

SAP Basis Configuration - Server

System description

1.4.2

2024-01-15

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 2001-2024

SEAL Systems AG Lohmühlweg 4 D-91341 Röttenbach Germany

Contents

	1	Intro	duction	7
			Conventions in this Documentation	8
			Activate the Retrace of your Viewing Path in PDF	9
			Variables in this Documentation	10
			Overview of Contents	11
Desc	rir	otion		13
	2	Over	view - Data for RFC Connection	15
	3	RFC	Destination - Configuration	17
	0	3.1	BEC Destination - Configuration on Server	18
		0.1	Unicode SAP System - Transfer with sapftp/saphttp	19
			saprfc.ini - RFC Client - Example	.21
			saprfc.ini - RFC Server - Example	.22
			saprfc.ini - Message Server - Example	23
		3.2	Establish the RFC Destination on the SAP System	24
			RFC Destination - Basis Data	25
			RFC Destination - Technical Settings	27
			RFC Destination - Unicode Settings	28
		3.3	Security Configuration for RFC and SAP Destinations	29
			Configure Security for Incoming Connections - reginfo	31
			Configure Security for Outgoing Connections - secinfo	33
			Security Configuration - Important Hints	35
			Activate Simulation Mode for Security Configuration	36
			Specify Prefix for Generic RFC Destinations	37
			Security Configuration - Background Knowledge	38
		3.4	Start and Test RFC Destination	39
			Start the RFC Destinations on the Server	40
			Determine RFC Destinations to be Started via the [ACTIVE] Section .	41
			Determine RFC Destinations to be Started via Call Parameters	42
			Test the RFC Destination on the SAP System	43
		3.5	Troubleshooting - RFC Destination	45
			saphttp/sapftp Start - Background Knowledge	47
			Hints for the Load Balancing	48
			Additional Messages and Debugging	50
			Activate DLL Version of sapftp/saphttp in Case of Bottlenecks	51
			Define the USE_GWHOST Parameter	52
			Activate the SAP Gateway Logging	53
			Activate RFC Trace	54
	_	.	Activate Trace Functions for sapftp/saphttp	55
	4	Statio	c RFC Destinations for SNC Support	56
			Establish Templates for sapttp/saphttp (sm59)	57
			Create Multiple sapttp/saphttp Destinations	60
			RFC Client - Assign Static sapitp/sapittp Destination	63
			RFC Server - Assign Static sapttp/saphttp Destination	64 СГ
	-		Support Central SAP Gateway	65 67
	5		Connection - Configuration	b/
		5.1	HITE Connection - Configuration on Server	60
			Create YSE	69 70
			ACTIVATE LOGON WITH BASIC AUTHENTICATION and SSL	70

	5.2	Create an HTTP Connection on the SAP System	72
		HTTP Connection - Basis Data	73
		HTTP Connection - Technical Settings	74
		HTTP Connection - Logon & Security	75
		HTTP Connection - Special Options	
6	Integ	gration via Web Service - SAP as Provider	79
	6.1	Required Authorizations	80
	6.2	Configuration on the Provider System (SAP)	
		Select the Service	
		Create the Binding on the Provider System	
		Determine URL for WSDL Access	85
	6.3	Troubleshooting - Analysis of Web Service Requests	
		Record and Display Web Service Requests	87
		Debug Web Service Requests	
7	Integ	gration via Web Service - SAP as Consumer	
	7.1	Required Authorizations	
	7.2	Configuration on the Consumer System (SAP)	91
		Select the ABAP Proxy	
		Create a Logical Port	
		Suppress the Message ID Transfer	
		Transfer of Large Amounts of Data	
	7.3	Advisable Behavior in the Case of Error	97
	7.4	Troubleshooting	
Refere	ence .		101
8	Conf	iguration Files - Reference	103
8	Conf 8.1	iguration Files - Reference cadrfc.ini - Logon Information	103 104
8	Conf 8.1	iguration Files - Reference cadrfc.ini - Logon Information System-/Client-Specific Logon Data	 103 104 107
8	Conf 8.1	iguration Files - Reference cadrfc.ini - Logon Information System-/Client-Specific Logon Data CadRfcUser Parameter	103 104 107 109
8	Conf 8.1	iguration Files - Reference cadrfc.ini - Logon Information System-/Client-Specific Logon Data CadRfcUser Parameter CadRfcPassword Parameter	103 104 107 109 109
8	Conf 8.1	iguration Files - Reference cadrfc.ini - Logon Information System-/Client-Specific Logon Data CadRfcUser Parameter CadRfcPassword Parameter CadRfcPasswordCoded Parameter	103 104 107 109 110 111
8	Conf 8.1	iguration Files - Reference cadrfc.ini - Logon Information System-/Client-Specific Logon Data CadRfcUser Parameter CadRfcPassword Parameter CadRfcPasswordCoded Parameter CadRfcClient Parameter	103 104 107 109 110 111 111 112
8	Conf 8.1	iguration Files - Reference cadrfc.ini - Logon Information System-/Client-Specific Logon Data CadRfcUser Parameter CadRfcPassword Parameter CadRfcPasswordCoded Parameter CadRfcClient Parameter CadRfcClient Parameter CadRfcLanguage Parameter	103 104 107 109 110 111 111 112 113
8	Conf 8.1	iguration Files - Reference cadrfc.ini - Logon Information System-/Client-Specific Logon Data CadRfcUser Parameter CadRfcPassword Parameter CadRfcPasswordCoded Parameter CadRfcClient Parameter CadRfcClient Parameter CadRfcLanguage Parameter CadRfcDestination Parameter	103 104 107 109 110 111 111 112 113 114
8	Conf 8.1	iguration Files - Reference cadrfc.ini - Logon Information System-/Client-Specific Logon Data CadRfcUser Parameter CadRfcPassword Parameter CadRfcPasswordCoded Parameter CadRfcClient Parameter CadRfcClient Parameter CadRfcLanguage Parameter CadRfcDestination Parameter CadDialogNetAddress Parameter	103 104 107 109 110 111 112 113 114 115
8	Conf 8.1 8.2	iguration Files - Reference cadrfc.ini - Logon Information System-/Client-Specific Logon Data CadRfcUser Parameter CadRfcPassword Parameter CadRfcPasswordCoded Parameter CadRfcClient Parameter CadRfcClient Parameter CadRfcLanguage Parameter CadRfcDestination Parameter CadDialogNetAddress Parameter	103 104 107 109 110 111 112 113 114 115 116
8	Conf 8.1 8.2	iguration Files - Reference cadrfc.ini - Logon Information System-/Client-Specific Logon Data CadRfcUser Parameter CadRfcPassword Parameter CadRfcPasswordCoded Parameter CadRfcClient Parameter CadRfcClient Parameter CadRfcLanguage Parameter CadRfcDestination Parameter CadDialogNetAddress Parameter Saprfc.ini - Connection Data Determine System Data forsaprfc.ini	103 104 107 109 110 111 112 113 114 115 116 118
8	Conf 8.1 8.2	iguration Files - Reference cadrfc.ini - Logon Information System-/Client-Specific Logon Data CadRfcUser Parameter CadRfcPassword Parameter CadRfcPasswordCoded Parameter CadRfcClient Parameter CadRfcClient Parameter CadRfcLanguage Parameter CadRfcDestination Parameter CadDialogNetAddress Parameter Saprfc.ini - Connection Data Determine System Data forsaprfc.ini Types of RFC Destinations and Module Classification	103 104 107 109 110 111 112 113 114 115 118 119
8	Conf 8.1 8.2	iguration Files - Reference	103 104 107 109 110 111 112 113 114 115 116 118 119 120
8	Conf 8.1 8.2	iguration Files - Reference cadrfc.ini - Logon Information System-/Client-Specific Logon Data CadRfcUser Parameter CadRfcPassword Parameter CadRfcPasswordCoded Parameter CadRfcClient Parameter CadRfcClient Parameter CadRfcClient Parameter CadRfcLanguage Parameter CadRfcDestination Parameter CadDialogNetAddress Parameter Saprfc.ini - Connection Data Determine System Data forsaprfc.ini Types of RFC Destinations and Module Classification Parameter Overview DEST Parameter	103 104 107 109 110 111 112 113 114 115 116 118 119 120 123
8	Conf 8.1 8.2	iguration Files - Reference cadrfc.ini - Logon Information System-/Client-Specific Logon Data CadRfcUser Parameter CadRfcPassword Parameter CadRfcPasswordCoded Parameter CadRfcClient Parameter CadRfcClient Parameter CadRfcClient Parameter CadRfcClient Parameter CadRfcDestination Parameter CadDialogNetAddress Parameter Saprfc.ini - Connection Data Determine System Data forsaprfc.ini Types of RFC Destinations and Module Classification Parameter Overview DEST Parameter	103 104 107 109 110 111 112 113 114 115 116 118 119 120 123 124
8	Conf 8.1 8.2	iguration Files - Reference cadrfc.ini - Logon Information System-/Client-Specific Logon Data CadRfcUser Parameter CadRfcPassword Parameter CadRfcClient Parameter CadRfcClient Parameter CadRfcLanguage Parameter CadRfcDestination Parameter CadRfcDestination Parameter CadRfcDestination Parameter CadDialogNetAddress Parameter Saprfc.ini - Connection Data Determine System Data forsaprfc.ini Types of RFC Destinations and Module Classification Parameter Overview DEST Parameter ASHOST Parameter	103 104 107 109 110 111 112 113 114 115 116 118 119 120 123 124 125
8	Conf 8.1 8.2	iguration Files - Reference cadrfc.ini - Logon Information System-/Client-Specific Logon Data CadRfcUser Parameter CadRfcPassword Parameter CadRfcPasswordCoded Parameter CadRfcClient Parameter CadRfcClient Parameter CadRfcClient Parameter CadRfcDestination Parameter CadDialogNetAddress Parameter Saprfc.ini - Connection Data Determine System Data forsaprfc.ini Types of RFC Destinations and Module Classification Parameter Overview DEST Parameter ASHOST Parameter SySNR Parameter	103 104 107 109 110 111 112 113 114 115 116 118 119 120 123 124 125 126
8	Conf 8.1 8.2	iguration Files - Reference cadrfc.ini - Logon Information System-/Client-Specific Logon Data CadRfcUser Parameter CadRfcPassword Parameter CadRfcPassword Coded Parameter CadRfcClient Parameter CadRfcLanguage Parameter CadRfcDestination Parameter CadRfcDestination Parameter CadDialogNetAddress Parameter Saprfc.ini - Connection Data Determine System Data forsaprfc.ini Types of RFC Destinations and Module Classification Parameter Overview DEST Parameter ASHOST Parameter SYSNR Parameter MSHOST Parameter	103 104 107 109 110 111 112 113 114 115 116 118 119 120 123 124 125 126 127
8	Conf 8.1 8.2	iguration Files - Reference cadrfc.ini - Logon Information System-/Client-Specific Logon Data CadRfcUser Parameter CadRfcPassword Parameter CadRfcPasswordCoded Parameter CadRfcClient Parameter CadRfcClient Parameter CadRfcClient Parameter CadRfcClient Parameter CadRfcDestination Parameter CadDialogNetAddress Parameter Saprfc.ini - Connection Data Determine System Data forsaprfc.ini Types of RFC Destinations and Module Classification Parameter Overview DEST Parameter ASHOST Parameter SYSNR Parameter MSHOST Parameter Parameter R3NAME	103 104 107 109 110 111 112 113 114 115 116 118 119 120 123 124 125 126 127 128
8	Conf 8.1 8.2	iguration Files - Reference cadrfc.ini - Logon Information System-/Client-Specific Logon Data CadRfcUser Parameter CadRfcPassword Parameter CadRfcPasswordCoded Parameter CadRfcClient Parameter CadRfcLanguage Parameter CadRfcDestination Parameter CadDialogNetAddress Parameter Saprfc.ini - Connection Data Determine System Data forsaprfc.ini Types of RFC Destinations and Module Classification Parameter Overview DEST Parameter ASHOST Parameter SYSNR Parameter MSHOST Parameter Parameter R3NAME GROUP Parameter Parameter	103 104 107 109 110 111 112 113 114 115 116 118 119 120 123 124 125 126 127 128 129
8	Conf 8.1 8.2	iguration Files - Reference	103 104 107 109 110 111 112 113 114 115 116 118 119 120 123 124 125 126 127 128 129 130
8	Conf 8.1 8.2	iguration Files - Reference	103 104 107 109 110 111 112 113 114 115 116 118 119 120 123 124 125 126 127 128 129 130 131
8	Conf 8.1 8.2	iguration Files - Reference	103 104 107 109 110 111 112 113 114 115 116 118 119 120 123 124 125 126 127 128 129 130 131 132
8	Conf 8.1 8.2	iguration Files - Reference cadrfc.ini - Logon Information System-/Client-Specific Logon Data CadRfcUser Parameter CadRfcPassword Parameter CadRfcPasswordCoded Parameter CadRfcClient Parameter CadRfcLanguage Parameter CadRfcDestination Parameter CadRfcDestination Parameter CadDialogNetAddress Parameter CadDialogNetAddress Parameter Saprfc.ini - Connection Data Determine System Data forsaprfc.ini Types of RFC Destinations and Module Classification Parameter Overview DEST Parameter TYPE Parameter ASHOST Parameter SYSNR Parameter Parameter R3NAME GROUP Parameter GWHOST Parameter GWHOST Parameter GWHOST Parameter Parameter SAPROUTER RFC_TRACE Parameter	103 104 107 109 110 111 112 113 114 115 116 118 119 120 123 124 125 126 127 128 129 130 131 132 133

	ABAP DEBUG Parameter	135
	USE SAPGUI Parameter	136
	UNICODE Parameter	137
	CODEPAGE Parameter	138
	SNC MODE Parameter	139
	SNC MYNAME Parameter	140
	SNC PARTNERNAME Parameter	141
	SNC QOP Parameter	142
	SNC SSO Parameter	143
	ASCS Parameter	144
	X509CERT Parameter	145
8.3 rfcserver.	cfg	146
	[ACTIVE] Section	147
	[SECTIONNAME] Section	148
9 Configuration T	ables - Reference	151
	/seal/bas_cr113 - Static Destination for RFC Server	152
	/seal/bas_cr114 '- Static Destination for RFC Client	153
	/seal/bas_cr142 - Define Parameters	155
10 Changes		157
	Changes with Release 1.4.2	158
	Changes with Release 1.4.1	159
	Changes with Release 1.4.0	160
	Changes with Release 1.3.5	161
	Changes with Release 1.3.3	162
	Changes with Release 1.3.2	163
	Changes with Release 1.3.1	164
	Changes with Release 1.3.0	165
	Changes with Release 1.2.8	166
	Changes with Release 1.2.6	167
		160
	Changes with Release 1.2.5	100
	Changes with Release 1.2.5 Changes with Release 1.2.4	
Bibliography	Changes with Release 1.2.5 Changes with Release 1.2.4	168 169 170
Bibliography Terminology	Changes with Release 1.2.5 Changes with Release 1.2.4	
Bibliography Terminology Abbreviations	Changes with Release 1.2.5 Changes with Release 1.2.4	168 169 170 171 172
Bibliography Terminology Abbreviations Keywords	Changes with Release 1.2.5 Changes with Release 1.2.4	168 169 170 171 172 173

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 add- ons 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 - connec- tion external sys- tem/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:RFC destination	alternatives	
HTTP connection, for example in combination with a REST interface		
 Web service with the SAP system as provider or consumer 		
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 and about the HTTPS support in [SAP_BASECONF_SNC_TEC] and [SAP_BASEC-ONF_HTTPS_TEC]	😳 reference	
This chapter deals with the following topics:	in this chapter	
\rightarrow Conventions in this Documentation, Page 8		
ightarrow Activate the Retrace of your Viewing Path in PDF, Page 9		
ightarrow Variables in this Documentation, Page 10		

 \rightarrow Overview of Contents, Page 11

Conventions in this Documentation

path specifica-
tionThe path information given in this documentation is relative to the installation
directory of PLOSSYS netdome. 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
Consolas italic	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 description you viewed earlier. This makes reading easier and helps to keep the central theme.

