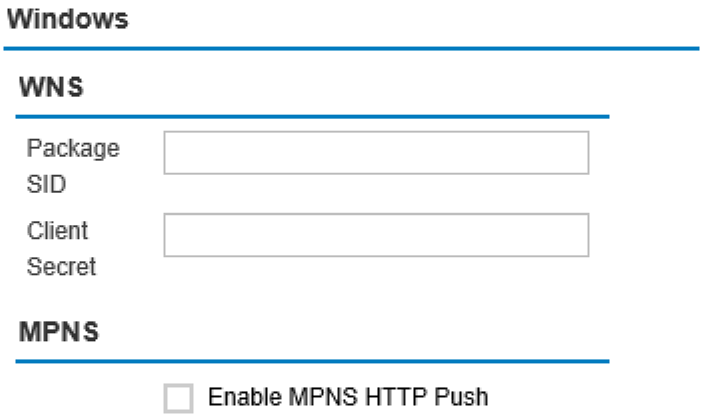
Android

API key

Sender ID

- Windows

Figure 3-49 Configure Push Notificationf for MS Windows



Windows

WNS

Package SID

Client Secret

MPNS

□ Enable MPNS HTTP Push

4. Save the configurations.

> **Note:**
> If you are on SAP Mobile Platform 3.0 SP12/SP13 or below. Google notification service GCM has recently changed its server-side certificates. Import the certificates in SMP Shared KeyStore Entries as X.509 Certificates and restart all the server nodes. Contact Innovapptive for Certificates.

3.10. Manage Resource File in SMP

Resource File in SMP 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, such as SMP Server, Port, Security profile, and Connection details in the resources text file and administer centrally by the SMP 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 SMP admin user.

When this resource file is updated, the application connects to the mobile platform (SMP) 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 Mobile Platform (SMP):

- Prepare and update the resource file (All platforms—iOS, Android, and Windows).
- Configure resource file for On Premise SMP.

The following topics help you with resource file management:

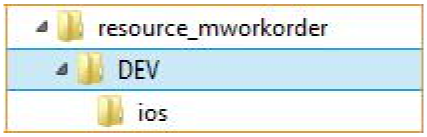
- Prepare and Update Resource File for SMP *(on page 124)*
- Use Resource File in SCP *(on page 56)*
- Use Resource File in SMP *(on page 135)*

3.10.1. Prepare and Update Resource File for SMP

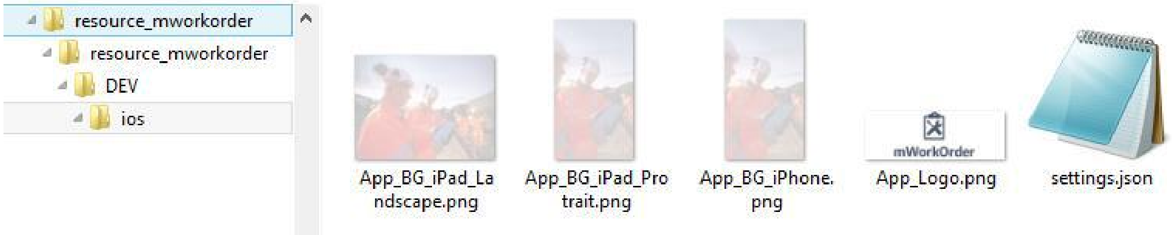
The **mWorkOrder** application resource file **resources_mworkorder.zip** on Windows platform is used as an example to demonstrate the procedure. Do your branding changes in the zip file that is provided by Innovapptive initial deployment.

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. • **Conditions:** Use uppercase alphabets. • **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. • **Conditions:** None • **Possible Values:** Development/Quality/Production.

Property	Description
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. • **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 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
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. • **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 "OfflineStatusColor":"#DF264D" in the json file.
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.

Property	Description
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.

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.
	Syntax:
	`{"id":<SequenceNumber>,"key":"<SAPLanguageCode>","value":`
	`"<LanguageName>"}`
	• **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.

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. • **Possible Values:** As required. For example, D30.

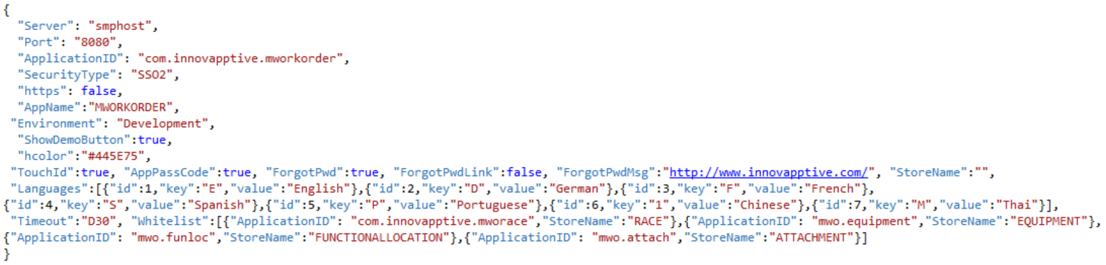
5. For each environment (Development, Quality, and Production), review and update the content block in entirety.

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 SMP servers, which will be used for mobile application connection. For example: smp.innovapptive.com
Port	• The application establishes the communication to the server based on the port number. • **Possible Values:** 8080, 8081. For example, HTTP/HTTPs (SMP default HTTP port 8080, HTTPs 8081, and custom ports for proxy)
Application-ID	• ID configured in SMP and the mobile application will use it to connect to server for the registration. • **Condition:** Use the same application ID as defined in SMP. • **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 SMP 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 SMP. 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 [Application-ID]	All Innovapptive applications require connection settings for RACE services and may also require other connection settings.

Parameter	Description
	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. 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. 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

3.10.2. Prepare and Update Resource File for SMP (MWO 2009 SP03 and above releases)

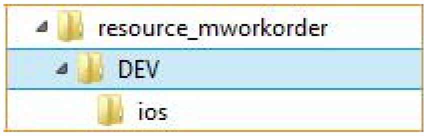
The **mWorkOrder** application resource file **resources_mworkorder.zip** on Windows platform is used as an example to demonstrate the procedure. Do your branding changes in the zip file that is provided by Innovapptive initial deployment.

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

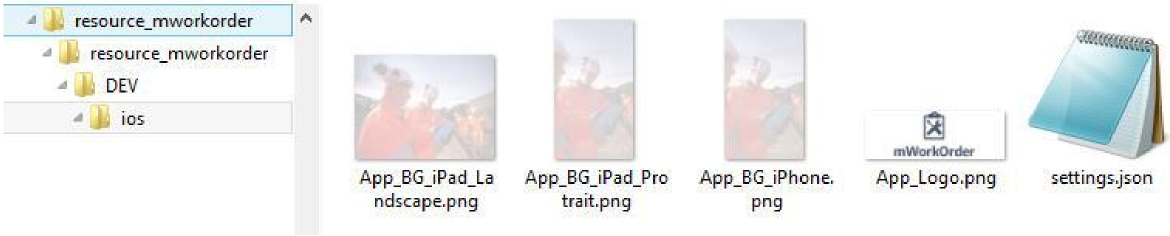
To prepare and update the resource file:

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.

   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. • **Conditions:** Use uppercase alphabets. • **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. • **Conditions:** None • **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. **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
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. • **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 "OfflineStatusColor":"#DF264D" in the json file.

Property	Description
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.
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. • **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. • **Conditions:** None • **Possible Values:** WORKORDER

Property	Description
StoreDescription	Helps you to identify the description regarding the store name. • **Conditions:** None • **Possible Values:** General
StoreIndex	Helps you to identify the index value of the store name and the order is in ascending order. • **Conditions:** None • **Possible Values:**1 or 2
StoreType	Helps you to identify the type of the store. • **Conditions:** None • **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.
	Syntax:
	`{"id":<SequenceNumber>,"key":"<SAPLanguageCode>","value":`
	`"<LanguageName>"}`
	• **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.

