

Pre-Install or Pre-Upgrade Configurations Guide 2208

Connected Worker Solutions



Title and Copyright

Copyright and **Terms of Use** for the Pre-Install or Pre-Upgrade Configurations Guide for mAssetTag, mWorkOrder, mInventory and all other solutions of *Connected Workforce Platform*[™].

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

Product Version: 2208

Release Date: 06 September 2022

Published Date: 06 September 2022

Document Version: 1.0

Copyright © 2022, Innovapptive Inc. and/or its affiliates. All rights reserved.

Primary Author: Innovapptive Inc.

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

Preface

Understand audience and conventions followed in this document.

Audience

This guide is for technical configurators who do configurations for mAssetTag, mWorkOrder, mInventory, mServiceOrder, mWorkList and 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.
<i>italic</i>	Indicates book titles, emphasis, or placeholder variables for which you supply values.
<code>monospace</code>	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

Title and Copyright.....	2
Preface.....	3
1. Pre-Install or Pre-Upgrade Configurations for Innovapptive Products.....	7
2. SAP BTP Configurations before Installing Innovapptive Products.....	8
3. Configure SAP NetWeaver Gateway—BgRFC.....	10
3.1. Before you Configure SAP NetWeaver Gateway - BgRFC.....	10
3.2. Create BgRFC Destination for Outbound Queues.....	10
3.3. Register BgRFC Destination for Outbound Queue.....	12
3.4. Create BgRFC Destination for Supervisor.....	14
4. Configure NetWeaver Gateway.....	16
4.1. Install SAP NetWeaver Gateway.....	16
4.1.1. System Requirements.....	17
4.2. Establish trust between Gateway and ECC.....	18
4.3. Define Connection Settings to SAP NetWeaver Gateway.....	20
4.4. Create the SAP System Alias for Applications.....	21
4.5. Activate SAP NetWeaver Gateway.....	22
4.6. Define Settings for Idempotent Services.....	23
4.7. Set Profile Parameters in SAP NetWeaver Gateway.....	24
4.8. Maintain HTTPS and HTTP Connections.....	26
4.9. Configure SAP Gateway virus scan profile.....	28
4.10. Create Periodical Tasks for Gateway.....	28
4.11. Clear Application Log Entries.....	29
4.12. Clear Query Result Log Entries.....	30
4.13. Install certificates for Geo location.....	31
5. Configure ECC.....	33
6. Configure Access for Deploying Innovapptive Products.....	34
6.1. Access Required for Configuring SAP BTP.....	36

6.2. Import Roles Using Transports.....	36
7. Configure SAP BTP for Deploying Innovapptive Products.....	39
7.1. Validate access to SAP BTP.....	40
7.2. Enable Mobile Services.....	40
7.3. Import Cloud Connector Root and Intermediate Certificates to Gateway Trust Store.....	42
7.4. Configure Access Control.....	42

1. Pre-Install or Pre-Upgrade Configurations for Innovapptive Products

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



Note:

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

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

Table 1-1
Innovapptive
Products

Product
mWorkOrder
mInventory
mServiceOrder
mAssetTag
RACE Dynamic Forms

2. SAP BTP Configurations before Installing Innovapptive Products

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

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

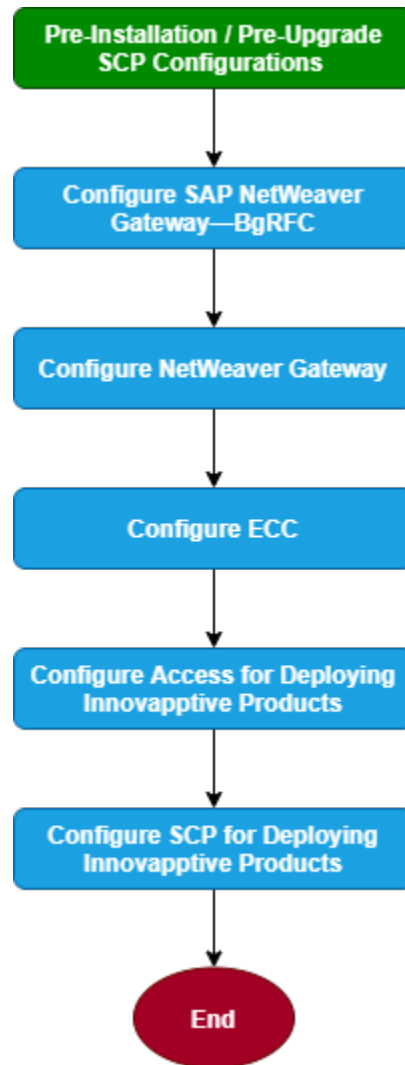


Table 2–1 Tasks for SAP BTP Configurations before Installing Innovapptive Products

Task	Reference to section
Configure SAP NetWeaver Gateway—BgRFC	Configure SAP NetWeaver Gateway—BgRFC (on page 10)
Configure NetWeaver Gateway	Configure NetWeaver Gateway (on page 16)
Configure ECC	Configure ECC (on page 33)
Configure Access for Deploying Innovapptive Products	Configure Access for Deploying Innovapptive Products (on page 34)
Configure SAP BTP for Deploying Innovapptive Products	Configure SAP BTP for Deploying Innovapptive Products (on page 39)

3. Configure SAP NetWeaver Gateway—BgRFC

This section helps you configure SAP NetWeaver Gateway—BgRFC

- [Before you Configure SAP NetWeaver Gateway - BgRFC \(on page 10\)](#)
- [Create BgRFC Destination for Outbound Queues \(on page 10\)](#)
- [Register BgRFC Destination for Outbound Queue \(on page 12\)](#)
- [Create BgRFC Destination for Supervisor \(on page 14\)](#)

3.1. Before you Configure SAP NetWeaver Gateway - BgRFC

Ensure that the following components are installed and configured:

System & Software

- SAP ECC Business Suite is installed and connected to mobile infrastructure (NetWeaver Gateway, SCPms).
- SAP NetWeaver Gateway 7.4 and above with SAP_GWFND component (SP 13 and above) and SAP_UI component (SP 13 and above).

Access

- SAP Basis System Admin with access to Gateway system.
- SAP Security Admin with access to Gateway system.

3.2. Create BgRFC Destination for Outbound Queues

Create a background remote function call (bgRFC) destination for communications in an outbound queue.

To create BgRFC Destination for the outbound queue:

1. In transaction **SPRO**, open SAP Reference IMG.
2. Navigate to **SAP NetWeaver, SAP Gateway, OData Channel, Configuration, Connection Settings, SAP NetWeaver Gateway to Consumer, Create RFC Destination for Outbound Queues**.
3. Click **Activity**.
4. Click **Create**.

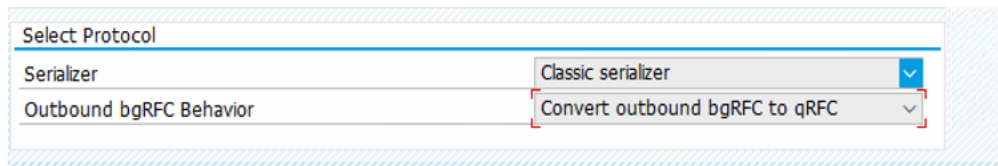
5. In the **RFC Destination** field, enter the name for the RFC destination **IWFND_BGRFC_DEST**.
6. In the **Connection Type** field, enter **3**.
7. In **Description 1** field, enter **RFC Destination for Outbound Queues**.
8. On the **Special Options** tab, select the **Transfer Protocol** as "**Classic with BgRFC**"/
"Classic Serializer" with **"Convert outbound bgRFC to qRFC"**.

