Pre-Install or Pre-Upgrade Configurations Guide 2009

Connected Worker Solutions

Title and Copyright

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

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

Product Version: *2009*

Document Version: *1.0*

Published Date: *19 November 2020*

Primary Author: Innovapptive Inc.

Preface

Understand audience and conventions followed in this document.

Audience

This guide is for technical configurators who do e 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 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. Pre-Install or Pre-Upgrade Configurations for Innovapptive Products

This guide contains instructions for pre-install or pre-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 before Installing Innovapptive Products *(on page 10)* for configuration instructions.
- If you are using SMP, check SMP Configurations before Installing Innovapptive Products *(on page 73)* 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 before you install the following Innovapptive products:

Table 1-1 Innovapptive Products

Product	Version (Release)
mAssetTag	6.1.0
mInventory	6.1.0
mServiceOrder	6.1.0
mShop	6.1.0
mWorklist	5.1.0
mWorkOrder	7.0.0
RACE Dynamic Forms	6.1.0
mWorkOrder	7.1.0
mAssetTag	7.2.0

Table 1-1 Innovapptive Products (continued)

Product	Version (Release)
mWorkOrder	7.2.0
mInventory	7.2.0
mAssetTag	7.3.0
mWorkOrder	7.3.0
mInventory	7.3.0
mAssetTag	7.4.0
mInventory	7.4.0
mWorkOrder	7.4.0
RACE Dynamic Forms	7.4.0
mAssetTag	2003
mInventory	2003
mWorkOrder	2003
mAssetTag	2006
mInventory	2006
mWorkOrder	2006
mAssetTag	2009
mInventory	2009
mWorkOrder	2009

2. SCP Configurations before Installing Innovapptive Products

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

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

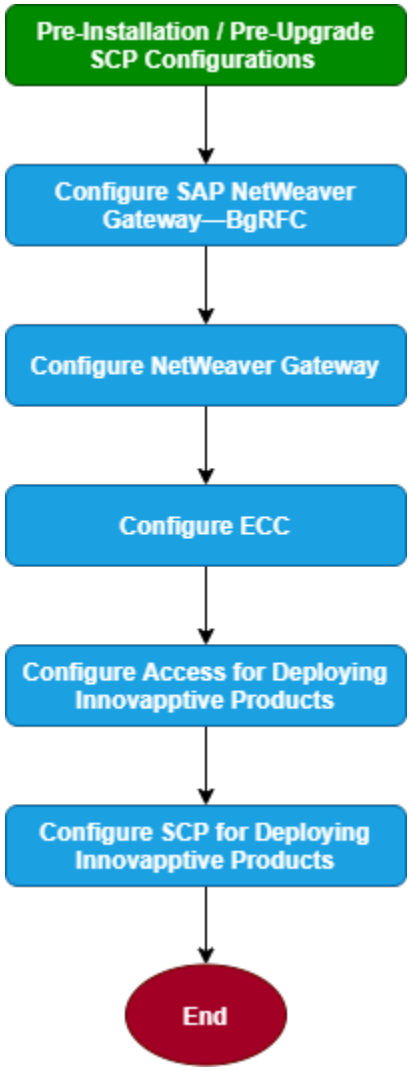


Table 2-1 Tasks for SCP Configurations before Instllaing Innovapptive Products

Task	Reference to section
Configure SAP NetWeaver Gateway—BgRFC	Configure SAP NetWeaver Gateway—BgRFC *(on page 11)*

Table 2-1 Tasks for SCP Configurations before Instllaing Innovapptive Products (continued)

Task	Reference to section
Configure NetWeaver Gateway	Configure NetWeaver Gateway *(on page 16)*
Configure ECC	Configure ECC *(on page 31)*
Configure Access for Deploying Innovapptive Products	Configure Access for Deploying Innovapptive Products *(on page 32)*
Configure SCP for Deploying Innovapptive Products	Configur SCP for Deploying Innovapptive Products *(on page 37)* • Validate access to SCP *(on page 38)* • Enable Mobile Services *(on page 41)* • Install and Configure Cloud Connector *(on page 43)* • Establish trust between SCP, Cloud Connector and SAP Gateway *(on page 53)*

2.1. Configure SAP NetWeaver Gateway—BgRFC

This section helps you configure SAP NetWeaver Gateway—BgRFC

- Before you Configure SAP NetWeaver Gateway - BgRFC *(on page 11)*
- Create BgRFC Destination for Outbound Queues *(on page 12)*
- Register BgRFC Destination for Outbound Queue *(on page 13)*
- Create BgRFC Destination for Supervisor *(on page 15)*

2.1.1. 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, SMP/SCPms).
- SAP NetWeaver Gateway 7.4 and above with SAP_GWFND component (SP 10 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.

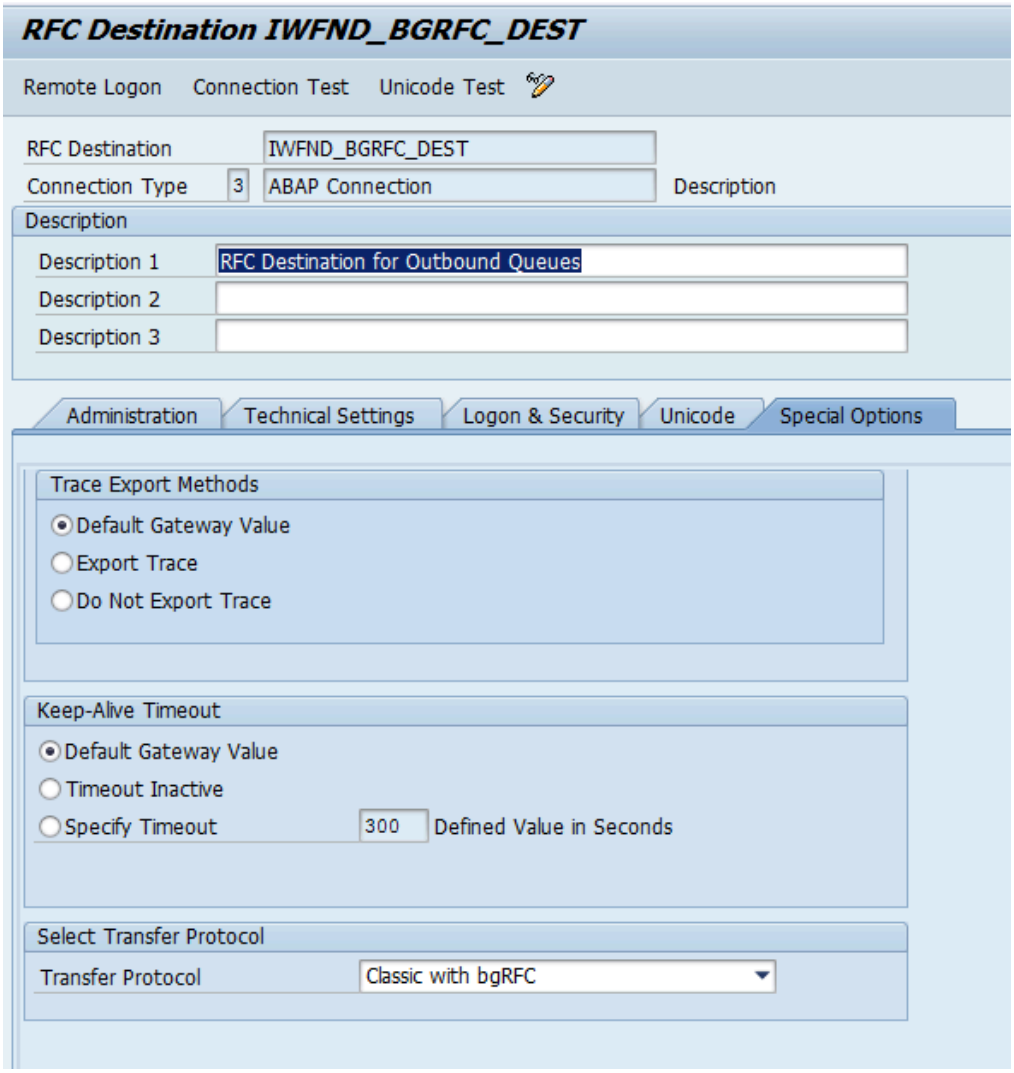
2.1.2. Create BgRFC Destination for Outbound Queues

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. For example **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**.

Figure 2-2 RFC Destination - Special Options tab



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

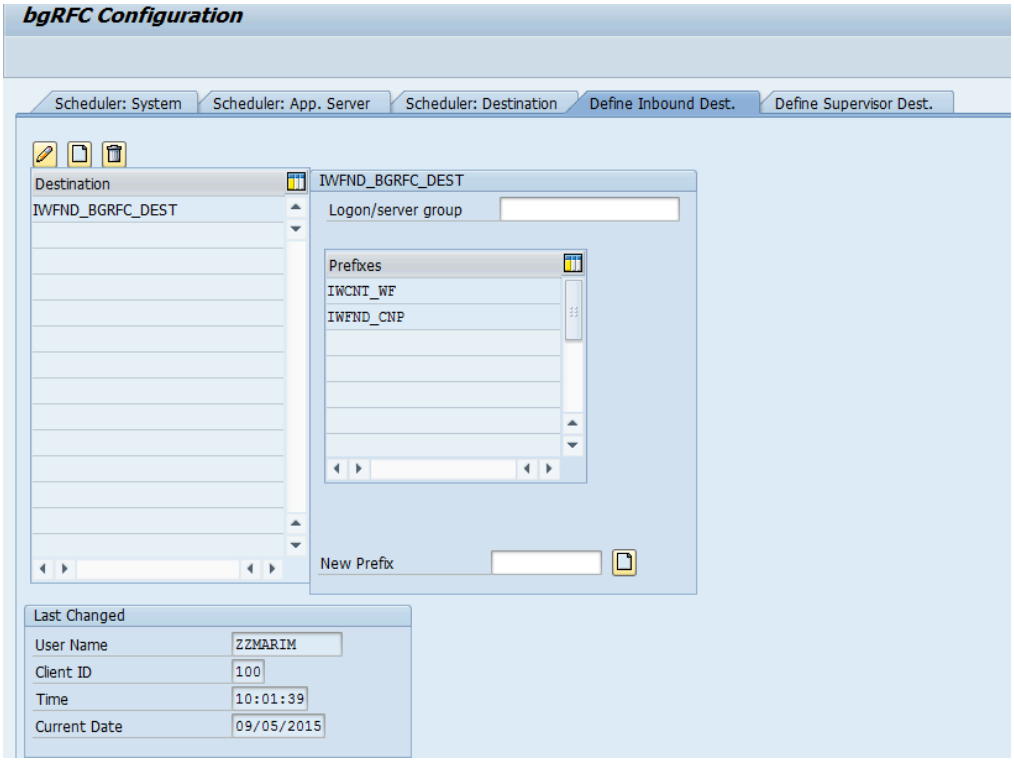
2.1.3. Register BgRFC Destination for Outbound Queue

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.

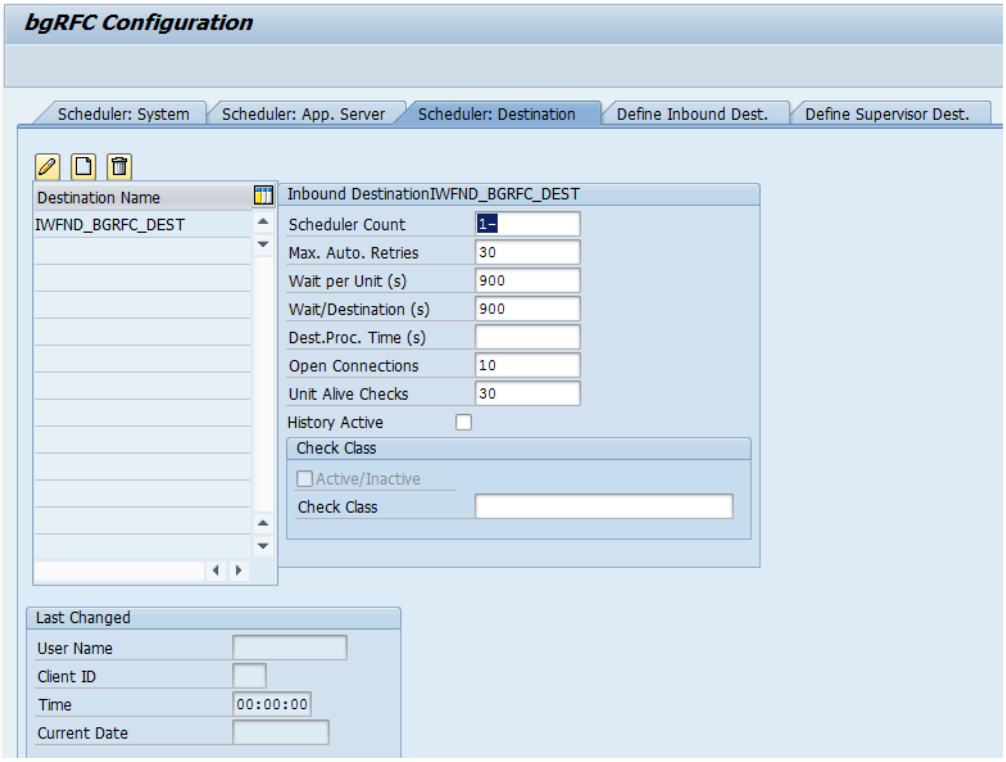
Figure 2-3 Define Inbound Destination



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 2-4 Scheduler: Destination tab



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

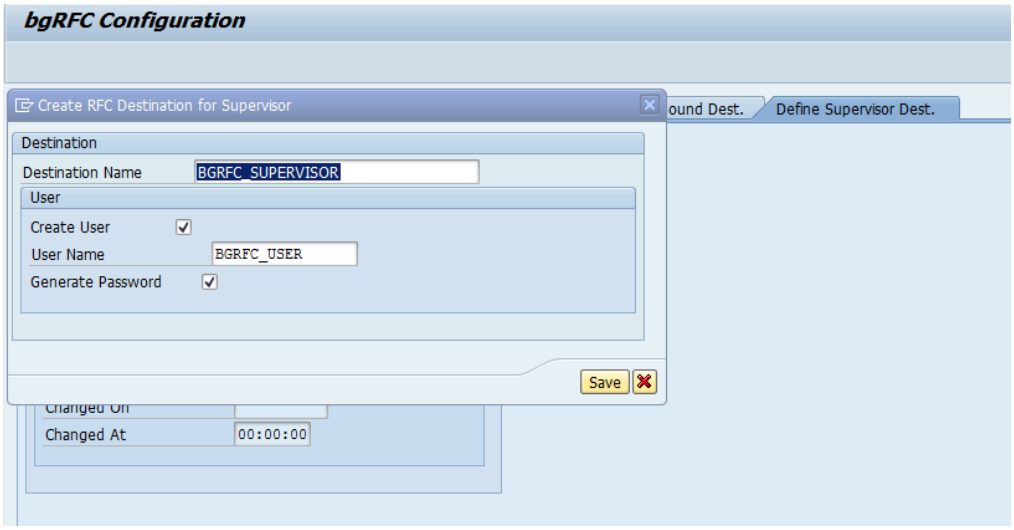
2.1.4. Create BgRFC Destination for Supervisor

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:

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 2-5 Create RFC Destination for Supervisor



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**.

2.2. 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**
  - SAP ECC Business Suite is installed and connected to the mobile infrastructure (NetWeaver Gateway, SMP/SCPms).
  - SAP NetWeaver Gateway 7.4 and above with SAP_GWFND component (SP 10 and above) and SAP_UI component (SP 13 and above).
- **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.
- SMP/SCPms host and port details for creating RFC.
- SMP push user credentials.

- **Assumptions**

  Port number for HTTP = 8000 and HTTPS = 8080.

2.2.1. 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 SP08.

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

2.2.1.1. System Requirements

Hardware

Table 2-2 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 2-3 Software Prerequisites for NetWeaver Gateway

Requirement	Specification
SAP NetWeaver Stack	Apply the latest kernel patch for the SAP NetWeaver version.
	Core Component

Table 2-3 Software Prerequisites for NetWeaver Gateway (continued)

Requirement	Specification
	• SAP NetWeaver 7.40 SPS08 • SAP NetWeaver Gateway Foundation SAP_GWFND SP 10 **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.

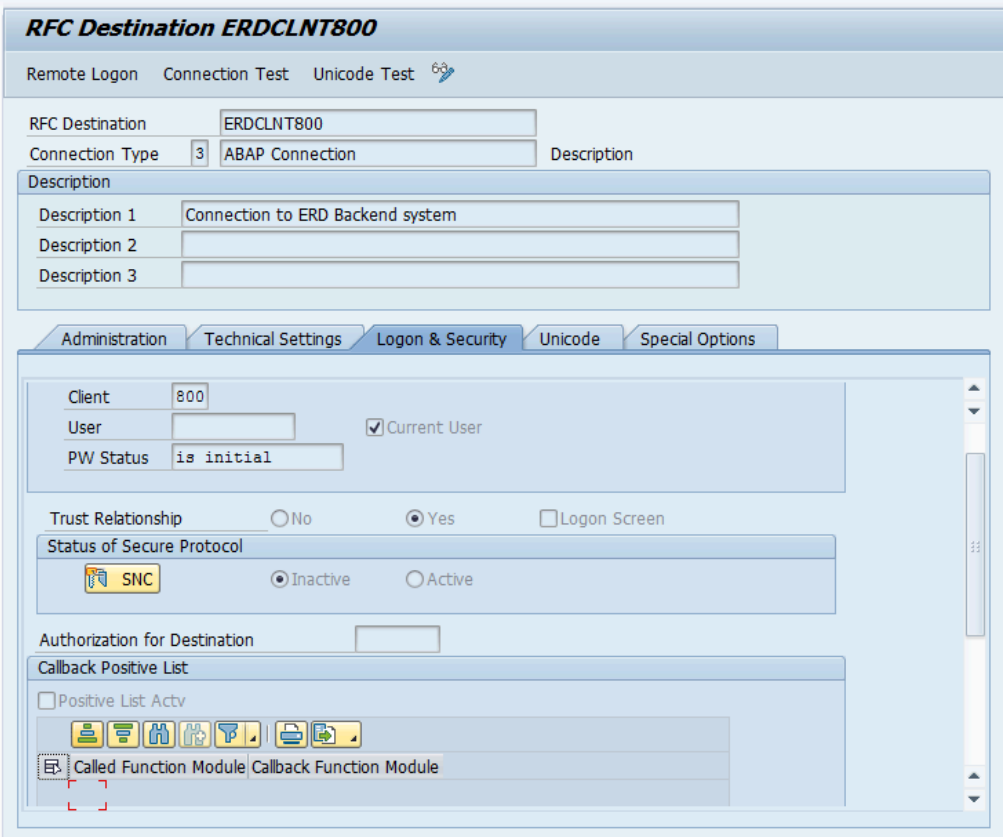
2.2.2. Establish trust between Gateway and ECC

Learn how to establish trust between Gateway and ECC.

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 2-6 RFC Destination

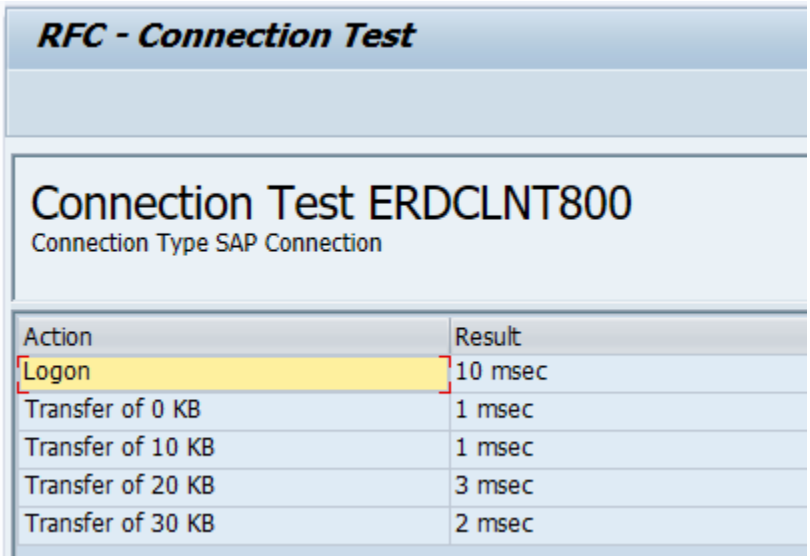


3. Enter **3** in the **Connection Type** field.
4. Enter description in the **Description 1** field. For example, **Connection to Backend System**.
5. Save your settings.
6. On the **Technical Settings** tab, select the option as per your system settings.
7. Enter the name of the SAP NetWeaver Gateway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

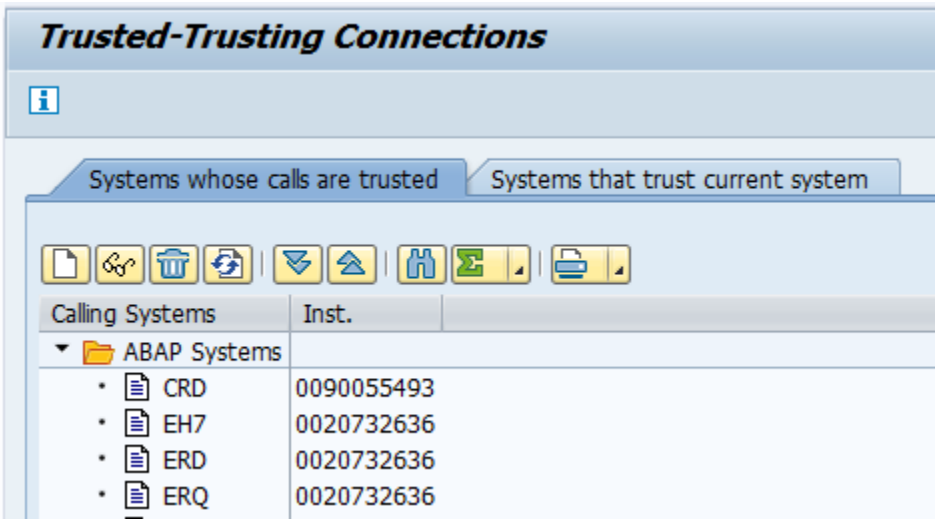
13. Save your settings.
14. Navigate to the **RFC** that you created in the previous step.
15. Select the current user on the **Logon & Security** tab.
16. Click **Yes**.
17. Save your settings.
18. Click **Connection Test**.

