Pre-Install or Pre-Upgrade Configurations Guide 2505

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: *2505*

Release Date: *07 May 2025*

Published Date: *07 May 2025*

Document Version: *1.0*

Primary Author: Innovapptive Inc.

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.
italic	Indicates book titles, emphasis, or place-holder variables for which you supply values.
`monospace`	Indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Related Products

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

Contact Innovapptive

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

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

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

Contents

1. 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

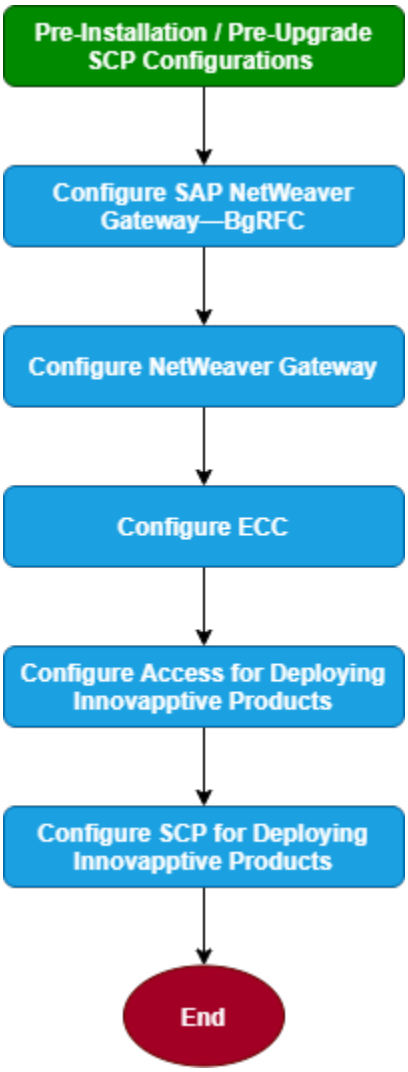


Table 2-1 Tasks for SAP BTP Configurations before Installing Innovapptive Products

Task	Reference to section
Configure SAP NetWeaver Gateway—BgRFC	Configure SAP NetWeaver Gateway—BgRFC *(on page 9)*
Configure NetWeaver Gateway	Configure NetWeaver Gateway *(on page 9)*
Configure ECC	Configure ECC *(on page 26)*
Configure Access for Deploying Innovapptive Products	Configure Access for Deploying Innovapptive Products *(on page 27)*
Configure SAP BTP for Deploying Innovapptive Products	Configure SAP BTP for Deploying Innovapptive Products *(on page 30)*

3. Configure NetWeaver Gateway

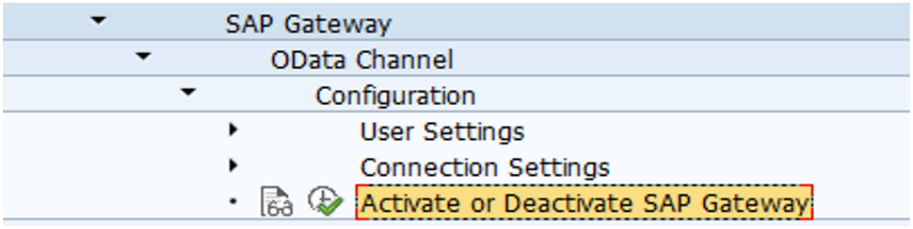
Configure SAP NetWeaver Gateway to define how some settings must work with your existing SAP ECC Business Suite system or Embedded ECC or S4 System.

3.1. Activate SAP NetWeaver Gateway for New System

Note:
(Ignore if gateway is already activated)

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.

3.2. Configure SAP NetWeaver Gateway—BgRFC

This section helps you configure SAP NetWeaver Gateway—BgRFC

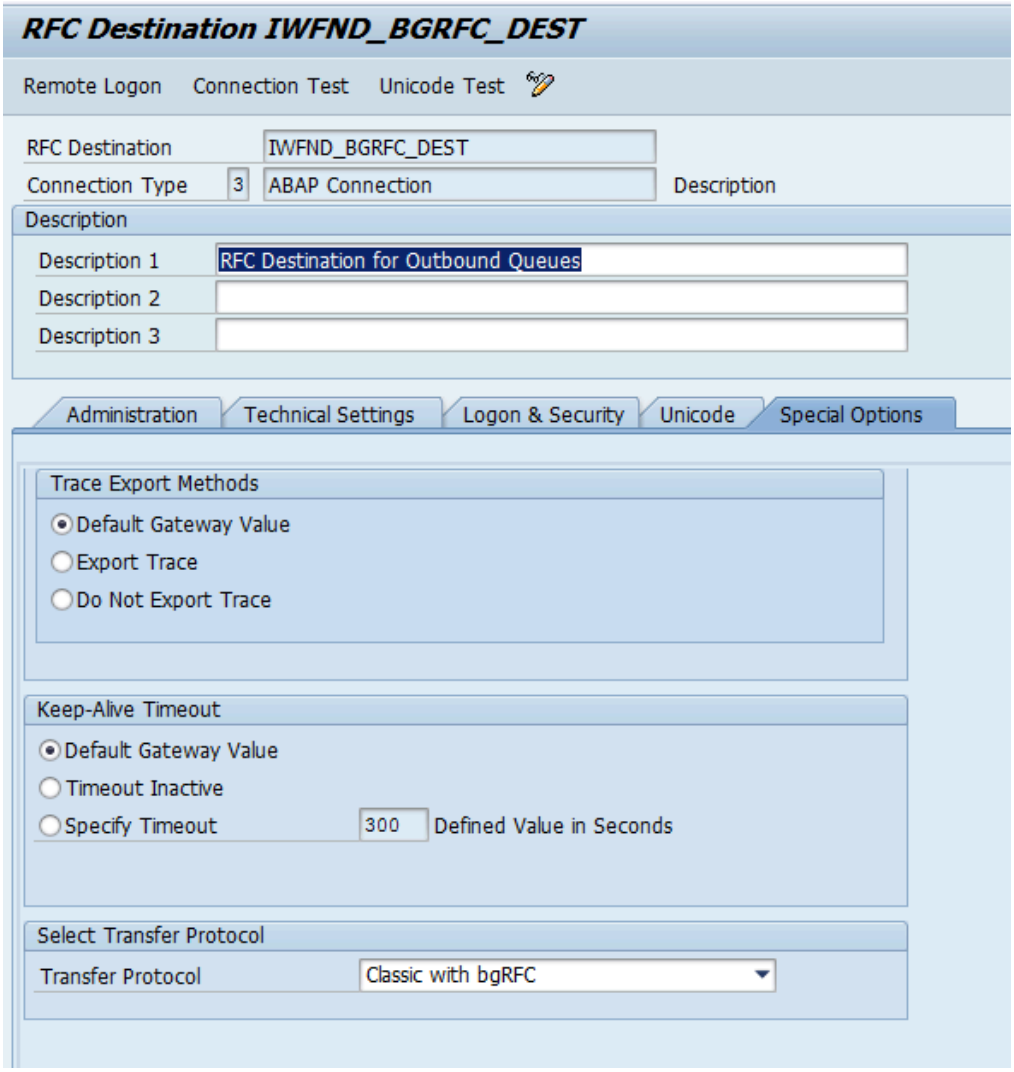
3.2.1. Create BgRFC Destination for Outbound Queues