Figure 3-1 RFC Destination – Special Options tab

The screenshot shows the SAP configuration interface for an RFC Destination named **IWFND_BGRFC_DEST**. At the top, there are tabs for **Remote Login**, **Connection Test**, and **Unicode Test**. Below these, the **RFC Destination** field contains **IWFND_BGRFC_DEST**, and the **Connection Type** is set to **3** (ABAP Connection). The **Description** section has three fields: **Description 1** is **RFC Destination for Outbound Queues**, while **Description 2** and **Description 3** are empty. A navigation bar at the bottom includes **Administration**, **Technical Settings**, **Logon & Security**, **Unicode**, and **Special Options** (which is currently selected). Under the **Special Options** tab, there are three sections: **Trace Export Methods** with radio buttons for **Default Gateway Value** (selected), **Export Trace**, and **Do Not Export Trace**; **Keep-Alive Timeout** with radio buttons for **Default Gateway Value** (selected), **Timeout Inactive**, and **Specify Timeout** (with a value of **300** and the text "Defined Value in Seconds"); and **Select Transfer Protocol** with a dropdown menu showing **Classic with bgRFC**.

If you do not find **Classic with BgRFC**, select the **Convert outbound bgRFC to qRFC**

Figure 3-2 RFC Destination – Special Options tab



Select Protocol	
Serializer	Classic serializer
Outbound bgRFC Behavior	Convert outbound bgRFC to qRFC

9. Click **Save**.
10. Click **Yes** on the confirmation message.
11. Click **Connection Test**.

3.3. Register BgRFC Destination for Outbound Queue

Register the BgRFC destination for the outbound queue to handle communications efficiently.

To register the BgRFC destination for the Outbound Queue:

1. In the transaction **SPRO**, open the SAP Reference IMG.
2. Navigate to **SAP NetWeaver, SAP Gateway, OData Channel, Configuration, Connection Settings, SAP Gateway to Consumer, Register RFC Destination for Outbound Queues**.
3. Click **Activity**.
4. Click **Create** on the **Define Inbound Dest.** tab.

Figure 3-3 Define Inbound Destination

bgRFC Configuration

Scheduler: System Scheduler: App. Server Scheduler: Destination **Define Inbound Dest.** Define Supervisor Dest.

Destination

IWFND_BGRFC_DEST

Logon/server group

Prefixes

IWCNT_WF

IWFND_CNP

New Prefix

Last Changed

User Name ZZMARIM

Client ID 100

Time 10:01:39

Current Date 09/05/2015

5. Enter **IWFND_BGRFC_DEST** in the **Inb. Dest. Name** field and click **<Enter>**.
6. In the **New Prefix** field, create entries, for example **IWFND_CNP** and **IWCNT_WF** and save the settings.

- Click **Create** on the **Scheduler: Destination** tab.

Figure 3-4 Scheduler: Destination tab

bgRFC Configuration

Scheduler: System Scheduler: App. Server **Scheduler: Destination** Define Inbound Dest. Define Supervisor Dest.

Destination Name: IWFND_BGRFC_DEST

Inbound Destination: IWFND_BGRFC_DEST

Scheduler Count: 1

Max. Auto. Retries: 30

Wait per Unit (s): 900

Wait/Destination (s): 900

Dest.Proc. Time (s):

Open Connections: 10

Unit Alive Checks: 30

History Active: ☐

Check Class: ☐ Active/Inactive

Check Class:

Last Changed:

User Name:

Client ID:

Time: 00:00:00

Current Date:

- In the confirmation message, click **Inbound**.
- Enter **IWFND_BGRFC_DEST** in the **Destination** field and click **Save**.

3.4. Create BgRFC Destination for Supervisor

Configure a supervisor destination for the BgRFC to receive configuration settings for the BgRFC scheduler. A supervisor starts or stops the schedulers.

To create the BgRFC destination for supervisor:

- In transaction **SPRO**, open SAP Reference IMG.
- Navigate to **SAP NetWeaver, SAP Gateway, OData Channel, Configuration, Connection Settings, SAP Gateway to Consumer, Create BgRFC Supervisor Destination**.
- Click **Activity**.
- In the **Define Supervisor Dest** tab, click **Create**.

Figure 3-5 Create RFC Destination for Supervisor

The screenshot shows the 'bgRFC Configuration' window with the 'Create RFC Destination for Supervisor' tab active. The 'Destination Name' field contains 'BGRFC_SUPERVISOR'. Under the 'User' section, the 'Create User' and 'Generate Password' checkboxes are selected, and the 'User Name' field contains 'BGRFC_USER'. The 'Changed At' field shows '00:00:00'. A 'Save' button is located at the bottom right of the dialog.

5. In the **Destination Name** field, enter **BGRFC_SUPERVISOR**.
6. In the **User Name** field, enter a user name. For example, **BgRFC_user**.
7. Select the **Create User** check box.
8. Select the **Generate Password** check box.
9. Click **Save**.
10. On the **BgRFC Destination** screen, click **Save**.

4. Configure NetWeaver Gateway

Configure SAP NetWeaver Gateway to define how some settings must work with your existing SAP ECC Business Suite system.

Prerequisites

Ensure the following components are installed and configured:

- **System & Software**

- For HUB architecture SAP ECC Business Suite / S4HANA is installed and connected to the mobile infrastructure (NetWeaver Gateway, SCPms).
- SAP NetWeaver Gateway 7.4 and above with SAP_GWFND component (SP 13 and above) and SAP_UI component (SP 13 and above).
- For EMBEDDED architecture SAP ECC Business Suite / S4HANA is installed and connected to the mobile infrastructure (SCPms).

- **Access**

- SAP Basis System Admin with access to Gateway and ECC systems.
- SAP Service marketplace access (S-User ID).

- **Dependency**

- ECC backend Business suite system host details to create RFC (in HUB).
- In EMBEDDED systems, LOCAL_RFC can be created & "Current user" ticked in Logon data of the RFC
- SCPms host and port details for creating RFC.

- **Assumptions**

Port number for HTTP = 8000 and HTTPS = 8080.

4.1. Install SAP NetWeaver Gateway

Install SAP NetWeaver Gateway using SAP NetWeaver Application Server ABAP (AS ABAP) add-on. Download the installation package from <http://service.sap.com/swdc>.

SAP NetWeaver 7.4 ABAP with Support Release 2 package includes NetWeaver 7.4 SP08 and Gateway component SAP_GWFND SP13.



Note:

Ensure that the SAP ECC Business Suite setup is completed and ready to be connected with the Gateway.

4.1.1. System Requirements

Hardware

Table 4-1 Hardware Prerequisites for NetWeaver Gateway

Requirement	Specification
Processor	Dual Core (2 logical CPUs) or higher, 2 GHz or higher
Random Access Memory (RAM)	8 GB or higher
Hard Disk Capacity	80 GB primary, or higher

Software

Table 4-2 Software Prerequisites for NetWeaver Gateway

Requirement	Specification
SAP NetWeaver Stack	Apply the latest kernel patch for the SAP NetWeaver version.
	Core Component • SAP NetWeaver 7.40 SPS08 • SAP NetWeaver Gateway Foundation SAP_GWFND SP 13  Note: Comprises functional scope of components IW_FND, GW_CORE, IW_BEP, and IW_HDB.
SAP Backend	SAP Business Suite system

For information about the Product Availability Matrix for SAP NetWeaver 7.4, see <https://support.sap.com/release-upgrade-maintenance/pam.html>.

For installation procedure, see the SAP document: <https://websmp208.sap-ag.de/~sapidb/011000358700000828172012E#q1>.

4.2. Establish trust between Gateway and ECC

Learn how to establish trust between Gateway and ECC. This is applicable in HUB Architecture.

