

SAP Basis Configuration - Server

System description

1.5.1

206-01-16

SEAL Systems

Copyright

This document and all its parts are protected by copyright. Their use without prior written consent by SEAL Systems is prohibited and subject to prosecution. In particular, this applies to reproduction, translation, microfilming and the storing and processing in electronic systems.

Customers that currently own a valid SEAL Systems software license for the product(s) described within the contents of this document, may freely distribute this documentation in electronic form (i. e. CD/File Server or Intranet) for internal usage only.

All product names mentioned are the registered trademarks of the associated companies.

Copyright 2001-2026

SEAL Systems AG
Lohmühlweg 4
D-91341 Röttenbach
Germany

Contents

| | | |
|------------|---|-----------|
| 1 | Introduction..... | 7 |
| | Conventions in this Documentation | 8 |
| | Activate the Retrace of your Viewing Path in PDF | 9 |
| | Variables in this Documentation | 11 |
| | Overview of Contents | 12 |
| | Description..... | 15 |
| 2 | RFC Destination (Classic) - Configuration..... | 17 |
| 2.1 | RFC Connection - Data - Overview..... | 18 |
| 2.2 | RFC Destination - Configuration on Server..... | 20 |
| | Unicode SAP System - Transfer with sapftp/saphttp | 21 |
| | saprfc.ini - RFC Client - Example | 24 |
| | saprfc.ini - RFC Server - Example | 25 |
| | saprfc.ini - Message Server - Example | 26 |
| | Assign Port - only for Message Servers | 28 |
| 2.3 | Establish the RFC Destination on the SAP System..... | 29 |
| | RFC Destination - Basis Data..... | 30 |
| | RFC Destination - Technical Settings | 32 |
| | RFC Destination - Unicode Settings | 33 |
| 2.4 | RFC and SAP Connections - Security Configuration | 34 |
| | Configure Security for Incoming Connections - reginfo | 36 |
| | Configure Security for Outgoing Connections - secinfo | 38 |
| | Security Configuration - Important Hints | 40 |
| | Activate Simulation Mode for Security Configuration..... | 41 |
| | Specify Prefix for Generic RFC Destinations | 42 |
| | Security Configuration - Background Knowledge | 43 |
| 2.5 | Start and Test RFC Destination | 44 |
| | Start the RFC Destinations on the Server | 45 |
| | Determine RFC Destinations to be Started via the [ACTIVE] Section | 46 |
| | Determine RFC Destinations to be Started via Call Parameters..... | 47 |
| | Test the RFC Destination on the SAP System | 48 |
| 2.6 | RFC Connection - Troubleshooting | 50 |
| | saphttp/sapftp Start - Background Knowledge | 52 |
| | Hints for the Load Balancing..... | 53 |
| | Additional Messages and Debugging..... | 55 |
| | Activate DLL Version of sapftp/saphttp in Case of Bottlenecks | 56 |
| | Define the USE_GWHOST Parameter | 57 |
| | Activate the SAP Gateway Logging..... | 58 |
| | Activate RFC Trace..... | 59 |
| | Activate Trace Functions for sapftp/saphttp..... | 60 |
| 3 | Static RFC Destinations for SNC Support..... | 61 |
| | Establish Templates for sapftp/saphttp (sm59) | 62 |
| | Create Multiple sapftp/saphttp Destinations..... | 65 |
| | RFC Client - Assign Static sapftp/saphttp Destination | 68 |
| | RFC Server - Assign Static sapftp/saphttp Destination | 69 |
| | Support Central SAP Gateway | 70 |
| 4 | HTTP Connection (REST) - Configuration..... | 72 |
| 4.1 | HTTP Connection - Configuration on Server..... | 73 |
| | Create PSE | 74 |

| | | |
|------------------------|---|------------|
| | Activate Logon with Basic Authentication and SSL | 75 |
| 4.2 | Create an HTTP Connection on the SAP System | 77 |
| | HTTP Connection - Basis Data | 78 |
| | HTTP Connection - Technical Settings | 79 |
| | HTTP Connection - Logon & Security | 80 |
| | HTTP Connection - Special Options | 82 |
| 5 | Web Service Integration (SOAP) - SAP as Provider | 84 |
| 5.1 | Required Authorizations | 85 |
| 5.2 | Configuration on the Provider System (SAP) | 86 |
| | Select the Service | 87 |
| | Create the Binding on the Provider System | 88 |
| | Determine URL for WSDL Access | 90 |
| 5.3 | Troubleshooting - Analysis of Web Service Requests | 91 |
| | Record and Display Web Service Requests | 92 |
| | Debug Web Service Requests | 93 |
| 6 | Web Service Integration (SOAP) - SAP as Consumer | 94 |
| 6.1 | Required Authorizations | 95 |
| 6.2 | Configuration on the Consumer System (SAP) | 96 |
| | Select the ABAP Proxy | 97 |
| | Create a Logical Port | 98 |
| | Suppress the Message ID Transfer | 100 |
| | Transfer of Large Amounts of Data | 101 |
| 6.3 | Advisable Behavior in the Case of Error | 102 |
| 6.4 | Troubleshooting | 104 |
| 7 | OData Service Activation | 106 |
| | Activate OData Service | 107 |
| | Activate OData Service for Applications - Basis | 109 |
| Reference | | 111 |
| 8 | Configuration Files - Reference | 113 |
| 8.1 | cadrfc.ini - Logon Information | 114 |
| | System-/Client-Specific Logon Data | 117 |
| | CadRfcUser Parameter | 119 |
| | CadRfcPassword Parameter | 120 |
| | CadRfcPasswordCoded Parameter | 121 |
| | CadRfcClient Parameter | 122 |
| | CadRfcLanguage Parameter | 123 |
| | CadRfcDestination Parameter | 124 |
| | CadDialogNetAddress Parameter | 125 |
| 8.2 | saprfc.ini - Connection Data | 126 |
| | Determine System Data for saprfc.ini | 128 |
| | Types of RFC Destinations and Module Classification | 129 |
| | Parameter Overview | 130 |
| | DEST Parameter | 133 |
| | TYPE Parameter | 134 |
| | ASHOST Parameter | 135 |
| | SYSNR Parameter | 136 |
| | MSHOST Parameter | 137 |
| | MSSERV Parameter | 138 |
| | R3NAME Parameter | 139 |
| | GROUP Parameter | 140 |

| | |
|--|------------|
| GWHOST Parameter | 141 |
| GWSERV Parameter..... | 142 |
| SAPROUTER Parameter | 143 |
| RFC_TRACE Parameter | 144 |
| SEAL_TRACE Parameter..... | 145 |
| ABAP_DEBUG Parameter..... | 146 |
| USE_SAPGUI Parameter | 147 |
| UNICODE Parameter..... | 148 |
| CODEPAGE Parameter | 149 |
| SNC_MODE Parameter | 150 |
| SNC_MYNAME Parameter | 151 |
| SNC_PARTNERNAME Parameter | 152 |
| SNC_QOP Parameter | 153 |
| SNC_SSO Parameter | 154 |
| ASCS Parameter..... | 155 |
| X509CERT Parameter..... | 156 |
| 8.3 sapnwrfc.ini - Connection Data | 157 |
| 8.3.1 Parameter Overview..... | 158 |
| 8.3.2 Parameters Depending on Connection Type..... | 161 |
| DEST Parameter..... | 162 |
| ASHOST Parameter..... | 163 |
| SYSNR Parameter..... | 164 |
| MSHOST Parameter..... | 165 |
| MSSERV Parameter | 166 |
| R3NAME Parameter..... | 167 |
| GROUP Parameter | 168 |
| GWHOST Parameter | 169 |
| GWSERV Parameter..... | 170 |
| 8.3.3 General Connection Parameters | 171 |
| SAPROUTER Parameter | 172 |
| SNC_LIB Parameter..... | 173 |
| SNC_MODE Parameter | 174 |
| SNC_MYNAME Parameter | 175 |
| SNC_PARTNERNAME Parameter | 176 |
| SNC_QOP Parameter | 177 |
| Parameter TRACE | 178 |
| CODEPAGE Parameter | 179 |
| NO_COMPRESSION Parameter..... | 180 |
| 8.3.4 Connection Parameters for Client Programs..... | 181 |
| USER Parameter | 182 |
| PASSWD Parameter | 183 |
| CLIENT Parameter..... | 184 |
| LANG Parameter..... | 185 |
| SNC_SSO Parameter | 186 |
| MYSAPSSO2 Parameter | 187 |
| X509CERT Parameter..... | 188 |
| LCHECK Parameter..... | 189 |
| USE_SAPGUI Parameter | 190 |
| ABAP_DEBUG Parameter..... | 191 |
| 8.4 rfcserver.cfg | 192 |
| [ACTIVE] Section | 193 |
| [SECTIONNAME] Section | 194 |

| | |
|---|------------|
| 9 Configuration Tables - Reference | 197 |
| /seal/bas_cr113 - Static Destination for RFC Server | 198 |
| /seal/bas_cr114 - Static Destination for RFC Client | 199 |
| /seal/bas_cr142 - Define Parameters | 201 |
| 10 Changes | 203 |
| Changes with Release 1.5.0 | 204 |
| Changes with Release 1.4.3 | 205 |
| Changes with Release 1.4.2 | 206 |
| Changes with Release 1.4.1 | 207 |
| Changes with Release 1.4.0 | 208 |
| Changes with Release 1.3.5 | 209 |
| Changes with Release 1.3.3 | 210 |
| Changes with Release 1.3.2 | 211 |
| Changes with Release 1.3.1 | 212 |
| Changes with Release 1.3.0 | 213 |
| Changes with Release 1.2.8 | 214 |
| Changes with Release 1.2.6 | 215 |
| Changes with Release 1.2.5 | 216 |
| Changes with Release 1.2.4 | 217 |
| Bibliography..... | 218 |
| Terminology..... | 219 |
| Abbreviations..... | 220 |
| Keywords | 221 |
| Index..... | 223 |

1 Introduction

SEAL Systems offers a range of integration modules for the output management systems or DPF from SEAL Systems as external system and SAP including additions for SAP PDM, creation of digital paper or plot reproduction services for SAP. For data exchange between the external system and the SAP system, the two systems must recognize each other.

subject - connection external system/SAP

The following documentation describes the necessary steps to establish connections between the external system and the SAP system to exchange data.

The following alternatives are available for data exchange between SAP and the external system, the configuration of which is discussed in this documentation:

alternatives

- RFC destination
- HTTP connection, for example in combination with a REST interface
- Web service with the SAP system as provider or consumer (SOAP)
- OData service

This chapter deals with the following topics:

in this chapter

→ *Conventions in this Documentation*, Page 8

→ *Activate the Retrace of your Viewing Path in PDF*, Page 9

→ *Variables in this Documentation*, Page 11

→ *Overview of Contents*, Page 12

Conventions in this Documentation

path specifica-
tion

The path information given in this documentation is relative to the installation directory of the output system. This is usually the home directory of the `plossys` user. The path information is indicated in Windows notation only in most cases. This corresponds to the Linux directory structures unless noted otherwise.

typography

The following table lists the typographical conventions employed in this documentation.

| Typographical Convention | Meaning |
|---------------------------------|---|
| Consolas | File names, paths, commands, menu items, keywords, special values, short scripts and examples |
| <i>Consolas italic</i> | Parameters; variables that must be replaced by current values |


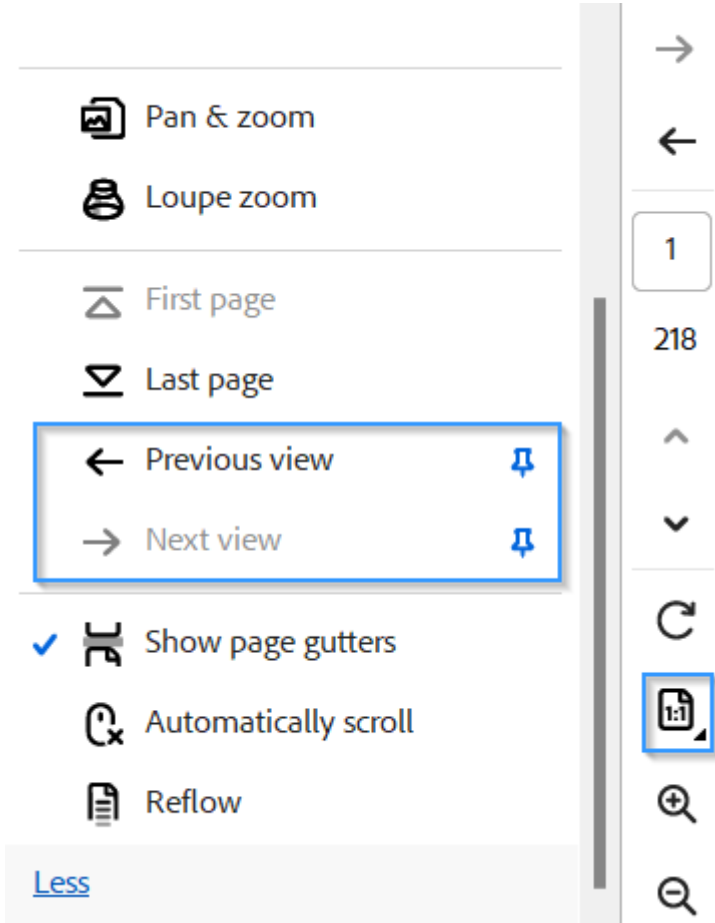
Activate the Retrace of your Viewing Path in PDF

Adobe Reader provides buttons to retrace your viewing path of PDF pages that you viewed earlier. This makes reading easier and helps to keep the central theme.

description

This is how you activate the buttons for retracing your viewing path in the PDF documentation as of Adobe Acrobat 2024:

instructions, as of Adobe Acrobat Pro 2024

| Step | Action |
|------|---|
| 1 | In the lower part of the right side menu, click on the black arrow on the symbol for the magnification factor  . |
| 2 | <p>Scroll down to the Other tools section and activate the two menu items:</p> <ul style="list-style-type: none"> • Previous View • Next View  |

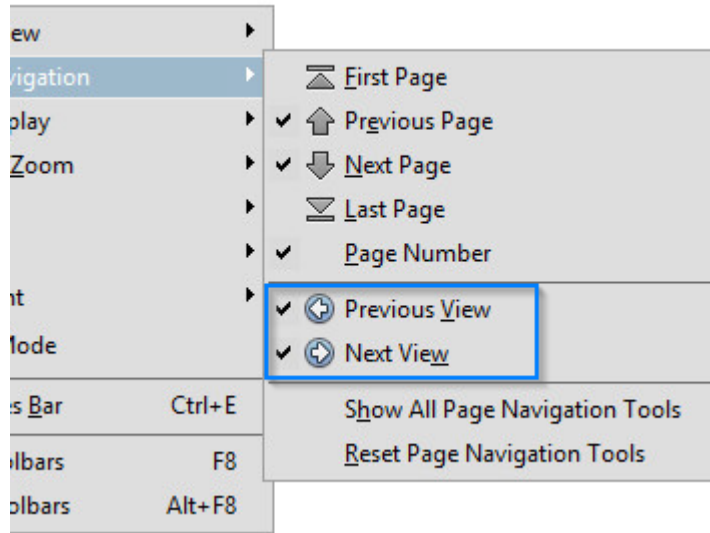
The icons for jumping to the previous/next view are displayed in the right side menu.

result

Activate the Retrace of your Viewing Path in PDF, Continuation

instructions, as of Adobe Reader 10

This is how you activate the buttons for retracing your viewing path in the PDF documentation as of Adobe Reader 10:

| Step | Action |
|------|---|
| 1 | <p>Activate the following options via the menu:</p> <ul style="list-style-type: none"> View - Show/Hide - Toolbar Items - Page Navigation Show Tools Previous View: Activate Next View: Activate  |

result

Adobe Reader offers the following buttons to allow you jumping forward and backward in the document while showing pages you viewed in the reverse order that you viewed them:



Variables in this Documentation

The variable *ModuleGlobal* represents the general module short cuts:

- pls
- dvs

meaning of *ModuleGlobal*

The variable *ModuleSelect* represents the individual modules:

- convserv
- convservdpf
- dvsviewserv
- filecheck
- rfcserver
- rfcserver

meaning of *ModuleSelect*

The variable *Action* represents the actions:

- start
- status
- stop

meaning of *Action*

Overview of Contents

| | |
|-------------|--|
| structure | This documentation has two parts: a description and a reference. The first part describes the functionality and the installation process using figures, step-by-step-procedures and explanatory texts. The second part serves as a detailed reference guide, containing configuration settings, keywords etcetera. |
| description | <p>The description deals with the following topics:</p> <p>→ <i>RFC Destination (Classic) - Configuration</i>, Page 17</p> <p>This chapter describes the required configuration settings for communication via classic RFC destinations (in contrast to communication via the SAP NetWeaver RFC Library NWRFC).</p> <p>→ <i>Static RFC Destinations for SNC Support</i>, Page 61</p> <p>This chapter explains how the connections for the data exchange between servers and SAP systems are established and tested in case of communications via static RFC destinations. Static RFC destinations offer the following advantages:</p> <ul style="list-style-type: none"> • SNC is supported for sapftp/saphttp. • Static RFC destinations can be explicitly enabled/restricted at the gateway. <p>Static RFC destinations are available for:</p> <ul style="list-style-type: none"> • RFC client: JSAPcli, for example, within PLOSSYS Distribution Engine for checking-out original files or for re-archiving • RFC server: DMS Loader/ABAP in RFC mode for files with storage not equal to KPRO (web server) XSA in RFC mode for files with storage not equal to KPRO (web server) (DMS View Server is not affected, as it uses the integrated sapftp/saphttp functionality of JRFC Server and no external processes). <p>→ <i>HTTP Connection (REST) - Configuration</i>, Page 72</p> <p>This chapter describes the configuration settings required for communication via HTTP connections, which are used in combination with a REST interface, for example.</p> <p>→ <i>Web Service Integration (SOAP) - SAP as Provider</i>, Page 84</p> <p>This chapter describes the establishing of a Web service integration (SOAP), if SAP serves as provider.</p> <p>→ <i>Web Service Integration (SOAP) - SAP as Consumer</i>, Page 94</p> <p>This chapter describes the establishing of a Web service integration (SOAP), if SAP serves as consumer.</p> <p>→ <i>OData Service Activation</i>, Page 106</p> <p>This chapter describes how to activate OData services in SAP.</p> |
| reference | The reference contains the following chapters: |

Overview of Contents, Continuation

→ *Configuration Files - Reference, Page 113*

This chapter explains the configuration files which are evaluated to establish a connection between the OM server and the SAP system in case of communication via classic RFC destinations or communication via SAP NetWeaver RFC Library NWRFC.

→ *Configuration Tables - Reference, Page 197*

This chapter contains an alphabetically sorted list of all configuration tables relevant for the basis configuration in SAP.

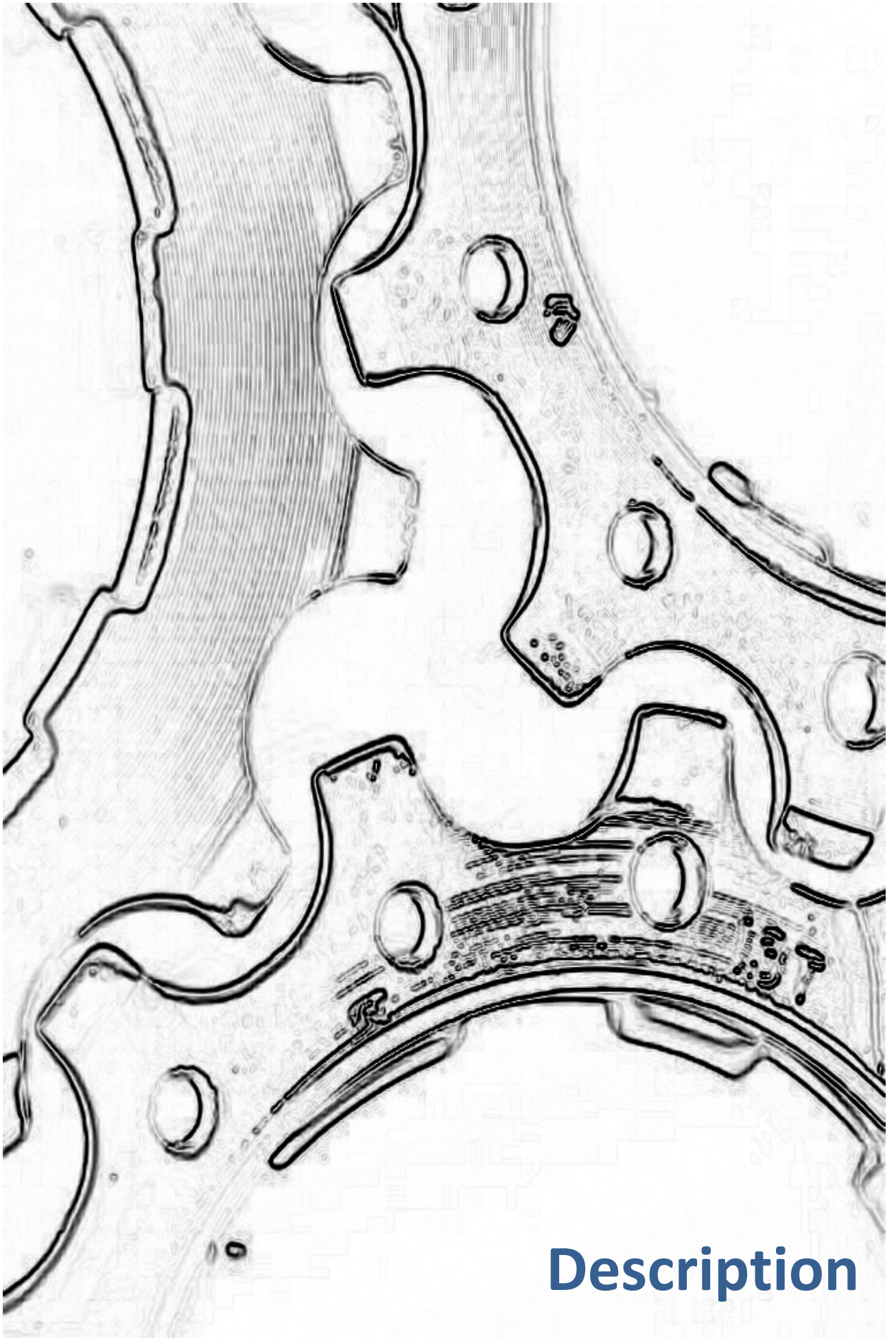
→ *Changes, Page 203*

changes

This chapter describes the most important changes for each released module version.

For an easier overview, a bibliography, terminology list, abbreviation list, and index are included at the end of the documentation. lists

Overview of Contents, Continuation




Description

2 RFC Destination (Classic) - Configuration

This chapter describes the required configuration settings for communication via classic RFC destinations (in contrast to communication via the SAP NetWeaver RFC Library NWRFC). introduction

RFC servers logon on the SAP gateway. SAP gateway
Application servers communicate with their local SAP gateways via an optional central gateway.


A message server is used for load balancing for RFC clients. message server

You may find information about a secure RFC communication via SNC and SSO in [SAP_BASECONF_SNC_TEC].  reference

This chapter deals with the following topics: in this chapter

- *RFC Connection - Data - Overview*, Page 18
- *RFC Destination - Configuration on Server*, Page 20
- *Establish the RFC Destination on the SAP System*, Page 29
- *RFC and SAP Connections - Security Configuration*, Page 34
- *Start and Test RFC Destination*, Page 44
- *RFC Connection - Troubleshooting*, Page 50

→ *Static RFC Destinations for SNC Support*, Page 61

 related topics

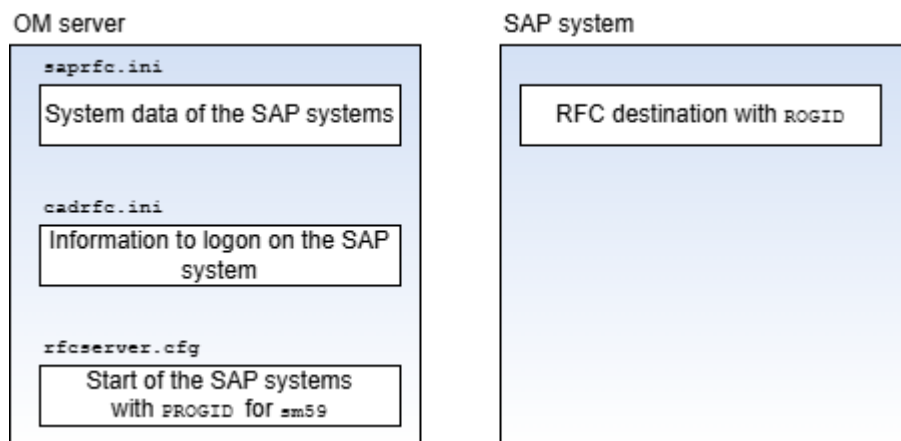
2.1 RFC Connection - Data - Overview

introduction

This chapter offers an overview of the relevant configuration files and their correlation in the context of communication via classic RFC destinations.

data for the connection via RFC

The data necessary for the RFC connection between OM servers and SAP systems is saved in the following files/transactions:



coherence between the data

The following important correlations exist between these settings:

RFC Connection - Data - Overview, Continuation

The image displays the configuration files for an RFC connection and the corresponding SAP GUI settings. It consists of three main parts:

- rfcserver.cfg:** A text file containing configuration parameters. The active section is highlighted with a blue box and labeled "Section with SAP systems for which the RFC destinations are to be started". The content includes:

```
! "Q(#) $Id: rfcserver.cfg,v 1.4 2006/12/24 00:00:00 sap Exp $"
!
!-----
! Start RFC Server for all PROGIDs in active sections.
!-----
!
[ACTIVE]
SECTION = DEU
!SECTION = TEST
SECTION = PROD
!-----
! Development system
!-----
[DEU]
DESTINATIONS = "X46RFC"
PROGID=SEAL-CONN-001
PROGID=SEAL-CONN-002
PROGID=SEAL-CONN-003
PROGID=SEAL-CONN-004
!-----
! Test system
!-----
[TEST]
DESTINATIONS = "T47RFC"
PROGID=SEAL-CONN-001
```
- saprfc.ini:** A text file containing system-specific data for the RFC destinations. It is labeled "Section with the SAP system data". The content includes:

```
DEST=X46RFC
TYPE=R
GWHOST=sap7
GWSERU=sapgw00
RFC_TRACE=0
UNICODE=0


DEST=T47RFC
TYPE=R
PROGID=Dummy
GWHOST=sap9
GWSERU=sapgw00
RFC_TRACE=0
```
- SAP GUI:** The "Technical Settings" tab of the RFC destination configuration. The "Activation Type" is set to "Registered Server Program". The "Registered Server Program" field contains the value "SEAL-CONN-001". A button labeled "Transaction sm59" is visible.

2.2 RFC Destination - Configuration on Server

SEAL Setup Suite The SEAL Setup Suite module queries the required data and inserts the data into the configuration files. Alternatively, you can customize the configuration files. The following chapters describe the customizing.

general proceeding

The configuration on the external server includes the following steps:

| Step | Description |
|------|--|
| 1 | Define the system data of the SAP systems to which the RFC destinations are to be established in <code>saprfc.ini</code> → <i>saprfc.ini - Connection Data, Page 126</i> |
| 2 | Define the RFC destinations to be started in <code>rfcserver.cfg</code> → <i>rfcserver.cfg, Page 192</i> |
| 3 | Specify the information for the first-time logon in: <code>cadrfc.ini</code> → <i>cadrfc.ini - Logon Information, Page 114</i>  Hint: You can modify the <code>cadrfc.ini</code> file on the installation directory. Afterwards you can distribute this file to the required directories. |
| 4 | Assign the ports if necessary: → <i>Assign Port - only for Message Servers, Page 28</i> |

in this chapter

This chapter deals with the following topics:

- *Unicode SAP System - Transfer with sapftp/saphttp, Page 21*
- *saprfc.ini - RFC Client - Example, Page 24*
- *saprfc.ini - RFC Server - Example, Page 25*
- *saprfc.ini - Message Server - Example, Page 26*
- *Assign Port - only for Message Servers, Page 28*

Unicode SAP System - Transfer with sapftp/saphttp

| | |
|---|--|
| <p>SAP provides different versions of the programs sapftp and saphttp for the data exchange with Unicode SAP systems and non-Unicode SAP systems.</p> | <p>Description</p> |
| <p>At the configuration of the SAP systems, you have to specify with UNICODE in saprfc.ini whether the SAP system is a Unicode or a non-Unicode system.</p> | <p>requirement - saprfc.ini</p> |
| <p>For each application server, which is used by the message server, a section has to exist in saprfc.ini with TYPE R, where beside the net address of the application server as GWHOST also UNICODE have to be specified correctly.</p> | <p>requirement - message server</p> |
| <p>This chapter is only relevant if you use Unicode SAP systems and non-Unicode SAP systems (mixed operation) and the Conversion Server module from SEAL Systems. Other modules, such as JRFC Server, automatically start sapftp_uc/sapftp_nuc and saphttp_uc/saphttp_nuc from SAP.</p> <p>If you only use Unicode SAP systems (no mixed operation with non-Unicode systems, determined via UNICODE in saprfc.ini), you can deactivate the wrapper program from SEAL Systems, see instructions below.</p> | <p>only required for mixed operation</p> |
| <p>For mixed operations, the wrapper program from SEAL Systems starts the correct variant of sapftp/saphttp.</p> | <p>wrapper program</p> |
| <p>The sapftp/saphttp wrapper program from SEAL Systems must be located in the tools\bin_xxx directory for mixed operation with Unicode SAP systems and non-Unicode SAP systems. Do not replace this program by the sapftp/saphttp program from SAP!</p> | <p>requirement - wrapper program</p> |

This is how you ensure that the program is the wrapper program:

| Step | Action |
|------|---|
| 1 | Determine the program version with: sapftp -v and saphttp -v |
| 2 | The wrapper program from SEAL Systems displays this result: <pre> ***** saphttp Version 1.0.0.3 of 2015-07-06 - \$Revision: 1.1 (C) 2013 SEAL Systems This programm calls the UNICODE/NON-UNICODE version of depending on command line args and saprfc.ini settings ----- Environment: RFC_INI Path to saprfc.ini. HTTP_TRACE=2 Write more debug output RFC_TRACE_DIR Log file directory with dev_http_seal.log SAPUNICODE=Y N Force unicode on/off, do not parse saprfc.in ***** </pre> |

Unicode SAP System - Transfer with sapftp/saphttp,

Continuation

| Step | Action |
|------|--|
| 3 | Replace the program if the display looks different, for example: <pre>SAPFTP Non-Unicode @(#) \$Id: //bas/721_REL/src/krn/ftp/ftpmain.c#7 \$ SAP @(#) \$Id: //bas/721_REL/src/krn/ftp/ftp.c#6 \$ SAP @(#) \$Id: //bas/721_REL/src/krn/ftp/ftpcmd.c#2 \$ SAP inifilename = xçÏ, ^.ini open Failed SAP release: 721 SAP release no: 7210</pre> |

requirement - DLLs

If the wrapper program is active, all necessary DLLs must exist, for instance under Windows in the tools\bin_xxx icuuc.dll, librfc32u.dll, libsapucum.dll, libsapucum.dll, sapnwrfc.dll.

effect and process

If Conversion Server from SEAL Systems starts an RFC destination, the value of UNICODE is read from saprfc.ini and the corresponding variant of sapftp and saphttp is started.

| Level | Processing |
|-------|--|
| 1 | The sapftp/saphttp wrapper program from SEAL Systems reads UNICODE from saprfc.ini. |
| 2 | If UNICODE=1: The wrapper program starts the sapftp_uc/saphttp_uc program from SAP. |
| 3 | If UNICODE=0: The wrapper program starts the sapftp_nuc/saphttp_nuc program from SAP. |


instructions - deactivate wrapper program

This is how you deactivate the wrapper program for pure Unicode SAP systems


| Step | Action |
|------|---|
| 1 | Open the following file in an editor: applications\server\sysstartstop.ini |
| 2 | Enter in the [INCLUDE] section: SAP-saphttp-sapftp= type_xxx |

Unicode SAP System - Transfer with sapftp/saphttp,

Continuation

| Step | Action |
|------|---|
| 3 | Open a SEAL shell and enter there: <code>sysinit "SAP-saphttp-sapftp"</code> |
| 4 | At the query enter: Y  Hint - effect: For pure Unicode SAP systems, this has the following effect: <ul style="list-style-type: none">• The wrapper programs are renamed to <code>sapftp.obs</code> and <code>saphttp.obs</code>.• <code>sapftp_uc</code> is copied to <code>sapftp</code> and <code>saphttp_uc</code> to <code>saphttp</code>. |

saprfc.ini - RFC Client - Example

 example -
without SNC


This example shows items in `saprfc.ini` for a RFC client destination, for example JSAPcli or DMS Rlist, without SNC:

```
DEST=W74
TYPE=A
SYSNR=01
ASHOST=roesap005.sealsystems.local
RFC_TRACE=0
ABAP_DEBUG=0
USE_SAPGUI=0
UNICODE=1
SNC_MODE=0
```