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

To create BgRFC Destination for the outbound queue:

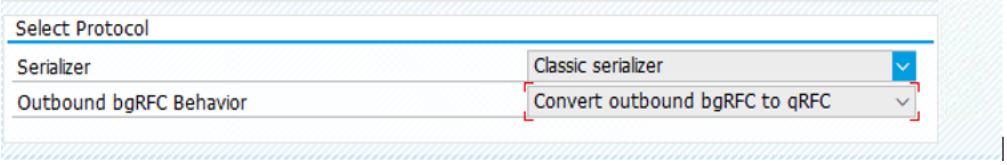
1. In transaction **SPRO**, open SAP Reference IMG.
2. Navigate to **SAP NetWeaver, SAP Gateway, OData Channel, Configuration, Connection Settings, SAP NetWeaver Gateway to Consumer, Create RFC Destination for Outbound Queues**.
3. Click **Activity**.
4. Click **Create**.
5. In the **RFC Destination**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



For new SAP versions, find **Classic with BgRFC**, select the **Convert outbound bgRFC qRFC**.

Figure 3-2 RFC Destination - Special Options tab



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

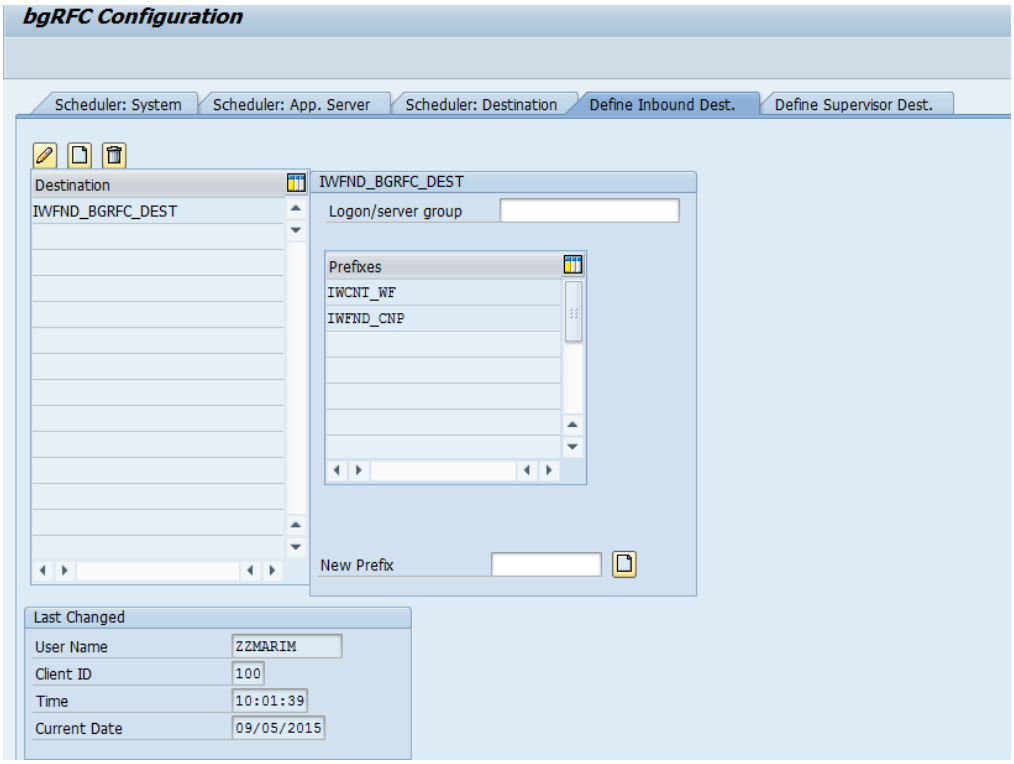
3.2.2. Register BgRFC Destination for Outbound Queue

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.

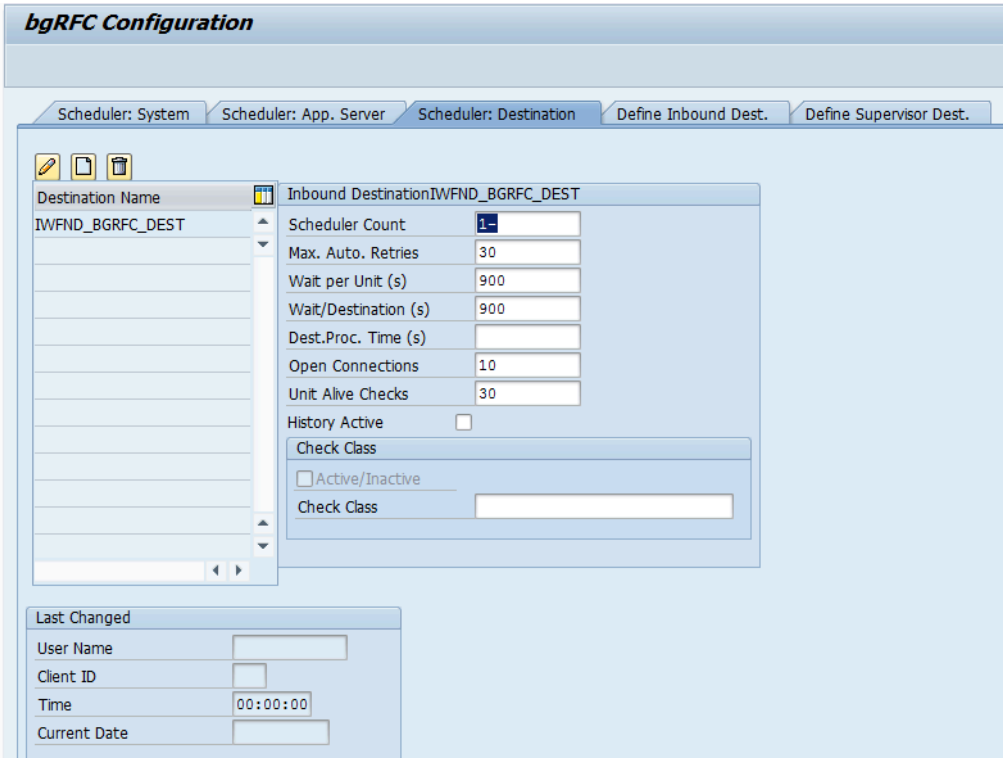
Figure 3-3 Define Inbound Destination



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.