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

Step	Action
1	 Activate the following options via the menu: View - Show/Hide - Toolbar Items - Page Navigation Show Tools Previous View: Activate Next View: Activate
	ew igation iga
	s <u>B</u> ar Ctrl+E S <u>h</u> ow All Page Navigation Tools Ilbars F8 <u>R</u> eset Page Navigation Tools olbars Alt+F8

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



meaning of Mod- uLeGLobal	 The variable <i>ModuLeGLobaL</i> represents the general module short cuts: pls dvs
meaning of <i>Mod-</i> uLeSeLect	<pre>The variable ModuLeSeLect represents the individual modules: convserv convservdpf dvsviewserv filecheck rfcserver rfcserver</pre>
meaning of Ac- tion	The variable Action represents the actions: start status stop

Variables in this Documentation

Overview of Contents

This documentation has two parts: a description and a reference. The first part structure 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.

The description deals with the following topics:

description

 \rightarrow Overview - Data for RFC Connection, Page 15

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

 \rightarrow RFC Destination - Configuration, Page 17

This chapter describes the configuration settings required for communication via RFC destinations.

 \rightarrow Static RFC Destinations for SNC Support, Page 56

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:

- 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

```
    RFC server:
DPF
    DMS Loader/ABAP
    XSA
    (DMS View Server is not affected))
```

→ HTTP Connection - Configuration, Page 67

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

 \rightarrow Integration via Web Service - SAP as Provider, Page 79

This chapter describes the establishing of an integration via Web service, if SAP serves as provider.

 \rightarrow Integration via Web Service - SAP as Consumer, Page 89

This chapter describes the establishing of an integration via Web service, if SAP serves as consumer.

The reference contains the following chapters:

 \rightarrow Configuration Files - Reference, Page 103

reference

Overview of Contents, Continuation

	This chapter explains the configuration files which are evaluated to establish a connection between the OM server and the SAP system in case of communica-tion via RFC destination.
	\rightarrow Configuration Tables - Reference, Page 151
	This chapter contains an alphabetically sorted list of all configuration tables relevant for the basis configuration in SAP.
changes	\rightarrow Changes, Page 157
	This chapter describes the most important changes for each released module version.
lists	For an easier overview, a bibliography, terminology list, abbreviation list, and index are included at the end of the documentation.



Overview - Data for RFC Connection 2

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

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

OM server

SAP	sy:	stem
-----	-----	------

saprfc.ini
System data of the SAP systems
cadrfc.ini
Information to logon on the SAP system
jrfcserver.cfg
Start of the SAP systems with progid for smss

SAP system	
RFC destination with ROGID	

Overview - Data for RFC Connection, Continuation

The following important correlations exist between these settings:

be-tween the data 🔏 [fcserver.cfg - (U:\s7\knott.20070611tstok.roett221.sapstartstop.winnt5\serv... 💻 🗖 🗙 Datei Editieren Werkzeuge Syntax Puffer Ansicht Hilfe "@(#) \$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 with SAP systems for which the RFC SECTION = DEU destinations are to be started *SECTION 7 TEST PROD SECTION : Kaprfc.ini - (U:\s7\knott.20070611tstok ! Development system Datei Editieren Werkzeuge Syntax Puffer Ansicht Hilfe DEST=X46RFC [DEV] TYPE-R DESTINATIONS = "X40KFC" Section with the SAP PROGID-SEAL-CONNC-001 GWHOST=sap7 system data GWSERU-sapgw00 PROGID=SEAL-CONNC-002 RFC_TRACE=0 PROGID-SEAL-CONNC-003 PROGID=SEAL-CONNC-004 UNICODE-0 DEST-T47RFC ! Test system TYPE=R PROGID-Dumny [TEST] GWHOST=sap9 DESTINATIONS = "T47RFC" GWSERU-sapgv00 PROGID-SEAL-CONNC-681 RFC TRACE=0 Logon & Security Administration echnical Settings MDMP & Unicode Special Activation Type O Start on Application Server Registered Server Program O Start on Explicit Host Transaction sm59 Start on Front-End Work Station Registered Server Program Program ID SEAL-CONNC-001

coherence

3 RFC Destination - Configuration

This chapter describes the configuration settings required for communication introduction via RFC destinations.

Alternatively, the following transfer types are available:alternative→ HTTP Connection - Configuration, Page 67in this chapterThis chapter deals with the following topics:in this chapter→ RFC Destination - Configuration on Server, Page 18>→ Establish the RFC Destination on the SAP System, Page 24>→ Security Configuration for RFC and SAP Destinations, Page 29>→ Start and Test RFC Destination, Page 39>→ Troubleshooting - RFC Destination, Page 45>

 \rightarrow Static RFC Destinations for SNC Support, Page 56

Related topics

3.1 **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 pro- The co

The configuration on the external server includes the following steps:

ceed-ing

Step	Description
1	Define the system data of the SAP systems to which the RFC desti-nations are to be established in
	saprfc.ini
	→ saprfc.ini - Connection Data, Page 116
2	Define the RFC destinations to be started in
	rfcserver.cfg
	\rightarrow rfcserver.cfg, Page 146
3	Specify the information for the first-time logon in:
	cadrfc.ini
	→ cadrfc.ini - Logon Information, Page 104
	🖉 Hint:
	You can modify the cadrfc.ini file on the installation directory. Afterwards you can distribute this file to the required directories.

in this chapter This chapter deals with the following topics:

 \rightarrow Unicode SAP System - Transfer with sapftp/saphttp, Page 19

- \rightarrow saprfc.ini RFC Client Example, Page 21
- → saprfc.ini RFC Server Example, Page 22
- → saprfc.ini Message Server Example, Page 23

Unicode SAP System - Transfer with sapftp/saphttp

SAP provides different versions of the programs sapftp and saphttp for the data exchange with Unicode SAP systems and non-Unicode SAP systems. The correct variant is started via the sapftp/saphttp wrapper program from SEAL Systems	Description
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.	requirement - saprfc.ini
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.	requirement - message server
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. In this case, you may skip this chapter.	Unicode SAP sys- tems only
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!	requirement - wrapper pro- gram

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: saphttp Version 1.0.0.3 of 2015-07-06 - \$Revision: 1.11 (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.ini

Unicode SAP System - Transfer with sapftp/saphttp,

Continuation

Step	Action
3	Replace the program if the display looks different, for example: SAPFTP Non-Unicode
	<pre>@(#) \$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</pre>
	inifilename =
	x¿Ì⊡, ¹.ini
	SAP release: 721 SAP release no: 7210

requirement - All required DLLs must exist, for instance under Windows in the directory tools\bin_xxx icuuc.dll, librfc32u.dll, libsapu16vc.dll, libsapucum.dll, sapnwrfc.dll.

effect and pro-
cessThe value of UNICODE defined in saprfc.ini is read when starting the RFC desti-
nation and the correct 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.

saprfc.ini - RFC Client - Example

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

 \rightarrow saprfc.ini - Connection Data, Page 116

related top-

ics



21

<pre> example - without SNC </pre>	This example shows items in saprfc.ini for a RFC server destination without SNC:
	DEST=W74RFC
	TYPE=R
	GWHOST=roesap005.sealsystems.local
	GWSERV=sapgw01
	RFC_TRACE=0
	SEAL_TRACE=0
	UNICODE=1
	SNC_MODE=0
SAP router	An SAP router can also be specified with :
	GWHOST=/H/saprouter.com/H/roegw003.sealsystems.local
Q example -	This example shows items in saprfc.ini for a RFC server destination with SNC:
with SNC	DEST=W74RFC
	TYPE=R
	GWHOST=roesap005.sealsystems.local
	GWSERV=sapgw01
	RFC_TRACE=0
	SEAL_TRACE=0
	UNICODE=1
	SNC_MODE=1
	<pre>SNC_MYNAME=p:CN=SEALRFC,OU=SEALSAP,O=SEAL,C=DE</pre>
	SNC_QOP=8

saprfc.ini - Message Server - Example

	\bigcirc
This example shows items in saprfc.ini for a connection via message server without SNC:	<pre> example - without SNC</pre>
DEST=W74	
TYPE=B	
MSHOST=roesap005.sealsystems.local	
R3NAME=W74	
GROUP=PUBLIC	
RFC_TRACE=0	
ABAP_DEBUG=0	
USE_SAPGUI=1	
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 complexing for a connection via message server	Qavampla
with SNC:	with SNC
with SNC: DEST=W74	with SNC
with SNC: DEST=W74 TYPE=B	with SNC
with SNC: DEST=W74 TYPE=B MSHOST=roesap005.sealsystems.local	with SNC
with SNC: DEST=W74 TYPE=B MSHOST=roesap005.sealsystems.local R3NAME=W74	with SNC
with SNC: DEST=W74 TYPE=B MSHOST=roesap005.sealsystems.local R3NAME=W74 GROUP=PUBLIC	with SNC
with SNC: DEST=W74 TYPE=B MSHOST=roesap005.sealsystems.local R3NAME=W74 GROUP=PUBLIC RFC_TRACE=0	with SNC
<pre>with SNC: DEST=W74 TYPE=B MSHOST=roesap005.sealsystems.local R3NAME=W74 GROUP=PUBLIC RFC_TRACE=0 ABAP_DEBUG=0</pre>	with SNC
<pre>with SNC: DEST=W74 TYPE=B MSHOST=roesap005.sealsystems.local R3NAME=W74 GROUP=PUBLIC RFC_TRACE=0 ABAP_DEBUG=0 USE_SAPGUI=1</pre>	with SNC
<pre>with SNC: DEST=W74 TYPE=B MSHOST=roesap005.sealsystems.local R3NAME=W74 GROUP=PUBLIC RFC_TRACE=0 ABAP_DEBUG=0 USE_SAPGUI=1 UNICODE=1</pre>	with SNC
<pre>with SNC: DEST=W74 TYPE=B MSHOST=roesap005.sealsystems.local R3NAME=W74 GROUP=PUBLIC RFC_TRACE=0 ABAP_DEBUG=0 USE_SAPGUI=1 UNICODE=1 SNC_MODE=1</pre>	with SNC
<pre>with SNC: DEST=W74 TYPE=B MSHOST=roesap005.sealsystems.local 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</pre>	with SNC
<pre>This example shows items in sapirtC.Init for a connection via message server with SNC: DEST=W74 TYPE=B MSHOST=roesap005.sealsystems.local R3NAME=W74 GROUP=PUBLIC RFC_TRACE=0 ABAP_DEBUG=0 USE_SAPGUI=1 UNICODE=1 SNC_MODE=1 SNC_MODE=1 SNC_MYNAME=p:CN=SEALRFC,OU=SEALSAP,O=SEAL,C=DE SNC_QOP=3</pre>	with SNC

 \rightarrow saprfc.ini - Connection Data, Page 116



3.2 Establish the RFC Destination on the SAP System

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

alternativeAlternatively, the following transfer types are available: \rightarrow HTTP Connection - Configuration, Page 67

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

Step	Action
1	Start the sm59 transaction.
2	Click Create:
	RFC Destination
	Connection Test 🛯 🎾
	RFC Destination
	Connection Type New Entry Description
	Description
	Description 1
	Description 2
	Description 3
	Administration Technical Settings Logon & Security MDMP &
	Gateway Options
3	\rightarrow RFC Destination - Basis Data, Page 25
4	\rightarrow RFC Destination - Technical Settings, Page 27
5	\rightarrow RFC Destination - Unicode Settings, Page 28
6	Save the settings.

RFC Destination - Basis Data

Enter the following basis data:

tings **Parameters** Value **RFC** Destination Unique identifier on the SAP system Example: SEAL-CONNC-001 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. 🥖 Hint - exception: When using Conversion Server, a different name must be specified in order to implement load balancing/ reliability, see scenario 1 in: \rightarrow Hints for the Load Balancing, Page 48 🥖 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. Т Connection Type Description Describing text Gateway Options -GWHOST as in saprfc.ini Gateway Host 🥖 Hint - exception: When using Conversion Server, this value may be empty in order to implement load balancing/reliability, see scenario 1 in: \rightarrow Hints for the Load Balancing, Page 48 Gateway Options -GWSERVas in saprfc.ini Gateway Service 🥖 Hint - exception: When using Conversion Server, this value may be empty in order to implement load balancing/reliability, see scenario 1 in: \rightarrow Hints for the Load Balancing, Page 48

necessary set-

RFC Destination - Basis Data, Continuation



RFC Destina	tion SEAL-CONNC-001
Connection Test	Unicode Test 🛛 🎾
RFC Destination Connection Type	SEAL-CONNC-001 T TCP/IP Connection
Description	
Description 1	SEAL-CONNC-001

RFC Destination - Technical Settings

Switch to the Technical settings tab.