SAP router


An SAP router can also be specified with :

```
GWHOST=/H/saprouter.com/H/roegw003.sealsystems.local
```

 example -
with SNC

This example shows items in `saprfc.ini` for a RFC client destination, for example JSAPcli or DMS Rlist, with SNC:


```
DEST=W74
TYPE=A
SYSNR=01
ASHOST=roesap005.sealsystems.local
RFC_TRACE=0
ABAP_DEBUG=0
USE_SAPGUI=0
UNICODE=1
SNC_MODE=1
SNC_MYNAME=p:CN=SEALRFC,OU=SEALSAP,O=SEAL,C=DE
SNC_QOP=3
SNC_PARTNERNAME=p:CN=roesap005.sealsystems.local, OU=SEALSAP, O=SEAL-
SYSTEMS, C=DE
```

 related top-
ics

→ *saprfc.ini - Connection Data*, Page 126

saprfc.ini - RFC Server - Example

This example shows items in `saprfc.ini` for a RFC server destination without SNC:

 example -
without SNC


```
DEST=W74RFC
TYPE=R
GWHOST=roesap005.sealsystems.local
GWSERV=sapgw01
RFC_TRACE=0
SEAL_TRACE=0
UNICODE=1
SNC_MODE=0
```

An SAP router can also be specified with :

SAP router


```
GWHOST=/H/saprouter.com/H/roegw003.sealsystems.local
```

This example shows items in `saprfc.ini` for a RFC server destination with SNC:


 example -
with SNC

```
DEST=W74RFC
TYPE=R
GWHOST=roesap005.sealsystems.local
GWSERV=sapgw01
RFC_TRACE=0
SEAL_TRACE=0
UNICODE=1
SNC_MODE=1
SNC_MYNAME=p:CN=SEALRFC,OU=SEALSAP,O=SEAL,C=DE
SNC_QOP=8
```

→ [saprfc.ini - Connection Data, Page 126](#)

 related top-
ics

saprfc.ini - Message Server - Example

 example -
without SNC


This example shows items in `saprfc.ini` for a connection via message server without SNC:

```
DEST=W74
TYPE=B
MSHOST=roesap005.sealsystems.local
MSSERV=3601
R3NAME=W74
GROUP=PUBLIC
RFC_TRACE=0
ABAP_DEBUG=0
USE_SAPGUI=1
UNICODE=1
SNC_MODE=0
```

SAP router

An SAP router can also be specified with :

```
GWHOST=/H/saprouter.com/H/roegw003.sealsystems.local
```


 example -
with SNC

This example shows items in `saprfc.ini` for a connection via message server with SNC:

```
DEST=W74
TYPE=B
MSHOST=roesap005.sealsystems.local
MSSERV=3601
R3NAME=W74
GROUP=PUBLIC
RFC_TRACE=0
ABAP_DEBUG=0
USE_SAPGUI=1
UNICODE=1
SNC_MODE=1
SNC_MYNAME=p:CN=SEALRFC,OU=SEALSAP,O=SEAL,C=DE
SNC_QOP=3
SNC_PARTNERNAME=p:CN=roesap005.sealsystems.local, OU=SEALSAP, O=SEAL-
SYSTEMS, C=DE
```

saprfc.ini - Message Server - Example, Continuation

→ *saprfc.ini - Connection Data*, Page 126


 related topics

Assign Port - only for Message Servers

| | |
|---------------------------|--|
| required if | <p>For RFC client connections via message servers (type B), a port must be explicitly assigned in the C:\Windows\System32\drivers\etc\services system file (Windows example) if MSSERV is not set or the symbolic system identifier is assigned, for example MSSERV=sapmsW74:</p> <ul style="list-style-type: none"> • sapmsSID 36XX/tcp, for example sapmsW74 3601/tcp (type B, RFC client connections via message server) If MSSERV is assigned to an explicit port, for example MSSERV=3601, no item in the system file is necessary. |
| automatic port assignment | <p>The following settings in the saprfc.ini file are automatically assigned the correct ports; they do not need to be entered in the system file C:\Windows\System32\drivers\etc\services (Windows example):</p> <ul style="list-style-type: none"> • sapdpXX32XX/tcp, for example sapdp01 3201/tcp (type A, RFC client connections via application server) • sapgwXXs 48XX/tcp (SNC), for example sapgw01s 4801/tcp sapgwXX 33XX/tcp (otherwise), for example sapgw01 3301/tcp (type R, RFC server connections via SAP gateway) |

Description The correct ports must be assigned to the SAP systems on the operating system.

instructions This is how you assign the ports to the SAP systems, using Windows as an example:

| Step | Action |
|------|---|
| 1 | <p>Open the following system file in an editor: C:\Windows\System32\drivers\etc\services</p> |
| 2 | <p>For RFC client connections via message server (type B), if MSSERV is not set or the symbolic system identifier is assigned, for example MSSERV=sapmsW74:</p> <p>Enter:</p> <ul style="list-style-type: none"> • sapmsSID 36XX/tcp <p> Example: sapmsW74 3601/tcp</p> |

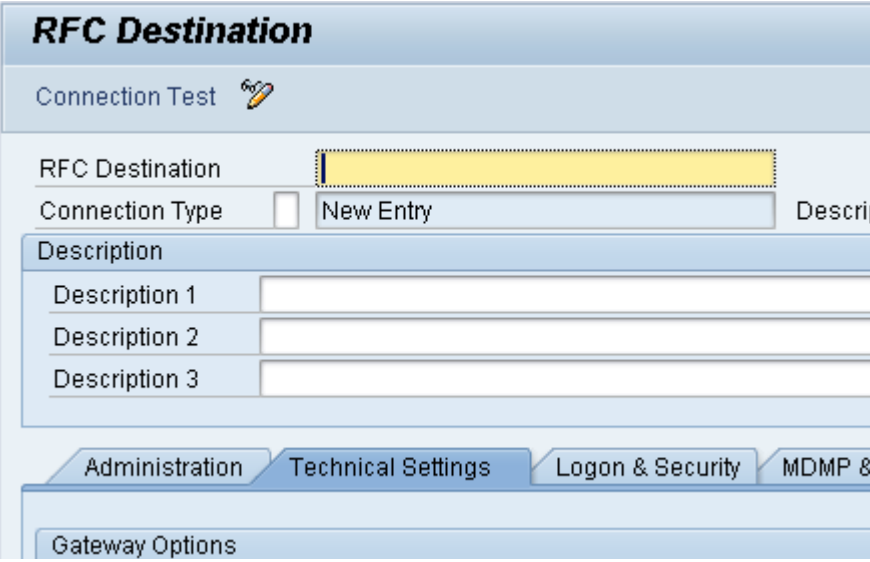
2.3 Establish the RFC Destination on the SAP System

An RFC destination can be used to transfer data from SAP to an external system. description

Alternatively, the following transfer types are available: alternative

→ *HTTP Connection (REST) - Configuration, Page 72*







This is how you create an RFC destination: procedure -
over-view

| Step | Action |
|------|--|
| 1 | Start the sm59 transaction. |
| 2 | Click Create:  |
| 3 | → <i>RFC Destination - Basis Data, Page 30</i> |
| 4 | → <i>RFC Destination - Technical Settings, Page 32</i> |
| 5 | → <i>RFC Destination - Unicode Settings, Page 33</i> |
| 6 | Save the settings. |

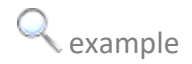
RFC Destination - Basis Data

necessary settings

Enter the following basis data:

| Parameters | Value |
|-----------------------------------|---|
| RFC Destination | <p><i>Unique identifier on the SAP system</i></p> <p> Example: SEAL-CONNC-001</p> <p> Hint - name identical to the program ID: For reasons of simplicity, the values of RFC destination and Program ID at the technical settings should be identical.</p> <p> Hint - exception: When using Conversion Server, a different name must be specified in order to implement load balancing/reliability, see scenario 1 in: → <i>Hints for the Load Balancing, Page 53</i></p> <p> Hint - ambiguous identifier: If the identifier is ambiguous the SAP system establish the connections to the server where the RFC server with this identifier is started first.</p> |
| Connection Type | T |
| Description | <i>Describing text</i> |
| Gateway Options - Gateway Host | <p><i>GWHOST</i> as in <i>saprfc.ini</i></p> <p> Hint - exception: When using Conversion Server, this value may be empty in order to implement load balancing/reliability, see scenario 1 in: → <i>Hints for the Load Balancing, Page 53</i></p> |
| Gateway Options - Gateway Service | <p><i>GWSERVas</i> in <i>saprfc.ini</i></p> <p> Hint - exception: When using Conversion Server, this value may be empty in order to implement load balancing/reliability, see scenario 1 in: → <i>Hints for the Load Balancing, Page 53</i></p> |

RFC Destination - Basis Data, Continuation








| RFC Destination SEAL-CONNC-001 | |
|---------------------------------------|---------------------|
| Connection Test | Unicode Test |
| RFC Destination | SEAL-CONNC-001 |
| Connection Type | T TCP/IP Connection |
| Description | |
| Description 1 | SEAL-CONNC-001 |

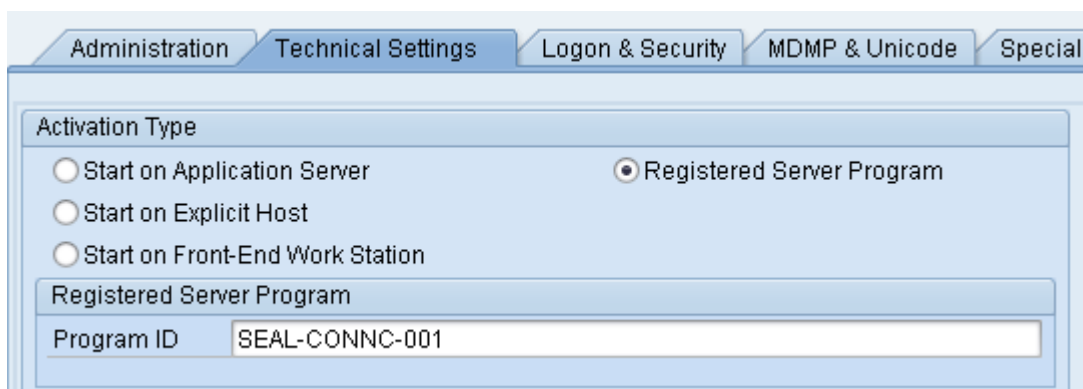
RFC Destination - Technical Settings

requirement Switch to the Technical settings tab.

necessary settings Enter the following technical settings:

| Parameter | Value |
|--|--|
| Activation Type | Registered server program |
| Registered Server Program - Program ID | <p><i>PROGID</i> identifier in the configuration file like <code>rfcserver.cfg</code> on the SEAL server</p> <p> Example: SEAL-CONNC-001</p> <p> Caution - upper/lower cases: The upper/lower case letters are evaluated!</p> <p> Caution - allow RFC destinations: As of EhP7 or kernel 721, destinations are no longer accepted automatically but have to be allowed manually in <code>reginfo/secinfo</code>:</p> <p>→ <i>RFC and SAP Connections - Security Configuration</i>, Page 34</p> <p> Hint - naming convention: The identifier can include letters, numbers, '+', '.', '-', and '_' characters!</p> |

 example



RFC Destination - Unicode Settings

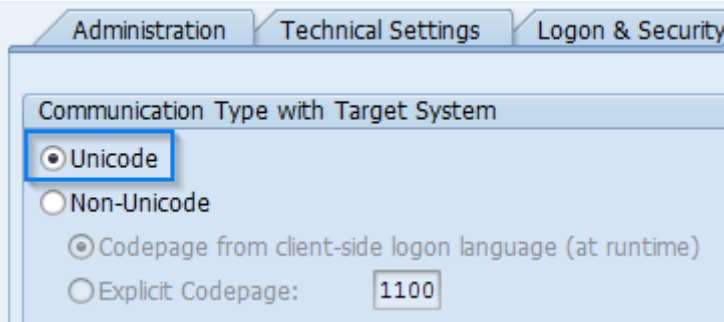
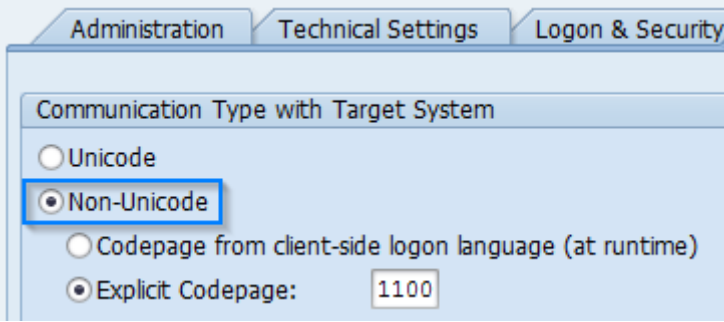

Switch to the tab:

requirement

- Unicode(as of ECC 6.0)
- MDMP & Unicode (up to release 6.40)
- Special Options (up to release 4.7)

Enter the following options:

necessary settings

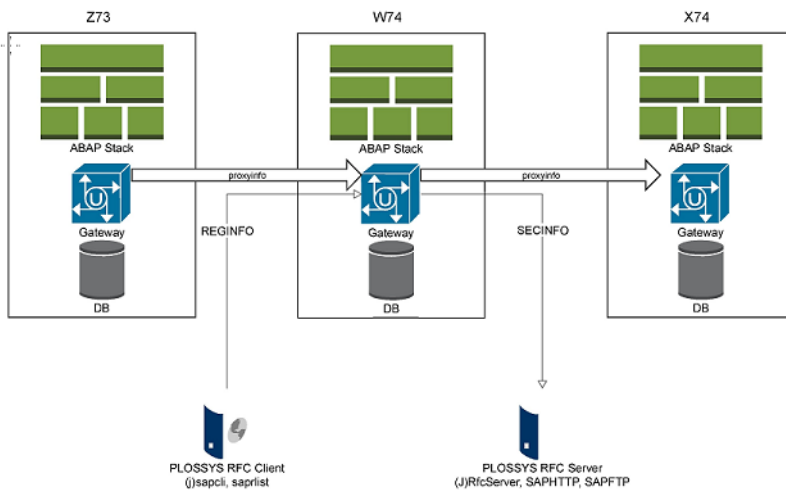
| Parameter | Value |
|--|--|
| as of release 6.40: Communication Type with Target System | <ul style="list-style-type: none"> • For JRFC Server: Unicode  |
| up to release 4.7: Character Width in Target System | <ul style="list-style-type: none"> • For RFC Server and Conversion Server: Non-Unicode Explicit Code Page (as of ECC 6.0)  <p> Caution - Conversion Server: The ConvUtl and ConvServSamp programs on the server are not Unicode-enabled! Therefore, Non-Unicode has to be activated!</p> |

2.4 RFC and SAP Connections - Security Configuration

reason Versions before EhP7 or kernel 721 automatically accept all destinations by default. As of EhP7 or kernel 721, destinations are no longer accepted automatically but have to be allowed manually.

connection types The security configuration in SAP can be used in order to avoid that unauthorized programs or users log on to SAP or connect to outside. The security configuration distinguishes the following connection types:

- `reginfo` - incoming connections (registrations and communication with registered programs)
- `secinfo` - outgoing connections (start attempts)
- `proxyinfo` - connections from SAP to SAP (not relevant in the context of SEAL Systems)



alternatives The following alternatives are provided at the security configuration:

- Explicit maintenance of `secinfo/reginfo`
See description below
- Profile parameter `gw/ac1_mode` (transaction: rz11)
Evaluated if `secinfo/reginfo` are not maintained
If `gw/ac1_mode=0`, all connections are allowed.
If `gw/ac1_mode=1`, all internal connections are allowed.

in this chapter This chapter deals with the following topics:

→ *Configure Security for Incoming Connections - reginfo*, Page 36

RFC and SAP Connections - Security Configuration,

Continuation

→ *Configure Security for Outgoing Connections - secinfo*, Page 38

→ *Security Configuration - Important Hints*, Page 40

→ *Activate Simulation Mode for Security Configuration*, Page 41


→ *Specify Prefix for Generic RFC Destinations*, Page 42

→ *Security Configuration - Background Knowledge*, Page 43

Configure Security for Incoming Connections - reginfo

instructions - >=
NW 7.45

This is how you specify the accepted registered programs on the SAP gateway in reginfo for SAP NetWeaver Application Server 7.45 or newer:


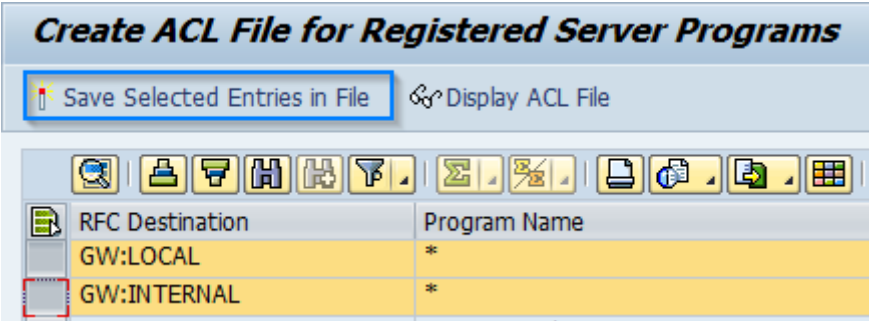

| Step | Action |
|------|--|
| 1 | Start the smgw transaction. |
| 2 | Select Goto →Expert Functions →External Security →Maintain ACL Files →Reginfo File |
| 3 | Enter the following line: P TP=* HOST=<IP address of the SEAL server> CANCEL=* ACCESS=*  Caution - important hints: Note the following hints when you enter the security configuration: → <i>Security Configuration - Important Hints, Page 40</i> |

instructions - <
NW 7.45

This is how you specify the accepted registered programs on the SAP gateway in reginfo for SAP NetWeaver Application Server older than 7.45:

| Step | Action |
|------|---|
| 1 | Start the smgw transaction. |
| 2 | Select Goto →Expert Functions →External Security →Display (reginfo) |


Configure Security for Incoming Connections - reginfo, Continuation

| Step | Action |
|------|---|
| 3 | <p>If the file does not exist, you can create it via:</p> <p>Goto</p> <ul style="list-style-type: none"> →Expert Functions →External Security →Create (reginfo) <p>Select the destinations, which are to be accepted, and save them via Save Selected Entries in File.</p> <p> Example:</p>  |
| 4 | <p>Enter the following lines in the <code>usr\sap\system\dveb-mgs00\data\reginfo.dat</code> file:</p> <pre>P TP=* HOST=<IP address of the SEAL server> CANCEL=* ACCESS=*</pre> <p> Caution - important hints:</p> <p>Note the following hints when you enter the security configuration:</p> <p>→ <i>Security Configuration - Important Hints, Page 40</i></p> |

Configure Security for Outgoing Connections - secinfo

instructions - >=
NW 7.45

This is how you specify the accepted programs to be started on the SAP gateway in secinfo for SAP NetWeaver Application Server 7.45 or newer:


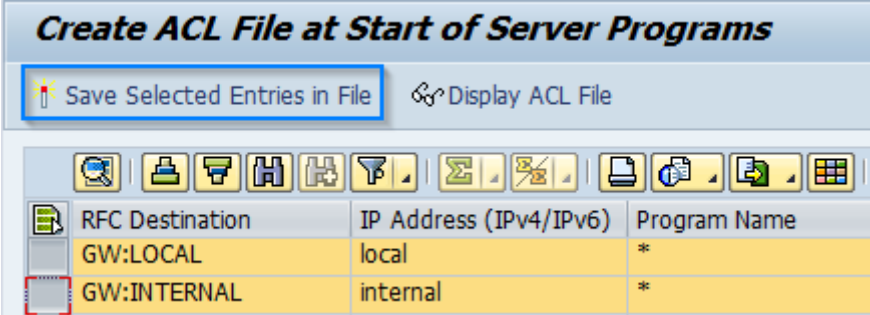

| Step | Action |
|------|---|
| 1 | Start the smgw transaction. |
| 2 | Select Goto →Expert Functions →External Security →Maintain ACL Files →Sec info |
| 3 | Enter the following line: P TP=* USER=* USER-HOST=<IP address of the SEAL server> HOST=<IP address of the SEAL server>  Caution - important hints: Note the following hints when you enter the security configuration: → <i>Security Configuration - Important Hints, Page 40</i> |

instructions - <
NW 7.45

This is how you specify the accepted programs to be started on the SAP gateway in secinfo for SAP NetWeaver Application Server older than 7.45:

| Step | Action |
|------|---|
| 1 | Start the smgw transaction. |
| 2 | Select Goto →Expert Functions →External Security →Display (secinfo) |

Configure Security for Outgoing Connections - secinfo, Continuation

| Step | Action |
|------|---|
| 3 | <p>If the file does not exist, you can create it via:</p> <p>Goto</p> <ul style="list-style-type: none"> →Expert Functions →External Security →Create (secinfo) <p>Select the destinations, which are to be accepted, and save them via Save Selected Entries in File.</p> <p> Example:</p>  |
| 4 | <p>Enter the following lines in the <code>usr\sap\system\dveb-mgs00\data\secinfo.dat</code> file:</p> <pre>P TP=* USER=* USER-HOST=<IP address of the SEAL server> HOST=<IP address of the SEAL server></pre> <p> Caution - important hints:</p> <p>Note the following hints when you enter the security configuration:</p> <p>→ <i>Security Configuration - Important Hints, Page 40</i></p> |

Security Configuration - Important Hints

note

Note the following issues at the security configuration:

- The first line has to start with: #VERSION=2
- Each line has to describe a complete rule, which starts with:
 - P: Permit
 - D: Deny
- If not all destinations/programs are accepted via TP=*, all destinations, which are used by SEAL Systems products, have explicitly to be specified, for instance ConvUtil.exe and ConvServSamp.exe.
You also may specify a prefix for generic RFC destinations and only allow RFC destinations with this prefix:
→ *Specify Prefix for Generic RFC Destinations, Page 42*
- The items depend on the order. The first matching rule is used and the reading of the rules is canceled.
For instance, if a rule is found, which denies SEAL Systems connections, the search is canceled. A rule below, which permits SEAL Systems connections, is not read and is therefore without effect.
- A rule at the end, which denies all connections, is not required, because it is set automatically by the system.
Exception: If the simulation mode is activated all connections are allowed.
- The rules have to be reread after changed in order to become effective.
- Activate the simulation mode before major changes in order to check the effects of the changes.
→ *Activate Simulation Mode for Security Configuration, Page 41*
Deactivate the simulation mode as soon as you are sure that the security settings are correct.

Activate Simulation Mode for Security Configuration


The simulation mode makes the creating of the security configuration easier. It specifies a rule at the end, which allows all connections. These are logged with a specific identifier. The security settings can be modified by means of these items.

purpose

The simulation mode is intended for analysis purposes only and does not increase in safety because the registration of non-specified connections is allowed, while a communication via these connections is denied.

This is how you activate the simulation mode:

instructions

| Step | Action |
|------|---|
| 1 | Start the transaction: smgw |
| 2 | Select: Goto →Expert Functions →Logging |
| 3 | Configure the Log Events area according to your wishes and activate in the Simulation Mode area: <ul style="list-style-type: none"> On: Activate  Hint - effects: The connection is allowed or denied if a matching rule is found. If there is no explicit rule for the connection the connection is allowed and logged in the gateway log file with Z as identifier. |
| 4 | Activate the change with Edit→Activate. |
| 5 | Deactivate the simulation mode as soon as you are sure that the security configuration is correct. |

Alternatively, you can set the gw/sim_mode profile parameter (transaction: rz11):

alternative



- If gw/sim_mode=0 (default) all connections without any explicit rule are denied. The simulation mode is deactivated.
- If gw/sim_mode=1 all connections without any explicit rule are allowed. The simulation mode is activated.

Specify Prefix for Generic RFC Destinations

description The server starts generic RFC destinations (sapftp and saphttp) at the check-out of files from the SAP system. For these, you can specify a prefix, for instance SEAL, in order to explicitly allow all destinations with this prefix.

required if These steps are only required as of EHP7 or kernel 721, if you do not want to allow generally all destinations with * in secinfo/reginfo but you want to restrict this setting as much as possible.

instructions This is how you specify the prefix for generic RFC destinations on the SAP system:

| Step | Action | | | | | | | | |
|------------|---|---------------|-------------|---------------|----------|------------|-----|--|-------|
| 1 | Start the se16n transaction with the sdokprof table. | | | | | | | | |
| 2 | Enter: <ul style="list-style-type: none"> • Key: RFC_PREFIX • Secondary Key: Empty or SAPFTP,SAPHTTP • Contents:SEAL_ (example)  Example: <table border="1" data-bbox="518 1108 1157 1187"> <thead> <tr> <th>Key</th> <th>User Client</th> <th>Secondary key</th> <th>Contents</th> </tr> </thead> <tbody> <tr> <td>RFC_PREFIX</td> <td>800</td> <td></td> <td>SEAL_</td> </tr> </tbody> </table>  Hint - SAP note: For further information see SAP note 750877. | Key | User Client | Secondary key | Contents | RFC_PREFIX | 800 | | SEAL_ |
| Key | User Client | Secondary key | Contents | | | | | | |
| RFC_PREFIX | 800 | | SEAL_ | | | | | | |

Security Configuration - Background Knowledge

The smgw transaction provides following useful functions additionally:

tips & tricks

- Gateway monitor: Goto→Trace→Gateway→Display File
Hints regarding all connections
- Clients logged on on SAP: Goto→Logged on Clients
Overview which clients/systems are logged on with which identification

Important SAP notes regarding the security configuration on <https://support.sap.com/notes>:

background
knowledge - SAP
notes

- General:
 - 1408081 - Basic settings for reg_info and sec_info
 - 1525125 - Update #1 to security note
 - 1105897 - GW: reginfo and secinfo with permit and deny ACL
 - 1425765 - Generating of sec_info reg_info
 - 2061464 - GW: Several smaller corrections in gateway
 - 2090489 - GW: Problems with registrations
- secinfo
 - 614971 - GW: Changes to the ACL list of the gateway (secinfo)
- recinfo
 - 1069911 - GW: Changes to the ACL list of the gateway (reginfo)
 - 1592493 - GW: Problems during the reginfo configuration
- proxyinfo
 - 910918 - GW: Parameter gw/prxy_info
- Gateway simulation mode
 - 1689663 - GW: Simulation mode for reg,sec and prxy_info

SAP WIKI items regarding the security configuration on <https://wiki.scn.sap.com/wiki>:

background
knowledge - SAP
WIKI

- Gateway Access Control List:
 - <https://wiki.scn.sap.com/wiki/display/SI/Gateway+Access+Control+Lists>
- SAP Network Interface and ACL Control
 - <https://wiki.scn.sap.com/wiki/display/SI/SAP+Network+Inter-face+and+ACL+control>

2.5 Start and Test RFC Destination

introduction This chapter explains how the connections for data exchange between the server and the SAP system are established and tested in the case of communication via dynamic RFC connection.

start script You can use the following alternatives as start script:

- *ModuleGlobalstart*, for instance *dvsstart*
- *sysstart System*, for instance *sysstart SAP*
- *ModuleSelectstart*, for instance *rfcserverstart*

process at the connection start The connections between the servers and the SAP systems are established as follows:

| Level | Processing |
|-------|--|
| 1 | → <i>Start the RFC Destinations on the Server, Page 45</i> |
| 2 | The start script determines the RFC destinations which are to be started: → <i>Determine RFC Destinations to be Started via the [ACTIVE] Section, Page 46</i> → <i>Determine RFC Destinations to be Started via Call Parameters, Page 47</i> |
| 3 | The start script determines the SAP system data for the RFC destinations which are to be started in <i>saprfc.ini</i> (DESTINATIONS in <i>ModuleSelect.cfg</i> like <i>rfcserver.cfg</i> and DEST in <i>saprfc.ini</i>). |
| 4 | The start script starts the RFC destinations to the SAP systems. |
| 5 | The SAP systems establish the connection to the SEAL servers via PROGID as specified in the <i>sm59</i> transaction: → <i>Test the RFC Destination on the SAP System, Page 48</i> |

in this chapter This chapter deals with the following topics:
→ *Start the RFC Destinations on the Server, Page 45*
→ *Determine RFC Destinations to be Started via the [ACTIVE] Section, Page 46*
→ *Determine RFC Destinations to be Started via Call Parameters, Page 47*
→ *Test the RFC Destination on the SAP System, Page 48*

Start the RFC Destinations on the Server

You can start the RFC destinations on the server as follows:

start on the server

- `plstart` or `sysstart PLOSSYS netdome`
Starts PLOSSYS netdome and all required RFC destinations
- `dvsstart` or `sysstart SAP`
Starts all required RFC destinations
- `rfcserverstart`, `jrffcserverstart`, `convservstart`, `convservdpfstart`, `filecheckstart`, `dvsviewserverstart`
Starts only the required RFC connections from the corresponding configuration file, for example `rfcserver.cfg`

You can check the status of the RFC destinations on the server as follows:



status check on the server

- `plsstatus` or `sysstatus PLOSSYS netdome`
Displays the status of PLOSSYS netdome and of all required RFC destinations
- `dvsstatus` or `sysstatus SAP`
Displays the status of all required RFC destinations
- `rfcserverstatus`, `jrffcserverstatus`, `convserverstatus`, `convservdpfstatus`, `filecheckstatus`, `dvsviewserverstatus`
Shows the status of the required RFC connections from the corresponding configuration file, for example `rfcserver.cfg`, on

Sometimes the RFC server can not be started, if a registration already exists on the SAP system. Stop the RFC server and test the connection on the SAP system to delete the registration; after that it should be possible to start the RFC server on the server again.

problems at start

Determine RFC Destinations to be Started via the [ACTIVE] Section

| | |
|---|---|
| format | <p>The [ACTIVE] section in <i>ModuleSelect.cfg</i> like <i>rfcserver.cfg</i> contains the section names with the RFC destinations which are to be started. Each section which is to be considered is assigned to a server name or to the general keyword SECTION:</p> <ul style="list-style-type: none"> • <i>SECTION=SectionName</i> If a section is assigned to the SECTION keyword it is considered for all servers. • <i>HostName=SectionName</i> If a section is assigned to a server it is considered only for this server. |
| evaluated by | The [ACTIVE] section is evaluated by all start scripts. |
| exception | <p>The [ACTIVE] section is ignored on these conditions:</p> <ul style="list-style-type: none"> • The SAP_START_SYSTEM environment variable is specified. • Section names are specified as parameters at the program start. |
|  example 1 | <p>The RFC destinations of the DEV, TEST and PROD sections are always to be started independently of the current server:</p> <pre>rfcserver.cfg: [ACTIVE] SECTION=DEV SECTION=TEST SECTION=PROD</pre> |
|  example 2 | <p>The following scenario is to be emulated:</p> <ul style="list-style-type: none"> • The RFC destinations of the DEV section are always to be started independently of the current server. • The RFC destinations of the DEV-EXT and PROD sections are to be started only if SEALSAP1 is the current server. • The RFC destinations of the DEV-EXT and TEST sections are to be started only if SEALSAP2 is the current server. <pre>rfcserver.cfg: [ACTIVE] SECTION=DEV SEALSAP1=DEV-EXT SEALSAP2=DEV-EXT SEALSAP2=TEST SEALSAP1=PROD</pre> |


Determine RFC Destinations to be Started via Call Parameters

The sections with the RFC destinations which are to be started are specified directly as parameters at the start. Multiple section names can be specified separated by blanks. format

The call parameters are only evaluated by the *ModuleSelectAction* scripts, for example *rfcserverstart*. The parameters specified at the start have the highest priority. The *SAP_START_SYSTEM* environment variable and the [ACTIVE] section are ignored. evaluated by

The parameters specified at the start are not evaluated by the *ModuleGlobalAction* scripts, like *dvsstart*, or *sysstart System*, like *sysstart SAP*. exception


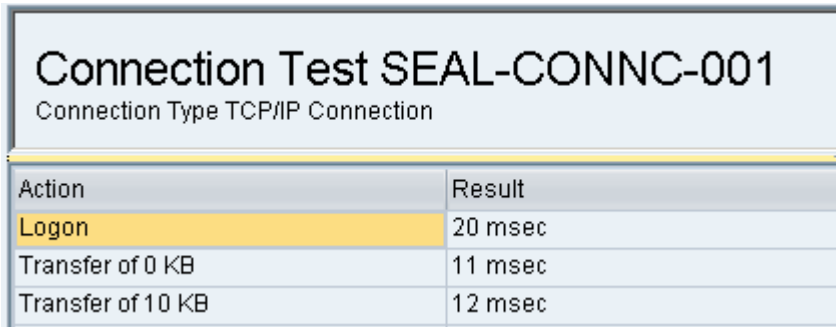
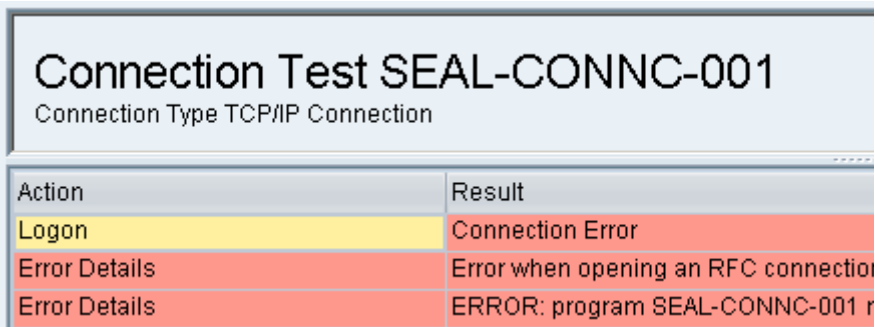
`rfcserverstart PROD`

 example


Test the RFC Destination on the SAP System

instructions -
connection test
on the SAP sys-
tem

This is how you test the RFC destination on the SAP system:

| Step | Action |
|------|--|
| 1 | Start the sm59 transaction. |
| 2 | Double-click the RFC destination which you want to test in the list TCP/IP connections. |
| 3 | Click Connection Test.  |
| 4 | In the case of success, you will get this result:  |
| 5 | In the case of error, you will get this result:  |