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

Figure 3-4 Scheduler: Destination tab



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

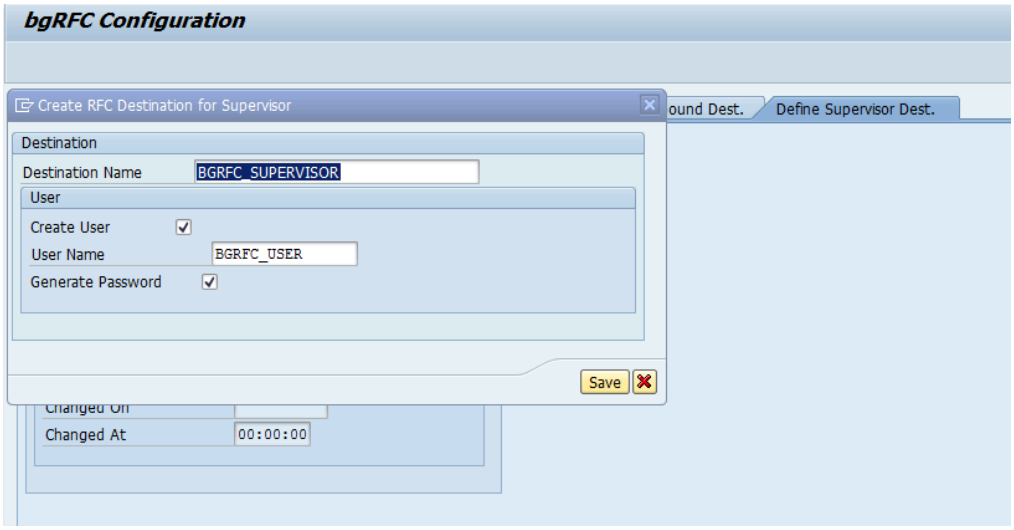
3.2.3. Create BgRFC Destination for Supervisor

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:

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

Figure 3-5 Create RFC Destination for Supervisor



5. In the **Destination Name** field, enter **BGRFC_SUPERVISOR**.
6. In the **User Name** field, enter a username. 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**.

3.3. 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:

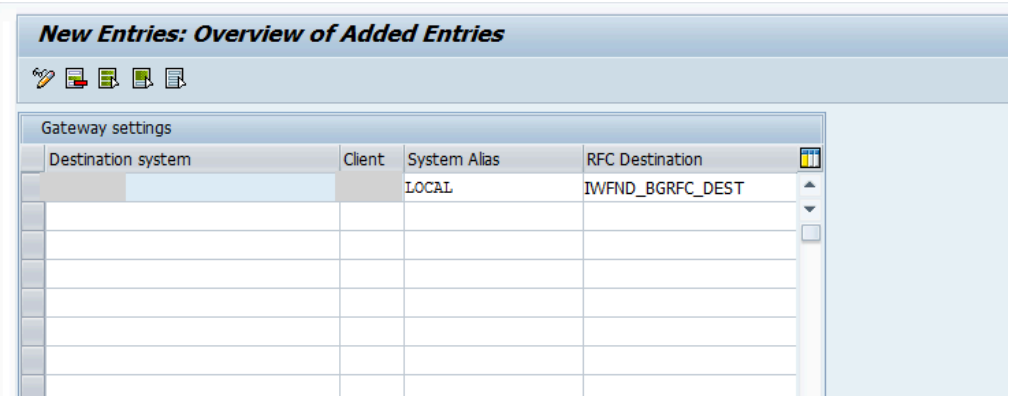
Before defining the connection settings, do the following:

- 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 3-6 Connection Settings: New Entries

4. Save your settings.

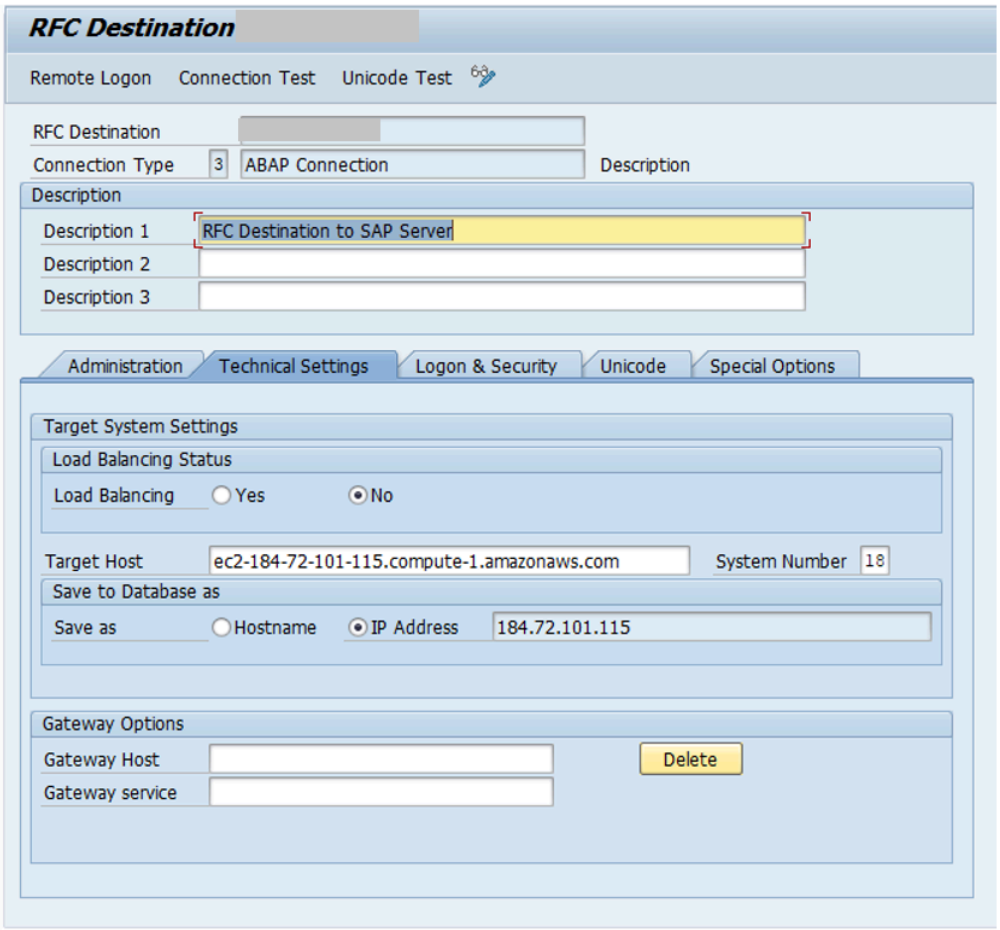
3.4. Establish trust between Gateway and ECC

