## Pre-Install or Pre-Upgrade Configurations Guide 2009

**Connected Worker Solutions** 



Copyright © 2012-2021, Innovapptive Inc. and/or its affiliates. All rights reserved

## 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*<sup>TM</sup>.

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

Product Version: 2009

Document Version: 1.0

Published Date: 19 November 2020

Copyright © 2020, Innovapptive Inc. and/or its affiliates. All rights reserved.

Primary Author: Innovapptive Inc.

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

## Preface

Understand audience and conventions followed in this document.

#### Audience

This guide is for technical configurators who do e configurations for mAssetTag, mWorkOrder, mInventory, mServiceOrder, mWorkList and other solutions of *Connected Workforce Platform*<sup>TM</sup>.

#### **Document Conventions**

Convention	Meaning
boldface	Indicates graphical user interface ele- ments associated with an action, or terms defined in text or the glossary.
italic	Indicates book titles, emphasis, or place- holder variables for which you supply val- ues.
monospace	Indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

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

#### **Related Products**

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

#### **Contact Innovapptive**

For information on Innovapptive products, visit the Innovapptive's Support Portal at http:// helpdesk.innovapptive.com. The updates to this document are published on this support portal. Check this website periodically for updated documentation.

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

## Contents

Title and Copyright	2
Preface	3
1. Pre-Install or Pre-Upgrade Configurations for Innovapptive Products	8
2. SCP Configurations before Installing Innovapptive Products	10
2.1. Configure SAP NetWeaver Gateway—BgRFC	11
2.1.1. Before you Configure SAP NetWeaver Gateway - BgRFC	11
2.1.2. Create BgRFC Destination for Outbound Queues	12
2.1.3. Register BgRFC Destination for Outbound Queue	13
2.1.4. Create BgRFC Destination for Supervisor	15
2.2. Configure NetWeaver Gateway	16
2.2.1. Install SAP NetWeaver Gateway	17
2.2.2. Establish trust between Gateway and ECC	18
2.2.3. Define Connection Settings to SAP NetWeaver Gateway	21
2.2.4. Create the SAP System Alias for Applications	
2.2.5. Activate SAP NetWeaver Gateway	22
2.2.6. Define Settings for Idempotent Services	22
2.2.7. Set Profile Parametes in SAP NetWeaver Gateway	23
2.2.8. Maintain HTTPS and HTTP Connections	25
2.2.9. Configure SAP Gateway virus scan profile	27
2.2.10. Create Periodical Tasks for Gateway	27
2.2.11. Clear Application Log Entries	28
2.2.12. Clear Query Result Log Entries	29
2.2.13. Install certificates for Geo location	30
2.3. Configure ECC	
2.4. Configure Access for Deploying Innovapptive Products	32
2.4.1. Access Required for Configuring SCP	34
2.4.2. Import Roles Using Transports	35

	2.5. Configur SCP for Deploying Innovapptive Products	37
	2.5.1. All About SCP Data Center	
	2.5.2. Validate access to SCP	38
	2.5.3. Enable Mobile Services	41
	2.5.4. Install and Configure Cloud Connector	43
	2.5.5. Establish trust between SCP, Cloud Connector and SAP Gateway	53
3	3. SMP Configurations before Installing Innovapptive Products	73
	3.1. Configure SAP NetWeaver Gateway–BgRFC	74
	3.1.1. Before you Configure SAP NetWeaver Gateway - BgRFC	74
	3.1.2. Create BgRFC Destination for Outbound Queues	75
	3.1.3. Register BgRFC Destination for Outbound Queue	76
	3.1.4. Create BgRFC Destination for Supervisor	78
	3.2. Configure NetWeaver Gateway	79
	3.2.1. Install SAP NetWeaver Gateway	80
	3.2.2. Establish trust between Gateway and ECC	
	3.2.3. Define Connection Settings to SAP NetWeaver Gateway	84
	3.2.4. Create the SAP System Alias for Applications	
	3.2.5. Activate SAP NetWeaver Gateway	
	3.2.6. Define Settings for Idempotent Services	85
	3.2.7. Set Profile Parametes in SAP NetWeaver Gateway	
	3.2.8. Maintain HTTPS and HTTP Connections	
	3.2.9. Configure SAP Gateway virus scan profile	90
	3.2.10. Create Periodical Tasks for Gateway	90
	3.2.11. Clear Application Log Entries	91
	3.2.12. Clear Query Result Log Entries	
	3.2.13. Install certificates for Geo location	93
	3.3. Configure ECC	
	3.4. Configure Access for Deploying Innovapptive Products	
	3.4.1. Access Required for Configuring SMP	

	3.4.2. Import Roles Using Transports	.98
3.5.	About SMP Server	100
	3.5.1. System Requirements for Installing SMP Server	100
	3.5.2. Install SMP Server	102

# 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:

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

## 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.





#### 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)

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

Task	Reference to section
Configure NetWeaver Gateway	Configure NetWeaver Gateway <i>(on page 16)</i>
Configure ECC	Configure ECC (on page 31)
Configure Access for Deploying Innovapp- tive Products	Configure Access for Deploying Innovapp- tive Products <i>(on page 32)</i>
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 Connec- tor (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.

DEC Dectionst	
KPC Destinati	ion IWFND_BGRFC_DEST
Remote Logon Co	nnection Test Unicode Test 💖
RFC Destination	IWFND_BGRFC_DEST
Connection Type	3 ABAP Connection Description
Description	
Description 1	RFC Destination for Outbound Queues
Description 2	
Description 3	
Administration	Technical Settings Logon & Security Unicode Special Options
OExport Trace ODo Not Export	Trace
OExport Trace ODo Not Export Keep-Alive Timeout	Trace
<ul> <li>Export Trace</li> <li>Do Not Export</li> <li>Keep-Alive Timeout</li> <li>Default Gateway</li> <li>Timeout Inactive</li> </ul>	Trace
<ul> <li>Export Trace</li> <li>Do Not Export</li> <li>Keep-Alive Timeout</li> <li>Default Gateway</li> <li>Timeout Inactive</li> <li>Specify Timeout</li> </ul>	Trace t t Y Value e S 300 Defined Value in Seconds
Export Trace     Do Not Export     Keep-Alive Timeout     Oefault Gateway     Timeout Inactive     Specify Timeout     Select Transfer Pro	Trace t t Y Value e Solution Defined Value in Seconds ttocol

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

bgRFC Configuration		
Scheduler: System Scheduler:	App. Server Scheduler: Destination Define Inbound Dest. Define Supervisor Dest.	
Dectination	TWEND BGREC DEST	
IWFND_BORFC_DEST		
	IWCNT_WF	
	IWFND_CNP "	
	· · · · · · · · · · · · · · · · · · ·	
4 5	New Prefix	
Last Changed		
User Name ZZMAR:	IM	
Client ID 100		
Time 10:01:	:39	
Current Date 09/05,	/2015	

- 5. Enter IWFND\_BGRFC\_DEST in the Inb. Dest. Name field and click <Enter>.
- 6. In the **New Prefix** field, create entries, for example **IWFND\_CNP** and **IWCNT\_WF** and save the settings.

- | 2 SCP Configurations before Installing Innovapptive Products
  - 7. Click Create on the Scheduler: Destination tab.