To define the trust between the Gateway and ECC:

1. On the SAP NetWeaver Gateway, open the **SM59** transaction and click **Create**.
2. In the **RFC Destination** field, enter the RFC destination name in the **<system id > CLNT <Client>** format.

Figure 4-1 RFC Destination

The screenshot displays the SAP SM59 transaction for creating an RFC Destination. The title bar reads "RFC Destination ERDCLNT800". Below the title bar are tabs for "Remote Logon", "Connection Test", and "Unicode Test". The main form contains the following fields and sections:

- RFC Destination:** ERDCLNT800
- Connection Type:** 3 (ABAP Connection)
- Description:** A section with three text boxes. "Description 1" contains "Connection to ERD Backend system".
- Administration Tab:** Contains fields for "Client" (800), "User" (empty), "PW Status" (is initial), and a "Current User" checkbox (checked).
- Trust Relationship:** Radio buttons for "No", "Yes" (selected), and "Logon Screen" (unchecked).
- Status of Secure Protocol:** A section with an "SNC" icon and radio buttons for "Inactive" (selected) and "Active" (unchecked).
- Authorization for Destination:** A text box (empty).
- Callback Positive List:** A section with a "Positive List Actv" checkbox (unchecked) and a table with two columns: "Called Function Module" and "Callback Function Module". The first row shows "Called Function Module" and "Callback Function Module".

3. Enter **3** in the **Connection Type** field.
4. Enter description in the **Description 1** field. For example, **Connection to Backend System**.
5. Save your settings.
6. On the **Technical Settings** tab, select the option as per your system settings.
7. Enter the name of the SAP NetWeaver Gateway system in the **Target Host** field.
8. Enter the SAP NetWeaver Gateway system number in the **System Number** field.
9. Save your settings.
10. Click **Create** in transaction **SMT1**.

A window for creating trusting relationships appears.

11. Enter the RFC destination that you created in the window.

An RFC logon to the SAP NetWeaver Gateway host occurs and the required information exchange happens.

12. Log on to the SAP NetWeaver Gateway host.

The trusted entry for the SAP NetWeaver Gateway host appears.

13. Save your settings.

14. Navigate to the **RFC** that you created in the previous step.

15. Select the current user on the **Logon & Security** tab.

16. Click **Yes**.

17. Save your settings.

18. Click **Connection Test**.

Figure 4-2 Connection Test

<i>RFC - Connection Test</i>	
Connection Test ERDCLNT800 Connection Type SAP Connection	
Action	Result
Logon	10 msec
Transfer of 0 KB	1 msec
Transfer of 10 KB	1 msec
Transfer of 20 KB	3 msec
Transfer of 30 KB	2 msec

Calls from the systems that are trusted is displayed on **Trusted - Trusting Connections** screen.

Figure 4-3 Trusted Calling Systems

<i>Trusted-Trusting Connections</i>					
 Systems whose calls are trusted Systems that trust current system          <table> <tr> <th>Calling Systems</th><th>Inst.</th></tr> <tr> <td> ABAP Systems - CRD - EH7 - ERD - ERQ </td><td> 0090055493 0020732636 0020732636 0020732636 </td></tr> </table>		Calling Systems	Inst.	ABAP Systems - CRD - EH7 - ERD - ERQ	0090055493 0020732636 0020732636 0020732636
Calling Systems	Inst.				
ABAP Systems - CRD - EH7 - ERD - ERQ	0090055493 0020732636 0020732636 0020732636				

4.3. Define Connection Settings to SAP NetWeaver Gateway

Identify the SAP Gateway for which you want to define connection settings. Once you identify, do the following:

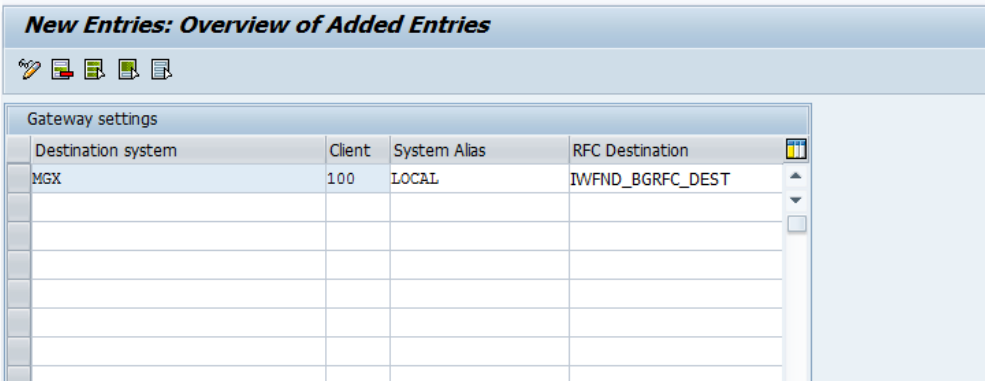
Before defining the connection settings, do the following:

- Define an RFC destination for SAP Gateway to broadcast events.
- Note down the system name, client ID and a system alias of the host of the SAP Gateway.

To define the connection settings:

1. In transaction SPRO, open SAP Reference IMG and navigate to **SAP NetWeaver, SAP Gateway Service Enablement, Backend OData Channel, Connection Settings to SAP Gateway, SAP Gateway Settings**.
2. Click **Activity**.
3. Click **New Entries** and enter the following:
 - **Destination System:** SID of the Gateway system. For EMBEDDED, it is System SID
 - **Client:** Client ID of the host of SAP NetWeaver Gateway. The client ID, you specify, must exist in the system.
 - **System Alias:** LOCAL.
 - **RFC Destination:** IWFND_BGRFC_DEST.

Figure 4-4 Connection Settings: New Entries



Gateway settings			
Destination system	Client	System Alias	RFC Destination
MGX	100	LOCAL	IWFND_BGRFC_DEST

4. Save your settings.

4.4. Create the SAP System Alias for Applications

To create the SAP system Alias for applications:

1. In the transaction SPRO, open SAP Reference IMG and navigate to **SAP NetWeaver, SAP Gateway, OData Channel, Configuration, Connection Settings, SAP Gateway to SAP System, Manage SAP System Aliases**.
2. Click **Activity**.
3. Click **New Entries**.
4. Enter the following details:
 - **SAP System Alias:** Name of the system Alias. Preferably create a new one as "INNOVAPPTIVE"
 - **Description:** Descriptive text for the system alias. For example, Innovapptive Mobile Applications
 - **Local GW:** Select the check box.
 - **For Local App:** Select the check box.
 - **RFC Destination:** Specify the RFC destination that you defined for backend SAP system.



Note:

For HUB systems, it is backend ECC RFC. For example ECDCLNT100 and For EMBEDDED systems, it is backend local RFC. For example LOCAL RFC

- Software Version: DEFAULT.
- System ID: Name of the SAP target system.
- Client: Target client.

Figure 4-5 Manage SAP System Aliases

Change View "Manage SAP System Aliases": Overview							
New Entries							
Manage SAP System Aliases							
SAP System Alias	Description	Local SAP	For Local App	RFC Destination	Software Version	System ID	Client
ERD	ECC Backend for Fiori	☒	☒	ERDCLNT800	DEFAULT	ERD	800
WS Provider System							

5. Save your settings.

4.5. Activate SAP NetWeaver Gateway

To activate the SAP NetWeaver Gateway:

1. In transaction SPRO, open SAP Reference IMG and navigate to **SAP NetWeaver, SAP Gateway, OData Channel, Configuration, Activate or Deactivate SAP NetWeaver Gateway**.
2. Click **Activity**.
3. Click **Activate**.

A message appears notifying the status.

4.6. Define Settings for Idempotent Services

You can configure idempotent services by scheduling a background job that ensures that the request messages in SAP NetWeaver Gateway occur only once.