Learn how to establish trust between Gateway and ECC. This is applicable only for 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 3-7 RFC Destination



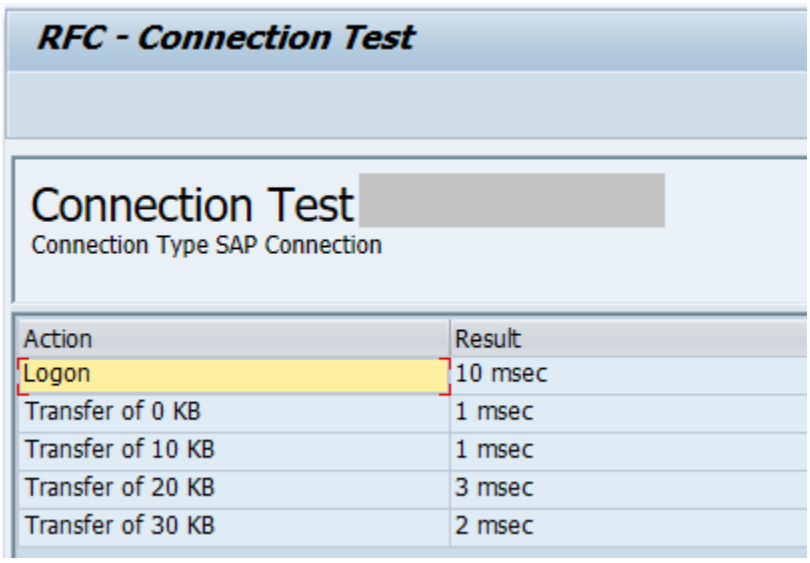
3. Enter **3** in the **Connection Type** field.
4. Enter description in the **Description 1** field. For example, **Connection to Backend System**.
5. Save your settings.
6. On the **Technical Settings** tab, select the option as per your system settings.
7. Enter the name of the SAP NetWeaver Gateway 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.

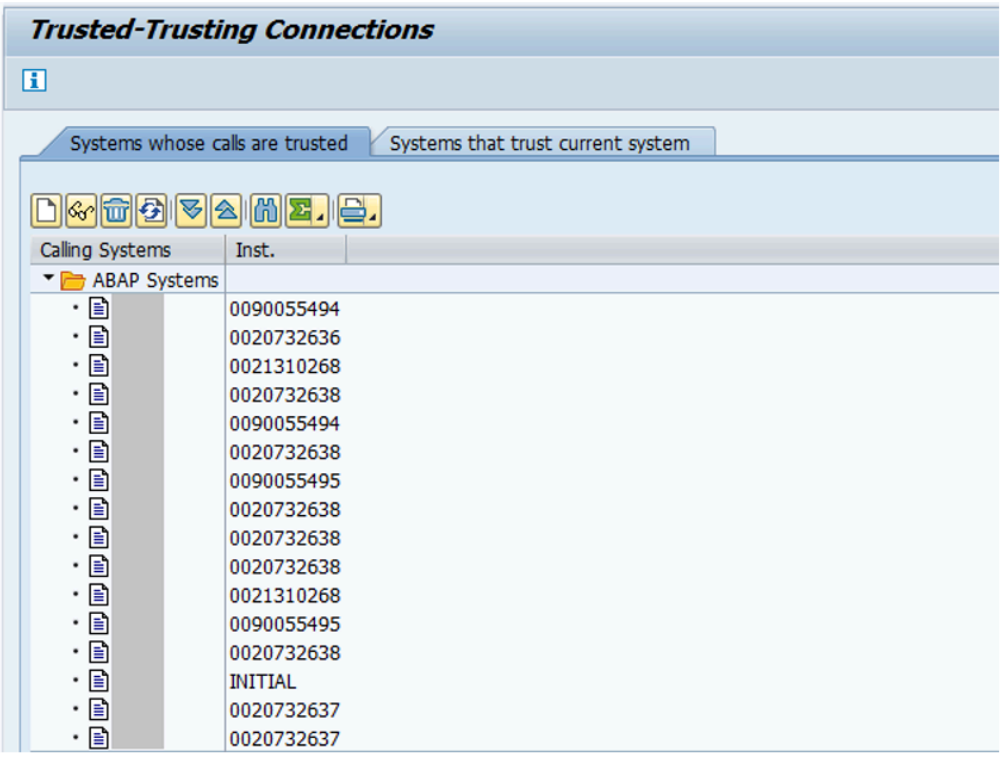
18. Click **Connection Test**.

Figure 3-8 Connection Test



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

Figure 3-9 Trusted Calling Systems



3.5. Create the SAP System Alias for Applications

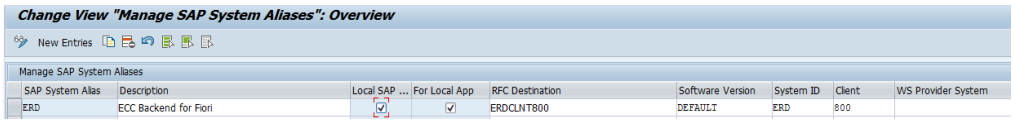
To create the SAP system Alias for applications:

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 3-10 Manage SAP System Aliases

5. Save your settings.

3.6. 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.

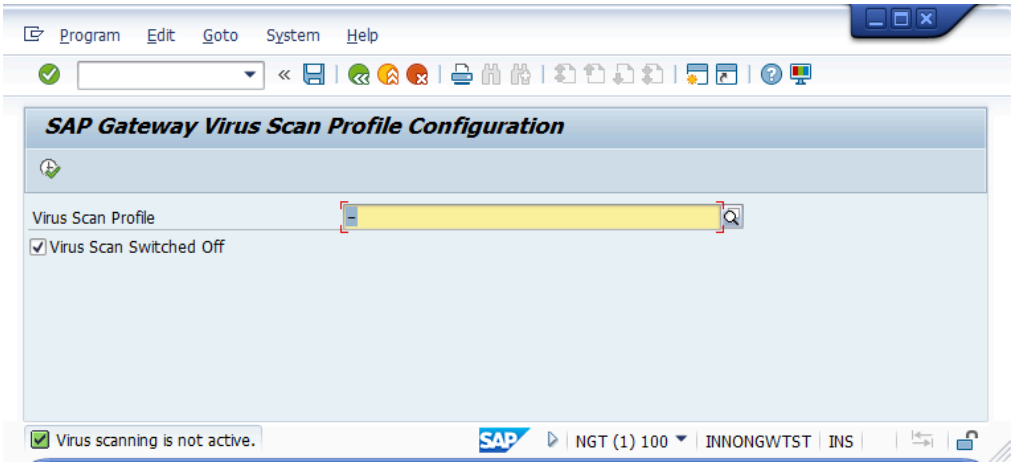
Note:
The Virus Scan must be enabled in Gateway only if the virus profile is defined.