Enter the following technical settings:

Parameter	Value
Activation Type	Registered server program
Registered Server Program - Program ID	PROGID identifier in the configuration file like rfcserver.cfg on the SEAL server Image: Construction of the server Image: Construction of
	As of EhP7 or kernel 721, destinations are no longer accepted automatically but have to be allowed manually in reginfo/secinfo:
	 → Security Configuration for RFC and SAP Destinations, Page 29 ✓ Hint - naming convention: The identifier can include letters, numbers, '+', '.', '-', and '_' characters!

		(🔍 example
Administration	Technical Settings	Logon & Security MDMP & Unicode Specia	il
Activation Type			
O Start on Appli	cation Server	Registered Server Program	
🔵 Start on Explic	cit Host		
OStart on Front	-End Work Station		
Registered Serve	er Program		
Program ID	SEAL-CONNC-001		

requirement

necessary set-

tings

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) necessary set-Enter the following options: tings Parameter Value as of release 6.40: For JRFC Server: • Unicode Communication Administration Technical Settings Logon & Security Type with Target System Communication Type with Target System Unicode up to release 4.7: Non-Unicode Character Width Codepage from client-side logon language (at runtime) in Target System 1100 O Explicit Codepage: For RFC Server and Conversion Server: • Non-Unicode Explicit Code Page (as of ECC 6.0) Technical Settings Logon & Security Administration Communication Type with Target System OUnicode Non-Unicode Codepage from client-side logon language (at runtime) • Explicit Codepage: 1100 Caution - Conversion Server: The ConvUtil and ConvServSamp programs on the server are not Unicode-enabled! Therefore, Non-Unicode has to be activated!

3.3 Security Configuration for RFC and SAP Destinations

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

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)



The following alternatives are provided at the security configuration:

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

This chapter deals with the following topics:

alternatives

in this chapter

Security Configuration for RFC and SAP Destina-

tions, Continuation

- \rightarrow Configure Security for Incoming Connections reginfo, Page 31
- ightarrow Configure Security for Outgoing Connections secinfo, Page 33
- → Security Configuration Important Hints, Page 35
- \rightarrow Activate Simulation Mode for Security Configuration, Page 36
- \rightarrow Specify Prefix for Generic RFC Destinations, Page 37
- \rightarrow Security Configuration Background Knowledge, Page 38

Configure Security for Incoming Connections reginfo

This is how you specify the accepted registered programs on the SAP gatewayinstructions ->=in reginfo for SAP NetWeaver Application Server 7.45 or newer:NW 7.45

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="" seal="" server="" the=""> CANCEL=*</ip>
	A Caution - important hints:
	Note the following hints when you enter the security configura- tion:
	\rightarrow Security Configuration - Important Hints, Page 35

This is how you specify the accepted registered programs on the SAP gatewayinstructions - <</th>in reginfo for SAP NetWeaver Application Server older than 7.45:NW 7.45

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

31

Configure Security for Incoming Connections -

reginfo, Continuation

Step	Action
3	If the file does not exist, you can create it via:
	Goto
	→Expert Functions
	→External Security
	→Create (reginfo)
	Select the destinations, which are to be accepted, and save them via Save Selected Entries in File.
	Create ACL File for Registered Server Programs
	🕈 Save Selected Entries in File 🐼 Display ACL File
	RFC Destination GW:LOCAL GW:INTERNAL
4	Enter the following lines in the usr\sap\ <i>system</i> \dveb- mgs00\data\reginfo.dat file:
	P TP=* HOST= <ip address="" of="" seal="" server="" the=""> CANCEL=* ACCESS=*</ip>
	Caution - important hints:
	Note the following hints when you enter the security configura- tion:
	ightarrow Security Configuration - Important Hints, Page 35

Configure Security for Outgoing Connections - secinfo

This is how you specify the accepted programs to be started on the SAP gatewayinstructions ->=in secinfo for SAP NetWeaver Application Server 7.45 or newer:NW 7.45

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="" seal="" server="" the=""></ip>
	HOST= <ip address="" of="" seal="" server="" the=""></ip>
	tion:
	ightarrow Security Configuration - Important Hints, Page 35

This is how you specify the accepted programs to be started on the SAP gatewayinstructions - <</th>in secinfo for SAP NetWeaver Application Server older than 7.45:NW 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	If the file does not exist, you can create it via:
	Goto
	→Expert Functions
	→External Security
	→Create (secinfo)
	Select the destinations, which are to be accepted, and save them via Save Selected Entries in File.
	Create ACL File at Start of Server Programs
	T Save Selected Entries in File
	RFC Destination IP Address (IPv4/IPv6) Program Name GW:LOCAL local * GW:INTERNAL internal *
4	Enter the following lines in the usr\sap\ <i>system</i> \dveb- mgs00\data\secinfo.dat file:
	<pre>P TP=* USER=* USER-HOST=<ip address="" of="" seal="" server="" the=""> HOST=<ip address="" of="" seal="" server="" the=""></ip></ip></pre>
	Note the following hints when you enter the security configura- tion:
	ightarrow Security Configuration - Important Hints, Page 35

Security Configuration - Important Hints

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 37

- 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.

 \rightarrow Activate Simulation Mode for Security Configuration, Page 36 Deactivate the simulation mode as soon as you are sure that the security settings are correct. note

Activate Simulation Mode for Security Configuration

purpose 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.

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.

instructions

This is how you activate the simulation mode:

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: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 $Edit \rightarrow Activate$.
5	Deactivate the simulation mode as soon as you are sure that the security configuration is correct.

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

The server starts generic RFC destinations (sapftp and saphttp) at the check-description 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.

These steps are only required as of EhP7 or kernel 721, if you do not want to required if allow generally all destinations with * in secinfo/reginfo but you want to restrict this setting as much as possible.

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

Step	Action		
1	Start the se16n transaction with the sdokprof table.		
2	<pre>Enter: Key: RFC_PREFIX Secondary Key: Empty or SAPFTP,SAPHTTP Contents:SEAL_ (example) Example:</pre>		
	KeyUserClientSecondary keyContentsRFC_PREFIX800SEAL_Image: Secondary keySEAL_Image: Secondary keySecondary keyImage: Secondary keySeconda		

Security Configuration - Background Knowledge

tips & tricks	 The smgw transaction provides following useful functions additionally: 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
background knowledge - SAP notes	Important SAP notes regarding the security configuration on https://support.sap.com/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) 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
background knowledge - SAP WIKI	 SAP WIKI items regarding the security configuration on https://wiki.scn.sap.com/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+Interface+and+ACL+control

3.4 Start and Test RFC Destination

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

You can use the following alternatives as start script:

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

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

Level	Processing
1	ightarrow Start the RFC Destinations on the Server, Page 40
2	The start script determines the RFC destinations which are to be started:
	\rightarrow Determine RFC Destinations to be Started via the [ACTIVE] Section, Page 41
	\rightarrow Determine RFC Destinations to be Started via Call Parameters, Page 42
3	The start script determines the SAP system data for the RFC desti- nations which are to be started in saprfc.ini (DESTINATIONS in <i>ModuLeSeLect</i> .cfg like rfcserver.cfg and DEST in saprfc.ini).
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 sm59 transaction:
	ightarrow Test the RFC Destination on the SAP System, Page 43

This chapter deals with the following topics:

in this chapter

 \rightarrow Start the RFC Destinations on the Server, Page 40

- \rightarrow Determine RFC Destinations to be Started via the [ACTIVE] Section, Page 41
- \rightarrow Determine RFC Destinations to be Started via Call Parameters, Page 42
- \rightarrow Test the RFC Destination on the SAP System, Page 43

start script

start on the serv- er	 You can start the RFC destinations on the server as follows: plsstart or sysstart PLOSSYS netdome Starts PLOSSYS netdome and all required RFC destinations dvsstart or sysstart SAP Starts all required RFC destinations rfcserverstart, jrfcserverstart, convservstart, convservdpfstart, filecheckstart, dvsviewserverstart Starts only the required RFC connections from the corresponding configu- ration file, for example rfcserver.cfg
status check on the server	 You can check the status of the RFC destinations on the server as follows: 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, jrfcserverstatus, convserverstatus, convservdpfstatus, filecheckstatus, dvsviewserverstatus Shows the status of the required RFC connections from the corresponding
problems at start	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.

Start the RFC Destinations on the Server

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

The [ACTIVE] section in *ModuLeSeLect*.cfg like rfcserver.cfg contains the format 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:

- SECTION=SectionName If a section is assigned to the SECTION keyword it is considered for all servers.
- HostName=SectionName
 If a section is assigned to a server it is considered only for this server.

 The [ACTIVE] section is evaluated by all start scripts.
 evaluated by

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

 • The SAP_START_SYSTEM environment variable is specified.
 exception

 • Section names are specified as parameters at the program start.
 exception

The RFC destinations of the DEV, TEST and PROD sections are always to be started independently of the current server:

rfcserver.cfg: [ACTIVE] SECTION=DEV SECTION=TEST SECTION=PROD

The following scenario is to be emulated:

- \checkmark example 2
- 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-EXTand TEST sections are to be started only if SEALSAP2 is the current server.

rfcserver.cfg: [ACTIVE] SECTION=DEV SEALSAP1=DEV-EXT SEALSAP2=DEV-EXT SEALSAP2=TEST SEALSAP1=PROD example 1

Determine RFC Destinations to be Started via Call Parameters

format	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.
evaluated by	The call parameters are only evaluated by the <i>ModuLeSeLectAction</i> 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.
exception	The parameters specified at the start are not evaluated by the <i>ModuLeGLobaLAc-tion</i> scripts, like dvsstart, or sysstart <i>System</i> , like sysstart SAP.
Q example	rfcserverstart PROD

Test the RFC Destination on the SAP System

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.	
	RFC Destination SEAL-CONNC-001	
	Connection Test Unicode Test 💖	
	RFC Destination SEAL-CONNC-001	
	Connection Type T TCP/IP Connection	
4	In the case of success, you will get this result:	
	RFC - Connection Test	
	Connection Test SEAL-CONNC-001 Connection Type TCP/IP Connection	
5	In the case of error, you will get this result:	
	RFC - Connection Test	
	Connection Test SEAL-CONNC-001 Connection Type TCP/IP Connection	
	Action Result	

instructions connection test on the SAP system

Test the RFC Destination on the SAP System, Continua-

tion

Step	Action			
6	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. You can check the current system ID of the target system with: Extras→System Information→Target System			
	Target System			
	System Name		SAP Release 753	
	Host Name	ROE-SAP-	Protocol Vers. 011	
	Database		Character Set 4102	
	Database Host		Integer BIG	
	Database System		Floating Point IEE	
			Kernel Release 753	
	OS	Win 2019		
	SAP Host ID			
	Time Zone (s)	3600 Summertime act	ive	
	System ID	ROE-SAP-PE-003		
	Network Address	10.100.100.127		
		-		

3.5 Troubleshooting - RFC Destination

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

P:	How is the correct connection determined when sapftp/saphttp is started?
L:	ightarrow saphttp/sapftp Start - Background Knowledge, Page 47
P:	Establishing several application server - what do you need to know?
L:	\rightarrow Hints for the Load Balancing, Page 48
Ρ:	Supporting a central SAP gateway - what needs to be considered?
L:	\rightarrow Support Central SAP Gateway, Page 65
Ρ:	Additional information is required for troubleshooting.
L:	\rightarrow Additional Messages and Debugging, Page 50
Ρ:	Transfer with sapftp/saphttp is very slow.
L:	\rightarrow Activate DLL Version of sapftp/saphttp in Case of Bottlenecks, Page 51
Ρ:	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:	\rightarrow Define the USE_GWHOST Parameter, Page 52
Ρ:	RFC destinations cannot be established.
	Possible cause is the update to EhP7 or kernel 721, where the desti- nations are no longer accepted automatically.
L:	ightarrow Security Configuration for RFC and SAP Destinations, Page 29
	The simulation mode may simplify the troubleshooting:
	ightarrow Activate Simulation Mode for Security Configuration, Page 36
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.

typical problems and their solutions

Troubleshooting - RFC Destination, Continuation

L:	Activate logging for the SAP gateway to find the cause of the error (JCO_ERROR_CANCELLED):
	\rightarrow Activate the SAP Gateway Logging, Page 53
	Activate the RFC trace to find the cause of the error (JCO_ERR_COM- MUNICATION):
	\rightarrow Activate RFC Trace, Page 54
	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:
	\rightarrow Activate Trace Functions for sapftp/saphttp, Page 55

saphttp/sapftp Start - Background Knowledge

When starting saphttp/sapftp, the current source node and the service for the description 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.

47

Hints for the Load Balancing

description	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.	
specify	The host name of the ap gateway service as Gater RFC destination on the S	oplication server is specified as Gateway Host and the way Service for the load balancing when creating the AP system.
select the ap- pli-cation server	It is advisable to select the application server with the least downtime as Gateway host. This should also be the system's database server.	
Caution - copy of the SAP system	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!	
overview	SEAL Systems products support load balancing/reliability in different ways:	
	Product	Load Balancing/Reliability

Product	Load Balancing/Reliability
Conversion Server	Scenario 1:
	Several application servers with one message server which convert independently - even in case of failure of another application server.
	Solution:
	• 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.
	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.

Hints for the Load Balancing, Continuation

Product	Load Balancing/Reliability
RFC Server: • DMS View Server	The functionality described as scenario 2 is supported by Conversion Server.
• Core Convert	Alternative when using JRFC Server:
	You may assign several JRFC Server via the same RFC destination.
	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 Imple- mentation (assignment and status query can be executed on different servers).
RFC client	RFC clients support the SAP load balancing via message servers (type B).
CD Installations	CD installations from SEAL Systems (type A) do not support the automatic load balancing.
	The configuration files, for instance saprfc.ini and rfcserver.cfg, must be modified and saved manually.