To define settings for Idempotent Services:

1. In transaction SPRO, open SAP Reference IMG and navigate to **SAP NetWeaver, SAP Gateway Service Enablement, Backend OData Channel, Connection Settings to SAP Gateway, Define Settings for Idempotent Services**.
2. Click **Activity**.
3. In **Document** section, enter **6** in the **Period in Hours** field.
4. In **Document ID** section, enter **12** in the **Period in Hours** field.
5. Click **Schedule**.

Figure 4-6 Idempotent Services Settings

Program SRT_WS_IDP_CUSTOMIZE

Jobs

Schedule Switch for IDP WS

Document

☒ Switch Document Tables

Job Name SAP_BC_IDP_WS_SWITCH_BD

Period in Days

Period in Hours 6

☐ Change Time of Next Switch 03.09.2016 09:39:06

Document ID

☒ Switch Document ID Tables

Job Name SAP_BC_IDP_WS_SWITCH_BDID

Period in Days

Period in Hours 12

☐ Change Time of Next Switch 18.09.2016 03:39:06

6. Click **Continue**.

4.7. Set Profile Parameters in SAP NetWeaver Gateway

Set the following profile parameters in the SAP NetWeaver Gateway system.

To set the profile parameters:

1. Go to transaction code **RZ11** and check if the parameters are set to the below-mentioned values. If not set, create the parameters in **RZ10** transaction under default profile.

Table 4-3 Profile Parameters

login/accept_sso2_ticket	1
login/create_sso2_ticket	2
icm/HTTPS/verify_client	1
icm/HTTPS/trust_client_with_issuer	*

icm/HTTPS/trust_client_with_subject	*
-------------------------------------	---

2. Activate SICF Services: **/sap/opu** and **/sap/bc/ping**.

Figure 4-7 SICF: /sap/opu

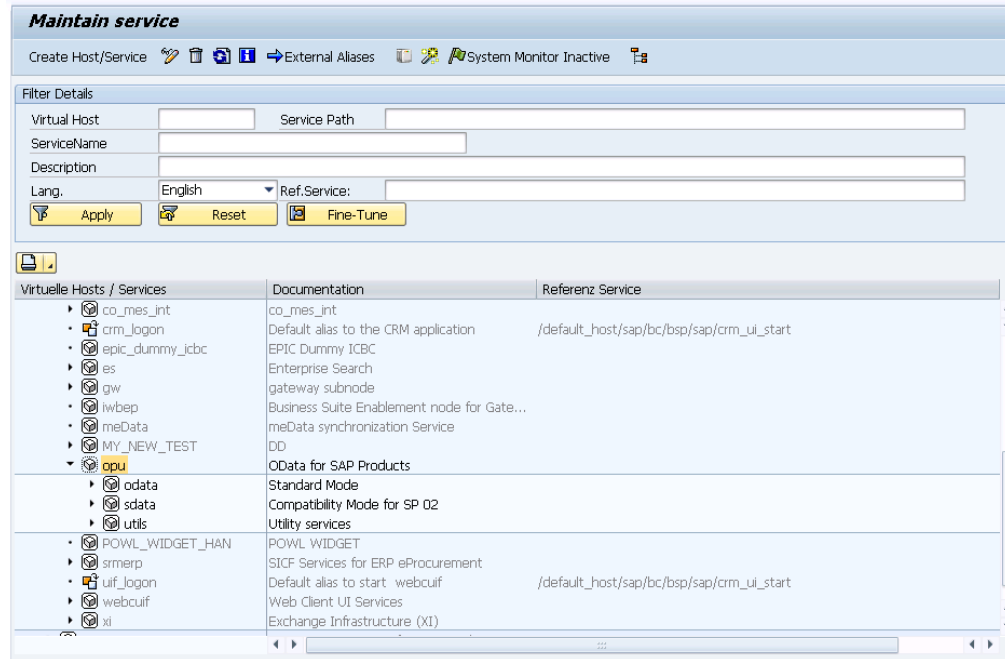
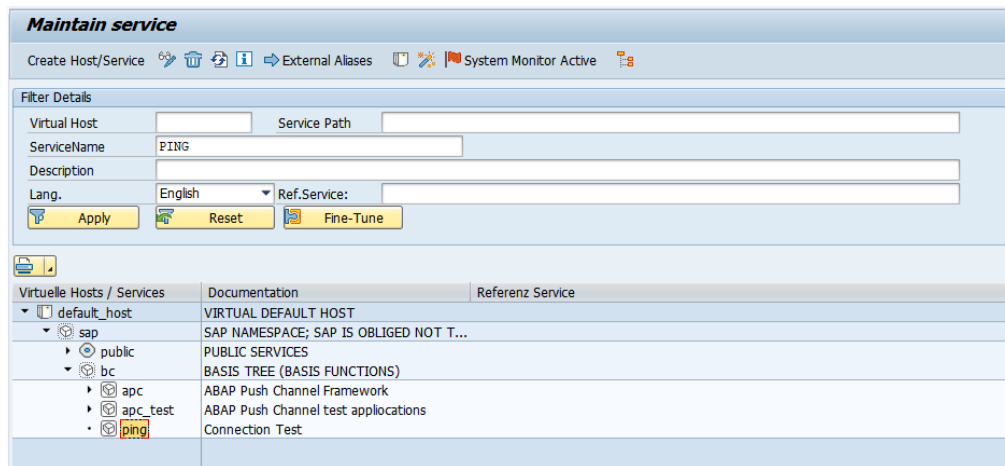


Figure 4-8 SICF: /sap/bc/ping



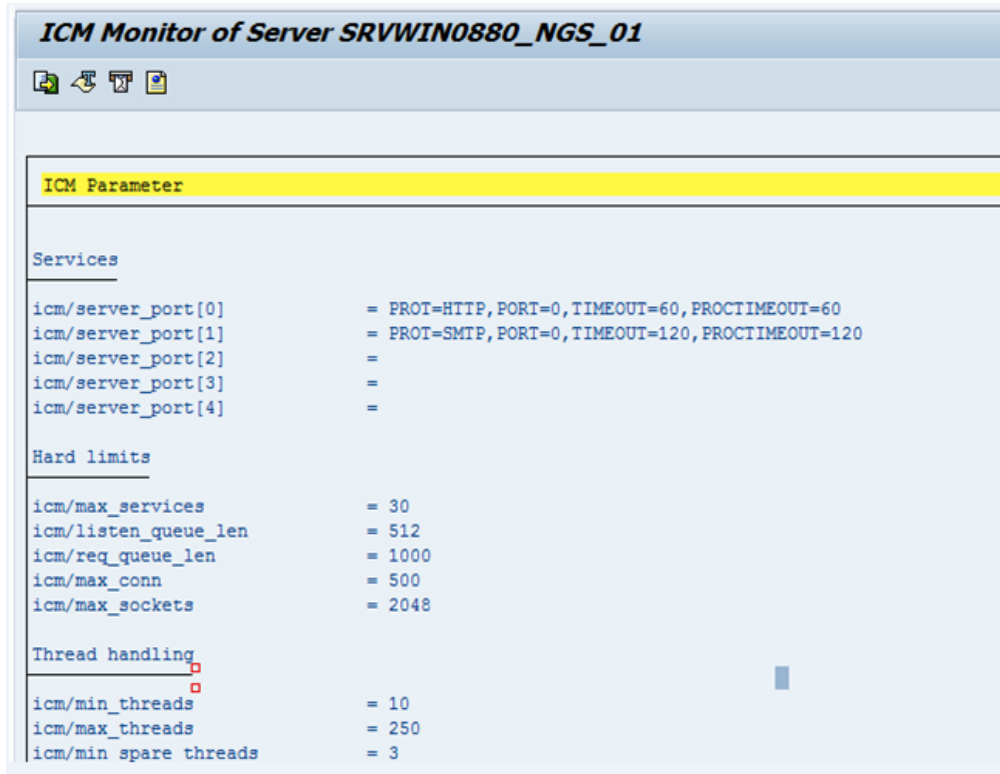
4.8. Maintain HTTPS and HTTP Connections

To maintain HTTPS and HTTP connections:

1. Run Tcode **RZ10** and set these parameters:

- icm/server_port_0 = PROT=HTTP, PORT=8000, TIMEOUT=600, PROCTIMEOUT=600
- icm/server_port_2 = PROT=HTTPS, PORT=8080, TIMEOUT=600, PROCTIMEOUT=600

Figure 4-9 ICM Parameters



2. Restart the system.
3. Go to **SMICM** transaction.
4. Click the **Services** tab and validate the HTTP and HTTPS connections.