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 3-11 Gateway Virus Scan Profile



3.7. 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 3-1 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 3-12 SICF: /sap/opu

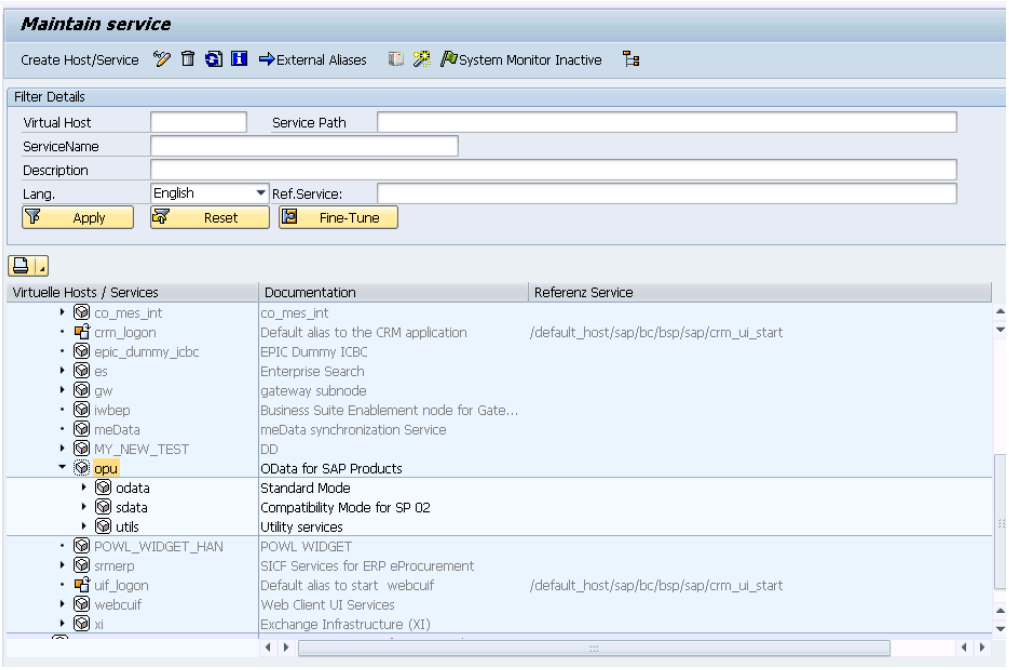
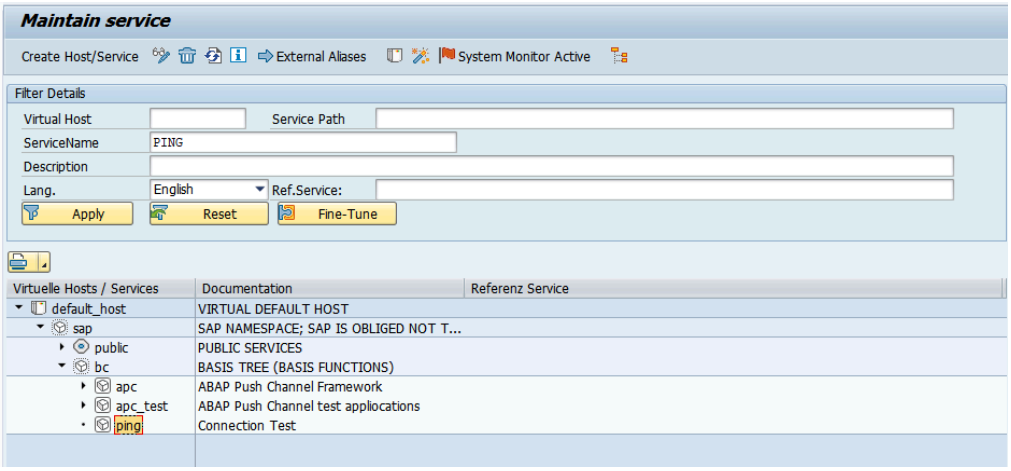


Figure 3-13 SICF: /sap/bc/ping



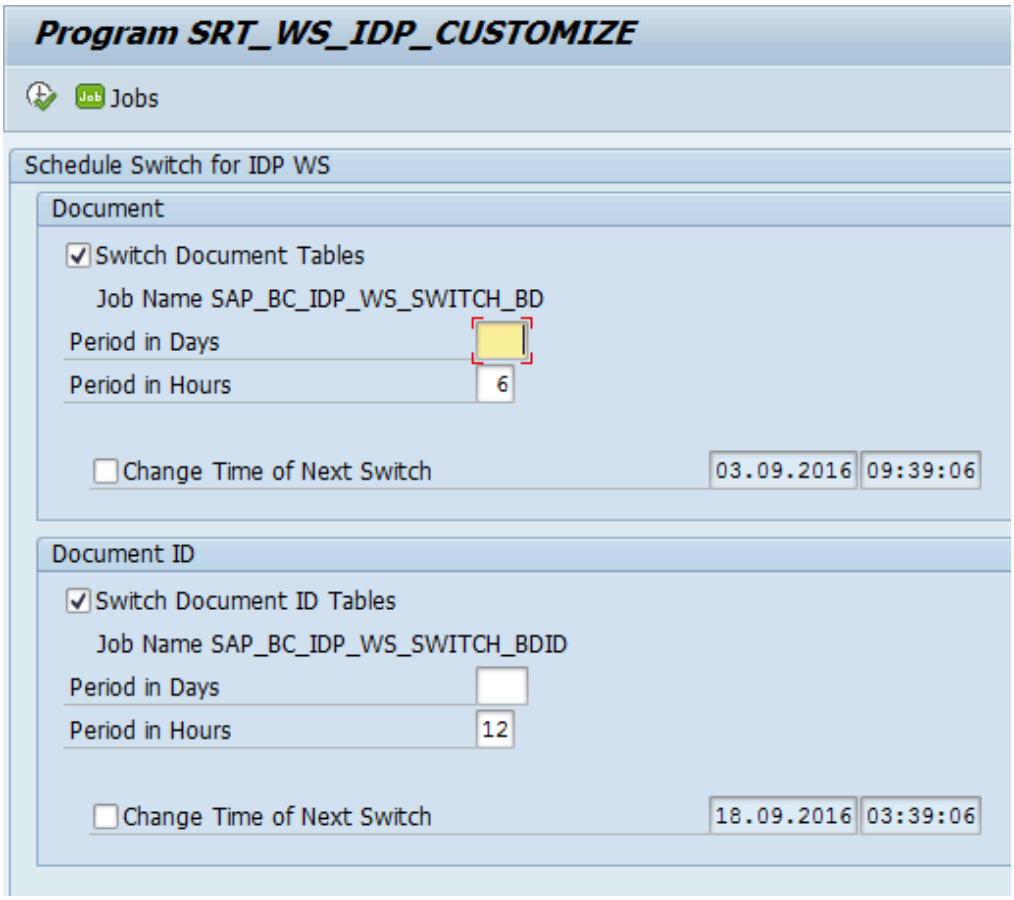
3.8. Define Settings for Idempotent Services