Additional	Messages and	Debugging

description	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.
activate trace	You activate the trace messages with RFC_TRACE in saprfc.ini.
messages	Alternatively, you can also activate the RFC trace or SAP Gateway logging within the SAP system:
	ightarrow Activate the SAP Gateway Logging, Page 53
	\rightarrow Activate RFC Trace, Page 54
debugging of sys- tem functions	You activate the debugging of system functions with ABAP_DEBUG in saprfc.ini.

Activate DLL Version of sapftp/saphttp in Case of Bottlenecks

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

The following requirement must be fulfilled:

requirements

- 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.

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

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

- description 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.
- instructions

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

Step	Action		
1	Start the /seal/img	transaction.	
2	Click 🍄 at		
	Basis Configuratio	on	
	→Define Parameter	rs	
	(table: /seal/bas_c	r142)	
3	 Specify the value of the USE_GWHOST parameter with: RFC server destinations: PARA_GWHST: Y or N RFC client destinations: PARA_GWHSB: Y or N Example: 		
	Parameter		
	Parameter ID	Parameter Value	Short Description
	PARA_DDEST Un 🔻	х	Unconditional use of destination NO
	PARA_GWHSB Pa 🔻	N	Value for USE_GWHOST with destin
	PARA_GWHST Pa 🔻	N	Wert for USE_GWHOST
	Default is for both p	oarameters: N	·

backgroundWhen using sapftp/saphttp, the host name is passed via the GWHOST parameterknowledgeand transferred to librfc23, for instance:

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.

<code>librfc32</code> 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

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

This is how you activate the SAP gateway logging:

Step	Action	
1	Start the transaction: smgw	
2	Select:	
	Goto	
	→Expert Functions	
	→Logging	
3	Activate the following op Network: Activate Security - (denied Activate	otions in the Log Events area: accesses without rules):
 Registered Programs: Activate Example: 		: Activate
	Gateway Logging for	roesap007_X74_00
	😏 🥕 🖷	
	File Name	
	Name of Log File	gw_log-2020-11-16
	File Name	gw_log-%y-%m-%d
		Special Character for Generating File Name
4	Display the log to search for the cause of the error:	
	Gateway Logging for	roesap007_X74_00
	🔁 🥕 🖷	
	File Name	
	Name of Log File	gw_log-2020-11-16

instructions

Activate RFC Trace

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.

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

 \rightarrow RFC_TRACE Parameter, Page 133

 \rightarrow SEAL_TRACE Parameter, Page 134

instructions

This is how you activate the RFC trace:

Step	Action			
1	Start the transaction: sm59			
2	Switch to the ta	b:Special Options		
	Administration	Technical Settings	Logon & Secur	ity Unicode
3	Activate the foll	owing option in the	Trace area:	
	• Set RFC Tra	ice: Activate		
	🥖 Hint - effects:			
	This automatically activates the Export Trace option in the Trace			
	Export Methods	section and overrid	es the gw/expo > 558254	rt_trace_leve
	Example:			
	~			
	Administration	Technical Settings	Logon & Secur	ity Unicode
	Special Flags			
		ction		REC Bit Options
		clon		N C Dic Options
	Trace			
	Trace Activate RFC Trac	e		

result

The following trace files are created:

- dev_jco_rfc.log
- jco_rfc*PID_UUID*.trc

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

Activate Trace Functions for sapftp/saphttp

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

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

Step	Action
1	Set following environment variable:
	• 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:
	• 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.

introduction	 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: 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
	 RFC server: DPF DMS Loader/ABAP XSA (DMS View Server is not affected))
in this chapter	This chapter deals with the following topics:
	ightarrow Establish Templates for sapftp/saphttp (sm59), Page 57
	ightarrow Create Multiple sapftp/saphttp Destinations, Page 60
	ightarrow RFC Client - Assign Static sapftp/saphttp Destination, Page 63
	ightarrow RFC Server - Assign Static sapftp/saphttp Destination, Page 64
	\rightarrow Support Central SAP Gateway, Page 65

4 Static RFC Destinations for SNC Support

Establish Templates for sapftp/saphttp (sm59)

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

- For RFC client (for example, for use by JSAPcli):
 - SEAL-CLT-SAPFTP
 - SEAL-CLT-SAPHTTP
- For RFC server (for example, for use by DMS View Server):
 - SEAL-SRV-SAPFTP

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

Step	Action	
1	Start the transaction: /n/seal/img	
2	Click ^I at Basis Configuration →Static Destinations →Establish RFC Destinations I Hint - alternative:	
2	Select the connection type on the left	
3	TCP/IP Connections (Type: T) RFC Connections > ABAP Connections > HTTP Connections to External Server > HTTP Connections to ABAP System > Internal Connections > Logical Connections > TCP/IP Connections	Type 3 G H I L T

Establish Templates for sapftp/saphttp (sm59), Conti-

nuation

Step	Action
4	Create three items with the following settings in the Technical Settings tab: • For RFC client - SAPFTP: • RFC Destination: SEAL-CLT-SAPFTP • Registered Server Program: Activate • Program ID: SEAL-CLT-SAPFTP • For RFC client - SAPHTTP: • RFC Destination: SEAL-CLT-SAPHTTP • Registered Server Program: Activate • Program ID: SEAL-CLT-SAPFHTP • For RFC server - SAPFTP: • RFC Destination: SEAL-SRV-SAPFTP • Registered Server Program: Activate • Program ID: SEAL-SRV-SAPFTP • Registered Server Program: Activate • Program ID: SEAL-SRV-SAPFTP • Registered Server Program: Activate • Program ID: SEAL-SRV-SAPFTP
	RFC Destination SEAL-CLT-SAPFTP Connection Type T TCP/IP Connection Description Description 1 SEAL-CLT-SAPFTP Description 2
	Administration Technical Settings Logon & Security Unice Activation Type Start on Application Server Registered Server Start on Application Server Start on Explicit Host Registered Server Start on Front-End Work Station Registered Server Program Program ID SEAL-CLT-SAPFTP
	Generally, you already have an RFC destination: Copy this and enter the settings mentioned above: Connection \rightarrow Copy (Ctrl+F12)

Establish Templates for sapftp/saphttp (sm59), Conti-

nuation

Step	Action		
5	 On the Technical Settings tab, enter the gateway options: Gateway Host: GWHOST from saprfc.ini Gateway Service: GWSERV from saprfc.ini Example: 		
	Gateway Host roesap005.sealsystems.local Gateway service sapgw01		
	Background info: JSAPcli uses this information for static sapftp/saphttp destinations.		
6	 For SNC destinations, enter in the Logon & Security tab under Security Options: SNC: SNC parameter, enter Active: Activate Example - SNC parameter: 		
	Destination SEAL-CLT-SAPFTP-SNC SNC Ac QoP Image: Default (profile parameter snc/data_protection/use) SNC names		
	<pre>Partners p:CN=SEALRFC,OU=SEALSAP,O=SEAL,C=DE Caution - saprfc.ini: The SNC settings in saprfc.ini must also be activated on the server: SNC_MODE=1 SNC_MODE=1 SNC_QOP=8 The system ID used is defined via rfcserver.cfg (RFC server) or cadefc ini (REC client)</pre>		

Create Multiple sapftp/saphttp Destinations

description If you use multiple RFC servers, for example for DPF, DMS View Server, which are to use static sapftp destinations, you must create a corresponding number of sapftp destinations.

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.

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

Step	Action
1	Start the transaction: /n/seal/img
2	Click [♀] at Basis Configuration →Static Destinations
	ightarrowCopy Template for Static sapftp/saphttp

Create Multiple sapftp/saphttp Destinations, Continua-

tion

Step	Action		
3	 Enter the following values for RFC client and then create the destinations with ⁽¹⁾: RFC client: Template SAPFTP: SEAL-CLT-SAPFTP Template for RFC client - SAPFTP from → Establish Templates for sapftp/saphttp (sm59), Page 57 Template SAPHTTP: SEAL-CLT-SAPHTTP Template for RFC client - SAPHTTP from → Establish Templates for sapftp/saphttp (sm59), Page 57 Number: Desired number of static destinations Example: 		
	Create SAPFTP and SAPHTTP Destinations		
	(P)		
	Template SAPFTP	SEAL-CLT-SAPFTP	
	Template SAPHTTP	SEAL-CLT-SAPHTTP	
	Number	3	
	 RFC server: Template SAPFTP: SEAL-SRV-SAPFTP Template for RFC server - SAPFTP from → Establish Templates for sapftp/saphttp (sm59), Page 57 Template SAPHTTP: Empty Number: Desired number of static destinations Example: 		
	Create SAPFTP and SAPHTTP Destinations		
	•		
	Template SAPFTP	SEAL-SRV-SAPFTP	
	Template SAPHTTP		
	Number	4	
	Background knowledge - no SAF RFC servers have an integrated s none needs to be created.	PHTTP required: saphttp destination so that	

When copying from the source destination to the target destination, the background knowledge

Create Multiple sapftp/saphttp Destinations, Continua-

tion

- SNC parameter are passed
- 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

As soon as you perform the configuration described here, static instead of description 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.

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

instructions

Step	Action			
1	Start the transaction: /n/seal/img			
2	Click [™] at Basis Configuration →Static Destinations →Create Static Destination for RFC Client (table:/seal/bas_cr114)			
3	 Enter: User Nam User with or empty SAPHTTP: Template for sapft/ SAPFTP: S Template for sapft/ Number: Number: template You can or → Create 	e: which the RFC clie (default) SEAL-CLT-SAPHTTP for RFC client - SAF b/saphttp (sm59), F EAL-CLT-SAPFTP for RFC client - SA b/saphttp (sm59), F of possible sapftp/se create this number <i>Multiple sapftp/se</i> e:	nt logs on to SAP PHTTP from → Est Page 57 PFTP from → Est Page 57 Saphttp destinations w Saphttp Destination	from cadrfc.ini, tablish Templates ablish Templates ons including the rith: ns, Page 60
	Static destina	tions for RFC Client	CADETD	Number
	User Name		SAPETP	Number
		SEAL-OLI-SAPHTIP	SEAL-CET-SAFFTP	<u> </u>

RFC Server - 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 RFC server - or for all RFC servers if RFC server is empty.

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

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

Action
Start the transaction: /n/seal/img
Click Basis Configuration →Static Destinations →Create Static Destination for RFC Server (table: /seal/bas_cr113)
 Enter: Server: RFC destination, for example from rfcserver.cfg, which should use a static sapftp destination Depending on how many servers are to use static sapftp desti- nations, you must create this number of destinations with: SAPFTP: SEAL-SRV-SAPFTP Template for RFC server - SAPFTP from → Establish Templates for sapftp/saphttp (sm59), Page 57 Example:
Static Destinations for RFC Server
Server SAPFTP
SEAL-CONNC-OKX74-002 SEAL-SRV-SAPFTP

Support Central SAP Gateway

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

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

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

This is how you support a central SAP gateway:

instructions

Step	Description
1	On the server, open:
	saprfc.ini
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:
	ASCS= <section central="" gateway="" of="" r="" sap="" the="" type=""></section>
	DEST=W74
	TYPE=B
	ASCS=W74RFC
3	Enter the data of the central SAP gateway in the section of type R that you specified in step 2 for ASCS.
	DEST=W74RFC
	TYPE=R
	GWHOST=roesap005.sealsystems.local
	GWSERV=sapgw01
	RFC_TRACE=0
	SEAL_TRACE=0
	UNICODE=1
	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.

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



Support Central SAP Gateway, Continuation

DEST=W74 TYPE=B MSHOST=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 GWHOST=roesap005.sealsystems.local GWSERV=sapgw01 RFC_TRACE=0 SEAL_TRACE=0 UNICODE=1 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.

note

5 HTTP Connection - Configuration

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

Alternatively, the following transfer types are available:	alternative
\rightarrow RFC Destination - Configuration, Page 17	

This chapter deals with the following topics:

 \rightarrow HTTP Connection - Configuration on Server, Page 68

 \rightarrow Create an HTTP Connection on the SAP System, Page 72

in this chapter

5.1 HTTP Connection - Configuration on Server

in this chapter This chapter deals with the following topics:

- \rightarrow Create PSE, Page 69
- \rightarrow Activate Logon with Basic Authentication and SSL, Page 70

Create PSE

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

This is how you create a PSE for HTTPS on the external server, using Windows instructions 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	Create the SAPSSLC PSE:
	 sapgenpse.exe gen_pse -noreq -p SAPSSLC.pse Caution - PIN:
	A PIN has to be entered for the creation. Remember the PIN for further configuration.
	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.
4	Integrate the root certificate and the intermediate certificate from Web server into the SAPSSLC PSE, for example:
	 sapgenpse.exe maintain_pk -p SAPSSLC.pse -mRootCertifi- cate.crt
	 sapgenpse.exe maintain_pk -p SAPSSLC.pse -mWebserver- Certificate.crt
5	Copy the SAPSSLC PSE if SAPSSLS.pse does not exist, with:
	cp SAPSSLC.pse SAPSSLS.pse
6	Create the cred_v2 file for the SEALService user via the execution of sapgenpse.exe, with the PIN from step 3, for instance: sapgenpse.exe seclogin -0 SEALServiceUser -p SAPSSLC.pse -x PIN sapgenpse.exe seclogin -0 SEALServiceUser -p SAPSSLS.pse -x PIN
7	Check the imported certificates: sapgenpse.exe maintain_pk -p SAPSSLC.pse -1 sapgenpse.exe maintain_pk -p SAPSSLS.pse -1

Activate Logon with Basic Authentication and SSL

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

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

Step	Action	
1	Open a SEAL shell and start the command:	
	sysinit dpf	
	Enter:	
	• 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:	
	sysinit -auto	
	Result:	
	As a result, the following items exist:	
	 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:	
	 File: customer\server\web\conf\auth-basic-dpf.conf: Add to LocationMatch: rest/ Example: 	
	<locationmatch "="" (dpf4c-sercive-v1.3="" pdflls-service-<br="">v1.0/ cgi-bin/testAuth/ /rest/dpf/v1/ /rest rest)"></locationmatch>	
4	Enter:	
	sysstop -full web	

Activate Logon with Basic Authentication and SSL,

Continuation

Step	Action	
5	Enter:	
	• 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:	
	• sysstart web	

5.2 Create an HTTP Connection on the SAP System

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

alternative Alternatively, the following transfer types are available:

 \rightarrow Establish the RFC Destination on the SAP System, Page 24

procedure -

This is how you create the HTTP connection required for the REST interface:

over-view

Step	Action
1	Start the sm59 transaction.
2	Select the connection type on the left: HTTP Connection to External Server (type: G) RFC Connections Type ABAP Connections 3 HTTP Connections to External Server G
3	Click Create: RFC Destination Connection Test 6 RFC Destination Connection Type G HTTP Connection to External Serv
4	\rightarrow HTTP Connection - Basis Data, Page 73
5	\rightarrow HTTP Connection - Technical Settings, Page 74
6	\rightarrow HTTP Connection - Logon & Security, Page 75
7	\rightarrow HTTP Connection - Special Options, Page 77
8	Save the settings.
9	 Activate the service required for HTTP transfer if it is deactivated: Transaction: sicf Start the display via vith: 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

Enter the following settings:

		tings
Parameters	Value	
RFC Destination	Unique identifier on the SAP system C Example: SEAL-REST-001	
Connection Type	G	
Description	Describing text	

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

necessary set-

 \bigcirc example

HTTP Connection - Technical Settings

requirement Switch to the Technical settings tab.

necessary set-

Enter the following settings:

tings

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				
Administration	Technical Settings	Logon & Security	Special Options]
Target System Se	ttings			
Target Host	winsrv-100.sealsystem	s.local	Service No.	9126
Path Prefix	/rest			

HTTP Connection - Logon & Security

Switch to the Logon & Security tab.