Figure 4-10 ICM Monitor

Active Services						
No.	Protocol	Service Name/Port	Host Name	Keep Alive	Proc.Timeo	Actv
☒	1 HTTP	8000	INNONGWDEV.internal.	600	600	✓
☐	2 SMTP	0	INNONGWDEV.internal.	120	120	✓
☐	3 HTTPS	443	INNONGWDEV.internal.	600	600	✓

4.9. Configure SAP Gateway virus scan profile

Application programs use virus scan profiles to check data for viruses. A virus scan profile comprises of the scanner groups that verify the document, and the process to scan.



Note:

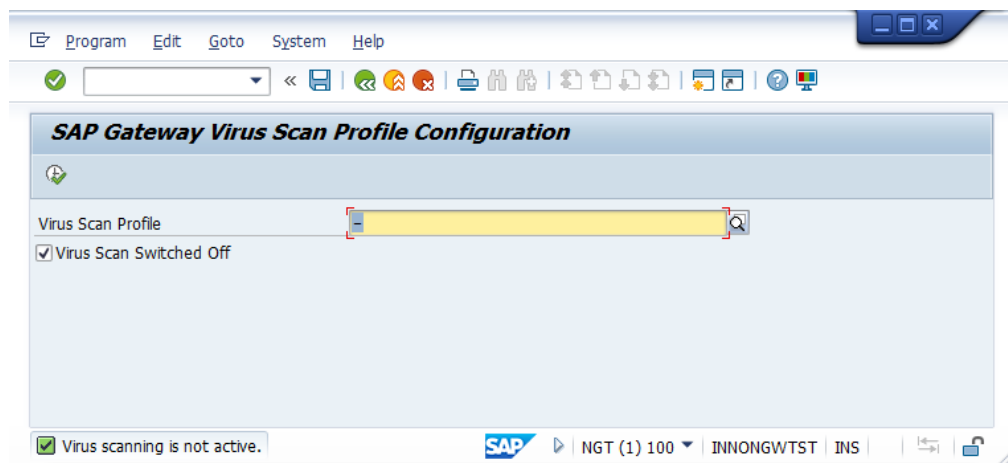
The Virus Scan must be enabled in Gateway only if the virus profile is defined.

For more information, see SAP Notes: 786179 - *Data security products: Application in the antivirus area*.

To disable SAP Gateway virus scan:

1. Go to **/n/IWFND/VIRUS_SCAN** transaction.
2. Select the **Virus Scan Switched Off** check box and execute.

Figure 4-11 Gateway Virus Scan Profile



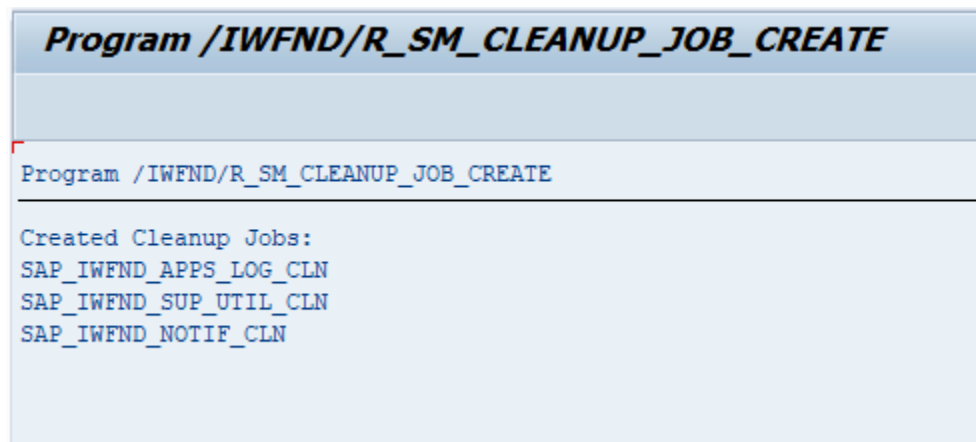
4.10. Create Periodical Tasks for Gateway

Periodical tasks like of disk and memory space cleanup ensure optimal performance of the Gateway system.

To create periodical tasks:

1. In the transaction SPRO, open SAP Reference IMG and navigate to **SAP NetWeaver, SAP Gateway, OData Channel, Administration, Cache Settings, Create Default Cleanup Jobs**.
2. Click **Activity**.
3. Following tasks are created:
 - **SAP_IWFND_SUP_UTIL_CLN**: Deletes logs of support utilities, such as error logs, traces, and performance logs.
 - **SAP_IWFND_APPS_LOG_CLN**: Deletes SAP Gateway entries from the application log.
 - **SAP_IWFND_NOTIF_CLN**: Deletes the SAP Gateway notifications.

Figure 4-12 Gateway Cleanup tasks



4.11. Clear Application Log Entries

To delete application log entries:

1. Go to **Transaction SE38**.
2. Enter the **Program** name as **SBAL_DELETE** and click **Execute**.
3. Set the criteria to delete the log entries.

Figure 4-13 Clear Log Entries Criteria

Application Log: Delete Expired Logs

Delete logs

All logs are deleted which satisfy the following selection conditions, and for which:

- the expiry date is reached or passed
- the expiry date is not defined

Expiry date

☐ Only logs which have reached their expiry date
☒ and logs which can be deleted before the expiry date
☐ Cannot delete log now since expiry date is in the future

Selection conditions

Object		to		
Subobject		to		
External ID		to		
Transaction code		to		
User		to		
Log number		to		
Problem class		to		
from (date/time)			00:00:00	
to (date/time)			00:00:00	

Options

☐ Only calculate how many
☐ Generate list
☒ Delete immediately

Delete by Number of Logs

COMMIT Counter

4. Go to **Program** in the menu bar and click **Execute in Background**.
5. Click **Continue**.
6. Click **Date/Time** button and enter the date and time when the program must be executed.
7. Click on **Period Values** button and set the frequency. (Preferably during non-peak hours)
8. Click **Save**.

4.12. Clear Query Result Log Entries

To delete the query result logs:

1. Go to **Transaction SE38**.
2. Enter the **Program** name as **/IWBEP/R_CLEAN_UP_QRL** and click **Execute**.
3. Set the criteria to delete the log entries in the **Selection Parameters** section.

Figure 4-14 Clear Log Entries Criteria

Cleanup of Query Result Log

Selection Parameters

Records Older Than (in Hours)

☒ Delete Log Headers

Control Parameters

☐ Execute in Test Mode

4. Go to **Program** in the menu bar and click **Execute in Background**.
5. Click **Continue**.
6. Click **Date/Time** button and enter the date and time when the program must be executed.
7. Click on **Period Values** button and set the frequency.
8. Click **Save**.