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. • **Possible Values:** As required. For example, D30.

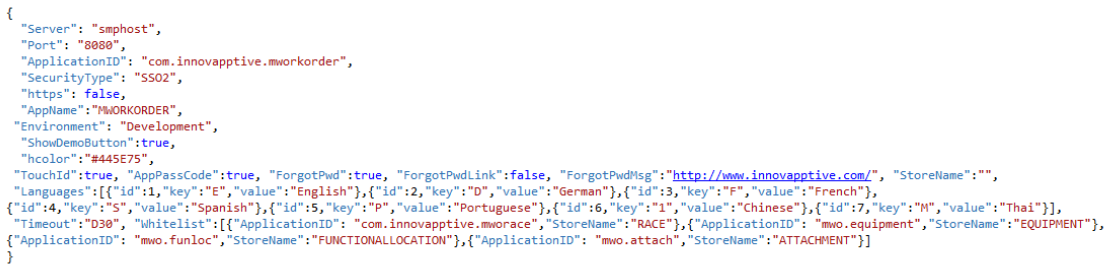
5. For each environment (Development, Quality, and Production), review and update the content block in entirety.

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 SMP servers, which will be used for mobile application connection. For example: smp.innovapptive.com
Port	• The application establishes the communication to the server based on the port number. • **Possible Values:** 8080, 8081. For example, HTTP/HTTPs (SMP default HTTP port 8080, HTTPs 8081, and custom ports for proxy)
Application-ID	• ID configured in SMP and the mobile application will use it to connect to server for the registration. • **Condition:** Use the same application ID as defined in SMP. • **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 SMP 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 SMP. 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 [Application-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.

Parameter	Description
Whitelist [StoreName]	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": "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

3.10.3. Use Resource File in SMP

The following topics help you with uploading resource file in SMP:

- Add back-end connection RACE URL and upload application help resource *(on page 135)*
- Add backend connection for Dolphin Services Integration (mWorklist only) *(on page 137)*
- Create Application and Upload Resource File *(on page 138)*

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

Add back-end connection RACE URL for the application. mWorkOrder application is used as example here.

Ensure that application is configured using the security guidelines detailed in the pre-installation guide.

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

1. Log in to **SMP Admin Cockpit** using the following **URL**: https://smphostname:port/Admin/
2. Click the **Application** tab.
3. Click the **App ID**. For example, **com.innovapptive.mworkorder**.
4. Click the **BACK END** tab and scroll to the bottom of the page.
5. In the **Back-end Connections** section, click **New**.
6. Enter the following details, as shown below:

- **Connection Name**: com.innovapptive.mworace

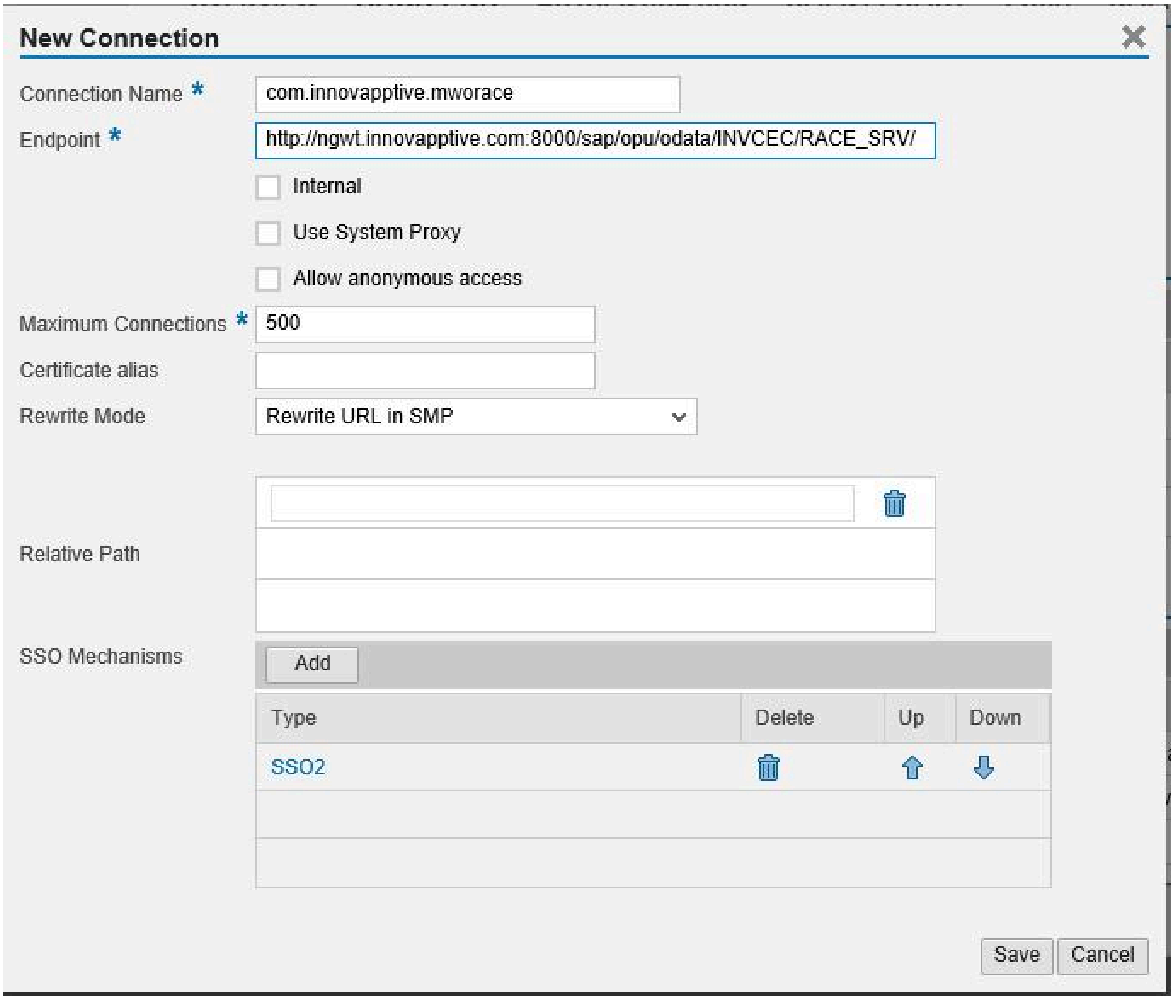
> **Note:**
> Connection name should be the same as used in the **settings.json** file.

- **Back-End URL:** http://GATEWAY: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.
    - Connection Name is **mwo.funloc** and back-end URL is http://GATEWAY:HTTP(s)/sap/opu/odata/INVMWO/MWOFUNLOCATION_SRV/
    - Connection Name is **mwo.equipment** and back-end URL is http://GATEWAY:HTTP(s)/sap/opu/odata/INVMWO/MWOEQUIPMENT_SRV/
    - Connection Name is **mwo.attach** and back-end URL is http://GATEWAY:HTTP(s)/sap/opu/odata/INVMWO/WOATTACHMENTS_SRV/

7. In SSO mechanisms, click **Add** and select **SSO2**.



New Connection

Connection Name *: com.innovapptive.mworace

Endpoint *: http://ngwt.innovapptive.com:8000/sap/opu/odata/INVCEC/RACE_SRV/

□ Internal

□ Use System Proxy

□ Allow anonymous access

Maximum Connections *: 500

Certificate alias:

Rewrite Mode: Rewrite URL in SMP

Relative Path:

SSO Mechanisms:

Type	Delete	Up	Down
SSO2	🗑	⇧	⇩

8. Save and test the app ID by a ping test.
9. 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.

3.10.3.2. Add backend connection for Dolphin Services Integration (mWorklist only)

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

To add backend connection for Dolphin Services Integration:

1. Log in to the SMP Admin Cockpit using the following URL: https://smphostname:port/Admin/
2. Click the **Application** tab.
3. Click the **App ID**, which reads as com.innovapptive.mworklist.
4. Click the **BACK END** tab and scroll to the bottom of the page.
5. In the Back-end Connections section, click **New**.
6. Enter the following details
   - **Connection Name**: com.innovapptive.dolphin.pts

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

   - **Endpoint:** http://GATEWAY:HTTP(s)/sap/opu/odata/DOL/AP_GW_SRV/
   - In SSO mechanisms, click **Add** and select **SSO2**
7. Click **Save**.