Figure 2-7 Connection Test



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

Figure 2-8 Trusted Calling Systems



2.2.3. 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:

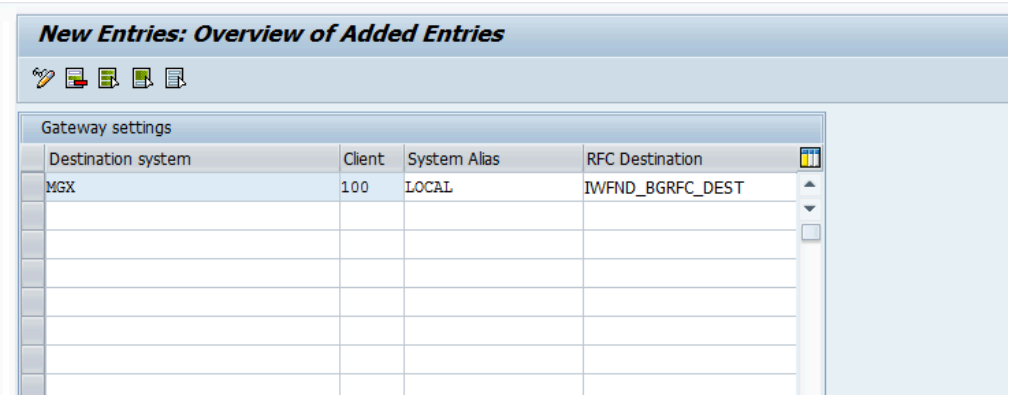
Before defining the connection settings, do the following:

- 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:** Host name of SAP NetWeaver Gateway.
    - **Client:** Client ID of the host of SAP NetWeaver Gateway. The client ID, you specify, must exist in the system.
    - **System Alias:** Unique name for the host of SAP NetWeaver Gateway.
    - **RFC Destination:** Name of the RFC destination to the host of SAP NetWeaver Gateway.

    Figure 2-9 Connection Settings: New Entries

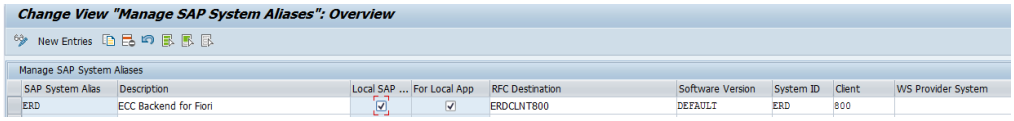
4. Save your settings.

2.2.4. 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.
    - **Description**: Descriptive text for the system alias.
    - **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.
    - Software Version: DEFAULT.
    - System ID: Name of the SAP target system.
    - Client: Target client.

    Figure 2-10 Manage SAP System Aliases



5. Save your settings.

2.2.5. 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.

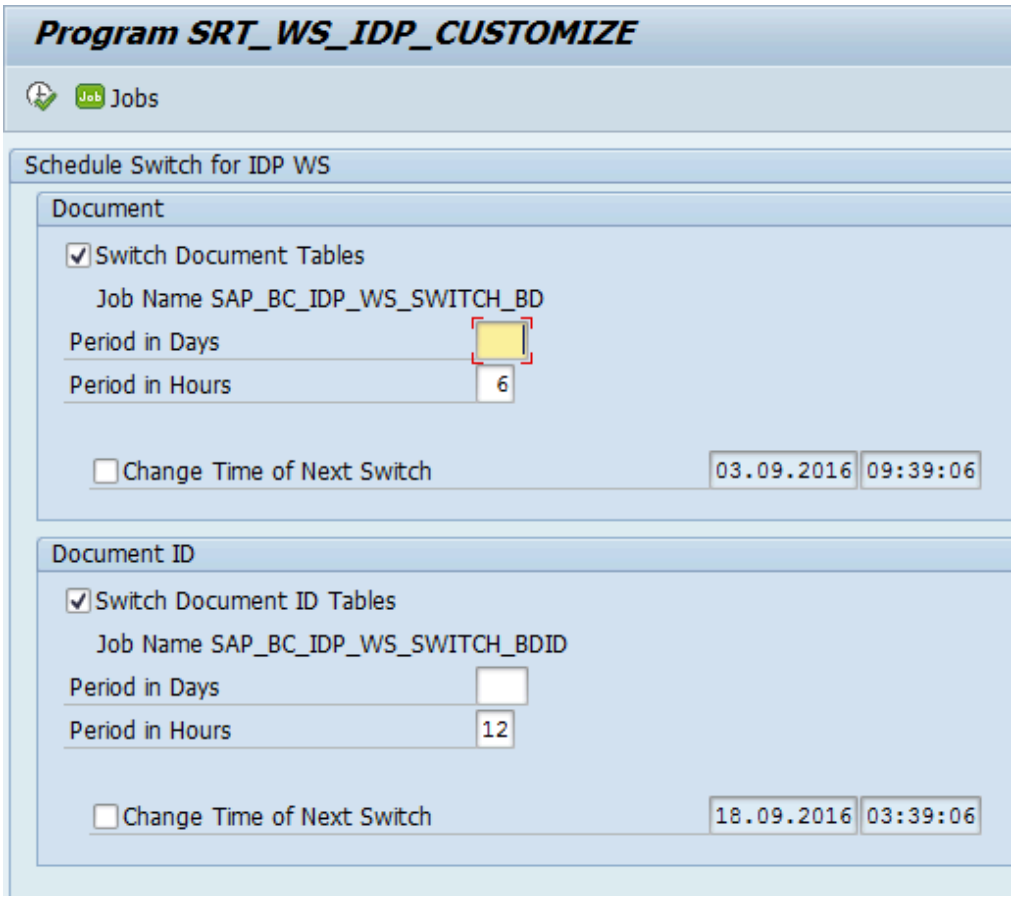
2.2.6. Define Settings for Idempotent Services

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 2-11 Idempotent Services Settings



6. Click **Continue**.

2.2.7. Set Profile Parametes 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 2-4 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 2-12 SICF: /sap/opu

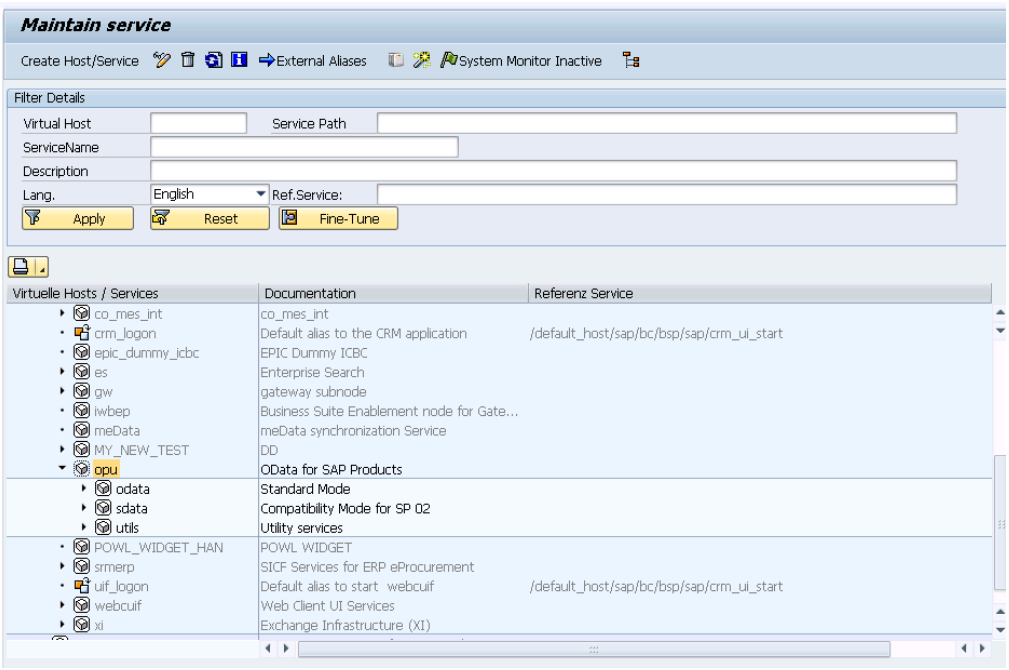
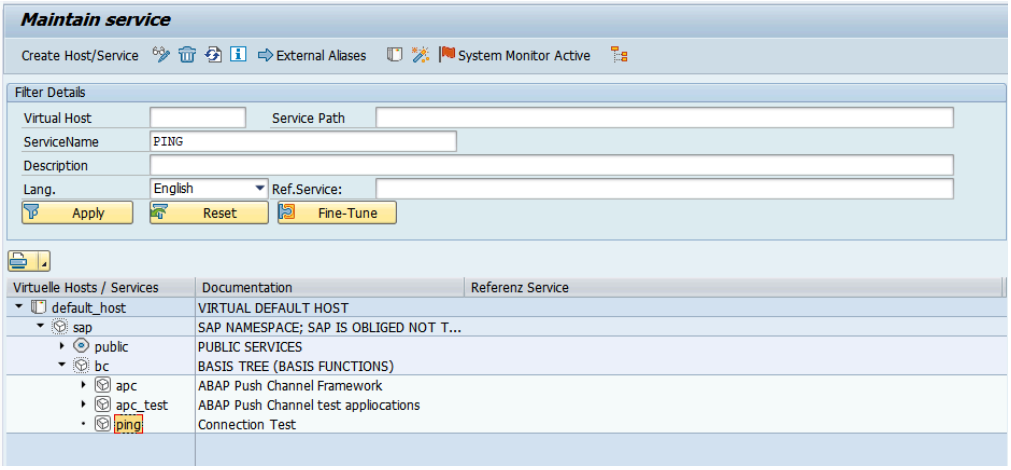


Figure 2-13 SICF: /sap/bc/ping

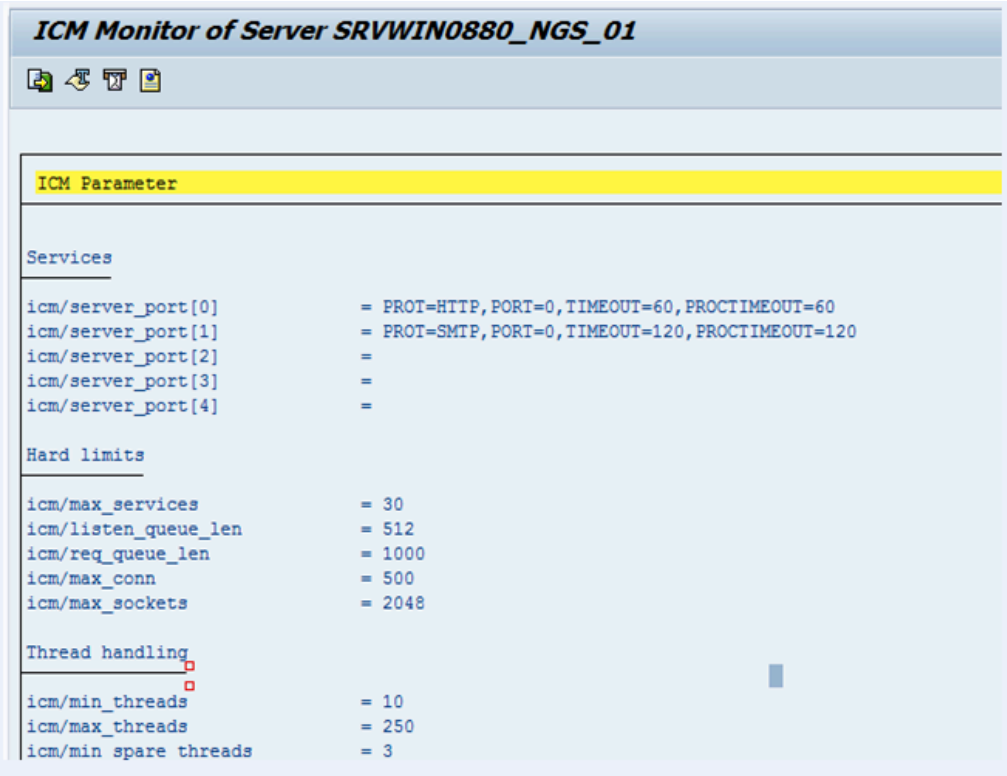


2.2.8. Maintain HTTPS and HTTP Connections

To maintain HTTPS and HTTP connections:

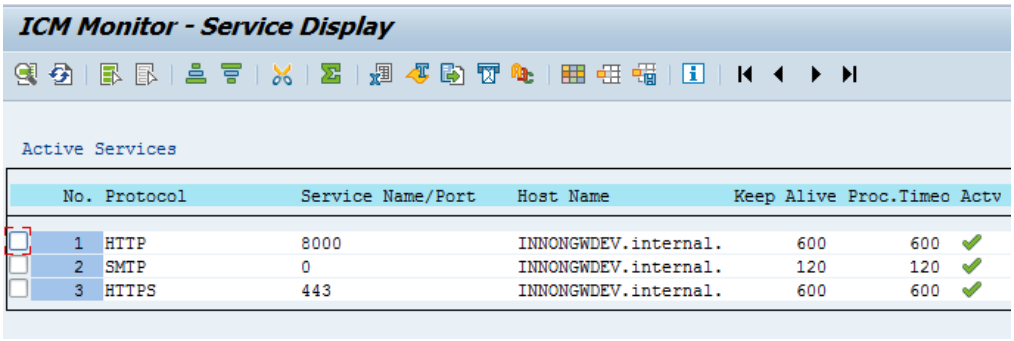
1. Run Tcode **RZ10** and set these parameters:
   - icm/server_port_0 = PROT=HTTP, PORT=8000, TIMEOUT=600, PROCTIMEOUT=600
   - icm/server_port_2 = PROT=HTTPS, PORT=8080, TIMEOUT=600, PROCTIMEOUT=600

Figure 2-14 ICM Parameters



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

Figure 2-15 ICM Monitor



2.2.9. 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.

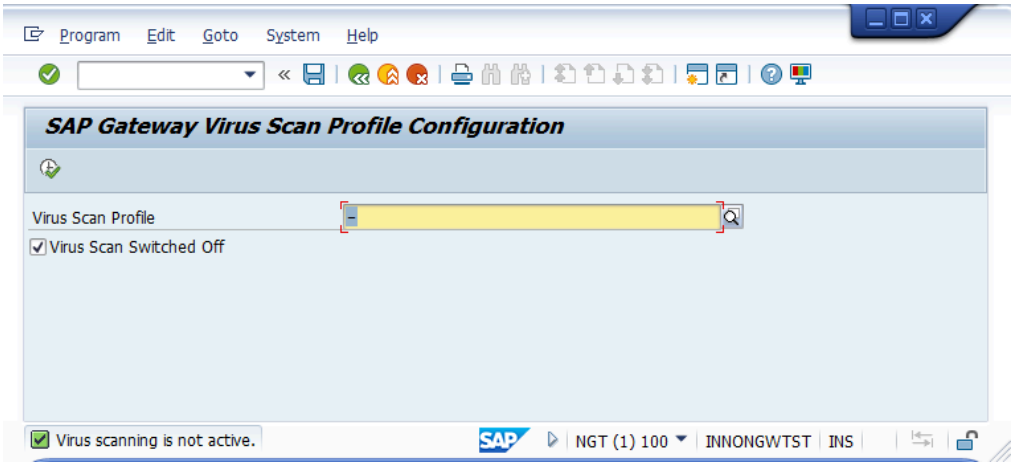
Note:
The Virus Scan must be enabled in Gateway only if the virus profile is defined.

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 2-16 Gateway Virus Scan Profile



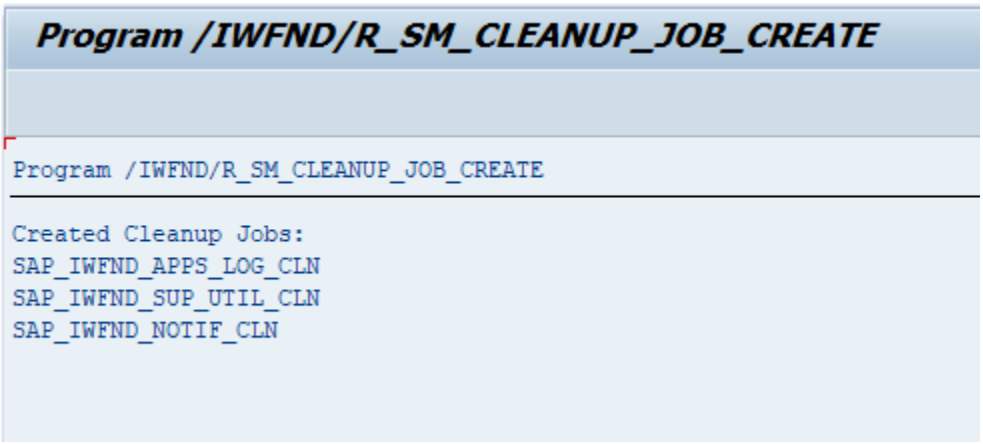
2.2.10. Create Periodical Tasks for Gateway

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 2-17 Gateway Cleanup tasks

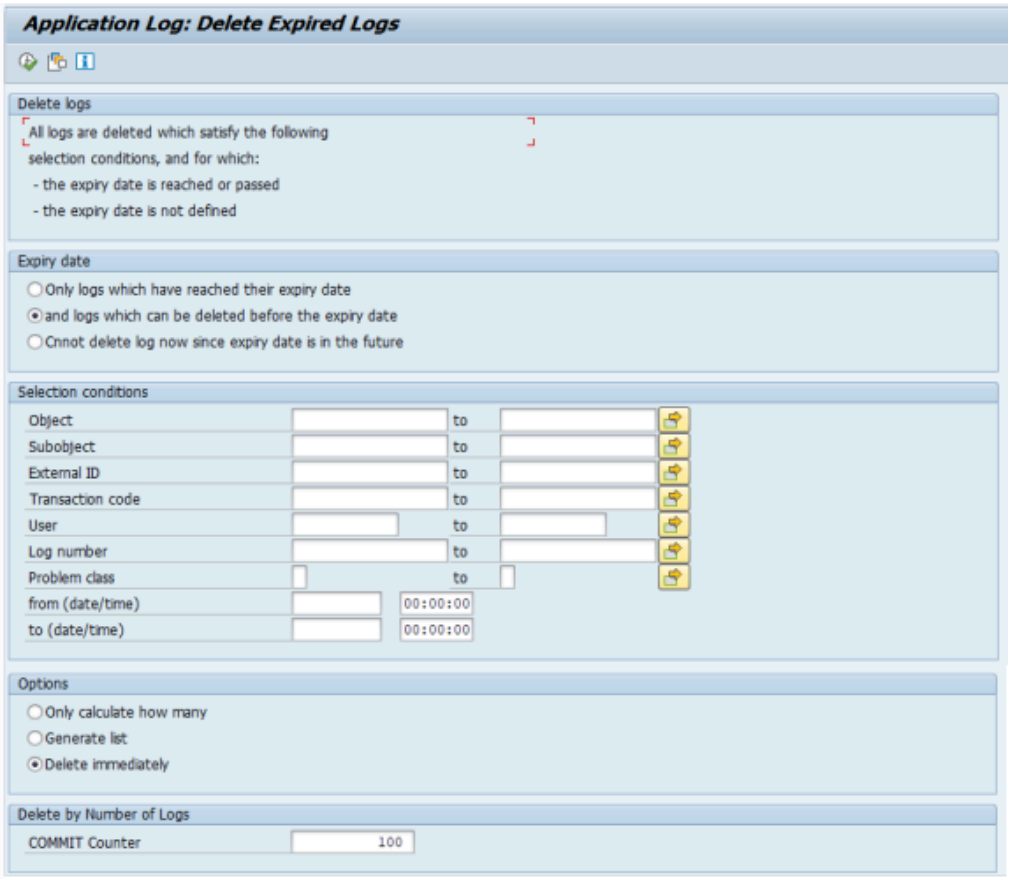


2.2.11. Clear Application Log Entries

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 2-18 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**.

2.2.12. 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 2-19 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**.

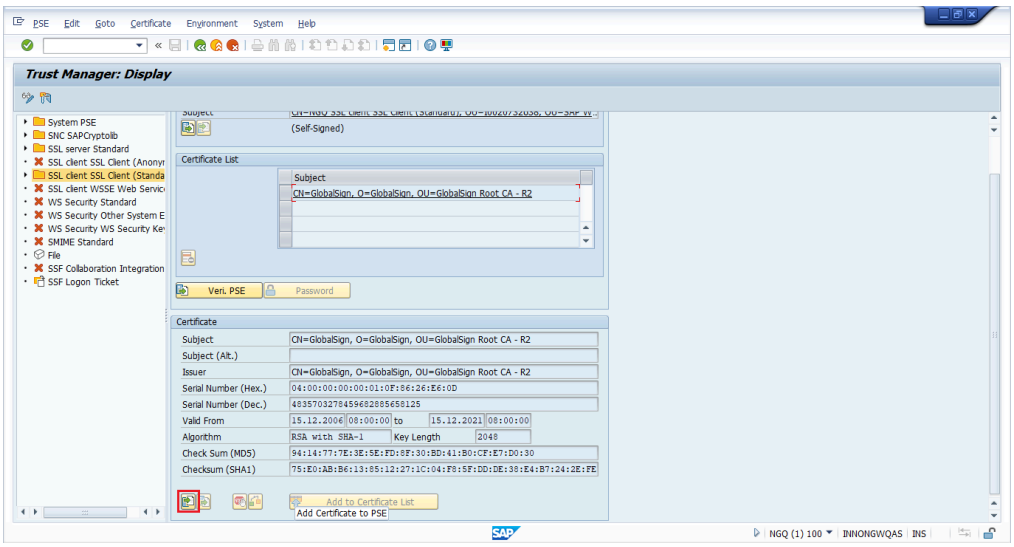
2.2.13. Install certificates for Geo location

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

To install the certificate:

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

Figure 2-20 Trust Manager



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

2.3. 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**.