Figure 2-4 Scheduler: D	Destination tab
-------------------------	-----------------

Scheduler Count Max. Auto. Retries Wait per Unit (s)	1- 30 900		
Max. Auto. Retries Wait per Unit (s)	30		
Wait per Unit (s)	900		
wate per one (5)	200		
Wait/Destination (s)	900		
Dest.Proc. Time (s)			
Open Connections	10		
Unit Alive Checks	30		
History Active			
Check Class			
Active/Inactive			
Check Class			
	Dest.Proc. Time (s) Open Connections Unit Alive Checks History Active Check Class Active/Inactive Check Class	Dest.Proc. Time (s) Open Connections 10 Unit Alive Checks 30 History Active Check Class Active/Inactive Check Class	Dest.Proc. Time (s) Open Connections 10 Unit Alive Checks 30 History Active Check Class Check Class Check Class

- 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

bgRFC Configuration		
Create RFC Destination for Supervisor	×	ound Dest. Define Supervisor Dest.
Destination		
Destination Name BGRFC_SUPERVISOR		
User		
Create User		
User Name BGRFC_USER		
Generate Password 🗸		
Save	×	
Changeu On		
Changed At 00:00:00		

- 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) addon. 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		

Requirement	Specification			
	<ul> <li>SAP NetWeaver 7.40 SPS08</li> <li>SAP NetWeaver Gateway Foundation SAP_GWFND SP 10</li> </ul>			
	Note: Comprises functional scope of components IW_FND, GW_CORE, IW_BEP, and IW HDB.			
SAP Backend	SAP Business Suite system			

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

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.

RFC Destination ERDCLNT800	
Remote Logon Connection Test Unicode Test 🥱	
RFC Destination     ERDCLNT800       Connection Type     3     ABAP Connection       Description     Description	
Description 1       Connection to ERD Backend system         Description 2	
Client 800 User Current User PW Status is initial	•
Trust Relationship ONo   Yes Logon Screen	
Status of Secure Protocol	
Authorization for Destination Callback Positive List Positive List Actv	
	* *

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

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

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

Trusted-Trusting Connections							
<b>i</b>							
Systems whose calls are trusted Systems that trust current system							
► <							
Calling Systems	Inst.						
ABAP Systems							
• 🖹 CRD	0090055493						
• 🖹 EH7	• 🖹 EH7 0020732636						
• 🖹 ERD	0020732636						
• 🖹 ERQ	0020732636						

## 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:

- 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

New Entries: Overview of Added Entries								
1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2								
Gateway settings								
Destination system	Client	System Alias	RFC Destination					
MGX	100	LOCAL	IWFND_BGRFC_DEST	-				
				-				

4. Save your settings.

## 2.2.4. Create the SAP System Alias for Applications

To create the SAP system Alias for applications:

- 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

	Change View "Manage SAP System Aliases": Overview								
🦻 New Entries 🗅 🗟 🕫 🗒 🖉 🖡									
	Manage SAP System Alases								
	SAP System Alias	Description	Local SAP	For Local App	RFC Destination	Software Version	System ID	Client	WS Provider System
	FPD	ECC Rackand for Fiori			ERDCI NITROO	DEFAILT	FPD	800	

5. Save your settings.

## 2.2.5. Activate SAP NetWeaver Gateway

To activate the SAP NetWeaver Gateway:

- 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:

- 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

Program SRT_WS_IDP_CUSTOMIZE	
🕼 🔤 Jobs	
Schedule Switch for IDP WS	
Document	
✓ Switch Document Tables	
Job Name SAP_BC_IDP_WS_SWITCH_BD	
Period in Days	
Period in Hours 6	
Change Time of Next Switch	03.09.2016 09:39:06
Document ID	
Switch Document ID Tables	
Job Name SAP_BC_IDP_WS_SWITCH_BDID	
Period in Days	
Period in Hours 12	
Change Time of Next Switch	18.09.2016 03:39:06

6. Click **Continue**.

### 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 belowmentioned 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

Maintain service					
Create Host/Service	😚 📅 🔁 🗓 🔿 External Aliases 🛛 🛛 🎊 🍋 System Monitor Active 📑				
Filter Details					
Virtual Host	Service Path				
ServiceName	PING				
Description					
Lang.	English Ref.Service:				
P Apply	Reset Pine-Tune				
Virtuelle Hosts / Service	es Documentation Referenz Service				
default_host	VIRTUAL DEFAULT HOST				
▼ 🛇 sap	Sap SAP NAMESPACE; SAP IS OBLIGED NOT T				
🕨 💿 public	S public PUBLIC SERVICES				
• 🛇 bc	O bc BASIS TREE (BASIS FUNCTIONS)				
🕨 🐨 P	apc ABAP Push Channel Framework				
<ul> <li> <u> <u> </u></u></li></ul>	▶ ⓒ apc_test ABAP Push Channel test appliocations				
• 🔞 ping Connection Test					

## 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

ICM Monitor of Server SRVWIN0880_NGS_01			
🞝 🖑 📅 📔			
ICM Parameter			
Services			
Services			
icm/server port[0]	= PROT=HTTP, PORT=0, TIMEOUT=60, PROCTIMEOUT=60		
icm/server port[1]	= PROT=SMTP, PORT=0, TIMEOUT=120, PROCTIMEOUT=120		
icm/server port[2]	=		
<pre>icm/server_port[3]</pre>	=		
<pre>icm/server_port[4]</pre>	-		
Hard limits			
<pre>icm/max_services</pre>	= 30		
icm/listen_queue_len	= 512		
icm/req_queue_len	= 1000		
icm/max_conn	= 500		
icm/max_sockets	= 2048		
Thread handling			
icm/min_threads	= 10		
icm/max_threads	= 250		
ICM/MIN spare threads	= 5		

- 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

IC	ICM Monitor - Service Display						
9	<b>3</b>	B B   🚢 Ŧ	🔀   🗵   🐙 🝜 🔯	🍋   🎟 🖽 🖷   🗓	4 ◆ ▶	M	
Act	tive S	Services					
	No.	Protocol	Service Name/Port	Host Name	Keep Alive	Proc.Timeo Actv	
	1	HTTP	8000	INNONGWDEV.internal.	600	600 🗹	
	2	SMTP	0	INNONGWDEV.internal.	120	120 🖌	
	3	HTTPS	443	INNONGWDFV internal	600	600 🖌	

## 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.

$\left( \right)$	Note:
l	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

년 Program Edit Goto System	Help	
🔮 🔍 👻 🧧	। 🗟 🚱 । 🚍 🛗 👘 👘 🕮 🗘 🖓 💭 💭 🔛 -	
SAP Gateway Virus Scan I	Profile Configuration	
•		
Virus Scan Profile	<u>-</u>	
✓ Virus Scan Switched Off		
Virus scanning is not active.	SAP 👂 NGT (1) 100 👻 INNONGWTST 🗄	INS 🛛 🔄 🔓

## 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:

- 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

Program /IWFND/R_SM_CLEANUP_JOB_CREATE
Program /IWFND/R_SM_CLEANUP_JOB_CREATE
Created Cleanup Jobs: SAP_IWFND_APPS_LOG_CLN SAP_IWFND_SUP_UTIL_CLN SAP_IWFND_NOTIF_CLN

## 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 L	og Entries Criteria
---------------------	---------------------

Application Log: Delete Expired Logs					
🍄 🥵 🗓					
Delete logs					
All logs are deleted which satisfy the fol selection conditions, and for which: - the expiry date is reached or passed - the expiry date is not defined	owing				
Expiry date					
<ul> <li>Only logs which have reached their e</li> <li>and logs which can be deleted before</li> <li>Cnnot delete log now since expiry data</li> </ul>	xpiry date a the expiry date te is in the future				
Selection conditions					
Object		to			
Subobject		to			
External ID		to		<u> </u>	
Transaction code		to		<u> </u>	
User		to		<u></u>	
Log number		to		<u> </u>	
Problem class		to		<u> </u>	
from (date/time)	00	0:00:00			
to (date/time)	00	:00:00			
Options					
Only calculate how many					
Generate list     Oelete immediately					
Delete by Number of Logs					
COMMIT Counter	100				