Enter the following settings:

necessary settings

requirement

Parameter	Value
Logon with User	Basic Authentication: Activate
	 user: user for logon
	 password: password for logon
	🖉 Hint - requirement:
	\rightarrow Activate Logon with Basic Authentication and SSL, Page 70
Logon with Ticket	• Do Not Send Logon Ticket: Activate
Security Options	SSL: Activate
	 SSL Certificate: DFAULT SSL Client (Standard)

 \bigcirc example

HTTP Connection - Logon & Security, Continuation

Administration	Technical Settings	Logon & Security	Special Options
Logon Procedure			
Logon with User			
O Do not use a u	user		
Basic Authenti	cation		
User	wsuser		
PW Status	saved		
Password	*****	*****	*****
Logon with Ticke	t		
Do Not Send I	.ogon Ticket		
O Send ticket w	ithout reference to targe	t system	
O Send assertion	ticket for dedicated targ	get system	
System ID	Client		
Security Options			
Status of Secure	Protocol		
SSL	◯ Inactive	 Active 	
SSL Certificate	DFAULT SS	SL Client (Standard)	✓ Cert. List
Authorization for D	Destination		

HTTP Connection - Special Options

Switch to the Special Options tab.

Enter the following settings:

Parameter	Value
Timeout	• ICM Default Timeout: Activate
	Maximum response time for the connection when sending an HTTP request.
HTTP Setting	HTTP 1.1: Activate
Status of HTTP Version	Protocol version of HTTP requests
HTTP Setting	• Compression
Compression Status	 Inactive: Activate
	 Status of Compressed Response
	No: Activate
HTTP Cookies	• Yes (All): Activate
	Handling of received cookies:

requirement

necessary settings

HTTP Connection - Special Options, Continuation

ample			
Administration T	echnical Settings	Logon & Security	Special Options
Timeout			
 ICM Default Timeout 			
○No Timeout			
O Specify Timeout	0 Time	out in Seconds (1 to 9	9999999)
HTTP Setting			
Status of HTTP Version	l		
HTTP Version	○HTTP 1.0	• HTTP 1.1	
Compression Status			
Compression	Inactive		
	Active (dep	pends on MIME type)	
	Active (full)	document)	
Status of Compressed F	Response		
Compressed Response	O Yes	No	
HTTP Cookies			
Type of Cookies Accept	tance		
Accept Cookies	○ No		
	• Yes (All)		
	🔘 Input Prom	ipt	

6 Integration via Web Service - SAP as Provider

This chapter describes the establishing of an integration via Web service, if SAP introduction serves as provider.

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



This chapter deals with the following topics:

in this chapter

- \rightarrow Required Authorizations, Page 80
- \rightarrow Configuration on the Provider System (SAP), Page 81
- \rightarrow Troubleshooting Analysis of Web Service Requests, Page 86

6.1 **Required Authorizations**

requirement - 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

6.2 Configuration on the Provider System (SAP)

This chapter deals with the following topics:

- \rightarrow Select the Service, Page 82
- \rightarrow Create the Binding on the Provider System, Page 83
- → Determine URL for WSDL Access, Page 85

81

Select the Service

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

Step	Action			
1	Start the SOA manager via	the soamanager	transaction.	
2	Switch to the Service Adm	inistration tab.		
3	Click:			
	Web Service Configurati	on		
	SOA Management (R3_800;W74;800)			
	Service Administration Te	echnical Administration	Logs and Tr	aces Ma
	Identifiable Business Context Define Identifiable Business Contexts Identifiable Business Context Referen Define Identifiable Business Context I	(IBCs) Ice references (IBC reference)	
	Design Time Cache Display central design time cache Web Service Configuration Configure service definitions, consum	ner proxies and service gr	oups	
4	Search for the desired ser	vice:		
	Click Search.			
	Web Service Configuration (R3_800;W74;800)			
	Design Time Object Search Configuration Search			
	 Search Criteria 			
	Object Type	v is	~	All
	Object Name	 ✓ contains 	~	*LAD*
5	Select the required service	e of type Service	Definitior	ı:
	Click the internal name of the service.			
	Search Result			
	Internal Name	Туре		Name
	SEAL/CO_ZLAD_WS_XML	Consumer Proxy		SEAL
	() /SEAL/ZLAD_XML	Service Definition		/SEAL/Z

Create the Binding on the Provider System

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

Step	Action
1	\rightarrow Select the Service, Page 82
2	Switch to the Configurations tab.
3	Click Create Binding. Overview Configurations Classifications Details Define Services and Bindings
	Create Service
	C Service/Binding Actions State
	▼ ZLAD_XML ĨĨĨĨĨ Active
4	<pre>Enter the name of the binding and click Next: Service Name: SEAL_ZLAD_XML (example) Description: Binding for SEAL_ZLAD_XML (example) New Binding Name: SEAL_ZLADXML (example) Web Service Configuration (R3_800;W74;800)</pre>
	Configuration of New Binding for Service Definition
	1 2 3 Service and Binding Name Provider Security SOAP Prof
	Back Next Finish Cancel

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

instructions

Create the Binding on the Provider System, Continuation

Step	Action		
5	Specify the required settings and click Finish:		
	• Communication Security: None (HTTP) act	vate	
	• Authentication Method:		
	No Authentication activate		
	• ABAP Service User:		
	Enter user name and password		
	Web Service Configuration (R3_800;W74;800)	
	Configuration: Service Definition '/SEAL/ZLAD_XML	.', Service	ZLAD_XML
	Save Edit		
	Provider Security Transport Settings Message Attachments	Identifiabl	e Business Context
	Transport Guarantee		
	Transport Level: None		
	Transport Level Security		
	None (http)		
	◯ SSL (https)		
	Message Level Security		
	None		
	O Symmetric Message Signature and Encryption		
	Asymmetric Message Signature		
	 Asymmetric Message Signature and Encryption 		
	Secure Conversation		
	Extended Signature and Header Protection		
	Authentication Settings	ABAP Ser	vice User
	Authentication Level: None	User Name:	SEAL5
	Authentication Method	Password:	•••••
	✓ No Authentication		
	Transport Channel Authentication		
	User ID/Password		
	X.509 SSL Client Certificate Single Sign On using SAP Assertion Ticket		
	Cinele Cine On union CDAlena		

Determine URL for WSDL Access

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

Step	Action
1	\rightarrow Select the Service, Page 82
2	Switch to the Configurations tab.
3	Click Open WSDL Generation for Binding.
	Web Service Configuration (R3_800;W74;800
	Details of Service Definition: /SEAL/ZLAD_XML
	Overview Configurations Classifications Details
	Define Services and Bindings Create Service Image: Create Service Image: Create Service Image: Create Service Image: Create Service Image: Create Service Image: Create Service Image: Create Service Image: Create Service Image: Create Service Image: Create Service Image: Create Service Image: Create Service
4	Copy the URL. WSDL Generation
	WSDL URL for Binding: http://ROESAP005.sealsystems.local:8001/sap/bc/srt/

6.3 Troubleshooting - Analysis of Web Service Requests

in this chapter This chapter deals with the following topics:

- \rightarrow Record and Display Web Service Requests, Page 87
- → Debug Web Service Requests, Page 88

Record and Display Web Service Requests

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

Step	Action		
1	Start the sicf transaction.		
2	Open the service tree for the SERVICE hierarchy type:		
	<pre>sap/bc/srt/rfc/sap/Web service Function/Client/Web service Name/Binding</pre>		
	<pre>/sap/bc/srt/rfc/seal/zlad_xml/020/zseal_ladxml/</pre>		
	Virtuelle Hosts / Services	Documentation	
	▼ 🚺 default_host	VIRTUAL DEFAULT HOST	
	▼ 🛞 sap	SAP NAMESPACE; SAP IS	
	▼ 🖗 bc	BASIS TREE (BASIS FUNC	
	▼ 🕥 srt	SOAP Runtime	
	▼ @ fc	SOAP Runtime for RFC	
	▼ 🕲 seal		
	Seal_adxml Seal_adxml		
3	Select the menu:		
	 Edit→Recorder→Activate Recording 		
	for incoming requests on the provider sy	/stem	
	 Client→Recorder→Activate Recording 	5	
	for outgoing requests on the consumer system		
4	Enter the desired settings and click Activate	2.	
5	Start the Web service.		
6	Display the recording with:		
	• Edit→Recorder→Display Recording		
	for incoming requests on the provider system		
	 Client→Recorder→Display Recording 		
	for outgoing requests on the consumers	system	

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

Debug Web Service Requests

requirement

 \rightarrow Required Authorizations, Page 80

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

Step	Action			
1	Start the sicf transaction.			
2	Open the service tree for the SERVICE hierarchy type:			
	<pre>sap/bc/srt/rfc/sap/Web service Function/Client/Web service Name/Binding</pre>			
	<pre>Lxample: /sap/bc/srt/rfc/seal/zlad_xml/020/zseal_ladxml/ zseal_ladxml</pre>			
	Virtuelle Hosts / Services	Documentation		
	default host	VIRTUAL DEFAULT HOST		
	▼ Sap SAP NAMESPACE			
	▼ ⊗ bc	BASIS TREE (BASIS FUNC		
	▼ ③ srt	SOAP Runtime		
	🔻 🎯 rfc	SOAP Runtime for RFC		
	✓ Ø seal			
	▼			
	▼ 🚱 020			
	▼			
	• 🕲 <mark>zseal_ladxml</mark>			
3	Select the menu:			
	Edit→Debugging→Activate Debugging			
4	Start the Web service.			
5	Debug the Web service in the debugger.			

7 Integration via Web Service - SAP as Consumer

This chapter describes the establishing of an integration via Web service, if SAP introduction serves as consumer.

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

 \rightarrow Integration via Web Service - SAP as Provider, Page 79



This chapter deals with the following topics:

 \rightarrow Required Authorizations, Page 90

 \rightarrow Configuration on the Consumer System (SAP), Page 91

- → Advisable Behavior in the Case of Error, Page 97
- → Troubleshooting, Page 99

related top-

in this chapter

7.1 Required Authorizations

requirement - 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

7.2 Configuration on the Consumer System (SAP)

The Web service, which you want to use from SAP, is started externally.	requirement	
This chapter deals with the following topics:	in this chapter	
\rightarrow Select the ABAP Proxy, Page 92		
\rightarrow Create a Logical Port, Page 93		
ightarrow Suppress the Message ID Transfer, Page 95		

 \rightarrow Transfer of Large Amounts of Data, Page 96

Select the ABAP Proxy

instructions This is how you select the ABAP proxy for which you want to establish the integration:

Step	Action			
1	Start the SOA manager via the soamanager transaction.			
2	Switch to the Service Administra	Switch to the Service Administration tab.		
3	Click:			
	Web Service Configuration			
	SOA Management (R3_800;W	74;800)		
	Service Administration Technical Adm	ninistration Logs and	Traces Ma	
	Identifiable Business Context			
	Define Identifiable Business Contexts (IBCs) Identifiable Business Context Reference			
	Define Identifiable Business Context references (I	BC reference)		
	Display central design time cache			
	Web Service Configuration Configure service definitions, consumer proxies a	nd service groups		
4	Search for the desired service:			
	Click soundh			
	Web Service Configuration (R3 800:W74:800)			
	Design Time Object Search Configuration Search			
	Control Crittoria			
	Search Criteria			
	Object Type	v is	All	
	Object Name	v contains	*LAD*	
	Maximum Number of Results: 100			
5	Select the desired consumer proxy	rfrom the Consumer	Proxy type:	
	Click the internal name of the con	sumer proxy.		
	Search Result			
	Internal Name	Туре	Name	
SEAL/CO_ZLAD_WS_XML Consumer Proxy			SEALZ	
	(SEAL /ZLAD YML	Service Definition	SEAL /7LA	

Create a Logical Port

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

This is how you create a logical port: instructions Action Step 1 \rightarrow Select the ABAP Proxy, Page 92 2 Switch to the Configurations tab. 3 Click Create - WSDL based Configuration. Web Service Configuration (X74;020) Details of Consumer Proxy: /SEAL/CO_ZLAD_WS_) Configurations Overview Details Define Levie I Dente 4 Enter the data for the logical pro and click Next: • Logical Port Name: WS_DPF4C_OK (example) Logical Port is Default: activate Description: Logical port for WS DPF4C OK (example) Web Service Configuration (X74;020) New WSDL based Configuration of Logical Port for 2 3 I) Logical Port Name WSDL Information **Rinding Selection** Web Service Configuration (X74:020) New WSDL based Configuration of Logical Port for