2.4. 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 2-5 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,

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

Role Name	Role Description	User	Transactions
			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
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 2-6 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, /

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

Role Name	Role Description	User	Transactions
			NSBRGFCCONF, /IW-BEP/TRACES, /IWFND/TRACES, /IWFND/MAINT_SERVICE, /IW-BEP/ERROR_LOG, /IWFND/ERROR_LOG, /IWFND/NOTIF_-CLEANUP/IWFND/CACHE_CLEANUP, /IWBEP/TRACES, /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

2.4.1. Access Required for Configuring SCP

Person who is configuring SCP requires an Administrator access for entire SCP 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 SCP Administrator.

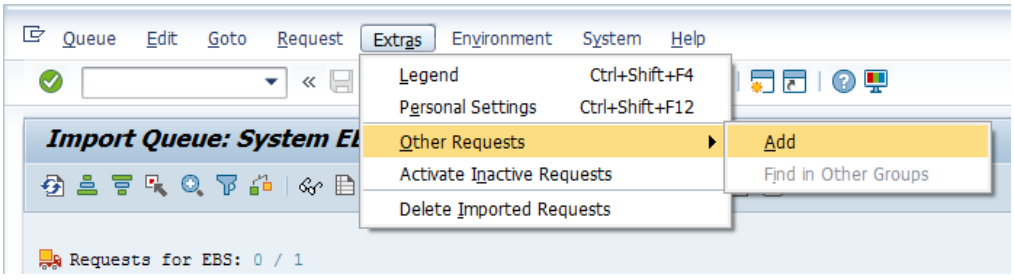
2.4.2. Import Roles Using Transports

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 2-21 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.

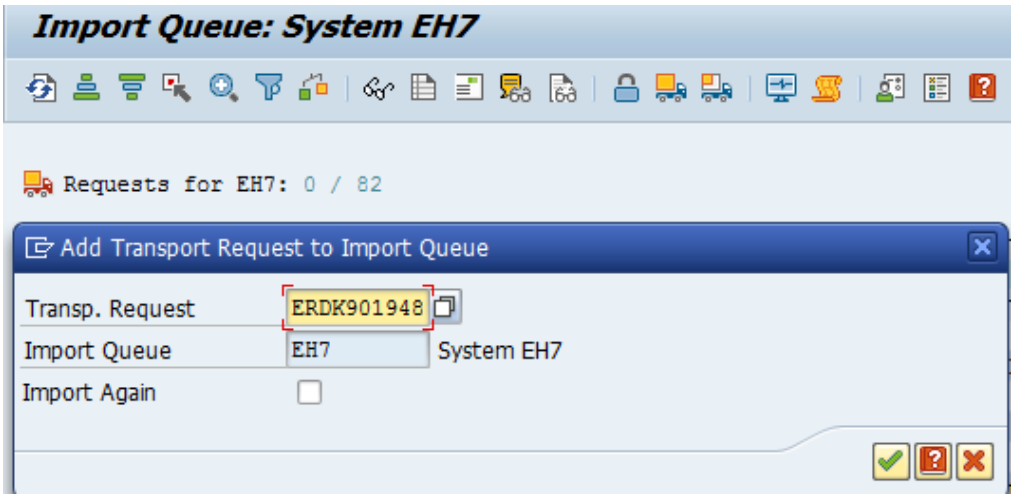
Table 2-7 SAP ECC Transports for Roles

Transport	Description	Dependency
ERDK904636	INNOV:ECC Project Team Roles	None

Table 2-8 SAP NWG Transports for Roles

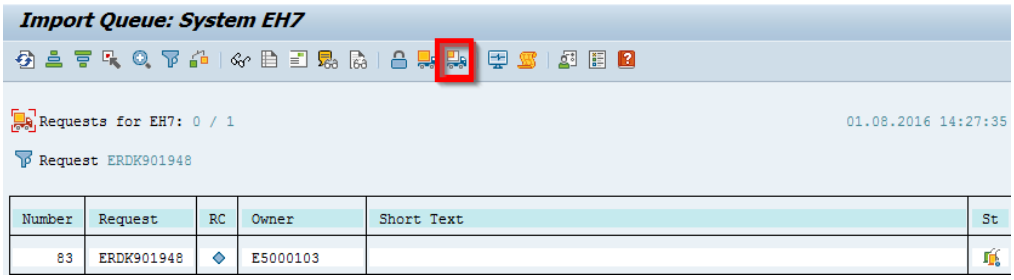
Transport	Description	Dependency
NGTK904332	INNOV:NWG Project Team Roles	None

Figure 2-22 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 2-23 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.

2.5. Configur SCP for Deploying Innovapptive Products

SAP Cloud Platform (SCP) configuration process consists of tasks like validating access to SCP, enabling mobile services, configuring cloud connector and so on.

Prerequisites

You need one of the following pre-packaged SCP accounts. For more information, contact SAP Partner Account Executive or Innovapptive Sales team.

- Get-Started Package
  - Developer Trial.
  - SAP Cloud Platform, starter edition (32GB).
  - SAP Cloud Platform, starter edition (64GB).
- Medium Business Packages (User-Based)
  - SAP Cloud Platform, professional edition.
  - SAP Cloud Platform, single application edition.
  - SAP Cloud Platform, multiple application edition.
- Enterprise Package (Resource-Based)
  - SAP Cloud Platform, app services package, standard edition.
  - SAP Cloud Platform, app services package, professional edition.
  - SAP Cloud Platform, app services package, premium edition.

Access Rights

To use Innovapptive mobile applications, you need SAP Cloud Platform Access with Admin Role along with the following:

- Enabled Application & Development Services
- Cloud Connector latest version

2.5.1. All About SCP Data Center

Access your SCP account based on the region where you are located.

The **SCP Data Center, Landscape Host details,** and **IP Range** details are in the following table:

Table 2-9 SCP Data Center Information

Account Type	Data Center	Landscape Host	IP Ranges
Customer or partner account	Europe	hana.ondemand.com	155.56.128.0/17
	United States (US East)	us1.hana.ondemand.com	65.221.12.0/24
	United States (US West)	us2.hana.ondemand.com	206.112.73.0/24
	Asia-Pacific (Australia)	ap1.hana.ondemand.com	210.80.140.0/24
Developer (trial) account	Europe (all developer accounts use this location)	hanatrial.ondemand.com	155.56.128.0/17

For example, if the Data Center is in Europe, the SCP Access URL is https://hana.ondemand.com.

2.5.2. Validate access to SCP

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

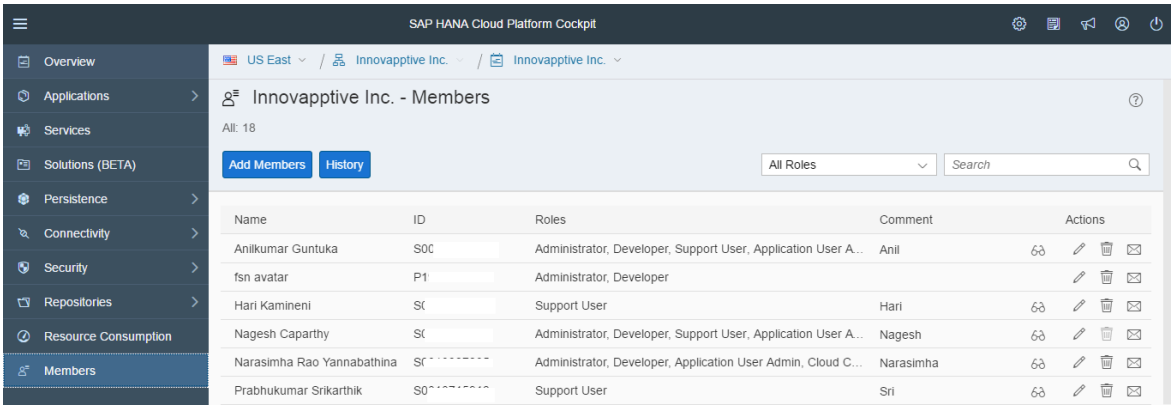
To validate access to SCP:

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

   Click **New Account** to create tenants such as Dev, QA, and PRD with SCP account.
3. Click on **Tenant** (sub account) to view the **Services** and validate the settings.

   Navigate to **Members** tab as shown below.

Figure 2-24 SCP Account Members



4. This tab helps you to add new members to the SCP Tenant. Use any of the predefined roles for the new members that you add.

Table 2-10 Roles for SCP Tenant Members

Role	Description
Administrator	• Manages account members • Creates new accounts using the self-service option • Moves quota between accounts (prerequisite: user must be assigned an administrator role in each account) • Manages subscriptions, trust, authorizations, and OAuth settings, and restart SAP HANA services on HANA databases. • Has developer permissions, except debugging. **Note:** This role grants permissions to view the Connectivity tab in the SAP Cloud Platform cockpit.

Role	Description
Cloud Connector Admin	Helps open secure tunnels via Cloud Connector from on-premise networks to cloud accounts. **Note:** This role also grants permissions to view the Connectivity tab in the SAP Cloud Platform cockpit.
Developer	• Performs development tasks, such as deploying, starting, stopping, and debugging applications. • Changes loggers and perform monitoring tasks, such as creating availability checks for applications and executing MBean operations. **Note:** This role is assigned to a newly created user by default.
Support User	Accesses account data, including metadata, configuration settings, and log files. This role is assigned to technical support engineers.

Role	Description
	Note: To read the database content, a database administrator must assign appropriate permissions to this role.
Application User Admin	• Manages user permissions on application level to access Java, HTML5 applications, and subscriptions. • Controls permissions by assigning users to specific application roles or by assigning users to groups, which you then assign to application roles. Also unassigns users from roles or groups. **Note:** Cannot manage account roles and perform actions on accounts. (for example, stopping or deleting applications).

2.5.3. Enable Mobile Services

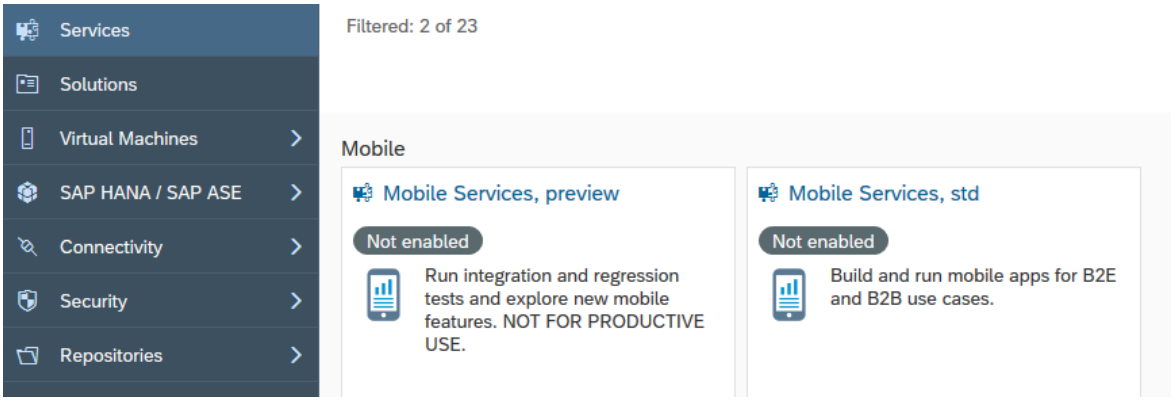
Enable mobile services, if you are logging into SCP for the first time.

To enable Mobile Services:

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

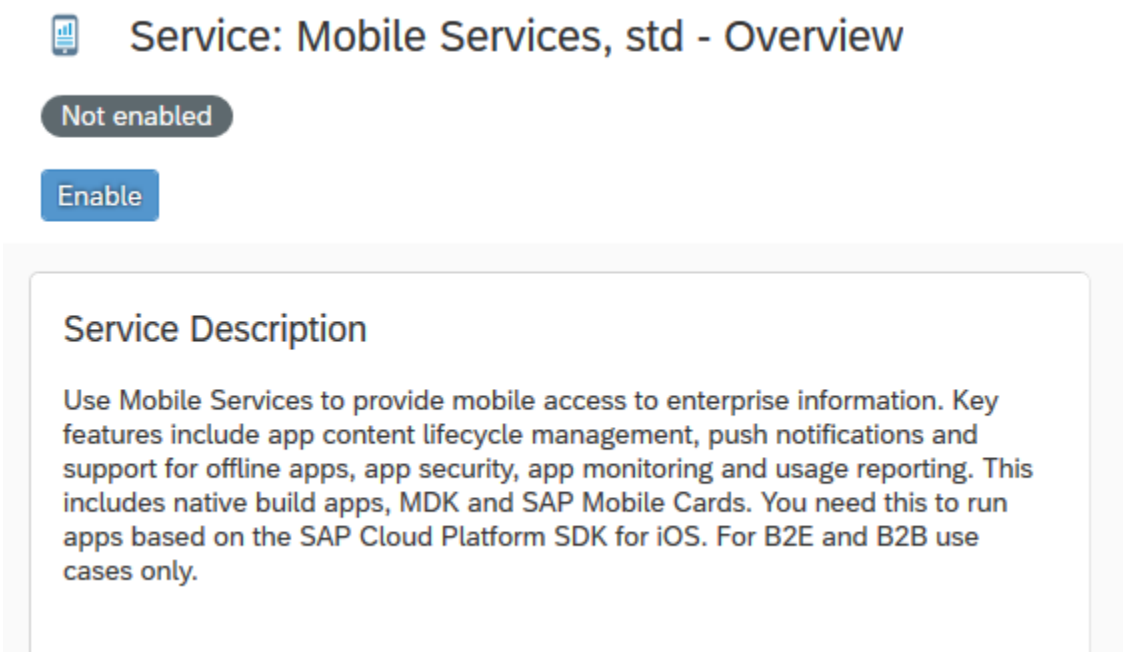
   For example, **Mobile Services, std** in the image

   Figure 2-25 Services, Mobile Services



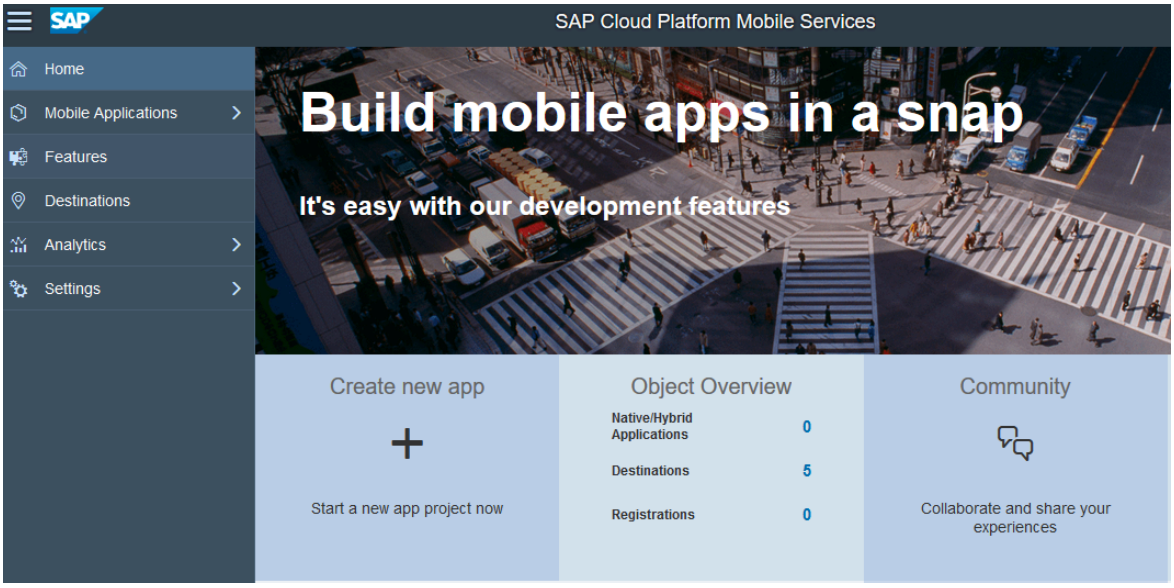
2. Click **Enable**.

   Figure 2-26 Mobile Services



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

Figure 2-27 Mobile Services portal



2.5.4. Install and Configure Cloud Connector

Cloud Connector connects on-demand applications in SAP Cloud Platform and on-premise systems and lets you the control cloud applications resources. This helps you benefit from existing assets without exposing the entire internal landscape.

The cloud connector runs as on-premise agent in a secured network and acts as a reverse invoke proxy between the on-premise network and SAP Cloud Platform. Consequently, you need not configure the on-premise firewall to allow external access from cloud to internal systems. With cloud connector, you can manage:

- On-premise systems and resources accessible to cloud applications.
- Cloud applications that make use of the cloud connector.

You can use the cloud connector in business-critical enterprise scenarios. It automatically re-establishes broken connections, provides audit logging of the inbound traffic and configuration changes.

In the **Scenarios** section below, follow the steps as per the protocol you use (**HTTP** or **RFC**).

Cloud Connector is available in two versions:

- **Developer**: This version does not require an Administrator or root privileges for the installation. Restrictions are:
    - It cannot be run in the background as a Windows Service or Linux daemon (with automatic start capabilities at boot time).
    - It does not support an automatic upgrade procedure. To update a *Developer* installation, you must delete the current installation, extract the new version, and redo configurations.
- **Production**: This version requires an Administrator or root permission for the installation. It can be set up to run as a Windows Service or Linux daemon in the background, and can easily be upgraded, retaining all configurations and customizations.

2.5.4.1. Advantages of Cloud Connector

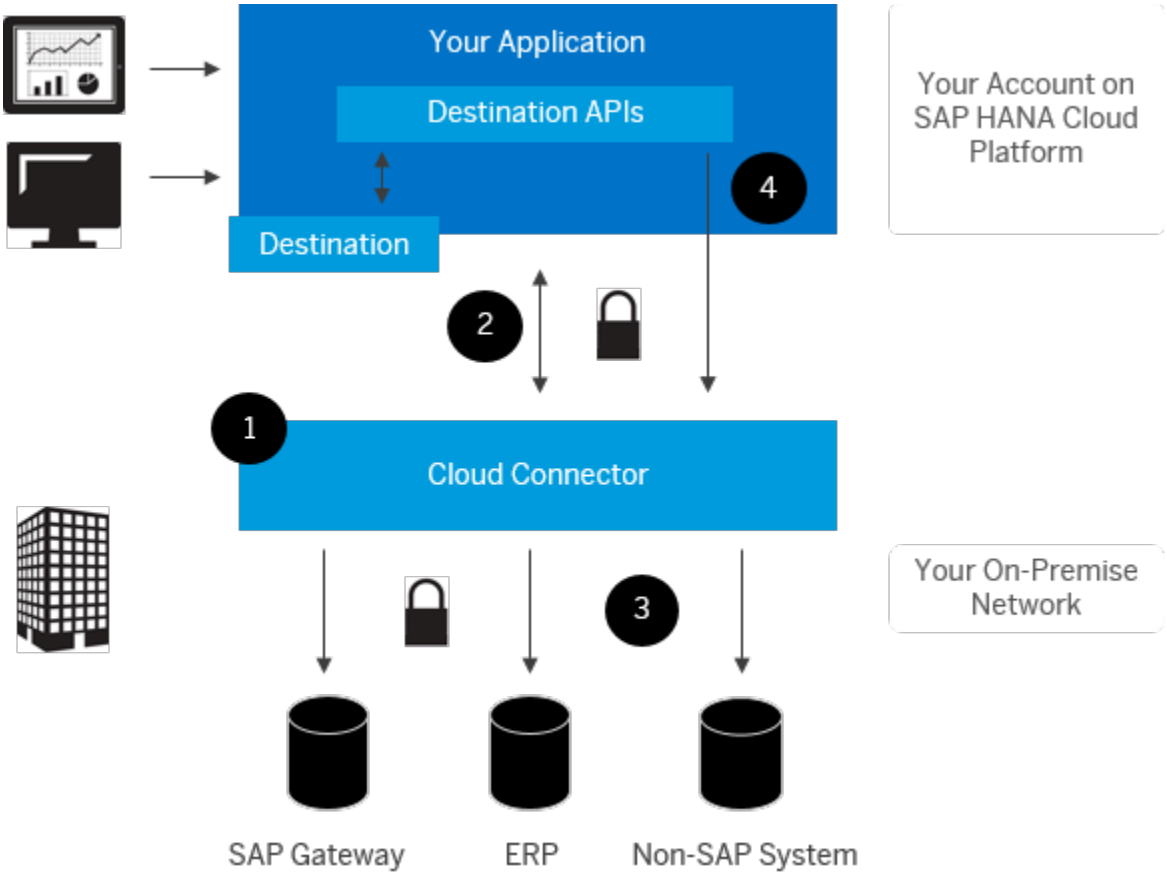
The cloud connector has these advantages:

- You do not have to open an inbound port of the on-premise network firewall to establish connectivity from SAP Cloud Platform. You can use all allowed outbound connections without any modifications.
- Supports multiple protocols. For example, supports RFC protocol that provides native access to ABAP systems and their function modules.
- Connects on-premise database or BI tools to SAP HANA databases in the cloud.
- Allows propagating identity of cloud users to on-premise systems in a secure way.
- Installs and configures easily as it is available with a low Total Cost of Ownership.

2.5.4.2. Connect Cloud Applications to On-Premise Systems

The following diagram illustrates how to connect cloud application to on-premise systems.

Figure 2-28 Connect Cloud App to On-prem



Note:
HANA Cloud Connector is also addressed as SAP Cloud Connector or just Cloud Connector.

2.5.4.3. Prerequisites for Connecting

Ensure that your systems meet the following requirements:

Table 2-11 Prerequisites for Connecting Cloud Applications to on-premise systems

Memory	Minimum 2 GB RAM, 4 GB recommended
Hard disk space	Minimum 3 GB, recommended 20 GB

Table 2-11 Prerequisites for Connecting Cloud Applications to on-premise systems (continued)

CPU	Minimum Single core 3 GHz, dual core 2 GHz recommended, x86-64 architecture compatible		
JDK	SAP JVM 64-bit (recommended)	Version 7	Cloud Connector 2.x
		Version 8	Cloud Connector 2.7.2 and higher
	Oracle JDK 64-bit	Version 7	Cloud Connector 2.x
		Version 8	Cloud Connector 2.7.2 and higher

Note:
It is recommended that you use Java 8, and update any installations running with Java runtime version 7 to Java 8.