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 3-14 Idempotent Services Settings



6. Click **Continue**.

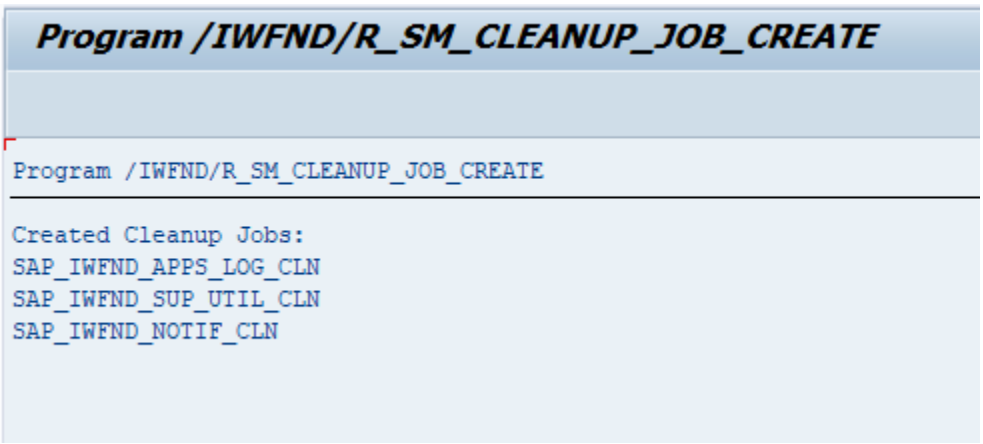
3.9. Create Periodical Tasks for Gateway

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 3-15 Gateway Cleanup tasks

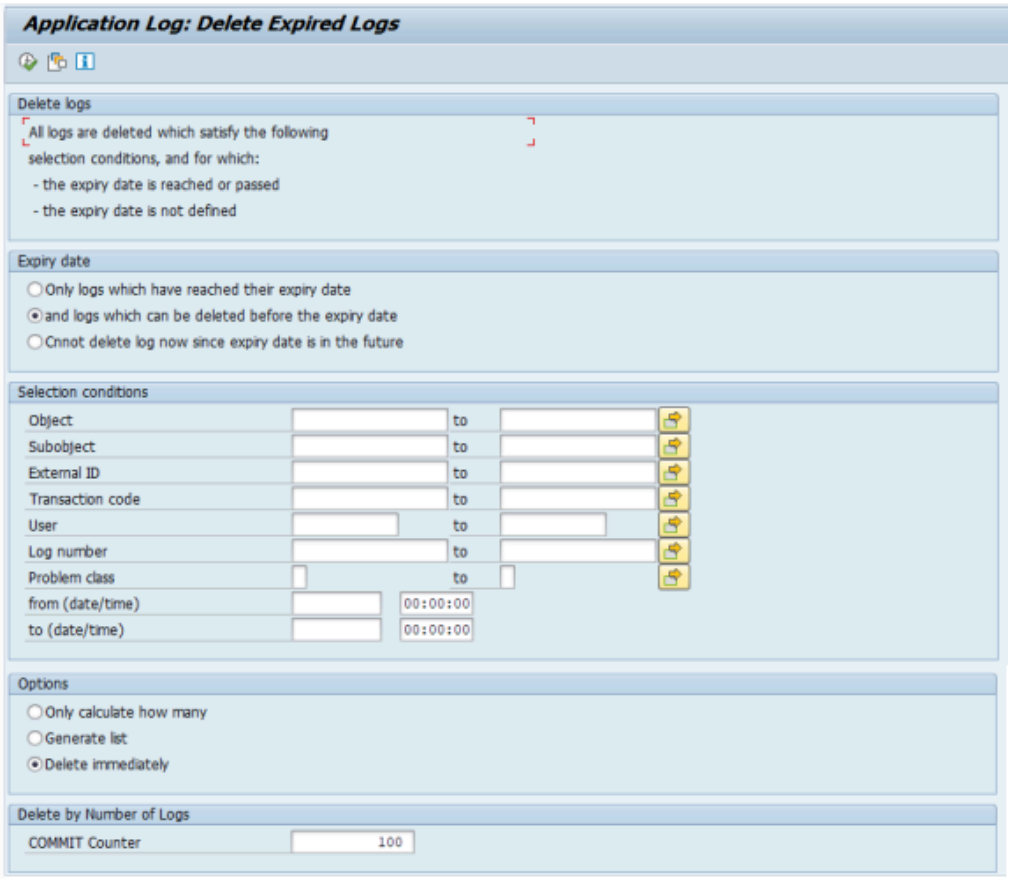


3.10. Clear Application Log Entries

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 3-16 Clear Log Entries Criteria



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**.

3.11. 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 3-17 Clear Log Entries Criteria

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. 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**.

5. 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 5-1 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, STMS_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, SWI1, SWI11, SWI14, SWI3, SW16, SWIE, SWUE, SWIA , SMARFORMS, SEGW,SE80,SE01, SWI5, SE63, SLXT

Table 5-1 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 5-2 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/*, SBGRFCCONF
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, /IWFND/APPS_LOG, /

Table 5-2 Roles on NetWeaver Gateway System and transactions (continued)

Role Name	Role Description	User	Transactions
			IWBEP/CACHE_-CLEANUP, SBGRFC-MON, SBGRFCCONF, SBGRFCHIST, SBGR-FCPERFMON, SBGR-FCSCHEDMON.
ZINV_NWG_PRJ_SE-CURITY	Innovapptive - Project Role - Gate-way Security	SAP Security Adminis-trator	SU01, RSPFPAR, SPRO, PFCG, SUIM, SM30, SE16, ST01, SU53, SU56, SU21, SU03
ZINV_NWG_PRJ_-CONFIGURATOR	AuthorizationsInno-vapptive - Project Role - Gateway Con-figurator Authoriza-tions	SAP Configurator	/IWBEP/*, /IWFND/*, SEGW, SE24, SE37, SE38, SSO2, SICF, SE16, SE11, SU01D, SU53, SB-GRFCMON, SBGRFC-CONF, SBGRFCHIST, SBGRFCPERFMON, SB-GRFCSCHEDMON