3.10.3.3. Create Application and Upload Resource File

Upload the resource file that you created at Prepare and Update Resource File for SMP *(on page 124)*.

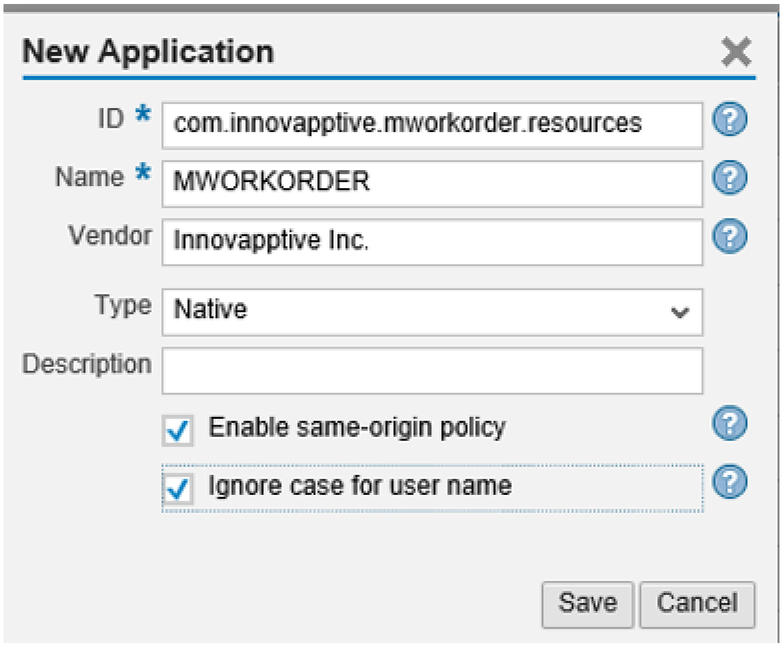
To create application and upload resource file:

1. Log in to the SMP server Admin URL: https://smphostname:port/Admin/
2. Click **Applications**.
3. Click **New** and enter the following details:

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.
Type	Native
Description	(Optional as required)

Select	Enable same-origin policy
Select	Ignore case for user name

Figure 3-50 New Application Creation (mWorkOrder example)



New Application

ID * com.innovapptive.mworkorder.resources

Name * MWORKORDER

Vendor Innovapptive Inc.

Type Native

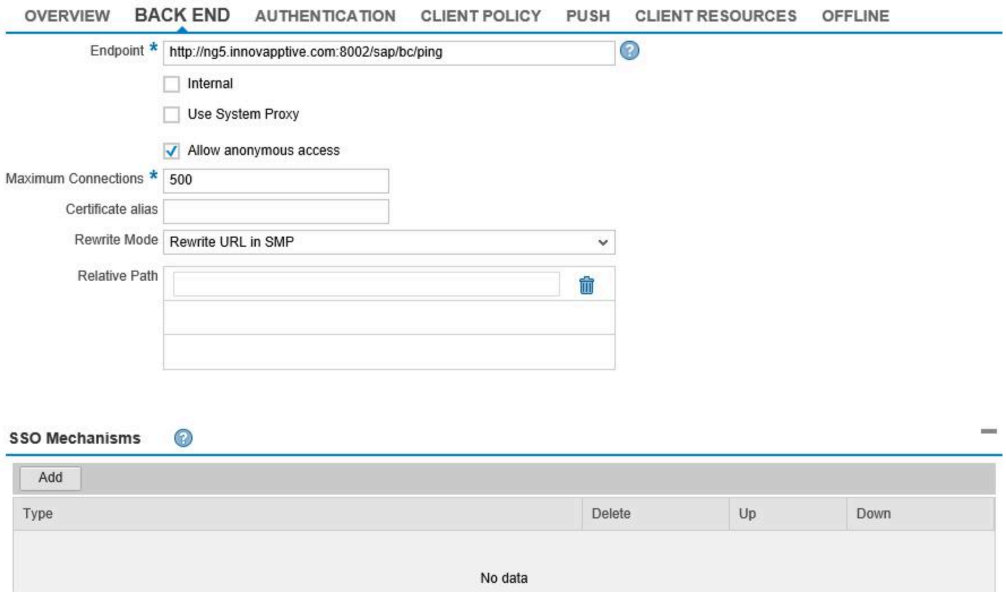
Description

☑ Enable same-origin policy

☑ Ignore case for user name

4. Click **Save**.
5. In the Applications Configurations page, click the **BACK END** tab.
    - Type the endpoint URL **http://gwserver.com:HTTP(s)Port/sap/bc/ping** in the **Endpoint** field.
    - Select the **Allow anonymous access** checkbox.

Figure 3-51 New Application Creation (mWorkOrder example)



Endpoint * http://ng5.innovapptive.com:8002/sap/bc/ping

□ Internal

□ Use System Proxy

☑ Allow anonymous access

Maximum Connections * 500

Certificate alias

Rewrite Mode Rewrite URL in SMP

Relative Path

Type	Delete	Up	Down
No data			

6. Click the **Authentication** tab.
    a. Enter **NOAUTH** in the Profile Name field.
    b. Click **Add**.
    c. From the Authentication Providers drop-down box, select **No Authentication Challenge**.
    d. Click **Save** to view the configurations and click **Save** again.
7. Click **Client Resources** tab.
    a. Enter the **Bundle Name** and **Version** as **resources_ios** and **1.0** respectively.
    b. Browse and upload the resource file.
8. Click **Save**.
9. Ping and test the service.

4. 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 141)*
- SAP Authorizations for mWorkOrder users *(on page 141)*
- SAP Authorizations for mInventory users *(on page 147)*
- SAP Authorizations for mAssetTag users *(on page 151)*
- User roles for RACE *(on page 162)*

4.1. 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.

4.2. 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 4-1 Roles for ECC System

Role Name	Description	Transactions	Authorization Objects
ZINV_MWO_ECC_END_USER_R2009	mWorkOrder - End User - ECC Authorizations - Release 2009	IW31, IW32, IW33, IW34, IW41, IW21, IW23, IL01, IL02, IL03, IE01, IE02, IE03, IK01, IK02, IK03, IK11, IK13, IQS1, IQS2, IQS3, QA03, QA11, QA32, QE03, QE11, CV03N, CS03, IP01, IP02, IP03, IW45, CS02, IP10	S_RFC, S_RFCACL
ZINV_MWO_ECC_RACE_ADM_R2009	mWorkOrder - RACE Admin - ECC Authorizations – Release 2009		S_RFC and S_RFCACL

Table 4-2 Roles for NetWeaver Gateway System

Role Name	Description	Authorizations
ZINV_MWO_NWG_END_USER_R2009	mWorkOrder - End User - Gateway Authorizations - Release 2009	S_RFC, S_RFCACL, S_SERVICE, S_TABU_DIS, S_USER_GRP
ZINV_MWO_NWG_RACE_ADM_R2009	mWorkOrder - RACE Admin - Gateway Authorizations – Release 2009	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.

4.2.1. Update Service authorization object for mWorkOrder

S_SERVICE authorization object with customer system generated service value.