- You can download the Cloud Connector installation archive from SAP Development Tools for Eclipse.
- JDK 7 or 8 must be installed. Due to problems with expired root CA certificates in older patches of JDK 7, it is recommended that you install the recent patches. You can download the latest SAP JVM from the SAP Development Tools for Eclipse page.

2.5.4.3.1. Supported Operating Systems for Cloud Connectors

Based on your cloud connector version, ensure that the required operating system is available.

Table 2-12 Supported Operating Systems for Cloud Connectors

Operating System Version	Architecture	Cloud Connector Version
Windows 7, Windows Server 2008 R2	x86_64	2.x
SUSE Linux Enterprise Server 11, Redhat Enterprise Linux 6	x86_64	2.x

Table 2-12 Supported Operating Systems for Cloud Connectors (continued)

Operating System Version	Architecture	Cloud Connector Version
Mac OS X 10.7 (Lion), Mac OS X 10.8 (Mountain Lion)	x86_64	2.x
Windows 8.1, Windows Server 2012, Windows Server 2012 R2	x86_64	2.5.1 and higher
SUSE Linux Enterprise Server 12, Redhat Enterprise Linux 7	x86_64	2.5.1 and higher
Mac OS X 10.9 (Mavericks), Mac OS X 10.10 (Yosemite)	x86_64	2.5.1 and higher
Windows 10	x86_64	2.7.2 and higher
Mac OS X 10.11 (El Capitan)	x86_64	2.8.1 and higher
Windows Server 2016	x86_64	2.9.1 and higher
Windows Server 2019, Mac OS X 10.12 (Sierra), Mac OS X 10.13 (High Sierra), Mac OS X 10.14 (Mojave)	x86_64	2.11.3 and higher
SUSE Linux Enterprise Server 15	x86_64	2.12.0 and higher
Redhat Enterprise Linux 8	x86_64	2.12.2 and higher

2.5.4.3.2. Data Centers Information for Connecting to Network

Connect to one of the following hosts (depending on the data center), to which you connect cloud connector:

Table 2-13 Network Connectivity Information

Data Center (Landscape host)	Hosts	IP Addresses
Europe (Rot) (hana.ondemand.com)	connectivitynotification.hana.ondemand.com	155.56.210.83
	connectivitycertsigning.hana.ondemand.com	155.56.210.43
	connectivitytunnel.hana.ondemand.com	155.56.210.84
Europe (Frankfurt) (eu2.hana.ondemand.com)	connectivitynotification.eu2.hana.ondemand.com	157.133.206.143

Table 2-13 Network Connectivity Information (continued)

Data Center (Landscape host)	Hosts	IP Addresses
	connectivitycertsigning.eu2.hana.ondemand.com	157.133.205.174
	connectivitytunnel.eu2.hana.ondemand.com	157.133.205.233
Europe (Amsterdam) (eu3.hana.ondemand.com)	connectivitynotification.eu3.hana.ondemand.com	157.133.141.140
	connectivitycertsigning.eu3.hana.ondemand.com	157.133.141.132
	connectivitytunnel.eu3.hana.ondemand.com	157.133.141.141
United States East (Ashburn) (us1.hana.ondemand.com)	connectivitynotification.us1.hana.ondemand.com	65.221.12.40
	connectivitycertsigning.us1.hana.ondemand.com	65.221.12.241
	connectivitytunnel.us1.hana.ondemand.com	65.221.12.41
United States West (Chandler) (us2.hana.ondemand.com)	connectivitynotification.us2.hana.ondemand.com	64.95.110.215
	connectivitycertsigning.us2.hana.ondemand.com	64.95.110.211
	connectivitytunnel.us2.hana.ondemand.com	64.95.110.214
United States East (Sterling) (us3.hana.ondemand.com)	connectivitynotification.us3.hana.ondemand.com	169.145.118.140
	connectivitycertsigning.us3.hana.ondemand.com	169.145.118.132
	connectivitytunnel.us3.hana.ondemand.com	169.145.118.141

Table 2-13 Network Connectivity Information (continued)

Data Center (Landscape host)	Hosts	IP Addresses
US States West (Colorado Springs) (us4.hana.ondemand.com)	connectivitynotification.us4.hana.ondemand.com	157.133.45.140
	connectivitycertsigning.us4.hana.ondemand.com	157.133.45.132
	connectivitytunnel.us4.hana.ondemand.com	157.133.45.141
Asia-Pacific (Australia) (ap1.hana.ondemand.com)	connectivitynotification.ap1.hana.ondemand.com	157.133.97.47
	connectivitycertsigning.ap1.hana.ondemand.com	157.133.97.27
	connectivitytunnel.ap1.hana.ondemand.com	157.133.97.46

2.5.4.4. Install Cloud Connector on Microsoft Windows

Before you install Cloud Connector on Microsoft Windows, ensure that you have:

Before proceeding, ensure you have the following:

- 64-bit operating system: Windows 7, Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019.
- Cloud Connector MSI installer from SAP Development Tools for Eclipse.
- Microsoft Visual Studio C++ 2013 runtime libraries (vcredist_x64.exe). This is mandatory.
- Java 7 or Java 8 installed.

To install cloud connector:

1. Double-click on the **<sapcc-<version>-windows-x64.msi>** installer and click **Next.**
2. Navigate to the installation directory and click **Next**.
   If you are doing an upgrade, select the previous installation directory.
3. Enter the port on which the administration UI can be reached and click **Next**.
   By default, the port is set to **8443**.

4. Select the JDK.
   List of JDKs of version 7 that are installed on the machine are displayed. If the JDK is not listed in the drop-down (for example, if it is an SAP JVM that is not registered in the Windows Registry upon installation), browse to the installation directory and select the JDK
5. Select whether the cloud connector should be started immediately after finishing the setup and click **Next**.
   List of JDKs of version 7 that are installed on the machine are displayed. If the JDK is not listed in the drop-down (for example, if it is an SAP JVM that is not registered in the Windows Registry upon installation), browse to the installation directory and select the JDK.
6. Click **Next**.
7. Click **Close**.

Note:
Cloud connector 2.x starts as a Windows Service in the Production environment. You can manage the service and Cloud Connector 2.0, under **Control Panel, Administrative Tools, Services**. Ensure that the service is executed by a user that has limited privileges. Typically, privileges allowed for service users are defined by your company policy.

2.5.4.5. Install Cloud Connector on Linux

Before you install Cloud Connector on Linux, ensure that you have:

- 64-bit operating system: SUSE Linux Enterprise Server 11, 12, or 15, or Redhat Enterprise Linux 6, 7, or 8.
- Cloud Connector RPM installer contained in the ZIP for Linux from SAP Development Tools for Eclipse.
- Java 7 or Java 8 installed.

Note:
You can execute the following commands:

- **rpm -qa | grep jvm**: To check the JVM version on your system.
- **rpm -i sapjvm-<version>-linux-x64.rpm**: To install the SAP JVM.

- Set the environment variable <JAVA_HOME> to the Java installation directory or add the Java installation's bin subdirectory to the <PATH> variable.

Note:
This is applicable only if you use the tar.gz archive for installation.

To install cloud connector:

1. Extract the sapcc-<version>-linux-x64.zip archive to an arbitrary directory using the command:

```
unzip sapcc-<version>-linux-x64.zip2
```

2. Navigate to the directory and install the extracted RPM using the command.

```
rpm -i com.sap.scc-ui-<version>.x86_64.rpm 3
```

Note:
You must have Super User or Administrator role can execute the command.

In the productive case, the Cloud Connector is started as a daemon. To manage the daemon process, execute:

```
System V init distributions: service scc_daemon stop|restart|start|status

systemd distributions: systemctl stop|restart|start|status scc_daemon
```

2.5.4.5.1. Start or Stop Cloud Connector manually

When you install Cloud Connector using RPM manager, it starts automatically and registers as a daemon process to ensure automatic restart of the Cloud Connector after a system reboot.

Execute the following commands to start, stop or restart Cloud Connector manually:

- System V init distributions: service scc_daemon start|stop|restart
- systemd distributions: systemctl start|stop|restart scc_daemon

Note:
You must have Super User or Administrator role to execute the commands.

2.5.4.6. Login to Cloud Connector

Login to Cloud Connector as an administrator or manager and do initial configurations.

To login to cloud connector:

1. Enter: *https://<hostname>:<port>* in a browser.
   - <hostname> refers to the machine on which the cloud connector is installed. If installed on your machine, you can enter localhost.
   - <port> is the cloud connector port specified during installation (default port is 8443).
2. Enter User Name/Password as Administrator/manage.
   The fields are case sensitive.
3. Click **Login**.
   Choose either master or shadow installation. Use **Master** if you are installing a single cloud connector instance or a main instance from a pair of cloud connector instance. For more information, see Installing a Failover Instance for High Availability.

2.5.4.6.1. Configure your password

When you login to Cloud Connector for first time, you must change the password.

In the mandatory password change screen that appears when you login, enter the following.

1. Enter your existing password.
2. Enter new password and repeat the password.
3. Click **Save**.

2.5.4.6.2. Initial setup

Cloud Connector starts a handshake with SAP Cloud Platform and establishes a secure SSL connection with the server where your on-demand applications are configured.

To set up the initial configuration, enter the following:

1. **Landscape Host**: Your SCP Host Name.
2. **Account Name**: ID from SCP Account/Tenant.
3. **Account User**: Cloud Connector Admin Username.
4. **Password**: Password of the ID.

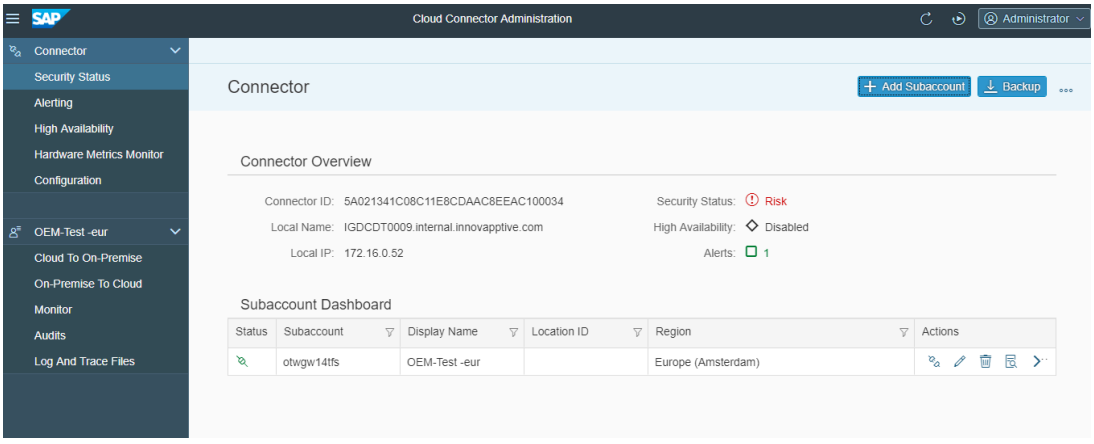
   No requests are passed from Cloud to back-end systems. To allow on-demand applications access back-end systems, Configure Access Control *(on page 58)*.

> **Note:**
> The internal network must allow access to the port. Specific configuration for opening the respective port(s) depends on the firewall software used. The default ports are **80** for HTTP and **443** for HTTPS. For RFC communication, you need to open a gateway port (default: 33+<instance number>and an arbitrary message server port. For a connection to a HANA Database (on SAP Cloud Platform) via JDBC, you need to open an arbitrary outbound port in your network. Mail (SMTP) communication is not supported.

To change proxy settings (for example, if the company firewall rules have changed), go to **Settings** menu. Some proxy servers require credentials for authentication.

Once the initial setup is completed successfully, the connection to the Cloud endpoint is opened.

Figure 2-29 Cloud endpoint



2.5.5. Establish trust between SCP, Cloud Connector and SAP Gateway

Establish trust between SCP, Cloud Connector and SAP system using self-signed certificates.

To establish trust, perform the following tasks:

1. Create Self-Signed Root CA for Cloud Connector *(on page 54)*.
2. Create an Intermediate Certificate for Cloud Connector *(on page 54)*.
3. Import the Certificate in the Cloud Connector machine *(on page 56)*.
4. Configure Cloud Connector to use Principal Propagation *(on page 57)*.
5. Configure SAP System to Support Principal Propagation *(on page 61)*.
6. Export SAP System Certificates for Cloud Connector *(on page 70)*.
7. Import Cloud Connector Root and Intermediate Certificates to Gateway Trust Store *(on page 72)*

2.5.5.1. Create Self-Signed Root CA for Cloud Connector

You can use an existing CA to create a self-signed CA. If you are using your own CA, create the certificate of that CA.

To create a self-signed root CA for Cloud Connector:

1. Execute the following commands:
   a. openssl genrsa -aes256 -out \HCC_CA.key 2048
   b. openssl req -sha256 -new -x509 -days 9999 -key \HCC_CA.key -out \HCC_CA.crt
2. Provide the input information for the Root CA & continue to input the asking value.
3. Create a single PKCS file safe keeping by running the following command:
   openssl pkcs12 -export -clcerts -in \HCC_CA.crt -inkey \HCC_CA.key - out \HCC_CA.p12

2.5.5.2. Create an Intermediate Certificate for Cloud Connector

To create an intermediate certificate for cloud connector:

1. Create the following file at the command (command for Linux OS):
   a. Linux OS
      - touch \certindex
      - echo 1000 > \certserial
      - echo 1000 > \crlnumbe

b. Windows OS

- echo certindex
- echo 1000 > \certserial
- echo 1000 > \crlnumbe

2. Create a CA configuration file:
   - Create a file with the following name: **ca.conf.**
   - Add this content to the file.

```
# vim ca.conf
          [ ca ]
          default_ca = myca
          [ crl_ext ]
          issuerAltName=issuer:copy
          authorityKeyIdentifier=keyid:always
          [ myca ]
          # Linux
          dir = ./
          # Windows - change this value to the working path for this guide
          # dir =C:\\OpenSSL-Win64\\bin\\
          new_certs_dir = $dir
          unique_subject = no
          certificate = $dir/HCC_CA.crt
          database = $dir/certindex
          private_key = $dir/HCC_CA.key
          serial = $dir/certserial
          default_days = 730
          default_md = sha1
          policy = myca_policy
          x509_extensions = myca_extensions
          crlnumber = $dir/crlnumber
          default_crl_days = 730
          [ myca_policy ]
          commonName = supplied
          stateOrProvinceName = supplied
          countryName = optional
          emailAddress = optional
          organizationName = supplied
          organizationalUnitName = optional
```

```
                        [ myca_extensions ]
                        basicConstraints = critical,CA:TRUE
                        keyUsage = critical,any
                        subjectKeyIdentifier = hash
                        authorityKeyIdentifier = keyid:always,issuer
                        keyUsage = digitalSignature,keyEncipherment,cRLSign,keyCertSign
extendedKeyUsage =
                        serverAuth
                        [ v3_ca ]
                        basicConstraints = critical,CA:TRUE,pathlen:0
                        keyUsage = critical,any
                        subjectKeyIdentifier = hash
                        authorityKeyIdentifier = keyid:always,issuer
                        keyUsage = digitalSignature,keyEncipherment,cRLSign,keyCertSign
extendedKeyUsage =
                        serverAuth
```

Note:
Change the dir value in the configure file as per your OS.

3. Create intermediate Key and CSR:
    a. openssl genrsa -out \intermediate.key 2048.
    b. openssl req -new -sha256 -key \intermediate.key -out \intermediate.csr.
    c. Provide the input information for the certificate and continue to input the asking value.
    d. openssl ca -batch -config \ca.conf -notext -in \intermediate.csr -out \intermediate.crt.
4. Convert Client Key to PKCS:
    a. Will merge the certificate and private key to create a single file.
    b. openssl pkcs12 -export -clcerts -in \intermediate.crt -inkey \intermediate.key -out \intermediate.p12.

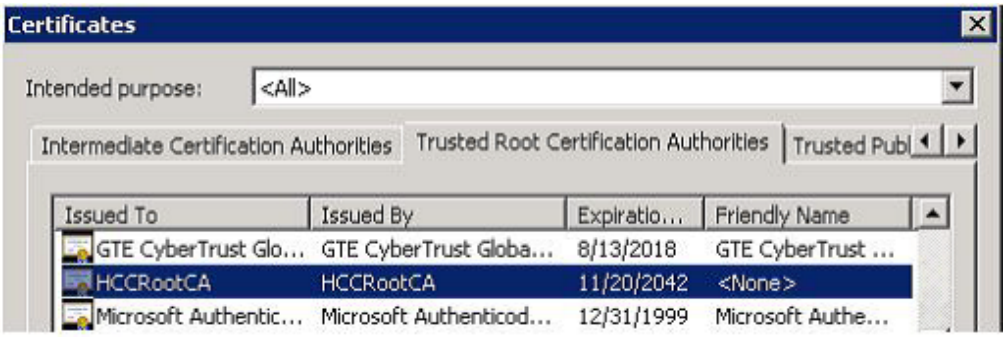
2.5.5.3. Import Certificate into the Cloud Connector Machine

Import HCC_CA.crt --- HCC Root CA and intermediate .p12—Intermediate CA with the “KEYCERTSIGN” in the property certificates into the HCC computer.

To import certificate into the cloud connector machine:

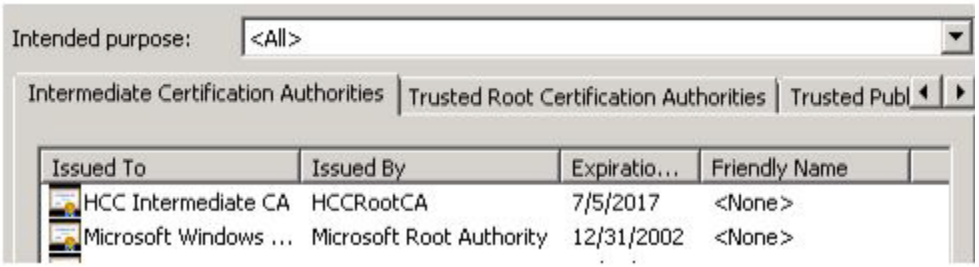
1. Right-click each certificate and select install, or from Internet Explorer open Internet Options and go to the **Content Tab** and select **Certificates.**
2. Import the **HCC_CA.crt** into the **Trusted Root Certification Authorities** certificate store.

Figure 2-30 Trusted Root Certification Authorities



3. Import the intermediate **.p12** into the **Intermediate Certification Authorities** certificate store.

Figure 2-31 Intermediate Certification Authorities

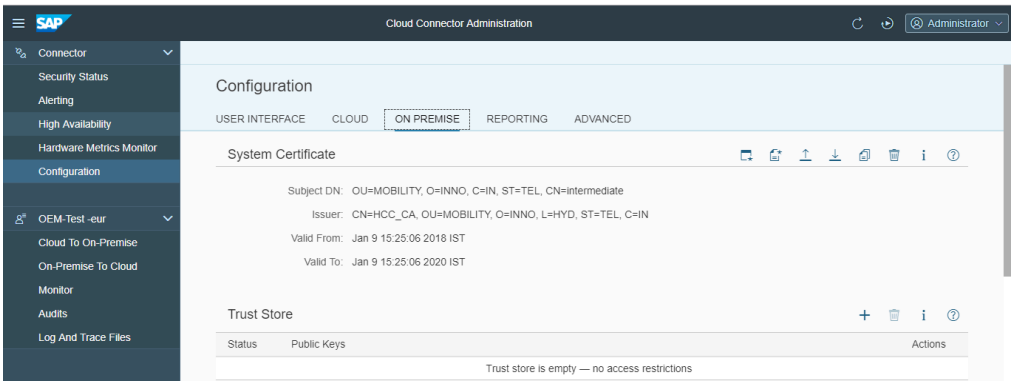


2.5.5.4. Configure Cloud Connector

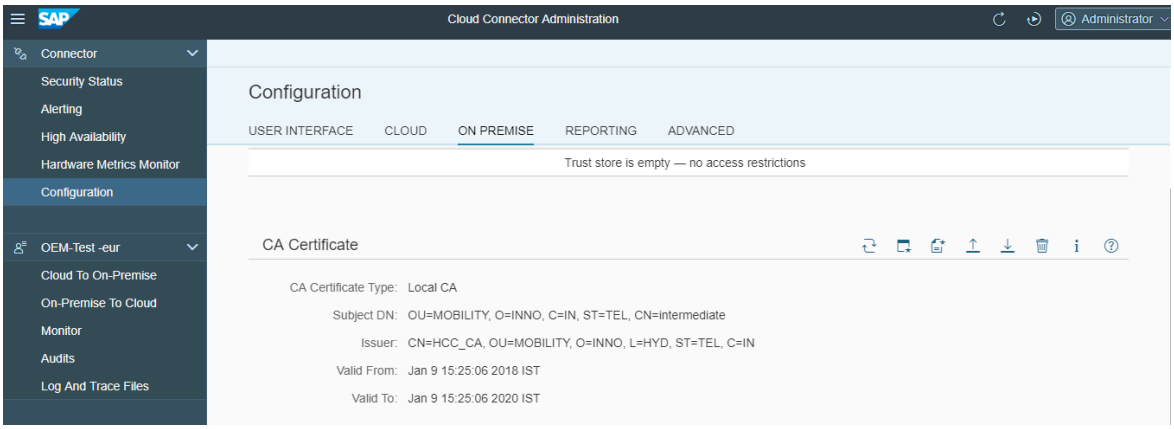
To configure the Cloud Connector:

1. Go to Configuration menu, **On Premise** tab.
2. Upload the Intermediate Certificate to Cloud Connector.

Figure 2-32 System Certificate section

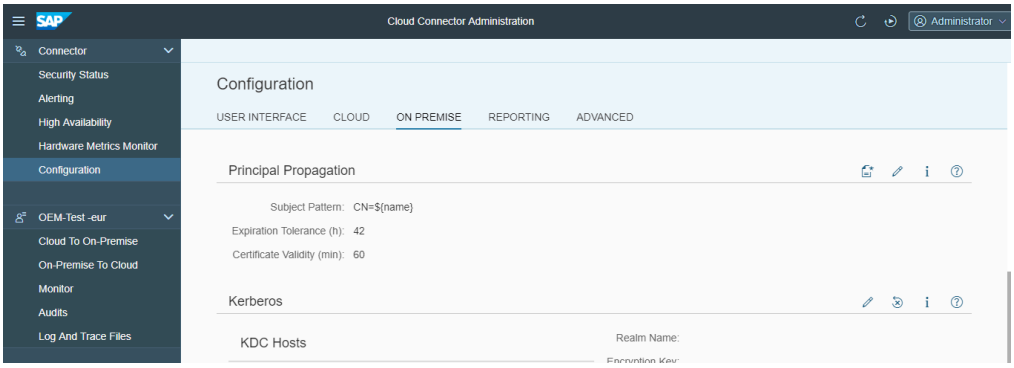


3. Upload Root CA file to CA Certificate.



4. Update the Principal Propagation Settings.

Figure 2-33 Principal Propagation Settings



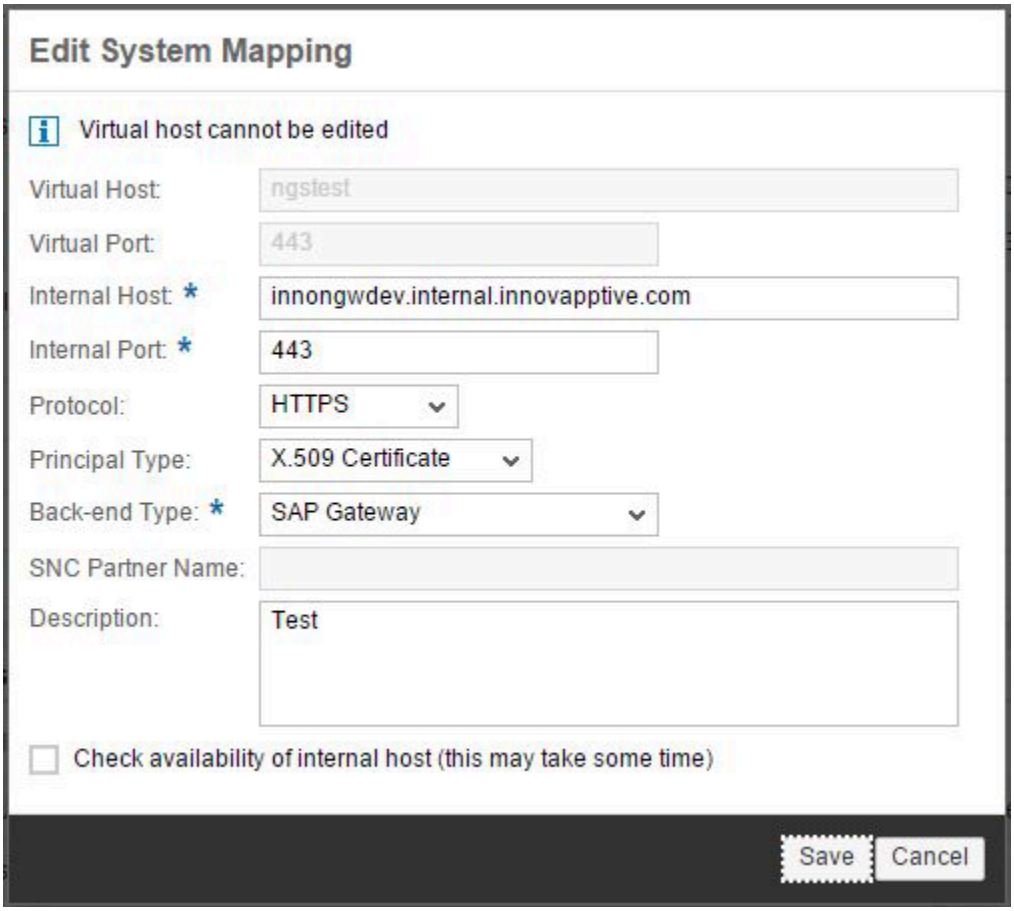
5. Upload the **Backend system server** certificate into **Trust Store.**

2.5.5.5. Configure Access Control

To configure access control:

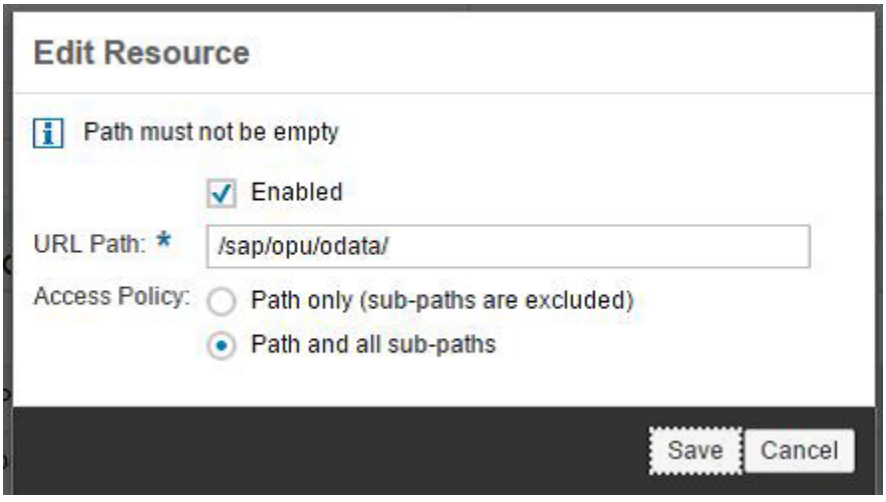
1. Click **Access Control** and click **Add** to add a new system mapping in HCC.
   Edit the existing mapping to support Principal propagation.

Figure 2-34 System Mapping



2. Add resource to access the ODATA Service.

Figure 2-35 Add Resource



3. Restart the Cloud Connector.

2.5.5.6. Configure SAP system to support principal propagation

The SSL server PSE contains the application server's security information. The PSE needs the information to communicate using SSL as the server component. For each SSL port that is activated (see the profile parameter icm/server_port_<xx>), set up a corresponding SSL server PSE to use.

The server's Distinguished Name is used to identify the server when a connection is established. If you have a system with multiple application server instances, use the following options to resolve the server identity:

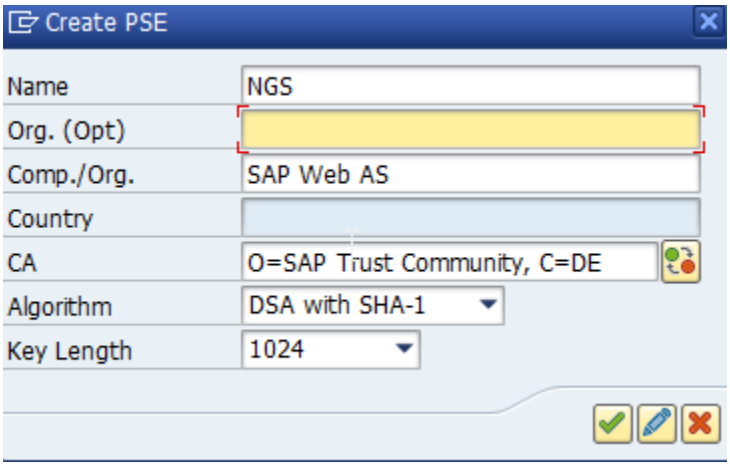
- Use a single system-wide SSL server PSE where the Distinguished Name is the same for all servers.
- Use server-specific SSL server PSEs for individual application servers.
- Use a combination of both types. (Some application servers use a system-wide SSL server PSE, and other application servers use server-specific SSL server PSEs.)

Note:
Use the trust manager (transaction STRUST) to maintain the PSEs.

SSL Setup—Creating the SSL Server PSE:

1. Select the SSL Server PSE node.
2. Click Create.

Figure 2-36 Create PSE



3. Enter the Distinguished Name parts for a default SSL server PSE in the corresponding fields. For the default SSL server PSE, use a wildcard character (*) as the host name in the **Name** field.

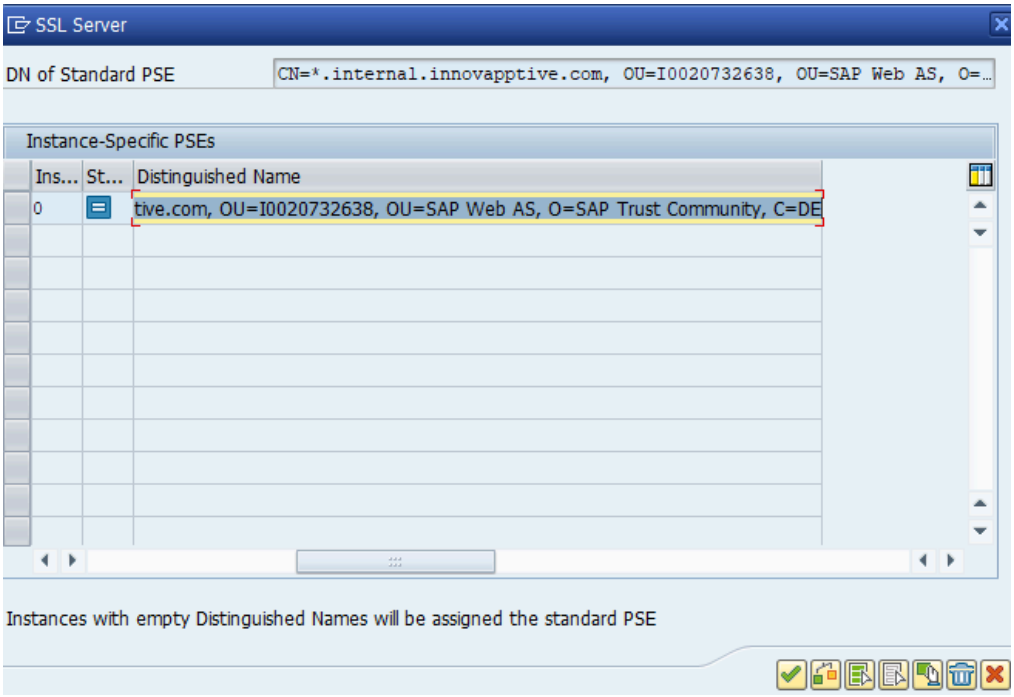
   For example,

- Name = *.mycompany.com
- Org. (opt.) = Test
- Comp./Org. = MyCompany
- Country = US

The system uses these components to build a default Distinguished Name to use for a system-wide PSE, and to build the server-specific names for individual PSEs.

The **SSL Server** screen appears where you can specify the individual application servers. Use the default Distinguished Name and system-wide SSL server PSE or individual PSEs. The default Distinguished Name appears in the **Default PSE DN** field. The server-specific Distinguished Names appear in the table in the **Distinguished Name** column.

Figure 2-37 SSL Server

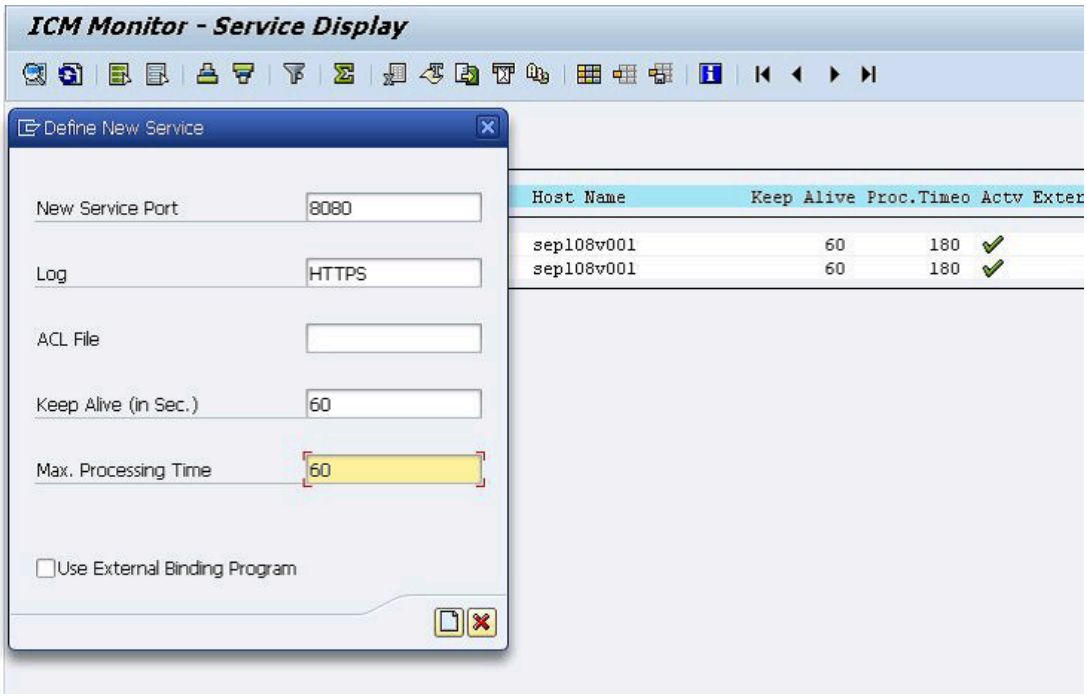


The system creates the SSL server PSEs and distributes them to the individual application servers.

2.5.5.7. Create HTTPS Service in SMICM

To create HTTPS service in SMICM:

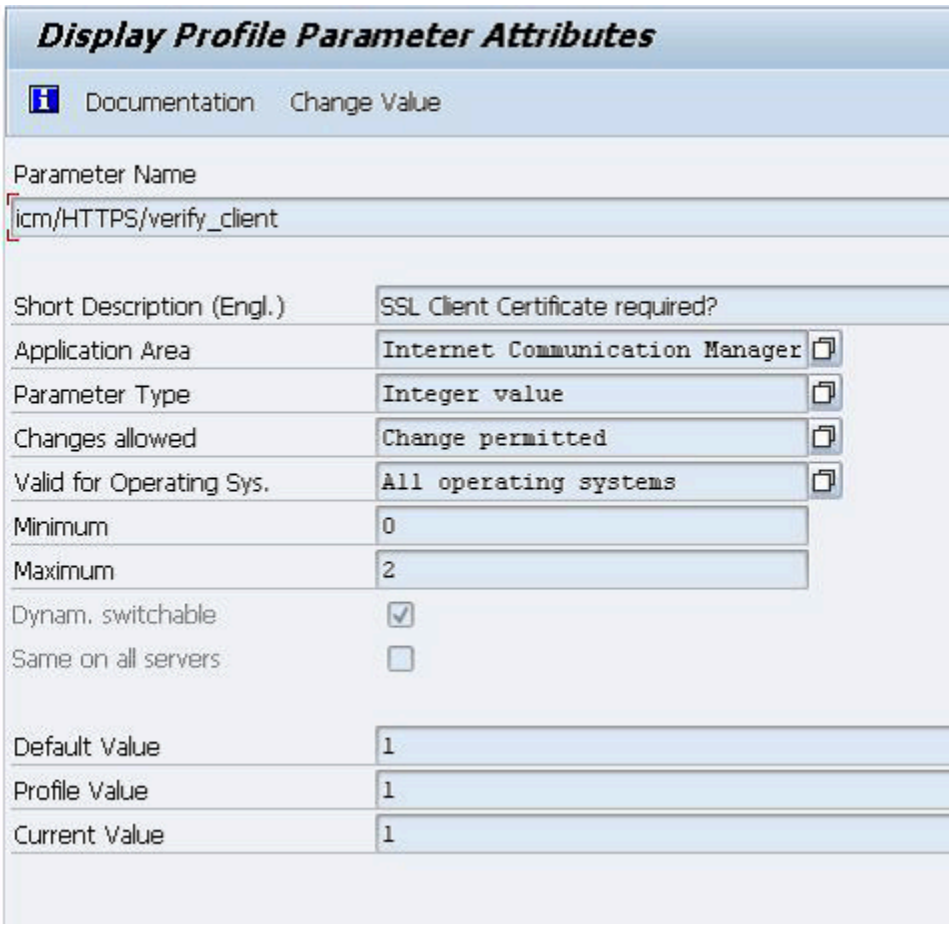
Figure 2-38 New Service Window



Profile Parameters

- Transaction code: **RZ11**
- Profile Parameter: icm/HTTPS/verify_client = 1

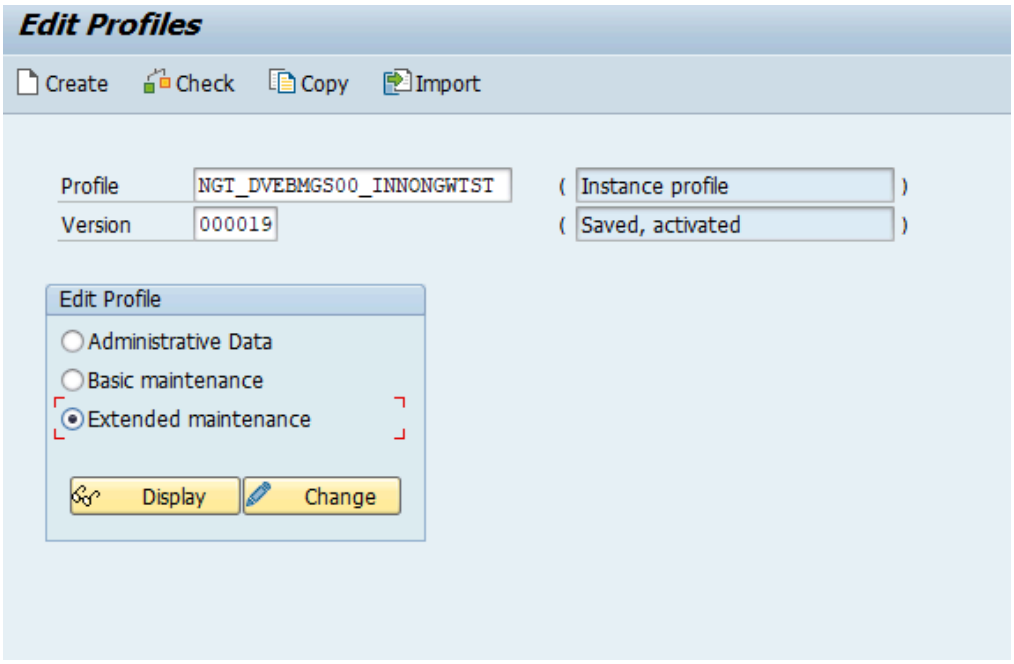
Figure 2-39 Profile Parameter Attributes



The ICM trusts the system certificate for principal propagation:

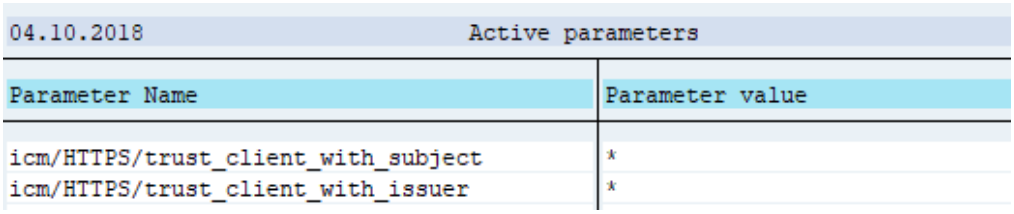
1. Transaction code: RZ10
2. Select the profile to edit, for example, the instance profile.
3. Select **Extended maintenance** and click **Change**.

Figure 2-40 Edit Profile



4. Create the following two parameters:
   - **icm/HTTPS/trust_client_with_issuer= ***
   - **icm/HTTPS/trust_client_with_subject= ***
5. Click **Save**.
6. Open the **ICM Monitor** (transaction code: SMICM) and restart the ICM. To do so,
   a. Choose **Administration > ICM > Exit Hard > Global.**
7. Verify that the two profile parameters have been taken over by ICM. To do so, **Goto > Parameter > Display.**

Figure 2-41 Active Parameters



8. Click **Save**.

2.5.5.8. Provide Logon Data

Use Transaction code: Sicf to provide Logon data:

1. Go to /default_host/sap/opu/odata.
2. Click **invmim.**
3. On the **Logon Data** tab, change the procedure to **Alternative Logon** Procedure.