Test the RFC Destination on the SAP System, Continuation

| Step | Action | | | | | | | | | | | | | | | | | | | | | | | | |
|-----------------|--|---------------|--|-------------|--|-----------|----------|----------|--|---------------|--|-----------------|--|----|----------|-------------|--|---------------|------|--|-------------------|-----------|----------------|-----------------|----------------|
| 6 | <p>In the case of error, check if the RFC server on the server is actually started and PROGID in rfcserver.cfg matches the Program ID in sm59.</p> <p> Hint - connection data: You can check the current system ID of the target system with: Extras→System Information→Target System</p> <table border="1" data-bbox="339 645 1204 1265"> <thead> <tr> <th colspan="2">Target System</th> </tr> </thead> <tbody> <tr> <td>System Name</td> <td></td> </tr> <tr> <td>Host Name</td> <td>ROE-SAP-</td> </tr> <tr> <td>Database</td> <td></td> </tr> <tr> <td>Database Host</td> <td></td> </tr> <tr> <td>Database System</td> <td></td> </tr> <tr> <td>OS</td> <td>Win 2019</td> </tr> <tr> <td>SAP Host ID</td> <td></td> </tr> <tr> <td>Time Zone (s)</td> <td>3600</td> </tr> <tr> <td></td> <td>Summertime active</td> </tr> <tr> <td>System ID</td> <td>ROE-SAP-PE-003</td> </tr> <tr> <td>Network Address</td> <td>10.100.100.127</td> </tr> </tbody> </table> | Target System | | System Name | | Host Name | ROE-SAP- | Database | | Database Host | | Database System | | OS | Win 2019 | SAP Host ID | | Time Zone (s) | 3600 | | Summertime active | System ID | ROE-SAP-PE-003 | Network Address | 10.100.100.127 |
| Target System | | | | | | | | | | | | | | | | | | | | | | | | | |
| System Name | | | | | | | | | | | | | | | | | | | | | | | | | |
| Host Name | ROE-SAP- | | | | | | | | | | | | | | | | | | | | | | | | |
| Database | | | | | | | | | | | | | | | | | | | | | | | | | |
| Database Host | | | | | | | | | | | | | | | | | | | | | | | | | |
| Database System | | | | | | | | | | | | | | | | | | | | | | | | | |
| OS | Win 2019 | | | | | | | | | | | | | | | | | | | | | | | | |
| SAP Host ID | | | | | | | | | | | | | | | | | | | | | | | | | |
| Time Zone (s) | 3600 | | | | | | | | | | | | | | | | | | | | | | | | |
| | Summertime active | | | | | | | | | | | | | | | | | | | | | | | | |
| System ID | ROE-SAP-PE-003 | | | | | | | | | | | | | | | | | | | | | | | | |
| Network Address | 10.100.100.127 | | | | | | | | | | | | | | | | | | | | | | | | |

2.6 RFC Connection - Troubleshooting

typical problems
and their solu-
tions

The following table illustrates typical problems (P) and their approaches (A):

| | |
|----|--|
| P: | How is the correct connection determined when sapftp/saphttp is started? |
| L: | → <i>saphttp/sapftp Start - Background Knowledge</i> , Page 52 |
| P: | Establishing several application server - what do you need to know? |
| L: | → <i>Hints for the Load Balancing</i> , Page 53 |
| P: | Supporting a central SAP gateway - what needs to be considered? |
| L: | → <i>Support Central SAP Gateway</i> , Page 70 |
| P: | Additional information is required for troubleshooting. |
| L: | → <i>Additional Messages and Debugging</i> , Page 55 |
| P: | Transfer with sapftp/saphttp is very slow. |
| L: | → <i>Activate DLL Version of sapftp/saphttp in Case of Bottlenecks</i> , Page 56 |
| P: | The check-out of files returns an error. Possibly, the following error is logged on Unicode systems: [E] E171 Only available with the RFC library from 4.0C onwards |
| L: | → <i>Define the USE_GWHOST Parameter</i> , Page 57 |
| P: | RFC destinations cannot be established. Possible cause is the update to EhP7 or kernel 721, where the destinations are no longer accepted automatically. |
| L: | → <i>RFC and SAP Connections - Security Configuration</i> , Page 34 The simulation mode may simplify the troubleshooting: → <i>Activate Simulation Mode for Security Configuration</i> , Page 41 |
| P: | RFC destinations - sporadic connection errors or program ProgamId not registered error A network component, for example a firewall, closes the TCP/IP connection without informing the external registered RFC server program. The external RFC server program waits endlessly for incoming RFC requests. |

RFC Connection - Troubleshooting, Continuation

L: Activate logging for the SAP gateway to find the cause of the error (JCO_ERROR_CANCELLED):

→ *Activate the SAP Gateway Logging*, Page 58

Activate the RFC trace to find the cause of the error (JCO_ERR_COMMUNICATION):

→ *Activate RFC Trace*, Page 59

Avoid idle time in the network, for example by pings at regular intervals to prevent the TCP-IP connection from being closed, see SAP note 1332022 or 1494757.

P: Problems with: sapftp/saphttp

L: Activate logging for sapftp/saphttp:

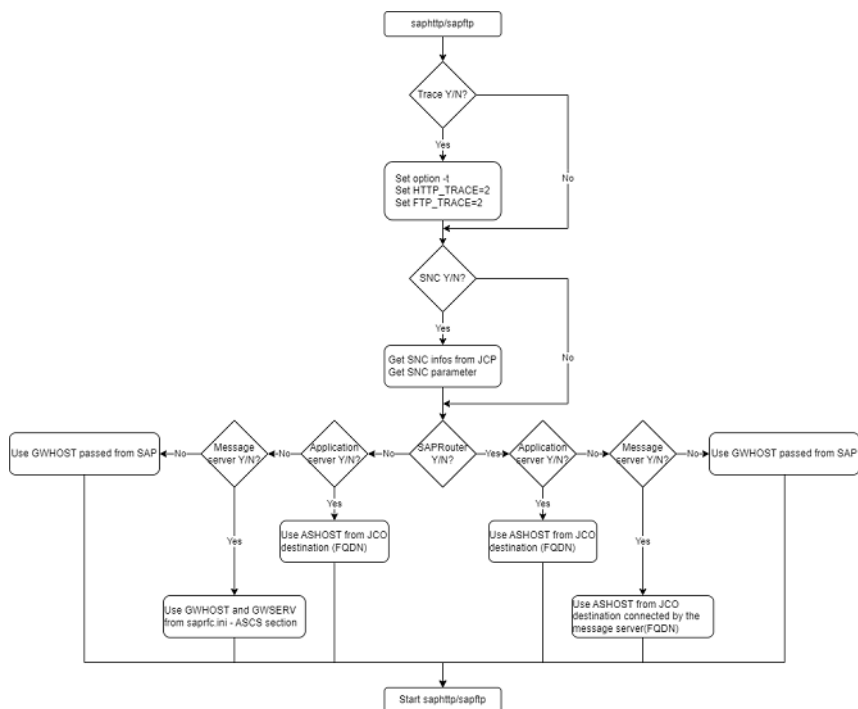
→ *Activate Trace Functions for sapftp/saphttp*, Page 60

saphttp/sapftp Start - Background Knowledge


description

When starting saphttp/sapftp, the current source node and the service for the correct connection must be determined, depending on whether an SAP router, an application server or a message server is used.

The following figure provides an overview of this determination.




Hints for the Load Balancing

| | |
|--|---|
| <p>If an SAP system consists of several application servers, for instance in order to distribute the workload (load balancing), one of these servers must be specified as the gateway so that only a single RFC server is started for this connection.</p> | <p>description</p> |
| <p>The host name of the application server is specified as Gateway Host and the gateway service as Gateway Service for the load balancing when creating the RFC destination on the SAP system.</p> | <p>specify</p> |
| <p>It is advisable to select the application server with the least downtime as Gateway host. This should also be the system's database server.</p> | <p>select the application server</p> |
| <p>If the SAP system is copied, for instance for validation purposes, these gateway options must be customized for the new (copied) system to use the RFC destination of the second system!</p> | <p> Caution - copy of the SAP system</p> |
| <p>SEAL Systems products support load balancing/reliability in different ways:</p> | <p>overview</p> |

| Product | Load Balancing/Reliability |
|--------------------------|--|
| <p>Conversion Server</p> | <p>Scenario 1: Several application servers with one message server which convert independently - even in case of failure of another application server. Solution:</p> <ul style="list-style-type: none"> • Establish the RFC destination (sm59 transaction) without any gateway option. • Establish one RFC server connection of type R with different names and application server but identical program ID for each application server. <p>Scenario 2: Load Balancing/Reliability Solution: This functionality is provided by the SAP standard conversion. Several RFC destinations (converter numbers) can be specified for each conversion.</p> |

Hints for the Load Balancing, Continuation

| Product | Load Balancing/Reliability |
|---|--|
| RFC Server: <ul style="list-style-type: none"> • DMS View Server • Core Convert | <p>The functionality described as scenario 2 is supported by Conversion Server.</p> <p>Alternative when using JRFC Server:</p> <p>You may assign several JRFC Server via the same RFC destination.</p> <p> Hint - restriction:</p> <p>The JRFC Server which will execute the function is selected by random. The execution of the individual functions must therefore be independently. This is only valid for parts of the BC XDC Interface Implementation (assignment and status query can be executed on different servers).</p> |
| RFC client | RFC clients support the SAP load balancing via message servers (type B). |
| CD Installations | <p>CD installations from SEAL Systems (type A) do not support the automatic load balancing.</p> <p>The configuration files, for instance <code>saprfc.ini</code> and <code>rfcserver.cfg</code>, must be modified and saved manually.</p> |

Additional Messages and Debugging

You can activate additional files with trace messages, if the RFC destinations cause difficulties. The debugging of system functions can be activated for RFC client destinations alternatively. description

You activate the trace messages with RFC_TRACE in `saprfc.ini`. activate trace messages
Alternatively, you can also activate the RFC trace or SAP Gateway logging within the SAP system:

→ *Activate the SAP Gateway Logging, Page 58*

→ *Activate RFC Trace, Page 59*

You activate the debugging of system functions with ABAP_DEBUG in `saprfc.ini`. debugging of system functions

Activate DLL Version of sapftp/saphttp in Case of Bottlenecks

required if These steps are only required if you want to use the DLL variant of the sapftp and saphttp programs due to performance reasons.

requirements The following requirement must be fulfilled:

- The sapftp.dll and saphttp.dll files must be located in the tools\bin_winxx directory.
- In the SAP system, the /seal/bas_dm_be_checkoutviewx function must exist.



instructions This is how you activate the DLL variant of the sapftp and saphttp programs:

| Step | Action |
|------|---|
| 1 | Edit the following file: plossys.ini |
| 2 | Enter: [rlistsap] CAD_CHECKOUT_DLL = Y |
| 3 | Enter: [rlistsap] BAPI_DOCUMENT_CHECKOUTVIEWX = /SEAL/BAS_DM_BE_CHECKOUTVIEWX ARC_CHECKOUT_RETRY_ERROR=Y |

Define the USE_GWHOST Parameter

The check-out of files from the SAP systems returns an error. One of the reasons could be that a wrong host name is used at the start of sapftp and saphttp - required for the check-out - when using several application servers. The determination of the host name can be influenced by the USE_GWHOST parameter.

This is how you specify the value for the USE_GWHOST parameter: instructions

| Step | Action | | | | | | | | | | | | | | | |
|------------------|---|-------------------------------------|--|--|--------------|-----------------|-------------------|------------------|---|-------------------------------------|------------------|---|----------------------------------|------------------|---|---------------------|
| 1 | Start the /seal/img transaction. | | | | | | | | | | | | | | | |
| 2 | Click  at Basis Configuration →Define Parameters (table: /seal/bas_cr142) | | | | | | | | | | | | | | | |
| 3 | Specify the value of the USE_GWHOST parameter with: <ul style="list-style-type: none"> • RFC server destinations: PARA_GWHST: Y or N • RFC client destinations: PARA_GWHSB: Y or N  Example: <table border="1" data-bbox="331 1137 1204 1355"> <thead> <tr> <th colspan="3">Parameter</th> </tr> <tr> <th>Parameter ID</th> <th>Parameter Value</th> <th>Short Description</th> </tr> </thead> <tbody> <tr> <td>PARA_DDEST Un...</td> <td>X</td> <td>Unconditional use of destination NO</td> </tr> <tr> <td>PARA_GWHSB Pa...</td> <td>N</td> <td>Value for USE_GWHOST with destir</td> </tr> <tr> <td>PARA_GWHST Pa...</td> <td>N</td> <td>Wert for USE_GWHOST</td> </tr> </tbody> </table> Default is for both parameters: N | Parameter | | | Parameter ID | Parameter Value | Short Description | PARA_DDEST Un... | X | Unconditional use of destination NO | PARA_GWHSB Pa... | N | Value for USE_GWHOST with destir | PARA_GWHST Pa... | N | Wert for USE_GWHOST |
| Parameter | | | | | | | | | | | | | | | | |
| Parameter ID | Parameter Value | Short Description | | | | | | | | | | | | | | |
| PARA_DDEST Un... | X | Unconditional use of destination NO | | | | | | | | | | | | | | |
| PARA_GWHSB Pa... | N | Value for USE_GWHOST with destir | | | | | | | | | | | | | | |
| PARA_GWHST Pa... | N | Wert for USE_GWHOST | | | | | | | | | | | | | | |

When using sapftp/saphttp, the host name is passed via the GWHOST parameter and transferred to librfc23, for instance: background knowledge

sapftp -xHostName


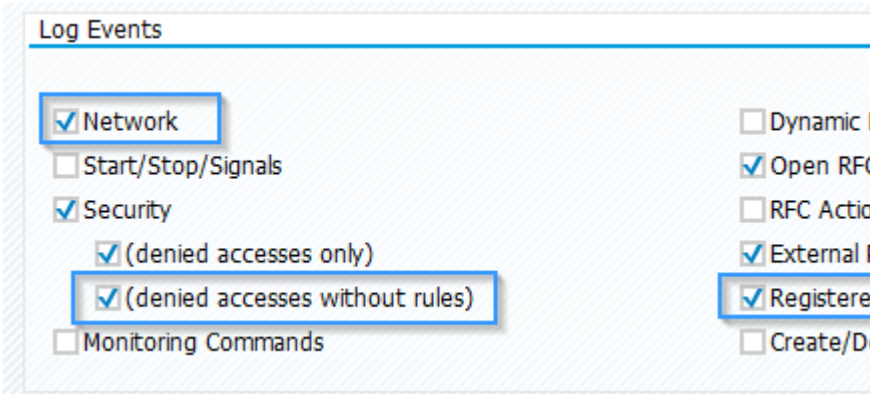

The *HostName* is previously determined via the Z_SYS_INFO function for RFC server destinations and via the SYSTEM_GET_CURRENT_GATEWAY function for RFC client destinations.

librfc32 uses the transferred value or determine the host name again for itself. This depends on the value of the USE_GWHOST parameter. With USE_GWHOST Y the transferred value is used, with USE_GWHOST N the host name is determined again.

Activate the SAP Gateway Logging

description If there are problems with RFC destinations, you can activate the RFC trace to search for the cause of the error in the generated trace files.

instructions This is how you activate the SAP gateway logging:

| Step | Action |
|------|---|
| 1 | Start the transaction: smgw |
| 2 | Select: Goto →Expert Functions →Logging |
| 3 | <p>Activate the following options in the Log Events area:</p> <ul style="list-style-type: none"> • Network: Activate • Security - (denied accesses without rules): Activate • Registered Programs: Activate <p> Example:</p>  |
| 4 | <p>Display the log to search for the cause of the error:</p> <hr/> <p>3 </p> <p>d</p> <p>» Generating File Name</p> <p>nth, %d=day, %h=hour, %t=minute, %s=second</p> |

Activate RFC Trace

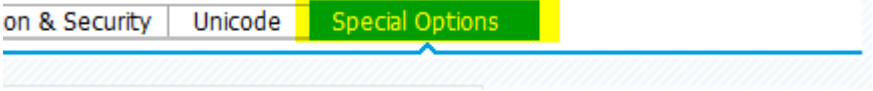


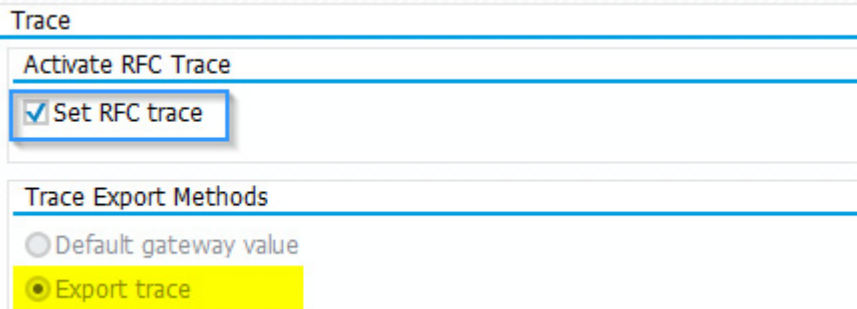
If there are problems with RFC destinations, you can activate the RFC trace to search for the cause of the error in the generated trace files. description

Alternatively, you can also activate the RFC trace on the server side: alternative

→ *RFC_TRACE* Parameter, Page 144

→ *SEAL_TRACE* Parameter, Page 145

This is how you activate the RFC trace: instructions

| Step | Action |
|------|---|
| 1 | Start the transaction: sm59 |
| 2 | Switch to the tab: Special Options  |
| 3 | Activate the following option in the Trace area: <ul style="list-style-type: none"> Set RFC Trace: Activate  Hint - effects: This automatically activates the Export Trace option in the Trace Export Methods section and overrides the gw/export_trace_level profile parameter. See also SAP note 558254.  Example:  |

The following trace files are created: result

- dev_jco_rfc.log
- jco_rfcPID_UUID.trc

After successful cause analysis, deactivate the option Set RFC Trace again. deactivate trace

Activate Trace Functions for sapftp/saphttp

description You can use environment variables to activate trace functions for sapftp/saphttp.

When sapftp/saphttp is started by JRFC Server, SEAL_TRACE=1 (or higher) is available in saprfc.ini as an alternative.

When sapftp/saphttp is started by JSAPcli, the -ft parameter or the SAPCLI_FULL_TRACE=1 environment variable is available as an alternative.

instructions This is how you activate the trace functions for sapftp/saphttp if they are not started by JRFC Server or JSAPcli:

| Step | Action |
|------|---|
| 1 | Set following environment variable: <ul style="list-style-type: none"> • For sapftp: FTP_TRACE=2 • For saphttp: HTTP_TRACE=2 |
| 2 | Activate the changed environment variables to make them available in the context of the SEALServiceuser: <ul style="list-style-type: none"> • sitwelcome • sysstop • Close SEAL shell • Open SEAL shell • sysstart Restart at least all processes, such as rlist, whose start is to be analysed by sapftp/saphttp. |

3 Static RFC Destinations for SNC Support

This chapter explains how the connections for the data exchange between servers and SAP systems are established and tested in case of communications via static RFC destinations. Static RFC destinations offer the following advantages:

introduction

- SNC is supported for sapftp/saphttp
- Static RFC destinations can be explicitly enabled/restricted at the gateway.

Static RFC destinations are available for:

- RFC client:
JSAPcli, for example, within PLOSSYS Distribution Engine for checking-out original files or for re-archiving
- RFC server:
DMS Loader/ABAP in RFC mode for files with storage not equal to KPRO (web server)
XSA in RFC mode for files with storage not equal to KPRO (web server)
(DMS View Server is not affected, as it uses the integrated sapftp/saphttp functionality of JRFC Server and no external processes).

This chapter deals with the following topics:

in this chapter

- *Establish Templates for sapftp/saphttp (sm59)*, Page 62
- *Create Multiple sapftp/saphttp Destinations*, Page 65
- *RFC Client - Assign Static sapftp/saphttp Destination*, Page 68
- *RFC Server - Assign Static sapftp/saphttp Destination*, Page 69
- *Support Central SAP Gateway*, Page 70

Establish Templates for sapftp/saphttp (sm59)





















description

The following templates must be established manually for the static sapftp/saphttp connections:


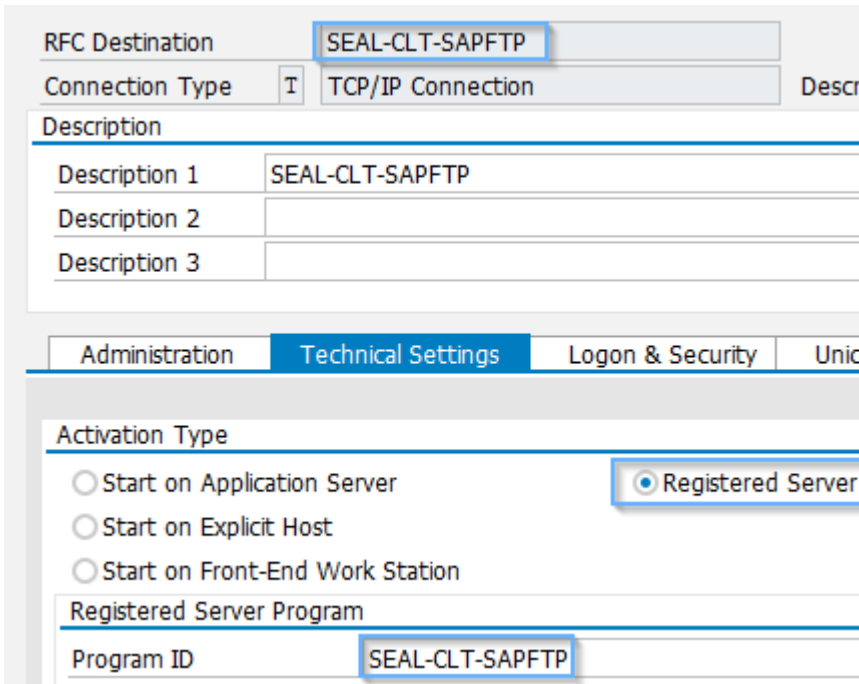

- For RFC client (for example, for use by JSAPcli):
 - SEAL-CLT-SAPFTP
 - SEAL-CLT-SAPHTTP
- For RFC servers (for example, for use by DMS Loader/ABAP in RFC mode for files with storage not equal to KPRO (web server)):
 - SEAL-SRV-SAPFTP

instructions




This is how you establish the necessary templates for the static sapftp/saphttp connections:

| Step | Action | | | | | | | | | | | | | | |
|---|---|-----------------|------|--|---|---|---|---|---|--|---|---|---|---|----------|
| 1 | Start the transaction: /n/seal/img | | | | | | | | | | | | | | |
| 2 | <p>Click  at</p> <p>Basis Configuration</p> <p>→Static Destinations</p> <p>→Establish RFC Destinations</p> <p> Hint - alternative:</p> <p>Start the sm59 transaction.</p> | | | | | | | | | | | | | | |
| 3 | <p>Select the connection type on the left:</p> <p>TCP/IP Connections (Type: T)</p> <table border="1"> <thead> <tr> <th>RFC Connections</th> <th>Type</th> </tr> </thead> <tbody> <tr> <td>>  ABAP Connections</td> <td>3</td> </tr> <tr> <td>>  HTTP Connections to External Server</td> <td>G</td> </tr> <tr> <td>>  HTTP Connections to ABAP System</td> <td>H</td> </tr> <tr> <td>>  Internal Connections</td> <td>I</td> </tr> <tr> <td>>  Logical Connections</td> <td>L</td> </tr> <tr> <td>>  TCP/IP Connections</td> <td>T</td> </tr> </tbody> </table> | RFC Connections | Type | >  ABAP Connections | 3 | >  HTTP Connections to External Server | G | >  HTTP Connections to ABAP System | H | >  Internal Connections | I | >  Logical Connections | L | >  TCP/IP Connections | T |
| RFC Connections | Type | | | | | | | | | | | | | | |
| >  ABAP Connections | 3 | | | | | | | | | | | | | | |
| >  HTTP Connections to External Server | G | | | | | | | | | | | | | | |
| >  HTTP Connections to ABAP System | H | | | | | | | | | | | | | | |
| >  Internal Connections | I | | | | | | | | | | | | | | |
| >  Logical Connections | L | | | | | | | | | | | | | | |
| >  TCP/IP Connections | T | | | | | | | | | | | | | | |

Establish Templates for sapftp/saphttp (sm59), Continuation

| Step | Action |
|------|--|
| 4 | <p>Create three items with the following settings in the Technical Settings tab:</p> <ul style="list-style-type: none"> • For RFC client - SAPFTP: <ul style="list-style-type: none"> • RFC Destination: SEAL-CLT-SAPFTP (maximum 28 characters) • Registered Server Program: Activate • Program ID: Value of RFC Destination • For RFC client - SAPHTTP: <ul style="list-style-type: none"> • RFC Destination: SEAL-CLT-SAPHTTP (maximum 28 characters) • Registered Server Program: Activate • Program ID: Value of RFC Destination • For RFC server - SAPFTP: <ul style="list-style-type: none"> • RFC Destination: SEAL-SRV-SAPFTP (maximum 28 characters) • Registered Server Program: Activate • Program ID: Value of RFC Destination <p> Example - RFC client - SAPFTP:</p>  <p> Hint - copy existing RFC destination: Generally, you already have an RFC destination in use. You can copy this and enter the settings mentioned above: Connection→Copy (Ctrl+F12)</p> |

Establish Templates for sapftp/saphttp (sm59), Continuation

| Step | Action | | | | | | | | | | | | |
|-----------------|--|---|-----------------------------|--|---------|---|---|-----------|--|--|----------|-------------------------------------|--|
| 5 | <p>On the Technical Settings tab, enter the gateway options:</p> <ul style="list-style-type: none"> Gateway Host: <i>GWHOST</i> from <i>saprfc.ini</i> Gateway Service: <i>GWSERV</i> from <i>saprfc.ini</i> <p> Example:</p> <div data-bbox="587 611 1284 741" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p style="text-align: center; border-bottom: 1px solid #0070c0; margin: 0;">Gateway Options</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;">Gateway Host</td> <td style="padding: 2px;">roesap005.sealsystems.local</td> </tr> <tr> <td style="padding: 2px;">Gateway service</td> <td style="padding: 2px;">sapgw01</td> </tr> </table> </div> <p>Background info: JSAPcli uses this information for static sapftp/saphttp destinations.</p> | Gateway Host | roesap005.sealsystems.local | Gateway service | sapgw01 | | | | | | | | |
| Gateway Host | roesap005.sealsystems.local | | | | | | | | | | | | |
| Gateway service | sapgw01 | | | | | | | | | | | | |
| 6 | <p>For SNC destinations, enter in the Logon & Security tab under Security Options:</p> <ul style="list-style-type: none"> SNC: SNC parameter, enter Active: Activate <p> Example - SNC parameter:</p> <div data-bbox="528 1160 1390 1361" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;">Destination</td> <td style="padding: 2px;">SEAL-CLT-SAPFTP-SNC</td> <td style="padding: 2px; text-align: right;"><input checked="" type="checkbox"/> SNC Active</td> </tr> <tr> <td style="padding: 2px;">QoP</td> <td style="padding: 2px;">8</td> <td style="padding: 2px;">Default (profile parameter snc/data_protection/use_...)</td> </tr> <tr> <td colspan="3" style="padding: 2px;">SNC names</td> </tr> <tr> <td style="padding: 2px;">Partners</td> <td colspan="2" style="padding: 2px;">p:CN=SEALRFC,OU=SEALSAP,O=SEAL,C=DE</td> </tr> </table> </div> <p> Caution - saprfc.ini: The SNC settings in <i>saprfc.ini</i> must also be activated on the server:</p> <ul style="list-style-type: none"> SNC_MODE=1 SNC_MYNAME=p:CN=SEALRFC,OU=SEALSAP,O=SEAL,C=DE SNC_QOP=8 <p>The system ID used is defined via <i>rfcserver.cfg</i> (RFC server) or <i>cadrfc.ini</i> (RFC client).</p> | Destination | SEAL-CLT-SAPFTP-SNC | <input checked="" type="checkbox"/> SNC Active | QoP | 8 | Default (profile parameter snc/data_protection/use_...) | SNC names | | | Partners | p:CN=SEALRFC,OU=SEALSAP,O=SEAL,C=DE | |
| Destination | SEAL-CLT-SAPFTP-SNC | <input checked="" type="checkbox"/> SNC Active | | | | | | | | | | | |
| QoP | 8 | Default (profile parameter snc/data_protection/use_...) | | | | | | | | | | | |
| SNC names | | | | | | | | | | | | | |
| Partners | p:CN=SEALRFC,OU=SEALSAP,O=SEAL,C=DE | | | | | | | | | | | | |

Create Multiple sapftp/saphttp Destinations


If you use multiple RFC servers, for example for DMS Loader/ABAP and XSA in RFC mode for files with storage not equal KPRO (web server), which are to use static sapftp destinations, you must create a corresponding number of sapftp destinations.

description






For the RFC client, it makes sense to create several static sapftp/saphttp destinations for parallel mode, for example multiple JSAPcli calls at the same time for checking-out the original files and for the re-archiving within PLOSSYS Distribution Engine.

This is how you create multiple sapftp/saphttp destinations based on the created templates:

instructions

| Step | Action |
|------|--|
| 1 | Start the transaction: /n/seal/img |
| 2 | Click  at Basis Configuration →Static Destinations →Copy Template for Static sapftp/saphttp (transaction: /n/seal/bas_cr_dest, program: /seal/ bas_cr_dest_create) |

Create Multiple sapftp/saphttp Destinations, Continuation

| Step | Action | | | | | | | | | | | | |
|------------------|--|------------------|------------------|-----------------|-----------------|--------|---|------------------|--|-----------------|-----------------|--------|---|
| 3 | <p>Enter the following values for RFC client and then create the destinations with  :</p> <ul style="list-style-type: none"> • RFC client: <ul style="list-style-type: none"> • Template SAPFTP: SEAL-CLT-SAPFTP Template for RFC client - SAPFTP from → <i>Establish Templates for sapftp/saphttp (sm59), Page 62</i> • Template SAPHTTP: SEAL-CLT-SAPHTTP Template for RFC client - SAPHTTP from → <i>Establish Templates for sapftp/saphttp (sm59), Page 62</i> • Number: Desired number of static destinations <p> Example:</p> <div data-bbox="528 887 1353 1144" style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p style="text-align: center;">Create SAPFTP and SAPHTTP Destinations</p> <p style="text-align: center;"></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 60%;">Template SAPHTTP</td> <td>SEAL-CLT-SAPHTTP</td> </tr> <tr> <td>Template SAPFTP</td> <td>SEAL-CLT-SAPFTP</td> </tr> <tr> <td>Number</td> <td style="text-align: center;">3</td> </tr> </table> </div> <ul style="list-style-type: none"> • RFC server: <ul style="list-style-type: none"> • Template SAPFTP: SEAL-SRV-SAPFTP Template for RFC server - SAPFTP from → <i>Establish Templates for sapftp/saphttp (sm59), Page 62</i> • Template SAPHTTP: Empty • Number: Desired number of static destinations <p> Example:</p> <div data-bbox="528 1480 1353 1738" style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p style="text-align: center;">Create SAPFTP and SAPHTTP Destinations</p> <p style="text-align: center;"></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 60%;">Template SAPHTTP</td> <td></td> </tr> <tr> <td>Template SAPFTP</td> <td>SEAL-SRV-SAPFTP</td> </tr> <tr> <td>Number</td> <td style="text-align: center;">4</td> </tr> </table> <p>Background knowledge - no SAPHTTP required: RFC servers have an integrated saphttp destination so that none needs to be created.</p> </div> | Template SAPHTTP | SEAL-CLT-SAPHTTP | Template SAPFTP | SEAL-CLT-SAPFTP | Number | 3 | Template SAPHTTP | | Template SAPFTP | SEAL-SRV-SAPFTP | Number | 4 |
| Template SAPHTTP | SEAL-CLT-SAPHTTP | | | | | | | | | | | | |
| Template SAPFTP | SEAL-CLT-SAPFTP | | | | | | | | | | | | |
| Number | 3 | | | | | | | | | | | | |
| Template SAPHTTP | | | | | | | | | | | | | |
| Template SAPFTP | SEAL-SRV-SAPFTP | | | | | | | | | | | | |
| Number | 4 | | | | | | | | | | | | |

background knowledge

When copying from the source destination to the target destination, the following values are set:

- Description 1 is passed
- SNC parameter are passed

Create Multiple sapftp/saphttp Destinations, Continuation

- The target destination is always configured as an Unicode SAP system
- Whitelist, timeout parameters and others are not passed, which is why the target destination must be checked again afterwards

RFC Client - Assign Static sapftp/saphttp Destination




description

As soon as you perform the configuration described here, static instead of dynamic RFC destinations are started for the specified user - or for all users if the user is empty.