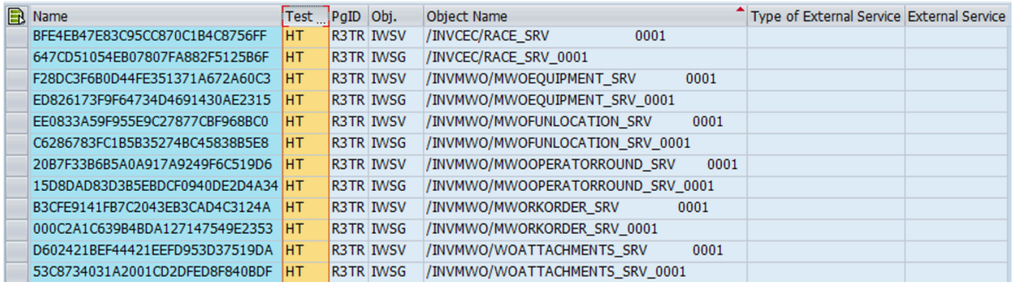
To update service values under S_SERVCE:

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

Table 4-3 S_SERVICE values

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

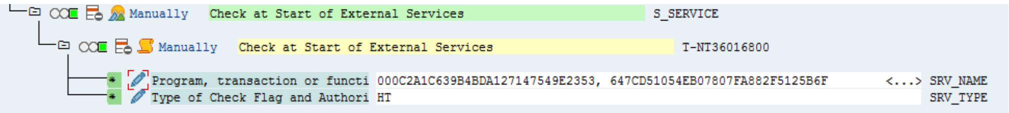
Figure 4-1 USOBHASH table



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		

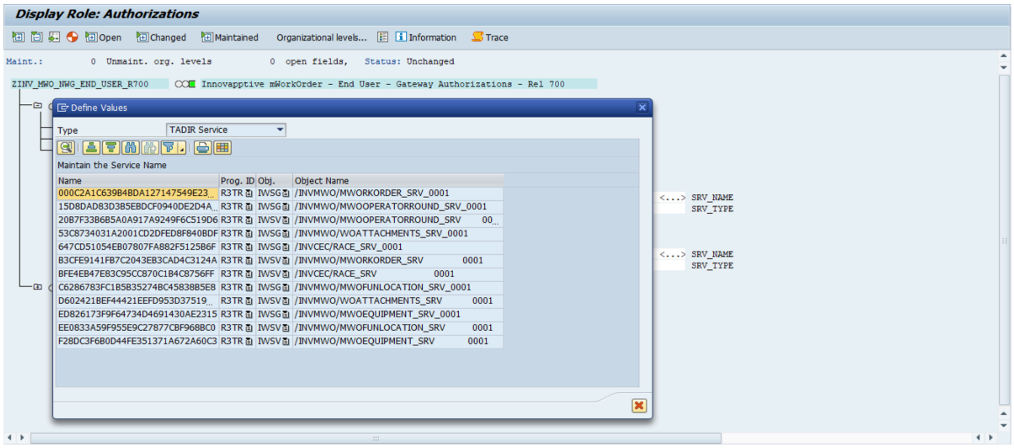
3. Pick the names of the hashed services (the 30-character length alpha numerical name) and use them under S_SERVICE - SRV_NAME.

Figure 4-2 Hashed Service Name



```
Manually  Check at Start of External Services  S_SERVICE
  Manually  Check at Start of External Services  T-NT36016800
    Program, transaction or functi 000C2A1C639B4BDA127147549E2353, 647CD51054EB07807FA882F5125B6F   <...> SRV_NAME
    Type of Check Flag and Authori HT                                                                  SRV_TYPE
```

Figure 4-3 Display Role Authorization



Display Role: Authorizations

```
Maint.:        0  Unmaint. org. levels        0  open fields,   Status: Unchanged

ZINV_MWO_NWG_END_USER_R700   Innovapptive mWorkOrder - End User - Gateway Authorizations - Rel 700
```

Define Values

Type: TADIR Service

Maintain the Service Name

Name	Prog. ID	Obj.	Object Name
000C2A1C639B4BDA127147549E23...	R3TR	IWSG	/INVMWO/MWORKORDER_SRV_0001
15D8DAD83D3B5EBDCF0940DE2D4A...	R3TR	IWSG	/INVMWO/MWOOPERATORROUND_SRV_0001
20B7F33B6B5A0A917A9249F6C519D6	R3TR	IWSV	/INVMWO/MWOOPERATORROUND_SRV 00...
53C8734031A2001CD2DFED8F840BDF	R3TR	IWSG	/INVMWO/WOATTACHMENTS_SRV_0001
647CD51054EB07807FA882F5125B6F	R3TR	IWSG	/INVCEC/RACE_SRV_0001
B3CFE9141FB7C2043EB3CAD4C3124A	R3TR	IWSV	/INVMWO/MWORKORDER_SRV 0001
BFE4EB47E83C95CC870C1B4C8756FF	R3TR	IWSV	/INVCEC/RACE_SRV 0001
C6286783FC1B5B35274BC45838B5E8	R3TR	IWSG	/INVMWO/MWOFUNLOCATION_SRV_0001
D602421BEF44421EEFD953D37519...	R3TR	IWSV	/INVMWO/WOATTACHMENTS_SRV 0001
ED826173F9F64734D4691430AE2315	R3TR	IWSG	/INVMWO/MWOEQUIPMENT_SRV_0001
EE0833A59F955E9C27877CBF968BC0	R3TR	IWSV	/INVMWO/MWOFUNLOCATION_SRV 0001
F28DC3F6B0D44FE351371A672A60C3	R3TR	IWSV	/INVMWO/MWOEQUIPMENT_SRV 0001

4.2.2. 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 145)* to understand how to import transports.

Table 4-4 SAP ECC Transports

Transport	Description	Dependency
ERDK909323	INNOV:ECC: R 2009 mWork-Order Application End User Roles	None

Table 4-5 SAP GW Transports

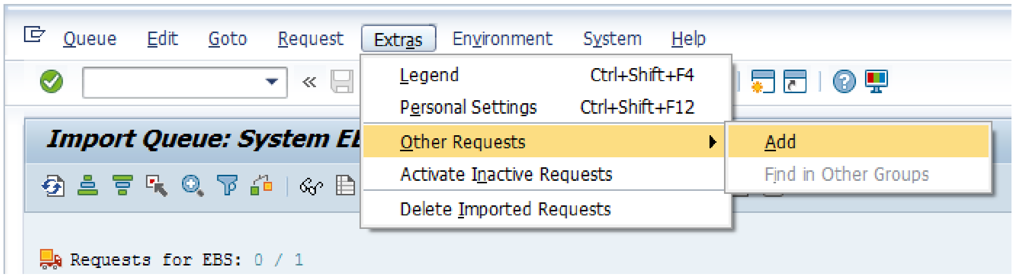
Transport	Description	Dependency
NGTK907881	INNOV:GW: R 2009 mWork-Order Application End User Roles	None

4.2.3. 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**.

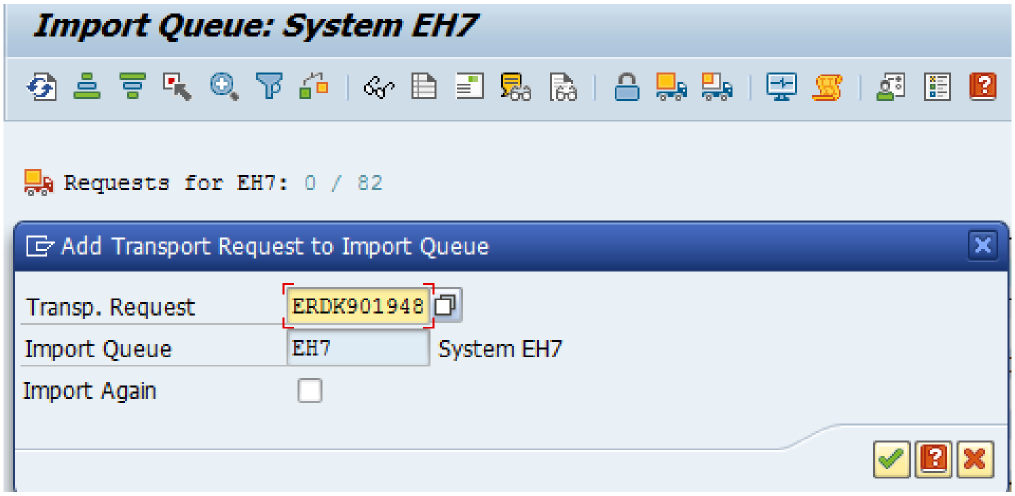
Figure 4-4 Import Queue



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 4-5 Add Transport Request to Import Queue