5.1. 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 BTP. 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. 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 6-1 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 31)*
Enable Mobile Services *(on page 31)*
Access your SAP BTP account based on the region where you are located. Check Regions 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 33)*
Configure Access Control *(on page 33)*

6.1. Validate access to SAP BTP

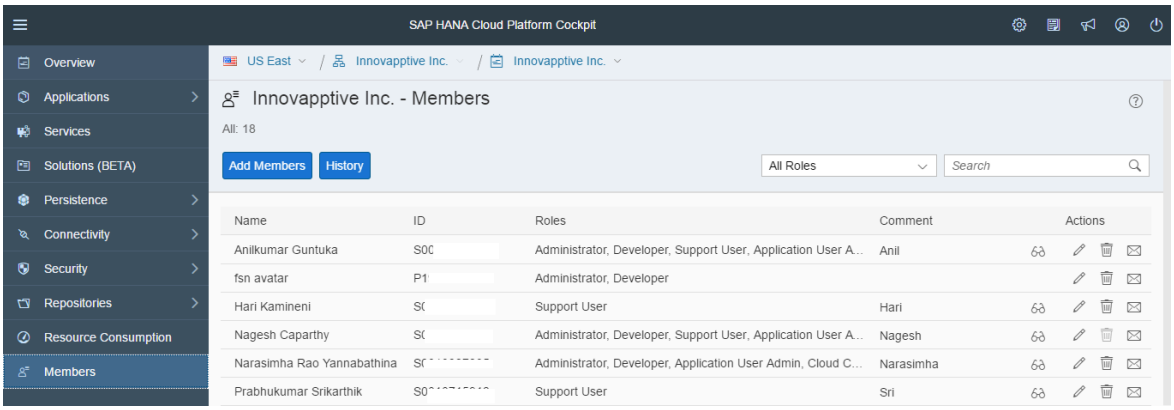
Validate the SAP BTP Access and add members to the team for Administration and Development activities.

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 6-1 SAP BTP Account Members



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

6.2. Enable Mobile Services

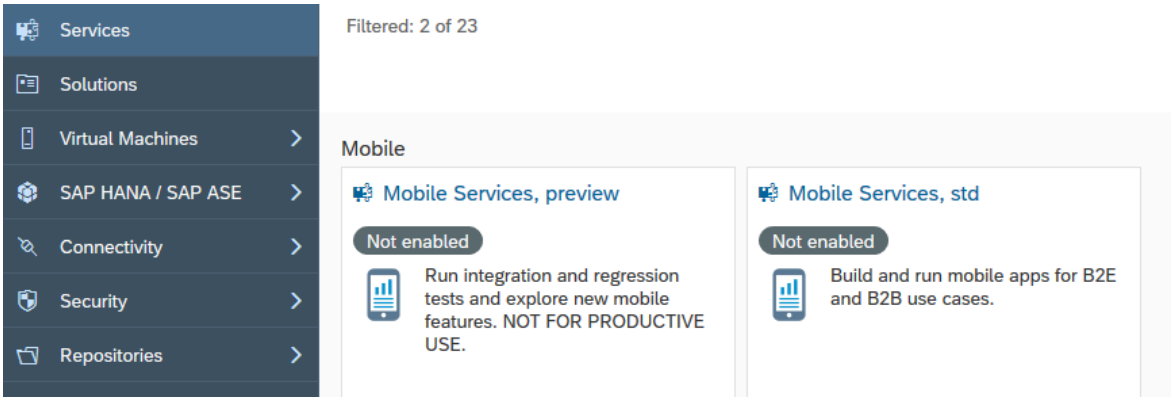
Enable mobile services, if you are logging into SAP BTP for the first time.

To enable Mobile Services:

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

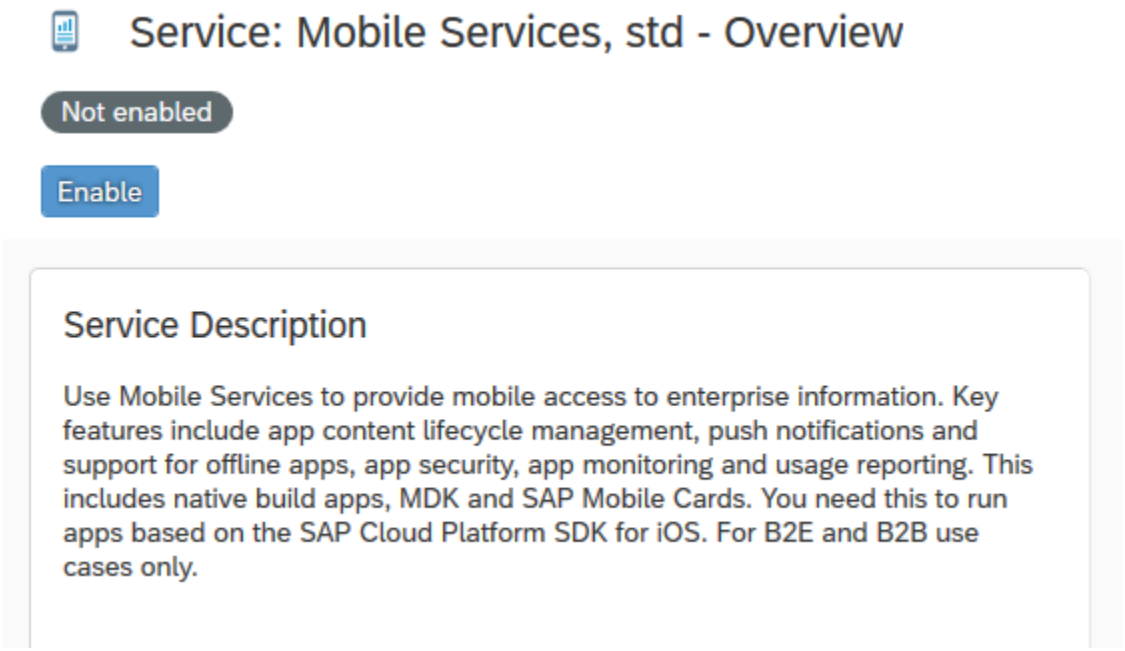
   For example, **Mobile Services, std** in the image