Dynamic RFC destinations are only used if no item exists for the user.

instructions

This is how you assign the templates for the RFC client:



| Step | Action | | | | | | | | | | | | |
|------------------------------------|---|------------------------------------|--------|--|--|-----------|---------|--------|--------|--|------------------|-----------------|---|
| 1 | Start the transaction: /n/seal/img | | | | | | | | | | | | |
| 2 | <p>Click  at</p> <p>Basis Configuration</p> <p>→Static Destinations</p> <p>→Create Static Destination for RFC Client</p> <p>(table: /seal/bas_cr114)</p> | | | | | | | | | | | | |
| 3 | <p>Enter:</p> <ul style="list-style-type: none"> • User Name: User with which the RFC client logs on to SAP from <code>cadrfc.ini</code>, or empty (default) • SAPHTTP: SEAL-CLT-SAPHTTP Template for RFC client - SAPHTTP from → <i>Establish Templates for sapftp/saphttp (sm59)</i>, Page 62 • SAPFTP: SEAL-CLT-SAPFTP Template for RFC client - SAPFTP from → <i>Establish Templates for sapftp/saphttp (sm59)</i>, Page 62 • Number: Number of possible sapftp/saphttp destinations including the template You can create this number of destinations with: → <i>Create Multiple sapftp/saphttp Destinations</i>, Page 65 <p> Example:</p> <table border="1" data-bbox="528 1738 1315 1868"> <thead> <tr> <th colspan="4">Static destinations for RFC Client</th> </tr> <tr> <th>User Name</th> <th>SAPHTTP</th> <th>SAPFTP</th> <th>Number</th> </tr> </thead> <tbody> <tr> <td></td> <td>SEAL-CLT-SAPHTTP</td> <td>SEAL-CLT-SAPFTP</td> <td>3</td> </tr> </tbody> </table> <p> Hint - number:</p> <p>The number includes the template. This means that for number 3, two destinations -001 and -002 are created in addition to the template.</p> | Static destinations for RFC Client | | | | User Name | SAPHTTP | SAPFTP | Number | | SEAL-CLT-SAPHTTP | SEAL-CLT-SAPFTP | 3 |
| Static destinations for RFC Client | | | | | | | | | | | | | |
| User Name | SAPHTTP | SAPFTP | Number | | | | | | | | | | |
| | SEAL-CLT-SAPHTTP | SEAL-CLT-SAPFTP | 3 | | | | | | | | | | |

RFC Server - Assign Static sapftp/saphttp Destination

As soon as you perform the configuration described here, static instead of dynamic RFC destinations are started for the specified RFC server - or for all RFC servers if RFC server is empty. description

Dynamic RFC destinations are only used if no item exists for the RFC server.

This is how you assign the templates for the RFC server: instructions

| Step | Action | | | | | | |
|------------------------------------|---|------------------------------------|--|--------|--------|---------------------|-----------------|
| 1 | Start the transaction: /n/seal/img | | | | | | |
| 2 | Click  at Basis Configuration →Static Destinations →Create Static Destination for RFC Server (table: /seal/bas_cr113) | | | | | | |
| 3 | Enter: <ul style="list-style-type: none"> • Server: RFC destination, for example from <code>rfcserver.cfg</code>, which should use a static sapftp destination Depending on how many servers are to use static sapftp destinations, you must create this number of destinations with: • SAPFTP: SEAL-SRV-SAPFTP Template for RFC server - SAPFTP from → <i>Establish Templates for sapftp/saphttp (sm59)</i>, Page 62  Example: <table border="1" style="margin-top: 10px; width: 100%;"> <thead> <tr> <th colspan="2" style="background-color: #d3d3d3;">Static Destinations for RFC Server</th> </tr> <tr> <th style="background-color: #d3d3d3;">Server</th> <th style="background-color: #d3d3d3;">SAPFTP</th> </tr> </thead> <tbody> <tr> <td style="background-color: #d3d3d3;">SEAL-CONN-OKX74-002</td> <td style="background-color: #d3d3d3;">SEAL-SRV-SAPFTP</td> </tr> </tbody> </table> | Static Destinations for RFC Server | | Server | SAPFTP | SEAL-CONN-OKX74-002 | SEAL-SRV-SAPFTP |
| Static Destinations for RFC Server | | | | | | | |
| Server | SAPFTP | | | | | | |
| SEAL-CONN-OKX74-002 | SEAL-SRV-SAPFTP | | | | | | |




Support Central SAP Gateway

requirement The destination via a central SAP gateway is only supported together with static RFC destinations.

restriction The following restrictions apply to the destination via a central SAP gateway:

- SNC is only supported on request.
- The connection via SAProuter is only supported on request.

instructions This is how you support a central SAP gateway:

| Step | Description |
|------|--|
| 1 | On the server, open: <code>saprfc.ini</code> |
| 2 | Only for RFC client destinations, such as JSAPcli In the section for the message server (B type), also enter the name of the section containing the data of the central SAP gateway with: <code>ASCS=<section of the central SAP gateway of type R></code>  Example: <code>DEST=W74</code> <code>TYPE=B</code> <code>ASCS=W74RFC</code> |
| 3 | Enter the data of the central SAP gateway in the section of type R that you specified in step 2 for ASCS.  Example: <code>DEST=W74RFC</code> <code>TYPE=R</code> <code>GWHOST=roesap005.sealsystems.local</code> <code>GWSERV=sapgw01</code> <code>RFC_TRACE=0</code> <code>SEAL_TRACE=0</code> <code>UNICODE=1</code>  Hint - RFC client/RFC server: For RFC client destinations, both sections are required. For RFC server destinations, the section with type R contains the data of the central SAP gateway. No further section is required. |

example

This example shows items in `saprfc.ini` for a connection via a central SAP gateway:

Support Central SAP Gateway, Continuation

```
DEST=W74
TYPE=B
MHOST=roesap005.sealsystems.local
R3NAME=W74
GROUP=PUBLIC
ASCS=W74RFC
RFC_TRACE=0
ABAP_DEBUG=0
USE_SAPGUI=1
# Enter data of the central SAP gateway as type R
DEST=W74RFC
TYPE=R
GHOST=roesap005.sealsystems.local
GWSERV=sapgw01
RFC_TRACE=0
SEAL_TRACE=0
UNICODE=1
```

For RFC client destinations, both sections are required.

note

For RFC server destinations, the section with type R contains the data of the central SAP gateway. No further section is required.

4 HTTP Connection (REST) - Configuration

introduction This chapter describes the configuration settings required for communication via HTTP connections, which are used in combination with a REST interface, for example.



reference

For information on HTTPS support, see [SAP_BASECONF_HTTPS_TEC].

in this chapter

This chapter deals with the following topics:

→ *HTTP Connection - Configuration on Server*, Page 73

→ *Create an HTTP Connection on the SAP System*, Page 77

4.1 HTTP Connection - Configuration on Server

This chapter deals with the following topics:

in this chapter

→ *Create PSE*, Page 74

→ *Activate Logon with Basic Authentication and SSL*, Page 75



Create PSE

requirement

The certificates have to be provided in the X.509 Base64 format.

instructions

This is how you create a PSE for HTTPS on the external server, using Windows as an example:

| Step | Action |
|------|--|
| 1 | Logon on the server as user who start the processes which use saphttp, for instance the SEALService user. |
| 2 | Switch to the SECUDIR directory. |
| 3 | <p>Create the SAPSSLC PSE:</p> <ul style="list-style-type: none"> sapgenpse.exe gen_pse -noreq -p SAPSSLC.pse <p> Caution - PIN: A PIN has to be entered for the creation. Remember the PIN for further configuration.</p> <p> Hint - PSE user: Note the format at ,distinguished name of PSE owner', for instance: CN=SEAL, OU=SEALSAP, O=SEAL, C=DE CN is mandatory, all other parameters could be empty.</p> |
| 4 | <p>Integrate the root certificate and the intermediate certificate from Web server into the SAPSSLC PSE, for example:</p> <ul style="list-style-type: none"> sapgenpse.exe maintain_pk -p SAPSSLC.pse -mRootCertificate.crt sapgenpse.exe maintain_pk -p SAPSSLC.pse -mWebserverCertificate.crt |
| 5 | <p>Copy the SAPSSLC PSE if SAPSSLS.pse does not exist, with:</p> <pre>cp SAPSSLC.pse SAPSSLS.pse</pre> |
| 6 | <p>Create the cred_v2 file for the SEALService user via the execution of sapgenpse.exe, with the PIN from step 3, for instance:</p> <pre>sapgenpse.exe seclogin -O SEALServiceUser -p SAPSSLC.pse -x PIN sapgenpse.exe seclogin -O SEALServiceUser -p SAPSSLS.pse -x PIN</pre> |
| 7 | <p>Check the imported certificates:</p> <pre>sapgenpse.exe maintain_pk -p SAPSSLC.pse -l sapgenpse.exe maintain_pk -p SAPSSLS.pse -l</pre> |

Activate Logon with Basic Authentication and SSL

The recommended logon method is to logon with user and basic authentication. description

This is how you activate basic authentication and SSL as logon method on the external server: instructions

| Step | Action |
|------|---|
| 1 | Open a SEAL shell and start the command: <pre>sysinit dpf</pre> Enter: <ul style="list-style-type: none"> • Do you want to configure DPF: Y • DPF Web authentication type: basic • User name for DPF Web basic authentication [wsuer]: RETURN • New password: Enter new password for wsuser and confirm again • Do you want to configure fastlogin: Y |
| 2 | Enter: <pre>sysinit -auto</pre> Result: As a result, the following items exist: <ul style="list-style-type: none"> • File: applications\server\web\apache\conf\extra\httpd-ssl.conf JkMount /rest/* seal-worker JkMount /rest seal-worker • File: applications\server\web\apache\conf\httpd.conf Include d:/SEAL/customer/server/web/conf/auth-basic-dpf.conf (example) |
| 3 | Enter in the include file of the last step: <ul style="list-style-type: none"> • File: customer\server\web\conf\auth-basic-dpf.conf: Add to LocationMatch: rest/ Example: <LocationMatch “/(dpf4c-sercive-v1.3/ pdflls-service-v1.0/ cgi-bin/testAuth/ /rest/dpf/v1/ /rest rest)”> |
| 4 | Enter: <ul style="list-style-type: none"> • sysstop -full web |

Activate Logon with Basic Authentication and SSL,

Continuation

| Step | Action |
|------|--|
| 5 | Enter: <ul style="list-style-type: none">• Do you want to configure Apache Web Server: Y• Should the web server support the secure HTTPS protocol: Y• Enter the SSL certification file [conf/sealsystems-ca]: Basis name of the certificate without path and without file extension• Should access only be allowed via HTTPS: Y• Do you want to configure fastlogin: Y |
| 6 | Enter: <ul style="list-style-type: none">• <code>sysstart web</code> |

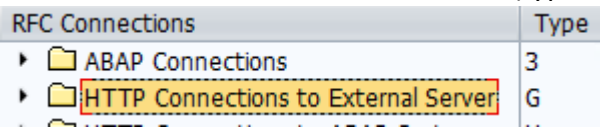
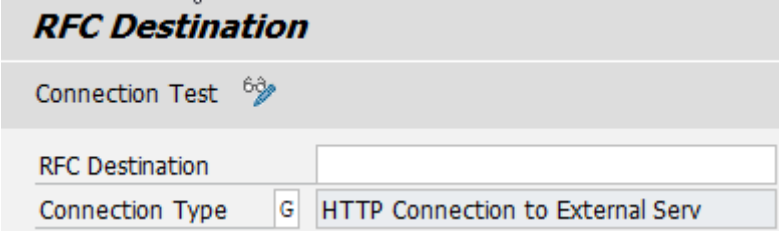

4.2 Create an HTTP Connection on the SAP System

An HTTP connection can be used to transfer data from SAP to an external system, for example in combination with a REST interface. description

Alternatively, the following transfer types are available: alternative

→ *Establish the RFC Destination on the SAP System, Page 29*


This is how you create the HTTP connection required for the REST interface: procedure - over-view


| Step | Action |
|------|--|
| 1 | Start the sm59 transaction. |
| 2 | Select the connection type on the left: HTTP Connection to External Server (type: G)  |
| 3 | Click Create:  |
| 4 | → <i>HTTP Connection - Basis Data, Page 78</i> |
| 5 | → <i>HTTP Connection - Technical Settings, Page 79</i> |
| 6 | → <i>HTTP Connection - Logon & Security, Page 80</i> |
| 7 | → <i>HTTP Connection - Special Options, Page 82</i> |
| 8 | Save the settings. |
| 9 | Activate the service required for HTTP transfer if it is deactivated: <ul style="list-style-type: none"> • Transaction: sicf • Start the display via  with: Hierarchy Type: SERVICE • Open tree display on the left: default_host - sap - bc • In the context menu check if service is active for: rest |

HTTP Connection - Basis Data

necessary settings

Enter the following settings:

| Parameters | Value |
|-----------------|---|
| RFC Destination | <i>Unique identifier on the SAP system</i>  Example: SEAL-REST-001 |
| Connection Type | G |
| Description | <i>Describing text</i> |

 example

| | |
|-----------------|------------------------------------|
| RFC Destination | SEAL-REST-001 |
| Connection Type | G HTTP Connection to External Serv |
| Description | |
| Description 1 | Process Output REST Interface |

HTTP Connection - Technical Settings


Switch to the Technical settings tab.

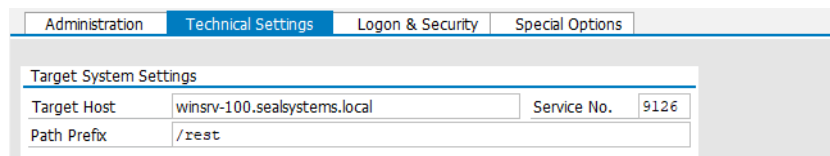
requirement

Enter the following settings:

necessary settings

| Parameter | Value |
|----------------|---|
| Target Host | IP addresses of the host with web service, for example: 10.100.53.47 |
| Service Number | 9125 (HTTP), 9126 (HTTPS) |
| Path prefix | /rest |

 example




The screenshot shows the SAP configuration interface with the 'Technical Settings' tab selected. The 'Target System Settings' section contains the following fields:


| Target System Settings | |
|------------------------|------------------------------|
| Target Host | winsrv-100.sealsystems.local |
| Service No. | 9126 |
| Path Prefix | /rest |

HTTP Connection - Logon & Security

requirement Switch to the Logon & Security tab.

necessary settings Enter the following settings:

| Parameter | Value |
|-------------------|--|
| Logon with User | <ul style="list-style-type: none"> Basic Authentication: Activate user: user for logon password: password for logon  Hint - requirement: → <i>Activate Logon with Basic Authentication and SSL, Page 75</i> |
| Logon with Ticket | Do Not Send Logon Ticket: Activate |
| Security Options | <ul style="list-style-type: none"> SSL: Activate SSL Certificate: DFAULT SSL Client (Standard) |

 example

HTTP Connection - Logon & Security, Continuation

The screenshot shows the 'Logon & Security' configuration page in SAP. It features a navigation bar at the top with tabs for 'Administration', 'Technical Settings', 'Logon & Security', and 'Special Options'. The main content is organized into three sections:

- Logon Procedure**:
 - Logon with User**:
 - Do not use a user
 - Basic Authentication
 - User: wsuser
 - PW Status: saved
 - Password: [Redacted]
 - Logon with Ticket**:
 - Do Not Send Logon Ticket
 - Send ticket without reference to target system
 - Send assertion ticket for dedicated target system
 - System ID: [Redacted]
 - Client: [Redacted]
- Security Options**:
 - Status of Secure Protocol**:
 - SSL: Inactive, Active
 - SSL Certificate: DFAULT SSL Client (Standard) Cert. List
 - Authorization for Destination: [Redacted]

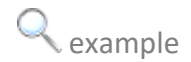
HTTP Connection - Special Options

requirement Switch to the Special Options tab.

necessary settings Enter the following settings:

| Parameter | Value |
|--|--|
| Timeout | <ul style="list-style-type: none"> ICM Default Timeout: Activate Maximum response time for the connection when sending an HTTP request. |
| HTTP Setting Status of HTTP Version | <ul style="list-style-type: none"> HTTP 1.1: Activate Protocol version of HTTP requests |
| HTTP Setting Compression Status | <ul style="list-style-type: none"> Compression <ul style="list-style-type: none"> Inactive: Activate Status of Compressed Response <ul style="list-style-type: none"> No: Activate |
| HTTP Cookies | <ul style="list-style-type: none"> Yes (All): Activate Handling of received cookies: |

HTTP Connection - Special Options, Continuation



| | | | |
|----------------|--------------------|------------------|------------------------|
| Administration | Technical Settings | Logon & Security | Special Options |
|----------------|--------------------|------------------|------------------------|

Timeout

ICM Default Timeout
 No Timeout
 Specify Timeout Timeout in Seconds (1 to 9999999)

HTTP Setting

Status of HTTP Version

HTTP Version HTTP 1.0 HTTP 1.1

Compression Status

Compression Inactive
 Active (depends on MIME type)
 Active (full document)

Status of Compressed Response

Compressed Response Yes No

HTTP Cookies


Type of Cookies Acceptance

Accept Cookies No
 Yes (All)
 Input Prompt
 Trigger Event

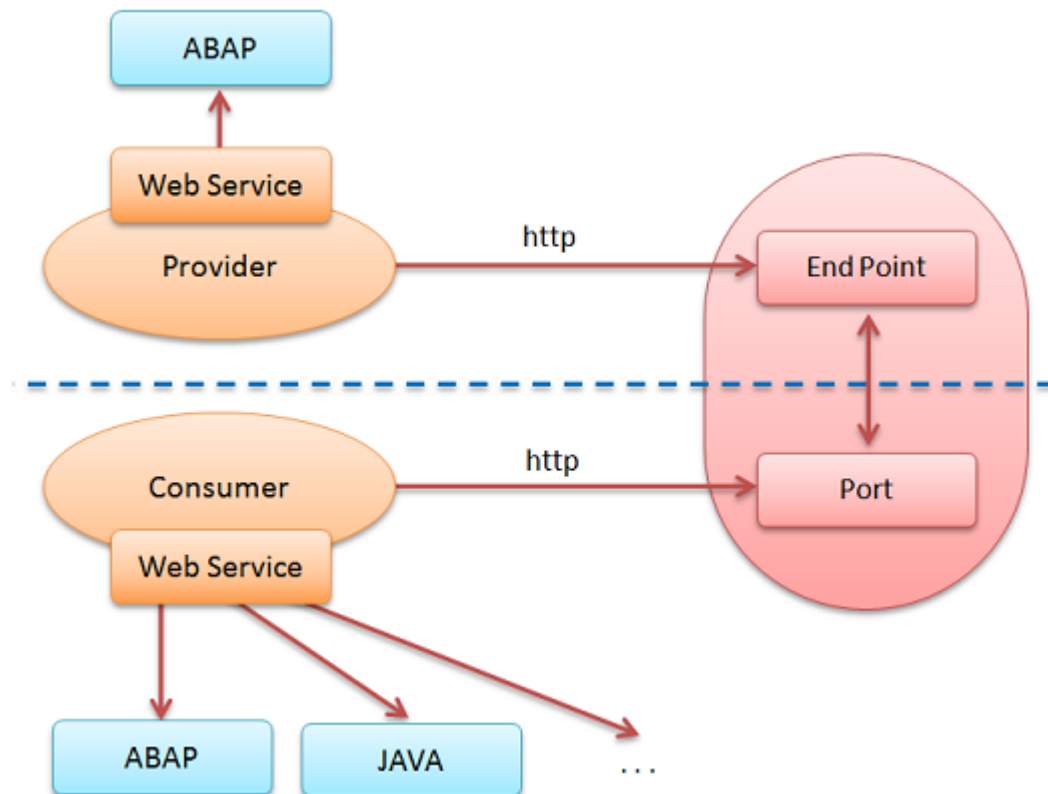
5 Web Service Integration (SOAP) - SAP as Provider

introduction This chapter describes the establishing of a Web service integration (SOAP), if SAP serves as provider.

description Functions that are implemented in different SAP software components may be combined via Web service to one process. This chapter describes the steps required to use the integration via Web service for SEAL Systems products.

 **related topics** → *Web Service Integration (SOAP) - SAP as Consumer*, Page 94

overview SAP as provider:



in this chapter This chapter deals with the following topics:

- *Required Authorizations*, Page 85
- *Configuration on the Provider System (SAP)*, Page 86
- *Troubleshooting - Analysis of Web Service Requests*, Page 91

5.1 Required Authorizations

The required authorizations have to be assigned to the users via the following roles (transaction: `su01`; maintenance of the authorizations via the profile generator with the `pfcg` transaction):

- User, who administrates the Web service via the SOA manager:
`SAP_BC_WEBSERVICE_ADMIN_TEC`
- SAP as provider - user, who is used as ABAP service user for the endpoint on the provider system:
`SAP_BC_WEBSERVICE_SERVICE_USER`
- SAP as provider - user, who want to debug the Web service requests:
`SAP_BC_WEBSERVICE_DEBUGGER`
- SAP as consumer - user, who starts the Web service:
`SAP_BC_WEBSERVICE_CONSUMER`

5.2 Configuration on the Provider System (SAP)

in this chapter

This chapter deals with the following topics:


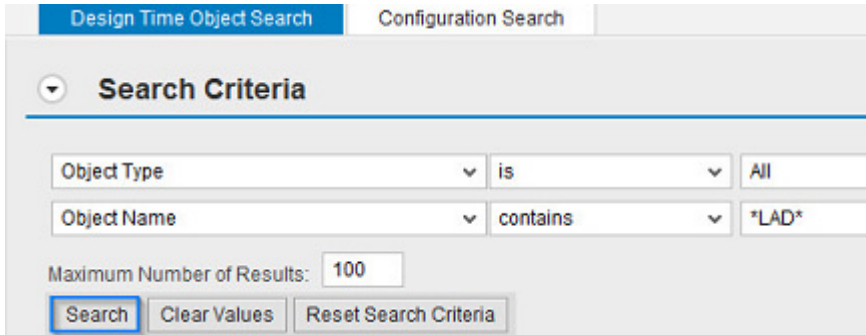
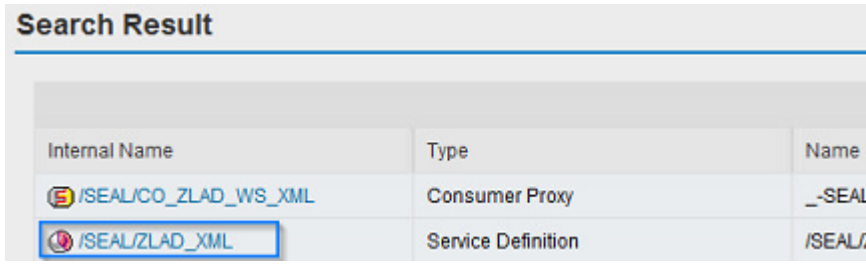
→ *Select the Service*, Page 87

→ *Create the Binding on the Provider System*, Page 88

→ *Determine URL for WSDL Access*, Page 90

Select the Service

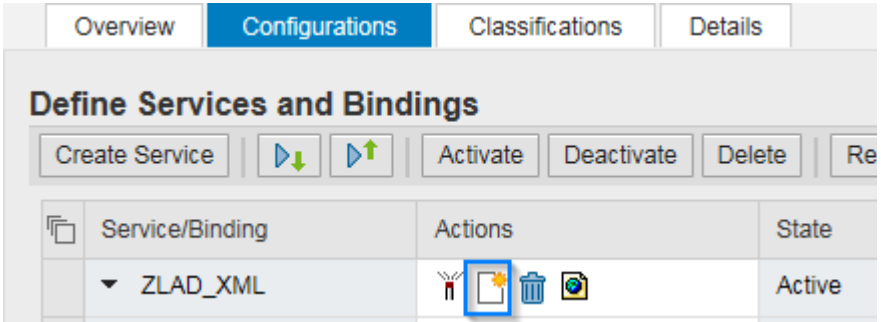
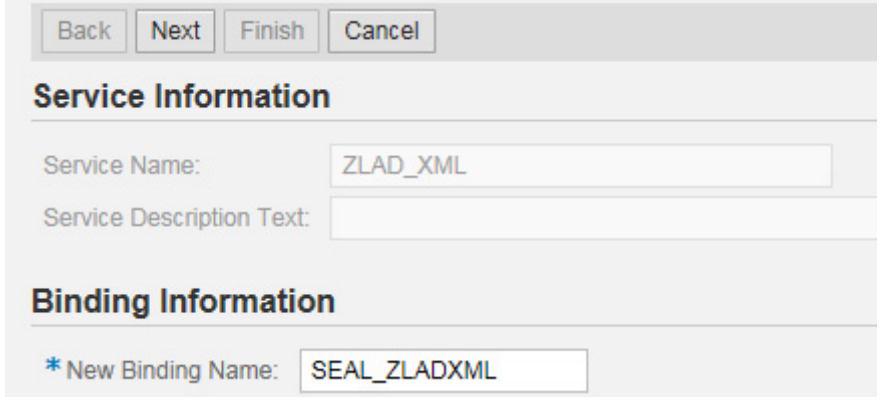
This is how you select the service which is provided by SEAL Systems and for which you want to establish the integration: [instructions](#)

| Step | Action |
|------|--|
| 1 | Start the SOA manager via the soamanager transaction. |
| 2 | Switch to the Service Administration tab. |
| 3 | Click: Web Service Configuration  |
| 4 | Search for the desired service: Click Search.  |
| 5 | Select the required service of type Service Definition: Click the internal name of the service.  |

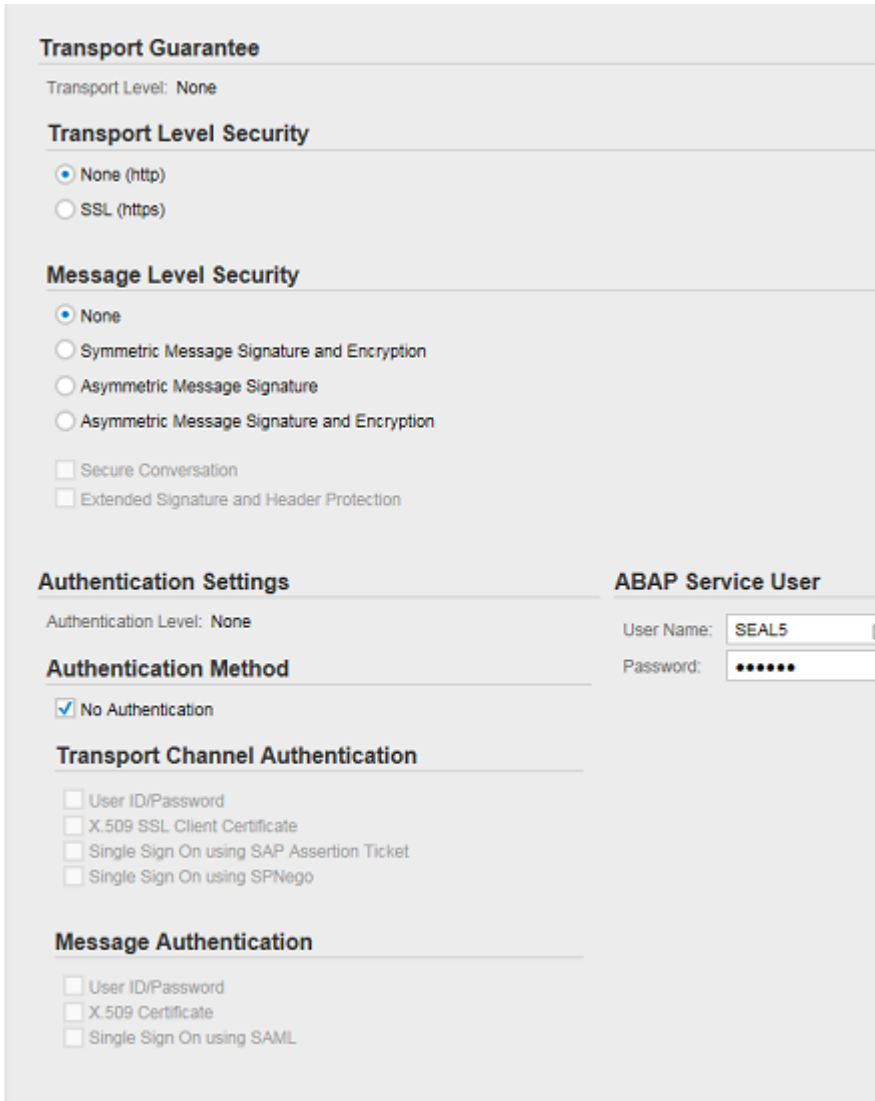
Create the Binding on the Provider System

description A binding has to be created on the provider system in order to provide the service.

instructions This is how you create a binding on the provider system:

| Step | Action |
|------|--|
| 1 | → <i>Select the Service, Page 87</i> |
| 2 | Switch to the Configurations tab. |
| 3 | Click Create Binding.  |
| 4 | Enter the name of the binding and click Next: <ul style="list-style-type: none"> • Service Name: SEAL_ZLAD_XML (example) • Description: Binding for SEAL_ZLAD_XML (example) • New Binding Name: SEAL_ZLADXML (example)  |

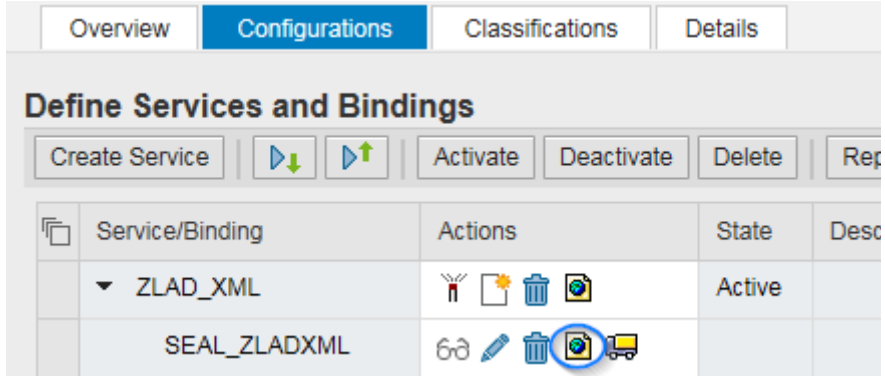
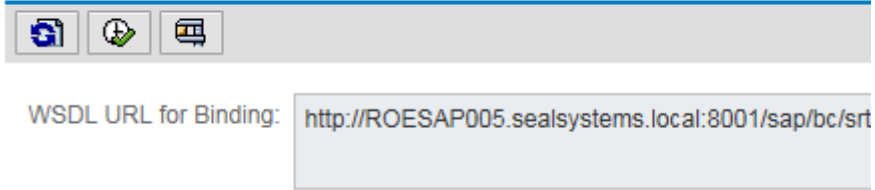
Create the Binding on the Provider System, Continuation

| Step | Action |
|------|--|
| 5 | <p>Specify the required settings and click Finish:</p> <ul style="list-style-type: none"> • Communication Security: None (HTTP) activate • Authentication Method: No Authentication activate • ABAP Service User: Enter user name and password  <p>Transport Guarantee Transport Level: None</p> <p>Transport Level Security</p> <p><input checked="" type="radio"/> None (http) <input type="radio"/> SSL (https)</p> <p>Message Level Security</p> <p><input checked="" type="radio"/> None <input type="radio"/> Symmetric Message Signature and Encryption <input type="radio"/> Asymmetric Message Signature <input type="radio"/> Asymmetric Message Signature and Encryption</p> <p><input type="checkbox"/> Secure Conversation <input type="checkbox"/> Extended Signature and Header Protection</p> <p>Authentication Settings ABAP Service User</p> <p>Authentication Level: None User Name: SEAL5 Password: ●●●●●●</p> <p>Authentication Method</p> <p><input checked="" type="checkbox"/> No Authentication</p> <p>Transport Channel Authentication</p> <p><input type="checkbox"/> User ID/Password <input type="checkbox"/> X.509 SSL Client Certificate <input type="checkbox"/> Single Sign On using SAP Assertion Ticket <input type="checkbox"/> Single Sign On using SPNego</p> <p>Message Authentication</p> <p><input type="checkbox"/> User ID/Password <input type="checkbox"/> X.509 Certificate <input type="checkbox"/> Single Sign On using SAML</p> |

Determine URL for WSDL Access

instructions

This is how you determine the URL for the WSDL access on the provider system, which you need for the creation of the logical port on the consumer system:

| Step | Action |
|------|--|
| 1 | → <i>Select the Service, Page 87</i> |
| 2 | Switch to the Configurations tab. |
| 3 | Click Open WSDL Generation for Binding.  |
| 4 | Copy the URL.  |

5.3 Troubleshooting - Analysis of Web Service Requests

This chapter deals with the following topics:

in this chapter

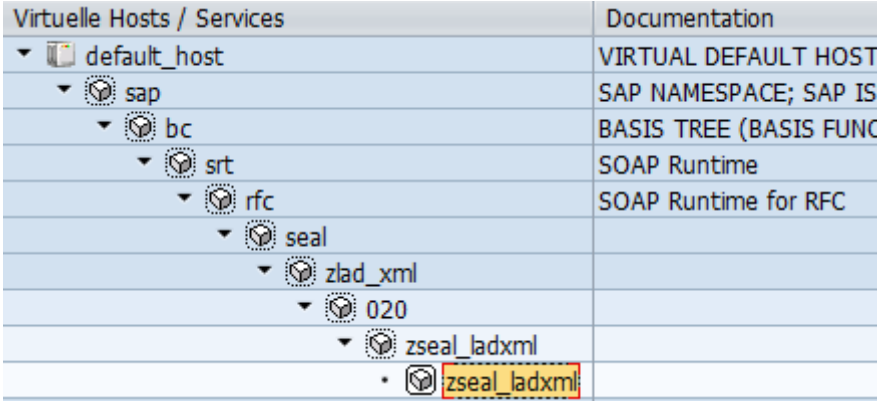
→ *Record and Display Web Service Requests*, Page 92

→ *Debug Web Service Requests*, Page 93

Record and Display Web Service Requests

instructions

This is how you use the recorder in order to record and display incoming and outgoing Web service requests on the provider system:

| Step | Action |
|------|---|
| 1 | Start the sicf transaction. |
| 2 | <p>Open the service tree for the SERVICE hierarchy type:</p> <p><i>sap/bc/srt/rfc/seal/Web service Function/Client/Web service Name/Binding</i></p> <p>Example:</p> <p><i>/sap/bc/srt/rfc/seal/zlad_xml/020/zseal_ladxml/zseal_ladxml</i></p>  |
| 3 | <p>Select the menu:</p> <ul style="list-style-type: none"> • Edit→Recorder→Activate Recording for incoming requests on the provider system • Client→Recorder→Activate Recording for outgoing requests on the consumer system |
| 4 | Enter the desired settings and click Activate. |
| 5 | Start the Web service. |
| 6 | <p>Display the recording with:</p> <ul style="list-style-type: none"> • Edit→Recorder→Display Recording for incoming requests on the provider system • Client→Recorder→Display Recording for outgoing requests on the consumer system |

trace messages

Activate additional trace messages for the troubleshooting on the provider system via Edit→Trace→Activate Trace.