Import Queue: System EH7

Requests for EH7: 0 / 82

Add Transport Request to Import Queue

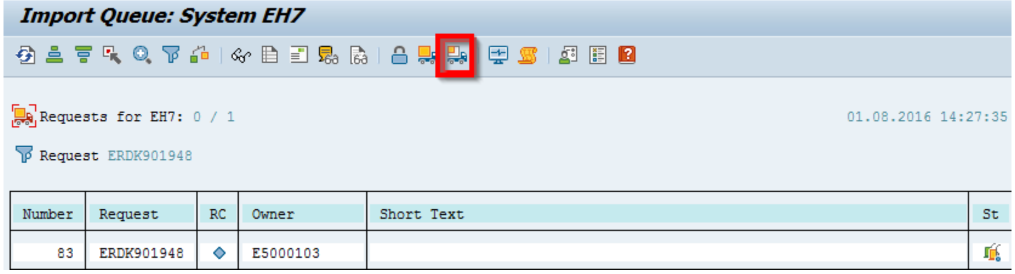
Transp. Request: ERDK901948

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 4-6 Truck icon



Import Queue: System EH7

Requests for EH7: 0 / 1 01.08.2016 14:27:35

Request ERDK901948

Number	Request	RC	Owner	Short Text	St
83	ERDK901948	◆	E5000103		

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.

4.3. 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 4-6 Roles for ECC System

Role Name	Description	Transactions	Authorization Objects
ZINV_MIM_ECC_END_USER_R2009	mInventory - End User - ECC Authorizations - Release 2009	MMBE, LX02, MIGO, MB1C, MB1A, HUMO, LT12, VL06O, VL02N, LT03, VL06I, HUIMV03, HUINV05, MI04, MI07, LI11N, LI20, LT10 & MB1B, ML81N, MI09	S_RFC, S_RFCACL
ZINV_MIM_ECC_RACE_ADM_R2009	mInventory - RACE Admin - ECC Authorizations – Release 2009		S_RFC, S_RFCACL

Table 4-7 Roles for NetWeaver Gateway System

Role Name	Description	Authorizations
ZINV_MIM_NWG_END_USER_R2009	mInventory - End User - Gateway Authorizations - Release 2009	S_RFC, S_RFCACL, S_SERVICE, S_USER_GRP & S_TABU_DIS
ZINV_MIM_NWG_RACE_ADM_R2009	mInventory - RACE Admin - Gateway Authorizations – Release 2009	S_RFC, S_RFCACL, S_SERVICE, S_TABU_DIS, S_USER_GRP, /INVCEC/RA

Table 4-8 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 4-9 Roles for EWM Authorizations

Role Name	Description	Transactions	Authorizations
ZINV_MIM_EWM_-END_USER_R2009	mInventory - End User - EWM Authorizations - Release 2009	/SCWM/MAT1 /SCWM/TODLV_I /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 /SCWM/PACK /SCWM/LOAD /SCWM/UNLOAD	S_RFC, S_RFCACL

Table 4-9 Roles for EWM Authorizations (continued)

Role Name	Description	Transactions	Authorizations
		/SCWM/ADHU /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.

4.3.1. 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 4-10 S_SERVICE values

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

Figure 4-7 USOBHASH table

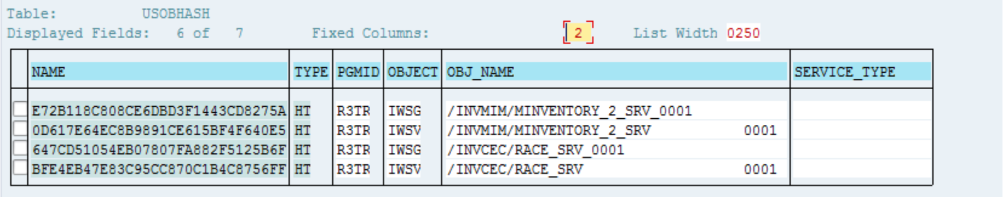
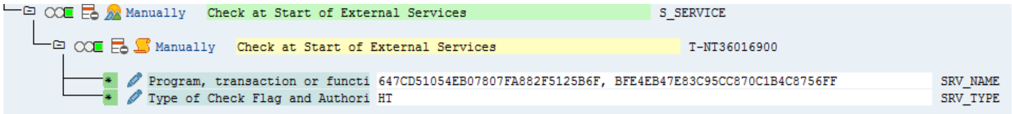


Table: USOBHASH
Displayed Fields: 6 of 7 Fixed Columns: 2 List Width 0250

NAME	TYPE	PGMID	OBJECT	OBJ_NAME	SERVICE_TYPE
E72B118C808CE6DBD3F1443CD8275A	HT	R3TR	IWSG	/INVMIM/MINVENTORY_2_SRV_0001	
0D617E64EC8B9891CE615BF4F640E5	HT	R3TR	IWSV	/INVMIM/MINVENTORY_2_SRV 0001	
647CD51054EB07807FA882F5125B6F	HT	R3TR	IWSG	/INVCEC/RACE_SRV_0001	
BFE4EB47E83C95CC870C1B4C8756FF	HT	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 4-8 Hashed Service Name



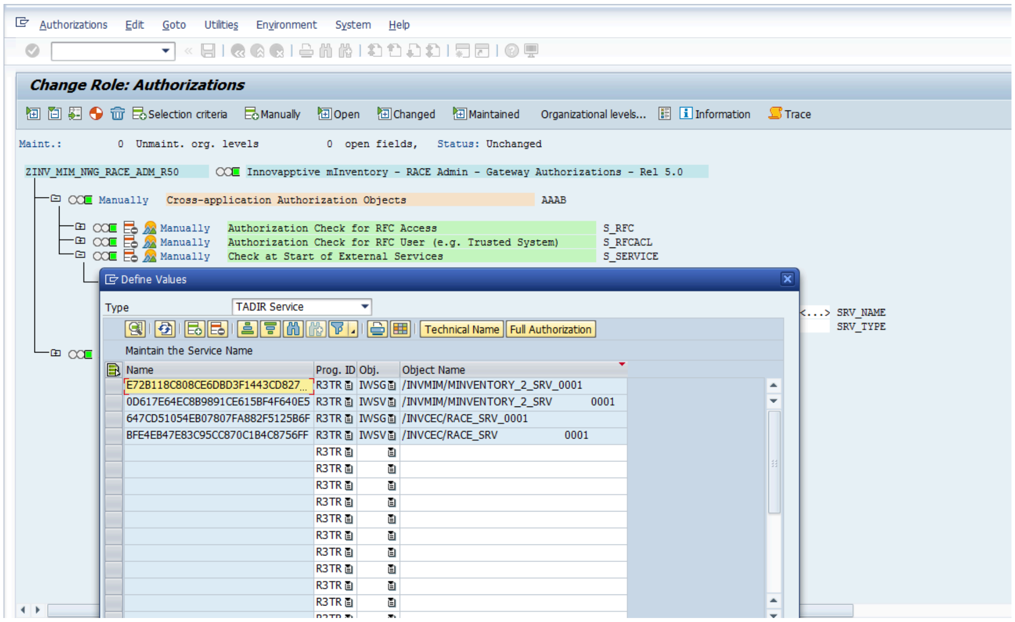
Manually Check at Start of External Services S_SERVICE