Create a Logical Port, Continuation

Step	Action			
5	Enter the WSDL access settings for the logical pro and click Finish:			
	WSDL Base: Via HTTP Access activate			
	 URL for WSDL Access: http://server:9125/dpf4c-service-v1.3/ convert?wsdl(example) 			
	Web Service Configuration (X74;020)			
	New WSDL based Configuration of Logical Port for			
	Logical Port Name WSDL Information Binding Selection			
	Back Next Finish Cancel			

Suppress the Message ID Transfer

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

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

Step	Action		
1	\rightarrow Select the ABAP Proxy, Page 92		
2	Switch to the Configurations tab.		
3	Select the desired logical port and click Edit.		
4	Switch to the Messaging tab:		
5	Enter: Message ID Protocol: Suppress ID Transfer Web Service Configuration (X74;020)		
	Configuration: Consumer Proxy '/SEAL/CO_ZLAD_		
	Save Edit Ping Web Service		
	Consumer Security Messaging Transport Settings Mess		
	Message ID (Synchronous)		
	Message ID Protocol: Suppress ID Transfer		
	🛕 Caution - default		
	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:		

Transfer of Large Amounts of Data

- description If you transfer large amounts of date in the Web service environment, you can use the SOAP Message Transmission Optimization Mechanism (MTOM).
- requirement MTOM is supported as of SAP release 7.20 or newer without restrictions, see SAP note 1582187.
- instructions This is how you activate the optimized XML transfer for large amounts of date on the consumer system:

Step	Action		
1	\rightarrow Select the ABAP Proxy, Page 92		
2	Switch to the Configurations tab.		
3	Select the desired logical port and click Edit.		
4	Switch to the Transport Settings tab.		
5	Enter:		
	• Optimized XML Transfer: MTOM		
	Web Service Configuration (X74;02	20)	
	Configuration: Consumer Proxy '/SEAL/	CO_ZLAD_	
	Save Edit Ping Web Service Consumer Security Messaging Transport Settings		
	Transport Binding		
	* URL Access Path:	/sap/bc/srt/rfc/sea	
	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 💌	
	Mavimum Mait far MO Oanauman	0	

Action

Step

7.3 Advisable Behavior in the Case of Error

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

Check if the URL is accessible: 1 Start the rswf test http program (transaction: sa38). • Enter the URL to be tested and click $^{\textcircled{}}$. Example: Test HTTP Connection Ð URL http://ok-win12-dom:9125/cgi-bin/ **Result:** A green status display in the first line indicates a successful connection, a red status display indicates an error. Example - HTTP connection successful: Test HTTP Connection Test HTTP Connection 00 ~response line HTTP/1.1 200 OK ~server_protocol HTTP/1.1 ~status code 200 ~status reason OK Example - HTTP connection is faulty: Test HTTP Connection Test HTTP Connection 00 HTTP/1.1 404 Not Four ~response line ~server protocol HTTP/1.1 404 ~status code ~status reason Not Found

Advisable Behavior in the Case of Error, Continuation

Step	Action			
2	If an error occur cause of the erro Manager at SEAL	rs, start the ICM mon or and forward this da . Systems if necessary	nitor ata to ':	to determine the exact o your Technical Project
	Transaction: smid	cm		
	Display trace	file:		
	Goto→Trace	File→Display All		
	• Save trace file	e:		
	Goto→Trace	File→Save Locally		
	🔄 List Edit <u>G</u>	oto <u>A</u> dministration	<u>S</u> etti	ngs S <u>y</u> stem <u>H</u> elp
		<u>T</u> race File	•	Display All Shift+F5
	<u> </u>	Trace Level		Display Start
	ICM Moni	Parameters	•	Display <u>E</u> nd
	9. 🔁 🖻 蒙	Statistics	•	Save Locally
		Memory Pipes		Reset
	ICM Status:	Host Name Buffer		Security Log
		Services Shift+F1		Dev_icmbnd
	Restart Afte Trace Level	Display Connections	Ĩ	
	Created Worl	Release Notes F9		/ 50 (Current / 1
	Connections	HTTP Server Cache	21	/ 500 (Current / 1
	Anene Fuciti	HTTP Log	21	/ 500 (Current / i
		HTTP Server	<u> - </u>	
	No. Thre	Back F3		Processed 1
	Hint - reset	trace file:	_	
	Eor a better o	verview vou can	dolot	o the trace file with
	Goto→Trace Fil	$e \rightarrow Reset and execute$	e the	erroneous call again.
	Hint - set tra	ace level:		
	In general the d	lofault traco lovol is s	uffic	iont. Vou can chango it
	with Goto→Trac	e Level→Set and	exec	ute the erroneous call
	again.			

7.4 Troubleshooting

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

P: The Web service returns an error message of the following type: SOAP:1.023 SRT: Processing error in Internet Communication Framework: ("ICF Error when receiving the response: IC-M_HTTP_CONNECTION_FAILED" Possible cause is that the Web service is not started. Start the Web service. A: **P**: The Web service returns an error message of the following type: Error while calling DPF Webservice SoapFaultCode:3 headers:[{http:// MustUnderstand schemas.xmlsoap.org/ws/2004/08/addressing}Action, {http:// schemas.xmlsoap.org/ws/2004/08/addressing}To] are not understood Possible cause is that the ID transfer of the message ID protocol is not suppressed. A: Suppress the message ID transfer: \rightarrow Suppress the Message ID Transfer, Page 95 **P**: The Web service returns an error message of the following type: SOAP:1.001 CX_SXML_PARSE_ERROR: An exception was raised. Error when parsing an XML stream: '<EOF> reached Possible cause is that the optimization of the transfer of large amounts of data is not activated. Optimize the transfer of large amounts of data: A: \rightarrow Transfer of Large Amounts of Data, Page 96 **P**: The Web service returns an error message of the following type: SOAP:1.007 SRT: Unsupported xstream found: ("HTTPCode 502: Bad Gateway") Possible cause is that the timeout is too small. A: Increase the timeout in server\web\apache\conf\workers.properties: worker.seal-worker.socket_timeout **P**: The Web service returns an error message of the following type: "HTTPCode 502: Bad Gateway" Possible cause is that the timeout is too small.

typical problems and their solu-

tions

Troubleshooting, Continuation

A:	Increase the timeout for the HTTP protocol via the smicm transac- tion with Goto \rightarrow Services and Service \rightarrow 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 transac- tion with Goto \rightarrow Services and Service \rightarrow Change:
	Keep Alive (in Sec.)
	Maximum Processing Time (ProcTimeout)



8 Configuration Files - Reference

This chapter explains the configuration files which are evaluated to establish a introduction connection between the OM server and the SAP system in case of communication via RFC destination.

This chapter deals with the following topics:

→ cadrfc.ini - Logon Information, Page 104

→ saprfc.ini - Connection Data, Page 116

 \rightarrow *rfcserver.cfg*, Page 146

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

103

in this chapter

	8.1 cadrfc.ini - Logon Information
introduction	This chapter contains the reference information about the cadrfc.ini configuration file.
requirement	The cadrfc.ini file is evaluated for RFC client connections. Other RFC server connections ignore this file.
ASCII/Unicode	Within cadrfc.ini only ASCII characters are supported. Unicode characters are not supported.
location	The cadrfc.ini file is located in the following directory:
	applications\server\sapserv\bin
🖉 hint - gXnet-	For gXnetplot, the file is located in:
plot	\$GRALPLOTLIB/PDM (servermenu - c - cdl - cd PDM)
purpose	The configuration file contains the necessary logon data which is evaluated by the BAPI and CAD interface.
	The interactive RFC clients use the logon data as default values for the initial logon dialog.
	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).
structure	 You can specify general as well as system- and client-specific logon data: 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\ <i>SystemName\Client</i>]
	[SAP\W74\020]or[SAP\W74]
Q example	Extract of an example for cadrfc.ini:
	*
	* SAP logon parameters
	*
	CadRfcUser SEALCPIC
	CadRfcPassword <sappwd></sappwd>
	#CadRfcPasswordCoded 0xe3f0e9c6604b14b3
	#CadR+cClient 010

cadrfc.ini - Logon Information, Continuation

CadRfcLanguage EN *_____ * Connection parameters *_____ * Logical destination CadRfcDestination W46 . . . *_____ * Parameters specific for Dialog interface (SapConnc) *_____ . . . * 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 . . .

Only a couple of parameters of the configuration file must be adjusted to the customize current system environment. Only these parameters are described below. The

cadrfc.ini - Logon Information, Continuation

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 cadrfc.ini.

System-/Client-Specific Logon Data

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

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

Step	Action
1	Enter:
	what rlistsap grep sapini.c
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 restriction of DMS Rlist, only the login data in the general (system and client independent) section of the file cadrfc.ini is used. The system- and client-specific login information is only evaluated during the processing of repro list jobs at runtime.

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.	A 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	system/client comparison

user to be used for logon.





🔨 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 meaning server to logon on the SAP system.

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 spec- ified with the parameter CadRfcPasswordCoded.
\bigcirc example	The item looks as follows: CadRfcPassword xyz

CadRfcPasswordCoded Parameter

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

This is how you create and save a coded password:

code the pass-word

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

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 meaning and RFC server to logon on the SAP system.

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:

🔍 example

CadRfcLanguage EN

CadRfcDestination Parameter

meaning	The CadRfcDestination parameter specifies the SAP system on which the RFC client and RFC server log on.
0	

example The item looks as follows:

CadRfcDestination W74

CadDialogNetAddress Parameter

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

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

The following value is used as default:

default

CadDialogNetAddress DEFAULT

introduction	This chapter contains the reference information about the saprfc.ini configuration file.
requirement: AS- CII/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:
	<pre>client\dvs\bin (RFC client connection)</pre>
	server\sapserv\conf (RFC server connection)
🖉 hint - gXnet-	For gXnetplot, the file is located in:
plot	\$GRALPLOTLIB/PDM (servermenu - c - cdl - 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 param- eter 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:
	→ Determine System Data forsaprfc.ini, Page 118
	ightarrow Types of RFC Destinations and Module Classification, Page 119
	\rightarrow Parameter Overview, Page 120
	\rightarrow DEST Parameter, Page 123
	\rightarrow TYPE Parameter, Page 124
	\rightarrow ASHOST Parameter, Page 125
	\rightarrow SYSNR Parameter, Page 126
	\rightarrow MSHOST Parameter, Page 127
	\rightarrow Parameter R3NAME, Page 128
	\rightarrow GROUP Parameter, Page 129
	\rightarrow GWHOST Parameter, Page 130
	\rightarrow GWSERV Parameter, Page 131
	\rightarrow Parameter SAPROUTER, Page 132
	\rightarrow RFC_TRACE Parameter, Page 133
	\rightarrow SEAL_TRACE Parameter, Page 134
	\rightarrow ABAP_DEBUG Parameter, Page 135

saprfc.ini - Connection Data, Continuation

- → USE_SAPGUI Parameter, Page 136
- \rightarrow UNICODE Parameter, Page 137
- \rightarrow CODEPAGE Parameter, Page 138
- → SNC_MODE Parameter, Page 139
- → SNC_MYNAME Parameter, Page 140
- \rightarrow SNC_PARTNERNAME Parameter, Page 141
- → SNC_QOP Parameter, Page 142
- → SNC_SSO Parameter, Page 143
- → ASCS Parameter, Page 144
- → X509CERT Parameter, Page 145

SAP Basis		You ca and so	an get the current SAP sys o on, from your SAP Basis	stem dat s.	a, such a	as instance num	ber, router strir	ıg
SAP logon		If SAP • SI • Gr • In • Me	GUI is installed, you can D oup/Server stance Number ssage Server	display	the SAP	system data als	so on SAP logon	:
0		• Ro	uter					
Q _{example}		• Ro	uter					
Q _{example} ≡		• Ro	uter SAP Logon 77	0		-	_ 🗆 ×	
Q example ≡ Variable Logon	0	• Ro	uter SAP Logon 77	0		– List View	- 🗆 ×	
example Variable Logon Connections	0	• Ro	uter SAP Logon 77	0	Ę	List View	- □ × ~	
example Variable Logon Connections Name	Syst	• Ro	uter SAP Logon 77 Group/Server	0 Instan	E. Message	List View w74 Server	_ 🗖 ×	
example Variable Logon Connections Name Name	Syst	 Ro SID W74 	Uter SAP Logon 77 Group/Server roesap005.sealsystems.local	0 Instan 01	E. Message	List View w74 Server	- 🗖 ×	
Connections Name Rame Karra (01) Rame (02)	Syst	 Ro SID W74 W74 	Uter SAP Logon 77 Group/Server roesap005.sealsystems.local roesap005.sealsystems.local	0 Instan 01 02	E Message	List View w74 Server	_ 🗆 ×	

Determine System Data forsaprfc.ini

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 SAPGUILandscape.xml file.