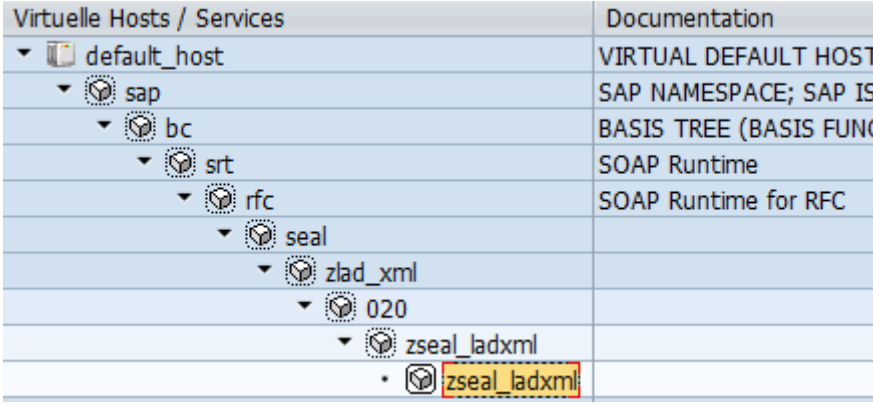
Debug Web Service Requests

→ *Required Authorizations*, Page 85

requirement

This is how you debug Web service requests on the provider system:


instructions

| Step | Action | | | | | | | | | | | | | | | | | | | | | | |
|----------------------------|---|----------------------------|---------------|--------------|----------------------|-----|-----------------------|----|------------------------|-----|--------------|-----|----------------------|------|--|----------|--|-----|--|--------------|--|--------------|--|
| 1 | Start the sicf transaction. | | | | | | | | | | | | | | | | | | | | | | |
| 2 | <p>Open the service tree for the SERVICE hierarchy type: <i>sap/bc/srt/rfc/sap/Web service Function/Client/Web service Name/Binding</i></p> <p>🔍 Example: <i>/sap/bc/srt/rfc/seal/zlad_xml/020/zseal_ladxml/zseal_ladxml</i></p>  <table border="1" data-bbox="327 824 1203 1227"> <thead> <tr> <th>Virtuelle Hosts / Services</th> <th>Documentation</th> </tr> </thead> <tbody> <tr> <td>default_host</td> <td>VIRTUAL DEFAULT HOST</td> </tr> <tr> <td> sap</td> <td>SAP NAMESPACE; SAP IS</td> </tr> <tr> <td> bc</td> <td>BASIS TREE (BASIS FUNC</td> </tr> <tr> <td> srt</td> <td>SOAP Runtime</td> </tr> <tr> <td> rfc</td> <td>SOAP Runtime for RFC</td> </tr> <tr> <td> seal</td> <td></td> </tr> <tr> <td> zlad_xml</td> <td></td> </tr> <tr> <td> 020</td> <td></td> </tr> <tr> <td> zseal_ladxml</td> <td></td> </tr> <tr> <td> zseal_ladxml</td> <td></td> </tr> </tbody> </table> | Virtuelle Hosts / Services | Documentation | default_host | VIRTUAL DEFAULT HOST | sap | SAP NAMESPACE; SAP IS | bc | BASIS TREE (BASIS FUNC | srt | SOAP Runtime | rfc | SOAP Runtime for RFC | seal | | zlad_xml | | 020 | | zseal_ladxml | | zseal_ladxml | |
| Virtuelle Hosts / Services | Documentation | | | | | | | | | | | | | | | | | | | | | | |
| default_host | VIRTUAL DEFAULT HOST | | | | | | | | | | | | | | | | | | | | | | |
| sap | SAP NAMESPACE; SAP IS | | | | | | | | | | | | | | | | | | | | | | |
| bc | BASIS TREE (BASIS FUNC | | | | | | | | | | | | | | | | | | | | | | |
| srt | SOAP Runtime | | | | | | | | | | | | | | | | | | | | | | |
| rfc | SOAP Runtime for RFC | | | | | | | | | | | | | | | | | | | | | | |
| seal | | | | | | | | | | | | | | | | | | | | | | | |
| zlad_xml | | | | | | | | | | | | | | | | | | | | | | | |
| 020 | | | | | | | | | | | | | | | | | | | | | | | |
| zseal_ladxml | | | | | | | | | | | | | | | | | | | | | | | |
| zseal_ladxml | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | <p>Select the menu: Edit→Debugging→Activate Debugging</p> | | | | | | | | | | | | | | | | | | | | | | |
| 4 | Start the Web service. | | | | | | | | | | | | | | | | | | | | | | |
| 5 | Debug the Web service in the debugger. | | | | | | | | | | | | | | | | | | | | | | |

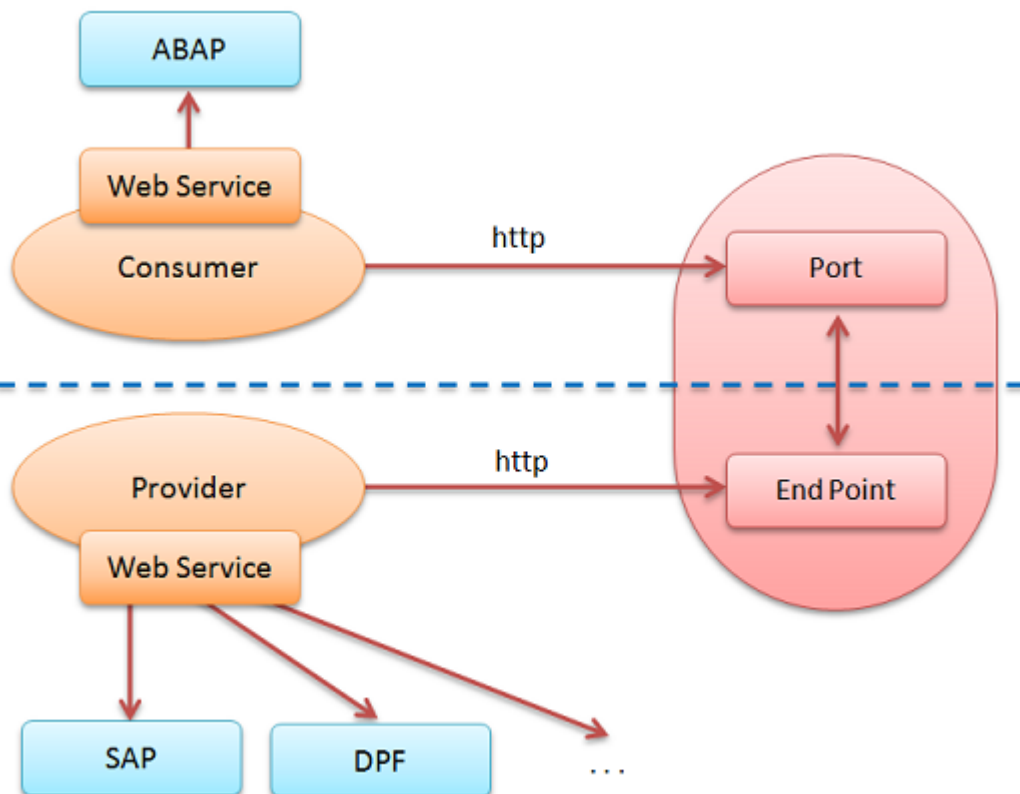
6 Web Service Integration (SOAP) - SAP as Consumer

introduction This chapter describes the establishing of a Web service integration (SOAP), if SAP serves as consumer.

description External functionality can be provided via Web service in order to be used by SAP as consumer.

 **related topics** → *Web Service Integration (SOAP) - SAP as Provider*, Page 84

overview SAP as consumer:



in this chapter This chapter deals with the following topics:

- *Required Authorizations*, Page 95
- *Configuration on the Consumer System (SAP)*, Page 96
- *Advisable Behavior in the Case of Error*, Page 102
- *Troubleshooting*, Page 104

6.1 Required Authorizations

The required authorizations have to be assigned to the users via the following roles (transaction: `su01`; maintenance of the authorizations via the profile generator with the `pfcg` transaction): requirement - roles

- User, who administrates the Web service via the SOA manager:
`SAP_BC_WEBSERVICE_ADMIN_TEC`
- SAP as provider - user, who is used as ABAP service user for the endpoint on the provider system:
`SAP_BC_WEBSERVICE_SERVICE_USER`
- SAP as provider - user, who want to debug the Web service requests:
`SAP_BC_WEBSERVICE_DEBUGGER`
- SAP as consumer - user, who starts the Web service:
`SAP_BC_WEBSERVICE_CONSUMER`

6.2 Configuration on the Consumer System (SAP)


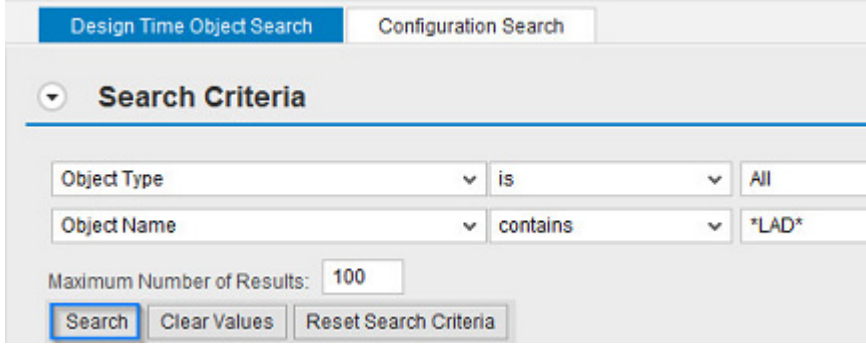
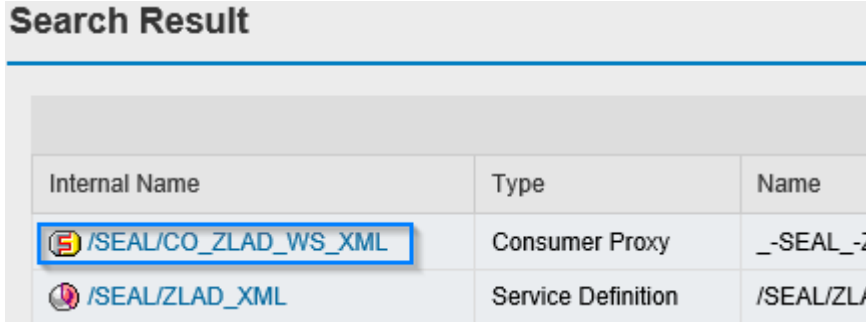
requirement The Web service, which you want to use from SAP, is started externally.

in this chapter This chapter deals with the following topics:

- *Select the ABAP Proxy*, Page 97
- *Create a Logical Port*, Page 98
- *Suppress the Message ID Transfer*, Page 100
- *Transfer of Large Amounts of Data*, Page 101

Select the ABAP Proxy

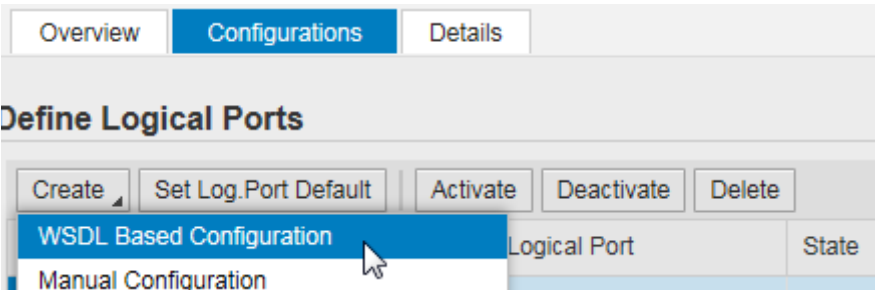
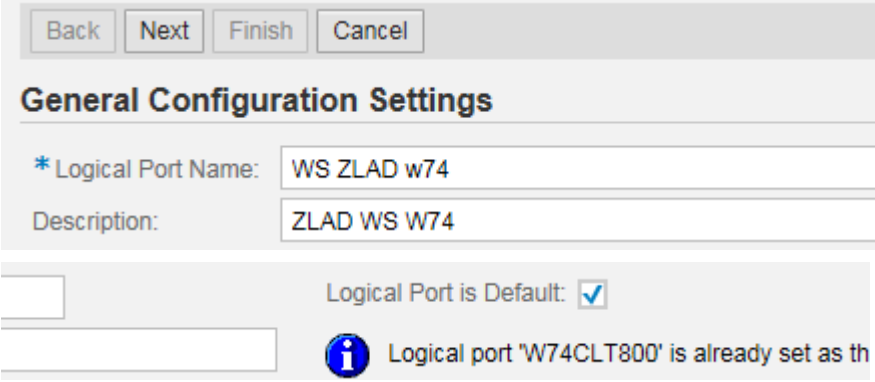
This is how you select the ABAP proxy for which you want to establish the integration: [instructions](#)

| Step | Action |
|------|---|
| 1 | Start the SOA manager via the soamanager transaction. |
| 2 | Switch to the Service Administration tab. |
| 3 | Click: Web Service Configuration  |
| 4 | Search for the desired service: Click Search.  |
| 5 | Select the desired consumer proxy from the Consumer Proxy type: Click the internal name of the consumer proxy. Search Result  |

Create a Logical Port

description A logical port has to be created for the communication between the service consumer and the external Web service.

instructions This is how you create a logical port:

| Step | Action |
|------|--|
| 1 | → Select the ABAP Proxy, Page 97 |
| 2 | Switch to the Configurations tab. |
| 3 | Click Create - WSDL based Configuration.  |
| 4 | Enter the data for the logical pro and click Next: <ul style="list-style-type: none"> • Logical Port Name: WS_DPF4C_OK (example) • Logical Port is Default: activate • Description: Logical port for WS_DPF4C_OK (example)  |

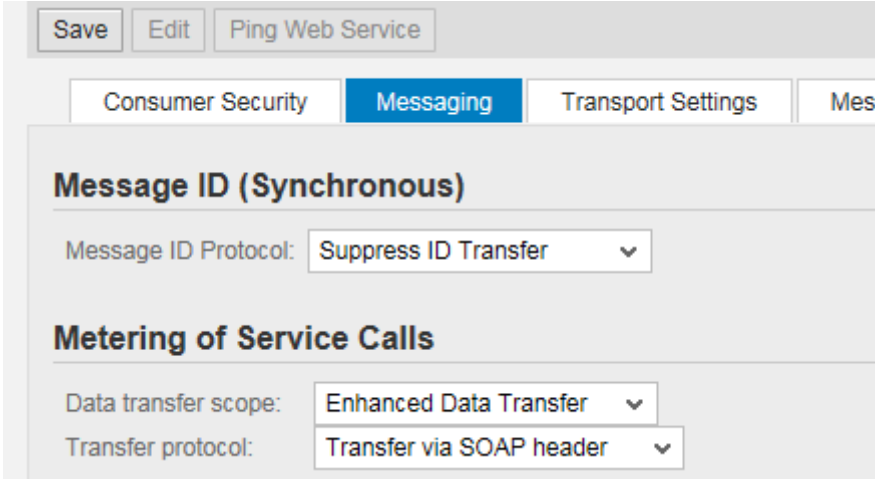
Create a Logical Port, Continuation

| Step | Action |
|------|---|
| 5 | <p>Enter the WSDL access settings for the logical pro and click Finish:</p> <ul style="list-style-type: none">• WSDL Base: Via HTTP Access activate• URL for WSDL Access: http://server:9125/dpf4c-service-v1.3/ convert?wsdl(example) <p>WSDL Access Settings</p> <p>WSDL Base: <input checked="" type="radio"/> Via HTTP Access <input type="radio"/> Via File <input type="radio"/> WSDL from Upload</p> <p>WSDL Location</p> <p>URL for WSDL Access: <input type="text" value="http://ROESAP005.sealsystems.local:8001/sa"/></p> |

Suppress the Message ID Transfer

description The ID transfer of the message ID protocol has to be suppressed.

instructions This is how you suppress the message ID transfer on the consumer system:

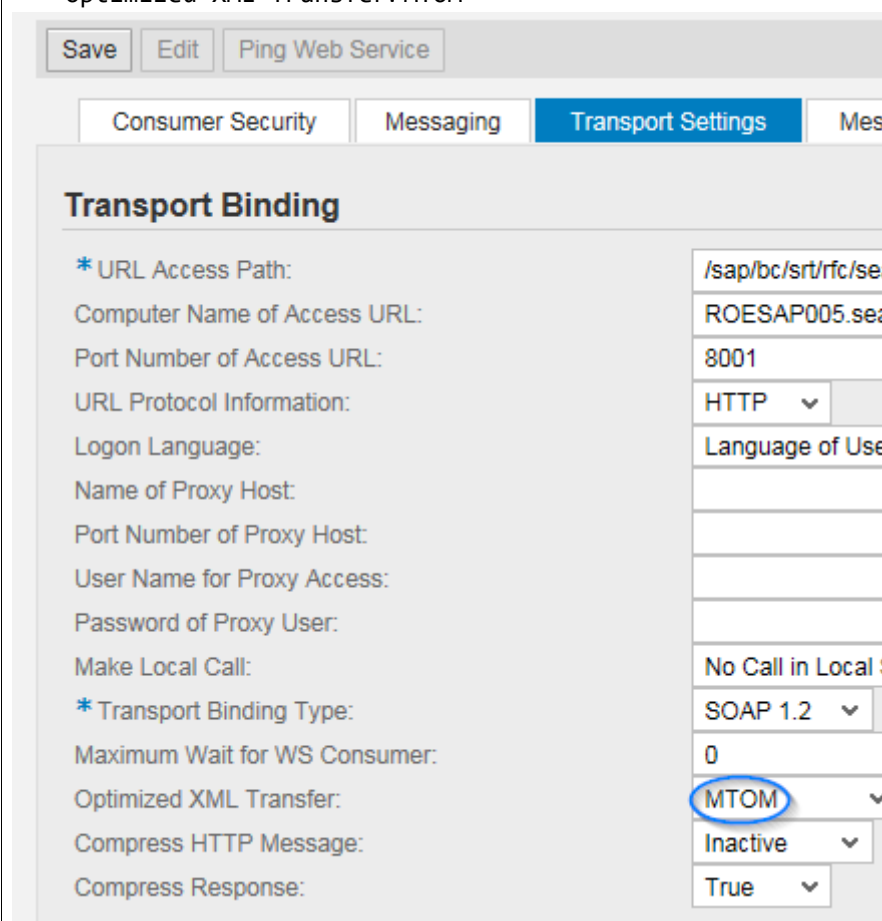
| Step | Action |
|------|--|
| 1 | → <i>Select the ABAP Proxy, Page 97</i> |
| 2 | Switch to the Configurations tab. |
| 3 | Select the desired logical port and click Edit. |
| 4 | Switch to the Messaging tab: |
| 5 | <p>Enter:</p> <ul style="list-style-type: none"> Message ID Protocol: Suppress ID Transfer  <p>Caution - default</p> <p>Up to SAP NetWeaver Application Server 7.3, Suppress ID Transfer is the default. As of SAP NetWeaver Application Server 7.4, this value has to be specified explicitly:</p> |

Transfer of Large Amounts of Data

If you transfer large amounts of data in the Web service environment, you can use the SOAP Message Transmission Optimization Mechanism (MTOM). description

MTOM is supported as of SAP release 7.20 or newer without restrictions, see SAP note 1582187. requirement








This is how you activate the optimized XML transfer for large amounts of data on the consumer system: instructions

| Step | Action |
|------|--|
| 1 | → <i>Select the ABAP Proxy, Page 97</i> |
| 2 | Switch to the Configurations tab. |
| 3 | Select the desired logical port and click Edit. |
| 4 | Switch to the Transport Settings tab. |
| 5 | Enter: <ul style="list-style-type: none"> Optimized XML Transfer: MTOM  <p>The screenshot shows the 'Transport Binding' configuration window. The 'Transport Settings' tab is active. The 'Optimized XML Transfer' dropdown menu is open, and 'MTOM' is selected and circled in blue. Other visible settings include 'URL Access Path' (/sap/bc/srt/rfc/se...), 'Computer Name of Access URL' (ROESAP005.sea...), 'Port Number of Access URL' (8001), 'URL Protocol Information' (HTTP), 'Logon Language' (Language of Use), 'Name of Proxy Host', 'Port Number of Proxy Host', 'User Name for Proxy Access', 'Password of Proxy User', 'Make Local Call' (No Call in Local...), '* Transport Binding Type' (SOAP 1.2), 'Maximum Wait for WS Consumer' (0), 'Compress HTTP Message' (Inactive), and 'Compress Response' (True).</p> |

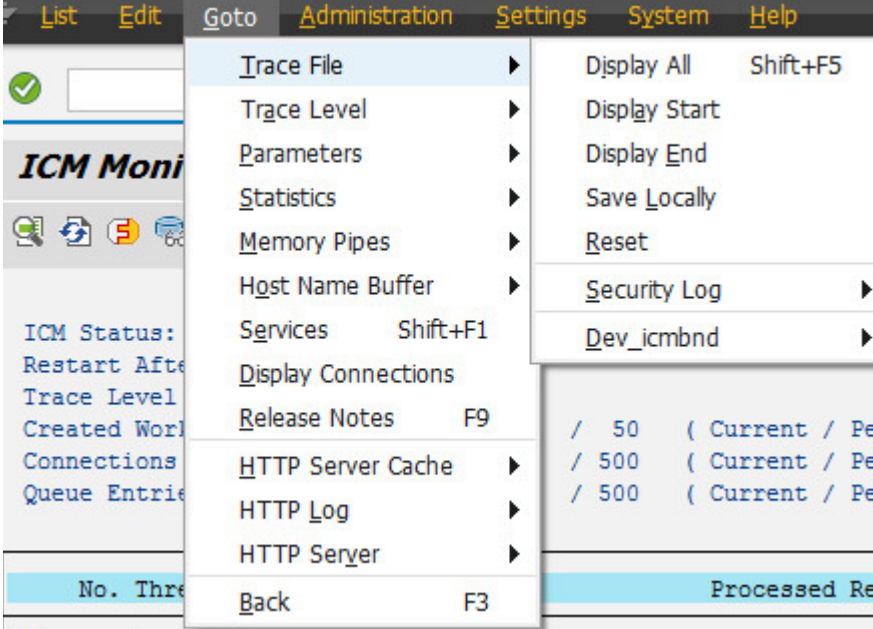


6.3 Advisable Behavior in the Case of Error

instructions

This is how you check the possible reasons in the case of error step by step:

| Step | Action |
|------|--|
| 1 | <p>Check if the URL is accessible:</p> <ul style="list-style-type: none"> Start the rswf_test_http program (transaction: sa38). Enter the URL to be tested and click . <p> Example:</p> <div data-bbox="518 640 1394 831" style="border: 1px solid #ccc; padding: 5px;"> <p>Test HTTP Connection</p> <p></p> <p>URL <input type="text" value="http://ok-win12-dom:9125/cgi-bin/"/></p> </div> <p>Result:</p> <p>A green status display in the first line indicates a successful connection, a red status display indicates an error.</p> <p> Example - HTTP connection successful:</p> <div data-bbox="518 1075 1347 1442" style="border: 1px solid #ccc; padding: 5px;"> <p>Test HTTP Connection</p> <p>Test HTTP Connection</p> <p></p> <pre>~response_line HTTP/1.1 200 OK ~server_protocol HTTP/1.1 ~status_code 200 ~status_reason OK</pre> </div> <p> Example - HTTP connection is faulty:</p> <div data-bbox="518 1547 1394 1915" style="border: 1px solid #ccc; padding: 5px;"> <p>Test HTTP Connection</p> <p>Test HTTP Connection</p> <p></p> <pre>~response_line HTTP/1.1 404 Not Found ~server_protocol HTTP/1.1 ~status_code 404 ~status_reason Not Found</pre> </div> |

Advisable Behavior in the Case of Error, Continuation

| Step | Action |
|------|---|
| 2 | <p>If an error occurs, start the ICM monitor to determine the exact cause of the error and forward this data to your Technical Project Manager at SEAL Systems if necessary:</p> <p>Transaction: smicm</p> <ul style="list-style-type: none"> • Display trace file: Goto→Trace File→Display All • Save trace file: Goto→Trace File→Save Locally  <p> Hint - reset trace file: For a better overview, you can delete the trace file with Goto→Trace File→Reset and execute the erroneous call again.</p> <p> Hint - set trace level: In general, the default trace level is sufficient. You can change it with Goto→Trace Level→Set and execute the erroneous call again.</p> |

6.4 Troubleshooting

typical problems
and their solu-
tions

The following table illustrates typical problems (P) and their approaches (A):

| | |
|----|--|
| P: | <p>The Web service returns an error message of the following type:</p> <pre>SOAP:1.023 SRT: Processing error in Internet Communication Framework: ("ICF Error when receiving the response: IC-M_HTTP_-CONNECTION_FAILED"</pre> <p>Possible cause is that the Web service is not started.</p> |
| A: | <p>Start the Web service.</p> |

| | |
|----|--|
| P: | <p>The Web service returns an error message of the following type:</p> <pre>Error while calling DPF Webservice SoapFaultCode:3 MustUnderstand headers:[{http://schemas.xmlsoap.org/ws/2004/08/addressing}Action, {http://schemas.xmlsoap.org/ws/2004/08/addressing}To] are not understood</pre> <p>Possible cause is that the ID transfer of the message ID protocol is not suppressed.</p> |
| A: | <p>Suppress the message ID transfer: → <i>Suppress the Message ID Transfer, Page 100</i></p> |

| | |
|----|---|
| P: | <p>The Web service returns an error message of the following type:</p> <pre>SOAP:1.001 CX_SXML_PARSE_ERROR: An exception was raised. Error when parsing an XML stream: '<EOF> reached</pre> <p>Possible cause is that the optimization of the transfer of large amounts of data is not activated.</p> |
| A: | <p>Optimize the transfer of large amounts of data: → <i>Transfer of Large Amounts of Data, Page 101</i></p> |

| | |
|----|--|
| P: | <p>The Web service returns an error message of the following type:</p> <pre>SOAP:1.007 SRT: Unsupported xstream found: ("HTTPCode 502: Bad Gateway")</pre> <p>Possible cause is that the timeout is too small.</p> |
| A: | <p>Increase the timeout in <code>server\web\apache\conf\workers.properties</code>: <code>worker.seal-worker.socket_timeout</code></p> |

| | |
|----|---|
| P: | <p>The Web service returns an error message of the following type:</p> <pre>"HTTPCode 502: Bad Gateway"</pre> <p>Possible cause is that the timeout is too small.</p> |
|----|---|

Troubleshooting, Continuation

A: Increase the timeout for the HTTP protocol via the `smicm` transaction with `Goto→Services` and `Service→Change`:

Keep Alive (in Sec.)

In addition to that, check the following DPF timeouts:

- `apache\conf\httpd.conf: Timeout 1200 (20 min)`
- `apache\conf\workers.properties: worker.seal-workers.socket_timeout 1200 (20 min)`
- `tomcat\conf\server.xml: connectionTimeout 600000(10 min, is generally not activated)`

P: The Web service returns an error message of the following type:

"`ICM_HTTP_TIMEOUT`"

Possible cause is that the timeout is too small.

A: Check the following values for the HTTP log via the `smicm` transaction with `Goto→Services` and `Service→Change`:

Keep Alive (in Sec.)