- 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

Cleanup of Query Result Lo	g
⊕ <sup>6</sup>	
Selection Parameters	
Records Older Than (in Hours)	168
✓ Delete Log Headers	
Control Parameters	
Execute in Test Mode	

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

## 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

면 pse Edit Goto Certificat	e En <u>v</u> ironment S <u>v</u> stem	Нер	
🖉 🔹 🔹	M 🕹 I 😒 😒 🥵 I 🖶	🖞   \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	
Trust Manager: Display	<b>/</b>		
9 m			
System PSE     Sic SAPCrystolb     Sic SAPCrystolb     Sic SAPCrystolb     Sic SaPCrystolb     Sic Saret Standard     W SSL dent SSL Cleft Change     Sic Sale SSL Cleft Standard     W SSecurity Standard     W SSecurity Standard     W SSecurity Other System     Sic Sale Standard     Grie     Sic Sale Standard     Golden Standard     Sic Scholboration Integration     Giss Loopon Ticket	augessi Certificate List	Isan-Hood Jak Lemin Jak Lemin Jakensen (Jakensen Jakensen), Use-Book (Jakensen) Subject Ol-GlobalSion, OL-GlobalSion, Root CA - 82 Password	\$
	Certificate		
	Subject	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	33
	Issuer	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	
	Serial Number (Hex.)	04:00:00:00:00:01:0F:86:26:E6:0D	
	Serial Number (Dec.)	4835703278459682885658125	
	Valid From	15.12.2006 08:00:00 to 15.12.2021 08:00:00	
	Algorithm	RSA with SHA-1 Key Length 2048	
	Check Sum (MD5)	94:14:77:7E:3E:5E:FD:8F:30:BD:41:B0:CF:E7:D0:30	
	Checksum (SHA1)	75:E0:AB:B6:13:85:12:27:1C:04:F8:5F:DD:DE:38:E4:B7:24:2E:FE	
• • • • • • • • • • • • • • • • • • •		Add to Certificate List Add Certificate to PSE	\$
		SAP	NGQ (1) 100 TINNONGWQAS INS

- 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.

Role Name	<b>Role Description</b>	User	Transactions	
ZINV_ECC_PRJ	Innovapptive -	SAP Basis Adminis-	SU01D, SBWP, SM59,	
BASIS	Project Role - ECC	trator	SMT1, ST22, SU53, ST-	
	Basis Authorizations		MS_IMPORT, SE37,	
			SE16, SM30, SM31, ST22	
ZINV_ECC_PRJ_DE-	Innovapptive -	SAP Developer	Developer access key,	
VELOPER	Project Role - ECC		Developer Debug ac-	
	Developer Autho-		cess SE11, SE12, SE16,	
	rizations		SE14, SE38, SE18, SE19,	

#### Table 2-5 Roles on ECC System and transactions

Role Name	Role Description	User	Transactions
			SE93, SM30, SM31, SE41,
			SE51, SE91, SE37, SE80,
			SE24, SWDD, SU01D,
			SU53, SBWP, SWUS,
			SWELS, SWEL, SWII,
			SWIII, SWI14, SWI3,
			SW16, SWIE, SWUE,
			SWIA , SMARFORMS,
			SEGW,SE80,SE01, SWI5,
			SE63, SLXT
ZINV_ECC_PRJ_SE-	Innovapptive -	SAP Security Ad-	SU01, RSPFPAR, SPRO,
CURITY	Project Role - ECC	ministrator	PFCG, SUIM, SM30,
	Security Authoriza-		SE16, ST01, SU53, SU56,
	tions		SU21, SU03
ZINV_ECC_PRJ	Innovapptive -	SAP Configurator	SPRO, SE11, SE38, SE24,
CONFIGURATOR	Project Role - ECC		SM36, SM37, SM30,
	Configurator Autho-		SE37, SBWP, SU53, SU3,
	rizations		SE16, SU01D

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

#### Table 2-6 Roles on NetWeaver Gateway System and transactions

Role Name	<b>Role Description</b>	User	Transactions
ZINV_NWG_PRJ BASIS	Innovapptive - Project Role - Gate- way Basis Authoriza- tions	SAP Basis Adminis- trator	RZ11, SM59, SMT1, SE01, ST22, SU53, SU01D, SPRO, STMS*, SM30, SMICM, SICF, STRUST, /IWBEP/*, / IWFND/*, SBGRFC- CONF
ZINV_NWG_PRJ_DE- VELOPER	Innovapptive - Project Role - Gate- way Developer Au- thorizations	SAP Developer	Developer ac- cess key, Develop- er Debug access SEGW, SE24, SE37, SE38, SSO2, SICF, /

Role Name	Role Name Role Description		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

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

## 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

도 <u>Q</u> ueue <u>E</u> dit	<u>G</u> oto <u>R</u> equest	Extras Environment	S <u>v</u> stem <u>H</u> elp	_
0	▼ « 🖯	<u>L</u> egend	Ctrl+Shift+F4	1 🔽 🗆 🛛 😨 💻
		Personal Settings	Ctrl+Shift+F12	
Import Que	ue: System El	Other Requests	•	Add
A 4 7 4 6	) 🔽 🖧 l Go 🗎	Activate I <u>n</u> active Re	quests	Find in Other Groups
		Delete Imported Re	quests	
齃 Requests for	: EBS: 0 / 1			2

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.

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

Import Queue	e: System EH7
Ð≜ ₹ % Q	7 🖆   🗞 🖹 📰 🞭 🗟   合 🛼 🛼   🛫 💆   🖉 📰 😰
具 Requests for E	H7: 0 / 82
🔄 Add Transport Red	uest to Import Queue
Transp. Request	ERDK901948
Import Queue	EH7 System EH7
Import Again	

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

Figure 2-23 Truck icon

Impor	Import Queue: System EH7						
Ø 🛎 🖥	🔁 🚢 🖷 🧏 🔍 🚏 🖆 🕼 🖹 🔜 🔜 🔒 🔛 🕮 🕮 🖾 🖪 🖻						
🔛 Reque:	Requests for EH7: 0 / 1 01.08.2016 14:27:35						
Number	Request	RC	Owner	Short Text	St		
83	ERDK901948		E5000103		Т <u>і</u>		
- 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:

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

Table 2-9 SCP Data Center Information

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

≡	SAP HANA Cloud Platform Cockpit			٥	2	R	8	ወ			
Ē	Overview	🎟 US East ~ / 品 Innovapp	otive Inc. 🕗 \mid 🖻 I	nnovapptive Inc. \vee							
٩	Applications >	ౖ≊ Innovapptive Inc. ·	a⁼ Innovapptive Inc Members						G	Ð	
¥\$	Services	All: 18									
•	Solutions (BETA)	Add Members History			All Roles	<ul> <li>✓ Search</li> </ul>				C	Ł
۲	Persistence >										
ষ্ঠ	Connectivity >	Name	ID	Roles		Comment		A	ctions		
•		Anilkumar Guntuka	SOC	Administrator, Developer, Support User, A	pplication User A	Anil	6	9	0		1
•	Security >	fsn avatar	P1	Administrator, Developer					Ø 1	D 🖂	3
	Repositories >	Hari Kamineni	SC	Support User		Hari	6	9	01	Ì D	3
0	Resource Consumption	Nagesh Caparthy	SC	Administrator, Developer, Support User, A	pplication User A	Nagesh	6	9	0		3
8	Members	Narasimha Rao Yannabathina	sc	Administrator, Developer, Application Use	r Admin, Cloud C	Narasimha	6	9	01	Ì D	3
		Prabhukumar Srikarthik	S0^	Support User		Sri	6	9	0	Ì D	3

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.