Manually Check at Start of External Services T-NT36016900

Program, transaction or functi 647CD51054EB07807FA882F5125B6F, BFE4EB47E83C95CC870C1B4C8756FF SRV_NAME

Type of Check Flag and Authori HT SRV_TYPE

Figure 4-9 Change Role Authorization



Change Role: Authorizations

Maint.: 0 Unmaint. org. levels 0 open fields, Status: Unchanged

ZINV_MIM_NWG_RACE_ADM_R50 Innovapptive mInventory - RACE Admin - Gateway Authorizations - Rel 5.0

Manually Cross-application Authorization Objects AAAB

Manually Authorization Check for RFC Access S_RFC

Manually Authorization Check for RFC User (e.g. Trusted System) S_RFCACL

Manually Check at Start of External Services S_SERVICE

<...> SRV_NAME

SRV_TYPE

Define Values

Type: TADIR Service

Maintain the Service Name

Name	Prog. ID	Obj.	Object Name
E72B118C808CE6DBD3F1443CD827...	R3TR	IWSG	/INVMIM/MINVENTORY_2_SRV_0001
0D617E64EC8B9891CE615BF4F640E5	R3TR	IWSV	/INVMIM/MINVENTORY_2_SRV 0001
647CD51054EB07807FA882F5125B6F	R3TR	IWSG	/INVCEC/RACE_SRV_0001
BFE4EB47E83C95CC870C1B4C8756FF	R3TR	IWSV	/INVCEC/RACE_SRV 0001
	R3TR		
	R3TR		
	R3TR		
	R3TR		
	R3TR		
	R3TR		
	R3TR		
	R3TR		
	R3TR		
	R3TR		

4.3.2. 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 145)* to understand how to import transports.

Table 4-11 SAP ECC Transports

Transport	Description	Dependency
ERDK909327	INNOV:ECC: R 2009 mInventory Application End User Roles	None

Table 4-12 SAP GW Transports

Transport	Description	Dependency
NGTK907883	INNOV:GW: R 2009 mInventory Application End User Roles	None

Table 4-13 SAP RLM Transports

Transport	Description	Dependency
EC7K900028	INNOV:RLM: R 2009 mInventory Application End User Roles	None

Table 4-14 SAP EWM Transports

Transport	Description	Dependency
H18K900161	INNOV:EWM: R 2009 mInventory Application End User Roles	None

4.4. 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 4-15 SAP Transaction Codes for mAssetTag

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

Table 4-16 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*
	S_RFCACL	• ACTVT = 16 • RFC_EQUSER = Y

Table 4-17 mAssetTag NetWeaver Gateway Authorizations

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

Table 4-17 mAssetTag NetWeaver Gateway Authorizations (continued)

User	Authorization Object	Authorizations
	S_TABU_DIS	• ACTVT = 03 • DICBERCLS = IW*
	S_RFCACL	• ACTVT = 16 • RFC_EQUSER = Y

4.4.1. Update Service authorization object for mAssetTag

Update the system specific S_SERVICE authorization object with customer system generated service value.

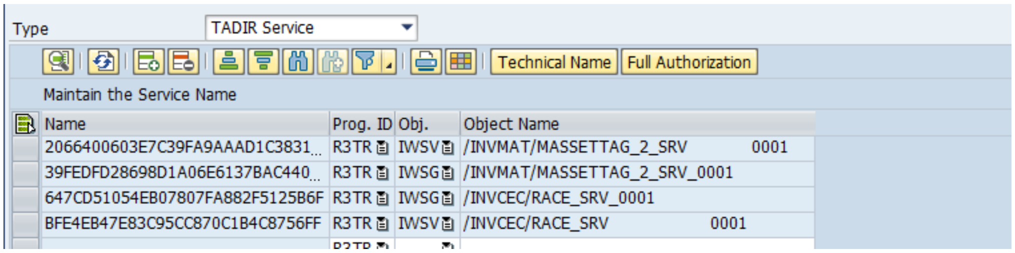
To update service values under S_SERVCE:

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

Table 4-18 S_SERVICE values

Test Status Type	**HT** (Hash Value for TADIR Object)
Object Type	**IWSG** (Gateway Service group metadata) **IWSV** (Gateway Business Suite Enablement – Service)
Object Name	/INVCEC/* and /INVMAT/*

Figure 4-10 USOBHASH table

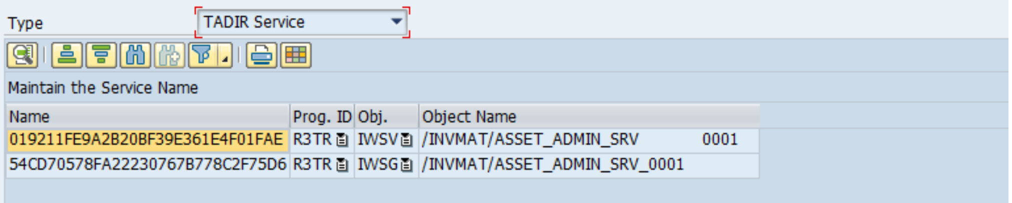


Type: TADIR Service

Maintain the Service Name

Name	Prog. ID	Obj.	Object Name
2066400603E7C39FA9AAAD1C3831...	R3TR	IWSV	/INVMAT/MASSETTAG_2_SRV 0001
39FEDFD28698D1A06E6137BAC440...	R3TR	IWSG	/INVMAT/MASSETTAG_2_SRV_0001
647CD51054EB07807FA882F5125B6F	R3TR	IWSG	/INVCEC/RACE_SRV_0001
BFE4EB47E83C95CC870C1B4C8756FF	R3TR	IWSV	/INVCEC/RACE_SRV 0001

Figure 4-11 USOBHASH table



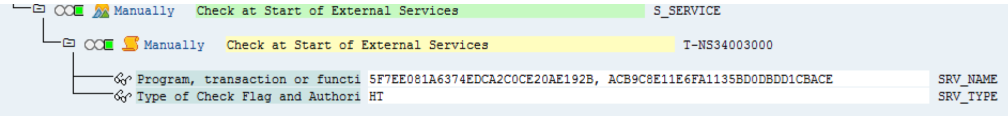
Type: TADIR Service

Maintain the Service Name

Name	Prog. ID	Obj.	Object Name	
019211FE9A2B20BF39E361E4F01FAE	R3TR	IWSV	/INVMAT/ASSET_ADMIN_SRV	0001
54CD70578FA22230767B778C2F75D6	R3TR	IWSG	/INVMAT/ASSET_ADMIN_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.

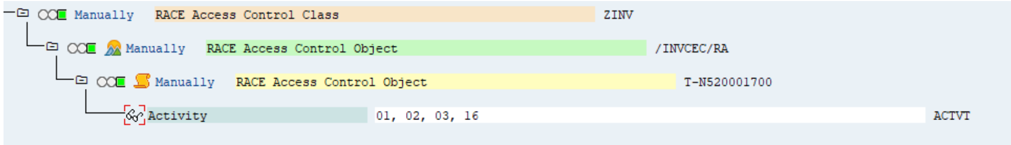
Figure 4-12 Hashed Service Name



```
Manually   Check at Start of External Services        S_SERVICE
  Manually   Check at Start of External Services        T-NS34003000
    Program, transaction or functi  5F7EE081A6374EDCA2C0CE20AE192B, ACB9C8E11E6FA1135BD0DBDD1CBACE   SRV_NAME
    Type of Check Flag and Authori  HT                                                                SRV_TYPE
```

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

Figure 4-13 Hashed Service Name



```
Manually   RACE Access Control Class        ZINV
  Manually   RACE Access Control Object        /INVCEC/RA
    Manually   RACE Access Control Object        T-N520001700
      Activity        01, 02, 03, 16        ACTVT
```

4.5. SAP Authorizations for mServiceOrder users

Application user requires access to the following transaction codes or relevant custom transaction codes and appropriate authorizations objects to use the mServiceOrder 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 4-19 Roles for ECC System