•

Types of RFC Destinations and Module Classification

The following types of RFC destinations can be distinguished:

type of RFC destinations

• RFC client via message server (type B)

RFC client via application server (type A)

• RFC server via SAP gateway (type R)

The modules from SEAL Systems can be classified in RFC client and RFC server modules and types

RFC Client	RFC Server
DMS Rlist	DMS Loader
DMS Scan	Conversion Server
JSAPcli, SAPcli	 RFC Server, JRFC Server, for instance for 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	RFC Client	RFC Server
	Application Server	Message Server	Gateway
DEST	x	x	Х
ТҮРЕ	A	В	R
ASHOST	x	-	-
SYSNR	x	-	-
MSHOST	-	х	-
GROUP	-	x	-
GWHOST	-	-	Х
GWSERV	-	-	Х
SAPROUTER	x	x	Х
RFC_TRACE	x	x	Х
SEAL_TRACE	-	-	Х
ABAP_DEBUG	x	x	-
USE_SAPGUI	x	x	-
UNICODE	x	x	Х
CODEPAGE	-	-	Х
SNC_MODE	x	х	Х
SNC_MYNAME	х	x	Х
SNC_PARTNER- NAME	X	X	-
SNC_QOP	x	x	Х
SNC_SSO	x	x	х
ASCS	x	x	-
X509CERT	x	x	Х

Parameter Overview, Continuation

The	following	table	contains	example	parameter	entries	for t	the	different	Q _{exa}	ample
coni	nection typ	es:									

Туре	Items
RFC client	DEST=W74
(application server)	TYPE=A
	ASHOST=/H/SEALDOS3/H/sapt60-1
	SYSNR=00
	RFC_TRACE=0
	ABAP_DEBUG=0
	USE_SAPGUI=0
	UNICODE=1
	SNC_MODE=1
	<pre>SNC_MYNAME=p:CN=SEALRFC, OU=SEALSAP, O=SEAL, C=DE</pre>
	<pre>SNC_PARTNERNAME=p:CN=T6B, OU=SEALSAP, O=SEAL, C=DE</pre>
	SNC_QOP=3
	SNC_SSO=1
	X509CERT=c:\seal\customer\server\sapserv\conf\sec\SEAL-RFC.crt
RFC client	DEST=W74
(message server)	TYPE=B
	MSHOST=/H/SEALDOS3/H/sapt60-2
	GROUP=Standard
	RFC_TRACE=0
	ABAP_DEBUG=0
	USE_SAPGUI=0
	UNICODE=1

Parameter Overview, Continuation

Туре	Items
RFC server gateway	DEST=W74RFC
	TYPE=R
	GWHOST=/H/SEALDOS3/H/sapt60-3
	GWSERV=sapgw00
	RFC_TRACE=0
	SEAL_TRACE=1
	UNICODE=1
	CODEPAGE=UTF-8
	SNC_MODE=1
	<pre>SNC_MYNAME=p:CN=SEALRFC, OU=SEALSAP, O=SEAL, C=DE</pre>
	SNC_QOP=8
	SNC_SSO=1



FC 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 ven-tion example of an SAP system name:

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 length char-acters. Lower versions only support a maximum of 8 characters.

The parameter DEST is evaluated for all destination types. validity

meaning	The TYPE parameter identifies the connection type.
values	The following connection types are available:
	 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.
A Caution - in- stance number/ port	Depending on the connection type, a port must be assigned to the instance number of the SAP system (xx) in the winnt\system32\drivers\etc\services system file:
	 Type A, RFC client connections via application server sapdpxx32xx/tcp
	 Type B, RFC client connections via message server sapmsgxx 36xx/tcp
	 Type R, RFC server connections via SAP gateway sapgwxx 48xx/tcp (SNC), sapgwxx 33xx/tcp (otherwise)
hint - auto- matic mapping	Items in the saprfc.ini file starting with sapgw are automatically mapped to the correct port, for instance sapgw00 to 3300 or sapgw01 to 3301. It is not required to map them explicitly in the system file.
A Caution - message server	For RFC destinations via message server (TYPE=B) with SAProuter, the following requirement must be fulfilled:
with SAProuter	• In the DNS, both the Windows host name of the message server and its SAPLOCALHOSTFULL as Fully Qualified Domain Names (FQDN) must be main-tained.
validity	The TYPE parameter is evaluated for all destination types.

TYPE Parameter

ASHOST Parameter

The ASHOST parameter contains the host address of the application server.	meaning
You can see the host address in:	system data
• Group/Server	
ASHOST=sapserver.com	\bigcirc example
→ Determine System Data forsaprfc.ini, Page 118	related top- ics
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 Begin of string with URL specification, rest truncated 	router
• /H/	
• Group/Server	
ASHOST=/H/saprouter.com/H/sapserver.com	
The ASHOST parameter is evaluated only for the following destination types:	validity

• Type A, RFC client connections via application server

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
\bigcirc example	SYSNR=00
related top- ics	→ Determine System Data forsaprfc.ini, Page 118
validity	The SYSNR parameter is evaluated only for the following destination types:Type A, RFC client connections via application server

SYSNR Parameter

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

You can see the host address in:	system data
• Message Server	
MSHOST=roemsg001.sealsystems.local	\bigcirc example
→ Determine System Data forsaprfc.ini, Page 118	Prelated top- ics
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 	

127

meaning	The R3NAME parameter contains the system ID of the SAP system
	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.
system data	You can see the system ID in:
	• SID
Q example	R3NAME=W74
related top- ics	→ Determine System Data forsaprfc.ini, Page 118
validity	The R3NAME parameter is evaluated only for the following destination types:Type B, RFC client connections via message server

Parameter R3NAME

GROUP Parameter

The GROUP parameter contains the group identifier of the message server.	meaning
You can see the group identifier of the message server in:Group/Server	system data
GROUP=PUBLIC \rightarrow Determine System Data forsantic ini Page 118	\bigcirc example
/ Determine System Data Joisupije, i age 110	ics
The GROUP parameter is evaluated only for the following destination types:	validity

• Type B, RFC client connections via message server

meaning	The GWHOST parameter contains the host address of the SAP gateway, preferably as a Fully Qualified Domain Name (FQDN). The SAP gateway is generally identical to the application server.
system data	You can see the host address in: • Group/Server
\bigcirc example	GWHOST=roegw001.sealsystesm.local
related top- ics	→ Determine System Data forsaprfc.ini, Page 118
background knowledge - SAP-	If an SAProuter is in use (for example: SAPROUTER=/H/saprouter.com/S/3299), the full name for GWHOST is automatically composed of:
Touter	 Router Begin of string with URL specification, rest truncated
	• /H/
	• Group/Server
	GWHOST=/H/saprouter.com/H/roegw001.sealsystems.local
validity	The GWHOST parameter is evaluated only for the following destination types:
	 Type R, RFC server connections via SAP gateway

GWHOST Parameter

GWSERV Parameter

The GWSERV parameter contains the group identifier of the SAP gateway.	meaning
 The group identifier of the SAP Gateway is composed of: sapgw Instance Number 	system data
GWSERV=sapgw00 → Determine System Data forsaprfc.ini, Page 118	 example related top- ics
The GWSERV parameter is evaluated only for the following destination types:	validity

• Type R, RFC server connections via SAP gateway

meaning	The SAPROUTER parameter contains the host address of the SAProuter.
system data	You can see the host address of the SAProuter in: • Router
\mathbb{Q} example	SAPROUTER=/H/saprouter.com SAPROUTER=/H/saprouter.com/S/sapgw01 (with optional port specification)
related top- ics	→ Determine System Data forsaprfc.ini, Page 118
🖉 hint - sym- bolic port	If the SAProuter string contains a symbolic port, for instance /S/sapgw01, this port has to be assigned in the system file: \rightarrow TYPE Parameter, Page 124
validity	 The SAPROUTER 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 Type R, RFC server connections via SAP gateway

Parameter SAPROUTER

RFC_TRACE Parameter

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

Trace messages are saved on the application server in the log directory in files location and name

jco_rfc_*.trc

dev_rfc*

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

CPIC*

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

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

The RFC_TRACE parameter is evaluated for all destination types.

133

4

values

validity

meaning	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.
values	The following values are available:
	 Ø 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
	Also writes Java memory status to the log file
A Caution - number	HTML files with the transferred data can quickly become extremely large; therefore the creation of HTML files should only be activated for trouble-shooting. By default, it is advisable to set SEAL_TRACE to 0 or 1.
default	Default is 0.
validity	The SEAL_TRACE parameter is evaluated only for the following destination types:Type R, RFC server connections via SAP gateway

SEAL_TRACE Parameter

ABAP_DEBUG Parameter

The ABAP_DEBUG parameter activates or deactivates the debugging of system meaning functions.

The USE_SAPGUI parameter must be set to 1 or 2 to enable the debugg	ing. requirement
The following values are available:	values
 Ø The debugging of the system functions is deactivated. This is the st case. 	tandard
• 1 The debugging of the system functions is activated for test purpos	es.
The ADAD DEDUC regression and used only for the following destinct:	on tunocu voliditu

The ABAP_DEBUG 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

meaning	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.
requirement	 The following requirements have to be fulfilled: 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.
values	 The following values are available: 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.
validity	 The USE_SAPGUI 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

USE_SAPGUI Parameter

UNICODE Parameter

The UNICODE parameter specifies if the SAP system is a Unicode or non-Unicode meaning system.

By means of this parameter the correct version of the programs sapftp and saphttp is determined.

 The following values are available:
 values

 • 0: The SAP system is a non-Unicode system.
 values

 • 1: The SAP system is a Unicode system.
 code page

 For Unicode systems, the coding can be specified with CODEPAGE:
 code page

 → CODEPAGE Parameter, Page 138
 values

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

meaning	The CODEPAGE parameter specifies the coding for Unicode systems.
interrelation	The code page is only evaluated in the case UNICODE=1.
default	The default code page is UTF-8. These is used in the following cases: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, 16LE, 32,), because only UTF-8 is supported.
validity	 The CODEPAGE parameter is only evaluated for the following destination types: Type R, RFC server connections via SAP gateway

CODEPAGE Parameter

SNC_MODE Parameter

The SNC_MODE parameter activates and deactivates SNC (activation sign).	meaning
 The following values are available: 0: SNC is deactivated. 1: SNC is activated. 	values
Default is Ø. default	
The SNC_MODE parameter is evaluated for all destination types. validity	

meaning	The SNC_MYNAME parameter contains the name of the user who executes remote function calls.
default	The default name is the name which is determined by the security product for the current user.
format	The name must use the following format: p:SEAL Server - DistinguishedName from SEALRFC.pse
Q example	p:CN=UniqueName, OU=Department, O=Company, C=CountryKey p:CN=SEALRFC, OU=SEALSAP, O=SEAL, C=DE
validity	The SNC_MYNAME parameter is evaluated for all destination types.

SNC_MYNAME Parameter

SNC_PARTNERNAME Parameter

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

The name must use the following format: format	
p:SAP System - DistinguishedName	
p:CN=UniqueName, OU=Department, O=Company, C=CountryKey p:CN=SEALRFC, OU=SEALSAP, O=SEAL, C=DE	Q example
The SNC_PARTNERNAME 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

meaning	The SNC_QOP parameter specifies the protection level (quality of protection).
values	 The following values are available: 1: Use authentication only 2: Use integrity protection (authentication) 3: Use confidentiality protection (integrity and authentication) 8: Use default values 0: Use maximum protection
default	• 9. Ose 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).
validity	The SNC_QOP parameter is evaluated for all destination types.

SNC_QOP Parameter

SNC_SSO Parameter

 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 form the SNC identity, while SNC is used for the encryption of the network communication. The parameter must be set for logon with user/password when SNC is activated. 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. 		
A minimum kernel patch of the SAP system is required, see SAP note 1701870.	requirement	
 The following values are available: 0: SSO is deactivated. Instead, user/password is used for logon, for example. 1: SSO is activated. 	values	
Default is 1.	default	
The SNC_SSO parameter is evaluated for all destination types.	validity	

meaning	The ASCS(ABAP SAP Central Services) parameter contains the name of the section of type R with the data of the central SAP gateway.
requirement	The ASCS parameter is only supported together with static RFC destinations.
Q example	Section name of type R with data from the central SAP gateway. ASCS=W74MSRFC
validity	 The ASCS parameter is evaluated only for the following destination types: Type A, RFC client connections via application server (only on request) Type B, RFC client connections via message server

ASCS Parameter
X509CERT Parameter

 The X509CERT parameter contains the certificate name if the logon with certificate meaning cate (SSO, single sign-on) is activated.
 meaning

 The certificate must be in the Based64 file format, in one line without BEGIN and END sequence.
 format

 The default name is:
 default

 %SEAL_CUSTOMDIR%\server\sapserv\conf\sec\SEALRFC.crt
 validity

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 <code>-cfgfile</code> parameter.
🖉 hint - gXnet-	For gXnetplot, the file is located in:
plot	servermenu - c - cdl - cd PDM
structure	The configuration file is divided into separate sections.
	 → [ACTIVE] Section, Page 147 [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 148 The remaining sections with exception of [ACTIVE] can be named user- defined.
Q example	Example for rfcserver.cfg:
	[ACTIVE] SEALSAP1 = DEV SEALSAP1 = T6A SEALSAP2 = PROD
	[DEV] DESTINATIONS = "X74RFC" PROGID = SEAL-BCXDC-001 PROGID = SEAL- BCXDC-002
	<pre>[T6A] DESTINATIONS = "T6ARFC" PROGID = SEAL-BCXDC-001 3 RLIGATE = %PLS- DATA%\io\rligate</pre>
	<pre>[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</pre>
comment char- acter	# 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.

8.3 rfcserver.cfg

[ACTIVE] Section

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

 The [ACTIVE] section is ignored on these conditions: 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. 	exceptions		
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		
The section may contain <i>ServerName</i> items or SECTION items. A mix of both is not allowed.			
The section may contain multiple <i>ServerName</i> or SECTION items. If <i>ServerName</i> 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.			
section.			

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 saprfc.ini and a list of the RFC destinations which are to be started with relation to their definitions in the SAP system via the sm59 transaction.		
advantage - SAP system data only once	The SAP system data must only be defined once in saprfc.ini even if several RFC destinations (PROGID) to one SAP system are started.		
advantage - sep- arate 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 - sep-	The name of the log files are composed of:		
arate log mes	ModuleName.SECTIONNAME_Number.log, for instance:		
	rfcserver.PROD_0.log		
	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 [SECTIONNAME] section is only evaluated on the following conditions: It exits as ServerName item with the current server name or as SECTION item in the [ACTIVE] section. The section name is specified via the SAP_START_SYSTEM environment variable. In this case the [ACTIVE] section is ignored. It is specified as parameter when directly executing rfcserver_start. In this case theSAP_START_SYSTEM environment variable and the [ACTIVE] section are ignored. 		
parameters	The following section describes the available parameters in the [SECTIONNAME] section.		
DESTINATIONS	 This name refers to saprfc.ini to determine the SAP system data. The value is a string: W74RFC Name of the system as specified in saprfc.ini at DEST Default: None 		

[SECTIONNAME] Section, Continuation

OTFCODEPAGE specifies the code page for downloading OTF data	OTFCODEPAGE
The value is a string:	
 ISO-8859-2 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 iden- tifier if multiple OM servers are to establish RFC destinations to the same SAP system.	
The identifier can include letters, numbers, '+', '.', '-', and '_' characters!	naming con-
The value is a string:	vention
 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/vali- dation 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	RLIGATE

start of JRFC Serverwith the call parameter -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 specifies the minimum memory at start. XMS 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 ХМХ XMX specifies the maximum memory. kint - recom-Specify a three times larger size than the maximum file size, which is to be mendation: 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 introduction relevant for the basis configuration in SAP.