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

Table 2-10 Roles for SCP Tenant Members

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	<ul> <li>Performs development tasks, such as deploying, starting, stop- ping, and debugging applica- tions.</li> <li>Changes loggers and perform monitoring tasks, such as creat- ing availability checks for appli- cations and executing MBean op- erations.</li> </ul>
	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 techni- cal support engineers.

Role	Description
	Note: To read the database content, a database administrator must assign appropriate permissions to this role.
Application User Admin	<ul> <li>Manages user permissions on application level to access Ja- va, HTML5 applications, and sub- scriptions.</li> <li>Controls permissions by assigning users to specific application roles or by assigning users to groups, which you then assign to appli- cation roles. Also unassigns users from roles or groups.</li> </ul>
	Note: Cannot manage account roles and perform actions on ac- counts. (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:

- | 2 SCP Configurations before Installing Innovapptive Products
  - 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

Service: Mobile Services, std - Overview
 Not enabled
 Enable
 Service Description
 Use Mobile Services to provide mobile access to enterprise information. Key features include app content lifecycle management, push notifications and support for offline apps, app security, app monitoring and usage reporting. This includes native build apps, MDK and SAP Mobile Cards. You need this to run apps based on the SAP Cloud Platform SDK for iOS. For B2E and B2B use cases only.

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	Minimum 3 GB, recommended 20 GB
space	

# 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 archi- tecture compatible			
JDK	SAP JVM 64-bit (recommend- ed)	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.

Operating System Version	Archi- tecture	Cloud Con- nector 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

Operating System Version	Archi- tecture	Cloud Con- nector 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 high- er
Redhat Enterprise Linux 8	x86_64	2.12.2 and high- er

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

## 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)	connectivitynotification.hana.ondemand-	155.56.210.83
(hana.ondemand.com)	.com	
	connectivitycertsigning.hana.ondemand-	155.56.210.43
	.com	
	connectivitytunnel.hana.ondemand.com	155.56.210.84
Europe (Frankfurt)	connectivitynotification.eu2.hana.onde-	157.133.206.143
(eu2.hana.ondemand.com)	mand.com	

Data Center (Landscape host)	Hosts	IP Addresses
	connectivitycertsigning.eu2.hana.onde- mand.com	157.133.205.174
	connectivitytunnel.eu2.hana.ondemand- .com	157.133.205.233
Europe (Amsterdam) (eu3.hana.ondemand.com)	connectivitynotification.eu3.hana.onde- mand.com	157.133.141.140
	connectivitycertsigning.eu3.hana.onde- mand.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.onde- mand.com	65.221.12.40
	connectivitycertsigning.us1.hana.onde- mand.com	65.221.12.241
	connectivitytunnel.us1.hana.ondemand- .com	65.221.12.41
United States West (Chan- dler)	connectivitynotification.us2.hana.onde- mand.com	64.95.110.215
(us2.hana.ondemand.com)	connectivitycertsigning.us2.hana.onde- mand.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.onde- mand.com	169.145.118.140
	connectivitycertsigning.us3.hana.onde- mand.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)	connectivitynotification.us4.hana.onde- mand.com	157.133.45.140
(us4.hana.ondemand.com )	connectivitycertsigning.us4.hana.onde- mand.com	157.133.45.132
	connectivitytunnel.us4.hana.ondemand- .com	157.133.45.141
Asia-Pacific (Australia) (ap1.hana.ondemand.com)	connectivitynotification.apl.hana.onde- mand.com	157.133.97.47
	connectivitycertsigning.ap1.hana.onde- mand.com	157.133.97.27
	connectivitytunnel.ap1.hana.ondemand- .com	157.133.97.46

Table 2-13 Network Connectivity Information (continued)

## 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.



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|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.

SAP					Cloud Connector	r Adm	ninistration					🛞 Admini:	strat
Connector	~												
Security Status		Conne	octor							+ Add S	ubaccount	↓ Backur	2
Alerting		CONIN	20101									outside	
High Availability													
Hardware Metrics Monitor	r	Conn	ector Overviev	N									
Configuration													
		C	onnector ID: 5A0	21341C	08C11E8CDAAC8	EEAC	C100034		Security Status: ① Risk				
OEM-Test -eur	$\sim$	l	.ocal Name: IGD	CDT000	9.internal.innovap	ptive.	com		High Availability: $\diamondsuit$ Disabled				
Cloud To On-Premise			Local IP: 172	16.0.52					Alerts: 🗖 1				
On-Premise To Cloud													
Monitor		Suba	ccount Dashb	oard									
Audits		Status	Subaccount	$\nabla$	Display Name	$\nabla$	Location ID	$\nabla$	Region	$\nabla$	Actions		
Log And Trace Files		8	otwgw14tfs		OEM-Test -eur				Europe (Amsterdam)		°0 /	<u> </u>	•••

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 = ./
	$\ensuremath{\texttt{\#}}$ Windows - change this value to the working path for this guide
	<pre># dir =C:\\OpenSSL-Win64\\bin\\</pre>
	new_certs_dir = \$dir
	unique_subject = no
	certificate = \$dir/HCC_CA.crt
	database = \$dir/certindex
	<pre>private_key = \$dir/HCC_CA.key</pre>
	serial = \$dir/certserial
	default_days = 730
	default_md = shal
	<pre>policy = myca_policy</pre>
	x509_extensions = myca_extensions
	crlnumber = \$dir/crlnumber
	default_crl_days = 730
	[ myca_policy ]
	commonName = supplied
	<pre>stateOrProvinceName = supplied</pre>
	countryName = optional
	emailAddress = optional
	organizationName = supplied
	organizationalUnitName = optional

	[ myca_extensions ]
	<pre>basicConstraints = critical,CA:TRUE</pre>
	keyUsage = critical,any
	<pre>subjectKeyIdentifier = hash</pre>
	<pre>authorityKeyIdentifier = keyid:always,issuer</pre>
	<pre>keyUsage = digitalSignature,keyEncipherment,cRLSign,keyCertSign</pre>
extendedKeyUsage =	
	serverAuth
	[ v3_ca ]
	<pre>basicConstraints = critical,CA:TRUE,pathlen:0</pre>
	keyUsage = critical,any
	<pre>subjectKeyIdentifier = hash</pre>
	<pre>authorityKeyIdentifier = keyid:always,issuer</pre>
	<pre>keyUsage = digitalSignature,keyEncipherment,cRLSign,keyCertSign</pre>
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	a Root Certin	cation Autro	onties			
Certificates						
Intended purpose:	<all></all>					_
Intermediate Certifica	ation Authorities	Trusted Root Co	ertification Aut	Authorities Trusted		
Issued To	Issued B	y	Expiratio	Friend	y Name	
GTE CyberTrus	Glo GTE Cyb	erTrust Globa	8/13/2018	GTE C	vberTrust .	

HCCRootCA

Figure 2-30 Trusted Root Certification Authorities

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

Microsoft Authentic... Microsoft Authenticod... 12/31/1999 Microsoft Authe...