4.13. Install certificates for Geo location

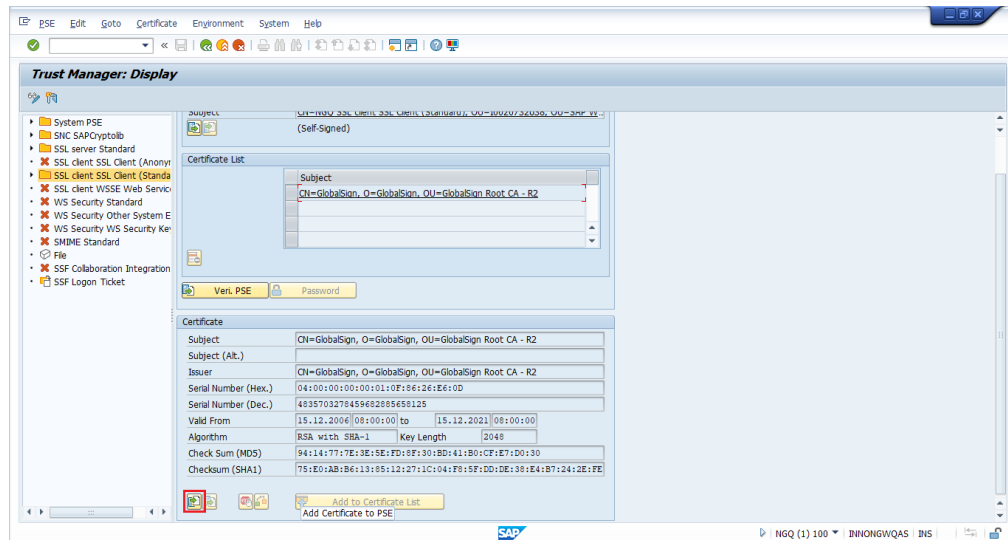
Geo Location certification is only applicable for Workorders, Notifications, Equipment, Functional Locations modules of mWorkorder and mServiceOrder applications. Do this only if this in scope.

To install the certificate:

| 4 - Configure NetWeaver Gateway

1. Navigate to transaction code: **STRUST**.
2. Click **SSL client SSL Client (Standard)**.
3. Click the **Import**  icon to import the certificate.

Figure 4-15 Trust Manager



4. Click on **Add to Certificate List** option.
5. Click **Save**.

5. Configure ECC

If you have HUB architecture, you must configure ECC.

To configure ECC:

1. On the SAP ECC system, open the transaction **SM59** and click **Create**.
2. In the **RFC Destination** field, enter the RFC destination name in the **<system id > CLNT <Client>** format.
3. Enter **3** in the **Connection Type** field.
4. Specify text in the **Description 1** field.
5. Save your settings.
6. On the **Technical Settings and Load Balancing** tab, select the option according to your system settings.
7. Enter the name of the SAP NetWeaver Gateway system in the **Target Host** field.
8. Enter the SAP NetWeaver Gateway system number in the **System Number** field.
9. Save your settings.
10. Click **Create** in transaction **SMT1**.
11. In the window for creating trusting relationships, enter the RFC destination that you created.
An RFC logon to the SAP NetWeaver Gateway host takes place and the necessary information is exchanged between the systems.
12. Log on to the SAP NetWeaver Gateway host.
The trusted entry for the SAP NetWeaver Gateway host appears.
13. Save your settings.
14. Navigate to the **RFC** that you created in the previous step.
15. Select the current user on the **Logon & Security** tab.
16. Click **Yes**.
17. Save your settings.
18. Click **Connection Test**.

6. Configure Access for Deploying Innovapptive Products

Understand the roles and access requirements for deploying Innovapptive mobile products.

The following table lists the roles that are packaged with Innovapptive mobile products and access to the transactions required for Basis Administrator, ABAP Developers, Configurators and Security Administrator on ECC and NetWeaver Gateway systems. Generate the role and use it or copy the role to appropriate enterprise naming convention, generate, and use.



Note:

On the Quality, Pre-Production, and Production systems, these users have access to the same set of transactions in read only mode.

Table 6-1 Roles on ECC System and transactions

Role Name	Role Description	User	Transactions
ZINV_ECC_PRJ_-BASIS	Innovapptive - Project Role - ECC Basis Authorizations	SAP Basis Administrator	SU01D, SBWP, SM59, SMT1, ST22, SU53, ST-MS_IMPORT, SE37, SE16, SM30, SM31, ST22
ZINV_ECC_PRJ_DEVELOPER	Innovapptive - Project Role - ECC Developer Authorizations	SAP Developer	Developer access key, Developer Debug access SE11, SE12, SE16, SE14, SE38, SE18, SE19, SE93, SM30, SM31, SE41, SE51, SE91, SE37, SE80, SE24, SWDD, SU01D, SU53, SBWP, SWUS, SWELS, SWEL, SW11, SW111, SW114, SW13, SW16, SWIE, SWUE, SWIA , SMARFORMS, SEGW,SE80,SE01, SWI5, SE63, SLXT

Table 6-1 Roles on ECC System and transactions (continued)

Role Name	Role Description	User	Transactions
ZINV_ECC_PRJ_SECURITY	Innovapptive - Project Role - ECC Security Authorizations	SAP Security Administrator	SU01, RSPFPAR, SPRO, PFCG, SUIM, SM30, SE16, ST01, SU53, SU56, SU21, SU03
ZINV_ECC_PRJ_CONFIGURATOR	Innovapptive - Project Role - ECC Configurator Authorizations	SAP Configurator	SPRO, SE11, SE38, SE24, SM36, SM37, SM30, SE37, SBWP, SU53, SU3, SE16, SU01D

Table 6-2 Roles on NetWeaver Gateway System and transactions

Role Name	Role Description	User	Transactions
ZINV_NWG_PRJ_BASIS	Innovapptive - Project Role - Gateway Basis Authorizations	SAP Basis Administrator	RZ11, SM59, SMT1, SE01, ST22, SU53, SU01D, SPRO, STMS*, SM30, SMICM, SICF, STRUST, /IWBEP/*, /IWFND/*, SBGRFC-CONF
ZINV_NWG_PRJ_DEVELOPER	Innovapptive - Project Role - Gateway Developer Authorizations	SAP Developer	Developer access key, Developer Debug access SEGW, SE24, SE37, SE38, SSO2, SICF, /NSBRGFCCONF, /IWBEP/TRACES, /IWFND/TRACES, /IWFND/MAINT_SERVICE, /IWBEP/ERROR_LOG, /IWFND/ERROR_LOG, /IWFND/NOTIF_CLEANUP/IWFND/CACHE_CLEANUP, /IWBEP/TRACES, /

Table 6–2 Roles on NetWeaver Gateway System and transactions (continued)

Role Name	Role Description	User	Transactions
			IWFND/APPS_LOG, / IWBEP/CACHE_ CLEANUP, SBGRFC- MON, SBGRFCCONF, SBGRFCHIST, SBGR- FCPERFMON, SBGR- FCSCHEDMON.
ZINV_NWG_PRJ_SE- CURITY	Innovapptive – Project Role – Gate- way Security	SAP Security Admin- istrator	SU01, RSPFPAR, SPRO, PFCG, SUIM, SM30, SE16, ST01, SU53, SU56, SU21, SU03
ZINV_NWG_PRJ_- CONFIGURATOR	AuthorizationsInno- vapptive – Project Role – Gateway Configurator Autho- rizations	SAP Configurator	/IWBEP/*, /IWFND/ *, SEGW, SE24, SE37, SE38, SSO2, SICF, SE16, SE11, SU01D, SU53, SBGRFCMON, SBGRFCCONF, SB- GRFCHIST, SBGR- FCPERFMON, SBGR- FCSCHEDMON

6.1. Access Required for Configuring SAP BTP

Person who is configuring SAP BTP requires an Administrator access for entire SAP BTP and all mobile services (**HanaMobileAdmin**). The user also requires an Administrator access to SAP Cloud Connector. Cloud Connector allows creation of new users. Share the SAP Cloud Connector credentials, you can create new users. An Administrator user created during the installation must be shared with the SAP BTP Administrator.