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 internal key of the value in addition to the description text.

This is how you display the internal keys:

Step	Action	
1	Click I in the icon bar of SAP GUIor 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 caution - rerestarted.

This chapter deals with the following topics:

- \rightarrow /seal/bas_cr113 Static Destination for RFC Server, Page 152
- \rightarrow /seal/bas_cr114 '- Static Destination for RFC Client, Page 153

→ /seal/bas_cr142 - Define Parameters, Page 155

display key

in this chapter

	/seal	/bas_cr113 - Static Destination for RFC Server
description	This con	figuration table specifies the static destinations for RFC server.
open the table	This is h	ow you open the table:
	Step	Action
	1	Click 🍄 at:
		Basis Configuration
		→Static Destinations
		ightarrowCreate Static Destination for RFC Server
		(table: /seal/bas_cr113)
overview	The tabl	e has the following parameters:
	Static L	
	SEAL-C	CONNC-OKX74-002 SEAL-SRV-SAPETP
	JENE 1	
Server	Server is	s the RFC server for which the static sapftp destination is to be used.
	The valu	e is a string:
	 SEAL 	-CONNC-001
	Default:	None
SAPFTP	SAPFTP is	s the name of the template for static sapftp destinations.
	The valu	e is a string:
	 SEAL Stati 	-CLT-SAPFTP c sapftp destination for RFC client
	• SEAL Stati	-SRV-SAPFTP c 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.

This is how you open the table:

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

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: /sea1/bas_cr114):	static sapftp/sa- phttp
User with which the RFC client logs on to SAP from cadrfc.ini	
In regard to the meaning in the access table (table: /sea1/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



open the table

description

/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.

This is how you 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:

Parameter			
	Parameter ID	Parameter Value	Short Description
	PARA_DDEST Un 🔻	х	Unconditional use of destination NONE with classification
	PARA_GWHSB Pa 🔻	N	Value for USE_GWHOST with destination BACK
	PARA_GWHST Pa 🔻	N	Wert for USE_GWHOST
	PARA_UCORR A1 🔻	х	Always run correction of OTF data length

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

Values of the following enumeration are supported:

PARA DDEST Unconditional Use of Destination NONE with Classifica-• tion

The DESTINATION parameter value is specified for the characteristic evaluation.

- PARA_GWHSB 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.

2024-01-15

1.4.2

Default: None

System description

overview

description

open the table

/seal/bas_cr142 - Define Parameters, Continuation

Parameter Value	Parameter Value specifies the value of the parameter. The possible values depend on the value of Parameter ID.
	Values of the following enumeration and any strings are supported depending on the value of Parameter ID:
	 PARA_DDEST as Parameter ID: 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.
	PARA_GWHSB as Parameter ID: • Y
	 Set USE_GWHOST for RFC client connections to Y. N (default) Set USE_GWHOST for RFC client connections to N.
	 PARA_GWHST as Parameter ID: Y Set USE_GWHOST to Y. N (default) Set USE_GWHOST to N.
	PARA_UCORR as Parameter ID: • empty (default)
	Consider configuration referred to SAP note 944778 at the length correc- tion of OTF data streams.
	• X Always execute the length correction in ST commands of OTF data streams.
	Default: See above
Short Descrip- tion	Short Description contains an explanation of the parameter.
	The value is a string:
	Purpose
	Default: None

10 Changes

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

This chapter deals with the following topics:

- \rightarrow Changes with Release 1.4.2, Page 158
- \rightarrow Changes with Release 1.4.1, Page 159
- ightarrow Changes with Release 1.4.0, Page 160
- \rightarrow Changes with Release 1.3.5, Page 161
- \rightarrow Changes with Release 1.3.3, Page 162
- \rightarrow Changes with Release 1.3.2, Page 163
- \rightarrow Changes with Release 1.3.1, Page 164
- \rightarrow Changes with Release 1.3.0, Page 165
- \rightarrow Changes with Release 1.2.8, Page 166
- \rightarrow Changes with Release 1.2.6, Page 167
- \rightarrow Changes with Release 1.2.5, Page 168
- \rightarrow Changes with Release 1.2.4, Page 169

in this chapter

logging	 The values for SEAL_TRACE in the saprfc.ini file have been extended with the following functionality: Ø No additional information in the log file 1 Sets the level of the log file: java.util.logging.FileHandler.level=ALL Also writes function list, environment variables, connection status to the log file Sets FTP_TRACE=2, HTTP_TRACE=2 Start sapftp/saphttp with -t 2 Writes additional HTML files with the transferred data Writes additional TLS information for URLs with https to the log file 3 Also writes Java memory status to the log file
sapftp/saphttp with SNC	 In addition to the dynamic RFC destinations, static RFC destinations are also supported. Static RFC destinations offer the following advantages: SNC is supported for sapftp/saphttp Static RFC destinations can be explicitly enabled/restricted at the gateway.
central SAP gate- way (ASCS)	 The static RFC destination supports the use of a central SAP gateway (ASCS). This offers the following advantages: SNC is supported for sapftp/saphttp Connections via local gateways can be blocked, which increases security.

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

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

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

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.

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

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

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 cadrfc.ini (this infor-
	mation 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 SEAL_TRACE parameter in the saprfc.ini file.

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

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!

The sap_conn_checker program is provided to evaluate SAP system data. sap_conn_check-

sap_conn_check
er

start depending on the current server. cfg depending on the current server.

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

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 \rightarrow refer to other terms in this section.

Customizing

Configuring the SAP system

cv04, cv04n

 \rightarrow 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 \rightarrow document information records and their assigned files are managed.

Document information record

A master record in the \rightarrow 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 /seal/, /sealc/ (for customer development) or /dvsrepro/ (old).

Transaction

Means of executing programs

Transaction code

Identifier naming a \rightarrow 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	
FIP	File Transfer Protocol	
055		
033	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 155

A

ABAP 172 ABAP_DEBUG 50, 135 Action 10 ACTIVE 147 Aktivierungsart 27 ASCS 144 ASHOST 125

B

Benutzername 153

С

CAD_CHECKOUT_DLL 51 CadDialogNetAddress 115 cadrfc.ini 104 CadRfcClient 112 CadRfcDestination 114 CadRfcLanguage 113 CadRfcPassword 110 CadRfcPasswordCoded 111 CadRfcUser 109 CODEPAGE 138 convservdpfstart 40 convservstart 40 CPIC* 133

D

DEST 123 DESTINATIONS 148 dev_jco_rfc.log 54 dev_rfc* 133 DISPLAY 115 DMS 172 DPF® 172 dvsstart 40 dvsviewserverstart 40

F

filecheckstart 40 FTP 172

G

Gateway-Host 25, 48 Gateway-Service 25, 48 GROUP 129 GWHOST 130 GWSERV 131

н

HOSTNAME 115

J

jco_rfc*.trc 133 jco_rfcPID_UUID.trc 54 jrfcserverstart 40

K

Kommunikationsart mit dem Zielsystem 28 Kurzbeschreibung 156

L

Logon Benutzer 109 Passwort unverschlüsselt 110

Μ

ModuleGlobal 10 ModuleSelect 10 MSHOST 127

0

oms_server 107 omscli 107 OSS 172 OTFCODEPAGE 149

Ρ

PARA_DDEST 156 PARA_GWHSB 156 PARA_GWHST 156 PARA_UCORR 156 Parameter-Id 155 Parameterwert 156 PDF 172 PDF/A 172 Pfadpräfx 74 PLM 172 PLOSSYS® 172 plsstart 40 PROGID 149 Programm ID 27 proxyinfo 29

R

R3NAME 128

reginfo 29 RFC 172 RFC_TRACE 50, 133 rfcserver.cfg 146 rfcserverstart 40 RLIGATE 149, 150 rlistsap 107 rswf_test_http 97

S

sap_conn_checker 118 sapcli 107 sapftp 19 sapftp.dll 51 SAPGUILandscape.xml 118 saphttp 19 saphttp.dll 51 saprfc.ini 116 **SAPROUTER 132** SEAL TRACE 134 sealencrypt 111 secinfo 29 Servicenummer 74 smicm 98 SNC MODE 139 SNC MYNAME 140 **SNC PARTNERNAME 141** SNC QOP 142 SNC_SSO 143 SYSNR 126 sysstart 40

T

TYPE 124

U

UNICODE 19, 137 USE_GWHOST 155 USE_SAPGUI 109, 136

Х

X509CERT 145 XMS 150 XMX 150

Z

Zeichenbreite im Zielsystem 28 Zielmaschine 74

Index

A

application server determine host name, USE_GWHOST 52 load balancing 48

B

basic authentication activate SAP 75 server 70

С

check-out error, determine host name 52 client 171 code page 138 Conversion Server, explicit 28 RFC Server, explicit 28 configuration SAP basic authentication, activate 75 SAP as consumer Web service 89 SAP as provider Web service 79 server 18 basic authentication, activate 70 PSE, create 69 configuration file overview 15 **Conversion Server 119** sm59 code page, explicit 28 non-Unicode 28 customizing 171 cv<xx>, cv<xx>n 171 cv04, cv04n 171

D

debug Web service request SAP as provider 88 requirement 80, 90 debugging system functions 50 developer license 171 dialog user 109 directory convention at the specification 8

repro list processing 149 **DLL** variant requirement 51 DMS 171 DMS Loader 119 DMS Loader/ABAP 119 **DMS** Repro requirement USE SAPGUI 136 DMS Rlist 119 restriction - system/client-spec. logon 107 DMS Scan 119 requirement USE SAPGUI 136 DMS View Server 119 Document information record 171 document management system 171 document, see document information record

E

error debugging, activate 135 proceeding, advisable 97 **RFC** destination SAP gateway logging, activate 53 trace message activate 50 trace message, activate 54, 133 starting the RFC server 40 system function, debugging 50 typical 99 typical problem 45 Web service SAP as consumer check 97 trace message display 98 SAP as provider debug request 88 record requests 87 trace message, activate 87

G

gateway central configure 65 requirement 65 restriction 65 saprfc.ini, example 65 local/central 7 settings for load balancing 48

H HTTP connection connection type 73 create 72 RFC destination 73 HTTPS see SAP_BASECONF_SNC_TEC 7

J

JRFC Server 119 configuration file 146 sm59 Unicode 28 JSAPcli 119

L

language at logon 113 on connection establishment, supported 113 load balancing between application server 48 gateway options 48 log file connection status, requirement 134 memory status, requirement 134 logon client 112 configuration 104 language 113 password coded 111 requirement 109 requirement - system/client-spec. user 107 restriction - system/client-spec. logon 107 system/client-spec. user 107

Μ

memory maximum 150 minimum at start 150 status log, requirement 134 message server load balancing for RFC clients 7 requirement 19 SAProuter 124 saprfc.ini, example 23 MTOM requirement 96

Ν

namespace 171

naming convention 171

0

OTF length correction in ST commands 156 overview configuration files 15 HTTP connection, create 72 RFC client/RFC server 119 RFC destination on SAP systems as of 4.7 24

Ρ

parallel processing 149 password coded 111 path specification, convention 8 PDF Icon zur einfachen Navigation aktivieren, ab Adobe Reader 10 9 PDF Longlife Suite - SAP Integration 119 PSE create, server 69

R

registration 40 registration, see logon repro list processing directory 149 requirement cadrfc.ini 104 connection status, log 134 debug Web service request SAP as provider 80, 90 DLL variant 51 DMS Repro 136 DMS Scan 136 gateway central 65 logon 109 memory status, log 134 message server 19 SAProuter 124 **MTOM 96** saprfc.ini 116 SAProuter message server 124 system/client-spec. logon 107 Unicode - separate section in rfcserver.cfg 148 Web service roles with authorizations 80, 90

restriction

gateway central 65 system/client-spec. logon 107 RFC client 119 **RFC** destination allow alternatives 29 prefix for secinfo/reginfo, specify 37 reginfo 31 >= NW 7.45 31 secinfo 33 >= NW 7.45 33 simulation mode 36 configuration on SAP systems as of 4.7 24 connection type 25 data, overview 15 logon data 104 RFC connection 25 SAP gateway logging, activate 53 SAP system data 116 security configuration 29 start 39 via ACTIVE section 41 via call parameters 42 static sapftp/saphttp destination, see static sapftp/saphttp destination status log, requirement 134 test 43 trace message activate 50, 54, 133 type 119 RFC Server 119 sm59 code page, explicit 28 non-Unicode 28 RFC server 119 error during start 40 saprfc.ini, example, saprfc.ini example RFC server 22 **RFF** client saprfc.ini, example, saprfc.ini example RFC client 21

S

SAP system data configuration 116 SAP system data

identify 118 SAPcli 119 sapftp activate trace message 55 saphttp activate trace message 55 saprfc.ini example gateway, central 65 message server 23 SAProuter requirement message server 124 server configuration 18 SNC activation sign 139 name of the communication partner 141 name of the user 140 quality of protection 142, 143 see SAP_BASECONF_SNC_TEC 7 SSO deactivate SNC SSO 143 see SAP_BASECONF_SNC_TEC 7 static sapftp/saphttp destination template, assign RFC client 63 RFC server 64 template, copy 60 template, establish 57 system user 109

Т

thread maximum number 149 timeout Web service 99 trace message display Web service SAP as consumer display 98 transaction 171 transaction code 171 transport 171

U

Unicode code page 138 configuration 19, 137 requirement - message server 19

```
requirement - separate section in rfcserv-
er.cfg 148
requirement - wrapper program 19
USE_GWHOST
parameter value, specify 155
```

V

variable Action 10 ModuleGlobal 10 ModuleSelect 10

W

Web service requirement roles with authorizations 80, 90 SAP as consumer ABAP proxy, select 92 check 97 configuration 89 large amounts of data, optimize transfer with MTOM 96 logical port, create 93 suppress message ID transfer 95 trace, display 98 SAP as provider binding, create 83 configuration 79 debug request 88 requests, record 87 service, select 82 trace, activate 87 URL, determine 85 timeout 99 wrapper program sapftp/saphttp for Unicode 19 digital signature 163