Maximum Processing Time (`ProcTimeout`)











7 OData Service Activation

| | |
|------------------------|--|
| introduction | This chapter describes how to activate OData services in SAP. |
| requirement release | The following requirements must be fulfilled in the context of the SAP system: <ul style="list-style-type: none">• SAP Business Suite as of EhP8 and S/4HANA on premise• SAPUI5 version 1.76.0 or newer• oData services with classic ABAP programming (SEGW) |
| in this chapter | This chapter deals with the following topics: <ul style="list-style-type: none">→ <i>Activate OData Service</i>, Page 107→ <i>Activate OData Service for Applications - Basis</i>, Page 109 |


Activate OData Service

This is how you check and activate an OData service:

instructions

| Step | Action | | | | | | | | | | | | | | |
|---|--|------------------|------------------------|------------------|--------------------------|-------------|---|-----------|----------|-------------------|---------------|-------------|--------|--------------------------|--------|
| 1 | Start the transaction: /n/iwfnd/maint_service | | | | | | | | | | | | | | |
| 2 | <p>Search for the OData service in the service catalog to ensure that the service is registered, and select it:</p> <ul style="list-style-type: none"> Technical Service Name: /seal/out_fio_srv (example) <p> Example</p> <div data-bbox="331 698 1211 846"> <p>Service Catalog</p> <table border="1"> <thead> <tr> <th>Type</th> <th>Technical Service Name</th> <th>Sr</th> <th>External Name</th> <th>Nsp.</th> <th>OA...</th> <th>Soft Stat</th> </tr> </thead> <tbody> <tr> <td>BEP</td> <td>/SEAL/OUT_FIO_SRV</td> <td>1</td> <td>OUT_FIO_SRV</td> <td>/SEAL/</td> <td><input type="checkbox"/></td> <td>Active</td> </tr> </tbody> </table> </div> <p> Hint - Soft State Status:</p> <p>In general, the soft state status does not have to be Active but can also be Not Supported.</p> <p>The Active status is only important for individual services; see the note in the product documentation.</p> | Type | Technical Service Name | Sr | External Name | Nsp. | OA... | Soft Stat | BEP | /SEAL/OUT_FIO_SRV | 1 | OUT_FIO_SRV | /SEAL/ | <input type="checkbox"/> | Active |
| Type | Technical Service Name | Sr | External Name | Nsp. | OA... | Soft Stat | | | | | | | | | |
| BEP | /SEAL/OUT_FIO_SRV | 1 | OUT_FIO_SRV | /SEAL/ | <input type="checkbox"/> | Active | | | | | | | | | |
| 3 | <p>Activate the OData service below the service catalog on the left with:</p> <ul style="list-style-type: none"> ICF Node: Activate <div data-bbox="331 1227 614 1451"> <p> ICF Node  Call</p> <ul style="list-style-type: none"> Activate Deactivate Delete Configure (SICF) </div> <p>Result: The oData service is activated</p> <div data-bbox="331 1527 1093 1720"> <p> ICF Node  Call Browser  SAP Gateway Client</p> <p>ICF Nodes</p> <table border="1"> <thead> <tr> <th>Status</th> <th>ICF Node</th> <th>Session Time-out</th> <th>Soft State</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td></td> <td>ODATA</td> <td>00:30:00</td> <td></td> <td>Standard Mode</td> </tr> </tbody> </table> </div> | Status | ICF Node | Session Time-out | Soft State | Description |  | ODATA | 00:30:00 | | Standard Mode | | | | |
| Status | ICF Node | Session Time-out | Soft State | Description | | | | | | | | | | | |
|  | ODATA | 00:30:00 | | Standard Mode | | | | | | | | | | | |








Activate OData Service, Continuation

| Step | Action | | | | | | | | | | | | |
|--|---|--|-------------------------------------|--|--|-------------------------|------|------------------|------------------|------------------------|--|-------|-------------------------------------|
| 4 | <p>Add a system alias below the service catalog on the right with Add System Alias:</p> <ul style="list-style-type: none"> • Service Document Identifier: /seal/out_fio_srv_001 (example) • SAP System Alias: LOCAL (example) • Default System: Activate <p> Example</p> <table border="1" data-bbox="523 734 1347 860"> <thead> <tr> <th colspan="4">Assign SAP System Aliases to OData Service</th> </tr> <tr> <th>Service Doc. Identifier</th> <th>U H.</th> <th>SAP System Alias</th> <th>Default System M</th> </tr> </thead> <tbody> <tr> <td>/SEAL/OUT_FIO_SRV_0001</td> <td></td> <td>LOCAL</td> <td><input checked="" type="checkbox"/></td> </tr> </tbody> </table> | Assign SAP System Aliases to OData Service | | | | Service Doc. Identifier | U H. | SAP System Alias | Default System M | /SEAL/OUT_FIO_SRV_0001 | | LOCAL | <input checked="" type="checkbox"/> |
| Assign SAP System Aliases to OData Service | | | | | | | | | | | | | |
| Service Doc. Identifier | U H. | SAP System Alias | Default System M | | | | | | | | | | |
| /SEAL/OUT_FIO_SRV_0001 | | LOCAL | <input checked="" type="checkbox"/> | | | | | | | | | | |

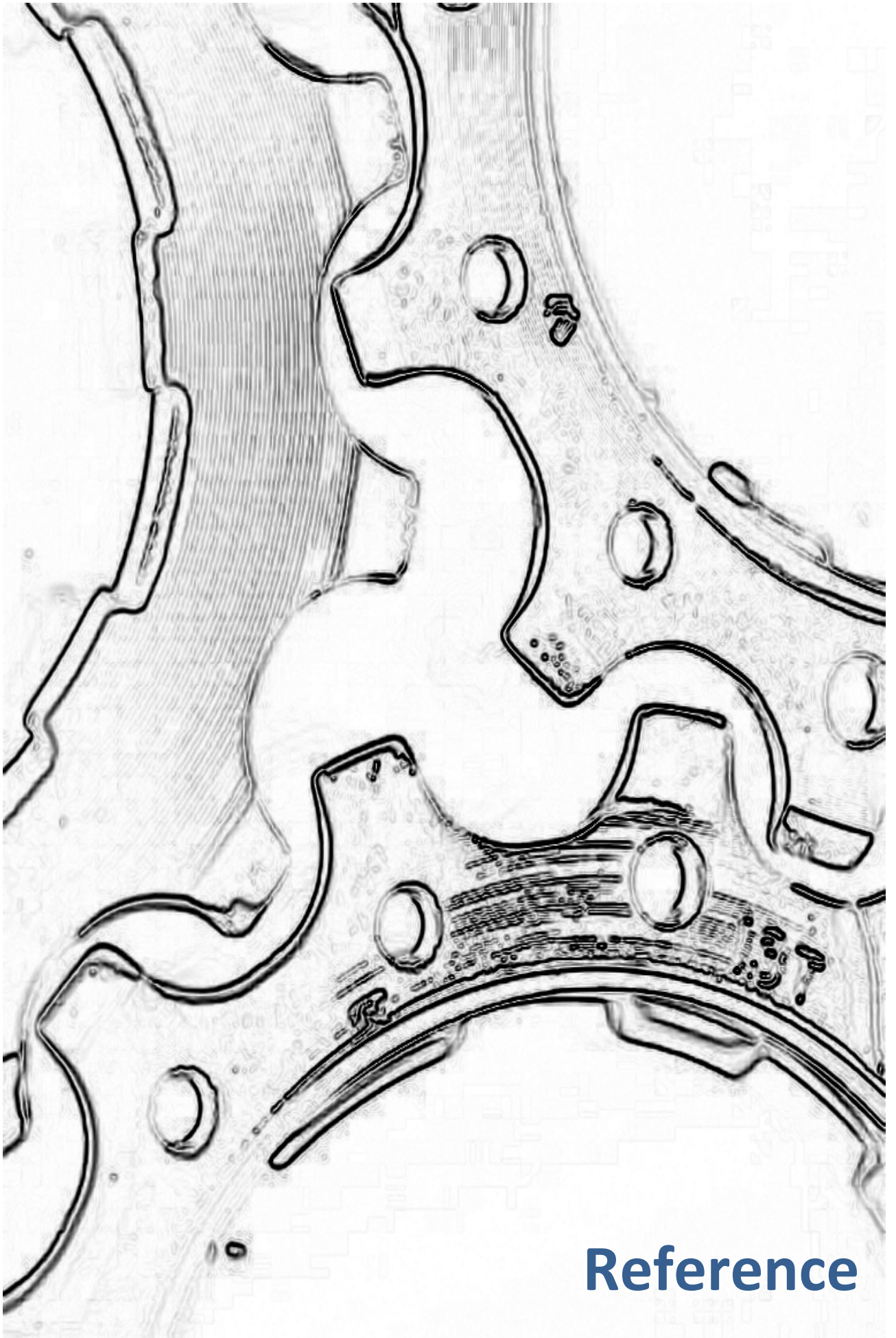
Activate OData Service for Applications - Basis

This is how you check and activate an OData service for an application:

instructions

| Step | Action | | | | | | | | |
|----------------|--|----------------|---------|--------------|--|--------------|--|--------------|-------------|
| 1 | Start the transaction: /nsicf | | | | | | | | |
| 2 | <p>Start the display via  with:</p> <p>Hierarchy Type: SERVICE</p> <p>Service Name: out_fia_ddc (example)</p> <p> Example</p> <div data-bbox="331 725 999 1088" style="border: 1px solid #ccc; padding: 5px;"> <p>Define Services</p> <p> </p> <p>Filter for Calling ICF Hierarchy</p> <table border="1" data-bbox="347 909 999 1088"> <tr> <td>Hierarchy Type</td> <td>SERVICE</td> </tr> <tr> <td>Virtual Host</td> <td></td> </tr> <tr> <td>Service Path</td> <td></td> </tr> <tr> <td>Service Name</td> <td>OUT_FIA_DDC</td> </tr> </table> </div> | Hierarchy Type | SERVICE | Virtual Host | | Service Path | | Service Name | OUT_FIA_DDC |
| Hierarchy Type | SERVICE | | | | | | | | |
| Virtual Host | | | | | | | | | |
| Service Path | | | | | | | | | |
| Service Name | OUT_FIA_DDC | | | | | | | | |
| 3 | <p>Open the tree view of the virtual host/service, check in the context menu whether the service is active and, if it is deactivated, activate it:</p> <ul style="list-style-type: none"> • default_host - sap - bc - bsp - seal - out_fia_ddc <p> Example</p> <div data-bbox="331 1397 999 1910" style="border: 1px solid #ccc; padding: 5px;"> <p>Virtual Hosts/Services</p> <ul style="list-style-type: none"> ▼ default_host <ul style="list-style-type: none"> ▼ sap <ul style="list-style-type: none"> ▼ bc <ul style="list-style-type: none"> ▼ bsp <ul style="list-style-type: none"> ▼ seal <ul style="list-style-type: none"> •  out_fia_ddc ▼ ui5_ui5 <ul style="list-style-type: none"> ▼ seal <ul style="list-style-type: none"> •  out_fia_ddc <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <ul style="list-style-type: none"> New Subelement Display Service Delete Service Rename Service Activate Service Deactivate Service </div> </div> | | | | | | | | |

Activate OData Service for Applications - Basis, Conti- nuation



Reference

8 Configuration Files - Reference

This chapter explains the configuration files which are evaluated to establish a connection between the OM server and the SAP system in case of communication via classic RFC destinations or communication via SAP NetWeaver RFC Library NWRFC.

introduction

This chapter deals with the following topics:

in this chapter

→ *cadrfc.ini* - Logon Information, Page 114

→ *saprfc.ini* - Connection Data, Page 126



→ *sapnwrfc.ini* - Connection Data, Page 157

→ *rfcserver.cfg*, Page 192

rfcserver.cfg serves as an example for the following configuration files:

- *alfilechecker.cfg*
- *alviewserver.cfg*
- *convserv.cfg*
- *convservdpf.cfg*
- *dvsviewserver.cfg*
- *filecheck.cfg*
- *jrfcserver.cfg*
- *rfcserver.cfg*

8.1 cadrfc.ini - Logon Information

| | |
|---|---|
| required if | The <code>cadrfc.ini</code> configuration file is only relevant for classic RFC destinations. |
| introduction | This chapter contains the reference information about the <code>cadrfc.ini</code> configuration file. |
| requirement | The <code>cadrfc.ini</code> file is evaluated for RFC client connections. Other RFC server connections ignore this file. |
| ASCII/Unicode | Within <code>cadrfc.ini</code> only ASCII characters are supported. Unicode characters are not supported. |
| location | The <code>cadrfc.ini</code> file is located in the following directory: <code>applications\server\sapserv\bin_...</code> |
|  hint - gXnet-plot | For gXnetplot, the file is located in: <code>\$GRALPLOTLIB/PDM (servermenu - c - cd1 - cd PDM)</code> |
| purpose | <p>The configuration file contains the necessary logon data which is evaluated by the BAPI and CAD interface.</p> <p>The interactive RFC clients use the logon data as default values for the initial logon dialog.</p> <p>The remaining RFC clients and RFC servers use the logon information for the initial logon when they start up. Later logons use the information saved in the job files (repro lists).</p> |
| structure | <p>You can specify general as well as system- and client-specific logon data:</p> <ul style="list-style-type: none"> • General logon data is specified in the configuration file without section name. • System- and client-specific logon data is specified in separate sections subsequent to the general logon data: [SAP\SystemName\Client] or [SAP\SystemName] Example: [SAP\W74\020] or [SAP\W74] |
|  example | <p>Extract of an example for <code>cadrfc.ini</code>:</p> <pre>*----- * SAP logon parameters *----- CadRfcUser SEALCPIC CadRfcPassword <SAPPWD> #CadRfcPasswordCoded 0xe3f0e9c6604b14b3</pre> |

cadrfc.ini - Logon Information, Continuation

```
#CadRfcClient 010
CadRfcLanguage EN
*-----
* Connection parameters
*-----
* Logical destination
CadRfcDestination W46
...
*-----
* Parameters specific for Dialog interface (SapConn)
*-----
...
* important for check-in/check-out
CadDialogNetAddress DEFAULT
*-----
* TRACE parameters 0 - set trace off | 1 - on
*-----
CadRfcTrace 0
CadTraceDir
*-----
* ABAP debug parameter 0 - set debug off | 1 - on
*-----
CadRfcAbapDebug 0
...
*-----
* system/client-specific logon data
*-----
[SAP\W74]
CadRfcUser SEALPE
CadRfcPasswordCoded 0xe3f0e9c6604b14b3
CadRfcClient 010
...
```

cadrfc.ini - Logon Information, Continuation

| | |
|-----------|--|
| customize | Only a couple of parameters of the configuration file must be adjusted to the current system environment. Only these parameters are described below. The remaining parameters have reasonable defaults and do not need to be adjusted. |
| restart | You must restart the DMS Rlist RFC client after you have changed parameters in <code>cadrfc.ini</code> . |

System-/Client-Specific Logon Data

The `rlistsap`, `sapcli`, `omscli` and `oms_server` programs must be linked with `sapini.c` version 1.14 or newer. requirement


To check the correct version, for example of `rlistsap`, execute the following steps:

| Step | Action |
|------|---|
| 1 | Enter: <code>what rlistsap grep sapini.c</code> |
| 2 | As result must be displayed: SAP-CAD \$Id: sapini.c,v 1.14 2005/10/12 ... The requirement is fulfilled if the version is 1.14 or newer. Otherwise contact your Technical Project Manager at SEAL Systems. |


With regard to DMS Rlist for the initial login to the SAP system during the start of DMS Rlist, only the logon data in the general (system and client independent) section of the file `cadrfc.ini` is used. The system- and client-specific logon information is only evaluated during the processing of repro list jobs at runtime. restriction

System- and client-specific logon data is specified in separate sections: structure

`[SAP\SystemName\Client]` or `[SAP\SystemName]`

 Example:

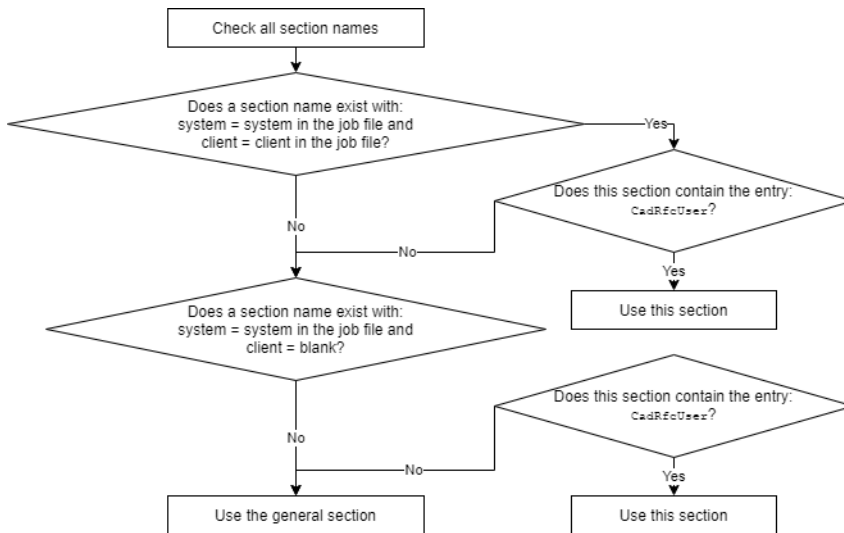
`[SAP\W74\020]` or `[SAP\W74]`

The sections containing the system- and client-specific logon data must be located at the end of the file after the general logon information.  Caution - at the end

The current system and the current client specified in the order file (repro list) are compared with the configuration entries in `cadrfc.ini` to determine the user to be used for logon. system/client comparison

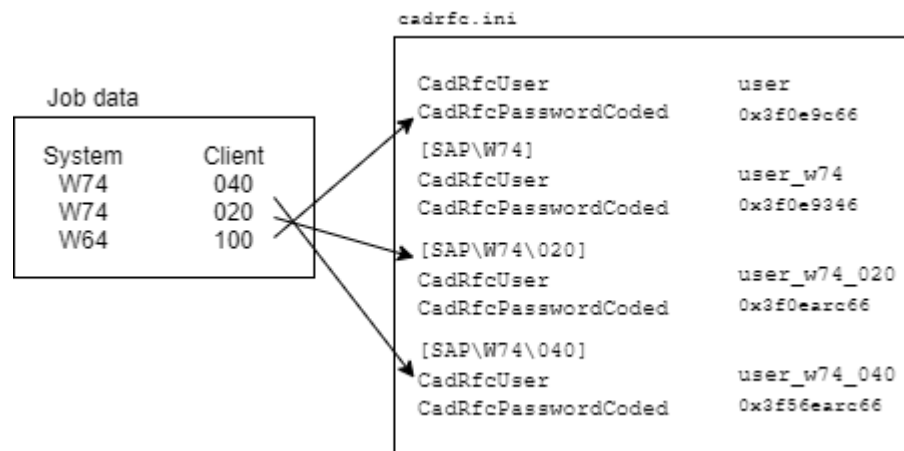
System-/Client-Specific Logon Data, Continuation

section determination The section of cadrfc.ini which is to be used for the current system/client specified in the order file is determined as follows:



example

The subsequent example demonstrates which user is used for logon dependent on the system/client in the job data.



CadRfcUser Parameter

The CadRfcUser parameter determines the user used by the RFC client or RFC server to logon on the SAP system. meaning

The following requirements must be fulfilled for a successful logon: requirement

- The specified user must be identically configured on all SAP systems.
- The user name must be entered in capitals.
- The interactive RFC clients require a dialog user.
- For security reasons, a system user is generally used for logon by the remaining RFC clients, for instance DMS loader and DMS Rlist, and the RFC servers.

Exception:


If USE_SAPGUI in `saprfc.ini` is specified as 1 or 2 a dialog user must be used!

CadRfcPassword Parameter

meaning The CadRfcPassword parameter specifies the uncoded password used by the RFC client and RFC server to logon on the SAP system.

alternative The password can be specified in a coded form with the CadRfcPasswordCoded parameter. For security reasons, the coded passwords are to be preferred.

requirement The CadRfcPassword parameter is ignored as soon as a coded password is specified with the parameter CadRfcPasswordCoded.

 **example** The item looks as follows:
CadRfcPassword xyz


CadRfcPasswordCoded Parameter

The CadRfcPasswordCoded parameter specifies the coded password used by the RFC client and RFC server to logon on the SAP system. This is the more secure variant compared to the previous CadRfcPasswordparameter.

meaning

This is how you create and save a coded password:

code the
pass-word

| Step | Action |
|------|--|
| 1 | Execute the program to encode the password: <code>sealencrypt.exe configpassword</code> |
| 2 | Enter the created coded password in the <code>cadrfc.ini</code> file.  Example: <code>CadRfcPasswordCoded e3f0e9c6604b14b3</code> |

CadRfcClient Parameter

meaning

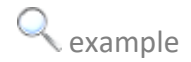
The `CadRfcClient` parameter determines the client used by the RFC client and RFC server to logon on the SAP system.

CadRfcLanguage Parameter

The CadRfcLanguage parameter specifies the language used by the RFC client and RFC server to logon on the SAP system. meaning

All two-character ISO-639-1 language codes installed on the SAP system can be specified as logon language. ISO-639-2B/T and ISO-639-3 are not supported.

The item looks as follows:



CadRfcLanguage EN

CadRfcDestination Parameter

meaning

The CadRfcDestination parameter specifies the SAP system on which the RFC client and RFC server log on.

example

The item looks as follows:

CadRfcDestination W74

CadDialogNetAddress Parameter


The `CadDialogNetAddress` parameter specifies the host name of the local machine. This is used for check-in and check-out files. meaning

If the `CadDialogNetAddress` parameter is not specified the value of the `HOSTNAME` (Windows) or `DISPLAY` (Unix) environment variable is used instead. environment variable

The following value is used as default: default

`CadDialogNetAddress DEFAULT`

8.2 saprfc.ini - Connection Data

| | |
|--|--|
| required if | The saprfc.ini configuration file is only relevant for classic RFC destinations. |
| introduction | This chapter contains the reference information about the saprfc.ini configuration file. |
| requirement: ASCII/Unicode | Within saprfc.ini only ASCII characters are supported. Unicode characters are not supported. |
| location | The saprfc.ini file is located in the following directory: client\dvs...\bin_... (RFC client connection) server\sapserv\conf (RFC server connection) |
|  hint - gXnetplot | For gXnetplot, the file is located in: \$GRALPLOTLIB/PDM (servermenu - c - cd1 - cd PDM) |
| contents | The configuration file contains parameter items with the system data for the individual SAP systems. This data is used to establish the RFC connections from the external server to the SAP systems. |
| structure | Dependent on the type of RFC destination - client or server - different parameter entries in saprfc.ini are required. All parameter entries concerning one type are grouped as one block without section name in the configuration file. |
| in this chapter | This chapter deals with the following topics: → <i>Determine System Data for saprfc.ini</i> , Page 128 → <i>Types of RFC Destinations and Module Classification</i> , Page 129 → <i>Parameter Overview</i> , Page 130 → <i>DEST Parameter</i> , Page 133 → <i>TYPE Parameter</i> , Page 134 → <i>ASHOST Parameter</i> , Page 135 → <i>SYSNR Parameter</i> , Page 136 → <i>MSHOST Parameter</i> , Page 137 → <i>MSSERV Parameter</i> , Page 138 → <i>R3NAME Parameter</i> , Page 139 → <i>GROUP Parameter</i> , Page 140 → <i>GWHOST Parameter</i> , Page 141 → <i>GWSERV Parameter</i> , Page 142 → <i>SAPROUTER Parameter</i> , Page 143 → <i>RFC_TRACE Parameter</i> , Page 144 |

saprfc.ini - Connection Data, Continuation


- *SEAL_TRACE* Parameter, Page 145
- *ABAP_DEBUG* Parameter, Page 146
- *USE_SAPGUI* Parameter, Page 147
- *UNICODE* Parameter, Page 148
- *CODEPAGE* Parameter, Page 149
- *SNC_MODE* Parameter, Page 150
- *SNC_MYNAME* Parameter, Page 151
- *SNC_PARTNERNAME* Parameter, Page 152
- *SNC_QOP* Parameter, Page 153
- *SNC_SSO* Parameter, Page 154
- *ASCS* Parameter, Page 155
- *X509CERT* Parameter, Page 156

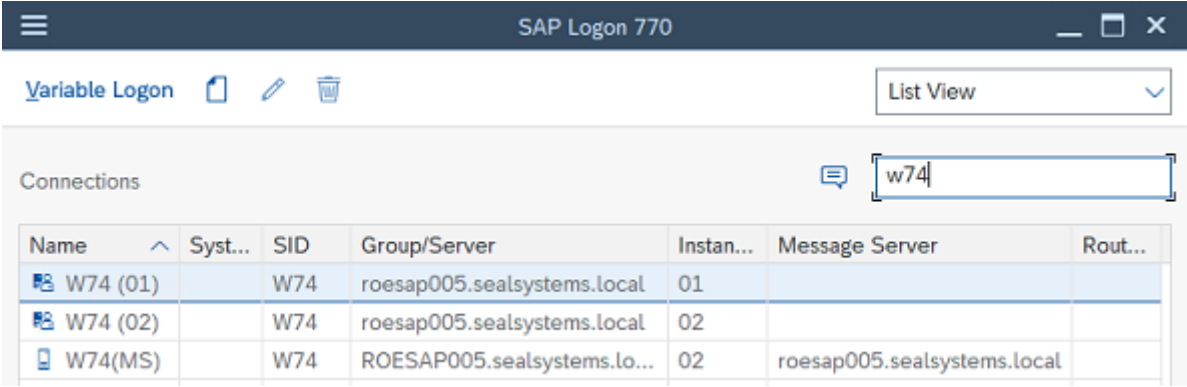
Determine System Data for `saprfc.ini`

SAP Basis You can get the current SAP system data, such as instance number, router string and so on, from your SAP Basis.

SAP logon If SAP GUI is installed, you can display the SAP system data also on SAP logon:

- SID
- Group/Server
- Instance Number
- Message Server
- Router

 example



The screenshot shows the SAP Logon 770 window with a search filter 'w74' applied. The table below represents the data shown in the screenshot.

| Name | Syst... | SID | Group/Server | Instan... | Message Server | Rout... |
|----------|---------|-----|-----------------------------|-----------|-----------------------------|---------|
| W74 (01) | | W74 | roesap005.sealsystems.local | 01 | | |
| W74 (02) | | W74 | roesap005.sealsystems.local | 02 | | |
| W74(MS) | | W74 | ROESAP005.sealsystems.lo... | 02 | roesap005.sealsystems.local | |

background knowledge Further system data, like the information whether it is a Unicode SAP system, can be determined for each system via the following program execution:

```
tools\bin_winnxx\sap_conn_checkerParameter
```

The data is configured in the `SAPGUI\landscape.xml` file.

Types of RFC Destinations and Module Classification

The following types of RFC destinations can be distinguished:

- RFC client via application server (type A)
- RFC client via message server (type B)
- RFC server via SAP gateway (type R)

type of RFC destinations

The modules from SEAL Systems can be classified in RFC client and RFC server modules as follows:

modules and types

| RFC Client | RFC Server |
|-----------------|--|
| DMS Rlist | DMS Loader |
| DMS Scan | Conversion Server |
| JSAPcli, SAPcli | RFC Server, JRFC Server, for instance for <ul style="list-style-type: none">• DMS Loader/ABAP• DMS View Server• PDF Longlife Suite - SAP Integration |

Parameter Overview

validity

Some parameters are evaluated for all connection types. In addition to these general parameters there are parameters which are only important for special connection types.

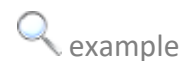
overview

The following table presents an overview of which parameters are evaluated for which connection type:

| Parameters | RFC Client Application Server | RFC Client Message Server | RFC Server Gateway |
|----------------------|----------------------------------|------------------------------|-----------------------|
| DEST | X | X | X |
| TYPE | A | B | R |
| ASHOST | X | - | - |
| SYSNR | X | - | - |
| MSHOST | - | X | - |
| MSSRV | - | X | - |
| GROUP | - | X | - |
| GWHOST | - | - | X |
| GWSERV | - | - | X |
| SAPROUTER | X | X | X |
| RFC_TRACE | X | X | X |
| SEAL_TRACE | - | - | X |
| ABAP_DEBUG | X | X | - |
| USE_SAPGUI | X | X | - |
| UNICODE | X | X | X |
| CODEPAGE | - | - | X |
| SNC_MODE | X | X | X |
| SNC_MYNAME | X | X | X |
| SNC_PARTNER- NAME | X | X | - |
| SNC_QOP | X | X | X |
| SNC_SSO | X | X | X |
| ASCS | X | X | - |
| X509CERT | X | X | X |

Parameter Overview, Continuation

The following table contains example parameter entries for the different connection types:



| Type | Items |
|------------------------------------|---|
| RFC client (application server) | DEST=W74 TYPE=A ASHOST=roesap005.sealsystems.local SYSNR=00 RFC_TRACE=0 ABAP_DEBUG=0 USE_SAPGUI=0 UNICODE=1 SNC_MODE=1 SNC_MYNAME=p:CN=SEALRFC, OU=SEALSAP, O=SEAL, C=DE SNC_PARTNERNAME=p:CN=T6B, OU=SEALSAP, O=SEAL, C=DE SNC_QQP=3 SNC_SSO=1 X509CERT=c:\seal\customer\server\sapserv\conf\sec\SEAL-RFC.crt |
| RFC client (message server) | DEST=W74 TYPE=B MSHOST=roemsg001.sealsystems.local MSSERV=3601 GROUP=Standard RFC_TRACE=0 ABAP_DEBUG=0 USE_SAPGUI=0 UNICODE=1 |

Parameter Overview, Continuation

| Type | Items |
|--------------------|--|
| RFC server gateway | DEST=W74RFC TYPE=R GWHOST=/H/saprouter.com/H/roegw001.sealsystems.local GWSERV=sapgw00 RFC_TRACE=0 SEAL_TRACE=1 UNICODE=1 CODEPAGE=UTF-8 SNC_MODE=1 SNC_MYNAME=p:CN=SEALRFC, OU=SEALSAP, O=SEAL, C=DE SNC_QOP=8 SNC_SSO=1 |



Caution - RFC client

For each RFC client, only one item is allowed, either one with TYPE=A for application server or one with TYPE=B for message server.

DEST Parameter

The DEST parameter contains the unique identifier for the SAP system. meaning

It refers to the DESTINATIONS item in the configuration file like rfcserver.cfg. It is used to determine the SAP system data for the RFC destination which should be established.

The identifier should indicate the SAP system and the type of the RFC destination. The following naming convention is advisable where W74 is used as example of an SAP system name: naming convention

| DEST Value | Using for |
|------------|---|
| W74 | RFC client connections via application server |
| W74 | RFC client connections via message server |
| W74RFC | RFC server connections via SAP gateway |

RFC server as of 1.3.3 or newer allows identifiers with a maximum of 32 characters. Lower versions only support a maximum of 8 characters. length

The parameter DEST is evaluated for all destination types. validity

TYPE Parameter

| | |
|---------|---|
| meaning | The TYPE parameter identifies the connection type. |
| values | <p>The following connection types are available:</p> <ul style="list-style-type: none"> • A RFC client connections via application server The connection via an application server is the standard connection type for RFC clients. This type is used by all interactive modules and by the modules DMS Rlist and DMS Loader. • B RFC client connections via message server The connection via a message server is available for RFC clients as an alternative to the connection via an application server. It is rarely used. It can be used for load distribution purposes (load balancing) to distribute the registration via the message server to several application servers. • R RFC server connections via SAP gateway RFC server or conversion server register with an intermediate SAP gateway where they then wait for queries from the SAP system or other RFC clients. Usually, an SAP gateway is running on each application server. |

Caution -port assignment

For RFC client connections via message servers (type B), a port must be explicitly assigned in the `C:\Windows\System32\drivers\etc\services` system file (Windows example) if `MSSERV` is not set or the symbolic system identifier is assigned, for example `MSSERV=sapmsw74`:

- `sapmsSID 36XX/tcp`, for example `sapmsw74 3601/tcp`
(type B, RFC client connections via message server)
If `MSSERV` is assigned to an explicit port, for example `MSSERV=3601`, no item in the system file is necessary.

automatic port assignment

The following settings in the `saprfc.ini` file are automatically assigned the correct ports; they do not need to be entered in the system file `C:\Windows\System32\drivers\etc\services` (Windows example):

- `sapdpXX32XX/tcp`, for example `sapdp01 3201/tcp`
(type A, RFC client connections via application server)
- `sapgwXXs 48XX/tcp` (SNC), for example `sapgw01s 4801/tcp`
`sapgwXX 33XX/tcp` (otherwise), for example `sapgw01 3301/tcp`
(type R, RFC server connections via SAP gateway)

Caution - message server with SAProuter

For RFC destinations via message server (TYPE=B) with SAProuter, the following requirement must be fulfilled:

- In the DNS, both the Windows host name of the message server and its `SAPLOCALHOSTFULL` as Fully Qualified Domain Names (FQDN) must be maintained.

| | |
|----------|--|
| validity | The TYPE parameter is evaluated for all destination types. |
|----------|--|

ASHOST Parameter


The ASHOST parameter contains the host address of the application server as a Fully Qualified Domain Name (FQDN). meaning


You can see the host address in: system data

- *Group/Server*

ASHOST=roesap005.sealsystems.local

→ *Determine System Data for saprfc.ini, Page 128*

 example

 related topics

If an SAProuter is in use (for example: SAPROUTER=/H/saprouter.com/S/3299), the full name for ASHOST is automatically composed of: background knowledge - SAP-router

- *Router*
Begin of string with URL specification, rest truncated
- */H/*
- *Group/Server*

ASHOST=/H/saprouter.com/H/roesap005.sealsystems.local

The ASHOST parameter is evaluated only for the following destination types: validity

- Type A, RFC client connections via application server

SYSNR Parameter

meaning The SYSNR parameter contains the instance number (up to release 4.7: system number) of the application server.

system data You can see the instance number in:

- *Instance Number*



example

SYSNR=00



related top-
ics

→ *Determine System Data for saprfc.ini*, Page 128

validity The SYSNR parameter is evaluated only for the following destination types:

- Type A, RFC client connections via application server

MSHOST Parameter


The MSHOST parameter contains the host address of the message server as a Fully Qualified Domain Name (FQDN). meaning


You can see the host address in: system data

- *Message Server*

MSHOST=roemsg001.sealsystems.local

→ *Determine System Data for saprfc.ini, Page 128*

 example

 related topics

If an SAProuter is in use (for example: SAPROUTER=/H/saprouter.com/S/3299), the full name for MSHOST is automatically composed of: background knowledge - SAP-router




- *Router*
Begin of string with URL specification, rest truncated
- */H/*
- *Message Server*

MSHOST=/H/saprouter.com/H/roemsg001.sealsystems.local

The MSHOST parameter is evaluated only for the following destination types: validity

- Type B, RFC client connections via message server

MSSERV Parameter

| | |
|--|--|
| meaning | The MSSERV parameter contains either the explicit port number, for example MSSERV=3601, or the system identifier. |
| system data | The system identifier of the message server is composed of: <ul style="list-style-type: none"> • sapms • <i>System ID (SID)</i> |
|  related topics | → <i>Determine System Data for saprfc.ini</i> , Page 128 |
|  example | MSSERV=sapmsW74 (system identifier) MSSERV=3601 (explicit port) |
|  Caution -port assignment | If MSSERV is not set or a symbolic system identifier is assigned, for example MSSERV=sapmsW74, an explicit port assignment in the C:\Windows\System32\drivers\etc\services system file (example Windows) is necessary. <ul style="list-style-type: none"> • sapmsSID 36XX/tcp, for example sapmsW74 3601/tcp If MSSERV is assigned to an explicit port, for example MSSERV=3601, no item in the system file is necessary. |
| validity | The MSSERV parameter is evaluated only for the following destination types: <ul style="list-style-type: none"> • Type B, RFC client connections via message server |

R3NAME Parameter

The R3NAME parameter contains the system ID of the SAP system..

meaning

In general, the DEST parameter corresponds to the system ID. In this case, R3NAME does not need to be specified.


Only if DEST does not correspond to the system ID is it necessary to enter R3NAME.

You can see the system ID in:


system data

- *SID*

R3NAME=W74

 example

→ *Determine System Data for saprfc.ini*, Page 128

 related topics

The R3NAME parameter is evaluated only for the following destination types:

validity

- Type B, RFC client connections via message server

GROUP Parameter

meaning The GROUP parameter contains the group identifier of the message server.

system data You can see the group identifier of the message server in:

- *Group/Server*



example

GROUP=PUBLIC



related top-
ics

→ *Determine System Data for saprfc.ini*, Page 128

validity The GROUP parameter is evaluated only for the following destination types:

- Type B, RFC client connections via message server


GWHOST Parameter

The GWHOST parameter contains the host address of the SAP gateway as a Fully Qualified Domain Name (FQDN). The SAP gateway is generally identical to the application server. meaning


You can see the host address in: system data

- *Group/Server*

GWHOST=roegw001.sealsystemsm.local

 example

→ *Determine System Data for saprfc.ini*, Page 128

 related topics

If an SAProuter is in use (for example: SAPROUTER=/H/saprouter.com/S/3299), the full name for GWHOST is automatically composed of: background knowledge - SAP-router




- *Router*
Begin of string with URL specification, rest truncated
- */H/*
- *Group/Server*

GWHOST=/H/saprouter.com/H/roegw001.sealsystems.local

The GWHOST parameter is evaluated only for the following destination types: validity

- Type R, RFC server connections via SAP gateway

GWSERV Parameter

| | |
|--|--|
| meaning | <p>The GWSERV parameter contains either the explicit port number, for example GWSERV=4801, or the group identifier of the SAP gateway.</p> <p>The GWSERV parameter contains the group identifier of the SAP gateway.</p> |
| system data | <p>The group identifier of the SAP Gateway is composed of:</p> <ul style="list-style-type: none"> • <code>sapgw</code> • <i>Instance Number</i> |
|  related topics | → <i>Determine System Data for saprfc.ini</i> , Page 128 |
|  example | <p>GWSERV=sapgw01s (group identifier)</p> <p>GWSERV=4801 (explicit port)</p> |
|  hint - automatic port assignment | <p>Items starting with <code>sapgw</code> are automatically assigned the correct port, for example <code>sapgw01</code> to <code>3301/tcp</code>, <code>sapgw02</code> to <code>3302/tcp</code> or <code>sapgw01s</code> to <code>4801/tcp</code>. They no longer need to be explicitly assigned in the <code>C:\Windows\System32\drivers\etc\services</code> system file (Windows example).</p> |
| validity | <p>The GWSERV parameter is evaluated only for the following destination types:</p> <ul style="list-style-type: none"> • Type R, RFC server connections via SAP gateway |

SAPROUTER Parameter

The SAPROUTER parameter contains the host address of the SAProuter.