11/20/2042 <None>

Figure 2-31 Intermediate Certification Authorities

tended purpose: <a>  </a>				-
Intermediate Certification Au	uthorities   Trusted Root C	ertification Aut	horities   Trusted Publ_	()
Issued To	Issued By	Expiratio	Friendly Name	
HCC Intermediate CA	HCCRootCA Microsoft Root Authority	7/5/2017 12/31/2002	<none> <none></none></none>	

# 2.5.5.4. Configure Cloud Connector

HCCRootCA

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

≡	SAP	Cloud Connector Administration				
×a	Connector 🗸					
	Security Status	Configuration				
	Alerting	Cloud Connector Administration       C       C         Configuration       USER INTERFACE       CLOUD       ON PREMISE       REPORTING       ADVANCED         System Certificate       C				
	High Availability	USER INTERFACE CLOUD ON PREMISE REPORTING ADVANCED				
	Hardware Metrics Monitor	System Certificate	្រា	Ŵ	i ⑦	
	Configuration					- 1
		Subject DN: OU=MOBILITY, O=INNO, C=IN, ST=TEL, CN=intermediate				
8	OEM-Test -eur 🗸 🗸 🗸	Issuer: CN=HCC_CA, OU=MOBILITY, O=INNO, L=HYD, ST=TEL, C=IN				
	Cloud To On-Premise	Valid From: Jan 9 15:25:06 2018 IST				
	On-Premise To Cloud	Valid To: Jan 9 15:25:06 2020 IST				
	Monitor					
	Audits	Trust Store	+	Ū	i 🕐	
	Log And Trace Files	Status Public Keys			Actions	
		Trust store is empty — no access restrictions				

3. Upload Root CA file to CA Certificate.

≡	SAP	Cloud Connector Administration	૮ હ	8	Administrator $\vee$
N <sup>R</sup> O	Connector N				
	Security Status	Configuration			
	Alerting	Configuration			
	High Availability	USER INTERFACE CLOUD ON PREMISE REPORTING ADVANCED			
	Hardware Metrics Monitor	Trust store is empty — no access restrictions			
	Configuration				
8⁼	OEM-Test -eur	CA Certificate 🔁 🖬 🏦	<u> </u>	Ū.	i
	Cloud To On-Premise				
	On-Premise To Cloud	Subject DN: OLI-MOBILITY O-INNO C-IN ST-TEL ON-intermediate			
	Monitor				
	Audits	Issuer: CN=HCC_CA, OU=MOBILITY, O=INNO, L=HYD, ST=TEL, C=IN			
	Log And Trace Files	Valid From: Jan 9 15:25:06 2018 IST			
	2031 110 1100	Valid To: Jan 9 15:25:06 2020 IST			

4. Update the Principal Propagation Settings.

SAP	Cloud Connector Administration			8 A	
Connector 🗸					
Security Status	Configuration				
Alerting	Comgulation				
High Availability	USER INTERFACE CLOUD ON PREMISE REPORTING ADVANCED				
Hardware Metrics Monitor					
Configuration	Principal Propagation	Ē	Ø	i	0
OEM-Test -eur 🗸 🗸	Subject Pattern: CN=\$(name)				
Cloud To On-Premise	Expiration Tolerance (h): 42				
On-Premise To Cloud	Certificate Validity (min): 60				
Monitor	Kalana				
Audits	Kerberos	0	ک	1	0
Log And Trace Files	KDC Hosts Realm Name:				
	Encontion Key				

Figure 2-33 Principal Propagation Settings

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

## 2.5.5.5. Configure Access Control

| 2 - SCP Configurations before Installing Innovapptive Products

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

Edit Resou	irce
Path must	not be empty
	Enabled
URL Path: *	/sap/opu/odata/
Access Policy:	<ul> <li>Path only (sub-paths are excluded)</li> </ul>
	<ul> <li>Path and all sub-paths</li> </ul>
	Save Cancel

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.)



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

SSL Setup-Creating the SSL Server PSE:

- | 2 SCP Configurations before Installing Innovapptive Products
  - 1. Select the SSL Server PSE node.
  - 2. Click Create.

Figure 2-36 Cre	ate PSE
🖙 Create PSE	×
Name	NGS
Org. (Opt)	[]
Comp./Org.	SAP Web AS
Country	
CA	O=SAP Trust Community, C=DE
Algorithm	DSA with SHA-1
Key Length	1024 💌

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.

_	-										
C	SSL S	erver									×
DN	N of Standard PSE CN=*.internal.innovapptive.com, OU=I0020732638, OU=									AS,	0=
1	Instan	ce-Spe	ecific PSEs								
	Ins	St	Distinguished Na	ime							<b>111</b>
	0		tive.com, OU=I	020732638,	OU=SAP We	b AS, O=SAP	Trust Community, (	C=DE			*
											-
_											
_											
_											
											-
	4 Þ									4 )	
			Bistin erit	h			L D C F				
IUS	cances	s with	empty Distinguis	neo wames w	viii de assigned	u the standard	I PSE				
								<b>/</b> i i i			<b>m</b> ×

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:

🕄 🕤   🛃 🗟   🛆 🐬	V   Z   A 4			M	
New Service Port	8080	Host Name	Keep Alive	Proc.Timeo	Actv Exte
		sep108v001	60	180	1
Log	HTTPS	sep108v001	60	180	1
ACL File					
Keep Alive (in Sec.)	60				
Max. Processing Time	[ <mark>60</mark>				
Use External Binding Pro	gram				

Figure 2-38 New Service Window

#### **Profile Parameters**

- Transaction code: RZ11
- Profile Parameter: icm/HTTPS/verify\_client = 1

Documentation Cha	nge Value	
Parameter Name		
icm/HTTPS/verify_client		
Short Description (Engl.)	SSL Client Certificate required?	
Application Area	Internet Communication Manage	r 🗇
Parameter Type	Integer value	ð
Changes allowed	Change permitted	đ
Valid for Operating Sys.	All operating systems	đ
Minimum	0	
Maximum	2	
Dynam. switchable		
Same on all servers		
Default Value	1	
Profile Value	1	
Current Value	1	

Figure 2-39 Profile Parameter Attributes

The ICM trusts the system certificate for principal propagation:

- | 2 SCP Configurations before Installing Innovapptive Products
  - 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	
Edit Profiles	
🗋 Create 📫 Check 🗈 Copy 🐑 Ir	nport
Profile NGT_DVEBMGS00_INNON Version 000019	IGWISI (Instance profile) (Saved, activated)
Edit Profile	
<ul> <li>Administrative Data</li> <li>Basic maintenance</li> <li>☑ Extended maintenance</li> <li>☑ Extended maintenance</li> <li>☑ Change</li> </ul>	

- 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

04.10.2018 Active par	rameters	
Parameter Name	Parameter value	
icm/HTTPS/trust_client_with_subject	*	
icm/HTTPS/trust_client_with_issuer	*	

8. Click **Save**.

## 2.5.5.8. Provide Logon Data

| 2 - SCP Configurations before Installing Innovapptive Products

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.

ath	/default_host	/sap/opu/	/odata/	
ervice Name	invmim		Service (Active)	
ang.	English	-	Cther Languages	
Description	Total I days			
Description 1	Namespa	асе		
Description 2				
Description 3				
Procedure	Altern	native Log	on Procedure   SAML Configuration	
Procedure Use All Lo Logon Data	Altern gon Procedures	ative Log	on Procedure  Security Session: Unrestricted	
Procedure Use All Lo Logon Data Client User	Altern gon Procedures	native Log	ion Procedure  SAML Configuration Security Session: Unrestricted	
Procedure Use All Lo Logon Data Client User Language	Altern gon Procedures	native Log	on Procedure   SAML Configuration  Security Session: Unrestricted	
Procedure Use All Lo Logon Data Client User Language Password St	Altern gon Procedures	ial	ion Procedure  SAML Configuration Security Session: Unrestricted	
Procedure Use All Lo Logon Data Client User Language Password St Security Req	Altern gon Procedures atus Initi uirement	native Log ∂ ▼] i.al	ion Procedure  SAML Configuration Security Session: Unrestricted	
Procedure Use All Lo Logon Data Client User Language Password St Security Reg O Standard	Altern gon Procedures atus Initi uirement	vial	Image: Solution procedure       SAML Configuration         Security Session:       Unrestricted	