Figure 2-42 Logon Data

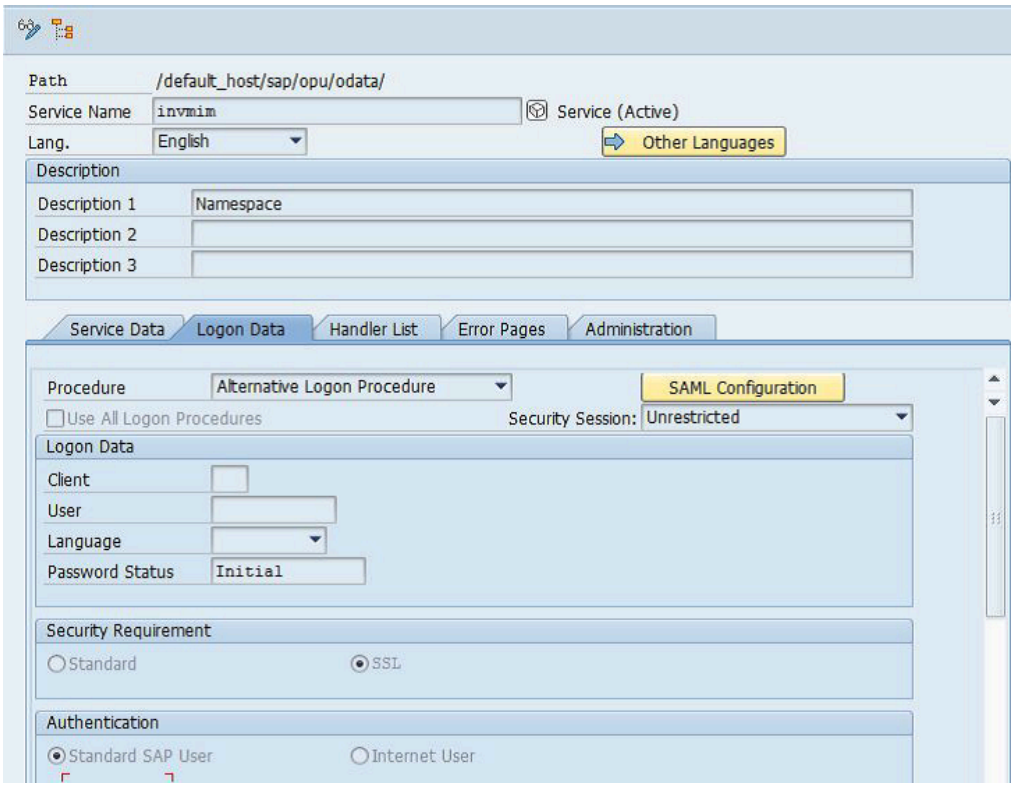
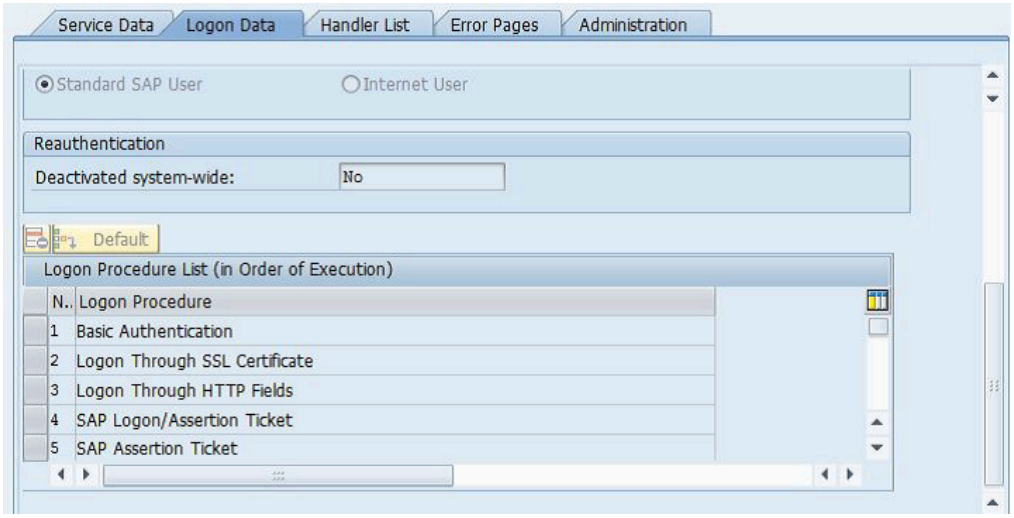


Figure 2-43 Logon Data



4. In **Security Requirements**, select **SSL**.

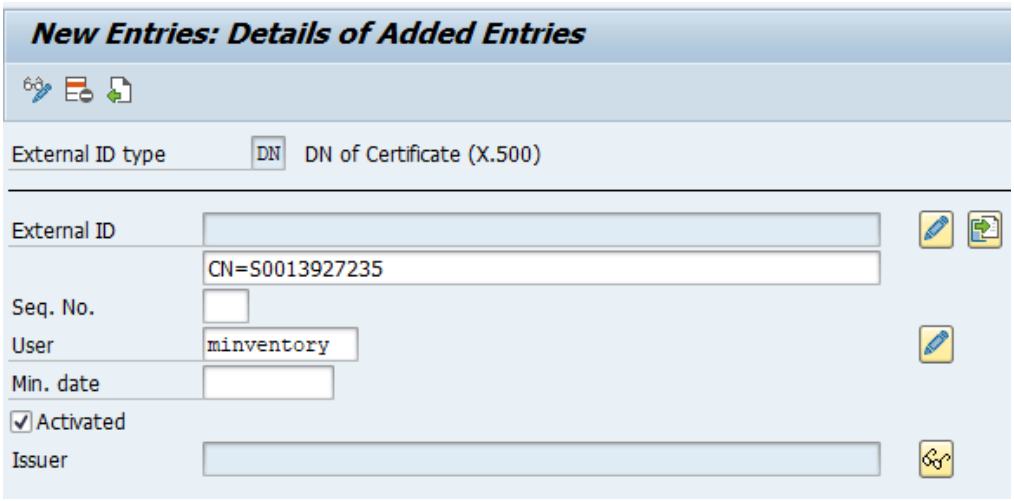
2.5.5.9. Mapping certificates to users

Map the certificates to respective users using Transaction code: EXTID_DN.

To map the certificates:

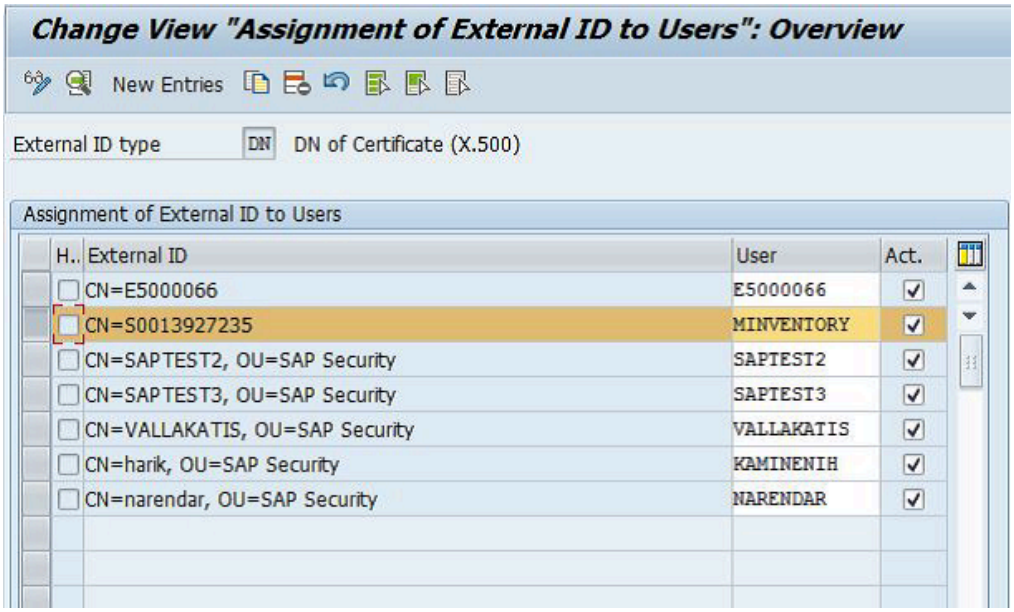
1. Switch to **Edit** mode.
2. Create a new entry.

Figure 2-44 Add Entry



3. Save the mapping.

Figure 2-45 Assign External ID to Users Overview



> **Note:**
> Ensure that the value for **CN** in External ID field is maintained in the same case as the user login ID.

To avoid authentication failures, you can maintain two entries with both lower- and upper-case user IDs.

Example: For user **gogier_con**, you can maintain the following entries:

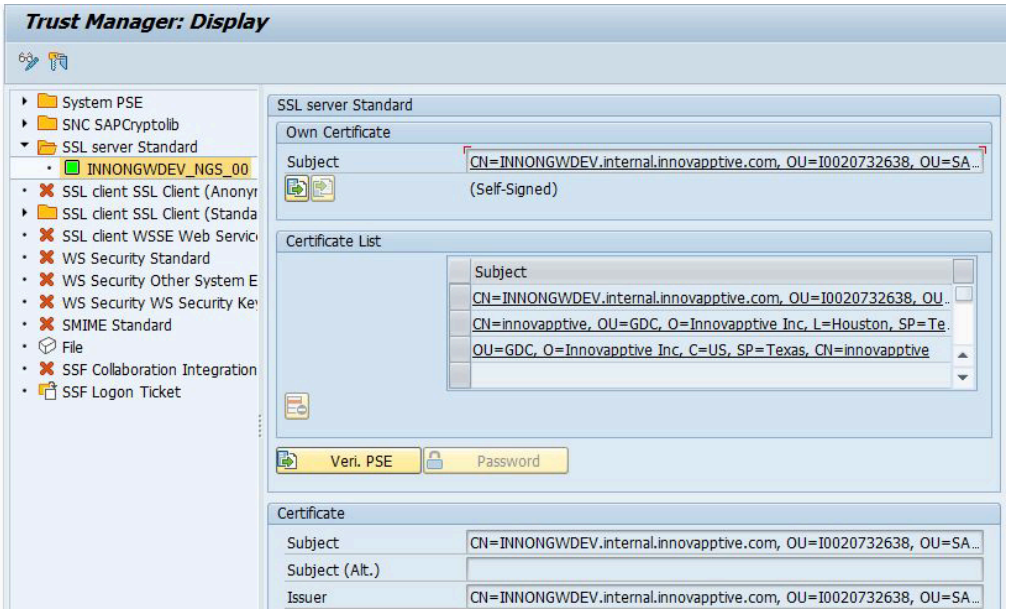
- CN=s0013927235, OU=Certification, O=SAP
- CN=S001392725, OU=Certification, O=SAP

2.5.5.10. Export SAP System Certificates to Cloud Connector

To export SSL Server certificate:

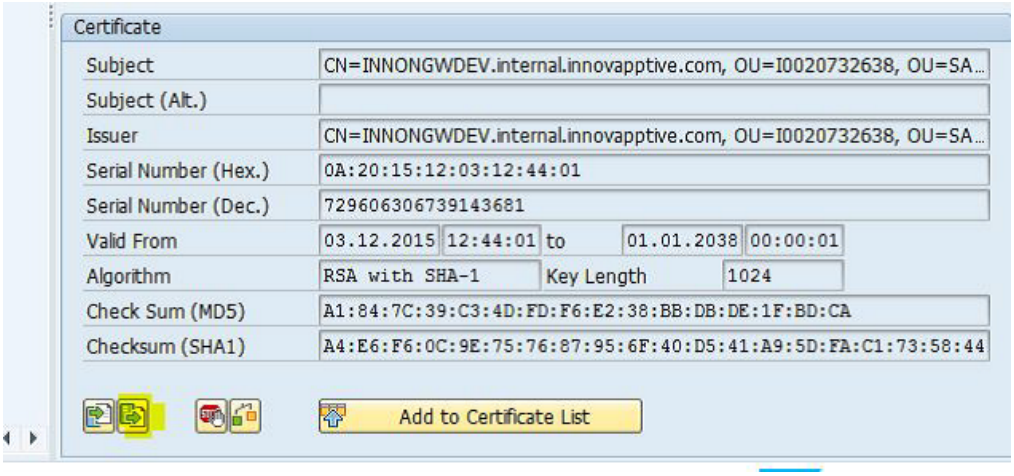
1. **Transaction code**: STRUST.
2. Open **SSL Server Standard** group and double click on the **certificate** node.

Figure 2-46 Trust Manager



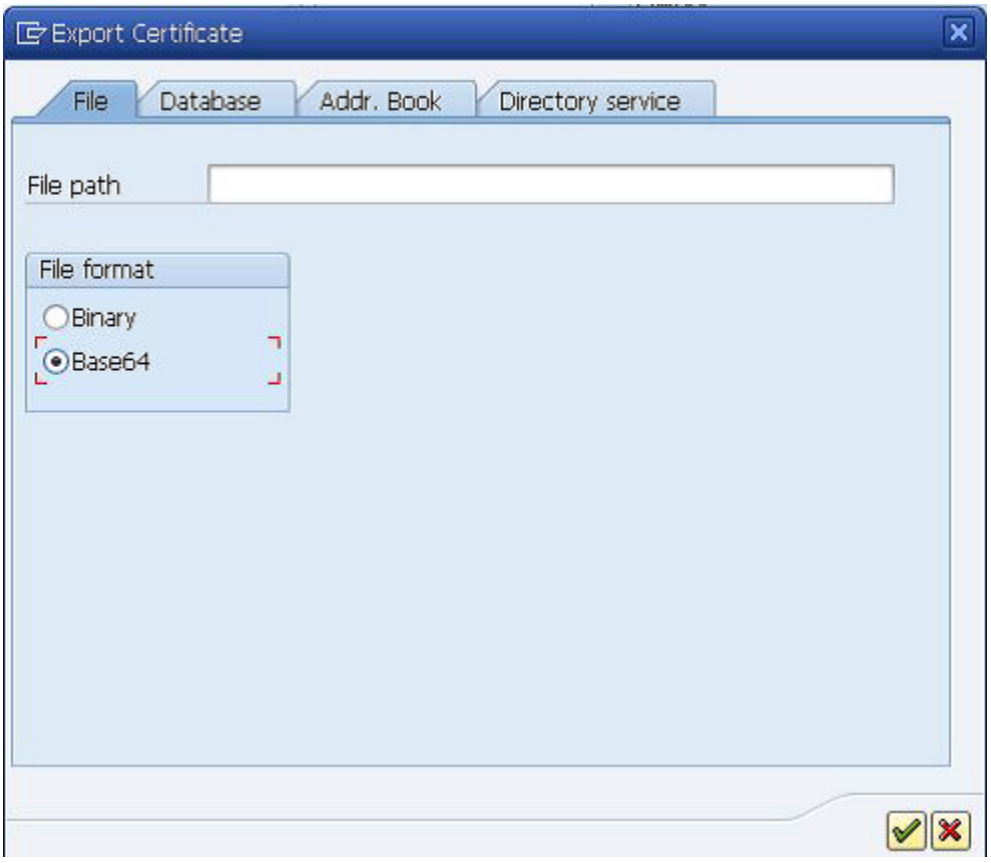
3. Double-click the Owner entry under **Own certificate** section and click **Export Certificate.**

Figure 2-47 Export Certificate



4. Save the certificate as **sed_ssl_server.crt**.

Figure 2-48 Export Certificate Path



5. Import the certificate to HCC trust store.

2.5.5.11. 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 **HCC_CA.cer** (HCC root certificate) file and click **Import**.
5. Click **Add to certificate list** to add the certificate to System PSE certificates list.

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

3. SMP Configurations before Installing Innovapptive Products

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

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

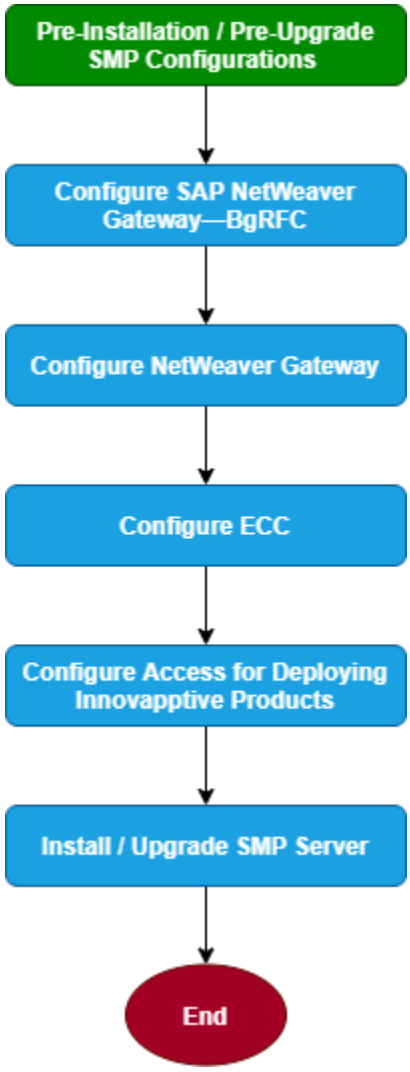


Table 3-1 Tasks for SMP Configurations before Instllaing Innovapptive Products

Task	Reference to section
Configure SAP NetWeaver Gateway—BgRFC	Configure SAP NetWeaver Gateway—BgRFC *(on page 11)*

Table 3-1 Tasks for SMP Configurations before Instllaing Innovapptive Products (continued)

Task	Reference to section
Configure NetWeaver Gateway	Configure NetWeaver Gateway *(on page 16)*
Configure ECC	Configure ECC *(on page 31)*
Configure Access for Deploying Innovapptive Products	Configure Access for Deploying Innovapptive Products *(on page 32)*
Install / Upgrade SMP Server	• Install SMP Server *(on page 102)* • Upgrade SMP Server *(on page 103)*

3.1. Configure SAP NetWeaver Gateway—BgRFC

This section helps you configure SAP NetWeaver Gateway—BgRFC

- Before you Configure SAP NetWeaver Gateway - BgRFC *(on page 11)*
- Create BgRFC Destination for Outbound Queues *(on page 12)*
- Register BgRFC Destination for Outbound Queue *(on page 13)*
- Create BgRFC Destination for Supervisor *(on page 15)*

3.1.1. 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, SMP/SCPms).
- SAP NetWeaver Gateway 7.4 and above with SAP_GWFND component (SP 10 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.

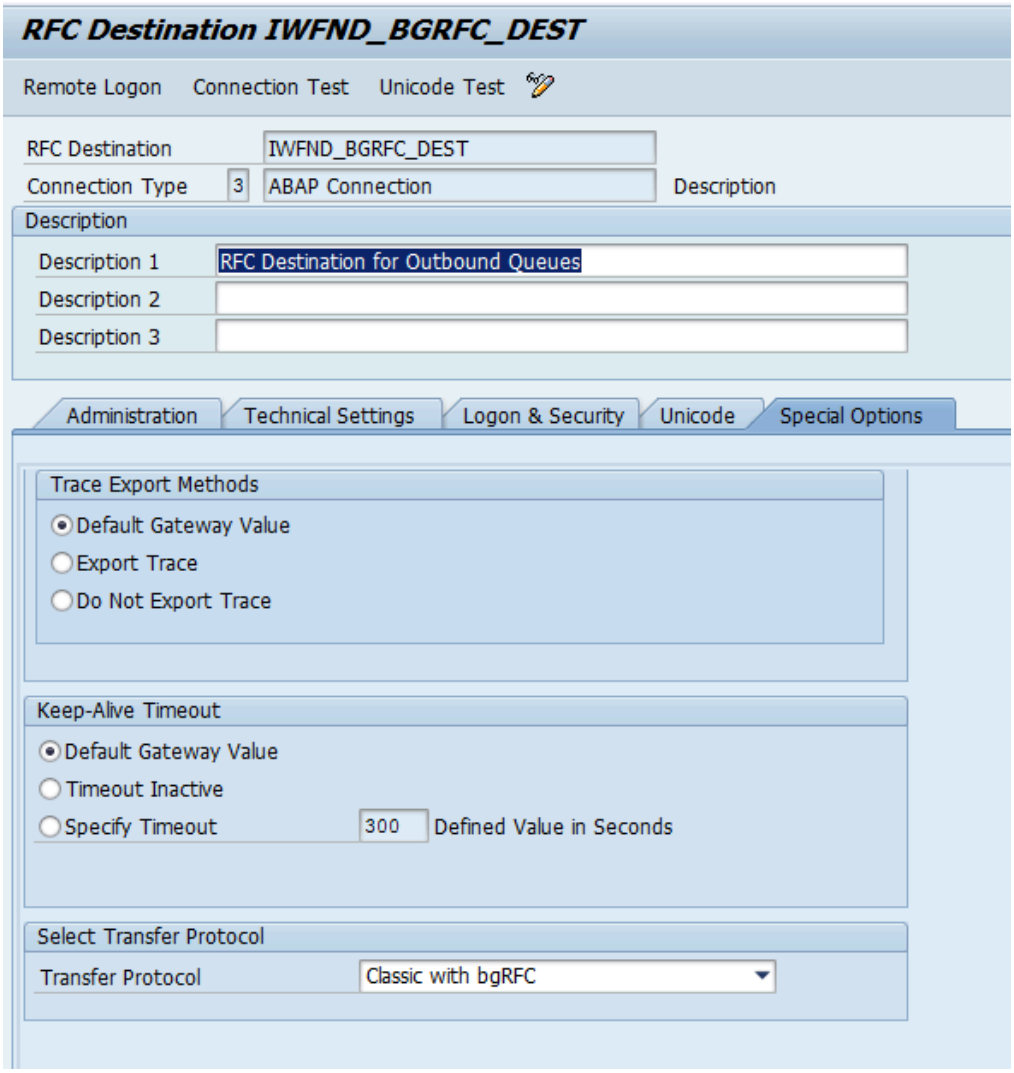
3.1.2. Create BgRFC Destination for Outbound Queues

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. For example **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**.

Figure 3-2 RFC Destination - Special Options tab



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

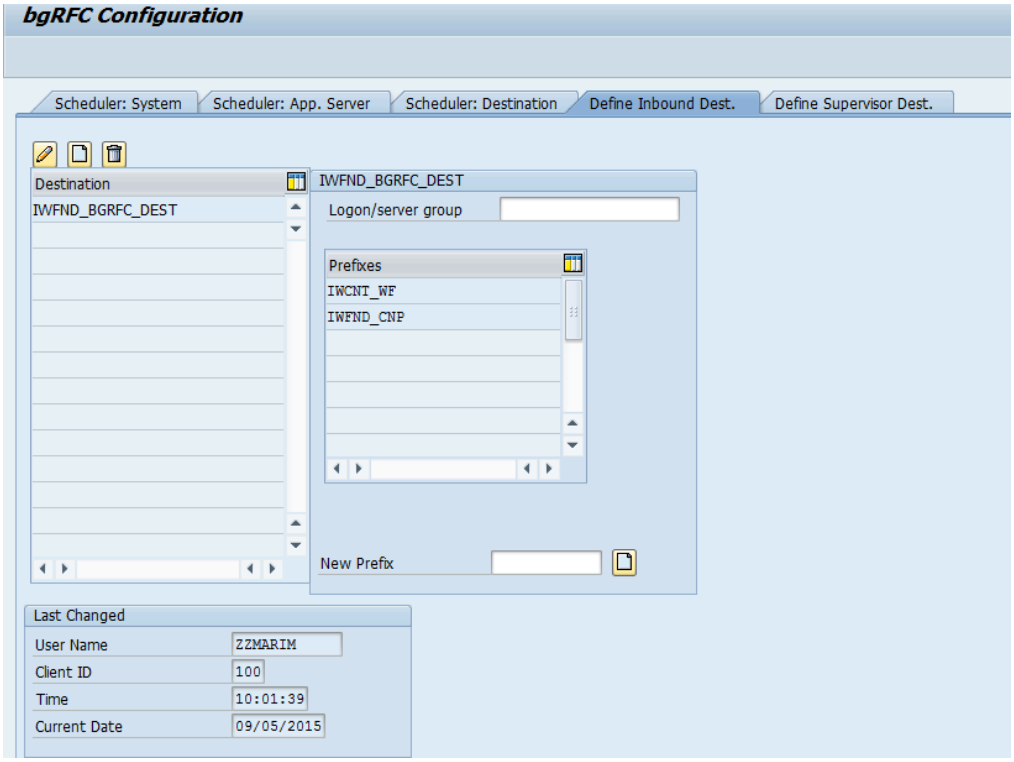
3.1.3. Register BgRFC Destination for Outbound Queue

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.