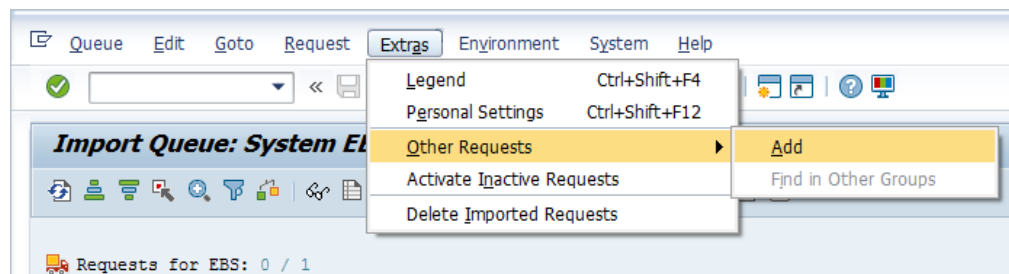
6.2. Import Roles Using Transports

Learn how to import roles into ECC and GW development/sandbox system.

To import roles using Transports:

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 that start with 'K90*' from software deployment package to the **USR/SAP/TRANS/COFILES** path on the SAP ECC & GW system.
 - b. Extract the zip files and copy all data files that start with R90* from the software deployment package to the **USR/SAP/TRANS/DATA** path on the SAP ECC & GW system.
3. Log in to the SAP GW & ECC System where you want to import transports.
4. Navigate to the transaction code **STMS_Import**.
5. Navigate to **Extras, Other Requests, Add**.

Figure 6-1 Import Queue



6. Enter the following transport number in the **Transp. Request** field and confirm by pressing the **ENTER** key to attach transports to the import queue.

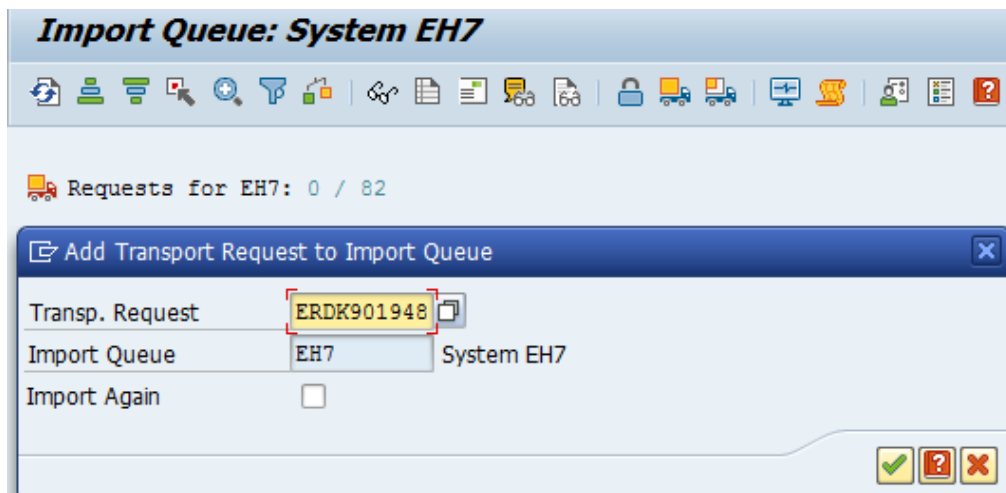
Table 6-3 SAP ECC Transports for Roles

Transport	Description	Dependency
ERDK904636	INNOV:ECC Project Team Roles	None

Table 6-4 SAP NWG Transports for Roles

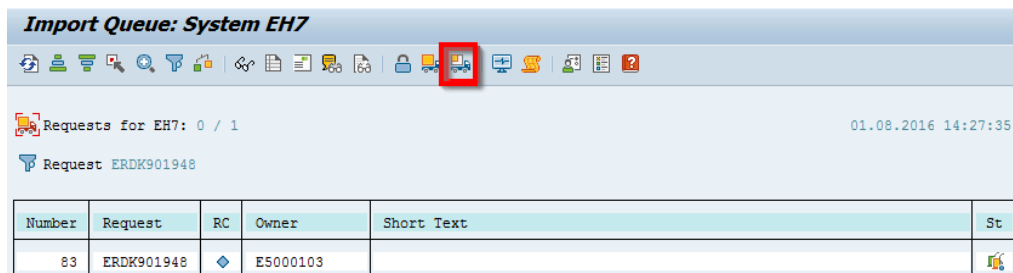
Transport	Description	Dependency
NGTK904332	INNOV:NWG Project Team Roles	None

Figure 6-2 Add Transport Request to Import Queue



7. Click **Yes** to proceed to the next step.
8. Select the transport request that needs to be imported.
9. Click the **Transport** icon.

Figure 6-3 Truck icon



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



Note:

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

7. Configure SAP BTP for Deploying Innovapptive Products

SAP BTP configuration process consists of tasks like installing and configuring cloud connector, validating access, enabling mobile services, and so on.

Table 7-1 Configuring SAP BTP for Deploying Innovapptive Products

Tasks
Check and Implement Prerequisites for Installing SAP Cloud Connector (SCC)
Check and Implement Sizing Recommendation for SCC
Install SAP BTP on you platform • Installation on Microsoft Windows OS • Installation on Linux OS • Installation on Mac OS X
Validate access to SAP BTP (on page 40)
Enable Mobile Services (on page 40)
Access your SAP BTP account based on the region where you are located. Check Re-gions and Hosts Available for the Neo Environment
 Note: From the list of BTP Neo Data Centers, Mobile Services is not available for the China (Shanghai) data center. that provide mobile services.
Complete Initial Setup
Configure Trust entities in the cloud connector
Install a System Certificate for Mutual Authentication
Configure a CA Certificate for Principal Propagation
Import Cloud Connector Root and Intermediate Certificates to Gateway Trust Store (on page 42)
Configure Access Control (on page 42)

7.1. Validate access to SAP BTP

Validate the SAP BTP Access and add members to the team for Administration and Development activities.

To validate access to SAP BTP:

1. Login to SAP BTP.
2. Under **Overview**, click **Account Name**.

Click **New Account** to create tenants such as Dev, QA, and PRD with SAP BTP account.

3. Click on **Tenant** (sub account) to view the **Services** and validate the settings.
Navigate to **Members** tab as shown below.

Figure 7-1 SAP BTP Account Members

Name	ID	Roles	Comment	Actions
Anilkumar Guntuka	S0C	Administrator, Developer, Support User, Application User A...	Anil	👤 ✎ 🗑️ ✉️
fsn avatar	P1	Administrator, Developer		👤 ✎ 🗑️ ✉️
Hari Kamineni	St	Support User	Hari	👤 ✎ 🗑️ ✉️
Nagesh Caparthy	St	Administrator, Developer, Support User, Application User A...	Nagesh	👤 ✎ 🗑️ ✉️
Narasimha Rao Yannabathina	St	Administrator, Developer, Application User Admin, Cloud C...	Narasimha	👤 ✎ 🗑️ ✉️
Prabhukumar Sriarthik	S0	Support User	Sri	👤 ✎ 🗑️ ✉️

4. This tab helps you to add new members to the SAP BTP Tenant. Use any of the predefined roles for the new members that you add.
 - a. [Check Predefined Platform Roles](#)
 - b. [Add Member to your Neo Sub-Account](#)