Figure 2-42 Logon Data

#### Figure 2-43 Logon Data

			1
)St	tandard SAP User	O Internet User	
eau	uthentication		
ead	ctivated system-wide:	No	
唐	1 Default		
Log	1 Default gon Procedure List (in Orde	of Execution)	
Log N.	Default gon Procedure List (in Orde Logon Procedure	of Execution)	<b></b>
_09 N.	Default     Jon Procedure List (in Orde     List (in Orde     List Compared and the second seco	of Execution)	
Log N. 1	Default     Jon Procedure List (in Orde     Logon Procedure     Basic Authentication     Logon Through SSL Certil	of Execution) ate	
Log N. 1 2 3	Default     Joon Procedure List (in Orde     Logon Procedure     Basic Authentication     Logon Through SSL Certif     Logon Through HTTP Fiel	of Execution) ate	
Log N. 1 2 3 4	Default     Jon Procedure List (in Orde     Logon Procedure     Basic Authentication     Logon Through SSL Certif     Logon Through HTTP Fiel     SAP Logon/Assertion Tick	of Execution) ate s	
Log N. 1 2 3 4 5	Default     Jon Procedure List (in Orde     Logon Procedure     Basic Authentication     Logon Through SSL Certif     Logon Through HTTP Fiel     SAP Logon/Assertion Ticket	of Execution) ate s	

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

New Entrie	s: Details of Added Entries	
🧐 🗟 🖏		
External ID type	DN of Certificate (X.500)	
External ID		🖉 🖻
	CN=S0013927235	
Seq. No.		
User	minventory	
Min. date		_
Activated		
Issuer		Se .

3. Save the mapping.

Figure 2-45 Assign External ID to Users Overview

Image: Second Stress       Image: Second Stress       Image: Second Stress         Image: Second Stress       Image: Second Stress         Image: Second Stress       Image: Second Stress         Image: Second Stress       Image: Second Stress			
ernal ID type DN of Certificate (X.500) signment of External ID to Users			
signment of External ID to Users			
H External ID			
THE CAUSE IN THE ACTION AND	User	Act.	
CN=E5000066	E5000066		
CN=S0013927235	MINVENTORY		-
CN=SAPTEST2, OU=SAP Security	SAPTEST2	•	н
CN=SAPTEST3, OU=SAP Security	SAPTEST3		
CN=VALLAKATIS, OU=SAP Security	VALLAKATIS		
CN=harik, OU=SAP Security	KAMINENIH		
CN=narendar, OU=SAP Security	NARENDAR	-	