   Figure 6-2 Services, Mobile Services



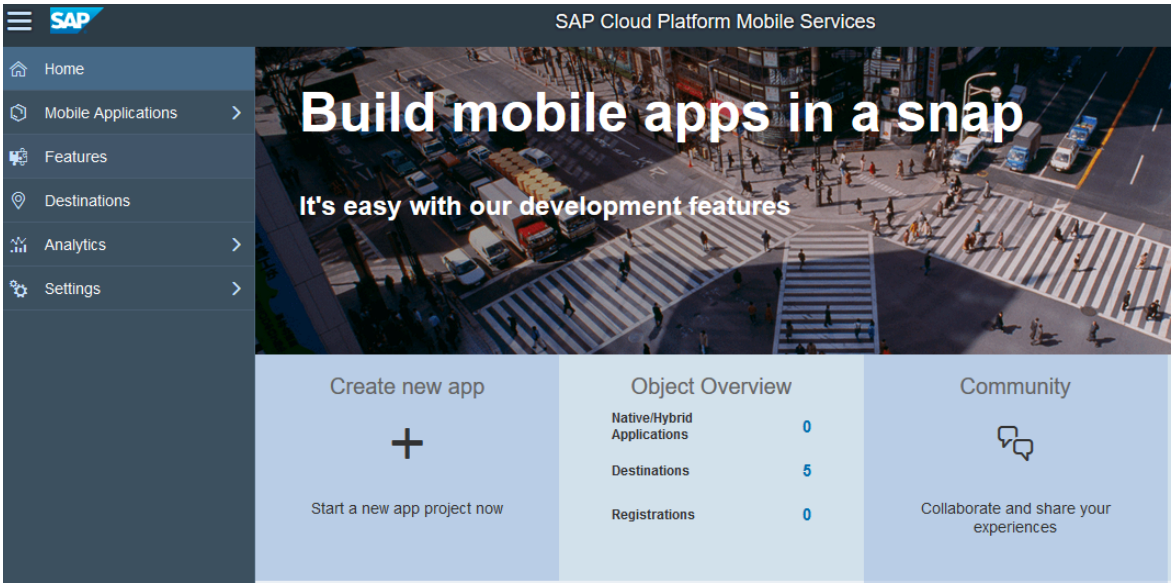
2. Click **Enable**.

   Figure 6-3 Mobile Services



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

Figure 6-4 Mobile Services portal



6.3. 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.

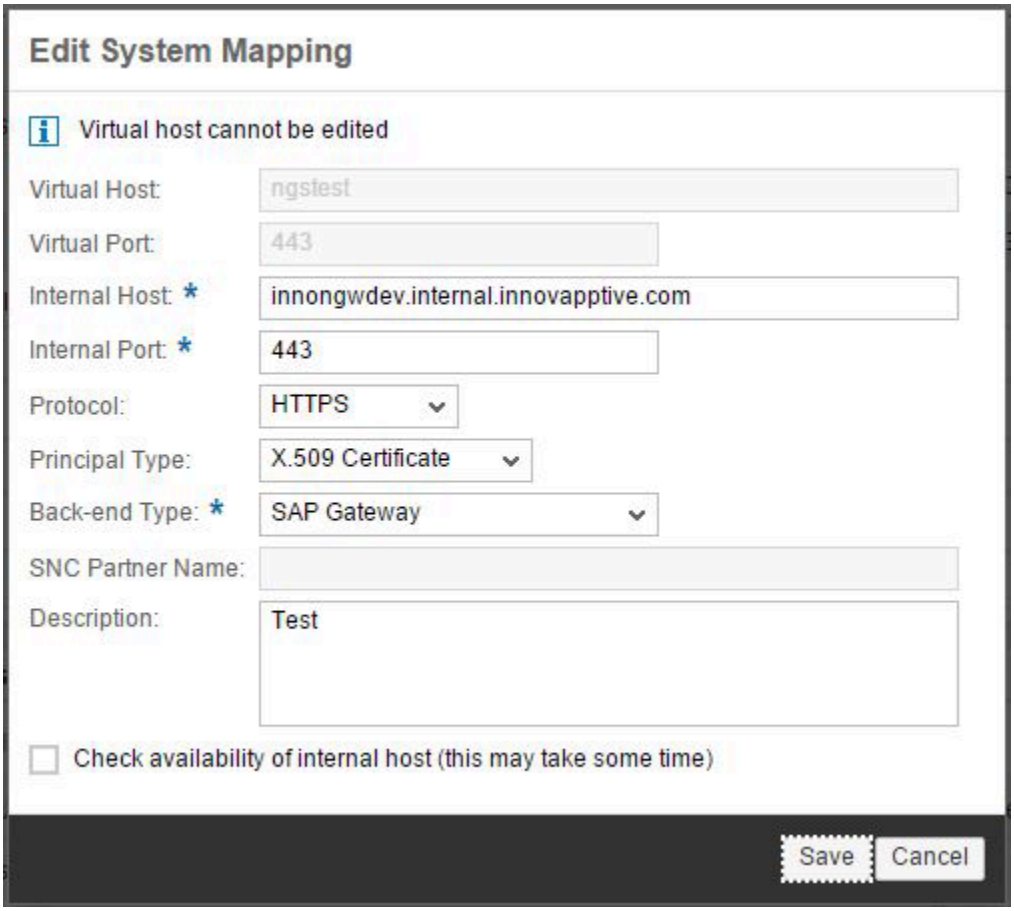
> **Note:**
> Repeat the same process to import Intermediate certificate.

6.4. Configure Access Control

To configure access control:

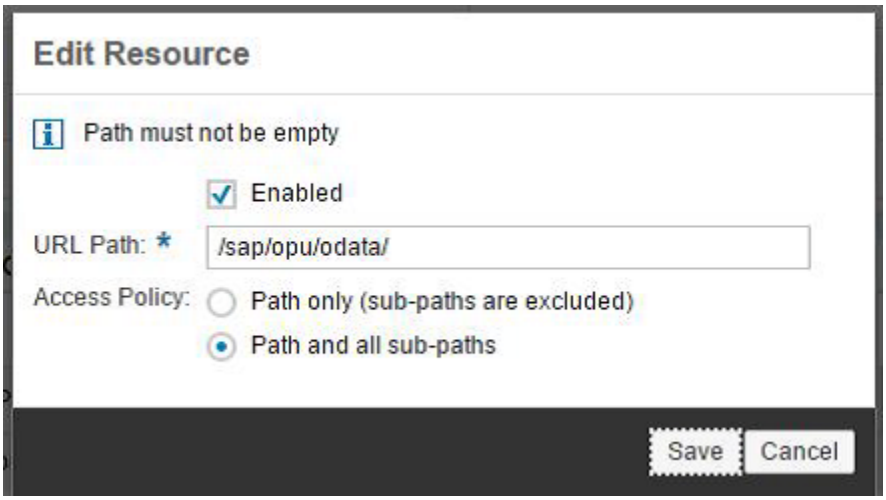
1. Click **Access Control** and click **Add** to add a new system mapping in HCC.
   Edit the existing mapping to support Principal propagation.

Figure 6-5 System Mapping



2. Add resource to access the ODATA Service.

Figure 6-6 Add Resource



3. Restart the Cloud Connector.