7.2. Enable Mobile Services

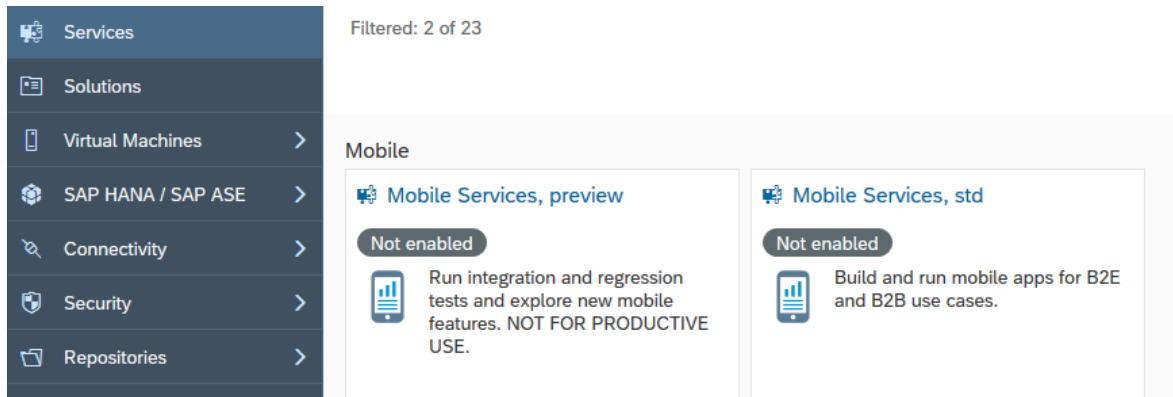
Enable mobile services, if you are logging into SAP BTP for the first time.

To enable Mobile Services:

1. Under **Services**, click the **Mobile Services** option.

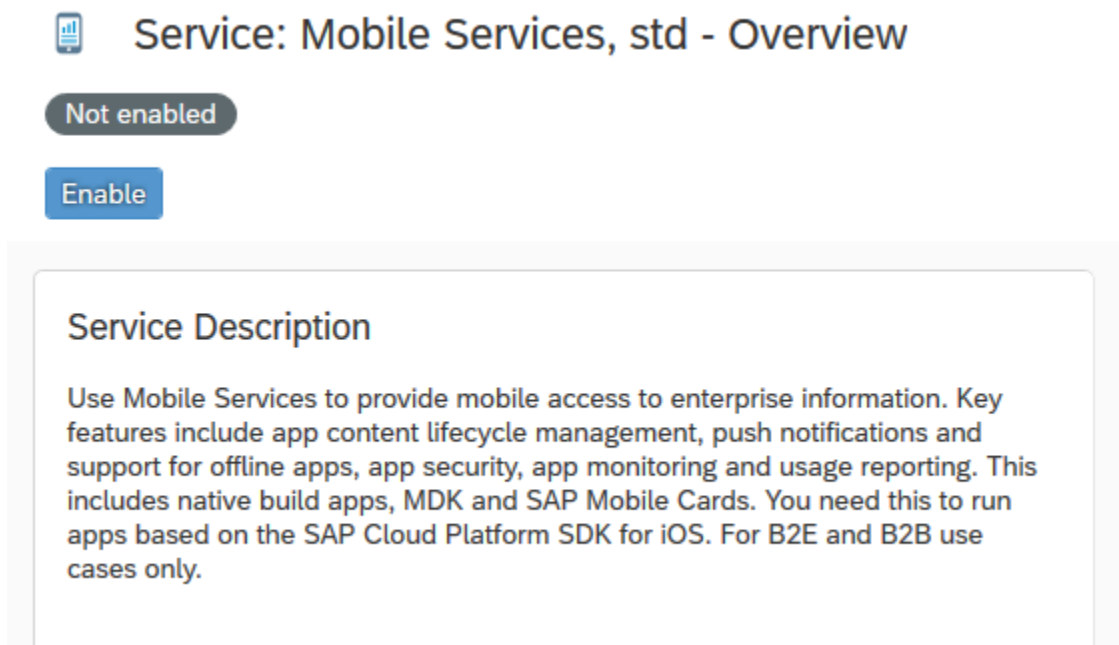
For example, **Mobile Services, std** in the image

Figure 7-2 Services, Mobile Services



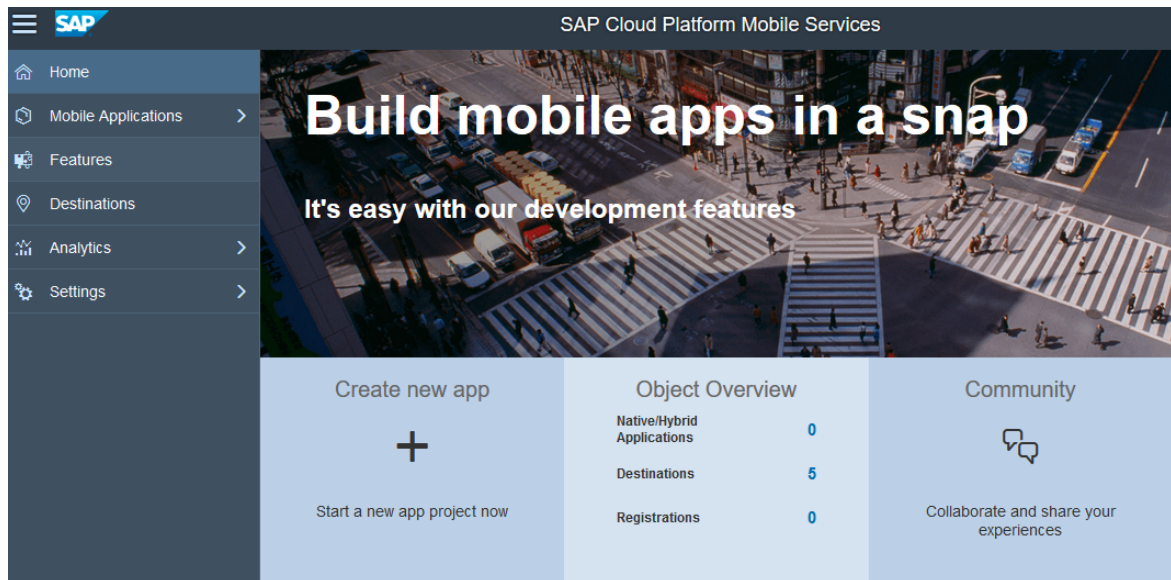
2. Click **Enable**.

Figure 7-3 Mobile Services



3. Click **Go to Service** to access the Mobile Services portal.

Figure 7-4 Mobile Services portal



7.3. Import Cloud Connector Root and Intermediate Certificates to Gateway Trust Store

To import Cloud Connector Certificates to SSL Server Standard:

1. **Transaction code:** STRUST.
2. Open **SSL Server Standard** group and double-click the **certificate** node.
3. Double-click the Owner entry under **Own certificate** section and click **Import Certificate**.
4. Browse for **CA Certificate** and **System Certificate** files and **Import** them.
5. Click **Add to certificate list** to add the certificate to System PSE certificates list.



Note:

Repeat the same process to import Intermediate certificate.

7.4. Configure Access Control

To configure access control:

1. Click **Access Control** and click **Add** to add a new system mapping in HCC.
Edit the existing mapping to support Principal propagation.

Figure 7-5 System Mapping

Edit System Mapping

i Virtual host cannot be edited

Virtual Host:

Virtual Port:

Internal Host: *

Internal Port: *

Protocol:

Principal Type:

Back-end Type: *

SNC Partner Name:

Description:

☐ Check availability of internal host (this may take some time)

2. Add resource to access the ODATA Service.

Figure 7-6 Add Resource

Edit Resource

i Path must not be empty

☒ Enabled

URL Path: *

Access Policy: ☐ Path only (sub-paths are excluded)
☒ Path and all sub-paths

3. Restart the Cloud Connector.