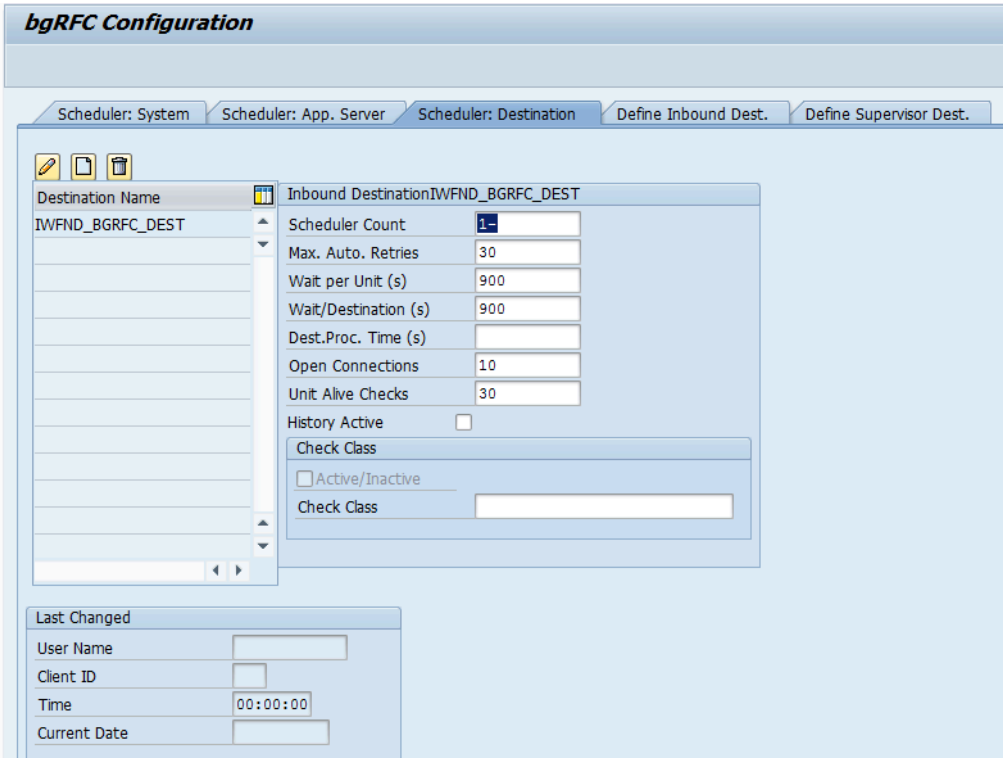
Figure 3-3 Define Inbound Destination



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**.

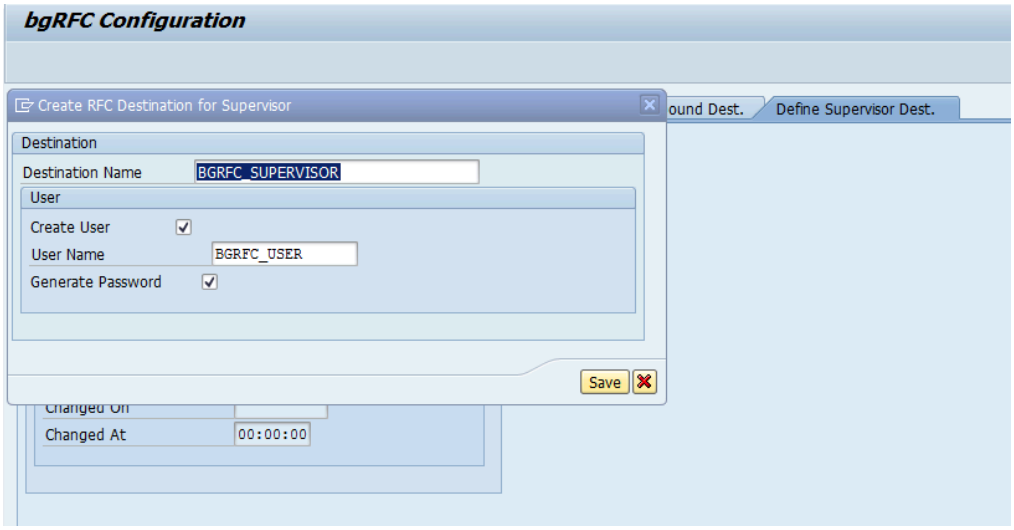
3.1.4. Create BgRFC Destination for Supervisor

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:

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 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**.

3.2. 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**
  - SAP ECC Business Suite is installed and connected to the mobile infrastructure (NetWeaver Gateway, SMP/SCPms).
  - SAP NetWeaver Gateway 7.4 and above with SAP_GWFND component (SP 10 and above) and SAP_UI component (SP 13 and above).
- **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.
- SMP/SCPms host and port details for creating RFC.
- SMP push user credentials.

- **Assumptions**

  Port number for HTTP = 8000 and HTTPS = 8080.

3.2.1. 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 SP08.

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

3.2.1.1. System Requirements

Hardware

Table 3-2 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 3-3 Software Prerequisites for NetWeaver Gateway

Requirement	Specification
SAP NetWeaver Stack	Apply the latest kernel patch for the SAP NetWeaver version.
	Core Component

Table 3-3 Software Prerequisites for NetWeaver Gateway (continued)

Requirement	Specification
	• SAP NetWeaver 7.40 SPS08 • SAP NetWeaver Gateway Foundation SAP_GWFND SP 10 **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.

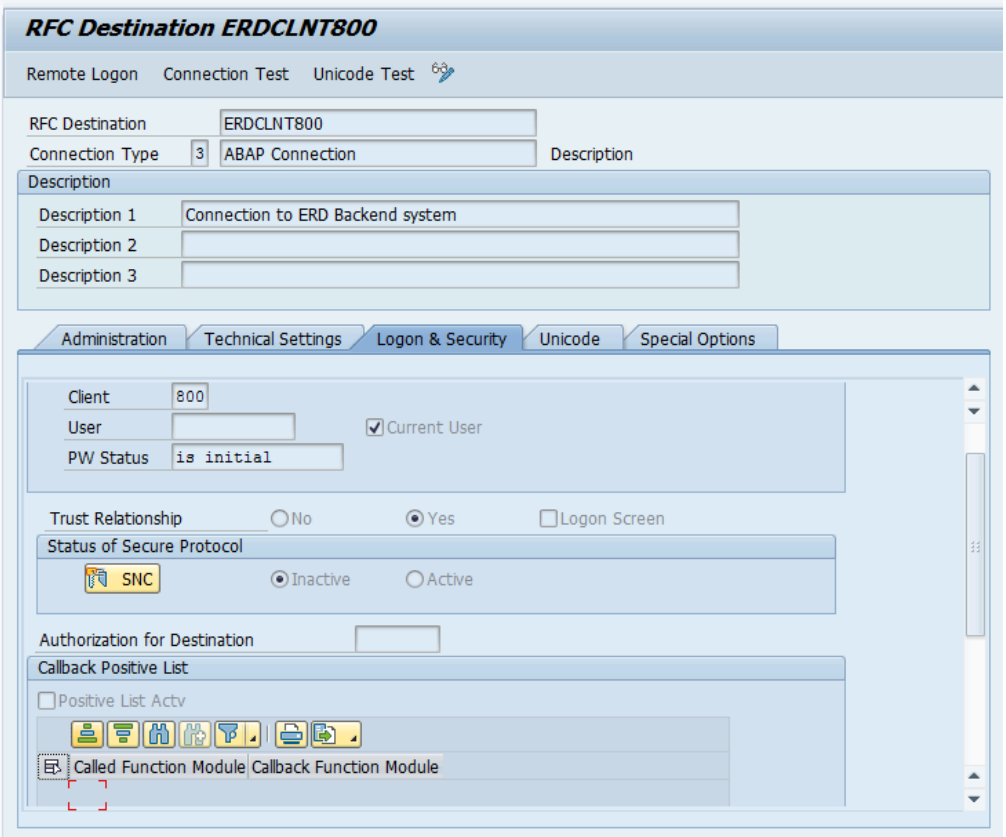
3.2.2. Establish trust between Gateway and ECC

Learn how to establish trust between Gateway and ECC.

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 3-6 RFC Destination

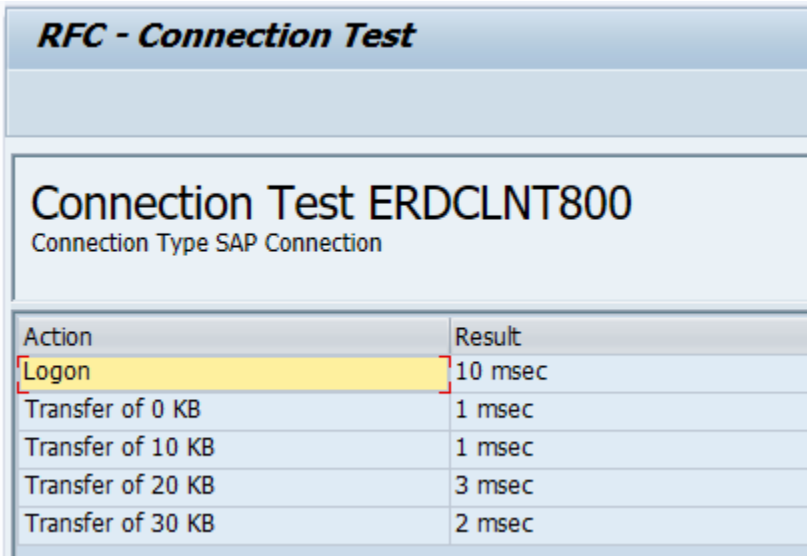


3. Enter **3** in the **Connection Type** field.
4. Enter description in the **Description 1** field. For example, **Connection to Backend System**.
5. Save your settings.
6. On the **Technical Settings** tab, select the option as per your system settings.
7. Enter the name of the SAP NetWeaver Gateway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

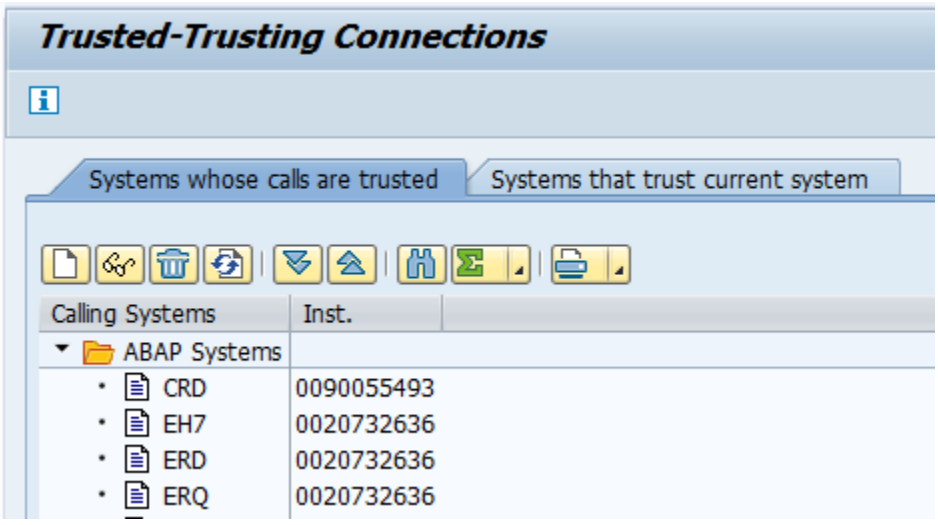
13. Save your settings.
14. Navigate to the **RFC** that you created in the previous step.
15. Select the current user on the **Logon & Security** tab.
16. Click **Yes**.
17. Save your settings.
18. Click **Connection Test**.

Figure 3-7 Connection Test



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

Figure 3-8 Trusted Calling Systems



3.2.3. 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:

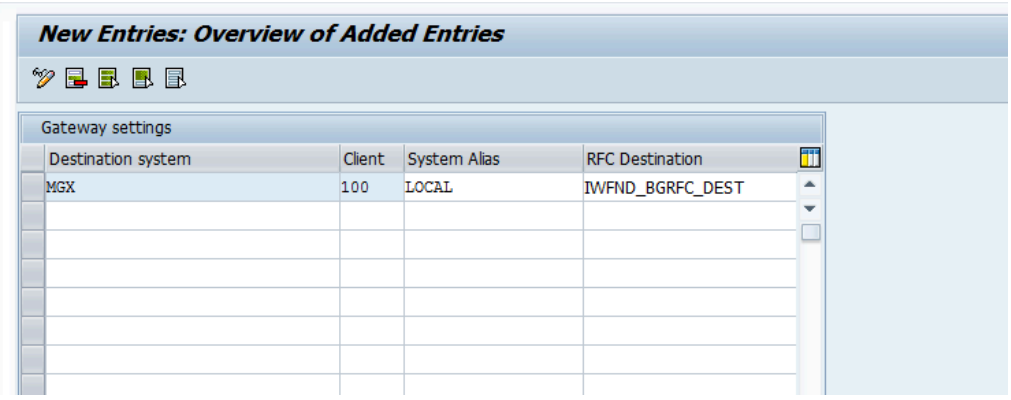
Before defining the connection settings, do the following:

- 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:** Host name of SAP NetWeaver Gateway.
    - **Client:** Client ID of the host of SAP NetWeaver Gateway. The client ID, you specify, must exist in the system.
    - **System Alias:** Unique name for the host of SAP NetWeaver Gateway.
    - **RFC Destination:** Name of the RFC destination to the host of SAP NetWeaver Gateway.

    Figure 3-9 Connection Settings: New Entries

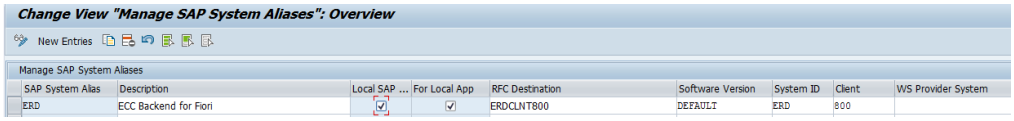
4. Save your settings.

3.2.4. 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.
    - **Description**: Descriptive text for the system alias.
    - **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.
    - 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.

3.2.5. 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.

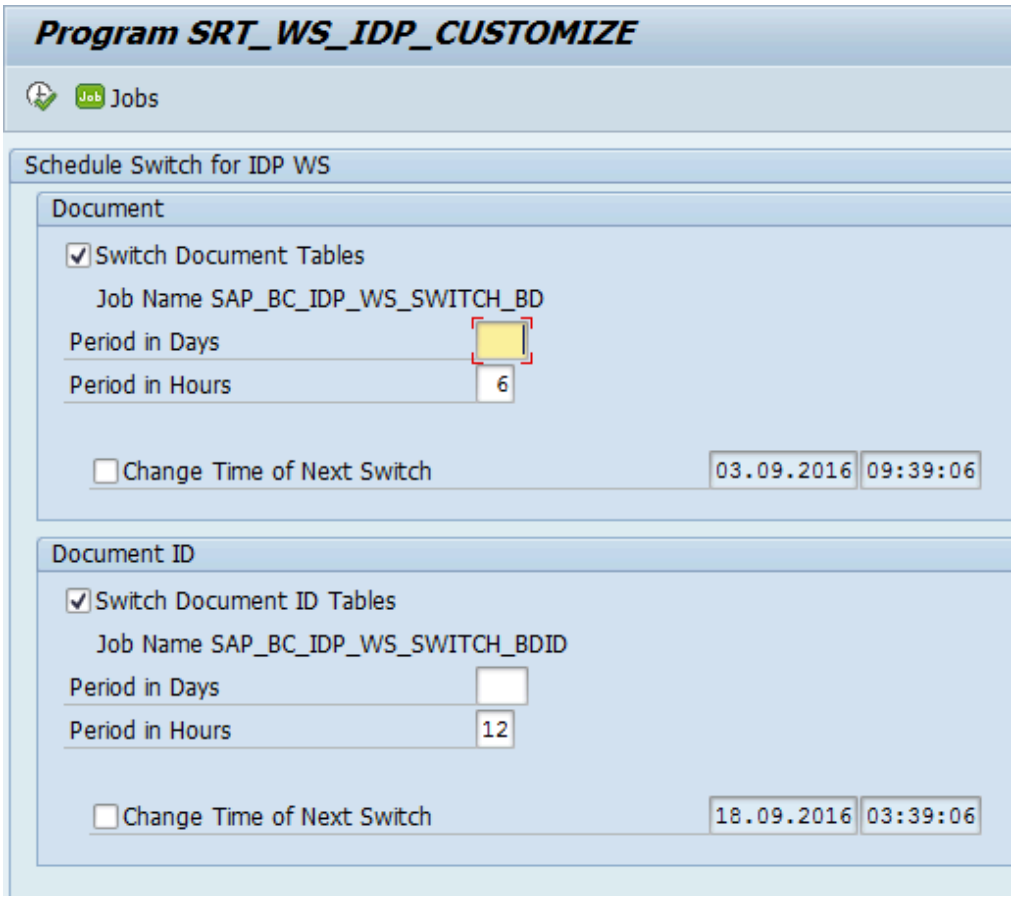
3.2.6. Define Settings for Idempotent Services

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 3-11 Idempotent Services Settings



6. Click **Continue**.

3.2.7. Set Profile Parametes 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 3-4 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

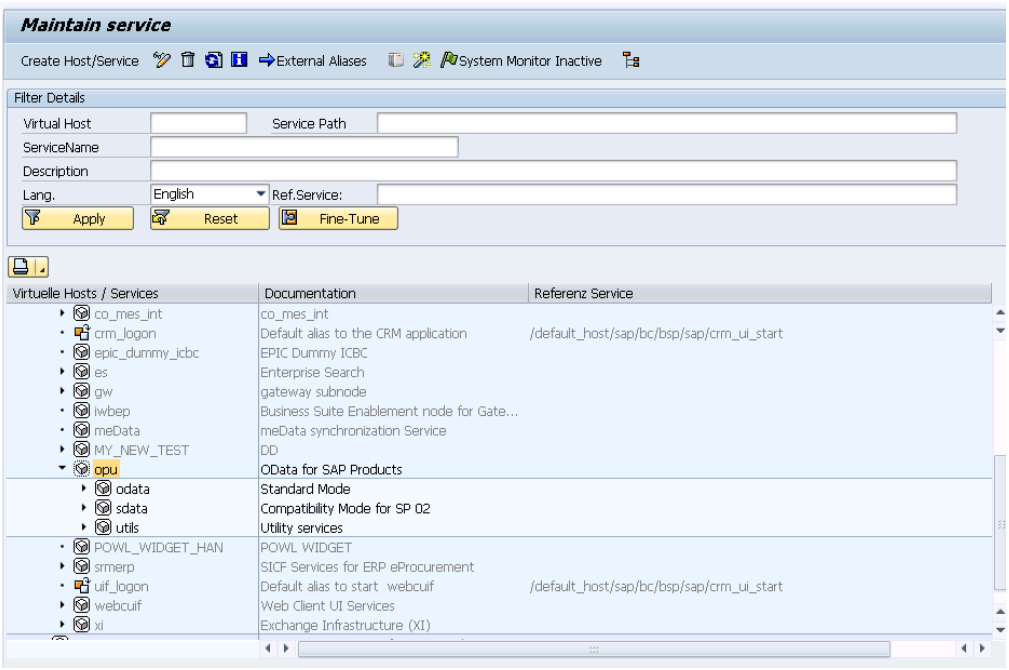
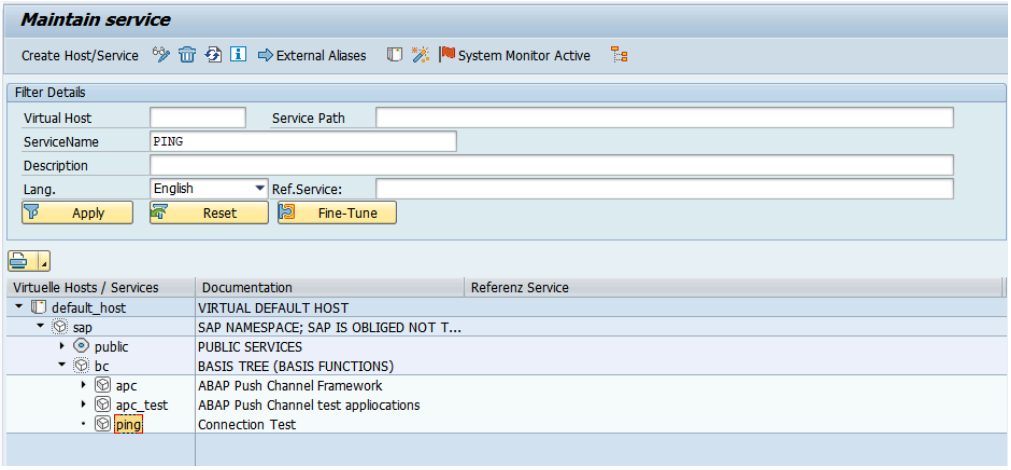