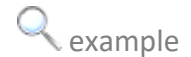
meaning

You can see the host address of the SAProuter in:

system data

- Router

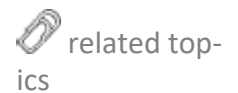
SAPROUTER=/H/saprouter.com (with default port 3299)



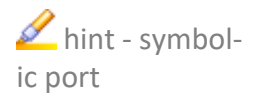
SAPROUTER=/H/saprouter.com/S/sapgw01 (with optional symbolic port)

SAPROUTER=/H/saprouter.com/S/3301 (with optional explicit port)

→ *Determine System Data for saprfc.ini*, Page 128



If the SAProuter string contains a symbolic port, for instance /S/sapgw01, this port has to be assigned in the system file:



→ *TYPE Parameter*, Page 134

The SAPROUTER parameter is evaluated only for the following destination types:

validity

- Type A, RFC client connections via application server
- Type B, RFC client connections via message server
- Type R, RFC server connections via SAP gateway

RFC_TRACE Parameter

meaning The RFC_TRACE parameter activates or deactivates the trace messages of the SAP components.

location and name Trace messages are saved on the application server in the log directory in files with the following names:

jco_rfc_*.trc

dev_rfc*

If the CPIC_TRACE environment variable is set to a value >0, the following file is created additionally:

CPIC*



Caution - size

Files with the trace messages can quickly become extremely large; therefore the trace messages should only be activated for test purposes. By default, it is advisable to deactivate the trace messages.

values

The following values are available:

- 0 The trace messages are deactivated.
- 1 Error messages
- 2 Additional warnings
- 3 Additional information
- 4 Additional process trace
- 5 Additional extended process trace
- 6 Additional restricted data trace
- 7 Additional data trace with metadata
- 8 Additional complete data trace with metadata

validity


The RFC_TRACE parameter is evaluated for all destination types.

SEAL_TRACE Parameter

The SEAL_TRACE parameter activates or deactivates additional information in the log file and the creation of HTML files containing the transferred data from and to SAP. meaning

The following values are available: values

- 0 No additional information in the log file
- 1
Sets the size of the log file: `java.util.logging.FileHandler.level=ALL`
Also writes function list, environment variables to the log file
Sets `FTP_TRACE=2`, `HTTP_TRACE=2`
Starts `sapftp/saphttp` with `-t`
- 2
Also writes HTML files with the transferred data
Also writes TLS information for URLs with `https` to the log file
- 3
Also writes Java memory status to the log file

HTML files with the transferred data can quickly become extremely large; therefore the creation of HTML files should only be activated for troubleshooting. By default, it is advisable to set SEAL_TRACE to 0 or 1.  Caution - number

Default is 0. default

The SEAL_TRACE parameter is evaluated only for the following destination types: validity

- Type R, RFC server connections via SAP gateway

ABAP_DEBUG Parameter

| | |
|-------------|---|
| meaning | The ABAP_DEBUG parameter activates or deactivates the debugging of system functions. |
| requirement | The USE_SAPGUI parameter must be set to 1 or 2 to enable the debugging. |
| values | <p>The following values are available:</p> <ul style="list-style-type: none">• 0 The debugging of the system functions is deactivated. This is the standard case.• 1 The debugging of the system functions is activated for test purposes. |
| validity | <p>The ABAP_DEBUG parameter is evaluated only for the following destination types:</p> <ul style="list-style-type: none">• Type A, RFC client connections via application server• Type B, RFC client connections via message server |

USE_SAPGUI Parameter

The USE_SAPGUI parameter determines if SAP GUI is used for communication. In addition to that it specifies if the dialogs are minimized after the end of the function. meaning

The following requirements have to be fulfilled: requirement

- USE_SAPGUI must be set to 2 for the modules DMS Repro and DMS Scan.
- If USE_SAPGUI is set to 1 or 2 a dialog user must be specified in `cadrfc.ini`! A system user causes error.

The following values are available: values

- 0
SAP GUI is not used for communication.
- 1
SAP GUI is used for communication. The dialogs remain open after the end of the function.
- 2
SAP GUI is used for communication. The dialogs are minimized after the end of the function.

The USE_SAPGUI parameter is evaluated only for the following destination types: validity

- Type A, RFC client connections via application server
- Type B, RFC client connections via message server

UNICODE Parameter

| | |
|-----------|--|
| meaning | <p>The UNICODE parameter specifies if the SAP system is a Unicode or non-Unicode system.</p> <p>By means of this parameter the correct version of the programs sapftp and saphttp is determined.</p> |
| values | <p>The following values are available:</p> <ul style="list-style-type: none">• 0: The SAP system is a non-Unicode system.• 1: The SAP system is a Unicode system. |
| code page | <p>For Unicode systems, the coding can be specified with CODEPAGE:</p> <p>→ <i>CODEPAGE Parameter</i>, Page 149</p> |
| validity | <p>The UNICODE parameter is evaluated only for the following destination types:</p> <ul style="list-style-type: none">• Type A, RFC client connections via application server• Type B, RFC client connections via message server• Type R, RFC server connections via SAP gateway |

CODEPAGE Parameter

The CODEPAGE parameter specifies the coding for Unicode systems.

meaning

The code page is only evaluated in the case UNICODE=1.

interrelation

The default code page is UTF-8. These is used in the following cases:

default

- Neither a general code page is specified in `saprfc.ini` nor a specific code page at the function start.
- The specified code page is not supported by Java.
- The specified code page is UTF-* (* = 7, 16, 16BE, 32, ...), because only UTF-8 and UTF-16LE are supported.

The CODEPAGE parameter is only evaluated for the following destination types:

validity

- Type R, RFC server connections via SAP gateway

SNC_MODE Parameter

meaning The SNC_MODE parameter activates and deactivates SNC (activation sign).

values The following values are available:

- 0: SNC is deactivated.
- 1: SNC is activated.

default Default is 0.

validity The SNC_MODE parameter is evaluated for all destination types.

SNC_MYNAME Parameter

The SNC_MYNAME parameter contains the name of the user who executes remote function calls. meaning

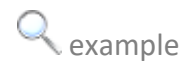
The default name is the name which is determined by the security product for the current user. default

The name must use the following format: format

p:SEAL Server - DistinguishedName from SEALRFC.pse

p:CN=UniqueName, OU=Department, O=Company, C=CountryKey

p:CN=SEALRFC, OU=SEALSAP, O=SEAL, C=DE




The SNC_MYNAME parameter is evaluated for all destination types. validity

SNC_PARTNERNAME Parameter

meaning The SNC_PARTNERNAME parameter contains the name of the communication partner (application server).

format The name must use the following format:
p:SAP System - DistinguishedName

 **example** *p:CN=UniqueName, OU=Department, O=Company, C=CountryKey*
p:CN=SEALRFC, OU=SEALSAP, O=SEAL, C=DE

validity The SNC_PARTNERNAME parameter is evaluated only for the following destination types:

- Type A, RFC client connections via application server
- Type B, RFC client connections via message server

SNC_QOP Parameter

The SNC_QOP parameter specifies the protection level (quality of protection). meaning

The following values are available: values

- 1: Use authentication only
- 2: Use integrity protection (authentication)
- 3: Use confidentiality protection (integrity and authentication)
- 8: Use default values
- 9: Use maximum protection

The default security level is 3 for RFC client connections via application server (TYPE=A) or message server (TYPE=B) and 8 for RFC server connections via SAP gateway (TYPE=R). default

The SNC_QOP parameter is evaluated for all destination types. validity

SNC_SSO Parameter

| | |
|-------------|---|
| meaning | <p>The SNC_SSO parameter activates or deactivates the single sign-on mechanism (SSO) of SNC. This allows to log on on the SAP ABAP backend with a user different from the SNC identity, while SNC is used for the encryption of the network communication.</p> <p>The parameter must be set for logon with user/password when SNC is activated.</p> <p>The parameter does not need to be set when logging on via certificate/PSE (SSO, single sign-on) in the SNC context. In this case, the default applies.</p> |
| requirement | A minimum kernel patch of the SAP system is required, see SAP note 1701870. |
| values | <p>The following values are available:</p> <ul style="list-style-type: none">• 0: SSO is deactivated. Instead, user/password is used for logon, for example.• 1: SSO is activated. |
| default | Default is 1. |
| validity | The SNC_SSO parameter is evaluated for all destination types. |

ASCS Parameter

The ASCS(ABAP SAP Central Services) parameter contains the name of the section of type R with the data of the central SAP gateway. meaning

The ASCS parameter is only supported together with static RFC destinations. requirement

Section name of type R with data from the central SAP gateway.  example

ASCS=W74MSRFC



The ASCS parameter is evaluated only for the following destination types: validity

- Type A, RFC client connections via application server (only on request)
- Type B, RFC client connections via message server

X509CERT Parameter

| | |
|----------|--|
| meaning | The X509CERT parameter contains the certificate name if the logon with certificate (SSO, single sign-on) is activated. |
| format | The certificate must be in the Based64 file format, in one line without BEGIN and END sequence. |
| default | The default name is: <code>%SEAL_CUSTOMDIR%\server\sapserv\conf\sec\SEALRFC.crt</code> |
| validity | The X509CERT parameter is evaluated for all destination types. |

8.3 sapnwrfc.ini - Connection Data

| | |
|---|--|
| <p>The <code>sapnwrfc.ini</code> configuration file is only relevant for communication via SAP NetWeaver RFC Library NWRFC as used by SAP connectors such as <code>seal-co-notifier</code> for reply to SAP.</p> | <p>required if</p> |
| <p>This chapter contains the reference information about the <code>sapnwrfc.ini</code> configuration file.</p> | <p>introduction</p> |
| <p>The <code>sapnwrfc.ini</code> file is located in the following directory: <code>C:\ProgramData\SEAL Systems\config</code></p> | <p>location</p> |
| <p>The configuration file contains parameter items with the system data for the individual SAP systems. This data is used to establish the RFC connections from the external server to the SAP systems.</p> | <p>contents</p> |
| <p>For RFC client connections via message servers, a port must be explicitly assigned in the <code>C:\Windows\System32\drivers\etc\services</code> system file (Windows example) if <code>MSSERV</code> is not set or the symbolic system identifier is assigned, for example <code>MSSERV=sapmsw74</code>:</p> <ul style="list-style-type: none"> • <code>sapmsSID 36XX/tcp</code>, for example <code>sapmsw74 3601/tcp</code> (RFC client connections via message server) If <code>MSSERV</code> is assigned to an explicit port, for example <code>MSSERV=3601</code>, no item in the system file is necessary. | <p> Caution -port assignment</p> |
| <p>The following settings in the <code>sapnwrfc.ini</code> file are automatically assigned the correct ports; they do not need to be entered in the system file <code>C:\Windows\System32\drivers\etc\services</code> (Windows example):</p> <ul style="list-style-type: none"> • <code>sapdpXX32XX/tcp</code>, for example <code>sapdp01 3201/tcp</code> (RFC client connections via application server) • <code>sapgwXXs 48XX/tcp</code> (SNC), for example <code>sapgw01s 4801/tcp</code> <code>sapgwXX 33XX/tcp</code> (otherwise), for example <code>sapgw01 3301/tcp</code> (RFC server connections via SAP gateway) | <p>automatic port assignment</p> |
| <p>For RFC destinations via message server with SAProuter, the following requirement must be fulfilled:</p> <ul style="list-style-type: none"> • In the DNS, both the Windows host name of the message server and its <code>SAPLOCALHOSTFULL</code> as Fully Qualified Domain Names (FQDN) must be maintained. | <p> Caution - message server with SAProuter</p> |
| <p>This chapter deals with the following topics:</p> <ul style="list-style-type: none"> → <i>Parameter Overview</i>, Page 130 → <i>Parameters Depending on Connection Type</i>, Page 161 → <i>General Connection Parameters</i>, Page 171 → <i>Connection Parameters for Client Programs</i>, Page 181 | <p>in this chapter</p> |

8.3.1 Parameter Overview

validity

Some parameters are evaluated for all connection types. In addition to these general parameters there are parameters which are only important for special connection types.

overview

The following table presents an overview of which parameters are evaluated for which connection type:

| Parameter | RFC Client Application Server | RFC Client Message Server | RFC Server Gateway |
|-----------------|----------------------------------|---------------------------------------|--|
| DEST | X | X Alternatives: R3NAME SYSID | X Alternatives: TPNAME PROGRAM_ID |
| ASHOST | X | - | - |
| SYSNR | X | - | - |
| MSHOST | - | X | - |
| MSSRV | - | X | - |
| GROUP | - | X | - |
| GWHOST | - | - | X |
| GWSERV | - | - | X |
| SAPROUTER | X | X | X |
| SNC_LIB | X | X | X |
| SNC_MYNAME | X | X | X |
| SNC_PARTNERNAME | X | X | X |
| SNC_QOP | X | X | X |
| TRACE | X | X | X |
| NO_COMPRESSION | X | X | X |
| USER | X | X | - |
| PASSWD | X | X | - |
| CLIENT | X | X | - |
| LANG | X | X | - |
| MYSAPSS02 | X | X | - |
| GETSS02 | X | X | - |
| X509CERT | X | X | - |

Parameter Overview, Continuation

| Parameter | RFC Client Application Server | RFC Client Message Server | RFC Server Gateway |
|------------|----------------------------------|------------------------------|-----------------------|
| LCHECK | X | X | - |
| USE_SAPGUI | X | X | - |
| ABAP_DEBUG | X | X | - |

The following table contains example parameter entries for the different connection types:



| Type | Items |
|------------------------------------|--|
| RFC client (application server) | <pre> DEST=W74 ASHOST=roesap005.sealsystems.local SYSNR=00 TRACE=0 ABAP_DEBUG=0 USE_SAPGUI=0 UNICODE=1 SNC_MYNAME=p:CN=SEALRFC, OU=SEALSAP, O=SEAL, C=DE SNC_PARTNERNAME=p:CN=T6B, OU=SEALSAP, O=SEAL, C=DE SNC_QOP=3 USER=SEALCPIC PASSWD=**** </pre> |
| RFC client (message server) | <pre> DEST=W74 MSHOST=roemsg001.sealsystems.local MSSERV=3601 GROUP=Standard TRACE=0 ABAP_DEBUG=0 USE_SAPGUI=0 X509CERT=c:\seal\customer\server\sapserv\conf\sec\SEAL-RFC.crt </pre> |

Parameter Overview, Continuation

| Type | Items |
|--------------------|--|
| RFC server gateway | DEST=W74RFC GWHOST=/H/saprouter.com/H/roegw001.sealsystems.local GWSERV=sapgw00 TRACE=0 SNC_MYNAME=p:CN=SEALRFC, OU=SEALSAP, O=SEAL, C=DE SNC_QOP=8 |

8.3.2 Parameters Depending on Connection Type

This chapter deals with the following topics:

in this chapter

- *DEST Parameter*, Page 133
- *ASHOST Parameter*, Page 135
- *SYSNR Parameter*, Page 136
- *MSSERV Parameter*, Page 137
- *MSSERV Parameter*, Page 138
- *R3NAME Parameter*, Page 167
- *GROUP Parameter*, Page 140
- *GWHOST Parameter*, Page 141
- *GWSERV Parameter*, Page 142

DEST Parameter

meaning The DEST parameter contains the unique identifier for the SAP system. It refers to the DESTINATIONS item in the configuration file like rfcserver.cfg. It is used to determine the SAP system data for the RFC destination which should be established.

naming convention The identifier should indicate the SAP system and the type of the RFC destination. The following naming convention is advisable where W74 is used as example of an SAP system name:

| DEST Value | Using for |
|------------|---|
| W74 | RFC client connections via application server |
| W74MS | RFC client connections via message server |
| W74RFC | RFC server connections via SAP gateway |

length RFC server as of 1.3.3 or newer allows identifiers with a maximum of 32 characters. Lower versions only support a maximum of 8 characters.

validity The parameter DEST is evaluated for all destination types.

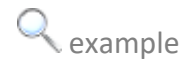
ASHOST Parameter

The ASHOST parameter contains the host address of the application server as a Fully Qualified Domain Name (FQDN). meaning

You can see the host address in: system data

- *Group/Server*

ASHOST=roesap005.sealsystems.local



If an SAProuter is in use (for example: SAPROUTER=/H/saprouter.com/S/3299/H/), the full name for ASHOST is automatically composed of: background knowledge - SAP-router


- *Router*
Begin of string with URL specification, rest truncated
- */H/*
- *Group/Server*

ASHOST=/H/saprouter.com/H/roesap005.sealsystems.local

The ASHOST parameter is evaluated only for the following destination types: validity

- RFC client connections via application server

SYSNR Parameter

| | |
|---|--|
| meaning | The SYSNR parameter contains the instance number (up to release 4.7: system number) of the application server. |
| system data | You can see the instance number in: <ul style="list-style-type: none">• <i>Instance Number</i> |
|  example | SYSNR=00 |
| validity | The SYSNR parameter is evaluated only for the following destination types: <ul style="list-style-type: none">• RFC client connections via application server |

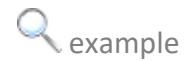
MSHOST Parameter

The MSHOST parameter contains the host address of the message server as a Fully Qualified Domain Name (FQDN). meaning

You can see the host address in: system data

- *Message Server*

MSHOST=roemsg001.sealsystems.local



If an SAProuter is in use (for example: SAPROUTER=/H/saprouter.com/S/3299/H/), the full name for MSHOST is automatically composed of:

background
knowledge - SAP-
router


- *Router*
Begin of string with URL specification, rest truncated
- */H/*
- *Message Server*

MSHOST=/H/saprouter.com/H/roemsg001.sealsystems.local

The MSHOST parameter is evaluated only for the following destination types: validity

- RFC client connections via message server

MSSERV Parameter

| | |
|---|---|
| meaning | The MSSERV parameter contains the explicit port number. |
|  example | MSSERV=3601 (explicit port) |
| required if | The MSSERV parameter only needs to be set in the following cases: <ul style="list-style-type: none">• The message server listens on a port that is not defined in the service system file. |
| default | The message server listens on the <i>sapmsSID</i> default port, example: <i>sapmsW74</i> , with the following item in the C:\Windows\System32\drivers\etc\services (example Windows) or /etc/services (example Linux) service system file: <ul style="list-style-type: none">• <i>sapmsSID 36XX/tcp</i>, for example <i>sapmsW74 3601/tcp</i> |
| validity | The MSSERV parameter is evaluated only for the following destination types: <ul style="list-style-type: none">• RFC client connections via message server |

R3NAME Parameter

The R3NAME parameter contains the system ID of the SAP system.. meaning


In general, the DEST parameter corresponds to the system ID. In this case, R3NAME does not need to be specified.

Only if DEST does not correspond to the system ID is it necessary to enter R3NAME.

You can see the system ID in: system data

- *SID*

R3NAME=W74

 example

The R3NAME parameter is evaluated only for the following destination types: validity


- RFC client connections via message server

GROUP Parameter

meaning The GROUP parameter contains the group identifier of the message server.

system data You can see the group identifier of the message server in:

- *Group/Server*

 example

GROUP=PUBLIC (default)

validity The GROUP parameter is evaluated only for the following destination types:

- RFC client connections via message server

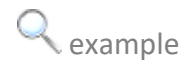
GWHOST Parameter

The GWHOST parameter contains the host address of the SAP gateway as a Fully Qualified Domain Name (FQDN). The SAP gateway is generally identical to the application server. meaning

You can see the host address in: system data

- *Group/Server*

GWHOST=roegw001.sealsystemsm.local



If an SAProuter is in use (for example: SAPROUTER=/H/saprouter.com/S/3299/H/), the full name for GWHOST is automatically composed of: background
knowledge - SAP-
router



- *Router*
Begin of string with URL specification, rest truncated
- */H/*
- *Group/Server*

GWHOST=/H/saprouter.com/H/roegw001.sealsystems.local

The GWHOST parameter is evaluated only for the following destination types: validity

- RFC server connections via SAP gateway

GWSERV Parameter

| | |
|--|--|
| meaning | <p>The GWSERV parameter contains either the explicit port number, for example GWSERV=4801, or the group identifier of the SAP gateway.</p> <p>The GWSERV parameter contains the group identifier of the SAP gateway.</p> |
| system data | <p>The group identifier of the SAP Gateway is composed of:</p> <ul style="list-style-type: none"> • sapgw • <i>Instance Number</i> |
|  example | <p>GWSERV=sapgw01s (group identifier)</p> <p>GWSERV=4801 (explicit port)</p> |
|  hint - automatic port assignment | <p>Items starting with sapgw are automatically assigned the correct port, for example sapgw01 to 3301/tcp, sapgw02 to 3302/tcp or sapgw01s to 4801/tcp. They no longer need to be explicitly assigned in the C:\Windows\System32\drivers\etc\services system file (Windows example).</p> |
| validity | <p>The GWSERV parameter is evaluated only for the following destination types:</p> <ul style="list-style-type: none"> • RFC server connections via SAP gateway |


8.3.3 General Connection Parameters

This chapter deals with the following topics:

in this chapter

- *SAPROUTER* Parameter, Page 143
- *SNC_LIB* Parameter, Page 173
- *SNC_MODE* Parameter, Page 174
- *SNC_MYNAME* Parameter, Page 151
- *SNC_PARTNERNAME* Parameter, Page 152
- *SNC_QOP* Parameter, Page 153
- Parameter *TRACE*, Page 178
- *CODEPAGE* Parameter, Page 149
- *NO_COMPRESSION* Parameter, Page 180

SAPROUTER Parameter

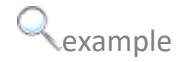
| | |
|---|--|
| meaning | The SAPROUTER parameter contains the host address and port number of the SAProuter. |
| format | The name must use the following format: <i>SAPROUTER=/H/RouterHostName/S/PortNumber/H/TargetHost/S/PortNumber</i> |
|  example | SAPROUTER=/H/saprouter.com/S/3399/H/target.com/S/3301 SAPROUTER=/H/target.com/S/3301 |
| validity | The SAPROUTER parameter is evaluated for all destination types. |

SNC_LIB Parameter

The SNC_LIB parameter specifies the library used for SNC communication (authorization, encryption, signature) meaning

Alternatively, the following environment variable can be set: SNC_LIB_64

SNC_LIB=sapcrypto.dll



The SNC_LIB parameter is evaluated for all destination types.

validity

SNC_MODE Parameter

meaning The SNC_MODE parameter activates and deactivates SNC (activation sign).

values The following values are available:

- 0: SNC is deactivated.
- 1: SNC is activated.

default Default is 0.

validity The SNC_MODE parameter is evaluated for all destination types.

SNC_MYNAME Parameter

The SNC_MYNAME parameter contains the name of the external program which sends remote function calls. meaning

The default name is the name which is determined by the security product for the current user. default

The name must use the following format: format

p:SEAL Server - DistinguishedName from SEALRFC.pse


p:CN=UniqueName, OU=Department, O=Company, C=CountryKey

SNC_MYNAME=p:CN=SEALRFC, OU=SEALSAP, O=SEAL, C=DE



The SNC_MYNAME parameter is evaluated for all destination types. validity

SNC_PARTNERNAME Parameter

| | |
|---|--|
| meaning | The SNC_PARTNERNAME parameter contains the name of the communication partner on the backend system. |
| format | The name must use the following format: <i>p:SAP System - DistinguishedName</i> |
|  example | <i>p:CN=UniqueName, OU=Department, O=Company, C=CountryKey</i> SNC_PARTNERNAME=p:CN=SEALRFC, OU=SEALSAP, O=SEAL, C=DE |
| validity | The SNC_MYNAME parameter is evaluated for all destination types. |

SNC_QOP Parameter

The SNC_QOP parameter specifies the protection level (quality of protection). meaning

The following values are available: values

- 1: Use digital signature only
 - 2: Use integrity protection (digital signature and encryption)
 - 3: Use confidentiality protection (integrity and authentication)
 - 8: Use default values from backend system
 - 9: Use maximum protection
-

The default security level is 3 for RFC client connections via application server (TYPE=A) or message server and 8 for RFC server connections via SAP gateway. default

The SNC_QOP parameter is evaluated for all destination types. validity

Parameter TRACE

meaning The TRACE parameter activates or deactivates the trace messages of the SAP components.

location and name Trace messages are saved on the application server in the log directory in files with the following names:

jco_rfc_*.trc

dev_rfc*

If the CPIC_TRACE environment variable is set to a value >0, the following file is created additionally:

CPIC*



Caution - size

Files with the trace messages can quickly become extremely large; therefore the trace messages should only be activated for test purposes. By default, it is advisable to deactivate the trace messages.

values The following values are available:

- 0 The trace messages are deactivated.
- 1 Brief
- 2 Verbose
- 3 Detailed
- 4 Full

validity The TRACE parameter is evaluated for all destination types.

CODEPAGE Parameter

| | |
|--|-------------|
| The CODEPAGE parameter specifies the coding for non-Unicode systems. | meaning |
| The CODEPAGE parameter only needs to be set in the following cases: | required if |
| <ul style="list-style-type: none">• Connection to a non-Unicode backend system with a non-ISO Latin-1 user or password | |
| <hr/> | |
| The CODEPAGE parameter is evaluated for all destination types. | validity |

NO_COMPRESSION Parameter

| | |
|----------|--|
| meaning | <p>The NO_COMPRESSION parameter deactivates compression of tables larger than 8 KB.</p> <p>This is useful for very large integer/binary tables with random data, where compression consumes resources without having any effect.</p> |
| default | <p>By default, all tables larger than 8 KB are compressed.</p> |
| values | <p>The following values are available:</p> <ul style="list-style-type: none">• 0 (default): Compression is activated. All tables larger than 8 KB are compressed.• 1: Compression is deactivated. |
| validity | <p>The NO_COMPRESSION parameter is evaluated for all destination types.</p> |

8.3.4 Connection Parameters for Client Programs

This chapter deals with the following topics:

in this chapter

- *USER Parameter*, Page 182
- *PASSWD Parameter*, Page 183
- *CLIENT Parameter*, Page 184
- *LANG Parameter*, Page 185
- *SNC_SSO Parameter*, Page 186
- *MYSAPSSO2 Parameter*, Page 187
- *X509CERT Parameter*, Page 188
- *LCHECK Parameter*, Page 189
- *USE_SAPGUI Parameter*, Page 147
- *ABAP_DEBUG Parameter*, Page 146

USER Parameter

meaning The USER parameter determines the user used by the RFC client to logon on the SAP system.

 example USER=SEALCPIC

requirement The following requirements must be fulfilled for a successful logon:

- The specified user must be identically configured on all SAP systems.
- The user name must be entered in capitals.
- The interactive RFC clients require a dialog user.
- For security reasons, a system user is generally used for logon by the remaining RFC clients, for instance SAP connectors.

Exception:
If USE_SAPGUI is specified as 1 or 2 a dialog user must be used!

validity The ASCS parameter is evaluated only for the following destination types:

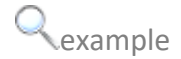
- RFC client connections via application server
- RFC client connections via message server

PASSWD Parameter

The PASSWD parameter determines the password used by the RFC client to logon on the SAP system. meaning

The password can be specified either in plain text or encrypted using SECRET or SECRET_FILE.

PASSWD=364de47d4d093ce8e7c65e244c08e7cb7fe2657e6cdd796a



For information on encrypting passwords, see →Secure the SAP Logon Data.




The ASCS parameter is evaluated only for the following destination types: validity

- RFC client connections via application server
- RFC client connections via message server

CLIENT Parameter

meaning The CLIENT parameter determines the client used by the RFC client to logon on the SAP system.

 example

CLIENT=020

validity The CLIENT parameter is evaluated only for the following destination types:

- RFC client connections via application server
- RFC client connections via message server

LANG Parameter

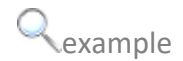
The LANG parameter specifies the logon language. meaning

The language is specified in one of the following formats: format

- ISO code - 2 digits, case-insensitive, for example DE
 - SAP-specific code—1 digit, case-sensitive, for example, D for German or d for Serbian
-

LANG=DE (ISO code)

LANG=D (SAP specific code)



The LANG parameter is evaluated only for the following destination types: validity

- RFC client connections via application server
- RFC client connections via message server

SNC_SSO Parameter

| | |
|-------------|---|
| meaning | <p>The SNC_SSO parameter activates or deactivates the single sign-on mechanism (SSO) of SNC. This allows to log on on the SAP ABAP backend with a user different from the SNC identity, while SNC is used for the encryption of the network communication.</p> <p>The parameter must be set for logon with user/password when SNC is activated.</p> <p>The parameter does not need to be set when logging on via certificate/PSE (SSO, single sign-on) in the SNC context. In this case, the default applies.</p> |
| requirement | A minimum kernel patch of the SAP system is required, see SAP note 1701870. |
| values | <p>The following values are available:</p> <ul style="list-style-type: none">• 0: SSO is deactivated. Instead, user/password is used for logon, for example.• 1: SSO is activated. |
| default | Default is 1. |
| validity | The SNC_SSO parameter is evaluated for all destination types. |

MYSAPSSO2 Parameter

The MYSAPSSO2 parameter activates the single sign-on (SSO) mechanism with logon via an SS02 ticket instead of logon via user name and password. meaning

The MYSAPSSO2 parameter is evaluated only for the following destination types: validity

- RFC client connections via application server
- RFC client connections via message server

X509CERT Parameter

| | |
|----------|---|
| meaning | The X509CERT parameter activates the logon via an X.509 ticket instead of logon via user name and password. |
| format | The X.509 certificate must be in the Base64 file format, in one line without BEGIN and END sequence. |
| default | The default name is: <code>%SEAL_CUSTOMDIR%\server\sapserv\conf\sec\SEALRFC.crt</code> |
| validity | The X509CERT parameter is evaluated only for the following destination types: <ul style="list-style-type: none">• RFC client connections via application server• RFC client connections via message server |

LCHECK Parameter

The LCHECK parameter can be used to establish a network connection without logging on, for example to execute a ping command. meaning

The following values are available: values

- 0:
Only a network connection is established without logging on.
Only useful for RFC_PING.
- 1 (default):
A network connection is established and a logon is performed.

The LCHECK parameter is evaluated only for the following destination types: validity

- RFC client connections via application server
- RFC client connections via message server

USE_SAPGUI Parameter

| | |
|-------------|--|
| meaning | The USE_SAPGUI parameter determines if SAP GUI is used for communication. |
| requirement | If SAP GUI is to be used for communication, SAP GUI must be installed on the server running the RFC client program. |
| values | The following values are available: <ul style="list-style-type: none">• 0 Communication without SAP GUI• 1 Communication via hidden ,SAP GUI which receives and ignores screen output• 2 Communication via visible SAP GUI |
| validity | The USE_SAPGUI parameter is evaluated only for the following destination types: <ul style="list-style-type: none">• RFC client connections via application server• RFC client connections via message server |

ABAP_DEBUG Parameter

The ABAP_DEBUG parameter activates or deactivates the debugging of system functions on SAP systems y 6.20. meaning

On SAP systems >= 6.20, it is recommended to use external breakpoints as an alternative.

For debugging on SAP systems < 6.20, SAP GUI must be installed on the server running the RFC client program. requirement



The following values are available: values

- 0
The debugging of the system functions is deactivated. This is the standard case.
- 1
The debugging of the system functions via an visible SAP GUI is activated for test purposes.