#### 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
```

69 🕅		
<ul> <li>System PSE</li> <li>SNC SAPCryptolib</li> <li>SSL server Standard</li> <li>SSL client SSL Client (Anony)</li> <li>SSL client SSL Client (Standard</li> <li>X SSL client SSE Veb Servic</li> <li>X WS Security Other System I</li> <li>X WS Security Other System I</li> <li>X WS Security WS Security Ke</li> <li>X SSE Collaboration Integration</li> <li>SSF Logon Ticket</li> </ul>	SSL server Standard Own Certificate Subject Certificate List	CN=INNONGWDEV.internal.innovapptive.com, OU=I0020732638, OU=SA         (Self-Signed)         Subject         CN=INNONGWDEV.internal.innovapptive.com, OU=I0020732638, OU         CN=INNONGWDEV.internal.innovapptive.com, OU=I0020732638, OU         CN=INNONGWDEV.internal.innovapptive.com, OU=I0020732638, OU         CN=Innovapptive, OU=GDC, O=Innovapptive Inc, L=Houston, SP=Te.         OU=GDC, O=Innovapptive Inc, C=US, SP=Texas, CN=innovapptive         Password
	Certificate	
	Subject	CN=INNONGWDEV.internal.innovapptive.com, OU=I0020732638, OU=SA
	Subject (Alt.)	
	Issuer	CN=INNONGWDEV.internal.innovapptive.com, OU=I0020732638, OU=SA

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

Subject	CN=INNONGWDEV.inter	nal.innovapptive.com, OU=I0020732638, OU=SA
Subject (Alt.)		
Issuer	CN=INNONGWDEV.inter	nal.innovapptive.com, OU=I0020732638, OU=SA
Serial Number (Hex.)	0A:20:15:12:03:12:4	4:01
Serial Number (Dec.)	729606306739143681	
Valid From	03.12.2015 12:44:01	to 01.01.2038 00:00:01
Algorithm	RSA with SHA-1	Key Length 1024
Check Sum (MD5)	A1:84:7C:39:C3:4D:F	D:F6:E2:38:BB:DB:DE:1F:BD:CA
Checksum (SHA1)	A4:E6:F6:0C:9E:75:7	6:87:95:6F:40:D5:41:A9:5D:FA:C1:73:58:44

Figure 2-47 Export Certificate

4. Save the certificate as **sed\_ssl\_server.crt**.

Figure 2-48 Export Certificate Path

	×
File Database Addr. Book Directory service	
File path	
File format	
OBinary	
le Base64	

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 Innovapp- tive Products	Configure Access for Deploying Innovapp- tive Products <i>(on page 32)</i>	
Install / Upgrade SMP Server	<ul> <li>Install SMP Server (on page 102)</li> <li>Upgrade SMP Server (on page 103)</li> </ul>	

# 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.

DEC Destinatio	
a c Desunatio	on IWFND_BGRFC_DEST
Remote Logon Con	nection Test Unicode Test 🎾
RFC Destination Connection Type	IWFND_BGRFC_DEST       3     ABAP Connection       Description
Description	
Description 1 Description 2 Description 3	RFC Destination for Outbound Queues
Administration	Technical Settings Logon & Security Unicode Special Options
Default Gateway     Export Trace     Do Not Export T	/ Value
Keep-Alive Timeout	
Default Gateway     Timeout Inactive     Specify Timeout	Value 300 Defined Value in Seconds
	ocol
Select Transfer Proto	

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

bgRFC Configuration	
Scheduler: System Scheduler: App. Serve	er Scheduler: Destination Define Inbound Dest. Define Supervisor Dest.
Destination IWFN	D BGRFC DEST
IWFND BGRFC DEST	n/server group
· · · ·	
Prefi	xes
IWCN	I_WF
IWFN	D_CNP H
A	
▼	
A P New	
Last Changed	
Liser Name ZZMARIM	
Client ID 100	
Time 10:01:39	
Current Date 09/05/2015	

- 5. Enter IWFND\_BGRFC\_DEST in the Inb. Dest. Name field and click <Enter>.
- 6. In the **New Prefix** field, create entries, for example **IWFND\_CNP** and **IWCNT\_WF** and save the settings.

- | 3 SMP Configurations before Installing Innovapptive Products
  - 7. Click Create on the Scheduler: Destination tab.

Figure 3-4 S	Scheduler:	Destination	tab
--------------	------------	-------------	-----

Destination Name		Inbound DestinationIWF	ND_BGRFC_DEST	
IWFND_BGRFC_DEST	*	Scheduler Count	1-	
	-	Max. Auto. Retries	30	
		Wait per Unit (s)	900	
		Wait/Destination (s)	900	
		Dest.Proc. Time (s)		
		Open Connections	10	
		Unit Alive Checks	30	
		History Active		
		Check Class		
		Active/Inactive		
	_	Check Class		
	÷			
4	Þ			
		]		
Last Changed				
User Name				
Client ID				
Time	00:0	0:00		

- 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

bgRFC Configuration		
Create RFC Destination for Supervisor	×	ound Dest. Define Supervisor Dest.
Destination		
Destination Name BGRFC_SUPERVISOR		
User		
Create User 🗸		
User Name BGRFC_USER		
Generate Password		
	-	
Save	×	
Changed On		
Changed At 00:00:00		

- 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) addon. 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	

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		

Table 3-3 Software Prerequisites for NetWeaver Gateway (con	tinued)
---	---------

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.

RFC Destination ERDCLNT800	
Remote Logon Connection Test Unicode Test 🌮	
RFC Destination         ERDCLNT800           Connection Type         3         ABAP Connection         Description           Description	
Description 1       Connection to ERD Backend system         Description 2	
Client 800 User PW Status is initial	•
Trust Relationship ONO O Yes Logon Screen	
Status of Secure Protocol       Image: SNC       Image: SNC         Image: SNC	33
Authorization for Destination	
Caliback Positive List	4

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

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

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

Figure	3-8	Trusted	Calling	Systems
<u> </u>				

Trusted-Trusting Connections					
i					
Systems whose calls are trusted Systems that trust current system					
N& TO A BA					
Calling Systems	Inst.				
ABAP Systems					
• 🖹 CRD	0090055493				
• 🖹 EH7	0020732636				
• 🖹 ERD	0020732636				
• 🖹 ERQ	0020732636				

## 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:

- 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

New Entries: Overvie	ew of Adde	ed Entries		
🦻 🖬 🖪 🖪				
Gateway settings				
Destination system	Client	System Alias	RFC Destination	
MGX	100	LOCAL	IWFND_BGRFC_DEST	-
				-

4. Save your settings.

## 3.2.4. Create the SAP System Alias for Applications

To create the SAP system Alias for applications:

- 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

	Change View "Manage SAP System Aliases": Overview								
1	😚 New Entries 🗅 🖶 🕫 🕃 💀								
	Manage SAP System Alases								
	SAP System Alias	Description	Local SAP	For Local App	RFC Destination	Software Version	System ID	Client	WS Provider System
	FRD	ECC Backend for Fiori			ERDCI NT800	DEFAILT	FRD	800	

5. Save your settings.

## 3.2.5. Activate SAP NetWeaver Gateway

To activate the SAP NetWeaver Gateway:

- 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:

- 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

Program SRT_WS_IDP_CUSTOMIZE	
🚱 🚥 Jobs	
Schedule Switch for IDP WS	
Document	
✓ Switch Document Tables	
Job Name SAP_BC_IDP_WS_SWITCH_BD	
Period in Days	
Period in Hours 6	
Change Time of Next Switch	03.09.2016 09:39:06
Document ID	
✓Switch Document ID Tables	
Job Name SAP_BC_IDP_WS_SWITCH_BDID	
Period in Days	
Period in Hours 12	
Change Time of Next Switch	18.09.2016 03:39:06

6. Click Continue.

## 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 belowmentioned 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

Maintain servio	ce				
Create Host/Service	🎾 🗊 🛐 🖪	➡External Aliases 🛛 İ	📋 🧏 🎤 System M	Nonitor Inactive 📲	
Filter Details					
Virtual Host		Service Path			
ServiceName					
Description					
Lang,	English '	Ref.Service:			
Apply	😽 Reset	Fine-Tune			
Virtuelle Hosts / Services	5	Documentation		Referenz Service	
Monte Comment     Mont	nt	co_mes_int			-
• 🖷 crm_logon		Default alias to the CRM application		/default_host/sap/bc/bsp/sap/crm_ui_start	-
• 🞯 epic_dumr	my_icbc	EPIC Dummy ICBC			
• 🞯 es		Enterprise Search			
• 🞯 gw		gateway subnode			
• 🞯 iwbep		Business Suite Enablement node for Gate			
• 🞯 meData		meData synchronizatio	n Service		
MY_NEW_	TEST	DD			-
• 🕲 opu		OData for SAP Produc	ts		
• 🞯 odata		Standard Mode			
🕨 🞯 sdata		Compatibility Mode for	SP 02		
🔄 🕐 🕑 utils		Utility services			
• 🞯 POWL_WI	IDGET_HAN	POWL WIDGET			
Simerp SICF Services for ERP eProcurement					
• 📆 uif_logon Default alias to start webcuif /default_host/sap/bc/bsp/sap/crm_ui_start					
<ul> <li>Webcuif</li> </ul>		Web Client UI Service:			
• 😡 🛪		Exchange Infrastructu	re (XI)		
		4 >			

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

Maintain service						
Create Host/Service	Create Host/Service 🤣 📅 🤂 🔢 🖨 External Aliases 🛛 🏷 🏴 System Monitor Active 📑					
Filter Details						
Virtual Host	Service Path					