Figure 3-13 SICF: /sap/bc/ping

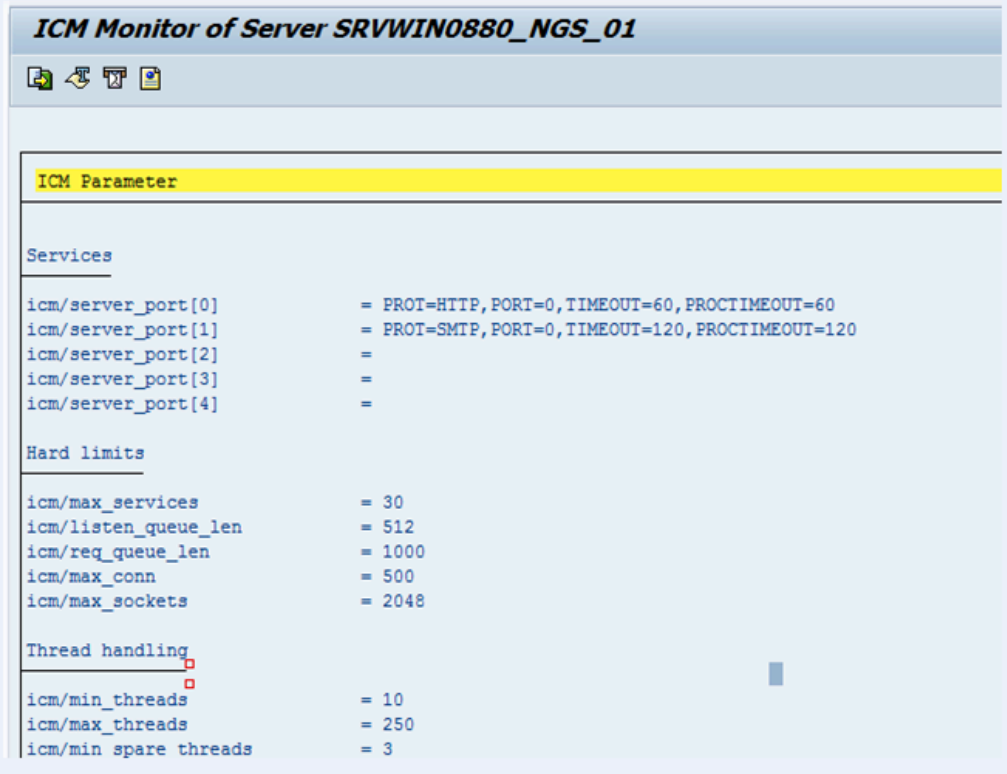


3.2.8. Maintain HTTPS and HTTP Connections

To maintain HTTPS and HTTP connections:

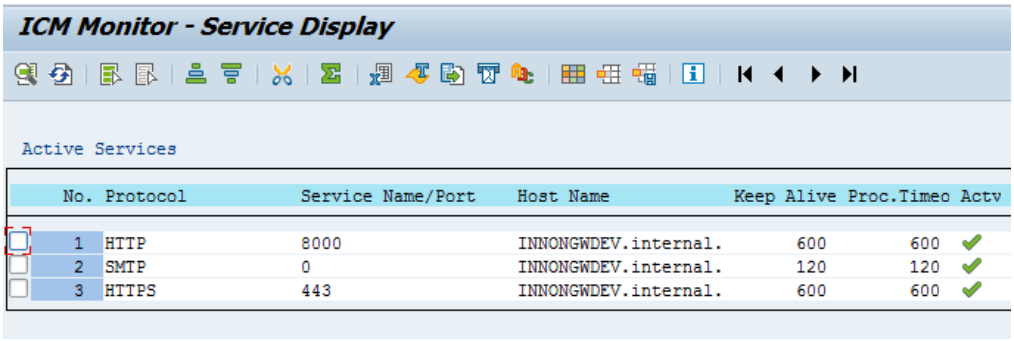
1. Run Tcode **RZ10** and set these parameters:
   - icm/server_port_0 = PROT=HTTP, PORT=8000, TIMEOUT=600, PROCTIMEOUT=600
   - icm/server_port_2 = PROT=HTTPS, PORT=8080, TIMEOUT=600, PROCTIMEOUT=600

Figure 3-14 ICM Parameters



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

Figure 3-15 ICM Monitor



3.2.9. 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.

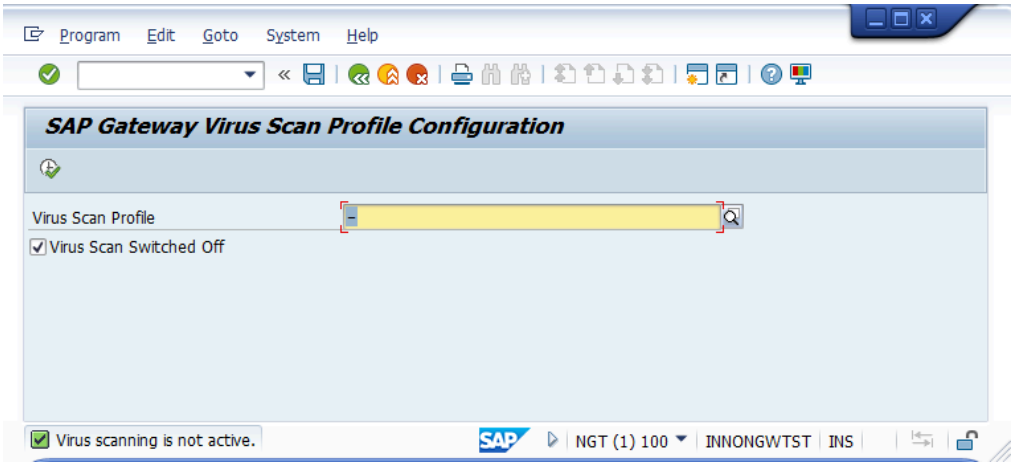
Note:
The Virus Scan must be enabled in Gateway only if the virus profile is defined.

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 3-16 Gateway Virus Scan Profile



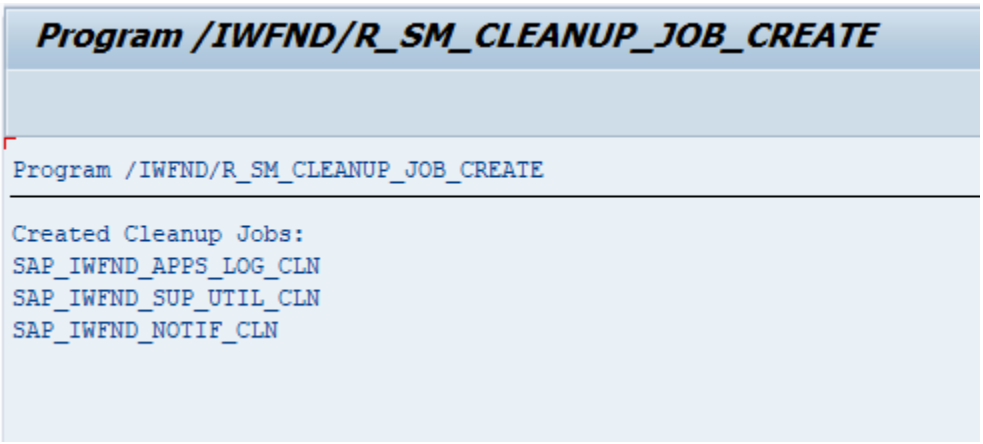
3.2.10. Create Periodical Tasks for Gateway

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 3-17 Gateway Cleanup tasks

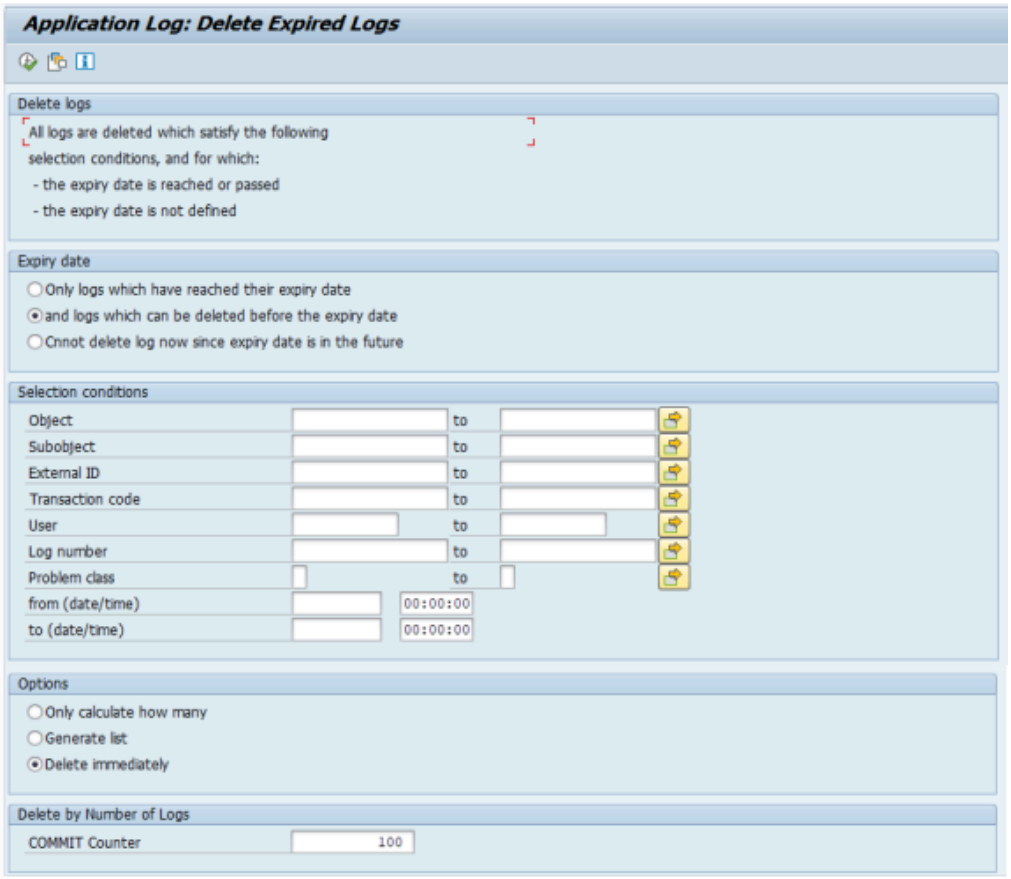


3.2.11. Clear Application Log Entries

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 3-18 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**.

3.2.12. 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 3-19 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**.

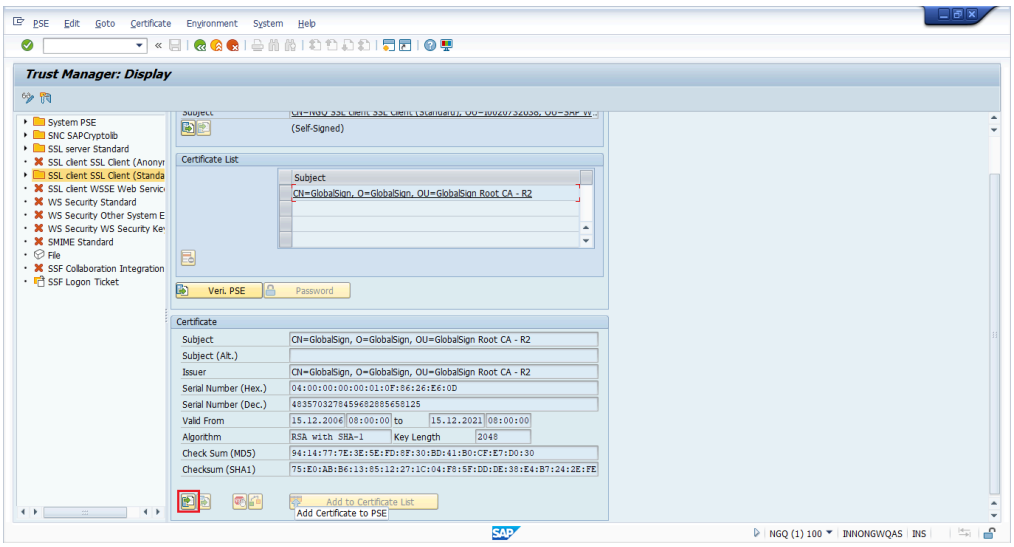
3.2.13. Install certificates for Geo location

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

To install the certificate:

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

Figure 3-20 Trust Manager



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

3.3. 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**.

3.4. 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 3-5 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,

Table 3-5 Roles on ECC System and transactions (continued)

Role Name	Role Description	User	Transactions
			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
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 3-6 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, /

Table 3-6 Roles on NetWeaver Gateway System and transactions (continued)

Role Name	Role Description	User	Transactions
			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, /IWBEP/CACHE_CLEANUP, SBGRFCMON, SBGRFCCONF, SBGRFCHIST, SBGRFCPERFMON, SBGRFCSCHEDMON.
ZINV_NWG_PRJ_SECURITY	Innovapptive - Project Role - Gateway Security	SAP Security Administrator	SU01, RSPFPAR, SPRO, PFCG, SUIM, SM30, SE16, ST01, SU53, SU56, SU21, SU03
ZINV_NWG_PRJ_CONFIGURATOR	AuthorizationsInnovapptive - Project Role - Gateway Configurator Authorizations	SAP Configurator	/IWBEP/*, /IWFND/*, SEGW, SE24, SE37, SE38, SSO2, SICF, SE16, SE11, SU01D, SU53, SBGRFCMON, SBGRFCCONF, SBGRFCHIST, SBGRFCPERFMON, SBGRFCSCHEDMON

3.4.1. Access Required for Configuring SMP

A user on the SMP System requires the following roles:

- SAP standard Administrator role in development environment.
- SAP Standard Help Desk role in non-development environment.

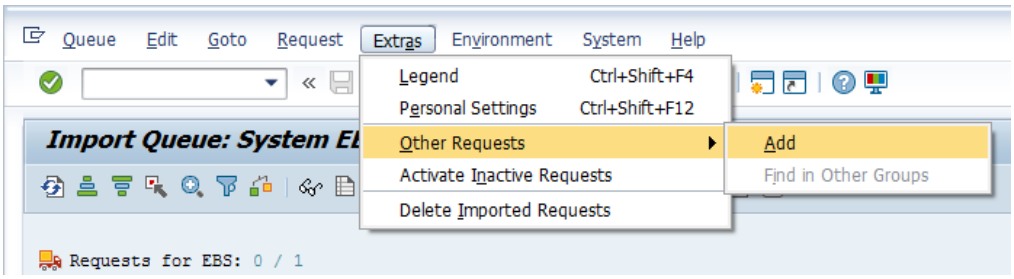
3.4.2. Import Roles Using Transports

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 3-21 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.

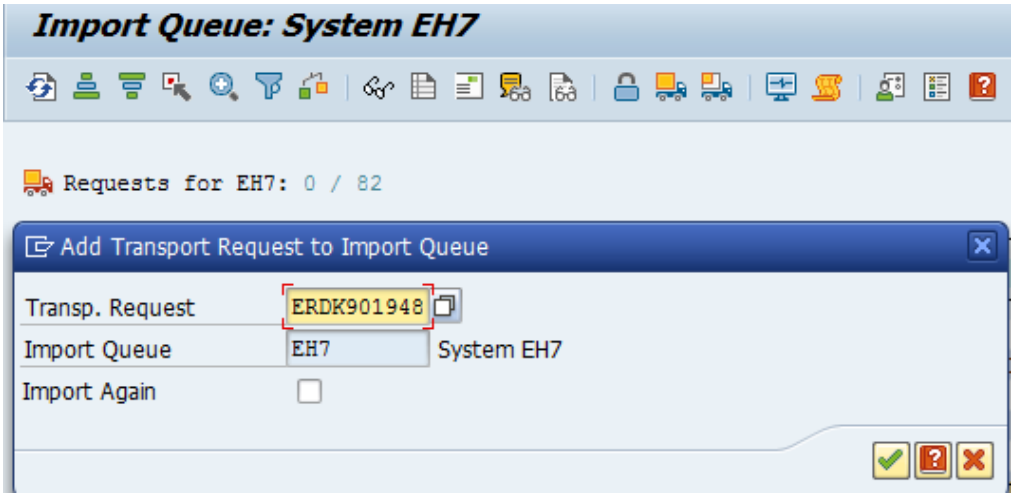
Table 3-7 SAP ECC Transports for Roles

Transport	Description	Dependency
ERDK904636	INNOV:ECC Project Team Roles	None

Table 3-8 SAP NWG Transports for Roles

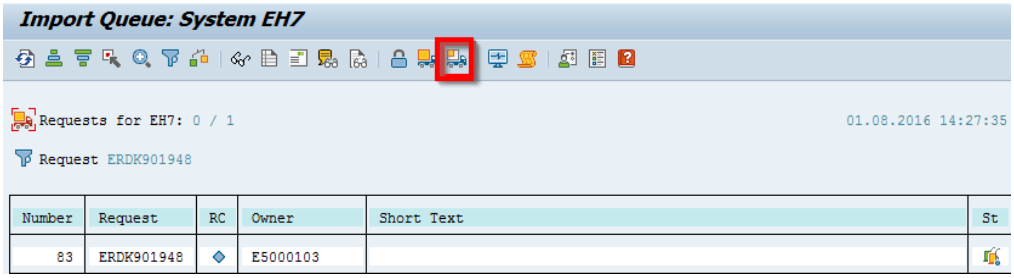
Transport	Description	Dependency
NGTK904332	INNOV:NWG Project Team Roles	None

Figure 3-22 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 3-23 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.

3.5. About SMP Server

SAP Mobile Platform (SMP) is a mobile enterprise application platform designed to simplify the task of creating applications that connect business data to mobile devices for workflow management and back-office integration. SMP provides a layer of middleware between heterogeneous back-end data sources, such as relational databases, enterprise applications and files, and the mobile devices that need to read and write back-end data.

If you are using SMP server or want to upgrade SMP server, follow the steps provided in this section:

- System Requirements for Installing SMP Server *(on page 100)*
- Install SMP Server *(on page 102)*
- Upgrade SMP Server *(on page 103)*

3.5.1. System Requirements for Installing SMP Server

To install the SMP server, ensure you have these minimum requirements:

System	Minimum Requirement
Processor	64-bit Intel Core2 Duo processor running at 2GHz or higher, or equivalent AMD processor
RAM	8GB
Disk Space for Installation	1.2GB

System	Minimum Requirement
Disk Space required for Server Database	50GB
Web browsers for Management Cockpit	**Windows**: • Internet Explorer 10 and later • Mozilla Firefox 10.x • Google Chrome 20 and later
	Mac: Safari 5.1 and later
JDK	SAP JVM 7 is required for SMP Java components, including the SMP Management API.
Reverse Proxy	SMP is compatible with HTTP/HTTPS reverse proxies that support X.509 (if required), cookie and header propagation, Web Sockets, and session affinity. SMP is tested with these proxies: • BigIP F5 • Citrix NetScaler 10.5 • Apache 2.4 • SAP Web Dispatcher 7.42 • SMP Relay Server 16.5.3 (as of SMP v3.0 SP06)
Afaria Server	Version 7 SP1, Hot Fix 8 and above
LDAP Servers	These servers are certified for use with SMP: • Microsoft Windows Server 2008 R2 Active Directory • Microsoft Windows Server 2012 R2 Active Directory • OpenDS 2.2 Update 1
Virtual Machine Support	SAP supports SMP running in a virtual machine if:

System	Minimum Requirement
	• The virtual machine is officially certified and approved by the operating system platform vendor. • The operating system running in the virtual machine is certified by SAP. • The hardware resources within the virtualization system are maintained as per the vendor recommendation.

3.5.2. Install SMP Server

Verify that the host on which you are installing SAP Mobile Platform (SMP) meets the prerequisites and you have Administrator access.

SAP Mobile Platform installer sets up the internal SAP SQL Anywhere database while installing the server.

To install the SMP Server:

1. Browse to the root directory of the SAP Mobile Platform installer.
   Default path is: **C:\installations\SMP\SAPSMPRT3010_0-20011876\ebf25654\SMP3ServerInstaller-win-3.0.10.0-1.**
2. Right-click the **setupAMD64.exe** and select **Run as Administrator**.
3. On the welcome screen, click **Next**.
4. On the End-user license agreement screen, select your **Country** and accept the terms of license agreement.
5. Click **Next**.
6. Enter the directory path for installation.
   Click **Browse** to select the folder.

   Note:
   - The total length of the path must be equal to or less than 38 characters.
   - Directory names in the path can contain only ASCII alphanumeric characters.
   - Underscore (_), hyphen (-), and period (.) characters. Two consecutive period characters are not allowed, and none of these characters may appear as the first character in a folder name
7. Select **Developer installation** you are installing a single-server development system and click **Next**.

To set up SMP using other database, select **Production installation**.

8. Select **Use the default SAP SQLAnywhere embedded database**.
   To use another database, select **Use another database you have already installed** and enter the database information such as **Host Name**, **Port number**, **Login**, **Password** and **Database Name**.

   > **Note:**
   > SMP 3.0 is compatible with SAP HANA, SAP ASE, DB2, Oracle and Microsoft SQL Server.

9. Click **Next**.
10. Enter the Keystore password and Admin username and password.

    > **Note:**
    > - For the Admin and Keystore passwords, only alphabetic and numeric characters, space, period, colon, dash, and hyphen are allowed.
    > - Keystore password is required when adding the Reverse Proxy SSL certificate in SMP trust store.

11. Click **Next**.
12. Enter HTTP, HTTPS, HTTPS mutual SSL port, and HTTPS admin port numbers.
13. Click **Next**.
14. Enter **Windows account name** and **password**.
    Create a user (for example, **smpServiceUser**) on the local system, to start/stop the SMP services/processes.
15. Click **Next**.
16. Click **Install**.
17. Select the MBO Runtime installer check box and enter the path of the .zip file to launch the installer after SMP is installed. This is an optional step.
18. Click **Finish** to start the SAP Mobile Platform Server Service.
    Access SMP Admin URL: https://<SMP Server host>:8083/Admin/ and enter the Admin username and password as specified during installation.

3.5.2.1. Upgrade SMP Server

If the version of SMP server that you are using do not match with the System Requirements for Installing SMP Server *(on page 100)* upgrade your SMP server.

To upgrade SMP Server

1. Go to SMP Server Installer folder.
   Default path is: C:\installations\SMP
   \SAPSMPRT3010P_1-20011876\ebf25741\SMP3ServerInstaller-win-3.0.10.1-1
2. Right-click **setupAMD64.exe** and select **Run as administrator**.
3. Click **Next**.
4. Click **Next**.
5. Enter password for **smpServiceUser** and click **Next**.
6. Click **Upgrade**.
7. Select the MBO Runtime installer check box and enter the path of the .zip file to launch the installer after SMP is installed. This is an optional step.
8. Click **Finish**.