The ABAP_DEBUG parameter is evaluated only for the following destination types: validity

- RFC client connections via application server
- RFC client connections via message server

8.4 rfcserver.cfg

| | |
|---|---|
| introduction | This chapter contains the reference information about the rfcserver.cfg configuration file. |
| location | The rfcserver.cfg file is located in the following directory: server\sapserv\conf\rfcserver.cfg The directory and the file can be specified differently from the standard by the RUNTIME_CONFIG environment variable and the -cfgfile parameter. |
|  hint - gXnet-plot | For gXnetplot, the file is located in: servermenu - c - cd1 - cd PDM |
| structure | The configuration file is divided into separate sections. <ul style="list-style-type: none"> → [ACTIVE] Section, Page 193 [ACTIVE] is the first section. Only section names which are specified in the section [ACTIVE] are regarded at the start of the RFC destinations. → [SECTIONNAME] Section, Page 194 The remaining sections with exception of [ACTIVE] can be named user-defined. |
|  example | Example for rfcserver.cfg: [ACTIVE] SEALSAP1 = DEV SEALSAP1 = T6A SEALSAP2 = PROD [DEV] DESTINATIONS = "X74RFC" PROGID = SEAL-BCXDC-001 PROGID = SEAL-BCXDC-002 [T6A] DESTINATIONS = "T6ARFC" PROGID = SEAL-BCXDC-001 3 RLIGATE = %PLSDATA%\io\rligate [PROD] DESTINATIONS = "W74RFC" PROGID = SEAL-BCXDC-001 5 PROGID = SEAL-BCXDC-002 3 PROGID = SEAL-BCXDC-003 RLIGATE = %PLSDATA%\io\stargate XMS = 128 XMX = 512 OTFCODEPAGE = ISO-8859-1 |
| comment character | # and ! are supported as comment characters. Within one file, only one of these comment characters has to be used. A combination of # and ! causes an error at the start. SEAL Systems provides the update_rfc_cfg.pl script (directory: install\rfc) in order to replace ! by #. |
| restart | A restart of JRFC Server is required after modifications in rfcserver.cfg. |

[ACTIVE] Section

This section lists the names of the sections containing the RFC destinations which are to be started. contents

The [ACTIVE] section is ignored on these conditions: exceptions

1. The `SAP_START_SYSTEM` environment variable is specified. In this case the sections names specified in the environment variable are evaluated for the start of the RFC destinations.
2. Section names are specified as parameters when directly executing `rfcserverstart`. In this case, also the `SAP_START_SYSTEM` environment variable is ignored.

The following section describes the available parameters in the [ACTIVE] section. parameters

This name refers to a section in `rfcserver.cfg` which contains further data. *ServerName* or SECTION

The section may contain *ServerName* items or SECTION items. A mix of both is not allowed.

The section may contain multiple *ServerName* or SECTION items. If *ServerName* items exist, only those are considered whose name matches the current server name. If SECTION items exist, all items are considered. For each considered item, a JRFC Server main process is started. Threads related to this main process are started for all RFC destinations which are listed as PROGID in the associated section.

The value is a string.

- PROD
Name of the section in `rfcserver.cfg` containing further data

Default: None

[SECTIONNAME] Section

| | |
|---------------------------------------|---|
| contents | This section contains the relation to the system data in <code>saprfc.ini</code> and a list of the RFC destinations which are to be started with relation to their definitions in the SAP system via the <code>sm59</code> transaction. |
| advantage - SAP system data only once | The SAP system data must only be defined once in <code>saprfc.ini</code> even if several RFC destinations (<code>PROGID</code>) to one SAP system are started. |
| advantage - separate start/stop | For all RFC destinations of one section, a JRFC Server main process is started and stopped. The subdivision into individual sections allows the start of some groups of RFC destinations while other remain stopped. |
| advantage - separate log files | The name of the log files are composed of: <i>ModuleName.SECTIONNAME_Number.log</i> , for instance: <code>rfcserver.PROD_0.log</code> Thus the log files contain only messages of a group of RFC destinations. It is easier to keep track of the status of one RFC destination. |
| Unicode and non-Unicode | If you want to establish RFC destinations to Unicode and non-Unicode systems, you must specify these destination in separate sections. Collect all RFC destinations to non-Unicode systems in a separate section and all RFC destinations to Unicode systems in another section. In this case, one main process is executed for the non-Unicode systems and another main process is executed for the Unicode systems. |
| requirement | The <code>[SECTIONNAME]</code> section is only evaluated on the following conditions: <ol style="list-style-type: none"> 1. It exits as <i>ServerName</i> item with the current server name or as <code>SECTION</code> item in the <code>[ACTIVE]</code> section. 2. The section name is specified via the <code>SAP_START_SYSTEM</code> environment variable. In this case the <code>[ACTIVE]</code> section is ignored. 3. It is specified as parameter when directly executing <code>rfcserver_start</code>. In this case the <code>SAP_START_SYSTEM</code> environment variable and the <code>[ACTIVE]</code> section are ignored. |
| parameters | The following section describes the available parameters in the <code>[SECTIONNAME]</code> section. |
| DESTINATIONS | This name refers to <code>saprfc.ini</code> to determine the SAP system data. The value is a string: <ul style="list-style-type: none"> • <code>W74RFC</code> Name of the system as specified in <code>saprfc.ini</code> at <code>DEST</code> Default: None |

[SECTIONNAME] Section, Continuation

OTFCODEPAGE specifies the code page for downloading OTF data..

OTFCODEPAGE

The value is a string:

- UTF-8
Code page supported by Java, see <https://docs.oracle.com/javase/8/docs/technotes/guides/intl/encoding.doc.html>

Default: iso-8859-1

PROGID is the unique identifier of the RFC destination as specified at Program ID in the SAP system in the sm59 transaction.

PROGID


This name refers to the data in sm59 in the SAP system. The SAP system data is determined via DESTINATIONS.

The section may contain multiple PROGID items. After each PROGID item the thread number, which are started from the JRFC Server main process as a maximum, can be optionally specified to allow a parallel processing.

If no PROGID item exists, the PROGID setting in `saprfc.ini` is used. If there also no item exists, no RFC destination is started.

It is advisable to use the server name as name component to get a unique identifier if multiple OM servers are to establish RFC destinations to the same SAP system.

The identifier can include letters, numbers, '+', '.', '-', and '_' characters!

 naming convention

The value is a string:

- SEAL-ALFILECHECK-*ShortCutNumber*
ArchiveLink FileChecker, `alfileche-cker.cfg`
- SEAL-ALVIEWS-*ShortCutNumber*
ArchiveLink View Server, `alviewserver.cfg`
- SEAL-BCXDC-*ShortCutNumber*
BC-XDC-interface, `rfcserver.cfg`
- SEAL-CONNC-*ShortCutNumber*
Output via JRFC Server, `rfcserver.cfg`, or RFC Server, `rfcserver.cfg`
- SEAL-DPF4C-*ShortCutNumber*
Conversion Server and PDF Longlife Suite SAP Integration - conversion/validation of files already checked-in, `convservdpf.cfg`
- SEAL-PDFLLS-*ShortCutNumber*
PDF Longlife Suite SAP-Integration - check-in, `filecheck.cfg`
- SEAL-VIEWS-*ShortCutNumber*
DMS View Server, `dvsviewserver.cfg`

Default: None

RLIGATE specifies the directory for the repro list processing. It is passed at the start of JRFC Server with the call parameter `-rligate`.

RLIGATE

[SECTIONNAME] Section, Continuation

The value is a string:

- %PLSDATA%\io\stargate
A final \ or / is automatically added if it is missing.

Default: %PLSDATA%\io\stargate

XMS

XMS specifies the minimum memory at start.


The value is an integer with possible values: 0, 64, 128, 256, 512, 1024

- 0
No memory parameter is passed.
- 512
Minimum memory at start in MB

Default: 64

XXM

XXM specifies the maximum memory.

 hint - recommendation:

Specify a three times larger size than the maximum file size, which is to be processed, as value.

The value is an integer with possible values: 0, 64, 128, 256, 512, 1024

- 0
No memory parameter is passed.
- 1024
Maximum memory in MB

Default: 256


9 Configuration Tables - Reference

This chapter contains an alphabetically sorted list of all configuration tables relevant for the basis configuration in SAP. introduction


Each configuration table and its fields is described in a separate section. description

When displaying the value help for certain fields, it is possible to display the internal key of the value in addition to the description text. internal key

This is how you display the internal keys: display key

| Step | Action |
|------|--|
| 1 | Click  in the icon bar of SAP GUI or press Alt+F12 alternatively and select the Options item. |
| 2 | Select on the left: Interaction Design→Visualization 1 |
| 3 | Activate in the Controls section: Show keys within dropdown lists |

After modifications of the configuration tables, the end application must be restarted.

 Caution - restart required

This chapter deals with the following topics:


in this chapter

Listing of all relevant configuration tables

/seal/bas_cr113 - Static Destination for RFC Server

description This configuration table specifies the static destinations for RFC server.

open the table This is how you open the table:

| Step | Action |
|------|---|
| 1 | Click  at: Basis Configuration →Static Destinations →Create Static Destination for RFC Server (table: /seal/bas_cr113) |

overview The table has the following parameters:

| Static Destinations for RFC Server | |
|------------------------------------|-----------------|
| Server | SAPFTP |
| SEAL-CONNC-OKX74-002 | SEAL-SRV-SAPFTP |

Server Server is the RFC server for which the static sapftp destination is to be used.
 The value is a string:

- SEAL-CONNC-001

Default: None

SAPFTP SAPFTP is the name of the template for static sapftp destinations.
 The value is a string:


- SEAL-CLT-SAPFTP
Static sapftp destination for RFC client
- SEAL-SRV-SAPFTP
Static sapftp destination for RFC server

Default: None

/seal/bas_cr114 - Static Destination for RFC Client

This configuration table specifies the static destinations for RFC clients. description

This is how you open the table: open the table

| Step | Action |
|------|---|
| 1 | Click  at: Basis Configuration →Static Destinations →Create Static Destination for RFC Client (table: /seal/bas_cr114) |

The table has the following parameters: overview

| Static destinations for RFC Client | | | | |
|------------------------------------|------------------|-----------------|--------|--|
| User Name | SAPHTTP | SAPFTP | Number | |
| | SEAL-CLT-SAPHTTP | SEAL-CLT-SAPFTP | 3 | |

The item is only evaluated if the user currently logged-on and the specified user match. User Name

If no user is specified, it is called a global setting. This is valid for all users for whom no specific configurations exist.

Regarding the meaning when assigning the template for static sapftp/saphttp connections for RFC client (Table: /seal/bas_cr114): static sapftp/saphttp

User with which the RFC client logs on to SAP from cadrfc.ini

In regard to the meaning in the access table (table: /seal/out_cr029): access table

The following tables display only defaults of the selected user.

The value is a string:

- SEAL1
User Name

Default: None

SAPHTTP is the name of the template for static saphttp destinations. SAPHTTP

The value is a string:

- SEAL-CLT-SAPHTTP
Static saphttp destination for RFC client

Default: None

SAPFTP is the name of the template for static sapftp destinations. SAPFTP

/seal/bas_cr114 - Static Destination for RFC Client,

Continuation

The value is a string:

- SEAL-CLT-SAPFTP
Static sapftp destination for RFC client
- SEAL-SRV-SAPFTP
Static sapftp destination for RFC server

Default: None

Number

Number specifies the maximum number of static sapftp/saphttp destinations to be started.

The value is an integer:

- 3

Default: 1


/seal/bas_cr142 - Define Parameters

General parameters are specified.

description

This is how you open the table:

open the table

| Step | Action |
|------|---|
| 1 | Start the transaction: /n/seal/img |
| 2 | Click  at Basis Configuration →Define Parameters (table: /seal/bas_cr142) |

The table has the following parameters:

overview

| Parameter | | | |
|-----------|------------------|-----------------|---|
| | Parameter ID | Parameter Value | Short Description |
| | PARA_DDEST Un... | X | Unconditional use of destination NONE with classification |
| | PARA_GWSB Pa... | N | Value for USE_GWHOST with destination BACK |
| | PARA_GWHST Pa... | N | Wert for USE_GWHOST |
| | PARA_UCORR A1... | X | Always run correction of OTF data length |

Parameter ID defines the parameter for which a value is to be specified. The possible values at Parameter Value depend on the value of Parameter ID.

Parameter ID

Values of the following enumeration are supported:

- PARA_DDEST Unconditional Use of Destination NONE with Classification
The DESTINATION parameter value is specified for the characteristic evaluation.
- PARA_GWSB Parameter Value of USE_GWHOST at BACK
The parameter value of USE_GWHOST is specified for RFC client connections (destination BACK).
- PARA_GWHST Parameter Value of USE_GWHOST
The parameter value of USE_GWHOST is specified for RFC server connections.
- PARA_NSWAP No byte swapping in OTF data with endianness mismatch
Swapping bytes in bitmap data on bigendian Unicode systems is suppressed.
- PARA_UCORR Correction in OTF Data Streams
The execution of the length correction in ST commands of OTF data streams is specified.

Default: None

/seal/bas_cr142 - Define Parameters, Continuation

| | |
|-------------------|---|
| Parameter Value | <p>Parameter Value specifies the value of the parameter. The possible values depend on the value of Parameter ID.</p> <p>Values of the following enumeration and any strings are supported depending on the value of Parameter ID:</p> <p>PARA_DDEST as Parameter ID:</p> <ul style="list-style-type: none"> • empty (default) Destination NONE is only used for selected transactions (mm02, cv0*, Conversion Server) at the characteristic evaluation in order to accelerate the data evaluation. • X or Y Destination NONE is used at all transactions at the characteristic evaluation. <p>PARA_GWHSB as Parameter ID:</p> <ul style="list-style-type: none"> • Y Set USE_GWHOST for RFC client connections to Y. • N (default) Set USE_GWHOST for RFC client connections to N. <p>PARA_GWHST as Parameter ID:</p> <ul style="list-style-type: none"> • Y Set USE_GWHOST to Y. • N (default) Set USE_GWHOST to N. <p>PARA_UCORR as Parameter ID:</p> <ul style="list-style-type: none"> • empty (default) Consider configuration referred to SAP note 944778 at the length correction of OTF data streams. • X Always execute the length correction in ST commands of OTF data streams. <p>Default: See above</p> |
| Short Description | <p>Short Description contains an explanation of the parameter.</p> <p>The value is a string:</p> <ul style="list-style-type: none"> • Purpose <p>Default: None</p> |

10 Changes

This chapter describes the most important changes for each released module version.

| This chapter deals with the following topics: | in this chapter |
|--|-----------------|
| → <i>Changes with Release 1.5.0</i> , Page 204 | |
| → <i>Changes with Release 1.4.3</i> , Page 205 | |
| → <i>Changes with Release 1.4.2</i> , Page 206 | |
| → <i>Changes with Release 1.4.1</i> , Page 207 | |
| → <i>Changes with Release 1.4.0</i> , Page 208 | |
| → <i>Changes with Release 1.3.5</i> , Page 209 | |
| → <i>Changes with Release 1.3.3</i> , Page 210 | |
| → <i>Changes with Release 1.3.2</i> , Page 211 | |
| → <i>Changes with Release 1.3.1</i> , Page 212 | |
| → <i>Changes with Release 1.3.0</i> , Page 213 | |
| → <i>Changes with Release 1.2.8</i> , Page 214 | |
| → <i>Changes with Release 1.2.6</i> , Page 215 | |
| → <i>Changes with Release 1.2.5</i> , Page 216 | |
| → <i>Changes with Release 1.2.4</i> , Page 217 | |

Changes with Release 1.5.0

| | |
|-------------------------------------|--|
| port assignment - message server | <p>If a port is explicitly assigned to the new MSSERV item in <code>saprfc.ini</code>, for example <code>MSSERV=3601</code>, no port assignment is necessary in the system file.</p> <p>If MSSERV is not set or a symbolic system identifier is assigned, for example <code>MSSERV=sapmsw74</code>, an assignment in the <code>C:\Windows\System32\drivers\etc\services</code> system file (example Windows) is necessary.</p> |
| port assignment - SAP gateway | <p>The automatic mapping of items from the <code>saprfc.ini</code> file that begin with <code>sapgw</code> to the correct ports has been reactivated. The ports no longer need to be explicitly assigned in the <code>C:\Windows\System32\drivers\etc\services</code> system file (Windows example).</p> |

Changes with Release 1.4.3

Items from the `saprfc.ini` file that begin with `sapgw` are no longer automatically assigned to the correct ports. The ports must always be explicitly assigned in the `C:\Windows\System32\drivers\etc\services` system file (example: Windows). port assignment

Changes with Release 1.4.2

| | |
|----------------------------|---|
| logging | <p>The values for SEAL_TRACE in the <code>saprfc.ini</code> file have been extended with the following functionality:</p> <ul style="list-style-type: none">• 0 No additional information in the log file• 1 Sets the level of the log file: <code>java.util.logging.FileHandler.level=ALL</code> Also writes function list, environment variables, connection status to the log file Sets <code>FTP_TRACE=2</code>, <code>HTTP_TRACE=2</code> Start <code>sapftp/saphttp</code> with <code>-t</code>• 2 Writes additional HTML files with the transferred data Writes additional TLS information for URLs with <code>https</code> to the log file• 3 Also writes Java memory status to the log file |
| sapftp/saphttp with SNC | <p>In addition to the dynamic RFC destinations, static RFC destinations are also supported. Static RFC destinations offer the following advantages:</p> <ul style="list-style-type: none">• SNC is supported for <code>sapftp/saphttp</code>• Static RFC destinations can be explicitly enabled/restricted at the gateway. |
| central SAP gateway (ASCS) | <p>The static RFC destination supports the use of a central SAP gateway (ASCS). This offers the following advantages:</p> <ul style="list-style-type: none">• SNC is supported for <code>sapftp/saphttp</code>• Connections via local gateways can be blocked, which increases security. |

Changes with Release 1.4.1

The activation of DPF via REST additionally supports the following options:

REST interface

- Logon with basic authentication
(no support of SAP logon tickets)
- Proxy
- SSL
- HTTP 1.1
- Compression
- HTTP cookies

Changes with Release 1.4.0

SAProuter

The connection via SAProuter is supported with the SAPROUTER parameter (configuration file: saprfc.ini).

Changes with Release 1.3.5

The current version of sapftp/saphttp requires the following DLLs in the tools\bin_xxx directory: sapnwrfccm.dll (non-Unicode) and sapnwrfc.dll (Unicode). DLL

Changes with Release 1.3.3

RFC destination In the supplied configuration files for the RFC connections, for example `rfcserver.cfg`, all RFC connections are inactive. The start of the desired RFC destinations has to be activated explicitly.

Changes with Release 1.3.2

If Unicode SAP systems are used only (no mixed operation with non-Unicode SAP systems, determined via UNICODE in `saprfc.ini`), `sysinit` automatically copies the Unicode version of `sapftp` and `saphttp` from SAP to `sapftp` and `saphttp` and replaces the wrapper program from SEAL Systems.

wrapper program

The `sapftp/saphttp` wrapper programs are delivered with digital signature.

Changes with Release 1.3.1

| | |
|------------|---|
| cadrfc.ini | As of JRFC Server version 2.0.2 or newer, the logon information for the initial logon is no longer required for RFC server connections in <code>cadrfc.ini</code> (this information was required for JRFC Server as of version 2.0.1). |
| logging | The logging of additional information, for instance memory usage and the creation of HTML files containing the transferred data from and to SAP can be activated via the <code>SEAL_TRACE</code> parameter in the <code>saprfc.ini</code> file. |

Changes with Release 1.3.0

The description of the integration via Web service has been inserted to the common basis documentation. Web service

Changes with Release 1.2.8

`cadrfc.ini`

As of JRFC Server 2.0.1 or newer, `cadrfc.ini` has to contain logon information for the initial logon also for RFC server connections. The data has to be located in a system-dependent section [`SAP\SystemName`] which specifies the client as `CadRfcClient` item. A client-dependent section will not be considered!

Changes with Release 1.2.6

The `sap_conn_checker` program is provided to evaluate SAP system data.

`sap_conn_checker`

Changes with Release 1.2.5

start depending
on the current
server

The RFC destinations which are to be started can be specified within the configuration file like `rfcserver.cfg` depending on the current server.

Changes with Release 1.2.4

| | |
|---|---------------------------------|
| <p>The UNICODE parameter in the <code>saprfc.ini</code> file is evaluated at the start of RFC connections. Dependent in this value the Unicode or non-Unicode variant of the <code>sapftp</code> and <code>saphttp</code> program is started. The wrapper programs <code>sapftp</code> and <code>saphttp</code> from SEAL Systems are used to determine the correct variant. It is not necessary to copy files.</p> | Unicode |
| <p>The SAP system data is specified only once in <code>saprfc.ini</code> for each SAP system. Multiple RFC connections are defined via <code>PROGID</code> items in the configuration file, for example <code>rfcserver.cfg</code>.</p> | SAP system data |
| <p>RFC destinations can be grouped within the configuration file like <code>rfcserver.cfg</code>. Each of these groups can be started and stopped individually.</p> | start in groups |
| <p>The required RFC connections for start, status request or stop can be specified via the environment variable <code>SAP_START_SYSTEM</code>.</p> | start with environment variable |
| <p>The required RFC connections for start, status request or stop can be specified via call parameters. This is not supported by <code>p1sstart</code> and <code>dvsstart</code>.</p> | start with call parameter |

Bibliography

[SAP_BASECONF_SAP_TEC]

SAP Basis Configuration - SAP, System Description, SEAL Systems

[SAP_BASECONF_SNC_TEC]

SAP Basis Configuration - SNC and RFC, System Description, SEAL Systems

Terminology

The following section explains the most important terms that are used in this documentation. Terms identified by → refer to other terms in this section.

Customizing

Configuring the SAP system

cv04, cv04n

→Transaction to start the search function in SAP DMS

cv<xx>, cv<xx>n

Transaction used for document search and management within the context of document management in SAP DMS (refer to the SAP online documentation)

Document

→Document information record

Document management system

In the document management system (short: DMS), the →document information records and their assigned files are managed.

Document information record

A master record in the →DMS containing management data for a document and original files. To each document information record, a identification key is assigned, consisting of four partial keys: type, number, part and version.

Developer license

Key giving an SAP user development authorizations

Client

A unit within an SAP system that is independent with regard to action, organization, and data functions. It also has separate master records in a table within the SAP system

Naming convention

Agreement regarding name assignment for development purposes, for example all developments in a system should be given a prefix of X, Y, or Z as these prefixes have been reserved for customers by SAP.

Namespace

Protected namespaces can be reserved upon request by SAP. The namespace for SEAL Systems is /sea1/, /sea1c/ (for customer development) or /dvsrepro/ (old).

Transaction

Means of executing programs

Transaction code

Identifier naming a →transaction in the SAP system

Transport

Exporting/importing data between SAP systems

Abbreviations

| | |
|----------|---|
| ABAP | Advanced Business Application Programming (SAP system programming language) |
| DPF® | Digital Process Factory® from SEAL Systems |
| DMS | Document management system |
| FTP | File Transfer Protocol |
| OSS | Online Support Service |
| PDF | Adobe Portable Document Format |
| PDF/A | Adobe Portable Document Format (PDF/A norm) |
| PLM | Product Lifecycle Management |
| PLOSSYS® | Product family from SEAL Systems |
| RFC | Remote Function Call |

Keywords

Symbols

/seal/bas_cr142 201

A

ABAP 220
ABAP_DEBUG 55, 146, 191
Action 11
ACTIVE 193
Aktivierungsart 32
ASCS 155
ASHOST 135, 163

B

Benutzername 199

C

CAD_CHECKOUT_DLL 56
CadDialogNetAddress 125
cadrfc.ini 114
CadRfcClient 122
CadRfcDestination 124
CadRfcLanguage 123
CadRfcPassword 120
CadRfcPasswordCoded 121
CadRfcUser 119
CLIENT 184
CODEPAGE 149, 179
convservdpfstart 45
convservstart 45
CPIC* 144, 178

D

DEST 133, 162
DESTINATIONS 194
dev_jco_rfc.log 59
dev_rfc* 144, 178
DISPLAY 125
DMS 220
DPF® 220
dvsstart 45
dvsviewserverstart 45

F

filecheckstart 45
FTP 220

G

Gateway-Host 30, 53
Gateway-Service 30, 53
GROUP 140, 168

GWHOST 141, 169
GWSERV 142, 170

H

HOSTNAME 125

J

jco_rfc*.trc 144, 178
jco_rfcPID_UUID.trc 59
jrfcserverstart 45

K

Kommunikationsart mit dem Zielsystem 33
Kurzbeschreibung 202

L

LANG 185
LCHECK 189
Logon
 Benutzer 119, 182
 Passwort 183
 unverschlüsselt 120

M

ModuleGlobal 11
ModuleSelect 11
MSHOST 137, 165
MSSERV 138, 166
MYSAPSSO2 187

N

NO_COMPRESSION 180

O

oms_server 117
omscli 117
OSS 220
OTFCODEPAGE 195

P

PARA_DDEST 202
PARA_GWHSB 202
PARA_GWHST 202
PARA_UCORR 202
Parameter-Id 201
Parameterwert 202
PASSWD 183
PDF 220
PDF/A 220
Pfadpräfx 79

PLM 220
PLOSSYS® 220
plsstart 45
PROGID 195
Programm ID 32
proxyinfo 34

R

R3NAME 139, 167
reginfo 34
RFC 220
RFC_TRACE 55, 144
rfcserver.cfg 192
rfcserverstart 45
RLIGATE 195, 196
rlistsap 117
rswf_test_http 102

S

sap_conn_checker 128
sapcli 117
sapftp 21
sapftp.dll 56
SAPGUILandscape.xml 128
saphttp 21
saphttp.dll 56
sapnwrfc.ini 157
saprfc.ini 126
SAPROUTER 143, 172
SEAL_TRACE 145
sealencrypt 121
secinfo 34
Servicenummer 79
smicm 103
SNC_LIB 173
SNC_MODE 150, 174
SNC_MYNAME 151, 175
SNC_PARTNERNAME 152, 176
SNC_QOP 153, 177
SNC_SSO 154, 186
SYSNR 136, 164
sysstart 45

T

TRACE 178
TYPE 134

U

UNICODE 21, 148
USE_GWHOST 201
USE_SAPGUI 119, 147, 190
USER 182

X

X509CERT 156, 188
XMS 196
XMX 196

Z

Zeichenbreite im Zielsystem 33
Zielmaschine 79

Index

A

- application server
 - determine host name, USE_GWHOST 57
 - load balancing 53

B

- basic authentication
 - activate
 - SAP 80
 - server 75

C

- check-out
 - error, determine host name 57
- client 219
- code page 149, 179
 - Conversion Server, explicit 33
 - RFC Server, explicit 33
- compression
 - deactivate for tables 180
- configuration
 - SAP
 - basic authentication, activate 80
 - SAP as consumer
 - Web service 94
 - SAP as provider
 - Web service 84
 - server 20
 - basic authentication, activate 75
 - PSE, create 74
 - configuration file
 - overview 18
 - Conversion Server 129
 - sm59
 - code page, explicit 33
 - non-Unicode 33
 - customizing 219
 - cv<xx>, cv<xx>n 219
 - cv04, cv04n 219

D

- debug
 - Web service request
 - SAP as provider 93
 - requirement 85, 95
- debugging
 - system functions 55
- developer license 219
- dialog user 119, 182

- directory
 - convention at the specification 8
 - repro list processing 195
- DLL variant
 - requirement 56
- DMS 219
- DMS Loader 129
- DMS Loader/ABAP 129
- DMS Repro
 - requirement USE_SAPGUI 147
- DMS Rlist 129
 - restriction - system/client-spec. logon 117
- DMS Scan 129
 - requirement USE_SAPGUI 147
- DMS View Server 129
- Document information record 219
- document management system 219
- document, see document information record

E

- error
 - debugging, activate 146, 191
 - proceeding, advisable 102
 - RFC destination
 - SAP gateway logging, activate 58
 - trace message activate 55
 - trace message, activate 59, 144, 178
 - starting the RFC server 45
 - system function, debugging 55
 - typical 104
 - typical problem 50
 - Web service
 - SAP as consumer
 - check 102
 - trace message
 - display 103
 - SAP as provider
 - debug request 93
 - record requests 92
 - trace message, activate 92

G

- gateway
 - central
 - configure 70
 - requirement 70
 - restriction 70
 - saprfc.ini, example 70
 - local/central 17
 - settings for load balancing 53

- H**
- HTTP connection
 - connection type 78
 - create 77
 - RFC destination 78
 - HTTPS
 - see SAP_BASECONF_SNC_TEC 17
- J**
- JRFC Server 129
 - configuration file 192
 - sm59
 - Unicode 33
 - JSAPcli 129
- L**
- language
 - at logon 123
 - on connection establishment, supported 123
 - load balancing
 - between application server 53
 - gateway options 53
 - log file
 - connection status, requirement 145
 - memory status, requirement 145
 - logon
 - client 122, 184
 - configuration 114
 - language 123
 - password
 - coded 121
 - requirement 119, 182
 - requirement - system/client-spec. user 117
 - restriction - system/client-spec. logon 117
 - system/client-spec. user 117
- M**
- memory
 - maximum 196
 - minimum at start 196
 - status log, requirement 145
 - message server
 - load balancing for RFC clients 17
 - requirement 21
 - SAProuter 134, 157
 - saprfc.ini, example 26
 - MTOM
 - requirement 101
- N**
- namespace 219
- naming convention 219
- O**
- OData service
 - activate 107
 - activate for application 109
 - OTF
 - length correction in ST commands 202
 - overview
 - configuration files 18
 - HTTP connection, create 77
 - RFC client/RFC server 129
 - RFC destination on SAP systems as of 4.7 29
- P**
- parallel processing 195
 - password
 - coded 121
 - path specification, convention 8
 - PDF
 - Icon zur einfachen Navigation aktivieren, ab Adobe Reader 10 9, 10
 - PDF Longlife Suite - SAP Integration 129
 - port
 - assign SAP system 28
 - PSE
 - create, server 74
- R**
- registration 45
 - registration, see logon
 - repro list processing
 - directory 195
 - requirement
 - cadrfc.ini 114
 - connection status, log 145
 - debug
 - Web service request
 - SAP as provider 85, 95
 - DLL variant 56
 - DMS Repro 147
 - DMS Scan 147
 - gateway
 - central 70
 - logon 119, 182
 - memory status, log 145
 - message server 21
 - SAProuter 134, 157
 - MTOM 101
 - SAP system, version 106
 - saprfc.ini 126
 - SAProuter

- message server 134, 157
 - system/client-spec. logon 117
 - Unicode - separate section in rfcserver.cfg 194
 - Web service
 - roles with authorizations 85, 95
- restriction
 - gateway
 - central 70
 - system/client-spec. logon 117
- RFC client 129
- RFC destination
 - allow
 - alternatives 34
 - prefix for secinfo/reginfo, specify 42
 - reginfo
 - 36
 - >= NW 7.45 36
 - secinfo
 - 38
 - >= NW 7.45 38
 - simulation mode 41
 - classic
 - SAP system data 126
 - configuration on SAP systems as of 4.7 29
 - connection type 30
 - data, overview 18
 - logon data 114
 - RFC connection 30
 - SAP gateway logging, activate 58
 - SAP NetWeaver RFC Library
 - SAP system data 157
 - security configuration 34
 - start 44
 - via ACTIVE section 46
 - via call parameters 47
 - static sapftp/saphttp destination, see static sapftp/saphttp destination
 - status log, requirement 145
 - test 48
 - trace message
 - activate 55, 59, 144, 178
 - type 129
- RFC Server 129
 - sm59
 - code page, explicit 33
 - non-Unicode 33
- RFC server 129
 - error during start 45
 - saprfc.ini, example, saprfc.ini
 - example
 - RFC server 25
- RFF client
 - saprfc.ini, example, saprfc.ini
 - example
 - RFC client 24
- S**
- SAP system data
 - configuration
 - RFC destination, classic 126
 - SAP NetWeaver RFC Library 157
 - identify 128
- SAPcli 129
- sapftp
 - activate trace message 60
- saphttp
 - activate trace message 60
- saprfc.ini
 - example
 - gateway, central 70
 - message server 26
- SAProuter
 - requirement
 - message server 134, 157
- server
 - configuration 20
- single sign-on (SSO)
 - activate 187
- SNC
 - activation sign 150, 174
 - library for SNC communication 173
 - name of the communication partner 152, 176
 - name of the program 175
 - name of the user 151
 - quality of protection 153, 177
 - see SAP_BASECONF_SNC_TEC 17
 - single sign-on (SSo)
 - deactivate 154, 186
- SSO
 - deactivate
 - SNC_SSO 154, 186
 - see SAP_BASECONF_SNC_TEC 17
 - static sapftp/saphttp destination
 - template, assign
 - RFC client 68
 - RFC server 69
 - template, copy 65
 - template, establish 62
 - system user 119, 182
- T**
- table

- compression, deactivate 180
- thread
 - maximum number 195
- timeout
 - Web service 104
- trace message
 - display
 - Web service
 - SAP as consumer
 - display 103
- transaction 219
- transaction code 219
- transport 219

U

- Unicode
 - code page 149
 - configuration 148
 - configuration for mixed operation 21
 - requirement - message server 21
 - requirement - separate section in rfcserver.cfg 194
- USE_GWHOST
 - parameter value, specify 201

V

- variable
 - Action 11
 - ModuleGlobal 11
 - ModuleSelect 11
- version
 - requirement, SAP system 106

W

- Web service
 - requirement
 - roles with authorizations 85, 95
 - SAP as consumer
 - ABAP proxy, select 97
 - check 102
 - configuration 94
 - large amounts of data, optimize transfer with MTOM 101
 - logical port, create 98
 - suppress message ID transfer 100
 - trace, display 103
 - SAP as provider
 - binding, create 88
 - configuration 84
 - debug request 93
 - requests, record 92
 - service, select 87

- trace, activate 92
- URL, determine 90
- timeout 104
- wrapper program
 - deactivate 22
 - sapftp/saphttp for mixed operation 21
 - wrapper program sapftp/saphttp for Unicode digital signature 211