ServiceName	PING					
Description						
Lang.	English Ref.Service:					
P Apply	Reset Pine-Tune					
Virtuelle Hosts / Service	es Documentation Referenz Service					
default_host	VIRTUAL DEFAULT HOST					
▼ 🛇 sap	SAP NAMESPACE; SAP IS OBLIGED NOT T					
🕨 💿 public	PUBLIC SERVICES					
▼ <sup>®</sup> bc BASIS TREE (BASIS FUNCTIONS)						
▶ 🞯 apc ABAP Push Channel Framework						
<ul> <li> <u> <u> </u></u></li></ul>	ABAP Push Channel test appliocations					
• 🕅 ping	Connection Test					

## 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

ICM Monitor of Server SRVWIN0880_NGS_01			
🞝 🖑 📅 📔			
ICM Parameter			
Services			
Services			
icm/server port[0]	= PROT=HTTP, PORT=0, TIMEOUT=60, PROCTIMEOUT=60		
icm/server port[1]	= PROT=SMTP, PORT=0, TIMEOUT=120, PROCTIMEOUT=120		
icm/server port[2]	=		
<pre>icm/server_port[3]</pre>	=		
<pre>icm/server_port[4]</pre>	-		
Hard limits			
<pre>icm/max_services</pre>	= 30		
icm/listen_queue_len	= 512		
icm/req_queue_len	= 1000		
icm/max_conn	= 500		
icm/max_sockets	= 2048		
Thread handling			
icm/min_threads	= 10		
icm/max_threads	= 250		
ICM/MIN spare threads	= 5		

- 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

IC	м м	onitor - Servi	ce Display			
9	<b>3</b>	B B   🚢 Ŧ	🔀   🗵   🐙 🝜 🔯	🍋   🎟 🖽 🖷   🗓	4 ◆ ▶	M
Act	tive S	Services				
	No.	Protocol	Service Name/Port	Host Name	Keep Alive	Proc.Timeo Actv
	1	HTTP	8000	INNONGWDEV.internal.	600	600 🗹
	2	SMTP	0	INNONGWDEV.internal.	120	120 🖌
	3	HTTPS	443	INNONGWDFV internal	600	600 🖌

## 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.

$\left( \right)$	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

도 Program Edit Goto System	Help	
🔮 🔍 👻 🤘	🔍 😪   🚔 🖞 👘 👘   🎝 🖆 🖓 💭 💭   💭 🔛	
SAP Gateway Virus Scan	Profile Configuration	
æ		
Virus Scan Profile	[]Q	
✓ Virus Scan Switched Off		
Virus scanning is not active.	🛂 🖓 🕨 NGT (1) 100 🔻 INNONGWTST	INS 🛛 🖘 📑

## 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:

- 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

Program /IWFND/R_SM_CLEANUP_JOB_CREATE	
F Program /IWFND/R_SM_CLEANUP_JOB_CREATE	
Created Cleanup Jobs: SAP_IWFND_APPS_LOG_CLN SAP_IWFND_SUP_UTIL_CLN SAP_IWFND_NOTIF_CLN	

## 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.

	Fiaure	3-18	Clear	Loa	Entries	Criteria
--	--------	------	-------	-----	---------	----------

Application Log: De	lete Expired Logs				
🍄 🔥 🗓					
Delete logs					
All logs are deleted which sati selection conditions, and for v - the expiry date is reached o - the expiry date is not defin	fy the following ihich: r passed 2d		-		
Expiry date					
<ul> <li>Only logs which have reach</li> <li>and logs which can be dele</li> <li>Cnnot delete log now since</li> </ul>	ad their expiry date ted before the expiry date expiry date is in the future				
selection conditions					
Object		to		- <u>-</u>	
Subobject		to			
External ID		to			
Transaction code		to			
User		to		<b></b>	
Log number		to			
Problem class		to	]	<b></b>	
from (date/time)	00:00	1:00			
to (date/time)	00:00	):00			
Options					
Only calculate how many					
<ul> <li>Generate list</li> <li>Delete immediately</li> </ul>					
Delete by Number of Logs					
COMMIT Counter	100				

- 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

Cleanup of Query Result Log
Selection Parameters
Records Older Than (in Hours) 168
✓Delete Log Headers
Control Parameters
Execute in Test Mode

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

## 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

면 PSE Edit Goto Certificat	e En <u>v</u> ironment System	н Нер	
🖉 🔹 🔹	🖯 I 🗟 🔕 😒 I 🗁 🕅	🖞   \$\\$ \$\\$ \$\\$ \$\\$   🜄 🗖   🖉 🖳	
Trust Manager: Display	v		
🤣 🕅			
System PSE           INS SNC SAPCrystolb           INS SL SAPCrystolb           INS SL SAPCrystolb           SSL dent SSL dent (Anony           SSL dent SSL dent (Monty           SSL dent WSE Web Servic           W SS sourty Other System E           W SS Sautry WS Security Ker           SSL Standard           SS SL Standard           SS SL Standard	Supers	UNT-TINUE JAL LIERIN, ESLERING I STILLINGUNG, COU-BOULUY 22(1936, COU-BON-W (Self-Signed) Subject CH-GlobalSion, O-GlobalSion, OU-GlobalSion Root CA - R2	÷
	Certificate		
	Subject	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	
	Subject (Alt.)		
	Issuer	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	
	Serial Number (Hex.)	04:00:00:00:00:01:0F:86:26:E6:0D	
	Serial Number (Dec.)	4835703278459682885658125	
	Valid From	15.12.2006 08:00:00 to 15.12.2021 08:00:00	
	Algorithm	KSA WITN SHA-1 Key Length 2048	
	Checksum (MD5)	Y4:14://:/E:3E:3E:12:37:10:04:F0:EF:DD:DE:20:F4:P7:24:2F.FF	
• • • • • • • • • • • • • • • • • • •		Add to Certificate List Add Certificate List Add Certificate Cist	
		SAP	NGQ (1) 100 V INNONGWQAS INS

- 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.

Role Name	<b>Role Description</b>	User	Transactions
ZINV_ECC_PRJ	Innovapptive -	SAP Basis Adminis-	SU01D, SBWP, SM59,
BASIS	Project Role - ECC	trator	SMT1, ST22, SU53, ST-
	Basis Authorizations		MS_IMPORT, SE37,
			SE16, SM30, SM31, ST22
ZINV_ECC_PRJ_DE-	Innovapptive -	SAP Developer	Developer access key,
VELOPER	Project Role - ECC		Developer Debug ac-
	Developer Autho-		cess SE11, SE12, SE16,
	rizations		SE14, SE38, SE18, SE19,

#### Table 3-5 Roles on ECC System and transactions

Role Name	<b>Role Description</b>	User	Transactions
			SE93, SM30, SM31, SE41,
			SE51, SE91, SE37, SE80,
			SE24, SWDD, SU01D,
			SU53, SBWP, SWUS,
			SWELS, SWEL, SWII,
			SWI11, SWI14, SWI3,
			SW16, SWIE, SWUE,
			SWIA , SMARFORMS,
			SEGW,SE80,SE01, SWI5,
			SE63, SLXT
ZINV_ECC_PRJ_SE-	Innovapptive -	SAP Security Ad-	SU01, RSPFPAR, SPRO,
CURITY	Project Role - ECC	ministrator	PFCG, SUIM, SM30,
	Security Authoriza-		SE16, ST01, SU53, SU56,
	tions		SU21, SU03
ZINV_ECC_PRJ	Innovapptive -	SAP Configurator	SPRO, SE11, SE38, SE24,
CONFIGURATOR	Project Role - ECC		SM36, SM37, SM30,
	Configurator Autho-		SE37, SBWP, SU53, SU3,
	rizations		SE16, SU01D

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

#### Table 3-6 Roles on NetWeaver Gateway System and transactions

Role Name	<b>Role Description</b>	User	Transactions
ZINV_NWG_PRJ BASIS	Innovapptive - Project Role - Gate- way Basis Authoriza- tions	SAP Basis Adminis- trator	RZ11, SM59, SMT1, SE01, ST22, SU53, SU01D, SPRO, STMS*, SM30, SMICM, SICF, STRUST, /IWBEP/*, / IWFND/*, SBGRFC- CONF
ZINV_NWG_PRJ_DE- VELOPER	Innovapptive - Project Role - Gate- way Developer Au- thorizations	SAP Developer	Developer ac- cess key, Develop- er Debug access SEGW, SE24, SE37, SE38, SSO2, SICF, /

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, / IWFND/APPS_LOG, / 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

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

## 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

Transport	Description	Dependency
NGTK904332	INNOV:NWG Project Team	None
	Roles	

#### Table 3-8 SAP NWG Transports for Roles

#### Figure 3-22 Add Transport Request to Import Queue

Import Queue: System EH7		
🔁 🚢 🐺 🍕 🏹	' 🖆   🗞 🗎 🗉 🔜 🔝   📇 🔩   😤 🖾   🖾 📔 🙆	
Requests for EH7	: 0 / 82	
🖙 Add Transport Request to Import Queue		
Transp. Request	ERDK901948	
Import Queue	EH7 System EH7	
Import Again		

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

Figure 3-23 Truck icon

Impor	t Queue: S	yste	m EH7		
🕗 主 亨 🥄 🔍 🍞 🇀   🛷 🖹 🗉 🔜 🔝   合 뵺 🔜 🖤 🏼 🗐 🗐 🗐					
🔛 Reques	Requests for EH7: 0 / 1 01.08.2016 14:27:35				
Number	Request	RC	Owner	Short Text	St
83	ERDK901948		E5000103		16

- 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 equiva- lent AMD processor
RAM	8GB
Disk Space for Installation	1.2GB

System	Minimum Requirement
Disk Space required for Server Data- base	50GB
Web browsers for Manage- ment Cockpit	Windows: • Internet Explorer 10 and later • Mozilla Firefox 10.x • Google Chrome 20 and later
	Mac: Safari 5.1 and later
JDK	Management API.
Reverse Proxy	<ul> <li>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:</li> <li>BigIP F5</li> <li>Citrix NetScaler 10.5</li> </ul>
	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 Ma- chine Support	SAP supports SMP running in a virtual machine if:

System	Minimum Requirement
	<ul> <li>The virtual machine is officially certified and approved by the op-</li> </ul>
	erating system platform vendor.
	<ul> <li>The operating system running in the virtual machine is certified</li> </ul>
	by SAP.
	<ul> <li>The hardware resources within the virtualization system are</li> </ul>
	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.