Role Name	Description	Transactions	Authorization Objects
ZINV_MSO_ECC_END_USER_R610	mServiceOrder - End User - ECC Authorizations - Release 6.1.0	CS03, CV03N, IA07, IA09, IE01, IE02, IE03, IK01, IK02, IK03, IK11, IK13, IL01, IL02, IL03, IQS1, IQS2, IQS3, IW21, IW22, IW23, IW31, IW32, IW33, IW34, IW41, IW42, IW43, IW45, IW51, IW52, IW53, MB1A, MIGO, MMBE, QA03, QA11, QA32, QE03, QE11, VA43, XD03	S_RFC, S_RFCACL
ZINV_MSO_ECC_RACE_ADM_R610	mServiceOrder - RACE Admin - ECC Authorizations - Release 6.1.0		S_RFC and S_RFCACL

Table 4-20 Roles for NetWeaver Gateway System

Role Name	Description	Authorizations
ZINV_MSO_NWG_END_USER_R610	mServiceOrder - End User - Gateway Authorizations - Release 6.1.0	S_RFC, S_RFCACL, S_SERVICE, S_TABU_DIS, S_USER_GRP
ZINV_MSO_NWG_RACE_ADM_R610	mServiceOrder - RACE Admin - Gateway Authorizations -Release 6.1.0	S_RFC, S_RFCACL, S_SERVICE, S_TABU_DIS, S_USER_GRP

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

4.5.1. Update Service authorization object for mServiceOrder

Update the system specific S_SERVICE authorization object with customer system generated service value.

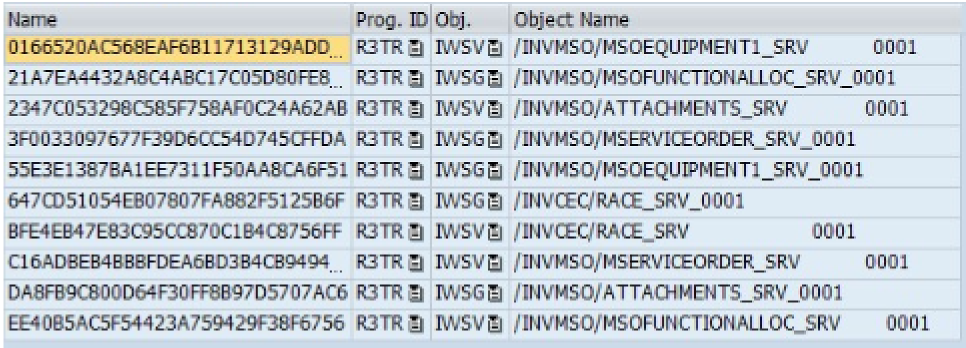
To update service values under S_SERVCE:

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

Table 4-21 S_SERVICE values

Test Status Type	**HT** (Hash Value for TADIR Object)
Object Type	**IWSG** (Gateway Service group metadata) **IWSV** (Gateway Business Suite Enablement – Service)
Object Name	/INVCEC/RACE_SRV*, /INVMSO/ *

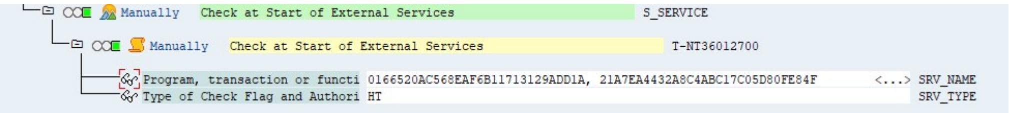
Figure 4-14 USOBHASH table



Name	Prog. ID	Obj.	Object Name
0166520AC568EAF6B11713129ADD...	R3TR	IWSV	/INVMSO/MSOEQUIPMENT1_SRV 0001
21A7EA4432A8C4ABC17C05D80FE8...	R3TR	IWSG	/INVMSO/MSOFUNCTIONALLOC_SRV_0001
2347C053298C585F758AF0C24A62AB	R3TR	IWSV	/INVMSO/ATTACHMENTS_SRV 0001
3F0033097677F39D6CC54D745CFFDA	R3TR	IWSG	/INVMSO/MSERVICEORDER_SRV_0001
55E3E1387BA1EE7311F50AA8CA6F51	R3TR	IWSG	/INVMSO/MSOEQUIPMENT1_SRV_0001
647CD51054EB07807FA882F5125B6F	R3TR	IWSG	/INVCEC/RACE_SRV_0001
BFE4EB47E83C95CC870C1B4C8756FF	R3TR	IWSV	/INVCEC/RACE_SRV 0001
C16ADBEB4BBBFDEA6BD3B4CB9494...	R3TR	IWSV	/INVMSO/MSERVICEORDER_SRV 0001
DA8FB9C800D64F30FF8B97D5707AC6	R3TR	IWSG	/INVMSO/ATTACHMENTS_SRV_0001
EE40B5AC5F54423A759429F38F6756	R3TR	IWSV	/INVMSO/MSOFUNCTIONALLOC_SRV 0001

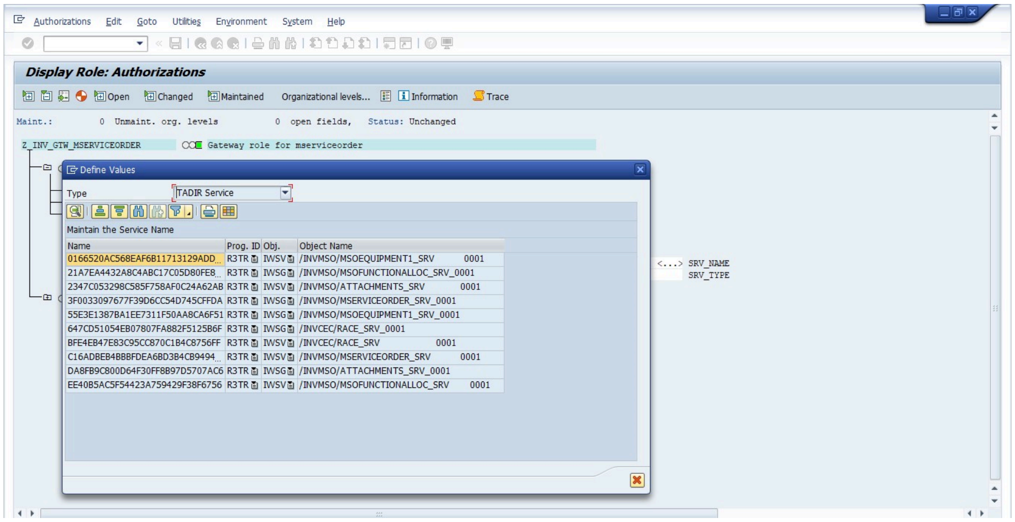
3. Pick the names of the hashed services (the 30-character length alpha numerical name) and use them under S_SERVICE - SRV_NAME.

Figure 4-15 Hashed Service Name



```
Manually   Check at Start of External Services                S_SERVICE
  Manually   Check at Start of External Services                T-NT36012700
    Program, transaction or functi 0166520AC568EAF6B11713129ADD1A, 21A7EA4432A8C4ABC17C05D80FE84F   <...> SRV_NAME
    Type of Check Flag and Authori HT                                                                       SRV_TYPE
```

Figure 4-16 Display Role Authorization



Display Role: Authorizations

Maint.: 0 Unmaint. org. levels 0 open fields, Status: Unchanged

Z_INV_GTW_MSERVICEORDER Gateway role for mserviceorder

Define Values

Type: TADIR Service

Maintain the Service Name

Name	Prog. ID	Obj.	Object Name
0166520AC568EAF6B11713129ADD...	R3TR	IWSV	/INVMSO/MSOEQUIPMENT1_SRV 0001
21A7EA4432A8C4ABC17C05D80FE8...	R3TR	IWSG	/INVMSO/MSOFUNCTIONALLOC_SRV_0001
2347C053298C585F758AF0C24A62AB	R3TR	IWSV	/INVMSO/ATTACHMENTS_SRV 0001
3F0033097677F39D6CC54D745CFFDA	R3TR	IWSG	/INVMSO/MSERVICEORDER_SRV_0001
55E3E1387BA1EE7311F50AA8CA6F51	R3TR	IWSG	/INVMSO/MSOEQUIPMENT1_SRV_0001
647CD51054EB07807FA882F5125B6F	R3TR	IWSG	/INVCEC/RACE_SRV_0001
BFE4EB47E83C95CC870C1B4C8756FF	R3TR	IWSV	/INVCEC/RACE_SRV 0001
C16ADBEB4BBBFDEA6BD3B4CB9494...	R3TR	IWSV	/INVMSO/MSERVICEORDER_SRV 0001
DA8FB9C800D64F30FF8B97D5707AC6	R3TR	IWSG	/INVMSO/ATTACHMENTS_SRV_0001
EE40B5AC5F54423A759429F38F6756	R3TR	IWSV	/INVMSO/MSOFUNCTIONALLOC_SRV 0001

<...> SRV_NAME
SRV_TYPE

4.5.2. Transports for mServiceOrder 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 145)* to understand how to import transports.

Table 4-22 SAP ECC Transports

Transport	Description	Dependency
ERDK904864	INNOV:ECC: R 6.1.0 mService-Order Application End User Roles	None

Table 4-23 SAP GW Transports

Transport	Description	Dependency
NGTK904541	INNOV:GW: R 6.1.0 mService-Order Application End User Roles	None

4.6. 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 4-24 Roles for ECC System

Role Name	Description	Transactions	Authorization Objects
ZINV_RDF_ECC_END_USER_R2009	RACE Dynamic Forms - End User - ECC Authorizations - Release 2009	/INVMGO/DOCFORM	S_RFC, S_RFCACL

Table 4-24 Roles for ECC System (continued)

Role Name	Description	Transactions	Authorization Objects
ZINV_RDF_ECC_RACE_ADM_R2009	RACE Dynamic Forms - RACE Admin - ECC Authorizations – Release 2009	-	S_RFC and S_RFCACL

Table 4-25 Roles for NetWeaver Gateway System

Role Name	Description	Authorizations
ZINV_RDF_NWG_END_USER_R2009	RACE Dynamic Forms - End User - Gateway Authorizations – Release 2009	S_RFC, S_RFCACL, S_SERVICE, S_USER_GRP
ZINV_RDF_NWG_RACE_ADM_R2009	RACE Dynamic Forms - RACE Admin - Gateway Authorizations – Release 2009	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.

4.6.1. Update Service authorization object for RACE Dynamic Forms

Update the system specific S_SERVICE authorization object with customer system generated service value.

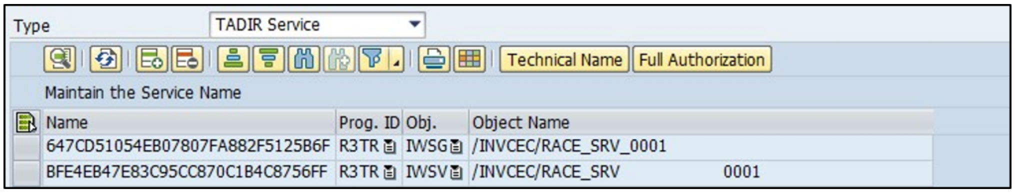
To update service values under S_SERVCE:

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

Table 4-26 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 4-17 USOBHASH table



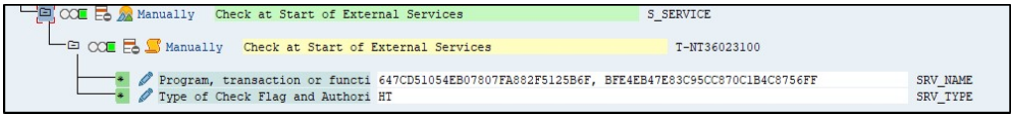
Type: TADIR Service

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 4-18 Hashed Service Name



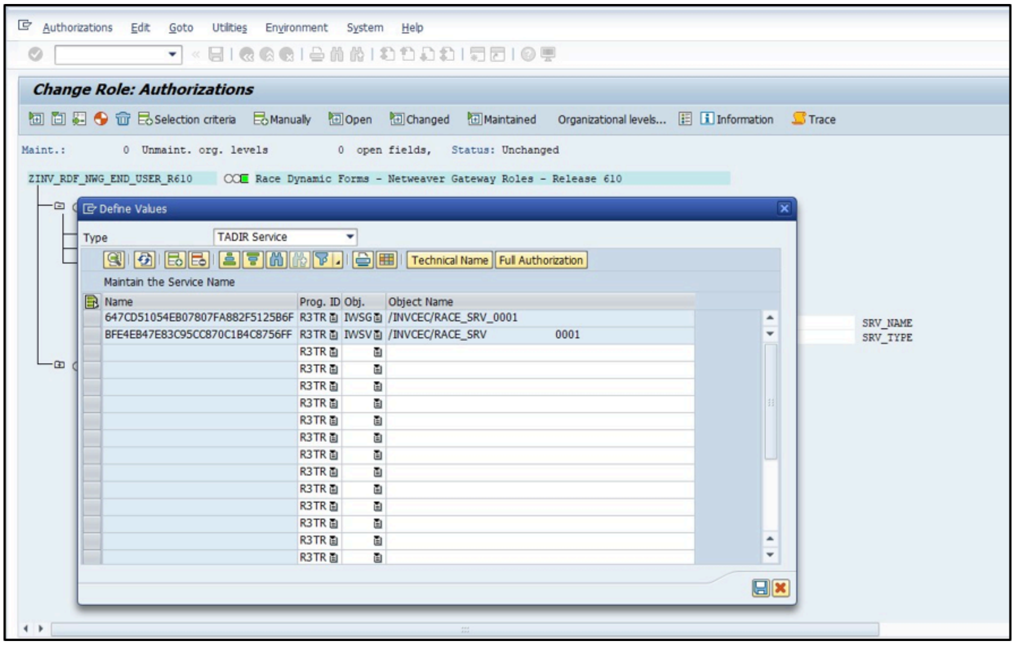
Manually Check at Start of External Services S_SERVICE

Manually Check at Start of External Services T-NT36023100

Program, transaction or functi 647CD51054EB07807FA882F5125B6F, BFE4EB47E83C95CC870C1B4C8756FF SRV_NAME

Type of Check Flag and Authori HT SRV_TYPE

Figure 4-19 Change Role Authorization



Change Role: Authorizations

Maint.: 0 Unmaint. org. levels 0 open fields, Status: Unchanged

ZINV_RDF_NWG_END_USER_R610 Race Dynamic Forms - Netweaver Gateway Roles - Release 610

Define Values

Type: TADIR Service

Maintain the Service Name

Name	Prog. ID	Obj.	Object Name	
647CD51054EB07807FA882F5125B6F	R3TR	IWSG	/INVCEC/RACE_SRV_0001	
BFE4EB47E83C95CC870C1B4C8756FF	R3TR	IWSV	/INVCEC/RACE_SRV	0001
	R3TR			
	R3TR			
	R3TR			
	R3TR			
	R3TR			
	R3TR			
	R3TR			
	R3TR			
	R3TR			
	R3TR			
	R3TR			
	R3TR			
	R3TR			

4.6.2. 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 145)* to understand how to import transports.

Table 4-27 SAP ECC Transports

Transport	Description	Dependency
ERDK905830	INNOV:ECC: R 2009 RACE DF Application End User Roles	None

Table 4-28 SAP GW Transports

Transport	Description	Dependency
NGTK905372	INNOV:GW: R 2009 RACE DF Application End User Roles	None

4.7. User roles for RACE

Following set of user roles are available for RACE application

Table 4-29 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